



Cisco TelePresence MCU 5300 Series

Printable Online Help

4.5(1.45)

15087

June 2014

Contents

Using the web interface	9
Logging into the web interface	10
Failing to log into the web interface	11
Joining and viewing conferences	12
Calling into conferences	13
Dialing in using a video endpoint	13
Dialing in using an audio-only phone	13
Using an auto attendant	15
Calling an auto attendant	15
Accessing the auto attendant	15
Participating in the conference	16
Leaving a conference	16
Using in-conference features from video endpoints	17
Controlling conference views	17
Understanding participants' status	18
Using far-end camera controls	19
Understanding in-conference status icons	20
The In call "*" menu	20
The conference welcome message	20
Being invited into a conference	22
Understanding how participants display in layout views	23
Big panes vs. small panes	23
Participants viewing themselves	24
Changing view focus	24
"Important" participants	24
"Important" participants combined with view focus	24
Clipped panes	25
Video stream vs. fixed bitmap images	26
Muted participants	26
Automatic lecture mode	26

H.243 floor and chair control	27
Managing conferences	29
Displaying conference lists	30
Active conferences	30
Scheduled conferences	32
Completed conferences	33
Adding and updating conferences	34
Adding a conference	34
Updating a conference	34
Ad hoc conferences	34
Adding configured endpoints	50
Using IDs and PINs	50
Using conference templates	51
Conference ownership	52
Reservation of MCU media ports	54
Content channel video support	57
Controlling in-conference features	64
Adding participants	64
Customizing layout views	65
Displaying conference statistics	68
Sending messages to all participants	70
Managing participants	71
Viewing the conference participant list	71
Customizing a participant's layout view	82
Controlling an active participant's camera	84
Viewing and adjusting a participant's audio levels	86
Selecting a custom participant view	87
Displaying statistics for a participant	88
Sending messages to individual participants	94
Sending DTMF to an audio bridge	95
Displaying diagnostics for a participant	95

Moving a participant	96
Creating auto attendants	97
Displaying the auto attendant list	97
Adding and updating an auto attendant	98
Adding a custom auto attendant banner	100
Managing endpoints	102
Displaying the endpoint list	103
Configuring H.323 endpoints	104
Configuring SIP endpoints	114
Managing gateways	125
Managing the built-in gatekeeper	126
Managing users	127
System defined users	128
User privilege levels	129
Displaying the user list	131
Deleting users	131
Adding and updating users	132
Adding a user	132
Updating a user	132
Updating your user profile	135
Changing your password	137
Configuring network and system settings	138
Configuring network settings	139
IP configuration settings	139
IP status	140
Ethernet configuration	140
Ethernet status	141
Automatic IPv6 address preferences	143
Configuring DNS settings	144
Viewing DNS status	144
Configuring IP routes settings	146

Port preferences	146
IP routes configuration	146
Configuring IP services	149
Configuring SNMP settings	151
System information	151
Configured trap receivers	151
Access control	152
Configuring QoS settings	153
QoS tags	153
Configuring the MCU	155
Displaying and resetting system time	156
System time	156
NTP	156
Configuring global conference settings	158
Conference settings	158
Advanced settings	162
Configuring encryption settings	172
Using encryption with SIP	173
Configuring H.323 gatekeeper settings	175
Gatekeeper settings	175
Gatekeeper status	178
Displaying active gatekeeper registrations	180
Configuring SIP settings	181
Configuring content settings	183
Media port settings and clustering	185
Clustering MCUs	185
Configuring the media port mode	186
Selected option	186
Upgrading and backing up the MCU	188
Upgrading the main MCU software image	188
Backing up and restoring the configuration	188

Enabling MCU features	189
Shutting down and restarting the MCU	190
Configuring security settings	191
Hashing passwords	191
Security settings	191
Serial console settings	191
Usage recommendations for advanced account security	192
Displaying system status	194
Displaying general status	195
Displaying conference status	197
Conference status	197
Video status	198
Audio status	199
Conference content channel	200
Preview	200
Received video	200
Transmitted video	200
Diagnostics	200
Displaying hardware health status	201
Displaying security status	202
Displaying cluster status	203
Displaying the cluster status of a master MCU	203
Displaying the cluster status on a slave MCU	204
MCU port matrix	206
Advanced topics	207
Working with the event logs	208
Event log	208
H.323/SIP log	209
Audit log	209
Call Detail Records	209
Working with the audit logs	210

Audit log	210
Using Call Home	211
Understanding security warnings	213
Logging using syslog	216
Syslog settings	216
Using syslog	217
SIP: Advanced	219
SIP implementation	219
Authentication details	219
Working with Call Detail Records	220
Call Detail Record log controls	220
Call Detail Record log	220
Feedback receivers	223
Customizing the user interface	224
Configuring user interface settings	224
Controlling the availability of public pages	225
Configuring welcome messages for the Login and Home pages	226
Adding headers and footers	226
Customizing voice prompts on the MCU	226
Voice prompt specification	230
Customizing auto attendant and text overlay font	231
Customization: More information	232
The factory default file set	232
Localization files	232
Customization files	232
Network connectivity testing	233
Configuring SSL certificates	234
Prerequisites	234
Managing the local certificate	235
Managing trust stores	235
Configuring SIP TLS verification	236

Configuring HTTPS verification	237
OCSP checks for client certificate revocation	238
Certificate details reference	240
Transitioning to certificate-based security	241
Enabling client certificates and certificate login (HTTPS connections)	241
Enabling OCSP checking	241
Requiring certificate-only login (all connections)	242
Further information	244

Using the web interface

Logging into the web interface	10
Failing to log into the web interface	11

Logging into the web interface

The MCU web interface is used for administering the MCU device, managing conferences, users, and pre-defined endpoints. You can also perform many conference-related tasks using the web interface that you cannot otherwise do.

When connecting to the MCU web interface, you must log in so that the MCU can associate the session with your configured user and a set of access privileges. The MCU has a set of configured users, and each user has a username and password that are used for logging in.

1. Using a web browser, enter the host name or IP address of the MCU.
2. To log in, click **Log in** and enter your assigned **Username** and **Password**.
3. Click **OK**

The main menu appears, restricting the available options based on your access privileges. Administrators have full access; standard users can create new conferences and manage their profiles; guest users typically can access publicly available conferences.

The **Login** page of the MCU displays a welcome banner which administrators can configure to display text relevant to your organization. For more information, refer to [Customizing the user interface](#).

Related topics

- [Failing to log into the web interface](#)

Failing to log into the web interface

When connecting to the MCU web interface, you must log in so that the MCU can associate the session with your configured user and a set of access privileges. The MCU has a set of configured users, and each user has an ID and password that are used for logging in.

The MCU does not support access via browsers that have cookies disabled. Check that your browser has cookies enabled if you are having trouble logging in.

If you see the **Access denied** page, you have not been able to log in for one of the following reasons:

- **Invalid username/password:** you have typed the incorrect username or password.
If Advanced account security mode is enabled and you incorrectly type the username or password three times and, if this is an administrator account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the **User** page)
- **No free sessions:** the maximum number of sessions allowed simultaneously on the MCU has been exceeded
- **Your IP address does not match that of the browser cookie you supplied:** try deleting your cookies and log in again
- **You do not have access rights to view this page:** you do not have the access rights necessary to view the page that you attempted to see
- **Page expired:** the **Change password** page can expire if the MCU is not entirely happy that the user who requested to change password, is actually the user submitting the change password request. (This may happen if you use a new browser tab to submit the request.)

Related topics

- [Configuring security settings](#)

Joining and viewing conferences

Calling into conferences	13
Using an auto attendant	15
Using in-conference features from video endpoints	17
Being invited into a conference	22
Understanding how participants display in layout views	23

Calling into conferences

Depending on how your system administrator has configured the MCU and conferences on it, you might be able to join conferences by simply dialing a phone number.

Dialing in using a video endpoint

Your system administrator may have configured the MCU to allow you to use your video endpoint to directly dial the conference by dialing a phone number. You will be required to enter the conference ID, and PIN if required. Or you may be able to dial by IP address and connect to the auto attendant. See [Using an auto attendant](#) for details.

Note that some video endpoints require that you activate the keypad before dialing. For example, you might need to press the # key.

Dialing in using an audio-only phone

If your phone system allows calls to the MCU, you may use your regular phone to join conferences as an audio-only contributor. You may need to enter the conference ID (and PIN, if required).

If your regular phone number is linked to your video endpoint, then when you use your phone to join a conference, the video portion of the conference will automatically appear on your video endpoint's screen. You can continue to use your regular phone for the audio portion of the conference. To do this, the video endpoint must be configured as that user's **associated video endpoint**. For more information, refer to [Adding and updating users](#).

The advantages to this method are that you are able to use the same method and phone to make video calls as you do traditional audio calls. You also may have improved audio signaling. However, this method requires significant configuration and setup from the system administrator. Your company's network may not have all the components available to support this method.

When in a conference using an audio-only phone, pressing *6 mutes your phone such that you will not be contributing audio to the conference; pressing *6 again unmutes your phone.

Using an IP VCR recording as the video contribution

Audio-only conference participants can show a recording from an IP VCR as their video contribution. To do this:

1. Register the MCU and the IP VCR with the gatekeeper.
2. Go to **Endpoints > Add H.323 endpoint** and add the recording as an H.323 endpoint.
3. Set the address as the recording number.
4. Go to **Users > Add user** and set up the user using [Adding and updating users](#) for more information and setting the **associated video endpoint** as the IP VCR recording.

Related topics

- [Displaying conference lists](#)
- [Using an auto attendant](#)
- [Using in-conference features with video endpoints](#)

- [Being invited to a conference](#)
- [Understanding how participants display in layout views](#)
- [Configuring H.323 endpoints](#)
- [Configuring SIP endpoints](#)
- [Adding and updating users](#)

Using an auto attendant

Your system administrator may have set up an auto attendant for you to use to join conferences. An auto attendant presents you with a series of menus from which you can choose a conference to join.

For further information about accessing conferences (including the use of DTMF tones), refer to [Cisco TelePresence Accessing Conferences Getting started guide MCU 4.3](#) in the product documentation area of the Cisco website.

Calling an auto attendant

There are typically two ways to call an auto attendant using your video endpoint. Your system administrator should provide you with information about which method you should use:

- Enter the IP address or host name of the MCU device
- Dial using a standard E.164 phone number

Accessing the auto attendant

When you successfully connect to the MCU, the auto attendant menu displays on your video screen, and you should also hear the audio instructions.

Navigate the auto attendant using the far-end camera controls (FECC) on your video endpoint. Use the up and down controls to highlight the option or item you require; use right to make your selection. To return to a previous menu from a sub-menu, use left.

You can jump to the end of the menu when at the start by using the up control; similarly, you will loop back to the start if you are at the end and use the down control. Note that there is a scroll bar in the bottom right of the video display to indicate where you are in the auto attendant menu. From anywhere in the menu, you can jump to the first entry by entering #2 on the keypad or to the last entry by entering #8.

By default, you join a conference by dialing the conference's numeric ID with the number keys on your endpoint and following it with a '#'. If a conference has both a **Numeric ID** and a **Guest numeric ID** set, you may enter either ID, and will join the conference as either a chairperson or guest as appropriate. As you start to enter a numeric ID, the sequence you have typed will be shown at the base of the auto attendant screen.

You may cancel the numeric ID entry (for instance to correct an error) by pressing '*'.

If you have connected to the auto attendant using an endpoint that has no FECC capability (for example many SIP endpoints), you can use the number keys on your endpoint to navigate the menus; this is called "DTMF navigation mode". DTMF navigation mode enables you to use the number keys: 2, 4, 6, and 8 in the place of up, left, right, and down respectively.

When in DTMF navigation mode, you will not be able to use the number keys to enter the numeric ID of a conference.

To toggle DTMF navigation mode:

- On first connecting to the auto attendant, press ##.
The message "DTMF menu navigation enabled" appears briefly at the bottom of the auto attendant display.
- When you've finished your navigation sequence, press ## to exit DTMF navigation mode.

The message "DTMF menu navigation disabled" appears briefly at the bottom of the auto attendant display.

Typically, you will have these options on the auto attendant:

Create new conference

This option enables you to start a new conference that takes place immediately (an "ad hoc" conference).

When you create this type of conference, you'll need to add a conference ID and you can choose to set a PIN (to restrict access to the conference). If you don't want a PIN, press # when prompted for a new conference PIN.

Other participants can then join the new conference as they would any other; by using the auto attendant or by calling in directly (see [Calling into conferences](#)).

As the system administrator, you can disable this option if you do not want users to be able to create conferences via the auto attendant.

Join a conference

Currently active or scheduled conferences may be listed here by conference name. Select the conference name to join the conference.

If the conference you want to join is not displayed, verify the auto attendant number, the conference name, and the start time, and verify that the system administrator has enabled the conference listing on the auto attendant.

Access other auto attendant menus

Your system administrator may link this auto attendant to other auto attendants, giving you access to additional conferences.

Participating in the conference

After you join a conference, the in-conference controls and features are the same regardless of how you joined the conference (see [Using in-conference features](#)).

Leaving a conference

When you want to leave a conference, you can either hang up or, if you want to return to the auto attendant, press *. Pressing * brings up the in call menu where you can press 1 to select **My actions** then 4 to select **Return to auto attendant**.

Related topics

- [Displaying conference lists](#)
- [Calling into conferences](#)
- Watching conferences (streaming)
- [Using in-conference features](#)
- [Being invited into a conference](#)

Using in-conference features from video endpoints

After you join a conference, you can control many conference features directly from your video endpoint. (For information about in-conference features using the web interface, see [Controlling in-conference features](#).)

- [Controlling conference views](#)
- [Understanding participants status](#)
- [Using far-end camera controls](#)
- [Understanding in-conference status icons](#)
- [The In call "*" menu](#)
- [The conference welcome message](#)

For further information about accessing conferences (including the use of DTMF tones), refer to the [MCU Accessing Conferences Getting started guide](#).

Controlling conference views

Your video endpoint typically has navigation keys, such as up/down and left/right (on a keyboard or remote control), that allow you to control the camera viewing angles. When connected to a conference, you can also use these controls to scroll through participants and conference layout formats (see [Understanding how participants display in layout views](#)).

Understanding conference views

When you join a conference, you will have a set of available layout options from which you can choose to display the conference participants. Typically you can choose from two primary groupings of layouts:

- **Same-size panes** — in these formats, all conference participants display in the same size pane on the video screen and thus have the same level of focus or importance. For example, a conference with four participants might display each in a pane sized to be a quarter (1/4) the size of your video screen.
- **Variable-size panes** — in these formats, conference participants display in various pane sizes on the video screen depending on their 'importance'. For example, a layout might display the participant who is speaking in a pane larger than the other conference participants. Or, you might choose to focus on a particular participant (see [Selecting participants](#)).

Choosing a conference view

To switch among available conference views:

1. Change the camera control to "far".
2. Use the up/down navigation keys to toggle through the available format options.
3. Refer to the table below for assistance interpreting the icons that appear on-screen.

Icon	Icon description
------	------------------



You are scrolling up through the layout views.



You are scrolling down through the layout views.






You have stopped scrolling through the layout views.

Selecting participants


When viewing a conference with variable-size panes (see [Variable-size panes](#)), you can choose which participant to display in the larger panes on the video screen; when viewing a conference with equal-sized panes, you can choose which participant displays in the top left pane. You do this by selecting the participant following these steps:





1. Change the camera control to "far".
2. Select a layout view.
3. Use the left/right navigation keys to scroll through the focused participants.
4. Refer to the table below for assistance interpreting the icons that appear on-screen.

Icon	Icon description
	You are scrolling through the participant list in a counter-clockwise direction.
	You are scrolling through the participant list in a clockwise direction.
	Speaking participant has the focus.

Understanding participants' status

During the conference, various icons might appear in the pane of specific participants. Refer to the table below for assistance interpreting these icons.







Icon	Icon description
	<p>This participant has been given priority in the layout views.</p> <p>A participant is made "important" using controls on the MCU web pages.</p>

	The audio quality from this participant is poor.
	The audio quality from this participant is good.
	The video quality from this participant is poor.
	The video quality from this participant is good.

Using far-end camera controls

While in a conference, you might need to change the camera settings for one of the conference participants. For example, if you want to zoom in on a particular speaker in a large group, or if you cannot see the speaker. To do this:

1. Change the camera control to "far".
2. Select the largest displayed participant pane.
3. Press Zoom. The far-end camera control icon appears, and you can now control the far-end camera.
4. Refer to the table below for assistance interpreting the icons that appear on-screen.




Icon	Icon description
	You are now controlling the viewing angle of the far-end video camera.
	You are moving the remote far-end camera down.
	You are moving the far-end video camera up.
	You are moving the far-end video camera to the left.
	You are moving the far-end video camera to the right.
	You are zooming in with the far-end video camera.



You are zooming out with the far-end video camera.

Understanding in-conference status icons

During the conference, various icons might appear in top left of the conference display. The appearance of these icons is controlled on the **Settings > Conferences** page (refer to [Configuring global conference settings](#)). Refer to the table below for assistance interpreting these icons.

Icon	Icon description
	There are both encrypted and unencrypted participants in this conference.
	This conference is being recorded.
	There are audio-only participants in this conference. The number of audio-only participants is displayed next to the icon.

The In call "*" menu

The In call "*" menu provides access to a number of in-conference options. Access the In call "*" main menu by pressing * on your numeric keypad:

- My actions - for local audio, video, floor control and layout options
- Participants - for participant list and, if authorized, to change the audio, video, and floor assignment of other participants.
- Conference actions - if authorized, for locking / unlocking the conference, adding a participant, or disconnecting all.
- Conference settings - if authorized, for adding / editing chair and guest PINs
- Mute my audio

A full reference to the in call menu features is in the [MCU Accessing Conferences Getting started guide](#).

The conference welcome message

You can configure a welcome message on the MCU and a duration for that message. Participants joining a conference on the MCU will see the message displayed at the bottom of their endpoint's display. After the configured message duration has elapsed, the message will be removed.

The **Conference welcome message** controls are on the **Settings > Conferences** page (refer to [Configuring global conference settings](#)).

If you change the welcome message when there are active participants, any participants' currently displayed welcome messages will only change if the new message is configured as *permanent*.

Related topics

- [Displaying conference lists](#)
- [Calling into conferences](#)
- [Using an auto attendant](#)
- [Being invited to a conference](#)
- [Understanding how participants display in layout views](#)
- [Configuring global conference settings](#)

Being invited into a conference

Depending on how your video endpoint is configured, an incoming video call might come through to your regular phone or to your video endpoint (see [Calling into conferences](#) for a brief description of the difference). Note that even if a video call arrives on your regular phone, the video portion of the call will appear on your associated video endpoint (if one is configured).

As with any other type of incoming call, you can choose to answer the call or not.

Related topics

- [Displaying conference lists](#)
- [Calling into conferences](#)
- [Using an auto attendant](#)
- [Using in-conference features with video endpoints](#)
- [Understanding how participants display in layout views](#)

Understanding how participants display in layout views

The default behavior of the MCU is to display the "loudest" participants in the most prominent layout panes. If there are more contributors than there are panes available, then the "quietest" participants are not shown.

However, different styles of layout introduce slight subtleties to this behavior, and in addition there are a few ways in which participants or conference administrators may change the system used for pane assignment. In particular, you may want to set the [pane placement](#) for a conference yourself.

On this page:

- [Big panes vs. small panes](#)
- [Participants viewing themselves](#)
- [Changing view focus](#)
- ["Important" participants](#)
- ["Important" participants combined with view focus](#)
- [Clipped panes](#)
- [Video streams vs. fixed bitmap images](#)
- [Muted participants](#)
- [Automatic lecture mode](#)
- [H.243 floor control](#)

Big panes vs. small panes



This layout can be seen as the most traditional video-conferencing view. Each participant is displayed in the same sized pane as the other participants. If there are more than four participants, the four most significant (the four loudest) are displayed, with one pane each.



By contrast, these example layouts have some larger panes, and the participants shown in those panes are seen as more significant than the other contributors. When allocating participants to panes, the MCU always fills the largest panes first. If there are more participants than panes then there will never be empty big panes and non-empty small panes.

To reduce the number of view changes when different participants speak (for example, when people change from being active speakers to inactive contributors), the MCU duplicates participant views for layouts with more than four small panes. For the three example layouts shown above, the participant(s) shown in the large pane(s) of the first two layouts will be duplicated in the surrounding small panes. However, the four small panes of the third layout will show different participants to those displayed in the three big panes. This reduces the impact of audio volume changes on the composed layout while not needlessly wasting view space. However, it is possible to configure the MCU not to duplicate participant views in this way if so desired (see [Configuring global conference settings](#)).

Participants viewing themselves

When considering which participants to show in which panes, a participant's self view has the lowest priority. This has two main implications:

- **Participant pane selection**

When choosing participants to display, the MCU considers the viewer last. This prevents the participant who is the active speaker from seeing only themselves. In this case, while everyone else will see the active speaker, the active speaker will see the previous active speaker in their biggest view pane.

- **View family layout selection**

When the MCU is required to choose a layout from a view family, it does so based on the number of video contributors to the conference. However, when calculating the number of video contributors for a particular view, the MCU does not consider any video stream being received from the viewer.

Thus, with five participants in a conference and everyone seeing the standard equal-sized view family (2x2, 3x3 or 4x4), each of the five contributing participants will always see the 2x2 view with themselves excluded.

You may configure the MCU never to show participants their own video stream in small panes (see [Configuring global conference settings](#)). If this is the case, then participants viewing layouts with some panes larger than others will never see their own video stream in any of the small panes, even if there are free slots. They may still appear in large panes, for example if the view focus is manually changed to show their video.

Changing view focus

Using the tilt (up and down) far-end camera controls on a connected video endpoint causes the view to change, cycling through the available families and then the conference-wide or per-participant custom layouts (if enabled).

In addition, the pan (left and right) far-end camera controls on a connected video endpoint can be used to focus the view on a particular participant, as opposed to the MCU allocating participants to panes based solely on the volume of the audio being received from them.

To reduce the disruption of the view when cycling through conference participants, there is a short delay after selecting a new focused participant before the rest of the view layout reverts to the "correct" arrangement of participants in panes.

"Important" participants

For each conference, one active participant can be set as "important". This means that the MCU considers this participant first when deciding which contributors to show in which layout panes, rather than their position in the list being set by how loudly they are speaking. See the [Control](#) setting in the [conference participant list](#).

"Important" participants combined with view focus

Both "Changing view focus" and "Important participants" above involve a single specific participant being shown in the biggest pane available, even if that participant is not currently the loudest speaker. This causes a potential conflict, which is resolved dependant on the type of layout.



In this type of view (a layout in which all panes are of equal size), the focused participant is shown in the first pane, the one at the top left. The important participant is shown in the "next" pane, normally the one immediately to the right of the first pane.



This type of layout displays a single big pane and several small panes. If the view focus has been changed (for instance with left and right far-end camera control operations), then the big pane shows the selected participant. If a conference participant has been set to "important" then its video stream is shown in one of the small panes.

However, if a participant has been set to "important" *and* the view is focused on a (different) specific participant, the focused participant is shown in the big pane, and the "important" participant is shown in one of the small panes.

If the view has been focused on a participant and the same participant is also set as "important" then that participant is shown in the big pane.



These layouts have two large panes and several smaller ones. If the view focus has been changed (for instance with left and right far-end camera control operations), then the upper or left large pane shows the focused participant. If a participant has been set to "important" then that video stream appears in the lower or right large pane.

If the same participant is focused *and* "important", that video stream appears in the upper or left pane.



For these layouts, if the view has been focused on a particular participant, that participant appears in the upper or left large pane. If a participant has been selected as "important", that participant will be shown in the lower or right large pane.

In layouts with three large panes, even if the view is focused on a specific participant and another has been set to "important", one large pane remains. This pane displays the "loudest" remaining participant.

Clipped panes

The majority of the conference layouts defined by the MCU, for example:



have in common that all of their panes, whether big or small, have the same aspect ratio as the view itself. That is, the panes' widths and heights are in the same proportion as the width and height of the encompassing view.

By comparison, there are some defined conference layouts, for example:



in which this aspect ratio preservation does not occur. In these cases, the MCU scales the participant video stream according to the larger dimension of the pane.

For example, in the layout to the left, the size of the top left pane is one half of the view width and two thirds of the view height. Because two thirds is greater than one half, the MCU scales the participant video stream to two thirds of its size and thus a small amount of the left and right of the original image will not appear in the final composed layout.

Video stream vs. fixed bitmap images

For video conference participants, the image that displays in the layout view pane is either the live video stream (if viewing from the video endpoint) or a captured video image from the current video stream (if viewing from the web interface).

However, audio-only participants do not have any associated video to display. Instead, you can assign a fixed image (in bitmap format) to a specific participant. When the participant joins a conference as an audio-only participant, this image appears in the layout pane. To enable this feature, the participant must be added as a user to the MCU, have an associated E.164 telephone, and have a designated image file uploaded. See [Adding and updating users](#).

Muted participants

Audio mute

Participants who have had their audio muted from the web interface do not contribute audio to the conference. Additionally, muted participants are not considered when the MCU calculates the loudest speakers to display in the largest panes, even if the participant had previously been in one of those positions.

Note that other participants will not have an indication that a participant has been muted. They simply will no longer hear that participant speaking.

Video mute

Participants who have had their video muted from the web interface do not contribute video to the conference. They will continue to contribute audio as normal, unless it is muted separately.

Automatic lecture mode

Automatic lecture mode allows a lecturer to be shown in full-screen view to the students. In this mode, the lecturer will continue to see the normal (continuous presence) view. That is, the lecturer will see the students and not himself. When **Automatic lecture mode** is enabled for a conference, the MCU identifies the loudest speaker as the lecturer. If you have configured a custom layout for the lecturer, that will override the normal continuous presence view. For the other participants (the students), the view of the lecturer (the loudest speaker) overrides any custom layout. You can enable automatic lecture mode for scheduled and/or ad hoc conferences either in the conference configuration or in the relevant conference template.

See [Adding and updating conferences](#) for details of how to configure automatic lecture mode.

H.243 floor and chair control

Some H.323 endpoints support a feature known as floor and chair control that is encompassed by the H.243 protocol. This is not currently supported by SIP.

The MCU supports the following H.243 features:

- a participant can "take the floor" in a conference. On "taking the floor" their video contribution is sent to all conference participants as a "1 x 1 view" (full-screen view). If the active floor (temporarily or permanently) has no video channel established to the MCU then endpoints will see their "normal" continuous presence view; if there is a video channel from the active floor participant, everyone will see that video (except for the person who currently has the floor), and this will override any view family or custom layout setting
- a participant can "take the chair". On "taking the chair", a participant can:
 - nominate a "broadcaster"; that is, they can choose which participant's video will be sent to all other participants in "1 x 1 view" (full-screen view)
 - decide to disconnect any other participant(s)
 - end the conference

Note that the ability of a participant to "take the chair" is affected by how they joined the conference. A participant who joined the conference as a guest will not be able to "take the chair".

- an endpoint can receive the names of the other endpoints in the same conference. Different endpoints act on this in different ways.

Whether or not these features are supported in a conference depends on the individual conference settings (**Conference > Add conference**). Refer to [Adding and updating conferences](#).

Where a conference supports floor and chair control, or floor control only:

- the MCU will advertise the ability to handle H.243 when establishing (and receiving) H.323 connections
- any H.243-capable endpoint can request the floor, and all endpoints (be they chairperson or guest) will be granted it as long as no other endpoint in that conference has already done so

Where the conference supports floor and chair control:

- any H.243-capable endpoint can request the chair, and any participant who has joined the conference as a chairperson will be granted it as long as no other endpoint in that conference has already done so

If an active participant in a conference has taken the chair or the floor, it is indicated in the status column of the **Participant list** page.

If you change the **Floor and chair control** for a conference currently taking place, there will be no immediate effect. That is, an existing floor or chair participant will not have that status removed.

For ad hoc conferences, you can alter the **Floor and chair control** setting, which is *Allow floor control only* by default, through that conference's configuration page when it is active.

Related topics

- [Customizing layout views](#)
- [Customizing a participant's layout view](#)

- [Viewing the conference participant list](#)
- [Selecting a custom participant view](#)

Managing conferences

Displaying conference lists	30
Adding and updating conferences	34
Controlling in-conference features	64
Managing participants	71
Creating auto attendants	97

Displaying conference lists

The **Conference List** displays information about active, scheduled, and completed conferences. To access this list, choose **Conferences**.

By default, the **Conference List** is accessible by all users (even those who have not logged into the MCU). However, administrators can disable public access to this list. To do so, go to **Settings > User interface**.

On this page:

- [Active conferences](#)
- [Scheduled conferences](#)
- [Completed conferences](#)

Active conferences

Active conferences are currently in progress. The following information is displayed for each conference:

Field	Field description	Usage tips
Name	The name of the conference, which is either the name entered when the conference was scheduled, or, in the case of certain specialized types of conferences, a name chosen automatically by the MCU when created.	Specialized conference types are described below in Description . Click the conference name to display detailed information about the conference and participants.
Description	Additional information about the conference, which can assist users joining conferences. You can add the description when scheduling a conference. If you do not add a description or the conference has not been scheduled in advance, the description displays one of the following: <ul style="list-style-type: none"> ■ <i><scheduled></i> The conference has been scheduled in advance using the MCU web interface, but the owner has not entered a description. ■ <i><ad hoc></i> The conference was created dynamically during an auto attendant session and will end when the last participant using the auto attendant exits the conference. ■ <i><auto attendant></i> This type of conference indicates that a participant is currently connected to the auto attendant and navigating the menus. 	
Owner	The configured owner of the conference.	See Conference ownership for additional information.

Registration	<p>The status of a conference with respect to its H.323 gatekeeper and/or SIP registration. Depending on the conference settings, there is a maximum of four registrations for each conference: H.323 numeric ID, H.323 guest numeric ID, SIP numeric ID, and SIP guest numeric ID. The Registration field will show failed if any of the registrations has not completed successfully.</p> <ul style="list-style-type: none"> ■ <i>n/a</i> This conference is not configured to be registered with a gatekeeper or SIP registrar; because of this, there is no applicable registration status to show ■ <i>Registering</i> This conference is in the process of registering with the gatekeeper or SIP registrar ■ <i>Failed</i> At least one of the registrations for this conference has failed ■ <i>Registered</i> All IDs associated with this conference have been registered successfully with the gatekeeper / SIP registrar ■ <i>Disabled</i> One or more of the IDs associated with this conference has been configured to be registered with the gatekeeper or SIP registrar, but that registration has not been attempted due to another setting taking precedence. For H.323 calls this might occur if, on Settings > Gatekeeper, either the H.323 gatekeeper usage is disabled or the Allow numeric ID registration for conferences option is unselected. For SIP calls this might occur if, on Settings > SIP, the Allow numeric ID registration for conferences is unselected <p>Note that when there is a problem with the registration, the status is a link to the conference's Statistics page.</p>	<p>If the MCU can connect to an H.323 gatekeeper, each numeric ID (for both chairperson and guest privileges) for a conference can be registered with that gatekeeper as a different directory number. This allows H.323 users to dial directly into a particular conference (with the correct privileges) instead of connecting first to the MCU's auto attendant and navigating the menu system.</p> <p>Likewise, if the MCU can connect to a SIP registrar, each conference can be registered with that registrar using either (or both) Numeric ID and Guest ID. This allows SIP users to dial directly into a particular conference (with the correct privileges) instead of connecting first to the MCU's auto attendant and navigating the menu system. Note that for SIP, unlike H.323, the conferences must be configured on the SIP registrar before the MCU can register them.</p> <p>There is a maximum of four registrations for each conference: H.323 numeric ID, H.323 guest numeric ID, SIP numeric ID, and SIP guest numeric ID. To view further details about the registrations for a conference, click the conference name and then the Statistics tab to view the conference's Statistics page.</p> <p>For tips on configuring gatekeepers, see Configuring H.323 gatekeeper settings.</p> <p>For tips on configuring SIP registrars, see Configuring SIP settings.</p> <p>For more information about configuring conferences (and chairperson and guest IDs and PINs), refer to Adding and updating conferences.</p>
---------------------	---	--

Participants	<p>The number of active participants in this conference. The number may be followed by further numbers, in parentheses, which highlight when participants are <i>pending</i> reconnection, <i>dormant</i> because they haven't yet been tried, or <i>failed</i> because the MCU has been unable to connect them.</p> <p>If a limit on the number of participants has been set for the conference, the Participants value is shown as <i>A / B</i>, where <i>A</i> is the number of active participants and <i>B</i> is the configured limit. If it has not been possible to reserve all of the required ports for a conference (for instance because of a configuration error), this value will display in red as an error indication.</p>	<p>If a conference is protected by a PIN and you are not logged in as the administrator, the number of participants is hidden until the PIN is entered. In this case, the Participants value displays as <i><PIN required></i>.</p>
Start time	When the conference began. If the conference started before today, the date also displays.	
Time remaining	How long the conference still has to run. If the conference does not have a limited duration, this column displays as <i><forever></i> .	

Scheduled conferences

Scheduled conferences are either in progress or are yet to start. You can review this list and make some changes to it:

- To remove a scheduled conference, select the conference via its associated check box and click **Delete selected**.
- To schedule a new conference, click **Add new conference** (see [Adding and updating conferences](#)).

Note: The MCU 4500 Series and MCU 4200 Series supports up to 200 scheduled conferences. The MCU 5300 Series and MCU 8510 supports up to 500 scheduled conferences.

Field	Field description	More information
Name	The name of the conference chosen when the conference was scheduled.	Click the conference name to display detailed information about the configuration of the conference and, if it is currently active, its participants.
Numeric ID	The number that you can dial to join the conference.	
Security	Whether a PIN is required to join the conference.	
Owner	The configured owner of the conference.	See Conference ownership for additional information.

Status	<p>Whether a conference is:</p> <ul style="list-style-type: none"> ■ <i>Yet to start</i> The conference's configured start time has not yet arrived. ■ <i>In progress</i> The conference is running and is available for video conferencing endpoints to join. A scheduled conference in this state will also appear in the Active conferences list. ■ <i>Awaiting repeat</i> The conference is not currently running, but has been previously active and is now waiting to be re-activated when the time of its next repetition is reached. 	<p>There is no explicit status for "finished" when a conference is not in progress and is not scheduled to become active again then it is moved to the Completed conferences list.</p>
Start time	When the conference began. If the conference started before today, the date also displays.	
End time	When the conference will end.	

Completed conferences

Completed conferences have finished and are not scheduled to repeat.

- To remove specific conferences from the list, select the conferences via their associated check boxes and click **Purge selected**.
- To remove all conferences from the list, click **Purge all**.

Field	Field description	More information
Name	The name of the conference chosen when the conference was scheduled.	Click the conference name to display detailed information about the configuration of the conference.
Owner	The configured owner of the conference.	See Conference ownership for additional information.
Start time	When the conference began. If the conference started before today, the date also displays.	
End time	When the conference ended.	

Related topics

- [Viewing the conference participant list](#)
- [Adding and updating conferences](#)

Adding and updating conferences

The information required to add or update a conference is nearly identical. Refer to these topics for details:

- [Adding a conference](#)
- [Updating a conference](#)
- [Adding configured endpoints](#)
- [Using IDs and PINs](#)

Adding a conference

To add a conference:

1. Go to **Conferences > Conference list**.
2. In the **Add new conference** section, select the required conference template from the **Template for new conference** drop down list and click **Add conference** to display the **Add conference** page. (See [Using conference templates](#) for more information on conference templates.
3. Complete the fields referring to the table below for the most appropriate settings for the conference. Note that the defaults that appear on the **Add conference** page are controlled by the conference's template. You can change these settings as required.
4. Click **Add conference** to add the conference and return to the **Conference List**. The recently added conference appears either in the **Active** or **Scheduled Conferences** depending on its scheduled start time.

Ad hoc conferences (if you allow them) are added by users in the auto attendant.

Updating a conference

To update an existing conference:

1. Go to **Conferences**.
2. Click a Conference name and then click the **Configuration** tab.
3. Edit the fields referring to the table below for the most appropriate settings for the conference.
4. Click **Update conference** to add the conference and return to the **Conference List**. The updated conference appears either in the **Active** or **Scheduled Conferences** depending on its scheduled start time.

Ad hoc conferences

The following settings can be updated for existing ad hoc conferences:

- **Description**
- **PIN**
- **Numeric ID registration**
- **Floor and chair control**
- **Automatic lecture mode**
- **Visibility**

- Send camera control to participants
- In call menu for chair
- In call menu for guest
- Content mode
- Encryption
- Layout control via FECC/DTMF
- Mute in-band DTMF
- Allow DTMF *6 to mute audio
- Mute on join
- Maximum video participants
- Maximum audio-only participants
- Outgoing transcoded codec
- Minimum outgoing bit rate
- Content contribution from endpoints
- Outgoing transcoded resolutions

See the table below for more information:

Field	Field description	Usage tips
Parameters		
Name	The name that users will see on auto attendant screens and on the MCU's web interface.	<p>Conference names must be unique; conferences cannot share names.</p> <p>Only scheduled conferences have a configurable Name. Ad hoc conferences use the 'conference number' entered by the participant who has created the conference as the Name and this is not configurable after the conference has been created.</p>
Description	Additional information about the conference, which can assist users joining conferences.	<p>Use the description to provide more detailed information about the conference than the name alone conveys.</p> <p>This is an optional field for scheduled conferences; ad hoc conferences cannot be given a description by default.</p>

Numeric ID	<p>The unique identifier used for dialing in to the conference (as a chairperson participant) using an auto attendant or through an H.323 gatekeeper or SIP registrar.</p> <p>For more information about chairpersons and guests, refer to Using IDs and PINs.</p>	<p>When connected to an auto attendant, participants can join a conference by typing its numeric identifier.</p> <p>If you plan to allow audio-only participants, then you will need to enter either a Numeric ID or a Guest numeric ID.</p> <p>If H.323 gatekeeper registration is enabled for a conference, the MCU attempts to register the conference with an E.164 telephone number, which is comprised of the Registration prefix and the numeric identifier.</p> <p>If SIP registration is enabled for a conference, then the Numeric ID is registered with the SIP registrar.</p> <p>Conferences that are simultaneously active must not share a Numeric ID. For example, a conference on a Tuesday and a conference on a Thursday can share a Numeric ID, whereas two permanent conferences cannot share a Numeric ID. The same number can be used for the Guest numeric ID, if there are two different PINs. Additionally, because the numeric identifier is used in gatekeeper registration, conferences and auto attendants cannot share a numeric identifier value.</p> <p>For more information, refer to Using IDs and PINs.</p> <p>For ad hoc conferences created via the auto attendant, the number allocated by the conference creator becomes the Numeric ID. If ad hoc conferences are registered with the gatekeeper and /or SIP registrar, participants can dial in using this number. Note that the actual number that H.323 participants will dial depends on whether prefixes are used in the Settings > Gatekeeper page.</p> <p>You cannot configure the Numeric ID of an ad hoc conference; the Numeric ID of an ad hoc conference is set by the conference creator as the "conference number" at the time the conference is created.</p>
-------------------	--	--

PIN	Provides a level of security to conference access.	<p>If a conference has a PIN set, users cannot join the conference or change its configuration without entering the correct PIN. Depending on the conference settings, it may be possible for participants to join a conference as a chairperson (using the Numeric ID and PIN), or as a guest (using the Guest numeric ID and Guest PIN).</p> <p>For an ad hoc conference, you can configure a PIN both at the time of conference creation and also while the conference is running. You can also force ad hoc conference creators to use a PIN (controlled on the Settings > Conferences page).</p>
Guest numeric ID	<p>The unique identifier used for dialing in to the conference (as a guest participant) using an auto attendant or through an H.323 gatekeeper or SIP registrar.</p> <p>For more information about chairpersons and guests, refer to Using IDs and PINs.</p>	<p>When connected to an auto attendant, participants can join a conference by typing its Guest numeric ID.</p> <p>If you plan to allow audio-only participants, then you will need to enter either a Numeric ID or a Guest numeric ID.</p> <p>If H.323 gatekeeper registration is enabled for a conference, and you have entered a Guest numeric ID, the MCU attempts to register the conference with an E.164 telephone number, which is comprised of the Registration prefix and the Guest numeric ID.</p> <p>If SIP registration is enabled for a conference, and you have entered a Guest numeric ID, then the Guest numeric ID is registered with the SIP registrar.</p> <p>Conferences that are simultaneously active must not share a Numeric ID. For example, a conference on a Tuesday and a conference on a Thursday can share a Numeric ID, whereas two permanent conferences cannot share a Numeric ID. The same number can be used for the Guest numeric ID, if there are two different PINs. Additionally, because the numeric identifier is used in gatekeeper registration, conferences and auto attendants cannot share a numeric identifier value.</p> <p>For more information, refer to Using IDs and PINs.</p> <p>Ad hoc conferences cannot be configured with Guest numeric IDs or Guest PINs.</p>

Guest PIN	Provides secure access to conferences for guest participants.	<p>If a conference has a PIN set, users cannot join the conference or change its configuration without entering the correct PIN. Participants joining as guests have restricted privileges. For more information, refer to Using IDs and PINs.</p> <p>Ad hoc conferences cannot be configured with Guest numeric IDs or Guest PINs.</p>
Owner	The owner of the conference, usually the user ID of the user account that the person who scheduled the conference logged in with.	<p>You may or may not be able to change the conference owner, depending on your privilege level. See Conference ownership for additional information.</p> <p>This setting does not apply to ad hoc conferences.</p>
Numeric ID registration	<p>Enables the MCU to attempt to register the Numeric ID and/or Guest numeric ID with the configured H.323 gatekeeper and/or SIP registrar.</p> <p>To globally enable the MCU to allow conferences to register to the SIP registrar, go to Settings > SIP and select Allow numeric ID registration for conferences.</p> <p>To globally enable the MCU to allow conferences to register to the gatekeeper, go to Settings > H.323 and select Allow numeric ID registration for conferences.</p>	<p>This setting applies to both the Numeric ID and Guest numeric ID (if you have set both). For more information, refer to Using IDs and PINs.</p> <p>For ad hoc conferences, whether or not they are registered with the gatekeeper and/or SIP registrar depends on the Numeric ID registration setting on the ad hoc conferences template. You can edit the Numeric ID registration setting for individual active ad hoc conferences. For more information about templates, see Using conference templates.</p> <p>For scheduled conferences, whether or not they are registered with the gatekeeper and/or SIP registrar depends on the configuration of the individual conference's Numeric ID registration setting.</p>
When only guests remain	<p>Controls what happens to the conference when the last participant with chairperson status leaves the conference. The options are:</p> <ul style="list-style-type: none"> ■ <i>Disconnect all participants</i>: this is the default option. When the last participant with chairperson status leaves the conference, all other participants will be disconnected ■ <i>Take no action</i>: all participants may continue the conference until the last one disconnects 	<p>This setting applies to scheduled conferences that include guest participants (that is, those who have joined the conference using the Guest numeric ID, or a cascade link on the master MCU).</p> <p>For more information about chairpersons and guests, refer to Using IDs and PINs.</p>

Automatic lecture mode

Automatic lecture mode is most useful when the conference is a lecture. The setting allows the lecturer (chair) to be shown in full-screen view to the students. In this mode, the lecturer will continue to see their normal (continuous presence) view. That is, the lecturer will see the students (guests) and not himself.

The MCU identifies the lecturer as being the loudest speaker and controls the layout seen by the other participant according to which mode is selected here.

Select from:

- **Disabled:** Automatic lecture mode is disabled.
- **Type 1:** The speaker sees continuous presence (or their custom layout) and all participants see the guest who is speaking (be they a chair or a guest).
- **Type 2:** All guests including the speaker see the last chair who spoke full screen. All chairs will see their custom layout.

If you have configured a custom layout for the lecturer, that will override the normal continuous presence view. For the other participants (the students), the view of the lecturer (the loudest speaker) overrides any custom layout.

During Type 1 lecture mode, whoever is the loudest speaker is seen full screen when all chairs have left the conference leaving only guests, the loudest speaker sees the continuous presence screen layout and can modify the layout whereas the other participants see the loudest speaker and cannot change the layout.

During Type 2 lecture mode, when all chairs have left the conference leaving only guests, the guests see a normal continuous presence view of each other and can then modify their layout.

Note that you can use the conference's **Mute on join** setting together with the settings for the lecturer's endpoint's **Initial audio status** to ensure that the full screen view does not get needlessly interrupted.

If you disable **Automatic lecture mode**, this change will take effect immediately, that is, the layout changes from full screen to continuous presence (or custom layout).

For ad hoc conferences, you can configure **Automatic lecture mode** through the ad hoc conferences template. You can also edit the **Automatic lecture mode** setting for individual active ad hoc conferences.

Timeout for Type 1 automatic lecture mode one	<p>This option is enabled if Type 1 automatic lecture mode is selected. The option determines how quickly the loudest speaker will appear in full-screen view to the other participants. Choose from:</p> <ul style="list-style-type: none">■ <i>Immediately</i>: As soon as the MCU identifies a participant as the loudest speaker, the MCU will show that participant in full screen to the other participants in the conference. The loudest speaker will continue to see their normal continuous presence conference view. If another participant interrupts the loudest speaker, that participant becomes the loudest speaker and will be seen in full screen by the other participants (and that participant will see their normal continuous presence view).■ <i>After 10 seconds</i>: When the MCU identifies a participant as the loudest speaker, if that participant continues to be the loudest speaker for 10 seconds then the MCU will show that participant in full screen view to the other participants. The loudest speaker will continue to see their normal continuous presence conference view. If another participant interrupts the loudest speaker, everyone will immediately see their normal continuous presence view. If the interrupter continues to speak for 10 seconds, the MCU identifies that participant as the loudest speaker who will then be shown in full screen to the other participants (and the new loudest speaker will continue to see their normal continuous presence view).■ <i>After 30 seconds</i>: As for <i>After 10 seconds</i>, but the MCU waits for 30 seconds before showing the loudest speaker in full screen view.■ <i>After 1 minute</i>: As for <i>After 10 seconds</i>, but the MCU waits for one minute before showing the loudest speaker in full screen view.■ <i>Disabled</i>: The loudest speaker will not be shown in full screen view to the other participants. All conference participants will see the normal continuous presence conference view, or a custom layout if one has been specified.
--	--

Visibility	<p>Indicates the visibility of the conference on the auto attendant and the web interface. The options are:</p> <ul style="list-style-type: none"> ■ <i>Public</i>: the conference will be listed in the auto attendant and be visible to all users of the web interface ■ <i>Private</i>: the conference will not be listed in any auto attendant except for auto attendants specifically set to show it. The conference will also only be visible in the web interface to the conference owner and to the admin user 	<p>For private conferences not visible on an auto attendant, participants will still be able to join the conference if they know the PIN.</p> <p>Note that only admin users can choose which conferences are visible on a given auto attendant.</p> <p>For ad hoc conferences, you can configure Visibility through the ad hoc conferences template. You can also edit the Visibility setting for individual active ad hoc conferences.</p> <p>For more information, refer to Adding and updating an auto attendant.</p>
Encryption	<p>The encryption setting for this conference, if you have the encryption feature key enabled.</p>	<p>If encryption is enabled unit-wide/blade-wide (through the Settings > Encryption page), you can set one of:</p> <ul style="list-style-type: none"> ■ <i>Required</i>: encryption must be used for this conference ■ <i>Optional</i>: encryption is optional for this conference <p>For ad hoc conferences, you can configure encryption through the ad hoc conferences template. You can also edit the Encryption setting for individual active ad hoc conferences.</p> <p>This setting is grayed-out if encryption is disabled on the Settings > Encryption page.</p> <p>Note that to be able to use encryption, the Encryption feature key must be present on the MCU.</p>
Invite pre-configured participants	<p>Indicates when the MCU should invite any pre-configured endpoints into a conference. The options are:</p> <ul style="list-style-type: none"> ■ <i>At the start of the conference</i> Pre-configured participants will be called as soon as the conference starts. ■ <i>When at least one other participant is present</i> Pre-configured endpoints will only be called after at least one other participant joins the conference. 	<p>Select which option fits your requirements best. Calling pre-configured endpoints <i>at the start of the conference</i> is most appropriate for repeating conferences with a particular start time.</p> <p>Calling pre-configured endpoints <i>when at least one other participant is present</i> is most appropriate for permanent conferences; such conferences are typically un-attended for much of the time, and it may only be useful to invite pre-configured endpoints when others are present.</p> <p>This setting only applies to scheduled conferences.</p>

Mute on join	<ul style="list-style-type: none"> ■ <i>Audio</i>: Check the box to mute the audio coming from endpoints that call in to this conference. ■ <i>Video</i>: Check the box to stop the video coming from endpoints that call in to this conference. <p>Participants who call in will have the selected channels muted as they join the conference. This setting does not apply when the MCU calls out to preconfigured endpoints or ad hoc participants.</p> <p>You can edit this setting on conference templates, preconfigured conferences, or active conferences.</p>	<p>If you want ad hoc conferences to use this option by default, configure the Mute on join settings of the ad hoc conferences template.</p> <p>Note that there are corresponding settings called Initial audio to MCU and Initial video to MCU that you can set for ad hoc participants and preconfigured endpoints. If either the endpoint's configuration or the conference's configuration requires that a media channel from the endpoint is muted when it joins the conference, then that channel will be muted. There is no precedence between these corresponding settings.</p> <p>Refer to Adding participants, Configuring an H.323 endpoint, or Configuring a SIP endpoint for more information.</p> <p>To toggle the mute on a participant's media channel during a conference, you can go to Conferences, click the name of the conference, and then click the participant name to bring up its status pages. Refer to Viewing the conference participant list for more information.</p>
Adaptive Gain Control on join	<p>Defines whether or not endpoints use Adaptive Gain Control (AGC) when they first join the conference. Check the box to enable AGC by default for endpoints joining this conference.</p>	<p>This is the conference-wide setting. There is a corresponding Initial Adaptive Gain Control setting on the endpoint configuration, or ad hoc participant configuration, which can override the conference-wide setting on an individual basis.</p> <p>Any manual changes to the participant volume will turn AGC off for that participant. You can manually enable or disable AGC for a participant that is already in the conference, on the Conference > Participants > <Name> > Audio page.</p>
Start locked	<p>Choose from:</p> <ul style="list-style-type: none"> ■ <i>Unlocked</i>: the conference is not locked. ■ <i>Locked</i>: the conference is locked from the start of the conference and only preconfigured participants can join. 	

Maximum video participants	<p>When the MCU is not in port reservation mode, this parameter sets a limit on the number of endpoints which can connect to the conference as video participants.</p> <p>A participant counts (as a single unit) towards the video limit whether the MCU is sending a video stream to that participant or a video stream is being received.</p>	<p>If you do not want to limit the number of participants who can join this conference and use video, leave this field blank.</p> <p>This field is only shown if the MCU is not in port reservation mode.</p> <p>This field only applies to scheduled conferences.</p>
Maximum audio-only participants	<p>When the MCU is not in port reservation mode, this parameter sets a limit on the number of endpoints which can connect to the conference as audio-only participants.</p> <p>A participant counts (as a single unit) towards the audio limit whether the MCU is sending an audio stream to that participant or an audio stream is being received.</p>	<p>If you do not want to limit the number of participants who can join this conference to use just audio, leave this field blank.</p> <p>This field is only shown if the MCU is not in port reservation mode.</p> <p>This field only applies to scheduled conferences.</p>
Video ports to reserve	<p>In port reservation mode, this parameter specifies the number of video ports to reserve.</p> <p>A participant counts (as a single unit) towards the video reservation value whether the MCU is sending a video stream to that participant or a video stream is being received.</p>	<p>This value is both a reservation and a limit; the MCU guarantees that this many video participants can connect to the conference, but no more than this will be able to join.</p> <p>This field is only shown if the MCU is in port reservation mode.</p>
Audio-only ports to reserve	<p>In port reservation mode, this parameter specifies the number of audio-only ports to reserve.</p> <p>A participant counts (as a single unit) towards the audio reservation value whether the MCU is sending an audio stream to that participant or an audio stream is being received.</p>	<p>This value is both a reservation and a limit; the MCU guarantees that this many audio-only participants can connect to the conference, but no more that this will be able to join.</p> <p>This field is only shown if the MCU is in port reservation mode.</p>

Participant controls

Floor and chair control	<p>Controls "Floor and chair control" settings for this conference. The options are:</p> <ul style="list-style-type: none"> ■ <i>Do not allow floor or chair control</i>: the use of floor and chair controls is not allowed in this conference ■ <i>Allow floor control only</i>: only floor control is allowed in this conference; chair control is not allowed. Any participant can 'take the floor' so long as no other participant has currently 'taken the floor' ■ <i>Allow floor and chair control</i>: both floor and chair control are allowed in this conference. Any participant can take the floor, and any chairperson participant can take the chair so long as no other participant has currently done so 	<p>Some H.323 endpoints support a feature known as floor and chair control that is encompassed by the H.243 protocol. For more information, refer to H.243 floor and chair control.</p> <p>If you change the Floor and chair control setting for a conference currently taking place, there will be no immediate effect. That is, an existing floor or chair participant will not have that status removed.</p> <p>If the unit-wide/blade-wide Floor and chair control setting on the Global conference settings page is set to <i>Disabled</i>, it will not be possible to use floor or chair control operations in any conference.</p> <p>For ad hoc conferences, you can configure the Floor and chair setting through the ad hoc conferences template. You can also edit the Floor and chair setting for active ad hoc conferences.</p>
Layout control via FECC / DTMF	<p>Prevents or permits conference participants changing their view layout or focused participant using far-end camera control (FECC) or DTMF tones or both. Choose from:</p> <ul style="list-style-type: none"> ■ <i>Disabled</i>: in this conference, participants will not be allowed to change their view layout using either FECC or DTMF, unless you have overridden this setting in an endpoint's individual configuration. ■ <i>FECC only</i>: in this conference, participants will only be allowed to change their view layout using FECC, unless you have overridden this setting in an endpoint's individual configuration. ■ <i>DTMF only</i>: in this conference, participants will only be allowed to change their view layout using DTMF, unless you have overridden this setting in an endpoint's individual configuration. ■ <i>FECC with DTMF fallback</i>: in this conference, participants will be allowed to change their view layout using FECC. If FECC is not available, this participant will be able to use DTMF. ■ <i>FECC and DTMF</i>: in this conference, participants will be allowed to change their view layout using both FECC or DTMF unless you have overridden this setting in an endpoint's individual configuration. 	<p>You may want to prevent participants from changing their view layout in a managed conference, or classroom environment.</p> <p>This is a per-conference option, but you can still configure Layout control via FECC / DTMF on a per-participant basis.</p> <p>For ad hoc conferences, you can configure Layout control via FECC / DTMF through the ad hoc conferences template. You can also edit this setting for individual active ad hoc conferences.</p> <p>When calling out to an endpoint, if you have configured Layout control via FECC / DTMF for that endpoint, it will override this setting (otherwise the endpoint will use the conference configuration for this setting).</p> <p>This setting will apply to endpoints which connect to the conference via an auto attendant or by dialing in directly.</p>

Send camera control to participants	<p>Specifies whether FECC or DTMF or both may control a far end camera. This setting combines with layout control via FECC/DTMF to control the camera of the far end and the layouts of the conference.</p> <ul style="list-style-type: none"> ■ <i>Disabled</i>: in this conference, participants will not be allowed to control a far end camera using either FECC or DTMF, unless you override this setting in an endpoint's individual configuration. ■ <i>FECC only</i>: in this conference, participants will be only be allowed to control a far end camera using FECC. ■ <i>DTMF only</i>: in this conference, participants will be only be allowed to control a far end camera using DTMF. ■ <i>FECC with DTMF fallback</i>: in this conference, participants will be allowed to control a far end camera using FECC. If FECC is not available, this participant will be able to use DTMF for camera control. ■ <i>FECC and DTMF</i>: in this conference, participants will be allowed to control a far end camera using either FECC or DTMF. 	<p>There are two control mechanisms, FECC and DTMF, either (or both) of which can be used for camera control and/or layout control. If one mechanism is allowed for camera control but not for layout control, then that mechanism only controls the far end camera and does not affect the layout. Similarly, if one mechanism is allowed for layout control but not for camera control, then it is not possible to control the camera with that mechanism. In these cases, the endpoint can use FECC or DTMF controls directly to change the layout or adjust the far end camera.</p> <p>When one control mechanism can control either the layout or the far end camera, then that mechanism will always control the layout until 'Zoom in' (FECC mechanism) or '1' (DTMF mechanism) is pressed. The control mechanism then switches over to control the camera.</p> <p>Far-end camera control always applies to the camera of the participant shown in the largest or top left pane (when panes are the same size). If you have no way to control the layout, then you cannot focus on a participant to allow you to adjust a particular camera.</p>
--	---	---

Mute in-band DTMF	<p>Set the option for the muting of in-band DTMF sent from endpoints in this conference. Note that this sets the conference configuration for this option, but you can also override it for individual endpoints in the conference (through the configuration of the individual endpoints). Choose from the following (the setting will be applied to all endpoints in the conference that are configured to <i>use the conference configuration</i> for Mute in-band DTMF):</p> <ul style="list-style-type: none"> ■ <i>Never</i>: the in-band DTMF will never be muted. Any DTMF tones sent from these endpoints will be audible to conference participants. ■ <i>Always</i>: the in-band DTMF will always be muted. Any DTMF tones sent from these endpoints will not be audible to conference participants. ■ <i>When used for MCU control</i>: if a participant is using in-band DTMF to control conference layout and for other in-conference features, the tones will be muted and will not be audible to conference participants. The MCU will only expect a participant to use DTMF for MCU control if Layout control via FECC / DTMF or Send camera control to participants is set to <i>DTMF only</i>, <i>FECC and DTMF</i>, or <i>FECC with DTMF fallback</i> and FECC has not been established, or if the participant is able to use the in call menu. 	<p>This is a per-conference option, but you can still enable or disable the muting of in-band DTMF on a per-participant basis.</p> <p>In some circumstances, you might need to override this setting for individual endpoints. For example, where a conference is cascaded onto an audio bridge, it might be useful for one of the participants in that conference to be able to send in-band DTMF to the MCU. This is for the purposes of sending the conference ID or PIN to the audio conferencing bridge. In this case, the Mute in-band DTMF setting for the endpoint of that participant needs to be <i>Never</i> (and you configure this in an endpoint's configuration, see Configuring an H.323 endpoint and Configuring a SIP endpoint).</p> <p>For ad hoc conferences, you can configure the Mute in-band DTMF setting through the ad hoc conferences template. You can also edit the Mute in-band DTMF setting for individual active ad hoc conferences.</p>
In call menu for chair	<p>In call menus allow conference participants to control many aspects of a conference while on a call without needing to access the web interface. These are controlled using menus accessed via the control keypad. Pressing * on the keypad activates the in call menus. Read more about these menus in the conference features topic.</p> <p>The in call menus can be made available to chairs only, or to both chairs and guest participants, or disabled completely.</p> <p>This parameter configures in call menus for chairs.</p>	<p>Chairs can be configured to have access to the in call menus at one of three command levels.</p> <p>Choose between:</p> <ul style="list-style-type: none"> ■ <i>Disabled</i>: The in call menu is not available to participants in this conference. ■ <i>Level 1 - Local</i>: Local commands - request floor, mute/unmute audio and video, change layout, view participants. ■ <i>Level 2 - Conference</i>: Level 1 commands plus Conference commands - assign floor to a participant, mute/unmute audio or video of participants, lock the conference, disconnect all participants, change a participant's volume, send DTMF tones to a participant, disconnect a participant. ■ <i>Level 3 - Advanced</i>: Levels 1 and 2 plus Advanced commands - add participant, add/change PIN/guest PIN.

In call menu for guest	<p>In call menus allow conference participants to control many aspects of a conference while on a call without needing to access the web interface. These are controlled using menus accessed via the control keypad. Pressing * on the keypad activates the in call menus.</p> <p>The in call menus can be made available to chairs only, or to both chairs and guest participants, or disabled completely.</p> <p>This parameter configures in call menus for guests.</p>	<p>Guests can be given access to Local commands only.</p> <p>Choose between:</p> <ul style="list-style-type: none"> ■ <i>Disabled</i>: The in-call menu is not available to participants in this conference. ■ <i>Level 1 - Local</i>: Local commands - request floor, mute/unmute audio and video, change layout, view participants.
-------------------------------	---	---

Content

Content mode	<p>The MCU can decode and then re-encode incoming content to ensure that the majority of participants can receive the content. This is the <i>Transcoded</i> content mode.</p> <p>The MCU can also retransmit the content without having to decode it, which is known as <i>Passthrough</i> mode. In this mode, the incoming content packet stream is repackaged and sent to endpoints in the conference that are capable of decoding the original stream. Passthrough mode does not use up a content port for that conference.</p> <p>The MCU also has a <i>Hybrid</i> content mode. In Hybrid mode, the incoming content stream is passed through to participants who are able to support the same codec as the original content stream (the Passthrough content stream). The MCU also encodes a stream, using the specified Outgoing transcoded codec, for endpoints who cannot decode the Passthrough content stream. Hybrid mode uses up a video port.</p> <p>Choose from:</p> <ul style="list-style-type: none"> ■ <i>Disabled</i>: The MCU does not transmit content. ■ <i>Passthrough</i>: The MCU does not transcode the content before transmission. The data is simply repackaged then sent to endpoints that support the original codec. ■ <i>Hybrid</i>: The MCU sends a passthrough stream to eligible endpoints, and a transcoded stream to other endpoints that advertise support for the Outgoing transcoded codec. ■ <i>Transcoded</i>: The MCU decodes the incoming stream and re-encodes it using the Outgoing transcoded codec, before sending it to all endpoints that support the Outgoing transcoded codec. 	<p>Sending of passthrough content to or from endpoints over encrypted connections is not supported, with the exception of encrypted H.323 to encrypted H.323.</p> <p>Endpoints that can only support resolutions below the minimum threshold will also only receive transcoded in hybrid, and no content in passthrough mode.</p> <p>Content previews are not supported in passthrough mode but are supported for hybrid content. In passthrough mode a black panel is displayed.</p> <p>A default content mode can be set in the conference template.</p>
---------------------	---	--

Outgoing transcoded codec	<p>The codec used to transcode the transcoded stream in transcoded and hybrid content. If hybrid mode is selected and a codec different to the incoming stream is selected, two codecs will be sent: the original codec in the passthrough content stream and the transcoded codec in the transcoded content stream.</p>	<p>Choose from:</p> <ul style="list-style-type: none"> ■ <i>Automatic</i> ■ <i>H.263+</i> ■ <i>H.264</i> <p>If <i>Automatic</i> is selected, the MCU will determine the best codec to use that will maximize the number of participants that can receive content.</p>
Content contribution from endpoints	<p>Whether, by default, endpoints are permitted to contribute the content channel for a conference through the mechanism of opening a content video channel.</p> <p>There can only be one endpoint contributing content video at any one time, and the MCU arbitrates between them. Therefore, even with this parameter set to <i>Enabled</i>, the ability of the endpoint to contribute content video will be affected by other endpoints' behavior.</p>	<p>If this setting is <i>Disabled</i>, it is still possible to enable content contribution on a per-endpoint basis when the conference is active. Similarly, it is possible to disable content contribution from specific endpoints, either while they are connected or via their configuration. For more information about endpoint configuration, refer to Configuring H.323 endpoints and/or Configuring SIP endpoints.</p> <p>This setting only applies to scheduled conferences. For ad hoc conferences, whether or not endpoints are allowed to contribute content is controlled by the Content contribution from endpoints setting in the ad hoc conference template.</p> <p>To use content, it must be enabled unit-wide/blade-wide on the Settings > Content page. See Configuring content settings for additional information on MCU-wide content configuration parameters.</p>
Outgoing transcoded resolutions	<p>Choose the resolution for the content channel that will be transmitted to endpoints in this conference:</p> <ul style="list-style-type: none"> ■ <i>4:3 resolutions only</i>: the MCU will encode the content and transmit it in a resolution of ratio 4:3 ■ <i>16:9 resolutions only</i>: the MCU will encode the content and transmit it in a resolution of ratio 16:9 ■ <i>Allow all resolutions</i>: the MCU will decide on the most optimal resolution depending on information about capabilities sent by the endpoints in the conference 	<p>For ad hoc conferences, transmitted content resolution is controlled by the ad hoc conference template.</p>

Minimum outgoing bit rate	<p>This field sets a lower limit on the bandwidth of the shared content video encoding sent to content receivers in a conference.</p> <p>Changing this setting when there are connected participants causes the MCU to re-assess whether there should be content video channels to those endpoints; the MCU will close existing channels and open new ones as appropriate.</p>	<p>A single content video stream is used for each conference, and this stream will be sent to all endpoints receiving the content channel as a separate video channel. If some endpoints are only able to receive low bit rate streams (for instance if they have called into the MCU at a low call rate), it is sometimes preferable to exclude those endpoints completely from the content stream rather than force all viewers to see a reduced bit rate channel.</p> <p>If you do not want to exclude endpoints from viewing the shared content video channel in a conference, make sure this is set to <i><no minimum></i>, which is the default setting.</p> <p>Where an endpoint cannot, for whatever reason, receive the content channel as an additional video channel, the MCU can show the content channel as part of the main video channel. That is, the participant will see the content as a pane in the conference layout. This functionality is controlled by the Display content in normal video channel setting (see below).</p> <p>Note that during a call, an endpoint can send a 'flow control message' to the MCU that could cause the MCU to reduce the bit rate to that endpoint to below the configured Minimum outgoing bit rate; in this case, the MCU will close the content channel to that participant. To re-enable content (which has been disabled in this way) to this participant, go to the conference's Participant list and use the content enable control. For more information about altering a participant's settings during a conference, refer to Viewing the conference participant list.</p>
Preferred minimum passthrough resolution	<p>The minimum resolution that will be passed on to endpoints</p>	<p>If an endpoint that can only receive content below the minimum joins a conference, the endpoint will not be sent a passthrough content stream or a transcoded content stream. If the MCU receives content with a resolution below this setting, then it will use the received resolution as the minimum instead. Grayed out if <i>Content mode</i> set to <i>Transcoded</i> or <i>Hybrid</i>.</p>
Start time and duration		
Start time	The time at which the conference will begin.	
Start date	The date on which the conference will begin.	

Set to current time	Sets the conference start time to the current time on the MCU.	The current time on the MCU is determined by the settings in the Settings > Time page, which can only be modified by the administrator. See Displaying general status for additional information.
Permanent	Allows you to retain a conference and its settings for an infinite period of time.	
Maximum duration	Limits the duration of the conference for one instance of the conference.	These fields are not available or necessary for conferences set to <i>permanent</i> .
Repetition		
Interval	Which days and / or weeks the conference repetitions will occur. The repetitions will always start at the same time of day: the conference's configured Start time (see above), and will last for the same amount of time: the configured Maximum duration .	The start date is taken into account when determining when the first repetition should occur. For instance, if the start date is a Wednesday and the conference is scheduled to repeat every Monday, Tuesday and Wednesday then it will occur only on Wednesday in the first week and on all three specified days in subsequent weeks.
Termination	If a conference is set to repeat, its repetitions can be configured to go on forever, stop after a certain date, or to occur only a certain number of times.	The first activation of a conference counts as a "repetition", so configuring a conference to repeat but terminate after 1 repetition is equivalent to it not repeating at all.

Adding configured endpoints

You can choose to pre-configure endpoints to be part of a conference. These endpoints will be automatically invited into the conference by the MCU. This is useful if you regularly invite the same participants into a conference. To select which previously configured endpoints will be pre-configured for this conference, press **Pre-configured participants**. (This button may also show a number in parentheses to indicate the number of participants that are currently pre-configured). Refer to [Adding participants](#) for more details.

Using IDs and PINs

There are two types of conference participant: chairperson and guest. IDs and PINs allow participants to connect to conferences as the correct participant type.

Chairperson participants use **Numeric ID** and optionally, **PIN**; guest participants use **Guest numeric ID** and optionally, **Guest PIN**.

A conference will not begin until the first chairperson joins. This means that guests will see a black screen/hear silence with on screen text 'Waiting for conference chairperson' and an audio prompt after five seconds and then every minute thereafter.

You can control the behavior when the last chairperson leaves the conference (that is the **When only guests remain** setting). The two options are:

- all participants are disconnected (default)
- all participants may continue the conference until the last one disconnects (*take no action*)

The permitted ID and PIN combinations are as follows:

- All IDs and PINs are blank
- Different chairperson ID and guest ID (this includes the cases where one is blank and the other is not)
- The same ID for chairperson and guest with different PINs (one of which may be blank)

Note that participants dragged and dropped into a conference on the web interface will be chairperson participants. Where no IDs or PINs are configured for a conference, all participants will be chairpersons regardless of how they join.

H.323 and SIP registration

Both Numeric ID and Guest numeric ID can be registered with an H.323 gatekeeper and/or SIP registrar to enable participants to dial in to conferences directly and as the correct participant type. The **Numeric ID registration** setting applies to both IDs.

Audio-only participants

Audio-only participants can be guest or chairperson participants by connecting to a conference using either a Guest or Chairperson ID. In the case of an audio-only guest, if no chairperson has yet joined the conference, they will hear an audio prompt informing them of that. The conference will start when the first chairperson joins.

Related topics

- [Using conference templates](#)
- [Displaying conference lists](#)
- [Adding participants](#)
- [Configuring H.323 gatekeeper settings](#)
- [Configuring SIP settings](#)
- [Displaying general status](#)
- [In call menus](#)

Using conference templates

Templates control the default settings for conferences. The MCU is shipped with the following default templates:

- The **top level** template
- The **ad hoc conferences** template

You can add additional templates below the top level template in a tree hierarchy. A newly created template will initially inherit the settings of the template selected as the parent template, but you can then tailor the settings of each template to the requirements of a particular conference. A template can be moved by selecting a new parent template in the [Template configuration page](#).

Templates can also be deleted. The parent of a deleted template becomes the parent of any child template below the deleted template.

The MCU supports up to 100 templates in total.

When you add a new scheduled conference from the [Conference list](#) page, you select the template that you want the conference to use from a drop down list. The selected template provides the settings that appear on the [Add conference](#) page which you can then change if required.

The ad hoc conference template provides the configuration for all ad hoc conferences. You can alter any of the conference settings during the conference.

For information about the conference configuration settings, refer to [Adding and updating conferences](#) which lists all conference configuration settings.

Related topics

- [Adding and updating conferences](#)
- [Configuring global conference settings](#)

Conference ownership

Each scheduled conference (i.e. conferences that are configured via the web interface with a start time and, optionally, a duration and repetition) has an associated *owner*. This owner is the ID of a configured user, and normally corresponds to the user who scheduled the conference.

Scope of conference ownership

Conference ownership affects only web interface control of conferences - in particular, it plays no part in validating video conferencing endpoints' attempts to join conferences when they connect to the MCU via H.323 or SIP. Restricting conference entry in this situation is accomplished via conference (or auto attendant) PINs, as before.

User privileges

The actual implications of conference ownership depend on the privilege of the user; specifically:

Privilege level	Effects of conference ownership
■ administrator ■ conference creation and full control	Users with these privilege levels are able to create and own conferences, and are able to exercise full control of all conferences.
■ conference creation and limited control	Users with these privilege levels are able to create and own conferences. They have full control of conferences they own, and limited control of conferences owned by other users.
■ conference creation	Users with these privilege levels are able to create and own conferences. They have full control of conferences they own, but no control of conferences owned by other users.
■ conference detail ■ conference list	Users with these privilege levels are not able to own conferences or change any conference's configuration.

Levels of conference control

As described above, a user privilege level confers a certain level of control over a conference, with that level of control possibly depending on whether that user is the conference owner or not. These conference control levels have the following meaning:

Conference control level	Description
■ full control	<p>This level of control permits the following operations:</p> <p>Participant control With full conference control, a user is able to disconnect participants, connect new participants to the conference, and end the conference whenever they want to.</p> <p>Configuration access A user with full conference control can view and modify any aspect of the conference's configuration. This includes the start time, end time, or repetition characteristics, and which endpoints are pre-configured as participants.</p> <p>Changing live conference parameters When the conference is in progress, a user with <i>full control</i> is permitted to send a text message to all connected participants' video displays and change the Conference custom layout. Additionally, full control includes all of the operations covered by <i>limited control</i>, detailed below.</p>
■ limited control	<p>This level of control permits the following operations:</p> <p>Viewing the participant list The participant list shows the names of the endpoints currently connected to the conference, a summary of that endpoint's status and, if they are a video participant, a thumbnail preview image of the video stream they are supplying. Thumbnail previews are shown by default, but you can configure the user interface not to show them. The setting that controls this is the Show video thumbnail images option on the Settings > User interface page. Note that the MCU will not show thumbnail previews on the participant list page if encryption is required for a conference. However, thumbnail previews will be shown for conferences where encryption is optional and there are encrypted participants.</p> <p>Via the participant list, it is also possible to mute (or stop muting) individual endpoints' audio, change the conference's "important" participant, and enable or disable the participants' ability to affect their own layouts via far-end camera control or DTMF tones.</p> <p>Controlling video sent to participants This includes being able to choose what view layout (or family) is used for constructing the conference view being sent to a participant, changing the Participant custom layout, and whether to send widescreen or standard format video to that endpoint.</p> <p>Controlling participant cameras The web interface can be used to send control commands (e.g. pan and tilt) to a remote participant's camera.</p> <p>Viewing audio status Waveforms of audio channels being sent to, and received from, the participant can be viewed, audio gain applied, and participant audio can be muted if required.</p> <p>Sending messages to individual participants Textual messages can be sent to an individual participant, and will appear on their displays.</p> <p>Viewing participant statistics and diagnostics This allows details of the media streams being sent to, and received from, participants to be viewed, plus endpoint-specific characteristics to be examined.</p>

-
- | | |
|---|---|
| <ul style="list-style-type: none">■ no control | This means that none of the above operations are possible. Depending on the specific privilege level, either the list of scheduled conferences will not be shown to the user, or the list will be shown but conferences over which the user has no control will be presented as names rather than hyperlinks. |
|---|---|
-

Changing the owner of a conference

A user whose privilege level is either *conference creation and full control* or *administrator* is also able to change the owner of a conference. A conference owner can be changed to either a user with conference creation rights or to "none", signifying that no user should be considered the owner of that conference. Also, when scheduling new conferences, users with these privileges are able to choose which owner is initially associated with the conference.

Deleting users who are conference owners

If a user account is deleted, any conferences owned by that user have their owner reset to "none".

Related topics

- [Adding and updating conferences](#)
- [User privileges](#)

Reservation of MCU media ports

The MCU is able, if required, to allocate its available media ports in advance to specific conferences. This means that it is able to guarantee that a certain number of participants will be able to join that conference, irrespective of how many other people are using the MCU for other conferences at the same time.

Media port types

The following types of media port are available on the MCU:

- video ports
- audio-only ports
- content channel ports

For information about the number and type of ports provided by each MCU model, refer to [MCU port matrix](#).

The term *video port* refers to a port that can be used by a video-conferencing endpoint for a call. Thus, a video port includes both video **and** audio streams (bidirectionally) and so the number of video ports available represents the number of "normal" video calls that the MCU is able to maintain simultaneously.

Participant port usage

In general, each endpoint in a conference is able to use either a video port or an audio-only port, though normally the MCU will assign video ports to video-capable devices and audio-only ports to audio-only devices.

If a video-capable device joins a conference which only has audio-only ports available, the MCU will assign it an audio-only port - that participant will be able to listen to other people and contribute their own audio to the conference but the MCU will not transmit video to it (and will not use any video received from it). If an audio-

only device such as a simple telephone joins a conference which has just video ports available, the MCU will assign it a video port, which includes audio capability. The video capability of that allocation will not be used, but the audio device will be able to participate as normal in the conference.

MCU media capacity

The total number of media ports available depends on the MCU model; refer to the product datasheets available on the web site, or to [MCU port matrix](#) for more information.

Configuring the MCU

How MCU media ports are allocated, and which options and settings are available, is controlled by the **Media port reservation** setting on the [Settings > Conferences](#) page.

On the MCU 4500 Series, the MCU 5300 Series, and the MCU MSE 8510 blade, the number and type of available media ports on the MCU is controlled by the port capacity mode - which you configure on the [Settings > Media ports](#) page.

Unreserved mode

This is the mode that the MCU runs in when the **Media port reservation** setting is configured as *Disabled*, and is the mode that the MCU uses by default. With this scheme, you can specify a maximum value for the number of video and audio-only ports each conference is allowed to use on the Conference configuration page. These limits are optional, and by default there is no configured limit.

The configured limits are strictly *maximum* values; in particular, setting such a limit does not guarantee that that many participants will be able to join the conference. It is perfectly possible to set these values such that the sum of the configured limits across all active conferences exceeds the total number of ports available on the MCU.

Reserved mode

This is the mode that the MCU runs in when the *Media port reservation* setting is configured as *Enabled*. With this scheme, each conference must be configured with a number of video ports to reserve and a number of audio-only ports to reserve. These values differ from the maximum port values set in [Unreserved mode](#) in a number of ways:

- **Reservations are guaranteed**
As well as being maximum values (i.e. enforcing limits on the number of conference participants), port reservation values also guarantee that that many endpoints are able to participate in the conference.
- **Port reservations are mandatory**
In unreserved mode, it is not necessary to specify a number of video or audio-only ports for a conference. In reserved mode, however, every conference must have configured reservations for both video and audio-only ports.
- **Over-allocation is not permitted**
Port reservations guarantee that a certain number of participants will be able to join a conference; because of this, the MCU will not permit these reservations to be configured such that the total number of reserved ports at any given time exceeds the total number of ports available. See [Clashing reservations](#) for additional information.

Clashing reservations

In order to honor configured port reservations, the MCU must ensure that at any given time the number of reserved ports does not exceed the total media capacity. This entails some level of *clash detection* when you schedule conferences or change their configuration.

The MCU considers two conferences to be clashing if they can ever be active simultaneously. When validating a conference schedule, the MCU looks at the maximum number of ports reserved by other conferences which can be active at the same time, and checks that the number of ports requested by the conference being added or changed is guaranteed to be available. If, for instance, the MCU has 20 video ports available in total, it will not be possible to set up two conferences which require 15 video ports each if they are scheduled such that they ever overlap.

In the simple case of conferences which start at specific times and end at specific times (or, indeed, are permanent), it is easy to see whether they clash. The more complex cases involve repetition, and it is important to bear in mind that port reservations are only permitted when the MCU can guarantee them for **every** repetition of a conference. As an example, a conference scheduled to run from 08:00 to 10:00 on the second Monday of each month will be deemed to clash with a conference configured to run from 09:00 to 09:30 *every* Monday, even though the former will only really clash with the latter every fourth or fifth week.

In general, to make best use of the available MCU media ports, you should not schedule conferences to be longer than needed, and you should limit repetitions, either by end date or number, wherever possible.

Ad hoc conferencing

Because port reservations are mandatory in **Reserved mode** every active conference must have configured values for the number of video ports and the number of audio-only ports to reserve for it. In turn this means that every active conference must be configured, and therefore *ad hoc conferences* are not permitted when in **Reserved mode**.

This affects the operation of the MCU in the following ways:

- **Auto attendant usage**
In reserved mode, the [Create new conference](#) option will not be shown on video auto attendant menus, even for auto attendants configured to display this option.
- **Auto attendant configuration**
When configuring new or existing [auto attendants](#) via the web interface, the *Creation of new conferences* parameter will not be available.
- **Calls to unknown E.164 number configuration**
This setting on the [Conference settings](#) page also offers a *Create new conference* option. This is not available in reserved mode and becomes equivalent to the *Disconnect caller* option.

Auto attendant connections

If a participant calls in to the MCU and connects to an auto attendant, the MCU does not know which conference they will join until they make a selection from the auto attendant menu.

In [Unreserved mode](#), the auto attendant connection allocates a media port from those not currently in use. If all of the media ports are in use, the endpoint's connection will be dropped by the MCU.

In [Reserved mode](#), the auto attendant connection effectively "borrows" a media port from those not currently in use. However, this borrowed media port has a lower priority than a media port used by a conference participant, and if the auto attendant connection "borrows" the last remaining media port, then that connection will be dropped if another endpoint connects directly to a conference and requires a reserved media port.

Changing MCU port reservation mode

In general, changing port reservation mode when there are active connections is not recommended. The effects of changing mode include, but are not necessarily limited to:

- **Destruction of ad hoc conferences**
Any ad hoc conferences in progress will be destroyed when changing to port reservation mode and their participants dropped because [ad hoc conferences](#) are not permitted in port reservation mode.
- **Participant disconnection**
Participants in a scheduled conference may be disconnected. For each conference, the maximum port usage values (for unreserved mode) and the ports to reserve (for reserved mode) are configured and stored separately. Therefore when changing port reservation mode, it is possible that there are more active participants than allowed in the particular mode. In this case, participants are disconnected to reduce the number to that allowed.

Related topics

- [Adding and updating conferences](#)
- [Configuring global conference settings](#)

Content channel video support

The MCU supports an additional video channel known as the *content channel* for each conference. This feature encompasses:

- H.239 video streams sent from the MCU to viewing H.323 endpoints
- Sourcing the content channel from an H.323 endpoint's H.239 video stream or a SIP endpoint supporting content using BFCP
- Streaming the content channel to users' desktop machines as a pane in the conference view
- Streaming the content channel to users' desktop machines as a separate window (where markup and text chat can also be used)(*)
- Showing the content as part of the *main video* channel, where an endpoint cannot, for whatever reason, receive the content channel as an additional video channel. That is, the participant will see the content as a pane in the conference layout
- Content

Content channel vs. main video

The H.239 protocol allows the MCU to support an additional video stream to or from each connected endpoint. Therefore, there are potentially three media streams between each endpoint and the MCU: audio, main video and content video.

The *main video* is the normal multi-pane conference view showing participants' video streams composed within the selected layout. The differences between the content channel video and the *main video* are:

- **Single layout**
Each participant in a conference can normally select their own individual main video layout (e.g. a 2 x 2 grid of other participants, one large focused pane plus eight smaller panes) and they are free to change this layout as many times as desired while they are connected to the conference.
By comparison the content channel video always shows just a single video stream, "full screen", and each viewing endpoint will see the same stream. The stream which constitutes the content channel can change

any number of times during the conference, but there can be at most one contributing stream at any given moment.

- **One channel per conference**

Each participant's main video stream is encoded independently; this means that each endpoint can be receiving its main video stream at a different bit rate, codec, or resolution to that being sent to other participants.

However, there is a single content video stream per-conference: the MCU sends the same bit rate and resolution to all endpoints receiving content. The bit rate and resolution used is chosen to maximize the number of viewers - for instance the resolution might be reduced if a new endpoint joins the conference and its content receive capabilities are more limited than those of the other participants. Note that in conferences that use encryption, the MCU can send encrypted and unencrypted content to different participants in the same conference (albeit with the same encryption key for every participant receiving encrypted content).

- **Differing characteristics**

The range of bit rates, resolutions and frame rates available to the MCU for sending the content channel via H.239 to H.323 video conferencing endpoints is potentially as wide as that for the main video channel.

However, in general, the main video channel is used for motion video (i.e. high frame rate streams) and the content channel for less dynamic video such as an accompanying presentation - typically high resolution, low frame rate.

However, the MCU allows flexibility in terms of nominating which of the available streams forms the content channel, as well as allowing control over which endpoints are permitted to start contributing content video.

- **Uni-directionality**

For the main video channel, a video conferencing endpoint would normally be both contributing (sending) a video stream to the MCU and receiving a video stream from it.

However the content channel works differently in that an endpoint can either be sending content video or receiving content video, but not both. A given endpoint may switch between being the contributor and a viewer during the conference, but it will never be both simultaneously.

Passthrough and hybrid content

In versions prior to 4.3, the MCU always decoded the incoming content stream and then re-encoded it using either H.263+ or H.264 before sending it out. This original mode is called *Transcoded* content. As of version 4.3, the MCU can be configured to pass-through a content stream without transcoding it to participants that can support the same content codec as the source content stream. This can reduce latency and increase quality and does not require a video port on the MCU. This is known as *Passthrough* content.

There are drawbacks with both of these content modes. In *Transcoded* mode, all participants will see the content encoded with the specified outgoing transcoded codec and a single participant could reduce the quality for other participants if it had limited codec support. In *Passthrough* mode, the MCU does no transcoding for content, which means that fewer endpoints may be able to decode the passed through content.

Hybrid content mode helps to avoid these drawbacks. In *Hybrid* mode, the incoming content stream is passed through to participants who are able to support the same codec as the original content stream (the *Passthrough* content stream). The MCU also encodes a second content stream with the specified outgoing transcoded codec for participants who cannot decode the original *Passthrough* content stream. *Hybrid* content mode uses up a video port.

The **Outgoing transcoded codec** for the content stream can be explicitly specified (either *H.263+* or *H.264*) or set to *Automatic*.

To edit these settings, go to the **Content** section of the conference's configuration page (go to **Conferences** then click on the conference name).

H.323/SIP endpoints' content channel support

For H.323 endpoints, depending on the specific endpoint and how it is configured, the content video stream may be displayed on a separate screen, or the endpoint may show the main video and the content video streams side by side on the same screen.

Irrespective of its content receive capability, an endpoint may or may not be able to contribute the content channel - typically, for this to be possible it will either need a second camera or some other video input such as a VCR or "video in" connection.

Some H.323 endpoints may have no support for the H.239 protocol. However, it is still possible for such endpoints to display the content channel - the MCU is able to show the content channel within a normal view pane in the same way as it displays other conference participants. This ability is controlled by the [unit-wide/blade-wide Display content in normal video channel](#) setting (see [Configuring content settings](#)).

Content channel sources

As described [above](#), a conference's content channel as sent to the set of receiving endpoints has a single source. There are several possible content channel sources:

- **H.239 video channel**

This is the most conventional content channel behavior - a H.323 conference participant opens a H.239 channel to the MCU and contributes a video stream, such as that supplied by a second camera or an attached PC.

Because there can be at most one content channel source, the H.323 endpoint needs to make a request to the MCU, and have that request accepted, before actual content channel contribution can start. If the conference already has an active content channel (for example, another endpoint is contributing H.239 video), the new request will be rejected by the MCU - it will be necessary to wait for the active contributor to cease sending H.239 video before the new endpoint is able to start. However, if you have enabled **Automatic content handover** (on the **Settings > Content** page), the new request will be granted automatically.

- **BFCP video channel**

BFCP (Binary Floor Control Protocol) is a protocol that allows for an additional video channel (known as the content channel) alongside the main video channel in a video-conferencing call that uses SIP. A SIP conference participant opens a BFCP channel to the MCU and contributes a video stream, such as that supplied by a second camera or an attached PC.

Because there can be at most one content channel source, the SIP endpoint needs to make a request to the MCU, and have that request accepted, before actual content channel contribution can start. If the conference already has an active content channel (for example, another endpoint is contributing content video), the new request will be rejected by the MCU - it will be necessary to wait for the active contributor to cease sending content video before the new endpoint is able to start. However, if you have enabled **Automatic content handover** (on the **Settings > Content** page), the new request will be granted automatically.

Note that the transmission of SIP content using BFCP is not supported on encrypted calls in any content modes. To allow content to be transmitted over SIP calls in a separate channel from main video, disable encryption on the MCU or on the target endpoint.

- **Participant main video**

It is also possible for the MCU to use a endpoint's main video channel as the conference's content channel (when in Transcoded or Hybrid content modes).

MCU content channel configuration

Unit-wide or Blade-wide configuration

At the MCU-wide level, the MCU can be configured to disallow the use of conference content channels completely.

You can choose to enable encryption on the MCU. When encryption is used, the content channel will be encrypted.

For more information on these configuration parameters, see [Configuring content settings](#) and [Configuring encryption settings](#).

Per-conference configuration

Assuming that content is enabled on the MCU unit-wide/blade-wide, each scheduled conference can be independently configured to allow content channel operations or not. If enabled, this has an impact on the conference's [port usage](#); if disabled, then all attempts by participants in that conference to open a content channel to the MCU will be unsuccessful.

If the MCU is configured to allow encryption, each individual conference can be configured to either require encryption or to optionally use encryption. The MCU can send either encrypted or unencrypted content to different participants in a conference depending on the capabilities of those participants' endpoints.

For more information on the conference configuration parameters relevant to the content channel, see [Adding and updating conferences](#).

Per-participant parameters

Content contribution

Content contribution refers to the ability of video conferencing devices to contribute the content channel video for a conference via the mechanism of opening a separate video channel, distinct from its [main video](#) stream. Specifically, this section does not deal with the use of content by the MCU when sending content channels to viewing devices or the use of other protocols to supply the content channel video for a conference.

For a conference configured with content channel video enabled, each endpoint in that conference is either permitted or prohibited from being able to contribute content video. H.239 is the protocol used by H.323 video conferencing endpoints to supply or receive content channel video; BFCP is the protocol used by SIP video conferencing endpoints to supply content channel video. Other content channel source configurations do not depend on any H.239 or BFCP contribution parameters.

Remember that what is termed *Content contribution* is more precisely described as the ability to **start** contributing content channel video via H.239/BFCP. The nature of the H.239 and BFCP protocols used between the MCU and endpoints is such that once an endpoint has successfully become the content source for a conference, the MCU is not then able to force that endpoint to stop contributing the content channel video.

While an endpoint is supplying the content channel for a conference, it is considered to be holding the virtual *content token* for the conference. This token must be relinquished before either another endpoint can start contributing video via H.239 or BFCP or a content channel source becomes active. This token is normally released by a specific endpoint operation (e.g. a "stop content" option), or by that endpoint leaving the conference. However, when **Automatic content handover** is enabled, the MCU will ask the endpoint (or computer) to return the token if there is another participant who wants to start contributing content.



When **Automatic content handover** is enabled, it allows another participant to start sending content without having to wait for the current content provider to stop sending content from his computer. In this case, the MCU will start sending the 'new' content to the participants in the conference and will ask the endpoint (or computer) that was originally providing content to return the token. **Automatic content handover** is a unit-wide/blade-wide configuration option on the **Settings > Content** page.

By default, participants' ability to contribute content video (technically, as above, to **start** contributing H.239 or BFCP video) is determined by the per-conference **Content contribution from endpoints** setting (**Conferences > Add new conference**).

The per-conference default **Content contribution from endpoints** setting can be overridden by individual endpoints' configuration. If such an endpoint's *Content contribution* setting is *<use conference default>* then the endpoint's ability to contribute content channel video will be determined initially from the conference setting. If the endpoint setting is *<enabled>* or *<disabled>* then this will override the conference setting and that endpoint will either always be prevented from using content, or always permitted (assuming the conference of which it is part is configured with content channel support). As well as being part of each endpoint's configuration, the **Content contribution** setting can also be specified when calling out to an endpoint by address.

Irrespective of per-conference or per-endpoint configuration parameters, if a conference is configured to allow content channel operations then it is possible to explicitly enable or disable individual conference participants' ability to use content via the web browser interface (assuming a user login with [full conference control](#)).

To change the content contribution setting for an active conference participant via the web interface, first navigate to that participant's **Display** page (go to **Conferences** and click the conference you want and then click on the name of the participant whose settings you want to change). If the conference has content enabled and the endpoint in question has content capabilities, you should be able to use one of the following controls:

-  allow participant to contribute content video
-  do not allow participant to contribute content video



If an endpoint's ability to contribute content video has been explicitly enabled or disabled via this mechanism, that enablement or disablement will take precedence over any current or future conference or participant configuration, even if the endpoint later moves to a different conference.

Use of main video as content channel

In addition to supporting the H.239 and BFCP protocols by which endpoints in a conference can supply the content channel video, the MCU also allows a participant's [main video](#) channel to be used for the content stream.

As detailed above, it is not possible to force an endpoint that has [started to contribute content video](#) to relinquish the virtual token that it holds. Thus, if you select an endpoint's main video channel to be the content channel source, this will only take effect if no other endpoint is supplying the content channel video stream (whether by H.239, BFCP, or through use of its main video stream). However, if you have enabled **Automatic content handover** on the **Settings > Content** page and you select an endpoint's main video channel to be the content source, this will take effect even if there is currently another content source in the conference.

To control the use of a participant's main video as the conference content channel source, the following controls are displayed on the per-conference participant list (next to the preview image of the video stream to which they relate):

-  use this participant's main video stream as the content channel
-  stop using this participant's main video stream as the content channel (revert to more conventional content channel behavior such as H.239)

In rare circumstances, if more than one participant's main video channel is configured to provide the content channel (for example where a participant configured in this way is moved to another conference where there is an existing participant providing his main video channel as the content channel), then all but the active (normally, first) one will be marked with the status: *Content: unable to use main video as source*

Port usage

Port reservation mode

Cisco TelePresence MCU 4200 Series and Cisco TelePresence MCU 5300 Series

If the MCU is operating in [reserved mode](#), enabling content for a conference requires the use of an additional video port. A single video port is needed for all content channel operations, irrespective of how many viewers there are; for example, a conference involving five video endpoints (one of which is contributing a content stream and the other four viewing it) will require six video ports - **Video ports to reserve** should be set to 5, and **Content channel video** set to "Enabled" in this specific example.

In reserved mode, a conference with content enabled will require a video port for content operations even if no current participants are actively making use of content.

Note that for the Cisco TelePresence MCU 4203, there are separate ports for content. For more information, refer to [MCU port matrix](#).

Cisco TelePresence MCU 4500 Series and Cisco TelePresence MCU MSE 8510

If the MCU is operating in [reserved mode](#), enabling content for a conference does not use a video port; instead, content uses one of the additional content ports provided by your MCU. A single content port is needed for all content channel operations, irrespective of how many viewers there are; for example, a conference involving five video endpoints (one of which is contributing a content stream and the other four viewing it) will require five video ports and one content port - **Video ports to reserve** should be set to 5, and **Content channel video** set to "Enabled" in this specific example.

In reserved mode, a conference with content enabled will require a streaming and content port for content operations even if no current participants are actively making use of content.

For more information about the number and types of ports provided by your MCU, refer to [MCU port matrix](#).

Unreserved mode

If the MCU is operating in [unreserved mode](#), enabling content for a conference will require a port to be allocated when content channel operations are first attempted for that conference. For instance, this could be when a participant opens a content channel or a user starts viewing the content channel via their web browser. When the port is no longer needed for the conference's content channel (e.g. when the last remaining participant disconnects) the port will be released for use by future participants or conferences.

Ad hoc conferences

All of the above-mentioned features, for instance content video streams between the MCU and video conferencing endpoints, are available for use with both scheduled and ad hoc conferences.

However, whereas for scheduled conferences the availability of content is determined by a per-conference configuration setting, for ad hoc conferences it is only possible to enable or disable content on a device-wide basis. This is accomplished via the **Content for ad hoc conferences** option on the [Content settings](#) web page—if this is "Enabled" then any ad hoc conference on the MCU may use content; if "Disabled" then none may do so.

Ad hoc conferences are not permitted when operating in [reserved mode](#).

Related topics

- [Configuring content settings](#)
- [Conference content channel](#)
- [Configuring H.323 endpoints](#)
- [Configuring SIP endpoints](#)

Controlling in-conference features

You can control many conference features from the MCU web browser:

- [Adding participants](#)
- [Viewing the participants list](#)
- [Customizing layout views](#)
- [Displaying conference statistics](#)
- [Sending messages to all participants](#)

Adding participants

You can add a participant to a conference in two ways: either on an "ad hoc" basis, where an endpoint previously unknown to the MCU is only configured when it is immediately required, or on a preconfigured basis, where the MCU uses its record of the endpoint in the conference configuration. An ad hoc participant's details must be provided each time the MCU invites it, while a preconfigured endpoint can be added to a conference in advance to be called whenever the conference is active. This is especially useful for recurring conferences. See [Adding preconfigured participants](#).

To call an endpoint immediately you can enter a participant's endpoint details or select a preconfigured endpoint and call out. The endpoint can be an H.323 or SIP endpoint. Follow the links below for the detailed procedures:

- [Adding an H.323 participant](#) (ad hoc)
- [Adding a SIP participant](#) (ad hoc)
- [Adding preconfigured participants](#)

Note that participants called by the MCU will have chairperson privileges by default. For more information about chairperson and guest privileges, refer to [Using IDs and PINs](#) in the Adding a conference topic.

Adding an H.323 participant

To call a participant with an H.323 endpoint into an active conference:

1. Go to **Conferences** to display the Conference List.
2. Click a Conference name and then click **Add participant**.
3. To add a new endpoint (one that you have not added as a configured endpoint):
 - i. Select the *H.323* radio button and in **Address**, enter the IP address, E.164 number, or H.323 alias of the participant's endpoint.
For information about other conference settings, refer to [Configuring H.323 endpoints](#).
 - ii. Click **Call endpoint**.
4. To invite an existing (configured) H.323 endpoint:
 - i. Scroll down to the **Endpoints** section and select the check box next to the endpoint name.
 - ii. Click **Add selected**.

Adding a SIP participant

To call a participant with a SIP endpoint in to an active conference:

1. Go to **Conferences** to display the Conference List.
2. Click a Conference name and then click **Add participant**.
3. To add a new endpoint (one that you have not added as a configured endpoint):
 - i. Select the *SIP* radio button and do one of the following:
 - For **Address**, enter the IP address, or SIP URI of the participant's endpoint (in the format 1234@example.com).
 - For **Address**, enter the number registered with the SIP registrar and select **Use SIP registrar** (ensuring that you have configured a SIP registrar on the **Settings > SIP** page).
For information about other conference settings, refer to [Configuring SIP endpoints](#)
 - ii. Click **Call endpoint**.
4. To invite an existing (configured) SIP participant:
 - i. Scroll down to the **Endpoints** section and select the check box next to the SIP endpoint name.
 - ii. Click **Add selected**.

Adding pre-configured participants

You can choose participants whose endpoints have been configured previously to be part of a scheduled conference. These participants will be automatically invited into the conference by the MCU every time the conference runs. This is useful if you regularly invite the same participants into a conference.

You can preconfigure up to 200 endpoints in this way.

To add previously configured endpoints to a conference:

1. Go to **Conferences** to display the Conference List.
2. Click a Conference name and then click the **Configuration** tab.
3. Click **Pre-configured participants**. The pre-configured participants page will be displayed. This page lists all the endpoints that have been configured on the MCU (see [Configuring an H.323 endpoint](#) and [Configuring a SIP endpoint](#)).
4. Select which endpoints you would like to add as pre-configured participants in this conference.
5. Press **Return to conference configuration**.
6. Make any other changes you require to the conference configuration, then click **Update conference**. (If you do not click **Update conference**, you will lose the selections of configured endpoints made in the previous steps.)

Related topics

- [Displaying conference lists](#)
- [Configuring H.323 endpoints](#)
- [Configuring SIP endpoints](#)

Customizing layout views

You can select custom layouts to use for all conference participants. To use this option:

1. Go to **Conferences**.
2. Click a Conference name and then click the **Custom layout** tab.
3. Click on the layout you want to use from those shown in the **Available layouts**. There are different numbers of panes and pane configurations to choose from.

The chosen layout is displayed enlarged to the left in the **Conference custom layout** section of the page and the *Enabled* radio button is selected.

4. If you want to select the participants who appear in a pane manually rather than letting the MCU make the most appropriate selection, click **Pane placement**.
See [Using pane placement](#) below.
5. To have all participants see this layout when they join the conference click **Make new participants see this view**.
6. If you also want all participants to see this view now, click **Switch all participants to this view**.

The following table explains the details that display.

Field	Field description	Usage tips
Conference custom layout		
Current status	Whether a custom layout can be used for this participant.	When you click a new layout from the Available layouts , <i>Enabled</i> is automatically chosen with the most recent layout selected.
Make new participants see this view	New participants joining this conference will view the conference with this custom layout rather than one of the default views (see Customizing a participant's layout display). To force all participants to use this layout, click Switch all participants to this view .	If a participant has chosen to use a custom conference layout (see Customizing a participant's layout display), their view will automatically update and switch to the new view.
Available layouts		
	Displays all the conference layouts that are available. Click a layout to select it and make it available.	You can only select one custom layout at a time.

Using pane placement

To have more control over which participant appears in which pane, you can use the Pane placement function. Pane placement works on a per conference basis.

Pane placement works on the selected custom layout in the **Conference custom layout** page - see [Customizing layout views](#). The chosen custom layout is shown with the panes numbered. The largest (and therefore most important) panes have the lowest numbers. Because the largest number of panes in any custom layout is 20, there are twenty drop down lists, one per pane. If the number of panes in the chosen layout is less than this, a gray line separates the panes that are used from those that do not apply to this layout.

The first time you open the pane placement page for a conference all the panes are set to <default>. The MCU decides which participant will appear in panes with this setting. See [Understanding how participants display in layout views](#) for more information.

For each pane you can select an alternative setting:

- <blank>: no participant appears in this pane
- <rolling>: this pane shows conference participants, automatically changing at the configured "Pane rolling interval" frequency from the **Settings > Conferences** page. All participants contributing video are shown in rolling panes except for any participants explicitly placed in other panes.

Note: Rolling panes stop rolling if the number of rolling panes is greater than or equal to the total number of video participants. In this scenario, participants will only be shown in the rolling panes and the default panes will remain black. This is to stop participants being shown more than once.

- **<loudest speaker>**: the participant who is speaking the loudest at any time appears in this pane
- **<content>**: this pane is reserved for the content channel (see [Content channel video support](#)). If the content channel is not used in this conference, this pane will be blank.
- **<name>**: the name of each pre-configured endpoint in this conference, and (if the conference is active) the names of all active participants whose endpoints were not pre-configured is displayed in the lists. If you select a specific participant (endpoint), that participant appears in this pane at all times.

To use pane placement:

1. Click *Enabled*.
2. For each pane that you want to control, select an entry from the drop down list.
3. For panes that you no longer want to control individually, select *<default>*.
4. Click **Update pane placement**.
5. To return to the **Custom layout** page, click **Custom layout**.

More about pane placement

When you use pane placement, bear in mind that:

- Pane placement only applies to conference custom layouts. If they are disabled so is pane placement
- You can mix panes set to *<default>* with panes that have other settings
- Any panes that you configure keep their setting even if you change the custom layout view. Therefore if you configure all the panes in the 20 pane layout and then move to one with only five panes, panes 1 to 5 will have the same settings as before. Panes 6 to 20 will also keep their settings, it is just that they are not used. Therefore if you subsequently move to a layout with say 10 panes, all ten panes have their settings pre-configured.
This does mean that if you have participants who need to be seen at all times, you should configure them in the lower numbered panes
- You must set up pane placement for each conference that you want to use it with
- You can set up pane placement before a conference starts and configure pre-configured endpoints in to particular panes. However you can only configure active participants whose endpoints are not pre-configured when the conference is running
- Pane placement persists over conference repetitions. If you set pane placement once, the same placements are ready to be used when the conference next repeats
- If you select a particular participant for a pane and they are disconnected for any reason, that pane appears blank
- After you set up pane placement, you can still change the layout for individual participants - and they can change their layout using the far-end camera controls unless you disable this for each participant individually. See [Customizing a participant's layout display](#).
- The left and right controls on a participant's far-end camera control, used to select a focused participant, have no effect when pane placement is in use
- Potentially, when pane placement is in use, a participant may appear in two panes at the same time. This happens for example if a pane is configured to show a particular participant and another pane is configured to show the loudest speaker; each time that participant is the loudest speaker, he will appear in both panes.

There is a setting on the MCU's [Settings > Conferences](#) page to control this behavior called **Loudest speaker pane placement behavior**

Related topics

- [Customizing a participant's layout display](#)
- [Understanding how participants display in layout views](#)
- [Content channel video support](#)

Displaying conference statistics

You can display statistics about a conference and use the information to quickly see how many participants are currently in the conference.

To access this option:

1. Go to **Conferences**.
2. Click a Conference name and then click the **Statistics** tab.

If the conference is active, statistics for that conference will be displayed. If the conference is completed only "No longer active" will be displayed.

Refer to the table below for information on interpreting this information.

Field	Field description
Start time	When the conference started.
End time	When the conference will complete. This will be the time at which the maximum duration of the conference will have elapsed. This setting displays as <i><permanent></i> if it has been configured to last forever.
Running time	The duration of this conference.

(Chairperson) gatekeeper ID	The status of a conference with respect to its H.323 gatekeeper and/or SIP registrations. The possible states are:
Guest gatekeeper ID	<ul style="list-style-type: none"> ■ <i>n/a</i> This conference is not configured to be registered with a gatekeeper or SIP registrar; because of this, there is no applicable registration status to show. ■ <i><number> registered</i> The conference has been registered successfully with the gatekeeper or SIP registrar and can be contacted using the number indicated.
(Chairperson) SIP registrar ID	<ul style="list-style-type: none"> ■ <i>Registering</i> This conference is in the process of registering with the gatekeeper or SIP registrar. ■ <i>Deregistering</i> The conference is in the process of unregistering with the gatekeeper or SIP registrar. This might occur if: <ul style="list-style-type: none"> ● Gatekeeper registration has been turned off (either for that conference only or for the entire MCU) ● The configured gatekeeper has just been changed and the MCU is in the process of unregistering from the previous gatekeeper before registering its conferences with the new one. ■ <i>Re-registration pending / Retry timeout</i> If the MCU fails to register a conference with the gatekeeper or SIP registrar, it enters these states temporarily before re-attempting the registration. ■ <i>Registration disabled</i> This ID has been specifically configured to be registered with the gatekeeper or SIP registrar, but some other configuration has overridden this, causing the registration to not be attempted. This state might occur if either of the H.323 gatekeeper usage or ID registration for scheduled conferences options on the Settings > Gatekeeper page is set to <i>Disabled</i>. ■ <i><no ID set></i> The conference is configured to register with a gatekeeper or SIP registrar, but has not had a numeric identifier set.
Guest SIP registrar ID	
Number of audio/video participants	The current number of contributing audio/video participants.
Highest number of audio/video participants	The largest number of contributing audio/video participants who have been in the conference at the same time.
Number of audio-only participants	The current number of contributing audio-only participants.
Highest number of audio-only participants	The largest number of contributing audio-only participants who have been in the conference at the same time.

Related topics

- [Adding participants](#)
- [Viewing the conference participant list](#)

Sending messages to all participants

You can send messages to all participants in a conference simultaneously. To access this option:

1. Go to **Conferences**.
2. Click a Conference name and then click the **Send message** tab.

This message appears overlaid on each participant's view.

Field	Field description	Usage tips
Message text	Enter the message to send to all conference participants.	Messages must be fewer than 256 characters, but depending on the viewing screen, messages at the higher-end of this limit might not display properly. Therefore, consider limiting messages to approximately 180 characters. Messages longer than 256 characters will not be truncated; they will not display at all. You can disable this setting from Settings > Conferences (see Configuring global conference settings).
Position	The vertical position of the message on the conference display.	Select from the top, middle, or bottom of the conference display.
Duration	How long the message appears on participants' video screens.	The default setting is 30 seconds. To remove all messages before they time out, click Clear message .

Related topics

- [Sending messages to individual participants](#)
- [Configuring global conference settings](#)

Managing participants

You can view detailed information about conference participants:

- [Viewing the conference participant list](#)
- [Customizing a participant's layout display](#)
- [Controlling the near-end camera](#)
- [Managing a participant's audio signals](#)
- [Creating a custom participant view](#)
- [Displaying statistics for a participant](#)
- [Sending messages to one participant](#)
- [Displaying diagnostics for a participant](#)
- [Moving a participant](#)

Viewing the conference participant list

The **Participant list** displays information about active and previous participants in the conference. To access this list, go to **Conferences** and click a Conference name. This page explains the information available in the participant list.

On this page:

- [Conference information](#)
- [Lock conference](#)
- [Active participants](#)
- [All-participant controls](#)
- [Previous participants](#)
- [Pre-configured participants](#)
- [Summary information](#)

Conference information

Above the list of participants, certain information about the conference is displayed:

- **This conference is being recorded:** If the conference is being recorded on an IP VCR, this message will appear.
- **Port usage:** Each conference may have either imposed limits on the maximum number of media ports it is able to use, or a certain number of media ports reserved for its use. This section shows the video port and audio-only port reservation or limit.
See the full description of [Port reservation](#) for additional information.
- **Content channel:** Whether the content channel is in use or not for this conference.
- **Encryption:** If you have the encryption feature key enabled, the encryption status of the conference will be shown, which will either be *not required* or *required*.

Lock conference

A locked conference is one where new participants cannot dial in. Existing participants will maintain their connection to the conference.

If a conference is locked, an icon will indicate this on the auto attendant. The auto attendant will also display the text: 'This conference is locked'.

Note that participants that are pre-configured via the API will be able to dial in to the conference even if it is locked. This allows conferences to be restricted to specific participants (known as whitelisting).

Admin users and the conference owner can lock and unlock a conference.

When the final participant leaves, by default, the conference will be automatically unlocked by the MCU. However, you can configure the MCU to keep a conference locked even when the final participant leaves. To configure this feature, go to **Settings > Conferences > Advanced settings**.

When a conference is locked, admin users and the conference owner will still be able to connect new endpoints and disconnect participants.

To lock a conference:



1. Go to **Conferences** and click on the name of the conference you want to lock. The Conference's Participant List displays.
2. Click **Lock conference** in the top right-hand corner of the page.

Active participants

Refer to the table below for details about the active participant list, which you can modify in the following ways:

- You can end the conference, forcing all participants to be dropped, by clicking **End conference**. For conferences that are "scheduled" rather than "ad hoc", ending the conference in this way causes any configured repetition to be cancelled. The ended conference would move from the "Scheduled conferences" list to the "Completed conferences" list. The configured duration of a completed conference reflects the actual duration of the conference rather than its original configured duration. For example, if a conference was scheduled to run from 09:00 until 10:00 (one hour) and the conference ended at 09:25, the configured duration would be changed to 25 minutes.
- You can add a new H.323 or SIP video conferencing endpoint to the conference (either creating a new endpoint or by choosing an existing one) by clicking **Add participant**. See [Adding participants](#).

Field	Field description	Usage tips
Type	Indicates whether the participant's endpoint is an H.323 or SIP endpoint.	

Participant	Displays the name of the endpoint.	
	The following may also be displayed:	
	<p><i>User: <user id></i></p> <p>If the participant has been resolved to a particular configured user (for instance by matching the participant's E.164 phone number against a configured value), then the appropriate user id will be shown here.</p>	<p>User names only display if the participant list is being viewed by an administrator, because only administrators have access to the configured user database.</p>
	<p><i>Configuration: <name></i></p> <p>This indicates that this participant corresponds to a pre-defined endpoint. The <name> shown is the endpoint's configured name.</p>	<p>Configured endpoint names only display if the participant list is being viewed by a user whose privilege level is <i>administrator</i> or <i>conference creation and full control</i>; only users with these privilege levels have access to the configured endpoint database.</p>
Importance control	<p> Applies important status to this participant.</p> <p> Removes important status from this participant.</p>	<p>When you make a participant "important", it sets this participant as the focused participant. For example, this participant is considered the loudest participant even if they are not speaking.</p> <p>Only one participant can be identified as "important", and no participant is set to "important" by default.</p> <p>This option affects the layout views for the conference and individual participants. See Selecting a custom participant view and Customizing layout views.</p> <p>If the content channel is made "important", one participant can still be important. On endpoints that support content, the content channel will be displayed in the content channel window and the important participant will be given the focus in the main video window. On endpoints that do not support content, the important participant will be ignored as the content channel will be given the focus.</p>

Mute controls

Some of these controls are not present on the participant list by default:



Prevent other participants from hearing this participant (like mic. mute).



Allow other participants to hear this participant's audio (like mic. unmute)



Prevent others from seeing this participant's video contribution (like camera mute).



Allow others to see this participant's video contribution (like camera unmute).



Prevent this participant from hearing the conference (like speaker mute).

Note: The endpoint may not always detect DTMF tones from the MCU after you mute the audio from the MCU.



Allow this participant to hear the conference (like speaker unmute).



Prevent this participant from seeing the conference (like screen mute).



Allow this participant to see the conference (like screen unmute).

You can configure whether these controls are shown by changing the **Participant list controls** on the [Settings > User interface](#) page (refer to [Customizing the user interface](#)).

If the controls are not configured to be shown, and if a participant has joined with a media channel muted, the relevant control appears temporarily to enable you to unmute the channel if required.

Disconnect control

Disconnects a participant from the conference

You can configure the MCU to require confirmation when someone attempts to disconnect an individual participant from a conference. This setting is on the [Settings > User interface](#) page.

Status	<p>Displays the time at which a participant connected to the conference. If a participant is not yet fully connected (for example, if the MCU has called a participant but it has not yet answered), then that is indicated here. The resolution of the participant's video stream is also displayed.</p> <p>The following additional indications may also be displayed:</p>	<p>If this column is selected as the sorting field, the listing is ordered according to when the participants connected to the conference.</p>
	<p><i>Waiting to redial:</i> The participant is not currently connected to the conference, but the call is persistent and the MCU is between redial attempts.</p>	
	<p><i>Recording:</i> Indicates that the conference is being recorded.</p>	
	<p><i>Encrypted</i> indicates that all media streams in both directions (to and from the endpoint and the MCU) are encrypted.</p> <p><i>Rx encrypted</i> indicates that all media streams received from this participant are encrypted.</p> <p><i>Tx encrypted</i> indicates that all media streams sent to this participant are encrypted.</p>	<p>Next to the encryption indication is the AES check code. This can be used in combination with information displayed by some endpoints to check that the encryption is secure.</p>
	<p><i>Pre-configured</i> indicates that this participant is in the conference because of a pre-configured endpoint.</p>	<p>See Adding pre-configured participants for additional information on adding endpoints to conferences in this way.</p>
	<p><i>No audio capabilities, No video capabilities</i></p> <p>These messages indicate that the MCU has not opened a media channel to a participant's endpoint because it has no capability to receive that type of channel. For example, if the endpoint is a simple telephone, you might expect to see "No video capabilities" shown here.</p>	
	<p><i>No common audio codecs, No common video codecs</i></p> <p>These messages indicate that the remote endpoint had declared media capabilities, but the MCU was not permitted to open a channel that the endpoint was prepared to receive.</p>	<p>This is most likely to occur if you have disabled one or more codecs in the "Audio codecs from MCU" or "Video codecs from MCU" configuration on the Advanced conference settings web page.</p>
	<p><i>No common audio formats, No common video formats</i></p> <p>These messages indicate that the remote endpoint had declared media capabilities including codecs that the MCU was permitted to send, but that the MCU was unable to transmit the specific formats declared.</p>	<p>This could occur if, for instance, the far end's advertised receive video sizes were all 4CIF (704 x 576 pixels) or above, and the MCU was set to not transmit above CIF (352 x 288 pixels).</p>
	<p><i>No common symmetric audio codecs, No common symmetric video codecs</i></p> <p>Indicates that the MCU was unable to open a media channel to the endpoint because the only possible channels it would be able to open were invalid due to a symmetry clash. This clash occurs when the remote endpoint declared that it is only able to receive certain types of media if it is also sending the same format, and the format in question is one that the MCU is able to send but not receive.</p>	

Audio port limit exceeded, Video port limit exceeded

These messages occur if a channel was unable to be opened solely because doing so would have exceeded the port limit. This limit may be a per-conference restriction or, for those conferences which impose no such limit, it could be that all of the MCU's available ports were in use.

Endpoint audio and video channels rejected, Endpoint audio channel rejected, Endpoint video channel rejected

Indicates that the MCU is unable to receive the media format that the endpoint is trying to transmit.

Tx: briefly describes the audio and main video streams transmitted by the MCU to this participant.

Rx: briefly describes the audio and main video streams received by the MCU from this participant.

The description typically includes the resolution, bitrate and codec used by the media stream. However, if a channel is muted, the description may be indicated in the Rx row, for example, as "muted remotely" (for H.323 endpoints) or <no video> (for SIP endpoints).

Content tx: <status>

This row (if present) shows one of two things: the characteristics of the content video channel being sent by the MCU to a participant, or the reason why no such stream is currently being transmitted. The status values that can be shown here are:

Content tx: pending: The MCU is able to send content video to the participant but is not currently doing so. This is normally because there is no active content channel video source for the conference. This status will also be shown for a participant which *is* the content channel video source and is also capable of receiving the currently active content video stream.

Content tx: disabled : Content is enabled for this conference, but this participant is not allowed to receive it. To enable content for this participant, configure the *Content video receive* setting for this participant's endpoint (refer to [Configuring H.323 endpoints](#)), or use the *enable* control for an active call.

Content tx: no common codecs: There is a per conference setting that determines which video codec is used by the MCU for outgoing transcoded content channels. The *Outgoing transcoded codec* parameter is on the conference configuration page (**Conferences** click on the conference to be configured, then click the **Configuration** tab and go to the **Content** section). This message means that the endpoint is able to receive content video, but not using the same codec as the MCU is configured to transmit.

Content tx: resolution mismatch, Content tx: bit rate mismatch: For each conference, the MCU uses a single video stream for all outgoing content connections to endpoints. This entails considering all endpoints' receive capabilities and deciding which resolution and bit rate to send in order to maximize the number of content channel viewers. These messages mean that the MCU has been unable to include this endpoint in the set of content viewers because of its limitations with regard to video resolution or bit rate. Note that it is possible to configure a lower limit on the bandwidth of the shared content video encoding which will cause a bit rate mismatch where an endpoint is only able to receive a low bit rate stream (refer to [Configuring content settings](#)).

Content tx: no common formats: This conference's configuration specifies that the content channel is transmitted in 16:9 resolutions only. However, this endpoint does not support 16:9 resolutions. To allow the MCU to select a content resolution that will accommodate the capabilities of all endpoints in the conference, change the *Transmitted content resolutions* setting in the conference's configuration to *Allow all resolutions*.

No *Content tx* status will be shown if the conference does not have content channel video enabled, or if the endpoint has no content capabilities.

You may change whether the MCU is prepared to send the conference content channel stream to an endpoint using content using the *enable* or *disable* control here. If sending of content video to an endpoint is currently not allowed, you will see the *enable* option, otherwise you will see the *disable* option.

For more information about using content, refer to [Content channel video support](#).

Content tx: <status> (continued):

Content tx: mode mismatch: The MCU supports only *presentation mode* for its content channels; specifically, H.239 *live mode* is not supported. This status message indicates that the endpoint is content-capable but does not support presentation mode.

Content tx: encryption not possible: The MCU is unable to send encrypted content video to this participant.

Content tx: unsupported packetization mode FURs ignored

The MCU has detected that the content link to this endpoint is experiencing problems, and has stopped sending video keyframes in response to Fast Update Requests (FURs) to avoid degrading the content video sent to other conference participants. The MCU will only enter this state if the **Video fast update request filtering** setting is *Enabled* (see [Configuring content settings](#)).

No *Content tx* status will be shown if the conference does not have content channel video enabled, or if the endpoint has no content capabilities.

You may change whether the MCU is prepared to send the conference content channel stream to an endpoint using content using the *enable* or *disable* control here. If sending of content video to an endpoint is currently not allowed, you will see the *enable* option, otherwise you will see the *disable* option.

For more information about using content, refer to [Content channel video support](#).

Content video source (main video), Content video source: The associated participant is currently supplying the conference's content channel video.

Content: unable to use main video as source: Use of this participant's main video source as the content (content channel) source has failed.

This is normally because there is already a source for the content channel; either another participant's main video channel which has been configured in the same way or a content video channel contributed by a connected endpoint.

Packet loss detected: This message appears if packet loss is detected between the MCU and the endpoint.

Click **View** to open the **Participant statistics** page and display details about the connection, for example the packet errors. See [Displaying statistics for a participant](#).

Conference chair: This endpoint has requested and been granted the chair.

For more information, refer to [H.243 floor and chair control](#).



Active floor: The endpoint has requested and been granted the floor and its media is being broadcast to all endpoints in the conference.

For more information, refer to [H.243 floor and chair control](#).

Inactive floor: This endpoint believes it has been granted the floor, but its media is not being shown to all endpoints in the conference.


This situation can occur when an endpoint requested the floor, was granted the floor, and was then moved to another conference where there was already an active floor participant.

For more information, refer to [H.243 floor and chair control](#).

	<p><i>Assigned floor:</i> This endpoint's media is being broadcast to all endpoints in the conference, although it did not request the floor itself.</p>	<p>This situation can occur if another endpoint, while chair, has issued H.243 commands to make that endpoint the floor.</p> <p>For more information, refer to H.243 floor and chair control.</p>
	<p><i>Some media channels encrypted :</i> Displayed if some media channels are not encrypted.</p>	
	<p><i>Cascade link to master, Cascade link from slave:</i> Indicates that this connection is a cascade link to or from another conference.</p>	
Preview	<p>Displays a sample still video capture of the participant.</p>	<p>Click the picture to update it.</p> <p>Note that conferences that are configured to require encryption do not show previews. Also note that previews can be disabled on the Settings > User interface page (refer to Customizing the user interface).</p>
	<p>Controls</p> <p>These controls are only available if the conference is configured with content enabled, and if the participant is contributing a main video channel.</p> <p> This control causes the MCU to attempt to use the participant's main video channel as the conference's content channel source. This will not be possible if the conference already has an active content channel source (either an endpoint's content video channel or another participant's main video activated via this control).</p> <p> This control causes the MCU to stop attempting to use the participant's main video channel as the conference's content channel source. It is necessary to use this control to switch to using a different endpoint's primary video channel or to enable content video contribution from endpoints.</p>	<p>See Content channel video support for additional information on H.239 and BFCP.</p>

All-participant controls


Although you may use the controls described above to manage one participant at a time, for example to mute that participant's audio, or to make them important, you may want to manage all participants at once. The **all-participant** controls permit you to do this. Note that you may continue to use the per-participant controls in conjunction with the all-participant controls. Refer to the table below for details of the controls available:

Field	Field description	Usage tips
Importance	 Makes all participants unimportant	If no participants are currently important, then this control will be unavailable.

Mute	<p> Mute audio from all participants (like mic. mute).</p> <p> Allow audio from all participants (like mic. unmute)</p> <p> Stop video from all participants (like camera mute).</p> <p> Allow video from all participants (like camera unmute).</p> <p> Prevent all participants from hearing the conference (like speaker mute).</p> <hr/> <p>Note: The endpoints may not always detect DTMF tones from the MCU after you mute the audio from the MCU.</p> <hr/> <p> Allow all participants to hear the conference (like speaker unmute).</p> <p> Prevent all participants from seeing the conference (like screen mute).</p> <p> Allow all participants to see the conference (like screen unmute).</p>	<p>Not all of the controls described here may be present in your participant list. You can configure which controls are shown by changing the Participant list controls on the Settings > User interface page (refer to Customizing the user interface).</p>
Disconnect	<p> Disconnects all participants from the conference.</p>	<p>If this conference was created ad hoc, then disconnecting all the participants will terminate the conference as well.</p>
View	<p> Selects <i>voice-switched</i> view for all participants (see Customizing a participant's layout view).</p> <p> Selects full screen view for all participants.</p> <p> Displays the layout selection panel from which you can select a layout view that all current participants will see. This panel offers the same choices as going to Conferences > Custom layout. (See Customizing layout views).</p>	<p>If all participants are watching the voice-switched view, then this control will be unavailable.</p>
Control	<p> Prevents participants from changing their own view layout from their endpoint.</p> <p> Allows participants to change their own view layout from their endpoint.</p>	<p>If no participants may control their own view layout, the <i>prevent</i> control will be unavailable. If all participants may control their own layout, the <i>allow</i> control will be unavailable.</p>

Previous participants

Refer to the table below to get details about the previous participant list. To delete this list, click **Clear previous participants record**.

Field	Field description	Usage tips
Type	Indicates whether the participant is an H.323 or SIP endpoint.	
Participant	Displays the name of the participant (endpoint).	
Controls	 Re-connects a participant to the conference.	<p>A previous participant can only be re-connected to a conference if their endpoint is a pre-configured endpoint.</p> <p>Note that if the original call to the conference was from the endpoint rather than the endpoint being invited by the MCU, then for the MCU to recognize it, that endpoint must be configured with Call-in match parameters. If the MCU did not recognize that the call was from a pre-configured endpoint then the re-connect control will not be available.</p> <p>For more information about configuring endpoints on the MCU refer to Configuring H.323 endpoints and Configuring SIP endpoints.</p>
Status	Displays the time at which a participant disconnected from the conference and who initiated the disconnect.	

Pre-configured participants

Refer to the table below to get details about pre-configured endpoints.

Field	Field description	Usage tips
Type	Indicates whether the participant is an H.323 or SIP endpoint.	
Name	Displays the name of the endpoint.	
Status	Displays the connection status of the pre-configured participant.	This field shows whether the participant is pending, connected, or disconnected, and the reason for failure if the participant has failed to connect to the conference.

Summary information



You may want to inform participants about conference details such as start time, and so on. Click the **Summary information** icon to display further details about a conference. This information may be copied to the clipboard for convenience.

Related topics



- [Adding participants](#)
- [Displaying statistics for a participant](#)









Customizing a participant's layout view

Every person viewing a conference sees a conference layout.

The layout divides the video screen into a collection of panes with participants' video streams displayed in those panes. You can customize the layout for an active participant as follows:

1. Go to **Conferences**.
2. Click a Conference name and then click on a participant's name.
3. Click the **Display** tab.

Field	Field description	Usage tips
Preview		
Video display	Displays static sample of video screen in the currently selected layout.	Click on the image to refresh the picture
Border	Adds a border thickness to display around the video image.	If the image is displaying off the edges of the participant's screen, add a border until the image displays properly.
Layout		
Family 1	Give prominence to one participant over the others.	The number of contributing conference participants determines the size of the large pane.
		
Family 2	Displays a single participant.	
		

Family 3 	<p>Displays the four most active participants without seeing them scaled down to a small size if there are lots of other participants.</p>	<p>Used when there are five or more video participants.</p>
Family 4    	<p>Gives equal prominence to up to 20 conference contributors, and is useful for a "roll call" of active participants.</p>	<p>The MCU automatically changes the layout to the 3 x 3 arrangement, and will continue to use this layout for up to 9 participants. With 10 or more participants, the 4 x 4 view is used, and with 17 or more participants the 5 x 4 view will be used. The MCU will then continue to use this layout even if there are more than 20 participants.</p>
Family 5 	<p>Gives prominence to two participants in the center of the view while showing smaller versions of other participants' video streams above and below.</p>	<p>This view is useful for observing a dialog between two participants or for viewing slides and a presenter.</p>
Conference custom layout	<p>Click Edit to choose or create a custom layout to be used by any participant.</p>	<p>See Customizing layout views.</p>
Participant custom layout	<p>Click Edit to choose a pre-configured custom layout for this participant.</p>	<p>See Selecting a custom participant layout.</p>
Controls		
	<p>These buttons control whether this participant is permitted to change the layout they see on the endpoint.</p>	
	<p>These buttons control whether the MCU alters the aspect ratio of the layout sent to the active participant. If the controls are available, you can force the MCU to compose the layout in a 4:3 aspect ratio (Send "normal" format video) or in a 16:9 aspect ratio (Send "widescreen" format video).</p>	<p>The available options for the resolution of transmitted video are controlled by the Transmitted video resolutions setting which can be configured for the whole MCU on the Settings > Conferences page or per configured endpoint (refer to Configuring an H.323 endpoint and/or Configuring a SIP endpoint).</p> <p>The widescreen setting on the active participant's display tab takes precedence over the preconfigured widescreen setting for the endpoint, which in turn takes precedence over the MCU-wide setting.</p>



These buttons control whether the active participant is allowed to contribute content to the conference.

Content contribution can also be defined in the conference template, the conference, or the endpoint's configuration. The setting on the active participant's display tab takes precedence over the endpoint configuration, which in turn takes precedence over the conference configuration. For more information, see [Content per-participant parameters](#).



These buttons control whether the video sent to the participant is stopped. If the video is stopped, the participant will not see the conference layout, but will still be able to hear the conference and can still contribute audio, video, and content to the conference.

Focused participant

Select which participant receives the focus on this participant's layout.

Depending on the types of participant in the conference (i.e. content channel, endpoint, audio-only participant), you can select from these options:

- *Voice-switched*: the loudest participant occupies the largest pane in the layout (the default setting)
- *Content channel*: the content channel occupies the largest pane in the layout
- *<participant name>*: you select a participant by name and then that participant occupies the largest pane in the layout

This setting will be overridden if a participant is identified as "important" on the Conference Participants List (see [Viewing the conference participants list](#)).

Related topics

- [Viewing conference participants list](#)
- [Understanding how participants display in layout views](#)
- [Customizing layout views](#)
- [Selecting a custom participant layout](#)
- [Using an auto attendant](#)

Controlling an active participant's camera

On the active participant's camera tab, you can preview the video from the camera, adjust its angle, zoom, and focus (if it has these features), and apply some other modifications to the incoming video stream.

1. Go to **Conferences**.
2. Click a Conference name and then click on a participant's name.
3. Click the **Camera** tab.

Camera preview





The page contains a small image from the video stream so you can preview what the conference should see from this endpoint. You can click the preview to update the image.

Camera controls

Field	Field description	Usage tips
Movement	Click the directional arrow buttons to change the view direction of the camera.	Some cameras are adjustable in all directions, others left and right only, and others up and down only. Many endpoints have fixed cameras, which will not respond to these controls.
Zoom	Click on the plus or minus buttons to adjust the zoom of the participant's camera.	Cameras that do not have zoom capability will not respond to these controls.
Focus	Click on the plus or minus buttons to adjust the camera's focus.	Cameras that do not have manual focus capability will not respond to these controls.

Video stream controls

These controls govern what the MCU does with the video stream coming from the active participant's camera, before composing it into the layout that it sends to all other participants.

Field	Field description	Usage tips
	Stop video from this participant (like camera mute).	The MCU does not use the participant's video when composing the layout that it sends to other participants.
	Allow video from this participant (like camera unmute).	The MCU will include the participant's video when composing the layout it sends to other participants.
 	Use these buttons to force widescreen aspect on the video from this participant, or to restore the aspect to the original as received.	
Video to use by default	<p>Allows you to replace a participant's video with that of another participant. <code><self></code> tells the MCU to display the participant's own video during conferences.</p> <p>If you select another preconfigured endpoint from the dropdown, the MCU will display the video stream from the selected endpoint in place of the participant's own video.</p>	<p>This feature can be useful in scenarios like translation, where you want to see the original speaker while you hear the translator. You do not need to alter any settings on the viewed participant, so in a translation scenario you would only change this setting on the translators' endpoints.</p> <p>This link is active whenever both participants are in the conference. The selected participant's video is always shown in place of the original participant's video; the original participant's video does not show in the conference, unless you explicitly show it using the pane placement feature.</p>

Related topics

- [Customizing a participant's layout display](#)
- [Managing participant's audio signals](#)
- [Selecting a custom participant layout](#)

- [Displaying statistics for a participant](#)
- [Sending messages to individual participants](#)
- [Using an auto attendant](#)

Viewing and adjusting a participant's audio levels

1. Go to **Conferences**.
2. Click a Conference name and then click on a participant's name.
3. Click the **Audio** tab.





Waveforms and statistics

- The **Participant audio** and **Conference audio** waveforms give a visual indicator of the current audio levels from the participant and from the conference. If the participant is the active speaker at the time when you click the audio tab, the waveforms should be similar. If a waveform is flat, it means the source is silent or muted.
- **AGC (Adaptive Gain Control)**: indicates the status of AGC for this endpoint. AGC can be set by the conference, or by the participant's configuration, or manually on this page. The manual setting for an active participant - on this page - always takes precedence over conference or participant configuration.
- **Current voice gain applied**: indicates how much amplification is applied to the voice signal at the time you access the page; the gain could have been applied manually or by AGC.
- **Audio energy (post gain stage)**: is the average of the whole audio signal, including manual or AGC gain, from this participant over time, compared with the maximum that the MCU can tolerate. The number is always negative as it is represented by a fraction of the maximum using a logarithmic scale. A mostly quiet signal will have larger negative numbers, while a very loud participant will be closer to 0.
- **Average voice level (pre gain stage)**: is an average of the audio signal's high points over time, measured against the maximum that the MCU can tolerate. The average voice level is useful when compared to the average background level; a large difference between the two means the voice is easily discernible from the background noise. If it is too close to the average background level, the audio may be improved by applying AGC or manual gain.
- **Average background level (pre gain stage)**: is an average of the signal's low points over time, measured against the maximum that the MCU can accept. It is always negative and a larger negative number means a lower background noise. If the average background level is too high, the conference may experience undesirable effects such as switching to this participant when the participant is not the active speaker.

Applying gain and muting audio

Use the controls described in the following table to adjust the active participant's audio levels, then click **Update** to apply your changes.

Field	Field description	Usage tips
-------	-------------------	------------

Gain control	<p>You can apply one of the following four gain control options by selecting the associated radio button:</p> <ul style="list-style-type: none"> ■ Use conference configuration: the participant inherits the conference's AGC setting. ■ Disable AGC: do not apply AGC to the audio from this participant. ■ Enable AGC: apply AGC to the audio from this participant. ■ Apply fixed gain: enter a dB value by which to adjust the participant's audio gain; a positive gain amplifies, and a negative gain attenuates, the participant audio. 1dB is approximately 60% change, 3dB is approximately 100% change and 5dB is approximately 300% change. For example, if the participant sounds twice as loud as everyone else, apply -3dB gain. 	<p>The selected gain control option is effective immediately, and persists until the participant leaves or the conference ends.</p> <p>If you need to set AGC in advance, you can do so on a per conference or per participant basis. You can apply AGC when inviting ad hoc participants or when preconfiguring endpoints.</p> <p>The gain control setting on this page - the active participant's audio page - takes precedence over any other gain control setting, whether that was preconfigured on the endpoint, the conference, or the template.</p>
Mute in-band DTMF	<p>This control determines whether the DTMF tones from this participant are audible to the conference. You can select one of the following:</p> <ul style="list-style-type: none"> ■ <i><use conference configuration></i>: DTMF from the active participant is either muted or audible to the conference, depending on the conference configuration. ■ <i>Disabled</i>: DTMF from this participant is audible to the MCU and is transmitted on to the other participants. ■ <i>Enabled</i>: DTMF from this participant is audible to the MCU but is not transmitted on to other participants. 	
	Prevents others from hearing this participant (like mic. mute).	
	Allows others to hear this participant (stop muting participant).	
	Prevents this participant from hearing the conference (like speaker mute).	
	<p>Note: The endpoint may not always detect DTMF tones from the MCU after you mute the audio from the MCU.</p>	
	Allows this participant to hear the conference (stop muting conference).	

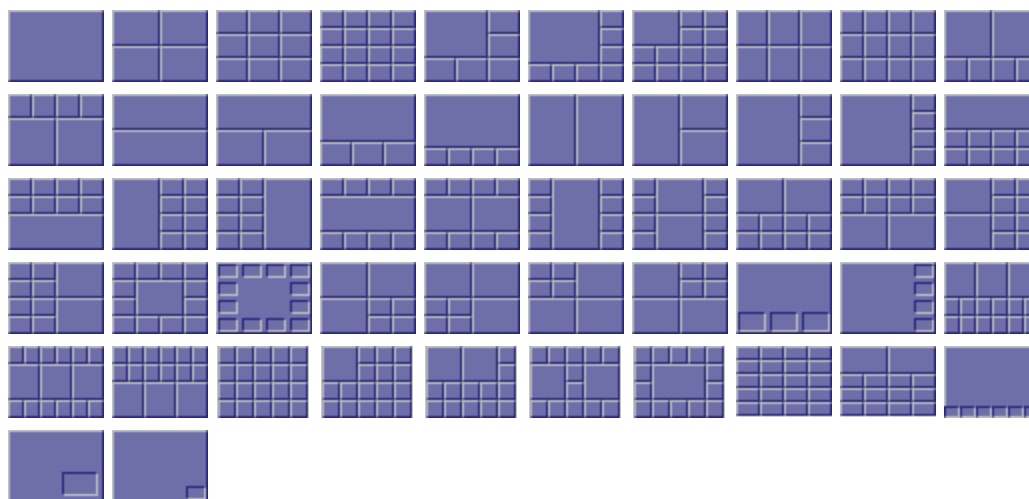
Selecting a custom participant view

You can add a custom layout to the choice of layouts available for this participant. You can customize this view by choosing this option:

1. Go to **Conferences**.
2. Click a Conference name and then click on a participant's name.
3. Click the **Custom layout** tab.

Field	Field description	Usage tips
Current status	Indicates whether a custom layout can be used for this participant.	When you click a new layout from the Available layouts , Enabled is automatically chosen with the most recent layout selected.
Available layouts	Displays all pre-configured layouts that are available to the participant. Click a layout to select it and make it available for the participant.	You can only select one custom layout per participant.

These layouts are designed to be suitable for all video conferencing situations:



These layouts are designed to be suitable for displaying composed views of standard (4:3) video streams on widescreen (16:9) displays:



Note that the layouts depicted with slightly darker shading for the 'picture in picture' participants indicate those layouts where the non-focused participants are slightly transparent and the focused participant can be seen 'through' the non-focused participants. These layouts are:



Related topics

- [Understanding how participants display in layout views](#)
- [Customizing layout views](#)
- [Customizing a participant's layout view](#)

Displaying statistics for a participant

You can view statistics about the video and audio streams between individual participants (endpoints) and the MCU by choosing this option:

1. Go to **Conferences**.
2. Click a Conference name and then click on a participant's name.
3. Click the **Statistics** tab.

If the participant is participating in the conference using audio only, the values for the video settings are not populated.

Media statistics


Media statistics provide detailed information about the actual voice and video streams (Realtime Transport Protocol (RTP) packets).


Note: MCU does not support ClearPath for the content channel.

Refer to the table below for additional information.

Field	Field description	Usage tips
Audio		
Receive stream	The audio codec in use, along with the current packet size (in milliseconds) if known.	If the MCU has received information that an endpoint has been muted at the far end, this will be indicated here.
Receive address	The IP address and port from which the media is originating.	
Encryption	Whether or not encryption is being used on the audio receive stream by this endpoint.	This field will only appear if the encryption feature key is present on the MCU.
Received jitter	The apparent variation in arrival time from that expected for the media packets (in milliseconds). The current jitter buffer also displays in parentheses.	You should expect to see small values for this setting. Consistently large numbers typically imply potential network problems. The jitter buffer shows the current playout delay added to the media to accommodate the packet arrival jitter. Large jitter values indicate a longer buffer.
Received energy	Represents the audio volume originating from the endpoint.	
Packets received	The number of audio packets destined for the MCU from this endpoint.	
Packet errors	The number of packet errors, including sequence errors, and packets of the wrong type.	You should expect to see small values for this setting. Consistently large numbers typically imply potential network problems.
Frame errors	Frame errors, as A/B where A is the number of frame errors, and B is the total number of frames received.	A frame is a unit of audio, the size of which is dependent on codec. You should expect to see small values for this setting. Consistently large numbers typically imply potential network problems.

Media information	If the time stamps or marker bits (or both) are detected to be unreliable in the incoming video stream, information will be displayed here.	This field is not displayed when there is no problem with the time stamps and marker bits. Where there is a problem the following text is displayed: "Media timestamps unreliable", "Media marker bits unreliable", or both if both conditions detected.
ClearPath FEC overhead	The overhead caused by sending FEC (forward error correction) packets.	
ClearPath FEC recovered	The number of packets recovered by the MCU through the use of FEC (forward error correction).	
Transmit stream	The audio codec being sent from the MCU to the endpoint, along with the chosen packet size in milliseconds.	
Transmit address	The IP address and port to which the media is being sent.	
Encryption	Whether or not encryption is being used on the audio transmit stream by this endpoint.	This field will only appear if the encryption key is present on the MCU.
Packets sent	A count of the number of packets that have been sent from the MCU to the endpoint.	
ClearPath FEC overhead	The overhead caused by sending FEC (forward error correction) packets.	
Video (primary channel and content shown separately)		
Receive stream	The codec in use and the size of the picture that the MCU is receiving from the specific participant. If the picture is a standard size (for example, CIF, QCIF, 4CIF, SIF) then this name is shown in parentheses afterwards.	
Receive address	The IP address and port (<IP address>:<port>) of the device from which video is being sent	
Encryption	Whether or not encryption is being used on the video receive stream from this endpoint.	This field will only appear if the encryption key is present on the MCU.
Channel bit rate	The negotiated bit rate available for the endpoint to send video in.	This value represents the maximum amount of video traffic that the remote endpoint will send to the MCU. It may send less data than this (if it does not need to use the full channel bit rate or the MCU has requested a lower rate), but it should not send more.

Receive bit rate	The bit rate (in bits per second) that the MCU has requested that the remote endpoint sends. The most-recently measured actual bit rate displays in parentheses.	<p>This value might be less than the Channel bit rate if:</p> <ul style="list-style-type: none"> ■ the MCU detects that the network path to the remote endpoint has insufficient capacity to maintain a higher traffic rate ■ that endpoint's video stream's position in the active conference compositions does not require it ■ it has been necessary to reduce the video bit rate because of the overall call bit rate; the audio bit rate plus the video bit rate should not exceed the call bit rate <p>For example, if all participants in the conference were watching a single participant at full screen, no other participants' video streams would be needed at all. So the MCU would request that those streams were sent at a low bit rate in order to avoid needless use of network bandwidth.</p> <p>If the receive bit rate has been limited to below the maximum channel bit rate, the reason for this limitation can be seen by moving over the  icon.</p>
Received jitter	Represents the variation in video packet at arrival time at the MCU.	
Delay applied for lipsync	The number of milliseconds by which the video follows the audio. Some endpoints send audio and video out-of-sync. The MCU ensures audio and video are played together.	
Packets received	The number of video packets destined for the MCU from this endpoint	
Packet errors	Video packet-level errors such as sequence discontinuities, incorrect RTP details, and so on. This is not the same as packets where the content (the actual video data) is somehow in error.	This value does not represent packets in which the actual video data in the packets is in error.
Frame rate	The frame rate of the video stream currently being received from the endpoint.	
Frame errors	The number of frames with errors versus the total number of video frames received.	
ClearPath FEC overhead	The number of packets recovered by the MCU through the use of FEC (forward error correction).	

ClearPath FEC recovered	The number of packets recovered through the use of FEC (forward error correction).	
ClearPath repair frames	The number of repair frames sent/received.	
Transmit stream	The codec, size and type of video being sent from the MCU to the endpoint.	
Transmit address	The IP address and port of the device to which the MCU is sending video.	
Encryption	Whether or not encryption is being used on the video transmit stream to this endpoint.	This field will only appear if the encryption key is present on the MCU.
Channel bit rate	The negotiated available bandwidth for the MCU to send video to the endpoint in.	
Transmit bit rate	The bit rate the MCU is attempting to send at this moment, which may be less than the channel bit rate which is an effective maximum. The actual bit rate, which is simply the measured rate of video data leaving the MCU, displays in parentheses.	<p>The Transmit bit rate value might be less than the Channel bit rate if :</p> <ul style="list-style-type: none"> ■ the remote endpoint receiving the video stream from the MCU has sent flow control commands to reduce the bit rate ■ it has been necessary to reduce the primary video bit rate to allow sufficient bandwidth for a content video stream <p>If the transmit bit rate has been limited to below the maximum channel bit rate, the reason for this limitation can be seen by moving over the  icon.</p>
Packets sent	The number of video packets sent from the MCU to this endpoint.	
Frame rate	The frame rate of the video stream currently being sent to the endpoint.	
Temporal/spatial	A number that represents the tradeoff between video quality and frame rate.	A smaller number implies that the MCU prioritizes sending quality video at the expense of a lower frame rate. A larger number implies that the MCU is prepared to send lower quality video at a higher frame rate.
ClearPath FEC overhead	The overhead caused by sending FEC (forward error correction) packets.	
ClearPath repair frames	The number of repair frames sent/received.	

Control statistics

Control statistics provide information about the control channels that are established in order that the endpoints can exchange information about the voice and video streams (Real Time Control Protocol (RTCP))

packets). Refer to the table below for additional information.

Field	Field description	Usage tips
Audio		
RTCP receive address	The IP address and port to which RTCP (Real Time Control Protocol) packets are being received for the audio and video streams	
Receiver reports	A count of the number of "receiver report" type RTCP packets seen by the MCU.	A single RTCP packet may contain more than one report of more than one type. These are generally sent by any device receiving RTP (Real Time Protocol) media from the network and are used for auditing bandwidth, errors, and so on by the MCU.
Packet loss reported	Media packet loss reported by receiver reports sent to the MCU by the far end.	
ClearPath FEC recovered	The number of packets reported by receiver reports as recovered by the endpoint through the use of FEC (forward error correction).	
Sender reports	A count of the number of "sender report" type RTCP packets received by the MCU.	These are typically sent by any device that is sending RTP media.
Other	A count of the number of reports seen by the MCU that are neither sender nor receiver reports.	
RTCP transmit address	The IP address and port to which the MCU is sending RTCP packets about this stream.	
Packets sent	The number of packets sent.	
Video (primary channel and content shown separately)		
RTCP receive address	The IP address and port to which RTCP (Real Time Control Protocol) packets are being sent for the audio and video streams.	
Receiver reports	A count of the number of "receiver report" type RTCP packets seen by the MCU.	A single RTCP packet may contain more than one report of more than one type. These are generally sent by any device receiving RTP (Real Time Protocol) media from the network and are used for auditing bandwidth, errors, and so on by the MCU.
Packet loss reported	Media packet loss reported by receiver reports sent to the MCU by the far end.	

ClearPath FEC recovered	The number of packets recovered through the use of FEC (forward error correction).	
Sender reports	A count of the number of "sender report" type RTCP packets received by the MCU.	These are typically sent by any device that is sending RTP media.
Other	A count of the number of reports seen by the MCU that are neither sender nor receiver reports.	
RTCP transmit address	The IP address and port to which the MCU is sending RTCP packets about this stream.	
Packets sent	The number of packets sent.	
Fast update requests	The number of fast update requests sent and received.	
Flow control messages	The number of flow control messages sent and received.	

Related topics

- [Displaying conference statistics](#)
- [Viewing the conference participant list](#)

Sending messages to individual participants

You can send a short text message to a specific participant currently in the conference. To do this:

1. Go to **Conferences**.
2. Click a Conference name and then click on a participant's name.
3. Click the **Send message** tab.

This message appears overlaid on the participant's view.

Field	Field description	Usage tips
Message text	Enter the message to send to this participant.	<p>Messages must be fewer than 256 characters, but depending on the viewing screen, messages at the higher-end of this limit might not display properly. So, consider limiting messages to about 180 characters. Messages longer than 256 characters will not be truncated; they will not display at all.</p> <p>You can disable this setting from Settings > Conferences (see Conference settings).</p>

Position	The vertical position of the message on the conference display.	Choose from the top, middle, or bottom of the conference display.
Duration	Indicates how long the message appears on the endpoint's video screen.	The default setting is 30 seconds. To remove a message before it times out, click Clear message .

Related topics

- [Sending messages to all participants](#)
- [Configuring global conference settings](#)

Sending DTMF to an audio bridge

If you are cascading a conference on the MCU to an audio conferencing bridge, you might want to send DTMF tones to that audio bridge for the purpose of entering a conference ID number and PIN. To access the DTMF keypad:

1. Go to **Conferences** and click on the conference name.
2. From the list of participants, click on the audio bridge's name.
3. Click the **Send DTMF** tab.

Pressing the keys on the DTMF keypad causes the MCU to generate the DTMF tones and send them in-band in the audio channel to the participant (in this case, the audio conferencing bridge). In this way, you can dial the audio conferencing bridge into a conference and then listen in to hear the instructions from the audio bridge. When the audio bridge requires DTMF entries, you can enter the required numbers by using the DTMF keypad.

Note that if you know exactly what the audio conferencing bridge is going to require when it is dialed into a conference, you can configure the bridge as an endpoint and set a DTMF sequence to be sent to that bridge. For more information about configuring endpoints refer to [Configuring H.323 endpoints](#) and/or [Configuring SIP endpoints](#).

Related topics

- [Configuring H.323 endpoints](#)
- [Configuring SIP endpoints](#)

Displaying diagnostics for a participant

You can view diagnostics for an individual participant's connection to the MCU by choosing this option:

1. Go to **Conferences**.
2. Click a conference name and then click on a participant's name.
3. Click the **Diagnostics** tab.

Participant diagnostics

This page shows various low-level details pertaining to the endpoint's communication with the MCU. You are not likely to need to use any of the information on this page except when troubleshooting specific issues under the guidance of Customer support.

Related topics

- [Viewing the conference participant list](#)

Moving a participant

You can move participants between conferences. Participants can be moved to any conference, but although participants can be moved from auto attendants they cannot be moved to them.

To move a participant:

1. Go to **Conferences > Move participants**.
2. Click and drag the name of the participant to the required destination conference.

Note that participants dragged and dropped into a conference on the web interface will be chairperson participants. (For more information about chairperson and guest participants, refer to [Adding and updating conferences](#).)

To move multiple participants:

1. Go to **Conferences > Move participants**.
2. Select the check boxes for every participant you want to move and drag them to the required destination conference.

To disconnect a participant from a conference:

1. Go to **Conferences > Move participants**.
2. Click and drag the name of the participant in to **Remove participant** area at the bottom of that page.

Note that dragging and dropping a participant in to the **Remove participant** area simply disconnects the participant from the conference. It does not remove them from a scheduled conference. That is, when the conference next runs that participant will be called if their endpoint is a pre-configured endpoint for that conference.

Related topics

- [Adding participants](#)
- [Understanding how participants display in layout views](#)
- [Customizing layout views](#)
- [Selecting a custom participant layout](#)
- [Using an auto attendant](#)

Creating auto attendants

The MCU allows you to configure auto attendants on it, which allows users to more easily join conferences.

- [Displaying the auto attendant list](#)
- [Adding and updating an auto attendant](#)
- [Adding a custom banner](#)

Displaying the auto attendant list

You can display an overview of the configured auto attendants on the MCU:

1. Go to **Conferences**.
2. Click the **Auto attendants** tab.

Field	Field description	Usage tips
Name	The name of the auto attendant	
Numeric ID	The number that you can dial to connect to the auto attendant	
H.323 gatekeeper	<p>The status of an auto attendant with respect to its gatekeeper registration. The possible states are:</p> <ul style="list-style-type: none"> ■ <i>n/a</i> This auto attendant is not configured to be registered with the gatekeeper; because of this, there is no applicable registration status to show. ■ <i>Registering</i> This auto attendant is in the process of registering with the gatekeeper. ■ <i>Deregistering</i> The auto attendant is in the process of unregistering with the gatekeeper. This might occur if: <ul style="list-style-type: none"> • Gatekeeper registration has been turned off (either for that auto attendant only or for the entire MCU) • The configured gatekeeper has just been changed and the MCU is in the process of unregistering from the previous gatekeeper before registering its auto attendants with the new one. ■ <i>Re-registration pending / Retry timeout</i> If the MCU fails to register an auto attendant with the gatekeeper, it enters these states temporarily before re-attempting the registration. ■ <i><number> registered</i> The auto attendant has been registered successfully with the gatekeeper and can be contacted using the number indicated. 	<p>For tips on configuring gatekeepers, see H.323 gatekeeper settings.</p>

SIP registrar	<p>The status of an auto attendant with respect to its SIP registration. The possible states are:</p> <ul style="list-style-type: none"> ■ <i>n/a</i> This auto attendant is not configured to be registered with the SIP registrar; because of this, there is no applicable registration status to show. ■ <i>Registering</i> This auto attendant is in the process of registering with the SIP registrar. ■ <i>Deregistering</i> The auto attendant is in the process of unregistering with the SIP registrar. This might occur if: <ul style="list-style-type: none"> • SIP registration has been turned off (either for that auto attendant only or for the entire MCU) • The configured SIP registrar has just been changed and the MCU is in the process of unregistering from the previous SIP registrar before registering its auto attendants with the new one. ■ <i>Re-registration pending / Retry timeout</i> If the MCU fails to register an auto attendant with the SIP registrar, it enters these states temporarily before re-attempting the registration. ■ <i><number> registered</i> The auto attendant has been registered successfully with the SIP registrar and can be contacted using the number indicated. 	For tips on configuring SIP, see SIP settings .
Security	Whether a PIN has been configured to restrict access to the auto attendant	
Calls	The total number of calls received by the auto attendant since the last restart	
Banner	A thumbnail of the custom banner, if one has been specified	

Related topics

- [Adding and updating an auto attendant](#)
- [Adding a custom banner](#)

Adding and updating an auto attendant

Auto attendants simplify the way participants can join conferences. By calling an auto attendant using their video endpoint, a participant can choose from menu options and join or start conferences. No gateway or gatekeeper is required. (The auto attendant is configured on the MCU.)

Adding an auto attendant

To add an auto attendant:

1. Go to **Conferences**.
2. Click the **Auto attendants** tab.
3. Click **Add new auto attendant**.

4. Refer to the table below for the most appropriate settings for the auto attendant.
5. After entering the settings, click **Add auto attendant**.

Updating an auto attendant

To update an existing auto attendant:

1. Go to **Conferences**.
2. Click the **Auto attendants** tab.
3. Click the name of an auto attendant.
4. Refer to the table below for the settings to change for this auto attendant.
5. After updating the settings, click **Update auto attendant**.

Field	Field description	Usage tips
Auto attendant		
Name	The name of the auto attendant.	
Title	An optional title to be shown at the top of the screen when an endpoint calls in to this auto attendant.	
Numeric ID	The number with which to register the auto attendant on the gatekeeper and/or SIP registrar.	See Configuring H.323 gatekeeper settings and SIP settings for details.
Numeric ID registration	Select <i>H.323 gatekeeper</i> if you want the Numeric ID to be registered with the H.323 gatekeeper; select <i>SIP registrar</i> if you want the Numeric ID registered with the SIP registrar.	Note that for SIP, you must configure the ID with the SIP registrar for the MCU to be able to register that ID.
PIN	Assigns a password to the auto attendant.	If you set a PIN, all participants using the auto attendant will be required to enter this password.
Re-enter PIN	Verifies the password.	
Creation of new conferences	If Enabled, displays the <i>Create new conference</i> option on the auto attendant so that the participant can create new ad hoc conferences using the auto attendant.	If disabled, participants will not be able to create new conferences from the auto attendant. Note that this option will not be available if you have enabled Media port reservation on the Settings > Conferences page. When using port reservation mode, there can be no ad hoc conferences. For more information about port reservation, refer to Reservation of MCU media ports .

Access to ad hoc conferences	If Enabled, displays ad hoc conferences as well as scheduled conferences as options on the auto attendant.	If disabled, participants can only view scheduled conferences; ad hoc conferences will not be shown. Note that this option will not be available if you have enabled Media port reservation on the Settings > Conferences page. When using port reservation mode, there can be no ad hoc conferences. For more information about port reservation, refer to Reservation of MCU media ports .
-------------------------------------	--	--

Visible scheduled conferences

All scheduled conferences	Enables all auto attendant participants to join any conferences scheduled to start while they are using the auto attendant.	If you select All scheduled conferences , this does not include conferences configured as private.
Selected scheduled conferences	Choose the conferences to list on the auto attendant by selecting check boxes.	Note that even conferences that have been configured as private conferences will appear on this list. So as the admin user, you can enable private conferences to appear on an auto attendant. If you leave the conference unselected, it will not appear on the auto attendant.

Links to other auto attendants

Select the name of any other configured auto attendant that you want to be accessible from the auto attendant that you are adding.

Related topics

- [Displaying the auto attendant list](#)
- [Adding a custom banner](#)

Adding a custom auto attendant banner

You can add a custom banner image to any auto attendant configured on the MCU as follows:

1. Go to **Conferences**.
2. Click the **Auto attendants** tab.
3. Click the name of a configured auto attendant.
4. Click the **Banner** tab.
5. Refer to the table below to determine the most appropriate settings.

Field	Field description	Usage tips
Auto attendant banner		
Default	Chooses the default MCU graphic to use for your banner.	

Specific to this auto attendant	The custom banner identified for this auto attendant. Click Remove banner to remove this graphic as the banner. Click Update after uploading a new graphic.	Nothing displays here until you upload the custom graphic as described below.
--	---	---

Banner upload

Banner for this auto attendant	The custom graphic to be used for a banner. Click Browse to locate the file on your hard drive.	The image file can be a JPEG, GIF or Windows BMP format with a maximum size of 1600 x 1200 pixels. If the file is smaller than this size, the MCU will scale it to fill the banner area previously occupied by the Cisco logo. Click Upload new file to display.
---------------------------------------	--	---

Note: There is a 90KB file size restriction on all platforms.

Related topics

- [Viewing the auto attendant list](#)
- [Adding and updating an auto attendant](#)

Managing endpoints

Displaying the endpoint list	103
Configuring H.323 endpoints	104
Configuring SIP endpoints	114

Displaying the endpoint list

To display the Endpoint List, go to **Endpoints**.

The Endpoint List displays all endpoints that have been configured within the MCU.

To add a new H.323 endpoint, select **Add H.323**.

To add a new SIP endpoint, select **Add SIP**.

To delete configured endpoints, check the ones you want to delete and select **Delete selected**.

Field	Field description
Name	The name of the endpoint.
Address	The IP address, host name, H.323 ID, E.164 number, or SIP URI of the endpoint.
Type	Whether it is an H.323 or SIP endpoint.

Related topics

- [Configuring H.323 endpoints](#)
- [Configuring SIP endpoints](#)

Configuring H.323 endpoints

You can configure H.323 endpoints to work with the MCU by choosing **Endpoints > Add H.323**. This makes it easier to add endpoints to conferences because you can select names from a list rather than adding network addresses.

A Cisco TelePresence IP VCR can be configured as an H.323 endpoint and added as a participant in a conference. If the IP VCR is configured to do so, it will start recording as soon as the conference starts. You can also configure a folder's Recording ID as an endpoint and in this way, when a conference starts, the IP VCR can start recording directly into a specific folder. For more information about using the IP VCR in this way, refer to the IP VCR's online help.

Recordings on an IP VCR can be configured as H.323 endpoints. In this way, an audio-only participant can contribute an IP VCR recording as his video stream (using the associated endpoint function, see [Adding and updating users](#)). This function is also useful where you have a recording that you might like to view within a conference.

Refer to the table below for tips on adding an H.323 endpoint to the MCU. After entering the settings, click **Add endpoint**.

Display parameters

Field	Field description	Usage tips
Name	The name of the endpoint.	

Call-out parameters

Field	Field description	Usage tips
Address	The IP address, host name, or an E.164 address (phone number).	

Redial behavior	<p>Defines whether and how the MCU will redial this endpoint if the connection fails:</p> <ul style="list-style-type: none">■ <i><use box-wide setting></i> This preconfigured participant inherits the redial behavior setting that the MCU uses by default for all preconfigured participants. This option is not available when you are configuring ad hoc participants.■ <i>Never redial</i> The MCU never attempts to redial a failed connection to this participant.■ <i>Redial until connected</i> The MCU redials this participant if it fails unexpectedly when first establishing a connection; the MCU never retries the connection if it fails after being established.■ <i>Redial on unexpected disconnection</i> The MCU redials this participant on any unexpected disconnection, whether it occurs while first being established or at any point thereafter. It does not attempt to redial if the participant deliberately ends the connection. <hr/> <p>Note: A deliberate disconnection, if it is not correctly signaled by the endpoint, may be interpreted as unexpected. If you experience this, reduce the call persistence behavior for the affected endpoint.</p> <hr/> <ul style="list-style-type: none">■ <i>Redial on any disconnection</i> The MCU redials this preconfigured participant when the connection closes, irrespective of whether the call fails or is deliberately ended by the participant.	<p>This setting defines redial behavior for an individual participant, which overrides the box-wide setting.</p>
------------------------	---	--

Redial limit	<p>Enables or disables the redial limit for this endpoint, and overrides the corresponding box-wide setting.</p>	<p>The redial limit allows the MCU to stop trying to reconnect a failed call. When the limit is enabled, the MCU will attempt to reconnect up to ten times: once immediately after the connection failure; four times at one minute intervals thereafter, and once every five minutes for a further five attempts.</p> <p>When the redial limit is disabled, the MCU continues retrying - once every five minutes - after those first ten attempts. It will do this until the connection is made. If the connection is never made, the MCU continues retrying until either the conference or the participant is destroyed.</p> <p>The redial pattern has an initial delay when the redial behavior is set to <i>Redial on any disconnection</i>. With that setting, the MCU does not immediately redial after a deliberate disconnection - it waits 30 seconds.</p>
DTMF sequence	<p>The DTMF sequence to send to an endpoint after it answers the call.</p> <p>The sequence may be up to 127 characters long and may include digits 0-9 and the following characters: * (star), # (pound/hash), and , (comma). The comma represents a two second pause.</p> <p>There is always a two second pause after the call connects, after which the MCU will send the DTMF tones at a rate of two per second. You can insert as many two second pauses as you need by inserting commas into the DTMF sequence. Leading and trailing commas are supported.</p>	<p>This sequence enables the MCU to navigate through an audio menu. This is useful where a conference on the MCU dials out to an audio-only conference on an audio bridge.</p> <p>You can configure the audio bridge as a pre-configured endpoint (either H.323 or SIP) and specify the DTMF sequence which will then be used whenever the bridge is added to any conference. Alternatively, you can add the audio bridge as an ad hoc participant to an individual conference.</p> <p>For example, assume you want the MCU to dial out to a PIN-protected audio conference on an audio bridge. The conference ID is 555 and the PIN is 888. The audio bridge requires that you press # after entering the ID and after entering the PIN. In this example the DTMF sequence could be: 555#,,888#. The two commas represent a four second pause which allows the audio bridge's automated menu system time to process the ID and request the PIN.</p>
Suppress audio during DTMF	<p>Suppresses the audio stream while initial DTMF connection sequence is being sent, so that other conference participants do not hear the audio of this participant or interactive voice responders reacting to the tones.</p> <p><i>Outgoing only</i> suppresses the audio to the endpoint while DTMF tones are sent to the endpoint.</p> <p><i>All</i> also suppresses both incoming and outgoing audio for the participant while the initial DTMF sequence is being sent to the endpoint.</p>	<p>This setting is independent of other audio muting mechanisms. Audio suppression is active for the duration of the DTMF tone sequence, including any deliberate pauses (commas in the DTMF sequence).</p>

Call-in match parameters

Field	Field description	Usage tips
-------	-------------------	------------

Name	This must be the name that the endpoint sends to the MCU	The endpoint is recognized if all filled-in fields in this section are matched. Fields left blank are not considered in the match.
IP address	The IP address of the endpoint	When you configure Call-in match parameters , an endpoint will be recognized as <i>this</i> pre-configured endpoint and the Conferencing parameters will be applied to a call from this endpoint.
E.164	The E.164 number with which the endpoint is registered with the gatekeeper	Note: call-in matching is not supported for the H.323 ID.

Conferencing parameters

Display name override	The name that is displayed in a conference as a label on the video from this endpoint. It is also the name of the endpoint as it appears on the MCU's web interface.	<p>The display name override is used in place of any identifier that appears on the endpoint's video or in the MCU's web interface. The endpoint could otherwise be identified by its H.323 id, its E.164 number, or its IP address.</p> <p>If you use only non-printing characters, such as spaces, as a display name override, the MCU respects this 'blank' name as a label for video from this endpoint. In this case, the MCU does not show the non-printing override value when listing the endpoint in the web interface; it shows one of the endpoint's other identifiers instead.</p> <p>Note that once an endpoint has connected, you cannot change the display name via the web interface.</p>
Motion / sharpness trade off	<p>Choose whether to use the MCU-wide setting for motion/sharpness trade off, or configure an individual setting for this endpoint. Select from:</p> <ul style="list-style-type: none"> ■ <i>Use box-wide setting:</i> this is the default value. In this case, the endpoint will use the motion/sharpness tradeoff setting from the Settings > Conferences page ■ <i>Favor motion:</i> the MCU favors motion over sharpness; that is, it will try and use a high frame rate at the cost of lower resolution. The MCU will choose a resolution that allows for a framerate of 25 frames per second or higher. ■ <i>Favor sharpness:</i> the MCU favors sharpness over motion; it will use the highest resolution that is being sent in (by any endpoint), and adjust downwards, to their highest advertised resolution, for other endpoints if necessary. ■ <i>Balanced:</i> the MCU will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second) 	<p>The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the endpoint and the MCU. This setting controls how the MCU will negotiate the settings to be used with this endpoint.</p>

Transmitted video resolutions	<p>Choose the setting for transmitted video resolutions from the MCU to this endpoint. This setting overrides the MCU-wide setting on the Settings > Conferences page.</p>	<p>Retain the default setting (<i>use box-wide setting</i>) unless you are experiencing problems with the display of certain resolutions by this endpoint.</p> <p>Endpoints advertise the resolutions that they are able to display. The MCU then chooses from those advertised resolutions, the resolution that it will use to transmit video. However, some endpoints do not display widescreen resolutions optimally. Therefore, you might want to use this setting to restrict the resolutions available to the MCU for transmissions to this endpoint.</p>
Content contribution	<p>Whether this endpoint is permitted to contribute the conference content channel. Select from:</p> <p><i><use conference default></i>: this endpoint will use the Content contribution from endpoints setting from the per-conference configuration.</p> <p><i>Enabled</i>: This endpoint is allowed to contribute the content channel, even if content contribution from endpoints is disabled in the per-conference configuration.</p> <p><i>Disabled</i>: This endpoint is not allowed to contribute the conference channel, even if content contribution from endpoints is enabled in the per-conference configuration.</p>	<p>This setting is provided to allow you to individually configure whether or not an endpoint is allowed to contribute content to a conference.</p> <p>To use the content channel, the Content status must be enabled at the MCU-wide level (on the Settings > Content page) and, for any given conference, Content mode must not be <i>Disabled</i> in the conference settings.</p>
Content receive	<p>Whether this endpoint is allowed to receive a separate content stream when in a conference.</p>	<p>This setting is provided to allow you to individually configure whether or not an endpoint is allowed to receive content from a conference.</p> <p>To use the content channel, the Content status must be enabled at the MCU-wide level (on the Settings > Content page) and for any given conference Content channel video must also be enabled in the per-conference configuration.</p>
View border size	<p>Select a border size for video transmitted to this endpoint.</p>	<p>This sets a border thickness to display around the video image. This is useful where the image is displaying off the edges of the participant's screen; use a border to force the image to display properly.</p> <p>Applying a border size here means that this border size will always be used for this endpoint's transmitted video. Note that you can also apply a border to a participant in a conference by going to Conferences and clicking on the name of the conference and then altering this participant's settings.</p>
Default view family	<p>Sets the layout family to be used when calling out to this endpoint.</p>	<p>If this is set to <i>Use box-wide setting</i> then the default view family that has been configured via the Conference settings page will be used.</p>

Preferred bandwidth from MCU	Identifies the network capacity (measured in bits per second) used by the media channels established by the MCU to a single participant.	These settings take priority over the Default bandwidth from MCU setting configured in the global conference settings.
Preferred bandwidth to MCU	The maximum combined media bandwidth advertised by the MCU to endpoints.	These settings take priority over the Default bandwidth to MCU setting configured in the global Conference settings (see Conference settings).
Layout control via FECC / DTMF	<p>Whether this endpoint is able to change their view layout via far-end camera control (FECC) or DTMF tones. Choose from:</p> <ul style="list-style-type: none"> ■ <i>use conference configuration</i>: the setting for Layout control via FECC / DTMF will be determined by the configuration of the conference ■ <i>Disabled</i>: the participant using this endpoint will not be allowed to change their view layout using either FECC or DTMF. This option also prevents the user from changing layout with the in call menu. ■ <i>FECC only</i>: the participant using this endpoint will be allowed to change their view layout using FECC ■ <i>DTMF only</i>: the participant using this endpoint will be allowed to change their view layout using DTMF ■ <i>FECC with DTMF fallback</i>: the participant using this endpoint will be allowed to change their view layout using FECC. If FECC is not available, this participant will be able to use DTMF ■ <i>FECC and DTMF</i>: the participant using this endpoint will be allowed to change their view layout using either FECC or DTMF, rather than only using DTMF as a fallback. 	<p>This setting takes precedence over the per-conference layout control setting for conferences into which the endpoint is invited.</p> <p>This layout control setting does not govern layout control using the in call menu. The setting governs layout control using the endpoint's DTMF or FECC controls while the user is <i>not</i> using the menu.</p>

Send camera control to other participants	<p>Specifies whether FECC or DTMF from this participant may control a far end camera. This setting combines with layout control via FECC/DTMF to control the camera of the far end and the layouts of the conference. This setting overrides the global conference setting for this endpoint.</p> <ul style="list-style-type: none"> ■ <i>Disabled</i>: This participant will not be allowed to control a far end camera using either FECC or DTMF. ■ <i>FECC only</i>: This participant will be only be allowed to control a far end camera using FECC. ■ <i>DTMF only</i>: This participant will be only be allowed to control a far end camera using DTMF. ■ <i>FECC with DTMF fallback</i>: This participant will be allowed to control a far end camera using FECC. If FECC is not available, this participant will be able to use DTMF for camera control. ■ <i>FECC and DTMF</i>: This participant will be allowed to control a far end camera using either FECC or DTMF. 	<p>There are two control mechanisms, FECC and DTMF, either (or both) of which can be used for camera control or layout control. If one mechanism is allowed for camera control but not for layout control, then that mechanism only controls the far end camera and does not affect the layout. Similarly, if one mechanism is allowed for layout control but not for camera control, then it is not possible to control the camera with that mechanism. In these cases, the endpoint can use FECC or DTMF controls directly to change the layout or adjust the far end camera.</p> <p>When one control mechanism can control either the layout or the far end camera, then that mechanism will always control the layout until "Zoom in" (FECC mechanism) or 1 (DTMF mechanism) is pressed. The control mechanism then switches over to control the camera.</p> <p>Far-end camera control always applies to the camera of the participant shown in the largest or top left pane (when panes are the same size). If you have no way to control the layout, then you cannot focus on a participant to allow you to adjust a particular camera.</p>
Mute in-band DTMF	<p>Use this option to mute in-band DTMF from this endpoint. Choose from:</p> <ul style="list-style-type: none"> ■ <i>use conference configuration</i>: the setting for Mute in-band DTMF will be determined by the configuration of the conference ■ <i>Never</i>: the in-band DTMF from this endpoint will never be muted. Any DTMF tones sent from this endpoint will be audible to conference participants ■ <i>Always</i>: the in-band DTMF from this endpoint will always be muted. Any DTMF tones sent from this endpoint will not be audible to conference participants ■ <i>When used for MCU control</i>: if a participant is using in-band DTMF to control conference layout and for other in-conference features, the tones will be muted and will not be audible to conference participants. The MCU will only expect a participant to use DTMF for MCU control if Layout control via FECC / DTMF or Send camera control to participants is set to <i>DTMF only</i>, <i>FECC and DTMF</i>, or <i>FECC with DTMF fallback</i> and FECC has not been established, or if the participant is able to use the in call menu. 	<p>In some scenarios, where a conference is cascaded onto an audio bridge, it might be useful for one of the participants in that conference to be able to send in-band DTMF to the MCU. This is for the purposes of sending the conference ID or PIN to the audio conferencing bridge. In this case, the Mute in-band DTMF setting for the endpoint of that participant needs to be <i>Never</i>. However, you can instead send DTMF tones to the audio conferencing bridge directly from the MCU; for more information refer to Sending DTMF to an audio bridge.</p> <p>Unless you need to configure a particular setting for this endpoint, set this to <i>use conference configuration</i> and ensure you have the Mute in-band DTMF setting as required in the conference configuration (see Adding and updating conferences).</p> <p>This setting takes precedence over the per-conference Mute in-band DTMF setting for conferences into which the endpoint is invited.</p>

Appear as a recording device	When this setting is enabled, the red recording indicator dot is visible to other conference participants.	This participant is labeled as a recorder on the conference participants page.
Video to use by default	<p>Allows you to replace this participant's video with that of another participant. Select <i><self></i> (default value) to display this participant's own video by default.</p> <p>If you select another preconfigured endpoint from the dropdown, the MCU will no longer use this participant's own video by default: instead, it will use the video stream from the selected endpoint in most circumstances, for example when this participant becomes the active speaker.</p>	<p>If the selected Video to use by default is not available, the MCU will use this participant's own video if possible.</p> <p>If the selected Video to use by default is available, you can still show this participant's own video if you need to by explicitly choosing it in specific layout pane selections.</p>
Dial out as	Determines whether this participant is a chair or a guest when in automatic lecture mode.	
Initial audio to MCU	Select <i>Active</i> or <i>Muted</i> to define whether audio from this endpoint should be muted whenever it first joins a conference.	<p>If this is <i>Muted</i>, then the MCU will mute the stream whenever it successfully invites the endpoint or recognizes the endpoint when it calls in.</p> <p>Audio from preconfigured endpoints can also be muted by the conference's Mute on join configuration, but only when they call in. In that case, if either the conference's Mute on join checkbox for Audio is checked, or the endpoint's Initial audio to MCU is <i>Muted</i> (or both) then the audio from the endpoint is muted when it joins the conference.</p>
Initial video to MCU	Select <i>Active</i> or <i>Stopped</i> to define whether video from this endpoint should be stopped whenever it first joins a conference.	<p>If this is <i>Stopped</i>, then the MCU will stop the stream whenever it successfully invites the endpoint or recognizes the endpoint when it calls in.</p> <p>Video from preconfigured endpoints can also be muted by the conference's Mute on join configuration, but only when they call in. In that case, if either the conference's Mute on join checkbox for Video is checked, or the endpoint's Initial video to MCU is <i>Muted</i> (or both) then the video from the endpoint is stopped when it joins the conference.</p>
Initial audio from MCU	<p>Select <i>Active</i> or <i>Muted</i> to define whether audio to this endpoint is muted whenever it first joins a conference.</p> <hr/> <p>Note: The endpoint may not always detect DTMF tones from the MCU after you mute the audio from the MCU.</p>	

Initial video from MCU	Select <i>Active</i> or <i>Stopped</i> to define whether video to this endpoint is stopped whenever it first joins a conference.	
Initial Adaptive Gain Control	Defines whether or not the endpoint uses Adaptive Gain Control (AGC) when it first joins the conference. Select <i><use conference configuration></i> to inherit the setting from the conference. Otherwise, you can select <i>Enabled</i> or <i>Disabled</i> to override the conference-wide AGC setting.	Any manual changes to the participant volume will turn AGC off for that participant. You can also manually enable or disable AGC for a participant that is already in the conference, on the Conference > Participants > <Name> > Audio page.
Automatic disconnection	When a participant disconnects from a conference and only endpoints set to Automatic disconnection are left, all those participants are disconnected.	Set to enabled if you want this endpoint to be automatically disconnected from conferences when only endpoints set to Automatic disconnection remain in a conference when any other participant has disconnected. Note that this setting is useful where you have configured an IP VCR as an endpoint so that the IP VCR can be automatically called into a conference to record the session. In this case, the IP VCR will stop recording when the conference ends (that is, when everyone has left the conference). For more information about using the IP VCR in this way, refer to the IP VCR online help.

Advanced interoperability parameters

Field	Field description	Usage tips
-------	-------------------	------------

Content negotiation	<p>This field allows the MCU to be configured so that content can be exchanged with third party MCUs in multi-level cascaded conferences over H.323. Choose from:</p> <ul style="list-style-type: none"> ■ <i>As master</i>: The MCU only acts as master in H.239 token negotiation. ■ <i>As slave</i>: The MCU acts as the slave in H.239 token negotiation and can send content to a master unit if it accepts the token request. ■ <i>Mimic slave</i>: The MCU mimics a slave during H.239 token negotiation, but does not actually act as a slave. The MCU still tries to send content to all other endpoints/units even if the third party MCU rejects the token request. 	<p>When exchanging content with an endpoint in a H.323 call, the MCU acts as a master unit and the endpoint as a slave unit for the purpose of H.239 token negotiation. However, in order for the MCU to exchange content with a cascaded third party MCU, the MCU must appear to the third party MCU to be a slave unit. The MCU can be configured as a true slave, in which case content will only be sent if the third party MCU master accepts the token request, or to mimic a slave (content is sent to all other connected endpoints even if the third party MCU rejects the token request).</p> <hr/> <p>Note: MCU to MCU SIP cascading is not supported. When doing SIP to SIP cascading, the MCU's BFCP negotiation fails and the content appears in the main video instead of a separate channel.</p> <hr/>
Custom codec selection	<p>Can be used to ensure only specific codecs are permitted on calls to (and received from) this endpoint.</p>	<p>If <i>Enabled</i>, you can select which codecs are allowed to be used when communicating with this endpoint. This setting overrides the MCU-wide codec selection on the Settings > Conference page.</p>

Related topics

- [Displaying the endpoint list](#)
- [Configuring SIP endpoints](#)

Configuring SIP endpoints

To configure the SIP endpoints to work with the MCU, go to **Endpoints > Add SIP**. This makes it easier to add endpoints to conferences because you can choose names from a list rather than adding network addresses.

Refer to the table below for tips on adding a SIP endpoint to the MCU. After entering the settings, click **Add endpoint**.

Field	Field description	Usage tips
Name	The name of the endpoint.	
Address	The IP address, host name, directory number, or SIP URI (in the format 1234@cisco.com).	The address of the SIP endpoint can be a directory number if you are using a SIP registrar. Note that square brackets are mandatory for IPv6 addresses.
Use SIP registrar	Allows calls to this endpoint to use a directory number (in the Address field) and the SIP registrar.	<p>This setting is dependent on the MCU-wide SIP registrar usage setting. If the MCU-wide setting is disabled, then the endpoint will not use the SIP registrar (irrespective of whether you check this box). If SIP registrar usage is enabled on the Settings > SIP page, then checking this box allows the endpoint to use the registrar.</p> <p>Only applicable if Outbound call configuration is set to <i>Use registrar</i>. If Use SIP registrar is checked, the dialed URI gets appended with Outbound domain if present, otherwise Outbound address gets appended. If Use SIP registrar is unchecked, then nothing is appended to the dialed URI. The Use SIP registrar check box has no effect if Outbound call configuration is set to <i>Call direct</i> or <i>Use trunk</i>.</p>

Outgoing transport	<p>Select the protocol to be used for call control messages for outgoing call connections to this endpoint.</p>	<p>If you want this endpoint to use the MCU-wide outgoing transport setting, select <i><use box-wide setting></i>. If this endpoint uses TCP, select TCP as the outgoing transport. If this endpoint uses UDP, select UDP as the outgoing transport. If this endpoint uses TLS, select TLS. Note that if you want the MCU to use TLS for call setup, you must have the encryption feature key and the TLS service must be enabled on the Network > Services page.</p> <p>Using TLS for call setup is not sufficient for the call to be considered encrypted such that it can participate in a conference which requires encryption. Where encryption is required in the conference configuration, a SIP call must use SRTP. For more information about SIP encryption, refer to Configuring encryption settings.</p> <p>This setting overrides the MCU-wide setting for Outgoing transport on the Settings > SIP page. For more information about configuring SIP, refer to Configuring SIP settings.</p>
---------------------------	---	--

Redial behavior	<p>Defines whether and how the MCU will redial this endpoint if the connection fails:</p> <ul style="list-style-type: none">■ <i><use box-wide setting></i> This preconfigured participant inherits the redial behavior setting that the MCU uses by default for all preconfigured participants. This option is not available when you are configuring ad hoc participants.■ <i>Never redial</i> The MCU never attempts to redial a failed connection to this participant.■ <i>Redial until connected</i> The MCU redials this participant if it fails unexpectedly when first establishing a connection; the MCU never retries the connection if it fails after being established.■ <i>Redial on unexpected disconnection</i> The MCU redials this participant on any unexpected disconnection, whether it occurs while first being established or at any point thereafter. It does not attempt to redial if the participant deliberately ends the connection. <hr/> <p>Note: A deliberate disconnection, if it is not correctly signaled by the endpoint, may be interpreted as unexpected. If you experience this, reduce the call persistence behavior for the affected endpoint.</p> <hr/> ■ <i>Redial on any disconnection</i> The MCU redials this participant when the connection closes, irrespective of whether the call fails or is deliberately ended by the participant.	<p>This setting defines redial behavior for an individual participant, which overrides the box-wide setting.</p>
------------------------	--	--

Redial limit	Enables or disables the redial limit for this endpoint, and overrides the corresponding box-wide setting.	<p>The redial limit allows the MCU to stop trying to reconnect a failed call. When the limit is enabled, the MCU will attempt to reconnect up to ten times: once immediately after the connection failure; four times at one minute intervals thereafter, and once every five minutes for a further five attempts.</p> <p>When the redial limit is disabled, the MCU continues retrying - once every five minutes - after those first ten attempts. It will do this until the connection is made. If the connection is never made, the MCU continues retrying until either the conference or the participant is destroyed.</p> <p>The redial pattern has an initial delay when the redial behavior is set to <i>Redial on any disconnection</i>. With that setting, the MCU does not immediately redial after a deliberate disconnection - it waits 30 seconds.</p>
DTMF sequence	<p>The DTMF sequence to send to an endpoint after it answers the call.</p> <p>The sequence may be up to 127 characters long and may include digits 0-9 and the following characters: * (star), # (pound/hash), and , (comma). The comma represents a two second pause.</p> <p>There is always a two second pause after the call connects, after which the MCU will send the DTMF tones at a rate of two per second. You can insert as many two second pauses as you need by inserting commas into the DTMF sequence. Leading and trailing commas are supported.</p>	<p>This sequence enables the MCU to navigate through an audio menu. This is useful where a conference on the MCU dials out to an audio-only conference on an audio bridge.</p> <p>You can configure the audio bridge as a pre-configured endpoint (either H.323 or SIP) and specify the DTMF sequence which will then be used whenever the bridge is added to any conference. Alternatively, you can add the audio bridge as an ad hoc participant to an individual conference.</p> <p>For example, assume you want the MCU to dial out to a PIN-protected audio conference on an audio bridge. The conference ID is 555 and the PIN is 888. The audio bridge requires that you press # after entering the ID and after entering the PIN. In this example the DTMF sequence could be: 555#,,888#. The two commas represent a four second pause which allows the audio bridge's automated menu system time to process the ID and request the PIN.</p>

Suppress audio during DTMF	<p>Suppresses the audio stream while initial DTMF connection sequence is being sent, so that other conference participants do not hear the audio of this participant or interactive voice responders reacting to the tones.</p> <p><i>Outgoing only</i> suppresses the audio to the endpoint while DTMF tones are sent to the endpoint.</p> <p><i>All</i> also suppresses both incoming and outgoing audio for the participant while the initial DTMF sequence is being sent to the endpoint.</p>	<p>This setting is independent of other audio muting mechanisms. Audio suppression is active for the duration of the DTMF tone sequence, including any deliberate pauses (commas in the DTMF sequence).</p>
Call-in match parameters	<p>These fields are used to identify incoming calls as being from the endpoint:</p> <ul style="list-style-type: none"> ■ Username: This must be the username that the endpoint sends to the MCU ■ IP address: The IP address of the endpoint 	<p>The endpoint is recognized if all filled-in fields in this section are matched. Fields left blank are not considered in the match.</p> <p>Note that in some cases a SIP registrar can cause a call to appear to come from the IP address of the registrar rather than the IP address of the endpoint. In this case, to use call-in match parameters, leave the IP address field blank and enter the correct username. The call will be matched by username.</p> <p>When using LCS, the username that will be matched is the user's display name (e.g. Peter Rabbit) rather than the sign-in name (bluecoat@cisco.com).</p>
Display name override	<p>The name that is displayed in a conference as a label on the video from this endpoint. It is also the name of the endpoint as it appears on the MCU's web interface.</p>	<p>The display name override is used in place of any identifier that appears on the endpoint's video or in the MCU's web interface. The endpoint could otherwise be identified by its SIP id, its E.164 number, or its IP address.</p> <p>If you use only non-printing characters, such as spaces, as a display name override, the MCU respects this 'blank' name as a label for video from this endpoint. In this case, the MCU does not show the non-printing override value when listing the endpoint in the web interface; it shows one of the endpoint's other identifiers instead.</p> <p>Note that once an endpoint has connected, you cannot change the display name via the web interface.</p>

Motion / sharpness trade off	<p>Choose whether to use the MCU-wide setting for motion/sharpness trade off, or configure an individual setting for this endpoint. Select from:</p> <ul style="list-style-type: none"> ■ <i>Use box-wide setting</i>: this is the default value. In this case, the endpoint will use the motion/sharpness tradeoff setting from the Settings > Conferences page ■ <i>Favor motion</i>: the MCU favors motion over sharpness; that is, it will try and use a high frame rate at the cost of lower resolution. The MCU will choose a resolution that allows for a framerate of 25 frames per second or higher. ■ <i>Favor sharpness</i>: the MCU favors sharpness over motion; it will use the highest resolution that is being sent in (by any endpoint), and adjust downwards, to their highest advertised resolution, for other endpoints if necessary. ■ <i>Balanced</i>: the MCU will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second) 	<p>The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the endpoint and the MCU. This setting controls how the MCU will negotiate the settings to be used with this endpoint.</p>
Transmitted video resolutions	<p>Choose the setting for transmitted video resolutions from the MCU to this endpoint. This setting overrides the MCU-wide setting on the Settings > Conferences page.</p>	<p>Retain the default setting (<i>use box-wide setting</i>) unless you are experiencing problems with the display of certain resolutions by this endpoint.</p> <p>Endpoints advertise the resolutions that they are able to display. The MCU then chooses from those advertised resolutions, the resolution that it will use to transmit video. However, some endpoints do not display widescreen resolutions optimally. Therefore, you might want to use this setting to restrict the resolutions available to the MCU for transmissions to this endpoint.</p>
Content contribution	<p>Whether this endpoint is permitted to contribute the conference content channel. Select from:</p> <p><use conference default>: this endpoint will use the Content contribution from endpoints setting from the per-conference configuration.</p> <p><i>Enabled</i>: This endpoint is allowed to contribute the content channel, even if content contribution from endpoints is disabled in the per-conference configuration.</p> <p><i>Disabled</i>: This endpoint is not allowed to contribute the conference channel, even if content contribution from endpoints is enabled in the per-conference configuration.</p>	<p>This setting is provided to allow you to individually configure whether or not an endpoint is allowed to contribute content to a conference.</p> <p>To use the content channel, the Content status must be enabled at the MCU-wide level (on the Settings > Content page) and, for any given conference, Content mode must not be <i>Disabled</i> in the conference settings.</p>

Content receive	Whether this endpoint is allowed to receive a separate content stream when in a conference.	<p>This setting is provided to allow you to individually configure whether or not an endpoint is allowed to receive content from a conference.</p> <p>To use the content channel, the Content status must be enabled at the MCU-wide level (on the Settings > Content page) and for any given conference Content channel video must also be enabled in the per-conference configuration.</p> <p>If set to <i>Disabled</i> the endpoint will not receive content or will receive the content in the normal video channel if that setting is enabled (Settings > Content > Display content in normal video channel).</p> <p>Note that Binary Floor Control Protocol (BFCP) content is supported.</p>
View border size	Choose a border size for video transmitted to this endpoint.	<p>This sets a border thickness to display around the video image. This is useful where the image is displaying off the edges of the participant's screen; use a border to force the image to display properly.</p> <p>Applying a border size here means that this border size will always be used for this endpoint's transmitted video. Note that you can also apply a border to a participant in a conference by going to Conferences and clicking on the name of the conference and then altering this participant's settings.</p>
Default view family	Sets the layout family to be used when calling out to this endpoint.	If this is set to <i>Use box-wide setting</i> then the default view family that has been configured via the Conference settings page will be used.
Preferred bandwidth from MCU	Identifies the network capacity (measured in bits per second) used by the media channels established by the MCU to a single participant.	These settings take priority over the Default bandwidth from MCU setting configured in the global conference settings.
Preferred bandwidth to MCU	The maximum combined media bandwidth advertised by the MCU to endpoints.	These settings take priority over the Default bandwidth to MCU setting configured in the global Conference settings (see Conference settings).

Layout control via FECC / DTMF	<p>Whether this endpoint is able to change their view layout via far-end camera control (FECC) or DTMF tones. Choose from:</p> <ul style="list-style-type: none"> ■ <i>use conference configuration</i>: the setting for Layout control via FECC / DTMF will be determined by the configuration of the conference ■ <i>Disabled</i>: the participant using this endpoint will not be allowed to change their view layout using either FECC or DTMF. This option also prevents the user from changing layout with the in call menu. ■ <i>FECC only</i>: the participant using this endpoint will be allowed to change their view layout using FECC ■ <i>DTMF only</i>: the participant using this endpoint will be allowed to change their view layout using DTMF ■ <i>FECC with DTMF fallback</i>: the participant using this endpoint will be allowed to change their view layout using FECC. If FECC is not available, this participant will be able to use DTMF ■ <i>FECC and DTMF</i>: the participant using this endpoint will be allowed to change their view layout using either either FECC or DTMF, rather than only using DTMF as a fallback. 	<p>This setting takes precedence over the per-conference layout control setting for conferences into which the endpoint is invited.</p> <p>This layout control setting does not govern layout control using the in call menu. The setting governs layout control using the endpoint's DTMF or FECC controls while the user is <i>not</i> using the menu.</p>
---------------------------------------	--	--

Send camera control to other participants	<p>Specifies whether FECC or DTMF from this participant may control a far end camera. This setting combines with layout control via FECC/DTMF to control the camera of the far end and the layouts of the conference. This setting overrides the global conference setting for this endpoint.</p> <ul style="list-style-type: none"> ■ <i>Disabled</i>: This participant will not be allowed to control a far end camera using either FECC or DTMF. ■ <i>FECC only</i>: This participant will be only be allowed to control a far end camera using FECC. ■ <i>DTMF only</i>: This participant will be only be allowed to control a far end camera using DTMF. ■ <i>FECC with DTMF fallback</i>: This participant will be allowed to control a far end camera using FECC. If FECC is not available, this participant will be able to use DTMF for camera control. ■ <i>FECC and DTMF</i>: This participant will be allowed to control a far end camera using either FECC or DTMF. 	<p>There are two control mechanisms, FECC and DTMF, either (or both) of which can be used for camera control or layout control. If one mechanism is allowed for camera control but not for layout control, then that mechanism only controls the far end camera and does not affect the layout. Similarly, if one mechanism is allowed for layout control but not for camera control, then it is not possible to control the camera with that mechanism. In these cases, the endpoint can use FECC or DTMF controls directly to change the layout or adjust the far end camera.</p> <p>When one control mechanism can control either the layout or the far end camera, then that mechanism will always control the layout until "Zoom in" (FECC mechanism) or 1 (DTMF mechanism) is pressed. The control mechanism then switches over to control the camera.</p> <p>Far-end camera control always applies to the camera of the participant shown in the largest or top left pane (when panes are the same size). If you have no way to control the layout, then you cannot focus on a participant to allow you to adjust a particular camera.</p>
Mute in-band DTMF	<p>Use this option to mute in-band DTMF from this endpoint. Choose from:</p> <ul style="list-style-type: none"> ■ <i>use conference configuration</i>: the setting for Mute in-band DTMF will be determined by the configuration of the conference ■ <i>Never</i>: the in-band DTMF from this endpoint will never be muted. Any DTMF tones sent from this endpoint will be audible to conference participants ■ <i>Always</i>: the in-band DTMF from this endpoint will always be muted. Any DTMF tones sent from this endpoint will not be audible to conference participants ■ <i>When used for MCU control</i>: if a participant is using in-band DTMF to control conference layout and for other in-conference features, the tones will be muted and will not be audible to conference participants. The MCU will only expect a participant to use DTMF for MCU control if Layout control via FECC / DTMF or Send camera control to participants is set to <i>DTMF only</i>, <i>FECC and DTMF</i>, or <i>FECC with DTMF fallback</i> and FECC has not been established, or if the participant is able to use the in call menu. 	<p>In some scenarios, where a conference is cascaded onto an audio bridge, it might be useful for one of the participants in that conference to be able to send in-band DTMF to the MCU. This is for the purposes of sending the conference ID or PIN to the audio conferencing bridge. In this case, the Mute in-band DTMF setting for the endpoint of that participant needs to be <i>Never</i>. However, you can instead send DTMF tones to the audio conferencing bridge directly from the MCU; for more information refer to Sending DTMF to an audio bridge.</p> <p>Unless you need to configure a particular setting for this endpoint, set this to <i>use conference configuration</i> and ensure you have the Mute in-band DTMF setting as required in the conference configuration (see Adding and updating conferences).</p> <p>This setting takes precedence over the per-conference Mute in-band DTMF setting for conferences into which the endpoint is invited.</p>

Appear as a recording device	When this setting is enabled, the red recording indicator dot is visible to other conference participants.	This participant is labeled as a recorder on the conference participants page.
Video to use by default	<p>Allows you to replace this participant's video with that of another participant. Select <i><self></i> (default value) to display this participant's own video by default.</p> <p>If you select another preconfigured endpoint from the dropdown, the MCU will no longer use this participant's own video by default: instead, it will use the video stream from the selected endpoint in most circumstances, for example when this participant becomes the active speaker.</p>	<p>If the selected Video to use by default is not available, the MCU will use this participant's own video if possible.</p> <p>If the selected Video to use by default is available, you can still show this participant's own video if you need to by explicitly choosing it in specific layout pane selections.</p>
Dial out as	Determines whether this participant is a chair or a guest in automatic lecture mode.	
Initial audio to MCU	Select <i>Active</i> or <i>Muted</i> to define whether audio from this endpoint should be muted whenever it first joins a conference.	<p>If this is <i>Muted</i>, then the MCU will mute the stream whenever it successfully invites the endpoint or recognizes the endpoint when it calls in.</p> <p>Audio from preconfigured endpoints can also be muted by the conference's Mute on join configuration, but only when they call in. In that case, if either the conference's Mute on join checkbox for Audio is checked, or the endpoint's Initial audio to MCU is <i>Muted</i> (or both) then the audio from the endpoint is muted when it joins the conference.</p>
Initial video to MCU	Select <i>Active</i> or <i>Stopped</i> to define whether video from this endpoint should be stopped whenever it first joins a conference.	<p>If this is <i>Stopped</i>, then the MCU will stop the stream whenever it successfully invites the endpoint or recognizes the endpoint when it calls in.</p> <p>Video from preconfigured endpoints can also be muted by the conference's Mute on join configuration, but only when they call in. In that case, if either the conference's Mute on join checkbox for Video is checked, or the endpoint's Initial video to MCU is <i>Muted</i> (or both) then the video from the endpoint is stopped when it joins the conference.</p>
Initial audio from MCU	<p>Select <i>Active</i> or <i>Muted</i> to define whether audio to this endpoint is muted whenever it first joins a conference.</p> <hr/> <p>Note: The endpoint may not always detect DTMF tones from the MCU after you mute the audio from the MCU.</p>	
Initial video from MCU	Select <i>Active</i> or <i>Stopped</i> to define whether video to this endpoint is stopped whenever it first joins a conference.	

Initial Adaptive Gain Control	Defines whether or not the endpoint uses Adaptive Gain Control (AGC) when it first joins the conference. Select <i><use conference configuration></i> to inherit the setting from the conference. Otherwise, you can select <i>Enabled</i> or <i>Disabled</i> to override the conference-wide AGC setting.	Any manual changes to the participant volume will turn AGC off for that participant. You can also manually enable or disable AGC for a participant that is already in the conference, on the Conference > Participants > <Name> > Audio page.
Automatic disconnection	When a participant disconnects from a conference and only endpoints set to Automatic disconnection are left, all those participants are disconnected.	Set to enabled if you want this endpoint to be automatically disconnected from conferences when only endpoints set to Automatic disconnection remain in a conference when any other participant has disconnected.
Custom codec selection	Can be used to ensure only specific codecs are permitted on calls to (and received from) this endpoint.	If <i>Enabled</i> , you can select which codecs are allowed to be used when communicating with this endpoint. This setting overrides the MCU-wide codec selection on the Settings > Conference page.

Related topics

- [Configuring SIP settings](#)
- [Configuring H.323 endpoints](#)
- [Displaying the endpoint list](#)

Managing gateways

Managing the built-in gatekeeper

Managing users

System defined users	128
User privilege levels	129
Displaying the user list	131
Adding and updating users	132
Updating your user profile	135
Changing your password	137

System defined users

The MCU is pre-configured with two user accounts ("admin" and "guest"), but you can also add other users (see [Adding and updating users](#)). Refer to the table below for descriptions of the pre-configured users.

User ID	Description	Usage tips
admin	<p>The MCU must have at least one configured user with administrator privileges. By default, the User ID is "admin" and no password is required.</p> <p>If you configure the MCU with advanced account security mode, the admin account requires a password that adheres to secure password criteria. For more information about advanced account security mode, refer to Configuring security settings.</p>	<p>After logging into the MCU for the first time (see Logging into the web interface), you can change the User ID and password for this account. The privilege level is fixed at <i>administrator</i> for the admin user - who can see all the pages and change settings.</p>
guest	<p>The MCU must have at least one configured user with access privileges below <i>administrator</i>. The fixed User ID for this user is "guest" and by default no password is required.</p> <p>If you configure the MCU with advanced account security mode, the guest account requires a password that adheres to secure password criteria. For more information about advanced account security mode, refer to Configuring security settings.</p>	<p>You cannot change the name of the "guest" User ID. You can add a password.</p>

You can modify the system defined user accounts if you need to. For example, for security, you should add a password to the admin account.

Note that you can also create new accounts with administrator or lower access privileges in addition to these pre-defined users (see [Adding and updating users](#)).

Related topics

- [Displaying the user list](#)
- [Adding and updating users](#)
- [Configuring security settings](#)
- [User privileges](#)
- [Updating your user profile](#)

User privilege levels

Every configured user in the MCU has an associated privilege level. There are six defined privilege levels which determine the amount of control the user has over the MCU and its settings. Refer to the table below for details.

Privilege level	Access
administrator	<p>The main difference between an administrator and users with lower privilege levels is that administrators can change settings that affect all conferences and the configuration of the MCU itself, whereas other users only have access to individual conferences and to their own profiles.</p> <p>Users with administrator access can:</p> <ul style="list-style-type: none"> ■ View MCU-wide status (Status) ■ Access all settings pages (Settings) ■ Perform software upgrades (Settings > Upgrade) ■ Change system-wide conference settings (Settings > Conferences) ■ View the Event log (Logs) ■ Manage users (Users) ■ Manage endpoints (Endpoints) ■ Configure auto attendants (Conferences > Auto attendants) ■ Fully control conferences (Conferences)
conference creation and full control	<p>Users with this privilege level can:</p> <ul style="list-style-type: none"> ■ Change their own profile (Profile) ■ View the list of active conferences (Conferences) ■ View participant lists for active conferences (Conferences) ■ Schedule new conferences (Conferences) ■ Fully control and modify all public conferences and the conferences they own (Conferences) ■ Manage endpoints (Endpoints)
conference creation and limited control	<p>Users with this privilege level can:</p> <ul style="list-style-type: none"> ■ Change their own profile (Profile) ■ View the list of active conferences (Conferences) ■ View participant lists for active conferences (Conferences) ■ Schedule new conferences (Conferences) ■ Fully control and modify conferences they own (Conferences) ■ Exercise limited control of conferences owned by other users (Conferences) <p>See Conference ownership for additional information on which actions are permitted (and forbidden) by limited control.</p>

conference creation	<p>Users with this privilege level can:</p> <ul style="list-style-type: none">■ Change their own profile (Profile)■ View the list of active conferences (Conferences)■ View participant lists for active conferences (Conferences)■ Schedule new conferences (Conferences)■ Fully control and modify conferences they own (Conferences)
conference detail	<p>Users with this privilege level can:</p> <ul style="list-style-type: none">■ Change their own profile (Profile)■ View the list of active conferences (Conferences)■ View participant lists for active conferences (Conferences)
conference list only	<p>Users with this privilege level can:</p> <ul style="list-style-type: none">■ Change their own profile (Profile). The 'guest' account is an exception; Users logging in as 'guest' may view the conference list but may not change the 'guest' profile.■ View the list of active conferences (Conferences)

Related topics

- [System defined users](#)
- [Displaying the user list](#)
- [Adding and updating users](#)
- [Updating a user's profile](#)

Displaying the user list

The **User list** page gives you a quick overview of all configured users on the MCU and provides a summary of some of their settings. To view the **User list** page, go to **Users**. Refer to the table below for assistance.

Field	Field description
User ID	The user name that the user needs to access the web interface of the MCU. Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.
Name	The full name of the user.
Privilege	Access privileges associated with this user. See User privileges for detailed explanations.
E.164	The associated E.164 telephone number.
Video endpoint	The associated video endpoint.
Picture	The configured image to display for this user.

Deleting users

To delete a user, select the user you want to delete and click **Delete selected users**. You cannot delete the 'admin' and 'guest' users.

Related topics

- [Adding and updating users](#)
- [System defined users](#)
- [User privileges](#)

Adding and updating users

You can add users to and update users on the MCU. Although most information is identical for both tasks, some fields differ.

The MCU supports up to 200 users.

Adding a user

To add a user:

1. Go to the **Users** page.
2. Click **Add new user**.
3. Complete the fields referring to the table below to determine the most appropriate settings for the user.
4. After entering the settings, click **Add user**.

Updating a user

To update an existing user:

1. Go to the **Users** page.
2. Click the username of the account you want to update.
3. Edit the user settings, referring to the following table as necessary.
4. After changing the settings, click the update button.

Field	Field description	More information
User ID	Identifies the log-in name that the user will use to access the MCU web interface.	Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters. The following user ids are reserved and cannot be added: <ul style="list-style-type: none">■ admin■ guest■ invalid■ system■ unknown
Name	The full name of the user.	

Password	<p>The required password, if any, up to a maximum of 31 characters. Enter the password in whichever character set you require, but note that some browsers and FTP clients do not support Unicode characters. The MCU never stores the password in plain text.</p>	<p>This field is only active when adding a new user. If you are updating an existing user, the field is called New password. Password changes are immediately effective, that is, any users logged in with the account will be logged out and must use the new password. This also applies to admin users changing their own accounts, who will be logged out as soon as they commit a new password.</p> <p>If the MCU is not using advanced account security mode, there are no password constraints. You can use any password or no password at all.</p> <p>In advanced account security mode (configured on the Settings > Security page), the password requirements are more stringent. Passwords must have:</p> <ul style="list-style-type: none"> ■ at least fifteen characters ■ at least two uppercase alphabetic characters ■ at least two lowercase alphabetic characters ■ at least two numeric characters ■ at least two non-alphanumeric (special) characters ■ no more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not <p>See Configuring security settings for more details.</p>
Re-enter password	Verifies the required password.	
Disable user account	Select to disable this account.	<p>This can be useful if you want to keep an account's details, but do not want anyone to be able to use it at the moment.</p> <p>You cannot disable the system-created admin account.</p> <p>The system-created 'guest' account is disabled by default. If you enable it, the MCU will create a security warning.</p> <p>In advanced account security mode, a non-admin account will expire after 30 days of inactivity; that is, the MCU will disable it. To re-enable a disabled account, clear this option.</p> <p>For more information about advanced account security mode, refer to Configuring security settings.</p>
Lock password	Prevents user from changing password.	This is useful where you want multiple users to be able to use the same user ID. The system-created guest account has <i>Lock password</i> enabled by default.
Force user to change password on next login	Select this option to force a user to change their password. Next time this user attempts to log in to the MCU, a change password prompt will appear.	<p>This option is enabled by default for a newly created account. It is a good idea for new users to set their own secure passwords.</p> <p>This option is not available for accounts where <i>Lock password</i> is selected.</p> <p>When the user changes his password, the MCU clears this check box automatically.</p>
Privilege level	The access privileges to be granted to this user.	See User privileges for detailed explanations.

E.164 phone number	Associates an E.164 telephone number with a user account.	If the MCU receives a call from the E.164 phone number provided, it matches the number to the user account. This allows the MCU to take appropriate action if the Associated video endpoint field is completed or a picture is uploaded for the user.
Associated video endpoint	Associates a configured endpoint with the user. This is used when a participant's video stream is from a separate device such as a web camera on a PC or a recording from an IP VCR.	<p>If you set an associated video endpoint for a user, when a call is received from the E.164 phone number, the MCU knows that that call is audio-only. To provide the user with a video stream, the MCU calls the endpoint entered in this field. The user then has the complete conference experience with the audio on the telephone and a separate video stream for example on a computer with a web camera installed. The audio and video streams are matched so that the layout views for all participants reflect the level of audio received on the call from the E.164 phone number.</p> <p>Do not set the user's E.164 phone number and Associated video endpoint as the same number. If a user is going to be a normal video endpoint user, simply enter the E.164 phone number and leave the associated video endpoint field set to <i>None</i>.</p> <p>If required, a user's video contribution can be a recording on an IP VCR. In this case the recording must first be configured as an H.323 endpoint on the MCU.</p> <p>See Adding an H.323 endpoint for information about adding endpoints.</p>

Picture upload

Upload image file	The image to be used if a user joins a conference as an audio-only participant calling from the E.164 phone number specified above and there is no associated video endpoint.	<p>This option is only available after you add the user.</p> <p>Because there is no video stream for the user, you can display a still image in the pane where the participant would normally appear.</p> <p>The maximum size of the picture is 176 x 144 pixels and the maximum file size is 500k.</p> <p>Click Browse to locate the image (jpg, gif, or Windows bmp file). Then, click Send file to upload the image to the MCU.</p> <p>The bitmap will only display if the user calls in to the MCU from the E.164 phone number using an audio-only device and there is no associated video endpoint.</p>
--------------------------	---	--

Related topics

- [System defined users](#)
- [Displaying the user list](#)
- [User privileges](#)
- [Updating your own profile](#)
- [Configuring H.323 endpoints](#)
- [Configuring security settings](#)

Updating your user profile

You can make some changes to your user profile. To do this, click **Profile** to reach the **User profile** page. This page is not available for administrators; these users manage their profiles via the **User** tab. Refer to the table below for tips.

Field	Field description	More information
Name	Your name, which identifies you to other users.	Changing this field does not change your log-in User ID.
E.164 phone number	Associates an E.164 telephone number with your user account.	<p>This limits the setup you will need to do each time you join a video conference. When the MCU receives a call from this number, it will be recognized as coming from your phone. If the device is an audio-only phone, you can set up an associated video endpoint and/or upload a picture file.</p> <p>This field is not available for the <i>admin</i> or <i>guest</i> accounts.</p>
Associated video endpoint	Associates a configured H.323 endpoint with your user account.	<p>If you call in to the MCU from your E.164 phone number using an audio-only device, the MCU calls your associated video endpoint and sends the conference video stream to that associated video endpoint (and receives a video-only stream from that endpoint).</p> <p>This field is not available for the <i>admin</i> or <i>guest</i> accounts.</p>
Change password		
Current password	Type your current password.	

Password	Type your new password.	<p>In advanced account security mode, a new password must be different to the previous 10 passwords that have been used with an account.</p> <p>Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.</p> <p>In advanced account security mode (configured on the Settings > Security page), passwords must have:</p> <ul style="list-style-type: none"> ■ at least fifteen characters ■ at least two uppercase alphabetic characters ■ at least two lowercase alphabetic characters ■ at least two numeric characters ■ at least two non-alphanumeric (special) characters ■ not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not <p>In advanced account security mode, a password must be different from the previous ten used with that account. Also, a password will expire if it is not changed within 60 days.</p> <p>If the MCU is not using advanced account security mode, any password can be used.</p> <p>Note that passwords are stored in the configuration.xml file as plain text unless the MCU is configured (or has ever been configured) to use advanced account security mode. For more information, refer to Configuring security settings.</p>
-----------------	-------------------------	--

Re-enter password	Verify your new password.
--------------------------	---------------------------

Picture upload

Upload bitmap file	<p>You can upload an image which will display in the conference when you join conferences in audio-only mode.</p>	<p>Click Browse to locate the bitmap image. Then, click Send file to upload the image to the MCU.</p> <p>The bitmap will only display if you call in to the MCU from your E.164 phone number using an audio-only device and you do not have an associated video endpoint.</p>
---------------------------	---	---

Changing your password

In advanced account security mode, passwords must have:

- at least fifteen characters
- at least two uppercase alphabetic characters
- at least two lowercase alphabetic characters
- at least two numeric characters
- at least two non-alphanumeric (special) characters
- not more than two consecutive repeating characters. That is, two repeating characters are allowed, three are not

In advanced account security mode, a new password must be different to the previous 10 passwords that have been used with an account.

In advanced account security mode, if a user logs in with a correct but expired password the MCU asks that user to change the password. If the user chooses not to change it, that user is allowed two more login attempts to change the password before the account gets disabled.

In advanced account security mode, users other than administrator users are not allowed to change their password more than once in a 24 hour period.

If the MCU is not in advanced account security mode, there are no criteria for password selection.

If the MCU is in advanced account security mode, the above criteria for passwords are displayed on the **Change password** page.

Related topics

- [Configuring security settings](#)
- [Understanding security warnings](#)

Configuring network and system settings

Configuring network settings	139
Automatic IPv6 address preferences	143
Configuring DNS settings	144
Configuring IP routes settings	146
Configuring IP services	149
Configuring SNMP settings	151
Configuring QoS settings	153

Configuring network settings

To configure the network settings on the MCU and check the network status, go to **Network > Port A** or **Network > Port B**.

The MCU has two Ethernet interfaces, Port A and Port B. The configuration pages for the two interfaces look and behave similarly, and so are described together. Differences will be noted as appropriate.

Port A and Port B can be configured to be allocated their IP addresses by DHCP (IPv4) or SLAAC/DHCPv6 (IPv6). Connect Port A to your local network and connect Port B to a second subnet or the internet depending on your application of the MCU.

On this page:

- [IP configuration settings](#)
- [IP status](#)
- [Ethernet configuration](#)
- [Ethernet status](#)

IP configuration settings

These settings determine the IP configuration for the appropriate Ethernet port of the MCU. When you have finished, click **Update IP configuration**.

Field	Field description	Usage tips
IPv4 configuration		
IP configuration	Specifies whether the port should be configured manually or automatically. If set to <i>Automatic via DHCP</i> the MCU obtains its own IP address for this port automatically via DHCP (Dynamic Host Configuration Protocol). If set to <i>Manual</i> the MCU will use the values that you specify in the Manual configuration fields below.	It is not possible to disable a port if it is being used to access the web user interface, however, it can be disabled via the serial connection. To disable a port that is currently being used to access the web interface via this field, change to a different port for web interface access.
Manual configuration		
IP address	The dot-separated IPv4 address for this port, for example 192.168.4.45	You only need to specify this option if you have chosen <i>Manual</i> IP configuration, as described above. If IP configuration is set to <i>Automatic by DHCP</i> this setting will be ignored.
Subnet mask	The subnet mask required for the IP address you want to use, for example 255.255.255.0	
Default gateway	The IP address of the default gateway on this subnet, for example 192.168.4.1	

IPv6 configuration

IP configuration Specifies whether the port should be configured manually or automatically, or disabled. If set to *Automatic via SLAAC/DHCPv6* the MCU obtains its own IP address for this port automatically. The protocol used will be SLAAC, Stateful DHCPv6, or Stateless DHCPv6 as indicated by the ICMPv6 Router Advertisement (RA) messages. If set to *Manual* the MCU will use the values that you specify in the Manual configuration fields below.

Manual configuration

IPv6 address	<p>The (hexadecimal) colon-separated IPv6 address for this port, for example [2001:db8:168:4::45].</p> <p>See Automatic IPv6 address preferences for more information about IPv6 addresses that are assigned automatically.</p>	<p>You only need to specify this option if you have chosen <i>Manual</i> IP configuration, as described above.</p> <p>If IP configuration is set to <i>Automatic via SLAAC/DHCPv6</i> this setting is ignored.</p> <p>When you enter an IPv6 address anywhere in the user interface, the address must be enclosed in square brackets [].</p>
Prefix length	The (decimal) prefix length value for the global IPv6 address for this port. In the above IPv6 address example, the prefix length is 64.	
Default gateway	Optionally, specifies the IPv6 address of the default gateway on this subnet.	The address can be global or link-local.

IP status

Use the IP status fields to verify the current IP settings for the appropriate Ethernet port of the MCU, which were obtained using DHCP/SLAAC or configured manually (see [IP configuration settings](#)) including:

- DHCP
- IP address
- Subnet mask
- Default gateway
- DHCPv6
- IPv6 address
- IPv6 default gateway
- IPv6 link-local address

Ethernet configuration

These settings determine the Ethernet settings for the appropriate port of the MCU. Refer to the table for assistance with these settings. When you have finished, click **Update Ethernet configuration**.

Field	Field description	Usage tips
Ethernet settings	Specify whether you want this Ethernet port to automatically negotiate its Ethernet settings with the device it is connected to, or if it should use the values that you specify in the Manual configuration fields below.	It is important that your Ethernet settings match those of the device to which this port is connected. For example, both devices must be configured to use automatic negotiation, or both configured with fixed and matching speed and duplex settings (see below).
Manual configuration		
Speed	Identifies the connection speed: <i>10 Mbit/s</i> or <i>100 Mbit/s</i> . Use automatic negotiation if a connection speed of <i>1000 Mbit/s</i> is required.	The connection speed must match that of the device to which this port is connected. You only need to select this option if you have chosen <i>Manual</i> Ethernet settings, as described above.
Duplex	Identifies the connection duplex mode: <ul style="list-style-type: none"> ■ <i>Full duplex</i> Both devices can send data to each other at the same time ■ <i>Half duplex</i> Only one device can send to the other at a time 	The duplex setting must match that of the device to which this port is connected. You only need to select this option if you have chosen <i>Manual</i> Ethernet settings, as described above.

Ethernet status

Field	Field description	Usage tips
Link status	Indicates whether this Ethernet port is connected to or disconnected from the network.	
Speed	The speed (<i>10/100/1000 Mbit/s</i>) of the network connection to the MCU on this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
Duplex	The duplex mode (<i>Full duplex</i> or <i>Half duplex</i>) of the network connection to this port.	This value is negotiated with the device to which this port is connected or based on your Manual configuration selected above.
MAC address	The fixed hardware MAC (Media Access Control) address of this port.	This value cannot be changed and is for information only.
Packets sent	Displays a count of the total number of packets sent from this port by the MCU. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the MCU is transmitting packets into the network.
Packets received	Displays a count of the total number of packets received by this port of the MCU. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the MCU is receiving packets from the network.

Statistics:	These fields display further statistics for this port.	Use these fields for advanced network diagnostics, such as resolution of problems with Ethernet link speed and duplex negotiation.
	<ul style="list-style-type: none">■ Multicast packets sent■ Multicast packets received■ Total bytes sent■ Total bytes received■ Receive queue drops■ Collisions■ Transmit errors■ Receive errors	

Related topics

- [Configuring DNS settings](#)
- [Configuring IP routing settings](#)
- [Configuring IP services](#)
- [Configuring SNMP settings](#)
- [Upgrading the firmware](#)
- [Network connectivity testing](#)

Automatic IPv6 address preferences

The table below details the address assignment preferences that are applied for IPv6 addressing based on the ICMPv6 Router Advertisements received when port configuration is set to Automatic.

RA flags			Preferred address
a	o	m	
0	0	0	Stateful DHCPv6
1	0	0	SLAAC
0	1	0	Stateful DHCPv6
1	1	0	Stateless DHCPv6
0	0	1	Stateful DHCPv6
1	0	1	Stateful DHCPv6
0	1	1	Stateful DHCPv6
1	1	1	Stateful DHCPv6

a: ICMPv6 prefix information, auto flag

o: ICMPv6, other flag

m: ICMPv6, managed flag

Related topics

- [Configuring network settings](#)

Configuring DNS settings

To configure DNS settings on the MCU, go to **Network > DNS**. These settings determine the DNS configuration for the MCU.

Click **Update DNS configuration** after making any changes.

Field	Field description	Usage tips
DNS configuration		
DNS configuration	Select a DNS server preference from the list or select <i>Manual</i> to specify DNS settings manually.	<p>If you select <i>Manual</i>, you must configure the name server(s) on this page. If you select one of the DHCP options, the MCU receives its nameserver address via DHCP on the interface you select.</p> <p>If <i>Automatic via DHCP</i> (IPv4) or <i>Automatic via SLAAC/DHCPv6</i> (IPv6) is selected for IP configuration (on the Ethernet Port's configuration page), no DNS name server will be available until the MCU receives the address via DHCP on that interface.</p> <p>For example, if you select <i>Via Port A DHCPv6</i> for DNS configuration, you must ensure that Port A is configured to use DHCPv6. Do this by going to the Network > Port A page and selecting <i>Automatic via SLAAC/DHCPv6</i> in the IP configuration field of the IPv6 interface.</p> <p>Note that if the DHCP server on your network does not supply DNS configuration information, then the MCU will have no ability to look up names. Additionally, for IPv6 the Router Advertisement packets determine whether or not DHCPv6 is used.</p>
Host name	Specifies a name for the MCU.	Depending on your network configuration, you may be able to use this host name to communicate with the MCU, without needing to know its IP address.
Name server	The IP address of the name server.	
Secondary name server	Identifies an optional second name server.	The secondary DNS server is only used if the first is unavailable. If the first server returns that it does not know an address, the secondary DNS server will not be queried.
Domain name (DNS suffix)	Specifies an optional suffix to add when performing DNS lookups.	<p>This option can allow you to use non-fully qualified host names when referring to a device by host name instead of IP address.</p> <p>For example, if the domain name is set to <i>cisco.com</i>, then a request to the name server to look up the IP address of host <i>endpoint</i> will actually lookup <i>endpoint.cisco.com</i>.</p>

Viewing DNS status

Use the DNS status fields to verify the current DNS settings for the MCU, including:

- Host name
- Name server
- Secondary name server
- Domain name (DNS suffix)

Related topics

- [Configuring network settings](#)
- [Configuring IP routing settings](#)
- [Configuring IP services](#)

Configuring IP routes settings

If the *Video Firewall* feature is enabled (see [Upgrading the firmware](#)), you will need to set up one or more routing settings to control how IP traffic flows in and out of the MCU.

It is important that these settings are configured correctly, or you may be unable to make calls or access the web interface.

To configure the route settings, go to **Network > Routes**.

On this page:

- [Port preferences](#)
- [IP routes configuration](#)
- [Current IP status](#)

Port preferences

If both Ethernet ports are enabled, it is necessary to specify which port is used in certain special circumstances. Make the appropriate selections described below. Click **Apply changes**.

Field	Field description	Usage tips
IPv4 gateway preference	In the absence of more specific routing (see IP routes configuration) the MCU sends packets to the default gateway. Each port can have a different default gateway but the MCU only permits one to be in use at a time, so this option selects which default gateway will be used for IPv4 packets.	If an Ethernet port is disabled, you cannot specify that the default gateway for that port is the one to use. See also Routes behavior with disabled ports below.
IPv6 gateway preference	In the absence of more specific routing (see IP routes configuration) the MCU sends packets to the default gateway. Each port can have a different default gateway but the MCU only permits one to be in use at a time, so this option selects which default gateway will be used for IPv6 packets.	If an Ethernet port is disabled, you cannot specify that the default gateway for that port is the one to use. See also Routes behavior with disabled ports below.

IP routes configuration

In this section you can control how IP packets should be directed out of the MCU. You should only change this configuration if you have a good understanding of the topology of the network(s) to which the MCU is connected.

Configuration of routes is divided into two sections: addition of new routes, and the display and removal of existing routes.

Adding a new IP route

To add a new route, enter the details using the table below for reference. Click **Add IP route** to make the addition. If the route already exists, or aliases (overlaps) an existing route, you will be prompted to correct the problem and try again. The MCU can support up to 128 routes in total.

Field	Field description	Usage tips
IP address / mask length	<p>Use these fields to define the type of IP addresses to which this route applies.</p> <p>IPv4 addresses must be in the dot-separated IPv4 format and IPv6 addresses must be in hexadecimal colon-separated IPv6 address format, while the mask length is chosen in the mask length field. IPv6 addresses must be enclosed in square brackets.</p> <p>The mask field specifies how many bits of the address are fixed; unfixed bits must be set to zero in the address specified.</p>	To route all IP addresses in the range 192.168.4.128 to 192.168.4.255 for example, specify the IP address as 192.168.4.128 and the mask length as 25, to indicate that all but the last seven bits address are fixed.
Route	Use this field to control how packets destined for addresses matching the specified pattern are routed.	<p>You may select <i>Port A</i>, <i>Port B</i> or <i>Gateway</i>. If <i>Gateway</i> is selected, specify the IP address of the gateway to which you want packets to be directed.</p> <p>Selecting <i>Port A</i> results in matching packets being routed to Port A's default gateway (see Configuring network settings).</p> <p>Selecting <i>Port B</i> will cause matching packets to be routed to Port B's default gateway.</p> <p>If Ethernet Port B is disabled, the option to route packets to Port B will be disabled.</p>

Viewing and deleting existing IP routes

Configured routes are listed below the **Add IP route** section in a separate section each for IPv4 and IPv6. For each route, the following details are shown:

- **Destination:** The IP address or address block that the route applies to.
- **Gateway:** The IP address of the gateway where matching packets will be routed through. This can be - if the destination is in the local subnets, the IP address of a default gateway of a particular network interface, or the IP address of a user specified gateway.
- **Port:** Physical network interface that matching packets will be sent through.
- **Type:** Whether the route has been configured automatically as a consequence of other settings, or added by the user as described above.

The *default* route is configured automatically in correspondence with the *Default gateway preference* field (see [Port preferences](#)) and cannot be deleted. Any packets not covered by manually configured routes will be routed according to this route.

Manually configured routes may be deleted by selecting the appropriate check box and clicking **Delete selected**.

Routes behavior with disabled ports

If you disable the Ethernet port that is currently specifying the default gateway, then there is no default gateway and the only destinations that are reachable are those that are either on the same subnet as the enabled Ethernet port or are covered by an explicit route that uses that port.

Similarly, if you disable the Ethernet port that is used by an explicit route, then destinations that are covered by that route cease to be reachable.

Note: Be very careful when changing routing as it is possible make the MCU unreachable from your PC (or any device used to connect to the web interface). You need to ensure that at all times one of the following is true:

- The MCU has an enabled interface on the same subnet as the PC.
 - The MCU has an explicit route that includes the PC's address and goes through an enabled interface.
 - The MCU does not have an explicit route that includes the PC's address but does have a default route through an enabled interface that reaches the PC.
-

Related topics

- [Configuring DNS settings](#)
- [Configuring network settings](#)
- [Configuring IP services](#)
- [Configuring SNMP settings](#)
- [Upgrading and backing up the MCU](#)
- [Network connectivity testing](#)

Configuring IP services

To configure IP services, go to **Network > Services**.

Use this page to control the type of services that may be accessed via Ethernet ports A and B. For example, if one Ethernet port is connected to a network outside your organization's firewall, you can restrict the level of access that external users are entitled to on that port by, for example, enabling HTTPS for IPv4 and IPv6.

To prevent accidental lock-outs, the system does not allow you to disable the service that is currently being used to administer the MCU. For example, if you are configuring the gateway over HTTP and coming in on Port A, then the option to change the HTTP service for Port A will be unavailable in the interface.

Refer to the table below for more details.

In addition to controlling the Ethernet interfaces over which a service operates, this page also allows an administrator to specify the port number on which that service is provided. If the port number for a service is changed, it is necessary to ensure that the new value chosen does not clash with the port number used by any of the other services. However, in most circumstances, the pre-configured default values will suffice.

The settings on this page apply to both IPv4 and IPv6 addressing. The page displays the IPv4 and/or IPv6 values per port, depending on whether IPv4 and/or IPv6 are enabled for the port. When specifying settings use the appropriate column for the required addressing scheme.

Note that by default SNMP Traps are sent to UDP port 162 (on the destination network management station); this is configurable. For more information, refer to [Configuring SNMP settings](#).

To reset all values back to their factory default settings, click **Reset to default** and then click **Apply changes**.

Field	Field description	Usage tips
TCP service		
HTTP	Enable/disable HTTP access on the specified interface or change the port that is used for this service.	<p>HTTP access is required to view and change the MCU web pages and read online help files. If you disable HTTP access on both Ports A and B, you will need to use the serial console interface to re-enable it.</p> <p>If you require advanced security for the MCU, enable HTTPS and disable HTTP access.</p> <p>If a port is disabled, this option will be unavailable.</p>
HTTPS	Enable/disable HTTPS access, or change the port number used for HTTPS, on the specified interface.	<p>This field is only visible if the MCU has the <i>Secure management (HTTPS)</i> feature key or an <i>Encryption</i> feature key installed. For more information about installing feature keys, refer to Upgrading and backing up the MCU.</p> <p>By default, the MCU has its own SSL certificate and private key. However, you can upload a new private key and certificates if required. For more information about SSL certificates, refer to Configuring SSL certificates.</p> <p>If a port is disabled, this option will be unavailable.</p>

Incoming H.323	Enable/disable the ability to receive incoming calls to the MCU using H.323 or change the port that is used for this service.	<p>Disabling this option will not prevent outgoing calls to H.323 devices being made by the MCU.</p> <p>That is, the MCU will need to dial out to conference participants who are using H.323.</p> <p>If a port is disabled, this option will be unavailable.</p>
SIP (TCP)	Allow/reject incoming calls to the MCU using SIP over TCP or change the port that is used for this service.	<p>Disabling this option will not prevent outgoing calls to SIP devices being made by the MCU. That is, the MCU will need to dial out to conference participants who are using SIP over TCP.</p> <p>Note that if a SIP Outbound connection is negotiated with the registrar, SIP calls incoming via the registrar will still be accepted by the MCU.</p> <p>If a port is disabled, this option will be unavailable.</p>
Encrypted SIP (TLS)	Allow/reject incoming encrypted SIP calls to the MCU using SIP over TLS or change the port that is used for this service.	<p>Disabling this option will not prevent outgoing calls to SIP devices being made by the MCU. That is, the MCU will need to dial out to conference participants who are using SIP over TLS.</p> <p>If a port is disabled, this option will be unavailable.</p>
UDP service		
SNMP	Enable/disable the receiving of the SNMP protocol on this port or change the port that is used for this service.	<p>If a port is disabled, this option will be unavailable.</p> <p>If you want to enable the receiving of the SNMP protocol on Port B, ensure that you have the video firewall as an activated feature (refer to Upgrading and backing up the MCU) and you have selected the check box for SNMP on Port B.</p> <p>Note that by default SNMP Traps are sent to port UDP port 162 (on the destination network management station); this is configurable. For more information, refer to Configuring SNMP settings.</p> <p>If you require advanced security for the MCU, disable the SNMP service.</p>
SIP (UDP)	Allow/reject incoming and outgoing calls to the MCU using SIP over UDP or change the port that is used for this service.	<p>Disabling this option will prevent calls using SIP over UDP.</p> <p>If a port is disabled, this option will be unavailable.</p> <p>If you want to allow incoming and outgoing SIP (UDP) calls on Port B, ensure that you have the video firewall as an activated feature (refer to Upgrading and backing up the MCU) and you have selected the check box for SIP (UDP) on Port B.</p>

Related topics

- [Configuring DNS settings](#)
- [Configuring network settings](#)
- [Configuring IP routes](#)
- [Configuring SNMP settings](#)
- [Configuring SSL certificates](#)

Configuring SNMP settings

To configure monitoring using SNMP, go to **Network > SNMP**.

The MCU sends out an SNMP trap when the device is shut down or started up. The SNMP page allows you to set various parameters; when you are satisfied with the settings, click **Update SNMP settings**.

Note that:

- The 'system uptime' that appears in the trap is the time since SNMP was initialized on the MCU (and therefore will differ from the **Uptime** reported by the MCU on the **Status > General** page).
- The SNMP MIBs are read-only.

System information

Field	Field description	Usage tips
Name	Identifies the MCU in the SNMP system MIB.	Usually you would give every device a unique name. The default setting is: Cisco TelePresence MCU
Location	The location that appears in the system MIB.	An optional field. Where you have more than one MCU, it is useful to identify where the MCU is located. The default setting is: <i>Unknown</i>
Contact	The contact details that appear in the system MIB.	An optional field. The default setting is: <i>Unknown</i> Add the administrator's email address or name to identify who to contact when there is a problem with the device. If SNMP is enabled for a port on the public network, take care with the details you provide here.
Description	A description that appears in the system MIB.	An optional field, by default this will indicate the model number of the MCU. Can be used to provide more information on the MCU.

Configured trap receivers

Field	Field description	Usage tips
Enable traps	Select this check box to enable the MCU to send traps.	If you do not select this check box, no traps will be sent.
Enable authentication failure trap	Select this check box to enable authentication failure traps.	You cannot select this check box unless you have selected to Enable traps above. Authentication failure traps are generated and sent to the trap receivers when someone tries to read or write a MIB value with an incorrect community string.
Trap receiver addresses 1 to 4	Enter the IP address or hostname for up to four devices that will receive both the general and the authentication failure traps.	The traps that are sent by the MCU for IPv4 are SNMP v1 traps. For IPv6 the MCU sends SNMP v2 traps. You can configure trap receivers or you can view the MIB using a MIB browser. You can set the UDP port number for the trap in the format <IP address>: <port number>. By default the UDP port number is 162. Note that square brackets are mandatory for IPv6 addresses.

Access control

Field	Field description	Usage tips
RO community	Community string/password that gives read-only access to all trap information.	Note that SNMP community strings are not secure. They are sent in plain text across the network.
RW community	Community string/password that gives read/write access to all trap information.	We recommend that you change the community strings before enabling SNMP as the defaults are well known.
Trap community	Community string/password that is sent with all traps.	Some trap receivers can filter on trap community.

Related topics

- [Configuring DNS settings](#)
- [Configuring network settings](#)
- [Configuring IP routes](#)
- [Configuring IP services](#)

Configuring QoS settings

Quality of Service (QoS) settings are defined on the [Network > QoS](#) page to set priorities for outbound traffic from the MCU. They are specified as 6-bit binary values (tags) in the *Type of Service* header field for IPv4 or the *Traffic Class* header field for IPv6, and can be interpreted by networks as Type of Service (ToS) or Differentiated Services (DiffServ).

QoS tags are supported for every IP packet type transmitted by the MCU: media (audio and video), streaming, signaling, and administration.

CAUTION: We advise you not to alter QoS settings unless you have specific requirements to do so.

Note: In a cluster, a slave MCU only tags OA&M (Operations, Administration, and Maintenance) types of traffic because the master MCU handles all other types of traffic on behalf of the cluster, and does the QoS tagging for those types. You can change the slave's **OA&M** QoS value on the slave's [Network > QoS](#) page.

QoS tags

Field (tag)	Defines priority for...
Audio	Audio data packets, including RTP and RTCP streams.
Video	Video data packets, including FECC, BFCP, RTP, and RTCP streams.
Signaling	H.225, H.245, and SIP signaling packets.
OA&M	Operations, Administration, and Maintenance packets, including HTTP, HTTPS, FTP, DNS, syslog, OCSP, and NTP traffic.

Any traffic that is not covered by one of these categories is tagged as **OA&M**.

ToS configuration

ToS uses six out of a possible eight bits. The MCU allows you to set bits 0 to 5, and places zeros for bits 6 and 7.

- Bits 0-2 set IP precedence (the priority of the packet).
- Bit 3 sets delay: 0 = normal delay, 1 = low delay.
- Bit 4 sets throughput: 0 = normal throughput, 1 = high throughput.
- Bit 5 sets reliability: 0 = normal reliability, 1 = high reliability.
- Bits 6-7 are reserved for future use and cannot be set using the MCU interface.

ToS configuration represents a tradeoff between precedence, delay, throughput, and reliability. Ensure that you maintain a balance when prioritizing packets, so that other packets on the network are not subject to undue delay (so for example, do not set every value to 1).

DiffServ configuration

DiffServ uses six out of a possible eight bits to set a codepoint. There are 64 possible codepoints. The MCU allows you to set bits 0 to 5, and places zeros for bits 6 and 7. The codepoint is interpreted by DiffServ nodes to determine how the packet is treated.

Default values

These are the default QoS settings on the MCU:

- *Audio 101110*
 - For ToS, this means IP precedence is set to 5 giving relatively high priority. Delay is set to low, throughput is set to high, and reliability is set to normal.
 - For DiffServ, this means expedited forwarding.
- *Video 100010*
 - For ToS, this means IP precedence is set to 4 giving quite high priority (but not as high as the audio precedence). Delay is set to normal, throughput is set to high, and reliability is set to normal.
 - For DiffServ, this means assured forwarding (codepoint 41).
- *Signaling 000000*
- *Admin 000000*

To revert to default values, click **Reset to default**.

Changes to QoS settings require a reboot to take effect.

More information

For more information about QoS, including ToS and DiffServ values, see the relevant RFCs on the Internet Engineering Task Force web site www.ietf.org:

- RFC 791
- RFC 2474
- RFC 2597
- RFC 3246

Related topic

- [Configuring network settings](#)

Configuring the MCU

Displaying and resetting system time	156
Configuring global conference settings	158
Configuring encryption settings	172
Configuring H.323 gatekeeper settings	175
Configuring SIP settings	181
Configuring content settings	183
Media port settings and clustering	185
Upgrading and backing up the MCU	188
Shutting down and restarting the MCU	190
Configuring security settings	191

Displaying and resetting system time

The system date and time for the MCU can be set manually or using the Network Time Protocol (NTP).

To configure Time settings, go to [Settings > Time](#).

Note that changing the time or NTP settings will have an effect on the recorded times in the Call Detail Records log. For more information, refer to [Working with Call Detail Records](#).

System time

The current system date and time is displayed.

If you do not have NTP enabled and need to update the system date and/or time manually, type the new values and click **Change system time**.

NTP

The MCU supports the NTP protocol. Configure the settings using the table below for help, and then click **Update NTP settings**.

The MCU re-synchronizes with the NTP server via NTP every hour.

If there is a firewall between the MCU and the NTP server, configure the firewall to allow NTP traffic to UDP port 123.

If the NTP server is local to Port A or Port B then the MCU will automatically use the appropriate port to communicate with the NTP server. If the NTP server is not local, the MCU will use the port that is configured as the default gateway to communicate with the NTP server, unless a specific IP route to the NTP server's network/IP address is specified. To configure the default gateway or an IP route, go to [Network > Routes](#).

Field	Field description	Usage tips
Enable NTP	If selected, use of the NTP protocol is Enabled on the MCU.	
UTC offset	The offset from the time zone that you are in from Co-ordinated Universal Time (UTC). UTC is in broad terms equivalent to Greenwich Mean Time. The offset allows you to set a local time appropriate to the geographic location of the MCU and/or adjust for daylight saving.	The offset can be -12:59 to 14:59 hours and can be set in the format hh:mm (or -hh:mm for negative offsets) to specify locations that vary from UTC in half hours. For example, for Rangoon which is six and a half hours ahead of UTC, the offset is 6:30. You do not need to enter the minutes for whole hours, so an offset of one hour is 1. You must update the offset manually when the clocks go backwards or forwards: the MCU does not adjust for daylight saving automatically.
NTP host	The IP address or hostname of the server that is acting as the time keeper for the network.	Note that square brackets are mandatory for IPv6 addresses.

Using NTP over NAT (Network Address Translation)

If NAT is used between the MCU and the NTP server, with the MCU on the NAT's local network (and not the NTP server), no extra configuration is required.

If NAT is used between the MCU and the NTP server, with the NTP server on the NAT's local network, then configure the NAT forwarding table to forward all data to UDP port 123 to the NTP server.

Related topics

- [Configuring IP route settings](#)

Configuring global conference settings

You can modify the global conference settings for the MCU choosing by **Settings > Conference**. However, many of these values can be overwritten by other MCU settings, for example individual conference, participant, or endpoint settings.

On this page:

- [Conference settings](#)
- [Advanced settings](#)

Conference settings

Refer to this table for assistance configuring the conference settings. After making any configuration changes, click **Apply changes**.

Field	Field description	Usage tips
Motion / sharpness trade off	<p>Choose the MCU-wide setting for motion/sharpness trade off. The options are:</p> <ul style="list-style-type: none"> ■ <i>Favor motion</i>: the MCU will try and use a high frame rate. That is, the MCU will strongly favor a resolution of at least 25 frames per second ■ <i>Favor sharpness</i>: the MCU will use the highest resolution that is appropriate for what is being viewed ■ <i>Balanced</i>: the MCU will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second) 	<p>The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the endpoint and the MCU. This setting controls how the MCU will negotiate the settings to be used with an endpoint.</p> <p>Note that the Motion/sharpness trade off setting for an individual endpoint will override this global conference setting during calls with that endpoint.</p>
Transmitted video resolutions	<p>Choose the global conference setting for transmitted video resolutions. This setting can be overridden by individual configured endpoint settings.</p>	<p>Retain the default setting (<i>Allow all resolutions</i>) unless you are experiencing problems with the display of certain resolutions by endpoints.</p> <p>Endpoints advertise the resolutions that they are able to display. The MCU then chooses from those advertised resolutions, the resolution that it will use to transmit video. However, some endpoints do not display widescreen resolutions optimally. In these cases, you might want to use this setting to restrict the resolutions available to the MCU.</p> <p>Note that you can configure this setting for individual configured endpoints if you do not need to restrict transmitted video resolutions for all endpoints.</p>

Default bandwidth from MCU	Identifies the network capacity (measured in bits per second) used by the media channels established by the MCU to a single participant.	When the MCU makes a call to an endpoint, the MCU chooses the maximum bandwidth that is allowed to be used for the media channels which comprise that call. This field sets that maximum bandwidth, and is the total bandwidth of the audio, video, and content channels combined. This setting can be overridden by individual endpoints' Preferred bandwidth from MCU values.
Default bandwidth to MCU	Sets the bandwidth that the MCU will advertise to the endpoint when it calls it.	This setting can be overridden by individual endpoints' Preferred bandwidth to MCU values.
Default view family	Determines which layout views (see Customizing layout views) new participants see when connecting to conferences.	Regardless of the family chosen here, participants can cycle through the available families using the far-end camera controls. See Understanding how participants display in layout views .
Use full screen view for two participants	When there are only two participants, each participant will see the other in full-screen view.	If selected, when there are only two participants in a conference, this will apply regardless of which layout was originally chosen for the conference. If you do not select this setting, then the default family view is used with unused panes blank.
Active speaker display	<p>When in a conference, there is generally one participant that the MCU recognizes as the <i>active speaker</i>, notionally the person currently speaking the loudest. This setting determines how the MCU displays that participant in conference views.</p> <ul style="list-style-type: none"> ■ <i>None</i> With this setting, no special action is taken when displaying the active speaker. ■ <i>Red border</i> Displays a red border around the active speaker. ■ <i>Green border</i> Displays a green border around the active speaker. 	Specifically, an active speaker is the participant who has been identified by the MCU as the current loudest speaker, and they are currently speaking. When you choose to have a border display around the active speaker, it will only display when that participant is speaking.
Media port reservation	Determines whether the MCU is operating in <i>Reserved mode</i> (Media port reservation <i>Enabled</i>) or <i>Unreserved mode</i> (Media port reservation <i>Disabled</i>).	Note that if you set this field to <i>Enabled</i> , you will not be able to create ad hoc conferences. See Port reservation modes for additional information.

Audio notifications	Allows various audible in-conference features to be enabled or disabled.	<p>The options are:</p> <ul style="list-style-type: none"> ■ <i>Conference timing</i>: audible messages to indicate when the conference's scheduled end time is approaching. ■ <i>Join and leave indications</i>: audible messages indicating when other participants join and leave the conference. ■ <i>Conference status</i>: audible status messages for example indicating to a participant that he is the only participant in a conference.
Overlaid icons	Allows various in-conference icons to be displayed on participants' endpoints.	<p>Depending on the check boxes that are selected, in-conference icons appear:</p> <ul style="list-style-type: none"> ■ <i>Important participant</i>: a crown icon appears on all participants' endpoints in the pane of the participant that has become important. ■ <i>Unsecured conferences</i>: encrypted participants in a conference where encryption is optional see an icon indicating that there are other participants who are unencrypted. ■ <i>Tunneled camera control</i>: an arrow icon appears on their endpoint when one participant uses the far-end camera control to control another's camera. ■ <i>Layout changes</i>: an icon appears on their endpoint when a participant changes their layout view. ■ <i>Recording indicator</i>: an icon (a red dot) appears near the top left of the conference display to indicate that the conference is being recorded. For the recording indicator to display, the recording must be made by an IP VCR running software version 2.1 or later, and the connection between the IP VCR and the MCU must be using H.323. ■ <i>Audio participants</i>: an icon appears near the top left of the conference display to indicate if there are any audio-only participants. To the right of the icon, the number of such participants will be displayed. If enabled, the icon will only display if there are one or more audio participants. Audio-only participants are participants that cannot be viewed; either the participant's endpoint cannot send video, the MCU has not allocated a video port to the participant, the participant has stopped their video, or the MCU has stopped the video received from the endpoint. ■ <i>Media quality</i>: an icon (video camera with a cross through it) appears when a participant is experiencing high packet loss or if the network link's bandwidth is too low for the type of channel to the MCU that the endpoint has established. <p>Refer to Using in-conference features with video endpoints to see all in-conference icons and their descriptions.</p>

Overlaid text	Allow various in-conference features to be enabled or disabled.	<p>Depending on the check boxes that are selected, in-conference messages appear:</p> <ul style="list-style-type: none"> ■ <i>Conference status</i>: messages appear when the conference's scheduled end time is approaching and when other participants join and leave the conference. Status messages can also be played for example when you are the only participant in a conference ■ <i>Conference timing</i>: a message appears when the conference's scheduled end time is approaching ■ <i>Join and leave indications</i>: messages appear when other participants join and leave the conference ■ <i>Text messages</i>: allows a message sent using the web interface to be displayed on participants' endpoints ■ <i>Content channel text chat</i>: messages that users can send one another via the content channel are displayed on participants' endpoints. Note that this functionality is only available if the web conferencing option (WCO) is activated on your MCU.
Overlaid logo duration	<p>This setting controls for how long (if at all) the Cisco logo is displayed to participants joining a conference. When displayed, the logo appears in the bottom right of a participant's conference display. Choose from:</p> <ul style="list-style-type: none"> ■ <i><never show></i> ■ <i>5 seconds</i> ■ <i>10 seconds</i> ■ <i>1 minute</i> ■ <i><permanent></i> 	
Conference welcome message	Allows you to enter a message that will be seen by participants joining conferences on the MCU. The message is displayed at the bottom of a participant's conference display.	The duration of the message is configured using the Conference welcome message duration control.
Conference welcome message duration	<p>This setting controls for how long (if at all) participants joining a conference will see the conference welcome message. Choose from:</p> <ul style="list-style-type: none"> ■ <i><never show></i> ■ <i>5 seconds</i> ■ <i>10 seconds</i> ■ <i>1 minute</i> ■ <i><permanent></i> 	

Time to show participant names	This setting controls whether (and for how long) participants shown in view panes are accompanied by their supplied name.	The "Conference welcome message" (described above) and any other overlaid textual messages (for instance information on how soon the conference is going to end, or endpoints leaving and joining the conference) will take priority over the displaying of participant names for the duration of those messages.
---------------------------------------	---	---

Advanced settings

You typically only need to modify these advanced settings if you are working with a support engineer or setting up more complicated configurations.

Field	Field description	Usage tips
Audio codecs from MCU	Restricts the MCU's choice of audio codecs to be used for transmitting audio to endpoints.	<p>When communicating with an endpoint, the MCU receives a list of supported audio codecs from the endpoint. The MCU chooses an audio codec from those available, and sends audio data to the endpoint in that format.</p> <p>Note that the Custom codec selection setting for an individual endpoint will override this global conference setting for calls to that endpoint.</p>
Audio codecs to MCU	Determines which audio codecs the MCU advertises to remote endpoints, restricting the endpoints' choice of channels available for sending audio data to the MCU.	Note that the Custom codec selection setting for an individual endpoint will override this global conference setting for calls from that endpoint.
Video codecs from MCU	Restricts the MCU's choice of video codecs to be used for transmitting main video (not content) to endpoints.	<p>This setting only affects main video, not content. The outgoing transcoded content video codec can be selected on a per conference basis. Click here for more information. The outgoing passthrough content video codec cannot be selected. The MCU always advertises support for both H.263+ and H.264.</p> <p>When communicating with an endpoint, the MCU receives a list of supported video codecs from the endpoint. The MCU chooses a video codec from those available, and sends video data to the endpoint in that format.</p> <p>Note that the Custom codec selection setting for an individual endpoint will override this global conference setting for calls to that endpoint.</p>
Video codecs to MCU	Determines which video codecs the MCU advertises to remote endpoints, restricting the endpoints' choice of channels available for sending main video data (not content) to the MCU.	<p>This setting only affects main video, not content. The incoming content video codec cannot be selected. The MCU always advertises support for both H.263+ and H.264.</p> <p>Note that the Custom codec selection setting for an individual endpoint will override this global conference setting for calls from that endpoint.</p>

ClearVision	When enabled, the MCU will upscale video streams from participants who are sending low resolution video with the purpose of making best use of the MCU's HD video capabilities.	<p>The MCU uses intelligent resolution upscaling technology to improve the clarity of low-resolution video. Select this setting to enable it to do so.</p> <p>ClearVision is not available if your MCU is running in Standard definition mode. To configure media port modes, go to Settings > Media ports.</p>
Video transmit size optimization	<p>Allows the MCU to vary the resolution and codec of the video being sent to a remote endpoint within the video channel established to that endpoint. The options are:</p> <ul style="list-style-type: none"> ■ <i>None</i>: Do not allow video size to be changed during transmission ■ <i>Dynamic resolution only</i>: Allow video size to be optimized during transmission ■ <i>Dynamic codec and resolution</i>: Allow video size to be optimized during transmission and/or dynamic codec selection 	<p>With this option enabled, the MCU can, for instance, decide to send CIF video within a 4CIF channel if this will increase the viewed video quality.</p> <p>The circumstances under which decreasing the video resolution can improve the video quality include:</p> <ul style="list-style-type: none"> ■ if the original size of the viewed video is smaller than the outgoing channel ■ if the remote endpoint has used flow control commands to reduce the bandwidth of the MCU video transmission <p>Typically, lowering the resolution means that the MCU can transmit video at a higher frame-rate.</p>
Video resolution selection mode	<p>This setting can be used to influence the choice of outgoing video resolution made by the MCU in certain circumstances.</p> <ul style="list-style-type: none"> ■ <i>Default</i> The MCU will use its normal internal algorithms to dynamically decide which resolution to send in order to maximize the received video quality. ■ <i>Favor 448p</i> The MCU will heavily favor sending 448p or w448p video (resolutions of 576 x 448 and 768 x 448 pixels respectively) to those endpoints that are known to work best with these resolutions. 	You should leave this at <i>Default</i> unless your environment dictates 448p or w448p resolutions only.
Video format	<p>Sets the format for video transmitted by the MCU.</p> <ul style="list-style-type: none"> ■ <i>NTSC</i> The MCU will transmit video at 30 frames per second (or a fraction or multiple of 30, for example: 15fps or 60fps) ■ <i>PAL</i> The MCU will transmit video at 25 frames per second (or a fraction or multiple of 25, for example: 12.5fps or 50fps) 	<p>This option should be set to match your endpoints' video configuration. If you set this incorrectly, the smoothness of the video both to and from the endpoints might suffer.</p> <p>NTSC is typically used in North America, while PAL is typically used in the UK and Europe.</p>

Maximum transmitted video packet size	Sets the maximum payload size (in bytes) of the packets sent by the MCU for outgoing video streams (from the MCU to connected video endpoints).	<p>We recommend that you use the default setting (1400 bytes) wherever possible. If you need to reduce the maximum payload size, we recommend a value of at least 1000 bytes; a maximum payload size that is too low reduces the overall bandwidth efficiency and may impact performance.</p> <p>Video streams generally contain packets of different lengths. This parameter only sets the <i>maximum</i> size of a transmitted network datagram. The MCU optimally splits the video stream into packets of this size or smaller. Thus, most transmitted packets will not reach this maximum size.</p>
Interlaced video optimization	Controls whether the MCU restricts video resolutions in order to reduce the effect of interlacing artifacts.	You should only enable this option if you are seeing video interlacing artifacts or on the advice of Customer support. Note that all resolution restrictions imposed by this setting apply only to video being sent from endpoints to the MCU.
Video receive bit rate optimization	Enables the MCU to send bandwidth control messages to optimize the video bandwidth being used.	<p>The MCU can send these messages to endpoints requesting that the bandwidth of the video that they are sending be decreased or increased, up to the maximum bandwidth of the channel.</p> <p>If the participant is very prominent, then the MCU will ask the endpoint to send video at a high bandwidth. If the participant is not being viewed at all (or only being viewed in very small view panes), the MCU will request that the video is sent at a lower rate to conserve network bandwidth.</p> <p>Note: When an HD-capable MCU is in one of the HD, HD+, or Full HD modes, this option is automatically enabled.</p> <p>On the MCU 4500 Series and the MCU MSE 8510, the optimizations are enabled in the HD modes but the control to disable them is deactivated; however, on the MCU 5300 Series, you can disable the optimizations when the MCU is in one of the HD modes. For more information, refer to Configuring media port settings.</p>

Flow control on video errors	Enables the MCU to request that the endpoint send lower speed video if it fails to receive all the packets which comprise the far end's video stream.	<p>The MCU can send these messages to endpoints requesting that the bandwidth of the video that they are sending be decreased based on the quality of video received by the MCU.</p> <p>If there is a bandwidth limitation in the path between the endpoint and the MCU, it is better for the MCU to receive every packet of a lower rate stream than to miss some packets of a higher rate stream.</p> <hr/> <p>Note: When an HD-capable MCU is in one of the HD, HD+, or Full HD modes, this option is automatically enabled.</p> <p>On the MCU 4500 Series and the MCU MSE 8510, Flow control on video errors is enabled in the HD modes but the control to disable it is deactivated; however, on the MCU 5300 Series, you can disable Flow control on video errors when the MCU is in one of the HD modes. For more information, refer to Configuring media port settings.</p>
Don't see yourself in small panes	Prevents the MCU from showing conference participants their own video in small panes of variable-sized pane views (and in conferences with equal-sized panes).	If this option is set, then a participant will never appear in a small pane (self-view), even if there is a free small pane available. They may still appear in larger panes, however, for example if the view focus is manually changed to show their video. See Understanding how participants display in layout views for more details.
Don't duplicate in small panes	Prevents the MCU from duplicating large-pane participants in small panes.	When using a conference view with some large and some small panes, the MCU will typically duplicate in a small pane the video of a participant shown in a large pane. This is done to minimize the switching of small panes in response to changes of participant focus in the large pane. If you would prefer not to duplicate participants in small panes in this way, select this option. For more details of view layouts, see Understanding how participants display in layout views .
Automatically make content channel important	Any new content channel in a conference will be treated as important and displayed prominently to all participants who see the content channel in their conference layout.	<p>When this setting is enabled, any endpoint successfully contributing content to a conference is immediately treated as important. This has the same affect as using the 'crown' icon in the content channel row of a conference's Participant list page.</p> <p>An administrator can remove the importance from the content channel at any time in the conference.</p> <p>This setting does not affect participants who view the content channel independently from their conference panes (for example, those viewing the content channel on a separate video screen).</p> <p>This setting will not affect those participants using pane placement. Participants using pane placement who have not allocated a pane to the content channel, will not see the content channel even if it is 'important'.</p>

Loudest speaker pane placement behavior	<p>When pane placement is in use, this option affects the potential duplication of participants that are specifically placed in view panes with view panes configured to show the conference's current active speaker.</p> <ul style="list-style-type: none"> ■ <i>Never duplicate placed participants</i> A pane set to show the loudest speaker will never show a participant that is specifically configured to be displayed in another layout pane. If another layout pane has been configured to show the participant which is the current active speaker, panes set to show the loudest speaker will instead show the conference's previous loudest speaker. If you never want a pane that is set to <i><loudest speaker></i> to duplicate a participant shown in another layout pane, choose this setting. ■ <i>Allow duplication of placed participants in small panes only</i> This is the default setting; panes configured to show the loudest speaker will be able to show participants that are configured to be displayed in one or more small panes for that layout, but not those shown in big panes. This is most appropriate when using layouts with more than one big pane, in order to make best use of the screen area. ■ <i>Allow duplication of placed participants in any pane</i> Panes set to <i><loudest speaker></i> will always show the current active speaker for a conference, whether or not any other layout panes have been specifically configured to show that participant. 	For more details of view layouts, see Understanding how participants display in layout views .
Pane rolling interval	When pane placement is in use, this option determines how often panes set to "rolling" change which participant they are showing.	For more details of view layouts, see Understanding how participants display in layout views , and Using pane placement [p.66] .
Maximum height of participant name within pane	Defines the maximum height of the participant's name as a percentage of the pane height.	Enter a percentage value. e.g. 20 will prevent the text from taking more than 20% of the pane height. The setting is particular to small panes; it does not scale the text beyond the text's own maximum size.

Voice switching sensitivity	Determines how easy it is for a participant to replace the active speaker for a conference based on how loudly they are speaking.	A value of 0 means that it is very difficult for the active speaker to be replaced; a value of 100 means the active speaker can be replaced very easily.
Incoming calls to unknown conferences or auto attendants	<p>Sets the default action when endpoints call into the MCU using an unknown E.164 number, conference number, or auto attendant. In other words, a number that does not correspond to any configured conference.</p> <ul style="list-style-type: none"> ■ <i>Default auto attendant</i> The endpoint will enter the default auto attendant from which they may join existing conferences or potentially create a new conference (see Using an auto attendant). This behavior is the same as if the endpoint had called the MCU using its IP address rather than a number. ■ <i>Disconnect caller</i> Endpoints are not allowed to call unknown conference or auto attendant numbers, and the call will be terminated. ■ <i>Create new ad hoc conference</i> A new conference will be created with the number called as its numeric identifier. The endpoint automatically joins this new conference. This option is not available if the MCU is in port reservation mode. 	This option can make it easier for callers to create ad hoc conferences if <i>Create new ad hoc conference</i> is selected. If you do not want callers to be able to create conferences in this way, select one of the other options.

Failed preconfigured participants redial behavior	<p>Defines whether and how the MCU will redial preconfigured endpoints if the connection fails:</p> <ul style="list-style-type: none">■ <i>Never redial</i> The MCU never attempts to redial a failed connection to a preconfigured participant.■ <i>Redial until connected</i> The MCU redials the preconfigured participant if it fails unexpectedly when first establishing a connection; the MCU never retries the connection if it fails after being established.■ <i>Redial on unexpected disconnection</i> The MCU redials preconfigured participants on any unexpected disconnection, whether it occurs while first being established or at any point thereafter. It does not attempt to redial if the participant deliberately ends the connection. <hr/> <p>Note: A deliberate disconnection, if it is not correctly signaled by the endpoint, may be interpreted as unexpected. If you experience this, reduce the call persistence behavior for the affected endpoint.</p> <hr/> ■ <i>Redial on any disconnection</i> The MCU redials the preconfigured participant when the connection closes, irrespective of whether the call fails or is deliberately ended by the participant.	<p>This setting defines the box-wide behavior for conferences dialing preconfigured participants. The setting may be overridden by the corresponding setting on individual preconfigured endpoints.</p> <p>Although this box-wide setting applies only to preconfigured endpoints, the equivalent option is provided when you are inviting ad hoc participants.</p>
--	---	---

Redial limit	Enables or disables the redial limit.	<p>The redial limit allows the MCU to stop trying to reconnect a failed call. When the limit is enabled, the MCU will attempt to reconnect up to ten times: once immediately after the connection failure; four times at one minute intervals thereafter, and once every five minutes for a further five attempts.</p> <p>When the redial limit is disabled, the MCU continues retrying - once every five minutes - after those first ten attempts. It will do this until the connection is made. If the connection is never made, the MCU continues retrying until either the conference or the participant is destroyed.</p> <p>The redial pattern has an initial delay when the redial behavior is set to <i>Redial on any disconnection</i>. With that setting, the MCU does not immediately redial after a deliberate disconnection - it waits 30 seconds.</p> <p>This setting enables or disables the redial limit for all conferences when they are redialing preconfigured participants. The setting may be overridden by the corresponding setting on individual preconfigured or ad hoc endpoints.</p>
Conferences remain locked when empty	When enabled, conferences remain locked when all participants leave the conference.	Without this option selected, when the final participant leaves a locked conference, the MCU unlocks that conference.
Use conference name as caller ID	If enabled, when the MCU is calling out to an endpoint, the caller ID that the endpoint will see is the conference name.	Without this option selected, the caller ID is the name of the MCU. This setting applies to both H.323 and SIP endpoints.
Require H.323 gatekeeper callers to enter PIN	Instructs the MCU to request conference participants dialing into protected conferences using an E.164 number via an H.323 gatekeeper to enter a PIN before they may join the conference.	<p>You may want participants joining a conference via a gatekeeper not to need to enter a PIN, even for protected conferences. If this is the case, do not set this option. If you want conferences to be protected, regardless of how participants connect, ensure you set this option.</p> <p>When this option is set, participants calling into a protected conference will be presented with PIN-entry screen instead of the normal conference view. The option has no effect for conferences with no PIN set.</p>
Require a PIN for ad hoc conferences	If this option is checked, a participant creating an ad hoc conference must enter a PIN for that conference. The MCU will not create the conference until the participant enters a PIN.	<p>When a PIN is required for ad hoc conferences, the auto attendant will wait forever for the participant to enter a PIN.</p> <p>This option is required in some highly secure environments.</p>
Minimum required PIN length for ad hoc conferences	The minimum number of digits required for a PIN.	This field is only available if Require a PIN for ad hoc conferences is selected. This forces a participant who is creating an ad hoc conference to protect it with a PIN with at least this number of digits.

Time to wait when setting up ad hoc conference PIN	<p>The timeout setting for a participant entering a PIN for an ad hoc conference that they are currently creating:</p> <ul style="list-style-type: none"> ■ <i><never configure PIN></i> Participants will never be prompted to enter a PIN when creating an ad hoc conference. ■ <i>10 seconds, 30 seconds, 1 minute</i> Participants will be prompted for a PIN when creating an ad hoc conference. If the participant does not enter a PIN during the configured time period, the conference will be created without a PIN. ■ <i><wait forever></i> Participants will be prompted for a PIN when creating an ad hoc conference. They must either enter a PIN to create an ad hoc conference with a PIN or press the hash/pound key (#) to create the conference without a PIN. 	<p>This global setting may be useful where participants creating ad hoc conferences rarely need to configure a PIN.</p> <p>This field is unavailable when Require a PIN for ad hoc conferences is selected. When a PIN is required for ad hoc conferences, the auto attendant will wait forever for the participant to enter a PIN.</p>
Advertise out of band DTMF	<p>If this option is checked, the MCU advertises the ability to receive out of band DTMF.</p> <p>If this option is checked, endpoints are allowed to send out of band DTMF. If this option is unselected, the MCU will not advertise the ability to accept out of band DTMF and endpoints will instead be forced to use in band DTMF.</p>	<p>Prior to release 4.1, the MCU always advertised to endpoints the ability to receive out of band DTMF tones. Now you can disable this functionality if required. If you unselect this option, endpoints are forced to send DTMF in band (in the audio channel). This means that the MCU can pass DTMF tones on to an audio conferencing bridge or to another MCU where a conference is cascaded.</p>
Enable resolutions above CIF to be sent to Cisco Unified CM	<p>If this option is checked, the MCU will send resolutions higher than CIF to Cisco Unified Communications Manager.</p>	<p>Prior to Release 4.2 of the MCU, CIF was sent to Cisco Unified Communications Manager registered endpoints.</p>
Enable transmission of 60fps	<p>Enables the MCU to send video at 60 frames per second (fps). Note that the MCU will only send 60fps video to endpoints that it knows are capable of receiving video at that frame rate. This feature is not available on the MCU 4200 Series products.</p>	<p>The <i>Motion / sharpness tradeoff</i> option in Conference settings above should be set to <i>Favor motion</i>.</p>
Disconnect inactive calls	<p>Enable to ensure the MCU disconnects a call when it detects that an endpoint stops sending media for a period of more than 30 seconds.</p>	

Related topics

- [Customizing conference layout views](#)
- [Displaying conference lists](#)
- [Using in-conference features with video endpoints](#)

Configuring encryption settings

You can configure the MCU to encrypt connections to and from H.323 and SIP endpoints.

The encryption technology that the MCU uses for encryption to and from H.323 endpoints is Advanced Encryption Standard (AES).

The encryption technology that the MCU uses for encryption to and from SIP endpoints is Secure Real-time Transport Protocol (SRTP).

To use encryption, you must have the Encryption feature key present on the MCU. For information about installing feature keys, refer to [Upgrading the firmware](#). To access encryption settings, go to **Settings > Encryption**.

Encryption is used when both devices in a call agree to use encryption; by default if one of the devices cannot use encryption (for example if a SIP endpoint does not support SRTP), the MCU will allow the call to be unencrypted, unless the conference configuration dictates that encryption is *Required*. Where encryption is required, calls that cannot use encryption will not be allowed.

When encryption is in use to and from H.323 endpoints, the MCU will encrypt audio, video, and content media. It does not encrypt control or authentication information.

When encryption is in use to and from SIP endpoints, the MCU will encrypt audio and video media using SRTP. Control or authentication information can also be encrypted using TLS. For more information refer to [Using encryption with SIP](#), below.

You can:

- configure the MCU to advertise its ability to encrypt connections, such that it will use encryption if an H.323 endpoint can use AES encryption.
- configure the MCU to advertise its ability to encrypt connections, such that it will use encryption if a SIP endpoint can use SRTP encryption.
- configure the MCU so that the default encryption option for new conferences is either *Optional* or *Required*. Be aware that anyone creating a new conference will be able to set the encryption setting for the conference to either *Optional* or *Required*.
- force new ad hoc conferences to use encryption (by correctly configuring the ad hoc conference template, see [Using conference templates](#)).

Note that using encryption does not affect the number of ports that are available on the MCU.

Note that the MCU will not show thumbnail previews on the **Conference participant** page if encryption is required for a conference. If you have the **Show thumbnail images** option selected on the **Settings > User interface** page, thumbnail previews will be shown for conferences where encryption is optional and there are encrypted participants.

Refer to this table for assistance configuring the encryption settings. After making any configuration changes, click **Apply changes**.

Field	Field description	Usage tips
-------	-------------------	------------

Encryption status	Whether the MCU is able to use encryption or not.	When encryption status is <i>Enabled</i> , the MCU advertises itself as being able to use encryption and will use encryption if required to do so by an endpoint. If this setting is <i>Enabled</i> , you can enable or disable the use of encryption on a per-conference basis. If this setting is <i>Disabled</i> , no conference will be able to use encryption.
SRTP encryption	Select the setting for media encryption for SIP calls: <ul style="list-style-type: none"> ■ <i>All transports</i>: If encryption is used for a call, the media will be encrypted using SRTP regardless of transport mechanism used for call control messages. ■ <i>Secure transports (TLS) only</i>: If encryption is used for a call, the media will only be encrypted in calls that are set up using TLS. ■ <i>Disabled</i>: SRTP will not be used for any calls. The MCU will not encrypt media for SIP calls. 	For more information refer to Using encryption with SIP , below. When disabled, the MCU will not advertise that it is able to encrypt using SRTP. It is only necessary to disable SRTP if it is causing problems.

Using encryption with SIP

The MCU supports the use of encryption with SIP. When encryption is in use with SIP, the audio and video media are encrypted using Secure Real-time Transport Protocol (SRTP). When using SRTP, the default mechanism for exchanging keys is Session Description Protocol Security Description (SDS). SDS exchanges keys in clear text, so it is a good idea to use SRTP in conjunction with a secure transport for call control messages. You can configure the MCU to also use Transport Layer Security (TLS) which is a secure transport mechanism that can be used for SIP call control messages.

Using TLS for call setup is not sufficient for the call to be considered encrypted such that it can participate in a conference which requires encryption. Where encryption is required in the conference configuration, a SIP call must use SRTP.

To configure the MCU to use SRTP to encrypt media in calls that are set up using TLS:

1. You must have the encryption feature key installed on your MCU.
2. Go to **Settings > Encryption** and set:
 - **Encryption status** to *Enabled*.
 - **SRTP encryption** to *Secure transports (TLS) only*.
3. Go to **Settings > SIP** and set **Outgoing transport** to *TLS*. To allow the MCU to accept incoming calls that use TLS, go to **Network > Services** and ensure that *Encrypted SIP (TLS)* is selected.

Note: It is possible to make encryption the default on newly created conferences by setting the **Encryption** field on the conference template settings to *Required*. Go to **Conferences > Templates**.

Related topics

- [Adding and updating conferences](#)
- [Upgrading the firmware](#)

Configuring H.323 gatekeeper settings

To configure gatekeeper settings, go to [Settings > H.323](#).

You can configure the MCU to use a gatekeeper, which can make it easier for end-users to join conferences using directory numbers rather than requiring them to know the IP address or host name of the MCU. The MCU can register up to 100 IDs with the gatekeeper; these IDs comprise conferences' **Numeric IDs**, the **MCU service prefix**, and the **H.323 ID**. If you need to register more than 100 IDs, use a **prefix for MCU registrations** to route calls to the MCU, rather than registering individual conferences with the gatekeeper. The use of prefixes is described further in the table below.

On this page:

- [Gatekeeper settings](#)
- [Gatekeeper status](#)

Gatekeeper settings

Refer to this table for assistance configuring the gatekeeper settings. After making any configuration changes, click **Apply changes**.

Field	Field description	Usage tips
H.323 gatekeeper usage	Enables the MCU to use an H.323 gatekeeper for registration of numeric identifiers for its conferences and/or auto attendants.	<p>When set to <i>Disabled</i> then no gatekeeper registrations are attempted (and existing registrations are torn down), regardless of other gatekeeper or per-conference settings.</p> <p>When set to <i>Enabled</i> registrations with the gatekeeper are attempted, and the gatekeeper is contacted for incoming and outgoing calls. If the gatekeeper does not respond, calls are still connected if possible. When set to <i>Required</i> registrations with the gatekeeper are attempted but calls are not connected if the gatekeeper cannot be contacted.</p>
H.323 gatekeeper address	Identifies the network address of the gatekeeper to which MCU registrations should be made.	<p>This can be specified either as a host name or as an IP address.</p> <p>This field will have no effect if H.323 Gatekeeper usage (see above) is set to <i>Disabled</i>.</p>
Gatekeeper registration type	Controls how the MCU identifies itself when registering with its configured gatekeeper.	<p>Cisco recommends that you use the <i>Terminal / gateway</i> option unless you are using a service prefix (in this case, use <i>Gateway</i>). Only use a different option if you are:</p> <ul style="list-style-type: none"> ■ having specific problems ■ using the VCS as a gatekeeper (with or without a service prefix), in which case use <i>MCU (standard)</i> ■ using the Cisco Gatekeeper (with or without a service prefix), in which case use <i>Gateway (Cisco GK compatible)</i> ■ using the VCON MXM Gatekeeper (with or without a service prefix), in which case use <i>MCU (compatible)</i> <p>Refer to the Knowledge Base in the Support section of the web site for more details about interoperability with gatekeepers.</p>

Ethernet port association	Whether a call involves consultation with the configured gatekeeper also depends on the <i>Port A</i> and <i>Port B</i> settings. For all incoming calls, and outgoing calls dialed by IP address rather than by E.164 phone number, the gatekeeper will be used to validate the connection only if the network port over which the connection is made is selected here.	<p>The check boxes that are available here depend on which interfaces are enabled. Check the boxes of the interface(s) and IP version(s) that you want to be registered to the gatekeeper.</p> <p>In the case of an incoming call to an address of the form <i><numeric ID>@<domain></i>, the admission query will use just the <i><numeric ID></i> to validate the connection.</p>
(Mandatory) H.323 ID to register	Specifies an identifier that the MCU can use to register itself with the H.323 gatekeeper.	<p>Before the MCU can register any IDs with the H.323 gatekeeper, it must make an MCU-wide registration.</p> <p>This field is required for the gatekeeper registration.</p> <p>This will have no effect if H.323 gatekeeper usage is disabled.</p>
Use password	If the configured gatekeeper required password authentication from registrants, select the Use password check box and type the password.	Note that where password authentication is used, the <i>(Mandatory) H.323 ID to register</i> will be used as the username.
Prefix for MCU registrations	Specifies an optional group of digits that are added to the beginning of each conference or auto attendant's numeric identifier before registering it with the H.323 gatekeeper.	<p>Conferences and auto attendants registered with a gatekeeper have a numeric identifier. The numeric identifier is a unique sequence of digits entered from a video-conferencing endpoint to connect directly to the conference or auto attendant. This eliminates the need for users to navigate additional menus or to know the IP address of the MCU.</p> <p>To usefully partition the dialing space, you might need to ensure that all registrations from a single MCU start with the same sequence of digits.</p> <p>Using registration prefixes also can benefit large-scale dial plan changes. For example, you can change all MCU registrations to begin with "121" instead of "11" by changing a single MCU configuration field rather than individually amending every conference or auto attendant's associated numeric identifier.</p> <p>If H.323 gatekeeper usage is disabled, this field will have no effect.</p> <p>Note that if you are also intending to use the MCU service prefix (see below), Cisco recommends that you set both prefixes to the same number.</p>

MCU service prefix	<p>If required, specify a group of digits which the H.323 gatekeeper may use to identify calls to be routed to the MCU.</p>	<p>This field is optional. If set, users dialing any number beginning with this prefix will have their call directed to the MCU. This might be useful if you want to create conferences in response to unknown E.164 numbers.</p> <p>Any numbers following the prefix will be identified by the MCU as a conference or auto attendant number. For example, if a conference has Numeric ID "3333" and you have set the service prefix to be "121", then a user dialing "1213333" will be connected to that conference.</p> <p>This field will have no effect if H.323 gatekeeper usage is disabled.</p> <p>Note that if you are also intending to use the Prefix for MCU registrations (see above), Cisco recommends that you set both prefixes to the same number.</p> <p>If the MCU is unable to match a call to a conference or auto attendant, the action for Incoming calls to unknown E.164 number will be applied. This is a setting on the Settings > Conferences page (see Configuring global conference settings). This action can be set to <i>Create new ad hoc conference</i>.</p>
Allow numeric ID registration for conferences	<p>This setting controls whether conferences' configured numeric IDs are allowed to be registered with the gatekeeper.</p> <p>This setting is the global control that <i>allows</i> or <i>disallows</i> conferences to be registered with the gatekeeper.</p> <p>Individual conferences will be registered or not depending on the per-conference Numeric ID registration setting which is on the Add conference page for scheduled conferences and for ad hoc conferences it is in the ad hoc conference template.</p>	<p>This would normally be <i>Enabled</i>; by setting it to <i>Disabled</i>, an administrator can prevent users from adding to the set of IDs registered with the configured gatekeeper, even if those users enable the gatekeeper Numeric ID registration setting for conferences they control. This may be desired when working with certain types of H.323 gatekeeper whose behavior in some modes is to disconnect active calls when the set of registered IDs changes.</p> <p>This setting affects both the registration of numeric IDs configured for scheduled conferences and the registration of ad hoc conferences.</p> <p>This field will have no effect if H.323 Gatekeeper usage is set to <i>Disabled</i>.</p>

Send resource availability indications	<p>Select this option if you want the MCU to inform the gatekeeper about its availability or non-availability. This information will be used by the gatekeeper when it is selecting where to place ad hoc conferences.</p> <p>Only use this option where multiple MCUs are registered with the <i>same</i> MCU service prefix on the same gatekeeper.</p> <p>If you select this option, you must configure the thresholds for conferences and/or video ports.</p> <p>Thresholds:</p> <ul style="list-style-type: none"> ■ Conferences: Enter any number of conferences between 0 and 200. (A value of 0 will mean that the MCU will always indicate 'unavailable'.) ■ Video ports: Enter a number between 0 and the number of video ports on your MCU; for example, on an MCU 4205, there are 12 video ports, so enter a number between 0 and 12. (A value of 0 will mean that the MCU will always indicate 'unavailable'.) 	<p>The ability of the MCU to send resource availability messages is useful in a network where there are multiple MCUs or where there are several media blades in an MSE.</p> <p>In an environment with multiple conferencing devices registered with the same gatekeeper, that gatekeeper should favor devices in the available state when choosing where to place new calls.</p> <p>For example, when one MCU sends the gatekeeper a message indicating that it is not available, the gatekeeper will then attempt to use a different MCU for new ad hoc conferences.</p> <p>Resource availability indications are most useful where the thresholds are configured such that the MCU informs the gatekeeper that it is unavailable when its resources are nearly used up.</p> <p>Conferences without any active participants do not contribute to the conference count; any video port in use is added to the video port count.</p> <p>When either threshold is equaled or exceeded, the MCU sends a message to indicate that it is not available; when the resource usage drops such that neither threshold is equaled or exceeded, the MCU sends a message indicating that it is available.</p> <p>You might choose to only configure one of the thresholds. You are probably aware of how your video conferencing resources tend to be used by participants and you need to consider this when configuring the thresholds. For example, you could have four people who have each started an ad hoc conference; you might know that it is usual for such conferences to end up having ten participants. In this case, on a 40-port MCU you could set the conference threshold to 4 to indicate that it will be out-of-resources very soon. On the same MCU if you set the video port threshold to 35 and left the conference threshold empty, another four or more people could begin ad hoc conferences on this MCU before the participants expected in the original four conferences had dialed in.</p> <p>When switching from Standard to High Definition mode on an HD-capable MCU, if the <i>Video ports</i> threshold is higher than the number of available video ports, the MCU will change the threshold value down to the number of video ports.</p>
---	---	---

Gatekeeper status

The MCU also displays brief status information about its registrations with the configured gatekeeper.

To display a complete list of all IDs that the MCU is attempting to register with the configured H.323 gatekeeper, click the [details](#) link in the **Number of active registrations** row of the gatekeeper status table; this takes you to the [Active registrations](#) page.

Field	Field description	Usage tips
-------	-------------------	------------

H.323 gatekeeper status	Displays the IP address of the gatekeeper currently being used by the MCU.	<p>This information might be useful if the gatekeeper has been specified with a host name rather than with an IP address.</p> <p>If the MCU has been unable to reach the configured gatekeeper and has instead registered with an alternate gatekeeper, the status displayed here will be "registered with alternate gatekeeper <IP address>".</p>
Registered address	Displays the local IP address and port number that the MCU has registered with the gatekeeper.	This information might be useful if the MCU has more than one IP address, for instance if both Ethernet interfaces are in use.
Alternate gatekeepers available	Displays the number of 'alternate' gatekeepers configured on the H.323 gatekeeper. This figure comes from the gatekeeper itself; if there are any 'alternate' gatekeepers configured, the gatekeeper tells the MCU their IP addresses.	<p>Where the configured gatekeeper has told the MCU about any configured 'alternate' gatekeepers and if the MCU loses contact with the configured gatekeeper, the MCU will attempt to register with each of the 'alternates' in turn. If none of the 'alternate' gatekeepers responds, the MCU will report that the registration has failed.</p> <p>If the MCU successfully registers with an 'alternate' gatekeeper:</p> <ul style="list-style-type: none"> ■ the H.323 gatekeeper status will indicate that registration is with an 'alternate' ■ the list of 'alternates' received from the new gatekeeper will replace the previous list ■ the MCU will only revert back to the original gatekeeper if the 'alternate' fails and only if the original gatekeeper is configured as an 'alternate' on the current gatekeeper's list of 'alternates' <p>Note that if the MCU registers with an 'alternate' that does not itself supply a list of 'alternates', the MCU will retain the original list and if it loses contact with the current gatekeeper, each one will be attempted from the top again as before.</p>
Resource availability status	Displays whether the gatekeeper is configured to send resource availability indications and if it is, it displays the current state of the resource availability status of the MCU.	<p>The possible statuses are:</p> <ul style="list-style-type: none"> ■ <i>resources available</i> ■ <i>resources unavailable</i> ■ <i><indications not configured></i>
Number of active registrations	Displays the number of E.164 numbers plus H.323 IDs plus prefixes that the MCU has registered with the gatekeeper.	<p>It also shows how many registrations are in progress but are not fully registered yet.</p> <p>Full information on the gatekeeper registrations being made by the MCU can be seen by clicking on details; this takes you to the Active registrations page.</p>
H.323 ID registration	Displays the identifier that the MCU has used to register itself with the H.323 gatekeeper.	For more information about the H.323 ID, refer to the table above.
MCU service prefix	Displays the identifier that the gatekeeper has registered for calls to be routed to the MCU.	For more information about this prefix, refer to the table above.

Related topics

- Displaying the built-in gatekeeper registration list
- [Displaying active gatekeeper registrations](#)

Displaying active gatekeeper registrations

To display a complete list of all IDs that the MCU is attempting to register with the configured H.323 gatekeeper, go to **Settings > H.323** and click **details**, shown next to the **Number of active registrations** status entry. You are taken to the **Active registrations** page. This page shows the complete set of IDs that the MCU is attempting to register with the configured H.323 gatekeeper, and includes the H.323 ID, prefixes, and specific E.164 number registrations for active conferences and configured auto attendants.

Filters

You can configure filters so that only specific registrations are shown in the list. This may help you to find a registration whose number or name you know if the list is very long.

The filtered registration list is automatically updated when you change the ID and Details filters; to stop filtering the list either delete the filters or click **Clear filters**. If both the ID filter and the Details filter are defined, the registration list will show only those entries which match both filters.

Field	Field description	Usage tips
ID filter	Type the ID, or a part of the ID for which you want to see details.	The filtered registration list is automatically updated when you change the ID filter.
Details filter	Type the text, or a part of the text that will appear in the "Details" column of the Registrations table. For example, type 'Conference' to filter the registrations to show all conferences that the MCU is attempting to register with the gatekeeper.	The filtered registration list is automatically updated when you change the Details filter. Applying a filter will filter all registrations and display any that match, even if those registrations are not on the page currently displayed.

Registration list

The registration list shows, for each registered ID, the type of that ID (H.323 ID, prefix or E.164 number), the object it relates to, and the status of that registration. If you want to modify or remove a specific registered ID, click on the link in its **Details** column to be taken to the relevant configuration page.

Related topics

- [Configuring H.323 gatekeeper settings](#)

Configuring SIP settings

The SIP settings page allows you to control the MCU SIP settings.

To access this information, go to [Settings > SIP](#).

To update the defaults, or change the configuration at any time, edit the fields referring to the table below for details and click **Apply changes**.

Field	Field description	Usage tips
Outbound call configuration	<p>This setting affects outgoing SIP calls and registration. The options are:</p> <p><i>Use registrar</i> enables SIP registration and routes outbound SIP calls via the registrar.</p> <p><i>Use trunk</i> disables SIP registration and tears down existing registrations. Routes outbound calls to the trunk destination, e.g. VCS or CUCM.</p> <p><i>Call direct</i> disables SIP registration and tears down existing registrations. Outbound SIP calls go directly (not via registrar or trunk).</p>	<p><i>Use registrar:</i></p> <ul style="list-style-type: none"> ■ Enables SIP registrations, on a system-wide basis, with the registrar address you provide. ■ Outgoing calls always go via registrar. ■ An outbound call will fail if the registrar does not respond. ■ Incoming calls should come through the registrar and will fail if the registrar does not respond. <p><i>Use trunk:</i></p> <ul style="list-style-type: none"> ■ Directs outbound SIP calls via the trunk to the SIP server address you provide. ■ The SIP server, for example Cisco Video Communication Server (VCS) or Cisco Unified Call Manager (CUCM), is responsible for the onward routing of outbound SIP calls from the MCU. ■ If the dialed SIP address does not have a domain then Outbound domain gets appended if present, otherwise Outbound address gets appended. <p><i>Call direct:</i></p> <ul style="list-style-type: none"> ■ The MCU will connect SIP calls directly if possible. It does not use the Outbound address or Outbound domain parameters. ■ The MCU does not attempt to use either the registrar or trunk.
Outbound address	The hostname or IP address of the SIP registrar or trunk destination.	The MCU ignores this field if Outbound call configuration is set to <i>Call direct</i> .
Outbound domain	The domain of the SIP registrar or trunk destination.	<p>The MCU ignores this field if Outbound call configuration is set to <i>Call direct</i>.</p> <p>The MCU uses this value in the following ways:</p> <ul style="list-style-type: none"> ■ username@outbounddomain to register a user with a SIP registrar (if SIP registration is enabled) ■ numericId@outbounddomain to register a conference's numeric ID with a SIP registrar (if conference has SIP registration enabled) ■ Any outbound SIP calls where the supplied address does not contain an @ symbol. <p>If you do not specify an outbound domain, the MCU uses the outbound address instead.</p>

Username	<p>The MCU uses this name if it registers with a SIP registrar.</p> <p>The MCU uses this name to authenticate with the SIP device (registrar, trunk destination, or endpoint) if that device requires authentication.</p>	<p>The MCU will use this name to register itself with the SIP registrar if you have enabled SIP registration. It will not register itself if you do not provide this, but it will still be able to register individual conferences (assuming they are enabled to register and have numeric IDs).</p> <p>If a conference does not have a numeric ID, then it cannot register. Calls out from such a conference will appear to come from the MCU's own SIP registration (this_username@outbounddomain). It is impossible for a participant to call into such a conference because it does not have a numeric ID.</p> <p>If you enter a full URI here (e.g. host@domain), then the MCU will ignore the Outbound domain setting.</p>
Password	<p>The MCU uses this password to authenticate with the SIP device (registrar, trunk destination, or endpoint) if that device requires authentication.</p>	<p>The SIP destination may not require authentication; if it does, you need to configure it to accept a log in from this username and password combination.</p>
Outbound transport	<p>Select the protocol that the MCU will use for outbound calls (and registrations, if enabled).</p> <p>One of <i>TCP</i>, <i>UDP</i>, or <i>TLS</i>.</p>	<p>The MCU uses this protocol for communicating with the SIP registrar or trunk destination.</p> <p>If you have the encryption feature key installed and want to encrypt signaling, select <i>TLS</i>.</p> <p>The MCU accepts incoming connections on whichever protocol the connection uses (TCP, UDP or TLS), and will respond using the same protocol, irrespective of this Outbound transport setting. Make sure that you enable those services on the Network > Services page.</p>
Allow numeric ID registration for conferences	<p>This field controls whether any conferences' configured numeric IDs are allowed to be registered with the registrar.</p> <p>This setting is the global control that <i>allows</i> or <i>disallows</i> conferences to be registered with the SIP registrar.</p> <p>Individual conferences will be registered or not depending on the per-conference Numeric ID registration setting which is on the Add conference page for scheduled conferences and for ad hoc conferences it is in the ad hoc conference template.</p>	<p>This would normally be <i>Enabled</i>; by setting it to <i>Disabled</i>, an administrator can prevent users from adding to the set of IDs registered with the configured registrar, even if those users enable the registrar Numeric ID registration setting for conferences they control. This may be desired when working with certain types of SIP registrars whose behavior in some modes is to disconnect active calls when the set of registered IDs changes.</p> <p>This setting affects both the registration of numeric IDs configured for scheduled conferences and the registration of the numeric IDs of ad hoc conferences.</p> <p>This field will have no effect if SIP registrar usage is set to <i>Disabled</i>.</p>

Related topics

- [SIP: Advanced](#)
- [Configuring SIP endpoints](#)
- [Configuring global conference settings](#)

Configuring content settings

The content settings affect the behavior of the MCU with regard to H.239 and BFCP (Binary Floor Control Protocol).

H.239 is the protocol that allows for an additional video channel (known as the content channel) alongside the main video channel in a video-conferencing call that uses H.323; BFCP is a protocol that allows for an additional video channel (known as the content channel) alongside the main video channel in a video-conferencing call that uses SIP.

For example, a conference participant may want to contribute a slide presentation from a laptop within a video conference.

For more information about content support in conferences, refer to [Content channel video support](#).

To access these settings, choose **Settings > Content**.

Refer to this table for assistance configuring the content settings. After making any configuration changes, click **Apply changes**.

Field	Field description	Usage tips
Content status	Controls whether the MCU as a whole is permitted to use content.	<p>If this setting is <i>Enabled</i>, you can still enable or disable the use of content on a per-conference basis. For more information about configuring individual conferences, refer to Adding and updating conferences.</p> <p>If this setting is <i>Disabled</i>, no conference will be able to use content.</p> <p>If this setting is <i>H.239 only</i>, no conference will be able to use BFCP content.</p> <p>Certain video conferencing endpoints and infrastructure such as gatekeepers may not operate correctly when communicating with equipment (such as the MCU) which declares H.239 capability. It may therefore be necessary to set this to <i>Disabled</i> in order to work with legacy devices (this will, of course, also prevent content video streams being used with any H.239- or BFCP-aware equipment).</p>

Display content in normal video channel	Sets whether the MCU will render content channel data in endpoints' main video channels.	<p>If there is an active content channel for a conference, it may be that the MCU is unable to open a content channel to a particular endpoint. For instance, that endpoint may have no content capability. Passthrough content cannot be sent in the main video channel. The message Content source (main video) - No effect in passthrough mode is displayed.</p> <p>In these cases, if this option is set to <i>Enabled</i>, the MCU will display the content channel video within a pane of the currently selected conference layout. In these cases, you might also want to enable the Automatically make content channel important option in the Settings > Conferences page which will make the content channel important at the same time.</p> <p>Note that SIP endpoints receive content from the MCU in the normal video channel (rather than in a separate channel). For this reason, this option must be enabled to allow SIP participants to see content.</p>
Video fast update request filtering	If this option is <i>Enabled</i> , the MCU will ignore fast update requests for a conference's content video channel received from endpoints whose connections are experiencing problems.	When this mode is active, it can prevent a large number of keyframes being sent in the shared content video encoding in response to fast update requests from a single endpoint. A high number of keyframes may reduce the video quality of the content channel for all conference participants, including those with good connections to the MCU.
Automatic content handover	Allows for rapid swapping between content from different participants in a video conference. In a conference where a participant is sending content, this feature allows another endpoint to start sending content without having to wait for the current content provider to stop sending content from his computer.	<p>The MCU applies this feature unit-wide.</p> <p>Therefore when it is enabled, all conferences on the MCU will allow automatic content handover.</p> <p>This option is disabled by default.</p>

Related topics

- [Content channel video support](#)
- [Configuring global conference settings](#)

Media port settings and clustering

The MCU has following media port modes and capacities:

Media port mode	Capacity
nHD	Up to w360p at 30fps.
SD	Up to w448p at 30fps.
HD	Up to 720p at 30fps or w448p at 60fps.
Full HD	Up to 1080p at 30fps (symmetric), or 720p at 60fps.

For information about the number of ports available on the different models of MCU, refer to [MCU port matrix](#).

Each Full HD participant requires four media port licenses. Each HD participant requires two media port licenses. Each SD participant requires one media port license. Each nHD participant requires 0.5 of a port license.

On an MCU 5320, to achieve the full capacity in Full HD mode you would need to allocate 40 port licenses to the MCU. To achieve full capacity in HD mode you need to allocate a total of 40 media port licenses to the MCU. To achieve the full capacity in SD mode you need to allocate a total of 40 media port licenses to the MCU. Full capacity in nHD mode requires 24 licenses (because each nHD port uses half a license).

To check the port license allocation on your MCU go to **Settings > Upgrade** and scroll down to the **Feature management** section.

Clustering MCUs

Two MCU 5300s can be clustered to increase capacity. The cluster will provide the sum of the capacities of the individual units, for example, if you cluster two MCU 5320s that each support 10 x 1080p participants you will have a cluster that supports 20 x 1080p participants.

Refer to the Cisco TelePresence MCU 5300 Series Getting started guide for information on how to set up and manage your cluster.

Setting the cluster mode

One of the MCUs acts as the master unit and the second as a slave. Set the cluster mode of each MCU in the cluster using the **Cluster mode** drop down list then click **Apply changes** and restart the MCU.

You can check the cluster mode of an MCU by going to **Status > Cluster**. See [Displaying cluster status on a master MCU](#) and [Displaying cluster status on a slave MCU](#) for more information.

When you have configured the units as master and slave, do not use the web interface of the slave unit for normal operations. All statistics and configuration information for the cluster can be accessed via the web interface of the master unit. The slave web interface is only used for upgrading code and for network configuration.

Some general points

Some points to note about clustering:

- Both units in a cluster must be running the same version of MCU software.
- The media port mode used by the cluster is the one configured on the master MCU.
- If you restart the master MCU the slave will also restart. All calls and conferences are terminated.
- Call Detail Records (CDRs) are stored on and accessible on the master MCU.
- Slave MCUs only have admin logins.

Upgrading clustered MCUs

If you need to upgrade the units in a cluster, first upload the new software images to each unit in the cluster and then restart the master. The slaves will automatically restart and the upgrade will be completed.

Configuring the media port mode

To change the media port mode go to **Settings > Media ports** and select the required media port mode from the drop down list then click **Apply changes**.

After enabling a mode, you must restart the MCU for changes to take effect.

Selected option

The selected option section shows you how many ports are available for each type of connection in the selected mode. The number of available ports will change when you switch between modes in the drop down menu. This is useful as it allows you to see the port availability before you enable either mode and restart the MCU.

Field	Field description
Media port mode	The required media port capacity. Choose from Full HD, HD, SD or nHD.
Full high definition video ports	The number of 1080p30 (symmetric) video ports available. Note: This is to transmit and receive at this resolution.
High definition video ports	The number of 720p30 video ports available.
Standard definition video ports	Up to w448p at 30fps.
nHD video ports	Up to w360p at 30fps.
Additional audio ports	<p>The number of audio-only ports available. Each audio port can be used by one voice-only participant in a video conference. When audio-only ports are unavailable, voice-only participants will use available video ports.</p> <p>On HD-capable MCUs, the additional audio ports value is 0 when the Media port mode is either <i>SD</i> or <i>nHD</i>.</p>

Related topics

- [Displaying cluster status on a master MCU](#)
- [Displaying cluster status on a slave MCU](#)
- [Reservation of MCU media ports](#)
- [MCU port matrix](#)

Upgrading and backing up the MCU

On this page:

- [Upgrading the main MCU software image](#)
- [Backing up and restoring the configuration](#)
- [Enabling MCU features](#)

Upgrading the main MCU software image

The main MCU software image is the only firmware component that you will need to upgrade.

To upgrade the main MCU software image:

1. Go to **Settings > Upgrade**.
2. Check the **Current version** of the main software image to verify the currently installed version.
3. Go to the [support pages](#) of the Cisco to identify whether a more recent image is available for downloading.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Log on to the MCU web browser interface.
7. Go to **Settings > Upgrade**.
8. Click **Browse** to locate the unzipped file on your hard drive.
9. Click **Upload software image**. The browser begins uploading the file to the MCU, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Main image upgrade completed."
10. The upgrade status displays in the **MCU software upgrade status** field.
11. [Shutting down and restarting the MCU](#).

Backing up and restoring the configuration

The Back up and restore section of the **Upgrade (Settings > Upgrade)** page allows you to back up and restore the configuration of the MCU using the web interface. This enables you to either go back to a previous configuration after making changes or to effectively "clone" one unit as another by copying its configuration.

To back up the configuration, click **Save backup file** and save the resulting "configuration.xml" file to a secure location.

To restore configuration at a later date, locate a previously-saved "configuration.xml" file and click **Restore backup file**. When restoring a new configuration file to an MCU, you can control which parts of the configuration are overwritten:

- If you select **Network settings**, the network configuration will be overwritten with the network settings in the supplied file. Typically, you would only select this check box if you were restoring from a file backed up from the same MCU or if you were intending to replace an out of service MCU. If you copy the network settings from a different, active, MCU and there is a clash (for instance, both are now configured to use the same fixed IP address) one or both boxes may become unreachable via IP. If you do not select **Network settings**, the restore operation will not overwrite the existing network settings, with the one exception of the QoS settings. QoS settings are overwritten regardless of the **Network settings** checkbox.

- If you select the **User settings** check box, the current user accounts and passwords will be overwritten with those in the supplied file. If you overwrite the user settings and there is no user account in the restored file corresponding to your current login, you will need to log in again after the file has been uploaded.

By default, the overwrite controls are not selected, and therefore the existing network settings and user accounts will be preserved.

Enabling MCU features

The MCU requires activation before most of its features can be used. (If the MCU has not been activated, the banner at the top of the web interface will show a prominent warning; in every other respect the web interface will look and behave normally.)

Advanced MCU features (such as *Video Firewall*) are not enabled as standard, and require additional activation. For information about configuring the video firewall, refer to the Knowledge Base section in the support pages of the web site.

If this is a new MCU you should receive the MCU already activated; if it is not, you have upgraded to a newer firmware version, or you are enabling a new feature, you may need to contact your supplier to obtain an appropriate activation code. Activation codes are unique to a particular MCU so ensure you know the MCU's serial number such that you may receive a code appropriate to your MCU.

Regardless of whether you are activating the MCU or enabling an advanced feature, the process is the same.

To activate the MCU or enable an advanced feature:

1. Check the **Activated features** (MCU activation is shown in this same list) to confirm that the feature you require is not already activated.
2. Enter the new feature code into the **Activation code** field exactly as you received it, including any dashes.
3. Click **Update features**. The browser window should refresh and list the newly activated feature, showing the activation code beside it. Activation codes may be time-limited. If this is the case, an expiry date will be displayed, or a warning that the feature has already expired. Expired activation codes remain listed, but the corresponding feature will not be activated.
If the activation code is not valid, you will be prompted to re-enter it.
4. Cisco recommends that you record the activation code in case you need to re-enter it in the future.

Successful MCU or feature activation has immediate effect and will persist even if the MCU is restarted.

Note that you can remove some MCU feature keys by clicking the **Remove** link next to the feature key in this page.

Related topics

- [Shutting down and restarting the MCU](#)

Shutting down and restarting the MCU

It is sometimes necessary to shut down the MCU, generally to restart as part of an upgrade (see [Upgrading and backing up the MCU](#)). You should also shut down the MCU before intentionally removing power from it.

Shutting down the MCU will cause all conference participants to be disconnected, and allows the MCU to ensure that all data (such as Call Detail Records) is stored correctly. You will lose network connectivity with the MCU for a few minutes while you restart the unit.

To shut down the MCU:

1. Go to **Settings > Shutdown**.
2. Click **Shut down MCU**.
3. Confirmation of shutdown is required; the button changes to **Confirm MCU shutdown**.
4. Click again to confirm.
5. The MCU will begin to shut down. The banner at the top of the page will change to indicate this. When the shutdown is complete, the button changes to **Restart MCU**.
6. Click this button a final time to restart the MCU.

Related topics

- [Upgrading and backing up the MCU](#)

Configuring security settings

To configure security settings for the MCU, go to **Settings > Security**.

- [Hashing passwords](#)
- [Security settings](#)
- [Serial console settings](#)
- [Usage recommendations for advanced account security](#)

Hashing passwords

By default the MCU hashes user passwords before storing them in the **configuration.xml** file. Passwords are stored as hash sums and are not stored anywhere on the MCU in plain text.

Security settings

If you make any changes, click **Update security settings** when you finish.

Field	Field description
Advanced account security mode	<p>Important! If you decide to enable advanced account security mode, you should first implement the recommendations below in Usage recommendations for advanced account security.</p> <p>Advanced account security has the following features:</p> <ul style="list-style-type: none"> ■ All current passwords (created when the MCU was not in advanced account security mode) will be expired and must be changed by the users when they next log in. ■ The MCU will demand that passwords fulfil certain criteria (using a mixture of alphanumeric and non-alphanumeric characters) and will apply certain rules on expiring and changing passwords. ■ The MCU will disable a user account after three consecutive incorrect password entry attempts. Administrator accounts are disabled for 30 minutes; other accounts are disabled indefinitely or until re-enabled by an administrator. ■ The MCU will disable any non-administrator account that is inactive for 30 days. Administrators can re-enable the account from the User page. ■ From the User page, administrators can also change the password for any user account, or enforce a password change by the user, or lock the password to prohibit password changes except by an administrator.
Redirect HTTP requests to HTTPS	<p>Enable this option to have HTTP requests to the MCU automatically redirected to HTTPS. The option is unavailable if either HTTP or HTTPS access is disabled on the Network > Services page.</p>
Idle web session timeout	<p>The timeout setting for idle web sessions, which can be set to a value between 1 minute and 60 minutes. If a web session expires, the user must log in again.</p> <p>Status web pages that auto-refresh will keep a web session active indefinitely. You can configure the MCU not to auto-refresh those pages, from the Settings > User interface page.</p>

Serial console settings

If you make any changes, click **Update console settings** when you finish.

Field	Field description
Hide log messages on console	The serial console interface displays log messages. If that is considered to be a security weakness in your environment, select this option to hide those messages.
Disable serial console input during startup	Enable this option for enhanced serial port security.
Require administrator login	Enable this option to require an administrator login by anyone attempting to connect to the MCU via the console port. If this is not enabled, anyone with physical access to the device (or with access to your terminal server) can potentially enter commands on the serial console.
Idle serial console session timeout	If you enable Require administrator login , you can configure a session timeout period for idle console sessions. The timeout value can be between 1 minute and 60 minutes. The administrator must log in again if a console session expires.

Usage recommendations for advanced account security

If you decide to enable advanced account security mode, we recommend that you first do the following:

- Back up your configuration.
The MCU gives the option to create a backup file when it asks for confirmation of the advanced account security request.
- Rename the default administrator account.
This is especially important where the MCU is connected to the public Internet, because security attacks often use "admin" when attempting to access a device with a public IP address. Even on a secure network, if the default administrator account is "admin", it is possible for innocent attempts to log into the MCU to cause the account to be locked out for 30 minutes.
- Create several accounts with administrator privileges.
This ensures that if an administrator account is locked out, you have another account through which to access the MCU.
- Create dedicated administrator accounts for each API application (if any) that accesses the MCU.
- Update the device password in TMS before enabling the functionality on the MCU.

Password format and usage

In advanced account security mode, user passwords are subject to the following rules on format and usage:

- At least fifteen characters.
- At least two uppercase alphabetic characters.
- At least two lowercase alphabetic characters.
- At least two numeric characters.
- At least two non-alphanumeric (special) characters.
- Not more than two consecutive repeating characters (two repeating characters are allowed but three are not).
- The password must be different from the previous 10 passwords used with the associated user account.
- The password will expire if it is not changed within 60 days.

- Except for users with administrator privileges, the password may not be changed more than once in 24 hours.

Note: If the MCU is configured to require certificate-based login only (*Require client certificate login* is enabled for HTTPS on the [Network > SSL certificates](#) page) every user account still requires a password to be defined, and the rules on password format and usage, including changing within 60 days, still apply.

Expired passwords

In advanced account security mode, if a user logs in with a correct but expired password, the MCU will prompt the user to change the password. If the user chooses not to change it, the user is allowed two more login attempts to change the password before the account is disabled.

Related topics

- [Managing security warnings](#)
- [Understanding security warnings](#)
- [Managing user accounts](#)
- [Configuring SSL certificates](#)

Displaying system status

Displaying general status	195
Displaying conference status	197
Conference content channel	200
Displaying hardware health status	201
Displaying security status	202
Displaying cluster status	203
MCU port matrix	206

Displaying general status

The **General status** page displays an overview of the MCU status. To access this information, go to **Status > General**.

Refer to the table below for details of the information displayed

Field	Field Description
System status	
Model	The specific MCU model.
Serial number	The unique serial number of the MCU.
Software version	The installed software version. You will need to provide this information when speaking to Customer support.
Build	The build version of installed software. You will need to provide this information when speaking to Customer support.
Uptime	The time since the last restart of the MCU.
Host name	The host name assigned to the MCU. You can change the host name at Network > DNS .
IP address	The local IP address of the MCU network interface used to access the MCU web user interface.
CPU load	The current processor utilization of the MCU.
Media processing load	<p>An overview of the current media loading of the MCU.</p> <p>If this unit is the master in a cluster, the media loading displayed here is the average load across the units in the cluster.</p> <p>If the total load is consistently high, you might need to add an additional MCU to better handle your video conferencing needs. Also, the total load may increase during periods of peak conference use.</p>
System time	
Current time	The system time on the MCU. Click New time to modify this value. The Time Settings page opens in which you can update the system date and time manually or refresh the time from an NTP server. For more information about the Time Settings page, refer to Displaying and resetting system time .
System log	
<ul style="list-style-type: none"> User requested shutdown User requested upgrade Unknown 	<p>The system log displays the last eight shutdown and upgrade events in date order with the most recent system log event at the top of the list.</p> <p>The log will also display "Unknown" if there has been an unexpected reboot or power failure, which you should report to customer support if it happens repeatedly.</p>

Diagnostic information

Download diagnostic information	If required to do so by Customer support, click Download diagnostic information to save a set of diagnostic files.
Download conference information	If required to do so by Customer support, click Download conference information to save a file which details information about active and scheduled conferences for diagnostic purposes.
Download network trace	If network trace has been enabled on the MCU, via the serial console, there is a Download network trace button here. Click this button to download the most recent network trace if it is required by your customer support representative.

Related topics

- [Displaying conference status](#)
- [Displaying hardware health status](#)
- [Configuring time settings](#)
- [Upgrading and backing up the MCU](#)
- [Shutting down the MCU](#)

Displaying conference status

The **Conference status** page displays the status of active and completed conferences and video and audio processing. To access this information, go to **Status > Conferences**.

Refer to the table below for assistance in interpreting the information displayed:

- [Conference status](#)
- [Video status](#)
- [Audio status](#)

For information about the number and type of ports provided by each MCU model, refer to [MCU port matrix](#).

Format of displayed values

In many cases, the values displayed on this page are shown in the format **A (B) / C**; this represents:

- **A** - the current value of this statistic
- **B** - the maximum achieved value of this statistic (since last reset)
- **C** - the maximum allowable number for this statistic (this varies by MCU model)

The maximum value (**C** above) for the "ports in use" fields depends on the number of port licenses allocated to the unit. One port license is required for standard definition (SD) ports, two for each high definition (HD) port.

Statistics for which there is no set maximum are displayed as **A (B)**, where **A** and **B** have the meanings described above.

Where the highest value attained is shown in parentheses (i.e. **B** in the above example), this value can be reset by selecting **Reset maximum values**. These values can be useful in monitoring peak MCU usage over a period of time.

Conference status

Conference status displays an overview of active and completed conferences.

Field	Field description
Active conferences	The number of conferences that are currently configured on the MCU.
Active auto attendants	The number of auto attendants that are currently in use. If you dial in with an endpoint to the auto attendant, this will go up by one. It does not reflect the number of configured auto attendants.
Completed conferences	<p>The number of conferences that were once active but are now not.</p> <p>Note : The number of completed conferences resets after a reboot. When the MCU reboots these completed conferences no longer appear on this page (this page displays runtime statistics). However, they will still appear on <code>conference.enumerate</code> and the Conferences > Conference list page (these pages display configured statistics).</p>
Completed auto attendants	The total number of calls into an auto attendant, excluding any in progress. If you call an auto attendant and enter into a conference or hang up the call, this number increases by one.

Active conference participants	The number of people currently in conferences.
Previous conference participants	The number of people who were previously participating in a conference (since the last time the MCU restarted).
Video ports in use	<p>This value is shown if the MCU is not operating in Port reservation mode, and shows the number of video ports in use. It also shows a maximum number, which is affected by the media port mode and by whether the MCU is in a cluster, and, on MCU 5300 units and MCU MSE 8510 blades, by how many media port licences have been assigned.</p> <p>This number corresponds to the number of connected participants that are either sending or receiving video.</p> <p>See the port matrix for more details.</p>
Audio-only ports in use	<p>This value is shown if the MCU is not operating in Port reservation mode, and shows the number of audio-only ports in use. This corresponds to the number of connected participants that are contributing or being sent audio but not video.</p> <p>There is also a maximum number, which is affected by the media port mode and by whether the MCU is in a cluster, and, on MCU 5300 units and MCU MSE 8510 blades, by how many media port licences have been assigned.</p>
Reserved video ports	This value is shown if the MCU is operating in Port reservation mode , and shows the total number of video ports reserved across the currently active conferences.
Reserved audio-only ports	This value is shown if the MCU is operating in Port reservation mode , and shows the total number of audio-only ports reserved across the currently active conferences.
Reserved video ports in use	This value is shown if the MCU is operating in Port reservation mode , and shows, of the number of video ports reserved, how many are actually being used by active conference participants.
Reserved audio-only ports in use	This value is shown if the MCU is operating in Port reservation mode , and shows, of the number of audio-only ports reserved, how many are actually being used by active conference participants.

Video status

Video status displays an overview of current video resource use.

Field	Field description	Usage tips
Incoming video streams	The number of video streams being received by the MCU.	Unicast indicates video streams sent directly to the MCU (incoming) or directly to the endpoints (outgoing) rather than multicast streams broadcast to the network and captured or sent by the MCU.
Outgoing video streams	The number of video streams being sent by the MCU.	

Total incoming video bandwidth	The total video data rate being received by the MCU.
---------------------------------------	--

Total outgoing video bandwidth	The total video data rate being sent by the MCU.
---------------------------------------	--

Audio status

Audio status displays an overview of current audio resource use.

Field	Field description	Usage tips
Incoming audio streams	The number of audio streams being received by the MCU.	Unicast indicates audio streams sent directly to the MCU (incoming) or directly to the endpoints (outgoing) rather than multicast streams broadcast to the network and captured or sent by the MCU.
Outgoing audio streams	The number of audio streams being sent by the MCU.	

Related topics

- [Displaying general status](#)
- [Displaying hardware health status](#)

Conference content channel

The **Conference content channel** page shows various status items related to a conference's content channel. To view this page, go to **Conferences > Conference list**, click the name of the conference about which you want more information and in the **Participants** column, click the Content channel link.

The displayed information is split into three sections:

Preview

This section shows a graphical representation of the current content channel. If there is no active content channel, a black rectangle appears here instead of a preview image. Where there is an active content channel, clicking on the preview image will cause it to update. Note that no preview is shown if the conference is configured as Passthrough content mode.

Received video

This section details the characteristics of the video stream supplying the content channel. This stream will either be an H.239 channel from one of the H.323 conference participants, or a BFCP (Binary Floor Control Protocol) channel from a SIP conference participant, or a *main video channel* configured for use as the content channel source.

Transmitted video

While there is at most one source video stream for a conference's content channel, the content channel can be viewed by several people, either via H.239 or BFCP to video conferencing endpoints.

The **Transmitted video** section of this page shows the number of viewers of each type, plus some statistics on the currently active H.239/BFCP video stream.

Passthrough viewers shows the number of content viewers viewing in Passthrough mode.

Diagnostics

It is possible to retrieve a set of diagnostics relating to the conference's content channel. This is accomplished by clicking on the **Download content channel diagnostics** control beneath the main table. You should not need to access these diagnostics except when directed to by Customer support.

Related topics

- [Content channel video support](#)
- [Configuring content settings](#)

Displaying hardware health status

The **Health status** page (**Status > Health**) displays information about the hardware components of the MCU.

Note: The **Worst status seen** conditions are those since the last time the MCU was restarted.

To reset these values, click **Clear**. Refer to the table below for assistance in interpreting the information displayed.

Field	Field description	Usage tips
Fans Voltages RTC battery	Displays two possible states: <ul style="list-style-type: none"> OK Out of spec States indicate both <i>Current status</i> and <i>Worst status seen</i> conditions.	The states indicate the following: <ul style="list-style-type: none"> <i>OK</i> - component is functioning properly <i>Out of spec</i> - Check with your support provider; component might require service If the <i>Worst status seen</i> column displays <i>Out of spec</i> , but <i>Current status</i> is <i>OK</i> , monitor the status regularly to verify that it was only a temporary condition.
Temperature	Displays three possible states: <ul style="list-style-type: none"> OK Out of spec Critical States indicate both <i>Current status</i> and <i>Worst status seen</i> conditions.	The states indicate the following: <ul style="list-style-type: none"> <i>OK</i> - temperature of the MCU is within the appropriate range <i>Out of spec</i> - Check the ambient temperature (should be less than 34 degrees Celsius) and verify that the air vents are not blocked <i>Critical</i> - temperature of MCU is too high. An error also appears in the event log indicating that the system will shutdown in 60 seconds if the condition persists If the Worst status seen column displays <i>Out of spec</i> , but Current status is <i>OK</i> monitor the status regularly to verify that it was only a temporary condition.

Related topics

- [Displaying general status](#)
- [Displaying conference status](#)

Displaying security status

The **Security status** page displays a list of active security warnings for the MCU. To access this information, go to **Status > Security**.

Security warnings identify potential weaknesses in the security of the MCU's configuration. Note that some security warnings might not be relevant for your organization. For example if the MCU is inside a secure network, enabling HTTP may not be a security issue. For information about all possible security warnings, refer to [Understanding security warnings](#).

To acknowledge a security warning, select that warning and click **Acknowledge selected**. Acknowledged warnings will not appear on the MCU's Home page. If the MCU reboots, the warnings are reset and previously acknowledged warnings will need re-acknowledging.

To fix a security issue, click on the **Action** link for the warning message relating to the issue. When you fix a security issue, the security warning disappears from this list (on the **Status > Security** page), but it will be logged in the Audit log. For more information about the audit log, refer to [Working with the audit logs](#).

Refer to the table below for details of the information displayed.

Field	Field Description
Warning	The text of the security warning.
State	<p>For every security warning, the state will one of:</p> <ul style="list-style-type: none">■ <i>New</i>: A new security warning is one that has been raised by the MCU, but you have not acknowledged it. New warnings also appear on the MCU Home page.■ <i>Acknowledged</i>: An acknowledged security warning is one that you have acknowledged, but have not fixed. <p>When you fix a security issue, the security warning disappears from this list, but it will be logged in the Audit log. For more information about the audit log, refer to Working with the audit logs.</p>
Action	For every security warning, there is a corresponding action that explains how to fix the security issue. Usually this is a link that takes you to the page where you can make the configuration change that will fix the security issue.

Related topics

- [Configuring security settings](#)
- [Working with the audit log](#)
- [Understanding security warnings](#)
- [Displaying conference status](#)
- [Displaying hardware health status](#)

Displaying cluster status

Displaying the cluster status of a master MCU

To display cluster status, go to **Status > Cluster**.

The table below describes the **Status > Cluster** page that displays for the **master** MCU in a cluster. For information about what details are displayed for a slave, see [Displaying cluster status on a slave MCU](#).

Field	Field description	Usage tips
IP	The IP address of a slave MCU or <i>Master</i> .	
Status	<p>The status of the master can only be OK which means that this MCU is operating correctly in the cluster. Possible statuses for the slave MCU are:</p> <ul style="list-style-type: none"> ■ OK: The master and slave are communicating correctly. ■ OK (last seen <number> seconds ago): The master has lost contact with the slave. The slave will restart itself and in this way it will rejoin the cluster. Wait a few minutes and then refresh the Status > Cluster page. ■ Still starting up: The slave is in the process of starting up. Wait a few minutes and then refresh the Status > Cluster page. ■ Lost contact <number> secs ago: The master has lost contact with the slave. The slave will restart itself and in this way it will rejoin the cluster. Wait a few minutes and then refresh the Status > Cluster page. ■ Failed, version mismatch: All MCUs in the cluster must be running the same version of software. This status message indicates that this MCU is running different software to the master. This MCU is not part of the cluster. Update all MCUs in the cluster to the same version of software. 	<p>If the status of the slave is OK, it is currently functioning in the cluster. For any of the other statuses, the slave MCU is not currently functioning as part of the cluster.</p> <p>If the slave MCU has a problem that causes it to no longer be part of the cluster, the cluster can continue to operate without the slave. There will just be fewer video ports available.</p> <p>If the slave MCU fails, participants in conferences will not be disconnected if there are sufficient resources on the master and they will continue to receive audio and video. In the worst case, the video will disappear, but the audio will continue because all audio is processed by the master MCU.</p> <p>If the master loses contact with the slave, the slave will automatically restart itself. In this way, it can rejoin the cluster.</p>
Media processing load	<p>An overview of the current media loading of each MCU in the cluster. The load may increase during periods of peak conference use.</p>	<p>Conferences are distributed between the MCUs in the cluster. The loads on the MCUs depend on the number of conferences running on each MCU and the sizes of those conferences.</p>

Port licenses	The number of port licenses on the MCU listed in this row.	All port licenses on the slave MCU are controlled by the master MCU. Depending on how you use the MCUs, you might want to allocate all port licenses to the master MCU or you might distribute them between the MCUs. It does not matter to the cluster how you have allocated the port licenses; in any case, the master controls all port licenses and even if an MCU has failed in the cluster, the master will continue to have access to any port licenses allocated to the failed MCU.
----------------------	--	--

Related topics

- [Displaying cluster status on a slave MCU](#)
- [Displaying general status](#)
- [Displaying hardware health status](#)
- [Displaying conference status](#)

Displaying the cluster status on a slave MCU

This topic applies only to MCUs that are configured as part of a cluster.

To display cluster status, go to **Status > Cluster**.

The table below describes the **Status > Cluster** page that displays on a **slave** in a cluster. For information about the details displayed on a master MCU, see [Displaying cluster status on a master MCU](#).

A slave MCU does not present the full MCU web interface. Some settings are only available on the master MCU.

The master MCU in a cluster inherits all the ports and port licenses from the slave MCU. Configure conferences and other MCU functionality from the web interface of the master MCU (accessible using the IP address displayed on the **Status > Cluster** page).

When you look at the **Status > Cluster** page on the slave MCU, it shows the status of the master MCU.

Field	Field description	Usage tips
Status	<p>Possible statuses for the master MCU are:</p> <ul style="list-style-type: none"> ■ <i>Still starting up</i>: the master MCU is in the process of starting up. Wait a few minutes and then refresh the Status > Cluster page. ■ <i>OK</i>: The master and slave are communicating correctly. ■ <i>Lost contact</i>: The slave MCU has lost contact with the master MCU. This status will only be momentarily visible because the slave MCU will quickly restart itself in this case. 	<p>If the slave MCU loses contact with the master MCU it will restart itself. This is the only way that the slave MCU can be correctly rejoined into the cluster. Usually, if a slave MCU has lost contact with the master this is because the master has itself restarted.</p>

Last seen	This field is only visible if the master has not been seen for 11 seconds. The slave MCU will automatically restart itself very soon after it loses contact with the master.
------------------	--

IP address	The IP address of the master MCU.
-------------------	-----------------------------------

Related topics

- [Displaying cluster status on a master MCU](#)
- [Displaying conference status](#)
- [Displaying general status](#)
- [Displaying hardware health status](#)

MCU port matrix

The port provision of the MCU is shown in the table below. Each video port can be used by one video-conferencing participant. Each audio-only port can be used by one voice-only participant in a video conference.

The number and type of available media ports on the MCU is controlled by the port capacity mode which you configure on the [Settings > Media ports](#) page.

Note: If port reservation is enabled, then activating a conference's content channel will cause that conference to consume one video port - even when content is not being delivered.

The MCU supports the following media port modes and capacities:

Media port mode	Capacity
nHD	Up to w360p at 30fps.
SD	Up to w448p at 30fps.
HD	Up to 720p at 30fps or w448p at 60fps.
Full HD	Up to 1080p at 30fps, or 720p at 60fps.

Port matrix table

Model	Mode	Licenses per port	Video ports	Audio-only ports
MCU 5310	nHD	0.5	24	0
	SD	1	20	0
	HD	2	10	10
	Full HD	4	5	5
MCU 5320	nHD	0.5	48	0
	SD	1	40	0
	HD	2	20	20
	Full HD	4	10	10

Related topics

- [Reservation of MCU media ports](#)
- [Configuring global conference settings](#)
- [Content channel video support](#)

Advanced topics

Working with the event logs	208
Working with the audit logs	210
Using Call Home	211
Understanding security warnings	213
Logging using syslog	216
SIP: Advanced	219
Working with Call Detail Records	220
Feedback receivers	223
Customizing the user interface	224
Customization: More information	232
Network connectivity testing	233
Configuring SSL certificates	234
Transitioning to certificate-based security	241

Working with the event logs

If you are experiencing complex issues that require advanced troubleshooting, you may need to collect information from the MCU logs. Typically, you will be working with Customer support who can help you obtain these logs.

Event log

The last 2000 status messages generated by the MCU are displayed in the **Event log** page (**Logs > Event log**). In general these messages are provided for information, and occasionally *Warnings* or *Errors* may be shown in the Event log. The presence of such messages is not cause for concern necessarily; if you are experiencing a specific problem with the operation or performance of the MCU, Customer support can interpret logged messages and their significance for you.

You can:

- Change the level of detail collected in the traces by editing the **Capture filter** page. You should not modify these settings unless instructed to do so by Customer support.
- Display the log as text: go to **Logs > Event log** and click **Download as text**.
- Change which of the stored Event log entries are displayed by editing the **Display filter** page
- Send the event log to one or more syslog servers on the network for storage or analysis. The servers are defined in the **Syslog** page. For more information, refer to [Logging using syslog](#)
- Empty the log by clicking **Clear log**.

Event capture filter

The Event capture filter allows you to change the level of detail to collect in the Event log traces.

Note: You should not modify these settings unless instructed to do so by Customer support. Modifying these settings can impair the performance of your MCU.

Normally, the capture filter should be set to the default of *Errors, warnings and information* for all logging sources. There is no advantage in changing the setting of any source without advice from Customer support. There is a limited amount of space available to store logged messages and enabling anything other than *Errors, warnings and information* could cause the log to become full quickly.

Event display filter

The Event display filter allows you to view or highlight stored Event log entries. Normally, you should not need to view or modify any of the settings on this page.

Syslog

You can configure the MCU to send event messages to up to four syslog servers. To add or remove a syslog server, go to **Logs > Syslog** and make the changes you require. See [Logging using syslog](#).

H.323/SIP log

The **H.323/SIP log** page records every H.323 and SIP message received or transmitted from the MCU. The log can be exported in an .xml file by clicking **Download as XML**.

By default the H.323/SIP log is disabled because it affects performance, but Customer support may ask you to enable it if there is a problem with an MCU in your network. To do this, click **Enable H323/SIP logging**.

Note that although the H.323/SIP log page can display up to 10 pages of logged messages the log file may begin to overwrite itself before the 10 pages are full.

Audit log

The audit log records any user action on the MCU which might compromise the security of the unit, of its functions, or of the network. For more information, refer to [Working with the audit logs](#).

Call Detail Records

In addition to the logs described above, the MCU can also store Call Detail Records (CDR) which may be used for auditing and billing purposes. Events in the log are displayed in the CDR log page. See [Working with Call Detail Records](#) for more details.

Related topics

- [Working with Call Detail Records](#)
- [Logging using syslog](#)

Working with the audit logs

The audit log records any user action on the MCU which might compromise the security of the unit, of its functions, or of the network.

By enabling auditing, all network settings, conference settings, security settings, creation/deletion of conferences, and any changes to the audit log itself are logged on the MCU.

All relevant actions on the MCU are logged, including those made through the serial console, the API, and the web interface. The module that has caused a log is listed within the details of that log and will be one of:

- **Web:** For configuration changes made through the web interface.
- **Serial:** For configuration changes made through the serial interface.
- **API:** For configuration changes made through the API.
- **System:** For audit messages from the MCU.

Each log also has a severity associated with it (Error, Severe Warning, Warning, Info, or Status Warning).

You must enable the audit log for it to record these actions.

To enable and view the audit log, go to [Logs](#) and select the **Audit log** tab.

Audit log

The last 2000 audit messages generated by the MCU are displayed in the **Audit log** page.

The last 100,000 audit messages are stored on the external compact flash if there is one; otherwise, the last 100,000 audit messages are stored internally. You can only view the last 2000 through the web interface, but you can download all stored audit messages (up to the 100,000) as XML.

You can delete audit messages. If you delete any audit messages, that will be audited in a new audit message.

You cannot send the audit log to a syslog server.

Related topics

- [Configuring security settings](#)
- [Understanding security warnings](#)

Using Call Home

Note: Call Home requires the MCU to have an *Encryption* feature key. Without this key, you can view the Call Home web page but the functionality will not be available.

Note: The MCU currently only supports anonymous reporting.

The MCU can submit reports about its status and any faults that it has experienced to the Cisco Call Home service. The MCU always uses a secure connection (HTTPS) to transmit reports to Call Home.

When Call Home is disabled (default setting), the device will not send a report of any type until you select a **Call Home mode**. When you have enabled Call Home, you can manually submit a report or configure the feature to work automatically.

When you use *Anonymous Call Home*, you will not be able to view anonymously submitted reports; they are only available to Cisco engineers and are only used to diagnose potential issues.

Note: If you have any questions about a Call Home report please contact Cisco TAC.

After choosing the Call Home mode *anonymous*, you can check **Automatic Call Home enabled** if you want the MCU to automatically submit reports. The device sends any pending reports as soon as you apply this change. After that, it will automatically send diagnostic reports about any unexpected device restarts or media resource restarts without further manual intervention.

If you prefer not to use automatic Call Home, you can click **Call Home now** to manually send reports at any time.

The *Device inventory* report is always available; its presence does not indicate any special condition or fault. If automatic Call Home is enabled, the MCU always sends these reports on startup.

To configure Call Home:

1. Go to **Logs > Call Home**.
The **Status** section shows whether this feature is enabled and what reports are currently available.
2. Select the **Call Home mode, Anonymous Call Home**.
3. (Optional) Click **Call Home now** to manually submit the **Current reports**.
4. (Optional) Check **Automatic Call Home enabled** if you want the MCU to submit reports without manual intervention.
5. Click **Apply changes**.
If Automatic Call Home is enabled, the MCU sends any pending reports now.

Table 1: Status fields

Field	Description
Call Home status	Indicates <i>Enabled - Anonymous Call Home</i> or <i>Disabled</i> status. (<i>Disabled</i> by default.) If Call Home is disabled, the MCU logs this in the event log during start up. The MCU also logs a message if Call Home mode is enabled (<i>Anonymous Call Home</i>) but is not configured to automatically submit reports.
Current reports	A list of available reports.

Submission status	Indicates the status of the latest reports submission, including date and time. Status is <i>Not sent</i> if no reports have been submitted.
Call Home now	Manually submits Current reports . A confirmation pop-up displays when manually submitting a report or enabling automatic reporting to indicate that data will be transmitted to Cisco. Report submissions are retried 3 times. If a submission fails after the third attempt this information is shown in the status field.
Dismiss warning (button)	Click to dismiss the warning that appears in the UI banner. This button is greyed out unless a warning has appeared in the UI banner.

Table 2: Configuration fields

Field	Description
Call Home mode	Enables <i>Anonymous Call Home</i> . (<i>Disabled</i> by default, no reports can be submitted.)
Automatic Call Home enabled	Allows the MCU to send diagnostic reports when necessary; also allows the MCU to send inventory reports when it starts up.

Understanding security warnings

The **Security status** page displays a list of active security warnings for the MCU. To access this information, go to **Status > Security**. Security warnings identify potential weaknesses in the security of the MCU's configuration. For more information on configuring security settings, refer to [Configuring security settings](#). For more detailed information on the security status, refer to [Displaying security status](#).

The table below details the warnings that appear, and the relevant actions needed to rectify them.

Warning	Action	Explanation
Advanced password security is disabled	Enable advanced account security mode in security settings	If advanced account security mode is not enabled, passwords will be stored in plain text in the configuration file, and therefore be unsecure. To enable advanced account security mode, go to Settings > Security and enable <i>Advanced account security mode</i> .
Hide log messages on console is disabled	Enable hide log messages on console in serial console settings	To hide log messages on the console, go to Settings > Security and select Hide log messages on console . This will stop event messages appearing on the console.
Require administrator login to console is disabled	Enable require administrator login in serial console settings	You must log in using an admin account to access serial console commands, in this way the serial console will be more secure. To do this, go to Settings > Security and select Require administrator login .
Guest account is enabled	Disable the guest account.	By default the guest user account is assigned the privilege of 'conference list only', meaning that users who log in as guest can view the list of active conferences and change their own profile. Disabling the guest account makes the MCU more secure. To disable the guest account, go to Users > User list and select Guest . Select Disable user account .
Admin account has default username	Change the admin account username	The MCU must have at least one configured user with administrator privileges. By default, the User ID is "admin" and no password is required. To change the admin account username, go to Users > User list and select admin . Enter a new username in the User ID field and click Update user settings .
Unsecured HTTP service is enabled	Disable HTTP in network TCP services	Information sent using HTTP (Web) is unsecured and not encrypted. To disable HTTP, go to Network > Services and deselect Web . We recommend that you enable Secure web .
Unsecured SNMP service is enabled	Disable SNMP in network UDP services	Information sent using SNMP is unencrypted and sent in plain text; therefore, it is possible for people to discover usernames and passwords easily. To disable SNMP, go to Network > Services and deselect SNMP .

Auto-refresh of web pages is enabled	Change auto-refresh interval to "No auto-refresh"	<p>If your MCU is set to auto-refresh it could mean that on an idle MCU a session will never time out.</p> <p>To turn off auto-refresh, go to Settings > User interface and change Status page auto-refresh interval to <i>No auto-refresh</i>.</p>
Audit logging of configuration changes is disabled	Enable the audit log	<p>If the audit log is disabled, the MCU will not create an audit log. To enable audit logs, go to Logs > Audit log and select Enable auditing.</p> <p>For more information on the audit log, refer to Configuring security settings.</p>
Audit logs hash check failed, audit system integrity compromised	Check system configuration for possible security changes	<p>If audit logs checks fail, it is possible that your MCU has been compromised. For example, someone may have taken the compact flash card out and deleted some audit logs.</p> <p>For more information on the audit log, refer to Configuring security settings</p>
Call encryption is disabled	Enable call encryption	<p>When encryption status is <i>Disabled</i>, no calls on the MCU will be able to use encryption.</p> <p>To enable encryption, go to Settings > Encryption. For Encryption status, select <i>Enabled</i>.</p>
Audit log above 75% capacity	Download and delete audit logs	<p>The audit log has a maximum capacity of 100,000 audit events, or the size limit of the compact flash card. When you are nearing either of these limits, the MCU will give you this warning. If you reach full capacity of the compact flash card, the MCU will 'wrap' meaning that older logs will be deleted. To rectify this problem download and clear the audit log.</p> <p>To do this, go to Logs > Audit log and select Download as XML. Once this has completed, click Delete all records.</p>
Audit log above 90% capacity	Download and delete audit logs.	<p>The audit log has a maximum capacity of 100,000 audit events, or the size limit of the compact flash card. When you are nearing either of these limits, the MCU will give you this warning. If you reach full capacity of the compact flash card, the MCU will 'wrap' meaning that older logs will be deleted. To rectify this problem download and clear the audit log.</p> <p>To do this, go to Logs > Audit log and select Download as XML. Once this has completed, click Delete all records.</p>
Audio participants overlaid icon disabled	Enable audio participants overlaid icon.	<p>The MCU provides icons in the corner of the video screen to give participants information about the conference.</p> <p>See Using in-conference features with video endpoints to see all in-conference icons and their descriptions.</p> <p>To enable the icons, go to Settings > Conferences. For Overlaid icons, select the icons you would like to be visible to participants.</p>
Unsecured conferences overlaid icon disabled	Enable unsecured conferences overlaid icon.	
Recording indicator overlaid icon disabled	Enable recording indicator overlaid icon.	

Encryption not available on this device	Add feature key for encryption.	To use encryption on your MCU you must have the Encryption feature key installed. To purchase this feature key, contact your reseller.
Default encryption setting for new ad hoc conferences set to optional	Set encryption to required in the template for new ad hoc conferences.	<p>When encryption status is <i>Enabled</i>, the MCU advertises itself as being able to use encryption and will use encryption if required to do so by an endpoint.</p> <p>To rectify this problem, go to Conferences > Templates > Ad hoc conferences. Set Encryption, to <i>Required</i>.</p> <p>To use encryption on your MCU you must have the Encryption feature key installed. To purchase this feature key, contact your reseller.</p>
SRTP encryption disabled	Enable SRTP encryption.	<p>When SRTP is disabled, the MCU will not advertise that it is able to encrypt using SRTP.</p> <p>To rectify this problem, go to Settings > Encryption. For SRTP encryption, select <i>Secure transports (TLS) only</i>. This means that if encryption is used for a call, the media will only be encrypted in calls that are set up using TLS.</p>
SRTP encryption enabled for all transports, including insecure transports (UDP and TCP)	Enable SRTP encryption for secure transports (TLS) only.	To rectify this problem, go to Settings > Encryption . For SRTP encryption , select <i>Secure transports (TLS) only</i> . This means that if encryption is used for a call, the media will only be encrypted in calls that are set up using TLS.
Default encryption setting for new scheduled conferences set to optional	Set encryption to required in the top level conference template.	<p>When you (or another user) create a new conference (by choosing Conferences and clicking Add new conference), you can set the encryption setting for the conference to be either <i>Optional</i> or <i>Required</i>.</p> <p>To ensure that all new scheduled conferences use encryption, go to Conferences > Templates and for Encryption, select <i>Required</i>.</p>
Conference list page is public	Disable public conference list page.	<p>You can allow users access to the conference list pages without having to authenticate with the MCU. By default, these pages are accessible to users who have not logged in.</p> <p>To force users to authenticate before they can access the conference list page, go to Settings > User interface, and in the Public pages section, deselect Conference list.</p>
Shell not secured for startup	Disable the serial input during startup.	<p>If Disable serial input during startup isn't selected, the serial console is not protected during application startup. This means users will have access to debug services in the operating system.</p> <p>To disable this, go to Settings > Security, and select Disable serial input during startup.</p>

Related topics

- [Configuring security settings](#)
- [Working with the audit log](#)
- [Displaying system status](#)

Logging using syslog

You can send the [Event log](#) to one or more syslog servers on the network for storage or analysis.

To configure the syslog facility, go to **Logs > Syslog**.

On this page:

- [Syslog settings](#)
- [Using syslog](#)

Syslog settings

Refer to this table for assistance when configuring Syslog settings:

Field	Field description	Usage tips
Host address 1 to 4	Enter the IP addresses of up to four Syslog receiver hosts.	The number of packets sent to each configured host will be displayed next to its IP address.

Facility value	<p>A configurable value for the purposes of identifying events from the MCU on the Syslog host. Choose from the following options:</p> <ul style="list-style-type: none"> ■ 0 - kernel messages ■ 1 - user-level messages ■ 2 - mail system ■ 3 - system daemons ■ 4 - security/authorization messages (see Note) ■ 5 - messages generated internally by syslogd ■ 6 - line printer subsystem ■ 7 - network news subsystem ■ 8 - UUCP subsystem ■ 9 - clock daemon (see Note) ■ 10 - security/authorization messages (see Note) ■ 11 - FTP daemon ■ 12 - NTP subsystem ■ 13 - log audit (see Note) ■ 14 - log alert (see Note) ■ 15 - clock daemon (see Note) ■ 16 - local use 0 (local0) ■ 17 - local use 1 (local1) ■ 18 - local use 2 (local2) ■ 19 - local use 3 (local3) ■ 20 - local use 4 (local4) ■ 21 - local use 5 (local5) ■ 22 - local use 6 (local6) ■ 23 - local use 7 (local7) 	<p>Choose a value that you will remember as being the MCU.</p> <hr/> <p>Note: Various operating system daemons and processes have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar.</p> <p>Various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages.</p> <hr/> <p>Processes and daemons that have not been explicitly assigned a Facility value may use any of the "local use" facilities (16 to 21) or they may use the "user-level" facility (1) - and these are the values that we recommend you select.</p>
-----------------------	---	--

Using syslog

The events that are forwarded to the syslog receiver hosts are controlled by the event log capture filter.

To define a syslog server, simply enter its IP address and then click **Update syslog settings**. The number of packets sent to each configured host is displayed next to its IP address.

Note: Each event will have a severity indicator as follows:

- 0 - Emergency: system is unusable (unused by the MCU)
 - 1 - Alert: action must be taken immediately (unused by the MCU)
 - 2 - Critical: critical conditions (unused by the MCU)
 - 3 - Error: error conditions (used by MCU *error* events)
 - 4 - Warning: warning conditions (used by MCU *warning* events)
 - 5 - Notice: normal but significant condition (used by MCU *info* events)
 - 6 - Informational: informational messages (used by MCU *trace* events)
 - 7 - Debug: debug-level messages (used by MCU *detailed trace* events)
-

Related topics

- [Working with the event logs](#)

SIP: Advanced

SIP implementation

The MCU implements SIP as defined in RFC 3261. Any product wanting to establish SIP calls with the MCU should implement INVITE, ACK, BYE, and CANCEL messages along with responses from 1xx to 6xx. The MCU acts as a client and does not return 5xx and 6xx responses itself; however, proxies and other intermediaries may do so.

To use a SIP registrar in conjunction with the MCU, you must register an ID for the MCU with the SIP registrar. The MCU can register itself, and individual conferences and auto attendants with a SIP registrar.

For video Fast Update Requests, the MCU uses a type that involves sending an INFO message with an XML body. This only applies to video endpoints, but these endpoints should be able to correctly reply to INFO requests whether or not they understand them as Fast Update Requests.

Authentication details

The username and password that you provide on the [Settings > SIP](#) page are the authentication details for all SIP authentication from the MCU. That is, for the SIP registrar and any SIP proxy. If you have individual conferences registered with the SIP registrar, the username will be the numeric identifier of the conference and the password will be the one entered on the [Settings > SIP](#) page.

Related topics

- [Configuring SIP settings](#)

Working with Call Detail Records

The MCU can display up to 20 pages of Call Detail Records. However, the MCU is not intended to provide long-term storage of Call Detail Records. If you intend to use the CDR log for purposes such as billing or reporting, you should download the Call Detail Records and store them independently of the MCU.

CDRs are logged to the MCU's dynamic memory unless you enable permanent storage. The memory will hold a comparatively small number of records, the oldest of which are deleted as new ones are stored.

If you enable permanent storage the logs are written to the MCU's permanent storage, which can hold a much greater number of records. However, when the allocated CDR log storage is full, the oldest logs are deleted as new ones are stored.

To view and control the CDR log, go to **Logs > CDR log**. Refer to the tables below for details of the options available and a description of the information displayed.

- [Call Detail Record log controls](#)
- [Call Detail Record log](#)

Call Detail Record log controls

The CDR log can contain a lot of information. The controls in this section help you to filter the display to show the information you find most useful. When you have finished making changes, click **Update display** to make those changes take effect. Refer to the table below for a description of the options:

Field	Field description	Usage tips
Current status	This field indicates whether CDR logging is enabled or disabled. Use (Enable CDR permanent storage and Disable CDR permanent storage) to change status.	<p>Enabling or disabling CDR logging has immediate effect. There is no need to press Update display after selecting one of these buttons.</p> <p>On the MCU 4200 series, MCU 4500 series and on the MCU MSE 8420, ensure that there is an external compact flash card in the slot on the front of the MCU.</p> <p>The MCU 5300 and MCU MSE 8510 have internal memory cards.</p>
Messages logged	The current number of CDRs in the log.	
Filter string	Use this field to limit the scope of the displayed Call Detail Records. The filter string is not case-sensitive.	The filter string applies to the Message field in the log display. If a particular record has expanded details, the filter string will apply to these as well.
Expand details	By default, the CDR log shows only brief details of each event. When available, select from the options listed to display more details.	Selecting <i>All</i> will show the greatest amount of detail for all messages, regardless of which other options are selected.

Call Detail Record log

This table shows the logged Call Detail Records, subject to any filtering applied (see [Call Detail Record log controls](#), above). The fields displayed and the list's associated controls are described below:

- [Downloading and clearing the log](#)
- [CDR log display](#)

Downloading and clearing the log

The CDR log includes all stored Call Detail Records, and all available details, regardless of the current filtering and display settings. You can download all or part of the CDR log in XML format using the web interface. When you start logging, the download button shows the range of record numbers but the delete button is grayed out until the log holds a certain number of logs.

To download the CDR log, click **Download as XML** to download all the log or **Download X to Y as XML** to download a range of events. (Note that if there are a large number of logged Call Detail Records, it may take several seconds to download and display them all.)

Note: Only download CDRs when the unit is not under heavy load, otherwise performance of the unit may be impaired.

The range of logs that you can download to the web interface works in groups. Therefore you may see **Download X to Y as XML** and Y will not increase even though the log is filling up. When a threshold is reached, then Y increases. However, you always have the option to download the full log with **Download as XML**.

In addition the web interface displays a maximum of 20 pages. If the log includes more events than can be displayed on those pages, the more recent events are displayed. Therefore you may see **Download X to Y as XML** where X keeps increasing when the page is refreshed. Again you can download the full log with **Download as XML**.

To clear the CDR log, click **Delete X to Y**. This will permanently remove Call Detail Records X to Y. Due to the way the CDR log works, it may not be possible to delete all records; the button name indicates which records can be deleted. For example, if you delete the 0-399 entries, then the 400th entry appears as the first entry in this page, even if you download the full log. The download button would then show that you can download for example 400-674 (if 674 is the maximum number of entries in the log) and the delete button will be grayed out again (because it is only available when a certain number of entries are in the log).

To avoid duplicate entries when you download repeatedly, each time delete the entries that you have just downloaded.

CDR log display

The CDR log list shows some or all of the stored records, depending on the filtering and display settings (see [Call Detail Record log controls](#)). Click on a column heading to sort by that field. Refer to the table below to understand the fields displayed in the CDR log list:

Field	Field description	Usage tips
# (record number)	The unique index number for this Call Detail Record.	

Time	The time at which the Call Detail Record was created.	Records are created as different conference events occur. The time the record was created is the time that the event occurred. Incoming CDR log events are stored with the local time stamp (not UTC). Changing the time (either by changing the system time or via an NTP update) causes new events in the CDR log to show the new time. No change will be made to existing logged CDR events
Conference	The number of the conference to which this record applies	Each new conference is created with a unique numeric index. All records pertaining to a particular conference display the same conference number. This can make auditing conference events much simpler.
Message	The type of the Call Detail Record, and brief details, if available.	The display settings allow you to display more extensive details for different record types. The filter string allows you to select for display only records where a particular word or string occurs.

Related topics

- [Working with the event logs](#)
- [Displaying and resetting system time](#)
- [Understanding security warnings](#)

Feedback receivers

The MCU publishes feedback events so that any receivers listening to the MCU can take action when something changes. To see the list of feedback receivers, click [Logs > Feedback receivers](#).

Each receiver in the list has the following details:

Field	Field description	Usage tips
Index	The position of the receiver in the list of receivers.	
Receiver URI	The fully qualified URI of the receiver.	The receiver may be a software application, for example Cisco TelePresence Management Suite, that can respond to the feedback events with an appropriate API call to retrieve the list of changes from the feedback source.
Source identifier	A string that the source will provide to the receiver when it is queried or when it publishes feedback events.	The string is optional and defaults to port A's MAC address on the source.

Customizing the user interface

On this page:

- Configuring user interface settings:
 - [Controlling the auto-refreshing of status pages on the MCU](#)
 - [Controlling the display of thumbnail preview images](#)
 - [Controlling the confirmation of participant disconnections](#)
 - [Toggling the controls for muting audio and stopping video of conference participants](#)
- [Controlling the availability of public pages](#)
- [Configuring welcome messages on the Login and Home pages](#)
- [Customizing voice prompts on the MCU](#)
- [Customizing auto attendant and text overlay fonts](#)

The MCU provides you with options for customizing the voice prompts, the viewing of thumbnail previews, the text of the welcome messages and for controlling the auto-refreshing of user interface pages.

Note: the user interface (that is the text you see on the web interface of the MCU) can be localized by Cisco. This type of customization is the localization of the text on the web interface and these online help pages. That is, the text has been translated into your local language. In the case where you have a localized MCU, the **Use localization package** check box will be selected. For more information refer to [Customization: more information](#).

Some localization packages are available at ftp.tandberg.com/pub/software/language_packs/codian/.

The MCU allows you to type using any character set when entering text into the web interface. For example, when naming endpoints or users, you can use any character set you require.

Configuring user interface settings

Controlling the auto-refreshing of status pages on the MCU

Some pages on the MCU can auto-refresh to ensure that the information displayed is current.

Caution: Auto-refreshing pages keep web sessions alive indefinitely meaning that an administrator login will never timeout. This may be considered to be a security weakness. Also, auto-refresh can impact performance on an MCU that is otherwise heavily loaded, particularly if multiple users are auto-refreshing the web interface.

To control the auto-refreshing of status pages on the MCU:

1. Go to **Settings > User interface**.
2. Choose the time interval for page auto-refreshes or, to stop pages from auto-refreshing, choose **No auto-refresh** (default).
The status pages affected by this control are as follows:
 - **Status > General**
 - **Status > Health**
 - **Status > Conferences**
 - **Status > Cluster** (Note that this page is only available on clustered MSE 8510 Media blades.
 - **Conferences > Conference name > Participants**

- [Conferences > Conference name > Statistics](#)
- [Conferences > Conference name > Participant > Statistics](#)
- [Conferences > Conference name > Participants > Content channel](#)

3. Click **Apply changes**.

Controlling the display of thumbnail preview images

To control the display of thumbnail preview images on the MCU:

1. Go to [Settings > User interface](#).
2. Choose whether you want to **Show video thumbnail images** or not. This controls whether or not you will see a preview of what an endpoint sees in the conference and participants pages that can show a preview of the conference. Note that thumbnail images will not be shown for conferences where encryption is required.
3. Click **Apply changes**.

Controlling the confirmation of participant disconnections

The default settings for the MCU allow you to disconnect, without confirmation, individual participants from a conference on the [Conference list > Conference > Participants](#) page. On the [Settings > User interface](#) page, you can configure the MCU to display an "Are you sure?" confirmation box when attempting to disconnect an individual participant. Note that all-participant disconnections always require confirmation.

To control the confirmation of individual-participant disconnections:

1. Go to [Settings > User interface](#).
2. If you want attempted individual-participant disconnections to require confirmation, enable the **Confirm individual participant disconnections** option and click **Apply changes**.

Toggling the controls for muting audio and stopping video of conference participants

Using the default settings of the MCU, a conference's [Conference list > Conference > Participants](#) page displays controls that allow the muting of a participant's audio and video channels. The [Settings > User interface](#) page allows you to control the presence or absence of these controls:

1. Go to [Settings > User interface](#).
2. For **Participant list controls**, select the control(s) that you want to appear on the [Participant list](#) page.

Controlling the availability of public pages

You can allow users access to the conference list pages without having to authenticate with the MCU.

By default, these pages are accessible to users who have not logged in. However, you can disable access as follows:

1. Go to [Settings > User interface](#).
2. In the **Public pages** section, enable **Conference list** as you require.
3. Click **Apply changes**.

Configuring welcome messages for the Login and Home pages

You can configure a message banner to appear on the Login page of the MCU. For example, some organizations might require some legal text on the login page of the MCU. You can also configure a message banner to appear on the Home page. You can configure a separate title (maximum: 100 characters) and text (maximum: 1500 characters) for each banner. To configure the message banners:

1. Go to **Settings > User interface**.
2. In the **Welcome messages** section, enter the text you require for the titles and the text of the messages.

Adding headers and footers

You can optionally configure header and footer text, with up to 100 characters each. The headers and footers will display on each page of the web user interface (except the help):

1. Go to **Settings > User interface**.
2. In the **Header and footer messages** section, enter the required text for the header and/or footer.
3. Click **Apply changes**.

Changes to headers or footers are recorded in the **Event log** and the **Audit log**.

Customizing voice prompts on the MCU

By default the MCU includes English voice prompts spoken by an American woman.

These prompts are used by the MCU to provide callers with information, for example: "Connecting you to your destination".

You may want to replace these prompts with your own in order to change the wording, language or accent used. Alternative prompts may be uploaded individually using the web interface. Alternatively, a collection of voice prompts may be uploaded in one go by means of a *resource package* (see [Uploading a customization package](#)).

Some customization packages are available on the [TANDBERG FTP site](#).

The customization of voice prompts is controlled via the web interface. Go to **Settings > User interface**. Refer to the sections below for details of the options available and for a description of the information displayed:

- [Using default US English voice prompts](#)
- [Uploading a customization package](#)
- [Viewing the available voice prompts](#)
- [Uploading and downloading customized voice prompts](#)
- [Voice prompt specification](#)
- [Making the best possible recordings](#)

Using default US English voice prompts

The default set of voice prompts is provided in US English and is the standard set of voice prompts supplied with the MCU. These are spoken by a female voice in Americanized English.

If your MCU is using customized voice prompts and you want to return to using the default set of voice prompts:

1. Go to **Settings > User interface**.
2. In the **Select customization** section, clear **Use customized voice prompts**.
3. If your MCU was provided to you as a localized MCU, clear **Use localization package** (this disables the package).
4. Click **Apply changes**.

Note: clicking **Delete** permanently removes the package from the MCU.

The default voice prompts will be applied immediately, although it may take a few seconds before everyone connected to the MCU is able to hear the new prompts.

Uploading a customization package

It is possible to upload a collection of alternative voice prompts to the MCU with a single upload operation, using a *customization package*. Such a package may have been supplied to you by Cisco or one of its representatives, or you may have created the package yourself (see [Downloading a customization package](#)).

To upload a package:

1. Go to **Settings > User interface**.
2. In the **Upload customization package** section, click **Browse** and locate the *.package* file on your computer.
3. Click **Upload package**.

The upload may take several seconds, depending on the size of the package file and the speed of your network connection. When the upload is complete, a status screen will be shown, displaying some or all of the individual voice prompt customizations included in the package if the upload was a success, or an error message if the upload failed for some reason.

To apply the uploaded customization package:

- In the **Select customization** section, select **Use customized voice prompts**.

Note: If you were already using uploaded alternative voice prompts on the MCU, then these will be immediately replaced by those in the customization package. If a particular customized file is not included in the package, then any existing customization is unchanged. This allows customization sets to be built up using several different packages if required.

Viewing the available voice prompts

You may review the voice prompt customizations available in the table headed **Voice prompts**. The **Voice prompts** list displays all voice prompt customizations, providing details for those which have alternatives uploaded. Because these lists can be quite long, by default they are hidden. Instead, the number of customizations (files) available is shown. If any have been modified (meaning an alternative customization

has been uploaded, either individually, or as part of a package), then this is indicated by an asterisk after the table name.

To expand any list to show all customizations, click **show file details**; you may subsequently hide it again by clicking **hide file details**.

In the expanded state, the table shows, for each customization, a description of the file, the standard MCU filename for the customization, and the length and date modified (uploaded) of alternative customizations present. Extra information is provided by the following symbols:

- Customizations where an alternative is available that can be individually uploaded or downloaded are indicated by two asterisks (**) after their name
- Customizations where an alternative is available that cannot be uploaded or downloaded individually are indicated by one asterisk (*) (these are files that have been provided by Customer support)
- Customizations that are part of a localization package from Cisco are indicated by a plus sign (+)

Uploading and downloading customized voice prompts

Refer to the sections below for details of further functionality provided by the **Installed voice prompts** list:

- [Uploading individual voice prompts](#)
- [Downloading individual voice prompts](#)
- [Downloading a customization package](#)
- [Deleting customized voice prompts](#)

Uploading individual voice prompts

You may upload individual voice prompts. To do this:

1. Go to **Settings > User interface**.
2. In the **Installed voice prompts** section, click **show files details** and locate the voice prompt file you require.
3. For that voice prompt, click **upload**. You may do this regardless of whether an alternative customization has already been uploaded.
4. You will be presented with a new screen, allowing you to locate and upload the customization of your choice. Click **Browse** to locate the voice prompt file on your computer. Voice prompt files must be in the following format:
 - Microsoft WAVE (.WAV) format
 - 16kHz (16000Hz) sample rate
 - Mono
 - Uncompressed
 - Maximum 10 seconds long

If you upload a file that is not in this format, the upload may fail or the voice prompt may sound distorted when heard by users. Use an audio editing package of your choice to make any conversions required. See [Making the best possible recordings](#) for how to obtain the best possible voice prompts for your MCU customization.

Note that in addition to the 10 second length limit per prompt, there is a total length limit of four minutes for the full set of prompts. That is, if all samples were played back-to-back, it should take no more than 240 seconds.

5. When you have located the file you want to upload, click **Upload customization**. If the upload is successful, a page displaying the size of the file uploaded will be displayed; otherwise an error will be

shown. If the upload fails, check your audio file matches the specification above before contacting your support representative.

Downloading individual voice prompts

You may want to review a customization that has been previously uploaded to the MCU. To do this,

1. Go to **Settings > User interface**.
2. In the **Installed voice prompts** section, locate the voice prompt file you require.
3. For that voice prompt, right-click **download** and choose **Save Target As** (or your web browser's equivalent operation). The file will be downloaded to your computer for reference.

Only alternative customizations can be downloaded in this way; the default voice prompts may not be downloaded. In addition, only customizations uploaded as individual files may be downloaded; those uploaded as part of a package may not be downloaded.

Downloading a customization package

Once you are satisfied with your customizations, you may want to apply the entire set to another MCU. Rather than individually uploading the alternative voice prompts to each one, you may create a *customization package*.

To create a customization package containing all of the alternative voice prompts previously uploaded:

1. Go to **Settings > User interface**.
2. Click **Download package** at the bottom of the **Installed voice prompts** list. The customization package will be downloaded to your computer.

A package may only contain resources uploaded as separate files; those uploaded as part of another package may not be included. The package download option may be unavailable if no voice prompts qualify for inclusion.

Deleting customized voice prompts

If you are dissatisfied with a voice prompt that you have uploaded to the MCU, you may delete it in the following manner:

1. Locate the voice prompt of interest in the list.
2. Click the check box to the left of the voice prompt.
3. Click **Delete selected** to remove the voice prompt.

Only alternative voice prompts may be deleted in this way; the default voice prompts cannot be deleted. If you delete an alternative customization, it will immediately revert to the default prompt, even if you have selected **Use customized voice prompts** at the top of the page.

You may want to delete all customizations. To do this, click **Delete all**. Remember that you may revert to the default set of voice prompts without needing to delete any alternative customizations (see [Using default voice prompts](#)).

Voice prompt specification

Below is a complete list of the voice prompts that may be customized. The default wording is shown for each prompt. You do not have to use exactly the same wordings if they are not appropriate for your needs, and are provided only as a guide.

Filename	Default wording
voice_prompt_conference_already_exists	I'm sorry, there is already a conference with that number
voice_prompt_conference_over	Your conference is now over. Goodbye
voice_prompt_connect_now	I'll connect you to your conference now
voice_prompt_enter_conference_id	Please enter the conference code now
voice_prompt_enter_conference_id_or_create	Please enter the conference number followed by the pound key, or press star to create a new conference
voice_prompt_enter_conference_pin	Please enter the security PIN for this conference now
voice_prompt_enter_new_conference_id	Please enter the conference number for the conference you are creating, followed by the pound key
voice_prompt_enter_new_conference_pin	Please enter the PIN for the conference you are creating, followed by the pound key; if you don't want a PIN, just press the pound key
voice_prompt_enter_new_conference_pin_short	Please enter the PIN for the conference you are creating, followed by the pound key
voice_prompt_enter_pin	Please enter the security PIN followed by the pound key
voice_prompt_fecc_usage	To join a conference you may use the far-end camera controls on your remote
voice_prompt_first_participant	You are the first participant to join the conference
voice_prompt_pin_incorrect	Sorry, I did not recognize that security PIN, please try again
voice_prompt_two_minutes	Your conference is scheduled to end in two minutes
voice_prompt_unknown_conference	Sorry, I did not recognize that conference code, please try again
voice_prompt_waiting_for_chairperson	Waiting for conference chairperson
voice_prompt_welcome	Hello, welcome to the conferencing system

Making the best possible recordings

There are many factors to consider when recording alternative voice prompts in order to get the best results. Below is a summary of the points to bear in mind.

Recording format

It is best to make each recording with the ideal settings and hence avoid any sample-rate or resolution changes. As discussed, the ideal format is Microsoft Wave (.WAV) format, uncompressed, mono, at 16 kHz and 16-bit resolution.

If you are unable to make mono recordings, the MCU can convert stereo recordings.

Background noise

It is important to minimize background noise (hiss) as much as possible. This includes ambient noises such as road noise and slamming doors etc. but also try to keep fan noise and similar to a minimum.

When played back by the MCU, samples with background noise are very apparent.

Consistency

If possible, record all voice prompts in one session. This will ensure that all voice and background conditions remain constant and the recorded voice will sound similar from prompt to prompt.

Volume

Record prompts using a relatively constant loudness of voice. Although it may take some trial and error, the best recordings will result from speaking loud enough that the voice is recorded loudly compared to any residual background noise, but not so loudly that it sounds distorted when played back.

Customizing auto attendant and text overlay font

A Cisco-supplied TrueType font is used for auto attendant and overlay text. This file is installed by default but, if it is not present on your MCU, it is also available from the software downloads area of the Cisco website.

To upload a font file:

1. Go to **Settings > User interface**.
2. In the **Overlay text** section, click the **Browse** button next to the **New font file** field.
3. Locate the required font file and click **Upload font**. The **Font file status** changes to **Present**.

Related topics

- [Upgrading and backing up the MCU](#)
- [Customization: More information](#)

Customization: More information

There are three customization levels on the MCU (for voice-prompts, web interface, help pages, and text messages):

- the factory default files that are provided in US English
- localization files that are sometimes installed by a reseller
- customized voice prompts files that can be uploaded and downloaded by you

Precedence

For every customizable file:

1. If there is a customization file present and **Enable customized files** is selected, that file will be used.
2. Otherwise, if **Use localization package** is selected, the MCU will use the localized file.
3. If 1 and 2 are not true, then the MCU will use the default US English file.

The factory default file set

The files that compose the default file set for the web interface, the voice prompts, the help pages, and text messages cannot be deleted. If you are using your own customization files or a localized MCU, you can return the MCU to using the default file set:

To return to the defaults:

1. Go to **Settings > User interface**.
2. Ensure both **Use localization package** and **Use customized voice prompts** are cleared.

Note that the default voice prompts will be used where there is no alternative voice prompt available, even if **Use customized voice prompts** is selected.

Localization files

In some parts of the world, MCUs are available where the help pages, the voice prompts, the text messages, and some of the web interface are in the local language. In this case, Cisco or the reseller has uploaded a package that provides localized files to replace files in the default file set. If you have a localized MCU, you are able to return to the default US English file set (see above). Localization is a global change and affects all customizable files. If you have a localized MCU, you cannot upload and download localized files on a file by file basis.

Some customization packages are available at ftp.tandberg.com/pub/software/language_packs/codian/.

Customization files

Customization files for voice prompts can be recorded and uploaded by any admin user of the MCU. These files can be uploaded one by one or as a package. You can create your own package by uploading all the files you require to an MCU and then downloading them as a package. For more information, refer to [Customizing the user interface](#). A customization package does not have to include a complete set of files. Where a file name duplicates an existing uploaded voice prompt file, that file will be overwritten.

Network connectivity testing

The Network connectivity page can be used for troubleshooting issues that arise because of problems in the network between the MCU and a remote video conferencing device being called (or a device from which a user is attempting to call the MCU).

The Network connectivity page enables you to attempt to 'ping' another device from the MCU's web interface and perform a 'traceroute' of the network path to that device. The results show whether or not you have network connectivity between the MCU and another device. You can see from which port the MCU will route to that address. For a hostname, the IP address to which it has been resolved will be displayed.

To test connectivity with a remote device, go to **Network > Connectivity**. In the text box, enter the IP address or hostname of the device to which you want to test connectivity and click **Test connectivity**. Note that IPv6 addresses must be enclosed in square brackets.

For each successful 'ping', the time taken for the ICMP echo packet to reach the host and for the reply packet to return to the MCU is displayed in milliseconds (the round trip time). The TTL (Time To Live) value on the echo reply is also displayed.

For each intermediate host (typically routers) on the route between the MCU and the remote device, the host's IP address and the time taken to receive a response from that host is shown. Not all devices will respond to the messages sent by the MCU to analyse the route; routing entries for non-responding devices is shown as <unknown>. Some devices are known to send invalid ICMP response packets (e.g. with invalid ICMP checksums); these responses are not recognized by the MCU and therefore these hosts' entries are also shown as <unknown>.

Note: The ping message is sent from the MCU to the IP address of the endpoint that you enter. Therefore, if the MCU has an IP route to the given IP address, regardless of whether that route lies out of port A or port B, the ping will be successful. This feature allows the MCU's IP routing configuration to be tested, and it has no security implications.

Note: If you are unable to ping the device then check your network configuration especially any firewalls using NAT.

Related topics

- [Configuring network settings](#)

Configuring SSL certificates

The MCU supports certificate-based user authentication over HTTPS, and is capable of mutual TLS authentication with the client. The client presents a certificate, signed by a certificate authority (CA), which the MCU trusts if it recognizes the CA from its trust store. Similarly, the client requests the MCU's local certificate and checks the signing CA against its own trust store.

To manage the MCU's local certificate and its trust stores for HTTPS and SIP TLS, and optionally to configure OCSP checks (Online Certificate Status Protocol) for HTTPS connections, go to **Network > SSL certificates**.

The SSL certificates page is also used to allow or enforce certificate-based login in place of standard, password-based login. Any attempts to authenticate with a revoked certificate are recorded in the MCU's **Audit log**.

In this topic:

- [Prerequisites](#)
- [Managing trust stores](#)
- [Configuring SIP verification](#)
- [Configuring HTTPS verification](#)
- [Configuring client certificate security](#)
- [Configuring server certificate security](#)
- [OCSP checks for client certificate revocation](#)
- [Certificate details reference](#)

Prerequisites

You should have your own local certificate and trust store(s), which must be in .pem format (Base64 encoded text).

HTTPS access to the web user interface requires the following prerequisites:

- The *Secure management (HTTPS)* or *Encryption* feature key must be installed on the MCU.
- HTTPS must be enabled on the **Network > Services** page.

To make SIP TLS calls between the MCU and remote parties requires the following prerequisites:

- The *Encryption* feature key must be installed on the MCU.
- A SIP username and password that are known by the registrar must be added to the **Settings > SIP** page.
- The **Encrypted SIP (TLS)** checkbox on the **Network > Services** page should be checked, for either IPv4 or IPv6, or both (depending on your requirements).
- The **Use local certificate for outgoing connections and registrations** checkbox should be checked if your environment dictates that the SIP registrar must receive the MCU's certificate.

Caution: A local certificate and private key are pre-installed on the MCU and are used by default for HTTPS access. As all MCUs have identical default certificates and keys, to ensure security we recommend that you replace it with your organization's own certificate and private key (see below).

Managing the local certificate

Uploading a local certificate and private key

1. Go to **Network > SSL certificates**.
2. Go to the **Local certificate configuration** section.
3. Click **Browse** for the **Certificate** field to navigate to the certificate *.pem* file.
4. Click **Browse** for the **Private key** field to navigate to the private key file that accompanies your certificate.
You must upload the certificate and its key simultaneously.
5. In the **Private key encryption password** field, type the relevant password.
6. Click **Upload certificate and key**.
The uploaded certificate overwrites the previously held certificate.
7. Restart the MCU.

Deleting a local certificate and private key

1. Go to the **Local certificate** section.
2. Click **Delete custom certificate and key**.
3. Restart the MCU.

Managing trust stores

A trust store is a collection of certificates from intermediate and root certificate authorities against which the MCU can attempt to verify client certificates it receives.

The MCU can hold three trust store files - one for HTTPS connections, one for SIP TLS connections and one for Call Home connections to verify the connection to the Smart Call Home server. When you upload a new trust store file, the previously held file is overwritten. The MCU has a certificate pre-installed, however, it is possible to delete and upload new certificates. You can also reset the certificate to default.'

Putting multiple CA certificates in a trust store

1. Open the first certificate in a text editor, and save it as *yourfilename.pem*.
2. Open the next certificate in your text editor, and copy all the lines from `-----Begin Certificate---` to `-----End Certificate-----` (inclusive).
3. Paste the text block at the end of *yourfilename.pem*.
Repeat this to copy as many certificate blocks into your *.pem* file as you need to, making sure not to modify any of the pasted text.
4. Save the resulting file.

Uploading a trust store

1. Go to **Network > SSL certificates**.
2. Go to the appropriate trust store configuration section (either the **SIP trust store**, **HTTPS trust store** or **Call Home trust store**).
3. Click **Browse** to navigate to your trust store *.pem* file (eg. *yourfilename.pem*).

4. Click **Upload trust store**.
5. Confirm that you wish to proceed.
The trust store is uploaded, replacing the previous one (if it existed).
Each certificate in the trust store appears in its own table row that shows pertinent certificate details in plain text.

Deleting a trust store

1. Go to **Network > SSL certificates**.
2. Go to the appropriate trust store configuration section (either the **SIP trust store**, **HTTPS trust store** or **Call Home trust store**).
3. Click **Delete trust store**.
4. Confirm that you wish to proceed.
The trust store is deleted.

Resetting the Call Home trust store to default

1. Go to **Network > SSL certificates**.
2. Go to the **Call Home trust store** configuration section.
3. Click **Reset trust store to default**.
4. Confirm that you wish to proceed.
The trust store is reset to default.

Configuring SIP TLS verification

You can configure the MCU to secure incoming and outgoing SIP calls using TLS. The MCU uses its SIP trust store to verify the certificate presented by the remote end of a SIP TLS connection.

1. Go to **Network > SSL certificates**.
2. Go to the **SIP trust store** section.
3. Select one of the options from the **Verification settings** field.
4. Click **Apply changes**.

SIP verification options	
No verification	All outgoing connections are permitted, even if the remote end does not present a valid and trusted certificate (remote end always trusted).
Outgoing calls only	Outgoing SIP TLS connections are only permitted if the remote end has a trusted certificate.
Outgoing and incoming calls	Outgoing and incoming SIP TLS connections are only permitted if the remote end has a trusted certificate.

Certificate identity requirements for SIP TLS

For an outgoing SIP TLS call, when inspecting the received certificate as part of the SIP TLS handshake, the MCU looks for either an IP address or a domain identifier for the remote party in the **URI** and **DNS** fields of the certificate's subject alternative name (**subjectAltName**) extension. If the **subjectAltName** is not

present, the MCU looks for either an IP address or a domain identifier in the certificate's Common Name (**CN**) field.

For an incoming SIP TLS call, the received certificate should be trusted by MCU's SIP Trust store.

You should ensure that the certificates presented by your SIP entities to the MCU contain both the SIP URI and the IP address of the entity.

The remote party must similarly be able to verify the MCU's local certificate against its trust store, so the local certificate must also be generated according to the guidelines above.

Note: If you require TLS on non-proxied SIP calls from the MCU, the MCU's local certificate must identify the MCU by its IP address. This requirement arises because the remote endpoint will be establishing TLS connections directly to the MCU, which provides its IP address as its identity.

Configuring HTTPS verification

The **HTTPS trust store** section is where you can configure certificate-based authentication for users logging in to the web interface and for applications interacting with the API. This section also lets you configure whether the MCU should verify server certificates, presented by an OCSP server or by feedback receivers, before allowing these connections.

CAUTION: If you transition from solely password-based client authentication to *any* level of certificate-based client authentication (including those that permit but do not require certificates), it is possible inadvertently to block client access to the MCU. This can happen if HTTP is disabled or if HTTP to HTTPS redirection is enabled. In such cases, a certificate that is trusted by the MCU must be presented by the client side (typically you the administrator) in order to log in. If no such client certificate exists then no one can log in.

We strongly recommend that you first review the option descriptions below and then follow the process in [Transitioning to certificate-based security](#).

Configuring client certificate security

1. Go to **Network > SSL certificates**.
2. Go to the **HTTPS trust store** section.
3. Select one of the options from the **Client certificate security** field.
4. Click **Apply changes**.

Client certificate security options	
Not required	Certificate-based client authentication is not required (default) and client certificates are ignored. Password-based authentication is required for all client access, whether by users over HTTPS or applications making API calls.
Verify certificate	Incoming HTTPS connections are only permitted if the client certificate is signed by an authority that the MCU trusts, but password-based login is <i>still required</i> to authenticate the client, for HTTPS, API, and other client connections.
Certificate-based authentication allowed	Incoming HTTPS connections are only permitted if the client certificate is signed by an authority that the MCU trusts and, if the certificate's common name matches a stored username, the client logs in as that user. However, if the certificate is trusted and the common name does not match, the client may log in with username and password.

Certificate-based authentication required	<p>Incoming HTTPS connections are only permitted if the client certificate is signed by an authority that the MCU trusts. The common name of the certificate must also match a stored username and password-based client authentication is not allowed.</p> <p>HTTP and FTP logins are blocked. If Require administrator login is checked (on Settings > Security), then console access is restricted to functions that do not require a login.</p> <hr/> <p>Note: The MCU requires every user account to have a password, even if <i>Certificate-based authentication required</i> is selected and thus clients may not use their passwords. Furthermore, if the MCU is in advanced account security mode, passwords must be replaced every 60 days. Users are not prompted to change their passwords when they log in using certificate-based authentication, so the passwords will expire and generate security warnings.</p> <hr/> <p>For the purpose of any timed access restrictions that exist on user accounts (typically password change intervals and inactive account expiry rules) any log in using a certificate is treated as a standard password-based login and will reset the timer accordingly.</p> <p>For information about how these options affect the API interface, see the <i>Cisco TelePresence MCU API Reference Guide</i>.</p>
--	--

Configuring server certificate security

1. Go to [Network > SSL certificates](#).
2. Go to the [HTTPS trust store](#) section.
3. Select one of the options from the **Server certificate security** field.
4. Click **Apply changes**.

Server certificate security options	
No verification	The MCU does not verify the server's certificate (if one is presented) when it makes an OCSP request or when it sends HTTPS feedback messages.
Verify certificate	The MCU requires a server certificate from the OCSP server or feedback receiver, and must be able to verify that the certificate is trusted by one of the authorities in its HTTPS trust store, before it completes the OCSP request or sends the HTTPS feedback message.

OCSP checks for client certificate revocation

You can optionally configure an external OCSP server, which the MCU will use to check the revocation status of client certificates presented with incoming HTTPS connection requests. The following details describe the MCU's OCSP checking mechanism.

- For chained certificates the OCSP check is performed only against the leaf certificate.
- The MCU supports SHA-1 hashing for OCSP.
- If the response from the OCSP server is anything other than *'good'* (that is, the client certificate is invalid, revoked, unknown, timed out, or in some other error condition) the MCU rejects the associated connection request.
- No further OCSP checking takes place after the connection is established. An active session will continue if a certificate is revoked during that session, but any subsequent connection attempts with the revoked certificate will be rejected.

CAUTION: If you enable OCSP checking for the MCU it is possible inadvertently to block *all* login access (including administrators) to the MCU. If you want to enable OCSP checking, we strongly recommend that you first review the option descriptions below and then follow the process in [Transitioning to certificate-based security](#).

Configuring the OCSP connection

1. Go to **Network > SSL certificates**.
2. Go to the **Online certificate status protocol (OCSP)** section.
3. Select *HTTPS certificates* in the **Certificates to check** field.
When you click **Apply changes**, the OCSP check for HTTPS certificates will be enabled; if you select *None* you will disable the check.
4. Enter the server address in the **OCSP server** field.
5. Check the **Require nonce** checkbox if the server requires this extra level of security.
6. Enter the **Maximum clock skew of OCSP server**, in seconds.
7. Enter the **Maximum age of OCSP server records**, in days.
8. Click **Apply changes**.

OCSP details reference

Online certificate status protocol (OCSP) field descriptions	
Certificates to check	<i>None</i> to disable OCSP checks or <i>HTTPS client certificates</i> to enable OCSP checks of HTTPS client certificates' revocation status.
OCSP server	<p>The URL of the external OCSP server.</p> <ul style="list-style-type: none"> ■ If the default port allocation is sufficient (port 80 for HTTP and port 443 for HTTPS) use one of these formats, as appropriate: <i>http://example.com</i>; <i>https://example.com</i>; <i>http://example.com/examplepath</i>; <i>https://example.com/examplepath</i> ■ To send to a non-standard port number (port 88 is used in the examples here) use one of these formats, as appropriate: <i>http://example.com:88</i>; <i>https://example.com:88</i>; <i>http://example.com:88/examplepath</i>; <i>https://example.com:88/examplepath</i>
Require nonce	<p>Determines whether OCSP queries must include a nonce extension (to prevent replay attacks).</p> <ul style="list-style-type: none"> ■ If enabled, the MCU includes a nonce in each OCSP request, and requires the nonce to be returned in the corresponding response. If the nonce is not returned, the associated connection request is rejected. ■ If disabled, the MCU does not send a nonce in OCSP requests.
Maximum clock skew of OCSP server	Specifies the maximum acceptable time (in seconds) for clock skew in OCSP responses. In this context the skew is the divergence between the respective system clocks on the MCU and on the OCSP server. If the skew exceeds this setting, then the OCSP responses may be treated as invalid.
Maximum age of OCSP server records	<p>Specifies the maximum acceptable age (in days) for certificates. The certificate age is derived from the response field <i>'thisUpdate'</i> which indicates when the returned status was last known to be correct. How this value is determined depends on the OCSP server configuration (often it is the last time the server was updated with a new Certificate Revocation List).</p> <p>The MCU rejects any response where the value of <i>'thisUpdate'</i> is later in the past than the time derived by counting back from current time by the number of days specified here (after accounting for clock skew).</p>

Certificate details reference

Field	Description
Subject	The business to which the certificate has been issued: <ul style="list-style-type: none">■ C Country where the business is registered■ ST State or province where the business is located■ L Locality or city where the business is located■ O Legal name of the business■ OU Organizational unit or department■ CN Certificate common name, or the domain name
Issuer	The issuer of the certificate. Where the certificate has been self-issued, these details are the same as for Subject .
Issued	Date on which the certificate was issued.
Expires	Date on which the certificate will expire.
Private key	Your web browser uses the SSL certificate public key to encrypt the data that it sends back to the MCU. The private key is used by the MCU to decrypt that data. The private key field is only present for the local certificate.

Related topics

- [Configuring security settings](#)
- [Configuring IP services](#)
- [Transitioning to certificate-based security](#)

Transitioning to certificate-based security

Certificate-based security methods carry a risk of inadvertently blocking all login access to the MCU. (If problems occur with the client certificate or the trust store, you will need to fall back to HTTP. If you cannot fall back — because HTTP is disabled or because HTTP to HTTPS redirection is set — then all access methods will be blocked.) We strongly recommend that you follow the procedure below when implementing certificate-based security:

- [Enabling client certificates and certificate login \(HTTPS connections\)](#)
- [Enabling OCSP checking](#)
- [Requiring certificate-only login \(all connections\)](#)

Enabling client certificates and certificate login (HTTPS connections)

To transition access handling for HTTPS connections from standard, password-based access to required client certificate validation and optionally to allow certificate-based login, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the MCU (**Network > SSL certificates**) and that the web browser(s) to be used to access the MCU are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and disable **Redirect HTTP requests to HTTPS** (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
 - a. Scroll to the **HTTPS trust store** section.
 - b. Set **Client certificate security** to *Verify certificate* (to have client certificate validation but no certificate login) or *Certificate-based authentication allowed* (to have client certificate validation and to allow certificate-based login).
 - c. Click **Apply changes**.
5. Now test that you are able to log in to the MCU over an HTTPS connection.
 - a. First verify that you can log in using the standard password login mechanism.
 - b. If you specified *Certificate-based authentication allowed* in the previous step, also verify that certificate-based login is working as expected. This step is recommended, although strictly not essential as *Certificate-based authentication allowed* mode still allows password login if certificate login fails.

Note: Provided that this procedure is successful, you can now disable HTTP (**Network > Services**) or enable redirection from HTTP to HTTPS (**Settings > Security**) if either are required by your configuration.

Enabling OCSP checking

Caution: The MCU will only perform OCSP checking if client certificate security mode is enabled. To do this go to **Network > SSL certificates** and set the **Client certificate security** option. When you first enable OCSP checking, set **Client certificate security** to one of the 'lesser' modes (*Verify certificate* or *Certificate-based authentication allowed*). If you want to set it to *Certificate-based authentication required*, only do so after you have completed the procedure for [Requiring certificate-only login \(all connections\)](#) and you are certain that OCSP checking is working correctly.

To enable OCSP checking for the MCU, do the following:

1. Ensure that an appropriate HTTPS trust store has been installed on the MCU (**Network > SSL certificates**).
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable* **Redirect HTTP requests to HTTPS**. This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
 - a. Scroll to the **Online certificate status protocol (OCSP)** section.
 - b. Set **Certificate to check** to *HTTPS client certificates*.
 - c. Enter the URL of the external OCSP server and set any options you require.
 - d. Click **Apply changes**.
5. Now test that you are able to log in to the MCU over an HTTPS connection. Only proceed to the next step if you can successfully log in.
6. Do one of the following, as appropriate for your configuration:
 - Go to **Network > Services** and disable HTTP.
 - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.

Requiring certificate-only login (all connections)

To transition from password-based authentication to required certificate-based authentication for *all* connection types, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the MCU (**Network > SSL certificates**) and that the web browser(s) to be used to access the MCU are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable* **Redirect HTTP requests to HTTPS** (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**:
 - a. Scroll to the **HTTPS trust store** section.
 - b. Set **Client certificate security** to *Certificate-based authentication allowed*.
Do NOT set **Client certificate security** to *Certificate-based authentication required* yet.
 - c. Click **Apply changes**.
5. Now test that you are able to log in to the MCU over an HTTPS connection *using a certificate*. Only proceed to the next step if you can successfully log in with a certificate.
6. Assuming the previous step succeeded, go to the **Client certificate security** option again and this time set it to *Certificate-based authentication required*.
7. Click **Apply changes** and confirm at the prompt.
It is now not possible to log in over HTTP. To log in over HTTPS requires a valid client certificate signed by a certificate authority, which matches the HTTPS trust store on the MCU.
8. Do one of the following, as appropriate for your configuration:
 - Go to **Network > Services** and disable HTTP.
 - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.

Related topics

- [Configuring SSL certificates](#)
- [Configuring security settings](#)
- [Configuring IP services](#)

Further information

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2014 Cisco Systems, Inc. All rights reserved.