CHAPTER 3

Configuring the Cisco Unified Videoconferencing 3515 MCU

This section describes the following topics:

About the Cisco Unified Videoconferencing 3515 MCU Administrator Interface

In the Cisco Unified Videoconferencing 3515 MCU Administrator interface, you can configure management policies, media processing, call management protocols, and services. Table 3-1 explains the tabs that appear in the Cisco Unified Videoconferencing 3515 MCU Administrator interface.

Table 3-1 MCU Administrator Interface Tabs

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

Figure 3-1 and Table 3-2 display and list the elements in the MCU Administrator interface.

Figure 3-1 MCU Administrator Interface Elements

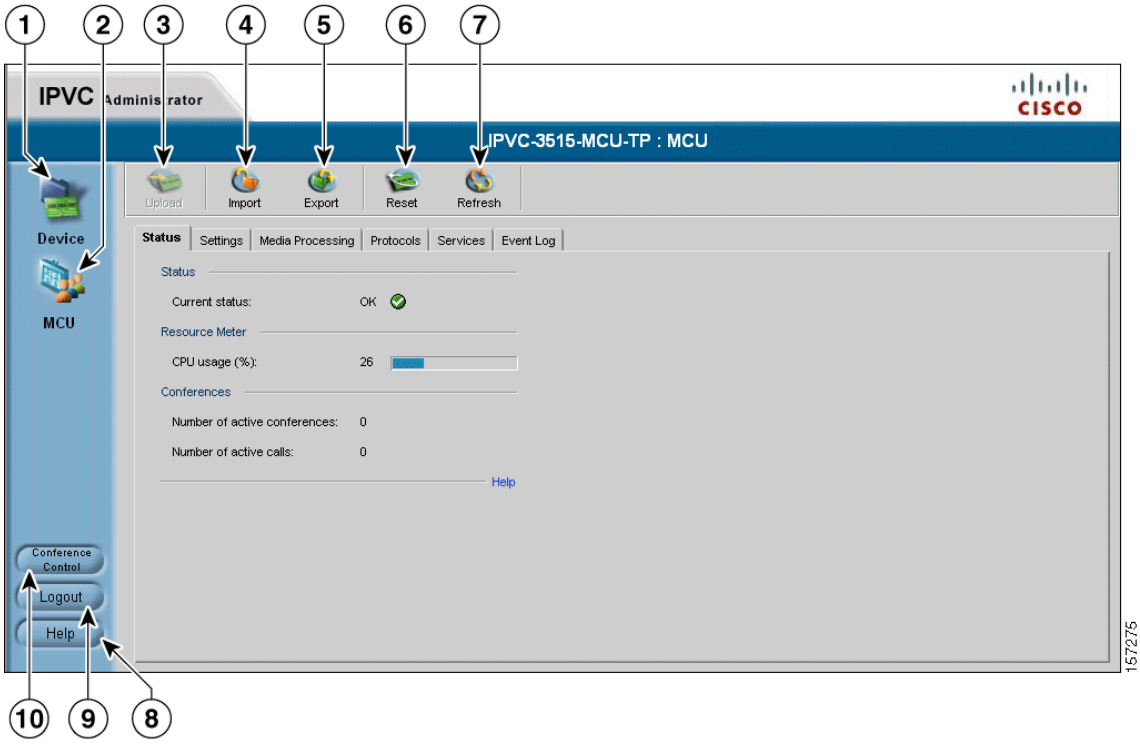


Table 3-2 MCU Administrator Interface Elements

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

About Administrators and Operators

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

- Viewing Administrators and Operators, page 3-4
- Adding Administrators and Operators, page 3-4

- Editing Administrator and Operator Settings, page 3-5
- Deleting Administrators and Operators, page 3-5

Viewing Administrators and Operators

In the Users tab, you can view user names that are registered with this MCU and their access level. Table 3-3 lists the elements that appear in the Users tab.

Table 3-3 User Tab Elements

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

Adding Administrators and Operators

In the Users tab, you can add Administrators.

Procedure

Step 1 In the Administrator interface, on the sidebar, click **Device**.

Step 2 Click the **Users** tab.

Step 3 Click **Add**.

The Add User dialog box appears.

Step 4 In the **User name** field, type the name you want the Administrator to log in with.

Step 5 In the **Access Level** field, choose the authorization level for this user:

- **Administrator**—Allows this user to launch the Administrator interface, use the Conference List that has links to web pages of current conferences, share conference chair control with another user, and access this device through Telnet, FTP, and the Cisco Upgrade Utility. You can assign up to ten users Administrator authorization.
- **Operator**—Allows this user to share conference chair control with another user and to access the Conference List that has links to web pages of current conferences. Up to 50 users can be assigned Operator authorization.

Step 6 In the **Password** field, type the password this user uses to log in with.

Step 7 In the **Repeat Password** field, re-type the password you typed in 6.

Step 8 Select the **Enable for Telnet/FTP** check box to allow this user to access this device through Telnet and FTP.

Step 9 On the toolbar, click **Upload**.

Editing Administrator and Operator Settings

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

Procedure

Step 1 In the Administrator interface, on the sidebar, click **Device**.

Step 2 Click the **Users** tab.

Step 3 Click the user you want to edit settings for.

Step 4 Click **Edit**

The Edit User dialog box appears.

Step 5 In the **User name** field, type the name you want the Administrator to log in with.

Step 6 In the **Access Level** field, choose the authorization level for this user:

- **Administrator**—Allows this user to launch the Administrator interface, use the Conference List that has links to web pages of current conferences, share conference chair control with another user, and access this device through Telnet, FTP, and the Cisco Upgrade Utility. You can assign up to ten users Administrator authorization.
- **Operator**—Allows this user to share conference chair control with another user and to access the Conference List that has links to web pages of current conferences. Up to 50 users can be assigned Operator authorization.

Step 7 In the **Password** field, type the password this user uses to log in with.

Step 8 In the **Repeat Password** field, re-type the password you typed in 6.

Step 9 Select the **Enable for Telnet/FTP** check box to allow this user to access this device through Telnet and FTP.

Step 10 On the toolbar, click **Upload**.

Deleting Administrators and Operators

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

Procedure

Step 1 In the Administrator interface, on the sidebar, click **Device**.

Step 2 Click the **Users** tab.

Step 3 Click the user you want to delete and then click **Delete**.

Viewing LED Information

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

Procedure

Step 1 In the MCU interface, on the sidebar, click **Device**.

Step 2 Click the **LED Monitoring** tab.

Step 3 Place the mouse cursor over the required LED in the LED Monitoring tab to view a description of that LED.

Viewing General Information About the MCU

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

Procedure

Step 1 In the MCU interface, on the sidebar, click **Device**.

Step 2 Click the **Basics** tab.

Table 3-4 describes the elements that appear in the Basics tab.

Table 3-4 Device Basic Tab Elements

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

Related Topics

- Updating Your License, page 3-7
- Viewing Software Version Details, page 3-7

- Setting the Time and Date on the MCU, page 3-7
- Setting the MCU Location, page 3-8

Updating Your License

You use the Basics tab to update your MCU license.

Procedure

Step 1 On the sidebar, click **Device**.

Step 2 Click the **Basics** tab.

The Licensing and Registration dialog box appears.

Step 3 Access the Cisco web site to register before requesting a new license key by clicking the **Click here to register at the web site** link, or by copying the URL that appears in the lower half of the screen into your browser.

Step 4 Type your new license key in the New license key field and click **Upload** to activate the new license key.

Viewing Software Version Details

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

Procedure

Step 1 On the sidebar, click **Device**.

Step 2 Click the **Basics** tab.

Step 3 Locate the Software version field and click **Details**.

The Version Details dialog box appears.

Setting the Time and Date on the MCU

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

Procedure

Step 1 In the Administrator interface, on the sidebar, click **Device**.

Step 2 Make sure the **Basics** tab is selected.

Step 3 Next to the Date/Time field, click **Change**.

The Change Time dialog box appears. The date and time the MCU reports appear in the Set time to field.

Step 4 In the **Change** field, select the unit of time that you want to change.

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

Step 5 In the **Set board time to** field, choose the up or down arrow to change that unit.

The unit you choose changes in the direction you choose: higher (up) or lower (down).

Step 6 Repeat step 4 and step 5 for as many units as you want to change.

Step 7 Select the **NTP enabled** check box to synchronize the time with a network server clock.

Step 8 On the toolbar, click **Upload**.

Setting the MCU Location

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

Procedure

Step 1 On the sidebar, click **Device**.

Step 2 Click the **Basics** tab.

Step 3 In the **Location** field, enter the location information about the MCU that you want to display.

The field displays up to 23 characters.

Step 4 On the toolbar, click **Upload** to save to configuration memory.

Viewing Address Settings

In the Addressing tab, you can view address information for the MCU such as IP address informations, Domain Name Server (DNS) information and Ethernet port speed and duplex. Table 3-5 describes the elements that appear on the Addressing tab.

Table 3-5 Addressing Tab Elements

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

Related Topics

- Changing Address Settings, page 3-9

Changing Address Settings

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

Procedure

Step 1 In the Administrator interface, on the sidebar, click **Device**.

Step 2 Click the **Addressing** tab.

Step 3 To change an IP address setting, do any of the following steps:

- In the **IP Address** field, type the IP address you want to assign to the MCU.
- In the **Router IP** field, type the IP address of the router you want the MCU to use.
- In the **Subnet Mask** field, type the subnet mask you want the MCU to use.

Step 4 To change or add DNS information, do the following steps:

- In the **DNS suffix** field, type the alias you want to assign to the current MCU.
- In the **Preferred DNS server** field, type the IP address of the primary DNS server that you want the MCU to use.

- In the **Alternate DNS server** field, type the IP address of the back-up DNS server that you want the MCU to use.

Step 5 In the **Port settings** field, choose the Ethernet port and duplex speed value you want to set.

Step 6 On the toolbar, click **Upload**.

Related Topics

- Viewing Address Settings, page 3-8

Changing the Administrator Interface Web Server Port

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

Procedure

Step 1 In the Administrator interface, on the sidebar, click **Device**.

Step 2 Click the **Web** tab.

Step 3 In the Web server port field, enter the port number.

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

Configuring Security

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

Procedure

Step 1 In the Administrator interface, on the sidebar, click **Device**.

Step 2 Click the **Security** tab.

Step 3 From the **Security mode** field, choose the access level you want the MCU to support:

- **Standard**—Allows SNMP, Telnet, FTP, and ICMP to access the MCU.
- **High (no Telnet or FTP)**—Allows access to the MCU only through SNMP and ICMP.
- **Maximum (no Telnet, FTP, SNMP, or ICMP)**—Disallows external programs to access the MCU.

Step 4 In the **SNMP Read community** and **Write community** fields, type default strings used to enable SNMP communication between the MCU and an external application such as the Cisco Upload Utility.

Viewing the Status Tab

The Status tab displays information about MCU resource usage and performance. Table 3-6 lists the information in the Status tab.

Table 3-6 Status Tab Sections

Section Name	Description
Status	Indicates the current operational state of the MCU as follows: • Error—Indicates that the MCU is not registered to a gatekeeper, or that the web connection is down. • OK.
Resource Meter	• CPU Usage (%) field—Indicates the percentage of MCU resources currently occupied. We recommend that this value not exceed 90 percent.
Conferences	• Number of active conferences—Indicates the number of conferences currently hosted on the MCU. • Number of calls—Indicates the current number of calls on the MCU.

Configuring Settings

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

Setting the User Interface Language

In the Basics section of the Settings tab, you can configure the language that the MCU supports. Table 3-7 lists the languages that the MCU supports.

Table 3-7 Supported Languages in the MCU User Interface

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

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Basic** button.

Step 4 In the MCU user interface language field, select the required language.

Setting the Unit Identifier

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

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Basics** button (if not already selected).

Step 4 In the MCU Identifier field, enter an identifier (up to a maximum of 15 characters). For example, “London office”.

Setting an Operator Number

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Basics** button.

Step 4 In the Operator field, enter an operator number.

Configuring DTMF Control

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

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Conference Control** button.

Step 4 Select the **Enable DTMF Conference control** check box.

Step 5 In the DTMF Conference Control prefix field, choose a symbol for starting the DTMF conference control session. You can select pound (#) or asterisk (*). The default is *.

Step 6 Select the **Enable H.243 Conference control** check box.

Configuring Themes

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Themes** button.

Step 4 In the Theme field, select one of the following themes:

- Modern (customizable)
- Classic (customizable)
- Classic Blue Freeze
- Classic Copper Autumn
- Classic Charlie Chaplin
- Classic Fresh Green

If you select any theme other than **Basic**, the font, subframe and border color are automatically set. If you select **Basic**, follow step 5 to step 10.

Step 5 In the Font background transparency field, choose one of the following settings:

- None—A solid background against which the text appears.
- Half—A moderate background against which the text appears.
- Full—A transparent background against which the text appears.

Step 6 In the Font size field, choose a font size:

- Small
- Normal
- Large

Step 7 In the Font foreground color, Font background color and Empty subframe color fields, click to select a color for these settings.

Step 8 You can display a default border around all participant sub-frames. Select the **Display default border** check box and click to select the default border color.

Step 9 You can set a default border for the active speaker. Select the **Display active speaker border** check box and click to select the active speaker border color.

Step 10 The Basic font field displays the font currently installed on the MCU. Select the **Enable extended font** check box to enable an additional font if one is installed on the MCU.

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

Configuring Quality of Service

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

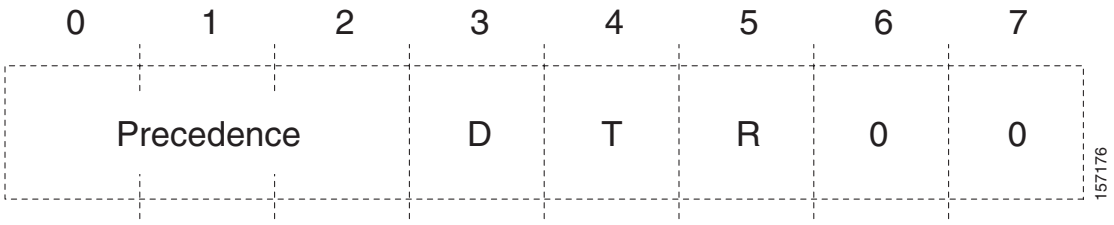
Quality of Service settings involve configuring the MCU to add a Quality of Service (QoS) IP Precedence code in the IP header of outbound packets. Routers on the network that support QoS can give precedence to such coded packets and facilitate the efficient transmission of packets. You can set priority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

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

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

You use the abstract parameters to choose the actual service parameters when transmitting a datagram through a particular network. The abstract parameters represent the three-way trade off between low delay, high throughput and high reliability. Increasing the performance of one of these parameters might result in reduced performance of the other two. Figure 3-2 represents the ToS field in the IP header.

Figure 3-2 TOS Field in the IP Header



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

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

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

The possible Precedence settings are as follows:

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

- 001 = Priority
- 000 = Routine

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Quality of Service** button.

Step 4 In the Quality of service support field, set the required IP ToS value for each media type by clicking one of the following radio buttons:

- None—Select to disable Quality of Service support
- Default—Select to assign the default IP ToS value for each media type. The default settings represent Cisco recommendations.
- Custom—Select to assign your own IP ToS value for each media type.

If you select **Default**, the system automatically enters Quality of Service settings. If you select **Custom**, follow the steps below.

Step 5 In the Voice Priority field of the Video Calls section, enter a whole number from 0 to 63 to set the priority level of voice packets that the MCU sends out. The default value is 34.

Step 6 In the Video Priority field of the Video Calls section, enter a whole number from 0 to 63 to set the priority level of video packets that the MCU sends out. The default value is 34.

Step 7 In the Voice Priority field of the Voice Calls section, enter a whole number from 0 to 63 to set the priority level of voice packets that the MCU sends out. The default value is 46.

Configuring MCU Dynamic Layouts

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

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Dynamic Layouts** button.

Step 4 Click a layout image to select or deselect that specific layout.

Configuring MCU Alert Indications

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

This section describes the following topics:

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

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

Table 3-8 lists alert indications as well as the SNMP trap associated with them.

Table 3-9 lists the structure of the standard *coldStart* and *warmStart* traps (as defined in RFC 1907) and the standard *linkDown* and *linkUp* traps (as defined in RFC 1573).

Table 3-8 MCU Alert Indications

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

Table 3-8 MCU Alert Indications (continued)

Event Type	Trap is sent when...
Power-up	The MCU has begun operation.
Services table is changed	The service table has been modified.

Table 3-9 Standard SNMP Trap Event Types

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Alert Indications** button.

Step 4 In the Events section, select the check boxes in the **Enabled in the Event Log** column for all the events that you want to trigger SNMP traps.

Step 5 For each event you enable, choose one of the following severities in the Severity column:

- Cleared—Enumeration 0. One or more previously reported alarms have been cleared.
- Information—Enumeration 1. Notification of a non-erroneous event.
- Critical—Enumeration 2. A service-affecting event has occurred and requires immediate corrective action.
- Major—Enumeration 3. A service-affecting event has occurred and requires corrective action to prevent the condition becoming more serious.
- Minor—Enumeration 4. A non-service-affecting event has occurred and requires corrective action to prevent the condition becoming more serious.
- Warning—Enumeration 5. A potential or impending service-affecting event has been detected, but no significant events have occurred yet. Action should be taken to further diagnose and correct the problems to prevent the condition becoming more serious.

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

Configuring SNMP Trap Servers

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Alert Indications** button.

Step 4 In the SNMP Traps Server section, click **Add**.

The SNMP Trap Servers Properties dialog box appears.

Step 5 In the SNMP Trap server address field, enter the address for the SNMP trap server.

Step 6 In the Port field, enter the port of the SNMP trap server. The default port for SNMP servers is 162.

Step 7 In the Enabled traps section, select which traps you want to enable:

- To disable a trap, click it in the Enabled traps area and then click **Remove**.
- To enable a trap, click it in the Disabled traps area and then click **Add**.
- To enable all traps, click **Add All**.
- To disable all traps, click **Remove All**.

Step 8 Click **Upload** to save your settings.

The configured SNMP trap server appears in the SNMP Trap Servers section.

Editing SNMP Trap Servers

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Alert Indications** button.

Step 4 In the SNMP Trap Servers section, click the configured SNMP trap server and then click the **Edit** button.

Step 5 Click **Upload** when you finish your edits.

Deleting SNMP Trap Servers

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Alert Indications** button.

Step 4 In the SNMP Trap Servers section, click the configured SNMP trap server and then click **Delete**.

Configuring Conference Management Settings

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Advanced** button.

Step 4 Select the **Register conference ID** check box to register existing conference IDs with the gatekeeper and SIP server to enable participants dialing in to a conference from remote locations to connect to the target conference on the MCU. This setting is deselected by default.

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

Step 5 In the Conferences can be created using field, choose one of the following methods through which conferences can be created:

- Scheduler only—Enables conference creation only using a conference scheduling application
- Scheduler, Web and Control API—Enables conference creation using a conference scheduling application, the Conference Control interface, or an external application that uses the MCU API.
- Scheduler, Web, Control API and dial-in (default)—Enable all the conference creation methods listed above, as well as dial-in for ad-hoc conference creation.

Step 6 Select the **When using the web, only operators or administrators can create a conference** check box to grant conference creation authorization only to users with Administrator or Operator privileges. If you want users with all levels of access to be able to create a conference, leave this option deselected.

Step 7 In the Participants can join the conference using field, choose one of the following methods through which participants can join a conference:

- Invite only—Participants can join a conference only when the MCU dials that participant.
- Invite and dial-in—Participants can join a conference either by MCU invitation or by dialing directly using a conference ID.

Step 8 In the Ad hoc conferences terminate when field, choose the method through which dial-in (ad hoc) conferences terminate:

- Last participant leaves—The conference terminates when the last participant leaves the conference.

- Conference creator leaves—The conference terminates when the conference creator leaves the conference.

Step 9 In the External conference authorization policy field, choose one of the following MCU authorization policies for creating or joining conferences:

- None—No authorization required.
- Notify—The MCU notifies an external application such as a conference scheduler that accesses or controls MCU resources about conference creation or joining.
- Authorize—The MCU requests authorization from an external application such as a conference scheduler which accesses or controls MCU resources to create conferences or allow participants to join conferences.

Configuring Delimiter Settings

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

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Advanced** button.

Step 4 In the PIN delimiter field, enter the characters used as a separator between the conference ID and conference PIN when dialing into a conference. A conference is created with this PIN if no conferences already exist with the specified number. Valid delimiters include the pound sign (#) and asterisk (*). The default PIN delimiter setting is three asterisks (***).

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

Disconnecting Participants on Communications (ICMP) Failure

When the MCU sends audio or video data to an unreachable endpoint, the network notifies the MCU using the ICMP protocol. The MCU can detect ICMP messages and disconnect the endpoint automatically. You enable automatic endpoint disconnection in the Advanced section of the Settings tab.

If this option is not selected, the MCU ignores ICMP error packets.

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Advanced** button.

Step 4 Select the **Disconnect participants on communication (ICMP) failure** check box.

Step 5 In the Disconnect on field, make one of the following sections:

- Audio failure—The call disconnects only if the audio connection fails. The call continues if the video connection fails and the audio connection remains. This is the default setting.
- Audio or video failure—The call disconnects if either the audio or video connection fails.

Sending Advanced Commands

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

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

Table 3-10 lists all available advanced commands.

Table 3-10 List of Available Advanced Commands

Command	Description	Parameters	Default
Conference control Web refresh interval	Indicates the length of time (in seconds) after which the Conference Control interface refreshes automatically.		10
DTMF forwarding	Indicates the target of DTMF forwarding.	to all—All endpoints in the conference. to gateways—To gateways only. to none—DTMF is disabled.	none
First audio announcement interval (msec)	Indicates the length of time (in milliseconds) between the start of the conference and the first audio announcement.		Disabled

Table 3-10 List of Available Advanced Commands (continued)

Command	Description	Parameters	Default
Font align	Determines whether text overlay (TOL) on a video screen is positioned away from picture borders.	All—Text positioned away from horizontal and vertical borders. Horizontal—Text positioned away from horizontal borders and centered horizontally. Vertical—Text positioned away from vertical borders and centered vertically. None—Text is always positioned bottom center.	All
G.728 mode	Determines the form of encoding for the G.728 audio codec RTP header.	Non-standard—For use if you experience audio problems when using VCON endpoints with the G.728 audio codec. Standard—For normal G.728 use with all endpoints except VCON products.	
H323 hide stack	Disables H.323 stack prints.		H.323 Stack printing is disabled by default.
H323 show stack	Enables H.323 stack prints. These print the protocol stack info and errors and are useful for debugging stack issues		
H323 show status	Prints a snapshot of H.323 stack-related information.		
Handle DTMF after XML notification	Instructs the MCU to send DTMF signals to an external server and other specified destinations.	no—MCU sends DTMF signals to the external server only. yes—MCU sends DTMF signals to the external server and to the destination set by the DTMF forwarding advanced command.	

Table 3-10 List of Available Advanced Commands (continued)

Command	Description	Parameters	Default
NTP synchronization period	Sets the Network Time Protocol synchronization period (in seconds) between the EMP and the MCU..		21600
Notify level	Sets the MCU log notify level filter	Fatal—MCU cannot continue to provide service (unrecoverable error). Error—User functionality problem (for example, call connect failure or no resources available). Warning—User functionality problem but the MCU can continue to provide service. Info—Status prints for Customer Support use. Advanced—Like Info but more detailed. Debug 1 through Debug 4—Debug levels.	Debug 3
Open in-band DTMF detection	Enables support for in-band DTMF signaling.	Always or Only when call connects	Always
QualiVision Settings hide	Disables the QualiVision Settings section in the Settings tab.		The QualiVision Settings section is hidden by default.
QualiVision Settings show	Enables the QualiVision Settings section in the Settings tab.		
SCCP hide stack	Disables SCCP stack prints.		
SCCP show status	Prints a snapshot of SCCP stack related information.		
Set MTU size	Determines the maximum packet size across the network.		1500

Table 3-10 List of Available Advanced Commands (continued)

Command	Description	Parameters	Default
Set terminal baud rate	Sets the baud rate of a serial terminal.	High (57600) Low (9600)	Low (9600)
Support RFC 2833 capability	Enables support for in-band DTMF signaling via packets within the audio channel as defined in the RFC 2833 standard.	disable or enable	enable

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Advanced** button.

Step 4 Click **Commands**.

The Advanced Commands dialog box appears.

Step 5 In the Command field, enter a command or choose one from the Available Commands field.

Step 6 In the Parameters field, enter a parameter value for the command (where applicable) or choose one from the Available Parameters field.

Step 7 Click **Send**.

The results of the advanced command appear in the **Results** field, indicating whether or not the MCU received and executed the command. If you send an invalid command, a "bad parameter" or "NOT FOUND" message appears.

Opening a Telnet Terminal

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

Procedure

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

Step 2 Click the **Settings** tab.

Step 3 Click the **Advanced** button.

Step 4 Click **Telnet**.

Step 5 A separate browser opens with a Telnet terminal. When you finish with your Telnet session, click **Disconnect**.

Viewing Media Processors

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

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

Protocols and the MCU

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

- Configuring H.323 Gatekeeper Settings, page 3-26
- Integrating SIP with the Cisco Unified Videoconferencing 3515 MCU, page 3-28
- Configuring the Cisco Unified Videoconferencing 3515 MCU to Use Cisco Unified CallManager, page 3-33

Configuring H.323 Gatekeeper Settings

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

- Configuring H.323 Gatekeeper Protocol Configuration, page 3-26
- Configuring Advanced H.323 Gatekeeper Protocol Settings, page 3-27

Configuring H.323 Gatekeeper Protocol Configuration

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

Procedure

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

Step 2 Click the **Protocols** tab.

Step 3 Make sure the H.323 button is selected.

The H.323 Protocol Configurations dialog box appears.

Step 4 Select the **Enable H.323 protocol** check box to enable the MCU to operate with the H.323 protocol.

Step 5 In the Gatekeeper Address field, enter the IP address of the gatekeeper.

Step 6 In the Gatekeeper Port field, enter the port number of the gatekeeper. The default port is 1719.

Step 7 Select the **Strip local gatekeeper zone prefix if it appears in incoming cells** check box if you want the MCU to strip the gatekeeper zone prefix from the dialed string of an incoming call. For example, if the zone prefix is 01 and you have selected this option, the MCU removes 01 from every dial string beginning 01. Do not use this feature if the gatekeeper is already set to perform zone stripping.

Step 8 If you did not perform step 7, skip to step 9. Otherwise, in the Local Zone Prefix field, enter the gatekeeper zone you want to strip.

Step 9 Click **Upload**.

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

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

Configuring Advanced H.323 Gatekeeper Protocol Settings

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

Before You Begin

Make sure the basic H.323 gatekeeper protocol settings are correct. See the "Configuring H.323 Gatekeeper Protocol Configuration" section on page 3-26 for more information.

Procedure

Step 1 In the H.323 Protocol Configurations dialog box click the **Advanced H.323 Settings** button.

The Advanced H.323 Setting dialog box appears.

Step 2 In the RAS Port field, enter the port on which the MCU conducts RAS registration messaging with the gatekeeper. The default port is 2719.

Step 3 In the Signaling Port field, enter the port on which the MCU carries call signalling messages to and from the gatekeeper. The default port is 2720.

Step 4 In the Registration refresh every field, enter the interval (in seconds) between registrations of the MCU to the gatekeeper. The default value is 60 seconds.

Step 5 In the MCU Registration Mode field, choose the mode of registration with the H.323 gatekeeper.

- MCU—Use this setting to connect H.323 calls via the MCU.
- Gateway—Use this setting to connect H.323 calls via a Cisco gateway. This is the default setting.

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

Step 7 Select the **Enable H.245 tunneling** check box to enable H.245 tunneling during call setup and connection between the MCU and incoming calls received through the gatekeeper.

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

Step 8 Click **OK**.

Integrating SIP with the Cisco Unified Videoconferencing 3515 MCU

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

Configuring SIP Proxy Settings

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

Procedure

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

Step 2 Click the **Protocols** tab.

Step 3 Make sure the **SIP** button is selected.

The SIP Protocol Configurations dialog box appears.

Step 4 Select the **Enable SIP protocol** check box to enable MCU communication with the SIP proxy.

Step 5 In the Default SIP domain field enter the SIP domain of the gateway as defined in the SIP server. An example of a SIP domain is *company.com*.

Step 6 Select the **Using Microsoft LCS** check box to enable the MCU to work with Microsoft Office Live Communication Server (LCS).

Step 7 In the SIP Server section, choose one of the following options:

- Select **Locate server automatically (using DNS)** if you wish the gateway to automatically locate one of the SIP proxy servers that are present in the domain.

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

- Select **Specify address** and enter the following:
- An IP address or host name of the SIP proxy, for example *proxy.company.com*.
- In the port field enter the communication port number of the SIP proxy address.
- In the type field select the transport connection type for sending messages to the SIP proxy according to the type supported by the SIP proxy—UDP or TCP. This field is mandatory. The default is UDP.

Step 8 Select the **Treat as outbound proxy** check box if you wish the Gateway to send all the SIP messages to the configured SIP proxy server. This is optional. The default is unchecked.

Step 9 Select the **Use Registrar** check box if you wish the Gateway to register with the SIP registrar using the name defined in the Registration name field, and to send service information to the registrar.

Step 10 If you selected **Use Registrar** in step 9, enter the following information:

- In the Address field enter the IP address or the host name of the SIP registrar. This field is mandatory.
- In the port field enter the communication port number of the SIP registrar address.
- In the type field select the transport connection type for sending registration requests to the registrar according to the type supported by the SIP registrar—UDP or TCP. This field is mandatory. The default is UDP.

Step 11 In the Local signaling port field enter the number of the signaling port on which the Gateway communicates with the SIP proxy. The default is 5060.

Configuring Advanced SIP Proxy Settings

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

Before You Begin

Make sure the basic SIP proxy settings are correct. See the "Configuring SIP Proxy Settings" section on page 3-28 for more information.

Procedure

Step 1 In the SIP Protocol Configurations dialog box click the **Advanced SIP Settings** button.

The Advanced SIP Setting dialog box appears.

Step 2 In the "From" header field select an addressing format that the gateway will use for the information sent in the "From" header of messages for outgoing calls.

- Select **Use local signaling IP address** if you wish the gateway to use its local signaling IP address.
- Select **Use fully qualified domain name (FQDN)** if you wish the gateway to use the FQDN. Enter the fully qualified domain name of the gateway, for example, *gateway.company.com*.

Step 3 In the "Contact" header field select the addressing format that the gateway will use for the information sent in the "Contact" header of messages for outgoing calls.

- Select **Use local signaling IP address** if you wish the gateway to use its local signaling IP address.

- Select **Use fully qualified domain name (FQDN)** if you wish the gateway to use the FQDN. Enter the fully qualified domain name of the gateway, for example, *gateway.company.com*.

Step 4 Select the **Use proxy digest authentication** check box to enable gateway authentication with a SIP proxy server using user name and password. Authentication is performed as defined in RFC 2617. This field is disabled by default.

Step 5 If you selected **Use proxy digest authentication** in step 4, enter the following:

- In the User name field enter the gateway user name. The user name must match the name defined on the SIP proxy server.
- In the Password field enter the gateway user password. The user password must match the password defined on the SIP proxy server.

Step 6 Select the **Use registrar digest authentication** check box to enable gateway authentication with a SIP registrar server using user name and password. Authentication is performed as defined in RFC 2617. This field is disabled by default.

Step 7 If you selected **Use registrar digest authentication** in step 6, enter the following:

- In the User name field enter the gateway user name. The user name must match the name defined on the SIP registrar server.
- In the Password field enter the gateway user password. The user password must match the password defined on the SIP registrar server.

Step 8 Select the **Enable Video Fast Update** check box to enable transport of Video Fast Update (VFU) requests to SIP endpoints.

Step 9 Select the **Support reliable provisional response (RFC 3262)** check box to enable the remote endpoint to request that the source endpoint sends an acknowledgment on receipt of 10x SIP messages.

Step 10 Select the **Use 'Empty Invite' when sending Invite messages to endpoints** check box to enable the remote endpoint to indicate preferred audio and video channels.

Step 11 Click **OK**.

About the MCU Dial Plan

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

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

The following sections describe these configurations:

- About Outgoing Calls from the MCU, page 3-31
- About Incoming Calls to the MCU, page 3-31
- Configuring the MCU as a UAC, page 3-31
- Configuring the MCU to Perform as a Separate SIP Domain, page 3-32

About Outgoing Calls from the MCU

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

Note If the user does not specify a domain in the dialing string, the MCU appends the default domain to the dialed string. You can configure the default domain in the SIP section of the Protocols tab. See the "Configuring SIP Proxy Settings" section on page 3-28 for more information.

About Incoming Calls to the MCU

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

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

Configuring the MCU as a UAC

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

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

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

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

Procedure

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

Step 2 Click the **Protocols** tab.

Step 3 Make sure the **SIP** button is selected.

The SIP Protocol Configurations dialog box appears.

Step 4 Select the **Use registrar** check box.

Step 5 In the Default Domain field, enter the default domain name as defined in the SIP proxy server.

Step 6 Click the **Settings** tab and then click the **Conference Mgmt** button.

Step 7 Make sure that the **Register conference ID** check box is selected.

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

Configuring the MCU to Perform as a Separate SIP Domain

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

Procedure

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

Step 2 Click the **Protocols** tab.

Step 3 Make sure the **SIP** button is selected.

The SIP Protocol Configurations dialog box appears.

Step 4 In the Default Domain field, enter the name of the domain in which the MCU operates.

For example, *company.com*.

Step 5 Configure the unique domain name of the MCU in the proxy internal routing tables (if supported) or in the relevant DNS server:

- For proxy internal routing tables, configure a rule such as:

Every URI of type *(any number)@mcu.company.com should be routed to the MCU IP address.

- For a DNS server, define a new rule entry of mcu.company.com. The address of this entry is the MCU IP.

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

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

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

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

Viewing SCCP Protocol Configurations

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

Procedure

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

Step 2 Click the **Protocols** tab.

Step 3 Click the **SCCP** button.

The SCCP Protocol Configurations dialog box displays the following settings:

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

Configuring the SCCP Protocol

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

Procedure

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

Step 2 Click the **Protocols** tab.

Step 3 Click the **SCCP** button.

The SCCP Protocol Configurations dialog box appears.

Step 4 Select the **Enable SCCP protocol** check box to allow the MCU to support the SCCP protocol.

Step 5 In the Active SCCP service prefix field, enter the prefix assigned to the MCU service that you want the Cisco Unified CallManager to use.

Note A default service prefix is automatically entered in this field. If you want to use this service, make sure that this is a valid service prefix for your network environment. See the "Services" section on page 3-37, for more information about creating MCU services.

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

Configuring a TFTP Server

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

Procedure

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

Step 2 Click the **Protocols** tab.

Step 3 Click the **SCCP** button.

The SCCP Protocol Configurations dialog box appears.

Step 4 In the TFTP Servers section, identify the TFTP server that you want the MCU to use.

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

Step 5 In the TFTP Servers section, click **Add** (or **Edit**).

The Add (or **Edit**) TFTP Server dialog box appears.

Step 6 In the IP address field, enter the IP address of the TFTP server you want the MCU to use to contact the Cisco Unified CallManager.

Step 7 In the Port field, enter the port number that you want the MCU to use to communicate with the TFTP server.

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

Adding a Cisco Unified CallManager

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

Procedure

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

Step 2 Click the **Protocols** tab.

Step 3 Click the **SCCP** button.

The SCCP Protocol Configurations dialog box appears.

Step 4 Select the **Change configuration locally** check box to manually add another Cisco Unified CallManager and configure SCCP settings for this Cisco Unified CallManager.

The Add button is activated.

Step 5 Click the **Add** button.

The Add CallManager dialog box appears.

Step 6 Set the required IP address and port number for the Cisco Unified CallManager and click **OK**.

The new Cisco Unified CallManager appears in the CallManagers section.

Step 7 Click **OK** to save your changes.

Viewing Advanced SCCP Protocol Settings

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

Table 3-11 describes the elements that appear in the Edit SCCP Protocol Configuration dialog box.

Table 3-11 Edit SCCP Protocol Configuration Dialog Box

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

Table 3-11 Edit SCCP Protocol Configuration Dialog Box (continued)

Field	Description
Initial timeout (sec)	Indicates the length of time the MCU waits for a response from the Cisco Unified CallManager before timing out on the first attempt to register.
Consequent timeout (sec)	Indicates the length of time the MCU waits for a response from the Cisco Unified CallManager before timing out on subsequent attempt to register.
Keep Alive	
Retries	Indicates the number of times the MCU will send the Keep Alive message to the Cisco Unified CallManager before acknowledging that the connection has failed.
Timeout (sec)	Indicates the interval at which the MCU sends Keep Alive messages.
Fail Over	
Recovery mode	Indicates the mode with which the MCU terminates calls when the connection to the Cisco Unified CallManager fails: • gracefully—Allows completion of current calls. • immediately—Terminates conference immediately. • timeout—Allows all conferences to continue for the interval specified in the Recovery timeout (sec) field.
Recovery timeout (sec)	Indicates the length of time the MCU allows calls to continue after the connection with the Cisco Unified CallManager fails.

Configuring Advanced SCCP Protocol Settings

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

Procedure

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

Step 2 Click the **Protocols** tab.

Step 3 Click the **Advanced SCCP Settings** button.

The Advanced SCCP Settings dialog box appears.

Step 4 In the Local port base field, enter a value for the communication port that you want the MCU to use to communicate with the Cisco Unified CallManager.

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

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

Step 5 In the Priority (0-63) field, enter the Differentiated Services Code Point (DSCP) value the Cisco Unified CallManager specifies that the MCU use for Quality of Service (QoS). You must convert the value to decimal notation.

Step 6 In the Retries field of the Registration section, enter a value setting the number of times you want the MCU to attempt to register with the Cisco Unified CallManager.

Step 7 In the Initial timeout (sec) field, enter a value in seconds setting the length of time the MCU waits for a response from the Cisco Unified CallManager before timing out on the first attempt to register.

Step 8 In the Consequent timeout (sec) field, enter a value in seconds setting the length of time the MCU waits for a response from the Cisco Unified CallManager before timing out on subsequent attempt to register.

Step 9 In the Retries field of the Keep Alive section, enter a value setting the number of times you want the MCU to send the Keep Alive message to the Cisco Unified CallManager before acknowledging that the connection has failed.

Step 10 In the Timeout (sec) field, enter a value in seconds setting the interval at which the MCU sends Keep Alive messages.

Step 11 In the Recovery mode field, choose the mode with which you want the MCU to terminate calls when the connection to the Cisco Unified CallManager fails:

- gracefully—Allow completion of current calls.
- immediately—Terminate conference immediately.
- timeout—Allow all conferences to continue for the interval specified in the Recovery timeout (sec) field.

Step 12 If you select **timeout** in the Recovery mode field, enter a value in seconds in the Recovery timeout (sec) field to set the length of time the MCU allows calls to continue after the connection with the Cisco Unified CallManager fails.

Step 13 Click **OK** to save your changes.

Step 14 Click **Cancel** to close the Advanced SCCP Settings dialog box without saving changes.

Services

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

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

When using an SCCP service the following limitations apply:

- No support for presentation view (Duo Video and H.239)
- No support for T.120 data collaboration
- No support for H.235 encryption
- Maximum resolution supported is CIF
- Maximum call rate supported is 768 Kbps

- The G.722.1 and G.723 audio codecs are not available
- No support for conference PINs
- No support for dial out

Working with Services

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

- Creating a New Service, page 3-38
- Creating a New SCCP Service, page 3-38
- Customizing Services, page 3-39

Creating a New Service

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

Procedure

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

Step 2 Click the **Services** tab.

Step 3 Click **Add**.

The Automatic Service Definition dialog box appears.

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

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

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

Step 6 Click **Upload**.

Creating a New SCCP Service

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

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

Procedure

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

Step 2 Click the **Services** tab.

Step 3 Click **Add**.

The Automatic Service Definition dialog box appears.

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

Step 5 Check the **SCCP service** check box.

Step 6 In the Service description field, type a description of the service in free text.

Step 7 Click **Upload**.

Customizing Services

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

- Configuring the Maximum Call Rate, page 3-39
- Configuring the Maximum Layout, page 3-40
- Configuring Advanced Video Settings, page 3-40
- Configuring Advanced Audio Settings, page 3-42
- Configuring Data Collaboration Support, page 3-43
- Configuring Presentation View, page 3-43
- Configuring Encryption Support, page 3-44
- Configuring Advanced Management and Security, page 3-45

Configuring the Maximum Call Rate

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

Procedure

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

Step 2 Click the **Services** tab.

Step 3 Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 4 In the Max call rate field, select the maximum call rate for the voice, video and data streams combined.

Step 5 Click **Upload**.

Configuring the Maximum Layout

The Max Layout field indicates the video layout displaying the maximum number of participants to which the conference view expands. Select **Audio only** to force the conference to be audio-only.

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 In the Max Layout field, a picture of the current maximum layout appears. Click the **Change** button to choose a new layout. For an audio-only conference, choose **Audio only**.

Step 4 Click **OK**.

Configuring Advanced Video Settings

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 Click the **Advanced Video Settings** button.

An Advanced Video Settings dialog box appears.

Step 4 The Video Codecs and Image Size section displays the choice of codecs that you prefer and the supported image size. The codecs are listed in declining order of preference with the most preferred codec listed first. Setting the codec priorities notifies the MCU and remote endpoints of your preferred video codecs. This is useful when more than one codec is supported by both sides. To select or change the codec priorities, follow these steps:

- To add a codec to the Available field, click it in the Selected field and then click **Add**. To remove a codec from the Available field, click it and then click **Remove**.
- To move a codec up the priority list, click it and then click the **Up** button. To move a codec down the priority list, click it and then click the **Down** button.

Step 5 In the Support image size up to field, choose the maximum incoming picture format supported in conferences using this service.

Step 6 In the Main (Participant) Layout section select the layout options you wish to define for this service.

Step 7 To configure automatic switching, select the **Enable auto switch** check box and type the interval in seconds. Auto switching allows participant images in the video layout periodically to change and display other conference participants according to the interval set.

Step 8 Select **Dynamically change layout as participants join or leave** to dynamically enlarge or reduce the displayed number of subframes.

Step 9 To configure removal of the self image, select **Enable 'No Self See'**.

Step 10 Select an option from the Display participants names field to show a participant's name at the bottom of each sub-frame.

Step 11 Select **Slightly reduce image size for optimal TV display** to change the display from PC screen mode to TV screen mode.

Step 12 From the Themes to use field, select a theme. Basic is the default.

Step 13 (Optional) In the Additional Layouts section, select the **Enable custom layouts** check box to define custom layouts to maintain backward compatibility with previous product versions.

Step 14 (Optional) Click the **Settings** button to define the layout options in the Custom Layout Settings dialog box.

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

Related Topics

- Configuring 3G Layout Settings, page 3-41
- Configuring Presentation View, page 3-43

Configuring 3G Layout Settings

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 In the Additional Layouts section, select the **Enable 3G videophone layout** check box to limit the layout for 3G videophone users.

Step 4 Click the **Settings** button to select the layout in the 3G Layout Settings dialog box.

Step 5 Click **OK** to return to the Automatic Service Definition dialog box.

Configuring Advanced Audio Settings

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

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

- G.711 A/μ law—Toll quality at 64 Kbps (A-Law/mu-Law).
- G.722—High-quality audio at 64 Kbps.
- G.722.1—High quality audio at 24 Kbps or 32 Kbps using a digital sampling rate ranging from 50 Hz up to 7 kHz.
- G.723.1—Voice quality audio at 5.3 Kbps or 6.4 Kbps.
- G.728—Near toll quality audio at 16 Kbps.
- G.729A—Audio at 8 Kbps.

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 Click the **Advanced Audio Settings** button to modify audio settings.

The Audio Settings dialog box appears.

Step 4 The Transcoder Priority field displays the choice of codecs that you prefer for audio transcoding. The codecs are listed in declining order of preference with the most preferred codec listed first. Setting these priorities notifies the MCU and remote endpoints of your preferred audio codecs. This is useful when more than one codec is supported by both sides. To change these priorities, follow these steps:

- To add a codec to the Available field, click it in the Selected field and then click **Add**. To remove a codec from the Available field, click it and then click **Remove**.
- To move a codec up the priority list, click it and then click the **Up** button. To move a codec down the priority list, click it and then click the **Down** button.

Step 5 In the Audio packet size field, enter the minimum audio packet size.

Step 6 In the Number of speakers to mix concurrently field, enter the maximum number of speakers in a conference who can be heard at the same time. The value you enter is the number of loudest speakers for whom the audio stream is mixed and sent to all conference participants. For example, if you enter **4**, the MCU mixes the audio stream of the four loudest speakers in the conference.

Step 7 In the Speaking duration to become ‘Active Speaker’ field, enter the interval (in milliseconds) before the voice-activated video-switching mechanism displays a new active speaker in the video image. The default setting is 3000 milliseconds.

Step 8 Select the **Automatically mute participants who join the conference** check box to have the MCU initially mute all participants joining the conference. Once the conference begins, the conference Chair Control can unmute selected participants. This is useful for lectures.

Step 9 If you performed step 8, you can select the **Do not mute first conference participant** check box to have the MCU mute all conference participants except the participant that joined the conference first.

Step 10 Click **OK**.

Configuring Data Collaboration Support

In the Data Collaboration section of the Automatic Services Definition dialog box you can configure the service to support T.120 data collaboration

Note Data collaboration configuration options are not available for SCCP services.

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 Select the **Support T.120 data conferencing** check box.

Step 4 If you performed step 3, you can select the **Allow access to data conferencing from MCU conference control** check box.

Step 5 Click **Upload**.

Configuring Presentation View

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 Check Support presentation view (Duo Video and H.239) and click the **Settings** button.

The Presentation View Settings dialog box appears.

Step 4 In the Presentation Video Codec field choose one of the following:

- H.263
- H.264

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

Step 5 In the Presentation Image Size field, choose the required image size.

Step 6 In the Presentation Frame Rate field, choose the required frame rate.

Step 7 Click **OK**.

Configuring Encryption Support

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

Note Encryption configuration options are not available for SCCP services.

About H.235 Encryption for H.323 Calls

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

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

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

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

The following channels support encryption:

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

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 In the Management and Security section, select the **Support encryption** check box to enable encryption.

Step 4 From the Encryption mode field, select the type of encryption:

- Best effort
- Encryption required
- Strong encryption required

Step 5 Click **Upload**.

Configuring Advanced Management and Security

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

- Configuring PIN Settings, page 3-45
- Configuring Service Dial-out Policies, page 3-46
- Configuring Service Indication Settings, page 3-46
- Configuring Port Reservations and Limits, page 3-47
- Configuring Support for Far End Camera Control, page 3-47

Configuring PIN Settings

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 Click the **Advanced Management and Security** button.

The Management and Security interface appears.

Step 4 Click the **PIN Settings** tab.

Step 5 Select the **Force conference PIN protection** check box if you want user to enter a PIN when creating or entering a conference using this service.

Step 6 Select the **Do not to ask for conference PIN when dialing-out to invitees** check box if you want only dial-in participants to enter the conference PIN.

Step 7 Click **OK**.

Configuring Service Dial-out Policies

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 Click the **Advanced Management and Security** button.

The Management and Security interface appears.

Step 4 Click the **Dial-out** tab.

Step 5 In the Invitation rights section, select one of the options to define whether anyone can invite or only the chair-controller can invite participants to the conference:

- Select **Anyone can invite...** if you want any user to be able to invite participants into the conference.
- Select **Only the chair can invite...** if you only want users with Chair Control-level access to invite participants into the conference.

Step 6 In the Re-dial and reconnect section, to define redial and reconnect policies follow these steps:

- Select the **Automatically redial invited participants...** check box for the MCU to redial endpoints that fail to respond to conference invites.
  - In the Number of redial attempts field, enter the number of redial attempts.
  - In the Delay between retries (seconds) field, enter a number representing the number of seconds between each redial attempt.
- Select the **Automatically reconnect participants...** check box for the MCU to automatically call disconnected terminals to attempt a reconnection. The MCU attempts reconnection three times.

Step 7 Click **OK**.

Configuring Service Indication Settings

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 Click the **Advanced Management and Security** button.

The Management and Security interface appears.

Step 4 Click the **Indications** tab.

Step 5 Select the **First participant entry** check box if you want a message played to the first participant entering a conference, informing the participant that they are the first one to enter.

Step 6 Select the **Participant entry** check box if you want an audio indication played when any additional participant enters a conference.

Step 7 Select the **Participant exit** check box if you want an audio indication played when any participant exits a conference.

Step 8 Select the **Conference termination** check box if you want an audio indication played when a conference ends.

Step 9 Click **OK**.

Configuring Port Reservations and Limits

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 Click the **Advanced Management and Security** button.

The Management and Security interface appears.

Step 4 Click the **Port Reservation & Limits** tab.

Step 5 Select the **Number of ports guaranteed (reserved) when a conference starts** check box. Enter the number of ports to reserve. The minimum value allowed is one port.

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

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

Step 7 Click **OK**.

Configuring Support for Far End Camera Control

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

Procedure

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

Step 2 Click the **Services** tab. Select the service you wish to configure and click **Add**.

The Automatic Service Definition dialog box appears.

Step 3 Click the **Advanced Management and Security** button.

The Management and Security interface appears.

Step 4 Click the **FECC** tab.

Step 5 Select the check box to enable FECC support.

Step 6 Click **OK**.

Viewing the Event Log

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

The Event Log tab displays the following information:

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

Saving Configuration Settings

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

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

Note This operation does not save the user access level profiles that authorize users to access the Administrator or Conference Control interfaces.

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

Procedure

Step 1 In the MCU interface, on the sidebar, click **Device**.

Step 2 Make sure that the settings in the Basics, Addressing, Web and Users tabs are correct.

Note Date parameters are not saved to the configuration file.

Step 3 Click **Upload** to save these settings.

Step 4 On the sidebar, click **MCU**.

Step 5 Review each of the configuration pages to ensure that these are the configuration settings you want to save.

Step 6 Click **Upload** to save these settings.

Step 7 On the toolbar, click **Export**.

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

The File Download dialog box appears.

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

Importing Configuration Settings

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

Procedure

Step 1 In the MCU interface, on the sidebar, click **MCU**.

Step 2 On the toolbar, click **Import**.

The Import a Configuration File page appears.

Step 3 Click **Browse**.

The Choose file dialog box appears.

Step 4 Navigate to and select the configuration file you want to import.

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

Step 5 Click **Open**.

The file path appears in the File Name field.

Step 6 Click **Import**.

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

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

Note Uploading the file resets the device.