Cisco TelePresence Advanced Media Gateway Version 1.1

Online help (printable format)

D14868.01

November 2011

Contents

Introduction

This document contains the full text of the online help for the Cisco TelePresence Advanced Media Gateway Series.

It is provided so that you can print or view the help text as a single document.

Logging in

This section describes how to log in to the Cisco TelePresence Advanced Media Gateway web interface.

Logging in to the web interface

When connecting to the Cisco TelePresence Advanced Media Gateway web interface, you must log in so that the Cisco TelePresence Advanced Media Gateway can associate the session with your configured user. The Cisco TelePresence Advanced Media Gateway has a set of configured users, which each have a username and password that are used for logging in.

1. Using a web browser, enter the host name or IP address of the Cisco TelePresence Advanced Media Gateway.
2. Enter your administrator **Username** and **Password** and then click **Log in**.
3. Click **OK**.

For more information, see Problems with logging in.

Problems with 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: an incorrect username or password has been typed.
- No free sessions: the maximum number of sessions allowed simultaneously on the Cisco TelePresence Advanced Media Gateway has been exceeded
- Your IP address does not match that of the browser cookie you supplied: try deleting your cookies and log in again
- Page expired: the **Change password** page can expire if the Cisco TelePresence Advanced Media Gateway 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.)

System status

This section describes how to display system status information.

Displaying the system status

The **System status** (**Status**) page displays an overview of the Cisco TelePresence Advanced Media Gateway status.

Refer to the table below for details of the information displayed.

Field	Field description	Usage tips
System status		
Model	Specific Cisco TelePresence Advanced Media Gateway model.	
Serial number	Unique serial number of the Cisco TelePresence Advanced Media Gateway.	You will need to provide this information when speaking to Cisco customer support.
Software version	Version of the currently installed software.	
Build	Build version of the currently installed software.	
Up time	Duration since the last restart of the Cisco TelePresence Advanced Media Gateway.	
Host name	Host name assigned to the AM gateway.	
IP address	IP address assigned to the Cisco TelePresence Advanced Media Gateway.	
CPU load	Current processor utilization of the AM gateway.	
Media processing load	Overview of the current media loading of the Cisco TelePresence Advanced Media Gateway.	
Call status		
Active calls	Number of calls currently active on the Cisco TelePresence Advanced Media Gateway.	
Completed calls	Number of successful calls handled by the Cisco TelePresence Advanced Media Gateway since it was last restarted.	
Total incoming video bandwidth	The total video data rate being received by the Cisco TelePresence Advanced Media Gateway.	

Total outgoing video bandwidth	The total video data rate being sent by the AM gateway.	
System log		
System log	Displays the most recent shutdown and upgrade events, with the most recent shown first.	Displays "unknown" if there has been an unexpected reboot or power failure. Report this to Cisco customer support if it happens repeatedly.
Diagnostic information		
Diagnostic information	In the event of an issue with the Cisco TelePresence Advanced Media Gateway, Cisco customer support may ask you for this diagnostic file to help with troubleshooting.	To retrieve a troubleshooting support file, click **Download file**.

See also Displaying hardware health status.

Displaying hardware health status

The **Health status** page (**Status > Health**) displays information about the hardware components of the Cisco TelePresence Advanced Media Gateway.

Note: The **Worst status seen** conditions are those since the last time the Cisco TelePresence Advanced Media Gateway was restarted. To reset these values, click **Clear**.

Field	Field description	Usage tips
Fans Voltages RTC battery	Displays these possible states: ■ OK ■ Out of spec States indicate both *Current status* and *Worst status seen* conditions.	The states indicate the following: ■ *OK* – component is functioning properly ■ *Out of spec* – check with your support provider; component might require service If the *Worst status seen* column displays *Out of spec*, but *Current status* is *OK*, monitor the status regularly to verify that it was only a temporary condition.
Temperature	Displays these possible states: ■ OK ■ Out of spec ■ Critical States indicate both *Current status* and *Worst status seen* conditions.	The states indicate the following: ■ *OK* – temperature of the Cisco TelePresence Advanced Media Gateway is within the appropriate range ■ *Out of spec* – Check the ambient temperature (should be less than 34 degrees Celsius) and verify that the air vents are not blocked ■ *Critical* – temperature of the Cisco TelePresence Advanced Media Gateway 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 *Out of spec*, but **Current status** is *OK* monitor the status regularly to verify that it was only a temporary condition.

Network settings

This section describes how to configure network settings, including DNS settings, IP routes and services, and QoS settings.

Configuring network settings

To configure network settings on the Cisco TelePresence Advanced Media Gateway and to check the network status, go to **Network > Port A** or **Network > Port B**.

The Cisco TelePresence Advanced Media Gateway has two Ethernet interfaces, Port A and Port B. However, Port B is for future expansion and cannot be enabled in the current release of the Cisco TelePresence Advanced Media Gateway. So although a **Network > Port B** page exists, you cannot change settings for Port B.

This topic describes the following items:

IP configuration settings

These settings determine the IP configuration for the appropriate Ethernet port of the Cisco TelePresence Advanced Media Gateway. Click **Update IP configuration** to apply any changes.

Field	Field description	Usage tips
IPv4 configuration		
IP configuration	Specifies whether the port should be configured manually or automatically. If set to *Automatic via DHCP* the Cisco TelePresence Advanced Media Gateway obtains its own IP address for this port automatically via DHCP (Dynamic Host Configuration Protocol). If set to *Manual* the Cisco TelePresence Advanced Media Gateway will use the values that you specify in the Manual configuration fields below.	Click **Update IP configuration** to request a new IP address if you have selected automatic configuration. Port A should never be disabled because it is the primary interface of the Cisco TelePresence Advanced Media Gateway.
Manual configuration		

IP address	Dot-separated IPv4 address for this port, for example 192.168.4.45.	You only need to specify these settings if you select *Manual* IP configuration. For Port A, if IP configuration is set to *Automatic by DHCP* these settings are ignored.
Subnet mask	Subnet mask required for the IP address, for example 255.255.255.0	
Default gateway	IP address of the default gateway on this subnet, for example 192.168.4.1	

IP status

The IP status section shows the current IP settings for the appropriate Ethernet port of the Cisco TelePresence Advanced Media Gateway, as follows, whether they were automatically or manually configured:

- DHCP
- IP address
- Subnet mask
- Default gateway

Ethernet configuration

These settings determine the Ethernet settings for the appropriate port of the Cisco TelePresence Advanced Media Gateway. When you have finished, click **Update Ethernet configuration**.

Field	Field description	Usage tips
Ethernet settings	Select *Automatic* or *Manual*. If you select *Manual*, you must also supply the speed and duplex settings (see below). Select *Automatic* if you want this Ethernet port automatically to negotiate its Ethernet settings with the connected device.	Your Ethernet settings must match those of the device to which this port is connected. That is, you must configure both devices to use automatic negotiation or configure both devices with the same fixed speed and duplex settings.
Manual configuration		
Speed	Identifies the connection speed: *10 Mbit/s* or *100 Mbit/s*. Use automatic negotiation if a connection speed of *1000 Mbit/s* is required.	The connection speed must match that of the device to which this port is connected. Only select this option if you chose manual configuration.

Duplex	Identifies the connection duplex mode: ■ *Full duplex* Both devices can send data to each other at the same time ■ *Half duplex* 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. Only select this option if you chose manual configuration.

Ethernet status

Field	Field description	Usage tips
Link status	Indicates whether or not this Ethernet link is connected.	
Speed	The speed (*10*/*100*/*1000 Mbit/s*) of this Ethernet link.	This value is negotiated with the device to which this port is connected or is based on your manual configuration.
Duplex	The duplex mode (*Full duplex* or *Half duplex*) of the network connection to this port.	This value is negotiated with the device to which this port is connected or is based on your manual configuration.
MAC address	The fixed hardware MAC (Media Access Control) address of this port.	This value is for information only and cannot be changed.
Packets sent	The total number of packets sent from this port by the Cisco TelePresence Advanced Media Gateway (includes all TCP and UDP traffic).	This information can help to confirm that the Cisco TelePresence Advanced Media Gateway is transmitting packets into the network.
Packets received	The total number of packets received by this port (includes all TCP and UDP traffic).	This information can help to confirm that the Cisco TelePresence Advanced Media Gateway is receiving packets from the network.
Statistics:	These fields display further statistics for this port. ■ Multicast packets sent ■ Multicast packets received ■ Total bytes sent ■ Total bytes received ■ Receive queue drops ■ Collisions ■ Transmit errors ■ Receive errors	This information can help to diagnose network issues, such as link speed and duplex negotiation issues.

DNS settings

To work with the DNS settings for the Cisco TelePresence Advanced Media Gateway, go to **Network > DNS**.

Configuring DNS settings

The available settings are described in the table below. Click **Update DNS configuration** to apply any changes.

Field	Field description	Usage tips
DNS configuration	Select a port and DHCP combination from the list or select *Manual* to specify DNS settings manually. If you select *Manual*, you must provide a name server address. You may also want to provide a secondary name server or domain name (DNS suffix).	If you select *Manual*, all DNS settings are as configured on this page. The Cisco TelePresence Advanced Media Gateway does not allow you to automatically configure the name server address if you have set a static IP address on the selected interface. For example, if you select *Via Port A DHCPv4* here but have also selected *Manual* in the IPv4 configuration section of the **Port A settings** page, the Cisco TelePresence Advanced Media Gateway will warn you that no DNS servers will be configured.
Host name	Specifies a name for the Cisco TelePresence Advanced Media Gateway.	Depending on your network configuration, you may be able to use this host name to communicate with the Cisco TelePresence Advanced Media Gateway, without needing to know its IP address.
Name server	The IP address of the name server.	Required if you select the *Manual* name server preference.
Secondary name server	Identifies an optional second name server.	The Cisco TelePresence Advanced Media Gateway queries the secondary DNS server if the primary is unavailable. If the first server is available but does not know an address, the Cisco TelePresence Advanced Media Gateway does not query the secondary DNS server.
Domain name (DNS suffix)	Specifies an optional suffix to add when performing DNS lookups.	Add a suffix if you want to use unqualified host names to refer to devices (instead of IP addresses). For example, if the domain name (suffix) is set to *cisco.com*, then a request to the name server to look up the IP address of host *endpoint* will actually look up *endpoint.cisco.com*.

View DNS status

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

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

Configuring IP routes settings

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

You may need to set up one or more routes to control how IP traffic flows in and out of the Cisco TelePresence Advanced Media Gateway. It is important that these routes are configured correctly, or you may be unable to make calls or access the web interface.

This topic describes the following items:

Port preferences

Field	Field description	Usage tips
IPv4 gateway preference	The IP address to which the Cisco TelePresence Advanced Media Gateway will send packets in the absence of more specific routing (see IP routes configuration).	You may only select Port A.

IP routes configuration

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

Add a new IP route

To add a new route:

1. Enter the IP address of the target network, and the mask length that defines the range of addresses.
2. Select whether the traffic to those addresses will be routed via **Port A**'s default gateway or a **Gateway** that you specify.
3. Click **Add IP route**.
   The new route is added to the list. If the route already exists, or aliases (overlaps) an existing route, the interface prompts you to correct the route.

Use the following table for reference:

Field	Field description	Usage tips

IP address / mask length	Use these fields to define the range of IP addresses to which this route applies. Enter the IP address of the target network in dotted quad format, setting any unfixed bits of the address to 0. Use the **mask length** field to specify how many bits are fixed (and thus how many are unfixed, giving the range of addresses).	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. The first 25 bits are fixed, which means that the last seven bits determine the range of addresses.
Route	Use this field to control how packets destined for addresses that match the specified pattern are routed.	You can select *Port A* or *Gateway*. If you select *Gateway* , specify the IP address of the gateway to which you want packets to be directed. If you select *Port A*, matching packets will be routed to Port A's default gateway (see Configuring network settings).

View or delete an existing IP route

Configured routes are listed below the **Add IP route** section. The following details are shown for each route:

- IP address pattern and mask.
- Where matching packets will be routed. Either *Port A* (meaning the default gateway configured for Port A) or <*IP address*> if a specific IP address has been specified.
- Whether the route was configured automatically as a consequence of other settings, or added manually.

The *default* route is configured automatically by your choice of *IPv4 gateway preference* field (see Port preferences) and cannot be deleted. Any packets destined for addresses that are not matched by your manually configured routes will be routed via the default gateway

You can delete manually configured routes. Select the appropriate check box and click **Delete selected**.

Current routes table

This table shows the current default gateway and name servers for Ethernet ports A and B. If you want to change the defaults for the Ethernet ports, go to **Network > Port A** or **Network > Port B**.

Configuring IP services

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

Use this page to allow or deny access to the listed web services on the Cisco TelePresence Advanced Media Gateway (see the table below for details).

To allow or deny access to a service, check or uncheck the box for the required service and (if necessary) edit the port numbers. Then click **Apply changes**.

To reset the values to their default settings, click **Reset to default**. Then click **Apply changes**.

Field	Field description	Usage tips
TCP service		
Web	Enable/disable web access on the appropriate port.	Web access is required to view and change the Cisco TelePresence Advanced Media Gateway web pages and read online help files. If you disable web access on Port A you will need to use the serial console interface to re-enable it. If a port is disabled, this option will be unavailable.
Secure web	Enable/disable secure (HTTPS) web access on the specified interface or change the port that is used for this service.	This field is only visible if the Cisco TelePresence Advanced Media Gateway has the *Encryption* feature key installed. For more information about installing feature keys, refer to Upgrading and backing up the Cisco TelePresence Advanced Media Gateway. By default, the Cisco TelePresence Advanced Media Gateway has its own SSL certificate and private key. You can upload a new private key and certificate if required (see Configuring SSL certificates). If a port is disabled, this option will be unavailable.
Incoming SIP (TCP)	Allow/reject incoming calls to the Cisco TelePresence Advanced Media Gateway using SIP over TCP or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to SIP devices being made by the Cisco TelePresence Advanced Media Gateway. If a port is disabled, this option will be unavailable.
Incoming Encrypted SIP (TLS)	Allow/reject incoming encrypted SIP calls to the Cisco TelePresence Advanced Media Gateway using SIP over TLS or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to SIP devices being made by the Cisco TelePresence Advanced Media Gateway. If a port is disabled, this option will be unavailable.

FTP	Enable/disable FTP access on the specified interface or change the port that is used for this service.	FTP can be used to upload and download Cisco TelePresence Advanced Media Gateway configuration. FTP is used only for configuration file changes, not for Microsoft© Lync® / MOC file transfers. You should consider disabling FTP access on any port that is outside your organization's firewall. If you require advanced security for the Cisco TelePresence Advanced Media Gateway, disable the FTP service. If a port is disabled, this option will be unavailable.
UDP service		
SNMP	Enable/disable receiving SNMP protocol on this port or change the port that is used for this service.	If a port is disabled, this option will be unavailable. By default, SNMP traps are sent to port UDP port 162 (on the destination network management station). This is configurable (see Configuring SNMP settings). If you require advanced security for the Cisco TelePresence Advanced Media Gateway, disable the SNMP service.
SIP (UDP)	Allow/reject incoming and outgoing calls to the Cisco TelePresence Advanced Media Gateway using SIP over UDP or change the port that is used for this service.	Disabling this option will prevent calls using SIP over UDP. If a port is disabled, this option will be unavailable.

Configuring SNMP settings

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

The Cisco TelePresence Advanced Media Gateway sends out an SNMP trap when the device is shut down or started up. The SNMP MIBs are read-only.

Note: The 'system uptime' in the trap is the time since SNMP was initialized on the Cisco TelePresence Advanced Media Gateway (and therefore differs from the **Uptime** reported by the Cisco TelePresence Advanced Media Gateway on the **Status > General** page).

From the SMNP page you can work with settings related to:

- System information
- Configured trap receivers
- Access control

Click **Update SNMP settings** to apply any changes.

System information

Field	Field description	Usage tips
Name	Identifies the Cisco TelePresence Advanced Media Gateway in the SNMP system MIB.	Usually you would give every device a unique name. The default setting is *Cisco AM GW*.
Location	Location that appears in the system MIB.	Optional. If you have multiple Cisco TelePresence Advanced Media Gateways, this setting is useful to identify them in the MIB. The default setting is *Unknown*.
Contact	Contact details that appear in the system MIB.	Optional. The default setting is *Unknown*. Add the administrator's email address or name to identify who to contact if 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	Description that appears in the system MIB.	Optional. By default this will indicate the model number of the Cisco TelePresence Advanced Media Gateway. Can be used to provide more information about the gateway.

Configured trap receivers

Field	Field description	Usage tips
Enable traps	Select this check box to enable the Cisco TelePresence Advanced Media Gateway 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.	To select this check box you must first select **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 Cisco TelePresence Advanced Media Gateway are all SNMP v1 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.

Access control

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

Configuring QoS settings

To configure Quality of Service (QoS) on the Cisco TelePresence Advanced Media Gateway for audio and video, go to **Network > QoS**.

QoS is a term that refers to a network's ability to customize the treatment of specific classes of data. For example, QoS can be used to prioritize audio transmissions and video transmissions over HTTP traffic. These settings affect all audio and video packets to H.323 endpoints. All other packets are sent with a QoS of 0.

The Cisco TelePresence Advanced Media Gateway allows you to set a 6-bit value for *Type of Service* that can be interpreted by networks as either Type of Service (ToS) or Differentiated Services (DiffServ).

Note: Do not alter the QoS settings unless you need to do so.

To configure the QoS settings you need to enter a 6-bit binary value.

Further information about QoS, including values for ToS and DiffServ, can be found in the following RFCs, available on the Internet Engineering Task Force web site www.ietf.org:

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

This topic describes the following items:

About QoS configuration settings

The table below describes the settings on the **Network > QoS** page.

Click **Update QoS settings** to apply any changes.

Field	Field description	Usage tips
Audio	Six bit binary field for prioritizing audio data packets on the network.	Do not alter this setting unless you need to.
Video	Six bit binary field for prioritizing video data packets on the network.	Do not alter this setting unless you need to.

ToS configuration

ToS configuration represents a tradeoff between the abstract parameters of precedence, delay, throughput, and reliability. ToS uses six out of a possible eight bits. The Cisco TelePresence Advanced Media Gateway allows you to set bits 0 to 5, and will place 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 Cisco TelePresence Advanced Media Gateway interface.

You need to create a balance by assigning priority to audio and video packets whilst not causing undue delay to other packets on the network. 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 Cisco TelePresence Advanced Media Gateway allows you to set bits 0 to 5, and will place zeros for bits 6 and 7. The codepoint is interpreted by DiffServ nodes to determine how the packet is treated.

Default settings

The default settings for QoS are:

- *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 Diff Serv, this means expedited forwarding.
- *Video 100010*:
  - For ToS, this means IP precedence is set to 4 giving quite high priority (but not quite 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).

To return the settings to their default values, click **Reset to default**.

Configuring SSL certificates

If the Cisco TelePresence Advanced Media Gateway has the *Secure management (HTTPS)* or *Encryption* feature key installed, and you enable *Secure web* on the **Network > Services** page, you will be able to access the web interface of the Cisco TelePresence Advanced Media Gateway using HTTPS.

Note: A certificate and key are also required if you select the SIP TLS service in **Network > Services**.

The Cisco TelePresence Advanced Media Gateway has a local certificate and private key pre-installed and it uses this to authenticate itself to the browser when you access the unit using HTTPS. However, we recommend that you upload your own certificate and private key to ensure security because all Cisco TelePresence Advanced Media Gateways have identical default certificates and keys.

Uploading or removing a custom certificate

To upload your own certificate and key, go to **Network > SSL certificates**. Complete the fields using the table below for help and click **Upload certificate and key**. Note that you must upload a certificate and key simultaneously. After uploading a new certificate and key, you must restart the Cisco TelePresence Advanced Media Gateway.

If you have uploaded your own certificate and key, you can remove it later if necessary, by clicking **Delete custom certificate and key**.

Fields on the SSL certificates page

The following table details the fields you see on the **Network > SSL certificates** page.

Field	Field description	Usage tips
Local certificate		

Subject	The details of the business to which the certificate has been issued: ■ C: the country where the business is registered ■ ST: the state or province where the business is located ■ L: the locality or city where the business is located ■ O: the legal name of the business ■ OU: the organizational unit or department ■ CN: the common name for the certificate, or the domain name	
Issuer	Details of the issuer of the certificate.	Where the certificate has been self-issued, these details will be the same as for the **Subject**.
Issued	The date on which the certificate was issued.	
Expires	The date on which the certificate will expire.	
Private key	Whether the private key matches the certificate.	Your web browser uses the SSL certificate's public key to encrypt the data that it sends back to the Cisco TelePresence Advanced Media Gateway. The private key is used by the Cisco TelePresence Advanced Media Gateway to decrypt that data. If the **Private key** field shows *Key matches certificate* then the data is securely encrypted in both directions.
Local certificate configuration		
Certificate	If your organization has bought a certificate, or you have your own way of generating certificates, you can upload it. Click **Choose File** to find and select the certificate file.	
Private key	Click **Choose File** to find and select the private key file that accompanies your certificate.	

Private key encryption password	If your private key is stored in an encrypted format, you must enter the password here so that you can upload the key to the Cisco TelePresence Advanced Media Gateway.	
Trust store		
Subject	The details of the trust store certificate. Usually a certificate issued by the authority that is used to verify the local certificate.	
Issuer	The details of the issuer of the trust store certificate.	These are the details of the trusted certification authority.
Issued	The date on which the trust store certificate was issued.	
Expires	The date on which the trust store certificate will expire.	
Trust store	The trust store is required to verify the identity of the remote end of a SIP TLS connection (incoming or outgoing call, or registration).	Browse to and select the trust store certificate file and then click **Upload trust store**. The store may contain multiple certificates. If verification is required (see next setting) the certificate of the remote party is verified against the trust store. The remote certificate must be in either the trust store or the trust chain of one of its certificates. To remove or replace the trust store, click **Delete trust store**.
Certificate verification settings	Determines the circumstances in which the remote certificate must be verified with the trust store.	Select one of: ■ *No verification*: The remote certificate is never verified against the trust store (remote end always trusted). ■ *Outgoing connections only*: The Cisco TelePresence Advanced Media Gateway attempts to verify the remote certificate for all outgoing SIP TLS connections. ■ *Outgoing connections and incoming calls*: The Cisco TelePresence Advanced Media Gateway attempts to verify the remote certificate for all incoming and outgoing SIP TLS connections. Click **Apply changes**.

Network connectivity testing

You can use the **Network connectivity** page to troubleshoot network issues between the Cisco TelePresence Advanced Media Gateway and a remote video conferencing device.

On this page you can ping another device from the Cisco TelePresence Advanced Media Gateway web interface and trace the route to that device. The results show whether or not you have network connectivity between the Cisco TelePresence Advanced Media Gateway and the remote host.

To test connectivity

To test connectivity with a remote device:

1. Go to **Network > Connectivity**.
2. In the text box, enter the IP address or hostname of the device to which you want to test connectivity.
3. Click **Test connectivity**.

Test results

The results show the outbound interface for the query and the IP address of the remote host.

The ping results show the roundtrip time in milliseconds and the TTL (Time To Live) value on the echo reply.

For each intermediate host (typically routers) between the Cisco TelePresence Advanced Media Gateway and the remote host, the host's IP address and response time are shown.

Non-responses or unrecognized responses

Not all devices will respond to the messages from the Cisco TelePresence Advanced Media Gateway. Routing entries for non-responding devices are shown as <*unknown*>. Some devices are known to send invalid ICMP response packets (for example, with invalid ICMP checksums). Invalid ICMP responses are also not recognized by the Cisco TelePresence Advanced Media Gateway so these responses are also shown as <*unknown*>.

Note: The ping message is sent from the Cisco TelePresence Advanced Media Gateway to the IP address of the remote host. Therefore, if the Cisco TelePresence Advanced Media Gateway has an IP route to the given host, regardless of whether that route lies out of port A or port B, the ping will be successful. This feature allows the Cisco TelePresence Advanced Media Gateway's IP routing configuration to be tested, and it has no security implications.

Note: If you are unable to ping the remote host, then check your network configuration - especially any firewalls using NAT.

Related topics

Configuring network settings

Configuration

This section describes how to perform configuration tasks, such as specifying system settings and resetting the system time.

Configuring system settings

To configure system settings, go to **Settings > System settings**. From here you can configure various settings relating to calls, security, and the user interface.

Click **Apply changes** to apply any changes.

Field	Field description	Usage tips
Call settings		
Motion / sharpness trade off	Choose the unit-wide setting for motion/sharpness trade off. The options are: ■ *Favor motion*: The Cisco TelePresence Advanced Media Gateway will try and use a high frame rate. That is, the gateway will strongly favor a resolution of at least 25 frames per second ■ *Favor sharpness*: The Cisco TelePresence Advanced Media Gateway will use the highest resolution that is appropriate for what is being viewed ■ *Balanced*: The Cisco TelePresence Advanced Media Gateway will select settings that balance resolution and frame rate (where the frame rate will not be less than 12 frames per second)	The settings for motion (frames per second) and sharpness (frame size or resolution) are negotiated between the participant and the Cisco TelePresence Advanced Media Gateway. This setting controls how the gateway negotiates the settings to be used with a participant.
Default bandwidth from AM Gateway	Identifies the network capacity (measured in bits per second) used by the media channels established by the Cisco TelePresence Advanced Media Gateway to a single participant.	When the Cisco TelePresence Advanced Media Gateway makes a call to a participant, it 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 and video channels combined.
Default bandwidth to AM Gateway	Sets the bandwidth that the Cisco TelePresence Advanced Media Gateway will advertise to the participant.	

Convert out-of-band to in-band DTMF	Select this option to have the Cisco TelePresence Advanced Media Gateway convert any out-of-band DTMF tones that it receives into in-band DTMF.	Both H.323 and SIP can send DTMF tones in-band (within the audio stream) and out-of-band. Out-of-band DTMF has the advantage that the tones do not sound over any voice, but will not be compatible with analogue telephones. For example, if you are calling out from an IP phone system through an Cisco TelePresence Advanced Media Gateway to a traditional call center with an automated audio menu, you must be using in-band DTMF tones to select an option, so this option may be required. IP phones can interpret in-band DTMF and will continue to work as expected with this option enabled.
Overlay participant name	Controls whether participants shown in view panes are accompanied by their supplied name.	Check the box to enable overlaying of participant names.
Welcome message	Allows you to enter a message that will be seen by participants joining calls on the Cisco TelePresence Advanced Media Gateway. The message is displayed at the bottom of a participant's conference display.	The duration of the message is configured using the **Welcome message duration** control (see below).
Welcome message duration	Controls for how long (if at all) participants joining a call will see the welcome message.	Choose from: ■ *<never show>* ■ *10 seconds* ■ *30 seconds* ■ *1 minute* ■ *<permanent>*
ClearVision	When enabled, the Cisco TelePresence Advanced Media Gateway will upscale video streams from participants who are sending low resolution video, with the purpose of making best use of the gateway's HD video capabilities.	The Cisco TelePresence Advanced Media Gateway uses intelligent resolution upscaling technology to improve the clarity of low-resolution video. Check this setting to enable it to do so. ClearVision is not available if your Cisco TelePresence Advanced Media Gateway is running in Standard definition mode. Go to **Settings > Resource settings** to configure this.
Allow widescreen video cropping	Determines how the Cisco TelePresence Advanced Media Gateway handles incoming widescreen video for standard 4:3 output configurations.	With this option enabled, the widescreen input video is cropped by the gateway rather than letterboxed.

Flow control on video errors	Allows the Cisco TelePresence Advanced Media Gateway to request a Microsoft® Lync™ / MOC client or a Communicator for Mac client to send lower speed video if the gateway fails to receive all the packets which comprise the far end's video stream.	The Cisco TelePresence Advanced Media Gateway can send these messages to request a decrease in the bandwidth of the video being sent by a Lync / MOC or Communicator for Mac client, based on the quality of video received by the gateway. If there is a bandwidth limitation in the path between the client endpoint and the Cisco TelePresence Advanced Media Gateway, it is better for the gateway to receive every packet of a lower rate stream than to miss some packets of a higher rate stream.
Conceal video errors	In the case of Lync / MOC clients, prevents the display of video frames with errors. When this setting is enabled, if the Cisco TelePresence Advanced Media Gateway encounters a video frame with errors then it sends instead the last fully decoded frame without errors to the Lync / MOC client.	Be aware that this setting may lead to the user seeing multiple frozen frames when there are video errors, even if the error itself is only on a very small portion of the video. This effect is usually caused by packet loss in the network, although it can be due to other causes.
Limit transmitted video from Communicator for Mac clients to VGA	In some Mac-based scenarios HD video can consume too much CPU on the MAC, which may lead to poor quality audio to and from the Communicator for Mac client. This setting restricts the video from Communicator for Mac clients to VGA. By reducing the CPU load on the Mac this minimizes the chances of degraded audio to and from the client. The client will still be able to *receive* HD video.	This setting has no effect on Microsoft Lync / MOC clients.

Video transmit size optimization	Allows the Cisco TelePresence Advanced Media Gateway to vary the resolution and codec of the video being sent to a remote participant within the video channel established to that participant. The options are: ■ *None*: Do not allow video size to be changed during transmission ■ *Dynamic resolution only*: Allow video size to be optimized during transmission ■ *Dynamic codec and resolution*: Allow video size to be optimized during transmission and/or dynamic codec selection	With this option enabled, the Cisco TelePresence Advanced Media Gateway can, for instance, decide to send CIF video within a 4CIF channel if this will increase the viewed video quality. The circumstances under which decreasing the video resolution can improve the video quality include: ■ if the original size of the viewed video is smaller than the outgoing channel ■ if the remote participant has used flow control commands to reduce the bandwidth of the Cisco TelePresence Advanced Media Gateway video transmission Typically, lowering the resolution means that the Cisco TelePresence Advanced Media Gateway can transmit video at a higher frame-rate.
Video resolution selection mode	Influences the choice of outgoing video resolution made by the AM Gateway. ■ *Default*: The Cisco TelePresence Advanced Media Gateway will use its normal internal algorithms to dynamically decide which resolution to send in order to maximize the received video quality. ■ *Favor 448p*: The Cisco TelePresence Advanced Media Gateway 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 *Default* unless your environment dictates 448p or w448p resolutions only.
Maximum transmitted video packet size	Sets the maximum payload size (in bytes) of the packets sent by the Cisco TelePresence Advanced Media Gateway for outgoing video streams (from the Cisco TelePresence Advanced Media Gateway to connected video participants).	Typically, you only need to set this value to lower than the default (1400 bytes) if there was a known packet size restriction in the path between the Cisco TelePresence Advanced Media Gateway and potential connected participants. Video streams generally contain packets of different lengths. This parameter only sets the *maximum* size of a transmitted network datagram. The Cisco TelePresence Advanced Media Gateway optimally splits the video stream into packets of this size or smaller. Thus, most transmitted packets will not reach this maximum size.

Audio codecs from AM Gateway	Restricts the Cisco TelePresence Advanced Media Gateway's choice of audio codecs to be used for transmitting audio to participants.	When communicating with a participant, the Cisco TelePresence Advanced Media Gateway receives a list of supported audio codecs from the participant. The Cisco TelePresence Advanced Media Gateway chooses an audio codec from those available, and sends audio data to the participant in that format.
Audio codecs to AM Gateway	Determines which audio codecs the Cisco TelePresence Advanced Media Gateway advertises to remote participants, restricting the participants' choice of channels available for sending audio data to the Cisco TelePresence Advanced Media Gateway. Some endpoints and network equipment do not support as many codecs as the Cisco TelePresence Advanced Media Gateway can offer. For best interoperation we recommend that at least one audio codec is left unselected in the **Audio codecs to AM Gateway** section.	
Video codecs from AM Gateway	Restricts the Cisco TelePresence Advanced Media Gateway's choice of video codecs to be used for transmitting video to participants.	When communicating with a participant, the Cisco TelePresence Advanced Media Gateway receives a list of supported video codecs from the participant. The Cisco TelePresence Advanced Media Gateway chooses a video codec from those available, and sends video data to the participant in that format.
Video codecs to AM Gateway	Determines which video codecs the Cisco TelePresence Advanced Media Gateway advertises to remote participants, restricting the participants' choice of channels available for sending video data to the Cisco TelePresence Advanced Media Gateway.	
User interface settings		
Show video thumbnail images	Choose whether you want to show video thumbnail images or not. This controls whether or not you will see a preview of what a participant sees in the conference and participants pages that can show a preview of the conference. Thumbnail images will not be shown for calls where encryption is required.	

Security settings		
Redirect HTTP requests to HTTPS	Enable this option to have HTTP requests to the Cisco TelePresence Advanced Media Gateway automatically redirected to HTTPS.	This option is unavailable if either HTTP (*Web*) or HTTPS (*Secure web*) access is disabled on the **Network > Services** page.

Related topics

Configuring IP services

Configuring resource settings

To configure resource settings, go to **Settings > Resource settings**. From here you can configure the video capacity of the Cisco TelePresence Advanced Media Gateway.

Click **Apply changes** after making any changes. The changes will not take effect until you restart the Cisco TelePresence Advanced Media Gateway. Click **OK** at the restart prompt and you will be directed to the Shutdown page.

Field	Field description	Usage tips
Call capability	The Cisco TelePresence Advanced Media Gateway has the following video capacity modes: ■ *Allow HD* supports high definition video calls at up to 720p at 30fps ■ *SD only* supports calls at up to w448p at 30fps	You must restart the Cisco TelePresence Advanced Media Gateway for any changes to this setting to take effect.
Call capacity	Shows the number of calls supported in the selected mode. This depends on the Cisco TelePresence Advanced Media Gateway model that you are using.	

Related topics

Configuring system settings.

Displaying and resetting system time

To configure time settings, go to **Settings > Time**.

You can manually set the system date and time for the Cisco TelePresence Advanced Media Gateway or let it use the Network Time Protocol (NTP) to synchronize its time.

System time

The current system date and time according to the Cisco TelePresence Advanced Media Gateway is displayed. To manually set the system date and time, type the new values and click **Change system time**.

NTP

The Cisco TelePresence Advanced Media Gateway supports the NTP protocol. If you want the Cisco TelePresence Advanced Media Gateway to automatically synchronize with an NTP server, enter the NTP settings and then click **Update NTP settings**.

The Cisco TelePresence Advanced Media Gateway synchronizes with the NTP server every hour.

If the NTP server is not local, the Cisco TelePresence Advanced Media Gateway 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 (see **Network > Routes**).

If a firewall exists between the Cisco TelePresence Advanced Media Gateway and the NTP server, configure the firewall to allow NTP traffic to UDP port 123.

Field	Field description	Usage tips
Enable NTP	Check the box if you want to enable the NTP protocol on the Cisco TelePresence Advanced Media Gateway.	
UTC offset	The offset of the time zone that you are in from UTC. The offset allows you to set a local time appropriate to the geographic location of the gateway or to adjust for daylight saving.	The offset can be -12 to 14 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 manually update this offset to account for regional changes to time zones, such as British Summer Time and other daylight saving schemes.
NTP host	The IP address or hostname of the server that is acting as the time keeper for the network.	

Using NTP over NAT (Network Address Translation)

No extra configuration is required if the NAT is local to the Cisco TelePresence Advanced Media Gateway's network.

If NAT is used on the NTP server's local network, you must configure the NAT forwarding table to forward NTP data from the Cisco TelePresence Advanced Media Gateway to UDP port 123 on the NTP server.

Related topics

Configuring IP routes settings

Maintenance

This section describes how to shutdown and restart the Cisco TelePresence Advanced Media Gateway, and how to perform backups and software upgrades.

Shutting down and restarting the gateway

On occasions you will need to shut down the Cisco TelePresence Advanced Media Gateway, typically to restart the device as part of an upgrade. You should also shut down the Cisco TelePresence Advanced Media Gateway before intentionally removing power from it.

Shutting down the gateway will disconnect all active calls.

To shut down the gateway:

1. Go to **Maintenance > Shutdown**.
2. Click **Shut down AM Gateway**.
   The button changes to **Confirm AM Gateway shutdown**.
3. Click the button again to confirm the shutdown.
4. When the shutdown completes, the button changes to **Restart AM Gateway**.
5. Click the button to restart the gateway.

Upgrading and backing up the gateway

This topic describes how to carry out the following tasks:

- Upgrading the main software image
- Upgrading the loader software image
- Backing up and restoring the configuration
- Activating the gateway and installing feature keys

Upgrading the main software image

The main Cisco TelePresence Advanced Media Gateway software image is the only firmware component that you will need to upgrade.

To upgrade the main software image:

1. Go to **Maintenance > Upgrade**.
2. Check the **Current version** of the main software image to verify the currently installed version.
3. Log on to the company support pages to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.
5. Unzip the image file.
6. Log on to the Cisco TelePresence Advanced Media Gateway web browser interface.
7. Go to **Maintenance > 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 Cisco TelePresence Advanced Media Gateway, and a new browser window opens to indicate the upload progress. When finished, the browser window refreshes and indicates that the "Main image upgrade completed."
10. The upgrade status displays in the **AM Gateway software upgrade status** field.
11. Shutdown and restart the Cisco TelePresence Advanced Media Gateway (see Shutting down and restarting the gateway).

Upgrading the loader software image

Upgrades for the loader software image are not typically available as often as upgrades to the main software image.

To upgrade the loader software image:

1. Go to **Settings > Upgrade**.
2. Check the **Current version** of the loader software to verify the currently installed version.
3. Go to the software download pages of the web site to identify whether a more recent image is available.
4. Download the latest available image and save it to a local hard drive.

5. Unzip the image file.
6. Click **Browse** to locate the unzipped file on your hard drive.
7. Click **Upload software image**. The browser begins uploading the file to the Cisco TelePresence Advanced Media Gateway, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Loader image upgrade completed."
8. The upgrade status displays in the **Loader upgrade status** field.
9. Shutdown and restart the Cisco TelePresence Advanced Media Gateway (see Shutting down and restarting the gateway).

Backing up and restoring the 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 Cisco TelePresence Advanced Media Gateway 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 in order to restore from a file backed up from the same Cisco TelePresence Advanced Media Gateway or to replace an out-of-service gateway. If you copy the network settings from a different, active, gateway and there is a clash (for instance, both are now configured to use the same fixed IP address) then one or both boxes may become unreachable via IP.
  If you do not select **Network settings**, then subject to one exception the restore operation will not overwrite the existing network settings. The exception is the QoS settings, which are overwritten regardless of the **Network settings** check box.
- 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.

You can also back up and restore the configuration of the Cisco TelePresence Advanced Media Gateway using FTP (see Backing up and restoring the configuration via FTP).

Activating the gateway and installing feature keys

The Cisco TelePresence Advanced Media Gateway requires activation before most of its features can be used. (If the Cisco TelePresence Advanced Media Gateway 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.)

If this is a new Cisco TelePresence Advanced Media Gateway you should receive the gateway already activated. In cases where it is not pre-activated, or you have upgraded to a newer firmware version, or want to enable a new feature, you may need to contact your supplier to obtain an appropriate feature key

(activation code). Feature keys are unique to a particular Cisco TelePresence Advanced Media Gateway so you will need the serial number of the gateway.

Regardless of whether you are activating the Cisco TelePresence Advanced Media Gateway itself or installing a feature key to activate an advanced feature, the process is the same.

To activate the gateway or install a feature key:

1. Check the **Activated features** list (Cisco TelePresence Advanced Media Gateway activation is shown in this same list) to verify that the feature you require is not already activated.
2. Enter the new feature key (activation code) into the **Activation code** field exactly as you received it, including any dashes.
3. Click **Update features**. The browser window will refresh and list the newly activated feature, with the feature key beside it. Feature keys 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 keys 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. We recommend that you record the feature key in case you need to re-enter it in the future.

Successful gateway or feature activation has immediate effect and will persist even if the Cisco TelePresence Advanced Media Gateway is restarted.

Note: You can remove some feature keys by clicking the **Remove** link next to the feature key in this page.

Backing up and restoring the configuration via FTP

You can back up and restore the configuration of the Cisco TelePresence Advanced Media Gateway through its web interface. To do so, go to **Settings > Upgrade**. For more information, see Upgrading and backing up the gateway.

You can also save the configuration of the Cisco TelePresence Advanced Media Gateway using FTP.

To back up the configuration via FTP:

1. Ensure that **FTP** is enabled on the **Network > Services** page.
2. Connect to the Cisco TelePresence Advanced Media Gateway using an FTP client. When asked for a user name and password, enter the same ones that you use to log in to the Cisco TelePresence Advanced Media Gateway's web interface as an administrator.
   You will see a file called configuration.xml. This contains the complete configuration of your Cisco TelePresence Advanced Media Gateway.
3. Copy this file and store it somewhere safe.

The backup process is now complete.

To restore the configuration using FTP:

1. Locate the copy of the configuration.xml file that you want to restore.
2. Ensure that **FTP** is enabled on the **Network > Services** page.
3. Connect to the Cisco TelePresence Advanced Media Gateway using an FTP client. When asked for a user name and password, use the same ones that use to log in to the Cisco TelePresence Advanced Media Gateway's web interface as an administrator.
4. Upload your configuration.xml file to the Cisco TelePresence Advanced Media Gateway, overwriting the existing file on the gateway.

The restore process is now complete.

Note: The same process can be used to transfer a configuration from one Cisco TelePresence Advanced Media Gateway to another of the same model number. However, before doing this, be sure to keep a copy of the original feature keys from the Cisco TelePresence Advanced Media Gateway whose configuration is being replaced.

If you are using the configuration file to configure a duplicate Cisco TelePresence Advanced Media Gateway, for example in a network where you have more than one, be aware that if the original Cisco TelePresence Advanced Media Gateway was configured with a static address, you will need to reconfigure the IP address on any others on which you have used the configuration file.

Calls

This section describes how to display information about calls, including the active calls list and participant information.

Displaying the active calls list

The **Calls** page displays all calls that are currently active on the Cisco TelePresence Advanced Media Gateway. You can disconnect an active call from the **Calls** page.

Field	Field Description	Usage tips
Source	The alias of the participant that initiated the call.	Click the alias name to go to the **Participant statistics** page for the source alias (see Displaying participant statistics for more information).
Destination	The alias of the participant that is receiving the call.	Click the alias name to go to the **Participant statistics** page for the destination alias. (see Displaying participant statistics for more information).
Start time	The time that the call was initiated.	Click **Start time** to toggle the order of the calls in the list.
Duration	The length of time the call has been active.	

To disconnect an active call

1. Go to **Calls**.
2. Check the box next to the call or calls you want to disconnect.
3. Click **Disconnect selected**.

Displaying call details

To view the **Call details** page, go to **Calls** and click the time stamp in the **Time** column for the call you want to display.

The **Call details** page lets you inspect detailed information about active calls:

Field	Field description	Usage tips
Call details		
Start time	Time stamp that records when the call was initiated.	
Duration	The total length of time that the call has been active.	This field is automatically refreshed.
Controls	A button that allows you to disconnect the call if necessary.	Click the button to disconnect the call.
Source		
Name	The alias of the participant that initiated the call.	
Proxy	The IP address of the participant that initiated the call.	
Status	Details of the transmitted (Tx) and received (Rx) audio and video streams.	
Encryption	A flag indicating whether or not the call is being encrypted by the source participant.	
Preview	A still JPEG image of the video that is being transmitted by the source participant. This field is disabled for encrypted calls.	Click the image to refresh it.
Destination		
Name	The alias of the participant that is receiving the call.	
IP	The IP address of the participant that is receiving the call.	
Status	Details of the transmitted (Tx) and received (Rx) audio and video streams.	
Encryption	A flag indicating whether or not the call is being encrypted by the destination participant.	
Preview	A still JPEG image of the video that is being transmitted by the destination participant.	Click the image to refresh it.

Displaying participant statistics

To view the **Participant statistics** page, go to **Calls** and click a source or destination alias.

The page displays statistics about the video and audio streams between individual callers (participants) and the Cisco TelePresence Advanced Media Gateway:

- Received audio statistics
- Transmitted audio statistics
- Received audio RTCP statistics
- Transmitted audio RTCP statistics
- Received video statistics
- Transmitted video statistics
- Received video RTCP statistics
- Transmitted video RTCP statistics

Refer to the table below for additional information.

Field	Field description	Usage tips
AUDIO		
Received audio		
Receive stream	The audio codec in use, along with the current packet size (in milliseconds) if known.	If the Cisco TelePresence Advanced Media Gateway has received information that a participant 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 the participant.	This field will only appear if the encryption feature key is present on the Cisco TelePresence Advanced Media Gateway.
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 participant.	

Packets received	The number of audio packets destined for the Cisco TelePresence Advanced Media Gateway from the participant.	
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.
Transmitted audio		
Transmit stream	The audio codec being sent from the Cisco TelePresence Advanced Media Gateway to the participant, 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 receive stream by the participant.	This field will only appear if the encryption feature key is present on the Cisco TelePresence Advanced Media Gateway.
Packets sent	A count of the number of packets that have been sent from the Cisco TelePresence Advanced Media Gateway to the participant.	
Received audio RTCP		
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 Cisco TelePresence Advanced Media Gateway.	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 Cisco TelePresence Advanced Media Gateway.
Packet loss reported	A count of the reported packet loss on the control channel.	
Sender reports	A count of the number of "sender report" type RTCP packets sent by the Cisco TelePresence Advanced Media Gateway.	These are typically sent by any device that is sending RTP media.
Transmitted audio RTCP		
RTCP transmit address	The IP address and port to which the Cisco TelePresence Advanced Media Gateway is sending RTCP packets about this stream.	
Receiver reports	A count of the number of "receiver report" type RTCP packets seen by the Cisco TelePresence Advanced Media Gateway.	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 Cisco TelePresence Advanced Media Gateway.
Sender reports	A count of the number of "sender report" type RTCP packets received by the Cisco TelePresence Advanced Media Gateway.	These are typically sent by any device that is sending RTP media.
Packets sent	A count of the number of packets that have been sent from the Cisco TelePresence Advanced Media Gateway to the participant.	
VIDEO		
Received video		
Receive stream	The codec in use and the size of the picture that the Cisco TelePresence Advanced Media Gateway 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 audio receive stream by the participant.	This field will only appear if the encryption feature key is present on the Cisco TelePresence Advanced Media Gateway.
Channel bit rate	The negotiated bit rate available for the participant to send video in.	This value represents the maximum amount of video traffic that the remote participant will send to the Cisco TelePresence Advanced Media Gateway. It may send less data than this (if it does not need to use the full channel bit rate or the Cisco TelePresence Advanced Media Gateway has requested a lower rate), but it should not send more.
Receive bit rate	The bit rate (in bits per second) that the Cisco TelePresence Advanced Media Gateway has requested that the remote participant sends. The most-recently measured actual bit rate displays in parentheses.	This value might be less than the *Channel bit rate*.
Received jitter	Represents the variation in video packet at arrival time at the Cisco TelePresence Advanced Media Gateway.	
Packets received	The number of video packets destined for the Cisco TelePresence Advanced Media Gateway from the participant	
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 participant.	
Frame errors	The number of frames with errors versus the total number of video frames received.	
Transmitted video		
Transmit stream	The codec, size and type of video being sent from the Cisco TelePresence Advanced Media Gateway to the participant.	
Transmit address	The IP address and port of the device to which the Cisco TelePresence Advanced Media Gateway is sending video.	

Encryption	Whether or not encryption is being used on the audio receive stream by the participant.	This field will only appear if the encryption feature key is present on the Cisco TelePresence Advanced Media Gateway.
Channel bit rate	The negotiated available bandwidth for the Cisco TelePresence Advanced Media Gateway to send video to the participant in.	
Transmit bit rate	The bit rate the Cisco TelePresence Advanced Media Gateway 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 Cisco TelePresence Advanced Media Gateway, displays in parentheses.	The *Transmit bit rate* value might be less than the *Channel bit rate*.
Packets sent	The number of video packets sent from the Cisco TelePresence Advanced Media Gateway to the participant.	
Frame rate	The frame rate of the video stream currently being sent to the participant.	
Temporal/spatial	A number that represents the tradeoff between video quality and frame rate.	A smaller number implies that the Cisco TelePresence Advanced Media Gateway prioritizes sending quality video at the expense of a lower frame rate. A larger number implies that the Cisco TelePresence Advanced Media Gateway is prepared to send lower quality video at a higher frame rate.
Received video RTCP		
RTCP receive address	The IP address and port to which RTCP 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 Cisco TelePresence Advanced Media Gateway.	A single RTCP packet may contain more than one report of more than one type. These are generally sent by any device receiving RTP media from the network and are used for auditing bandwidth, errors, and so on by the Cisco TelePresence Advanced Media Gateway.
Packet loss reported	A count of the reported packet loss on the control channel.	

Sender reports	A count of the number of "sender report" type RTCP packets sent by the Cisco TelePresence Advanced Media Gateway.	These are typically sent by any device that is sending RTP media.
Estimated bandwidth	The bandwidth that the Microsoft© Lync® / MOC client estimates is available for receiving calls from the Cisco TelePresence Advanced Media Gateway.	
Packet loss notifications	The number of packets the Cisco TelePresence Advanced Media Gateway detects has been lost during the call. If there is packet loss, the field also shows the sequence number of the last packet that was lost.	
Video preference	A message sent from the Lync / MOC client to the Cisco TelePresence Advanced Media Gateway to indicate the preferred video resolution for the call. This is set by the MOC window size.	
Other	A count of the number of reports seen by the Cisco TelePresence Advanced Media Gateway that are neither sender nor receiver reports.	
Transmitted video RTCP		
RTCP transmit address	The IP address and port to which the Cisco TelePresence Advanced Media Gateway is sending RTCP packets about this stream.	
Receiver reports	A count of the number of "receiver report" type RTCP packets seen by the Cisco TelePresence Advanced Media Gateway.	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 Cisco TelePresence Advanced Media Gateway.
Sender reports	A count of the number of "sender report" type RTCP packets sent by the Cisco TelePresence Advanced Media Gateway.	These are typically sent by any device that is sending RTP media.
Estimated bandwidth	The bandwidth that the Lync / MOC client estimates is available for transmitting calls to the Cisco TelePresence Advanced Media Gateway.	

Packet loss notifications	The number of packets the Lync / MOC client detects has been lost during the call. If there is packet loss, the field also shows the sequence number of the last packet that was lost.
Video preference	A message sent from the Cisco TelePresence Advanced Media Gateway to the Lync/ MOC client indicates the preferred video resolution for the call.
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 participant diagnostics

Displaying participant diagnostics

To view the **Participant diagnostics** page, go to **Calls** and click a source or destination alias; then click **Diagnostics**.

The page displays diagnostic information about the selected call participant's connection to the Cisco TelePresence Advanced Media Gateway. You are unlikely to need to use the information on this page except when troubleshooting specific issues under the guidance of Cisco customer support.

Related topics

Displaying participant statistics

Proxies

This section describes how to manage proxies.

Displaying the proxy list

The **Proxies** page displays a list of the proxies configured for your Cisco TelePresence Advanced Media Gateway. The proxies list controls which Cisco TelePresence Video Communication Server (Cisco VCS) the Cisco TelePresence Advanced Media Gateway can accept calls from.

Each Cisco VCS required as a proxy must be listed in the proxies list. Calls received by the Cisco TelePresence Advanced Media Gateway from an IP address that is not on the proxies list are rejected.

Note: The Cisco TelePresence Advanced Media Gateway must also be configured as a neighbor on any Cisco VCS in the proxy list that is running software version X6.1 or earlier. This is not needed for any Cisco VCS running software version X7 or later.

The table below explains the information shown on the **Proxies** page.

Field	Description
Name	A descriptive name that identifies the proxy.
Address	The IP address of the proxy.

Related topics

Adding, editing and deleting proxies

Adding, editing and deleting proxies

You can add a new proxy for the Cisco TelePresence Advanced Media Gateway or edit or delete an existing proxy.

Adding a proxy

1. Go to **Proxies** > **Add new proxy**.
2. Enter the details of the new proxy (the table below describes the fields available).
3. Click **Add proxy**.

Field	Description	Usage tips
Name	A descriptive name for the proxy.	You can configure up to 50 proxies.
Address	The IP address of the proxy. Optionally you can specify a port number for the Cisco VCS, using standard *IP:port* address notation (for example, *x.x.x.x:y*).	If a port is specified, the Cisco TelePresence Advanced Media Gateway will use that port for signaling toward the Cisco VCS.

Editing a proxy

1. Go to **Proxies**.
2. Click the name of the proxy that you want to edit.
3. Edit the details of the proxy as required.
4. Click **Update proxy**.

Deleting a proxy

1. Go to **Proxies**.
2. Select the proxy or proxies that you want to delete.
3. Click **Delete selected proxies**.
4. Click **OK**.

Related topics

Displaying the proxy list

Users

This section describes how to manage user configuration data.

Displaying the user list

The **User list** page provides summary information about configured users on the Cisco TelePresence Advanced Media Gateway. To view the **User list** page, go to **Users**.

Field	Field description
User ID	The user name that the user needs to access the web interface of the Cisco TelePresence Advanced Media Gateway. Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters. For information about adding, deleting or changing users see Adding, updating and deleting users.
Name	The full name of the user.

Adding, updating and deleting users

To manage users on the Cisco TelePresence Advanced Media Gateway, log in as administrator and go to the **Users** page.

Adding a user

1. In the **Users** page, click **Add new user**.
2. Complete the relevant fields for the user (see table below).
3. Click **Add user**.

Deleting a user

1. In the **Users** page, select the appropriate user.
2. Click **Delete selected users**.
   You cannot delete the *admin* user.

Updating a user

1. In the **Users** page, select the appropriate user.
2. Complete the relevant fields for the user (see table below).
3. Click **Update user settings** to change the user's information settings or **Update password** to change the user's password.

Field	Field description	More information
User ID	Login name the user will use to access the Cisco TelePresence Advanced Media Gateway 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.
Password	Required password (if any).	Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.
Re-enter password	Verifies the required password.	

Logs

This section describes how to work with logs and Call Detail Records.

Working with the event logs

If you experience complex issues that require advanced troubleshooting, you may need to collect information from the Cisco TelePresence Advanced Media Gateway logs. Typically, you will be working with Cisco customer support who can help you obtain these logs.

Event log

The last 2000 status messages generated by the Cisco TelePresence Advanced Media Gateway are displayed in the **Event log** page (**Logs > Event log**). Usually these are information messages, although occasionally *Warnings* or *Errors* may appear 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 Cisco TelePresence Advanced Media Gateway, Cisco 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 Cisco 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.
- 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.

CAUTION: Do not modify these settings unless instructed to do so by Cisco customer support. Modifying these settings can impair the performance of the Cisco TelePresence Advanced Media Gateway.

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 Cisco 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 Cisco TelePresence Advanced Media Gateway 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).

SIP log

The SIP log page records every SIP message received or transmitted from the Cisco TelePresence Advanced Media Gateway. The log can be exported in an .xml file.

By default the SIP log is disabled because it affects performance, but Cisco customer support may ask you to enable it if there is a problem with an Cisco TelePresence Advanced Media Gateway in your network.

Working with the CDR log

The Cisco TelePresence Advanced Media Gateway can display up to 20 pages of Call Detail Records (CDRs). However, the Cisco TelePresence Advanced Media Gateway is not intended to provide long-term storage of CDRs and you must download and store them elsewhere.

Note: When the CDR log is full, the oldest logs are overwritten.

To work with the CDR log, go to **Logs > CDR log**.

About the CDR log list

The CDR log list shows some or all of the stored records, depending on the filtering and display settings. Click any column heading to sort by that field. The fields in the CDR log list are as follows:

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 connection events occur. The time the record was created is the time that the event occurred. Incoming CDR log requests 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.
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.

Customising the CDR log display

The CDR log can contain a lot of information. The controls in this section help you to select the most useful information for display. When you have finished making changes, click **Update display** to make those changes take effect. The available options are as follows:

Field	Field description	Usage tips

Current status	This field indicates whether CDR logging is enabled or disabled. Use (**Enable logging** and **Disable logging**) to change status. If you enable logging, the Cisco TelePresence Advanced Media Gateway writes the CDRs to the compact flash card. If you disable logging, CDRs are still generated but are not written to compact flash.	Enabling or disabling CDR logging has immediate effect. There is no need to click **Update display** after selecting one of these buttons. Ensure that a compact flash card is available.
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 *All* will show the greatest amount of detail for all messages, regardless of which other options are selected.

Downloading 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 greyed 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**.

Clearing the log

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 greyed 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.

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 **Maintenance > Logs > Syslog**.

This topic describes the following items:

- 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	A configurable value for the purposes of identifying events from the Cisco TelePresence Advanced Media Gateway on the Syslog host. Choose from the following options: *0 - kernel messages* *1 - user-level messages* *2 - mail system* *3 - system daemons* *4 - security/authorization messages (see Note 1)* *5 - messages generated internally by syslogd* *6 - line printer subsystem* *7 - network news subsystem* *8 - UUCP subsystem* *9 - clock daemon (see Note 2)* *10 - security/authorization messages (see Note 1)* *11 - FTP daemon* *12 - NTP subsystem* *13 - log audit (see Note 1)* *14 - log alert (see Note 1)* *15 - clock daemon (see Note 2)* *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)*	Choose a value that you will remember as being the Cisco TelePresence Advanced Media Gateway. Note the following points: ■ 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. ■ Also, various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages. 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). We recommend that you select these values.

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:

0 - Emergency: system is unusable (unused by the Cisco TelePresence Advanced Media Gateway)

1 - Alert: action must be taken immediately (unused by the Cisco TelePresence Advanced Media Gateway)

2 - Critical: critical conditions (unused by the Cisco TelePresence Advanced Media Gateway)

3 - Error: error conditions (used by Cisco TelePresence Advanced Media Gateway *error* events)

4 - Warning: warning conditions (used by Cisco TelePresence Advanced Media Gateway *warning* events)

5 - Notice: normal but significant condition (used by Cisco TelePresence Advanced Media Gateway *info* events)

6 - Informational: informational messages (used by Cisco TelePresence Advanced Media Gateway *trace* events)

7 - Debug: debug-level messages (used by Cisco TelePresence Advanced Media Gateway *detailed trace* events)