Cisco TelePresence Advanced Media Gateway Version 1.0

Online help (printable format)

D14731.02

November 2010

Contents

Logging in to the web interface

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

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

The **Login** page of the AM gateway displays a welcome banner which administrators can configure to display text relevant to your organization. For more information, refer to Customizing the user interface.

Failing to log into the web interface

Cisco TelePresence Advanced Media (AM) Gateway web interface, you must log in so that the AM gateway can associate the session with your configured user and a set of access privileges. The AM gateway has a set of configured users, and each user has an ID and password that are used for logging in.

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

- **Invalid username/password**: you have typed the incorrect username and/or password.

  If Advanced account security mode is enabled and you incorrectly type the username and/or password three times and if this is an admin account, it is disabled for 30 minutes; for any other account, it is disabled indefinitely (or until you, the administrator, re-enable the account from the **User** page)
- **No free sessions**: the maximum number of sessions allowed simultaneously on the AM 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
- **You do not have access rights to view this page**: you do not have the access rights necessary to view the page that you attempted to see
- **Page expired**: the **Change password** page can expire if the AM 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.)

Displaying the system status

The **System status** (**Status**) page displays an overview of the AM gateway status.

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

Field	Field description	Usage tips
System status		
Model	Specific AM gateway model.	
Serial number	Unique serial number of the AM 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 AM gateway.	
Host name	Host name assigned to the AM gateway.	
IP address	IP address assigned to the AM gateway.	
CPU load	Current processor utilization of the AM gateway.	
Media processing load	Overview of the current media loading of the AM gateway.	
Call status		
Active calls	Number of calls currently active on the AM gateway.	
Completed calls	Number of successful calls handled by the AM gateway since it was last restarted.	
Total incoming video bandwidth	The total video data rate being received by the AM 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 AM gateway, Ciosco customer support may ask you for this diagnostic file to help with troubleshooting.	To retrieve a troubleshooting support file, click **Download file**.

Displaying hardware health status

The **Health status** page (**Status > Health**) displays information about the hardware components of the AM gateway.

Note: The **Worst status seen** conditions are those since the last time the AM gateway was restarted.

To reset these values, click **Clear**. Refer to the table below for assistance in interpreting the information displayed.

Field	Field description	Usage tips
Fans **Voltages** **RTC battery**	Displays two possible states: • 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 three 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 AM 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 AM 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 connectivity testing

The Network connectivity page can be used for troubleshooting issues that arise because of problems in the network between the AM gateway and a remote video conferencing device being called (or a device from which a user is attempting to call the AM gateway).

The Network connectivity page enables you to attempt to 'ping' another device from the AM gateway's web interface and perform a 'traceroute' of the network path to that device. The results show whether or not you have network connectivity between the AM gateway and another device. You can see from which port the AM gateway will route to that address. For a hostname, the IP address to which it has been resolved will be displayed.

To test connectivity with a remote device, go to **Network > Connectivity**. In the text box, enter the IP address or hostname of the device to which you want to test connectivity and click **Test connectivity**.

For each successful 'ping', the time taken for the ICMP echo packet to reach the host and for the reply packet to return to the AM gateway is displayed in milliseconds (the round trip time). The TTL (Time To Live) value on the echo reply is also displayed.

For each intermediate host (typically routers) on the route between the AM gateway and the remote device, the host's IP address and the time taken to receive a response from that host is shown. Not all devices will respond to the messages sent by the AM gateway to analyse the route; routing entries for non-responding devices is shown as <unknown>. Some devices are known to send invalid ICMP response packets (e.g. with invalid ICMP checksums); these responses are not recognized by the AM gateway and therefore these hosts' entries are also shown as <unknown>.

Note: The ping message is sent from the AM gateway to the IP address of the endpoint that you enter. Therefore, if the AM gateway has an IP route to the given IP address, regardless of whether that route lies out of port A or port B, the ping will be successful. This feature allows the AM gateway’s IP routing configuration to be tested, and it has no security implications. If you are unable to ping the device then check your network configuration especially any firewalls using NAT.

Displaying the user list

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

Field	Field description
User ID	The user name that the user needs to access the web interface of the AM gateway. Although you can enter text in whichever character set you require, note that some browsers and FTP clients do not support Unicode characters.
Name	The full name of the user.

Deleting users

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

Adding a new user

To add a new user, click **Add new user**. See Adding and updating users for more information.

Adding and updating users

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

The AM gateway has admin level users only. It is not possible to set any other privilege level.

Adding a user

To add a user:

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

Updating a user

To update an existing user:

1. Go to the **Users** page.
2. Click a user name.
3. Edit the fields as required referring to the table below to determine the most appropriate settings for the user.
4. After entering the settings, click **Update user settings**.

Field	Field description	More information
User ID	Identifies the log-in name that the user will use to access the AM 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.
Name	The full name of the user.	
Password	The 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. Note that this field is only active when adding a new user. If you are updating an existing user and want to change that user's password, click **Change password** instead.
Re-enter password	Verifies the required password.	

Configuring network settings

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

The AM 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 AM gateway. Therefore, although there is a **Network > Port B settings** page, you cannot change any settings for Port B.

In this section:

- IP configuration settings
- IP status
- Ethernet configuration
- Ethernet status

IP configuration settings

These settings determine the IP configuration for the appropriate Ethernet port of the AM gateway. When you have finished, click **Update IP configuration** and then reboot the AM gateway.

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 AM gateway obtains its own IP address for this port automatically via DHCP (Dynamic Host Configuration Protocol). If set to *Manual* the AM gateway will use the values that you specify in the Manual configuration fields below.	Click **Renew DHCP** 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 AM gateway.
Manual configuration		
IP address	The dot-separated IPv4 address for this port, for example 192.168.4.45.	You only need to specify this option if you have chosen *Manual* IP configuration, as described above. For Port A, if the IP configuration setting is set to *Automatic by DHCP* this setting will be ignored.
Subnet mask	The subnet mask required for the IP address you wish to use, for example 255.255.255.0	
Default gateway	The IP address of the default gateway on this subnet, for example 192.168.4.1	
DNS configuration		
Host name	Specifies a name for the AM gateway.	Depending on your network configuration, you may be able to use this host name to communicate with the AM gateway, without needing to know its IP address.
Name server	The IP address of the name server.	

Field	Field description	Usage tips
Secondary name server	Identifies an optional second name server.	The secondary DNS server is only used if the first is unavailable. If the first returns that it does not know an address, the secondary DNS server will not be queried.
Domain name (DNS suffix)	Specifies an optional suffix to add when performing DNS lookups.	This can allow you to use non-fully qualified host names when referring to a device by host name instead of IP address. For example, if the domain name is set to *cisco.com*, then a request to the name server to look up the IP address of host *endpoint* will actually lookup *endpoint.cisco.com*.

IP status

Use the IP status fields to verify the current IP settings for the appropriate Ethernet port of the AM gateway, which were obtained using DHCP or configured manually (see IP configuration settings) including:

- Host name
- DHCP
- IP address
- Subnet mask
- Default gateway
- Name server
- Secondary name server
- Domain name (DNS suffix)

Ethernet configuration

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

Field	Field description	Usage tips
Ethernet settings	Specify whether you want this Ethernet port to automatically negotiate its Ethernet settings with the device it is connected to, or if it should use the values that you specify in the Manual configuration fields below.	It is important that your Ethernet settings match those of the device to which this port is connected. For example, both devices must be configured to use automatic negotiation, or both configured with fixed and matching speed and duplex settings (see below).
Manual configuration		
Speed	Identifies the connection speed: *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. You only need to select this option if you have chosen *Manual* Ethernet settings, as described above.
Duplex	Identifies the connection duplex mode: ► *Full duplex* Both devices can send data to each other	The duplex setting must match that of the device to which this port is connected. You only need to select this option if you have

Field	Field description	Usage tips
	at the same time ▶ *Half duplex* Only one device can send to the other at a time	chosen *Manual* Ethernet settings, as described above.

Ethernet status

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

Configuring IP routes settings

You need to set up one or more routing settings to control how IP traffic flows in and out of the AM gateway.

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

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

In this section:

- Port preferences
- IP routes configuration
- Current IP status

Port preferences

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

Field	Field description	Usage tips
Default gateway preference	The IP address to which the AM gateway will send packets in the absence of more specific routing (see IP routes configuration).	You may only select Port A.
Name server (DNS) preference	The IP address to which the AM gateway will send requests to look up unrecognized host names in order to determine their corresponding IP addresses.	You may only select Port A.

IP routes configuration

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

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

Adding a new IP route

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

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

Viewing and deleting existing IP routes

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

- The IP address pattern and mask
- Where matching packets will be routed, with the possibilities being:
- Port A - meaning the default gateway configured for Port A
- <IP address> - a specific address has been chosen
- Whether the route has been configured automatically as a consequence of other settings, or added by the user as described above.

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

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

Current IP status

This table shows the current default gateway and name server(s) for Ethernet Ports A and B. No fields can be changed, and are provided for reference when configuring the other parameters described in the sections above.

Configuring IP services

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

Use this page to control the type of services that may be accessed via Ethernet Ports A and B. Refer to the table below for more details.

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

Field	Field description	Usage tips
TCP service		
Web	Enable/disable web access on the appropriate port.	Web access is required to view and change the AM 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 appropriate port.	This field is only visible if the AM gateway has the *Secure management (HTTPS)* feature key or an *Encryption* feature key installed. For more information about installing feature keys, refer to Upgrading and backing up the AM gateway. By default, the AM gateway has its own SSL certificate and private key. However, you can upload a new private key and certificates if required. For more information about SSL certificates, refer to Configuring SSL certificates. If a port is disabled, this option will be unavailable.
Incoming SIP (TCP)	Allow/reject incoming calls to the AM 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 AM gateway. If a port is disabled, this option will be unavailable.
Incoming Encrypted SIP (TLS)	Allow/reject incoming encrypted SIP calls to the AM 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 AM gateway. If a port is disabled, this option will be unavailable.

Field	Field description	Usage tips
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 AM gateway configuration. **Note:** FTP is only used for configuration file changes not for Microsoft Office Communicator file transfers. You should consider disabling FTP access on any port that is outside your organization's firewall. If a port is disabled, this option will be unavailable.
UDP service		
SNMP	Enable/disable the receiving of the 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. You must use the same port number for both Port A and Port B. The number is automatically refreshed for Port B. Note that by default SNMP Traps are sent to port UDP port 162 (on the destination network management station); this is configurable. For more information, refer to Configuring SNMP settings. If you require advanced security for the AM gateway, disable the SNMP service.
SIP (UDP)	Allow/reject incoming and outgoing calls to the AM 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. You must use the same port number for both Port A and Port B. The number is automatically refreshed for Port B.

Configuring system settings

The **System settings** page allows you to configure the following settings:

- Call settings
- User interface settings

Click **Apply changes** after making any changes to the settings.

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 AM gateway will try and use a high frame rate. That is, the AM gateway will strongly favor a resolution of at least 25 frames per second • *Favor sharpness*: The AM gateway will use the highest resolution that is appropriate for what is being viewed • *Balanced*: The AM 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 AM gateway. This setting controls how the AM gateway will negotiate 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 AM gateway to a single participant.	When the AM gateway makes a call to a participant, the AM gateway chooses the maximum bandwidth that is allowed to be used for the media channels which comprise that call. This field sets that maximum bandwidth, and is the total bandwidth of the audio, video, and content channels combined.
Default bandwidth to AM gateway	Sets the bandwidth that the AM gateway will advertise to the participant when it calls it.	
Convert out-of-band to in-band DTMF	Select this option to have the AM 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 AM gateway to a traditional call center with an automated audio menu, you will need to be using in-band DTMF tones to select an option, so this option may be required. Note that IP phones can interpret in-band DTMF and will continue to work as expected with this option enabled.
Overlay participant name	This setting 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 AM 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).

Field	Field description	Usage tips
Welcome message duration	This setting 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 AM gateway will upscale video streams from participants who are sending low resolution video with the purpose of making best use of the AM gateway's HD video capabilities.	The AM 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 AM gateway is running in Standard definition mode. Go to **Settings > Resource settings** to configure this.
Flow control on video errors	Enables the AM gateway to request that the endpoint send lower speed video if it fails to receive all the packets which comprise the far end's video stream.	The AM gateway can send these messages to endpoints requesting that the bandwidth of the video that they are sending be decreased based on the quality of video received by the AM gateway. If there is a bandwidth limitation in the path between the endpoint and the AM gateway, it is better for the AM gateway to receive every packet of a lower rate stream than to miss some packets of a higher rate stream.
Video transmit size optimization	Allows the AM 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 AM 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 AM gateway video transmission Typically, lowering the resolution means that the AM gateway can transmit video at a higher frame-rate.

Field	Field description	Usage tips
Video resolution selection mode	This setting can be used to influence the choice of outgoing video resolution made by the AM gateway. • *Default*: The AM 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 AM 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 AM gateway for outgoing video streams (from the AM 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 AM 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 AM 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 AM gateway's choice of audio codecs to be used for transmitting audio to participants.	When communicating with a participant, the AM gateway receives a list of supported audio codecs from the participant. The AM 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 AM gateway advertises to remote participants, restricting the participants' choice of channels available for sending audio data to the AM gateway. Some endpoints and network equipment do not support as many codecs as the AM gateway can offer. For best interoperation it is recommended that at least one audio codec is left unselected in the **Audio codecs to AM gateway** section.	
Video codecs from AM gateway	Restricts the AM gateway's choice of video codecs to be used for transmitting video to participants.	When communicating with a participant, the AM gateway receives a list of supported video codecs from the participant. The AM 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 AM gateway advertises to remote participants, restricting the participants' choice of channels available for sending video data to the AM gateway.	

Field	Field description	Usage tips
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. Note that thumbnail images will not be shown for conferences where encryption is required.	
Security settings		
Redirect HTTP requests to HTTPS	Enable this option to have HTTP requests to the AM 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.

Configuring resource settings

The **Resource settings** page allows you to configure the video capacity of the AM gateway.

Click **Apply changes** after making any changes to the settings. A message is displayed telling you that you need to shut down and restart the unit for these changes to take effect. Click **OK**. You are directed to the Shutdown page to shut down and restart the AM gateway to apply the changes.

Field	Field description	Usage tips
Call capability	The AM 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 AM gateway for any changes to this setting to take effect.
Call capacity	The number of calls supported in the selected mode is shown. This depends on the model of AM gateway you are using.	

Displaying and resetting system time

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

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

System time

The current system date and time is displayed.

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

NTP

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

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

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

If the NTP server is local to Port A or Port B then the AM gateway will automatically use the appropriate port to communicate with the NTP server. If the NTP server is not local, the AM 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. To configure the default gateway or an IP route, go to **Network > Routes**.

Field	Field description	Usage tips
Enable NTP	If selected, use of the NTP protocol is Enabled on the AM gateway.	
UTC offset	The offset of the time zone that you are in from Greenwich Mean Time.	You must update the offset manually when the clocks go backwards or forwards: the AM gateway does not adjust for daylight saving automatically.
NTP host	The IP address or hostname of the server that is acting as the time keeper for the network.	

Using NTP over NAT (Network Address Translation)

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

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

Configuring SNMP settings

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

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

Note that:

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

System information

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

Configured trap receivers

Field	Field description	Usage tips
Enable traps	Select this check box to enable the AM 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.	You cannot select this check box unless you have selected to **Enable traps** above. Authentication failure traps are generated and sent to the trap receivers when someone tries to read or write a MIB value with an incorrect community string.

Field	Field description	Usage tips
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 AM 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.	Note that SNMP community strings are not secure. They are sent in plain text across the network. It is advisable to change the community strings before enabling SNMP as the defaults are well known.
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 AM 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. All other packets are sent with a QoS of 0.

The AM gateway allows you to set six bits 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 six 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

In this section:

About QoS configuration settings

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

Click **Update QoS settings** after making 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 AM 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 AM 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 AM 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 the default settings, click **Reset to default**.

Displaying the proxy list

The **Proxies** page displays a list of the proxies configured for your AM gateway. The proxies list controls which VCSs the AM gateway can accept calls from. Each AM gateway must be configured as a neighbor on a VCS and the VCS must be listed as a proxy in the proxies list. Calls received by the AM gateway from an IP address not on the proxies list are rejected.

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.

To add a new proxy:

1. Click Add new proxy.
2. See Adding and editing proxies.

To delete a proxy:

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

Adding and editing proxies

You can add a new proxy for the AM gateway or edit the details of an existing proxy.

To add a new proxy:

1. Go to **Proxies** > **Add new proxy**.
2. Enter the details of the new proxy referring to the table below.
3. Click **Add proxy**.

You can also add a new proxy by clicking **Add proxy** from the **Proxies** page.

To edit an existing proxy:

1. Go to **Proxies**.
2. Click the name of the proxy you want to edit.
3. Edit the proxy's details referring to the table below.
4. Click **Update proxy**.

Field	Description	Usage tips
Name	A descriptive name to be given to the proxy.	You can configure up to 50 proxies.
Address	The IP address of the proxy.	
Outgoing transport	The protocol to be used for call control messages for outging call connections.	Select either *UDP*, *TCP*, or *TLS*. This must match the protocol configured on the VCS that the AM gateway is neighbored with.

Displaying the active calls list

The **Calls** page displays all the calls that are currently active on the AM gateway. You can disconnect an active call from the **Calls** page.

Click on **Details** next to a call to go to the **Call details** page for that call. See Displaying the call details for further information.

The table below explains the information on 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.
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 further information.
Start time	The time that the call was initiated.	Click on **Start time** to toggle the order of the calls in the list. See Displaying the call details for further information.
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

The **Call details** page (**Calls** then click the time stamp in the **Time** column of the call you want to display the details of) allows you to inspect detailed information about active calls.

The table below explains the content of the **Call details** page.

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.	Click your browser's refresh button to update this field.
Controls	A button that allows you to disconnect the call if necessary.	Click  to disconnect the call.
Source		
Name	The alias of the participant that initiated the call.	
IP	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.	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.

Upgrading and backing up the AM gateway

On this page:

Upgrading the main AM gateway software image

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

To upgrade the main AM gateway 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 onto the 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 AM gateway web browser interface.
7. Click **Browse** to locate the unzipped file on your hard drive.
8. Click **Upload software image**. The browser begins uploading the file to the AM gateway, and a new browser window opens to indicate the progress of the upload. When finished, the browser window refreshes and indicates that the "Main image upgrade completed."
9. The upgrade status displays in the **AM gateway software upgrade status** field.
10. Shutting down and restarting the AM 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 AM 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. Shutting down and restarting the AM 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 a AM gateway you can control which parts of the configuration are overwritten:

- If you select the **Network settings** box, the network configuration will be overwritten with the network settings in the supplied file. Typically, you would only select this check box if you were restoring from a file backed up from the same AM gateway or if you were intending to replace an out of service AM gateway. If you copy the network settings from a different, active, AM gateway and there is a clash (for instance, both are now configured to use the same fixed IP address) one or both boxes may become unreachable via IP.
- If you 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.

Note that you can also back up and restore the configuration of the AM gateway using FTP. For more information, refer to Backing up and restoring the configuration using FTP.

Enabling AM gateway features

The AM gateway requires activation before most of its features can be used. (If the AM 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 AM gateway you should receive the AM gateway already activated; if it is not, you have upgraded to a newer firmware version, or you are enabling a new feature, you may need to contact your supplier to obtain an appropriate activation code. Activation codes are unique to a particular AM gateway so ensure you know the unit's serial number such that you may receive a code appropriate to your AM gateway.

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

To activate the AM gateway or enable an advanced feature:

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

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

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

Shutting down and restarting the AM gateway

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

Shutting down the AM gateway will disconnect all active calls.

To shut down the AM gateway:

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

Configuring SSL certificates

If the AM 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 AM gateway using HTTPS. The AM gateway has a local certificate and private key pre-installed and this will be used by default when you access the unit using HTTPS. However, we recommend that you upload your own certificate and private key to ensure security as all AM gateways have identical default certificates and keys.

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 AM gateway.

If you have uploaded your own certificate and key, you can remove it later if necessary; to do this, click **Delete custom certificate and key**.

The table below 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	The 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 AM gateway. The private key is used by the AM gateway to decrypt that data. If the **Private key** field shows 'Key matches certificate' then the data is securely encrypted in both directions.

Field	Field description	Usage tips
Local certificate configuration		
Certificate	If your organization has bought a certificate, or you have your own way of generating certificates, you can upload it. Browse to find the certificate file.	
Private key	Browse to find 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 AM gateway.	
Trust store		
Subject	The details of the business to which the trust store 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	The details of the issuer of the trust store certificate.	Where the certificate has been self-issued, these details will be the same as for the **Subject**.
Issued	The date on which the trust store certificate was issued.	
Expires	The date on which the trust store certificate will expire.	
Certificate verification settings	Choose to what extent the AM gateway will verify the identity of the far end for a connection: • *No verification*: all outgoing connections are permitted to proceed, even if the far end does not present a valid and trusted certificate. • *Outgoing connections only*: outgoing connections are only permitted if the far end has a certificate which is trusted. • *Outgoing connections and incoming calls*: outgoing connections and incoming connections for SIP calls using TLS must have a certificate which is trusted otherwise the AM gateway will not allow the connection to proceed.	Outgoing connections are connections such as SIP calls which use TLS.

Displaying participant statistics

The **Participant statistics** page (**Calls**, then click a source or destination alias) displays statistics about the video and audio streams between individual callers (participants) and the AM gateway.

The **Participant statistics** page is divided into the following sections:

- 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 AM 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 AM 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 AM 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.

Field	Field description	Usage tips
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 AM 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 AM gateway.
Packets sent	A count of the number of packets that have been sent from the AM 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 AM 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 AM 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 AM 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 AM gateway is sending RTCP packets about this stream.	
Receiver reports	A count of the number of "receiver report" type RTCP packets seen by the AM 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 AM gateway.
Sender reports	A count of the number of "sender report" type RTCP packets received by the AM 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 AM gateway to the participant.	
VIDEO **Received video**		
Receive stream	The codec in use and the size of the picture that the AM 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.	

Field	Field description	Usage tips
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 AM 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 AM gateway. It may send less data than this (if it does not need to use the full channel bit rate or the AM gateway has requested a lower rate), but it should not send more.
Receive bit rate	The bit rate (in bits per second) that the AM 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 AM gateway.	
Packets received	The number of video packets destined for the AM 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 AM gateway to the participant.	
Transmit address	The IP address and port of the device to which the AM 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 AM gateway.
Channel bit rate	The negotiated available bandwidth for the AM gateway to send video to the participant in.	
Transmit bit rate	The bit rate the AM 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 AM 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 AM 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 AM gateway prioritizes sending quality video at the expense of a lower frame rate. A larger number implies that the AM gateway is prepared to send lower quality video at a higher frame rate.

Field	Field description	Usage tips
Received video 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 AM 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 AM 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 AM gateway.	These are typically sent by any device that is sending RTP media.
Estimated bandwidth	The bandwidth that the Microsoft Office Communicator (MOC) client estimates is available for receiving calls from the AM gateway.	
Packet loss notifications	The number of packets the AM 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 MOC to the AM 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 AM gateway that are neither sender nor receiver reports.	
Transmitted video RTCP		
RTCP transmit address	The IP address and port to which the AM gateway is sending RTCP packets about this stream.	
Receiver reports	A count of the number of "receiver report" type RTCP packets seen by the AM 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 AM gateway.
Sender reports	A count of the number of "sender report" type RTCP packets sent by the AM gateway.	These are typically sent by any device that is sending RTP media.
Estimated bandwidth	The bandwidth that the Microsoft Office Communicator (MOC) client estimates is available for transmitting calls to the AM gateway.	
Packet loss notifications	The number of packets the MOC 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 AM gateway to the MOC indicate the preferred video resolution for the call.	

Field	Field description	Usage tips
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.	

Displaying participant diagnostics

The **Participant diagnostics** page (**Calls**, click a source or destination alias, then click **Diagnostics**) displays diagnostic information about the selected call participant's connection to the AM gateway. You are not likely to need to use any of the information on this page except when troubleshooting specific issues under the guidance of Cisco customer support.

Working with the event logs

If you are experiencing complex issues that require advanced troubleshooting, you may need to collect information from the AM 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 AM gateway are displayed in the **Event log** page (**Maintenance > Logs > Event log)**. In general these messages are provided for information, and occasionally *Warnings* or *Errors* may be shown in the Event log. The presence of such messages is not cause for concern necessarily; if you are experiencing a specific problem with the operation or performance of the AM 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. For more information, refer to Logging using syslog
- Empty the log by clicking **Clear log**.

Event capture filter

The Event capture filter allows you to change the level of detail to collect in the Event log traces.

Note: You should not modify these settings unless instructed to do so by Cisco customer support. Modifying these settings can impair the performance of your AM 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 AM 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 AM 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 a unit in your network.

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**.

In this section:

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 AM 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 AM gateway. **Note:** Various operating system daemons and processes have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar. 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) - and these are the values that we recommend you select.

Using syslog

The events that are forwarded to the syslog receiver hosts are controlled by the event log capture filter.

To define a syslog server, simply enter its IP address and then click **Update syslog settings**. The number of packets sent to each configured host is displayed next to its IP address.

Note: Each event will have a severity indicator as follows:

- 0 – Emergency: system is unusable (unused by the AM gateway)
- 1 – Alert: action must be taken immediately (unused by the AM gateway)
- 2 – Critical: critical conditions (unused by the AM gateway)
- 3 – Error: error conditions (used by AM gateway *error* events)
- 4 – Warning: warning conditions (used by AM gateway *warning* events)
- 5 – Notice: normal but significant condition (used by AM gateway *info* events)
- 6 – Informational: informational messages (used by AM gateway *trace* events)
- 7 – Debug: debug-level messages (used by AM gateway *detailed trace* events)

Working with Call Detail Records

The AM gateway can display up to 20 pages of Call Detail Records. However, the AM gateway is not intended to provide long-term storage of Call Detail Records. You must download the Call Detail Records and store them elsewhere.

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

To view and control the CDR log, go to **Maintenance > Logs > CDR log**. Refer to the tables below for details of the options available and a description of the information displayed.

Call Detail Record log controls

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

Field	Field description	Usage tips
Current status	This field indicates whether CDR logging is enabled or disabled. Use the two buttons (**Enable logging** and **Disable logging**) to change status.	Enabling or disabling CDR logging has immediate effect. There is no need to press **Update display** after selecting one of these buttons.
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.

Call Detail Record log

This table shows the logged Call Detail Records, subject to any filtering applied (see Call Detail Record log controls, above). The fields displayed and the list's associated controls are described below:

Downloading and clearing the log

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 maxmium of 20 pages. If the log includes more events than can be displayed on those pages, the more recent events are displayed. Therefore you may see **Download X to Y as XML** where X keeps increasing when the page is refreshed. Again you can download the full log with **Download as XML**.

To clear the CDR log, click **Delete X to Y**. This will permanently remove Call Detail Records X to Y. Due to the way the CDR log works, it may not be possible to delete all records; the button name indicates which records can be deleted. For example, if you delete the 0-399 entries, then the 400th entry appears as the first entry in this page, even if you download the full log. The download button would then show that you can download for example 400-674 (if 674 is the maximum number of entries in the log) and the delete button will be 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.

CDR log display

The CDR log list shows some or all of the stored records, depending on the filtering and display settings (see Call Detail Record log controls). Click on a column heading to sort by that field. Refer to the table below to understand the fields displayed in the CDR log list:

Field	Field description	Usage tips
# (record number)	The unique index number for this Call Detail Record.	
Time	The time at which the Call Detail Record was created.	
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.

Further information about CDR time field

The CDR log time stamp is stored in UTC time and not local time like the Event log, but converted to local time when displayed in the CDR log.

Changing the time and NTP's UTC Offset (on the **Settings > Time** page) will affect the CDR log time in the following ways:

- Changing the time, either changing the system time or via an NTP update will cause new CDR logs to show the new time but no change will be made to existing logged CDR events.
- With NTP enabled, setting a UTC offset will change the displayed time for all the CDR events; the stored time will remain the same because it is stored in UTC and the offset is applied for display purposes.
- Enabling or disabling NTP when an offset is configured will cause the display time to change for all existing events and the UTC time will change for logging future CDR events. This is because, when NTP is disabled, the current time is treated as UTC with an offset of 0.

Backing up and restoring the configuration using FTP

You can back up and restore the configuration of the AM gateway through its web interface. To do so, go to **Settings > Upgrade**. For more information, refer to Upgrading and backing up the AM gateway.

You can also save the configuration of the AM 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 AM 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 AM gateway's web interface as an administrator.
   You will see a file called configuration.xml. This contains the complete configuration of your AM 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 AM gateway using an FTP client. When asked for a user name and password, use the same ones that use to log in to the AM gateway's web interface as an administrator.
4. Upload your configuration.xml file to the AM gateway, overwriting the existing file on the AM gateway's.

The restore process is now complete.

Note: that the same process can be used to transfer a configuration from one AM gateway unit to another. However, before doing this, be sure to keep a copy of the original feature keys from the unit whose configuration is being replaced.

If you are using the configuration file to configure a duplicate unit, for example in a network where you have more than one AM gateway, be aware that if the original unit was configured with a static address, you will need to reconfigure the IP address on any other units on which you have used the configuration file.