Cisco TelePresence IP Gateway Version 2.0

Online Help (Printable Format)

D14804.02

November 2012

Contents

Introduction

This document contains the text of the online help for the Cisco TelePresence IP Gateway Version 2.0 web user interface. It is provided so that the help text can be viewed or printed as a single document.

Logging into the web interface

The Cisco TelePresence IP Gateway web interface is used to administer the Cisco TelePresence IP GW 3500 Series and IP GW MSE 8350.

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

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

The main menu appears, offering options based on your access privileges.

Failing to log into the web interface

When connecting to the Cisco TelePresence IP Gateway web interface, you must log in so that the gateway can associate the session with your configured user and a set of access privileges. The IP 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.
- **No free sessions**: the maximum number of sessions allowed simultaneously on the IP 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 IP 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.)

Getting started with the Cisco TelePresence IP Gateway

Ensure you have correctly completed the physical setup of the Cisco TelePresence IP Gateway following the instructions contained in the Getting Started Guide that accompanied the unit.

Note: We recommend that you change the admin account to use a password as soon as possible. To do that, go to **Users**, click the admin link, and provide the required user information.

Step one: Configure Ethernet Port B settings

The default setting for the IP GW Ethernet ports is auto-sensing mode. If the switch ports to which you connect the IP GW are not also set to auto-sensing mode, then you need to configure the IP GW Ethernet ports to use the same speed and duplex mode. Both ends of the Ethernet connection must be configured in the same way. For example, either configure both ends of the link to be auto-sensing or configure both ends to operate at the same speed and duplex.

During your initial configuration of the IP gateway following the instructions in the Getting Started Guide, you will have configured Port A using the command line interface.

Note: To establish a 1000Mbps connection, both ends of the link must be configured as auto-sensing

1. To configure Ethernet Port B, go to **Network > Port B**.
2. Enter the IP address, subnet mask, and default gateway for the port.
3. Click **Update IP configuration**.

Step two: Configure an H.323 gatekeeper and/or SIP registrar (optional)

If you have H.323 endpoints, using an H.323 gatekeeper can make it easier for callers to make their call. You can configure the IP gateway to use an external gatekeeper or its own built-in gatekeeper.

If you have SIP endpoints, using a SIP registrar can make it easier for callers to make their call.

- To configure the use of an H.323 gatekeeper, go to **Settings > H.323**
- To configure the use of a SIP registrar, go to **Settings > SIP**

For more information refer to Configuring gatekeeper settings and Configuring SIP settings.

The built-in gatekeeper can be used to bridge between two networks allowing endpoints connected to each port to use the same gatekeeper. This enables callers on the same port to call each other without the call being routed through the IP gateway, whilst calls from one port to the other are routed transparently through the IP gateway. For more information, refer to Using the built-in gatekeeper to bridge between two networks

Step three: Configure the auto attendant menus

Depending on the configuration of your dial plan, and the settings for failed calls, callers can be connected to the auto attendant. You can configure the auto attendant to allow callers to:

- dial E.164 numbers
- be connected to the operator
- dial IP addresses
- choose an address book
- select an endpoint to which to connect
- select a call group to which to connect
- choose a video to watch
- view a video you have chosen to automatically play
- hear an audio prompt that you have recorded

By default, the IP gateway creates an individually-configurable auto attendant for each port.

When you configure endpoints and call groups you can choose whether those endpoints and call groups will appear as options in either auto attendant.

- To configure auto attendant menus, go to **Menus >Menu builder**

When you configure endpoints and call groups you can choose whether those endpoints and call groups will appear in an internal address book that can be displayed by the auto attendant.

For more information, refer to Configuring auto attendant menus, Configuring failed call settings, Understanding the dial plan, Configuring call groups, and Configuring endpoints.

Step four: Configure an operator (optional)

An operator is a person who can put calls through on the IP gateway. You can use the dial plan to automatically connect calls to an operator, you can allow callers to directly dial an operator, and you can have an operator as an option on the auto attendant. An operator connects the calls one by one as calls reach the top of the operator's call queue. An operator can put calls through to configured endpoints and call groups that have been given names in the system, or to any other endpoint by manually entering the IP address or E.164 number of the endpoint.

- To configure an operator, go to **Settings > Users**

For more information, refer to: Understanding operator features and Configuring operator settings.

Step five: Add endpoints (optional)

You can configure endpoints to work with the IP GW. For configured endpoints, the operator can simply choose the endpoint's name from a list, rather than having to type in the endpoint's address when a caller wants to be connected to that endpoint.

When you configure an endpoint, you can select whether or not that endpoint will appear in the internal address book, thereby enabling a caller to connect to that endpoint, without the caller having to know its address.

- To configure endpoints, go to **Endpoints**

For more information, refer to: Configuring endpoints.

Step six: Configure failed call settings

Calls can fail for a number of different reasons. For each failure type, you can configure the IP gateway to act in one of three ways. You configure the failed-call action by port; that is, you can configure different actions for each port.

- To configure failed call settings, go to **Dial plan > Failed calls**

For more information refer to Configuring failed call settings.

Step seven: Configure the dial plan

The default behavior of the IP gateway is to reject all calls. You must configure a dial plan to allow permitted calls to be placed. There are a number of different ways in which you can use the dial plan. For example, you can configure a particular prefix that will forward calls to the operator and another to connect callers to the auto attendant.

- To configure the dial plan, go to **Dial plan**

For more information, refer to the topics: Understanding the dial plan, Adding and updating dial plan rules, Example dial plan rules, Dial plan syntax, and Displaying and testing the dial plan.

Step eight: Train the operator and instruct callers how to make calls through the IP gateway

If you have an operator, you must provide them with some training in how to answer and connect calls; in the case of an operator who has not used a video phone before, it might also be a good idea to provide some guidance for that. For more information, refer to Using the IP gateway – for operators.

End users will need to know how to make calls through the Cisco TelePresence IP Gateway. For example, are you going to provide a quick-dial option for contacting the operator? Are you going to allow callers to dial IP addresses? For more information, refer to Dialing the IP gateway — for end-users.

Configuring global call settings

To modify the global call settings for the Cisco TelePresence IP Gateway go to **Settings > Calls**.

In this section:

Call settings

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

Field	Field description	Usage tips
Maximum video size	Identifies the greatest video size that the IP gateway will send and receive when connected to a video endpoint.	Note that this setting only applies when the IP gateway is processing the media (that is, the call is transcoded). In a non-transcoded call, the size of the video is determined by the endpoints. For more information about non-transcoded mode, refer to the information for the *Allow non-transcoded calls* setting, below.
Motion / sharpness trade off	Choose the unit-wide setting for motion/sharpness trade off. The options are: • **Favor motion**: the IP gateway will try and use a high frame rate. That is, the IP gateway will strongly favor a resolution of at least 25 frames per second • **Favor sharpness**: the IP gateway will use the highest resolution that is appropriate for what is being viewed • **Balanced**: the IP 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 endpoint and the IP gateway. This setting controls how the IP gateway will negotiate the settings to be used with an endpoint.
Default bandwidth from IP gateway	Identifies the network capacity (measured in bits per second) used by the media channels established by the IP gateway to a single caller.	When the IP gateway makes a call to an endpoint, the IP 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 channel and video channel combined. Before setting the value for the default bandwidth to and from the IP gateway, consider the amount of bandwidth available on your network. As a general rule, you

Field	Field description	Usage tips
		should set the default bandwidth to be less than the available bandwidth. Where you have connected the IP gateway to the internet via an ADSL connection, we recommend that you set the default bandwidth from the IP gateway to half of your upstream ADSL bandwidth (that is the connection from your network to your Internet Service Provider). Bear in mind that this setting affects traffic on both ports of the IP gateway.
Default bandwidth to IP gateway	Sets the bandwidth that the IP gateway will advertise to the endpoint when it calls it.	<*same as transmit*> will set the default bandwidth to the IP gateway to the same value as the default bandwidth *from* the IP gateway. Under most circumstances, <*same as transmit*> is the appropriate setting. However, in the case of an ADSL connection, you can set the default bandwidth to the IP gateway to be higher than the default bandwidth from the IP gateway; but bear in mind that this setting affects traffic on both ports of the IP gateway.
Dial-out timeout	Sets the length of time for which the IP gateway will attempt to make a connection to an endpoint. After this time has elapsed and if there is no response from the endpoint, the IP gateway will stop attempting to connect and will proceed to the failed call action.	The default setting is 30 seconds. The failed call action is dependant on how the call was placed. For more information, refer to Configuring failed call settings. Note that if you set it to 0, it will never stop attempting to connect to an endpoint that is not responding.
Allow non-transcoded calls	Selecting this option allows non-transcoded calls on the IP gateway. If you want to allow high definition (HD) calls to take place (or any calls of above 4CIF resolution) through the IP gateway, you must select this option.	This option is only available if you have the High Definition (HD) video feature key installed. For more information about installing feature keys, refer to Upgrading the firmware. When you enable non-transcoded calls, the IP gateway will prefer to use non-transcoded mode for any call where that is possible. For example, for H.323 to H.323 calls where the endpoints have common codecs and resolutions available, non-transcoded mode will be used. This is likely to be the case for most H.323 to H.323 calls.

Field	Field description	Usage tips
Encryption status	If you have the encryption feature key installed, you can configure the IP gateway to encrypt calls and to accept encrypted calls. Choose from: • **Optional**: Encryption will be used if one of the endpoints in the call requires it. Where both endpoints are also set to *encryption optional*, whether or not encryption will be used is decided by the endpoints. In transcoded calls, it is possible for one part of the call to be encrypted and the other part not to be encrypted; in a non-transcoded call, encryption is either used for both parts of the call or not at all • **Required**: Encryption must be used by both parts of the call (that is, by both endpoints in the calls) • **Disabled**: Encryption will not be used by any call	For information about installing feature keys, refer to Upgrading the firmware. AES encryption is used for H.323 calls. SRTP encryption is used for SIP calls. Note that non-transcoded calls will only take place where you have the HD video feature key installed and the **Allow non-transcoded calls** option selected. For more information refer to Using encryption with the IP gateway .

Advanced settings

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

Field	Field description	Usage tips
Audio codecs from IP gateway	Restricts the IP gateway's choice of audio codecs to be used for transmitting audio to endpoints.	When communicating with an endpoint, the IP gateway receives a list of supported audio codecs from the endpoint. The IP gateway chooses an audio codec from those available, and sends audio data to the endpoint in that format.
Audio codecs to IP gateway	Determines which audio codecs the IP gateway advertises to remote endpoints, restricting the endpoints' choice of channels available for sending audio data to the IP gateway.	
Video codecs from IP gateway	Restricts the IP gateway's choice of video codecs to be used for transmitting video to endpoints.	When communicating with an endpoint, the IP gateway receives a list of supported video codecs from the endpoint. The IP gateway chooses a video codec from those available, and sends video data to the endpoint in that format.
Video	Determines which video codecs the IP	

Field	Field description	Usage tips
codecs to IP gateway	gateway advertises to remote endpoints, restricting the endpoints' choice of channels available for sending video data to the IP gateway.	
Video format	Sets the format for video transmitted by the IP gateway. • **NTSC** The IP gateway will transmit video at 30 frames per second (or a fraction of 30, for example: 15fps) • **PAL** The IP gateway will transmit video at 25 frames per second (or a fraction of 25, for example: 12.5fps)	This option should be set to match your endpoints' video configuration. If you set this incorrectly, the smoothness of the video both to and from the endpoints might suffer. NTSC is typically used in North America, while PAL is typically used in the UK and Europe.
Maximum transmitted video packet size	Sets the maximum payload size (in bytes) of the packets sent by the IP gateway for outgoing video streams (from the IP gateway to connected video endpoints).	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 IP gateway and potential connected endpoints. Video streams generally contain packets of different lengths. This parameter only sets the *maximum* size of a transmitted network datagram. The IP gateway optimally splits the video stream into packets of this size or smaller. Thus, most transmitted packets will not reach this maximum size.
Flow control on video errors	Enables the IP 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 IP 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 IP gateway. If there is a bandwidth limitation in the path between the endpoint and the IP gateway, it is better for the IP gateway to receive every packet of a lower rate stream than to miss some packets of a higher rate stream.
Use endpoint name as caller ID	When enabled, when the IP gateway connects to an endpoint, the caller ID that the endpoint will see is the name of the calling endpoint.	Without this option selected, the caller ID that the called party will see is the model name of the IP gateway. For example: *IP GW 3520*.
Display "Audio only call" video screen	When the IP gateway receives a call from an audio-only device, if that call is to be connected to a device that can receive video, then the IP gateway can send a display. This	For video endpoints receiving an audio-only call, it can be reassuring to see a display that confirms that no part of the call is missing.

Field	Field description	Usage tips
	display reads "Audio only call". When enabled, the IP gateway will send this display to the destination of audio-only calls.	However, for audio-only calls placed through the IP gateway to an MCU, a video port will be used unnecessarily; where video ports are at a premium, deselect this option.
Content channel video	For transcoded calls, this option controls whether or not endpoints may receive H.239 content. If this option is disabled, content will not be available to any endpoint. For non-transcoded calls, this option has no effect and endpoints will receive content even if the option is disabled.	
Convert out-of-band to in-band DTMF	Select this option to have the IP 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 (OOB). OOB DTMF has the advantage that the tones do not sound over any voice, but will not be compatible with analogue phones. For example, if you are calling out from an IP phone system through an IP 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 setting may be required. Outgoing OOB DTMF over SIP is not supported. In such cases, if this setting is enabled, the gateway converts the DTMF to in-band (and then forwards it over SIP). If this setting is not enabled, the DTMF is not forwarded. Note that IP phones can interpret in-band DTMF and will continue to work as expected with this option enabled.
SRTP encryption	Select the setting for media encryption for SIP calls: • *All transports*: If encryption is used for a call, the media will be encrypted using SRTP regardless of transport mechanism used for call control messages. • *Secure transports (TLS) only*: If encryption is used for a call, the media will only be encrypted in calls that are set up using TLS. • *Disabled*: SRTP will not be used for any calls. The IP gateway will not encrypt media for SIP calls. **CAUTION:** The interface allows you to	For more information refer to Using encryption with SIP. When disabled, the IP gateway will not advertise that it is able to encrypt using SRTP. It is only necessary to disable SRTP if it is causing problems.

Field	Field description	Usage tips
	disable SRTP encryption even if device-wide encryption is required for the IP gateway (**Encryption status** option is set to *Required*). If **Encryption status** is *Required*, and you set this option to *Disabled*, then all SIP calls will fail.	

Configuring failed call settings

Calls can fail for a number of different reasons. For each failure type, you can configure the Cisco TelePresence IP Gateway to act in one of three ways:

- **Disconnect**: the call will be disconnected
- **Auto attendant** (with a choice of all configured menus): the call will be connected to the selected auto attendant menu
- **Operator**: the call will be transferred to the operator

There are failed-call settings for each port. That is, you can configure different actions for calls that fail on each port. For example, for 'external' calls, it might be appropriate never to disconnect due to a failure, but rather to return the call to the operator.

To configure failed call settings, go to **Dial plan > Failed calls**. To toggle between the Port A and Port B failed call settings, use the Port link on the right of the display.

Refer to this table for assistance in configuring failed call settings. After making any configuration changes, click **Apply changes**.

Field	Field description	Usage tips
Direct dialing fails	Configure the action for calls where the caller attempts to direct dial a number but fails to be connected.	Calls can be forwarded to either the operator, or to any auto attendant menu, or disconnected.
Dialing from auto attendant fails	Configure the action for calls where the caller connects to the auto attendant and attempts to dial a number or select an endpoint, but is never connected to a destination.	Calls can be returned to any auto attendant menu, disconnected, or forwarded to the operator.
Calls forwarded from the operator fail	Configure the action for call that are forwarded to the operator and then fail.	Calls can be disconnected, returned to the operator, or forwarded to any auto attendant menu.
Connections to the operator fail	Configure the action for a caller that attempts to connect to the operator but the call fails (for example because the operator was not present).	This is the action for calls for when the status of the operator is 'not present' (for example, the operator has gone home) and therefore you cannot select Operator for the action.

Displaying the calls list

To display the calls list go to **Calls**. The Calls list displays all active calls on the Cisco TelePresence IP Gateway together with their basic settings.

The operator uses the Calls list (which appears as the **Operator home** page) to put calls through to the endpoints on the network. The operator either selects the endpoint to which to connect a call from the list of configured endpoints or enters the number for that endpoint.

Active calls fall into three categories:

- **Operator calls**: the call currently connected to the operator and any calls in the operator's queue
- **Auto attendant calls**: all calls currently connected to the auto attendant
- **Through calls**: all calls that are currently connected to an endpoint through the Cisco TelePresence IP Gateway not including operator calls and auto attendant calls

For active calls, you can display further details; to do so, click the Caller link for the call about which you want to view further details (see Displaying call statistics).

To disconnect a through call or a call currently in the auto attendant, click the **Disconnect** button for that call. This option is only available to admin users.

Field	Field description	Usage tips
Operator		
Caller	For a configured endpoint, the name of the endpoint. For an unconfigured endpoint, if a name is supplied by the endpoint, that will be displayed, otherwise either the E.164 number or IP address will be displayed.	Click on the name (or number) of the caller to display call statistics (see Displaying call statistics). Beneath the caller's name (or number) is the AES check code. This can be used in combination with information displayed by some endpoints to check that the encryption is secure.
Endpoint list	When a call is received by the operator, every configured endpoint is listed.	The operator can select to put through a call to any of the listed endpoints by selecting that endpoint.
Forwarding address	If a call to an unconfigured endpoint is received by the operator, the forwarding address must be typed into the text box that appears. The operator must also select the correct outgoing protocol for the call. The available protocols are configured on the **Settings > Operator** page.	Configure endpoints where possible as connecting calls to configured endpoints is easier than typing addresses; refer to Configuring endpoints.
Time of connection	The time that the call was first connected to the IP gateway.	
Duration	The duration of the call.	This is timed from the time of connection.

Field	Field description	Usage tips
Status	The status of the call.	One of: **Queued**: The call is queuing to talk to the operator **Connected**: The call is connected to the operator. This status will only be seen on units that do not have non-transcoded calls enabled (on the **Settings > Calls** page). **Connected (transcoded)**: The call is connected to the operator and is a transcoded call **Connected (non-transcoded)**: The call is connected to the receiving device and is a non-transcoded call **On hold**: The operator has put the call on hold to speak to the receiver **Ringing**: The operator has put the caller on hold and is ringing the receiving device
Auto attendant		
Caller	For a configured endpoint, the name of the endpoint. For an unconfigured endpoint, if a name is supplied by the endpoint, that will be displayed, otherwise either the E.164 number or IP address will be displayed.	Click on the name (or number) of the caller to display call statistics (see Displaying call statistics).
Time of connection	The time that the call was first connected to the IP gateway.	
Duration	The duration of the call.	This is timed from the time of connection.
Disconnect	Disconnect this call.	
Through calls		
Caller	For a configured endpoint, the name of the endpoint. For an unconfigured endpoint, if a name is supplied by the endpoint, that will be displayed, otherwise either the E.164 number or IP address will be displayed.	Click on the name(or number) of the caller to display call statistics (see Displaying call statistics).
Receiver	Displays: **Waiting for receiver to answer**: until the receiver answers the call, or voicemail is activated When the call is answered, if the receiving endpoint for the call is a configured endpoint, the endpoint name will be	If the receiver does not answer the call, and no voicemail service is available, then the action for the call will depend on how the caller came to be connected to the receiver and on the configuration options for failed calls (**Dial plan > Failed calls**). For more information, refer to

Field	Field description	Usage tips
	displayed. For an unconfigured endpoint, if a name is supplied by the endpoint, that will be displayed, otherwise either the E.164 number or IP address will be displayed.	Configuring failed call settings. How long the IP gateway will continue to attempt to get a connection to an endpoint that is not responding is controlled by the dialout timeout setting on the **Settings > Calls** page.
Time of connection	The time that the call was first connected to the IP gateway.	
Duration	The duration of the call.	This is timed from the time of connection.
Status	The status of the call.	One of: **Ringing**: The receiving device is ringing **Connected**: The call is connected to the receiving device. This status will be seen on units that do not have non-transcoded calls enabled (on the **Settings > Calls** page). **Connected (transcoded)**: The call is connected to the receiving device and is a transcoded call **Connected (non-transcoded)**: The call is connected to the receiving device and is a non-transcoded call
Disconnect	Disconnect this call.	

Displaying statistics for a call

You can view statistics about the video and audio streams between individual callers (endpoints) and the Cisco TelePresence IP Gateway by choosing this option:

1. Go to **Calls**.
2. Click a caller's name.
3. Click the **Statistics** tab.

If the caller is using audio only, the values for the video settings are not populated.

Media statistics

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

Refer to the table below for additional information.

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

Field	Field description	Usage tips
		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.
Transmit stream	The audio codec being sent from the IP gateway to the endpoint, along with the chosen packet size in milliseconds.	
Transmit address	The IP address and port to which the media is being sent.	
Encryption	Whether or not encryption is being used on the audio transmit stream by this endpoint.	This field will only appear if the encryption key is present on the IP gateway.
Packets sent	A count of the number of packets that have been sent from the IP gateway to the endpoint.	
Video (primary channel and content shown separately)		
Receive stream	The codec in use and the picture size that the IP gateway is receiving from the specific call. If the picture is a standard size (for example, CIF, QCIF, 4CIF, SIF) then this name is shown in parentheses.	
Receive address	The IP address and port (<*IP address*>:<*port*>) of the device from which video is being sent	
Encryption	Whether or not encryption is being used on the video receive stream from this endpoint.	This field will only appear if the encryption key is present on the IP gateway.
Channel bit rate	The negotiated bit rate available for the endpoint to send video in.	This value represents the maximum amount of video traffic that the remote endpoint will send to the IP gateway. It may send less data than this (if it does not need to use the full channel bit rate or the IP gateway has requested a lower rate), but it should not send more.
Receive bit rate	The bit rate (in bits per second) that the IP gateway has requested that the remote endpoint sends. The most-recently	This value might be less than the Channel bit rate for example, if the IP gateway detects that the network path to the remote

Field	Field description	Usage tips
	measured actual bit rate displays in parentheses.	endpoint has insufficient capacity to maintain a higher traffic rate. If the receive bit rate has been limited to below the maximum channel bit rate, the reason for this limitation can be seen by moving over the icon.
Received jitter	Represents the variation in video packet at arrival time at the IP gateway.	
Delay applied for lipsync	The number of milliseconds by which the video follows the audio.	
Packets received	The number of video packets destined for the IP gateway from this endpoint	
Packet errors	Video packet-level errors such as sequence discontinuities, incorrect RTP details, and so on. This is not the same as packets where the content (the actual video data) is somehow in error.	This value does not represent packets in which the actual video data in the packets is in error.
Frame rate	The frame rate of the video stream currently being received from the endpoint.	
Frame errors	The number of frames with errors versus the total number of video frames received.	
Transmit stream	The codec, size and type of video being sent from the IP gateway to the endpoint.	
Transmit address	The IP address and port of the device to which the IP gateway is sending video.	
Encryption	Whether or not encryption is being used on the video transmit stream to this endpoint.	This field will only appear if the encryption key is present on the IP gateway.
Channel bit rate	The negotiated available bandwidth for the IP gateway to send video to the endpoint in.	
Transmit bit rate	The bit rate the IP 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 IP gateway, displays in parentheses.	The Transmit bit rate value might be less than the Channel bit rate if the remote endpoint receiving the video stream from the IP gateway has sent flow control commands to reduce the bit rate. If the transmit bit rate has been limited to below the maximum channel bit rate, the reason for this limitation can be seen by moving over the icon.

Field	Field description	Usage tips
Packets sent	The number of video packets sent from the IP gateway to this endpoint.	
Frame rate	The frame rate of the video stream currently being sent to the endpoint.	
Temporal/spatial	A number that represents the tradeoff between video quality and frame rate.	A smaller number implies that the IP gateway prioritizes sending quality video at the expense of a lower frame rate. A larger number implies that the gateway is prepared to send lower quality video at a higher frame rate.

Control statistics

Control statistics provide information about the control channels that are established in order that the endpoints can exchange information about the voice and video streams (Real Time Control Protocol (RTCP) packets). Refer to the table below for additional information.

Field	Field description	Usage tips
Audio		
RTCP receive address	The IP address and port to which RTCP packets are being received for the audio and video streams	
Receiver reports	A count of the number of "receiver report" type RTCP packets seen by the IP 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 IP gateway.
Packet loss reported	Media packet loss reported by receiver reports sent to the IP gateway by the far end.	
Sender reports	A count of the number of "sender report" type RTCP packets received by the IP gateway.	These are typically sent by any device that is sending RTP media.
RTCP transmit address	The IP address and port to which the IP gateway is sending RTCP packets about this stream.	
Packets sent	The number of packets sent.	
Video (primary channel and content shown separately)		
RTCP receive address	The IP address and port to which RTCP 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 IP 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 IP gateway.
Packet loss reported	A count of the reported packet loss on the control channel.	
Sender	A count of the number of "sender report"	These are typically sent by any device that is

Field	Field description	Usage tips
reports	type RTCP packets sent by the IP gateway.	sending RTP media.
RTCP transmit address	The IP address and port to which the IP gateway is sending RTCP packets about this stream.	
Packets sent	The number of packets sent.	
Fast update requests	The number of fast update requests sent and received.	
Flow control messages	The number of flow control messages sent and received.	

Viewing a connected endpoint's diagnostics

You can view diagnostics for an endpoint's connection to the Cisco TelePresence IP Gateway while the call is in progress. To view the diagnostics:

1. Go to **Calls**.
2. Click a caller's name to display the *Call statistics* page.
3. Click the **Diagnostics** tab.

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

Understanding the dial plan

The Cisco TelePresence IP Gateway uses the dial plan to determine how to route IP calls either between the networks connected to Port A and Port B, or within those networks. When the IP gateway receives a request to initiate a new IP call, it examines the called number (if available), and uses the dial plan to determine whether to reject the call, find out which number should be called to initiate the outgoing part of the call, and to check whether or not the call should be connected to the operator or auto attendant.

There are a number of different ways in which you can use the dial plan. For example, you can use the dial plan to connect outside callers to an operator who can then connect the call, or you could configure the dial plan to allow internal callers to directly call any endpoint on their network.

The dial plan is actually divided into two; a dial plan for calls arriving on Port A and a dial plan for calls arriving on Port B. The behavior of the two dial plans is identical.

The maximum number of rules that can be added to each dial plan is 255.

Refer to the sections below for more information about the use and administration of dial plans:

- Rules
- Using rules
- Rule ordering

Rules

Dial plans are administered using rules. Rules and their addition and control are identical for each dial plan.

Each rule has a name and comprises:

- a Condition that must be matched for the rule to be invoked
  The condition can be set to match any called number, to match a call that has no called number, or can specify the called number by specific number or pattern.
- an Action that is carried out if the rule is invoked
  The action can be to reject the call, enter the auto attendant, to call the operator, or to specify the number/address to call (which can be a pattern matching, for example, the original called number).

Using rules

Each dial plan comprises a set of rules. When the IP gateway receives a new incoming call, it selects the appropriate dial plan, then compares the called number (if available) to the condition of each rule in that dial plan until a match is found. When a match is found, no more rules are checked, and the action of the matching rule is used to determine what should be done next; typically the outgoing part of the connection will be initiated - calling a number specified by the action, the auto attendant is displayed or the connection will be rejected and the incoming part terminated.

If a dial plan contains no rules, or if no rule's condition matches the called number, calls are rejected by default.

Note that the IP gateway can apply the dial plan to calls dialed using the auto attendant. This means that callers are able to use the same set of numbers regardless of whether they are dialing direct on their endpoint or dialing in the auto attendant. It also means that if you have a catch-all rule that connects callers to the auto attendant, calls matching that rule will never leave the auto attendant.For more information on adding and modifying dial plan rules, see Adding and updating dial plan rules.

Rule ordering

Rules are always checked in the same order for each incoming call. This means that a dial plan can be designed to handle specific calling cases first, then general calls if no specific cases match. For example, a dial plan might be set up to call a particular endpoint if an incoming call is received to a specific number, but all other incoming calls get connected to an operator. Such a dial plan might look like this:

1. *Condition*: **Called number is "6056"** / *Action*: **Call this number $A** (this calls the original dialed number).
2. *Condition*: **Match any called number** / *Action*: **Call the operator**

Clearly rule ordering is important to achieve this functionality. You can view and test the rule list comprising a dial plan, and modify the ordering of the rules by dragging and dropping as required. (You can also use the up and down links to reorder.) For more information, see Displaying and testing the dial plan.

Displaying and testing the dial plan

The dial plan is actually made up of two, separate dial plans: one for calls arriving on Port A and one for calls arriving on Port B. Refer to the sections below for more information.

To display or modify the Port A dial plan, go to **Dial plan > Port A**. To display or modify the Port B dial plan, go to **Dial plan > Port B** (using the Port B link on the right of the screen). Note that if Port B is disabled on the **Network > Port B** page, there will not be a dial plan for Port B.

Displaying the rules list

As described above, the dial plan comprises a set of rules that are followed in response to the incoming part of a connection in order to determine how to proceed with the outgoing part of the connection.

You can view the set of rules comprising a dial plan as a list, with rules checked from top to bottom. Refer to the table below for details of the fields displayed.

Field	Field description	More information
Name	The unique number assigned to this rule and the rule's name.	Click on a number or name to view and modify rule details (see Adding and updating dial plan rules).
Condition	Which called numbers will cause this rule to be invoked.	Possible conditions include: • **Called number is "1025"** meaning this rule is invoked if the called number is exactly as stated • **No called number** meaning this rule is invoked if the caller uses the IP address or hostname of the IP gateway • **Match any called number** meaning this rule is always invoked if checked
Action	What will happen if this rule is invoked.	Possible actions include: • **Reject the call**: if this rule is invoked the call will be terminated and the outgoing part of the call will not be established • **Enter the auto attendant "<menu name>"** : the call will be connected to the named auto attendant menu • **Call the operator**: the call will be connected to the operator • **Call this number "xxx"**: where xxx represents what is displayed: ○ a pattern

Field	Field description	More information
		○ a hostname ○ an IP address meaning that "xxx" will be called if this rule is invoked. The protocol that the call will use is also listed
*** (asterisk)**	Identifies the rule you have just moved.	If you have just moved a rule in the list, it will be marked with an asterisk (*). This is to help you see the changes you have made.

Modifying the rules list

To change the order of rules, drag and drop the rule that you want to move or use the up and down links.

To add a rule, click **Add rule** (see Adding and updating dial plan rules).

To remove a rule, select one (or more) and click **Delete selected rules**.

Testing the dial plan

It may take some experimentation to create the dial plan that you require. The Cisco TelePresence IP Gateway provides a facility to test the dial plan to see how your set of rules acts on a particular number.

To test the dial plan:

1. Go to **Dial plan**.
2. If you want to test how the dial plan acts
   - on a particular number or address for a call arriving on Port A, ensure you are on the **Port A dial plan** tab
   - on a particular number or address for a call arriving on Port B, ensure you are on the **Port B dial plan** tab
3. In the **Test dial plan** section, enter the number to test and click **Test number**.

The Cisco TelePresence IP Gateway displays the number that you have tested, the rule that the condition matched, the outcome (that is, whether the call was rejected, the call was forwarded to the auto attendant or the operator, or the number that has been dialed in response).

Adding and updating dial plan rules

This page describes how to add rules to the dial plan and how to update rules (also see Example dial plan rules).

To display or modify the Port A dial plan, go to **Dial plan > Port A**. To display or modify the Port B dial plan, go to **Dial plan > Port B** (using the Port B link on the right of the screen). Note that if Port B is disabled on the **Network > Port B** page, there will not be a dial plan for Port B).

The maximum number of rules that you can add to each dial plan is 255.

Adding dial plan rules

To add a dial plan rule:

1. Go to **Dial Plan** and select the Port A or Port B page as required.
2. Click **Add rule**.
3. Type a name for the rule.
4. For Condition choose one of:
    - *Match any called number*: this condition matches any called number and also includes calls where the called number is not known or unavailable. Generally, this kind of rule should be used towards the bottom of the dial plan list to match numbers not recognized by more specific rules higher up.
    - *No called number*: this condition matches when the caller uses the IP address or hostname of the Cisco TelePresence IP Gateway.
    - *Called number matches*:
        - To match a specific number, enter that specific number.

          Example: to match calls to "001234", type **001234**. The condition will match that and only that number.

          Use S to match * (asterisk) and use P to match # (pound/hash). Examples: to match calls to "*234", type S234; to match calls to "#0987", type P0987
        - To match a more general number, use the wildcard character, D. This matches any digit as well as # and *.

          Example: to match any number that starts with "55" followed by exactly two more digits, type **55DD**. This condition will match "5500", "5523", "5555", "5599", etc. but not "55" or "55233".
        - For more general matching, you may use one of the three repeat characters. These modify the character immediately before, whether it is a specific digit or the wildcard character. The repeat characters are:
          ? match once or zero times.
          + match once or more.
          ***** match zero or more times.
          For example, "5+" means " match at least one 5, but possibly more".
          "D*" means "match any digit, any number of times". D matches any digit as well as # and *.

          Example: to match any number that starts with "01", has any amount of digits in the middle, and ends with "5", type **01 D* 5**.
        - To include any of the incoming called digits in the outgoing called number, enclose each substitution group in a set of parentheses. Note that if you want to include the complete number, you do not need to enclose the whole expression in parentheses.

Example: to match any number starting with "678", then followed by three or four digits, and you want the final digits to form part of the called number, type the expression: **678 (DDDD?)**. This will match "6780000", "678123", "6789999" etc. but not "67822" or "775000".

5. For Action (that is, what happens to the outgoing part of the call if this rule is invoked) choose one of:
   - *Reject the call*: the call will be terminated and the outgoing part of the call will not be established.
   - *Enter the auto attendant*: the call will be connected to the auto attendant. Using the drop-down menu, select the auto attendant menu to display to callers whose call matches this rule. For more information refer to Configuring auto attendant menus.
   - *Call the operator*: the call will be connected to the operator.
   - *Call this number*: the outgoing call will be placed to the number that is entered here. Type a number, or an IP address or hostname.
     - To call a specific number (you can also specify an IP address or hostname), type that number (or IP address or hostname).

       Example: to specify that when this rule is invoked, the MCU with hostname my_mcu is called, type **my_mcu**.

       Example: suppose the domain "example.com" has an H.323 service (SRV) record set up. To call an H.323 video endpoint residing in that domain, e.g. with URI example.person@example.com, set an action to call **example.person@example.com**. For information about domain (DNS) SRV records, see RFC 2782.
     - To call a specific extension, separate the IP address or hostname from the extension by typing a exclamation mark (!).

       Example: to call the MCU with IP address "10.2.1.33", and try to join a conference with numeric identifier "00000", type **10.2.1.33 ! 00000**
     - To include any of the digits from the incoming called number in the outgoing number, specify a substitution, by typing the dollar sign ($) followed by a index. Valid indices are:
       A: substitute the entire incoming called number.
       1..9: substitute the digits enclosed in the relevant set of parentheses of the condition.

       Example: for all calls matching the condition of "55 (DDDD)", set an action to call the MCU with name "my_mcu" and join the call to the conference with identifier that matches "(DDDD)". For this example, type the action of **my_mcu ! 00 $1**. In this case, an incoming call to "551234" will attempt to join conference with numeric identifier "001234" on the MCU with the name "my_mcu".

       When you have entered the number, select the protocol from the drop-down list:
       - For H.323 calls, choose between:
         - *H.323 (without gatekeeper)*: the call will be treated as an H.323 protocol call; no gatekeeper will be consulted
         - *H.323 using a configured gatekeeper*: you can select a gatekeeper to be queried for calls matching this rule. The gatekeeper specified here will override the port-associated gatekeeper
       - For SIP calls, choose between:
         - *SIP (without registrar)*: the call will be treated as a SIP call; no registrar will be consulted

- *SIP using a configured registrar*: you can select the registrar to be consulted for calls matching this rule

6. Click **Add rule**.

Updating dial plan rules

To update an existing dial plan rule:

1. Go to **Dial plan** and find the rule you want to modify.
2. Click on the number or name of the rule to view its details.
3. Modify the rule details using the information listed above in Adding dial plan rules to help you.
4. Click **Update rule**.

Dial plan syntax

This page describes the syntax that you can use when adding dial plans.

Syntax for conditions (*Called number matches*)

When you configure the *Condition* for a dial plan rule, you may want to specify a pattern for the called number rather than specifying any of: called number, no called number or the exact called number.

The table below describes the syntax you can you to express a pattern for the *Called number matches* field in the condition of a rule:

Syntax	Description	Example
Numbers 0 to 9	To match a specific number, enter that number.	Example: to match calls to "001234", type 001234. The condition will match that and only that number.
S	To match an * (known as an asterisk or star), enter an S.	Example: to match calls to "**1234", type SS1234. The condition will match that and only that number.
P	To match a # (known as a pound or hash), enter a P.	Example: to match calls to "#1234", type P1234. The condition will match that and only that number.
D	To match any digit, use the wildcard character **D**	Example: to match any number that starts with "623" followed by exactly two more digits, type 623DD. This condition will match "62300", "62323", "62355", "62399", etc. but not "623" or "623233".
?	To match once or zero times, use **?**	Example: "6?" means match one 6 or no 6s, and is useful when used with the wildcard "**D**" where you do not know how long a number will be. The expression: "67800D?" will match "67800" and "678004" but not "67800666".
+	To match once or more, use **+**	Example: "5+" means "match at least one 5, but possibly more".
*	To match zero or more times, use *. This is useful when used with the wildcard: "D*" means "match any digit, any number of times".	Example: to match any number that starts with "01", has any amount of digits in the middle, and ends with "5", type **01 D* 5**.
()	Parentheses indicate substitution groups. To include any of the incoming called digits in the outgoing called number, enclose them in parentheses. Note that if you want to include the complete number, you do not need to enclose the whole expression in parentheses.	Example: to match any number starting with "678", then followed by a number of other digits, and you want the final digits to form part of the called number, type the expression: 678 (D*). This will match "6780000", "678123", "6789999" etc. but not "775000".

Syntax for actions (*Call this number*)

When you configure the *Action* for a dial plan rule, you may want to specify a pattern for the number to call, rather than specifying any of: call original called number, reject the call, or the exact number to call.

The table below describes the syntax you can use to express a pattern for the *Call this number* field in the action of a rule:

Syntax	Description	Example
Letters and numbers for address	To call a specific number (you can also specify an IP address or hostname), type that number (or IP address, hostname, or H.323 URI).	Example: to specify that when this rule is invoked, the MCU with hostname my_mcu is called, type **my_mcu**.
!	To call a specific extension, separate the IP address or hostname from the extension by typing an exclamation mark (**!**).	Example: to call the MCU with IP "10.2.1.33", and try to join a con ference with numeric identifier "00000", type **10.2.1.33 ! 00000**. Example: Suppose the domain “example.com” has a H.323 service (SRV) record set up. To call a H.323 video endpoint residing in that domain, e.g. with URI example.person@example.com, set an action to call **example.person@example.com**. For information about domain (DNS) SRV records, see RFC 2782.
$	To include any of the digits from the incoming called number in the outgoing number, specify a substitution, by typing the dollar sign ($), followed by a index. Valid indices are: **A**: substitute the entire incoming called number. **1 to 9** : substitute the digits enclosed in the nth set of parentheses of the condition.	Example: for all calls matching the condition of "55 (DDDD)", set an action to call the MCU with name "my_mcu" and join the call to the conference with identifier that matches "(DDDD)". For this example, type the action of **my_mcu ! 00 $1**. In this case, an incoming call to "551234" will attempt to join conference with numeric identifier "001234" on the MCU with the name "my_mcu". Note that if the substitution creates an empty number, the call will be rejected; in the above example, an incoming call to 55 would result in an empty substitution.

Example dial plan rules

Use the examples on this page to help you configure your own dial plan rules.

Note that you need to consider both the Port A and Port B dial plans. Depending on how you have configured your network and which networks you have connected to Port A and Port B, you might need to configure different dial plans for each port.

Rules are always checked in the same order for each incoming call. This means that a dial plan must be designed to handle specific calling cases first, then general calls if no specific cases match. You might want to put a catch-all rule at the bottom of the dial plan; for example, a rule that will connect any call that does not match any of the preceding rules to the operator.

Examples on this page:

To see example rules working together in a dial plan, refer to Example dial plan.

Dial the operator

Using a gatekeeper, you can configure an extension so that callers can easily connect to the operator. For this example to work, both the Cisco TelePresence IP Gateway and the caller's endpoint must be registered with the same gatekeeper. In this example, the IP gateway has a dial plan prefix of 98 registered with the gatekeeper. This rule forwards any calls to 980 to the operator:

#	Condition	Action	Description
0	Called number matches "980"	Call the operator	This rule forwards all calls to the dialed number to the operator.

Note that you can also set the action for a call to the IP address or hostname of the IP gateway to call the operator.

Dial an IP address

The dial plan can be used to allow callers to dial IP addresses. This can be useful where the IP gateway is between a company network and the internet. In this example, the IP gateway is registered with a gatekeeper with dial plan prefix 98 and the caller's endpoint is registered with the same gatekeeper.

#	Condition	Action	Description
1	Called number matches "98 (D*) S (D*) S (D*) S (D*)"	Call this number: $1.$2.$3.$4	This rule takes an IP address with stars (asterisks) used to replace dots, and converts it into a dot-separated IP address and calls that IP address. For example, the caller dials: 98198*192*12*12 The IP gateway calls: 198.192.12.12

Dial in to a conference on an MCU

You can configure the dial plan to allow callers to dial in to conferences on an MCU. For this example to work, the IP gateway and the caller's endpoint must both be registered with the same gatekeeper. In this example, the IP gateway is registered with a dial plan prefix of 98.

#	Condition	Action	Description
2	Called number matches "980 (D*)"	Call this number: 192.168.12.10 ! $1	In this rule, the caller dials 980 followed by the numeric ID of the conference they require on the MCU with the given IP address. In this example, the MCU has IP address 192.168.12.10. For example to dial a conference on that MCU with a numeric ID of 2222, the caller will dial: 9802222

Setting the action for a call to the IP address or hostname of the IP gateway

Use the dial plan to configure the action for a call to the IP address or hostname of the Cisco TelePresence IP Gateway. Use of this rule does not require the use of a gatekeeper.

#	Condition	Action	Description
3	No called number	Depending on the action you require, one of: • Reject the call • Enter the auto attendant • Call the operator • Call this number <number>	Use of this rule in the dial plan (so long as it is above any rule with condition: **Match any called number**), controls the action for a call to the IP address or hostname of the IP gateway: • **Reject the call**: all calls to the IP address/hostname will be rejected - the call will not be allowed. • **Enter the auto attendant**: all calls to the IP address/hostname will be connected to the auto attendant. Note that you must also specify the name of the auto attendant menu to which you want • **Call the operator**: all calls to the IP address/hostname will be connected to the operator. • **Call this number <number>**: connect all calls to the IP address/hostname to the same endpoint.

Example dial plan

This page shows an example dial plan and explains how individual calls will match rules in the dial plan.

In the example, the Cisco TelePresence IP Gateway has registered a prefix of 98 with the gatekeeper. The IP gateway has been configured to apply the dial plan to numbers dialed in the auto attendant.

#	Condition	Action	Description
0	**Called number matches** "980"	**Call the operator**	This rule forwards all calls to 980 to the operator.
1	**Called number matches** "981 (D+) S (D+) S (D+) S (D+) S (D+)"	**Call this number** "$1 . $2 . $3 . $4 : $5"	This rule takes an IP address (with stars used to replace dots) combined with an extension number. For example, if a caller wants to dial extension 1234 on an unit with IP address 10.12.12.12, that caller will dial: 98110*12*12*12*1234
2	**Called number matches** "981 (D+) S (D+) S (D+) S (D+)"	**Call this number** "$1.$2.$3.$4"	This rule takes an IP address with stars (asterisks) used to replace dots, and converts it into a dot-separated IP address and calls that IP address.
3	**Called number matches** "980 (D+)"	**Call this number**: 192.168.12.10:$1	This rule connects a caller to a service on and H.323 gateway. For example, where 192.168.12.10 is the IP address of an MCU, the caller can connect to a conference by dialing the conference ID. In this rule, the caller dials 980 followed by the numeric ID of the conference they require on the MCU with the given IP address. In this example, the MCU has IP address 192.168.12.10.
4	**Called number matches** "982(D+)"	**Call this number**: $1	In this rule, the IP gateway dials the gatekeeper-registered E.164 number dialed by the caller. For example, a caller wanting to dial extension 1234 dials: 9821234
5	**No called number**	**Enter the auto attendant "<menu name>"**	Use of this rule in the dial plan controls the action for a call to the IP address or hostname of the IP gateway: With the action set to *Enter the auto attendant <menu name>* , all calls to the IP address/hostname will be connected to the named menu of the auto attendant.
6	**Match any called number**	**Reject the call**	This is a catch-all rule that will reject any call that does not match any of the above rules. In this example, it will prevent callers from dialing E.164 numbers in the auto attendant.

How the dial plan is applied to incoming calls

The following table shows which rule is matched when callers dial particular numbers. Note that the IP gateway will apply the dial plan that corresponds to the port on which the call arrived (dial plan A for calls arriving on Port A, dial plan B for calls arriving on Port B). The order of the rules is important. The IP gateway attempts to match an incoming call to a rule starting at the top of the list and works down until it finds a match. You can change the order of the rules by dragging and dropping or by using the up and down links on the right of the dial plan list.

Caller dials	Matched rule number	Outcome
98198*192*12*12	2	Call "98.192.12.12".
980	0	Call the operator.
9812*23*123*23*3456	1	Call "2.23.123.23!3456".
IP address of IP gateway	5	Enter the auto attendant.
9827654	4	Call extension "7654"
7890	6	Call rejected.
9804444	3	Call "192.168.12.10!4444" In this example, this connects the caller to conference 4444 on MCU with IP address 192.168.12.12

Displaying the user list

The User list gives you a quick overview of all configured users on the Cisco TelePresence IP Gateway and provides a brief overview of some of their settings. To display this list, 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 IP 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.
Privilege	Access privileges associated with this user.

Deleting users

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

Adding and updating users

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

Adding a user

To add a user:

1. Go to the **Users** page.
2. Click **Add 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 **Users**.
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 IP 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	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 passwords are stored in the configuration.xml file as plain text unless the IP gateway is configured to hash stored passwords. For more information, refer to Configuring security settings. 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.	
Privilege level	The access privileges to be granted to this user.	The available privilege levels are as follows: • **Operator**: An operator can log in to and

Field	Field Description	More Information
		view the **Operator home** page, put calls through, and set the operator status • **Administrator**: An administrator can make any configuration change and put calls through on the IP gateway
Operator endpoint	Choose an endpoint for an operator user.	If this user is an operator and you have added the operator's endpoint as a configured endpoint (**Endpoints > Add endpoint**), select the endpoint from the drop-down list. A *Create new* option on the drop-down list allows you to configure a new endpoint for this operator.
Present	Use this checkbox to tell the IP gateway whether or not this operator is available to answer calls.	This control is only for use when you have selected an *Operator endpoint*. It informs the IP gateway whether this operator is available or not. For example, if an operator is not present, unselect this checkbox and the IP gateway will not put calls through to this operator.

System defined users

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

User ID	Description	Usage tips
admin	The IP gateway must have at least one configured user with administrator privileges. By default, the User ID is "admin" and no password is required.	After logging into the IP gateway for the first time (see Logging into the web interface), you can change the User ID and password for this account. The privilege level is fixed at *administrator* for the admin user - who can see all the pages and change settings.
guest	The IP gateway must have at least one configured user with access privileges below *administrator*. The fixed User ID for this user is "guest" and by default no password is required.	You cannot change the name of the "guest" User ID, but you can add a password.

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

Displaying the endpoint list

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

The Endpoint List displays all endpoints that have been configured within the Cisco TelePresence IP Gateway. This is the list of endpoints from which an operator can choose when connecting a caller to an endpoint in the internal address book. Endpoints that are configured to appear in the internal address book can be selected by callers who have connected to the internal address book from an auto attendant menu. For more information, refer to Configuring endpoints.

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

To add a new call group, select **Add call group**. A call group is a group of two or more endpoints that has a name and can be selected as the recipient of a call. When a call group receives a call, all endpoint in the call group will ring and the first one to be answered takes the call.

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

Field	Field description
Name	The name of the endpoint.
Address	The IP address, host name, H.323 ID, E.164 number, or SIP URI of the endpoint. As each call group comprises several endpoints, no IP address will be displayed for a call group.
Type	Whether it is an H.323 or SIP endpoint or a Call group.

Configuring endpoints

You can configure endpoints to work with the Cisco TelePresence IP Gateway by choosing **Endpoints > Add Endpoint**. For configured endpoints, the operator can simply choose the endpoint's name from a list, rather than having to type in the endpoint's address and know whether the endpoint uses SIP or H.323. When you configure an endpoint, you can select whether or not that endpoint will be shown on the auto attendant, thereby enabling a caller to select to be connected to that endpoint, rather than having to know and enter the address of that endpoint.

Refer to the table below for tips on configuring an endpoint on the Cisco TelePresence IP Gateway. After entering the settings, click **Add endpoint**.

Field	Field description	Usage tips
Name	The name of the endpoint.	
Show in internal address book	Select this option if you want this endpoint to appear in the internal address book. When this option is selected for an endpoint and the internal address book is available as an option on an auto attendant menu, callers who are connected to that auto attendant can select to be connected to this endpoint.	All configured endpoints appear in the operator's list of endpoints. For more information about using the internal address book in an auto attendant menu, refer to Configuring auto attendant menus.
Address	The IP address, host name, E.164 address (phone number), H.323 ID, or URI of the endpoint.	
Protocol	The protocol that the endpoint uses.	For H.323 calls, choose between: • **H.323 (without gatekeeper)**: the call will be treated as an H.323 protocol call; no gatekeeper will be consulted • **H.323 using a configured gatekeeper**: you can select a gatekeeper to be queried for calls from this endpoint. The gatekeeper specified here will override the port-associated gatekeeper For SIP calls, choose between: • **SIP (without registrar)**: the call will be treated as a SIP call; no registrar will be consulted • **SIP using a configured registrar**: you can select the registrar to be consulted for all calls from this endpoint

Configuring call groups

You can group configured endpoints into call groups. When a call group receives a call, all endpoints in the call group will ring and the first to be answered will take the call. Call groups can be useful in organizations that have, for example, sales or support teams where anyone from the team can take a call. Call groups will appear on the list of configured endpoints from which the operator can select to forward a call; call groups can also be configured to appear on either port's auto attendant thereby enabling a caller to select to be connected to that call group, rather than having to know and enter the address of an endpoint.

Refer to the table below for tips on configuring a call group on the Cisco TelePresence IP Gateway. After entering the settings, click **Add call group** .

Field	Field description	Usage tips
Name	The name of the call group.	
Show in internal address book	Select this option if you want this call group to appear in the internal address book. When this option is selected for a call group and the internal address book is available as an option on an auto attendant menu, callers who are connected to that auto attendant can select to be connected to this call group.	All configured call groups and endpoints appear in an operator's list of endpoints. For more information about using the internal address book in an auto attendant menu, refer to Configuring auto attendant menus.
Member endpoints	Select from the list of configured endpoints, the endpoints that comprise this call group.	

Understanding operator features

The operator is a person who can put calls through on the Cisco TelePresence IP Gateway. You can use the dial plan to automatically connect calls to the operator, you can have the operator as an option on the auto attendant, and connection to the operator is an option for failed calls. The operator connects the calls one by one as calls reach the top of the operator's call queue.

The operator can put calls through to configured endpoints and call groups that have been given names in the system, or to any other endpoint by manually entering the IP address, hostname, URI, H.323 ID, or E.164 number of the endpoint. An operator can choose to speak to the proposed receiver of a call before connecting the caller.

You can configure one or more operators.

Setting up an operator

To set up an operator:

1. Go to **Users** and add a user with privilege level: *Operator*. Choose the operator's endpoint from the drop-down list of endpoints (or choose *Create new* to configure an endpoint for the operator). If the operator is currently available to answer calls, set the Operator as *Present*. For more information, refer to Adding and updating users.
2. Go to **Settings > Operator** and configure the global operator settings. For more information, refer to Configuring operator settings.
3. Create a dial plan appropriate to your requirements. Note that you can use the dial plan to automatically connect certain callers to the operator. For more information, refer to Understanding the dial plan.
4. If you want the operator to appear as an option on an auto attendant, go to **Menu builder** and create an entry for that auto attendant that has the *Action* as *Call operator*. For more information, refer to Creating auto attendant menus.
5. Go to **Dial plan > Failed calls** and configure actions for what happens when connections to the operator fail and calls forwarded by the operator fail. Note that the actions for failed calls are configured separately for each port on the Cisco TelePresence IP Gateway. To toggle between the failed call settings for each port, use the **Port A B** links on the top right of the **Failed calls** tab. For more information, refer to Configuring failed call settings.

Operator status

If you are using an operator, the IP gateway must be told when the operator is present and when he/she is not present. Operators are able to do this for themselves as this functionality is available for users who are logged in with privilege level: Operator.

To update the status of the operator, go to **Users** and click the name of the operator whose status you want to update. Use the **Present** option to tell the IP gateway whether the operator is available to answer calls or not.

Note that if all operators are absent, for calls that are forwarded to the operator, the IP gateway will either transfer to the auto attendant or disconnect, depending on the configured action on the **Dial plan > Failed calls** page. This is also true for callers who are waiting in the operator queue and all operators become 'absent'. These calls will also be treated with the action for *Connections to the operator fail* that you configure on the **Dial plan > Failed calls** page. For more information about failed calls, refer to Configuring failed call settings.

What does the operator do?

When a call is received by the operator it appears in the operator's queue at the top of the **Calls list** page. The operator then has the ability to put that call through to any configured endpoint or call group (they all appear in a drop-down menu), or the operator can type the forwarding address of the endpoint to which to connect the call.

The **Calls list** page is the primary interface that the operator will use to connect calls; when viewed by an operator (that is, someone who has logged in with with a user account with privilege level: *operator*), the Calls list page is known as the **Operator home** page. It is possible for the operator to connect calls using the interface on the operator's endpoint and this is described in “Using the IP gateway – for operators”.

The operator can choose whether to put a call through to the receiver directly or whether to put the caller on hold and speak to the call receiver before connecting the call.

When a operator logs in to the unit, only the **Operator home** page and a log in page are accessible. An operator must update the Operator's status at the bottom of their Operator's home page when they arrive at work and when they leave.

Note that when using the **Operator home** page, an operator cannot connect calls to endpoints in the Cisco TMS address book. An operator can access the address book from their endpoint. For more information about the Cisco TMS address book, refer to Configuring the Cisco TMS address book.

Configuring operator settings

To configure operator settings, go to **Settings > Operator**. For more information about setting up an operator, refer to Understanding operator features.

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

Operator menu

Field	Field description
Operator strategy	Select from the drop-down menu to control how the Cisco TelePresence IP Gateway puts through calls to multiple operators. Choose from: *Priority:* The IP gateway will put the call through to the first available operator in the list of operators on the **Settings > Operator** page. If this operator does not answer the call, the IP gateway will try the next operator in the list. This process will continue until an operator answers the call. *Round robin:* The IP gateway will put calls through to the operators in turn. That is, each call will be put through to the operator who has least recently answered a call. *Try all:* All operators receive the call simultaneously; the first operator to answer takes the call.
Automatically disable operator when call fails	With this option selected, when a call to an operator fails (that is, the operator does not answer the call) the IP gateway will disable that particular operator. Disabling the operator is the same as deselecting the **Present** checkbox on the **User** page; that operator will not receive calls until he is marked as present again.
Outgoing protocols	Select, from the list of available protocols, those protocols that you will allow the operator(s) to use when forwarding calls. The operator can choose one of the selected protocols from a drop down list for a forwarded call. One of the options is *Dial plan*; with this option selected, the operator will also have the option of selecting to use the dial plan to determine the protocol to use for the outgoing part of the call.

Operator status menu

If you have an operator, the IP gateway must be told when the operator is present and when he/she is not present. Operators are able to do this for themselves as this functionality is available for users who are logged in with privilege level: Operator.

To update the status of the operator, go to **Settings > Operator**, click on the name of the operator whose status you want to update and select/deselect the **Present** option as appropriate.

Note that when one operator is absent, for calls that are forwarded to the operator, the IP gateway if there is more than one operator, the IP gateway will attempt to connect the call to another operator according to the configured operator strategy (see the table above for more information). If there are no available operators, the IP gateway will either transfer to the auto attendant or disconnect, depending on the configured action on the **Dial plan > Failed calls** page.

Using the IP gateway — for operators

As the operator, you answer the calls one-by-one that arrive in your operator queue. You will speak to callers on your video endpoint and connect their calls.

In this section:

What does the operator do?

When you receive a call, it appears in the operator's queue at the top of the **Operator home** page. You then have the ability to put that call through to any configured endpoint (they appear in a drop-down menu), or you can type the forwarding address (or extension number) of the person to whom the caller wants to speak. The endpoint to which you put through a call can either be a video-endpoint or an audio-only telephone.

Operator availability

You must update the Operator's status at the bottom of your **Operator home** page when you arrive at work and when you leave. The Cisco TelePresence IP Gateway is configured to provide callers with other options when you are unavailable.

To tell the IP gateway if you are available or not:

1. Using your web browser, log in on the IP gateway. (Your administrator will show you how to do this.) When you have logged in, the web browser will display the **Operator home** page.
2. When you are available and at your desk, click **Set as present**.
3. When you leave your desk, click **Set as absent**.

Using the Operator home page

To access the **Operator home** page:

- Using your web browser, log in on the Cisco TelePresence IP Gateway. (Your administrator will show you how to do this.) When you have logged in, the web browser will display the **Operator home** page.

The Operator list

The Operator list is at the top of the **Operator home** page.

The number of calls that can appear in the Operator list is dependant on the model of Cisco TelePresence IP Gateway.

The caller at the top of the list represents the person to whom you are currently speaking and are about to connect. If you successfully connect this call, it will appear in the Through calls list further down the

Operator home page. When you connect the caller at the top of the list, you will be connected to the next caller in the list.

Connecting calls using the Operator home page

Depending on how the Cisco TelePresence IP Gateway has been configured, you will connect calls either by choosing a name on the Endpoint list, or by typing a forwarding address (or a combination of the two).

To connect a call by choosing a name:

1. When the caller has told you to whom he wants to speak, make a selection from the Endpoint list drop-down menu. As shown below:

2. Tell the caller you are connecting the call and click **Connect**. This connects the call.

The endpoints and call groups that appear in this list are configured through the administrator's Cisco TelePresence IP Gateway web interface. Note that operators cannot access the Cisco TMS address book through the **Operator's home** page.

To connect a call by typing the forwarding address or extension number:

1. Ensure Endpoint list is set to **<Type address>**.
2. Type the IP address or extension number in the *Forwarding address* text box.
3. Depending on how the Cisco TelePresence IP Gateway has been configured, you might also need to select the protocol for the endpoint to which you are going to connect (your administrator must provide you with this information). The screen shot below shows an example of an IP address typed into the *Forwarding address* text box and the dial plan selected as the method of deciding the protocol of the destination endpoint:

4. Tell the caller you are connecting the call and click **Connect**. This connects the call.

Speaking to the destination before connecting a call

When you answer a call, you can choose to put the caller on hold and speak to the destination before you connect the call. To do this, complete the steps above to connect a call, but do not click Connect, instead click Speak to receiver. When you are speaking to the destination, to connect the caller to the destination, hang up. Note that if the destination hangs up, then you will be reconnected to the caller. If the caller hangs up while you are talking to the destination, a message will appear on the screen: "Caller disconnected".

Using your endpoint to connect calls

When you answer a call on your endpoint, you can connect the call using the interface of your endpoint. This means that you will use the number keypad on your endpoint's controller to select the options on your endpoint's screen.

To connect calls using your endpoint:

1. Answer the call and speak to the caller.
2. Press # (hash/pound) on your endpoint's controller to change the view to picture-in-picture and access your list of options:
    - **dial a number**: You can dial an IP address (in the format 10*12*123*34) or an E.164 number using your number keypad. Press # to go to the next page. The available options on the next page will depend on the configuration of the Cisco TelePresence IP Gateway; you might have to select the protocol to cause the unit to dial the number (talk to your administrator about this) or simply select *Call*. Pressing 1 will enable you to redial.
    - **the internal address book**: Select an entry from the address book or search.
    - **the Cisco TMS address book**: Whether or not the Cisco TMS address book is available will depend on the configuration of the IP gateway. Select an entry from the address book or search.

    For more information about searching in an address book, refer to Dialing the IP gateway — for end-users.

3. When you select to call the destination, the original caller will be put on hold and when the receiver of the call answers the call, you will be able to speak to them.
4. To connect the caller to the destination, hang up. Note that you can hang up before the receiver answers the call and the caller will be directly connected to the receiver without you first speaking to the receiver.

What is the auto attendant?

On the **Operator home** page, beneath the Operator list, is the Auto attendant list. This displays a list of callers currently using the auto attendant.

The auto attendant is an interface that provides callers with the ability to connect themselves to endpoints, or directly dial endpoints on your network. Dialing the operator is one method that callers can use to be connected to endpoints on your network; dialing the auto attendant is another method. When callers dial the auto attendant, their call is connected to the Cisco TelePresence IP Gateway and their endpoint displays the auto attendant screen. The administrator can configure the auto attendant to provide audio instructions for callers. The auto attendant screen provides options for callers which can include a direct dialing option, the ability to choose an endpoint to which to connect (similar to your Endpoint list as described above), and the option to have the call connected to you (the operator).

Note that as the operator, if a caller is unable to connect successfully via the auto attendant, that caller might be transferred to you and a short reason for the failure of the call will be displayed at the bottom of you Operator home page; you will deal with the call in the normal way, but if the caller mentions a particular problem, it is worth informing your administrator.

What are through calls?

On the **Operator home** page, the list of through calls appears beneath the Auto attendant list. Through calls are all calls that are currently connected to an endpoint through the Cisco TelePresence IP Gateway not including calls in your Operator list and calls in the Auto attendant list.

Guidance for operators

Using the Cisco TelePresence IP Gateway might be your first experience of video communications. If so, there are a number of issues to bear in mind to ensure that the experience is a happy one for both you and your callers:

- **Think about the positioning of your equipment**. You will not want to have to turn your back on your caller, so you will need to be mindful of how your equipment is arranged. Your endpoint will need to be adjacent to the PC on which you access the web interface of the Cisco TelePresence IP Gateway.
- **Think about your backdrop**. Ask your administrator to make a call to you to check that your backdrop is both appropriate and tidy. Callers might be able to see more than you imagine. Also check that there will not be a lot of background noise. For example, is there music playing or a lot of office noise in the near vicinity?
- **Remember that you are live on the caller's video screen and can be seen**.
- **Treat callers as you would treat visitors to your organization**. For example, if you are talking to a video caller, it would be impolite to break off to talk to somebody else.
- As you will use a web browser to connect calls on the Cisco TelePresence IP Gateway, ensure that you keep one instance of your browser open on the **Operator home** page at all times.

Creating auto attendant menus

The Cisco TelePresence IP Gateway provides a highly flexible menu-creation feature. This enables you to create a menu (or a multi-layered menu structure) to provide end users with the options they require when they connect to the IP gateway. Menus can provide end users with access to videos, operators, address books, dial-it-yourself functions, and audio files.

To create a menu, go to **Menus > Menu builder**. Use the information in the tables below to help you create a menu, or refer to the guided tasks below the tables for further guidance.

In this section:

Menus

Field	Field description
Choose menu	
Choose menu	Select the menu that you want to edit or: • to add a menu, click **Add menu** • to delete a menu, select that menu name and click **Delete menu**
Menu properties	
Name	The name of the menu you have selected to edit. For a new menu, type a name for the menu..
Display text	Text that will appear on the menu above any menu options.

Prompt	Tell the IP gateway if you want to use a video or voice prompt with this menu item. Choose from:
	• *None*: No prompt will be used with this menu
	• *Local voice*: A voice prompt stored on the IP gateway will be used with this menu. Specify the voice prompt as follows:
	  ○ *Prompt ID*: From the drop-down menu, select the prompt you require
	  ○ *Loop*: Select this option if you want the prompt played continuously in a loop while an endpoint is connected to this auto attendant menu
	  ○ *Play on first visit only*: The menu will play this prompt the first time the caller sees this menu. On subsequent visits to this menu during this call, the prompt will not play. For subsequent calls from the same endpoint, the prompt will play on the first visit to the menu
	• *Remote video*: A video accessed through a Cisco TelePresence IP

Field	Field description
	VCR (IP VCR) will be used with this menu. Specify the video prompt as follows: ○ *IP VCR*: From the drop-down menu, select the IP VCR on which the video is stored. To configure an IP VCR, go to **Menus > Voice/video prompts** ○ *Numeric ID*: Type the Numeric ID that identifies the recording on the IP VCR which you want to use as the prompt ○ *Display*: Choose a size for the video prompt. *Small* will place the video into a pane within the auto attendant menu. *Full screen* plays the video at full screen size on the calling endpoint. Note that you can instead choose to only play the audio from the video recording (*Audio* only). The caller will be returned to the auto attendant menu when the video has finished playing ○ *Loop*: Check this option if you want the prompt played continuously in a loop while an endpoint is connected to this auto attendant menu • *Play on first visit only*: The menu will play this prompt the first time the caller sees this menu. On subsequent visits to this menu during this call, the prompt will not play. For subsequent calls from the same endpoint, the prompt will play on the first visit to the menu
Timeout	Specify a timeout in seconds after which the Timeout action will be applied. Note: any audio or video prompts associated with the menu will be allowed to finish, even if the timeout period elapses before the prompt finishes. For example, if you specify a 10-second timeout for a menu that has an associated 20-second audio prompt, the timeout action is applied after 20 seconds (when the prompt finishes) rather than after the 10-second timeout.
Timeout action	Select an action that will be invoked when any voice or video prompt has played and the timeout period has elapsed. Choose from: • *Do nothing*: the caller will remain connected to the menu • *Disconnect*: the call will be disconnected from the IP gateway • *Operator*: the caller will be connected to the operator • *Menu entry*: if you choose this option, you must then select the menu entry from the drop-down list that you would like for timed-out callers

Menu entries

Field	Field description
Choose entry	
Choose entry	Select the menu entry that you want to edit or: • to add an entry, click **Add entry** • to delete an entry, select that entry name and click **Delete entry**

Field	Field description
	• to rearrange the ordering of the entries on the menu, use the **Move up** and **Move down** buttons
Entry properties	
Caption	Type the text that will appear on the menu for this entry.
Color	Specify the color for the text using RGB values. To clear the RGB values, click **Clear**.
PIN	If you want to PIN-protect this menu entry, type a PIN. When a caller selects this menu option, he must enter the correct PIN to proceed.
Action	Select an action from the drop-down list for this menu entry: • *No action*: nothing will happen if the caller selects this menu entry • *Dial number*: the caller will be able to dial a number, or a URI and/or an IP address. You must specify how the IP gateway will interpret what the caller dials: ○ *Rewrite a*b*c*d into a.b.c.d*: allows callers to dial by IP address ○ *Prefix with*: type a prefix to be added to all numbers dialed by callers. The prefix does not apply when a caller enters an IP address ○ *H.323 (without gatekeeper)*: the IP gateway will place the call as an H.323 call without consulting a gatekeeper ○ *H.323 using <configured gatekeeper name>*: the IP gateway will place the call as an H.323 call using the named gatekeeper. To configure a named gatekeeper, go to **Settings > H.323** ○ *SIP without registrar*: the IP gateway will place the call as a SIP call without consulting a SIP registrar ○ *SIP using <configured registrar name>*: the IP gateway will place the call as a SIP call using the named registrar. To configure a named registrar, go to **Settings > SIP** • *Call operator*: the caller will be connected to the operator. If the operator is unavailable, the *Connections to the operator fail* action from the **Dial plan > Failed calls** page will be invoked • *Call specified number* : the caller will be connected to the endpoint you specify: ○ *Address*: Depending on the protocol you select, you can enter an IP address, a hostname, an E.164 number, or a URI ○ *Protocol*: From the drop-down list, select the protocol required to make the call to the endpoint you have specified • *Call pre-configured endpoint*: the caller will be connected to the endpoint you specify. Select the endpoint from the list of pre configured endpoints. The endpoints that appear on this list are configured on the **Endpoints** page • *Go to menu*: the caller will be connected to the menu that you select from the drop-down list of configured menus • *Go to internal address book*: the caller will be able to select an endpoint to which he will be connected. The list of endpoints that comprise the internal address book are those which you have configured on the **Endpoints** page with *Show in internal address book* checked

Field	Field description

	• *Go to TMS address book*: the caller will be able to select an endpoint to which he will be connected from the Cisco TelePresence Management Suite (Cisco TMS) address book. To configure the Cisco TMS address book, go to **Settings > TMS address book**. For more information, refer to Configuring the Cisco TMS address book
	• *Play video*: the caller will be connected to a video stored on the Cisco TelePresence IP VCR.
	  ○ *IP VCR*: From the drop-down menu, select the Cisco TelePresence IP VCR on which the video is stored. To configure a Cisco TelePresence IP VCR, go to **Menus > Voice/video prompts**
	  ○ *Numeric ID*: Type the Numeric ID that identifies the recording on the Cisco TelePresence IP VCR which you want to use as the prompt
	  ○ *Full screen*: plays the video at full screen size on the calling endpoint
	
	For more information about using a Cisco TelePresence IP VCR in conjunction with an IP gateway, refer to Creating auto attendant voice and video prompts

Creating a menu

To create a menu:

1. Go to **Menus** and ensure you are on the **Menu builder** tab.
2. Click **Add menu** and in the *Name* text box, type a name for your menu.
3. If you want text to appear at the top of the menu (for example, to provide instruction or further information to the caller) enter your text in the *Display text* text box.
4. You might want to specify a timeout action:
    a. Specify a timeout in seconds after which the *Timeout action* will be applied. The timeout counter starts at the end of any audio or video prompt associated with this menu.
    b. Select a *Timeout action* that will be invoked when any voice or video prompt has played and the timeout period has elapsed. Choose from:
        - *Do nothing*: the caller will remain connected to the menu
        - *Disconnect*: the call will be disconnected from the IP gateway
        - *Operator*: the caller will be connected to the operator
        - *Menu entry*: if you choose this option, you must then select the menu entry from the drop-down list that you would like for timed-out callers
5. Click **Save menu**.
6. Edit your dial plan such that the correct callers will be connected to this menu. To do this, go to **Dial plan** and add a rule where the *Action* is *Enter the auto attendant* and choose the menu you have just created from the drop-down list. For more information about dial plans, refer to Adding and updating dial plan rules.

Adding a video to the menu you have just created

To add video to the menu:

1. On the **Menu builder** tab, ensure you have highlighted the menu to which you want to add a video.
2. From the *Prompt* drop-down list, select *Remote video*.

3. From the *IP VCR* drop-down list, select the Cisco TelePresence IP VCR on which the video is stored. Note that you must pre-configure the Cisco TelePresence IP VCR on the **Menus > Voice/Video prompts** page. For more information refer to Creating auto attendant voice and video prompts.
4. Type the *Numeric ID* that identifies the recording on the Cisco TelePresence IP VCR which you want to use.
5. Choose a size for the video prompt. *Small* will place the video into a pane within the auto attendant menu. *Full screen* plays the video at full screen size on the calling endpoint. The caller will be returned to the auto attendant menu when the video has finished playing.
6. Choose the option you require from:
   - *Loop*: Check this option if you want the prompt played continuously in a loop while an endpoint is connected to this auto attendant menu
   - *Play on first visit only*: The menu will play this prompt the first time the caller sees this menu. On subsequent visits to this menu during this call, the prompt will not play. For subsequent calls from the same endpoint, the prompt will play on the first visit to the menu
7. Click **Save menu**.

Creating a menu with accompanying audio

To create a menu with accompanying audio:

1. Create a menu as described in *Creating a menu*, above.
2. Decide where the audio recording will be stored:
   - You can store up to ten short audio files on the IP gateway, know as local voice
   - You can store multiple recordings remotely on a Cisco TelePresence IP VCR. Cisco TelePresence IP VCR recordings can be used as audio-only recordings

   For local voice recordings:

   a. From the *Prompt* drop-down list, select *Local voice*.
   b. From the *Prompt ID* drop-down list, select the *User prompt* that you want to use for you menu's audio. Note that the actual recording can be made before or after you create your menu. For information about creating voice prompts to be stored locally, refer to Customizing the user interface
   c. Choose the option you require from:

      - *Loop*: Select this option if you want the prompt played continuously in a loop while an endpoint is connected to this auto attendant menu
      - *Play on first visit only*: The menu will play this prompt the first time the caller sees this menu. On subsequent visits to this menu during this call, the prompt will not play. For subsequent calls from the same endpoint, the prompt will play on the first visit to the menu

   For recordings on a Cisco TelePresence IP VCR:

   a. From the *Prompt* drop-down list, select *Remote video*.
   b. From the *IP VCR* drop-down list, select the Cisco TelePresence IP VCR on which the video is stored. Note that you must pre-configure the Cisco TelePresence IP VCR on the **Menus > Voice/Video prompts** page. For more information refer to Creating auto attendant voice and video prompts.
   c. Type the *Numeric ID* that identifies the recording on the Cisco TelePresence IP VCR which you want to use.
   d. From the *Display* drop-down list, select *Audio only*.

e. Choose the option you require from:

- *Loop*: Select this option if you want the prompt played continuously in a loop while an endpoint is connected to this auto attendant menu
- *Play on first visit only*: The menu will play this prompt the first time the caller sees this menu. On subsequent visits to this menu during this call, the prompt will not play. For subsequent calls from the same endpoint, the prompt will play on the first visit to the menu

3. Click **Save menu**.

Creating auto attendant voice and video prompts

To configure Cisco TelePresence IP VCRs on the Cisco TelePresence IP Gateway, go to **Menus** and click the **Voice/video prompts** tab.

To add a Cisco TelePresence IP VCR, click **Add IP VCR**. For more information about adding a Cisco TelePresence IP VCR, refer to Adding/editing an IP VCR.

To edit a configured Cisco TelePresence IP VCR, click on the name of that Cisco TelePresence IP VCR.

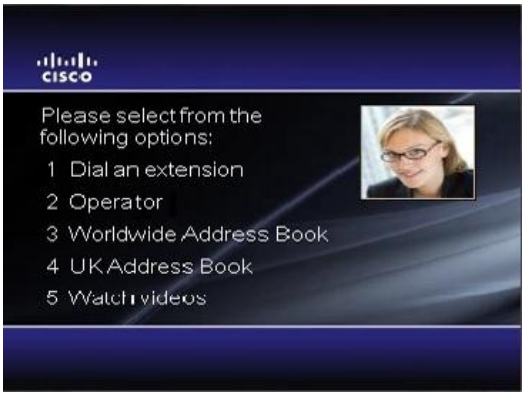
To delete a Cisco TelePresence IP VCR, select the Cisco TelePresence IP VCR that you want to delete and click **Delete selected**.

In this section:

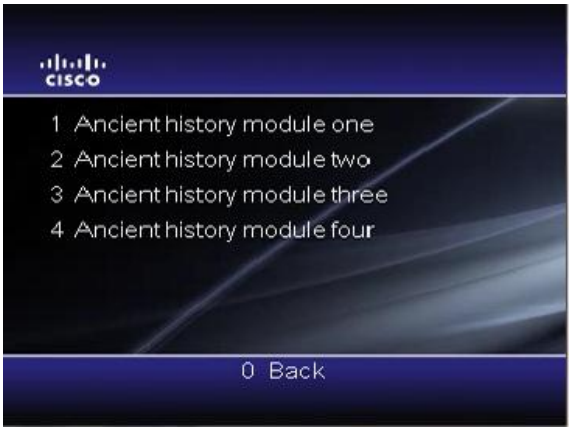
Field	Field description
Name	The name of the configured Cisco TelePresence IP VCR.
Address	The IP address or hostname of the Cisco TelePresence IP VCR, or the registered prefix and the gatekeeper to be used for connections to this Cisco TelePresence IP VCR if one has been selected.

Video prompts

To provide flexibility in the creation of auto attendant menus, you can configure up to five Cisco TelePresence IP VCRs on the IP gateway. This enables you to play any recording from a configured Cisco TelePresence IP VCR as a video on the IP gateway either in full-screen mode, or as a pane on the menu screen. For example, there might be five options on your auto attendant menu and to the right of that you could choose to have a video of a person describing those options in greater detail, as in the following screenshot of a call into an IP gateway auto attendant menu:



Alternatively, you can use the IP gateway to enable callers to access menus of videos. For example, a university might record lectures and store these on a Cisco TelePresence IP VCR and provide access to these recordings for off-campus students through the IP gateway. In this scenario, there would be a series of different menus enabling a student to navigate to his course and to the required video menu, as in the following screenshot of a call into an IP gateway auto attendant menu:



Voice prompts

By default the IP gateway includes a number of English voice prompts spoken by a female American voice. These prompts are used by the IP gateway to provide callers with information, for example: "Connecting you to your destination". You can upload your own versions of these voice prompts — either in another language, or using wording more appropriate to the environment in which the IP gateway is being used. Customizing the voice prompts on the IP gateway is described in Customizing the user interface.

In addition to the voice prompts that are installed on the IP gateway, you might require additional voice prompts to be used in conjunction with the menu items that you create. There are two methods to provide these additional voice prompts: 'Local voice prompts' and 'Remote IP VCR voice prompts' and these are described below.

Local voice prompts

You can upload up to ten voice prompts of your own creation onto the Cisco TelePresence IP Gateway. These voice prompts can each be up to 10 seconds in duration. To upload and manage local voice prompts, go to **Settings > User interface**. The topic Customizing the user interface describes how to record and upload these additional voice prompts. For more information about using voice prompts in auto attendant menus, refer to Creating auto attendant menus.

Remote IP VCR voice prompts

You can use videos stored on a Cisco TelePresence IP VCR as voice prompts. In this case, the IP gateway only plays the audio channel from the recording and ignores the video channel.

Adding/editing an IP VCR

To provide flexibility in the creation of auto attendant menus, you can configure up to five Cisco TelePresence IP VCRs on the Cisco TelePresence IP Gateway. This enables you to play any recording from a configured Cisco TelePresence IP VCR as a video on the IP gateway either in full-screen mode, or as a pane on the menu screen.

To view a list of Cisco TelePresence IP VCRs configured on the IP gateway, go to **Menus > Voice/video prompts**.

To add a Cisco TelePresence IP VCR, go to **Menus > Voice/video prompts** and click **Add IP VCR**. Refer to the information in the table below for information about the fields on that page.

Field	Field description
Name	Type a name for this Cisco TelePresence IP VCR.
Address	Type the IP address, hostname, or gatekeeper prefix for this Cisco TelePresence IP VCR.
Gatekeeper	From the drop-down menu, choose the gatekeeper to be used for connections from the IP gateway to this Cisco TelePresence IP VCR. If a gatekeeper is not required, choose *<none>*. The gatekeepers that appear on this list are configured on the **Settings > H.323** page.

Customizing an auto attendant's background and text

You can customize the auto attendant menus by:

- Uploading a background image of your choice
- Setting a color for menu items
- Setting a color for navigational options that appear at the bottom of the menu screens
- Setting a color for the borders around video that does not appear as full-screen video (for example picture-in-picture operator video)

To customize an auto attendant's background image and text:

1. Go to **Menus** and select the **Customization** tab.
2. Browse to find your background image on your network or computer.
3. Click **Upload and apply**.
4. Make any other changes you require using the table below for more information about the available settings.
5. Click **Update**.

This table describes the available options:

Field	Field description	Usage tips
Background upload		
Background image	If you have uploaded a background image, it will be displayed here. The custom graphic will be used for all auto attendant menus.	If no background image is displayed here, the auto attendant menus will use the default background image. To upload an image, click **Browse** to search for the image and click **Upload** and apply to upload the image to the IP gateway and to use it as the new background for auto attendant menus.
Customization		
Body text color	Type the RGB value for the body text color.	The body text includes any descriptive text on auto attendant menus and will be the default color for menu items. Note that you can change the text color for menu items on the **Menus > Menu builder** tab.
Footer text color	Type the RGB value for the footer text color.	The footer text is the text that appears at the bottom of the auto attendant menus. This includes navigational instructions such as **# Next** and **0 Back** for example.
Border color	Set the border color for any video that appears in a pane in the auto attendant menus (that is, not full screen video).	Choose between black and white for the border color. Black is the default border color.

Configuring the Cisco TMS address book

The Cisco TelePresence IP Gateway's auto attendant menus can display the Cisco TelePresence Management Suite (Cisco TMS) address book. Cisco TMS v 12.0 and later supports this feature. You must configure the Cisco TMS to provide the IP gateway with the required address books.

For more information about configuring an auto attendant to display the Cisco TMS address book, refer to Creating auto attendant menus.

Field	Field description	Usage Tips
Address	The IP address or hostname of the Cisco TMS.	If the Cisco TMS is correctly configured, the Cisco TMS will configure this setting itself. That is, you will not have to edit this field yourself. However, if there are any problems and the Cisco TMS has not configured this setting itself, type the IP address of the Cisco TMS.
Path	The path to the required address book on the Cisco TMS.	If the Cisco TMS is correctly configured, the Cisco TMS will configure this setting itself. That is, you will not have to edit this field yourself. However, if there are any problems and the Cisco TMS has not configured this setting itself, type the path of the Cisco TMS.
Gatekeeper to use for H.323 calls	Select the gatekeeper that will be used for all calls to H.323 endpoints in the Cisco TMS address book.	When a caller or the operator selects to forward a call to a endpoint listed in the Cisco TMS address book, Cisco TMS might return an E.164 number to the IP gateway. You must select the gatekeeper to be used for these calls to be completed successfully. The gatekeepers that appear in the drop-down menu are configured on the **Settings > H.323** page.
Registrar to use for SIP calls	Select the SIP registrar to use for all calls to SIP endpoints in the Cisco TMS address book.	When a caller or the operator selects to forward a call to a endpoint listed in the Cisco TMS address book, Cisco TMS might return a SIP URI to the IP gateway. Some calls might require a SIP registrar to be configured. The SIP registrars that appear in the drop-down menu are configured on the **Settings > SIP** page.

Configuring H.323 settings

To display the H.323 settings page, go to **Settings > H.323**. This page lists the gatekeepers configured on the Cisco TelePresence IP Gateway, with their IP address and status, and the ports by which each gatekeeper is physically attached to the IP gateway.

You can configure up to two H.323 gatekeepers on the IP gateway. Where there are two gatekeepers, they must be physically on different networks (that is, attached to different ports). You can only associate a maximum of one gatekeeper with each port. Subject to some exceptions as mentioned below, the gatekeeper that is associated with a port is the one that the IP gateway will query when a call is incoming or outgoing on that port.

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

To delete a configured gatekeeper, check the one you want to delete and select **Delete selected**.

To edit the settings of a configured gatekeeper, click the name of the gatekeeper (refer to Configuring gatekeeper settings).

To associate a gatekeeper with a port, configure the H.323 settings at the bottom of the H.323 settings page.

Field	Field description
Name	The name of the gatekeeper.
Address	The IP address or host name of the gatekeeper.
IP route	The port via which the gatekeeper is connected or in the case of the built-in gatekeeper: *Both ports (Internal GK)*. If a gatekeeper is on the subnet local to either port, the IP gateway will list that port here. Otherwise, the IP gateway will use the IP routes (configured on the **Network > Routes** page) to determine on which port the gatekeeper is to be found. For example, there might be a route configured to the gatekeeper's subnet or the IP gateway will use the default route. Usually, the port with which the gatekeeper is associated will be the same port as the one to which the gatekeeper is connected. The exception to this is the built-in gatekeeper which will both appear to be connected to both ports and can be used to bridge between two networks and associated with both ports.
Status	For an enabled gatekeeper, the number of active registrations and the number of pending registrations are displayed. If this gatekeeper usage is disabled, that is indicated here. A control to enable/disable this gatekeeper is provided here. Note that if you disable the gatekeeper here, you are disabling the IP gateway's ability to register to this gatekeeper, rather than disabling the gatekeeper itself (which for the built-in gatekeeper you can do on the **Built-in gatekeeper** page).

H.323 settings

Field	Field description
Port A / Port B associated gatekeeper	The drop-down selection box lists the gatekeepers configured on the IP gateway. If you want to associate a gatekeeper with a port, select it here. The associated gatekeeper for a port is the gatekeeper to which the IP gateway sends a query for all incoming connections on that port, and for all outgoing connections on that port that are dialed by IP address rather than by E.164 phone number (unless the dial plan or the configuration of an endpoint specifies otherwise). By querying the gatekeeper, the IP gateway ascertains whether or not the gatekeeper permits the call. In the case of an incoming call to an address in the format <numeric ID>@<domain>, the admission query used to validate the connection will be stripped to <numeric ID>. If no gatekeeper is associated with a port, either here or explicitly in a dial plan rule, the IP gateway will always make the call (outgoing calls) or accept the call (incoming calls). It does not require validation from a gatekeeper before handling a call on that port. One gatekeeper can be associated with both ports. One port can have a maximum of one associated gatekeeper.
Port A / Port B gatekeeper required	If you want all calls arriving on a port to be controlled by a gatekeeper, configure the port as *'gatekeeper required'*. Where a gatekeeper is required, calls cannot be made without querying a gatekeeper. Leave this checkbox unselected if you want the call to be connected if possible even without querying a gatekeeper. If a port is configured as 'gatekeeper required', and if the queried gatekeeper does not respond to a query regarding a call, the IP gateway will reject the call (if the query was regarding an incoming call) or not make the call (if the query was regarding an outgoing call). If a port is configured as 'gatekeeper required', this setting will be imposed by the IP gateway whether it is the gatekeeper associated with the port that is used or whether a dial plan rule or a configured endpoint's settings dictate the use of a different gatekeeper.

Displaying the built-in gatekeeper registration list

The Cisco TelePresence IP Gateway contains a built-in gatekeeper with which devices can register multiple IDs. IDs can be numbers, H.323 IDs (e.g. Fredsendpoint) or prefixes.

Up to 25 devices can be registered without a feature key. Feature keys can be purchased to increase this number.

Note: The IP gateway can register with its own built-in gatekeeper. The IP gateway then counts as one registered device. See Configuring gatekeeper settings.

Configuring the built-in gatekeeper

To start the gatekeeper:

1. Go to **Network > Services** and select the H.323 gatekeeper check box to open a port for the gatekeeper. (On the Cisco TelePresence IP Gateway, ports are not open by default for security reasons.)
2. Go to **Gatekeeper**, select *Enabled* in the Status field and click **Apply changes**. If you attempt to enable the built-in gatekeeper without opening the port, an error message is displayed.

Configuring neighboring gatekeepers

You can optionally configure the built-in gatekeeper with up to two neighboring gatekeepers. This means that if the built-in gatekeeper receives a request (known as an Admission Request or ARQ) to resolve an ID to an IP address and that ID is not currently registered with it then it will forward that request to its neighbor gatekeeper(s), as a Location Request (LRQ). The built-in gatekeeper will then use the information received from the neighbor(s) to reply to the original request.

You can also configure the behavior of the built-in gatekeeper on receipt of LRQs from another gatekeeper. It can:

- send LRQs regarding unknown IDs to its neighbor(s)
- reply to LRQs from other gatekeepers
- accept LCFs (Locations Confirms) from non-neighboring gatekeepers

Refer to this table for assistance when configuring the built-in gatekeeper:

Field	Field description	Usage tips
Status	Enables or disables the built-in gatekeeper.	To use the built-in gatekeeper, you must enable it here.
Full proxy (Port A/Port B)	Controls the behavior of the built-in gatekeeper on receiving a directly-dialed (that is, not via the auto attendant or operator) call from a registered endpoint to an IP address or E.164 number. The options are: • *Disabled*: The gatekeeper will check whether or not the call is allowed, but will not proxy the	To control gatekeeper behavior for calls into Port A, use the *Full proxy (Port A)* control. To control the proxy mode of gatekeeper behavior for calls into Port B, use the *Full proxy (Port B)* control. Options for Port B are not available if Port B is disabled (to enable Port B go to **Network > Port B**). For Port A, *Between ports* is not available as an option if Port B is disabled.

Field	Field description	Usage tips
	call through itself. The call will still be able to take place if the two endpoints are on the same network or if there is an explicit route between the endpoints' networks. • *Between ports (to registered aliases)*: This option allows calls dialed by E.164 number from a registered endpoint on one port to a registered endpoint on the other port. (The endpoints must be registered with either the built-in gatekeeper or with a neighbored gatekeeper.) The built-in gatekeeper will proxy the signaling and media for allowed calls through itself. Calls dialed by IP address will not be allowed. • *Between ports (any destination)*: For calls from a registered endpoint on one port to an endpoint on the other port, the built-in gatekeeper will proxy the signaling and media for allowed calls through itself. Note that for calls dialed by E.164 numbers, both endpoints must be registered with the built-in gatekeeper (or a neighbored gatekeeper). For calls dialed by IP address, only the calling endpoint must be registered.	
Neighbor gatekeeper 1 and 2	Enter the IP address(es), or hostname(s) (or <host>:<port number> to specify a port other than the default of 1719 on the neighboring gatekeeper), of the neighboring gatekeeper(s).	These are the gatekeepers to which the built-in gatekeeper will send an LRQ if it has received an ARQ to resolve an ID which it does not currently have registered. The built-in gatekeeper will then use the information received from the neighbor(s) to reply to the original request.
Accept LRQs	Configures the built-in gatekeeper to reply to LRQs from other gatekeepers.	These requests can come from any gatekeeper which has the IP gateway's built-in gatekeeper configured as one of its neighbors.
Forward LRQs for unknown IDs	Configures the built-in gatekeeper to send (or not to send) LRQs	Unless you have selected to *Accept LRQs*, you cannot configure the IP gateway to

Field	Field description	Usage tips
	regarding unknown IDs to its neighbor(s). Choose from the options: • *Disabled*: The IP gateway will only respond to LRQs about IDs registered with itself. It will not forward LRQs about IDs that are not registered with itself to neighboring gatekeepers. • *Enabled, using local return address*: The IP gateway will put, in the LRQ, its own address as the return address for the LCF. • *Enabled, using received return address*: The IP gateway will put, in the LRQ, the address of the gatekeeper that originated the request as the return address for the LCF. Use this option only if you are configuring the IP gateway to operate in an environment with a multiple-level gatekeeper hierarchy. For example, the 'received address' is required by the national gatekeepers connected to the Global Dialing Scheme (GDS).	forward any LRQs. Enabling *using received return address* can be a significant security risk. Only use this setting with proper cause.
Accept LCFs from non-neighbors	This setting enables the built-in gatekeeper to accept LCF message responses from any IP address.	This setting is for use in environments with a multiple-level gatekeeper hierarchy. For example, this feature is required by the national gatekeepers connected to the Global Dialing Scheme (GDS). Enabling this setting can be a significant security risk. Only use this setting with proper cause.

Gatekeeper status

The number of registered devices is shown in the format X / Y where Y is the number of registered devices that your built-in gatekeeper is licensed for. Equally, the total number of registered IDs is shown as Z / 1000, where 1000 is the maximum number of registrations allowed over all registered devices.

Below these summary figures is a table showing individual registrations. Registrations can be viewed by registered ID (the "ID view") or by device (the "Registration view"), giving complete and easily searchable lists. Switch between the views by clicking on the appropriate button.

The Registration view shows the summary per device (also known as the registrant), while the ID view shows individual registrations. This means that registrations from the same device are not necessarily listed together in the ID view but the view can be sorted by Registrant or Index to help you identify IDs belonging to the same registrant.

ID view

Field	Field description	Usage tips
ID	The ID which the registrant has registered with the gatekeeper.	IDs can be numbers, H.323 IDs or prefixes.
Type	The type of registration.	One of: E.164 (digits), H.323 ID or Prefix.
Index	This registrations index within the total number of registrations that this registrant has made with the gatekeeper.	In the format X / Y where Y is the number of registrations that this registrant has made with the built-in gatekeeper, and X is this particular registration's position within the total. Therefore, if a device registered 3 IDs with the gatekeeper and this was the second registration to be made, the Index would be 2 / 3.
Registrant	The IP address of the device that this registration was made from.	If the remote device has indicated via the RAI (Resource Availability Indication) mechanism that it is close to its resource limit, the Registrant will be labeled as "almost out of resources".

Registration view

This view shows a one-line summary for each device registered with the built-in gatekeeper.

To deregister one or more devices (and all registrations for these devices), select the check boxes for the appropriate entries and then click **Deregister selected**.

Field	Field description	Usage tips
Registrant	The IP address of the device.	If the remote device has indicated via the RAI (Resource Availability Indication) mechanism that it is close to its resource limit, the Registrant will be labeled as "almost out of resources".
H.323 ID	The registered H.323 ID of the device.	To help identify registering devices, if the registrant has registered a H.323 ID (which will typically be its device name) that H.323 ID is shown here. If the device has registered multiple H.323 IDs, only the first is displayed.
Registered IDs	The number of registrations that this device has made with the built-in gatekeeper.	Click **(view)** to display individual registrations for the selected device. (The format is the same as the ID view, but the table only includes entries for one device.)
Registration time	The time today or date and time of the last registration.	

Using the built-in gatekeeper to bridge between two networks

In some configurations, you might want callers on the Port A network to be able to dial directly to endpoints on the Port B network and/or vice versa (as opposed to using the operator or auto attendant). For endpoints registered with the built-in gatekeeper calls can be transparently routed through the Cisco TelePresence IP Gateway. For calls dialed by E.164 number, the dial plan must be correctly configured and both endpoints must be registered with the built-in gatekeeper. For calls dialed by IP address, only the calling endpoint must be registered with the IP gateway. Firstly, you must configure the built-in gatekeeper as follows:

1. Go to **Network > Services** and check **H.323 gatekeeper** for Port A and Port B.
2. Go to **Gatekeeper** and enable the built-in gatekeeper. Click **Apply changes**.
3. Set the IP gateway to use its built-in gatekeeper. Go to **Settings > H.323** and click **Add gatekeeper**:
   i. Type a name for the gatekeeper.
   ii. Enable *H.323 gatekeeper usage*.
   iii. For *H.323 gatekeeper address*, enter the IP address of the IP gateway (set the address to 127.0.0.1 or localhost).
   iv. For *Gatekeeper registration type*, select *Gateway*.
   v. Type an H.323 ID for the IP gateway and if required, enter a dial plan prefix (or prefixes). Use of a dial plan prefix causes the IP gateway to make a second registration with the gatekeeper. The gatekeeper will forward any E.164 numbers starting with this prefix to the IP gateway.
   vi. Click **Apply changes**.
4. In the **Settings > H.323** page, associate the gatekeeper that you have just created with both Port A and Port B.

For registered endpoints dialing by E.164 number:

When dialing an E.164 number, endpoints registered with the built-in gatekeeper can call endpoints on the same network directly, but when calling to an endpoint on the other side of the IP gateway, the IP gateway can detect this and the connection can be transparently routed through it. To use the built-in gatekeeper in this way, the dial plan must be correctly configured.

For the port or ports for which you want to allow calls to be bridged to endpoints on the other port, create an entry in the dial plan. For example, if you want to allow calls coming in on Port A to be bridged to endpoints on Port B, create a entry in the Port A dial plan as follows:

1. In the web interface, go to **Dial plan > Port A** and click **Add rule**.
2. Type a name for the rule.
3. For *Condition*, select *Match any called number*.
4. For *Action*, select *Call this number $A* using the built-in gatekeeper.
5. Click **Add rule** to add the rule to the dial plan.
6. Ensure that this rule will be matched - that is, make sure that it does not come after another 'Match any called number' rule in the dial plan.
7. Go to **Gatekeeper** and set *Full proxy (Port A/Port B)* to *Between ports (to registered aliases)*.

When using the built-in gatekeeper in this way, you can configure the same dial plan for each port if you require callers on both ports to have this functionality.

For registered endpoints dialing by IP address:

When dialing an IP address, endpoints registered with the built-in gatekeeper can call endpoints on the same network directly, but when calling to an endpoint on the other side of the IP gateway, the IP gateway can detect this and the connection will be transparently routed through it. Only the calling endpoint must be registered with the IP gateway. To use the built-in gatekeeper in this way, the *Full proxy (Port A/Port B)* setting on the **Gatekeeper** page must be set to *Between ports (any destination)*.

Configuring gatekeeper settings

To configure settings for a gatekeeper, go to **Settings > H.323** and click the name of the gatekeeper for which you want to modify settings or click Add gatekeeper to add a new gatekeeper.

By having the Cisco TelePresence IP Gateway registered with a gatekeeper, callers can dial E.164 numbers even if they cannot access the gatekeeper themselves. For example, callers can direct-dial endpoints via the IP gateway using directory numbers rather than requiring them to know the IP address or host name of the endpoint.

Using a gatekeeper can also make it easier for the operator; if there are a lot of unconfigured endpoints, it will be easier for the operator to type E.164 numbers than IP addresses.

If are using an MCU and you have the IP gateway registered with the same gatekeeper as the MCU, then callers can easily dial-in to conferences. For example, if the MCU is registered with a prefix of 7, with a conference running with a numeric ID of 42, caller can dial 742 from the IP gateway to join that conference.

You can register the IP gateway with an external gatekeeper or you can enable its own built-in gatekeeper.

Note that endpoints on both ports on the IP gateway can use the built-in gatekeeper and if set up as described in Using the built-in gatekeeper to bridge between two networks, any endpoint can dial any other endpoint using an E.164 number; when dialing an E.164 number, endpoints registered with the built-in gatekeeper will then call endpoints on the same network directly, but when calling to an endpoint on the other side of the IP gateway, the IP gateway will detect this and will transparently route the connection.

In this section:

Gatekeeper settings

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

Field	Field description	Usage tips
Name	Type a name for the gatekeeper.	This is a useful way of quickly identifying a gatekeeper where you have configured more than one gatekeeper.
H.323 gatekeeper usage	Enables the IP gateway to register with an H.323 gatekeeper.	When set to *Disabled* then no gatekeeper registrations are attempted with this gatekeeper (and existing registrations with this gatekeeper are torn down), regardless of other gatekeeper settings. When set to *Enabled* registrations with this gatekeeper are attempted, and this gatekeeper can then be contacted for incoming and outgoing calls. If the gatekeeper does not respond, calls are still connected if possible unless gatekeeper use is set to *Required* (for the port on which a call arrived) on the **Settings > H.323** page.
H.323 gatekeeper address	Identifies the network address of the gatekeeper to which IP gateway registrations should be made.	This can be specified either as a host name or as an IP address. This field will have no effect if *H.323 Gatekeeper usage* (see above) is set to *Disabled*. The gatekeeper can be either the built-in gatekeeper enabled on the **Gatekeeper** page (see Displaying the built-in gatekeeper registration list) or an external gatekeeper. To use the built-in gatekeeper enter "127.0.0.1". For an external gatekeeper, enter its host name or IP address.
Gatekeeper registration type	Controls how the IP gateway identifies itself when registering with its configured gatekeeper.	Cisco recommends that you use the *Terminal / gateway* option unless you are using a service prefix (in this case, use *Gateway*). Only use a different option if you are: • having specific problems • using the Cisco Gatekeeper (with or without a service prefix), in which case use *Gateway (Cisco GK compatible)* Refer to Product Support section of the web site for more details about interoperability with gatekeepers.

Field	Field description	Usage tips
H.323 ID	Specify an identifier that the IP gateway can use to register itself with the H.323 gatekeeper.	Before the IP gateway can register any IDs with the H.323 gatekeeper, it must make a unit-wide registration. This field is required for the gatekeeper registration. This will have no effect if *H.323 gatekeeper usage* is disabled.
Use password	If the configured gatekeeper required password authentication from registrants, check the *Use password* box and type the password.	Note that where password authentication is used, the *(Mandatory) H.323 ID to register* will be used as the username.
Dial plan prefix	Causes the IP gateway to make further registrations with the gatekeeper. The gatekeeper will forward any E.164 numbers starting with prefixes entered here to the IP gateway.	You can enter one or more dial plan prefixes. Use spaces to separate multiple prefixes. This is an optional field. Callers using endpoints also registered with the gatekeeper, can dial registered prefixes to access the IP gateway. The IP gateway will then determine what to do with the call depending on the rules in the dial plan. In this way, you can use dial plan rules to enable different types of calls to be handled in different ways by the IP gateway. For example, calls prefixed in one way could be forwarded directly to the operator and calls prefixed in another way could be forwarded to the auto attendant, or transferred directly to a call group.
Send resource availability indications	Select this option if you want the IP gateway to inform the gatekeeper about its availability or non-availability. This information will be used by the gatekeeper when it is selecting where to place calls. Only use this option where multiple IP gateways are registered with the *same* IP gateway dial plan prefix on the same gatekeeper. When selected, the IP gateway will inform the gatekeeper when it is unavailable (that is, all its ports are already in use).	The ability of the IP gateway to send resource availability messages is useful in a network where there are multiple IP gateways or where there are several IP gateway blades in an MSE. In an environment with multiple IP gateways registered with the same gatekeeper, that gatekeeper should favor devices in the available state when choosing where to place new calls. For example, when one IP gateway sends the gatekeeper a message indicating that it is not available, the gatekeeper will then attempt to use a different IP gateway for new calls. When all ports are in use, the IP gateway sends a message to indicate that it is not available; when one or more ports becomes available, the IP gateway sends a message

Field	Field description	Usage tips
		indicating that it is available.

Gatekeeper status

The Cisco TelePresence IP Gateway also displays brief status information about its registrations with the configured gatekeeper.

Field	Field description	Usage tips
Current status	Displays the IP address of the gatekeeper currently being used by the IP gateway.	This information might be useful if the gatekeeper has been specified with a host name rather than with an IP address.
Registered address	Displays the local IP address and port number that the IP gateway has registered with the gatekeeper.	This information might be useful if the IP gateway has more than one IP address, for instance if both Ethernet interfaces are in use.
IP route	The port via which the gatekeeper is connected or in the case of the built-in gatekeeper: *Both ports (Internal GK)*.	If a gatekeeper is on the subnet local to either port, the IP gateway will list that port here. Otherwise, the IP gateway will use the IP routes (configured on the **Network > Routes** page) to determine on which port the gatekeeper is to be found. For example, there might be a route configured to the gatekeeper's subnet or the IP gateway will use the default route. Usually, the port with which the gatekeeper is associated will be the same port as the one to which the gatekeeper is connected. The exception to this is the built-in gatekeeper which will both appear to be connected to both ports and can be used to bridge between two networks and associated with both ports.
Alternate gatekeepers available	Displays the number of 'alternate' gatekeepers configured on the H.323 gatekeeper. This figure comes from the gatekeeper itself; if there are any 'alternate' gatekeepers configured, the gatekeeper tells the IP gateway their IP addresses.	Where the configured gatekeeper has told the IP gateway about any configured 'alternate' gatekeepers and if the IP gateway loses contact with the configured gatekeeper, the IP gateway will attempt to register with each of the 'alternates' in turn. If none of the 'alternate' gatekeepers responds, the IP gateway will report that the registration has failed. If the IP gateway successfully registers with an 'alternate' gatekeeper: • The *H.323 gatekeeper status* will indicate that registration is with an 'alternate'.

Field	Field description	Usage tips
		• The list of 'alternates' received from the new gatekeeper will replace the previous list. • The IP gateway will only revert back to the original gatekeeper if the 'alternate' fails and only if the original gatekeeper is configured as an 'alternate' on the current gatekeeper's list of 'alternates'. Note that if the IP gateway registers with an 'alternate' that does not itself supply a list of 'alternates', the IP gateway will retain the original list and if it loses contact with the current gatekeeper, each one will be attempted from the top again as before.
Number of active registrations	Displays the number of E.164 numbers plus H.323 IDs plus prefixes that the IP gateway has registered with the gatekeeper.	It also shows how many registrations are in progress but are not fully registered yet.

Configuring SIP settings

The SIP settings page lists the SIP registrars configured on the Cisco TelePresence IP Gateway. It allows you to configure SIP settings for the IP gateway.

To display the SIP settings page, go to **Settings > SIP**.

The SIP settings page lists the SIP registrars configured on the IP gateway. It also shows the IP address, registrar type, and the status for each SIP registrar.

You can configure up to five SIP registrars on the IP gateway.

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

To delete a configured SIP registrar, select the one you want to delete and click Delete selected.

To edit the settings of a configured SIP registrar, click the name of the registrar (refer to Configuring SIP registrar settings).

Field	Field description
Name	The name of the SIP registrar.
Address	The IP address or host name of the SIP registrar.
Type	The type of SIP registrar, which will be one of: • **Standard SIP**: for non-Microsoft SIP registrars • **Microsoft LCS**: for Microsoft SIP registrars
Status	The status of the IP gateway with this SIP registrar. The status will be one of: • **Registered**: the IP gateway is registered with the SIP registrar • **Registering**: the IP gateway is registering with the SIP registrar • **Unregistered**: the IP gateway is not registered with the SIP registrar

SIP settings

Field	Field description
Username	The global SIP login name for the IP gateway. This will be used where necessary for user identification, and authentication in SIP calls where there is no registrar.
Password	The global SIP password for the IP gateway. This will be used where necessary for user identification, and authentication in SIP calls where there is no registrar.
SIP proxy address	Identifies the network address of the SIP proxy. If you have a SIP proxy and a SIP caller does not use the SIP registrar, the call will try and use the proxy to resolve the address for the call.
Maximum bit rate from Microsoft OCS/LCS clients	Select a maximum bit rate to use from Microsoft OCS/LCS clients. Microsoft OCS/LCS clients will try to use the maximum bit rate that the IP gateway advertises during the initial call setup. In most scenarios, you will not want

Field	Field description
	OCS/LCS clients to use the *Default bandwidth from IP gateway* that is configured on the **Settings > Calls** page (Configuring global call settings). Use this setting to select an appropriate bit rate for Microsoft OCS/LCS clients. <*limit disabled*> will cause the IP gateway to advertise the *Default bandwidth from IP gateway.*
Outgoing transport	The global setting for the protocol to be used for call control messages for outgoing call connections. This setting will only be used where SIP is used without a registrar. If your SIP devices use TCP, select TCP as the outgoing transport. If your SIP devices use UDP, select UDP as the outgoing transport. If you want to use encrypted SIP, select TLS. Note that if you want to use encrypted SIP: • the IP gateway must have the encryption feature key • encryption must be enabled unit-wide on the **Settings > Calls** page • the TLS service must be enabled on the **Network > Services** page The IP gateway accepts incoming connections using TCP, UDP, or TLS providing those services are enabled on the **Network > Services** page (Configuring network services).

Configuring SIP registrar settings

To allow callers with SIP endpoints to connect to the Cisco TelePresence IP Gateway by dialing a directory number rather than an IP address, you must configure a SIP registrar. The settings on this page control the IP gateway's interaction with the SIP registrar and with SIP endpoints.

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

Field	Field description	Usage tips
Name	Type a name for the SIP registrar.	This is a useful way to identify a registrar where more than one has been configured.
SIP registration settings	Specifies the level of SIP registration for the IP gateway.	Can be set to: • *No registration*: The IP gateway will not register with the SIP registrar. This means that a user with a SIP endpoint can only connect to the IP gateway by dialing its IP address or hostname • *Register IP GW*: Enables callers to dial in to the auto attendant of the IP gateway
SIP registrar address	Identifies the network address of the SIP registrar to which IP gateway registrations should be made.	This can be specified either as a host name or as an IP address. This field will have no effect if **SIP registration settings** is set to *No registration*.
SIP registrar type	Choose between: • *Standard SIP*: for non-Microsoft SIP registrars • *Microsoft OCS/LCS*: for Microsoft SIP registrars	Your choice is dependent on the type of SIP registrar you are using. If you are using Microsoft OCS or LCS, you will also need to configure the OCS or LCS to recognize the IP address of the IP gateway and treat it as authenticated. This field will have no effect if **SIP registration settings** is set to *No registration*.
Use local certificate for outgoing connections and registrations	Select this option to force the IP gateway to present its local certificate when registering with the SIP registrar.	Often, the SIP registrar will not require the local certificate from the IP gateway. Only select this option if your environment dictates that the SIP registrar must receive the local certificate.
Username	The login name for the IP gateway on the SIP registrar.	You need to configure the SIP registrar with details of the devices that will register with it and create a login for each device. If you are using Microsoft OCS or LCS, you need to enter the full URI (for example,

Field	Field description	Usage tips
		IPGW@example.com).
Password	The password for the IP gateway on the SIP registrar.	You need to configure the SIP registrar with details of the devices that will register with it and create a login for each device. The password configured on this page needs to match the password in the SIP registrar.
Outgoing transport	Identifies the protocol to be used for call control messages for outgoing call connections.	If your SIP devices use TCP, select TCP as the outgoing transport. If your SIP devices use UDP, select UDP as the outgoing transport. If you want to use encrypted SIP, select TLS. Note that if you want to use TLS, you must have the encryption feature key (or the Secure management feature key) and the TLS service must be enabled on the **Network > Services** page. The IP gateway can accept connections on TCP, UDP, and TLS providing those services are enabled on the **Network > Services** page (Configuring network services).

SIP: Advanced

SIP implementation

The IP gateway implements SIP as defined in RFC 3261. Any product wanting to establish SIP calls with the IP gateway should implement INVITE, ACK, BYE, and CANCEL messages along with responses from 1xx to 6xx. The IP gateway acts as a client and does not return 5xx and 6xx responses itself; however, proxies and other intermediaries may do so.

To use a SIP registrar in conjunction with the IP gateway, you must register an ID for the IP gateway with the SIP registrar.

For video Fast Update Requests, the IP gateway uses a type that involves sending an INFO message with an XML body. This only applies to video endpoints, but these endpoints should be able to correctly reply to INFO requests whether or not they understand them as Fast Update Requests.

Using the IP gateway — for end-users

Depending on how the Cisco TelePresence IP Gateway has been configured, there are a number of different ways to dial the IP gateway, and to call endpoints or other services via the IP gateway.

In this section:

Dialing the IP gateway by IP address

Depending on the configuration of the unit, you might be allowed to dial the IP gateway using its IP address. You will be connected to either the auto attendant or the operator (for more information refer to Using the auto attendant and Dialing the operator, below).

Dialing the IP gateway by E.164 number or prefix

Depending on the configuration of the unit, you might be allowed to dial an E.164 number or prefix. In this scenario, for H.323 callers there will be a gatekeeper and for SIP callers there will be a registrar.

Depending on the configuration of your unit, dialing an E.164 number might connect you to the auto attendant or the operator (for more information refer to Using the auto attendant and Dialing the operator, below); it could also connect you directly to an endpoint, a video conference or to another service on the network.

Dialing by IP address and extension

Depending on the configuration of your unit, you might be allowed to dial a combination of an IP address or domain name and E.164 number or extension. Depending on the configuration of your unit, dialing a combination of an IP address and E.164 number (or extension) might connect you to the auto attendant or the operator (for more information refer to Using the auto attendant and Dialing the operator, below); it could also connect you directly to an endpoint, a video conference or to another service on the network.

- **SIP**: On SIP phones to dial a combination of IP address/domain name and E.164 number or extension, you will use the following syntax:
  <xxxx>@<IP address/domain name of IP gateway>
  For example, to dial 4545 on a IP gateway with an IP address of 10.10.10.12, you will dial:
  4545@10.10.10.12
- **Cisco TelePresence endpoints (H.323 and SIP)**: Certain Cisco TelePresence endpoints allow you to use the SIP format to dial a combination of IP address/domain name and E.164 number. You will use the following syntax:
  <xxxx>@<IP address/domain name of IP gateway>
  For example, to dial 4545 on an IP gateway with an IP address of 10.10.10.12, you will dial:
  4545@10.10.10.12
- **H.323**: See your endpoint documentation for information about how to dial a combination of E.164 number and IP address/domain name. On some endpoints, you can use the following syntax:
  <IP address/domain name >##<number>
  For example, to dial 4545 on a IP gateway with a domain name of operator.uk.example.com, you

will dial:
operator.uk.example.com##4545

Using the auto attendant

Depending on the configuration of your unit, when you connect to the IP gateway you might see an on screen menu known as an auto attendant. An auto attendant can present you with a series of options. These options could include the ability to dial a number, view a video, make a selection from an address book, and speak to an operator.

You can use either Far-End Camera Control (FECC) or Dual Tone Multi Frequency (DTMF) tones to navigate the auto attendant. DTMF is the default mechanism for navigating the auto attendant; to enable FECC, refer to your endpoint's documentation.

Use the navigation keys to scroll through menu options:

- for FECC, enable FECC on your endpoint and use the up, down, left, and right keys
- for DTMF tones, use the number key that corresponds to the menu item you require

Dialing in the auto attendant

Depending on the configuration of your unit (see above), you might be allowed to dial E.164 numbers and IP addresses in an auto attendant menu.

You can dial an IP address (in the format 10*12*123*34) or an E.164 number using your number keypad. Press # to go to the next page. The available options on the next page will depend on the configuration of the IP gateway; you might have to select the protocol to cause the unit to dial the number (talk to your administrator about this) or simply select Call. Pressing 1 will enable you to redial.

If you are allowed to dial IP addresses with extensions, you can dial extensions in the following way: enter the IP address (replacing dots with stars), and append the IP address with two stars (asterisks) followed by the extension number. Then press # to get to the next page as explained above.

For example to to dial extension 654 on 10.2.11.12, dial:

10*2*11*12**654#

Note that in this way, you might also be able to connect to conferences on an MCU. For example by dialing the IP address of the MCU followed by the ID of a conference on that MCU. For example to dial into conference with ID: 1234 on MCU with IP address: 10.12.136.12, dial:

10*12*136*12**1234#

Using the auto attendant from an audio-only phone

When you dial the auto attendant from an audio-only IP phone, if your administrator has configured the IP gateway to provide audio prompts, you will hear the audio-prompts:

- If you know the extension you require, dial the numbers and press # (pound/hash key)
- If you want to be transferred to the operator, press * (star/asterisk key)

Clearly, you will not be able to select from any of the other options that the same auto attendant offers to audio-visual endpoints (that is, you will not be able to select from the directory of endpoints that might be displayed on the auto attendant).

Using an address book

When you choose to use an address book as a method for finding the person to whom you want to speak, you will use the number keypad (or Far End Camera Control) to select from the available entries. Where there are multiple entries on multiple pages, use the following keypad controls to navigate around the address book:

- # (hash pound) to go to the next page
- * (star/asterisk) to return to the previous page
- 0 (zero) to return to the top of the address book menu

To search in an address book:

1. Use the number keypad to select the address book you require.
2. Press 1 to search the address book:
    - You can search the address book using 'multi-tap text entry mode'. This means that you must press a key multiple times to access the list of letters on that key. For instance, pressing the"2" key once displays an "a", twice displays a "b", and three times displays a "c". To enter a space, use the '1' key. Multi-tap text entry mode is the default method for searching an address book
    - You can also use 'predictive text entry mode'. This means that for each letter in the name for which you are searching, you simply press the number corresponding to the letter and, as long as the name exists in the address book, the IP gateway will find the entry. When using predictive text entry mode, you must leave out any punctuation and spaces; for example, John Smith is 564676484
3. When you have found the address book entry that you want, press 0 to access DTMF selection mode and then press the number that corresponds to the option you require.

Dialing the operator

Depending on the configuration of the unit, there might be an operator with whom you can talk. The operator has the ability to transfer your call for you. There may be a quick-dial route to connecting to the operator and the operator might be an option on a menu.

Using playback controls when you are watching a video on the IP gateway

Depending on the configuration of the unit, you might be able to choose a video to watch.

When a video is playing in full-screen mode, you can use your endpoint's number pad to control the play back as follows:

- Press 6 to fast forward (note that the video will appear as a still while the fast-forward icon is flashing). Press 6 again to resume play back
- Press 4 to rewind (note that the video will appear as a still while the rewind icon is flashing). Press 4 again to resume play back
- Press # to pause the video. Press # again to resume playback
- Press 0 to return to the auto attendant menu

Configuring network settings

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

The IP gateway has two Ethernet interfaces, *Port A* and *Port B*. The configuration pages for the two interfaces look and behave similarly, and so are described together.

Both Port A and Port B can be configured to be allocated its IP address by DHCP. Connect Port A to your local network and connect Port B to a second subnet or the internet depending on your application of the IP gateway.

In this section:

IP configuration settings

These settings determine the IP configuration for the appropriate Ethernet port of the Cisco TelePresence IP Gateway. When you have finished, click **Update IP configuration** and then reboot the IP 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 IP gateway obtains its own IP address for this port automatically via DHCP. If set to *Manual* the IP gateway uses 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 IP 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 selected *Manual* IP configuration, as described above. If IP configuration is set to *Automatic by DHCP* this setting is 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.	

IP status

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

- DHCP
- IP address
- Subnet mask
- Default gateway

Ethernet configuration

These settings determine the Ethernet settings for the appropriate port of the Cisco TelePresence IP Gateway. 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 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. You only need to select this option if you have 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 IP 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 IP gateway. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the unit is transmitting packets into the network.
Packets received	Displays a count of the total number of packets received by this port of the IP gateway. This includes all TCP and UDP traffic.	When troubleshooting connectivity issues, this information can help you confirm that the unit 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 Cisco TelePresence IP Gateway. It is important that these settings are configured correctly, or you may be unable to make calls or to access the web interface.

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

In this section:

Port preferences

If both Ethernet ports are enabled, you need to specify which port is used in certain special circumstances. Make the appropriate selection as described below and then click **Apply changes**.

Field	Field description	Usage tips
IPv4 gateway preference	The IPv4 address to which the IP gateway will send packets in the absence of more specific routing (see IP routes configuration). Therefore, it only makes sense to have precisely one default gateway, even though *different* default gateways may have been configured for Ports A and B. Use this option to decide which port's default gateway configuration to use as the IP gateway's default gateway.	If Ethernet Port B is disabled, you cannot specify that port as the default gateway preference. Selecting Port B as default gateway preference and then disabling Port B will cause the preference to revert to Port A.

IP routes configuration

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

Adding a new IP route

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

The maximum number of routes that can be added manually is 128.

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 dot-separated IPv4 format. 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	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.

	set to zero in the address specified.	
Route	Use this field to control how packets destined for addresses matching the specified pattern are routed.	You may select *Port A*, *Port B* or *Gateway*. If *Gateway* is selected, specify the IP address of the gateway to which you want packets to be directed. Selecting *Port A* or *Port B* causes matching packets to be routed to the default gateway for Port A or Port B respectively (Configuring network settings explains how to specify default gateways). If Ethernet Port B is disabled, the *Port B* route option is unavailable.

Viewing and deleting existing IP routes

Configured routes are listed below the **Add IP route** controls. 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
  - Port B - meaning the default gateway configured for Port B
  - **<**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 checkbox and clicking **Delete selected**.

Packets are not re-routed from disabled ports

If you disable a port, be aware that any packets that attempt to route to that port will be discarded. The gateway does not re-route them to an alternative port. This applies whether the packets are routed to the port manually (through a specific route configuration) or automatically (no specific route is configured and the port in question is defined as the default gateway).

You should take care to avoid this situation.

DNS settings

To configure DNS settings on the IP gateway and to view DNS status, go to **Network > DNS**.

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

Field	Field description	Usage tips
DNS configuration		
DNS configuration	Select a port and DHCP combination from the list or select *Manual* to specify DNS settings manually. If you select *Manual*, all DNS settings are as configured on this page.	If you select a DHCP setting, no DNS name server will be used until the value to use is received via DHCP on that interface. For example, if you select *Via Port A DHCPv4* as the DNS setting, then you must configure Port A to use DHCP by setting the IP configuration field for Port A in the IPv4 section of the Port A IP configuration page (**Network > Port A**) to *Automatic via DHCP*. If the DHCP server on your network does not supply DNS configuration information, then the gateway will have no ability to look up names.
Host name	Specifies a name for the gateway.	Depending on your network configuration, you may be able to use this host name to communicate with the IP gateway, without needing to know its IP address.
Name server	The IP address of the name server.	
Secondary name server	Identifies an optional second name server.	The secondary DNS server is only used if the first is unavailable. If the first server returns that it does not know an address, the secondary DNS server will not be queried.
Domain name (DNS suffix)	Specifies an optional suffix to add when performing DNS lookups.	This option 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 look up *endpoint.cisco.com*.

DNS status

Use the DNS status fields on this page to view the current DNS settings for the IP gateway.

Configuring IP services

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

Use this page to control the type of services that may be accessed via Ethernet Ports A and B. For example, if one Ethernet port is connected to a network outside your organization's firewall, and you want to restrict the level of access that external users are entitled to, for example, by disabling FTP access via Port B. Refer to the table below for more details.

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

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.

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 specified interface or change the port that is used for this service.	Web access is required to view and change the Cisco TelePresence IP Gateway web pages and read online help files. If you disable web access on both Ports A and B 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 IP gateway has the *Secure management (HTTPS)* feature key or an *Encryption* feature key installed. For more information about installing feature keys, refer to Upgrading the firmware. By default, the IP 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 H.323	Enable/disable the ability to receive incoming calls to the IP gateway using H.323 or change the port that is used for this service.	Disabling this option will not prevent outgoing calls to H.323 devices being made by the IP gateway.
Incoming SIP (TCP)	Allow/reject incoming calls to the IP 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 IP gateway.

Field	Field description	Usage tips
Incoming Encrypted SIP (TLS)	Allow/reject incoming encrypted SIP calls to the IP 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 IP gateway. That is, outgoing connections from the IP gateway can use SIP over TLS, depending on the SIP settings and the SIP registrar settings. For more information, refer to Configuring SIP settings and Configuring SIP registrar settings 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 IP gateway configuration. 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		
SIP (UDP)	Allow/reject incoming and outgoing calls to the IP 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.
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.
H.323 gatekeeper	Enable/disable access to the built-in H.323 gatekeeper or change the port that is used for the built-in H.323 gatekeeper.	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 SNMP settings

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

The Cisco TelePresence IP 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 IP gateway (and therefore will differ from the *Uptime* reported by the IP gateway on the **Status** > **General** page).
- The SNMP MIBs are read-only.

System information

Field	Field description	Usage tips
Name	Identifies the IP gateway in the SNMP system MIB.	Usually you would give every device a unique name. The default setting is: IP GW
Location	The location that appears in the system MIB.	An optional field. Where you have more than one IP gateway, it is useful to identify where the IP gateway 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 IP gateway's model number. Can be used to provide more information on the IP gateway.

Configured trap receivers

Field	Field description	Usage tips
Enable traps	Select this check box to enable the IP 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

Field	Field description	Usage tips
		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 IP 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 Cisco TelePresence IP 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 and SIP endpoints. All other packets are sent with a QoS of 0.

The IP 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 IP 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 IP 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 IP 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**.

Configuring security settings

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

Field	Field Description
Security settings	
Hash stored passwords	Enable this option if you want the IP gateway to hash passwords before storing them in the configuration.xml file. If you do not choose to hash stored passwords be aware that all user passwords are stored in plain text in the configuration file, which might be a security issue. Note that hashing user passwords is an irreversible process.
Redirect HTTP requests to HTTPS	Enable this option if you want HTTP requests to the IP gateway to be redirected automatically to HTTPS. This option is unavailable if either HTTP (*Web*) or HTTPS (*Secure web*) access is disabled on the **Network > Services** page.

Displaying and resetting system time

The system date and time for the Cisco TelePresence IP 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 IP gateway supports the NTP protocol. Configure the settings using the table below for help, and then click **Update NTP settings**.

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

If there is a firewall between the IP 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 IP gateway will automatically use the appropriate port to communicate with the NTP server. If the NTP server is not local, the IP 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 IP 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 IP 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 IP gateway and the NTP server, with the IP gateway on the NAT's local network (and not the NTP server), no extra configuration is required.

If NAT is used between the IP 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.

Upgrading and backing up the IP gateway

If you need to upgrade the firmware or activate features on the Cisco TelePresence IP Gateway, refer to these topics:

CAUTION: You must always back up your configuration (the configuration.xml file) before you upgrade the software. If you use Call Detail Records (CDR) for billing, auditing, or any other purpose, you must also download and save your current CDR data. Some software releases will reformat the configuration file in a way that is not compatible with earlier software versions, and in some cases downgrading back to a previous version will destroy existing CDR records.

Upgrading the main IP gateway software image

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

To upgrade the main IP gateway software image:

1. Go to **Settings > 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 IP gateway web browser interface.
7. Go to **Settings > Upgrade**.
8. Click **Browse** to locate the unzipped file on your hard drive.
9. Click **Upload software image**. The browser begins uploading the file to the IP 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."
10. The upgrade status displays in the IP gateway *software upgrade status* field.
11. Shutting down and restarting the IP 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 IP 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 IP gateway.

Backing up and restoring the configuration

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

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

To restore configuration at a later date, locate a previously-saved "configuration.xml" file and click **Restore backup file**. When restoring a new configuration file to an IP 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 if you were restoring from a file backed up from the same IP gateway or if you were intending to replace an out of service IP gateway. If you copy the network settings from a different, active, IP 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 do not select **Network settings**, the restore operation will not overwrite the existing network settings, with the one exception of the QoS settings. QoS settings are overwritten regardless of the **Network settings** 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.

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

Enabling IP gateway features

The IP gateway requires activation before most of its features can be used. (If the IP 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 IP gateway you should receive the IP 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 IP gateway so ensure you know the IP gateway's serial number such that you may receive a code appropriate to your IP gateway.

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

To activate the IP gateway or enable an advanced feature:

1. Check the *Activated features* (IP 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. It is recommended that you record the activation code in case you need to re-enter it in the future.

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

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

Shutting down and restarting the IP gateway

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

Shutting down the IP gateway will disconnect all active calls.

To shut down the IP gateway:

1. Go to **Settings > Shutdown**.
2. Click **Shut down IP gateway**.
3. Confirmation of shutdown is required; the button changes to **Confirm IP gateway shutdown**.
4. Click again to confirm.
5. The IP 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 IP gateway**.
6. Click this button a final time to restart the IP gateway.

Displaying general status

The General Status displays an overview of the Cisco TelePresence IP Gateway status. To access this information, go to **Status > General.**

Refer to the table below for details of the information displayed

Field	Field Description
System status	
Model	The specific Cisco TelePresence IP Gateway model.
Serial number	The unique serial number of the Cisco TelePresence IP Gateway.
Software version	The installed software version. You will need to provide this information when speaking to Customer support.
Build	The build version of installed software. You will need to provide this information when speaking to Customer support.
Uptime	The time since the last restart of the gateway.
Host name	The host name assigned to the gateway.
Slot number in chassis (8350 only)	The slot number in the chassis in which the Cisco TelePresence IP Gateway is currently installed. If the gateway displays a message reporting that the blade is missing, ensure that each blade is firmly secured in the chassis. Close both retaining latches on the front of the blade. Using a number 1 Phillips screwdriver, tighten the screws in the retaining latches with a clockwise quarter turn.
IP address	The IP address assigned to the gateway.
CPU load	The current processor utilization of the gateway.
Media processing load	An overview of the current media loading of the gateway.
Current time	The system time on the gateway. Click **New time** to modify this value. The **Time Settings** page opens in which you can update the system date and time manually or refresh the time from an NTP server. For more information about the **Time Settings** page, refer to Displaying and resetting system time.
System log	
• User requested shutdown • User requested upgrade • Unknown	The system log displays the last eight shutdown and upgrade events in date order with the most recent system log event at the top of the list. The log will also display "unknown" if there has been an unexpected reboot or power failure, which you should report to Technical support if it happens repeatedly.

Displaying call status

The Call Status displays an overview of current calls on the Cisco TelePresence IP Gateway. To access this information, go to **Status > Calls.**

Refer to the table below for details of the information displayed

Format of displayed values

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

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

For the IP GW 8350 blade, the maximum value (**C** above) for the "ports in use" fields depends on the number of port licenses allocated to the IP gateway.

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

Where the highest value attained is shown in parentheses (**B** in the above example), this value can be reset by selecting Reset maximum values. These values can be useful in monitoring peak IP gateway usage over a period of time.

Field	Field description
Call status	
Through calls	The number of calls currently connected to their final destination. This number does not include calls that are currently with the operator or the auto attendant.
Auto attendant connections	The number of calls currently connected to the auto attendant.
Operator connections	The number of calls currently connected to the operator.
Queued for operator	The number of calls currently in the queue for the operator.
Video ports in use	The number of video ports in use. This corresponds to the number of calls that are either sending or receiving video.
Audio-only ports in use	The number of audio-only ports in use. This corresponds to the number of calls that are either sending or receiving audio but not video.
Video status	
Incoming video	The number of video streams currently being received by the IP gateway.

Field	Field description
streams	
Outgoing video streams	The number of video streams currently being sent by the IP gateway.
Total incoming video bandwidth	The total video data rate being received by the IP gateway.
Total outgoing video bandwidth	The total video data rate being sent by the IP gateway.
Audio status	
Incoming audio streams	The number of audio streams being received by the IP gateway.
Outgoing audio streams	The number of audio streams being sent by the IP gateway.

Displaying hardware health status

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

Note: The **Worst status seen** conditions are those since the last time the IP 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 (3500 only) **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 IP 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 IP 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.

Working with the event logs

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

Event log

The last 2000 status messages generated by the IP gateway are displayed in the Event log page (**Logs > Event log**). In general these messages are provided for information, and occasionally Warnings or Errors may be shown in the Event log. The presence of such messages is not cause for concern necessarily; if you are experiencing a specific problem with the operation or performance of the IP gateway, Cisco customer support can interpret logged messages and their significance for you.

You can:

- Display the log as text by going to **Logs > Event log** and clicking **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 (see Logging using syslog).
- Empty the log by clicking **Clear log**.
- 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).

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 IP 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.

Logging using syslog

You can send the Event log to one or more syslog servers on the network for storage or analysis.

To configure the syslog facility, go to **Logs > Syslog**

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

Working with Call Detail Records

The Cisco TelePresence IP Gateway can display up to 20 pages of Call Detail Records. However, the IP 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 **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. When you enable logging, the IP gateway writes the CDRs to the compact flash card.	Enabling or disabling CDR logging has immediate effect. There is no need to press **Update display** after clicking one of these buttons. Ensure there is a compact flash card available - either in the slot on the front of the IP gateway or internally.
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 checked.

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

To clear the CDR log, click **Delete X to Y**. This will permanently remove Call Detail Records X to Y. Due to the way the CDR log works, it may not be possible to delete all records; the button name indicates which records can be deleted. For example, if you delete the 0-399 entries, then the 400th entry appears as the first entry in this page, even if you download the full log. The download button would then show that you can download for example 400-674 (if 674 is the maximum number of entries in the log) and the **Delete** button will be 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.	Records are created as different connection events occur. The time the record was created is the time that the event occurred.
Connections	The number of the connection to which this record applies	Each new connection is created with a unique numeric index. All records pertaining to a particular connection display the same connection number. This can make auditing connection events much simpler.
Message	The type of the Call Detail Record, and brief	The display settings allow you to display

Field	Field description	Usage tips
	details, if available.	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

Logging H.323 or SIP messages

The H.323/SIP log page records every H.323 and SIP message received or transmitted from the IP gateway.

By default the H.323/SIP log is disabled because it affects performance. However, Cisco customer support may ask you to enable it if there is a problem with an IP gateway in your network. To do this, click **Enable H323/SIP logging**.

Optionally the log can be exported in an .xml file. To do this, click **Download as XML**.

When you are satisfied that the issue is resolved, you should disable H323/SIP logging and then clear the H323/SIP log (click **Clear log**) to avoid impacting the performance of the unit in future.

Backing up and restoring the configuration using FTP

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

To back up the configuration via FTP:

1. Ensure that the FTP service is enabled on the **Network > Services** page.
2. Connect to the IP 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 IP gateway's web interface as an administrator.
   You will see a file called configuration.xml. This contains the complete configuration of your IP 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 IP gateway using an FTP client. When asked for a user name and password, use the same ones that use to log in to the unit's web interface as an administrator.
4. Upload your configuration.xml file to the IP gateway, overwriting the existing file on the IP gateway.

The restore process is now complete.

Note: that the same process can be used to transfer a configuration from one 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 IP gateway, for example in a network where you have more than one IP gateway, be aware that if the original IP gateway was configured with a static address, you will need to reconfigure the IP address on any other unit or blade on which you have used the configuration file.

Using encryption with the IP gateway

To use encryption, you must have the Encryption feature key present on the Cisco TelePresence IP Gateway. For information about installing feature keys, refer to Upgrading the firmware. If you have the encryption feature key installed, you can configure the IP gateway to encrypt calls and to accept encrypted calls.

The encryption technology that the IP gateway uses for encryption to and from H.323 endpoints is Advanced Encryption Standard (AES). Where encryption is used for H.323 calls, the IP gateway encrypts and decrypts all the media to and from the H.323 endpoint

The encryption technology that the IP gateway uses for encryption to and from SIP endpoints is Secure Real-time Transport Protocol (SRTP). When encryption is in use to and from SIP endpoints, the IP gateway will encrypt audio and video media using SRTP. Control or authentication information can also be encrypted using TLS. For more information refer to Using encryption with SIP, below.

Encryption is used where both devices in a call agree to use encryption; by default if one of the devices cannot use encryption (for example if a SIP endpoint does not support SRTP), the IP gateway will allow the call to be unencrypted, unless you have configured the IP gateway to *require* encyrption. Where encryption is required, calls that cannot used encryption will not be allowed.

Enabling encryption on the IP gateway

To enable encryption:

1. Go to **Settings > Calls**.
2. For *Encryption status*, select one of:
   - *Optional*: Encryption will be used if one of the endpoints in the call requires it. Where both endpoints are also set to encryption optional, whether or not encryption will be used is decided by the endpoints. In transcoded calls, it is possible for one part of the call to be encrypted and the other part not to be encrypted; in a non-transcoded call, encryption is either used for both parts of the call or not at all
   - *Required*: Encryption must be used by both parts of the call (that is, by both endpoints in the calls)
3. Click **Apply changes**.

Using encryption with SIP

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

Using TLS for call setup is not sufficient for the call to be considered encrypted such that it will be allowed if the IP gateway requires encryption. Where encryption is required for calls, a SIP call must use SRTP.

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

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

Customizing the user interface

In this section:

The Cisco TelePresence IP Gateway provides you with options for customizing the voice prompts, the text prompts in the auto attendant menus, and the text of the welcome messages.

Note: the user interface (that is the text you see on the web interface of the IP gateway) can be localized by us or by your reseller. This type of customization is the localization of the text on the web interface and these online help pages. That is, the text has been translated into your local language. In the case where you have a localized IP gateway, the Use localization package check box will be selected. For more information refer to **Customization: more information**.

Some localization packages are available on the company FTP site.

The IP gateway allows you to type using any character set when entering text into the web interface. For example, when naming endpoints or users, you can use any character set you require.

Configuring welcome messages for the Login and Home pages

You can configure a message banner to appear on the Login page of the IP gateway. For example, some organizations might require some legal text on the Login page. You can also configure a message banner to appear on the Home page. You can configure a separate title (maximum: 100 characters) and text (maximum: 1500 characters) for each banner. To configure the message banners:

1. Go to **Settings > User interface**.
2. In the **Welcome messages** section, enter the text you require for the titles and the text of the messages.

Customizing voice prompts on the IP gateway

By default the IP gateway includes English voice prompts spoken by an American woman.

These prompts are used by the IP gateway to provide callers with information, for example: "Connecting you to your destination".

You may want to replace these prompts with your own in order to change the wording, language or accent used. Alternative prompts may be uploaded individually using the web interface. Alternatively, a collection of voice prompts may be uploaded in one go by means of a *resource package* (see Uploading a customization package).

Some customization packages are available on the company FTP site.

On the IP gateway, you can also record up to ten more voice prompts for use with the auto attendant menus you create. This customization page tells you how to make the best recordings and how to upload them to a unit. For more information about creating auto attendant menus, refer to Creating auto attendant menus.

The customization of voice prompts is controlled via the web interface. Go to **Settings > User interface**. Refer to the sections below for details of the options available and for a description of the information displayed:

- Viewing the available voice prompts
- Uploading and downloading customized voice prompts
- Voice prompt specification
- Making the best possible recordings

Using default US English voice prompts

The default set of voice prompts is provided in US English and is the standard set of voice prompts supplied with the IP gateway. These are spoken by a female voice in Americanized English.

If your IP gateway is using customized voice prompts and you want to return to using the default set of voice prompts:

1. Go to **Settings > User interface**.
2. If your IP gateway was provided to you as a localized IP gateway, clear **Use localization package**.
3. Click **Apply changes**.

The default voice prompts will be applied immediately, although it may take a few seconds before everyone connected to the IP gateway is able to hear the new prompts.

Uploading a customization package

It is possible to upload a collection of alternative voice prompts to the Cisco TelePresence IP Gateway with a single upload operation, using a *customization package*. Such a package may have been supplied to you by Cisco or one of its representatives, or you may have created the package yourself (see Downloading a customization package).

To upload a package:

1. Go to **Settings > User interface**.
2. In the **Upload customization package** section, click **Browse** and locate the *.package* file on your computer.
3. Click **Upload package**.

The upload may take several seconds, depending on the size of the package file and the speed of your network connection. When the upload is complete, a status screen will be shown, displaying some or all of the individual voice prompt customizations included in the package if the upload was a success, or an error message if the upload failed for some reason.

Note: If you were already using uploaded alternative voice prompts on the IP gateway, then these will be immediately replaced by those in the customization package. If a particular customized file is not included in the package, then any existing customization is unchanged. This allows customization sets to be built up using several different packages if required.

Viewing the available voice prompts

You may review the voice prompt customizations available in the table headed **Voice prompts**. The **Voice prompts** list displays all voice prompt customizations, providing details for those which have alternatives uploaded. Because these lists can be quite long, by default they are hidden. Instead, the number of customizations (files) available is shown. If any have been modified (meaning an alternative customization has been uploaded, either individually, or as part of a package), then this is indicated by an asterisk after the table name.

To expand any list to show all customizations, click **show file details**; you may subsequently hide it again by clicking **hide file details**.

In the expanded state, the table shows, for each customization, a description of the file, the standard IP gateway filename for the customization, and the length and date modified (uploaded) of alternative customizations present. Extra information is provided by the following symbols:

- Customizations where an alternative is available that can be individually uploaded or downloaded are indicated by two asterisks (**) after their name
- Customizations where an alternative is available that cannot be uploaded or downloaded individually are indicated by one asterisk (*) (these are files that have been provided by Customer support)
- Customizations that are part of a localization package from Cisco or your reseller are indicated by a plus sign (+)

Uploading and downloading customized voice prompts

Refer to the sections below for details of further functionality provided by the **Installed voice prompts** list:

- Uploading individual voice prompts
- Downloading individual voice prompts
- Downloading a customization package
- Deleting customized voice prompts

Uploading individual voice prompts

You may upload individual voice prompts. To do this:

1. Go to Settings > User interface.
2. In the Installed voice prompts section, click show files details and locate the voice prompt file you require.
3. For that voice prompt, click upload. You may do this regardless of whether an alternative customization has already been uploaded.
4. You will be presented with a new screen, allowing you to locate and upload the customization of your choice. Click Browse to locate the voice prompt file on your computer. Voice prompt files must be in the following format:
    - Microsoft WAVE (.WAV) format
    - 16kHz (16000Hz) sample rate
    - Mono
    - Uncompressed
    - Maximum 10 seconds long

    If you upload a file that is not in this format, the upload may fail or the voice prompt may sound distorted when heard by users. Use an audio editing package of your choice to make any conversions required. See Making the best possible recordings for how to obtain the best possible voice prompts for your IP gateway customization.

    Note that in addition to the 10 second length limit per prompt, there is a total length limit of four minutes for the full set of prompts. That is, if all samples were played back-to-back, it should take no more than 240 seconds.
5. When you have located the file you want to upload, click Upload customization. If the upload is successful, a page displaying the size of the file uploaded will be displayed; otherwise an error will be shown. If the upload fails, check that your audio file matches the specification above before contacting your support representative.

On the IP gateway when you upload a voice prompt, the IP gateway will start using the new voice prompt immediately.

Downloading individual voice prompts

You may wish to review a customization that has been previously uploaded to the IP gateway. To do this,

1. Go to **Settings > User interface**.
2. In the **Installed voice prompts** section, locate the voice prompt file you require.
3. For that voice prompt, right-click **download** and choose **Save Target As** (or your web browser's equivalent operation). The file will be downloaded to your computer for reference.

Only alternative customizations can be downloaded in this way; the default voice prompts may not be downloaded. In addition, only customizations uploaded as individual files may be downloaded; those uploaded as part of a package may not be downloaded.

Downloading a customization package

Once you are satisfied with your customizations, you may want to apply the entire set to another IP gateway. Rather than individually uploading the alternative voice prompts to each one, you may create a *customization package*.

To create a customization package containing all of the alternative voice prompts previously uploaded:

1. Go to **Settings > User interface**.
2. Click **Download package** at the bottom of the **Installed voice prompts** list. The customization package will be downloaded to your computer.

A package may only contain resources uploaded as separate files; those uploaded as part of another package may not be included. The package download option may be unavailable if no voice prompts qualify for inclusion.

Deleting customized voice prompts

If you are dissatisfied with a voice prompt that you have uploaded to the IP gateway, you may delete it in the following manner:

1. Locate the voice prompt of interest in the list.
2. Click the check box to the left of the voice prompt.
3. Click **Delete selected** to remove the voice prompt.

Only alternative voice prompts may be deleted in this way; the default voice prompts cannot be deleted. If you delete an alternative customization, it will immediately revert to the default prompt.

You may want to delete all customizations. To do this, click **Delete all**. Remember that you may revert to the default set of voice prompts without needing to delete any alternative customizations (see Using default voice prompts).

Voice prompt specification

Below is a complete list of the voice prompts that may be customized. The default wording is shown for each prompt. You do not have to use exactly the same wordings if they are not appropriate for your needs, and are provided only as a guide.

Filename	Default wording
voice_prompt_connecting_you	Connecting you to your destination
voice_prompt_in_queue	Thank you for waiting. The operator will answer the call as soon as possible
voice_prompt_connect_to_operator	Connecting you to the operator
voice_prompt_could_not_connect	Sorry, we could not connect your call
voice_prompt_receiver_busy	Destination busy
voice_prompt_no_answer	Your call was not answered
voice_prompt_operator_unavailable	Sorry, the operator is unavailable
voice_prompt_goodbye	Goodbye
voice_prompt_enter_queue	The operator will answer the call as soon as possible
voice_prompt_dial	Enter the number followed by the pound key
voice_prompt_user_1 to voice_prompt_user_10	You can upload up to ten voice prompts of your own creation onto the IP gateway. These voice prompts can each be up to 10 seconds in duration. To upload and manage local voice prompts, go to **Settings > User interface**. The topic Customizing the user interface describes how to record and upload these additional voice prompts. For more information about using voice prompts in auto attendant menus, refer to Creating auto attendant menus

Making the best possible recordings

There are many factors to consider when recording alternative voice prompts in order to get the best results. Below is a summary of the points to bear in mind.

Recording format

It is best to make each recording with the ideal settings and hence avoid any sample-rate or resolution changes. As discussed, the ideal format is Microsoft Wave (.WAV) format, uncompressed, mono, at 16 kHz and 16-bit resolution.

If you are unable to make mono recordings, the IP gateway can convert stereo recordings.

Background noise

It is important to minimize background noise (hiss) as much as possible. This includes ambient noises such as road noise and slamming doors etc. but also try to keep fan noise and similar to a minimum.

When played back by the IP gateway, samples with background noise are very apparent.

Consistency

If possible, record all voice prompts in one session. This will ensure that all voice and background conditions remain constant and the recorded voice will sound similar from prompt to prompt.

Volume

Record prompts using a relatively constant loudness of voice. Although it may take some trial and error, the best recordings will result from speaking loud enough that the voice is recorded loudly compared to any residual background noise, but not so loudly that it sounds distorted when played back.

Customizing text prompts on the IP gateway

By default the Cisco TelePresence IP Gateway includes a number of text prompts that appear on the auto attendant menus (the interface a caller sees on their endpoint).

These prompts are used by the IP gateway to provide callers with information, for example: "Back" "Cancel".

You may want to replace these text prompts with your own in order to change the wording or language used. The text prompts are all contained in one text file which you can edit. This text file supports the use of UTF8 characters.

To customize the text prompts:

1. Go to **Settings > User interface**.
2. In the **Installed customizations** section, click **show file details**.
3. Click **Download default** to download the text file that comprises the text prompts.
4. Edit the file to use the language or wording you require. Note, do not edit the numbers and the colons that appear at the beginning of each line. Also, do not insert any line breaks into this file.
5. On the **Settings > User interface** page, click **upload** to upload your text file. The IP gateway will immediately use the customized text prompts.

Customization: More information

There are three customization levels on the Cisco TelePresence IP Gateway (for voice-prompts, web interface, help pages, and text messages):

- the factory default files that are provided in US English
- localization files that are sometimes installed by a reseller
- customized voice prompts files that can be uploaded and downloaded by you

Precedence

For every customizable file:

1. If there is a customization file present, that file will be used.
2. Otherwise, if **Use localization package** is checked, the unit will use the localized file.
3. If 1 and 2 are not true, then the IP gateway will use the default US English file.

The factory default file set

The files that compose the default file set for the web interface, the voice prompts, the text prompts, the help pages, and text messages cannot be deleted. If you are using your own customization files or a localized IP gateway you can return the IP gateway to using the default file set:

To return to the defaults:

1. Go to **Settings > User interface**.
2. Ensure **Use localization package** is unchecked.
3. Delete any customized voice prompts.
4. If there is a customized text prompt file, delete it.

Localization files

In some parts of the world, IP gateways are available where the help pages, the voice prompts, the text messages, and some of the web interface are in the local language. In this case, Cisco or the reseller has uploaded a package that provides localized files to replace files in the default file set. If you have a localized IP gateway, you are able to select to return to the default US English file set (see above). Localization is a global change and affects all customizable files. If you have a localized IP gateway, you cannot upload and download localized files on a file by file basis.

Some Cisco customization packages are available on the company FTP site.

Customization files

Customization files for voice prompts can be recorded and uploaded by any admin user of the IP gateway. These files can be uploaded one by one or as a package. You can create your own package by uploading all the files you require to an IP gateway and then downloading them as a package. For more information, refer to Customizing the user interface. A customization package does not have to include a complete set of files. Where a file name duplicates an existing uploaded voice prompt file, that file will be overwritten.

Network connectivity testing

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

The Network connectivity page enables you to attempt to 'ping' another device from the IP 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 IP gateway and another device. You can see from which port the IP 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 IP 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 IP 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 IP 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 IP gateway and therefore these hosts' entries are also shown as <unknown>.

Note: The ping message is sent from the IP gateway to the IP address of the endpoint that you enter. Therefore, if the 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 IP gateway's IP routing configuration to be tested, and it has no security implications.

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

Configuring SSL certificates

If the Cisco TelePresence IP 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 IP gateway using HTTPS. The IP 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 IP 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 IP 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 IP gateway. The private key is used by the IP 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		

Field	Field description	Usage tips
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 IP 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.	
Trust store	You can upload a trust store of master certificates that the IP gateway will use to verify the identity of a certificate presented by the other end of a Transport Layer Security (TLS) connection. The trust store must be in '.pem' format. To delete a trust store certificate from the IP gateway, click the **Delete trust store** button.	Uploading a new trust store replaces the existing store.
Certificate verification	Choose to what extent the IP gateway will verify the identity of the far end for a	Outgoing connections are connections such

Field	Field description	Usage tips
settings	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 IP gateway will not allow the connection to proceed.	as SIP calls which use TLS.

Further information

Details of software licenses relating to this product are available in the online help.