# Cisco TelePresence IP Gateway Version 2.0(3.34)

## Software Maintenance Release Notes
## May 2014

## Contents



Version 2.0(3.34) is a maintenance software release for the following Cisco TelePresence IP Gateway products:

- IP GW 3510
- IP GW 3520
- IP GW 3540
- IP GW MSE 8350

For clarity in this document, the generic term “IP gateway” is used except where a particular product is referenced.

## Product documentation

The following documents provide guidance on product installation, configuration, and operation:

- *Cisco TelePresence IP GW 3500 Series Getting Started*
- *Cisco TelePresence IP GW MSE 8350 Getting Started*
- *Cisco TelePresence IP Gateway Remote Management API Reference Guide*
- *Cisco TelePresence IP Gateway Online Help* (printable format)

All product documentation can be found on Cisco.com.

# Changes in Version 2.0(3.32)

## User interface changes

Version 2.0(3.32) includes changes to the IP gateway web user interface:

- DNS settings are on a new **Network > DNS** page (moved from **Network > Port A / Port B**).
- Security settings are on a new **Settings > Security** page (moved from **Settings > Upgrade**).
- An optional setting to redirect HTTP requests to HTTPS is now available (**Settings > Security**).
- The **Events** page is now known as the **Logs** page.
- It is now possible to delete a trust store (**Network > SSL certificates**).
- The IP gateway configuration can be backed up and restored via the web interface (**Settings > Upgrade**).
- The IP gateway now uses session-based user authentication (see next section).

## Session-based user authentication

This release also implements session-based user authentication on the IP gateway. The gateway no longer uses digest-based authentication and therefore is less secure if you are using HTTP. Some third-party tools may stop working as a result. We recommend that you use HTTPS to protect user names and passwords (the **Encryption** feature key is required for HTTPS).

**Note: Automatic transcoding of Cisco VCS interworked calls**

In this release the IP gateway will automatically transcode calls that have been interworked through a Cisco TelePresence Video Communication Server (Cisco VCS). This change is only relevant to IP gateways that include the **Allow non-transcoded calls** option (**Settings > Calls** page). In previous releases, if this option was enabled, a Cisco VCS interworked call might end up non-transcoded, which could potentially cause interoperability issues. In this release, the IP gateway will transcode all Cisco VCS interworked calls, even when configured to allow non-transcoded calls.

Each transcoded call uses one media port.

# New features in Version 2.0(1.7)

## HTTPS access for TMS

Release 2.0(1.7) introduces support for HTTPS access for the Cisco TelePresence Management Suite (Cisco TMS). When this option is enabled the IP gateway will use HTTPS to access the address book on the Cisco TMS, otherwise it will use an unencrypted HTTP connection. To enable HTTPS access, go to **Settings > TMS address book** and check the *Use HTTPS for access* check box.

# New features in Version 2.0(1.2)

## Menu building system

Release 2.0(1.2) provides a new, highly flexible menu-building system. 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 gateway. Menus can provide end users with access to videos, operators, address books, dial-it-yourself functions, and audio files.

One feature of this menu-building system enables you to use customized voice prompts. The default 'Welcome' prompt from the previous release of the IP gateway is no longer appropriate and you will want to create your own customized voice prompts that are appropriate to the deployment scenario of your gateway. Until you specify a voice prompt to be used, none will be used when a caller is first connected to an auto attendant menu.

When you upgrade the IP gateway to this release, two new menus, called 'Port A menu' and 'Port B menu' will be created, which will provide the same options as the existing auto attendant menus. Any dial plan rules on Port A with action *Enter the auto attendant* now connect the caller to the 'Port A menu', and likewise for Port B.

The default menus for both ports contain the following options:

- *Operator*: as in the previous release
- *Dial*: as in the previous release
- *Internal address book*: this option will contain all endpoints configured on the gateway

Videos are accessed through a Cisco TelePresence IP VCR. Customized voice prompts can be stored locally on the IP gateway or accessed through a Cisco TelePresence IP VCR. You can configure your menus with a background image of your choice and choose an appropriate text color for the on-screen options. To create a customized menu system, go to **Menus**.

## Improved on-screen operator interface

The operator now has a picture in picture user interface, accessible by the operator pressing # (the pound/hash key) while in a call. This provides three options:

- *Dial*: dial a number or IP address using the dial menu
- *Internal address book*: displays a list of all configured endpoints
- *External address book*: displays the Cisco TelePresence Management Suite (Cisco TMS) address book if one has been configured (see Cisco TMS address book below)

For more information about the operator, refer to the online help.

## API support

Release 2.0(1.2) introduced an API for the IP gateway. The API is documented in the *Cisco TelePresence IP Gateway Remote Management API Reference Guide*.

## Cisco TMS address book

The auto attendant menus and on-screen operator interface for the IP gateway can display the Cisco TMS address book. Cisco TMS v 12.0 and later supports this feature. You must configure the Cisco TMS to provide the gateway with the required address books. To configure the Cisco TMS address book on the gateway, go to **Settings > TMS address book**.

## CDRs

The IP gateway is able to generate Call Detail Records (CDR) which can be used for auditing and billing purposes. When logging is enabled, records are generated whenever a new call is established or terminated, when the auto attendant forwards a call, and so forth.

To use the CDR feature, there must be a 256 Mb compact flash card available — in the slot in the front of the unit. To access the CDRs, go to **Events > CDR log**.

## HTTPS for secure web access

In release 2.0(1.2), you can access the web interface of the IP gateway using HTTPS. This is more secure than using HTTP. To use HTTPS, you must install either the 'Secure management (HTTPS)' feature key or the 'Encryption' feature key which you might already be using for AES encryption.

To enable HTTPS web access, go to **Network > Services** and enable *Secure web*. 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 an SSL certificate and private key, go to **Network > SSL certificates**.

## Secure storage of user passwords

Release 2.0(1.2) introduced the hashing of stored user passwords. You can configure the IP gateway to hash user passwords before storing them in the *configuration.xml* file. The *configuration.xml* file is used for backing up and restoring the configuration of the gateway. If you do not select to hash stored passwords, all user passwords are stored in plain text in the *configuration.xml*; this might be a security issue. If you select to hash stored passwords, they will not be stored anywhere on the gateway in plain text; instead the passwords will be stored as hash sums.

To hash stored user passwords:

1. For Release 2.0(1.2) and Release 2.0(1.7), go to **Settings > Upgrade** and scroll to the *Security settings* section. For Release 2.0(3.32) and later, go to **Settings > Security**.
2. Select *Hash stored passwords* and click **Update security settings**. You will see a warning telling you that this is an irreversible step.
3. If you are sure you want to hash stored user passwords, click **Confirm hash passwords**.

**Note:** You can transfer configuration files between Cisco TelePresence IP Gateways with hashed passwords, but you cannot transfer a configuration file from a gateway that uses hashed passwords to a gateway that does not use password hashing. Also, if you downgrade the gateway to an earlier software version then you will need to reset the configuration.

## Port licensing for the IP GW MSE 8350 blade

Release 2.0(1.2) introduced support for port licenses on the Cisco TelePresence IP GW MSE 8350 blade. Port licenses are provided so that you can control the number of ports that are licensed without requiring new hardware (up to the maximum available on a particular blade type). Also you can share the licenses over a number of Cisco TelePresence MSE 8000 blades of the same type to provide redundancy. Finally, you can swap a blade with a spare of the same type as required without needing to change the port license configuration.

Port licenses apply to a particular blade type and therefore you need different license keys for each type of blade; for example, one license key for IP GW MSE 8350 blades and another for media blades.

For port licensing to operate on your IP GW MSE 8350 blade, you need to have upgraded your Cisco TelePresence Supervisor MSE 8000 (Supervisor) software to version 1.2(1.2). Supervisor version 1.2(1.2) introduces port licensing on the MSE 8000. We recommend that you upgrade your Supervisor before upgrading the IP GW MSE 8350 blade to this release. When you upgrade the Supervisor to release 1.2(1.2), you will need to have the license keys to hand.

## Cisco TMS support for the Cisco TelePresence IP Gateway

Cisco TMS release 12.0 includes support for the IP gateway from this release onwards. You can register a IP gateway with the Cisco TMS, which will then display information about the gateway.

## SIP encryption

### SRTP support

Release 2.0(1.2) introduced support for Secure Real-time Transport Protocol (SRTP). SRTP is an encryption format widely used in SIP. When SRTP is in use, the audio and video media are encrypted. When using SRTP, the default mechanism for exchanging keys is Session Description Protocol Security Description (SDES). SDES exchanges keys in clear text which means that even though the media is encrypted, someone who read the key exchange could decrypt the call, 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.

You can configure the gateway to use SRTP only for calls that use TLS, or for all transports (TCP and UDP as well). To configure which calls will use SRTP, use the SRTP encryption option on the **Settings > Calls** page. For more information about using TLS, see below.

To use SRTP encryption, you must have the *Encryption* feature key present on the gateway.

**Note:** SRTP will not be used for calls with Microsoft Office Communications Server (OCS).

### TLS support

Release 2.0(1.2) introduced support for Transport Layer Security (TLS). TLS enables the signaling portion of a SIP call to be encrypted. This is important because without this, if the call uses SRTP (see above), the key exchange will be in clear text in this part of the call.

To use TLS, you must have either the *Encryption* feature key or the *Secure management (HTTPS)* feature key present on the IP gateway. You can configure to use TLS for all SIP calls on the **Settings > SIP** page.

Regardless of whether or not you choose to use TLS for outgoing connections, the IP gateway will accept incoming calls using TCP, UDP, and TLS providing those services are enabled on the **Network > Services** page.

If you have the IP gateway set to *Encryption Required* (on the **Settings > Calls** page) then a SIP call must use SRTP.

### TLS certificate verification

Release 2.0(1.2) introduced the ability to import a certificate trust store. This enables you to configure the IP gateway to verify the identity of the far end of a connection when using TLS (Transport Layer Security). For example, the trust store can be used by the gateway to verify the identity of a SIP endpoint that will receive an outgoing call.

To upload a trust store (in *.pem* format), go to **Network > SSL certificates**. Refer to the online help topic *Configuring SSL certificates* for more information.

When you have uploaded a trust store, you can choose to what extent the IP gateway will verify the connection. Note that in the following descriptions, outgoing connections are connections such as SIP calls which use TLS:

- No verification: all outgoing connections are permitted to proceed, even if the far end does not present a valid and trusted certificate. This is the default setting
- Outgoing connections only: outgoing connections are only permitted if the far end has a certificate which is in the trusted store
- Outgoing connections and incoming calls: for all outgoing connections and for incoming SIP calls that use TLS, there must be a certificate which is listed in the trusted store otherwise the gateway will not allow the connection to proceed

## Alternate gatekeepers

Release 2.0(1.2) introduced support for the use of alternate gatekeepers. That is, where the configured gatekeeper has told the IP gateway about any configured alternate gatekeepers and if the gateway loses contact with the configured gatekeeper, the gateway will attempt to register with each of the alternates in turn. If none of the alternate gatekeepers responds, the 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
- The list of alternates received from the new gatekeeper will replace the previous list
- The 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:** If the gateway registers with an alternate that does not supply a list of alternates, the 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.

## RAI support for gatekeeper load balancing

Release 2.0(1.2) provides support for Resource Availability Indicators (RAIs) for gatekeepers. This feature enables 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.

This feature is to be used where multiple gateways are registered with the same gateway dial plan prefix on the same gatekeeper. When in use, the gateway will inform the gatekeeper when it is unavailable (that is, all its ports are already in use). Gatekeepers that support this functionality will favor gateways in the available state when choosing where to place new calls.

## Ping from web interface

Release 2.0(1.2) provides a facility on the web interface to perform a ping to a remote device. This can be used to troubleshoot network issues between the IP gateway and a video conferencing device. To perform a ping, go to **Network > Connectivity**. For each successful ping, the time taken for the packet to reach the host and for the reply packet to return to the gateway is displayed in milliseconds (the round trip time). The TTL (Time To Live) value on the echo reply is also displayed.

## H.323 URI dialing using DNS SRV

Release 2.0(1.2) supports the use of H.323 URI dialing using DNS SRV. For example, dialing can now be in the format of **`example.person@example.com`**

## Display local IP address and port number that gateway has registered with gatekeeper

In release 2.0(1.2), the status section of the **Settings > H.323 settings > Gatekeeper** page displays the local address and port that the IP gateway has registered with the configured gatekeeper. It displays, for instance, whether the Port A or Port B address has been used, and also whether the default H.323 port (1720) is registered, or a different value as set on the **Network > Services** page.

## NTLM authentication

Release 2.0(1.2) supports NTLM authentication for use with Microsoft OCS and LCS. Where NTLM authentication is required, the username and password from the **Settings > SIP** page will be used to generate authentication values when the IP gateway is challenged by the OCS/LCS server. Therefore, where NTLM is used, the gateway no longer needs to be configured as a trusted host on the server, so long as NTLM is enabled.

## Extended support for SDP in SIP

Release 2.0(1.2) introduced support for SIP devices that do not send the capabilities in the initial INVITE, but instead delay it to the ACK. Note that the IP gateway sends capabilities in the INVITE.

This release also introduces support for subsequent UPDATE messages to include an SDP.

## OCS bandwidth limitation

Release 2.0(1.2) introduced a control to limit bandwidth specifically to Microsoft OCS and LCS clients. Microsoft OCS/LCS clients will try to use the maximum bit rate that the IP gateway advertises during the initial call setup. The maximum bit rate that is advertised is the *Default bandwidth from IP gateway* that is configured on the **Settings > Calls** page. In most scenarios, you will not want OCS/LCS clients to use that bit rate as it may cause excessive loading on the PC client. Instead, use the new *Maximum bit rate from Microsoft OCS/LCS clients* control on the **Settings > SIP** page to select an appropriate bit rate for Microsoft OCS/LCS clients. Note that if you do want OCS/LCS clients to try to use the maximum bit rate that the IP gateway advertises during the initial call setup, set this control to <*limit disabled*> which will cause the gateway to advertise the *Default bandwidth from IP gateway* to OCS and LCS clients.

## H.460 18/19 client support

Release 2.0(1.2) provides client support for H.460 18/19. This enables the IP gateway to make H.460 calls using H.460 servers such as the Cisco VCS and the TANDBERG Border Controller.

## Index for online help

The online help accessible from the web interface of the IP gateway now provides an index.

# Resolved issues

The following issues were found in previous releases and are resolved in 2.0(3.34).

## Resolved since Version 2.0(3.32)

| Identifier | Description |
|---|---|
| CSCuo21597 | **Symptom:**<br>Cisco TelePresence IP Gateway Series (3510, 3520, 3540 and 8350) includes a version of openssl that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160.<br><br>This bug has been opened to address the potential impact on this product.<br><br>**Conditions:**<br>Device with default configuration running blade software 2.0(3.32). Release 2.0(1.11) is NOT affected by this vulnerability.<br><br>**Workaround:**<br>Not currently available.<br><br>**Further Problem Description:**<br>Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html<br><br>**PSIRT Evaluation:**<br>The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/5:<br><br>https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C<br><br>The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.<br><br>CVE-2014-0160 has been assigned to document this issue.<br><br>Additional information on Cisco's security vulnerability policy can be found at the following URL:<br><br>http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html |

## Resolved since Version 2.0(1.11)

| Identifier | Description |
|---|---|
| CSCub32208 | In some circumstances, the IP gateway stopped responding to HTTP(S) requests on both the web interface and API calls. This recent problem has been attributed to Firefox browser version 14.0.1 (the first release code of Firefox 14; release date: 17th July 2012) and is improved in this release. This version of Firefox is still not recommended; Firefox 15 should be used instead (release date: 28th August 2012). See also the limitations section of these release notes. |
| CSCtq42519 | In Version 2.0(1.11), if the IP gateway was set to require encryption, it would unexpectedly reboot in the case of audio-only calls from an ISDN gateway or audio-only calls between two MXP Series endpoints. This is now fixed. |
| CSCtq51058 | In previous releases, for outgoing SIP calls where the gateway was registered to a Cisco VCS, the SIP registrar address was defined as an IP address, and the dial plan directed the outbound call to a domain name, the gateway INVITE would set the Request-URI (RURI) to *xyz@ipaddress* instead of |

| Identifier | Description |
|---|---|
| | *xyz@domain name*. This is now fixed. |
| CSCtq91170 | In previous releases SIP calls initiated by the gateway might fail with SIP parse error warnings (where one-and-a-half SIP messages arrived in one Ethernet frame). This is now fixed. |
| CSCtr77633 | In previous releases, if **Use endpoint name as caller ID** was enabled for the IP gateway (**Settings > Calls**), when dialing out (SIP) from the IP gateway the *From* address did not include the caller (SIP) endpoint's display name. Only the SIP URI of the IP gateway was included in the *From* address to the callee. The callee saw the caller's display name as "ipgw@1.2.3.4:12345". This is now fixed. |
| CSCtr80297 | In previous releases, if the gateway was registered to a Cisco TMS, the gateway might unexpectedly reboot while in idle state after receipt of RPC messages from the TMS. This is now fixed. |
| CSCtr80303 | In previous releases, with certain endpoints, the gateway might unexpectedly reboot (the cause was traced to unusually fast use of the DTMF buttons on the menu system). This is now fixed. |
| CSCts82298 | In previous releases SIP to H.323 interworked calls into the IP gateway (interworked by a VCS) would drop after a couple of minutes. No ARQ was sent from the IP gateway for the incoming call, which caused the call to be disconnected by the VCS. This is now fixed. |
| CSCtz90435 | In previous releases, when making a call via an IP gateway to a Microsoft Office Communicator (MOC R2) client using VCS X5.2, the MOC would stick in the *Answering call…* stage after answering the call. This is now fixed. |
| CSCtz90445 | In previous releases downloading the *configuration.xml* file from the IP gateway over FTP led to invalid XML and missing data. This is now fixed. |
| CSCtz90462 | In previous releases the gatekeeper settings were not reflected on the IP gateway web interface after uploading a new *configuration.xml* file. The IP gateway did not register to the gatekeeper as a result. This is now fixed. |

## Resolved since Version 2.0(1.7)

| Internal reference | Description |
|---|---|
| 108766 | In previous releases it was not possible to dial the gateway using dial plans containing multiple hashes. This is fixed in 2.0(1.11). |
| 108854 | Previous releases of the gateway were unable to forward out of band DTMF tones from HDX endpoints. This is fixed in 2.0(1.11). |
| 109124 | In previous releases, where a proxy was configured for a registrar, the gateway attempted to resolve the registrar domain name instead of sending it directly to the proxy. This is fixed in 2.0(1.11). |
| 109423 | In previous releases, if a call made from a Cisco phone was put on hold and then resumed, only the audio channel was reopened. This is fixed in 2.0(1.11). |
| 109800 | In previous releases a crash could potentially occur when an incoming caller hung up at the same time as, or just before, the far end answered. This is fixed in 2.0(1.11). |

## Resolved since Version 2.0(1.2)

| Internal reference | Description |
|---|---|
| 105543 | In previous releases the gateway could unexpectedly reboot, especially when calls were looped back to the same gateway. This is fixed in release 2.0(1.7). |
| 106885 | Interoperability with high resolutions from the Cisco TelePresence Codec C90 has been improved. |
| 107197 | In previous releases issues existed when using Far End Camera Control with some TANDBERG endpoints. This is fixed in release 2.0(1.7). |
| 107585 | In previous releases interoperability issues with the Polycom V700 caused video to be received at a very low bit rate. This is fixed in release 2.0(1.7). |
| 107670 | In previous releases sending content between two Cisco TelePresence Codec C90s via a IP gateway could cause an unexpected reboot. This has been fixed in release 2.0(1.7). |
| 108268 | Version 2.0(1.7) improves interoperability for the G.729 codec with third party endpoints. |
| 108455 | Version 2.0(1.7) improves video quality when the gateway is handling fragmented packets in non-transcoded mode. |
| 108461 | In previous releases media was not always established when Office Communicator calls from Microsoft OCS connected to a IP gateway with a SIP registration to VCS. This is fixed in release 2.0(1.7). |

## Resolved in Version 2.0(1.2)

| Internal reference | Description |
|---|---|
| 103876 | In previous releases it was not possible to upgrade a IP gateway using FTP. This is fixed in release 2.0. |
| 105066 | Interoperability issues with the Cisco VTA have been fixed. |
| 105448 | In previous releases calls to Polycom VSXs could fail. This was caused by the gateway sending video at a high frame per second rate. This is fixed in release 2.0. |
| 106466 | In previous releases content could be sent using CIF resolution even when higher resolutions were possible. This is fixed in release 2.0. |

# Limitations

The following limitations apply to the IP gateway.

| Identifier | Description |
|---|---|
| CSCtz90426 | Outgoing out-of-band DTMF over SIP is not supported. As a workaround, you can specify that out-of-band DTMF should be converted to in-band (on the **Settings > Calls** page enable the **Convert-out-of-band to in-band DTMF** setting). The gateway will then convert the DTMF tones to in-band and forward them over SIP. |

## No support for Firefox 14

Firefox 14 is not supported for use with the Cisco TelePresence IP Gateway. We strongly recommend that you refrain from using Firefox 14 to access the gateway web interface. This version of the browser causes an issue that was not present in previous versions and which has been fixed in the following version (Firefox 15).

# Interoperability

We endeavor to make the IP gateway interoperable with all relevant standards-based equipment. However, it is not possible to test all scenarios. The following list describes the equipment and software revisions that were tested for interoperability with this release. The absence of a device or revision does not imply a lack of interoperability.

**Note:** Unless otherwise stated, Cisco Unified Communications Manager (Cisco Unified CM) Version 8.6(1a) and Cisco TelePresence Video Communication Server (Cisco VCS) Version X7.0 were used in the interoperability tests.

## Call scenarios

Interoperability testing often requires interworking from one signaling/call control protocol to another. The following table defines the paths for the various call scenarios used in the interoperability tests (not all call scenarios were tested with all equipment). By convention the endpoint is placed first and the IP gateway is last in the descriptions:

| Call scenario | Path description |
|---|---|
| SIP | Endpoint <--SIP--> IP GW<br>A registrar is used but not shown here. |
| H.323 | Endpoint <--H.323--> IP GW<br>A gatekeeper is used but not shown here. |
| H.323 to SIP interworking | Endpoint <--H.323--> VCS <--SIP--> IP GW |
| SIP to H.323 interworking | Endpoint <--SIP--> VCS <--H.323--> IP GW |
| Cisco Unified CM to Cisco VCS H.323 | Endpoint <--SIP--> CUCM <--SIP--> VCS <--H.323--> IP GW |
| Cisco Unified CM to Cisco VCS SIP | Endpoint <--SIP--> CUCM <--SIP--> VCS <--SIP--> IP GW |

## Endpoints interoperability

This section lists interoperability issues with endpoints, grouped by manufacturer. Specific limitations that may exist for particular endpoints, such as no encryption support, are not listed and were omitted from the interoperability tests.

### Cisco endpoints

| Equipment | Software revision | Comments |
|---|---|---|
| Cisco IP Video Phone E20 | TE4.1.1.273710 | Tested Cisco Unified CM to Cisco VCS SIP and Cisco Unified CM to Cisco VCS H.323 (non-transcoded and transcoded). No unresolved issues found. |
| Cisco TelePresence System Codec C60 | TC5.1.0 | No unresolved issues found. |
| Cisco Jabber Video for TelePresence | 4.3 | Tested SIP and SIP-H.323 interworked. No issues found. |
| Cisco TelePresence System 1700 MXP | F9.1.2 | Tested H.323 and SIP.<br>FECC negotiation can take several seconds on SIP calls. |
| Cisco TelePresence System 3000/ System 500 | 1.8.1(34) and 1.9.0(46) | Tested Cisco Unified CM to Cisco VCS SIP and Cisco Unified CM to Cisco VCS H.323.<br>■ A known encryption issue with interworking to the CTS causes calls to appear encrypted on the IP gateway when they should not appear as encrypted.<br>■ Video on CTS appears frozen at low bandwidth.<br>■ Low bandwidth SIP calls result in frozen video on the CTS.<br>■ If encryption is disabled on the CTS-3000/CTS-500, calling via an IP gateway that requires encryption results in a half-encrypted call. This issue is resolved in Cisco VCS Version X7.2. |
| Cisco Unified IP Phone 7985G | 4.1(7) | Tested SIP-H.323 interworked and Cisco Unified CM to Cisco VCS SIP.<br>■ A VCS issue currently affects this endpoint when interworked.<br>■ The endpoint may not be able to decode video from the IP gateway when H.263+ is negotiated. The endpoint sends repeated Fast Update Requests but does not decode the key frames sent by the gateway in response.<br>■ DTMF in interworked calls does not work (the gateway does not support DTMF over KPML).<br>■ H.323 transcoded calls exhibit sub-optimal behavior. |
| Cisco Unified IP Phone 9971 | 9-2-3-27 | Tested SIP and SIP-H.323 interworked.<br>■ G.729 calls do not work correctly when interworked.<br>■ Interworked calls can take a long time to connect. These issues are resolved in Cisco VCS Version X7.2. |
| Cisco Unified Video Advantage | 2.2.2.0 | Tested Cisco Unified CM to Cisco VCS SIP and SIP-H.323 interworked.<br>■ Transcoded H.323 calls do not work due to an issue on the gateway side. |

### Polycom endpoints

| Equipment | Software revision | Comments |
|---|---|---|
| Polycom HDX 4500 | 3.0.3.1-19040 | Tested H.323 and SIP.<br>■ The IP gateway cannot receive H.261 video during SIP calls because the endpoint does not advertise H.261. This does not affect functionality if other codecs are enabled.<br>■ The endpoint cannot send simultaneous H.263+ main video and H.264 content. All other codec combinations work.<br>■ Delay in opening the audio channel can result in early part of voice prompt not being heard at the endpoint (CSCtz01271)<br>■ Using *only* the Siren 14 audio codec is not supported in some cases (when the codec is not advertised by the endpoint).This does not affect functionality if other codecs are enabled. (CSCtz21120) |
| Polycom VVX | 4.0.1.13681 | Tested H.323 (non-transcoded and transcoded) and SIP.<br>■ H.323 non-transcoded. In one call scenario, when this endpoint is set to H.263, the IP gateway receives H.263 CIF but transmits H.263+, which the endpoint fails to decode. The other endpoint in this scenario was a Cisco TelePresence System Codec C40. Other codecs were unaffected.<br>■ H.323 non-transcoded. When this endpoint is configured for H.264 and G.722.1C or Siren14, the call fails to connect. The other endpoint in the call was a Cisco TelePresence System Codec C40.<br>■ H.323 transcoded. When *only* G722.1 Annex C or Siren 14 is enabled, with the endpoint running version 5.0.1.11086, calls to the IP gateway auto attendant work, but if the dial plan is set to dial the endpoint directly or the endpoint is dialed through the auto attendant the call fails. |
| Polycom ViewStation | 6.0.5 | Tested H.323 and H.323-SIP interworked.<br>No issues found. (One issue was detected in initial testing but is now resolved.) |
| Polycom QDX 6000 | 4.0.2 | Tested H.323 and SIP.<br>■ If this endpoint has encryption set to “when available”, it advertises encryption as “required” rather than “optional”. Consequently, if encryption is disabled on the IP gateway then calls to or from this endpoint will fail.<br>■ Hissing audio was experienced when using G.711 and G.722 during encrypted calls.<br>■ H.261 and Siren14 are not advertised by this endpoint when using SIP. |

### Sony endpoints

| Equipment | Software revision | Comments |
|---|---|---|
| Sony PCS-G50 | 2.72 | Tested H.323 and H.323-SIP interworked.<br>■ In some circumstances in H.323 calls, no audio is heard on this endpoint.<br>■ Encrypted interworked calls with this endpoint are not supported. (CSCtz12733) |
| Sony PCS-1 | 3.42 | Tested H.323 and H.323 to SIP interworking.<br>Audio between the IP gateway and this endpoint is not supported on interworked calls if the endpoint **Audio Mode** setting is *MPEG4 Audio* or *Auto*. |
| Sony PCS-XG80 | 2.31 | Tested H.323 and SIP.<br>■ Some endpoint issues were observed with negotiation of G.728 and G.711. |
| Sony PCS-HG90 | 2.22 | Tested H.323 and H.323-SIP interworked.<br>■ This endpoint is HD only and cannot be used in transcoded calls except in audio-only mode.<br>■ Encryption is applied only to part of the call path. |

### TANDBERG legacy endpoints

| Equipment | Software revision | Comments |
|---|---|---|
| TANDBERG Classic 6000 | E5.3 PAL | Tested H.323 and H.323-SIP interworked.<br>Encrypted calls at bandwidths greater than 768 kbps between a Tandberg Classic endpoint and Cisco TelePresence MCU may result in various video problems.<br>RTCP timestamps from the Cisco TelePresence MCU 5300 Series are unreliable. |
| TANDBERG 150 MXP | L6.1 | Tested H.323 and SIP.<br>No issues found. |

### Other endpoints

| Equipment | Software revision | Comments |
|---|---|---|
| LifeSize Room 200 | 4.7.18 | Tested SIP and H.323.<br>■ Transcoded calls result in video from a CTS endpoint appearing vertically stretched with H.264 and horizontally stretched with H.263+.<br>■ Transcoded H.323 calls cause purple blocks to appear on this endpoint.<br>■ Encrypted SIP calls are not supported between the gateway and this endpoint. |
| Panasonic KX-VC300 | 2.30 | Tested SIP and SIP-H.323 interworked.<br>■ Encryption and 1080p resolution is not supported between this endpoint and non-Panasonic equipment.<br>■ Most transcoded H.323 calls fail.<br>■ Video corruption is observed on video from this endpoint. |
| Radvision SCOPIA | 2.5.0208 | Tested H.323 and SIP. The following behavior was observed for this endpoint: |

| Equipment | Software revision | Comments |
|---|---|---|
| XT1000 | | ■ Encrypted SIP calls are not supported.<br>■ Squashed video is sent by the endpoint when using H.263+.<br>■ If the endpoint is set to “Favour Motion” it sends approximately 17 fps video. |

## Infrastructure interoperability

This section lists known interoperability issues with infrastructure components.

| Equipment | Software revision | Comments |
|---|---|---|
| Cisco TelePresence Content Server | S5.3 | Tested H.323 and SIP. No issues found. |

# Updating the software

## Prerequisites and software dependencies

**CAUTION:** You **must** back up your configuration **before** you upgrade the software.
You must remember the administrator user name and password for the configuration backup file in case you ever need to use it.

**CAUTION:** If you use CDR data for any purpose (such as billing or auditing) you **must** also download and **save** the current CDR data before you upgrade.

## Backup instructions

You can back up the IP gateway configuration via the web interface or via FTP. To use the web interface, go to **Settings > Upgrade** and follow the backup instructions in the online help. To use FTP, follow these steps:

1. Make sure that the FTP service is enabled on the **Network > Services** page.
2. Connect to the IP gateway using an FTP client.
3. Log in as an administrator (use the administrator credentials that you would use to connect to the web interface). You will see a file called *configuration.xml*. This contains the complete configuration of the device.
4. Copy the *configuration.xml* file to a secure location.

If you subsequently need to downgrade to a previous version of the software, you can re-apply the *configuration.xml* backup file to return the device to its former configuration. The backup file also includes all activation keys for the device.

## Before you start

The software upgrade process requires a hardware restart. Make sure that the IP gateway is not in use, or warn any active users who may be affected by the loss of service.

Have the following items available:

- The new software image file.
- The current software image file (in case you need to reverse the upgrade).
- The backup *configuration.xml* file.
- The administrator user name and password for the backup file.
- If applicable, make sure that the CDR data has been downloaded and saved.

# Upgrade instructions

**Note:** The upgrade may take some time to complete (you can monitor progress through the serial port).

## Process using the web interface

1. Download the image file from Cisco.com.
2. Unzip the image file to a local folder.
3. In an Internet Explorer-compatible web browser, navigate to the IP address of the IP gateway.
4. Sign in as an administrator. On a new device the default user name is *admin* with no password.
5. Go to **Settings > Upgrade**.
6. In the **Main software image** section, specify the location of the software image file.
7. Click **Upgrade software image**.

   The web browser uploads the file to the gateway. This takes some time depending on your network connection. Do not navigate away from the upgrade page or refresh the page during the upload process.

   When the upload completes, the browser refreshes automatically and displays an upload completed message.
8. Close the completion message.
9. On the main upgrade page, click **Shutdown**. This option changes to **Confirm IPGW shutdown**. Click to confirm.
10. Click **Restart IPGW and Upgrade**. (This button appears in the **Upgrade** page during this process.)

    The device reboots and upgrades as it restarts. This may take some time to complete.

**Note:** If you are logged out due to inactivity, sign in again as an administrator and click **Restart IPGW and upgrade** on the **Upgrade** page to complete the upgrade.

## Process using FTP

1. Connect to the IP gateway via FTP.
   For example, from a command prompt type **ftp *<gateway IP address>***.
2. Sign in as an administrator. On a new device, the default user name is *admin* with no password.
3. Upload the upgrade file.
   For example, from the FTP prompt type **put *<image filename>*.**
4. When the upload completes, reboot the device. You can reboot from the **Upgrade** page on the web interface.
5. The device upgrades as it restarts.

# Downgrade instructions

If you need to reverse your upgrade, you can re-install an earlier version of the software. The downgrade procedure is the same as for the upgrade except that it uses the earlier software image.

## Prerequisites and software dependencies

**CAUTION:** If you use CDR data for any purpose you **must** download and **save** the CDR data before you downgrade to an earlier version. The downgrade process will delete all existing CDRs.

**CAUTION:** Do not downgrade to any software version that is numbered between 2.0(1.12) and 2.0(2.17) inclusive. These versions were temporary, customer-specific builds that are unsuitable for general use.

## Downgrade procedure

To downgrade the software back to an earlier release:

1. Go to **Settings > Upgrade**.
2. In the **Restore configuration** section, navigate to and select the appropriate *configuration.xml* backup file.
3. Check the **User settings** check box.
4. If required, check the **Network settings** check box.
5. Click **Restore backup file**.
6. When the configuration is restored, you need to re-install the required former software version.

# Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com username and password.
3. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the Search field and click Search.
2. From the list of bugs that appears, use the Filter drop-down list to filter on either Keyword, Modified Date, Severity, Status, or Technology.

Use **Advanced Search** on the Bug Search Tool Home page to search on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

# Getting help

If you experience any problems when configuring or using the IP gateway, see the Product documentation section of these release notes. If you cannot find the answer you need in the documentation, check the web site at http://www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

# Document revision history

| Date | Revision | Description |
|---|---|---|
| May 2014 | 03 | Maintenance release |
| November 2012 | 02 | Maintenance release |
| June 2010 | 01 | Maintenance release |