Cisco TelePresence ISDN GW 3241 & MSE 8321 Version 2.2(1.122) P

Software Maintenance Release Notes
March 2017

Contents

Introduction

This release note accompany software maintenance release Version 2.2(1.122) for the Cisco TelePresence ISDN GW 3241 unit and the Cisco TelePresence ISDN GW MSE 8321 blade.

This document lists and describes the new features introduced by the 2.2 release and issues resolved in this maintenance release.

For clarity in this document, the term “ISDN gateway” is used in references that include both the ISDN GW 3241 unit and the ISDN GW MSE 8321 blade.

Product Documentation

All product documentation can be found on Cisco.com. The following documents provide guidance on product installation, configuration, and operation:

- *Cisco TelePresence ISDN GW 3241 Getting Started Guide*
- *Cisco TelePresence ISDN GW MSE 8321 Getting Started Guide*
- *Cisco TelePresence ISDN Gateway Remote Management API Reference Guide*
- *Cisco TelePresence ISDN Gateway Version 2.2 Online Help (printable format)*

New features in Version 2.2

Native Support for SIP

The ISDN gateway now provides native support for Session Initiation Protocol (SIP) and external interworking is not necessary to connect SIP calls. Direct calling and proxy-routed calling is supported. Other significant aspects of the SIP implementation include:

- SRTP-based encryption using Transport Layer Security (TLS) is supported.
- Content sharing via Binary Floor Control Protocol (BFCP) is supported over TCP and UDP.
- The gateway can receive out-of-band DTMF signaling for SIP and supports RFC 2833 and Key Press Markup Language (KPML). This can be used to drive the IP-side auto attendant. When the ISDN leg of a call is a telephone call, the gateway can convert received out-of-band to in-band and forward it over ISDN.
- For video fast update control, the gateway supports Full Intra Request (FIR) or Picture Loss Indication (PLI) messaging depending on the endpoint capabilities (PLI is always preferred). If the far end supports neither method the gateway uses SIP INFO messages.
- For flow control, on the ISDN side no standards-based mechanism exists and it is not possible for the far end to flow-control the gateway. In the case of packet loss the IP endpoint at the far end may use the RTCP receiver reports generated by the gateway to flow control itself.
- Call transfer from the gateway is not currently possible. This release does not support SIP REFER message based call transfers.

Important! Configuration of Unified CM SIP trunks
In Cisco Unified Communications Manager (Unified CM) environments, we recommend that the SIP trunk for the gateway is set to “Early Offer” in the Unified CM. If the SIP trunk is set to “Delayed Offer” and multiple ISDN gateways exist in the call path, SIP calls may be limited to G.711 audio even if the calling endpoint supports advanced codecs.

Note: As in earlier releases, the algorithms for call number matching in the gateway dial plan support numeric values only. Using alphanumeric ids can result in complex dial plan manipulation requirements. Where possible we recommend that call number schemes for the gateway are defined with numerics only.

Dial Plan Enhancements

Matching against the calling number is now supported. Dial plan rules can match against a specific calling number, and optionally can manipulate the calling number before it is forwarded to the IP or ISDN side. Manipulation of the calling number facilitates simplified callback mechanisms and can also be used to provide calling party identification where the caller ID is absent. Examples are provided in the online help.

You can also now match against incoming call type (video or telephone) and incoming call protocol (H.323 or SIP). The outgoing call type can be set to use the incoming type.

Settings for dial plan rules have been reorganised into required and optional groups in the web user interface.

The gateway API now supports dial plan management. API calls are available to query, modify, add, delete, and test dial plans. An API counter is also available to monitor usage of dial plan rules.

Security Features

64 Character User IDs

The ISDN gateway can now accept and store usernames up to 64 Unicode characters long. This applies anywhere that the gateway can accept a username—via the web interface, an API call, FTP or serial console login, or from a client certificate (common name).

Tighter Password Security

The ISDN gateway never stores passwords in plain text. Passwords are hashed (using SHA-2) before being stored. This applies even if an unhashed password is provided in a configuration file.

Mutual Authentication

The ISDN gateway now supports certificate-based user authentication over HTTPS, using mutual TLS authentication between certificates on the user (client) side and certificates held in an HTTPS trust store on the gateway. This feature is configurable in the form of different login modes, and is managed through the **Network > SSL certificates** page. (Configuration options and associated certificate requirements are explained in Appendix A Mutual authentication connections and certificate identity requirements.)

The gateway supports certificate chains. It checks the certificate chain for the client against its own trust store. If the certificate is trusted, the gateway can also perform an OCSP (Online Certificate Status Protocol) check of the leaf certificate (see next section).

OCSP checks of Client Certificates

The ISDN gateway can now use OCSP to check client certificate revocation status against a pre-configured OCSP server. If the OCSP server responds that the certificate is 'good', the gateway allows the client to authenticate with the certificate. In all other cases the gateway will reject the certificate and prevent authentication.

The gateway always uses its known OCSP server and does not check any OCSP servers specified by the client certificate. The feature is configurable to include a nonce. Static Certificate Revocation Lists are not supported.

CAUTION: When enabling OCSP checking for the gateway it is possible to inadvertently block *all* login access (including administrators) to the application. If you decide to enable OCSP checking we strongly recommend that you first review Appendix B Transitioning to certificate-based security.

Certificate-Based Login

Because the ISDN gateway now supports mutual authentication, it is possible for users to authenticate and log in using a client certificate rather than entering a username and password. With certificate-based login, the gateway checks the usernames in its configuration file for a match to the common name in the client certificate. If a match exists, the user who presents the certificate is logged in automatically and does not need to enter a username and password.

The ability to log in with a username and password is retained, and the gateway can be configured to operate with or without certificate-based login. Certificate-based login can be specified as optional or as a required alternative to password-based login.

CAUTION: When setting certificate-based authentication options for the gateway it is possible to inadvertently block *all* login access (including administrators) to the application. If you decide to implement certificate-based authentication we strongly recommend that you first review Appendix B Transitioning to certificate-based security.

The gateway now supports four login modes, listed here from lowest to highest security level:

1	**Not required**	Default. No client-side authentication is required and client certificates are irrelevant to the gateway. All users log in with usernames and passwords. Password-based login is the sole authentication mechanism over all interfaces (HTTPS, HTTP, FTP, and serial).
2	**Verify certificate**	Clients must have a trusted certificate if they wish to log in using HTTPS. Password-based login is required over HTTPS. Password-based login is allowed as usual over HTTP, FTP, and serial interfaces.
3	**Certificate-based authentication allowed**	Clients must have a trusted certificate if they wish to log in using HTTPS. Certificate-based login is allowed over HTTPS. If the certificate common name matches a gateway username, the user is logged in automatically. If no match exists, the user can use password-based login instead. Password-based login is allowed as usual over HTTP, FTP, and serial interfaces.
4	**Certificate-based authentication required**	Clients must have a trusted certificate if they wish to log in using HTTPS. Certificate-based login is required over HTTPS *and* all other connection types. No password login is allowed and HTTP, FTP, and serial interfaces are effectively disabled (except for functions that do not require login).

Effect of Certificate-Based Authentication on the API

If certificate-based authentication is allowed, the standard authentication parameters (**`authenticationUser`** and **`authenticationPassword`**) are required in API messages only if the client certificate is insufficient for login purposes. If certificate-based authentication is required, the parameters are ignored altogether and a client certificate must be used for login purposes, meaning that only HTTPS access is possible.

Additional QoS Functionality

The ISDN gateway can now tag all outgoing traffic with configurable quality of service (QoS) information. This applies to both Ethernet ports on the gateway, whether on IPv4 or IPv6 networks. The gateway can tag these traffic types:

- **Audio**, **Video**, and **Telephony** for the various data streams (**Telephony** applies to media from ISDN telephone calls). Note that a non-telephone ISDN call that contains only audio (for whatever reason) is considered to be **Audio**.
- **Signaling** for H.225, H.245, and SIP messaging.
- **OA&M** (Operations, Administration and Maintenance) for all other traffic.

Auto Attendant Enhancements

If the auto attendant is busy, calls are queued until a connection becomes available. For ISDN video callers in the queue, the ISDN gateway now plays an audio message (voice prompt) and displays a banner on the auto attendant until a connection is available (using H.261 for video and G.711 for audio). For ISDN telephone callers, the ringing state is maintained. The voice prompt and the auto attendant banner can optionally be replaced with customized versions (**Settings > User interface** page and **Settings > Auto attendant** page respectively).

The maximum number of concurrent connections to the auto attendant is now 20.

Codec Support Enhancements

The G.722.1 audio codec is supported in this release, for both H.323 and SIP. By default G.722.1 support is disabled. It can be enabled from the **Settings > ISDN** page (scroll to the **ISDN codec settings** section).

Colon Separator for Extension Dialing No Longer Supported

The colon (:) symbol is no longer supported as an extension separator in dial plan rules. From Version 2.2 an exclamation mark (!) is the only permitted extension separator for new rules. The ISDN gateway will automatically interpret any colon separators in existing rules as exclamation marks (in this release the underlying configuration entries are left unchanged). The colon separator is reserved for alternative use in future releases.

Fallback to Telephone If Video Call Fails

This feature is not supported in leased line configurations. For non-leased line configurations you can now specify that if an incoming video call request fails in the IP to ISDN direction, the ISDN gateway should attempt to connect a telephone call for the outward leg (it will only attempt this if the network cause error indicates that a telephone call might succeed). Fallback only happens at call setup time and is not attempted after a second channel connects.

Miscellaneous Changes

- Out-of-band DTMF can be advertised to the IP side in the case of ISDN telephone calls, using the **Advertise out-of-band DTMF (telephone and auto attendant)** option on the **Settings > ISDN** page. If this option is enabled then out-of-band DTMF will now also be advertised for calls connected to the (IP side) auto attendant. Technically this applies to all call types, although received out-of-band tones will be converted to in-band only in the case of telephone calls.
- Additional bandwidth values are available for call bandwidth limits and downspeeding control.
- New time limits (12 hours and 23 hours) are available for call duration control.
- Detailed call information for active calls (**ISDN > ISDN calls** page) now includes packet statistics, received/forwarded codec capabilities, and current codecs for audio, video, and extended video.
- Web status pages, such as **Status > General** or **ISDN > ISDN calls**, no longer auto-refresh by default. You can manually specify an auto-refresh interval on the **Settings > User interface** page.

User Interface Changes

- Header and footer text (up to 100 Unicode characters each) can now be configured for the web user interface. Configured headers and footers will appear on all pages except online help.
- New **Settings > SIP** page to configure a SIP proxy is now available.
- New settings added to various pages to support the new or modified features in this release.
- Settings for dial plan rules have been reorganised.
- For leased line configurations only, the **Maximum call bandwidth** setting has been removed from the dial plan pages (the setting is irrelevant in leased line mode and should not have appeared). The equivalent global bandwidth settings are retained in case administrators need to switch between modes.

CDR Format Changes (for SIP)

The DN field in Call Detail Records (CDR) on the ISDN gateway now supports up to 161 characters. Any SIP URIs that exceed this length are truncated, and an entry is written to the event log. The DN field for SIP URIs is an attribute of the existing H.323 event “H.323_endpoint_details” and the DN field is now used for both H.323 and SIP.

API Changes

This release introduces the following new API calls:

Retrieve H.323 gatekeeper settings.	gatekeeper.query
Retrieve SIP configuration information.	sip.query
Retrieve or modify ISDN configuration settings.	isdn.settings.modify isdn.settings.query
Retrieve or modify dial plan settings, including a count of dial plan use since the last reboot.	dialplan.rule.add dialplan.rule.delete dialplan.rule.modify dialplan.rule.query dialplan.modify dialplan.query
Reset the dial plan use counter.	dialplan.resetcounter
Test dial plans against specified parameters, including calling/called numbers and incoming port.	dialplan.test

The existing isdn.port.query call now has these new fields:

- overlapReceivingLength
- nationalPrefix
- internationalPrefix.

Resolved and Open Issues in Version 2.2(1.122)

Use the links below to find up-to-date information about issues resolved since Version 2.2(1.106) and open issues in this version in the Cisco Bug Search tool.

Issue type	Link
Resolved Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283626579&rls=2.2(1.122)&sb=fr&bt=custV
Open Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283626579&sb=afr&sts=open&svr=5nH&bt=custV

Limitations

Restricted SIP Audio with Unified CM in Back-to-Back Gateways

As mentioned in the new features list, in Cisco Unified Communications Manager (Unified CM) environments with back-to-back ISDN gateways, SIP calls may be limited to G.711 audio even if the endpoint supports advanced codecs. This occurs if the SIP trunk is set to “Delayed Offer” in the Unified CM. To avoid this situation we recommend that you set the SIP trunk for the gateway to “Early Offer”.

Automatic Link-Local IPV6 Assignment on Disabled Interface

When you enable IPv6 on any of the Ethernet ports on the ISDN gateway (**Network > Port A** or **Network > Port B**), the gateway automatically assigns a link-local IPv6 address to each Ethernet port, even if the port is disabled. An IP address that is assigned to a disabled Ethernet port may not be apparent on the web interface.

Link-Local Addresses

Link-local IPv6 addresses are generated using the MAC address of each physical interface, and are thus unique per physical interface. No restrictions are imposed on link-local IPv6 addresses and all services enabled on their corresponding global IPv6 address are available on the link-local address. They support basic configuration and administration services (such as the web interface) but may not support full functionality such as making and receiving calls. Full functionality is only guaranteed for the main global IPv6 address on each interface.

We recommend that you use a PC with a single network interface connected to the local subnet when trying to access the ISDN gateway web interface using its link-local IPv6 address. Login may fail otherwise, because web browsers do not support URL redirection for an address with a scope ID.

Interoperability

We endeavor to make the ISDN gateway interoperable with all relevant standards-based equipment. While it is not possible to test all scenarios, the testing that the data below is based on covers all the most common functions of the listed endpoints and infrastructure.

Software Versions

Unless otherwise stated, the following software versions were used for this interoperability testing:

- Cisco TelePresence ISDN gateway Version 2.2
- Cisco Unified Communications Manager (Unified CM) Version 10.0.1.10000-24
- Cisco TelePresence Video Communication Server (Cisco VCS) Version X8.5

About the Interoperability Section

This interoperability section 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.

The following table describes the call paths for the various call scenarios used in the interoperability tests. Not all call scenarios were used with all equipment.

Interoperability testing often requires interworking from one signaling/call control protocol to another. The following table summarizes the call paths that were tested for each interoperability scenario. The call path descriptions place the endpoint first and the ISDN gateway last as a general convention:

Call Scenario	Call Path Description
SIP	Endpoint <--SIP--> ISDN GW A proxy is used but is not shown here.
H.323	Endpoint <--H.323--> ISDN GW A gatekeeper is used but is not shown here.
SIP to H.323 interworking	Endpoint <--SIP--> VCS <--H.323--> ISDN GW
Unified CM	Endpoint <--SIP--> Unified CM <--SIP--> ISDN GW
ISDN	Endpoint <--ISDN--> ISDN GW

Endpoints

This section lists interoperability issues with endpoints, by manufacturer. Where an endpoint has limitations, such as a lack of support for encryption or content, the interoperability tests omitted the limitations and they are not listed here.

An infrastructure issue may manifest itself as an issue with a particular endpoint or series of endpoints. Issues of this nature are listed separately under Infrastructure.

Cisco Endpoints

Equipment	Software Revision	Comments
Cisco IP Video Phone E20	TE4.1	Tested SIP, H.323, and Unified CM. ■ For encrypted SIP calls with content disabled, using hold/resume causes encryption to fail on the resume (CSCue08030).
Cisco Jabber for iPad	9.1	Tested SIP and SIP to H.323 interworking.
Cisco Jabber for Windows	9.1.0	Tested Unified CM.
Cisco Jabber Video for TelePresence (Windows)	4.5	Tested SIP and SIP to H.323 interworking.
Cisco TelePresence System 1700 MXP	F9.1.2	Tested SIP and H.323.
Cisco TelePresence System Codec C60	TC5.1.4	Tested SIP and H.323.
Cisco TelePresence System Codec 6000 MXP	F9.2	Tested ISDN.
Cisco TelePresence System EX90	TC5.1.4	Tested SIP, H.323, and Unified CM.
Cisco TelePresence System 500-37	1.9.2	Tested Unified CM. ■ This endpoint does not display content from the ISDN gateway (CSCue04043).
Cisco TelePresence TX9000	1.9.2	Tested Unified CM. ■ This endpoint does not display content from the ISDN gateway (CSCue04043).
Cisco Unified IP Phone 9971	9-3-2-10	Tested Unified CM.

Polycom Endpoints

Equipment	Software Revision	Comments
Polycom HDX 4500	3.0.5-22695	Tested SIP and H.323.
Polycom VSX 7000e	9.0.6.2	Tested ISDN. ■ Encryption failed to establish. ■ Intermittent video freezing was observed.
Polycom VVX 1500	4.0.2.11307	Tested SIP and H.323.

Sony Endpoints

Equipment	Software Revision	Comments
Sony PCS-G50	2.72	Tested H.323, SIP to H.323 interworking, and ISDN. ■ In some configurations, H.263+ content on this endpoint may appear black over H.323 or non-existent over SIP to H.323 interworking.
Sony PCS-XG80	2.36	Tested SIP and H.323. Content from the endpoint was not tested. ■ When calling over SIP, this endpoint only supports the first audio and video codecs that it advertises. If the ISDN gateway chooses a different audio or video codec from the advertised set, the endpoint may not be able to decode the audio or video from the gateway. ■ In some circumstances, blank video may be observed when H.263 is negotiated. To workaround this, disable H.263.

Other Endpoints

Equipment	Software Revision	Comments
LifeSize Room 200	4.7.21	Tested SIP and H.323. ■ Encrypted SIP calls are not supported between the ISDN gateway and this endpoint. ■ G.722.1 Annex C is not supported on SIP calls between the ISDN gateway and this endpoint.
LifeSize Team	LS_TM1_4.7.22	Tested SIP and H.323.
Radvision Scopia XT1000	2.5.406	Tested SIP and H.323.

Infrastructure

Equipment	Software Revision	Comments
Cisco TelePresence Content Server	S5.3	Tested SIP and H.323.
Cisco TelePresence ISDN Link	IL1.0.0	Tested ISDN.

Updating to Version 2.2

Software Dependencies

In the case of the ISDN GW MSE 8321 blade, the Cisco TelePresence Supervisor MSE 8050 (Supervisor) blade must be running software Version 2.2 or later.

Prerequisites

The software upgrade process requires a hardware restart. Schedule a downtime window and notify users of when the service will be unavailable. The duration of an upgrade can be up to 25 minutes.

Have the following available and complete the backup processes described before you proceed to upgrade the software:

- New software package.
- Current software image file (in case you need to reverse the upgrade).
- Back up of the configuration (the configuration.xml file).
- You will require the administrator user name and password for the configuration backup file if you ever need to use the backup. If you attempt to downgrade / restore the software and you cannot load an appropriate configuration file, you may be unable to log in to the device.
- If you use Call Detail Records (CDRs), or any other logs, for billing, auditing or other purposes, you must download and save your logged data. When the device reboots as part of the upgrade, all existing CDRs will be deleted.
- Back up the audit logs. Unpredictable results will occur with the audit log files if you subsequently need to downgrade the software for any reason.
- Administrative access to all units to be upgraded.
- The model numbers and serial numbers of your devices in case you need to contact Cisco Technical Support.

CAUTION: Make sure that all the backup processes described in this section have been completed before you start the upgrade. Failure to do so could result in data loss.

Backup Configuration Instructions

Using the Web Interface

1. In a web browser, navigate to the web interface of the device.
2. Sign in as an administrator.
3. Go to **Settings > Upgrade.**
4. In the **Backup and restore** area, click **Save backup file**.
5. Copy the resulting *configuration.xml* file to a secure location.

Using FTP

1. Check that the device supports FTP and that the FTP service is enabled on the **Network > Services** page.
2. Connect to the device using an FTP client.
3. Log in as an administrator (use the administrator credentials that you would use to connect to the web interface).
4. Copy the *configuration.xml* file to a secure location.

CAUTION: You must remember the administrator user name and password for the configuration backup file in case you ever need to use the backup.

Upgrade Instructions

Using the Web Interface

1. Unzip the image file locally.
2. In a web browser, navigate to the web interface of the device.
3. Sign in as an administrator.
   The username is **admin** and there is no password on a new device.
4. Go to **Settings > Upgrade**.
5. In the **Main software image** section, locate the **New image file** field. Browse to and select the unzipped new image file.
6. Click **Upload software image**.
   The web browser uploads the file to the device, which may take a few minutes.

   Note: Do not browse away from the **Upgrade** page, or refresh the page, during the upload process—this will cause the upload to fail.

   A pop-up window displays to show upload progress. When complete, close the message. The web browser refreshes automatically and displays the message *Main image upload completed*.
7. Click **Shutdown N-port ISDN-IP gateway**. This option will now change to **Confirm N-port ISDN-IP gateway**. Click to confirm.
8. Click the **Restart N-port ISDN-IP gateway and upgrade** button. This button only appears in the **Upgrade** page during this process.

   The device will reboot and upgrade itself. This can take up to 25 minutes.

   Note: You may be logged out due to inactivity. If this happens, log in again, go to **Settings > Upgrade** and click **Restart N-port ISDN-IP gateway and upgrade**.
9. Go to the **Status** page to verify that the device is using the new version.
10. If necessary, restore your configuration. Refer to the online help for details.

Using FTP

1. Check that the device supports FTP and that the FTP service is enabled on the **Network > Services** page.
2. Unzip the image file locally.
3. Connect to the ISDN gateway using an FTP client.
4. Log in as an administrator (use the administrator credentials that you would use to connect to the web interface).
5. Upload the image file to the root.
6. Reboot the hardware after the upload.
   You can reboot via the **Upgrade** page on the web interface. The device upgrades itself when it restarts.
7. Log in to the web interface and go to the **Status** page to verify that the device is using the new version.
8. If necessary, restore your configuration. Refer to the online help for details.

Note: You can monitor the upgrade progress via the serial port.

Downgrade Instructions

If you need to reverse the upgrade, you can re-install the former version of the software. The downgrade procedure is the same as the upgrade procedure except you will use the earlier software image.

CAUTION: Make sure that all relevant backup processes described in Prerequisites have been completed before you start the downgrade. Failure to do so could result in data loss.

Long User IDs

Post-downgrade, any user IDs over 31 characters are displayed as “long_user_id” followed by a truncated MD5 hash of the long user ID. Long user IDs remain available if the device is subsequently upgraded again, and if necessary can be accessed in the meantime by downloading the configuration file and retrieving the “long_utf8_id” fields.

Software Dependencies

It is not possible to revert from Version 2.2(*n.nn*) to any software version earlier than Version 2.0(*n.nn*).

Downgrade Procedure

You need the correct version of the software and your corresponding saved configuration before you proceed.

1. Follow the upgrade procedure using the earlier software image.
2. Reboot the hardware and check the status via the web interface.
   The status report indicates the software version.
3. Restore your configuration from the saved XML file:
   a. Go to **Settings > Upgrade**.
   b. In the **Restore configuration** area, navigate to and select the appropriate *configuration.xml* backup file.
   c. Check the **User settings** check box.
   In this context, user settings include the **Advanced account security mode** and **Idle web session timeout** options configured on the **Settings > Security** page.
   d. If required, check the **Network settings** check box.
   In this context, network settings include the **Redirect HTTP requests to HTTPS** option configured on the **Settings > Security** page.
   e. Click **Restore backup file**.

   For more information, refer to the online help topic “Upgrading and backing up or restoring the ISDN gateway”.

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:

4. Type the product name in the **Search** field and click **Search**.
5. 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.

Technical Support

If you experience any problems when configuring or using the device, 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.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit http://www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

Document Revision History

Date	Description
October 2012	EFT release
November 2012	EFT2 release
January 2013	Release candidate
January 2013	First release for 2.2
January 2013	Revised to include resolved issues CSCue30768 and CSCty87845
October 2013	Maintenance release 1
May 2014	Maintenance release 2
October 2014	Maintenance release 3
May 2015	Maintenance release 4
September 2015	Maintenance release 5
June 2016	Maintenance release 6

Date	Description
March 2017	Maintenance release 7

Appendix A: Mutual Authentication Connections and Certificate Identity Requirements

Local Certificate

The ISDN gateway can have only one local certificate. In all cases where the gateway needs to present a certificate to another party, the gateway uses the certificate listed in the **Local certificate** section of the **Network > SSL certificates** page. The gateway ships with a default certificate which you should replace if you want to use the certificate for security purposes.

Your local certificate must be configured in such a way that it can be correctly identified by the remote party, whether the remote party is an HTTPS client of the ISDN gateway, an HTTPS server to which the gateway connects, or a SIP entity that either calls the gateway or is called by the gateway.

Connections that may Involve Certificate Exchange

Connection Type	Settings on **Network > SSL certificates** Page
Incoming SIP call (to ISDN gateway)	**Verification settings:** *Outgoing and incoming calls*
Outgoing SIP call (from ISDN gateway)	**Verification settings:** *Outgoing calls only* or *Outgoing and incoming calls*
Web interface user (to ISDN gateway)	**Client certificate security:** *Verify certificate*, *Certificate-based authentication allowed*, or *Certificate-based authentication required*
API user (to ISDN gateway)	**Client certificate security:** *Verify certificate*, *Certificate-based authentication allowed*, or *Certificate-based authentication required*
OCSP server (from ISDN gateway)	**Server certificate security:** *Verify certificate*
Feedback receiver (from ISDN gateway)	**Server certificate security:** *Verify certificate*

SIP TLS Connections and Certificate Identity Requirements

For the following secure SIP connection types, you should ensure that the ISDN gateway's local certificate, and any certificates presented to the gateway, can be identified and verified according to the following guidelines.

Outgoing SIP Calls (ISDN Gateway Acting as a Client)

The ISDN gateway performs a SIP TLS handshake with the called party, and the parties must be able to verify each other's certificates.

The ISDN gateway verifies that the received certificate is trusted by checking against its SIP trust store. The certificate must be signed by an authority that is in the gateway's SIP trust store.

The ISDN gateway identifies the owner of the certificate as follows:

- The gateway looks for either an IP address or a domain identifier for the remote party in the **`URI`** and **`DNS`** fields of the certificate's subject alternative name (**`subjectAltName`**) extension.
- If the **`subjectAltName`** is not present, the gateway looks for either an IP address or a domain identifier in the certificate's Common Name (**`CN`**) field.

Note: If you require TLS on non-proxied SIP calls from the ISDN gateway, the gateway's local certificate **must** identify the gateway by its IP address. This requirement arises because the remote endpoint will be establishing TLS connections directly to the gateway, which provides its IP address as its identity.

Incoming SIP Calls (ISDN Gateway Acting as a Server)

The ISDN gateway performs a SIP TLS handshake with the calling party, and the parties must be able to verify each other's certificates.

The ISDN gateway verifies that the received certificate is trusted by checking against its SIP trust store. The certificate must be signed by an authority that is in the gateway's SIP trust store.

HTTPS Connections and Certificate Identity Requirements

For the following secure HTTP connection types, you should ensure that the ISDN gateway's local certificate, and any certificates presented to the gateway, can be identified and verified according to the following guidelines.

Client Connections (ISDN Gateway Acting as a Server)

This applies when API users and web interface users connect to the ISDN gateway if those clients are required, by the gateway's configuration, to present certificates.

The ISDN gateway verifies that the received certificate is trusted by checking against its HTTPS trust store. The certificate must be signed by an authority that is in the gateway's HTTPS trust store.

If certificate-based login is allowed or required, the ISDN gateway also checks the received certificate's common name. If it matches with a stored username, then the client logs in as that user.

Server Connections (ISDN Gateway Acting as a Client)

This applies when the ISDN gateway connects to a feedback receiver or an OCSP server if those servers are required, by the gateway's configuration, to present certificates.

The ISDN gateway verifies that the received certificate is trusted by checking against its HTTPS trust store. The certificate must be signed by an authority that is in the gateway's HTTPS trust store.

The ISDN gateway identifies the owner of the certificate as follows:

- The gateway checks the **`DNS`** field of the certificate's subject alternative name (**`subjectAltName`**) extension for a domain identifier.
- If the **`DNS`** field is absent (or if the whole **`subjectAltName`** extension is absent), then the gateway will look at the common name for a domain identifier (IP address is not allowed in common name).
- The gateway also checks the **`IP address`** field of the certificate's **`subjectAltName`** extension, if present.

Appendix B: Transitioning to Certificate-Based Security

Certificate-based security methods carry a risk of inadvertently blocking all login access to the ISDN gateway. (If problems occur with the client certificate or the trust store, you will need to fall back to HTTP. If you cannot fall back—because HTTP is disabled or because HTTP to HTTPS redirection is set—then all access methods will be blocked.) To avoid this we strongly recommend that you follow the corresponding procedure below when implementing certificate-based security options:

- Enabling client certificates and certificate login (HTTPS connections)
- Enabling OCSP checking
- Requiring certificate-only login (all connections)

Enabling Client Certificates and Certificate Login (HTTPS Connections)

To transition access handling for HTTPS connections from standard, password-based access to required client certificate validation and optionally to allow certificate-based login, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the ISDN gateway (**Network > SSL certificates**) and that the web browser(s) to be used to access the ISDN gateway are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and disable **Redirect HTTP requests to HTTPS** (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
   a. Scroll to the **HTTPS trust store** section.
   b. Set **Client certificate security** to *Verify certificate* (to have client certificate validation but no certificate login) or *Certificate-based authentication allowed* (to have client certificate validation and to allow certificate-based login).
   c. Click **Apply changes**.
5. Now test that you are able to log in to the ISDN gateway over an HTTPS connection.
   a. First verify that you can log in using the standard password login mechanism.
   b. If you specified *Certificate-based authentication allowed* in the previous step, also verify that certificate-based login is working as expected. This step is recommended, although strictly not essential as *Certificate-based authentication allowed* mode still allows password login if certificate login fails.

Note: Provided that this procedure is successful, you can now disable HTTP (**Network > Services**) or enable redirection from HTTP to HTTPS (**Settings > Security**) if either are required by your configuration.

Enabling OCSP Checking

CAUTION: The ISDN gateway will only perform OCSP checking if client certificate security mode is enabled. To do this go to **Network > SSL certificates** and set the **Client certificate security** option. When you first enable OCSP checking, set **Client certificate security** to one of the 'lesser' modes (*Verify certificate* or *Certificate-based authentication allowed*). If you want to set it to *Certificate-based authentication required*, only do so after you have completed the procedure for Requiring certificate-only login (all connections) and you are certain that OCSP checking is working correctly.

To enable OCSP checking for the ISDN gateway, do the following:

1. Ensure that an appropriate HTTPS trust store has been installed on the ISDN gateway (**Network > SSL certificates**).
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable* **Redirect HTTP requests to HTTPS**. This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**.
   a. Scroll to the **Online certificate status protocol (OCSP)** section.
   b. Set **Certificate to check** to *HTTPS client certificates*.
   c. Enter the URL of the external OCSP server and set any options you require.
   d. Click **Apply changes**.
5. Now test that you are able to log in to the ISDN gateway over an HTTPS connection. Only proceed to the next step if you can successfully log in.
6. Do one of the following, as appropriate for your configuration:
   - Go to **Network > Services** and disable HTTP.
   - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.

Requiring Certificate-Only Login (All Connections)

To transition from password-based authentication to required certificate-based authentication for all connection types, do the following:

1. Ensure that an appropriate HTTPS trust store is installed on the ISDN gateway (**Network > SSL certificates**) and that the web browser(s) to be used to access the ISDN gateway are configured with a valid client certificate.
2. Go to **Network > Services** and enable both HTTP and HTTPS.
3. Go to **Settings > Security** and *disable* **Redirect HTTP requests to HTTPS** (uncheck the check box). This ensures that you can fall back to HTTP if problems occur.
4. Go to **Network > SSL certificates**:
   a. Scroll to the **HTTPS trust store** section.
   b. Set **Client certificate security** to *Certificate-based authentication allowed*.
   c. Do NOT set **Client certificate security** to *Certificate-based authentication required* yet.
   d. Click **Apply changes**.
5. Now test that you are able to log in to the ISDN gateway over an HTTPS connection *using a certificate*. Only proceed to the next step if you can successfully log in with a certificate.
6. Assuming the previous step succeeded, go to the **Client certificate security** option again and this time set it to *Certificate-based authentication required*.
7. Click **Apply changes** and confirm at the prompt.
8. It is now not possible to log in over HTTP. To log in over HTTPS requires a valid client certificate signed by a certificate authority, which matches the HTTPS trust store on the ISDN gateway.
9. Do one of the following, as appropriate for your configuration:
   - Go to **Network > Services** and disable HTTP.
   - Go to **Settings > Security** and enable **Redirect HTTP requests to HTTPS**.