# Cisco TelePresence ISDN Link

## Software Release Notes

D1498114

February 2020

# Contents

# Document Revision History

| Revision | Date | Description |
|---|---|---|
| 14 | 18th February 2020 | Release of IL1.1.11 |
| 13 | 7th January 2020 | Release of IL1.1.10 |
| 12 | 5th October 2018 | Release of IL1.1.9 |
| 11 | 12th June 2018 | Release of IL1.1.8 |
| 10 | 4th June 2018 | Updated Interoperability list |
| 09 | 13th December 2017 | Release of IL1.1.7 security patches |
| 08 | 14th June 2016 | Release of IL1.1.6 security patches |
| 07 | 23rd June 2015 | Release of IL1.1.5 security patches / FIPS fix |
| 06 | 22nd October 2014 | Release of IL1.1.4 for Shellshock |
| 05 | 16th July 2014 | Release of IL1.1.3 |
| 04 | 27th June 2014 | Release of IL1.1.2 |
| 03 | 2nd May 2014 | Release of IL1.1.1, fix for OpenSSL “Heartbleed” issue |
| 02 | 7th February 2013 | Release of IL1.1.0 |
| 01 | 23rd July 2012 | Initial release of IL1.0.0 |

# Introduction to ISDN Link Software

These release notes describe the features and capabilities included in the Cisco TelePresence ISDN Link software.

Cisco ISDN Link uses a FIPS approved cryptographic module and was found to be FIPS compliant through an independent compliance review.

The Telepresence ISDN Link software can be downloaded from http://www.cisco.com.

# Deferred software versions

A software version is deferred when we find critical issues within the software. This is to prevent users from downloading and installing affected software versions. Replacement software will always be in place before a software version is deferred.

## Software and deferral policy

Affected software versions with issues will be deferred on a regular basis from the download section on cisco.com to avoid providing potential vulnerable software after security fixes.

## IL1.1.10 is deferred

IL1.1.10 is deferred due to a checksum issue.

# New features and functionality in IL1.1.11

IL1.1.11 is released to correct a checksum error in IL1.1.10. No change in features and functionality from IL1.1.10 release as listed in “New features and functionality in IL1.1.10”.

# New features and functionality in IL1.1.10

There are no new features in this release. This is primarily a security fix release.

# New features and functionality in IL1.1.9

There are no new features in this release. This is primarily a bug fix release.

# New features and functionality in IL1.1.8

Upgraded to use OpenSSL 1.0.2o.6.2.238. There are no other new features in this release except bug fixes.

# New features and functionality in IL1.1.7

There are no new features in this release. This is a security release.

# New features and functionality in IL1.1.6

There are no new features in this release. This is primarily a security release.

# New features and functionality in IL1.1.5

There are no new features in this release. This is primarily a security release.

# New features and functionality in IL1.1.4

There are no new features in this release. This release is to primarily deal with the Shellshock Bash vulnerabilities CVE-2014-6271 and CVE-2014-7169.

# New features and functionality in IL1.1.3

Added support for H.264 Sample Aspect Ratio signalling.

# New features and functionality in IL1.1.2

IL1.1.2 is recommended to be used with TC7.2.0 on the paired codec. TC7.2.0 will be released in August 2014.

## Support for G.728 and G.729

G.728 and G.729 audio protocols support added in ISDN Link. The protocols must also be supported by the paired codec.

G.729 is supported by all codecs running TC 6.1.0 and later.

G.728 is supported by the following list of codecs running TC 7.2.0 and later:

- C90, SX20, MX200 G2, MX300 G2: Full support
- C40, C60, EX90: Only for point-to-point calls (not multisite)

## Down Speeding of Outgoing Calls

New configuration of xConfiguration H320 Downspeed: On/Off. This selects if ISDN Link can down speed current call(s) if all available bandwidth is in use, and another outgoing call is requested from paired codec.  The default setting is ON.

## Video Loopback modes

It is now possible for special test scenarios to enable video loopback on the PRI and BRI circuits.  Please see the admin guide for more information.  These modes are non-persistent, so after a restart of the ISDN Link they will be disabled.

# New features and functionality in IL1.1.1

There are no new features in this release, only fix from IL1.1.0 is for openSSL “Heartbleed” bug (CSCuo26686).

NOTE – Customers previously provided with IL1.1.1 Pre-Alpha 1 with a fix for third party interoperability issues please note that the fix in the pre-alpha is **not included** in this release. The interoperability issues will be addressed in the next release (IL1.1.2) to be released shortly.

# New features and functionality in IL1.1.0

## Automatic Pairing of ISDN Link and Endpoint (Requires TC6.0)

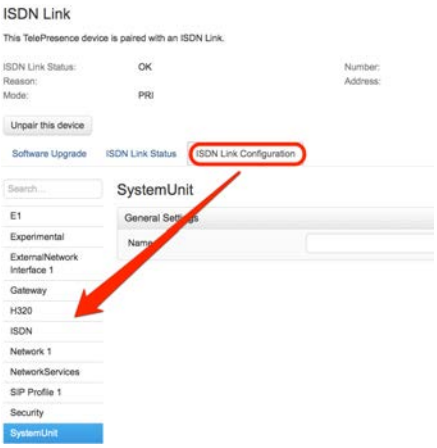
Previously there was a fair amount of manual configuration from the serial interface in order to setup the ISDN Link.

With IL1.1 and TC6.0 you can now connect an unconfigured ISDN Link and from the web interface of the endpoint search and pair with the ISDN Link (see ISDN Link Installation Guide 1.1 for more details)


## Configuration of ISDN Link from the Endpoint (Requires TC6.0)

Once you have paired the device with an endpoint you will now be able to configure the device from the web page of the endpoint.

Please see the ISDN Link Installation Guide for some typical examples of settings for various configurations.




## Software Upgrade Via Web Interface of Paired Endpoint (Requires TC6.0)

The ISDN Link can now be easily upgraded from the paired endpoint, using the web interface of the paired endpoint.

## Better Call Integration (Requires TC6.0)

With IL1.0/TC5.x you had to enter a complicated dial string in order to dial ISDN calls.  With IL1.1 and TC6.0 you now just enter the ISDN number to dial and then select the call as ISDN and the call rate and press call.

If primarily dialing through the ISDN Link you can set your default call to H.320 and default call rate to that desired on the endpoint web interface, then all you need to do is enter the number to dial and press Call.

See ISDN Link Installation Guide for more details on how to place calls.



## AAC-LD

AAC-LD is now supported with the ISDN Link in this release.

## Encryption

Encryption is now supported in this release.

## Favourites

Frequently dialled numbers can be stored in the favourites list.

**IL1.1.0 is recommended for use with TC6**.  It can still be used with older software using the previous manual pairing method but it is highly recommended to use it with TC6.0 (with new pairing method) to obtain the benefits of the new features providing enhanced usability and managability. Please see Upgrading from Previous Release IL1.0/TC5.x to IL1.1/TC6.0 Page - 21 if you are already using an ISDN Link with IL1.0.

For automatic pairing discovery and general operation the ISDN Link must be on the same network segment as the endpoint it will pair to. Recommended installation is for the endpoint that is to be used with the ISDN Link to be cabled directly into the ISDN Link via the dedicated port on the ISDN Link for the endpoint.

The new pairing method with TC6.0 and IL1.1 is known as automatic pairing as opposed to the previous pairing method known as manual pairing. If using a previous release you must upgrade and re-pair the ISDN Link and endpoint using the new method to obtain the benefits of all the new features. You can still use the ISDN Link in manual pairing mode.

# Upgrading ISDN link Software (From IL1.1.1)

Use the web interface of the paired endpoint to upload and apply the new software to the ISDN Link.

Login to the codec as admin then proceed to Configuration -> Peripherals -> Manage ISDN Link. Look for the Upload Software section on the webpage, then browse to the ISDN Link package (s51500il_1_1_x.pkg) and press upload. Once the package is uploaded press the Install button and the ISDN Link will install the software and reboot to apply the upgrade. This can take a couple of minutes so please wait for the message saying the ISDN Link was successfully upgraded.

To confirm the new software is applied, use the web interface of the paired codec and go to Configuration -> Peripherals and under ISDN Link you should see the software version that you uploaded.

# Upgrading from Release IL1.0.0/TC5.x to IL1.1.0/TC6.0

Note – for new installations please refer to the ISDN Link Installation Guide for pairing and configuration examples, this procedure is for previous installations using TC5.x and IL1.0.

The recommended method of upgrading from TC5/IL1.0 would be as follows:

1. Upgrade endpoint to TC6.0 (license key required)
2. Upgrade the ISDN Link from IL1.0 to IL1.1
    a. If your ISDN Link has IP connectivity to Internet then you can login as admin and enter the command:
        i. **xcom SystemUnit SoftwareUpgrade URL: "http://ftp.tandberg.com/pub/software/endpoints/isdnlink/il1/s51500il1_1_0.pkg" UserName: "" password:""**
        ii. Nothing should happen while the file is downloaded, then the ISDN Link will restart.
        iii. Confirm that the ISDN Link has been updated when it restarts, login as admin and enter **xstat sys soft** and confirm you have IL1.1.
    b. If no Internet access you can download the file to a local computer and use scp to copy the file onto the ISDN Link:
        i. You need to enable root if not already enabled. Login as admin on ISDN Link and enter **systemtools rootsettings on [PASSWORD]** where PASSWORD is the password you want – Please set a password!
        ii. use WinSCP or scp to copy the IL1.1 file to /appl/installsw
            - example for scp
                a. **scp s51500il1_1_0.pkg root@ip.address.of.isdnlink:/appl/installsw**
            - Using WinSCP (Windows)
                a. Connect as root using SCP to ISDN Link
                b. Drag and drop the file from local(left) drive into the /appl folder on the ISDN Link
                c. You will now get a dialogue box saying **/appl/*.*** change the ***.*** to **installsw** so you see this -> **/appl/installsw**
                d. You will be asked to confirm to overwrite file

e. When finishes you will get an error message. Press OK. The file has been copied OK even though file size is 0.

iii. reboot the ISDN Link (**reboot** as root or **xcom boot** as admin)

iv. Confirm the ISDN Link has been updated to IL1.1, by logging in as admin after it restarts and enter **xstat sys soft**

v. You can now disable root access on ISDN Link by logging in as admin and using command **systemtools rootsettings off**

3. Now the ISDN Link will be on IL1.1 and endpoint on TC6.0 but still in manual pairing mode.
4. To enable the auto pairing mode (will give you access to the new feature allowing for easy dialing and management from TC6 endpoint) login to ISDN Link as admin and enter the command **xConfiguration Gateway PairingMode: Auto**
5. You will get a red alarm on the ISDN Link (it now has lost connection to endpoint)
6. Now follow the steps shown in the ISDN Installation Guide for IL1.1 for information on how to pair the endpoint and ISDN Link and how to place calls.

From this release onwards (once you have re-paired the ISDN Link and endpoint) you will now upgrade the software on the ISDN Link using the web interface of the paired endpoint – no more need for SCP.

# Resolved Issues in IL1.1.10

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCvo28194 | Cisco Telepresence Endpoint Command Shell Injection Vulnerability identified by CVE(s): CVE-2019-1878 |
| N.A | SSH - Add support for new preferred cipher codes |
| N.A | Include security updates (OPENSSL, TAR, NTP, CURL) |

# Resolved Issues in IL1.1.9

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCvm75614 | FIPS mode support in ISDNLINK not working |

# Resolved Issues in IL1.1.8

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCvj83061 | Codec/ISDNLINK SIP leg will not always be encrypted or Call failure |

# Resolved Issues in IL1.1.7

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCvc94656 | OpenSSL identified by CVE(s): CVE-2017-3731 CVE-2017-3730 CVE-2017-3732 |
| CSCvd72203 | NTPd security vulnerabilities identified by CVE(s): CVE-2016-9042, CVE-2017-6464, CVE-2017-6462, CVE-2017-6463, CVE-2017-6455, CVE-2017-6452, CVE-2017-6459, CVE-2017-6458, CVE-2017-6451, CVE-2017-6460, CVE-2015-8138, CVE-2016-7431 |
| CSCvb48612 | OpenSSL identified by CVE(s): CVE-2016-6304 CVE-2016-6305 CVE-2016-2183 CVE-2016-6303 CVE-2016-6302 CVE-2016-2182 CVE-2016-2180 CVE-2016-2177 CVE-2016-2178 CVE-2016-2179 CVE-2016-2181 CVE-2016-6306 CVE-2016-6307 CVE-2016-6308 CVE-2016-6309 CVE-2016-7052 |
| CSCvf01522 | OpenSSL identified by CVE(s): CVE-2017-3731 CVE-2017-3730 CVE-2017-3732 |
| CSCvh14064 | NTPd security vulnerabilities identified by CVE(s): CVE-2016-9311, CVE-2016-9310, CVE-2016-7427, CVE-2016-7428, CVE-2016-9312, CVE-2016-7431, CVE-2016-7434, CVE-2016-7429, CVE-2016-7426, CVE-2016-7433 |

| CDETS ID | Summary |
|---|---|
| NoRef | OpenSSL identified by CVE(s): CVE-2016-7054, CVE-2016-7053, CVE-2016-7055 |
| CSCvh14081 | OpenSSL identified by CVE(s): CVE-2016-6304 CVE-2016-6305 CVE-2016-2183 CVE-2016-6303 CVE-2016-6302 CVE-2016-2182 CVE-2016-2180 CVE-2016-2177 CVE-2016-2178 CVE-2016-2179 CVE-2016-2181 CVE-2016-6306 CVE-2016-6307 CVE-2016-6308 CVE-2016-6309 CVE-2016-7052 |
| NoRef | NTPd security vulnerabilities identified by CVE(s): CVE-2016-4957, CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956 |

# Resolved Issues in IL1.1.6

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCuz52446 | OpenSSL issues - CVE-2016-2108 CVE-2016-2107 CVE-2016-2105 CVE-2016-2106 CVE-2016-2109 CVE-2016-2176 |
| CSCuy34865 | Vulnerability in as glibc and identified by CVE-2015-7547 |
| CSCux95136 | NTPd security vulnerabilities affecting all versions of NTPd 4.x |
| CSCva05478 | Codec takes around 60 seconds to restore video after hold/resume |

# Resolved Issues in IL1.1.5

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCut45963 | Fix for CVE-2015-0204 and CVE-2015-0286. |
| CSCus42828 | Fix for CVE-2015-0205. |
| CSCus31382 | OpenSSL security fix CVE-2014-3567 |
| CSCus27280 | NTPd.org Vulnerabilities |
| CSCuu97161 | Enabling FIPS mode causes cyclic reboot |

Related Fix in TC7.3.3

| CDETS ID | Summary |
|---|---|
| CSCut79607 | Codec in FIPS mode will not pair with ISDN Link |

# Resolved Issues in IL1.1.4

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCur05025 | Fix for Shellshock - CVE-2014-6271 and CVE-2014-7169 |
| CSCuq01874 | Callee change audio codec on session refresh with ISDN Link (low bandwidth calls) |

# Resolved Issues in IL1.1.3

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCup91619 | Added support for h.264 SampleAspectRatio signalling for ISDN Link |

# Resolved Issues in IL1.1.2

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCup63973 | No Video received from Skopia MCU/Radvision B40 GW |
| CSCui42670 | Customer has to enable capset filter to get access to RMX conference |
| CSCuo23422 | ISDN Link feature for BRI/PRI E1/T1 loopback for troubleshooting |
| CSCup64012 | Not allowing to make outgoing BRI call unless one (or more) interfaces are active on L1 |
| CSCue73049 | Enabling SIP outbound cause registration failure |
| CSCug68580 | Add capability to down speed the call |
| CSCup64029 | Add support for G.729 audio protocol |
| CSCuo04038 | Unmute on ISDN call can take up to 8 seconds to hear audio |
| CSCun68244 | Presentation Issues between SX20 - ISDN Link to Polycom VSX |
| CSCup64059 | SIP log output could be incomplete |

| CDETS ID | Summary |
|---|---|
| CSCup23978 | Fix latest vulnerabilities in OpenSSL |
| CSCuo41275 | BFCP Token Issue - Presentation not seen or sent in main |

# Resolved Issues in IL1.1.1

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCuo26686 | The Cisco TelePresence ISDN Link includes a version of openssl that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160 aka “Heartbleed” |

# Resolved Issues in IL1.1.0

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

• Internet connection

• Web browser

• Cisco.com user ID and password

To use the Bug Search Tool, follow these steps:

**Step 1** To access the Bug Search Tool, go to http://www.cisco.com/cisco/psn/bssprt/bss

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field, then click **Go**.

ISDN Link

| CDETS ID | Summary |
|---|---|
| CSCud31836 | Incoming calls with microphone muted on calling system caused a crash on ISDN Link |
| CSCub66283 | Noise during negotiation with Polycom RMX bridge |
| CSCub78084 | Video refresh, freeze, and black screen calling through ISDN GW |
| CSCuc76025 | Incoming call from a mobile one way audio (inbound to ISDN Link) only – **Requires IL1.1/TC6.0** |

# Known limitations

| Reference ID | Equipment | Summary |
|---|---|---|
| CSCun31807 | ISDN Link | The ISDN Link does not support FECC (Far End Camera Control) |
| CSCun95177 | PBX/Service Provider - BRI | BRI Lines need to be configured to Point to Multi-point lines and not Point to Point lines in the PBX or from service provider. |
| NA | Paired Endpoint / ISDN Link | All communication between the ISDN Link and Endpoint is done using IPv6. Do not disable IPv6 on the endpoint (Will see a warning if paired to ISDN Link) |
| NA | ISDN Link / Endpoint | Calls via the ISDN Link will cause a SIP call to be placed from endpoint to the ISDN Link, which is connected immediately. There will be some delay in the ISDN Link establishing the external (ISDN/Net) call. During this period the endpoint will receive no audio/video and just show a black image until connection is established to the far end.<br>**This is improved in TC6.0/IL1.1.** |
| NA | ISDN Link | With encryption enabled the maximum number of calls possible (video or audio) is reduced from three to two |

| | | |
|---|---|---|
| NA | ISDN Link | The dialling method is quite complex with TC5.x/IL1.0.<br>**Resolved with TC6.0/IL1.1 in auto-pair mode.** |
| NA | ISDN Link | The ISDN Link has no web interface or management functionality.<br>**With TC6.0/IL1.1, the ISDN Link is now managed via the web interface of the paired endpoint.** |
| | ISDN Link | When enabling FIPS mode on the endpoint please unpair the ISDN Link from the codec first. Enable FIPS on the codec which cause a factory reset. Then setup the codec as required (enable FIPS on the ISDN Link if required) then pair the two together again. |

# Interoperability

The systems below have been tested and verified with this software release.

## Endpoint Interoperability (Pairing)

| Equipment | Software revision | Protocol | Comments |
|---|---|---|---|
| C20, C40, C60, C90, SX20, SX80, MX200 (G1 and G2), MX300 (G1 and G2), EX60, and EX90 | TC7.3.12 | SIP | Use TC7.3.12 and above with IL1.1.7 and above |
| All cisco endpoint devices that supports CE9.3.0 onwards | From CE9.3.0 | SIP | IL1.1.7 onwards, supported from CE9.3.0 |

# References and related documents

The following table lists documents and web sites referenced in this document. All product documentation can be found on our web site.

| Name | Document reference |
|---|---|
| Cisco website | http://www.cisco.com |
| Cisco Software Download | http://www.cisco.com/cisco/software/navigator.html?i=!ch |
| Cisco TelePresence User Documentation | http://www.cisco.com/go/telepresence/docs |

## Software filename

The correct software filename is listed in the following table.

| Cisco ISDN Link | Software for ISDN Link | Release ID |
|---|---|---|
| AES Encryption | S51500il_1_1_11.pkg | 0862ce5 |
| AES Encryption | S51500il_1_1_10.pkg | 257e8dd |
| AES Encryption | S51500il_1_1_9.pkg | 6a01202 |
| AES Encryption | S51500il_1_1_8.pkg | ae9f13e |
| AES Encryption | S51500il_1_1_7.pkg | 65cc814 |
| AES Encryption | S51500il_1_1_6.pkg | a337554 |
| AES Encryption | S51500il_1_1_5.pkg | cf982a9 |
| AES Encryption | S51500il_1_1_4.pkg | c6ff645 |
| AES Encryption | S51500il_1_1_3.pkg | 1673c43 |
| AES Encryption | S51500il_1_1_2.pkg | 5c0564b |
| AES Encryption | S51500il_1_1_1.pkg | 2c65b7d |
| AES Encryption | S51500il_1_1_0.pkg | 247d2f9 |
| AES Encryption | S51500il_1_0_0_.pkg | 287829 |

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.



NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.