Release Notes for Cisco TelePresence System Software Release IX 9

First Published: 2018-08-22

Last Modified: 2022-03-14

Release Notes for Cisco TelePresence System Software Release IX 9

These release notes describe new features, and open and closed hardware and software caveats for the Cisco TelePresence System Software Release IX 9. The Cisco TelePresence System IX5000 and IX5200 use this software.

A copy of the source code used in this product that is licensed under the General Public License Version 2.0 can be obtained by emailing a request to cts-gpl@cisco.com.

New in Release IX 9.1.4

There are no new features in this release. This release provides bug fixes only.

See the Unresolved Caveats in Release IX 9.1.4, on page 11 for a list of the unresolved caveats for this release.

See the Resolved Caveats in Release IX 9.1.4, on page 11 for a list of the resolved caveats for this release.

New in Release IX 9.1.3

There are no new features in this release. This release provides bug fixes only.

See the Unresolved Caveats in Release IX 9.1.3, on page 12 for a list of the unresolved caveats for this release.

See the Resolved Caveats in Release IX 9.1.3, on page 12 for a list of the resolved caveats for this release.

New in Release IX 9.1.2

There are no new features in this release. This release provides bug fixes only.

See the Unresolved Caveats in Release IX 9.1.2, on page 13 for a list of the unresolved caveats for this release.

See the Resolved Caveats in Release IX 9.1.2, on page 13 for a list of the resolved caveats for this release.

New in Release IX 9.1.1

The following feature is new in this release:

- TMS High Mode Support, on page 2

See the Unresolved Caveats in Release IX 9.1.1, on page 16 for a list of the unresolved caveats for this release.

See the Resolved Caveats in Release IX 9.1.1, on page 17 for a list of the resolved caveats for this release.

TMS High Mode Support

From IX 9.1.1 onward, TMS can add IX endpoints in high mode as well. The CA signed certificates required by the TMS server which is running on high mode needs to be uploaded as a service certificate in IX web UI. After the uploaded certificate is selected, both the IX web UI and calendaring service will start using the same CA signed certificate for authentication purposes.

New in Release IX 9.1.0

There are no new features in this release. This release provides bug fixes only.

Note IX Release 9.1.0 first published on Cisco.com on 14-Jun-2019.

The IX 9.1.0(3) release with enhanced security causes connectivity issues between the existing TMS and IX solution. The existing TMS must be updated to match the enhanced security in IX 9.1.0(3). The TMS team is working on CSCvq22807 to address the issues. Therefore, IX 9.1.0(3) is removed from Cisco.com, and is replaced with IX 9.1.0(4) to keep the existing solution intact.

We will release an enhanced security version of IX with TMS upgrade as a solution in the near future.

See the Unresolved Caveats in Release IX 9.1.0, on page 19 for a list of the unresolved caveats for this release.

See the Resolved Caveats in Release IX 9.1.0, on page 20 for a list of the resolved caveats for this release.

New in Release IX 9.0.1

There are no new features in this release. This release provides bug fixes only.

See the Unresolved Caveats in Release IX 9.0.1, on page 22 for a list of the unresolved caveats for this release.

See the Resolved Caveats in Release IX 9.0.1, on page 22 for a list of the resolved caveats for this release.

New in Release IX 9.0.0

The following features are new in this release:

- Active Control Feature, on page 3
- New CLI Commands, on page 3
- New Display Firmware, on page 3

See the Unresolved Caveats in Release IX 9.0.0, on page 26 for a list of the unresolved caveats for this release.

See the Resolved Caveats in Release IX 9.0.0, on page 27 for the list of resolved caveats for this release.

Touch 10 User Interface Update

In IX 9.0.0, a new release of Touch software has been added, which contains Touch10 device bug fixes and the user interface changes. With IX 9.0, Touch10 control device for IX series video systems provides a new look and feel experience, in line with other Cisco video systems. The Touch10 user interface screen panels and the icons now look similar to MX and SX Series Endpoint's Touch device.

Active Control Feature

Active Control allows conference participants to administer a conference on the Cisco Meeting Server using the video system's interfaces.

Each user can see the participant list, change the video layout, disconnect participants, and so on, from the interface.

The following functions have been added as part of the Active Control feature implementation on IX5000; no other active control functionalities are currently supported.

- Participant List Display on the Touch Device
- Handling audio mute and unmute requests from remote

With Active Control enabled, IX gets a participant list from remote that shows all meeting participants and IX pushes this list to display on the Touch device. This list updates dynamically, based on the participant join and drop from meeting.

In a CMS hosted conference with the active control feature enabled, the conference resource can send mute and unmute messages to IX5000 endpoints, based on admin or other participants actions.

When IX5000 gets a MUTE request, the microphones are muted and the microphone LEDs are turned RED. In addition to this, the MUTE icon and the appropriate text are displayed on the main center display. IX users can unmute themselves if they want.

In the case of an UNMUTE request from remote, IX5000 is not unmuted directly. A message shows up on the center display screen to request that the user unmute the audio locally.

New CLI Commands

The following CLI commands have been added in this release:

- set activecontrolmode
- show activecontrolmode

For more information, see the *Command-Line Interface Reference Guide for Cisco TelePresence Immersive Systems*, located here: https://www.cisco.com/c/en/us/support/collaboration-endpoints/ix5000-series/products-command-reference-list.html

New Display Firmware

In IX 9.0.0, new Display Firmware, **51.01.04**, has been included with the improvements to address the black screen issues. As per IX Escalation data, unstable power can cause the display to stick in an unknown state, and no video displays on the screen. Display Firmware, **51.01.04**, prevents the displays from getting into an unknown state.

Important Notes for IX Software Releases

See the following sections for important notes about IX software releases.

IX5000 9.1.4 COP file installation on CUCM

Starting in IX5000 Release 9.1.4 the COP files will have a `.sha512` extension in their names instead of the `.sgn` extension. The IX5000 9.1.4 COP file, **cmterm-IX.9-1-4-5R-K9.P3.cop.sha512**, is signed with a new signing key. During COP file installation on CUCM14SU1 and above select

cmterm-IX.9-1-4-5R-K9.P3.cop.sha512. If you are installing 9.1.4 COP file on CUCM versions prior to 14 you may need to install the **ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn** COP file first. See the enable COP readme for specifics on versions that contain the 2021 native signing key.

https://www.cisco.com/web/software/282204704/18582/ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn-COP-Readme.pdf

If the current active CUCM version does not contain a new native signing key, it will be necessary to install the **ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn** COP file first if it has not been installed previously. If the new signing key is not present on CUCM, a **No valid upgrade options were found** or **The selected file is not valid** error will be displayed when trying to install 9.1.4 COP file.

In the case IX system with preloaded version of IX software 8.1.0 and planning to register IX system on CUCM 14.0 SU1 or above, then it is recommended to go with step (8.1.0 -> 8.2.0 -> 8.3.1.1 -> 9.0.0 -> 9.1.3 -> 9.1.4) using available SHA512 signed images on cisco.com instead of direct upgrade from 8.1.0 to 9.1.4.

IMMEDIATE IX SOFTWARE UPGRADE REQUIRED

FOLLOW ALL STEPS IN THIS SECTION AFTER YOU PHYSICALLY INSTALL YOUR SYSTEM

Your IX system comes preloaded with a downrev version of IX software. You must upgrade your system to the latest version on Cisco.com before you use your system to place and receive calls.

Preinstallation Requirements

Due to some issues with the preloaded software, make the following changes to your system before you load the software (requires signing in to Unified CM and the IX system administration GUI):

- Make sure that a Certificate Trust List (CTL) is not present on your system and, if present, delete it. To check, after initial system boot, log in to the IX System administration GUI using the IP address (default username and password is admin / cisco), navigate to **Configuration** > **Call Control Manager**, and click **Delete Certificate Trust List**. For more information, see the "Certificates" section of the "Understanding the Fields In the Interface" section of the *Administration Guide for Cisco TelePresence Software Release IX 8*.

Tip: Some browsers do not allow you to navigate directly to the Configuration page. If you have any problems, click **Monitoring**, then click **Configuration**.

After you perform the preceding changes, but before you begin first-time set up, you must download the latest IX software version from Cisco.com and load it to your IX system from this link (cisco.com log in ID required):

https://software.cisco.com/download/navigator.html

Navigate to the IX release software using the path **Products** > **Collaboration Endpoints** > **TelePresence IX 5000 Series** and select the model for your system. On the Download Software page, select the latest release.

While the system software is upgrading for the first time, you might see the following symptoms, which do not indicate a problem:

- The progress bar might freeze.
- The system reboots several times.
- The screen changes from the blue progress screen, with progress bar, to a blank screen.

Do not perform any corrective actions, and wait for the upgrade to complete.

For general information about adding the software to Unified CM and upgrading the software, see the "Configuring Cisco Unified Communications Manager for Your Cisco TelePresence System" section of the *IX5000 and IX5200 First-Time Setup* document.

Required Pre- and Post-Installation Steps

To make sure that Touch 10 devices initialize properly, you must perform all steps as described in the "Preventing Touch 10 Bootup Issues" section of the *IX5000 and IX5200 First-Time Setup* document. Failing to perform these steps could cause your Touch 10 devices to become inoperable.

Note Before you start the first-time setup, you must disable Proximity for the Touch 10 devices. For more information, see CSCvk42541 in Unresolved Caveats in Release IX 9.0.0, on page 26.

Unified CM Device Pack Requirements

Make sure that your Unified CM software has the minimum required device pack version.

- The minimum device pack version for 9.1.2 is 9.1(2.13063)
- The minimum device pack version for 10.5 is 10.5(1.12016).

Older versions for these Unified CM releases do not have the Cisco TelePresence IX5000 as a device type.

For device package compatibility, see the Cisco Unified Communications Manager Device Package Compatibility Matrix: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html

Tip: For an IX5200, configure the device type as Cisco TelePresence IX5000 (18 seats).

Proximity-Based Content Sharing Support

Note The **Proximity Share From Clients** enable option is not available on CUCM versions prior to 10.5.2.

The following table shows the Cisco Unified CM device pack version required to enable or disable "Proximity Share To Clients" on the Cisco Unified CM.

Unified CM Version	Device Pack Version
12.0.1	12.0.1.22022
11.5.1	11.5.1.16083
11.0.1	11.0.1.25097
10.5.2	10.5.2.18155
9.1	Not available

Required Pre- and Post-First Time Setup (FTS) Steps

Make sure that proximity service is disabled on the IX5000 system before the start of FTS. This prevents the connection of proximity-app devices (laptop or mobile) to IX5000 systems during FTS. Proximity service can be enabled or disabled from Touch 10 devices.

To disable, click the **settings** icon on the Touch 10 device, located at top left corner, and then change **Intelligent Proximity** mode to off.

After the completion of FTS, proximity service has to be enabled to use proximity feature for content sharing.

System Behavior During Times of Network Congestion

Anything that degrades network performance can affect Cisco TelePresence voice and video quality and, in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks such as an internal port scan or security scan
- Attacks that occur on your network, such as a denial-of-service attack

To reduce or eliminate any adverse effects to a TelePresence conference, schedule any administrative network tasks during a time when the Cisco TelePresence system is not being used, or exclude TelePresence systems from the testing.

Jitter and Packet Loss Statistics Include IX System Statistics

When you view network jitter statistics on the Touch 10, and network jitter and latency statistics in the system logs, note that these numbers include jitter and latency statistics that are internal to your IX system as well as for your overall network.

Downgrade the Software

IX software downgrades through Unified CM aren't supported. The following limitations apply:

- Using the Swap Loads operation in the Unified CM Device Defaults Configuration to downgrade is not supported.
- Keeping a version lower than the current Active/Inactive version of your phone load might create issues with registration and the IX WebUI.
- You can only switch the IX software version to the version stored on the inactive partition on the IX system. Typically, this is the version immediately prior to the release version being used.

To switch your IX system to the down rev version stored on the inactive partition, perform the following steps.

Procedure

Step 1 Use SSH to start a CLI session on your IX system.

Step 2 Enter the show version command to verify the IX software versions that are stored in the active and inactive partitions.

Example

The example below shows the IX software versions where IX 8.1.1 is stored in the active partition and IX 8.1.0.1 is stored in the inactive partition.

admin: **`show version`**

```
Active: IX 8.1.1(59) P3 2016-03-19 13:01:17
Inactive: IX 8.1.0.1(11) P3 2015-12-16 13:50:22
loads file information
Active (cmterm-IX8-1-1-59R-K9.P3)
IX: IX.8-1-159R-K9.P3.deb.SPA
Touch: CTSDEV10-442-11-0-1KKPL-112.pkg
Inactive: (cmterm-IX.8-1-0-1-11R-K9.P3)
IX: IX.8-1-0-1-11R-K9.P3.deb.SPA
Touch: CTSDEV10-442-11-0-1KKPL-112.pkg
```

To downgrade, you need to switch the active and inactive partitions so that the older software version is in the active partition.

Step 3 In Unified CM, enter **Device** > **Phone**.

Step 4 Search for Device Type and specify the search criteria as “contains” and specify “IX5000” in the search text. Click **Find**.

Step 5 Click on the Device Name for the IX system.

Step 6 In the **Device Information** area, change the Phone Load Name to a dummy name. This prevents the IX system from booting, allowing access to change the software version. Click **Save**.

You must change the Phone Load Name to a dummy name. Note that removing the Phone Load Name and leaving the field name blank will not work.

Step 7 Reenter the CLI session on your IX system.

Step 8 Enter the **`utils system switch-version`** command to switch the inactive partition to the active partition.

The IX software version stored in the inactive partition now becomes the version used for the active phone load.

Example

admin: **`utils system switch-version`**

```
Switching to Inactive Image: IX 8.1.0.1(11) P3 2015-12-16 13:50:22
Are you sure you want to switch the system, this will cause a system reset
Enter “yes” to switch and restart or any other key to abort
continue:
```

Step 9 Enter the show version command again to verify that the downgraded software version is now in the active partition.

Example

The example below shows the IX software versions where IX 8.1.0.1 is now stored in the active partition and IX 8.1.1 is stored in the inactive partition.

admin: **`show version`**

```
Active: IX 8.1.0.1(11) P3 2015-12-16 13:50:22
Inactive: IX 8.1.1(59) P3 2016-03-19 13:01:17
loads file information
Active (cmterm-IX.8-1-0-1-11R-K9.P3)
IX: IX.8-1-0-1-11R-K9.P3.deb.SPA
Touch: CTSDEV10-442-11-0-1KKPL-112.pkg
Inactive: (cmterm-IX8-1-1-59R-K9.P3)
```

```
IX: IX.8-1-159R-K9.P3.deb.SPA
Touch: CTSDEV10-442-11-0-1KKPL-112.pkg
```

Step 10 Exit the CLI session and reenter the Unified CM interface.

Step 11 (Optional) Return to the **Device Information Area** for the IX system. Change the Phone Load Name from the dummy name to the IX software version now stored in the active partition on the system. Click **Save**.

Step 12 Repeat this procedure for each IX system that you want to downgrade.

Software Compatibility with Other Devices

For information about compatibility with other systems, see the *Cisco TelePresence IX System Software Compatibility* document at https://www.cisco.com/c/en/us/td/docs/telepresence/ix_sw/compatibility/ix5k_b_ix-sw-compatibility.html.

Exceptions with Other Cisco Devices

Presentation Sharing While in a Multipoint Call

During multipoint calls when using TelePresence Server and TelePresence Conductor, resource optimization can cause presentation sharing to downgrade from 1080p resolution at 30 fps (1080p 30) to 1080 5 fps. This condition can cause video from a whiteboard presentation to look jerky.

In addition, TelePresence Conductor must be configured to enable 1080p30 (1920 tokens on conductor) (CSCur22200).

Exceptions with Third-Party Endpoints

No exceptions found.

Important Notes for IX System Hardware

See the following sections for important notes about IX system hardware.

Table Furniture Care

The IX system table surface is made with top-grade natural wood. The table surface is not scratch resistant. Please treat the table surface with care as delicate furniture. When retracting or returning the presentation cable, the three-headed adapter should not be pulled across the table top because this can scratch the surface.

Note Once the table has been delivered and accepted, it is the customer’s responsibility to take care and maintain the look of the table surface. Cisco will NOT be responsible for damages due to negligence or improper care.

Supported IX Auxiliary Devices

This section contains auxiliary devices that can be used with the IX systems.

The Cisco TelePresence system works best when suitable devices are attached using good quality cables and connectors. Cisco does not supply the cable that connects auxiliary devices to the codec.

Displays

This section describes the display choices you have with your Cisco TelePresence System.

Qualified Cisco Displays

The following displays are qualified for use with Cisco TelePresence System running IX software:

- 42-inch display, part number CTS-5K-DISP42 (Spare is CTS-5K-DISP42=)

  Note The release notes previously reported that the 42-inch display, part number CTS-MON-42-WW is a qualified Cisco display. This part number is not a qualified Cisco display for the IX system.

- 55-inch display, part number CTS-MON-55-WW

  Note HDMI-to-HDMI cables are not supported for display connections to the IX codec. You must use the HDMI-to-DVI cable for the displays (DVI on the display side). Some versions of the 55-inch display do not include a DVI input; use the included DVI-to-HDMI adapter to connect cables to the HDMI input on the display.

Cisco has supported two different 55-inch displays from the following vendors:

- Sampo

  The Sampo display is currently available.

- Samsung LH55MECPGGC/ZA

  The Samsung display is no longer available.

If using the Samsung display, before use, turn off all on-screen display (OSD) capability (see Turn Off On-Screen Display, on page 9). This prevents the display from showing messages after you stop sharing a presentation. If using the Sampo display, OSD capability is disabled by default.

Turn Off On-Screen Display

To turn off OSD on the Samsung display, complete the following steps using the remote control that comes with the system, or use the joystick control on the back of the display.

Procedure

Step 1 Turn the display on.

Step 2 Press **MENU** on the remote, or press the center of the joystick and move the joystick to select the menu option (the choice on the left), to bring up the menu for the display.

Step 3 Using the up and down arrows, navigate to System in the menu panel.

Step 4 Press **Enter** if using a remote, or press the center of the joystick if using the joystick on the display, to select the System choice.

Step 5 Using the up and down arrows, navigate to General and press either **Enter** on the remote, or the center of the joystick on the display.

This choice does not appear initially. Scroll down to see it.

Step 6 Navigate to **OSD Display** and press **Enter** or the center of the joystick.

Step 7 Set all three OSD choices (Source OSD, No Signal OSD, and MDC OSD) to Off (the default is On) to disable OSD messages.

Step 8 Press **EXIT** on the remote, or move the joystick to the previous menu choices, until the menu no longer displays.

Use of Nonqualified Displays with Your IX System

Cisco does not support nonqualified displays with your IX system. If you are using a nonqualified display with the IX system, unforeseen issues and adverse failures can result. When troubleshooting, Cisco and Cisco TAC will request that nonqualified auxiliary displays be disconnected to isolate system-related issues.

Document Cameras

The following WolfVision document cameras (object cameras) have been tested for use with IX systems:

- Model: EYE-12, Version: V1.30b
- Model: VZ-C6, Version: V1.35a
- Model: VZ-C12-3, Version: V1.25c

Note You cannot control the document camera using the Touch 10 interface. Use the remote control that is provided with the document/object camera.

LCD Displays and Viewing Angle

Since the IX5000 uses LCD displays instead of the plasma displays used in earlier CTS/TX immersive systems, the display quality may be reduced from some viewing angles. Viewing angles from the side are typically affected. If there is poor lighting in the room and the user is looking across the displays of the IX, the colors can change across screens. This is a normal property of LCD displays.

Hot Swapping of IX Components Not Supported

Hot swapping of IX system components is not supported. Before swapping out components, you must shut the system down, then restart it after the new components are installed.

Systems Cannot be Connected to a Router

Be sure that you connect your TelePresence system to a switch; this device cannot be directly connected to a router.

The router is not capable of creating Virtual Local Area Network (VLAN), which is required in the network design for the Cisco Voice and Video Solution. Please check the *Cisco Video and TelePresence Architecture Design Guide* as your reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/videodg/vidguide/infrastr.html

Software Agreements and Licensing

For complete software licensing information, access the **Software Licensing Information** page on Cisco.com at the following link:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/ix5000-series/products-licensing-information-listing.html

Caveats in Release IX 9

View Caveats

You can use the Cisco Bug Search Tool to find information on open and resolved issues for the Cisco TelePresence IX5000 Series, 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.

The Bug Search Tool help pages have further information on how to use the Bug Search Tool.

Procedure

Step 1 In your web browser, go to the Bug Search Tool.

Step 2 Sign in with a Cisco.com user ID and password.

Step 3 Do one of these things:

- Enter the bug identifier in the Search field and click **Search**.
- In the Product field type `Cisco TelePresence IX5000 Series` and specify the release you want to search.

Step 4 Filter the bug list using the **Modified Date**, **Status**, and **Severity Rating** drop down lists.

Unresolved Caveats in Release IX 9.1.4

For more details on bugs, enter the Cisco Identifier into the search field of the Bug Search Tool.

Table 1: Unresolved Caveats in Release IX 9.1.4

Sl. No.	Cisco Identifier	Headline
1	CSCvh45762	IX5000 not accessible, got into hung state.

Resolved Caveats in Release IX 9.1.4

For more details on bugs, enter the Cisco Identifier into the search field of the Bug Search Tool.

Table 2: Resolved Caveats in IX 9.1.4

Sl. No.	Cisco Identifier	Headline
1	CSCvy14468	IX5000 Web server vulnerable to redirection page cross site scripting attack
2	CSCvy14462	HTTP security headers not detected vulnerability in IX5000
3	CSCvu49465	Vulnerability: X.509 certificate subject CN does not match entry name
4	CSCvp57432	SSH Server Public Key Too Small Vulnerability in IX5000
5	CSCvm17580	Display Firmware version is showing different when checking in logs

Unresolved Caveats in Release IX 9.1.3

For more details on bugs, enter the Cisco Identifier into the search field of the Bug Search Tool.

Table 3: Unresolved Caveats in Release IX 9.1.3

Sl. No.	Cisco Identifier	Headline
1	CSCvh45762	IX5000 not accessible, got into hung state.

Resolved Caveats in Release IX 9.1.3

For more details on bugs, enter the Cisco Identifier into the search field of the Bug Search Tool.

Table 4: Resolved Caveats in IX 9.1.3

Sl. No.	Cisco Identifier	Headline
1	CSCvw29156	Generated CSR by IX for LSC via CUCM cannot be signed by 3rd party CA
2	CSCvw64381	IX-CMS Call drop due to call de-escalated to Audio Only with G.711
3	CSCvu49489	SSH Vulnerabilities: SSH weak message authentication code algorithm
4	CSCvu49476	SSH Vulnerabilities: CBC, RC4 and 3DES Ciphers supported by SSH server
5	CSCvv85538	Call statistics are not updating in IX5000 WebUI
6	CSCvv26276	"Remote disconnected" sysop log printed, while local endpoint initiated 'BYE' SIP request
7	CSCvv98225	jQuery version before 3.5.0 vulnerable to attack
8	CSCvv71255	BFCP mode content sharing failed multiple times
9	CSCvt98786	Name of participant should be displayed in participant list of conference call

Sl. No.	Cisco Identifier	Headline
10	CSCvx29676	IX5000 device not negotiating BFCP in a call, when registered to CUCM ver 14.0

Unresolved Caveats in Release IX 9.1.2

CSCvh45762

Symptom

- No WebUI Access
- No Admin CLI access
- Frozen video on IX screens
- Call drop.
- No Logging.

Conditions

None

Workaround

Power cycle

Resolved Caveats in Release IX 9.1.2

CSCvh69872

Symptom

IX5000 shows only the first contact method, even though user has multiple contact methods.

Conditions

Any one user should have more than one contact method.

ex:

Name: xyz

SIP: 1234@xx.xx.xx.xx

Phone: 1234567890

IP: xx.xx.xx.xx

Workaround

None

CSCvp52864

Symptom

During CAPF operation to install new LSC to IX5000 the CTL file is downloaded from the TFTP server. But it is rejected by IX due to signature algorithm used by the server.

This causes the CAPF operation to not take place.

The error below is seen in the IX logs:

2019-04-25 17:24:14: ERROR CTL file rejected: ctl

Conditions

CUCM 11.5.1 with TFTP File Signature Algorithm set to SHA-512 in Enterprise Parameter.

IX8.3 (and 9.1)

Workaround

Set TFTP File Signature Algorithm to use the default SHA-1.

CSCvs38186

Symptom

During start up of IX5000 Mic gain value is 0(default). Once Mic gain value set using 'utils micgain set', its value can't be changed to 0 again,since 'utils micgain set' command range is from 3-9.

Conditions

1. set micagain value in between 3 to 9 using admin command 'utils micgain set'.
2. Try to update micgain value to 0

Workaround

None

CSCvt25474

Symptom

TMS is unable to communicate with IX5000 showing unresponsive and potentially causing issues with auto-connect meetings and scheduling.

Conditions

IX5000 version should be 9.1.1 and CAPF certificate files should not be present in IX5000

TMS-15.10

CUCM cluster security mode should be non-secure

Workaround

- Requires root access so must be done by TAC
- Stop tbcss service "/etc/init.d/Tbcss stop"
- Verify the cert directory exists "ls /nv/security/secure-ccm-certs"
- If it doesn't, create it with "mkdir -p /nv/security/secure-ccm-certs"
- Copy self signed web certificate to cucm certs directory "cp /tmp/https-cert.pem /nv/security/secure-ccm-certs/capf0.pem"

- Start tbcss service "/etc/init.d/Tbcss start"
- Force refresh on TMS and confirm IX5000 is now showing a response

CSCvt32486

Symptom

In a P2P call, Busy tone not stopping when remote endpoint rejects the call.

Conditions

1. IX5000 version should be 9.1.1,9.1.0,9.0.1
2. IX5000 registered as non-secure endpoint to CUCM.
3. Dial Remote Endpoint(which is already in another call), and reject the call from Remote

Workaround

Reboot the system or make a new call

CSCvt46946

Symptom

No audio heard from IX on Webex Room 55 after 15 min of call

Conditions

IX and Room 55 register to the same CUCM

Room 55 with multisite call to IX and audio only add-in on Room 55

Workaround

None

CSCvt66100

Symptom

In a P2P call between IX5000 & Cloud registered WebEx board 55, when WebEx board 55 shared a presentation using Cisco Teams App , the audio heard on IX side is too bad.

Conditions

1. WebEx board should be registered as Cloud endpoint
2. Cisco Teams app should be connected with WebEx board
3. Share Team app presentation in a call

Workaround

None

CSCvu43116

Symptom

On April 29, 2020, the Salt Open Core team notified their community regarding the following two CVE-IDs:

CVE-2020-11651: Authentication Bypass Vulnerability

CVE-2020-11652: Directory Traversal Vulnerability

Cisco TelePresence IX5000 Series, Cisco Modeling Labs Corporate Edition (CML) and Cisco Virtual Internet Routing Lab Personal Edition (VIRL-PE) incorporate a version of SaltStack that is running the salt-master service that is affected by these vulnerabilities.

Cisco has released software updates that address these vulnerabilities. There is a workaround that addresses these vulnerabilities.

This advisory is available at the following link:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-salt-2vx545AG

Conditions

Salt services are enabled by default on IX5000 Series endpoints.

Workaround

From Root either of the following commands will show the service/process:

"service --status-all | grep salt"

"ps -aux | grep salt"

Only the salt-master service needs to be stopped using the following:

"service salt-master stop"

Note This service will be re-enabled upon reboot, so the salt-master service will need to be stopped again after any reboot of the Host CPU.

Workaround has been provided to stop salt-master service on IX5000 system. With uploading modified IX system script file all salt-stack services (salt-minion, salt-syndic, salt-master) will be stopped during reboot itself.

Check with IX Escalation team for workaround.

Unresolved Caveats in Release IX 9.1.1

CSCvh45762

Symptom

IX5000 not accessible, got into hung state.

- No WebUI Access
- No Admin CLI access
- Frozen video on IX screens
- Call drop.
- No Logging.

Conditions

None

Workaround

Power Cycle

CSCvs62429

Symptom

Log generation status does not show up,when "Generate Log" button pressed after downloading logs.

But Log is generating in the back ground. During this time,pressing "Download logs" button throws "Unable to send file download" error, until log generation completes.

Conditions

Only occurs in Firefox browsers.

Workaround

Use browser other than Firefox (or) Refresh the page (or) logout and login again.

Resolved Caveats in Release IX 9.1.1

CSCuz80695

Symptom

IX5000 web UI alarms say Admin Web UI and Calendar Service not running

IX5000 says "Calendar Service is not running" and "Admin Web UI Service is not running" in the web UI list of alarms. There is no impact.

Conditions

None

Workaround

Ignore the alarms.

CSCvq41417

Symptom

IX5000 cannot be added to TMS in High Security mode

Conditions

TMS security Mode should be High.

Workaround

None

CSCvq57676

Symptom

IX cannot decrypt encrypted TFTP file from CUCM ,if there is no LSC or MIC cert present in IX

IX5000 unable to decrypt, encrypted config file from CUCM and IX5000 downloads unencrypted config file from CUCM.

Conditions

When IX5000 configured to use encrypted TFTP file from CUCM and IX5000 does not have LSC or MIC.

Workaround

To use encrypted config file, check LSC or MIC present in IX5000.

Or uncheck "TFTP Encrypted Config" in Phone security Profile of IX5000.

CSCvq87478

Symptom

"Unable to send file download", when user presses "Download logs" in webUI after reboot.

"Unable to send file download" in WebUI, while trying to download logs using "Download Logs" button in WebUI

Conditions

Generate Logs in IX5000 using "Generate Logs" button in WebUI.

Restart the system.

Try to download Logs using "Download Logs" button in WebUI

Workaround

Generate logs again and download, after reboot.

CSCvr16198

Symptom

Unable to download logs from webui when the logs are generated via admin command.

Conditions

Generate logs using admin command "utils logs generate" and Try downloading logs from WebUI "Download Logs" button

Workaround

Do Log generation and download from same interface, either CLI or WebUI.

CSCvr59560

Symptom

IX5200 no animation after hanging up, after upgrade to IX9.1

after upgrade from 8.3 to 9.1

-No animation after hanging up

No Impact

Conditions

While 'Multipoint mode' is "Use Endpoint" in CUCM-IX profile.

Workaround

Keep 'Multipoint mode' as "Use Media Resource Group List".

CSCvr98530

Symptom

The system and touch panel time is one-hour ahead of the current time in Brazil

The system and touch panel time are one-hour ahead of the current time in Brazil. For example, if the current time in Brazil is 12:45 PM, then the touch panel and system time would display 1:45 PM as if the system is observing DST.

Conditions

Brazil is not observing DST in 2019.

Workaround

Currently, the workaround is to set the date/time group to use America/Recife which is GMT-3 and assign the device pool which that date/time group to the IX5000/5200 systems.

Unresolved Caveats in Release IX 9.1.0

CSCuw56092

Symptom

Call fails and unit gets reboot. The reboot reason in rc.log MAY show "Reboot Initiated from ASIC hang found" and sym000xx.log will record "[fglrx] ASIC hang happened"

Conditions

None

Workaround

Reboot IX5000

See “Note” below.

CSCve10940

Symptom

IX reboots due to dispEngD zombie followed by call failure. The reboot reason in rc.log is "dispEngD has turned into a zombie"

Conditions

none

Workaround

None

See “Note” below.

CSCve80443

Symptom

IX dropped call as dsp module reset. This is a unique case where vdsp log error show as "'h264 encoder': not ready after ages"

Conditions

None

Workaround

Reboot IX

See “Note” below.

CSCvh45762

Symptom

IX5000 not accessible, got into hung state.

- No WebUI Access
- No Admin CLI access
- Frozen video on IX screens
- Call drop
- No Logging

Conditions

None

Workaround

Power cycle

See “Note” below.

Note for CSCuw56092, CSCve10940, CSCve80443, and CSCvh45762

Extensive research confirms these four bugs (CSCve80443, CSCvh45762, CSCve10940, and CSCuw56092) are associated with AC power instabilities at the IX5x00 deployment sites. Field data demonstrates that unstable power can result in one or more of the associated IX5x00 “bug signatures” that are similar and connected to one another. Since we cannot recreate these incidents at will in our development labs, we are unable to root-cause and resolve these issues.

Field activities have demonstrated that IX5x00 incidents can be reduced dramatically with following mitigations:

1. The installation of an uninterruptible power supply (“UPS”)
2. A weekly reboot of the IX5x00 endpoint.

Resolved Caveats in Release IX 9.1.0

CSCux42126

Symptom

Remote account created on May 31 with 1 day as expiry.

After 12 days,Trying to create remote account with same user name. But "Account Name already exists" error message appeared.

Conditions

In IX versions below 9.1.0.

Workaround

Manually disable & enable the account using "utils remote_account disable" & "utils remote_account enable" admin commands

CSCvo81989

Symptom

IX5000 fails to register with a secure profile to CUCM using LSC when the CAPF certificate has been signed by a 3rd party CA.

Conditions

CAPF is signed by a 3rd party and an LSC is pushed to the IX when registering with a secure profile.

Workaround

Use a non-secure profile or clear the LSC certificate and use the build in MIC for client verification.

CSCvp25784

Symptom

"Restart" button on the touch 10 is greyed out (though still functions normally).

Conditions

Running IX9.0 with the new touch 10 interface.

Workaround

None, button still works as expected but the UI is misleading.

CSCvp25812

Symptom

IX5000 Touch 10 UI Does Not Display Upcoming Meetings Popup Number

No number next to the "meetings" icon on the touch 10 indicating number of upcoming meetings as seen on the CE endpoints.

Conditions

None

Workaround

None.

CSCvp30926

Symptom

Upgraded from 8.3.1 to 9.0.1 and a call is setup, the mute button is not engaged several times unless the call is placed on hold and then resumed.

Conditions

On Software version when upgraded from 8.3.1 to 9.0.1 the Mute button does not always respond when calling WebEx room.

Workaround

Place call on hold and resume.

Unresolved Caveats in Release IX 9.0.1

CSCvh45762

Symptom

- No WebUI Access
- No Admin CLI access
- Frozen video on IX screens
- Call drop
- No Logging

Conditions

None

Workaround

Power cycle.

Resolved Caveats in Release IX 9.0.1

CSCuv69836

Symptom

IX5000 sysop logs always seem to copy over the center video statistics to the left and right sides.

Conditions

This is regardless of whether the call was 3 screen call or single screen call

Workaround

None

CSCuw87529

Symptom

Micboard always showing connected in SNMP even when disconnected

Conditions

Disconnect micboard from IX system and run SNMP command.

Workaround

None

CSCux18706

Symptom

When from the CLI of an IX-5xxx Unit, the command "utils service list" is issued, the unit shows even the Services which are Dead.

Conditions

The CLI of the IX-Units shows the dead services, on the system.

Service	State
System_Log	[Running]
Cisco_Log	[Dead]
DHCP_Srvr	[Running]
NTP	[Dead]
SNMP_Srvr	[Running]
Discovery_Protocol	[Running]
TouchCtrl_Srvr	[Running]
MSI_Services	[Dead]
8021x	[Dead]
Calling_Services	[Running]
Security_Srvr	[Running]
Provisioning_Srvr	[Running]

Workaround

Not applicable

CSCva44717

Symptom

Touch 10 get stuck on unusual screen after ending meeting

Conditions

IX5000 on 8.1.1 and adds audio add in participant on an existing multipoint meeting

Workaround

Press Home Button on Touch

CSCva86421

Symptom

The route pattern has special characters, however the special characters are stripped off and call is not routed.

Example: 2**914089061666

Final pattern 914089061666 no match to be routed in Communications Manager

Conditions

Customer tries tapping the Live Desk number from Touch10 this will not dial the string. The customer can manually dial the same string from the Touch10 and the call completes.

Workaround

Manually dial the number

CSCvf65395

Symptom

System fails to fully connect to a call and then becomes unresponsive to additional attempts. In at least one case it was reported that calling services showed as stopped. In all instances after the failed call attempt the codec becomes unusable for any additional calls, and must be rebooted to resolve the issue.

Conditions

Inbound or outbound call is triggered that starts a delay in the call setup process. No specific trigger is known about the call details at this time.

Workaround

Reboot the system

CSCvi44694

Symptom

IX5000 sysop logs refer to Encoder/Decoder as Platinum

Conditions

None

Workaround

None

CSCvi73713

Symptom

G.722 audio on IX5000 calls sounds poor

Conditions

AAC-LD audio was not negotiated.

Workaround

Fix audio negotiation so AAC-LD is negotiated if possible (CUCM region audio codec preference lists).

CSCvk00066

Symptom

System upgrades fail with the error "ERROR Codec firmware upgrade is disabled" in sysop. Additionally, the entry "autoUpgrade=true" field is missing from the nv registry which can be viewed by running "show tech runtime".

Conditions

The autoUpgrade=true field is missing from the nv registry at the time of the upgrade attempt.

Workaround

None. The registry needs to be manually corrected by TAC.

CSCvm22348

Symptom

Over time some IX5000 touch panels are not showing the same time as the HostCPU.

Conditions

Touch panels that have not rebooted or had to repair in long enough for time drift to occur.

Workaround

Unplug/re-plug the connection between Touch Device and IX5000.

or

Restart the TouchCtrl_Srvr

Below are the steps:

1. SSH and logon as admin
2. utils service restart TouchCtrl_Srvr

CSCvm46260

Symptom

Presentation statistics are not showing on touch panel of the IX5000.

Conditions

Whenever you share a presentation to the IX5000 remotely the presentation.

Workaround

Monitor presentation statistics from sysop logs instead of touch panel

CSCvn19535

Symptom

Incorrect display serial numbers are shown in the log or the output of Admin CLI.

Conditions

None

Workaround

None

CSCvn31747

Symptom

"Please wait..." will be displayed at the bottom of the Center screen of the IX system after the call has de-escalated from an Ad-hoc back to point to point.

Conditions

- CMS is configured as Media Resource for escalating ad hoc in CUCM.
- IX5000 configured to escalate to CMS for ad hoc calls when merging 2 calls.
- TIP needs to be enabled in call settings on CMS.

Workaround

- Hold/Resume call after it has de-escalated to an point-to-point call will
- Disable TIP in call settings in CMS (NOTE: this will mean you will only see one screen on a three screen system)

CSCvn64406

Symptom

video does not switching properly on IX after copying content to main screen

Conditions

need to copy content and move it to main screen

Workaround

remove content from main screen

CSCvo10195

Symptom

IX5000 on the live support number, if you configure + it will not dial the character

Conditions

configure live support number starting with +, for example +1234445555. configuration is accepted and saved however if you use the button it will strip the +, so it will dial 1234445555

Workaround

None

Unresolved Caveats in Release IX 9.0.0

CSCvj17942

Symptom

Switching does not work after moving the presentation to main display when joining a PMR/CMS meeting.

Conditions

The switching issue only happens when the user moves the presentation to the center main display.

Workaround

None

CSCvk42541

Symptom

During First-Time Setup, the speaker and mic-bar icons are disappearing quickly when speaker and microphone tests are in-progress.

Conditions

Run First-Time Setup.

Workaround

Disable 'Intelligent Proximity' from Touch 10 device.

CSCvk62799

Symptom

IX shows “remote participant cannot receive presentation” in Webex calls

Conditions

1. The issue happens on Webex meetings only.
2. Only when the remote user joined the meeting and shared the presentation, then a local user joined the meeting, local user will see the message.

Workaround

None

Resolved Caveats in Release IX 9.0.0

CSCuw92649

Symptom

Upcoming meeting alert for next day's meeting seen the previous day

Conditions

Meeting scheduled for next day.

Upcoming meeting alert is displayed on touch on current day.

Meeting alert displays tomorrow's meeting.

Workaround

Dismiss meeting alert.

CSCva23098

Symptom

Fill light setting on IX5000 doesn't remains after a call or reboot

Conditions

After change the fill light setting in the touch panel of the IX5000, it backs to its original position around 75% after the system is rebooted or after a call.

Workaround

None

CSCvf65536

Symptom

No results for alpha numeric contact search on IX Touch Device

Conditions

Cannot do alpha numeric contact search on IX Touch

Workaround

None

CSCvg64976

Symptom

Blank screen issues

Conditions

IX display firmware updated to 51.00.09 to address blank screen issues. This firmware shuts OFF the display backlight, but leaves all the electronics fully ON when IX Software issues the 'Standby' command,

Workaround

None

CSCvh29813

Symptom

The camera button/icon on the touch panel do not respond randomly (To Select Sit/Stand Position of camera) and all other options do work without any issues (i.e. System information, calling buttons etc. were accessible).

Conditions

When "User Locale" is set to "Deutsch" on IX5000 device profile

Workaround

Temporary WorkAround: Unplug/Replug Touch Panel or Reboot the IX5000

Permanent WorkAround: Set "User Locale" to "English, United States"

CSCvh54806

Symptom

IX5000 CTL Installation fails when CTL serial number starts with "0"

Conditions

We still see "Certificate Operation Status: Operation Pending" under CAPF function on Device profile on CUCM. and "ERROR LSC update unsuccessful" on IX5000 sysop Logs.

Workaround

Re-Generate certs as there is a chance of getting CTL with serial which do not start with "0"

CSCvh89969

Symptom

Lack of information in the release notes

Conditions

In the 8.3 release notes shows in the section "Important Notes for IX Software Releases" -> "Unified CM Device Pack Requirements" -> Make sure that your Unified CM software has the minimum required device pack version.

- The minimum device pack version for 9.1.2 is 9.1(2.13063)
- The minimum device pack version for 10.5 is 10.5(1.12016).

Workaround

Upgrade to CUCM 11.5(1)SU4 or lager.

CSCvi07858

Symptom

Not able to disable Proximity Content Share To Clients.

Conditions

CUCM enables proximity content share to clients by default. There is no option to disable it.

Workaround

None

CSCvi26599

Symptom

IX does not display Merge Failed error on TMS Scheduled calls

Conditions

Audio add-in traverses SIP trunk to another CUCM cluster and goes out MGCP GW.

1. One IX 5000 shares content locally.
2. TMS Scheduled conference auto connects both IX 5000's - Conference name is Cisco Testing
3. Two way A/V established, IX sees presentation from 8.2.3 IX.

4. Either IX 5000 dials audio add-in locally, dials external audio participant (cell phone) and hits **Merge**.
5. Merge succeeds.
6. Two conferences are seen via CMM - the adhoc conference (named Conference) and the original space conference (named Cisco Testing) and the two are cascaded.
7. After merge, TIP seems to fail, and content will also no longer be shared (assumed due to lack of BFCP between the two cascaded conferences).

Workaround

- Have audio participants connect directly to meeting.
- If ad hoc calls are not desired on IX, set **Multipoint Mode** to Use Endpoint.
- Use rendezvous or dial-in meetings—behavior only occurs when TMS schedules a meeting on CMS.

CSCvi80635

Symptom

Multiple Vulnerabilities in ntp

Conditions

None

Workaround

None

CSCvi80645

Symptom

Multiple Vulnerabilities in openssl

Conditions

None

Workaround

None

CSCvi86823

Symptom

Error Message On Touch When Call Ended Due to Packet Loss Not Clear

Conditions

When a call is automatically ended due to packet loss the touch panel displays the error message "Remote Abnormal Release Duration". This is not clear and does not suggest to the user to investigate the network for the source of the loss. This message used to read something more like "Call ended due to network issues" and had in older versions.

Workaround

None

CSCvi91468

Symptom

Multiple Vulnerabilities in libssh2

Conditions

None

Workaround

None

CSCvj78486

Symptom

Mute LED button is not changing color

Conditions

This issue observed when there is an incoming which IX is already in a call. MUTE button color is not changing with unmute operation after incoming-call dropped by remote. MUTE button always stays RED.

Workaround

None

CSCvj83958

Symptom

No presentation send from IX to 3rd Party bridge

Conditions

Third part bridge does not send pending and grand sequence.

Workaround

None

CSCvj84412

Symptom

A vulnerability in the web UI of Cisco TelePresence IX5000 Series Software could allow an unauthenticated, remote attacker to conduct a cross-frame scripting (XFS) attack against a user of the web UI of the affected software.

The vulnerability is due to insufficient protections for HTML inline frames (iframes) by the web UI of the affected software. An attacker could exploit this vulnerability by persuading a user of the affected UI to navigate to an attacker-controlled web page that contains a malicious HTML iframe. A successful exploit could allow the attacker to conduct click-jacking or other client-side browser attacks on the affected system.

Conditions

A device running an affected version of software.

Workaround

None

CSCvj90534

Symptom

Multiple Vulnerabilities in libtiff5

Conditions

None

Workaround

None

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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 of this document are considered uncontrolled. See the current online version for the latest version.

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