Cisco TelePresence Conductor XC2.4.1

Release Notes
October 2014

Contents

Product documentation

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

- *Cisco TelePresence Conductor Administrator Guide*
- *Cisco TelePresence Conductor Getting Started Guide*
- *Cisco TelePresence Conductor Virtual Machine Installation Guide*
- *Cisco TelePresence Conductor with Cisco TelePresence VCS (B2BUA) Deployment Guide*
- *Cisco TelePresence Conductor with Cisco TelePresence VCS (Policy Service) Deployment Guide*
- *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*
- *Cisco TelePresence Conductor Clustering with Cisco TelePresence VCS (B2BUA) Deployment Guide*
- *Cisco TelePresence Conductor Clustering with Cisco TelePresence VCS (Policy Service) Deployment Guide*
- *Cisco TelePresence Conductor Clustering with Cisco Unified CM Deployment Guide*
- *Cisco TelePresence Conductor Certificate Deployment Guide*
- *Cisco TelePresence Multiway Deployment Guide*
- *Cisco TelePresence Conductor API Guide*

New features in XC2

New features in XC2.4.1

This is a maintenance release.

New features in XC2.4

Cascading of conferences hosted on TelePresence Servers

This version of the TelePresence Conductor supports cascading of conferences hosted on TelePresence Servers in a similar way to cascading of conferences hosted on TelePresence MCUs. TelePresence Server version 4.0(1.57) or later is required for this to work.

Cascading a conference results in resources being used on a secondary conference bridge when the primary conference bridge does not have enough resources available for all the participants.

The web interface allows you to specify the maximum number of cascades allowed for a conference. This number determines how many resources are reserved on the primary conference bridge purely for creating cascade links to other conference bridges.

If all available resources on the primary conference bridge are used up, a cascade link is created to one or more conference bridges to expand the size of the conference beyond the resource capabilities of the primary conference bridge. The resources used for each cascade link are equivalent to the resources that would be used by one participant receiving 720p/30fps video, stereo audio and the content quality selected on the conference template. These resources are allocated on the primary and on the cascade conference bridge.

Only single screen endpoints are supported on cascade links connecting TelePresence Servers. Therefore, if a multiscreen endpoint joins a conference on a cascade conference bridge, participants on the same cascade bridge will see all screens, whereas participants on the primary bridge and on other cascade bridges will only see one screen (the screen showing the loudest speaker).

Cascade links connecting TelePresence Servers support up to 720p/30fps video. Participants viewing video over a cascade link (that is, video from a participant hosted on a different conference bridge) will see a maximum video quality of 720p/30fps.

Participants on the same conference bridge will see full high quality video if all of the following apply:

- Higher quality video (1080p/30fps or 720p/60fps) has been configured on the TelePresence Conductor's conference template.
- The endpoint of the main displayed participant is providing that high quality video.
- The participants' own endpoint supports high quality video.

Improved conference placement algorithm

The algorithm that determines the conference bridge on which TelePresence Conductor places a new conference has been improved.

Note: We strongly recommend that all conference bridges within a pool have the same capacity, so that conferences can be distributed efficiently across conference bridges. If there are conference bridges with different capacities in the same pool, this may lead to unbalanced conference placement in some scenarios.

Minimum TelePresence Server version alarm has been updated

The minimum recommended version of TelePresence Server software is now 4.0. The alarm that is raised when an older version of TelePresence Server software is used has been updated accordingly.

Alarm raised when no Encryption feature key enabled

A new alarm has been added that is raised when one or more conference bridges used by the TelePresence Conductor do not have the Encryption feature key enabled. The Encryption feature key is required for back-to-back user agent (B2BUA) links and recommended for Policy Service links.

Alarm raised when the same conference bridge has been added to TelePresence Conductor more than once

A new alarm has been added that is raised when the same conference bridge has been added to the TelePresence Conductor more than once. The TelePresence Conductor check whether the conference bridges' serial numbers are identical.

Warning displayed when advanced template parameters on primary and cascade TelePresence MCUs are different

A new warning has been added that is displayed when the advanced parameters on the primary and cascade TelePresence MCUs are configured differently. In a future version of the TelePresence Conductor software, the cascade advanced parameters may be removed.

User interface changes

- The field **Number of cascade ports to reserve** on the **Conference templates** page has been renamed to **Maximum number of cascades**. It is now also applicable to conference templates based on TelePresence Server Service Preferences and the default value has been changed to '0'.
- It is no longer possible to turn off the administrator session timeout (for serial port, HTTPS or SSH) on the TelePresence Conductor. The session timeout must now be within the range of 1 to 65535 minutes.
- The **SNMP** page now displays a **Description** field, which allows you to define a description of the system as viewed by SNMP.

API changes

- A new optional parameter, **`bestEffort`**, has been added to the XML-RPC call **`factory.webex.add`**. This parameter determines whether the TelePresence Conductor should attempt to add a WebEx conference when insufficient resources were reserved at conference creation.
- The default value for the **`reserved_cascades`** attribute of the **`confBundle`** object has been changed to '0'. When the attribute is omitted, it is assumed to be '0', which means that cascading is disabled.

New features in XC2.3.1

This is a maintenance release.

New features in XC2.3

New Capacity Management API

A new API allows management applications (such as Cisco TMS) to obtain information about a conference and its associated resources. The API returns information about the capacity of a conference bridge that will be used for a conference with a given dialed alias.

New Provisioning API

A new API allows management applications (such as Cisco TMS) to provision conferences on TelePresence Conductor. The API allows the client to create a new ConfBundle on the TelePresence Conductor. A ConfBundle consists of information related to a conference and can have a number of aliases and auto-dialed participants associated with it. These aliases and auto-dialed participants are separate from conference aliases and auto-dialed participants configured via the TelePresence Conductor's web interface and can be edited via the Provisioning API only.

Direct match alias lookup

TelePresence Conductor version XC2.3 supports direct match alias lookup for conferences created via the Provisioning API. Allowing direct match alias configuration dramatically reduces the lookup time for tens of thousands of aliases.

In previous versions, conferences configured on TelePresence Conductor used regular expressions (RegEx) to match aliases. This allowed multiple aliases to create conferences with minimum configuration on TelePresence Conductor. However, when thousands of aliases were configured, conference lookup time and create time started to increase, and fine grain control of allowed conferences was difficult.

In version XC2.3 direct match alias lookup is supported only when using the new Provisioning API. All conferences configured directly via the TelePresence Conductor's web interface or XML RPC API continue to use RegEx lookup.

Numeric dialing with Unified CM

Unified CMs append the TelePresence Conductor's IP address (one of the additional IP addresses configured on TelePresence Conductor's user interface) or hostname instead of the domain to numeric dial strings. For example, when an endpoint dials the string **`1234`**, Unified CM will send the dial string **`1234@10.0.0.1`** to TelePresence Conductor. When TelePresence Conductor attempts to do an exact match of the dial string, it will not be able to match the dial string to an alias, because the user will have provisioned an alias that uses a domain, for example **`1234@domain.com`**.

A new API (the SIP Domain API) resolves this issue. You can set the SIP domain on TelePresence Conductor. TelePresence Conductor will transform incoming dial strings to include the SIP domain rather than an IP address or hostname, which will make it possible to compare the dial string with provisioned aliases.

Note that this modification to the URI is only internal to the TelePresence Conductor. The outgoing call URI does not change.

Collaboration meeting room information available on the web interface

You can use the **Collaboration meeting rooms** page to search for one or more Collaboration Meeting Rooms (CMRs) that have been configured via the TelePresence Conductor's Provisioning API using a management tool such as Cisco TMS. For each CMR, details on aliases, auto-dialed participant and other related data can be viewed. The data associated with a CMR is configured via the Provisioning API. It cannot be modified via the TelePresence Conductor's web interface and it cannot be used by conferences configured via the web interface.

Increased number of TelePresence Server calls supported

In older versions of TelePresence Server software it was possible to connect only up to 104 participants in total to either a standalone TelePresence Server or cluster of TelePresence Servers. In TelePresence Server version 4.0 it will be possible to connect up to 200 participants in total (up to 104 per conference). Changes to TelePresence Conductor allow support for these new limits.

Audio-only quality setting added

You can configure audio-only conferences on TelePresence Servers using a new predefined 'Audio-only (no video, mono audio)' conference quality setting.

Segment switching support

TelePresence Server version 4.0 supports segment switching, which allows multiscreen endpoints to switch just the screen of another multiscreen endpoint that contains the loudest speaker rather than all screens. This feature works only for multiscreen endpoints that provide loudest pane information and for TelePresence Server version 4.0. It is ignored otherwise. The default is to have segment switching enabled.

The feature can be enabled or disabled via:

- TelePresence Conductor's web interface (on the **Conference template** page)
- Cisco TMS's web interface (via the **Custom Parameters** on the **Create new CMR Template** page)
- the `advanced_parameters` attribute of the `ConfBundle` object when using the TelePresence Conductor's Provisioning API directly

The TelePresence Server must be:

- connected to the TelePresence Conductor
- running version 4.0 or later
- configured in *Remotely managed* mode

H.264 - SVC signaling passthrough

The TelePresence Conductor back-to-back user agent (B2BUA) now passes through all H.264-SVC (scalable video codec) signaling. This will allow endpoints to use the hybrid conference and multistream endpoint support on the TelePresence Server when it is available. A hybrid conference includes some audio and video streams that are switched and some that are transcoded. See *TelePresence Server Release Notes* for more information.

H.265 passthrough

The TelePresence Conductor back-to-back user agent (B2BUA) now passes through all H.265 signaling. Like H.264 - SVC signaling this will allow endpoints to use the hybrid conference and multistream endpoint support on the TelePresence Server when it is available.

Encrypted iX passthrough

Previously the iX protocol, used for example to support the ActiveControl feature on the TelePresence Server, was passed through the TelePresence Conductor's B2BUA. Now the B2BUA also allows Encrypted iX to pass through.

SIP Remote Party ID (RPID) passthrough

The TelePresence Conductor's B2BUA now supports the passthrough of SIP RPID, which is a SIP header used by Unified CM to convey calling and connected line identity. SIP RPID is defined in the document draft-ietf-sip-privacy-04. Although RPID is non-standard, it is implemented by a large number of vendors and is included in most of Cisco's SIP products.

TelePresence Conductor forwards the SIP RPID header without checking the validity of the identity information contained in the header or the authority of the source. To indicate this, TelePresence Conductor sets the `screen` parameter to *no*.

TelePresence Conductor does not support the ability to set the display name field to 'anonymous' for endpoints requesting anonymity. All display names are forwarded on as they are.

Secure conference configuration passthrough

Previously when configuring a conference on Cisco TMS, the secure conference parameter was ignored. This has now changed and the configuration is passed on to the conference bridges.

Certificate management

- The management of CA certificates has been improved, allowing you to view, upload and delete individual CA certificates.
- New installations of TelePresence Conductor software now ship with a temporary trusted CA, and a server certificate issued by that temporary CA. We strongly recommend that you replace the server certificate with one generated by a trusted certificate authority, and that you install CA certificates for the authorities that you trust. If you upgrade to this release from an earlier installation of TelePresence Conductor software, your existing server and trusted CA certificates will not be affected.

Other enhancements and usability improvements

- The online help has a new skin and an improved search capability.
- When configuring firewall rules:
  - You can choose whether to drop or reject denied traffic. On upgrade to XC2.3 or later, any existing "deny" rules will now drop the traffic; prior to XC2.3 the traffic would have been rejected.
  - If you have made several changes there is now an option to revert all changes. This discards all pending changes and resets the working copy of the rules to match the current active rules.
  - You can more easily change the order of the rules by using up/down arrow buttons to swap the priorities of adjacent rules.
- Improved web interface usability when switching between SRV and address record resolution modes when configuring the address of an LDAP server for remote user account authentication.
- You have the option to take a tcpdump while diagnostic logging is in progress.
- The diagnostic logging feature has been extended to include:
  - a tcpdump that can be enabled cluster-wide
  - an xconfig file
  - an xstatus file
  - an indication on the web administration page of which user / IP address initiated the logging

  The xconfig and xstatus files are taken at the start of the logging process.
- It is now possible to view all matching intrusion protection triggers for a particular category.

New features in XC2.2.2

This is a maintenance release.

New features in XC2.2.1

New option key supporting up to 50 concurrent call sessions

From Cisco TelePresence Conductor version XC2.2.1 a new option key is available for the Virtual Machine TelePresence Conductor which supports up to 50 concurrent call sessions. This option key can be obtained from your Cisco representative. It provides access to Cisco TAC (Technical Assistance Center) support and is suitable for small and medium-sized deployments.

See Limitations [p.18] for information on the limitations when running TelePresence Conductor with this option key installed.

New features in XC2.2

Improved TIP-compliant endpoint support

Multiscreen endpoints that are compliant with the TelePresence Interoperability Protocol (TIP) do not need to be pre-configured any longer. The TelePresence Conductor is now able to retrieve the number of screens and the associated resources that are required on the conference bridge via TIP. The TelePresence Conductor no longer over-allocates resources on the conference bridge for multiscreen endpoints.

However, these improvements are only applicable to deployments where SIP signaling is routed via the TelePresence Conductor; Cisco VCS deployments using the external policy service continue to work as in previous releases. Additionally, the TelePresence Conductor still over-allocates resources initially for reserved chairperson participants and for escalated Unified CM ad hoc conferences.

360p video support

The TelePresence Conductor now supports 360p video for TelePresence Servers running software version 3.1 or later. There is a new pre-defined quality level with 360p video and mono audio defined that can be selected for conference templates and pre-configured endpoint codecs. New quality levels can be added that use 360p video.

Support for TelePresence Server software on new hardware

The TelePresence Conductor now supports new hardware platforms for the TelePresence Server software version 3.1. It supports the platforms Cisco Multiparty Media 310 and Cisco Multiparty Media 320, as well as the Cisco TelePresence Server on Virtual Machine.

Alarm for minimum conference bridge version

The TelePresence Conductor now raises a minimum version alarm when connected to a TelePresence MCU running version 4.3 or lower, and when connected to a TelePresence Server running version 3.0 in remotely managed mode. If a TelePresence Server is running version 2.x and/or is in locally managed mode, TelePresence Conductor will raise an alarm stating that the conference bridge is running in the wrong mode.

These older conference bridge versions do not support some of the new features for XC2.2.

Automated intrusion protection

An automated intrusion protection feature has been added. It can be used to detect and block malicious traffic and to help protect the TelePresence Conductor from dictionary-based attempts to breach login security.

Automated protection should be used in combination with the existing firewall rules feature - use automated protection to temporarily block specific threats and use firewall rules to block permanently a range of known host addresses.

Changes to B2BUA security status handling

The TelePresence Conductor back-to-back user agent (B2BUA) now modifies the conference security status to be unencrypted when the inbound SIP connection is over TCP and the outbound SIP connection is over TLS. For the conference security status to be encrypted, SIP signaling must be encrypted on all call legs.

ActiveControl support

The TelePresence Conductor now allows ActiveControl to be negotiated between an endpoint and TelePresence Servers that support this feature. To operate, ActiveControl must be enabled on a TelePresence Server version 3.1 or later by enabling the iX protocol on the TelePresence Conductor under **Conference templates > Advanced template parameters**. Information about capabilities and limitations of this feature is available in the *Cisco TelePresence Server Release Notes*.

Allow or disallow conference creation

A conference alias can now be configured to either allow or disallow conference creation. If the conference alias is configured to disallow conference creation, participants can only join the conference via that alias if the conference already exists. The conference can still be created via the API or by dialing a different conference alias defined for the same conference.

New XML-RPC API parameter added for maximum conference duration

A new XML-RPC parameter has been added to the TelePresence Conductor API that allows API users to override the maximum conference duration configured on the conference template with a lower value.

New XML-RPC API parameter added for number of endpoint screens

A new XML-RPC parameter has been added to the TelePresence Conductor API that allows API users to override the number of endpoint screens configured on the conference template with a lower value. This parameter is only applicable to conference templates that:

- point to a Service Preference containing TelePresence Server pools
- have **Allow multiscreen** set to *Yes*
- have a **Maximum screens** value that is greater than the value specified in the API parameter

Firewall rules configuration

When configuring the firewall rules priority, it is now easier to change the order of the rules by using up/down arrow buttons to swap the priorities of adjacent rules.

Managing trusted CA certificates

The TelePresence Conductor's server and trusted CA certificates can now be viewed in either a human-readable, decoded format, or in raw PEM format.

Administrator authentication source

When configuring the source for administrator account authentication, the *Remote* option is now labeled as *Remote only*. You can no longer access the TelePresence Conductor via a locally configured admin account if a *Remote only* authentication source is in use.

The *Local* option has also been renamed to *Local only*.

Improved user interface

Changes have been made to improve the TelePresence Conductor user interface.

New features in XC2.1

Limited system capacity when running without a release key

The TelePresence Conductor can be run without a release key. In this mode the system capacity is limited; only a single un-clustered conference bridge can be enabled and the TelePresence Conductor cannot be clustered.

Where the TelePresence Conductor has no release key, only "community support" is available. This is a self / collaborative support effort, using technical forums like https://supportforums.cisco.com/community/netpro/collaboration-voice-video/telepresence. TAC support is only available for TelePresence Conductors that have a release key; for further details see https://www.cisco.com/web/services/portfolio/product-technical-support/index.html.

For deployments in production environments we recommend that customers upgrade to a fully licensed installation of TelePresence Conductor.

New features in XC2.0.3

This is a maintenance release.

New features in XC2.0.2

This is a maintenance release.

New features in XC2.0.1

This is a maintenance release.

New features in XC2.0

Cisco TelePresence Server support

A new conference bridge type of Cisco TelePresence Server is supported in this release of the TelePresence Conductor. Conference bridge pools can now be made up of either TelePresence Servers or TelePresence MCUs.

Cisco Unified Communications Manager support

The TelePresence Conductor now supports direct connection to Cisco Unified Communications Manager for ad hoc and rendezvous calls. Endpoints can be registered with either Unified CM or Cisco VCS and call into the same conference.

Addition of multiple IP addresses

Multiple IP addresses can be added on TelePresence Conductor. A different IP address is needed on the TelePresence Conductor for each ad hoc Unified CM location and each rendezvous Unified CM location. This allows the TelePresence Conductor to mimic Unified CM's expectation that it is connecting to separate conference bridges in each location, for ad hoc and rendezvous calls.

Known and unknown multiscreen endpoint support for TelePresence Server conferences

The TelePresence Conductor supports endpoints with more than one screen in conferences hosted on TelePresence Servers.

Cisco TelePresence System (CTS) series endpoints, including Cisco TelePresence System T3, can be pre-configured, in which case they will be allocated the resources defined for the endpoint, or supported without pre-configuration, in which case they will be allocated the resources defined for the conference template.

Other customized multiscreen endpoints have to be pre-configured if sufficient resources are to be allocated on the TelePresence Servers used in the relevant conferences.

Support for third-party and customized multiscreen TelePresence systems (i.e. those other than CTS3xxx, TX9000 or T3) require the optional third-party interop key on the TelePresence Server.

Resource optimization

Resource optimization allows resources that are initially over-allocated on a TelePresence Server to be recovered and re-allocated for other participants, allowing more participants to be handled by a single TelePresence Server.

XML-RPC API support to communicate between Cisco TMS and TelePresence Server 3.0

The TelePresence Conductor API now has support added to translate information being sent between Cisco TelePresence Management Suite and TelePresence Server version 3.0 running in 'Remotely managed' mode. See *Cisco TelePresence Management Suite Release Notes* for information on when this support has been added to the Cisco TMS.

Improvements to logging

Filtered event logs can now be downloaded from the UI.

It is possible to specify the remote syslog server mode as one of the following:

- Legacy BSD format
- IETF syslog format
- IETF syslog using TLS connection
- Custom

The Configuration Log page provides a list of all changes to the TelePresence Conductor configuration, providing users with an audit trail of the TelePresence Conductor configuration.

System Administration session timeout and limits

It is now possible to set a session time out, as well as limits for concurrent sessions and concurrent logins per administrator account for web, SSH and serial sessions.

Certificate signing request (CSR)

The TelePresence Conductor can now generate server certificate signing requests, which removes the need to use an external mechanism to generate and obtain certificate requests.

Firewall rules

Firewall rules can now be added to the TelePresence Conductor, which provide the ability to configure IP table rules to control access to the TelePresence Conductor at the IP level.

Addition of multiple administrator accounts

It is now possible to add multiple administrator accounts with pre-determined access level settings.

Other changes and improvements

Improvements have been made to the TelePresence Conductor web interface.

Resolved issues

Resolved in XC2.4.1

The following issues were found in previous releases and were resolved in XC2.4.1:

Identifier	Description
CSCur05556	**Symptom:** An unauthenticated attacker can bypass the web UI authentication check and gain access to the administration web UI. **Conditions:** The attacker must possess a specially crafted web cookie. **Workaround:** There is no workaround, but the attack surface can be reduced by disabling web access from outside the enterprise.
CSCur02103	**Symptoms:** TelePresence Conductor includes a version of Bash that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs: ■ CVE-2014-6271 ■ CVE-2014-6277 ■ CVE-2014-6278 ■ CVE-2014-7169 ■ CVE-2014-7186 ■ CVE-2014-7187 This bug has been opened to address the potential impact on this product. **Conditions:** The API over HTTP(S) or/and SSH but authentication is required to exploit this vulnerability. **Workaround:** Configure firewall rules on TelePresence Conductor (using feature on TelePresence Conductor) to deny HTTP(S) and SSH access from unknown IP address (or/and address range) If TelePresence Conductor is behind the firewall, manage SSH/HTTP(S) traffic to TelePresence Conductor products.
CSCuq43935	**Symptom:** When you enter a primary PIN on a conference template's advanced parameters, the PIN appears as "not set" for the cascade. The interface warns you about the mismatch, even though you cannot correct it. **Conditions:** On a Conductor XC2.4 conference template that allows cascades, when entering chair/guest PINs as advanced parameters. This issue was also present in XC2.3 although the warning was not yet implemented in that version. **Workaround:** Not required. The cascade PIN is actually correctly set but the warning and interface are misleading.

Resolved in XC2.4

The following issues were found in previous releases and were resolved in XC2.4:

Identifier	Description
CSCuh49198	**Symptom:** From version XC2.2 the Conductor ensures that there is enough space available on the TelePresence Server for the participant dialing in, any reserved chairpersons, any auto-dialed participants and one extra participant. This can cause the situation where there are sufficient resources available on a TelePresence Server for the participant dialing in, the reserved chairpersons and the auto-dialed participants, but the conference fails because there is not enough space for the extra participant on the same TelePresence Server. If there is another pool with a TelePresence Server that has enough capacity the conference will be placed on that conference bridge **Conditions:** This only affects conferences on TelePresence Servers, not MCUs

Identifier	Description
CSCud10101	**Symptom:** Auto-dialed participant calls which are configured not to “keep conference alive” can be left in a conference if participants try but fail to enter the conference, or no chair participants arrive on a Lecture-type conference.

Resolved in XC2.3.1

The following issues were found in previous releases and were resolved in XC2.3.1:

Identifier	Description
CSCur05556	**Symptom:** An unauthenticated attacker can bypass the web UI authentication check and gain access to the administration web UI. **Conditions:** The attacker must possess a specially crafted web cookie. **Workaround:** There is no workaround, but the attack surface can be reduced by disabling web access from outside the enterprise.
CSCur02103	**Symptoms:** TelePresence Conductor includes a version of Bash that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs: ■ CVE-2014-6271 ■ CVE-2014-6277 ■ CVE-2014-6278 ■ CVE-2014-7169 ■ CVE-2014-7186 ■ CVE-2014-7187 This bug has been opened to address the potential impact on this product. **Conditions:** The API over HTTP(S) or/and SSH but authentication is required to exploit this vulnerability. **Workaround:** Configure firewall rules on TelePresence Conductor (using feature on TelePresence Conductor) to deny HTTP(S) and SSH access from unknown IP address (or/and address range) If TelePresence Conductor is behind the firewall, manage SSH/HTTP(S) traffic to TelePresence Conductor products.

Resolved in XC2.3

The following issues were found in previous releases and were resolved in XC2.3:

Identifier	Description
CSCuo20306	**Symptom:** Cisco Telepresence Conductor includes a version of openssl that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160. This bug has been opened to address the potential impact on this product. **Conditions:** Device with default configuration. The following Cisco Telepresence Conductor versions are affected by this vulnerability: XC2.0 XC2.1 XC2.2 XC2.2.1 **Workaround:** Not currently available. **Further Problem Description:** Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html
CSCuh94523, CSCui00969	**Symptom:** An alias attempting to use a conference template with the advanced template parameter 'Custom layout' set to the value 0 fails to be created. **Conditions:** The customer checks the advanced template parameter 'Custom layout' for an MCU and leaves the value as the default of 0 in their configuration. **Workaround:** Uncheck the 'Custom layout' parameter in the advanced template parameters configuration or change the value to correspond with a valid layout family index value in the range of 1 to 59. **Notes:** The default value has been changed to 5.
CSCui12885	**Symptom:** Cisco TMS repeatedly outdials participants if the call that the TelePresence Server outdials is put on hold by the receiving endpoint. **Conditions:** If a TelePresence Server performs an outdial (e.g. at the request of TMS via Conductor) and on receipt of the call, the called party puts the call on hold, Conductor interprets the feedback from TelePresence Server as though the endpoint has dropped the call. Conductor reports this back to TMS which then tries to redial the call. **Workaround:** None
CSCuh65199	**Symptoms:** Unexpected system restart due to application failure. **Conditions:** Run any xmlrpc call through API using the authentication credentials of API access account that contain at least one Unicode encoded character. **Workaround:** Not use any unicode encoded characters in their username or password. (If the special character is not obvious, it could be that username/password copied from a text editor rather than typing them in manually, this often causes the unicode representation of normal characters making them hard to distinguish. In this scenario it is advised to manually type the user/pass in through the web rather than copy and paste).

Resolved in XC2.2.2

The following issues were found in previous releases and were resolved in XC2.2.2:

Identifier	Description
CSCuo20306	**Symptom:** Cisco Telepresence Conductor includes a version of openssl that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160. This bug has been opened to address the potential impact on this product. **Conditions:** Device with default configuration. The following Cisco Telepresence Conductor versions are affected by this vulnerability: XC2.0 XC2.1 XC2.2 XC2.2.1 **Workaround:** Not currently available. **Further Problem Description:** Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved in XC2.2.1

There are no issues that were resolved in XC2.2.1.

Resolved in XC2.2

The following issues were found in previous releases and were resolved in XC2.2:

Identifier	Description
CSCuh98153	There was an inconsistency in the Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide (XC2.1) in regards to the recommended SIP setting on the TelePresence Server. This has been corrected in the XC2.2 version of the deployment guide.
CSCuh95327	The TelePresence Conductor deployment guides did not mention specifically that multiscreen auto-dialed participants are not supported. This has been corrected in the XC2.2 version of the deployment guide.
CSCuh30073	The TelePresence Conductor online help pages contained some incorrect regular expression examples. These have been corrected in the XC2.2 version of the online help.
CSCug78943	When configuring two TelePresence Server conference pools in a prioritized list using Service Preferences on TelePresence Conductor, conferences were only ever placed in the first pool. Lower priority pools were not used. This has been fixed in XC2.2.
CSCui42333	Failure to make a call via TelePresence Conductor (i.e. scheduled call from TMS) when the dial-out URL contained unicode strings. This has been fixed in XC2.2.
CSCug62478	The conference bridge status page on Telepresence Conductor sometimes reported an incorrect number of TelePresence Server screen licenses. This has been fixed in XC2.2.
CSCuf38907	Enhancement request for TelePresence Conductor to support auto detection of endpoint multiscreen capabilities via TIP. This feature was added in XC2.2 (Note that it still requires "Provision for multiscreen" to be set).

Identifier	Description
CSCui21923	The Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide (XC2.1) detailed steps on how to upload a self-signed server certificate to TelePresence Conductor. Because Unified CM may not support the default TelePresence Conductor server certificate the recommendation has been changed to use an officially signed server certificate instead.
CSCuh15866	MCU 4501 running 4.4(3.49) experienced high CPU load when connected to TelePresence Conductor via HTTPS. There were no issues when connected via HTTP. This has been fixed in XC2.2.
CSCug88040	When configuring TelePresence Conductor according to "Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide", with the neighbor zone profile set to "Infrastructure device" and with a TelePresence Conductor cluster, VCS still routed conference calls to any Out Of Service TelePresence Conductors causing call failure. The deployment guide has been modified to recommend a neighbor zone profile setting of "Custom" with "Automatically respond to SIP searches" set to "On", which will avoid these issues.
CSCue71379	The TelePresence Conductor B2BUA deployment needed to pass through max-rcmd-nalu-size in the SDP for H.264 in order to support the CTS 10bears codec as it advertised H.264 restricted pack mode 1. This issue has been fixed in XC2.2.

Resolved in XC2.1

There are no issues that were resolved in XC2.1.

Resolved in XC2.0.3

The following issues were found in previous releases and were resolved in XC2.0.3:

Identifier	Description
CSCuo20306	**Symptom:** Cisco Telepresence Conductor includes a version of openssl that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160. This bug has been opened to address the potential impact on this product. **Conditions:** Device with default configuration. The following Cisco Telepresence Conductor versions are affected by this vulnerability: XC2.0 XC2.1 XC2.2 XC2.2.1 **Workaround:** Not currently available. **Further Problem Description:** Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved in XC2.0.2

The following issues were found in previous releases and were resolved in XC2.0.2:

Identifier	Description
CSCue89279	**Symptom:** FUR (Fast picture update) messages get dropped if they contain a stream ID - this means that no video or blocky video may be seen, especially if the data network drops video packets. TS prior to TS3.0(2.46) did not send stream IDs for main video. **Diagnosis:** This problem will only be seen if Conductor without this fix in is used with TS >= 3.0 (2.46). **Versions affected:** XC2.0 and XC2.0.1 **Workaround:** Avoid upgrading TS to >= 3.0 (2.46) until Conductor is upgraded.

Resolved in XC2.0.1

The following issues were found in previous releases and were resolved in XC2.0.1:

Identifier	Description
CSCud97851	**Symptom:** Incident report generated. The switchboard process is automatically restarted by the app so there is a limited impact on the customer. **Diagnosis:** **Versions affected:** XC2.0 **Workaround:** None.

Resolved in XC2.0

The following issues were found in previous releases and were resolved in XC2.0:

Identifier	Description
CSCub46878	**Symptom:** Maximum latency for Telepresence Conductor is not documented. **Diagnosis:** None. **Versions affected:** XC1.2 **Workaround:** None.
CSCua01811	**Symptom:** Cannot load "trusted CA certificates file" onto Conductor via the web interface. **Diagnosis:** None. **Versions affected:** XC1.2 **Workaround:** Load "trusted CA certificates file" onto Conductor using SCP.
CSCub84541	**Symptom:** Logins on the web can be slow to complete. **Diagnosis:** When remote authentication is enabled, all logins (not just remote users) can be delayed by many seconds if the LDAP server is slow to respond. **Versions affected:** XC1.2 **Workaround:** None, however delays from the LDAP server are outside the control of the Conductor. **Additional Information:** The fix in X8.0 disables LDAP checks for local users, removing local user delays. Remote user delays will still exist if the LDAP server is slow to respond, but this is outside the control of the Conductor.

Open issues

The following issues apply to this version of the Cisco TelePresence Conductor.

Identifier	Description
CSCuq56985	**Symptom:** Conductor not creating new conference with MCU video ports available **Conditions:** Attempting to create conferences with 1 participant with limited video port availability. Not allowing cascading. **Versions affected:** XC2.3 or later **Workaround:** Cascade, add more video ports.
CSCuq18666	**Symptom:** A DX-series phone joins a video bridge through Conductor. When the DX starts presenting the video from the bridge freezes. **Conditions:**Under the network Topology: DXs < -- > CUCM < -- > Conductor < -- > TP Server (or TS) 1. Multiple DX call to TP bridge. 2. Video is working and every DX is fine. 3. One DX starts sharing content. 4. Other DXs or MX/CTS video freezes. **Workaround:** Disable Early Offer on the SIP trunk from UCM to Conductor. Hold/Resume on the endpoint with frozen video will not allow video to recover. The user must disconnect and dial back into the bridge.
CSCun63044	**Symptom:** The Conductor documentation does not describe in detail how the implementation of syslog works. There is no documentation as to what messages match what facilities. **Versions affected:** XC1.2 or later **Workaround:** None
CSCud02050	**Symptom:** If a Lecture-type conference is created on the Conductor with an auto-dialed Content Server, the recording device is started as soon as the user dials in, even before they have successfully entered their PIN. If the user disconnects without entering any PIN code, the auto-dialed content server stays in the conference and records for the maximum time defined in the template. This occurs even when on Conductor, under Conference configuration > Auto dialed participants the option 'Keep conference alive' is set to 'No', which means that the conference should automatically end when only this auto-dialed participant remains. In practice the auto-dialed participant will only clear when the last participant actually leaves the conference, after they have joined successfully. **Versions affected:** XC1.2 or later **Workaround:** Ensure that there is a maximum duration on any conferences that is may affect, so that the auto-dialed participant is not left recording forever.
CSCuf34880	**Symptom:** TelePresence Conductor may wait up to 30 seconds before releasing resources between conferences. This can potentially cause the following two issues: ■ it can cause a lack of resources with back-to-back scheduled conferences ■ it can cause the overall utilization of the TelePresence Conductor to go up when a participant repeatedly leaves and joins an ad hoc conference, resulting in the participant eventually not being able to join back into the conference any more **Versions affected:** XC2.0 or later **Workaround:** None

Limitations

Full capacity TelePresence Conductor version XC2.4.1 supports:

- 30 conference bridges
- 30 conference bridge pools
- 30 Service Preferences
- 1000 conference templates
- 1000 conference aliases
- Conference bridge types of Cisco TelePresence MCU and Cisco TelePresence Server
- Scheduling with Cisco TMS using either a single TelePresence Server, a single TelePresence MCU or a pool of identical sized TelePresence MCUs
- Clustering of up to 3 TelePresence Conductors to achieve resilience (full capacity versions only)

It does not support:

- T3 point to point calls escalated to a conference functionality
- Auto-dialed participants that are multiscreen endpoints
- Advanced parameters for auto-dialed participants that are part of conferences hosted on TelePresence Servers
- Geographic cascading with TelePresence Servers as conference bridges
- Scheduling with Cisco TMS using pools with multiple TelePresence Servers or pools with multiple TelePresence MCUs of different sizes
- Use of dedicated audio ports on TelePresence MCUs

The following limitations apply to the three different capacity versions of the TelePresence Conductor:

	TelePresence Conductor Essentials (free)	**TelePresence Conductor Select**	**Full capacity TelePresence Conductor**
Suitable deployment	Small Recommended for: ■ testing and reviewing new releases ■ proof of concept demonstrations	Small to medium-sized	Medium-sized to large
Total number of conference bridges supported	1 (standalone)	30	30
Maximum number of concurrent call sessions supported	The number of calls supported by the conference bridge	50	2400
Clustering of TelePresence Conductors supported for resilience	No	Yes (limited to 2 TelePresence Conductor Select)	Yes (up to 3 full capacity TelePresence Conductors)

	TelePresence Conductor Essentials (free)	TelePresence Conductor Select	Full capacity TelePresence Conductor
Access to TAC support	No (for deployment in production environments we recommend upgrading to one of the other two capacity versions)	Yes	Yes
Available as virtual machine or appliance	Virtual machine only	Virtual machine only	Virtual machine and appliance
Release and option keys required to install	No release or option key required	Option key to support 50 concurrent call sessions required	Full capacity TelePresence Conductor release key required

Scheduling with Cisco TMS

As the scheduling solution with Cisco TMS has notable limitations at this time, we recommend carefully considering these limitations and their workarounds prior to deployment. Upcoming releases of TelePresence Conductor and Cisco TMS will address these limitations, and an updated deployment guide for TelePresence Conductor with Cisco TMS will be made available at that time.

Current limitations:

- TelePresence Conductor may wait up to 30 seconds before releasing resources between meetings. This may cause denial of inbound and outbound calls for back-to-back meetings and utilization spikes when participants repeatedly leave and join a meeting. Bug toolkit identifier for this issue: CSCuf34880 [p.17]
- Cisco TMS scheduling with TelePresence Conductor does not currently support WebEx Enabled TelePresence.

Interoperability

The interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco TelePresence products.

Planned changes to future releases

In a future version of TelePresence Conductor the following changes are planned:

- Removal of the following feature:
  - **Support for TelePresence Conductor working as a policy server with the Cisco VCS.** In a future release TelePresence Conductor must be deployed using TelePresence Conductor's back-to-back user agent (B2BUA), with a SIP trunk to a Cisco VCS or a Unified CM.
  - **Ability to configure cascade advanced parameters for TelePresence MCU.** In a future release of TelePresence Conductor it may not be possible to configure advanced template parameters for cascade conference bridges separately from advanced template parameters for the primary conference bridge. We therefore recommend that you already configure the advanced parameters for primary and cascade conference bridges identically.
- Changes to the minimum supported versions for the following products:

- For Cisco VCS: version X7.2 or later
- For Unified CM: version 9.1.2 or later

Upgrading to XC2.4.1

Upgrade requirements

Note:

- Releases XC2.3 or later include a patch for CVE-2014-0160.
- After upgrading to XC2.3 or later we strongly recommend that you generate and install new server certificates on your TelePresence Conductor systems.

The upgrade requires you to have:

- a valid **Release key**, if you are upgrading the major release of the TelePresence Conductor (for example from XC1.2 to XC2.4.1).
  A release key is not required for:
  - dot releases (for example XC2.0 to XC2.4.1)
  - systems that are running without a release key and with limited capacity (as TelePresence Conductor Essentials)

  Note: If you do not supply a valid release key when upgrading the major release, your system will run as TelePresence Conductor Essentials with limited capacity.
- a software image file for the component you want to upgrade, stored in a location that is locally accessible from your client computer.

To avoid any performance degradation we recommend that you upgrade the TelePresence Conductor while the system is inactive.

Upgrading a standalone TelePresence Conductor

To upgrade a TelePresence Conductor that is not in a cluster the following procedure should be followed:

1. Log into the TelePresence Conductor web interface.
2. Create a backup of your configuration (under **Maintenance > Backup and restore**).
3. Upgrade using the **Upgrade** page (**Maintenance > Upgrade**) as described in the *Cisco TelePresence Conductor Administrator Guide*.

Upgrading a cluster of TelePresence Conductors

To upgrade a cluster of TelePresence Conductors the following procedure should be followed:

1. Remove the TelePresence Conductor that should be upgraded from the cluster, as described in the relevant *Cisco TelePresence Conductor Clustering Deployment Guide*.
2. Log into the web interface.
3. Create a backup of your configuration (under **Maintenance > Backup and restore**).
4. Upgrade using the **Upgrade** page (**Maintenance > Upgrade**) as described in the *Cisco TelePresence Conductor Administrator Guide*.

Optional configuration step if TelePresence Conductor Provisioning API is used

We recommend that any existing provisioned conferences on TelePresence Conductor are re-provisioned after an upgrade to XC2.4.1.

If the TelePresence Conductor's Provisioning API has been used to provision CMRs (Collaboration Meeting Rooms) using Cisco TMSPE version 1.2 or later, we recommend that you follow these steps:

1. In Cisco TMS, go to **Systems > Provisioning > Users**
2. Click **TelePresence Conductor Settings**
3. Click the icon to *Purge CMRs on TelePresence Conductor* (hover over the icons for the tool tip description)
4. Click **Purge CMRs**
5. Close the **TelePresence Conductor Settings** window
6. Click **Regenerate CMRs** (if the option is grayed out, refresh the page)

Downgrading from XC2.4.1

When downgrading from XC2.4.1 to XC2.2 or earlier, it is important that you do not use the same configuration that you had on the system while running XC2.4.1.

We recommend that you do a backup of your configuration before every upgrade or downgrade. When downgrading we advice you to restore the configuration back to what it was when running the earlier software version.

Using the Bug Search Tool

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

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

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

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

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

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

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

Technical support

If you cannot find the answer you need in the documentation, check the website at 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: www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

Additional information

Secure communications

For secure communications (HTTPS and SIP/TLS) we recommend that you replace the Cisco TelePresence Conductor default certificate with a certificate generated by a trusted certificate authority. See Cisco TelePresence Conductor Certificate Creation and Use Deployment Guide for TelePresence Conductor to generate certificate signing requests and install certificates.

Hardware shutdown procedure

The TelePresence Conductor uses a hard drive for storing logs. We recommend that you shut down the appliance prior to it being unplugged to ensure a clean shutdown process. This can be done from the web interface.

Initial installation

Initial configuration of the TelePresence Conductor IP address, subnet and gateway can be accomplished through the installation wizard via the serial port or through the front LCD panel. See *Cisco TelePresence Conductor Getting Started*.

Virtual machine

From XC1.2 the TelePresence Conductor software can run on VMware.

Before you can order your release key and any option keys, you must first download and install the .ova file in order to obtain your hardware serial number. The TelePresence Conductor provides limited capacity until a valid release key is entered.

Note that the .ova file is only required for the initial install of the TelePresence Conductor software on VMware. Subsequent upgrades should use the .tar.gz file.

See *Cisco VCS on Virtual Machine Installation Guide* for full installation instructions.

Third-party software included in TelePresence Conductor

Third-party software used in the TelePresence Conductor includes:

Third-party software	Version
Apache	2.4.2
OpenSSL (modified and packaged as CiscoSSL)	1.0.1e patched for CVE-2014-0160

This product includes copyrighted software licensed from others. A list of the licenses and notices for open source software used in this product can be found at: http://www.cisco.com/en/US/products/ps11775/products_licensing_information_listing.html.

Document revision history

Date	Revision	Description
October 2014	13	Release of Cisco TelePresence Conductor XC2.4.1
October 2014	12	Release of Cisco TelePresence Conductor XC2.3.1
September 2014	11	Release of Cisco TelePresence Conductor XC2.4
April 2014	10	Release of Cisco TelePresence Conductor XC2.2.2
April 2014	09	Release of Cisco TelePresence Conductor XC2.0.3
April 2014	08	Release of Cisco TelePresence Conductor XC2.3
February 2014	07	Updated description of minimum version alarm feature
October 2013	07	Release of Cisco TelePresence Conductor XC2.2.1
February 2014	06	Updated description of minimum version alarm feature
September 2013	06	Updated with resolved issues in XC2.2.
August 2013	05	Release of Cisco TelePresence Conductor XC2.2
May 2013	04	Release of Cisco TelePresence Conductor XC2.1
March 2013	03	Release of Cisco TelePresence Conductor XC2.0.2
February 2013	02	Release of Cisco TelePresence Conductor XC2.0.1
December 2012	01	Release of Cisco TelePresence Conductor XC2.0

Legal notices

Copyright notice

A list of the conditions of use can be found at:

http://www.cisco.com/en/US/docs/telepresence/infrastructure/conductor/license_info/Cisco_Conductor_EULA.pdf

This product includes copyrighted software licensed from others. A list of the licenses and notices for open source software used in this product can be found at:

http://www.cisco.com/en/US/products/ps11775/products_licensing_information_listing.html

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/).

This product includes software developed by the University of California, Berkeley and its contributors.

IMPORTANT: USE OF THIS PRODUCT IS SUBJECT IN ALL CASES TO THE COPYRIGHT RIGHTS AND THE TERMS AND CONDITIONS OF USE REFERRED TO ABOVE. USE OF THIS PRODUCT CONSTITUTES AGREEMENT TO SUCH TERMS AND CONDITIONS.