Cisco TelePresence Conductor XC2.0.3

Release Notes
April 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 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 (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*

New features in XC2

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 XC2.0.3

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
CSCuc88654	**Symptom:** Conductor does not handle audio only ports on MCUs, it only supports video ports Conductor only handles video participants joining a conference, and so it does not attempt to use MCU audio only ports. If the video ports get used up on an MCU, Conductor will roll over to using the next MCU pool in the service preference, it will not add users as audio only participants. **Versions affected:** XC1.2 or later **Workaround:** None
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. **Versions affected:** XC1.2 or later **Workaround:** Ensure that there is a maximum duration on any conferences that this may affect, so that the auto-dialed participant is not left waiting forever.

Limitations

TelePresence Conductor version XC2.0.3 supports:

- 30 conference bridges
- 30 conference bridge pools

- 30 Service Preferences
- 1000 conference templates
- 1000 conference aliases
- a maximum of 2400 concurrent calls
- a maximum of 104 concurrent calls per cluster of TelePresence Server blades
- conference bridge types of Cisco TelePresence MCU and Cisco TelePresence Server
- conference cascading on TelePresence MCUs only

It does not support:

- T3 point to point calls escalated to a conference functionality
- conference cascading on TelePresence Servers
- auto-dialed participants that are multiscreen endpoints
- advanced parameters for auto-dialed participants that are part of conferences hosted on TelePresence Servers

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.

Equipment	Minimum software version	Comments
Cisco Unified Communications Manager	8.6.2	
Cisco TelePresence Video Communication Server (VCS)	X7.0.1	
Cisco TelePresence MCU 4200 series	4.2	
Cisco TelePresence MCU 4500 series	4.2	
Cisco TelePresence MSE8000 blades 8420 and 8510	4.2	
Cisco TelePresence MCU 53XX series	4.3 (2.30)	All other MCUs used by the same TelePresence Conductor need to be running release 4.3(2.18) or later.
Cisco TelePresence Server	3.0 (2.46)	TelePresence Server must be running in 'Remotely managed' mode.
Cisco TelePresence Management Suite	13.1.2	Cisco TMS version 14.1 and TelePresence Conductor version XC1.2 are required to support scheduling on TelePresence Conductor.

Upgrading to XC2.0.3

Note:

- This XC2.0.3 release includes a patch for CVE-2014-0160.
- After upgrading to XC2.0.3 we strongly recommend that you generate and install new server certificates on your TelePresence Conductor systems.

Note that you will need a release key if you are upgrading to a new major release (for example from. XC1.2 to XC2.0). It is not required for dot releases (for example from XC1.1 to XC1.2).

Upgrading a standalone TelePresence Conductor

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

1. Stop the Cisco VCS from sending requests to TelePresence Conductor.
2. Log into the TelePresence Conductor web interface.
3. Create a backup of your configuration.
4. Upgrade using the **Upgrade** page (**Maintenance > Upgrade**) as described in the 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.
4. Upgrade using the **Upgrade** page (**Maintenance > Upgrade**) as described in the *Cisco TelePresence Conductor Administrator Guide*.

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
April 2014	09	Release of Cisco TelePresence Conductor XC2.0.3
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

The product that is covered by these release notes is protected under copyright, patent, and other intellectual property rights of various jurisdictions.

TANDBERG is now part of Cisco. Tandberg Telecom UK Limited is a wholly owned subsidiary of Cisco Systems, Inc.

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.