Cisco TelePresence Conductor XC3.0.2

Release Notes
Revised March 2015

Contents

Product documentation 1
New features in XC3 2
Open and resolved issues 4
Limitations 5
Interoperability 6
Planned changes to future releases 6
Upgrading to XC3.0.2 7
Downgrading from XC3.0.2 8
Using the Bug Search Tool 8
Technical support 9
Additional information 9
Document revision history 10
Legal notices 10

Product documentation

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

- *Cisco TelePresence Conductor Administrator 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 with Cisco TMS Deployment Guide*
- *Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified CM Deployment Guide*
- *Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS Deployment Guide*
- *Cisco TelePresence Conductor Certificate Deployment Guide*

- *Cisco TelePresence Multiway Deployment Guide*
- *Cisco TelePresence Conductor API Guide*

New features in XC3

New features in XC3.0.2

This is a maintenance release.

New features in XC3.0.1

API change

The XML RPC API call **`factory.conferencecreate`** has a new optional parameter called **`factoryOverrideConferenceDisplayName`**. It allows you to override the conference display name, which is normally generated automatically by TelePresence Conductor.

New features in XC3.0

Authentication required when changing an administrator account password

When you add a new administrator account or change the password for an existing administrator account, you are now required to authenticate yourself by entering your current administrator password. There are now two pages for editing administrator account details: one for changing the password and one for editing the remaining account details.

Ability to mark pools within a Service Preference to be used for scheduling

On the **Service Preference** page of the TelePresence Conductor user interface you can mark pools to be used for scheduling. Only marked pools will be included in Capacity Management API requests that clients such as Cisco TMS make. If you configure the marked pool to contain only a single conference bridge and you do not include the same pool in more than one Service Preference, Cisco TMS can use the pool for dedicated-bridge scheduling.

Note: After an upgrade to XC3.0, all existing pools in all Service Preferences are marked to be used for scheduling.

Support for WebEx calls to be included in scheduled conferences

It is now possible for scheduled conferences on TelePresence Conductor to include WebEx calls as well as TelePresence calls. Cisco TMS scheduling with TelePresence Conductor now supports Cisco Collaboration Meeting Rooms Hybrid (formerly known as WebEx enabled TelePresence).

Support for participant role determined by PIN

Conferences provisioned using the TelePresence Conductor Provisioning API, for example via Cisco TMSPE, now allow participant role to be determined by PIN. Hosts and guests dial the same alias and then experience different privileges based on the PIN they have entered. Guest PINs are optional. This feature is supported on TelePresence MCUs and on TelePresence Servers version 4.1 or later.

Ability to specify whether guests must wait for a host to join a conference first

It is now possible to specify in the TelePresence Conductor Provisioning API whether guests must wait for a host to join the conference before they are able to join. This setting is only applicable to

- Conferences provisioned through the Provisioning API (for example by Cisco TMSPE)
- Conferences hosted on TelePresence Servers

Support for multistream calls

Multistream calls are now supported when you are using endpoints and TelePresence Servers that also support this feature. TelePresence Conductor forwards the relevant SDP (session description protocol) information from the endpoints to the TelePresence Servers.

Support for up to three SIP trunk destinations

You can specify up to three SIP trunk destinations, consisting of an IP address and a SIP port, for each rendezvous Location defined on the TelePresence Conductor user interface. The TelePresence Conductor considers all SIP trunk destinations for a Location as equivalent and may use any one of the destinations for out-dial calls, as long as the destination is reachable. The TelePresence Conductor maintains only one of the destinations, it does not load balance the dial-out calls across the configured destinations. If the current destination becomes unreachable, it automatically chooses a new SIP trunk destination.

SIP trunk destinations cannot be specified for ad hoc Locations, unless the **Conference type** of the Location is set to *Both*.

TelePresence Conductor regularly polls its SIP trunk destinations and reports reachability changes

TelePresence Conductor uses a SIP OPTIONS ping to regularly poll all SIP trunk destinations configured for the call control devices that are connected to it. This includes all Unified CMs and any Cisco VCSs connected using the back-to-back user agent (B2BUA).

If there is a response from the SIP trunk destination, it is considered to be reachable. If there is a change in the reachability, either from reachable to unreachable or vice versa, the state is reported in an event log message. If any SIP trunk destinations are unreachable, an alarm is raised. The alarm is lowered if all SIP trunk destinations are reachable again.

Syslog publish filter

You can now filter the logs that TelePresence Conductor sends to each remote syslog host by severity level.

For example, your syslog host is typically receiving syslog messages from multiple systems, so you may want to limit TelePresence Conductor to sending only "Error" messages (and anything more severe) to this host. If you want to leave the host untouched while troubleshooting a TelePresence Conductor problem, you could configure a second, temporary, host to receive "Debug" level (most verbose = messages of all severities). Then you could safely remove the configuration after resolving the issue, without risking your primary syslog host.

User interface change

The menu path to the **IP** and **Ethernet** pages has changed to **System > Network interfaces > IP** and **System > Network interfaces > Ethernet** respectively.

API changes

- The XML RPC API call **`factory.conferencecreate`** has a new optional parameter called **`factoryLayout`**. It takes the following values:
  - equal
  - active
  - prominent
  - single

It allows you to override the layout specified within the **layout** parameter of the **ConfBundle** object in the Provisioning API.

- The XML RPC API has a new call - **factory.conferencemodify**. It allows you to modify the values of the parameters that were set when the conference was created using the call **factory.conferencecreate**.
- The XML RPC API calls **conference.create** and **conference.modify** have been deprecated. Use **factory.conferencecreate** and **factory.conferencemodify** instead.
- The API call **factory.conferencecreate** now returns the **factoryConferenceId** and **conferenceName** values where possible. This includes successful calls as well as some failed calls.
- The XML RPC API call **participant.message** now allows the API client to specify the position and duration of the message displayed on the participant's screen.
- It is now possible for API clients to lock and unlock a conference on TelePresence Conductor. If a conference is locked, it keeps running with its existing participants. No new participants can dial into a locked conference, but API clients, such as Cisco TMSPE, can add more participants to a conference via the API call **participant.add**. The XML RPC API calls **factory.conferencemodify** and **conference.modify** have a new Boolean parameter called **locked**.
- The XML RPC API call **participant.enumerate** has a new return value - **factoryCallState**. It is returned as part of the participant struct and takes the values disconnected, ringing, connected, awaitingTrigger, callLegFailed and retrying. The new **factoryCallState** allows TelePresence Conductor to provide to its API clients more detailed state information about the participants in a conference.
- The Provisioning API object **ConfBundle** has a new Boolean attribute called **guests_wait_for_host**. It allows you to specify whether guests must wait for a host before they can join a conference. It is only applicable to TelePresence Server hosted conferences. The attribute is ignored for TelePresence MCU hosted conferences. The default value is *False*.
- The strings **factoryConferenceId** and **factory_conference_id** that are returned after issuing the API call **factory.conferencecreate** have been modified. They are now opaque strings that no longer resemble UUIDs.

Other changes

The certificate signing request storage location changed in XC3.x.

When you generate a CSR in XC2.x, the application puts **csr.pem** and **privkey_csr.pem** into **/tandberg/persistent/certs**.

When you generate a CSR in XC3.x, the application puts **csr.pem** and **privkey.pem** into **/tandberg/persistent/certs/generated_csr**.

If you want to upgrade from XC2.x and have an unsubmitted CSR, then we recommend discarding the CSR before upgrade, and then regenerating the CSR after upgrade.

Open and resolved issues

Follow the links below to read the most recent information about the open and resolved issues in this release. You need to refresh your browser after you log in to the Cisco Bug Search Tool.

Table 1: Bug Search Tool queries for this release

Issue type	Link to list of issues
Open issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283884153&rls=XC3.0.2&sb=anfr&sts=open&svr=3nH&srtBy=byRel&bt=custV
Resolved issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283884153&rls=XC3.0.2&sb=anfr&sts=fd&svr=3nH&srtBy=byRel&bt=custV
All issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283884153&rls=XC3.0.2&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Limitations

Full capacity TelePresence Conductor version XC3.0.2 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
- 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
- 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

	TelePresence Conductor Essentials (free)	TelePresence Conductor Select	Full capacity TelePresence Conductor
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)
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

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.
- Cisco TMS scheduling with TelePresence Conductor does not currently support CMRs that have been provisioned using Cisco TMSPE.

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.

Scheduling with Cisco TMS

To support scheduling with Cisco TMS the minimum required versions are TelePresence Conductor XC3.0 or later and Cisco TMS 14.6 or later. See Scheduling with Cisco TMS [p.6] for current limitations.

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
- Deprecated support for the following products:
  - Cisco TelePresence MCU MSE 8420
  - Cisco TelePresence MCU 4200 Series

Upgrading to XC3.0.2

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 XC2.4 to XC3.0.
  A release key is not required for:
  - dot releases (for example XC2.3 to XC2.4)
  - 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 XC3.0.2.

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 XC3.0.2

When downgrading from XC3.0.2 to XC2.2 or earlier, it is important that you do not use the same configuration that you had on the system while running XC3.0.2.

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 *TelePresence Conductor 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	Description
March 2015	Updated interoperability and limitations with Cisco TMS scheduling
February 2015	Release of Cisco TelePresence Conductor XC3.0.2
February 2015	Release of Cisco TelePresence Conductor XC3.0.1
January 2015	Release of Cisco TelePresence Conductor XC3.0

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.