Cisco TelePresence Conductor XC4.3.2

Release Notes

First Published: January 2018

Product Documentation

Note: If no specific guide exists for your particular software version, the last published version will be applicable.

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 Collaboration Meeting Rooms (CMR) Premises Deployment Guide Release 5.0*
- *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

XC4.3.2 is a maintenance release. For more information, see Open and Resolved Issues, page 7. It also introduces the new features detailed below.

Changes to TLS and Cipher Suite Defaults

From XC4.3.2, TelePresence Conductor defaults to TLS version 1.2 when establishing secure connections for the following services:

- HTTPS
- SIP

For improved security, TLS 1.2 or later is recommended for all encrypted sessions. If required (typically for compatibility reasons with legacy equipment) the minimum TLS versions can be configured to use versions 1.0 or 1.1 via the xConfiguration CLI commands (see TLS Version Configuration Examples, page 3).

Note: On upgrade and new installations the system will default to the new secure TLS version 1.2. Check that all browsers and equipment that must connect to TelePresence Conductor supports TLS version 1.2.

New Cipher Suites

You can configure the cipher suite and minimum supported TLS version for each service via the xConfiguration CLI commands. For more information, see the Reference section of the Online Help or the Administration Guide.

These services and new cipher suites are shown in the table below. (The cipher strings are in OpenSSL format.)

Services	Cipher Suite Values (Defaults)
HTTPS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
SIP TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH

Note: The "aNULL" cipher is not allowed for inbound SIP connections. When you configure SIP TLS ciphers, the string you supply is used unmodified for outbound connections, but it acts as if "!aNULL" were appended when handling inbound connections.

Known Issues

The following are known issues with TLS version 1.2 support and you will need to downgrade the relevant TLS version setting on Conductor via the xConfiguration CLI commands to a mutually supported TLS version:

- Legacy endpoint TLS version support:
  - MXP and TE Series devices do not support TLSv1.2
  - TC < 7.3.3 does not support TLSv1.1 or TLSv1.2
  - TC 7.3.6 removed support for TLSv1.0

  - Jabber Video for TelePresence on Windows 7 does not support TLSv1.1/1.2 (supported from Windows 8.1, see below)
- Windows:
  - Windows 7 and Windows Server 2008 R2 added TLSv1.1/1.2 support but **off** by default; post Windows 8.1 they are on by default. This impacts Jabber Video for TelePresence, TMS, Lync and other software and services running on Windows using the OS TLS APIs.
  - Windows Server 2003.does not support TLSv1.1 or TLSv1.2.
- Third-party endpoints:
  - Lifesize Icon 600 does not support TLSv1.2
- Restarts:
  - SIP requires a restart after changing cipher suite configuration or TLS protocol version.
- Cisco
  - TMS-PE currently only supports TLSv1.0.

TLS Version Configuration Examples

It may be necessary to enable older versions of TLS on TelePresence Conductor for compatibility with other devices. For example, TMS-PE requires the use of TLS 1.0. To allow this:

1. Log in as `admin` on the console.
2. Enter the command: `xconfiguration Ciphers HTTPSProtocol Value: "minTLSv1.0"`

   Note that this also allows the use of TLSv1.0 for connections from web browsers and for API connections.

If you have a device that uses Conductor's feedback receivers and is not compatible with TLSv1.2, configure Conductor as follows:

1. Log in as `admin` on the console.
2. Enter the command: `xconfiguration Ciphers outbound_HTTPS_TLS_versions Value: "TLSv1:TLSv1.1:TLSv1.2"`

   Note that this also allows the use of the specified versions of TLS for connections to conference bridges.

   You can omit "TLSv1" or "TLSv1.1" if you know it is not needed. However, it is useful to leave "TLSv1.2" in the configuration even if you know it will not currently be used as it avoids any incompatibility if you later upgrade the other device.

Support for ESXi 6.5

Telepresence Conductor now supports ESXi 6.5.

New Features in XC4.3

Mute voice prompts

Update to the **Conference localization** feature (**Conference configuration** > **Global settings**) which lets you select a language for the voice and text prompts used with TelePresence Server-hosted conferences.

The **Voice prompts** menu was added, allowing you to enable (*Yes*) or disable (*No*) voice prompts. The default setting is `Yes`.

Note: Localized voice prompts require TelePresence Server software release 4.3 or later.

Voice and text prompts support for Dutch

Update to the **Conference localization** feature (**Conference configuration** > **Global settings**). The **Language** menu now offers the Dutch language for voice and text prompts.

Multiparty license expiration warning

An alarm was added (Status > Alarms) which displays three days before a Multiparty license will expire.

New Features in XC4.2

Conference localization

The **Conference localization** feature (**Conference configuration** > **Global settings**) lets administrators select a language for the voice and text prompts used with TelePresence Server-hosted conferences.

Languages include:

English (US), English (UK), Chinese (Simplified), Chinese (Traditional), Danish, Finnish, French (European), French (Canada), German, Italian, Japanese, Korean, Polish, Portuguese (Brazil), Russian, Spanish (European), Spanish (Latin America), Swedish and Turkish.

For a complete list of voice and text prompts and details on how to add custom voice prompts on TelePresence Server, refer to the Reference section of the Cisco TelePresence Conductor XC4.2 Administration Guide.

Note: Localized voice prompts require TelePresence Server software release 4.3 or later.

Support for temporary Multiparty Licenses

Temporary Multiparty Licenses let you test Multiparty Licensing without buying a license. These trial licenses are temporarily valid for a specific duration. If you decide not to install permanent Multiparty Licenses (SMP or PMP), note that when the temporary license expires, **Conductor automatically reverts to screen licensing mode**. So meetings will fail if no screen licenses are installed on TelePresence Server at that time.

In XC4.2, notification is not given prior to license expiry, so it’s important to track the duration of temporary licenses. This issue is resolved in XC4.3. When a temporary license expires, the number of licenses is automatically recomputed without it. If the Multiparty License count goes down to zero, the Conductor reverts to Screen License mode at midnight local time on the day after the last license expires.

Multiparty Licensing enforcement

Multiparty Licensing is now enforced by allowing administrators 15 calendar days of non-compliance in a rolling window of 60 calendar days. On the 15th day, an “out-of-compliance” banner is displayed on all endpoints within all conferences. The out-of-compliance banner can only be removed by obtaining and installing more Multiparty Licenses.

There is also a 60-day grace period after the first non-compliance during which the banner will not be displayed.

Support for 2048-bit encryption for SSL

Selected by default. Added to support Cisco TMS.

Note: Please note that upgrading Conductor to XC4.2 requires upgrade to TMS 15.2, TMSPE 1.7 and Java 8 on systems where TMS components are installed. Java 8 must be installed on the TMS before the Conductor is upgraded. Conductor’s security certificates default to 4096-bit. Customers who use 4096-bit certificates must edit the java.security file to ensure conferences are successful. For details, see the Upgrading to XC4.2 section.

Resource usage reporting enhancements

Resource usage logging now includes all the conference bridges it manages, regardless of whether they've been used. Unused bridges are shown as 0%. The **resource_utilization_updated** event in the usage report (**Maintenance** > **Diagnostics** > **Usage report**) is recorded for each bridge at midnight of each day. This eliminates the need to use macros in a manual process outside of Conductor for graphing the capacity of all available bridges regardless of whether they were actually used during the window of the graph.

Cluster communication protocol change

UDP/IPSec are replaced with TCP/TLS to improve reliability and enhance security. When you upgrade a cluster, the cluster comes up in TLS permissive mode. Permissive mode does not verify certificates when establishing a connection with clustering peers.

TCP port 4371 is used for cluster recovery and port 4372 is used for database synchronization.

'Guests wait for host' feature for Lecture conference type on TelePresence Server

This feature (**Conference configuration** > **Conference templates**) determines whether or not guests must wait for a host to join a conference before seeing, hearing and sharing a presentation with other participants.

Yes: Guests joining before the host must wait for the host to join.

No: Guests do not have to wait for the host to join. (Default)

Note: This feature has always been available through the API.

New Features in XC4.1

Usage report

A new page called **Usage report** (**Maintenance** > **Diagnostics** > **Usage report**) lets you download a log file that contains usage information. Up to 10 GB of log entries can be stored and available for download. Logging is automatically enabled and runs when events take place. Available download formats include CSV, XML and JSON. The report is designed to help you determine everyday bridge utilization and hourly usage.

Conference placement settings

This setting on the new **Global settings** page **(Conference configuration** > **Global settings**), allows you to specify how Conductor selects bridges. Choose the option that corresponds with the most common type of conference in your company.

- Favor Scheduled: selects the bridge with the fewest conferences currently in progress (better for conferences that start at the same time). This is the default setting.
- Favor CMRs: selects the bridge with the most spare capacity (better for conferences with staggered start times).

Support for Active Meeting Manager in TMSPE

Conference hosts can now control their Personal CMRs using Active Meeting Manager in TMSPE, providing a user-friendly alternative to using the endpoint control panel and replacing the capabilities of Conference Control Center in TMS.

Note: Scheduled meetings are not currently supported with Active Meeting Manager.

SIP domain override settings

If you are using a deployment that does not include a TMSPE, you can configure the SIP domain on the new **Global settings** page **(Conference configuration** > **Global settings**). When a SIP call comes in, the Conductor IP address or FQDN will be replaced with the configured SIP domain. The results will be matched against the configured aliases.

Example: 1234@conductor_ip / 1234@conductor_fqdn becomes 1234@configured_sip_domain

Note: The SIP domain overrides additional IP FQDNs

API changes

- Added the following new parameters to the Support for the `conference.enumerate` API call:
  - `factoryConfBundleId`: The UUID associated with this Conference Bundle/CMR. This is pushed by TMSPE using the ConfBundle API. This attribute is returned only when the conference is a CMR.

- `factoryOwnerId`: The `ownerID` that is passed when the Conference Bundle/CMR is configured. This is pushed by TMSPE using the ConfBundle API. This value is returned when Conductor can associate the conference with an `ownerID`.

New Features in XC4.0

Multiparty licenses

This new TelePresence Server licensing model is user-based instead of screen-based.

Two types of Multiparty licenses are supported:

- Personal Multiparty (PMP). Each license is assigned to a specific user. PMP licenses are suitable for users who initiate conferences frequently.
- Shared Multiparty (SMP). Each license is shared by multiple users, but only in one conference at a time. SMP licenses are suitable for users who initiate conferences infrequently.

To support Multiparty Licensing, connections between TelePresence Conductor and the conference bridges must use HTTPS. (We recommend HTTPS in any case.)

Multiparty Licensing requires the following product versions:

- TMS 15.0 or later
- TMSPE 1.5 or later
- TelePresence Server 4.2 or later

Support for Unified CM:

- Unified CM 10.5 is recommended.
- Earlier versions can be used, but have not been fully tested by Cisco in time for this release.
- The minimum supported version of Unified CM is 8.6.2.

If any issue arises using Unified CM with Multiparty Licensing, contact the Cisco Technical Assistance Center (TAC) for support. We will document issues in the release notes and, if necessary, create new defects (viewable using the Bug Search Tool).

Note: Cisco may decide to not resolve defects depending on the Unified CM version and the impact of the defect. If a defect is not resolved, you must choose to either upgrade to a newer version of Unified CM to resolve the issue or keep your existing version and accept that the issue will continue to exist.

Note: The total license capacity of Personal Multiparty (PMP) or Shared Multiparty (SMP) license option keys in a cluster is the sum of the individual PMP or SMP keys configured on each peer in the cluster.

FQDNs for additional IP addresses for LAN 1

An FQDN is required for additional IP addresses if you want to use a public certificate authority to sign the Conductor certificate. The recommended way to configure Conductor is to add for ad hoc and rendezvous addresses and to add those into the public certificate.

TelePresence Server encryption key no longer required

An encryption key is no longer required to use TelePresence Server version 4.2 or later. The message on the **Conference bridge status** page has changed from "Encryption key installed" to "Signaling encryption enabled". Before TelePresence Server version 4.2, signaling encryption was enabled only if the encryption key was installed. The term "Encryption Key" is replaced with "Media Encryption Key" beginning in version 4.2. Most customers outside of Russia will still want to install this key. Encryption keys installed in TelePresence Servers running a software version earlier than 4.2 are automatically converted to media encryption keys when upgrading to version 4.2 or later.

User interface changes

On the **Option keys** page there is a new field called **Multiparty licensing for TelePresence Servers**. This field allows you to choose whether all TelePresence Servers managed by this TelePresence Conductor should use Multiparty licenses or not. If Multiparty License mode is enabled, the TelePresence Conductor manages the licenses for all TelePresence Servers. If Multiparty License mode is disabled, all TelePresence Servers manage their own screen licenses.

Note: To use Multiparty Licensing mode, at least one option key for Personal Multiparty or Shared Multiparty must be installed.

A new page called **Multiparty license status** (**Status** > **Multiparty licenses**) has been added. This page displays PMP and SMP license usage and compliance status when multiparty license mode is enabled.

Two new alarms have been added to indicate when usage of multiparty licenses has exceeded the number of licenses installed on the TelePresence Conductor cluster:

- PMP license alarm: Raised when the number of PMP license owners exceeds the number of installed PMP licenses.
- SMP license alarm: Raised when the peak number over the last 60 days of SMP-licensed conferences exceeds the number of installed SMP licenses.

Note: For more information about Multiparty License mode and usage, refer to Adding Option and Release Keys, page 140, and Multiparty License Status, page 124, in the Cisco TelePresence Conductor Administrator Guide (XC4.0).

On the **Overview** page there is a new field called **Multiparty license status** which indicates when Multiparty License mode is enabled or disabled. Clicking the field name takes you to the **Multiparty license status** page, where you can view the number of installed and used licenses.

On the **IP** page, when adding additional addresses for LAN 1, there is new field called **FQDN**.

API changes

- Support for the `conference.create` struct `ownerID`.
- Support for the `factory.conferencecreate` struct `factoryOwnerId`.
- Addition of a new Owner API, which consists of an array of `Owner` objects, PUT and DELETE methods.
- Addition of the new `ConfBundle` attribute `owner_id`(optional, string).
- Addition of the `multipartylicense` REST API.
  - Addition of the new value `multiparty_license` for the attribute `bridge_capabilities`, used in the `ServiceInfo` object.

Open and Resolved Issues

Follow the links below to read the most recent information about the open and resolved issues in this release.

Resolved Issues

Issues seen in previous releases that are fixed in XC4.3.2:

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283884153&rls=XC4.3.2&sb=fr&sts=fd&bt=empCustV

Open Issues

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283884153&rls=XC4.3.2&sb=afr&sts=open&bt=empCustV

Limitations

Full capacity TelePresence Conductor version XC4.3.2 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 2 TelePresence Conductors to achieve resilience (full capacity versions only)
- Multiparty license limits:
  - PMP: 50,000 licenses
  - SMP: 1,200 concurrent meetings

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
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 2 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
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.

Adding TelePresence Conductor to Cisco TMS

If TelePresence Conductor is configured with Automatic Discovery Protection (available in **System -> System Administration -> System Protection**) enabled (on), then adding TelePresence Conductor to Cisco TMS may not be successful. The workaround is to ensure that Automatic Discovery Protection is disabled (off). However, note that it is important to do this across all Conductor nodes in a cluster (where clustering is used). Automatic Discovery Protection is configured via the web interface in **System Protection > System** tab. Once a TelePresence Conductor has been successfully added to Cisco TMS, Automatic Discovery Setting can be re-enabled if desired.

Endpoint support to allow dial back into TelePresence Server hosted conferences

This release adds support that allows endpoints to dial back into TelePresence Server hosted conferences during instances like after a missed or accidental call drop. This is possible only if the conference is available for dial-in.

In order to achieve this, TelePresence Conductor sets the correct SIP header information (**From** field) while dialing to the endpoints from TelePresence Server, to allow the endpoint to dial back in.

Conductor will populate the **SIP** header with <**conference_number>@<domain**> where domain is determined as follows:

1. If configured, the domain set in Conductor's web interface under **Conference Configuration" -> "Global Settings" -> "SIP domain for numeric URIs** will be used in all situations.
2. Else, Conductor will attempt to determine the domain based on information it receives while creating the conference.
3. If Conductor is unable to identify a domain using the methods given above, then the Bridge IP address will be used.
   Note: Dial-back will not be possible in this case.

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, page 9 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
- Support for the following products will be deprecated in a future release:
  - MCU 4500 Series
  - Cisco TelePresence Server 7010

  Note that Cisco TelePresence MCU MSE 8420 and 4200 Series are no longer supported by TelePresence Conductor with this release.

Upgrading to XC4.3.2

Upgrade Requirements

Note:

- Upgrading to XC4.3.2 requires upgrade to TMS 15.2 and TMSPE 1.7. Java 8 must be installed on TMS or any system where TMS components are installed.
- 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.
- If a TelePresence Server is upgraded to version 4.2 while it is controlled by a Conductor running software version earlier than XC4.0, the Conductor will generate an encryption key alarm until it is upgraded to release XC4.1. You can ignore this alarm, because TelePresence Server 4.2 supports TLS even if an encryption key is not installed. To avoid the alarm, you can upgrade Conductor to version XC4.1 before upgrading the TelePresence Server to version 4.2. However, this method is not recommended and not guaranteed to be supported in the future.
- Customers who use 4096-bit certificates must follow the procedure in Enabling 4096-bit Encryption, page 11.

The upgrade requires the following:

- a valid **Release key**, if you are upgrading to a major release of the TelePresence Conductor (for example from XC3.0 to XC4.3.2).

  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 to a 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.
- release notes for the software version you are upgrading to — additional manual steps may be required.

Installing the release key and activating the software

Full version upgrades or downgrades require a current service contract. Register for a software upgrade license and activate the software using the following steps:

- Register for a version upgrade at: http://www.cisco.com/go/license
- Receive an activation key email containing release key (version-specific)
- Download the correct software version at: http://www.cisco.com/go/support
- Install the software following the steps for upgrading a standalone Conductor or cluster of Conductors.
- Install the release key from the activation key email.

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*.

Enabling 4096-bit Encryption

To enable 4096-bit encryption on TMSPE, the following procedure must be followed:

Edit **<jre-path>\lib\security\java.security** and insert an entry for bouncy castle as below (shown in **bold**). The other entries are incremented by 1, so the contents should be:

```
security.provider.1=sun.security.provider.Sun

security.provider.2=org.bouncycastle.jce.provider.BouncyCastleProvider

security.provider.3=sun.security.rsa.SunRsaSign

security.provider.4=sun.security.ec.SunEC
security.provider.5=com.sun.net.ssl.internal.ssl.Provider

security.provider.6=com.sun.crypto.provider.SunJCE

security.provider.7=sun.security.jgss.SunProvider

security.provider.8=com.sun.security.sasl.Provider

security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI

security.provider.10=sun.security.smartcardio.SunPCSC

security.provider.11=sun.security.mscapi.SunMSCAPI
```

Note: If you do not make the above change, users will not be able to edit their Personal Collaboration Meeting Rooms (CMRs) and TMSPE will not be able to access Conductor. In addition, the following error will be displayed in the TMSPE logs: *VMR::ConductorConnector - TelePresence Conductor failure with: Could not generate DH keypair*.

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 XC4.3.2.

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 XC4.3.2

When downgrading from XC4.3.2 to XC3.0 or earlier, it is important that you do not use the same configuration that you had on the system while running XC4.3.2.

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.

Obtaining Documentation and Submitting a Service Request

Use the Cisco Notification Service to create customized flexible notification alerts to be sent to you via email or by RSS feed.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Additional information

Call Rate Performance

As part of Cisco's ongoing validation of key product metrics for new application releases, we have confirmed that TelePresence Conductor's maximum supported incoming call rate is 100 calls per minute for each peer in a cluster or when used stand-alone. For a cluster of two peers, the aggregate incoming call rate is a maximum of 200 calls per minute, but neither peer should individually exceed 100 incoming calls per minute at any time.

As the overall size of a deployment increases it is possible that the join latency will increase and that it will take longer for conference metrics to stabilize.

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.

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

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 and supported VMware versions.

Systems Deployed Using XC3.0 OVA or Earlier

Between XC3.0 and XC4.0, the OVA file was modified to add CPU and RAM reservations. If you have deployed XC3.0 OVA or earlier we recommend that you add CPU and RAM reservations manually via vSphere to remain compliant.

Note: The specification-based VM recommends a minimum CPU speed of 2.8GHz, regardless of deployment size. The option of lower reservations maintains backwards compatibility.

Recommended Reservations

For small deployment	3600 MHz CPU 4 GB RAM
For medium deployments	4800 MHz CPU 6GB RAM

Document Revision History

Date	Description
January 2018	Re-release of Cisco TelePresence Conductor XC4.3.2 maintenance release.
September 2017	Release of Cisco TelePresence Conductor XC4.3.2 maintenance release.
June 2017	Updated to include VM note re. systems deployed using XC3.0 OVA or earlier.
March 2017	Release of Cisco TelePresence Conductor XC4.3.1 maintenance release.
January 2017	Open and Resolved Issues links updated. Note added re. incorrect OVA file labelling. See Virtual Machine, page 13
December 2016	Limitation added—Optimization not currently working.
September 2016	Release of Cisco TelePresence Conductor XC4.3

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.

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.

Cisco Legal Information

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

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

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

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

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

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

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

Cisco Legal Information

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