Cisco TelePresence Management Suite 15.0

Software Release Notes
Last Updated on March 2016

Product Documentation

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

- *Cisco TelePresence Management Suite Installation and Upgrade Guide*
- *Cisco TelePresence Management Suite Administrator Guide*
- *Cisco TMS Extensions Deployment Guides*

New Features in 15.0

Moved Audit Log Settings to TMS Tools

Improved application security by moving the following settings to TMS Tools:

- **Administrative Tools > Configuration > General Settings > Enable Auditing**
- **Administrative Tools > TMS Server Maintenance > Audit Log data purge settings**

You can no longer edit the audit log settings from the Cisco TMS application.

To enable auditing and to view and purge audit log data, go to **TMS Tools > Advanced Security Settings > Auditing**.

Improved Cisco TMS Performance

The overall performance of Cisco TMS has been significantly improved by running IIS Application Pool in a 64-bit mode.

Removed Support for Legacy Systems

The support for the following systems has been removed from Cisco TMS:

- VCON endpoints
- BioData Babylon Encryptor
- AdTran Atlas systems

After removing support for VCON endpoints, BioData Babylon Encryptor, and AdTran Atlas systems, Cisco TMS 15.0 will now handle these legacy systems as follows:

- Any VCON endpoints, BioData Babylon Encryptor and AdTran Atlas systems in your Cisco TMS will display **SystemType** as *System Not Found*.
- These endpoints should be added to Cisco TMS as *Unmanaged Endpoint*.

Removed Reports

The following reports have been removed from Cisco TMS:

- **Reporting > System > Low Battery On Remote Control**
- **Reporting > System > FTP Audit**
- **Reporting > Return On Investment > Return On Investment Global**
- **Reporting > Return On Investment > Return On Investment Local**
- **Reporting > CO2 Savings**
- **Reporting > Network > Packet Loss Log**
- **Reporting > Network > Packet Loss Conference**
- **Reporting > Network > Bandwidth Usage**

In addition the following fields have been removed from **Administrative Tools > Configuration > Statistics Settings**:

- **Statistics ROI Average System Cost**
- **Statistics ROI Average Travelling Cost**
- **Statistics ROI/CO2 Average Number of Participants per Endpoint**
- **Statistics ROI/CO2 Minimum Call Duration**
- **Statistics CO2 Cost Per Travel Per Person (Kg CO2)**

The **Network History** menu under **Network** has been renamed as **History** and has been moved to **Reporting > System**.

Removed Checking of Client Certificates

Request Client Certificates for HTTPS API has been removed from **Transport Layer Security Options** in **Cisco TMS Tool > Security Settings > Advanced Security Settings**.

Removed Export Report to PDF Feature

The option to export reporting data to a PDF file is no longer available in Cisco TMS. For all reports that supported this feature, the **Report** tab and the following buttons have been removed:

- **Export Report to PDF**
- **Conference Report** from **Booking > List Conference**.

It is possible to extract reporting data using the **Export to Excel** feature.

The **Disable Statistics Report** field has also been removed from **Administrative Tools > Configuration > Statistics Settings**.

Renamed Statistics Settings Menu

The **Statistics Settings** menu name has been changed to **Reporting Settings**. In addition the following fields have also been updated under **Administrative Tools > Configuration > Reporting Settings**:

- **Reporting History (in days)**
- **Reporting Default Start Time**
- **Reporting Default End Time**

Enabled Early Join for Scheduled Point to Point Calls

Participants in a point-to-point conference are now able to join five minutes prior to the scheduled time when **Allow Participants to Join 5 Minutes Early** under **Conference Connection** in **Administrative Tools > Configuration > Conference Settings** is set to *Yes*. This enables the "Join" button to appear for all types of participants in a conference.

Added Option to Choose a Preferred Call Protocol

The option **Preferred Protocol in Routing** allows you to choose a call protocol between *H.323* and *SIP* when routing a conference. This feature is added in **Administrative Tools > Configuration > Conference Settings**, under **Advanced** section.

Added System Support

Support for the endpoints that run on Collaboration Endpoint Software (CE) 8.0 has been added to Cisco TMS.

Updated Settings for Endpoints

Users of Collaboration Endpoint Software 8.0 will now be able to configure Cisco Intelligent Proximity Settings in Cisco TMS.

The new setting has been added to **Systems > Navigator >** select an end point that runs on Collaboration Endpoint Software 8.0 **> Settings > Cisco Proximity Settings**.

Added New Configuration Template

The configuration template for Collaboration Endpoint Software 8.0 has been added to Cisco TMS.

Configurable User Credentials to Add CE

An option to change the user name (other than the "admin" user) is added to create and manage CE software endpoints in Cisco TMS for communication. You can edit passwords of CE endpoints for the credentials that is currently used in Cisco TMS. This changes the password on the endpoint and makes Cisco TMS use the new password. To edit the password in Cisco TMS, select the CE endpoint to use and navigate to **Settings > Edit Settings** in **General** and type in the **Password** text box.

Security Enhancements

This release includes security enhancement features to Cisco TMS.

Improved Communication Security

For enhanced secure communication, two security settings have been merged into a single new setting, **Communication Security**. We have removed the options **Secure-Only Device Communication** and **Validate**

Certificates in **Administrative Tools > Configuration > Network Settings** under the **Secure-Only Device Communication** section. Now you can set the level of Communication Security between *Medium*, *Medium-high* and *High* for all connections of Cisco TMS, described below:

- *Medium*: Cisco TMS prefers HTTPS for communication, but falls back to HTTP. It remembers the last used protocol for the system in the previous communication and continues to use the same protocol. Insecure protocols like Telnet and SNMPv2 are also used.
- *Medium-High*: Cisco TMS will communicate only using SSL for connections. SSL includes HTTPS and SSH.
- *High*: Cisco TMS will communicate only using SSL for connections and will check that valid and signed certificates are present during communications.

For new installations and upgrades, the default value is set to *Medium*. However, you can change the settings for higher communication security. When *Medium-High* or *High* is selected, systems such as CTS, TCS, and Polycom HDX will lose some or all functionalities in Cisco TMS.

To find this new setting, navigate to **Cisco TMS Tools > Security Settings > Advanced Security Settings** below **Transport Layer Security Options**.

Improved Banner Functionality

Cisco TMS now adds custom banners to email templates in addition to web UI and reports. You can also choose color and text for banners from Cisco TMS Tools application. To apply banners, navigate to **Cisco TMS Tools > Security Settings > Advanced Security Settings**, under **Banners**.

Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA)

Support for WebEx Exceptions

WebEx exceptions are now supported in Cisco TMSBA if booked with the **OwnedExternally** flag, if the Cisco TMSBA client announces API version 16 or above. This Cisco TMSBA feature is in preparation for exception support in a future WebEx release. See Cisco Collaboration Meeting Rooms (CMR) Hybrid Release Notes for your version of Cisco TMS and WebEx Meeting Center for updates on WebEx support for recurring meeting series exceptions.

The following *WebExInstanceType* elements a client can use to schedule a WebEx conference with exception:

- *Normal*: The instance WebEx data is the same as the series WebEx data.
- *Modify*: The instance WebEx data is different from the series WebEx data.
- *Delete*: There is no WebEx data for the instance.

OwnedExternally

The **OwnedExternally** attribute of the WebEx object controls whether the WebEx meeting was originally booked by an external client. This attribute is primarily intended for use by Cisco TMSXE and other Cisco products, but could also be used by other Cisco TMSBA clients when scheduling Cisco CMR Hybrid meetings.

Cisco TMSBA clients that book with **OwnedExternally** set to *True* are responsible for integrating with the WebEx cloud on their own. The client must first schedule a meeting in the WebEx cloud using the WebEx APIs, and then provide the WebEx details (such as the *SiteUrl*, *HostKey*, and other attributes) returned by the WebEx API to Cisco TMSBA when scheduling the telepresence part of the Cisco CMR Hybrid meeting. When **OwnedExternally** is set *True*, Cisco TMS will attempt no validation of the provided WebEx data, as this is expected to be the responsibility of the client.Cisco TMS will only reserve a conference bridge for the meeting, and instruct the bridge to dial out to WebEx (use the dial string specified by the client in the *SipUrl* element) at the scheduled start time.

When booking with **OwnedExternally** set *True*, Cisco TMSBA allows WebEx to be added to or removed from single instances of recurrent series, as well as moving instances of Cisco CMR Hybrid -enabled recurrent series in time. For conference series where WebEx is **OwnedExternally**, Cisco TMSBA also supports providing different WebEx data for individual instances of the series, such as changing some instances to use a different WebEx site.

Resolved and Open Issues

Follow the link below to find up-to-date information about the resolved issues in this release:

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283688292&rls=15.0&sb=anfr&srtBy=byRel&bt=custV

You need to refresh your browser after you log in to the Cisco Bug Search Tool.

Limitations

Feature	Limitation
Time zone support	■ The Cisco TMS server time zone cannot be changed. ■ International time zone amendments such as changes to DST dates or time zone regions are automatically updated on the Cisco TMS server and in Cisco TMS through Microsoft Windows Updates. The same is not true of endpoints running Cisco TelePresence TE or TC software—they have a manual pre-defined list of time zones, so any changes to DST dates or time zone regions will not be reflected. This can lead to time zone mismatch errors on direct-managed endpoints. Scheduling will not be affected, but Cisco TMS could fail to read/write time zone data.
TelePresence Conductor scheduling	TelePresence Conductor waits 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: CSCuf34880. This limitation will be addressed in coming releases of TelePresence Conductor and Cisco TMS. See also scheduling improvements [p.1]
TelePresence Conductor scheduling	Multiple TelePresence Conductor cluster nodes are not supported in Cisco TMS.
TelePresence Conductor scheduling	Scheduling Cisco TMSPE-generated Collaboration Meeting Rooms is not supported.
TSP Audio and meeting extension	If two meetings are allocated the same TSP audio number by WebEx, Cisco TMS has no awareness of this when deciding whether to extend the meeting. This could lead to two conferences containing the same audio participants.

Feature	Limitation
Monitoring and reporting	▪ Conferences using FindMe and Multiway may cause duplicates in Conference Control Center and Reporting. ▪ Conferences where participants have been put on hold or have been transferred may cause duplicates in Conference Control Center and Reporting. ▪ Conference Control Center and Graphical Monitor will not work in Google Chrome version 42 and above as it no longer supports Netscape Plugin Application Programming Interface (NPAPI). Until the support for Netscape Plugin Application Programming Interface (NPAPI) is completely removed in a future release, you may try the following steps to open Conference Control Center and Graphical Monitor in Google Chrome: a. In your system open Command Prompt as an Administrator. b. Run **reg add HKLM\software\policies\google\chrome\EnabledPlugins /v 1 /t REG_SZ /d java** command. c. Restart Google Chrome. ▪ The auto refresh functionality for Participants snapshot and Event Log data in Conference Control Center does not work in any version of Google Chrome.
WebEx	▪ Advanced recurrence patterns are not supported for CMR Hybrid. When booking from the New Conference page, include WebEx before specifying the recurrence pattern to display only supported recurrence patterns. ▪ Deleting a recurrent meeting series while one instance is ongoing will delete the meeting in Cisco TMS but not in WebEx. This is because WebEx does not allow changes to ongoing meetings, this includes deletion. ▪ Selecting *Medium-High* or *High* option for **Communication Security** in Cisco TMS Tools, will lose some or all functionalities in Cisco TMS.
Collaboration Edge	Cisco TMS does not currently support devices that are behind Collaboration Edge.
Expressway	Cisco Expressway-C and Cisco Expressway-E will display in Cisco TMS with system type TANDBERG VCS.
System Type field	Some systems that previously contained TANDBERG in the system type may still show up as TANDBERG in Cisco TMS. This is primarily based on Cisco TMS reading the system type directly from the system's API. In some cases, Cisco TMS added the system type where one was not available through the API. Therefore, the name may continue to show up with TANDBERG in the system type.
Bottom Banners	When Bottom banner is enabled in Cisco TMS Tool, using Cisco TMS Web application in Internet Explorer 10 with enhanced security configuration enabled, disables the links and buttons at bottom of the window.
Cisco TMSPE fails to communicate with Cisco TMS	Cisco TMSPE fails to communicate with Cisco TMS when the new security mode is set to *High* in Cisco TMS 15.0. This limitation will be addressed in forthcoming releases of Cisco TMSPE.
Scheduling meetings in Cisco TMS	In some cases, Cisco TMS does not allow to book a recurrence meeting, if it overlaps with a meeting that is scheduled for 24 hours or more. Bug toolkit identifier: CSCux64873.

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.

Upgrading to 15.0

Before You Upgrade

Redundant Deployments

Customers using a redundant Cisco TMS deployment must read the upgrade instructions in Cisco TelePresence Management Suite Installation and Upgrade Guide 15.0 before upgrading to Cisco TMS15.0.

Upgrading from 14.4 or 14.4.1

Customers upgrading from 14.4 or 14.4.1 that use Cisco TMSXE or Cisco TMSXN must follow the upgrade procedure described in Cisco TelePresence Management Suite Installation and Upgrade Guide 15.0 when upgrading to Cisco TMS15.0.

Upgrading From a Version Earlier than 14.2

Customers upgrading from a version of Cisco TMS earlier than 14.2 must read the upgrade instructions in Cisco TelePresence Management Suite Installation and Upgrade Guide 15.0 before upgrading to Cisco TMS15.0.

Prerequisites and Software Dependencies

See *Cisco TelePresence Management Suite Installation and Upgrade Guide* for the full list of compatible operating systems and database servers.

Upgrade Instructions

Cisco TMS uses the same installation program for both new installations of Cisco TMS and upgrades of previous Cisco TMS versions.

See *Cisco TelePresence Management Suite Installation and Upgrade Guide* for complete instructions for upgrade or installation.

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

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 at: www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Document Revision History

Table 1 Cisco TMS release notes revisions

Date	Revision	Description
August 2016	03	Added scheduling meetings in Cisco TMS limitation.
March 2016	02	Updated 'Removed Export Report to PDF Feature' section
July 2015	01	Release of Cisco TMS 15.0

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

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)