



Cisco TelePresence Management Suite 15.6

Software Release Notes

First Published: September 2020

Preface

Change History

Table 1 Software Release Notes Change History

Date	Change	Reason
February 2018	Updates	Cisco TMS 15.6

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 15.6

SQL Native Client 11 requirement

If Cisco TMS has an externally hosted SQL Server, then SQL Native client 11 must be installed on Cisco TMS server before installation of Cisco TMS.

Default Selection in External Tab of Add Participants Pop-Up Window

When external participants are added to the conference, the default protocol that is listed depends on the protocol that is chosen as **Preferred Protocol in Routing** in the **Conference Settings** page.

Support for Non Default Port of Cisco VCS

If Cisco VCS is configured to listen on a specific port other than the default port, then port number is mandatory to add Cisco VCS in Cisco TMS. The default port is 443. Cisco VCS can be added as **IP:PORT** in Cisco TMS.

Cisco Spark Room 55

Cisco TMS now supports Cisco Spark Room 55 endpoints on CE 9.1.3 software.

Support for handling Load Balancing on Cisco Meeting Server

Cisco TMS sets `activeWhenEmpty` parameter to **false** for enabling the load balancing of new calls on a Cisco Meeting Server conference created by Cisco TMS.

For more information, refer to [Cisco Meeting Server Release Notes 2.2](#).

Note: This feature is available only for Cisco Meeting Server 2.2 and above.

Support for Meeting Owner in Cisco Meeting Server Scheduled Meeting

Cisco TMS sets the name of the Cisco TMS user who schedules the meeting (or who the meeting is scheduled on behalf of) to the **meetingScheduler** field in Cisco Meeting Server co-space when a meeting is allocated. If this user is

part of the Cisco Meeting Server users list, then the user is set as the owner for the co-space for the scheduled duration. It is updated only when the meeting is allocated on the co-space and is active only for the meeting duration.

Note: This feature is available only for Cisco Meeting Server 2.2 and above.

Support for SuperCOP files

Cisco TMS now supports using SuperCOP files for upgrading all endpoints that support CE 9.x software.

Note: Endpoint upgrade using **.loads** extension file is supported only if the **Upgrade Mode** is **'Expert'**. The **.loads** file uploaded via SuperCOP files have the **Target** and **Version** fields which are displayed as **Unknown**.

Support for handling Participant/s name change

When a participant/s name is changed in CUCM or in Cisco TMS for a future meeting, then Cisco TMS updates the changed name of the participant of the future meeting in the **Export Detailed Log** of Cisco TMS.

Notes:

- For CUCM managed participant/s, it may take maximum upto one minute for the updated device name to be reflected in **Export Detailed Log**.
- For TMS managed participant/s, it may take maximum upto four hours for the updated device name to be reflected in **Export Detailed Log**.

Support for Microsoft Windows Server 2016, SQL Server 2016, ESXi 6.5 and .Net 4.6

Cisco TMS now supports the following:

- Microsoft Windows Server 2016 64 bit
- Microsoft SQL Server 2016 64 bit
- ESXi 6.5
Note: Cisco TMS has been qualified with VMware File system 5, as VMware File system 6 has a known issue with ESXi 6.5. You have to continue with File System 5, until the issue is fixed.
- .Net 4.6 is supported and Cisco TMS is not qualified on .Net 4.7. For more information, see [.Net 4.7 compatibility issue with Cisco TMS](#) in [Limitations](#) section.

Removed Support

Support has been removed for:

- Microsoft Windows Server 2008 R2
- Microsoft SQL Server 2008 R2 (Since Cisco TMSAE supports Microsoft SQL Server 2008 R2 and earlier version, Cisco TMSAE is not supported on Cisco TMS 15.6.)

Improved AXL and RIS Interoperability with CUCM

Cisco TMS uses **JSessionID** in CUCM AXL and RIS API request to align with the CUCM best practices guidelines. **JSessionID** allows CUCM clients to use a single session for making multiple AXL and RIS requests.

Customization of SQL connection string

Cisco TMS introduces a new option **Enable the use of 'MultiSubnetFailover' for SQL Connection** that allows you to handle SQL Server failover conditions. The feature can be configured from **Cisco TMS Tools>Configuration>Cisco TMS Database Connection**

During Microsoft SQL Server failover, Cisco TMS attempts to connect to **Microsoft SQL Server Failover Cluster** or **High Availability Group Listener**. If **Enable the use of 'MultiSubnetFailover' for SQL Connection** option is selected, MultiSubnetFailover allows faster failover and significantly reduce the failover time.

Note: If **Enable the use of 'MultiSubnetFailover' for SQL Connection** option is selected for a SQL connection other than **High Availability Group Listener** or **Microsoft SQL Server Failover Cluster**, it may result in a negative performance impact and is not supported.

Features in Previous Releases

For information about new features in previous releases refer to the following links:

[Cisco TMS 15.5](#)

[Cisco TMS 15.4](#)

[Cisco TMS 15.3](#)

[Cisco TMS15.2.1](#)

[Cisco TMS 15.1](#)

[Cisco TMS 15.0](#)

[Cisco TMS 14.6.2](#)

[Cisco TMS 14.6.1](#)

[Cisco TMS 14.6](#)

Resolved and Open Issues

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

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283688292&rls=15.6&sb=anfr&bt=cust
V

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

Limitations

Feature	Limitation
Time zone support	<ul style="list-style-type: none"> ■ 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.

Feature	Limitation
TelePresence Conductor scheduling	<ul style="list-style-type: none"><li data-bbox="565 310 1430 478">■ 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<li data-bbox="565 487 1430 541">■ Multiple TelePresence Conductor cluster nodes can be added in Cisco TMS but only primary TelePresence Conductor can be used for scheduling.<li data-bbox="565 550 1430 611">■ 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	<ul style="list-style-type: none"> ■ 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 does not work in Google Chrome version 42 and above, Firefox 52 and above, Opera and Microsoft Edge. Until the support for Netscape Plugin Application Programming Interface (NPAPI) is completely removed in a future release for Google Chrome and Firefox, you may try the following options to open Conference Control Center and Graphical Monitor: <ul style="list-style-type: none"> - Use Internet Explorer, version 10 or 11. - Re-enable NPAPI Plugin Support in Firefox 52 (32-bit) only, by overriding Firefox default settings: <ol style="list-style-type: none"> a. To enable NPAPI plugins in Firefox 52 (32-bit) only, use the <code>about:config</code> setting. Add new Boolean string <code>plugin.load_flash_only</code> and set it to <code>false</code>. b. Restart the browser. - Download and use Firefox 52 (32-bit) ESR (Extended Support Release) only, where NPAPI plugins will continue to work till March 2018. Note: If Firefox 52 (32-bit) ESR (Extended Support Release) is installed, then ensure that no other stand-alone Firefox software versions are installed. - Use IE Tab extension in Google Chrome: <ol style="list-style-type: none"> a. Run Internet Explorer (IE) inside Chrome (https://www.ietab.net/). b. When the IE Tab extension is installed in Google Chrome, you can click the IE icon that appears next to the address bar in 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. ■ The meeting details appear gradually in Conference Control Center when Communication Security is set to <i>High</i> under TMS Tools > Security Settings > Transport Layer Security Options. ■ We recommend to perform one of the following to improve the performance: <ul style="list-style-type: none"> - Select <i>Medium</i> or <i>Medium-High</i> security mode for Communication Security in TMS Tools > Security Settings > Transport Layer Security Options. - Use less number of users in Conference Control Center when the Communication Security is set to <i>High</i>.

Feature	Limitation
WebEx	<ul style="list-style-type: none"> ■ 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 <i>Medium-High</i> or <i>High</i> option for Communication Security in Cisco TMS Tools, will lose some or all functionalities in Cisco TMS. ■ If the meeting is booked with WebEx, when you later change the conference owner in Cisco TMS, the conference owner details will only reflect in Cisco TMS and not in WebEx. Further, when you try to update the meeting in Cisco TMS, it may result in an error.
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	<p>Cisco TMSPE fails to communicate with Cisco TMS when the security mode is set to <i>High</i> in Cisco TMS 15.6.</p> <p>This limitation will be addressed in forthcoming releases of Cisco TMSPE.</p>
TelePresence Conductor Clustering	<ul style="list-style-type: none"> ■ There will be no failover support for aliases if the primary TelePresence Conductor is down. If the administrator has changed some aliases in the peer TelePresence Conductor when the primary TelePresence Conductor is down, the peer TelePresence Conductor's aliases cannot be updated in TMS until the primary node is active. ■ In this release only the feedback from the primary TelePresence Conductor will be processed by Cisco TMS. This means that adhoc resolving may have impact, when the primary TelePresence Conductor is down. ■ In this release there is no support for clustered TelePresence Conductor in scheduling, routing and load balancing.
Phone Book on IX Endpoint	<p>Cisco TMS is unable to detect the software version when you add an IX endpoint.</p> <p>The Phone Book tab for IX endpoint under Systems > Navigator is configurable only for version 8.2. IX endpoint cannot fetch phone book data from Cisco TMS when you add any older version below 8.2.</p> <p>You must add an IX version 8.2 to configure phone book and then use it from the endpoint.</p>

Feature	Limitation
Virtual machine loses network connectivity intermittently for the following product versions: <ul style="list-style-type: none"> ■ VMware ESXi 5.0.x ■ VMware ESXi 5.1.x ■ VMware ESXi 5.5.x ■ VMware ESXi 6.0.x 	Windows 2012 virtual machines that use E1000/E1000e driver, experience loss of network connectivity. This issue would occur in the following environments: <ul style="list-style-type: none"> ■ The virtual machine is Windows 2012 or Windows 2012 R2. ■ The virtual machine is using E1000 or E1000E driver. A work around for this issue is to use VMXNET3 instead of E1000 or E1000e driver. For more information see the following article: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2109922
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.
Cisco Meeting Server status	Cisco TMS does not display <i>No Response from Main System</i> log in Conference Event Log when a Cisco Meeting Server goes down during an ongoing conference.
Ignore Scheduled Meeting and Continue Active Call	This feature works only when a bridge is dialing to an endpoint.
Adding systems	<ul style="list-style-type: none"> ■ Via IPv4 and IPv6: Cisco TMS adds a system via IPv4 and the same system can also be added via IPv6 and vice versa. ■ Via hostname and IPv6: When you add a Cisco Meeting Server to Cisco TMS using hostname, then same Cisco Meeting Server can also be added to Cisco TMS using IPv6 with different System ID.
Cisco Meeting Server 2.1	To prevent overlapping redial behavior, you must set the value in Conference Settings > Connection Timeouts to minimum 45 seconds.
Cisco Meeting Server	There will not be any information about external dial-ins in the conference event log.
Private meeting	Private meeting feature depends upon the privacy mode for the particular endpoint. Note: Known endpoints like CTS have the privacy setting set as not to display the meeting title in the upcoming meeting list.
Support for non default port of Cisco VCS	When a Cisco VCS is added using non default port in Cisco TMS, SNMP discovery is not possible. This is a known design limitation and the SNMP community name has to be added manually in the System Navigator to clear the SNMP ticket.
.Net 4.7 compatibility issue with Cisco TMS	Cisco TMS runs successfully on Microsoft .Net Framework 4.6. However, during regular windows update, Microsoft .Net Framework 4.7 is installed. Cisco TMS is not compatible with .Net Framework 4.7 and hence this specific update has to be removed. For more information, refer to https://blogs.msdn.microsoft.com/dotnet/2017/06/13/microsoft-net-framework-4-7-is-available-on-windows-update-wsus-and-mu-catalog/ . After the update is removed, restart the server. Cisco TMS will run without any issue. Note: When .Net Framework 4.7 is installed and if you try to install Cisco TMS, then the error message ".NET Framework 4.5 is not installed" is displayed.

Feature	Limitation
Resource Availability Check on Extension	If ' Resource Availability Check on Extension ' is set to ' Ignore ' with ' Extend Conference Mode ' set to ' Automatic Best Effort ', and ' Allow participants to Join Early ' is set to Yes , unexpected results could occur when one participant of the meeting is in a back-to-back point-to-point meeting.

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 15.6

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 15.6](#) before upgrading to Cisco TMS 15.6.

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 15.6](#) when upgrading to Cisco TMS 15.6.

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 15.6](#) before upgrading to Cisco TMS 15.6.

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.

Note: Before upgrading to Cisco TMS 15.6, ensure that the Windows Updates are up to date.

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.



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.

© 2017 Cisco Systems, Inc. All rights reserved.

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)