Cisco TelePresence Management Suite 15.13.8

Software Release Notes

First Published: July 2026

Contents

Preface

Change History

Table 1 Software Release Notes Change History

Date	Change	Reason
July 2026	Release of Software	Cisco TMS 15.13.8

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 15.13.8

Security Hardening

This release focuses exclusively on security hardening. For more information refer Bug Search Tool

Features in Previous Releases

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

Cisco TMS 15.13.7

Cisco TMS 15.13.6

Cisco TMS 15.13.5

Cisco TMS 15.13.4

Cisco TMS 15.13.3

Cisco TMS 15.13.2

Cisco TMS 15.13.1

Cisco TMS 15.13

Cisco TMS 15.12

Cisco TMS 15.11

Cisco TMS 15.10

Cisco TMS 15.9

Cisco TMS 15.8

Cisco TMS 15.7

Cisco TMS 15.6.1

Cisco TMS 15.6

Resolved Issues

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

https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&rls=15.13*&prdNam=Cisco%20TelePresence%20Management%20Server

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

Open Issues

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

https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&rls=15.13*&prdNam=Cisco%20TelePresence%20Management%20Server

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.

Feature	Limitation
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. ▪ Multiple TelePresence Conductor cluster nodes can be added in Cisco TMS but only primary TelePresence Conductor can be used for scheduling. ▪ Scheduling Cisco TMSPE-generated Collaboration Meeting Rooms is not supported. **Note**: Telepresence Conductor has already been end of life (Feb 6, 2019) and will have no future releases. For more information, refer to https://www.cisco.com/c/en/us/products/collateral/conferencing/telepresence-conductor/eos-eol-notice-c51-739456.html
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** 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**: – Use Internet Explorer, version 10 or 11. – Re-enable NPAPI Plugin Support in Firefox 52 (32-bit) only, by overriding Firefox default settings: a. To enable NPAPI plugins in Firefox 52 (32-bit) only, use the `about:config` setting. Add new Boolean string `plugin.load_flash_only` and set it to `false`. 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: 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 *High* under **TMS Tools > Security Settings > Transport Layer Security Options**. ▪ We recommend to perform one of the following to improve the performance: – Select *Medium* or *Medium-High* 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 *High*.

Feature	Limitation
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. ▪ 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	Cisco TMSPE fails to communicate with Cisco TMS when the security mode is set to *High* in Cisco TMS 15.6 and later versions. This limitation will be addressed in forthcoming releases of Cisco TMSPE.
TelePresence Conductor Clustering	▪ 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 Conductoris down. ▪ In this release there is no support for clustered TelePresence Conductor in scheduling, routing and load balancing.
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 *No Response from Main System* log in **Conference Event Log** when 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.

Feature	Limitation
Adding systems	▪ 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 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	▪ There will not be any information about external dial-ins in the conference event log. ▪ In Cisco Meeting Server 2.1, to prevent overlapping redial behavior you must set the value in **Conference Settings > Connection Timeouts** to minimum 45 seconds.
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.
Cisco TMS LiveService does not correctly co-relate a participant to a specific coSpace	This issue occurs, as there are no polling or feedback mechanism available for Cisco Meeting Server integration with Cisco TMS. Cisco TMS is unable to correctly identify participants if they are external(not managed by Cisco TMS) and part of coSpaces. In such use cases, use TelePresence Server/MCU bridges.
Booking Invite email contains non multisite video address	When you schedule a conference using combination of multisite and non multisite endpoints and no bridge is involved, with the direction as dial out. Then, the booking invite email contains all participants URI for both multisite and non multisite.
SuperCOP File	SuperCOP files with size more than 2 GB are not supported. If the SuperCOP file is more than 2 GB, then you must use individual COP file for each endpoint.
Early Join Caveat	During 'Early Join Time', if a TMS managed endpoint participant is removed from a scheduled conference, then at conference launch time LiveService will disconnect that endpoint's existing active call.
Event log shows call disconnected for CUCM dial in endpoints, even if the call is in connected state in Cisco Meeting Server deployment.	For this to work, proper configuration has to be done in CUCM route patterns to ensure that the URI in Cisco TMS and the one at the connection time in endpoint should be the same. Cisco TMSwill mark the meeting as Connected or Disconnected based on the feedback logs from Endpoint.
Participant Template	When a participant template is created using Cisco Meeting Server, the '**Reusable**' option will not work for Dialouts.
Phonebook	Cisco TMS does not support 'File Based Phone Book' source in High/Medium-High mode.
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.

Feature	Limitation
Cisco IX5000	From Cisco TMS version15.10, SSH mode of communication will no longer be supported with Cisco IX5000.
Skype Dual Home Domain	When Skype Dual Home Domain is changed from Cisco TMSXE to Cisco TMS or it is changed for Cisco Meeting Server within Cisco TMS, then the newly configured Skype Dual Home Domain is effective only for future meeting bookings.
Default IP Bandwidth Configuration	It is recommended to set Cisco TMS Default IPBandwidth to 6144kbps or less while using ISDN participants in scheduled conference created by Cisco TMS Booking API.The Default IP Bandwidth can be configured in **Administrative Tools** > **Configuration** > **Conference Settings** > **Default IP Bandwidth**.

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 15.13.8

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 before upgrading to Cisco TMS 15.13.8.

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 when upgrading to Cisco TMS 15.13.8.

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 before upgrading to Cisco TMS 15.13.8.

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 15.13.8, 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.

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. (1721R)