Cisco TelePresence Management Suite 15.2.1

Software Release Notes
September 2020

Preface

Change History

Table 1 Software Release Notes Change History

Date	Change	Reason
May 2016	Cisco TMS Support for Two-Node Conductor Clusters feature is no longer in preview status.	Cisco TMS15.2.1
April 2016	Addition of new features.	Cisco TMS 15.2.1

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 15.2.1

ESXi 6.0 Support

Cisco TMS now supports ESXi 6.0. It also works with the previous version 5.5.

Cisco TMS Support for Two-Node Conductor Clusters

TelePresence Conductor cluster support has been added to Cisco TMS.

You can configure Cisco TMS to automatically transfer to the subordinate Conductor if the primary Conductor node fails. Cisco TMS monitors the status of the primary node through a mix of polling and feedback requests. Failover happens only while the primary node is down, and Cisco TMS reroutes to the primary Conductor when it is available again.

Cisco TMS support for two-node Conductor clusters allows TMS to continue to manage scheduled meetings after a Conductor node failure, without requiring manual intervention on the TMS.

The following elements have been added to Cisco TMS user interface:

- In **Systems > Navigator**, the **Clustering** tab has been added for each clustered TelePresence Conductor to view the status of primary and peer TelePresence Conductors.
- A new Conductorfailover-liveservice log is introduced and enabled by default. It records all occurrences of failover transfers between TelePresence Conductor nodes.

You can still add a primary TelePresence Conductor that is down for maintenance and marked in red.

For future compatibility we recommend that TelePresence Conductor clusters are configured with no more than two nodes. If you currently deploy three-node clusters, you should consider removing a node. Cisco may discontinue the ability to add a third node to a cluster in a future software release.

While the primary node is down you can continue to schedule meetings as normal, without any manual intervention on the TMS. Some Conference Control Center functions are also available. If the primary node is still down at the scheduled start time, TMS switches the meeting to the subordinate node. Note that TMS does not display the subordinate node as an available bridge for booking. Conductor cluster behavior remains unchanged - calls may drop and have to dial back into their meetings, and some services may be temporarily unavailable during the cluster's recovery from a node failure. Cisco TMSPE and its associated functions do not failover. Three-node Conductor clusters are not supported for this feature.

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=15.2.1&sb=anfr&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.
TelePresence Conductor scheduling	Multiple TelePresence Conductor cluster nodes can be added in Cisco TMS but only primary TelePresence Conductor can be used for scheduling.
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. ■ 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*.
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.

Feature	Limitation
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 15.2.1. 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 Conductor is down. ■ In this release there is no support for clustered TelePresence Conductor in scheduling, routing and load balancing.
Virtual machine loses network connectivity intermittently for the following product versions: ■ 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: ■ 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.
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 15.2.1

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 TMS15.2.1.

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 TMS15.2.1.

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 TMS15.2.1.

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.

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)