Cisco TelePresence Management Suite 15.3

Software Release Notes

First Published: June 2017

Preface

Change History

Table 1 Software Release Notes Change History

Date	Change	Reason
June 2017	Updates	Cisco TMS 15.3

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 15.3

Support for Cisco Meeting Server (CMS) as a Managed Bridge

Cisco Meeting Server can now be added in Cisco TMS as a managed bridge to schedule a conference. The key benefits of using CMS for scheduling are as follows:

- Unprecedented capacity to manage a huge number of calls on a Clustered Call Bridge.
- Automatic failover with no single point of failure for meetings that are about to begin, when an alternate IP is configured.

You can add CMS from **Systems > Navigator > Add Systems** and after it is successfully added, the CMS can be viewed in **Systems > Navigator**. A CMS can also be added with the IPv6 address when IPv6 is configured for the CMS. Enter the address in `[IPv6 address]:port number` format to add the CMS. Note that the port number is mandatory for IPv6.

To add a CMS, it is mandatory to enter a valid **Username** and **Password**. You can configure and manage multiple CMS bridges in Cisco TMS.

Cisco TMS supports CMS version 2.0 and above. CMS can only be tracked by *IP Address* or *Hostname*.

Configuration

CMS **System Status** can be viewed under **Systems > Navigator >** Select a CMS **> Summary**.

TMS triggers tickets in the CMS **Summary** page if the following options are not configured:

- When a CMS is added for the first time, the system name is displayed as *No Name*. Enter a system name in the **Name** field under **Systems > Navigator >** Select a CMS **> Settings > General**.
- When **Domain**, **Numeric ID Base** and **Numeric ID Quantity** fields are blank. Enter the details under **Settings > Extended Settings** and save.
- When the pre-configured alternate IP is no longer part of the clustered call bridge. Select an alternate IP in the **Settings > Edit Settings > Network Settings > Alternate IP** drop down list, then enter the username and password to complete the configuration.

Dial Numbers

Perform the following steps to configure your Dial Numbers:

1. Navigate to **Systems > Navigator >** Select a CMS**> Settings > Extended Settings**.
2. Enter appropriate details in **Domain**, **Numeric ID Base** and **Numeric ID Quantity** fields.
3. Click **Save**.

We recommend not to change the Dial Number settings frequently and only do so if necessary. Do the following before you make any changes in dial number configuration when it is required:

- Make the changes during a maintenance window only.
- If future conferences are scheduled, run the **Diagnostics Tool** after making the changes.
- Be aware that the **Save** button is disabled during an ongoing conference.

Web Bridge URI

WebBridge URI configuration is done under **Systems > Navigator >** Select a CMS**> Settings**.

Web Bridge URI will be included in the conference booking confirmation email and in the **Meeting Landing Page**. This option allows a user to click and join a meeting instantly. **Web Bridge URI** in Cisco TMS should only be configured when the **Web Bridge** is configured in CMS. You must enter the same URI that is configured on CMS for **Web Bridge**. Specify a port along with the URI, if the port is not set to the default port 443.

Failover

CMS failover support has also been added in this release. You can now configure an **Alternate IP** in TMS. Select an alternate IP address from the **Alternate IP** drop down list, then enter the username and password to configure failover support. The alternate IP addresses are fetched from the CMS that is configured with clustered call bridges.

Note that CMS failover support on Cisco TMS, is intended to handle the conferences that are about to begin. The failover functionality does not work for an **ongoing** conference. Only one **Alternate IP** configuration is supported by Cisco TMS. If both the master node and alternate IP are down, Cisco TMS does not use other clustered call bridges that are part of the master CMS.

- Only one CMS cluster call bridge node has to be managed by TMS. If an existing TMS-managed CMS needs to be clustered. First remove the nodes from TMS. Then configure the cluster call bridges in CMS and add one of the nodes as a managed node in TMS.
- To uncluster an existing Cisco TMS managed CMS, first remove the managed CMS node from Cisco TMS, then uncluster the call bridges in CMS. Execute **database cluster remove** and **factory-reset app** on CMS console to ensure that the node is completely unclustered.
- During failover, the conference event logs show the primary CMS instead of alternate CMS. The details about the current failover can be seen in the `log-cmsfailover-liveservice` log and by default the level is INFO.

CMS Coexistence

Cisco TMS introduces the coexistence feature to use CMS as the preferred bridge for a set of users. This feature is used to migrate a group of users into CMS. It overrides all the global preferences and is controlled by the *EnableCMSTrial* registry.

A message *"CMS Trial Mode is enabled. Refer to TMS Release Notes for more information."* is displayed in **Administrative Tools > Configuration > Conference Settings > Advanced > Preferred MCU Type in Routing**, when CMSTrial registry is enabled.

To create a coexistence, first assign an IP Zone to the users and then assign the same IP Zone to a CMS. All the meetings will be scheduled on CMS, when an user from that IP Zone books a meeting.

The *EnableCMSTrial* registry key is disabled by default . To enable this feature, change the *EnableCMSTrial* registry key value to *one*.

CMS Profiles

Cisco TMS checks the callProfile and callLegProfile that are created by Cisco TMS on CMS, in every 24 hours. If the profiles are deleted, Cisco TMS recreates the profiles and reassociates them with the cospaces that are created by Cisco TMS. Administrators can perform a **Force Refresh** in the **View Settings** page to initiate the process manually without waiting for 24 hours. System-level profiles are used for the period that the TMS-created profiles are deleted.

Unsupported Features

The following features are not supported for CMS in Cisco TMS:

- WebEx enabled conferences
- **Conference Control Center**
  You can however view CMS in the **Edit Conference** and **Add Participants** section for the conferences that are scheduled on other bridges.
- **ISDN Bandwidth** and **ISDN Restrict**
- Best Impression Routing
- Least Cost Routing
- Recording with TCS

The **Feedback Log** and **Call Log** tabs under **Systems > Navigator >** Select a CMS**> Log** have been removed for CMS.

The **Enforce Management Settings** has also been removed from **Systems > Navigator >** Select a CMS**>Settings > Edit Settings**

Scheduling

After you upgrade to TMS 15.3, prescheduled meetings still behave in the same way the original booked meetings.Cisco TMS does not force the meetings to run on CMS.

You can now select CMS as **Preferred MCU Type in Routing** from **Administrative Tools > Configuration > Conference Settings > Advanced**.

When you add CMS as a participant and schedule a conference, the **IP Bandwidth** field in **Booking > New Conference > Advanced Settings** is disabled. The highest bandwidth value 6144 kbps is selected. CMS does not have any bandwidth restriction to host a conference.

The following options can only be selected under **Booking > New Conference > Advanced Settings**, when you add CMS and book a new conference:

- *Continuous Presence* in **Picture Mode**.
- *Automatic Best Effort* in **Extend Mode**.
- *If Possible* in **Secure**.

When you add CMS as the main bridge and schedule a conference, the option to mute audio and video is disabled for all the participants.

The conference and participants templates support for CMS is in-line with TelePresence Conductor.

Notes

- After you upgrade to TMS 15.3, pre-scheduled meetings still behave in the same way the original booked meetings. Cisco TMS does not force the meetings to run on CMS.
- If the master database of CMS cluster goes down just before scheduled time, then the scheduled conference might not be successfully initiated in CMS.

Support for Phone Book on IX Endpoints

Support for phone book on IX endpoints has been added in Cisco TMSfor IX version 8. 2. Phonebook support for IX is only in Medium security mode.

The **Phone Book** tab under **Systems > Navigator > Select an IX endpoint** has been enabled for IX endpoints. In addition, you can select an IX endpoint under **Phone Books > Manage Phone Books >** select a Phone Book **> Set On System**.

Support for DX Endpoints

Cisco TMS now supports CE 8.2 software on DX 70 and DX 80 endpoints.

Support for SQL 2014

Cisco TMS now supports SQL 2014.

Support for .NET 4.6

Cisco TMS now supports .NET version 4.6.

Behavior Change in TLS Communication Security

The following communication security modes have been enhanced for all Cisco TMS connections:

- *Medium:* Cisco TMS prefers HTTPS or TLS 1.0, TLS 1.1 and TLS 1.2.
- *Medium-High:* Cisco TMS will communicate using SSL for connections. SSL includes HTTPS and SSH. It also supports TLS 1.2 and TLS 1.1.
- *High:* Cisco TMS will communicate only using SSL for connections and will check that valid and signed certificates are present during communication. It also supports only TLS 1.2 with proper Certificate validation.

Note that the immersive CTS and TX endpoints require *Medium* security mode to work in Cisco TMS.

Russian Time Zone Awareness

Novosibirsk Oblast time zone is moved from *North Central Asia Standard Time UTC+06:00* to *North Asia Standard Time (UTC+07:00)*, hence *North Central Asia Standard Time (UTC+06:00)* is now represented as **Almaty**.

Cisco TMS has been updated with the following changes:

- *(UTC+06:00) Novosibirsk* time zone has been renamed to *(UTC+06:00) Almaty*.
- *(UTC+06:00) Novosibirsk* time zone users should now select *(UTC+07:00) Krasnoyarsk*.

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=15.3&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.

Feature	Limitation
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 15.3. 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.
Phone Book on IX Endpoint	Cisco TMS is unable to detect the software version when you add an IX endpoint. 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. You must add an IX version 8.2 to configure phone book and then use it from the endpoint.
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.
CMS Meeting End notification	Cisco TMS does not push meeting end notifications to CMS as CMS does not support it. However, TMS managed endpoints will continue to receive notifications from TMS for CMS hosted conferences.

Feature	Limitation
CMS status	Cisco TMS does not display *No Response from Main System* log in **Conference Event Log** when a CMS goes down during an ongoing conference.
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 a CMS to Cisco TMS using hostname, then same CMS can also be added to Cisco TMS using IPv6 with different System ID.

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 15.3

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 TMS15.3.

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 TMS15.3.

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 TMS15.3.

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.

© 2016 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)