Cisco TelePresence Management Suite Provisioning Extension 1.7

Software Release Notes

Last Updated: October 2017

Version 1.7

Preface

Change History

Table 1 Software Release Notes Change History

Date	Change	Reason
October 2017	Updated required Cisco TMS version	Cisco TMSPE 1.7
May 2016	Updated Java 8 support information	Cisco TMSPE 1.7
April 2016	Addition of a new feature	Cisco TMSPE 1.7

Introduction

This document describes the main features of Cisco TelePresence Management Suite Provisioning Extension version 1.7, and changes from previous versions.

Product Documentation

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

- *Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS Deployment Guide*
- *Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified Communications Manager Deployment Guide*
- *Cisco TelePresence FindMe User Guide*

New in 1.7

Notice of Deprecation – Active Meeting Manager preview feature

The Active Meeting Manager (AMM) preview feature needs WebSockets technology. As popular browsers do not support WebSockets, Cisco has decided to deprecate the Active Meeting Manager feature set in an upcoming release. Customers are therefore advised not to deploy this feature.

ESXi 6.0 Support

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

Java 8 Requirement

It is mandatory to have Java 8 or higher to install or upgrade Cisco TMSPE 1.7.

To enable 4096-bit encryption on Cisco TMSPE, the following procedure must be followed for the Java software on Cisco TMSPE:

Edit **<jre-path>\lib\security\java.security** and insert an entry for bouncy castle as below (shown in **bold**). The other entries are incremented by 1, so the contents should be:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.3=sun.security.rsa.SunRsaSign
```

```
security.provider.4=sun.security.ec.SunEC
security.provider.5=com.sun.net.ssl.internal.ssl.Provider
security.provider.6=com.sun.crypto.provider.SunJCE
security.provider.7=sun.security.jgss.SunProvider
security.provider.8=com.sun.security.sasl.Provider
security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.10=sun.security.smartcardio.SunPCSC
security.provider.11=sun.security.mscapi.SunMSCAPI
```

Note: If you do not make the above change, TMSPE cannot access Conductor and users will not be able to edit their Personal Collaboration Meeting Rooms (CMRs). In addition, the following error is displayed in the TMSPE logs: *VMR::ConductorConnector - TelePresence Conductor failure with: Could not generate DH keypair*.

Resolved and Open Issues

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

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613664&rls=TMSPE1.7&sb=anfr&bt=custV

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

Limitations

Feature	Limitation
Java support	Upgrading Java during operation of this product is not supported. **Caution:** Do not upgrade Java while Cisco TMSPE is running. Disable the Windows service prior to any upgrade. We strongly recommend disabling automatic Java updates on the server.
Smart Scheduler	▪ The site administrator configured for communication with Cisco TMS will receive an e-mail notification every time a meeting is booked or updated in Smart Scheduler. ▪ Modifying single instances of recurrent meetings is currently not possible in Smart Scheduler. Series with exceptions created in Cisco TMS or other booking interfaces may not be modified using Smart Scheduler. ▪ Modifying a previously booked meeting series with a computer set to a different time zone than used for the original booking, will change the recurrence pattern's end date to use the latest time zone.
Named Pipe connection issues using SQL Express	In the MSDE mode using the Named Pipe protocol, connection to the database may fail with the error " The specified network name is no longer available" . The problem is seen on Windows Server 2008, and can be solved with the following hotfixes: Windows Server 2008 R2: http://support.microsoft.com/kb/2194664http://support.microsoft.com/kb/2444328 Note that the default connection protocol is TCP/IP.
Dual network interface not supported	Like Cisco TMS, this extension does not support the use of two network interfaces. (Identifier CSCtx52264)

Feature	Limitation
Language settings	In the Self Service Portal, the **Language** setting for each particular user in **Account Settings** does not influence the language setting in Cisco TMS.
McAfee Antivirus	McAfee Antivirus will occasionally corrupt files required for Cisco TMSPE to run. Disable McAffe Antivirus during install.
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.

Updating to Cisco TMSPE 1.7

Prerequisites and Software Dependencies

Cisco TelePresence Management Suite Provisioning Extension 1.7 requires:

- Cisco TMS 15.2.1.
- Cisco TelePresence Conductor XC4.2 or later version. Also, this version is required for Multiparty Licensing to work.
- Java 8 or higher version.

One or both of the following is also required:

- Cisco VCS X8.5 or later.
- Unified CM 9.1.2 or later.
  Unified CM 10.5.2 is required for ad hoc calls to support the use of PMP licenses.

For installation instructions, full system requirements, and other prerequisites, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* for Cisco VCS or Unified CM.

Migrating from Cisco TMS Agent Legacy

Direct migration to this version of Cisco TMSPE is not supported.

Before upgrading to 1.7, customers running Cisco TMS Agent Legacy must migrate by way of:

- Cisco TMS 13.2.x
- Cisco TMSPE 1.0

Instructions for migration can be found in *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* for Cisco TMSPE 1.0 with Cisco TMS 13.2.5

Upgrading from Previous Versions

High-level Workflow

Cisco TelePresence Management Suite Provisioning Extension relies on and integrates with multiple other products.

When upgrading your deployment:

1. Upgrade Cisco TMS to the required version following the instructions in *Cisco TMS Installation and Upgrade Guide*.

2. Upgrade Cisco TMSPE.
3. Upgrade other systems such as TelePresence Conductor as required.

Upgrading Cisco TMSPE

If the Server is Running Java 6 or 7

To upgrade from Cisco TMSPE 1.1 or 1.0 if the server is still running Java 6 or 7:

1. Uninstall Cisco TMSPE on the server. Do not remove any other files.
2. Install Java 8.
3. Ensure that all critical Windows Updates are installed on your server.
4. Close all open applications and disable virus scanning software.
5. Extract the Cisco TMSPE installer from the zip archive to the Cisco TMSPE server.
6. Run the installer as administrator.
7. Follow the installer instructions

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)