Cisco TelePresence Management Suite Extension for Microsoft Exchange 5.6

Software Release Notes

First Published: September 2017

Software Version 5.6

Preface

Change History

Table 1 Software Release Notes Change History

Date	Change	Reason
September 2017	Release of software	Cisco TMSXE 5.6.

Introduction

Cisco TelePresence Management Suite Extension for Microsoft Exchange integrates Cisco TelePresence Management Suite with Office 365, and Microsoft Exchange 2016, 2013, and 2010, allowing organizers to book video conference resources through their Outlook clients.

If upgrading from a version earlier than 4.0.3, make sure to read for precise instructions on the order of Cisco TMS and Cisco TMSXE upgrades and disabling Cisco TMSXE services.

This document describes bug fixes that were done in Cisco TelePresence Management Suite Extension for Microsoft Exchange version 5.6 and new features were added in the current release.

New in 5.6

Cisco TMSXE supports .NET Framework 4.6

Cisco TMSXE works on .NET Framework 4.6. If .NET Framework is lower than 4.6, you cannot install Cisco TMSXE. In a co-deployment model, Cisco TMS and Cisco TMSXE can be co-located on the same server and .Net Framework 4.6 is supported. Cisco TMSXE is not qualified on .Net Framework 4.7. For more information, see .Net 4.7 compatibility issue with Cisco TMSXE, page 5 in Limitations, page 4 section.

Cisco TMSXE supports TLS 1.2

Cisco TMSXE supports TLS 1.0, 1.1 and 1.2 for communication. It is available in Cisco TMSXE **Configuration tool> Advanced Settings Tab>Transport Layer Security (TLS)**. Cisco TMSXE Admin can select any of the following options:

- By default **Enable the use of TLS 1.0 and TLS 1.1** is selected, Cisco TMSXE communicates with either one of the TLS versions that is 1.0, 1.1 or 1.2.
- When **Enable the use of TLS 1.0 and TLS 1.1** is not selected, Cisco TMSXE communicates only with TLS version 1.2. Also, **Use HTTP** option is disabled in **Cisco TMS** and **Exchange Web Services** tabs.
  Note: If the Admin has already selected **Use HTTP** option in **Cisco TMS** and **Exchange Web Services** tabs and deselects **Enable the use of TLS 1.0 and TLS 1.1** option then **Use HTTP** option will be deselected and disabled.

Support for Microsoft Windows Server 2016 and ESXi 6.5

Cisco TMSXE now supports the following:

- Microsoft Windows Server 2016 64 bit
- ESXi 6.5
  Note: Cisco TMSXE 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.

Removed Support

Support has been removed for Microsoft Windows Server 2008 R2.

Features in Previous Releases

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

Cisco TMSXE 5.5

Cisco TMSXE 5.4

Cisco TMSXE 5.3

Cisco TMSXE5.2

Cisco TMSXE 5.1

Cisco TMSXE 5.0

Cisco TMSXE 4.1

Changes to Interoperability

Ensure that you read the Interoperability, page 5 section of this document, which contains important information about upcoming changes to Exchange version support and support for older versions of the product.

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=5.6&sb=anfr&bt=custV

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

Limitations

Limitation	Description
Large deployments using Office 365	Office 365 limitations on mail quantities may affect booking confirmations and declines to users in very large deployments. For numbers, see Microsoft's documentation: Recipient and sender limits.
Editing a series with an ongoing meeting in Outlook Web App with Office 365	Editing a series while an occurrence is ongoing will cause the ongoing meeting to end if using OWA with Office 365.
Personal calendars not automatically updated	Microsoft Exchange does not allow other applications to access and modify personal calendars. When an existing booking is modified using Cisco TMS, Cisco TMSXE will update the room (resource) calendar, but not the calendars of the organizer and the participants. The organizer must distribute the updated information to the participants.

Extending ongoing meetings can cause participants to be dropped	If extending an ongoing meeting to a time when one or more participants are already scheduled for another meeting, these participants will automatically be rejected from the meeting in Exchange. Cisco TMS subsequently drops the participants from the conference and a decline message is sent to the organizer. This behavior is as expected with mailboxes set not to allow conflicts in Microsoft Exchange, and is not caused by Cisco TMS or Cisco TMSXE. No support for per-resource subject line settings.
No support for per-resource subject line settings	Make sure the following settings are configured identically for all Exchange resources to be added to Cisco TMSXE: ■ **Delete the subject** ■ **Add the organizer's name to the subject** ■ **Remove the private flag on an accepted meeting** See Cisco TelePresence Management Suite Extension for Microsoft Exchange Deployment Guide for information on how to configure these settings.
External Dial String mismatch - Meeting update using forms template	It is not possible to update an Externally hosted dial string in a recurrent or a non-recurrent meeting in Cisco TMS from Microsoft Outlook.
Meetings with external participants can be created either with Scheduling Mailbox feature or Forms Template	As per current design, combining the Scheduling Mailbox feature and Forms Template for a single meeting is not recommended.
Creating a CMR Hybrid meeting by clicking Save in MS Outlook.	When the organizer has created a CMR Hybrid private meeting, Cisco TMS does not treat it as a private conference. If the organizer has only saved the meeting in MS Outlook.
Viewing a private appointment in Exchange 2013 and 2016 Outlook Web Access	When an organizer creates a private appointment with room mailbox in Exchange 2013 and 2016 Outlook Web Access (OWA), the other users who have permission to access the room mailbox can view the original private appointment title and also will be able to open the appointment.
.Net 4.7 compatibility issue with Cisco TMSXE	Cisco TMSXE runs successfully on Microsoft .Net Framework 4.6. However, during regular windows update, Microsoft .Net Framework 4.7 is installed. Cisco TMSXE 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 TMSXE will run without any issue.

.

Interoperability

Ensure that you read this section which contains important information about upcoming changes to Exchange version support and support for older versions of the product.

Upgrade Instructions

For complete upgrade instructions, please see *Cisco TelePresence Management Suite Extension for Microsoft Exchange Deployment Guide (5.6)*.

Prerequisites and Software Dependencies

In order to perform an in-place upgrade, the installed version of Cisco TMSXE must be 3.0 or later. If an earlier version is installed, the administrator must perform a full installation with data migration.

See *Cisco TelePresence Management Suite Extension for Microsoft Exchange Installation Guide (3.0)* for migration instructions.

Upgrading to Cisco TMSXE 5.6

Upgrading when Cisco TMS is version 14.4 or 14.4.1

If upgrading Cisco TMS and Cisco TMSXE and the former is version 14.4 or 14.4.1:

- Disable the Cisco TMSXE service, on both nodes if clustered, before upgrading Cisco TMS.
- Start the service when both Cisco TMS and Cisco TMSXE is upgraded on all servers/nodes.

Upgrading from Versions Earlier than 3.1

- After upgrading Cisco TMSXE from a 3.0.x version, a re-replication of all bookings in Cisco TMS will be performed on startup to clean up discrepancies between Cisco TMS and Exchange resource mailboxes. Depending on the size of your Cisco TMS database and the number of bookings, this process may take a very long time to complete, and we therefore strongly recommend performing the upgrade off hours.
- Migration from Cisco TMSXE 2.x is no longer supported.
  Customers currently running Cisco TMSXE 2.x must migrate to Microsoft Exchange 2010 and Cisco TMSXE 3.0.2, which includes the necessary tools for migrating Cisco TMSXE. They can then upgrade to the latest version.

Before You Start

We strongly recommend using the Cisco TMSXE Deployment Guide to get the complete overview of prerequisites and best practices for installations and upgrades.

Make sure you are logged in as a local administrator on the server.

Running the Installer

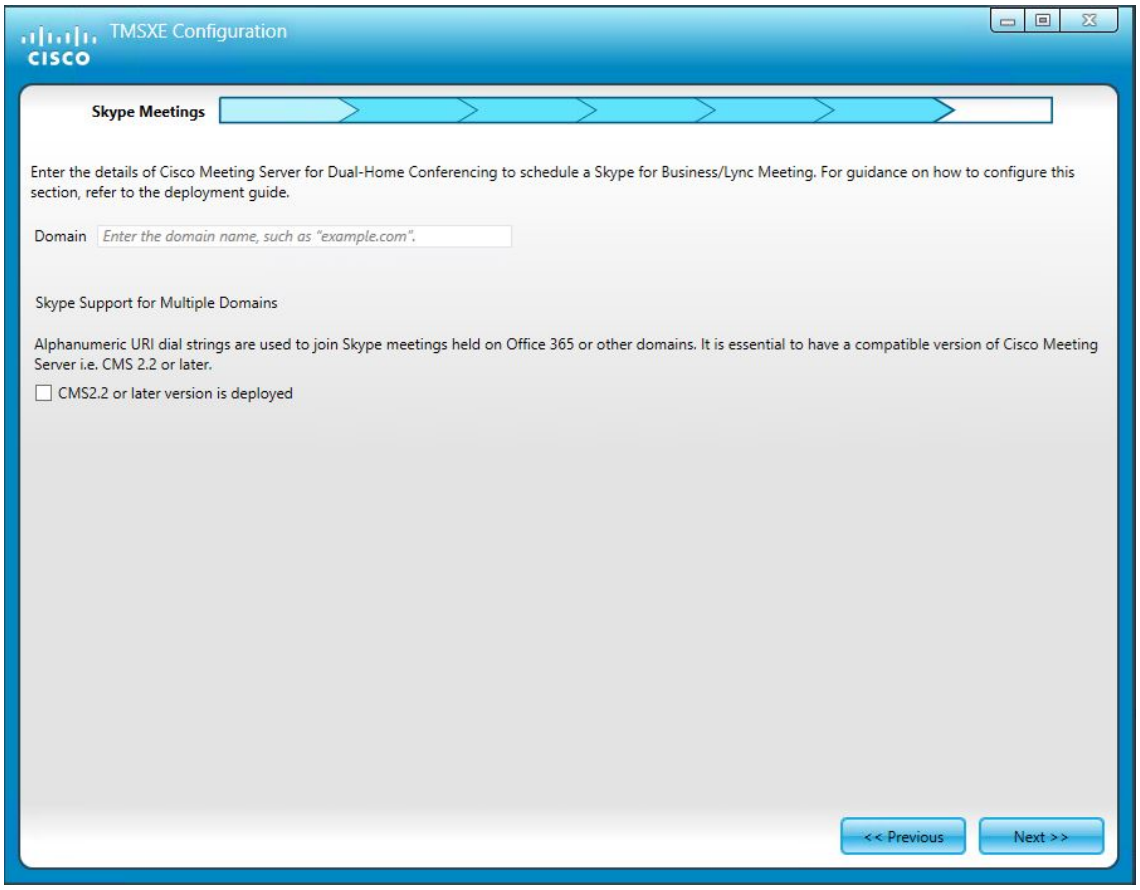
1. Stop the Cisco TMSXE Windows service, on both nodes if upgrading a clustered deployment.
2. Check Windows Update and install any critical updates to the .NET framework on the server or servers where Cisco TMSXE will be installed. Make sure the .NET version is 4.6. Reboot the server after installing if prompted.
3. Place the installation files on the server.
4. Run the Cisco TMSXE installer and accept the End-User License Agreement (EULA) to start the installation process.
5. The installer will detect that you have a previous installation of Cisco TMSXE. Click **Upgrade** to continue.
6. Click **Next** to start the setup.
7. Accept the terms in the license agreement and click **Next**.

8. Select which components to include with your installation:
   - Cisco TMS Booking Service is required if you plan to use WebEx Productivity Tools with TelePresence.

     If you enable this, you are prompted to modify or confirm the name of the IIS application pool to which you want Booking Service installed. .
   - Cisco TMSXE Clustering is required if you want to set up Cisco TMSXE with redundancy. See the deployment guide for further instructions on upgrading to a clustered deployment.
   - Performance Monitors can be enabled to allow monitoring of Cisco TMSXE performance using standard Windows tools.
9. If an earlier version of Cisco TMSXE is currently installed, you are prompted to upgrade.
   - Click **Yes** to continue. Upgrading removes the old version and upgrades the existing Cisco TMS database.
   - Click **No** to abort the installation and leave the current installation untouched.
10. When the upgrade is completed, click **Finish**.
11. The configuration tool launches.

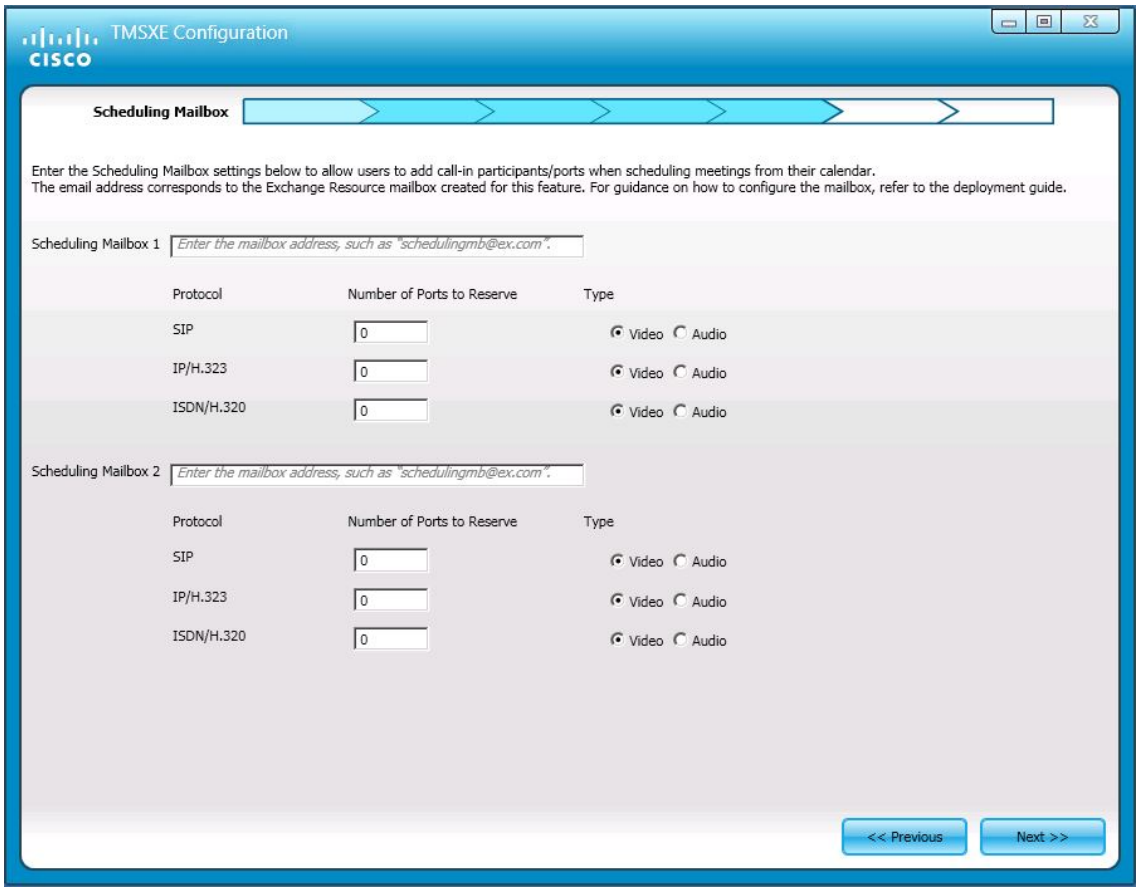
Configuring Skype Meetings in Cisco TMSXE

1. Click through the configuration wizard and in the **Skype Meetings** tab, enter the Cisco Meeting Server's domain name that is configured for Dual Home Conferencing in the **Domain** field.
2. Click **Next** to enter details in the other tabs.



Configuring Scheduling Mailbox in Cisco TMSXE

1. Click through the configuration wizard and in the **Scheduling Mailbox** tab, enter Scheduling mailbox's email addresses in the **Scheduling Mailbox** fields. Enter the number of ports to be reserved for each protocol in the **Number of Ports To Reserve**. Select the call type as audio or video in the **Type** field.
2. Click **Next** to enter details in the other tabs.

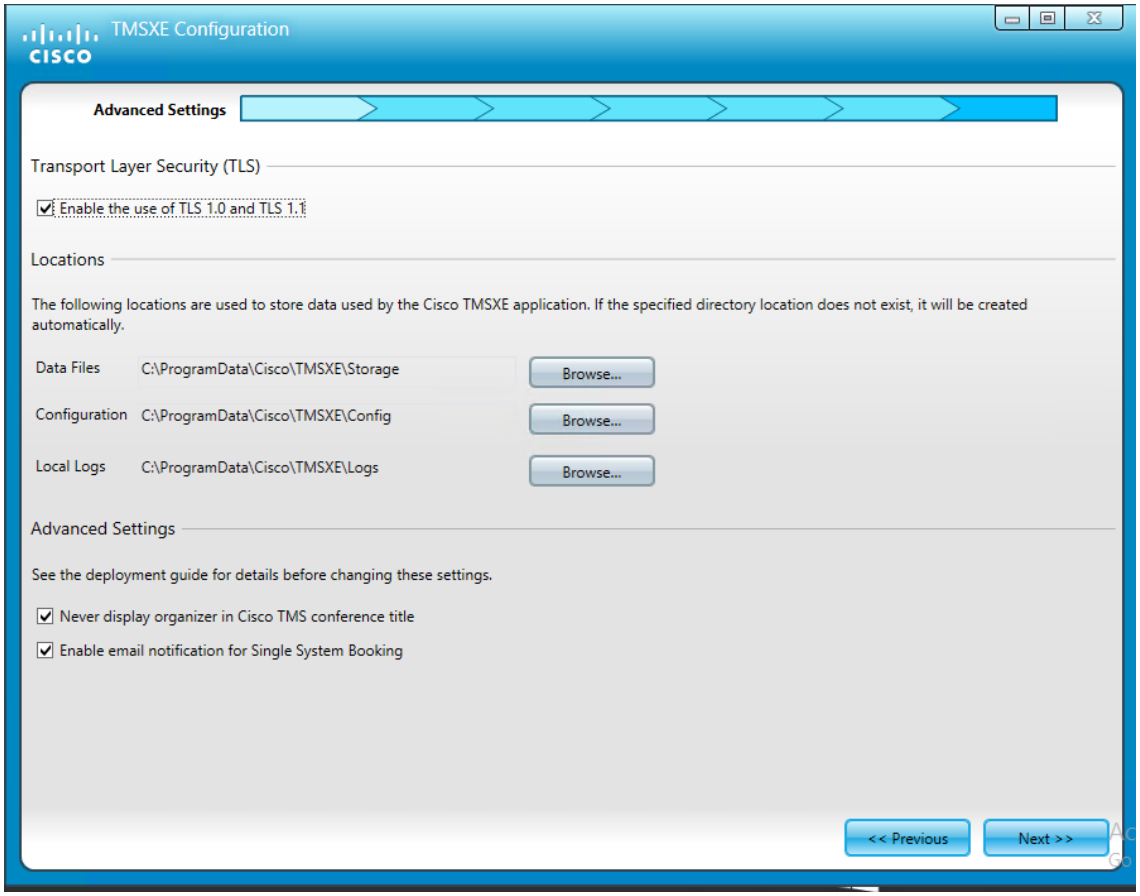


Configuring Advanced Settings in Cisco TMSXE

1. Click through the configuration wizard and in the **Advanced Settings** tab > **Transport Layer Security (TLS)** section, by default, **Enable the use of TLS 1.0 and TLS 1.1** field is selected. This enables Cisco TMSXE to communicate with either one of the TLS versions that is 1.0, 1.1 or 1.2.

- If **Enable the use of TLS 1.0 and TLS 1.1** is deselected Cisco TMSXE communicates only with TLS 1.2 . Also, the **Use HTTP** option is disabled in **Cisco TMS** and **Exchange Web Services** tabs.
  Note: If the Admin has already selected **Use HTTP** option in **Cisco TMS** and **Exchange Web Services** tabs and deselects **Enable the use of TLS 1.0 and TLS 1.1** option then **Use HTTP** option will be deselected and disabled.

2. Click **Next** to enter details in the other tabs.


TMSXE Configuration
Advanced Settings
Transport Layer Security (TLS)
Enable the use of TLS 1.0 and TLS 1.1
Locations
The following locations are used to store data used by the Cisco TMSXE application. If the specified directory location does not exist, it will be created automatically.
Data Files
C:\ProgramData\Cisco\TMSXE\Storage
Browse...
Configuration
C:\ProgramData\Cisco\TMSXE\Config
Browse...
Local Logs
C:\ProgramData\Cisco\TMSXE\Logs
Browse...
Advanced Settings
See the deployment guide for details before changing these settings.
Never display organizer in Cisco TMS conference title
Enable email notification for Single System Booking
<< Previous
Next >>

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)