Cisco TelePresence Management Suite Extension for Microsoft Exchange 5.10

Deployment Guide

Last Updated: March 2020

Contents

Introduction

Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE) is an extension for Cisco TelePresence Management Suite that enables videoconference scheduling via Microsoft Outlook, and replicates Cisco TMS conferences to Outlook room calendars.

This deployment guide describes how to prepare for, set up, and configure a new deployment, as well as upgrading from a previous version of Cisco TMSXE, and troubleshooting issues that may arise during deployment or general operation.

Related documents

The following table lists documents and websites referenced in this document, and other supporting documentation. All documentation for the latest version of Cisco TelePresence Management Suite Extension for Microsoft Exchange can be found at: www.cisco.com/en/US/products/ps11472/tsd_products_support_series_home.html

Title	Link
Cisco TelePresence Management Suite Extension for Microsoft Exchange Software Release Notes (5.10)	cisco.com
Cisco TelePresence Management Suite Extension for Microsoft Exchange User Guide (5.10)	cisco.com
Cisco Telepresence Management Suite Booking API Programming Reference Guide	cisco.com

Training

Training is available online and at our training locations. For more information on all the training we provide and where our training offices are located, visit www.cisco.com/go/telepresencetraining

Glossary

A glossary of TelePresence terms is available at: tp-tools-web01.cisco.com/start/glossary/

Prerequisites

This section details the prerequisites and best practices for installing Cisco TMSXE5.10, whether performing a new installation or upgrading from a previous version of the product.

Estimating Your Deployment Size

The requirements for Cisco TMS depend on and grow with the size and complexity of the deployment. The complexity of an installation is driven primarily by the volume of activity and number of endpoints controlled by and bookable in Cisco TMS.

Use the following chart to identify the relative size of your deployment. If your intended deployment matches multiple level criteria, apply the highest level.

	Regular and Cisco BE6000	Large
Cisco TMS	■ < 200 controlled systems ■ < 100 concurrent participants ■ < 50 concurrent ongoing scheduled conferences	■ < 5000 systems that use system licenses, that is, controlled systems, systems registered to Unified CM that are added to Cisco TMS, and Unmanaged Rooms. Adding more than 5000 such systems is not supported. ■ < 1800 concurrent participants ■ < 250 concurrent ongoing scheduled conferences
Cisco TMSXE	< 50 endpoints bookable in Microsoft Exchange	< 1800 endpoints bookable in on-premises Microsoft Exchange or < 1000 endpoints bookable in Office 365 or a combination of on-premises Exchange and Office 365 Note that with Office 365, latency towards Exchange is likely to be greater than for an on-premises deployment. This may lead to Cisco TMSXE occasionally saving a booking before all related events have been processed. Users will then receive multiple email notifications for the same booking.
Cisco TMSPE	■ < 1000 Collaboration Meeting Rooms ■ < 2000 Cisco VCS-provisioned users (Note: Cisco VCS provisioning not supported on BE6000)	■ < 48,000 Collaboration Meeting Rooms ■ < 100,000 Cisco VCS-provisioned users

Co-residency	All three applications and Microsoft SQL Server may be co-resident.	■ Cisco TMSXE must be on a dedicated server. ■ Cisco TMS and Cisco TMSPE must use an external SQL Server.

Other factors that influence Cisco TMS performance and scale include:

- The number of users accessing the Cisco TMS web interface.
- Concurrency of scheduled or monitored conferences.
- The use of ad hoc conference monitoring.
- Simultaneous usage of Cisco TMSBA by multiple extensions or custom clients. Booking throughput is shared by all scheduling interfaces including the Cisco TMS New Conference page.

Actual booking speed will vary based on the meeting size, features, and schedule complexity around the meeting.

Hardware Requirements

Find the appropriate hardware requirements below based on your estimated deployment size.

All applications including SQL Server may also be installed on virtual machines with specifications corresponding to these hardware requirements

Regular Deployment and Cisco Business Edition 6000

In a regular deployment, Cisco TMS and extensions can be co-located on the same server.

	Requirement	Cisco BE6000
CPU	2 cores (Xeon 2.4 GHz or larger), dedicated	1 vCPU
Memory	8 GB, dedicated	4 GB vRAM, dedicated
Disk space provided on server	60 GB	60 GB

Note that Cisco TMSPE on Cisco Business Edition 6000 does not include Cisco VCS-based user provisioning for end-points or FindMe.

Large Deployment

In a large deployment, Cisco TMSXE and SQL Server must be external, while Cisco TMS and Cisco TMSPE are always co-resident.

Cisco TMS and Cisco TMSPE Server

	Requirement
CPU	2 cores (Xeon 2.4 GHz or larger), dedicated
Memory	8 GB, dedicated
Disk space provided on server	80 GB

Cisco TMSXE Server

The requirements for this server correspond to the recommended hardware requirements for the supported operating systems.

Recommended Cisco TMS Configuration Changes

To decrease the load on SQL Server and Cisco TMS services in a large deployment, we strongly recommend the following settings :

- **Administrative Tools > Configuration > Conference Settings**: Set **Default Reservation Type for Scheduled Calls** to *One Button To Push*
- **Administrative Tools > Configuration > General Settings**: Set **Route Phone Book Entries** to *No*
- **Administrative Tools > Configuration > Network Settings**: Set **Enable Ad Hoc Conference Discovery** to *Only for MCUs* or *No*.

Cisco TMSXE Server Software Requirements

The software requirements are independent of the size of your deployment. For size-appropriate hardware requirements, see Estimating Your Deployment Size, page 9 and Hardware Requirements, page 10.

Note: You must have Local server administrator rights for all Cisco TMSXE installations, upgrades, configurations, and Cisco TMSXE tool usage.

Software

Table 1 Software Requirements for the Cisco TMSXE Server

Product	Version
Microsoft Windows Server	■ 2019 (64 bit) ■ 2016 (64 bit) ■ 2012 R2 (64-bit) ■ 2012 Note: The server operating system must be English, Japanese, or Chinese.
Microsoft .NET Framework	■ .NET Framework Full (extended) is required ■ Version 4.8, 4.7

Active Directory and DNS

Active Directory system requirements correspond to AD requirements for Exchange.

The Cisco TMSXE server must:

- be configured to use a DNS server with service records for the Active Directory domain of the Exchange server.
- have network access to Active Directory, meaning no firewall must be blocking traffic, and LDAP and Global Catalog must be open.

Updating the **Display Name** of an Active Directory account requires restarting the Cisco TMSXE Windows service for the new name to be applied.

In case there is a change in display name of a Scheduling Mailbox, the functionality may be impacted until Cisco TMSXE service is restarted.

If the email address noted in the **mail** attribute in Active Directory is populated, then it must be unique across all objects within Active Directory. Cisco TMSXE uses this field for Active Directory look ups.

Cisco TMS Requirements

Table 2 Requirements for the Cisco TMS Server

Version	15.10
Network	HTTPS (recommended) or HTTP connectivity is required from Windows Server hosting Cisco TMSXE.

Licensing Requirements

Each telepresence endpoint to be booked through Cisco TMSXE must already have been added to Cisco TMS and licensed for general Cisco TMS usage.

Additionally, in order to use Cisco TMSXE for booking these endpoints, you must have one of the following:

- One Cisco TMSXE - Extension for Microsoft Exchange option key per 25 telepresence endpoints integrated with Cisco TMS, usually recommended for smaller deployments. See below for detail on how system licenses are activated.
- One Application Integration Package option key per Cisco TMSXE deployment . This option is recommended for deployments with a large number of endpoints.

If both license keys are present, Cisco TMS will only use the Application Integration Package key.

Enabling Option Keys

To enable an option key in Cisco TMS:

1. Go to **Administrative Tools > Configuration > General Settings**.
2. In the **Licenses and Option Keys** pane, click **Add Option Key**.
3. Input the option key string.
4. Click **Save**.

Per System Licensing

Once the per system option key has been activated in Cisco TMS, the **Allow Remote Bookings** setting determines whether each system is using a license.

This setting is void and hidden if the Application Integration Package option is used. If both option keys are added, only the Application Integration Package option will be used by Cisco TMS.

The first time a system is booked through Cisco TelePresence Management Suite Extension Booking API, **Allow Remote Bookings** will be toggled to *Yes* for that system in Cisco TMS, provided a license is available. If no more licenses are available, **Allow Remote Bookings** will be left as *No* for that system, and the requested booking will be denied. A Cisco TMS ticket will be generated to notify the administrator that no more licenses are available.

Note that Cisco TMSXE performs a test bookings as each endpoint is added through the configuration tool, thus also enabling Allow Remote Bookings.

To view and/or modify the setting:

1. In Cisco TMS, go to **Systems > Navigator**.
2. Select the system you want.
3. Click the Settings tab.

4. In the **TMS Scheduling Settings** pane, you will find *Allow Remote Bookings*.

   If the setting is *Yes*, the system is currently using an Exchange Integration Option license.

5. To disable the setting:
   a. Click **Edit Settings**.
   b. Uncheck *Allow Remote Bookings*.
   c. Click **Save**.

Microsoft Exchange Requirements

Table 3 Requirements for the Microsoft Exchange server

Requirement	Description
Microsoft Exchange	Tested versions: ■ Microsoft Exchange 2016 ■ Microsoft Exchange 2013 and 2013 Service Pack 1. ■ Microsoft Office 365 for enterprise (Exchange online) up to and including version 15.0.898.9. We will test new versions as they are made available to us. To find out which exact version of Office 365 your organization has, follow these instructions from Microsoft: Verify Office 365 tenant version and status ■ Microsoft Exchange 2010 Service Pack 3.
Windows Server	Tested versions: ■ Microsoft Windows Server 2019 ■ Microsoft Windows Server 2016 ■ Microsoft Windows Server 2012 R2 ■ Microsoft Windows Server 2012
Exchange Web Services (EWS)	Must be enabled on the Exchange server.
Active Directory	Must be available on premises. If using Office 365, Active Directory Federation Services and the Windows Azure Active Directory Sync tool are required. By default, the **Use HTTP** option in the **Exchange Web Services** tab is unchecked. This enables you to establish a secure connection between Cisco TMSXE and Active Directory.

Client Access Server Redundancy and Autodiscover

Cisco TMSXE supports multiple Client Access Servers (CAS) using:

- Autodiscover, which must be enabled both in the Exchange environment and in the Cisco TMSXE configuration tool.

- A network load balancer (NLB):
  - With Exchange 2010, the NLB must be set up to use exchangeCookie *or* have a sticky IP connection (affinity) to one CAS server.
  - In the case of a CAS failover (2010) or mailbox failover (2013 or 2016), performance will be impacted during re-subscription. If the network load balancer cannot reach the primary CAS, Cisco TMSXE will be redirected to another CAS and re-subscribe to resource mailboxes, as subscriptions are stored per CAS instance (2010) or mailbox server (2013 or 2016).
  - For guidance on configuration, see the TechNet article *Load Balancing Requirements of Exchange Protocols*.

Certificate Authentication

Optionally, the Cisco TMSXE service user can authenticate with Exchange and Active Directory using a client certificate and password rather than a username and password.

- The Exchange CAS must be configured to use client certificate authentication. See Exchange documentation for instructions.
- You must have a valid Personal Information Exchange (PKCX #12) (.pfx) client certificate that is reachable from the Cisco TMSXE file system.

OAuth for Office 365

Optionally, the Cisco TMSXE can be configured to use OAuth for Office 365 to authenticate with Exchange online with alternate Active Directory, rather than using certificate authentication or using a username and password.

Client Requirements

Cisco TMSXE has been tested with the following clients and Exchange versions:

Table 4 Exchange Server and Client versions

Client	Exchange version(s)
Office 365	Office 365
Microsoft Outlook 2013	Office 365 and Exchange 2013
Outlook Web App	Exchange 2010, 2013 and 2016
Microsoft Outlook 2010	Exchange 2010
Microsoft Outlook 2016	Office 365 and Exchange 2016

Advanced settings are available with the Cisco TelePresence form, which can only be used with a local Outlook client for Windows.

Before installing Cisco TMSXE 5.10, make sure both Outlook and Exchange are already set up so that users are able to book meetings that include room mailboxes.

Deployment Scenarios and Best Practices

This section discusses the supported deployment scenarios for Cisco TMSXE, and the features, limitations, and best practices to observe with each scenario.

On-Premises Exchange Deployments

Cisco TMSXE can be deployed entirely with on-premises Exchange servers. For version requirements, see Microsoft Exchange Requirements, page 13.

For environments that mix on-premises Exchange with Office 365, see Exchange Hybrid Deployments, page 15.

Mixed Exchange Environments

Combining Exchange servers with different supported versions of Exchange in the same deployment is supported, provided CAS autodiscovery is enabled and all CAS servers are running Exchange 2016 or 2013 or 2010.

Microsoft Office 365 Deployments

Cisco TMSXE supports Office 365-based deployments with both CAS and mailbox servers in the cloud. For all deployments, Active Directory *must* be on premises in order to work with Cisco TMS, Cisco TMSXE must access the same Active Directory Forest as Cisco TMS.

Cisco TMSXE requires the use of Autodiscovery CAS.

Limitations

- Office 365 plans for small businesses are not supported with Cisco TMSXE due to the limited feature sets available with these subscription models.
- Access to advanced telepresence settings and Webex Productivity Tools with TelePresence requires a local Outlook client.

  Users who only have webmail access can book Cisco Collaboration Meeting Rooms Hybrid meetings using the Webex Scheduling Mailbox.

Exchange Hybrid Deployments

Office 365 may be deployed in combination with on-premises Exchange servers. Cisco TMSXE supports combining Exchange servers on-premises and in the cloud provided that:

- On-premises Exchange servers are either Exchange 2016 (recommended) or Exchange 2013 or Exchange 2010.
- Active Directory is on premises, which is required to work with Cisco TMS. Cisco TMSXE must access the same Active Directory Forest as Cisco TMS.

Redundant Deployments

Clustering and load balancing as described below are supported with Exchange 2010 and later.

Cisco TMSXE Service Clustering

Active/passive redundancy for the Cisco TMSXE service is supported through clustering. Clustering support must be enabled when Cisco TMSXE is installed on the first node.

The nodes will share configuration and data folders, but write their logs to separate local locations. Which node is currently active/passive is written to the log on **INFO** level. Note that for any troubleshooting situation, log sets from both the nodes will be required.

If one node goes down, the other will automatically become active. A failover may be forced by stopping the service on the active node, or rebooting the server.

For prerequisites and setup instructions, see Installing Cisco TMSXE with Service Clustering, page 56.

Supported Redundancy Models

When setting up Cisco TMSXE with redundancy, the following scenarios are supported, in conjunction with a load-balanced Cisco TMS setup as described in the "Redundant deployments" chapter of *Cisco TelePresence Management Suite Installation and Upgrade Guide*:

Redundancy is not supported with small deployments where Cisco TMS and Cisco TMSXE are co-hosted on the same server as described in Guidance on Large Deployments, page 16.

Guidance on Large Deployments

Cisco TMSXE automatically changes the underlying configuration to better support deployments with large numbers of mailboxes added.

With a large deployment, beware of the following:

- The time it takes to populate the configuration tool systems list, to validate all systems, and to import existing meetings from mailboxes added, may be substantial.
- As the number of linked systems increases, the time between Exchange mailbox checks increases, which means that sometimes Cisco TMSXE sends the booking to Cisco TMS before having information about all participants for a meeting.
  - This behavior will typically be seen in deployments with more than 1700 mailboxes added to Cisco TMSXE.
  - This may lead to users receiving multiple confirmations for the same booking, if more than one room is booked.
  - The resulting meeting will function as intended, but the extra notifications and partial bookings may be confusing to users.

Best Practices for all Deployments

Install, Upgrade, and Add Mailboxes During Off Hours

We strongly recommend upgrades be performed during off hours to minimize down time for users and risk of out of sync conditions.

If adding existing mailboxes that already contain bookings to your Cisco TMSXE deployment, you must do this off hours, due to the expected impact on Cisco TMS performance during first-time replication.

Provide Users with Guidance

If deploying the Webex Scheduling Mailbox or the Cisco TelePresence form, we recommend that users be provided with a link to *Cisco TelePresence Management Suite Extension for Microsoft Exchange User Guide* for a simple overview of how the advanced settings work.

Mailbox Configurations and the "Private" Flag

In order to avoid conflicting settings, all room mailboxes added to Cisco TMSXE must be configured to handle booking subjects and privacy settings in the same way. This means that the following settings must be applied to all or none of the mailboxes:

- **Remove the private flag on an accepted meeting (RemovePrivateProperty)**

As a best practice, we recommend not to rely on the "Private" flag for security. If the flag is allowed on accepted meetings, make sure to restrict access only to opening the resource calendars.

The "Private" flag will be accepted within the Outlook client and also supported by Cisco TMS. The meeting subjects are not viewable on endpoints that supports the "Meetings" calendar.

If a booking that has a "Private" flag in Exchange has its participants or recurrence pattern modified in Cisco TMS, the "Private" flag is retained when these changes are replicated to Exchange.

Notes:

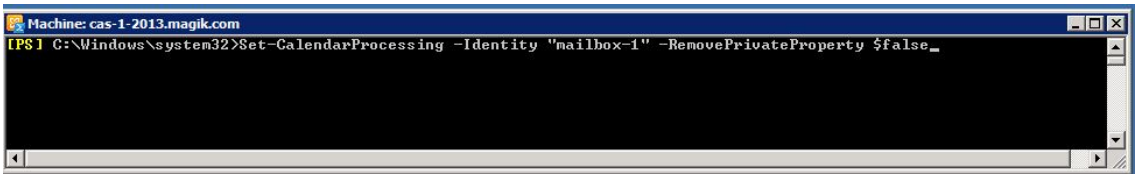
1. If the Privacy Flag is modified from MS Outlook, the organizer will not get a confirmation mail.
2. If a user has full permission for a room mailbox, then they are able to view and open the private appointment scheduled with the room by other users, in it's room calendar via Outlook Web App (OWA). However this is not possible via MS Outlook. In MS Outlook, the room calendar's private appointment details are not shown. This behavior is seen in Outlook 2013 and 2016.

See Preparing Resource Mailboxes with Delegates, page 28 for detailed instructions on the required and supported settings for mailboxes.

Configuring RemovePrivateProperty in Microsoft Exchange Server

To set up RemovePrivateProperty:

1. In **Microsoft Exchange Server**, open **Microsoft Exchange Management shell**.
2. Execute **RemovePrivateProperty** command to set mailbox property as **RemovePrivateProperty = False** .
   For example: **Set-CalendarProcessing -Identity "<room mailbox>" -RemovePrivateProperty $false**.
   The following screenshot provides an example of **RemovePrivateProperty** command that is executed in Microsoft Exchange 2013 Management Shell.



Autodiscovery Configuration

Autodiscovery creates additional resiliency in case of CAS failure, but with the trade-off that Cisco TMSXE start-up time increases. In large deployments a significant increase of start-up time can be observed.

Secure Communication

We recommend that secure communication be used between the servers. HTTPS is therefore the default communication protocol, and the **Use HTTP** setting in the configuration tool is disabled by default when installing the software, both for communicating with Cisco TMS and with Exchange Web Services.

In order for this communication to work as desired, Cisco TMS and Exchange must both present valid certificates to Cisco TMSXE.

Certificate Requirements

A certificate issued from a trusted CA (Certificate Authority) in the customer network is considered a valid certificate if it also:

- matches the host name of the machine that the certificate is issued for, and the address that the client uses to access the server.
- has not expired.
- comes from an issuing CA that has not expired.
- complies with the company's internal certificate policy

A company CA must therefore issue certificates for Cisco TMS and Exchange matching the URL used to access them, usually the FQDN.

To verify that you have certificates that are valid and working:

1. Launch Internet Explorer on the Cisco TMSXE server.
2. Enter the URL for the Exchange CAS and verify that the URL field turns green.
3. Enter the URL for the Cisco TMS server and verify that the URL field turns green.

No warnings regarding certificates should be displayed.

Untrusted Certificates

Certificates that do not meet the above listed requirements are considered to be *untrusted* and must not be used in a production setting.

If, during initial setup, the certificates encountered for Cisco TMS or Exchange do not validate, the configuration tool will prompt the administrator, offering to **Allow Untrusted Certificates**. This setting cannot be reverted and must only be used if installing in a test environment.

Limitations for all Deployments

For an overview of supported scenarios and recommended settings, see Configuring Required Settings, page 26.

Booking Limitations

If booking a meeting through Outlook, Cisco TMS, or any other booking interface, whose duration is three minutes or less, the meeting will not be processed by Cisco TMSXE.

- Cascading to additional MCUs when the number of participants exceeds the capacity of the first MCU is not supported.

  To support such scenarios, set up Cisco TelePresence Conductor as the preferred MCU in Cisco TMS.

- When a service user is performing all bookings, the booking permissions are the same for all users. Individual permissions and restrictions in Cisco TMS are ignored.
- Meetings in the past cannot be changed or deleted, and you cannot move a meeting from the past to the future.
- If sufficient system licenses are not available at the time of editing an existing booking, the booking will be deleted.
- Yearly recurrence is not supported.

- When the Smart Scheduler is used, booking permissions for endpoints configured on Cisco TMS through Microsoft Outlook using Cisco TMS/ Cisco TMSXE combination, works in the expected manner. However, permissions configured on Cisco TMS for video endpoints are not adhered, when booking is done using the Smart Scheduler.

Booking Horizon and Recurrence

Cisco TMS will decline any meeting request that is not within its booking horizon or that has an unsupported recurrence pattern:

- Series with more than 100 occurrences or with no end date.
- Meetings including occurrences outside of the Cisco TMS booking window. We strongly recommend configuring identical booking windows for Cisco TMS and all integrated resource mailboxes in Exchange.
- Meetings in the past.
- The declined meeting will also be deleted from Exchange's resource calendar.

Ongoing Meetings

Updating a single meeting that is currently ongoing is possible, but will not always be successful.

- Modifying any meeting, extending the meeting will fail if it creates a booking conflict for any of the participants.
- Modifying single meetings, including meetings that are part of a series:
  - Editing the start time will not work and Cisco TMS will throw an exception.
  - Editing the meeting so that it would be required to be disconnected and re-routed will not be successful.
  - Any other aspects of the meeting can be modified, but if the number of participants exceeds the available capacity of the MCU or TelePresence Server, Cisco TMS will throw an exception and the participants will not be added.
- *Deleting* a recurrent series while a meeting in the series is ongoing will cause the ongoing meeting to end.
- *Modifying* a recurrent series while a meeting in the series is ongoing will turn the ongoing occurrence into a single meeting, separate from the series:
  - Any occurrences of the modified series that are in conflict with the ongoing meeting, will not be created.
  - Any past occurrences in the series will not be modified.
  - Pending occurrences are assigned new conference IDs.
  - If the end time or date is edited for the series, the entire series will get deleted.
  - Any changes done to the series that creates conflict with the separated meeting will delete the series.
- Editing an ongoing meeting's end time to overlap with a future meeting may lead to deletion of the ongoing meeting.

Cisco Webex Collaboration Meeting Room Cloud

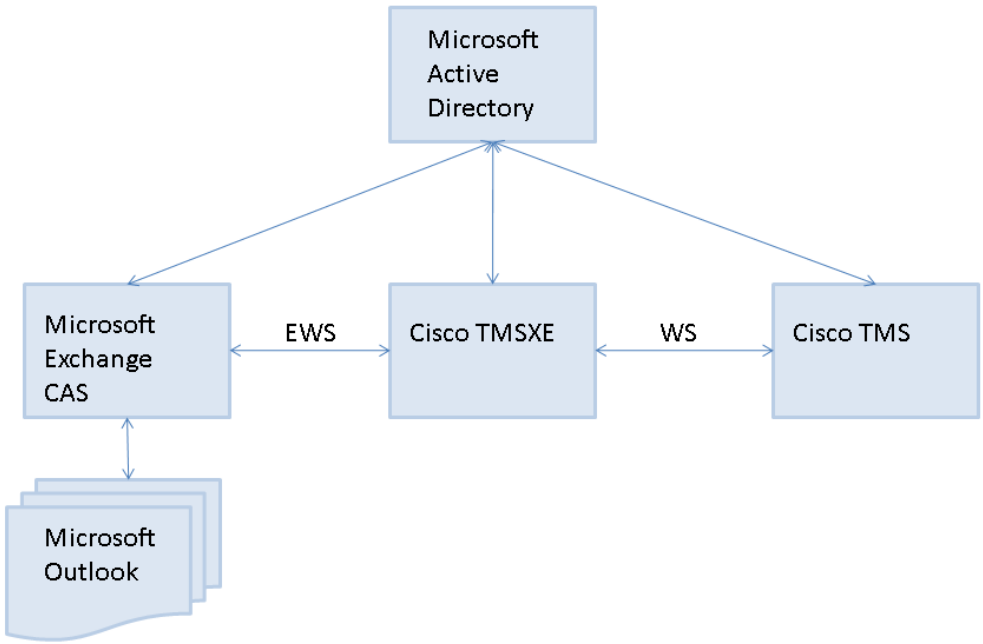
In a solution including Cisco Webex CMR Cloud, Webex Productivity Tools with TelePresence gets the appropriate SIP URI from Webex and includes this information in the calendar invite sent to the Microsoft Exchange room mailboxes. Cisco TMSXE gets this information from Microsoft Exchange and passes it to Cisco TMS, where it is then booked as an externally hosted conference. The external conference is booked with the value of **Default Reservation Type for Scheduled Calls** as configured in **Cisco TMS> Administrative Tools -> Configuration -> Conference Settings -> Conference Creation**.

Note: No extra configurations are required other than those needed for standard Cisco TMSXE functionality.

.

System Architecture and Overview

System Overview



Cisco TMSXE communicates with Exchange or Office 365 using Exchange Web Services (EWS).

Using Web Services, Cisco TMSXE passes booking requests to Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA) and receives accept/decline messages.

Depending on the protocol used, Cisco TMSXE uses port 80 (HTTP communication) or port 443 (HTTPS communication).

The Booking Process

The sections below describe how bookings are created in Outlook or Cisco TMS and replicated through Cisco TMSXE.

See also Limitations for all Deployments, page 18.

Outlook to Cisco TMS

1. Using Outlook, the organizer creates a meeting request containing one or more video resources and, optionally, the Webex Scheduling Mailbox, then clicks **Send**.

   Organizers may book from their own calendar or from a resource calendar.

2. Exchange checks resource calendars for availability and does one of the following:
   - sends an initial confirmation to the organizer that the resources are now booked and passes requests on to Cisco TMSXE.
   - notifies the organizer that none of the resources are available.

     In this scenario, Cisco TMSXE is not contacted, and the organizer must re-initiate a booking (step 1).
   - notifies the organizer that one or more resources are unavailable *and* sends an initial confirmation that some of the resources are now booked. The requests for these resources are passed on to Cisco TMSXE.

     In this scenario, the organizer must either change the meeting time or find other resources that are available at the desired time, and modify the booking using Outlook.
3. Cisco TMSXE gathers up requests from Exchange and passes them on to Cisco TMS.
4. Cisco TMS checks system availability as relevant.
   - If the conference connection type is requested to be *Automatic Connect*, *One Button to Push*, *Manual Connect*, or *No Connect*, Cisco TMS will also attempt to book routing resources for the conference.
   - If only one video resource and no external participants are requested, no routing attempts will be made, regardless of the conference connection type that is requested and stored for the conference.
   - If the *Reservation* connection type is requested, the video resources (rooms) are reserved, but no routing resources are booked.
5. On receiving the results of the booking requests, Cisco TMSXE does one of the following:
   - If routing was requested and successful, routing information is sent to the organizer.
   - If one or more resources could not be reserved, or if routing was requested but unsuccessful, Cisco TMS will save the meeting as *Defective*. For more on this scenario, see Defective Meetings, page 21.
   - If no routing was requested and all resources could be reserved, no notifications are sent.

Defective Meetings

A *Defective* conference in Cisco TMS has been booked by an external client that encountered a resource conflict or routing problem.

A defective conference retains all properties of the booking request without setting up routing or consuming telepresence resources. Until all issues are resolved, Cisco TMS will not initiate a defective conference or send it to endpoints.

- In the case of a routing issue, all endpoints in the booking will be set to *Busy* for the scheduled time, keeping the reservation while the administrator or user resolves the issue.
- In the rare case of an endpoint reservation conflict, the endpoints will not be set to *Busy* for the defective booking.

Defective conferences can be corrected by the organizer or the administrator:

- Users who book conferences that are saved as defective will be notified by email and can resolve most issues by changing their request and rescheduling from their client.
- Administrators can locate and resolve defective conferences in Cisco TMS by going to **Administrative Tools > Diagnostics > Conference Diagnostics** or **Booking > List Conferences**.

  Conferences that are defective because of configuration errors or a permanent lack of routing resources must be resolved by an administrator.

When scheduling a series where only some occurrences have a resource conflict or routing issue, Cisco TMS will only store the problematic occurrences as defective, leaving the remaining occurrences unaffected.

Master Participant

The videoconference master is the participant in the conference who is considered to be the "chair" and the one who will be prompted to start a manually connected conference, or extend the meeting if more time is needed. Not all endpoints are able to be the videoconference master, as this feature relies on functionality not available for all types of endpoints.

When booking from Outlook, Cisco TMS will set the first resource in the **Location** field as the master participant provided this endpoint has master participant capabilities. If the first resource is not capable of being the master, Cisco TMS will choose another endpoint from the participant list. The Video Conference master should be mentioned in the **Location** field of the appointment for a **Manual Connect** conference, else the conference type will be changed to **No Connect** in Cisco TMS.

Cisco TMS to Exchange

1. Using the Cisco TMS web interface, the organizer books a conference.
2. Every minute Cisco TMSXE polls Cisco TMS and gets all updates to bookings since the last polling.
3. Cisco TMSXE creates or updates bookings in Outlook resource calendars, including subject, room participants, and a message body that includes information about who booked the meeting in Cisco TMS.

Not all conference properties are replicated to Exchange when a conference is booked through Cisco TMS:

- Advanced settings are not replicated.
- Organizer and all participants are not included in the **To:** field.
- When specified through Cisco TMS, the master participant is not reflected in the order of the rooms in the **Location:** field.

Updating Outlook-Created Bookings using Cisco TMS

When a meeting booked through Outlook is updated using Cisco TMS, resource calendars are updated, but the organizer's calendars is not, as Cisco TMSXE does not have permissions to modify the calendars of personal mailboxes.

If rooms are added to a booking from Cisco TMS, the organizer will not be able to remove them using Outlook.

Replication Delays

When booking from Outlook, Cisco TMSXE will wait for approximately one minute to collect all the info about the meeting before passing the booking to Cisco TMS.

If updating a meeting in Cisco TMS that has also been modified by an Outlook user, Cisco TMSXE will wait to push the change from Cisco TMS :

- While the change done in Outlook is being pushed to Cisco TMS.
- Until the item has been left unmodified in Exchange for 4 minutes.

Preparing to Install or Upgrade

Some procedures need to be carried out prior to running the Cisco TMSXE installer. The procedures include creating an account in Active Directory and creating a mailbox for that service account in the Exchange environment.

For a deployment that includes Microsoft Office 365, you can create the service account like any other account that is created in the local Active Directory.

Backing Up and Upgrading the Backend

Before any installation or upgrade we strongly recommend backing up all mailboxes that will be used.

For new installations, we particularly recommend backing up any existing room mailboxes that will be repurposed as telepresence room mailboxes prior to installing.

You must also upgrade to the required version of Cisco TMS before initiating any installation or upgrade of Cisco TMSXE.

Installing or Upgrading Cisco TMS

Before installing or upgrading Cisco TMSXE, install the required version of Cisco TMS, following the instructions in *Cisco TelePresence Management Suite Installation and Getting Started Guide*.

If upgrading Cisco TMS, you will need to perform the following procedures in the order they are listed:

1. Stop the Cisco TMSXE Windows service if you have an existing installation.
2. Follow the instructions in *Cisco TMS Installation and Upgrade Guide* to upgrade Cisco TMS.
3. Follow the instructions in this document to upgrade Cisco TMSXE.

Upgrading Cisco TMS from a Version Earlier than 14.2

If upgrading from a Cisco TMS version earlier than 14.2 and using Cisco TMSXE for booking from different time zones, you may need to upgrade to 14.3.2 and run the Time Zone Update Tool to correct time zone data on bookings before upgrading to the version of Cisco TMS required to install this version of Cisco TMSXE.

For detail on how to proceed and who needs to run the time zone update tool, see *Cisco TMS Installation and Upgrade Guide*.

Preparing for a New Installation

The option to perform a new installation of Cisco TMSXE will only be available if no previous 3.x version is found. (If you already have Cisco TMSXE 3.x installed, running the installer will prompt you to upgrade.)

Perform a clean installation of Cisco TMSXE 5.10 if:

- You do not have an existing deployment of Cisco TMSXE.
- You want to set up a test environment/deployment to see how Cisco TMSXE works.

Where an existing deployment exists, we strongly recommend that administrators upgrade.

Creating a Cisco TMSXE Service User in Active Directory

In Exchange Management Console, create a new user mailbox as a service user for Cisco TMSXE with the username and password of your choice. The service user will let Cisco TMSXE connect to Microsoft Exchange and Cisco TMS and

Active Directory Forest.

Creating a Cisco TMS User for Cisco TMSXE

1. In Cisco TMS, go to **Administrate Tools > User Administrations > Users**.
2. Click **New**.
3. Add the details for the previously created Cisco TMSXE service user.
4. Permissions in Cisco TMS are controlled on a group level. You must do one of the following:
   - Add the account to a group with a smaller subset of permissions, see Setting Up Minimal Required Permissions, page 24 below.
   - Add the service user to the site administrator group, which has universal access.

For each integrated system, the service user must also have the right to book. This is enabled by default for all default user groups in Cisco TMS.

Setting Up Minimal Required Permissions

In order for Cisco TMSXE to be able to book endpoints and access booking information from Cisco TMS, you must make the service user a site administrator or a member of a group that has the following permissions:

- *Read* and *Book* under **Systems > Navigator >** Select a system **> Folder and System Permissions > System Permissions**.
- *Read* under **Systems > Navigator >** Select a folder **> Folder and System Permissions > Folder Permissions** for all the folders above the system in Cisco TMS folder structure.

To view and/or modify the permissions for a Cisco TMS user group:

1. Go to Administrative **Tools > User Administration > Groups**.
2. Hover over the group you want, click the drop-down arrow and select **Set Permissions**.
3. Under **Booking**, make sure enabled permissions include:
   - *List Conferences - All*
     - *Read*
     - *Update*
   - *Misc*
     - *Booking*
     - *Book on behalf of*
     - *Approve Meeting*
4. Click **Save** if any modifications have been made.

Specifying Default Conference Settings

Default settings used for all bookings regardless of booking interface are specified in Cisco TMS. These settings are not transparent to the organizer booking from Outlook; we therefore recommend communicating these defaults to users/organizers in your organization.

To modify the default conference settings:

1. Go to **Administrative Tools > Configuration > Conference Settings**.
2. Make sure all default settings are configured as desired. For field-level explanations of the settings, see the built-in help (click the question mark in the upper right corner).
3. If not using Webex Productivity Tools with TelePresence or the Cisco TelePresence form, pay special attention to the field **Default Reservation Type for Scheduled Calls**:
   - If you want all scheduled conferences to be automatically routed and connected at the conference start time, set to *Automatic Connect*.
   - If you want the calls to be set up, but not automatically launched, opt for *One Button to Push* or *Manual Connect*.
   - If the setting is *Reservation*, no routing resources will be scheduled unless the organizer specifies a different conference type using the Cisco TelePresence form.
4. Click **Save** to apply the changes.

Creating Mailboxes for Cisco TMS Endpoints in Exchange

Before endpoints can be added to Cisco TMSXE, they must be represented by a room mailbox in Exchange.

Using PowerShell, Exchange admin center, or Exchange Management Console, create one room mailbox for each of your endpoints, such as **boardroom@example.com**.

For details on how to create room mailboxes, see:

- Exchange 2016, Office 365 and Exchange 2013: *Create and Manage Room Mailboxes*
- Exchange 2010: *Create a Room or Equipment Mailbox*

To simplify Cisco TMSXE setup, we recommend using the endpoint's Cisco TMS display name as the mailbox name (with any spaces removed).

All room mailboxes must then be configured with the appropriate settings and permissions. See the instructions for your version of Exchange in Configuring the Room Mailboxes, page 25.

Repurposing Existing Mailboxes

If an endpoint is in a meeting room that already has a room mailbox, the mailbox can be repurposed for Cisco TMSXE booking.

Note that any existing bookings in repurposed mailboxes will be replicated to Cisco TMS when Cisco TMSXE starts up. You will get the option to determine whether email notifications should be sent to organizers if any of these bookings fail. Any bookings in the past will not be replicated.

Repurposed mailboxes must also be configured following the instructions in Configuring the Room Mailboxes, page 25.

Setting Up PowerShell for Use with Office 365

Before you can configure mailboxes for use with Cisco TMSXE, you must enable Windows PowerShell to work with Office 365, following the below instructions from Microsoft:

1. Install and Configure Windows PowerShell
2. Connect Windows PowerShell to the Service

Configuring the Room Mailboxes

This section describes the necessary steps to configure room mailboxes for use with Cisco TMSXE.

These steps are required in the following scenarios:

- A new installation using new or repurposed resource mailboxes
- One or more new systems being added to your deployment during upgrade

Administrators upgrading from Cisco TMSXE 3.x do not need to reconfigure their mailboxes, but may still want to verify that all resource mailboxes are configured correctly and identically as described below.

The configuration tool will pop up a warning and errors will be written to the event log for most incorrect mailbox configurations. Note that if **AutoAccept** is not turned on, this will be logged as an INFO message in the Cisco TMSXE log.

In addition to the required configurations below, we recommend that room mailboxes be configured to give users a minimum of *Read* access so that free/busy information is available to organizers when booking.

Configuring Required Settings

Make sure that all resource mailboxes are configured identically and in line with the requirements outlined in the table below.

Differing settings between mailboxes can cause mismatches between Cisco TMS and Exchange.

Shell Parameter	Required Value	Description
`AutomateProcessing`	*AutoAccept*	Sets the mailbox to automatically process invitations
`BookingWindowInDays`	Must be between 1 and 1080. See description for recommendation.	Specifies for how long into the future users will be allowed to schedule meetings. We strongly recommend that this setting match that of Cisco TMS: **Administrative Tools > Configuration > Conference Settings > Conference Create Options >Booking Window (in days)**.
`EnforceSchedulingHorizon`	*True*	Specifies that recurring meetings that continue outside of the booking window will be rejected.
`AllowConflicts`	*False*	Prevents the mailbox from accepting overlapping bookings, which is not supported by Cisco TMS.
`ConflictPercentageAllowed`		These two settings may be set to anything so long as **AllowConflicts** is *False*. Any occurrences of a recurrent series that are in conflict with existing bookings will then be deleted as exceptions by Exchange before the booking is handled by Cisco TMSXE and Cisco TMS.
`MaximumConflictInstances`		
`DeleteSubject`	*False* (recommended) or *True*	We recommend disabling the option to delete meeting subjects. However, if it is a requirement for some room mailboxes that this option be enabled, it must be set to *True* for all mailboxes.
`AddOrganizerToSubject`	*False* or *True*	Sets the mailbox to never add the organizer's name to the subject of a booking. Optionally, this may be set to *true* for all mailboxes. Note that enabling both this setting and the setting to delete the subject will cause meeting subjects to be blank in Cisco TMS and Cisco TMSXE.
`RemovePrivateProperty`	*False*(recommended) or *True*	We recommend to disable this option, so that you are able to schedule private meetings. When set to True, this setting removes the "Private" flag for all meetings accepted by the mailbox. The setting must be identical for all mailboxes added to Cisco TMSXE. For further information, see Best Practices for all Deployments, page 16.

Shell Parameter	Required Value	Description
`CalendarRepairDisabled` (Set-Mailbox)	*True* (strongly recommended)	Disables the Calendar Repair Assistant (CRA) for the mailbox. There is no GUI option to modify this setting. The CRA is disabled by default in Exchange 2010 and enabled by default in later versions including Office 365.

For more information on the above settings, see:

- *Configure Resource Mailbox Options in Windows PowerShell (Office 365 Help)*
- *Configure User and Resource Mailbox Properties (Exchange 2010 Help)*

To verify that the above settings are active:

- Use the shell command `Get-CalendarProcessing -id [mailbox] | fl`
- To verify that the Calendar Repair Assistant is disabled, use the command `Get-Mailbox -id [mailbox] | ft CalendarRepairDisabled`

For more information on the above console settings, see the Microsoft TechNet article .

Setting Up Impersonation and Throttling

Office 365, Exchange 2016, Exchange 2013, and Exchange 2010

Cisco strongly recommends the use of impersonation for Cisco TMSXE. To prevent throttling issues with requests and grant the service user the necessary privileges, you must enable impersonation for the service user in Exchange and during Cisco TMSXE configuration.

Note: Configuring the use of an **ApplicationImpersonation** role within Exchange is not required when using OAuth for authentication.

To set up impersonation:

1. Use the shell cmdlet `New-ManagementRoleAssignment` and run the following command:

   ```
   New-ManagementRoleAssignment –Name:impersonationAssignmentName –
   Role:ApplicationImpersonation –User:[ServiceUser]
   ```

2. When configuring Exchange Web Service settings for Cisco TMSXE, make sure to enable **Service User Impersonation**.

This will allow the service user to impersonate all other users in the organization. To set limitations, use a management scope in Exchange; you can create a new one or use an existing scope for this. This can be used to restrict the service account impersonation for Room Mailboxes that Cisco TMSXE requires access.

For instructions and more detailed information from Microsoft on management scopes and impersonation, see:

- Configuring Exchange Impersonation
- ApplicationImpersonation Role

Alternative for Exchange 2010

For Exchange 2010, you may opt out of using the recommended option of impersonation by instead granting Full Access Permissions to all resource mailboxes for the service user and applying a throttling policy, both of which need to be performed at this stage. For instructions, see Appendix 1: Configuring Exchange 2010 Without Mailbox Impersonation, page 95. Even though this works, it is not recommended.

Preparing Resource Mailboxes with Delegates

Using delegates for room mailboxes is supported by Cisco TMSXE, but *not* when using Productivity Tools with Outlook.

Cisco TMSXE has been tested with the following three delegate setups:

- Email-based: a user or group is defined as a delegate for the resource mailbox, and invites are forwarded to the user. The delegate accepts or declines invites from their own mailbox.
- Calendar-based: a user or group is defined as a delegate for the resource mailbox with *Editor* permissions, and invites are forwarded to the user. The delegate accepts or declines invites directly in the resource calendar.
- Room administrator: a user is defined as a room administrator with a minimum of *Editor* access to the resource mailbox, granting them the permissions to edit existing meetings in the resource calendar, create new meetings directly in the calendar, and accept or decline new meeting invites.

Double-booking is not supported with Cisco TMSXE regardless of delegate setup.

Recommended settings for mailboxes with delegates and/or room administrators:

AutomateProcessing : AutoAccept

AllowConflicts : False

ForwardRequestsToDelegates : True

TentativePendingApproval : True

ResourceDelegates : (list of delegate users)

RequestOutOfPolicy : {}

AllRequestOutOfPolicy : False

BookInPolicy : {}

AllBookInPolicy : False

RequestInPolicy : {}

AllRequestInPolicy : True

Upgrading to Cisco TMSXE 5.10

Order of upgrading Cisco TMSXE and Cisco TMS

1. Stop Cisco TMSXE service on both nodes, if clustered.
2. Upgrade Cisco TMS environment
3. Upgrade Cisco TMSXE.

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.

  For information on monitoring re-replication, see Appendix 3: Monitoring Re-Replication When Upgrading from 3.0.x, page 99

- 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

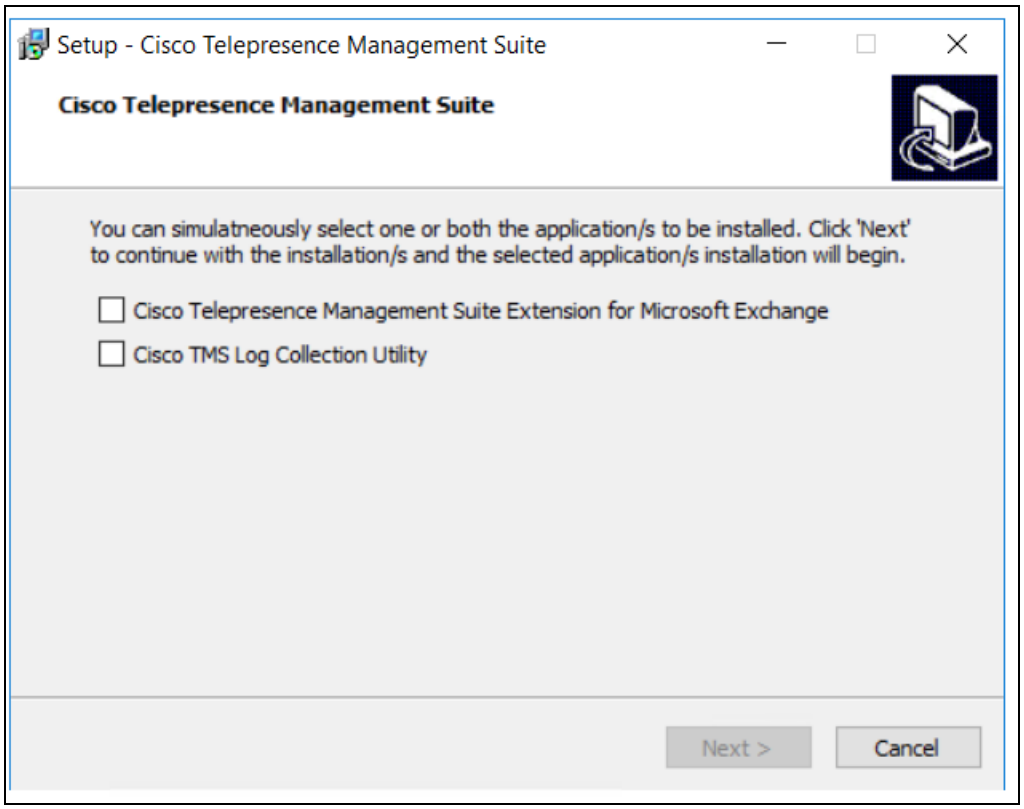
Make sure that:

- All Prerequisites, page 9 are met.
- You have considered all Best Practices for all Deployments, page 16.
- You have followed the steps in Backing Up and Upgrading the Backend, page 23.
- You are logged in as a local administrator on the Windows Server that will be hosting Cisco TMSXE.

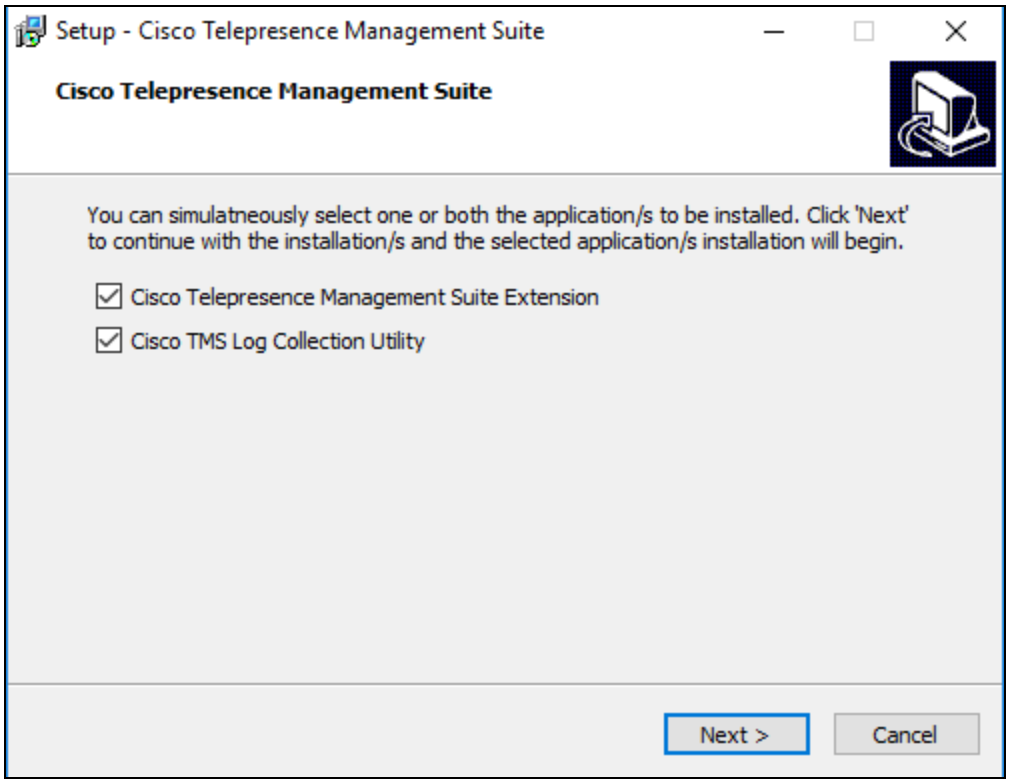
If you want to upgrade to a clustered deployment, see Installing Cisco TMSXE with Service Clustering, page 56.

Running the Installer

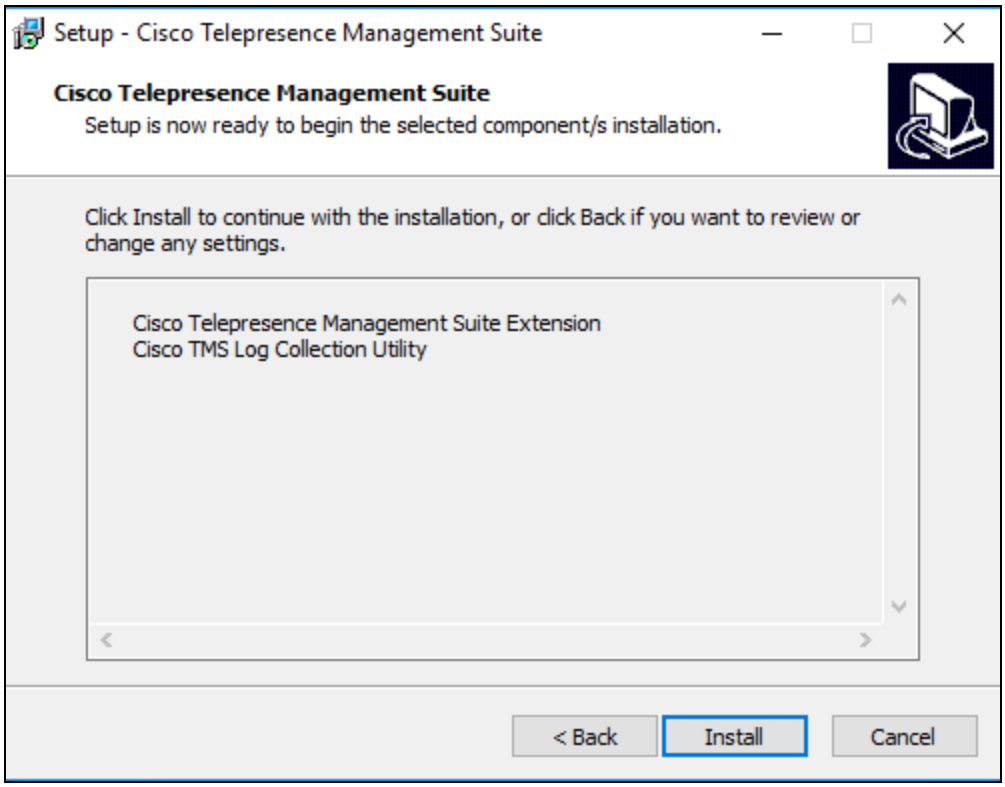
1. Disable anti virus software.
2. Stop the Cisco TMSXE Windows service, on both nodes if upgrading a clustered deployment.
3. Check Windows Update and install any critical updates to the .NET framework on the server or servers where Cisco TMSXE will be installed. Make sure all prerequisites are met. Reboot the server after installing if prompted.
4. Place the installation files on the server.
   a. Extract the **Cisco TMSXE.zip** archive to a folder.
   b. Run the **Cisco TMSXE** executable as an administrator.
   c. When the installer package is executed, a dialog box will appear which displays the following options:
      1. Cisco Telepresence Management Suite Extensions
      2. Cisco TMS Log Collection Utility



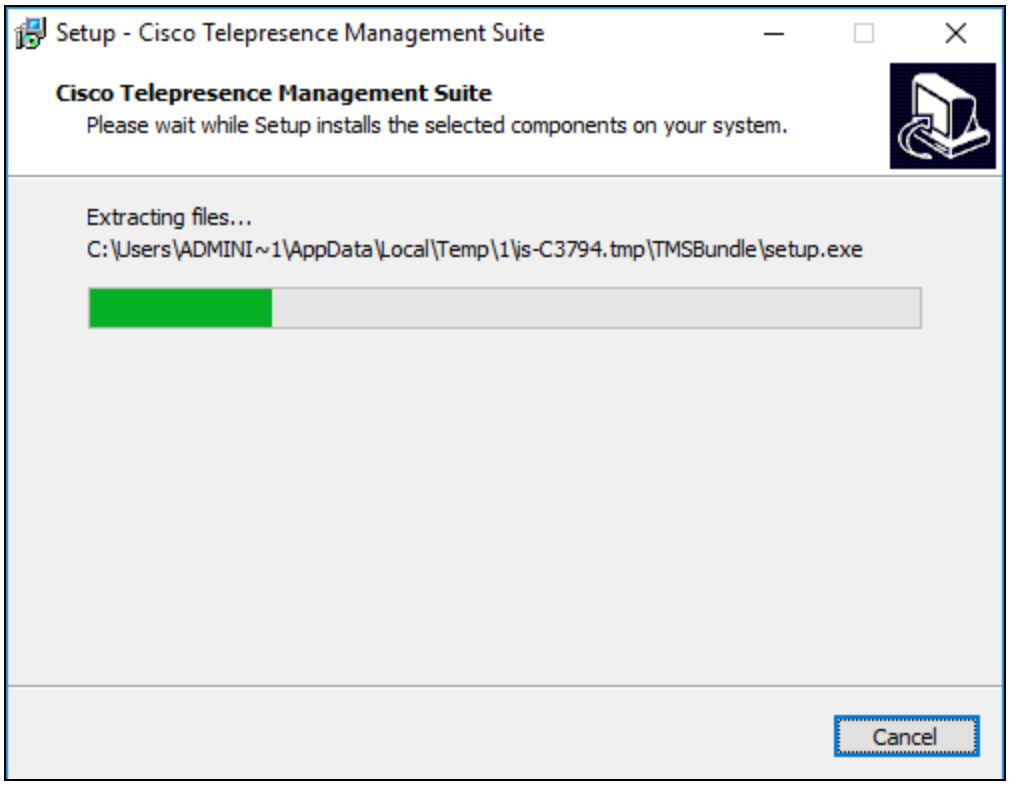
a. Select the application that you want to install and click '**Next**'.



b. Click **'Install'** to install the selected applications.



c. The installation will begin.



Note: If both options are selected, Cisco TMSXE will be installed followed by Cisco TMS Log Collection Utility installation.

5. In the Cisco TMSXE installer accept the End-User License Agreement (EULA) to start the installation process.
6. The installer will detect that you have a previous installation of Cisco TMSXE. Click **Upgrade** to continue.
7. Click **Next** to start the setup.
8. Accept the terms in the license agreement and click **Next**.

9. 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. See , page 1 for further information.
   - Cisco TMSXE Clustering is required if you want to set up Cisco TMSXE with redundancy. See Installing Cisco TMSXE with Service Clustering, page 56 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. The following table provides information about the performance counters and it's description.

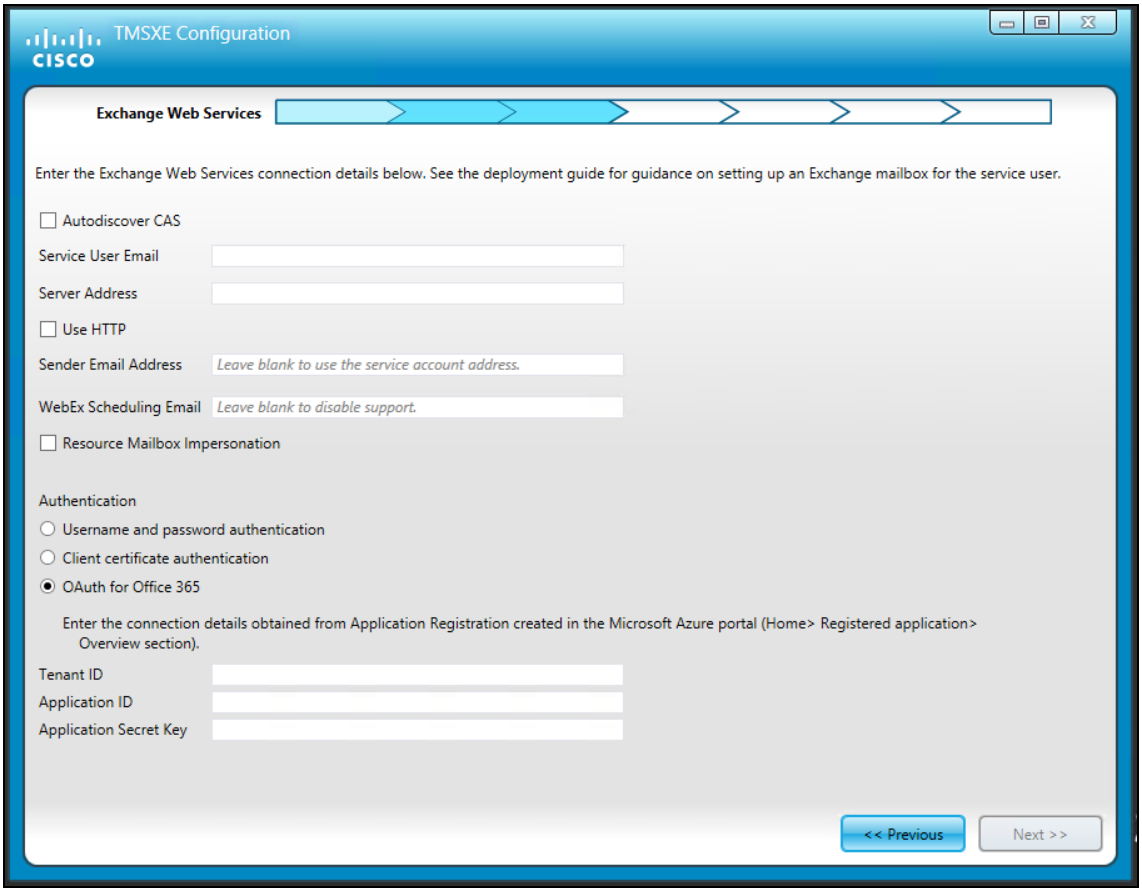
Performance Counters	Description
Active Conferences	Number of running Finite State Machines (FSM) in TMSXE
Conference Event Processors	Number of threads processing Exchange mail events
Conference Events Queued	Number of Exchange mail events waiting to be processed by TMSXE
Conference Processor Queue	Number of TMSXE threads for processing conference
EWSCallDuration	Total amount of time used by TMSXE for making EWS calls to Exchange server
EWSCallsPrSecond	Number of EWS calls made by TMSXE per second
EWSConcurrent	Constant, number of threads TMSXE uses to make EWS calls
EWSTimeSpent	Number of ticks spent by TMSXE making EWS calls since start of TMSXE process
Subscription Avg time between process	Average time between EWS subscription processed by TMSXE
Subscription NormalQueueLength	Length of normal queue for EWS subscription to be processed
Subscription PriorityQueueLength	Length of priority queue for EWS subscription to be processed
Subscription ProcessingQueueLength	Length of queue for EWS subscription waiting to be processed
Subscription with error	Number of EWS subscription with errors
TMSCallDuration	Total amount of time used by TMSXE for making TMS booking API calls
TMSCallsPrSecond	Number of Booking API calls made by TMSXE per second
TMSConcurrent	Constant, number of threads TMSXE uses to make TMS Booking API calls
TMSTimeSpent	Number of ticks spent by TMSXE making TMS Booking API calls since start of TMSXE process

10. 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.
11. When the upgrade is completed, click **Finish**.
12. The configuration tool launches.

13. Enable anti virus software.

Configuring Cisco TMSXE

1. Click through the configuration wizard, modifying settings and adding systems if needed.
2. All settings from the previous version are kept and will be re-validated as you click **Next**.
3. At the Exchange Web Services step, you may choose to configure new settings, such as:
   - Autodiscover CAS. Note that enabling this disables the Server Address field and relies on Autodiscovery being enabled in your Exchange environment.
   - Resource mailbox impersonation, which eliminates the need for full mailbox access.
   - WebEx Scheduling Mailbox.
   - OAuth for Office 365



4. Click **Finish** when all settings have been validated.

   A prompt will ask you whether you want to start the Cisco TMSXE service.

   - If upgrading a clustered deployment, decline, and repeat the above procedure for the second node before starting the service on both nodes.
   - If you decline, you must manually start the service when you are ready, following the instructions in Starting and Stopping the Cisco TMSXE Service, page 70.

Performing a New Installation

This section describes the required steps to install Cisco TMSXE 5.10 when no previous Cisco TMSXE deployment exists.

Before You Start

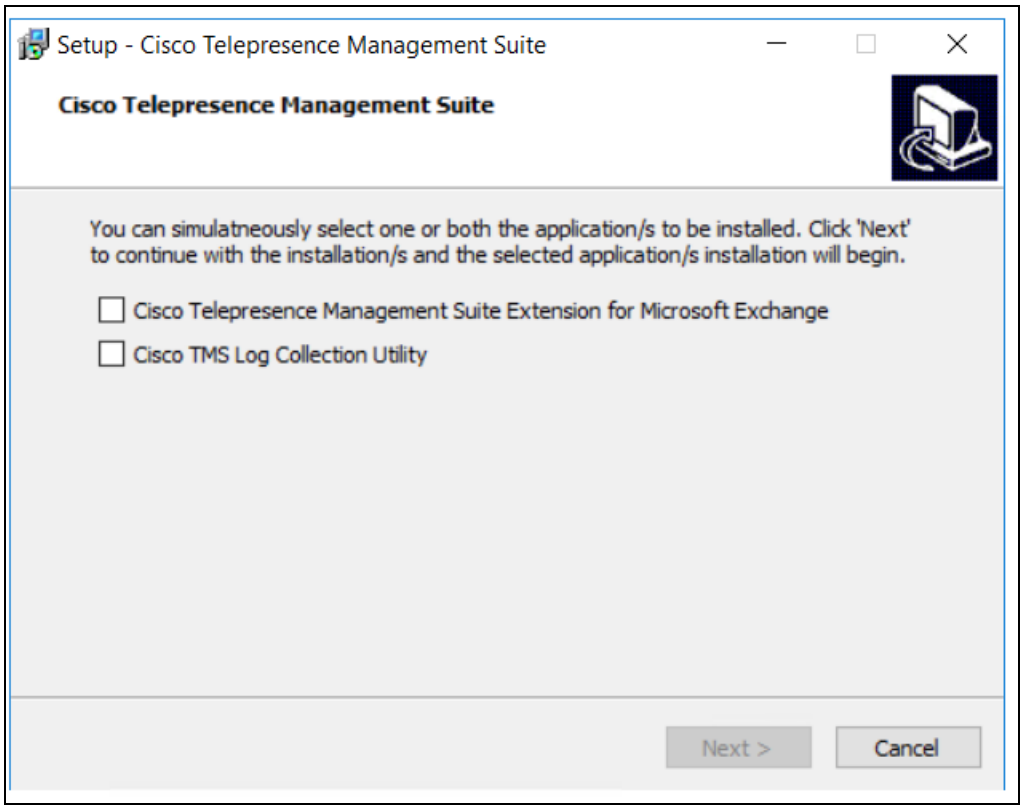
Make sure that:

- All Prerequisites, page 9 are met.
- You have considered Best Practices for all Deployments, page 16.
- You have completed all steps described in Preparing for a New Installation, page 23.
- You are logged in as a local administrator on the installing server.
- Ensure that .NET is a supported version

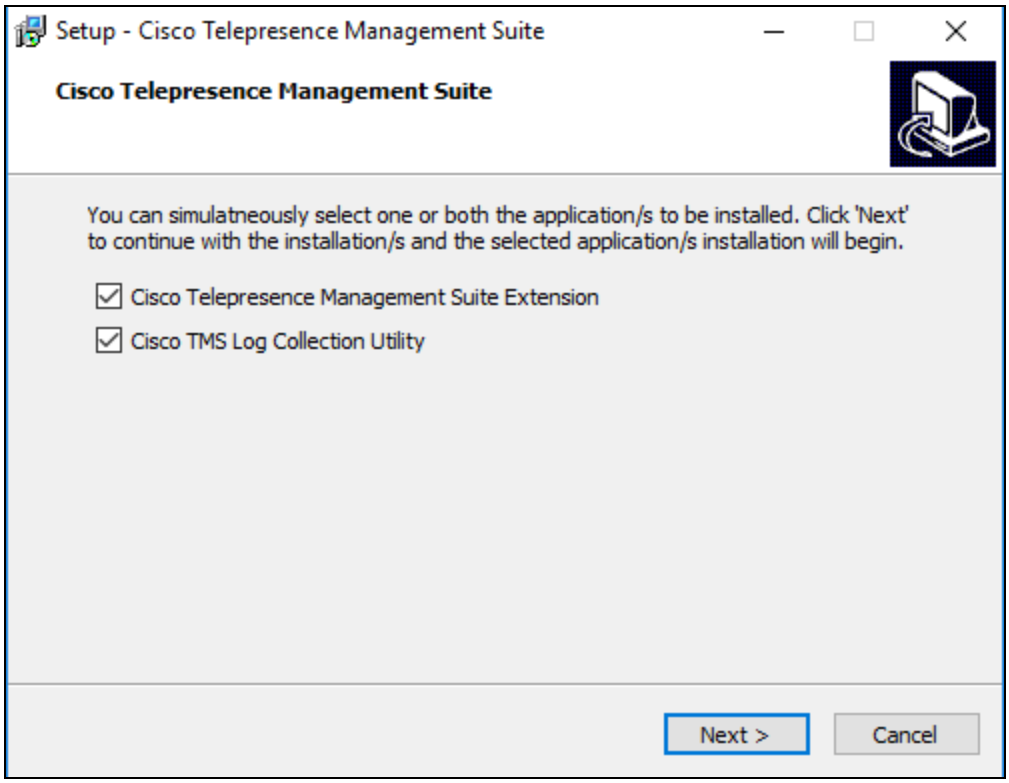
If you want to set up a clustered deployment, see Installing Cisco TMSXE with Service Clustering, page 56.

Running the Installer

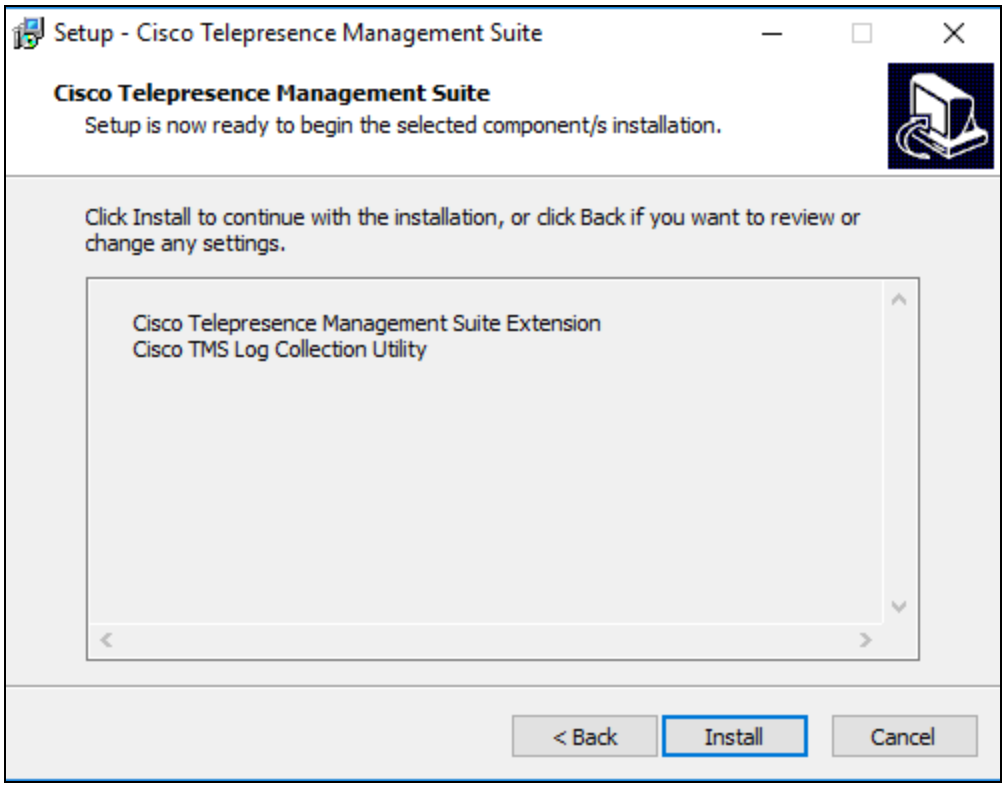
1. Check Windows Update and install any critical updates to the .NET framework on the server or servers where Cisco TMSXE will be installed. Make sure all prerequisites are met. Reboot the server after installing if prompted.
2. Place the installation files on the server.
    a. Extract the **Cisco TMSXE.zip** archive to a folder.
    b. Run the **Cisco TMSXE** executable as an administrator.
    c. When the installer package is executed, a dialog box will appear which displays the following options:
        1. Cisco Telepresence Management Suite Extensions
        2. Cisco TMS Log Collection Utility



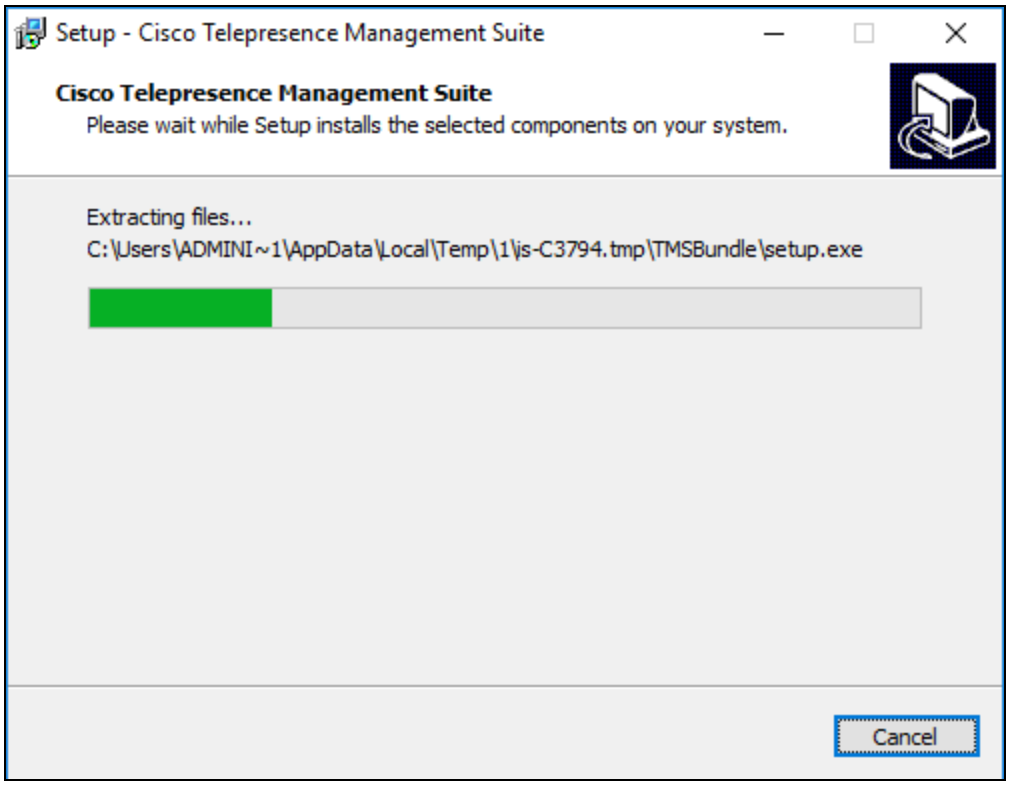
a. Select the application that you want to install and click '**Next**'.



b. Click **'Install'** to install the selected applications.



c. The installation will begin.



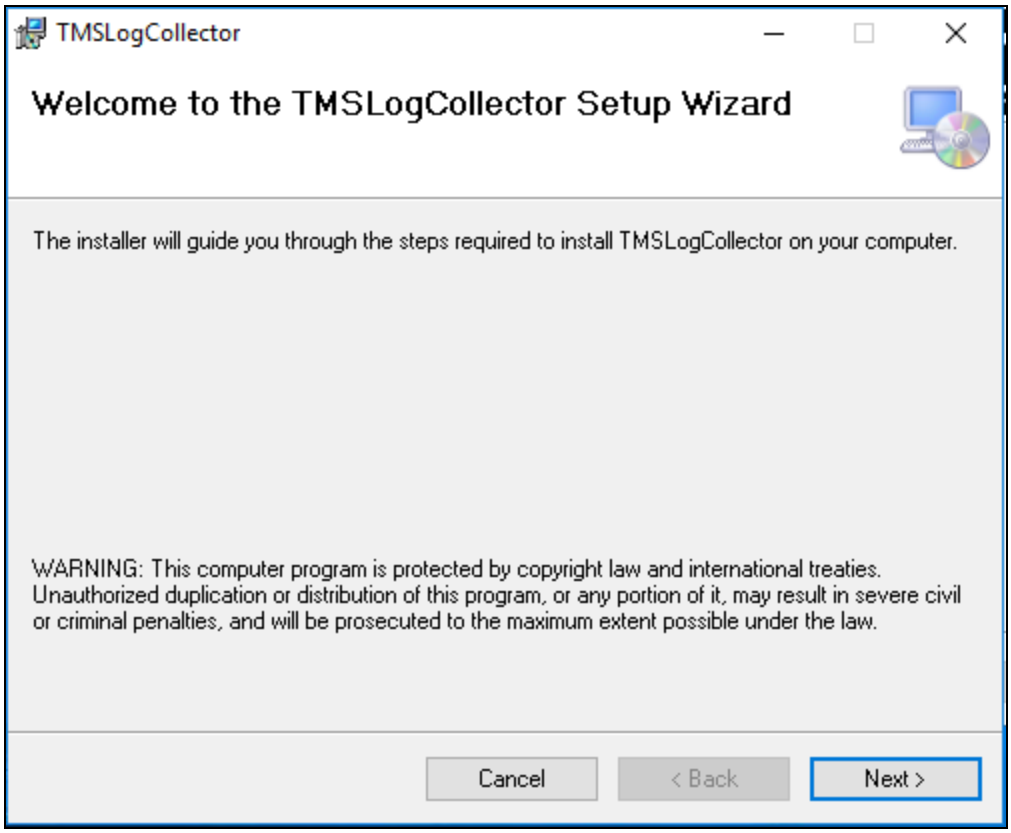
Note: If both options are selected, Cisco TMSXE will be installed followed by Cisco TMS Log Collection Utility installation.

3. In the Cisco TMSXE installer accept the End-User License Agreement (EULA) to start the installation process.
4. Select which components to include with your installation:
   - Cisco TMS Booking Service is required if you plan to use Webex Productivity Tools with TelePresence.

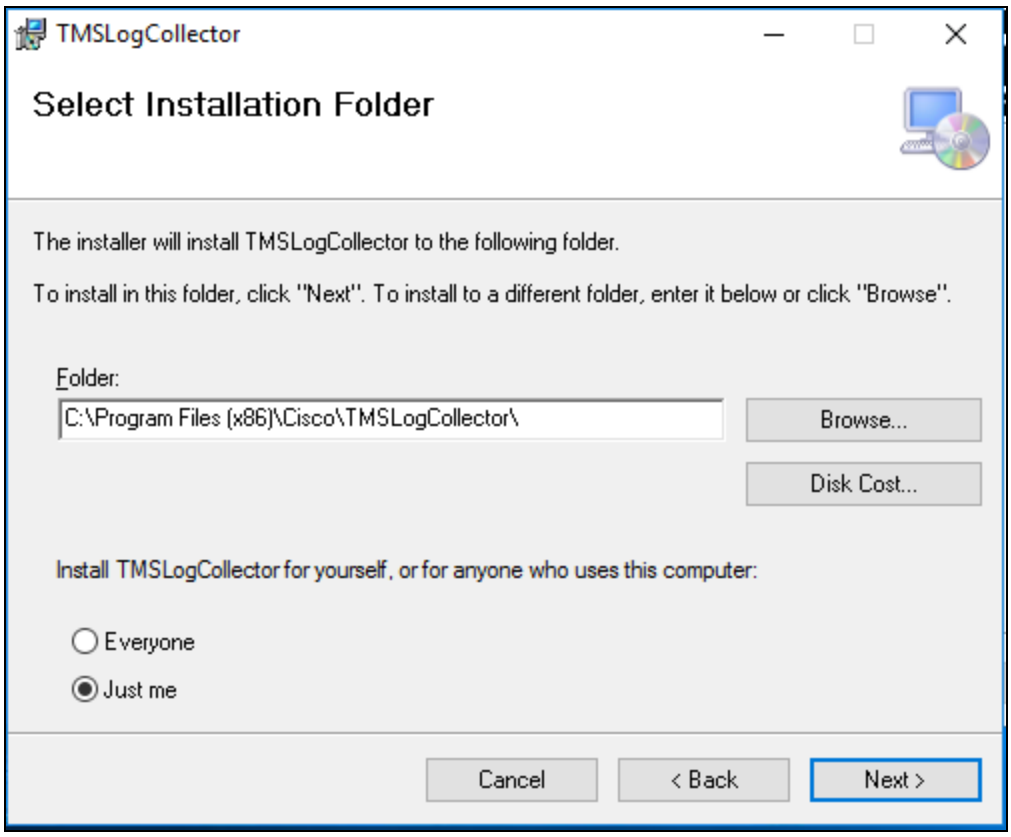
     If you enable this, you are prompted to modify or confirm the name of the IIS application pool to which you want Booking Service installed. See , page 1 for further information.
   - Cisco TMSXE Clustering is required if you want to set up Cisco TMSXE with redundancy. See Installing Cisco TMSXE with Service Clustering, page 56 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.
5. When you have selected the appropriate components for your deployment, click **Next**.
6. Click **Install**.
7. Click **Finish** when the installation is done to close the installer window and launch the Cisco TMSXE configuration tool.

Installing Cisco TMS Log Collection Utility

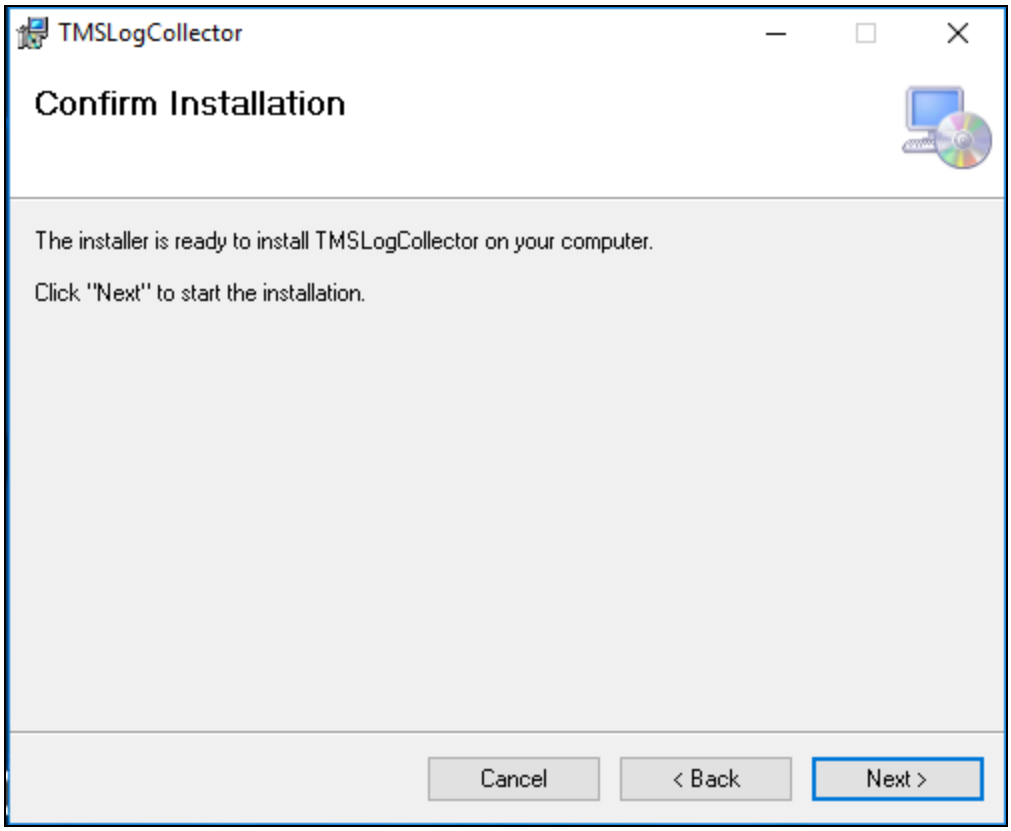
1. After Cisco TMS installation is completed, then Cisco TMS Log Collection Utility installation dialog box will be displayed. For more information on how to begin Cisco TMS Log Collection Utility installation, refer to **Step 4** in Performing a New Installation, page 35 section. Click **'Next'** to continue.



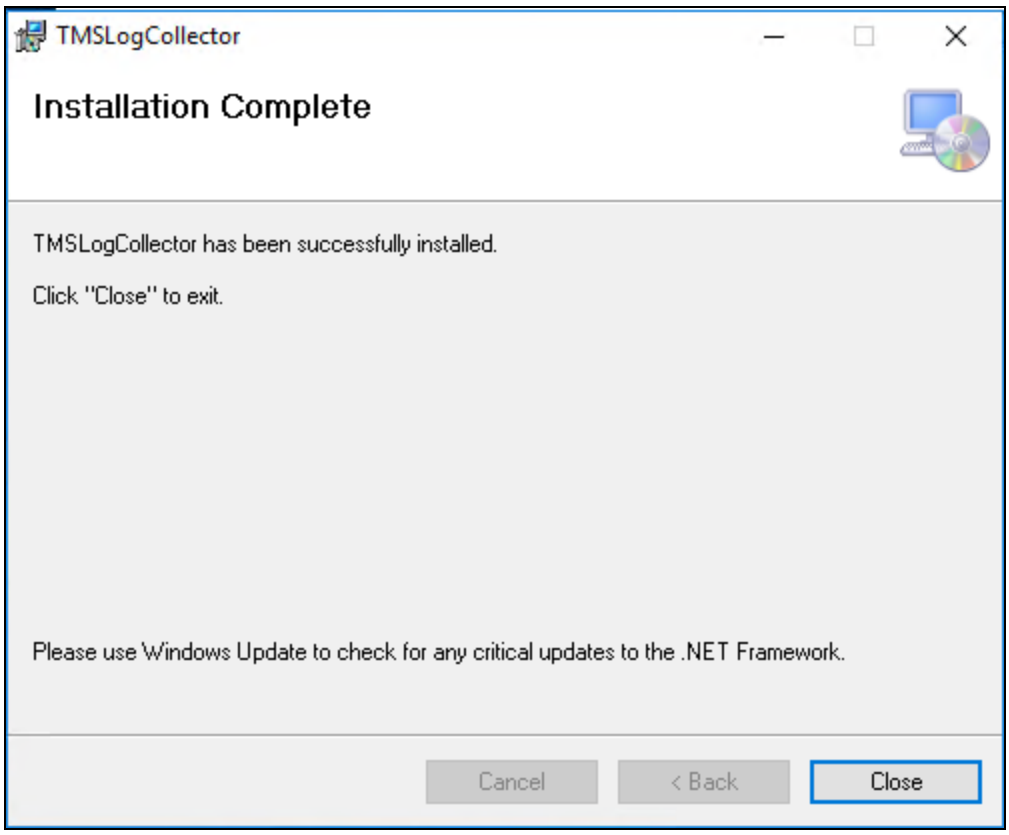
2. Browse to the directory/folder in which you want to install Cisco TMS Log Collection Utility. Select the option if you want to install Cisco TMS Log Collection Utility for self or for everyone. Click **'Next'** to continue

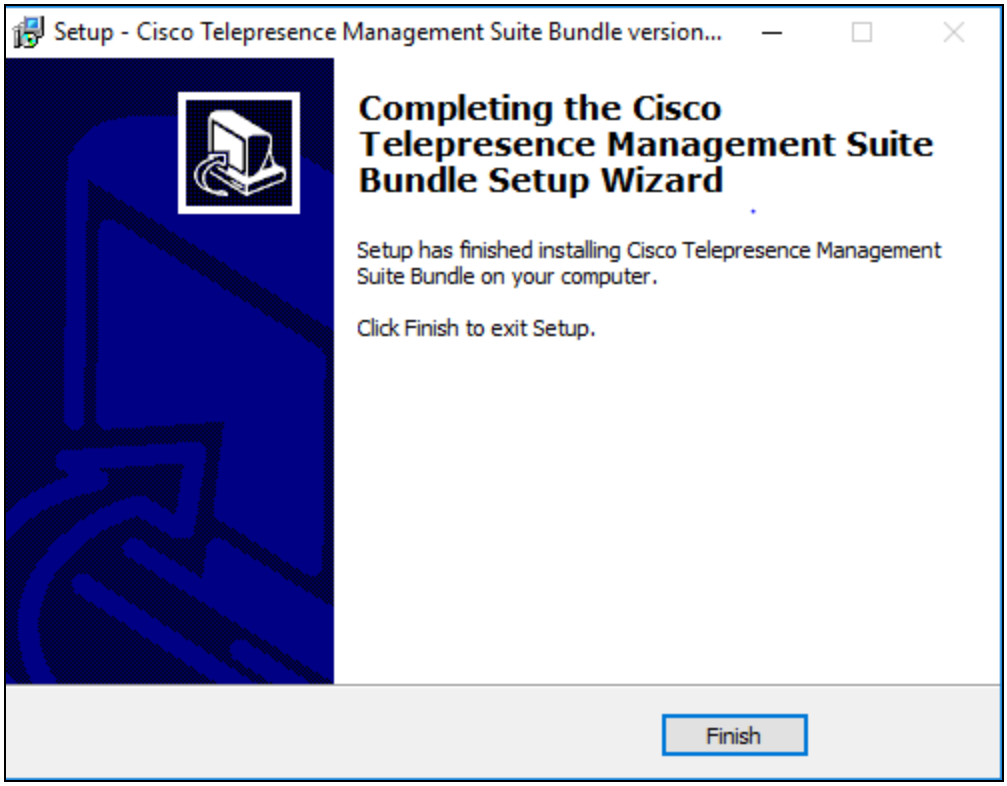


3. Click **'Next'** to start installation.

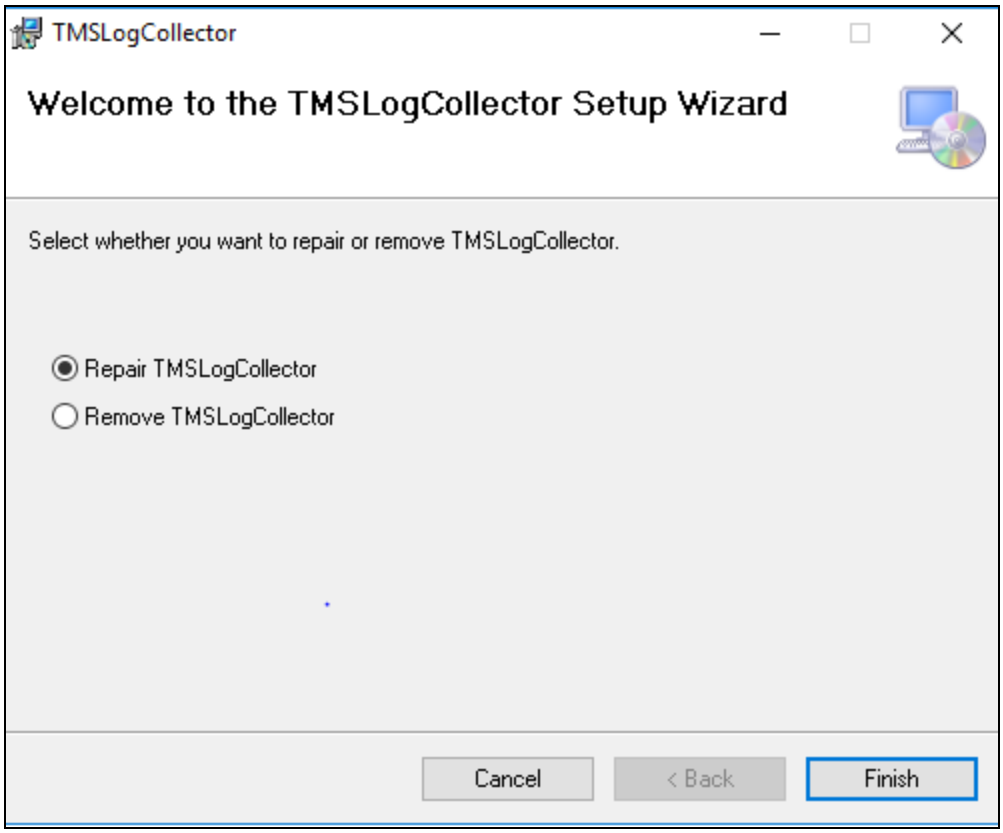


4. The installation will begin.
5. Once the installation is successfully completed, click **'Close'** to exit.


TMSLogCollector
Installation Complete
TMSLogCollector has been successfully installed.
Click "Close" to exit.
Please use Windows Update to check for any critical updates to the .NET Framework.
Cancel
< Back
Close


Setup - Cisco Telepresence Management Suite Bundle version...
Completing the Cisco Telepresence Management Suite Bundle Setup Wizard
Setup has finished installing Cisco Telepresence Management Suite Bundle on your computer.
Click Finish to exit Setup.
Finish

Note: When both the applications are already installed and user tries to run the installer package again, then Cisco TMSXE will work as per its original behavior. However for Cisco TMS Log Collection Utility, a dialog box will appear to Repair or to Remove Cisco TMS Log Collection Utility.



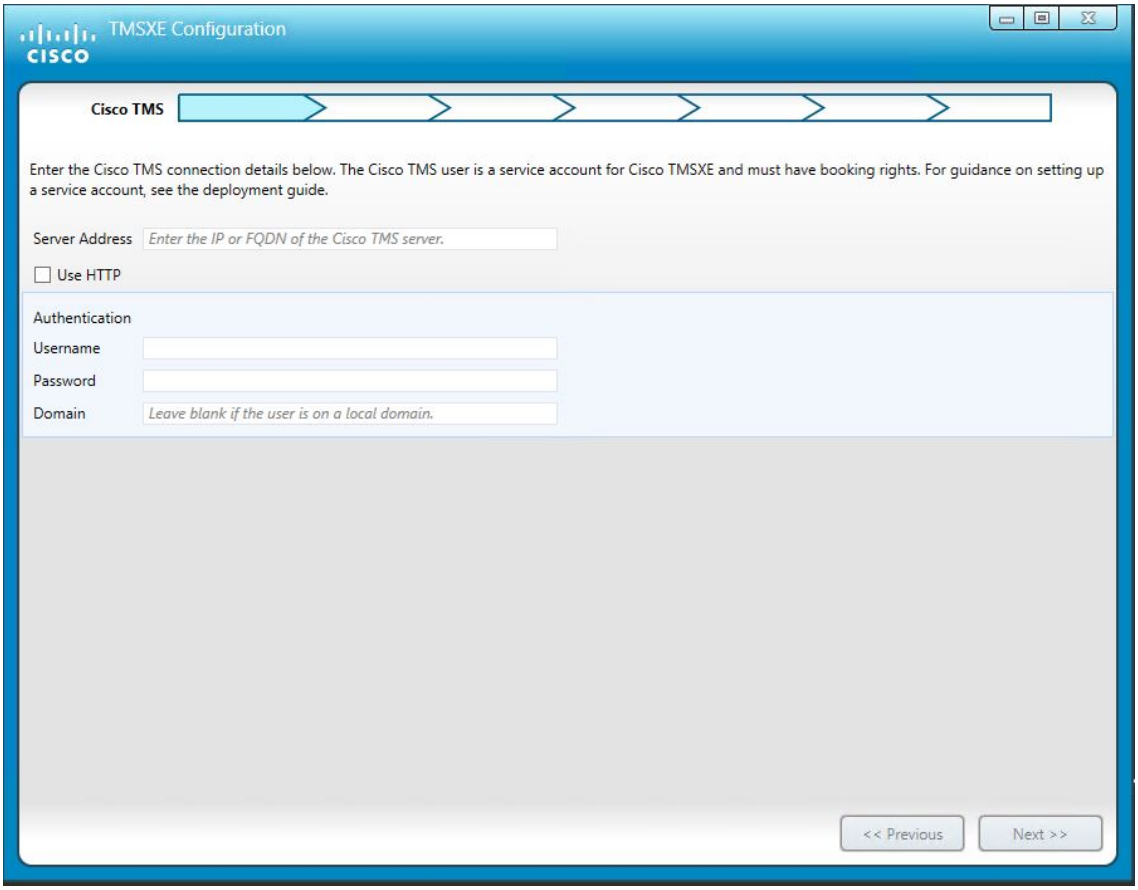
Configuring Cisco TMSXE

Most fields in the configuration tool are required. Clicking **Next** validates the settings provided for each step of the initial configuration. If one or more settings cannot be validated, you will be returned to the previous step to allow for corrections.

This procedure describes each step of the configuration process. For detail on each of the available fields, see the Configuration Reference, page 51 below.

1. Provide your Cisco TMS connection details on the first step, and determine how to authenticate.

   If you do not have Cisco TMS set up to use HTTPS, make sure to check *Use HTTP*.
   If you are using a redundant setup with a network load balancer for Cisco TMS, enter the virtual address of the network load balancer here.


TMSXE Configuration
cisco
Cisco TMS
Enter the Cisco TMS connection details below. The Cisco TMS user is a service account for Cisco TMSXE and must have booking rights. For guidance on setting up a service account, see the deployment guide.
Server Address
Enter the IP or FQDN of the Cisco TMS server.
Use HTTP
Authentication
Username
Password
Domain
Leave blank if the user is on a local domain.
<< Previous
Next >>

2. At the **Active Directory Settings** tab, you can select Mode from the **Mode Selection** section. By default, **Active Directory Mode (Recommended)** option is selected and it is also recommended. The **Allow organizers without Cisco TMS username (Non-Active Directory Mode only)** option has been moved from **Advanced Settings** tab to **Active Directory Settings** tab and this option is available only when the **Non-Active Directory Mode** is selected. The **Alternate Active Directory** for Organizer lookup option is available only if the **Active Directory Mode (Recommended)** is selected. Also, in **Alternate Active Directory for Organizer lookup**, if the Use **Alternate Active Directory** is selected, you will not be able to save the settings unless correct values are provided. When the Use **Alternate Active Directory** option is selected, it allows you to configure the details of the alternate directory like:
   - User name
   - Password
   - Domain
   - Global Catalog Server

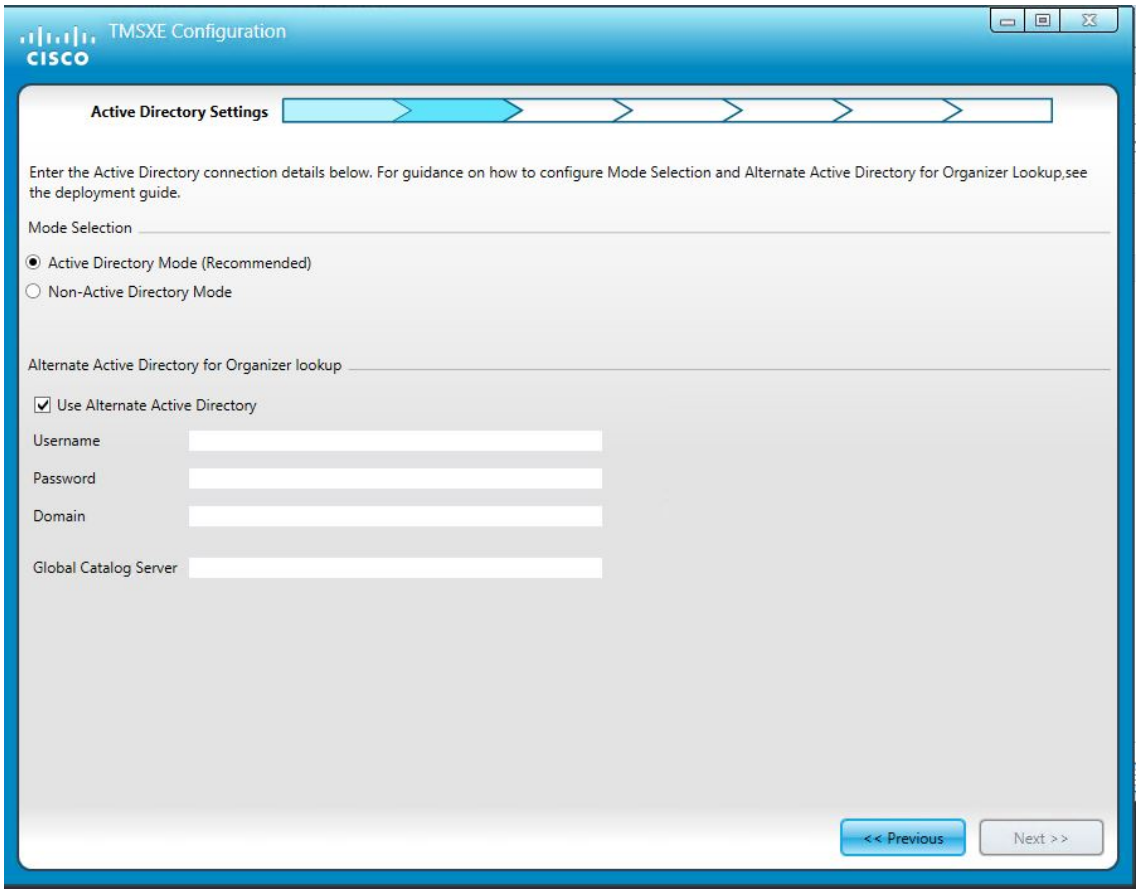
   Note: The Username and Domain field supports UPN and Pre-Windows 2000 (NetBIOS) format. The use of UPN or NetBIOS form of authentication is determined by the form used for the Domain setting. If a NETBIOS domain is used for the **Domain** field, credentials are sent in the form of **Domain\Username**. If an FQDN is used for the **Domain** field, the credentials are sent in the form of a **UPN, username@domain**.

   The preferred (and highly recommended) setting for the **Global Catalog Server** is the FQDN of the Active Directory Domain. If you want to point to a specific **Global Catalog Server**, use the FQDN of the server. The server does not support an FQDN that points to a network load balancer.

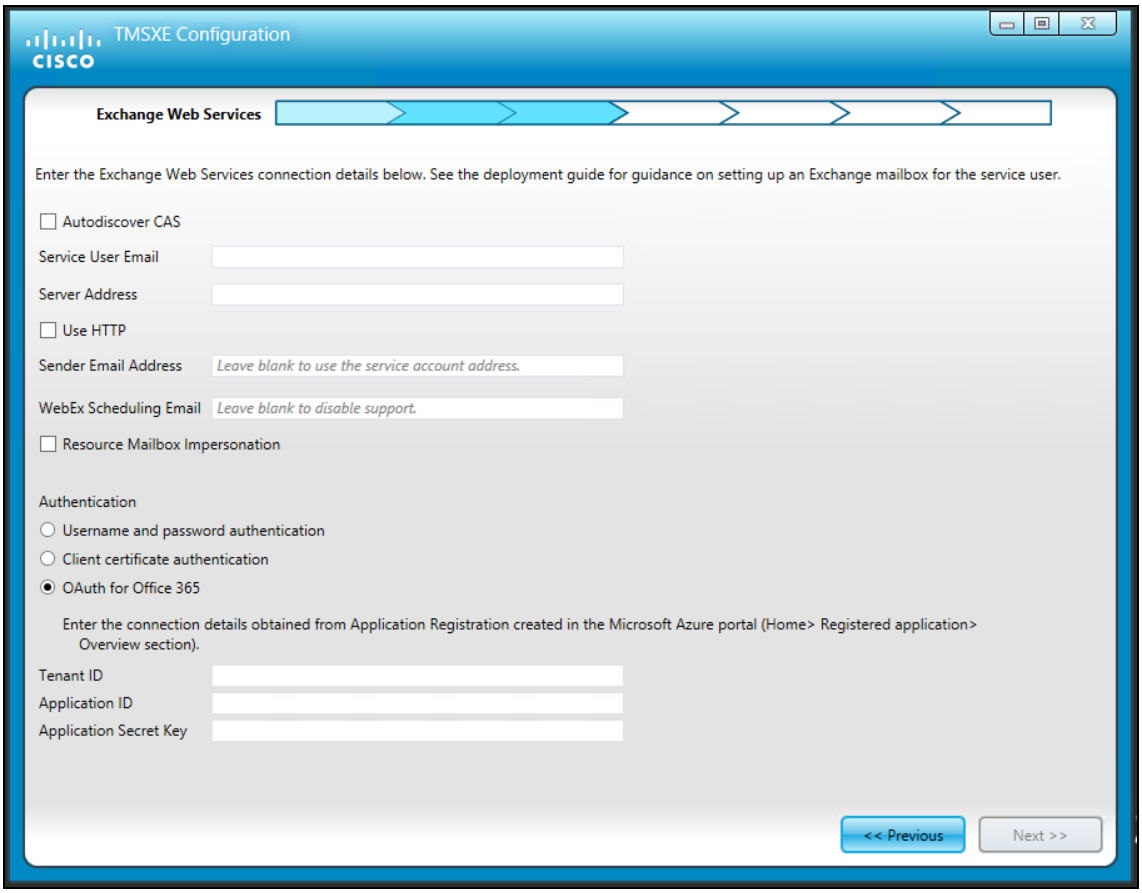
   The existing functionality of enabling **Non-Active Directory Mode** through command prompt can be performed in **Mode Selection** section of **Active Directory Settings** tab. Hence the dependency of enabling **Non-Active Directory Mode** through command prompt is removed.

   Use the **Alternate Directory Settings** option only when the authentication domain for the Microsoft Exchange deployment is different from the Active Directory FQDN. It is recommended that you use the **Alternate Directory Settings** option only when required.

   The limitation of **Alternate Directory Settings** is that when you use **Alternate Directory Settings**, the authentication against **Alternate Directory** to access **Alternate Directory** cannot be done with a certificate.


TMSXE Configuration
CISCO
Active Directory Settings
Enter the Active Directory connection details below. For guidance on how to configure Mode Selection and Alternate Active Directory for Organizer Lookup,see the deployment guide.
Mode Selection
Active Directory Mode (Recommended)
Non-Active Directory Mode
Alternate Active Directory for Organizer lookup
Use Alternate Active Directory
Username
Password
Domain
Global Catalog Server
<< Previous
Next >>

3. For Exchange Web Services, provide all connection details.
   - Enable **Autodiscover CAS** if this is set up for your environment, or include the address of your Exchange Client Access Server (CAS). This will disable the **Server Address** field.
   - Enable **Resource Mailbox Impersonation** if using impersonation for Exchange Web Services access. **Note**: It is mandatory to select this option in case of OAuth for Office 365.
   - You must also determine how to authenticate.



Click **Next** to submit your settings. Should the connection fail, you will be prompted with an option to view the Exchange Web Services (EWS) log to troubleshoot.

After viewing the log, close it and click **Return to Settings** to correct any errors and re-submit.

4. The Systems configuration step includes a list of all endpoints in Cisco TMS that are available for integration.

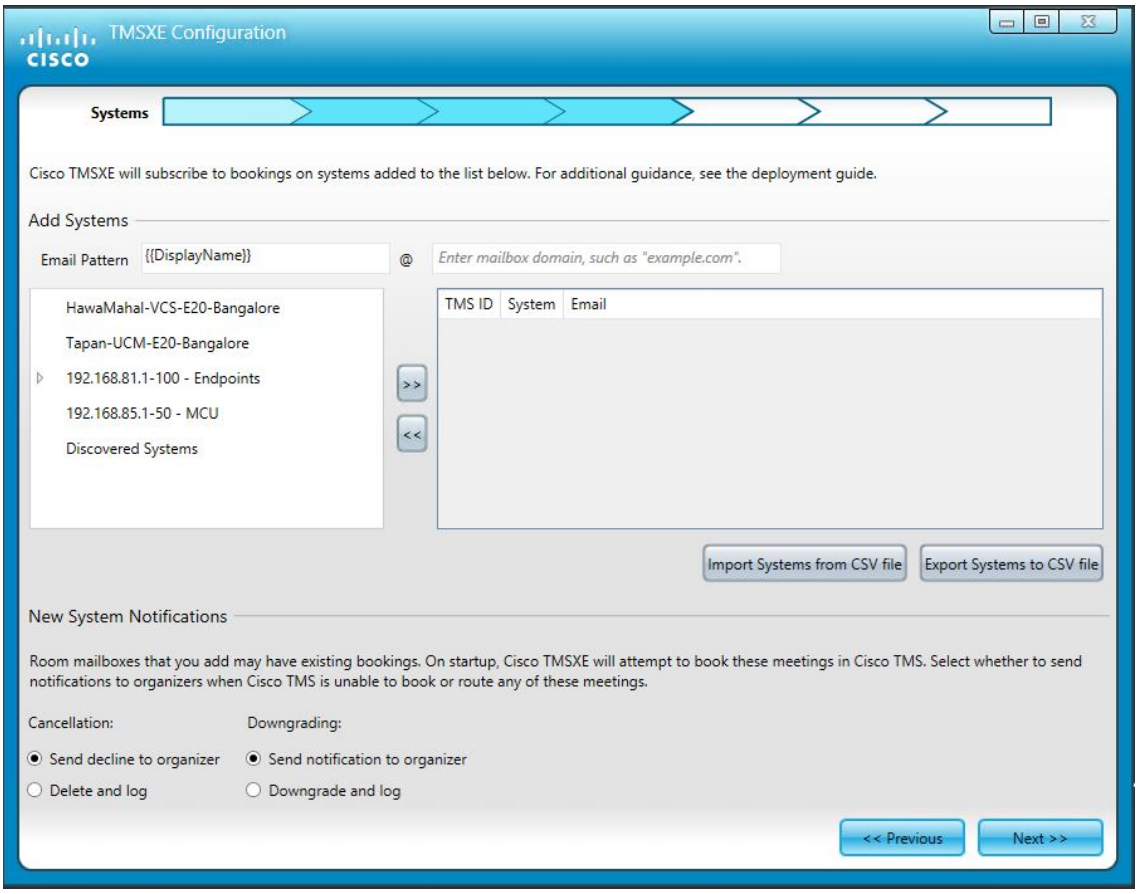
   Note that room mailboxes must already be available in Exchange, or validation of this step will fail. (See Creating Mailboxes for Cisco TMS Endpoints in Exchange, page 25.)

   To add systems to Cisco TMSXE, you can:

   - Import a list of mailboxes and systems from a .csv file that complies with the file format described in System Import and Export, page 53).
   - Add the systems one by one:
     1. Modify the email address pattern to generate the names of your room mailboxes. Use primary SMTP addresses for the room mailboxes, aliases are not supported. Two optional variables are available:
        - `{{TmsId}}` translates to the system's numeric system ID from Cisco TMS.
        - `{{DisplayName}}` translates to the system's display name in Cisco TMS. Note that any spaces in the display name will be removed automatically.
     2. Select endpoints in the left-hand list and click **>>** to add them to Cisco TMSXE. Use `Ctrl` or `Shift` to select multiple endpoints.
     3. Modify individual email addresses as needed by double-clicking on them after they have been added to the right-hand list.

   You must also choose whether to notify organizers during first-time replication between new mailboxes and systems. If there are conflicts or incompatibilities with Cisco TMS during first-time replication, Exchange bookings may be:

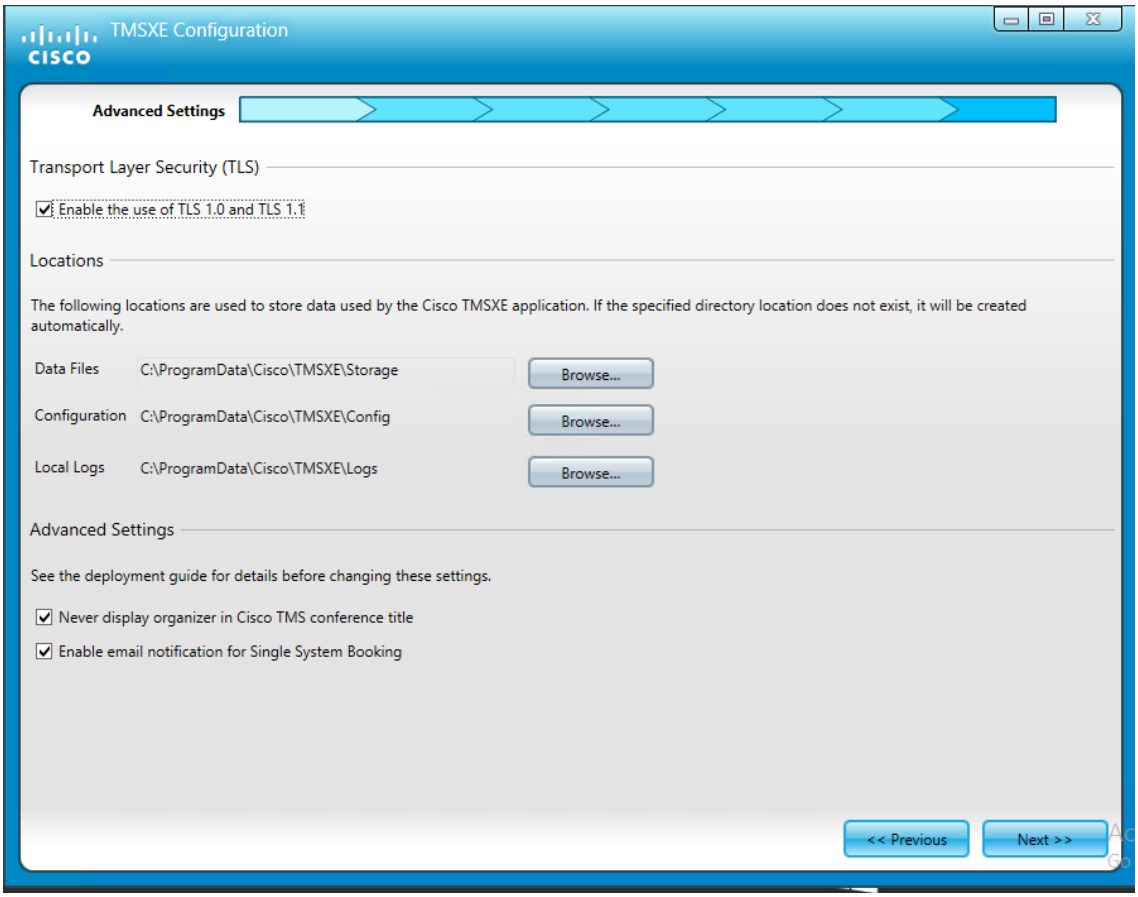
   - cancelled due to conflict or incompatibility
   - downgraded to *Reservation* with no routing due to conflict or incompatibility. For more information on downgraded meetings, see New System Notifications, page 54.



Click **Next** to proceed to validation of systems and mailboxes. Note that this may take a while if you have a large number of systems; for 250 endpoints, the process could take about 90 seconds.

5. Under Locations, confirm that you want to use the default folder locations for logs, data, and configuration files, or modify them as needed.

   If you have configured mailboxes to delete the subject and add the organizer's name to subject, determine how to handle the organizer's name, see Never Display Organizer in Cisco TMS Conference Title, page 55



6. A new check box **Enable email Notification for Single System Booking** has been added in the **Advance Settings** tab. You have to select it to receive an email confirmation for a single system booking.
7. The next step confirms that the configuration process is completed. Click **Finish**. A prompt will ask you whether you want to start the Cisco TMSXE service.
8. Starting the service will initiate first-time replication between Cisco TMS and Cisco TMSXE.
   - Start the service immediately only if configuration of all added systems is completed in Cisco TMS, and you have a maintenance window, as Cisco TMS performance will be impacted during replication.
   - Decline if you are not ready to start the service at this point, and follow the instructions in Starting and Stopping the Cisco TMSXE Service, page 70 when you are ready to start Cisco TMSXE.

If any validation steps fail during the configuration process, see the section Errors During Configuration, page 86.

Configuration Reference

Table 5 Configuration Tool Field Reference

Field	Description
Cisco TMS	
Server Address	This is the IP address or fully qualified domain name (FQDN) for the Cisco TMS server. Do not include the protocol (HTTP or HTTPS). A colon and specific port number may be included. If using a secure connection with certificates, you must provide the FQDN. If you are using a redundant setup with a network load balancer for Cisco TMS, enter the virtual address of the network load balancer here.
Use HTTP	In communication with Cisco TMS, encryption is used by default. This option disables secure communication with Cisco TMS.
Username	The username you have created for the Cisco TMSXE service user to log into Cisco TMS. For more information, see Creating a Cisco TMSXE Service User in Active Directory, page 23.
Password	The password for the above user.
Domain	The authentication domain for the user being used to access Cisco TMS.
Active Directory Settings	
Mode Selection	Select **Active Directory Mode (Recommended)** or **Non-Active Directory Mode**.
Alternate Active Directory for Organizer lookup	The **Alternate Active Directory for Organizer lookup** option is available only if the **Active Directory Mode (Recommended)** is selected. In **Alternate Active Directory for Organizer lookup**, if the **Use Alternate Active Directory** is selected, you will not be able to save the settings unless correct values are provided. We recommend to use the **Alternate Directory Settings** tab when OAuth for Office 365 is configured on Cisco TMSXE. If **Use Alternate Active Directory** option is selected, it allows you to configure the details of the alternate directory like: ■ **Username**–The Active Directory user. ■ **Password**–The password for the above user. ■ **Domain**–The authentication domain for the user being used to access **Active Directory**. ■ **Global Catalog Server**–The global catalog server for the above domain. Note: For the **Global Catalog Server**, the preferred value is the FQDN of the Active Directory Domain because the **Global Catalog Server** is first attempted to be identified and reached using **Global Catalog SRV DNS** records. An FQDN of a specific Global Catalog Server can be used, but it is not preferred. If a specific server FQDN is used, then it must be an individual server.
Exchange Web Services Active Directory Settings	
CAS Autodisover	This option relies on the Autodiscover service in MS Exchange to be functional for the SMTP domains used within Cisco TMSXE.

Table 5 Configuration Tool Field Reference (continued)

Field	Description
Service User Email	If using the autodiscover feature, provide the full email address of the Cisco TMSXE service user. See Creating a Cisco TMSXE Service User in Active Directory, page 23.
Server Address	If not using the Autodiscover feature, provide the address of the Exchange Client Access Server (CAS), entered as a fully qualified domain name (FQDN). ■ Do not include the protocol (HTTP or HTTPS). ■ A colon and specific port number may be included.
Use HTTP	In communication with Exchange Web Services, encryption is used by default. This option disables secure communication with EWS.
Sender Email Address	The email address used as the **From:** address of all notifications to organizers booking through Cisco TMSXE. Leave blank to use the Cisco TMSXE service user email address. If you want organizers to receive notifications from an address they can reply to, a support email address or similar can be added here. Note that you must grant the service user *Send as* permissions for this address, see: ■ Office 365: *Manage Permissions for Recipients* ■ Exchange 2016: *Add-ADPermission* ■ Exchange 2013: *Add-ADPermission* ■ Exchange 2010: *Manage Send As Permissions for a Mailbox*
WebEx Scheduling Email	The address of the WebEx Scheduling Mailbox. For more information, see Scheduling Mailbox, page 61.
Resource Mailbox Impersonation	Specify whether to make the Cisco TMSXE service user impersonate room mailboxes when contacting Exchange, to avoid throttling issues due to a high number of calls from one account. This setting is required for Office 365 and recommended for Exchange 2016, 2013 and 2010. Note: ■ On Exchange 2010, you can opt to apply a throttling policy instead, see Appendix 1: Configuring Exchange 2010 Without Mailbox Impersonation, page 95.
Username and password authentication	Authenticate with the username and password of the service user created in Exchange/Active Directory, see Creating a Cisco TMSXE Service User in Active Directory, page 23. ■ **Username**–The Cisco TMSXE service user in Exchange/Active Directory. ■ **Password**–The password for the above user. ■ **Domain**–The authentication domain for the user being used to access EWS.
Client certificate authentication	Authenticate with a client certificate and password. ■ **Certificate**–Browse for the client certificate to use for authentication with Exchange. For prerequisites for using this authentication mode, see Certificate Authentication, page 14. ■ **Password**–The password for the above certificate.

Table 5 Configuration Tool Field Reference (continued)

Field	Description
OAuth for Office 365	Authenticate connection details obtained from Application Registration in the Microsoft Azure portal. ■ **Tenant ID**: ID representing an organization within Azure Active Directory (AAD) in which you have created the application. ■ **Application ID**: GUID that uniquely identifies your application registered in AAD ■ **Application Secret Key**: The secret key that the application uses to prove its identity when requesting a token. For more information on registering Cisco TMSXE application in Microsoft Azure Active Directory, refer to **Appendix 6: Application Registration in the Microsoft Azure Portal, page 102**
Systems	
Email Pattern	■ When building the email pattern, the optional variables **{{TmsId}}** and **{{DisplayName}}** translate to the endpoint's **TMS System ID** and **Display Name** in Cisco TMS respectively. Any whitespaces in the display name will be removed automatically. ■ To simplify setup when there are many systems to add, using the Cisco TMS display name as the mailbox name is therefore recommended. For instructions, see Creating Mailboxes for Cisco TMS Endpoints in Exchange, page 25. ■ The email domain defaults to your domain. ■ If the mailbox names in your organization cannot be represented by such a pattern, each email address can be edited manually after they have been added to the right-hand list on this configuration tab.
System Import and Export	Instead of adding mailboxes one by one to the list, you may import a comma-separated list of mailboxes and the Cisco TMS systems you want to associate them with. The list must be stored as a .csv file, and the valid format is the following, where the header row and **System Name** field are optional, and the second row contains example values: **TMS ID, System Name,Email** **42,Meeting Room 1,meetingroom1@example.com** You can also export a list of already-added systems in the same format.

Table 5 Configuration Tool Field Reference (continued)

Field	Description
New System Notifications	When adding existing room mailboxes to Cisco TMSXE, their calendars may already contain future bookings. On addition, Cisco TMSXE will perform a two-way synchronization, attempting to book all existing meetings from the Exchange mailbox in Cisco TMS and replicating any existing bookings for the associated system in Cisco TMS to Exchange. When a booking is incompatible during synchronization with Cisco TMS, Exchange bookings will be declined and Cisco TMS bookings preferred where they exist. You can opt to: ■ *Send decline to organizer*–the meeting owner receives notification that the meeting has been declined by Cisco TMS. ■ *Delete and log*–the meeting is silently declined, but the administrator can find the declined meetings in the Cisco TMSXE log. In the event of routing problems or certain other issues with the synchronized meeting, Cisco TMSXE can "downgrade" a meeting to the *Reservation* type, where no automatic call setup is performed and routing resources are not reserved. Similar to declines, you can select whether to notify the meeting organizer or silently downgrade the meeting and log it. For more information about downgrading of meetings, see Messages from Cisco TMSXE, page 74.

Table 5 Configuration Tool Field Reference (continued)

Field	Description
Advanced Settings	
Data Files	Cisco TMSXE stores files at these default locations on the drive where Cisco TMSXE is installed (usually C:): ■ \ProgramData\Cisco\TMSXE\Storage for data files ■ \ProgramData\Cisco\TMSXE\Config for configuration files ■ \ProgramData\Cisco\TMSXE\Logs for error and event logs The ProgramData Windows folder is hidden by default and located on the drive where Cisco TMSXE is installed. When configuring a Cisco TMSXE cluster, there will be four fields:
Configuration	■ **Shared Data Files** ■ **Shared Configuration** ■ **Local Configuration** ■ **Local Logs** Shared Data Files and Shared Configuration must be changed to point to network shares where all nodes have read/write access. **Local Configuration** contains username and password data that can only be decrypted on the local server and must not be shared between nodes. Local Logs may point to a network share, but each node *must* have a separate folder for logs.
Logs	Room mailbox configuration (Calendar settings) from Exchange server are fetched in a .CSV file (The .CSV file name is 'MonitoredMailboxCalendarProperties.CSV'). In standalone mode, the .CSV file is available in 'Configuration' folder. In cluster mode, the .CSV file is available in 'Shared Configuration' folder. The .CSV file is available after the configuration settings are saved. This file is updated on every successful **Save** operation. **Note**: If the values of 'RequestOutOfPolicy', 'BookInPolicy', 'RequestInPolicy', 'AdditionalResponse' settings have special characters like Carriage Return (CR), Line Field (LF) and ',' then Cisco TMSXE removes CR, replaces LF with " " and ',' with ' ;' in the .CSV file. This allows the .CSV file to be parsed in a simple manner. For example, opening the .CSV file with Microsoft Excel.
Never Display Organizer in Cisco TMS Conference Title	When a resource mailbox is set to both **Delete Subject** and **Add Organizer to Subject**, enabling this setting keeps the subject for the meeting entirely blank.
Enable email Notification for Single System Booking	A check box **Enable email Notification for Single System Booking** has been added in the **Advance Settings** tab. You have to select it to receive an email confirmation for a single system booking.

Setting Up a Redundant Deployment

Cisco TMSXE clustering provides active/passive redundancy for the Cisco TMSXE service.

This section provides instructions for setting up redundance for Cisco TMSXE . For an overview of supported scenarios and how redundancy works, see Redundant Deployments, page 15.

Limitations

- Redundancy is not supported for small deployments where Cisco TMSXE resides on the Cisco TMS server.

Installing Cisco TMSXE with Service Clustering

During installation or upgrade, you can choose whether to implement active/passive redundancy for Cisco TMSXE by enabling cluster support.

Before You Start

Ensure that both servers meet the Cisco TMSXE Server Software Requirements, page 11 and are ready for installation.

You can upgrade from an existing, non-clustered installation to a clustered one, provided the following:

- The first node is running a stand alone deployment of a supported version of Cisco TMSXE.
- The second node does not have any Cisco TMSXE application or data files on it prior to installation. For instructions on complete removal of Cisco TMSXE from a server, see Uninstalling Cisco TMSXE, page 76.

Setting Up a Network Share for Cluster Configuration

Before installing Cisco TMSXE with clustering, you must make a network share available that has read and write access for both nodes and the user that will configure Cisco TMSXE.

- The share and both nodes must be members of an Active Directory domain where sharing with machine accounts is possible.
- The accounts must have file share permissions and file permissions to the folder.
- You must *not* locate the network share on either of the nodes, or use a mapped drive letter.

Note that while you may opt to place the log folder on a network share, each Cisco TMSXE node *must* have a separate log location. The log level is part of the shared configuration.

Example Setup

In this example on a Windows Server 2012 R2 installation, the configuration will be stored on the server **filestore.example.com**, while the nodes where Cisco TMSXE will be installed are **tmsxe1.example.com** and **tmsxe2.example.com**. The administrator performing the installation is a domain user named **tmsxeadmin**.

Creating a folder and editing file share permissions:

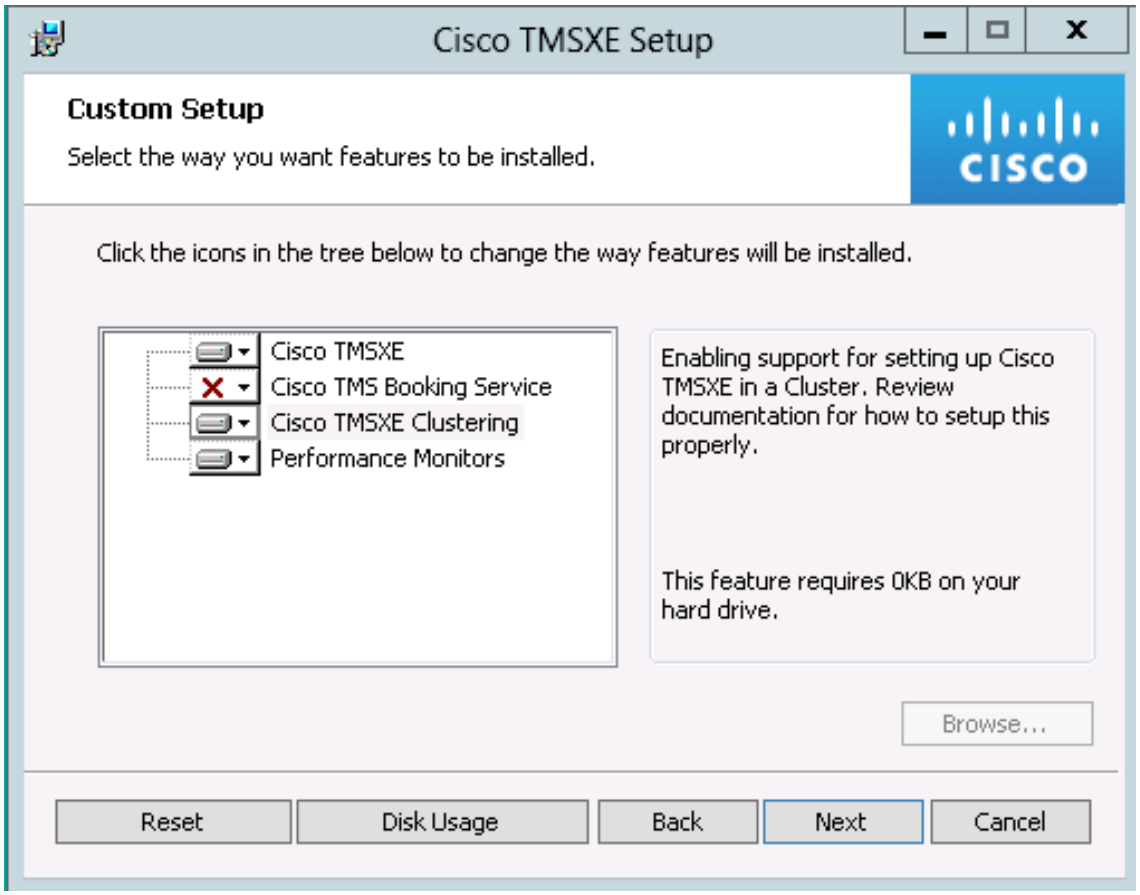
1. On **filestore.example.com**, create a folder tmsxeconfig.
2. To enable folder sharing, go to **Properties > Sharing > Advanced Sharing**.
3. Check **Share this Folder**.
4. Click **Permissions**.
5. Click **Add**, then **Object Types**, and make sure that **Computers** and **Users** are checked.
6. In the entry field for object names, enter **tmsxe1**, **tmsxe2**, and **tmsxeadmin**.
7. Click **OK**.
8. Select **tmsxe1** and set **Change** to *Allow*. Repeat for the remaining two accounts.
9. Click **OK**, then click **OK** again to exit the permissions for the file share.

Editing file permissions:

1. In **Properties > Security**, click **Edit**.
2. Click **Add**, then **Object Types**, and make sure that **Computers** and **Users** are checked.
3. In the entry field for object names, enter **tmsxe1**, **tmsxe2**, and **tmsxeadmin**.
4. Click **OK**.
5. Select **tmsxe1** and set **Modify** to *Allow*. Repeat for the remaining two accounts.
6. Click **OK**, then click **Close** to save the new settings.

Performing the Installations

For new installations and upgrades on both nodes, follow the instructions for running the installer, making sure to enable clustering.

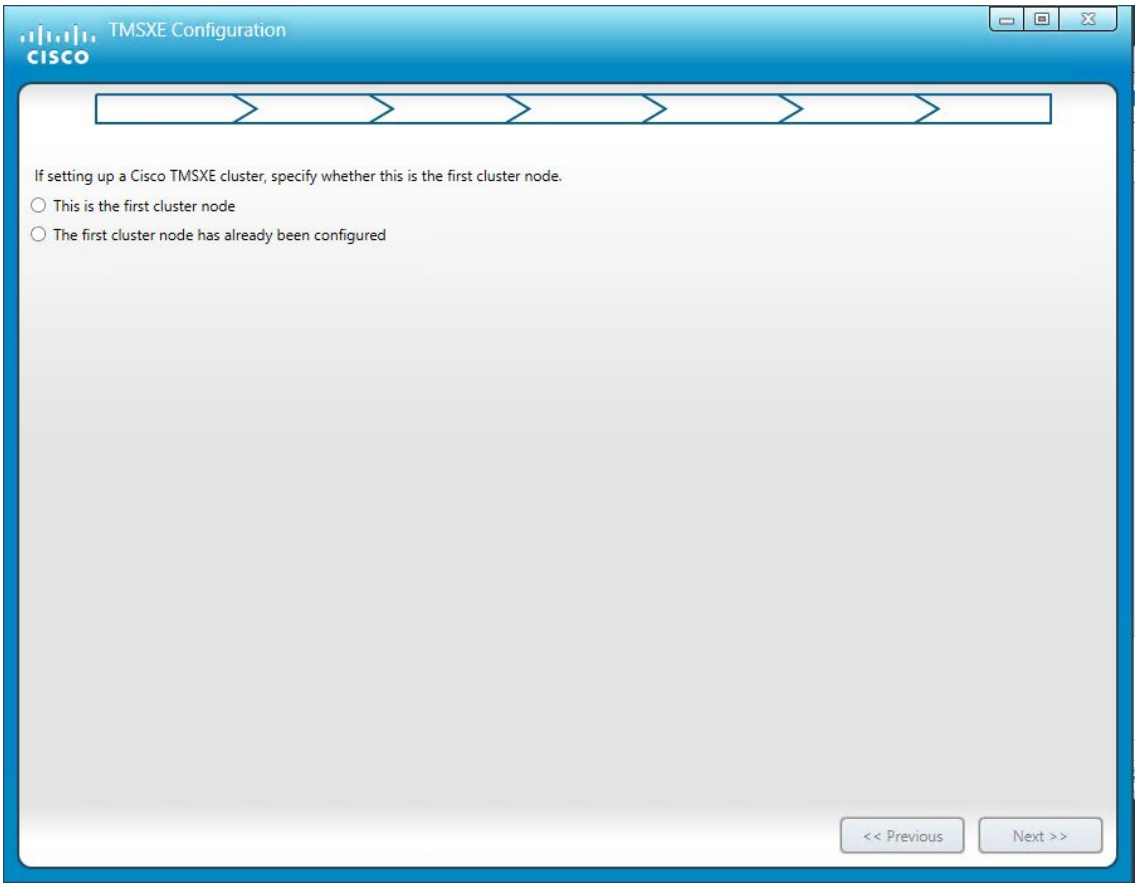


Configuring the First Node

When the configuration tool opens:

1. If this is a new installation, specify on the first step that this is the first node in the cluster.

   This configuration step will not be available if you are upgrading an existing installation.



2. Follow the instructions for configuring a regular installation as described in Configuring Cisco TMSXE, page 43, making sure to add a minimum of one system on the Systems tab.
3. On the Advanced Settings tab, change the folder locations for shared data and configuration files to be on a network share to which both nodes have read/write access, for example:

   \\server\share\Config

   - For a new installation, these location fields will be called **Shared Data Files** and **Shared Configuration**.
   - For an upgrade from a non-clustered deployment, the fields are called **Data Files** and **Configuration**.
   - **Local Configuration** contains usernames and passwords that can only be decrypted on the local server and must *not* be shared.
4. TMSXE Configuration tool creates folders in the Shared folder based on the names provided in Step 3. For example: **\\server\share\config** path in the shared configuration creates a folder in the shared location called "**config**" and automatically populates the files within that folder. Similarly, **\\server\share\storage** path in the shared storage creates a folder in the shared location called "**storage**" and copies all files to the storage folder automatically.
5. Click **Next** to proceed to validation of systems and mailboxes. Note that this may take a while if you have a large number of systems; for 250 endpoints, the process could take about 90 seconds.

Configuring the Second Node

Before configuring the second node, stop Cisco TMSXE service on first node. Perform the following steps when the configuration tool opens:

1. On the first tab, specify that the first node has already been configured.
2. Follow the instructions in step 2 in Configuring Cisco TMSXE, page 43
3. Provide the necessary Exchange connection details, which must be exactly the same as for the first node.

   Cisco TMSXE will use this detail to identify the primary node, and all configuration data that can be shared, will be imported and validated.

4. An overview of the imported data is displayed.
   - Red marks will be shown if some or all of the data could not be validated, with guidance on addressing the issues:
     1. Resolve any issues on the first node or with access to network shares.
     2. On this node, go back to the previous step, and re-validate the import.
   - When green checkmarks are shown, click **Next**.
5. Enter authentication details for Cisco TMS and Exchange.

   These need to be stored per server and cannot be imported.

6. Click **Next** to validate all settings.
7. Click **Save** to save the settings.
8. Start the Cisco TMSXE Service in first node and second node from the Windows Service.

Note: After all the fields have been validated in the **Exchange Settings** tab, then Cisco TMSXE Admin has to enter details in **Cisco TMS** tab and also in **Active Directory Settings** tab. Click **Next** to complete the validation for both the tabs.

Verifying the Cluster Setup

Using remote desktop, connect to one or both of the nodes and do one of the following:

- Start the configuration tool, and the first screen will include information about the current state of the cluster.
- Check TMSXE-log.txt, which includes information about which node is active and the state of the node you are connected to.

To test that failover is working:

1. Stop the Cisco TMSXE service on the active node.
2. Verify using the log or configuration tool on the second node that it has been promoted to active.

Changing the Configuration for an Existing Cluster

You can add and remove systems from the configuration tool while the Cisco TMS service is running in clustered mode. You cannot, however, replace a system while the service is running.

To make any other configuration changes, including replacing an existing system, you must stop the Cisco TMSXE service on both nodes before launching the configuration tool, and make the changes on both nodes before restarting the service. We recommend stopping the service on the passive node first.

Changing Credentials

We strongly recommend against changing the Exchange service user for a clustered deployment, as the cluster information is stored on the service user in Exchange, and adding a new service user to Cisco TMSXE will create a new cluster.

To change the password or the certificate for an existing user, this must always be done for both nodes in parallel.

Changing the Exchange or Cisco TMS Credentials

To avoid one node encountering a password error, we recommend turning off both nodes before making the change:

1. Turn off the service on the passive node.
2. Turn off the service on the active node.
3. Change the password for the service user in Active Directory.
4. Add new password using the configuration tool on the first node.
5. Add new password using the configuration tool on the second node.
6. Start service on first node.
7. Start service on second node.

Changing the Client Certificate

To update the client certificate to a new one that authenticates the same service user, typically because the old certificate is due to expire:

1. Turn off the service on the passive node.
2. Turn off the service on the second node.
3. Change the client certificate using the configuration tool on this node.
4. Change the client certificate using the configuration tool on the second node.
5. Start the service on this node.
6. Start the service on the second node.

Configuring Additional Features

When Cisco TMSXE is installed and configured, users will be able to book telepresence meetings from Outlook by adding telepresence-enabled rooms as locations for their meetings. The meetings will use default settings from Cisco TMS.

If you want users to be able to change certain settings on a per-meeting basis, include WebEx in their meeting, or schedule call-in and call-out participants, you must make additional features available to your users. The available options are described in this chapter.

Scheduling Mailbox

Scheduling Mailbox feature allows users to schedule a multi-point meeting without having to add Telepresence rooms directly. Microsoft Exchange/Office 365 administrator creates a special user or resource/room mailbox, that allows users to include Dial-ins/External participants to their meeting by adding this mailbox to their Outlook meeting request. Cisco TMSXE then adds the configured number of dial-in ports along with the protocol and dial-in type to the conference. The meeting confirmation email contains the dial-in information, which can then be shared with the intended participants. The email address of both the Scheduling Mailboxes must be unique and only be used for the Scheduling Mailbox feature.

Note: Scheduling Mailbox feature is recommended in Cisco TMSXE Active Directory mode. For the Scheduling Mailbox feature to work in Non-Active Directory mode, the 'scheduling mailboxes alias', 'display name', and 'user' part of the email address must be same.

Creating and Configuring Scheduling Mailboxes

Create and configure the mailbox using either Exchange Admin Center, Exchange Management Console, or Exchange Management Shell:

1. Create a new resource mailbox with the desired Scheduling Mailbox name. For instructions, see:
   - Exchange 2016, Office 365 and Exchange 2013: *Create and Manage Room Mailboxes*
   - Exchange 2010: *Create a Room or Equipment Mailbox*
2. If using Exchange 2010 without mailbox impersonation, you must give the Cisco TMSXE service user account Full Mailbox Access to this mailbox. For instructions, see:
   - Exchange 2010: *Allow Mailbox Access*
3. Modify the mailbox properties:
   a. Turn off the Calendar Attendant for the mailbox. For instructions, see:
      - Exchange 2016: *Set-CalendarProcessing*
      - Office 365 and Exchange 2013: *Set-CalendarProcessing*
      - Exchange 2010: *Configure User and Resource Mailbox Properties*
   b. Make sure new requests are not automatically marked as tentative by disabling **AddNewRequestsTentatively** (also known as **Mark new meeting requests as Tentative**) for the mailbox.
   c. Set **ForwardRequestsToDelegates** to *False*.
   d. For Office 365, Exchange 2016, Exchange 2013, and Exchange 2010: Set `CalendarRepairDisabled` to *True*.

A user mailbox with the above settings will still work with Exchange 2010, but not with Exchange 2016, Exchange 2013 and Office 365.

Shell Parameter	Required Value	Description
`AutomateProcessing`	*None*	Calendar processing is disabled on the mailbox.
`BookingWindowInDays`	Must be between 1 and 1080. See description for recommendation.	Specifies for how long into the future users will be allowed to schedule meetings. We strongly recommend that this setting match that of Cisco TMS: **Administrative Tools > Configuration > Conference Settings > Conference Create Options >Booking Window (in days)**.
`EnforceSchedulingHorizon`	*True*	Specifies that recurring meetings that continue outside of the booking window will be rejected.
`AllowConflicts`	*False*	Prevents the mailbox from accepting overlapping bookings, which is not supported by Cisco TMS.
`ConflictPercentageAllowed`		
`MaximumConflictInstances`		
`AddNewRequestsTentatively`	*False*	Specifies not to have the Calendar Attendant put new calendar items tentatively on the calendar.
`ForwardRequestsToDelegates`	*False*	
`CalendarRepairDisabled`	*True* (strongly recommended)	

Additional Recommendations

We also recommend the following configurations:

- Using Exchange Management Console **Mail Flow Settings** or Exchange Management Shell, stricten the message delivery restrictions as needed.

  For example, require senders to be authenticated, only allow from people in a specific group, or similar.

  For instructions, see:

  - Exchange 2016: *Configure Message Delivery Restrictions for a Mailbox*
  - Office 365 and Exchange 2013: *Configure Message Delivery Restrictions for a Mailbox*
  - Exchange 2010: *Configure Message Delivery Restrictions*

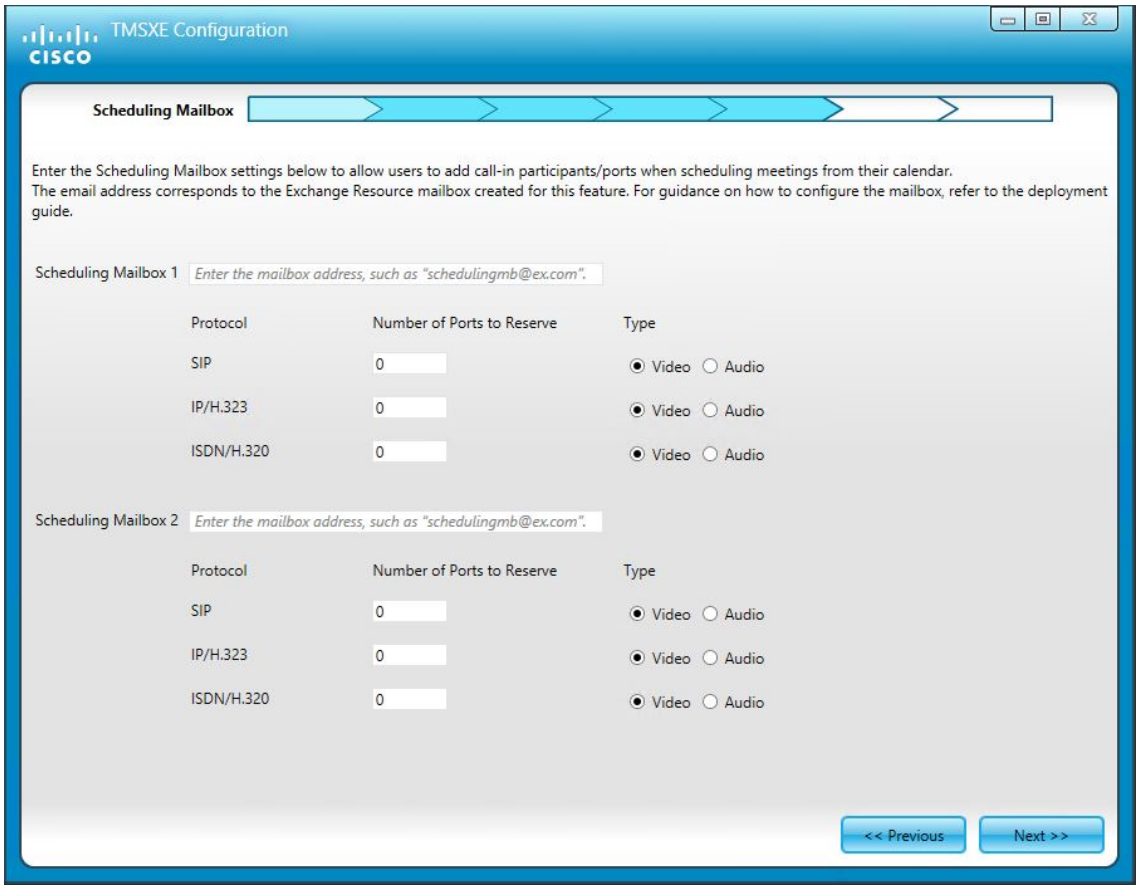
- Using AD Users and computers or Powershell, set the Active Directory user account to disabled.

  See the TechNet article *Disable or Enable a User Account* for instructions.

Configuring Scheduling Mailbox in Cisco TMSXE

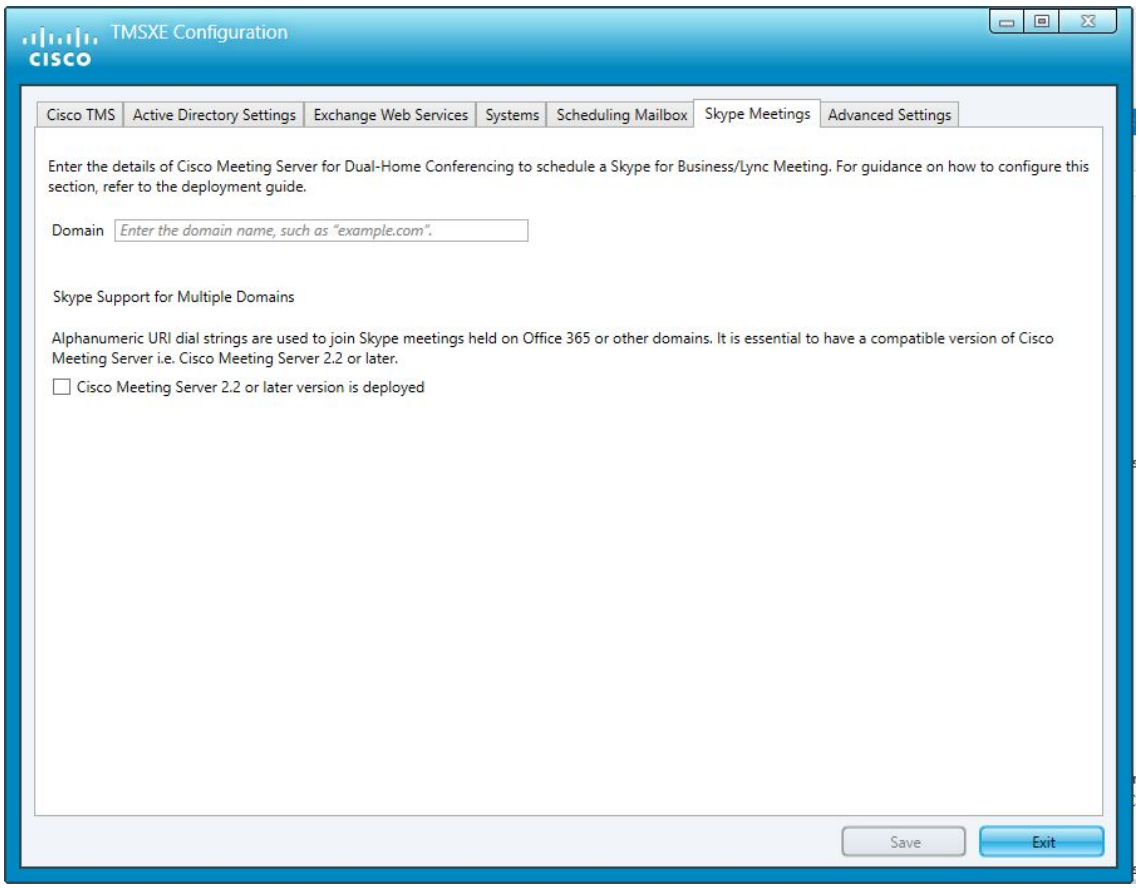
1. Click through the configuration wizard and in the **Scheduling Mailbox** Tab, enter the following information:
   a. Resource mailboxes
   b. Number of ports
   c. Dial-in type (audio or video) for each protocol

   The email address of both the Scheduling Mailboxes must be unique. The total number of ports across all configured Scheduling Mailboxes for the same Protocol and Call Type combination can not exceed 99 ports.
   For more information on Scheduling Mailbox, see , page 1.
2. Click **Next** to enter details in the other tabs.



Configuring Skype Meetings in Cisco TMSXE

1. Click through the configuration wizard and in the **Skype Meetings**Tab, enter Cisco Meeting Server's domain name that is configured for Dual Home Conferencing in the **Domain** field.
2. In the **Skype Support for Multiple Domains** section, select the **Cisco Meeting Server version 2.2 or later version is deployed** option to ensure that the entered Cisco Meeting Server domain is of 2.2 or later version.
   This allows Cisco TMSXE to support Office 365 Skype meeting by fetching an alphanumeric URI from the Skype meeting.
   Note: Cisco TMSXE creates an externally hosted conference in Cisco TMS with alphanumeric URI as a video address. If Cisco TMSXE Admin does not select the **Skype Support for Multiple Domains** section and only enters the **Domain** name, Cisco TMSXE fetches the Skype Conference id from the Skype meeting and it will not work for Office 365 Dual-Home conferencing.
3. Click **Next** to enter details in the other tabs.



Note: If deployment is using numericid instead of alphanumeric URI then ensure Enterprise Voice is enabled. Refer Microsoft documentation for procedure to enable Enterprise Voice in Enable the users for Enterprise Voice on premises article.

Conference Settings for Externally Hosted Skype Meetings

Skype conference type is based on the default conference type that is selected in Cisco TMS. To enable OBTP or auto-connect for externally hosted Skype meetings, perform the following steps:

1. In Cisco TMS, go to **Administrative Tools > Configuration > Conference Settings > Conference Creation**.
2. Set the **Default Reservation for Scheduled Calls** field to **One Button To Push** or **Automatic Connect**.

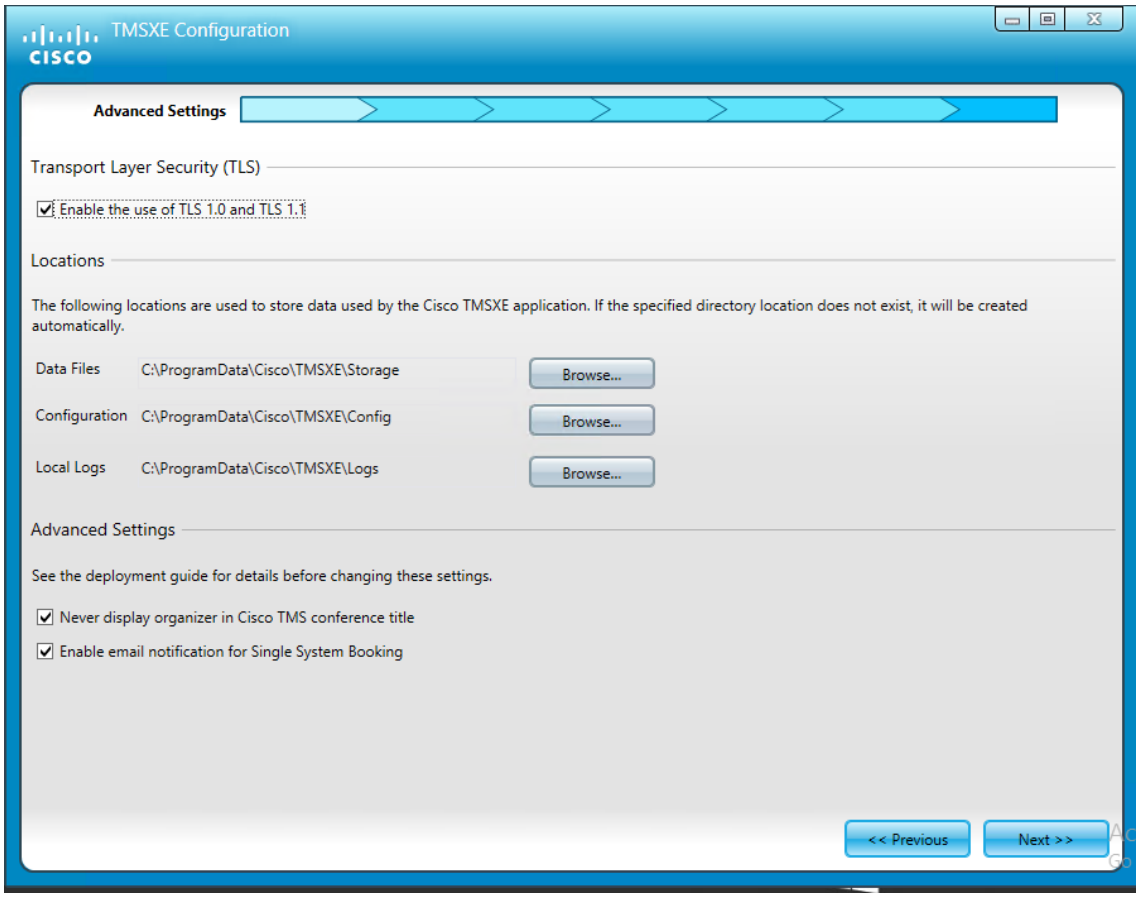
Note: These settings are applied to all scheduled conferences in Cisco TMS as default. For more information, refer to *Cisco TelePresence Management Suite Administrator Guide*.

In Cisco TMS 15.5 and Cisco TMSXE 5.5, this has been verified with OBTP and automatic connect of externally hosted Skype meetings.

Support for TLS 1.2

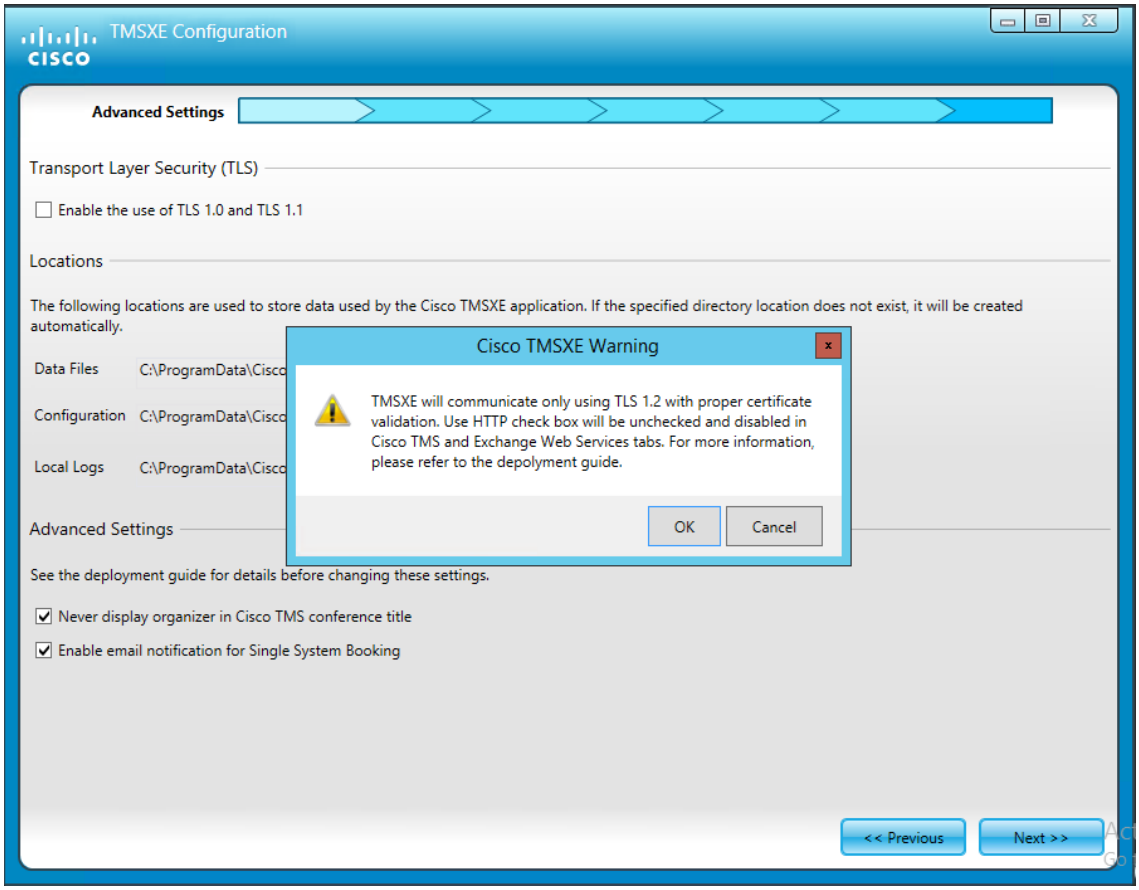
Cisco TMSXE supports TLS 1.0, 1.1 and 1.2 for communication. It is available in Cisco TMSXE **Configuration tool> Advanced Settings Tab>Transport Layer Security (TLS)**. Cisco TMSXE Admin can select any of the following TLS versions:

- 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.


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 >>

- 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.



Note that the above mentioned security settings impacts only Cisco TMSXE outbound connections. Unsupported TLS versions for Cisco TMSXE inbound connections can be disabled via Windows registry. For guidance, see the TLS/SSL Settings article.

In order to TLS 1.2 communication to work as desired, Cisco TMS and Exchange must both present valid certificates to Cisco TMSXE. To configure valid certificates, refer to Certificate Requirements, page 17 section.

Additional information about Security Settings

- Cisco TMSXE does not control support for SSLv3 and below versions, and 3DES.

  For guidance to disable SSLv3 and below versions, and 3DES, refer to Microsoft article on Cryptographic Algorithms and Protocols.

- Cisco TMSXE does not control any Ciphers.

  - For guidance on supported Ciphers, refer to Microsoft article on Cipher Suites.

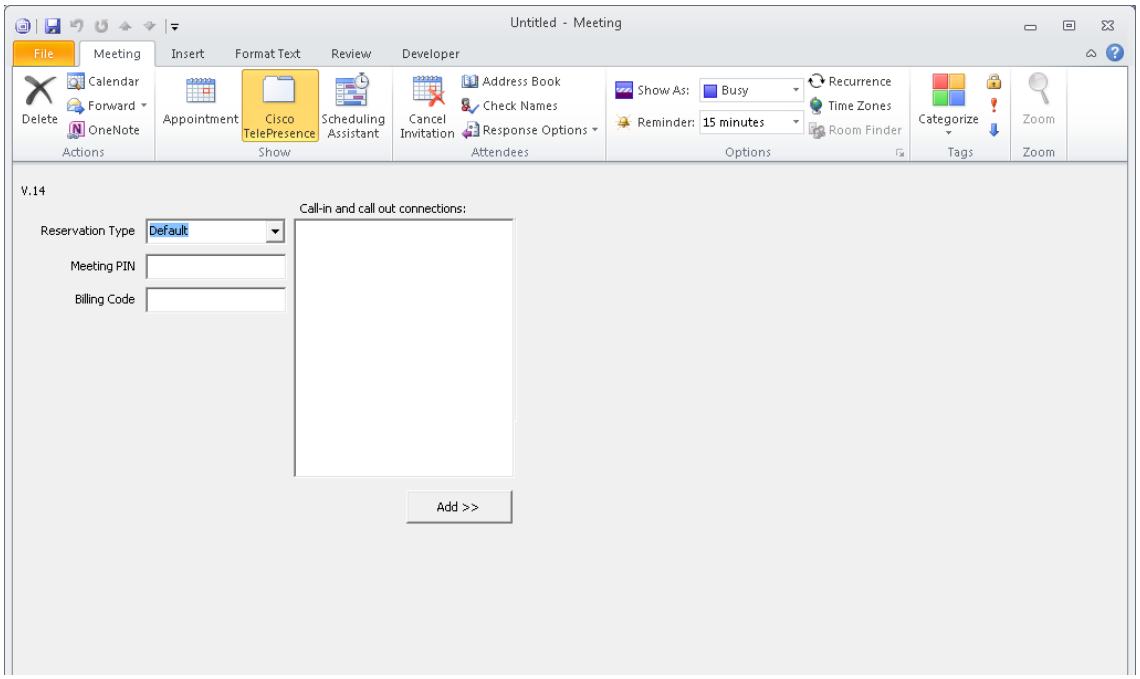
  - For guidance to configure the set of supported Ciphers, refer to Microsoft article on Configuring Cipher Suite Priority Order.

  - For guidance to disable the RC4 Cipher Suites, refer to the Microsoft article on disabling RC4.

Deploying the Cisco TelePresence Advanced Settings Form

The Cisco TMSXE deliverable includes a custom form that adds functionality to Outlook clients when creating or modifying videoconference meetings.

Available settings include specifying conference parameters and adding external participants. A detailed description of the available functionality can be found in *Cisco TMSXE User Guide (5.10)*.



The deployment and use of this form is optional. The form can also be added to an installation at any time in the future.

The form is an alternative to WebEx Productivity Tools with TelePresence for users that do not have WebEx, but need access to advanced telepresence settings.

The form does not contain an option to include WebEx in the meeting, but it may be used in combination with Scheduling Mailbox, page 61.

Limitations

Note that:

- Custom forms only work with Outlook for Windows.
- Custom forms are disabled by default. To enable the custom forms, refer to Using Cisco TelePresence Form requires 'custom form scripts' to be enabled , page 95 section.
- The Organizational Forms Library is not supported in Office 365, which means the form can only be published locally (see below).
- Editing the form is not supported.
- Outlook security does not allow previewing a meeting invite if the meeting was created using the Cisco form. When using the Reading Pane in Outlook, you must open the invite to view the meeting details.

Best Practice

As a best practice, we recommend that the form be placed in the Organizational Forms Library, which makes for simple distribution to all users and will automate any future updates to the form. You must either use an existing Organizational

Forms Library on your Exchange server, or create a new one before the custom form can be imported into the library.

Deployment with the Organizational Forms Library requires the following three steps:

1. Creating the Organizational Forms Library, page 68
2. Publishing the Cisco TelePresence Form, page 68
3. Configuring Clients to Use the Form, page 69

Administrators who are upgrading and that are already using the Cisco TelePresence form, need only refer to step 2.

The form can also be loaded manually per Outlook client, without using the Organizational Forms Library. In this case, step 1 can be omitted, but the form must be published locally before it can be used. Follow the instructions in Publishing the Cisco TelePresence Form, page 68.

Creating the Organizational Forms Library

You Exchange environment may lack the required infrastructure to support the Organizational Forms Library. The necessary steps required for publishing the Cisco TelePresence form will therefore vary based on whether Public Folders are already present.

Setting Up an Organizational Forms Library

See available documentation regarding Public Folders and Organization Forms Libraries in Exchange:

- Exchange 2016: *How to create an organizational forms library in Exchange Online and Exchange Server*
- Exchange 2013: *Create an Organizational Forms Library in Exchange 2013*
- Exchange 2010: *Create an Organizational Forms Library*

Publishing the Cisco TelePresence Form

Before the form can be used, it must be published using an Outlook client. If using the Organizational Forms Library, this library must be in place before following the steps below, see Creating the Organizational Forms Library, page 68.

Acquiring the Form

On the server where Cisco TMSXE was installed:

1. Locate the VideoConference-*.oft in the Cisco TMSXE .zip archive.
2. Copy the file to a client computer with Outlook installed.

Publishing from Outlook 2016 or 2013 or 2010

1. Log into Outlook and make sure you do not have a booking request open. If publishing to the Organizational Forms Library, you must log in as the user that has *Owner* permissions for the forms library.
2. On the ribbon, go to **File > Options > Customize Ribbon**.
3. Check *Developer* and click **OK**.
4. On the ribbon, go to **Developer > Design a Form...**.
5. In the dialog that opens, change the **Look In** dropdown menu to *User templates in File System*.
6. Click **Browse**.
7. Locate the .oft file on the computer, and open it.
8. From the **Publish** dropdown button, select **Publish Form As...**.

9. In the dialog that opens, change the **Look In** dropdown menu to one of the following:
   - *Organizational Forms Library* if you want to make the form available to several users.
   - *Personal Forms Library* if you are publishing only for use with the current user account.
10. Enter names in the two fields exactly as described below (case sensitive):
   - **Display name:** Meeting
   - **Form name:** VideoConference
11. Click **Publish** when complete.

The form will now be published and available for users to choose as their appointment form, see Configuring Clients to Use the Form, page 69.

Configuring Clients to Use the Form

Publishing the form makes it available to users, but does not force their Outlook client to use the form. Configuring Outlook to use the form is a one-time client configuration that can be done by each user, or by making changes to the Microsoft Windows Registry. Registry changes can be done automatically using methods such as Group Policy.

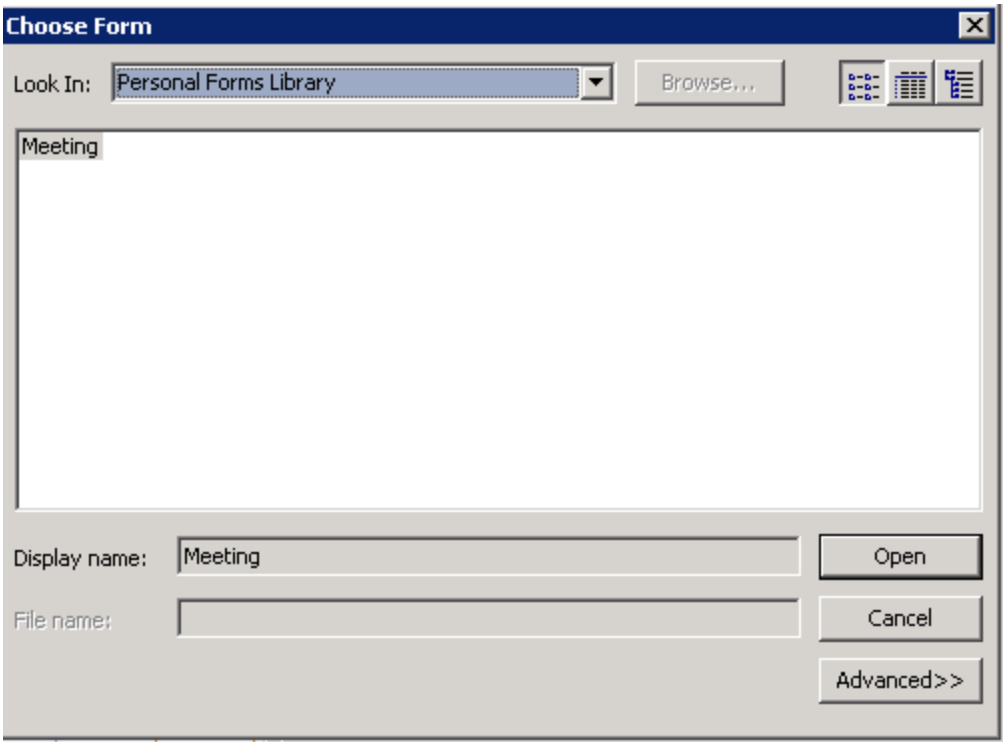
The Microsoft article *How to globally change the default forms in Outlook by using the Forms Administrator utility* describes and links to a utility for creating registry keys to change the default form.

Manually Configuring Clients to Use the Form

To configure the form per computer, each user must complete the following steps:

1. Open the Outlook client and go to the calendar.
2. In the left-side folder view, right-click the **Calendar** entry and select **Properties**.
3. Outlook 2010 only: Click the Folder tab, then click Calendar Properties.
4. The Calendar Properties window will open with the General tab selected.
5. From the **When posting to this folder, use** drop-down list, select *Forms*.

6. A dialog will open. In the **Look In** drop-down menu, make sure to select the library where the form was published, either *Organizational Forms Library* or *Personal Forms Library*.



7. An entry named Meeting will be displayed. Select it and click **Open.**
8. You will be returned to the Calendar Properties page. Click **OK** to save your changes

The client will now use the Cisco TelePresence form for all Calendar actions and have the Cisco TelePresence tab available when creating new booking requests.

Maintaining Cisco TMSXE

Starting and Stopping the Cisco TMSXE Service

Cisco TMSXE is a service that can be started and stopped from the Windows Server Services snap-in.

The Cisco TMSXE configuration tool will stop the service for you when you need to make configuration changes beyond adding and removing endpoints, and prompt you to restart the service when you close the tool. If you decline these prompts, you must manually start and stop the service.

Note that in a clustered deployment, you must stop the service on both nodes to enable edit configuration, and restart both services once configuration changes are complete.

The configuration tool must be closed and initial configuration must be completed before the service can start.

1. Open Server Manager.
2. Go to **Configuration > Services > Cisco TMSXE**.
3. Right-click Cisco TMSXE and select **Start** or **Stop**.

If the service fails to start, the error will be logged. See Troubleshooting, page 85 for more information.

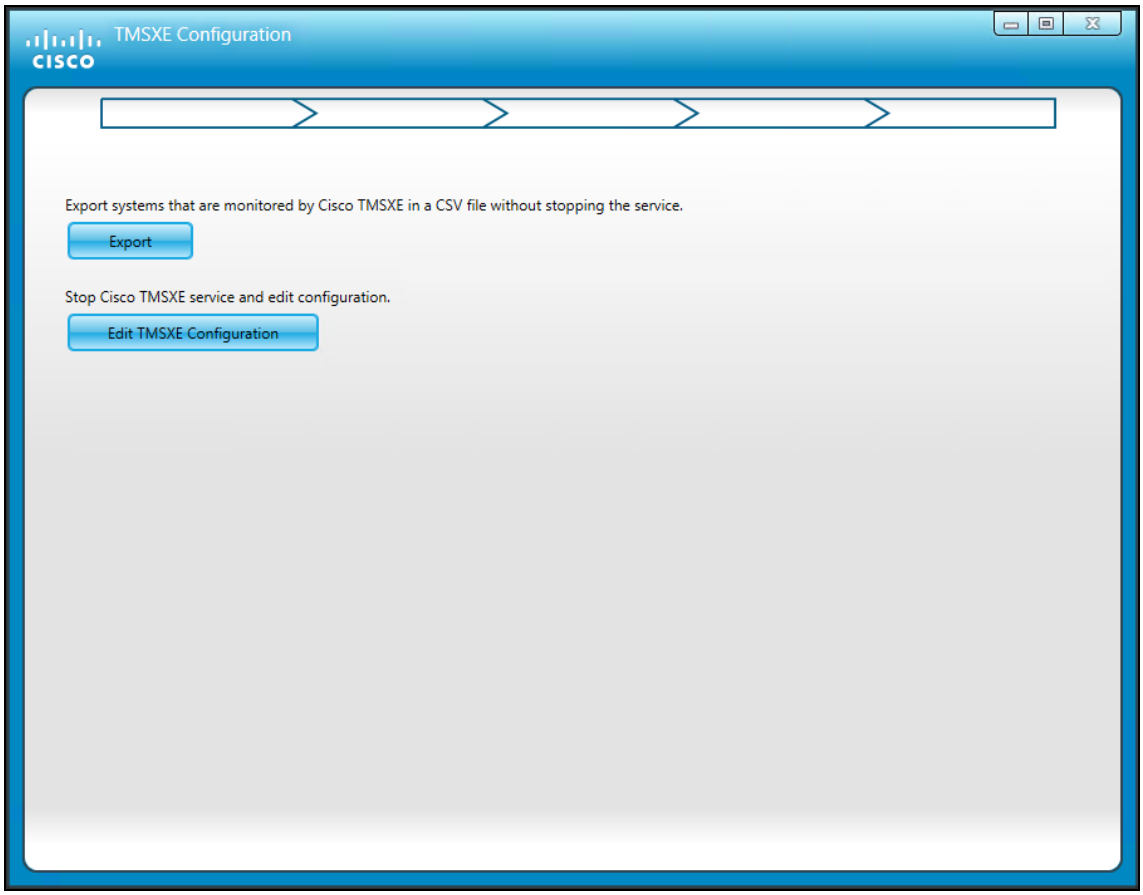
If any booking or modification requests are made while the service is halted, they will be queued and then processed as soon as the service is restarted.

Launching the configuration tool

To launch the tool:

- Go to the Windows Server **Start** menu or Start screen: **Start > All Programs > Cisco > Cisco TMSXE Configuration**

On tool startup, you will be asked whether you want to to stop the Cisco TMSXE service. You can leave the service running if adding a new system or removing an existing one. For edit configuration options, you must stop the service.



If you stopped the Cisco TMSXE service when starting the tool, you will be prompted to restart it when you exit.

Switches

The tool supports the following switches:

- `-help` displays a short help file.
- `-wizard` runs the configuration tool in setup wizard mode, intended to make sure all required fields are completed at initial setup. If no configuration is detected, a prompt will ask the user whether to migrate settings from an existing deployment.

For regular administrative tasks, run the configuration tool without any command-line arguments.

Adding, Removing, and Replacing Endpoints

This section describes how to add, remove, and replace endpoints and mailboxes to your deployment when Cisco TMSXE is in operation.

Adding Endpoints

If adding existing mailboxes that already contain bookings to your Cisco TMSXE deployment, you must do this off hours, due to the expected impact on Cisco TMS performance during first-time replication.

To add one or more endpoints to your deployment, follow the steps below. Note that the procedure is identical for clustered and non-clustered Cisco TMSXE:

1. Ensure that the endpoints are already added to Cisco TMS and that sufficient system licenses for Cisco TMSXE are available, if using a per-system option key.
2. Create or repurpose room mailboxes for the endpoints, following the instructions in Creating Mailboxes for Cisco TMS Endpoints in Exchange, page 25.
3. Ensure that the mailboxes are correctly configured, following the instructions in Configuring the Room Mailboxes, page 25.
4. Start the configuration tool by going to **Start > All Programs > Cisco > Cisco TMSXE Configuration.**.
5. Click **Edit TMSXE Configuration** in **Stop Cisco TMSXE service and edit configuration**n section.
6. Navigate to **Systems** tab.
7. There are two ways to add endpoints:
   - Manually add each endpoint:
     1. Modify the email address pattern to generate the names of your room mailboxes. Use primary SMTP addresses for the room mailboxes, aliases are not supported. Two optional variables are available:
        - `{{TmsId}}` translates to the system's numeric system ID from Cisco TMS.
        - `{{DisplayName}}` translates to the system's display name in Cisco TMS. Note that any spaces in the display name will be removed automatically.
     2. Select endpoints in the left-hand list and click **>>** to add them to Cisco TMSXE. Use `Ctrl` or `Shift` to select multiple endpoints.
     3. Modify individual email addresses as needed by double-clicking on them after they have been added to the right-hand list.
   - Click **Import Systems from CSV file** to import a comma-separated list of endpoints with email addresses and Cisco TMS system IDs.

     The list must be stored as a .csv file, and the valid format is the following, where the header row and **System Name** field are optional, and the second row contains example values:

     TMS ID, System Name,Email
     42,Meeting Room 1,meetingroom1@example.com
8. Click **Save**.

   The added mailboxes are validated. Note that this may take a while if you have added a large number of systems; for 250 endpoints, the process could take about 90 seconds.
9. Click **Exit**.

   The changes will be applied after a minimum of 10 minutes. In some cases it may take up to 30 minutes.

Removing Endpoints

The procedure is identical for clustered and non-clustered environments:

1. Start the configuration tool by going to **Start > All Programs > Cisco > Cisco TMSXE Configuration**.
2. Click **Edit TMSXE Configuration** to **Stop Cisco TMSXE service and edit configuration**.
3. Navigate to **Systems** tab.
4. In the list of systems added to Cisco TMSXE, locate the system(s) you want. Use `Shift` or `Ctrl` to select multiple systems. Click **<<**.
5. When done, click **Save** to validate the remaining systems.
6. Click **Exit** to close the configuration tool.

   The changes will be applied after a minimum of 10 minutes. In some cases it may take up to 30 minutes.

The above procedure will remove the endpoint and its mailbox from Cisco TMSXE, while the mailbox and system remain bookable independently in Cisco TMS and Exchange.

Disabling Remote Booking options

If using Cisco TMSXE- Extension for Microsoft Exchange option key, you must also disable a setting in Cisco TMS to prevent the removed endpoint from using a license.

Update the system as follows:

1. In Cisco TMS, go to **Systems > Navigator**.
2. Select the system you want.
3. Click the Settings tab.
4. In the **TMS Scheduling Settings** pane, you will find *Allow Remote Bookings*.

   If the setting is *Yes*, the system is currently using an Exchange Integration Option license.
5. To disable the setting:
   a. Click **Edit Settings**.
   b. Uncheck *Allow Remote Bookings*.
   c. Click **Save**.

Removing Endpoints from a Deployment

To remove endpoints completely from your deployment, you must also:

- Delete the mailbox from Exchange.
- Delete the system from Cisco TMS.

Replacing an Endpoint

You must stop the Cisco TMSXE service and enable edit configuration mode in the configuration tool if you need to:

- associate an endpoint already in Cisco TMSXE with a new mailbox.
- associate a mailbox already in Cisco TMSXE with a different endpoint.
- re-add an endpoint that has previously been removed, for example for maintenance.

In a clustered deployment, make sure to:

- stop the service on both nodes, starting with the passive node, before making any configuration changes.
- complete all changes before restarting both services.

Messages from Cisco TMSXE

When organizers book videoconferences using Outlook, they will receive messages both from Exchange and Cisco TMSXE.

Cisco TMSXE will send messages when:

- Routing is successfully set up for a conference with one of the following settings:
  - *Automatic Connect*
  - *Manual Connect*
  - *No Connect*
  - *One Button to Push*
- A requested conference routing is unsuccessful, and the conference is booked as *Reservation* instead (see below).
- A conference with the setting *Reservation* was successfully booked, but one or more resources were not available.

No notification is sent from Cisco TMSXE in the following cases:

- All resources are available for a conference successfully booked with the *Reservation* setting.
- A meeting is deleted by the organizer.

Also note that Cisco TMSXE never sends notifications about bookings or updates made in Cisco TMS. Notifications will be sent by Cisco TMS depending on system settings.

For guidance on identifying and correcting problematic or failed bookings in Cisco TMS, see Identifying and Correcting Defective, Downgraded, and Declined Meetings, page 89.

Email Notifications

The templates used to notify organizers are found in Cisco TMS. However, Cisco TMSXE can inject errors, warnings, and informational text into email messages sent by Cisco TMS.

These messages can be modified by the administrator.

Modifying the Templates

Avoid removing or changing any text in curly brackets, as these are variables that embed other messages.

All templates are created on first service startup in the Cisco TMSXE configuration folder, by default C:\ProgramData\Cisco\TMSXE\Config and all template names start with template_ and a descriptive name. Templates for HTML email contain HTML in the filename, not the extension.

To modify a template:

1. Open the template file in a text or HTML editor that does not automatically alter any of the markup or headers.
2. Edit the contents and/or formatting to your liking.
3. Save the modified file without the .sample extension.
4. Restart the Cisco TMSXE service for the modified template to be applied.

All .sample files are overwritten/reverted to default on each service startup, and missing template files are regenerated.

Backing up, moving, and uninstalling Cisco TMSXE

Backing Up Cisco TMSXE

Storage of passwords for Exchange, Cisco TMS, and Active Directory is encrypted using the Microsoft CryptoAPI.The passwords are encrypted using Cisco TMSXE's password entropy in combination with the encryption Data Protection Scope set to LocalMachine. The passwords can therefore only be decrypted by processes running on the server hosting Cisco TMSXE.

This also means that in order to retain encrypted passwords in the configuration, a full backup of Cisco TMSXE must include the entire OS of the server.

However, if retyping the passwords when reinstalling after a restore is an acceptable option, the backup needs only contain the contents of the configuration, storage, and log folders. These files should be copied to the new target before reinstalling.

Moving the Application to a New Server

Whether a server is being decommissioned or you are expanding your deployment and need more hardware capabilities, follow the instructions below to carry over the Cisco TMSXE configuration, list of monitored systems, and replication states to a new server.

Before You Start

The same version of Cisco TMSXE must be used on both servers, and no changes to the configuration must be made during the move.

- If an upgrade is also needed, perform the upgrade on the original server before starting the process of moving the application.
- If configuration changes are planned, perform them on the new server after the move is completed and you have verified that the service is running and functional.
- If the server is part of a clustered deployment, give the new server/node access to the network share that holds the cluster's configuration and data files before moving the application. For more information, see Installing Cisco TMSXE with Service Clustering, page 56.

Moving the Application

1. Install Cisco TMSXE on the new server. For instructions, see Performing a New Installation, page 35.
2. When prompted to start the configuration tool, click **Yes**.
3. Starting the configuration tool will create the necessary program data folder structure.
4. Close the configuration tool.
5. Stop the Cisco TMSXE Windows service on the original server.
6. Copy the following folders from the original server:
   - /config
   - /storage
   - /logs

   Their default location is C:\ProgramData\Cisco\TMSXE\. If they have been moved to custom locations,you can see these in the Locations tab of the configuration tool on the original server.
7. On the new server, place the folders in their default location, regardless of their location on the original server, and confirm that you want to overwrite the existing folders and files.

8. Run the configuration tool.
9. Click **OK** when receiving notifications that password fields are corrupted.
10. On the Cisco TMS tab, do the following:
    a. Update the **Hostname** field if required.

       If, for example, you are moving Cisco TMSXE from sharing a server with Cisco TMS, the hostname can no longer be "localhost".

    b. Enter the password.
    c. Do not click **Save**, as this will fail until the Exchange Web Services password has been entered.
11. Go to the Exchange Web Services tab and do the following:
    a. Enter the password.
    b. Click **Save**.
12. Optionally, if you want a custom location for the configuration files:
    a. Go to the Advanced Settings tab.
    b. Modify the file paths as desired.
    c. Click **Save**.
13. Close the configuration tool.
14. Start the Cisco TMSXE service.

After Moving the Application

Do not reactivate any services related to Cisco TMSXE on the original server after the move.

We strongly recommend removing Cisco TMSXE from the original server, see Uninstalling Cisco TMSXE, page 76 if not decommissioning the server itself.

Uninstalling Cisco TMSXE

1. Log on to the Cisco TMSXE server as an administrator.
2. Go to **Control Panel > Programs and Features**.
3. Right-click Cisco TMSXE and select **Uninstall**.

Removing Cisco TMSXE from the Server

After uninstalling the software:

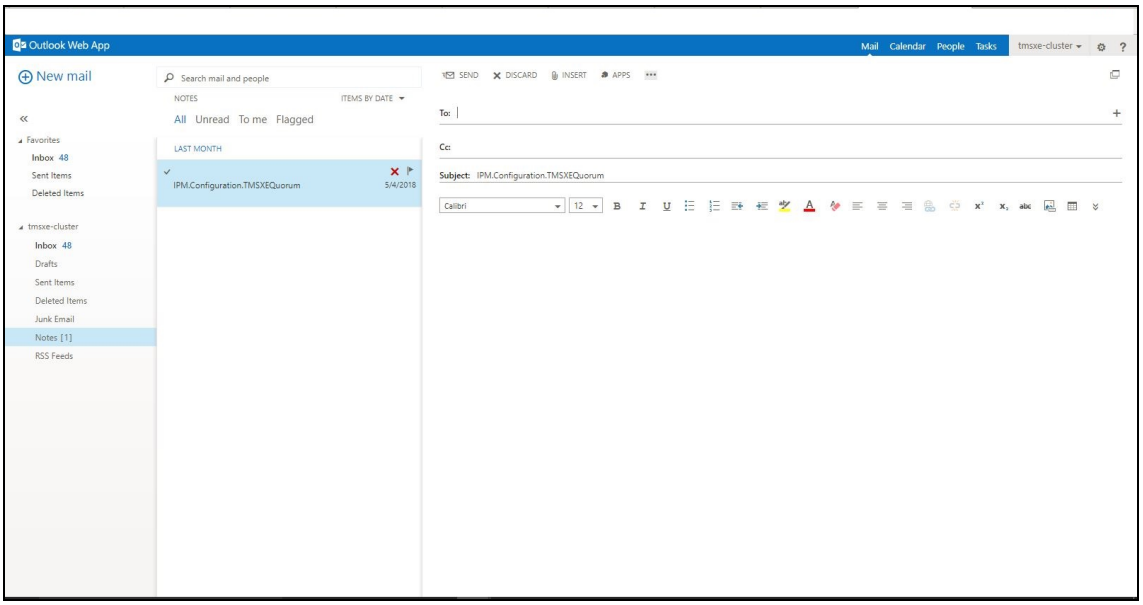
1. Delete all data directories, by default:
   - C:\ProgramData\Cisco\TMSXE\Storage
   - C:\ProgramData\Cisco\TMSXE\Config
   - C:\ProgramData\Cisco\TMSXE\Logs
2. Delete the registry entry HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\TMSXE.

Remove Cisco TMSXE cluster

Remove everything from the server as given in section Removing Cisco TMSXE from the Server, page 76.
Note: If Cisco TMSXE clustered environment is removed, the node file must also be removed from Cisco TMSXE server mailbox. For more information, refer to Removing Cisco TMSXE cluster environment , page 77.

Removing Cisco TMSXE cluster environment

1. Login to First Node server and uninstall Cisco TMSXE. For more information, refer to section Uninstalling Cisco TMSXE, page 76.
2. Delete Cisco TMSXE folder and also the following folders within it:
   a. C:\ProgramData\Cisco\TMSXE\Storage
   b. C:\ProgramData\Cisco\TMSXE\Config
3. Delete the registry entry HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\TMSXE.
4. Login to Second Node server and uninstall Cisco TMSXE. For more information, refer to section Uninstalling Cisco TMSXE, page 76
5. Delete Cisco TMSXEfolder and also the following folders within it:
   a. C:\ProgramData\Cisco\TMSXE\Storage
   b. C:\ProgramData\Cisco\TMSXE\Config
6. Delete the registry entry HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\TMSXE.
7. Delete Shared Data (**\\server\share\storage**) and Configuration (**\\server\share\config)** folders from Shared Location.
8. Login to Cisco TMSXE server mailbox and navigate to **Notes**.
   a. Select the Node file and click **Discard**. The node file is deleted. Refer to the following screenshot.



Legacy Deployment Options

Cisco Collaboration Meeting Rooms Hybrid

Cisco CMR Hybrid can be used with Cisco TMSXE and any supported version of Exchange, allowing users to book telepresence meetings with a Webex component directly from their mail client. Cisco CMR Hybrid conference is a telepresence conference hosted on a Cisco TMS managed on-premise bridge, which has a Webex hosted meeting as an auto dialed participant.

Requirements

In order to use Cisco TMSXE for meetings that include Webex, Cisco TMS must be set up with:

- one or more Webex sites
- Webex credentials for each user (not service user), either manually added or using Webex/Cisco TMS single sign-on

Limitations

Private Flag

When the organizer has created a CMR Hybrid private , Cisco TMS does not treat it as a private conference.

Deployment Scenarios and Best Practices

There are three ways to book CMR Hybrid meetings with Cisco TMSXE which are:

- Cisco TMS setting
- Webex Scheduling Mailbox
- Webex Productivity Tools with TelePresence

The use of at least one of these options is required. However, using multiple options are supported.

Cisco TMS setting

Cisco TMS can be configured to add Webex to all scheduled conferences, when possible. It should be noted that the organizers booking from Outlook may not realize that Webex is included until receiving the booking confirmation.

Webex Scheduling Mailbox

The Webex Scheduling Mailbox is a simple way for meeting organizers to include a Webex conference with default settings in their telepresence meeting.

The administrator creates a special room mailbox allowing users to include Webex in their telepresence meeting by adding this mailbox to their Outlook meeting request.

Note that:

- This solution is intended for the creation of CMR Hybrid meetings with both Webex and telepresence.
- The mailbox must not be used to schedule Webex-only meetings, as telepresence infrastructure resources will be booked and used during the meeting even if no telepresence rooms or call-in telepresence participants are included.
- If Webex was requested and successfully booked, links to join and other Webex details are included in the booking confirmation to organizer.
- If Webex could not be booked, the telepresence meeting booking confirmation will contain a Webex error message stating the problem.

The Webex Scheduling Mailbox communicates with Webex by way of Cisco TMSXE/Cisco TMSBA/ Cisco TMS. Using this method, whether or not to include Webex is considered a property of the telepresence meeting.

Webex Productivity Tools with TelePresence

Productivity Tools let users book telepresence with Webex from Outlook and modify advanced settings for both components.

For limitations on Productivity Tools and versions of Exchange and Outlook, see the documentation for your version of Webex Meeting Center.

Webex Productivity Tools with TelePresence communicates directly with Webex. Therefore, Webex Productivity Tools with TelePresence may be used to book Webex-only meetings as well as CMR Hybrid meetings with both telepresence and Webex.

Requirements

In order to use WebEx Productivity Tools with TelePresence, you must include Cisco TMS Booking Service when installing Cisco TMSXE.

For Booking Service to work, you must enable HTTPS for Default Web Site in IIS on the server where Cisco TMSXE and Booking Service are both installed. In a redundant deployment, this must be done on both nodes.

If IIS is not present on the server prior to installation, it will be automatically installed with Booking Service. You must then configure HTTPS for Default Web Site after installation.

Limitations

- Delegates for room mailboxes are supported with Cisco TMSXE, but not if Productivity Tools are used with Outlook.
- Cisco TMSXE does not allow you to book Webex with Telepresence meeting/s using Productivity Tools, when Cisco TMSXE services are stopped.

Installation and Configuration

Cisco TMS Setting

In **Cisco TMS Portal > Administrative Tools > Configuration > WebEx Hybrid Settings**, set '**Add WebEx Hybrid to All Conferences**' to **Yes**. For more information, refer to Cisco TelePresence Management Suite Administrator Guide.

Webex Scheduling Mailbox

Creating and Configuring Webex.

Create and configure the mailbox using either Exchange Admin Center, Exchange Management Console, or Exchange Management Shell:

1. Create a new resource mailbox called "Webex" . For instructions, see:
   - Exchange 2016, Office 365 and Exchange 2013: *Create and Manage Room Mailboxes*
   - Exchange 2010: *Create a Room or Equipment Mailbox*
2. If using Exchange 2010 without mailbox impersonation, you must give the Cisco TMSXE service user account Full Mailbox Access to this mailbox. For instructions, see:
   - Exchange 2010: *Allow Mailbox Access*

3. Modify the mailbox properties:
   a. Turn off the Calendar Attendant for the mailbox. For instructions, see:
      - Exchange 2016: *Set-CalendarProcessing*
      - Office 365 and Exchange 2013: *Set-CalendarProcessing*
      - Exchange 2010: *Configure User and Resource Mailbox Properties*
   b. Make sure new requests are not automatically marked as tentative by disabling **AddNewRequestsTentatively** (also known as **Mark new meeting requests as Tentative**) for the mailbox.
   c. Set **ForwardRequestsToDelegates** to *False*.
   d. For Office 365, Exchange 2016, Exchange 2013, and Exchange 2010: Set `CalendarRepairDisabled` to *True*.

Note that we previously recommended that the Webex Scheduling Mailbox be created as a user mailbox. Starting with Exchange 2013, user mailboxes are no longer compatible with the required settings for the Webex Scheduling Mailbox.

.

Additional Recommendations

We also recommend the following configurations:

- Using Exchange Management Console **Mail Flow Settings** or Exchange Management Shell, stricten the message delivery restrictions as needed.

  For example, require senders to be authenticated, only allow from people in a specific group, or similar.

  For instructions, see:

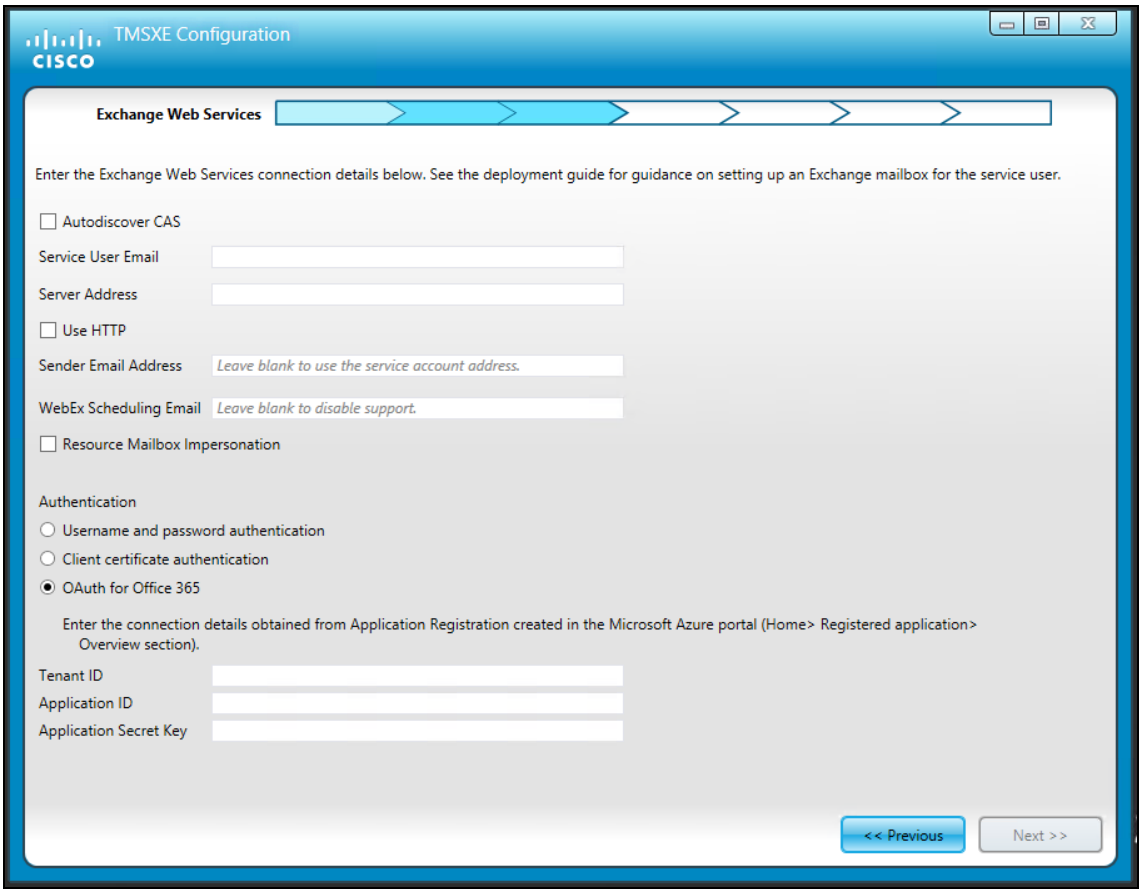
  - Exchange 2016: *Configure Message Delivery Restrictions for a Mailbox*
  - Office 365 and Exchange 2013: *Configure Message Delivery Restrictions for a Mailbox*
  - Exchange 2010: *Configure Message Delivery Restrictions*

Adding the Mailbox to Cisco TMSXE

You can add the mailbox to the Cisco TMSXE configuration wizard immediately after installation or upgrade.

If adding the mailbox at a later stage:

1. Open the configuration tool and go to the Exchange Web Services tab.
2. In the **WebEx Scheduling Email** field, fill in the email address of your newly created WebEx Scheduling Mailbox.



Webex Productivity Tools with TelePresence

If you did not include the Cisco TMS Booking Service during initial installation, follow these instructions to add it to your deployment:

1. On the Cisco TMSXE server, go to Control Panel.
2. Select Programs and Features.
3. Right-click on "Cisco TMSXE" and select **Change**.

   This starts the installer and allows you to change your installation.

4. Follow all instructions provided by the installer and opt to include Cisco TMS Booking Service.

   When the installation is complete, a virtual directory called TMSService will be available under Default Web Site in IIS .

Note that installing the Booking Service forces a restart of IIS. This will affect Cisco TMS if the two are co-located, although this is only recommended for small deployments, see Best Practices for all Deployments, page 16.

Configuring IIS for HTTPS

For Booking Service to work, you must enable HTTPS for Default Web Site in IIS on the server where Cisco TMSXE and Booking Service are both installed. In a redundant deployment, this must be done on both nodes.

If IIS is not present on the server prior to installation, it will be automatically installed with Booking Service. You must then configure HTTPS for Default Web Site after installation.

For general guidance, see for example the IIS article *How to Set Up SSL on IIS 7*.

For Webex Productivity Tools with TelePresence to operate, you must also:

1. Open IIS Manager.
2. Go to **IIS > SSL Settings**.
3. Set **Client certificates** to *Ignore*.

Setting Up Communication between Webex and Cisco TMSXE

1. On your Webex site, go to **Manage Site > Site Settings > OneTouch TelePresence Options**.
2. In the **Cisco TMSXE Host Address** field, enter the full address of the Booking Service by including the hostname of the server in the following address: **https://<hostname>/TMSService/Booking.svc**.
3. Save the update.

For overall instructions on setting up Cisco Collaboration Meeting Rooms Hybrid, see *Cisco Webex Enabled TelePresence Configuration Guide*

Cisco TMS Booking Service Redundancy

Cisco TMS Booking Service can be set up, within a Cisco TMSXE cluster, for an active/active redundancy using a network load balancer (NLB) to ensure high availability, but does not increase performance.

Prerequisites

- The NLB must support Windows authentication, as the probe URL is authenticated.

  We recommend using F5 BIG-IP version 11.4.1, which has been tested and is known to work with Cisco TMSXE.

- The Cisco TMSXE servers must use a certificate where the Common Name (CN) is a DNS entry pointing to the virtual IP of the network load balancer.
- Setup a Cisco TMSXE cluster with the TMS Booking Service installed and configured on both nodes.

Deploying the Load Balancer

1. Set the NLB to probe this URL on both nodes every 15 seconds: /TMSService/Booking.svc/Status/Health
2. For performance reasons, you must set up the load balancer to have a sticky connection to one of the nodes.

   When the primary node cannot be reached, the load balancer will switch to the secondary node.

3. Create a DNS record for the virtual IP of the NLB.
4. Add this NLB hostname to WebEx as the **Cisco TMSXE Host Address**, see , page 1.

Probe Responses

Cisco TMS Booking Service checks the connection to Cisco TMS every 15 seconds.

When regularly probing each Booking Service node as described above:

- HTTP 200 OK will be returned if the connections to AD and Cisco TMS are alive, and the location of the configuration files is available.
- HTTP 503 Service Unavailable will be returned with one or more messages detailing the error if there is a problem with any of the above connections.

Troubleshooting

This section covers troubleshooting of issues that may arise during installation, configuration, and operation of Cisco TMSXE. It also describes how to use the logging features.

Reading the Windows Event Log

1. Right-click on **Computer** in the Start menu, Start screen, Desktop, or Explorer, and select **Manage**.
2. Go to **Server Manager > Diagnostics > Event Viewer > Applications and Services Logs > Cisco TMSXE**
3. Press `F5` to update the log pane, which lists information about startup, errors, and location of logs.

How Logging Works

Cisco TMSXE creates several logs to assist in troubleshooting. The default location for these logs is C:\ProgramData\Cisco\TMSXE\Logs.

The location can be reconfigured using the configuration tool during or after installation, see Configuration Reference, page 51.

- TMSXE-log-file.txt logs all activities of the Cisco TMSXE Windows service.
- TMSXE-conference-history-log-file.txt is a filtered view of the above, logging all conference events.
- TMSXE-decline-downgrade-log-file.txt is a filtered view of the above, logging all declined or downgraded meetings. See Filtered Log for Declined and Downgraded Conferences, page 85.
- TMSXEConfig-log-file.txt logs the activities of the configuration tool.
- TMSXEService-log-file.txt logs the activities of Cisco TMS Booking Service, the synchronous booking proxy. The file will only be generated if Booking Service has been installed and accessed.
- TMSXEMeetingAnalyzerApplication-log-file.txt logs the activities of Meeting Analyzer. Note that the meeting analysis results are in the reports you retrieve from inside of the tool itself. This log contains any connection issues and other errors encountered by the tool during operation.

All log files have a size limit of 5Mb. When this limit is reached:

- A new file with the same name is created.
- The old log file is renamed to include the suffix .1.
- If a .1 file already exists, that file is renamed to .2, and so on.
- The maximum number of log files to store is 15. When a log file reaches the suffix .15, it will be deleted the next time the current log file reaches 5Mb.

Note: You have to manually delete the old **TMSXE-conference-history-log-file_YYYYMMDD.txt** and TMSXE-decline-downgrade-log-file_ **YYYYMMDD.txt** as per your requirement. In the case of an upgrade where there are preexisting logs with the old file names, none of those old logs will be removed. It is recommended that those old logs are manually deleted or archived, in accordance to the customer's requirements.

Filtered Log for Declined and Downgraded Conferences

The log file TMSXE-decline-downgrade-log-file.txt is created by the Cisco TMSXE Windows service. This log includes all log entries from TMSXE-log-file.txt that relate to bookings that have been:

- declined by Cisco TMS
- downgraded by Cisco TMSXE and subsequently booked as *Reservation* in Cisco TMS.

A maximum of 20 logs are kept on the server. When 20 logs have been accumulated, the first will be overwritten. If you need to retain logs for a longer period of time, create your own backup procedure for these logs.

Sample log messages for declines and downgrades:

- Booking as requested fails: **Saving routed conference failed, will try to downgrade to reservation only**
- Reservation (downgrade) successful: **Conference successfully downgraded to Reservation Only**
- Reservation fails: **Failed to reserve all systems for conference**
- Booking declined: **Conference with single TMS participant declined**

Turning on Debug Logging

The default log level is informational. For debugging purposes, doing the following will change the log level:

1. Open Notepad or another text editor as an administrator.
2. Locate the Cisco TMSXE Config folder on your computer, by default located in C:\ProgramData\Cisco\TMSXE\Config. Note that the ProgramData Windows folder is hidden by default.
3. Change the drop-down to look for *All Files*.
4. Open the file Log4net.config.
5. In the line that says **<level value ="INFO" />**, replace `"INFO"` with `"DEBUG"`.
6. Save and close the file.

This setting significantly increases the size of each log. We strongly recommend reverting the log level back to "INFO" after debugging. The steps to revert are the same as above.

TMSXE-conference-history-log only has an INFO level and will not be affected by a change to DEBUG.

Logging in a Clustered Deployment

Although the log location may be placed on a network drive, this location may not be shared; each node *must* have its own logs.

The Log4net.config file is a part of the shared configuration, which means that enabling and disabling debug logging automatically affects both nodes.

Installation Fails

If installing Cisco TMSXE with Booking Service, installation will fail if:

- the default site in IIS has been manually deleted.

  To solve this problem, manually create a site in IIS and retry the installation.

- the site is set up only with an HTTPS binding in IIS.

  To solve this problem, add an HTTP binding and retry the installation.

Errors During Configuration

Error messages during the Cisco TMSXE configuration process while using the configuration tool generally indicate problems connecting to other systems. The initial troubleshooting step should always be verifying that all connection details including usernames and passwords are correct.

Untrusted Certificates

By default, Cisco TMSXE uses HTTPS for secure communication with Cisco TMS and Exchange Web Services.

If, during initial setup, the configuration tool detects that untrusted certificates are presented by one or both of these servers, a prompt will notify you of this.

This prompt also provides the option to **Allow Untrusted Certificates**, with the caveat that this setting should only be used for test environments, as it is not considered safe and cannot be reverted.

For more information on the Cisco TMSXE security model and what is defined as a trusted certificate, see *Cisco TelePresence Management Suite Extension for Microsoft Exchange Administrator Guide (3.0)*.

Remote Name Could Not Be Resolved

If you include the protocol (HTTP or HTTPS) when filling in the Cisco TMS server address, you will get the following error message:

"Cannot connect to Cisco TMS using the details provided. Verify that all fields are filled in correctly and save again. Error is: The remote name could not be resolved: 'http'."

Remove the protocol from the server address, leaving only the IP address or FQDN, and click **Next** again to validate the settings and proceed with setup.

Cisco TMS Service User Account Does Not Belong to a Group That Has "Book on behalf of" Permissions

- Permissions in Cisco TMS are controlled on a group level. You must ensure that the account set up for the service user must belong to a group that has the permission "Book on behalf of". See Creating a Cisco TMS User for Cisco TMSXE, page 24.
- This error may also be displayed in the case of incorrect IIS authentication settings on the Cisco TMS server.

A Time Zone with the Specified ID Could Not Be Found

If during validation of Exchange settings you receive an error message saying that connecting to the Exchange CAS server was not possible and the message from the server is "A timezone with the specified ID could not be found", this error message may indicate a time zone misconfiguration or a missing Windows update on the Exchange CAS server or servers.

We recommend that all Windows Servers involved in a Cisco TMS/Cisco TMSXE/Exchange deployment be kept up to date in all Microsoft published time zone update packages.

See the Windows KB article December 2010 cumulative time zone update for Windows operating systems for more information and download links.

Unbookable or Unlicensed Systems

The configuration tool will present an error message if you add one or more systems to Cisco TMSXE that are either missing licensing for Cisco TMSXE or are not bookable for another reason.

Licensing

To complete configuration and make Cisco TMSXE start up, you must do one of the following:

- Make sure all systems added to Cisco TMSXE are licensed for Outlook booking per theCisco TMS Requirements, page 12.
- Make sure all systems added to Cisco TMSXE are licensed for Outlook booking per the licensing requirements,

see *Cisco TelePresence Management Suite Extension for Microsoft Exchange Installation Guide*.

- Remove any unlicensed systems.

Not Bookable

An endpoint may not be possible to book for other reasons. For example, an administrator may have disabled *Allow Bookings* in Cisco TMS because the endpoint is undergoing maintenance.

If you try to add an endpoint that is not bookable to Cisco TMSXE, the error message will include the system ID of affected endpoint(s).

To complete configuration and make Cisco TMSXE start up, you must do one of the following:

- Make all affected systems bookable.
- Remove all systems causing errors from Cisco TMSXE and add the systems back in when they can be booked.

Cisco TMSXE Configuration Error while Accessing Files

An error is displayed when, Cisco TMSXE Configuration Tool is unable to access the folder location, or the files contained therein. There can be various causes for this error, which could not be limited to that file or folder. The reasons could be:

- The file/ folder may not exist.
- The file/ folder/ share permissions are not set to appropriate access.
- The folder location is not accessible. For example, a network share may be offline.

Cisco TMSXE provides an additional caution when you reset to the local default and manually update locations. You have to be cautious about re-setting the values to default, as it removes the previously configured cluster settings and resets locations to the local default. Ensure that the configuration locations are accessible before updating the locations.

Caution: Be careful while making any changes to the configured paths, as any incorrect settings could have advert effects on the deployment. This includes use of the "**Reset to Default**" function.

Cisco TMSXE Service Does Not Start

If you receive an error message stating that the service "started and then stopped", the configuration tool is probably open. Close the configuration tool and try running the service again.

If this is not the case, look at the event log for the ERROR displayed before the “Shutting down..” message. See Reading the Windows Event Log, page 85.

Other possible reasons the service will not start:

- The service cannot connect to Exchange Web Services or Cisco TMS anymore
- The service doesn’t have write permissions to the log folder.
- Files in the Cisco TMSXE folder are in use.
- Configuration is incomplete. Launch the configuration tool, review and fill in all fields, close the tool and try running the service again.
- One or more systems are not possible to book in Cisco TMS. See Unbookable or Unlicensed Systems, page 87.

No Bookings are Accepted or Declined

If no accept/decline messages are received from one or more of the endpoints you are trying to book, auto-acceptance may not have been turned on for the room mailbox. See Creating Mailboxes for Cisco TMS Endpoints in Exchange, page

25 for detail on setting this option for your version of Exchange.

You may also be running a version of Exchange 2010 older than Service Pack 3, which is the current requirement. Forms using scripts, such as the Cisco TelePresence form, were not supported by the automatic accept feature in Exchange 2010 up to SP2, and any booking from a client that has such a form will be left pending in the room mailbox. To solve this problem, upgrade to Microsoft Exchange SP3.

Bookings Not Replicating

If bookings do not replicate neither to or from Exchange:

- Check the event log for connection issues with Exchange or Cisco TMS. (See Reading the Windows Event Log, page 85.)
- Verify that the TMSXE service is running.

Also note that Cisco TMSXE can only update room calendars, not organizer calendars. Changes made to a booking in Cisco TMS will therefore be viewable in room calendars, but not in the organizer's calendar.

Identifying and Correcting Defective, Downgraded, and Declined Meetings

When a booking encounters an issue in Cisco TMS, this can result in the meeting being saved as defective, downgraded to type Reservation (no routing), or declined as summarized in the table below.

Table 6 Booking issues, causes, and resolutions

Root Cause	Result	Resolutions
Meeting is outside of the Cisco TMS booking horizon, uses an unsupported recurrence pattern, or overlaps with an existing meeting.	Declined by Cisco TMS	Organizer or administrator must book again with valid details. Administrator must align booking windows for all resource mailboxes in Exchange with general booking window in Cisco TMS. Administrator must disallow double booking of telepresence rooms in Exchange.
Booking encounters a resource conflict in Cisco TMS .	Saved as defective by Cisco TMS	The organizer or administrator must update the booking to eliminate the resource conflict, or free up resources and re-save the booking from either Outlook or Cisco TMS.
One or more participants (telepresence rooms) cannot be scheduled into a meeting due to configuration issues such as missing software licenses or booking permissions, or scheduling with the endpoint has been disabled.	Tentatively downgraded by Cisco TMSXE, declined by Cisco TMS if this fails.	The administrator must resolve the configuration or license issue and restore the meeting to its original type (typically *Automatic Connect* or *One Button To Push*).

Declined and Downgraded Meetings

Reading the Logs

Logs for Cisco TMSXE are available in the default location C:\ProgramData\Cisco\Cisco TMSXE\Logs.

An entry will be created in the log file TMSXE-decline-downgrade-log-file.txt for each participant that is declined or downgraded.

Example log entries for typical decline scenarios:

- 2014-08-19 14:39:50,402 [30] INFO TMSXEBestEffortCommitter - Saving conference as requested was declined (conference can never be booked): Unexpected recurrence pattern frequency type encountered: Yearly
- 2014-08-19 14:39:50,318 [10] INFO TMSXEBestEffortCommitter - Saving conference as requested was declined (conference can never be booked): Number of occurrences must be between 1 and 100.

Re-Creating Declined Meetings

To resolve declined meetings:

1. Identify the declined meetings using the log.
2. Do one of the following:
   - Re-create these bookings in Cisco TMS on behalf of the organizers at an available time with a supported recurrence pattern.
   - Contact the organizers and ask them to re-create their bookings using Outlook.

Correcting Downgraded Meetings

When downgrading a meeting, Cisco TMSXE will try to book all participants as *Reservation*. Any failing participants will be declined, and the meeting will be declined if all participants fail. In the latter case, see the procedure for declined meetings.

To correct a downgraded meeting:

1. Identify the downgraded meetings and failing participants using the log.
2. Correct the configuration or license issue for the failing participants.
3. Using Cisco TMS, re-add the corrected participants to the original bookings.
4. For each downgraded meeting, change the **Type** to *One Button To Push* or *Automatic Connect*.

Defective Meetings

A *Defective* conference in Cisco TMS has been booked by an external client that encountered a resource conflict or routing problem.

A defective conference retains all properties of the booking request without setting up routing or consuming telepresence resources. Until all issues are resolved, Cisco TMS will not initiate a defective conference or send it to endpoints.

- In the case of a routing issue, all endpoints in the booking will be set to *Busy* for the scheduled time, keeping the reservation while the administrator or user resolves the issue.
- In the rare case of an endpoint reservation conflict, the endpoints will not be set to *Busy* for the defective booking.

Defective conferences can be corrected by the organizer or the administrator:

- Users who book conferences that are saved as defective will be notified by email and can resolve most issues by changing their request and rescheduling from their client.
- Administrators can locate and resolve defective conferences in Cisco TMS by going to **Administrative Tools > Diagnostics > Conference Diagnostics** or **Booking > List Conferences**.

  Conferences that are defective because of configuration errors or a permanent lack of routing resources must be resolved by an administrator.

When scheduling a series where only some occurrences have a resource conflict or routing issue, Cisco TMS will only store the problematic occurrences as defective, leaving the remaining occurrences unaffected.

Correcting Defective Meetings

To identify and attempt to correct bookings saved as *Defective*, we recommend the following procedure:

1. In Cisco TMS, go to **Administrative Tools > Diagnostics > Conferences Diagnostics**.
2. Select all entries.
3. Click **Autocorrect**.

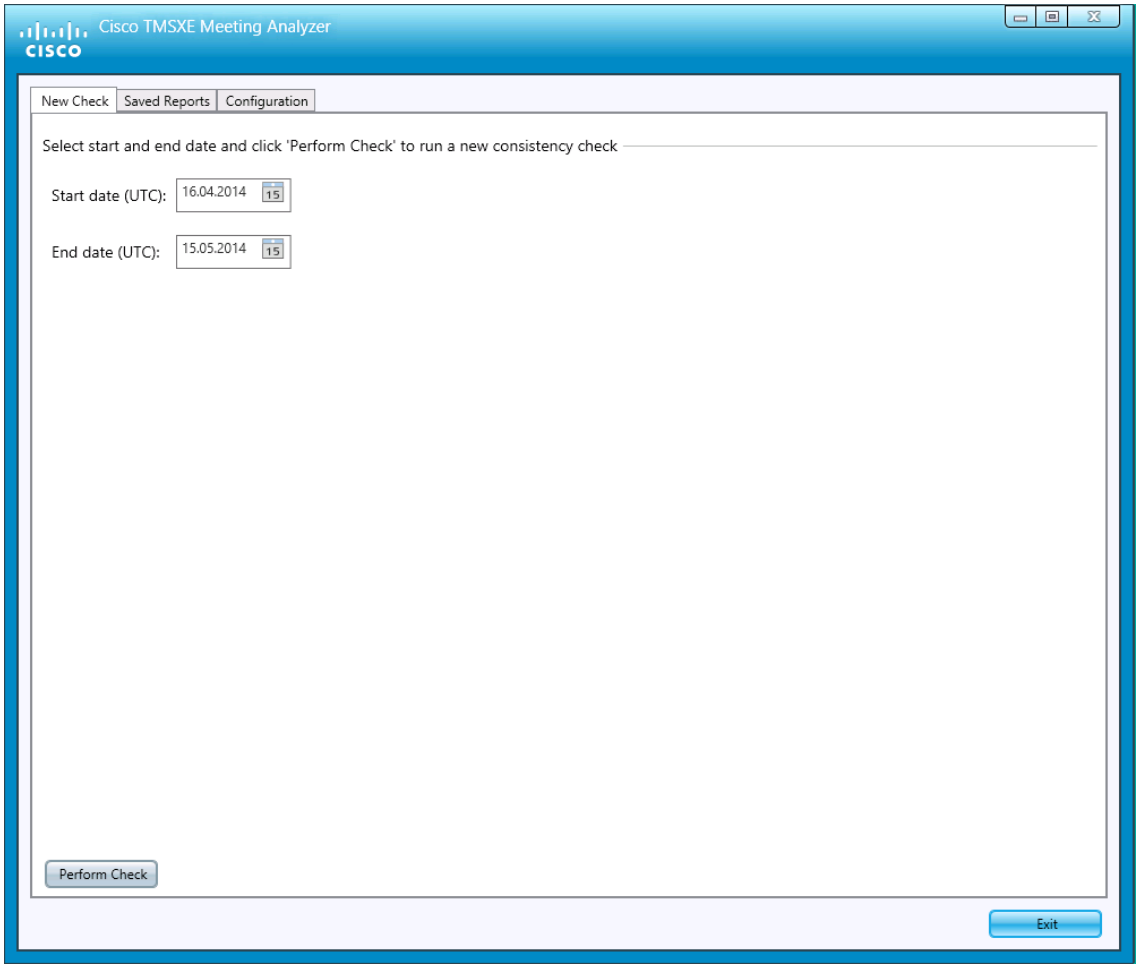
   Cisco TMS will now attempt to re-save all problematic conferences and series, re-routing any instances or series as necessary.

4. Click Refresh to see an updated status field for each entry. When no more entries are in the *Autocorrect Pending* state, go through any remaining entries one by one to determine what caused the booking to be defective and how to resolve it:
   a. Click on the conference title to view the conference information page.
   b. Click on the **Event Log** tab on the lower half of the conference information page. The log will display detail on the routing and/or resource issue.
   c. Click **Edit** and update the booking properties as required to resolve the issue; typically:
      - If the problem is a temporary lack of bridge resources, the conference must be moved or made less resource intensive (remove participants).
      - If the problem is a permanent lack of bridge resources, the environment needs more resources before the booking can be resolved.

   The Cisco TMS booking interface will only allow you to save your changes if the changes resolve all the booking issues. Meetings cannot be saved as *Defective* when booking from Cisco TMS itself.

Identifying Inconsistencies between Cisco TMS and Cisco TMSXE

The Cisco TMSXE Meeting Analyzer, that is installed alongside Cisco TMSXE on the server, helps administrators and support engineers identify discrepancies between bookings in Cisco TMS and Exchange.



Process Overview

Running Meeting Analyzer will:

- get all bookings–conferences from Cisco TMS and meetings from Exchange–that include rooms monitored by Cisco TMSXE.
- compare the properties of each booking between the two sources, highlighting any discrepancies in a report.
- highlight any meetings that exists in only one of the systems.

The following properties are compared:

- Whether the meeting is part of a recurrent series (recurrence patterns are not compared)
- Start time, in UTC
- End time, in UTC
- Participants that are systems added to Cisco TMSXE
- Cisco TMS title/Exchange subject if **Include meeting titles in consistency check** is enabled

Any meetings that are being replicated while the Meeting Analyzer is running will be shown as erroneous until replication has completed.

Best Practices

Do not make changes to Cisco TMSXE configuration while Meeting Analyzer is running. Meeting Analyzer loads this configuration on startup only.

As running Meeting Analyzer leads to significant load on the server, especially with a large selected date range and number of bookings, we strongly recommend that you run Meeting Analyzer:

- off hours.
- with the shortest possible date range if urgent troubleshooting is needed during business hours, to reduce impact on server performance.

Changing the Default Configuration

Use the Configuration tab to change the storage location and file name pattern for reports, and default time range for consistency checks.

Note that unless you use a variable in the report file name, each new report will overwrite the previous one. The default name pattern is BookingConsistencyCheckResult-{{timestamp}}.xml.

You can also enable **Include meeting titles in consistency check** to make Meeting Analyzer compare titles from Cisco TMS with subjects from Exchange.

Performing an Immediate Check

1. Start the tool, located in **Start > All Programs > Cisco > Cisco TMSXE Meeting Analyzer**.
2. Specify the date range for which to check booking consistency.

   You can use the date picker or type the date directly.

   The default date range is 1 month, the maximum date range is 2 years.

3. Click **Run**.

   Depending on the size of the database, the consistency check may take a long time. When the check is complete, a report of bookings with inconsistencies will be displayed as a table with Cisco TMS data on the left and Exchange data on the right.

   All meetings are displayed as series, and any inconsistency at an instance level will also be flagged on the series level.

   If there is a participant mismatch, it will be displayed on the side of the system that has a participant with no match.

4. Click the plus sign next to a list entry to drill down and see details.

   Inconsistent properties are highlighted in red.

5. Click **Save** to store the report before exiting the tool.

You can access reports from previous consistency checks by going to the Saved Reports tab.

Resolving and Avoiding Inconsistencies

Should Exchange contain the correct information for a meeting that is missing or incorrect in Cisco TMS, you must ask the organizer to re-send the meeting invitation for the information to replicate to Cisco TMS.

One root cause for Cisco TMS and Exchange becoming out of sync is users updating or cancelling bookings in Outlook without sending updates to all participants. Let your users know that sending updates is a best practice and required to keep calendars in sync. This is also covered in *Cisco TMSXE User Guide*.

Re-setting the transaction ID to 0 causes Cisco TMSXE to re-replicate all bookings with Cisco TMS as the master. This will resolve most inconsistencies that may arise where Cisco TMS is presumed to be correct.

In the case of the replicator from Cisco TMS to Cisco TMSXE hanging, which would cause a large amount of inconsistencies, try restarting the service. If this is not successful, contact your Cisco support representative.

Setting Up a Scheduled Task

To perform a regular analysis of booking consistency, we recommend setting up a scheduled Windows task using the command-line interface for Meeting Analyzer.

To access CLI, run MeetingAnalyzerCommand.exe. The configuration tool is located in the Cisco TMSXE installation folder. The default program path is C:\Program Files\Cisco\TMSXE\MeetingAnalyzerCommand.exe.

Run the tool directly from its location. The command may not include the entire file path.

Table 7 Command-line interface reference

Switch	Parameter	Description
`help`	–	Output a list of supported commands.
`noOfDays`	Integer, maximum 730	The number of days starting from today's date to include in the analysis.
`filename`	Complete file name or name pattern with a .xml extension	Write to file with either: ■ a given name (report is overwritten on each analysis) ■ a name with the given pattern. The default name pattern is MeetingAnalyzerReport-{{timestamp}}.xml.

For instructions on setting up scheduled tasks in Windows Server 2012, see the Microsoft article *Configure a Scheduled Task Item*.

License Check Fails After Reinstalling

If performing a reinstallation rather than an upgrade, the Cisco TMS license check for Cisco TMSXE may fail.

To resolve this, do one of the following:

- Perform an IIS reset on Cisco TMS. If the setup is redundant, do this on both nodes.
- Wait 30 minutes before restarting the Cisco TMSXE configuration tool and connecting to Cisco TMS.

Time Zone Change Caveat

If the Cisco TMSXE server's time zone is modified while the Cisco TMSXE service is running, bookings will stop replicating between Cisco TMS and Exchange.

Should this happen, perform the following procedure:

1. Stop the TMSXE service.
2. Open the Cisco TMSXE ProgramData folder (default location C:\ProgramData\Cisco\TMSXE\, a hidden folder).
3. Rename the Storage folder to **Storage.old**.
4. Restart the TMSXE service.

The Storage folder will be recreated by Cisco TMSXE and booking replication will resume.

Using Cisco TelePresence Form requires 'custom form scripts' to be enabled

Cisco TelePresence form does not work with Outlook as Microsoft disabled the custom form script by default. To enable the custom form script, you must update the Outlook client and then set the Registry Keys. To set the Registry Keys, refer to Custom form script is now disabled by default article.

Appendixes

Appendix 1: Configuring Exchange 2010 Without Mailbox Impersonation

If not enabling the **Mailbox Impersonation** setting, which allows the Cisco TMSXE user to impersonate any resource mailbox, you must instead:

- Grant Full Access Permissions to the service user.
- Apply a throttling policy for Exchange.

Both procedures are described below.

Granting Full Access Permissions to the Service User

There are two ways to do grant these permissions.

Using Exchange Management Console:

1. Use the EMC console tree to navigate to **Recipient Configuration > Mailbox** and select the mailbox you want to configure.
2. Right-click on the room mailbox and select **Manage Full Access Permissions...**.
3. Click **Add...**.
4. Add the previously created Cisco TMSXE service user and click **Manage**.
5. Click **Finish**.

If using the Exchange Management Shell:

Enter the following commands, replacing **[mailbox]** with the name of the mailbox you are configuring, **@** sign and domain not included:

```
Add-MailboxPermission -identity [mailbox] -User [service user] -AccessRights FullAccess.
```

Repeat one of these procedures for each mailbox.

Applying the Cisco TMSXE Throttling Policy for Exchange 2010

This section is only relevant to administrators deploying Cisco TMSXE with Exchange 2010.

With Exchange 2010 SP1, Microsoft has enabled the client throttling policy feature by default. For more information, see the Microsoft article *Understanding Client Throttling Policies*.

If no throttling policy has been configured, Microsoft will apply a default policy to all users. The default throttling policy is tailored for user load and not for an enterprise application like Cisco TMSXE.

In order for all Cisco TMSXE features to work, a custom throttling policy must be applied to the Cisco TMSXE application user.

To apply the Cisco TMSXE throttling policy:

1. Log in to the Exchange 2010 CAS server.
2. Open Exchange Management Shell.

3. Create a custom throttling policy:
   a. `New-ThrottlingPolicy Cisco_TMSXE_ThrottlingPolicy`
   b. `Set-ThrottlingPolicy -Identity Cisco_TMSXE_ThrottlingPolicy -EWSFastSearchTimeoutInSeconds 300 -EWSFindCountLimit 6000 -EWSMaxConcurrency $null -EWSMaxSubscriptions 5000 -EWSPercentTimeInAD 200 -EWSPercentTimeInMailboxRPC 300 -EWSPercentTimeInCAS 500`
4. Assign the policy to the Cisco TMSXE user:
   a. `$b = Get-ThrottlingPolicy Cisco_TMSXE_ThrottlingPolicy`
   b. `Set-Mailbox -Identity [service user] -ThrottlingPolicy $b`

Note that if you encounter any errors after applying the Cisco TMSXE throttling policy, you can revert back to the Microsoft throttling policy, see Restoring the Microsoft Throttling Policy, page 98.

Throttling Policy Parameter Definitions and Values

The default values used in the above steps satisfy most Cisco TMSXE deployments. If your deployment requires adjustments, you can adjust the Set-ThrottlingPolicy values and rerun step 3b above.

The table below describes each of the parameters and values for the Set-Throttling Policy command of Exchange 2010 SP1.

Parameter name	Description	Cisco TMSXE Default	Note
EWSFastSearchTimeoutInSeconds	Specifies the amount of time that searches made using Exchange Web Services continue before they time out. If the search takes more than the time indicated by the policy value, the search stops and an error is returned.	300	Each Cisco TMSXE call has a default time out of 180 second. 300 is granted since each call could be phased out.
EWSFindCountLimit	The maximum result size of FindItem or FindFolder calls that can exist in memory on the Client Access server at the same time for this user in this current process. If an attempt is made to find more items or folders than your policy limit allows, an error is returned. However, the limit isn't strictly enforced if the call is made within the context of an indexed page view. Specifically, in this scenario, the search results are truncated to include the number of items and folders that fit within the policy limit. You can then continue paging into your results set using additional FindItem or FindFolder calls.	6000	This parameter governs the maximum number of entries for all requests combined at a given time. Cisco TMSXE only requests for 200 entries to be returned.

Parameter name	Description	Cisco TMSXE Default	Note
EWSMaxConcurrency	How many concurrent connections an Exchange Web Services user can have against an Exchange server at one time. A connection is held from the moment a request is received until a response is sent in its entirety to the requestor. If users attempt to make more concurrent requests than their policy allows, the new connection attempt fails. However, existing connections remain valid. The EWSMaxConcurrency parameter has a valid range from 0 through 100 inclusive.	$null	Due to the nature of EWS notification, you can't measure the number of concurrent requests. $null value is required to indicate that no throttling is necessary for this criteria.
EWSPercentTimeInAD	The percentage of a minute that an Exchange Web Services user can spend executing LDAP requests (PercentTimeInAD). A value of 100 indicates that for every one-minute window, the user can spend 60 seconds of that time consuming the resource in question.	200	The value is higher than 100 since this counts for all concurrent requests at any given time.
EWSPercentTimeInMailbox RPC	The percentage of a minute that an Exchange Web Services user can spend executing mailbox RPC requests (PercentTimeInMailboxRPC).	300	The value is higher than 100 since it counts for all concurrent requests at any given time.
EWSPercentTimeInCAS	The percentage of a minute that an Exchange Web Services user can spend executing Client Access server code (PercentTimeInCAS).	500	The value is higher than 100 since this counts for all concurrent requests at any given time.
EWSMaxSubscriptions	The maximum number of active push and pull subscriptions that a user can have on a specific Client Access server at the same time. If a user tries to create more subscriptions than the configured maximum, the subscription fails, and an event is logged in Event Viewer.	5000	Set to (2 * the number of managed rooms). We recommend that you allocate a number that allows for future growth.

Restoring the Microsoft Throttling Policy

If for any reason you encounter errors applying the Cisco TMSXE throttling policy for Exchange 2010 SP1, you can revert back to the default Microsoft throttling policy:

1. Log in to the CAS server for Exchange 2010.
2. Open Exchange Management Shell application.
3. Remove Throttling policy association from Cisco TMSXE application user: `Set-Mailbox -Identity [service user] -ThrottlingPolicy $null`.
4. Remove the custom policy: `Remove-ThrottlingPolicy Cisco_TMSXE_ThrottlingPolicy`.

Appendix 2: Setting up Cisco TMSXE Without an Active Directory Connection

Cisco TMSXE can be used in deployments where the Active Directory domain cannot be reached by Cisco TMSXE.

Note that in this deployment scenario, the information about users available to Cisco TMSXE and Cisco TMS will be very limited.

Caution: Before you start deploying Cisco TMSXE in this mode, consult with your Cisco **account team. This mode of operation is only recommended for scenarios with very particular requirements. Once operational, the setting cannot be reverted.**

Booking Ownership

Cisco TMSXE passes the email address of the organizer to Cisco TMS, which will attempt to resolve this to the email address of an existing user. Booking ownership will then be assigned as follows:

- If the email address matches an existing user, that user will own the booking.
- If no current user matches the address, but AD lookup is enabled and a match is found in AD, the user will be added to Cisco TMS as the owner of the booking.
- If no user matches the address, and no user is found in AD or lookup is not enabled, behavior depends on the Cisco TMSXE setting **Allow organizers without usernames (Non-AD Mode only)**:
  - If enabled, Cisco TMS will create a special user based on the email address. This user will not be able to log into Cisco TMS, but will have ownership of all bookings made from the same address.
  - If disabled, all meetings booked through Cisco TMSXE from this address will be owned by the service user, and not linked to the individual organizer in Cisco TMS.

Installing with Non-AD Mode

To run Cisco TMSXE in Non-Active Directory Mode, select **Non-Active Directory Mode** in the **Active Directory Settings** tab.

Then follow the regular instructions for installation in this document until you get to the configuration stage.

Configuring Non-AD Mode

- On the Active Directory Settings tab of the configuration tool, select **Non-Active Directory Mode**.

  Confirm by clicking **Go to Non-AD Mode** in the dialog that opens.

- On the Active Directory Settings tab, determine whether to enable **Allow organizers without Cisco TMS username (Non AD-mode only)**.
  - Enabling this setting makes the organizer the owner of the meeting in Cisco TMS. If a user corresponding to the organizer's email address does not exist, Cisco TMS will create it.
  - Disabling this setting will make the service user in Cisco TMS the owner of all bookings from Cisco TMSXE.

Cisco Collaboration Meeting Rooms Hybrid

For Cisco Collaboration Meeting Rooms Hybrid to work with Non-AD Mode:

- **Allow organizers without usernames** must be enabled.
- Cisco TMS must be pre-populated with user profiles that correspond to email addresses in Exchange.
- Webex Single Sign On must be enabled in Cisco TMS, or each user profile must be pre-populated with Webex credentials.

Productivity Tools will not work in Non-AD Mode.

Limitations

The following restrictions apply when using Non-AD Mode:

- Only Cisco TMS administrators may update Cisco TMSXE-created bookings from Cisco TMS.
- If **Allow organizers without usernames** is enabled, user email addresses must not be changed in Cisco TMS, as this will break the connection between user and bookings.

  If AD lookup is not enabled in Cisco TMS, any user can change their own email address. We therefore strongly recommend blocking all direct access to Cisco TMS for Cisco TMSXE end users.

- Productivity Tools are not compatible with Non-AD Mode.

Appendix 3: Monitoring Re-Replication When Upgrading from 3.0.x

The first time the service is launched after upgrade, a re-replication of all existing bookings in Cisco TMS will be performed.

With a large database, this process may take as long as 3-5 hours, but the application will be operative while this is ongoing.

If you want to monitor the re-replication at any stage, you must turn on DEBUG mode for the service log.

See How Logging Works, page 85 for instructions on locating and using the logs.

When the process has completed, an INFO message with the following statement will be added to the service log:

No changes on TMS

Notifications of series, single meetings, and occurrences that have been updated during re-replication, is logged in INFO messages. For example, a series or single meeting that did not exist in Exchange and has been replicated from Cisco TMS will be logged as "New item saved".

When a telepresence meeting exist in Exchange that does not exist in Cisco TMS, that meeting will be deleted. Most deletions are logged as "Deleting item of type", followed by a specification of which type of meeting is deleted. However, where several transactions are performed on the same meeting during re-replication, this may be logged differently.

To find the conference ID, read upwards from the appropriate log message to locate the closest "Cleaning up conference" message.

Note that re-replication only affects meetings that have not yet happened. If you see the message "Not updating", it means that a discrepancy was discovered that is in the past and will therefore not be corrected.

Restarting an Interrupted Upgrade

If the process is interrupted after installation is completed but before the configuration wizard is launched, the re-setting of the transaction IDs may not have been performed, and launching the Cisco TMSXE service will not initiate a re-replication.

To find out whether the transaction IDs have been reset, look in the configuration log for an INFO message containing the statement:

Finished resetting transaction id on all systems

See How Logging Works, page 85 for instructions on locating and using the logs.

You will also find separate statements for each affected system, including their Cisco TMS system IDs.

If you cannot find these statements, perform the following steps:

1. Open a command prompt.

   By default, the configuration tool is located in C:\Program Files\Cisco\TMSXE\ConfigurationApp.exe

2. Run the configuration tool using the switches `-wizard -resetAllTransactionIds`.

   The configuration tool starts up.

3. Follow the instructions in Appendix 3: Monitoring Re-Replication When Upgrading from 3.0.x, page 99 .

The -resetAllTransactionsIds switch

The `-resetAllTransactionIds` switch initiates a one-time cleanup of discrepancies between Cisco TMS and Exchange.

Caution: The re-replication process may take a long time to complete and must be performed off-hours, as calendars will be out of sync until the process has completed.

Appendix 4: Performing a Trial Import of Existing Meetings

When repurposing resource mailboxes that already include upcoming, scheduled meetings, you can use the Cisco TMSXE trial import feature to see which meetings will be bookable in Cisco TMS.

You must not have any systems in Cisco TMSXE prior to running the trial import, and after it has completed, Cisco TMS and Cisco TMSXE must both be re-set.

1. Take a snapshot of the Cisco TMS database using standard SQL tools.
2. Run the Cisco TMSXE installer with the command line parameter `TRIALIMPORT=1`.
3. When the configuration tool launches, configure the Cisco TMS and Exchange connections.
4. On the Systems tab, add a compiled .csv file of mailbox addresses mapped to the corresponding systems in Cisco TMS.
5. Complete configuration and start the Cisco TMSXE service when prompted.
   - The service stops automatically after the trial import has completed.
   - The decline and downgrade log lets you know which meetings could not be imported and why.
   - Cisco TMS **Booking > List Conferences** or **Administrative Tools > Diagnostics > Conference Diagnostics** can be used to identify any bookings saved as *Defective* in Cisco TMS.

To get products into a functional state after a trial import, you have to:

1. Restore the Cisco TMS database snapshot.
2. Reset Cisco TMSXE:
   a. From the Cisco TMSXE program folder, run the command `ConfigurationApp.exe -EndTrialImportMode` to disable trial import mode without opening the configuration tool itself.
   b. In the Services panel, disable the Cisco TMSXE Windows service.

      The service must remain disabled until you are ready to perform a final import.

   c. The systems you added during trial import are stored in the MonitoredSystems.xml file in the Cisco TMSXE configuration folder.
      - Keep this file if you will import meetings from the same endpoints mapped to the same mailboxes again.
      - Remove the file to be able to import using a different endpoint/mailbox setup.

Appendix 5: Proxy Configuration

Introduction

Cisco TMSXE is a server-based application written in .NET. This allows to utilize custom configuration files for Cisco TMSXE executables to allow the use of system level proxy settings. This would override the proxy setting configurations within the user profiles of the contexts, that the executables are ran under. The following three executables need to be considered when configuring the proxy settings:

1. **Cisco TMSXEService.exe** : The main Windows Service executable of the Cisco TMSXE service.
2. **ConfigurationApp.exe** : The executable for the Cisco TMSXE Configuration tool.
3. **MeetingAnalyzeApp.exe** : The executable for the Cisco TMSXE Meeting Analyzer tool.

Beginning within the installation of Cisco TMSXE 5.9, each of these executables has a default blank configuration file. The configuration file exists along with each executable and is named as the full name of the executable with the file extension as "**config**". For example:

Executable File Name	Configuration File Name
Cisco TMSXEService.exe	Cisco TMSXEService.exe.config
ConfigurationApp.exe	ConfigurationApp.exe.config
MeetingAnalyzerApp.exe	MeetingAnalyzerApp.exe.config

Sample configuration files are also included along with the executable and configuration files. These sample configuration files have the file extension of "**sample**". For Example:

Configuration File Name	Sample Configuration File Name
Cisco TMSXEService.exe.config	Cisco TMSXEService.exe.config.sample
ConfigurationApp.exe.config	ConfigurationApp.exe.config.sample
MeetingAnalyzerApp.exe.config	MeetingAnalyzerApp.exe.config.sample

Each of the sample configuration files contains a link to the Microsoft publish documentation for the "defaultProxy" element of the "system.net" section of the .NET configuration file, as well as a few basic examples of common configurations. defaultProxy Element

To use the sample configuration files, for each of the three executable config files, do the following:

1. Backup the current config file.
2. Copy the config.sample file to be the new config file.
3. Edit the new config file as needed.

The use of these custom config files will override any proxy configuration that currently exists for the user context that the executables are ran under. For the Cisco TMSXEService.exe executable, this is the executable of the Windows Service for Cisco TMSXE, and runs under the user context of the local system account "Network Service". The other two executables run under the user context of the Windows user that is logged into the Windows Server at the time of running the applications of the Cisco TMSXE Configuration application and the Meeting Analyzer application.

The first property that needs to be configured is the value for "**proxyaddress**".

Change the current value to the proper proxy server location that the Cisco TMSXE executable must use.

Configuring a bypass list is optional, depending upon the requirements of the over-all deployment.

These configuration files are for the local installation of Cisco TMSXE. If the deployment is of a clustered design, this custom configuration must be done on each Cisco TMSXE node.

This method for utilizing a proxy server for the Cisco TMSXE executables has been tested with proxy servers that do not require user authentication.

Upgrade Cisco TMSXE

To upgrade Cisco TMSXE application that has the proxy configuration, do the following for three executable config files:

1. Backup the current config file with proxy settings and rename it to **config.Proxy**
2. Complete the Cisco TMSXE application upgrade.
3. Edit the new config file created during upgrade, and add the required proxy settings from **config.Proxy** file.

Appendix 6: Application Registration in the Microsoft Azure Portal

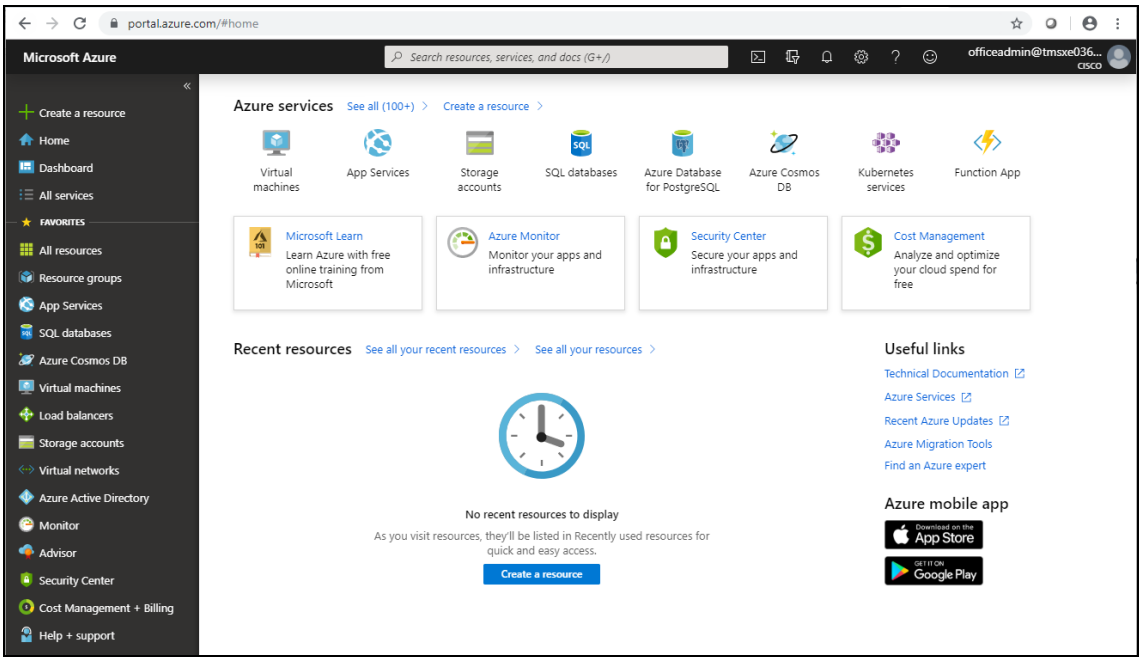
Configuration of OAuth for Office 365(modern authentication) in Exchange Web Services tab of Cisco TMSXEapplication involves the following two steps:

1. Application Registration in the Microsoft Azure Portal, page 102
   Note: This is one-time activity.
2. OAuth for Office 365 configuration in Cisco TMSXE configuration tool, page 110

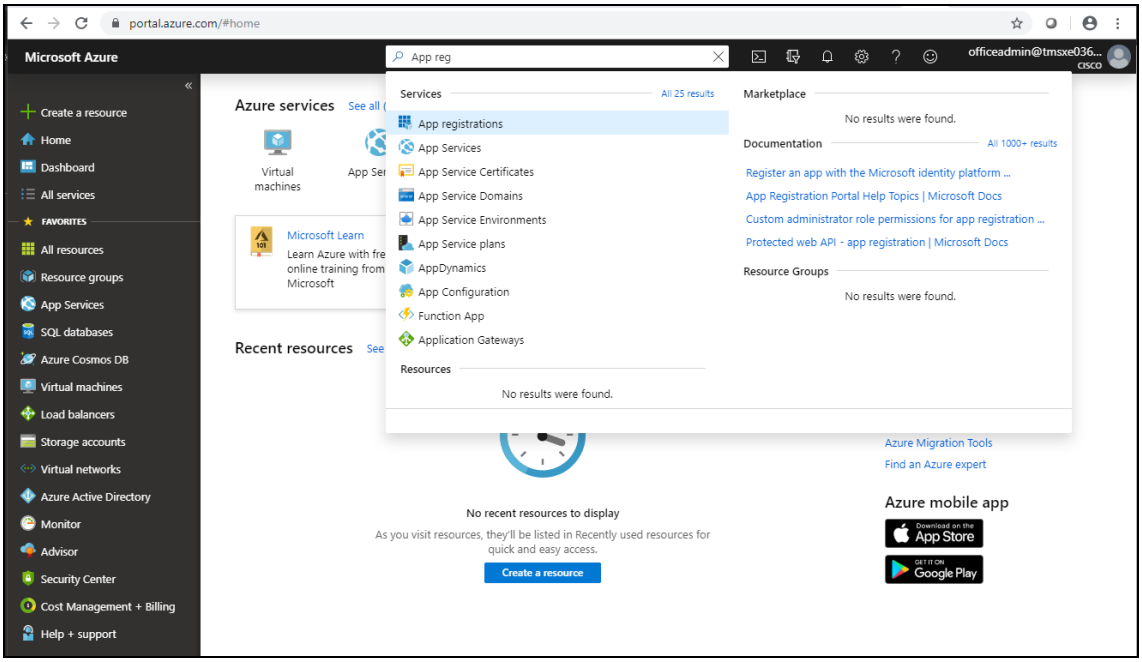
Application Registration in the Microsoft Azure Portal

Following are the steps to register Cisco TMSXE application in Azure Active Directory.

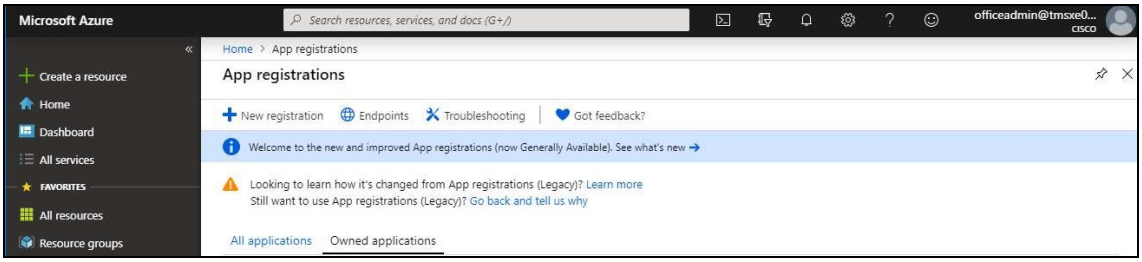
1. Login to https://portal.azure.com using **administrator** credentials.



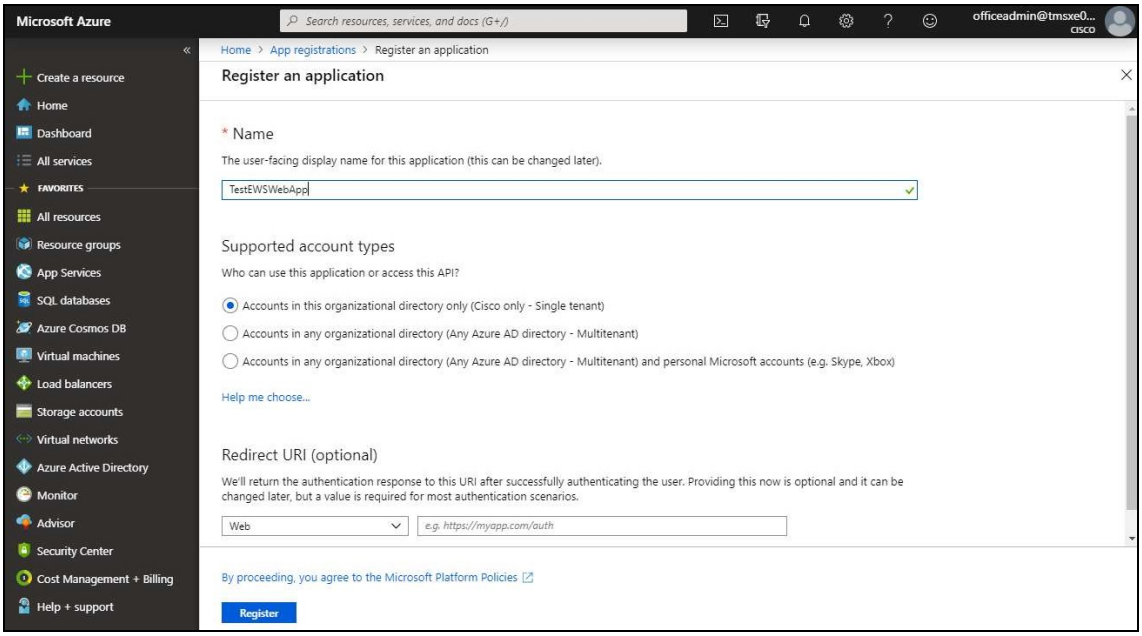
2. Search for '**App reg**' in the Search bar and select '**App registrations**' listed under **Services**.



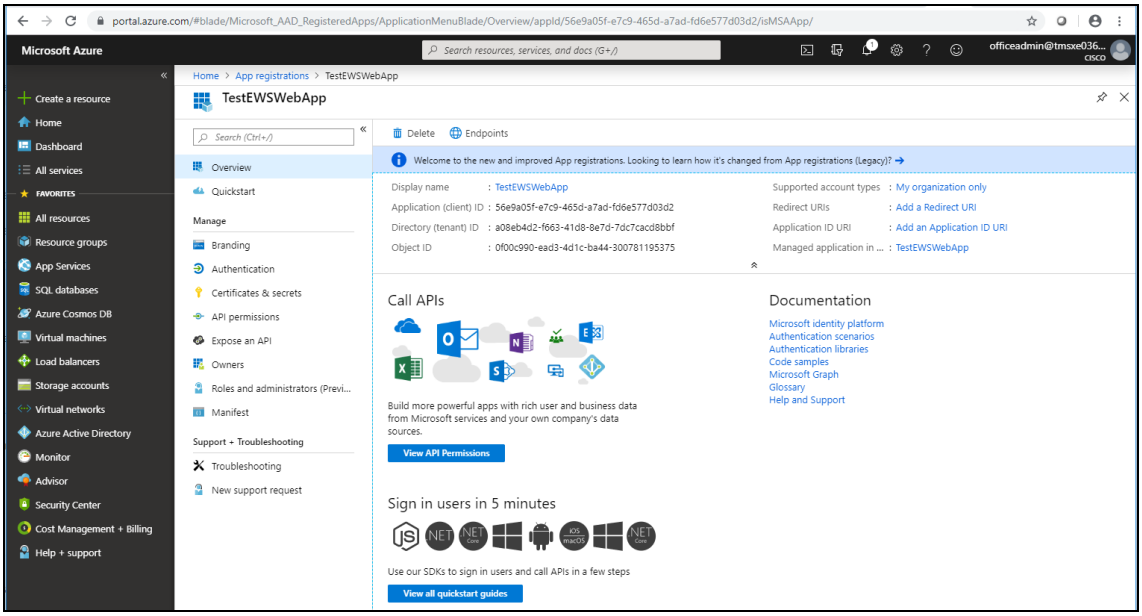
3. Click '**+ New registration**' to register the new application.



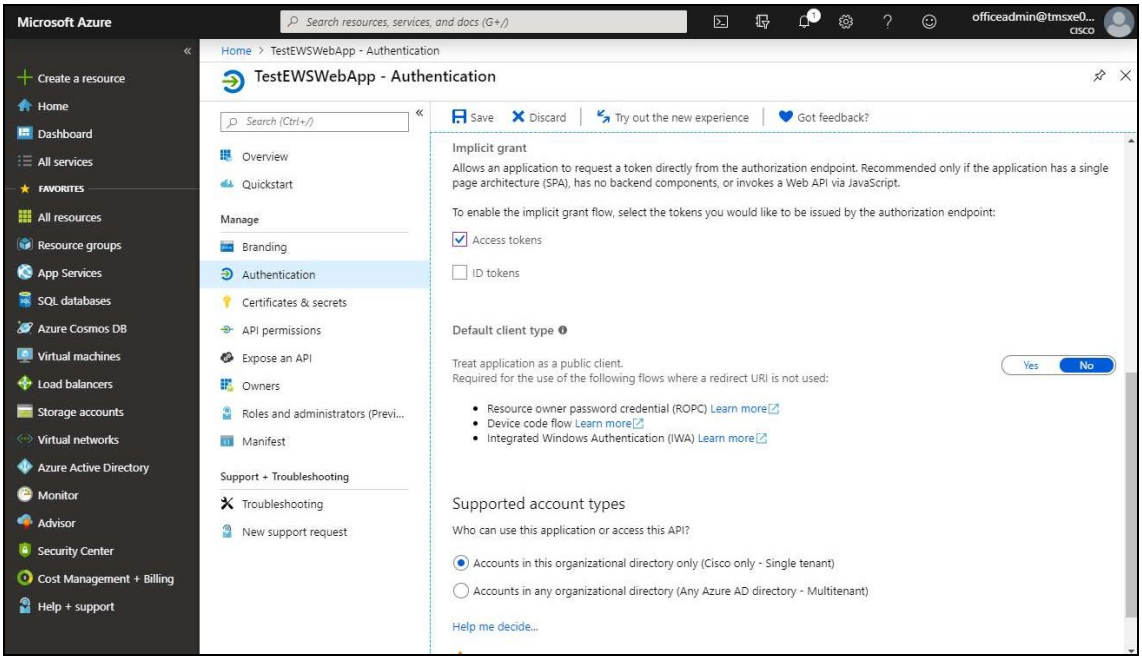
4. Enter the preferred naming convention that can be identified as Cisco TMSXE. Select the supported account types and click '**Register**'.
Note: It is recommended to select ' Accounts in this organizational directory only'



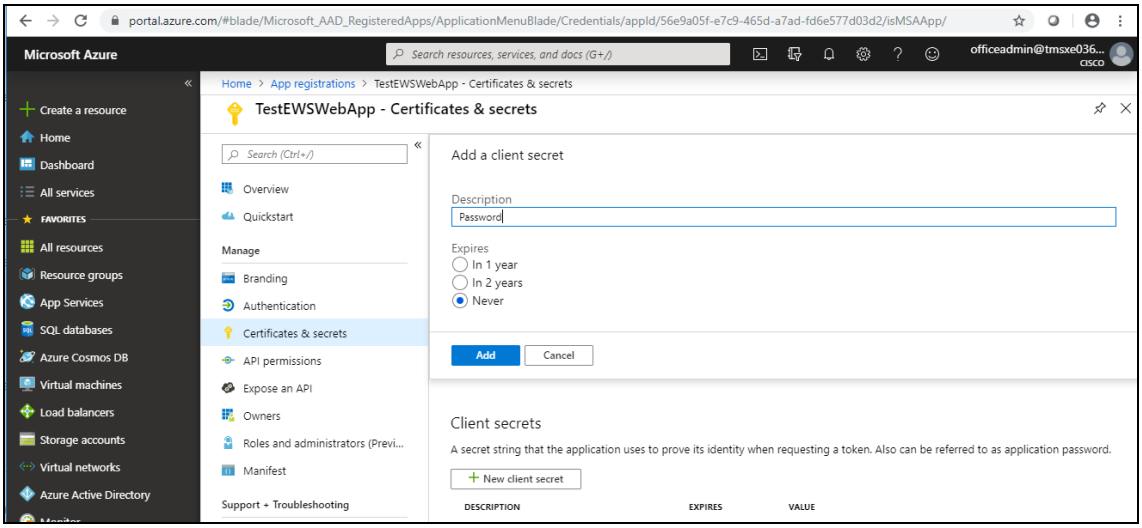
5. Click **Overview** and make a note of the Application (client) ID, Directory (tenant) ID.

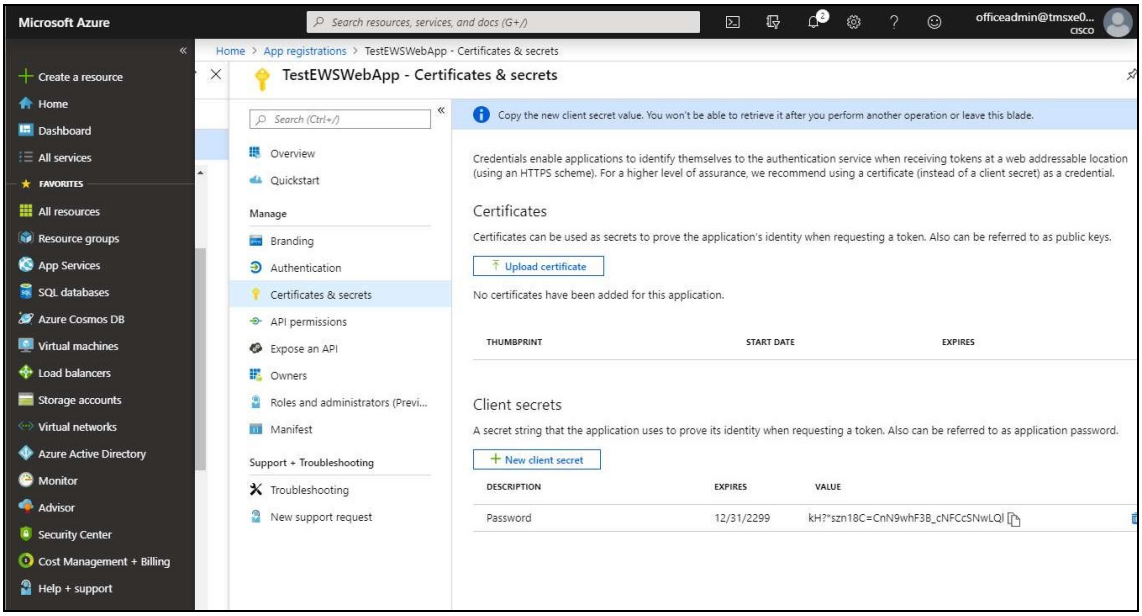


6. Select **Authentication** option
7. Select '**Access tokens**' check box.
8. Select ' **Accounts in this organizational directory only**' from **Supported account types** section.
   Note: This is the recommended option.
9. Click **Save**.

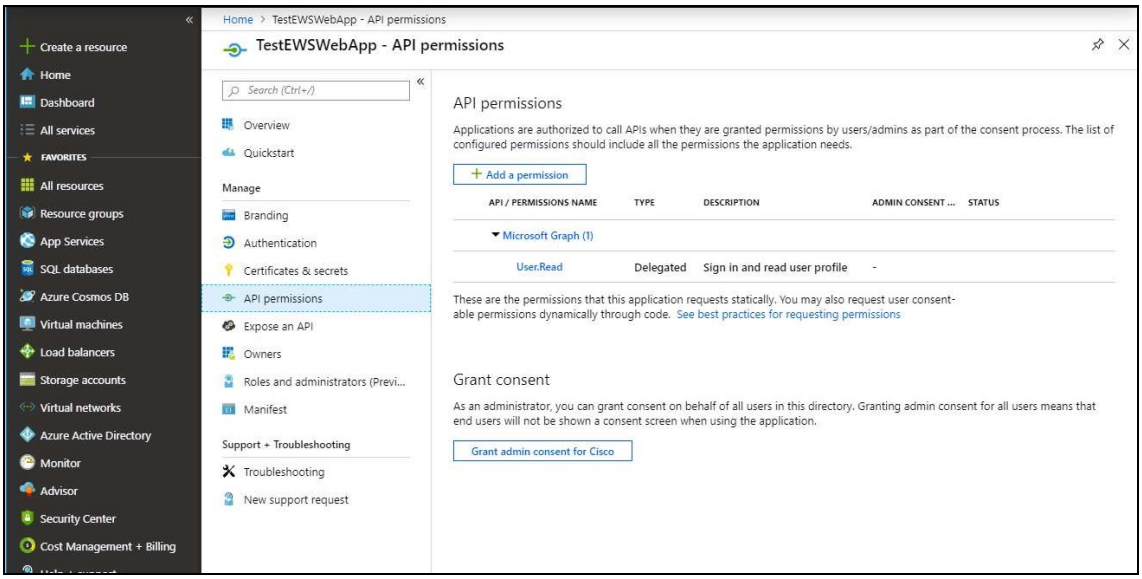


10. Click '**Certificates & Secrets: Create "New client secret**', enter a description about the secret key in '**Description**' text box, select '**Never**' option from '**Expires**' section and click **Add** to generate the secret key. Make a copy of the secret key value and keep it safe. This is one of the three required fields for OAuth for Office 365 (modern authentication) configuration in Cisco TMSXE Configuration tool.

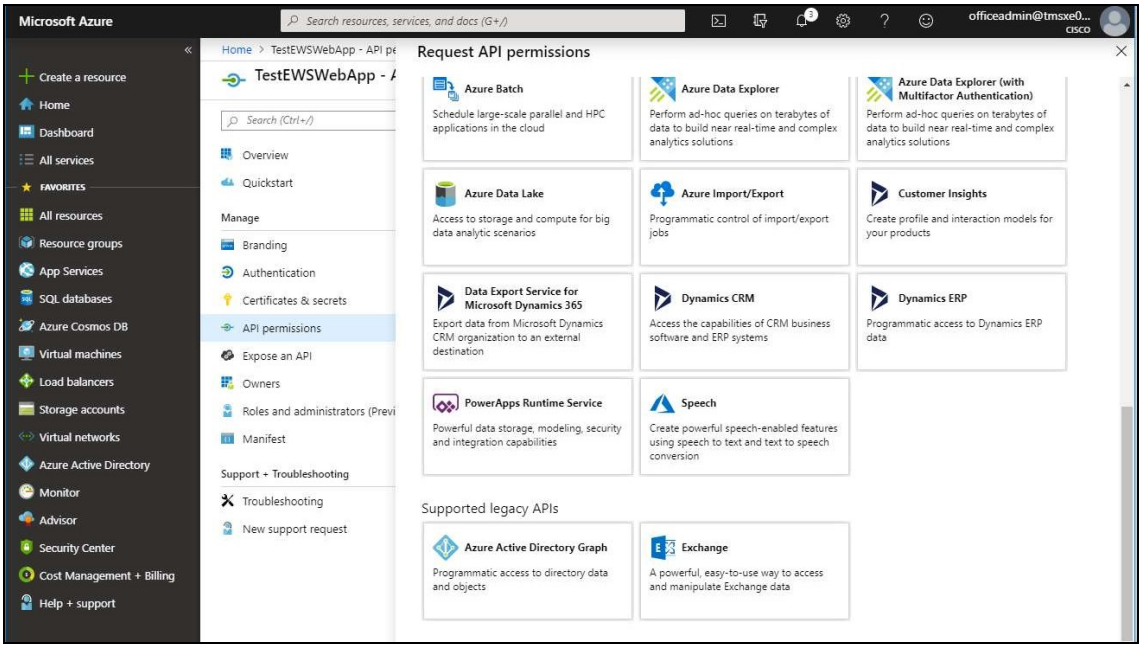


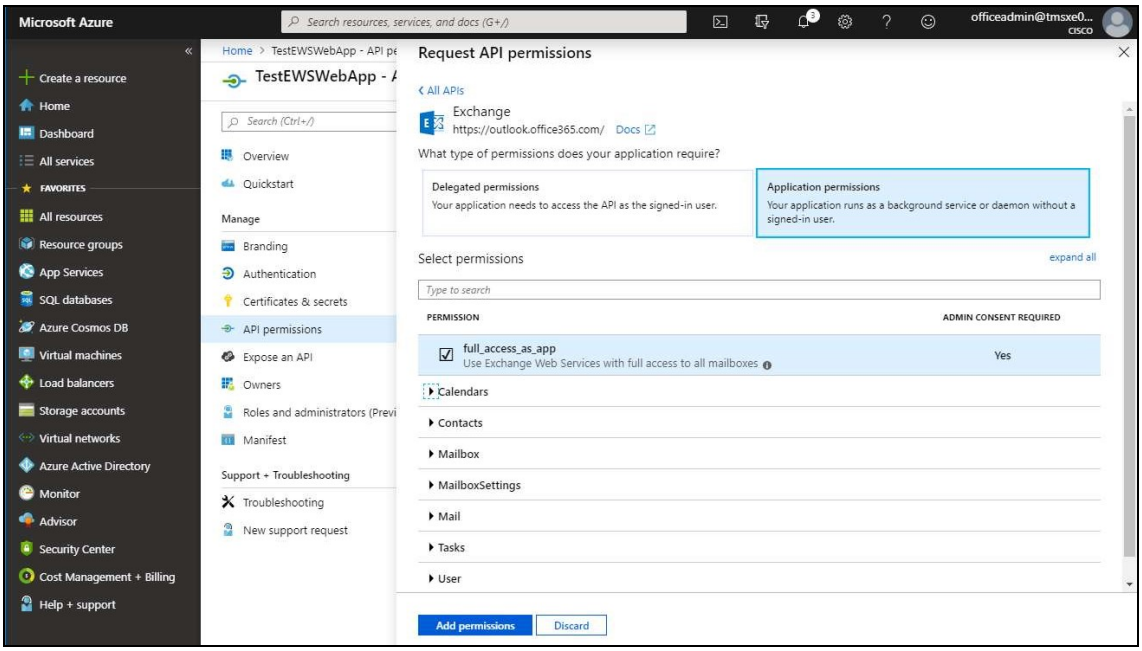


11. Click **API permissions> + Add Permissions**.


Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Home > TestEWSWebApp - API permissions
TestEWSWebApp - API permissions
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
API permissions
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs.
Add a permission
API / PERMISSIONS NAME
TYPE
DESCRIPTION
ADMIN CONSENT ...
STATUS
Microsoft Graph (1)
User.Read
Delegated
Sign in and read user profile
-
These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions
Grant consent
As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.
Grant admin consent for Cisco

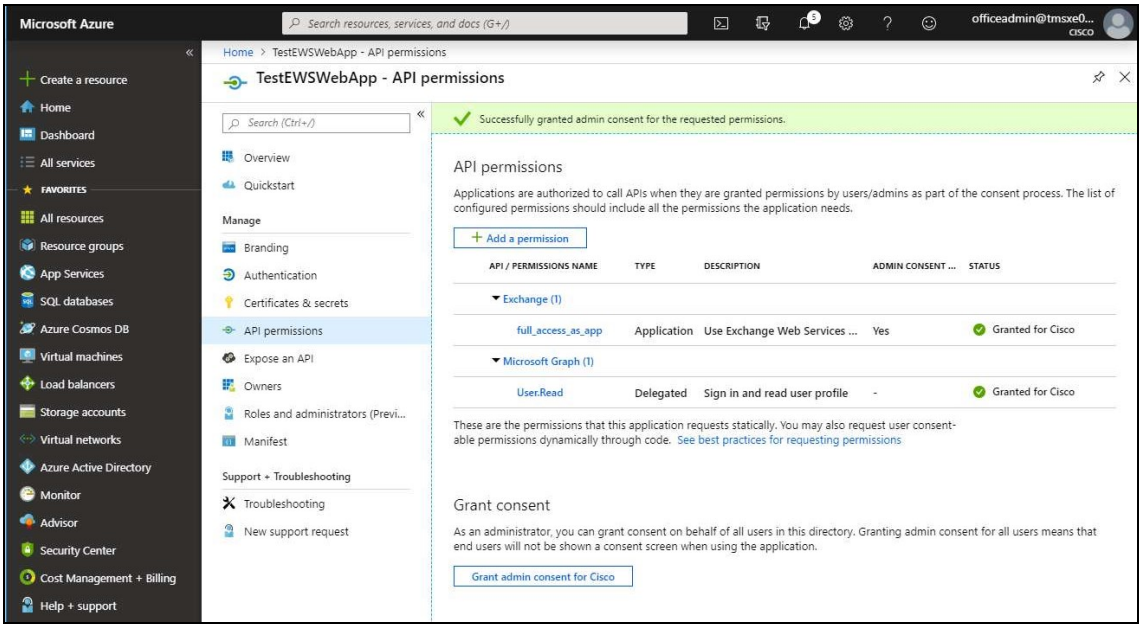
12. Select '**Exchange> Application permissions**.



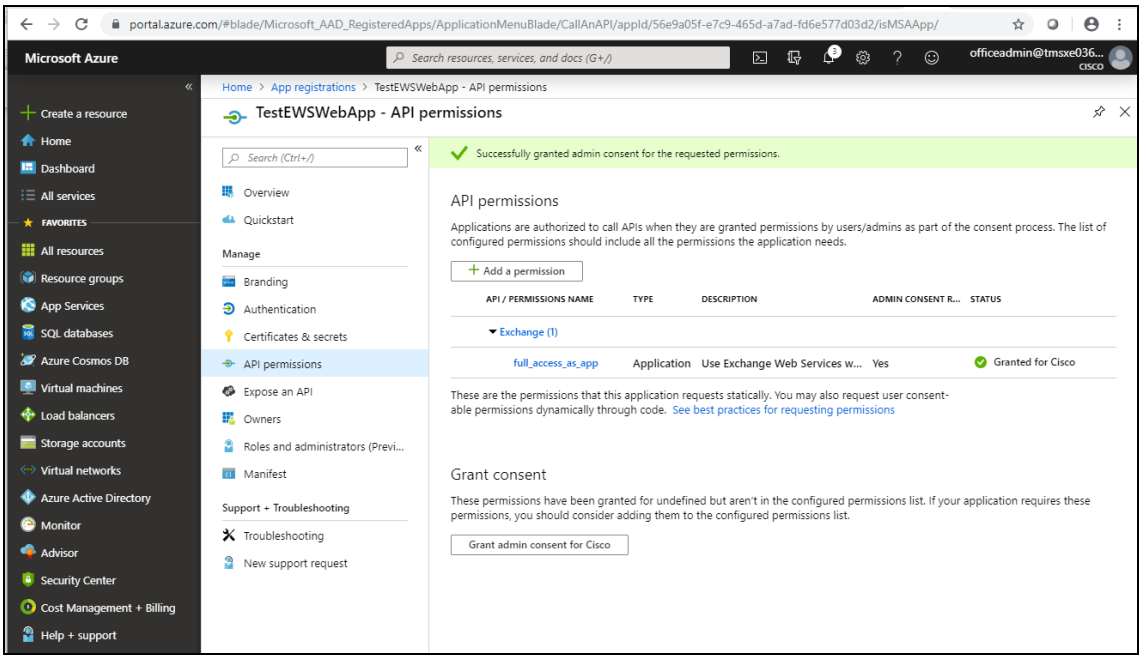


13. Select '**full_access_as_app**' check box and click **Add permissions**.

14. Click **API Permissions > Grant consent > Grant Admin consent for Cisco.**



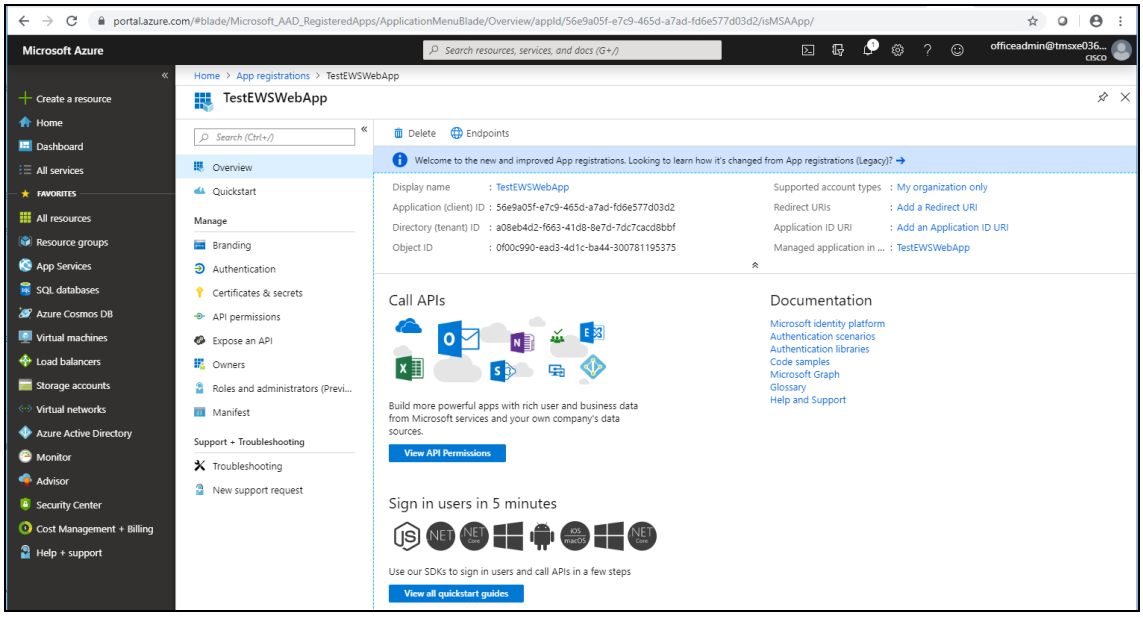
15. Click **Microsoft Graph** (if available) and un-check '**User.Read**' option and click **Update Permissions**.
16. Click **API Permissions > Grant consent > Grant Admin consent for Cisco.**



The application registration procedure for Cisco TMSXE application in Microsoft Azure portal is completed.

The Tenant ID, Application ID and Secret key obtained from the above steps will be used in OAuth for Office 365 in Cisco TMSXE configuration.

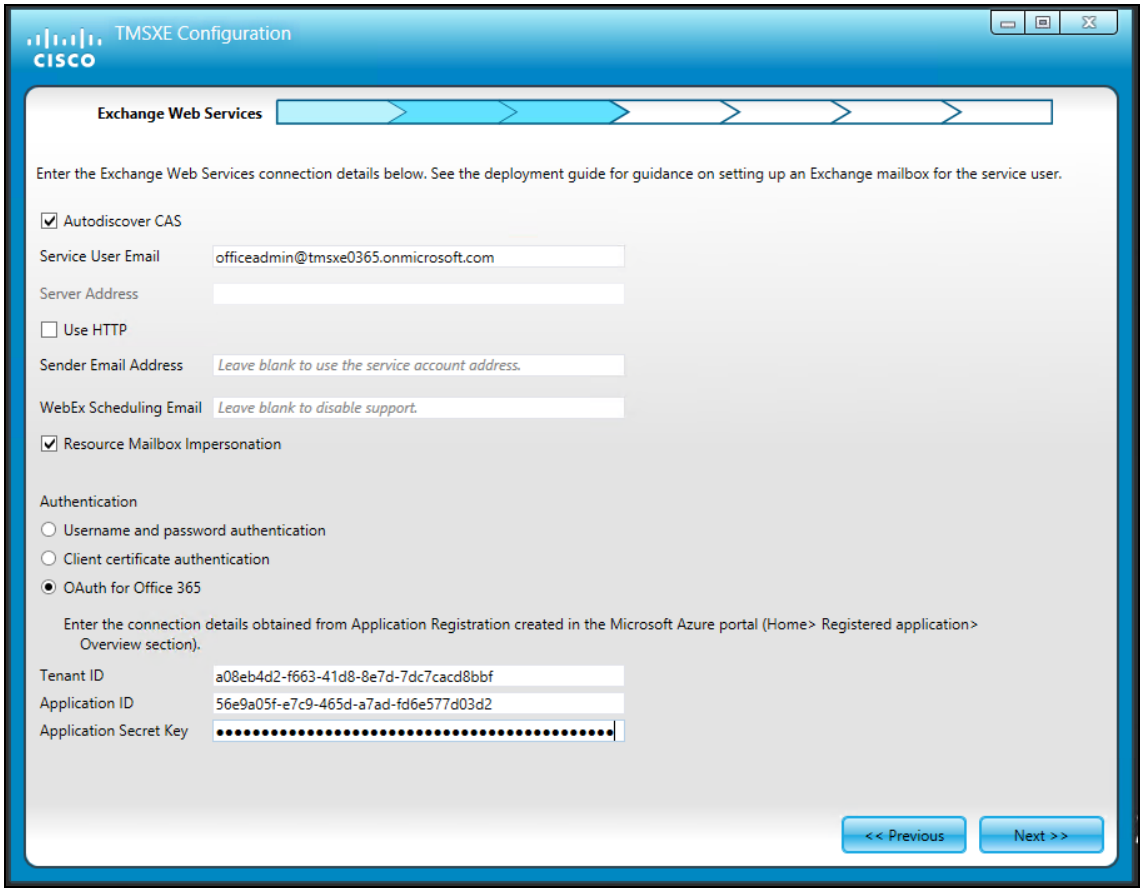
Note: The Tenant ID, Application ID details can be obtained from Overview section.



The Client secret key (For more information refer to Step 10) is required and must be given in the Cisco TMSXE user interface.

OAuth for Office 365 configuration in Cisco TMSXE configuration tool

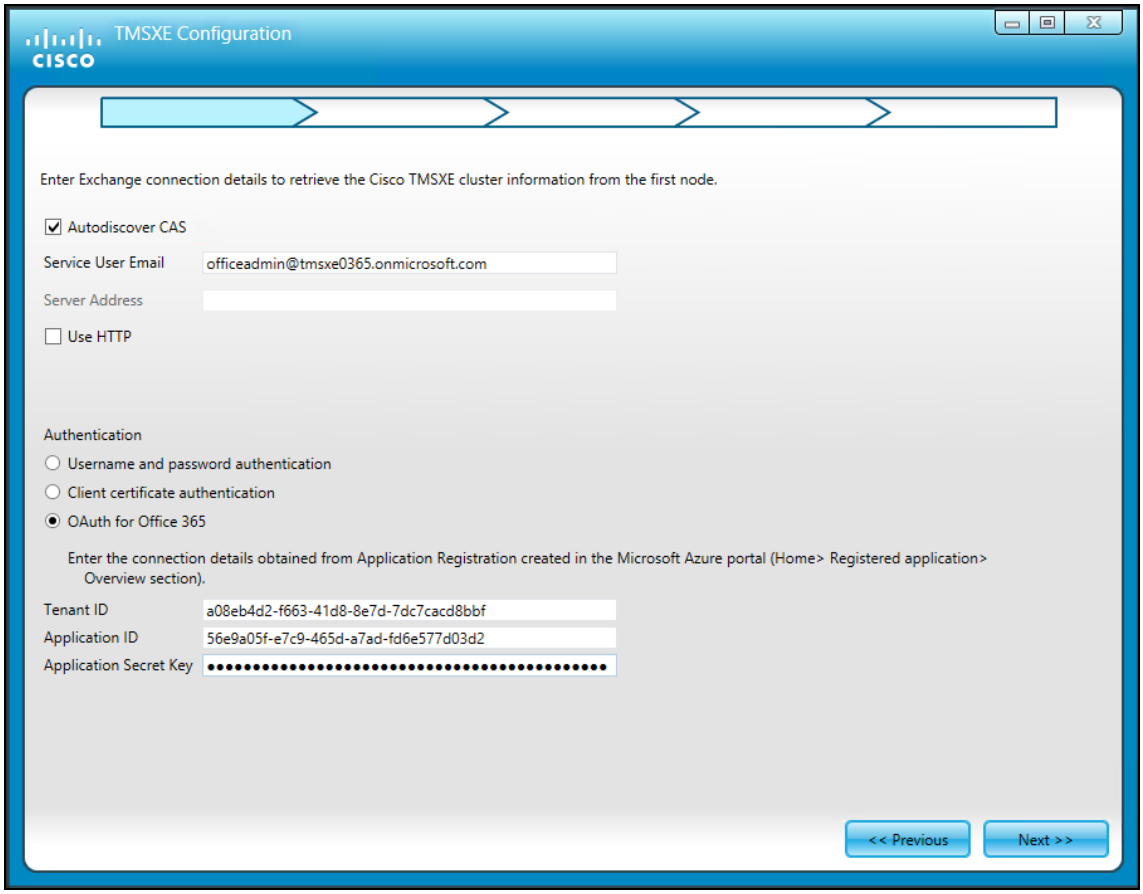
After installing Cisco TMSXEversion 5.10, when you navigate to Exchange Web Services tab the '**OAuth for Office 365**' option is available to configure OAuth credentials. When you select ' OAuth for Office 365' , the Tenant ID, Application ID and Application SecretKey fields are enabled and you have to enter the respective values as defined in Application Registration in the Microsoft Azure Portal. After all the three field values are provided, the '**Next**' button is enabled to proceed with the configuration steps.



Notes:

- Existing users who are upgrading to Cisco TMSXE 5.10 from a lower version can optionally configure OAuth for Office 365 or can continue using their existing configuration.
- In case of cluster mode, same configuration must be done on both the cluster.
- If OAuth for Office 365 is selected, then it is mandatory to select 'Resource Mailbox Impersonation' option.
- Use the Alternate Directory Settings option only when the Microsoft Office 365 authentication domain is different from the Active Directory FQDN. It is recommended that you use the Alternate Directory Settings option only when required.

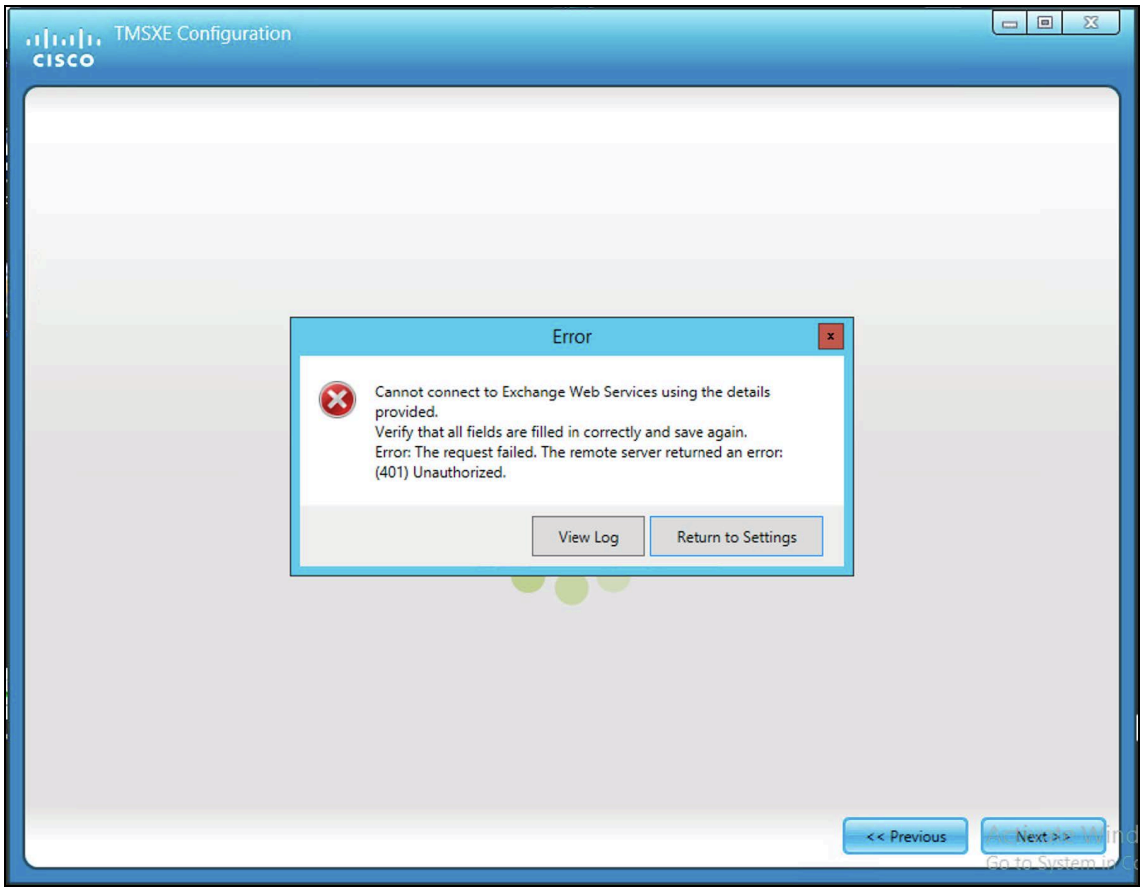
The following screen shot is for node 2 (cluster mode), where you will directly get Exchange Configuration Page first. You have to provide configuration details that are same as node 1 details.



After successful configuration of Cisco TMSXE, start Cisco TMSXE service.

Note: In cluster mode, when OAuth for Office 365 configurations are updated with a different set of Tenant ID, Application ID and Application Secret Key values on node 1 , the updated Tenant ID and Application ID values are also reflected in the Cisco TMSXE Configuration tool of node 2. However, the Application Secret Key value must be manually updated in node 2.

Cisco TMSXE displays an error message, if the given values are incorrect.



Notices

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.

Accessibility Notice

Cisco is committed to designing and delivering accessible products and technologies.

You can find more information about Cisco accessibility here:

www.cisco.com/web/about/responsibility/accessibility/index.html

Document Revision History

Date	Description
November 2019	Release of Cisco TMSXE 5.10.
April 2019	Release of Cisco TMSXE 5.9.
December 2018	Release of Cisco TMSXE 5.8.
July 2018	Release of Cisco TMSXE 5.7.
September 2017	Release of Cisco TMSXE 5.6.
April 2017	Release of Cisco TMSXE 5.5.
December 2016	Release of Cisco TMSXE 5.4.
August 2016	Release of Cisco TMSXE 5.3.
October 2014	Release of Cisco TMSXE 4.1. Includes new section in Troubleshooting on handling downgraded, defective, and declined meetings.
July 2014	Release of Cisco TMSXE 4.0.3. Includes changes to the update procedures.
May 2014	Release of Cisco TMSXE 4.0.1. Upgrade instructions updated to include information on clustering.
May 2014	Release of Cisco TMSXE 4.0. First publication of this deployment guide, which replaces the separate installation and administrator guides for Cisco TMSXE.

Cisco Legal Information

Cisco Trademark

Cisco Trademark