Cisco TelePresence Management Suite Extension for Microsoft Exchange

Deployment Guide

Version 4.0

D15111 02

September 2017

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.

Support for Office 365 in technical preview—extended field trial

We have extended the Early Field Trial (EFT) program for Cisco TMSXE supporting Office 365 (Exchange Online).

- Until the EFT program completes, Cisco TMSXE is not supported for production use with Office 365.
- When the EFT program completes, we will provide an update to documentation and/or software.

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 (4.0)	cisco.com
Cisco TelePresence Management Suite Extension for Microsoft Exchange User Guide (4.0)	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 TMSXE4.0, 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	Large
Cisco TMS	■ < 200 controlled systems ■ < 100 concurrent participants ■ < 50 concurrent ongoing scheduled conferences	■ < 5000 controlled systems ■ < 1800 concurrent participants ■ < 250 concurrent ongoing scheduled conferences
Cisco TMSXE	< 50 endpoints bookable in Microsoft Exchange	< 1800 endpoints bookable in Microsoft Exchange
Cisco TMSPE	■ < 1000 Collaboration Meeting Rooms ■ < 2000 Cisco VCS-provisioned users	■ < 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

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

	Requirement
CPU	2 cores (Xeon 2.4 GHz or larger), dedicated
Memory	8 GB, dedicated
Disk space provided on server	60 GB

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 [p.7] and Hardware requirements [p.7].

Software

Table 1: Software requirements for the Cisco TMSXE server

Product	Version
Microsoft Windows Server	■ 2012 up to build 9600 ■ 2008 Service Pack 2 (64-bit) ■ 2008 R2 Service Pack 1
Microsoft .NET Framework	■ .NET Framework Full (extended) is required ■ Version 4.0 or later

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. The communication will be authenticated using the Cisco TMSXE Exchange service user account. For account setup instructions, see Creating a Cisco TMSXE service user in Active Directory [p.22].

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

Cisco TMS Booking Service requirements

In order to use WebEx Productivity Tools with TelePresence, you must include Cisco TMS Booking Service when installing Cisco TMSXE. Booking Service uses IIS, the Windows Server web server.

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 further detail, see Configuring IIS for HTTPS [p.49].

Cisco TMS requirements

Table 2: Requirements for the Cisco TMS server

Version	14.4
Network	HTTPS (recommended) or HTTP connectivity is required from the Cisco TMSXE server to Cisco TMS.

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 installation. 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**.

WebEx Enabled TelePresence requirements

In order to use Cisco TMSXE to book 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

For guidance on setting up WebEx Enabled TelePresence with or without single sign-on, see *WebEx Enabled TelePresence Configuration Guide*.

Microsoft Exchange requirements

Table 3: Requirements for the Microsoft Exchange server

Requirement	Description
Microsoft Exchange	Tested versions: ■ Microsoft Exchange 2013. Note that Service Pack 1 is currently not supported. ■ 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 **Support for Office 365 in technical preview—extended field trial** We have extended the Early Field Trial (EFT) program for Cisco TMSXE supporting Office 365 (Exchange Online). • Until the EFT program completes, Cisco TMSXE is not supported for production use with Office 365. • When the EFT program completes, we will provide an update to documentation and/or software. ■ Microsoft Exchange 2010 Service Pack 3. ■ Microsoft Exchange 2007 Service Pack 3
Windows Server	Tested versions: ■ Microsoft Windows Server 2012 ■ Microsoft Windows Server 2008 R2 ■ Microsoft Windows Server 2008
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.

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.
  - With Exchange 2007, the NLB must be set up to have a sticky IP connection (affinity) to one CAS server.
  - In the case of a CAS failover (2010 and 2007) or mailbox failover (2013), 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 and 2007) or mailbox server (2013).
  - 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.

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 (technical preview)	Office 365 (technical preview)
Microsoft Outlook 2013	Office 365 (technical preview) and Exchange 2013
Outlook Web App	Exchange 2010 and 2013
Microsoft Outlook 2010	Exchange 2010
Microsoft Outlook 2007 SP2	Exchange 2007

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 4.0, 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.

WebEx Enabled TelePresence deployments

WebEx Enabled TelePresence 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.

There are two ways to book WebEx Enabled TelePresence meetings with Cisco TMSXE: the WebEx Scheduling Mailbox and WebEx Productivity Tools with TelePresence.

- For requirements, see WebEx Enabled TelePresence requirements [p.11].
- For an overview of the entire WebEx Enabled TelePresence solution, see *Cisco WebEx Enabled TelePresence Configuration Guide*.

The WebEx Scheduling Mailbox

The WebEx Scheduling Mailbox can be used to schedule WebEx Enabled TelePresence meetings with any version of Exchange, by adding a special email address to the meeting invite.

For setup instructions, see Setting up the WebEx Scheduling Mailbox [p.46].

WebEx Productivity Tools with TelePresence

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

Using Productivity Tools with Cisco TMSXE requires the installation and configuration of Cisco TMS Booking Service.

For setup instructions, see Setting up WebEx Productivity Tools with TelePresence with Cisco TMSXE [p.48].

Delegates for room mailboxes are not supported with Cisco TMSXE.

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

On-premises Exchange deployments

Cisco TMSXE can be deployed entirely with on-premises Exchange servers. For version requirements, see Microsoft Exchange requirements [p.11].

For environments that mix on-premises Exchange with Office 365, see Hybrid deployments(technical preview) [p.14].

Limitations with Exchange 2007

Some newer features are not available or supported for Exchange 2007 deployments with Cisco TMSXE:

- clustering of the Cisco TMSXE services
- autodiscovery of the Client Access Server (CAS Autodiscover)
- resource mailbox impersonation
- hybrid deployments where CAS and/or mailbox servers are in the cloud

Support for Exchange 2007 will be discontinued in a future release.

Mixed Exchange environments

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

Microsoft Office 365 deployments(technical preview)

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.

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 WebEx Enabled TelePresence meetings using the WebEx Scheduling Mailbox.

Hybrid deployments(technical preview)

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 2013 (recommended) or Exchange 2010.
- Active Directory is on premises, which is required to work with Cisco TMS.
- All users are in the same environment (on premises or Office 365) as the room mailboxes they will book, and the WebEx Scheduling Mailbox, if applicable. This is due to a Microsoft limitation on hybrid deployments. Note that the same service user can be used cross premises. For more information on these Microsoft limitations, see the Microsoft support article Cross-premises Calendar editing is unavailable in a hybrid deployment of Exchange Online in Office 365 and on-premises Exchange Server.

Making sure rooms are visible to all mailboxes

For cross-premises visibility of calendars:

- Create the service user, the WebEx Scheduling Mailbox, and all room mailboxes on an on-premises server.
- Move these mailboxes to the cloud using any of Microsoft's standard procedures or tools.

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 locations. Which node is currently active/passive is written to the log on INFO level. Note that for any troubleshooting situation, both logs 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 [p.39].

Cisco TMS Booking Service redundancy

Redundancy for Cisco TMS Booking Service is supported through the use of a network load balancer (NLB). This redundant setup ensures high availability, but does not increase performance.

For prerequisites and setup instructions, see Setting up redundancy for Cisco TMS Booking Service [p.44].

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*:

- If not using Productivity Tools, installing without Booking Service, and setting up two cluster nodes for the Cisco TMSXE service, following the instructions in Installing Cisco TMSXE with service clustering [p.39].
- If using Productivity Tools:
  - setting up two cluster nodes for the Cisco TMSXE service following the instructions in Installing Cisco TMSXE with service clustering [p.39].
  - installing Booking Service on both nodes and set up a network load balancer for the Booking Service nodes, following the instructions in Setting up redundancy for Cisco TMS Booking Service [p.44].

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 [p.15].

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:

- **Delete the subject**
- **Add the organizer's name to the subject**
- **Remove the private flag on an accepted meeting**

As a best practice, we recommend not relying on the "Private" flag for security. If allowing the flag on accepted meetings, make sure to restrict access to opening the resource calendars, or users will still be able to see to all meeting information in Outlook.

While the "Private" flag will be respected within the Outlook client, it is not supported by Cisco TMS, and meeting subjects will be freely viewable:

- in Cisco TMS
- on endpoints that support the "Meetings" calendar

The body of the meeting request and the list of attendees are not sent to Cisco TMS.

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

See Configuring required settings [p.26] for detailed instructions on the required and supported settings for mailboxes.

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

Using delegates for room mailboxes is not supported by Cisco TMSXE.

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 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.

Modifying ongoing meetings

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

When modifying any meeting:

- if the meeting is using an MCU that does not support WebEx, WebEx may not be added, as the meeting would have to be disconnected and re-routed for this to work.
- extending the meeting will fail if it creates a booking conflict for any of the participants.

When modifying single meetings, including meetings in a series:

- editing the start time will not work and Cisco TMS will throw an exception.
- 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.

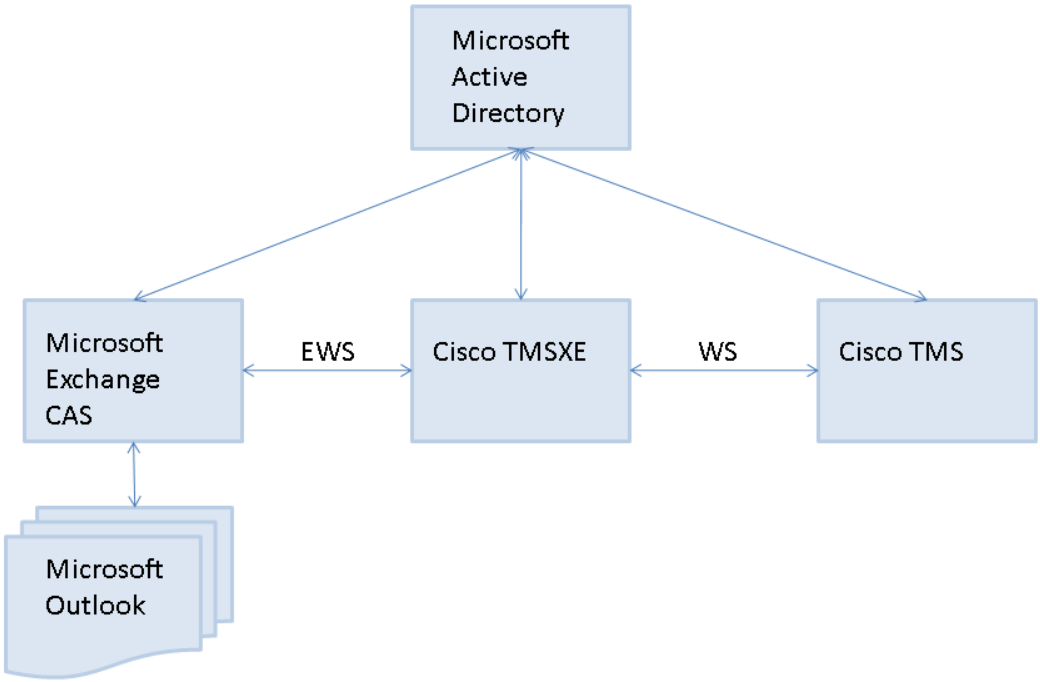
When *deleting* a recurrent series while a meeting in the series is ongoing, the ongoing meeting will end.

When *modifying* a recurrent series while a meeting in the series is ongoing, the ongoing occurrence is turned into a single meeting, separate from the series, and:

- 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.

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 [p.17].

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 and WebEx 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.
   - If the WebEx Scheduling Mailbox was invited to the meeting, Cisco TMS will attempt to include WebEx.
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 TMSXE will request that Cisco TMS book the systems without routing (step 4). For more on this scenario, see Conference routing unsuccessful [p.58].
   - If no routing or WebEx was requested and all resources could be reserved, no notifications are sent.
   - 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.

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.

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.

Communication with WebEx

- 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 WebEx Enabled TelePresence meetings with both telepresence and WebEx.
- 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.
  Booking WebEx-only conferences using this method is possible, but not recommended, as it will trigger the use of MCU resources even if no telepresence participants have been booked. Organizers will be notified of this in their booking confirmation.

Preparing to install or upgrade

Some procedures need to be carried out prior to running the Cisco TMSXE installer. The procedures depend on whether you are upgrading or performing a new installation, and on which version of Microsoft Exchange you are using.

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 (14.4 is required), 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. Back up the Cisco TMS database.
2. Stop the Cisco TMSXE Windows service if you have an existing installation.
3. Follow the instructions in *Cisco TMS Installation and Upgrade Guide* to upgrade Cisco TMS.
4. 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 4.0 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 Exchange and

Cisco TMS.

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 [p.23] 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 a certain set of permissions.

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:
   - *Read*
   - *Update*
   - *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.

Including WebEx by default

Cisco TMSXE booking is also affected by the WebEx settings in Cisco TMS, located at **Administrative Tools > Configuration > WebEx Settings**.

Note that the field **Add WebEx To All Conferences** will make Cisco TMS include WebEx in any booking, and organizers booking from Outlook may not realize that WebEx is included until receiving the booking confirmation.

Per-conference settings

If using WebEx Productivity Tools with TelePresence or the custom Cisco TelePresence booking form, organizers will be able to change some of these settings on a per-conference basis.

For information on rolling out the form to users, see Deploying the Cisco TelePresence advanced settings form [p.50].

For information on configuring Cisco TMSXE for WebEx Productivity Tools with TelePresence, see Setting up WebEx Productivity Tools with TelePresence with Cisco TMSXE [p.48].

For more detail on how booking works for users, see *Cisco TelePresence Management Suite Extension for Microsoft Exchange User Guide (4.0)*.

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:

- Office 365 and Exchange 2013: *Create and Manage Room Mailboxes*
- Exchange 2010: *Create a Room or Equipment Mailbox*
- Exchange 2007: *How to Create an 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 [p.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 [p.25].

Setting Up PowerShell for Use with Office 365(technical preview)

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.

Setting up impersonation and throttling

Office 365, Exchange 2013, and Exchange 2010

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.

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.

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 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 [p.73].

Exchange 2007

For Exchange 2007, you must set up full access permissions for the service user. Impersonation is not supported.

There are two ways to set full access permissions for Exchange 2007; using Exchange Management Console or Exchange Management Shell.

In Exchange Management Console:

1. Use the EMC tree to navigate to **Recipient Configuration > Mailbox** and select the mailbox you want to configure.
2. Right-click the room mailbox and select **Manage Full Access Permission...**.
3. Add the Cisco TMSXE service user.
4. Proceed to the Exchange Management Shell instructions below.

If using Exchange Management Shell, enter the following command, replacing `[mailbox]` with the name of the mailbox you are configuring, `@` sign and domain not included:

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

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`	*0*	
`MaximumConflictInstances`	*0*	Prevents the mailbox from accepting recurrent meetings where some instances conflict with existing bookings.

Shell parameter	Required value	Description
`DeleteSubject`	*False* (recommended) or *True*	We recomment turning off this option to delete meeting subjects. However, if it is a requirement for some room mailboxes that this option be enabled, it must the 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`	*True* (recommended) or *False*	This setting removes the "Private" flags for all meetings accepted by the mailbox. The setting does not need to be enabled, but must be identical for all mailboxes added to Cisco TMSXE. Also note that the "Private" flag is not supported by Cisco TMS. For further information, see Best practices for all deployments [p.16].
`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)*
- *Set-MailboxCalendarSettings (Exchange 2007 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 Exchange 2007, use the shell command **`Get-MailboxCalendarSettings - id [mailbox] | fl`**

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

Upgrading to Cisco TMSXE 4.0

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 [p.78]
- 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 [p.7] are met.
- You have considered all Best practices for all deployments [p.16].
- You have followed the steps in Backing up and upgrading the backend [p.22].
- You are logged in as a local administrator on the installing server.

If you want to upgrade to a clustered deployment, see Installing Cisco TMSXE with service clustering [p.39].

Running the installer

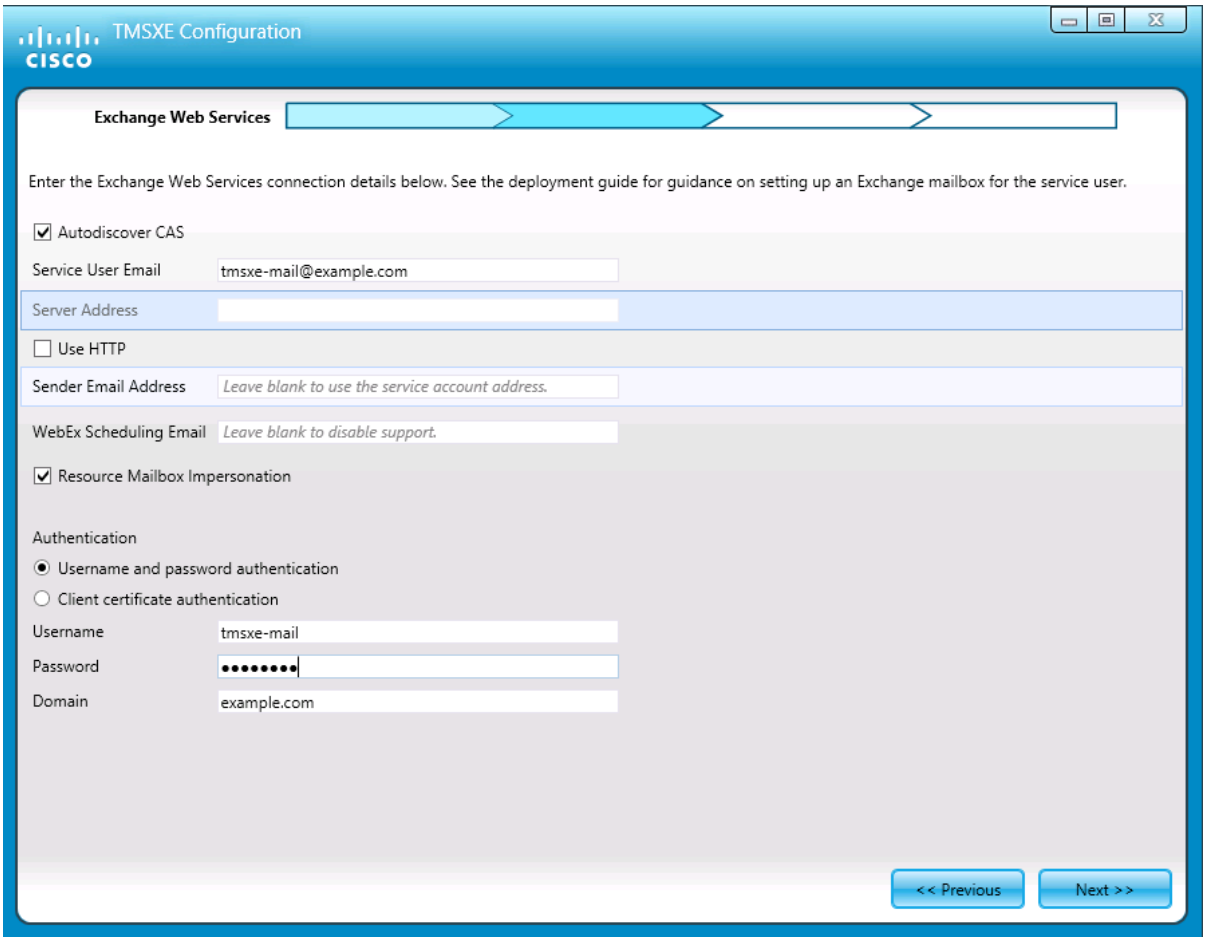
1. Stop the Cisco TMSXE Windows service, on both nodes if upgrading a clustered deployment.
2. Check Windows Update and install any critical updates to the .NET framework on the server where Cisco TMSXE will be installed. Make sure the .NET version is 4.0 or later. Reboot the server after installing if prompted.
3. Place the installation files on the server.
4. Run the Cisco TMSXE installer and accept the End-User License Agreement (EULA) to start the installation process.
5. The installer will detect that you have a previous installation of Cisco TMSXE. Click **Upgrade** to continue.
6. Click **Next** to start the setup.
7. Accept the terms in the license agreement and click **Next**.
8. Select which components to include with your installation:
   - Cisco TMS Booking Service is required if planning to use WebEx Productivity Tools with TelePresence.
     If enabling this, you will be prompted to modify or confirm the name of the IIS application pool to which you want Booking Service installed. See Setting up WebEx Productivity Tools with TelePresence with Cisco TMSXE [p.48] 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 [p.39] for further information

- Performance Monitors can be enabled to allow monitoring Cisco TMSXE performance using standard Windows tools.

9. Follow all remaining instructions provided by the installer.
10. When the upgrade is completed, click **Finish**.
    The configuration tool launches.

Configuring Cisco TMSXE

1. Click through the configuration wizard, modifying settings and adding systems if needed.
   All settings from the previous version are kept and will be re-validated as you click **Next**.
2. 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, but is not supported for Exchange 2007.
   - WebEx Scheduling Mailbox.



3. 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 [p.54].

Performing a new installation

This section describes the required steps to install Cisco TMSXE 4.0 when no previous Cisco TMSXE deployment exists.

Before you start

Make sure that:

- All Prerequisites [p.7] are met.
- You have considered Best practices for all deployments [p.16].
- You have completed all steps described in Preparing for a new installation [p.22].
- You are logged in as a local administrator on the installing server.

If you want to set up a clustered deployment, see Installing Cisco TMSXE with service clustering [p.39].

Running the installer

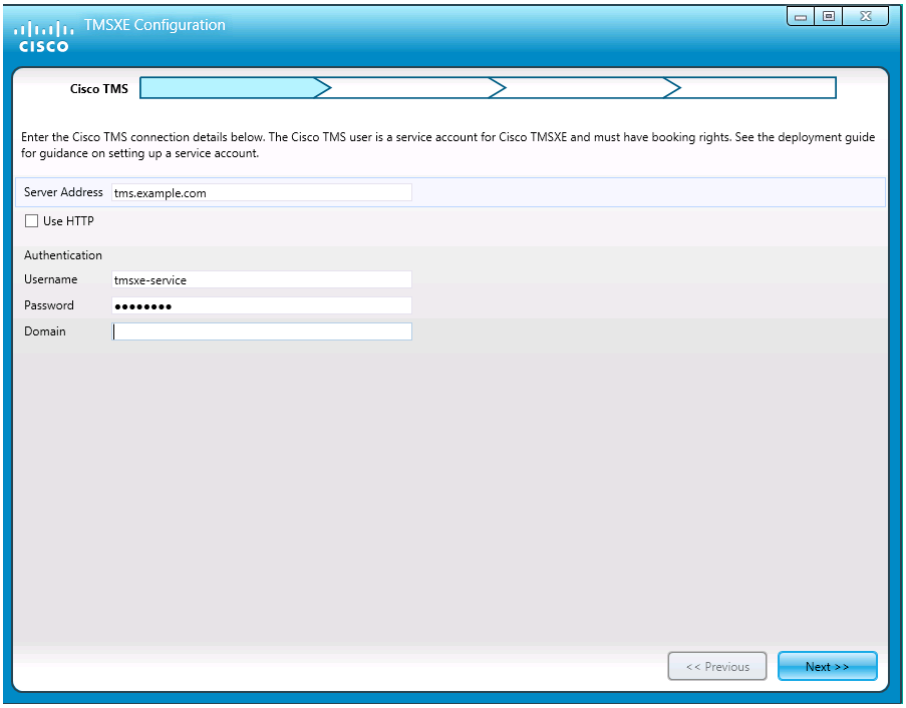
1. Check Windows Update and install any critical updates to the .NET framework on the server where Cisco TMSXE will be installed. Make sure the .NET version is 4.0 or later. Reboot the server after installing if prompted.
2. Place the installation files on the server.
3. Run the Cisco TMSXE installer and 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 planning to use WebEx Productivity Tools with TelePresence.
     If enabling this, you will be prompted to modify or confirm the name of the IIS application pool to which you want Booking Service installed. See Setting up WebEx Productivity Tools with TelePresence with Cisco TMSXE [p.48] 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 [p.39] for further information
   - Performance Monitors can be enabled to allow monitoring 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.

Configuring Cisco TMSXE

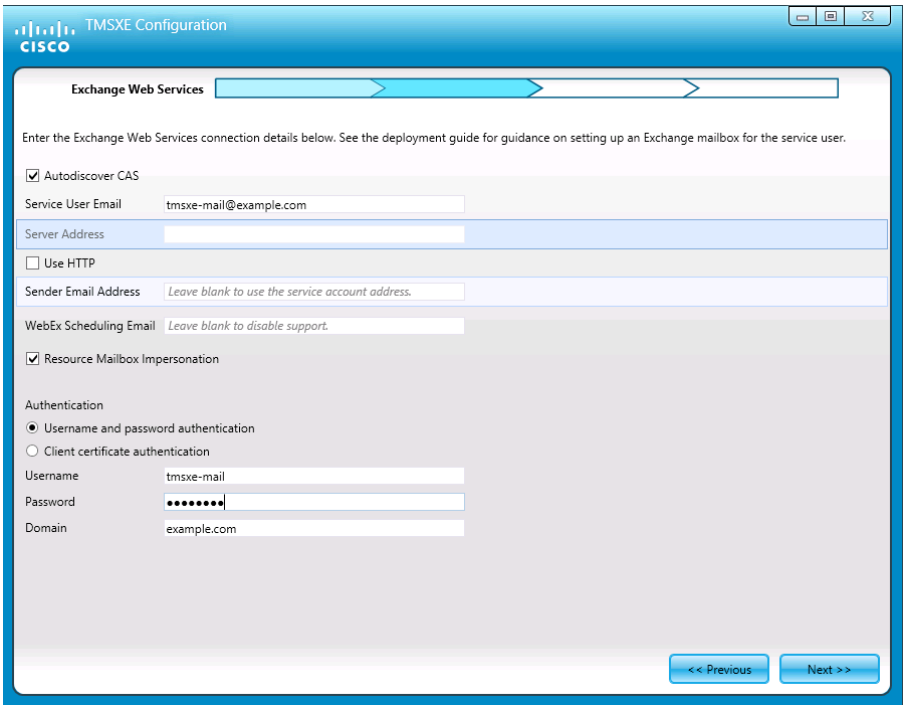
Most fields in the configuration tool are required. Clicking **Next** validates the settings provided for each step of the initial configuration. If one or more settings cannot be validated, you will be returned to the previous step to allow for corrections.

This procedure describes each step of the configuration process. For detail on each of the available fields, see the Configuration reference [p.35] 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.



2. 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 Exchange 2013 or Exchange 2010 without full mailbox access for the service user.
   - You must also determine how to authenticate.

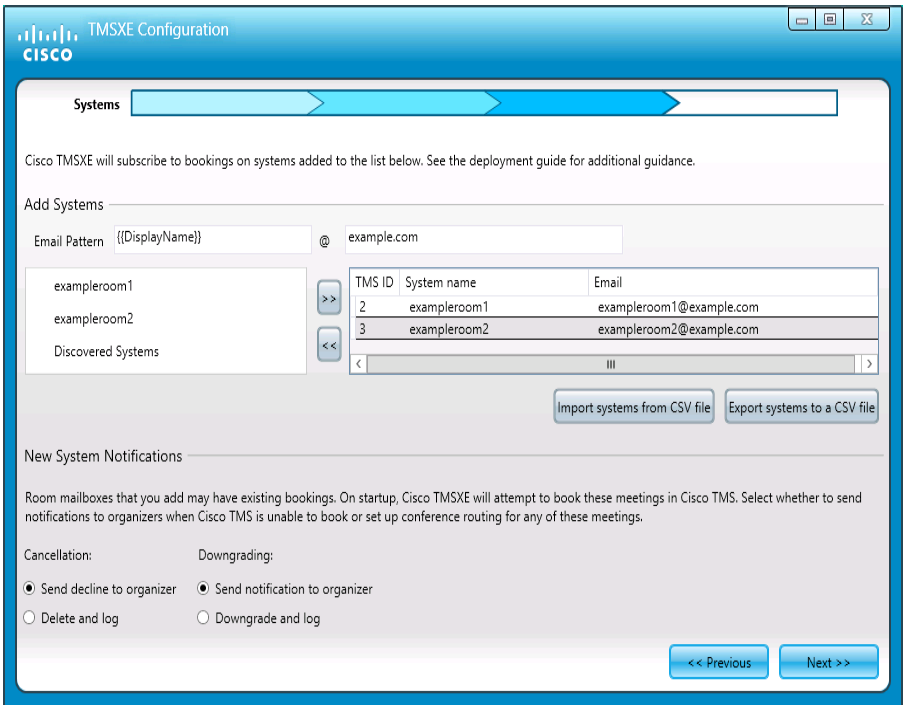


Click **Next** to submit your settings. Should the connection fail, you will be prompted with an option to view the Exchange Web Services (EWS) log to troubleshoot.
After viewing the log, close it and click **Return to Settings** to correct any errors and re-submit.

3. 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 [p.24].)
   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 [p.37]).
   - Add the systems one by one:
     i. 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.

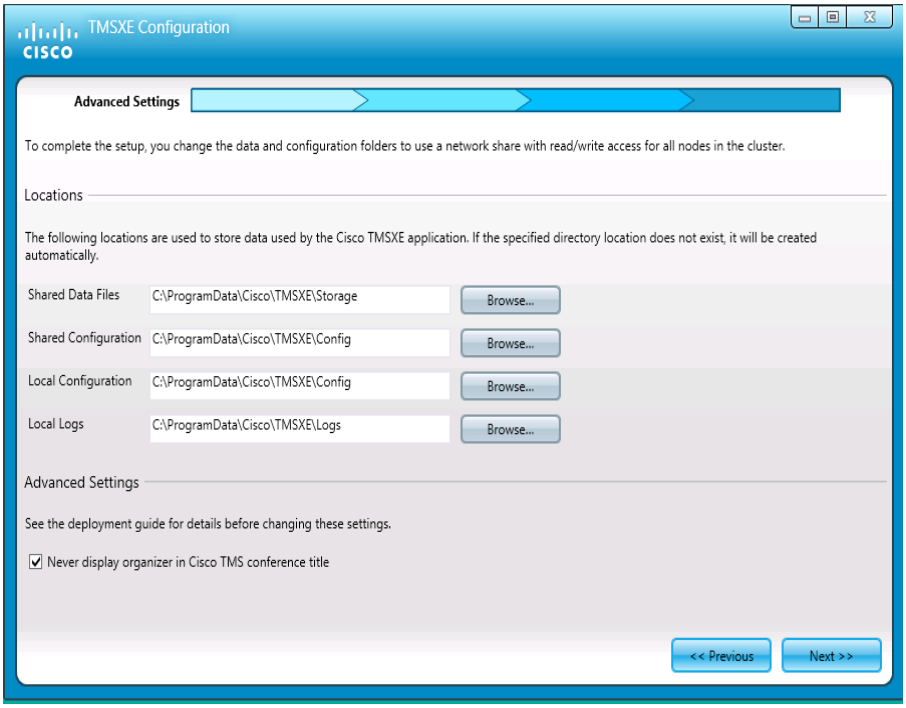
     ii. Select endpoints in the left-hand list and click **>>** to add them to Cisco TMSXE. Use **`Ctrl`** or **`Shift`** to select multiple endpoints.
     iii. Modify individual email addresses as needed by double-clicking on them after they have been added to the right-hand list.

   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 [p.37].



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.

4. 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 [p.38]



5. 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.

6. 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 [p.54] when you are ready to start Cisco TMSXE.

If any validation steps fail during the configuration process, see the section Errors during configuration [p.66].

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 [p.22].
Password	The password for the above user.
Domain	The domain that the Cisco TMS server is in.
Exchange Web Services	
CAS Autodisover	Specify whether to allow autodiscovery of the Exchange CAS (client access server). This feature relies on an autodiscover service being configured on the domain.
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 [p.22].
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.

Table 5: Configuration tool field reference (continued)

Field	Description
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 2013: *Add-ADPermission* ■ Exchange 2010: *Manage Send As Permissions for a Mailbox* ■ Exchange 2007: *How to Grant the Send As Permission for a Mailbox*
WebEx Scheduling Email	The address of the WebEx Scheduling Mailbox. For more information, see Setting up the WebEx Scheduling Mailbox [p.46].
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 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 [p.73]. ■ On Exchange 2007, impersonation is not supported. You must give the service user full access permissions. See Setting up impersonation and throttling [p.25].
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 [p.22]. ■ **Username**—The Cisco TMSXE service user in Exchange/Active Directory. ■ **Password**—The password for the above user. ■ **Domain**—The domain the Exchange server is in.
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 [p.12]. ■ **Password**—The password for the above certificate.
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 [p.24]. ■ 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.

Table 5: Configuration tool field reference (continued)

Field	Description

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.

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 Conference routing unsuccessful [p.58].

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.
Configuration	When configuring a Cisco TMSXE cluster, there will be four fields: ■ **Shared Data Files** ■ **Shared Configuration** ■ **Local Configuration** ■ **Local Logs**
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.
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.

Setting up a redundant deployment

Cisco TMSXE clustering provides active/passive redundancy for the Cisco TMSXE service. To achieve redundancy for Cisco TMS Booking Service, you must also deploy a network load balancer.

This section provides instructions for setting up redundance for both Cisco TMSXE and Cisco TMS Booking Service. For an overview of supported scenarios and how redundancy works, see Redundant deployments [p.15].

Limitations

- Redundancy is not supported with Exchange 2007
- Redundancy is not supported for small deployments where Cisco TMSXE resides on the Cisco TMS server.
- Load-balancing of Cisco TMS Booking Service is only supported in combination with Cisco TMSXE clustering and a redundant Cisco TMS deployment.

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 [p.8] 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 Cisco TMSXE 3.x.
- 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 4.0 [p.63].

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.
- We recommend that you only make the network share accessible to the machine accounts of both nodes and the administrator performing the installation.

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 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:

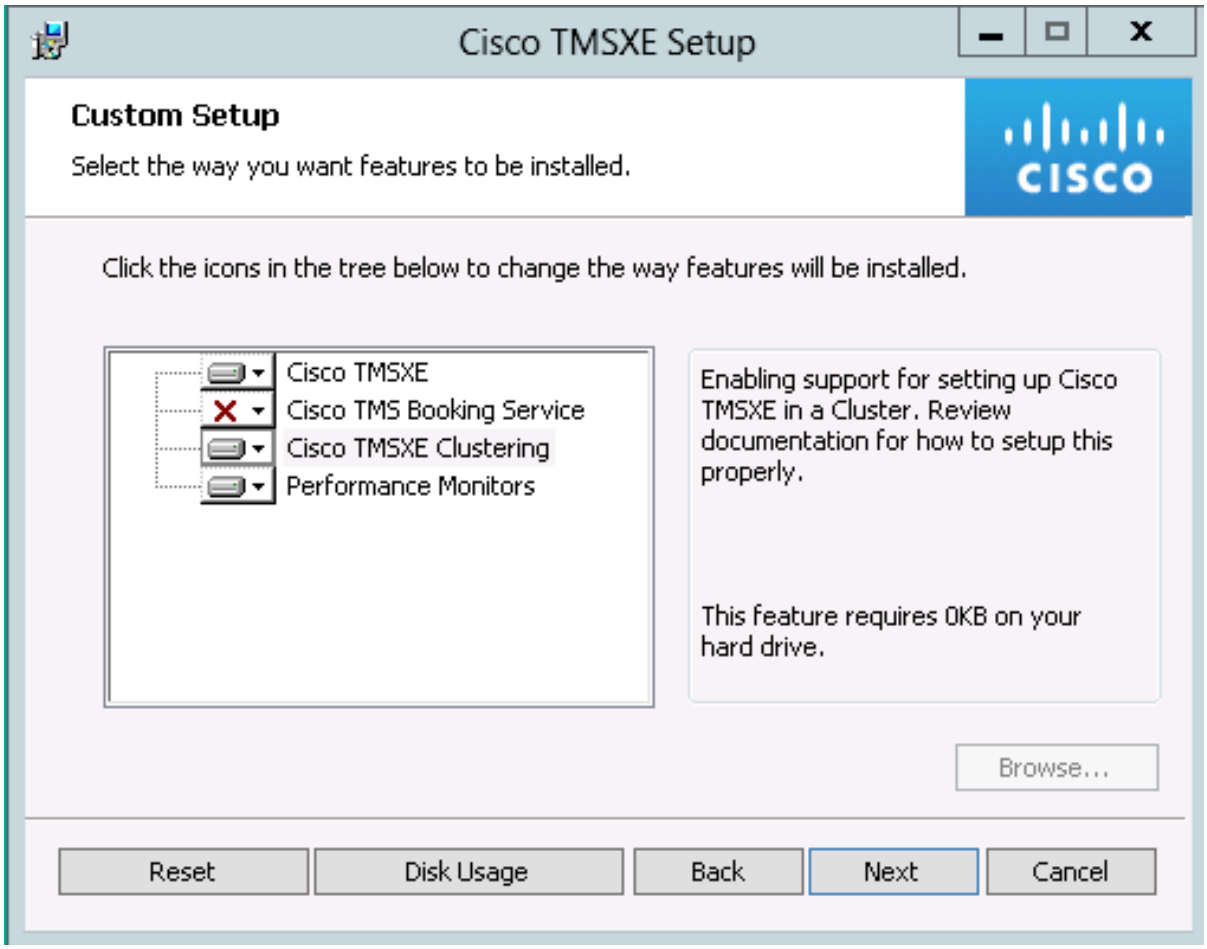
1. On **`filestore.example.com`**, create a folder **tmsxeconfig**.
2. To enable folder sharing, go to **Properties > Sharing > Advanced Sharing**.
3. Check **Share this Folder**.
4. Click **Permissions**.
5. Click **Add**, then **Object Types**, and make sure that **Computers** and **Users** are checked.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

Performing the installations

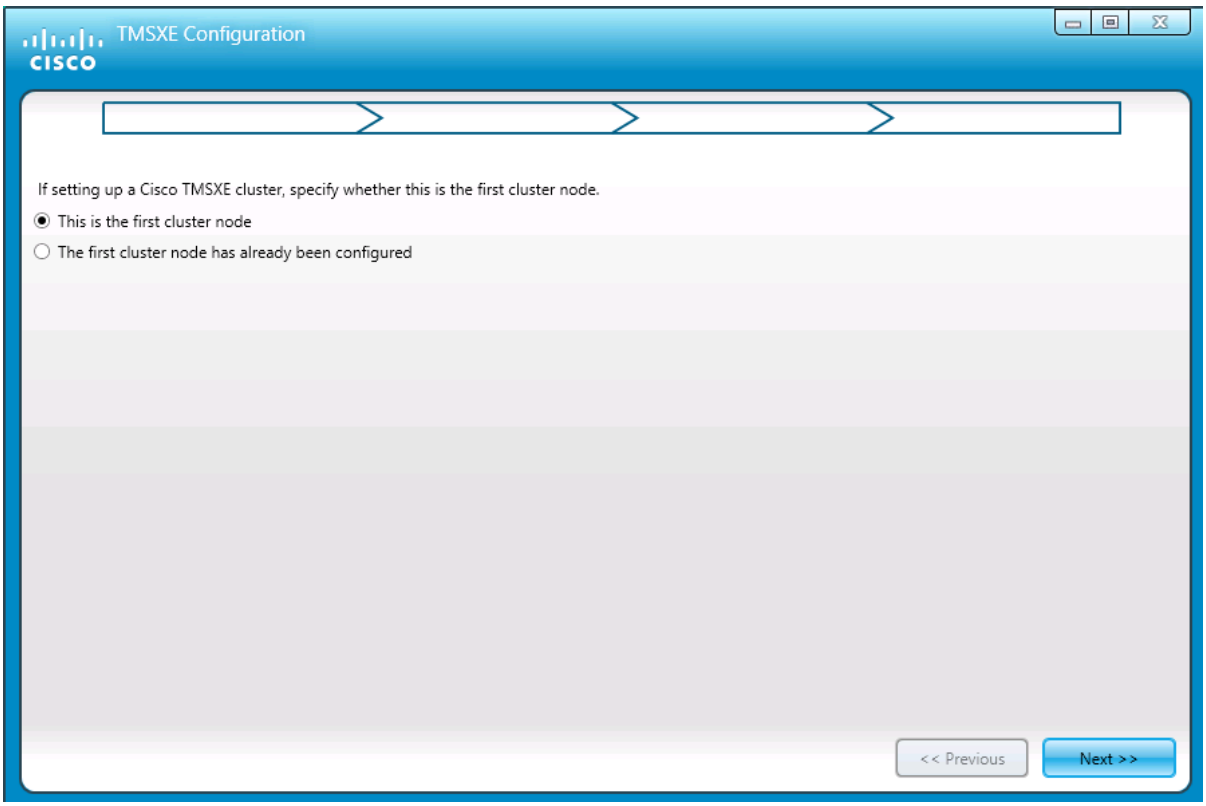
For new installations and upgrades on both nodes, follow the instructions for running the installer, making sure to enable clustering.



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 [p.31], 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. Click **Save**.

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. 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.
3. 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:

   i. Resolve any issues on the first node or with access to network shares.
   ii. On this node, go back to the previous step, and re-validate the import.
- When green checkmarks are shown, click **Next**.

4. Enter authentication details for Cisco TMS and Exchange.
   These need to be stored per server and cannot be imported.
5. Click **Next** to validate all settings.
6. Click **Next** to save the settings.
7. Click **Finish**.

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.

Setting up redundancy for Cisco TMS Booking Service

Cisco TMS Booking Service can be set up with active/active redundancy using a network load balancer (NLB) to ensure high availability.

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.

Before you start

- Set up identical installations of Cisco TMSXE, including Booking Service, on both nodes following the instructions in Installing Cisco TMSXE with service clustering [p.39].
- Note that as for the Cisco TMS service, logs for the Booking Service nodes are separate, but the log level is a part of the shared configuration.

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 Setting up communication between WebEx and Cisco TMSXE [p.49].

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.

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.

Setting up the WebEx Scheduling Mailbox

For deployments where WebEx Enabled TelePresence is available, 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 user or resource/room mailbox, as described below, 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 WebEx Enabled TelePresence 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.

Before you start

Make sure that all WebEx Enabled TelePresence requirements [p.11] are met.

Creating and configuring the mailbox

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:
   - Office 365 and Exchange 2013: *Create and Manage Room Mailboxes*
   - Exchange 2010: *Create a Room or Equipment Mailbox*
   - Exchange 2007: *How to Create an Equipment Mailbox*
2. If using Exchange 2007 or 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* or
   - Exchange 2007: *How to Allow Mailbox Access*
3. Modify the mailbox properties:
   a. Turn off the Calendar Attendant for the mailbox. For instructions, see:
      - Office 365 and Exchange 2013: *Set-CalendarProcessing*
      - Exchange 2010: *Configure User and Resource Mailbox Properties*
      - Exchange 2007: *How to Disable the Auto-Processing of Meeting Messages*

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 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.

A user mailbox with the above settings will still work with Exchange 2010 and Exchange 2007, but not with Exchange 2013 and Office 365.

Additional recommendations

We also recommend the following configurations:

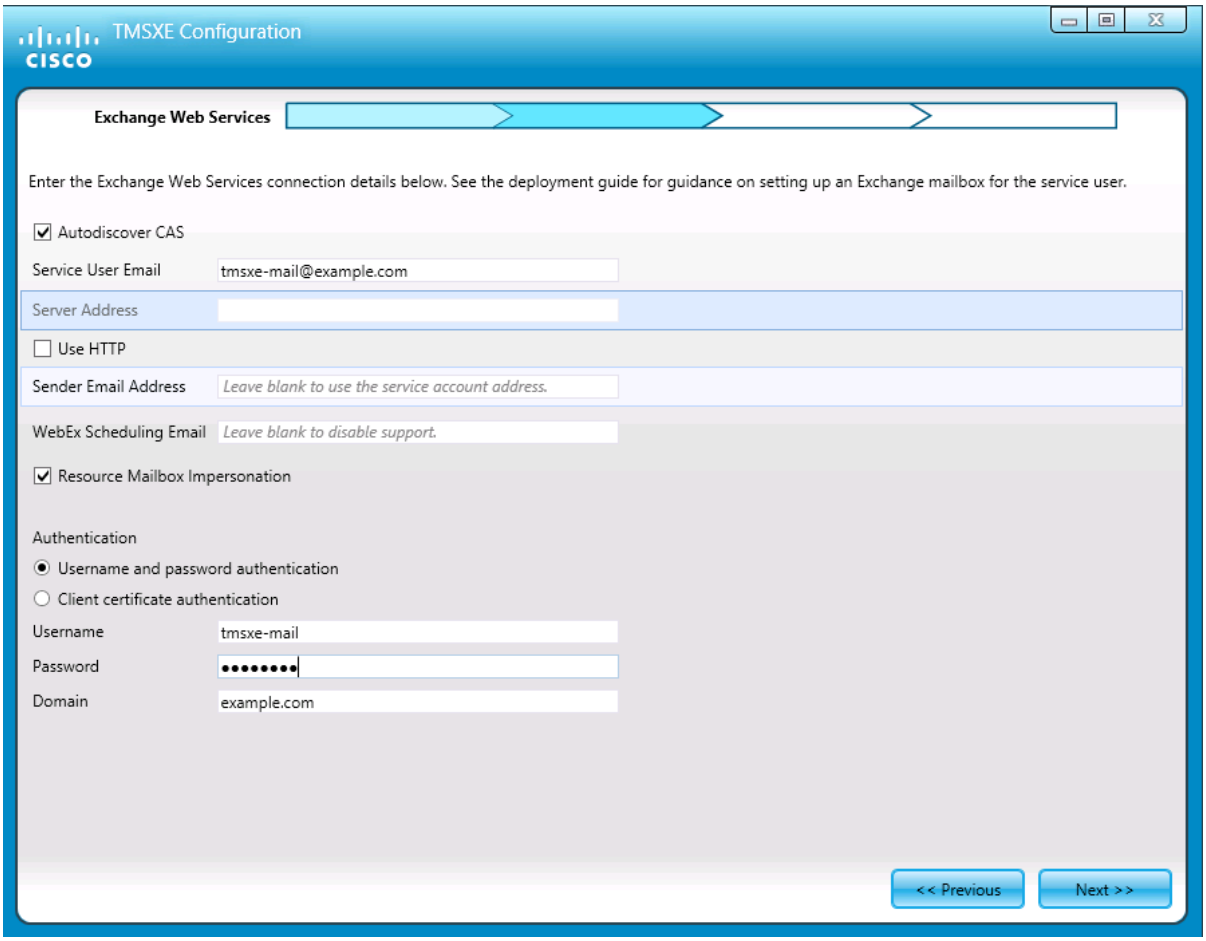
- Using Exchange Management Console **Mail Flow Settings** or Exchange Management Shell, stricten the message delivery restrictions as needed.
  For example, require senders to be authenticated, only allow from people in a specific group, or similar.
  For instructions, see:
  - Office 365 and Exchange 2013: *Configure Message Delivery Restrictions for a Mailbox*
  - Exchange 2010: *Configure Message Delivery Restrictions*
  - Exchange 2007: *How to 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.

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.



3. Click **Save**.

Setting up WebEx Productivity Tools with TelePresence with Cisco TMSXE

WebEx Productivity Tools with TelePresence adds a special panel to Outlook for Windows that allows users to synchronously book and configure:

- WebEx Enabled TelePresence meetings that include both WebEx and telepresence.
- WebEx-only meetings.
- Telepresence-only meetings.

The panel provides access to simple and advanced settings for both WebEx and telepresence, including the option of adding call-in and call-out telepresence participants, and allowing WebEx participants to join the meeting ahead of start time.

Note that all organizers must be set up with a WebEx user for Productivity Tools to work, even when booking telepresence-only meetings.

Detailed instructions on configuration and deployment of WebEx Productivity Tools with TelePresence can be found in *Cisco WebEx Site Administration User's Guide*, which is available as webhelp and PDF from your WebEx site.

Installing and configuring Cisco TMS Booking Service

To allow WebEx Productivity Tools with TelePresence to communicate with Cisco TMSXE you must have Booking Service installed.

You can set up Booking Service with load balancing.

- For guidance on supported scenarios, see Redundant deployments [p.15].
- For setup instructions, see Setting up redundancy for Cisco TMS Booking Service [p.44].

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 [p.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

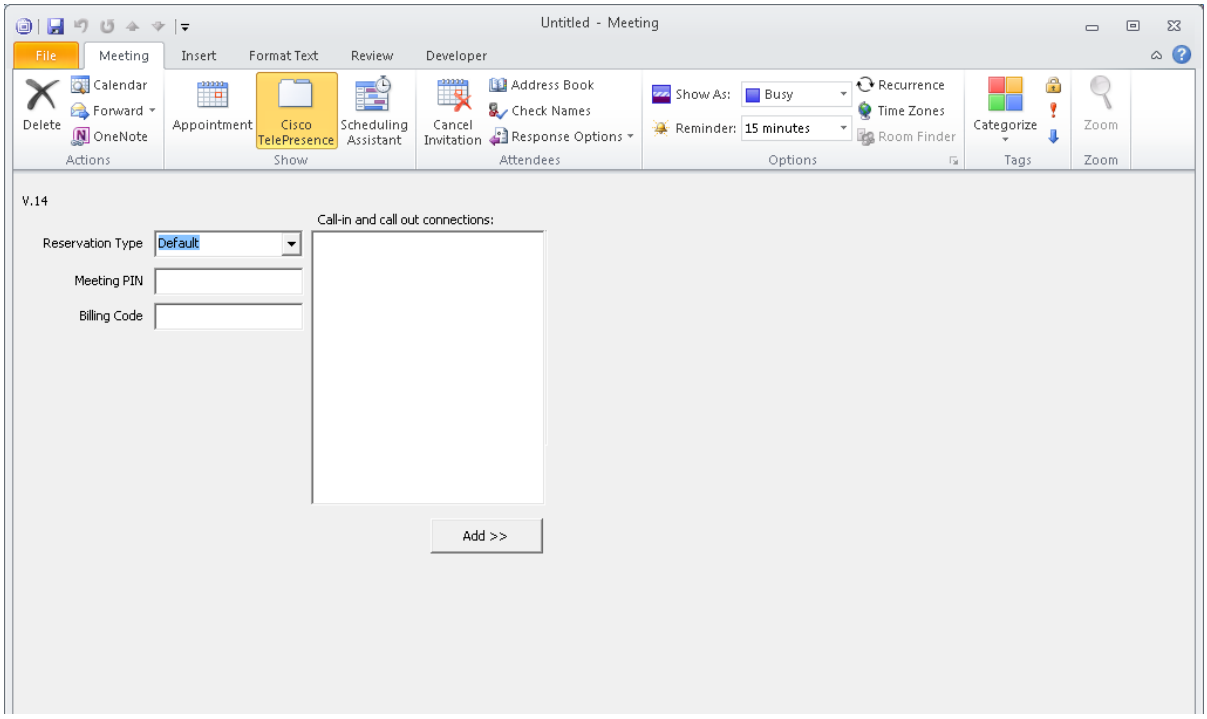
1. On your WebEx site, go to **Manage Site > Site Settings > OneTouch TelePresence Options**.
2. In the **Cisco TMSXE Host Address** field, enter the full address of the Booking Service by including the hostname of the server in the following address:
   `https://<hostname>/TMSService/Booking.svc`.
3.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

For overall instructions on setting up WebEx Enabled TelePresence, see *Cisco WebEx Enabled TelePresence Configuration Guide*.

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 (4.0)*.



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 Setting up the WebEx Scheduling Mailbox [p.46].

Limitations

Note that:

- custom forms only work with Outlook for Windows.
- 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.

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 [p.51]
2. Publishing the Cisco TelePresence form [p.51]
3. Configuring clients to use the form [p.52]

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 [p.51].

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 2013: *Create an Organizational Forms Library in Exchange 2013*
- Exchange 2010: *Create an Organizational Forms Library*
- Exchange 2007: *How to Create an Organizational Forms Library in Exchange 2007*

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 [p.51].

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 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 [p.52].

Publishing from Outlook 2007

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. In the menu go to **Tools > Forms... > Design a Form...**
3. Change the **Look In** dropdown menu to *User templates in File System*.
4. Click **Browse**.
5. Locate the **.oft** file on the computer, and open it.
6. From the **Publish** dropdown button, select **Publish Form As...**.
7. 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.
8. Enter names in the two fields as described below:
   - **Display name:** Meeting
   - **Form name:** VideoConference
9. 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 [p.52].

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.

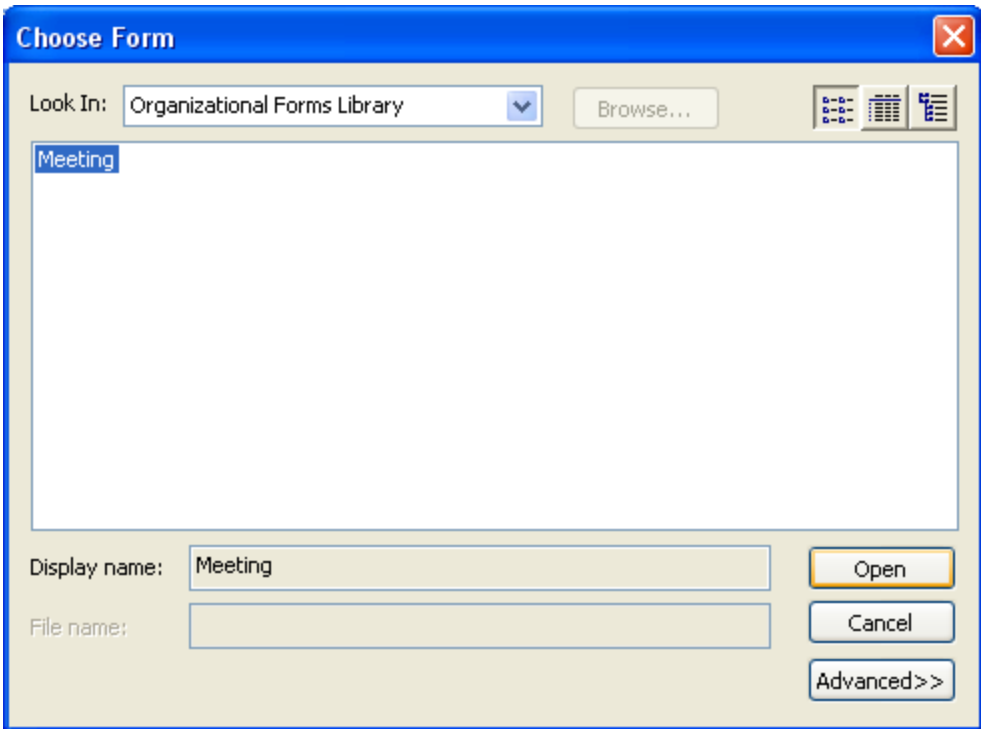
The Microsoft article *How to globally change the default forms in Outlook by using the Forms Administrator utility* describes and links to a utility for creating registry keys to change the default form.

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** dropdown 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 full 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 [p.65] for more information.

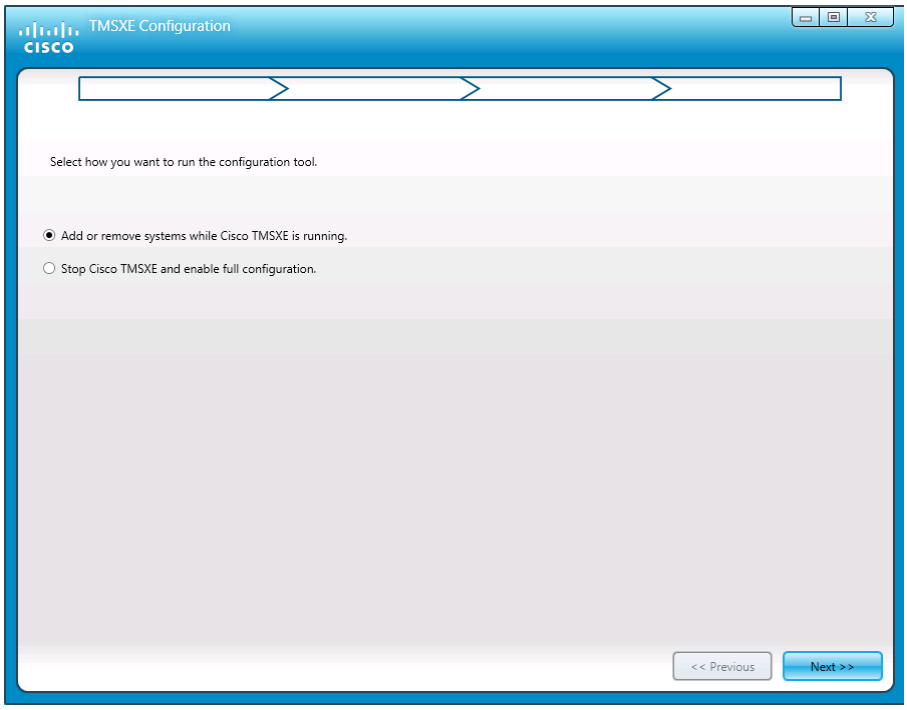
If any booking or modification requests are made while the service is halted, they will be queued and then processed as soon as the service is restarted.

Launching the configuration tool

To launch the tool, do one of the following:

- Go to the Windows Server **Start** menu or Start screen: **Start > All Programs > Cisco > Cisco TMSXE Configuration**
- Run it as administrator from the command prompt. The configuration tool is located in the Cisco TMSXE installation folder, by default the program path is **C:\Program Files\Cisco\TMSXE\ConfigurationApp.exe**.

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 full 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.

Note that while systems can be added and removed without stopping the Cisco TMSXE service, replacing an endpoint or mailbox, or re-adding one that has previously been removed, requires stopping the service and enabling full configuration mode in the configuration tool.

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 [p.24].
3. Ensure that the mailboxes are correctly configured, following the instructions in Configuring the room mailboxes [p.25].
4. Start the configuration tool by going to **Start > All Programs > Cisco > Cisco TMSXE Configuration**.
5. Select *Add or remove systems while Cisco TMSXE is running* and click **Next**.
6. There are two ways to add endpoints:
   - Manually add each endpoint:
     i. 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.

     ii. Select endpoints in the left-hand list and click **>>** to add them to Cisco TMSXE. Use **`Ctrl`** or **`Shift`** to select multiple endpoints.

     iii. 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
     ```

7. 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.
8. 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. Select *Add or remove systems while Cisco TMSXE is running* and click **Next**.
3. In the list of systems added to Cisco TMSXE, locate the system(s) you want. Use **`Shift`** or **`Ctrl`** to select multiple systems. Click **<<**.
4. When done, click **Save** to validate the remaining systems.
5. 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 the Exchange Integration Option license flag

If using the Exchange Integration 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 full 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 Only* 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 Only* 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.

Conference routing unsuccessful

Multipoint Control Units (MCUs) are used for routing conferences involving multiple endpoints.

When an organizer tries to book a conference that will be automatically routed, Cisco TMS locates and reserves the necessary routing resources if they are available.

If MCU resources are insufficient or unavailable at the requested time:

1. Cisco TMS will decline the booking.
2. Cisco TMSXE will not pass this message along to the organizer, but instead request that Cisco TMS simply reserve the endpoints without routing.
3. Cisco TMS re-processes the request as a *Reservation* conference.
4. Provided the endpoints can be booked, confirmation is sent to Cisco TMSXE, and the organizer is notified that the request was only partially successful.

Note that if routing is unavailable for one occurrence of a meeting series, the entire series will be "downgraded" to *Reservation*.

When modifying existing bookings:

- if modifying a single occurrence of a meeting series, any resulting downgrades will now only apply to the occurrence.
- if modifying an ongoing meeting, Cisco TMSXE will not downgrade the meeting unless the time of the meeting is changed to outside the original meeting timespan. If not modifying the time of the meeting, adding unavailable rooms will cause those rooms to be dropped, leaving the original booking intact.

The notification sent to the organizer includes detail on why routing failed and a suggestion to ask the videoconference administrator for assistance.

Beyond scheduling conflict/capacity issues, potential reasons for failed routing include, but are not limited to:

- Dial protocol compatibility issues, for example, an H.323-only endpoint trying to dial a SIP-only endpoint, with no interworking configured.
- A dial-out participant has no provided number.
- Conference requires encryption, but one participant does not support or signal support for encrypted communication.
- The route contains one or more systems that have been deleted from Cisco TMS.

Alternate reason for downgrade

Due to replication delays, Exchange and Cisco TMS will for short periods of time have divergent information about which resources are available.

If a booking is created or updated from Outlook and contains a room resource that is booked in Cisco TMS during this time, Cisco TMSXE will downgrade the meeting to *Reservation* and send a "Conference routing unsuccessful" message to the organizer with information about the unavailable resource.

While this is not a frequent scenario, it is important to note that it is not solved by addressing routing resources. As soon as replication has completed, the meeting can be re-booked with any connection type, without the unavailable room resource.

For more information about replication delays, see The booking process [p.19].

Re-submitting the routing request

If able to free up existing routing resources, add MCU capacity, or otherwise resolve the resource issue, the connection type of the conference must be explicitly modified using either Cisco TMS, the Cisco TelePresence form in Outlook, or WebEx Productivity Tools with TelePresence by adjusting the connection type back to that originally requested.

If there is a capacity issue and MCU capacity cannot be made available at the requested time, the conference must be rescheduled.

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.

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

Template name	Description
ConferenceDowngraded	Subject for notification that a booking with routing requested, has been booked as *Reservation*, usually due to lack of routing resources. See Conference routing unsuccessful [p.58].
ConferenceSaved	Subject for notification that a conference has been successfully booked or updated.
UnknownProcessingError	Subject for notification of failed booking or update.
BookingBodyConferenceDowngraded	Notification body template for when a meeting has been downgraded to *Reservation Only*.
BookingBodyConferenceDowngraded MigrationMode	Identical to the above, but used in "migration" mode when existing bookings in Exchange are re-booked in Cisco TMS. Contains information to organizers that videoconference backend changes are ongoing.
BookingBodyConferenceDowngraded AndSomeWereNotBooked	Notification body template for when a meeting has been downgraded to *Reservation Only* and some requested endpoints were not available.
BookingBodyConferenceDowngraded AndSomeWereNotBookedMigrationMode	Identical to the above, but used in "migration" mode when existing bookings in Exchange are re-booked in Cisco TMS. Contains information to organizers that videoconference backend changes are ongoing.
BookingBodyUnknownProcessingError	Notification body template for error situations where a request could not be processed. Contains an error message from server.

Template name	Description
DeclineBody	Notification body template for when a system could not be booked in Cisco TMS.
DeclineBodyMigrationMode	Identical to the above, but used in "migration" mode when existing bookings in Exchange are re-booked in Cisco TMS. Contains information to organizers that videoconference backend changes are ongoing.
RouteBody	Template for routing information for Cisco TMS. If there is a particular service or person that organizers should contact when encountering routing problems, such information may be added to this template.
TMSParticipantWithoutDisplayName ButOnlyId	Template that determines how to refer to systems that do not have a display name set in Cisco TMS.

Modifying the templates

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 and restoring Cisco TMSXE

Align your Cisco TMSXE backup strategy with your Cisco TMS database (**tmsng**) backup strategy. For an overview of database maintenance best practices, see the "Database maintenance planning" section of *Cisco TMS Installation and Upgrade Guide*.

When restoring Cisco TMSXE from backup, you must:

- restore the Cisco TMS **tmsng** database at the same time.
- ensure that the Cisco TMSXE backup is taken very shortly before the tmsng backup. We recommend scheduling Cisco TMSXE backups 10 minutes earlier than the database backups.

Setting up a backup routine

To set up regular Cisco TMSXE backups:

1. Identify the backup interval you use for backing up **tmsng** as described above.
2. Set up a scheduled task that backs up the Cisco TMSXE configuration and storage directories. In a clustered deployment, these will be on a file share. In a default setup with no clustering, the locations are:
   - **C:\ProgramData\Cisco\TMSXE\Config**
   - **C:\ProgramData\Cisco\TMSXE\Storage**
3. Configure the backup interval to match the tmsng backup interval, and ensure that the Cisco TMSXE backups are scheduled to run ten minutes prior to the scheduled tmsng backup.

Restoring from a backup

To restore Cisco TMSXE from a backup:

1. Stop the Cisco TMSXE service, on both servers if in a clustered deployment.
2. Replace the current configuration and storage folders with the backed-up versions.
3. Note that replacing folders may reset folder permissions. Verify that the NETWORK SERVICE account still has *Full control* permissions to both folders.
4. On the Cisco TMS server, stop all six windows services starting with "TMS" and the IIS service (World Wide Web Publishing Service).
5. Using SQL Server Management Studio, restore the **tmsng** database to a snapshot created 10 minutes after the Cisco TMSXE backup you have already restored to.
6. Start all TMS services and IIS.
7. Start the Cisco TMSXE service, on both nodes if in a clustered deployment.
   Cisco TMSXE will now reprocess all Exchange bookings and updates since the restore point, and push them to Cisco TMS again. Organizers will then get new acceptance and decline email messages for all changes made during this window. Note that conferences potentially could get new bridge numbers when they are reprocessed.

Backing up for an upgrade

You can use the procedure above to back up and restore Cisco TMSXE in the case of needing to roll back an upgrade as well, with the following additions:

1. Prior to upgrading, create a fresh copy of the Cisco TMSXE configuration and storage folders.
2. Immediately after creating that backup, back up the **tmsng** database as well.
3. Upgrade Cisco TMSXE to the new version.
4. If you have to roll back Cisco TMSXE to the previous version after the upgrade, follow the steps in Restoring from a backup [p.61], but use the Cisco TMSXE files and **tmsng** backup from steps 1 and 2 above instead of copies from scheduled backups.

WebEx Enabled TelePresence users

Note that this procecure does not roll back WebEx bookings, and that duplicate WebEx bookings may occur as a result.

Restoring on a different server

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 or servers hosting Cisco TMSXE.

This also means that in order to retain encrypted passwords in the event that you need to restore Cisco TMSXE on a different server, a full backup of Cisco TMSXE must include the entire OS of the server, or both servers in a clustered deployment.

However, if retyping the passwords when reinstalling after a restore is an acceptable option, the backup procedures described above are sufficient.

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 [p.39].

Moving the application

1. Install Cisco TMSXE on the new server. For instructions, see Performing a new installation [p.31].
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 4.0 [p.63] if not decommissioning the server itself.

Uninstalling Cisco TMSXE 4.0

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**.

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 [p.35].

- **TMSXE-log-file.txt** logs the activities of the Cisco TMSXE Windows service
- **TMSXE-decline-downgrade-log-file_YYYYMMDD.txt** is a filtered view of the above, see Filtered log for declined and downgraded conferences [p.65].
- **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.

The 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.

Filtered log for declined and downgraded conferences

The log file **TMSXE-decline-downgrade-log-file_YYYYMMDD.txt** is created every day 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 for all of the above logs:

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 the log. We strongly recommend reverting the log level back to "INFO" after debugging. The steps to revert are the same as above.

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)*.

The 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.

The 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. 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 [p.23].

Mailbox database is temporarily unavailable

If you get the above error message when validating the Exchange Web Services settings during configuration, Cisco TMSXE is failing to connect to Exchange.

You may need to restart the Exchange Information Store before retrying the validation step. See the Microsoft knowledge base article *Services for Exchange Server 2007 or Exchange Server 2010 cannot start automatically after you install Exchange Server 2007 and Exchange Server 2010 on a global catalog server* for more information.

The Client Access Server version does not match ...

If you get an error message when submitting the Exchange connection details that "The Client Access Server version does not match the accessed resource's Mailbox Server version", you have likely changed your deployment to use Exchange 2010, but forgotten to update the Exchange server address to be that of the 2010 CAS server.

Update the server address and try validating again.

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 always installing the latest cumulative time zone update, the minimum requirement for compatibility being the December 2010 cumulative update.

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 [p.9].
- 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.

The 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 [p.65].

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 [p.68].

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 [p.24] 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

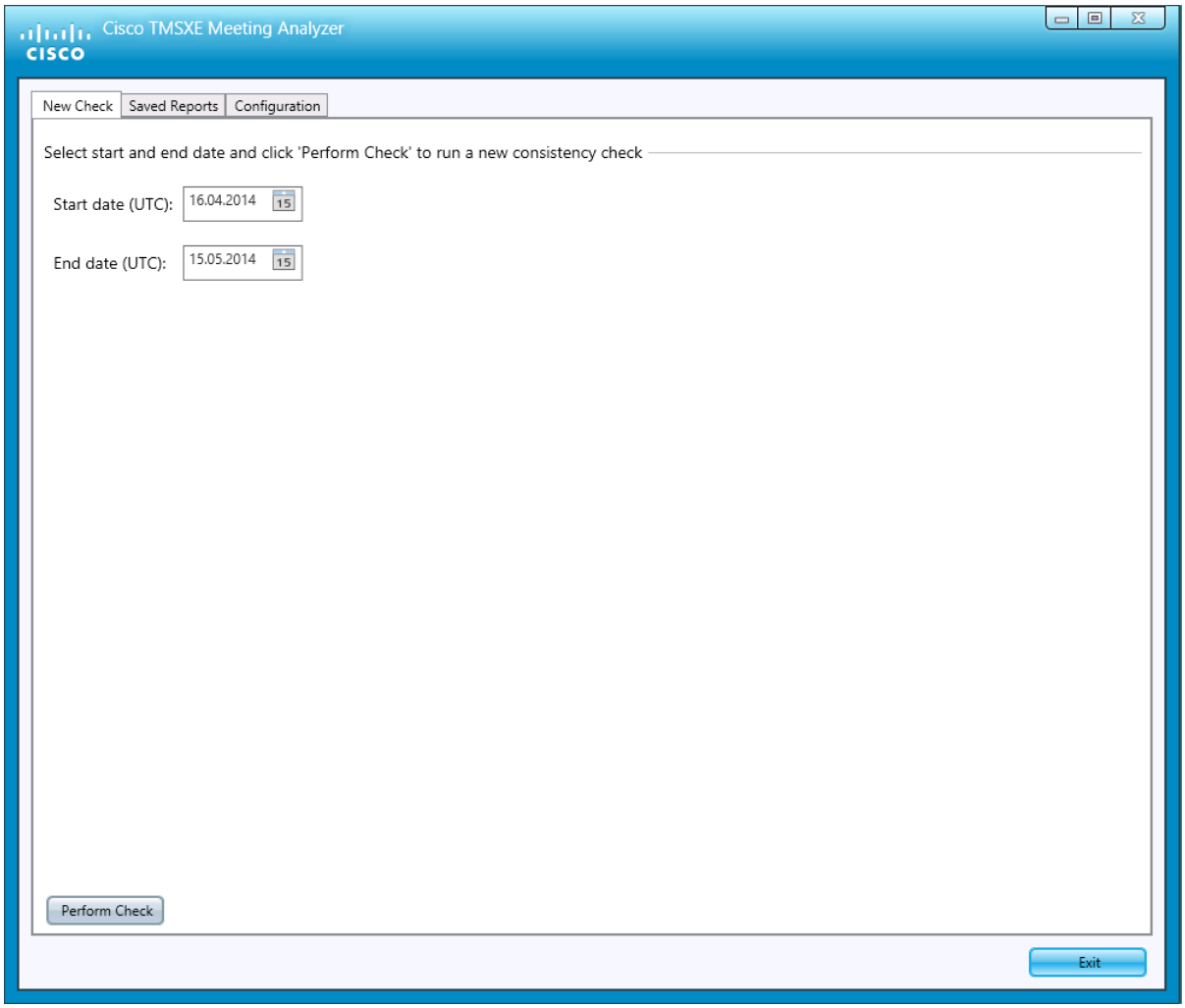
If bookings do not replicate neither to or from Exchange:

- Check the event log for connection issues with Exchange or Cisco TMS. (See Reading the Windows event log [p.65].)
- 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 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

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

Best practices

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 running Meeting Analyzer off hours.

If urgent troubleshooting is needed during business hours, run Meeting Analyzer with the shortest possible date range to reduce impact on server performance.

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

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 inconsistencies

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.

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.

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 the CLI, run **BookingConsistencyCheckerCommand.exe**. Note that it must be run directly from its location, the command may not include the entire file path.

Table 6: 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 **BookingConsistencyCheckResult-{{timestamp}}.xml**.

For instructions on setting up scheduled tasks in Windows Server 2008 and 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.

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 [p.76].

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.

Parameter name	Description	Cisco TMSXE Default	Note
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.
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.

Parameter name	Description	Cisco TMSXE Default	Note
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 without data loss.

Administrators configuring Cisco TMSXE without an Active Directory connection must choose whether to allow Cisco TMS to generate users based on organizer email addresses, which may or may not correspond to existing users in Cisco TMS. This setting is called **Allow organizers without usernames (Non-AD Mode only)**. If disabled, all meetings booked through Cisco TMSXE will be owned by the service user in Cisco TMS, rather than linked to an individual organizer.

Installing with Non-AD mode

To be able to run Cisco TMSXE in Non-Active Directory mode, launch the Cisco TMSXE installer by entering the following on the command line:

```
TMSXESetup.msi NONADCONNECTIONMODE=1
```

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

Configuring Non-AD mode

- On the **Exchange Web Services** tab of the configuration tool, enable **Non-Active Directory Mode**. Confirm by clicking **Go to Non-AD Mode** in the dialog that opens.
- On the **Advanced 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.

WebEx Enabled TelePresence

For WebEx Enabled TelePresence 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 [p.65] for instructions on locating and using the logs.

When the process has completed, a DEBUG 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 [p.65] 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 [p.78] .

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.

Notices

Technical support

If you cannot find the answer you need in the documentation, check the website at www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit: www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

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	Revision	Description
July 2014	02	Upgrade instructions updated to include information on clustering. Section on backing up and restoring Cisco TMSXE added. Procedure for setting up file share and file permissions for clustering made more explicit. Caution added that non-AD mode should only be used in very particular scenarios and after consulting with Cisco.
May 2014	01	Release of Cisco TMSXE 4.0. First publication of this deployment guide, which replaces the separate installation and administrator guides for Cisco TMSXE.