Cisco TelePresence Management Suite Extension for Microsoft Exchange

Installation Guide

Version 3.1.3

D14890 07

December 2013

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 installation guide describes how to prepare for and set up a new deployment, as well as upgrading from a previous versions of Cisco TMSXE. Initial configuration and troubleshooting of the installation are also included in this guide.

For a functional overview of the application, see *Cisco TelePresence Management Suite Extension for Microsoft Exchange Administrator Guide*.

Migration from versions prior to 3.0 unsupported

Migrating from Cisco TMSXE 2.x is not supported in 3.1.3.

If your current version of Cisco TMSXE is earlier than 3.0:

1. Migrate to Cisco TMSXE 3.0.2 using the accompanying tools and documentation.
2. Upgrade to Cisco TMSXE 3.1 following the instructions in this guide.

Prerequisites

This section details the prerequisites and best practices for installing Cisco TMSXE3.1.3, whether performing a new installation or upgrading from a previous version of the product.

System requirements for Cisco TMSXE

Hardware requirements

Minimum hardware requirements for Cisco TMSXE are identical to the recommended hardware requirements for the supported operating systems.

Software requirements

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

Virtual machines

Installing and running Cisco TMSXE on a virtual machine is supported, as long as the VM meets the recommended requirements for running Windows Server 2008 or Windows Server 2008 R2.

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.14].
- be located in the same forest as Cisco TMS if organizers are to be able to authenticate with Cisco TMS.

Note that 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

Booking Service requires HTTPS to be configured for DefaultSite in IIS on the Cisco TMSXE server.

If IIS is not present on the server prior to installation of Cisco TMSXE, it will be automatically installed with Booking Service. HTTPS must then be configured after installation to allow Booking Service to operate.

Cisco TMS requirements

Version	14.3 or later
Network	HTTPS (recommended) or HTTP connectivity is required from the Cisco TMSXE server to Cisco TMS.

Licensing

In order to use Cisco TMSXE, you must have either:

- 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 systems to be integrated.

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

Note that each telepresence endpoint to be integrated with Exchange must already have been added to, and licensed for use with, Cisco TMS.

Once the Cisco TMSXE – Extension for Microsoft Exchange option key has been activated in Cisco TMS, the **Allow Remote Bookings** setting determines whether each system is using a license. (Note that if an Application Integration Package option is also activated, the setting will be void and therefore hidden.)

The first time Exchange booking is used for a system, **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 still be set to *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.

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:

- A WebEx Enabled TelePresence option key.
- One or more WebEx sites.
- Single sign-on or specified WebEx credentials for each user (not service user).

For guidance on setting up WebEx Enabled TelePresence, see *WebEx Enabled TelePresence 2.0 Configuration Guide for Cisco TelePresence Management Suite*.

Microsoft Exchange requirements

Requirement	Description
Microsoft Exchange	Supported versions: ■ Microsoft Exchange 2010 Service Pack 3 recommended and required if using the Cisco TelePresence form. If not using the form, Service Pack 2 is supported. Note that errors will be logged on system connect if using SP2, and that support for SP2 will be discontinued in a coming release of Cisco TMSXE. ■ Microsoft Exchange 2007 Service Pack 3
Windows Server	Supported versions: ■ Microsoft Windows Server 2008 R2 ■ Microsoft Windows Server 2008
Exchange Web Services (EWS)	Must be enabled on the Exchange server.
Throttling policies	For Microsoft Exchange 2010, special throttling policies must be applied to allow sufficient traffic load from Cisco TMSXE to Exchange via Exchange Web Services (EWS). See Applying the Cisco TMSXE Throttling Policy for Exchange 2010 [p.20]

Redundant Client Access Servers

Cisco TMSXE supports redundant client access servers (CAS), provided that a network load balancer is set up with a sticky IP connection (affinity) to one CAS server. For guidance on configuration, see the TechNet article *Load Balancing Requirements of Exchange Protocols*.

If the network load balancer cannot reach this primary CAS,Cisco TMSXE will be redirected to another CAS and re-subscribe to resource mailboxes, as subscriptions are stored per CAS instance. This may impact performance while re-subscription is ongoing.

Requirements for certificate authentication (optional)

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 supports booking with:

- Microsoft Outlook 2007 SP2
- Microsoft Outlook 2010
- Outlook Web Access (Exchange 2007)
- Outlook Web App (Exchange 2010)

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

Before installing Cisco TMSXE 3.1.3, make sure both Outlook and Exchange are already set up so that users are able to book meetings that include room mailboxes.

Deployment best practices

We recommend installing Cisco TMSXE on a standalone server.

Small deployments

Cisco TMSXE may be co-located with Cisco TMS in smaller deployments, with the following prerequisites:

- The server must have a minimum of 4GB RAM.
- A maximum of 50 telepresence endpoints are available for booking in Cisco TMS and Cisco TMSXE.

Large deployments

With a default configuration, Cisco TMSXE supports up to 500 resource mailboxes linked to endpoints in Cisco TMS.

If planning a deployment with more than 500 systems bookable through Cisco TMSXE, contact your Cisco support representative for guidance, and refer to identifier CSCum00849. With specific configurations available from Cisco, up to 5000 mailboxes are supported.

Security

We strongly recommend setting up Cisco TMSXE to use secure (HTTPS) communication with both Cisco TMS and Exchange Web Services.

If one or both servers present a certificate that is not valid, the Cisco TMSXE configuration tool will offer the option of allowing untrusted certificates. We strongly advise only allowing this if the installation is purely for testing purposes. The setting cannot be reverted.

For more information, see Setting up secure communication [p.24].

Virtualization

Cisco TMSXE may be installed on a virtual machine. See System requirements for Cisco TMSXE [p.6] for information on virtual server requirements.

Redundancy

Deploying Cisco TMSXE with a redundant Cisco TMS setup is supported when employing a network load balancer as described in the "Redundant deployments" chapter of *Cisco TelePresence Management Suite Administrator Guide*.

Redundant setups of Cisco TMSXE are not supported in the current version.

Advanced settings and the Cisco TelePresence form

Deployment and use of the Cisco TelePresence custom meeting request form, which makes advanced conference settings available to Outlook users, is optional. Note that editing this form is not supported.

If deploying 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

We strongly recommend against using delegates for room mailboxes that are added to Cisco TMSXE, as this will lead to out-of-sync conditions where Exchange and Cisco TMS do not have the same booking information.

Additionally, 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** (note that combining this setting with the above setting will lead to blank meeting subjects)
- **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 there. 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 Exchange 2010 mailboxes [p.18] and Configuring Exchange 2007 mailboxes [p.17] for detailed instructions on the required and supported settings for mailboxes.

Booking limitations

Booking through Cisco TelePresence Management Suite Extension Booking API has the following limitations:

- The use of setup and teardown buffers in Cisco TMS is not supported.
- 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 default 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.
- You cannot move a meeting from the past to the future. This includes changing the start time of a meeting that is already ongoing.

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 modifying a recurrent series while an occurrence is ongoing:

- changing the start time will be applied to the entire series, and the ongoing meeting will be disrupted. Meetings set to connect automatically will be reconnected.
- any other modifications will be applied to upcoming instances only, and the ongoing meeting will be marked as an exception in Cisco TMS.

Preparing to install

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.

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

Backing up mailboxes

We recommend always backing up all existing room mailboxes from Exchange prior to upgrading or installing Cisco TMSXE.

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

Installing or upgrading Cisco TMS

When preparing to install Cisco TMSXE, start by installing/upgrading to the latest version of Cisco TMS (14.2 or later 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. Stop the Cisco TMSXE Windows service if you have an existing installation.
2. Follow the instructions in the installation guide to upgrade Cisco TMS, making sure to back up the database when prompted.
3. Run the Cisco TMS Time Zone Update Tool on the Cisco TMSXE server if you have an existing installation. Instructions are in the Cisco TMS installation guide.
4. Install or upgrade Cisco TMSXE following the instructions in this document.

Preparing for an upgrade

After upgrading to Cisco TMS 14.2, consider whether you need to run the Cisco TMS Time Zone Update Tool on the Cisco TMSXE server before upgrading Cisco TMSXE.

Cisco TMS 14.2 introduced time zone support for all booking-related data. As this support was previously missing, some bookings created using earlier versions of Cisco TMS and its extensions may currently have incorrect time zone information. This is mostly an issue for recurrent meeting series that span a daylight savings time (DST) change event.

Run the time zone update tool following the procedures provided if:

- You have users scheduling conferences from both the United States and Europe, or both the northern and the southern hemispheres.

- You are in a country where DST rules vary between states or regions, for example Australia.

You do *not* need to perform these procedures if Cisco TMS and all organizers booking meetings on your telepresence network are in the same time zone or in time zones with the same DST rules, such as the United States excluding Arizona and Hawaii.

Procedures for obtaining and running the tool are provided in *Cisco TelePresence Management Suite Installation Guide*. Finish these procedures before upgrading Cisco TMSXE.

Re-replication after upgrade

Note that when starting the Cisco TMSXE service after upgrading to 3.1.3, all bookings will be re-replicated to remove inconsistencies that may exist between Exchange and the Cisco TMS database. With a large database, this process may take as long as 3-5 hours, but the application will be operative while this is ongoing.

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 3.1.3 if:

- You do not have an existing deployment of Cisco TMSXE 3.0.x, 2.3.1, 2.3, or 2.2.
- 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 (if the version is 3.0.x).

Migrating from Cisco TMSXE 2.x is not supported in 3.1.3.

If your current version of Cisco TMSXE is earlier than 3.0:

1. Migrate to Cisco TMSXE 3.0.2 using the accompanying tools and documentation.
2. Upgrade to Cisco TMSXE 3.1 following the instructions in this guide.

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.

Note that once you have set up Cisco TMSXE to use this service user, you must not change service users, whether during operation, or as part of an upgrade. The link between meetings in Exchange and Cisco TMS is tied to the service user GUID.

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.15] 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/ord 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**, and **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 Only*, 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 Cisco TelePresence advanced settings form [p.37].

For information on configuring Cisco TMSXE for WebEx Productivity Tools with TelePresence, see WebEx Productivity Tools with TelePresence [p.36].

For more detail on how booking works for users, see *Cisco TelePresence Management Suite Extension for Microsoft Exchange User Guide (3.1.3)*.

Adding Cisco TMS managed endpoints to Exchange

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

Use the Exchange Management Console (EMC) to create one room mailbox for each of your endpoints, such as **`boardroom@example.com`**. See the Microsoft Exchange documentation for details on how to create room mailboxes.

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 to give theCisco TMSXE service user full access permission. Follow the instructions for your version of Exchange in Configuring the room mailboxes [p.16].

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.16].

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.

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

Configuring Exchange 2007 mailboxes

All room mailboxes must be configured to treat resource information identically to avoid conflicts. Permissions can be set either using the console or the shell, properties must be set using Exchange Management Shell.

Granting Full Access Permission for the service user

There are two ways to set these permissions.

Using 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 step 2 in the Exchange Management Shell instructions below.

If using 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 [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.
`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.

Shell parameter	Required value	Description
`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 Deployment best practices [p.10].

To verify that the above settings are active, use the shell command **`Get-MailboxCalendarSettings -id [mailbox]|fl`**

For more information about the above parameters, see *Set-MailboxCalendarSettings (Exchange 2007 Help)*.

When you have completed configuration for all mailboxes, proceed to Setting up secure communication [p.24].

Configuring Exchange 2010 mailboxes

All room mailboxes must be configured to treat resource information identically to avoid conflicts. Most permissions and properties for room mailboxes in Exchange 2010 can be set either using the console or the shell.

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.

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.

Console field	Shell parameter	Required value	Description
Enable the Resource Booking Attendant (**Resource General** tab)	`AutomateProcessing`	*AutoAccept*	Sets the mailbox to automatically process invitations
Booking window (days) (**Resource Policy** tab)	`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)**.
Reject repeating meetings that have an end date beyond the booking window (**Resource Policy** tab)	`EnforceSchedulingHorizon`	*True*	Specifies that recurring meetings that continue outside of the booking window will be rejected.
Allow conflicting meeting requests (**Resource Policy** tab)	`AllowConflicts`	*False*	Prevents the mailbox from accepting overlapping bookings, which is not supported by Cisco TMS.
Conflict percentage allowed (**Resource Policy** tab)	`ConflictPercentageAllowed`	*0*	
Maximum conflict instances (**Resource Policy** tab)	`MaximumConflictInstances`	*0*	Prevents the mailbox from accepting recurrent meetings where some instances conflict with existing bookings.
Delete the subject (**Resource Information** tab)	`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.

Console field	Shell parameter	Required value	Description
Add the organizer's name to the subject (**Resource Information** tab)	`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.
Remove the private flag on an accepted meeting (**Resource Information** tab)	`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 Deployment best practices [p.10].
	`CalendarRepairDisabled` (Set-Mailbox)	*True* (strongly recommended)	Disables the Calendar Repair Assistant (CRA) for the mailbox. There is no GUI option to modify this setting.

To verify that the above settings are active, use the shell command **`Get-CalendarProcessing -id [mailbox]|fl`**

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

For more information on the above console settings, see the Microsoft TechNet article *Configure User and Resource Mailbox Properties*.

When all Exchange 2010 room mailboxes are configured, proceed to Applying the Cisco TMSXE Throttling Policy for Exchange 2010 [p.20].

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.23].

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`**.

Setting up 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 green certificates to Cisco TMSXE.

Certificate requirements

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

- matches the host name of the machine that the certificate is issued for.
- 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 their host names.

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

1. Launch Internet Explorer on the Cisco TMSXE server.
2. Enter the URI for the Exhange Server and verify that the URI field turns green.
3. Enter the URI for the Cisco TMS server and verify that the URI 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.

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 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 Telepresence with WebEx 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.8] are met.

Creating and configuring the mailbox

Create and configure the mailbox using either Exchange Management Console or Powershell:

1. Create a new user mailbox called "WebEx".
   See Create a Mailbox (Exchange 2010 Help) or How to Create a Mailbox for a New User (Exchange 2007 Help) for instructions.
2. Give the Cisco TMSXE service user account Full Mailbox Access to this mailbox.
   See Allow Mailbox Access (Exchange 2010 Help) or How to Allow Mailbox Access (Exchange 2007 Help) for instructions.
3. Modify mailbox properties:
   a. Turn off the Calendar Attendant for the mailbox.
      See Configure User and Resource Mailbox Properties (Exchange 2010 Help) or How to Disable the Auto-Processing of Meeting Messages (Exchange 2007 Help) for instructions
   b. Make sure new requests are not automatically marked as tentative by disabling **AddNewRequestsTentatively** (**Mark new meeting requests as Tentative** if using the Calendar Settings tab) for the mailbox.
   c. Set **ForwardRequestsToDelegates** to *False*.
   d. Exchange 2010 only: Set **`CalendarRepairDisabled`** to *True*.

Additional recommendations

We also recommend the following configurations:

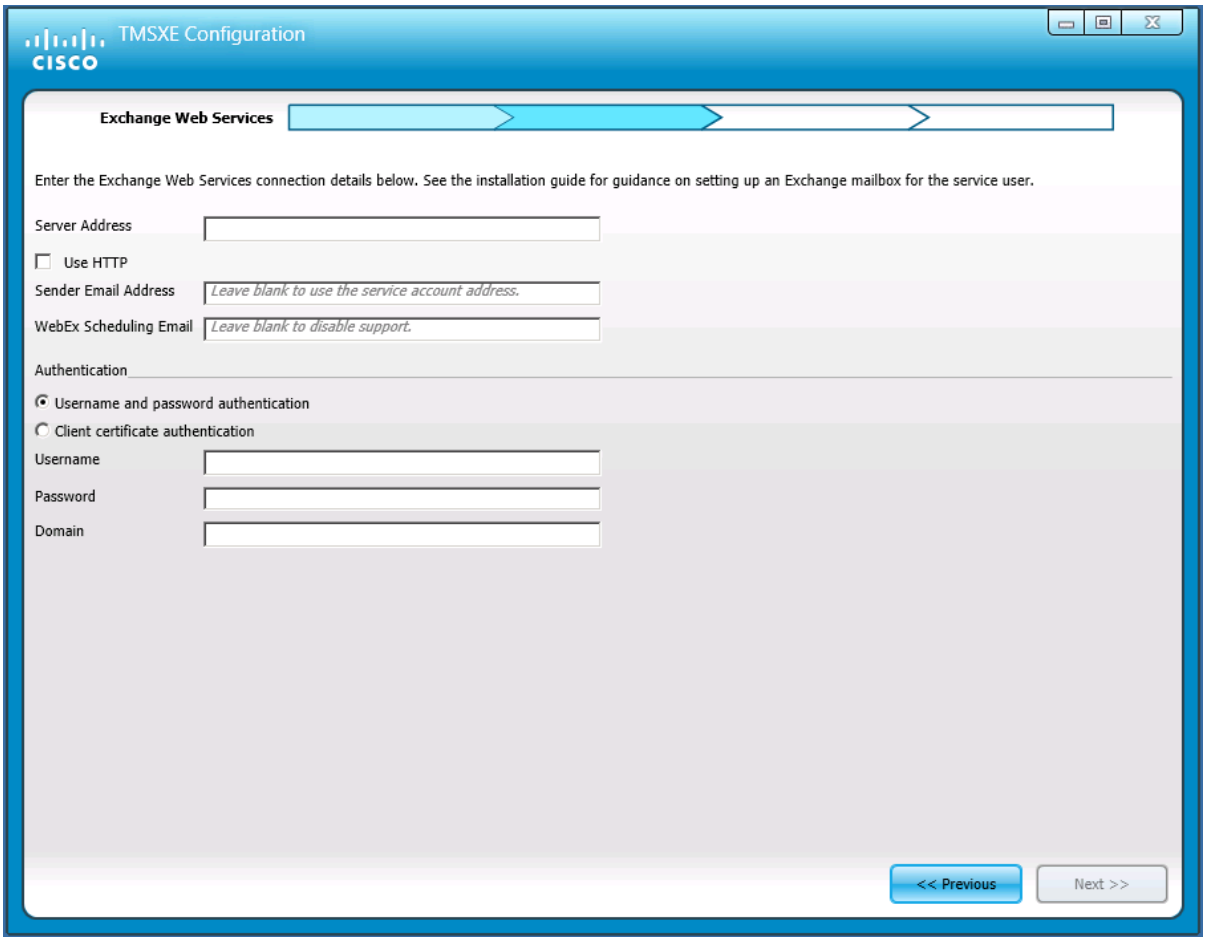
- Using Exchange Management Console **Mail Flow Settings** or Powershell, stricten the message delivery restrictions as needed.
  For example, require senders to be authenticated, only allow from people in a specific group or similar.
  See *Configure Message Delivery Restrictions (Exchange 2010 Help)* or *How to Configure Message Delivery Restrictions (Exchange 2007 Help)* for instructions.
- 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.


TMSXE Configuration
cisco
Exchange Web Services
Enter the Exchange Web Services connection details below. See the installation guide for guidance on setting up an Exchange mailbox for the service user.
Server Address
Use HTTP
Sender Email Address
Leave blank to use the service account address.
WebEx Scheduling Email
Leave blank to disable support.
Authentication
Username and password authentication
Client certificate authentication
Username
Password
Domain
<< Previous
Next >>

3. Click **Save**.

Upgrading to Cisco TMSXE 3.1.3

After upgrading Cisco TMSXE from a 3.x version, a re-replication of all bookings in Cisco TMS will be performed on startup. This process will 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. We therefore strongly recommend performing the upgrading during off hours.

Before you start

Make sure that:

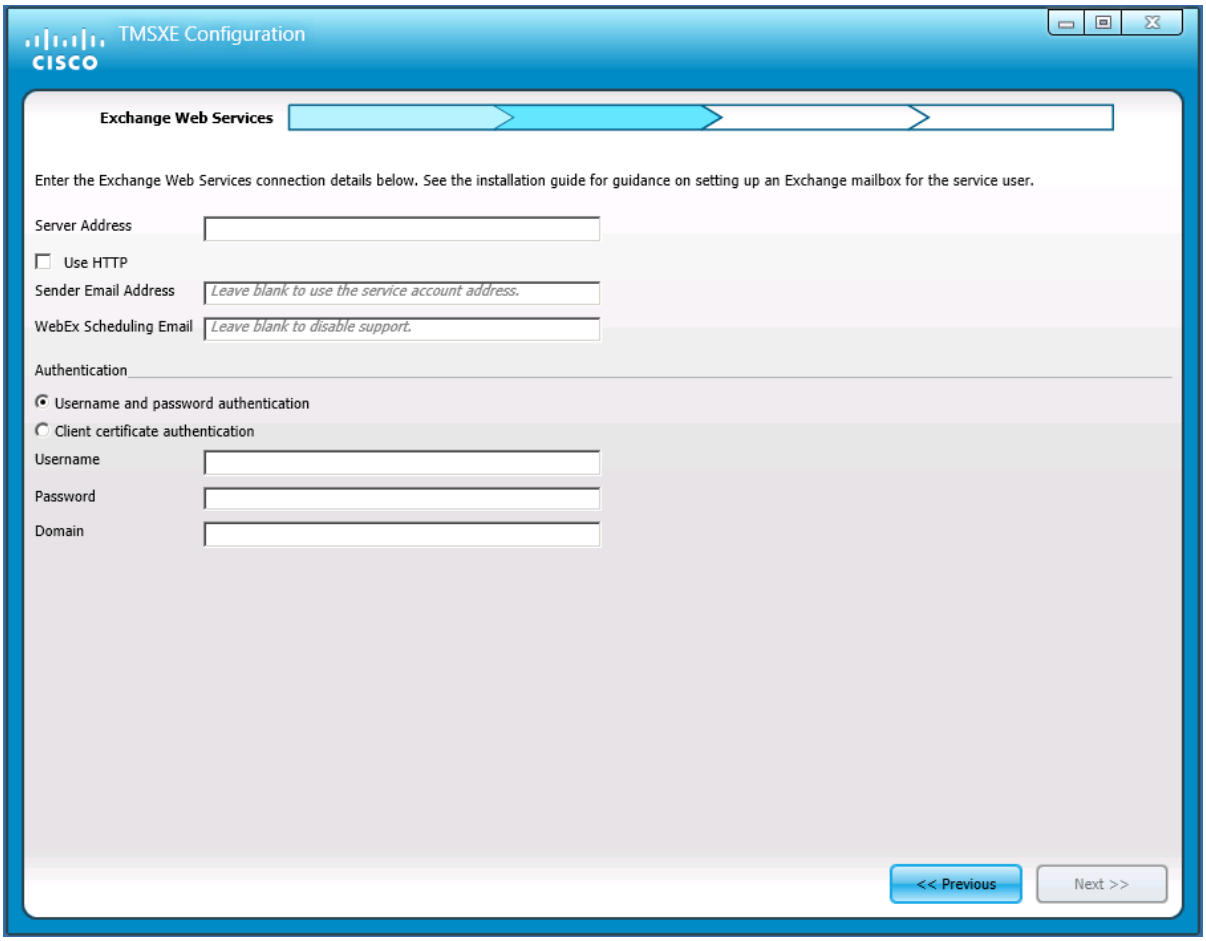
- All Prerequisites [p.6] are met.
- You have considered all Deployment best practices [p.10].
- You have followed the steps in Backing up and upgrading the backend [p.13], including the time zone update if required.

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. The installer will detect that you have a previous installation of Cisco TMSXE. Click **Upgrade** to do so.
5. Click **Next** to start the setup.
6. Accept the terms in the license agreement and click **Next**.
7. If you are going to use Cisco TMSXE with WebEx Productivity Tools with TelePresence:
   a. Opt to include Cisco TMS Booking Service.
   b. Modify or confirm the name of the IIS application pool to which you want the Booking Service installed.
8. Follow all remaining instructions provided by the installer.
9. 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. If you have configured a WebEx Scheduling Mailbox, add the email address for this mailbox at the Exchange Web Services step.



3. Click **Finish** when all settings have been validated.
   A prompt will ask you whether you want to start the Cisco TMSXE service. If you decline, follow the instructions in Starting the service [p.42] when you are ready to start Cisco TMSXE.
   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.

Monitoring and following up on re-replication

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.45] 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.45] for instructions on locating and using the logs.

You will also find separate statements for each affected system, including theirCisco 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 inConfiguring Cisco TMSXE [p.27] .

The -resetAllTransactionsIds switch

The **`-resetAllTransactionIds`** switch is intended to initiate a one-time cleanup to clean up discrepancies between Cisco TMS and Exchange caused by issues in a previous version and changes to time zone handling.

CAUTION: Do not use this switch unless performing an upgrade as described above or expressly instructed to use it by a Cisco representative. The re-replication process may take a very long time to complete and must be performed off-hours, as the systems will be out of sync until the process has completed.

Performing a new installation

This section describes the required steps to install Cisco TMSXE 3.0 or later with Exchange 2007 or Exchange 2010 when no previous Cisco TMSXE deployment exists.

Before you start

Make sure that:

- All Prerequisites [p.6] are met.
- You have considered all Deployment best practices [p.10].
- You have completed all steps described in Preparing for a new installation [p.14].

Running the installer

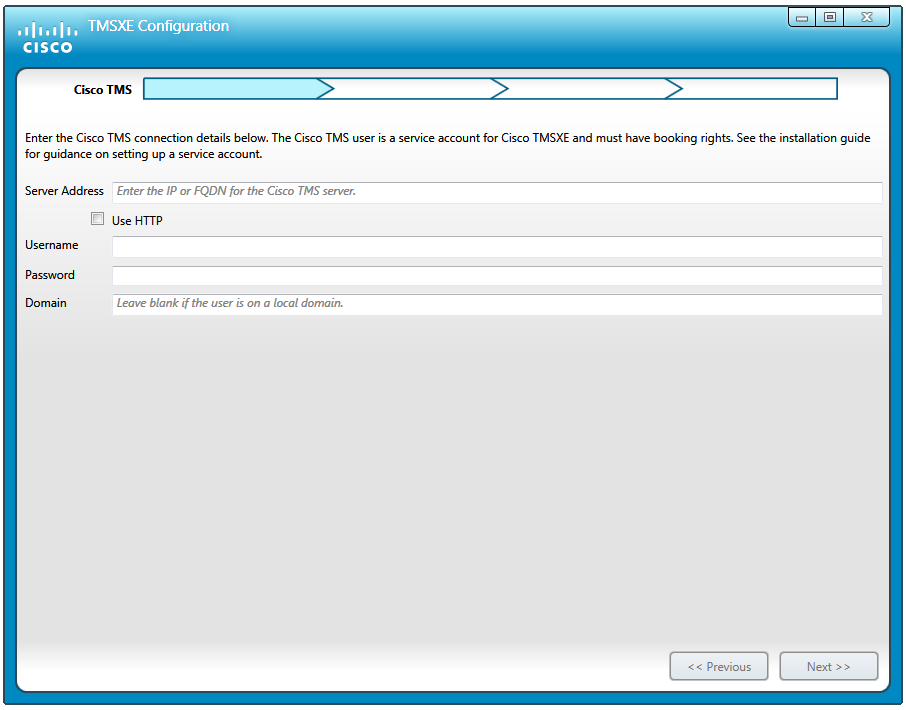
1. Check Windows Update and install any critical updates to the .NET framework on the server where Cisco TMSXE will be installed. Make sure the .NET version is 4.0 or later. Reboot the server after installing if prompted.
2. Place the installation files on the server.
3. Run the Cisco TMSXE installer and accept the End-User License Agreement (EULA) to start the installation process.
4. Select *Perform a new installation* as your installation mode.
5. Follow all instructions provided by the installer.
6. If you are going to use Cisco TMSXE with WebEx Productivity Tools with TelePresence:
   a. Opt to include Cisco TMS Booking Service.
   b. Modify or confirm the name of the IIS application pool to which you want the Booking Service installed.
7. Click **Finish** when the installation is done to close the installer window and launch the Cisco TMSXEconfiguration tool.

Configuring Cisco TMSXE

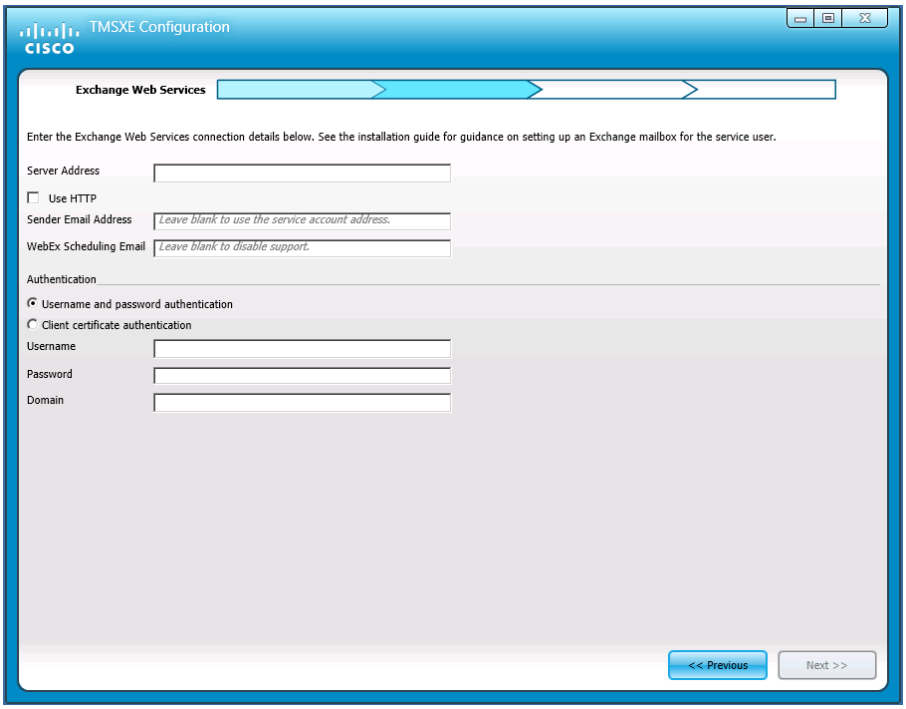
Most fields in the configuration tool are required. Clicking **Next** validates the settings provided for each step of the initial configuration. If one or more settings cannot be validated, you will be returned to the previous step to allow for corrections.

This procedure describes each step of the configuration process. For detail on each of the available fields, see the Configuration reference [p.33] 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 with a valid certificate, 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.



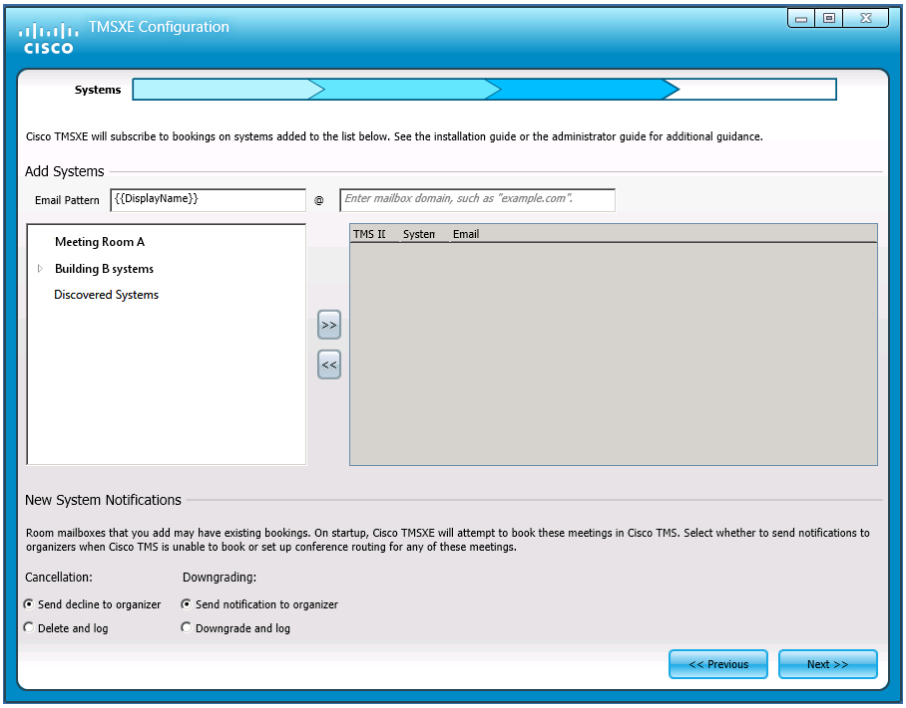
2. For **Exchange Web Services** provide all connection details including the address of your Exchange Client Access Server (CAS), and determine how to authenticate.



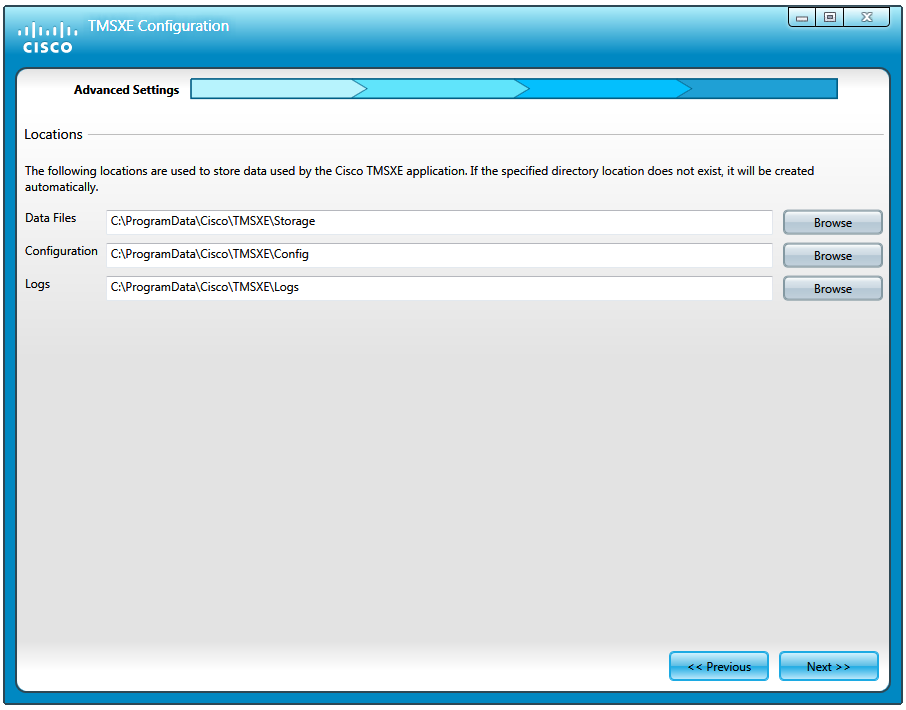
3. At the **Systems** configuration step, you will find a list of all systems in Cisco TMS that are endpoints available for integration with Cisco TMSXE. Beware that this procedure does not create any mailboxes; all room mailboxes provided must already exist in Exchange, or validation of this step will fail. (See Adding Cisco TMS managed endpoints to Exchange [p.16].)
   a. Modify the email address pattern to generate the names of your room mailboxes. Be sure to use primary SMTP addresses for the room mailboxes, as 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.

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



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. If you decline, follow the instructions in Starting the service [p.42] when you are ready to start Cisco TMSXE.

If any validation steps fail during the configuration process, see the section Errors during configuration [p.46].

Configuration 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 a secure connection with certificates is used, the FQDN must be provided. 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.14].
Password	The password for the above user.
Domain	The domain the Cisco TMS server is in.
Exchange Web Services	
Server Address	The address of the Exchange Client Access Server (CAS), must be 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.

Field	Description
Use HTTP	In communication with Exchange Web Services, encryption is used by default. This option disables secure communication with EWS.
Sender Email Address	The email address used as the **From:** address of all notifications to organizers booking through Cisco TMSXE. Leave blank to use the Cisco TMSXE service user email address. If you want organizers to receive notifications from an address they can reply to, a support email address or similar can be added here. Note that you must grant the service user *Send as* permissions for this address, see: ■ *Manage Send As Permissions for a Mailbox* (Exchange 2010 Help) ■ *How to Grant the Send As Permission for a Mailbox* (Exchange 2007 Help)
WebEx Scheduling Email	The address of the WebEx Scheduling Mailbox. For more information, see Setting up the WebEx Scheduling Mailbox [p.24].
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.14]. ■ **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. Note that once you have set up Cisco TMSXE to use this service user, you must not change service users, whether during operation, or as part of an upgrade. The link between meetings in Exchange and Cisco TMS is tied to the service user GUID.
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 Requirements for certificate authentication (optional) [p.8]. ■ **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. See Adding Cisco TMS managed endpoints to Exchange [p.16]. ■ 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.
Advanced Settings	
Data Files	Data files are stored at this location. Default: **\ProgramData\Cisco\TMSXE\Storage** on the drive where Cisco TMSXE is installed. The **ProgramData** Windows folder is hidden by default.
Configuration	The Cisco TMSXE configuration file will be stored at this location. Default: **\ProgramData\Cisco\TMSXE\Config** on the drive where Cisco TMSXE is installed. The **ProgramData** Windows folder is hidden by default.

Field	Description
Logs	Event and error logs are stored at this location. Default: **\ProgramData\Cisco\TMSXE\Logs** on the drive where Cisco TMSXE is installed. The **ProgramData** Windows folder is hidden by default.

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.

WebEx Productivity Tools with TelePresence

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

- Telepresence with WebEx 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.

Deploying WebEx Productivity Tools with TelePresence for Cisco TMSXE

This section covers how to configure Cisco TMS Booking Service to work with IIS and WebEx.

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 Cisco TMS Booking Service

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

If you did not include the Cisco TMS Booking Service during initial installation:

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 Deployment best practices [p.10].

Configuring IIS for HTTPS

Booking Service requires HTTPS to be configured for DefaultSite in IIS on the Cisco TMSXE server.

If IIS is not present on the server prior to installation of Cisco TMSXE, it will be automatically installed with Booking Service. HTTPS must then be configured after installation to allow Booking Service to operate.

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

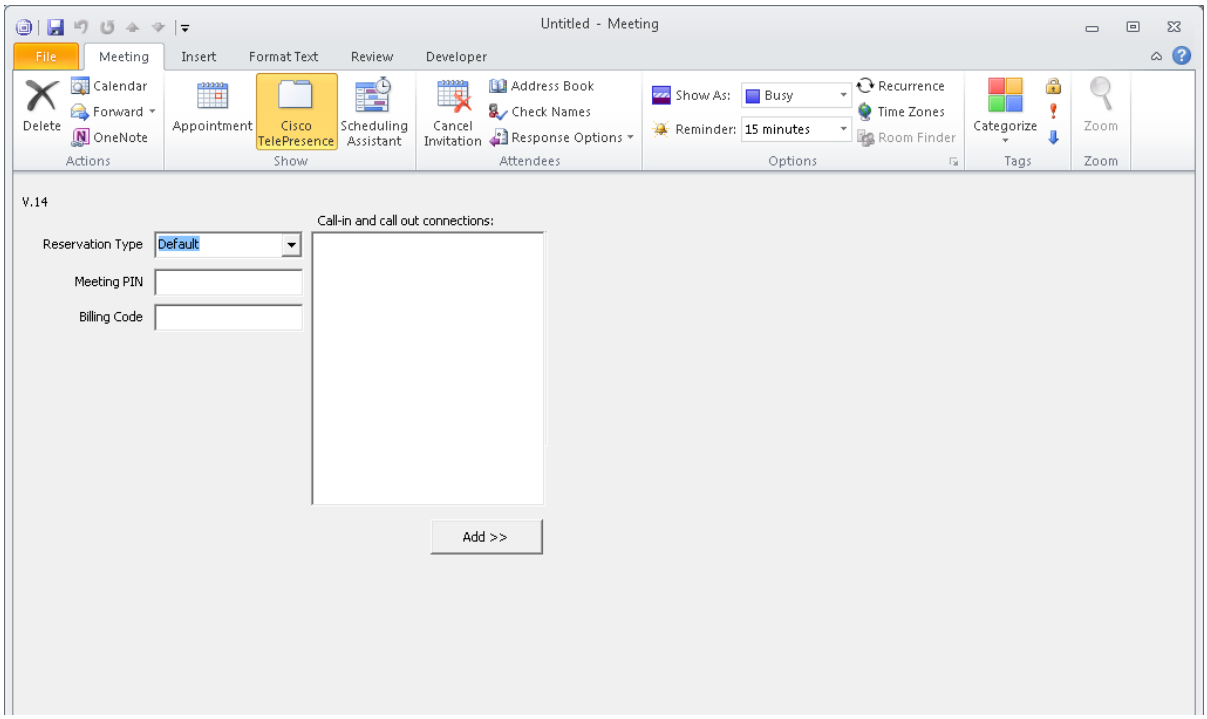
1. On your WebEx site, go to **Manage Site > Site Settings > OneTouch TelePresence Options**.
2. In the **Cisco TMSXE Host Address** field, enter the full address of the Booking Service by including the hostname of the server in the following address:
   `https://<hostname>/TMSService/Booking.svc`.
3.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

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

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 (3.1.3)*.



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.24].

Deploying the Cisco TelePresence form

If opting to use the Cisco TelePresence form, we recommend that it 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.

Form deployment requires the following three steps for a new installation:

1. Creating the Organizational Forms Library [p.39]
2. Publishing the Cisco TelePresence form [p.39]
3. Configuring clients to use the form [p.40]

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 dropped, but the form must be published locally before it can be used. Follow the instructions in Publishing the Cisco TelePresence form [p.39].

Creating the Organizational Forms Library

Exchange 2007 and 2010 environments 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 present and on how Exchange was installed.

Exchange installation differences

During the installation of the first Exchange Server 2007 as a new Organization, the setup prompted the installing administrator with "Do you have any client computers running Outlook 2003 and earlier or Entourage in your organization?".

- If the administrator answered *Yes*, a Public Folder database and Organizational Forms library was automatically created.
- If the administrator answered *No*, no Public Folders were created, and creating a Public Folder Database is most likely required to be able to publish the Cisco TelePresence form.

Also, if Exchange Server 2007 was installed alongside an existing Exchange Server 2003 environment, the Public Folder database should have been created and configured to replicate with the existing 2003 Public Folder database and Organizational Forms Library.

Setting up an Organizational Forms Library

Administrators should see Microsoft's documentation regarding Public Folders and Organization Forms Libraries in Exchange 2007.

- Microsoft TechNet article: How to Create an Organizational Forms Library in Exchange 2007
- Exchange 2010 SP1 help: Create an Organizational Forms Library

Publishing the Cisco TelePresence form

Before the form can be used, it must be published using an Outlook client. If using the Organizational Forms Library, this library must be in place before following the steps below, see Creating the Organizational Forms Library [p.39].

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 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.40].

Publishing from Outlook 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.40].

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.

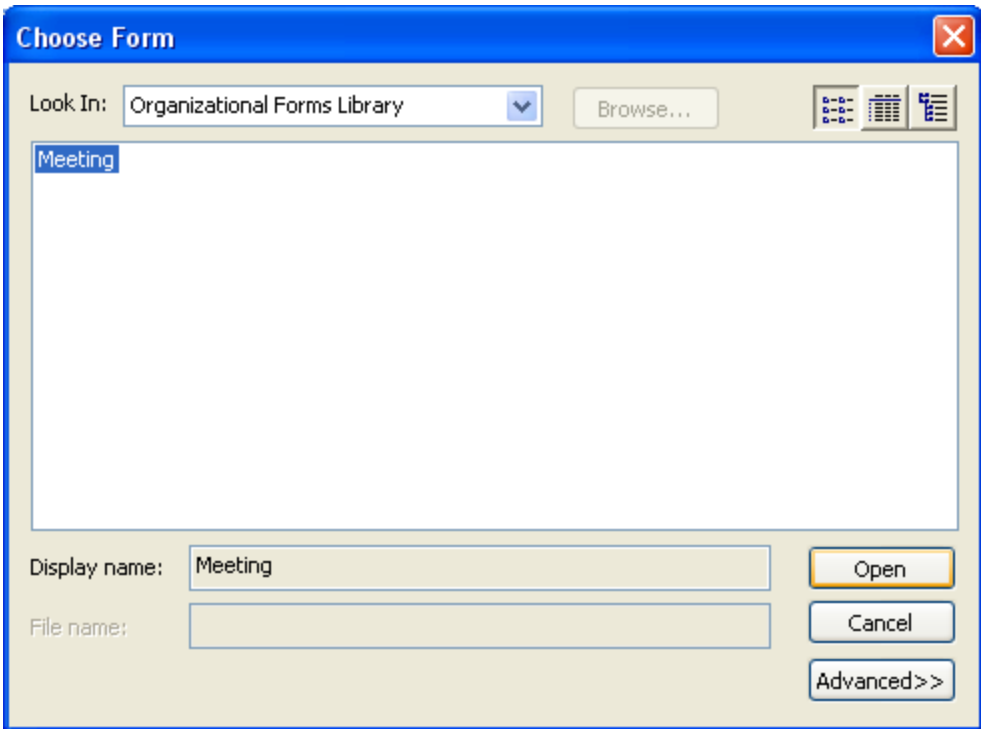
The Microsoft article *How to globally change the default forms in Outlook by using the Forms Administrator utility* describes and links to a utility for creating registry keys to change the default form.

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.

Running the Cisco TMSXE service

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

Before you make any changes to configurations, including adding or removing endpoints from Cisco TMSXE, you must stop the Cisco TMSXE service, and restart it when the configuration tool is closed.

Starting the service

After configuration, a prompt will ask whether to start the Cisco TMSXE service.

If you decline this prompt, you must start the process manually as described below. 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**.

If the service fails to start, the error will be logged. See Troubleshooting [p.45] for more information.

Stopping the service

The Cisco TMSXE service must be stopped before the configuration tool can be opened. A prompt to stop the service will be presented if you launch the configuration tool while Cisco TMSXE is running.

If you need to stop the service for other reasons:

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

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.

Moving and uninstalling Cisco TMSXE

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.

Moving the application

1. Install Cisco TMSXE on the new server. For instructions, see Performing a new installation [p.30].
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.

Uninstalling Cisco TMSXE 3.1.3

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 **Software-Cisco-TMSXE**.

Troubleshooting

This section covers troubleshooting of issues that may arise during installation and initial configuration and startup of the product. For instructions on troubleshooting the application, see *Cisco TelePresence Management Suite Extension for Microsoft Exchange Administrator Guide*.

Reading the Windows event log

1. Right-click on **Computer** in the Start menu, 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.33].

- **TMSXE-log-file.txt** logs the activities of the Cisco TMSXE Windows service
- **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.

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.

Turning on debug logging

The default log level is informational. To change the log level for debugging:

1. Open Notepad 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.

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.14].

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.7].
- 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.45].

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.47].

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 Adding Cisco TMS managed endpoints to Exchange [p.16] 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.45].)
- 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.

Appendix 1: Using 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. This mode of operation is only recommended for scenarios with very particular requirements.

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

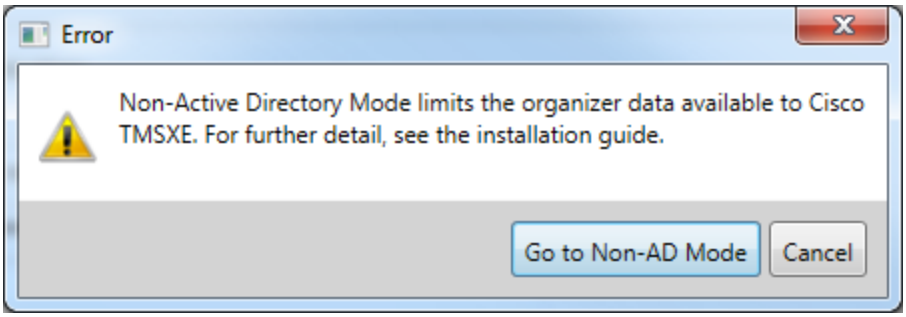
To be able to run Cisco TMSXE in Non-Active Directory mode, launch the Cisco TMSXE installer by entering the following on the command line:

```
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.

Limitations

The following restrictions apply when using Non-AD Mode:

- Only 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.

Bibliography

All documentation for the latest version of Cisco TMSXE can be found at http://www.cisco.com/en/US/products/ps11472/tsd_products_support_series_home.html.

Title	Reference	Link
Cisco TelePresence Management Suite Extension for Microsoft Exchange User Guide (3.1.3)	D14892	

Relevant Microsoft articles

Title	URL
Load Balancing Requirements of Exchange Protocols	http://technet.microsoft.com/en-us/library/ff625248.aspx
Understanding Client Throttling Policies	http://technet.microsoft.com/en-us/library/dd297964.aspx
Move Mailboxes from Exchange 2003 Servers to Exchange 2010 Servers	http://technet.microsoft.com/en-us/library/dd638187.aspx
Move Mailboxes from Exchange 2007 Servers to Exchange 2010 Servers	http://technet.microsoft.com/en-us/library/dd638192.aspx
Convert a Mailbox	http://technet.microsoft.com/en-us/library/bb201749.aspx
Manage Send As Permissions for a Mailbox (Exchange 2010 Help)	http://technet.microsoft.com/en-us/library/bb676368.aspx
How to Grant the Send As Permission for a Mailbox (Exchange 2007 Help)	http://technet.microsoft.com/en-us/library/aa998291(EXCHG.80).aspx
How to Create an Organizational Forms Library in Exchange 2007	http://technet.microsoft.com/en-us/library/cc540468(EXCHG.80).aspx
Create an Organizational Forms Library (Exchange 2010)	http://technet.microsoft.com/en-us/library/gg236889.aspx
How to globally change the default forms in Outlook by using the Forms Administrator utility	http://support.microsoft.com/kb/241235/EN-US/
December 2010 cumulative time zone update for Windows operating systems	http://support.microsoft.com/kb/2443685