Cisco TelePresence Management Suite Extension for Microsoft Exchange

Installation Guide

Version 3.0

D14890 04

September 2012

Contents

Introduction **5**

Requirements **6**

System requirements for Cisco TMSXE 6
- Hardware requirements 6
- Software requirements 6
- Virtual machines 6
- Active Directory 6

Migration requirements 6
Cisco TMS requirements 7
- Enabling option keys 7
- Per system licensing 7

Microsoft Exchange requirements 8
Client requirements 8

Deployment best practices **9**

Security 9
Virtualization 9
Redundancy 9
Advanced settings and the Cisco form 9
Setup and teardown buffers 9
Mailbox configurations and the "Private" flag 10

Preparing for migration **11**

Schedule migration off-hours 11
Supported migration scenarios 11
Upgrading Cisco TMS 11
Exporting settings from Cisco TMSXE 2.3.x or 2.2 11
Uninstalling Cisco TMSXE 2.3.x or 2.2 12
Disabling Exchange Integration Service Account setting 12
Disabling Outlook Direct Booking on resource mailboxes 12
Moving mailboxes 13
Converting Exchange 2003 mailboxes 13

Preparing for a clean installation **14**

Upgrading Cisco TMS 14
Creating a Cisco TMSXE service user in AD 14
Creating a Cisco TMS user for Cisco TMSXE 14
- Setting up minimal required permissions 14

Specifying default conference settings 15
- Per-conference settings 15

Adding Cisco TMS managed endpoints to Exchange 15
- Repurposing existing mailboxes 16

Configuring the room mailboxes **17**

Configuring Exchange 2007 mailboxes 17
- Using Exchange Management Console 17
- Using Exchange Management Shell 17

Configuring Exchange 2010 mailboxes 18
- Using Exchange Management Console 18

Using the Exchange Management Shell ... 18
Applying the Cisco TMSXE Throttling Policy for Exchange 2010 SP1 ... 20
Throttling Policy Parameter Definitions and Values ... 20
Restoring the Microsoft Throttling Policy ... 22
Setting up secure communication ... 23
Certificate requirements ... 23
Untrusted certificates ... 23
Migrating from Cisco TMSXE 2.3.x or 2.2 ... 24
Consistency check and data scrubbing during migration ... 24
Corrupted data removed ... 24
Inconsistent data temporarily deleted ... 24
Booking re-generation ... 24
Installing with migrated settings ... 24
Configuring and migrating ... 25
Restarting an interrupted migration process ... 28
Using the migration log ... 28
Verifying booking data tagged as permanently deleted ... 29
Following up on temporary deletions ... 29
Performing a clean installation ... 30
Configuring Cisco TMSXE ... 30
Configuration reference ... 33
Upgrading version 3.0 to 3.0.1 ... 35
Deploying the Cisco form ... 36
Creating the Organizational Forms Library ... 37
Exchange installation differences ... 37
Setting up an Organizational Forms Library ... 37
Publishing the Cisco form ... 37
Acquiring the form ... 37
Publishing from Outlook 2007 ... 37
Publishing from Outlook 2010 ... 38
Configuring clients to use the form ... 38
Manually configuring clients to use the form ... 39
Running the Cisco TMSXE service ... 40
Starting the Cisco TMSXE service ... 40
Stopping the Cisco TMSXE service ... 40
Troubleshooting the installation ... 41
Reading the Windows event log ... 41
The Cisco TMSXE log ... 41
Turning on debug logging ... 41
Errors during configuration ... 42
Untrusted certificates ... 42
The remote name could not be resolved ... 42
The Cisco TMS user account does not belong to a group that has "Book on behalf of" permissions ... 42
Mailbox database is temporarily unavailable ... 42
The Client Access Server version does not match 42

A timezone with the specified ID could not be found 43
Unbookable or unlicensed systems 43
The Cisco TMSXE service does not start 43
No bookings are accepted or declined 44
Exchange 2010 issues with Cisco form 44
Bookings not replicating 45
Uninstalling the software **46**
Removing Cisco TMSXE from the server 46
Bibliography **47**
Relevant Microsoft articles 47

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 migrating settings and data from older 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 (3.0)*.

Requirements

This section details requirements for setting up a Cisco TMSXE 3.0 deployment.

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

Active Directory system requirements correspond to AD requirements for Exchange.

DNS

The Cisco TMSXE server must be configured to use a DNS server with service records for the Active Directory domain of the Exchange server.

Migration requirements

Cisco TMSXE 3.0 supports migration from the following previous versions of Cisco TMSXE:

- 2.3.1
- 2.3
- 2.2

Cisco TMS requirements

Version	13.1.2 or later
Network	HTTPS (recommended) or HTTP connectivity is required from the Cisco TMSXE server to Cisco TMS.
Licensing	Either: ■ One Cisco TelePresence Management Suite Extension for Microsoft Exchange option key per 25 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 system to be integrated with Exchange must already have been added to, and licensed for use with, Cisco TMS.

Once the Exchange Integration Option has been activated in Cisco TMS, the **Allow Remote Bookings** setting determines whether each system is using a license.

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 manually 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** set to *Yes* or *No*.
5. If you want to modify the setting, click **Edit Settings**.
6. Use the checkbox to toggle the setting.
7. Click **Save**.

Note: The **Allow Remote Bookings** setting is only visible if one or more Microsoft Exchange option keys have been activated in Cisco TMS. If an Application Integration Package option is also activated, the setting will be void and therefore hidden.

Microsoft Exchange requirements

Requirement	Description
Microsoft Exchange	Supported versions: ■ Microsoft Exchange 2010 Service Pack 1 ■ Microsoft Exchange 2010 Service Pack 2 ■ Microsoft Exchange 2007 Service Pack 3
Microsoft Server	Supported versions: ■ Microsoft Server 2008 R2 ■ Microsoft Server 2008
Exchange Web Services (EWS)	Must be enabled on the Exchange server.
Throttling policies	For Microsoft Exchange 2010 SP1, special throttling policies must be applied. See Applying the Cisco TMSXE Throttling Policy for Exchange 2010 SP1 [p.20]

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 form, which can only be used with a local Outlook client.

Before installing Cisco TMSXE 3.0, 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.

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.

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.23].

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 *Cisco TelePresence Management Suite Redundancy Deployment Guide*.

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

Advanced settings and the Cisco form

Deployment and use of the Cisco form, which contains advanced conference settings, is optional. Note that editing this form is not supported.

If deploying the Cisco form, we recommend that users be provided with a link to *Cisco TelePresence Management Suite Extension for Microsoft Exchange User Guide (3.0)* for a simple overview of how the advanced settings work.

Setup and teardown buffers

As setup and teardown buffers are currently not supported by the Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA), we strongly advise configuring Cisco TMS not to use setup and teardown buffers for new conference bookings.

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 includes settings such as:

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

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.

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.

Preparing for migration

Because Cisco TMSXE 3.0 must be installed on a separate server from Microsoft Exchange, no upgrade path exists for previous versions of Cisco TMSXE that had to reside on the Exchange server.

To keep existing settings and conference data from a previous deployment, migration is necessary:

- Migration prevents the administrator from having to re-configure Cisco TMSXE and re-add all endpoints.
- Migration of conference data scrubs the data to identify any discrepancies in existing bookings and avoid duplicate bookings in the upgraded deployment.

This section describes the required steps you must follow before installing with settings and data migration.

Schedule migration off-hours

We recommend that migration be performed outside of peak office hours in your organization if possible.

If organizers delete bookings using Outlook during backend migration, this deletion cannot be detected by Cisco TMSXE, and the deleted bookings will be automatically regenerated with no warning when Cisco TMSXE starts up.

Supported migration scenarios

Three different scenarios for migrating data from Cisco TMSXE 2.3.1, 2.3, or 2.2 to Cisco TMSXE 3.0 are supported:

- Both deployments are with Exchange 2007
- Original deployment uses Exchange 2007, new deployment uses Exchange 2010
- Original deployment uses Exchange 2003, new deployment uses Exchange 2010

Note that this guide does not detail Exchange migration or how to move mailboxes, only requirements and procedures specific to installing Cisco TMSXE with settings and data migration.

Upgrading Cisco TMS

When preparing to install Cisco TMSXE, start by installing/upgrading to the latest version of Cisco TMS (13.1.2 or later is required).

Back up the database and follow the installation instructions in *Cisco TelePresence Management Suite Installation and Getting Started Guide* for the appropriate version of Cisco TMS.

Exporting settings from Cisco TMSXE 2.3.x or 2.2

To export your existing Cisco TMSXE configuration:

1. Choose the correct export application for your Exchange server from the Cisco TMSXE deliverable archive. Two versions are available:
   - **ExportSettingsApp32bit.exe** for exporting from Exchange 2003.
   - **ExportSettingsApp64bit.exe** for exporting from Exchange 2007.

2. Place the application on a network location accessible to both the original Exchange server and the new Cisco TMSXE server.
3. On the original Exchange server, run the application by double-clicking it, or start it from the command line.

All settings and endpoint data except passwords will be exported to **exported_cisco_tmsxe_settings.txt**, which will be placed in the same folder as the application.

Uninstalling Cisco TMSXE 2.3.x or 2.2

To uninstall the product, either:

- Select **Uninstall** from the product's **Start** menu group on the Exchange Server.
- Use **Add/Remove programs** from the server's Control Panel.

The program will leave its log folder, registry keys, and associated accounts in place to accommodate future installations or upgrades.

For data migration to work, booking watermarks must be intact. Therefore, do *not* delete the program files folder. The default location for this folder is C:\Program Files\Cisco\Conferencing eXtensions for Microsoft Exchange, or, if upgraded from a version older than 2.3, C:\Program Files\TANDBERG\.

Disabling Exchange Integration Service Account setting

This setting was used by previous versions of Cisco TMSXE, but is no longer in use. In Cisco TMS:

1. Go to **Administrative Tools > User Administration > Users**.
2. Search or browse to locate the service user for Cisco TMSXE.
3. Hover the list entry and click the dropdown arrow to display the menu.
4. Select **Edit**.
5. Change the setting **Exchange Integration Service Account** to *No*.
6. Save the change.

Disabling Outlook Direct Booking on resource mailboxes

Due to changes in the architecture and technologies of both Cisco TMSXE and Exchange, the direct booking model used with previous versions of Cisco TMSXE on Exchange 2003 and some deployments of Exchange 2007 is no longer available.

Outlook Direct Booking is incompatible with the automatic accept feature for room mailboxes in Exchange 2010 and will create conflicts if not disabled prior to migration.

Before moving the mailboxes to Exchange 2010, do the following:

1. Log into Outlook as the resource mailbox to be converted.
2. Go to **Tools > Options... > Calendar Options... > Resource Scheduling...**
3. Uncheck *Automatically accept meeting requests and process cancellations*.

Repeat the above steps for each mailbox before proceeding to Moving mailboxes [p.13].

Moving mailboxes

If migrating to Exchange 2010, make sure the service user mailbox and all room mailboxes have been moved to the new server before installing Cisco TMSXE.

For instructions, see the Exchange Server SP1 help:

- Move Mailboxes from Exchange 2003 Servers to Exchange 2010 Servers
- Move Mailboxes from Exchange 2007 Servers to Exchange 2010 Servers

If migrating from an Exchange 2007 deployment, you can now proceed to Applying the Cisco TMSXE Throttling Policy for Exchange 2010 SP1 [p.20].

If migrating from Exchange 2003, the mailboxes need further preparation. Proceed to Converting Exchange 2003 mailboxes [p.13].

Converting Exchange 2003 mailboxes

Room mailboxes transferred from Exchange 2003 must also be converted to room resource mailbox format before they can be used by Cisco TMSXE.

For instructions, see the Microsoft article Convert a Mailbox.

When all mailboxes are converted, proceed to Configuring the room mailboxes [p.17].

Preparing for a clean installation

Perform a clean installation of 3.0 only in these situations:

- You do not have an existing deployment of Cisco TMSXE 2.2, 2.3, or 2.3.1.
- You want to set up a test environment/deployment to see how Cisco TMSXE works.

We strongly recommend that administrators with existing deployments use the option to migrate their settings and data.

Should you prefer to perform a clean installation even though a previous deployment exists, all Cisco TMSXE 2.x software components and data *must* be removed from the server prior to installing Cisco TMSXE 3.0, and room mailboxes must either be deleted or emptied of all contents.

Upgrading Cisco TMS

When preparing to install Cisco TMSXE, start by installing/upgrading to the latest version of Cisco TMS (13.1.2 or later is required).

Back up the database and follow the installation instructions in *Cisco TelePresence Management Suite Installation and Getting Started Guide* for the appropriate version of Cisco TMS.

Creating a Cisco TMSXE service user in AD

In Exchange Management Console, create a new user mailbox for Cisco TMSXE with the username and password of your choice.

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:
   - Make the service user a site administrator with universal access.
   - Add the account to a group with a smaller subset of permissions, see Setting up minimal required permissions [p.14] below.
5. Hover over the user in the list, click the drop-down arrow and select **Edit**.
6. Verify that the setting **Exchange Integration Service Account** is set to *No*.
7. Click **Save**.

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 work, 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:

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 the Cisco 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 form.
4. Click **Save** to apply the changes.

Per-conference settings

If using the custom Cisco 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 form [p.36]. For more detail on how the form works for users, see *Cisco TelePresence Management Suite Extension for Microsoft Exchange User Guide (3.0)*.

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.17].

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.

Repurposed mailboxes must also be configured following the instructions in Configuring the room mailboxes [p.17].

Configuring the room mailboxes

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

Note that these steps are only required if you are either:

- Performing a clean installation.
- Migrating from an Exchange 2003 deployment.
- Adding one or more new systems to your deployment.

If migrating from an existing Exchange 2007 deployment with no new systems, these mailbox configurations are already in place.

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.

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.

Using Exchange Management Shell

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

1. **`Add-MailboxPermission [mailbox] -User "[service user]" -AccessRights FullAccess`**. This does the same as the above EMC procedure; grants full access to the Cisco TMSXE service user mailbox.
2. **`Set-MailboxCalendarSettings -id [mailbox] -AutomateProcessing AutoAccept`**. This sets the mailbox to automatically process invitations.
3. **`Set-MailboxCalendarSettings -id [mailbox] -RemovePrivateProperty $True`**. This setting removes the "Private" flags for all meetings accepted by the mailbox. The setting does not need to be enabled, but must be identical for all mailboxes added to Cisco TMSXE. Also note that the "Private" flag is not supported by Cisco TMS. For further information, see Deployment best practices [p.9].
4. **`Set-MailboxCalendarSettings [mailbox] -DeleteSubject:$false`**. This turns off the option to delete meeting subjects. If it is a requirement for some room mailboxes that this option be enabled, it must the set to *true* for all mailboxes. Differing settings between mailboxes can cause mismatches between Cisco TMS and Exchange.

5. **`Set-MailboxCalendarSettings -id [mailbox] -AddOrganizerToSubject $False`**. This 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.
6. **`Get-MailboxCalendarSettings -id [mailbox]|fl`**. This outputs all mailbox calendar settings so you can verify that the above settings are now active.

Repeat the above procedures for each endpoint.

When done configuring all mailboxes, proceed to Setting up secure communication [p.23].

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.

Using Exchange Management Console

Granting full access to the service user:

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**.
6. Right-click on the room mailbox again and select **Properties**.
7. In the **Resource General** tab, enable the resource booking attendant to automate room responses to meeting invitations.
8. Go to the **Resource Information** tab and ensure that the following settings are identical for all of your room mailboxes integrated with Cisco TMSXE:
   - **Delete the subject**
   - **Add the organizer's name to the subject**
   - **Remove the private flag on an accepted meeting**

Repeat the above procedure for each mailbox.

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

Using the Exchange Management Shell

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::

1. **`Add-MailboxPermission -identity [mailbox] -User [service user] -AccessRights FullAccess`**. This grants the service user full access to the room mailbox.

2. **`Get-MailboxPermission -identity [mailbox]`**. View the above setting to verify that the change is active.
3. **`Set-CalendarProcessing -identity [mailbox] -AutomateProcessing AutoAccept`**. This sets the mailbox to automatically process invitations.
4. **`Set-CalendarProcessing -identity [mailbox] -RemovePrivateProperty $true`**. 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.9].
5. **`Set-CalendarProcessing -identity [mailbox] -DeleteSubject $false`**. This turns off the option to delete meeting subjects. If it is a requirement for some room mailboxes that this option be enabled, it must the set to *true* for all mailboxes. Differing settings between mailboxes can cause mismatches between Cisco TMS and Exchange.
6. **`Set-CalendarProcessing -identity [mailbox] -AddOrganizerToSubject $false`**. This sets the mailbox to never add the organizer to the subject of a booking. Optionally, this may be set to *true* for all mailboxes.
7. **`Get-CalendarProcessing -identity [mailbox] | fl`**. This outputs all mailbox calendar processing settings so you can verify that the above settings are now active.

When all Exchange 2010 room mailboxes are configured, proceed to Applying the Cisco TMSXE Throttling Policy for Exchange 2010 SP1 [p.20].

Applying the Cisco TMSXE Throttling Policy for Exchange 2010 SP1

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.22].

Throttling Policy Parameter Definitions and Values

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

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

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

Migrating from Cisco TMSXE 2.3.x or 2.2

This section describes the data scrubbing process that happens during migration, and the steps that must be performed to install with settings and data migration.

Consistency check and data scrubbing during migration

When the configuration tool has validated all imported systems and mailboxes, booking data migration starts.

In order to make existing conference data compatible with Cisco TMSXE 3.0, the configuration tool first puts the data that is being migrated through a series of validity and consistency checks.

Subsequent to this consistency check, data scrubbing is performed:

- Bookings that are consistent across both Cisco TMS and Exchange are kept on both servers.
- Bookings with corrupted data are permanently deleted as described below.
- Bookings with inconsistent data are temporarily deleted as described below.

All operations during migration are logged. See Using the migration log [p.28] for detail.

Corrupted data removed

- Bookings that were originally created in Cisco TMS, but now only exist in Exchange, are assumed to be corrupted as a result of previous synchronization failure. The tool will therefore automatically remove all such bookings. These deletions are permanent.
- Exchange bookings with corrupted/unreadable properties are permanently deleted.

Inconsistent data temporarily deleted

If inconsistencies are found between instances of the same booking in Cisco TMS and Exchange, the booking will be kept in the system where it originated, and temporarily deleted from the other system.

Booking re-generation

The next migration step starts Cisco TMSXE 3.0 in migration mode and attempts to re-generate these bookings in the system where they are missing. This process ensures consistency and avoids duplication.

Installing with migrated settings

This section describes the required steps to install Cisco TMSXE 3.0 if you have an existing deployment of a previous version of Cisco TMSXE for Exchange 2003 or 2007.

Before you start, make sure all requirements are met, and that you have followed all the required steps in Preparing for migration [p.11].

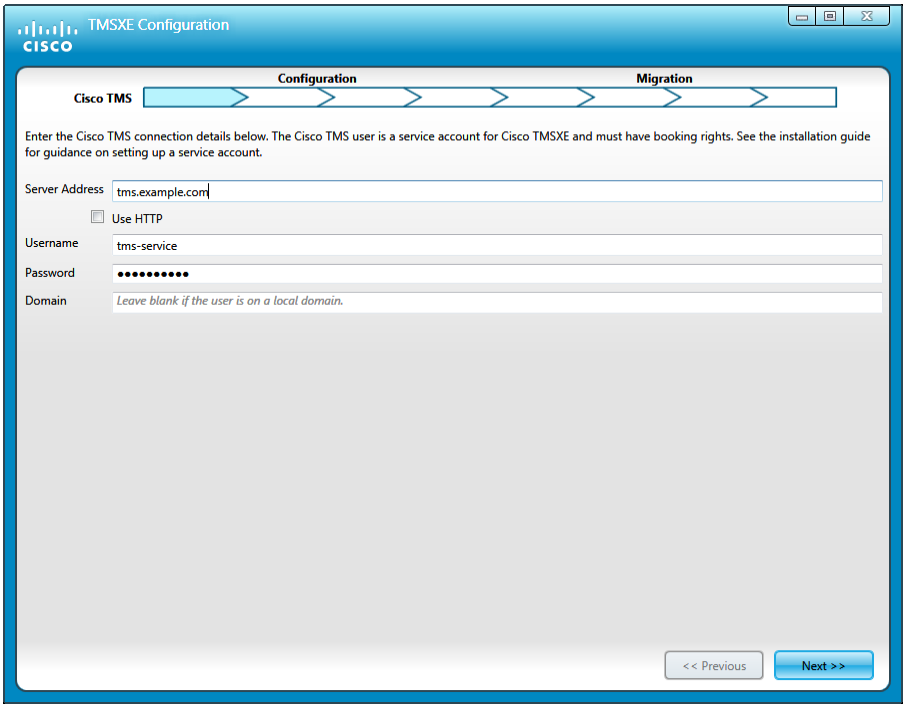
1. Check Windows Update and install any critical updates to the .NET framework on the server where Cisco TMSXE will be installed. Make sure the .NET version is 4.0 or later. Reboot the server after installing if prompted.
2. Place the installation files on the server.

3. Run the Cisco TMSXE installer and accept the End-User License Agreement (EULA) to commence the installation process.
4. Select the "Migrate" installation mode. Browse to locate the exported settings file, click **Next** and wait for the settings file to be read.
5. Follow all instructions provided by the installer.
6. Click **Finish** when the installer is done to close the installer window and launch the Cisco TMSXE configuration tool.

Configuring and migrating

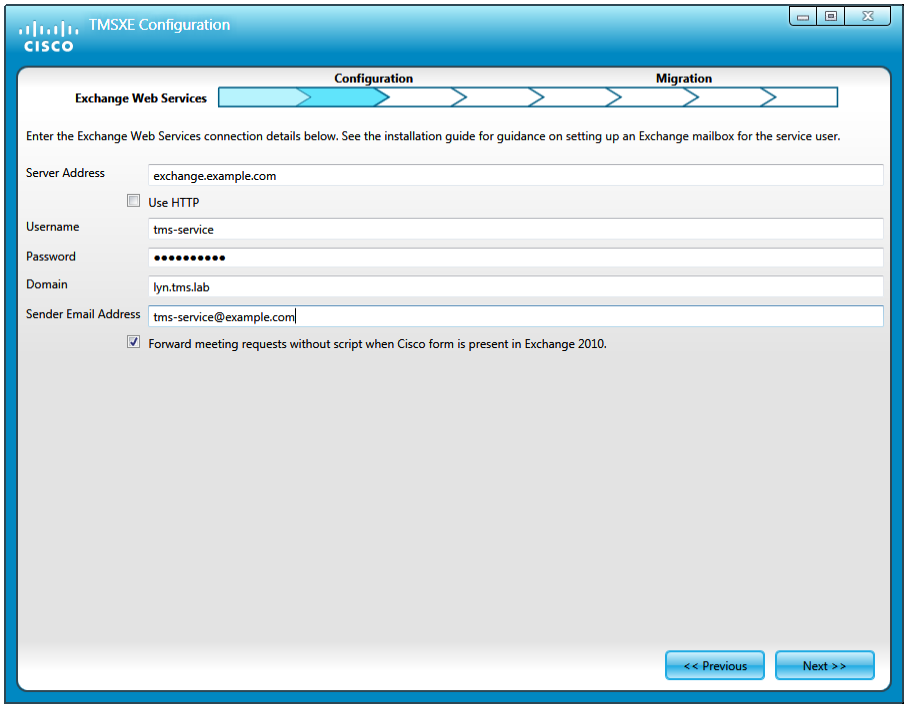
Most fields in the configuration tool are required. Clicking **Next** validates the settings provided for each step of the initial configuration. If one or more settings cannot be validated, you will be returned to the previous step to allow for corrections.

1. Configure your **Cisco TMS** connection details by verifying that all imported settings are correct, and providing the password.

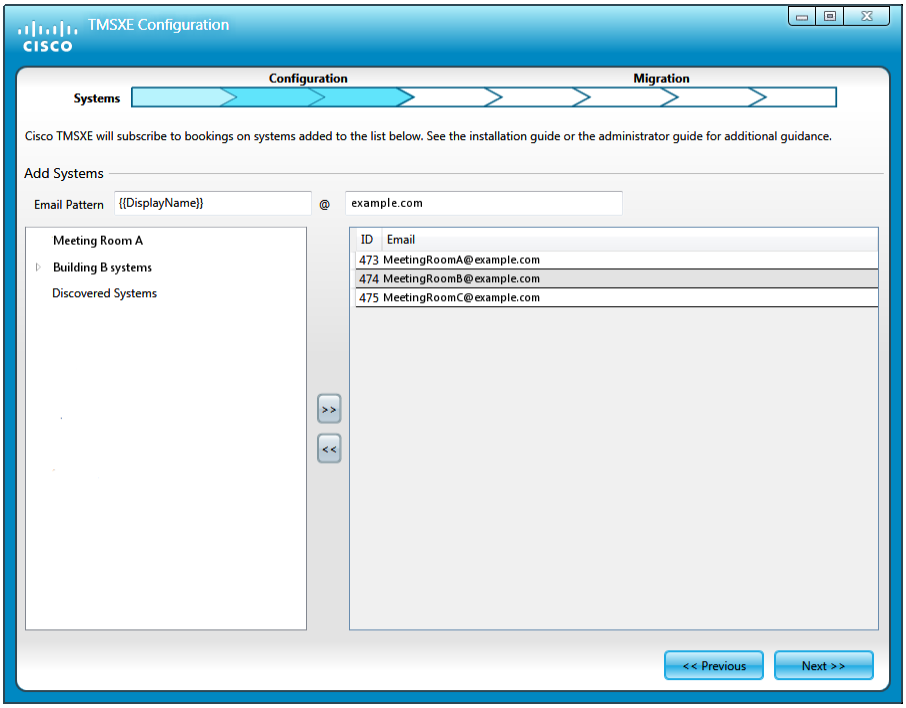


2. For **Exchange Web Services**:
   - Verify that all imported settings are correct, and provide the password.
   - Update the Exchange server address to that of your current Exchange Client Access Server (CAS).
   - If you are using the Cisco form in Exchange 2010, enable *Forward meeting requests without script when Cisco form is present in Exchange 2010*. See Exchange 2010 issues with Cisco form [p.44] for

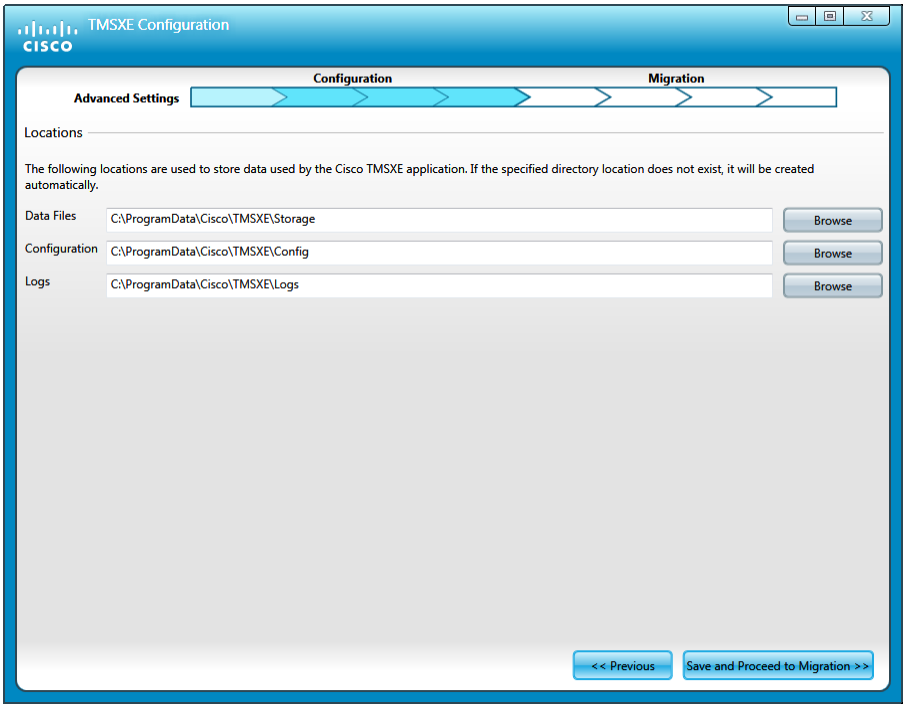
further information.



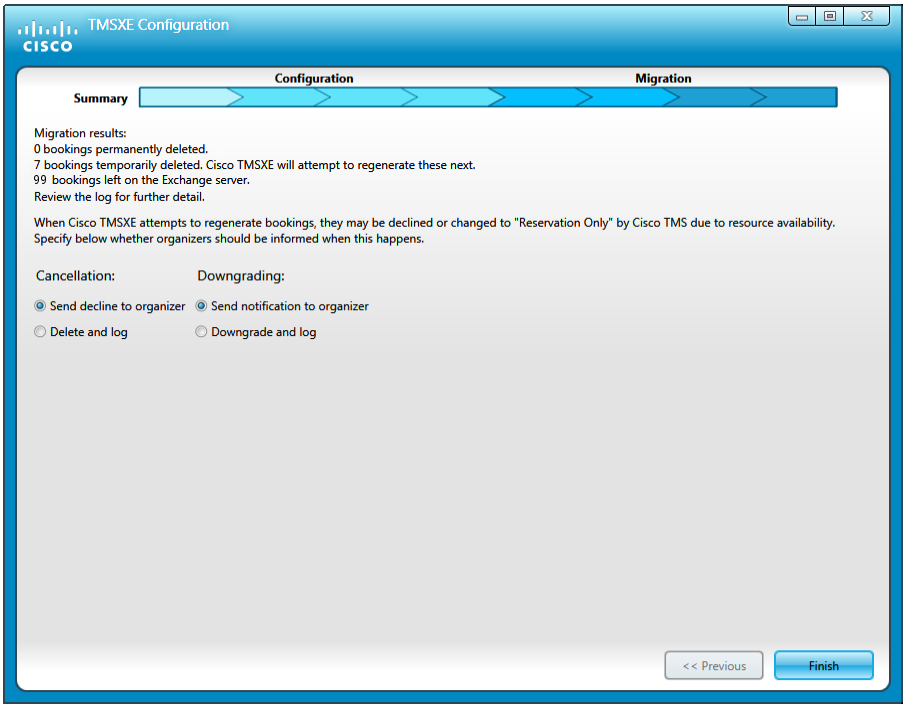
3. At the **Systems** configuration step, check that the list of TMS system IDs and corresponding mailboxes is populated in the right-hand pane, and click **Next** for validation of systems and mailboxes. Note that this may take a while if you have a large number of systems; for 250 endpoints, the process 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. Click **Save and Proceed to Migration**.



5. The tool checks Cisco TMS and Exchange for consistency in existing bookings. For more detail, see Consistency check and data scrubbing during migration [p.24]. The results of this consistency check are listed in the next migration step, and you are given two choices:
   - Continue migration. The configuration tool will delete the tagged bookings. All operations are logged, and the results are displayed in the next step.
   - Cancel the migration. You must then review the log and manually delete/re-schedule bookings as desired, then restart the configuration and migration process. For more information on this option, see Using the migration log [p.28].
6. Specify whether organizers should be notified if re-generation or routing of a temporarily deleted booking is unsuccessful. If routing is unsuccessful, the booking will be "downgraded" to a *Reservation Only* meeting where only the endpoints and rooms are reserved.



7. When you have completed the migration process, 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 Cisco TMSXE service [p.40] when you are ready to start Cisco TMSXE.

If any validation steps fail during the configuration process, see the section Errors during configuration [p.42].

Restarting an interrupted migration process

If you cancel the process prior to or during migration, perform these steps to resume:

1. Open a command prompt.
2. Run the configuration tool using the switch **`-migratewizard`**.
3. When the configuration tool starts up, go back to the Installing with migrated settings [p.24] procedure and step through the configuration phase to resume migration.

Using the migration log

The migration process writes to the standard Cisco TMSXE log and is available in the log folder, by default **\ProgramData\Cisco\TMSXE\Logs** on the drive where Cisco TMSXE was installed. The **ProgramData** Windows folder is hidden by default.

To find the relevant section of the log, look for:

```
INFO MigrationProcess - Started migration data scrub
```

The section ends with:

```
INFO MigrationProcess - Completed migration data scrub
```

All future conference bookings found during migration are tagged in the log as either:

- `is marked for deletion on the [Exchange or Cisco TMS server], will be lost`
- `is marked for deletion on the [Exchange or Cisco TMS server], will be regenerated by Cisco TMSXE`
- `has been kept on the Exchange server`

Verifying booking data tagged as permanently deleted

If you want to manually verify that no valid data is lost when bookings are tagged as permanently deleted, use the TMSConferenceId or conference title found in the log, if available, to locate the deleted conference in Cisco TMS:

1. Go to **Bookings > List Conferences**.
2. Use the **Find** field to search for the conference ID number or conference subject, making sure that the **Start** and **End** dates span the conference dates as reported in the log, and that the **Status** field is set to *Deleted*.
3. Notify the organizer that a corrupted booking exists in their name, letting them know that they need to re-schedule the conference if the booking is still valid.

Following up on temporary deletions

The migration step subsequent to the data scrubbing attempts to recreate all temporarily deleted bookings, as well as any bookings that only exist in Exchange, in Cisco TMS.

Before this step, the administrator must determine whether or not organizers should be notified directly if any of these bookings fail, that is, if a booking cannot be re-generated in Cisco TMS, or if routing resources are not available for the meeting.

Failure to route or book a conference is logged regardless of the notification preference. Note that if routing fails, the conference is booked as *Reservation Only*, and the conference must be re-booked with a conference type that includes routing after resources have been made available.

For more information on conference types, routing failure, notifications to organizers and how to modify notification templates, see *Cisco TelePresence Management Suite Extension for Microsoft Exchange Administrator Guide*.

Performing a clean 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 requirements are met, and that you have completed all steps described in Preparing for a clean installation [p.14].

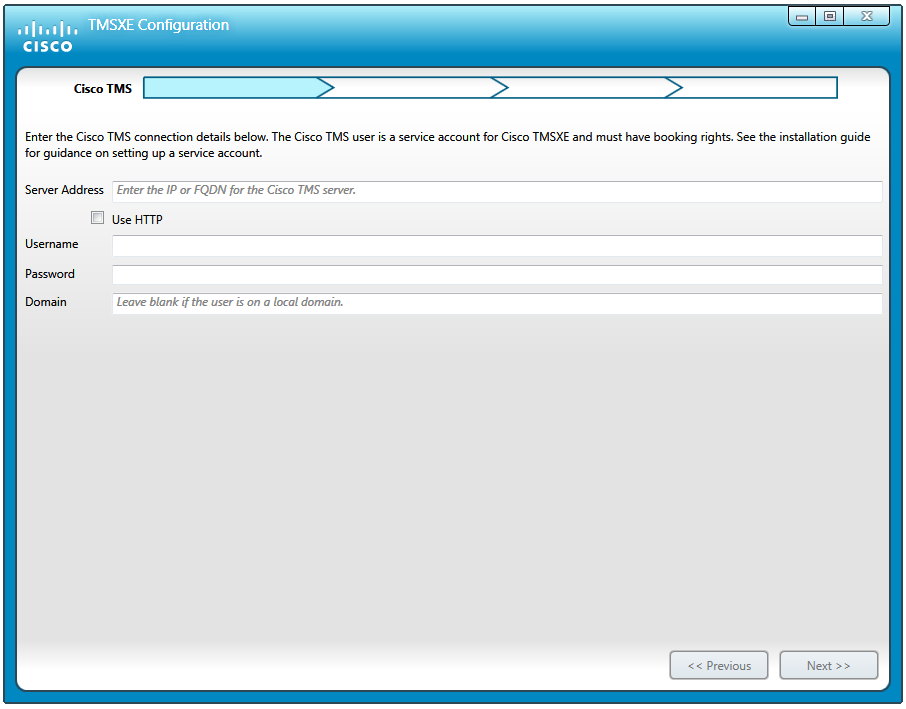
1. Check Windows Update and install any critical updates to the .NET framework on the server where Cisco TMSXE will be installed. Make sure the .NET version is 4.0 or later. Reboot the server after installing if prompted.
2. Place the installation files on the server.
3. Run the Cisco TMSXE installer and accept the End-User License Agreement (EULA) to commence the installation process.
4. Select the *Clean* installation mode.
5. Follow all instructions provided by the installer.
6. Click **Finish** when the installation is done to close the installer window and launch the Cisco TMSXE configuration tool.

Configuring Cisco TMSXE

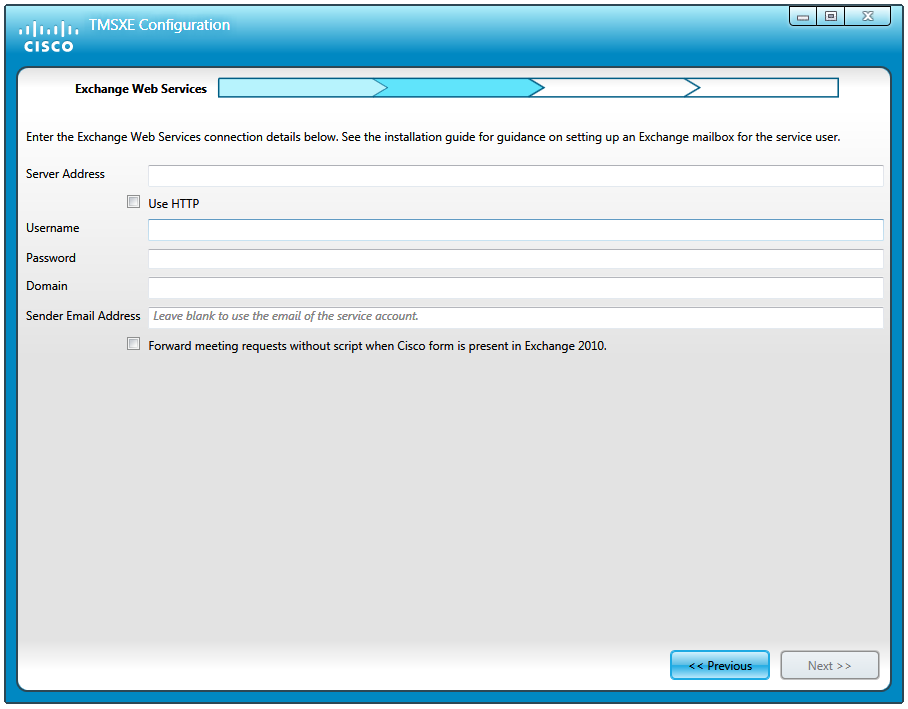
Most fields in the configuration tool are required. Clicking **Next** validates the settings provided for each step of the initial configuration. If one or more settings cannot be validated, you will be returned to the previous step to allow for corrections.

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

1. Provide your **Cisco TMS** connection details on the first step. 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).
   - If you are using the Cisco form in Exchange 2010, enable *Forward meeting requests without script when Cisco form is present in Exchange 2010*.



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

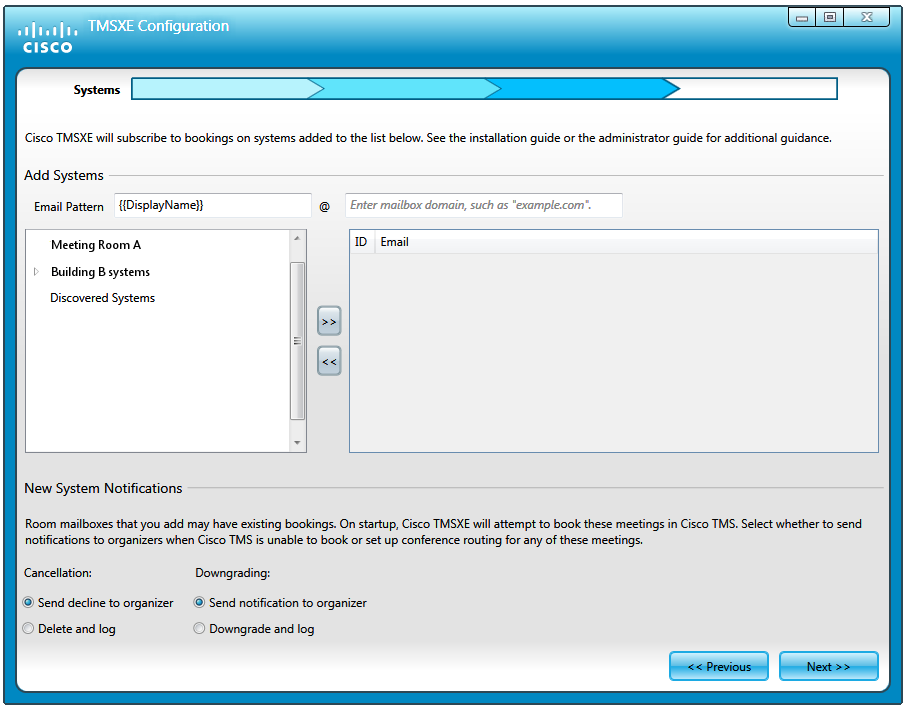
Cisco TMS managed endpoints to Exchange [p.15].)

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.

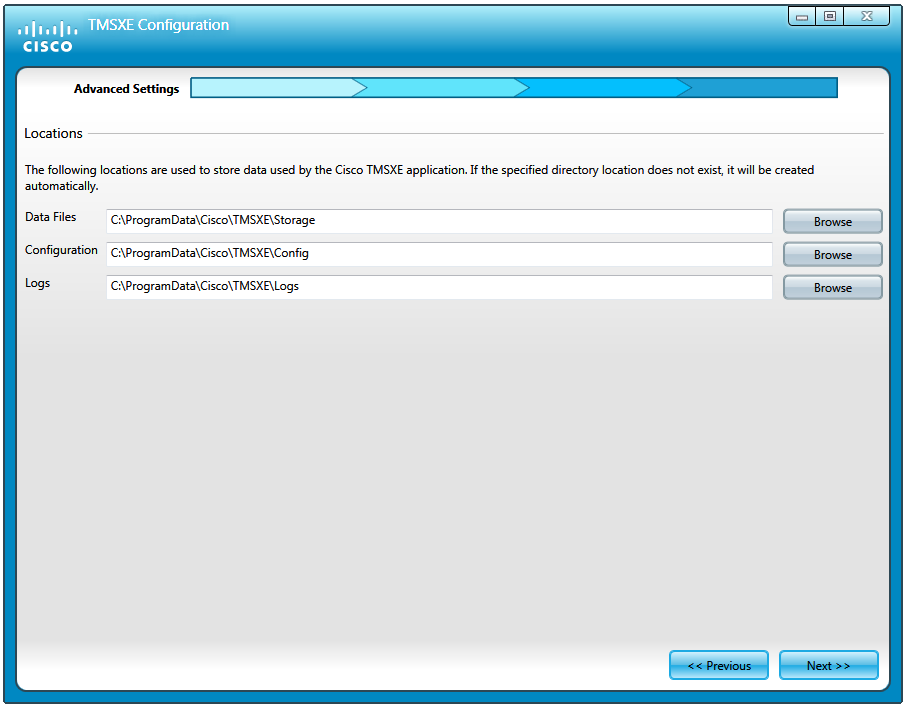
b. Select endpoints in the left-hand list and click **>>** to add them to Cisco TMSXE. Use **`Ctrl`** or **`Shift`** to select multiple endpoints.

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 Cisco TMSXE service [p.40] when you are ready to start Cisco TMSXE.

If any validation steps fail during the configuration process, see the section Errors during configuration [p.42].

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 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.
Password	The password for the above user.
Domain	The domain the Cisco TMS server is in.
Exchange Web Services	

Field	Description
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.
Use HTTP	In communication with Exchange Web Services, encryption is used by default. This option disables secure communication with EWS.
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.
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 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)
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.15]. ■ 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.
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.

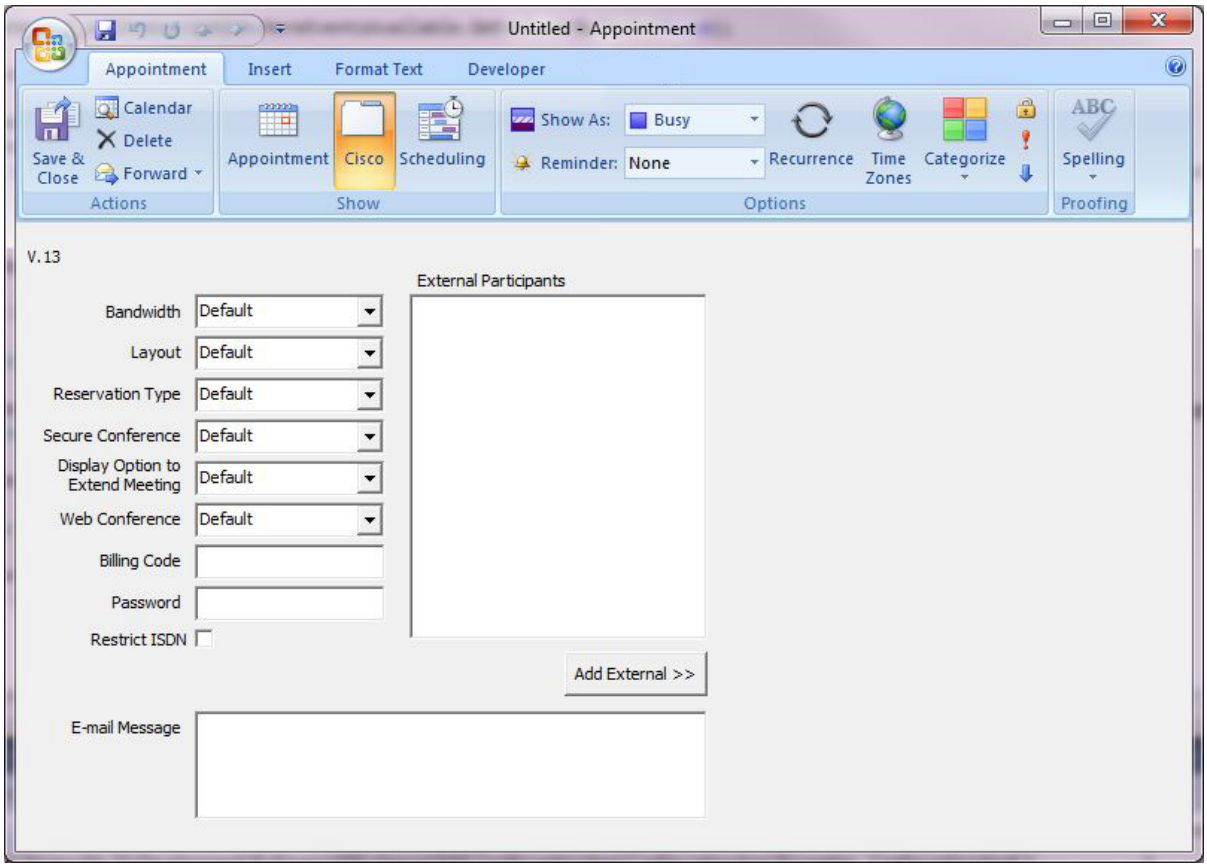
Upgrading version 3.0 to 3.0.1

To upgrade Cisco TMSXE 3.0 to version 3.0.1:

1. Unzip the deliverable archive on the Cisco TMSXE server.
2. Run the installer.
3. A prompt will notify you that a previous version is detected on the server. Click **Upgrade**. The setup wizard launches.
4. Click **Next** to start the setup.
5. Accept the terms in the license agreement and click **Next**.
6. Follow all instructions provided by the installer.
7. When the upgrade is completed, click **Finish**. The configuration tool launches.
8. Step through the configuration tool. All settings from the previous version are kept and will be re-validated as you click **Next**.
9. 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 Cisco TMSXE service [p.40] when you are ready to start Cisco TMSXE.

Deploying the Cisco form

Cisco TMSXE includes a custom form that can be used to add 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 (3.0)*.



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

If opting to use the Cisco 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.37]
2. Publishing the Cisco form [p.37]
3. Configuring clients to use the form [p.38]

Administrators that are migrating from older versions already using the Cisco 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 form [p.37].

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 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 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 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.37].

Acquiring the form

On the server where Cisco TMSXE was installed:

1. Locate the **Video Conference Form** folder created in the Cisco TMSXE installation path.
2. From this folder, copy the file **VideoConference.oft** 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.38].

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. In the menu, go to **File > Options > Customize Ribbon**.
3. Select *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.38].

Configuring clients to use the form

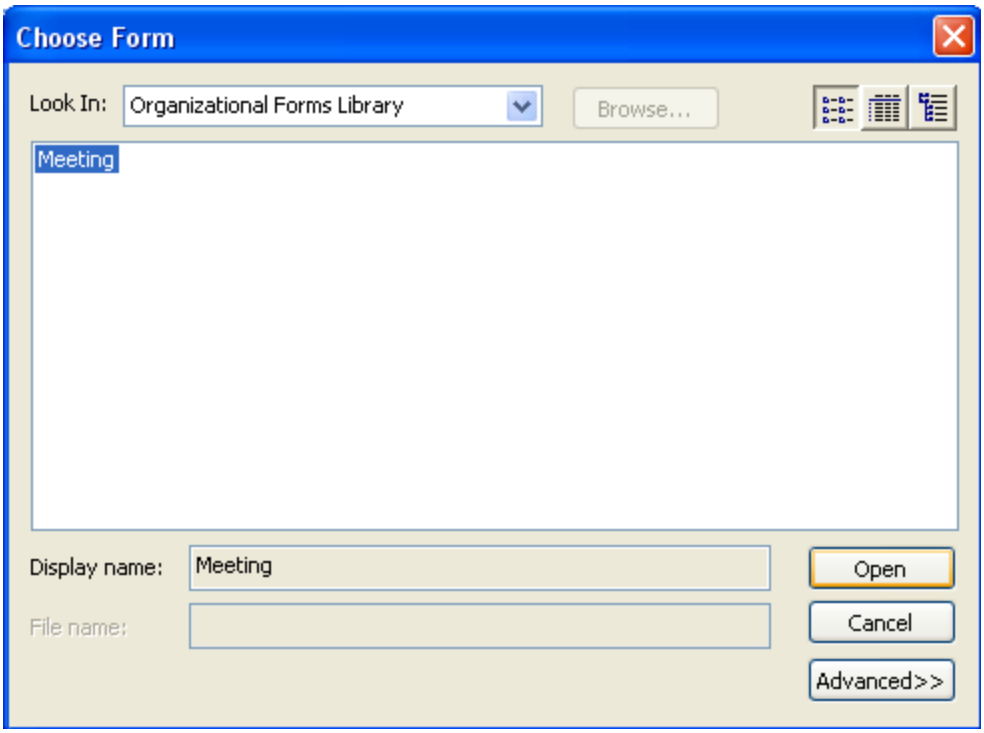
Publishing the form makes it available to users, but does not force their Outlook client to use the form. Configuring Outlook to use the form is a one-time client configuration that can be done by each user, or by making changes to the Microsoft Windows Registry. Registry changes can be done automatically 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. The **Calendar Properties** window will open with the **General** tab selected.
4. From the **When posting to this folder, use** dropdown list, select *Forms*.
5. 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*.



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

The client will now use the Cisco form for all Calendar actions and have the **Cisco** 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 the solution, you must stop the service, and restart it when the configuration tool is closed.

Starting the Cisco TMSXE 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 (including migration, if appropriate) 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 the installation [p.41] for more information.

Stopping the Cisco TMSXE service

The 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.

Troubleshooting the installation

This section covers troubleshooting of issues that may arise during installation and initial configuration and startup of the product.

Reading the Windows event log

1. Right-click on **Computer** in the Start menu, Desktop or Explorer, and select **Manage**.
2. Go to **Computer Management > System Tools > 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.

The Cisco TMSXE log

Cisco TMSXE creates a log to assist in troubleshooting.

The file is called **tmsxe-log-file.txt**, with the default location **C:\ProgramData\Cisco\TMSXE\Logs**. The location can be reconfigured using the configuration tool during or after installation, see Configuration reference [p.33].

The log file has a size limit of 5Mb. When this limit is reached:

- A new **tmsxe-log-file.txt** file 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 configuration process 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 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 performed a

migration to 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 timezone 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 timezone misconfiguration or a missing Windows update on the Exchange CAS server.

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.41].

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.
- Migration is incomplete. Launch the configuration tool from the command line using the **`-migratewizard`** switch, complete the migration process, 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.43].

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.15] for detail on setting this option for your version of Exchange.
- If you are running Exchange 2010, one or more organizers may have the Cisco form installed or present in their Outlook client. Forms using scripts are not supported by the automatic accept feature in Exchange 2010, and any booking from a client that has such a form will be left pending in the room mailbox. For resolutions to this problem, see below.

Exchange 2010 issues with Cisco form

Using the Cisco custom form requires the use of a special setting during configuration.

As the automatic accept feature in Exchange 2010 does not support the use of custom forms with scripts, all bookings from an Outlook client linked to this form will fail to be processed by the room mailbox.

Enabling the workaround

On the **Exchange Web Services** tab of the configuration tool, check *Forward meeting requests without script when Cisco form is present in Exchange 2010*.

The meeting requests will now be forwarded with the script section removed, so that the mailboxes may process them. Note that this will generate additional notifications to organizers. Setting up automatic filters for these notifications is strongly recommended.

The alternative to using this setting is removing the form from your deployment altogether.

Removing the form

Organizational Forms Library

If the form is only distributed through the Organizational Forms Library:

1. Remove the form or the folder containing the form from the Organizational Forms Library. Note that this must be done by an administrator with *Owner* permissions for the library.
2. Disable any forced registry settings specifying that this form be used.

Local form

If some users have the form locally installed, they must follow these instructions before they will be able to make any bookings in Exchange 2010:

1. Go to **Tools > Options > Other**, click **Advanced Options…**, then **Custom Forms…**, then **Manage Forms...**
2. Select and delete the **VideoConference.oft** form.
3. Click **Clear Cache**.
4. Ensure that bookings will now be created using the default form:
   a. Right-click on **Calendar** in the left-side Calendar pane.
   b. Select **Properties…**.
   c. Set **When posting to this folder, use** to *IPM.Appointment*.

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.41].)
- 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.

Uninstalling the software

1. Log on to the Cisco TMSXE server as an administrator.
2. From the Control Panel, uninstall Cisco TMSXE.

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**.

Bibliography

Title	Reference	Link
Cisco TelePresence Management Suite Extension for Microsoft Exchange User Guide (3.0)	D14892	

Relevant Microsoft articles

Title	URL
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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.