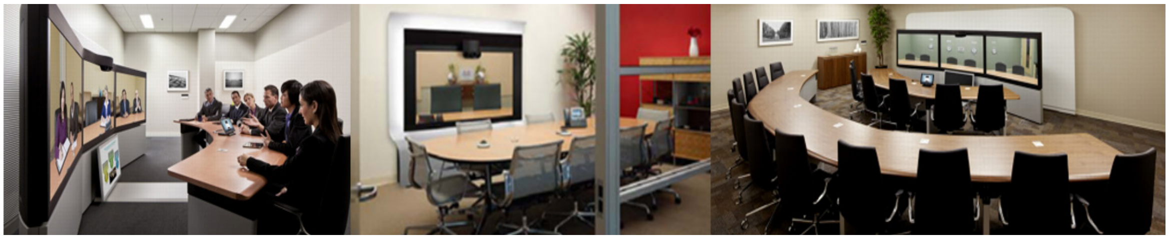


CHAPTER 6

Configuring Cisco TelePresence Management Suite

Revised: January 2014

Contents

This chapter describes how to configure Cisco TelePresence Management Suite (Cisco TMS) for Cisco WebEx Enabled TelePresence meetings. It contains the following sections:

Prerequisites

- Cisco TMS software release 14.3.1 or later is required.
- Cisco TMSXE software release 3.1 or later is required, if using Microsoft Outlook to schedule meetings.

  There are two options for scheduling using Microsoft Outlook:

  - Using the WebEx Productivity Tools Plug-In for Microsoft Outlook
  - Using WebEx Scheduling Mailbox
- Cisco TMSPE software release 1.1 or later is required, if using Smart Scheduler to schedule meetings
- The WebEx integration option key must be installed on Cisco TMS before configuring the WebEx feature.

Note Multiple WebEx sites are supported.

- MCU calls to WebEx support SIP only. The following settings must be configured for SIP:
  - In Cisco TMS: Allow Incoming and Outgoing SIP URI Dialing must be set to **Yes** in the Cisco TMS Scheduling Settings for each MCU used for Cisco WebEx Enabled TelePresence meetings.
  - For MCU and TelePresence Server, refer to the Configuring Cisco TelePresence Management Suite, page 6-1 for more information.

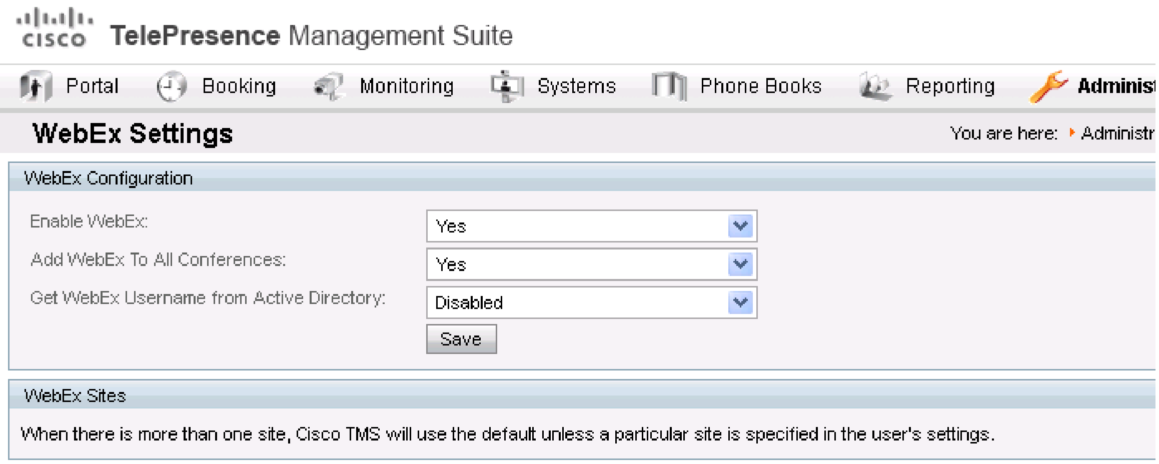
Configuring the Cisco WebEx Feature in Cisco TMS

To configure the Cisco WebEx feature in Cisco TMS, do the following:

Step 1 Go to **Administrative Tools** > **Configuration** > **WebEx Settings**.

The WebEx Settings page appears. See Figure 6-1.

Figure 6-1 Enabling WebEx in Cisco TMS



WebEx Settings

WebEx Configuration

Enable WebEx: Yes

Add WebEx To All Conferences: Yes

Get WebEx Username from Active Directory: Disabled

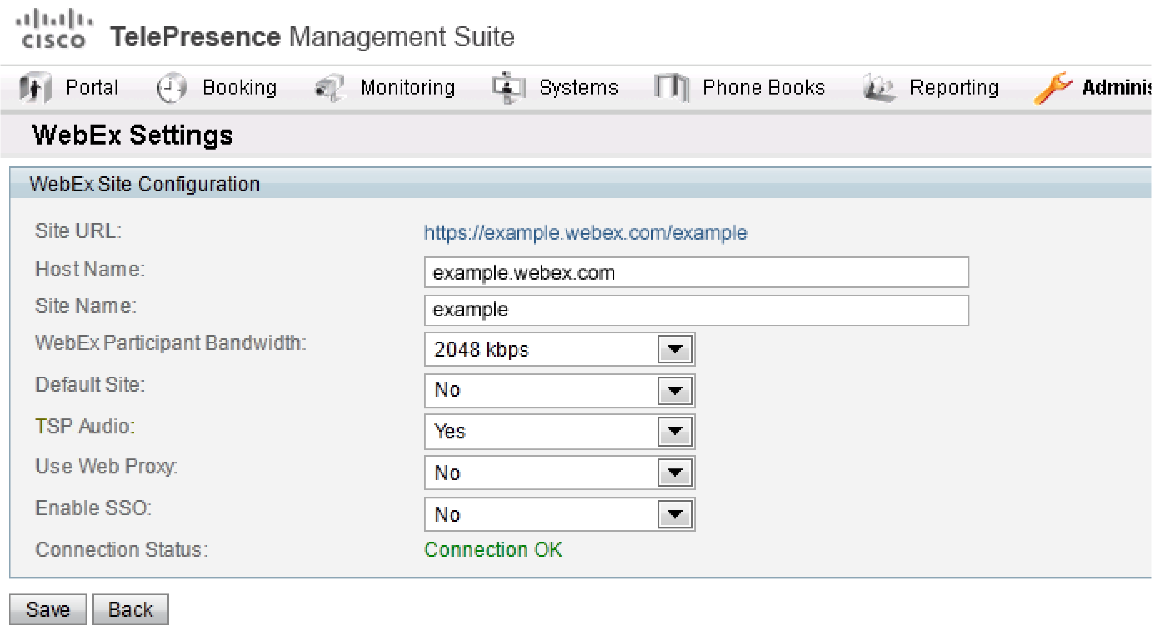
WebEx Sites

When there is more than one site, Cisco TMS will use the default unless a particular site is specified in the user's settings.

Step 2 Click **Add Site**.

The WebEx Site Configuration page appears. See Figure 6-2.

Figure 6-2 Configuring a WebEx Site



WebEx Settings

WebEx Site Configuration

Site URL:	https://example.webex.com/example
Host Name:	example.webex.com
Site Name:	example
WebEx Participant Bandwidth:	2048 kbps
Default Site:	No
TSP Audio:	Yes
Use Web Proxy:	No
Enable SSO:	No
Connection Status:	Connection OK

Step 3 In the Host Name field, enter the hostname for the WebEx site.

Step 4 In the Site Name field, create a name for the WebEx site.

Note The Site URL must follow this format: **https://[HostName]/[SiteName]**. For example: *https://example.webex.com/example*. If you wish, you can use the page number as the Site Name. The page number appears immediately after the Host Name when you navigate to your WebEx site. For example, when using a browser to navigate to your WebEx site: *https//example.webex.com*, you would see something similar to: *https://example.webex.com/mw01010*. In this example, ***mw01010*** is the page number.

Step 5 For “WebEx Participant Bandwidth”, select the maximum bandwidth per meeting to allow from MCU to WebEx.

Note Bandwidth can be limited in MCU and VCS.

Step 6 (Optional) Default Site. If one or more WebEx sites already exist, you can designate the site as the default WebEx site, by selecting **Yes**.

Note New users are automatically set to use the default site the first time they schedule a meeting with WebEx.

Step 7 Set “TSP Audio” to **Yes** if you are going to use TSP or PSTN audio.

Note If Yes is selected for TSP Audio, Cisco TMS will **only** use TSP audio. SIP audio will **not** work.

Step 8 Click **Save**.

Step 9 In the WebEx Configuration section, do the following:

a. Set “WebEx Enabled” to **Yes**.

b. Set “Add WebEx To All Conferences” to **Yes**.

Step 10 Click **Save**.

Configuring WebEx Users in Cisco TMS

To schedule meetings using Cisco TMS, users must have a username and password that the server is configured to trust.

Cisco TMS authenticates the following accounts:

- Local accounts on the Windows Server where Cisco TMS is installed
- Accounts the server trusts through domain membership and Active Directory (AD)

For each user that successfully logs into Cisco TMS, a new user profile is created based on their username and the user is prompted to enter information into their profile. Existing Windows or AD user passwords are used but they are not stored in Cisco TMS. If a user’s Windows/AD password changes, they must use that updated password when logging into Cisco TMS.

User Requirements for Scheduling WebEx-enabled Meetings

To schedule WebEx-enabled meetings using Cisco TMS, Cisco TMS users must have the following stored in their Cisco TMS user profile:

- WebEx username
- WebEx password (unless single sign on is enabled)
- The WebEx site on which they have an account.

Note This WebEx site must also be added to Cisco TMS, as described in Configuring the Cisco WebEx Feature in Cisco TMS, page 6-2.

There are three ways to enable a Cisco TMS user’s account for WebEx scheduling:

- Administrator edits the Cisco TMS user’s profile.

  For details, see Configuring a Cisco WebEx Enabled TelePresence User in Cisco TMS, page 6-6
- The Cisco TMS user edits their profile by logging in to Cisco TMS and clicking their username at the bottom left corner of the Cisco TMS Web UI.
- Administrator enables ‘Lookup User Information from Active Directory, ‘Get WebEx Username from Active Directory’ and (optionally) Single Sign On (SSO).

  The benefits of having the Active Directory lookup features enabled are that the user account information including WebEx username is automatically added to each new Cisco TMS user. WebEx password must still be added by the administrator or user, however, if Single Sign On is enabled, WebEx password is not required. With the Active Directory and Single Sign On features enabled, only the WebEx site must be selected for the user, if there are multiple WebEx sites configured on

Cisco TMS. If there is only one WebEx site, Cisco TMS will use that site. If there are multiple sites configured, Cisco TMS will automatically select the WebEx site designated as the 'Default', unless the user's Cisco TMS profile is edited to specify a different WebEx site.

For details, see Configuring Automatic User Lookup from Active Directory, page 6-5 and Configuring Single Sign On in Cisco TMS, page 6-11

Configuring Automatic User Lookup from Active Directory

If you are using Active Directory (AD), you can configure Cisco TMS to automatically populate user profile information. When you enable this feature, details about the user will automatically be imported when they first access Cisco TMS and synchronized periodically. If you use a field in Active Directory for WebEx username (e.g. the AD username or email address), you can configure Cisco TMS to import the WebEx username as well by enabling the 'Get WebEx Username from Active Directory' feature in the WebEx Settings page.

Configuring Active Directory Lookup in Cisco TMS

Active Directory Lookup imports and updates user information in Cisco TMS automatically. Optionally, Cisco TMS can also import the WebEx username.

By activating the AD lookup, WebEx and Cisco TMS automatically synchronize user information at given intervals. By doing this, each user of WebEx will only have to enter their password and not their username when booking and entering conferences.

If you do not configure AD lookup, the user will have to enter username and password for communication between Cisco TMS and WebEx.

To configure Active Directory Lookup, do the following:

Step 1 Go to **Administrative Tools** > **Configuration** > **Network Settings**.

Step 2 In the Active Directory pane, set "Lookup User Information from Active Directory" to **Yes**.

Step 3 Enter information in the remaining fields in the Active Directory pane and click **Save**.

For information about each field, refer to the Cisco TMS Help.

To configure 'Get WebEx Username from Active Directory', do the following:

Step 1 Go to **Administrative Tools** > **Configuration** > **WebEx Settings**.

Step 2 In the WebEx Configuration pane, use the "Get WebEx Username from Active Directory" menu to select the field in AD where you are storing the WebEx username.

Step 3 Click **Save**.

For more information, refer to the Cisco TMS Help.

How WebEx Bookings Work

For WebEx booking to work, the booking user must have a WebEx username and password defined as their WebEx Username and WebEx Password in their Cisco TMS profile. This ensures that the correct user “owns” the meeting in WebEx and can log in and operate the WebEx conference.

When Single Sign On (SSO) is enabled for the WebEx site, users with WebEx accounts can book WebEx-enabled meetings with Cisco TMS without requiring their WebEx password be stored in their Cisco TMS user profile. When SSO is configured and a user schedules a meeting, their WebEx username from their Cisco TMS user profile is passed to the WebEx site to complete the booking. For information about how to configure SSO, see Configuring Single Sign On in Cisco TMS, page 6-11.

The remaining fields are not mandatory, but are used for other Cisco TMS features. Later, if you are using Active Directory, you can configure Cisco TMS to populate these fields automatically for new users.

Configuring a Cisco WebEx Enabled TelePresence User in Cisco TMS

This configuration is not required if the following three conditions are true:

- ‘Lookup User Information from Active Directory’ and ‘Get WebEx Username from Active Directory’ are enabled, as described in Configuring Automatic User Lookup from Active Directory, page 6-5
- Single Sign On is enabled, as detailed in Configuring Single Sign On in Cisco TMS, page 6-11.
- The user will use the default WebEx site for scheduling WebEx meetings

To configure a Cisco WebEx Enabled TelePresence user in Cisco TMS, do the following:

Step 1 Go to **Administrative Tools** > **User Administration** > **Users**

Step 2 Click **New** to add a new user or click the name of an existing user to add WebEx scheduling capabilities to their profile and click **Edit**.

Step 3 Enter Windows/AD Username, First Name, Last Name and Email Address.

Note If an existing user or AD lookup is enabled, some fields will already contain information.

Step 4 For WebEx Username, enter the username for the user’s WebEx account.

Step 5 For WebEx Password, enter the password for the user’s WebEx account.

Step 6 For WebEx Site, select the WebEx site to which the user is registered.

Note If no WebEx site is selected, the WebEx site configured as the default will be used.

Step 7 Make any other settings in the Cisco TMS user profile and click **Save**.

Configuring Port Reservations for MCU and TelePresence Server in Cisco TMS

Cisco highly recommends configuring MCU and TelePresence Server to reserve ports for each scheduled meeting.

When enabled, the number of ports reserved for the conference is enforced. Therefore if the TelePresence portion of the meeting has 5 ports and 5 participants have joined on TelePresence, if the meeting invitation is forwarded to a 6th person, they will not be able to join the meeting on TelePresence.

If port reservations are not enabled, the meeting is booked with 5 TelePresence ports and the invite is forwarded, additional participants up to the maximum available ports at that time are able to join on TelePresence. This could cause another scheduled meeting to fail. As a result, Cisco recommend s always enabling port reservations for MCU and TelePresence Server.

Enabling Port Reservations for MCU

To enable port reservations for MCU, do the following in Cisco TMS:

Step 1 Go to **Systems** > **Navigator**.

Step 2 Select an MCU.

Step 3 Click the **Settings** tab.

Step 4 Click **Extended Settings**.

Step 5 Set “Limit Ports to Number of Scheduled Participants” to **On**.

Step 6 Click **Save**.

Step 7 Repeat steps 2 through 6 for all other MCUs.

Enabling Port Reservations for TelePresence Server

To enable port reservations for TelePresence Server, do the following in Cisco TMS:

Step 1 Go to **Systems** > **Navigator**.

Step 2 Select a TelePresence Server.

Step 3 Click the **Settings** tab.

Step 4 Click **Extended Settings**.

Step 5 Set “Limit Ports to Number of Scheduled Participants” to **On**.

Step 6 Click **Save**.

Step 7 Repeat steps 2 through 6 for all other TelePresence Servers.

Configuring Hybrid Content Mode for MCU in Cisco TMS

Configuring any MCUs that will be used for Cisco WebEx Enabled TelePresence meetings with WebEx to use the hybrid content mode is required. In hybrid mode the incoming content stream is passed through, giving the best possible quality. It is also decoded and used to create a second, lower resolution stream for anyone who cannot receive the passthrough stream. This uses up a video port but ensures that users get the advantages both of transcoding and passthrough.

To configure hybrid content mode on the MCU in Cisco TMS, do the following:

Step 1 Go to **Systems** > **Navigator**.

Step 2 Click the MCU name.

Step 3 Click the **Settings** tab and then click **Extended settings**.

Step 4 Set “Content Mode” to **Hybrid** and click **Save**.

Configuring Lobby Screen for TelePresence Server in Cisco TMS

Configuring all TelePresence Servers that will be used for Cisco WebEx Enabled TelePresence meetings with WebEx to set Lobby Screen to “On” is required.

To configure the Lobby Screen on the TelePresence Server in Cisco TMS, do the following:

Step 1 Go to **Systems** > **Navigator**.

Step 2 Click the TelePresence Server name.

Step 3 Click the **Settings** tab and then click **Extended settings**.

Step 4 Set “Use Lobby Screen for conferences” to **On** and click **Save**.

How the Lobby Screen Affects the First TelePresence Participant in a Meeting if the WebEx Welcome Screen is Disabled

If the WebEx Welcome Screen is disabled, the user experience of the first TelePresence participant in a meeting that uses TelePresence Server varies depending on how the “Use Lobby Screen for conferences” setting for TelePresence Server is configured in TMS. Table 6-1 describes what the first TelePresence participant in a meeting will see in different scenarios. To ensure that the first TelePresence participant never sees a black screen, make sure you set “Use Lobby Screen for conferences” to **Yes** for all TelePresence Servers you will use for WebEx Enabled TelePresence meetings as described in the previous section.

Table 6-1 Effect of Lobby Screen on First TelePresence Participant when WebEx Welcome Screen is Disabled

TelePresence Server Lobby Screen Setting	WebEx Enabled TelePresence meeting?	At least one WebEx participant?	Webex participant has camera enabled?	First TelePresence participant will see
No	No. TelePresence only.	N/A	N/A	Black screen (until at least one other TelePresence participant joins)
No	Yes	No	N/A	Black screen (until at least one other TelePresence or WebEx participant joins)
No	Yes	Yes	No	Silhouette image of WebEx participant
No	Yes	Yes	Yes	Video of WebEx participant
Yes	No. TelePresence only.	N/A	N/A	Lobby screen (until at least one other TelePresence participant joins)
Yes	Yes	No	N/A	Lobby screen (until at least one other TelePresence or WebEx participant joins)
Yes	Yes	Yes	No	Silhouette of WebEx participant
Yes	Yes	Yes	Yes	Video of WebEx participant

Configuring Conference Settings in Cisco TMS

This section provides information on the recommended and optional conference settings that can be configured in Cisco TMS for WebEx Enabled TelePresence meetings.

Default Setup and Teardown Buffers

Cisco recommends configuring the default setup and teardown buffers so that the TelePresence portion of the meeting starts and ends at the scheduled time.

Note Users scheduling a meeting using TMS, can change the setup and teardown buffers for each individual meeting if they want to.

To configure default setup and teardown buffers Cisco TMS, do the following:

Step 1 Go to **Administrative Tools** > **Configuration > Conference Settings**.

Step 2 In the Conference Create section, make the following settings:

- For Default Setup Buffer, select **0**.
- For Default Tear Down Buffer, select **0**.

Step 3 Click **Save**.

Default Picture Mode

Cisco recommends configuring Default Picture Mode to Continuous Presence. This allows multiple participants to be seen on screen at the same time for meetings that use MCU. TelePresence Server is always set to display multiple participants (called ActivePresence on the TelePresence Server).

To configure Default Picture Mode in Cisco TMS, do the following:

Step 1 Go to **Administrative Tools** > **Configuration > Conference Settings**.

Step 2 In the Conference Create Options section, set the following option:

- For Default Picture Mode, select **Continuous Presence**.

Step 3 Click **Save**.

Conference Connection/Ending Options

Cisco recommends configuring the Conference Connection/Ending Options in TMS so that if a meeting runs beyond the scheduled end time, participants are warned if there are not enough resources to extend the meeting.

To configure Conference Connection/Ending Options in Cisco TMS, do the following:

Step 1 Go to **Administrative Tools** > **Configuration > Conference Settings**.

Step 2 In the Conference Connection/Ending Options section, set the following options:

- For Supply Contact Information on Extend Meeting Scheduling Conflict, select **Yes**.

  This enables participants to see contact information when a meeting extension is not possible, due to a booking conflict.

Note This option is not supported by CTS, Jabber Video, and other endpoints that do not support direct messaging from TMS.

- For Show In-Video Warnings About Conference Ending, select **Yes**.

  TelePresence participants will receive a text message displayed in the video by the bridge, notifying them that the meeting will be ending.

  This feature is compatible with the following bridges:

- MCU 42xx, 45xx, 84xx, 85xx, 5xxx
- TelePresence Server 70xx, 87xx

Note Because WebEx is a single participant connection to the MCU/TelePresence Server, the in-video text message will only be visible to WebEx participants when a TelePresence user is the active speaker.

- (Optional) You can configure the length, timing and content of the in-video warnings, by setting the following options:
  - Message Timeout (in seconds): The number of seconds that a warning message will be displayed. Default setting: 10 seconds.
  - Show Message X Minutes Before End: The number of minutes before the end of a meeting that the warning message will appear.

    This message can be shown multiple times by separating the minutes with comma. For example **1,5** will display a warning message 1 minute and 5 minutes before the conference ends. Default setting: 1,5 (1 and 5 minutes).

Note For TelePresence MPS bridges, only 10, 5 and 1 can be entered here and will be displayed as a number icon on the screen. All other systems can be configured with any number intervals, and will show the Meeting End notification followed by the text string entered in Contact Information to Extend Meetings.

  - Contact Information to Extend Meetings: This field allows you to customize what follows the Meeting End notification. You can enter contact information such as the telephone number or name of a contact person who can extend the meeting for you.

    The text configured here applies to both the In-Video warnings about conference end sent from bridges to all participants in a conference, and to Meeting End notifications sent to individual participants by Cisco TMS.

Step 3 Click **Save**.

Configuring Single Sign On in Cisco TMS

Cisco TMS has the option to enable Single Sign On (SSO) for meetings booked by users with WebEx accounts. When SSO is configured and a user schedules a WebEx-enabled meeting, the WebEx username in their Cisco TMS user profile is passed to the WebEx site to complete the booking.

With SSO configured, it is only required to store the user's WebEx username in their Cisco TMS user profile. The user's WebEx password is not required.

There are two ways to add a user's WebEx username to their Cisco TMS user profile:

- A TMS Site Administrator manually enters the WebEx Username in a user's profile.

  When an organizer schedules a meeting with WebEx using Cisco TMS, Cisco TMS sends the meeting information to the WebEx site with that WebEx username designated as the WebEx host.

Note When a user has selected a WebEx site that has SSO enabled in TMS, Site Administrator privileges are required to edit the WebEx Username field. Users cannot edit their WebEx Username.

- Enable Cisco TMS to import WebEx usernames from Active Directory (AD)

Note You can use any field in AD. Email address and username are the most commonly used.

When an organizer schedules a meeting with WebEx using Cisco TMS, Cisco TMS requests AD for the WebEx username of the meeting organizer using the username and password that the Cisco TMS administrator filled in on the Network Settings page for AD lookup.

When AD supplies Cisco TMS with the WebEx username of the organizer, Cisco TMS sends the meeting information to the WebEx site with that WebEx username designated as the WebEx host.

Prerequisites

Before configuring SSO in Cisco TMS, you must work with the WebEx Cloud Services team to determine the following information that needs to be configured in both Cisco TMS and in the WebEx cloud:

- **Partner Name**

  This value must be determined by the WebEx team, because it must be unique among all WebEx customers. Contact the WebEx account team for this information.

  Example: **examplesso.webex.com**

- **Partner Issuer (IdP ID)**

  This is the Identity Provider, which is your TMS. This value must be determined by the WebEx team. Contact the WebEx account team for this information.

  Cisco recommends using a name to indicate your company's TMS.

  Example: **exampletms**

- **SAML Issuer (SP ID)**

  This refers to the Service Provider, which is WebEx. This value must be determined by the WebEx team. Contact the WebEx account team for this information.

  Example: **https://examplesso.webex.com/examplesso**

- **AuthnContextClassRef**

  This is the authentication context. The IdP authenticates the user in different contexts, e.g., X509 cert, Smart card, IWA, username/password).

  Use the default value automatically provided by TMS.

Configuring SSO in Cisco TMS

To configure SSO in Cisco TMS, do the following:

1. Ensure the WebEx site on which you want to enable SSO has been created in Cisco TMS.

See Configuring the Cisco WebEx Feature in Cisco TMS, page 6-2 for details.

2. Generate a certificate to secure the connection between Cisco TMS and the WebEx site.

   See Generating a Certificate for WebEx, page 6-13 for details.

3. Enable Partner Delegated Authentication on the WebEx site.

   See Enabling Partner Delegated Authentication on the WebEx site, page 6-16 for details.

4. Enable SSO in Cisco TMS.

   See Enabling SSO in Cisco TMS, page 6-17 for details.

Generating a Certificate for WebEx

WebEx requires that a certificate pair (public certificate and private key) be used to authenticate Cisco TMS to the WebEx cloud.

Certificate pair requirements:

- Public certificate must be in PEM format - to send to the WebEx Cloud Services team
- Certificate and private key bundled in a PKCS12-formatted file - for upload to Cisco TMS

You can generate a new certificate or use an existing one, such as the one used to enable HTTPS on your Cisco TMS server.

Using an Existing Certificate Signed by a Trusted Authority

If you currently use a certificate signed by a trusted authority, Cisco recommends using the existing certificate and key pair for your WebEx configuration. How you proceed is determined by if the private key is exportable, available or unavailable.

If Private Key is Exportable

If your private key is exportable, do the following:

Step 1 Using the Windows Certificate Manager Snap-in, export the existing key/certificate pair as a PKCS#12 file.

Step 2 Using the Windows Certificate Manager Snap-in, export the existing certificate as a Base64 PEM encoded .CER file.

Step 3 Provide this .CER file to the WebEx Cloud Services team.

Step 4 Use the PKCS#12 file you created in step 2, to upload to TMS in Enabling SSO in Cisco TMS, page 6-17

If Private Key is Not Exportable, but Key/Certificate Pair Available

If your private key is not exportable, but you have the key/certificate pair available elsewhere, do the following:

Step 1 Use Windows Certificate Manager Snap-in to export your existing certificate in a Base64 PEM file.

Step 2 Provide this Base64 PEM file to the WebEx Cloud Services team.

Step 3 Create a PKCS#12 key/certificate pair by using the command in step 10 of Using OpenSSL to Generate a Certificate, page 6-14.

Step 4 Use this PKCS#12 file to upload to TMS in Enabling SSO in Cisco TMS, page 6-17.

If Private Key is Not Exportable or Available

If your private key is not exportable and it is not available elsewhere, you will need to create a new certificate.

To create a new certificate, follow all the steps in Using OpenSSL to Generate a Certificate, page 6-14.

Creating a Key/Certificate Pair Signed by a Certificate Authority

If you do not have a key and certificate pair, but have a certificate authority you use, do the following:

Step 1 Create a new key/certificate pair to use for the WebEx SSO configuration using OpenSSL, following the steps in Using OpenSSL to Generate a Certificate, page 6-14.

Step 2 Create a Base64 PEM encoded version of the signed certificate using step 8 Using OpenSSL to Generate a Certificate, page 6-14

Step 3 Provide this version of the certificate to the WebEx Cloud Services team.

Step 4 Create a PKCS#12 key/cert pair by using the command in step 10 of Using OpenSSL to Generate a Certificate, page 6-14.

Step 5 Use this PKCS#12 file to upload to TMS in Enabling SSO in Cisco TMS, page 6-17.

Creating a Self-signed Key/Certificate Pair

If you do not have a key and certificate pair and do not have a certificate authority to use, you will need to create a self-signed certificate.

To create a self-signed key, do the following:

Step 1 Follow the steps in Using OpenSSL to Generate a Certificate, page 6-14.

Step 2 In step 6, follow the procedure to create a self-signed certificate signing request.

Step 3 Follow steps 7 through 9 and provide the base64 PEM file of self-signed certificate to the WebEx Cloud Services team.

Step 4 Follow step 10 to create a PKCS#12 PFX file

Step 5 Upload to TMS in Enabling SSO in Cisco TMS, page 6-17.

Using OpenSSL to Generate a Certificate

OpenSSL is an open source project designed to run on Unix and Linux. There is a Windows version available from Shining Light Productions: http://slproweb.com/products/Win32OpenSSL.html. Before using OpenSSL to generate a certificate, you must have OpenSSL installed. For more information, go to: http://www.openssl.org/.

To generate the TMS certificates required for WebEx and TMS, you must complete the following steps:

1. Generate a private key
2. Generate a certificate signing request (CSR)
3. Have a certificate authority sign the CSR
4. Provided the signed certificate to the WebEx team.
5. Convert the signed certificate and private key into a PKCS#12 formatted file
6. Upload the converted certificate and private key to TMS

To use OpenSSL to generate a certificate, do the following:

Step 1 In Windows, open a command prompt.

Step 2 Navigate to the openssl\bin installation directory.

Step 3 Generate a private key using following command:

```
openssl genrsa -out tms-privatekey.pem 2048
```

Step 4 Generate a certificate signing request (CSR) using the private key above:

```
openssl req -new -key tms-privatekey.pem -config openssl.cfg  -out tms-certcsr.pem
```

Step 5 Enter the data requested, including:

- Country
- State or province
- Organization name
- Organization unit
- Common name (this is the Cisco TMS FQDN)
- (Optional) Email address, password, company name

Step 6 Send the Cisco TMS certificate signing request file “tms-certcsr.pem” to be signed by a trusted certificate authority (CA) or self sign a certificate signing request using OpenSSL or Windows CA.

- For details on how to submit a certificate request to a trusted certificate authority, contact that certificate authority.
- To self-sign a certificate signing request using OpenSSL, use the following command. **tms-certcsr.pem** is your certificate signing request in PEM format. **tms-privatekey.pem** is your private key in PEM format. **days** is the number of days you'd like the certificate to be valid.

  ```
  openssl x509 -req -days 360 -in tms-certcsr.pem -signkey tms-privatekey.pem -out tms-cert.pem
  ```

  The resulting **tms-cert.pem** is your self-signed certificate.
- To self-sign a certificate signing request using Windows CA, use Windows Certificate Manager Snap-in. For details on how to submit a certificate request using Windows Certificate Manager Snap-in, refer to the documentation for Windows Certificate Manager Snap-in.

Step 7 When your certificate authority has signed your certificate request, they send a signed certificate to you, You should receive the signed certificate **tms-cert.der** back from the CA.

If the certificate is on an email or web page and not in its own file, copy the contents starting with the -----BEGIN CERTIFICATE----- line and through the -----END CERTIFICATE----- line. Save the contents to a text file and name the file **tms-cert.der**.

Step 8 Convert the signed certificate from .der to .pem using the following OpenSSL command:

openssl x509 -inform der -in tms-cert.cer -out tms-cert.pem

Note If the certificate authority provides you the signed certificate in .pem format, you can skip this step.

Step 9 Provide this signed certificate to the WebEx Cloud Services team.

Step 10 Combine the signed certificate .pem with the private key created in step 3:

openssl pkcs12 -export -inkey tms-privatekey.pem -in tms-cert.pem -out tms-cert-key.p12 -name tms-cert-key

You should now have a Cisco TMS certificate that contains the private key for SSO configuration to upload to Cisco TMS.

Before uploading this certificate to TMS, you must enable partner delegated authentication on your WebEx site. For more information, refer to Enabling Partner Delegated Authentication on the WebEx site in the next section. After enabling delegated authentication, use the combined certificate and private key you generated in step 10 above to upload to Cisco TMS in step 4 of Enabling SSO in Cisco TMS, page 6-17 to complete the SSO configuration.

Enabling Partner Delegated Authentication on the WebEx site

Before you can enable partner delegated authentication on your WebEx site, the WebEx Cloud Services team must make site provisioning changes to configure your TMS as a delegated partner.

These steps are required for enabling partner delegated authentication on your WebEx site:

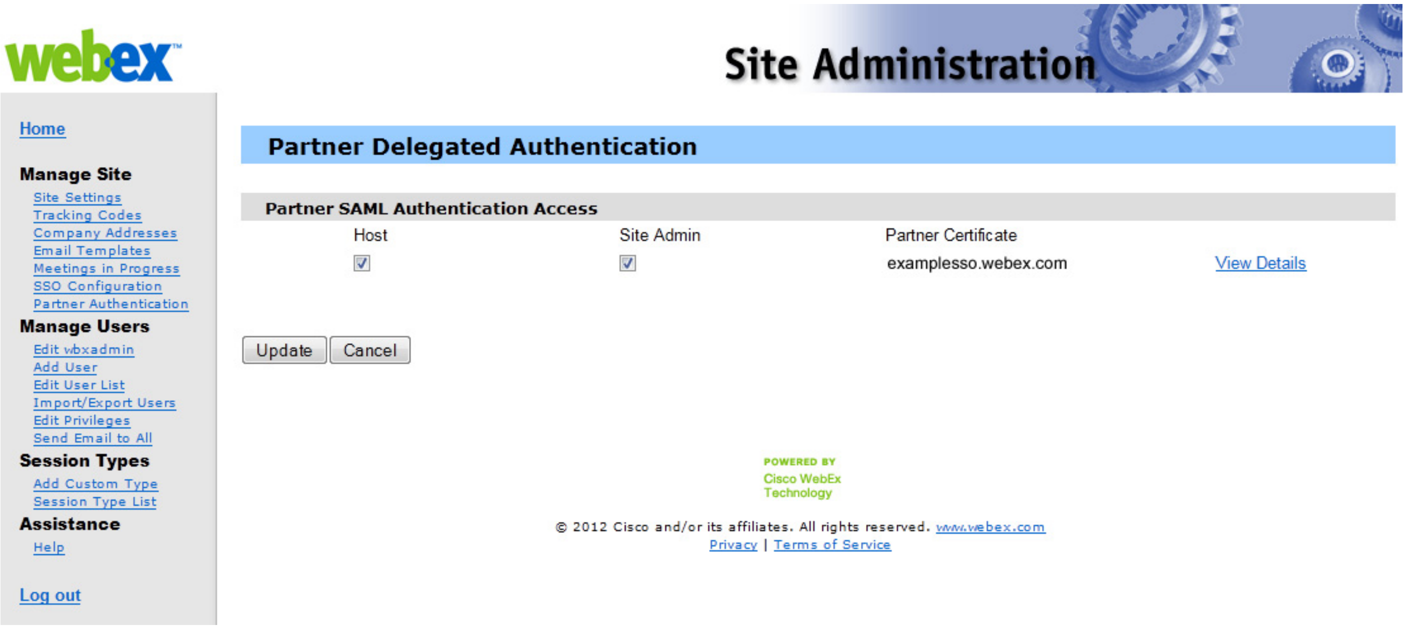
1. Request that the WebEx Cloud Services team add a Partner Certificate for your TMS, configured for SAML 2.0 federation protocol.
2. Provide the public certificate for your TMS to the WebEx Cloud Services team. For details on how to create a certificate, see Generating a Certificate for WebEx, page 6-13.
3. After the WebEx Cloud Services team notifies you that this step is complete, enable partner delegated authentication for both Host and Admin accounts in the Site Administration for your WebEx site, as described below.
4. Proceed with the section “Enabling SSO in Cisco TMS”.

To enable partner delegated authentication on your WebEx site, do the following:

Step 1 Log into your WebEx administrative site and go to **Manage Site > Partner Authentication**.

The Partner Delegated Authentication page appears.

Figure 6-3 Partner Delegated Authentication on the WebEx Administrative Site



Partner Delegated Authentication

Partner SAML Authentication Access

Host	Site Admin	Partner Certificate	
☑	☑	examplesso.webex.com	View Details

Step 2 In the Partner SAML Authentication Access section, make sure both **Host** and **Site Admin** are checked and click **Update**.

Enabling SSO in Cisco TMS

Before you begin, make sure you have the following information:

- Certificate Password (if required)
- Partner Name
- Partner Issuer (IdP ID)
- SAML Issuer (SP ID)
- AuthnContextClassRef

Note Before enabling SSO, you must enable Partner Delegated Authentication on your WebEx site. For more information, refer to Enabling Partner Delegated Authentication on the WebEx site, page 6-16.

To enable SSO in Cisco TMS, do the following:

Step 1 Log into Cisco TMS, and go to **Administrative Tools** > **Configuration** > **WebEx Settings**.

Step 2 In the WebEx Sites pane, click the site name of the WebEx site on which you want to enable SSO.

The WebEx Site Configuration pane appears.

Step 3 For Enable SSO, select **Yes**.

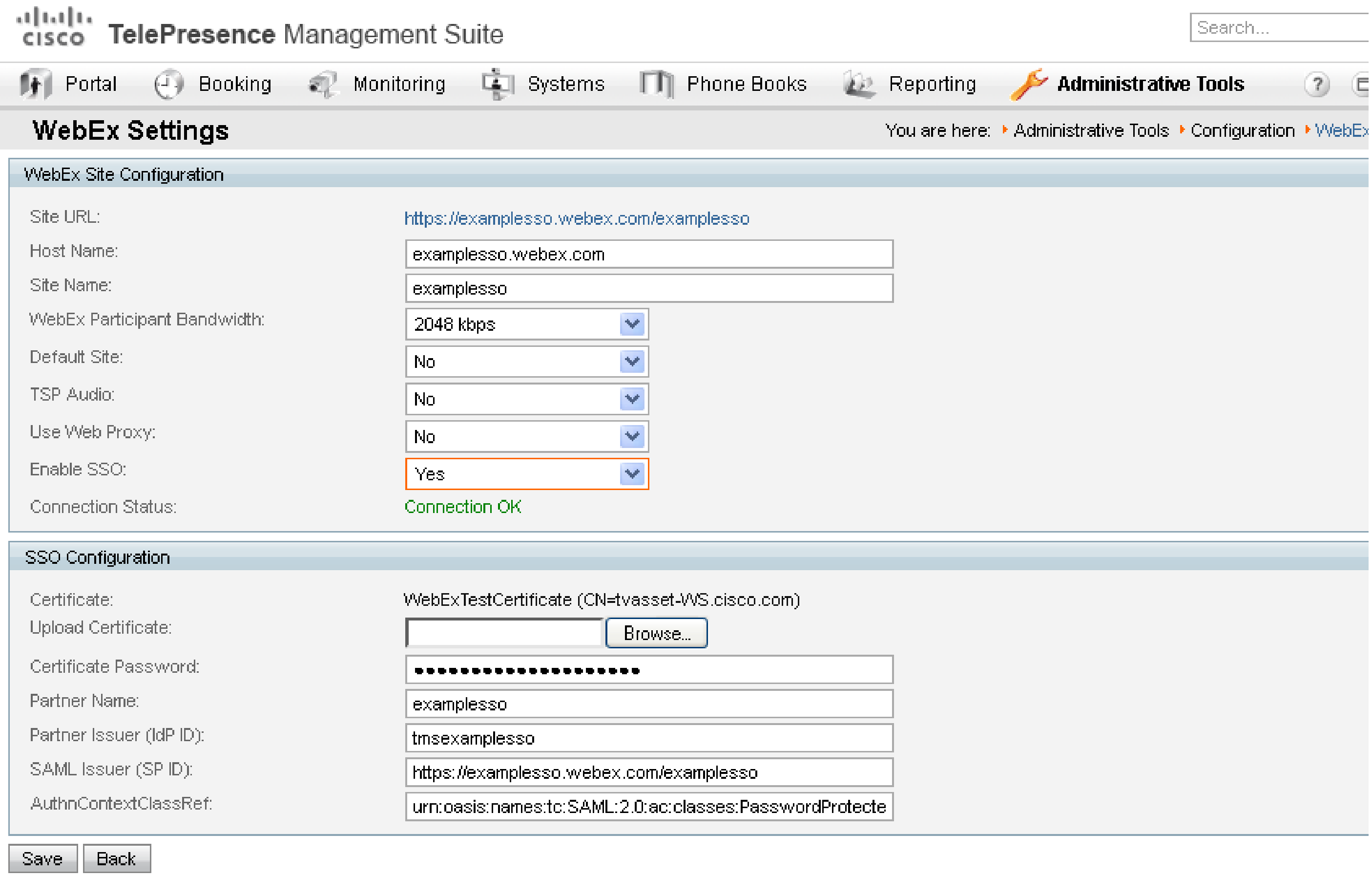
The SSO Configuration pane appears.

Step 4 Click **Browse** and upload the PKS #12 private key certificate (.PFX) you generated in Generating a Certificate for WebEx, page 6-13.

Step 5 Complete the rest of the SSO configuration fields using the password and other information that you selected when generating the certificate.

Step 6 Click **Save**.

Figure 6-4 WebEx Settings SSO Configuration in Cisco TMS



WebEx Site Configuration

Site URL:	https://examplesso.webex.com/examplesso
Host Name:	examplesso.webex.com
Site Name:	examplesso
WebEx Participant Bandwidth:	2048 kbps
Default Site:	No
TSP Audio:	No
Use Web Proxy:	No
Enable SSO:	Yes
Connection Status:	Connection OK

SSO Configuration

Certificate:	WebExTestCertificate (CN=tvasset-WS.cisco.com)
Upload Certificate:	
Certificate Password:	••••••••••••••••••••••
Partner Name:	examplesso
Partner Issuer (IdP ID):	tmsexamplesso
SAML Issuer (SP ID):	https://examplesso.webex.com/examplesso
AuthnContextClassRef:	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtecte

Supported Configurations for TMS to Schedule on Behalf of the WebEx Host

While the focus of the previous section was how to configure SSO on TMS, it is also possible to configure SSO on the WebEx site itself. As a result, it's helpful to understand all the supported configurations for scheduling of WebEx Enabled TelePresence meetings.

There are three possible supported configurations to allow the TMS to schedule on behalf of the WebEx host:

1. WebEx site does not use SSO and TMS does not have SSO configured (no partner delegated authentication relationship with the WebEx site)

- WebEx host login: The WebEx username and password are stored in WebEx, and the user authenticates directly to the WebEx site.
- TMS scheduling: The host's WebEx username and password are also stored in their TMS personal profile. This must be maintained by the user, if they have access to the TMS, or by the TMS administrator. The TMS passes both username and password to WebEx at scheduling time.

2. WebEx site does not use SSO, but TMS does have SSO configured (partner delegated authentication relationship with the WebEx site).
   - WebEx host login: The WebEx username and password are stored in WebEx, and the user authenticates directly to the WebEx site.
   - TMS scheduling: The host's WebEx username is stored in a TMS personal profile (a TMS admin task) but the WebEx password is not stored in TMS. TMS is trusted to schedule for that user.
3. WebEx site uses SSO, and TMS has SSO configured (partner delegated authentication relationship with the WebEx site).
   - WebEx host login: The WebEx user logs in through the SSO identity service provider.
   - TMS scheduling: The host's WebEx username is stored in a TMS personal profile (a TMS admin task) but the WebEx password is not stored in TMS. TMS is trusted to schedule for that user.