Configuring Settings

This module describes how to configure your settings.

- Configuring Your Company Information, page 2
- Configuring Your Branding Settings, page 3
- Configuring Your Meeting Settings, page 4
- About Configuring Your Audio Settings, page 5
- Configuring Your Video Settings, page 9
- Configuring Your Mobile Settings, page 9
- Configuring Quality of Service (QoS), page 10
- Configuring Passwords, page 11
- Configuring Your Email Settings, page 14
- Configuring Your Download Settings, page 16
- Managing Certificates, page 18
- Generating SSL Certificates, page 19
- Importing SSO IdP Certificates, page 23
- Importing Secure Teleconferencing Certificates, page 23
- Configuring User Session Security, page 25
- Configuring Federated Single Sign-On (SSO) Settings, page 25
- Configuring Your Cloud Features, page 29
- Configuring Virtual Machine Security, page 29

Configuring Your Company Information

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings**. If you are viewing one of the other settings pages, you can also select **Company Information** under the Settings section.

Step 3 Complete the fields on the page and select **Save**.

Option	Description
Company Name	Your company or organization name.
Address 1	Address line 1.
Address 2	Address line 2.
City	Your city.
State/Province	Your state or province name.
ZIP/Postal Code	ZIP or other postal code.
Country/Region	Your country or region name.
Business Phone	Drop-down menu with country code and field for business phone with area code.
Time Zone	Your time zone.
Language	Your language. Language setting affects the following: • The sign-in page seen by administrators when they activate their administrator accounts for the first time. • The default audio prompts played for call-in teleconference users.
Locale	Your locale. The locale setting affects the display of times, dates, currency, and numbers.

Configuring Your Branding Settings

Before You Begin

Prepare the following before configuring your branding settings:

- A 120x32 PNG, GIF, or JPEG image containing your company logo
- Your company's privacy statement URL
- Your company's terms of service statement URL
- Your company's support URL

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Branding**.

Step 3 Complete the fields on the page and select **Save**.

Option	Description
Company Logo	Browse to your logo file. Your logo must be in PNG, JPEG, or GIF format. The maximum dimensions are 120x32 pixels and the maximum file size is 5 MB.
Privacy Statement	Enter a URL to your company's privacy statement.
Terms of Service	Enter a URL to your company's terms of service.
Custom Footer Text	The text you enter will be in the footer of all end-user and administrator emails that are sent by your system.
Header Background Color	Select this option to turn off the default background color. Note that this affects all browser bars and emails.
Support Contact URL	Enter the URL to your company's support web page.

Removing a Company Logo

Before You Begin

Create a transparent 120x32 PNG or GIF file.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Branding**.

Step 3 For the Company Logo field, select **Browse** and choose your transparent 120x32 PNG or GIF file.

Step 4 Select **Save**.
Your previous company logo is replaced by your blank PNG or GIF file. Confirm that the original logo has been removed.

Configuring Your Meeting Settings

Configure your meeting settings to control which features participants can use. Configure the following features:

- Join meeting settings
- Maximum participants per meeting (meeting size)

Note This setting is limited by the system size configured during deployment. See Confirming the Size of Your System for more information.

- Participant privileges

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Meetings**.

Step 3 In the Join meeting settings section, select your options.
Default settings are **Allow participants to join meetings before host**, **Allow participants to join teleconference before host**, and **First participant to join will be the presenter**. Participants can join meetings up to 15 minutes before the starting time if **Allow Attendees to join Meetings before Host** is selected. Optionally select **Anyone can present in the meeting**.

Note If you deselect **Allow participants to join meetings before host** the **First participant to join will be the presenter** feature is automatically deselected.

Step 4 Select the maximum participants per meeting by dragging the slider. The maximum number of participants for your system is configured during deployment. Following are the system size settings and corresponding maximum meeting sizes.

System Size	Maximum Meeting Size
50	50

System Size	Maximum Meeting Size
250	100
800	100
2,000	100

Step 5 In the participant privileges section, select your options. **Chat**, **Polling**, **Document review and presentation**, and **Sharing and remote control** are selected by default. The selected participant privileges appear in the users' controls.
Recording is disabled by default. Select **Record** to record and store meetings on your storage server.

Note You must configure a storage server to enable recording. See Configuring a Storage Server for more information.

Step 6 Select **Save**.

About Configuring Your Audio Settings

The first time you configure your audio settings, you are guided through the process by a wizard that helps you set your CUCM SIP configuration and call-in access numbers. After you have completed the wizard and configured your initial audio settings, you can configure all other audio settings.

Configuring Your Audio Settings for the First Time

The first time you configure your audio settings, you must specify which features you want and you must configure your CUCM settings. A wizard guides you through the first-time installation procedure.

Before You Begin

You must enable teleconferencing and configure CUCM before you proceed with your audio configuration. You must configure CUCM on two systems if you plan to provide teleconferencing high availability. Refer to the Planning Guide for more information. To proceed you must obtain the following information:

- Prepare a list of call-in access numbers that your participants use to call into meetings.
- Obtain a valid secure conferencing certificate if you plan to use TLS/SRTP teleconferencing encryption. See the Importing Secure Teleconferencing Certificates, on page 23 page for more information.

  Note This feature is not available in Russia or Turkey.

- Your teleconferencing server type (load balancer or application server).

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Audio**.
The **Audio** page appears and your Current Audio Features are displayed.

Step 3 Select **Next**.
The **SIP Configuration** page appears. This page displays the SIP configuration information you need to configure CUCM including the IP address and port number for each server type.

Step 4 Select **Turn On Maintenance Mode** and **Continue** to confirm.

Step 5 Select **Next**.
The **Enable Teleconference: CUCM Setting** page appears, displaying your current settings.

Step 6 Select **Edit** to change your settings.
The **CUCM (Cisco Unified Communication Manager)** dialog box appears.

Step 7 Complete the fields in the **CUCM (Cisco Unified Communication Manager)** dialog box as follows:

a) Enter an IP address for CUCM 1 IP Address and optionally for CUCM 2 IP Address.
Note CUCM 2 is not required but it is recommended for teleconferencing high availability.

b) Enter the port number for your system. The port number must match the port number assigned in CUCM. (**Default:** 5062)

c) Use the **Transport** dropdown menu to select the transport type for your system. (**Default:** TCP)
Note If you select TLS as your transport type, you must import a valid secure conferencing certificate for each of your CUCM servers, export the SSL certificate and upload it into CUCM, and configure your system's fully qualified domain name (FQDN) as the SIP domain name on each CUCM server. See Importing Secure Teleconferencing Certificates, on page 23 for more information on importing your certificates and Configuring CUCM in the Planning Guide for more information on CUCM.

d) Select **Continue**.

Your new or updated CUCM settings appear on the **Enable Teleconference: CUCM Setting** page.

Step 8 Select **Next**.
The **Enable Teleconference: Access Number Setting** page appears.

Step 9 Select **Edit**.
The **Call-in Access Numbers** dialog box appears.

Step 10 Select **Add** to add a call-in access number.
A line is added in the dialog box for the phone label and number. Each time you select **Add**, an additional line appears in the dialog box.

Step 11 Enter the **Phone Label** and **Phone Number** for each access number that you add and select **Continue** after you have finished adding numbers.
Note Make sure you only add numbers that you have configured in CUCM. The numbers you add appear in email invitations and your Cisco WebEx Meetings client.

Example:
Enter "Headquarters" for the **Phone Label** and "888-555-1212" for the **Phone Number**.

The access numbers you entered are added to your system and you are returned to the **Enable Teleconference: Access Number Setting** page. The page now indicates how many access numbers have been configured.

Step 12 Select **Save**.
The wizard informs you that you have successfully configured your teleconferencing features.

Step 13 (Optional) Enter a display name in the **Display Name** dialog box.

Step 14 (Optional) Enter a valid caller ID in the **Caller ID** dialog box.
Note The caller ID is limited to numerical characters and dash (-) and has a maximum length of 32 characters.

Step 15 (Optional) Configure your WebEx Call Me setting (**Default**: Press 1 to connect to meeting). Optionally deselect this option to bypass the requirement to press **1** to connect to a meeting.
Note We do not recommend that you deselect this option unless your phone system is incapable of sending a **1** digit.

Step 16 (Optional) Select your **Telephone entry and exit tone**.

- Beep (default)
- No tone
- Announce name

Step 17 (Optional) If IPv6 is configured on your system, set your **IPv6 Teleconferencing** setting to **On** or **Off**. (**Default**: Off. A setting of **Off** indicates that IPv4 is the setting.)
Note The **IPv6 Teleconferencing** option is not available on systems not configured for IPv6.

Step 18 Select **Save**.

Step 19 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Configuring Your Audio Settings

Before You Begin

If you have not already configured your audio settings, see the Configuring Your Audio Settings for the First Time, on page 5 section.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Audio**.

Step 3 Select **Turn On Maintenance Mode** and **Continue** to confirm.

Step 4 Configure your **Edit Audio Features** settings.

Option	Description
Teleconference	• User Call In and Call Me service–Enables users to attend a teleconference by calling specified phone numbers or by receiving a Call Me call from the system. • Call In–Enables users to attend a teleconference by calling specified phone numbers. • OFF–Disables all calling features.
Voice connection using computer	• ON • OFF

Step 5 In the Edit Teleconference Settings section, select the **Edit** link under CUCM (Cisco Unified Communication Manager) to change your settings.

Option	Description
CUCM 1 IP Address	Enter the hostname or an IP address for your CUCM 1 system.
CUCM 2 IP Address	(Optional) Enter the hostname or an IP address for your CUCM 2 (load balancing) system. **Note** CUCM 2 is not required but it is recommended for teleconferencing high availability.
Port Number	Enter a valid port number. Make sure the port number matches the setting in CUCM. **Default:** 5062
Transport	Select the transport type. **Note** If you select TLS as your transport type, you must import a valid secure conferencing certificate for each of your CUCM servers, export the SSL certificate and upload it into CUCM, and configure your system's fully qualified domain name (FQDN) as the SIP domain name on each CUCM server. See Importing Secure Teleconferencing Certificates, on page 23 for more information on importing your certificates and Configuring CUCM in the Planning Guide for more information on CUCM. **Default:** TCP

The **CUCM (Cisco Unified Communications Manager)** dialog box appears. Complete the fields and select **Continue**.

Step 6 In the Edit Teleconference Settings section, select the **Edit** link under Call In Access Numbers to add, change, or delete your access numbers.

a) Select **Add** and enter a phone label and phone number for each new access number you want to add.
b) To delete a number, select the **Delete** link at the end of the line.
c) Enter updated information in the phone label and phone number fields for any access number you want to change.

d) Select **Continue** when you are finished.

Note Make sure you only add numbers that you have configured in CUCM. The numbers you add appear in email invitations and your Cisco WebEx Meetings client.

Step 7 Enter a display name in the **Display Name** dialog box.

Step 8 Enter a valid caller ID in the **Caller ID** dialog box.

Note The caller ID is limited to numerical characters and dash (-) and has a maximum length of 32 characters.

Step 9 Configure your WebEx Call Me setting (**Default**: Press 1 to connect to meeting). Optionally deselect this option to bypass the requirement to press **1** to connect to a meeting.

Note Cisco does not recommend that you deselect this option unless your phone system is incapable of sending a **1** digit.

Step 10 Select your **Telephone entry and exit tone**.

- Beep (default)
- No tone
- Announce name

Step 11 If IPv6 is configured on your system, set your **IPv6 Teleconferencing** setting to **On** or **Off**. (**Default**: Off. A setting of **Off** indicates that IPv4 is the setting.)

Note The **IPv6 Teleconferencing** option is not available on systems not configured for IPv6.

Step 12 Select **Save**.

Step 13 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Configuring Your Video Settings

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Video**.

Step 3 Select **On** or **Off** and then select **Save**. (**Default:** On).

Configuring Your Mobile Settings

Note Android is not supported in Cisco WebEx Server 1.0.

Before You Begin

To configure mobile settings you must add public access on your system during deployment. See Adding Public Access to Your System for more information.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Mobile**.

Step 3 Configure your mobile settings by selecting which mobile platforms your system supports and then select **Save**. (**Default:** iOs WebEx application)

Configuring Quality of Service (QoS)

Differentiated Services (DiffServ) code point (DSCP) settings determine the QoS for the audio and video media signaling, as defined in RFC 2475. Cisco recommends that you retain the default value. The other values are available for the rare instances when the network requires a different DSCP setting. For more information, see the "Network Infrastructure" chapter of the Cisco Unified Communications Solution Reference Network Design (SRND) that applies to your version of Cisco Unified Communications Manager at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html.

Following are the default values:

- WebEx Audio (Media)
  - IPv4 QoS Marking: **EF DSCP 101110**
  - IPv6 QoS Marking: **EF DSCP 101110**
- WebEx Audio (Signaling)
  - IPv4 QoS Marking: **CS3 (precedence 3) DSCP 011000**
- WebEx Voice Connection Using Computer
  - IPv4 QoS Marking: **AF41 DSCP 100010**
- WebEx Video
  - IPv4 QoS Marking: **AF41 DSCP 100010**

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Quality of Service**.

Step 3 Select QoS marking settings using the appropriate dropdown menus and then select **Save**.

Configuring Passwords

You can configure password settings for the following:

- General Passwords—Controls password expiration periods and enables you to force users to change their passwords either immediately or at a specified interval.
- User Passwords—Enables you to configure password strength for user accounts including mixed case, length, character types and usage, dynamic web page text controls, and setting up a list of unacceptable passwords.
- Meeting Passwords—Enables you to enforce password usage for meetings and to configure password strength for meetings including mixed case, length, character types and usage, dynamic web page text controls, and setting up a list of unacceptable passwords.

Note If SSO is enabled on your system, the settings on the **General Password** and **User Password** pages and the password change controls on the **Edit User** page no longer apply to host accounts.

Configuring Your General Password Settings

Your general password settings enable you to configure account deactivation and password age limitations. All password settings on this page are optional and can be toggled on (checked) or off (unchecked).

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Password Management** > **General Password**.

Step 3 (Optional) Select the **Deactivate host account after number day(s) of inactivity** checkbox and enter the number of days in the text field. (**Default**: Checked and set for 90 days)

Note This feature only applies to host accounts. You cannot deactivate an administrator account using this feature. To deactivate an administrator account, see Deactivating Users.

Step 4 (Optional) Select the **Force all users to change password every number day(s)** checkbox and enter the number of days in the text field. (**Default**: Unchecked)

Step 5 (Optional) Select **Force all users to change password on next login**. (**Default**: Unchecked)

Step 6 Select **Save**.

Configuring Your User Password Settings

Configure your user password requirements and limitations.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Password Management** > **User Password**.

Step 3 Change your user password settings by configuring the fields on the page.

Option	Description
Require strong passwords for user accounts	Select this option to enable the remaining options. **Default**: Selected
Minimum length of characters	Minimum character requirement. **Default**: Selected and **6** characters
Minimum number of alphabetic characters	Minimum alphabetical (non-numeric, non-special characters). **Default**: Selected and **1** character
Minimum number of numeric characters	Minimum numerical (non-alphabetical, non-special characters). **Default**: Selected and **1** number
Minimum number of special characters	Minimum special (non-alphabetical, non-numeric characters). **Default**: Not selected and **1** character
Must include mixed case	Password must contain uppercase and lowercase alphabetical characters. **Default**: Selected
Do not allow any character to be repeated more than 3 times	No one character (alphabetical, numeric, or special) can be repeated more than three times. **Default**: Selected
List of unacceptable passwords	Administrator-specified list of unusable passwords. **Default**: Not selected
Company name, site name, user email address, and host name are always unacceptable	Do not use these specific names. **Default**: Not selected
Must not include previous *n* passwords	Do not use previously used passwords. Select a number from the dropdown menu to specify the number of previous passwords you cannot use. **Default**: Not selected **Default number**: 3

Step 4 Select **Save**.

Configuring Your Meeting Passwords

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Password Management** > **Meeting Password**.

Step 3 Change your meeting password settings by configuring the fields on the page.

Note All options are not selected by default.

Option	Description
All meetings must have passwords	Requires all meetings to have passwords.
Require strong passwords for meetings	Select this option to enable the remaining options.
Minimum character length	Minimum character requirement. **Default**: 6
Minimum number of alphabetic characters	Minimum alphabetical (non-numeric, non-special characters). **Default**: 1
Minimum number of numeric characters	Minimum numerical (non-alphabetical, non-special characters). **Default**: 1
Minimum number of special characters	Minimum special (non-alphabetical, non-numeric characters). **Default**: 1
Must not contain these special characters (space, \, ', ", /, &, <, >, =, [,])	Select this option to prohibit the use of these characters.
Must include mixed case	Password must contain uppercase and lowercase alphabetical characters.
List of unacceptable passwords	Administrator-specified list of unusable passwords.

Option	Description
Company name, site name, user email address, host name, and meeting topic are always unacceptable	Select this option to prohibit theuse of these words or character strings.

Step 4 Select **Save**.

Configuring Your Email Settings

You can configure your email settings and templates. Your email templates have default settings that you can optionally change.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Email**.
The **Variables** page opens.

Step 3 Enter your **Reply-To** email address, your **From Name**, and select **Save**.

Step 4 Select **Templates**. See About Email Templates, on page 14 for descriptions of each template type.
The **Templates** page appears. Select the **Common** or **Meetings** tab. **Common** is the default.

Step 5 To configure email templates, select the desired template link on the **Common** and **Meetings** tab.

Step 6 Make changes (if any) to the email template you selected and select **Save**.

Example:
Select the **Account Reactivated** template link on the **Common** tab. Make changes to the fields in the **Account Reactivated** dialog box and select **Save**.
The default **From Name** and **Reply-To** values are taken from the settings you configure on the **Variables** page.

About Email Templates

Use the email templates to communicate important events to users. There are two types of email templates:

- Common–Including lost password, host and invitee notifications, recording availability, and other general notices.
- Meetings–Including meeting invitations, cancellations, updates, reminders, and information notices.

Table 1: Common Email Templates

Title	Description
Account Reactivated	Sent to a user after an administrator reactivates the user's account.
Forgot Password–Password Changed	Sent to a user after he has reset his password from the end-user site.
Forgot Password–Reset Password	Sent to a user after he has reset his password from the end-user site. This email asks the user to create a new password.
PT-Host Notification	Sent to a meeting host after a meeting is scheduled using Productivity Tools.
PT-Invitee Notification	Sent to meeting invitees after a meeting is scheduled using Productivity Tools.
Recording Available for Host	Sends the host a link to a meeting recording.
SSO Activation Email	Sent after Single Sign-On (SSO) is enabled.
Send Email To All Users	Sends an email to all users on the system.
Setup Cisco WebEx–Android	Informs users about the Cisco WebEx app for Android and provides a download link for the app.
Setup Cisco WebEx–iPhone/iPad	Informs users about the Cisco WebEx app for iPhone/iPad and provides a download link for the app.
Share Recording	Sends selected meeting attendees a link to a meeting recording.
Share Recording from MC	Sends selected meeting attendees a link to a meeting recording. Attendees selected by the host in Meeting Center after selecting **Leave Meeting**.
Welcome Email	Sent to a new administrator after his or her account is created.

Table 2: Meetings Email Templates

Title	Description
In-Progress Meeting Invite for Attendee	Sent to users when a host invites them to a meeting while the meeting is in progress.
Instant Meeting Invite for Host	Sent to the host and attendees when the host selects **Meet Now**.
Meeting Canceled for Attendee	Informs a user that a scheduled meeting has been canceled.

Title	Description
Meeting Canceled for Host	Sent to a meeting's host to confirm cancellation of a meeting.
Meeting Information Updated for Alternate Host	Provides meeting information to the alternate host when the meeting settings have been changed.
Meeting Information Updated for Attendee	Provides meeting information for a meeting invitee when the meeting settings have been changed.
Meeting Information Updated for Host	Provides meeting information to the host when the meeting settings have been changed.
Meeting Information Updated for Host	Provides meeting information for the meeting's host when the meeting settings have been changed.
Meeting Reminder for Alternate Host	Sends a meeting reminder to the meeting's alternate host.
Meeting Reminder for Host	Sends a meeting reminder to the meeting's host.
Meeting Rescheduled for Alternate Host	Sends updated meeting information to the alternate host.
Meeting Rescheduled for Attendee	Sends updated meeting information to attendees.
MeetingInfo Updated for Alternate Host	Sends a meeting confirmation to the alternate host.
MeetingInfo Updated for Attendee	Sends a meeting invitation to attendees.
MeetingInfo Updated for Host	Sends a meeting confirmation to the host.

Configuring Your Download Settings

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Downloads**.

Step 3 Select the **Auto update WebEx desktop applications** check box to configure periodic automatic updates. (**Default**: checked.)

Step 4 Select your download method:

- Permit users to download WebEx desktop applications
- Manually push Cisco WebEx Meetings and Productivity Tools to user’s desktop

If you select **Permit users to download WebEx desktop applications**, you can select **Save** to finish your Download configuration. No further action is necessary. If you select **Manually push Cisco WebEx Meetings and Productivity Tools to user’s desktop**, proceed to the next step.

Use the **Manually push Cisco WebEx Meetings and Productivity Tools to user's desktop** option to enable conferencing for users who do not have administrator permissions.

If you select **Manually push Cisco WebEx Meetings and Productivity Tools to user's desktop**, the Cisco WebEx Meetings and Productivity Tools sections appear on the page.

Step 5 In the Cisco WebEx Meetings section, select your Cisco WebEx Meetings platform from the dropdown menu, select a language from the dropdown menu, select **Download**, and select **Save** to save the file to your system.

Note The default language is the language you have configured in your company information. See Configuring Your Company Information, on page 2 for more information.

Step 6 In the Productivity Tools section, select a language from the dropdown menu, select **Download**, and select **Save** to save the file to your system.

Note The default language is the language you have configured in your company information. See Configuring Your Company Information, on page 2 for more information.

Step 7 Select **Save** to save your download settings.

About Downloads

This product can be used on Windows PCs where users have administrator privileges and on those that do not. This section provides basic information about downloads. For detailed information on configuring downloads refer to the About Downloads section of the Planning Guide.

On PCs without administrator privileges:

- We recommend that you push the Cisco WebEx Meetings application and Productivity Tools to end-user desktops offline before you inform end-users that user accounts have been created for them. This ensures that your users can start and join meetings from their web browsers and Windows desktops the first time they sign in.
- You can acquire the .MSI installers for each from the **Admin** > **Settings** > **Downloads** page. See Configuring Your Download Settings, on page 16 for more information.
- If you decide against pushing the applications to your users, they can still access these applications from the end-user download pages. However, if their PCs prohibit installation of downloaded applications, they will not be able to complete the installation process.
- When users join meetings by using their web browser (the Cisco WebEx Meetings application can still be downloaded on demand) they can join meetings successfully. In addition, the Cisco WebEx Meetings application attempts to perform an installation to speed up the process of starting or joining future meetings. This fails because their PCs do not have administrator privileges.

On PCs with administrator privileges:

- Users can download and install the Cisco WebEx Meetings application and Productivity Tools from the end-user download pages. No additional administrator action is required.
- Users are advised to install the Productivity Tools the first time they sign in.
- The Cisco WebEx Meetings application is downloaded on-demand the first time a user joins a meeting and is installed silently on the user's PC.

Managing Certificates

Certificates are used to ensure secure communication between the components of your system. When your system is first deployed, it is configured with a self-signed certificate. While a self-signed certificate can last for up to five years, we strongly recommend that you configure certificates that are validated by a certificate authority. A certificate authority ensures that communication between your virtual machines is authenticated. Note that you must install a certificate for each virtual machine on your system.

The following certificate types are supported:

- SSL—Required on all systems.
- SSO IdP—For SSO with identity provider (IdP) certificates.
- Secure teleconferencing—Required for TLS teleconferencing. You can configure up to two secure teleconferencing certificates, one for each CUCM system that you choose to configure.

All systems must have a SSL certificate. This product supports the following SSL certificates:

- Self-signed
- Certificate authority-signed
- External certificate authority-signed

You cannot update your certificates. If you add virtual machines to your system or change any of your existing virtual machines, you must generate new certificates for each virtual machine on your system.

SSL certificates can become invalid for the following reasons:

- Your system size has been expanded, resulting in the deployment of new virtual machines. The fully qualified domain names (FQDNs) of these new virtual machines are not present in your original SSL certificate.
- Your system has been upgraded, resulting in the deployment of new virtual machines. The FQDNs of these new virtual machines are not present in your original SSL certificate.
- A high-availability system has been added, resulting in the deployment of new virtual machines. The FQDNs of these new virtual machines are not present in your original SSL certificate.
- The Cisco WebEx site URL has changed. This URL is not present in your original SSL certificate.
- The Administration site URL has changed. This URL is not present in your original SSL certificate.
- The FQDN of the administration virtual machine has changed. This FQDN is not present in your original SSL certificate.
- Your current SSL certificate has expired.

If your SSL certificate becomes invalid for any reason, your system will automatically generate new self-signed certificates and you are informed of this change by a global warning message at the top of the Administration site page indicating that SSL has become invalidated.

Generating SSL Certificates

Your system must have a SSL certificate configured. This product supports the following types of SSL certificates:

- Self-signed
- Certificate authority-signed
- External certificate authority-signed

Generating a Certificate Signing Request (CSR)

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Turn On Maintenance Mode** and **Continue** to confirm.

Step 3 Select **Settings** > **Security** > **Certificates** > **Generate CSR**.

Step 4 Complete the fields on the **Generate CSR (Certificate Signing Request)** page.

Option	Description
Common Name	Select **Subject Alternative Name** certificate or **Wildcard** certificate.
Subject Alternative Name **Note** This option appears only if you select **Subject Alternative Name** for your Common Name type.	Your administration site and virtual machine names. No subject alternative names are required if you selected a wildcard common name.
Organization	Enter your organization name.
Department	Enter your department name.
City	Enter your city.
State/Province	Enter your state or province.
Country	Select your country.

Option	Description
Key Size	Select your key size from the following options: • 2048 • 3072 • 4096 **Default**: 2048 (Recommended)

Step 5 Select **Generate CSR**.
The **Download CSR** dialog box appears.

Step 6 Select **Download**.
You receive a ZIP file that contains the CSR and the associated private key. The CSR file is called csr.pem and the private key file is called csr_private_key.pem.

Step 7 Back up your system using VMware Data Recovery. See Creating a Backup Using VMware vCenter for more information.

Note Backing up your system preserves the private key in the event that you need to restore it.

Step 8 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Importing a SSL Certificate

You can import a SSL certificate using this feature. Cisco WebEx Meetings Server supports X.509 certificates with PEM and DER encoding and PKCS12 Archives.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **Certificates** > **More Options** > **Import SSL Certificate**.
If you already have a certificate installed, the system warns you that importing a new certificate will overwrite it.

Step 3 Select **Continue**.

Step 4 Select **Browse** and choose your certificate file.
You must choose an X.509-compliant certificate or certificate chain. Valid types include:

- PEM/DER encoded certificate: .CER / .CRT / .PEM / .KEY
- PKCS12 encrypted certificate: .P12 / .PFX

You can import a certificate chain using a PKCS#12 file or a single file of PEM blocks. If use a PEM file, It must be formatted as follows:

- (Optional) If you want to upload a private key, the private key must be the first block in the file. It can be encrypted or un-encrypted. It should be in PKCS#8 format, PEM encoded. If it is encrypted, you must enter the password to decrypt it in the passphrase field.
- The next element must be the certificate of the intermediate certificate authority that issued your certificate in PEM encoded X.509 format.
- You can include as many intermediate certificates as you use in your infrastructure. The certificate of the root certificate authority should not be included. If you are using a private certificate authority, you must make sure that the root certificate is distributed to all clients.

All the certificates must be uploaded together in one file. You cannot upload one certificate and then add the intermediate certificates later. You might want to upload the intermediate certificates if you are using a certificate authority that uses intermediate certificates and the intermediate certificates are not distributed in their clients. Uploading them will prevent certificate warnings.

PKCS#12 files must have a .p12 extension. They should only contain the certificates and private key (optional).

Step 5 Select **Upload**.
After you select **Upload**, the system will determine if your certificate is valid. A certificate can be invalid for the following reasons:

- The certificate file is not a valid certificate file.
- The certificate file you selected has expired.
- Your public key must be at least 2048 bits.
- The server domains in the certificate do not match the site URL.
- The private key that was automatically generated by the system is not compatible with the certificate.

If the certificate is valid, proceed to the next step. If the certificate is invalid, you cannot upload it. You must select a valid certificate before you can continue.

Step 6 (Optional) Enter a passphrase in the **Passphrase** field.
Note A passphrase is required to decrypt PKCS12 archives or an encrypted private key (if uploaded .pem files contain the private key).

Step 7 Select **Continue**.
Your system imports your SSL certificate and displays it in a scrollable certificate file dialog box.

Step 8 Select **Turn On Maintenance Mode** and **Continue** to confirm.

Step 9 Select **Continue** on the **SSL Certificate** page to complete the import.

Step 10 Select **Done**.

Step 11 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Exporting a SSL Certificate

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **Certificates** > **More Options** > **Export SSL Certificate**.

Step 3 Save the certificate file.

What to Do Next

Ensure that both administrators and end users are able to sign in to the administration or web pages without seeing any site not trusted browser warnings.

Downloading Your CSR and Private Key

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **More Options** > **Download CSR**.
A dialog box appears asking you to save the file, CSR.zip, which contains the CSR and private key.

Step 3 Select a location on your system to save the file and select **OK**.

Step 4 Back up your private key file, csr-private-key.pem, in the event that you need it later.

Generating a Self-Signed Certificate

A self signed certificate is automatically generated after you deploy your system. We recommend that you install a certificate that is signed by a certificate authority. You can generate a new self-signed certificate at any time by using this feature.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Turn On Maintenance Mode** and **Continue** to confirm.

Step 3 Select **Settings** > **Security** > **Certificates** > **More Options** > **Generate self-signed certificate**.

Step 4 Complete the fields on the **General Self Signed Certificate** page.

Option	Description
Certificate Name	Enter a name for your self signed certificate. (Required)

Option	Description
X.509 Subject Name	The hostname of your system. (Not configurable)
Organization	Enter your organization name.
Department	Enter your department name.
City	Enter your city name.
State/Province	Enter the name of your state or province.
Country	Select your country name.

Step 5 Select **Generate Certificate and Private Key**.
Your certificate file is generated and displayed.

Step 6 Select **Done**.

Step 7 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Importing SSO IdP Certificates

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **SSO IdP Certificate**.

Step 3 Select **Browse** and choose your SSO IdP certificate.

Step 4 Select **Upload**.
Your certificate file is displayed.

Step 5 Select **Done** to submit your certificate.

Importing Secure Teleconferencing Certificates

Secure teleconferencing certificates are only required if TLS conferencing is enabled. If TLS conferencing is not enabled, this option is not available.

Before You Begin

Secure teleconferencing certificates are required for your CUCM servers when TLS is selected as the transport type in your audio settings. See About Configuring Your Audio Settings, on page 5 for more information.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **Certificates**.
The Secure Teleconferencing Certificate section displays one of the following two messages:

- This system does not require secure teleconferencing certificates because TLS teleconferencing is not enabled.
- CUCM secure conferencing certificates are required for TLS teleconferencing which is enabled on this system.

If secure teleconferencing certificates are required, an **Import Certificate** button is shown for each CUCM server that must be configured.

Step 3 Select **Turn On Maintenance Mode** and **Continue** to confirm.

Step 4 Select **Import Certificate** for CUCM 1.
The **Secure Teleconferencing Certificate** page appears.

Step 5 Enter a certificate name.

Step 6 Select **Browse** and choose your certificate file.

Step 7 Select **Upload**.
After you select **Upload**, the system will determine if your certificate is valid.

If the certificate is valid, proceed to the next step. If the certificate is invalid, you cannot upload it. You must select a valid certificate before you can continue.

Step 8 Select **Continue**.
Your system imports your SSL certificate and displays it in a scrollable certificate file dialog box. You are notified that you have imported an SSL certificate.

Step 9 Select **Continue** on the **Secure Teleconferencing Certificate** page to complete the import.

Step 10 Select **Done**.

Step 11 Return to step 4 and repeat the process for your CUCM 2 server.

Step 12 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Configuring User Session Security

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **User Sessions**.

Step 3 Complete the fields on the **User Sessions** page to set the web page expiration time.

Option	Description
Web page expiration	Configure days, hours, and minutes before users are automatically signed out. **Default**: One hour and 30 minutes.
Mobile or Productivity Tools expiration (SSO)	Configure days, hours, and minutes before users are automatically signed out. **Default**: 14 days **Note** This field only appears if SSO is configured.

Step 4 Select **Save**.

Configuring Federated Single Sign-On (SSO) Settings

Configuring SSO enables your end-users to sign into the system using their corporate credentials, thereby giving you a way to integrate the product with your corporate directory. You may also configure SSO to create or manage user accounts on the fly when users attempt to sign in.

Note Configuring SSO can be a complex operation and we strongly recommend that you contact your Cisco Channel Partner or Cisco Advanced Services before you continue.

Before You Begin

- Before you enable the federated single sign-on feature, you must generate a set of public and private keys and an X.509 certificate that contains the public key. Once you have a public key or certificate, you must upload it in the Managing Certificates, on page 18 section.

Note After you have enabled SSO, user credentials are managed by your corporate authentication system. Certain password management features no longer apply to your users. See Configuring Passwords, on page 11 and Editing Users for more information. Note that even though administrators are also end users, administrators do not sign in using SSO. They sign in using their administrator credentials for this product.

- Configure a SSO IdP certificate to use this feature. See Importing SSO IdP Certificates, on page 23 for more information.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **Federated SSO**.

Step 3 After you have generated public and private keys and an X.509 certificate, as described in the pre-requisites, select **Continue**.

Step 4 Select your initiation method:

- SP (Service Provider) Initiated–Users select a link to the service provider and are temporarily redirected to the identity provider for authentication. Users are then returned to the link they initially requested.
- IdP (Identity Provider) Initiated–Users start at their identity provider, log in, and are then redirected to a landing page at the service provider.

Step 5 Complete the fields and select your options on the **SSO Configuration** page:

Note Refer to your IdP configuration file to complete the IdP fields. Select the **IdP Certificate** link.

Field	Description
SP (Service Provider) Initiated	Select this option for service provider initiated sign in.
AuthnRequest signed	Select this option to require that the AuthnRequest message must be signed by the service provider's private key. **Note** You must select this option if you want your exported SAML metadata file to include your site's SSL certificate.
Destination	The SAML 2.0 implementation URL of IdP that receives authentication requests for processing. **Note** This field appears only when **AuthnRequest signed** is selected.
IdP (Identity Provider) Initiated	Select this option for identity provider initiated sign in.

Field	Description
Target page URL parameter name	Your system redirects to this URL when SSO is successful. **Default**: TARGET **Note** On an IdP-initiated system, the URL must be a combined URL in the following format: your service login URL, "?" or "&," the target page URL parameter, "=" (if it is not present), and the target URL.
SAML issuer (SP ID)	Enter the same SP ID configured for IdP. Reference the SAML2 protocol.
Issuer for SAML (IdP ID)	Enter the same ID configured for IdP. Reference the SAML2 protocol.
Customer SSO service login URL	The assertion consumption URL for SAML2 in IdP.
NameID format	Select the same NameID format that you set in IdP. The NameID is the format in which you send the user ID in the assertion and single logout request from Cisco WebEx. See the SAML protocol for guidance. We recommend that you set the email address as your NameID. Doing so will make the process of using SSO easy for end users who have already set up their accounts based on their email address on the system. Using other NameID formats is supported but not recommended. Using an alternative NameID format might cause a non-SSO user to no longer access his previously created account before you configured the system for SSO. **Default**: Unspecified
AuthnContextClassRef	Enter the value that is configured in IdP. AuthnContextClassRef is the value that appears in the AuthnRequest message. **Default**: urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
Default Webex target page URL	Your system redirects to this URL when SSO is successful. The default page is the Cisco WebEx meeting page which is the same as a normal login.
Customer SSO error URL	Your system redirects to this URL when SSO is not successful. By default, the error page is a common Cisco WebEx error page.

Field	Description
Single logout	This option enables single logout which is defined by the SAML2 protocol. If you have chosen the SSO option but not the single logout option, the sign out option does not appear on end-user pages. Deselect this option for ADFS 2.0. **Note** IdP-Initiated SLO is not supported in this version.
Customer SSO service logout URL **Note** This option appears only when Single logout is selected.	Enter the assertion consumption URL for SAML2 in IdP.
Auto account creation	Users without a Cisco WebEx account are unable to sign in. If you select this option, an account is automatically created for new users when they attempt to sign in.
Auto account update	If you select this option, user information is updated when there is an "updateTimeStamp" in the SAML2 assertion with more recent user information than the current data in Cisco WebEx.
Remove UID domain suffix for Active Directory UPN	Select this option to authenticate users without a domain suffix. The **Remove UID domain suffix for Active Directory UPN** option works in the following cases: • The NameId format is email, and UID format is the X509 subject name or User Principal Name (UPN). • The NameId format is the X509 subject name or UPN.

Step 6 Select **Enable SSO**.
The **Review SSO Settings** page appears. Review your settings and select **Save**.

Disabling SSO

Before You Begin

Disabling SSO will disable your users' ability to sign in with their company credentials. Make sure you inform your users that you are disabling SSO and that they can still sign in with their Cisco WebEx credentials.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **Federated SSO**.

Step 3 Find the sentence, "If you would like to disable SSO please click here." Select the **click here** link.

Step 4 Select **Disable SSO** to confirm.
The **Federated SSO** page appears with a banner that confirms you have disabled SSO.

Configuring Your Cloud Features

You can configure your system so that your users can use a single version of the Cisco WebEx Productivity Tools that can be used with both their Cisco WebEx Meetings Server and SaaS WebEx accounts.

Note Your system supports Cisco WebEx SaaS releases WBS27, WBS28, and Cisco WebEx Meetings 1.2.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **Cloud Features**.

Step 3 (Optional) Select the **Enable users to sign in to SaaS WebEx accounts from WebEx Productivity Tools** check box.

Step 4 (Optional) Select the **Enable users to view training videos hosted online by Cisco WebEx** check box.

Step 5 Select **Save**.

Configuring Virtual Machine Security

Your virtual machine security features include the ability to update your encryption keys and enable or disable FIPS-compliant encryption.

Updating Your Encryption Keys

Cisco WebEx Meetings Server uses internally generated encryption keys to secure all communications between the virtual machines on your system. Use this feature to update your encryption keys periodically.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **Virtual Machines**.

Step 3 Select **Turn On Maintenance Mode** and **Continue** to confirm.

Step 4 Select **Update Encryption Keys**.

Step 5 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

About FIPS

The Federal Information Processing Standard (FIPS) provides greater security for your system. Enabling FIPS results in reduced compatibility with popular web-browsers and operating systems (including problems signing into the system, 404 errors, and starting and joining meetings) unless you take the following actions:

- Ensure that your Windows PCs are running at least Windows XP SP3 or above.
- Update all Windows computers to Microsoft Internet Explorer 8 or above regardless of whether your users' desired web browser is Internet Explorer, Mozilla Firefox, or Google Chrome. Your users must provide Internet Explorer 8 on all computers because our FIPS-enabled clients (Cisco WebEx Meetings, Productivity Tools, and WebEx Recording Player) use FIPS-enabled system libraries that are only available on Internet Explorer 8 and above.
- Configure **Internet settings** on all user computers to TLS encryption:
  - On your PC desktop, select **Control Panel** > **Internet Options** > **Advanced** > **Security** > **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2**. We recommend selecting all three options for maximum compatibility but you must at least select **Use TLS 1.0**.
  - On your PC desktop, select **Control Panel** > **Internet Options** > **Advanced** > **Security** > **Use SSL 3.0**. We recommend selecting this option for maximum compatibility.
- If your users plan to host meetings for guests (for example, people who do not work for your company) you must inform your guest users to manually update their operating systems and browsers as described above before they join your meetings. If they do not perform the above steps, they will experience compatibility issues. We recommend that you include the above instructions in your meeting invitations. You can do this by editing the appropriate meeting invitations available on your Administration site at **Settings** > **Email** > **Templates.**

Enabling FIPS Compliant Encryption

Use this feature to enable your Federal Information Processing Standard (FIPS) compliant encryption setting.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **Virtual Machines**.

Step 3 Select **Turn On Maintenance Mode** and **Continue** to confirm.

Step 4 Select **Enable** to enable FIPS compliant encryption and **Continue** to confirm.
FIPS compliant encryption is configured on your system.

Step 5 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Disabling FIPS Compliant Encryption

Use this feature to disable Federal Information Processing Standard (FIPS) compliant encryption on your system.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Settings** > **Security** > **Virtual Machines**.

Step 3 Select **Turn On Maintenance Mode** and **Continue** to confirm.

Step 4 Select **Disable** to disable FIPS compliant encryption and **Continue** to confirm.
FIPS compliant encryption is disabled on your system.

Step 5 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.