Configuring Settings

Configuring Company Information

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 (Optional) To change the Language setting, select **Turn On Maintenance Mode**.
You do not have to turn on maintenance mode when modifying the other settings on the **Company Info** page.

If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 Select **Settings**. If you are viewing one of the other settings pages, you can also select **Company Information** under the Settings section.

Step 4 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: • Sign-in page seen by administrators when they activate their administrator accounts for the first time • Language of reports. (See Managing Reports
Locale	Your locale. The locale setting affects the display of times, dates, currency, and numbers.

Step 5 (Optional) If you changed the language, select **Turn Off Maintenance Mode** and **Continue** to confirm.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Configuring the General Branding Settings

Before You Begin

Prepare the following before configuring general branding:

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

Important When customizing your site, make the necessary updates to each section and then select **Save** only after all branding changes are complete. Saving updates one section at a time might cancel some of your changes.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

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

Option	Description
Logo	The logo must be in PNG, JPEG, or GIF format. The maximum dimensions are 120x32 pixels and the maximum file size is 5 MB. The logo appears to the right of banner on the WebEx site. The Cisco logo appears in the bottom right corner of the page.
Privacy Statement	URL to your company privacy statement.
Terms of Service	URL to your company terms of service.
Custom Footer Text	The text you enter is displayed in the footer of all end-user and administrator web pages and emails that are sent by your system.
Header Background Color	Select this option to turn off the default background color, including all browser bars and emails.
Online Help	Select the online help option that applies to your environment. If users are prevented from accessing the Internet, select the customized help option and enter the URLs to your company videos, user guides, and FAQs.

Option	Description
Support Contact URL	URL to your company support web page.

Removing a Company Logo

Before You Begin

Create a transparent 120x32 PNG or GIF file.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 For the Company Logo field, select **Browse** and choose the 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 Meeting Settings

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

- **Join meeting settings**
- **Maximum number of Web participants per meeting**
- **Participant privileges**

The configuration of the meeting size does not limit the number of call-in, audio-only participants. If the meeting size limit is 2, only 2 attendees can join by using the Web, VoIP, or call-out options. However, more attendees can join the meeting on an audio-only basis up to the capacity of the system. See Confirming the Size of Your System.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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** lets participants join meetings up to 15 minutes before the starting time.
- **Allow participants to join teleconference before host** lets participants participating by teleconference join meetings up to 15 minutes before the starting time.
- **First participant to join will be the presenter** makes the first participant to join the meeting presenter. If you uncheck **Allow participants to join meetings before host**, the **First participant to join will be the presenter** feature is automatically unchecked.
- Optionally, **Anyone can present in the meeting** allows anyone to take the Presenter ball.
- Optionally, **Send a meeting report summary to the host** that provides:
  - Host—Meeting hostname.
  - Meeting Number—Cisco WebEx meeting number.
  - Topic—Name of the meeting configured by the host.
  - Start Time—Starting time and date of the meeting.
  - End Time—Ending time and date of the meeting.
  - Invitees—Identification of people invited to the meeting.
  - Participants—Identification of those who participated in the meeting including hosts.
  - Call-in numbers—Dial-in audio numbers.

Step 4 Select the maximum participants per meeting by dragging the slider:

Maximum Number of Participants	System Size
50	50 user system (single data center)
250	250 user system (single data center) 250 user system (multi-data center)
500	800 or 2000 user system (single data center) 800 or 2000 user system (multi-data center) [1]
?	

[1] Support for meetings with 500 participants depends on system loading conditions.

Step 5 In the **Participant privileges** section, select your options.

Option	Description
Chat	If selected, hosts can make the chat feature available to meeting participants.
Polling	If selected, hosts can create polling question areas, where participants can answer multiple choice or short answer questions, and then submit the results.
Document review and presentation	If selected, hosts can make the File Sharing feature available to meeting participants.
Sharing and Remote Control	If selected, hosts can share applications, web browsers, video, and other files, or share their desktop screen. With remote control, hosts can allow participants to control shared applications, documents, or files.

Chat, **Polling**, **Document review and presentation**, and **Sharing and Remote Control** are selected by default. The selected participant privileges appear in the users' controls.

Step 6 Select **Record** to record and store meetings on the storage server.

a) Select **Send notification email to host and attendees when the meeting recording is ready** to enable email notifications. If enabled, the system sends an email to the host and to anyone else who received a meeting invitation.

b) Select **Restrict viewing and downloading of recording to signed in users** to allow only system users, not guests, to view or download a meeting recording.

Recording is disabled by default. Also, you must configure a storage server to enable recording. See Adding an NFS or SSH Storage Server for more information.

Step 7 Select **File transfer** to allow users to share files during a meeting.

Step 8 Select **Save**.

About Meeting Security

Cisco WebEx Meetings Server enables different meeting security features depending on the following factors:

- User type: host, alternate host, user (signed in), and guest.
- Meeting has a password or no password.
- Password is hidden or visible in the meeting invitation.
- Password is hidden or visible in the email meeting invitation.
- Behavior displayed on the meeting join page (see the following tables).

Table 1: Password is Excluded When Scheduling Your Meeting

User Type	Password Displayed in Email Invitation and Reminder	Meeting Detail Page
Host	Yes	Yes

User Type	Password Displayed in Email Invitation and Reminder	Meeting Detail Page
Alternate host	Yes	Yes
Invitee	No	No
Forwarded invitee	No	No

Table 2: Password is Included When Scheduling Your Meeting

User Type	Password Displayed in Email Invitation and Reminder	Meeting Detail Page
Host	Yes	Yes
Alternate host	Yes	Yes
Invitee	Yes	Yes
Forwarded invitee	Yes	Yes

- Join Before Host feature is on or off:
  - On: Invitees or guests can join the meeting from 15 minutes before the start time to the end of the meeting time.
  - Off: Invitees or guests cannot join the meeting before host. The host or alternate host can start the meeting, then the invitees can join.
- Join Teleconference before Host feature is on or off:
  - On: If the host does not start the teleconference in the meeting client, then invitees can join the teleconference before the host.
  - Off: If the host does not start the teleconference in the meeting client, then invitees cannot join the teleconference before the host.
- First participant can Present feature is on or off:
  - On: When Join before host is configured, the first participant is the presenter.
  - Off: The host always has the ball.

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.

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:

- A list of call-in access numbers that your participants use to call into meetings.
- The CUCM IP address.
- (Optional) A valid, secure conferencing certificate if you plan to use TLS/SRTP teleconferencing encryption. See Importing Secure Teleconferencing Certificates, on page 63 for more information.

Note This feature is not available in Russia or Turkey.

Configuring Your Audio Settings for the First Time

The first time you configure your audio settings, a wizard guides you through the installation procedure. You must configure Cisco Unified Communications Manager (CUCM) as part of this process.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off.
If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 Select **Settings** > **Audio** > **CUCM on Data Center One/Two**.
The **CUCM Setting** page appears.

Step 4 (Optional) Select **Edit** to modify the CUCM IP addresses.

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

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

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

a) Enter an IP address for the CUCM 1 IP address and optionally for the CUCM 2 IP address.
These IP addresses must correspond to the primary and optionally secondary CUCM node that are part of the Cisco Unified Communications Manager Group, as set on the device pool that is configured on the Application Point SIP Trunks in CUCM. See "Configuring a SIP Trunk for an Application Point" in the *Planning Guide* at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html for more details.

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 numbers assigned in CUCM. (**Default:** 5060 and 5062)

c) Use the **Transport** drop-down menu to select the transport type for your system. (**Default:** TCP)
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 the system fully qualified domain name (FQDN) as the SIP domain name on each CUCM server. See Importing Secure Teleconferencing Certificates, on page 63 for more information about importing your certificates, and "Configuring Cisco Unified Communications Manager (CUCM)" in the *Planning Guide* for more information about managing call control 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.
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.
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). Select this option to bypass the requirement to press **1** to connect to a meeting.

Note We do not recommend that you select 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 supported and 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.)

Step 18 Select the **System Audio Language** users hear when they dial in to the audio portion of a WebEx meeting or when they use the Call Me service.

Step 19 Select **Save**.

Step 20 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

Modifying Audio Settings

Before You Begin

If you are configuring your audio settings for the first time, see Configuring Your Audio Settings for the First Time, on page 8.

Note Turning on Maintenance Mode is not required to configure or change the Blast Dial, Call-in Service Languages, Display Name, or Caller ID audio settings.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off.
If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 Select **Settings** > **Audio**.

Step 4 Select **Global Settings**. Configure your audio feature settings.
For audio configuration, there are global settings and each data center has local settings. Global settings are applied to all data centers. *Local* settings apply to individual data centers.

Option	Description
WebEx Audio	• 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. A meeting host cannot start a Blast Dial meeting. • Off—Disables all calling features. A meeting host cannot start a WebEx audio, Blast Dial, or Personal Conference meeting.
Personal Conferencing	• Select the **Enable Personal Conferencing** check box to allow users to start and dial in to personal conference meetings. • Select **Allow participants to join Personal Conference meetings before host** to allow participants to start the audio portion of a Personal Conference meeting by entering only the participant access code; no host PIN is required.
Voice connection using computer	• **On** allows a computer voice connection. • **Off** denies a computer voice connection.

Step 5 Configure Blast Dial as described in About WebEx Blast Dial, on page 13.

Step 6 Select **Edit** in Call-In Access Numbers section 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. To delete a number, select the **Delete** link at the end of the line.
b) Enter updated information in the phone label and phone number fields for any access number you want to change.
c) Select **Continue**.
Your changes are not saved until you select **Save** on the previous page.

Make sure that 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 Select **Edit** in the Call-in Service Languages section to add, change, or delete languages available for users calling in to the audio portion of a meeting.

a) Select **Add** and enter a route pattern associated with each call-in number you want to provide language choices to users calling in to the audio portion of a meeting.
All users who call the call-in numbers associated with the route pattern can choose from the configured language selections. For example, if you configure English, Spanish, and French as the language selections, when a user calls the call-in number associated with the route pattern, the caller hears the greeting in English but is given the choice to select either Spanish or French. If a user selects Spanish, the initial audio prompts are spoken in Spanish.

Note The default language is set to the language configured for **Settings** > **Audio** > **Global Settings** > **System Audio Language**.

b) To delete an entry, select **X** at the end of the line.
c) To change an entry, type a different route pattern and select different language settings.
d) Select **Continue**.
Your changes are not saved until you select **Save** at the bottom of the page.

Make sure you only add route patterns that have been configured in CUCM.

Step 8 Use the **Transport** drop-down list to select the transport type for your system and port number for each server. (**Default:** TCP)
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, upload it into CUCM, and configure your system fully qualified domain name (FQDN) as the SIP domain name on each CUCM server. See Importing Secure Teleconferencing Certificates, on page 63 for more information about importing your certificates, and "Configuring Cisco Unified Communications Manager (CUCM)" in the *Planning Guide* for more information about managing call control on CUCM.

Make sure the port number matches the setting in CUCM.

Step 9 Enter a display name in the **Display Name** dialog box.
This is the name displayed on a meeting participant's IP phone when using the Call Me service or calling into Cisco WebEx Meeting Server (CWMS).

Step 10 Enter a valid caller ID in the **Caller ID** dialog box.
The caller ID is limited to numerical characters and dashes (-), and has a maximum length of 32 characters.

Step 11 Configure your WebEx Call Me setting (**Default**: Press 1 to connect to meeting). Optionally select this option to bypass the requirement to press **1** to connect to a meeting.
We do not recommend that you select this option unless your phone system is incapable of sending a **1** digit.

Step 12 Select your **Telephone entry and exit tone**.

- Beep (default)
- No tone
- Announce name

Step 13 If IPv6 is supported and configured on your system, set your **IPv6 Teleconferencing** setting to **On** or **Off**. (**Default**: **Off** indicates that IPv4 is the setting.)

Step 14 Select **Show call-in user phone numbers in Participant Report** to display user phone numbers in the report.
To include all phone numbers in a Multi-data Center environment, this parameter must be set on each data center.

Step 15 Select the **System Audio Language** users hear when they dial in to the audio portion of a Cisco WebEx meeting or when they use the Call Me service.
This setting appears as the default language for the Call-in Service Languages.

Step 16 Select **Save**.

Step 17 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

Editing Audio CUCM

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off.
If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 Select **Settings** > **Audio** > **CUCM Data Center**.

Step 4 Select **Edit** CUCM (Cisco Unified Communications Manager) to change the settings.

a) In **CUCM 1 IP Address**, enter the IP address for your CUCM 1 system.
b) (Optional) Enter the IP address for your CUCM 2 (load balancing service) system.
CUCM 2 is not required, but we recommend that you include this parameter for teleconferencing high availability.

Step 5 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

About WebEx Blast Dial

Cisco WebEx Blast Dial lets users identified as meeting hosts, call a phone number and enter a host PIN (if necessary) to instantly start the audio portion of a meeting. At the same time, the system automatically places calls to a list of participants defined for that Blast Dial group.

Within minutes, the host can begin discussing an urgent matter or provide detailed instructions for handling an important issue with the people who have approval authority or are trained for emergency situations. In addition to starting the audio portion of the meeting, the host can access an automatically generated email to start the online portion of the meeting to share images, video, or electronic information with the meeting participants.

The calls are initiated in a block, depending on the size of the system. A 50-user system initates 3 calls. A 250-user system initates 15 calls. An 800-user system initates 48 calls. A 2000-user system initates 40 calls. The delay is by design. It prevents dialing out to a large number of users at the same time to avoid affecting normal system operations.

When a call in the initial block is answered or times out, the system calls the next participant. This continues until all participants have been contacted. For example, if the system is configured for 3 attempts, the system

does not initiate the 4th call; it calls the next participant. Each call attempt lasts 20 seconds. (See Editing Blast Dial Group Settings, on page 17 for information on setting the number of call retries.)

When the system calls a person on a participants list, that person answers the call and enters a participant PIN (if necessary) to join the audio portion of the meeting. Once the audio portion of the meeting is in progress, a host can press *# to hear the names of the people who have joined the meeting. (The host can also look at the Participants list in the online portion of the meeting.) Any participant can choose not to answer the call or remove themselves from a Blast Dial group. An administrator can delete a person from a Blast Dial group at any time.

Each Blast Dial group can have the maximum number of participants supported by each size CWMS system (see the "System Capacity Matrix" section in the *Cisco WebEx Meetings Server Planning Guide and System Requirements* for details). An administrator configures the Blast Dial group and its participants, but relies on the meeting host to provide the group settings and the information for the Participants list. An administrator can add participants to a Blast Dial group by entering them manually on the Blast Dial page, or by importing a ParticipantsTemplate file completed by a host.

Downloading the Group Template

Use the link provided to download a Group Template to send to the person who will host meetings for a Blast Dial group.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 Select the **GroupTemplate** link to download the template a host uses to provide the general settings, such as group name and host PIN, for the new Blast Dial group.

Step 4 Email the Group Template to the host of the Blast Dial group. Ask the host to complete the template and return it to you.

What to Do Next

If you have the information to create a new group, go to Adding a Blast Dial Group, on page 14.

To import participants, delete the instructions and rows with example text in the Participants template file and go to Importing a Participants List, on page 20.

To manually add participants for a group, go to Adding Blast Dial Participants, on page 17.

Adding a Blast Dial Group

For each Blast Dial group, specify a group name, a route pattern, and a call-in number. Both the route pattern and the call-in number must be defined in CUCM and copied into the Blast Dial page. To provide a level of security for the meetings, configure a host PIN and a participant PIN. For each group, select the **Host** check box for at least one of the internal participants to make that user a host. There must be at least one host for each Blast Dial group. You can designate several internal participants as hosts for a Blast Dial group and all hosts can start the audio portion of a Blast Dial meeting. However, a meeting host requires a license to start the online portion of a Blast Dial meeting.

Note

When the Blast Dial group is configured, the system sends an email to the host with the host PIN and Call-in number. All participants receive an email with the participant PIN and Call-in number. A host calls the Call-in number and enters a host PIN to start a meeting. Participants answer the Blast Dial call (or call the call-in number if they miss the call) and enter a participant PIN (if required). Unlike other types of Cisco WebEx meetings that automatically end after 24 hours, a Blast Dial meeting continues until the last person ends his or her call or leaves the online portion of the meeting. When there is only one person in the meeting, a warning message appears every 15 minutes, "You are the only participant in this meeting. The meeting will automatically end in:". The clock decrements from 2 to 0 minutes. The user can select **Continue** to extend the meeting.

Note When a host starts the online portion of a Blast Dial meeting, DTMF tones are disabled.

Before You Begin

Configure a route pattern and corresponding call-in number in the Cisco Unified Communications Manager for every Blast Dial group. Each Blast Dial group requires its own dedicated call-in number. See "Call Routing Setup" in the *Cisco Unified Communications Manager Administration Guide* for details about route patterns.

Download the **Group Template** file and send it to the host of the Blast Dial group. The host should complete the template and return it. Use the information in the template to create the Blast Dial group.

When you create a Blast Dial Group you have an option to upload a Custom Greeting in the form of a .WAV file. All custom audio prompts, including Blast Dial prompts, are 8KHz, 16-bit, 64kbps, momo, CCITT u-law (G.711).

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 In the Blast Dial section, select **Add Group**.

Step 4 Enter a **Group Name**.

Step 5 Type a **Route Pattern**.
One route pattern must be configured in Cisco Unified Communications Manager for each Blast Dial group.

Step 6 Type the **Call-in Number** associated with the route pattern configured for this Blast Dial group.
Each Blast Dial group needs a dedicated call-in number. A host dials the call-in number to initiate a Blast Dial meeting.

Note This call-in number must be redirected to the route pattern selected for this group in the Cisco Unified Communications Manager. See http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for details.

Step 7 (Optional) Type an alphanumeric password in the **Meeting Password** field.
If configured, participants enter this password to join the online portion of a Blast Dial meeting.

Note The rules that govern the meeting password are set in **Settings** > **Password Management** > **Meeting Password**. See Configuring Meeting Settings, on page 4 for details.

Step 8 Choose one of the **Host PIN** options:

- (Default) Select **Automatically generate a host PIN** and move the slider to the desired security level. As you move the slider, the PIN and security level changes. Select **Refresh** to generate another number.
- Select **Type a host PIN** and type a numeric PIN. When this option is selected, a PIN is required.

  A 3-digit PIN has low security, a 4-digit to 7-digit PIN has medium security, and an 8-digit to 10-digit PIN has a high level of security.

  Note A host PIN cannot be a single-number or sequential-number sequence, such as 11111 or 1234567.

- Select **None** if you do not want to require a host to enter a PIN to start a Blast Dial meeting.

  Note When this option is selected, any user who knows the call-in number can initiate a Blast Dial meeting.

Step 9 Choose one of the **Participant PIN** options:

- (Default) Select **None** if you do not want to require a participant to enter a PIN to join a Blast Dial meeting.
- Select **Type a participant PIN** and type a numeric PIN. When this option is selected, a PIN is required.

  A 3-digit PIN has low security, a 4-digit to 7-digit PIN has medium security, and an 8-digit to 10-digit PIN has a high level of security.

  Note A participant PIN cannot be a single-number or sequential-number sequence, such as 11111 or 1234567.

Step 10 Select the number of **Call Attempts** the system should make to call a participant.
The system calls each participant the number of times selected for Call Attempts. If a user lists four phone numbers on their **My Accounts** page (for internal users) or an administrator enters four phone numbers in the CSV file imported into the system, the system dials the first number the number of times selected for Call Attempts, then calls the second number the number of times selected for Call Attempts, and so on. After the system dials each phone number the number of times selected for Call Attempts, the system stops calling the participant. If **Unlimited** is selected for this field, the system continues to call the participants until they answer the call or until the Blast Dial meeting ends.

- 1 (The system calls each participant one time.)
- 3 (default)
- 5
- 10
- Unlimited (Select this option when company policy dictates that the system continues to call participants until they join the meeting.)

Step 11 Select the **Add Participants** link in the **Internal List** section.

Step 12 In the **Internal List**, enter an email address for at least one host and select + to add each person to the Participants list.

Step 13 Select the **Host** check box to designate the internal user as a meeting host.

Step 14 (Optional) Select the **Add Participants** link in the **External List** section.

Step 15 (Optional) For external users, enter a name, email address, and a phone number, and then select **Add** to add the person to the Participants list. See Adding Blast Dial Participants, on page 17 for details about external users.

Step 16 Select **Save** to save your changes.
The Blast Dial group is added to the system.

What to Do Next

To import a list of participants, export a CSV file with pre-configured column headings. See Exporting a Participants List, on page 19 and Importing a Participants List, on page 20 for details.

To create a small blast dial list or to add a few new people to an existing list, see Adding Blast Dial Participants, on page 17.

To delete a blast dial group, see Deleting a Blast Dial Group, on page 17.

Editing Blast Dial Group Settings

You can change the blast dial group settings, including the participants list.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 In the Blast Dial section, select a **Group Name**.

Step 4 Change the editable fields. Fields marked with an asterisk are required.

Step 5 To make changes to an entry in the participants list, select **X** to delete an entry, and then add the entry again with the updated data.

Step 6 Select **Update** to save the changes.

Deleting a Blast Dial Group

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 In the Blast Dial section, select **X** next to the group you want to delete.

Step 4 Select **OK** to confirm.
The Blast Dial group and related participants lists are deleted from the system.

Adding Blast Dial Participants

After you configure the settings for a Blast Dial group, create the internal and external Participants list. The system calls the members of the internal and external participants lists when a host initiates a WebEx Blast Dial meeting, dialing the members of the internal list first followed by the members of the external list.

Internal participants' company email addresses are associated with the information on their **My Account** pages. The system uses the internal user's email address to gather a user's name and phone numbers from their **My Account** page. (If the phone number of an internal user is listed in the template, it is ignored.)

If there is more than one number is listed on the **My Account** page, the system dials the first non-empty phone number, typically the participant's office number. If the call is not answered, the system calls the second phone number in the list, such as the mobile number. This is repeated until it reaches the last configured phone at end of list in **My Account** page. The number of cycles depends on the number of call attempts set in Blast dial group on the Administration page. (See Editing Blast Dial Group Settings, on page 17 and "Updating Your Account Information" in the *Cisco WebEx Meetings Server User Guide*.) The default is three call attempts.

External participants can participate in WebEx Blast Dial meetings as guests. However, because they do not have company email addresses and associated **My Account** pages, a name, email address, and a phone number must be entered on the **Blast Dial** dialog for external participants. The system dials the participant phone numbers in consecutive order.

External participants cannot host a WebEx Blast Dial meeting.

To add participants:

- Enter a participant's information in the fields provided in the Internal List or External List sections of the template.
- Or ask the person who will host the Blast Dial meetings to select the **Participants Template** link on their **My Account** page and download the template file. The host enters the participants' information and sends the complete template to an administrator to import into the system.
- Or export a participants list to a CSV file, enter the required information, and import the updated CSV file.

The system checks all participant entries and automatically moves entries between participants lists if an internal user's email address is entered in the external participants list. If the system cannot locate the email address for an entry in the internal participants list in the database, that entry is moved to the external list. To make the relocated entry valid, a user name and phone number must be entered.

Before You Begin

Contact the person who will host the Blast Dial meetings and ask the host to select the **Participants Template** link on the **My Account** page to download a template file. The host should enter the participants' information and send the complete template to an administrator. See "Downloading the Group and Participants Templates" section in the *Cisco WebEx Meetings Server User Guide*.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 In the Blast Dial section, select a **Group Name** link.

Step 4 You can export the existing Participants list, modify the CSV file, and import the file to add or change participant's information.

Note The first time you select **Export List**, the system exports an empty CSV file with the appropriate column headings.

Step 5 To import participants:

- Select **Tab** or **Comma** to indicate which type of CSV file you are importing, tab-delimited or comma-delimited.
- Select **Browse** and then select the CSV file to be imported.
- Select **Import**.

Step 6 To add individual entries in the provided fields:

- For internal participants, type an email address and select + to add the entry.
- For external participants, type a participant's name, an email address, and a phone number including the country code. Then select **Add**.

The newly added participants appear in the Internal List or External List.

Step 7 (Optional) Select the **Host** check box to designate a person as a host.
Note The system requires at least one internal participant to be designated as a host for each blast dial group.

Step 8 Select **Save** to save the blast dial group settings and the newly added entries in the participants list.
A person designated as a host receives an email notification which includes the host PIN, participant PIN, meeting password (if configured), and blast dial call-in number. All other participants receive an email notification which includes the participant PIN and meeting password (if configured).

What to Do Next

To modify an entry in a participants list, see Editing Blast Dial Group Settings, on page 17.

To import a participants list, see Importing a Participants List, on page 20.

To export a participants list, see Exporting a Participants List, on page 19.

Exporting a Participants List

Before you create a participants list, select **Export List** to export a blank CSV file with the proper column headings. Otherwise, the system exports all participant information for this Blast Dial group. The exported list that contains both internal and external participants contains: NAME, EMAIL, PHONENUMBER1, PHONENUMBER2, PHONENUMBER3, PHONENUMBER4, and ISHOST.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 Select a **Group Name** in the Blast Dial section.

Step 4 Select **Export List** in the Participants section.
The participant data is exported as a CSV file.

Step 5 On the export dialog, select to open the file with a specific application or save the file and download it.

Step 6 Access the exported CSV file and add, change, or delete participant data.

For external participants, the system requires a **name**, **email address**, and one **phone number**. For internal participants, the system requires only a user's company **email address**. At least one internal user must be assigned a host role.

Note If you enter participant information that is not required, for example a name for an internal user, the system does not save this information when the CSV file is imported. However, if information is incomplete, for example you forgot to enter a name for an external participant, the system imports the information but displays an error message. Incorrect entries are considered invalid and are not saved to the database.

- **Name** (required for external participants)—Enter a person's first and last name in any format desired. All symbols are allowed, but < and > are not recommend. This name appears in the External List and in email messages the system sends to participants with information about joining a Blast Dial meeting. If the name is too long for an External List, it is truncated. (Names in emails are never truncated.) For internal users, the name is retrieved from the user's WebEx **My Account** page.
- **Email** (required for all participants)—The system uses this address to send PIN and call-in information, send links to the online portion of a Blast Dial meeting, and to determine if a person is an internal or external participant. If an email address is stored on the Cisco WebEx Meetings Server, the person is an internal participant and the system automatically detects the name and phone information from the user's WebEx **My Account** page. If the email address is external, the system uses the name and phone numbers entered in the CSV file.
- **Phone Number** (required for external participants)—Enter up to four phone numbers, including the country code, for external participants. The system dials the phone numbers in order, meaning Phonenumber1, then Phonenumber2, and so on. Enter at least one phone number for each external participant. The characters: 0~9, (,), - are allowed. The CWMS system does not identify, verify format, or convert the phone number; it just forwards the entry to CUCM.
- **Role** (for internal participants only)—Enter **host** for all internal user who will be meeting hosts. Hosts receive an email with the host PIN, participant PIN, and call-in number. More that one person can be designated as a host.

What to Do Next

Go to Importing a Participants List, on page 20.

Importing a Participants List

Before You Begin

Prepare a comma-delimited or tab-delimited (CSV) file containing the participant information. You can export the current participant list values to a CSV file, modify the file, and import it to add or change participant information.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 Select a **Group Name** in the Blast Dial section.

Step 4 Select **Tab** or **Comma** to indicate the type of CSV file you are importing.

Step 5 Select **Browse** and then select the CSV file to be imported.

Step 6 Select **Import**.
The file is imported to the system.

Step 7 Select **Update** to save the participant information.
The imported participants' information is saved to the database.

What to Do Next

Scroll through the participants lists to view the participants' information and verify that the values were imported correctly.

Go to Exporting a Participants List, on page 19 to export a participants list.

Configuring Video Settings

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 Select **360p**, **180p** or **Off** and then select **Save**.
Refer to the "About Meeting Recordings" section of the CWMS Planning Guide for approximate storage requirements.

Configuring Your Mobile Device Settings

If your system is configured to permit more than one call-in access number, the system assumes that the first number is a toll-free access number and attempts this number first. The application does not connect if this number is not reachable from the mobile network. Make sure that this number is accessible from the mobile network.

When using an iOS mobile device and the data center certificates are not from a well-known certificate authority, it is necessary to import both data center SSL certificates into the iOS mobile device. Otherwise, iOS mobile device displays an error when trying to launch a meeting.

We recommend that Android mobile device users import both data center certificates before attempting to launch a meeting. After importing certificates into the Android device, the device shall trust the WebEx sites and does not show a warning message when starting a meeting from this site.

Note Android is supported in Cisco WebEx Meetings Server 2.0 and higher. Both the iOS and Android WebEx applications are enabled by default.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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 and Android WebEx applications.

The iOS and Android WebEx applications work the same as the Cisco WebEx desktop application; from an internal intranet or external Internet.

What to Do Next

For Cisco WebEx Meetings Server Release 2.0 and later, see Exporting an SSL Certificate for Mobile Devices, on page 58 for information about exporting certificates to email to your mobile device users.

Related Topics

Configuring Your Audio Settings, on page 7

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.

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**

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

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

About QoS Marking

See the tables below for QoS marking information to deployments that have traffic going through an Internet Reverse Proxy server versus a deployment in which no traffic is going through an Internet Reverse Proxy server.

QoS Marking on Cisco WebEx Meetings Server Systems With Traffic Moving Through an Internet Reverse Proxy Server

Traffic	QoS Marking
SIP Audio—media—CWMS to Endpoint	Yes
SIP Audio—signalling—CWMS to Endpoint	Yes
PC Audio—media—CWMS to Client	No
PC Audio—signalling—CWMS to Client	No
PC Audio—media—Client to CWMS	No
PC Audio—signalling—Client to CWMS	No
PC Video—media—CWMS to Client	No
PC Video—signalling—CWMS to Client	No
PC Video—media—Client to CWMS	No
PC Video—signalling—Client to CWMS	No

QoS Marking on Cisco WebEx Meetings Server Systems With No Traffic Moving Through an Internet Reverse Proxy Server

Traffic	QoS Marking
SIP Audio—media—CWMS to Endpoint	Yes
SIP Audio—signalling—CWMS to Endpoint	Yes

Traffic	QoS Marking
PC Audio—media—CWMS to Client	Yes
PC Audio—signalling—CWMS to Client	Yes
PC Audio—media—Client to CWMS	No
PC Audio—signalling—Client to CWMS	No
PC Video—media—CWMS to Client	Yes
PC Video—signalling—CWMS to Client	Yes
PC Video—media—Client to CWMS	No
PC Video—signalling—Client to CWMS	No

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—Configures 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—Enforces password usage for meetings and configures 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 or LDAP is enabled on your system:

- The settings on the **General Password** and **User Password** pages and the password security controls on the **Edit User** page do not apply to host account passwords.
- These settings do apply to administrator and auditor passwords when those credentials are used to sign in to a Cisco WebEx Administration site.
- Administrators must use their SSO or LDAP credentials to sign in to and manage meetings they host. (Auditors cannot host meetings.)

General Password Settings

All password settings on this page are optional and can be toggled on (checked) or off (unchecked).

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 Select **Force all users to change password every number day(s)** and enter the number of days in the text field. (**Default**: Unchecked)
Password aging is disabled if users are authenticated by using LDAP.

Step 4 Select **Force all users to change password on next login**. (**Default**: Unchecked)
Forcing password change is disabled if users are authenticated by using LDAP.

Step 5 Select **Enable user account locking**. (**Default**: Unchecked)
To prevent unauthorized access to a system, the system automatically locks an account after a number of failed sign-in attempts. When an account is locked, email with unlock instructions is sent to all administrators and the locked account holder.Administrators can unlock another administrator's locked account (see Unlocking an Account).

More parameters display:

- Number of consecutive sign-in failures [*number*].
- Forget the failed sign-in attempt after [*number*] minutes.
- Remove the lock on the user account after [*number*] minutes.
- Send email notifications to locked users.

Step 6 Select **Save**.

Configuring User Password Requirements and Limitations

These settings apply to both the administrator and the end users when the system uses default authentication. These settings apply only to the administrator when the system uses Lightweight Directory Access Protocol (LDAP) authentication or single sign-on (SSO) authentication; end user passwords are managed by an AD server or an IdP server.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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 character length	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 hostname are always unacceptable	Do not use these specific names. **Default**: Selected
Must not include previous *n* passwords	Do not use previously used passwords. Select a number from the drop-down list to specify the number of previous passwords you cannot use. **Default**: Selected **Default number**: 5

When creating a password, users are advised to not:

- Repeat a character more than three times.
- Use your name, email address, site name, or company name as part of your password.

- Use any of your 5 previous passwords.
- Include a quote mark (") or a space.

Step 4 Select **Save**.

Configuring the Meeting Password Settings

Use this feature to configure meeting password parameters. The table describes when users must enter a password to attend a meeting.

Password Configured	Password Excluded from Email Invitation	Meeting Creator Signed In	Host Signed In	Invitee Signed In	Guest Signed In	Guest Not Signed In
No	n/a	Password is not required.	Password is not required.	Password is not required.	Password is not required.	Password is not required.
Yes	Yes	Password is not required.	Password is not required.	Password is not required.	Password is required.	Password is required.
Yes	No	Password is not required.	Password is not required.	Password is not required.	Password is required and the field is automatically filled.	Password is required.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

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

- **All meetings must have passwords** requires all meetings to have passwords.
- **Meetings password is optional** meeting passwords can be required by the host.
- Require strong passwords for meetings enables the remaining options:
  - **Minimum character length** requires the password to be at least this number of characters. **Default**: 6
  - **Minimum number of alphabetic characters** requires at least this number of alphabetical characters. **Default**: 1
  - **Minimum number of numeric characters** requires at least this number of numeric characters. **Default**: 1

- **Minimum number of special characters** requires at least this number of special characters. **Default**: 1
- **Must not contain these special characters (space, \, ', ", /, &, <, >, =, [,])** prohibits the use of these characters.
- Must include mixed case requires the password must contain uppercase and lowercase alphabetical characters.
- **List of unacceptable passwords** lists illegal passwords.
- **Company name, site name, user email address, hostname, and meeting topic are always unacceptable** prohibits the use of these words or character strings.

Step 4 Select **Save**.
The change is applied to future meetings when they are scheduled; meetings scheduled prior to the parameter changes are not affected.

Configuring Your Email Settings

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

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 Enter your **From Name**, your **From Email Address**, your **Reply-To** email address, and then select **Save**.
The system derives the default **From Name**, **From Email Address**, and **Reply-To** values from the settings that you configure on the **Variables** page. You can enter a person's name in the **From Name** on the **Variables** page, but meeting invitations use the host's email address.

Step 4 Select **Templates**.
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. Update the fields in the **Account Reactivated** dialog box and select **Save**.

About Email Templates

Use the email templates to communicate important events to users. Each email template has variables that you must configure. See the table below for descriptions of the variables in each template.

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 3: Common Email Templates

Title	Description	Variables
AD Activation	Sent to a user after an AD account has been activated.	• %SiteURL% • %DisplayName% • %SSOSignINLink% • %OrgLogo% • %Participants% • %Support% • %CustomFooterText% • %Year%
AD-Sync Failed	Sent to an administrator after a failed synchronization.	• %FullName% • %Failure_Reason% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
AD-Sync Success	Sent to an administrator after a successful synchronization.	• %FullName% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Account Reactivated	Sent to a user after an administrator reactivates the user's account.	• %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Forgot Password–Password Changed	Sent to a user after he has reset his password from the end-user site.	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
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.	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
PT PCN Meeting Invitation—Invitee	Sent to meeting invitees after a meeting is scheduled by using Productivity Tools from a Personal Conference account.	• %HostName% • %Topic% • %TeleconferencingInfo% • %MeetingLink% • %MeetingNumber% • %MeetingPassword% • %MeetingSpace% • %SiteURL% • %Support% • %CustomFooterText%
PT Meeting Invitation—Invitee	Sent to meeting invitees after a meeting is scheduled by using Productivity Tools.	• %MeetingLink% • %HostName% • %Topic% • %TeleconferencingInfo% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support% • %CustomFooterText%

Title	Description	Variables
Recording Available for Host	Sends the host a link to a meeting recording.	• %SiteURL% • %OrgLogo% • %DisplayName% • %Topic Name% • %Duration% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
SSO Activation Email	Sent after Single Sign-On (SSO) is enabled.	• %SiteURL% • %DisplayName% • %participants% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Send Email To All Users	Sends an email to all users on the system.	• %SiteURL% • %Subject% • %OrgLogo% • %AttendeeName% • %Body% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
Setup Cisco WebEx—Mobile Device	Informs users about the Cisco WebEx app for mobile devices and provides a download link for the app.	• %SiteURL% • %Subject% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Share Recording	Sends selected meeting invitees a link to a meeting recording.	• %HostName% • %HostEmail% • %OrgLogo% • %HostName% • %RestrictionMessage% • %TopicName% • %Duration% • %RecordingTime% • %PersonalizedMessage% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
Share Recording from MC	Sends selected meeting invitees a link to a meeting recording. Participants selected by the host in Meeting Center after selecting **Leave Meeting**.	• %HostName% • %HostEmail% • %OrgLogo% • %AttendeeName% • %Topic Name% • %Duration% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Users—Password Changed	Sends users an email when their password has been changed.	• %SiteURL% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Welcome Email	Sent to a new administrator after his or her account is created.	• %SiteURL% • %DisplayName% • %SiteURL% • %Support% • %participants% • %CustomFooterText% • %Year%

Table 4: Meetings Email Templates

Title	Description	Variables
Blast Dial Meeting Invite for Host	Sent to the host when a host dials a Blast Dial call-in number to start a meeting.	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %HostPin% • %NeedInfo_InternalUser% • %Support% • %CustomFooterText% • %Year%
Blast Dial Meeting Invite for Attendee	Sent to participants when a host dials a Blast Dial call-in number to start a meeting.	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %ParticipantPin% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText% • %Year%
Blast Dial Meeting Group Deleted	Sent to the members of the Blast Dial group when an administrator deletes the group.	• %SiteURL% • %BlastDialGroupName% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
In-Progress Blast Dial Meeting Invite for Host	Sent to other hosts when a host invites them to a meeting while the meeting is in progress.	• %SiteURL% • %BlastDialGroupName% • %HostName% • %MeetingInfoURL% • %AccessNumber% • %HostPin% • %MeetingPassword% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText% • %Year%
In-Progress Blast Dial Meeting Invite for Attendee	Sent to users when a host invites them to a meeting while the meeting is in progress.	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %ParticipantPin% • %MeetingPassword% • %NeedInfo_InternalUser% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
Blast Dial Meeting Information Updated for Host	Provides meeting information to a host when the meeting settings have been changed.	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %HostPin% • %NeedInfo_InternalUser% • %Support% • %CustomFooterText% • %Year%
Blast Dial Meeting Information Updated for Attendee	Provides meeting information to participants when the meeting settings have been changed.	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %ParticipantPin% • %NeedInfo_InternalUser% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
In-Progress Meeting Invite for Attendee	Sent to users when a host invites them to a meeting while the meeting is in progress.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Instant Meeting Invite for Host	Sent to the host and invitees when the host selects **Meet Now**.	• %SiteURL% • %Topic% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
Meeting Canceled for Attendee	Informs a user that a scheduled meeting has been canceled.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText% • %Year%
Meeting Canceled for Host	Sent to the meeting host to confirm cancellation of a meeting.	• %SiteURL% • %Topic% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText% • %Year%

Title	Description	Variables
Meeting Information Updated for Alternate Host	Provides meeting information to the alternate host when the meeting settings have been changed.	• %HostName% • %HostEmail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Meeting Information Updated for Attendee	Provides meeting information for a meeting invitee when the meeting settings have been changed.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
Meeting Information Updated for Host	Provides meeting information to the host when the meeting settings have been changed.	• %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Meeting Reminder for Alternate Host	Sends a meeting reminder to the meeting alternate host.	• %HostName% • %HostEmail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
Meeting Reminder for Host	Sends a meeting reminder to the meeting host.	• %SiteURL% • %Topic% • %OrgLogo% • %HostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Meeting Rescheduled for Alternate Host	Sends updated meeting information to the alternate host.	• %HostName% • %HostEmail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
Meeting Rescheduled for Attendee	Sends updated meeting information to invitees.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
MeetingInfo for Alternate Host	Sends a meeting confirmation to the alternate host.	• %HostName% • %HostEmail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
MeetingInfo for Attendee	Sends a meeting invitation to invitees.	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
MeetingInfo for Host	Sends a meeting confirmation to the host.	• %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
PCN Meeting Auto Reminder—Host	Sends an automatic meeting reminder to the meeting host (Personal Conference accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingNumberNoSpaces% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
PT PCN Meeting Manual Reminder—Host	Sends a manual meeting reminder to the meeting's host (PCN accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingNumberNoSpaces% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%

Title	Description	Variables
PT PCN Meeting Manual Reminder—Invitee	Sends a manual meeting reminder to invitees (Personal Conference accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
PT PCN Meeting Notification—Host	Sends a meeting notification to the host (Personal Conference accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingNumberNoSpaces% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%

Title	Description	Variables
PCN Meeting Instant Invitation—Host	Sends an instant meeting notification to the host (Personal Conference accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %SiteURL% • %Support%
PCN Meeting In Progress Invitation—Invitee	Sends an instant meeting notification to an invitee (Personal Conference accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Title	Description	Variables
PCN Meeting Schedule Change—Host	Sends a schedule change notification to the host (Personal Conference accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingNumberNoSpaces% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
PCN Meeting Schedule Change—Invitee	Sends a schedule change notification to an invitee (Personal Conference accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Title	Description	Variables
PCN Meeting Rescheduled—Invitee	Sends a meeting rescheduled notification to an invitee (Personal Conference accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
PCN Meeting Canceled—Host	Sends a meeting cancellation notification to a host (Personal Conference accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%
PCN Meeting Canceled—Invitee	Sends a meeting cancellation notification to an invitee (Personal accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%

About Application Downloads

You can mass-deploy CWMS applications by using the tools available to you on the Administration site. The applications available for download include are:

- WebEx Meetings Application—The core application for scheduling, attending, or hosting meetings.

  Running the WebEx Meetings application on a virtualized operating system is not supported.

  If a user does not have the WebEx Meetings application installed, the first time a user joins a meeting it is downloaded to the PC. This can be configured to be done on-demand or silently. The user has the option of using the Cisco WebEx Meetings application for the duration of the meeting and having it removed when the meeting is over or performing an installation of the application to speed up the process of starting or joining future meetings. This might fail because the user does not have administrator privileges.

- WebEx Productivity Tools—Provides an interface between other applications, such as Microsoft™ Outlook®, allowing the management of meetings through those applications.

  After an update or upgrade to a system, any old versions of WebEx Productivity Tools should be removed and the latest version installed.

- WebEx Network Recording Player—Plays back the recordings of meetings. This can include any material displayed during the meeting.

In CWMS the .MSI installer for the applications is available from the **Admin** > **Settings** > **Downloads** page. See "Downloading Applications from the Administration Site" in the CWMS Planning Guide for more information.

We recommend that you push the applications to user computers offline, before you inform those end-users that accounts have been created for them. This ensures that your users can start and join meetings and play network recordings the first time they sign in.

Where users have administrator privileges, you can enable users to download the applications from the end-user **Downloads** page and install the applications themselves. No additional administrator action is required.

When **upgrading** to Cisco WebEx Meetings Server Release 1.5MR3 or later in a locked-down environment where user PCs do not have administrator privileges, before you start the upgrade procedure push the new version of the WebEx Meetings application to all user PCs.

Configuring Your Download Settings

You can configure your system so that administrators can manually download Cisco WebEx desktop applications to users, or you can enable users to perform their own downloads.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

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

Note If you plan to manually push WebEx Productivity Tools to your users, we recommend that you uncheck this option.

When this option is selected, after users install an updated version of Cisco WebEx Productivity Tools, the version of WebEx Productivity Tools displayed in the **Programs and Features** in the Windows Control Panel shows an older version number. However, the version displayed in the **About WebEx Productivity Tools** in the WebEx Assistant shows the correct version This is a known issue and will be fixed in a later release.

Step 4 Select your download method:

- Permit users to download WebEx desktop applications
- Manually push 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 WebEx Meetings and Productivity Tools to user's desktop**, the WebEx Meetings Application, Productivity Tools, and WebEx Network Recording Player sections appear on the page. Proceed to the next step.

Step 5 For each application that you want to download and install, select **Download** and select **Save** to save a ZIP file to your system that contains installers for the corresponding application.
Each ZIP file contains application installers for all supported languages and platforms.

Step 6 Select **Save** to save your download settings.

Configuring Security

Managing Certificates

Certificates ensure secure communication between the components of your system. When your system is deployed, it is configured with a self-signed certificate. While a self-signed certificate can last for up to five years, we recommend that you configure certificates that are validated by a certificate authority. A certificate authority ensures that communication between your virtual machines is authenticated. A system can have multiple virtual machines. Only one certificate is required for a data center. Except for the IRP virtual machine, the system certificate includes the fully qualified domain names (FQDNs) for all other virtual machines, site URLs, and administration URLs.

After performing a major upgrade, for example from 1.x to 2.6.1.39 by using the OVA file, the system has only a self signed internal SSL certificate installed. This self signed internal SSL certificate has a common name/subject as the Admin Site URL; the old SSL certificate has the common name/subject set to the Site URL. Since the Internal SSL Certificate only allows certificates with the common name set as the Admin Site URL, the old certificate cannot be re-applied and you must generate new certificates immediately after the upgrade. You can either use the old SSL certificate as an external certificate and generate another Internal SSL Certificate for internal users or generate a new SAN certificate with the common name changed from the Site URL to the Admin Site URL.

The following certificate types are supported:

- SSL—Required on all systems.
- SSO IdP—For SSO with identity provider (IdP) certificates. (See Importing SSO IdP Certificates, on page 62.)
- 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.
- SMTP—Required if your email server is TLS-enabled.

About Generating a CSR or Certificate

You cannot update your certificates or Certificate Signing Request (CSR), but you can generate a certificate or a CSR at any time. If you add virtual machines to your system or change any of your existing virtual machines, generate new certificates for each virtual machine on your system.

SSL certificates can become invalid for the following reasons:

- A data center is joined to the system.
- Your system size has been expanded, 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 automatically generates new self-signed certificates. You receive notification of this change; a global warning message appears at the top of the Administration site page indicating that SSL has become invalidated.

Certificate Structure

Certificates contain names, representing to whom they are issued. The Common Name (CN) is always there and considered the "official name." Other names are aliases or in certificate terminology, Subject Alternative Names (SANs). These are not mandatory, but are used when a group of entities (persons, servers). share a certificate, such as in CWMS.

In CWMS certificates, those are the DNS names of the CWMS pieces (VM FQDNs, WebEx Site URL, and WebEx Administration URL). Prior to CWMS version 2.5MR5 there was one certificate set for all machines in CWMS. Those certificate names are based on the WebEx Site URL. Alternative names were everything else except the FQDNs of the Internet Reverse Proxies.

In CWMS version 2.5MR5 and higher, there are internal certificates and optionally external certificates. If you do not have IRPs (public access is not enabled), then external certificates are not available. If you do have IRPs (public access is enabled), then you optionally can have an external certificate just for IRPs. If there are no external certificates, then the Internal Certificate is used for all.

With this change, internal certificates have a CN based on the common Administration URL. SANs are based on the local WebEx Administration URL, WebEx Site URL, and internal FQDNs.

External certificates have a CN based on the WebEx Common Site URL. SANs are based on the Local Site URL and the Common Site URL.

For CWMS 2.5MR5 and later, when you upload new certificates, CWMS validates only the CN. The CN for internal certificates must match the Administration Site URL and the CN for external certificates must match the WebEx Common Site URL. After you upgrade to CWMS 2.5MR5 or later, your existing certificates still work. However, if you want to upload new certificates, the CNs for the new certificates must follow these guidelines.

Wildcard Certificates

Because CWMS 2.5MR5 and later validate only the CN for certificates, the following rules apply to wildcard certificates:

- The CN must contain the wildcard.
- The wildcard name cannot be used as a SAN.

For example, if you generate a certificate with CN = cisco.com and SAN, DNS = *.cisco.com, the certificate upload fails with the following message:

```
Server domains in the certificate do not match the WebEx site URL.
```

About Generating SSL Certificates

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

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

Before 2.5MR5, a single certificate was used for the whole system. For 2.5MR5 and later, both internal and external certificates can be used.

To use a single certificate to support all hostnames internally and externally, generate and upload only the Internal certificate. This internal certificate uses the Admin URL as the common name, but it includes all system hostnames.

An external certificate is not necessary, as it only supports the Site URL. If the external certificate is updated, the internal certificate is not used externally.

When manually generating a self-signed certificate, you can choose between the Common URL and the Local Administration URL for the Common Name (CN).

When generating a Certificate Signing Request (CSR), you can choose between wildcard, local, or common URL (Site URL or Administration URL). The List of Subject Alternative Names (SANs) is:

- Invisible if the CN is a wildcard (covers a full domain).
- Pre-populated but you can modify it if the CN is a URL that does not cover a full domain. We recommend keeping the pre-populated list, but you can add entries. We strongly recommend against removing any pre-populated items from the list.

Generating a Certificate Signing Request (CSR)

The hashing method used to generate Certificate Signing Request (CSR) and private key for SSL certificates in CWMS 2.0 and earlier versions use SHA1. CWMS 2.5 and above uses SHA2 (SHA256).

Both internal and external application certificates and CSRs have the following options:

- Key types:
  - RSA
  - EC
- For RSA key type key length is 2048.
- RSA Hash algorithms:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Key sizes and hash algorithms for EC certificates:
  - Key size 256:
    - SHA256
    - SHA384
    - SHA512
  - Key size 384:
    - SHA384
    - SHA512
  - Key size 512:
    - SHA512

Some Certification Authorities do not support the Key Agreement extension. Cisco WebEx Meetings Server does not require this extension.

External and Internal certificates must be the same type. The external certificate depends on the internal certificate. For example, if a system has an RSA Internal certificate then the **Generate External Self-signed**

page has just one Key type option, RSA (same as the external certificate key type). You cannot generate or upload external certificates with a different key type than the installed internal key type.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Certificates** > **Certificates on CWMS System**.
On a Multi-data Center system, continue with **Certificates on CWMS System or Certificates on Datacenter *N***

Step 3 Select **Generate CSR** for the desired type of CSR.
On November 1, 2015, Certification Authorities (e.g. VeriSign, GoDaddy, and so forth) will stop issuing certificates for internal domain names (e.g. domain.local, domain.internal). Before CWMS version 2.0MR9, you could upload only a single SSL certificate with Subject Alternative Names for all components in the deployment, but this requires you to purchase expensive SAN SSL certificates for a complete solution. As of CWMS version 2.5MR5 you can purchase on WebEx Site URL SSL a certificate from Certification Authority for use on IRP servers, and use Self-signed SSL certificates for the internal network virtual machines.

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

Option	Description
Common Name	Select **Local Site URL** certificate, **Global Site URL** certificate, or **Wildcard** certificate.
Subject Alternative Names 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.
Key Size	Select the key size 2048.

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 by using VMware Data Recovery or VMware vSphere Data Protection.
Backing up your system preserves the private key if it becomes necessary to restore it.

Importing a SSL Certificate

Cisco WebEx Meetings Server supports X.509 certificates with PEM and DER encoding, and PKCS12 archives.

Users might have problems joining meetings if their system uses a self-signed certificate. To avoid this, configure the client side to use self-signed certificates.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off.
If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 Select **Settings** > **Security** > **Certificates** > **Certificates on CWMS System**.
On a Multi-data Center system, continue with **Certificates on CWMS System or Certificates on Datacenter *N***

Step 4 Select **More Options** > **Import SSL Certificate/private key**.
If you already have a certificate installed, the system warns you that importing a new certificate will overwrite it.

Step 5 Select **Browse** and choose your certificate.
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 you use a PEM file, it must be formatted as follows:

- (Optional) 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 a password to decrypt it.
- 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, 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 can upload the intermediate certificates to prevent certificate warnings if you are using a certificate authority that uses intermediate certificates and the intermediate certificates are not distributed in their clients.

If the certificates come with a certificate chain, you must combine an intermediate certificate and an end-user certificate into one file. The sequence is that the intermediate certificate is first, and the end user certificate is next. The two certificates are back to back; there is no space between them.

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

Step 6 Select **Upload**.
The system determines if the certificate is valid. A certificate might be invalid for the following reasons:

- The certificate file is not a valid certificate file.
- The certificate file has expired.
- Your public key is less than 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.
- It does not contain all the host names in the system (other than DMZ host names) or the site and administration URLs. In a MDC system, it must contain the global site, local site, and administration URLs.

Step 7 (Optional) Enter the **Passphrase**.
A passphrase is required to decrypt PKCS12 archives or an encrypted private key (if the uploaded PEM files contain the private key).

Step 8 Select **Continue**.
Your system imports your SSL certificate and displays it in a scrollable certificate file dialog box.

Step 9 Select **Done**.

Step 10 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

Exporting an SSL Certificate

Download the Secure Socket Layer (SSL) certificate:

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Certificates** > **Certificates on CWMS System**.
On a Multi-data Center system, continue with **Certificates on CWMS System or Certificates on Datacenter *N***

Step 3 Select **More Options** > **Export SSL Certificate**.
An option to open or save the certificate appears.

Step 4 Save the certificate file.

What to Do Next

Verify that administrators and end users are able to sign in to the administration or common web pages without seeing any *site not trusted* warnings.

Exporting an SSL Certificate for Mobile Devices

Apple iPhones or iPads running Apple iOS 5.0 or later have a built-in, trusted root certificate. If your company uses a self-signed certificate or if the root certificate installed on your Cisco WebEx Meetings Server is not on the Apple Trusted Certificate Authority list, you must export a SSL certificate and email it to your users to install on their mobile devices before they can join a WebEx meeting.

Exporting an SSL certificate is required only if you are using a self-signed certificate. If you are using a trusted Certificate Authority-signed certificate, exporting a SSL certificate is not required.

Before You Begin

Verify that the trusted root certificate pre-installed on a user's Apple iPhone or iPad is on the Apple Trusted Certificate Authority list. See http://support.apple.com/kb/ht5012 for details.

Verify that users have an active, high-speed internet connection for their mobile devices.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Certificates** > **Certificates on CWMS System**.
On a Multi-data Center system, continue with **Certificates on CWMS System or Certificates on Datacenter *N***

Step 3 Select **More Options** > **Export SSL Certificate**.
An option to open or save the certificate appears.

Step 4 Save the certificate file to your local hard drive.

Step 5 Attach the saved certificate file to an email and send it to each authorized user iOS email account.

Step 6 Users open the email on their mobile devices, save the file, and install the certificate file on their mobile devices:

a) Tap **Install** on the **Install Profile** page.
b) Tap **Install Now** on the Unsigned Profile dialog.
c) Enter an iOS password.
d) Tap **Next**.
e) Tap **Done**.

Downloading a CSR and Private Key

You can use this procedure to obtain the private key from the CWMS. If you do not own the file, contact the Cisco Technical Assistance Center for assistance.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Certificates** > **Certificates on CWMS System**.
On a Multi-data Center system, continue with **Certificates on CWMS System or Certificates on Datacenter *N***

Step 3 Select **More Options** > **Download CSR**.
A dialog box appears asking you to save the CSR.zip file that contains the CSR and private key.

Step 4 Select a location on your system to save the file and select **OK**.

Step 5 Back up your private key file, `csr-private-key.pem`, in case 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.

Note Users might have problems joining meetings if their system uses a self-signed certificate, unless the administrator on the client side has configured the system to use self-signed certificates.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Certificates** > **Certificates on CWMS System**.
On a Multi-data Center system, continue with **Certificates on CWMS System or Certificates on Datacenter *N***

Step 3 Select **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)
X.509 subject name	The hostname of your system is the site URL. On an MDC system, you can choose between the local site URL and the global site URL.

Option	Description
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**.
If you need to use the same SSL certificate after a major upgrade, you must upload the private key generated with the CSR that is used to get the certificate. The private key must be the first block in the certificate file.

Your certificate file is generated and displayed.

Step 6 Select **Done**.

Restoring an SSL Certificate

If your certificate becomes invalid or you perform a disaster recovery on your system, you can restore SSL certificates. Cisco WebEx Meetings Server supports X.509 certificates with PEM and DER encoding, and PKCS12 archives.

Before You Begin

You have a backup of the certificates and the private key (if used by your system).

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off.
If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 Select **Settings** > **Security** > **Certificates** > **Certificates on CWMS System**.
On a Multi-data Center system, continue with **Certificates on CWMS System or Certificates on Datacenter *N***

Step 4 Select **More Options** > **Import SSL Certificate/private key**.

If you already have a certificate installed, the system warns you that importing a new certificate overwrites the existing certificate.

Step 5 Select **Continue**.

Step 6 Select **Browse** and choose your certificate file.
Choose an X.509-compliant certificate or a 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. Format PEM files as follows:

- (Optional) Combine the private key file (csr_private_key.pem) and the certificate received from your certificate authority (CA) into one file. The private key must be the first block in the file. The file can be encrypted or unencrypted and be in the PKCS#8 format and PEM encoded. If the file is encrypted, 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. Don't include the certificate of the root certificate authority. The server certificate is the last block in the file. If you use a private certificate authority, you must distribute the root certificate to all clients.

Upload all certificates together in one file. You cannot upload one certificate and then add the intermediate certificates later. You can 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 the intermediate certificates prevents certificate warnings.

PKCS#12 files must have a .p12 extension and contain only the certificates and optionally, the private key.

Step 7 Select **Upload**.
After you select **Upload**, the system will determine whether 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 is 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 the system automatically generated 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. To continue, select a valid certificate.

Step 8 (Optional) Enter a **Passphrase**.
A passphrase is required to decrypt PKCS12 archives or an encrypted private key (if uploaded .pem files contain the private key).

Step 9 Select **Continue**.

Your system imports your SSL certificate and displays it in a certificate file dialog box.

Step 10 Select **Continue** on the **SSL Certificate** page to complete the import.

Step 11 Select **Done**.

Step 12 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

Importing SSO IdP Certificates

For service provider-initiated single sign-on (SSO) with a signed authentication request in a Multi-data Center (MDC) system, you must import the certificate from each data center into the Identity Provider (IdP). The certificate must be a Token-Signing certificate, in Base-64 encoded X.509 format. (Cisco WebEx Meeting Server cannot use its private key to decrypt the assertion.)

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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 SMTP Certificates

Importing SMTP certificates from a local computer to the CWMS system.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Certificates** > *datacenter* > **SMTP Certificate** > **Import Certificate**.

Step 3 Select **Browse** and choose your SMTP certificate.

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

Step 5 If your system is not in Maintenance Mode, select **Continue** to enter Maintenance Mode.

Step 6 Select **Done** to submit your certificate.

Step 7 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

Step 8 Select **Continue**.
The system restarts.

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 Configuring Your Audio Settings, on page 7 for more information.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off.
If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 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 4 Select **Import Certificate** for CUCM *n*.
The **Secure Teleconferencing Certificate** page appears.

Step 5 Enter a certificate name.

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

Note If CUCM uses self-signed certificates, then use the CallManager.pem file. If CUCM uses third-party certificates, then use the Root Certificate Authority (CA) certificate. See "Downloading CUCM Certificates" in the *Planning Guide* for more details on how to download a CUCM certificate to your local hard drive.

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 **Done**.

Step 10 Return to step 4 and repeat the process for the next CUCM server.

Step 11 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

Configuring User Session Security

You can configure how long sessions can remain inactive before users are automatically signed out.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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.
Simultaneous user sessions	Configure the number of user sessions (of the same kind) a user can start at any given time or select **Unlimited**.
Simultaneous administrator sessions	Configure the maximum number of administrator sessions a user can open at any given time or select **Unlimited**.
Display important sign-in information	Select this option to display the IP address from which the user signed in and the number of failed sign-in attempts. **Default**: selected.

Step 4 Select **Save**.

Certificate Revocation Checking

When enabled, shows a warning if the certificate authority server is not reachable or the certificate has been revoked.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Certificate Revocation Checking**.

Step 3 Enable or disable Certificate Revocation Checking
Checked: A warning displays if the certificate authority server is not reachable or the certificate has been revoked.

Unchecked: If a server certificate has been revoked or the certificate authority server is not reachable, there is no warning.

Step 4 Select **Save**.

Encrypting Sensitive Information

This feature enables stronger encryption of sensitive information that is shared between the Cisco WebEx Meetings Server and the client application. After you enable this feature, you can block old encryption of sensitive information, or allow both old and new encryption.

Encrypt Meeting Content

You can encrypt meeting content between the Cisco WebEx Meetings Server and the users.

The client application must be compatible with this feature. Older client applications can still connect to Cisco WebEx Meetings Server for backward compatibility.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all data centers for the system.

Step 2 Select **Settings** > **Security** > **Encrypt Sensitive Information**.

Step 3 Select **Encrypt meeting content between the Cisco WebEx Meetings Server and the users**.

Important Once you enable this option, you cannot disable it.

Step 4 Confirm that you want to proceed.

Step 5 Select **Save**.

Block Unencrypted Meeting Content

You can block unencrypted meeting content between the Cisco WebEx Meetings Server and the users. You can disable this option at any time.

Important When you enable this option, synchronize all of the data centers in Maintenance Mode.

After you enable this option, older client applications will not connect to the Cisco WebEx Meetings Server.

Before You Begin

Encrypt meeting content between the Cisco WebEx Meetings Server and the users must be enabled. Otherwise, the option to block unencrypted meeting content is dimmed.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Encrypt Sensitive Information**.

Step 3 Select **Block unencrypted meeting content between the Cisco WebEx Meetings Server and the users**.
On Jabber versions 11.5 and earlier, when this feature is enabled the Jabber client displays the error "The WebEx meeting is not available. Cannot start the meeting, error code: 47." The meeting room does not launch; however, the meeting is created on CWMS.

Step 4 Select **Save**.

Step 5 Select **Continue** to confirm putting system in to Maintenance Mode.
Turning on Maintenance Mode on all of the active data centers shuts down conferencing activity. Users cannot sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings. If this data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover could cause a brief interruption in active meetings.

Step 6 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

Remove Un-secure Data from URLs (Short Link)

When the elimination of un-secure data is enabled, links use only short URLs (one UUID parameter); all meeting, recording, and user links only accept short URLs:

- Join meeting
- Invite meeting
- Start meeting
- Meeting information
- Change password
- Playback recording
- Share recording
- Create password

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Short Link**

Step 3 Select **Eliminate unsecure data from URL links**.
New meeting, recording, and user link URLs are in a short URL format (no more than one UUID parameter) that eliminates insecure data. Long URL links (more than one UUID parameter) that existed before un-secure URL data was enabled are allowed to pass. Long URLs created after the blocking of un-secure data was enabled are not allowed to pass.

Step 4 (Optional) Select **Block all long URL links**.
All long URLs are blocked, no matter when they were originated.

Once enabled this feature cannot be disabled.

Any long meeting link URLs that contains insecure data are no longer valid. Users must update meetings scheduled before this parameter was enabled for them to comply with the short URL requirement and be passed by the system.

Step 5 Select **Save**.

Configuring Federated Single Sign-On (SSO) Settings

The CWMS system supports Single Sign-on (SSO) systems based on the industry standard Security Assertion Markup Language (SAML) 2.0 protocol.

SSO allows clients to use their on-premises SSO system to simplify the management of their CWMS system. With SSO, users securely sign into the system by using their corporate sign-in credentials. You can also configure SSO to create or manage user accounts on the fly when users attempt to sign in. User login credentials are not sent to Cisco, protecting corporate sign-in information.

Note Enabling SSO overrides users login settings. Make sure you inform users before you enable SSO.

After making a change to an existing user's email address, that user must wait until the Exchange server, Outlook, and CWMS server are synchronized before the scheduling of a meeting by a delegate (proxy) user hosted by that user with the modified email. Also attempting to schedule an alternate host with a recently modified email address will fail. The address book in Outlook is synchronized with the Exchange server once a day. When an email address is changed on the Exchange server, that change is not immediately propagated to Outlook. If, prior to synchronization, a user attempts to schedule a meeting for a user with a modified email address or identify them as an alternate host, the system receives the old email address and issues a notice that the user cannot be found. Manually synchronizing the systems does not solve this issue. Note that this is not a CWMS issue, but a result of the way Outlook and Exchange are designed.

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

- **Note** After you have enabled SSO, user credentials are managed by the authentication system. Certain password management features no longer apply to your users. See Configuring Passwords, on page 24 and Editing Users for more information.

- Configure a SSO IdP certificate to use this feature. See Importing SSO IdP Certificates, on page 62 for more information.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Certificates** > **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 from where 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.
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.

Field	Description
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. If you use a format other than an email address,users will no longer be able to sign in to a WebEx site if SSO is disabled. **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 sign in.
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.
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.

Field	Description
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 disables a user's 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.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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 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.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off.
If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 Select **Settings** > **Security** > **Virtual Machines**.

Step 4 Select **Update Encryption Keys**.

Step 5 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

About FIPS

The Federal Information Processing Standard (FIPS) 140 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. A cryptographic module is a "set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary." The cryptographic module is what is being validated.

FIPS 140 Requirements

At a very high level, the FIPS 140 requirements apply to the following module characteristics:

- Implementation of FIPS-approved algorithms
- Specific management of the key life cycle

- Approved generation of random numbers
- Self-tests of cryptographic algorithms, image integrity, and random number generators (RNGs)

Cisco WebEx Meetings Server uses CiscoSSL 2.0 to achieve FIPS 140-2 Level 2 compliance.

With FIPS Enabled

Enabling FIPS might result in reduced compatibility with popular web-browsers and operating systems. Symptoms can include, but are not limited to, 404 errors, problems signing into the system, and starting and joining meetings.

Cisco recommends that you take the following actions:

- Ensure that your Windows PCs are running Windows 7 or later.
- Update all Windows computers to Microsoft Internet Explorer 11 regardless of the browsers actually used: Internet Explorer, Mozilla Firefox, or Google Chrome. Internet Explorer 11is required on all computers. Our FIPS-enabled clients (Cisco WebEx Meetings, Productivity Tools, and WebEx Recording Player) use FIPS-enabled system libraries available only with Internet Explorer 11.
- Configure **Internet settings** on all computers to use TLS encryption. Open **Control Panel** > **Internet Options** > **Advanced** > **Security** > **Use TLS 1.0** and **Use TLS 1.2**. We recommend that select both options for maximum compatibility, but **Use TLS 1.0** is required.

These steps apply to guest attendees (for example, people who do not work for your company). If guests do not complete these steps, they can experience compatibility issues. We recommend that you include these steps 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.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off.
If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 Select **Security** > **Settings** > **Virtual Machines**.

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

Step 5 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

Disabling FIPS Compliant Encryption

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

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off.
If the data center is part of a Multidata Center (MDC) system, in-progress meetings fail over to an active data center. The failover can cause a brief interruption in active meetings. See About Maintenance Mode for information. Turning on Maintenance Mode for all active data centers shuts down all conference functionality. No one can sign in to the WebEx site, schedule meetings, join meetings, or play meeting recordings.

Step 3 Select **Security** > **Settings** > **Virtual Machines**.

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

Step 5 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

About Next Generation Encryption (NGE, Suite B)

Next Generation Encryption (NGE) groups together the algorithms and specifications (e.g. key sizes) that are considered strong enough to provide protection for at least the coming decade. It is a set of advanced cryptographic technologies that updates all areas of cryptography components.

In multi-data center environments, all data centers must have the same kind of certificate. When certificate type is changed on only one data center, a warning is shown recommending that the administrator modify the certificate type on the other data centers.

When a system is using external certificates, the external certificates must be the same kind as the internal certificates. If there is a mismatch, a warning is shown indicating the mismatch.

The benefits of including NGE are:

- ECDSA certificates can be used on an administration interface for application certificates.

- ECDSA certificates can be imported from CUCM, SSO IdP and mail server (SMTP).
- Certificate-loading modules that can work with ECDSA.

The security modes are:

- FIPS & NGE off (default)
- FIPS on
- NGE on

Note Integration with Jabber releases before 11.5 does not work with CWMS 2.6 if there are EDCSA certificates on CWMS.

Suite B is a set of cryptographic algorithms promulgated by the National Security Agency as part of the Cryptographic Modernization Program that serve as an interoperable cryptographic base for both unclassified information and most classified information.

The Suite B components are:

- Advanced Encryption Standard (AES) with key sizes of 128 and 256 bits. For traffic flow, AES should be used with either the Counter Mode (CTR) for low bandwidth traffic or the Galois/Counter Mode (GCM) mode of operation for high bandwidth traffic (see Block cipher modes of operation) symmetric encryption.
- Elliptic Curve Digital Signature Algorithm (ECDSA) described in digital signatures
- Elliptic Curve Diffie-Hellman (ECDH) described in key agreement
- Secure Hash Algorithm 2 (SHA-256 and SHA-384) described in message digest

The NGE relationship to Suite B is:

- NGE is a super set of Suite B.
- It upgrades all crypto mechanisms—New/Upgraded algorithms, key sizes, protocols and entropy.
- Compatible with existing security architectures, e.g., DMVPN, GETVPN, p2p SA's.
- Standards based components that are available today in next-generation solutions.
- Targets Suite B (US), FIPS-140 (US/Canada), and NATO.

What works with ECDSA certificates:

- All browser interfaces.
- Meeting scheduling works from the browser and productivity tools.
- Jabber 11.5 and higher.
- Secure teleconferencing with CUCM 11 and higher.
- Directory integration with CUCM 11 and higher works with ECDSA on the CWMS side and RSA on the CUCM side. Starting in CUCM version 11.5, both sides will support ECDSA.

Enabling Next Generation Encryption (NGE)

Enabling NGE restricts the system to only new cryptographic suites, and disables older, weaker cryptographic suites.

Before You Begin

Verify that the existing application certificates meet NGE requirements. If they do not, you can choose to:

- Abort the operation and leave the system unchanged.
- Continue. The system will generate self-signed Elliptic Curve Digital Signature Algorithm (ECDSA) certificates and enable NGE mode.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 Select **Enable** in the Suite B Encryption section.

Step 4 Select **Save**.
All data centers are automatically put into Maintenance Mode and FIPS is enabled.

Step 5 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

FIPS is automatically enabled.

Disabling Next Generation Encryption (NGE)

Disabling NGE opens the system to all cryptographic suites including older, weaker suites.

Before You Begin

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

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

Step 3 Select **Disable** in the Suite B Encryption section.

Step 4 Select **Save**.
All data centers are automatically put into Maintenance Mode.

Step 5 Turn off Maintenance Mode.

When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata Center (MDC) system, you are redirected to the global admin URL. The DNS resolution policy determines which data center you see. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

See Turning Maintenance Mode On or Off.

Meeting service on the data center is restored.

FIPS remains enabled.

Uploading a Security Sign-in Warning Message

For secure sites that require users to read a security message and accept an agreement before signing in to the site, upload a file that contains warning text.

To remove the sign-in warning message, go to Configuring a Security Sign-in Warning, on page 79.

Before You Begin

Create a text file (.txt) with the warning to be displayed before a user signs in to a WebEx Common site or an Administration site. The text file must use UTF-8 characters and encoding.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Sign-in Warning**.

Step 3 Select **Browse** and the text file to be uploaded.

Step 4 Select **Upload**.
The file is uploaded and immediately appears on all sign-in pages.

Configuring the Application Audit Log

If your site is required to store audit information about system changes, configure the Application Audit Log settings.

If a person is identified as an Auditor, the **Meeting Logging Settings** and the **Logging Settings** options are visible and configurable only by the Auditor. If your system does not have a person with the Auditor role, the

Meeting Logging Settings and the **Logging Settings** options are visible and configurable by a System Administrator, SSO Administrator, or LDAP Administrator.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Application Audit Log**.
Two files are generated on the system, `admin_audit.log` for Administration Application and `end_user_audit.log` for the End-user Application.

Step 3 Select **Enable Audit Log** to enable the creation of the audit logs.
The Administration Application audit log documents the actions that change the state of the CWMS system, administrator authentication, changes in settings, actions taken by the administrator (such as importing users), and so forth. (It does not show general application errors.)

The End-user Application includes information about the user authentication, profile, meeting changes, and so forth.

If there is a Remote Syslog Server, audit logs are backed up. All audit logs are synchronized to the Remote Syslog Server, regardless of the selected Remote Syslog Event Level.

Step 4 To backup application syslog information to a remote syslog server, enter the parameters for the **Primary Remote Syslog Server**.
The events in the Remote Syslog Event Level menu are organized in order of importance.

a) Enter the **IPv4 Address** and **Port Number** if you want the system to backup application syslog information to a remote syslog server.
b) Select the protocol.
c) Select the **Remote Syslog Event Level**.
When you select an event level, the preceding levels are selected as well. For example, if you select the **Error** event level, the system captures Error, Critical, Alert, and Emergency events.

The level only affects the operating system logs and severity of those messages.

Emergency event level is the default. In the Auditor view, the alarm for log partition is also displayed.

This Event Level affects all the other logs synced by syslog, such as OS logs. Audit logs are synced as files; there is no filter for levels. No matter what level of Event is set, all the logs are synced.

Note The Remote Syslog Server is not used just for Audit logs, but for all syslog. These logs are not intended to monitor the health of the system.

Step 5 (Optional) To backup application syslog information to a secondary remote syslog server, enter the parameters for the Secondary Remote Syslog Server.

Step 6 (Optional) To delete old log archives, select the date to purge prior log archives in **Log Purging Settings** and select **Purge Log Archive**.

Step 7 Set the **Minimum percentage of free space on the log partition**, by moving the slide bar.
The parameter for the logging service makes sure the selected percentage of free space on the log partition is available. The default is 20 percent.

When an Auditor accesses this window from the Auditor tab, the configuration for the Log Partition Alarm appears.

Step 8 Set the **Retain log archives for no more than the selected number of days**.
The default is 40 days.

Step 9 Select **Save**.

What to Do Next

See Viewing and Editing Alarms for details about setting alarm thresholds.

Configuring a Security Sign-in Warning

The Security Sign-in Warning displays the warning message on the Common WebEx site, Administration WebEx site, and CLI sign-in pages.

Step 1 Sign in to Site Administration.
In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Select **Settings** > **Security** > **Sign-in Warning**.

Step 3 Browse in message and select **Upload** or select **Remove Message**.
Message is added to the system and will display on sign-in pages or the file is removed from the system and will not appear on sign-in pages.