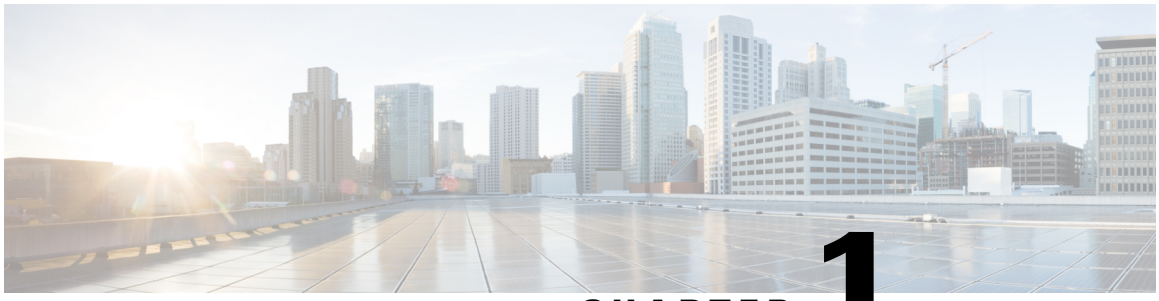
Cisco WebEx Meetings Server Administration Guide Release 2.5

First Published: 2014-07-30

Last Modified: 2017-11-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

System Overview

Product Licensing Information

Links to licensing information for this product:

- http://www.webex.com/license.html
- http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
- http://www.webex.com/CiscoWebExMeetingsServerSEULA.html

About Product Documentation

The Cisco WebEx Meetings Server Guides provides detailed procedures planning, deploying, and managing your system:

These include installation and networking checklists, to enable you to gather information and make decisions prior to the actual deployment.

In addition, we cover post-deployment, system-altering procedures, such as:

- Adding a high availability (HA)
- Expanding the system to a larger system size
- Updating or upgrading your system to the latest version

The Cisco WebEx Meetings Server Administration Guide describes how to use the features available to you on the Administration site and includes the following sections:

- Dashboard—Your dashboard displays your system monitor and includes links to your alarm settings, **Meeting Trends** page, **Resource History** page, system pages, and settings pages.

- User management—Add, import, activate, and deactivate users, configure tracking codes, and email the users on your system with these features. See Managing Users, on page 95 for more information.
- System—Configure system properties, site and administration site URLs, servers, SNMP settings, and licenses with these features. See Configuring Your System, on page 125 for more information.
- Settings—Configure your settings including company information, branding features, meeting settings, audio, video, mobility, quality of service, passwords, email settings, downloads, and security settings with these features. See Configuring Settings, on page 163 for more information.
- Report management—Configure and view your monthly reports. See Managing Reports, on page 241 for more information.
- Support access and information—Open and view support cases, configure debugging features, and conduct system resource and meeting tests using these features. See Using the Support Features, on page 271 for more information.

Terms

Terms used when describing this product.

Data Center—The physical hardware that includes at least one device that contains an instance of a system.

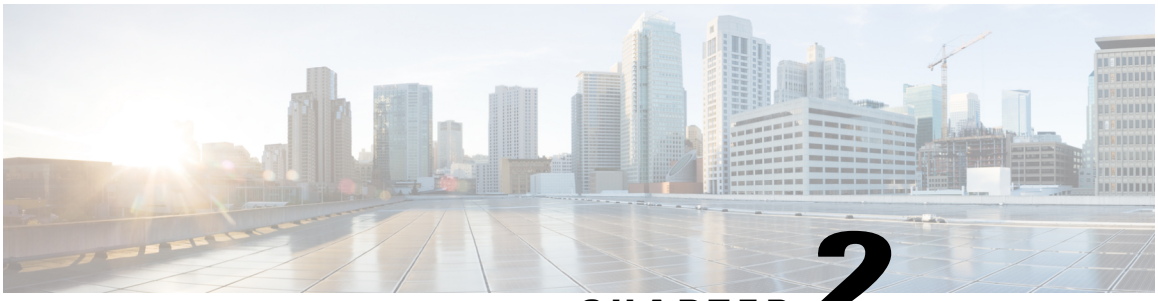
High Availability—A redundant system that exists locally in parallel with the primary system. If the primary system fails, the High Availability system replaces the failed functionality and an alert is sent. The failover is transparent to users.

Server—A single instance of a Cisco WebEx Server. Multiple data centers can be joined and function as a single system.

System—The Cisco WebEx Server system application that includes one or more physical data centers.

PART I

Cisco WebEx Meetings Server Deployment



CHAPTER 2

Using VMware vSphere With Your System

Using VMware vSphere

The virtual machines for your system are deployed with VMware vSphere. Cisco WebEx Meetings Server must be installed on VMware virtual machines, subject to the following constraints:

- Use VMware vSphere 5.0, 5.0 Update 1, 5.0 Update 2, 5.1, 5.1 Update 1, 5.5 or 6.0 (CWMS 2.6MR1 and higher).

  Use VMware vSphere 5.5, 6.0, or 6.5.

  Earlier releases of vSphere are not supported.
- Use VMware ESXi 5.0, 5.0 Update 1, 5.0 Update 2, 5.1, 5.1 Update 1, 5.5 or 6.0 (CWMS 2.6MR1 and higher).

  Use of earlier ESXi releases results in confusing error messages about **unsupported hardware** that do not explicitly list the problem.
- Verify that the DNS server configured with the ESXi host can resolve the hostnames of the virtual machines that are deployed on that ESXi host.
- You must use VMware vCenter to manage the ESXi hosts on which the Cisco WebEx Meetings Server system is deployed.
- When powering down a virtual machine, always select **Power** > **Shut Down Guest** for each virtual machine. (Do not use the **Power Off** option.)

Important VMWare Tools for CWMS is automatically installed during system deployment and should not be upgraded manually. See docwiki.cisco.com/wiki/VMware_Tools for more information on VMWare Tools.

Note For details on supported VMware configurations, see the *Cisco WebEx Meetings Server Planning Guide and System Requirements*.

Configuring the ESXi Host to Use an NTP Server

Configure the ESXi host to use Network Time Protocol (NTP) for device clock synchronization and verify that the NTP servers are reachable. In a multi-data center environment, synchronization of the data center clocks is critical to maintaining the data sharing between data centers. For detailed instructions, see the VMware ESXi documentation.

Step 1 Using the vSphere client, select the ESXi host in the inventory panel.

Step 2 Select **Configuration** > **Time Configuration** in the Software section.

Step 3 Select **Properties**.

Step 4 Select **NTP Client Enabled**.

Step 5 Select **Options** to configure the NTP server settings.
We recommend that you select **Start and stop with host** to reduce the possibility of the ESXi host time becoming incorrect.

Creating a Backup by Using VMware vCenter

Backups are traditional file systems that leverage VMware technology and SAN-based data transfer. VMware® Data Recovery creates backups of virtual machines without interrupting their use or the data and services they provide. Data Recovery uses a virtual machine appliance and a client plug-in to manage and restore backups. The backup appliance is provided in open virtualization format (OVF). The Data Recovery plug-in requires the VMware vSphere Client.

Data Recovery manages existing backups, removing backups as they become older. It also supports de-duplication to remove redundant data. Before doing any system-altering procedure, we recommend that you create a backup of each of the virtual machines by using VMware Data Recovery (available in VMware vSphere Release 5.0) or vSphere Data Protection (available in vSphere Release 5.1). (VMware Data Recovery/vSphere Data Protection is included with VMware vSphere, except in the vSphere Essentials Kit. See http://www.vmware.com/pdf/vdr_11_admin.pdf for more information.)

Backups can also be created by using a storage server. See Adding an NFS or SSH Storage Server, on page 146 for more information.

Virtual machine *snapshots* are *pictures* of your system at a specific point in time, and are not the same as backups. For performance reasons, we recommend that you use backups and keep your virtual machine

backups in a storage location that is different from the physical drives that contain your virtual machines. For more information on snapshots and known performance issues, see Taking a Snapshot by using VMware vCenter, on page 7.

Step 1 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off, on page 90.
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, on page 88 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 2 Follow the instructions in your VMware vSphere documentation and use VMware Data Recovery (called VMware vSphere Data Protection starting with vSphere Release 5.1) to create a backup of the system and each of your virtual machines.
For complete details on this backup, see the *VMware Data Recovery Administration Guide* or the *vSphere Data Protection Administration Guide*.

Note We recommend that you delete backups after a system-altering procedure is complete, you have tested the system, and you are satisfied with the results. Restoring a data center from old backups or snapshots might cause unexpected behavior.

Taking a Snapshot by using VMware vCenter

Virtual machine snapshots are used to quickly recover a virtual machine after a system-altering procedure. Snapshots are *pictures* of your system at a specific point in time, and are not the same as backups (see Creating a Backup by Using VMware vCenter, on page 6). If the original virtual machine disk file is lost, you cannot recover the virtual machine with the snapshot. We recommend that in addition to taking snapshots, that you backup your system.

Snapshots are stored on the physical drives containing your virtual machines. If you do not delete these snapshots in a timely manner, end users might experience degraded audio and video due to a known issue that affects virtual machine performance. Therefore, we recommend that you use backups and keep your virtual machine backups in a storage location that is different from the physical drives that contain your virtual machines. Also, snapshots can be used for updates, but for system upgrades we recommend that you delete all snapshots and backup the original system before performing an upgrade.

For more information on this known issue with VMware snapshots, go to the VMware web site and read the white paper, *Best Practices for Running VMware vSphere on Network Attached Storage*. You can also search the VMware KnowledgeBase for **snapshot impact performance** for additional information.

Before doing most system-altering procedures, we recommend that you backup the system (especially when performing an upgrade or expansion) and take a snapshot (when performing an update) of each of the virtual machines. You can backup your system by using VMware Data Recovery (VMware vSphere Data Protection) starting with vSphere Release 5.1 or take a snapshot of each virtual machine. (VMware Data Recovery/vSphere Data Protection is included with VMware vSphere, except in the vSphere Essentials Kit.)

Be sure to read the preparation section for the specific procedure. We list specific considerations for each procedure.

We recommend you keep snapshots no longer than 24 hours. If you want to keep them longer, we recommend that you create a backup instead. For more information on VMware Data Recovery (VMware vSphere Data

Protection starting with vSphere Release 5.1) see Creating a Backup by Using VMware vCenter, on page 6.

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, on page 90.
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, on page 88 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 On VMware vCenter, select **Power** > **Shut Down Guest** for each of the virtual machines.

Step 4 Select **Snapshot** > **Take Snapshot** for each virtual machine.

Step 5 Enter a name for the snapshot and select **OK**.
Label the snapshot for each virtual machine with the same prefix, for example, `August 20`, so you know that these snapshots were done at the same time.

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, on page 90.

Meeting service on the data center is restored.

What to Do Next

- Test your system to confirm that it is successful.
- If you must revert to a snapshot, be sure the snapshot for each virtual machine was taken at the same time. Powering on a system with mismatched snapshots might result in database corruption.

Removing a Snapshot

Removal of snapshots while the system is active causes performance issues. To avoid a reduction of system performance, take the system offline before removing snapshots.

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, on page 90.

Turning on Maintenance Mode on all active data centers shuts down conferencing activity and prevents users from signing in to the WebEx site, scheduling meetings, joining meetings, or playing meeting recordings. If this data center is part of a Multi-data Center (MDC) system and another data center is active, in-progress meetings will fail over to the active data center. This might cause a brief interruption in active meetings. See About Maintenance Mode, on page 88 for information about which system tasks require Maintenance Mode to be turned on.

Step 3 In the VMware vCenter, select **VM** > **Power** > **Shut Down Guest** on each of the virtual machines in the data center. For complete details on using vSphere, see the VMware ESXi and vCenter Server documentation.

Step 4 To remove the snapshots for all the VMs, right-click **VM** > **Snapshot** > **Snapshot Manager**.

Step 5 Select the snapshot and select **Delete**.

Step 6 Select **Yes** to confirm this action.

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, on page 90.

Meeting service on the data center is restored.

Attaching an Existing VMDK File to a New Virtual Machine

How to attach a Virtual Machine Disk (VMDK) from an existing Administration virtual machine to a new Administration virtual machine by using VMware vCenter when you expand or upgrade your system. (The system data stored on Hard disk 4 of the Admin virtual machine is reused.)

Caution Make a copy of the Hard disk 4 base VMDK file and copy that file to the virtual machine folder of the Admin virtual machine in the upgraded or expanded system. If you simply attach Hard disk 4, the data is still stored in the virtual machine folder of the old Admin virtual machine. If you accidentally delete the existing Admin virtual machine in the vCenter inventory, the current system loses access to Hard disk 4.

Be sure to copy the original base VMDK file for Hard disk 4, and not a snapshot of this VMDK file.

If you are using Direct-attached storage (DAS), migrate the VMDK to a logical unit number (LUN) where the new Admin virtual machine can access it.

Note We refer to the Admin virtual machine before the system-altering procedure as the *current* Admin virtual machine. The Admin virtual machine following expansion or upgrade, is named the *upgrade* Admin virtual machine.

Step 1 Navigate the inventory in VMware vCenter and find the current Admin virtual machine for your system.

Step 2 Right-click the virtual machine name and select **Edit Settings...**.
The **Virtual Machine Properties** window is displayed.

Step 3 Select the **Hardware** tab, then select **Hard disk 4**.

Step 4 For future reference, copy and paste into another document, the **Disk File** location.
This specifies the location of the VMDK in VMware vCenter.

The string is similar to `[EMC-LUN10-RAID5] webex-sysA-admin/webex-sysA-admin_3.vmdk`. If you have previously upgraded your system, the filename does not follow the naming convention of the existing virtual machine.

Step 5 Write down the storage location for Hard disk 4 and the virtual machine folder name.
The folder name string is similar to `[EMC-LUN8-RAID5] webex-sysB-admin`.

Step 6 Close the **Edit Settings...** window without making any changes.

Step 7 Change the vCenter view into the Datastore and Datastore Cluster view. Select **View** > **Inventory** > **Datastores and Datastore Clusters**.

Step 8 Select the storage location where the current Admin virtual machine is located (from Step 5) and select **Browse this datastore**.

Step 9 Select the storage location where your upgraded (for the expanded or upgraded system) Admin virtual machine is located and select **Browse this datastore**.

Step 10 Arrange the two datastore browser windows (for the current and expanded or upgraded Admin virtual machine) side-by-side so that you can see both Admin virtual machine folders.

Step 11 Open both virtual machine folders and copy the VMDK from the current Admin virtual machine folder to the updated Admin virtual machine folder.

a) In the current Admin virtual machine folder, locate the VMDK that is associated with Hard disk 4. Refer to the file location you wrote down in Step 4 to confirm accuracy.
b) Right-click on the file and select **Copy**.
c) Right-click inside the upgraded Admin virtual machine folder and select **Paste**. When the paste operation is completed, close both datastore windows.
d) Return the vCenter view to a list of hosts and clusters by selecting **View** > **Inventory** > **Hosts and Clusters**.

Step 12 Navigate the inventory in VMware vCenter and find the expanded or upgraded Admin virtual machine for your system.

Step 13 Right-click the expanded or updated virtual machine name and select **Edit Settings...**.
The **Virtual Machine Properties** window is displayed.

Step 14 Select the **Hardware** tab, then select **Hard disk 4**.

Step 15 Select **Remove**.
This action does not remove the virtual disk immediately. Instead, the existing virtual disk is scheduled for removal.

Step 16 Select **Add**.

The **Add Hardware** wizard is displayed.

Step 17 Select **Hard Disk**, then **Next**.

Step 18 Select **Use an existing virtual disk**, then **Next**.

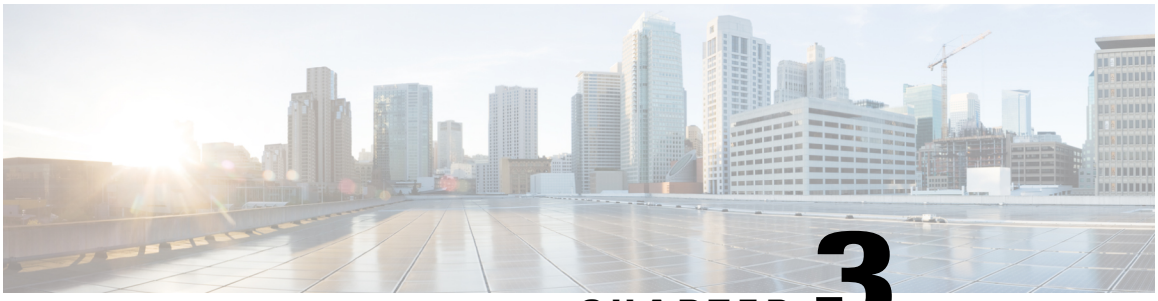
Step 19 Select **Browse**, and navigate to the datastore where the expanded or upgraded Admin virtual machine is located. Navigate to the new Admin virtual machine folder. Double-click this folder, then select the virtual disk you copied over in Step 11. Select **OK**.

Step 20 In the **Virtual Device Node** drop-down list select **SCSI (0:3)**, then select **Next**.

Step 21 Review your changes and if they are correct, select **Finish**. Otherwise, select **Back** and fix any errors.
Once the wizard is complete, a new disk marked for addition in the Hardware tab is shown.

Step 22 Commit both the Add and Remove operations by selecting **OK**.

Step 23 View this virtual machine reconfiguration task in the VMware vCenter **Recent Tasks** pane to ensure that there are no errors.



CHAPTER 3

General Information for System Deployment

System Sizes

Systems are identified by the number of concurrent users supported:

- 50 concurrent users (also known as a *micro* system)
  - Typically supports a company between 500 and 1000 employees
  - Primary system [(without High Availability (HA)] comprises an Admin virtual machine, and an optional Internet Reverse Proxy (IRP) machine.
- 250 concurrent users (also known as a *small* system)
  - Typically supports a company between 2500 and 5000 employees
  - Primary system (without HA) comprises an Admin virtual machine, a Media virtual machine, and an optional Internet Reverse Proxy (IRP) machine.
- 800 concurrent users (also known as a *medium* system)
  - Typically supports a company between 8000 and 16,000 employees.
  - Primary system (without HA) comprises an Admin virtual machine, a Media virtual machine, and an optional Internet Reverse Proxy (IRP) machine.
- 2000 concurrent users (also known as a *large* system)
  - Typically supports a company between 20,000 and 40,000 employees.

- Primary system (without HA) comprises an Admin virtual machine, 3 Media virtual machines, 2 Web machines, and an optional Internet Reverse Proxy (IRP) machine.

Terms Used During the Deployment

WebEx Site URL—Secure HTTP URL for users to host and attend meetings in a single-data center environment.

WebEx Administration URL—Secure HTTP URL for administrators to configure, monitor, and manage the system in a single-data center environment.

Public VIP—virtual IP address for the WebEx site URL.

Private VIP—virtual IP address for the Administration site URL or the virtual IP address for the WebEx site URL (for internal users only, if you have a split-horizon DNS).

WebEx Common URL—used by the DNS to redirect the user to the data center where the user performs meeting-related tasks, such as scheduling or hosting meetings. Which data center DNS chooses is transparent to the user. The WebEx Common URL is simply a convenient location for a user to enter the system. If a data center goes down, nothing changes for the user, including the URL used to access meetings, because the DNS redirects the user to the surviving data center.

Administration Common URL—is often referenced as simply the *Administration URL*. It is used by the DNS to redirect an administrator to the management data center to where the administrator logs into the system. Which data center the DNS chooses is transparent to the administrator (however, the string in the URL bar changes depending on which data center the administrator is using to access the system). The Administration Common URL is simply a convenient target an administrator uses to enter the system.

Administration Local URLs—are specific to each data center in a Multi-data Center (MDC) system. When signing in through the Administration Common URL, the DNS redirects the administrator to the Administration Local URL for the management data center. Any system modifications, such as assigning a license to a user, are performed on the management data center and replicated to all data centers in the MDC system.

An administrator can choose a specific data center to modify from within the CWMS application, but selecting another data center to modify does not change the Administration Local URL, because the administrator's access to the system remains with the data center chosen by the DNS when the administrator logged into the system. The administrator's modifications to another data center in the MDC system pass through the management data center chosen by the DNS to the target data center.

An MDC system has a minimum of two Administration Local URLs, one for every data center in the system.

Local URLs that are specific to each data center.

System Profile Information

Common Site URL		
Common Administration URL		
DC1 and DC2 Virtual IP addresses		
	Data Center 1	**Data Center 2**

Local Site URLs		
Local Administrator URLs		
Public Virtual IP Addresses		
Private Virtual IP Addresses		
DNS Server		
Administration Virtual Machine IP Address		
Media Virtual Machine IP Address 1		
Media Virtual Machine IP Address 2		
Media Virtual Machine IP Address 3		
Web Virtual Machine IP Address 1		
Web Virtual Machine IP Address 2		
DMZ Virtual Machine IP Address (optional)		
CWMS Administrator Email Addresses		
Administrator Password		
Remote Access[1]		
Remote Access Password		
Call Manager IP Address		
Cisco Call Manager Administrator ID		
Cisco Call Manager Password		
CWMS Dial-in Numbers		
Phone Numbers		

1 Remote access is not enabled unless the account is active.

Installation Checklist

Restriction You must use VMware vCenter to manage the ESXi hosts on which the Cisco WebEx Meetings Server system is deployed.

Networking Changes

See the *Cisco WebEx Meetings Server Planning Guide*. Consider the following:

- Public access: whether users external to your firewall can host and access meetings from the Internet or mobile devices. We recommend allowing public access, because it provides a better user experience for your mobile workforce.
- Type of DNS setup at your company: split-horizon DNS or a non-split horizon DNS (most common DNS configuration). For more information about DNS setup, see the *Cisco WebEx Meetings Server Planning Guide*.
- Open port 10200 from the administrator desktop to the Admin virtual machine. Port 10200 is used by the web browser during the deployment.

Required Information

The required information varies if you are doing an automatic deployment (supported for 50 concurrent users, 250 concurrent users, and 800 concurrent users) systems or manual deployment (supported for all system sizes). We recommend that you select an automatic deployment unless you are deploying a 2000-user system that always requires a manual deployment.

Choose the appropriate checklist for your deployment type:

- Required Information for an Automatic Deployment, on page 16
- Required Information for a Manual Deployment, on page 19

Required Information for an Automatic Deployment

This is the information required for your system, in order.

Note Add the virtual machine FQDNs, IP addresses, WebEx and Administration site URLs, and VIP addresses to your DNS servers before you start the system deployment. We use this information to lookup IP addresses for you during the deployment.

To avoid DNS issues, test these URLs and IP addresses before you start the OVA deployment. Otherwise, the system deployment might fail until you correct these errors.

The Fully Qualified Domain Name (FQDN) of the Primary System must be 50 characters or less to have all components up on primary system. If the FQDN is longer than 50 characters, MZM, CB, and WWP components will be in a DOWN state. (FQDN=Primary System name including the domain.)

Field Name	Description	Value For Your System
vCenter URL	Secure HTTP address of the vCenter server for the virtual machines in your system.	
vCenter Username	Username to deploy the virtual machines for your system. This user must have administrator privileges: to deploy, configure, power on or off, and delete virtual machines.	
vCenter Password	Password of the vCenter user.	
(250 and 800 concurrent user systems only) ESXi Host	ESXi host for the media virtual machine. **Note** This ESXi host must be on the same vCenter as the **vCenter URL**.	
(250 and 800 concurrent user systems only) Data store	Data store for the media virtual machine.	
(250 and 800 concurrent user systems only) Virtual Machine Port Group	Port group for the media virtual machine. **Note** Cisco recommends that you choose the same port group that you selected for the Admin virtual machine.	
(250 and 800 concurrent user systems only) FQDN for the media virtual machine	FQDN (all lowercase characters) for the media virtual machine.	

Field Name	Description	Value For Your System
(250 and 800 concurrent user systems only) IPv4 address for the media virtual machine	IPv4 address for the media virtual machine. We automatically lookup the corresponding IPv4 address for this media virtual machine.	
(Public access only) ESXi host	ESXi host for the Internet Reverse Proxy virtual machine. **Note** We recommend that you select a different ESXi host than you chose for the Admin and other internal virtual machines. To enable traffic to the Internet Reverse Proxy, be sure the ESXi host is configured with a port group that can route the VLAN whose IP address is used by the Internet Reverse Proxy.	
(Public access only) Data store	Data store for the Internet Reverse Proxy virtual machine.	
(Public access only) Virtual Machine Port Group	Port group for the Internet Reverse Proxy virtual machine. **Note** For security reasons, Cisco recommends that you select a different port group than you chose for the Admin virtual machine.	
(Public access only) FQDN for the Internet Reverse Proxy	FQDN (all lowercase characters) for the Internet Reverse Proxy virtual machine.	
(Public access only) Internet Reverse Proxy IPv4 Address	IPv4 address for the Internet Reverse Proxy virtual machine. We automatically lookup the corresponding IPv4 address for this Internet Reverse Proxy virtual machine.	
(Public access only) IPv4 Gateway	IPv4 gateway for the Internet Reverse Proxy virtual machine.	
(Public access only) IPv4 Subnet Mask	Subnet mask for the Internet Reverse Proxy virtual machine.	
(Public access only) Primary DNS Server IPv4 Address	DNS server for the Internet Reverse Proxy virtual machine.	

Field Name	Description	Value For Your System
(Public access only) Secondary DNS Server IPv4 Address	(Optional) Additional DNS server for the Internet Reverse Proxy virtual machine.	
Public VIP	IP address for the WebEx site URL (site users access to host and attend meetings)	
Private VIP	• IP address for the Administration site URL (for administrators to configure, monitor, and manage the system) • IP address for the WebEx site URL (for internal users only, if you have a split-horizon DNS).	
WebEx Site URL	Secure HTTP URL (all lowercase characters) for users to host and attend meetings.	
WebEx Administration URL	Secure HTTP URL (all lowercase characters) for administrators to configure, monitor, and manage the system.	

What to do Next

With this information, start the system deployment by entering the deployment URL in a browser window. (The deployment URL is displayed in the console window for the Admin virtual machine.)

Note If the system is rebooted before the configuration is complete, a new passcode is generated and you must use the deployment URL with the new passcode.

Required Information for a Manual Deployment

In a manual deployment, you create all the virtual machines for your system by using the OVA wizard from your vSphere client. You then install your system by using manual deployment.

When deploying a 2000-user system, you must deploy the system manually.

Note Add the virtual machine FQDNs, IP addresses, WebEx and Administration site URLs, and VIP addresses to your DNS servers before you start the system deployment. We use this information to check network connectivity at the end of the deployment.

To avoid any DNS issues, test these URLs and IP addresses before you start the OVA deployment. Otherwise, the system deployment might fail until you correct these errors.

The Fully Qualified Domain Name (FQDN) of the Primary System must be 50 characters or less to have all components up on primary system. If the FQDN is longer than 50 characters, MZM, CB, and WWP components will be in a DOWN state. (FQDN=Primary System name including the domain.)

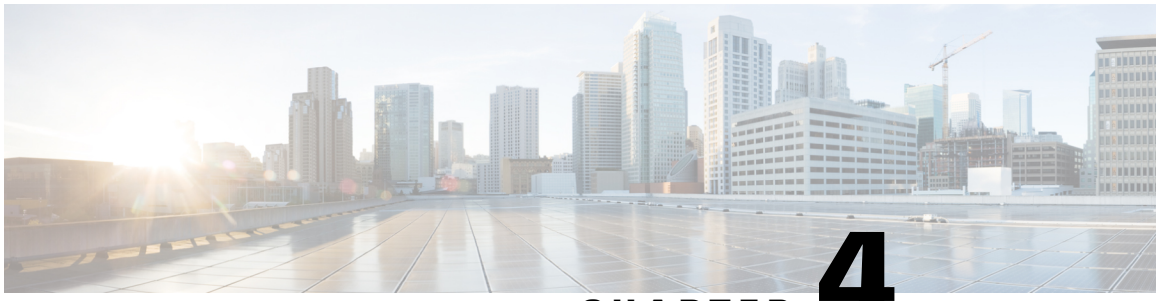
This is the information required for your system, in order.

Field Name	Description	Value For Your System
Public VIP	IP address for the WebEx site URL (site users access to host and attend meetings)	
Private VIP	• IP address for the Administration site URL (for administrators to configure, monitor, and manage the system) • IP address for the WebEx site URL (for internal users only, if you have a split-horizon DNS).	
WebEx Site URL	Secure HTTP URL (all lowercase characters) for users to host and attend meetings.	
WebEx Administration URL	Secure HTTP URL (all lowercase characters) for administrators to configure, monitor, and manage the system.	
FQDN for the internal virtual machines	Depending on the system size, this is the FQDN (all lowercase characters) of the media and web virtual machines.	
(Public access only) FQDN of the Internet Reverse Proxy	To add public access, enter the FQDN (all lowercase characters) of the Internet Reverse Proxy virtual machine.	

What to do Next

With this information, start the system deployment by entering the deployment URL in a browser window. (The deployment URL is written in the console window for the Admin virtual machine.)

Note If the system is rebooted before the configuration is complete, a new passcode is generated and you must use the deployment URL with the new passcode.



CHAPTER 4

Deploying a System: Workflows and Procedures

Deploying a System Automatically: Workflow

Deploying a System Manually: Workflow

Deploying the OVA File From the VMware vSphere Client

The OVA template creates two virtual NICs for each virtual machine. However, only the Administration virtual machines uses both virtual NICs. All other Cisco WebEx Meetings Server (CWMS) virtual machines, only one virtual NIC is used and the other one is disconnected.

This procedure is provided as a general guidance. The screens you see during the OVA deployment depends upon your vCenter, storage, and networking configuration, and might be different from what is described in this procedure. See your VMware vSphere documentation for complete information on the OVA wizard.

Before You Begin

Obtain the Cisco WebEx Meetings Server OVA file for your system and place it in a location that is accessible from VMware vSphere. Use the VMware vSphere client to deploy the Administration virtual machine for your system.

You must use VMware vCenter to manage the ESXi hosts on which the Cisco WebEx Meetings Server system is deployed. Using the vSphere client, sign in to vCenter and deploy the OVA file for the Admin virtual machine.

Step 1 Sign in to your VMware vSphere client.
Be sure to sign in as a user that includes administrator privileges: to deploy, configure, power on or off, and delete virtual machines.

Step 2 Select **File** > **Deploy OVF Template...**

Step 3 Select **Browse** to navigate to the location of the OVA file. Select **Next**.
You can select the **Cisco WebEx Meetings Server** link to go to a Web page with detailed information about this system.

Step 4 Read the End User License Agreement and select **Accept**, then select **Next**.

Step 5 Navigate to and select the location in the vCenter inventory where you want to place the Admin virtual machine.

Step 6 Enter the name of the virtual machine for your system size and select **Next**. For more information on selecting the correct size for your company, see General Information for System Deployment, on page 13.
You must deploy the Admin virtual machine before deploying any other virtual machines. If you select automatic deployment (recommended), we deploy the other virtual machines for you. If you choose manual deployment (required for a 2000 concurrent users system), then after deploying the Admin virtual machine, you must deploy the other virtual machines by using this same wizard.

Cisco recommends you include the type in the virtual machine name; for example, include "Admin" in your Admin virtual machine name to easily identify it in your vCenter inventory.

All the internal virtual machines for your system must be in the same subnet as the Admin virtual machine. (Depending on the system size you select, you might need one or more media and web internal virtual machines.)

Step 7 From the drop-down list, select the virtual machine for your system size and select **Next**.
Be sure to deploy the Admin virtual machine before any other virtual machines in your system.

Step 8 Navigate through the vCenter inventory and select the ESXi host or cluster where you want to deploy the virtual machines for your system. Select **Next**.

Step 9 If the cluster contains a resource pool, select the resource pool where you want to deploy the OVA template and select **Next**.
Resource pools share CPU and memory resources working with VMware features such as DRS or vMotion. Resource pools must be dedicated to a single ESXi Host. VMware resource pools are not recommended for use with Cisco WebEx Meetings Server.

Step 10 Select the datastore for your virtual machine and the kind of provisioning for your virtual machine.
You must select **Thick Provisioning** and create the maximum virtual disk space required for your system. With Thin Provisioning, VMware allocates the file system space on an *as-needed* basis that can result in poor performance. Lazy zero is sufficient and eager zero is acceptable, but eager zero will take more time to complete.

Step 11 Set up network mapping. For each source network, select a destination network from the drop-down list in the **Destination Networks** column. Select **Next**.

Note Both the VM Network and the VIP Network must be mapped to the same value in the Destination Network column. You can ignore the warning message about multiple source networks mapped to the same host network.

Step 12 Enter the following information for the virtual machine, then select **Next**:

- Hostname of the virtual machine (do not include the domain here)
- Domain for the virtual machine
- IPv4 address (Eth0) of the virtual machine
- Subnet mask of the virtual machine
- Gateway IP address
- Primary DNS server that contains entries for the hostname and IP address of this virtual machine

- Secondary DNS server that contains entries for the hostname and IP address of this virtual machine (A system with only one DNS server configured is at risk, because it creates a single point-of-failure. We recommend that you configure a secondary DNS server to create network redundancy.)
- Language displayed during the install process, following the power on of this virtual machine

Note To avoid DNS issues, you can test the URLs and IP addresses before you start the OVA deployment. The deployment will fail if there are errors.

Step 13 Confirm the information that you have entered. If there are any mistakes, select **Back** and change the values.

Step 14 If you are manually upgrading a system, select **Finish**, skip the balance of this procedure and continue with the next step in Upgrading Your System Manually, on page 66. (Copying data from the original system to the upgrade system by using manual deployment should be performed after the upgraded system is deployed, but not yet powered on.) Otherwise, check **Power on after deployment** and select **Finish**.

Step 15 If you are deploying an Admin virtual machine, go to vCenter and open a console window for the virtual machine. Once it powers on, we will check the networking information you entered during the OVA deployment.
If we are able to confirm connectivity, a green checkmark appears.

If there is a problem, a red X appears. Fix the error and re-attempt the OVA deployment.

Step 16 Write down the case-sensitive URL displayed in the console window.
An administrator uses this URL to continue the system deployment.

If the system is re-booted before the configuration is complete, a new passcode is generated and you must use the URL with the new passcode.

What to Do Next

If you are performing a manual deployment, we recommend that you deploy the rest of the virtual machines for your system at this time. This avoids any issues such as time outs when powering on virtual machines.

If the deployment is successful, continue with system deployment in a browser window.

If the deployment failed, see Checking Your Networking Configuration After a Failed OVA Deployment, on page 27.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Checking Your Networking Configuration After a Failed OVA Deployment

Confirm the networking entries for the virtual machine.

Important Do not use **Edit Settings...** for any of the virtual machines in your system, other than after a failed deployment. Once the system is up and running, you must use the WebEx Administration site to make any further edits to virtual machine settings. If you use your vSphere client, those changes will not be accepted by the system.

Note For detailed steps, see your VMware vSphere documentation.

Step 1 In the vSphere client, select **Power** > **Shut Down Guest** on the virtual machine.

Step 2 Find the virtual machine in the Inventory and right-click **Edit settings...**.

Step 3 Select the **Options** tab.

Step 4 Select **Properties** and confirm that all the networking information has been entered correctly. If any changes are required, redeploy the OVA with the correct settings.
One possible networking issue is that the VLAN routing is not set up correctly for the ESXi host. Because the virtual machine is on that VLAN, the virtual machine won't have network connectivity. From the network where the ESXi host resides, you should be able to ping the default gateway IP address of the VLAN you will be using for the virtual machines in your system.

Related Topics

Deploying the OVA File From the VMware vSphere Client, on page 25

Selecting Your Language for Setup

Determine your preferred language for setting up the system.

Note Do not close this browser window until the system deployment is complete. If you close the browser early, it might be necessary to restart the deployment.

CWMS System is the default name of the data center after an upgrade; it is not translated from English in any of the other languages.

Before You Begin

Be sure you have deployed the Admin virtual machine from VMware vCenter. See Deploying the OVA File From the VMware vSphere Client, on page 25

Step 1 Select the language from the drop-down menu.

Step 2 Select **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Confirming the Deployment

Step 1 Specify whether you are deploying a new system, or expanding an existing system.

Step 2 Click **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Confirming the Size of Your System

You selected the size of your system when you deployed the Admin virtual machine by using the OVA file.

Step 1 To confirm that the system size you selected during the OVA deployment is correct, click **Next**.

Step 2 If the system size is incorrect, click **I want to change System Size**.

Step 3 Using your VMware vSphere client, locate the Admin virtual machine with the incorrect system size.

Step 4 Click **Power** > **Shut Down Guest** for the virtual machine.

Step 5 Right-click the virtual machine and click **Delete from Disk**.

Step 6 Redeploy the OVA file and select the Admin virtual machine for the correct system size.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Choosing What System to Install

Step 1 Determine the type of installation.

- If you are installing this system for the first time, then choose **Install a primary system**.
- If you have installed a primary system and are adding a redundant High Availability (HA) system, then choose **Create a High Availability (HA) redundant system**.

Do not attempt install a HA system before installing the primary system, as you cannot use the HA system unless the primary system has first been installed.

Step 2 Select **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Choosing the Type of Deployment

You can choose automatic or manual deployment of the system virtual machines. Your choice of automatic or manual deployment depends on the following considerations:

- If you have time constraints, an automatic deployment is faster than a manual deployment.
- If you prefer step-by-step guidance, this guidance is provided during an automatic deployment.
- If you are familiar with VMware vCenter and do not want to provide us your vCenter credentials, select manual deployment.

We recommend that you select **Automatic** unless you are deploying a 2000-user system, which always requires a manual deployment.

Step 1 Choose one of the deployment options:

- **Automatic**: We deploy all the virtual machines required for your system.
- **Manual**: You manually deploy each virtual machine by using VMware vCenter. After answering a few questions about your system, you are provided with a list of the virtual machines required for your system.

Step 2 Click **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Providing VMware vCenter Credentials

If you select an automatic deployment, Cisco WebEx Meetings Server requires your vCenter credentials to deploy the virtual machines for you.

Before You Begin

All the ESXi hosts for your system must belong to the same VMware vCenter.

Step 1 Enter the secure https URL for the vCenter where the system will be deployed.

Step 2 Enter the username that we will use to deploy the virtual machines. The vCenter user must include administrator privileges that allow that administrator to deploy, configure, power on and off, and delete virtual machines.

Step 3 Enter the password for this username.

Step 4 Select **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24

Choosing vCenter Settings for Your Media and Web Virtual Machines

The media virtual machine is required for small, medium, and large systems. The web virtual machine is required for large systems.

Step 1 From the drop-down list, choose the ESXi host for the media or web virtual machine.

Step 2 Choose the datastore for the media or web virtual machine.

Step 3 Choose the virtual machine port group for the media or web virtual machine.
Cisco recommends you choose the same port group that you selected for the Admin virtual machine.

Step 4 Select **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24

Entering Networking Information for the Media and Web Virtual Machines

After you enter the fully qualified domain name of the media and web virtual machines, Cisco WebEx Meetings Server populates the networking information.

Note The media and web virtual machines must be on the same subnet as the Admin virtual machine. Do not edit the domain, IPv4 gateway, subnet mask, or DNS servers for the media or web virtual machines.

Step 1 Enter the FQDN of the media and web virtual machines.

Step 2 Select **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Automatically: Workflow, on page 24

Adding Public Access

If you add public access by using IRP, users outside the firewall can host or attend meetings from the Internet or mobile devices. IRP virtual machines can be added to a system at any time on a per-data center basis. Adding IRP to one data center in a Multi-data Center (MDC) environment gives users outside the firewall access to the entire system. To prevent external access, all IRP virtual machines must be removed from a system.

For security reasons, we recommend that you locate the Internet Reverse Proxy on a subnet different from the subnet occupied by the Administration virtual machine. This ensures network level isolation between the Internet Reverse Proxy and your internal (Admin and media, if applicable) virtual machines.

In a Multi-data Center (MDC) environment, the data centers cannot be expanded or upgraded. Secondary data centers must be removed from the MDC, making it a Single-data Center (SDC) environment. The MDC environment can be restored after the data centers are modified and it is verified that the data center sizes and versions match.

Before You Begin

It is not necessary to connect your storage server to an Internet Reverse Proxy (IRP) server.

If there is a firewall between the Administration virtual machines and the IRP virtual machines, the temporary IP address must be allowed through the firewall.

Step 1 Choose whether or not external users can host or attend meetings.

- If you want to add public access, confirm that **Create an Internet Reverse Proxy virtual machine** is selected.
- If you want only internal users (those behind the company firewall) to host or attend meetings, then uncheck **Create an Internet Reverse Proxy virtual machine**.

Step 2 Select **Next**.

What to Do Next

- With public access: Choosing vCenter Settings for Internet Reverse Proxy (IRP), on page 33
- Without public access: Entering the Private VIP Address, on page 34
- For IPv6 client connections: Configuring IPv6 for Client Connections, on page 132

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Choosing vCenter Settings for Internet Reverse Proxy (IRP)

Before You Begin

Verify that the firewall ports required by VMware vCenter are open so that vCenter can deploy the Internet Reverse Proxy (IRP) virtual machine. For more information on the required firewall ports, see the *Cisco WebEx Meetings Server Planning Guide*.

Step 1 From the drop-down list, choose the ESXi host for the IRP virtual machine.
Step 2 Choose the datastore for the IRP.
Step 3 Choose the virtual machine port group.
Step 4 Select **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Entering Networking Information for the Internet Reverse Proxy (IRP)

Before You Begin

Add the hostnames and IP addresses of Internet Reverse Proxy (IRP) servers in your DNS servers, to enable lookup from an external network.

If you have DNS servers to support lookup from internal networks, add the information to these servers too. This configuration enables a secure connection between your internal virtual machines and the IRP servers.

Step 1 Enter the following:

- Fully qualified domain name (FQDN)
- IPv4 gateway

- IPv4 subnet mask
- Primary DNS server IPv4 address
- (Optional) Secondary DNS server IPv4 address

If you entered the hostname and IP address of the Internet Reverse Proxy virtual machine in your DNS servers, the **IPv4 Address** field populates automatically.

Step 2 Select **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Entering the Public VIP Address

- This public VIP address must be visible from both the Internet and the internal network (split-horizon DNS only).
- This public VIP address must be on the same subnet as the Internet Reverse proxy.
- If you do not have a split-horizon DNS, then all users use the Public VIP address to host and attend meetings.
- If you have a split-horizon DNS, and added public access, then external users use the Public VIP address to host and attend meetings.

For more information on non-split horizon and split-horizon DNS, and public access, see the *Cisco WebEx Meetings Server Planning Guide*.

Note If you are creating a High Availability (HA) system, you do not need to reenter this information, as we will use the information you entered for the primary system.

- Enter the public VIP IPv4 address and select **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Entering the Private VIP Address

Administrators configure, monitor, and maintain the system from the Administration site URL that maps to the private VIP address.

If you have a split-horizon DNS, then internal users also use the Private VIP address to host and attend meetings.

If you are adding a High Availability (HA) system, you do not need to reenter this information; we will use the information you entered for the primary system.

Before You Begin

The private virtual IP (VIP) address must be on the same subnet as your internal (Admin and Media, if applicable) virtual machines.

- Enter the IPv4 private VIP address and select **Next**.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Entering the WebEx Common Site and Administration Site URLs

The Common Site URL allows users to schedule and host meetings, and access meeting recordings. The Administration Site URL provides management of the system. If you are adding a High Availability (HA) system, it is not necessary to reenter this information; the primary system URLs should match the HA system URLs.

Step 1 Enter the WebEx Common Site and WebEx Administration Site secure (https) URLs.
The WebEx Common Site URL must be different from the WebEx Administration URL.

Do not reuse the hostnames of the virtual machines in the hostname portion of the WebEx URLs.

Step 2 Select **Next**.

Related Topics

WebEx Site and WebEx Administration URLs, on page 35
Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

WebEx Site and WebEx Administration URLs

WebEx Site URL

Users access the WebEx site URL to schedule, host, or attend meetings. This URL resolves to either the private VIP address or the public VIP address, depending on whether or not you are using a split-horizon DNS.

- Resolves to the public VIP address for all users, when you do not have split-horizon DNS.
- Resolves to the public VIP address for external users when you have split-horizon DNS.
- Resolves to the private VIP address for internal users when you have split-horizon DNS.

Note Ports 80 and 443 must be open for the WebEx site URL.

WebEx Administration URL

Administrators access the WebEx Administration URL to configure, manage, and monitor the system. This URL resolves to the private VIP address.

Note Ports 80 and 443 must be open for the WebEx Administration URL.

Names for the WebEx Site and WebEx Administration URLs

You may choose almost any names for these URLs, comprising all lowercase characters. However, you cannot use the following as the hostname in the URLs:

- the same name as the hostnames for any of the virtual machines in the system
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver

- url0107ld
- version
- WBXService
- webex

Confirming that the Network is Configured Correctly

This screen provides links to online help for the networking changes required for your system. The online help provides details on DNS server changes as well as firewall settings.

You must make the DNS server and firewall changes that allow us to test network connectivity.

If you have not done so already, complete the networking configuration and select **Next**.

If you are testing an automatic deployment, we deploy the virtual machines required for your system when you select **Next**.

If you are testing a manual deployment, enter the hostnames for your virtual machines and deploy them (if you have not deployed them already).

When the deployment is complete, test them by powering them on and verifying that all the virtual machines powered on successfully.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25

Deploying the Virtual Machines Automatically

Based on the information that you entered earlier, we deploy the virtual machines required for your system.

The deployment requires several minutes to complete. Do not leave this page until all the virtual machines have deployed and are powered on, unless error messages appear.

When the status column shows all green checks, the deployment is complete with no errors. You can change the FQDNs for the virtual machines by clicking **Detect virtual machines**.

SUMMARY STEPS

1. (Optional) After the status column shows all green checks, click **Next**.
2. If errors are indicated, fix the errors.
3. Power off and delete the virtual machines involved with the errors.
4. Click **Next** to redeploy the system.

DETAILED STEPS

Step 1 (Optional) After the status column shows all green checks, click **Next**.

Step 2 If errors are indicated, fix the errors.

You can click **Download log file** to obtain the log file for the deployment. The log provides information that you can use to troubleshoot a failed deployment.

Step 3 Power off and delete the virtual machines involved with the errors.

Step 4 Click **Next** to redeploy the system.

Related Topics

Deploying a System Automatically: Workflow, on page 24

Deploying Virtual Machines Manually

After providing information about the virtual machines in the system, connect to each of the virtual machines. Virtual machines for extension units appear in this list.

Note Do not leave this browser page until the system is connected to all of the virtual machines, unless a connection fails with an error message to indicate the problem.

Step 1 Enter the fully qualified domain names (FQDNs) for the virtual machines required for your system.
You entered the Admin virtual machine FQDN earlier, when you deployed it from the OVA file.

Step 2 If you have not done so already, using VMware vCenter, deploy the virtual machines.

Step 3 Power on all of the virtual machines and verify that they powered on successfully.

Step 4 Click **Detect virtual machines**.
We establish connections to these virtual machines. This can take several minutes.

Step 5 Wait until the **Connected** status appears for each the virtual machine.

Step 6 After the status column shows all green checks, click **Next**.

Step 7 If errors are indicated, fix the errors.
You can click **Download log file** to obtain the log file for the deployment. The log provides information that you can use to troubleshoot a failed deployment.

Step 8 Power off and delete the virtual machines involved with the errors.

Step 9 Click **Next** to redeploy the system.

Related Topics

Deploying a System Manually: Workflow, on page 25

Checking the System

The system check verifies the configuration parameters of your system. This includes confirming that the virtual machines have the required minimum configuration, and validating the WebEx site and WebEx Administration URLs.

The system check takes several minutes to complete. Do not leave this page until all the checks have been completed successfully, or the system check fails and shows error messages indicating the problem.

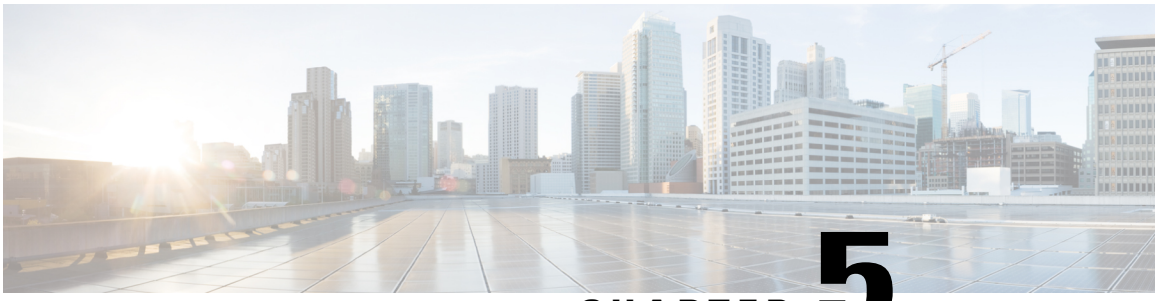
If you reload the page before the checks are complete, you are returned to the first page of this system deployment. When the checks are completed successfully, the first page of configuration utility appears.

The Administration site URL used during the deployment process is the Administration virtual machine hostname. During basic configuration, the hostname is replaced with the Administration site URL. As a result, the first time you sign in to the Administration site, the system might prompt you to accept the certificate exception.

- Complete one of the following:
  - If there are no errors and the status shows all green checks, select **Next** and continue with Configuring an Email (SMTP) Server, on page 138. In rare cases, you might see **Not tested**. This does not mean that there are any problems with your virtual machines. It simply states that system checks were not completed; for example, the entry might display because there was a temporary loss of network connectivity. Once you complete the deployment, you can sign in to the Administration site and check these resources.
  - If there is a problem with network connectivity, verify that the WebEx Site URL, Administration URL, and IP addresses are entered correctly. Verify that these sites are in the same subnet, and the parameters have been correctly entered in the DNS servers.
  - If there are problems with your system meeting the minimum system capacity, you have two options:
    - Power down all the virtual machines from VMware vCenter and manually delete them. Then retry the system deployment on a system with resources that meet or exceed the minimum requirements.
    - Proceed with your current installation. If you do, you must acknowledge that you forgo the right to request technical support from Cisco. Confirm by checking the error message check box and select **Next**.
  - If there are any problems with one or more of your virtual machines, power off the virtual machines with errors and manually delete them by using the VMware vCenter. Fix the issues and retry the system deployment.
- Select **Continue** to go to the basic configuration where you begin by setting up the mail server (Configuring an Email (SMTP) Server, on page 138) and identifying an administrator (Creating Administrator Accounts, on page 125). If another administrator will complete the basic configuration, send this URL to that administrator.

Related Topics

Deploying a System Automatically: Workflow, on page 24
Deploying a System Manually: Workflow, on page 25



CHAPTER 5

Altering the System After Deployment

Preparing for a System-Altering Procedure

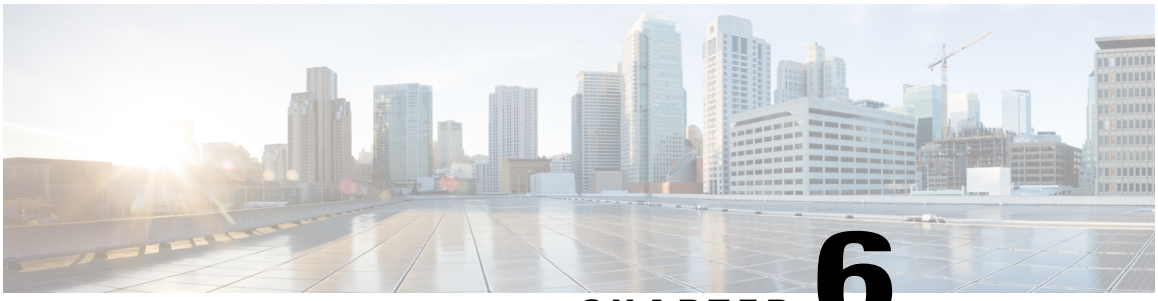
Events that are system-altering and require advance preparation by the administrator are:

- Adding or removing a high availability (HA) system. See Adding a High Availability System, on page 43.
- Updating the system to a later version (by using an ISO update file).
- Upgrading the system by deploying a parallel system and transferring the original system data to the upgraded system (by using an OVA file). See Upgrading Your System, on page 61.
- Expanding the system to a larger size. See Expanding Your System, on page 49.

Note Because these procedures require exclusive access to the system, users cannot access the system for meetings. Be sure to schedule this procedure during a time that will be least disruptive to your users.

Be sure to coordinate with other system administrators before starting a system-altering procedure. Other system administrators should not access the system during this procedure. If they do so, their changes are not saved, and the result can be unpredictable.

Backups are not required for these actions. If you do not need to create backups of your virtual machines, then you do not need to complete this procedure. However, as a best practice, we recommend creating a backup. For complete details on this backup, see Creating a Backup by Using VMware vCenter, on page 6, the *VMware Data Recovery Administration Guide*, or the *vSphere Data Protection Administration Guide*.



CHAPTER 6

Adding a High Availability System

Preparing to Add High Availability (HA) to a System

A High Availability (HA) system is a local, redundant system that is created, then added to a primary system. In the event of a virtual machine failure, the system falls back to the HA system.

If you are planning to add HA and update the system, we recommend that you add HA before updating the system, then update the combined (primary and HA) system; the HA system is updated automatically when the primary system is updated. If you update the primary system first, then to add HA, you must independently deploy and then update the HA system (so both the primary and HA systems are at the same version).

The HA system has the following constraints:

- A system running HA cannot join a Multi-data Center (MDC). (To remove HA, see Removing High Availability from a System, on page 47.)
- The HA system size must be the same as the primary system size.
- The HA system must be at the same release version as the primary system.

  If you update the primary system, the HA system must be updated.
- If the primary system currently has HA and you are deploying a new HA system, you cannot reuse the virtual machines in the original HA system. Remove the old HA virtual machines before deploying the new HA system with new virtual machines.
- Because this process adds new virtual machines to your system, your current security certificate becomes invalid and requires an updated certificate unless you are using a self-signed certificate.
- Your HA system must be configured with the same OVA and patch as your primary system. If the versions of your primary and high-availability systems do not match, you are instructed to upgrade to the higher version of the two.

- The HA system internal virtual machines must be on the same subnet as the primary system internal virtual machines.
- If you have added public access on the primary system, add it to the HA system. Also, the HA system Internet Reverse Proxy virtual machine must be on the same subnet as the primary system Internet Reverse Proxy virtual machine.
- Most of the features on your HA system are prohibited. For example you do not have access to the HA system to upgrade, configure SNMP, access storage or configure email servers. You can view system properties, but modification to the HA system is prohibited.
- Load Balancing is not configurable; it is automatic and built into the system. Any Load Balancer configured as separate machine is not supported.

Before You Begin

The following conditions must be met before adding HA to a primary system:

- Verify:
  - The target primary system is deployed and not part of an MDC.
  - There is a redundant network between virtual machines.
  - The network is a 10–gbps high-bandwidth network.
  - Network Time Protocol (NTP) configured on the primary and HA system, and that the clocks are synchronized.
- Create a backup of the primary system. See Creating a Backup by Using VMware vCenter, on page 6.
- Verify that all virtual machines are functioning normally. Determine virtual machine status by viewing the System Monitor on the Dashboard.
- We recommend that you take a snapshot on the high-availability virtual machines before you perform this procedure. Redo the procedure from the snapshot in the event of an error.
- Record the fully qualified domain name (FQDN) of the high-availability virtual machine; you must know the FQDN to add high-availability to the primary system.

Deploying a System for High Availability (HA)

High Availability (HA) is deployed like a primary system, except that during the deployment the system identifies it as a HA system. The HA system is then linked to the primary system that uses the HA system as a fallback in the event of a primary system failure. A primary system failure is transparent to users.

To add HA to a system:

Step 1 Deploy a parallel system by using Deploying a System Automatically: Workflow, on page 24or Deploying a System Manually: Workflow, on page 25. When the process asks if you are deploying a primary system or HA, choose HA. We recommend that you use the same process to deploy the HA system that you used to deploy the primary system. If you do not know which process was used to deploy the primary system, use the procedures to deploy the system

automatically, unless you are deploying a large (2000 concurrent users) system. All large systems require that you deploy the system manually.

Step 2 Verify the HA and primary system versions match:

1. In a separate browser window, sign in to the primary system WebEx Administration site.
2. On the **Dashboard** tab, verify that the primary system version number in the **System** pane matches the version of the HA.

   If the versions match, continue.
3. If the primary system is at a later version than the HA system, redeploy the HA system by using an OVA file with a matching version of the software or update the HA system.

What to Do Next

Link the HA system to the primary system by using Linking a High Availability System to a Primary System, on page 45.

When you update a high-availability system, after you reboot the system and the reboot process is complete, we recommend that you wait an extra 15 minutes before starting the procedure to add high-availability to the system.

Linking a High Availability System to a Primary System

To link the primary system to a deployed HA system completing the integration of HA into the primary system:

Before You Begin

Verify that this system is not part of a Multi-data Center (MDC) system. (HA is not supported in a MDC environment.)

Create a High Availability (HA) system by using the same process that you used to create the primary system described in Deploying a System for High Availability (HA), on page 44.

Step 1 Notify users and administrators that the system is being put into Maintenance Mode.
When you schedule a maintenance window to perform this task, the system performs a system reboot when you turn off maintenance mode. A system reboot takes approximately 30 minutes depending on the size of your system.

Step 2 Sign into the primary system administration site.

Step 3 In the System section, select the **View More** link.

Step 4 Select **Add High Availability System**.

Step 5 Follow the instructions on the **System Properties** page to add the HA system.

Step 6 Enter the fully-qualified domain name (FQDN) of the Administration site virtual machine of the high-availability system and select **Continue**.

The readiness of both the primary system and the HA system is validated. If both systems are ready, then you see a green **Add** button. (Do not select it if your system is not in Maintenance Mode.) If either system is not ready, an error message is displayed. Fix the error and attempt the procedure again.

Step 7 Select **Add**.

Note If "Error code: Database-64" displays, repeat this procedure by using a snapshot of the high-availability virtual machines.

Your high-availability system is added and automatically configured to serve as a backup in the event of a primary system failure.

Step 8 Sign back into the Administration site after the restart is complete.

To remove HA, see Removing High Availability from a System, on page 47.

High Availability System Behavior After Component Failure

When specific media and platform components running on a virtual machine go down, these components are automatically restarted by the system. Affected meetings fail over to other available resources in the same or another virtual machine in the system (for other than a standalone 50-user system).

High-Availability Systems

On high-availability (HA) systems Cisco WebEx Meetings Server will recover for these components when there is a single component failure:

- A single service on one virtual machine.
- A virtual machine.
- A single physical server or blade, which hosts up to two virtual machines (as long as the virtual machine layout conforms to the specifications listed in the *Cisco WebEx Meetings Server Planning Guide*).
- A single network link, assuming the network is provisioned in a fully redundant manner.
- A single Cisco Unified Communications Manager (CUCM) node, assuming CUCM is provisioned in a redundant manner.

Following the single component failure, the Cisco WebEx Meetings Server system behaves as follows:

- For a period of up to three minutes, application sharing, audio voice connection using computer and video might be interrupted. Cisco WebEx Meetings Server allows three minutes for the failure to be detected and to reconnect all the affected meeting clients automatically. Users should not need to close their meeting clients and rejoin their meeting.
- Some failures might cause teleconferencing audio connections to disconnect. If that happens, users will need to reconnect manually. Reconnection should succeed within two minutes.
- For some failures not all clients and meetings are affected. Meeting connections are normally redistributed across multiple virtual machines and hosts.

Additional Information For a 2000 User System

A 2000 user system provides some high-availability functionality without the addition of a HA system. For a 2000 user system without high availability:

- Your system still functions after the loss of any one of the web or media virtual machines but system capacity will be impaired.
- Loss of the Administration virtual machine renders the system unusable.

For a 2000 user system with high availability:

- Loss of any one virtual machine (administration, media, or web) does not affect your system. Your system will still run at full capacity even with the loss of any one physical server that is hosting the primary virtual machines (administration and media or web and media) or the HA virtual machines (administration and media or web).
- When a failed virtual machine is restarted, it rejoins the system and the system returns to its normal working state.
- When a media virtual machine fails, meetings hosted on that server are briefly interrupted, but the meeting fails over to an alternate media virtual machine. Users must manually rejoin the desktop audio and video sessions.
- When a web virtual machine fails, existing web sessions hosted on that virtual machine also fail. Users must sign in to the Cisco WebEx site again and establish a new browser session that will be hosted on an alternate web virtual machine.
- When an administration virtual machine fails, any existing administrator sessions also fail. Administrators must sign in again to the Administration site and establish a new browser session that will be hosted on the alternate administration virtual machine. Also, there might be a brief interruption to any existing administrator or end-user meeting sessions.

Removing High Availability from a System

Step 1 Sign in to the Administration site.

Step 2 Select **Turn On Maintenance Mode**.

Step 3 Select **View More** in the System section.

Step 4 Select **Remove High Availability System**.
The **Remove High Availability System** page appears displaying the fully qualified domain name (FQDN) of your high-availability system.

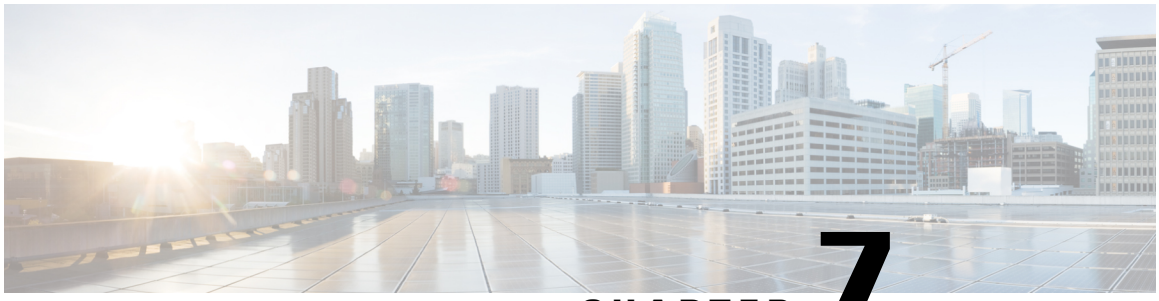
Step 5 Select **Continue**.
After you have removed a high-availability system, you cannot add the same high-availability system back into the system. To restore high availability, you must deploy a high-availability system by using the OVA file. See Adding a High Availability System, on page 43 for more information.

Your high-availability system is removed.

Step 6 Open VMware vCenter and remove the high-availability system by using the **Delete from Disk** command.

Step 7 Select **Turn Off Maintenance Mode** and **Continue** to confirm.

The system reboots.



CHAPTER 7

Expanding Your System

Preparing for System Expansion

System expansion requires the deployment of a new primary system, and the transfer of the system data and Host licenses from the original system to the expanded system.

A Multi-data Center (MDC) system cannot be expanded. It must be reduced to a Single Data Center system:

- Remove secondary data centers. (See Removing a Data Center, on page 268.) Typically this is the data center that is not running the license manager.
- Expand the primary, single-data center system by following the instructions in this chapter.
- Obtain MDC licenses for the expanded system and load the licenses on the primary system.
- Create a new secondary data center of the same size as the primary data center.
- Join the data centers. (See Joining a Data Center to a Multi-Data Center System, on page 264.)

Considerations for an Expanded System

Consider the following:

- When you expand a CWMS system that has NFS storage configured, ensure that the newly deployed virtual machines of the expanded system have the same access privileges to the NFS storage as did the original system. Otherwise expansion process will fail at the System Check phase.
- Budgeting for any additional hardware.
- Anticipating the number of concurrent meetings and their average size over the next few months.
- When an original system is upgraded or expanded, a parallel system is created. If there is time left in the trial period of the original system, that time is transferred to the upgraded or expanded system. Valid Permanent Host licenses on the original system must be transferred to an upgraded or expanded system by *rehosting* the licenses. (See Re-hosting Licenses after a Major System Modification, on page 256.)

Expanding the System Size

Before You Begin

Remove all VMware snapshots. Do not take any snapshots during the expansion process. To remove snapshots, see Removing a Snapshot, on page 8.

Obtain the Open Virtualization Archive (OVA) file first used to install this system. For example, if you deployed a version 2.0 system, obtain the base version 2.0.1.2 OVA.

Table 1: Expansion Checklist

Field Name	Current Value For Your System
WebEx Site URL	
Administration Site URL	
Private VIP Address	
Public VIP Address	

When expanding a Multi-data Center (MDC) system, it is necessary to remove any secondary data centers. (Typically the data center not running the License Manager See Removing a Data Center, on page 268.)

Note Upgrading from an unencrypted version to an encrypted version or upgrading from an encrypted version to an un-encrypted version is not supported. Obtain the OVA based on your existing system deployment.

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 If you are expanding an MDC system, remove the all but the primary data center.
See Removing a Data Center, on page 268.

Step 3 If you are expanding an MDC system, create a new data center running Cisco WebEx Meeting Server to be joined after the primary system is expanded.
See Creating a Multi-data Center (MDC) System, on page 259.

Step 4 Create a backup of the original system. (See Creating a Backup by Using VMware vCenter, on page 6.)

Step 5 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off, on page 90.
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, on page 88 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 6 Select **Continue**.

Step 7 Select **System** > **View More**.

Step 8 Select **Expand System Size**.

Step 9 Select **Continue**.
Your system checks connectivity to the virtual machines. If there are connectivity problems with one or more virtual machines, you must fix the problems before you can continue. If there are no connectivity problems, your system performs an automatic backup. When the backup is complete, you are notified that you can proceed with your expansion.

Step 10 Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the original system.

Step 11 Using the vSphere client, deploy the Admin virtual machine for the new system size.
If you are performing an automatic expansion, we create the other virtual machines for your system. If you are performing a manual expansion, you can create the other virtual machines for your system. (See Deploying the OVA File From the VMware vSphere Client, on page 25.)

Step 12 Attach **Hard disk 4** from the original system Admin virtual machine to the Admin virtual machine for the expanded system. (See Attaching an Existing VMDK File to a New Virtual Machine, on page 9.)

Step 13 Power on the Admin virtual machine for the expanded system and write down the deployment URL. If you are performing an automatic expansion, we power on the other virtual machines for your system. If you are performing a manual expansion, power on the other virtual machines for your system.

Step 14 Enter the deployment URL into a web browser and continue the deployment of your expanded system.

Step 15 Select your preferred language for the deployment of the expanded system. (See Selecting Your Language for Setup, on page 28.)

Step 16 Select **Expand the capacity of existing system** > **Next**.

Step 17 Confirm the system size. (See Confirming the Size of Your System, on page 29.)
This system size must be larger than or equal to the original system.

Step 18 Select **Install a primary system**.

Step 19 Select automatic or manual deployment. (See Choosing the Type of Deployment, on page 30.)
If you chose manual deployment, continue to the next step. If you chose automatic deployment:

a) Enter your vCenter credentials so that we can deploy the virtual machines for you. (See Providing VMware vCenter Credentials, on page 30.)
b) Select the ESXi host, data store, and virtual machine port group for the Media virtual machine. (See Choosing vCenter Settings for Your Media and Web Virtual Machines, on page 31.)
c) Enter the fully qualified domain name of the Media virtual machine.
If you have already updated your DNS server with entries for the expanded system, then we look up the IP address for you. (See Entering Networking Information for the Media and Web Virtual Machines, on page 31.)

Use the same OVA file you first used to install the system. Deploy an Admin virtual machine for the new system size.

Your system notifies you when the expansion is complete.

Step 20 If you want public access for your expanded system, then verify that there is a check in the **Create an Internet Reverse Proxy virtual machine** check box. Otherwise, uncheck this check box. (See Adding Public Access to Your System by using IRP, on page 129.)
If you have chosen to add public access:

a) Select the ESXi host, data store, and virtual machine port group for the Internet Reverse Proxy (IRP) virtual machine.

b) Enter the hostname and networking information for the IRP virtual machine.

Step 21 Enter the public VIP address for the WebEx site URL. (See Entering the Public VIP Address, on page 34.)
You can enter the same public VIP address that you use for your original system, or change it to a new IP address. If you change it, then make the necessary updates in the DNS server.

Step 22 Enter the private VIP address for the WebEx site URL. (See Entering the Private VIP Address, on page 34.)
You can enter the same private VIP address that you use for your original system, or change it to a new IP address. If you change it, then make the necessary updates in the DNS server.

Step 23 Enter the WebEx Common site URL. (See Entering the WebEx Common Site and Administration Site URLs, on page 35.)
Participants access this URL to host and attend meetings. This URL resolves to the private VIP address or the public VIP address, depending on whether or not you are using a split-horizon DNS.

You can enter the same WebEx Common site URL that you used for your original system, or change to a new one. If you do change it, then make the necessary updates in the DNS server.

Note If users attempt to use the original URL, those users cannot: After this change is made, system traffic coming from hostnames, other than the ones currently configured, is dropped.

- Host or join meetings
- Log in from web pages, productivity tools, or mobile applications
- Playback recordings

Step 24 Enter the WebEx Administration site URL for administrators to access the Cisco WebEx Administration site. (See Entering the WebEx Common Site and Administration Site URLs, on page 35.)
This URL resolves to the private VIP address.

You can enter the same WebEx Administration site URL that you use for the original system, or change to a new one. If you do change it, then make the necessary updates in the DNS server.

Step 25 Verify that you have made all the networking, DNS server, and firewall configuration changes required for your system. (See Confirming that the Network is Configured Correctly, on page 37.)

Step 26 After your virtual machines have deployed successfully, select **Next** to continue to the system check. (See Deploying Virtual Machines Manually, on page 38.)
Along with the system check, we update the expanded system with any required maintenance release updates to match the software version of the original system. (These updates might take up to an hour.) When complete, the system restarts. (See Checking the System, on page 39.)

Step 27 Select **Restart**.

Step 28 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 29 If you are expanding an MDC system, join it to the MDC system. (See Joining a Data Center to a Multi-Data Center System, on page 264.)

Step 30 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, on page 90.

Meeting service on the data center is restored.

Step 31 Select **Continue**.

The system restarts. You can sign into the Administration site when the restart is completed.

Note If you originally created the virtual machines by using the Cisco WebEx Meetings Server 2.0 OVA file, then you might see a "Cannot access server" error message. If this happens, then use the VMware vSphere client and "Restart Guest" for all the virtual machines in the system.

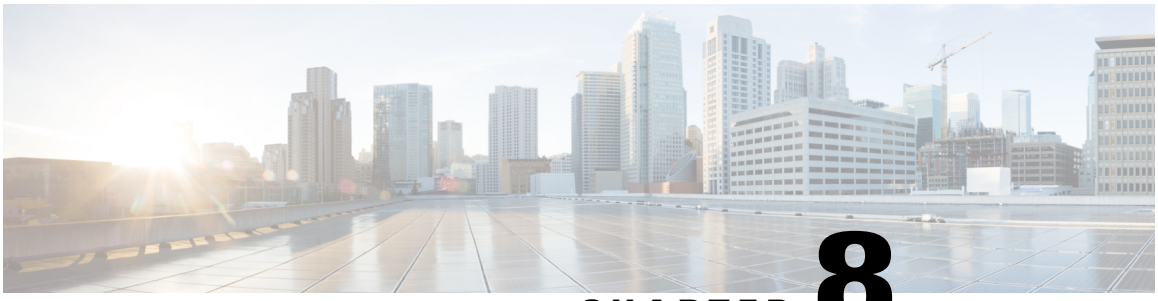
Step 32 Test the expanded system. (See About System Testing, on page 69.)

If the expansion is unsuccessful, then power off the expanded system and power on the original system. If necessary, contact Cisco TAC for further assistance.

Step 33 Rehost the Host licenses or the MDC licenses as appropriate for the expanded system. (See Re-hosting Licenses after a Major System Modification, on page 256.)

What to Do Next

Update the system to the desired MR.



CHAPTER 8

Updating Your System

About Updating a System

In a Single-data Center (SDC) system, the data center must be put into Maintenance Mode. In a Multi-data Center system (MDC), all data centers can be brought down for updating, or in some cases the data centers can be brought down one-at-a-time. The process for bringing data centers down one-at-a-time and maintaining service to the users is referred to as a Zero-downtime Update. Check the release notes for which Cisco WebEx Meeting Server version is eligible for a Zero-downtime Update. If you are performing a Zero-downtime Update, we recommend that you update all other data centers in the system as soon as possible after updating the first data center.

An *upgrade* is defined as a replacement of the system to deploy major modifications that we made to the system. For example, replacing a system currently running version 1.5 to run version 2.0 that includes support for a new operating system. An *update* is defined as overwriting an existing (original) system to take advantage of modifications that we made to improve the system. An *expand* is defined as enlarging an existing system, but not changing the application version. For example, you might update a system from version 1.5 to 1.5MR, upgrade a system from 1.5 to 2.0, or expand a system from 800 users to 2000 users. In all cases, the processes include transferring all of the data from the original system to the updated, upgraded, or expanded system.

The complete update procedure, including backing up your virtual machines, can take up to an hour depending on the following factors:

- System size
- Database size
- Speed of and load on the vCenter

Supported Upgrade Paths

This release of Cisco WebEx Meetings Server supports upgrades from release 1.x to 2.5. The following points apply:

- An upgrade is defined as a replacement of the system to deploy major modifications that we made to the system.
- An update is defined as an incremental modification of the system. Updates deploy fixes and minor improvements.
- All the data from the original system, except for logs and log captures, transfers to the updated or upgraded system.
- When upgrading, you cannot skip a major version of the software and go directly to a companion maintenance release (MR).

  For example, to upgrade from 1.5MR5 to a 2.0MR, *upgrade* from 1.5MR5 to 2.0 and then *update* to the 2.0MR.

Use the following table to determine your upgrade path to Cisco WebEx Meetings Server Release 2.5.

Installed Release	2.5 Release	Path
1.0 to 1.1	2.5	**1** Update to 1.5 **2** Update to 1.5MR3 **3** Upgrade to 2.5
1.5 to 1.5MR2	2.5	**1** Update to 1.5MR3 **2** Upgrade to 2.5
1.5MR3 or later	2.5	Upgrade to 2.5
2.0 to 2.0MR2	2.5	**1** Update to 2.0MR3 **2** Update to 2.5
2.0MR3 or later	2.5	Update to 2.5
2.5 or any 2.5MR Single-data Center (SDC) or Multidata Center (MDC)	Any 2.5MR	Update to the 2.5MR

Note When data centers are deployed, one of the choices is between Audio Encrypted -AE or Audio Unencrypted -AU. Once deployed, systems cannot be converted from one type to the other, nor can data archived or backed up from one type of system be uploaded to the other type of system. When updating or upgrading a system, the audio encryption status cannot be changed. The only way to change a system from one type of audio encryption to another is to deploy a new system.

For more information, see the *Cisco WebEx Meetings Server Administration Guide Release 2.5* at http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html and the *Cisco WebEx Meetings Server Planning Guide and System Requirements Release 2.5* at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

Updating Data Centers

This procedure describes how to update a Single Data Center (SDC) system or a Multi-data Center (MDC) system where the system is taken offline by placing all data centers in Maintenance Mode.

Before You Begin

Place the ISO image in the vCenter datastore and connecting to the CD/DVD as described in Connecting to an ISO Image from the CD/DVD Drive, on page 59.

Step 1 Get the latest update files from Cisco at http://www.cisco.com/cisco/software/navigator.html.
The update package for your system includes an ISO image. You cannot *skip* some versions of the software. For example, you must install the Cisco WebEx Meetings Server version 1.1 (Build 1.1.1.9.A) before applying 1.5MR3. Check the release notes for the correct version to use.

Step 2 Notify other system administrators that they should not access any data center being updated during this procedure. If they do so, their changes are not saved and the result can be unpredictable.

Step 3 Clear your browser cache.
Static resources are cached to enhance the performance of web pages; however, the data cached can be incorrect. Therefore, we recommend that you clear your browser cache.

Step 4 Sign into the Administration sites.
Do not close the browser windows until the data centers are restarted or re-booted, as you might not be able to sign back into the Administration sites.

Step 5 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off, on page 90.
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, on page 88 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 6 Make backups of all of the virtual machines in all data centers in this system (unless you are recovering from a failed update).
(See Creating a Backup by Using VMware vCenter, on page 6.)

Step 7 Select **System**.

Step 8 Select the data center you want to update.

Step 9 Select **Upgrade**.
The **Upgrade System** page appears.

Step 10 Select **Update** > **Continue**.
The **Validate ISO Image** page appears.

Step 11 Select **I have connected to the ISO image and am ready to proceed** > **Continue**.
The ISO image is read for conditions such as down time requirements.

The **Update System** page appears.

Step 12 Select **I have taken backups of all virtual machines on all data center** > **Continue**. Do not close the browser window; otherwise, you will be unable to return to this page.
It might take up to an hour to complete an Update. If you see that the restart button has not yet appeared, verify the update status of the primary data center to confirm that there are no errors in the Update and that the Update is proceeding.

Important Do not shutdown or reboot any data center while another data center is updating; otherwise, it can cause the Update to fail.

Once the Update on all data centers is complete, the **Restart** button appears, confirming the success of the update.

Step 13 Select **Continue**.

Caution Once you select **Continue**, you cannot stop the Update procedure. If an issue arises during the procedure and it does not complete successfully, then you must use your backups to restore all data centers in the system. *Do not close the browser window*, otherwise you will not be able to return to this page. If a browser session is closed or lose connection for any reason, you must check the splash screen of the virtual machines to verify that the update has finished successfully, then reboot the system manually.

Important Do not shutdown or reboot any data center while another data center is updating; otherwise, it can cause the Update to fail.

Once the Update completes a new page appears confirming the success of the Update.

Restart becomes active when all data centers in the system are updated.

Step 14 Select **Restart** to restart the system.
The Cisco WebEx Administration site sign on page appears.

Step 15 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 16 Check the release notes for this update, and determine whether any post-update tasks are required. If additional tasks are required, complete them before you take the system out of Maintenance Mode.

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, on page 90.

Meeting service on the data center is restored.

Step 18 Test the system. See About System Testing, on page 69 for recommended tests.

What to Do Next

We recommend that when you are satisfied with the operation, that you remove all backups.

If the previously deployed Cisco WebEx Meetings Application or Productivity Tools are different versions or build numbers from a newly deployed version of the application, it might be necessary to push the Cisco WebEx Meetings Application or Productivity Tools to the users. See the *Cisco WebEx Meetings Application and Productivity Tools Compatibility Matrix* section of the Cisco WebEx Meetings Server Planning Guide and System Requirements, found at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

Connecting to an ISO Image from the CD/DVD Drive

For the fastest update, we recommend that you mount the ISO image in the vCenter datatstore. However, if you place it in a local disk accessible to the vSphere client, be sure the vSphere client has a hard-wired connection into your company Intranet (not over VPN).

To place the ISO image in the vCenter datastore and connect to the CD/DVD, complete the following steps:

Step 1 Get the desired ISO image from Cisco at http://www.cisco.com/cisco/software/navigator.html.

Step 2 Verify that you have the appropriate permissions.

Step 3 Select the ESXi host for the Admin virtual machine *of the data center to be updated*. Select the **Summary** tab and double-click the **datastore1** name under **Storage**.

Step 4 On the **Datastore and Datastore clusters** window, select **Browse this datastore**.

Step 5 Select the green up arrow icon (Upload file) and load the update ISO file.

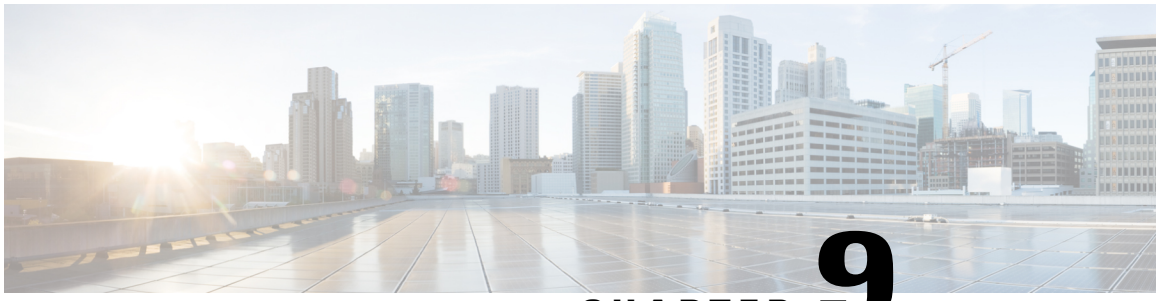
Step 6 Select the Admin virtual machine in the VMware vCenter inventory.

Step 7 Select the **CD/DVD** icon for the Admin virtual machine.

Step 8 Select **CD/DVD drive 1** > **Connect to ISO image** on a local disk or on a datastore.

Step 9 Confirm that the CD/DVD drive is connected.

a) Right-click the Admin virtual machine name in the vCenter inventory and select **Edit Settings...**.
b) In the **Hardware** tab, select **CD/DVD drive 1**.
c) If unchecked, check the **Connected** check box.
d) Select **OK**.



CHAPTER 9

Upgrading Your System

Supported Upgrade Paths

This release of Cisco WebEx Meetings Server supports upgrades from release 1.x to 2.5. The following points apply:

- An upgrade is defined as a replacement of the system to deploy major modifications that we made to the system.
- An update is defined as an incremental modification of the system. Updates deploy fixes and minor improvements.
- All the data from the original system, except for logs and log captures, transfers to the updated or upgraded system.
- When upgrading, you cannot skip a major version of the software and go directly to a companion maintenance release (MR).

  For example, to upgrade from 1.5MR5 to a 2.0MR, *upgrade* from 1.5MR5 to 2.0 and then *update* to the 2.0MR.

Use the following table to determine your upgrade path to Cisco WebEx Meetings Server Release 2.5.

Installed Release	2.5 Release	Path
1.0 to 1.1	2.5	**1** Update to 1.5 **2** Update to 1.5MR3 **3** Upgrade to 2.5

Installed Release	2.5 Release	Path
1.5 to 1.5MR2	2.5	1 Update to 1.5MR3 2 Upgrade to 2.5
1.5MR3 or later	2.5	Upgrade to 2.5
2.0 to 2.0MR2	2.5	1 Update to 2.0MR3 2 Update to 2.5
2.0MR3 or later	2.5	Update to 2.5
2.5 or any 2.5MR Single-data Center (SDC) or Multidata Center (MDC)	Any 2.5MR	Update to the 2.5MR

Note When data centers are deployed, one of the choices is between Audio Encrypted -AE or Audio Unencrypted -AU. Once deployed, systems cannot be converted from one type to the other, nor can data archived or backed up from one type of system be uploaded to the other type of system. When updating or upgrading a system, the audio encryption status cannot be changed. The only way to change a system from one type of audio encryption to another is to deploy a new system.

For more information, see the *Cisco WebEx Meetings Server Administration Guide Release 2.5* at http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html and the *Cisco WebEx Meetings Server Planning Guide and System Requirements Release 2.5* at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

Configuring Your High-Availability System

When you update a high-availability system, you reboot the system. After the reboot process appears to be complete, we recommend that you wait an extra 15 minutes before you begin your add high-availability system procedure.

Important Before you deploy a data center, choose between Audio Encrypted -AE or Audio Unencrypted -AU. After deployment, you cannot convert from one type to the other. Data archived or backed up from one type of system cannot be uploaded to the other type of system. You cannot change the audio encryption type during an upgrade or during an update. The only way to change a system from one type of audio encryption to the other is to deploy a new system.

Before You Begin an Upgrade

In preparation to upgrade a system, either automatically or manually, complete the following tasks:

- Obtain the OVA file required for the upgrade.

Note Upgrading from an unencrypted version to an encrypted version or upgrading from an encrypted version to an unencrypted version is not supported. Obtain the OVA based on your existing system deployment.

- Remove all VMware snapshots of the original (existing) system. Do not take any snapshots during the upgrade process. To remove snapshots, see Removing a Snapshot, on page 8.
- Create a backup for each virtual machine in your original (existing) system. (See Creating a Backup by Using VMware vCenter, on page 6.)
- Plan a maintenance outage. During the upgrade process, the original system is placed into maintenance mode and requires exclusive access to the system. During this time, users cannot access the system for meetings. Schedule this portion of the upgrade for a time that is the least disruptive to your users.
- Plan for the increased size of the data stores. The original system and the upgraded system share data stores until testing of the upgraded system is complete and you remove the original system.
- Verify that the original system hostnames and IP addresses are reused in the upgraded system. Also that the internal virtual machines for both systems are on the same subnet. If you have added public access, the Internet Reverse Proxy virtual machines for the original system and the upgraded system must be on the same subnet.
- Verify that the DNS server can resolve the vCenter hostname. Test the link by pinging the hostname.

Note After an upgrade, **CWMS System** is the default name of the data center; it is not translated to any other language.

Upgrading Your System Automatically

This procedure lists the high-level tasks needed to complete an automatic upgrade. It includes links to sections of the *Cisco WebEx Meetings Server Administration Guide* (at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html) that provide the detailed steps necessary to complete each task.

Before You Begin

Before upgrading a system by using the automatic upgrade process:

- In a Multi-data Center (MDC) environment, the data centers cannot be expanded or upgraded. Secondary data centers must be removed from the MDC, making it a Single-data Center (SDC) environment. The MDC environment can be restored after the data centers are modified and it is verified that the data center sizes and versions match.

- Notify other system administrators that they should not access or make changes to the original system during the upgrade, as their changes might yield unpredictable results.
- Provide and configure one additional IP address and hostname that will be used temporarily for the administration virtual machine on the upgraded system. This can be any available IP address in the VLAN. The hostname can be anything you want, as this IP address and hostname will be released at the end of the upgrade process.

  The original system and the upgraded system are both powered up during this process. The temporary IP address and hostname prevents IP conflicts during this part of the procedure. After the data is transferred from the original system to the modified system, the original system is powered down. At the end of the process, the modified system is taken out of maintenance mode and re-boots.

  During the reboot, the temporary IP address and hostname are released and the modified system uses the original administration virtual machine IP address and hostname.

  If there is a firewall between the administration virtual machines and the IRP virtual machines, the temporary IP address must be allowed through the firewall.
- Do not manually power on or shut down either system.
- Verify that vSwitch is not used on ESXi hosts as a distributed switch. Automatic processes do not support vSwitch Distributed Switch on CWMS ESXi hosts. Change to a standard switch or use a manual process. (See Upgrading Your System Automatically, on page 63, Upgrading Your System Manually, on page 66, or Expanding the System Size, on page 50.)

Step 1 Clear your browser cache.
Static resources are cached to enhance the performance of web pages; however, the data cached can be incorrect. Therefore, we recommend that you clear your browser cache.

Step 2 Go to the license manager on the original system and generate a license request by selecting **System** > **View more** > **Manage Licenses**.
License manager opens in a new tab.

Step 3 Select **Generate License Request**.
A pop-up appears with the license request text. Copy the text and save the license request in a convenient location as it might be necessary to use the manual re-host procedure to reclaim your licenses. This information can also help Cisco to find your licenses. (See Fulfilling Licenses by Using the License Manager, on page 253.)

Step 4 Using the vSphere client, deploy the Admin virtual machine (by using the temporary IP address) for the upgraded system by selecting the configuration with the **Auto-upgrade** suffix, for example `250 Users Admin Auto-upgrade`. Use the same host as the original system Admin virtual machine.

Step 5 Verify that the Upgrade Administration virtual machine can reach the original system disks.
The Administration virtual machines are on the same ESXi host and have access to the same data stores, therefore they should be able to view both sets of disks. The datastore used by the Administration virtual machine datastore (vmdk) files should be visible through the vCenter (by using the same vCenter credentials that the automatic upgrade process uses).

Step 6 Power on the Administration virtual machine for the upgraded system and write down the deployment URL displayed on the virtual machine console.

Step 7 Enter the deployment URL into a web browser URL field.

Step 8 Enter the Administration and vCenter URLs and credentials, so we can deploy the virtual machines for you. (See Providing VMware vCenter Credentials, on page 30.)

Step 9 To deploy any additional virtual machines, select **Continue**.
Until you begin the setup of the upgraded system and the original system is placed in maintenance mode, users can hold meetings, but administrators should not modify the original system virtual machines.

Step 10 Note the names of the automatically-created virtual machines listed in vCenter.
The format for virtual machine names is `CWMS_hostname_MMDDHHmm` where `mm`=minute

When the upgrade is complete, the virtual machines do not display. To find the virtual machines that were created as part of the CWMS upgrade, you can search based on this format.

The progress of the upgrade is displayed on the deployment URL of the upgraded system and on the VMware console connected to the primary system Admin virtual machine. The VMware console provides the deployment URL to use in case the browser window inadvertently closes during the upgrade process.

Step 11 To automatically put the system in maintenance mode and begin the setup of the upgraded system, select **Continue**.
A message displays when Maintenance Mode is enabled, which might take up to 30 minutes.

Step 12 To launch the upgraded Cisco WebEx Administration site, select **Sign In to Administration Site** and sign in.

Step 13 Wait for the system to come to a good state, then turn off maintenance mode on the upgraded system and select **Continue**.
It can take a few minutes for the meeting service to become available. Your system is ready for users to start meetings when all the virtual machines listed on the **System Properties** page display a status of Good (green). See Turning Maintenance Mode On or Off, on page 90.

The system reboots.

Step 14 Test the upgraded system. (See About System Testing, on page 69.)
When your upgraded system is running satisfactorily, you can delete your original system to free the original system resources. Keep the upgraded system running while deleting the original system to prevent the accidental removal of the Hard disk 4 base VMDK file that might be accessed by the upgraded system.

If the upgrade is unsuccessful, power off the upgraded system, power on the original system, and contact Cisco TAC.

Step 15 Re-host and update the license version as appropriate for the upgraded system. (See About Host Licenses, on page 250 and Re-hosting Licenses after a Major System Modification, on page 256).
If the previously deployed Cisco WebEx Meetings Application or Productivity Tools are different versions or build numbers from a newly deployed version of the application and the upgrade is not blocked, you are notified by an upgrade warning dialog box. It might be necessary to push the Cisco WebEx Meetings Application or Productivity Tools to the users. See the *Cisco WebEx Meetings Application and Productivity Tools Compatibility Matrix* section of the Cisco WebEx Meetings Server Planning Guide, found at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

Within 180 days or less the license-free grace period shall expire. If the original system had valid licenses, those licenses must be re-hosted in 180 days or less. If the original system was operating in the license-free grace period, the remaining unexpired days are transferred to the upgraded system.

What to Do Next

If the previously deployed Cisco WebEx Meetings Application or Productivity Tools are different versions or build numbers from a newly deployed version of the application and the upgrade is not blocked, you are

notified by an upgrade warning dialog box. It might be necessary to push the Cisco WebEx Meetings Application or Productivity Tools to the users. See the *Cisco WebEx Meetings Application and Productivity Tools Compatibility Matrix* section of the Cisco WebEx Meetings Server Planning Guide and System Requirements, found at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

Upgrading Your System Manually

This procedure lists the high-level tasks needed to complete a manual upgrade. It includes links to sections of the *Cisco WebEx Meetings Server Administration Guide* (at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html) that provide the detailed steps necessary to complete each task.

Before You Begin

In a Multi-data Center (MDC) environment, the data centers cannot be expanded or upgraded. Secondary data centers must be removed from the MDC, making it a Single-data Center (SDC) environment. The MDC environment can be restored after the data centers are modified and it is verified that the data center sizes and versions match.

Verify that the upgraded system can access the disks for the original system Admin virtual machine. (Hard disk 4 is copied from the original system to the upgraded system.)

Do not power on and run both systems at the same time, because the hostnames and IP addresses from the original virtual machines are used in the upgraded system.

Step 1 Clear your browser cache.
Static resources are cached to enhance the performance of web pages; however, the data cached can be incorrect. Therefore, we recommend that you clear your browser cache.

Step 2 Go to **System** > **(Licenses) View More**.
The **License** window opens.

Step 3 Go to the license manager and generate a license request by selecting **Manage Licenses**.
License manager opens in a new tab.

Step 4 Select **Generate License Request**.
A popup appears with the license request text. Copy the text and save the license request in a convenient location as it might be necessary to use the manual rehost procedure to reclaim your licenses. This information can also help Cisco to find your licenses. (See Fulfilling Licenses by Using the License Manager, on page 253.)

Step 5 Log in to the Administration site of the original system.

Step 6 Go to the System tab and select **Upgrade**.

Step 7 Select **Major Upgrade**.

Step 8 Select **Continue** to archive the original system data and put the system into maintenance mode.

Step 9 Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the original system.

Step 10 Deploy all of the upgraded system virtual machines, including the high availability (HA) and Internet Reverse Proxy (IRP) virtual machines.
If you are deploying a Multi-data Center (MDC), do not deploy a HA machine; MDC does not support HA.

During deployment there is an option to **Power on VM after deployment**. Verify that this is *not* checked or that the VMs have been started manually before the next step is complete; otherwise, it will cause the VMs to deploy as a new

system and create a new deployment instead of migrating the data. If the VMs are powered on, they must be deleted and redeployed before proceeding.

Step 11 Copy the data from your original system to the Admin virtual machine for the upgraded system. (See Attaching an Existing VMDK File to a New Virtual Machine, on page 9.)

Step 12 Power on the upgraded Admin virtual machine and write down the deployment URL displayed on the virtual machine console. (See Adding a High Availability System.)
If the system includes HA, do not set up the HA virtual machines from HA Admin Deployment; allow the upgrade script to discover the HA virtual machines.

Step 13 Power on the other upgraded virtual machines.

Step 14 Enter the deployment URL into a web browser.

Step 15 Select **Continue** to launch the system setup.
The progress of the upgrade is displayed on the deployment URL of the upgraded system and on the VMware console connected to the primary system Admin virtual machine.

The VMware console provides the deployment URL to use in case the browser window inadvertently closes during the upgrade process.

Step 16 Wait for the system to come to a good state, then turn off maintenance mode and select **Continue**.
It can take a few minutes for the meeting service to become available. Your system is ready for users to start meetings when all the virtual machines listed on the **System Properties** page display a status of Good (green). See Turning Maintenance Mode On or Off, on page 90.

Step 17 Test the upgraded system. (See About System Testing, on page 69.)
When your upgraded system is running satisfactorily, you can delete your original system to free the original system resources. Keep the upgraded system running while deleting the original system to prevent the accidental removal of the Hard disk 4 base VMDK file that might be accessed by the upgraded system.

If the upgrade is unsuccessful, power off the upgraded system, power on the original system, and contact Cisco TAC.

Step 18 Rehost and update the license version as appropriate for the upgraded system. (See About Host Licenses, on page 250 and Re-hosting Licenses after a Major System Modification, on page 256).
If the previously deployed Cisco WebEx Meetings Application or Productivity Tools are different versions or build numbers from a newly deployed version of the application and the upgrade is not blocked, you are notified by an upgrade warning dialog box. It might be necessary to push the Cisco WebEx Meetings Application or Productivity Tools to the users. See the *Cisco WebEx Meetings Application and Productivity Tools Compatibility Matrix* section of the Cisco WebEx Meetings Server Planning Guide, found at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

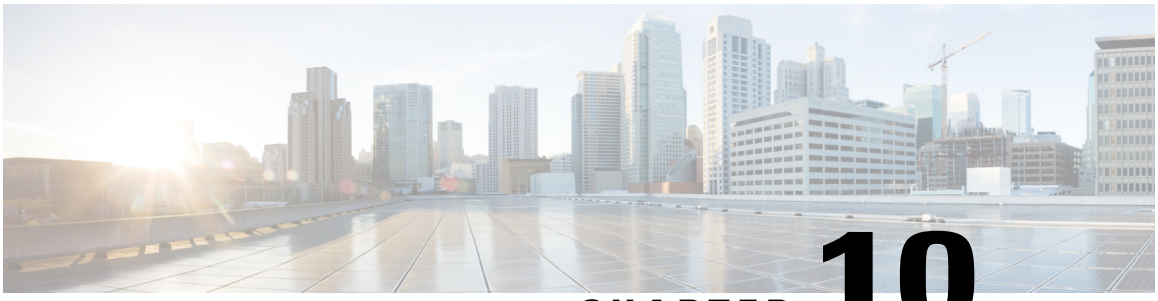
Within 180 days or less, the license-free grace period shall expire. If the original system had valid licenses, those licenses must be rehosted in 180 days or less. If the original system was operating in the license-free grace period, the remaining unexpired days are transferred to the upgraded system.

Step 19

What to Do Next

If the previously deployed Cisco WebEx Meetings Application or Productivity Tools are different versions or build numbers from a newly deployed version of the application and the upgrade is not blocked, you are notified by an upgrade warning dialog box. It might be necessary to push the Cisco WebEx Meetings Application or Productivity Tools to the users. See the *Cisco WebEx Meetings Application and Productivity Tools Compatibility Matrix* section of the Cisco WebEx Meetings Server Planning Guide and System

Requirements, found at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.



CHAPTER 10

Testing Your System

About System Testing

Most of the system test are accomplished by using the CWMS system, for example by Using the Meetings Test, on page 70 and Using the System Resource Test, on page 70.

When testing an upgraded system, you can keep the original system until you have finished testing the upgraded system (but because they share some parameters, such as IP addresses, you cannot power on both systems at the same time). Once you are satisfied with the results of the upgraded system tests, you can remove (forever) the original system. Be sure your upgraded system is running when removing the original system. This prevents accidental removal of the base virtual machine disk (VMDK) file that must be accessed by the upgraded system.

Some of the recommended tests to run on the system are.

- Add, edit, activate, and deactivate users. (See Managing Users, on page 95.)
- Schedule and hold a meeting.
- Reschedule an existing meeting.
- Delete a series of scheduled meetings.
- Add and open a meeting attachment from the meeting invitation.
- Record a meeting and play back the recording.

The system can also be tested by:

- Confirming that the Network is Configured Correctly, on page 37
- Checking the System, on page 39
- Confirming that the primary system will failover to the HA system by removing the physical connection to the primary system and verifying that Cisco WebEx is running on the HA system.

Using the Meetings Test

Step 1 Sign in to the Administration site.

Step 2 Select **Support** > **Meetings Test**.

Step 3 Select **Next**.
Your system runs a meetings test, verifying its ability to schedule, start, and join a meeting. The results of the test appear within a few minutes.

Using the System Resource Test

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, on page 90.
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, on page 88 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 **Support** > **System Resource Test**.

Step 4 Select **Next**.
The results of the test are posted for the following:

- CPU, memory, network, and storage for each host on your system
- Internal and external connectivity checks for your site and administration URLs

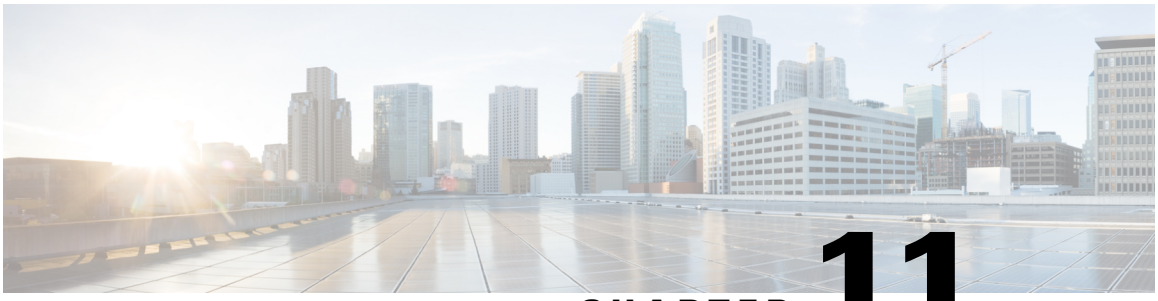
Step 5 Turn off Maintenance Mode.
When you turn off Maintenance Mode, the system determines whether a restart or a reboot is required, and displays the appropriate message. A restart takes approximated 3 to 5 minutes and a reboot takes approximately 30 minutes. If the data center is part of a Multidata 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, on page 90.

Meeting service on the data center is restored.

PART II

Cisco WebEx Meetings Server Configuration



CHAPTER 11

Using Your Dashboard

About the Dashboard

The dashboard is the home page of the administration site and provides several parameters and graphs key monitoring features.

The dashboard includes the following sections:

- System Monitor—Displays the system status and time stamp and includes the following subsections:
  - Meetings and Users—Status of meetings in progress and usage. Displays the number of meetings currently in progress and the number of *distinct* participants (usage). The status LED indicates whether the meetings in progress and usage are under or over the configured alarm threshold. A green status LED indicates under the configured threshold while red indicates over the configured threshold. See Viewing and Editing Alarms, on page 77 for more information about configuring alarms.
  - Alarm icon—Select the Alarm icon to view and edit the alarm threshold settings you have configured. Alarm thresholds are displayed on the **Alarms** page in numerical form. By default, alarm thresholds are displayed as a percentage. See Viewing and Editing Alarms, on page 77 for more information about configuring alarms.

    You can configure alarms for the following:
    - Meetings In Progress—Indicate when current meetings are experiencing issues.
    - Usage—Total number of distinct users using the system. Occasionally participants are in multiple sessions, but participants are only counted once.
    - Storage—Recording and database backup storage space used.

Note The storage alarm appears if you have configured a storage server. See Adding an NFS or SSH Storage Server, on page 146 for more information.

Meeting recording is disabled if the storage usage is over the threshold.

- Log Partition—Amount of space used to store the Application Audit Log.

Note If an Auditor is configured for your system, this alarm is only visible to the Auditor.

- License Usage—Percentage of permanent licenses assigned to host users.
- Grace Licenses—Indicates whether grace licenses are assigned to host users.

- Data Center—Lists the name of each data center, whether Maintenance Mode is on or off, the amount of storage used for each data center, and the status of data replication. See About the Data Center Information Displayed on the Dashboard, on page 75 for more details.
- Meeting Trend—A graph of the number of meetings held on the system during a specified time. Use the **From** and **To** fields to set the time for the meeting trend information and for the meetings displayed in the Meetings list. You can select a point on the Meeting Trend graph to list the meetings on the Meetings list that occurred during the time specified on the graph. To view meetings that occurred during a specific time of day, mouse over the graph and select the desired time.
- Meeting Search—Find a meeting by entering specific search criteria, such as meeting number, meeting topic, or a date range.
- Meetings—The total number of meetings that occurred during the selected time, the meeting topics, hosts, numbers of participants, and the state of the meeting. If a data point has not been selected from the Meeting Trend graph, all meetings for the time period are shown. You can sort each column of information in the Meetings list, and the meetings are displayed in order by state: In progress, Ended, and Not started.

  Selecting a **Meeting Topic** in the list displays details of the meeting, including: Meeting number, start time, end time, general status, and indicates if the meeting has been analyzed in detail. Prior to analysis, the Status parameter shows the overall status of the meeting as it relates to quality. Select **Analyze Meeting Detail** to perform a detailed analysis of the meeting and generate a log. After the log has been compiled, the general Status of the meeting might change based on the detailed investigation performed by the analysis. The date and time the log was generated is displayed and you are sent email with the log file download information. You can also download the log from the dashboard by selecting **Download Log**.

Note If a meeting is not attended by the meeting host, the meeting is terminated 30 minutes after last participant exits the meeting, regardless of the scheduled end time, and shows as being in progress until this time expires.

- Maintenance—Schedules a maintenance window announcing when maintenance mode will be turned on and off. See Scheduling a Maintenance Window, on page 86 and About Maintenance Mode, on page 88 for more information.
- Last System Backup—Time and date that the last backup was taken; the filename, size, and location of the backup; and the date and time of the next backup. It also notifies you if the backup failed and the date of the first backup attempt if one has not been created yet. A separate backup link is provided for each data center.

Note Only appears if you have configured a storage server.

- System—Displays the maximum number of users who can simultaneously participate in meetings, the version number, product URL, whether public access is allowed, if it is a high availability system, and the number of user licenses. Select **View More** to go to Configuring Your System, on page 125.
- Users—Displays the number of active users, whether Directory Integration is configured, when the next synchronization will occur (if configured), and the selected type of authentication. Select **View More** to go to Editing Users, on page 112.
- Settings—Shows the maximum number of participants allowed in each meeting, audio type, and whether or not WebEx HQ video is enabled. Select **View More** to go to Configuring Settings, on page 163.

About the Data Center Information Displayed on the Dashboard

The System Monitor section of the dashboard displays status information for the data centers that comprise your system. If you have a single data center system, the data center name automatically assigned by the system is **CWMS System**, but the status information is dynamically updated for the single data center. In a multi-data center system, each data center is listed in a separate row by the name you entered during the join data center process and the status information is dynamically updated separately and displayed for each data center.

- Status—This column displays the status of each data center. Status can be Good, Partial Service, Blocked, or Down.
  - Good—All components of the data center are working properly. No system-generated email messages sent to the administrator.
  - Partial Service—Some of the components of the data center are not working properly, but the data center is providing service. The system sends an email to the administrator indicating that this data center needs attention.
  - Blocked—The system has blocked service on this data center and is redirecting all activity to another data center. The system sends an email to the administrator to indicate that service is down, data is being redirected to another data center, and this data center needs attention.
  - Down—The operation of a data center has degraded to the point where it can no longer provide reliable service and failover to an operational data center is in progress. The system sends an email to the administrator to indicate that service is down, data is being redirected to another data center, and this data center needs attention.

In a Multi-data Center (MDC) environment, some components are capable of cascading, so the disabled service on this data center might be provided by another data center. This is not an indication of overall system status; it applies only to the status of this data center.

- Blocked or Down and Maintenance Mode is on—The data center status continues to show that the data center is blocked. When Maintenance Mode is turned off AND all components are again up and running, the status changes.
- Unreachable—Another data centers cannot communicate with this data center. The system sends an email to the administrator asking them to check the network connectivity between the data centers.

- Maintenance—Indicates whether a data center has Maintenance Mode turned On or Off.
- Storage—The amount of storage used on the storage server connected to each data center. **Not Configured** displays If a storage server is not connected to the system.
- Data Replication—Indicates whether data replication is occurring between the data centers in an MDC system.

When a data center is in the Blocked or Down state, users might experience the following:

- In-progress meetings are automatically moved to an operational data center after a few minutes; similar to what happens in a failover situation. There is no impact on PCN or Blast Dial meetings.
- Previously scheduled meetings that have not started move to the operational data center. No other actions are required for the host or participants.
- Users sign in to a WebEx site URL in the usual manner, but the system redirects the sign-in to the operational data center.
- Administrators can sign in to the blocked data center as well as the operational data center.
- Administrators receive a system-generated email which explains which data center is in the blocked state, and information explaining some of the possible causes.

Monitoring CPU, Memory, and Network Usage

To monitor CPU, memory, and network usage, we recommended that you use the performance tab of each CWMS virtual machine in vSphere client or vSphere Web client. The advantage to monitoring performance a of CWMS virtual machines by using vSphere client or vSphere Web client is that each virtual machine can be monitored separately and for a specified period of time. If an issue that affects the system negatively exists, it is easier to precisely troubleshoot.

To monitor CPU usage refer to http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.monitoring.doc%2FGUID-FC93B6FD-DCA7-4513-A45E-660ECAC54817.html. Variations and spikes in CPU usage is expected; however, during general system use all levels should be less than 90 percent.

To monitor Memory usage refer to http://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.monitoring.doc/GUID-C442423F-18CD-4F01-914E-286ED6C72BC6.html. During normal operation Memory usage should be stable. Some variations are expected, but an increasing trend over a long period of time might indicate a pending issue that will soon affect system performance.

To monitor Network usage refer to http://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.monitoring.doc/GUID-41B7E742-B387-4638-A150-CB58E2ADD89F.html.

Network usage can vary widely in reference to a CWMS virtual machine, and spikes in network usage (for example during a backup) are expected.

Viewing and Editing Alarms

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 the alarm **icon**.
The **Alarms** page appears.

Step 3 To modify, activate, or deactivate alarm thresholds, select **Edit**.
The **Edit Alarms** page appears. Select **Percentage %** to view the alarm threshold as a percentage or **Number #** to view the alarm threshold as a number. The default setting is **Percentage %**.

Step 4 Select the check boxes for the alarms that you want enabled and select the interval for each enabled alarm.

Option	Description
Meetings In Progress	Meetings in progress alarm threshold. • If set to **Percentage %**, move the selector bar to set from 2 to 99 percent. • If set to **Number #**, enter a number from 2 to 99 percent. **Default**: Selected with an interval of **one hour**.
Usage	System usage alarm threshold. • If set to **Percentage %**, move the selector bar to set from 2 to 99 percent. • If set to **Number #**, enter the number of users. **Default**: Selected with an interval of **12 hours**.
Storage	Storage threshold in GB. The maximum storage threshold is calculated as (the total space–recording buffer size). The size of the recording buffer depends on the size of your system [50-user (1 GB), 250-user (5 GB), 800-user (16 GB), or 2000-user (40 GB)], the number of Cisco WebEx meetings held, and the length of the recorded meetings. Larger user systems (800– and 2000–user systems) require more storage to accommodate larger database backups. In general, plan to provide enough storage space for three backup files. • If set to **Percentage %**, move the selector bar to set from 2 to 99 percent. • If set to **Number #**, enter the number of gigabytes. **Default**: Not selected. Interval is **one hour**. **Note** This section appears only if you have configured a storage server. Recording is disabled if the storage usage exceeds this threshold. See Adding an NFS or SSH Storage Server, on page 146 for more information.

Option	Description
Log Memory Usage	Amount of disk space used for logs. If a user is configured as an Auditor during system deployment, this alarm is visible and configurable only by the Auditor on the **Auditing** tab. If your system does not have an Auditor role, an Administrator, SSO Administrator, or LDAP Administrator can see and configure this alarm. • If set to **Percentage %**, move the selector bar to set from 2 to 99 percent. • If set to **Number #**, enter the number of gigabytes. Set the **Interval** to indicate how often the system checks log memory usage.
License Usage	Permanent license use. • If set to **Percentage %**, move the selector bar to set from 2 to 99 percent. • If set to **Number #**, enter the number of gigabytes. Set the **Interval** to indicate how often the system checks the number of assigned licenses.
Grace Licenses	Grace license use. Select **Notification was sent to the Grace license holder** to send notifications to users when one of the selected conditions is met: • A user is assigned a Grace license. • A Grace license assigned to a user is expired. • All Grace licenses are assigned.

An email is sent to administrators when an alarm exceeds a threshold. The interval is used to suppress multiple alarms within the specified time to avoid sending too many emails about the same issue.

Step 5 Select **Save**.
Your alarm settings are saved and the **Alarms** page is updated with your changes.

Viewing Meeting Trends

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 Above the **Meeting Trend** graph set a trend period by selecting the **From** and **To** date and time.

- You can view meeting trend data from the four previous months, the current month, and one month in the future.

- Meetings scheduled before midnight and extending to the following day are displayed on the graph by the meeting start date.
- If a meeting is disconnected due to a system problem and then reconnected, it is counted twice on the Meeting Trends graph.
- Meeting trend data for one-month and six-month views is based on Greenwich Mean Time (GMT) and is therefore not accurately displayed over a 24-hour period. For example, if your system hosts 200 meetings during a given day, the database records the occurrence of those meetings based on GMT and not local time. Meeting trend data for one-day and one-week views are based on the user's time zone.
- A green track indicates meetings that are in progress or that have ended. Future meetings are shown in yellow.
- If the selected time range is 24 hours, the data points for passed or in-progress meetings are in five-minute intervals and future meetings are in one-hour intervals.
- If the selected time range is longer than one day but shorter than or equal to one week, the data points for passed, in progress, or future meetings are in shown in one-hour intervals.
- If the selected time range is longer than one week, the data points for passed, in progress, or future meetings are shown in one-day intervals.

The **Meeting Trend** graph shows the total number of meetings that occurred during the selected time period. The **Meetings** list below the graph lists all the meetings during the selected trend period.

Note Some meeting trend entries might appear to be duplicated, because they have the same name. An entry is created every time a meeting is started. Therefore, if a meeting is started, stopped, and restarted, multiple entries with the same meeting name are shown.

Step 3 To view a list of meetings that occurred at a particular time:

a) Click a particular location on the **Meeting Trend** graph to list the meetings that occurred within 5 minutes of the selected time in the **Meetings** list below the graph. See Viewing the Meetings List, on page 79 for more information.

b) Select the graph symbol below the **From** and **To** fields to display a list of date and times when meetings occurred between the From and To period. Then select a date from the drop-down list.
The data points shown in the drop-down menu are the same as those shown on the graph. They are made accessible primarily for the benefit of users with a keyboard and screen reader.

Mouse over the graph to see the total number of meetings that occurred at that time.

What to Do Next

- See Viewing the Meetings List, on page 79 to view more information about a meeting.
- See Finding a Meeting, on page 81 for more information about using the **Meeting Search** tab.

Viewing the Meetings 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 Above the Meeting Trend graph set a trend period by selecting the **From** and **To** date and time.
By default, the Meetings list displays the meetings for the current 24-hour period. See Viewing Meeting Trends, on page 78 for more information.

By default the Meetings list displays meetings in the order of their scheduled start time.Meetings are displayed in order of status: In Progress, Ended, Not Started. Information displayed in the Meetings list includes:

- Time range selected in the trend chart
- Meeting Topic
- Host 's name
- Number of participants
- State of the meeting: In Progress, Ended, Not Started

Note A status icon displays in the first column to indicate the state of the meetings that are in-progress or have ended as *good (green)*, *fair (yellow)*, or *poor (red)*.

- Fair (yellow) indicates the audio/video delay or jitter taking place during the meeting has reached a minor threshold and should be monitored and investigated to determine the cause.
- Poor (red) indicates the audio/video delay or jitter taking place during a meeting has reached a major threshold.
- If the majority of the meetings displayed in the Meetings list indicate a status of poor, then contact the Cisco Technical Assistance group (TAC) for assistance.
- The following table provides more details for the different meeting status indicators.

Category	Good	Fair	Poor
Data Round Trip Time	Less than 3000 ms.	3000–5999 ms.	6000 ms. and higher
Audio Round Trip Time	Less than 100 ms.	100–299 ms.	300 ms. and higher
Audio Packet Loss	Less than 5 percent	5–9 percent	10 percent and higher
Audio Jitter	Less than 100 ms.	100–499 ms.	500 ms. and higher
Video Round Trip Time	Less than 100 ms.	100–499 ms.	500 ms. and higher
Video Packet Loss	Less than 20 percent	20–49 percent	50 percent and higher
Video Jitter	Less than 100 ms.	100–499 ms.	500 ms. and higher

Step 3 (Optional) Select a column heading to sort the meetings.

Step 4 Use the pagination function to view the next or previous page.

- A maximum of 10 meetings display on each page.

- You might see duplicate meeting entries in the Meetings list. A meeting entry is created every time a meeting is started. Therefore, if a meeting is started, stopped, and restarted, multiple meeting entries with the same name are displayed in the list.

Step 5 Select a **meeting topic** in the Meetings list to display more meeting information.
The list expands to show meeting details, such as the names of the participants, the start and end time, and the meeting status.

- Select **time stamp** to go to the **Meeting Analysis Report** page.
- Select **Download Log** to download the System Information Capture (Infocap) Log to your local drive.

Step 6 (Optional) To refine your search, select the **Meeting Search** tab.
Additional search fields appear.

What to Do Next

- See Viewing a Meeting Analysis Report, on page 82 for more detailed meeting information.
- See Downloading Cisco WebEx Meeting Logs, on page 84 to download a compressed file with several meeting logs. Use these logs to troubleshoot issues that participants experienced during a meeting.
- See Finding a Meeting, on page 81 to refine your search results or find a specific meetings.

Finding a Meeting

Step 1 Sign in to the Administration site.

Step 2 In the Meeting Trend section, select the **Meeting Search** tab.

Step 3 Enter your search criteria.
Search for meetings by using some or all of the following fields:

- Meeting Number or Host Name
- Status—Select All, Good, Fair, or Poor from the drop-down menu.
- Meeting Topic—You can enter the first few letters of the meeting topic to find all meetings with similar topics.
- From Date and Time—Use the calendar icon and drop-down menu to select the date and time.
- To Date and Time—Use the calendar icon and drop-down menu to select the date and time.

Step 4 Select **Search**.
The **Search Results** lists the meetings that match the search criteria.

Step 5 To start another search, select **Clear**.
The system clears the search fields, but the results from the previous search remain in the **Search Results**.

Step 6 Select a **meeting topic** in the Meetings list to display more meeting information.
The list expands to show meeting details, such as the names of the participants, the start and end time, and the meeting status.

- Select **time stamp** to go to the **Meeting Analysis Report** page.
- Select **Download Log** to download the System Information Capture (Infocap) Log to your local drive.

What to Do Next

To view additional meeting information, see Viewing a Meeting Analysis Report, on page 82.

To download a zipped file with meeting logs, see Downloading Cisco WebEx Meeting Logs, on page 84.

Viewing a Meeting Analysis Report

Additional information about a Cisco WebEx meeting and its participants is available on the **Meetings Analysis Report** page.

Before You Begin

One or more meetings are displayed in the Meetings list on the **Meeting Trend** tab. See Viewing the Meetings List, on page 79 for details.

Step 1 Select a **meeting topic** displayed in the Meetings list on the Meeting Trend tab.

Step 2 In the Meetings list, select **Analyze Meeting Detail**.
While the system is processing the information, the date and time the system started generating the information is displayed with a status of Pending. When the system is finished generating the information, the date and time become an active link and the Pending status changes to a Download log active link.

Step 3 Select the **date and time** link to view the **Meeting Analysis Report** page.
The following information displays:

- Meeting Topic
- Host's email address
- Status—Current status of the meeting. Values: Not Started, In-Progress, Ended.
- Start Time—Date and time the meeting started.
- End Time—Date and time the meeting ended.
- Online Meeting ID—The meeting ID assigned to the online portion of the meeting.
- Join Before Host—Indicates whether participants are allowed to join the meeting before the meeting host.
- Data Center—Shows the name of the data center used for the meeting. In a single data center environment, the name is always CWMS System.
- Meeting Number—A 9-digit number assigned to the meeting.
- Health—The general health of the meeting. Values can be Normal, Fair, or Poor.
- Scheduled Start Time—The date and time the meeting was scheduled to begin.
- Scheduled End Time—The date and time the meeting was scheduled to end.

- Audio Meeting ID—The meeting ID assigned to the audio portion of the meeting.
- Audio Meeting Started First—Indicates whether the audio portion of the meeting was started before the online portion of the meeting.

Note When the system refreshes the window, the meeting details are closed. Select the meeting topic again to display the date and time or Download log links.

Step 4 Select the **Meeting Messages** tab to display the Function, Time, and Messages generated during a meeting.

Step 5 Select the **Participants** tab to display the following information for each meeting participant:

- Participant's name
- Join Time
- Browser
- Client IP address—IP address of the WebEx site.
- Leave Time—Time the participant left the meeting.
- Leave Reason—Reason for leaving a meeting. Values are Normal or Timeout.
- Phone Number—Number of the phone that participants use to attend the meeting.
- VoIP Latency
- Audio QoS—Quality of the audio during the meeting. Values are Normal or Bad.
- Video QoS—Quality of the video during the meeting. Values can be Normal or Bad.
- Client Latency—Latency from the meeting client to the Data Meeting server. Values can be Normal or Bad.
- Hosting Server—Name of the virtual machine that hosted the meeting. It is part of the fully-qualified domain name (FQDN) of the virtual machine that hosted the meeting. For example, if a micro VM FQDN is `susmicro-vm.orionqa.com`, then `susmicro-vm` is displayed.

What to Do Next

See Downloading Cisco WebEx Meeting Logs, on page 84 to download a compressed file with several meeting logs.

Downloading Cisco WebEx Meeting Logs

While a Cisco WebEx meeting is in-progress or when a meeting has ended, you can download system-generated meeting logs that provide information for troubleshooting an issue users experienced during a meeting.

Step 1 Sign in to the Administration site.

Step 2 Select the Meeting Trend tab, then select a **From** and **To** range to display a graph of meetings that occurred during the selected time frame.

Step 3 Click a particular location on the **Meeting Trend** graph to list the meetings that occurred within 5 minutes of the selected time in the **Meetings** list below the graph.

Step 4 Select a **meeting topic** in the **Meetings** list.
Information about the selected meeting display below the meeting topic.

Step 5 Select **Download logs**.

What to Do Next

See About Meeting Logs, on page 84 for more information about the downloaded meeting logs.

About Meeting Logs

Your downloaded Meeting Logs compressed file contains the following logs:

Data Conference Log

This log contains information about the online portion of a meeting.

- Conference ID
- Meeting ID
- Scheduled Start Time
- Start Time
- End Time
- Host Email Address
- Site URL
- Meeting Type—Meeting client
- Meeting Name—The meeting topic.
- Primary Call-in Number
- Secondary Call-in Number
- Delete Meeting When Ended—Indicates whether this meeting is deleted from the Meetings details page when the meeting ends.
- Meeting Status

- Application Sharing—indicates whether the application sharing feature was used during a meeting.
- Regular Telephony—Indicates whether participants called the meeting using telephones.
- Hybrid Telephony
- Eureka Video
- Eureka VoIP
- MMP VoIP
- Hybrid VoIP
- MMP Video
- NBR2
- Mobile
- Audio Broadcast
- Audio Broadcast for Mobile

Multimedia Log

This log provides information about audio streaming, audio switching, and SVC stream adaptation to the meeting client as it relates to MMP.

- Meeting Name
- Conference ID
- Session Type
- Participants
- Total Join
- MCS Server
- Start Time
- End Time
- Duration

Teleconference Log

This log contains information about a teleconference meeting.

- TeleConf ID
- App Server
- Callers
- Callback
- Call-in
- Start Time

- End Time
- Duration
- Description
- Account Type

Web Join Event Log

This log contains information about the web join events.

- Meeting Name—Displays the meeting topic.
- Conference ID—Data conference instance ID.
- Site ID—The name of the Cisco WebEx site.
- Participants—Total number of participants that joined the meeting from a Web browser.

Note The host that starts the meeting is not included in this total.

- Total Join—The total number of people who joined the meeting.
- Start Time—Starting date and time of the meeting.
- End Time—Ending date and time of the meeting.
- Duration—Amount of time, in minutes, the meeting lasted.
- End Reason—Reason the meeting ended.

Scheduling a Maintenance Window

When you turn on Maintenance Mode, all in-progress meetings end and the Meet Now function becomes unavailable. Before you perform system maintenance for a Single Data Center system, schedule a maintenance window and notify users in advance. Inform users that during a maintenance window, meetings currently in progress are terminated and that they cannot schedule meetings that overlap the maintenance window. If you are running a Multi-data Center system and only one system is put into Maintenance Mode, meetings transparently failover to the active system and there is no need to notify users.

For example, an administrator wants to bring a Single Data Center system down for one hour for maintenance. The administrator can try to schedule a time when no meetings appear to be scheduled. If meetings are scheduled, the administrator should notify the meeting hosts about the maintenance window. Hosts can then reschedule their meetings for another time, outside of the maintenance window. If a host tries to hold a scheduled meeting anyway, it will be terminated.

If the planned tasks require an extended period of time to complete, such as uploading a new Certificate Authority (CA) certificate, schedule a longer maintenance window. For example, when you schedule your maintenance window, specify a start time of 30 minutes before you plan to turn on Maintenance Mode. This allows a grace period for all meetings to end gracefully. Also we recommend that you add an hour to any maintenance window. The extra time allows the system to become functional after the reboot that might occur. You might also want to start one or more instant meetings to test the modified settings, before the users attempt to schedule or host meetings.

While some system maintenance tasks do not require that you turn on Maintenance Mode, the tasks that do require extra time to complete a restart or a reboot, after you turn off Maintenance Mode. A system restart takes only a few minutes (approximately 3-5 minutes), but a reboot takes approximately 30 minutes. See Turning Maintenance Mode On or Off, on page 90 for more details.

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 **Schedule Maintenance**.
The **Schedule Maintenance Window** displays.

Step 3 Use the calendar tool and the time drop-down menu to select the date and start time for the maintenance window.

Step 4 Enter the duration of the maintenance window by specifying the number of hours and minutes.

Step 5 Select **Schedule**.
When the maintenance window begins, users receive an error message if they attempt to schedule a meeting that falls within the scheduled maintenance window. Scheduling a maintenance window does not automatically put the system into Maintenance Mode; that must be done by an administrator.

The scheduled maintenance window date, start time, and duration displays in the Maintenance pane.

What to Do Next

See Emailing Users, on page 123 for details about notifying users of system maintenance events.

Changing a Scheduled Maintenance Window

After you schedule a maintenance window, you can reschedule the date and time or delete it.

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 **Dashboard**.

Step 3 Select the displayed system maintenance date and time.

Step 4 On the **Schedule Maintenance Window**, you can:

- Enter a different start date and time.
- Modify the duration hour and minutes.
- Select **Delete** to remove the maintenance window.

If you finish your system maintenance early, you can either reduce the duration time or select **Delete** on the **Schedule Maintenance Window**.

What to Do Next

Turn on Maintenance Mode before you modify system properties. See About Maintenance Mode, on page 88 for information about which system properties require Maintenance Mode to be turned on.

About Maintenance Mode

Many configuration changes require that you put your system into Maintenance Mode. Maintenance Mode shuts down all conference functionality on a data center, so you should alert users by scheduling the maintenance windows (see Scheduling a Maintenance Window, on page 86).

For more information, see Turning Maintenance Mode On or Off, on page 90.

Putting a data center in Maintenance Mode does the following:

- Disconnects users and closes all meetings. If you put a data center that is part of a Multi-data Center (MDC) system into Maintenance Mode, meetings in progress fail over to the active data center.
- Prevents users from signing in from web pages, the Outlook plug-in, and mobile applications. Emails are automatically sent when the system is taken out of Maintenance Mode.
- Stops access to meeting recordings.
- Prevents users from scheduling or hosting meetings.

The system continues to send automatic notification emails to users and administrators.

Use the following table to help determine which tasks require you to turn on Maintenance Mode and the action your system performs after you turn off Maintenance Mode, so you can plan the downtime. When Maintenance Mode is required, the system provides reminder messages if you attempt to perform a task without turning on Maintenance Mode.

Task	Reference	Maintenance Mode Required	Reboot or Restart
Adding or removing High Availability	Adding a High Availability System, on page 43	Y	Reboot
Adding or removing public access	Adding Public Access to Your System by using IRP, on page 129 or Removing Public Access, on page 131	Y	Restart
Change the system default language	Configuring Company Information, on page 163	Y	Restart
Changing your host or admin account URLs	Changing Your WebEx Site Settings, on page 136	Y	Restart
Changing your mail server	Configuring an Email (SMTP) Server, on page 138	N	N/A

Task	Reference	Maintenance Mode Required	Reboot or Restart
Changing your virtual IP address	Changing the Private and Public Virtual IP Addresses, on page 129	Y	Reboot
Configuring and changing branding settings	Configuring the General Branding Settings, on page 165	N	N/A
Configuring and changing many of the audio settings	Configuring Your Audio Settings, on page 169 Configuring Your Audio Settings, on page 169	Y	Restart
Configuring and changing the Call-In Access Numbers, Display Name, and Caller ID audio settings.	Modifying Audio Settings, on page 172	N	N/A
Configuring and changing quality of service settings	Configuring Quality of Service (QoS), on page 184	N	N/A
Configuring and changing SNMP settings	Configuring Your SNMP Settings, on page 153	Y	Restart
Configuring certificates	Managing Certificates, on page 213	Y	Restart or Reboot
Configuring disaster recovery settings	Disaster Recovery by Using the Storage Server, on page 150	Y	Restart
Configuring FIPS-compatible encryption	Enabling FIPS Compliant Encryption, on page 234	Y	Restart
Configuring storage servers	Adding an NFS or SSH Storage Server, on page 146	Y	Restart
Configuring virtual machine security	Configuring Virtual Machine Security, on page 233	Y	Reboot
Expanding system size	Preparing for System Expansion, on page 49	Y	Restart
Performing updates or upgrades	Upgrading Your System, on page 61	Y	Restart
Updating shared keys	Managing Certificates, on page 213	Y	Restart

Task	Reference	Maintenance Mode Required	Reboot or Restart
Using the System Resource test	Using the System Resource Test, on page 70	Y	Restart

Each of your virtual machines has a console window that indicates when it is in Maintenance Mode. You can open the console windows in the vCenter inventory bar (for navigation). The console windows provide the URL of the system, type of system (primary, high availability, or public access), type of deployment (50 user, 250 user, 800 user, or 2000 user system), and the current system status including the time and date of the status change. The time displayed is configured in your **Company Info** settings. See Configuring Company Information, on page 163 for more information.

Completing System Maintenance Tasks

After you finish modifying your system configuration you can turn off Maintenance Mode. The system monitors the modifications and automatically makes the determination as to whether a restart or a reboot is required. The system displays a message to indicate the requirement:

- The changes that you made require a system restart that takes only a few minutes.
- The changes that you made require a system reboot that takes approximately 30 minutes, depending on the size of your system. During this time, conference functionality is unavailable.

When Maintenance Mode is off, the **Dashboard** page refreshes. Your system is ready for users to successfully start meetings when all of the virtual machines, listed on the **System Properties** page, display a status of Good (green). See Turning Maintenance Mode On or Off, on page 90 for more information.

If Maintenance Mode is off but the scheduled maintenance window is still in effect, users will be able to host and attend previously scheduled meetings, but will not be able to schedule new meetings until after the maintenance window ends.

Turning Maintenance Mode On or Off

Turning on Maintenance Mode for all active data centers shuts down conference functionality and prevents users from signing in to the WebEx site, scheduling or joining meetings, and playing meeting recordings. Some actions do not require that all data centers in a Multi-data Center (MDC) environment be put into Maintenance Mode. If you put all of data centers are put into Maintenance Mode, meetings in progress will end. When you turn off Maintenance Mode, the system determines whether a restart (takes approximately 3 - 5 minutes), or a reboot (takes approximately 30 minutes), is required and displays the appropriate message. See About Maintenance Mode, on page 88 for information about which system tasks require Maintenance Mode to be turned on.

Before You Begin

Schedule a maintenance window and notify users about the scheduled system maintenance time. See Scheduling a Maintenance Window, on page 86 for details.

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 From the **Dashboard**, select **Manage Maintenance Mode**.
The **Manage Maintenance Mode** dialog displays.

Step 3 Select the data center to put into Maintenance Mode, or deselect the data center to be taken out of Maintenance Mode.

Step 4 Select **Save**.

Step 5 (Optional) Back up your virtual machines.

Step 6 (Optional) To determine if the system is fully operational, select **Dashboard** > **System** > **View More** (in the System section).
Conferencing functions can resume when the **Status** for all of the listed virtual machines is **Good** (green).

Using the HostID and ConfID to Locate a Meeting Recording

You can use the HostID and the ConfID values for a meeting to locate the path to the recording for that meeting.

Before You Begin

Familiarize yourself with the Network File System (NFS) directory structure.

Step 1 Obtain the full name of the meeting host, the date and time of the meeting, and the meeting number.

Step 2 In CWMS Site Administration, go to **Users** > **Import/Export Users** and click **Export**.
The system sends you an email with the **users.csv** file attached.

Step 3 In CWMS Site Administration, go to **Reports** > **Customize your report**, and then select a time period that includes the date and time when the meeting took place.
The system sends you an email with the **CustomReport.zip** file attached.

Step 4 Extract **MeetingInformation.csv** from the **CustomReport.zip** file.

Step 5 Open the **users.csv** file and use the name of the host to find the **User ID** for the host (first column of the file).
The **User ID** is the same as the **HostID** used in the directory structure.

Step 6 Open the **MeetingInformation.csv** file, and sort the data by date.

Step 7 Search for the **Meeting Number** and ensure that the details you gathered in Step 1 match.

Step 8 Find the **Meeting ID** value.
The **Meeting ID** is the same as the **ConfID** used in the directory structure.

Step 9 Use the information that you gathered to construct the path for the recording:
NFSstorageIPaddressorFQDNpath/1/HostID%1000/HostID/ConfID%1000/ConfID.
Example: Where UserID=2711 and MeetingID=49782

HostID%1000 of 2711 = 711

HostID = 2711

ConfID%1000 of 49782 = 782

ConfID = 49782

Full path = NFSstorageIPaddressorFQDNpath/1/711/2711/782/49782

Related Topics

Network File System Storage, on page 92

Network File System Storage

The Network File System (NFS) storage structure is organized into five directories (folders):

`1`—This directory contains all consolidated recordings and the following sub-directory structure:

- `HostID%1000`—If the host ID is larger than three digits, this sub-directory name is based on last three digits of the host ID.
- `HostID`—This sub-directory name matches the full host ID and is unique to each user.
- `ConfID%1000`—If the conference ID is larger than three digits, this sub-directory name is based on last three digits of the conference ID.
- `ConfID`—This sub-directory name matches the full conference ID and is unique to each conference. This sub-directory includes the following sub-directories:
  - `RecordingData`—This directory contains all of the consolidated recording files required for streaming the recording. Files present are wbxcbr.dat , wbxcbr.idx , wbxcbr.conf , Wbxcbr_tel.wav, wbxmcsr.dat , wbxmcsr.idx , and public.wbxcbr .
  - `RecordingPac`—The system creates this directory only after a host downloads the recording file from the WebEx Site. This directory contains an ARF recording file that people can play locally on their PC by using NBR Player.

Table 2: Determining the HostID%1000 or the ConfID%1000 Sub-directory Names

Condition	First Sub-directory Name
The host ID or full conference ID is 6534.[2]	534
The host ID or full conference ID is 23045.[3]	45
The host ID or full conference ID is 35000.[4]	0
The host ID or full conference ID is 42.[5]	42

2 The host ID or full conference ID contains more than three digits, the sub-directory name is based on the last three digits of the ID.

3 If the last three digits of the host ID or full conference ID contain leading zeros, the system strips them from the sub-directory name.

4 If the last three digits of the host ID or full conference ID are all zeros, the sub-diretory name is 0.

5 If the host ID or full conference ID contains fewer than three digits, the sub-directory name matches it.

Calendar year named directory —For the year 2017 the directory name is 2017. The system creates a new folder for each year. If you have had the CWMS solution for a few years, you can see other directories such as 2016, 2015, and 2014 directories. The system uses this directory to temporarily store meeting recording files during meetings. After a meeting ends, the system consolidates the associated files from this directory and moves them into the directory named `1`. This directory contains the following sub-directory structure:

- Month (by number) named directory—The system creates a directory for every month of that year (1 to 12).
- `Conf ID` directory—This directory contains the following sub-directories:
  - Action—This directory contains the .dct recording files for the associated meeting (Conf ID).
  - Data—This directory contains the .dat and .idx recording files for the associated meeting (Conf ID).

`Avatars`—The system stores all images for avatars inside this folder.

`nfskeepalive`—This folder contains files that contain information about the regular checks of component access to NFS storage. There are two types of files in this directory and both are for system use only:

- Files with number names –These files are empty.
- Files with .nkl extension—Files with names beginning with wbxcb or wbxmcs and having .nkl extensions contain 0.

`Snapshot_folder`—These directories store the daily backups of the system. The system can create more than one Snapshot_folder. The system takes a backup before running a MINOR update, and these backup files are not automatically deleted from the NFS storage. For every MINOR update run on the system, the system creates a Snapshot_folder with backups taken just before the update was run.

Related Topics

Using the HostID and ConfID to Locate a Meeting Recording, on page 91

CHAPTER 12

Managing Users

About Managing Users

You can add users individually by using the GUI or import user accounts stored in a comma-separated or tab-delimited (CSV) file. See Creating Comma- or Tab-Delimited Files, on page 97.

The system supports a lifetime maximum of 400,000 user accounts, the sum of both active and deactivated user accounts. (This lifetime maximum number of user accounts is large enough to accommodate the anticipated growth in the user database of any organization.)

You can add and deactivate user accounts, but you cannot delete them. A deactivated user can be reactivated as necessary. Reactivated user accounts regain access to the meetings, recordings, and other data that they had access to before they were deactivated.

User accounts are based on the email address of the user. If the email address of a user is changed outside the system, the user might not be able to use the system until the email address is reconciled.

To prevent unauthorized sign-in to the system, deactivate any users who leave your organization. You can deactivate users in the following ways:

- If your system does not use integrated SSO, you can deactivate users individually by using the GUI or by importing a CSV file with the ACTIVE field set to N for all the users you want to deactivate. See Activating or Deactivating Users or Administrators, on page 114 for more information.
- If your system uses integrated SSO you must deactivate users by removing them from the corporate directory in your SAML 2.0 IdP. This procedure cannot be performed through this product.
- Use the password configuration feature to deactivate users after a specified period of time. See General Password Settings, on page 186 for more information.

For Cisco WebEx Meetings Server Release 2.5, there are additional user roles: SSO Administrator, LDAP Administrator, and Auditor.

Auditor Role

Auditor Role

The Auditor role is added by using Adding Users, on page 111.

The Auditor role is a special role created for environments that need to audit sign-ins and configuration changes made by administrators. An auditor can configure log settings and generate Application Audit logs to meet company security and JITC-compliance requirements.

The First Administrator has Auditor privileges by default, and is the only one who can activate the Auditor role for another user. When doing so, the Auditor privileges are taken away from the First Administrator. If an Auditor is also a System Administrator, that person has a System Auditing role.

The Auditor role separates administrative actions from system monitoring as follows:

- Turn auditing on or off.
- Configure CWMS to synchronize with the remote syslog servers.
- Perform log purging.
- Configure alarms for the log partition.
- Generate log captures.
- An Auditor *does not have Host privileges* and cannot schedule meetings by using the Auditor account. An Auditor can attend meetings as a participant.
- If the Administrator and Auditor roles are not separated, only the Administrator role exists.
- If the Administrator and Auditor roles are separated when the system is deployed, a First Administrator role is created (described as the *emergency account*). After system deployment, only the First Administrator emergency account can create an Auditor. The First Administrator can create as many auditors as desired after the system has been deployed by using the Adding Users, on page 111 procedure..

- The Auditor is local only; it cannot come from synchronization with any external user base.
- Auditor parameters (such as the name) can be modified, but once created the Auditor role cannot be deactivated or reassigned to another user ID.
- An Auditor cannot modify user parameters. An Auditor can only see and configure settings on the Auditor tab.

The Auditor role is a unique role with the following aspects:

Note If an Auditor is not configured, all administrators have access to and can configure the Application Audit Log settings on the **Settings** > **Security** > **Application Audit Log** page and the Log Memory Usage alarm on the **Dashboard** > **Alarms** > **Edit Alarms** page. If an Auditor is configured, administrators can view these pages, but they cannot modify them.

Creating Comma- or Tab-Delimited Files

The system can import and export user account values contained in a comma- or tab-delimited (CSV) file. (A spreadsheet application, such as Microsoft Excel, can be used to manage CSV files.) If an account in an imported CSV file does not exist, the account is added. If the account exists, imported CSV account values replace the current values.

The system can export a CSV file containing user account values that can be modified and imported back into the system or a new system.

To successfully import a CSV file, the following criteria must be met:

- All fields listed in the table are required. We recommend that before importing a CSV file, that you export the current database to a CSV file to confirm the structure of the file. If a field is missing, an error message appears. For example,
  Incorrect file format. Custom10 is required.
- Field values can be empty, unless indicated otherwise.
- Valid characters in the CSV file are limited to those contained in UCS Transformation Format—8 bit (UTF-8).
- When adding a new user account, the **UserId** field can be blank if the **Email** field contains an email address that is not used by another user account. If the email address matches the email address in another user account, the user account in the CSV file is not added.
- When editing a user account, the **UserId** and **Email** values must match an existing user account. If they do not match a user account, none of the current values are changed to the CSV values.
- Up to ten **Tracking Code Groups** can be defined. Tracking code group names must be unique. Do not use predefined field names (USERID, ACTIVE, FIRSTNAME, LASTNAME, EMAIL, LANGUAGE, HOSTPRIVILEGE, TIMEZONE, and so forth) for tracking codes.

Table 3: Field Names, Descriptions, and the Acceptable Values

Field Name	Description	Size and Type of Value
USERID	User ID. **Important** This field is generated by the system and must be left blank.	1 to 19 alphanumeric characters
ACTIVE	Indicate whether or not this user is active.	Y or N
FIRSTNAME	User's first name. This field cannot be empty.	1 to 32 character string
LASTNAME	User's last name. This field cannot be empty.	1 to 32 character string
EMAIL	User's email address.	1 to 192 alphanumeric character string
LANGUAGE	Language of the user. (See CSV File Field Values, on page 99.)	1 to 64 character string
HOSTPRIVILEGE	Host privileges.	ADMN or HOST If the import file does not specify a value, the system applies the default user account type. (**Settings** > **User Management** > **Default user account type**)
TIMEZONE	Time zone where the user is located. (See CSV File Field Values, on page 99.)	Time zone name
DIVISION	Tracking code group 1. This field is configurable on the Tracking Codes page. (See Configuring Tracking Codes, on page 115.)	1 to 128 character string
DEPARTMENT	Tracking code group 2. This field is configurable on the Tracking Codes page. (See Configuring Tracking Codes, on page 115.)	1 to 128 character string
PROJECT	Tracking code group 3. This field is configurable on the Tracking Codes page. (See Configuring Tracking Codes, on page 115.)	1 to 128 character string

Field Name	Description	Size and Type of Value
OTHER	Tracking code group 4. This field is configurable on the Tracking Codes page. (See Configuring Tracking Codes, on page 115.)	1 to 128 character string
CUSTOM5	Custom field 5. (See Configuring Tracking Codes, on page 115.)	1 to 128 character string
CUSTOM6	Custom field 6.	1 to 128 character string
CUSTOM7	Custom field 7.	1 to 128 character string
CUSTOM8	Custom field 8.	1 to 128 character string
CUSTOM9	Custom field 9.	1 to 128 character string
CUSTOM10	Custom field 10.	1 to 128 character string
COUNTRY	Country of user.	1 to 128 character string

The following topics provide additional information:

- Exporting All User Accounts to a CSV File, on page 110
- Importing User Accounts from a CSV File, on page 110
- Transferring User Accounts Between Systems by using a CSV File, on page 111
- Configuring Tracking Codes, on page 115

CSV File Field Values

Language Field Values

Following are examples of the LANGUAGE field values that you can use in a CSV file.

Field Value	Language
en-us	U.S. English
zh-cn	Simplified Chinese
zh-tw	Traditional Chinese
jp	Japanese
ko	Korean

Field Value	Language
fr	French
de	German
it	Italian
es-me	Castellon Spanish
es	Latin American Spanish
nl	Dutch
pt-br	Portuguese
ru	Russian

Time Zone Field Values

Following are the TIMEZONE field values that you can set in a CSV file.

Field Value	GMT
Marshall Islands	-12 hr
Samoa	-11 hr
Honolulu	-10 hr
Anchorage	-9 hr
San Francisco	-8 hr
Tijuana	-8 hr
Arizona	-7 hr
Denver	-7 hr
Chihuahua	-7 hr
Chicago	-6 hr
Mexico City	-6 hr
Saskatchewan	-6 hr
Tegucigalpa	-6 hr

Field Value	GMT
Bogota	-5 hr
Panama	-5 hr
New York	-5 hr
Indiana	-5 hr
Caracas	-4.5 hr
Santiago	-4 hr
Halifax	-4 hr
Newfoundland	-3.5 hr
Brasilia	-3 hr
Buenos Aires	-3 hr
Recife	-3 hr
Nuuk	-3 hr
Mid-Atlantic	-2 hr
Azores	-1 hr
Reykjavik	0 hr
London	0 hr
Casablanca	0 hr
West Africa	1 hr
Amsterdam	1 hr
Berlin	1 hr
Madrid	1 hr
Paris	1 hr
Rome	1 hr
Stockholm	1 hr

Field Value	GMT
Athens	2 hr
Cairo	2 hr
Pretoria	2 hr
Helsinki	2 hr
Tel Aviv	2 hr
Amman	2 hr
Istanbul	2 hr
Riyadh	3 hr
Nairobi	3 hr
Tehran	3.5 hr
Moscow	4 hr
Abu Dhabi	4 hr
Baku	4 hr
Kabul	4.5 hr
Islamabad	5 hr
Mumbai	5.5 hr
Colombo	5.5 hr
Ekaterinburg	6 hr
Almaty	6 hr
Kathmandu	6.75 hr
Bangkok	7 hr
Beijing	8 hr
Perth	8 hr
Singapore	8 hr

Field Value	GMT
Taipei	8 hr
Kuala Lumpur	8 hr
Tokyo	9 hr
Seoul	9 hr
Adelaide	9.5 hr
Darwin	9.5 hr
Yakutsk	10 hr
Brisbane	10 hr
Sydney	10 hr
Guam	10 hr
Hobart	10 hr
Vladivostok	11 hr
Solomon Islands	11 hr
Wellington	12 hr
Fiji	12 hr

Country Field Values

The COUNTRY field is *optional* and, if included, follows the TIMEZONE field. These are examples of the COUNTRY field values that you can use in a CSV file:

Afghanistan

Albania

Algeria

American Samoa

Andorra

Angola

Anguilla

Antarctica

Antigua (including Barbuda)

Argentina
Armenia
Aruba
Ascension Islands
Australia
Austria
Azerbaijan
Bahamas
Bahrain
Bangladesh
Barbados
Belarus
Belgium
Belize
Benin
Bermuda
Bhutan
Bolivia
Bosnia-Herzegovina
Botswana
Brazil
British Virgin Islands
Brunei
Bulgaria
Burkina Faso
Burundi
Cambodia
Cameroon
Canada
Cape Verde Island
Cayman Islands
Central African Republic
Chad Republic
Chile
China
Colombia

Comoros
Cook Islands
Costa Rica
Croatia
Cuba
Cyprus
Czech Republic
Democratic Republic of the Congo
Denmark
Diego Garcia
Djibouti
Dominica
Dominican Republic
Ecuador
Egypt outside Cairo
El Salvador
Equatorial Guinea
Eritrea
Estonia
Ethiopia
Faeroe Islands
Falkland Islands
Fiji Islands
Finland
France
French Depts. (Indian Ocean)
French Guiana
French Polynesia
Gabon Republic
Gambia
Georgia
Germany
Ghana
Gibraltar
Greece
Greenland

Grenada
Guadeloupe
Guantanamo (U.S. Naval Base)
Guatemala
Guinea
Guinea-Bissau
Guyana
Haiti
Honduras
Hong Kong
Hungary
Iceland
India
Indonesia
Iran
Iraq
Ireland
Israel
Italy
Ivory Coast
Jamaica
Japan
Jordan
Kazakhstan
Kenya
Kiribati
Korea, North
Korea, South
Kuwait
Kyrgyzstan
Laos
Latvia
Lebanon
Lesotho
Liberia
Libya

Liechtenstein
Lithuania
Luxembourg
Macao
Macedonia
Madagascar
Malawi
Malaysia
Maldives
Mali
Malta
Marshall Islands
Mauritania
Mauritius
Mayotte Island
Mexico
Micronesia
Moldova
Monaco
Mongolia
Montenegro
Montserrat
Morocco
Mozambique
Myanmar
Namibia
Nauru
Nepal
Netherlands
Netherlands Antilles
New Caledonia
New Zealand
Nicaragua
Niger
Nigeria
Niue

Norfolk Island
Northern Mariana Islands
Norway
Oman
Pakistan
Palau
Panama
Papua New Guinea
Paraguay
Peru
Philippines
Poland
Portugal
Puerto Rico
Qatar
Republic of the Congo
Romania
Russia
Rwanda
San Marino
Sao Tome
Saudi Arabia
Senegal Republic
Serbia
Seychelles Islands
Sierra Leone
Singapore
Slovakia
Slovenia
Solomon Islands
Somalia
South Africa
Spain
Sri Lanka
St Helena
St Kitts and Nevis

St Lucia
St Pierre and Miguelon
St Vincent
Sudan
Suriname
Swaziland
Sweden
Switzerland
Syria
Taiwan
Tajikistan
Tanzania
Thailand
Togo
Tonga Islands
Trinidad and Tobago
Tunisia
Turkey
Turkmenistan
Turks and Caicos
Tuvalu
Uganda
Ukraine
United Arab Emirates
United Kingdom
United States of America
Uruguay
Uzbekistan
Vanuatu
Vatican City
Venezuela
Vietnam
Wallis And Futuna Islands
Western Samoa
Yemen
Zambia

Zimbabwe

Exporting All User Accounts to a CSV File

You can export selected users to a CSV 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 **Users** > **Import/Export Users**.

Step 3 Select **Export**.
Your user data is exported as a CSV file. The system emails the administrator a link to the exported file download. A **Download exported csv file** link appears in the window.

Step 4 Select the link to download the file and follow the instructions.

Importing User Accounts from a CSV File

To import a CSV file to the system:

Before You Begin

Prepare a comma- or tab-delimited (CSV) file containing the user account information. You can export the current system user account values to a CSV file, modify the file, and import it to add or change user accounts. See Exporting All User Accounts to a CSV File, on page 110 and Creating Comma- or Tab-Delimited Files, on page 97 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 **Users** > **Import/Export Users**.
The **Import/Export Users** page appears.

Step 3 Select **Import**.
The **Import Users** page appears.

Step 4 Select **Browse** and then select the CSV file to be imported.

Step 5 Select **Comma** or **Tab** to indicate which type of CSV file you are importing, comma-delimited or tab-delimited.

Step 6 Select **Import**.
The file is imported and the system sends an email indicating how many user accounts were imported successfully and how many accounts failed to be added or modified.

What to Do Next

Select **Users** to view the user accounts and verify that the values were imported correctly.

Transferring User Accounts Between Systems by using a CSV File

To transfer user accounts from one system to another by using a CSV file:

Step 1 Sign in to the Administration site on the system that contains the source of the user accounts to be transferred.

Step 2 Select **Users** > **Import/Export Users**.

Step 3 Select **Export**.
Your user data is exported as a CSV file. The system emails the administrator a link to the exported file download. A **Download exported csv file** link appears in the window.

Step 4 Optionally, open the exported CSV file, modify the user account values as needed, and save the CSV file. (See Creating Comma- or Tab-Delimited Files, on page 97 for more information.)

Step 5 Sign in to the target system Administration site.

Step 6 Select **Users** > **Import/Export Users**.
The **Import/Export Users** page appears.

Step 7 Select **Import**.
The **Import Users** page appears.

Step 8 Select **Browse** and then select the CSV file to be imported.

Step 9 Select **Comma** or **Tab** to indicate which type of CSV file you are importing, comma-delimited or tab-delimited.

Step 10 Select **Import**.
The file is imported and the system sends an email indicating how many user accounts were imported successfully and how many accounts failed to be added or modified.

What to Do Next

Select **Users** to view the user accounts and verify that the values were imported correctly.

Adding Users

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 **Users** > **Add User**.

Step 3 Select the account type (**Auditor**, **Host**, or **Administrator**).

The Auditor option is visible, but is an available option only for the First Administrator.

Step 4 Complete the fields with the user information. Fields marked with an asterisk are required fields.

Important Users are identified to the system by Email address. If a user Email address is changed and the user remains active, the Email address on CWMS must also be changed or that user will not receive notifications.

Step 5 Check the **Session Type Allowed** in the Privileges section assigned to the user.
Selecting one of the highlighted session types shows the Session Type Features.

Step 6 Select the audio types (Telephony Privilege) allowed for this user.
Call-in teleconferencing allows the user to host a teleconference that participants can attend by calling a telephone number.

Call-back teleconferencing allows the user to host a session in which participants receive a telephone call from the WebEx service to join the teleconference. Each participant calls a telephone number and then hangs up the call. The service then calls that participant's telephone number.

Integrated VoIP allows the user to host as session that includes an Internet telephone (voice-over-IP) access to the teleconference.

Step 7 Select **Save**.
Cisco WebEx Meetings Server sends an Email to the user with a **Create Password** link. A user must create a password before signing in to the WebEx Common site.

The Create Password link expires after 72 hours. If the link has expired, the user can select the **Forgot Password** link to receive a new email message that gives them another opportunity to create a password.

The user is added to the system.

Editing Users

Change user account information or reserve a permanent host license for this user.

Important Users are identified to the system by Email address. If using SSO and a user Email address is changed and that user remains active, we recommend that you change the Email address on CWMS or that user will not receive notifications until the systems are synchronized.

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.

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 **Users**.
The default number of users shown on each page is 50. Use the **Users Per Page** drop-down menu to change the setting.

The list of users appears.

Step 3 Select the user to edit by double-clicking the user name.

Step 4 Select an **Account Type**.
Auditor separates administrative actions from system monitoring. (An existing user account cannot be changed to an Auditor account. The Auditor must be created by the First Administrator. See Auditor Role, on page 96 for more information.)

Host can schedule meetings and start meetings if they have an assigned license. A host can start up to two simultaneous meetings, but will receive an error when attempting to start a third meeting.

Attendee Only can attend meetings, but not schedule, start, host, or be an alternate host.

Administrators are created on the Add User page. Administrators can configure settings during system deployment and can make other users Hosts, Administrators, SSO Administrators, or LDAP Administrators. If an Auditor is configured on a system, an administrator cannot configure the Application Audit Log settings.

SSO or LDAP Administrators can change configuration settings after the system is operational. These users are synchronized into the system when the system is an SSO-integrated system or an LDAP-integrated system. Only the option that applies to your system appears as an account type. SSO and LDAP Administrators sign-in to the WebEx site URL and select the **Administration Site** link to connect to the Administration site. This type of administrator can add other administrators on the Add User page, can make users hosts, or make other users (synchronized on an SSO integrated or LDAP integrated system) SSO Administrators or LDAP Administrators..

Step 5 Make changes to the editable fields in the **Account Information** section. Fields marked with an asterisk are required.

Step 6 (Optional) Select **Reserve license** to provide this user with a permanent license to host meetings.
Typically, if available, a host license is granted when a user hosts a meeting for the first time. This option reserves an available license in the license pool and assigns it to the user without the user having to host a meeting. See About Host Licenses, on page 250 for details.

Step 7 (Optional) Select **Require user to change password at next sign in**.
If SSO or LDAP is enabled on your system, this feature is disabled for host accounts. It is available only for administrator and auditor passwords used to sign-in to the Administration site. Administrator and auditor continue to use the SSO or LDAP credentials to sign-in to their WebEx site.

Step 8 Check the **Session Type Allowed** in the Privileges section assigned to the user.
Selecting one of the highlighted session types shows the Session Type Features.

Step 9 Select the audio types (Telephony Privilege) allowed for this user.
Call-in teleconferencing allows the user to host a teleconference that participants can attend by calling a telephone number.

Call-back teleconferencing allows the user to host a session in which participants receive a telephone call from the WebEx service to join the teleconference. Each participant calls a telephone number and then hangs up the call. The service then calls that participant's telephone number.

Integrated VoIP allows the user to host as session that includes an Internet telephone (voice-over-IP) access to the teleconference.

Step 10 Select **Save**.

The changes are saved. Saving the parameters does not alter the status of the account. (See Activating or Deactivating Users or Administrators, on page 114.)

Unlocking an Account

To prevent unauthorized access, the system can automatically lock out an account holder account. This feature is off by default. The conditions that would cause an account holder to be locked out, such as number of failures or the period of inactivity, and how many minutes the account remains locked are configurable. When an account is locked, the system sends the locked account holder and all administrators an email indicating that the account is locked.

The following sections describe how to unlock an account.

Unlocking an Account from an Email

An administrator can select **Unlock Account** in the email to unlock their account. This option is off by default.

Unlocking an Account from a User Profile

An administrator that is not locked out of the system can select the locked-out account holder from the list on the **Users** tab to display the **Edit User** page and then select the **Unlock** link in the message displayed at the top of that page to unlock the account and notify the account holder that the account has been unlocked. This option is always on.

When an administrator account is locked, another administrator can select the **Unlock** link in the message that appears at the top of the **Edit User** page to unlock the account on behalf of the locked-out administrator.

Waiting Until the Timer Expires

When an account is locked and the optional timer is set, the account holder can log in when the timer expires.

Activating or Deactivating Users or Administrators

Use this feature to activate deactivated accounts or reactivate inactive accounts. The only accounts that cannot be deactivated are the Auditor accounts. Alternatively, you can activate an account by setting the parameter in a CSV file and importing it. See Importing User Accounts from a CSV File, on page 110 for more information.

Note

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 **Users**.

Step 3 Select the check boxes for any inactive users you want to activate. Or select the check boxes for any active users you want to deactivate.

Step 4 Select **Actions** > **Activate** or **Actions** > **Deactivate**.
The selected accounts are modified and the status for each account reflects the updated status.

Finding Users

You can sort users by type, for example active or host, or by the type of license assigned to hosts. In addition to sorting users, you can also search users by first, last, or full name and by email address. The search results display user profile and license information.

Step 1 Sign in to the Administration site.

Step 2 Select **Users**.

Step 3 Select a category from the drop-down menu to sort users.

Step 4 (Optional) Use the **Expire in** drop-down to sort users with temporary licenses by license expiration (expired, 1 month, 3 months, 6 months).

Step 5 Type a user's name (first, last, or full name) or email address in the search field and select **Search**.

Configuring Tracking Codes

Use tracking codes to categorize meeting usage, such as breaking out the data for a project or a department. The tracking codes appear as options when you add or edit users.

Configure the following parameters for each tracking code:

- **Tracking code group–**Active groups can be chosen when you add or edit users.
- **Input mode–**Controls how the tracking code parameters appear when creating or editing a user.
- **Usage–**Prevents the group from displaying, being an optional entry, or a required entry.

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 **Users** > **Tracking Codes**.

Step 3 (Optional) Enter the name of each group you want to configure in the **Tracking code group** column.

The default group names are Division, Department, Project, Other, and Custom5 through Custom10. Any of the group names can be changed.

Note Tracking code group names should be unique and you should not use predefined field names (USERID, ACTIVE, FIRSTNAME, LASTNAME, EMAIL, LANGUAGE, HOSTPRIVILEGE, TIMEZONE).

Step 4 Select **Text Input** or **Dropdown Menu** for each tracking code in the **Input mode** column.

- Select **Text Input**. The administrator enters the tracking code in a text field creating or editing a user.
- Select **Dropdown menu**. An **Edit list** link appears next to the **Input mode** field. Select the **Edit list** link to configure the values for this tracking code. See Editing Tracking Codes, on page 116 for more information.

Step 5 Select **Not used** to prevent the tracking code from displaying when that user is created or edited. Select **Optional** to display, but not require a tracking code. Select **Required** to make assigning a tracking code to a user a requirement.

Step 6 Select **Save**.
Your tracking code parameters are saved.

Editing Tracking Codes

A list of tracking codes can be associated with a specific group that displays when adding or editing a user. This feature manages the tracking codes that display when those codes are selected from a drop-down menu.

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 **Dropdown Menu** in the **Input mode** column for the group that you want to list tracking codes in the drop-down menu.
If you select **Text Input**, an input field displays next to the group where the administrator can enter any valid string.

Step 3 (Optional) If you chose **Dropdown Menu**, select **Edit list** to configure the values for this tracking code. The **Edit Tracking Code List** dialog box appears.
In addition to creating, editing, or deleting codes, you can deactivate or activate the code and indicate that a code in the list is the default code.

- Select **Show active codes only** to display only active tracking codes. Deselect this option to show all tracking codes. You cannot select this option the first time you configure tracking codes.
- Enter the drop-down menu code in the **Code** text box. This string is limited to 128 characters. If there are no empty tracking codes shown, select **Add 20 more lines** to add 20 more configurable tracking codes. The maximum number of tracking codes is 500 lines.
- Select **Default** to make a code the default selection.
- **Active** is selected by default. Uncheck **Active** to make a tracking code inactive. Inactive tracking codes do not appear on this tracking code group drop-down menu.
- Select **Update** to associate the codes with the group. You are returned to the **Tracking Codes** window.

Step 4 Select **Save** to save your settings.

Configuring Directory Integration

Directory integration enables your system to populate and synchronize your Cisco WebEx Meetings Server user database with the CUCM user database that is then integrated with an LDAP directory.

Directory integration simplifies user profile administration in the following ways:

- Imports user profiles from CUCM to Cisco WebEx Meetings Server.
- Periodically updates the Cisco WebEx Meetings Server database with new or modified user attributes in the CUCM database including each user's first name, last name, and email address. Cisco WebEx Meetings Server differentiates users by their email addresses, so if users have the same first name and last name but different email addresses, Cisco WebEx Meetings Server treats them as different users.
- Periodically checks the CUCM database for inactive user entries and deactivates their user profiles from the Cisco WebEx Meetings Server database.
- Enables the system to use LDAP authentication to authenticate Cisco WebEx Meetings Server directory integration users against the external directory.
- Supports fully encrypted LDAP integration when Secure LDAP (SLDAP) is enabled on CUCM and the LDAP server.
- All users configured in CUCM are synchronized to Cisco WebEx Meetings Server and their accounts are activated. You can optionally deactivate accounts after the synchronization is complete. All active users in CUCM are synchronized into Cisco WebEx Meetings Server. Inactive users are not imported into Cisco WebEx Meetings Server. (Users can be manually added into CUCM for environments where LDAP/AD is not available or configured in CUCM.)

Before You Begin

Make sure the following prerequisites are met before you proceed with directory integration:

- In Site Administration **Settings** > **User Management**, set the **Default user account type** to **Host** or to .
- Schedule synchronization during off-peak hours or on weekends to minimize the impact on your users.
- Verify that you have a supported version of Cisco Unified Communications Manager (CUCM). Refer to the http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-configure.html for more information.
- Obtain CUCM administrative user credentials (required to add a CUCM server for directory integration).
- Configure AXL and LDAP directory service on CUCM. CUCM is required to import users into your Cisco WebEx Meetings Server system. Use CUCM to do the following:
  - Enable Cisco AXL Web Service
  - Enable Cisco directory synchronization
  - Configure LDAP integration

- Configure LDAP authentication

See Using CUCM to Configure AXL Web Service and Directory Synchronization, on page 122 and Using CUCM to Configure LDAP Integration and Authentication, on page 122. Refer to the http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html for additional information.

- Make sure that all users who require host privileges are available in CUCM. Any user not in CUCM will not be able to host meetings (all users can join as a guest). If necessary, create CUCM groups or filters, which include only the users that you want to import from CUCM.

Note If you do not use CUCM groups, the system imports all active CUCM users during the first directory synchronization. Inactive CUCM users are not imported. The system imports only active new and modified users during subsequent synchronizations. Deactivate user accounts that you do not want to give host access to. Note that a host license is only consumed in Cisco WebEx Meetings Server when a user actually hosts a meeting. Accounts that do not host meetings do not consume licenses. See "Managing Licenses" in Managing Host Licenses, on page 249 for more information about license consumption.

- Users without email address are not imported.
- If users have multiple accounts that use the same first name and last name but are assigned different email addresses on CUCM, when these users are imported to Cisco WebEx Meetings Server these addresses are treated as different users. CUCM users are unique by username so an administrator can create multiple user accounts with the same email address. However, accounts on the Cisco WebEx Meeting Server are unique by email address. Therefore, if multiple CUCM user accounts have the same email address, the administrator for CUCM should manually edit these user accounts to make the email addresses unique before importing those accounts to the Cisco WebEx Meetings Server.
- When LDAP authentication is enabled, Cisco WebEx Meetings Server uses port 8443 to connect to CUCM when you select the **Synchronize Now**, or check the **Next synchronization** option and enter a date and time.
- Cisco WebEx Meetings Server supports passwords up to 64 characters. When creating a user on CUCM, ensure that a password is no more than 64 characters. Users with passwords greater than 64 characters will not be able to sign into Cisco WebEx.

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) **Turn On Maintenance Mode**.
Maintenance mode is *not required* to perform directory integration but a large synchronization can affect system performance. You can put your system into maintenance mode to prevent users from using the system during a synchronization.

Step 3 Select **Users** > **Directory Integration**.

Step 4 (Optional) Select the server (under CUCM) to enter your CUCM server information if you have not done so already:

- IP Address or fully qualified domain name (FQDN)
- Username
- Password

The username and password can be your CUCM administrator or AXL username and password. After you configure your CUCM information, the IP address or FQDN of your CUCM server appears under the CUCM icon.

Note After you have configured your CUCM information, changing it is a complex procedure that can cause user synchronization problems and is not recommended.

Step 5 Select **CUCM User Groups for Filtering** to add only those users in the selected CUCM User Groups in to Cisco WebEx Meeting Server.

Step 6 (Optional) Select **Full Synchronization** to synchronize all users in the selected CUCM groups. When it is not selected, the system synchronizes only the users updated or added to the selected CUCM groups since the most recent update of the Directory Service user profile.
This option affects only the Synchronize Now option in the next step; it does not affect a scheduled (Next) synchronization.

We recommend that this action be performed as part of events such as, the CUCM server has been changed on CWMS, the email addresses of users have been changed on CUCM, or a user is deleted from the group on CUCM.

Depending on the size of the CUCM user database, system performance could be impacted when you chose to synchronize the entire database.

Step 7 Synchronize your Cisco WebEx Meetings Server system with your LDAP directory service. You can perform your synchronization in the following ways:

- Select **Synchronize Now** to perform a synchronization immediately. You cannot cancel synchronization once it starts. You are sent an email when the synchronization is complete. The other administrators on your system are not notified after a **Synchronize Now**.
- Select **Next synchronization** and enter a date and time to schedule synchronization. You can chose to **Repeat** synchronization at regular intervals.

In an MDC system, the synchronization of each data center should be performed either at different times or it should be active on only one of the data centers to avoid the degradation of system performance.

If you select **Synchronize Now**, your system immediately performs a synchronization. If you schedule a synchronization, it occurs at the specified date and time. All administrators receive an email after a scheduled synchronization is complete. If you want to prevent future synchronization, you can deselect **Next synchronization**.

The following attributes are mapped during the synchronization process:

CUCM Attribute	Cisco WebEx Meetings Server Attribute
First Name	First Name
Last Name	Last Name
Mail ID	Email Address

Note The first name and last name in Cisco WebEx Meetings Server are components of the full name that is displayed to users.

Mapped attributes in Cisco WebEx Meetings Server cannot be updated by end users.

If your synchronization fails, an error message appears on the page and an email with detailed information about the error is sent to the administrator. Select **View Log** to see a detailed explanation of the error. The logs provided include a deactivated user report, failed user report, and a summary.

After you have performed at least one synchronization, a summary of your last synchronization appears indicating whether or not it was completed, the time and date it was completed (using the time and date configured in your Company Info settings), and a listing of user changes including the following:

- Added—The number of new users added.
- Deactivated—The number of users who were deactivated.

Step 8 Select **Save** if you have configured or changed your synchronization schedule or your administrator notification settings.

Step 9 Select the **Users** tab and make sure that the correct users have been synchronized.

a) Select **Remote users** on the drop-down menu to filter the user list. Make sure that the users you wanted synchronized are present in the list. Remote users are imported into Cisco WebEx Meetings Server through a directory synchronization. If a user is created locally first and is overwritten by a directory synchronization, this user will become a remote user, not a local user.

b) Select **Local users** to see which users were not included in the synchronization. Local users are created locally by a Cisco WebEx Meetings Server administrator. Local users can be added manually or imported using a CSV file.

Step 10 Make sure your CUCM and Cisco WebEx Meetings Server synchronization schedules are sequential. Your CUCM synchronization must occur first and your Cisco WebEx Meetings Server synchronization should occur immediately afterward.

Step 11 (Optional) Select or deselect **Notify administrators when synchronization completes** and then select **Save**. This option is selected by default and only informs administrators after a *scheduled* synchronisation.

Step 12 Select **Enable LDAP Authentication**.

Note If your system is configured to use SSO, you must first disable SSO. See Disabling SSO, on page 233 for more information. If your system is not configured to use SSO, it uses its default authentication until you enable LDAP authentication.

After enabling LDAP we recommend that administrators use Active Directory server for user management including adding, disabling, and modifying users. After enabling LDAP authentication, all participants must use their LDAP credentials to sign in to the WebEx site.

Step 13 Make sure that your users can sign into the system with their AD domain credentials.

Step 14 (Optional) If you put your system in maintenance mode **Turn Off Maintenance Mode**.

Step 15 (Optional) If you have performed a synchronization, you can select **Notify Now** to notify users by email that accounts have been created for them on your Cisco WebEx Meetings Server system or when their accounts have been changed. You can optionally select **Automatically send out notifications**, which automatically sends an email to your newly added users after each synchronization. After any change to the authentication settings (for example, enabling LDAP), the Users–Password Changed email is sent to affected users.
When you select **Notify Now**

- All users receive only one notification in their lifetime. Subsequent synchronization do not cause additional emails to be sent.
- "Users that require notification" indicates all users that are active and have not been notified yet.
- Inactive users or local users are not sent any notification.
- Adding a local user on Cisco WebEx Meetings Server sends an email to this user. However, this user must be added on your CUCM Active Directory server before he can sign in to the WebEx site.

- You can only send notifications to users who were added using the synchronization feature.
- It might take a few minutes for your email notifications to be sent to your users. This delay is caused by several factors that are external to your Cisco WebEx Meetings Server system including your email server, network connectivity issues, and spam catchers on individual email accounts.

Your system sends the following emails:

- The AD Activation Email is sent to each user the first time they are imported into your system in a synchronization. Users do not receive this email on subsequent synchronization.
- The User Password–Changed email is sent to users who were created locally on your system.

See "About "Email Templates (v2.6 and Earlier)" for information on customizing these email templates.

Note If you are using Directory Integration with LDAP authentication, users configured in CUCM are synchronized into Cisco WebEx Meeting Server as hosts and use their LDAP credentials to sign in to their WebEx site. However, if you change an imported user account type from **host** to **administrator**, the user receives an email with a Create Password link. A user selects this link and enters a new password for Cisco WebEx Meetings Server. The user will use this newly created password to sign in to the Administration site, but will continue to use the LDAP credentials to sign in to their WebEx site.

Synchronizing User Groups

Administrator can create groups of users in CUCM. For example, an administrator might create a user group consisting of users who will be allowed to use Cisco WebEx Meetings Server. From CWMS, the administrator can filter and import certain users by selecting specific user groups.

Before You Begin

Use CUCM to create groups of users. Refer to the "User Management Configuration" section in the *Cisco Unified Communications Manager Administration Guide* http://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html 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 **Users** > **Directory Integration**.

Step 3 Select the **CUCM Groups for Filtering** link.

Step 4 Check the user groups to be synchronized.

Note If no groups are selected, directory integration synchronizes all user groups.

Step 5 Select **Save**.

Step 6 Select Synchronize Now to perform the synchronization. The time this process takes varies depending on the number of users being synchronized.

Note The system remembers which user groups were previously synchronized. If you do not select a user group that was previously synchronized, the users in the unselected user group will be deactivated during the synchronization process.

When the synchronization is finished, the system displays the number of users added and deactivated.

Step 7 Select **View Log** for summary information about the users who were imported or deactivated during the synchronization process.

Using CUCM to Configure AXL Web Service and Directory Synchronization

Use CUCM to configure AXL Web Service and directory synchronization.

Before You Begin

Perform this procedure before you use the Directory Integration feature. See Configuring Directory Integration, on page 117 for more information.

Step 1 Sign in to your CUCM account.

Step 2 Select **Cisco Unified Serviceability** from the top right dropdown menu and then select **Go**.

Step 3 Select **Tools** > **Service Activation**.

Step 4 Select **Cisco AXL Web Service** and **Cisco DirSync** and then select **Save**.

Note If a Cisco Unified Call Manager (CUCM) failover condition occurs in a data center that is part of a Multi-data Center (MDC) system, the CUCM administrator credentials should work for all CUCMs in that data center.

What to Do Next

Use CUCM to configure LDAP integration and authentication if you have not already done so. See Using CUCM to Configure LDAP Integration and Authentication, on page 122 for more information.

Using CUCM to Configure LDAP Integration and Authentication

Use CUCM to configure LDAP integration and authentication.

Important Users are identified to the system by Email address. If a user Email address is changed and the user remains active, the Email address on CWMS must also be changed or that user will not receive notifications.

Note If CUCM is configured for Directory Integration, you can choose to use SSO, LDAP, or local authentication.

Before You Begin

Perform this procedure before you use the Directory Integration feature. See Configuring Directory Integration, on page 117 for more information.

Step 1 Sign in to your Cisco Unified Call Manager (CUCM) account.

Step 2 Select **Cisco Unified CM Administration** from the top right drop-down menu and then select **Go**.

Step 3 Select **File** > **LDAP** > **LDAP System**.

Step 4 Select **Enable Synchronizing from LDAP Server**, select **Microsoft Active Directory** for the LDAP Server Type, select **sAMAccountName** for the LDAP Attribute for User ID, and select **Save**.

Step 5 Select the check box for your LDAP server and then select **Add New**.

Step 6 Complete the fields on the LDAP Directory page and then select **Save**.

Step 7 On the LDAP Authentication page, select the **Use LDAP Authentication for End Users** check box, complete the fields on the page, and then select **Save**.

What to Do Next

Use CUCM to configure Cisco AXL Web Service and Cisco Directory Sync if you have not already done so. See Using CUCM to Configure AXL Web Service and Directory Synchronization, on page 122 for more information.

Emailing Users

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 To send email notifications to users, select **Users** > **Email Users**.

Step 3 Enter a target user email address or an email alias in the **To** field, or leave the field blank to send email to all users.

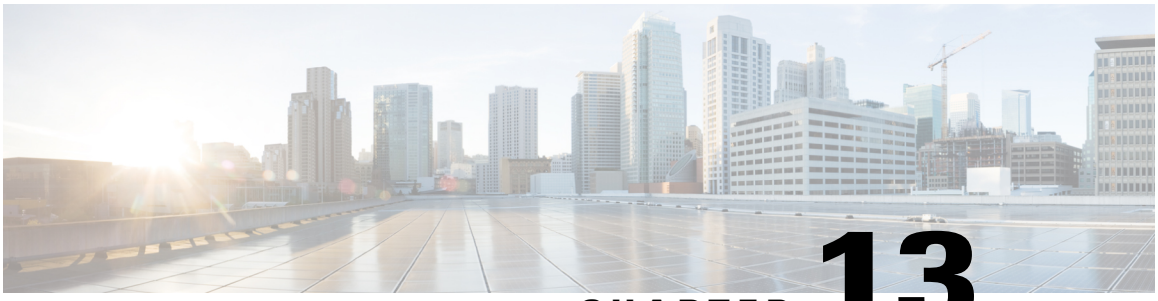
Step 4 (Optional) Enter email addresses or an email alias in the **BCC** field.

Step 5 Enter the subject in the **Subject** field.

Step 6 Enter a message in the **Message** field.

Step 7 Select **Send**.
It might take a few minutes for your emails to be received by the users. This delay might be caused by several factors that are external to your Cisco WebEx Meetings Server system, including your email server, network connection speed, and spam catchers on individual email accounts.

Your email is sent.



CHAPTER 13

Configuring Your System

Creating Administrator Accounts

The system creates a First Administrator account. This administrator must sign into the system, create a password, and add other administrators. Until then, no other administrator can have access to the system. As part of the process, the First Administrator (and only the First Administrator) can create an Auditor account, separating the administrator and auditor. This can be done as part of the deployment process or the First Administrator can create an Auditor by using (**Users** > **Edit Users**) to modify the role. (See Auditor Role, on page 96 for more information.)

Before You Begin

A mail server for the system to use to send emails to administrators must be configured. See Configuring an Email (SMTP) Server, on page 138 for instructions.

Step 1 Enter the first and last names of the administrator.

Step 2 Enter the complete administrator email address and confirm it by entering it again.

Step 3 (Optional) Select **Create an auditor account** to add an Auditor to the system.

Step 4 Select **Next** to create the initial password.

Step 5 Enter a password and confirm it by entering it again.

Step 6 Select **Submit** to sign in to the WebEx Administration site.

Step 7 Sign into the system and add administrators and users. Upon creation of each new account, the system sends an email to that person, welcoming them and asking that user to sign in and change the initial password.
Upon initial sign in, each administrator is offered a tutorial of the system. The administrators can view the tutorial immediately or view it on demand.

Auditor Role

Auditor Role

The Auditor role is added by using Adding Users, on page 111.

The Auditor role is a special role created for environments that need to audit sign-ins and configuration changes made by administrators. An auditor can configure log settings and generate Application Audit logs to meet company security and JITC-compliance requirements.

The First Administrator has Auditor privileges by default, and is the only one who can activate the Auditor role for another user. When doing so, the Auditor privileges are taken away from the First Administrator. If an Auditor is also a System Administrator, that person has a System Auditing role.

The Auditor role separates administrative actions from system monitoring as follows:

- Turn auditing on or off.
- Configure CWMS to synchronize with the remote syslog servers.
- Perform log purging.
- Configure alarms for the log partition.
- Generate log captures.
- An Auditor *does not have Host privileges* and cannot schedule meetings by using the Auditor account. An Auditor can attend meetings as a participant.
- If the Administrator and Auditor roles are not separated, only the Administrator role exists.
- If the Administrator and Auditor roles are separated when the system is deployed, a First Administrator role is created (described as the *emergency account*). After system deployment, only the First

Administrator emergency account can create an Auditor. The First Administrator can create as many auditors as desired after the system has been deployed by using the Adding Users, on page 111 procedure..

- The Auditor is local only; it cannot come from synchronization with any external user base.
- Auditor parameters (such as the name) can be modified, but once created the Auditor role cannot be deactivated or reassigned to another user ID.
- An Auditor cannot modify user parameters. An Auditor can only see and configure settings on the Auditor tab.

The Auditor role is a unique role with the following aspects:

Note If an Auditor is not configured, all administrators have access to and can configure the Application Audit Log settings on the **Settings** > **Security** > **Application Audit Log** page and the Log Memory Usage alarm on the **Dashboard** > **Alarms** > **Edit Alarms** page. If an Auditor is configured, administrators can view these pages, but they cannot modify them.

Configuring System Properties

Configure your system properties by selecting **System** > **View More** in the System section.

Changing Virtual Machine Settings

Use this feature to change virtual machine settings. Do not use VMware vCenter to change virtual machine settings.

During deployment, you can only configure IPv4 settings. After deployment, you can configure IPv6 settings if you have an IPv6 connection between your Internet Reverse Proxy in the DMZ network and your internal virtual machines.

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, on page 90.
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, on page 88 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 (Optional) Take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter, on page 7.)

Step 4 Select **System** > **View Details**.

Step 5 Select the virtual machine name in the Primary System or High Availability System section.
You can modify the following virtual machine settings:

- Fully Qualified Domain Name (FQDN) in lowercase characters

- Primary DNS Server
- Secondary DNS Server
- Subnet Mask/Prefix
- Gateway

The Virtual Machine field is grayed out. The system automatically retrieves the IP address by resolving the host name to the IP address of a virtual machine in the DNS server. See Changing the IP Address of a Virtual Machine while Retaining the Hostname, on page 128 for more information about changing an IP address of a virtual machine.

Step 6 Select **Save**.
Your changes are saved and the virtual machine is re-booted.

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, on page 90.

Meeting service on the data center is restored.

What to Do Next

If you make changes to any of your virtual machines, you must deploy a new certificate on all virtual machines in each data center unless you are using wildcard certificates for systems in the same domain. For more information see Managing Certificates, on page 213.

Changing the IP Address of a Virtual Machine while Retaining the Hostname

If you change the hostname of a virtual machine that is part of your deployment, the corresponding IP address is picked up automatically from the DNS. This procedure explains how to change the IP address of a virtual machine and keep the same hostname.

Step 1 Configure a temporary hostname in the DNS server.

Step 2 Complete the Changing Virtual Machine Settings, on page 127 procedure to change the hostname of the virtual machine to the temporary hostname you entered in the DNS server.
When you take the system out of maintenance mode, the new temporary hostname takes effect. The original hostname is no longer part of the deployment after making this change.

Step 3 Change the IP address of the original hostname in the DNS to the new IP address.

Step 4 Using the Changing Virtual Machine Settings, on page 127 procedure, change the temporary hostname of the virtual machine to the original hostname.
When you take the system out of maintenance mode, the original hostname takes effect. Your original hostname with the new IP address is configured.

Changing the Private and Public Virtual IP Addresses

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, on page 90.
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, on page 88 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 **System**, select the *data center*, and select **View Details** in the System section.
The **Properties** page appears.

Step 4 To modify the IP addresses, in the Virtual IP Address section select a link in the Type column.

Step 5 Enter the virtual IP addresses.

Step 6 Enter the virtual IP address, subnet mask, and gateway in the IPv6 Address column if you have enabled IPv6 for client connections.
The public and private virtual IP addresses must be on separate IPv6 subnets.

Step 7 Select **Save**.

Step 8 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, on page 90.

Meeting service on the data center is restored.

Configuring Public Access

Public access enables people external to your network to host or attend online meetings through the Internet or mobile devices. Removing public access will remove public virtual IP address settings for your WebEx site URLs and terminate external access to your site.

Adding Public Access to Your System by using IRP

The requirements for Internet Reverse Proxy (IRP) in an MDC environment are:

- The process for adding or removing IRP is the same for a Single-data Center system as they are for a MDC system.
- When adding a data center to a MDC system, all data centers or none of the data centers should be configured to use IRP.

- One IRP node is used per data center.
- Modifying IRP requires that the system be place in Maintenance Mode. In a MDC system, IRP can be added or removed one system at a time to avoid a service interruption.
- In a MDC environment, adding or removing a local public VIP on one data center does not affect the other data centers.

For a description of internal Internet Reverse Proxy topology, see the *Cisco WebEx Meetings Server Planning Guide*.

Before You Begin

To enable public access you must first configure an Internet Reverse Proxy virtual machine to serve as your public access system. Start VMware vCenter and perform the following:

- Back up your virtual machines using VMware Data Recovery (vSphere 5.0) or VMware vSphere Data Protection (vSphere 5.1). This enables you to revert the changes if necessary. See Creating a Backup by Using VMware vCenter, on page 6 for more information.
- Deploy an Internet Reverse Proxy virtual machine using the same OVA file that you used to deploy your administrator virtual machine. Your Internet Reverse Proxy virtual machine must be on the same subnet as the public virtual IP address.

Note If you have a High Availability system, you must also deploy an Internet Reverse Proxy virtual machine for your High Availability system.

Deploy an Internet Reverse Proxy virtual machine by using the same OVA file that you used to deploy your administrator virtual machine.

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, on page 90.
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, on page 88 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 **System** > **View Details**.

Step 4 Select **Add Public Access**.

Step 5 Enter your Internet Reverse Proxy virtual machine in the **FQDN** field.
There are two fully qualified domain name (FQDN) fields if your system is configured for high availability. Enter your high availability FQDN in the second field.

Step 6 Select **Detect virtual machines**.
If your system is not configured for High Availability, a table appears displaying the Internet Reverse Proxy virtual machine.

If your system is configured for High Availability, a table appears displaying the primary system Internet Reverse Proxy virtual machine and the high availability Internet Reverse Proxy virtual machine.

If your system has any updates that are incompatible with the OVA version you used to create the Internet Reverse proxy virtual machine, you receive an error message and cannot proceed until you redeploy the Internet Reverse Proxy virtual machine by using an appropriate OVA file.

Step 7 Select **Continue**.

Step 8 Enter the IP address from the same subnet that you used to configure your Internet Reverse Proxy virtual machine in the **Public (VIP) Virtual IPv4 Address** field and select **Save**.
Your system is updated and public access is configured. Keep your browser window open for the entire process.

If your system requires minor updates compatible with the OVA version you used for creating the Internet Reverse Proxy virtual machine, they are automatically applied to your Internet Reverse Proxy virtual machine.

Step 9 If your system requires minor updates, you are prompted to select **Restart** after the updates are complete.
After the system restarts, you receive a confirmation message indicating that you have added public access.

Step 10 Verify your configuration. If you are satisfied, you can delete the virtual machine backup that you configured before performing this procedure.

Step 11 Select **Done**.

Step 12 Verify that your security certificates are still valid.
Because this procedure changes your virtual machines, it might affect your certificates. If necessary, your system provides a self-signed certificate to keep your system functioning until you can reconfigure your certificates. See Managing Certificates, on page 213 for more information.

Step 13 Make any necessary changes to your DNS servers.

Step 14 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, on page 90.

Meeting service on the data center is restored.

Removing Public Access

Before You Begin

Back up your virtual machines using VMware Data Recovery or VMware vSphere Data Protection. See Creating a Backup by Using VMware vCenter, on page 6 for more information. Make sure you power on your virtual machines after your backup is complete.

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, on page 90.
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, on page 88 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 **System** and then select the **View More** link in the System section.
The **Properties** page appears.

Step 4 Select the desired site, select **Remove Public Access**, and select **Continue**.
After you remove public access from your site, you cannot add the same Internet proxy virtual machine to that site. To reconfigure public access, you must start over by redeploying an Internet reverse proxy virtual machine from the OVA file. See Adding Public Access to Your System by using IRP, on page 129 for more information.

Public access is removed from the site.

Step 5 Select **Done**.

Step 6 Open VMware vCenter. Power off, and delete the Internet Reverse Proxy machine (and high-availability Internet reverse proxy machine, if deployed) from your system.

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, on page 90.

Meeting service on the data center is restored.

Configuring IPv6 for Client Connections

When you have a non-split-horizon network topology, all users (internal and external) with an IPv6 client connection can access the WebEx site URL using the public VIP address to host and access online meetings. When the private IPv6 virtual IP address information is configured, administrators with an IPv6 client connection can sign in to the Administration site.

Note

- The IPv6 private virtual IP address must be on the same IPv6 subnet as the Admin virtual machine.
- The IPv6 public virtual IP address must be on the same IPv6 subnet as the Internet Reverse Proxy virtual machine.

Before You Begin

Consider the following when configuring an IPv6 client connection:

- Configuring an IPv6 connection only for non-split-horizon network topologies.
- IPv4 address information should already be configured for internal virtual machines and the Internet Reverse Proxy.

- The IPv4 private and public virtual IP addresses should already be configured before you configure an IPv6 public virtual IP address.
- The private and public virtual IP address for IPv6 client connections are on separate subnets.
- Configure the DNS servers so your Administration site URL points to the private IPv6 and the private IPv4 virtual IP addresses.
- Configure the DNS servers so your WebEx site URL points to the public IPv6 and the public IPv4 virtual IP addresses.

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, on page 90.
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, on page 88 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 **System** and then select the **View More** link in the System section.

Step 4 In the Virtual IP Address section, select a link in the **Type** column.

- Select the *Public* link to configure the IPv6 address for accessing the WebEx Site URL.
- Select the *Private* link to configure the IPv6 address for accessing the Administration URL.

The Private or Public Virtual IP Address page displays the previously entered IPv4 IP address, subnet mask, and gateway IP address of the WebEx Site URL and Administration URL.

Step 5 In the IPv6 **Address** column, enter the IPv6 IP address, subnet mask, and gateway IP address of the WebEx Site URL and Administration URL.

Step 6 Select **Save**.

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, on page 90.

Meeting service on the data center is restored.

Changing the CWMS Subnet

Important Perform this procedure from a computer that belongs to the same subnet as the CWMS. Site Administration is accessible from either the original or the new subnet for the CWMS.

Before You Begin

If you plan to keep the same DNS servers, keep the old DNS entries until the change is complete. If you are changing DNS servers, configure the servers, turn off Maintenance Mode, and then change the subnet.

To keep the same fully qualified domain names (FQDNs) and change only the IP addresses, you must do this in two stages by using temporary names. Typically you can change the IP address of a server only if you also change its name. This is to avoid a change simply by changing a DNS entry. However, Admin and Site URLs do not fall into this category. Sometimes that the computer making all the administrative changes appears to be unable to browse to the Admin URL pages. If that happens, make sure that you can ping `nslookup` and if necessary, flush the local PC DNS cache after any changes.

We recommend for all versions of CWMS:

- Create a Remote Support Account before beginning any maintenance work.
- Apply for new certificates to be used when the IP address change is completed. In the interim, the system can use a self-signed certificate.
- Verify that the DNS entries are prepared and ready. If the virtual machines do not restart, restart only the Admin virtual machine and change the Network Adapter #2 assignment. The IRP can remain up, and you can change the assignment for Network Adapter #2 when you see the Admin virtual machine rebooting.

Note During the subnet change, you must edit the virtual machine settings to move the virtual NICs to another VLAN. You cannot simply power off, change the system, and power it back on. Turn off Maintenance Mode to apply the changes and cause all the virtual machines to reboot. If you fail to change the VLANs after the virtual machines reboot, the network interfaces appear, but they cannot communicate.

Step 1 Create new DNS entries for new (or temporary) names pointing to new addresses.

a) Go to the Admin window, open the servers one-by-one, and enter the new FQDNs.
b) Turn on Maintenance Mode.
c) Verify that all parameters are correct for the new subnet (including the subnet mask and gateway).

Step 2 After making the changes, go back into each server and verify that the FQDNs are entered correctly.

Step 3 Turn Off Maintenance Mode and monitor the virtual machine consoles in the vSphere client.
The time between turning off Maintenance Mode and the completion of the reboot can be long.

Step 4 When a virtual machine comes up from reboot, change the VLAN for Network adapter 1.
You can do this step live, without powering the system off and back on.

The Admin and virtual IP address (VIP) addresses must be on the same subnet. When the system comes back up, the VIP is on a different subnet than the Admin node. This scenario is acceptable only temporarily.

Step 5 Open the VIP pages and edit the IP addresses of the Public and Private VIPs.
We recommend that you revisit the settings to confirm that the changes are accurate.

Step 6 (Optional) Open General Settings and change the URLs (only if you planned for this change).
This process doesn't need temporary values. If you change the site URL, old meeting links stop working.

Step 7 Turn off Maintenance Mode.
The system reboots. Sometimes the system simply restarts and fails to reboot. Monitor the virtual machine console. If the system doesn't reboot all nodes after you turn off Maintenance Mode, reboot the Admin nodes manually.

Step 8 After the virtual machines come up from reboot, change the VLAN for Network adapter 2.
It isn't necessary to power the system off and back on.

The system belongs to the new subnet.

What to Do Next

If you used temporary names, Replace the Temporary Names, on page 135.

Replace the Temporary Names

Complete this procedure to replace the temporary names with the original fully qualified domain names (FQDN).

Step 1 In the DNS, connect the permanent names to the new IP addresses.
To change the FQDN for the new IP addresses, use Site Administration. Open the servers one-by-one to enter permanent names.

Step 2 Optionally edit the URLs.

Step 3 Turn off Maintenance Mode.

Step 4 After the system reboots, delete the unused entries from DNS.

Step 5 Verify that the system works correctly by accessing the Admin URL. We also recommend that you test access to meeting recordings on the NFS and test the system by creating a new recording.

Step 6 Double check the CUCM trunks and modify IP addresses as necessary.

Configuring General Settings

General settings include the following parameters:

- Site Settings—Manages the site URL.
- Administration Site Settings—Manages the administration site URL.

Virtual IP addresses are shown in the information block and can be managed on the **System** > **Properties**.

Changing Your WebEx Site Settings

Use this procedure to change the original WebEx site URL to a new URL. You configured your original WebEx site URLs during deployment. In an MDC system, the WebEx site URL is configured during the process of joining data centers. For more information about site URL configuration and naming conventions, see WebEx Site and WebEx Administration URLs, on page 35.

After this change is made, system traffic coming from hostnames, other than the ones currently configured, is dropped.

Before You Begin

We recommend that you notify users of the pending change and suggest that before the change is made that they download any recordings they want to retain.

If users attempt to use the original URL, those users cannot:

- Host or join meetings
- Log in from web pages, productivity tools, or mobile applications
- Play back recordings

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, on page 90.
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, on page 88 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 **System** > **(Configuration/General settings) View More**.
The General Settings window displays.

Step 4 If this is an MDC system, select the data center.

Step 5 In the Site Settings section to be modified, select **Edit**.

Step 6 Enter the URLs and select **Save**.

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, on page 90.

Meeting service on the data center is restored.

What to Do Next

- Update your site certificate to ensure secure access. See Managing Certificates, on page 213 for more information.
- Notify hosts that they should reschedule all meetings.

Setting the Time Zone, Language, and Locale

Before You Begin

Step 1 From the Administration web site, navigate to **Settings** > **Company Info**

Step 2 Select the local **Time Zone** for this system from the drop-down list.

Step 3 Select the **Language**.

Step 4 Select the country **Locale**.

Step 5 Select **Save**.

Changing Your Administration Site Settings

Use this procedure to change the original administration site URL to a new URL. You configured your original administration site URL setting during deployment. In an MDC system, your administration site URL is configured during the process of joining data-centers. For more information about site URL configuration and naming conventions, see WebEx Site and WebEx Administration URLs, on page 35.

Before You Begin

We recommend that you notify users of the pending change and suggest that before the change is made that they download any recordings they want to retain.

If users attempt to use the original URL, those users cannot:

- host or join meetings
- log in from web pages, productivity tools, or mobile applications
- playback recordings

Step 1 Sign in to the Administration site.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off, on page 90.
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, on page 88 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 **System**.

Step 4 In the Configuration section, select **View More**.

Step 5 In the Administration Settings section, select **Edit**.

Step 6 Enter your new Administration site URLs in the dialog box and select **Save**.

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, on page 90.

Meeting service on the data center is restored.

What to Do Next

Update your site certificate to ensure secure access. See Managing Certificates, on page 213 for more information.

Notify hosts that they should reschedule all meetings.

Configuring Servers

Use these features to configure your servers:

- SMTP Server—The SMTP server handles the sending of email from Cisco WebEx Meeting Server to the destination.
- Storage Server—The NFS server is the storage server where the system stores all the meeting recordings.

Configuring an Email (SMTP) Server

Configure an Email server to enable your system to send meeting invitations and other communications to users.

It is important that the Email server is always operational. Email is the primary method of communication with your users including recording notifications, meeting information changes, account status, and many other important announcements. (See also Adding Users, on page 111.)

Turning on Maintenance Mode is not required to change these properties.

Important Users are identified to the system by Email address. If a user Email address is changed and the user remains active, the Email address on CWMS must also be changed or that user will not receive notifications.

CWMS cannot establish a connection with Exchange if the password contains special character, such as ^, &, *, (), _, +, or /\.

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 **System** and select **View More** in the Servers section.

Step 3 In the **SMTP Server** section, select **Edit**.

Step 4 Enter the fully qualified domain name (FQDN) of a mail server that the system uses to send emails.

Step 5 (Optional) Select **TLS enabled** to enable Transport Layer Security (TLS). (Basic authentication is enabled by default.)

Step 6 (Optional) Edit the **Port** field to change the default value.
The SMTP default port numbers are 25 or 465 (secure SMTP port).

Note The Web node and Admin node send SMTP requests to the configured Email server. If there is a firewall between the internal Web and Admin virtual machines and the Email server, SMTP traffic might be blocked. To ensure Email server configuration and Email notification work properly, port 25 or 465 (secure SMTP port number) must be open between the Email server and the Web and the Admin virtual machines.

Step 7 (Optional) Enable mail server authentication, select **Server authentication enabled**. If you enable authentication, enter the **Username** and **Password** credentials necessary for the system to access the corporate mail server.
Emails from the system are sent by using `admin@<WebEx-site-URL>`. Ensure that the mail server can recognize this user.

For micro, small, or medium systems, email notifications come from the administration virtual machines (either the primary or high-availability system).

For large systems, email notifications come from the web virtual machines (either on the primary or high-availability system). In a large system, there are two web virtual machines on the primary system and one web virtual machine on the high-availability system.

Step 8 Select **Save**.

What to Do Next

See Activating or Deactivating Users or Administrators, on page 114, Adding Users, on page 111, and Editing Users, on page 112.

Email Templates

A list of email templates:

- All Admins - Welcome Email
- Forgot Password - Reset Password-Admin
- Forgot Password - Password Changed-Admin

- Import finished
- Import aborted
- Export finished
- Export aborted
- Orion Site URL changed-Admin
- Orion Admin URL changed-Admin
- Primary admin - License-free Trial Started
- 1st alarm: Buy license
- 2nd alarm: Buy license
- Free license expired
- Licenses added successfully
- License converted successfully
- 1st alarm: Convert license
- 180 day expiration
- Alarm: SSL Certificate expiring
- SSL Certificate expired
- Alarm: SSO IdP Certificate expiring
- SSO IdP Certificate expired
- Alarm: Secure TC Certificate expiring
- Sec TC Certificate expired
- Monthly Report ready
- Customized Report ready
- Customized Log ready
- Alarm: Meeting Errors
- Alarm: Meeting participants
- Alarm: CPU usage
- Alarm: Memory usage
- Alarm: Network bandwidth usage
- Alarm: Storage usage
- Account Deactivated
- Send Email to All Users
- Account Reactivated-Admin
- Clear Alarm: CPU usage

- Clear Alarm: Meeting Errors
- Clear Alarm: Meeting participants
- Clear Alarm: Memory usage
- Clear Alarm: Network bandwidth usage
- Clear Alarm: Storage usage
- HA system present
- No HA system
- Back In Compliance
- AD-Sync Success
- AD-Sync Failed
- Account Locked
- Account Locked-Unlock
- Alarm License - user grace license allocated
- Alarm License - warn admin of user grace license allocation
- Alarm License - warn admin of grace license expiration
- Alarm License - warn admin when all grace licenses are used up
- Alarm License - warn admin when license usage over threshold
- Alarm audit logs
- Alarm MDC - DB Replication
- Clear Alarm MDC - DB Replication
- Alarm HA System - DB Replication Status
- Clear Alarm HA System - DB Replication Status
- Alarm MDC - Datacenter Status
- Alarm MDC - Datacenter Unreachable
- Alarm MDC - Datacenter Blocked
- Clear Alarm MDC - Datacenter Status
- Clear Alarm MDC - Datacenter Unreachable
- Conflict in user profiles auto-corrected
- Email when clocks are back to normal
- Email when clocks drift
- Meeting Summary report for Host

Example Alarms

- **Alarm: Meeting Issues**

Configurable percent: n%

Subject: Alert: Meetings experiencing issues has reached %n% of %MaxData%

On your Cisco WebEx site n% meetings in progress are experiencing issues.

- **Alarm: Meeting participants**

  Configurable percent: n%

  Subject: Alert: Online meeting participants has reached n% of %Total%

  Number of online meeting participants has reached n% of system capacity.

- **Alarm: CPU usage**

  Alert: CPU usage has reached %X% MHz of %Y% MHz (75%)

  CPU usage has reached 75%

- **Alarm: Memory usage**

  Alert: Memory usage has reached %X% GB of %Y% GB (75%)

  Memory usage has reached 75%

- **Alarm: Network bandwidth usage**

  Subject: Alert: Network bandwidth usage has reached %X% Mbps of %Y% Mbps (75%)

  Network bandwidth usage has reached 75%

- **Alarm: Storage usage**

  Subject: Alert: Storage usage has reached %X% GB of %Y% GB (75%)

  Because your storage usage has reached 75%, meeting recording is disabled for all users to ensure optimal performance for WebEx meetings.

  Users will not be able to record meeting until storage is available on the Network File Server storage system.

- **Alarm License - user grace license allocated**

  Subject: Alert: Your temporary host license expires in 180 days

  Your temporary host license expires in 180 days.

  Contact your administrator to install permanent licenses.

- **Alarm License - warn admin of user grace license allocation**

  Subject: Alert: Temporary host licenses expire in 180 days

  %NumberofLicenses% temporary licenses expire in 180 days.

  Install additional permanent licenses to enable these users to host meetings.

- Alarm License - warn admin of grace license expiration

  Subject: Alert: Temporary host licenses expired

  %NumberofLicenses% temporary licenses expired.

  Install additional permanent licenses to enable these users to host meetings.

- **Alarm License - warn admin when all grace licenses are used up**

  Subject: Alert: All licenses assigned

All licenses are assigned and new users cannot host meetings.

Install additional permanent licenses to enable users to host meetings.

- **Alarm License - warn admin when license usage over threshold**

  Configurable threshold : $n

  Subject: Alert: Licenses usage over threshold

  $n of all permanent licenses are assigned. Install additional permanent licenses to allow more users to host meetings.

- **Alarm audit logs**

  Configurable percent = n%

  Subject: Alert: Audit logs are nearing capacity

  The log partition is n% of full capacity.

  Increase free disk space.

  Or you can navigate to **Settings** > **Application Audit Log** > **Application Audit Log** on CWMS system section **Log Purging Settings**.

  Select date before all log archives are to be deleted and click Purge Log Archive.

- **Alarm MDC - DB Replication**

  %ReplicationStatus% = Inactive, Limited

  Subject: Alert: Data synchronization between datacenters has been %ReplicationStatus%

  Data synchronization from DC-1 to DC-2 has been %ReplicationStatus%. Verify that the state of the network link between the data centers is good and meets Multi-datacenter requirements.

- **Alarm HA System - DB Replication Status**

  Subject: Alert: Data synchronization has been Inactive

  Data synchronization in the data center has been Inactive. Verify that the network connection between the virtual machines meets the High Availability requirements.

- **Alarm MDC - Datacenter Status**

  %DatacenterStatus% = Partial Service, Down

  Subject: Alert: Datacenter is %DatacenterStatus%

  The MyDatacenter1 data center is in a %DatacenterStatus% state and the system is attempting to fix the problem.

  System is operating normally, but a data center has an issue that should be addressed as soon as possible. If this is intentional, then ignore this message.

- **Alarm MDC - Datacenter Unreachable**

  Subject: Alert: The MyDatacenter2 datacenter is unreachable

  The MyDatacenter2 datacenter is not reachable from the MyDatacenter1 datacenter. It is not operational or is disconnected from the network.

  If you are working with the data center and it was brought down intentionally, you can ignore this message.

- **Alarm MDC - Datacenter Blocked**

Subject: Alert: Datacenter is Blocked

The MyDatacenter1 datacenter is blocked. The system is redirecting end user traffic to the other data center and is attempting to self-correct the problem.

The <site name> system continues to operate normally and this data center problem is transparent to users, but the issue should be addressed as soon as possible. If you are working with the datacenter and it was put into this state intentionally, you can ignore this message.

- **Email when clocks drift**

  Subject: Customized log file is ready

  A clock drift between the Admin virtual machines of data centers DC-1 and DC-2 was detected. Synchronization of the clocks is critical to maintaining consistency of data shared by these data centers.

  This problem is transparent to the end users, but the issue should be addressed as soon as possible.

  Verify that the correct NTP servers are configured on the virtual machine hosts on both data centers and that the NTP servers are reachable from those hosts.

Configuring an NTP Server

Set the NTP server to the correct time from a time source and adjust the local time in each connecting computer. If you choose not to use an NTP server make sure that the time on the ESXi host is correct.

Important NTP is mandatory in a Multi-data Center (MDC) environment.

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 **System.**

Step 3 Under Servers, select the **View More** link.

Step 4 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off, on page 90.
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, on page 88 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 5 Under NTP Server, select the **Edit** link.

Step 6 Specify the NTP server or select the local server.
If you select **Use NTP server to update time**, you must also enter the IP address of the NTP server.

Step 7 Select **Save**.

Step 8 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, on page 90.

Meeting service on the data center is restored.

Configuring a Storage Server

Use a storage server to back up your system for disaster recovery (see Disaster Recovery by Using the Storage Server, on page 150) and to store meeting recordings. The supported storage methods are Network File System (NFS) and Secure Storage (SSHFS). Verify that your storage server is accessible from all internal virtual machines. There is also a VMware-provided VMware Data Recovery feature to backup the virtual machines.

You do not need to connect your storage server to external virtual machines such as external Internet Reverse Proxy (IRP) servers.

Your storage server backs up the following data daily:

- Certain system settings
- User information
- Meeting information
- SSL certificates uploaded into the system
- The site URL

Backups are performed daily and are initially set for 4:20 a.m. local time. Cisco WebEx Meetings Server runs during the backup process without any interruption to meetings, recordings, or other functions. The system does not remove the previous backup until the following daily backup is complete to ensure that a backup is available.

Your system takes approximately five minutes to back up 500 MB. The time it takes to back up your system depends on storage speed, NFS speed, and other factors. A 70-GB database takes approximately 1 hour to back up and 10 minutes to transfer it to the NFS. Transfer time is 12 MB/sec to allow other network communication and to ensure the continuous operation of the system.

Secure Storage includes the following features:

- Encrypted communication.
- Limit storage server access to authorized accounts.
- Permissions are mapped to a defined user; 777 permissions on storage are no longer required.

Restriction Cisco WebEx Meetings Server must have exclusive use of the NFS share, because the system runs various scripts on NFS files and directories. Do not manually create files or directories in the NFS share used by Cisco WebEx Meetings Server

Adding an NFS or SSH Storage Server

Configure your system to use the storage server for meeting recordings and disaster recovery. Your choice of storage server depends on the configuration of your system.

Before You Begin

Port 22 is used for Secure Storage.

Ports 111, 1110, 2049, 4045 are standard ports for various NFS services and NFS configurations of NFS server implementations.

- NFS traffic requires ports 111 (TCP and UDP) and 2049 (TCP and UDP).
- Cluster status requires port 1110 (TCP) and client status requires port 1110 (UDP).
- NFS lock manager requires port 4045 (TCP and UDP).

Make sure that you configure your Unix access privileges so that your system can store user-generated content and system backups. (Applies to NFS storage.)

On Linux-based storage systems, configure the read and write permissions for anonymous users for the directory to be used for your Network File System (NFS). See Connect a Linux Client to the NFS Share , on page 149.

On Windows-based storage systems, enable the **Network Access: Let Everyone permissions apply to anonymous users** setting. In addition, you must provide the Everyone user group read and write permissions for the NFS. See Configure an NFS Share, on page 148.

We recommend using openSSH server for secure storage. However, this feature is independent of the make of the SFTP server and the feature should work with every server supporting this protocol.

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, on page 90.
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, on page 88 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 On the System tab, in the Servers section, select **(Servers) View More**.
If a storage server is present on your system, it is displayed on this page. If there is no storage server present on your system, you are given the option to add one.

Step 4 In the Storage Server section, select **Add a Storage Server now** or **Edit**.

Step 5 Select **NFS** or **Secure Storage**.

Step 6 (Optional) If you selected **NFS**: and . Otherwise, go to the next step.

a) Enter the NFS mount point.
b) Select **Save**.
The system confirms your NFS mount point.
c) Select **Continue**.

You are sent a confirmation message that your storage server has been added.

Step 7 (Optional) If you chose **Secure Storage**.

a) Enter the username for Secure Storage.
Usernames must begin with a lowercase letter. Ending a username with a dollar sign ($) is allowed.

Allowed characters: Lowercase letters, numbers, underscore, and dollar sign. All other characters are forbidden.

b) Enter the password for Secure Storage.

c) Enter the name of the storage server in the **Secure Storage Mount Point** field.
Allowed characters: `[A-Z] [a-z] [0-9] !#$()+,-:;=_][{}~`

Forbidden characters: `/\" ' ` %&*<>?|^`

d) Select **Save**.

The system confirms your mount point. You are sent a confirmation message that your storage server has been added.

Step 8 Select **Done**.

Step 9 (Optional) Click the **System Backup Schedule (time)** to display the System Backup Schedule pop-up window, select a time from the drop-down menu, and then select **Save**.
A daily backup occurs at the time you selected.

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, on page 90.

Meeting service on the data center is restored.

What to Do Next

Make sure that:

- Your storage server is accessible from outside of Cisco WebEx Meetings Server.
- Your storage server is powered on.
- There is network connectivity to your storage server.
- Mount/access is possible from a non-Cisco WebEx Meetings Server machine.
- Your storage server is not full.

Note If a user inadvertently deletes a recording from the **Cisco WebEx Meeting Recordings** page and the recording is saved on the Network File System (NFS) storage server, you can contact the Cisco Technical Assistance Center (TAC) for assistance in recovering the recording.

Install NFS File Services

Step 1 Launch Server Manager.

Step 2 On the top menu, select **Manage**.

Step 3 Select **Add Roles and Features**.
The **Before you begin** window appears.

Step 4 Select **Next**.
The **Select installation type** window appears.

Step 5 Verify that **Role-based or feature-based installation** is selected and select **Next**.
The **Server selection** window appears.

Step 6 Select **Next**.
The **Select server roles** window appears.

Step 7 Expand **File and Storage Services** > **File and iSCSI Services**, and then check **Server for NFS**.

Step 8 Select **Next**.
The **Select feature** window appears.

Step 9 Select **Next**.

Step 10 Confirm the installation details, and then select **Install**.

Configure an NFS Share

Configure an NFS share:

Before You Begin

Install NFS file services. (See Install NFS File Services , on page 148.)

Step 1 Launch File Explorer.

Step 2 Create a new directory for your NFS share.

Step 3 Right-click the directory and select **Properties**.

Step 4 Select the **NFS Sharing** tab.

Step 5 Select **Manage NFS Sharing**….

Step 6 Check **Share this folder** and enter 65534 in **Anonymous UID** and **Anonymous GID**.
Anonymous UID defaults to –2. On 16-bit machines, this value can fail because anonymous (nfsnobody) UID –2 is equivalent to 65534 in 16-bit numbers. (See www.troubleshooters.com/linux/nfs.htm).

Step 7 Enter a **Share** name.
This is the name used when a user connects to this NFS share.

Step 8 Select **Permissions**.

Step 9 Select **Add** and enter the IP address or hostname of the client connections.

Step 10 Choose Read–Write access or Read-Only access and select **OK**.

Step 11 Select **Apply** > **OK**
An NFS share is hosted on a Windows Server 2012 R2.

What to Do Next

Connect a Linux Client to the NFS share. (See Connect a Linux Client to the NFS Share , on page 149.)

Connect a Linux Client to the NFS Share

Step 1 Log on to a Linux server or desktop.
Open a terminal window, if you are in a Desktop version of the operating system.

Step 2 Create a new directory on which to mount the Windows NFS share. For example, `mkdir/postprod`.

Step 3 Mount the NFS share to the new directory. For example, `mount.nfs slfileserver01:/postprod /postprod`

Step 4 If the client has Read–Write access, test the share by creating a new file. For example, `touch file01.txt`.

Changing to a Different Storage Server

When you switch your storage server from the current NFS or SSH NFS to a replacement, the stored files become inaccessible. To restore access, transfer all meeting recordings, and backups to the new storage 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 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off, on page 90.
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, on page 88 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 **System** > **(Servers) View More** > **Remove Storage Server**.

Step 4 Manually transfer recording and backup files from the old storage server to the new storage server.
We cannot provide specific instructions for transferring these files, because each system is unique.

Step 5 In the Storage Server section, select **Add a Storage Server now**.

Step 6 Enter the replacement NFS mount point or the replacement Secure Storage username.
Usernames must begin with a lowercase letter. Ending a username with a dollar sign ($) is allowed.

Allowed characters: Lowercase letters, numbers, underscore, and dollar sign. All other characters are forbidden.

Example:
`user1`

Step 7 Enter the replacement NFS mount point or the replacement Secure Storage password.

Example:
`*******`

Step 8 Enter the replacement NFS mount point or the replacement Secure Storage mount point.

Example:
`192.168.10.10:/CWMS/backup`

Step 9 Select **Save**.
The system confirms your replacement NFS mount point or Secure Storage mount point.

Step 10 (Optional) Select **Yes** to perform the disaster recovery procedure or select **No** to skip this step.
If there are no system backup files on the replacement storage server, this step is automatically skipped. For additional information about disaster recovery, see Disaster Recovery by Using the Storage Server, on page 150.

Step 11 Select **Continue**.
You receive a confirmation message that your storage server has been added.

Step 12 Select **Done**.

Step 13 (Optional) You can change the default time for the daily backup. In the Storage Server section, click the System Backup Schedule **time** and select another time from the drop-down list. Then select **Save**.
A daily backup occurs at the time you selected.

Step 14 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, on page 90.

Meeting service on the data center is restored.

Disaster Recovery by Using the Storage Server

A disaster could be a network crash, server failure, data center outage, or other event that makes your system unusable. There are two types of disaster recovery:

- Single-data Center (SDC) disaster recovery—You can reinstall your SDC system in the same data center and restore it to the same state by using storage server backups.
- Multi-data Center (MDC) disaster recovery—If one data center fails, you can access the MDC system through the second data center, restore the damaged data center, and join the data centers to restore the

MDC system. If the failed data center hosts the License Manager, it might be necessary to reinstall the License Manger, as it can run on only one system at a time.

After you configure a storage server, your system is backed up on a daily basis. A system backup notice appears on your dashboard that includes information about the latest backup. Only one backup system is kept in storage at a time. After you perform an upgrade or update, the backup from your previous Cisco WebEx Meetings Server version is retained. We recommend that you do not use the same storage directory for different Cisco WebEx Meetings Server installations.

Note that disaster recovery:

- Takes more than 30 minutes
- Overwrites your settings with the settings on the latest backup
- Requires you to perform additional steps to restore service to your users (detailed in *What To Do Next* in this section)

This procedure backs up certain system settings, user information, meeting information, SSL certificates uploaded into the system, and the site URL. The backup process does not store VMware credentials or IP address information for individual virtual machines. (There is also a VMware-provided VMware Data Recovery feature to back up the virtual machines. See http://www.vmware.com/pdf/vdr_11_admin.pdf for more information.) When you perform a disaster recovery, you must manually reapply certain settings including the following:

- Connections to certain external components, for example Cisco Unified Communications Manager (CUCM).
- SSL certificates (in case the hostnames of the disaster recovery system differ from those in the original system).
- On SDC systems, you can optionally use the same IP address or hostname. On multi-data centers systems, you can optionally use the original IP addresses or hostnames for your primary system.

Perform this procedure after a disaster has occurred and you have lost the ability to use your system.

Before You Begin

To perform disaster recovery procedures:

- A storage server must have been configured. If you do not have a storage server configured, the **Disaster Recovery** option is not available and backups are not created. See Adding an NFS or SSH Storage Server, on page 146 for more information.
- Your recovery system must be the same deployment size and software version as your original system.

  For a high-availability (HA) system, you must first configure disaster recovery and then configure HA on that system. If you have a HA system that requires recovery from a disaster, you must first restore your system and then configure HA on the restored system. For more information on HA, see Adding a High Availability System, on page 43.
- A backup OVA stored on NFS is not sufficient to rebuild a system. We recommend that you have the current OVA file stored outside the system for disaster recovery. In this context, disaster recovery includes the need to recover from a failed *update*. The OVA file must be ordered by using a product upgrade tool or through customer service. Sometimes this can be a lengthy process, hence our recommendation to have access to the OVA file for the current system prior to making a system altering procedure.

If you have software subscription, you can order an OVA file through the product upgrade tool (PUT) at http://tools.cisco.com/gct/Upgrade/jsp/productUpgrade.jsp by using your contract number. If you choose edelivery, you can download it from the site. If you need assistance with this process or do not have access to PUT, contact your account team or customer service. Your Cisco Customer Service Contacts can be found here at http://www.cisco.com/cisco/web/siteassets/contacts/index.html#~tab-b

Step 1 Sign in to the Administration site on a system from where you can restore your deployment.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off, on page 90.
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, on page 88 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 **System** > **(Servers) View More** > **Add Storage Server**.

Step 4 Select **Secure Storage**.

Step 5 Enter the name and password for your storage server in the **NFS Mount Point** field and select **Save**.

Example:
192.168.10.10:/CWMS/backup.

Step 6 Select **Continue** to proceed with disaster recovery.
If the recovery system deployment size and software version matches your original system, you can proceed with disaster recovery. If the system has a different deployment size or software version, you cannot proceed until you redeploy the application on your recovery system so that the deployment size and software version match the original deployment. The IP address or hostname does not have to match your original deployment.

Step 7 Select one of the following actions to continue:

- **Cancel—**Back up your pre-existing system before adding a storage server. After you back up your system, return to this page and select **Continue** to proceed.
- **Continue—**Overwrite your pre-existing system and continue with disaster recovery.

The disaster recovery process begins. If you close your browser, you cannot sign back into the system until the process is completed.

Step 8 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, on page 90.

Meeting service on the data center is restored.

What to Do Next

You must perform the following procedures to restore service to your users:

- Reconfigure your teleconferencing settings. Refer to Configuring CUCM in the Planning Guide for more information.
- Reconfigure your SSO settings. See Configuring Federated Single Sign-On (SSO) Settings, on page 229 for more information.
- Reconfigure your SNMP settings. See Configuring Your SNMP Settings, on page 153 for more information.
- Reconfigure your certificates. You might have to reload your SSL certificates if they do not match the SSL certificates that are configured on the recovery system. See Restoring an SSL Certificate, on page 222 for more information.
- The recovered system is initially configured for License Free Mode that expires in 180 days. Re-host your previous system licenses on the recovered system. See Re-hosting Licenses after a Major System Modification, on page 256 and About Host Licenses, on page 250 for more information.
- Configure your DNS settings so that your site URL points to the current VIP. Your VIP on the restored system might be different from what you had on your original system. You must complete your DNS configuration for end users to use their original links to sign into or join meetings on the restored system. See Changing the Private and Public Virtual IP Addresses, on page 129 for more information.
- If you have configured your system for Directory Integration and enabled LDAP authentication, verify that your CUCM credentials work. After you take your system out of maintenance mode and your system reboot is complete, sign in to the Administration site, select **Users** > **Directory Integration**, and then select **Save**. If your CUCM credentials are incorrect, you receive an **Invalid Credentials** error message. If you receive this error message, enter the correct credentials and select **Save** again. (See "Configuring Directory Information.")

Configuring Your SNMP Settings

You can configure the following SNMP settings:

- Community strings—SNMP community strings authenticate access to MIB objects and function as an embedded password.
- USM users—Configure user-based security (USM) to provide additional message-level security. Select an existing USM configuration to edit it or add additional USM configurations. Other than the default USM user, serveradmin, which has read and write privileges to MIB information, all new USM users that you configure only have read-only privileges to MIB information.
- Notification destinations—Use this feature to configure the trap/inform receiver.

Configuring Community Strings

You can add and edit community strings and community string access privileges.

Adding Community Strings

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, on page 90.
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, on page 88 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 **System** and select the **View More** link in the SNMP section.

Step 4 Select **Add** in the Community Strings section.

Step 5 Complete the fields on the **Add Community String** page.

Option	Description
Community String Name	Enter your community string name. Maximum length: 256 characters.
Access Privileges	Set access privileges for the community string. Options include: • ReadOnly • ReadWrite • ReadWriteNotify • NotifyOnly • None **Default**: ReadOnly
Host IP Address Information	Select your host IP address information type. (Default: **Accept SNMP Packets from any Hosts**) If you select **Accept SNMP Packets from these Hosts**, a dialog box appears below the selection. Enter host names and IP addresses separated by commas.

Select **Add**.

The community string is added to your system.

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, on page 90.

Meeting service on the data center is restored.

Editing Community Strings

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, on page 90.
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, on page 88 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 **System** and select the **View More** link in the SNMP section.

Step 4 Select a community string name link in the Community Strings section.

Step 5 Change the desired fields on the **Edit Community String** page.

Option	Description
Community String Name	Change your community string name. Maximum length: 256 characters.
Access Privileges	Set access privileges for the community string: • ReadOnly • ReadWrite • ReadWriteNotify • NotifyOnly • None **Default**: ReadOnly
Host IP Address Information	Select your host IP address information type. **Default**: Accept SNMP Packets from any Hosts **Accept SNMP Packets from these Hosts**: a dialog box appears below the selection. Enter host names and IP addresses separated by commas.

Select **Edit**.

Your community string information is changed.

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, on page 90.

Meeting service on the data center is restored.

Configuring USM Users

You can add and edit your USM users.

Adding USM Users

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, on page 90.
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, on page 88 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 **System** and then select **View More** in the SNMP section.

Step 4 Select **Add** in the USM Users section.

Step 5 Complete the fields on the **Add USM User** page.

Option	Description
USM User Name	Enter the USM user name you want to configure. Maximum 256 characters.
Security Level	Select the security level. The security level you select determines which algorithms and passwords you can set for the user. Options include: • noAuthNoPriv—No authentication algorithm and password and no privacy algorithm and password for the user. • authPriv—Enables you to configure authentication algorithm and password and privacy algorithm and password for the user. • authNoPriv—Enables you to configure authentication algorithm and password for the user. **Default**: noAuthNoPriv
Authentication Algorithm	Select the authentication algorithm for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**. **Default**: SHA

Option	Description
Authentication Password	Enter the authentication password for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**.
Privacy Algorithm	Select the privacy algorithm for the user. **Note** This option appears only if the security level is set to **authPriv**. **Default**: AES128
Privacy Password	Enter the privacy password for the user. **Note** This option appears only if the security level is set to **authPriv**.

Step 6 Select **Add**.
The USM user is added to your system.

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, on page 90.

Meeting service on the data center is restored.

Editing USM Users

Note The default USM user, serveradmin, is used internally. An administrator can change the USM user name and privacy password for the serveradmin user, but cannot change the security level, authentication algorithm, or privacy algorithm for this user.

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, on page 90.
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, on page 88 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 **System** and then select **View More** in the SNMP section.

Step 4 Select a USM user in the USM Users section.

Step 5 Change the desired fields on the **Edit USM User** page.

Option	Description
USM User Name	Change the USM user name. Maximum 256 characters.
Security Level	Select the security level. The security level you select determines which algorithms and passwords you can set for the user. Options include: • noAuthNoPriv—No authentication algorithm and password and no privacy algorithm and password for the user. • authPriv—Enables you to configure authentication algorithm and password and privacy algorithm and password for the user. • authNoPriv—Enables you to configure authentication algorithm and password for the user. **Default**: noAuthNoPriv
Authentication Algorithm	Select the authentication algorithm for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**. **Default**: SHA
Authentication Password	Change the authentication password for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**.
Privacy Algorithm	Select the privacy algorithm for the user. **Note** This option appears only if the security level is set to **authPriv**. **Default**: AES128
Privacy Password	Change the privacy password for the user. **Note** This option appears only if the security level is set to **authPriv**.

Step 6 Select **Edit**.
The USM user information is changed.

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, on page 90.

Meeting service on the data center is restored.

Configuring Notification Destinations

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, on page 90.
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, on page 88 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 **System** and select the **View More** link in the SNMP section.

Step 4 Select a notification destination link from the **Notification Destinations** list.

Step 5 You can edit the following fields for your notification destination:

Option	Description
Destination Hostname / IP Address	The hostname or IP address of the virtual machine you want to set up as a notification destination.
Port Number	The port number for your virtual machine. **Default**: 162
SNMP Version	Your SNMP version. **Default**: V3
Notification Type	Select **Inform** or **Traps**. **Default**: Inform
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 156 for more information.
Community String **Note** This option appears only when SNMP Version is not set to V3.	Select community strings. See Configuring Community Strings, on page 153 for more information.

Step 6 Select **Save**.
Your notification destination changes are saved.

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, on page 90.

Meeting service on the data center is restored.

Editing a Notification Destination

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, on page 90.
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, on page 88 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 **System** and select the **View More** link in the SNMP section.

Step 4 Select a notification destination link from the **Notification Destinations** list.

Step 5 You can edit the following fields for your notification destination:

Option	Description
Destination Hostname / IP Address	The hostname or IP address of the virtual machine you want to set up as a notification destination.
Port Number	The port number for your virtual machine. **Default**: 162
SNMP Version	Your SNMP version. **Default**: V3
Notification Type	Select **Inform** or **Traps**. **Default**: Inform
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 156 for more information.

Option	Description
Community String **Note** This option appears only when SNMP Version is not set to V3.	Select community strings. See Configuring Community Strings, on page 153 for more information.

Step 6 Select **Save**.
Your notification destination changes are saved.

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, on page 90.

Meeting service on the data center is restored.

Managing Meeting Recordings

The list of recordings can be searched by title, creation date, or owner ID (meeting host).

The list of recordings can be sorted by file name, date, size, or owner.

An administrator can list, filter, or delete meeting recordings.

An auditor can list or filter meeting recordings.

An administrator or auditor cannot playback or download meeting recordings.

Delete Meeting Recordings

When a recording is marked for deletion, the recording status is updated in the database and the recording is no longer listed in the recordings list on the screen. After 6 months the recording is deleted from the file storage (NFS).

The owner of the recording is not notified that the recording has been deleted.

Step 1 Select **System** > **Recordings — View More** to access the Manage Recordings screen.

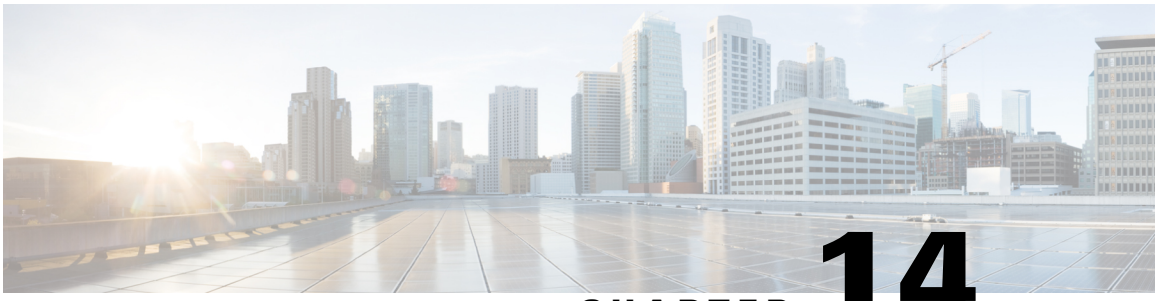
Step 2 Check the box to select the recordings to be deleted.

Step 3 Select **Delete**.

System Backup

Backups are performed daily, initially set for 4:20 a.m. local time. Cisco WebEx Meetings Server runs during the backup process without any interruption to meetings, recordings, or other functions. The system does not remove the previous backup until the following daily backup is complete to ensure that a backup is available.

Your system takes approximately five minutes to back up 500 MB. The time it takes to back up your system is dependent on storage speed, NFS speed, and other factors. A 70 GB database takes approximately one hour to back up and 10 minutes to transfer to the NFS. Transfer time is 12 MB/sec to allow other network communication and to ensure the continuous operation of the system.



CHAPTER 14

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, on page 88 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, on page 241
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.
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, on page 29.

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) [6]
?	

6 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.

Option	Description
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, on page 146 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 4: Password is Excluded When Scheduling Your Meeting

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

Table 5: 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 225 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, on page 90.
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, on page 88 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 225 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, on page 90.

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 170.

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, on page 90.
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, on page 88 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.

Option	Description
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 175.

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 225 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, on page 90.

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, on page 90.

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, on page 88 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, on page 90.

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 179 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 176.

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 182.

To manually add participants for a group, go to Adding Blast Dial Participants, on page 179.

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 166 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 179 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 181 and Importing a Participants List, on page 182 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 179.

To delete a blast dial group, see Deleting a Blast Dial Group, on page 179.

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 179 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 179.

To import a participants list, see Importing a Participants List, on page 182.

To export a participants list, see Exporting a Participants List, on page 181.

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 182.

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 181 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 220 for information about exporting certificates to email to your mobile device users.

Related Topics

Configuring Your Audio Settings, on page 169

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
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

Traffic	QoS Marking
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, on page 114).

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

Option	Description
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 6: 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 7: 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 224.)
- 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, on page 90.
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, on page 88 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, on page 90.

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.
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.

Option	Description
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, on page 90.
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, on page 88 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, on page 90.

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, on page 90.

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 169 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, on page 90.
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, on page 88 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, on page 90.

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**.

Option	Description
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, on page 90.

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 186 and Editing Users, on page 112 for more information.
- Configure a SSO IdP certificate to use this feature. See Importing SSO IdP Certificates, on page 224 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.
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

Field	Description
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.
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, on page 90.
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, on page 88 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, on page 90.

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, on page 90.
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, on page 88 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, on page 90.

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, on page 90.
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, on page 88 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, on page 90.

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, on page 90.

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, on page 90.

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 240.

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, on page 77 for details about setting alarm thresholds.

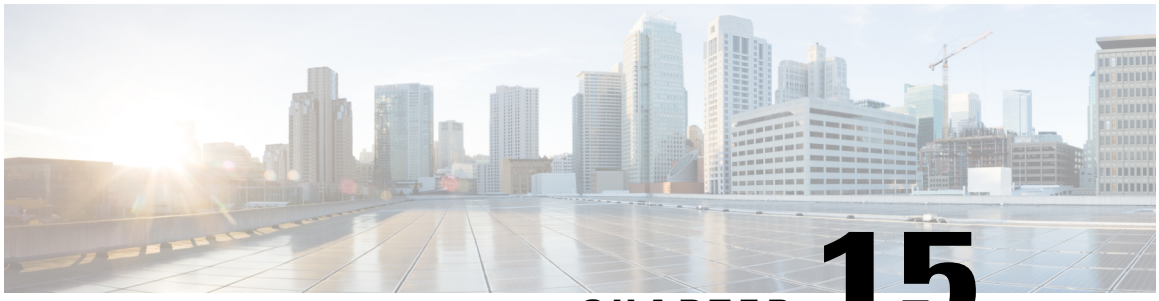
Configuring a Security Sign-in Warning

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.



CHAPTER 15

Managing Reports

About Monthly Reports

For real-time meeting status, view the Dashboard (About the Dashboard, on page 73). For more information about the meeting status, see Viewing the Meetings List, on page 79.
You can view monthly reports and customize reports for specific date ranges. Your reports use the language, locale, and time zone settings configured on the **Company Information** page. See Configuring Company Information, on page 163 for more information.

Important When your system is deployed or upgraded, there is no data available for any of the reports, except the Customized Details Report, until the end of the first month. In that case, the **Download** links and all the other reports described in this section are not available until after the end of the first month.

System Summary Report

Your System Summary Report contains the following reports:

- Service Adoption—A graph depicting the number of unique hosts and attendants over the previous three months.
- User Licenses—The percentage of purchased host licenses the system is using and the number of host licenses used during the past six months. Use these numbers to predict future host license needs and adjust your license purchases accordingly. See Fulfilling Licenses by Using the License Manager, on page 253 for more information.
- System Size—The meeting participant peak and the percentage of system size that peak usage consumed. The graph depicts the meeting participant peaks over the past three months and the expected growth rate over the next three months.

- Storage—The storage usage of your data archive and recordings both as a percentage of total storage space and in total gigabytes (GB). The graph depicts the total storage over the past three months and expected growth rate over the next three months. Use this report to monitor your storage usage. To add storage space, manually copy your existing storage data archive and recordings to your new storage server before you activate it.

Note If you have configured a storage server, this report appears. See Adding an NFS or SSH Storage Server, on page 146 for more information.

- Network—This report displays the following:
  - Your peak network bandwidth consumption in Mbps.
  - A graph depicting the peak network bandwidth consumption in Mbps over the past three months and the expected growth rate over the next three months (the red bar indicates maximum network bandwidth).
  - A pie chart indicating the percentage of bandwidth consumed by each of your system resources.

  Reports draw their data from the database. The monitoring module writes 0 to the database if the bandwidth consumption is less than 1 Mbps. Therefore, a 0 in the report means that feature is not using significant network bandwidth.
- System Planned Downtime & Unplanned Outage—This report displays the following:
  - Your average system uptime over the past three months.
  - The average time of your unplanned system outages over the past three months.
  - The average number of meetings disrupted due to outages over the past three months.
  - A graph depicting the planned downtime and unplanned outages over the past three months and the expected growth rate over the next three months.

Note Increased downtime is sometimes a reflection of increased usage. Be sure to compare your downtime statistics with the usage statistics displayed in other reports.

Meeting Summary Report

Your Meeting Summary Report contains the following reports:

- Meeting Status—A graph depicting the meeting status over the past month, the percentage of meetings that experienced problems, and the total number of meetings held during the month. D
- Meeting Size—A graph depicting the sizes of the meetings held on your system over the past month, a breakdown of the meeting sizes, and detailed information about the largest meeting held during the month.
- Meeting Feature Usage—This report displays the following:
  - The most used feature over the past month including the total number of minutes the feature was used.

- The fastest growing feature on your system over the past month including the growth rate.
- A graph depicting usage in minutes for each feature on your system.
- A graph depicting the growth rate of the fastest growing feature on your system.

- Top Active Participant Email Domains—This report displays the following:
  - A graph depicting the top active participant email domains.
  - A breakdown of the participant email domains.
  - A listing of the top three email domains used by meeting participants on your system.

- Peak Day and Hour—Two graphs. The first graph depicts the busiest day of the week over the past month. The second graph depicts the busiest time of day on your system over the past month.

Downloading Monthly Reports

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 **Reports** from the menu bar.
The **Reports** window shows.

Step 3 Select the link for the monthly report you want to download.

Generating Customized Details Reports

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 **Reports** > **Customize your report**.

Step 3 Select the date range of the reports you want to view and select **Submit**.
The default is the most recent month. You can select a date range extending up to six months back.

The **Customized Report Request Submitted** page appears displaying the dates of your customized report. An email is sent to you with a link to your customized report in CSV format.

Step 4 Select **Done**.

About Customized Details Reports

When you generate customized details reports, you receive an email containing an archive with the following reports in CSV format:

- **Fraud Attempts Report—**Displays any failed telephony access attempts where the caller enters the wrong host or participant access codes or host PIN three times while attempting to start or join a Personal Conference meeting:
  - Access Number Called—The Cisco WebEx call-in number dialed to start or join a Personal Conference meeting.
  - Calling Number—The phone number of the phone used to place the call.
  - Start Time of Call—The date and time of the call.
  - 1st Access Code Attempted—The first invalid access code entered by the caller.
  - Email of 1st Access Code Owner (if available)—The email address of the user associated with the first invalid access code, if the access code is associated with a valid Cisco WebEx Meetings Server account.
  - 2nd Access Code Attempted—The second invalid access code entered by the caller.
  - Email of 2nd Access Code Owner (if available)—The email address of the user associated with the second invalid access code, if the access code is associated with a valid Cisco WebEx Meetings Server account.
  - 3rd Access Code Attempted—The third invalid access code entered by the caller.
  - Email of 3rd Access Code Owner (if available)—The email address of the user associated with the third invalid access code, if the access code is associated with a valid Cisco WebEx Meetings Server account.
- **Meeting Report—**Contains information on all meetings that took place during the specified period:
  - MeetingID—Unique conference ID generated by your system when the meeting was scheduled.
  - Meeting Number—Cisco WebEx meeting number.
  - Subject—Name of the meeting configured by the host.
  - HostName—Meeting host name.
  - Start Time—Starting time and date of the meeting.
  - Duration—Duration of the meeting in minutes.
  - Number of Participants—Number of participants including hosts.

    Note If a guest or host joins a meeting twice, the system adds duplicate joins for the guest, but a single join for the host to the participant count.
  - Status of each meeting
  - Number of Call-In Audio Minutes

- Number of Call-Back Audio Minutes
- Number of VoIP Minutes
- Number of Video Minutes
- Number of Recording Minutes
- Recording Interval—Start and stop time for each recording created during the meeting.
- Number of WebSharing Minutes—Total number of minutes that all participants spend in the web meeting (for example, if three participants attend the web meeting portion of a meeting that lasts 10 minutes, the number of web sharing minutes is 30).
- Participants—A list of the meeting participants.
- Host Platform/Browser—Version of the operating system and browser the host was using when the host started a Cisco WebEx meeting.
- Host IP Address—IP address used by the host when the host started a Cisco WebEx meeting.
- TrackingCodes—After changing tracking code settings, you must wait until after midnight (GMT) for the changes to be effective. Until then, the old tracking codes are valid.
- Host Email—Email address of the meeting host.

- **Network Bandwidth Utilization Report**—Network bandwidth consumption for each day in the specified period for each of the following features:
  - Maximum Bandwidth Consumption for Audio (mbps)
  - Maximum Bandwidth Consumption for Audio VoIP (mbps)
  - Maximum Bandwidth Consumption for Video (mbps)
  - Maximum Bandwidth Consumption for Web Sharing (mbps)

  A consumption of 0 (zero) indicates that the feature was not used on that date. A consumption of less than 1 is displayed if less than 1 Mbps was consumed on the specified date.

  Network bandwidth consumption for video includes video from cameras and video file sharing from web meetings. If video is disabled for your site, you cannot turn on a camera for video but you can still share video files. This results in some network bandwidth consumption for video which is included in reports. This is the only situation that causes network bandwidth consumption for video when video is disabled for a site.
- Storage Capacity Utilization Report—Displays the total disk space used as of the listed date and the number of recorded meetings that occurred for each date.

Note This report is only included if you have configured a storage server. See Adding an NFS or SSH Storage Server, on page 146 for more information.

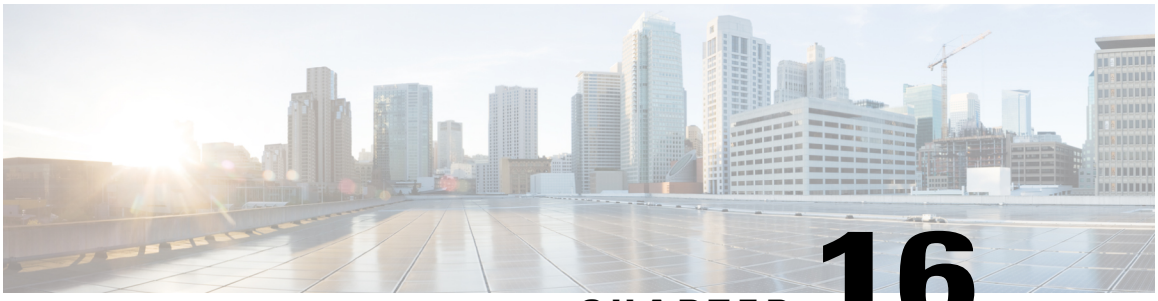
- **Participants Report**—The history of meetings, the time each meeting started, and the tracking code applied for each meeting.
  - Meeting ID—Unique conference ID generated by your system when the meeting was scheduled.

- Conference Name—Name of the meeting the host entered in the **What** field when scheduling a meeting.
- Username—Host's username.
- Joining Time—Time and date when a user joined a Cisco WebEx meeting.
- Leaving Time—Time and date when a user left a Cisco WebEx meeting.
- Duration—Amount of time, in minutes, a user participated in a Cisco WebEx meeting.
- Platform/Browser—Version of the operating system and browser used by a host when the host started a Cisco WebEx meeting.
- Client IP Address—IP address of the WebEx client used by a host or participant to start or attend a Cisco WebEx meeting.
- Datacenter—Name of the Data Center on which the meeting was held. This field is populated only in Multi-data Center (MDC) systems.
- Session Start Time—Time the session started.
- Session End Time—Time the session ended.
- Type of Session—Session type can be video (web sharing), VoIP (telephony connection), call-in, or call-back.
- Session Duration—Length of time the session lasted.
- Phone Number—Phone number of the phone used to place the call in to the WebEx meeting.
- Tel. Server—Telephone server.

- **System Downtime Report**—System downtime information for the specified period and includes the following fields:
  - Category—Out of Service or Maintenance. Out of Service indicates an outage. Maintenance indicates a planned maintenance window.
  - Service—The affected features.
  - Start of Downtime—Date and time the downtime started.
  - End of Downtime—Date and time the downtime ended.
  - Number of Meetings Disrupted—Number of meetings disrupted. This field is blank for Maintenance downtimes because those are planned. If no meetings were scheduled during an Out Of Service downtime, the number is 0.

- **User License Utilization Report**—There are two versions of this report. One version displays license usage for the past 30 days and is titled UserLicenseUtilizationReportForLastMonth.csv and the other version displays license usage for the current month (the first day of the month through the current day) and is titled UserLicenseUtilizationForThisMonth.csv. Each of these reports includes the following fields:
  - User Name—User name of the meeting host.
  - E-mail address—Email address of the meeting host.
  - Meeting ID—Unique conference ID generated by your system when the meeting was scheduled.

- Meeting Number—Cisco WebEx meeting number.
- Start Time—Date and time the meeting started.
- Simultaneous Meeting—Number of simultaneous meetings scheduled by the same user. Each simultaneous meeting that is recorded results in an additional line added to this report for the user who scheduled the simultaneous meeting.



CHAPTER 16

Managing Licenses

Managing Host Licenses

A system supported by a single data center does not require a system license. When you initially deploy this product, you are given a 180-day trial period that allows an unlimited number of Trial Host licenses. After your trial period expires, you are required to purchase Permanent Host licenses for all users who host meetings. Licenses are not required for users who schedule or attend meetings, but do not host any meetings.

If you deploy a system supported by multiple data centers, you must purchase Multi-data Center (MDC) feature licenses. There is no grace period or trial period for MDC licenses. MDC licenses must be hosted on the primary data center before attempting to join data centers in an MDC system. To deploy a MDC system, see Creating a Multi-data Center (MDC) System, on page 259.

About MDC Licenses

There is no trial period for a new Multi-data Center (MDC). MDC feature licenses are purchased for your system size before data centers are joined. The MDC licenses are hosted on the primary data center; the data center that another data center is joined with to form a system, typically the data center that is running the license manager. If you upgrade or grow an existing MDC system, you must purchase the licenses of the correct version and size in 90 days or less.

- Permanent MDC Licenses—Purchased to allow data centers to be joined into a single MDC system. Each system must have a license; therefore, a minimum of two licenses must be purchased.
- Grace MDC Licenses—Limited to 90 days, you can upgrade or grow data centers in a MDC system before purchasing the required licenses. After this system modification, you have 90 days to resolve any license issues, such as purchasing MDC licenses for a larger system. If licenses of the appropriate size and version are not installed before the Grace MDC period expires, the data center that is not hosting the License Manager is disabled.
- Demonstration MDC Licenses—Temporary license support for a MDC system. Issuing Demonstration MDC licenses is determined by the vendor on a case-by-case basis and the duration that the licenses are valid is determined when the licenses are issued.

About Host Licenses

This product has **Host-based Licensing** requiring that you purchase a license for each user that **hosts** meetings or is manually assigned a license. A user does not consume a Host license by attending or scheduling a meeting on behalf of others. The license usage calculation for reporting purposes occurs once per month, for example, once from January 1 through 31, and once from February 1 through 28, and so forth.

Note When upgrading from a previous version, all licenses that were on the original system are released from their assignment to users. Users can reacquire licenses by hosting meetings or being manually assigned licenses. This is also true when installing a Multi-data Center (MDC) system. Host licenses are lost on the data center joining the MDC system. Those licenses can be re-hosted on the MDC system after the join.

From the **Reports** page, you can request a report that provides the total number of licenses consumed. In addition, we recommend that you view the PDF Summary Report that shows license consumption trends. By viewing the overall license trend, you can plan for future license purchases more effectively, to match the growing adoption of this system within your company.

Types of Host Licenses

A Host license is required to host a meeting. A license is not required to schedule or attend a meeting. The types of Host licenses are:

- **Permanent Host License—**An installed Host license purchased to allow a user to host meetings that is assigned to that user the first time that person hosts a meeting. A Host license can be manually assigned to a user by an administrator; a user does not have to wait to host a meeting to be assigned a license. If there is a user with a Grace license and a Permanent Host license becomes available, either by removal of a host or the purchase of additional Permanent Host licenses, the permanent license is assigned to the host with a Grace license.

  In version 2.5 or higher, a user never consumes more than one Permanent Host license and can host a maximum of two meetings at the same time. Also, a Permanent Host license is released for use by another host only when the user of that license is deactivated (as opposed to version 2.0 where the licenses of hosts that do not host meetings for a period of time are released). If someone attempts to host a meeting and:

  - There are no licenses available.
  - The license of the host has expired since the meeting was scheduled or the meeting host has been deactivated.

  An error message displays and the meeting cannot be started. (See Exceeding the Number of Available Licenses, on page 252.)

- **Trial Host License—**Temporary Host licenses assigned automatically in a system that is in the Trial period.

- **Grace Host License—**A temporary license consumed by a meeting host in a *Permanent License environment* where all of the permanent licenses have been consumed. A limited number of Grace Host Licenses are temporarily available for a system with Permanent Host Licenses (a system not in a trial period) if the number of installed licenses is briefly exceeded. Warnings about the excess licenses are displayed to the administrator. Temporary Grace Host licenses in this scenario are associated with a user

for 180 days. When a Permanent Host license becomes available, the Permanent Host license is associated with the user and the Grace license is released. If after 180 days the user with a Grace Host license has not acquired a Permanent Host license, the user is no longer allowed to host meetings. (See Exceeding the Number of Available Licenses, on page 252 for more information on system behavior when the number of Permanent Host licenses is exceeded.)

When a user with a Permanent Host license is deactivated, the license is returned to the license pool. Active users with Grace Host licenses are not automatically granted the Permanent Host license. You must select **Reserve license** (see Editing Users, on page 112) to release the Grace Host license and grant that user a Permanent Host license. Otherwise, the Permanent Host license remains in the pool until a new user is added to the system and hosts a meeting. In this event, the unused permanent license is associated with the new user.

- **Demonstration License—**Temporary host licenses with varying valid durations provided by a vendor on a case-by-case basis. (They are primarily used for testing.) When these licenses expire, your system returns to its previous license status. A Demonstration Host license expires whether or not it is assigned to a user.
- **Local Host Licenses—**Licenses managed on the local data center.
- **Remote Host Licenses—**Licenses managed by using Active Directory.
- **Expired Host License—**A temporary host license that has been invalidated because the time allotted has been exceeded. A user with an Expired Host license can still attend meetings and schedule meetings for others.

License Status of Users

This section describes the relationship between the status of users and how host licenses are counted:

- Participant—An individual that attends meetings, but does not host meetings, and does not have control over the host features, such as presenting content unless the participant is designated by a host to be the presenter. No host licenses are consumed by meeting participants. This user can also schedule meetings on behalf of others without consuming a host license.
- Meeting Host—Schedules and attends meetings in the capacity of the meeting host, and is allowed control over selected features, such as identifying a presenter or muting another participant. Hosting a meeting consumes a license and that license is retained by that user until the user is deactivated. The Host license can take several forms. (See Types of Host Licenses, on page 250 for more information on Host license forms.)
- Alternate Host—Identified when the meeting is scheduled as someone who can assume the host role in the absence of the meeting host. If the meeting host who scheduled the meeting does not attend, the alternate host is given control over most of the same features as the meeting host. The license needed to host the meeting is validated against the status of the user who scheduled the meeting. In other words, the user who scheduled the meeting must have a valid license at the time of the meeting, even if that user does not attend the meeting.
- Join Before Host (JBH)—Allows participants to join a meeting before the arrival of the host or an alternate host.
- Overlapping Meetings—Two or more meetings that are scheduled during the same time of day by the same host. Starting with CWMS Release 2.5, a user can host a maximum of two simultaneous meetings, consuming only one license; no user can host more than two meetings at the same time.

Exceeding the Number of Available Licenses

During the free trial period, the number of licenses available on any size system is only limited by the size of the system. Once you have purchased and installed licenses on your system, you must make sure you have enough Installed licenses to accommodate all hosts on your system.

If the number of installed licenses is briefly exceeded, a Grace license can be acquired by a new host. (Grace licenses are described in detail in Types of Host Licenses, on page 250.)

If the number of active hosts on your system regularly exceeds the number of Installed licenses, an email is sent to the administrator indicating that the number of Installed licenses has been exceeded and recommends purchasing additional licenses. You must reduce your license usage or increase the number of licenses on your system so that it meets or exceeds the number of active hosts.

The audit manager runs once per day (at 2:00 a.m.) to adjust the number of licenses used as necessary. If the number of hosts has dropped below the number of Installed licenses, the licenses exceeded condition ends. If the number of active hosts still exceeds the number of licenses, email is sent to the administrator each month indicating that the licenses exceeded condition still exists.

Starting in version 2.5, users with licenses can continue to use the system, but users without licenses cannot host meetings. If there are no licenses available when an unlicensed user schedules a meeting, the user is notified that they might not be able to host that meeting due to the lack of licenses.

In all versions, the Administration site continues to be available, so an administrator can sign in, add licenses, and restore users ability to host meetings and access recordings.

Obtaining Licenses

During the system trial period, use your dashboard to view usage, resource history, and meeting trends to determine how many users are hosting and attending meetings on your system. After you have been using the product for a few months, you can use your monthly summary reports and customized details reports to help you determine how many Permanent Host licenses you need. Your monthly summary reports display statistics on service adoption and user license usage. Service Adoption statistics show you the rate at which new *users* are adopting your system by displaying the rate of adoption for the previous three months and predicting the growth rate over the next three months. Host License statistics display *host* license usage over the previous three months and expected growth over the next three months.

There is no trial period for Multi-data Center (MDC) licenses; you must obtain MDC licenses before creating an MDC system. You must purchase a minimum of two MDC licenses, one for each data center in the system. (All licenses are installed on the data center hosting the License Manager.)

Obtain Host or MDC licenses by:

- Using eFulfillment (see Fulfilling Licenses by using eFulfilment, on page 254).
- Using file-based fulfillment (see Fulfilling Licenses by Using the License Manager, on page 253).
- Contacting TAC to open a case for ordering licenses (see Fulfilling Licenses by Contacting TAC, on page 255).

Refer to the Managing Host Licenses, on page 249 section of *Cisco WebEx Meetings Server Administration Guide* for more information on managing your licenses.

License Manager Connection

When you purchase licenses, you use an embedded license manager tool to enter your PAK and register your licenses. License manager performs synchronization every 12 hours to update the license status and last compliance time. If two days pass with no connection to a license manager, an email is sent to your administrator to inform him that a license manager is unable to synchronize with your system. You are given a 180-day grace period to reconnect to a license manager.

A new email is sent to the administrator at the end of each month that the system is unable to connect with license manager to indicate the date when the system will be disabled. If your system reconnects with license manager before the six-month grace period passes, this condition ends.

If your system does not reconnect with license manager within 180 days, your system is set to Maintenance Mode and cannot be enabled until the issue is resolved. The email message informs the administrator of the date when this will occur. When your system is in Maintenance Mode, users are not able to schedule, host, or attend meetings, or access recordings on the system. The Administration site functions normally, so an administrator can sign in to the system, but the system must reconnect with license manager to end this condition and restore the ability for users to schedule, host, attend meetings, and access recordings.

Fulfilling Licenses by Using the License Manager

Obtain Host and Multi-data Center (MDC) licenses by using the embedded Cisco Enterprise License Manager:

Before You Begin

Contact your sales representative to order Host and Multi-data Center (MDC) licenses for your system. Your sales representative sends you an email that contains your Product Authorization Key (PAK).

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 **System** and then select the **View More** link in the **Licenses** section.

Step 3 Select **Manage Licenses**
Your browser opens a new tab or window containing a license manager. (The license manager is embedded in Cisco WebEx Meetings Server; it is not an external website.)

Step 4 Select **License Management** > **Licenses**.

Step 5 Select **Generate License Request**.
The **License Request and Next Steps** dialog box appears.

Step 6 Copy the highlighted text in the field and select **Cisco License Registration**.

Step 7 Log in to your Cisco account and display **Product License Registration**.

Step 8 Enter the Product Authorization Key (PAK) that you received from your Cisco sales representative in the **Product Authorization Key** field and select **Next**.
The **Fulfill PAK** page or **Assign SKUs to Devices** tab appears.

Step 9 Enter the quantity of licenses from each PAK that you are activating in the **Quantity to Assign** field.

Step 10 Paste the contents of the License Request that you generated and copied into the **Paste the content....** field and select **Next**.

The **Review** tab displays.

Step 11 Make sure the contact email address is correct. Optionally change the contact email address in the **Send to** field.

Step 12 Review the page and select **I agree to the Terms of the license**.

Step 13 Select **Get License**
The **License Request Status** dialog box appears.

Step 14 Obtain your license file in one of the following ways:

- Select **Download** to download your license file (.bin).
- Extract your license file (.bin) from the ZIP archive sent to you by email.

Step 15 Return to the Administration site and select **System** and then select the **View More** link in the **Licenses** section.

Step 16 Select **Manage Licenses**.
Your browser opens a **Licenses** window.

Step 17 Select **Fulfill Licenses from File** in the Other Fulfilment Options menu.

Step 18 Select **Browse** and select the license file (.bin) that you downloaded or extracted from the ZIP file in your email.

Step 19 Select **Install**.
Your license file is installed. Check the license information that is displayed to ensure that it is correct.

Step 20 Select **Current** in the Fulfilment Date column.
The **License Fulfilment** page appears. Verify that the information displayed in the **Licenses Fulfilled** section is correct.

Fulfilling Licenses by using eFulfilment

Fulfill the license order by entering the Product Authorization Key (PAK) in the license manager without using the web site.

Before You Begin

Contact your Cisco sales representative to order Host and Multi-data Center (MDC) licenses for your system. Your sales representative will send you an email that contains your Product Authorization Key (PAK).

eFulfillment requires that a network connection between the system and Cisco Systems, Inc. can be established. Verify that your system is not behind a firewall that does not allow access. If access is not allowed, use file-based fulfillment (see Fulfilling Licenses by Using the License Manager, on page 253) or contact TAC to open a case for ordering licenses (see Fulfilling Licenses by Contacting TAC, on page 255.

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 **System** and then select the **View More** link in the Licenses section.

Step 3 Select **Manage Licenses**

Your browser opens a new tab or window containing the license manager embedded in Cisco WebEx Meetings Server. (The license manager site is not an external web site.)

Step 4 Select **Fulfill Licenses from PAK**.
The **Fulfill Licenses from PAK** wizard appears.

Step 5 Enter the PAK that you received from your Cisco sales representative in the **Product Authorization Key** field and select **Next**.
The **Fulfill PAK** page appears.

Step 6 Select **Add licenses from a new PAK**.

Step 7 Enter the PAK code in the *** PAK code** box and select **Next**.

Step 8 Log in by using your cisco.com user ID and password.
The **Fulfill Licenses** window appears indicating the number of licenses available.

Step 9 Select **Fulfill** in the **Actions** column.

Step 10 Click the **Install** column to edit the values.

Step 11 Enter the number licenses you want to fulfill for this system. If the PAK supports partial fulfillment, the range is from 1 to the number of licenses remaining in the PAK.

Step 12 Select **Save**.

Step 13 Select **OK**.
The **Fulfill Licenses** window appears. The value in the **Install** column shows the number of licenses you elected to fulfill.

Step 14 Select **Next**.
The **Review Contents** window appears. The **Current Values** column shows the number of active licenses. The **After Fulfillment** column shows how many licenses you will have when eFulfillment is complete.

Step 15 Select **Next**.

Step 16 Select **By checking this box I acknowledge that I have read, understand, and agree to be bound by, the terms and conditions of the End User License Agreement.**

Step 17 Select **Finish**.
A **Connecting to license server** progress bar displays while the license manager connects to Cisco to fulfill your licenses. When the eFulfillment is complete, a new line added in the **Licenses** window. The **Fufillment Date** column shows the current date followed by **- Current**. You can select this link to display the details of your licenses, including the type and number of licenses that are installed on this system.

Fulfilling Licenses by Contacting TAC

Before You Begin

Obtain your registration ID number. You can find your registration ID number by opening your Enterprise License Management tool and selecting **About**.

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 **Support** and call the TAC at the listed number.

Step 3 File a case, requesting the number of Host and Multi-data Center (MDC) licenses you want. We process your request and enable the additional licenses on your system.

Step 4 Select **System**.

Step 5 Check the License section to confirm that the licenses have been added.

Re-hosting Licenses

Re-hosting moves Host or MDC licenses on a system that is being joined to an MDC system, upgraded, expanded, or replaced to the surviving system for a limited period of time. If the licenses are not re-hosted, they cannot be upgraded. For example, when a system is upgraded from version 1.5MR3 to version 2.0, Host licenses originally hosted on the 1.5MR3 system can be re-hosted on the 2.0 system for 180 days before they must be replaced by licenses valid for the 2.0 version. If the 1.5 Host licenses running on the 2.0 system are not replaced within 180 days, the system is shut down until the issue of the licenses is resolved. (The only task allowed is adding Host licenses on the system. See Re-hosting Licenses after a Major System Modification, on page 256.)

If the original system was operating without licenses and within a Trial license period, the remaining number of Host license-free days is transferred to the modified system.

Accessing the GLO Request Form

To display the Global Licensing Operations (GLO) request form, select **Contact Us** on the Product License Registration page (https://tools.cisco.com/SWIFT/LicensingUI/Quickstart). On the GLO Support Contact Information page, select **request**.

Before You Begin

Be prepared to provide the following information:

- Contact information
- Problem description
- Product name and licensing activity (such as resend license information or upgrade license)
- Entitlement information (such as a product serial number)

Re-hosting Licenses after a Major System Modification

After a system has been modified as the result of an action, such as an upgrade or expansion, and testing is complete, the next step is to re-host your licenses.

If you have a Multi-data Center (MDC) system and that system has been expanded, you must purchase larger MDC licenses. If it has been upgraded, you have 90 days to upgrade the MDC licenses. Re-hosted licenses are automatically invalidated on the original system. Before you begin the re-host, preserve a *license request* from the original system in case it is needed to re-host the licenses on the original system due to some error in modifying that system.

When re-hosting licenses, the number of licenses that you can re-host is limited to the number of licenses on the original system. The preferred method of re-hosting licenses is through the Product License Registration portal.

If the original system had Host licenses, the modified system allows you a 180-day period before upgraded Host licenses are required, allowing you time to test the upgraded system before re-hosting the original licenses on the upgraded system. Once the licenses are re-hosted, the trial period ends. Re-hosting can be done by using the Product License Registration Portal at http://tools.cisco.com/SWIFT/LicensingUI/Home. (See Accessing the GLO Request Form, on page 256.)

Generate a License Request

To acquire a license request for the original system:

Step 1 From the original system Administration window, select **System**.

Step 2 Select **(under Licenses) view more** > **Manage Licenses**.

Step 3 Select **Other Fulfillment Options** > **Generate License Request**.

Step 4 Copy the content and save the license request in a file on the PC.

What to Do Next

Register the licenses. See Register Licenses to be Re-hosted, on page 257 for instructions.

Register Licenses to be Re-hosted

To use the Product License Registration portal, Log in at https://tools.cisco.com/SWIFT/LicensingUI/Quickstart. You are sent an email containing your re-hosted licenses. Note that if you are doing the re-host as part of a software upgrade, you must re-host (see Re-hosting Licenses after a Major System Modification, on page 256) and upgrade the old version of the licenses on your upgraded system. An error message, such as **You are using an invalid license file with your current deployment** might display on the administration site of your upgraded system. This is expected. The message includes an expiration date indicating when your system will be shut down if you do not upgrade the Host licenses before this date. The only task that you can perform after this date is to install licenses.

What to Do Next

After re-hosting the licenses, complete the license upgrade before the date shown to assure the uninterrupted use of the system. See Fulfilling Licenses by Using the License Manager, on page 253 for more information.

Upgrading Licenses after a Software Modification

After a software modification, installed licenses are re-hosted from the original system on the upgraded system. (See Re-hosting Licenses after a Major System Modification, on page 256 for more information.) After the licenses have been re-hosted, they can be upgraded for use on the upgraded system.

The association of users to licenses is deleted. Users are associated with licenses the first time they host a meeting.

To upgrade your Installed licenses by using eFulfilment:

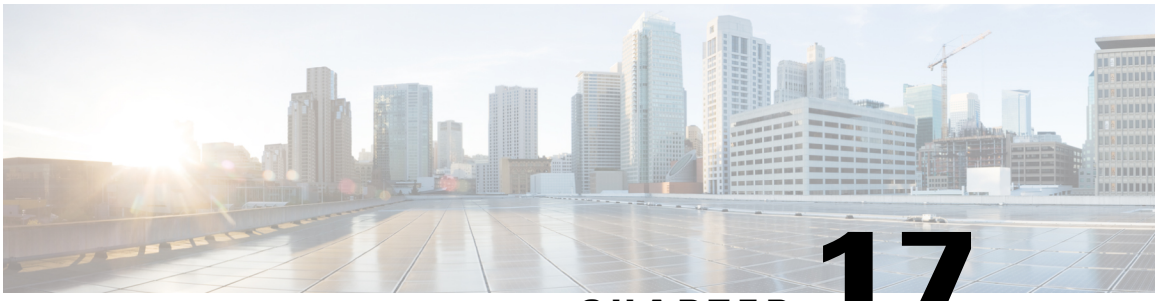
1. Obtain a Product Authorization Key (PAK) code from your vendor.
2. From the **System** window select **(under Licenses) view more**>**Manage Licenses**> **Licenses**> **Fulfil Licenses from PAK**. The **Fulfil Licenses from PAK** window is shown.
3. Enter the PAK code and select **Next**.
4. Log in by using your cisco.com account credentials. The **Fulfill Licenses from PAK** window is shown.
5. Click the Install column to select the number of licenses you want to install.
6. Indicate the number of licenses to be installed and select **Save**. The licenses are installed on the system as part of the eFulfillment from the PAK.

Note The number of licenses that you can install is limited to the number of licenses available from the upgrade PAK and cannot exceed the number of licenses that were re-hosted from the original system.

To upgrade the version of your Installed licenses from a license file:

1. Obtain a license file from your vendor by using **cisco.com/go/license**.
2. From the **System** window select **(under Licenses) view more**>**Manage Licenses**> **Licenses**> **Fulfil licenses from file**. The **Install Licenses File** window is shown.
3. Browse in the license file. The file is shown on the **Licenses** window.

The licenses are updated.



CHAPTER 17

Creating a Multi-data Center (MDC) System

Creating a Multi-data Center (MDC) System

About Multi-data Centers

The Multi-data Center (MDC) licensed feature is available in version 2.5 and higher. It allows two CWMS systems to be joined into a single MDC system. One license must be purchased for each CWMS data center in an MDC system. MDC licenses should be purchased before you attempt to deploy MDC. (A system with a single data center does not need a feature license.) MDC licenses are further described in About MDC Licenses, on page 249.

The meeting client uses the Round Trip Time (RTT) to determine on which data center to start meeting. (This is an automated process and cannot be configured by the host or the administrator.)

Load Balancing is not configurable; it is automatic and built into the system. Any Load Balancer configured as separate machine is not supported.

Network requirements between data centers can be found in the "Network Requirements for Multi-data Center" chapter of the CWMS Planning Guide at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

Advantages of a Multi-data Center System

The advantages include:

- End user access to all data centers by using one URL and one set of phone numbers; the existence of MDC is transparent to end users.
- Host licenses, recordings, and related management data migrate freely between joined data centers.
- Users can dial into meetings without geographic restrictions; attend meetings by dialing local phone numbers.
- Data centers can (optionally) be located in different geographic areas.
- Zero-downtime during some planned maintenance events, when the data centers can be running different CWMS 2.5 *update* versions. Consult the release notes at http://www.cisco.com/c/en/us/support/

conferencing/webex-meetings-server/products-release-notes-list.html to determine which CWMS versions can run simultaneously.

Occasionally, data centers in an MDC system can be running different *update* versions. Consult the release notes at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-release-notes-list.html to determine which CWMS versions can run simultaneously.

- A disaster recovery environment that is transparent to users. If one data center fails for any reason, the other data center supports users.

Although in an MDC environment the data centers are all running CWMS and considered peers, for the purpose of describing the process for joining data centers in a system, the relationship between data centers are considered *primary* and *secondary*. Before the Join, the primary data center supports the *system* you want to retain, and shall be the location of the license manager. The secondary data center becomes part of the MDC system. The distinction is important especially if you are joining data centers that have been actively supporting users. User information and content are deleted from the secondary data center.

Note There is redundancy, but no increase in capacity when a data center is added to an MDC system. If a 2000-port data center is added to an MDC system supported by a 2000-port data center the resulting system is a 2000-port MDC.

If you are joining a new, secondary CWMS system data center that has no user data to an MDC system, continue to Preparing an MDC System to Receive Data Center Join Requests, on page 263.

If you are joining an active, secondary CWMS system data center that includes user data to an MDC system, continue to Preparing to Join an Active CWMS Data Center to a MDC System, on page 261.

Blocking Mode

Each data center polls its components for their status every 5 seconds. Under certain failure conditions a data center automatically turns on Blocking Mode to prevent end users from accessing a data center with failed components, allowing time for the system to attempt to fix itself. In an MDC environment, user activity transparently fails over to the active data center. Once the components of the data center in Blocking Mode are again operational, the data center exits Blocking Mode. Email notifications are sent to administrators when a data center goes into or recovers from Blocking Mode.

Blocking Mode ON conditions are triggered when all the following are true:

- One or more of the telephony components or data base replication fails.
- The condition has existed for 5 minutes or more.
- Another data center in the MDC system is operational.

End-user access to a data center in Blocking Mode is prevented; all user activity is redirected to the active data center. Administrators can access the administration site on the blocked data center to monitor its condition and to troubleshoot issues.

Blocking Mode OFF conditions are automatic and are triggered by all of the components returning to a good state. Access by end-users is restored and the data center returns to polling its components every 5 seconds.

Preparing to Join an Active CWMS Data Center to a MDC System

Important Joining CWMS data centers requires the use of RSA self-signed certificates. Before you begin the join, ensure that you remove Certificate Authority (CA) certificates from both data centers.

When you join a secondary CWMS system data center that has been in service to users, it has acquired or been configured with user data that might be lost when it is joined to a Multi-data Center (MDC). In a Single-data Center environment, one CWMS data center serves the user community. When a MDC system is desired, typically a new CWMS data center is created and joined to the MDC system before that data center is put it into service and therefore, there is no user information, licenses, or configuration information of value to retain on what will become the secondary data center during the Join. However, if you are joining two active data centers, user content is overwritten or inaccessible:

- All global data is overwritten. (Configuration parameters local to the data center are preserved.)
- User information, scheduled meetings, reports, and related emails that was on the secondary data center is deleted.
- Meeting recordings are inaccessible to users. The recordings remain intact on the NAS, but they cannot be accessed or recovered by users. (See Preserving Recordings before Joining a MDC System, on page 262.)
- Host licenses are lost, but Permanent Host licenses that were hosted on the secondary data center can be recovered by re-hosting them on the MDC system. If the primary data center is removed from the system, the licenses must be re-hosted on another data center running License Manager.

  If the primary data center goes off-line for any reason, it must be brought back online before host licenses can be modified. If the managing data center cannot be recovered, surviving data centers go into a grace mode for 180 days. To recover, Permanent Host licenses must be re-hosted before the grace period ends. (See Re-hosting Licenses, on page 256.) If the licenses are not re-hosted before the grace period ends, the system is put into Maintenance Mode until the licenses are re-hosted.
- The user-to-host license associations on an active secondary data center are lost when data centers are joined. Users that were hosts on an active secondary data center can recover their licenses simply by hosting meetings on the joined system or an administrator can manually assign host licenses from the data center managing the licenses.

The following information on secondary data centers is retained after a join:

- System-specific configurations, such as Cisco Unified Call Manager (CUCM).
- Language settings, such as IVR language settings.
- Audio settings.
- Blast Dial information.

Preserving CWMS Data on a Secondary Data Center Before a Join

The CWMS data on a secondary data center being joined to a MDC system is overwritten or rendered inaccessible. If you are joining a CWMS data center that has not been put into service, there is no meaningful data to preserve and you can continue to Preparing an MDC System to Receive Data Center Join Requests, on page 263. Otherwise, consider preserving critical data.

When a secondary data center joins a MDC system, that data center loses:

- User-Host license associations
- Host licenses (that can be recovered by re-hosting them on the MDC systemRe-hosting Licenses after a Major System Modification, on page 256)
- Scheduled meetings (that must be manually rescheduled on the MDC system)
- Meeting recordings that can be preserved by:
  - Asking users to download and retain recordings locally.
  - Archived for retrieval by a system administrator.
  - Both. (Recommended)

Meeting recordings "live" on the NFS, so they are not lost; they are not accessible to users from CWMS.

Preserving Recordings before Joining a MDC System

Under the `NFS:/nbr` directory are the `Recording`, `nfskeepalive`, and `Snapshot` directories. To archive the files, copy `NFS1:/nbr/1/*` to `NFS2:/nbr/1`.

Note This procedure is provided as an example. The process for your system might vary.

For the purposes of the example steps, assume the NFS is on DC1 and named `sanjose-nfs:/cisco/cwms` and the NFS on DC2 is named `rtp-nfs:/cisco/cwms`.

Before You Begin

- Access to a Linux machine with root access to the NFS. (Any flavor will do, Redhat, CentOS, and so forth.)
- If the NFS has an IP-based filtering or access control for mounting, then add the Linux host IP to the access list.

Step 1 cd/tmp

Step 2 Create a new temporary directory that will be used to mount the NFS of DC1. `mkdir nfs-dc1`.

Step 3 Create a new temporary directory that will be used to mount the NFS of DC2 : `mkdir nfs-dc2`.

Step 4 Mount DC1 NFS to `/tmp/nfs-dc1` : `mount -t nfs -o vers=3,rw,soft,timeo=400` *`sanjose-nfs:/cisco/cwms`* **`/tmp/nfs-dc1/`**

Step 5 Mount DC2 NFS to `/tmp/nfs-dc2` : `mount -t nfs -o vers=3,rw,soft,timeo=400` *`rtp-nfs:/cisco/cwms`* **`/tmp/nfs-dc2/`**.

Step 6 Synchronize the recordings : `rsync -av --exclude='*Snapshot*/' nfs-dc1/ nfs-dc2`.

Step 7 Unmount the DC1 NFS : `umount nfs-dc1`.

Step 8 Unmount the DC2 NFS : `umount nfs-dc2`.

Step 9 Delete the DC1 NFS temporary mount directory : `rm -r nfs-dc1`.

Step 10 Delete the DC2 NFS temporary mount directory : `rm -r nfs-dc2`.

Preparing an MDC System to Receive Data Center Join Requests

Data centers can be joined and managed as a single system. This procedure describes how to prepare the *primary* data center that is already servicing the *system* to receive Join requests from the *secondary* data center:

Before You Begin

The following is a list of tasks that a system administrator must complete to ensure that joining a data center to a system is successful.

1. Remove Certificate Authority (CA) certificates from both data centers. Joining CWMS data centers requires the use of RSA self-signed certificates.
2. Verify that all data centers are running the same CWMS software version.
3. Verify that all data centers are running the same software types. For example, verify that all data centers are Audio Encrypted -AE or Audio Unencrypted -AU. (Systems cannot be converted from one type of audio encryption to the other; a new system must be created.)
4. Verify that all data centers are the same system size.
5. Network Time Protocol (NTP) is required for all data centers, and all data centers must be on the same NTP time.
6. All virtual machine hosts must be configured with NTP servers.
7. NTP servers must be reachable from the virtual machine hosts. (Errors might occur if the DNS or firewall does not pass NTP or if the wrong NTP server configured.)
8. Install the Multi-data Center (MDC) licenses (two minimum) on the primary data center that is running the license manager.
9. All data centers in the system must have Internet Reverse Proxy (IRP) enabled or disabled. There cannot be a mismatch. After the Join, IRP can be added to or removed from any data center such that all data centers are configured the same way regarding IRP.
10. None of the data centers are running High Availability (HA). (See Removing High Availability from a System, on page 47.)
11. Verify that storage is configured on both data centers or none of the data centers. If storage is configured, the data centers should use storage on different servers or at least different folders.
12. Verify that all data centers are using the same authentication mode. The authentication mode can be LDAP, SSO, or default mode.
13. Verify that the DNS has entries for all Local URLs, all Common URLs, and all hostnames. The Administration Common URL must be associated with only one IP address when the Join is executed. The WebEx Common URL must be associated with only one IP address when the Join is executed. After the data center is joined to a system, the common URL should be returning two IP addresses.

14 Verify the CUCM transports on both data centers use the same protocol. The transport protocol can be TCP, UDP, or TLS.

Step 1 Notify users on the secondary system of the Join. If the secondary data center has not been a part of any active system, skip this step. If this data center is supporting an active system, see Preparing to Join an Active CWMS Data Center to a MDC System, on page 261.
User data, scheduled meetings, and access to meeting recordings on the secondary data center is lost when data centers are joined. Before you send a Join request from the secondary data center, notify all users that if they want to preserve any meeting recordings, they should download the recordings to their local PCs.

Step 2 Select **Data Centers** > **Add Data Center** > **Prepare System for Join**

Step 3 Enter:

- Local Site URL—User site URL that allows users to schedule, attend, or host meetings. When the network is not configured with split-horizon DNS (the most common configuration), this URL resolves to the public VIP address of this system for all users. When the network is configured with split-horizon DNS, this URL resolves to the private VIP address of this system for internal users and to the public VIP address of this system for external users.
- Local Administration URL—System administration URL that resolves to the private VIP address for this data center.
- Local Data Center Name—Identifies the primary data center on the local system.

Step 4 Download the certificate that will be used to Join the systems.
The certificate from the primary data center must be uploaded to a secondary data center prior to the join. Certificates are modified by the system, so it is best not to try to reuse old certificates to accomplish a join.

Note When using Safari, the downloaded certificate is saved as `CAcert.pem.txt`. This is the default behavior of the Safari browser. To restore the `.pem` extension (before uploading the certificate), delete the `.txt` string.

Step 5 Select **Done**.

Step 6 Sign in to the secondary data center and send a Join request from that data center. See Joining a Data Center to a Multi-Data Center System, on page 264 for instructions.

Joining a Data Center to a Multi-Data Center System

The Join request is sent from a *secondary* data center to the *primary* data center the data center supporting the CWMS Multi-data Center (MDC) system. After the join, the primary data center retains its data and access to meeting recordings. All meeting information and recordings on the secondary data center are rendered inaccessible. The MDC feature licenses and Permanent Host licenses are typically hosted and managed on the primary data center. There is no trial period for an MDC system; MDC licenses must be loaded on the primary data center prior to the Join. Without an available MDC license on the primary data center, a secondary data center cannot join a system.

Note When joining data centers, the primary data center certificates are updated. The new certificates are self-signed and automatically regenerated to include the new URLs from the secondary data center. This mismatch causes a certificate warning in the browser when you access the primary data center or the MDC Administration site. Accept the warnings and follow the standard procedure to update the system certificates. (See Managing Certificates, on page 213.)

Note *When joining data centers that use languages other than English*, there is **always** a brief period during the Join operation when the task list appears in English. Error messages might also appear in multiple languages during a Join. (The balance of the text on the page appears in the original language.)

When the **Database tables are synchronized** task is launched, the expected task list language behavior is:

- If the Administrator account is hosted on all data centers and they are configured with the same language settings, the task list displays in English during the **Database tables are synchronized** task. After the tables are synchronized, the task names return to the language of the Administrator.
- If the Administrator account is hosted on the primary data center, and that administrator has an account on a data center that is joining the system and that data center is set to a different language than the primary data center, the task list displays in English while the database tables are synchronizing. After synchronization, the task list switches to the language the administrator set on the primary data center.
- If the Administrator account is hosted solely on the secondary data center joining the system, and the Administrator does not have an account on the primary data center that will remain after the Join, the task list displays in English while the database tables are synchronizing. Once the system finishes synchronization, there is no further language change and no **Done** button. To continue, the administrator must:

  1. Close the current browser window.
  2. Open a new window by using the local administration URL of the secondary data center.
  3. Sign in by using an Administrator account on the primary data center.
  4. Select **Data Centers** > **Add Data Center** and verify the status.

Before You Begin

Network Time Protocol (NTP) must be configured as follows:

- NTP is required for all data centers and all data centers must be on the same NTP time.
- All virtual machine hosts must be configured with NTP servers.
- NTP servers must be reachable from the virtual machine hosts. (Errors might occur if the DNS or firewall does not pass NTP or if the wrong NTP server configured.)

If this data center is supporting an active system, Host licenses supported on this data center are removed. These Host licenses can be re-hosted on the data center hosting the License Manager. (See Re-hosting Licenses,

on page 256.) We recommend that you save a license request from this data center before you start the join in case you later need help from TAC to locate your licenses.

Important Joining CWMS data centers requires the use of RSA self-signed certificates. Before you begin the join, ensure that you remove Certificate Authority (CA) certificates from both data centers.

TLS 1.0 is marked as **Medium Vulnerability** by a PCI Vulnerability Scanning vendor. After the data center has joined the MDC, other certificates can be added to the system. See www.nist.gov/manuscript-publication-search.cfm?pub_id=915295 and www.tenable.com/blog/pci-ssc-announces-the-end-of-ssl-usage-for-the-payment-card-industry.

Step 1 To send a request to join an MDC system from a secondary data center, select **Data Centers** > **Add Data Center** > **Join Systems**.

Step 2 Enter:

- **Remote System Certificate—**Upload the System Certificate downloaded from the other data center during the "Preparing an MDC System to Receive Data Center Join Requests, on page 263" process.

  Note When using Safari, the downloaded certificate is saved as `CAcert.pem.txt`. This is the default behavior of the Safari browser. To restore the `.pem` extension (before uploading the certificate), delete the `.txt` string.

- **Remote Common Administration URL—**System administration URL that resolves to the private VIP address of the data center that you prepared to be joined.
- **Remote Administration Email—**Email address used for accessing the data center you are joining.
- **Remote Administrator Password—**Password that allows administrative access to the data center you prepared for the Join.
- **Local Data Center Name—**Identifies the secondary data center on the local system.

Step 3 Select **Continue**.
The Join Data Center task list displays.

Note During the **Database tables are synchronized** task, all the users in the secondary data center are deleted and users listed on the primary data center are replicated over to the secondary data center. The system cannot get the administrator's language (as there are no users on DC2) and the interface defaults to displaying in English.

If the administrator of the secondary data center also exists on the primary data center, then after the administrator signs into the secondary data center, the system displays the administrator's language (unless the language configured on the primary data center for that administrator is a different language than what is configured on the secondary data center).

If the administrator of the secondary data center also exists on the primary data center (or there is an error in the database synchronization), then the system displays in English.

Step 4 Take all data centers in the MDC system out of Maintenance Mode.

What to Do Next

Add the Pointers to the DNS Server

- **Common site URL**—Public VIP address for each data center.
- **Common Administration URL**—Private VIP address of both data centers.
- **Local Site URL** (of a data center)—Public VIP address of that data center.
- **Local Site URL** (of the other data center)—Public VIP address of that data center.
- **Local Administration Site URL** (of a data center)—Private VIP address of that data center.
- **Local Administration Site URL** (of the other data center)—Private VIP address of that data center.

Modify the Audio Access Numbers and Service Language

The audio access number and service language configured on the primary data center are configured as the global access number and service language, replacing the original access number and service language configuration. If necessary, go to global configuration and adjust the access numbers and service language appropriately. (See Modifying Audio Settings, on page 172.)

Disaster Recovery in a Multi-data Center Environment

In a Multi-data Center (MDC) environment where one data center has failed due to a hardware or system issue, we recommend replacing the failed data center by creating a new data center and joining that data center to the system. (See also Disaster Recovery by Using the Storage Server, on page 150). The replacement data center is quickly populated with the user information. If the License Server is on the failed data center, the MDC and user licenses must be re-hosted (see Re-hosting Licenses, on page 256) on the replacement data center.

The remaining data center supports the system as long as it is up. However, the system does not have any redundancy in this scenario.

If the Data Base node of one data center goes down, data changes happening in the other data center are queued up. This queued data is synced when the failed data center comes up or when a replacement data center is joined.

If the queue grows beyond the limit, the data center stops queuing to prevent disk from becoming full and thus risking its own functionality. If the queue has exceeded the limit, the MDC does not attempt to synchronize data, even if the failed data center comes up; the system will no longer be an MDC from that point on.

Proper email notifications are sent out when failure is anticipated.

Step 1 Sign on to the Administration site of the surviving data center.

Step 2 Remove the failed data center from the system.
(See Removing a Data Center, on page 268).

Step 3 Create a new data center to replace the failed data center.
The version of the replacement data center should match the version of the surviving data center.

Step 4 Complete the local configurations, such as CUCM, SNMP, and so forth, matching the failed data center.

Step 5 Prepare the surviving data center in the system to receive Join requests.
(See Preparing an MDC System to Receive Data Center Join Requests, on page 263).

Step 6 Join the new data center to the system.
(See Joining a Data Center to a Multi-Data Center System, on page 264).

The data from the surviving data center is replicated on the new data center.

Step 7 Update the DNS with the new URL and IP address information.

Removing a Data Center

When a data center is removed from a Multi-data Center (MDC) system, all CWMS settings are removed. Parameters that applied to the removed data center are deleted from the surviving data center.

Note In a Multi-data Center (MDC) environment the License Manager is running on only one data center; it cannot run on more than one data center. If you remove the data center that is hosting the License Manager, you have 90 days to configure the License Manager on another data center and re-host the licenses. (See Register Licenses to be Re-hosted, on page 257.)

Before You Begin

Make a backup of the system and the data center to be removed.

Remove all the DNS and Communications Manager entries.

Step 1 Power-off the virtual machines for the data center being removed.

Step 2 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 3 Select **Data Centers**.
The **Data Centers** window appears.

Step 4 (Optional) Verify that the data center is unreachable.
You can verify this manually or you can begin the process of removing the data center and let CWMS check availability. If the data center can be pinged, the remove process does not proceed, and an error message appears.

Step 5 To send a request to remove a data center from a MDC system, select **Remove** in the **Action** column.
If the data center being removed is hosting the License Manager, a warning appears. There is also a warning that DNS changes are required.

The primary data center is put into Maintenance Mode and the **Remove Data Center** window appears showing the progress of the action.

Step 6 Select **Continue**

Step 7 When all tasks are green, select **Done**.
The data center is removed and you are returned to the **Data Centers** window.

Step 8 Verify that the data center was removed.
URLs for system access change and system only retains the global URLs.

Step 9 Remove all DNS entries for the removed data center and map the Public and Private virtual IP addresses of the surviving data center to the global URLs.

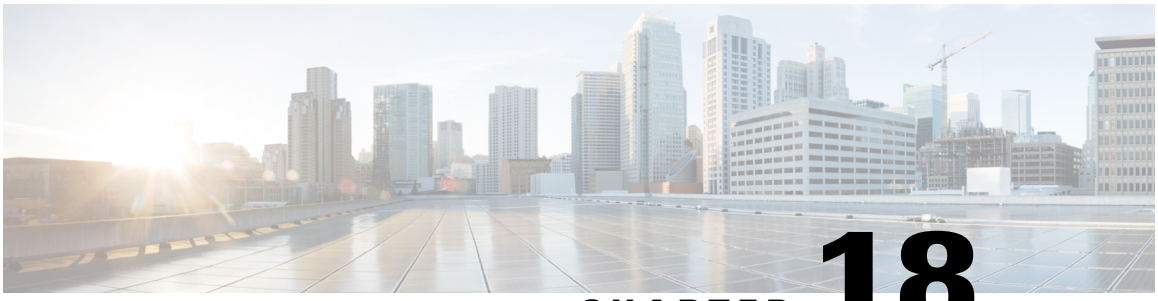
Step 10 Turn off Maintenance Mode.

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, on page 90.

Meeting service on the data center is restored.

Step 11 (Optional) If you removed the data center that hosts the License Manager, re-host the License Manager and licenses on the surviving data center.



CHAPTER 18

Using the Support Features

Customizing Your Log

You can generate log files that show activity on your entire system or for specific meetings. Use the log files to troubleshoot problems or to submit to the Cisco Technical Assistance Center (TAC) when you need assistance.

Note We recommend that you generate your log file during non-business hours. The large size of the log file can affect system performance.

Note Log data is retained for 40 days. However, if you upgrade from a Cisco WebEx Meetings Server 2.0 deployment to Release 2.5, the log data from Release 2.0 is not transferred to the Cisco WebEx Meetings Server 2.5 system and therefore not available after the upgrade to Release 2.5 is complete.

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 **Support** > **Logs**.

Step 3 Complete the fields on the **Customize Your Log** page and select **Submit**.

Field	Description
(Optional) Case ID	Enter your Cisco TAC case ID. Case IDs are obtained from the Cisco TAC when they are assisting you with a case. Using this feature enables you to associate the logs you generate with the case ID.
Type	Select the log type. You can select **Overall System Log** or **Particular Meeting Log**. An Overall System Log contains all the specified log information for your system and Particular Meeting Log collects logs and data from the database for MATS processing. **Default**: Overall System Log
Range	Select the range for your log. You must specify starting and ending date and time for your log. The limit is 24 hours. Log data is only available for the last 40 days. **Note** To generate logs longer than 24 hours you must repeat this operation, selecting consecutive date-time ranges. Each operation results in the creation of a separate log file. For example: To generate logs from January 1 to January 3, first select a date range from January 1 to January 2, select **Submit** and download the log file created. Next select a date range from January 2 to January 3, Select **Submit** and download the log file created.
Include	Specify the data you want to include in your log. **Default**: All Activities

The system generates your log and sends you an email that contains a link to download the log.

Setting Up a Remote Support Account

If you are having technical issues and contact the Cisco TAC for assistance, you can set up a remote support account to grant a TAC representative temporary access to your system. This product does not provide CLI access to administrators and therefore requires a TAC representative to troubleshoot some issues.

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 **Support** > **Remote Support Account**.

Step 3 Select **Enable Remote Support**.

Step 4 Complete the fields on the **Remote Support Account** page and select **Create Account**.

Field	Description
Remote Support Account Name	Enter a name for your remote support account (6–30 characters).
Account Life	Specify the duration of the account in hours. The maximum is 720 hours (30 days).

The **Remote Support Account Creation** dialog box appears, displaying your pass phrase code. Contact Cisco TAC and provide the Remote Support Account Name and the pass phrase code to allow Cisco Support personnel access to your system.

Disabling a Remote Support Account

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 **Support** > **Remote Support Account**.

Step 3 Next to the status message, "Remote Support is enabled," select the **Disable It** link.
The remote support account is disabled.