Cisco WebEx Meetings Server Administration Guide Release 1.5

First Published: August 16, 2013

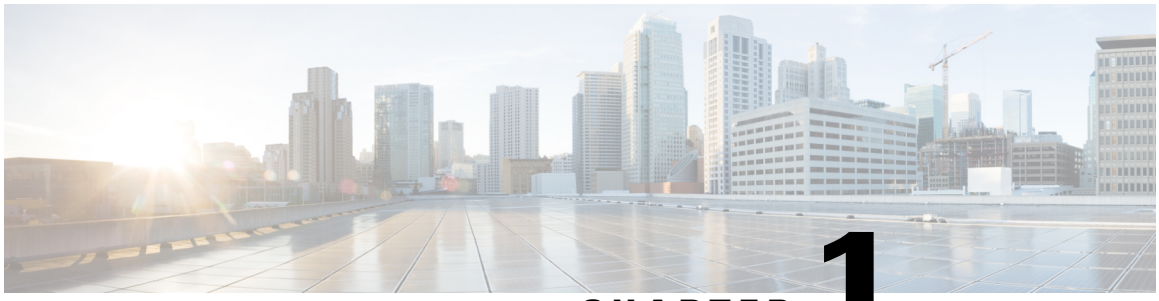
Last Modified: April 18, 2014

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

PART I

Cisco WebEx Meetings Server Installation Guide



CHAPTER 1

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, or 5.1.

  Earlier releases of vSphere are not supported.

- Use VMware ESXi 5.0, 5.0 Update 1, or 5.1.

  Use of earlier ESXi releases results in confusing error messages about **unsupported hardware** that do not explicitly list the problem.

- Ensure 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.

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

Configuring the ESXi Host to Use an NTP Server

The system uses the ESXi host to set the time. Configure the ESXi host to use Network Time Protocol (NTP) for clock synchronization.

Note This is a high-level procedure. For detailed instructions, see your VMware ESXi documentation.

Important Be sure to set up NTP configuration from the ESXi host.

Procedure

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

Step 2 Select the **Configuration** tab and select **Time Configuration** in the Software section.

Step 3 Select **Properties** at the top right of the panel.

Step 4 Select **NTP Client Enabled**.

Step 5 Select **Options** to configure the NTP server settings.
Cisco recommends you select **Start and stop with host** to lessen 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 Configuring a Storage Server 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.

Procedure

Step 1 Place the system in maintenance mode. For complete details, see About Maintenance Mode.
Be sure there are no active meetings and that you have selected a time where there will be minimal impact to your users.

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 your 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 Cisco recommends you delete backups after your system-altering procedure is complete, you have tested the system, and you are satisfied with the results.

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). We recommend that in addition to taking snapshots, that you backup your system.

Note If the original virtual machine disk file is lost, you cannot recover the virtual machine with the snapshot.

Snapshots are stored on the physical drives containing your virtual machines. If you do not delete these snapshots in a timely manner, your end users might experience degraded audio and video due to a known issue that affects virtual machine performance. Therefore, for performance reasons, we recommend that you use backups or 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. (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, Cisco recommends that you backup your system (especially when performing an upgrade) or take a snapshot (particularly 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.)

For performance reasons, be sure to keep your virtual machine snapshots in a storage location that is different from the physical drives that contain your virtual machines.

Be sure to read the preparation section for the specific procedure. Cisco lists specific considerations for each procedure.

Remember If your system comprises multiple virtual machines, select **Power** > **Shut Down Guest** and take a snapshot of each virtual machine in your system. Label the snapshot for each virtual machine with the same prefix, for example, August 20, so you know these snapshots were done at the same time.

Note Cisco recommends you keep snapshots no longer than 24 hours. If you want to keep them longer, then 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.

Procedure

Step 1 Place the system in maintenance mode. For complete details, see About Maintenance Mode.
Be sure there are no active meetings and that you have selected a time where there will be minimal impact to your users.

Step 2 On VMware vCenter, select **Power** > **Shut Down Guest** for each of the virtual machines.

Step 3 Select **Snapshot** > **Take Snapshot** for each virtual machine.

Step 4 Enter a name for the snapshot and select **OK**.

What to Do Next

- Complete the procedure and test your system to confirm that it is successful.
- If you need to 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 may result in possible database corruption.

Attaching an Existing VMDK File to a New Virtual Machine

This section describes how to attach a Virtual Machine Disk (VMDK) from an existing Admin virtual machine to a new Admin virtual machine by using VMware vCenter. This procedure is used when you expand or upgrade your system. (We reuse the system data stored on Hard disk 4 of the Admin virtual machine.)

Caution Make a copy of the Hard disk 4 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.

Note If you are using Direct-attached storage (DAS), you must 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.

Procedure

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_3-000001.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 your existing Admin virtual machine is located (from Step 5) and select **Browse this datastore**.

Step 9 Select the storage location where your newly deployed (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 expanded or 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 expanded or 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**.

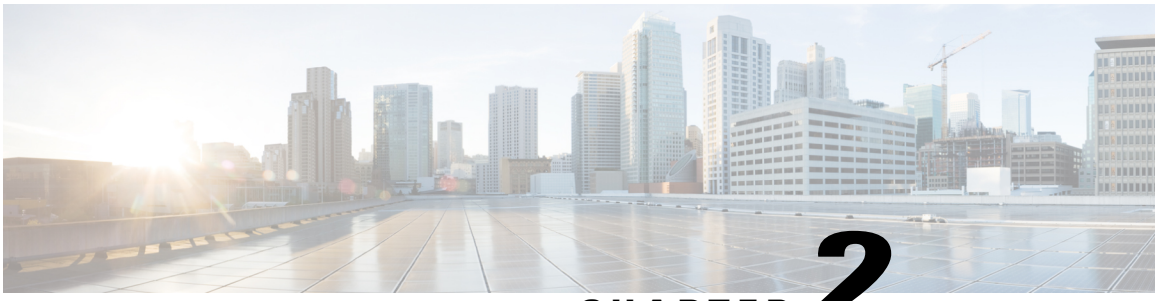
Step 19 Select **Browse**, and navigate to the datastore where the expanded or upgraded Admin virtual machine is located. Navigate to the new Admin virtual machine folder. Double-click this folder, then select the virtual disk you copied over in Step 11. Select **OK**.

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 there are no errors.



CHAPTER 2

Networking Checklist For Your System

Networking Checklist for a System with Public Access and Non-Split-Horizon DNS

During the deployment of your system, we display a page with links to the networking checklists. These checklists provide a summary of the DNS server, firewall, and other networking changes that are required for a successful deployment. Be sure to make these necessary changes prior to starting the deployment, as we do a network connectivity check near the end of the deployment process.

Note The non-split horizon DNS is the most common DNS configuration for companies. For more information about non-split horizon DNS, see the *Cisco WebEx Meetings Server Planning Guide*.

Note If you are deploying a large system, then you must choose a manual deployment.

Select the correct checklist in the *Cisco WebEx Meetings Server Planning Guide*.

- Automatic deployment: see "Networking Checklist For an Installation or Expansion With Automatic Deployment, Public Access, and a Non-Split-Horizon DNS"
- Manual deployment: see "Networking Checklist For an Installation or Expansion With Manual Deployment, Public Access, and a Non-Split Horizon DNS"

Networking Checklist for a System with Public Access and Split-Horizon DNS

During the deployment of your system, we display a page with links to the networking checklists. These checklists provide a summary of the DNS server, firewall, and other networking changes that are required for

a successful deployment. Be sure to make these necessary changes prior to starting the deployment, as we do a network connectivity check near the end of the deployment process.

Note If you are deploying a large system, then you must choose a manual deployment.

Select the correct checklist in the *Cisco WebEx Meetings Server Planning Guide*.

- Automatic deployment: see "Networking Checklist For an Installation or Expansion With Automatic Deployment, Public Access, and a Split-Horizon DNS"
- Manual deployment: see "Networking Checklist For an Installation or Expansion with Manual Deployment, Public Access, and a Split-Horizon DNS"

Networking Checklist for a System With No Public Access

During the deployment of your system, we display a page with links to the networking checklists. These checklists provide a summary of the DNS server, firewall, and other networking changes that are required for a successful deployment. Be sure to make these necessary changes prior to starting the deployment, as we do a network connectivity check near the end of the deployment process.

Note If you are deploying a large system, then you must choose a manual deployment.

Select the correct checklist in the *Cisco WebEx Meetings Server Planning Guide*.

- Automatic deployment: see "Networking Checklist For an Installation or Expansion with Automatic Deployment and No Public Access"
- Manual deployment: see "Networking Checklist For an Installation or Expansion With Manual Deployment and No Public Access"

CHAPTER 3

Deploying a System Automatically

General Concepts For Your System Deployment

System Sizes

- 50 concurrent users system
  - Typically supports a company between 500 and 1000 employees
  - Primary system (without HA) comprises an Admin virtual machine and an optional Internet Reverse Proxy (for public access)
- 250 concurrent users 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 (for public access)
- 800 concurrent users 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 (for public access)
- 2000 concurrent users 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 (for public access)

Terms Used During the Deployment

Field Name	Description
WebEx Site URL	Secure http URL for users to host and attend meetings.
WebEx Administration URL	Secure http URL for administrators to configure, monitor, and manage the system.
Public VIP	IP address for the WebEx site URL
Private VIP	• IP address for the Administration site URL • IP address for the WebEx site URL (for internal users only, if you have a split-horizon DNS).

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 appropriate networking checklist for your deployment. There are two considerations:

- Public access: whether or not users external to your firewall, can host and access meetings from the Internet or mobile devices.

  Cisco recommends public access as it results in 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 these types of DNS setup, see the *Cisco WebEx Meetings Server Planning Guide*.

- Open port 10200 from the administrator's desktop to the Admin virtual machine.

  Port 10200 is used by the web browser during the deployment.

Select the right checklist for your deployment:

- Networking Checklist for a System with Public Access and Non-Split-Horizon DNS, on page 9
- Networking Checklist for a System With No Public Access, on page 10
- Networking Checklist for a System with Public Access and Split-Horizon DNS, on page 9

Required Information

Note 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). Cisco recommends you select an automatic deployment unless you are deploying a 2000 user system, that requires a manual deployment. Refer to the appropriate link below.

Choose one of the following for a checklist of information required for your deployment type:

- Required Information For an Automatic Deployment, on page 13
- Required Information For a Manual Deployment, on page 41

Required Information For an Automatic Deployment

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

Note Be sure to 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 look up IP addresses for you during the deployment.

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

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 above.	
(250 and 800 concurrent user systems only) Datastore	Datastore 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 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	Fully qualified domain name (all lowercase characters) for the media virtual machine.	
(250 and 800 concurrent user systems only) IPv4 address for the media virtual machine	IPv4 address for the media virtual machine. We will automatically look up the corresponding IPv4 address for this media virtual machine.	

Field Name	Description	Value For Your System
(Public access only) ESXi host	ESXi host for the Internet Reverse Proxy virtual machine. **Note** Cisco recommends that you select a different ESXi host than you chose for the Admin and other internal virtual machine. 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) Datastore	Datastore 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	Fully qualified domain name (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 will automatically look up 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.	
(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)	

Field Name	Description	Value For Your System
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.

Deploying the OVA File From the VMware vSphere Client

Before deploying your system, you must use the VMware vSphere client to deploy the Admin virtual machine for your system.

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

Before You Begin

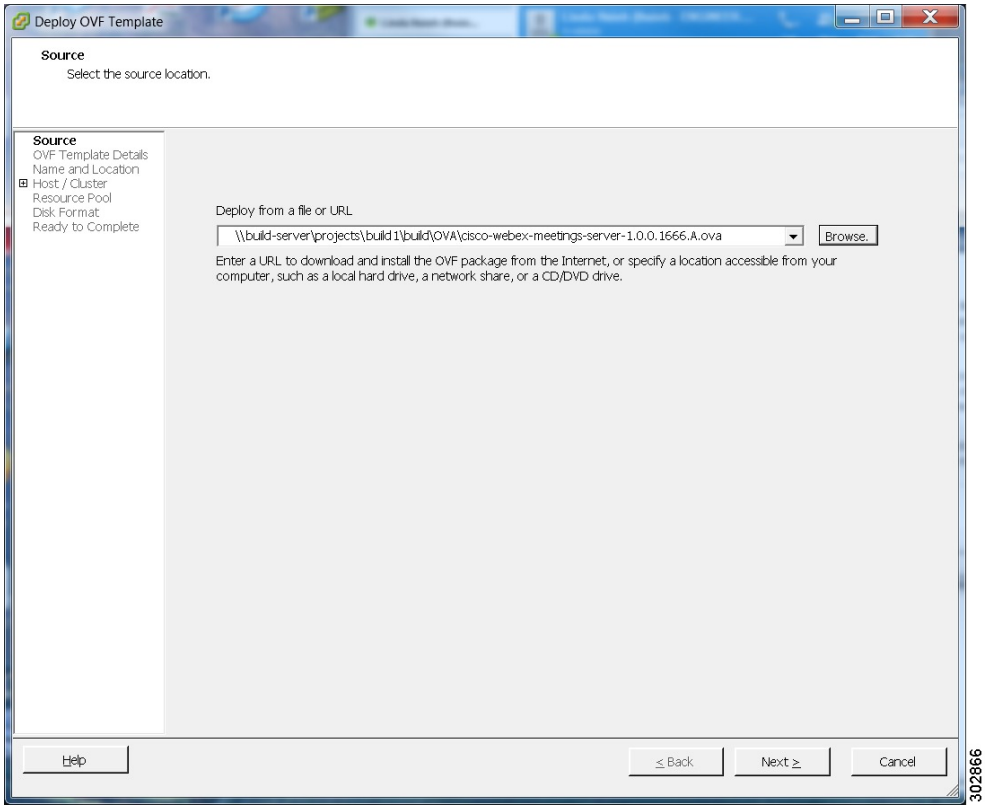
Obtain the Cisco WebEx Meetings Server OVA file for your system and place it in a location that is accessible from VMware vSphere.

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.

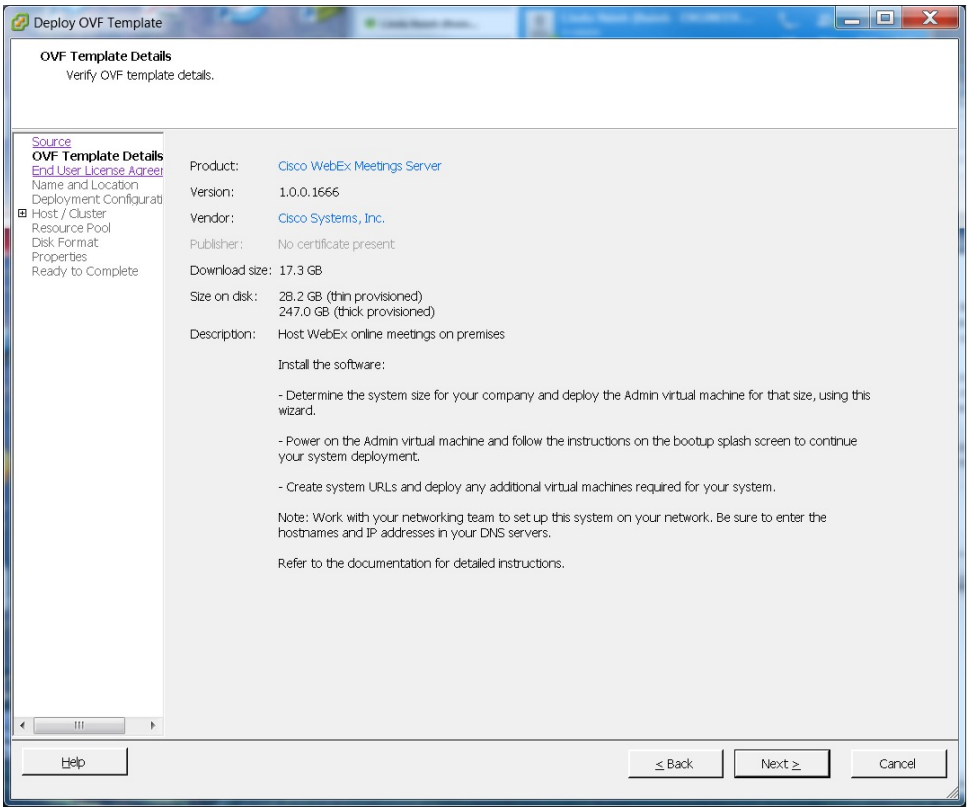
Procedure

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**.

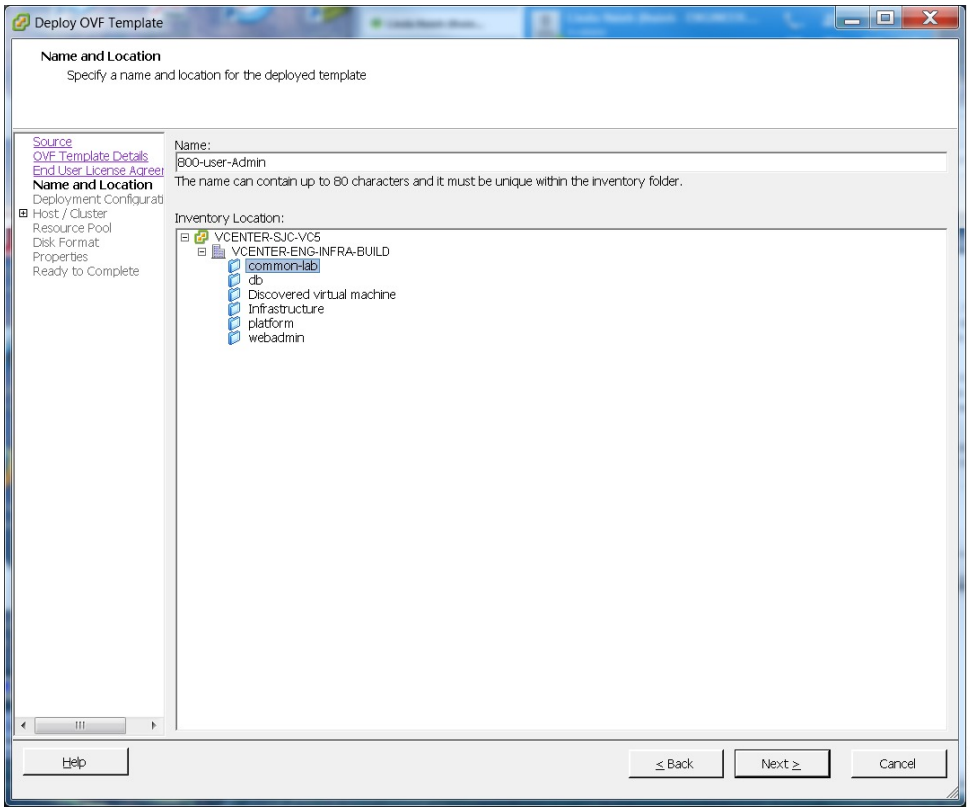
Step 5 Navigate to and select the location in the vCenter inventory where you want to place the Admin virtual machine.

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 System Sizes.

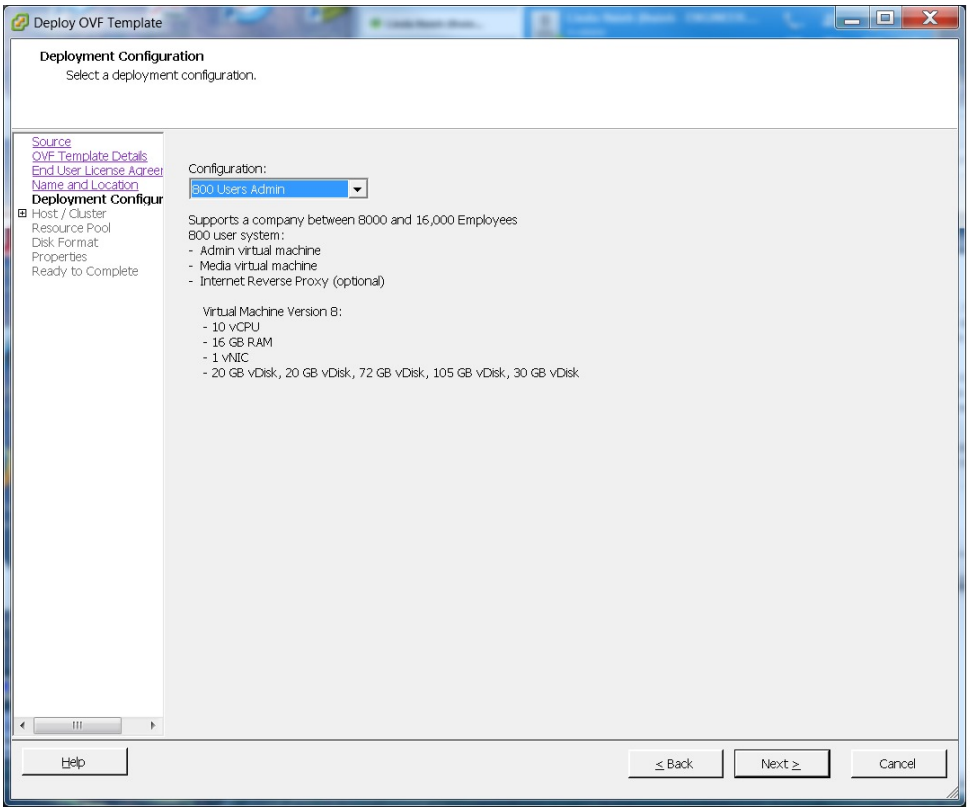
Note You must deploy the Admin virtual machine before deploying any other virtual machines. If you select automatic deployment (recommended), we deploy the other virtual machines for you. If you choose manual deployment (required for 2000 concurrent users system), then after deploying the Admin virtual 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.

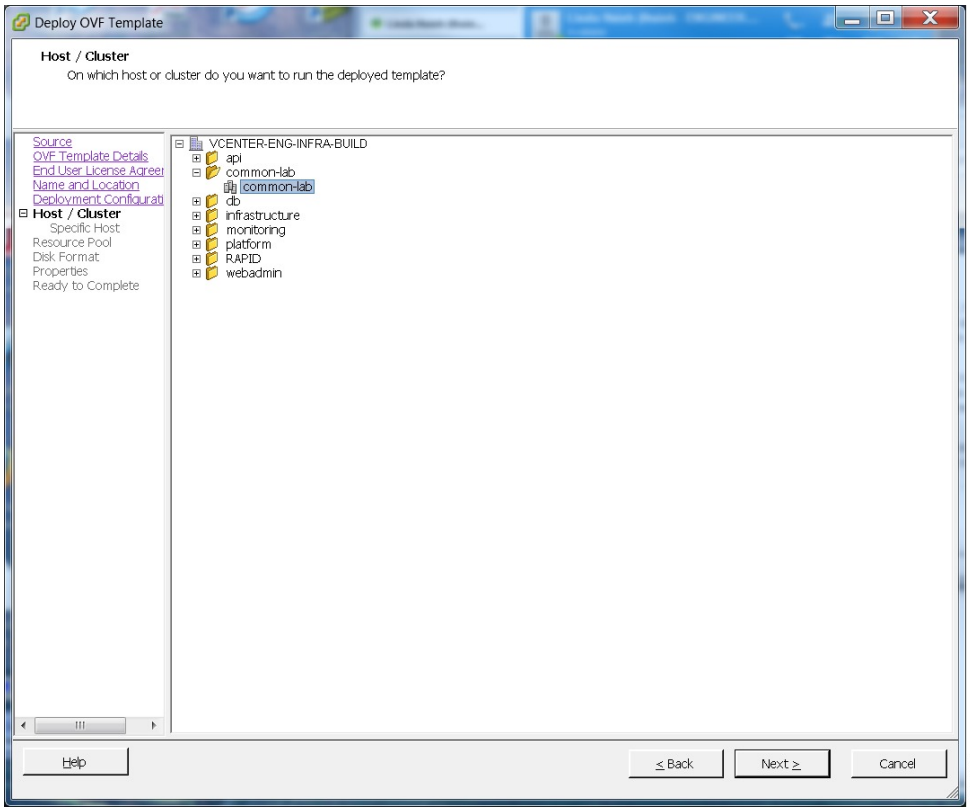
Note All the internal virtual machines for your system must be in the same subnet as the Admin virtual machine. (Depending on the system size you select, you might need one or more media and web internal virtual machines.)



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.

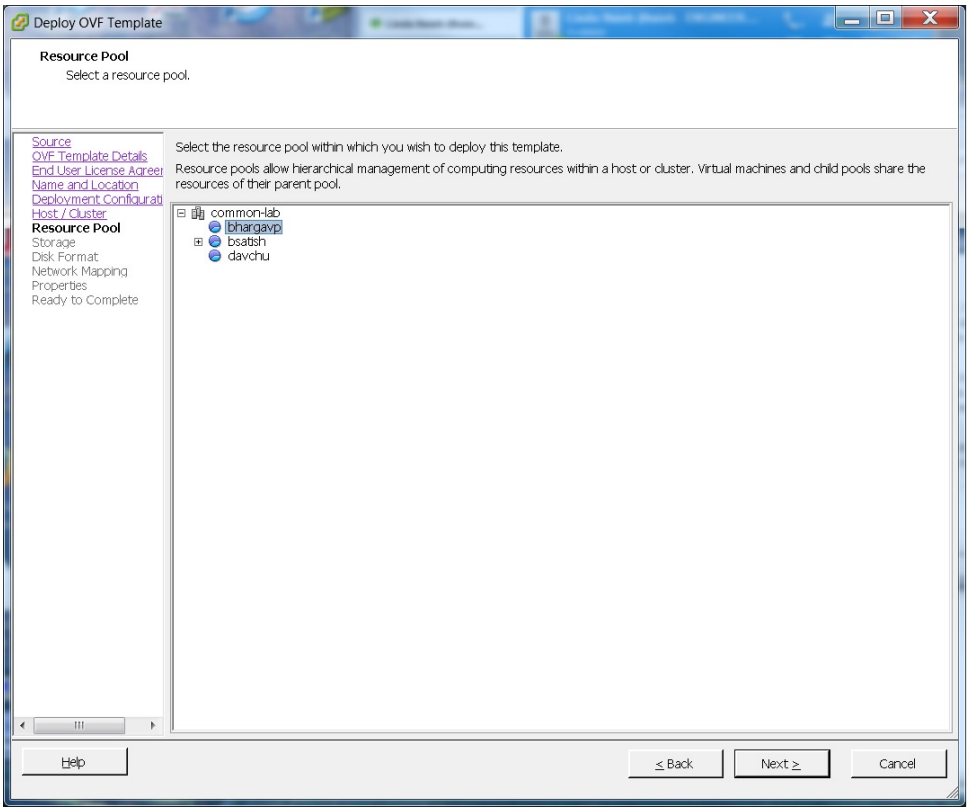


Step 8 Navigate through the vCenter inventory and select the ESXi host or cluster where you want to deploy the virtual machines for your system. Select **Next**.

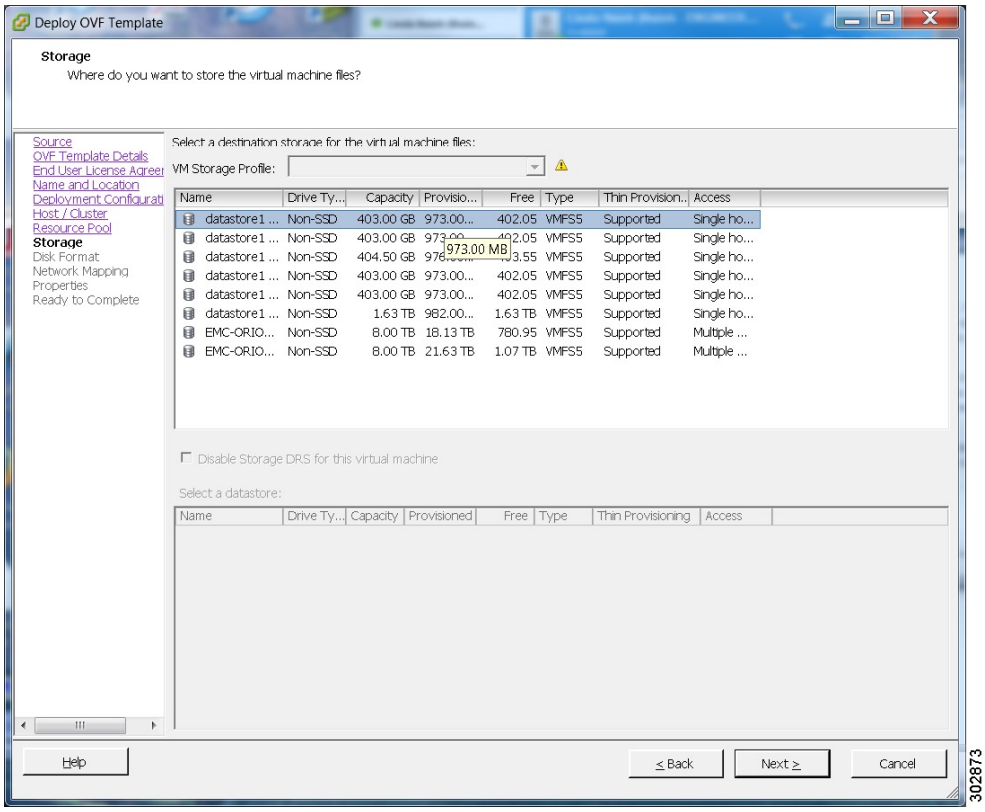


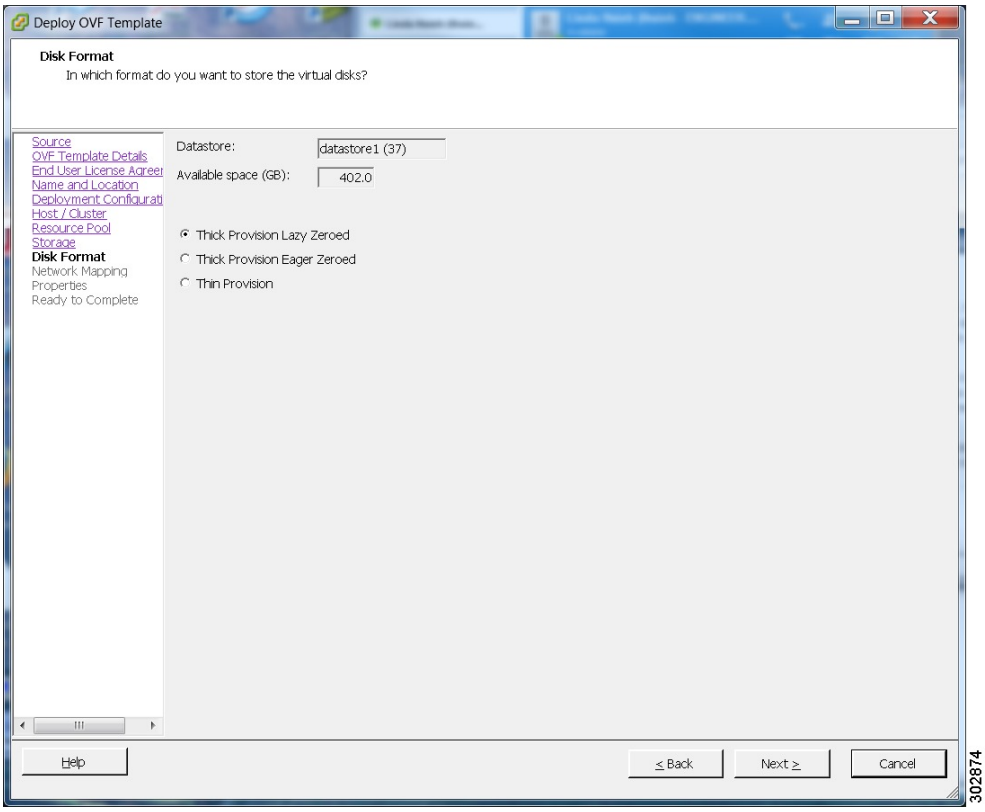
Step 9 If the cluster contains a resource pool, select the resource pool where you want to deploy the OVA template and select **Next**.

Resource pools share CPU and memory resources or to work 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.



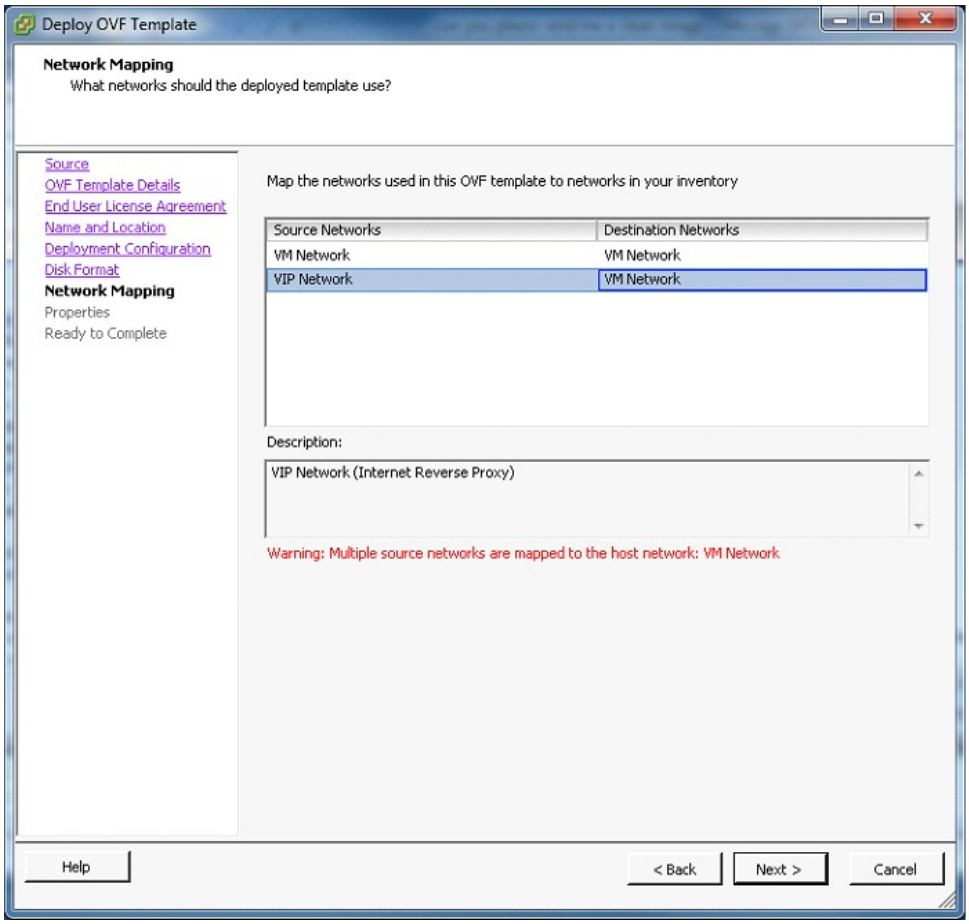
Step 10 Select the datastore for your virtual machine and the kind of provisioning for your virtual machine. You must select **Thick Provisioning** and create the maximum virtual disk space required for your system. With Thin Provisioning, VMware allocates the file system space on an *as-needed* basis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


Deploy OVF Template
Storage
Where do you want to store the virtual machine files?
Source
OVF Template Details
End User License Agreer
Name and Location
Deployment Configurati
Host / Cluster
Resource Pool
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Select a destination storage for the virtual machine files:
VM Storage Profile:
Name
Drive Ty...
Capacity
Provisio...
Free
Type
Thin Provision...
Access
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 404.50 GB 976.00... 403.55 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 1.63 TB 982.00... 1.63 TB VMFS5 Supported Single ho...
EMC-ORIO... Non-SSD 8.00 TB 18.13 TB 780.95 VMFS5 Supported Multiple ...
EMC-ORIO... Non-SSD 8.00 TB 21.63 TB 1.07 TB VMFS5 Supported Multiple ...
973.00 MB
Disable Storage DRS for this virtual machine
Select a datastore:
Name
Drive Ty...
Capacity
Provisioned
Free
Type
Thin Provisioning
Access
Help
< Back
Next >
Cancel
302873



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**.

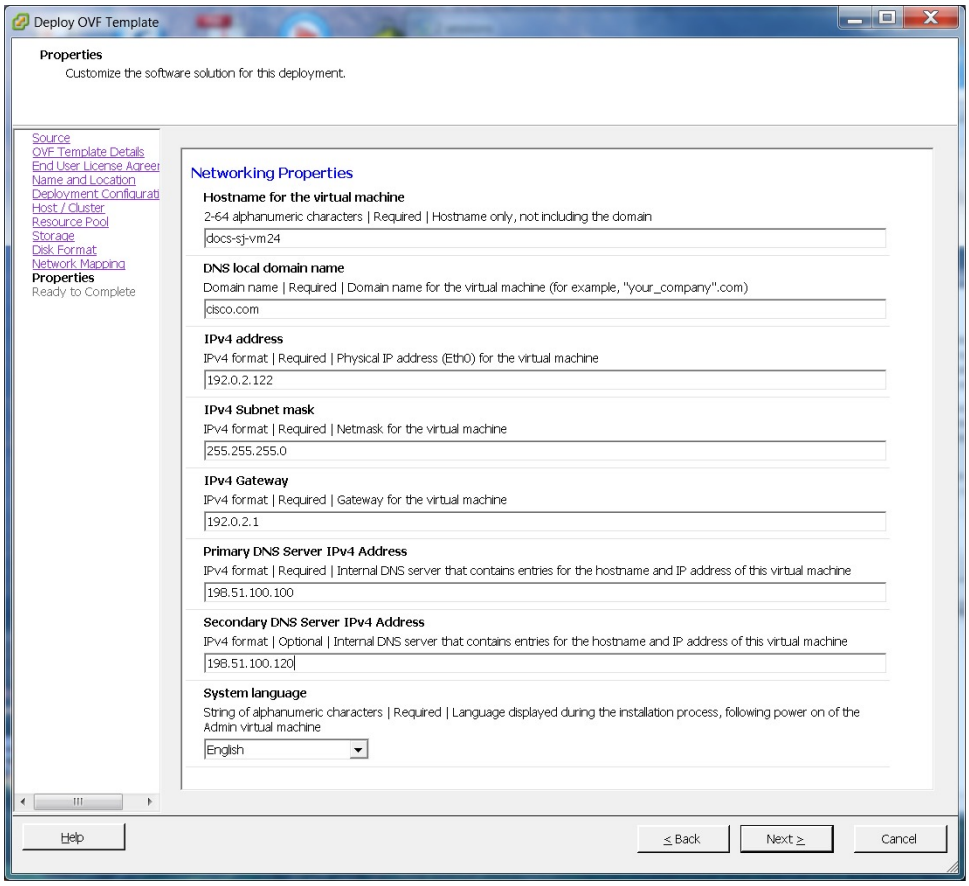
Note Both the VM Network and the VIP Network must be mapped to the same value in the Destination Network column. You can ignore the warning message about multiple source networks mapped to the same host network.



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

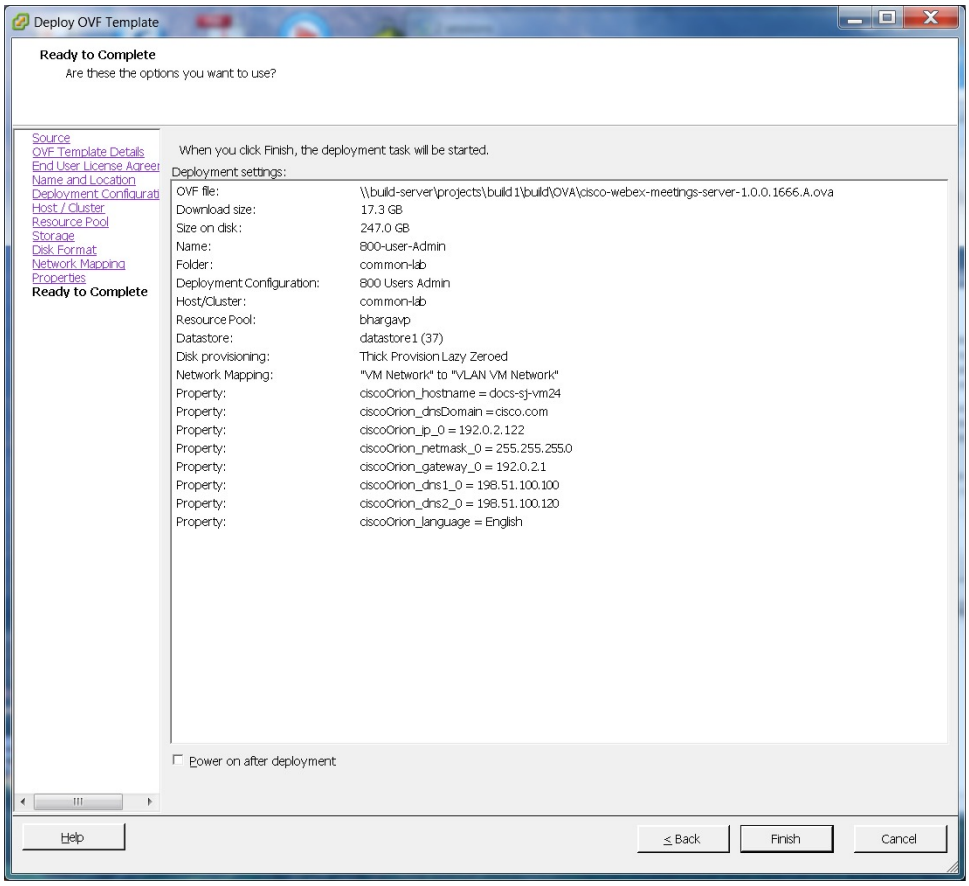
- Hostname of the virtual machine (do not include the domain here)
- Domain for the virtual machine
- IPv4 address (Eth0) of the virtual machine
- Subnet mask of the virtual machine
- Gateway IP address
- Primary DNS server that contains entries for the hostname and IP address of this virtual machine
- Secondary DNS server that contains entries for the hostname and IP address of this virtual machine
- 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 the balance of this procedure and continue with the next step in Upgrading the System Manually. (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 is displayed.
- If there is a problem, a red X is displayed. Fix the error and re-attempt the OVA deployment.

Step 16 When all the information is confirmed, write down the case-sensitive URL displayed in the console window. A software administrator will type this URL into a web browser, and continue the system deployment.

Note 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, Cisco recommends 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.

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.

Procedure

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.

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, you may have to restart the deployment.

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 16

Procedure

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

Step 2 Select **Next**.

Confirming the Deployment

To confirm that you are deploying a new system or expanding an existing system, select **Next**.

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.

- Confirm that the system size you selected during the OVA deployment is correct.
  - If the system size you selected is correct, then select **Next**.
  - If the system size you selected is incorrect, then select **I want to change System Size**.

a) Using your VMware vSphere client, select **Power** > **Shut Down Guest** for the Admin virtual machine with the incorrect system size.
b) Right-click the virtual machine and select **Delete from Disk**.
c) Redeploy the OVA file and select the Admin virtual machine for the correct system size.

Choosing What System to Install

Procedure

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 already installed a primary system and want a redundant High Availability system, then choose **Create a High Availability (HA) redundant system**.

Note You should not install a HA system before installing the primary system, as you cannot use the HA system unless the primary system has been installed.

Step 2 Select **Next**.

Choosing the Type of System Deployment

You can choose automatic or manual deployment of the system virtual machines.

Procedure

Step 1 Select automatic or manual deployment:

- **Automatic**: This is the fastest installation method. We deploy all the virtual machines required for your system.
  We recommend that you select **Automatic** unless you are deploying a 2000-user system that requires a manual deployment.
- **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.

Your choice of automatic or manual deployment depends upon the following:

- 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.

Step 2 Select **Next**.

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.

Procedure

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**.

Choosing vCenter Settings for your Media Virtual Machine

The media virtual machine is required for 250 user and 800 users system deployments.

Procedure

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

Step 2 Choose the datastore for the media virtual machine.

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

Step 4 Select **Next**.

Entering Networking Information for the Media Virtual Machine

By entering the fully qualified domain name of the media virtual machine, Cisco WebEx Meetings Server attempts to populate the networking information.

Note The media virtual machine 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 virtual machine.

Procedure

Step 1 Enter the FQDN of the Media virtual machine.
You should have already entered the hostname and IP address of the media virtual machine in your DNS servers. Cisco WebEx Meetings Server looks up and populates the **IPv4 Address**.

Step 2 Select **Next**.

Adding Public Access

If you add public access, users can host or attend meetings from the Internet or mobile devices. For additional information on setting this up for your company, see the *Cisco WebEx Meetings Server Planning Guide*.

Note You can always change this option later, through the WebEx Administration site.

Procedure

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

- If you want to add public access, confirm that the **Create an Internet Reverse Proxy virtual machine** check box has a check.
- If you want only internal users (behind your company's firewall) to host or attend meetings, then uncheck the **Create an Internet Reverse Proxy virtual machine** check box.

Step 2 Select **Next**.

What to Do Next

- With public access: Choosing vCenter Settings for Internet Reverse Proxy, on page 32
- Without public access: Entering the Private VIP Address, on page 34
- For IPv6 client connections: Configuring IPv6 for Client Connections

Configuring Reverse Proxy (for External Access)

The Internet Reverse Proxy enables users to host or attend meetings from the Internet or mobile devices.

Public access requires an Internet Reverse Proxy virtual machine. Enter the values you wrote down in your installation checklist. 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.

-

Choosing vCenter Settings for Internet Reverse Proxy

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

Procedure

Step 1 From the drop-down list, choose the ESXi host for the Internet Reverse Proxy virtual machine.

Step 2 Choose the datastore for the Internet Reverse Proxy.

Step 3 Choose the virtual machine port group for the Internet Reverse Proxy.

Step 4 Select **Next**.

Entering Networking Information for the Internet Reverse Proxy

The Internet Reverse Proxy enables users to host or attend meetings from the Internet or mobile devices.

- Enter the hostname and IP address of the Internet Reverse Proxy in your DNS servers to enable lookup from an external network.
  If you have DNS servers that enable look up from internal networks, enter the hostname and the IP address of the Internet Reverse Proxy in these DNS servers as well. This enables a secure connection between your internal virtual machines (administration and media, if applicable) and the Internet Reverse Proxy.
- Enter the following for the Internet Reverse Proxy:
  - Fully qualified domain name (FQDN)
    You should have already entered the hostname and IP address of the Internet Reverse Proxy virtual machine in your DNS servers. We will look up and populate the **Ipv4 Address** field for you.
  - IPv4 gateway
  - IPv4 subnet mask
  - Primary DNS server IPv4 address
  - (Optional) Secondary DNS server IPv4 address
- Select **Next**.

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**.

Entering the Private VIP Address

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

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

Note If you are adding 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.

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**.

WebEx Site and WebEx Administration URLs

WebEx Site URL

End users access the WebEx site URL to 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.

WebEx Administration URL

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

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 site URLs:

- the same name as the hostnames for any of the virtual machines comprising 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

Entering the WebEx Site and Administration URLs

These URLs provide access and 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. The URLs have these limitations:

- You cannot reuse the hostnames of the virtual machines in your system in the hostname portion of the Administration or WebEx site URLs.
- The WebEx Site URL must be different from the WebEx Administration URL.
- Enter the following secure (https) URLs:
  - WebEx site URL for users to host and attend meetings
  - WebEx Administration URL for system administrators to manage your system
- Select **Next**.

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.

Deploying the Virtual Machines

Based on the information 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 (or error messages are displayed indicating the deployment failed).

When the status column shows all green checks, the deployment is complete with no errors. Select **Next**.

If errors are indicated, fix the errors and select **Next** to redeploy the system. You can select **Download log file** to obtain the log file for this deployment. The log provides a record of the deployment, that can be used to troubleshoot a failed deployment.

Note Before redeploying a system, be sure to power off and delete any virtual machines involved with the errors; otherwise, during a redeployment you might see error messages about existing virtual machines.

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.

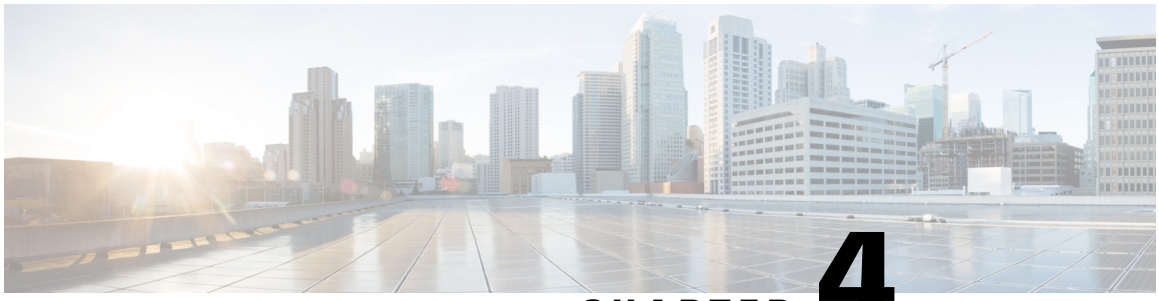
If you reload the page before the checks are complete, you are returned to the first page of this system deployment. When the checks are completed successfully, the first page of configuration utility appears.

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. 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) and identifying an administrator (Creating Administrator Accounts). If another administrator will complete the basic configuration, send this URL to that administrator.



CHAPTER 4

Deploying a System Manually

General Concepts For Your System Deployment

System Sizes

- 50 concurrent users system
    - Typically supports a company between 500 and 1000 employees

- Primary system (without HA) comprises an Admin virtual machine and an optional Internet Reverse Proxy (for public access)

- 250 concurrent users 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 (for public access)

- 800 concurrent users 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 (for public access)

- 2000 concurrent users 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 (for public access)

Terms Used During the Deployment

Field Name	Description
WebEx Site URL	Secure http URL for users to host and attend meetings.
WebEx Administration URL	Secure http URL for administrators to configure, monitor, and manage the system.
Public VIP	IP address for the WebEx site URL
Private VIP	• IP address for the Administration site URL • IP address for the WebEx site URL (for internal users only, if you have a split-horizon DNS).

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 appropriate networking checklist for your deployment. There are two considerations:

- Public access: whether or not users external to your firewall, can host and access meetings from the Internet or mobile devices.

  Cisco recommends public access as it results in 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 these types of DNS setup, see the *Cisco WebEx Meetings Server Planning Guide*.

- Open port 10200 from the administrator's desktop to the Admin virtual machine.

  Port 10200 is used by the web browser during the deployment.

Select the right checklist for your deployment:

- Networking Checklist for a System with Public Access and Non-Split-Horizon DNS, on page 9
- Networking Checklist for a System With No Public Access, on page 10
- Networking Checklist for a System with Public Access and Split-Horizon DNS, on page 9

Required Information

Note 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). Cisco recommends you select an automatic deployment unless you are deploying a 2000 user system, that requires a manual deployment. Refer to the appropriate link below.

Choose one of the following for a checklist of information required for your deployment type:

- Required Information For an Automatic Deployment, on page 13
- Required Information For a Manual Deployment, on page 41

Required Information For a Manual Deployment

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

You must choose a manual deployment if you are deploying a 2000 user system.

Note Be sure to 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 will use this information to check network connectivity at the end of the deployment.

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

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 you selected, the fully qualified domain name (all lowercase characters) of the media and web virtual machines.	
(Public access only) FQDN of the Internet Reverse Proxy	If you plan to add public access, then you need to enter the fully qualified domain name (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.

Deploying the OVA File From the VMware vSphere Client

Before deploying your system, you must use the VMware vSphere client to deploy the Admin virtual machine for your system.

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

Before You Begin

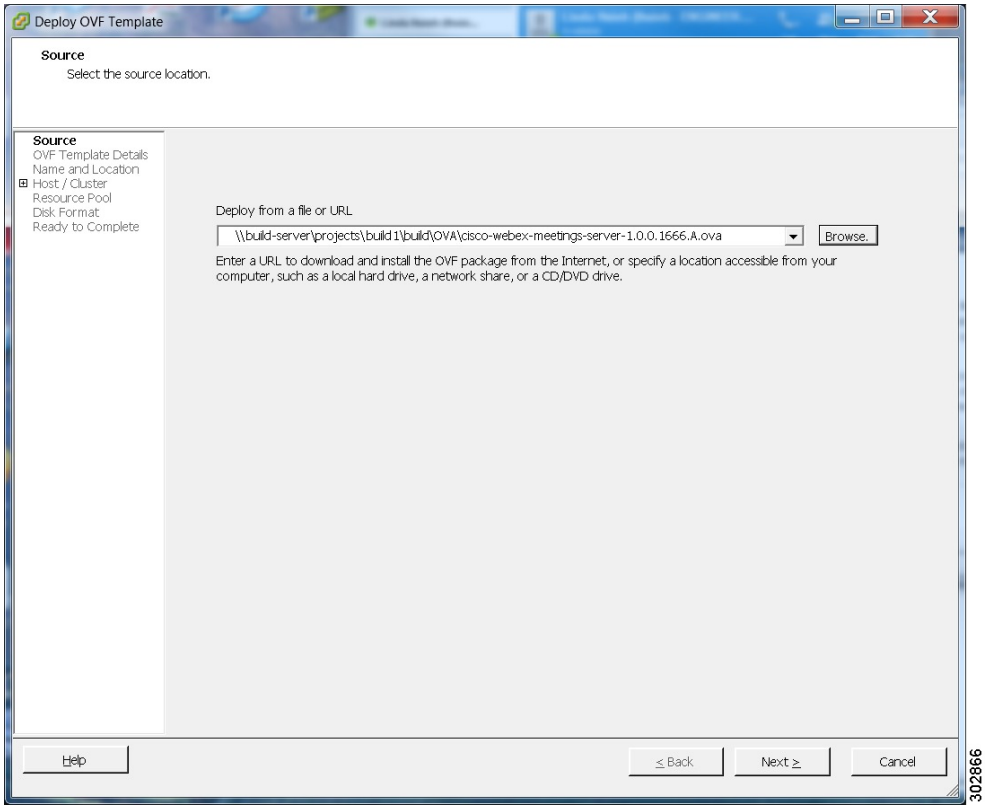
Obtain the Cisco WebEx Meetings Server OVA file for your system and place it in a location that is accessible from VMware vSphere.

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.

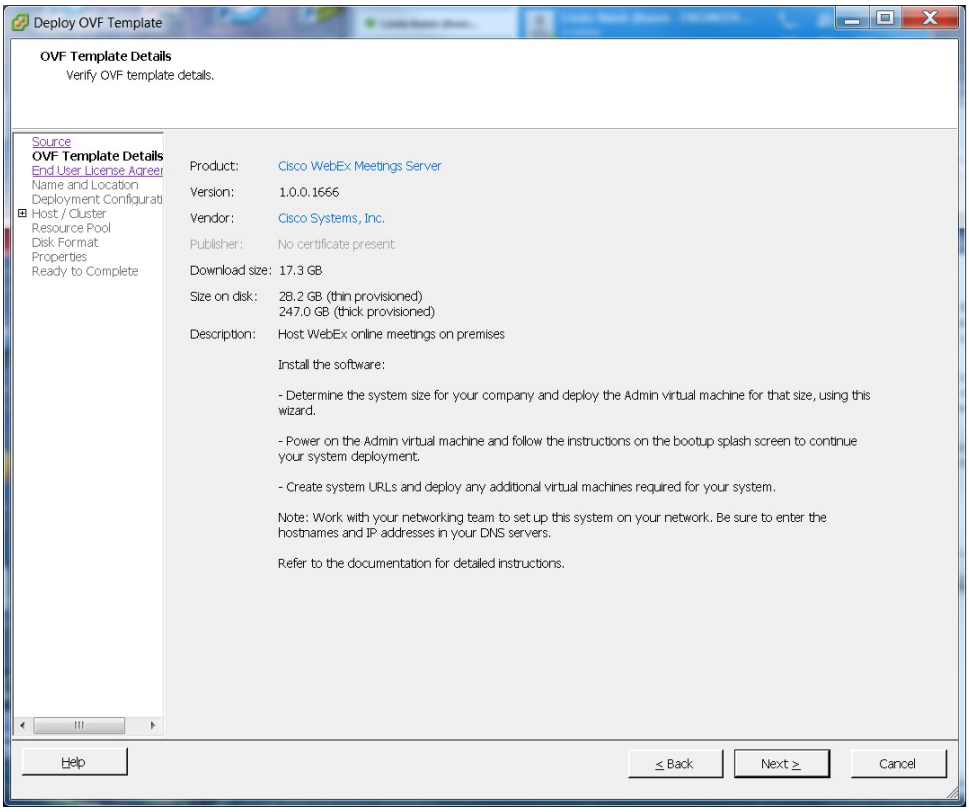
Procedure

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**.

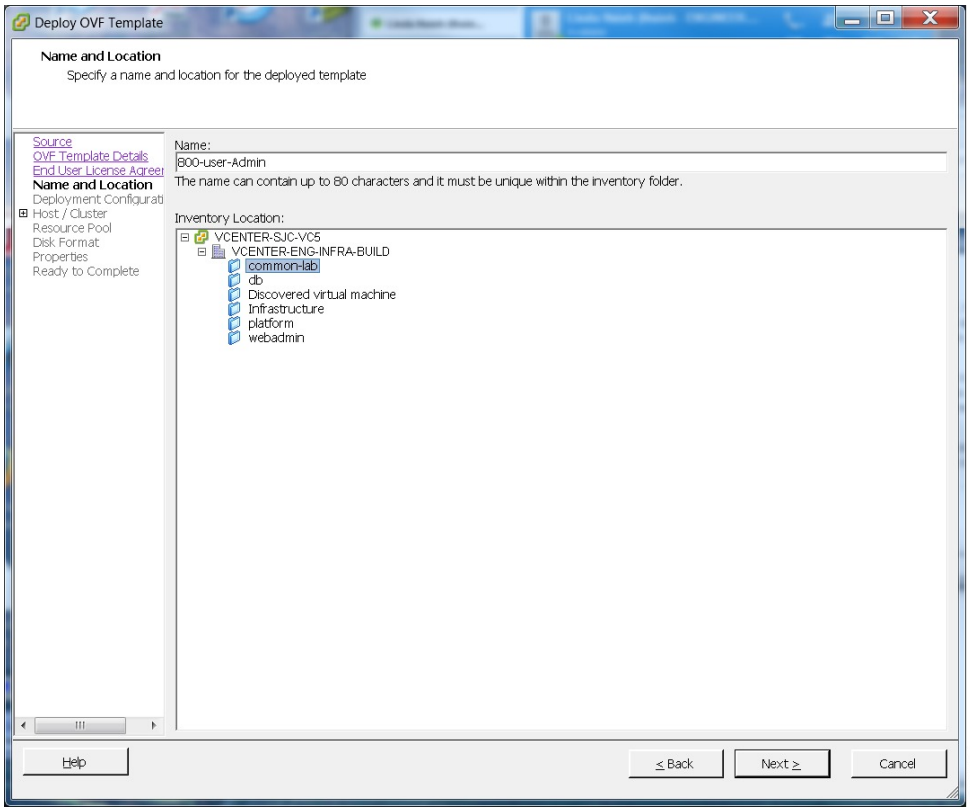
Step 5 Navigate to and select the location in the vCenter inventory where you want to place the Admin virtual machine.

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 System Sizes.

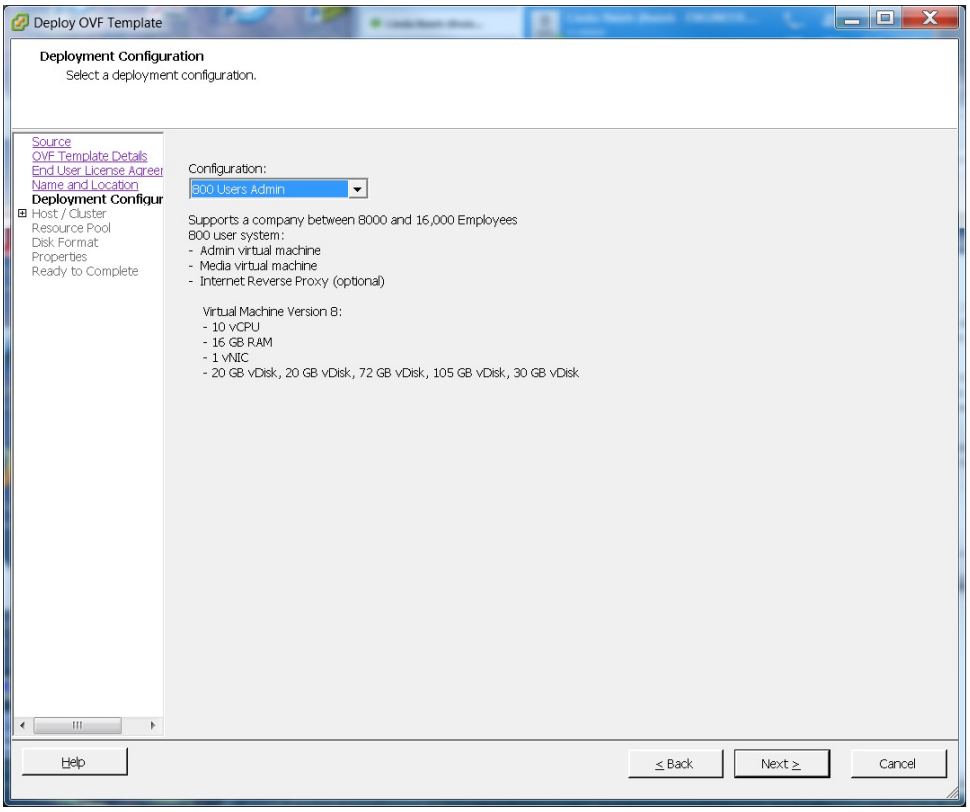
Note You must deploy the Admin virtual machine before deploying any other virtual machines. If you select automatic deployment (recommended), we deploy the other virtual machines for you. If you choose manual deployment (required for 2000 concurrent users system), then after deploying the Admin virtual 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.

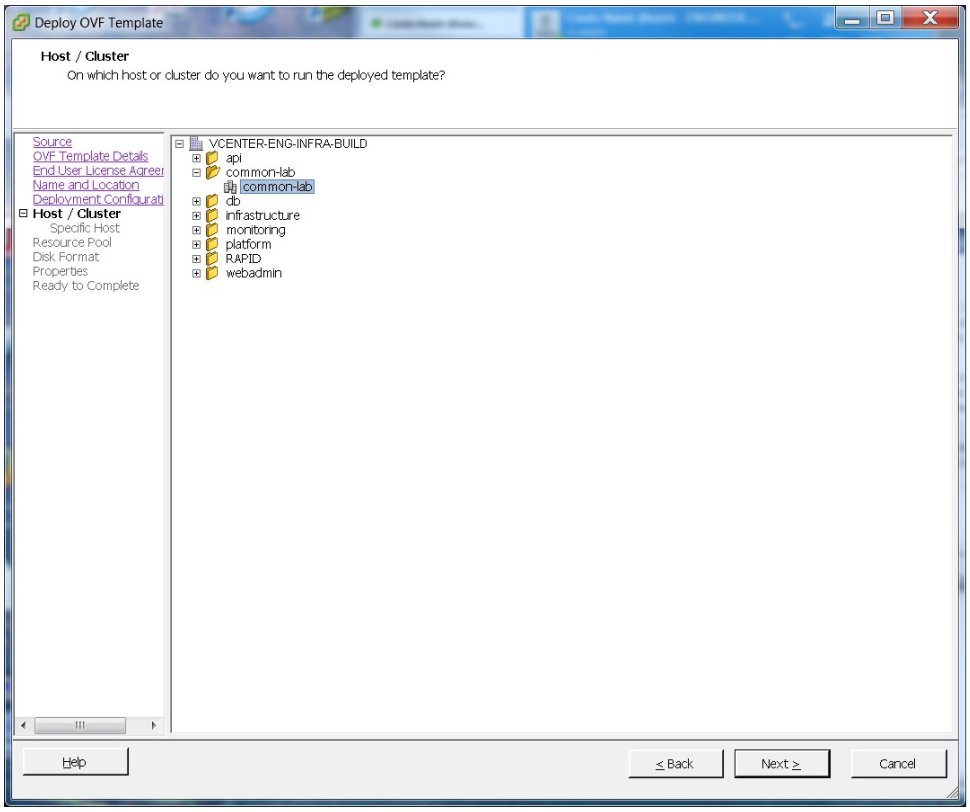
Note All the internal virtual machines for your system must be in the same subnet as the Admin virtual machine. (Depending on the system size you select, you might need one or more media and web internal virtual machines.)



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.

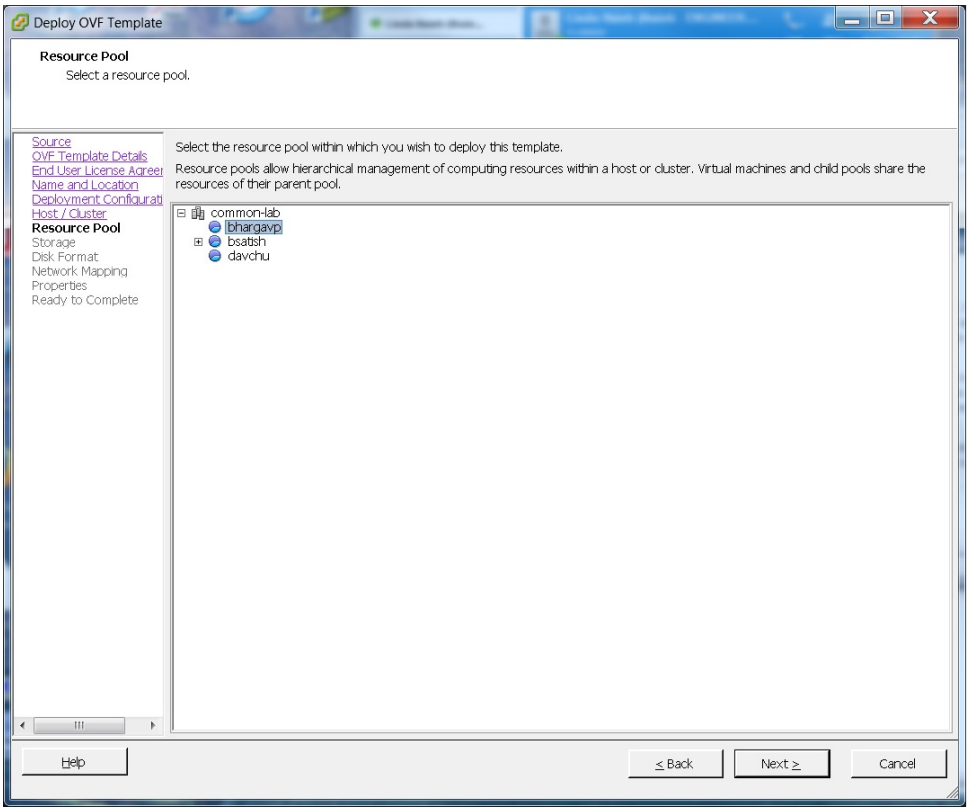


Step 8 Navigate through the vCenter inventory and select the ESXi host or cluster where you want to deploy the virtual machines for your system. Select **Next**.

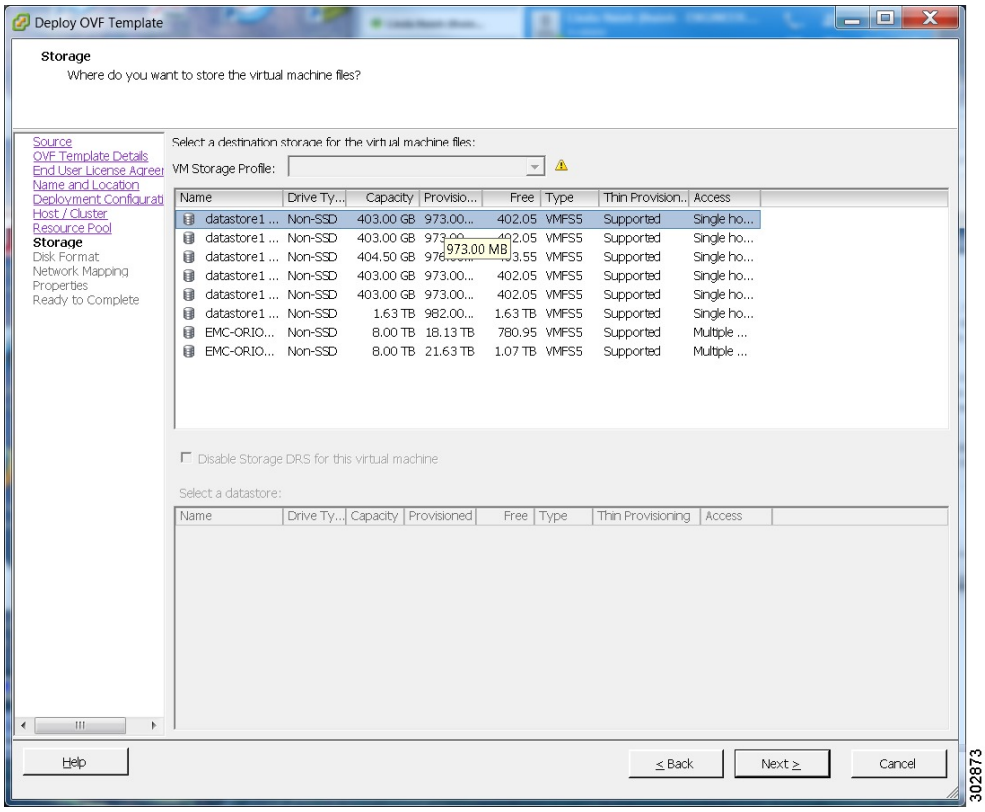


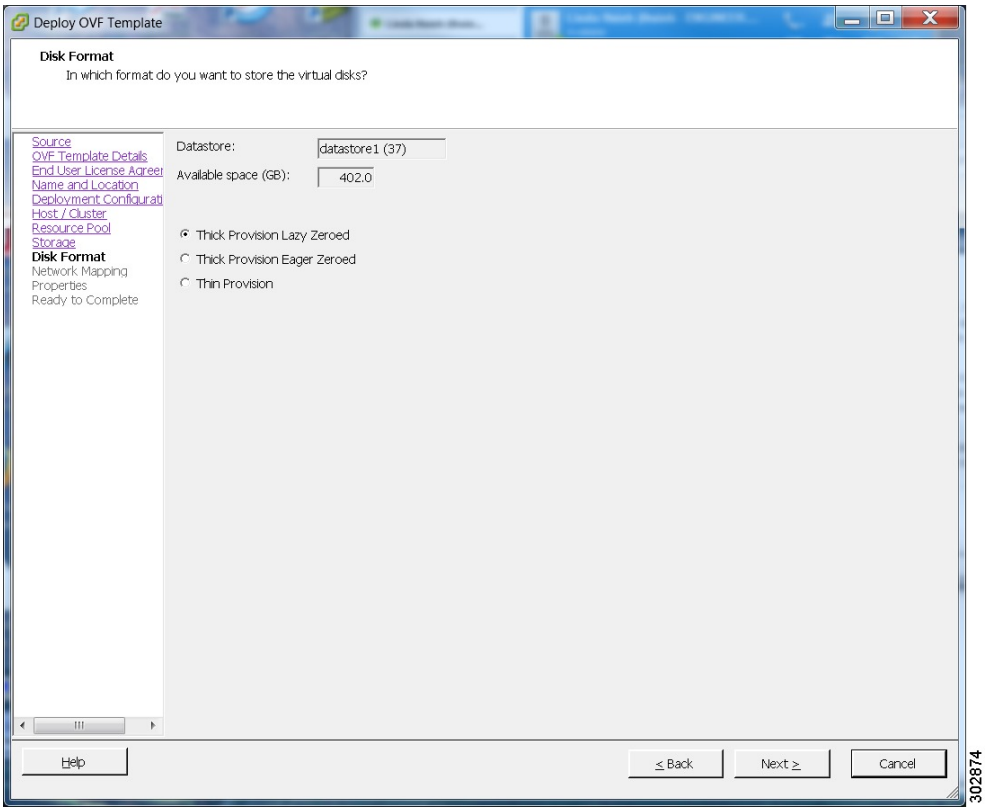
Step 9 If the cluster contains a resource pool, select the resource pool where you want to deploy the OVA template and select **Next**.

Resource pools share CPU and memory resources or to work 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.



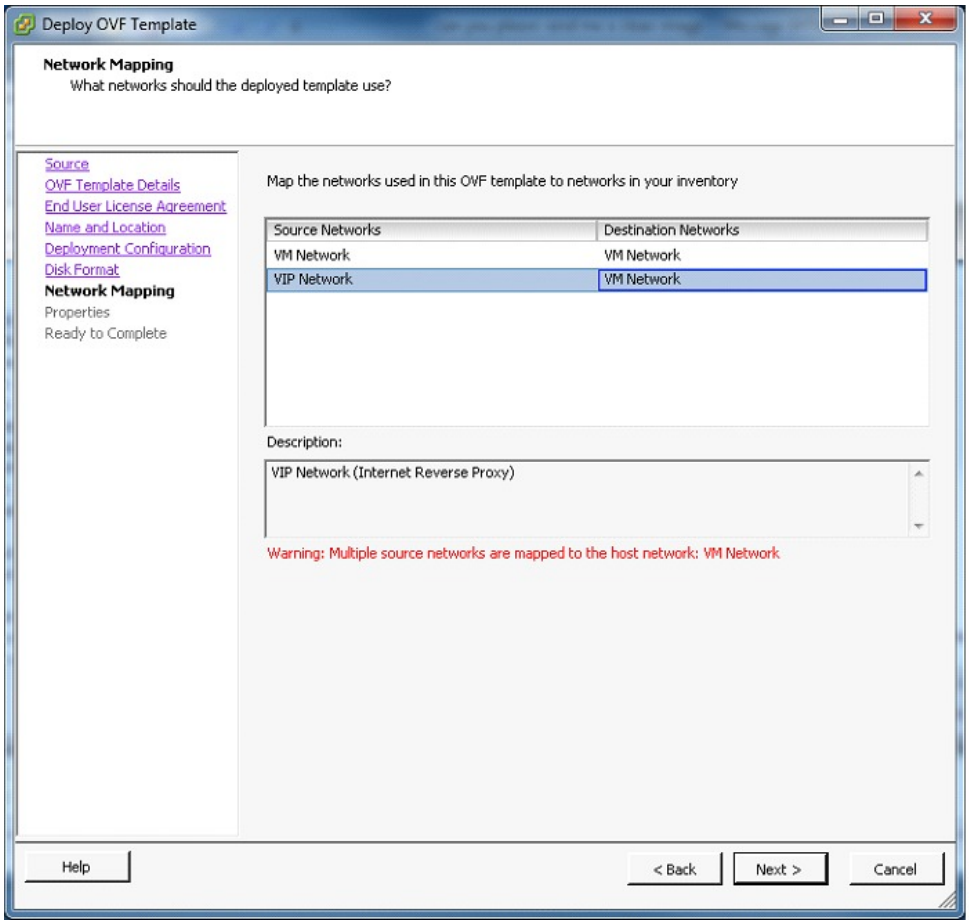
Step 10 Select the datastore for your virtual machine and the kind of provisioning for your virtual machine. You must select **Thick Provisioning** and create the maximum virtual disk space required for your system. With Thin Provisioning, VMware allocates the file system space on an *as-needed* basis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


Deploy OVF Template
Storage
Where do you want to store the virtual machine files?
Source
OVF Template Details
End User License Agreer
Name and Location
Deployment Configurati
Host / Cluster
Resource Pool
Storage
Disk Format
Network Mapping
Properties
Ready to Complete
Select a destination storage for the virtual machine files:
VM Storage Profile:
Name
Drive Ty...
Capacity
Provisio...
Free
Type
Thin Provision...
Access
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 404.50 GB 976.00... 403.55 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 403.00 GB 973.00... 402.05 VMFS5 Supported Single ho...
datastore1 ... Non-SSD 1.63 TB 982.00... 1.63 TB VMFS5 Supported Single ho...
EMC-ORIO... Non-SSD 8.00 TB 18.13 TB 780.95 VMFS5 Supported Multiple ...
EMC-ORIO... Non-SSD 8.00 TB 21.63 TB 1.07 TB VMFS5 Supported Multiple ...
973.00 MB
Disable Storage DRS for this virtual machine
Select a datastore:
Name
Drive Ty...
Capacity
Provisioned
Free
Type
Thin Provisioning
Access
Help
< Back
Next >
Cancel
302873



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**.

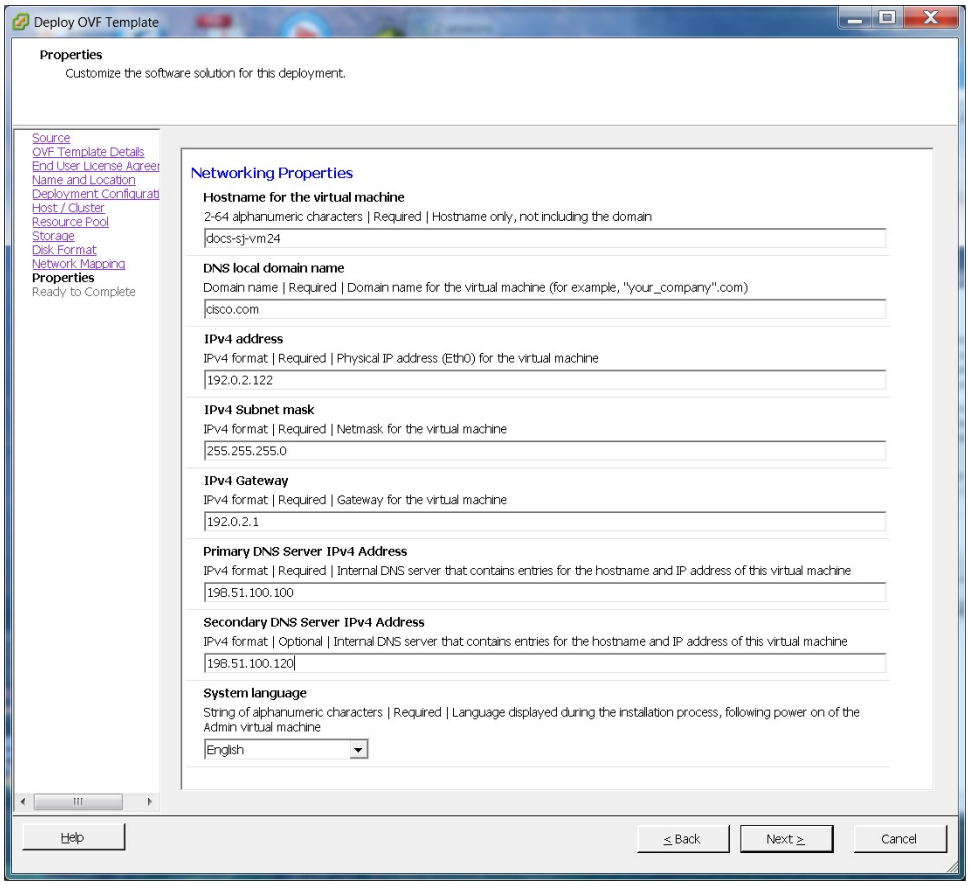
Note Both the VM Network and the VIP Network must be mapped to the same value in the Destination Network column. You can ignore the warning message about multiple source networks mapped to the same host network.



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

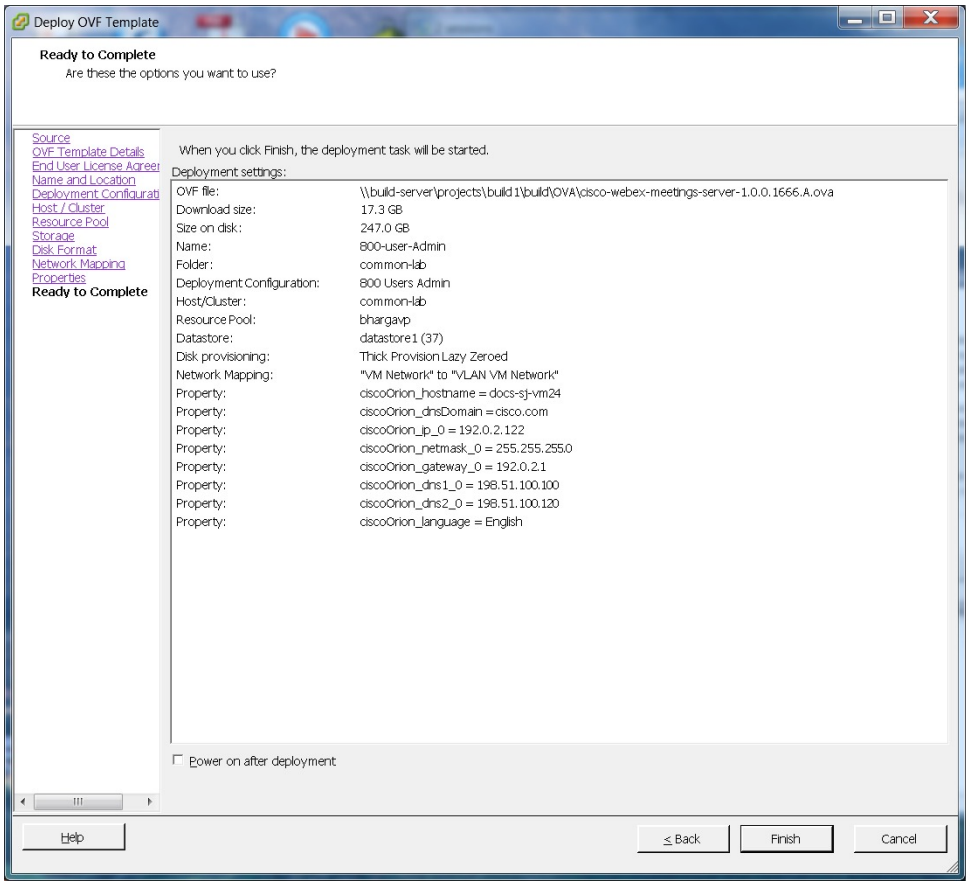
- Hostname of the virtual machine (do not include the domain here)
- Domain for the virtual machine
- IPv4 address (Eth0) of the virtual machine
- Subnet mask of the virtual machine
- Gateway IP address
- Primary DNS server that contains entries for the hostname and IP address of this virtual machine
- Secondary DNS server that contains entries for the hostname and IP address of this virtual machine
- 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 the balance of this procedure and continue with the next step in Upgrading the System Manually. (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 is displayed.
- If there is a problem, a red X is displayed. Fix the error and re-attempt the OVA deployment.

Step 16 When all the information is confirmed, write down the case-sensitive URL displayed in the console window. A software administrator will type this URL into a web browser, and continue the system deployment.

Note 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, Cisco recommends 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.

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.

Procedure

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.

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, you may have to restart the deployment.

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 16

Procedure

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

Step 2 Select **Next**.

Confirming the Deployment

To confirm that you are deploying a new system or expanding an existing system, select **Next**.

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.

- Confirm that the system size you selected during the OVA deployment is correct.
  - If the system size you selected is correct, then select **Next**.
  - If the system size you selected is incorrect, then select **I want to change System Size**.

a) Using your VMware vSphere client, select **Power** > **Shut Down Guest** for the Admin virtual machine with the incorrect system size.
b) Right-click the virtual machine and select **Delete from Disk**.
c) Redeploy the OVA file and select the Admin virtual machine for the correct system size.

Choosing What System to Install

Procedure

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 already installed a primary system and want a redundant High Availability system, then choose **Create a High Availability (HA) redundant system**.

Note You should not install a HA system before installing the primary system, as you cannot use the HA system unless the primary system has been installed.

Step 2 Select **Next**.

Choosing the Type of System Deployment

You can choose automatic or manual deployment of the system virtual machines.

Procedure

Step 1 Select automatic or manual deployment:

- **Automatic**: This is the fastest installation method. We deploy all the virtual machines required for your system.
  We recommend that you select **Automatic** unless you are deploying a 2000-user system that requires a manual deployment.
- **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.

Your choice of automatic or manual deployment depends upon the following:

- 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.

Step 2 Select **Next**.

Adding Public Access

If you add public access, users can host or attend meetings from the Internet or mobile devices. For additional information on setting this up for your company, see the *Cisco WebEx Meetings Server Planning Guide*.

Note You can always change this option later, through the WebEx Administration site.

Procedure

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

- If you want to add public access, confirm that the **Create an Internet Reverse Proxy virtual machine** check box has a check.

- If you want only internal users (behind your company's firewall) to host or attend meetings, then uncheck the **Create an Internet Reverse Proxy virtual machine** check box.

Step 2 Select **Next**.

What to Do Next

- With public access: Choosing vCenter Settings for Internet Reverse Proxy, on page 32
- Without public access: Entering the Private VIP Address, on page 34
- For IPv6 client connections: Configuring IPv6 for Client Connections

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**.

Entering the Private VIP Address

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

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

Note If you are adding 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.

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**.

WebEx Site and WebEx Administration URLs

WebEx Site URL

End users access the WebEx site URL to 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.

WebEx Administration URL

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

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 site URLs:

- the same name as the hostnames for any of the virtual machines comprising 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

Entering the WebEx Site and Administration URLs

These URLs provide access and 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. The URLs have these limitations:

- You cannot reuse the hostnames of the virtual machines in your system in the hostname portion of the Administration or WebEx site URLs.
- The WebEx Site URL must be different from the WebEx Administration URL.
- Enter the following secure (https) URLs:
  - WebEx site URL for users to host and attend meetings
  - WebEx Administration URL for system administrators to manage your system
- Select **Next**.

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.

Deploying Virtual Machines

After providing information about the virtual machines in the system, we will attempt to connect to each of the virtual machines deployed for your system.

Note Do not leave this page until the system has connected to all the virtual machines, or the connection failed with error messages indicating the problem.

Procedure

Step 1 Enter the fully qualified domain names (FQDNs) for any additional 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 all the additional virtual machines required for the system.

Step 3 Power on all these virtual machines and verify that they powered on successfully. Then select **Detect virtual machines**.
We establish connections to these virtual machines. This might take several minutes.

Step 4 Wait until a **Connected** status is displayed for each the virtual machine, then complete one of the following:

- If there are no errors, the status shows all green checks. If you are satisfied with the configuration so far, select **Next**. Otherwise, you can change the FQDNs of the virtual machines by again selecting **Detect virtual machines**.
- If you see errors, fix the errors and select **Next** to continue.
  Note You can select **Download log file** to obtain the log file for this deployment, providing a record that can be used to troubleshoot a failed deployment.
- If there are other problems with one or more of the virtual machines, from the VMware vCenter power off the virtual machines with errors and manually delete them. (If you do not delete them, you might see error messages regarding these virtual machines.) After fixing the problems, redeploy the virtual machines from the OVA file and select **Detect virtual machines**.

Checking the System

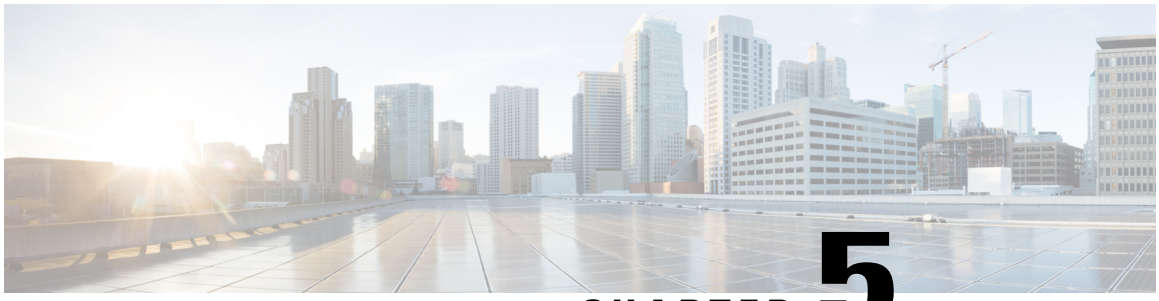
The system check verifies the configuration parameters of your system. This includes confirming that the virtual machines have the required minimum configuration, and validating the WebEx site and WebEx Administration URLs.

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. 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) and identifying an administrator (Creating Administrator Accounts). If another administrator will complete the basic configuration, send this URL to that administrator.



CHAPTER 5

Configuring Your Mail Server, Time Zone, and Locale

Configuring an eMail (SMTP) Server

Configure a mail server to enable your system to send meeting invitations and other communications to users.

Note It is important that the mail 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.

Procedure

Step 1 Sign into the Administration web site.

Step 2 Select **System** and select **View More** in the Servers section.

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

Step 4 In the **SMTP Server** section, select **Edit**.

Step 5 Enter the fully qualified domain name (FQDN) of a mail server that the system will use to send emails.

Step 6 Optionally select **TLS enabled**.

Step 7 Optionally 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 mail server. If there is a firewall between the internal Web and Admin virtual machines and the mail server, the SMTP traffic might be blocked. To ensure mail server configuration and mail notification work properly, port 25 or 465 (secure SMTP port number) must be open between the mail server and the Web and the Admin virtual machines.

Step 8 Optionally to 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 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 three web virtual machines on the primary system and one web virtual machine on the high-availability system.

Step 9 Select **Save**.

Setting the Time Zone, Language, and Locale

Procedure

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**.

Creating Administrator Accounts

The system creates a single administrator account as part of the deployment process. 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.

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 for instructions.

Procedure

Step 1 Enter the first and last names of the administrator.

Step 2 Enter the administrator's complete email address and confirm it by entering it again.

Step 3 Select **Next** to create the initial password.

Step 4 Enter a password and confirm it by entering it again.

Step 5 Select **Submit** to sign in to the WebEx Administration site.

Step 6 Sign into the system and add administrators and users. Upon creation of each new administrator or user, the system sends an email to that user, 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.

Testing the System

Most of the system test are accomplished by using the system. Additional tests to validate the system can be performed by using the diagnostic tools provided on the support pages for this product, for example by Using the Meetings Test and Using the System Resources Test.

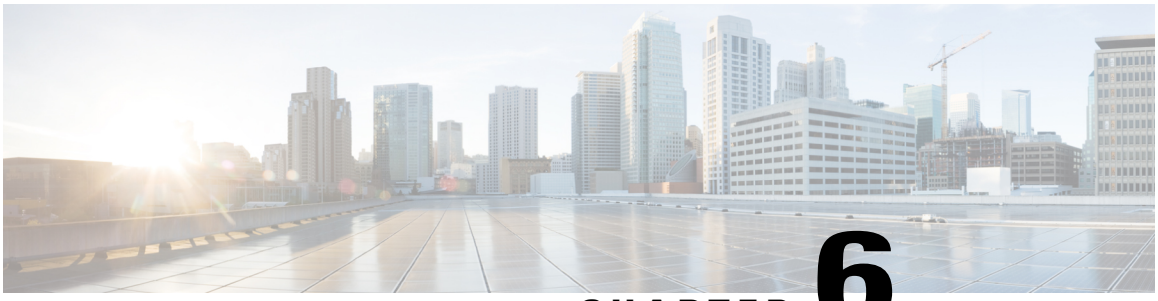
When testing an upgraded system, you can keep the original system until you have finished testing the upgraded system (but because they share some parameters, such as IP addresses, you cannot power on both systems at the same time). Once you are satisfied with the results of the upgraded system tests, 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
- 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
- Checking the System
- Confirming Your Primary System and Your HA System Are at the Same Version
- 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.



CHAPTER 6

Altering the System After Installation

This chapter lists the different system-altering procedures that you may do following the initial deployment of your system.

Adding HA, Updating, Upgrading, or Expanding the System

The following procedures are considered *system-altering*, and requires advance preparation by the administrator:

- Adding or removing a high availability (HA) system
- Updating the system to a later version by using an ISO update file
- Upgrading the system by redeploying the system from a OVA file for the upgrade version
- Expanding the system size from the current size to a larger size

You will put the system in maintenance mode when performing these procedures. Because of this, you may want to schedule several of these procedures together; for example, expanding the system and updating the system during the same maintenance window.

Keep in mind the following constraints:

- If you have already added HA to your system, and would like to expand or upgrade the system, you must to redeploy the HA system following the upgrade.

  System expansion or upgrade requires the deployment of a new primary system, and the transfer of the system data from the original system to the expanded or upgraded system.
- When deploying a new system, you are asked to choose between deploying a primary system or the HA system - you cannot deploy both at once. Therefore, you must first deploy the primary system with the OVA file, then deploy the HA system with the same OVA file used for the primary system.
- If you are planning to add HA to a system and update it (with an ISO update file), we recommend that you add HA before updating it, then update the combined (primary and HA) system. If you update the primary system first, then to add HA, you must deploy then update the HA system (so both the primary and HA systems are at the same version).

- The update procedure updates the entire system, with or without an Internet Reverse Proxy.

Preparing For a System-Altering Procedure

This section describes how to prepare for a major system-altering procedure: expanding your system, adding a high availability system, enabling public access, updating or upgrading your system, and so forth, by creating a backup of your system.

Although you might choose to do so, backups are not required for an expansion or upgrade of your system. Do not take snapshots before or during a system-altering procedure. During an expansion or an upgrade, you deploy a new system and transfer data from your existing system to the new system. If there is a problem with the expansion or upgrade, you can power off the new system and power on the existing system.

Caution Because this procedure requires 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.

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. They must wait until this procedure is completed, then sign in to Cisco WebEx Administration to do their task.

Note Be sure to coordinate with other system administrators before starting a system-altering procedure.

Attention If you do not need to create a backup of your virtual machines, then you do not need to complete this procedure. However, as a best practice, Cisco recommends creating a backup. Backups enable you to revert the system if the procedure is unsuccessful.

Procedure

Step 1 Sign in to the Cisco WebEx Administration site.

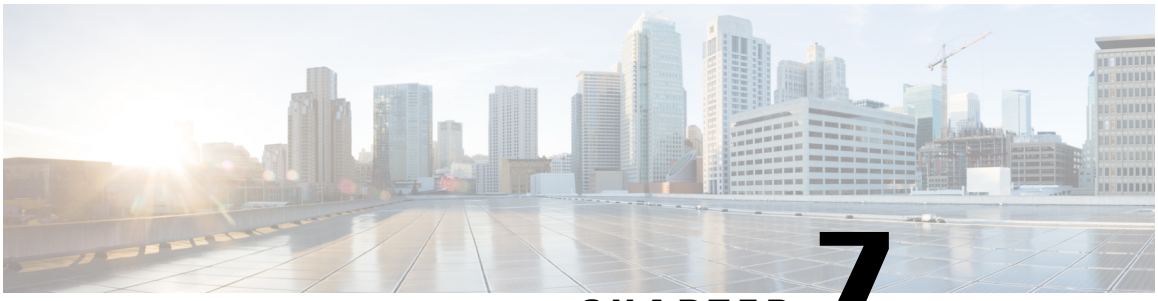
Step 2 Select **Turn On Maintenance Mode**.

Step 3 Use VMware Data Recovery (called VMware vSphere Data Protection starting with vSphere Release 5.1) to create a backup of each of your virtual machines.
A backup will help you revert your virtual machine to its state before the system-altering procedure. For further information, see Creating a Backup by using VMware vCenter. For complete details on this backup, see the *VMware Data Recovery Administration Guide* or the *vSphere Data Protection Administration Guide*.

Note If you are preparing to do an expansion or upgrade, then remove all VMware snapshots on your existing system. This prevents accidental removal of Hard disk 4 's base VMDK file, which may be accessed by the expanded or upgraded system.

Step 4 Sign back in to the Cisco WebEx Administration site, but do not turn off maintenance mode.

Step 5 Continue with the system-altering procedure.



CHAPTER 7

Adding a High Availability System

Considerations When Adding 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.

The HA system has the following constraints:

- 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 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 high-availability 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 will be 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, you must 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.

Note Most of the features on your high-availability system are prohibited. For example you do not have access to upgrade, SNMP configuration, storage access, or email servers on your high-availability system. You can view system properties, but modification is prohibited.

Before You Begin

The following conditions should be met before adding High Availability (HA) to a primary system:

- Verify that the target primary system is deployed.
- Put the primary system is in maintenance mode.
- Create a backup of the primary system. See Creating a Backup by using VMware vCenter.
- Verify that all virtual machines are functioning normally. Determine virtual machine status by viewing the System Monitor as described in About Your Dashboard.
- 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:

Procedure

Step 1 Deploy a parallel system by using Deploying a System Automaticallyor Deploying a System Manually. 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 Deploying a System Automatically process, unless you are deploying a large (2000 concurrent users) system. All large systems require Deploying a 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.

   If the primary system is at a later version than the HA system, then you must either redeploy the HA system by using a 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.

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

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

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

Procedure

Step 1 Notify users and administrators that the system is being put into Maintenance Mode.

Step 2 Sign into the primary system administration site.

Step 3 Select **Turn On Maintenance Mode**.

Step 4 In the System section, select the **View More** link.

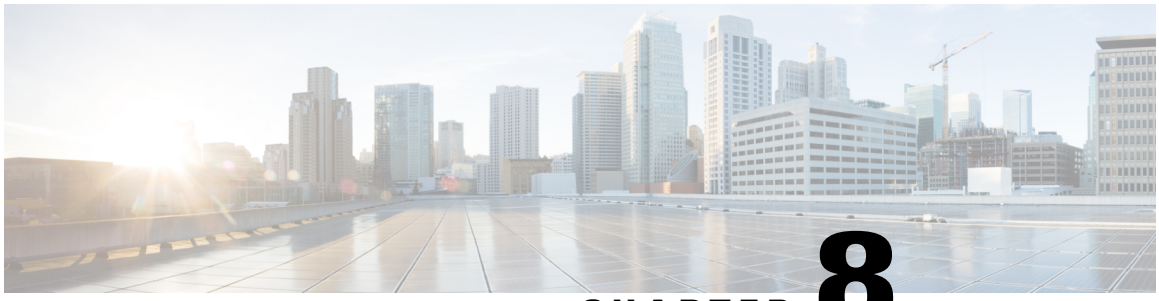
Step 5 Select **Add High Availability System**.

Step 6 Follow the instructions on the **System Properties** page to add the HA system.

Step 7 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 will 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 8 Select **Add**.
Your high-availability system is added and automatically configured to serve as a backup in the event of a primary system failure.

Step 9 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system reboots. You can sign back into the Administration site after the restart is complete.



CHAPTER 8

Expanding Your System to a Larger System Size

Preparing for System Expansion

This section describes the prerequisites a system expansion.

Expansion of a system requires that your existing system licenses be re-hosted on the expanded system. (See Re-hosting Licenses after a Software Upgrade.)

Determining the Size of the New System

Consider the following:

- A budget for any additional hardware
- The anticipated number of concurrent meetings and their average size over the next few months

Obtaining the Information Required For Your System Expansion

- Obtain the OVA file used to install the existing system's version.
- Complete the expansion checklist.

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

Preparing For a System-Altering Procedure

This section describes how to prepare for a major system-altering procedure: expanding your system, adding a high availability system, enabling public access, updating or upgrading your system, and so forth, by creating a backup of your system.

Although you might choose to do so, backups are not required for an expansion or upgrade of your system. Do not take snapshots before or during a system-altering procedure. During an expansion or an upgrade, you deploy a new system and transfer data from your existing system to the new system. If there is a problem with the expansion or upgrade, you can power off the new system and power on the existing system.

Caution Because this procedure requires 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.

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. They must wait until this procedure is completed, then sign in to Cisco WebEx Administration to do their task.

Note Be sure to coordinate with other system administrators before starting a system-altering procedure.

Attention If you do not need to create a backup of your virtual machines, then you do not need to complete this procedure. However, as a best practice, Cisco recommends creating a backup. Backups enable you to revert the system if the procedure is unsuccessful.

Procedure

Step 1 Sign in to the Cisco WebEx Administration site.

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

Step 3 Use VMware Data Recovery (called VMware vSphere Data Protection starting with vSphere Release 5.1) to create a backup of each of your virtual machines.
A backup will help you revert your virtual machine to its state before the system-altering procedure. For further information, see Creating a Backup by using VMware vCenter. For complete details on this backup, see the *VMware Data Recovery Administration Guide* or the *vSphere Data Protection Administration Guide*.

Note If you are preparing to do an expansion or upgrade, then remove all VMware snapshots on your existing system. This prevents accidental removal of Hard disk 4 's base VMDK file, which may be accessed by the expanded or upgraded system.

Step 4 Sign back in to the Cisco WebEx Administration site, but do not turn off maintenance mode.

Step 5 Continue with the system-altering procedure.

Expanding the System by using Automatic Deployment

Before You Begin

Note The system before expansion is referred to as the *original* system. The system following expansion is the *expanded* system.

Schedule a time that is least disruptive to your users to do the system expansion.

Put the primary system in maintenance mode before starting the system expansion.

Caution Because this procedure requires 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.

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.

Considerations Before Expanding the System

- Be sure to remove all VMware snapshots of your original system before starting the expansion procedure.
- You can reuse the same hostnames and IP addresses for the original virtual machines in the expanded system. However, only the original system or the expanded system can be powered on; both systems cannot be powered on and running at the same time.
- If you had HA on the your original system, then after the deployment of the expanded system you must add HA to the expanded system. You cannot reuse the HA system, as it is not retained after an expansion.
- You can keep the original system until you have finished testing the expanded system. Once testing is complete and you are satisfied with the expanded system, you can remove the original (pre-expansion) system.
- The internal virtual machines for the original system and the expanded system must be on the same subnet.
- If you have added public access, the Internet Reverse Proxy virtual machines for the original system and the expanded system must be on the same subnet.
- When you add a new virtual machine to the system, your current security certificate and public and private keys become invalid and require an update, unless you are using a self-signed certificate.

  Certificates include hostnames and URLs. The certificate and keys become invalid because they do not include the new virtual machine. For complete information on certificates and keys, see Managing Certificates.
- Be sure the expanded system can access the disks for the original system Admin virtual machine. You will be copying Hard disk 4 to the expanded system.
- Be sure your expanded system is up and running while removing or deleting your original system. This prevents accidental removal of the Hard disk 4 base VMDK file that might be accessed by the expanded system.

Expanding the System

The overall tasks to expand the system are:

1. Create a backup of the original system.
2. Use the same OVA file you used to deploy your original system and deploy the Admin virtual machine for the new system size.
3. Copy the data from your original system to the Admin virtual machine for the expanded system.
4. Deploy any additional virtual machines for the new system size.
5. Test the expanded system.
6. Re-host the licenses.

Summary of Tasks to Expand the System by using Automatic Deployment

Note This table includes links to other sections of the *Cisco WebEx Meetings Server Administration Guide*. Each of these sections provides detailed information on the specific task. After you complete each task, return to this table to complete the next task. (Use Previous View and Next View in Adobe Acrobat to move easily between this table and the individual task procedures.)

Task	Description	For Details, See
1	Prepare the original system for expansion.	You completed this task earlier in this chapter. It is included in this table for completeness.
2	Prepare for a system-altering procedure.	You completed this task earlier in this chapter. It is included in this table for completeness.
3	Initiate the expansion procedure from the Administration site of the original system.	Expanding the System Size
4	Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the original system.	
5	Using the vSphere client, deploy the Admin virtual machine for the new system size.	Deploying the OVA File From the VMware vSphere Client
6	Attach **Hard disk 4** from the original system's Admin virtual machine to the Admin virtual machine for the expanded system.	Attaching an Existing VMDK File to a New Virtual Machine
7	Power on the Admin virtual machine for the expanded system and write down the deployment URL.	
9	Enter the deployment URL into a web browser and continue the deployment of your expanded system.	
10	Select your preferred language for the deployment of the expanded system.	Selecting Your Language for Setup

Task	Description	For Details, See
11	Confirm the system size. (This system size must be larger than or equal to the original system.)	Confirming the Size of Your System
13	Select **Install a primary system**.	Choosing What System to Install
14	Select an automatic deployment.	Choosing the Type of System Deployment
15	Enter your vCenter credentials so that we may deploy the virtual machines for you.	Providing VMware vCenter Credentials
16	Select the ESXi host, datastore, and virtual machine port group for the media virtual machine.	Choosing vCenter Settings for your Media Virtual Machine
17	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 will look up the IP address for you.)	Entering Networking Information for the Media Virtual Machine
18	If you want public access for your expanded system, then ensure there is a check in the **Create an Internet Reverse Proxy virtual machine** check box. Otherwise, uncheck this check box. **Note** If you have not enabled public access, skip to Task 19.	Adding Public Access
19	If you have added public access, then select the ESXi host, data store, and virtual machine port group for the Internet Reverse Proxy virtual machine.	Choosing vCenter Settings for Internet Reverse Proxy
20	Enter the hostname and networking information for the Internet Reverse Proxy.	Entering Networking Information for the Internet Reverse Proxy
21	Enter the public VIP address for the WebEx site URL. **Note** You can enter the same public VIP address that you use for your original system, or change to a new IP address. If you do change it, then make the necessary updates in the DNS server.	Entering the Public VIP Address
22	Enter the private VIP address for the WebEx Administration URL. **Note** You can enter the same private VIP address that you use for your original system, or change to a new IP address. If you do change it, then make the necessary updates in the DNS server.	Entering the Private VIP Address

Task	Description	For Details, See
23	Enter the WebEx site URL. 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.) **Note** You can enter the same WebEx site URL that you use for your original system or change to a new one. If you do change it, then make the necessary updates in the DNS server. Make sure you retain your original site URL on the DNS server. Redirect your original site URL to the new site URL. If users attempt to use the original URL and you have not redirected it to the new URL, they will not be able to host or join meetings.	Entering the WebEx Site and Administration URLs
24	Enter the WebEx Administration URL for administrators to access Cisco WebEx Administration and internal participants to host or attend meetings (only with a split-horizon DNS). (This URL resolves to the Private VIP address.) **Note** You can enter the same WebEx Administration URL that you use for your original system or change to a new one. If you do change it, then make the necessary updates in the DNS server.	Entering the WebEx Site and Administration URLs
25	Check that you have made all the networking, DNS server, and firewall configuration changes required for your system.	Confirming that the Network is Configured Correctly
26	Once your virtual machines have deployed successfully, then select **Next** to continue to the system check.	Deploying the Virtual Machines
27	Along with the system check, we update the expanded system with any required updates to match the software version of the original system, before expansion. (These updates might take up to an hour.) When complete, the system restarts.	Checking the System
28	Sign in to Cisco WebEx Administration.	
29	Test the expanded system. If the expansion is unsuccessful, then power off the expanded system and power on the original system. Contact Cisco TAC for further assistance.	Testing the System
30	Re-host the licenses as appropriate for the expanded system.	About Licenses Re-hosting Licenses after an Upgrade

Expanding the System by using Manual Deployment

Before You Begin

Note The system before expansion is referred to as the *original* system. The system following expansion is the *expanded* system.

Schedule a time that is least disruptive to your users to do the system expansion.

Put the primary system in maintenance mode before starting the system expansion.

Caution Because this procedure requires 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.

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.

Considerations Before Expanding the System

- Be sure to remove all VMware snapshots of your original system before starting the expansion procedure.
- You can reuse the same hostnames and IP addresses for the original virtual machines in the expanded system. However, only the original system, or the expanded system, can be powered on at any given time. Both systems cannot be powered on and running at the same time.
- If you have already added a HA system to your original system, then following deployment of the expanded system, you must add a new HA system. You cannot reuse the original HA system as it is not retained, following the expansion.
- You might want to keep the original system until you have finished testing the expanded system. Once testing is complete and you are satisfied with the expanded system, you can remove the original (pre-expansion) system.
- The internal virtual machines for the original system and the expanded system must be on the same subnet.
- If you have added public access, then the Internet Reverse Proxy virtual machines for the original system and the expanded system must be on the same subnet.
- When you add a new virtual machine to the system, your current security certificate and public and private keys become invalid and require an update, unless you are using a self-signed certificate.

  Certificates include hostnames and URLs. The certificate and keys become invalid because they do not include the new virtual machine. For complete information on certificates and keys, see Managing Certificates, on page 180.
- Be sure the expanded system can access the disks for the original system's Admin virtual machine. You will be copying over Hard disk 4 to the expanded system.

- Be sure your expanded system is up and running while removing or deleting your original system. This prevents accidental removal of Hard disk 4 's base VMDK file, which may be accessed by the expanded system.

Expanding the System

The overall tasks to expand the system are:

1. Create a backup of your original system.
2. Use the same OVA file you used to deploy your original system and deploy the Admin virtual machine for the new system size.
3. Copy the data from your original system to the Admin virtual machine for the expanded system.
4. Using the OVA, deploy any additional virtual machines for the new system size.
5. Test the expanded system.
6. Re-host the licenses.

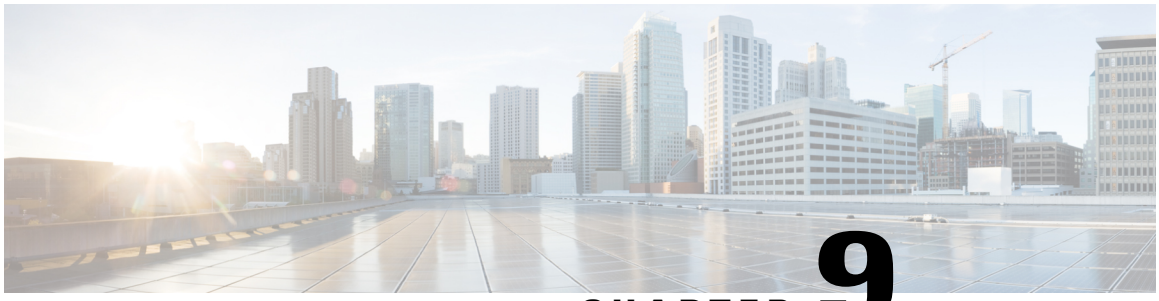
Summary of Tasks to Expand the System Using a Manual Deployment

Note This table includes links to other sections of the *Cisco WebEx Meetings Server Administration Guide*. Each of these sections provides detailed information on the specific task. After you complete each task, return to this table to complete the next task. (Use Previous View and Next View in Adobe Acrobat to move easily between this table and the individual task procedures.)

Task	Description	For Details, See
1	Prepare the original system for expansion.	You completed this task earlier in this chapter. It is included in this table for completeness.
2	Prepare for a system-altering procedure.	You completed this task earlier in this chapter. It is included in this table for completeness.
3	Initiate the expansion procedure from the Administration site of the original system.	Expanding the System Size
4	Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the original system.	
5	Using the vSphere client, deploy the Admin virtual machine for the new system size. **Note** At this time, you may also create the other virtual machines for your system.	Deploying the OVA File From the VMware vSphere Client, on page 16
6	Attach **Hard disk 4** from the original system's Admin virtual machine to the Admin virtual machine for the expanded system.	Attaching an Existing VMDK File to a New Virtual Machine, on page 6

Task	Description	For Details, See
7	Power on the Admin virtual machine for the expanded system and write down the deployment URL. **Note** At this time, you may also power on the other virtual machines in your system. Be sure all the virtual machines power on successfully.	
9	Enter the deployment URL into a web browser and continue the deployment of your expanded system.	
10	Select your preferred language for the deployment of the expanded system.	Selecting Your Language for Setup, on page 28
11	Confirm the system size. (This system size must be larger than or equal to the original system.)	Confirming the Size of Your System, on page 29
12	Select **Install a primary system**.	Choosing What System to Install, on page 29
13	Select a manual deployment.	Choosing the Type of System Deployment, on page 30
14	If you want public access for your expanded system, then ensure there is a check in the **Create an Internet Reverse Proxy virtual machine** check box. Otherwise, uncheck this check box.	Adding Public Access, on page 31
15	Enter the public VIP address for the WebEx site URL. **Note** You may enter the same public VIP address that you use for your original system, or change to a new IP address. If you do change it, then make the necessary updates in the DNS server.	Entering the Public VIP Address, on page 33
16	Enter the private VIP address for the WebEx Administration URL. **Note** You may enter the same private VIP address that you use for your original system, or change to a new IP address. If you do change it, then make the necessary updates in the DNS server.	Entering the Private VIP Address, on page 34

Task	Description	For Details, See
17	Enter the WebEx site URL. 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.) **Note** You may enter the same WebEx site URL that you use for your original system, or change to a new one. If you do change it, then make the necessary updates in the DNS server. Make sure you retain your original site URL on the DNS server. Redirect your original site URL to the new site URL. If users attempt to use the original URL and you have not redirected it to the new URL, they will not be able to host or join meetings.	Entering the WebEx Site and Administration URLs, on page 35
18	Enter the WebEx Administration URL for administrators to access Cisco WebEx Administration and internal participants to host or attend meetings (only with a split-horizon DNS). (This URL resolves to the Private VIP address.) **Note** You may enter the same WebEx Administration URL that you use for your original system, or change to a new one. If you do change it, then make the necessary updates in the DNS server.	Entering the WebEx Site and Administration URLs, on page 35
19	Check that you have made all the networking, DNS server, and firewall configuration changes required for your system.	Confirming that the Network is Configured Correctly, on page 36
20	Once your virtual machines have deployed successfully, then select **Next** to continue to the system check.	Deploying Virtual Machines
21	Along with the system check, we update the expanded system with any required updates to match the software version of the original system, before expansion. (These updates may take up to an hour.) When complete, the system restarts.	Checking the System
22	Sign in to Cisco WebEx Administration.	
23	Test the expanded system. If the expansion is unsuccessful, then power off the expanded system and power on the original system. Contact Cisco TAC for further assistance.	Testing the System
24	Re-host the licenses as appropriate for the expanded system.	About Licenses Re-hosting Licenses after an Upgrade



CHAPTER 9

Updating the System

Preparing to Update an Existing System

The complete update procedure, including backing up your virtual machines, might take up to an hour depending on the system size and the size of the database.

Before You Begin

Verify that the intent is to update the original system (not upgrade the system). An *update* is defined as overwriting an existing (original) system to take advantage of modifications that we made to improve the system. For example, you might update a system from version 1.5 to 1.5MR. An *upgrade* is defined as deploying a replacement of the original system to take advantage of major modifications. For example replacing a system currently running version 1.0 to run version 2.0 that includes support for a new operating system. If you are upgrading a system, use the Updating the System procedure. Check the release notes for the correct procedure to use. In both cases, all of the data from the original system is transferred to the updated or upgraded system.

Get the latest update file from Cisco at Cisco Software Download (external)

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) or version 1.5 (Build 1.5.1.6.A) before applying 1.5 MR2. Check the release notes for the correct version to use.

Because the update procedure requires exclusive access to the system, notify users that they cannot access the system for meetings. Be sure to schedule the update during a time that will be least disruptive to your users.

Notify other system administrators that they should not access the system during this procedure. If they do so, their changes are not saved and the result can be unpredictable; they must wait until this procedure is completed before signing in to the Cisco WebEx Administration site.

Procedure

Step 1 Sign in to the Cisco WebEx Administration site.

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

Step 3 Select the **System** tab, then select **Upgrade**.

Step 4 Select **update**.

Step 5 In the VMware vSphere client, select **Power** > **Shut Down Guest** on each of the virtual machines in your system.
For complete details on using vSphere, see the VMware ESXi and vCenter Server documentation.

Step 6 Once the virtual machines are powered off, use VMware Data Recovery (or VMware vSphere Data Protection available with vSphere Release 5.1) to create a backup of each of your virtual machines.
A backup returns your virtual machine to its state before the update if necessary. For further information, see Creating a Backup by using VMware vCenter. For complete details on this backup, see the *VMware Data Recovery Administration Guide* or the *vSphere Data Protection Administration Guide*.

Note You can also take a snapshot, but you should delete all snapshots in approximately 24 hours, or you might experience data performance issues. For more information, see Taking a Snapshot by using VMware vCenter.

Caution Create backups of all your virtual machines, because the update procedure makes changes to your existing virtual machines, and once the update procedure begins you will not be able to undo the update.

Step 7 In the VMware vSphere client, power on each of the virtual machines in your system.

Step 8 Log in to the Cisco WebEx Administration site, but do not turn off maintenance mode.

Step 9 Select the **System** tab, then select **Upgrade**.

Step 10 Select **update** to return to the **Update System** page.

What to Do Next

Go to Connecting to an ISO Image from the CD/DVD Drive.

Connecting to an ISO Image from the CD/DVD Drive

For the fastest update, Cisco recommends that you mount the ISO image in the vCenter datatstore. However, if you place it in a local disk on 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:

Before You Begin

Get the desired ISO image from Cisco:

Download Software

Verify that you have the appropriate permissions.

Procedure

Step 1 Select the ESXi host for the Admin virtual machine. Select the **Summary** tab and double-click the **datastore1** name under **Storage**.

Step 2 On the **Datastore and Datastore clusters** window, select **Browse this datastore**.

Step 3 Select the green up arrow icon (Upload file) and load the update ISO file.

Step 4 Select the Admin virtual machine in the VMware vCenter inventory.

Step 5 Select the **CD/DVD** icon for the Admin virtual machine.

Step 6 Select **CD/DVD drive 1** > **Connect to ISO image** on a local disk or on a datastore.

Step 7 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**.

Continuing the Update Procedure

Before You Begin

You have completed:

- Preparing to Update an Existing System, on page 85
- Connecting to an ISO Image from the CD/DVD Drive, on page 86

Procedure

Step 1 After connecting the update ISO image, select **Continue** on the **Update System** page in the Cisco WebEx Administration site.

Step 2 Check the **I have connected to the ISO file and am ready to proceed** check box.

Step 3 Select **Continue**.

Caution Once you select **Continue**, you will not be able to stop the update procedure. If an issue arises during the update procedure, and it does not complete successfully, then you must use your backups to restore the system.

The update procedure may take up to an hour. Do not close the browser window, as you will be unable to return to this page.

Once the update completes, a new page is displayed, confirming the success of the update.

Note There is an intermittent issue where the update completes successfully, but you do not see text stating **System Updated** and a **Restart** button. If the update does not complete, and it has been longer than an hour, then you can attempt to turn off maintenance mode. If you cannot turn off maintenance mode, then the update is still in progress. Once the update is finished, reboot all virtual machines from vCenter. Wait for the virtual machines to come online and verify the system version on the dashboard.

Step 4 Select **Restart** to restart the system.
This page has a default timeout value of 90 minutes. Be sure you restart the system within this time period, or change the default timeout to a longer period of time.

What to Do Next

Continue with Completing the Update, on page 88.

Completing the Update

Before You Begin

This is a continuation from Continuing the Update Procedure, on page 87.

Procedure

Step 1 Once the update has completed successfully, select **Restart**.
Once the system has restarted, the Cisco WebEx Administration site sign in page is displayed.

Step 2 Sign in to Cisco WebEx Administration. The updated version is displayed on the dashboard.

Step 3 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 4 After completing any post-update configuration, select **Turn Off Maintenance Mode**.

Step 5 Test and check the system. You can accomplish these tests and validate your system by using two diagnostic tools provided on the support pages for this product: the Meetings Test and the System Resources test.

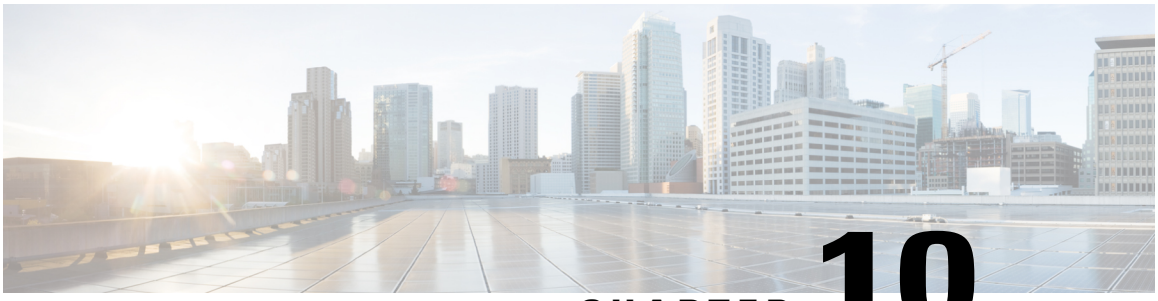
- Add, edit, activate, an deactivate users.
- Schedule and hold a meeting.
- Reschedule an existing meeting.
- Delete a series of meetings or a future meeting.
- Open a meeting attachment.
- Play a meeting recording.

What to Do Next

- If you find issues, then use VMware Data Recovery (vSphere Data Protection) or your system snapshots to revert to your previous version. Check the ISO network connection and ensure there are no issues.
- If the update is successful, use the updated system for awhile. Once you are satisfied, be sure to delete the virtual machine backups or snapshots created before the update.

PART II

Cisco WebEx Meetings Server Configuration Guide



CHAPTER 10

Using Your Dashboard

This module describes the features on your Cisco WebEx Server dashboard and how to use them.

About Your Dashboard

This section describes the features on your dashboard and how to use them. The dashboard is the home page of the administration site and provides several displays and graphs of key monitoring features.

The dashboard includes the following sections:

- System messages—One or more system messages appear in a bar at the top of the page. Three types of system messages might appear at the top of the page:
  - Warning—Indicated by a red bar. Warning messages indicate the system is in a special state. For example, maintenance mode.
  - Alert—Indicated by a yellow bar. Alerts indicate time-sensitive issues such as license expiration dates.
  - Information—Indicated by a blue bar. Informational messages that notify you of important information. For example, these messages might inform you that a first-time tutorial is available or display the status of a disaster recovery procedure.
- System Monitor—This section displays the system status and time stamp and includes the following subsections:
  - Status—Indicates overall system status, Good or Down.
  - Meetings in Progress—Select to open the **Meeting Trend** page that displays the total number of participants and meetings on your system over a specified period of time. You can select the following:

- 1 day—By default, data for the previous day is displayed. Use the date selector to select a single day during the preceding six-month period.
- 1 week—By default, data for the previous week is displayed. Use the date selector to select a single week during the preceding six-month period.
- 1 month—By default, data for the previous month is displayed. Use the date selector to select a single month during the preceding six-month period.
- 6 months—The previous six-month period is displayed. The date selector disappears since you have selected the maximum period.
- Time of day—To view meetings that occurred during a specific time of day, mouse over the graph and select the desired time.

◦ Usage—Displays the current participant count both as a percentage of total resources and the number of participants. You can select the Usage graph to open the **Meeting Trend** page. You can select a point on the Participants or Meetings graphs to show the Meeting list for the time slot specified on the graph.

◦ Alarms—Displays the alarm threshold settings you have configured. By default, alarm thresholds are displayed as a percentage. Select **Number #** to change the alarm information to numerical data. Alarm thresholds are displayed in the System Monitor section in graphical form and on the **Alarms** page in numerical form. You can select the graphs in the System Monitor section to view the Resource History page for the alarms that you have configured. See Viewing Your Resource History for more information.

You can configure alarms for the following:

◦ Meetings In Progress—Indicates when current meetings are experiencing issues.

◦ Usage—The total number of users currently using the system.

◦ CPU—Shows the value of the one virtual machine in the system with the highest CPU usage out of all virtual machines in the system.

◦ Memory—Shows the value for the one virtual machine in the system with the highest memory usage.

◦ Network—Total system bandwidth used.

◦ Storage—Recording and database backup storage space used.

Note The storage alarm appears if you have configured a storage server. See Configuring a Storage Server for more information.

◦ Process status—Displays the performance of several key system features. The status of each feature is described as Good, Fair, or Down.

◦ Video

◦ Audio

◦ Web Sharing

◦ Recording (appears if you have configured a storage server)

◦ Start/Join Meetings

For video, audio, and web sharing, monitoring is performed on each client-server connection based on a threshold defined for the corresponding parameters used to determine status of a meeting. An alert is sent to from the meeting monitoring agent to a meeting monitoring receiver if one of corresponding parameters from a client connection goes beyond the threshold. Most of the settings are measured in milliseconds.

For web sharing, additional criteria is added to determining meeting status. This criteria includes a minimum of three alerts from the same connection within three minutes with one third or more of the total number of participants experiencing the same issues.

For telephony issues, the meeting status is based on the severity of the error.

The guidelines for process status are as follows:

- Good—All services on your system are operating.
- Fair—Your system is operating at reduced capacity. Periodically recheck your system. If it is still displaying a status of fair after 48 hours, contact the Cisco TAC for assistance. See Using the Support Features for more information.
- Down—All services on your system are not running. Contact the Cisco TAC for assistance. See Using the Support Features for more information.

- System Backup—Displays the time and date that the last backup was taken. It also notifies you if the backup failed and the date of the first backup attempt if one has not been created yet.

Note Only appears if you have configured a storage server.

- System—Displays the maximum number of users on your system, the version number, product URL, and the number of user licenses. If you are using a free-trial edition of Cisco WebEx Server, this section also indicates how many days are remaining in your trial period when there are 30 days or less. Select **View More** to go to Configuring Your System.
- Settings—Displays your current system settings including the maximum number of participants allowed in each meeting, audio type, whether or not video and mobile features are enabled, and Single Sign-On (SSO) status. Select **View More** to go to Configuring Settings, on page 143.

Viewing and Editing Alarms

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Dashboard** > **Alarms**.
The **Alarms** page appears displaying the current alarm thresholds.

Step 3 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	Displays the meetings in progress 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	Displays the current system 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**.
CPU	Displays the current CPU threshold in MHz. • If set to **Percentage %**, move the selector bar to set from 2 to 99 percent. • If set to **Number #**, enter number of MHz. **Default**: Not selected. Interval is **one hour**.
Memory	Displays the current memory threshold in GB. • If set to **Percentage %**, move the selector bar to set from 2 to 99 percent. • If set to **Number #**, enter the number of GB **Default**: Not selected. Interval is **one hour**. **Note** The Memory gauge shows an approximation of the memory used by the one virtual machine that has the highest memory load. When the gauge is in the red zone for a short periods of time, it is not an indication that the system is in a critical state or that it needs immediate attention. High memory use might be an indicator that there are other system performance issues that should be addressed. If memory usage exceeds 90 percent for a long period of time, we recommend that you review the vCenter memory usage and CPU statistics. If those statistics are found to be out-of-range, consider modifying your system to reduce the load.
Network	Displays the current network bandwidth threshold in Mbps. • If set to **Percentage %**, move the selector bar to set from 2 to 99 percent. • If set to **Number #**, enter the number of Mbps. **Default**: Not selected. Interval is **one hour**.

Option	Description
Storage	Displays the current 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 user system (50 user, 250 user, 800 user, or 2000 user system), 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. See Recommended Storage for Backup Files for details. • If set to **Percentage %**, move the selector bar to set from 2 to 99 percent. • If set to **Number #**, enter the number of GB. **Default**: Not selected. Interval is **one hour**. **Note** This section only appears if you have configured a storage server. See Configuring a Storage Server, on page 131 for more information.

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. The interval for each alarm can be:

- One hour
- Six hours
- 12 hours
- 24 hours

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

Viewing Your Resource History

Your resource history contains detailed graphs for each alarm configured on your system. The current values for meetings, participants, and storage are shown in the right-side panels. See Viewing and Editing Alarms for more information on the alarms you can configure.

You can view your resource history by selecting the alarm graphs on the **System Monitor** window. See About Your Dashboard for more information. For example, select the CPU graph and the **Resource History** window appears.

You can select a network graph on the **Resource History** page to open a **Network History** graph. Your **Network History** graphs display the network bandwidth usage for several categories. You can also select any of the following categories to see their bandwidth consumption displayed on the graph:

- Voice connection using computer
- Teleconference
- Web Sharing

- Video

If you have a storage server configured, you can select the Storage box in the right column of your **Resource History** or **Network History** page to see a **Storage History** graph. This graph shows how much space has been used on your storage server.

Viewing Meeting Trends

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Dashboard**.
When Dashboard page is reloaded, Meeting Trend shows the meeting data for today (from 12:00 am to 12:00 am the next day). Meeting List lists meeting details.

Step 3 Use the **From** and **To** fields to set the time period 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 slot specified on the graph. To view meetings that occurred during a specific time of day, mouse over the graph and select the desired time. The Meetings list shows the total number of meetings that occurred during the selected time period, the meeting topics, hosts, numbers of participants, and the state of the meeting. 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.

Note
- 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.

The Meeting Trend graph is updated with your new settings.

Note The display of future meetings on Meeting Trend might be delayed up to 24 hours.

Step 4 (Optional) Select the date using the calendar tool under the graph. Check the **Show future meetings** checkbox to display future meetings on your graph.
The Meeting Trend graph is updated with your new settings. You can mouse over Meeting Trend to display information for a particular time. For example, [2 pm, 3] means there were 3 meetings in the time period of 2:00 pm to 3:00 pm.

There is an icon between the Time range selector and the Meeting Trend graph to show or hide the Meeting data list. These data points are the same as shown on the graph. They are made accessible primarily for the benefit of users with a keyboard and screen reader.

For 24-hour time range, the data for passed and in-progress meetings are in 5 minute intervals. Future meetings are in one-hour intervals. When the time range is greater than 24 hours and less than one week, all data points

are in one hour intervals. When the time range is larger than 1 week, all data points are in one day intervals. Past and in-progress meeting data are shown in green. Future meetings are shown in orange.

Step 5 (Optional) Select the **Participants** or **Meetings** graph for meeting information including the following:

- Status
- Meeting Topic
- Host
- Participant
- State

Enter search terms in the field above the table to filter the meeting list. The meeting list can be sorted by selecting the header of the key column.

Step 6 The current system status is displayed in the right column of the page.
System status can be

- Good—All services on your system are operating.
- Down—All services on your system are not running. Contact the Cisco TAC for assistance. See Using the Support Features for more information.

Step 7 Select the alarm status box in the right column to see the **Resource History** for the alarms.

Using the Meetings in Progress Chart to Address Meeting Issues

When you receive an email indicating that there are issues with meetings, perform the following steps to determine the cause.

Procedure

Step 1 Select the link in the meeting issue email that you received.

Step 2 Sign in to the Administration site.

Step 3 On the Dashboard, select the **Meetings in Progress** chart.
The **Meeting Trend** page displays.

Step 4 Select the far right edge of the graph to open a detailed table showing the status of each current meeting. You can use the detailed information presented in the table to help determine the cause of the issue described in the email you received. Select the Meeting Trend at the data point corresponding to the time when the system reported meeting issues. For example, assume that at 10:00 a.m. an email was sent reporting meeting issues. Go to the dashboard and select the 10:00 a.m. data point on Meeting Trend. The meeting list shows the details for those meetings. Meetings with performance issues are displayed in the Status column in red or yellow.

About Maintenance Mode

Many configuration changes require that you put your system into maintenance mode. Maintenance mode shuts down conferencing activity so you need to schedule your maintenance windows to ensure minimal down time for your users. The Maintenance Mode button is present on all pages in the administration site.

After you determine when you want to put your system in maintenance mode, select the **Email Users** feature to notify your users in advance that they will be unable to join or host meetings during the maintenance window. See Emailing Users for more information.

Putting your system in maintenance mode does the following:

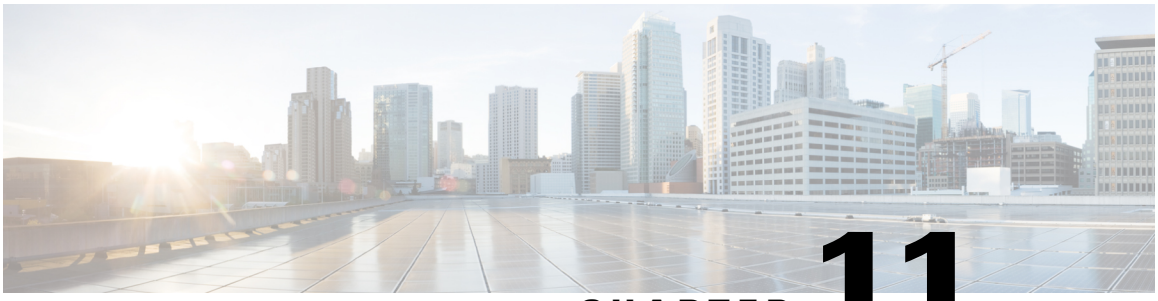
- Closes all current meetings.
- Disconnects all users from those meetings.
- Prevents users from signing in from web pages, the Outlook plug-in, and mobile applications. Emails are automatically sent when the system is taken out of maintenance mode.

You must put your system in maintenance mode to perform the following tasks:

- Adding and removing high availability systems. See Configuring a High Availability System, on page 122 for more information.
- Adding and removing public access by deploying or removing an Internet Reverse Proxy. See Adding Public Access to Your System and Removing Public Access, on page 127 for more information.
- Change the system default language. See Configuring Your Company Information, on page 144 for more information.
- Changing your host or admin account URLs. See Changing Your Site Settings, on page 128 for more information.
- Changing your mail server. See Configuring an eMail (SMTP) Server for more information.
- Changing your system language and locale. See Configuring Your Company Information, on page 144 for more information.
- Changing your virtual IP address. See Changing Your Virtual IP Address, on page 125 for more information.
- Configuring and changing audio settings. See About Configuring Your Audio Settings, on page 148 for more information.
- Configuring and changing branding settings. See Configuring Your Branding Settings, on page 145 for more information.
- Configuring and changing quality of service settings. See Configuring Quality of Service (QoS), on page 154 for more information.
- Configuring certificates. See Managing Certificates, on page 180 for more information.
- Configuring disaster recovery settings. See Using the Disaster Recovery Feature, on page 133 for more information.
- Configuring FIPS-compatible encryption. See Enabling FIPS Compliant Encryption, on page 194 for more information.

- Configuring and changing SNMP settings. See Configuring Your SNMP Settings, on page 135 for more information.
- Configuring storage servers. See Configuring a Storage Server, on page 131 for more information.
- Configuring virtual machine security. See Configuring Virtual Machine Security, on page 193 for more information.
- Expanding system size. See Expanding the System Size, on page 127 for more information.
- Performing minor updates, major upgrades, and expanding your system. See Updating the System, on page 85 for more information.
- Updating shared keys. See Managing Certificates, on page 180 for more information.
- Using the System Resource test. See Using the System Resource Test for more information.

Each of your virtual machines has a console window that indicates when it is in maintenance mode. You can open the console windows in your 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-, 250-, 800-, or 2,000-user system), and current system status including whether maintenance mode is on or off and the time and date of the status change. The time displayed is configured in your Company Info settings. See Configuring Your Company Information, on page 144 for more information.



CHAPTER 11

Managing Users

This section describes how to manage users on your system.

About Managing Users

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

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.

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 Deactivating Users 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 Configuring Your General Password Settings for more information.

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, but the field values can be empty If a field is missing, an error message appears. For example,
  Incorrect file format. Custom10 is required.
- 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 should be unique. Do not use predefined field names (USERID, ACTIVE, FIRSTNAME, LASTNAME, EMAIL, LANGUAGE, HOSTPRIVILEGE, TIMEZONE, and so forth) for tracking codes.

The table lists the required field names, descriptions, and the acceptable values.

Field Name	Description	Size and Type of Value
USERID	User ID. **Note** This field is automatically generated by the system and must be left blank when importing a CSV file.	1 to 19 alphanumeric characters

Field Name	Description	Size and Type of Value
ACTIVE	Indicate whether or not this user is active.	Y or N
FIRSTNAME	User's first name.	1 to 32 character string
LASTNAME	User's last name.	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 for more information.	1 to 64 character string
HOSTPRIVILEGE	Host privileges.	ADMN or HOST
TIMEZONE	Time zone where the user is located. See CSV File Field Values for more information.	Time zone name
DIVISION	User's division. For tracking code group 1. This field is configurable on the Tracking Codes page. See Configuring Tracking Codes for more information.	1 to 128 character string
DEPARTMENT	User's department. For tracking code group 2. This field is configurable on the Tracking Codes page. See Configuring Tracking Codes for more information.	1 to 128 character string
PROJECT	User's project. For tracking code group 3. This field is configurable on the Tracking Codes page. See Configuring Tracking Codes for more information.	1 to 128 character string
OTHER	Other information. For tracking code group 4. This field is configurable on the Tracking Codes page. See Configuring Tracking Codes for more information.	1 to 128 character string
CUSTOM5	Custom field 5. See Configuring Tracking Codes for more information.	1 to 128 character string
CUSTOM6	Custom field 6.	1 to 128 character string
CUSTOM7	Custom field 7.	1 to 128 character string

Field Name	Description	Size and Type of Value
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

The following topics provide additional information:

- Exporting User Accounts to a CSV File
- Importing User Accounts from a CSV File
- Transferring User Accounts Between Systems by using a CSV File
- Configuring Tracking Codes

CSV File Field Values

Language Field Values

Following are examples of the country code values that you can use in the a CSV file.

Field Value	Language
en-us	U.S. English
zh-cn	Simplified Chinese
zh-tw	Traditional Chinese
jp	Japanese
ko	Korean
fr	French
de	German
it	Italian
es-me	Castilian Spanish
es	Latin American Spanish
nl	Dutch
pt-br	Portuguese
ru	Russian

Time Zone Field Values

Following are the time zone (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
Bogota	-5 hr
New York	-5 hr
Indiana	-5 hr
Caracas	-4.5 hr
Halifax	-4 hr
Newfoundland	-3.5 hr
Brasilia	-3 hr
Buenos Aires	-3 hr
Recife	-3 hr

Field Value	GMT
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
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

Field Value	GMT
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
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

Field Value	GMT
Vladivostok	11 hr
Solomon Islands	11 hr
Wellington	12 hr
Fiji	12 hr

Exporting User Accounts to a CSV File

To export a CSV file:

Procedure

Step 1 Sign in to the Administration site.

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.

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 User Accounts to a CSV File and Creating Comma- or Tab-Delimited Files for more information.

Procedure

Step 1 Sign in to the system Administration site.

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 that 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:

Procedure

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.

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 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 that 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

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Users** > **Add User**.

Step 3 Select your account type (**Host** or **Administrator**).

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

Step 5 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 site.

Note The Create Password link expires after 72 hours.

The user is added to your system.

Editing Users

You can change user information and activate or deactivate user accounts with the edit user feature.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Users**.
The list of users appears. The default number of users shown on each page is 50. You can optionally select the **Users Per Page** drop-down menu and change the setting to **50** or **100**.

Step 3 Select a user to edit.

Step 4 Make changes to the editable fields. Fields marked with an asterisk are required.

Step 5 Optionally select the **Force this user to change password on next login** check box.

Note If SSO is enabled on your system, this feature does not apply to host accounts.

Step 6 Optionally activate or deactivate an account:

- Select **Activate** to reactivate an inactive account.
- Select **Deactivate** to deactivate an account.

Note Activating or deactivating an account does not save any other changes you have made to the account. You must select **Save** to save your changes.

Step 7 Select **Save**. This saves your changes without altering the status of the account.

Activating Users

After you add or import host and administrator accounts, they are active by default. Use this feature to reactivate inactive users.

Alternatively you can activate an account on the **Edit User** page. See Editing Users, on page 110 for more information.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Users**.

Step 3 Select the check boxes for any inactive users you want to activate.

Step 4 Select **Actions** > **Activate**.
The selected accounts are activated and the status for each account should now be "Active."

Deactivating Users

You can deactivate host and administrator accounts. Deactivating an account prevents the owner of the accounts from doing the following:

- Signing in from web pages, the Outlook plugin, and mobile applications
- Hosting or attending meetings
- Managing the system (if the user was an administrator)

Alternatively you can deactivate an account on the **Edit User** page. See Editing Users, on page 110 for more information.

Note Administrators cannot deactivate their own accounts.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Users**.

Step 3 Select the check boxes for any active users you want to deactivate.

Step 4 Select **Actions** > **Deactivate** and confirm by selecting **OK**.
The selected accounts are deactivated and the status for each account should now be "Inactive."

Configuring Tracking Codes

You can configure tracking codes to track host usage in specified groups. For example, you can configure tracking codes for projects or departments. The tracking codes you configure appear as options when you add or edit users.

You must configure the following for each tracking code:

- Tracking code group–Configure your tracking code groups. Tracking code groups are used when you add and edit users. The defaults are Division, Department, Project, Other, and Custom5 through Custom10.

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

- Input mode–Select **Text field** or **Dropdown menu**.
- Usage–Select **Not used**, **Optional**, or **Required.**

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Users** > **Tracking Codes**.

Step 3 Optionally enter the name of each tracking group you want to configure in the **Tracking code group** column. You do not need to change any of the fields if you intend to use the default values.

Step 4 Select **Text Input** or **Dropdown Menu** in the **Input mode** column for each tracking code.
If you select **Text Input** then you enter your tracking code name in a text field. If you select **Dropdown menu** an **Edit list** link appears next to your **Input mode** field. Select the **Edit list** link to configure the values in the dropdown menu for that tracking code. See Editing Tracking Codes, on page 112 for more information.

Note If you select **Dropdown menu** for one of your tracking code groups, you must select **Edit list** and enter one or more options for the associated dropdown menu.

Step 5 Select **Not used**, **Optional**, or **Required** in the **Usage** column for each tracking code.

Note You should only change the Usage to **Required** or **Optional** after you have configured a dropdown menu list. An error message appears if you attempt to configure a usage setting other than **Not used** if you have not configured the Tracking code group and Input mode first.

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

Editing Tracking Codes

By default, tracking codes are displayed as text boxes. If you want to display tracking code options in a dropdown menu you must configure a list of options. After you select **Dropdown menu** from the **Input mode** dropdown menu, an **Edit list** link appears.

Before You Begin

To edit your tracking codes you must select **Users** > **Tracking Codes** and select **Dropdown menu** for your **Input mode**.

Procedure

Step 1 Select the **Edit list** link.
The **Edit Tracking Code List** dialog box appears.

Step 2 Configure the fields in the **Edit Tracking Codes List** dialog box.

a) Select **Show active codes only** to display only active tracking codes when you open this dialog box. Deselect this option to show all tracking codes. Note that you cannot select this option the first time you configure tracking codes for each **Input mode**.
b) Select **Go to first empty tracking code** to go to the first page with empty code fields.
c) **Active** is selected by default. You can uncheck **Active** to make a tracking code inactive. Inactive tracking codes do not appear on this tracking code group's dropdown menu. Check **Active** to activate an inactive tracking code.
d) Enter the menu item name in the **Code** text box. Limit: 128 characters.
e) Select the **Default** radio button to make this menu item the default selection for the dropdown menu.
f) Select **Add 20 more lines** to add 20 more configurable tracking code lines. Navigation links (**Next**, **Previous**, and page numbers) are added if you have more than 20 lines to display. Limit: 500 lines (25 pages).
g) Select a **Sort** radio button to set the sorting method (**Do not sort**, **Sort ascending**, **Sort descending**) for the tracking codes. Note that **Sort** only works for the current page.

Step 3 Select **Update** to save your settings.
Your settings are saved and the **Edit Tracking Code List** page closes.

Configuring Directory Integration

Directory integration enables your system to populate and synchronize your Cisco WebEx Meetings Server user database with the Cisco Unified Communications Manager (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.

Before You Begin

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

- We recommend that you schedule synchronization during off-peak hours or on weekends to minimize the impact on your users.
- Make sure you have a supported version of Cisco Unified Communications Manager (CUCM). Refer to the Cisco WebEx Meetings Server System Requirements for more information.
- Obtain CUCM administrative user credentials (required to add a CUCM server for directory integration).
- You must configure AXL and LDAP directory service on CUCM before you can use the directory integration feature. 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 and Using CUCM to Configure LDAP Integration and Authentication. Refer to the CUCM documentation 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 sign in and host meetings (all users can join as a guest). If necessary, create CUCM groups or filters which consist of only the users you want to import from CUCM.

Note All active CUCM users are imported into Cisco WebEx Meetings Server during your first directory synchronization. Inactive CUCM users are not imported. Only active new and modified users are imported during any subsequent synchronization. You must deactivate user accounts in Cisco WebEx Meetings Server 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 Configuring Your System for more information on license consumption.

- Users with no 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 user's password is no more than 64 characters. Users with passwords greater than 64 characters will not be able to sign in to Cisco WebEx.

Procedure

Step 1 Sign in to your Cisco WebEx Meetings Server Administration site.

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

Note 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 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 If you have already configured your CUCM settings, this step is not necessary and you can proceed to the next step. 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 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.
  Note You cannot cancel synchronization after it starts.
- Select the **Next synchronization** check box and enter a date, time, and repeat mechanism to schedule future synchronizations.

If you select **Synchronize Now**, your system immediately performs a synchronization. The time this process takes varies depending on the number of users being synchronized. You receive an email when the synchronization is complete. The other administrators on your system are not notified after a **Synchronize Now**. 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 6 Select **Save** if you have configured or changed your synchronization schedule or your administrator notification settings.

Step 7 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 8 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 9 (Optional) Select or deselect **Notify administrators when synchronization completes** and then select **Save**. This option is selected by default and only informs administrators after scheduled synchronizations.

Step 10 Select **Enable LDAP Authentication**.

Note If your system is configured to use SSO, you must first disable SSO. See Disabling SSO 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. Administrators, however, still use their Cisco WebEx Meetings Server credentials to sign in to the Administration site.

Step 11 Make sure that your users can sign into the system with their AD domain credentials.

Step 12 If you put your system in maintenance mode select **Turn Off Maintenance Mode**.

Step 13 (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 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's 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.

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 113 for more information.

Procedure

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**.

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 118 for more information.

Using CUCM to Configure LDAP Integration and Authentication

Use CUCM to configure LDAP integration and authentication.

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 for more information.

Procedure

Step 1 Sign in to your CUCM account.

Step 2 Select **Cisco Unified CM Administration** from the top right dropdown 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 **sAM Account Name** for the LDAP Attribute for User ID, and select **Save**.

Step 5 Select the checkbox 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 for more information.

Emailing Users

Use this tool to send email to your users.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Users** > **Email Users**.

Step 3 Enter a target user email address or an email alias in the **To** field.

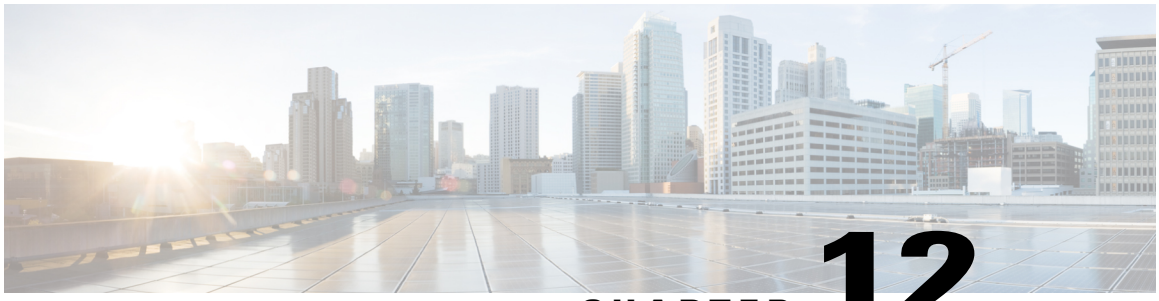
Step 4 Optionally enter email addresses in the **BCC** field.

Step 5 Enter your subject in the **Subject** field.

Step 6 Enter your message in the **Message** field.

Step 7 Select **Send**.
Your email is sent.

Note 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.



CHAPTER 12

Configuring Your System

This module describes how to use the administrator pages to configure your system.

Configuring System Properties

Configure your system properties by selecting System and View More in the System section.

Changing Your Virtual Machine Settings

Use this feature to change your virtual machine settings.

Note Do not use VMware vCenter to edit your virtual machine settings.

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 To modify the settings of a virtual machine select the virtual machine name link in the Primary System or High Availability System section.

Step 5 You can modify the following virtual machine settings:

- Fully Qualified Domain Name—Your system's FQDN.
- Virtual Machine—Your virtual machine IP address.

- Primary DNS Server
- Secondary DNS Server
- Subnet Mask/Prefix
- Gateway

Note During deployment, you can only configure IPv4 settings. After deployment, you can configure IPv6 settings on this page if you have an IPv6 connection between you Internet Reverse Proxy in the DMZ network and your internal virtual machines.

Step 6 Select **Save**.
Your changes are saved and the virtual machine is rebooted.

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

What to Do Next

If you make changes to any of your virtual machines, you must obtain new certificates for each virtual machine on your system unless you are using wildcard certificates for systems in the same domain. For more information, see Managing Certificates, on page 180.

Configuring a High Availability System

A high availability system is a redundant system that provides backup in the event of a primary system failure.

Linking a High Availability System to a Primary System

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

Before You Begin

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

Procedure

Step 1 Notify users and administrators that the system is being put into Maintenance Mode.
Step 2 Sign into the primary system administration site.
Step 3 Select **Turn On Maintenance Mode**.
Step 4 In the System section, select the **View More** link.
Step 5 Select **Add High Availability System**.
Step 6 Follow the instructions on the **System Properties** page to add the HA system.
Step 7 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 will 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 8 Select **Add**.
Your high-availability system is added and automatically configured to serve as a backup in the event of a primary system failure.

Step 9 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system reboots. You can sign back into the Administration site after the restart is complete.

Removing a High Availability System

Before You Begin

You must have a secondary system currently configured as your high-availability system.

Procedure

Step 1 Sign in to the Administration site.

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

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

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**.

Note After you have removed a high-availability system, you cannot add the same high-availability system back to your site. To reconfigure high availability, you must start over by redeploying a high-availability system from the OVA file. See Adding a High Availability System, on page 69 for more information.

Your high-availability system is removed.

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

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

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 System Requirements* and 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.

Changing Your Virtual IP Address

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 In the Virtual IP Address section, select a link in the Type column.

Example:
Select **Private** for the private virtual IP address.

Step 5 Enter your new virtual IP address in the VIP IPv4 Address field.

Step 6 Select **Save**.

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

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

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 4 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.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **System** and then select the **View More** link in the System section.

Step 4 Select **Add Public Access**.

Step 5 Enter your Internet Reverse Proxy virtual machine in the **FQDN** field.

Note 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 after you redeploy the Internet reverse proxy virtual machine using an appropriate OVA file compatible with updates on your primary system.

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. Make sure you keep your browser window open for the entire process.

If your primary 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. If no updates are required, proceed to the following step.
After your 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 180 for more information.

Step 13 Make any necessary changes to your DNS servers.

Step 14 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Removing Public Access

Before You Begin

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 your changes if necessary. See Creating a Backup by using VMware vCenter, on page 4 for more information. Make sure you power on your virtual machines after your backup is complete.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **System** and then select the **View More** link in the System section.

Step 4 Select the desired site, select **Remove Public Access**, and select **Continue**.
Public access is removed from the site.

Note 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, on page 125 for more information.

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

Expanding the System Size

Before You Begin

Before you perform a system expansion, see Expanding Your System to a Larger System Size, which describes all the pre-requisite steps you should take before using this feature and how to expand your system using automatic or manual deployment.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **System** and select the **View More** link in the System section.

Step 4 Select **Expand System Size**.

Step 5 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. After the backup is complete, you are notified that you can proceed with your expansion.

Step 6 Deploy the OVA file using one of the following methods:

- Expanding the System by using Automatic Deployment
- Expanding the System by using Manual Deployment

Your system notifies you once the expansion is complete.

Step 7 Select **Restart**.

Step 8 Sign in to the Administration site.

Step 9 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Configuring General Settings

To access your general settings, select **System** and the **View More** link under Configuration > General settings. General settings include the following features:

- Site Settings—Use this feature to configure or change your site URL. This feature also displays your site private virtual IP address and site public virtual IP address.
- Administration Settings—Use this feature to configure or change your administration site URL. This feature also displays your administration site private virtual IP address.

Changing Your Site Settings

Use this feature to change your site URL. You configure your original site URL setting during deployment. For more information about site URL configuration and naming conventions, see WebEx Site and WebEx Administration URLs, on page 34.

Before You Begin

Make sure you retain your original site URL on the DNS server. Redirect your original site URL to the updated site URL. If users attempt to use the original URL and you have not redirected it to the new URL, they will not be able to host or join meetings or log in from web pages, productivity tools, and mobile apps.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **System** > **Configuration** > **General settings** > **View More**.

Step 4 In the Site Settings section, select **Edit**.

Step 5 Enter your new site URL in the dialog box and select **Save**.

Step 6 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

What to Do Next

Update your site certificate to ensure secure access. See Managing Certificates, on page 180 for more information.

Changing Your Administration Settings

You configure your original administration site URL setting during deployment. For more information about administration site configuration and naming conventions, see WebEx Site and WebEx Administration URLs, on page 34.

Before You Begin

Make sure you retain your original administration site URL on the DNS server. Redirect your original administration site URL to the updated administration site URL. If users attempt to use the original URL and you have not redirected it to the new URL, they will not be able to host or join meetings or log in from web pages, productivity tools, and mobile apps.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **System** > **Configuration** > **General settings** > **View More**.
The **General settings** page appears.

Step 4 In the Administration Settings section, select **Edit**.

Step 5 Enter your new administration site URL in the dialog box and select **Save**.

Step 6 Select **Turn Off Maintenance Mode** and **Continue** to confirm.

Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

What to Do Next

Update your site certificate to ensure secure access. See Managing Certificates, on page 180 for more information.

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 all the meeting recordings are stored.

Configuring an eMail (SMTP) Server

Configure a mail server to enable your system to send meeting invitations and other communications to users.

Note It is important that the mail 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.

Procedure

Step 1 Sign into the Administration web site.

Step 2 Select **System** and select **View More** in the Servers section.

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

Step 4 In the **SMTP Server** section, select **Edit**.

Step 5 Enter the fully qualified domain name (FQDN) of a mail server that the system will use to send emails.

Step 6 Optionally select **TLS enabled**.

Step 7 Optionally 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 mail server. If there is a firewall between the internal Web and Admin virtual machines and the mail server, the SMTP traffic might be blocked. To ensure mail server configuration and mail notification work properly, port 25 or 465 (secure SMTP port number) must be open between the mail server and the Web and the Admin virtual machines.

Step 8 Optionally to 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 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 three web virtual machines on the primary system and one web virtual machine on the high-availability system.

Step 9 Select **Save**.

Configuring a Storage Server

Use your storage server to back up your system and store meeting recordings. During a Disaster Recovery (see Using the Disaster Recovery Feature), these backups can be used to restore the system. (The currently supported storage method is Network File System (NFS). Make sure 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. See http://www.vmware.com/pdf/vdr_11_admin.pdf for more information.)

Note 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 on a daily basis:

- 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 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 it to the NFS. Transfer time is 12 MB/sec in order to allow other network communication and to ensure the continuous operation of the product.

Before You Begin

Make sure that you configure your Unix access privileges so that your system can store user-generated content and system backups.

On Linux-based storage systems, this depends on the configuration of your read/write permissions for anonymous users for a specific directory to be used for your Network File System (NFS).

On Windows-based storage systems, this depends on 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.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **System**.

Step 4 In the Servers section, select **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 configure one.

Step 5 In the Storage Server section, select **Add a Storage Server now**.

Step 6 Enter the NFS mount point and select **Save**.
The system confirms your NFS mount point.

Step 7 Select **Continue**.
You receive a confirmation message that your storage server has been added.

Step 8 Select **Done**.

Step 9 (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 menu. Then select **Save**.
A daily backup occurs at the time you selected instead of the initially set time of 4:20 a.m. local time.

Step 10 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

What to Do Next

Configure your system to use the storage server for the following:

- Meeting recordings.
- Disaster recovery. See Using the Disaster Recovery Feature, on page 133 for more information.

To ensure proper operation of your storage server, 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 but the recording is saved on the Network File System (NFS) storage server, contact the Cisco Technical Assistance Center (TAC) for assistance in recovering the recording.

Using the Disaster Recovery Feature

Use the disaster recovery features to recover your deployment after a system failure or other disaster. 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:

- One data center disaster recovery—If you have a single data center and your system becomes unavailable, you can reinstall your system in the same data center and restore it to the same state.
- Two data center disaster recovery—If you have two data centers and your system becomes unavailable on the first data center, you can access the system on your second data center and restore the first data center to the same state.

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 chapter)

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 backup the virtual machines. See http://www.vmware.com/pdf/vdr_11_admin.pdf for more information.) In the event that 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 deployments with one data center, you can optionally use the same IP address or hostname. On deployments with two data centers, you can optionally use the same IP address or hostname 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 Configuring a Storage Server for more information.
- You must have access to a system from where you can restore your deployment. See the information on one data center and two data center disaster recovery, below.
- Your recovery system must be the same deployment size and software version as your original system.

  For a high-availability system, you must first configure disaster recovery and then configure high availability on that system. If you have a high-availability system that requires recovery from a disaster, you must first restore your system and then configure high availability on the restored system. For more information on high availability, see Adding a High Availability System.

Procedure

Step 1 Sign in to the Administration site on a system from where you can restore your deployment.

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

Step 3 Select **System** > **Servers** > **Add Storage Server**.

Step 4 Enter the name of your storage server in the **NFS Mount Point** field and select **Save**.

Example:
192.168.10.10:/CWMS/backup.

Step 5 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 6 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 you 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 7 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

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 for more information.
- Reconfigure your SNMP settings. See Configuring Your SNMP Settings 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 a SSL Certificate for more information.
- The recovered system is initially configured for License Free Mode that will expire in 180 days. Re-host your previous system licenses on the recovered system. See Re-hosting Licenses after a Software Upgrade and About Licenses 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 Your Virtual IP Address 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 Integration for more 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

Procedure

Step 1 Sign in to the Administration site.

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

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

Editing Community Strings

Procedure

Step 1 Sign in to the Administration site.

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

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. 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 **Edit**.

Your community string information is changed.

Step 6 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Configuring USM Users

You can add and edit your USM users.

Adding USM Users

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **System** and then select **View More** in the SNMP section.

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

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

Editing USM Users

Note The default USM user, serveradmin, is used internally and the user can only change the password but not security level, auth, and privacy algorithm.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **System** and then select **View More** in the SNMP section.

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

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**.

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

Configuring Notification Destinations

You can configure virtual machines on your system to generate SNMP notifications or traps for the following:

- Virtual machine startup (cold start trap)
- All alarm conditions

Procedure

Step 1 Sign in to the Administration site.
Step 2 Select **System** and select the **View More** link in the SNMP section.
Step 3 Select **Turn On Maintenance Mode** and **Continue** to confirm.
Step 4 Select **Add new Notification Destination** under **Notification Destinations**.
Step 5 Configure 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

Option	Description
Notification Type	Select **Inform** or **Traps**. **Default**: Traps
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 137 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 135 for more information.

Step 6 Select **Add**.
Your notification destination is added.

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

Editing a Notification Destination

Configuring Notification Destinations

Procedure

Step 1 Sign in to the Administration site.
Step 2 Select **System** and select the **View More** link in the SNMP section.
Step 3 Select **Turn On Maintenance Mode** and **Continue** to confirm.
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

Option	Description
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 137 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 135 for more information.

Step 6 Select **Save**.
Your notification destination changes are saved.

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

CHAPTER 13

Configuring Settings

This module describes how to configure your settings.

Configuring Your Company Information

Procedure

Step 1 Sign in to the Administration site.

Step 2 If you want to change the Language setting, select **Turn On Maintenance Mode** and **Continue** to confirm.

Note You do not have to turn on maintenance mode when modifying the other settings on the **Company Info** page.

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 the following: • The sign-in page seen by administrators when they activate their administrator accounts for the first time. • The default audio prompts played for call-in teleconference users.
Locale	Your locale. The locale setting affects the display of times, dates, currency, and numbers.

Step 5 Select **Turn Off Maintenance Mode** and **Continue** to confirm.

Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Configuring Your Branding Settings

Before You Begin

Prepare the following before configuring your branding settings:

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Removing a Company Logo

Before You Begin

Create a transparent 120x32 PNG or GIF file.

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Configuring Your Meeting Settings

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

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

Note This setting is limited by the system size configured during deployment. See Confirming the Size of Your System, on page 29 for more information.

- Participant privileges

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

System Size	Maximum Meeting Size
50	50
250	100
800	100
2,000	100

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

Note You must configure a storage server to enable recording. See Configuring a Storage Server, on page 131 for more information.

Step 6 Select **Save**.

About Meeting Security

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

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

Table 1: Password is Excluded When Scheduling Your Meeting

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

Table 2: Password is Included When Scheduling Your Meeting

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

- Join before host is on/off.
  - On: Invitees or guests can join the meeting before the host, 15 minutes before the scheduled start time.
  - Off: IInvitees 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 is on/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 is on/off.
  - On: When Join before host is configured, the first participant is the presenter.
  - Off: The host always has the ball.

About Configuring Your Audio Settings

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

Configuring Your Audio Settings for the First Time

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

Before You Begin

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

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

Note This feature is not available in Russia or Turkey.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **Settings** > **Audio**.
The **Audio** page appears and your Current Audio Features are displayed.

Step 4 Select **Next**.
The **SIP Configuration** page appears. This page displays the SIP configuration information you need to configure CUCM including the IP address and port number for each server type.

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

Step 6 Select **Edit** to change your settings.
The **CUCM (Cisco Unified 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 CUCM 1 IP Address and optionally for CUCM 2 IP Address.
These IP addresses need to 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* 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 number assigned in CUCM. (**Default:** 5062)

c) Use the **Transport** drop-down menu to select the transport type for your system. (**Default:** TCP)

Note If you select TLS as your transport type, you must import a valid secure conferencing certificate for each of your CUCM servers, export the SSL certificate and upload it into CUCM, and configure your system's fully qualified domain name (FQDN) as the SIP domain name on each CUCM server. See Importing Secure Teleconferencing Certificates 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.

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

Example:
Enter "Headquarters" for the **Phone Label** and "888-555-1212" for the **Phone Number**.
The access numbers you entered are added to your system and you are returned to the **Enable Teleconference: Access Number Setting** page. The page now indicates how many access numbers have been configured.

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

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

Step 14 (Optional) Enter a valid caller ID in the **Caller ID** dialog box.

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

Step 15 (Optional) Configure your WebEx Call Me setting (**Default**: Press 1 to connect to meeting). Optionally 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 configured on your system, set your **IPv6 Teleconferencing** setting to **On** or **Off**. (**Default**: Off. A setting of **Off** indicates that IPv4 is the setting.)

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

Step 18 Select 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.

Step 19 Select **Save**.

Step 20 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Configuring Your Audio Settings

Before You Begin

If you have not already configured your audio settings, see the Configuring Your Audio Settings for the First Time, on page 148 section.

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Configure your audio feature settings.

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. • OFF–Disables all calling features.
Personal Conferencing	• Select the **Enable Personal Conferencing** check box to allow users to start and dial in to personal conference meetings. • Select the **Allow participants to join Personal Conference meetings before host** check box 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 • OFF

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

Option	Description
CUCM 1 IP Address	Enter the hostname or an IP address for your CUCM 1 system.
CUCM 2 IP Address	(Optional) Enter the hostname or an IP address for your CUCM 2 (load balancing service) system. **Note** CUCM 2 is not required but it is recommended for teleconferencing high availability.

Option	Description
Port Number	Enter a valid port number. Make sure the port number matches the setting in CUCM. **Default:** 5062
Transport	Select the transport type. **Note** If you select TLS as your transport type, you must import a valid secure conferencing certificate for each of your CUCM servers, export the SSL certificate and upload it into CUCM, and configure your system's fully qualified domain name (FQDN) as the SIP domain name on each CUCM server. See Importing Secure Teleconferencing Certificates, on page 187 for more information on importing your certificates and "Configuring CUCM" in the *Cisco WebEx Meetings Server Planning Guide* for more information about CUCM. **Default:** TCP

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

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

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

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

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

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

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

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

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

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

- Beep (default)
- No tone
- Announce name

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

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

Step 12 Select **Save**.

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

Configuring Your Video Settings

Procedure

Step 1 Sign in to the Administration site.

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

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

Configuring Your Mobile Settings

Note Android is not supported in Cisco WebEx Meetings Server 1.5 and earlier.

Before You Begin

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

Note that 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 the mobile app defaults to attempting this number first. The app will not connect if this number is not reachable from the mobile network. Make sure that this number is accessible from the mobile network.

Procedure

Step 1 Sign in to the Administration site.

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

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

Configuring Quality of Service (QoS)

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

Following are the default values:

- WebEx Audio (Media)
  - IPv4 QoS Marking: **EF DSCP 101110**
  - IPv6 QoS Marking: **EF DSCP 101110**
- WebEx Audio (Signaling)
  - IPv4 QoS Marking: **CS3 (precedence 3) DSCP 011000**

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select QoS marking settings using the appropriate 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

Traffic	QoS Marking
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
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—Enables you to configure password strength for user accounts including mixed case, length, character types and usage, dynamic web page text controls, and setting up a list of unacceptable passwords.
- Meeting Passwords—Enables you to enforce password usage for meetings and to configure password strength for meetings including mixed case, length, character types and usage, dynamic web page text controls, and setting up a list of unacceptable passwords.

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

Configuring Your General Password Settings

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

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 (Optional) Select the **Deactivate host account after number day(s) of inactivity** checkbox and enter the number of days in the text field. (**Default**: Checked and set for 90 days)
If you use the default setting, a user is deactivated if he or she has not hosted or scheduled a meeting for 90 consecutive days.

Note This feature only applies to host accounts. You cannot deactivate an administrator account using this feature. To deactivate an administrator account, see Deactivating Users, on page 111.

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

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

Step 6 Select **Save**.

Configuring Your User Password Settings

Configure your user password requirements and limitations.

Procedure

Step 1 Sign in to the Administration site.

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

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

Option	Description
Require strong passwords for user accounts	Select this option to enable the remaining options. **Default**: Selected
Minimum character length	Minimum character requirement. **Default**: Selected and **6** characters

Option	Description
Minimum number of alphabetic characters	Minimum alphabetical (non-numeric, non-special characters). **Default**: Selected and **1** character
Minimum number of numeric characters	Minimum numerical (non-alphabetical, non-special characters). **Default**: Selected and **1** number
Minimum number of special characters	Minimum special (non-alphabetical, non-numeric characters). **Default**: Not selected and **1** character
Must include mixed case	Password must contain uppercase and lowercase alphabetical characters. **Default**: Selected
Do not allow any character to be repeated more than 3 times	No one character (alphabetical, numeric, or special) can be repeated more than three times. **Default**: Selected
List of unacceptable passwords	Administrator-specified list of unusable passwords. **Default**: Not selected
Company name, site name, user email address, and host name are always unacceptable	Do not use these specific names. **Default**: Selected
Must not include previous *n* passwords	Do not use previously used passwords. Select a number from the dropdown menu to specify the number of previous passwords you cannot use. **Default**: Selected **Default number**: 5

Step 4 Select **Save**.

Configuring Your Meeting Passwords

Use this feature to configure meeting password parameters. The following table describes which users must enter a password when a meeting is configured with one.

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 not required.	Password not required.	Password not required.	Password not required.	Password not required.
Yes	Yes	Password not required.	Password not required.	Password not required.	Password required.	Password required.
Yes	No	Password not required.	Password not required.	Password not required.	Password required. Password can be prefilled.	Password required. Password can be prefilled.

Procedure

Step 1 Sign in to the Administration site.

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

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

Note All options are not selected by default.

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

Option	Description
Must include mixed case	Password must contain uppercase and lowercase alphabetical characters.
List of unacceptable passwords	Administrator-specified list of unusable passwords.
Company name, site name, user email address, host name, and meeting topic are always unacceptable	Select this option to prohibit the use of these words or character strings.

Step 4 Select **Save**.

Configuring Your Email Settings

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Note If you enter a person's name in the From Name on the Variables page, but meeting invitations will reflect the host's email address.

Step 4 Select **Templates**. See About Email Templates, on page 160 for descriptions of each template type.
The **Templates** page appears. Select the **Common** or **Meetings** tab. **Common** is the default.

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

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

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

Note If you enter a person's name for **From Name** on the **Variables** page, the system automatically replaces the person's name with the WebEx site URL for all meeting invitations.

About Email Templates

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

There are two types of email templates:

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

Table 3: Common Email Templates

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

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

Title	Description	Variables
Forgot Password–Reset Password	Sent to a user after he has reset his password from the end-user site. This email asks the user to create a new password.	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
PT PCN Meeting Invitation—Invitee	Sent to meeting invitees after a meeting is scheduled using Productivity Tools from a PCN account.	• %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %Meeting Space% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
PT PCN Meeting Notification—Host	Sent to a meeting host after a meeting is scheduled using Productivity Tools from a PCN account.	• %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %Meeting Space% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
PT—Host Notification	Sent to a meeting host after a meeting is scheduled using Productivity Tools.	• %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%
PT—Invitee Notification	Sent to meeting invitees after a meeting is scheduled using Productivity Tools.	• %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%
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%

Title	Description	Variables
SSO Activation Email	Sent after Single Sign-On (SSO) is enabled.	• %SiteURL% • %DisplayName% • %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%
Setup Cisco WebEx—Android	Informs users about the Cisco WebEx app for Android and provides a download link for the app.	• %SiteURL% • %Subject% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
Setup Cisco WebEx—iPhone/iPad	Informs users about the Cisco WebEx app for iPhone/iPad and provides a download link for the app.	• %SiteURL% • %Subject% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Share Recording	Sends selected meeting attendees a link to a meeting recording.	• %HostName% • %HostEmail% • %OrgLogo% • %AttendeeName% • %HostName% • %Topic Name% • %Duration% • %Recording Time% • %Personalized Message% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

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

Table 4: Meetings Email Templates

Title	Description	Variables
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 attendees when the host selects **Meet Now**.	• %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %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_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText% • %Year%
Meeting Canceled for Host	Sent to a meeting's host to confirm cancellation of a meeting.	• %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %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's 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's 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 attendees.	• %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 attendees.	• %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's host (PCN accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
PCN Meeting Invitation—Invitee	Sends a meeting invitation to invitees (PCN accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

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

Title	Description	Variables
PCN Meeting Notification—Host	Sends a meeting notification to the host (PCN accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
PCN Meeting Instant Invitation—Host	Sends an instant meeting notification to the host (PCN accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %SiteURL% • %Support%

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

Title	Description	Variables
PCN Meeting Schedule Change—Invitee	Sends a schedule change notification to an invitee (PCN accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
PCN Meeting Rescheduled—Invitee	Sends a meeting rescheduled notification to an invitee (PCN accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

Title	Description	Variables
PCN Meeting Canceled—Host	Sends a meeting cancellation notification to a host (PCN accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%
PCN Meeting Canceled—Invitee	Sends a meeting cancellation notification to an invitee (PCN accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%

Configuring Your Download Settings

Procedure

Step 1 Sign in to the Administration site.

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

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

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**, proceed to the next step.

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.

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.

About Downloads

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

On PCs without administrator privileges:

- We recommend that you push the WebEx Meetings application and Productivity Tools to end-user desktops offline before you inform end-users that user accounts have been created for them. This ensures that your users can start and join meetings from their web browsers and Windows desktops the first time they sign in.
- You can acquire the .MSI installers for each from the Administration site at the **Settings** > **Downloads** page. See Configuring Your Download Settings, on page 179 for more information.
- If you decide against pushing the applications to your users, they can still access these applications from the end-user download pages. However, if their PCs prohibit installation of downloaded applications, they will not be able to complete the installation process.
- When users join meetings by using their web browser (the WebEx Meetings application can still be downloaded on demand) they can join meetings successfully. In addition, the WebEx Meetings application attempts to perform an installation to speed up the process of starting or joining future meetings. This fails because their PCs do not have administrator privileges.

On PCs with administrator privileges:

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

Managing Certificates

Certificates are used to ensure secure communication between the components of your system. When your system is first deployed, it is configured with a self-signed certificate. While a self-signed certificate can last for up to five years, we strongly recommend that you configure certificates that are validated by a certificate

authority. A certificate authority ensures that communication between your virtual machines is authenticated. Note that you must install a certificate for each virtual machine on your system.

The following certificate types are supported:

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

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

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

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

SSL certificates can become invalid for the following reasons:

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

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

Generating SSL Certificates

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

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

Generating a Certificate Signing Request (CSR)

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Option	Description
Common Name	Select **Subject Alternative Name** certificate or **Wildcard** certificate.
Subject Alternative Names **Note** This option appears only if you select **Subject Alternative Name** for your Common Name type.	Your administration site and virtual machine names. No subject alternative names are required if you selected a wildcard common name.
Organization	Enter your organization name.
Department	Enter your department name.
City	Enter your city.
State/Province	Enter your state or province.
Country	Select your country.
Key Size	Select your key size from the following options: • 2048 **Default**: 2048 (Recommended)

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

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

Step 7 Back up your system using VMware Data Recovery (vSphere 5.0) or VMware vSphere Data Protection (vSphere 5.1). See Creating a Backup by using VMware vCenter, on page 4 for more information.
Note Backing up your system preserves the private key in the event that you need to restore it.

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

Importing a SSL Certificate

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

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **Settings** > **Security** > **Certificates** > **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 4 Select **Continue**.

Step 5 Select **Browse** and choose your certificate file.
You must choose an X.509-compliant certificate or certificate chain. Valid types include:

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

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

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

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

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

Step 6 Select **Upload**.
After you select **Upload**, the system will determine if your certificate is valid. A certificate can be invalid for the following reasons:

- The certificate file is not a valid certificate file.
- The certificate file you selected has expired.
- Your public key must be at least 2048 bits.

- The server domains in the certificate do not match the site URL.
- The private key that was automatically generated by the system is not compatible with the certificate.

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

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

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

Exporting a SSL Certificate

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Save the certificate file.

What to Do Next

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

Downloading Your CSR and Private Key

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Generating a Self-Signed Certificate

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

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Option	Description
Certificate name	Enter a name for your self signed certificate. (Required)
X.509 subject name	The hostname of your system. (Not configurable)
Organization	Enter your organization name.
Department	Enter your department name.
City	Enter your city name.
State/Province	Enter the name of your state or province.
Country	Select your country name.

Step 5 Select **Generate Certificate and Private Key**.

Note If you need to use the same SSL certificate after a major upgrade, you must upload the private key generated with the CSR 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**.

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

Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Restoring a SSL Certificate

In the event that your certificate becomes invalid or you have performed a disaster recovery on your system, you can restore a SSL certificate using this feature. Cisco WebEx Meetings Server supports X.509 certificates with PEM and DER encoding and PKCS12 Archives.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **Settings** > **Security** > **Certificates** > **More Options** > **Import SSL Certificate**.
If you already have a certificate installed, the system warns you that importing a new certificate will overwrite it.

Step 4 Select **Continue**.

Step 5 Select **Browse** and choose your certificate file.
You must choose an X.509-compliant certificate or certificate chain. Valid types include:

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

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

- (Optional) If you want to reapply a previous private/public key pair for disaster recovery, combine the public 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 followed by the public key. It can be encrypted or unencrypted. It should be in PKCS#8 format and PEM encoded. If it is encrypted, you must enter the password to decrypt it in the passphrase field.
- The next element must be the certificate of the intermediate certificate authority that issued your certificate in PEM encoded X.509 format.
- You can include as many intermediate certificates as you use in your infrastructure. The certificate of the root certificate authority should not be included. If you are using a private certificate authority, you must make sure that the root certificate is distributed to all clients.

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

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

Step 6 Select **Upload**.
After you select **Upload**, the system will determine if your certificate is valid. A certificate can be invalid for the following reasons:

- The certificate file is not a valid certificate file.
- The certificate file you selected has expired.
- Your public key must be at least 2048 bits.

- The server domains in the certificate do not match the site URL.
- The private key that was automatically generated by the system is not compatible with the certificate.

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

Step 7 (Optional) Enter a passphrase in the **Passphrase** field.

Note A passphrase is required to decrypt PKCS12 archives or an encrypted private key (if uploaded .pem files contain the private key).

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

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

Step 10 Select **Done**.

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

Importing SSO IdP Certificates

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

Importing Secure Teleconferencing Certificates

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

Before You Begin

Secure teleconferencing certificates are required for your CUCM servers when TLS is selected as the transport type in your audio settings. See About Configuring Your Audio Settings, on page 148 for more information.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **Settings** > **Security** > **Certificates**.
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 1.
The **Secure Teleconferencing Certificate** page appears.

Step 5 Enter a certificate name.

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

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

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

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

Step 9 Select **Done**.

Step 10 Return to step 4 and repeat the process for your CUCM 2 server.

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

Configuring User Session Security

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 4 Select **Save**.

Configuring Federated Single Sign-On (SSO) Settings

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

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

Before You Begin

- Before you enable the federated single sign-on feature, you must generate a set of public and private keys and an X.509 certificate that contains the public key. Once you have a public key or certificate, you must upload it in the Managing Certificates, on page 180 section.

  Note After you have enabled SSO, user credentials are managed by your corporate authentication system. Certain password management features no longer apply to your users. See Configuring Passwords, on page 155 and Editing Users, on page 110 for more information. Note that even though administrators are also end users, administrators do not sign in using SSO. They sign in using their administrator credentials for this product.

- Configure a SSO IdP certificate to use this feature. See Importing SSO IdP Certificates, on page 187 for more information.

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select your initiation method:

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

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

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

Field	Description
SP (Service Provider) Initiated	Select this option for service provider initiated sign in.
AuthnRequest signed	Select this option to require that the AuthnRequest message must be signed by the service provider's private key. **Note** You must select this option if you want your exported SAML metadata file to include your site's SSL certificate.
Destination	The SAML 2.0 implementation URL of IdP that receives authentication requests for processing. **Note** This field appears only when **AuthnRequest signed** is selected.
IdP (Identity Provider) Initiated	Select this option for identity provider initiated sign in.
Target page URL parameter name	Your system redirects to this URL when SSO is successful. **Default**: TARGET **Note** On an IdP-initiated system, the URL must be a combined URL in the following format: your service login URL, "?" or "&," the target page URL parameter, "=" (if it is not present), and the target URL.
SAML issuer (SP ID)	Enter the same SP ID configured for IdP. Reference the SAML2 protocol.

Field	Description
Issuer for SAML (IdP ID)	Enter the same ID configured for IdP. Reference the SAML2 protocol.
Customer SSO service login URL	The assertion consumption URL for SAML2 in IdP.
NameID format	Select the same NameID format that you set in IdP. The NameID is the format in which you send the user ID in the assertion and single logout request from Cisco WebEx. See the SAML protocol for guidance. We recommend that you set the email address as your NameID. Doing so will make the process of using SSO easy for end users who have already set up their accounts based on their email address on the system. Using other NameID formats is supported but not recommended. If you use a format other than an email address,users will no longer be able to sign in to a WebEx site if SSO is disabled. **Default**: Unspecified
AuthnContextClassRef	Enter the value that is configured in IdP. AuthnContextClassRef is the value that appears in the AuthnRequest message. **Default**: urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
Default Webex target page URL	Your system redirects to this URL when SSO is successful. The default page is the Cisco WebEx meeting page which is the same as a normal login.
Customer SSO error URL	Your system redirects to this URL when SSO is not successful. By default, the error page is a common Cisco WebEx error page.
Single logout	This option enables single logout which is defined by the SAML2 protocol. If you have chosen the SSO option but not the single logout option, the sign out option does not appear on end-user pages. Deselect this option for ADFS 2.0. **Note** IdP-Initiated SLO is not supported in this version.
Customer SSO service logout URL **Note** This option appears only when Single logout is selected.	Enter the assertion consumption URL for SAML2 in IdP.

Field	Description
Auto account creation	Users without a Cisco WebEx account are unable to sign in. If you select this option, an account is automatically created for new users when they attempt to sign in.
Auto account update	If you select this option, user information is updated when there is an "updateTimeStamp" in the SAML2 assertion with more recent user information than the current data in Cisco WebEx.
Remove UID domain suffix for Active Directory UPN	Select this option to authenticate users without a domain suffix. The **Remove UID domain suffix for Active Directory UPN** option works in the following cases: • The NameId format is email, and UID format is the X509 subject name or User Principal Name (UPN). • The NameId format is the X509 subject name or UPN.

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

Disabling SSO

Before You Begin

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

Procedure

Step 1 Sign in to the Administration site.
Step 2 Select **Settings** > **Security** > **Federated SSO**.
Step 3 Find the sentence, "If you would like to disable SSO please click here." Select the **click here** link.
Step 4 Select **Disable SSO** to confirm.
The **Federated SSO** page appears with a banner that confirms you have disabled SSO.

Configuring Your Cloud Features

You can configure your system so that your users can use a single version of the Cisco WebEx Productivity Tools that can be used with both their Cisco WebEx Meetings Server and SaaS WebEx accounts or to view training videos hosted online by Cisco WebEx.

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select **Save**.

Configuring Virtual Machine Security

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

Updating Your Encryption Keys

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select **Update Encryption Keys**.

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

About FIPS

The Federal Information Processing Standard (FIPS) 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 might include, but are not limited to, problems signing into the system, 404 errors, and starting and joining meetings.

Cisco recommends that you take the following actions:

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

Enabling FIPS Compliant Encryption

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

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **Settings** > **Security** > **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 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Disabling FIPS Compliant Encryption

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

Procedure

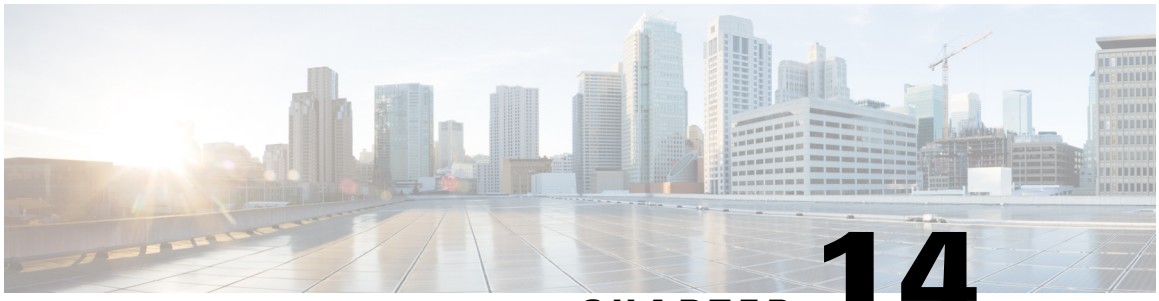
Step 1 Sign in to the Administration site.

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

Step 3 Select **Settings** > **Security** > **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 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.



CHAPTER 14

Managing Your Reports

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 Your Company Information, on page 144 for more information.

Note When your system is newly deployed or recently 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.

Downloading Monthly Reports

You can view and download monthly summary reports from this page. Reports are displayed in PDF format.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Reports**.

Step 3 Select the **Download** link for the monthly report you want to view.

About Monthly Reports

Your Monthly Summary Report contains the following sections:

System Summary Report

Your System Summary Report contains the following reports:

- Service Adoption—This report displays a graph depicting the number of unique hosts and attendants over the previous three months and the expected growth rate over the next three months.
- User Licenses—This report displays the percentage of purchased licenses your are using and a graph depicting the number of licenses used over the past three months and the expected growth rate over the next three months. You can use these numbers to predict future license usage and adjust your license purchases accordingly. See Fulfilling Licenses by using the License Manager for more information.
- System Size—This report displays your 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—This report displays 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. If you need to add additional storage space you must manually copy your existing storage data archive and recordings to your new storage server before you activate it.

Note This report only appears if you have configured a storage server. See Configuring a Storage Server, on page 131 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.
- 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—This report displays 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. For real-time meeting status, view the Dashboard. See About Your Dashboard for more information. For more information about the meeting status, see Viewing the Meetings List.
- Meeting Size—This report displays 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—This report displays 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.

Generating Customized Details Reports

Procedure

Step 1 Sign in to the Administration site.

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—This 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. This report includes the following fields:
  - 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—This report contains information on all meetings that took place during the specified period and includes the following fields:
  - MeetingID—The unique conference ID generated by your system when the meeting was scheduled.
  - Meeting Number—The Cisco WebEx meeting number.
  - Subject—The name of the meeting configured by the host.
  - HostName—The meeting host.
  - Start Time—The starting time and date of the meeting.
  - Duration—Duration of the meeting in minutes.
  - Number of Participants—The number of participants including hosts.
  - Status—The status of each meeting.

    Note For clarification

  - Number of Call-In Audio Minutes

- Number of Call-Back Audio Minutes
- Number of VoIP Minutes
- Number of Video Minutes
- Number of Recording Minutes
- Number of WebSharing Minutes—The 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.
- TrackingCodes—The tracking codes applied by the host when scheduling the meeting.

- Network Bandwidth Utilization Report—This report contains a list of 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)

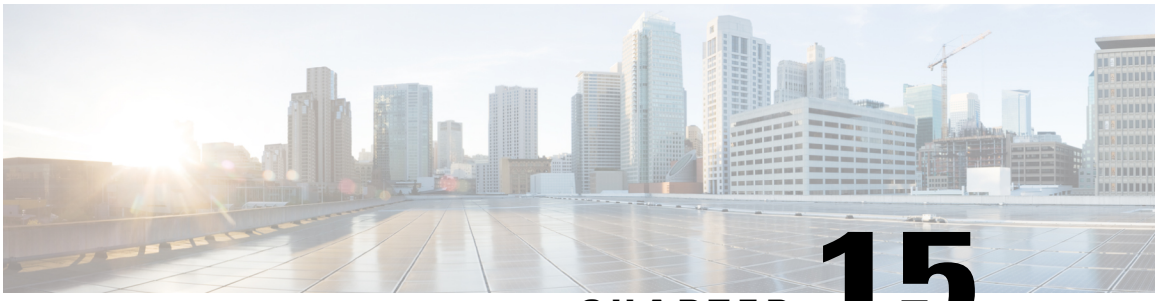
  A consumption of 0 (zero) indicates that the feature was not used on that date. A consumption of less than 1 is displayed if less than 1 Mbps was consumed on the specified date.

  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—This 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 Configuring a Storage Server for more information.

- System Downtime Report—This report contains 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—Lists 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—Lists the 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—The user name of the meeting host.
  - E-mail address—Email address of the meeting host.
  - Meeting ID—The unique conference ID generated by your system when the meeting was scheduled.
  - Meeting Number—The Cisco WebEx meeting number.
  - Start Time—The date and time the meeting started.
  - Simultaneous Meeting—Indicates the 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 15

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 30 days. However, if you upgrade a Cisco WebEx Meetings Server 1.x deployment to Release 2.0, the log data from Release 1.x will not be transferred to the Cisco WebEx Meetings Server 2.0 system and therefore not available after the upgrade to Release 2.0 is complete.

Procedure

Step 1 Sign in to the Administration site.

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.

Field	Description
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 30 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

Your log is generated and an email is sent to you containing 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.

Procedure

Step 1 Sign in to the Administration site.

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).
Decoder Version	Select **2- Webex Meetings Server**. **Note** If you have a remote support account that was active prior to the release of Cisco WebEx Meetings Server Version 1.5, you do not have to configure this setting.

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

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Support** > **Remote Support Account**.

Step 3 Next to the status message, "Remote Support is enabled," select the **Disable It** link.
Your remote support account is disabled.