Cisco WebEx Meetings Server Administration Guide

First Published: October 21, 2012

Last Modified: October 21, 2012

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

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 and 5.0 Update 1.

  Earlier releases of vSphere are not supported.

- Use VMware ESXi 5.x.

  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.

Note For complete 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 Using VMware vCenter

Before doing any system-altering procedure, Cisco recommends that you take a backup of each of the virtual machines. You may do so by using VMware Data Recovery or taking a virtual machine snapshot. (VMware Data Recovery is included as part of VMware vSphere.)

Note Virtual machine snapshots are a "picture" of your system at a specific point in time, and are not the same as backups.

Caution If you take snapshots, they are stored on the physical drives containing your virtual machines. If you do not delete these snapshots in a timely manner, your end users may begin to experience degraded audio and video due to a known issue that affects virtual machine performance. Therefore, for performance reasons, be sure to 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 this known performance issue, see Taking a Snapshot Using VMware vCenter, on page 5.

Procedure

Step 1 Place the system in maintenance mode. For complete details, see About Maintenance Mode, on page 112
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 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*.

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 Using VMware vCenter

Before doing any system-altering procedure, Cisco recommends that you take a backup of each of the virtual machines. You may do so by using VMware Data Recovery or taking a virtual machine snapshot. (VMware Data Recovery is included as part of VMware vSphere.)

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

Note Virtual machine snapshots are a "picture" of your system at a specific point in time, and are not the same as backups.

Remember If your system comprises multiple virtual machines, be sure to take a snapshot of each virtual machine, after selecting **Power** > **Shut Down Guest**. 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.

Caution If you take snapshots, they are stored on the physical drives containing your virtual machines. If you do not delete these snapshots in a timely manner, your end users may begin to experience degraded audio and video due to a known VMware issue that affects virtual machine performance.

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 may also search the VMware KnowledgeBase for "snapshot impact performance" for additional information.

Note Cisco recommends you keep snapshots no longer than approximately 24 hours. If you want to keep them longer, then create a backup instead. For more information on VMware Data Recovery, see Creating a Backup Using VMware vCenter, on page 4.

Procedure

Step 1 Place the system in maintenance mode. For complete details, see About Maintenance Mode, on page 112. 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 VMDK files from an existing Admin virtual machine to a new Admin virtual machine, using VMware vCenter.

Although there are multiple reasons for moving a virtual disk VMDK file, this section focuses only on the procedure, for moving data from one Admin virtual machine to another Admin virtual machine. You will use this procedure 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 it directly into the virtual machine folder of the Admin virtual machine in the upgraded or expanded system. If you simply attach Hard disk 4, then 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, then your current system will lose access to Hard disk 4.

Note If you are using Direct-attached storage (DAS), then you must migrate the virtual machine VMDK file to a 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 "existing" Admin virtual machine. The Admin virtual machine, following expansion or upgrade, is named the "new" Admin virtual machine.

Procedure

Step 1 Navigate the inventory in VMware vCenter and find the existing 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 that VMDK file in VMware vCenter.

The string is similar to `[EMC-LUN10-RAID5] webex-sysA-admin/webex-sysA-admin_3-000001.vmdk`.

Step 5 Note and write down the storage location for Hard disk 4 and the virtual machine folder name.
The 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 existing and new 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 file from the existing Admin virtual machine folder to the new Admin virtual machine folder.

a) In the existing Admin virtual machine folder, locate the VMDK file 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 new 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 new (expanded or upgraded) Admin virtual machine for your system.

Step 13 Right-click the newly deployed 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 new 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) Hard disk 4**, then select **Next**.

Step 21 Review your changes, and if it is correct, select **Finish**. Otherwise, select **Back** and fix any errors.

Once the wizard is complete, you will see a new disk marked for addition in the Hardware tab.

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

Installing Your System Using Automatic Deployment

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

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 will use this information to look up IP addresses for you during the deployment.

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 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.	
(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.	

Field Name	Description	Value For Your System
(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 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)	
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 for users to host and attend meetings.	
WebEx Administration URL	Secure http URL 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 may differ slightly from this procedure. See your VMware vSphere documentation for complete information on the OVA wizard.

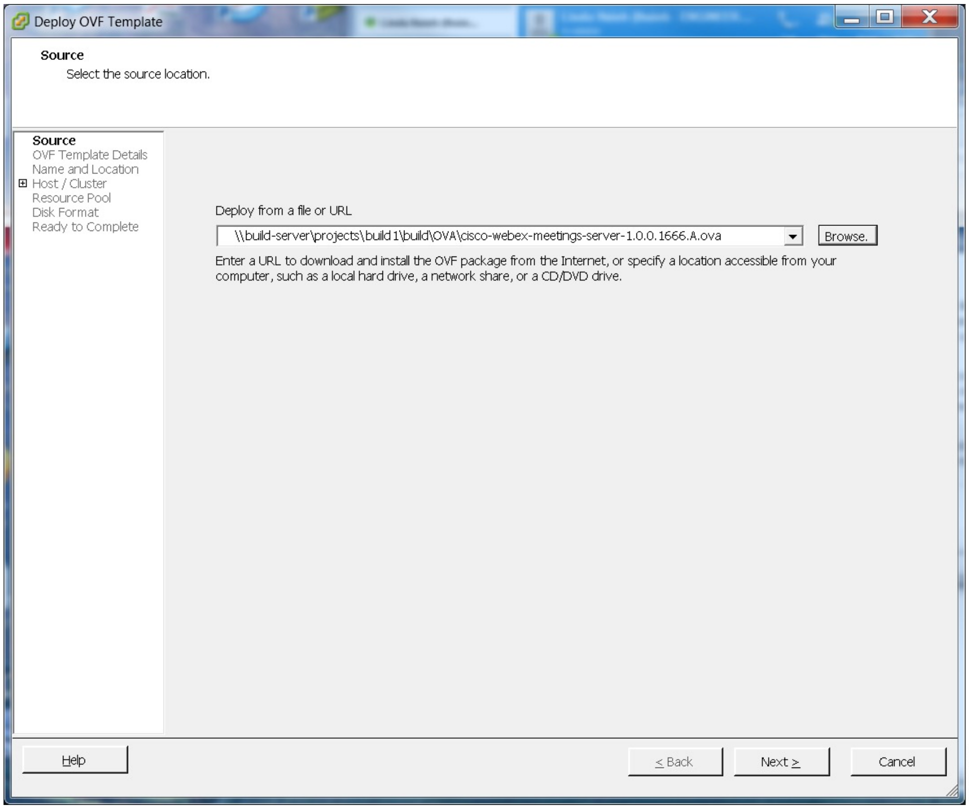
Before You Begin

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

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 and off, and delete virtual machines.

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



Source
Select the source location.

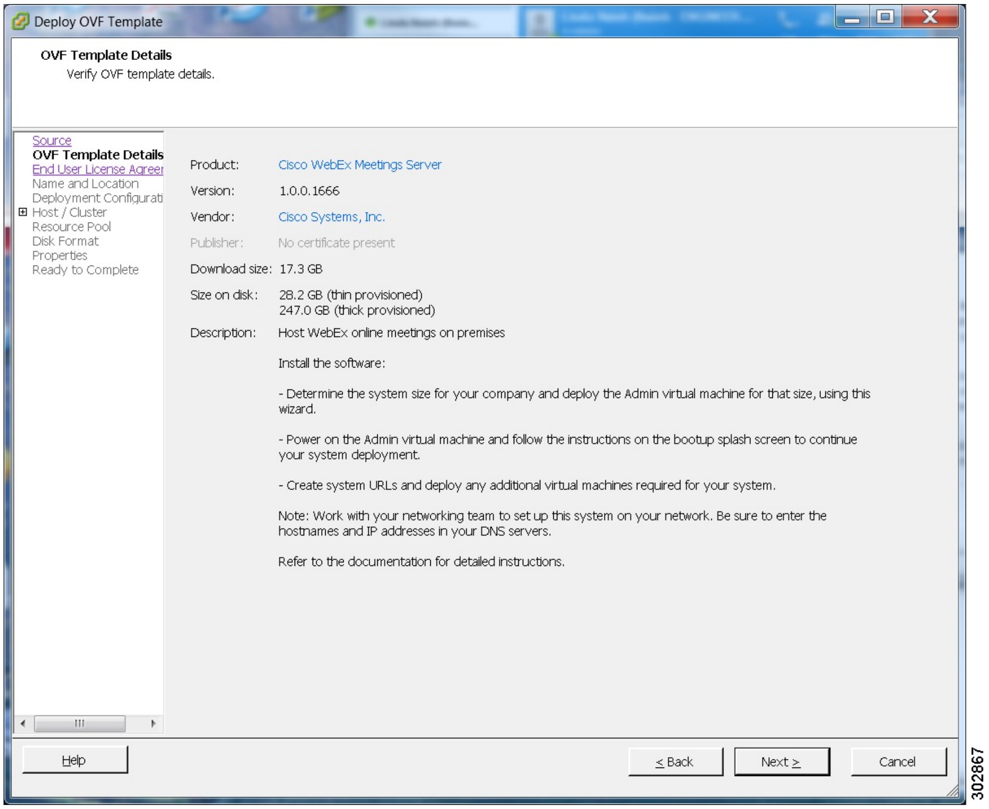
Deploy from a file or URL

\\build-server\projects\build1\build\OVA\cisco-webex-meetings-server-1.0.0.1666.A.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

302866

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



OVF Template Details

Verify OVF template details.

Product: Cisco WebEx Meetings Server

Version: 1.0.0.1666

Vendor: Cisco Systems, Inc.

Publisher: No certificate present

Download size: 17.3 GB

Size on disk: 28.2 GB (thin provisioned)
247.0 GB (thick provisioned)

Description: Host WebEx online meetings on premises

Install the software:

- Determine the system size for your company and deploy the Admin virtual machine for that size, using this wizard.

- Power on the Admin virtual machine and follow the instructions on the bootup splash screen to continue your system deployment.

- Create system URLs and deploy any additional virtual machines required for your system.

Note: Work with your networking team to set up this system on your network. Be sure to enter the hostnames and IP addresses in your DNS servers.

Refer to the documentation for detailed instructions.

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

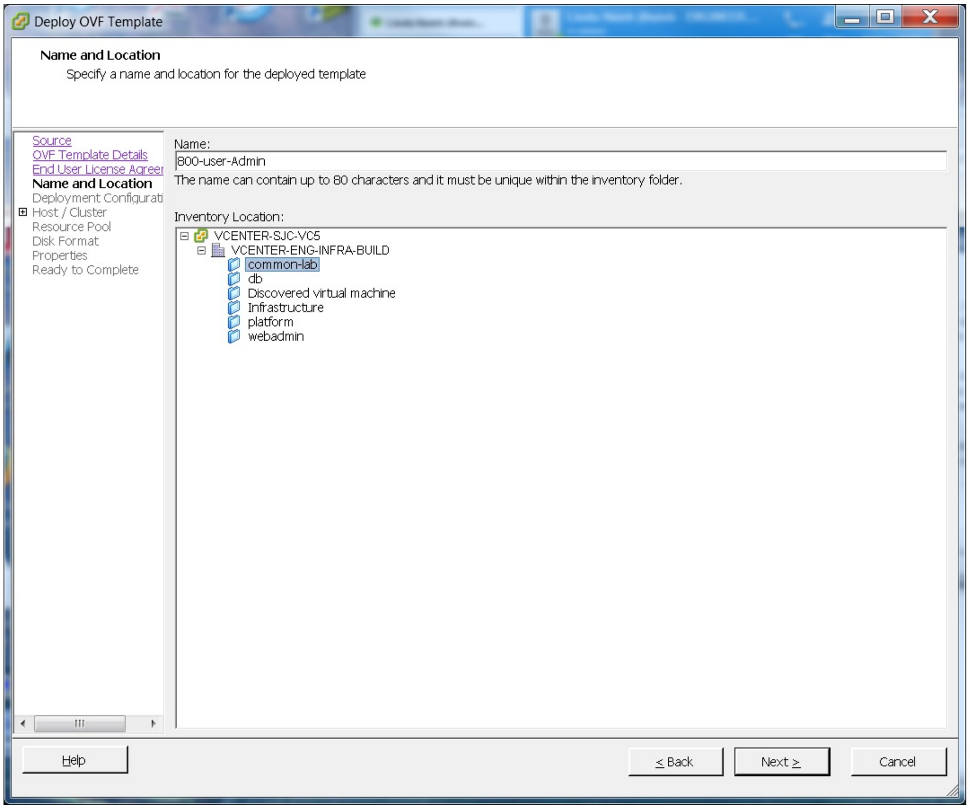
Step 5 Navigate to, and select the location, in the vCenter inventory, where you'd like to place the Admin virtual machine.

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, on page 12.

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

Cisco recommends you include the type in the virtual machine name; for example, "Admin" in your Admin virtual machine name, to identify it easily 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 may need one or more media and web internal virtual machines.)



Name and Location

Specify a name and location for the deployed template

Name: 800-user-Admin

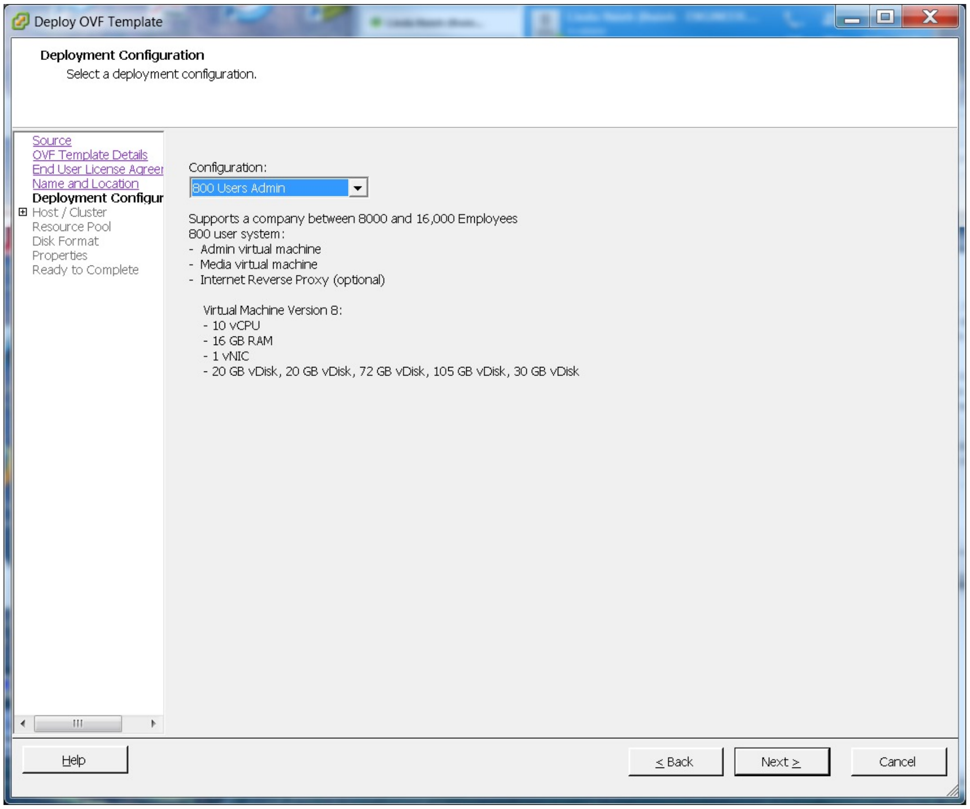
The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:

302869

Step 7 From the drop-down list, select the virtual machine for your system size then select **Next**.

Be sure to deploy the Admin virtual machine before any other virtual machines in your system.



Deployment Configuration

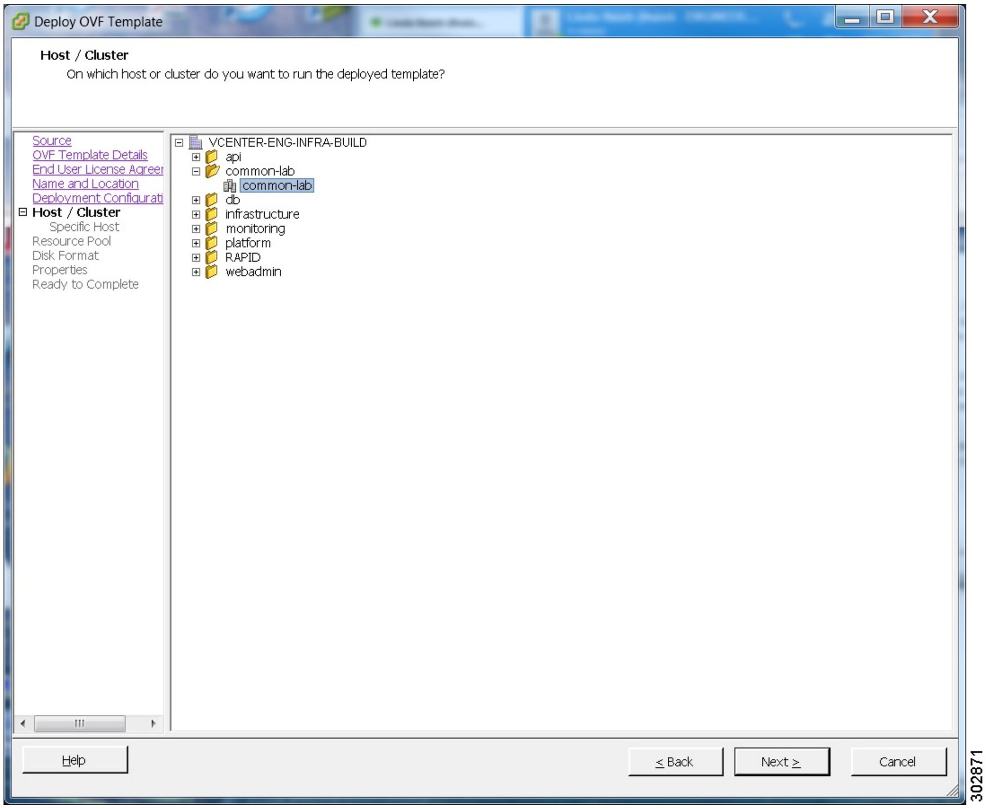
Select a deployment configuration.

Configuration: 800 Users Admin

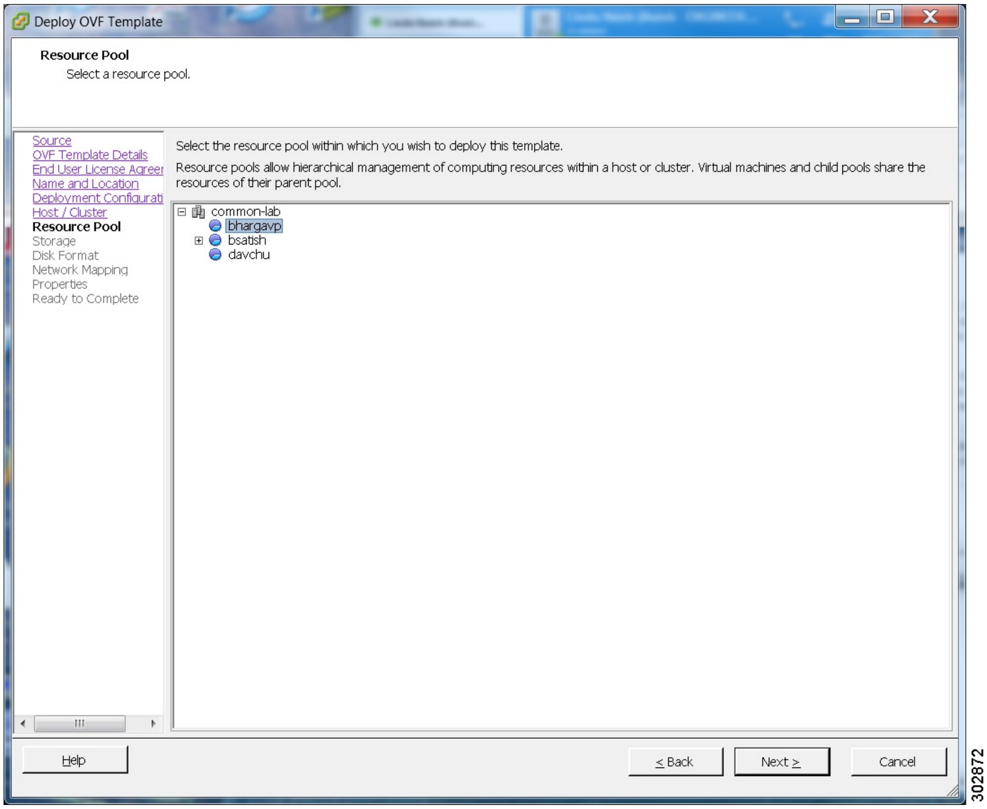
Supports a company between 8000 and 16,000 Employees
800 user system:
- Admin virtual machine
- Media virtual machine
- Internet Reverse Proxy (optional)

Virtual Machine Version 8:
- 10 vCPU
- 16 GB RAM
- 1 vNIC
- 20 GB vDisk, 20 GB vDisk, 72 GB vDisk, 105 GB vDisk, 30 GB vDisk

Step 8 Navigate thru 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, then select the resource pool where you want to deploy the OVA template and select **Next**.



Deploy OVF Template

Resource Pool

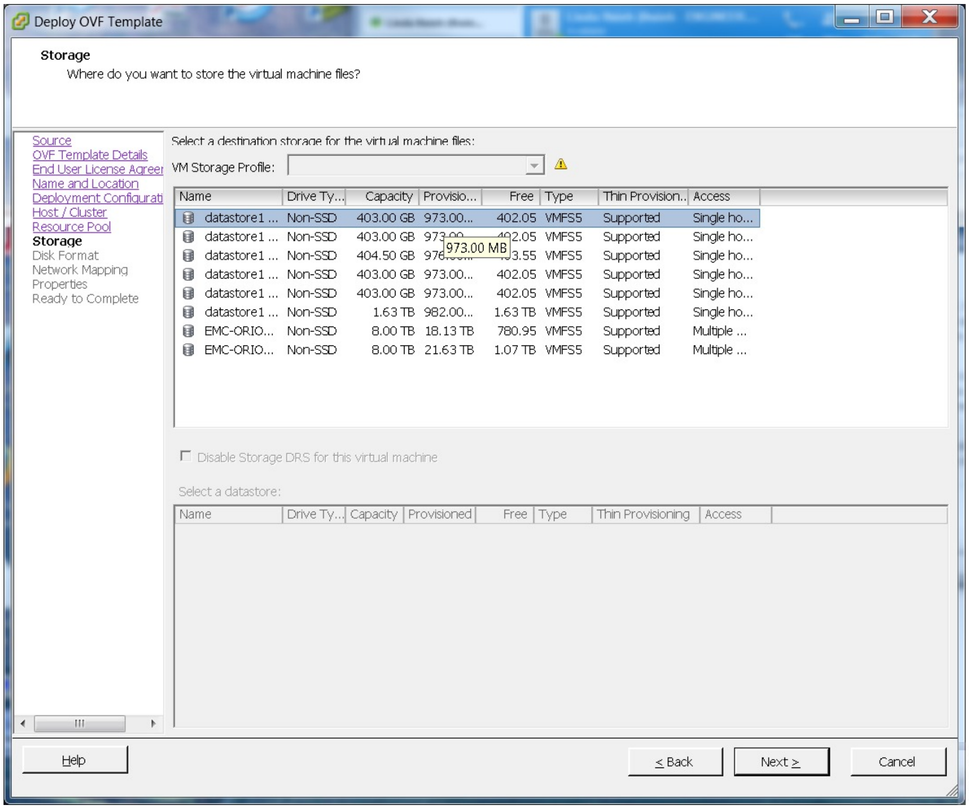
Select a resource pool.

Select the resource pool within which you wish to deploy this template.

Resource pools allow hierarchical management of computing resources within a host or cluster. Virtual machines and child pools share the resources of their parent pool.

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 Provision**, VMware allocates the file system space on an "as-needed" basis, resulting in poor performance.



Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

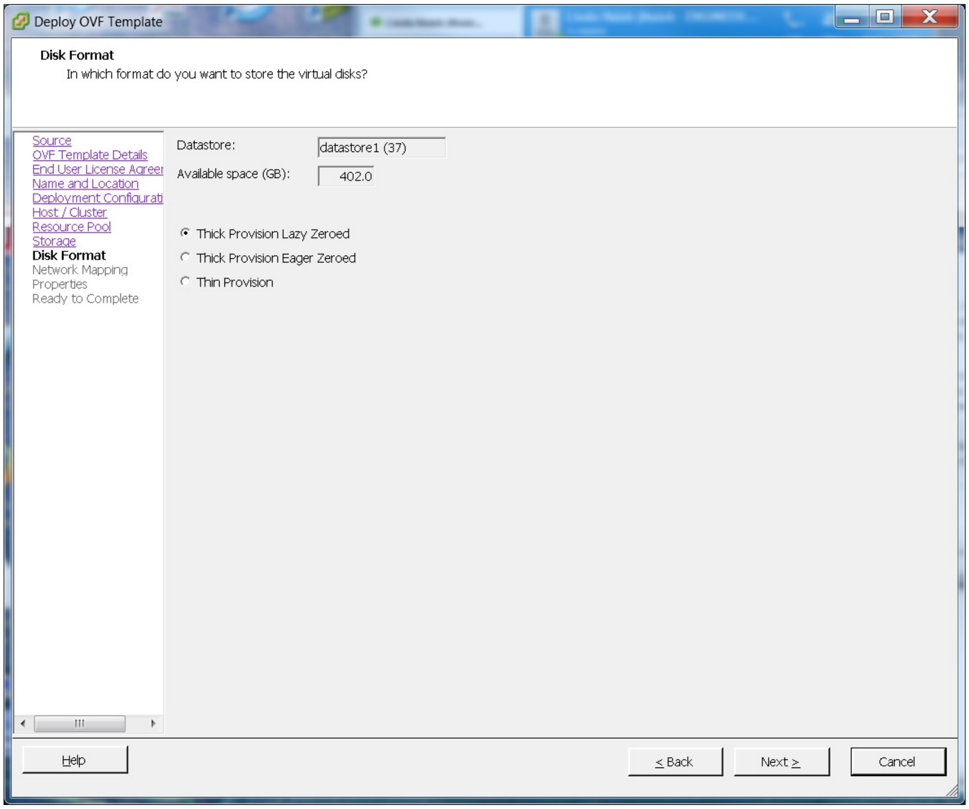
VM Storage Profile:

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[illegible]	[illegible]3.55	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 ...

☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Ty...	Capacity	Provisioned	Free	Type	Thin Provisioning	Access



Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1 (37)

Available space (GB): 402.0

● Thick Provision Lazy Zeroed

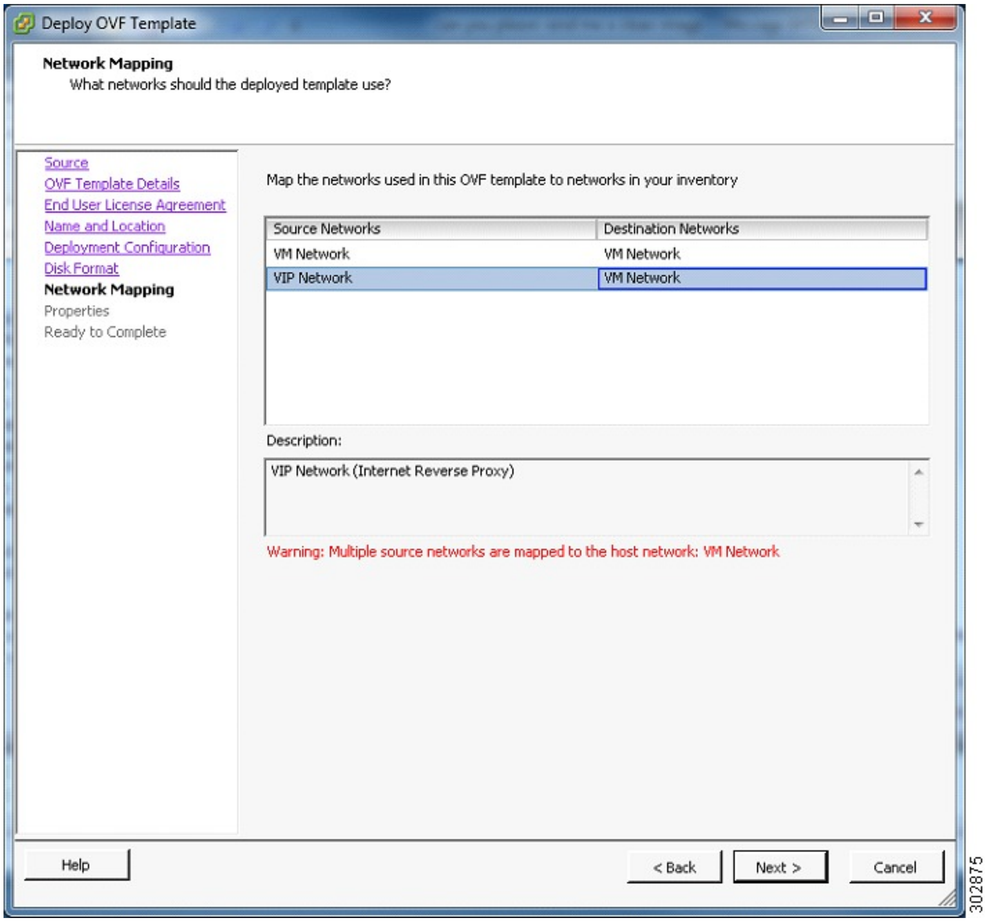
○ Thick Provision Eager Zeroed

○ Thin Provision

302874

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.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	VM Network
VIP Network	VM Network

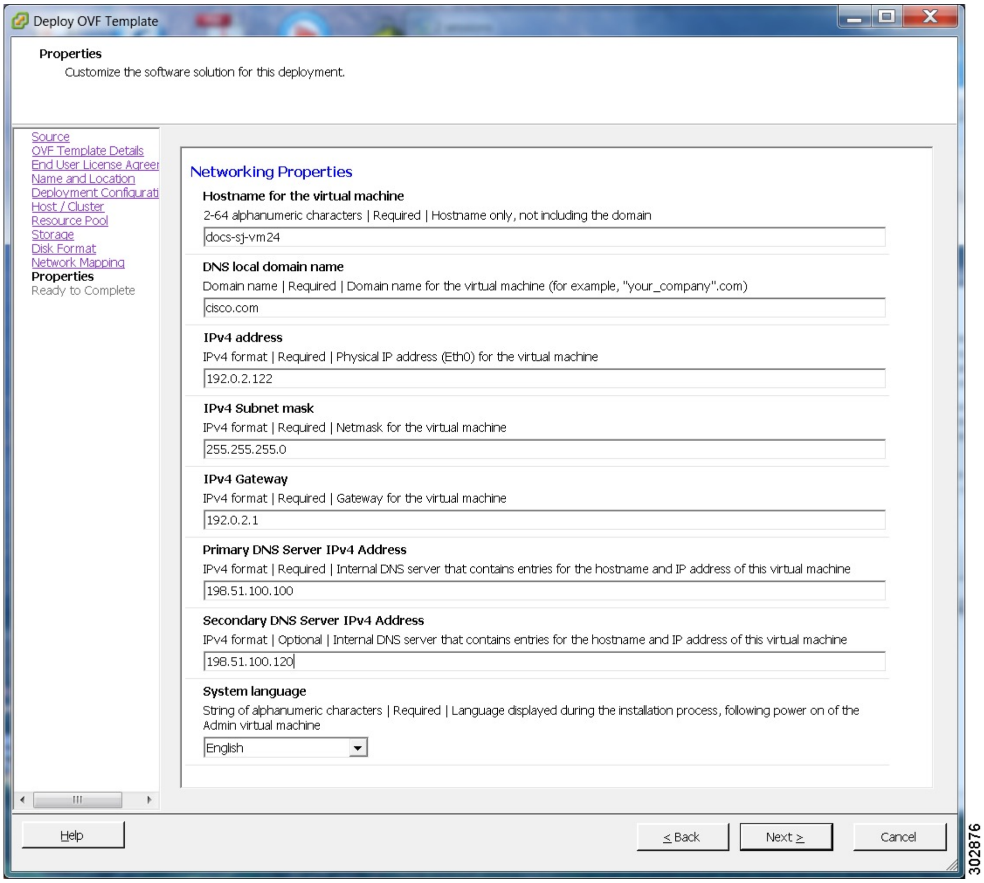
Description:

VIP Network (Internet Reverse Proxy)

Warning: Multiple source networks are mapped to the host network: VM Network

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

- Hostname of the virtual machine (do not include the domain as you will enter this in the next field)
- 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



Properties

Customize the software solution for this deployment.

Networking Properties

Hostname for the virtual machine

2-64 alphanumeric characters | Required | Hostname only, not including the domain

docs-sj-vm24

DNS local domain name

Domain name | Required | Domain name for the virtual machine (for example, "your_company".com)

cisco.com

IPv4 address

IPv4 format | Required | Physical IP address (Eth0) for the virtual machine

192.0.2.122

IPv4 Subnet mask

IPv4 format | Required | Netmask for the virtual machine

255.255.255.0

IPv4 Gateway

IPv4 format | Required | Gateway for the virtual machine

192.0.2.1

Primary DNS Server IPv4 Address

IPv4 format | Required | Internal DNS server that contains entries for the hostname and IP address of this virtual machine

198.51.100.100

Secondary DNS Server IPv4 Address

IPv4 format | Optional | Internal DNS server that contains entries for the hostname and IP address of this virtual machine

198.51.100.120

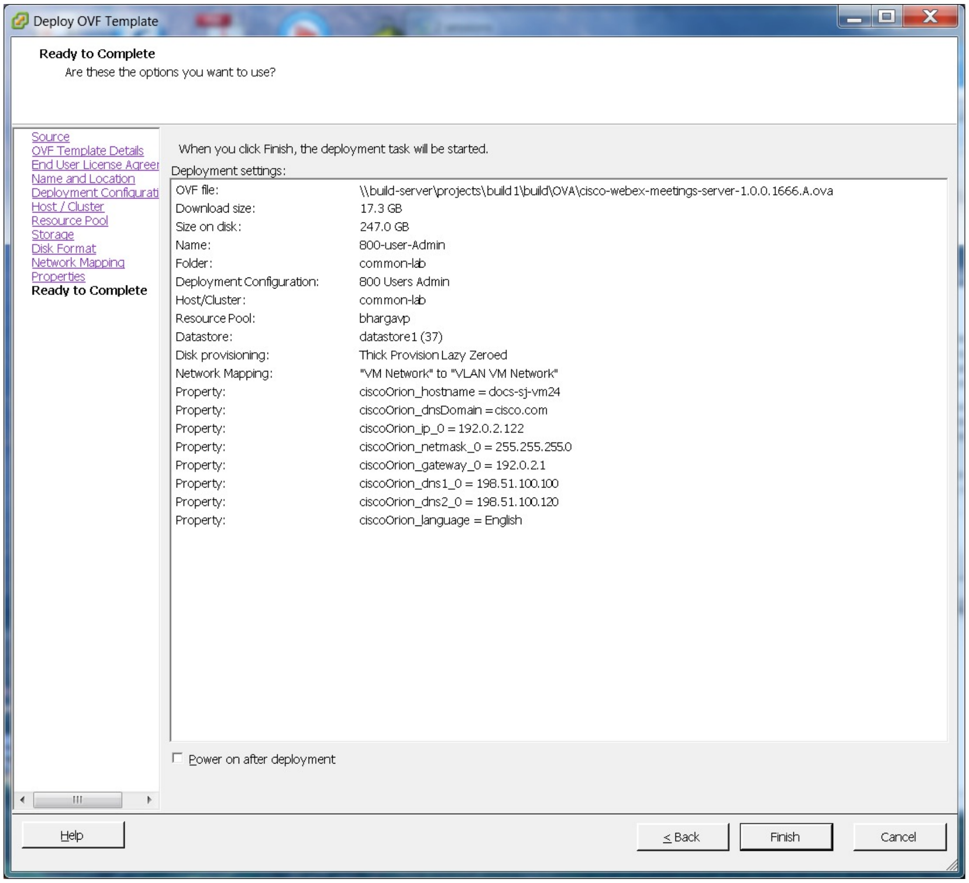
System language

String of alphanumeric characters | Required | Language displayed during the installation process, following power on of the Admin virtual machine

English

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

Step 14 Check the **Power on after deployment** check box, then select **Finish**.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	\\build-server\projects\build1\build\OVA\cisco-webex-meetings-server-1.0.0.1666.A.ova
Download size:	17.3 GB
Size on disk:	247.0 GB
Name:	800-user-Admin
Folder:	common-lab
Deployment Configuration:	800 Users Admin
Host/Cluster:	common-lab
Resource Pool:	bhargavp
Datastore:	datastore1 (37)
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"VM Network" to "VLAN VM Network"
Property:	ciscoOrion_hostname = docs-sj-vm24
Property:	ciscoOrion_dnsDomain = cisco.com
Property:	ciscoOrion_ip_0 = 192.0.2.122
Property:	ciscoOrion_netmask_0 = 255.255.255.0
Property:	ciscoOrion_gateway_0 = 192.0.2.1
Property:	ciscoOrion_dns1_0 = 198.51.100.100
Property:	ciscoOrion_dns2_0 = 198.51.100.120
Property:	ciscoOrion_language = English

☐ Power on after deployment

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 check mark is displayed.
- If there is a problem, a red X mark is displayed. Fix the error and reattempt the OVA deployment.

Step 16 Once 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 rebooted 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 doing a manual deployment, then you may choose to deploy all the virtual machines for your system at this time.
- If the deployment is successful, then continue with system deployment in a browser window.
- If the deployment has failed, see Checking Your Networking Configuration After a Failed OVA Deployment, on page 28

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 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

Determine how you want to deploy any other virtual machines that are required for your system. If you selected a 2000 user system, then you must select a manual deployment.

Procedure

Step 1 Select whether you want to deploy the virtual machines yourself, or you want us to deploy them for you.

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

  Note By using Cisco WebEx Administration, you can still make changes to your system, following deployment.

- **Manual**: You must manually deploy each virtual machine using VMware vCenter. After answering a few more questions about your system, we will provide a list of virtual machines required for your system.

Your decision about 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, then select an automatic deployment.
- If you are familiar with VMware vCenter and do not want to provide your vCenter credentials, then select manual deployment.

Step 2 Select **Next**.

Providing VMware vCenter Credentials

If you select an automatic deployment, then we require your vCenter credentials to deploy the virtual machines for you.

Before You Begin

Note the following:

- All the virtual machines for your system must belong to the same VMware vCenter.
- The vCenter username and password you enter below must include administrator privileges: to deploy, configure, power on and off, and delete virtual machines.

Procedure

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

Step 2 Enter the username that we will use to deploy the virtual machines.

Step 3 Enter the password for the username entered previously.

Step 4 Confirm that you entered the vCenter information correctly and 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, we will attempt to populate the networking information for you.

Note The media virtual machine must be on the same subnet as the Admin virtual machine. Therefore, you cannot edit the domain, IPv4 gateway, subnet mask, and 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. We will look up and populate the **Ipv4 Address** field.

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 your Internet Reverse Proxy, on page 32
- Without public access: Entering the Private VIP Address, on page 33

Choosing vCenter Settings for your Internet Reverse Proxy

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

Although this is not mandated, for security reasons, Cisco recommends that you place the Internet Reverse Proxy on a different subnet from the Admin virtual machine. This ensures network level isolation between the Internet Reverse Proxy and your internal (Admin and media, if applicable) virtual machines. This is a good security practice for isolating your DMZ network from your internal network.

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 the Networking Information for the Internet Reverse Proxy

The Internet Reverse Proxy enables users to host or attend meetings from the Internet or mobile devices. Cisco recommends you use a different subnet than your internal (Admin and media, if applicable) virtual machines.

Before You Begin

- For security reasons, Cisco recommends the Internet Reverse Proxy should be located on your DMZ network.

- Enter the hostname and IP address of the Internet Reverse Proxy in your DNS servers to enable lookup from an external network.

Note If you have DNS servers that enable look up from internal networks, then 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 (Admin, and media, if applicable) and the Internet Reverse Proxy.

- Enter the following for the Internet Reverse Proxy and select **Next**:
    - ◦ 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

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. 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

- 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.

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.

- Enter the following secure (https) URLs and select **Next**.
  - WebEx site URL for users to host and attend meetings
  - WebEx Administration URL for system administrators to manage your system

Confirming That Your 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.

Note You must make the necessary DNS server and firewall changes, as we will test network connectivity in the next step.

- If you have not done so already, complete the networking configuration and select **Next**.
  Once you select **Next**:
  - Automatic deployment: We will start deploying the virtual machines required for your system.
  - Manual deployment: On the next screen, you will enter the hostnames for your virtual machines and deploy them, if you have not deployed them already. If you have already deployed them, then power them on and verify all the virtual machines power on successfully.

Deploying Your Virtual Machines

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

Note The deployment takes several minutes to complete. Do not leave this page until all the virtual machines have deployed and powered on successfully, or the deployment failed, with error messages indicating the problem.

- Complete one of the following
  - ◦ If there are no errors, then when the status shows all green checks, select **Next.**
  - ◦ If you see errors, fix the errors and select **Next**.

Note You may want to select **Download log file** to obtain the log file for this deployment. This enables you to have a record of the deployment, which you may use to troubleshoot a failed deployment.

Note Before redoing the deployment, be sure to power off and delete any virtual machines with errors. Otherwise, you may see error messages about existing virtual machines when you redo the system deployment.

Checking Your System

Based on the information you entered earlier, we are checking the configuration of your system. We are confirming that the virtual machines have the required minimum configuration, and are validating the WebEx site and WebEx Administration URLs.

Note 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, with error messages indicating the problem.

Note If you reload the page before the checks have completed, you will be returned to the first page of this system deployment. However, if the checks have completed, you are taken to the first page of basic configuration (where you set up the mail server and an administrator).

- Complete one of the following:
    - If there are no errors, then when the status shows all green checks, select **Next**. Continue with Setting Up the Mail Server For Your System, on page 63.
    - If there is a problem with network connectivity, then check that your WebEx Site and Administration URLs and IP addresses were entered correctly. Check that these sites are in the correct subnet, and have been entered in your DNS servers correctly.
    - If there are problems with your system meeting the minimum system capacity, then you have two choices.
        - We recommend you power down all the virtual machines from VMware vCenter and manually delete them. Then reattempt the system deployment on a system with resources that meet or exceed the minimum requirements.
        - You may choose to proceed with your current installation. If you do you, 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 other problems with one or more of your virtual machines, then from VMware vCenter, power off these virtual machines with errors and manually delete them. Then reattempt the system deployment after fixing the problems.

Note Before redoing the deployment, be sure to power off and delete any virtual machines with errors. Otherwise, you may see error messages about existing virtual machines when you redo the system deployment.

-
    - In rare cases, you may see **Not tested**.
      This does not mean that there is any problem with your virtual machines. It simply states that we did not complete system checks; for example, due to a temporary loss of network connectivity. Once you complete the deployment, you can sign in to the Administration site and check these resources.

- Select **Continue** to go to the first page of basic configuration (where you set up the mail server and an administrator). If another administrator will do the basic configuration, then write down and send this URL to the software administrator.

CHAPTER 4

Installing Your System Using Manual Deployment

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

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.

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)	

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 for users to host and attend meetings.	
WebEx Administration URL	Secure http URL 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 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 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 may differ slightly from this procedure. See your VMware vSphere documentation for complete information on the OVA wizard.

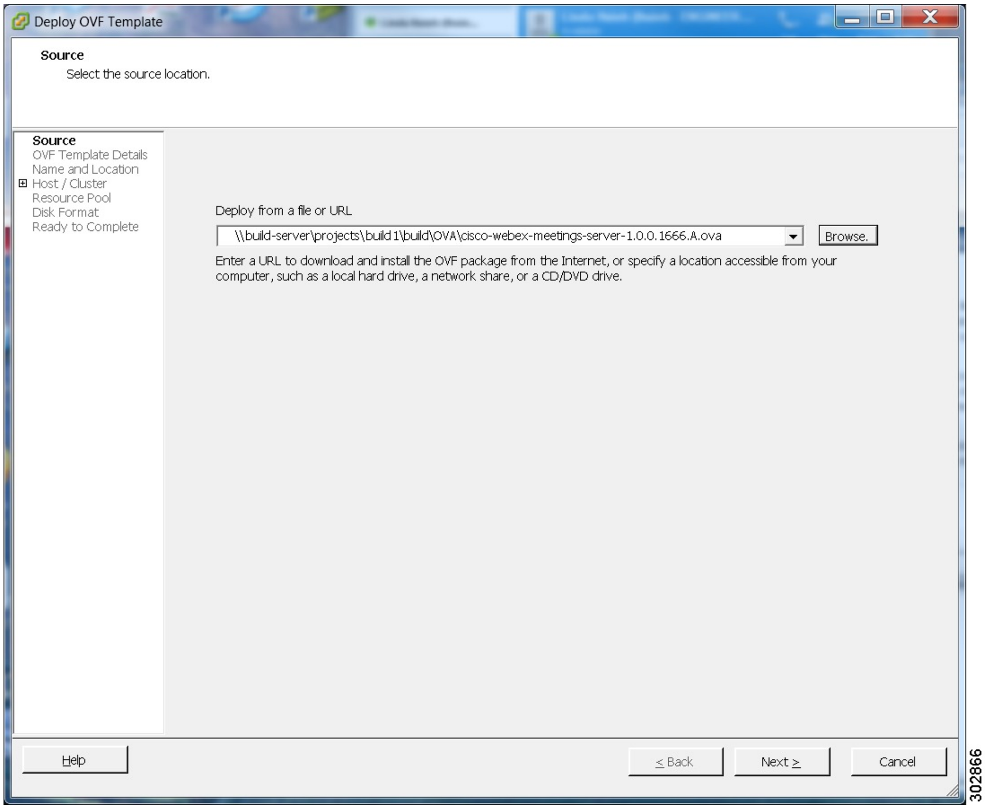
Before You Begin

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

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 and off, and delete virtual machines.

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



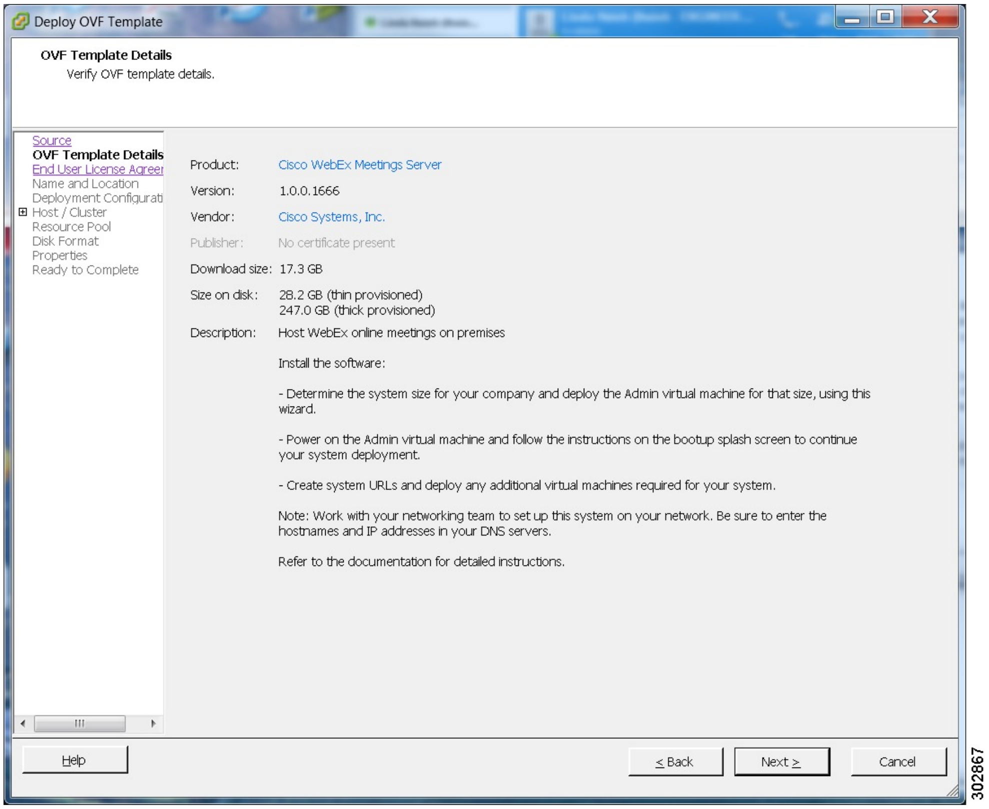
Source
Select the source location.

Deploy from a file or URL

\\build-server\projects\build 1\build\OVA\cisco-webex-meetings-server-1.0.0.1666.A.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

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



Deploy OVF Template

OVF Template Details

Verify OVF template details.

Product: Cisco WebEx Meetings Server

Version: 1.0.0.1666

Vendor: Cisco Systems, Inc.

Publisher: No certificate present

Download size: 17.3 GB

Size on disk: 28.2 GB (thin provisioned)
247.0 GB (thick provisioned)

Description: Host WebEx online meetings on premises

Install the software:

- Determine the system size for your company and deploy the Admin virtual machine for that size, using this wizard.

- Power on the Admin virtual machine and follow the instructions on the bootup splash screen to continue your system deployment.

- Create system URLs and deploy any additional virtual machines required for your system.

Note: Work with your networking team to set up this system on your network. Be sure to enter the hostnames and IP addresses in your DNS servers.

Refer to the documentation for detailed instructions.

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

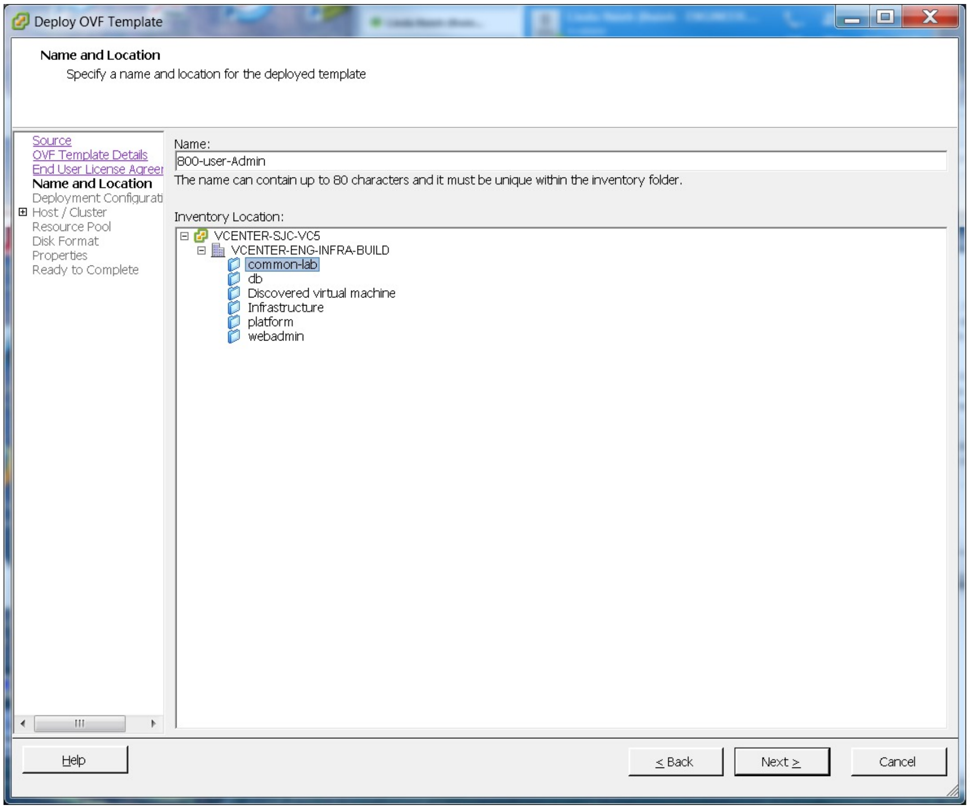
Step 5 Navigate to, and select the location, in the vCenter inventory, where you'd like to place the Admin virtual machine.

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, on page 12.

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

Cisco recommends you include the type in the virtual machine name; for example, "Admin" in your Admin virtual machine name, to identify it easily 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 may need one or more media and web internal virtual machines.)



Name and Location

Specify a name and location for the deployed template

Name:

800-user-Admin

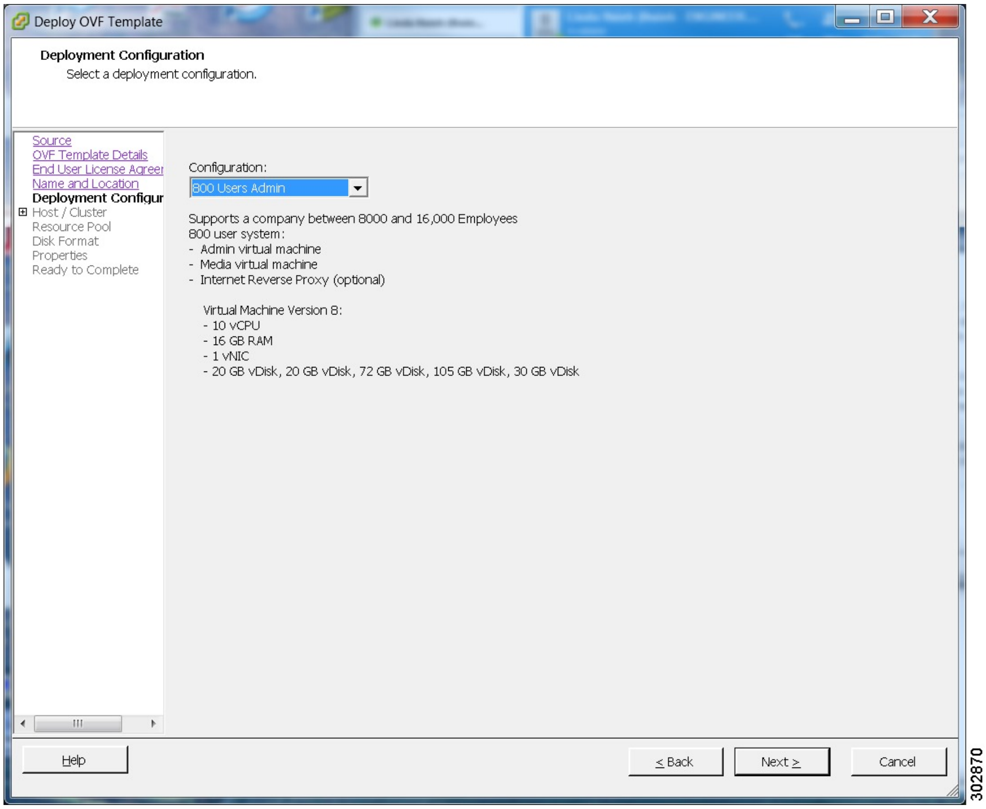
The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:

- VCENTER-SJC-VC5
  - VCENTER-ENG-INFRA-BUILD
    - common-lab
    - db
    - Discovered virtual machine
    - Infrastructure
    - platform
    - webadmin

302869

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



Deployment Configuration

Select a deployment configuration.

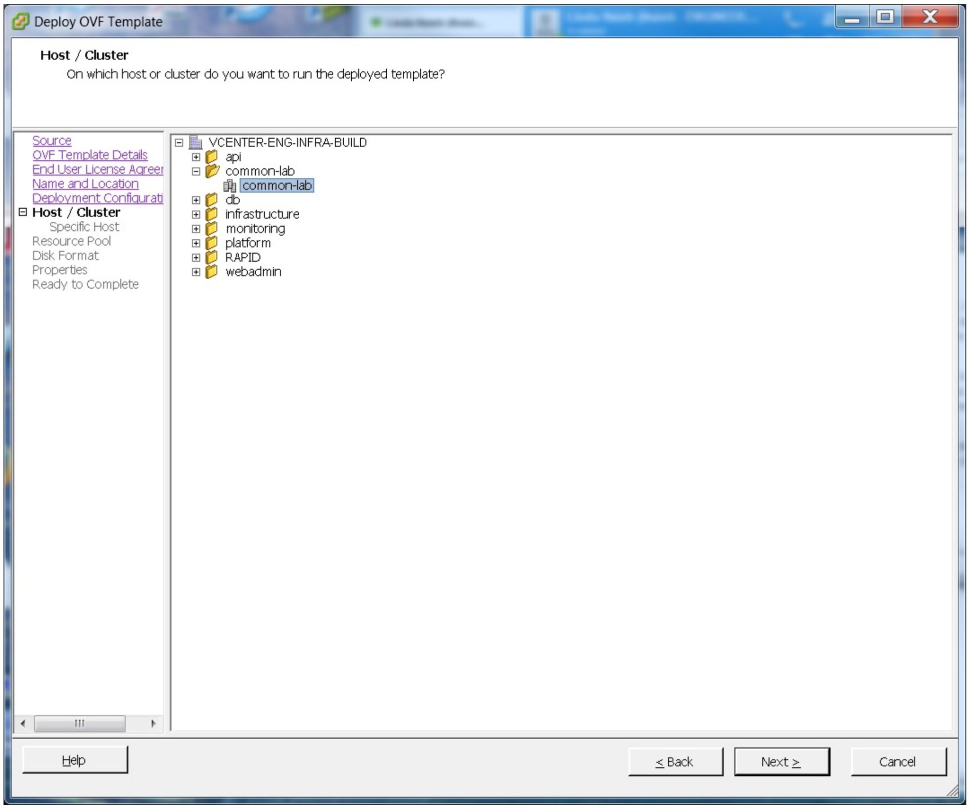
Configuration:

800 Users Admin

Supports a company between 8000 and 16,000 Employees
800 user system:
- Admin virtual machine
- Media virtual machine
- Internet Reverse Proxy (optional)

Virtual Machine Version 8:
- 10 vCPU
- 16 GB RAM
- 1 vNIC
- 20 GB vDisk, 20 GB vDisk, 72 GB vDisk, 105 GB vDisk, 30 GB vDisk

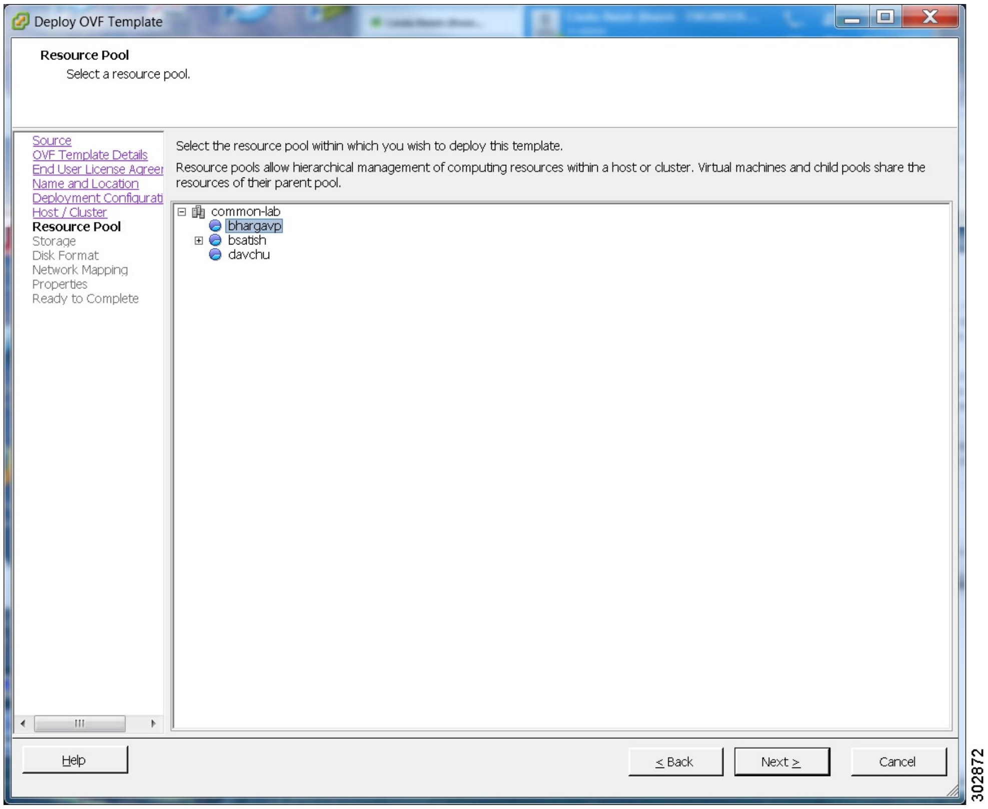
Step 8 Navigate thru the vCenter inventory and select the ESXi host or cluster where you want to deploy the virtual machines for your system. Select **Next**.



Host / Cluster

On which host or cluster do you want to run the deployed template?

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



Resource Pool

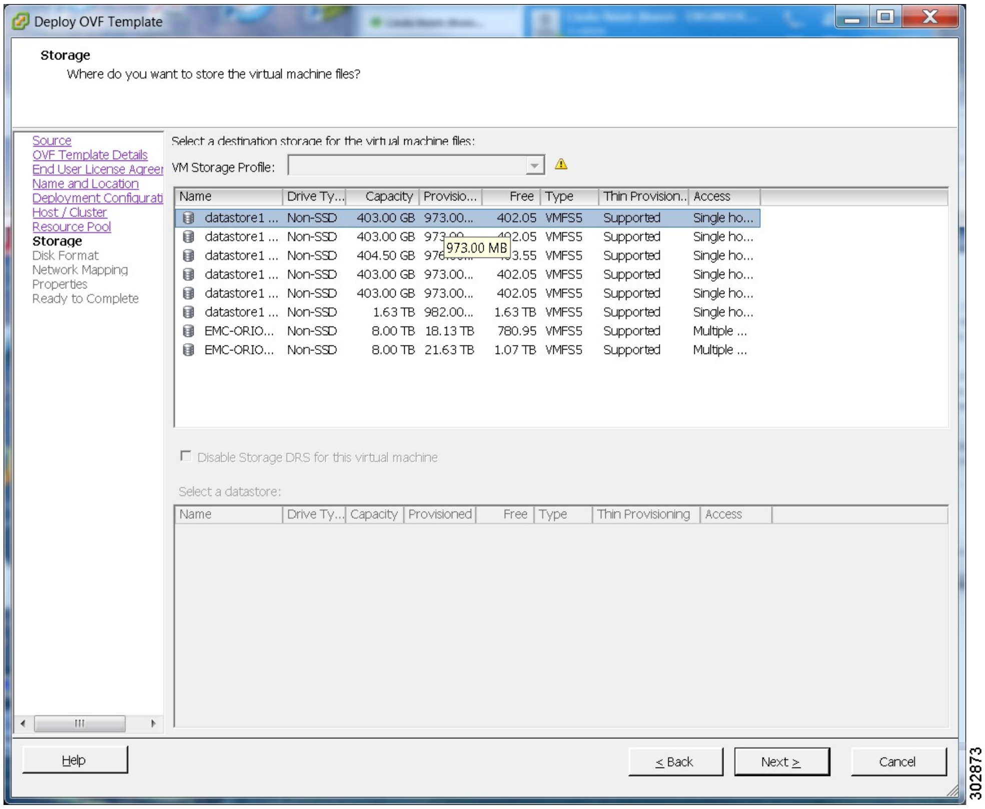
Select a resource pool.

Select the resource pool within which you wish to deploy this template.

Resource pools allow hierarchical management of computing resources within a host or cluster. Virtual machines and child pools share the resources of their parent pool.

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 Provision**, VMware allocates the file system space on an "as-needed" basis, resulting in poor performance.



Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

VM Storage Profile:

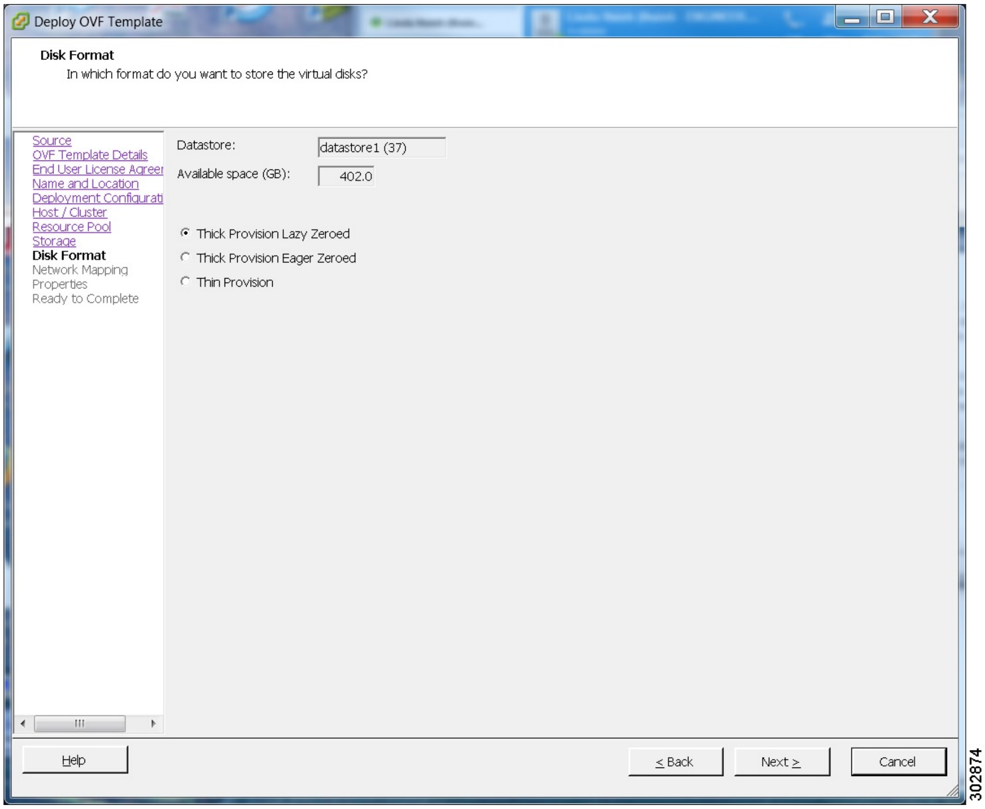
Name	Drive Ty...	Capacity	Provisio...	Free	Type	Thin Provision...	Access
datastore1 ...	Non-SSD	403.00 GB	973.00...	402.05	VMFS5	Supported	Single ho...
datastore1 ...	Non-SSD	403.00 GB	973.00...	402.05	VMFS5	Supported	Single ho...
datastore1 ...	Non-SSD	404.50 GB	976...	403.55	VMFS5	Supported	Single 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



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1 (37)

Available space (GB): 402.0

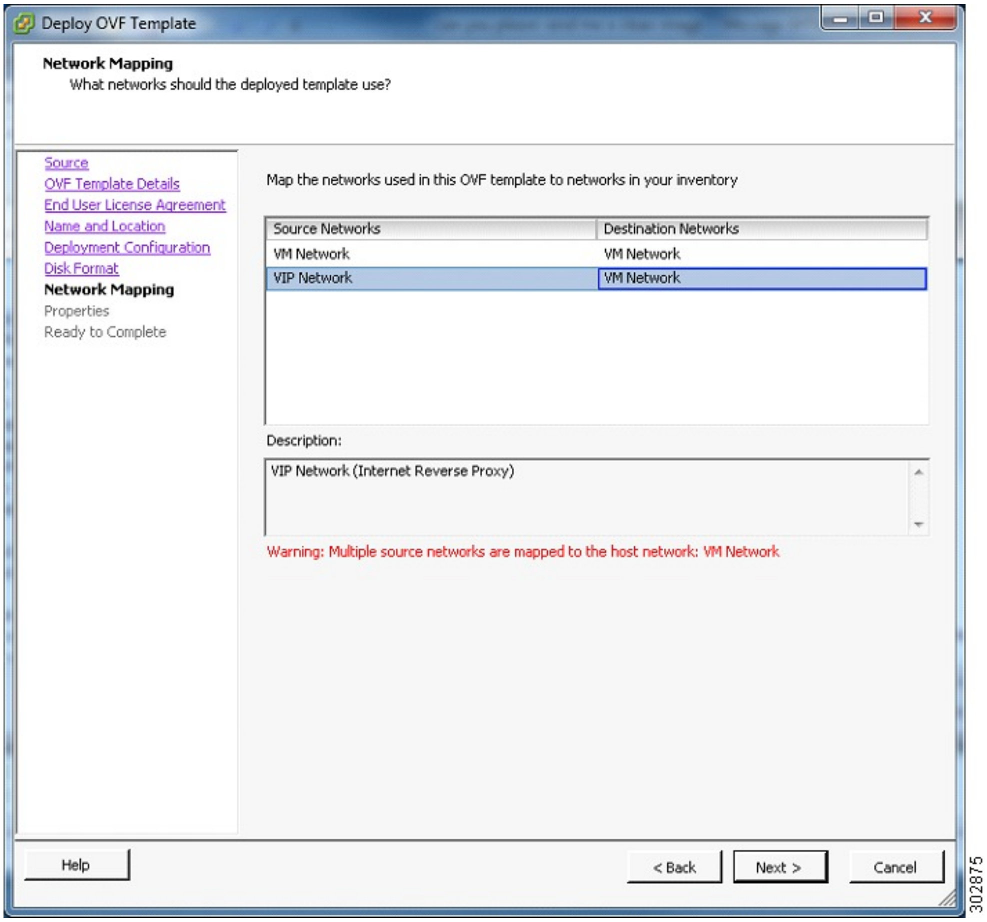
● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

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.



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	VM Network
VIP Network	VM Network

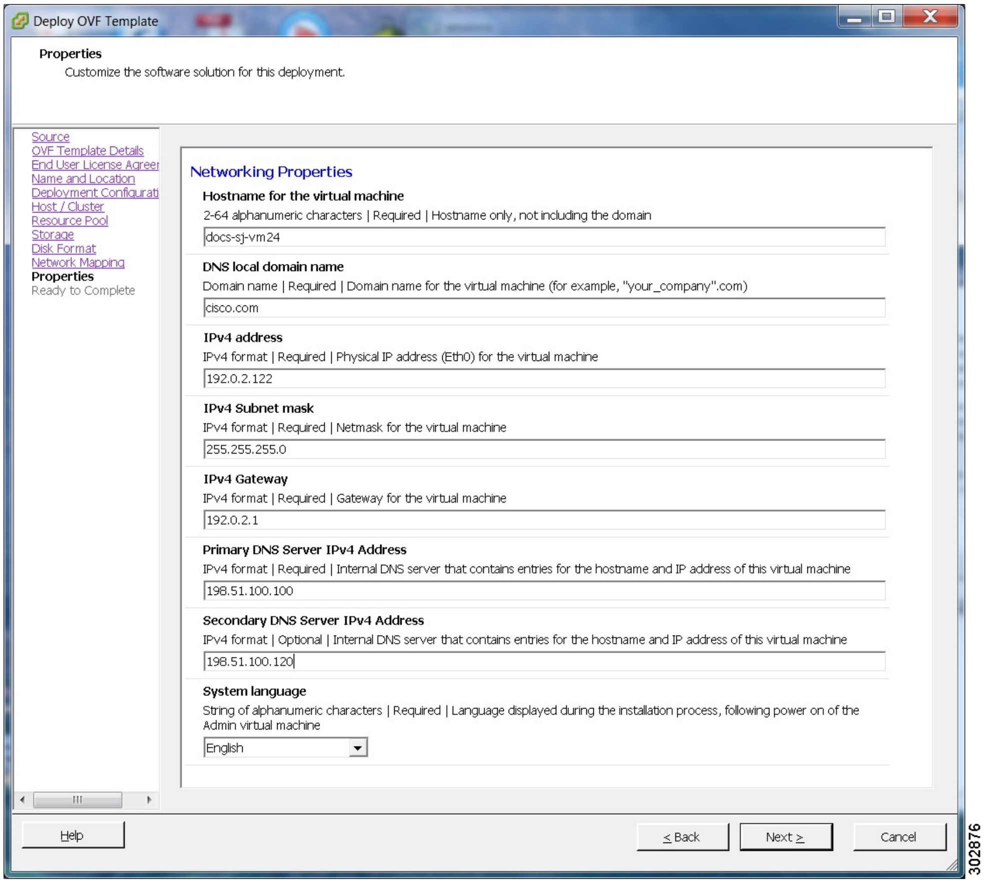
Description:

VIP Network (Internet Reverse Proxy)

Warning: Multiple source networks are mapped to the host network: VM Network

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

- Hostname of the virtual machine (do not include the domain as you will enter this in the next field)
- 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



Properties

Customize the software solution for this deployment.

Networking Properties

Hostname for the virtual machine

2-64 alphanumeric characters | Required | Hostname only, not including the domain

docs-sj-vm24

DNS local domain name

Domain name | Required | Domain name for the virtual machine (for example, "your_company".com)

cisco.com

IPv4 address

IPv4 format | Required | Physical IP address (Eth0) for the virtual machine

192.0.2.122

IPv4 Subnet mask

IPv4 format | Required | Netmask for the virtual machine

255.255.255.0

IPv4 Gateway

IPv4 format | Required | Gateway for the virtual machine

192.0.2.1

Primary DNS Server IPv4 Address

IPv4 format | Required | Internal DNS server that contains entries for the hostname and IP address of this virtual machine

198.51.100.100

Secondary DNS Server IPv4 Address

IPv4 format | Optional | Internal DNS server that contains entries for the hostname and IP address of this virtual machine

198.51.100.120

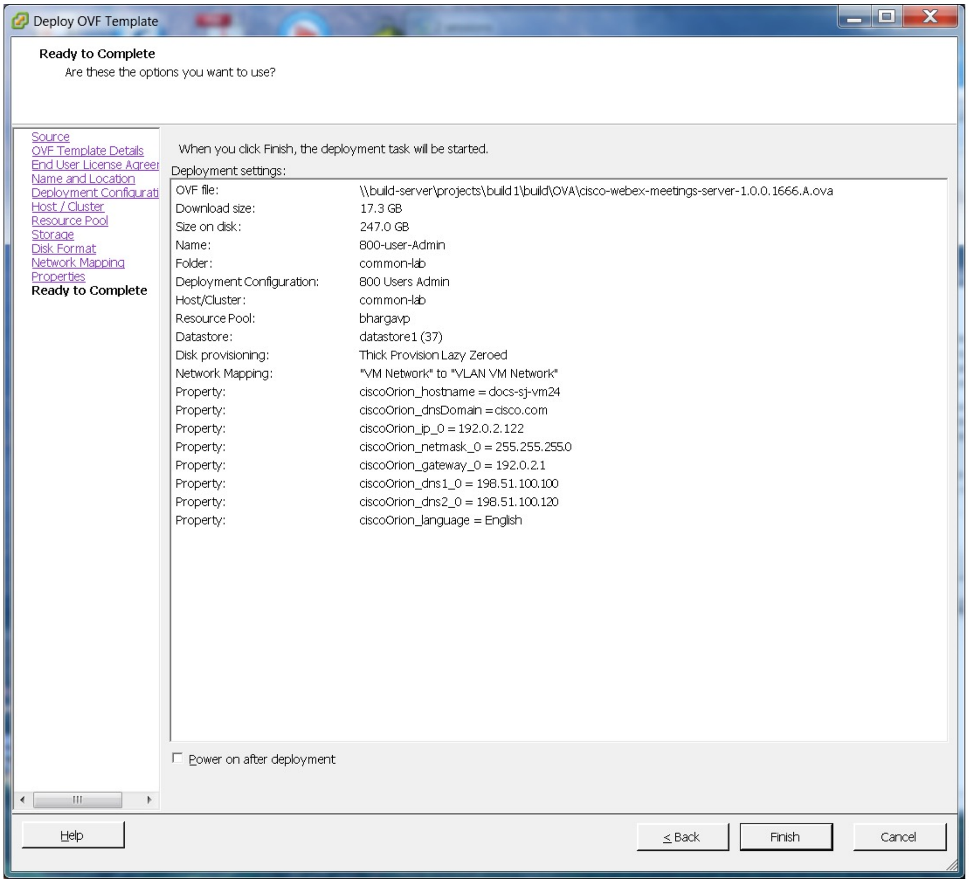
System language

String of alphanumeric characters | Required | Language displayed during the installation process, following power on of the Admin virtual machine

English

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

Step 14 Check the **Power on after deployment** check box, then select **Finish**.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	\\build-server\projects\build1\build\OVA\cisco-webex-meetings-server-1.0.0.1666.A.ova
Download size:	17.3 GB
Size on disk:	247.0 GB
Name:	800-user-Admin
Folder:	common-lab
Deployment Configuration:	800 Users Admin
Host/Cluster:	common-lab
Resource Pool:	bhargavp
Datastore:	datastore1 (37)
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"VM Network" to "VLAN VM Network"
Property:	ciscoOrion_hostname = docs-sj-vm24
Property:	ciscoOrion_dnsDomain = cisco.com
Property:	ciscoOrion_ip_0 = 192.0.2.122
Property:	ciscoOrion_netmask_0 = 255.255.255.0
Property:	ciscoOrion_gateway_0 = 192.0.2.1
Property:	ciscoOrion_dns1_0 = 198.51.100.100
Property:	ciscoOrion_dns2_0 = 198.51.100.120
Property:	ciscoOrion_language = English

□ Power on after deployment

302877

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 check mark is displayed.
- If there is a problem, a red X mark is displayed. Fix the error and reattempt the OVA deployment.

Step 16 Once 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 rebooted 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 doing a manual deployment, then you may choose to deploy all the virtual machines for your system at this time.
- If the deployment is successful, then continue with system deployment in a browser window.
- If the deployment has failed, see Checking Your Networking Configuration After a Failed OVA Deployment, on page 28

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 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

Determine how you want to deploy any other virtual machines that are required for your system. If you selected a 2000 user system, then you must select a manual deployment.

Procedure

Step 1 Select whether you want to deploy the virtual machines yourself, or you want us to deploy them for you.

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

  Note By using Cisco WebEx Administration, you can still make changes to your system, following deployment.

- **Manual**: You must manually deploy each virtual machine using VMware vCenter. After answering a few more questions about your system, we will provide a list of virtual machines required for your system.

Your decision about 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, then select an automatic deployment.
- If you are familiar with VMware vCenter and do not want to provide your vCenter credentials, then 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 your Internet Reverse Proxy, on page 32
- Without public access: Entering the Private VIP Address, on page 33

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. 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

- 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.

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.

- Enter the following secure (https) URLs and select **Next**.
    - WebEx site URL for users to host and attend meetings
    - WebEx Administration URL for system administrators to manage your system

Confirming That Your 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.

Note You must make the necessary DNS server and firewall changes, as we will test network connectivity in the next step.

- If you have not done so already, complete the networking configuration and select **Next**.
  Once you select **Next**:
    - Automatic deployment: We will start deploying the virtual machines required for your system.
    - Manual deployment: On the next screen, you will enter the hostnames for your virtual machines and deploy them, if you have not deployed them already. If you have already deployed them, then power them on and verify all the virtual machines power on successfully.

Deploying Your 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 your system.

Step 3 Power on all these virtual machines and verify that they powered on successfully. Then select **Detect virtual machines**.
We are attempting to connect to these virtual machines. This may take several minutes.

Step 4 Wait until **Connected** status is displayed for all the virtual machines, then complete one of the following

- If there are no errors, then the status shows all green checks. If you are satisfied, select **Next**. Otherwise, you may still change the FQDNs of the virtual machines, then select **Detect virtual machines** again.
- If you see errors, fix the errors and select **Next**.
  Note You may want to select **Download log file** to obtain the log file for this deployment. This enables you to have a record of the deployment, which you may use to troubleshoot a failed deployment.
- If there are other problems with one or more of your virtual machines, then from VMware vCenter, power off these virtual machines with errors and manually delete them. After fixing the problems, redeploy the virtual machines from the OVA file, then select **Detect virtual machines**.
  Note Before redoing the deployment, be sure to power off and delete any virtual machines with errors. Otherwise, you may see error messages about existing virtual machines.

Checking Your System

Based on the information you entered earlier, we are checking the configuration of your system. We are confirming that the virtual machines have the required minimum configuration, and are validating the WebEx site and WebEx Administration URLs.

Note 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, with error messages indicating the problem.

Note If you reload the page before the checks have completed, you will be returned to the first page of this system deployment. However, if the checks have completed, you are taken to the first page of basic configuration (where you set up the mail server and an administrator).

- Complete one of the following:
  - If there are no errors, then when the status shows all green checks, select **Next**. Continue with Setting Up the Mail Server For Your System, on page 63.
  - If there is a problem with network connectivity, then check that your WebEx Site and Administration URLs and IP addresses were entered correctly. Check that these sites are in the correct subnet, and have been entered in your DNS servers correctly.
  - If there are problems with your system meeting the minimum system capacity, then you have two choices.
    - We recommend you power down all the virtual machines from VMware vCenter and manually delete them. Then reattempt the system deployment on a system with resources that meet or exceed the minimum requirements.
    - You may choose to proceed with your current installation. If you do you, 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 other problems with one or more of your virtual machines, then from VMware vCenter, power off these virtual machines with errors and manually delete them. Then reattempt the system deployment after fixing the problems.

Note Before redoing the deployment, be sure to power off and delete any virtual machines with errors. Otherwise, you may see error messages about existing virtual machines when you redo the system deployment.

  - In rare cases, you may see **Not tested**.
    This does not mean that there is any problem with your virtual machines. It simply states that we did not complete system checks; for example, due to a temporary loss of network connectivity. Once you complete the deployment, you can sign in to the Administration site and check these resources.

- Select **Continue** to go to the first page of basic configuration (where you set up the mail server and an administrator). If another administrator will do the basic configuration, then write down and send this URL to the software administrator.

CHAPTER 5

Configuring Your Mail Server, Time Zone, and Locale

Setting Up the Mail Server For Your System

By setting up this mail server, the system can use your corporate mail server to send emails to administrators (alerts, alarms, reports, and so on) and users (meeting invitations, password resets, and so on).

Before You Begin

You must have successfully completed the deployment of the virtual machines required for your system.

Procedure

Step 1 Enter the fully qualified domain name (FQDN) of a mail server that the system will use to send emails.

Step 2 If you want **TLS enabled**, then check this check box.

Step 3 You may edit the **Port** field if you do not want to use the default value.
By default, the SMTP port number is 25, or 465 (secure SMTP port number).

Note If there is a firewall between the internal virtual machines and the mail server, then these ports may be blocked. To ensure mail traffic can pass, make sure these ports are open between the mail server and your system.

Step 4 If you want to enable mail server authentication, check the **Server authentication enabled** check box.
If you enable server authentication, then the **Username** and **Password** fields are displayed.

Step 5 If displayed, enter the **Username** and **Password** credentials for the system to access your corporate mail server.

Emails from the system are sent by admin@<WebEx-site-URL>. Ensure that the mail server can recognize this user.

Step 6 Select **Next**.

Setting Up the Time Zone and Locale for the System

Procedure

Step 1 Select the local time zone for your system from the drop-down list.

Step 2 Select the country locale for your system from the drop-down list.

Step 3 Select **Next**.

Confirming the Mail Server, Time Zone, and Locale Settings

You entered these settings on the previous screens.

- Review the information you entered previously. If there are any mistakes, then select **Back**. Otherwise, select **Next**.

Setting Up the First Administrator Account for Your System

The system creates a single administrator account as part of the deployment process. This administrator will receive an activation email from the system, requesting a sign in and creation of a password.

Caution This administrator must sign into the system, create a password, and add additional administrators and users. Otherwise, no other user will have access to the system.

Before You Begin

You must have correctly set up a mail server for the system to send emails to administrators and users.

Procedure

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

Step 2 Enter the administrator's complete email address.

Step 3 Select **Submit**.

Depending on your network speed and mail server, the administrator will receive a welcome email in under 15 minutes, asking the administrator to confirm the account by signing in to the system and creating a password. After sign in, the administrator can view a tutorial that explains how to use the system.

Step 4 We recommend you keep this page open until the administrator receives the activation email. Be sure to bookmark this **Email Confirmation** page as well. You may use the bookmark to return to this page to resend the email, if necessary. Otherwise, you will be unable to resend the activation email.
If the administrator does not receive that email, it may be an issue with your corporate mail server or the activation email may have gone into the junk or spam email folder.

Important Without an activation email, no one will be able to sign in to the system, forcing a redo of the system deployment.

Step 5 The administrator must sign in to the system and add additional users. Upon creation of the new user, the system sends an email to each user, welcoming and asking the user to sign in and create a password.
Upon initial sign in, each administrator will have an opportunity to view a tutorial of the system. The administrators can view the tutorial immediately, or decide to view it later.

Testing the System

These are some of the tests to run on 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, and 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.

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, then you will need to redeploy the HA system again, following the upgrade.

  System expansions or upgrades requires the deployment of a new system, with the transfer of the system data 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 a HA system, as well as update it (with an ISO update file), then we recommend you first add the HA system, then update the combined (primary and HA) system.

  The update procedure updates the entire system, with or without a HA system. If you update the system first, then to add HA, you first need to deploy the HA system, then update the HA system (so both the primary and HA systems are at the same version). If you add HA first, then the update procedure updates the combined primary and HA system at the same time.

- 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 on.

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

Step 4 Once all the virtual machines are powered off, then use VMware Data Recovery to create a backup of each of your virtual machines.
A backup will help you revert your virtual machine to its state before the update. For further information, see Creating a Backup Using VMware vCenter, on page 4. For complete details on this backup, see the *VMware Data Recovery Administration Guide*.

Note You may also take snapshots, but you must delete these in approximately 24 hours, or you may experience data performance issues, common to virtual machine snapshots. For more information, see Taking a Snapshot Using VMware vCenter, on page 5.

Step 5 In the VMware vSphere client, power on each of the virtual machines in your system.

Step 6 Sign back in to the Cisco WebEx Administration site, but do not turn off maintenance mode.

Step 7 Continue with the system-altering procedure.

CHAPTER 7

Adding a High Availability System

Adding a HA System Using Automatic Deployment

Before You Begin

- You must have successfully deployed a primary system.
- The primary system is in maintenance mode.
- Create a backup of both the primary and HA systems. See Creating a Backup Using VMware vCenter, on page 4.

Considerations Before Adding a High Availability System

A high availability system is a redundant system that is added to, and becomes part of your system. It provides high availability in the event of a virtual machine failure.

The High Availability (HA) system has the following constraints

- The HA system must be at the same release version as the primary system.

  If you have updated the primary system, then be sure to do the same for the HA system.
- If you are entitled (with the appropriate service contract), then Cisco recommends you deploy the HA system using the OVA file that is the same base version (before any patches) as the primary system.
- The HA system size must be the same as the primary system.
- If you have added public access on the primary system, then you must add it to the HA system as well.

- The HA system's internal virtual machines must be on the same subnet as the primary system's internal virtual machines.
- If you have added public access, then the HA system's Internet Reverse Proxy virtual machine must be on the same subnet as the primary system's Internet Reverse Proxy virtual machine.
- Because this process affects the virtual machines in your system, your current security certificate may become invalid and require an update.
- If you previously had an HA system, removed it, and are redeploying a new HA system, then you will not be able to reuse the virtual machines in the previous HA system. You must redeploy a new HA system with new virtual machines.

Summary of Tasks to Add a High Availability System Using Automatic Deployment

Follow these tasks in order.

Task	Description	For Details, See
1	Using the VMware vSphere client, deploy the Admin virtual machine for the HA system.	Deploying the OVA File From the VMware vSphere Client, on page 16
2	Power on the Admin virtual machine of the HA system, and write down the deployment URL.	
3	Enter the URL into a web browser and continue the deployment of your HA system.	
4	Select your preferred language for the deployment of the HA system.	Selecting Your Language for Setup, on page 28
5	Confirm the system size for the HA system. (This system size must match the primary system.)	Confirming the Size of Your System, on page 29
6	Select **Create a High Availability (HA) redundant system**.	Choosing What System to Install, on page 29
7	Select an automatic deployment. (For simplicity, Cisco recommends making the same selection as for your primary system.)	Choosing the Type of System Deployment, on page 29
8	Enter your vCenter credentials so that we may deploy the HA system's virtual machines for you.	Providing VMware vCenter Credentials, on page 30
9	As applicable, select the ESXi host, datastore, and virtual machine port group for the media virtual machine for the HA system. **Note** Choose the same virtual machine port group as used for the primary system.	Choosing vCenter Settings for your Media Virtual Machine, on page 31
10	As applicable, enter the fully qualified domain name of the HA system's media virtual machine. (If you have already updated your DNS server with entries for the HA system, then we will look up the IP address for you.)	Entering Networking Information for the Media Virtual Machine, on page 31

Task	Description	For Details, See
11	If you have added public access for your primary 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, then skip to Task 14.	Adding Public Access, on page 31
12	If you have added public access, select the ESXi host, datastore, and virtual machine port group for the Internet Reverse Proxy virtual machine for the HA system. **Note** Choose the same virtual machine port group as used for the primary system.	Choosing vCenter Settings for your Internet Reverse Proxy, on page 32
13	Enter the hostname and networking information for the Internet Reverse Proxy.	Entering the Networking Information for the Internet Reverse Proxy, on page 32
14	Check that you have made all the networking, DNS server, and firewall configuration changes required for your HA system.	Confirming That Your Network is Configured Correctly, on page 36
15	Once your HA system's virtual machines have deployed successfully, then select **Next** to continue to the HA system check.	Deploying Your Virtual Machines, on page 36
16	Once the HA system check has completed successfully, then select **Next**.	Checking Your System, on page 37
17	Confirm that the primary system and the HA system are at the same version. If not, then update the HA system.	Confirming Your Primary System and Your HA System Are at the Same Version, on page 75
18	Add this high availability system to the primary system in Cisco WebEx Administration.	Adding a High Availability System, on page 76

Adding a HA System Using Manual Deployment

Before You Begin

- You must have successfully deployed a primary system.
- The primary system is in maintenance mode.
- Create a backup of both the primary and HA systems. See Creating a Backup Using VMware vCenter, on page 4.

Considerations Before Adding a High Availability System

A high availability system is a redundant system that is added to, and becomes part of your system. It provides high availability in the event of a virtual machine failure.

The High Availability (HA) system has the following constraints

- The HA system must be at the same release version as the primary system.

  If you have updated the primary system, then be sure to do the same for the HA system.
- If you are entitled (with the appropriate service contract), then Cisco recommends you deploy the HA system using the OVA file that is the same base version (before any patches) as the primary system.
- The HA system size must be the same as the primary system.
- If you have added public access on the primary system, then you must add it to the HA system as well.
- The HA system's internal virtual machines must be on the same subnet as the primary system's internal virtual machines.
- If you have added public access, then the HA system's Internet Reverse Proxy virtual machine must be on the same subnet as the primary system's Internet Reverse Proxy virtual machine.
- Because this process affects the virtual machines in your system, your current security certificate may become invalid and require an update.
- If you previously had an HA system, removed it, and are redeploying a new HA system, then you will not be able to reuse the virtual machines in the previous HA system. You must redeploy a new HA system with new virtual machines.

Summary of Tasks to Add a High Availability System Using Manual Deployment

Follow these tasks in order.

Task	Description	For Details, See
1	Using the VMware vSphere client, deploy the Admin virtual machine for the HA system.	Deploying the OVA File From the VMware vSphere Client, on page 16
2	Power on the Admin virtual machine of the HA system, and write down the deployment URL.	
3	Enter the URL into a web browser and continue the deployment of your HA system.	
4	Select your preferred language for the deployment of the HA system.	Selecting Your Language for Setup, on page 28
5	Confirm the system size for the HA system. (This system size must match the primary system.)	Confirming the Size of Your System, on page 29
6	Select **Create a High Availability (HA) redundant system**.	Choosing What System to Install, on page 29
7	Select a manual deployment. (For simplicity, Cisco recommends making the same selection as for your primary system.)	Choosing the Type of System Deployment, on page 29
8	If you have added public access for your primary 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

Task	Description	For Details, See
9	Check that you have made all the networking, DNS server, and firewall configuration changes required for your HA system.	Confirming That Your Network is Configured Correctly, on page 36
10	Once your HA system's virtual machines have deployed successfully, then select **Next** to continue to the HA system check.	Deploying Your Virtual Machines, on page 60
11	Once the HA system check has completed successfully, then select **Next**.	Checking Your System, on page 37
12	Confirm that the primary system and the HA system are at the same version. If not, then update the HA system.	Confirming Your Primary System and Your HA System Are at the Same Version, on page 75
13	Add this high availability system to the primary system in Cisco WebEx Administration.	Adding a High Availability System, on page 76

Confirming Your Primary System and Your HA System Are at the Same Version

The HA system must be at exactly the same release as your primary system. The version of the HA system is listed on this browser page. To check the version of the primary system, complete the following on the primary system:

Procedure

Step 1 In a separate browser window, sign in to the WebEx Administration site on the primary system.

Step 2 On the **Dashboard** tab, check the primary system version number in the **System** pane in the top right corner.

Step 3 If the primary system is at a later version than the HA system, then you will either need to redeploy the HA system using a newer OVA file (for a later version of the software), or update the HA system.

Note If you need to update the HA system, first back up the virtual machines. For complete details, see Creating a Backup Using VMware vCenter, on page 4.

Step 4 If an update is required, then after deploying the HA system, select **update** on the browser connected to the HA system.

Step 5 Download the appropriate update file from the Cisco Software Center: http://www.cisco.com/cisco/software/navigator.html

Place the update file on a local disk or on a datastore available to the HA system.

Step 6 Select **Continue** on the browser connected to the HA system.

Step 7 Connect the CD/DVD drive to the ISO update file in the Admin virtual machine of the HA system. See Connecting the Update ISO Image From the CD/DVD Drive, on page 90.

Step 8 Check the **I have connected to the ISO file and am ready to proceed** check box and 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 this browser window, as you will be unable to return to this page.

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

Step 9 Select **Restart**.
Once the system has restarted, the HA created system page is displayed, with a message indicating the success of the update.

What to Do Next

Add this high availability system to the primary system in Cisco WebEx Administration on the primary system.

Adding a High Availability System

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.

Note Complete the following procedure on the primary system.

Before You Begin

- Install Cisco WebEx on a second virtual machine from the OVA file to be used as your high availability system.

  Note Your high-availability system must be the same size as your primary system.

- Your high-availability system must be configured with the same OVA and patch as your primary system. If your primary and high-availability systems' versions do not match, you will be instructed to upgrade to the higher version.
- Copy the high-availability virtual machine fully qualified domain name (FQDN). You must know the FQDN to add your high-availability system.
- Verify that all virtual machines are functioning normally. Determine virtual machine status by viewing the System Monitor as described in About Your Dashboard, on page 105.

Procedure

Step 1 Sign in to the Administration site.

Step 2 On the primary system, in the System section, select the **View More** link.

Step 3 Select **Add High Availability System**.

Step 4 Follow the instructions on the **System Properties** page to add this HA system.

Example:

Step 5 Enter the FQDN of the Administration site virtual machine of the high-availability system and select **Continue**.
We will validate the readiness of both the primary system and the HA system for this add HA procedure.

- If both systems are ready, then you will see a green **Add** button. Do not select it until you put your system into maintenance mode.
- If either system is not ready, then you will see an error message. Fix the error and attempt the add high availability procedure again.

Step 6 Select **Turn On Maintenance Mode**, then 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 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.

Testing the System

These are some of the tests to run on 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, and 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.

CHAPTER 8

Expanding Your System to a Larger System Size

Preparing for System Expansion

This section describes the prerequisites and best practices for a system expansion.

Determining Your System's New Size

Consider the following:

- Budget for hardware
- Number of concurrent meetings, and the average size of these meetings, for the next few months and years

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 on.

⚠ **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 may 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 In the VMware vSphere client, power off each of the virtual machines in your system. Select **Power** > **Shut Down Guest** .
For complete details on using vSphere, see the VMware ESXi and vCenter Server documentation.

Step 4 Once all the virtual machines are powered off, then use VMware Data Recovery to create a backup of each of your virtual machines.
A backup will help you revert your virtual machine to its state before the update. For further information, see Creating a Backup Using VMware vCenter, on page 4. For complete details on this backup, see the *VMware Data Recovery Administration Guide*.

Note You may also take snapshots, but you must delete these in approximately 24 hours, or you may experience data performance issues, common to virtual machine snapshots. For more information, see Taking a Snapshot Using VMware vCenter, on page 5.

Step 5 In the VMware vSphere client, power on each of the virtual machines in your system.

Step 6 Sign back in to the Cisco WebEx Administration site, but do not turn off maintenance mode.

Step 7 Continue with the system-altering procedure.

Expanding the System Using Automatic Deployment

Before You Begin

In this section, we refer to the system before expansion as the "existing 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.

Other system administrators should not access the system during this procedure. If they do so, their changes are not saved, and the result may 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.

Expanding the System

The overall tasks to expand the system are:

1. Create a backup of your existing system.
2. Use the same OVA file you used to deploy your existing system and deploy the Admin virtual machine for the new system size.
3. Copy the data from your existing 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.

Considerations Before Expanding the System

Note the following:

- You may choose to reuse the same hostnames and IP addresses for the existing virtual machines in the expanded system. However, only the existing 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 existing system, then following deployment of the expanded system, you must add a new HA system. You cannot reuse the existing HA system as it is not retained, following the expansion.
- You may want to keep the existing 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 existing (pre-expansion) system.

- The internal virtual machines for the existing 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 existing system and the expanded system must be on the same subnet.
- Because this process affects the virtual machines in your system, your current security certificate may become invalid and require an update.
- Be sure the expanded system can access the disks for the existing system's Admin virtual machine. You will be copying over Hard disk 4 to the expanded system.

Summary of Tasks to Expand the System Using an Automatic Deployment

Task	Description	For Details, See
1	Prepare the existing system for expansion.	Preparing for System Expansion, on page 79
2	Prepare for a system-altering procedure.	Preparing For a System-Altering Procedure, on page 68
3	Initiate the expansion procedure from the Administration site of the existing system.	Expanding System Size, on page 133
4	Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the existing 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, on page 16
6	Attach **Hard disk 4** from the existing 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
7	Power on the Admin virtual machine for the expanded system and write down the deployment URL.	
8	Enter the deployment URL into a web browser and continue the deployment of your expanded system.	
9	Select your preferred language for the deployment of the expanded system.	Selecting Your Language for Setup, on page 28
10	Confirm the system size. (This system size must be larger than or equal to the existing system.)	Confirming the Size of Your System, on page 29
11	Select **Install a primary system**.	Choosing What System to Install, on page 29
12	Select an automatic deployment.	Choosing the Type of System Deployment, on page 29
13	Enter your vCenter credentials so that we may deploy the virtual machines for you.	Providing VMware vCenter Credentials, on page 30

Task	Description	For Details, See
14	Select the ESXi host, datastore, and virtual machine port group for the media virtual machine.	Choosing vCenter Settings for your Media Virtual Machine, on page 31
15	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, on page 31
16	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, then skip to Task 19.	Adding Public Access, on page 31
17	If you have added public access, then select the ESXi host, datastore, and virtual machine port group for the Internet Reverse Proxy virtual machine.	Choosing vCenter Settings for your Internet Reverse Proxy, on page 32
18	Enter the hostname and networking information for the Internet Reverse Proxy.	Entering the Networking Information for the Internet Reverse Proxy, on page 32
19	Enter the public VIP address for the WebEx site URL. **Note** You may enter the same public VIP address that you use for your existing 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
20	Enter the private VIP address for the WebEx Administration URL. **Note** You may enter the same private VIP address that you use for your existing 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 33
21	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 existing 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

Task	Description	For Details, See
22	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 existing 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
23	Check that you have made all the networking, DNS server, and firewall configuration changes required for your system.	Confirming That Your Network is Configured Correctly, on page 36
24	Once your virtual machines have deployed successfully, then select **Next** to continue to the system check.	Deploying Your Virtual Machines, on page 36
25	Along with the system check, we update the expanded system with any required updates to match the software version of the existing system, before expansion. (These updates may take up to an hour.) When complete, the system restarts.	Checking Your System, on page 37
26	Sign in to Cisco WebEx Administration.	
27	Test the expanded system. If the expansion is unsuccessful, then power off the expanded system and power on the existing system. Contact Cisco TAC for further assistance.	Testing the System, on page 65

Expanding the System Using Manual Deployment

Before You Begin

In this section, we refer to the system before expansion as the "existing 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.

Other system administrators should not access the system during this procedure. If they do so, their changes are not saved, and the result may 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.

Expanding the System

The overall tasks to expand the system are:

1. Create a backup of your existing system.
2. Use the same OVA file you used to deploy your existing system and deploy the Admin virtual machine for the new system size.
3. Copy the data from your existing 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.

Considerations Before Expanding the System

Note the following:

- You may choose to reuse the same hostnames and IP addresses for the existing virtual machines in the expanded system. However, only the existing 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 existing system, then following deployment of the expanded system, you must add a new HA system. You cannot reuse the existing HA system as it is not retained, following the expansion.
- You may want to keep the existing 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 existing (pre-expansion) system.
- The internal virtual machines for the existing 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 existing system and the expanded system must be on the same subnet.
- Because this process affects the virtual machines in your system, your current security certificate may become invalid and require an update.
- Be sure the expanded system can access the disks for the existing system's Admin virtual machine. You will be copying over Hard disk 4 to the expanded system.

Summary of Tasks to Expand the System Using a Manual Deployment

Task	Description	For Details, See
1	Prepare the existing system for expansion.	Preparing for System Expansion, on page 79
2	Prepare for a system-altering procedure.	Preparing For a System-Altering Procedure, on page 68

Task	Description	For Details, See
3	Initiate the expansion procedure from the Administration site of the existing system.	Expanding System Size, on page 133
4	Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the existing 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, on page 16
6	Attach **Hard disk 4** from the existing 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
7	Power on the Admin virtual machine for the expanded system and write down the deployment URL.	
8	Enter the deployment URL into a web browser and continue the deployment of your expanded system.	
9	Select your preferred language for the deployment of the expanded system.	Selecting Your Language for Setup, on page 28
10	Confirm the system size. (This system size must be larger than or equal to the existing system.)	Confirming the Size of Your System, on page 29
11	Select **Install a primary system**.	Choosing What System to Install, on page 29
12	Select a manual deployment.	Choosing the Type of System Deployment, on page 29
13	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
14	Enter the public VIP address for the WebEx site URL. **Note** You may enter the same public VIP address that you use for your existing 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
15	Enter the private VIP address for the WebEx Administration URL. **Note** You may enter the same private VIP address that you use for your existing 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 33

Task	Description	For Details, See
16	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 existing 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
17	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 existing 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
18	Check that you have made all the networking, DNS server, and firewall configuration changes required for your system.	Confirming That Your Network is Configured Correctly, on page 36
19	Once your virtual machines have deployed successfully, then select **Next** to continue to the system check.	Deploying Your Virtual Machines, on page 60
20	Along with the system check, we update the expanded system with any required updates to match the software version of the existing system, before expansion. (These updates may take up to an hour.) When complete, the system restarts.	Checking Your System, on page 37
21	Sign in to Cisco WebEx Administration.	
22	Test the expanded system. If the expansion is unsuccessful, then power off the expanded system and power on the existing system. Contact Cisco TAC for further assistance.	Testing the System, on page 65

Testing the System

These are some of the tests to run on 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, and 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.

CHAPTER 9

Updating the System

Updating Your System

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

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

Other system administrators should not access the system during this procedure. If they do so, their changes are not saved, and the result may be unpredictable. They must wait until this procedure is completed, then sign in to Cisco WebEx Administration to do their task.

Before You Begin

Be sure to get the latest update file from the Cisco Software Center:

http://www.cisco.com/cisco/software/navigator.html

The update file for your system is a zipped ISO image.

Procedure

Step 1 Sign in to the Cisco WebEx Administration site.

Step 2 Select the **System** tab, then select **Upgrade** in the top right pane.

Step 3 Select **update**.

Step 4 Select **Turn On Maintenance Mode**.

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, then use VMware Data Recovery to create a backup of each of your virtual machines.
A backup will help you revert your virtual machine to its state before the update. For further information, see Creating a Backup Using VMware vCenter, on page 4. For complete details on this backup, see the *VMware Data Recovery Administration Guide*.

Note You may also take a snapshot, but you must delete these in approximately 24 hours, or you may experience data performance issues, common to virtual machine snapshots. For more information, see Taking a Snapshot Using VMware vCenter, on page 5.

Caution Be sure to create backups of all your virtual machines. Because the update procedure makes changes to your existing virtual machines, you will not be able to undo the update, once the update procedure starts.

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

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

Step 9 Select the **System** tab, then select **Upgrade** in the top right pane. Select **update** to return to the **Update System** page.

What to Do Next

Go to Connecting the Update ISO Image From the CD/DVD Drive, on page 90.

Connecting the Update ISO Image From the CD/DVD Drive

You will attach the update file as an ISO image to your Admin virtual machine's CD/DVD drive.

Note 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, then be sure the vSphere client has a local hardwire connection into your company's Intranet (not over VPN).

To place the ISO image in the vCenter datastore, be sure you have the appropriate permissions then complete the following:

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

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

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

Before You Begin

Be sure to get the latest update file from the Cisco Software Center:

http://www.cisco.com/cisco/software/navigator.html

The update file for your system is a zipped ISO image.

Procedure

Step 1 Select the Admin virtual machine in the VMware vCenter inventory.

Step 2 Select the CD/DVD icon for the Admin virtual machine, then select **CD/DVD drive 1** > **Connect to ISO image** on a local disk or on a datastore.

Step 3 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:

- Updating Your System, on page 89
- Connecting the Update ISO Image From the CD/DVD Drive, on page 90

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.

What to Do Next

Continue with Completing the Update Procedure, on page 92.

Completing the Update Procedure

Before You Begin

This is a continuation from Continuing the Update Procedure, on page 91.

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.

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 Data Recovery 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 before the update.

CHAPTER 10

Upgrading the System

This chapter describes how to upgrade your system by redeploying it with an upgrade OVA file.

Note This section is included for completeness, as it is part of the product. However, you will not be able to upgrade your software until we provide an OVA file for the new release.

Preparing For an Upgrade

This section describes the prerequisites and best practices to upgrade your system.

Note This section is included for completeness, as it is part of the product. However, you will not be able to upgrade your software until we provide an OVA file for the new release.

Obtaining the Information Required For Your Upgrade

You upgrade your system by redeploying it with the upgrade OVA file.

- Obtain the OVA file required for the upgrade.
- Complete the upgrade checklist.

Field Name	Current Value For Your System
WebEx Site URL	
Administration Site URL	

Field Name	Current Value For Your System
Private VIP Address	
Public VIP Address	

Upgrading the System Using Automatic Deployment

Before You Begin

In this section, we refer to the system before upgrade as the "existing system". The system, following upgrade, is the "upgraded system."

- Schedule a time that is least disruptive to your users to do the system upgrade.
- Put the primary system in maintenance mode before starting the system upgrade.

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 may 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.

Upgrading the System

The overall tasks to upgrade the system are:

1. Create a backup of your existing system.
2. Use the upgrade OVA file and deploy the Admin virtual machine for the new system.
3. Copy the data from your existing system to the Admin virtual machine for the upgraded system.
4. Deploy any additional virtual machines for the upgraded system.
5. Test the upgraded system.

Considerations Before Upgrading the System

Note the following:

- You may choose to reuse the same hostnames and IP addresses for the existing virtual machines in the upgraded system. However, only the existing system, or the upgraded 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 existing system, then following deployment of the upgraded system, you must add a new HA system at the same release version as the upgraded system. You cannot reuse the existing HA system as it is not retained, following the upgrade.
- You may want to keep the existing system until you have finished testing the upgraded system. Once testing is complete and you are satisfied with the upgraded system, you can remove the existing (pre-upgrade) system.
- The internal virtual machines for the existing system and the upgraded system must be on the same subnet.
- If you have added public access, then the Internet Reverse Proxy virtual machines for the existing system and the upgraded system must be on the same subnet.
- Because this process affects the virtual machines in your system, your current security certificate may become invalid and require an update.
- Be sure the upgraded system can access the disks for the existing system's Admin virtual machine. You will be copying over Hard disk 4 to the upgraded system.

Summary of Tasks to Upgrade the System Using an Automatic Deployment

Task	Description	For Details, See
1	Prepare the existing system for the upgrade.	Preparing For an Upgrade, on page 93
2	Prepare for a system-altering procedure.	Preparing For a System-Altering Procedure, on page 68
3	Initiate the upgrade procedure from the Administration site of the existing system.	Upgrading Your System, on page 133
4	Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the existing system.	
5	Using the vSphere client, deploy the Admin virtual machine for the upgraded system.	Deploying the OVA File From the VMware vSphere Client, on page 16
6	Attach **Hard disk 4** from the existing system's Admin virtual machine to the Admin virtual machine for the upgraded system.	Attaching an Existing VMDK File to a New Virtual Machine, on page 6
7	Power on the Admin virtual machine for the upgraded system and write down the deployment URL.	
8	Enter the deployment URL into a web browser and continue the deployment of your upgraded system.	
9	Select your preferred language for the deployment of the upgraded system.	Selecting Your Language for Setup, on page 28
10	Confirm the system size. (This system size must be the same size as the existing system.)	Confirming the Size of Your System, on page 29

Task	Description	For Details, See
11	Select **Install a primary system**.	Choosing What System to Install, on page 29
12	Select an automatic deployment.	Choosing the Type of System Deployment, on page 29
13	Enter your vCenter credentials so that we may deploy the virtual machines for you.	Providing VMware vCenter Credentials, on page 30
14	As applicable, select the ESXi host, datastore, and virtual machine port group for the media virtual machine.	Choosing vCenter Settings for your Media Virtual Machine, on page 31
15	As applicable, enter the fully qualified domain name of the media virtual machine. (If you have already updated your DNS server with entries for the upgraded system, then we will look up the IP address for you.)	Entering Networking Information for the Media Virtual Machine, on page 31
16	If you want public access for your upgraded 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, then skip to Task 19.	Adding Public Access, on page 31
17	If you have added public access, then select the ESXi host, datastore, and virtual machine port group for the Internet Reverse Proxy virtual machine.	Choosing vCenter Settings for your Internet Reverse Proxy, on page 32
18	Enter the hostname and networking information for the Internet Reverse Proxy.	Entering the Networking Information for the Internet Reverse Proxy, on page 32
19	Enter the public VIP address for the WebEx site URL. **Note** You may enter the same public VIP address that you use for your existing 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
20	Enter the private VIP address for the WebEx Administration URL. **Note** You may enter the same private VIP address that you use for your existing 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 33

Task	Description	For Details, See
21	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 existing 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
22	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 existing 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
23	Check that you have made all the networking, DNS server, and firewall configuration changes required for your system.	Confirming That Your Network is Configured Correctly, on page 36
24	Once your virtual machines have deployed successfully, then select **Next** to continue to the system check.	Deploying Your Virtual Machines, on page 36
25	When the system check is done, select **Continue** and sign in to Cisco WebEx Administration.	Checking Your System, on page 37
25	Test the upgraded system. If the upgrade is unsuccessful, then power off the upgraded system and power on the existing system. Contact Cisco TAC for further assistance.	Testing the System, on page 65

Upgrading the System Using Manual Deployment

Before You Begin

In this section, we refer to the system before upgrade as the "existing system". The system, following upgrade, is the "upgraded system."

- Schedule a time that is least disruptive to your users to do the system upgrade.
- Put the primary system in maintenance mode before starting the system upgrade.

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 may 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.

Upgrading the System

The overall tasks to upgrade the system are:

1. Create a backup of your existing system.
2. Use the upgrade OVA file and deploy the Admin virtual machine for the new system.
3. Copy the data from your existing system to the Admin virtual machine for the upgraded system.
4. Deploy any additional virtual machines for the upgraded system.
5. Test the upgraded system.

Considerations Before Upgrading the System

Note the following:

- You may choose to reuse the same hostnames and IP addresses for the existing virtual machines in the upgraded system. However, only the existing system, or the upgraded 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 existing system, then following deployment of the upgraded system, you must add a new HA system at the same release version as the upgraded system. You cannot reuse the existing HA system as it is not retained, following the upgrade.
- You may want to keep the existing system until you have finished testing the upgraded system. Once testing is complete and you are satisfied with the upgraded system, you can remove the existing (pre-upgrade) system.
- The internal virtual machines for the existing system and the upgraded system must be on the same subnet.
- If you have added public access, then the Internet Reverse Proxy virtual machines for the existing system and the upgraded system must be on the same subnet.
- Because this process affects the virtual machines in your system, your current security certificate may become invalid and require an update.
- Be sure the upgraded system can access the disks for the existing system's Admin virtual machine. You will be copying over Hard disk 4 to the upgraded system.

Summary of Tasks to Upgrade the System Using a Manual Deployment

Task	Description	For Details, See
1	Prepare the existing system for the upgrade.	Preparing For an Upgrade, on page 93
2	Prepare for a system-altering procedure.	Preparing For a System-Altering Procedure, on page 68
3	Initiate the upgrade procedure from the Administration site of the existing system.	Upgrading Your System, on page 133
4	Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the existing system.	
5	Using the vSphere client, deploy the Admin virtual machine for the upgraded system.	Deploying the OVA File From the VMware vSphere Client, on page 16
6	Attach **Hard disk 4** from the existing system's Admin virtual machine to the Admin virtual machine for the upgraded system.	Attaching an Existing VMDK File to a New Virtual Machine, on page 6
7	Power on the Admin virtual machine for the upgraded system and write down the deployment URL.	
8	Enter the deployment URL into a web browser and continue the deployment of your upgraded system.	
9	Select your preferred language for the deployment of the upgraded system.	Selecting Your Language for Setup, on page 28
10	Confirm the system size. (This system size must be the same size as the existing system.)	Confirming the Size of Your System, on page 29
11	Select **Install a primary system**.	Choosing What System to Install, on page 29
12	Select a manual deployment.	Choosing the Type of System Deployment, on page 29
18	If you want public access for your upgraded 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
19	Enter the public VIP address for the WebEx site URL. **Note** You may enter the same public VIP address that you use for your existing 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

Task	Description	For Details, See
20	Enter the private VIP address for the WebEx Administration URL. **Note** You may enter the same private VIP address that you use for your existing 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 33
21	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 existing 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
22	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 existing 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
23	Check that you have made all the networking, DNS server, and firewall configuration changes required for your system.	Confirming That Your Network is Configured Correctly, on page 36
24	Once your virtual machines have deployed successfully, then select **Next** to continue to the system check.	Deploying Your Virtual Machines, on page 60
25	When the system check is done, select **Continue** and sign in to Cisco WebEx Administration.	Checking Your System, on page 37
25	Test the upgraded system. If the upgrade is unsuccessful, then power off the upgraded system and power on the existing system. Contact Cisco TAC for further assistance.	Testing the System, on page 65

Testing the System

These are some of the tests to run on 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, and 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.

PART II

Cisco WebEx Meetings Server Configuration Guide

CHAPTER 11

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 are present to notify you of important information. For example, to inform you that a first-time tutorial is available or to 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 of Good or Down.
    - Meetings in Progress—Select to open the **Meeting Trend** page which 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.
    - 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 status of alarms you have configured. By default, alarm information is displayed as a percentage. Select **Number #** to change the alarm information to numerical data. Alarm threshold is 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, on page 110 for more information.

    You can configure alarms for the following:

    - Meetings In Progress—Indicates when current meetings are experiencing issues.
    - Usage—The total users currently using the system.
    - CPU—Total system CPU used in MHz.
    - Memory—Total system memory used in GB.
    - Network—Total system bandwidth used in Mbps.
    - Storage—Storage space used in GB.

    Note The storage alarm appears if you have configured a storage server. See Configuring a Storage Server, on page 137 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

  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, on page 189 for more information.
  - Down—All services on your system are not running. Contact the Cisco TAC for assistance. See Using the Support Features, on page 189 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, on page 127.

- 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 151.

- About Your Dashboard, page 107

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 are present to notify you of important information. For example, to inform you that a first-time tutorial is available or to 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 of Good or Down.
  - ◦ Meetings in Progress—Select to open the **Meeting Trend** page which 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.

  - 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 status of alarms you have configured. By default, alarm information is displayed as a percentage. Select **Number #** to change the alarm information to numerical data. Alarm threshold is 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, on page 110 for more information.

    You can configure alarms for the following:

    - Meetings In Progress—Indicates when current meetings are experiencing issues.
    - Usage—The total users currently using the system.
    - CPU—Total system CPU used in MHz.
    - Memory—Total system memory used in GB.
    - Network—Total system bandwidth used in Mbps.
    - Storage—Storage space used in GB.

      Note The storage alarm appears if you have configured a storage server. See Configuring a Storage Server, on page 137 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

  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, on page 189 for more information.
  - Down—All services on your system are not running. Contact the Cisco TAC for assistance. See Using the Support Features, on page 189 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, on page 127.
- 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 151.

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 threshold.

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**.

Option	Description
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**.
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**.
Storage	Displays the current storage threshold in GB. The maximum storage threshold is calculated as (the total space – recording buffer size) where recording buffer size is 1 GB for micro, 5 GB for small, 16 GB for medium, and 40 GB for large. • 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 137 for more information.

An alarm email is sent to administrators if an alarm condition exists. The interval is used to suppress multiple alarms within the specified time to avoid sending too many alarm emails. 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. Meetings, participants, and storage are shown as the current values in the right-side panels. See Viewing and Editing Alarms, on page 109 for more information on the alarms you can configure.

You can view your resource history by selecting the alarm graphs on the **System Monitor** page. See About Your Dashboard, on page 105 for more information. For example, select the CPU graph and the **Resource History** page 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:

- VoIP
- Phone
- 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** and select the **Meetings in Progress** graph or **Usage** chart.

Step 3 Optionally change the view by selecting a different trend period:

- 1 day (default)—Data for one day displayed on the graph in five-minute intervals.

  Note If you select **Show future meetings**, the interval changes to one hour for future meetings.

- 1 week—Data for one week displayed on the graph in one-hour intervals.
- 1 month—Data for one month displayed on the graph in one-day intervals.
- 6 months—Data for a six-month period displayed on the graph in one-day intervals.

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 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.

The Meeting Trend graph is updated with your new settings.

Step 4 Optionally 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.

Step 5 Optionally select the **Participants** or **Meetings** graphs for meeting information including the following:

- Meeting Topic
- Host
- Participant
- State
- Status
- Note

Enter search terms in the field above the table to filter the meeting list.

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, on page 189 for more information.

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

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, on page 125 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 128 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 132 for more information.
- Change the system default language. See Configuring Your Company Information, on page 152 for more information.
- Changing your host or admin account URLs. See Changing Your Site Settings, on page 134 for more information.

- Changing your mail server. See Configuring a Mail Server, on page 136 for more information.
- Changing your system language and locale. See Configuring Your Company Information, on page 152 for more information.
- Changing your virtual IP address. See Changing Your Virtual IP Address, on page 130 for more information.
- Configuring and changing audio settings. See About Configuring Your Audio Settings, on page 155 for more information.
- Configuring and changing branding settings. See Configuring Your Branding Settings, on page 153 for more information.
- Configuring and changing quality of service settings. See Configuring Quality of Service (QoS), on page 160 for more information.
- Configuring certificates. See Managing Certificates, on page 168 for more information.
- Configuring disaster recovery settings. See Using the Disaster Recovery Feature, on page 138 for more information.
- Configuring FIPS-compatible encryption. See Enabling FIPS Compliant Encryption, on page 180 for more information.
- Configuring and changing SNMP settings. See Configuring Your SNMP Settings for more information.
- Configuring storage servers. See Configuring a Storage Server, on page 137 for more information.
- Configuring virtual machine security. See Configuring Virtual Machine Security for more information.
- Expanding system size. See Expanding System Size, on page 133 for more information.
- Performing minor updates, major upgrades, and expanding your system. See Updating the System, on page 89 for more information.
- Updating shared keys. See Managing Certificates, on page 168 for more information.
- Using the System Resource test. See Using the System Resource Test, on page 192 for more information.

CHAPTER 12

Managing Users

This section describes how to manage users on your system.

About Managing Users

You can add users individually or import lists of users stored in a comma- or tab-delimited file.

You can add and deactivate user accounts but you cannot delete them. Deactivation enables you to make a user inactive but provides the ability to reactivate the user later if necessary. Reactivated user accounts regain access to meetings, recordings, and other data that they had access to before they were deactivated.

The system supports a lifetime maximum of 400,000 user accounts. This number represents the total of both active and deactivated user accounts. This lifetime maximum number is large enough to accommodate expected growth in the user database.

To prevent unauthorized sign-in to the system, make sure to 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 or by importing a comma- or tab-delimited file with the ACTIVE field set to N for each user you want to deactivate. See

Deactivating Users, on page 117 and About Comma- and Tab-Delimited Files, on page 118 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 is not performed by this product.
- Use the password configuration feature to deactivate users after a specified period of time. See Configuring Your General Password Settings, on page 161 for more information.

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**.
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 116 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 116 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."

About Comma- and Tab-Delimited Files

Use a spreadsheet application such as Microsoft Excel to organize your user data. Save or export your spreadsheet as a comma- or tab-delimited file. Your system supports UCS Transformation Format—8 bit (UTF-8). The characters you enter in your file are limited to those specified in UTF-8. If your file contains non-ASCII characters, verify that it uses a unicode comma or tab delimiter.

Include the following fields in your comma- or tab-delimited file:

- USERID–The user ID.

  Note This field is automatically generated by the system and must be left blank when performing imports.

- ACTIVE–Whether or not this user is active. Enter **Y** or **N** (Required).
- FIRSTNAME–User's first name. (Required)
- LASTNAME–User's last name. (Required)
- EMAIL–User's email address. (Required)
- LANGUAGE–Language of the user. See Setting Import File Field Values, on page 119 for more information.
- HOSTPRIV–Host privileges. Enter **ADMN** or **HOST**.
- TIMEZONE–Time zone in which the user is located. See Setting Import File Field Values, on page 119 for more information.
- DIVISION–User's division. For tracking code group 1. This field is configurable on the **Tracking Codes** page. See Configuring Tracking Codes, on page 124 for more information.
- DEPARTMENT–User's department. For tracking code group 2. This field is configurable on the **Tracking Codes** page. See Configuring Tracking Codes, on page 124 for more information.
- PROJECT–User's project. For tracking code group 3. This field is configurable on the **Tracking Codes** page. See Configuring Tracking Codes, on page 124 for more information.
- OTHER–Other information. For tracking code group 4. This field is configurable on the **Tracking Codes** page. See Configuring Tracking Codes, on page 124 for more information.
- CUSTOM5–Custom field 5.
- CUSTOM6–Custom field 6.
- CUSTOM7–Custom field 7.
- CUSTOM8–Custom field 8.
- CUSTOM9–Custom field 9.

- CUSTOM10–Custom field 10.

Setting Import File Field Values

Language Field Values

Following are the country code field values that you can set in your import file.

Field Value	Language
en-us	U.S. English
en-uk	U.K.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 field values that you can set in your import file.

Field Value	GMT	Location
Dateline	-12 hr	Marshall Islands
Samoa	-11 hr	Samoa
Hawaii	-10 hr	Honolulu

Field Value	GMT	Location
Alaska	-9 hr	Anchorage
Pacific	-8 hr	San Francisco
Mountain	-7 hr	Arizona
Mountain	-7 hr	Denver
Central	-6 hr	Chicago
Mexico Central	-6 hr	Mexico City
Central	-6 hr	Saskatchewan
S. American Pacific	-5 hr	Bogota
Eastern	-5 hr	New York
Eastern	-5 hr	Indiana
Atlantic	-4 hr	Halifax
S. American Western	-4 hr	Caracas
Newfoundland	-3.5 hr	Newfoundland
S. American Eastern	-3 hr	Brasilia
S. American Eastern	-3 hr	Buenos Aires
Mid-Atlantic	-2 hr	Mid-Atlantic
Azores	-1 hr	Azores
Greenwich	0 hr	Casablanca
Greenwich Mean	0 hr	London
Central European	1 hr	Amsterdam
Central European	1 hr	Paris
Central European	1 hr	Berlin
Eastern European	2 hr	Athens
Egypt	2 hr	Cairo

Field Value	GMT	Location
South Africa	2 hr	Pretoria
Eastern European	2 hr	Helsinki
Israel	2 hr	Tel Aviv
Saudi Arabia	3 hr	Riyadh
Russia	3 hr	Moscow
Nairobi	3 hr	Nairobi
Iran	3.5 hr	Tehran
Arabian	4 hr	Abu Dhabi
Baku	4 hr	Baku
Afghanistan	4.5 hr	Kabul
West Asia	5 hr	Ekaterinburg
Ekaterinburg	5 hr	Islamabad
India	5.5 hr	Bombay
Colombo	5.5 hr	Colombo
Central Asia	6 hr	Almaty
Bangkok	7 hr	Bangkok
China	8 hr	Beijing
Australia Western	8 hr	Perth
Singapore	8 hr	Singapore
Taipei	8 hr	Taipei
Japan	9 hr	Tokyo
Korea	9 hr	Seoul
Yakutsk	9 hr	Yakutsk
Australia Central	9.5 hr	Adelaide

Field Value	GMT	Location
Australia Central	9.5 hr	Darwin
Australia Eastern	10 hr	Brisbane
Australia Eastern	10 hr	Sydney
West Pacific	10 hr	Guam
Tasmania	10 hr	Hobart
Vladivostok	10 hr	Vladivostok
Central Pacific	11 hr	Solomon Islands
New Zealand	12 hr	Wellington
Fiji	12 hr	Fiji
Central European	1 hr	Stockholm
Mexico Pacific	-8 hr	Tijuana
Mexico Mountain	-7 hr	Chihuahua
S. America Western	-4.5 hr	Caracas
Malaysia	8 hr	Kuala Lumpur

Importing Users

Before You Begin

Prepare a comma- or tab-delimited file containing your users' information. See About Comma- and Tab-Delimited Files, on page 118 for more information.

Procedure

Step 1 Sign in to the 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 comma- or tab-delimited file that you want to import.

Step 5 Select the **Tab** or **Comma** radio button to indicate which type you are importing.

Step 6 Select **Import**.
Your file is imported. After the import is complete, the system sends an email indicating how many records were imported successfully and how many failed.

What to Do Next

Select **Users** to see the users on your system. Make sure your users were imported properly.

Exporting Users

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 with a link to download the exported file.

Importing Users to a New System by Using an Exported File

Perform the following steps to import users to a new system using an exported file.

Procedure

Step 1 Sign in to the Administration site on the system you want to export users from.

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

Step 3 Select **Export**.
Your user data is exported as a comma- or tab-delimited file.

Step 4 Open the exported file, delete all USERIDs from the file, and resave the file.

Step 5 Sign in to the Administration site on the system to which you want to import users.

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 file you exported above.

Step 9 Select the **Tab** or **Comma** radio button to indicate which type you are importing.

Step 10 Select **Import**.
Your file is imported. After the import is complete, the system sends an email indicating how many records were imported successfully and how many failed.

What to Do Next

Select **Users** to see the users on your system. Make sure your users were imported properly.

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.
- 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 125 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.

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 user's email address or an email alias you want to email in the **To** text box.

The **To** field is optional for 50-user and 250-user deployments, and required for 800-user and 2,000-users deployments. If you do not specify a recipient, the email is sent to the first administrator configured on the system.

Step 4 Optionally enter email addresses in the **BCC** text box.

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

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

Step 7 Select **Send**.

CHAPTER 13

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 **System** and select **View More** in the System section.

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

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 Your can configure your system with IPv4 or IPv6 virtual machine settings. During deployment, you can only configure IPv4 settings but you update your virtual machine to IPv6 on this page.

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 168.

Configuring a High Availability System

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

Adding a High Availability System

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.

Note Complete the following procedure on the primary system.

Before You Begin

- Install Cisco WebEx on a second virtual machine from the OVA file to be used as your high availability system.

  Note Your high-availability system must be the same size as your primary system.

- Your high-availability system must be configured with the same OVA and patch as your primary system. If your primary and high-availability systems' versions do not match, you will be instructed to upgrade to the higher version.
- Copy the high-availability virtual machine fully qualified domain name (FQDN). You must know the FQDN to add your high-availability system.
- Verify that all virtual machines are functioning normally. Determine virtual machine status by viewing the System Monitor as described in About Your Dashboard, on page 105.

Procedure

Step 1 Sign in to the Administration site.

Step 2 On the primary system, in the System section, select the **View More** link.

Step 3 Select **Add High Availability System**.

Step 4 Follow the instructions on the **System Properties** page to add this HA system.

Example:

Step 5 Enter the FQDN of the Administration site virtual machine of the high-availability system and select **Continue**. We will validate the readiness of both the primary system and the HA system for this add HA procedure.

- If both systems are ready, then you will see a green **Add** button. Do not select it until you put your system into maintenance mode.
- If either system is not ready, then you will see an error message. Fix the error and attempt the add high availability procedure again.

Step 6 Select **Turn On Maintenance Mode**, then 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 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.

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

Step 3 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 4 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 71 for more information.

Your high-availability system is removed.

Step 5 Open VMware vCenter and remove the high-availability system using the **Delete from Disk** command.

Changing Your Virtual IP Address

Procedure

Step 1 Sign in to the Administration site.

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

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

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 dialogue box.

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.

Launch VMware vCenter and perform the following:

- Back up your virtual machines using VMware Data Recovery. This enables you to revert the changes if necessary. See Creating a Backup 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. See Adding Public Access, on page 31 for more information.

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

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

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 168 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. This enables you to revert your changes if necessary. See Creating a Backup 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 **System** and then select the **View More** link in the System section.

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

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 130 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 System Size

Before You Begin

Before you perform a system expansion, see Expanding Your System to a Larger System Size, on page 79, 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 **System** and select the **View More** link in the System section.

Step 3 Select **Expand System Size**.

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

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 Using Automatic Deployment , on page 81
- Expanding the System Using Manual Deployment, on page 84

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.

Upgrading Your System

The **Upgrade** page gives you the option to update, upgrade, or expand your system.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **System** > **Upgrade**.

Step 3 Select the type of upgrade you want to perform and select **Continue**:

- Minor update or upgrade—Requires you to download the latest update before you can continue. See Updating the System, on page 89 for more information.
- Major upgrade with system redeployment—Requires you to download the OVA upgrade file before you can continue. See Upgrading the System, on page 93 for more information.
- Expand system size—See Expanding System Size, on page 133 for more information.

Your proceed to the update, upgrade, or expand page.

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

Step 5 Perform your update, upgrade, or expansion as described in the associated section.

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 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

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 **System** > **Configuration** > **General settings** > **View More**.

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

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 168 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 **System** > **Configuration** > **General settings** > **View More**.
The **General settings** page appears.

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

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 168 for more information.

Configuring Servers

Use these features to configure your servers:

- SMTP Server—The SMTP server handles the sending of email from the email client to the destination.
- Storage Server—The NFS server is the storage server where all the meeting recordings will be stored.

Configuring a Mail Server

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

Note It is very important that your 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 in to the Administration site.

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

Step 3 Select **Edit** in the Mail Server section.

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

Step 5 Enter your mail server hostname and optionally select the **TLS Enabled** check box.

Step 6 Enter your mail server port number and optionally select the **Server Authentication Enabled** check box.

Step 7 Select **Continue**.

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.

Configuring an SMTP Server

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **System.**

Step 3 Under Servers, select the **View More** link.

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

Step 5 Under SMTP Server, select the **Edit** link.

Step 6 Complete the SMTP server fields:

- Host Name–The host name of your SMTP server.
- Port–The port number for your SMTP server.
- User Name–User name for the email client.

- Password–Password for the user.

Step 7 Optionally select the **TLS Enabled** and **Server Authentication Enabled** check boxes.

Step 8 Select **Save**.

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 a Storage Server

Your storage server backs up your database and recorded meetings on a daily basis.

Before You Begin

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

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **System**.

Step 3 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 4 Select **Turn On Maintenance Mode** and **Continue** to confirm.

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

Step 6 Enter the NFS mount point and select **Continue**.
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 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 138 for more information.

Using the Disaster Recovery Feature

Use the disaster recovery features to recover your deployment after any type of 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 it to the same state.

After you have configured a storage server, your system is backed up on a daily basis. A system backup notice appears on your dashboard that displays information about the latest backup. If you perform a disaster recovery the latest backup is used. 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," below).

Perform the procedure below after a disaster has occurred and you have lost the ability to use your system.

Before You Begin

- To perform disaster recovery procedures, you must have a storage server configured. See Configuring a Storage Server, on page 137 for more information. If you do not have a storage server configured, the **Disaster Recovery** option is not available.
- You must have access to a system on which 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.

  Disaster recovery can be performed on systems with or without high availability. However, you cannot configure disaster recovery on a high-availability system. You must configure disaster recovery first and then you can configure high availability on that system. If you have a high-availability system that requires disaster recovery, your must restore your system and then reconfigure high availability on your restored system. For more information on high availability, see Adding a High Availability System, on page 71.

Procedure

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

Step 2 Select **System** > **Servers** > **Add Storage Server**.

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

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

Example:

Enter ip://xyz/yu.

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. If this happens, you must redeploy the application on your recovery system so that the deployment size and software version match the original deployment.

Step 6 Select one of the following to continue:

- **Cancel**—To back up your pre-existing system before adding a storage server. After you back up your system you return to this page and can select **Continue** to proceed.
- **Continue**—To 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, on page 175 for more information.
- Reconfigure your SNMP settings. See Configuring Your SNMP Settings, on page 139 for more information.
- Reconfigure your certificates. See Managing Certificates, on page 168 for more information. You might have to reload your SSL certificates if they do not match the SSL certificates that are configured on the recovery system.
- Your recovery system is initially configured for License Free Mode which expires in 180 days. Re-host your previous system's licenses on the recovery system. See About Licenses, on page 148 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, on page 130 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. The default community string is CWS-Public. Select **CWS-Public** to edit it or add additional community strings.
- 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.
- 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 **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** 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 **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 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

Option	Description
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

Option	Description
Authentication Algorithm	Select the authentication algorithm for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**. **Default**: SHA
Authentication Password	Change the authentication password for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**.
Privacy Algorithm	Select the privacy algorithm for the user. **Note** This option appears only if the security level is set to **authPriv**. **Default**: AES128
Privacy Password	Change the privacy password for the user. **Note** This option appears only if the security level is set to **authPriv**.

Step 6 Select **Edit**.
The USM user information is changed.

Step 7 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
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 142 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 140 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
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 142 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 140 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.

Managing Licenses

When you purchase this product, you are given a 180-day free trial period. After your free trial period expires, you are required to purchase licenses for your users. To obtain licenses, you use an embedded version of Cisco Enterprise License Manager. Refer to the *Cisco WebEx Meetings Server Planning Guide* for more information.

Before You Begin

Contact your Cisco sales representative to order licenses for your system. Your sales representative will send you an email that contains your Product Authorization Key (PAK).

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **Manage Licenses**
Your browser opens a new tab or window containing Cisco Enterprise License Manager (ELM).

Note This version of ELM is embedded in Cisco WebEx Meetings Server. The ELM site is not an external web site.

Step 4 Select **License Management** > **Licenses**.

Step 5 Select **Generate License Request**.
The **License Request and Next Steps** dialog box appears.

Step 6 Copy the selected text in the field and select **Cisco License Registration**.

Step 7 Log in to your Cisco account.
The **Product License Registration** page appears.

Step 8 Enter the PAK that you received from your Cisco sales representative in the **Product Authorization Key** field and select **Next**.
The **Fulfill PAK** page appears.

Step 9 Paste the contents of the License Request that you copied above into the field, enter the quantity of licenses you are purchasing, and select **Next**.

Step 10 Review the page and select **I agree to the Terms of the license**.

Step 11 Make sure the contact email address is correct. Optionally change the contact email address in the **Send to** field.

Step 12 Select **Get License**
The **License Request Status** dialog box appears.

Step 13 Obtain your license file in one of the following ways:

- Select **Download** to download your license file (.bin).
- Extract your license file (.bin) from the ZIP archive sent to you by email.

Step 14 Return to the Administration site and select **System** and then select the **View More** link in the Licenses section.

Step 15 Select **Manage Licenses**.
Your browser opens a new tab or window containing Cisco Enterprise License Manager (ELM).

Step 16 Select **Install License File**.

Step 17 Select **Browse** and select the license file (.bin) that you downloaded or extracted from the ZIP file in your email.

Step 18 Select **Install**.
Your license file is installed. Check the license information that is displayed to ensure that it is correct.

Step 19 Select **System** and select **View More** in the License section.
The **User Licenses** page appears. Ensure that the information displayed is correct.

Adding Licenses

Before You Begin

Obtain your registration ID number. You can find your registration ID number by opening your Enterprise License Management tool and selecting **About**.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Support** and call the TAC at the listed number.

Step 3 File a case, requesting the number of additional licenses you want.
Cisco processes your request and enables the additional licenses on your system.

Step 4 Select **System**.

Step 5 Check the License section to confirm that your additional licenses have been added.

About Licenses

This product has User-Based Licensing which requires that you purchase a license for each user that intends to host meetings. We count licenses as follows:

- If a user hosts at least one meeting per 30-day window, then that user consumes one license. If this user hosts additional meetings in this same 30-day window, the user still only consumes one license, unless this user hosts simultaneous meetings.
- If a user hosts simultaneous meetings (at the same date and time), then the system counts an additional license for each simultaneous meeting hosted by this user in the 30-day window.
- If a user hosts no meetings in the 30-day window, then this user consumes no licenses.

Note There is currently a known issue that causes no licenses to be consumed if a user attends only the teleconference portion of a meeting (and not the web portion). In future versions of this product, attending either the teleconference or web portion of a meeting (or both) will result in a license use.

Note The system counts license use for each user every 30 days, as shown in the following table.

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in 30 Days
User A schedules a meeting but does not host it.	January 1	9:00 a.m.	No	0
User B hosts one meeting.	January 2	9:00 a.m.	No	1
User C hosts two meetings on different dates and times.	January 3 January 4	9:00 a.m. 10:00 a.m.	No	1

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in 30 Days
User D hosts two meetings on the same date and time.	January 6 January 6	9:00 a.m. 9:00 a.m.	Yes (2)	2
User E hosts two meetings on the same date and time, and another two simultaneous meetings on a different date and time within the month.	January 6 January 6 January 10 January 10	9:00 a.m. 9:00 a.m. 4 p.m. 4 p.m.	Yes (2)	2
User F hosts two meetings on the same date and time neither of which he attends, although the meetings occur.	January 7 January 7	9:00 a.m. 9:00 a.m.	Yes (2)	2
User G hosts a meeting and passes host rights to another participant during the meeting. The user then hosts a 2nd meeting that runs simultaneously with the 1st meeting.	January 8 January 8	9:00 a.m. 9:00 a.m.	Yes (2)	2
User H hosts a meeting but all of the meeting participants join the teleconference only (not the web portion) with the **Join Before Host** option selected.	January 9	9:00 a.m.	No	0
User J hosts two meetings on the same date and time but all of the meeting participants join the teleconference only (not the web portion) with the **Join Before Host** option selected.	January 10 January 10	9:00 a.m. 9:00 a.m.	No	0

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in 30 Days
User K hosts a meeting and passes host rights to another participant during the meeting. The user then hosts a 2nd meeting that runs simultaneously with the 1st meeting but all of the 2nd meeting participants join the teleconference only (not the web portion) with the **Join Before Host** option selected.	January 11 January 11	10:00 a.m. 10:00 a.m.	No	1

From the **Reports** page, you may request a CSV report that totals all the licenses consumed during a 30-day window. However, for convenience, we recommend you view the PDF Summary Report that shows month-by-month license consumption trends. By viewing the overall license trend, you can plan for future license purchases more effectively, to match the growing adoption of this system within your company.

Caution As a convenience, the system permits license consumption to exceed the number of licenses actually installed on the system. In these situations, you and the other administrators will receive ‘Licenses are in Overage’ emails. In addition, the Dashboard displays messages indicating you have up to 180 days to purchase additional licenses to cover the gap. During this 180-day period, the system will continue to function normally for end users. However, once the 180 days elapse, then the system will shut down for all end users until an administrator installs additional licenses.

- While the system is shut down, end users may no longer schedule, host, or attend meetings. They will see a "Site under maintenance" message in the end user WebEx site.
- However, the Cisco WebEx Administration site will still function normally, so that an administrator can sign in and add licenses. Once the additional licenses are installed, then end users can again access the WebEx site and host and attend meetings.

CHAPTER 14

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

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

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

Configuring Your Branding Settings

Before You Begin

Prepare the following before configuring your branding settings:

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Removing a Company Logo

Before You Begin

Create a transparent 120x32 PNG or GIF file.

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Configuring Your Meeting Settings

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

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

  Note This setting is limited by the system size configured during deployment. See Confirming the Size of Your System, 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 Attendees to join Meetings before Host** is selected. Optionally select **Anyone can present in the meeting**.

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

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

System Size	Maximum Meeting Size
50	50

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

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

Note You must configure a storage server to enable recording. See Configuring a Storage Server, on page 137 for more information.

Step 6 Select **Save**.

About Configuring Your Audio Settings

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

Configuring Your Audio Settings for the First Time

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

Before You Begin

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

- Prepare a list of call-in access numbers that your participants use to call into meetings.
- Obtain a valid secure conferencing certificate if you plan to use TLS/SRTP teleconferencing encryption. See the Importing Secure Teleconferencing Certificates, on page 173 page for more information.

  Note This feature is not available in Russia or Turkey.

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

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

a) Enter an IP address for CUCM 1 IP Address and optionally for CUCM 2 IP Address.

Note CUCM 2 is not required but it is recommended for teleconferencing high availability.

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

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

Note If you select TLS as your transport type, you must import a valid secure conferencing certificate for each of your CUCM servers, export the SSL certificate and upload it into CUCM, and configure your system's fully qualified domain name (FQDN) as the SIP domain name on each CUCM server. See Importing Secure Teleconferencing Certificates, on page 173 for more information on importing your certificates and Configuring CUCM in the Planning Guide for more information on CUCM.

d) Select **Continue**.

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

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

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

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

Step 11 Enter the **Phone Label** and **Phone Number** for each access number that you add and select **Continue** after you have finished adding numbers.

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

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

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

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

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

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

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

Step 15 (Optional) Configure your WebEx Call Me setting (**Default**: Press 1 to connect to meeting). Optionally deselect this option to bypass the requirement to press **1** to connect to a meeting.

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

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

- Beep (default)
- No tone
- Announce name

Step 17 (Optional) If IPv6 is configured on your system, set your **IPv6 Teleconferencing** setting to **On** or **Off**. (**Default**: Off. A setting of **Off** indicates that IPv4 is the setting.)

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

Step 18 Select **Save**.

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

Configuring Your Audio Settings

Before You Begin

If you have not already configured your audio settings, see the Configuring Your Audio Settings for the First Time, on page 155 section.

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

Option	Description
CUCM 1 IP Address	Enter the hostname or an IP address for your CUCM 1 system.
CUCM 2 IP Address	(Optional) Enter the hostname or an IP address for your CUCM 2 (load balancing) system. **Note** CUCM 2 is not required but it is recommended for teleconferencing high availability.
Port Number	Enter a valid port number. Make sure the port number matches the setting in CUCM. **Default:** 5062
Transport	Select the transport type. **Note** If you select TLS as your transport type, you must import a valid secure conferencing certificate for each of your CUCM servers, export the SSL certificate and upload it into CUCM, and configure your system's fully qualified domain name (FQDN) as the SIP domain name on each CUCM server. See Importing Secure Teleconferencing Certificates, on page 173 for more information on importing your certificates and Configuring CUCM in the Planning Guide for more information on CUCM. **Default:** TCP

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

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

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

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

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

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

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

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

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

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

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

- Beep (default)
- No tone
- Announce name

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

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

Step 12 Select **Save**.

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

Configuring Your Video Settings

Procedure

Step 1 Sign in to the Administration site.

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

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

Configuring Your Mobile Settings

Note Android is not supported in Cisco WebEx Server 1.0.

Before You Begin

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Configuring Quality of Service (QoS)

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

Following are the default values:

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Configuring Passwords

You can configure password settings for the following:

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

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

Configuring Your General Password Settings

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Note This feature only applies to host accounts. You cannot deactivate an administrator account using this feature. To deactivate an administrator account, see Deactivating Users, on page 117.

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

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

Step 6 Select **Save**.

Configuring Your User Password Settings

Configure your user password requirements and limitations.

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 4 Select **Save**.

Configuring Your Meeting Passwords

Procedure

Step 1 Sign in to the Administration site.

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

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

Note All options are not selected by default.

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

Step 4 Select **Save**.

Configuring Your Email Settings

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select **Templates**. See About Email Templates, on page 164 for descriptions of each template type.
The **Templates** page appears. Select the **Common** or **Meetings** tab. **Common** is the default.

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

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

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

About Email Templates

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

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

Table 1: Common Email Templates

Title	Description
Account Reactivated	Sent to a user after an administrator reactivates the user's account.

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

Table 2: Meetings Email Templates

Title	Description
In-Progress Meeting Invite for Attendee	Sent to users when a host invites them to a meeting while the meeting is in progress.
Instant Meeting Invite for Host	Sent to the host and attendees when the host selects **Meet Now**.
Meeting Canceled for Attendee	Informs a user that a scheduled meeting has been canceled.
Meeting Canceled for Host	Sent to a meeting's host to confirm cancellation of a meeting.
Meeting Information Updated for Alternate Host	Provides meeting information to the alternate host when the meeting settings have been changed.

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

Configuring Your Download Settings

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select your download method:

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

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

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

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

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

Note The default language is the language you have configured in your company information. See Configuring Your Company Information, on page 152 for more information.

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

Note The default language is the language you have configured in your company information. See Configuring Your Company Information, on page 152 for more information.

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

About Downloads

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

On PCs without administrator privileges:

- We recommend that you push the Cisco WebEx Meetings application and Productivity Tools to end-user desktops offline before you inform end-users that user accounts have been created for them. This ensures that your users can start and join meetings from their web browsers and Windows desktops the first time they sign in.
- You can acquire the .MSI installers for each from the **Admin** > **Settings** > **Downloads** page. See Configuring Your Download Settings, on page 166 for more information.
- If you decide against pushing the applications to your users, they can still access these applications from the end-user download pages. However, if their PCs prohibit installation of downloaded applications, they will not be able to complete the installation process.
- When users join meetings by using their web browser (the Cisco WebEx Meetings application can still be downloaded on demand) they can join meetings successfully. In addition, the Cisco WebEx Meetings application attempts to perform an installation to speed up the process of starting or joining future meetings. This fails because their PCs do not have administrator privileges.

On PCs with administrator privileges:

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

Managing Certificates

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

The following certificate types are supported:

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

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

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

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

SSL certificates can become invalid for the following reasons:

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

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

Generating SSL Certificates

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

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

Generating a Certificate Signing Request (CSR)

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

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

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

Step 7 Back up your system using VMware Data Recovery. See Creating a Backup Using VMware vCenter, 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 **Settings** > **Security** > **Certificates** > **More Options** > **Import SSL Certificate**.
If you already have a certificate installed, the system warns you that importing a new certificate will overwrite it.

Step 3 Select **Continue**.

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

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

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

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

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

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

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

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

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

Step 6 (Optional) Enter a passphrase in the **Passphrase** field.

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

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

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

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

Step 10 Select **Done**.

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

Exporting a SSL Certificate

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Save the certificate file.

What to Do Next

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

Downloading Your CSR and Private Key

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Generating a Self-Signed Certificate

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Option	Description
Certificate Name	Enter a name for your self signed certificate. (Required)
X.509 Subject Name	The hostname of your system. (Not configurable)

Option	Description
Organization	Enter your organization name.
Department	Enter your department name.
City	Enter your city name.
State/Province	Enter the name of your state or province.
Country	Select your country name.

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

Step 6 Select **Done**.

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

Importing SSO IdP Certificates

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

Importing Secure Teleconferencing Certificates

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

Before You Begin

Secure teleconferencing certificates are required for your CUCM servers when TLS is selected as the transport type in your audio settings. See About Configuring Your Audio Settings, on page 155 for more information.

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

Step 5 Enter a certificate name.

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

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

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

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

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

Step 10 Select **Done**.

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

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

Configuring User Session Security

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 4 Select **Save**.

Configuring Federated Single Sign-On (SSO) Settings

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

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

Before You Begin

- Before you enable the federated single sign-on feature, you must generate a set of public and private keys and an X.509 certificate that contains the public key. Once you have a public key or certificate, you must upload it in the Managing Certificates, on page 168 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 161 and Editing Users, on page 116 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 173 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. Using an alternative NameID format might cause a non-SSO user to no longer access his previously created account before you configured the system for SSO. **Default**: Unspecified
AuthnContextClassRef	Enter the value that is configured in IdP. AuthnContextClassRef is the value that appears in the AuthnRequest message. **Default**: urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
Default Webex target page URL	Your system redirects to this URL when SSO is successful. The default page is the Cisco WebEx meeting page which is the same as a normal login.
Customer SSO error URL	Your system redirects to this URL when SSO is not successful. By default, the error page is a common Cisco WebEx error page.
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.

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 5 Select **Save**.

Configuring Virtual Machine Security

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

Updating Your Encryption Keys

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select **Update Encryption Keys**.

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

About FIPS

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

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

Enabling FIPS Compliant Encryption

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

Disabling FIPS Compliant Encryption

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

CHAPTER 15

Generating and Viewing Reports

You can view monthly reports and customize reports for specific date ranges.

Note Your reports use the language, locale, and time zone settings configured on the **Company Information** page. See Configuring Your Company Information, on page 152 for more information.

- Downloading Monthly Reports, page 183
- About Monthly Reports, page 183
- Generating Customized Details Reports, page 185
- About Customized Details Reports, page 185

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 Managing Licenses, on page 146 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 137 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, see your dashboard. See About Your Dashboard, on page 105 for more information.

- 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:

- 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
    - Status
    - 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
    - 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)

Note 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.

- 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, on page 137 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—This report displays license date for the past 30 days and 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 16

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.

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 the administrator 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 for the account in hours. The maximum is 30 days (720 hours).

The **Remote Support Account Creation** dialog box appears, providing your pass phrase code. Contact Cisco and provide the pass phrase code to enable Cisco Support personnel to access 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.

Using the Meetings Test

Procedure

Step 1 Sign in to the Administration site.

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

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

Using the System Resource Test

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Support** > **System Resource Test**.

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

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

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

Step 5 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 17

Troubleshooting

Refer to the Cisco WebEx Meetings Server Troubleshooting Guide on Cisco.com.