Cisco WebEx Meetings Server Administration Guide Release 2.0

First Published: February 27, 2013

Last Modified: February 27, 2013

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

CONTENTS

PART I Cisco WebEx Meetings Server Installation Guide 1

CHAPTER 1 Using VMware vSphere With Your System 3

- Using VMware vSphere 3
- Configuring the ESXi Host to Use an NTP Server 4
- Creating a Backup Using VMware vCenter 4
- Taking a Snapshot Using VMware vCenter 5
- Attaching an Existing VMDK File to a New Virtual Machine 6

CHAPTER 2 Networking Checklist For Your System 9

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

CHAPTER 3 Installing Your System Using Automatic Deployment 11

- General Concepts For Your System Deployment 12
- Installation Checklist 13
- Required Information For an Automatic Deployment 13
- Deploying the OVA File From the VMware vSphere Client 16
  - Checking Your Networking Configuration After a Failed OVA Deployment 28
- Selecting Your Language for Setup 28
- Confirming the Deployment 29
- Confirming the Size of Your System 29
- Choosing What System to Install 29
- Choosing the Type of System Deployment 30
- Providing VMware vCenter Credentials 30
- Choosing vCenter Settings for your Media Virtual Machine 31
- Entering Networking Information for the Media Virtual Machine 31

Adding Public Access 32
Choosing vCenter Settings for Your Internet Reverse Proxy 32
Entering the Networking Information for the Internet Reverse Proxy 33
Entering the Public VIP Address 33
Entering the Private VIP Address 34
WebEx Site and WebEx Administration URLs 34
Entering the WebEx Site and Administration URLs 36
Confirming That Your Network is Configured Correctly 36
Deploying Your Virtual Machines 36
Checking Your System 37

CHAPTER 4 **Installing Your System Using Manual Deployment** 39
General Concepts For Your System Deployment 39
Installation Checklist 40
Required Information For a Manual Deployment 41
Deploying the OVA File From the VMware vSphere Client 42
Checking Your Networking Configuration After a Failed OVA Deployment 54
Selecting Your Language for Setup 54
Confirming the Deployment 55
Confirming the Size of Your System 55
Choosing What System to Install 55
Choosing the Type of System Deployment 56
Adding Public Access 56
Entering the Public VIP Address 57
Entering the Private VIP Address 57
WebEx Site and WebEx Administration URLs 58
Entering the WebEx Site and Administration URLs 59
Confirming That Your Network is Configured Correctly 60
Deploying Your Virtual Machines 60
Checking Your System 61

CHAPTER 5 **Configuring Your Mail Server, Time Zone, and Locale** 63
Setting Up the Mail Server For Your System 63
Setting Up the Time Zone and Locale for the System 64
Confirming the Mail Server, Time Zone, and Locale Settings 64

Setting Up the First Administrator Account for Your System 64
Testing the System 65

CHAPTER 6 Altering the System After Installation 67
Adding HA, Updating, Upgrading, or Expanding the System 67
Preparing For a System-Altering Procedure 68

CHAPTER 7 Adding a High Availability System 71
Adding a HA System Using Automatic Deployment 71
Adding a HA System Using Manual Deployment 73
Confirming Your Primary System and Your HA System Are at the Same Version 75
Adding a High Availability System 76
Testing the System 77

CHAPTER 8 Expanding Your System to a Larger System Size 79
Preparing for System Expansion 79
Preparing For a System-Altering Procedure 80
Expanding the System by using Automatic Deployment 81
Expanding the System by using Manual Deployment 85
Testing the System 89

CHAPTER 9 Updating the System 91
Updating Your System 91
Connecting the Update ISO Image From the CD/DVD Drive 92
Continuing the Update Procedure 93
Completing the Update Procedure 94

CHAPTER 10 Upgrading the System 97
Preparing For an Upgrade 97
Upgrading the System Automatically 98
Upgrading the System Manually 99
Testing the System 101
License Re-host and Upgrade 101
Re-hosting Licenses after a Software Upgrade 102
Upgrading Licenses after a Software Upgrade 102

PART II Cisco WebEx Meetings Server Configuration Guide 105

CHAPTER 11 Using Your Dashboard 107

About Your Dashboard 107
Viewing and Editing Alarms 109
Viewing Meeting Trends 111
Viewing the Meetings List 111
Scheduling a Maintenance Window 112
About Maintenance Mode 113
Turning Maintenance Mode On or Off 116
Changing a Scheduled Maintenance Window 116

CHAPTER 12 Managing Users 119

About Managing Users 119
About Comma- and Tab-Delimited Files 120
CSV File Field Values 121
Adding Users 125
Editing Users 126
Activating Users 126
Deactivating Users 127
Deactivating Users Using Import 127
Importing Users 128
Exporting Users 128
Importing Users to a New System by Using an Exported File 129
Configuring Tracking Codes 129
Editing Tracking Codes 130
Configuring Directory Integration 131
Synchronizing User Groups 135
Using CUCM to Configure AXL Web Service and Directory Synchronization 135
Using CUCM to Configure LDAP Integration and Authentication 136
Emailing Users 137

CHAPTER 13 Configuring Your System 139

Configuring System Properties 139

Changing Your Virtual Machine Settings 139
Configuring a High Availability System 140
Adding a High Availability System 140
Removing a High Availability System 142
System Behavior After Component Failure 142
Changing Your Virtual IP Address 143
Configuring Public Access 144
Adding Public Access to Your System 144
Removing Public Access 145
Expanding System Size 146
Upgrading Your System 147
Configuring General Settings 147
Changing Your Site Settings 148
Changing Your Administration Settings 148
Configuring Servers 149
Configuring a Mail Server 149
Configuring an SMTP Server 150
Configuring a Storage Server 150
Using the Disaster Recovery Feature 152
Configuring Your SNMP Settings 154
Configuring Community Strings 154
Adding Community Strings 155
Editing Community Strings 156
Configuring USM Users 156
Adding USM Users 157
Editing USM Users 158
Configuring Notification Destinations 159
Editing a Notification Destination 160
Configuring Notification Destinations 160
Managing Licenses 161
About Licenses 162
Adding Licenses 168
Re-hosting Licenses after a Software Upgrade 168

CHAPTER 14 Configuring Settings 171

Configuring Your Company Information 172
Configuring Your Branding Settings 173
Removing a Company Logo 173
Configuring Your Meeting Settings 174
About Meeting Security 175
About Configuring Your Audio Settings 176
Configuring Your Audio Settings for the First Time 176
Configuring Your Audio Settings 179
Configuring Your Video Settings 181
Configuring Your Mobile Settings 181
Configuring Quality of Service (QoS) 181
About QoS Marking 182
Configuring Passwords 183
Configuring Your General Password Settings 183
Configuring Your User Password Settings 184
Configuring Your Meeting Passwords 185
Configuring Your Email Settings 186
About Email Templates 187
Configuring Your Download Settings 207
About Downloads 208
Managing Certificates 208
Generating SSL Certificates 209
Generating a Certificate Signing Request (CSR) 210
Importing a SSL Certificate 211
Exporting a SSL Certificate 212
Downloading Your CSR and Private Key 212
Generating a Self-Signed Certificate 213
Restoring a SSL Certificate 214
Importing SSO IdP Certificates 215
Importing Secure Teleconferencing Certificates 215
Configuring User Session Security 216
Configuring Federated Single Sign-On (SSO) Settings 217
Disabling SSO 220
Configuring Your Cloud Features 221
Configuring Virtual Machine Security 221

Updating Your Encryption Keys 221
About FIPS 222
Enabling FIPS Compliant Encryption 222
Disabling FIPS Compliant Encryption 223

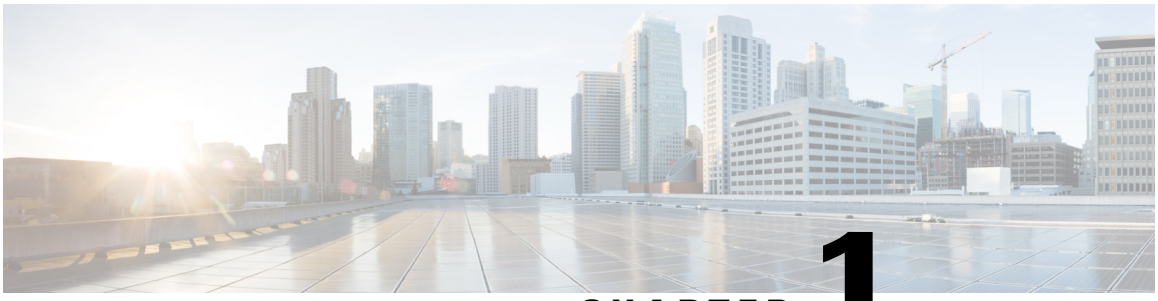
CHAPTER 15 Managing Your Reports 225
Downloading Monthly Reports 225
About Monthly Reports 225
Generating Customized Details Reports 227
About Customized Details Reports 227

CHAPTER 16 Using the Support Features 231
Customizing Your Log 231
Setting Up a Remote Support Account 232
Disabling a Remote Support Account 233
Using the Meetings Test 233
Using the System Resource Test 234

PART I

Cisco WebEx Meetings Server Installation Guide

- Using VMware vSphere With Your System, page 3
- Networking Checklist For Your System, page 9
- Installing Your System Using Automatic Deployment, page 11
- Installing Your System Using Manual Deployment, page 39
- Configuring Your Mail Server, Time Zone, and Locale, page 63
- Altering the System After Installation, page 67
- Adding a High Availability System, page 71
- Expanding Your System to a Larger System Size, page 79
- Updating the System, page 91
- Upgrading the System, page 97



CHAPTER 1

Using VMware vSphere With Your System

- Using VMware vSphere, page 3
- Configuring the ESXi Host to Use an NTP Server, page 4
- Creating a Backup Using VMware vCenter, page 4
- Taking a Snapshot Using VMware vCenter, page 5
- Attaching an Existing VMDK File to a New Virtual Machine, page 6

Using VMware vSphere

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

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

  Earlier releases of vSphere are not supported.

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

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

- Ensure that the DNS server configured with the ESXi host can resolve the hostnames of the virtual machines that are deployed on that ESXi host.
- You must use VMware vCenter to manage the ESXi hosts on which the Cisco WebEx Meetings Server system is deployed.

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

Backup allows traditional file-based backup software to leverage VMware virtual machine snapshot technology and efficient SAN-based data transfer. Before doing any system-altering procedure, we recommend that create a backup of each of the virtual machines. You can do so by using VMware Data Recovery (called VMware vSphere Data Protection starting with vSphere Release 5.1), or by taking virtual machine snapshots. (VMware Data Recovery/vSphere Data Protection is included with VMware vSphere, except in the vSphere Essentials Kit.)

Virtual machine snapshots are *pictures* of your system at a specific point in time, and are not the same as backups. Snapshots are stored on the physical drives containing your virtual machines. If you do not delete these snapshots in a timely manner, your end users might experience degraded audio and video due to a known issue that affects virtual machine performance. Therefore, for performance reasons, we recommend that you use backups and keep your virtual machine backups in a storage location that is different from the physical drives that contain your virtual machines.

For more information on snapshots and 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

Be sure there are no active meetings and that you have selected a time where there will be minimal impact to your users.

Step 2 Follow the instructions in your VMware vSphere documentation and use VMware Data Recovery (called VMware vSphere Data Protection starting with vSphere Release 5.1) to create a backup of your system and each of your virtual machines.
For complete details on this backup, see the *VMware Data Recovery Administration Guide* or the *vSphere Data Protection Administration Guide*.

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

Taking a Snapshot Using VMware vCenter

Virtual machine snapshots are *pictures* of your system at a specific point in time, and are not the same as backups. Snapshots are stored on the physical drives containing your virtual machines. If you do not delete these snapshots in a timely manner, your end users might experience degraded audio and video due to a known issue that affects virtual machine performance. Therefore, for performance reasons, we recommend that you use backups or keep your virtual machine backups in a storage location that is different from the physical drives that contain your virtual machines. (For more information on this known issue with VMware snapshots, go to the VMware web site and read the white paper, *Best Practices for Running VMware vSphere on Network Attached Storage*. You can also search the VMware KnowledgeBase for "snapshot impact performance" for additional information.)

Before doing most system-altering procedures, Cisco recommends that you backup your system or take a snapshot of each of the virtual machines. You can backup your system by using VMware Data Recovery (VMware vSphere Data Protection starting with vSphere Release 5.1) or taking a snapshot of each virtual machine. (VMware Data Recovery/vSphere Data Protection is included with VMware vSphere, except in the vSphere Essentials Kit.)

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

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

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

Note Cisco recommends you keep snapshots no longer than approximately 24 hours. If you want to keep them longer, then create a backup instead. For more information on VMware Data Recovery (VMware vSphere Data Protection starting with vSphere Release 5.1), see Creating a Backup Using VMware vCenter, on page 4.

Procedure

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

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

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

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

What to Do Next

- Complete the procedure and test your system to confirm that it is successful.
- If you need to revert to a snapshot, be sure the snapshot for each virtual machine was taken at the same time. Powering on a system with mismatched snapshots may result in possible database corruption.

Attaching an Existing VMDK File to a New Virtual Machine

This section describes how to attach 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`. If you have previously upgraded your system, the filename does not follow the naming convention of the existing virtual machine.

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

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

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

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

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

Step 10 Arrange the two datastore browser windows (for the 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**.

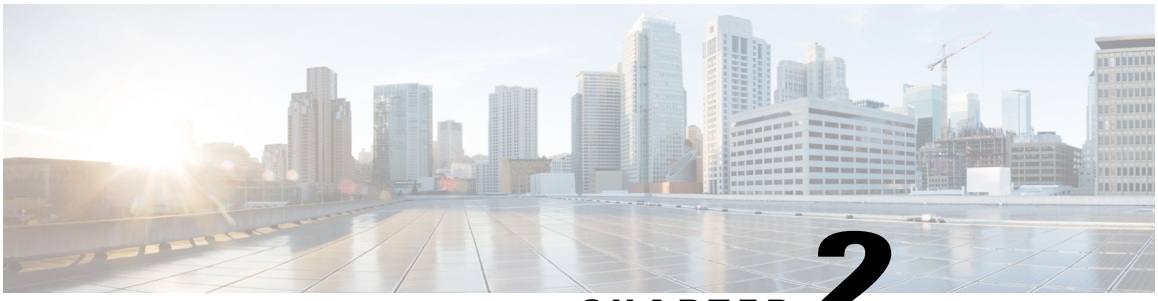
Step 19 Select **Browse**, and navigate to the datastore where the new expanded or upgraded Admin virtual machine is located. Navigate to the new Admin virtual machine folder. Double-click this folder, then select the virtual disk you copied over in Step 11. Select **OK**.

Step 20 In the **Virtual Device Node** drop-down list, select **SCSI (0:3)**, 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, page 9
- Networking Checklist for a System with Public Access and Split-Horizon DNS, page 9
- Networking Checklist for a System With No Public Access, page 10

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, page 12
- Installation Checklist, page 13
- Required Information For an Automatic Deployment, page 13
- Deploying the OVA File From the VMware vSphere Client, page 16
- Selecting Your Language for Setup, page 28
- Confirming the Deployment, page 29
- Confirming the Size of Your System, page 29
- Choosing What System to Install, page 29
- Choosing the Type of System Deployment, page 30
- Providing VMware vCenter Credentials, page 30
- Choosing vCenter Settings for your Media Virtual Machine, page 31
- Entering Networking Information for the Media Virtual Machine, page 31
- Adding Public Access, page 32
- Choosing vCenter Settings for Your Internet Reverse Proxy, page 32
- Entering the Networking Information for the Internet Reverse Proxy, page 33
- Entering the Public VIP Address, page 33
- Entering the Private VIP Address, page 34
- WebEx Site and WebEx Administration URLs, page 34
- Entering the WebEx Site and Administration URLs, page 36
- Confirming That Your Network is Configured Correctly, page 36
- Deploying Your Virtual Machines, page 36
- Checking Your System, page 37

General Concepts For Your System Deployment

System Sizes

- 50 concurrent users system
  - Typically supports a company between 500 and 1000 employees
  - Primary system (without HA) comprises an Admin virtual machine and an optional Internet Reverse Proxy (for public access)
- 250 concurrent users system
  - Typically supports a company between 2500 and 5000 employees
  - Primary system (without HA) comprises an Admin virtual machine, a Media virtual machine, and an optional Internet Reverse Proxy (for public access)
- 800 concurrent users system
  - Typically supports a company between 8000 and 16,000 employees
  - Primary system (without HA) comprises an Admin virtual machine, a Media virtual machine, and an optional Internet Reverse Proxy (for public access)
- 2000 concurrent users system
  - Typically supports a company between 20,000 and 40,000 employees
  - Primary system (without HA) comprises an Admin virtual machine, 3 Media virtual machines, 2 Web machines, and an optional Internet Reverse Proxy (for public access)

Terms Used During the Deployment

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

Installation Checklist

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

Networking Changes

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

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

  Cisco recommends public access as it results in a better user experience for your mobile workforce.

- Type of DNS setup at your company: split-horizon DNS or a non-split horizon DNS (most common DNS configuration).

  For more information about these types of DNS setup, see the *Cisco WebEx Meetings Server Planning Guide*.

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

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

Select the right checklist for your deployment:

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

Required Information

Note The required information varies if you are doing an automatic deployment (supported for 50 concurrent users, 250 concurrent users, and 800 concurrent users) systems or manual deployment (supported for all system sizes). Cisco recommends you select an automatic deployment unless you are deploying a 2000 user system, that requires a manual deployment. Refer to the appropriate link below.

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

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

Required Information For an Automatic Deployment

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

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

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

Field Name	Description	Value For Your System
vCenter URL	Secure http address of the vCenter server for the virtual machines in your system.	
vCenter Username	Username to deploy the virtual machines for your system. This user must have administrator privileges: to deploy, configure, power on or off, and delete virtual machines.	
vCenter Password	Password of the vCenter user.	
(250 and 800 concurrent user systems only) ESXi Host	ESXi host for the media virtual machine. **Note** This ESXi host must be on the same vCenter, as the vCenter URL above.	
(250 and 800 concurrent user systems only) Datastore	Datastore for the media virtual machine.	
(250 and 800 concurrent user systems only) Virtual Machine Port Group	Port group for the media virtual machine. **Note** Cisco recommends you choose the same port group that you selected for the Admin virtual machine.	
(250 and 800 concurrent user systems only) FQDN for the media virtual machine	Fully qualified domain name (all lowercase characters) for the media virtual machine.	
(250 and 800 concurrent user systems only) IPv4 address for the media virtual machine	IPv4 address for the media virtual machine. We will automatically look up the corresponding IPv4 address for this media virtual machine.	

Field Name	Description	Value For Your System
(Public access only) ESXi host	ESXi host for the Internet Reverse Proxy virtual machine. **Note** Cisco recommends that you select a different ESXi host than you chose for the Admin and other internal virtual machine. To enable traffic to the Internet Reverse Proxy, be sure the ESXi host is configured with a port group that can route the VLAN whose IP address is used by the Internet Reverse Proxy.	
(Public access only) Datastore	Datastore for the Internet Reverse Proxy virtual machine.	
(Public access only) Virtual Machine Port Group	Port group for the Internet Reverse Proxy virtual machine. **Note** For security reasons, Cisco recommends that you select a different port group than you chose for the Admin virtual machine.	
(Public access only) FQDN for the Internet Reverse Proxy	Fully qualified domain name (all lowercase characters) for the Internet Reverse Proxy virtual machine.	
(Public access only) Internet Reverse Proxy IPv4 Address	IPv4 address for the Internet Reverse Proxy virtual machine. We will automatically look up the corresponding IPv4 address for this Internet Reverse Proxy virtual machine.	
(Public access only) IPv4 Gateway	IPv4 gateway for the Internet Reverse Proxy virtual machine.	
(Public access only) IPv4 Subnet Mask	Subnet mask for the Internet Reverse Proxy virtual machine.	
(Public access only) Primary DNS Server IPv4 Address	DNS server for the Internet Reverse Proxy virtual machine.	
(Public access only) Secondary DNS Server IPv4 Address	(Optional) Additional DNS server for the Internet Reverse Proxy virtual machine.	
Public VIP	IP address for the WebEx site URL (site users access to host and attend meetings)	

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

What To Do Next

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

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

Deploying the OVA File From the VMware vSphere Client

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

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

Before You Begin

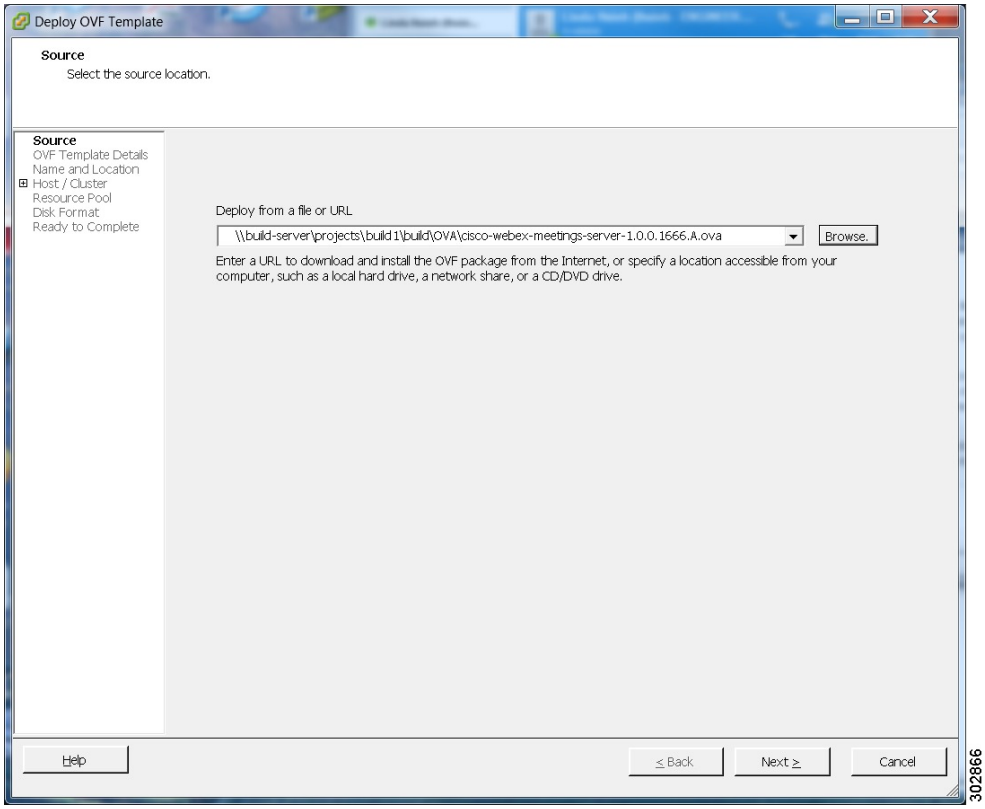
Obtain the Cisco WebEx Meetings Server OVA file for your system and place it in a location that is accessible from VMware vSphere.

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

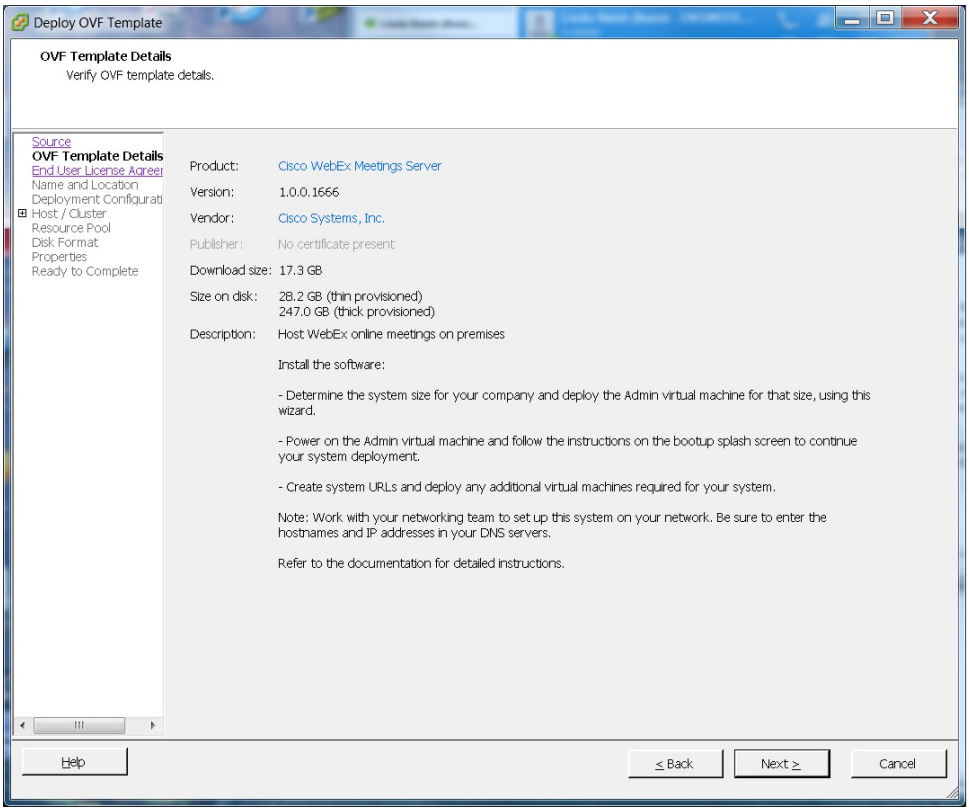
Procedure

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

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



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.



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

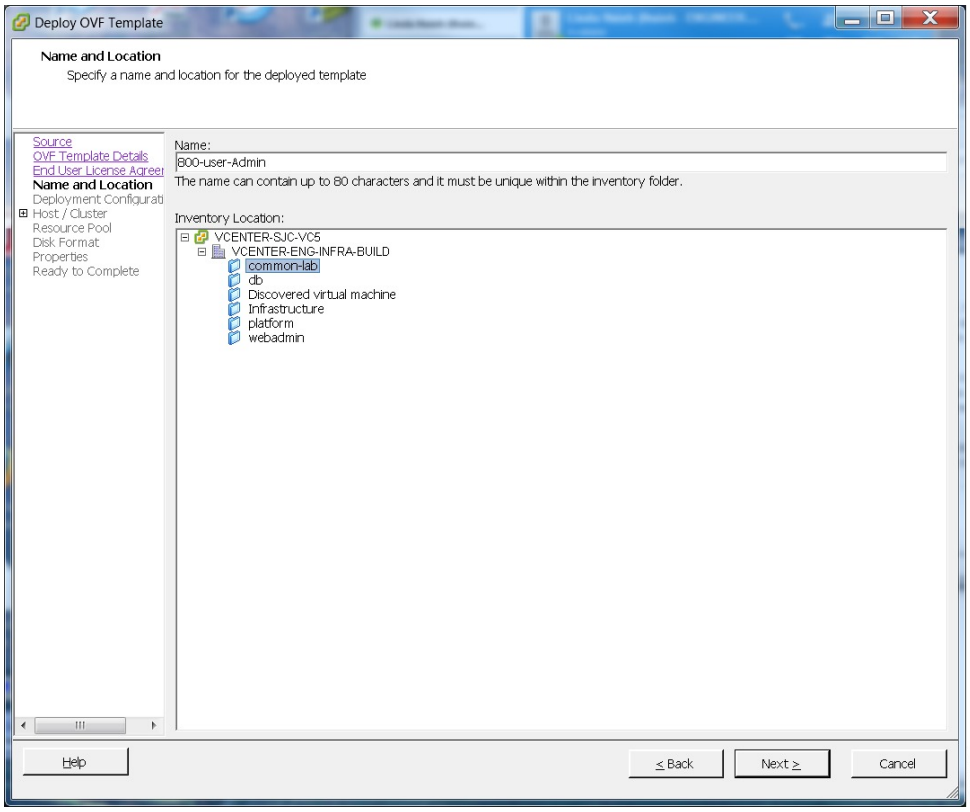
Step 5 Navigate to, and select the location, in the vCenter inventory, where you'd like to place the Admin virtual machine.

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.

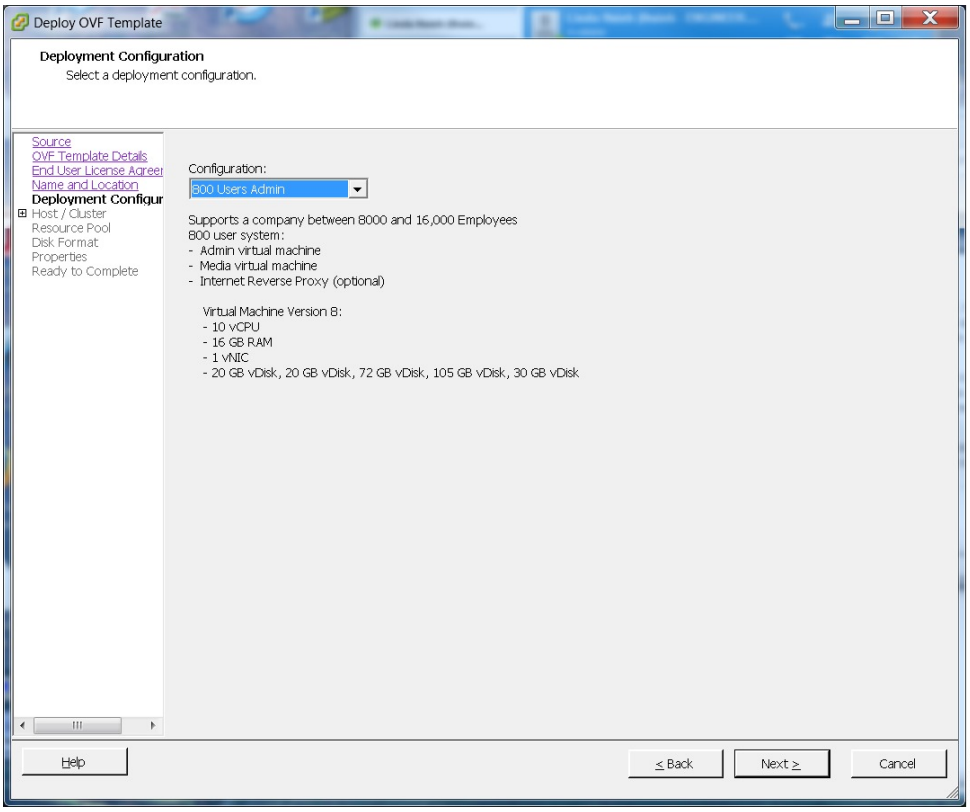
Note You must deploy the Admin virtual machine before any other virtual machines. If you select automatic deployment (recommended), then we will deploy the other virtual machines for you. If you choose manual deployment (required for 2000 concurrent users system), then you will deploy the other virtual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

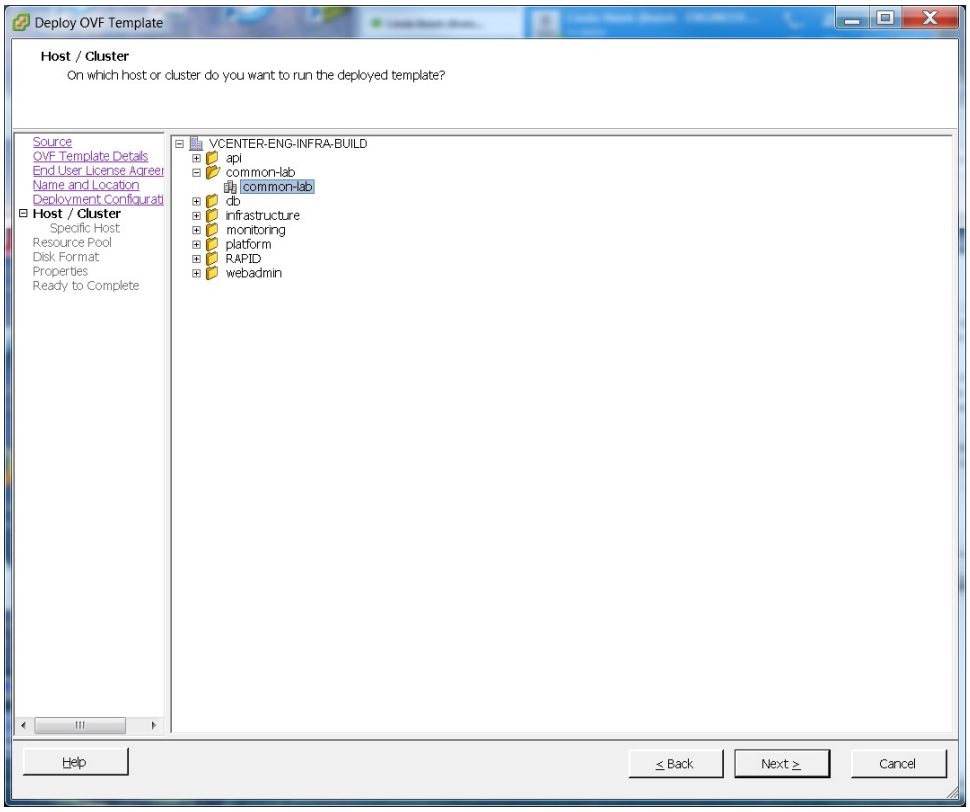
Note All the internal virtual machines for your system must be in the same subnet as the Admin virtual machine. (Depending on the system size you select, you may need one or more media and web internal virtual machines.)



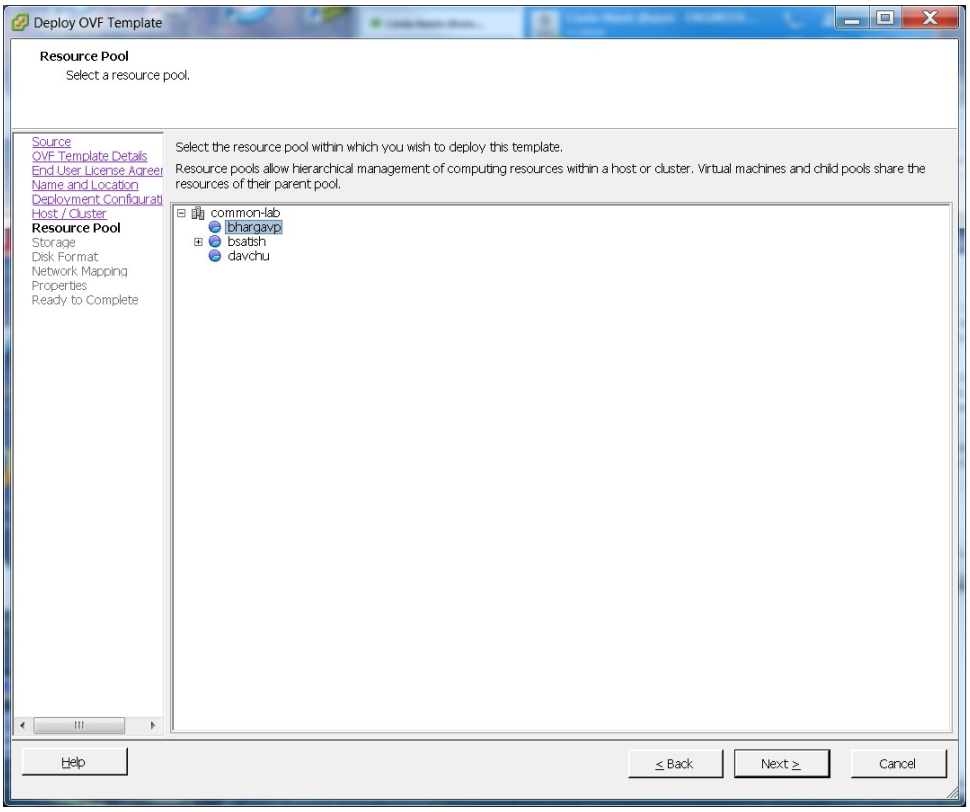
Step 7 From the drop-down list, select the virtual machine for your system size then select **Next**.
Be sure to deploy the Admin virtual machine before any other virtual machines in your system.



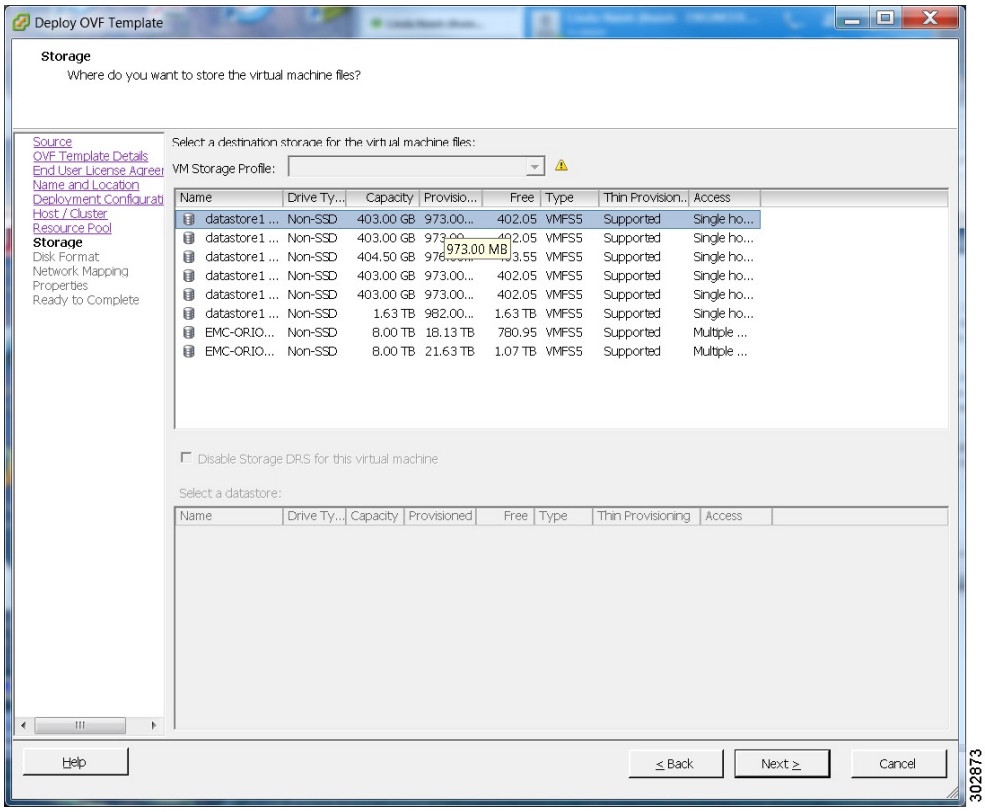
Step 8 Navigate thru the vCenter inventory and select the ESXi host or cluster where you want to deploy the virtual machines for your system. Select **Next**.

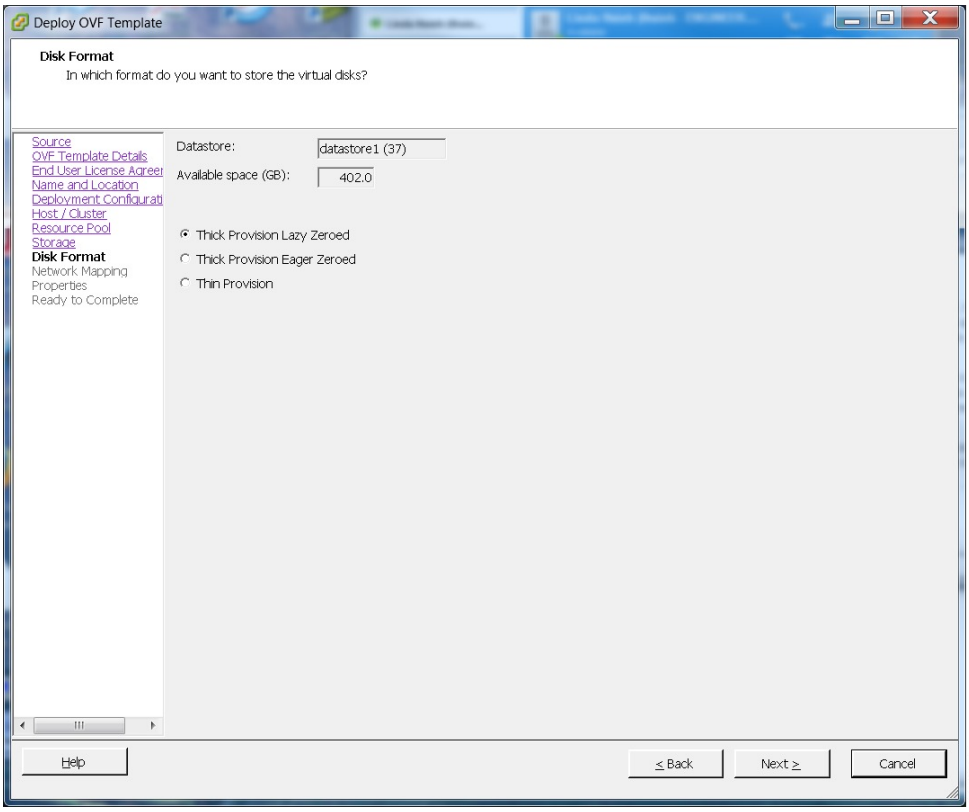


Step 9 If the cluster contains a resource pool, then select the resource pool where you want to deploy the OVA template and select **Next**.
Resource pool in this context refers to storage, and not the allocation of CPU and memory. VMware resource sharing is not supported in this release of Cisco WebEx Meetings Server.



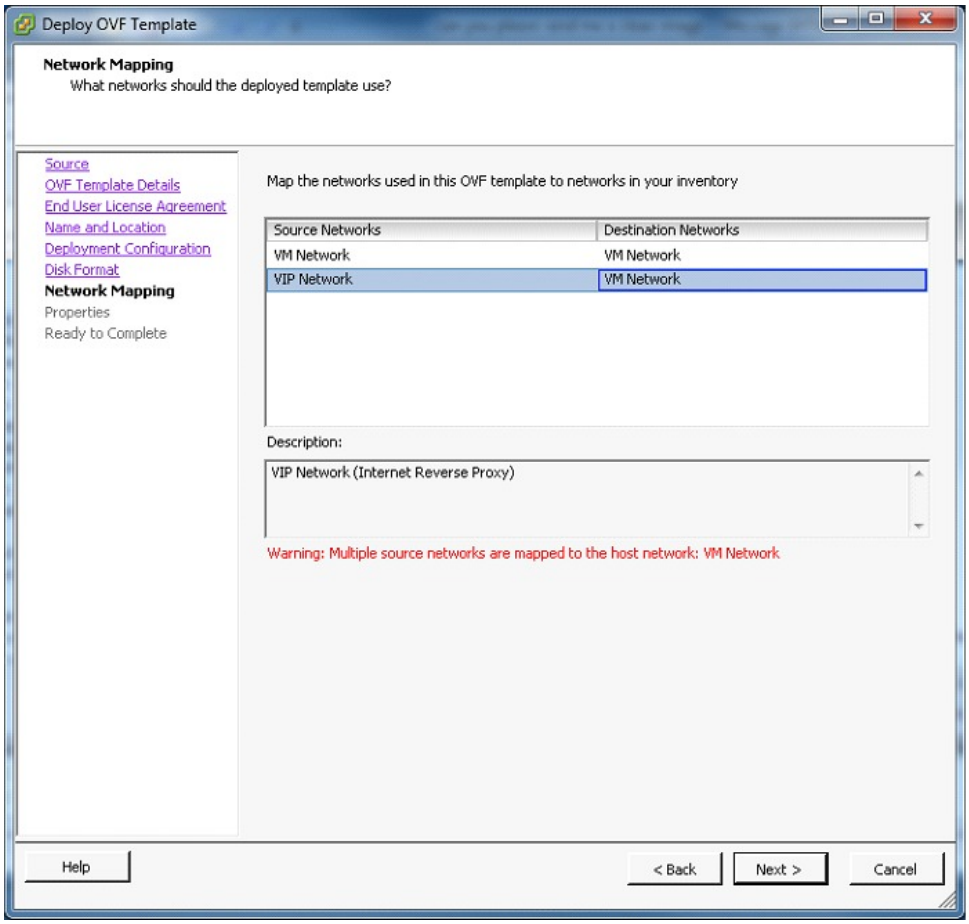
Step 10 Select the datastore for your virtual machine and the kind of provisioning for your virtual machine.
You must select thick provisioning and create the maximum virtual disk space required for your system. With **Thin Provision**, VMware allocates the file system space on an "as-needed" basis, resulting in poor performance.


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



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

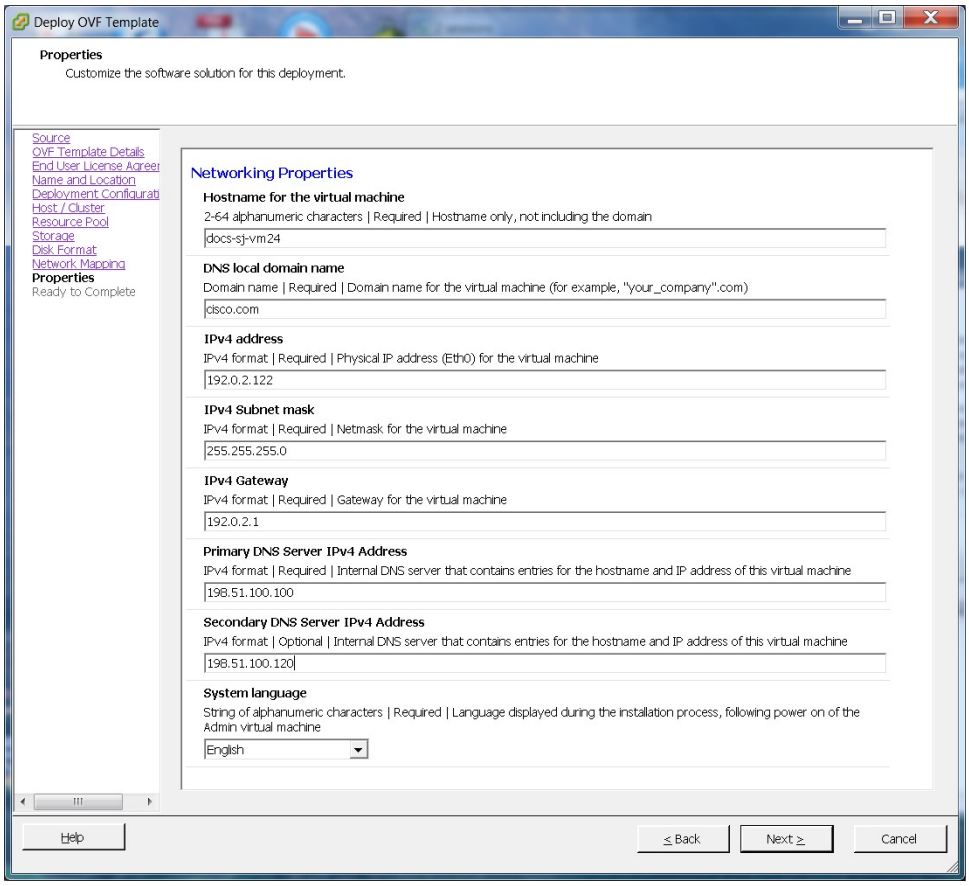
Note Both the "VM Network" and the "VIP Network" must be mapped to the same value in the "Destination Network" column. You can ignore the warning message about multiple source networks mapped to the same host network.



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

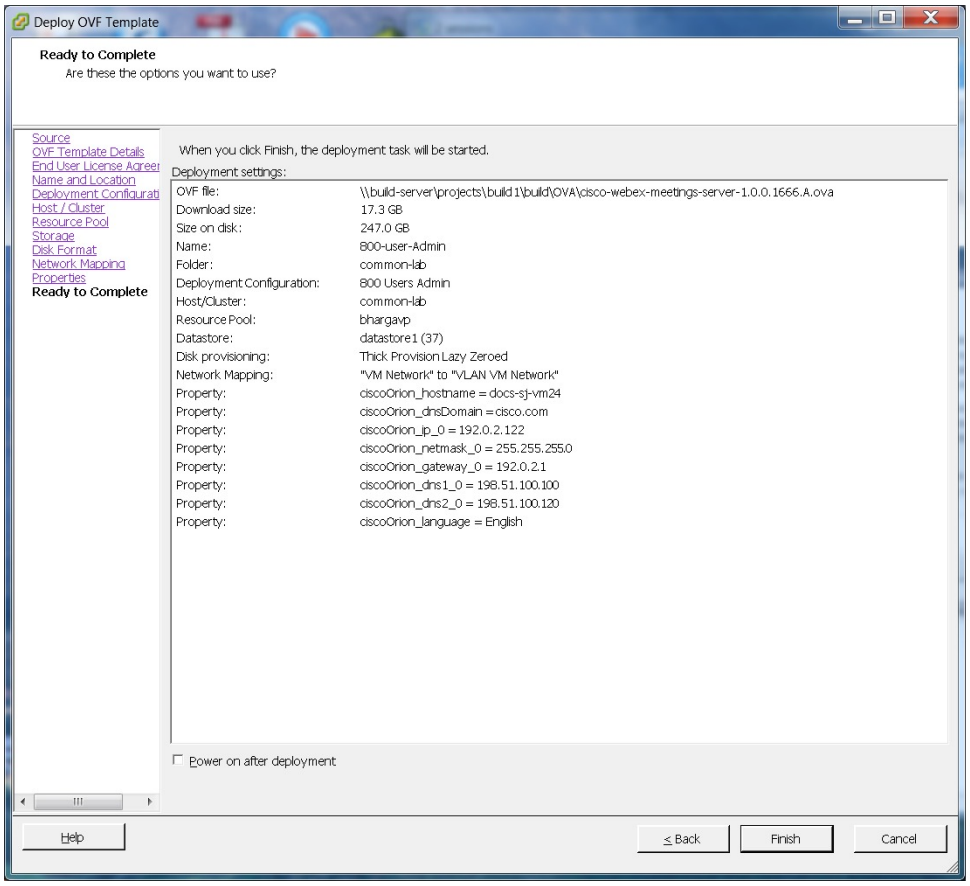
- Hostname of the virtual machine (do not include the domain as you will enter this in the next field)
- Domain for the virtual machine
- IPv4 address (Eth0) of the virtual machine
- Subnet mask of the virtual machine
- Gateway IP address
- Primary DNS server that contains entries for the hostname and 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

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



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**.



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 Cisco recommends you deploy the rest of the virtual machines for your system at this time. This avoids any issues including time outs or when powering on virtual machines.
- 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 Deployment

Procedure

Step 1 Confirm if you are deploying a new system or expanding an existing system.

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 34

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.

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

Procedure

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

Step 2 Choose the datastore for the Internet Reverse Proxy.

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

Step 4 Select **Next**.

Entering 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.

Before You Begin

- For security reasons, Cisco recommends the Internet Reverse Proxy should be located on a different subnet from the Admin virtual machine.
- 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, comprising all lowercase characters. However, you cannot use the following as the hostname in the site URLs:

- the same name as the hostnames for any of the virtual machines comprising the system
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version
- WBXService
- webex

Entering the WebEx Site and Administration URLs

- 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).

Note The Administration site URL used during the deployment process is the Admin virtual machine's hostname. However, during the basic configuration the hostname is replaced with the actual Administration site URL. As a result, the first time you sign in to the Administration site, the system may prompt you to accept the certificate exception.

- 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.

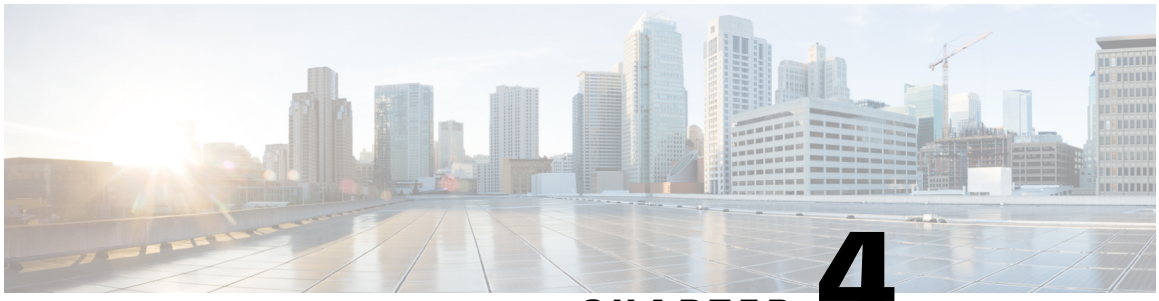
- We recommend you power down all the virtual machines from VMware vCenter and manually delete them. Then reattempt the system deployment on a system with resources that meet or exceed the minimum requirements.
- You may choose to proceed with your current installation. If you do, you must acknowledge 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, page 39
- Installation Checklist, page 40
- Required Information For a Manual Deployment, page 41
- Deploying the OVA File From the VMware vSphere Client, page 42
- Selecting Your Language for Setup, page 54
- Confirming the Deployment, page 55
- Confirming the Size of Your System, page 55
- Choosing What System to Install, page 55
- Choosing the Type of System Deployment, page 56
- Adding Public Access, page 56
- Entering the Public VIP Address, page 57
- Entering the Private VIP Address, page 57
- WebEx Site and WebEx Administration URLs, page 58
- Entering the WebEx Site and Administration URLs, page 59
- Confirming That Your Network is Configured Correctly, page 60
- Deploying Your Virtual Machines, page 60
- Checking Your System, page 61

General Concepts For Your System Deployment

System Sizes

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

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

- 250 concurrent users system
  - Typically supports a company between 2500 and 5000 employees
  - Primary system (without HA) comprises an Admin virtual machine, a Media virtual machine, and an optional Internet Reverse Proxy (for public access)

- 800 concurrent users system
  - Typically supports a company between 8000 and 16,000 employees
  - Primary system (without HA) comprises an Admin virtual machine, a Media virtual machine, and an optional Internet Reverse Proxy (for public access)

- 2000 concurrent users system
  - Typically supports a company between 20,000 and 40,000 employees
  - Primary system (without HA) comprises an Admin virtual machine, 3 Media virtual machines, 2 Web machines, and an optional Internet Reverse Proxy (for public access)

Terms Used During the Deployment

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

Installation Checklist

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

Networking Changes

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

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

  Cisco recommends public access as it results in a better user experience for your mobile workforce.

- Type of DNS setup at your company: split-horizon DNS or a non-split horizon DNS (most common DNS configuration).

  For more information about these types of DNS setup, see the *Cisco WebEx Meetings Server Planning Guide*.

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

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

Select the right checklist for your deployment:

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

Required Information

Note The required information varies if you are doing an automatic deployment (supported for 50 concurrent users, 250 concurrent users, and 800 concurrent users) systems or manual deployment (supported for all system sizes). Cisco recommends you select an automatic deployment unless you are deploying a 2000 user system, that requires a manual deployment. Refer to the appropriate link below.

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

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

Required Information For a Manual Deployment

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

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

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

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

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

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

What To Do Next

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

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

Deploying the OVA File From the VMware vSphere Client

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

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

Before You Begin

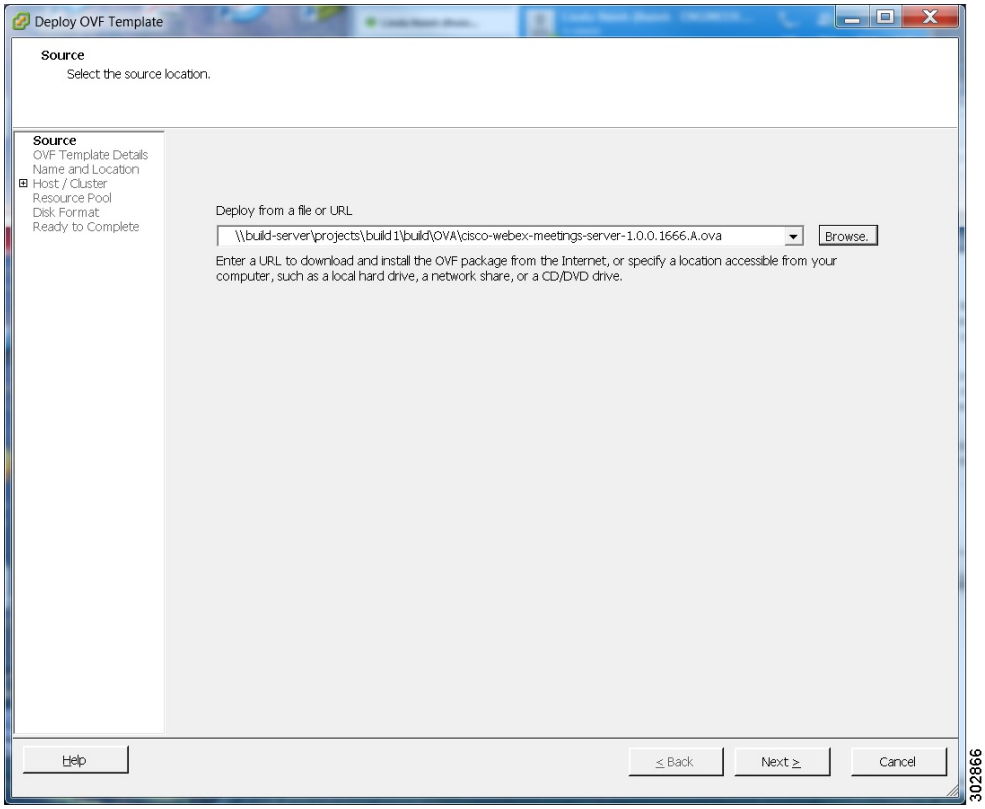
Obtain the Cisco WebEx Meetings Server OVA file for your system and place it in a location that is accessible from VMware vSphere.

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

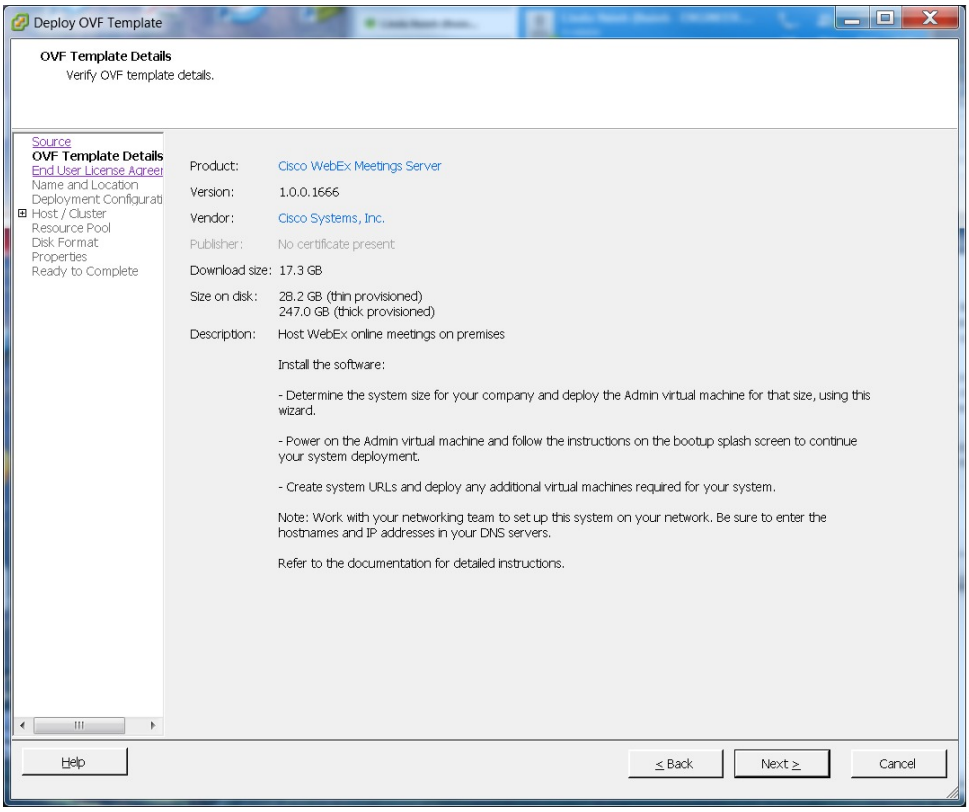
Procedure

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

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



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.



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

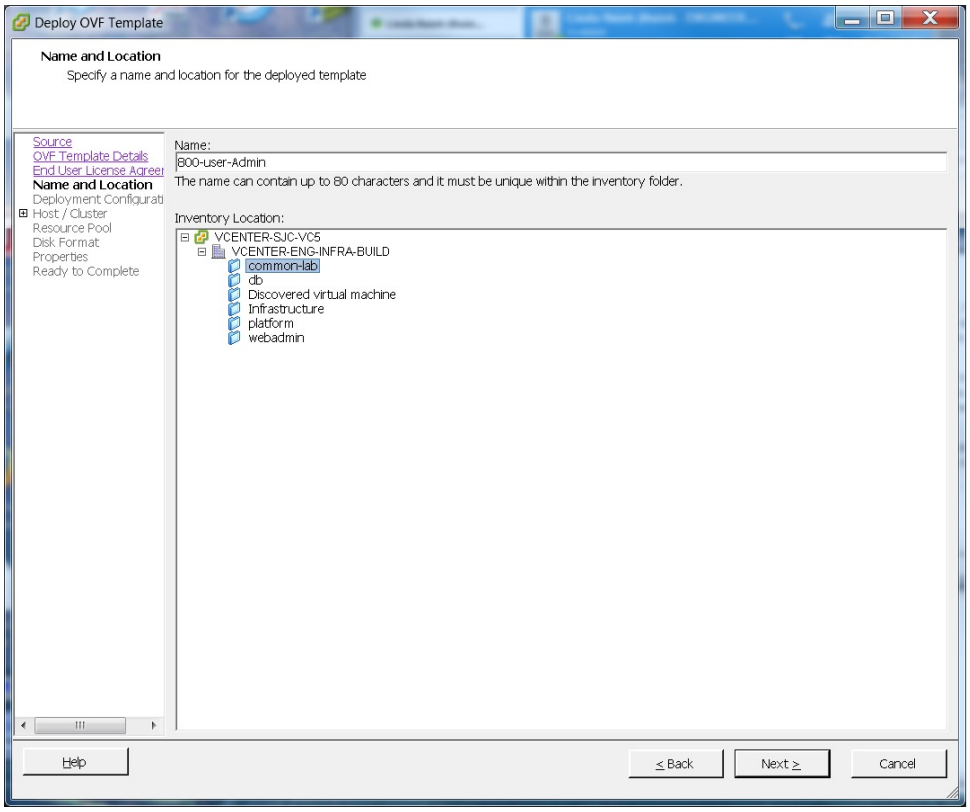
Step 5 Navigate to, and select the location, in the vCenter inventory, where you'd like to place the Admin virtual machine.

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.

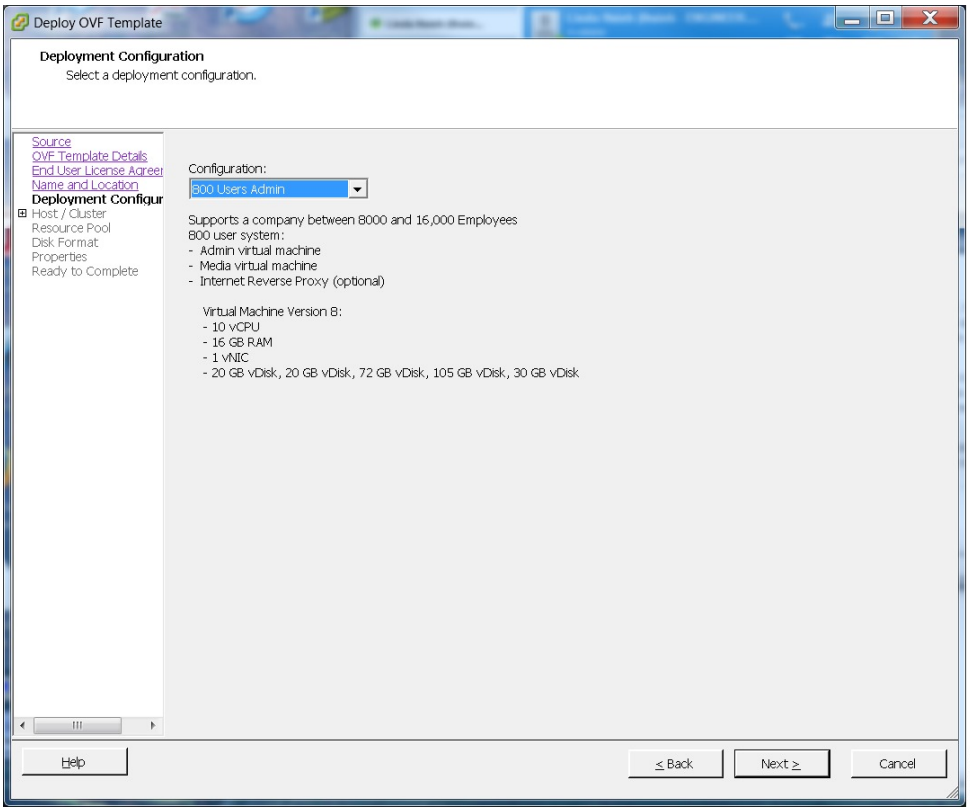
Note You must deploy the Admin virtual machine before any other virtual machines. If you select automatic deployment (recommended), then we will deploy the other virtual machines for you. If you choose manual deployment (required for 2000 concurrent users system), then you will deploy the other virtual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

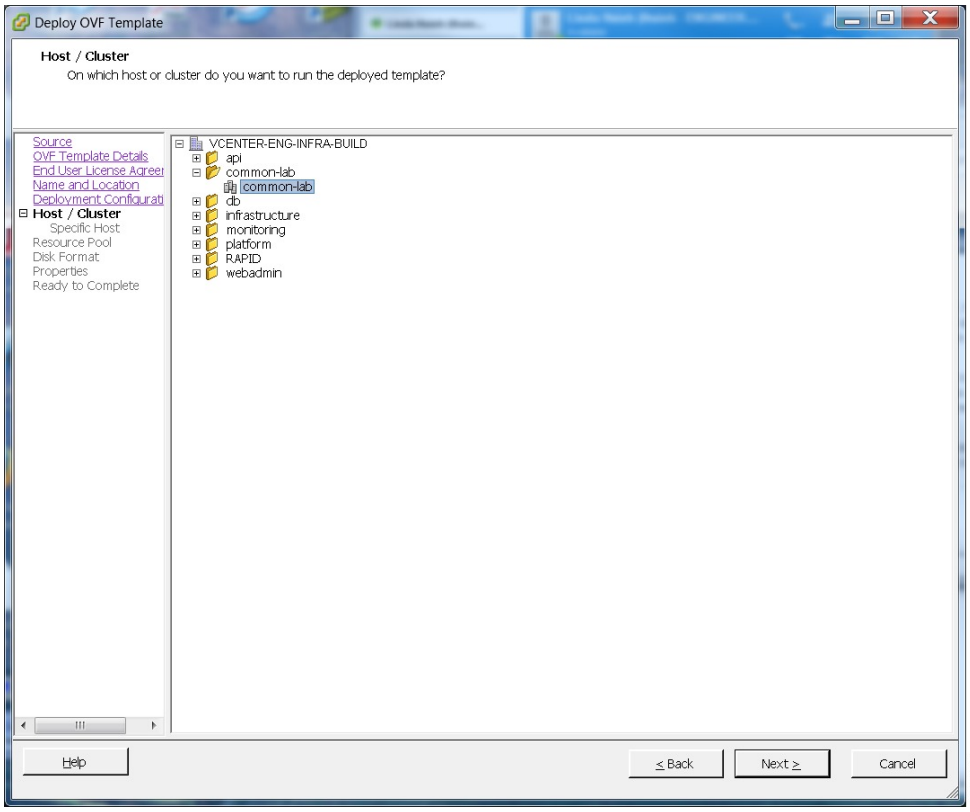
Note All the internal virtual machines for your system must be in the same subnet as the Admin virtual machine. (Depending on the system size you select, you may need one or more media and web internal virtual machines.)



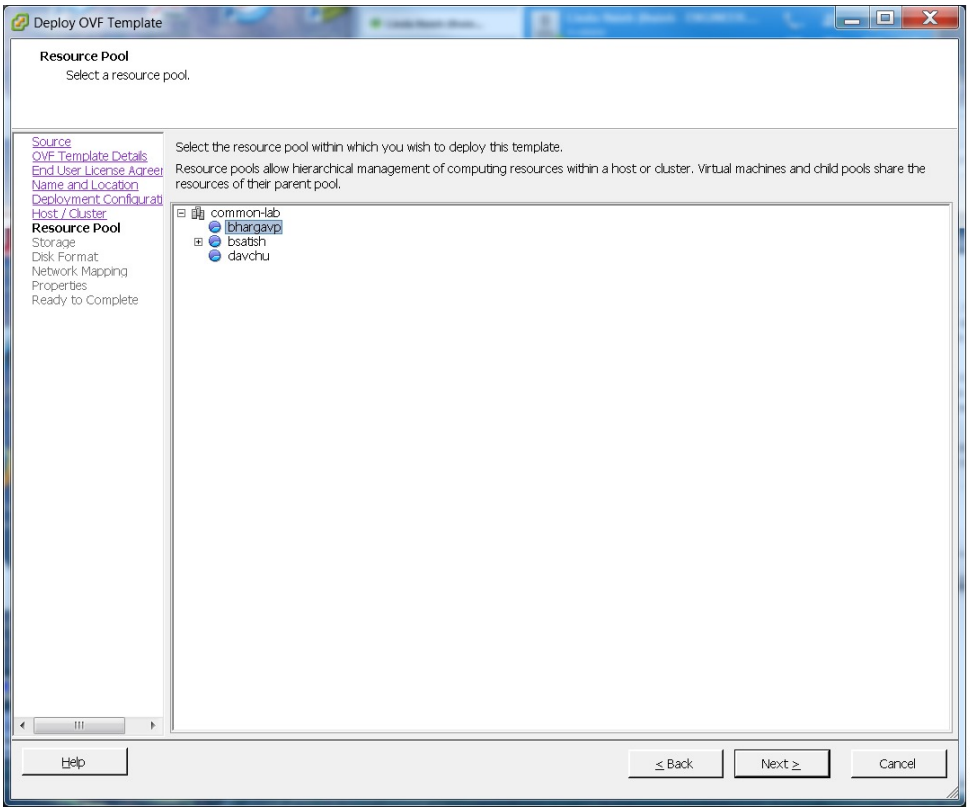
Step 7 From the drop-down list, select the virtual machine for your system size then select **Next**.
Be sure to deploy the Admin virtual machine before any other virtual machines in your system.



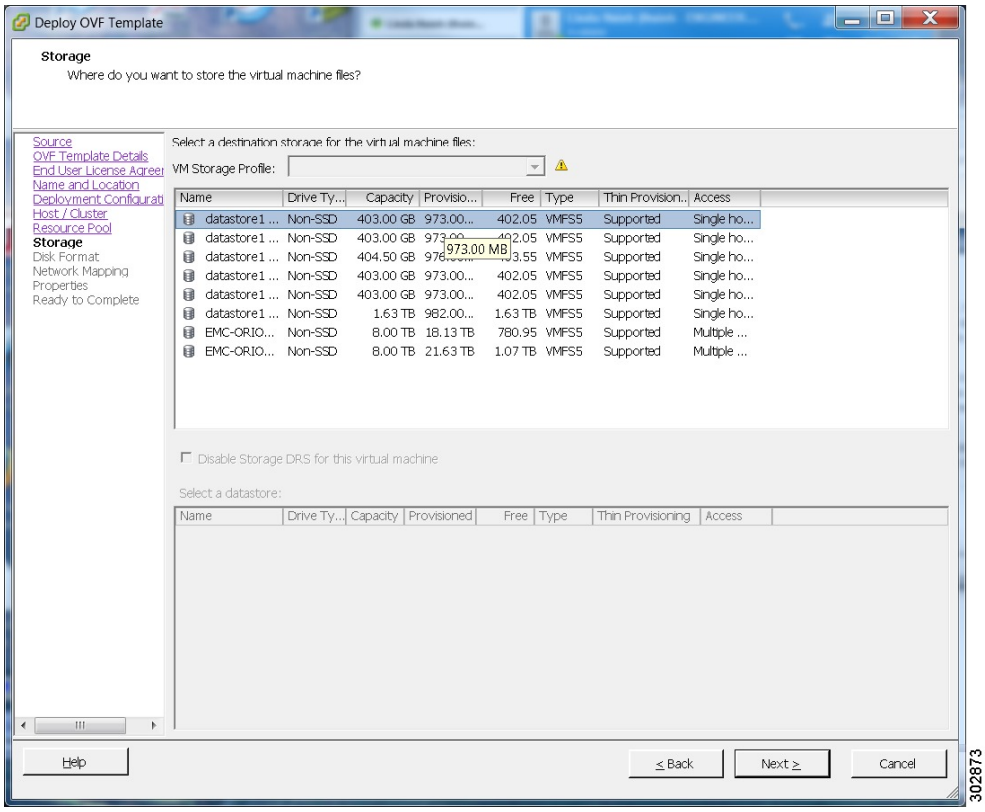
Step 8 Navigate thru the vCenter inventory and select the ESXi host or cluster where you want to deploy the virtual machines for your system. Select **Next**.

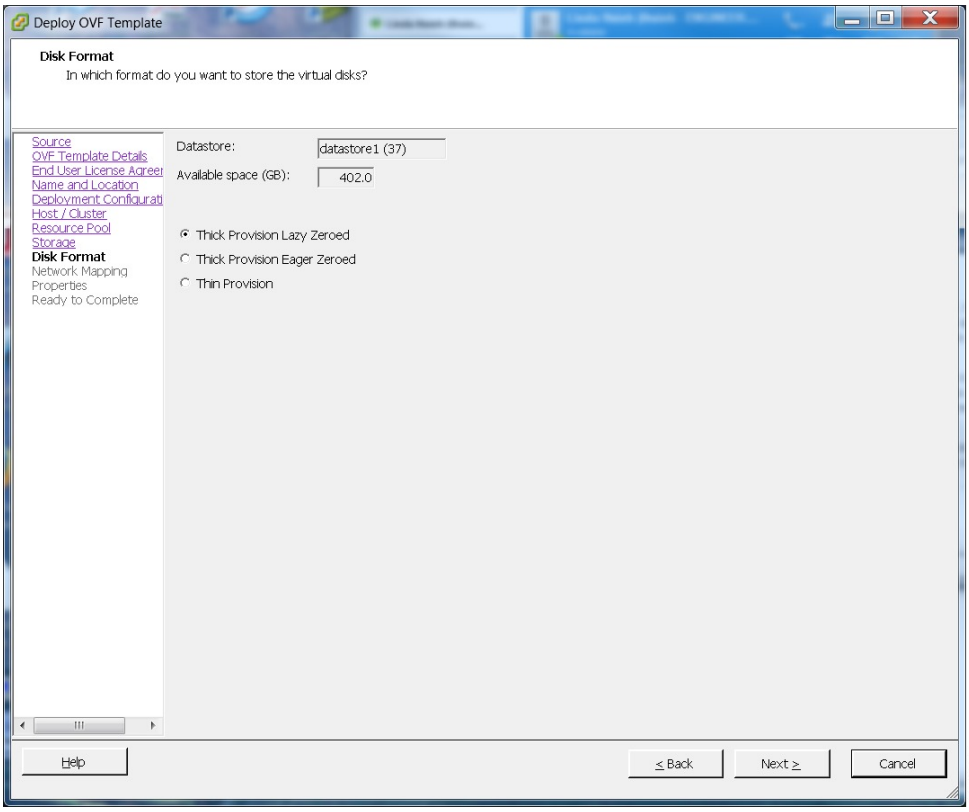


Step 9 If the cluster contains a resource pool, then select the resource pool where you want to deploy the OVA template and select **Next**.
Resource pool in this context refers to storage, and not the allocation of CPU and memory. VMware resource sharing is not supported in this release of Cisco WebEx Meetings Server.



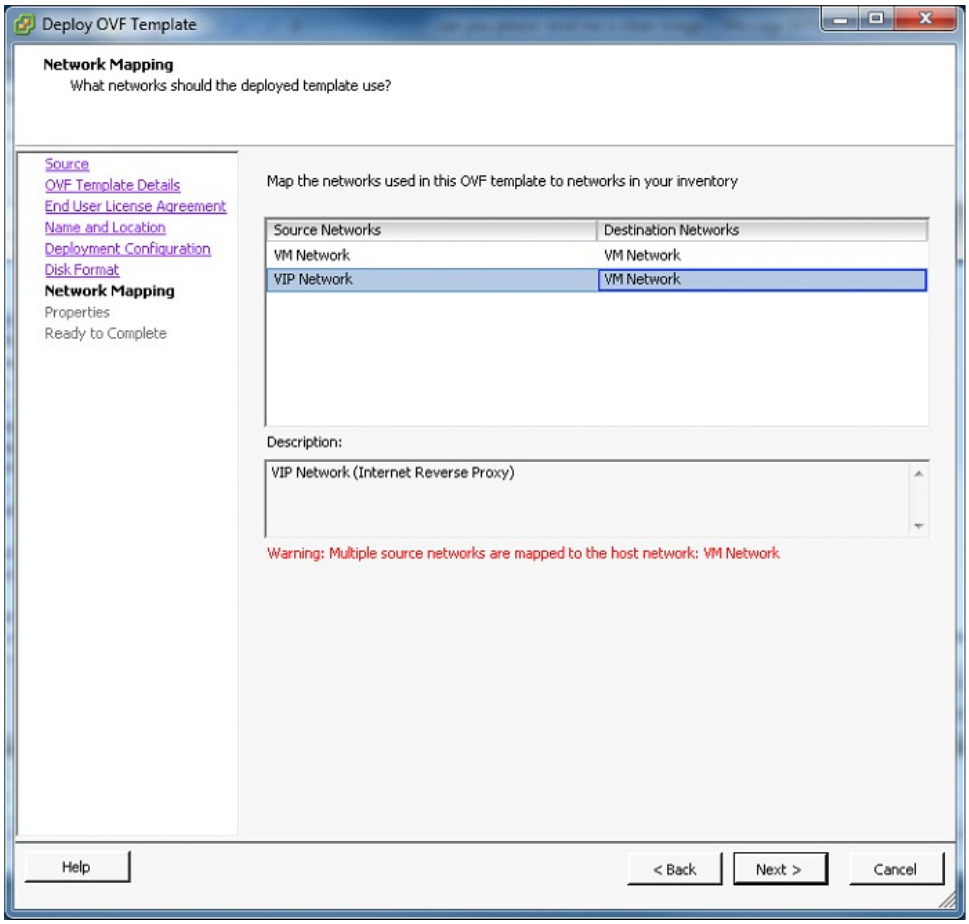
Step 10 Select the datastore for your virtual machine and the kind of provisioning for your virtual machine.
You must select thick provisioning and create the maximum virtual disk space required for your system. With **Thin Provision**, VMware allocates the file system space on an "as-needed" basis, resulting in poor performance.


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



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

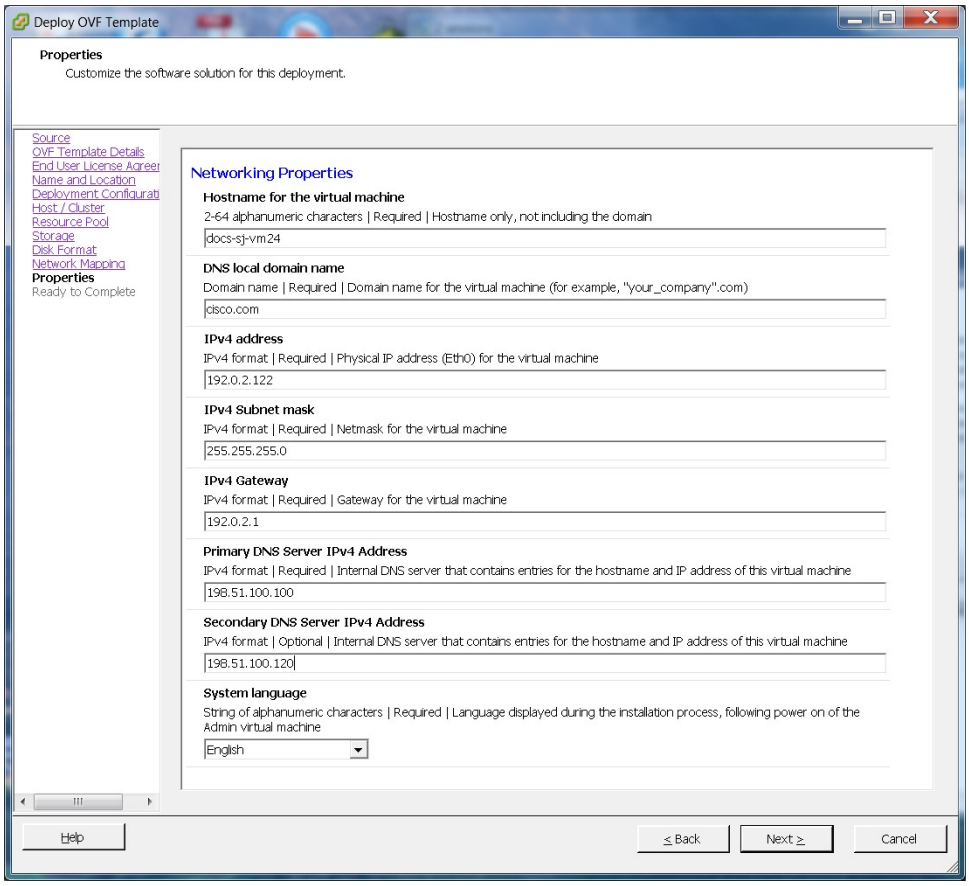
Note Both the "VM Network" and the "VIP Network" must be mapped to the same value in the "Destination Network" column. You can ignore the warning message about multiple source networks mapped to the same host network.



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

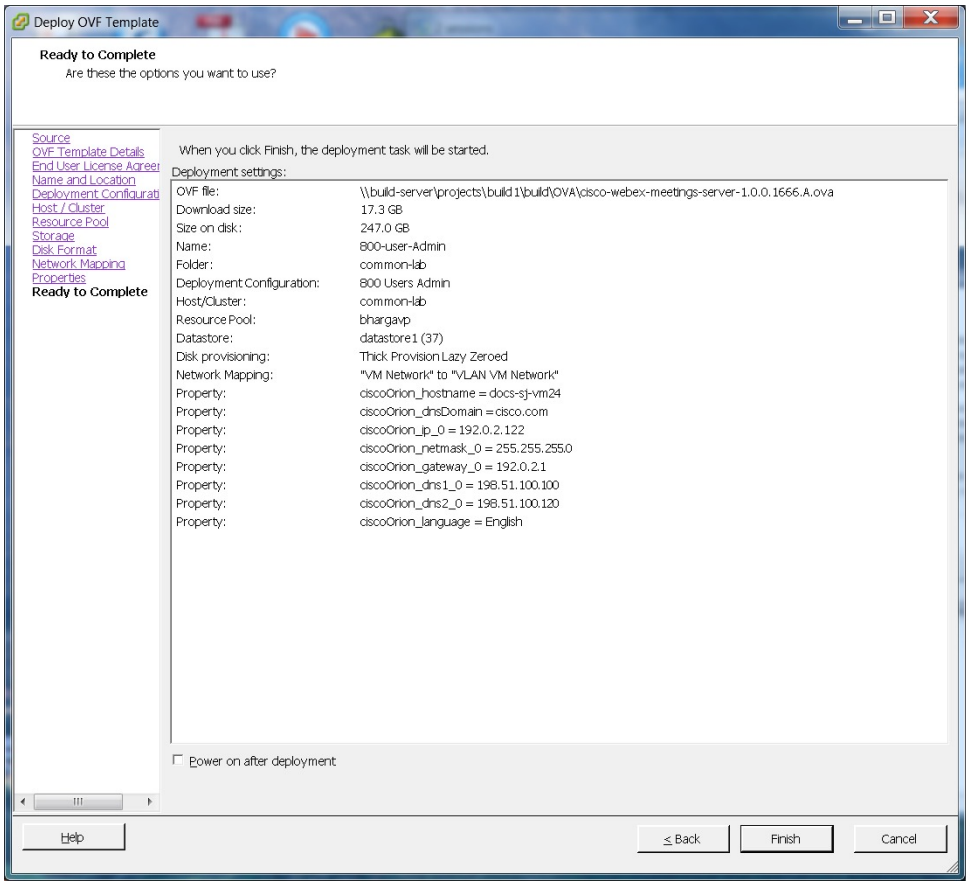
- Hostname of the virtual machine (do not include the domain as you will enter this in the next field)
- Domain for the virtual machine
- IPv4 address (Eth0) of the virtual machine
- Subnet mask of the virtual machine
- Gateway IP address
- Primary DNS server that contains entries for the hostname and 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

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



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**.



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 Cisco recommends you deploy the rest of the virtual machines for your system at this time. This avoids any issues including time outs or when powering on virtual machines.
- 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 Deployment

Procedure

Step 1 Confirm if you are deploying a new system or expanding an existing system.

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 34

Entering the Public VIP Address

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

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

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

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

Entering the Private VIP Address

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

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

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

Before You Begin

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

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

WebEx Site and WebEx Administration URLs

WebEx Site URL

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

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

WebEx Administration URL

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

Names for the WebEx Site and WebEx Administration URLs

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

- the same name as the hostnames for any of the virtual machines comprising the system
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services

- emails
- maintenance
- manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version
- WBXService
- webex

Entering the WebEx Site and Administration URLs

- 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).

Note The Administration site URL used during the deployment process is the Admin virtual machine's hostname. However, during the basic configuration the hostname is replaced with the actual Administration site URL. As a result, the first time you sign in to the Administration site, the system may prompt you to accept the certificate exception.

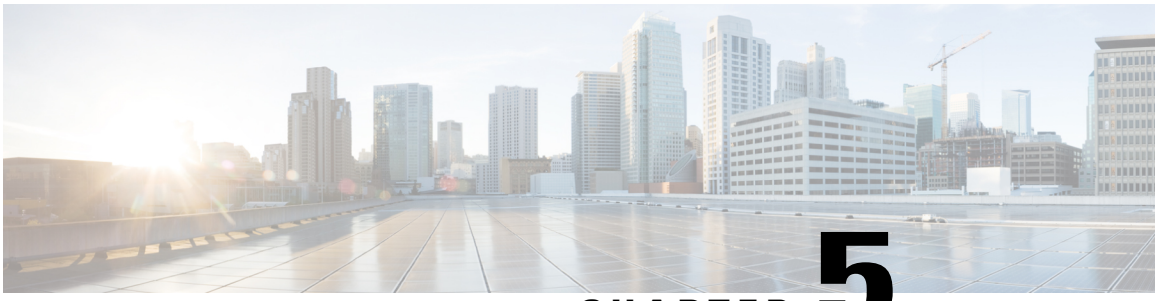
- Complete one of the following:
  - If there are no errors, then when the status shows all green checks, select **Next**. Continue with Setting Up the Mail Server For Your System, on page 63.
  - If there is a problem with network connectivity, then check that your WebEx Site and Administration URLs 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 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, page 63
- Setting Up the Time Zone and Locale for the System, page 64
- Confirming the Mail Server, Time Zone, and Locale Settings, page 64
- Setting Up the First Administrator Account for Your System, page 64
- Testing the System, page 65

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

Before You Begin

If you are running Windows 7 and have your Cisco WebEx site open in an Internet Explorer 10 browser, you may want to select the document Internet Explorer 10 standards to make sure all the buttons in the application work properly.

- Select **Tools** > **Developer Tools**.
- At the top of the Developer Tools window, select **Document Mode: IE7 Standards** > **Internet Explorer 10 Standards**.

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.

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, then confirm it by entering it again.

Step 3 Select **Next** to create your password.

Step 4 Enter your password, then confirm it by entering it again.

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

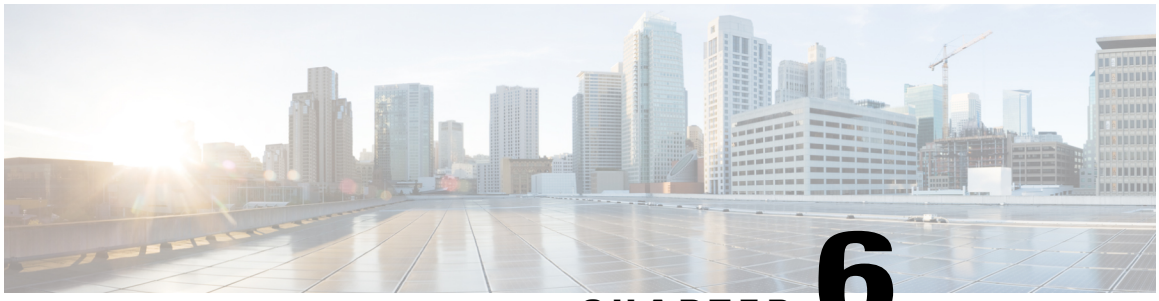
Step 6 You must sign in to the system and add additional users. Upon creation of each new user, the system sends an email to each user, welcoming and asking the user to sign in and create a password.
Upon initial sign in, each administrator will have an opportunity to view a tutorial of the system. The administrators can view the tutorial immediately, or decide to view it later.

Testing the System

Some of the recommended tests to run on the system are listed in this section. 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.

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

- 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, page 67
- Preparing For a System-Altering Procedure, page 68

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, by creating a backup of your system.

Although you may choose to do so, backups are not required for an expansion or upgrade of your system. During an expansion or an upgrade, you deploy a new system and transfer data from your existing system to the new system. If there is a problem with the expansion or upgrade, you can power off the new system and continue to use your existing system.

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

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

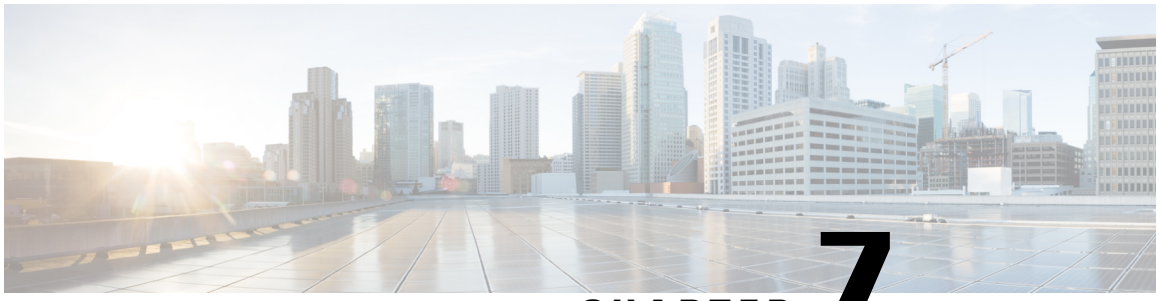
Step 2 Select **Turn On Maintenance Mode**.

Step 3 Use VMware Data Recovery (called VMware vSphere Data Protection starting with vSphere Release 5.1) to create a backup of each of your virtual machines.
A backup will help you revert your virtual machine to its state before the system-altering procedure. For further information, see Creating a Backup Using VMware vCenter, on page 4. For complete details on this backup, see the *VMware Data Recovery Administration Guide* or the *vSphere Data Protection Administration Guide*.

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

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

Step 5 Continue with the system-altering procedure.



CHAPTER 7

Adding a High Availability System

- Adding a HA System Using Automatic Deployment, page 71
- Adding a HA System Using Manual Deployment, page 73
- Confirming Your Primary System and Your HA System Are at the Same Version, page 75
- Adding a High Availability System, page 76
- Testing the System, page 77

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 adds virtual machines to your system, your current security certificate will become invalid and require an update unless you are using a self-signed certificate.
- 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 30
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 32
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 33
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 adds virtual machines to your system, your current security certificate will become invalid and require an update unless you are using a self-signed certificate.
- 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 30
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 32

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 92.

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.

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.

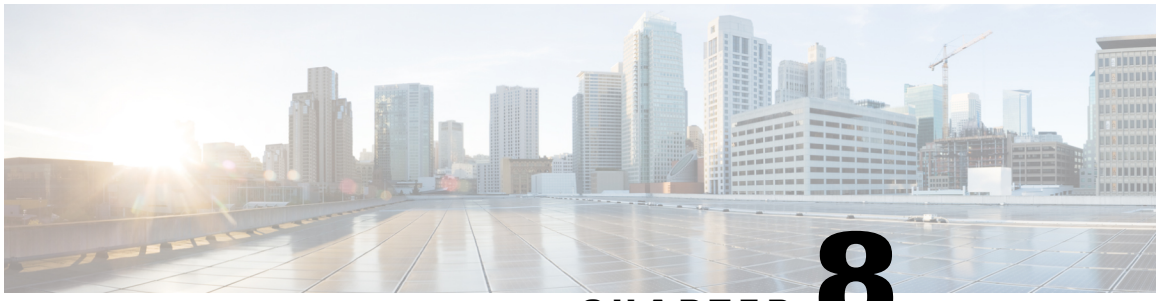
Step 7 Select **Turn Off Maintenance Mode** and **Continue** to confirm.
Your system restarts after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Testing the System

Some of the recommended tests to run on the system are listed in this section. 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.

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

- 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, page 79
- Preparing For a System-Altering Procedure, page 80
- Expanding the System by using Automatic Deployment , page 81
- Expanding the System by using Manual Deployment, page 85
- Testing the System, page 89

Preparing for System Expansion

This section describes the prerequisites a system expansion.

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

Determining the Size of the New System

Consider the following:

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

Obtaining the Information Required For Your System Expansion

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

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

Field Name	Current Value For Your System
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, by creating a backup of your system.

Although you may choose to do so, backups are not required for an expansion or upgrade of your system. During an expansion or an upgrade, you deploy a new system and transfer data from your existing system to the new system. If there is a problem with the expansion or upgrade, you can power off the new system and continue to use your existing system.

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

Other system administrators should not access the system during this procedure. If they do so, their changes are not saved, and the result 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 Use VMware Data Recovery (called VMware vSphere Data Protection starting with vSphere Release 5.1) to create a backup of each of your virtual machines.
A backup will help you revert your virtual machine to its state before the system-altering procedure. For further information, see Creating a Backup Using VMware vCenter, on page 4. For complete details on this backup, see the *VMware Data Recovery Administration Guide* or the *vSphere Data Protection Administration Guide*.

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

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

Step 5 Continue with the system-altering procedure.

Expanding the System by using Automatic Deployment

Before You Begin

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

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

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.
6. Re-host the licenses.

Considerations Before Expanding the System

Note the following:

- Be sure to remove all VMware snapshots of your existing system before starting the expansion procedure.

- You can 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; both systems cannot be powered on and running at the same time.
- If you had HA on the your existing system, then after the deployment of the expanded system you must add HA to the expanded system. You cannot reuse the HA system, as it is not retained after an expansion.
- You can keep the 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, the Internet Reverse Proxy virtual machines for the existing system and the expanded system must be on the same subnet.
- When you add a new virtual machine to the system, your current security certificate and public and private keys become invalid and require an update, unless you are using a self-signed certificate.

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

Summary of Tasks to Expand the System by using Automatic Deployment

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

Task	Description	For Details, See
1	Prepare the existing system for expansion.	You completed this task earlier in this chapter. It is included in this table for completeness.
2	Prepare for a system-altering procedure.	You completed this task earlier in this chapter. It is included in this table for completeness.
3	Initiate the expansion procedure from the Administration site of the existing system.	Expanding System Size, on page 146
4	Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the existing system.	

Task	Description	For Details, See
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.	
9	Enter the deployment URL into a web browser and continue the deployment of your expanded system.	
10	Select your preferred language for the deployment of the expanded system.	Selecting Your Language for Setup, on page 28
11	Confirm the system size. (This system size must be larger than or equal to the existing system.)	Confirming the Size of Your System, on page 29
13	Select **Install a primary system**.	Choosing What System to Install, on page 29
14	Select an automatic deployment.	Choosing the Type of System Deployment, on page 30
15	Enter your vCenter credentials so that we may deploy the virtual machines for you.	Providing VMware vCenter Credentials, on page 30
16	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
17	Enter the fully qualified domain name of the media virtual machine. (If you have already updated your DNS server with entries for the expanded system, then we will look up the IP address for you.)	Entering Networking Information for the Media Virtual Machine, on page 31
18	If you want public access for your expanded system, then ensure there is a check in the **Create an Internet Reverse Proxy virtual machine** check box. Otherwise, uncheck this check box. **Note** If you have not enabled public access, skip to Task 19.	Adding Public Access, on page 32
19	If you have added public access, then select the ESXi host, data store, and virtual machine port group for the Internet Reverse Proxy virtual machine.	Choosing vCenter Settings for Your Internet Reverse Proxy, on page 32
20	Enter the hostname and networking information for the Internet Reverse Proxy.	Entering the Networking Information for the Internet Reverse Proxy, on page 33

Task	Description	For Details, See
21	Enter the public VIP address for the WebEx site URL. **Note** You can enter the same public VIP address that you use for your 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
22	Enter the private VIP address for the WebEx Administration URL. **Note** You can enter the same private VIP address that you use for your 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 34
23	Enter the WebEx site URL. Participants access this URL to host and attend meetings. (This URL resolves to the private VIP address or the public VIP address, depending on whether or not you are using a split-horizon DNS.) **Note** You 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 36
24	Enter the WebEx Administration URL for administrators to access Cisco WebEx Administration and internal participants to host or attend meetings (only with a split-horizon DNS). (This URL resolves to the Private VIP address.) **Note** You 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 36
25	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
26	Once your virtual machines have deployed successfully, then select **Next** to continue to the system check.	Deploying Your Virtual Machines, on page 36
27	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 might take up to an hour.) When complete, the system restarts.	Checking Your System, on page 37
28	Sign in to Cisco WebEx Administration.	

Task	Description	For Details, See
29	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
30	Within the next 180 days the license-free grace period shall expire. Re-host and update the license version as appropriate for the expanded system.	About Licenses Re-hosting Licenses after a Software Upgrade

Expanding the System by 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 can be unpredictable. They must wait until this procedure is completed, then sign in to Cisco WebEx Administration to do their task.

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

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. Using the OVA, deploy any additional virtual machines for the new system size.
5. Test the expanded system.
6. Re-host the licenses.

Considerations Before Expanding the System

Note the following:

- Be sure to remove all VMware snapshots of your existing system before starting the expansion procedure.
- 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.
- When you add a new virtual machine to the system, your current security certificate and public and private keys become invalid and require an update, unless you are using a self-signed certificate.

  Certificates include hostnames and URLs. The certificate and keys become invalid because they do not include the new virtual machine. For complete information on certificates and keys, see Managing Certificates, on page 208.
- 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.
- Be sure your expanded system is up and running while removing or deleting your existing system. This prevents accidental removal of Hard disk 4 's base VMDK file, which may be accessed by the expanded system.

Summary of Tasks to Expand the System Using a Manual Deployment

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

Task	Description	For Details, See
1	Prepare the existing system for expansion.	You completed this task earlier in this chapter. It is included in this table for completeness.
2	Prepare for a system-altering procedure.	You completed this task earlier in this chapter. It is included in this table for completeness.

Task	Description	For Details, See
3	Initiate the expansion procedure from the Administration site of the existing system.	Expanding System Size, on page 146
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. **Note** At this time, you may also create the other virtual machines for your system.	Deploying the OVA File From the VMware vSphere Client, on page 16
6	Attach **Hard disk 4** from the 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. **Note** At this time, you may also power on the other virtual machines in your system. Be sure all the virtual machines power on successfully.	
9	Enter the deployment URL into a web browser and continue the deployment of your expanded system.	
10	Select your preferred language for the deployment of the expanded system.	Selecting Your Language for Setup, on page 28
11	Confirm the system size. (This system size must be larger than or equal to the existing system.)	Confirming the Size of Your System, on page 29
12	Select **Install a primary system**.	Choosing What System to Install, on page 29
13	Select a manual deployment.	Choosing the Type of System Deployment, on page 30
14	If you want public access for your expanded system, then ensure there is a check in the **Create an Internet Reverse Proxy virtual machine** check box. Otherwise, uncheck this check box.	Adding Public Access, on page 32
15	Enter the public VIP address for the WebEx site URL. **Note** You may enter the same public VIP address that you use for your 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
16	Enter the private VIP address for the WebEx Administration URL. **Note** You may enter the same private VIP address that you use for your 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 34
17	Enter the WebEx site URL. Participants access this URL to host and attend meetings. (This URL resolves to the private VIP address or the public VIP address, depending on whether or not you are using a split-horizon DNS.) **Note** You may enter the same WebEx site URL that you use for your 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 36
18	Enter the WebEx Administration URL for administrators to access Cisco WebEx Administration and internal participants to host or attend meetings (only with a split-horizon DNS). (This URL resolves to the Private VIP address.) **Note** You may enter the same WebEx Administration URL that you use for your 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 36
19	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
20	Once your virtual machines have deployed successfully, then select **Next** to continue to the system check.	Deploying Your Virtual Machines, on page 60
21	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
22	Sign in to Cisco WebEx Administration.	

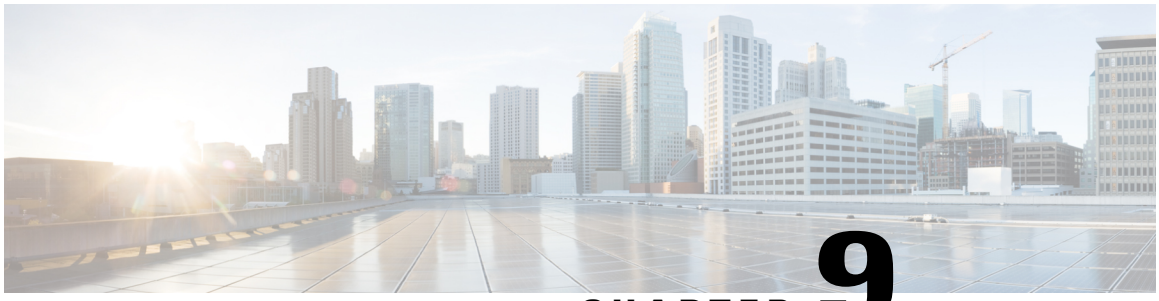
Task	Description	For Details, See
23	Test the expanded system. If the expansion is unsuccessful, then power off the expanded system and power on the existing system. Contact Cisco TAC for further assistance.	Testing the System, on page 65
24	Within the next 180 days the license-free grace period shall expire. Re-host and update the license version as appropriate for the expanded system.	About Licenses Re-hosting Licenses after a Software Upgrade

Testing the System

Some of the recommended tests to run on the system are listed in this section. 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.

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

- 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, page 91
- Connecting the Update ISO Image From the CD/DVD Drive, page 92
- Continuing the Update Procedure, page 93
- Completing the Update Procedure, page 94

Updating Your System

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.

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

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

Before You Begin

Get the latest update file from the Cisco Software Center:

Cisco Software Center (external)

The update package for your system includes a zipped ISO image. You cannot *skip* a FCS version of the software and go directly to a maintenance release (MR) version. For example, you can go from 1.0 to 1.5.1.6 (the 1.5 FCS version), but you cannot go from version 1.0 to 1.5MR.

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 (called VMware vSphere Data Protection starting with vSphere Release 5.1) to create a backup of each of your virtual machines.
A backup will help you revert your virtual machine to its state before the 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* or the *vSphere Data Protection Administration Guide*.

Note You may also take a snapshot, but you must delete these in approximately 24 hours, or you might 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.

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 91
- Connecting the Update ISO Image From the CD/DVD Drive, on page 92

Procedure

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

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

Step 3 Select **Continue**.

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

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

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

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

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

What to Do Next

Continue with Completing the Update Procedure, on page 94.

Completing the Update Procedure

Before You Begin

This is a continuation from Continuing the Update Procedure, on page 93.

Procedure

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

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

Step 3 Check the release notes for this update, and determine whether any post-update tasks are required. If additional tasks are required, complete them before you take the system out of maintenance mode.

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

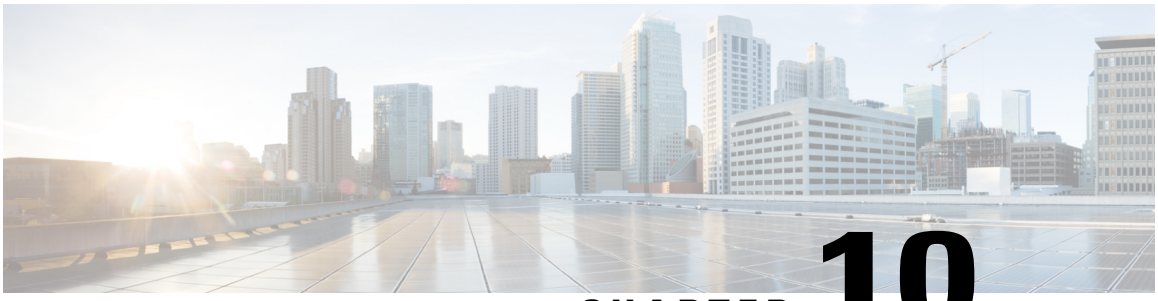
Step 5 Test and check the system. You can accomplish these tests and validate your system by using two diagnostic tools provided on the support pages for this product: the Meetings Test and the System Resources test.

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

What to Do Next

- If you find issues, then use VMware Data Recovery (vSphere Data Protection) or your system snapshots to revert to your previous version. Check the ISO network connection and ensure there are no issues.

- If the update is successful, use the updated system for awhile. Once you are satisfied, be sure to delete the virtual machine backups or snapshots created before the update.



CHAPTER 10

Upgrading the System

- Preparing For an Upgrade, page 97
- Upgrading the System Automatically, page 98
- Upgrading the System Manually, page 99
- Testing the System, page 101
- License Re-host and Upgrade, page 101

Preparing For an Upgrade

Your system can be upgraded by redeploying it with an upgraded OVA (Virtual Server Template) file. An *upgrade* is defined as a replacement of the system to deploy major modifications that we made to the system. For example replacing a system currently running version 1.0 to run version 2.0 that includes support for a new operating system. Do not use this procedure if you are performing an *update*, defined as an incremental modification of the system to deploy fixes and minor improvements, for example updating a system running version 1.0 to run version 1.1 (see Updating the System). In both cases, all of the data from the original system is transferred to the updated or upgraded system.

When upgrading, you cannot *skip* a FCS version of the software and go directly to a companion maintenance release (MR). You must upgrade to the most recent FCS version and then *update* the system to a MR version.

The system can be upgraded automatically or manually. **We recommend that you upgrade the system by using the automatic process.**

Note We refer to the system in place before initiating the upgrade as the *original* system. The system in place following upgrade is referred to as the *upgraded* system.

Before You Begin an Automatic or Manual Upgrade

Before upgrading a system automatically or manually, the following issues should be addressed:

- Obtain the OVA file required for the upgrade.
- Create a backup for each virtual machine in your original (existing) system. (See Creating a Backup Using VMware vCenter.)

- Plan a maintenance outage. During the upgrade process the original system is placed into maintenance mode and requires exclusive access to the system; users cannot access the system for meetings during this time. Schedule this portion of the upgrade for a time that is the least disruptive to your users.
- The original system hostnames and IP addresses are reused in the upgraded system. Also the internal virtual machines for both systems are on the same subnet. If you have added public access, the Internet Reverse Proxy virtual machines for the original system and the upgraded system should be on the same subnet.

Upgrading the System Automatically

Before You Begin an Automatic Upgrade

Before upgrading a system by using the automatic upgrade process, the following issues should be addressed:

- Notify other system administrators that they should not access or make changes to the original system during the upgrade, as their changes might yield unpredictable results.
- Provide and configure one additional IP address that will be used temporarily for the upgraded system.
- Do not manually power on or shut down either system.
- Verify that the upgraded system can access the disks for the original system Admin virtual machine.

Using Automatic Upgrade

This table lists the high-level tasks needed to complete an automatic upgrade. It includes links to sections of the *Cisco WebEx Meetings Server Administration Guide* that provide the detailed steps necessary to complete each task. (To move easily between this table and the individual task in Adobe Acrobat, select Previous View or Next View.)

Task	Description	For Details, See
1	Go to the license manager (**System** > **View more** > **Manage Licenses**) on the original system and generate a license request. Save the license request in a convenient location as it might be necessary to use the manual re-host procedure to reclaim your licenses. This information can help Cisco to find your licenses.	Managing Licenses
2	Using the vSphere client, deploy the Admin virtual machine for the upgraded system by selecting the configuration with the **Auto-upgrade** suffix, for example **250 Users Admin Auto-upgrade**.	
3	Power on the Administration virtual machine for the upgraded system and write down the deployment URL displayed on the virtual machine console.	
4	Enter the deployment URL into a web browser URL field.	

Task	Description	For Details, See
5	Enter the Administration and vCenter URLs and credentials, so we can deploy the virtual machines for you.	Providing VMware vCenter Credentials
6	To deploy any additional virtual machines, select **Continue**. (Until you begin the setup of the upgraded system and the original system is placed in maintenance mode, users can hold meetings, but administrators should not modify the original system virtual machines.)	The progress of the upgrade is displayed on the deployment URL of the upgraded system and on the VMware console connected to the primary system Admin virtual machine. The VMware console provides the deployment URL to use in case the browser window inadvertently closes during the upgrade process.
7	Note the names of the automatically-created virtual machines listed in vCenter. The format for virtual machine names is: CWMS_hostname_MMDDHHmm where mm=minute When the upgrade is complete, the virtual machines do not display. To find the virtual machines that were created as part of the CWMS upgrade, you can search based on this format.	
8	To put the original system in maintenance mode and begin the setup of the upgraded system, select **Continue**.	
9	To launch the upgraded Cisco WebEx Administration site, select **Sign In to Administration Site**. A 180-day license-free grace period begins.	
10	Turn off maintenance mode. The system reboots.	
11	Test the upgraded system. If the upgrade is unsuccessful, power off the upgraded system and power on the original system.	Testing the System
12	Within the next 180 days the license-free grace period shall expire. Re-host and update the license version as appropriate for the upgraded system.	About Licenses Re-hosting Licenses after a Software Upgrade

Upgrading the System Manually

Before You Begin a Manual Upgrade

Before upgrading a system, the following issues should be addressed:

- Remove all VMware snapshots of the original (existing) system.
- Do not power on and run both systems at the same time, because the hostnames and IP addresses from the original virtual machines are used in the upgraded system.
- Verify that the upgraded system can access the disks for the original system Admin virtual machine. (Hard disk 4 will be copied from the original system to the upgraded system.)

Tasks to Upgrade the System Manually

Some of the tasks in this table include links to other sections of the *Cisco WebEx Meetings Server Administration Guide*. These sections provide detailed information on that task. (To move easily between this table and the individual task in Adobe Acrobat, select Previous View or Next View.)

Task	Description	For Details, See
1	Using the vSphere client, deploy the Admin virtual machine for the upgraded system, by using the same hostnames and IP addresses that were used in the original system. You should also create the other virtual machines for your system, by using the same hostnames and IP addresses that were used in the original system. If the original system has high availability (HA), create the HA virtual machines.	Deploying the OVA File From the VMware vSphere Client
2	Login to the Administration site of the original system.	
3	Go to the System tab and select **Upgrade**.	
4	Select **Major Upgrade**.	
5	Select **Continue** to archive the original system data and put the system into maintenance mode.	
6	Using the VMware vSphere client, select **Power** > **Shut Down Guest** on the virtual machines for the original system.	
7	Copy the data from your original system to the Admin virtual machine for the upgraded system.	Attaching an Existing VMDK File to a New Virtual Machine
8	Power on the upgraded Admin virtual machine and write down the deployment URL on the VM console.	
9	Power on the other upgraded virtual machines.	
10	Enter the deployment URL into a web browser.	
11	Select **Continue** to launch the system setup.	The progress of the upgrade is displayed on the deployment URL of the upgraded system and on the VMware console connected to the primary system Admin virtual machine. The VMware console provides the deployment URL to use in case the browser window inadvertently closes during the upgrade process.
12	When the system setup is complete, select **Sign in to Administration site**.	

Task	Description	For Details, See
13	Test the upgraded system. When your upgraded system is running satisfactorily, you can delete your original system to free the original system resources. Keep the upgraded system running while deleting the original system to prevent the accidental removal of the Hard disk 4 base VMDK file that might be accessed by the upgraded system. If the upgrade is not running satisfactorily, power off the upgraded system and power on the original system. Contact Cisco TAC for further assistance.	Testing the System
14	Within the next 180 days, update the license version as appropriate for the upgraded system. You can re-host the licenses from your original system to the upgraded system.	About Licenses Re-hosting Licenses after a Software Upgrade

Testing the System

Some of the recommended tests to run on the system are listed in this section. 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.

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

- 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.

License Re-host and Upgrade

Following a software upgrade, trial licenses are valid for 180 days. Before the 180-day trial licenses expire, you should test your system, then re-host and upgrade your licenses. Re-hosting allows the licenses on the original system to be upgraded for use on the upgraded system. If the licenses are not re-hosted, they cannot be upgraded.

Re-hosting Licenses after a Software Upgrade

After CWMS software has been upgraded and testing is complete or an existing system has been expanded, the next step is to re-host your licenses. Re-hosted licenses are automatically invalidated on the original system. Before you begin the re-host, preserve the original license request in case it is needed to manually re-host the licenses.

To use the self-service portal and obtain the licenses, log into the portal with the same CCO account that was used to fulfil the licenses for the original system.

To acquire a license request for the original system:

1. Go to the license manager by selecting **System** window select **(under Licenses) view more** > **Manage Licenses** on their original system.
2. Select **Generate License Request**.
3. Save the request.

If this account is not available or if you login and do not find licenses associated with this account, perform a manual re-host.

An upgraded system allows you a 180-day grace period before licenses are required, allowing you time to test the system before re-hosting the licenses on the upgraded system. Re-hosting can be done by using the Product License Registration Portal (http://tools.cisco.com/SWIFT/LicensingUI/Home), or manually, or by opening a case with Cisco.

When re-hosting licenses, the number of licenses that you can install is limited to the number of licenses on the original system.

What to do Next

After re-hosting the licenses, they should be installed on the upgraded system. (See Managing Licenses.)

Note The license installed on the upgraded system will be the same version as the license from the original system. When the licenses are installed, an error displays: **You are using an invalid license file for your current deployment. Your system will be disabled on *mm/dd/yy* if this continues.** This is expected. Complete the license upgrade before the date shown to assure the uninterrupted use of the system.

Upgrading Licenses after a Software Upgrade

After a software upgrade, licenses are re-hosted from the original system on the upgraded system. (See Re-hosting Licenses after a Software Upgrade for more information.) After the licenses have been re-hosted, they can be upgraded for use on the upgraded system.

To upgrade your licenses by using eFulfilment:

1. Obtain a Product Authorization Key (PAK) code from your vendor.
2. From the **System** window select **(under Licenses) view more**>**Manage Licenses**> **Licenses**> **Fulfil Licenses from PAK**. The **Fulfil Licenses from PAK** window is shown.
3. Enter the PAK code and select **Next**.
4. Log in by using your CCO account credentials. The **Fulfill Licenses from PAK** window is shown.
5. Click the Install column to select the number of licenses you want to install.

6 Indicate the number of licenses to be installed and select **Save**. The licenses are installed on the system as part of the eFulfillment from the PAK.

Note The number of licenses that you can install is limited to the number of licenses installed from the upgrade PAK cannot exceed the number of licenses that were re-hosted from the original system.

7 Install the licenses from the license file by using the instructions in the Re-hosting Licenses after a Software Upgrade section.

To upgrade your licenses from a license file:

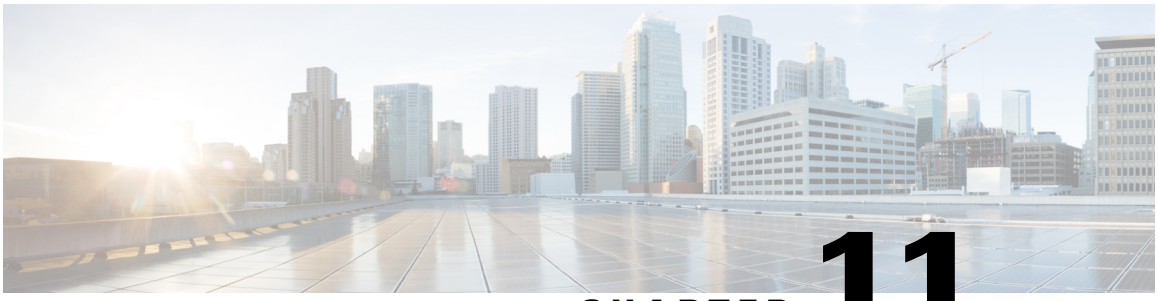
1 Obtain a license file from Cisco by using **cisco.com/go/license**.
2 From the **System** window select **(under Licenses) view more**>**Manage Licenses**> **Licenses**> **Fulfil licenses from file**. The **Install Licenses File** window is shown.
3 Browse in the license file. The file is shown on the **Licenses** window.

The licenses are updated automatically.

PART II

Cisco WebEx Meetings Server Configuration Guide

- Using Your Dashboard, page 107
- Managing Users, page 119
- Configuring Your System, page 139
- Configuring Settings, page 171
- Managing Your Reports, page 225
- Using the Support Features, page 231



CHAPTER 11

Using Your Dashboard

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

- About Your Dashboard, page 107
- Viewing and Editing Alarms, page 109
- Viewing Meeting Trends, page 111
- Viewing the Meetings List, page 111
- Scheduling a Maintenance Window, page 112
- About Maintenance Mode, page 113
- Turning Maintenance Mode On or Off, page 116
- Changing a Scheduled Maintenance Window, page 116

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 parameters and graphs key monitoring features.

The dashboard includes the following sections:

- System Monitor—Displays the system status and time stamp and includes the following subsections:
  - Meetings and Users—Displays the total number of meetings and users and a status for each on your system: green indicates operational, yellow indicates some meetings or users are experiencing problems, red indicates the system is down.
  - Alarm icon—Select the Alarm icon to view and edit the alarm threshold settings you have configured. Alarm thresholds are displayed on the **Alarms** page in numerical form. By default, alarm thresholds are displayed as a percentage. To configure alarm thresholds, select **Edit**. On the **Edit Alarms** page, select **Number #** to change the alarm information to numerical data. See Viewing and Editing Alarms for more information about configuring alarms.

    You can configure alarms for the following:
    - Meetings In Progress—Indicates when current meetings are experiencing issues.

- Usage—The total number of users currently using the system.
- CPU—The CPU usage of the virtual machine with the highest CPU usage out of all virtual machines in this system.
- Memory—The approximate amount of memory used by the one virtual machine that has the highest memory load.

Note When the gauge is in the red zone for short periods of time, it not an indication that the system is in a critical state or that it needs immediate attention. High memory use might indicate that there are other system performance issues. If memory usage exceeds 90 percent for a long period of time, we recommend that you review the vCenter memory usage and CPU statistics. If those statistics are found to be out-of-range, consider modifying your system to reduce the load.

- Network—Total system bandwidth used.
- Storage—Recording and database backup storage space used.

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

- Meeting Trend Graph and Meetings List—A graph of the number of meetings held on your system over a specified period of time. Use the **From** and **To** fields to set the time period for the meeting trend information and for the meetings displayed in the Meetings list. You can select a point on the Meeting Trend graph to list the meetings on the Meetings list that occurred during the time slot specified on the graph. To view meetings that occurred during a specific time of day, mouse over the graph and select the desired time. The Meetings list shows the total number of meetings that occurred during the selected time period, the meeting topics, hosts, numbers of participants, and the state of the meeting. You can sort each column of information in the Meetings list, and the meetings are displayed in order by state: In progress, Ended, and Not started.
- Maintenance—The scheduled maintenance window. This section lets you schedule a maintenance window to configure your system or change your settings, and start maintenance. See About Maintenance Mode for more information.
- Last System Backup—The time and date that the last backup was taken; the file name, size, and location of the backup; and the date and time of the next backup. It also notifies you if the backup failed and the date of the first backup attempt if one has not been created yet.

Note Only appears if you have configured a storage server.

- System—The maximum number of users on your system, the version number, product URL, whether public access is allowed, if it is a high availability system, and the number of user licenses. If you are using a free-trial edition of Cisco WebEx Server and there are 30 days or less remaining in the trial period, this section also indicates how many days remain before the trial period expires. Select **View More** to go to Configuring Your System.

- Users—The total number of active users when Directory Integration is configured, whether synchronization is configured, and the type of authentication. Select **View More** to go to Editing Users.
- Settings—The current system settings, including the maximum number of participants allowed in each meeting, audio type, and whether or not video or mobile features are enabled. Select **View More** to go to Configuring Settings.

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

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

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

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

Viewing Meeting Trends

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Dashboard**.

Step 3 Above the **Meeting Trend** graph set a trend period by selecting the **From** and **To** date and time.

- Meetings scheduled before midnight and extending to the following day are displayed on the graph by the meeting start date.
- If a meeting is disconnected due to a system problem and then reconnected, it is counted twice on the Meeting Trends graph.
- Meeting trend data for one-month and six-month views is based on Greenwich Mean Time (GMT) and is therefore not accurately displayed over a 24-hour period. For example, if your system hosts 200 meetings during a given day, the database records the occurrence of those meetings based on GMT and not local time. Meeting trend data for one-day and one-week views are based on the user's time zone.
- A green track indicates meetings that are in progress or that have ended. Future meetings are shown in yellow.
- The data point interval for meetings that are in progress or that have ended is 5 minutes, and the interval on the graph resembles a stair on a staircase. The data point interval for future meetings is 1 hour and the data point interval resembles a triangle.

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

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

Step 4 Optionally click a particular location on the **Meeting Trend** graph to list the meetings that occurred within 5 minutes of the selected time in the **Meetings** list below the graph. See Viewing the Meetings List, on page 111 for more information.

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

Viewing the Meetings List

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Dashboard**.

Step 3 Above the Meeting Trend graph set a trend period by selecting the **From** and **To** date and time. See Viewing Meeting Trends, on page 111 for more information.

Note
- By default, the Meetings list displays the meetings for the current 24-hour period.
- Scheduled meetings that are not started by the scheduled time are not included in the Meeting Trend graph or the Meetings list .

The Meetings list displays the total number of meetings and lists all the meetings that are scheduled, in progress, or have ended during the selected trend period. Meetings are displayed in order of status: In Progress, Ended, Not Started. Information displayed in the Meetings list includes:

- The entered trend period
- Meeting Topic
- Host
- Number of participants
- State of the meeting: In Progress, Ended, Not Started

Note Meetings that have a status of *In Progress* or *Ended* display a green, yellow, or red LED in the first column to indicate the state of the meeting as *good*, *fair*, or *poor*. Fair (yellow) indicates the audio/video delay or jitter taking place during the meeting has reached a minor threshold and should be monitored and investigated to determine the cause. Poor (red) indicates the audio/video delay or jitter taking place during the meeting has reached a major threshold and the Administrator should contact the Cisco Technical Assistance group (TAC) for assistance.

Step 4 Optionally select a column heading to sort the meetings.

Step 5 Use the pagination function to view the next or previous page.

Note
- A maximum of 50 meetings display on each page.
- Only 500 meetings are displayed for any trend period. Break the trend period into shorter periods of time if there are a marge number of meetings for a given period.
- You may see duplicate meeting entries in the Meetings list. An meeting entry is created every time a meeting is started. Therefore, if a meeting is started, stopped, and restarted, multiple meeting entries with the same name are displayed in the list.

Scheduling a Maintenance Window

Before you perform system maintenance, you should schedule a maintenance window. During this scheduled time, users cannot host or attend meetings and meetings in progress will end. An administrator must manually turn on maintenance mode after the scheduled maintenance window time begins; the system will not automatically place put the system into maintenance mode.

While some system maintenance tasks do not require you to turn on maintenance mode, be aware that the tasks that do require your system to be in maintenance mode will require extra time after you turn on maintenance mode for the system to complete a restart or reboot. The system *restart* takes only a few minutes (approximately 3-5 minutes) but the *reboot* takes approximately 30 minutes. See for About Maintenance Mode, on page 113more details.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Dashboard**.

Step 3 Select **Schedule Maintenance**.
The **Schedule Maintenance Mode** dialog displays.

Step 4 Select the date and start time for the maintenance window using the calendar tool and the time drop-down menu.

Step 5 Enter the duration of the maintenance window by specifying the number of hours and minutes.

Step 6 Select **Schedule**.
The scheduled maintenance window date, start time and duration displays in the Maintenance pane.

What to Do Next

- See Turning Maintenance Mode On or Off, on page 116 for information about turning on maintenance mode.
- See Emailing Users, on page 137 for details about notifying users about the system maintenance.

About Maintenance Mode

Many configuration changes require that you put your system into maintenance mode. Turning maintenance mode on and off is a manual process. You use the **Turn On Maintenance Mode** button located on the **Dashboard** page to put your system into maintenance mode. This button switches to **Turn Off Maintenance Mode** once maintenance mode is turned on. Although we recommend you schedule a maintenance window and put your system into maintenance mode during that scheduled period of time, you are not required to schedule a maintenance window before you turn on maintenance mode. See Scheduling a Maintenance Window, on page 112 for more details. You can turn on maintenance mode at any time.

Putting your system into maintenance mode shuts down conferencing activity, which means the system:

- Ends all meetings currently in progress.
- Disconnects all users from those meetings.
- Prevents users from signing in from web pages, the Outlook plug-in, and mobile applications.
- Blocks users from scheduling and hosting new Cisco WebEx meetings.

While your system has maintenance mode turned on, the following functions are available:

- Meet Now - Start or attend instant meetings. Administrators can use this functionality to test Cisco WebEx meetings while modifying system configuration settings.
- System configuration - an administrator can modify any system properties.
- Previously scheduled meetings - users can host and attend meetings that were schedule before a maintenance window was scheduled or maintenance mode was turned on.
- Email notifications - the system can send automatic notification emails to users and administrators.

You must manually turn on maintenance mode when you are ready to begin system maintenance. See Turning Maintenance Mode On or Off, on page 116 for more details.

The following tasks do not require your system to be in maintenance mode:

- Changing your mail server. See Configuring a Mail Server, on page 149 for more information.
- Configuring and changing the Call-In Access Numbers, Display Name, and Caller ID audio settings. See About Configuring Your Audio Settings, on page 176 for more information.
- Configuring and changing quality of service settings. See Configuring Quality of Service (QoS), on page 181 for more information.

You must turn on maintenance mode before you perform the following tasks. The system provides reminder messages if you attempt to perform these tasks without turning on maintenance mode first.

- Adding and removing high availability systems. See Configuring a High Availability System, on page 140 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 145 for more information.
- Change the system default language. See Configuring Your Company Information, on page 172 for more information.
- Changing your host or admin account URLs. See Changing Your Site Settings, on page 148 for more information.
- Changing your system language and locale. See Configuring Your Company Information, on page 172 for more information.
- Changing your virtual IP address. See Changing Your Virtual IP Address, on page 143 for more information.
- Configuring and changing many of the audio settings. See About Configuring Your Audio Settings, on page 176 for more information.
- Configuring and changing branding settings. See Configuring Your Branding Settings, on page 173 for more information.
- Configuring certificates. See Managing Certificates, on page 208 for more information.
- Configuring disaster recovery settings. See Using the Disaster Recovery Feature, on page 152 for more information.
- Configuring FIPS-compatible encryption. See Enabling FIPS Compliant Encryption, on page 222 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 150 for more information.
- Configuring virtual machine security. See Configuring Virtual Machine Security for more information.
- Expanding system size. See Expanding System Size, on page 146 for more information.
- Performing minor updates, major upgrades, and expanding your system. See Updating the System, on page 91 for more information.
- Updating shared keys. See Managing Certificates, on page 208 for more information.

- Using the System Resource test. See Using the System Resource Test, on page 234 for more information.

When you are finished modifying your system configuration and you have verified that the Cisco WebEx meetings conferencing functions are working properly (by using the Meet Now feature), you can turn off maintenance mode. Depending on the system properties you modified, the system:

- Becomes operational quickly because maintenance mode was not required for your updates.
- Displays a message to indicate the changes you made require a system *restart* that takes only a few minutes
- Displays a message to indicate the changes you made require a system *reboot* that takes approximately 30 minutes, depending on the size of your system

The tasks that require a system *reboot* include

- Adding and removing high availability systems.
- Changing your virtual IP address
- Configuring virtual machine security
- Configuring certificates

Note Modifying configure certificates properties will require either a restart or a reboot. The system will determine which action is required and display the appropriate message when you select **Turn Off Maintenance Mode**. See Managing Certificates, on page 208 for more information.

You should add extra time when scheduling your maintenance window to account for a system restart or reboot after system configuration. When the restart or reboot process is complete, you'll see the button name on the **Dashboard** change to **Turn On Maintenance Mode**.

Note If you finish system maintenance before the scheduled maintenance window end time, users will be able to host and attend previously scheduled meetings, but the system will prevent them from scheduling new meetings.

Each of your virtual machines has a console window that indicates when it is in maintenance mode. You can open the console windows in your vCenter inventory bar (for navigation). The console windows provide the URL of the system, type of system (primary, high availability, or public access), type of deployment (50-, 250-, 800-, or 2,000-user system), and current system status including whether maintenance mode is on or off and the time and date of the status change. The time displayed is configured in your Company Info settings. See Configuring Your Company Information, on page 172 for more information.

When you upgrade your system to Cisco WebEx Meetings Server Release 2.0 from Release 1.0, after the virtual machines have been deployed for your upgraded system, your system must be placed into maintenance mode while the upgrade process sets up your upgraded system. During the automatic upgrade process, maintenance mode is automatically turned on at the appropriate time and a message is displayed to let you know when this occurs. If you are performing a manual upgrade, turning on maintenance mode is a manual process. The upgrade process provides a message to indicate when you should turn on maintenance mode.

Turning Maintenance Mode On or Off

Before you modify your system configuration, you should start maintenance mode. See About Maintenance Modefor information about which system properties do not require maintenance mode to be turned on.

Note When maintenance mode is turned on, users cannot schedule, host, or attend meetings. Meetings currently in progress will end.

Before You Begin

Schedule a maintenance window and notify users about the scheduled system maintenance time. See Scheduling a Maintenance Window, on page 112 for more details.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Dashboard**.

Step 3 Select **Turn On Maintenance Mode**.
The **Turn On Maintenance Mode** dialog displays. Be sure to read about the condition of your system while maintenance mode is turned on.

Step 4 Select **Continue** when you're ready to start system maintenance.
A message displays indicating that your system is in maintenance mode. The **Turn Off Maintenance Mode** button displays.

Step 5 (Optional) Back up your virtual machines.

Step 6 Select **Turn Off Maintenance Mode** when you are finished configuring your system.
Depending on the system properties you modified, it can take a few minutes or approximately 30 minutes before users can sign in and resume conferencing activities.

Changing a Scheduled Maintenance Window

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

Note You can put your system in maintenance mode any time during the schedule maintenance window by selecting **Start Maintenance**.

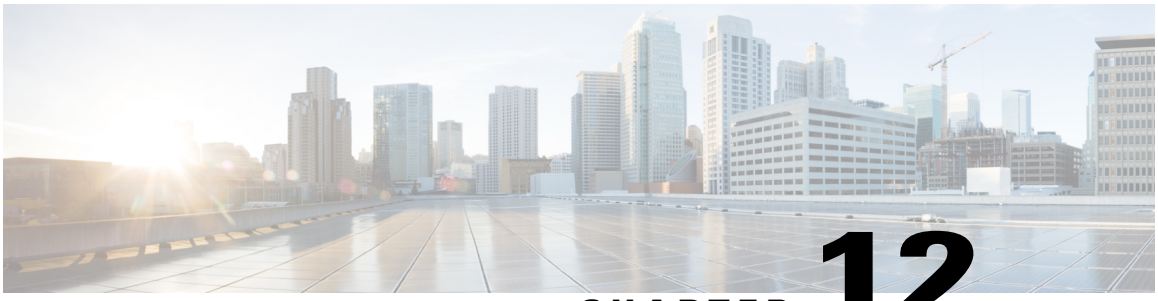
Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Dashboard**.

Step 3 Select the displayed **maintenance link**.

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



CHAPTER 12

Managing Users

This section describes how to manage users on your system.

- About Managing Users, page 119
- About Comma- and Tab-Delimited Files, page 120
- Adding Users, page 125
- Editing Users, page 126
- Activating Users, page 126
- Deactivating Users, page 127
- Deactivating Users Using Import, page 127
- Importing Users, page 128
- Exporting Users, page 128
- Importing Users to a New System by Using an Exported File, page 129
- Configuring Tracking Codes, page 129
- Configuring Directory Integration, page 131
- Synchronizing User Groups, page 135
- Using CUCM to Configure AXL Web Service and Directory Synchronization, page 135
- Using CUCM to Configure LDAP Integration and Authentication, page 136
- Emailing Users, page 137

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 127 and About Comma- and Tab-Delimited Files, on page 120 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 183 for more information.

About Comma- and Tab-Delimited Files

To use a spreadsheet application, such as Microsoft Excel, to organize your user data, save or export your spreadsheet as a comma- or tab-delimited (CSV) 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.

To successfully import a comma- or tab-delimited file all fields listed in the table are required. The field values can be empty. If a field is missing, an error message appears. For example, "Incorrect file format. Custom10 is required."

Field Name	Description	Size and Type of Value
USERID	User ID. **Note** This field is automatically generated by the system and must be left blank when importing a CSV file.	1 to 19 alphanumeric characters
ACTIVE	Whether or not this user is active.	Y or N
FIRSTNAME	User's first name.	1 to 32 character string
LASTNAME	User's last name.	1 to 32 character string
EMAIL	User's email address.	1 to 192 alphanumeric character string
LANGUAGE	Language of the user. See CSV File Field Values for more information.	1 to 64 character string
HOSTPRIVILEGE	Host privileges.	ADMN or HOST
TIMEZONE	Time zone where the user is located. See CSV File Field Values for more information.	Time zone name

Field Name	Description	Size and Type of Value
DIVISION	User's division. For tracking code group 1. This field is configurable on the Tracking Codes page. See Configuring Tracking Codes for more information.	1 to 128 character string
DEPARTMENT	User's department. For tracking code group 2. This field is configurable on the Tracking Codes page. See Configuring Tracking Codes for more information.	1 to 128 character string
PROJECT	User's project. For tracking code group 3. This field is configurable on the Tracking Codes page. See Configuring Tracking Codes for more information.	1 to 128 character string
OTHER	Other information. For tracking code group 4. This field is configurable on the Tracking Codes page. See Configuring Tracking Codes for more information.	1 to 128 character string
CUSTOM5	Custom field 5.	1 to 128 character string
CUSTOM6	Custom field 6.	1 to 128 character string
CUSTOM7	Custom field 7.	1 to 128 character string
CUSTOM8	Custom field 8.	1 to 128 character string
CUSTOM9	Custom field 9.	1 to 128 character string
CUSTOM10	Custom field 10.	1 to 128 character string

CSV File Field Values

Language Field Values

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

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

Field Value	Language
jp	Japanese
ko	Korean
fr	French
de	German
it	Italian
es-me	Castilian Spanish
es	Latin American Spanish
nl	Dutch
pt-br	Portuguese
ru	Russian

Time Zone Field Values

Following are the time zone (TIMEZONE) field values that you can set in a CSV file.

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

Field Value	GMT
Saskatchewan	-6 hr
Tegucigalpa	-6 hr
Bogota	-5 hr
Panama	-5 hr
New York	-5 hr
Indiana	-5 hr
Caracas	-4.5 hr
Santiago	-4 hr
Halifax	-4 hr
Newfoundland	-3.5 hr
Brasilia	-3 hr
Buenos Aires	-3 hr
Recife	-3 hr
Nuuk	-3 hr
Mid-Atlantic	-2 hr
Azores	-1 hr
Reykjavik	0 hr
London	0 hr
Casablanca	0 hr
West Africa	1 hr
Amsterdam	1 hr
Berlin	1 hr
Madrid	1 hr
Paris	1 hr

Field Value	GMT
Rome	1 hr
Stockholm	1 hr
Athens	2 hr
Cairo	2 hr
Pretoria	2 hr
Helsinki	2 hr
Tel Aviv	2 hr
Amman	2 hr
Istanbul	2 hr
Riyadh	3 hr
Nairobi	3 hr
Tehran	3.5 hr
Moscow	4 hr
Abu Dhabi	4 hr
Baku	4 hr
Kabul	4.5 hr
Islamabad	5 hr
Mumbai	5.5 hr
Colombo	5.5 hr
Ekaterinburg	6 hr
Almaty	6 hr
Kathmandu	6.75 hr
Bangkok	7 hr
Beijing	8 hr

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

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 126 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 126 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."

Deactivating Users Using Import

You can use the import feature to deactivate user accounts.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **Users** > **Import/Export Users** > **Export**.
Wait for a few moments for the **Download exported csv file** link to appear.

Step 3 Select **Download exported csv file** and save the CSV file to your hard drive.

Step 4 Open the CSV file. In the ACTIVE column and make the following changes:

a) Enter N for each user you want to deactivate.

b) Delete all records for users that you do not want to change.

Step 5 Select **Users** > **Import/Export Users** > **Import**.

Step 6 Select **Browse**, select your updated CSV file, select **Comma**, and then select **Import**.
The updated user records are overwritten and the selected user accounts are deactivated.

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 120 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 130 for more information.

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

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

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

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

Editing Tracking Codes

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

Before You Begin

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

Procedure

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

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

a) Select **Show active codes only** to display only active tracking codes when you open this dialog box. Deselect this option to show all tracking codes. Note that you cannot select this option the first time you configure tracking codes for each **Input mode**.

b) Select **Go to first empty tracking code** to go to the first page with empty code fields.

c) **Active** is selected by default. You can uncheck **Active** to make a tracking code inactive. Inactive tracking codes do not appear on this tracking code group's dropdown menu. Check **Active** to activate an inactive tracking code.

d) Enter the menu item name in the **Code** text box. Limit: 128 characters.

e) Select the **Default** radio button to make this menu item the default selection for the dropdown menu.
f) Select **Add 20 more lines** to add 20 more configurable tracking code lines. Navigation links (**Next**, **Previous**, and page numbers) are added if you have more than 20 lines to display. Limit: 500 lines (25 pages).
g) Select a **Sort** radio button to set the sorting method (**Do not sort**, **Sort ascending**, **Sort descending**) for the tracking codes. Note that **Sort** only works for the current page.

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

Configuring Directory Integration

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

Directory integration simplifies user profile administration in the following ways:

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

Before You Begin

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

- We recommend that you schedule synchronizations during off-peak hours or on weekends to minimize the impact on your users.
- Make sure you have a supported version of Cisco Unified Communications Manager (CUCM). Refer to the Cisco WebEx Meetings Server System Requirements for more information.
- Obtain CUCM administrative user credentials (required to add a CUCM server for directory integration).

- You must configure AXL and LDAP directory service on CUCM before you can use the directory integration feature. CUCM is required to import users into your Cisco WebEx Meetings Server system. Use CUCM to do the following:
  - Enable Cisco AXL Web Service
  - Enable Cisco directory synchronization
  - Configure LDAP integration
  - Configure LDAP authentication

  See Using CUCM to Configure AXL Web Service and Directory Synchronization, on page 135 and Using CUCM to Configure LDAP Integration and Authentication, on page 136. Refer to the CUCM documentation for additional information.
- Make sure that all users who require host privileges are available in CUCM. Any user not in CUCM will not be able to sign in and host meetings (all users can join as a guest). If necessary, create CUCM groups or filters which consist of only the users you want to import from CUCM.

Note If you do not use CUCM groups, all active CUCM users are imported into Cisco WebEx Meetings Server during your first directory synchronization. Inactive CUCM users are not imported. Only active new and modified users are imported during subsequent synchronizations. You must deactivate user accounts in Cisco WebEx Meetings Server that you do not want to give host access to. Note that a host license is only consumed in Cisco WebEx Meetings Server when a user actually hosts a meeting. Accounts that do not host meetings do not consume licenses. See "Managing Licenses" in Configuring Your System, on page 139 for more information on license consumption.

- Users with no email address are not imported.
- If users have multiple accounts that use the same first name and last name but are assigned different email addresses on CUCM, when these users are imported to Cisco WebEx Meetings Server these addresses are treated as different users. CUCM users are unique by username so an administrator can create multiple user accounts with the same email address. However, accounts on the Cisco WebEx Meeting Server are unique by email address. Therefore, if multiple CUCM user accounts have the same email address, the administrator for CUCM should manually edit these user accounts to make the email addresses unique before importing those accounts to the Cisco WebEx Meetings Server.

Procedure

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

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

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

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

Step 4 Enter your CUCM server information if you have not done so already:

- IP Address or fully qualified domain name (FQDN)

- Username
- Password

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

Note If you have already configured your CUCM settings, this step is not necessary and you can proceed to the next step. After you have configured your CUCM information, changing it is a complex procedure that can cause user synchronization problems and is not recommended.

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

Step 6 Synchronize your Cisco WebEx Meetings Server system with your LDAP directory service. You can perform your synchronization in the following ways:

- Select **Synchronize Now** to perform a synchronization immediately.
  Note You cannot cancel synchronization after it starts.
- Select the **Next synchronization** check box and enter a date, time, and repeat mechanism to schedule future synchronizations.

If you select **Synchronize Now**, your system immediately performs a synchronization. The time this process takes varies depending on the number of users being synchronized. You receive an email when the synchronization is complete. The other administrators on your system are not notified after a **Synchronize Now**. If you schedule a synchronization, it occurs at the specified date and time. All administrators receive an email after a scheduled synchronization is complete. If you want to prevent future synchronizations, you can deselect the **Next synchronization** check box.

The following attributes are mapped during the synchronization process:

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

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

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

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

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

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

Step 7 Select **Save** if you have configured or changed your synchronization schedule or your administrator notification settings.

Step 8 Select the **Users** tab and make sure that the correct users have been synchronized.

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

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

Step 9 Make sure your CUCM and Cisco WebEx Meetings Server synchronization schedules are sequential. Your CUCM synchronization must occur first and your Cisco WebEx Meetings Server synchronization should occur immediately afterward.

Step 10 (Optional) Select or deselect **Notify administrators when synchronization completes** and then select **Save**. This option is selected by default and only informs administrators after scheduled synchronizations.

Step 11 Select **Enable LDAP Authentication**.

Note If your system is configured to use SSO, you must first disable SSO. See Disabling SSO, on page 220 for more information. If your system is not configured to use SSO, it uses its default authentication until you enable LDAP authentication.

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

Step 12 Make sure that your users can sign into the system with their AD domain credentials.

Step 13 If you put your system in maintenance mode select **Turn Off Maintenance Mode**.

Step 14 (Optional) If you have performed a synchronization, you can select **Notify Now** to notify users by email that accounts have been created for them on your Cisco WebEx Meetings Server system or when their accounts have been changed. You can optionally select **Automatically send out notifications**, which automatically sends an email to your newly added users after each synchronization. After any change to the authentication settings (for example, enabling LDAP), the Users–Password Changed email is sent to affected users.
When you select **Notify Now**

- All users receive only one notification in their lifetime. Subsequent synchronizations do not cause additional emails to be sent.
- "Users that require notification" indicates all users that are active and have not been notified yet.
- Inactive users or local users are not sent any notification.
- Adding a local user on Cisco WebEx Meetings Server sends an email to this user. However, this user must be added on your CUCM Active Directory server before he can sign in to the WebEx site.
- You can only send notifications to users who were added using the synchronization feature.
- It might take a few minutes for your email notifications to be sent to your users. This delay is caused by several factors that are external to your Cisco WebEx Meetings Server system including your email server, network connectivity issues, and spam catchers on individual email accounts.

Your system sends the following emails:

- The AD Activation Email is sent to each user the first time they are imported into your system in a synchronization. Users do not receive this email on subsequent synchronizations. See About Email Templates, on page 187 for information on customizing this email template.
- The User Password–Changed email is sent to users who were created locally on your system. See About Email Templates, on page 187 for information on customizing this email template.

Synchronizing User Groups

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

Before You Begin

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

Procedure

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

Step 2 Select **Users** > **Directory Integration**.

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

Step 4 Check the user groups to be synchronized.

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

Step 5 Select **Save**.

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

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

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

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

Using CUCM to Configure AXL Web Service and Directory Synchronization

Use CUCM to configure AXL Web Service and directory synchronization.

Before You Begin

Perform this procedure before you use the Directory Integration feature. See Configuring Directory Integration, on page 131 for more information.

Procedure

	Command or Action	Purpose
Step 1	Sign in to your CUCM account.	
Step 2	Select **Cisco Unified Serviceability** from the top right dropdown menu and then select **Go**.	
Step 3	Select **Tools** > **Service Activation**.	
Step 4	Select **Cisco AXL Web Service** and **Cisco DirSync** and then select **Save**.	

What to Do Next

Use CUCM to configure LDAP integration and authentication if you have not already done so. See Using CUCM to Configure LDAP Integration and Authentication, on page 136 for more information.

Using CUCM to Configure LDAP Integration and Authentication

Use CUCM to configure LDAP integration and authentication.

Before You Begin

Perform this procedure before you use the Directory Integration feature. See Configuring Directory Integration, on page 131 for more information.

Procedure

	Command or Action	Purpose
Step 1	Sign in to your CUCM account.	
Step 2	Select **Cisco Unified CM Administration** from the top right dropdown menu and then select **Go**.	
Step 3	Select **File** > **LDAP** > **LDAP System**.	
Step 4	Select **Enable Synchronizing from LDAP Server**, select **Microsoft Active Directory** for the LDAP Server Type, select **sAM Account Name** for the LDAP Attribute for User ID and then select **Save**.	
Step 5	Select the checkbox for your LDAP server and then select **Add New**.	
Step 6	Complete the fields on the LDAP Directory page and then select **Save**.	
Step 7	On the LDAP Authentication page, select the **Use LDAP Authentication for End Users** check box, complete the fields on the page, and then select **Save**.	

What to Do Next

Use CUCM to configure Cisco AXL Web Service and Cisco Directory Sync if you have not already done so. See Using CUCM to Configure AXL Web Service and Directory Synchronization, on page 135 for more information.

Emailing Users

Use this tool to send email to your users.

Procedure

Step 1 Sign in to the Administration site.

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

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

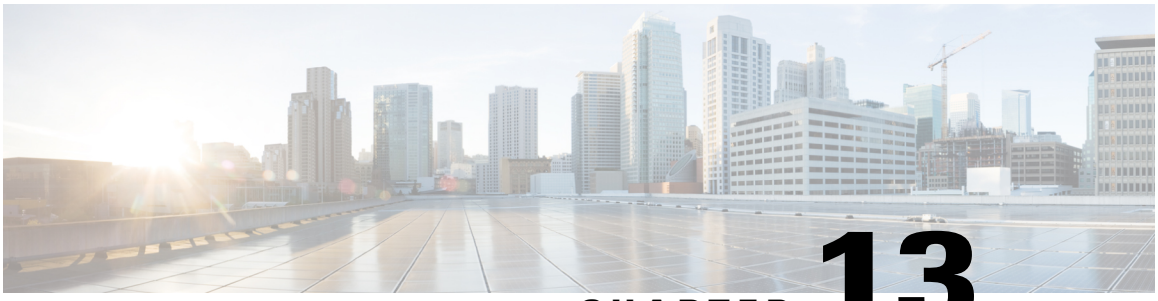
Step 4 Optionally enter email addresses in the **BCC** field.

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

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

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

Note It might take a few minutes for your emails to be received by the users. This delay might be caused by several factors that are external to your Cisco WebEx Meetings Server system, including your email server, network connection speed, and spam catchers on individual email accounts.



CHAPTER 13

Configuring Your System

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

- Configuring System Properties, page 139
- Upgrading Your System, page 147
- Configuring General Settings, page 147
- Configuring Servers, page 149
- Configuring Your SNMP Settings, page 154
- Managing Licenses, page 161

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 208.

Configuring a High Availability System

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

Note Turn on maintenance mode before you add or remove a high availability system. When you schedule a maintenance window to perform this task, be aware that the system performs a system reboot when you turn off maintenance mode. A system reboot takes approximately 30 minutes depending on the size of your system.

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.

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.

System Behavior After Component Failure

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

High-Availability Systems

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

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

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

- For a period of up to three minutes, application sharing, audio voice connection using computer and video might be interrupted. Cisco WebEx Meetings Server allows three minutes for the failure to be

detected and to reconnect all the affected meeting clients automatically. Users should not need to close their meeting clients and rejoin their meeting.

- Some failures might cause teleconferencing audio connections to disconnect. If that happens, users will need to reconnect manually. Reconnection should succeed within two minutes.
- For some failures not all clients and meetings are affected. Meeting connections are normally redistributed across multiple virtual machines and hosts.

Additional Information For a 2000-User System

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

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

For a 2000-user system with high availability:

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

Changing Your Virtual IP Address

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **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. Your system reboots after you turn off maintenance mode. You can sign back into the Administration site after restart is complete.

Note It takes approximately 30 minutes for your system to complete the system reboot. When you schedule a maintenance window for system maintenance that includes this task, be sure to account for the system reboot time period when you specify the duration of your scheduled maintenance window. See Scheduling a Maintenance Window, on page 112 for more information.

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 (vSphere 5.0) or VMware vSphere Data Protection (vSphere 5.1). 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 32 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 208 for more information.

Step 13 Make any necessary changes to your DNS servers.

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

Removing Public Access

Before You Begin

Back up your virtual machines using VMware Data Recovery (vSphere 5.0) or VMware vSphere Data Protection (vSphere 5.1). This enables you to revert your changes if necessary. See Creating a Backup 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 144 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 by using Automatic Deployment , on page 81
- Expanding the System by using Manual Deployment, on page 85

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 for more information.
- Major upgrade with system redeployment—Requires you to download the OVA upgrade file before you can continue. See Upgrading the System for more information.
- Expand system size—See Expanding System Size for more information.

The update, upgrade, or expand page is shown.

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

Step 5 Perform the 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

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

Before You Begin

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

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **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 208 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 208 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

Use your storage server to back up your system and store meeting recordings. The currently supported storage method is Network File System (NFS). Make sure that your storage server is accessible from all internal virtual machines.

Note You do not need to connect your storage server to external virtual machines such as external Internet Reverse Proxy (IRP) servers.

Your storage server backs up the following on a daily basis:

- Certain system settings
- User information
- Meeting information
- SSL certificates uploaded into the system

- The site URL

Backups are performed daily and are initially set for 4:20 a.m. local time. Cisco WebEx Meetings Server runs during the backup process without any interruption to meetings, recordings, or other functions. The system does not remove the previous backup until the following daily backup is complete to ensure that a backup is available.

Your system takes approximately five minutes to back up 500 MB. The time it takes to back up your system is dependent on storage speed, NFS speed, and other factors. A 70 GB database takes approximately one hour to back up and 10 minutes to transfer it to the NFS. Transfer time is 12 MB/sec in order to allow other network communication and to ensure the continuous operation of the product.

Before You Begin

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

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

On Windows-based storage systems, this depends on the **Network Access: Let Everyone permissions apply to anonymous users** setting. In addition, you must provide the Everyone user group read and write permissions for the NFS.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **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 **Save**.
The system confirms your NFS mount point.

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

Step 8 Select **Done**.

Step 9 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 152 for more information.

To ensure proper operation of your storage server, make sure that

- Your storage server is accessible from outside of Cisco WebEx Meetings Server.
- Your storage server is powered on.
- There is network connectivity to your storage server.
- Mount/access is possible from a non-Cisco WebEx Meetings Server machine.
- Your storage server is not full.

Note If a user inadvertently deletes a recording from the Cisco WebEx Meeting Recordings page but the recording is saved on the Network File System (NFS) storage server, contact the Cisco Technical Assistance Center (TAC) for assistance in recovering the recording.

Using the Disaster Recovery Feature

Use the disaster recovery features to recover your deployment after a system failure or other disaster. A disaster could be a network crash, server failure, data center outage, or other event that makes your system unusable. There are two types of disaster recovery:

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

After you configure a storage server, your system is backed up on a daily basis. A system backup notice appears on your dashboard that includes information about the latest backup. Only one backup system is kept in storage at a time. After you perform an upgrade or update, the backup from your previous Cisco WebEx Meetings Server version is retained. We recommend that you do not use the same storage directory for different Cisco WebEx Meetings Server installations.

Note that disaster recovery:

- Takes more than 30 minutes
- Overwrites your settings with the settings on the latest backup
- Requires you to perform additional steps to restore service to your users (detailed in *What To Do Next* in this chapter)

This procedure backs up certain system settings, user information, meeting information, SSL certificates uploaded into the system, and the site URL. The backup process does not store VMware credentials or IP address information for individual virtual machines. In the event that you perform a disaster recovery, you must manually reapply certain settings including the following:

- Connections to certain external components, for example Cisco Unified Communications Manager (CUCM)
- SSL certificates (in case the hostnames of the disaster recovery system differ from those in the original system)

- On deployments with one data center, you can optionally use the same IP address or hostname. On deployments with two data centers, you can optionally use the same IP address or hostname for your primary system.

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

Before You Begin

To perform disaster recovery procedures:

- A storage server must have been configured. If you do not have a storage server configured, the **Disaster Recovery** option is not available and backups are not created. See Configuring a Storage Server for more information.
- You must have access to a system from where you can restore your deployment. See the information on one data center and two data center disaster recovery, below.
- Your recovery system must be the same deployment size and software version as your original system.

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

Procedure

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

Step 2 Select **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 **Save**.

Example:
192.168.10.10:/CWMS/backup.

Step 5 Select **Continue** to proceed with disaster recovery.
If the recovery system deployment size and software version matches your original system, you can proceed with disaster recovery. If the system has a different deployment size or software version, you cannot proceed until you redeploy the application on your recovery system so that the deployment size and software version match the original deployment. The IP address or hostname does not have to match your original deployment.

Step 6 Select one of the following actions to continue:

- **Cancel—**Back up your pre-existing system before adding a storage server. After you back up your system you return to this page and select **Continue** to proceed.
- **Continue—**Overwrite your pre-existing system and continue with disaster recovery.

The disaster recovery process begins. If you close your browser, you cannot sign back into the system until the process is completed.

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

What to Do Next

You must perform the following procedures to restore service to your users:

- Reconfigure your teleconferencing settings. Refer to Configuring CUCM in the Planning Guide for more information.
- Reconfigure your SSO settings. See Configuring Federated Single Sign-On (SSO) Settings, on page 217 for more information.
- Reconfigure your SNMP settings. See Configuring Your SNMP Settings, on page 154 for more information.
- Reconfigure your certificates. You might have to reload your SSL certificates if they do not match the SSL certificates that are configured on the recovery system. See Restoring a SSL Certificate for more information.
- The recovered system is initially configured for License Free Mode that will expire in 180 days. Re-host your previous system licenses on the recovered system. See Re-hosting Licenses after a Software Upgrade and About Licenses for more information.
- Configure your DNS settings so that your site URL points to the current VIP. Your VIP on the restored system might be different from what you had on your original system. You must complete your DNS configuration for end users to use their original links to sign into or join meetings on the restored system. See Changing Your Virtual IP Address for more information.
- If you have configured your system for Directory Integration and enabled LDAP authentication, verify that your CUCM credentials work. After you take your system out of maintenance mode and your system reboot is complete, sign in to the Administration site, select **Users** > **Directory Integration**, and then select **Save**. If your CUCM credentials are incorrect, you receive an **Invalid Credentials** error message. If you receive this error message, enter the correct credentials and select **Save** again. See Configuring Directory Integration, on page 131 for more information.

Configuring Your SNMP Settings

You can configure the following SNMP settings:

- Community strings—SNMP community strings authenticate access to MIB objects and function as an embedded password.
- USM users—Configure user-based security (USM) to provide additional message-level security. Select an existing USM configuration to edit it or add additional USM configurations. Other than the default USM user, serveradmin, which has read and write privileges to MIB information, all new USM users that you configure only have read-only privileges to MIB information.
- Notification destinations—Use this feature to configure the trap/inform receiver.

Configuring Community Strings

You can add and edit community strings and community string access privileges.

Adding Community Strings

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **Add** in the Community Strings section.

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

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
Privacy Password	Enter the privacy password for the user. **Note** This option appears only if the security level is set to **authPriv**.

Step 6 Select **Add**.

The USM user is added to your system.

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

Editing USM Users

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select a USM user in the USM Users section.

Step 5 Change the desired fields on the **Edit USM User** page.

Option	Description
USM User Name	Change the USM user name. Maximum 256 characters.
Security Level	Select the security level. The security level you select determines which algorithms and passwords you can set for the user. Options include: • noAuthNoPriv—No authentication algorithm and password and no privacy algorithm and password for the user. • authPriv—Enables you to configure authentication algorithm and password and privacy algorithm and password for the user. • authNoPriv—Enables you to configure authentication algorithm and password for the user. **Default**: noAuthNoPriv
Authentication Algorithm	Select the authentication algorithm for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**. **Default**: SHA
Authentication Password	Change the authentication password for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**.

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

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

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

Configuring Notification Destinations

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

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

Procedure

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

Option	Description
Destination Hostname / IP Address	The hostname or IP address of the virtual machine you want to set up as a notification destination.
Port Number	The port number for your virtual machine. **Default**: 162
SNMP Version	Your SNMP version. **Default**: V3

Option	Description
Notification Type	Select **Inform** or **Traps**. **Default**: Traps
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 156 for more information.
Community String **Note** This option appears only when SNMP Version is not set to V3.	Select community strings. See Configuring Community Strings, on page 154 for more information.

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

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

Editing a Notification Destination

Configuring Notification Destinations

Procedure

Step 1 Sign in to the Administration site.
Step 2 Select **System** and select the **View More** link in the SNMP section.
Step 3 Select **Turn On Maintenance Mode** and **Continue** to confirm.
Step 4 Select a notification destination link from the **Notification Destinations** list.
Step 5 You can edit the following fields for your notification destination:

Option	Description
Destination Hostname / IP Address	The hostname or IP address of the virtual machine you want to set up as a notification destination.
Port Number	The port number for your virtual machine. **Default**: 162
SNMP Version	Your SNMP version. **Default**: V3

Option	Description
Notification Type	Select **Inform** or **Traps**. **Default**: Inform
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 156 for more information.
Community String **Note** This option appears only when SNMP Version is not set to V3.	Select community strings. See Configuring Community Strings, on page 154 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 six-month 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 Prime License Manager (PLM).
Note This version of PLM is embedded in Cisco WebEx Meetings Server. The PLM 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 **Prime License Manager** 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 Prime License Manager (PLM).

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.

What to Do Next

To add additional licenses at a later date, you must contact your Cisco sales representative and indicate how many additional licenses you want to purchase. The additional licenses are then applied to your account.

About Licenses

About User-Based Licensing

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 month, that user consumes one license. If the same user hosts additional meetings in the same month, the user still only consumes one license, unless this user hosts simultaneous meetings. The license usage calculation occurs once per month (for example, once from January 1 through 31, once from February 1 through 28, and so forth).

- If a user hosts simultaneous meetings (two or more meetings scheduled for the same date and time), then the system counts an additional license for each simultaneous meeting hosted by this user during the month.
- If a user hosts no meetings during a given month, this user consumes no licenses for that month.
- Host licenses may not be shared or used by anyone other than the user to whom the license is assigned.

Your system allows license consumption to exceed the number of licenses installed on your system. Administrators receive **licenses exceeded** emails and dashboard notices informing them that they must either reduce license consumption or purchase more licenses within six months. During this six-month period, your system continues to function normally for your users. If you have not reduced license consumption or purchased more licenses after six months, the system shuts down for all users until an administrator installs more licenses.

When the system is shut down, users cannot schedule, host, or attend meetings, or access meeting recordings. Users see a **Site under maintenance** message when they go to the WebEx site. The Administration site functions normally, so an administrator can sign in and add licenses to address the licenses exceeded condition at any time. After the additional licenses have been installed, users are able to access the WebEx site, host meetings, attend meetings, and access recordings.

From the **Reports** page, you can request a report that provides the total number of licenses consumed during the month. In addition, we recommend that 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.

Note You should purchase a license for each user that intends to host meetings. The system currently 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 One Month
User A schedules a meeting but does not host it.	January 1	9:00 a.m.	No	0
User B starts one meeting.	January 2	9:00 a.m.	No	1
User C starts two meetings on different dates and times.	January 3 January 4	9:00 a.m. 10:00 a.m.	No	1
User D starts two meetings on the same date and time.	January 6 January 6	9:00 a.m. 9:00 a.m.	Yes (2)	2

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in One Month
User E starts two meetings on the same date and time, and another two meetings on different dates and times 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 starts two meetings on the same date and time neither of which he attends, although the meetings are attended by others.	January 7 January 7	9:00 a.m. 9:00 a.m.	Yes (2)	2
User G starts a meeting and passes host rights to another participant during the meeting. The user then starts a second meeting that runs simultaneously with the first meeting.	January 8 January 8	9:00 a.m. 9:00 a.m.	Yes (2)	2
User H schedules 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	1
User J schedules 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.	Yes (2)	2

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in One Month
User K starts a meeting and passes host rights to another participant during the meeting. The user then schedules a second meeting that runs simultaneously with the first meeting, but all of the second 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.	Yes (2)	2
User L starts three Personal Conferences (not the web portion) with account 1, account 2 and account 3 at the same date but different times.	January 12	9:00 a.m. 10:00 a.m. 11:00 a.m.	No	1
User M starts three Personal Conferences (not the web portion) with account 1, account 2 and account 3 at the same date and time.	January 13	9:00 a.m.	Yes (3)	3
User N starts a meeting and a Personal Conference (not the web portion) at the same date but at different times.	January 14	9:00 a.m. 10:00 a.m.	No	1
User P starts a meeting and a Personal Conference (not the web portion) at the same date and time.	January 15	9:00 a.m. 9:00 a.m.	Yes (2)	2
User Q starts a Personal Conference (not the web portion) at 9:00 am, January 16. User Q launches the web portion at 9:10 am, January 16.	January 16	9:00 a.m. 9:10 a.m.	No	1

Six-Month Free-Trial Period

After you sign in to this product for the first time and complete the first-time-experience wizard, your six-month free-trial begins. During the free trial, administrators can configure the system and your users can schedule, host, and attend meetings. A banner appears at the top of the Administration site indicating how many months remain in your free trial. One month before your free trial ends, you receive an email that informs you that you must purchase and install licenses or your system will be disabled.

At the end of your free trial, your system is disabled. You can sign in to your system but you cannot use any other features until you add licenses. Refer to the *Cisco WebEx Meetings Server Administration Guide* for more information on managing your licenses.

Obtaining Licenses

Contact your Cisco sales representative to order licenses for your system. When you contact your sales representative, you will need to specify how many licenses you want. You will need one license for each employee in your organization who will be hosting meetings.

There are several ways you can determine how many licenses you will need. You can use your dashboard to view usage, resource history, and meeting trends to determine how many users are hosting and attending meetings on your system. After you have been using the product for a few months, you can use your monthly summary reports and customized details reports to help you determine how many licenses you need. Your monthly summary reports display statistics on service adoption and user license usage. Service adoption statistics show you the rate at which new users are adopting your system by displaying the rate of adoption for the previous three months and predicting the growth rate over the next three months. User license statistics display license usage over the previous three months and expected growth over the next three months.

After you purchase licenses from your Cisco sales representative, he will send you an email that contains your Product Authorization Key (PAK). Use the licenses tool at the Administration site to enter your PAK and register your licenses. Refer to the *Cisco WebEx Meetings Server Administration Guide* for more information on managing your licenses.

Exceeding Your Licenses

Once you have purchased and configured licenses on your system, you must make sure you have enough licenses to accommodate all active hosts on your system. Your system checks every month to determine if there are enough licenses for each active host. The license count is reset each calendar month. If the number of active hosts on your system exceeds the number of licenses, an email is sent to the administrator notifying him that he has exceeded his licenses. You are given a six-month grace period to reduce your license usage or increase the number of licenses on your system so that it meets or exceeds the number of active hosts. If you do not reduce your license usage or purchase enough licenses to meet usage before the end of the six-month period, your system will be disabled. The email message informs the administrator of the date when this will occur.

The system checks and adjusts the license numbers displayed on the administration site. The audit manager runs once per day (at 2:00 a.m.) to adjust the number of licenses used as necessary. At the end of each month the system checks license usage. If the number of hosts has dropped below the number of licenses, the licenses exceeded condition ends. If the number of active hosts still exceeds the number of licenses, a new email is sent to your administrator each month that notifies him that the licenses exceeded condition still exists and the date when the system will be disabled.

If you still have a licenses exceeded condition for straight six months, your system is disabled and the administrator receives an email notifying him what has occurred. After your system is disabled your users

will be unable to schedule, host, or attend meetings, or access recordings on your system. The Administration site will function normally so an administrator can sign in and add licenses. Once an administrator has added licenses to the system, users will regain the ability to schedule, host, and attend meetings, and access recordings.

Temporary Licenses

If you have temporary licenses configured on your system, your temporary license status appears on a banner on each page of the Administration site. The banner informs you of how many temporary licenses you have configured and when those temporary licenses expire. When temporary licenses expire your system returns to its previous license status.

Out-of-Date Licenses

If you upgrade your system, you must also update your licenses. Once you have upgraded your system, an email is sent to your administrator notifying him that he has been given a six-month grace period to update the licenses. If you do not update your licenses before the end of the six-month period, your system will be disabled. The email message informs the administrator of the date when this will occur.

The system checks and adjusts the license numbers displayed on the administration site. The audit manager runs once per day (at 2:00 a.m.) to adjust the out-of-date licenses number as necessary. At the end of each month, the system checks to see if the licenses have been updated from the previous period. If the licenses have been updated, the out-of-date license condition ends. If the licenses have not been updated yet, a new email is sent to your administrator each month that notifies him that the out-of-date license condition still exists and the date when the system will be disabled.

If you still have an out-of-date license condition after six months, your system is disabled and the administrator receives an email notifying him what has occurred. After your system is disabled your users will be unable to schedule, host, or attend meetings, or access recordings on your system. The Administration site will function normally so an administrator can sign in and update licenses. Once an administrator has updated the licenses, users will regain the ability to schedule, host, and attend meetings, and access recordings.

Prime License Manager (PLM) Connection Lost

When you purchase licenses, you use an embedded PLM tool to enter your PAK and register your licenses. PLM performs synchronization every 12 hours to update the license status and last compliance time. If two days pass with no connection to PLM, an email is sent to your administrator to inform him that PLM is unable to synchronize with your system. You are given a six-month grace period to reconnect to PLM. If your system does not reconnect with PLM before the end of the six-month period, your system is disabled. The email message informs the administrator of the date when this will occur.

A new email is sent to your administrator at the end of each month that the system is unable to connect with PLM informing the administrator of the date when the system will be disabled. If your system reconnects with PLM before the six-month grace period passes, this condition ends.

If your system is still unable to connect to PLM after six months, your system is disabled and the administrator receives an email notification of what has occurred. When your system is disabled, users are not able to schedule, host, or attend meetings, or access recordings on the system. The Administration site functions normally, so an administrator can sign in to the system but the system must reconnect with PLM to end this condition and restore the ability for users to schedule, host, and attend meetings, and access recordings.

Actions that Require New Licenses

The following system-altering actions require that you install new licenses:

- Expansion—See Expanding Your System to a Larger System Size, on page 79 for more information.

- Upgrade—See Upgrading the System, on page 97 for more information.
- Disaster Recovery—See Using the Disaster Recovery Feature, on page 152 for more information.

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 the licenses have been added.

Re-hosting Licenses after a Software Upgrade

After CWMS software has been upgraded and testing is complete or an existing system has been expanded, the next step is to re-host your licenses. Re-hosted licenses are automatically invalidated on the original system. Before you begin the re-host, preserve the original license request in case it is needed to manually re-host the licenses.

To use the self-service portal and obtain the licenses, log into the portal with the same CCO account that was used to fulfil the licenses for the original system.

To acquire a license request for the original system:

1. Go to the license manager by selecting **System** window select **(under Licenses) view more** > **Manage Licenses** on their original system.
2. Select **Generate License Request**.
3. Save the request.

If this account is not available or if you login and do not find licenses associated with this account, perform a manual re-host.

An upgraded system allows you a 180-day grace period before licenses are required, allowing you time to test the system before re-hosting the licenses on the upgraded system. Re-hosting can be done by using the Product License Registration Portal (http://tools.cisco.com/SWIFT/LicensingUI/Home), or manually, or by opening a case with Cisco.

When re-hosting licenses, the number of licenses that you can install is limited to the number of licenses on the original system.

What to do Next

After re-hosting the licenses, they should be installed on the upgraded system. (See Managing Licenses.)

Note The license installed on the upgraded system will be the same version as the license from the original system. When the licenses are installed, an error displays: **You are using an invalid license file for your current deployment. Your system will be disabled on *mm/dd/yy* if this continues.** This is expected. Complete the license upgrade before the date shown to assure the uninterrupted use of the system.

CHAPTER 14

Configuring Settings

This module describes how to configure your settings.

- Configuring Your Company Information, page 172
- Configuring Your Branding Settings, page 173
- Configuring Your Meeting Settings, page 174
- About Configuring Your Audio Settings, page 176
- Configuring Your Video Settings, page 181
- Configuring Your Mobile Settings, page 181
- Configuring Quality of Service (QoS), page 181
- Configuring Passwords, page 183
- Configuring Your Email Settings, page 186
- Configuring Your Download Settings, page 207
- Managing Certificates, page 208
- Generating SSL Certificates, page 209
- Importing SSO IdP Certificates, page 215
- Importing Secure Teleconferencing Certificates, page 215
- Configuring User Session Security, page 216
- Configuring Federated Single Sign-On (SSO) Settings, page 217
- Configuring Your Cloud Features, page 221
- Configuring Virtual Machine Security, page 221

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 participants to join Meetings before host** and **Allow participants to join teleconference before host** are selected. Optionally select **Anyone can present in the meeting**.

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

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

System Size	Maximum Meeting Size
50	50

System Size	Maximum Meeting Size
250	100 (no HA), 250 (with HA)
800	100 (no HA), 250 (with HA)
2,000	100 (no HA), 250 (with HA)

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 150 for more information.

Step 6 Select **Save**.

About Meeting Security

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

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

Table 1: Password is Excluded When Scheduling Your Meeting

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

Table 2: Password is Included When Scheduling Your Meeting

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

User Type	Password Displayed in Email Invitation and Reminder	Meeting Detail Page
Alternate host	Yes	Yes
Invited attendee	Yes	Yes
Forwarded attendee	Yes	Yes

- Join before host is on/off.
  - On: Attendee/guest/invited attendee can join the meeting before the host, 15 minutes before the scheduled started time.
  - Off: Attendee/guest/invited attendee cannot join the meeting before host. The host or alternate host can start the meeting, then the attendees can join.
- Join teleconference before host is on/off.
  - On: If the host does not start the teleconference in the meeting client, then attendees can join the teleconference before the host.
  - Off: If the host does not start the teleconference in the meeting client, then attendees cannot join the teleconference before the host.
- First attendee can present is on/off.
  - On: When Join before host is configured, the first attendee is the presenter.
  - Off: The host always has the ball.

About Configuring Your Audio Settings

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

Configuring Your Audio Settings for the First Time

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

Before You Begin

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

- Prepare a list of call-in access numbers that your participants use to call into meetings.
- Your CUCM IP address.

- (Optional) Obtain a valid secure conferencing certificate if you plan to use TLS/SRTP teleconferencing encryption. See the Importing Secure Teleconferencing Certificates, on page 215 page for more information.

Note This feature is not available in Russia or Turkey.

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **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 Communications Manager)** dialog box appears.

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

a) Enter an IP address for CUCM 1 IP Address and optionally for CUCM 2 IP Address.
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 215 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 select this option to bypass the requirement to press **1** to connect to a meeting.

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

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

- Beep (default)
- No tone
- Announce name

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

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

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

Step 19 Select **Save**.

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

Configuring Your Audio Settings

Before You Begin

If you have not already configured your audio settings, see the Configuring Your Audio Settings for the First Time, on page 176 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
WebEx Audio	• User Call In and Call Me service–Enables users to attend a teleconference by calling specified phone numbers or by receiving a Call Me call from the system. • Call In–Enables users to attend a teleconference by calling specified phone numbers. • OFF–Disables all calling features.
Voice connection using computer	• ON • OFF

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

Option	Description
CUCM 1 IP Address	Enter the hostname or an IP address for your CUCM 1 system.
CUCM 2 IP Address	(Optional) Enter the hostname or an IP address for your CUCM 2 (load balancing service) system. **Note** CUCM 2 is not required but it is recommended for teleconferencing high availability.
Port Number	Enter a valid port number. Make sure the port number matches the setting in CUCM. **Default:** 5062

Option	Description
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 215 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 select this option to bypass the requirement to press **1** to connect to a meeting.

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

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

- Beep (default)
- No tone
- Announce name

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

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

Step 12 Select **Save**.

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

Configuring Your Video Settings

Procedure

Step 1 Sign in to the Administration site.

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

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

Configuring Your Mobile Settings

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

Before You Begin

To configure mobile settings you must add public access on your system during deployment. See Adding Public Access to Your System, on page 144 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**

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**.

About QoS Marking

See the tables below for QoS marking information for deployments with and without Internet reverse proxy servers configured.

QoS Marking on Cisco WebEx Meetings Server Systems With Internet Reverse Proxy Configured

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

QoS Marking on Cisco WebEx Meetings Server Systems Without Internet Reverse Proxy Configured

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

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

Configuring Passwords

You can configure password settings for the following:

- General Passwords—Controls password expiration periods and enables you to force users to change their passwords either immediately or at a specified interval.
- User Passwords—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 127.

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

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

Step 6 Select **Save**.

Configuring Your User Password Settings

Configure your user password requirements and limitations.

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Option	Description
List of unacceptable passwords	Administrator-specified list of unusable passwords. **Default**: Not selected
Company name, site name, user email address, and host name are always unacceptable	Do not use these specific names. **Default**: Selected
Must not include previous *n* passwords	Do not use previously used passwords. Select a number from the dropdown menu to specify the number of previous passwords you cannot use. **Default**: Selected **Default number**: 5

Step 4 Select **Save**.

Configuring Your Meeting Passwords

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

Password Configured	Password Excluded from Email Invitation	Meeting Creator Signed In	Host Signed In	Invitee Signed In	Guest Signed In	Guest Not Signed In
No	n/a	Password not required.	Password not required.	Password not required.	Password not required.	Password not required.
Yes	Yes	Password not required.	Password not required.	Password not required.	Password required.	Password required.
Yes	No	Password not required.	Password not required.	Password not required.	Password required. Password can be prefilled.	Password required. Password can be prefilled.

Procedure

Step 1 Sign in to the Administration site.

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

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

Note All options are not selected by default.

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

Step 4 Select **Save**.

Configuring Your Email Settings

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 4 Select **Templates**. See About Email Templates, on page 187 for descriptions of each template type.
The **Templates** page appears. Select the **Common** or **Meetings** tab. **Common** is the default.

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

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

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

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

About Email Templates

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

There are two types of email templates:

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

Table 3: Common Email Templates

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

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

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

Title	Description	Variables
PT—Host Notification	Sent to a meeting host after a meeting is scheduled using Productivity Tools.	• %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%
PT—Invitee Notification	Sent to meeting invitees after a meeting is scheduled using Productivity Tools.	• %Topic% • %HostName% • %Meeting Link% • %Meeting Number% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%
Recording Available for Host	Sends the host a link to a meeting recording.	• %SiteURL% • %OrgLogo% • %DisplayName% • %Topic Name% • %Duration% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

Title	Description	Variables
SSO Activation Email	Sent after Single Sign-On (SSO) is enabled.	• %SiteURL% • %DisplayName% • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Send Email To All Users	Sends an email to all users on the system.	• %SiteURL% • %Subject% • %OrgLogo% • %AttendeeName% • %Body% • %SiteURL% • %Support% • %CustomFooterText% • %Year%
Setup Cisco WebEx—Android	Informs users about the Cisco WebEx app for Android and provides a download link for the app.	• %SiteURL% • %Subject% • %OrgLogo% • %DisplayName% • %SiteURL% • %Support% • %CustomFooterText% • %Year%

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

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

Table 4: Meetings Email Templates

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

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

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

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

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

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

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

Title	Description	Variables
PCN Meeting Auto Reminder—Host	Sends an automatic meeting reminder to the meeting's host (PCN accounts only).	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • % MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumber% • %SiteURL% • %Support%
PCN Meeting Invitation—Invitee	Sends a meeting invitation to invitees (PCN accounts only).	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

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

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

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

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

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

Configuring Your Download Settings

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select your download method:

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

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

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

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

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

About Downloads

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

On PCs without administrator privileges:

- We recommend that you push the WebEx Meetings application and Productivity Tools to end-user desktops offline before you inform end-users that user accounts have been created for them. This ensures that your users can start and join meetings from their web browsers and Windows desktops the first time they sign in.
- You can acquire the .MSI installers for each from the Administration site at the **Settings** > **Downloads** page. See Configuring Your Download Settings, on page 207 for more information.
- If you decide against pushing the applications to your users, they can still access these applications from the end-user download pages. However, if their PCs prohibit installation of downloaded applications, they will not be able to complete the installation process.
- When users join meetings by using their web browser (the WebEx Meetings application can still be downloaded on demand) they can join meetings successfully. In addition, the WebEx Meetings application attempts to perform an installation to speed up the process of starting or joining future meetings. This fails because their PCs do not have administrator privileges.

On PCs with administrator privileges:

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

Managing Certificates

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

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

The following certificate types are supported:

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

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

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

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

SSL certificates can become invalid for the following reasons:

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

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

Generating SSL Certificates

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

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

Generating a Certificate Signing Request (CSR)

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

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

Step 7 Back up your system using VMware Data Recovery (vSphere 5.0) or VMware vSphere Data Protection (vSphere 5.1). See Creating a Backup 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/private key**.
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 **Done**.

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

Exporting a SSL Certificate

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Save the certificate file.

What to Do Next

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

Downloading Your CSR and Private Key

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Generating a Self-Signed Certificate

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

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

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

Your certificate file is generated and displayed.

Step 6 Select **Done**.

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

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

Restoring a SSL Certificate

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

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **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 reapply a previous private/public key pair for disaster recovery, combine the public key file (csr_private_key.pem) and the certificate received from your certificate authority (CA) into one file. The private key must be the first block in the file followed by the public key. It can be encrypted or unencrypted. It should be in PKCS#8 format and PEM encoded. If it is encrypted, you must enter the password to decrypt it in the passphrase field.
- The next element must be the certificate of the intermediate certificate authority that issued your certificate in PEM encoded X.509 format.
- You can include as many intermediate certificates as you use in your infrastructure. The certificate of the root certificate authority should not be included. If you are using a private certificate authority, you must make sure that the root certificate is distributed to all clients.

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

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

Step 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.

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 176 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 **Done**.

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

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

Configuring User Session Security

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 4 Select **Save**.

Configuring Federated Single Sign-On (SSO) Settings

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

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

Before You Begin

- Before you enable the federated single sign-on feature, you must generate a set of public and private keys and an X.509 certificate that contains the public key. Once you have a public key or certificate, you must upload it in the Managing Certificates, on page 208 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 183 and Editing Users, on page 126 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 215 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 or to view training videos hosted online by Cisco WebEx.

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select **Save**.

Configuring Virtual Machine Security

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

Updating Your Encryption Keys

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

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **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) 140 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. A cryptographic module is a "set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary." The cryptographic module is what is being validated.

FIPS 140 Requirements

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

- Implementation of FIPS-approved algorithms
- Specific management of the key life cycle
- Approved generation of random numbers
- Self-tests of cryptographic algorithms, image integrity, and random number generators (RNGs)

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

With FIPS Enabled

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

Cisco recommends that you take the following actions:

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

Enabling FIPS Compliant Encryption

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

Procedure

Step 1 Sign in to the Administration site.

Step 2 Select **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

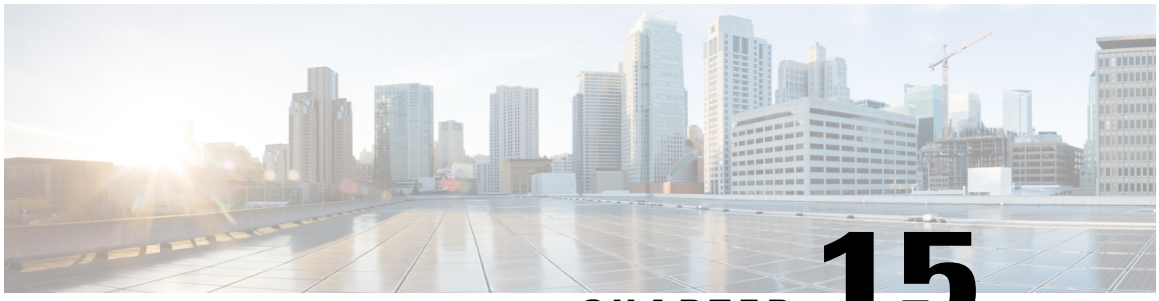
Step 1 Sign in to the Administration site.

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

Managing Your Reports

You can view monthly reports and customize reports for specific date ranges. Your reports use the language, locale, and time zone settings configured on the **Company Information** page. See Configuring Your Company Information, on page 172 for more information.

Note When your system is newly deployed or recently upgraded, there is no data available for any of the reports except the Customized Details Report until the end of the first month. In that case, the **Download** links and all the other reports described in this section are not available until after the end of the first month.

- Downloading Monthly Reports, page 225
- About Monthly Reports, page 225
- Generating Customized Details Reports, page 227
- About Customized Details Reports, page 227

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 161 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 150 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 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:

- Fraud Attempts Report—This report displays any failed telephony access attempts where the caller enters the wrong host or participant access codes or host PIN three times while attempting to start or join a Personal Conference meeting. This report includes the following fields:
  - Access Number Called—The Cisco WebEx call-in number dialed to start or join a Personal Conference meeting.
  - Calling Number—The phone number of the phone used to place the call.
  - Start Time of Call—The date and time of the call.
  - 1st Access Code Attempted—The first invalid access code entered by the caller.
  - Email of 1st Access Code Owner (if available)—The email address of the user associated with the first invalid access code, if the access code is associated with a valid Cisco WebEx Meetings Server account.
  - 2nd Access Code Attempted—The second invalid access code entered by the caller.
  - Email of 2nd Access Code Owner (if available)—The email address of the user associated with the second invalid access code, if the access code is associated with a valid Cisco WebEx Meetings Server account.
  - 3rd Access Code Attempted—The third invalid access code entered by the caller.
  - Email of 3rd Access Code Owner (if available)—The email address of the user associated with the third invalid access code, if the access code is associated with a valid Cisco WebEx Meetings Server account.
- Meeting Report—This report contains information on all meetings that took place during the specified period and includes the following fields:
  - MeetingID—The unique conference ID generated by your system when the meeting was scheduled.
  - Meeting Number—The Cisco WebEx meeting number.
  - Subject—The name of the meeting configured by the host.
  - HostName—The meeting host.
  - Start Time—The starting time and date of the meeting.
  - Duration—Duration of the meeting in minutes.
  - Number of Participants—The number of participants including hosts.
  - Status
  - Number of Call-In Audio Minutes
  - Number of Call-Back Audio Minutes
  - Number of VoIP Minutes
  - Number of Video Minutes
  - Number of Recording Minutes
  - Recording Interval— Specifies the start and stop time for each recording created during the meeting.

- Number of WebSharing Minutes—The total number of minutes that all participants spend in the web meeting (for example, if three participants attend the web meeting portion of a meeting that lasts 10 minutes, the number of web sharing minutes is 30).
- Participants—A list of the meeting participants.
- Host Platform/Browser—The version of the operating system and browser used by the host when the host started a Cisco WebEx meeting.
- Host IP Address—The IP address used by the host when the host started a Cisco WebEx meeting.
- TrackingCodes—The tracking codes applied by the host when scheduling the meeting.

- Network Bandwidth Utilization Report—This report contains a list of network bandwidth consumption for each day in the specified period for each of the following features:
  - Maximum Bandwidth Consumption for Audio (mbps)
  - Maximum Bandwidth Consumption for Audio VoIP (mbps)
  - Maximum Bandwidth Consumption for Video (mbps)
  - Maximum Bandwidth Consumption for Web Sharing (mbps)

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

  Network bandwidth consumption for video includes video from cameras and video file sharing from web meetings. If video is disabled for your site, you cannot turn on a camera for video but you can still share video files. This results in some network bandwidth consumption for video which is included in reports. This is the only situation that causes network bandwidth consumption for video when video is disabled for a site.
- Storage Capacity Utilization Report—This report displays the total disk space used as of the listed date and the number of recorded meetings that occurred for each date.

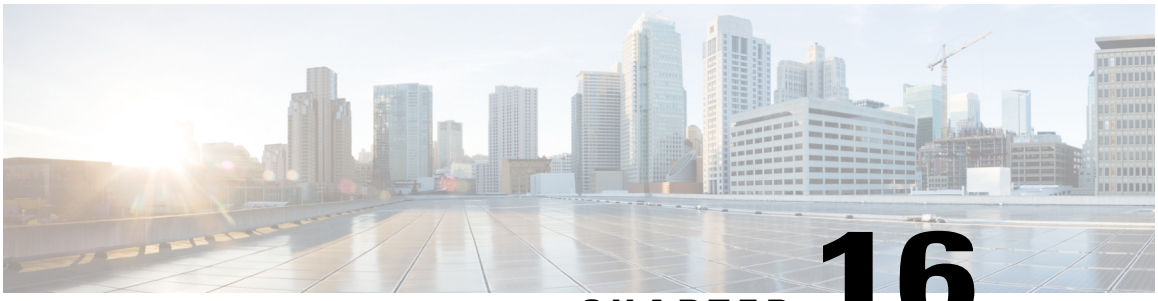
Note This report is only included if you have configured a storage server. See Configuring a Storage Server, on page 150 for more information.

- Participants Report—This report shows the history of meetings, the time each meeting started, and the tracking code applied for each meeting.
  - Meeting ID—The unique conference ID generated by your system when the meeting was scheduled.
  - Conference Name—The name of the meeting the host entered in the **What** field when scheduling a meeting.
  - Username—The user name of the meeting host.
  - Joining Time—The time and date when a user joined a Cisco WebEx meeting.
  - Leaving Time—The time and date when a user left a Cisco WebEx meeting.
  - Duration—The amount of time in minutes a user participated in a Cisco WebEx meeting.
  - Platform/Browser—The version of the operating system and browser used by a host or participant when they started or joined a Cisco WebEx meeting.

- Client IP Address—The IP address of the WebEx client used by a host or participant to start or attend a Cisco WebEx meeting.
- Session Start Time—?????.
- Session End Time—????.
- Type of Session—???.
- Session Duration—The amount of time ??.
- Phone Number—The call-in number the host and participants used to start or join a Cisco WebEx meeting.
- Tel. Server—?????.

- System Downtime Report—This report contains system downtime information for the specified period and includes the following fields:
  - Category—Out of Service or Maintenance. Out of Service indicates an outage. Maintenance indicates a planned maintenance window.
  - Service—Lists the affected features.
  - Start of Downtime—Date and time the downtime started.
  - End of Downtime—Date and time the downtime ended.
  - Number of Meetings Disrupted—Lists the number of meetings disrupted. This field is blank for Maintenance downtimes because those are planned. If no meetings were scheduled during an Out Of Service downtime the number is 0.

- User License Utilization Report—There are two versions of this report. One version displays license usage for the past 30 days and is titled UserLicenseUtilizationReportForLastMonth.csv and the other version displays license usage for the current month (the first day of the month through the current day) and is titled UserLicenseUtilizationForThisMonth.csv. Each of these reports includes the following fields:
  - User Name—The user name of the meeting host.
  - E-mail address—Email address of the meeting host.
  - Meeting ID—The unique conference ID generated by your system when the meeting was scheduled.
  - Meeting Number—The Cisco WebEx meeting number.
  - Start Time—The date and time the meeting started.
  - Simultaneous Meeting—Indicates the number of simultaneous meetings scheduled by the same user. Each simultaneous meeting that is recorded results in an additional line added to this report for the user who scheduled the simultaneous meeting.



CHAPTER 16

Using the Support Features

- Customizing Your Log, page 231
- Setting Up a Remote Support Account, page 232
- Disabling a Remote Support Account, page 233
- Using the Meetings Test, page 233
- Using the System Resource Test, page 234

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 you containing a link to download the log.

Setting Up a Remote Support Account

If you are having technical issues and contact the Cisco TAC for assistance, you can set up a remote support account to grant a TAC representative temporary access to your system. This product does not provide CLI access to administrators and therefore requires a TAC representative to troubleshoot some issues.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **Enable Remote Support**.

Step 4 Complete the fields on the **Remote Support Account** page and select **Create Account**.

Field	Description
Remote Support Account Name	Enter a name for your remote support account (6–30 characters).
Account Life	Specify the duration for the account in hours. The maximum is 30 days (720 hours).
Decoder Version	Select **2- Webex Meetings Server**. **Note** If you have a remote support account that was active prior to the release of Cisco WebEx Meetings Server Version 1.5, you do not have to configure this setting.

The **Remote Support Account Creation** dialog box appears, 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.