Configuring Your System

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

Configuring System Properties

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

Changing Virtual Machine Settings

Use this feature to change virtual machine settings. Do not use VMware vCenter to change virtual machine settings.

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

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

Turning on Maintenance Mode on all active data centers shuts down conferencing activity and prevents users from signing in to the WebEx site, scheduling meetings, joining meetings, or playing meeting recordings. If this data center is part of a Multi-data Center (MDC) system and another data center is active, in-progress meetings will fail over to the

active data center. This might cause a brief interruption in active meetings. See About Maintenance Mode for information about which system tasks require Maintenance Mode to be turned on.

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

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

Step 5 You can modify the following virtual machine settings:

- Fully Qualified Domain Name (FQDN) in lowercase characters
- Primary DNS Server
- Secondary DNS Server
- Subnet Mask/Prefix
- Gateway

The Virtual Machine field is grayed out. The system automatically retrieves the IP address by resolving the host name to the IP address of a virtual machine in the DNS server. See Changing the IP Address of a Virtual Machine, on page 2 for more information about changing an IP address of a virtual machine.

Step 6 Select **Save**.
Your changes are saved and the virtual machine is re-booted.

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

What to Do Next

If you make changes to any of your virtual machines, you must deploy a new certificate on all virtual machines in each data center unless you are using wildcard certificates for systems in the same domain. For more information see Managing Certificates.

Changing the IP Address of a Virtual Machine

If you change the hostname of a virtual machine that is part of your deployment, the corresponding IP address is picked up automatically from the DNS. This procedure explains how to change the IP address of a virtual machine and keep the same hostname.

Step 1 Configure a temporary hostname in the DNS server.

Step 2 Complete the Changing Virtual Machine Settings, on page 1 procedure to change the hostname of the virtual machine to the temporary hostname you entered in the DNS server.
When you take the system out of maintenance mode, the new temporary hostname takes effect.

The original hostname is no longer part of the deployment after making this change.

Step 3 Change the IP address of the original hostname in the DNS to the new IP address.

Step 4 Using the Changing Virtual Machine Settings, on page 1 procedure, change the temporary hostname of the virtual machine to the original hostname.
When you take the system out of maintenance mode, the original hostname takes effect.

Your original hostname with the new IP address is configured.

Changing the Virtual IP Address

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

Step 3 Select **System**, select the *data center*, and select **View More** in the System section.
The **Properties** page appears.

Step 4 To modify the IP addresses, in the Virtual IP Address section select a link in the Type column.

Step 5 Enter the virtual IP addresses.

Step 6 Enter the virtual IP address, subnet mask, and gateway in the IPv6 Address column if you have enabled IPv6 for client connections.
The public and private virtual IP addresses must be on separate IPv6 subnets.

Step 7 Select **Save**.

Step 8 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Configuring Public Access

Public access enables people external to your network to host or attend online meetings through the Internet or mobile devices. Removing public access will remove public virtual IP address settings for your WebEx site URLs and terminate external access to your site.

Adding Public Access to Your System by using IRP

The requirements for Internet Reverse Proxy (IRP) in an MDC environment are:

- The process for adding or removing IRP is the same for a Single-data Center system as they are for a MDC system.
- When adding a data center to a MDC system, all data centers or none of the data centers should be configured to use IRP.
- One IRP node is used per data center.
- Modifying IRP requires that the system be place in Maintenance Mode. In a MDC system, IRP can be added or removed one system at a time to avoid a service interruption.
- In a MDC environment, adding or removing a local public VIP on one data center does not affect the other data centers.

For a description of internal Internet Reverse Proxy topology, see Internal Internet Reverse Proxy (IRP) Network Topology.

Before You Begin

To enable public access you must first configure an Internet Reverse Proxy virtual machine to serve as your public access system. Start VMware vCenter and perform the following:

- Back up your virtual machines using VMware Data Recovery (vSphere 5.0) or VMware vSphere Data Protection (vSphere 5.1). This enables you to revert the changes if necessary. See Creating a Backup by using VMware vCenter for more information.
- Deploy an Internet Reverse Proxy virtual machine using the same OVA file that you used to deploy your administrator virtual machine. Your Internet Reverse Proxy virtual machine must be on the same subnet as the public virtual IP address.

Note If you have a High Availability system, you must also deploy an Internet Reverse Proxy virtual machine for your High Availability system.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.

Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

Step 3 Select **System** > **View More**.

Step 4 Select **Add Public Access**.

Step 5 Enter your Internet Reverse Proxy virtual machine in the **FQDN** field.
There are two fully qualified domain name (FQDN) fields if your system is configured for high availability. Enter your high availability FQDN in the second field.

Step 6 Select **Detect virtual machines**.
If your system is not configured for High Availability, a table appears displaying the Internet Reverse Proxy virtual machine.

If your system is configured for High Availability, a table appears displaying the primary system Internet Reverse Proxy virtual machine and the high availability Internet Reverse Proxy virtual machine.

If your system has any updates that are incompatible with the OVA version you used to create the Internet Reverse proxy virtual machine, you receive an error message and cannot proceed until you redeploy the Internet Reverse Proxy virtual machine by using an appropriate OVA file.

Step 7 Select **Continue**.

Step 8 Enter the IP address from the same subnet that you used to configure your Internet Reverse Proxy virtual machine in the **Public (VIP) Virtual IPv4 Address** field and select **Save**.
Your system is updated and public access is configured. Keep your browser window open for the entire process.

If your system requires minor updates compatible with the OVA version you used for creating the Internet Reverse Proxy virtual machine, they are automatically applied to your Internet Reverse Proxy virtual machine.

Step 9 If your system requires minor updates, you are prompted to select **Restart** after the updates are complete.
After the system restarts, you receive a confirmation message indicating that you have added public access.

Step 10 Verify your configuration. If you are satisfied, you can delete the virtual machine backup that you configured before performing this procedure.

Step 11 Select **Done**.

Step 12 Verify that your security certificates are still valid.
Because this procedure changes your virtual machines, it might affect your certificates. If necessary, your system provides a self-signed certificate to keep your system functioning until you can reconfigure your certificates. See Managing Certificates for more information.

Step 13 Make any necessary changes to your DNS servers.

Step 14 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Removing Public Access

Before You Begin

Back up your virtual machines using VMware Data Recovery or VMware vSphere Data Protection. See Creating a Backup by using VMware vCenter for more information. Make sure you power on your virtual machines after your backup is complete.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

Step 3 Select **System** and then select the **View More** link in the System section.
The **Properties** page appears.

Step 4 Select the desired site, select **Remove Public Access**, and select **Continue**.
After you remove public access from your site, you cannot add the same Internet proxy virtual machine to that site. To reconfigure public access, you must start over by redeploying an Internet reverse proxy virtual machine from the OVA file. See Adding Public Access to Your System by using IRP, on page 4 for more information.

Public access is removed from the site.

Step 5 Select **Done**.

Step 6 Open VMware vCenter. Power off, and delete the Internet Reverse Proxy machine (and high-availability Internet reverse proxy machine, if deployed) from your system.

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Configuring IPv6 for Client Connections

When you have a non-split-horizon network topology, all users (internal and external) with an IPv6 client connection can access the WebEx site URL using the public VIP address to host and access online meetings. When the private IPv6 virtual IP address information is configured, administrators with an IPv6 client connection can sign in to the Administration site.

Note

- The IPv6 private virtual IP address must be on the same IPv6 subnet as the Admin virtual machine.
- The IPv6 public virtual IP address must be on the same IPv6 subnet as the Internet Reverse Proxy virtual machine.

Before You Begin

Consider the following when configuring an IPv6 client connection:

- Configuring an IPv6 connection only for non-split-horizon network topologies.
- IPv4 address information should already be configured for internal virtual machines and the Internet Reverse Proxy.
- The IPv4 private and public virtual IP addresses should already be configured before you configure an IPv6 public virtual IP address.
- The private and public virtual IP address for IPv6 client connections are on separate subnets.
- Configure the DNS servers so your Administration site URL points to the private IPv6 and the private IPv4 virtual IP addresses.
- Configure the DNS servers so your WebEx site URL points to the public IPv6 and the public IPv4 virtual IP addresses.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

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

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

- Select the *Public* link to configure the IPv6 address for accessing the WebEx Site URL.

- Select the *Private* link to configure the IPv6 address for accessing the Administration URL.

The Private or Public Virtual IP Address page displays the previously entered IPv4 IP address, subnet mask, and gateway IP address of the WebEx Site URL and Administration URL.

Step 5 In the IPv6 **Address** column, enter the IPv6 IP address, subnet mask, and gateway IP address of the WebEx Site URL and Administration URL.

Step 6 Select **Save**.

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Changing the CWMS Subnet

Steps to change the CWMS subnet.

Before You Begin

If you are you keeping the same DNS servers, keep the old DNS entries until the change is complete. If you are changing DNS servers, make the change to the servers, turn off Maintenance Mode, and then change the subnet.

If you are keeping the same fully-qualified domain names (FQDNs) and changing only the IP addresses, you must do this in two stages by using temporary names. Typically you can change the IP address of a server only if you also change its name. This is to avoid a change simply by changing a DNS entry. However, Admin and Site URLs do not fall into this category. There might be times that the computer making all the administrative changes appears to be unable to browse to the Admin URL pages. If that happens, make sure that you can ping `nslookup` and if necessary, flush the local PC DNS cache after any changes.

We recommend for all versions of CWMS:

- Create a Remote Support Account prior to beginning any maintenance work.
- Apply for new certificates to be used when the IP address change is completed. In the interim, the system can use a self-signed certificate.
- Verify that the DNS entries are prepared and ready. If the virtual machines do not restart, restart only the Admin virtual machine and change the Network Adapter #2 assignment. The IRP can remain up, and you can change the assignment for Network Adapter #2 when you see the Admin virtual machine rebooting.

Note The trick in the subnet change is that you must edit the virtual machine settings to move the virtual NICs to another VLAN, because you cannot simply power off, make changes to the system, and power it on. You must turn off Maintenance Mode to apply the changes and cause all the virtual machines to reboot. If you fail to change the VLANs after the virtual machines reboot, the network interfaces display, but they will not be able to communicate.

Step 1 Create new DNS entries for new (or temporary) names pointing to new addresses.
a) Go to the Admin window, open the servers one-by-one, and enter the new FQDNs.
b) Turn on Maintenance Mode.
c) Verify that all the parameters are correct for the new subnet (the subnet mask and gateway are often forgotten).

Step 2 After making the changes, go back into each server and verify that the FQDNs are entered correctly.

Step 3 Turn Off Maintenance Mode and monitor the virtual machine consoles in the vSphere client.

Step 4 When a virtual machine comes up from reboot, change the VLAN for Network adapter 1. (This can be done live; there is no need to power the system off and back on.)
The time between turning Maintenance Mode off and the completion of the reboot can be long. When the system comes up, it should work, but the (virtual IP address) VIP will be on a different subnet than the Admin node. This is acceptable temporarily.

Step 5 Open the VIP pages and edit the IP addresses of the Public and Private VIPs.
We recommend that you re-visit the settings to confirm that the changes are accurate.

Step 6 (Optional) Open General Settings and change the URLs (only if you planned for this change). This process does not need temporary values. If the site URL is changed, old meeting links will stop working.

Step 7 Turn off Maintenance Mode. The system restarts. (Although it should reboot, sometimes it simply restarts and fails to reboot. Monitor the virtual machine console. If the system does not reboot all nodes after Maintenance Mode is turned off, reboot the ADMIN nodes manually.
The system restarts. Although it should reboot, sometimes it simply restarts and fails to reboot. Monitor the virtual machine console. If the system does not reboot all nodes when Maintenance Mode is turned off, reboot the Admin nodes manually.

Step 8 As soon as the virtual machines come up from reboot, change the VLAN for Network adapter 2.
It is not necessary to power off and power on the system

The system is in the new subnet.

What to Do Next

If you used temporary names, complete the following procedure:

1. In the DNS, connect the permanent names to the new IP addresses. It might be necessary to change the FQDN of the new IP addresses. Go to CWMS Admin pages and open the servers one-by-one to enter permanent names.
2. Optionally edit the URLs.
3. Turn off Maintenance Mode.

4 After the system reboots, delete the unused entries from DNS.

5 Verify the system is working correctly by accessing the Admin URL. We also recommend that you test access to meeting recordings on the NFS and test the system by creating a new recording.

6 Double check CUCM trunks and modify IP addresses as necessary.

Configuring General Settings

General settings include the following parameters:

- Site Settings—Manages the site URL.
- Administration Site Settings—Manages the administration site URL.

Virtual IP addresses are shown in the information block and can be managed on the **System** > **Properties**.

Changing Your Site Settings

Use this feature to configure or change your Administration site URL, and the Local Administration site URL, if you have Multi-data Center (MDC) System. You configured your original site URLs during deployment. In an MDC system, the local site URL is configured during the process of joining data centers. For more information about site URL configuration and naming conventions, see WebEx Site and WebEx Administration URLs.

Before You Begin

Make sure you retain your original site URL on the DNS server, and 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 applications.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

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

The General Settings window displays.

Step 4 Select the data center if this is a MDC system.

Step 5 In the Site Settings section to be modified, select **Edit**.

Step 6 Enter the URLs and select **Save**.

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

What to Do Next

Update your site certificate to ensure secure access. See Managing Certificates for more information.

Changing Your Administration Settings

You configure your original administration site URL setting during deployment. In an MDC system, your Local Administration site URL is configured during the process of joining data-centers. For more information about administration site configuration and naming conventions, see WebEx Site and WebEx Administration URLs.

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 applications.

Step 1 Sign in to the Administration site.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

Turning on Maintenance Mode on all active data centers shuts down conferencing activity and prevents users from signing in to the WebEx site, scheduling meetings, joining meetings, or playing meeting recordings. If this data center is part of a Multi-data Center (MDC) system and another data center is active, in-progress meetings will fail over to the

active data center. This might cause a brief interruption in active meetings. See About Maintenance Mode for information about which system tasks require Maintenance Mode to be turned on.

Step 3 Select **System**.

Step 4 In the Configuration section select **View More**.

Step 5 In the Administration Settings section, select **Edit**.

Step 6 Enter your new Administration site URLs in the dialog box and select **Save**.

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

What to Do Next

Update your site certificate to ensure secure access. See Managing Certificates for more information.

Configuring Servers

Use these features to configure your servers:

- SMTP Server—The SMTP server handles the sending of email from Cisco WebEx Meeting Server to the destination.
- Storage Server—The NFS server is the storage server where all the meeting recordings are stored.

Configuring an Email (SMTP) Server

Configure an Email server to enable your system to send meeting invitations and other communications to users.

It is important that the Email server is always operational. Email is the primary method of communication with your users including recording notifications, meeting information changes, account status, and many other important announcements. (See also Adding Users.)

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

Note Turning on Maintenance Mode is not required to change these properties.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

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

Step 3 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

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

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

Step 6 (Optional) Select **TLS enabled** to enable Transport Layer Security (TLS). (Basic authentication is enabled by default.)

Step 7 (Optional) Edit the **Port** field to change the default value.
The SMTP default port numbers are 25 or 465 (secure SMTP port).

Note The Web node and Admin node send SMTP requests to the configured Email server. If there is a firewall between the internal Web and Admin virtual machines and the Email server, the SMTP traffic might be blocked. To ensure Email server configuration and Email notification work properly, port 25 or 465 (secure SMTP port number) must be open between the Email server and the Web and the Admin virtual machines.

Step 8 (Optional) Enable mail server authentication, select **Server authentication enabled**. If you enable authentication, enter the **Username** and **Password** credentials necessary for the system to access the corporate mail server.
Emails from the system are sent by `admin@<WebEx-site-URL>`. Ensure that the mail server can recognize this user.

For micro, small, or medium systems, email notifications come from the administration virtual machines (either the primary or high-availability system).

For large systems, email notifications come from the web virtual machines (either on the primary or high-availability system). In a large system, there are three web virtual machines on the primary system and one web virtual machine on the high-availability system.

Step 9 Select **Save**.

What to Do Next

See Activating or Deactivating Users and Administrators from the Users Page, Adding Users, and Editing Users.

Adding a Storage Server

Use the storage server to back up your system and store meeting recordings. During a Disaster Recovery (see Disaster Recovery by using the Storage Server, on page 19), these backups can be used to restore the system. (The supported storage method is Network File System (NFS)). Verify that your storage server is accessible from all internal virtual machines. (There is also a VMware-provided VMware Data Recovery feature to backup the virtual machines. See http://www.vmware.com/pdf/vdr_11_admin.pdf for more information.)

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

Restriction Do not manually create files or directories in the NFS share used by Cisco WebEx Meetings Server, as it runs various scripts on NFS files and directories. The NFS storage server must be for the exclusive use of Cisco WebEx Meetings Server.

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). (See Connect a Linux Client to the NFS Share , on page 17.)

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. (See m_ConfiguringNFSShare.ditamap.)

Step 1 Sign in to the Administration site.

In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

Step 3 In the Servers section, select **Servers** > **(Servers) View More**.
If a storage server is present on your system, it is displayed on this page. If there is no storage server present on your system, you are given the option to add one.

Step 4 In the Storage Server section, select **Add a Storage Server now**.

Step 5 Enter the NFS mount point and select **Save**.
The system confirms your NFS mount point.

Step 6 Select **Continue**.
You receive a confirmation message that your storage server has been added.

Step 7 Select **Done**.

Step 8 (Optional) You can change the default time for the daily backup. In the Storage Server section, click the System Backup Schedule **time** and select another time from the drop-down menu. Then select **Save**.
A daily backup occurs at the time you selected.

Step 9 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

What to Do Next

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

- Meeting recordings.
- Disaster recovery. See Disaster Recovery by using the Storage Server, on page 19 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.

Install NFS File Services

Install NFS file services:

Step 1 Launch Server Manager.
Step 2 On the top menu, select **Manage**.
Step 3 Select **Add Roles and Features**.
The **Before you begin** window appears.
Step 4 Select **Next**.
The **Select installation type** window appears.
Step 5 Verify that **Role-based or feature-based installation** is selected and select **Next**.
The **Server selection** window appears.
Step 6 Select **Next**.
The **Select server roles** window appears.
Step 7 Expand **File and Storage Services** > **File and iSCSI Services**, and then check **Server for NFS**.
Step 8 Select **Next**.
The **Select feature** window appears.
Step 9 Select **Next**.
Step 10 Confirm the installation details, and then select **Install**.

What to Do Next

Configure an NFS Share

Configure an NFS share:

Before You Begin

Install NFS file services. (See Install NFS File Services , on page 16.)

Step 1 Launch File Explorer.

Step 2 Create a new directory for your NFS share.

Step 3 Right-click the directory and select **Properties**.

Step 4 Select the **NFS Sharing** tab.

Step 5 Select **Manage NFS Sharing**….

Step 6 Check **Share this folder** and enter 65534 in **Anonymous UID** and **Anonymous GID**.

Step 7 Enter a **Share** name.
This is the name used when a user connects to this NFS share.

Step 8 Select **Permissions**.

Step 9 Select **Add** and enter the IP address or hostname of the client(s) allowed connections.

Step 10 Choose Read–Write access or Read-Only access and select **OK**.

Step 11 Select **Apply** > **OK**
An NFS share is hosted on a Windows Server 2012 R2.

What to Do Next

Connect a Linux Client to the NFS share. (See Connect a Linux Client to the NFS Share , on page 17.)

Connect a Linux Client to the NFS Share

Step 1 Log onto a Linux server or desktop.
Open a terminal window, if you are in a Desktop version of the operating system.

Step 2 Create a new directory on which to mount the Windows NFS share. For example `mkdir/postprod`.

Step 3 Mount the NFS share to the new directory. For example `mount.nfs slfileserver01:/postprod /postprod`
If the client has Read–Write access, test the share by creating a new file. For example `touch file01.txt`.

Step 4 If the client has Read–Write access, test the share by creating a new file

Changing to a Different Storage Server

Switching a storage server from the current NFS or SSH NFS to a replacement NFS or SSH NFS can render recordings unaccessible unless you transfer the recordings and backups to the new storage server.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

Step 3 Select **System** > **(Servers) View More** > **Remove Storage Server**.

Step 4 Manually transfer recordings and backup files from the old storage server to the new storage server.
Specific instructions for transferring recordings and backups cannot be provided, as each system is unique.

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

Step 6 Enter the replacement NFS mount point or the replacement Secure Storage username, password, and mount point and select **Save**.
NFS storage example NFS Mount Point: `192.168.10.10:/CWMS/backup`.

Secure Storage Example:

- Storage Server Username: `user1`
- Storage Server Password: `*******`
- Storage Server Mount point: `192.168.10.10:/CWMS/backup`

The system confirms your replacement NFS mount point or Secure Storage mount point.

Step 7 (Optional) Select **Yes** to perform the disaster recovery procedure or select **No** to skip this step.
If there are no system backup files on the replacement storage server, this step is automatically skipped. For additional information regarding disaster recovery, see Disaster Recovery by using the Storage Server, on page 19.

Step 8 Select **Continue**.
You receive a confirmation message that your storage server has been added.

Step 9 Select **Done**.

Step 10 (Optional) You can change the default time for the daily backup. In the Storage Server section, click the System Backup Schedule **time** and select another time from the drop-down menu. Then select **Save**.
A daily backup occurs at the time you selected.

Step 11 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.

When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Disaster Recovery by using the Storage Server

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

- Single-data Center (SDC) disaster recovery—You can reinstall your SDC system in the same data center and restore it to the same state by using storage server backups.
- Multi-data Center (MDC) disaster recovery—If one data center fails, you can access the MDC system through the second data center, restore the damaged data center, and join the data centers to restore the MDC system.

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

Note that disaster recovery:

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

This procedure backs up certain system settings, user information, meeting information, SSL certificates uploaded into the system, and the site URL. The backup process does not store VMware credentials or IP address information for individual virtual machines. (There is also a VMware-provided VMware Data Recovery feature to backup the virtual machines. See http://www.vmware.com/pdf/vdr_11_admin.pdf for more information.) In the event that you perform a disaster recovery, you must manually reapply certain settings including the following:

- Connections to certain external components, for example Cisco Unified Communications Manager (CUCM).
- SSL certificates (in case the hostnames of the disaster recovery system differ from those in the original system).
- On SDC systems, you can optionally use the same IP address or hostname. On multi-data centers systems, you can optionally use the original IP addresses or hostnames for your primary system.

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

Before You Begin

To perform disaster recovery procedures:

- A storage server must have been configured. If you do not have a storage server configured, the **Disaster Recovery** option is not available and backups are not created. See Adding a Storage Server, on page 14 for more information.
- You must have access to a system from where you can restore your deployment. See the information on Single-data Center (SDC) and Multi-data Center (MDC) disaster recovery, below.
- Your recovery system must be the same deployment size and software version as your original system.

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

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

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

Step 3 Select **System** > **(Servers) View More** > **Add Storage Server**.

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

Example:
192.168.10.10:/CWMS/backup.

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

Step 6 Select one of the following actions to continue:

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

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

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.

When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

What to Do Next

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

- Reconfigure your teleconferencing settings. Refer to Configuring CUCM in the Planning Guide for more information.
- Reconfigure your SSO settings. See Configuring Federated Single Sign-On (SSO) Settings for more information.
- Reconfigure your SNMP settings. See Configuring Your SNMP Settings, on page 21 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 Major System Modification and About Host 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 the Virtual IP Address, on page 3 for more information.
- If you have configured your system for Directory Integration and enabled LDAP authentication, verify that your CUCM credentials work. After you take your system out of maintenance mode and your system reboot is complete, sign in to the Administration site, select **Users** > **Directory Integration**, and then select **Save**. If your CUCM credentials are incorrect, you receive an **Invalid Credentials** error message. If you receive this error message, enter the correct credentials and select **Save** again. See Configuring Directory Integration for more information.

Configuring Your SNMP Settings

You can configure the following SNMP settings:

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

• Notification destinations—Use this feature to configure the trap/inform receiver.

Configuring Community Strings

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

Adding Community Strings

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

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

Step 4 Select **Add** in the Community Strings section.

Step 5 Complete the fields on the **Add Community String** page.

Option	Description
Community String Name	Enter your community string name. Maximum length: 256 characters.
Access Privileges	Set access privileges for the community string. Options include: • ReadOnly • ReadWrite • ReadWriteNotify • NotifyOnly • None **Default**: ReadOnly
Host IP Address Information	Select your host IP address information type. (Default: **Accept SNMP Packets from any Hosts**) If you select **Accept SNMP Packets from these Hosts**, a dialog box appears below the selection. Enter host names and IP addresses separated by commas.

Select **Add**.

The community string is added to your system.

Step 6 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Editing Community Strings

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

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

Step 4 Select a community string name link in the Community Strings section.

Step 5 Change the desired fields on the **Edit Community String** page.

Option	Description
Community String Name	Change your community string name. Maximum length: 256 characters.
Access Privileges	Set access privileges for the community string: • ReadOnly • ReadWrite • ReadWriteNotify • NotifyOnly • None **Default**: ReadOnly

Option	Description
Host IP Address Information	Select your host IP address information type. **Default**: Accept SNMP Packets from any Hosts **Accept SNMP Packets from these Hosts**: a dialog box appears below the selection. Enter host names and IP addresses separated by commas.

Select **Edit**.

Your community string information is changed.

Step 6 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Configuring USM Users

You can add and edit your USM users.

Adding USM Users

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

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

Step 4 Select **Add** in the USM Users section.

Step 5 Complete the fields on the **Add USM User** page.

Option	Description
USM User Name	Enter the USM user name you want to configure. Maximum 256 characters.
Security Level	Select the security level. The security level you select determines which algorithms and passwords you can set for the user. Options include: • noAuthNoPriv—No authentication algorithm and password and no privacy algorithm and password for the user. • authPriv—Enables you to configure authentication algorithm and password and privacy algorithm and password for the user. • authNoPriv—Enables you to configure authentication algorithm and password for the user. **Default**: noAuthNoPriv
Authentication Algorithm	Select the authentication algorithm for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**. **Default**: SHA
Authentication Password	Enter the authentication password for the user. **Note** This option appears only if the security level is set to **authPriv** or **authNoPriv**.
Privacy Algorithm	Select the privacy algorithm for the user. **Note** This option appears only if the security level is set to **authPriv**. **Default**: AES128
Privacy Password	Enter the privacy password for the user. **Note** This option appears only if the security level is set to **authPriv**.

Step 6 Select **Add**.
The USM user is added to your system.

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Editing USM Users

Note The default USM user, serveradmin, is used internally. An administrator can change the USM user name and privacy password for the serveradmin user, but cannot change the security level, authentication algorithm, or privacy algorithm for this user.

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

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

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

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

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

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

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

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Configuring Notification Destinations

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

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

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

Turning on Maintenance Mode on all active data centers shuts down conferencing activity and prevents users from signing in to the WebEx site, scheduling meetings, joining meetings, or playing meeting recordings. If this data center is part of a Multi-data Center (MDC) system and another data center is active, in-progress meetings will fail over to the

active data center. This might cause a brief interruption in active meetings. See About Maintenance Mode for information about which system tasks require Maintenance Mode to be turned on.

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

Step 4 Select **Add new Notification Destination** under **Notification Destinations**.

Step 5 Configure the following fields for your notification destination:

Option	Description
Destination Hostname / IP Address	The hostname or IP address of the virtual machine you want to set up as a notification destination.
Port Number	The port number for your virtual machine. **Default**: 162
SNMP Version	Your SNMP version. **Default**: V3
Notification Type	Select **Inform** or **Traps**. **Default**: Traps
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 24 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 22 for more information.

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

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.

Editing a Notification Destination

Configuring Notification Destinations

Step 1 Sign in to the Administration site.
In a Multi-data Center system, the DNS determines which data center Dashboard appears. All data centers can be managed from this Dashboard.

Step 2 Turn on Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
Unless you are expanding a system, we recommend that you take a snapshot of each virtual machine. (See Taking a Snapshot by using VMware vCenter.)

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

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

Step 4 Select a notification destination link from the **Notification Destinations** list.

Step 5 You can edit the following fields for your notification destination:

Option	Description
Destination Hostname / IP Address	The hostname or IP address of the virtual machine you want to set up as a notification destination.
Port Number	The port number for your virtual machine. **Default**: 162
SNMP Version	Your SNMP version. **Default**: V3
Notification Type	Select **Inform** or **Traps**. **Default**: Inform
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 24 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 22 for more information.

Step 6 Select **Save**.

Your notification destination changes are saved.

Step 7 Turn off Maintenance Mode. See Turning Maintenance Mode On or Off for Version 2.5 and Later.
When you turn off Maintenance Mode, the system determines if a *restart* (takes approximately 3 - 5 minutes) or a *reboot* (takes approximately 30 minutes) is required and displays the appropriate message. If this data center is part of a Multi-data Center (MDC) system, the administrator is re-directed to the global admin URL. The data center that the administrator sees is determined by the DNS resolution policy. If Key Regeneration is enabled, taking one data center out of Maintenance Mode automatically takes all data centers in the system out of Maintenance Mode.

Meeting service for users on this data center is restored.