Configuring Your System

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

Configuring System Properties

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

Changing Your Virtual Machine Settings

Use this feature to change your virtual machine settings.

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 5 You can modify the following virtual machine settings:

- Fully Qualified Domain Name—Your system's FQDN.
- Virtual Machine—Your virtual machine IP address.
- Primary DNS Server
- Secondary DNS Server
- Subnet Mask/Prefix
- Gateway

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

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

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

What to Do Next

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

Configuring a High Availability System

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

Adding a High Availability System

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

Note Complete the following procedure on the primary system.

Before You Begin

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

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

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

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 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.

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 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 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 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 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 6 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, which describes all the pre-requisite steps you should take before using this feature and how to expand your system using automatic or manual deployment.

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **Expand System Size**.

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

Step 5 Select **Continue**.
Your system checks connectivity to the virtual machines. If there are connectivity problems with one or more virtual machines, you must fix the problems before you can continue. If there are no connectivity problems, your system performs an automatic backup. After the backup is complete, you are notified that you can proceed with your expansion.

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

- Expanding the System Using Automatic Deployment
- Expanding the System Using Manual Deployment

Your system notifies you once the expansion is complete.

Step 7 Select **Restart**.

Step 8 Sign in to the Administration site.

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

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, on page 8 for more information.

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

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

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

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

Configuring General Settings

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

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

Changing Your Site Settings

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.

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 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.

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 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.

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 14 for more information.

Using the Disaster Recovery Feature

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

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

After you have configured a storage server, your system is backed up on a daily basis. A system backup notice appears on your dashboard that displays information about the latest backup. If you perform a disaster recovery the latest backup is used. Only one backup system is kept in storage at a time. After you perform an upgrade or update, the latest 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," below).

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, CUCM)
- SSL certificates (in case the hostnames of the disaster recovery system differ from those in the original system)

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

Before You Begin

- To perform disaster recovery procedures, you must have a storage server configured. See Configuring a Storage Server, on page 12 for more information. If you do not have a storage server configured, the **Disaster Recovery** option is not available and no backup will be available.
- You must have access to a system on which you can restore your deployment. See the information on one data center and two data center disaster recovery, below.
- Your recovery system must be the same deployment size and software version as your original system.

  Disaster recovery can be performed on systems with or without high availability. However, you cannot perform disaster recovery on a high-availability system. You must complete disaster recovery first and then you can configure high availability on that system. If you have a high-availability system that

requires disaster recovery, you must restore your system first and then configure high availability on your 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 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:
Enter 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. If this happens, you must redeploy the application on your recovery system so that the deployment size and software version match the original deployment.

Step 6 Select one of the following to continue:

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

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

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

What to Do Next

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

- Reconfigure your teleconferencing settings. Refer to Configuring CUCM in the Planning Guide for more information.
- Reconfigure your SSO settings. See Configuring Federated Single Sign-On (SSO) Settings for more information.
- Reconfigure your SNMP settings. See Configuring Your SNMP Settings, on page 16 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.
- Your recovery system is initially configured for License Free Mode which expires in six months. Re-host your previous system's licenses on the recovery system. See 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, on page 5 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. The default password for the default USM user, serveradmin, is not secure because all Cisco WebEx Meetings Server users have the same default password. We strongly recommend that you change the default password.
- 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.

Option	Description
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.

Option	Description
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.

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

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

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

Configuring Notification Destinations

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

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 5 Configure the following fields for your notification destination:

Option	Description
Destination Hostname / IP Address	The hostname or IP address of the virtual machine you want to set up as a notification destination.
Port Number	The port number for your virtual machine. **Default**: 162
SNMP Version	Your SNMP version. **Default**: V3
Notification Type	Select **Inform** or **Traps**. **Default**: Traps
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 18 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 16 for more information.

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

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

Editing a Notification Destination

Configuring Notification Destinations

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

Option	Description
Destination Hostname / IP Address	The hostname or IP address of the virtual machine you want to set up as a notification destination.
Port Number	The port number for your virtual machine. **Default**: 162
SNMP Version	Your SNMP version. **Default**: V3
Notification Type	Select **Inform** or **Traps**. **Default**: Inform
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 18 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 16 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 Enterprise License Manager (ELM).

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 15 Select **Manage Licenses**.

Your browser opens a new tab or window containing Cisco Enterprise License Manager (ELM).

Step 16 Select **Install License File**.

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

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

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

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, then that user consumes one license. If this 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, etc.)
- If a user hosts simultaneous meetings (at the same date and time), then the system counts an additional license for each simultaneous meeting hosted by this user during the month.
- If a user hosts no meetings during a given month, then this user consumes no licenses for that month.

If you perform a major upgrade or disaster recovery on your system, you must configure new virtual machines and therefore you must also obtain new licenses.

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

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in One Month
User B hosts one meeting.	January 2	9:00 a.m.	No	1
User C hosts two meetings on different dates and times.	January 3 January 4	9:00 a.m. 10:00 a.m.	No	1
User D hosts two meetings on the same date and time.	January 6 January 6	9:00 a.m. 9:00 a.m.	Yes (2)	2
User E hosts two meetings on the same date and time, and another two simultaneous meetings on a different date and time within the month.	January 6 January 6 January 10 January 10	9:00 a.m. 9:00 a.m. 4 p.m. 4 p.m.	Yes (2)	2
User F hosts two meetings on the same date and time neither of which he attends, although the meetings occur.	January 7 January 7	9:00 a.m. 9:00 a.m.	Yes (2)	2
User G hosts a meeting and passes host rights to another participant during the meeting. The user then hosts a 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 hosts a meeting but all of the meeting participants join the teleconference only (not the web portion) with the **Join Before Host** option selected.	January 9	9:00 a.m.	No	1

Scenario	Meeting Date	Meeting Start Time	Simultaneous Meetings	Licenses Consumed in One Month
User J hosts two meetings on the same date and time but all of the meeting participants join the teleconference only (not the web portion) with the **Join Before Host** option selected.	January 10 January 10	9:00 a.m. 9:00 a.m.	No	0
User K hosts a meeting and passes host rights to another participant during the meeting. The user then hosts 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

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.

Caution Your system allows license consumption to exceed the number of licenses installed on your system. However, administrators will 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 will see a "Site under maintenance" message when they go to the WebEx site. The Administration site will function normally so an administrator can sign in and add enough licenses to address the licenses exceeded condition. Once additional licenses have been installed, users will once again be able to access the WebEx site and 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 for more information.
- Upgrade—See Upgrading the System for more information.
- Disaster Recovery—See Using the Disaster Recovery Feature, on page 14 for more information.