Configuring Your System

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

Configuring System Properties

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

Changing Your Virtual Machine Settings

Use this feature to change your virtual machine settings.

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 5 You can modify the following virtual machine settings:

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

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

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

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

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

What to Do Next

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

Configuring a High Availability System

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

Linking a High Availability System to a Primary System

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

Before You Begin

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

Procedure

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

Step 2 Sign into the primary system administration site.

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

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

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

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

Step 7 Enter the fully-qualified domain name (FQDN) of the Administration site virtual machine of the high-availability system and select **Continue**.

The readiness of both the primary system and the HA system is validated. If both systems are ready, then you will see a green **Add** button. (Do not select it if your system is not in Maintenance Mode.) If either system is not ready, an error message is displayed. Fix the error and attempt the procedure again.

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

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

Removing a High Availability System

Before You Begin

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select **Remove High Availability System**.
The **Remove High Availability System** page appears displaying the fully qualified domain name (FQDN) of your high-availability system.

Step 5 Select **Continue**.
Note After you have removed a high-availability system, you cannot add the same high-availability system back to your site. To reconfigure high availability, you must start over by redeploying a high-availability system from the OVA file. See Adding a High Availability System for more information.
Your high-availability system is removed.

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

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

System Behavior After Component Failure

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

High-Availability Systems

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

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

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

- For a period of up to three minutes, application sharing, audio voice connection using computer and video might be interrupted. Cisco WebEx Meetings Server allows three minutes for the failure to be detected and to reconnect all the affected meeting clients automatically. Users should not need to close their meeting clients and rejoin their meeting.
- Some failures might cause teleconferencing audio connections to disconnect. If that happens, users will need to reconnect manually. Reconnection should succeed within two minutes.
- For some failures not all clients and meetings are affected. Meeting connections are normally redistributed across multiple virtual machines and hosts.

Additional Information For a 2000 User System

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

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

For a 2000 user system with high availability:

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

- When an administration virtual machine fails, any existing administrator sessions also fail. Administrators must sign in again to the Administration site and establish a new browser session that will be hosted on the alternate administration virtual machine. Also, there might be a brief interruption to any existing administrator or end-user meeting sessions.

Changing Your Virtual IP Address

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

Step 6 Select **Save**.

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

Configuring Public Access

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

Adding Public Access to Your System

Before You Begin

To enable public access you must first configure an Internet Reverse Proxy virtual machine to serve as your public access system.

Start VMware vCenter and perform the following:

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

Note If you have a high-availability system, you must also deploy an Internet reverse proxy virtual machine for your high-availability system.

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select **Add Public Access**.

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

Note There are two fully qualified domain name (FQDN) fields if your system is configured for high availability. Enter your high availability FQDN in the second field.

Step 6 Select **Detect virtual machines**.

- If your system is not configured for high availability, a table appears displaying the Internet reverse proxy virtual machine.
- If your system is configured for high availability, a table appears displaying the primary system Internet Reverse Proxy virtual machine and the high availability Internet reverse proxy virtual machine.

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

Step 7 Select **Continue**.

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

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

Step 9 If your system requires minor updates, you are prompted to select **Restart** after the updates are complete. If no updates are required, proceed to the following step.
After your system restarts, you receive a confirmation message indicating that you have added public access.

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

Step 11 Select **Done**.

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

Step 13 Make any necessary changes to your DNS servers.

Step 14 Select **Turn Off Maintenance Mode** and **Continue** to confirm.

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

Removing Public Access

Before You Begin

Back up your virtual machines using VMware Data Recovery (vSphere 5.0) or VMware vSphere Data Protection (vSphere 5.1). This enables you to revert your changes if necessary. See Creating a Backup by using VMware vCenter for more information. Make sure you power on your virtual machines after your backup is complete.

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Note After you remove public access from your site, you cannot add the same Internet proxy virtual machine to that site. To reconfigure public access, you must start over by redeploying an Internet reverse proxy virtual machine from the OVA file. See Adding Public Access to Your System, on page 5 for more information.

Step 5 Select **Done**.

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

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

Expanding the System Size

Before You Begin

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

Procedure

Step 1 Sign in to the Administration site.

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

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

Step 4 Select **Expand System Size**.

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

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

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

Your system notifies you once the expansion is complete.

Step 7 Select **Restart**.

Step 8 Sign in to the Administration site.

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

Configuring General Settings

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

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

Changing Your Site Settings

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

Before You Begin

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

What to Do Next

Update your site certificate to ensure secure access. See Managing Certificates 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 **Turn On Maintenance Mode** and **Continue** to confirm.

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

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

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

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

What to Do Next

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

Configuring Servers

Use these features to configure your servers:

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

Configuring an eMail (SMTP) Server

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

Note It is important that the mail server is always operational. Email is the primary method of communication with your users including recording notifications, meeting information changes, account status, and many other important announcements.

Procedure

Step 1 Sign into the Administration web site.

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

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

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

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

Step 6 Optionally select **TLS enabled**.

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

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

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

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

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

Step 9 Select **Save**.

Configuring a Storage Server

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

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

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

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

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

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

Before You Begin

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

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

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

Procedure

Step 1 Sign in to the Administration site.

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

Step 3 Select **System**.

Step 4 In the Servers section, select **View More**.
If a storage server is present on your system, it is displayed on this page. If there is no storage server present on your system, you are given the option to configure one.

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

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

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

Step 8 Select **Done**.

Step 9 (Optional) You can change the default time for the daily backup. In the Storage Server section, click the System Backup Schedule **time** and select another time from the drop-down menu. Then select **Save**.
A daily backup occurs at the time you selected instead of the initially set time of 4:20 a.m. local time.

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

What to Do Next

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

- Meeting recordings.
- Disaster recovery. See Using the Disaster Recovery Feature, on page 13 for more information.

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

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

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

Using the Disaster Recovery Feature

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

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

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

Note that disaster recovery:

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

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

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

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

Before You Begin

To perform disaster recovery procedures:

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

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

Procedure

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

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

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

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

Example:
192.168.10.10:/CWMS/backup.

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

Step 6 Select one of the following actions to continue:

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

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

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

What to Do Next

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

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

Configuring Your SNMP Settings

You can configure the following SNMP settings:

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

Configuring Community Strings

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

Adding Community Strings

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

Select **Add**.

The community string is added to your system.

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

Editing Community Strings

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

Select **Edit**.

Your community string information is changed.

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

Configuring USM Users

You can add and edit your USM users.

Adding USM Users

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

Step 6 Select **Add**.

The USM user is added to your system.

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

Editing USM Users

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

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

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

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

Configuring Notification Destinations

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

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

Procedure

Step 1 Sign in to the Administration site.

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

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

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

Step 5 Configure the following fields for your notification destination:

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

Option	Description
Notification Type	Select **Inform** or **Traps**. **Default**: Traps
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 17 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 15 for more information.

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

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

Editing a Notification Destination

Configuring Notification Destinations

Procedure

Step 1 Sign in to the Administration site.

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

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

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

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

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

Option	Description
Notification Type	Select **Inform** or **Traps**. **Default**: Inform
USM Users **Note** This option appears only when SNMP Version is set to V3.	Select USM users. See Configuring USM Users, on page 17 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 15 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.