Configure Cisco Unified Operating System

Access Cisco Unified Communications Operating System Administration

Note Do not use the browser controls (for example, the Back button) while you are using Cisco Unified Communications Operating System Administration.

Procedure

Step 1 Log in to Emergency Responder.

Step 2 From the Navigation menu in the upper right corner of the Emergency Responder Administration page, choose **Cisco Unified OS Administration** and click **Go**.

The Cisco Unified Communications Operating System Administration Logon window appears.

Note You can also access Cisco Unified Communications Operating System Administration directly at **http://**"server-name"**/cmplatform**.

Step 3 Enter your Administrator username and password.

Note The Administrator username and password are established during installation or created by using the CLI.

Step 4 Click **Submit.**

The Cisco Unified Communications Operating System Administration window appears.

Recover Administrator and Security Passwords

If you lose the administrator password or security password, use the following procedure to reset these passwords.

To perform the password recovery process, you must be connected to the system through the system console, that is, you must have a keyboard and monitor connected to the server. You cannot recover a password when connected to the system through a secure shell session.

Caution The security password on all servers in the server group must match. Change the security password on all machines, or the servers will not communicate with one another.

Caution You must reset each server in a server group after you change its security password. Failure to reboot the servers causes system service problems and problems with the Emergency Responder Administration page on the subscriber server.

Note During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

Step 1 Log in to the system with the following username and password:

- Username: **pwrecovery**
- Password: **pwreset**

The Welcome to platform password reset window displays.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.

The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.

Note For this test, you must use a data CD, not a music CD.

The system tests to ensure that you have inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.

The password must contain at least 6 characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password gets reset, and you get prompted to press any key to exit the password reset utility.

View Cisco Unified OS Information

Using the CiscoUnifiedOS Administration web pages, you can view the status of the operating system, platform hardware, or the network. The following sections describe how to display this information.

View ServerGroup Information

Procedure

Step 1 From the main CiscoUnified Operating System Administration web page, select **Show** > **ServerGroup**. The ServerGroup page appears.

Step 2 For descriptions of the fields on the ServerGroup page, see Table 1.

View Hardware Status

Procedure

Step 1 From the main CiscoUnifiedOperating System Administration web page, select **Show** > **Hardware**. The Hardware Status page appears.

Step 2 For descriptions of the fields on the Hardware Status page, see Table 1.

View Network Status

The network status information that appears depends on whether Network Fault Tolerance is enabled. When Network Fault Tolerance is enabled, Ethernet port 1 automatically takes over network communications if Ethernet port 0 fails. If Network Fault Tolerance is enabled, network status information appears for the network ports Ethernet 0, Ethernet 1, and Bond 0. If Network Fault Tolerance is not enabled, status information appears only for Ethernet 0.

Procedure

Step 1 From the CiscoUnifiedOperating System Administration web page, select **Show > Network**.
The Network Settings page appears.

Step 2 See Table 1 for descriptions of the fields on the Network Settings page.

View Installed Software

Procedure

Step 1 From the CiscoUnifiedOperating System Administration web page, select **Show > Software**.

The Software Packages page appears.

Step 2 For a description of the fields on the Software Packages page, see Table 1.

View System Status

Procedure

Step 1 From the CiscoUnifiedOperating System Administration web page, select **Show > System**.
The System Status page appears.

Step 2 See Table 1 for descriptions of the fields on the System Status page.

View IP Preferences

Procedure

Step 1 From the CiscoUnifiedOperating System Administration web page, select **Show > IP Preference**.
The IP Preferences page appears.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3, on page 5.

To filter or search records:

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click **Clear Filter** to remove all added search criteria.

Step 3 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Display and Modify Cisco Unified OS Settings

Use the Settings options to display and modify IP settings, host settings, and Network Time Protocol (NTP) settings. The following sections describe how to display and modify CiscoUnifiedOS settings.

Set Up Ethernet Settings

The Ethernet Settings options allow you to view and change Dynamic Host Configuration Protocol (DHCP), port, and gateway information.

The Ethernet Configuration page allows you to enable or disable DHCP, to specify the Ethernet port IP address and subnet mask, and to specify the IP address for the network gateway.

Note All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The maximum transmission unit (MTU) on Eth0 defaults to 1500.

Procedure

Step 1 From the CiscoUnifiedOS Administration web page, select **Settings > IP > Ethernet**.
The Ethernet Configuration page appears.

Step 2 Modify the Ethernet settings by entering the new values in the appropriate fields. For a description of the fields on the Ethernet Configuration page, see Table 1.

Note If you enable DHCP, then the Port Information and Gateway Information settings are disabled and cannot be changed.

Step 3 Click **Save** to preserve your changes.

Set Up NTP Servers

Ensure that external NTP server is stratum 9 or higher (1–9). To add, delete, or modify an external NTP server, follow these steps.

Note You can only configure the NTP server settings on the Publisher.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Settings > NTP Servers**.

The **NTP Server List** page appears. For details about the **NTP Server List** page, see NTP Server List.

Step 2 You can add, delete, or modify an NTP server:

- To delete an NTP server, check the check box in front of the appropriate server and click **Delete Selected**.
- To add an NTP server, click **Add**. The **NTP Server Configuration** page appears. Enter the hostname or IP address, and then click **Save**.
- To modify an NTP server, click the IP address. The **NTP Server Configuration** page appears. Modify the hostname or IP address and then click **Save**.

Note Any change you make to the NTP servers can take up to five minutes to complete. Whenever you make any change to the NTP servers, you must refresh the page to display the correct status.

Step 3 To refresh the **NTP Server Settings** page and display the correct status, choose **Settings > NTP Servers**.

Note After deleting, modifying, or adding NTP server, you must restart all both the Publisher and Subscriber for the changes to take affect.

Set Up SMTP Settings

The SMTP Settings window allows you to view or set the SMTP hostname and indicates whether the SMTP host is active.

Tip If you want the system to send you e-mail, you must configure an SMTP host.

Procedure

Step 1 From the CiscoUnifiedOS Administration web page, select **Settings > SMTP**.

The SMTP Settings page appears. For details about the SMTP Settings page, see SMTP Settings.

Step 2 Enter the hostname or IP address of the SMTP host.

Step 3 Click **Save**.

Set Up Time Settings

Before you begin

Note Before you can manually configure the server time, you must delete any NTP servers that you have configured. See Set Up NTP Servers , on page 6 for information about deleting NTP servers.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Settings > Time**. The **Time Settings** page appears. For details about the **Time Settings** page, see Time Settings.

Step 2 Enter the date and time for the system.

Step 3 Click **Save**.

Manage Software Versions

You can use this option both when you are upgrading to a newer software version or when you must fall back to an earlier software version.

Caution This procedure causes the system to restart and become temporarily out of service.

Procedure

Step 1 From the CiscoUnifiedOS Administration web page, select **Settings > Version**.
The **Version Settings** page appears. For details about the Version Settings page, see Version Settings.

Step 2 Click **Restart** to restart the version running on the active partition.

The system restarts on the current partition without switching versions.

Step 3 Click **Shutdown** to shut down the system.

The system halts all processes and shuts down.

Note The hardware does not power down automatically.

Caution If you press the power button on the server, the system immediately shuts down.

Step 4 Click **Switch Versions** to shut down the system that is running on the active disk partition and then automatically restart the system using the software version on the inactive partition.

The system restarts and the partition that is currently inactive becomes active.

Note The **Switch Version** button only appears if there is software installed on the inactive partition.

Note You can use this option when you are upgrading to a newer software version or when you must fall back to an earlier software version.

Change IP Addresses for Emergency Responder Servers

You can change the IP address of either the Emergency Responder Publisher, Emergency Responder Subscriber, or both the Emergency Responder Publisher and Subscriber.

The following sections provide information on changing IP addresses on the Emergency Responder servers.

Change IP Address of Emergency Responder Publisher or Standalone Server

Before you begin

Note Update the IP address information about your DNS server before you begin changing the IP address on the server.

Procedure

Step 1 Change the IP address on the Emergency Responder Publisher by using one of the following options:

- In Cisco Unified Operating System Administration, enter the new IP address in **Settings > IP > Ethernet**.
- On the CLI, configure the new IP address with the **set network ip** command.

Step 2 Reboot the Emergency Responder Publisher or Standalone server and wait until it is fully operational. For a Standalone server, go to Step 7 once the server is operational.

Step 3 When the Emergency Responder Publisher is fully operational, login to Cisco Unified Operating System Administration on the Emergency Responder Subscriber.

Step 4 Choose **Settings > IP > Publisher**. Cisco Unified Operating System Administration displays the old IP address of the Publisher. Enter the new IP address of the Publisher in the Edit box and click **Save**.

Step 5 Reboot the Emergency Responder Subscriber immediately, so that the Emergency Responder Publisher maintains communication with the Emergency Responder Subscriber.

Step 6 Verify the replication using the **utils dbreplication status** CLI command. The value on each server should equal two.

Step 7 Verify that the CTI ports are registered on the Emergency Responder Publisher server. If the CTI ports are not registered, you must recreate the CTI ports by deleting the ports and adding them back in again.

Related Topics

Ethernet Configuration
Create Required CTI Ports

Change IP Address of Emergency Responder Subscriber

Before you begin

Update the IP address information about your DNS server before you begin changing the IP address on the server.

Procedure

Step 1 Change the IP address on the Emergency Responder Subscriber by using one of the following options:

- In Cisco Unified Operating System Administration, enter the new IP address in **Settings > IP > Ethernet**.
- On the CLI, configure the new IP address with the **set network ip** command.

Step 2 Reboot the Emergency Responder Subscriber.

Step 3 After the Emergency Responder Subscriber is fully operational, reboot the Emergency Responder Publisher.

Step 4 Verify that the replication using the **utils dbreplication status** CLI command. The local server will have a value of 2 and the remote server will have a value of 3 with the status as Local and Connected on Publisher and Subscriber.

Related Topics

Ethernet Configuration

Change IP Address of Emergency Responder Publisher and Subscriber

If you are planning to change the IP address of both the Publisher and Subscriber, you must change the IP addresses on the servers sequentially, starting with the subscriber first.

Caution Do not begin to change the IP address of the publisher server until you have completed the task of changing the IP address on the subscriber.

For information about changing the IP address of the Emergency Responder Subscriber server, see Change IP Address of Emergency Responder Subscriber , on page 9.

For information about changing the IP address of the Emergency Responder Publisher server, see Change IP Address of Emergency Responder Publisher or Standalone Server , on page 8.

Security Management

The information in the following sections describes how to perform security and IPsec management tasks.

Set Internet Explorer Security Options

You need to ensure that your Internet Explorer security settings are configured correctly so that you can download certificates from the server.

Procedure

Step 1 Start Internet Explorer.
Step 2 Navigate to **Tools > Internet Options**.
Step 3 Click **Advanced**.
Step 4 Scroll down to the Security section on the **Advanced** tab.
Step 5 If necessary, clear the **Do not save encrypted pages to disk** check box.
Step 6 Click **OK**.

Certificate Management

The following sections describe the functions you can perform using the Certificate Management menu options.

Display Certificates

Procedure

Step 1 Select **Security > Certificate Management** from the **CiscoUnifiedOS Administration** web page.
The **Certificate List** page appears. For details about the Certificate List page, see Certificate Management.
Step 2 Use the Find controls to filter the certificate list.
Step 3 Click the file name to view details of a certificate or trust store.
The **Certificate Configuration** page displays information about the certificate.
Step 4 Select **Back To Find/List** in the Related Links list to return to the **Certificate List** page then click **Go**.

Download Certificate or CTL to Your Local System

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.

The **Certificate List** page appears. Click the filename of the certificate or CTL.

Step 2 Use the **Find** controls to filter the certificate list.

Step 3 Click the filename of the certificate or CTL.
The **Certificate Configuration** page appears.

Step 4 Click **Download**.

Step 5 In the **File Download** dialog box, click **Save**.

Certificate Deletion or Regeneration

The following sections describe deleting and regenerating a certificate.

Delete Certificate

Caution Deleting a certificate can affect your system operations. Any existing CSR for the certificate that you choose from the Certificate list gets deleted from the system, and you must generate a new CSR. For more information, see Generate Certificate Signing Request, on page 14.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.
The **Certificate List** page appears.

Step 2 Use the Find controls to filter the certificate list.

Step 3 Click the file name of the certificate or CTL.

The **Certificate Configuration** page appears.

Step 4 Click **Delete**.

Regenerate Certificate

Caution Regenerating a certificate can affect your system operations.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.
The **Certificate List** page appears.

Step 2 Click **Generate New**.
The **Generate Certificate** dialog box opens.

Step 3 Choose a certificate name from the Certificate Name list. For a description of the certificate names that display, see the following table.

Table 1: Certificate Names and Descriptions

Name	Description
tomcat	This self-signed root certificate gets generated during installation for the HTTPS server.
ipsec	This self-signed root certificate gets generated during installation for IPsec connections with MGCP and H.323 gateways.

Step 4 Click **Generate New**.

Certificate or Certificate Trust List Uploads

Caution Uploading a new certificate or Certificate Trust List (CTL) file can affect your system operations. After you upload a new tomcat certificate or certificate trust list, you must restart the Cisco Tomcat service by entering the CLI command **utils service restart Cisco Tomcat**.

Note The system does not distribute trust certificates to other cluster servers automatically. If you must have the same certificate on more than one server, you must upload the certificate to each server individually.

The following sections describe how upload a CA root certificate, application certificate, or CTL file to the server.

Upload Certificate or CTL File

Procedure

Step 1 Select **Security > Certificate Management** from the CiscoUnifiedOS Administration web page.
The **Certificate List** page appears.

Step 2 Click **Upload Certificate**.
The Upload Certificate dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 If you are uploading an application certificate that was issued by a third party CA, enter the name of the CA root certificate in the **Root Certificate** text box. If you are uploading a CA root certificate, leave this text box empty.

Step 5 Select the file to upload by doing one of the following steps:

- Enter the path to the file in the **Upload File** text box.
- Click the **Browse** button and navigate to the file, then click **Open**.

Step 6 Click **Upload File** to upload the file to the server.

Upload Trusted Certificate

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.
The **Certificate List** page appears.

Step 2 Click **Upload CTL**.
The **Upload Certificate Trust List** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 If you are uploading an application certificate that was issued by a third-party CA, enter the name of the CA root certificate in the **Root Certificate** text box. If you are uploading a CA root certificate, leave this text box empty.

Step 5 Select the file to upload by doing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse** and navigate to the file, then click **Open**.

Step 6 Click **Upload File** to upload the file to the server.

Use Third-Party CA Certificates

CiscoUnifiedOS supports certificates that a third-party Certificate Authority (CA) issues with PKCS # 10 Certificate Signing Request (CSR). The following procedure outlines this process, with references to additional documentation.

Procedure

Step 1 Generate a CSR on the server.

Step 2 Download the CSR to your PC.

Step 3 Use the CSR to obtain an application certificate from a CA.
Get information about obtaining application certificates from your CA.

Step 4 Obtain the CA root certificate.
Get information about obtaining a root certificate from your CA.

Step 5 Upload the CA root certificate to the server.

Step 6 Upload the application certificate to the server.

Step 7 Restart the services that are affected by the new certificate.
For all certificate types, restart the corresponding service (for example, restart the Tomcat service if you updated the Tomcat certificate). In addition, if you updated the certificate for CAPF or Unified CM, restart the TFTP service.

Related Topics

Generate Certificate Signing Request, on page 14
Download Certificate or CTL to Your Local System , on page 10

Third-Party CA Certificates , on page 14
Certificate or Certificate Trust List Uploads , on page 12
Use Control Center

Generate Certificate Signing Request

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.
The Certificate List page appears.

Step 2 Click **Generate CSR**.
The **Generate Certificate Signing Request** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 Click **Generate CSR**.

Download Certificate Signing Request

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.
The **Certificate Lis**t page appears.

Step 2 Click **Download CSR**.
The **Download Certificate Signing Request** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 Click **Download CSR**.

Step 5 Click **Save** in the File Download dialog box.

Third-Party CA Certificates

To use an application certificate that a third-party CA issue, you must obtain from the CA both the signed application certificate and the CA root certificate. You can get information about obtaining these certificates from your CA. The process varies among CAs.

CAPF and Emergency Responder CSRs include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the Extension Request method, you must enable the X.509 extensions that are listed on the final page of the CSR generation process.

CiscoUnifiedOS generates certificates in DER and PEM encoding formats and generates the CSRs in PEM encoding format. It accepts certificates in DER and DER encoding formats.

Validity of X.509 Certificates

X.509 certificates are only valid until a specific date. Cisco Emergency Responder restricts the upload of certificates that has validity of more than 30 years.

Set Up Certificate Expiration Monitor

The system can automatically send you an e-mail when a certificate is close to its expiration date.

Before you begin

To update information about the C**ertificate Expiration Monitor** page, the Cisco Certificate Expiry Monitor service must be running.

Procedure

Step 1 Select **Security > Certificate Monitor** from the **CiscoUnifiedOS Administration** web page.
The **Certificate Monitor** page appears.

Step 2 Enter the required configuration information. See Table 1 for a description of the Certificate Monitor Expiration fields.

Step 3 Click **Save** to save your changes,.

IPsec Management

The following topics describe how to manage IPsec.

Note IPsec does not get automatically set up between servers in the server group during installation.

Display or Change Existing IPsec Policy

Note Because any changes that you make to an IPsec policy during a system upgrade are lost, do not modify or create IPsec policies during an upgrade.

Caution IPsec, especially with encryption, affects the performance of you system.

Procedure

Step 1 Select **Security > IPsec Configuration** from the **CiscoUnifiedOS Administration** web page.

Caution Any changes that you make to the existing IPsec policies can impact your normal system operations.

The **IPsec Policy Configuration** page appears.

Step 2 Click the **Display Detail** link. The **Association Details** page appears. For an explanation of the fields in this page, see Table 2.

Set Up IPsec Policy

Note Because any changes you make to an IPsec policy during a system upgrade are lost, do not modify or create IPsec policies during an upgrade.

Caution IPsec, especially with encryption, affects the performance of you system.

Procedure

Step 1 Select **Security > IPsec Configuration** from the **CiscoUnifiedOS Administration** web page.
The **IPsec Policy List** page appears.

Step 2 Click **Add New**.
The **IPsec Policy Configuration** page appears.

Step 3 Click **Next**.
The **Setup IPsec Policy and Association** page appears.

Step 4 Enter the appropriate information about the **IPsec Policy Configuration** page. For a description of the fields on this page, see Table 2.

Step 5 Click **Save** to set up the new IPsec policy.

Manage Existing IPsec Policies

To display, enable or disable, or delete an existing IPsec policy, follow this procedure:

Note Because any changes that you make to an IPsec policy during a system upgrade are lost, do not modify or create IPsec policies during an upgrade.

Caution IPsec, especially with encryption, affects the performance of your system.

Caution Any changes that you make to the existing IPsec policies can impact your normal system operations.

Procedure

Step 1 Navigate to **Security > IPsec Configuration**.

Note To access the Security menu items, you must log in to Cisco Unified Communications Operating System Administration again by using your Administrator password.

The IPsec Policy List window displays.

Step 2 Follow these steps to display, enable, or disable a policy :

a) Click the policy name.
The **IPsec Policy Configuration** window displays.
b) To enable or disable the policy, check or uncheck the **Enable Policy** check box.
c) Click **Save**.
d) If you disable the policy, you must run the **utils ipsec restart** command for the disable changes to take effect.

Step 3 Follow these steps to delete one or more policies:

a) Select the check box next to the policies that you want to delete.

Select **Select All** to select all policies or **Clear All** to clear all the check boxes.

b) Click **Delete Selected**.

Software Upgrades

The information in the following sections describes how to perform software upgrades.

Software Upgrade Overview

The Software Upgrade pages enable you to upgrade Emergency Responder software from a DVD (local source) or from a network location (remote source) that the Emergency Responder server can access. The Emergency Responder Publisher must be upgraded first, followed by the Subscriber.

With Emergency Responder 8.6 and later, you cannot install upgrade software on your server while the system continues to operate. A Refresh Upgrade is required for all upgrades from Emergency Responder 8.6 or earlier to the most recent version of Emergency Responder. A Refresh Upgrade is a fresh install on the inactive partition, with embedded data migration. A Refresh Upgrade requires server downtime. This is less critical in a redundant system with both Emergency Responder Publisher and Subscriber.

Before you begin the upgrade, back up your system.

When you install the upgrade software, there will be a temporary server outage while the Emergency Responder software is installed. After you begin the upgrade, using either the command line or graphical user interface, the data will be migrated, and the system will automatically reboot, at which point the server outage begins. The duration of this outage depends on your configuration and amount of data. A notification email is sent at the start and end of Refresh Upgrade.

If an administrator makes changes during the upgrade process such as exporting data, then that data could be lost after upgrade.

The previous software remains in the inactive partition until the next upgrade.

A manual switch back can revert to the old version. If the upgrade fails, the system automatically reverts to the previous version. Your configuration information migrates automatically to the upgraded version in the active partition.

If for any reason you decide to back out of the upgrade, you can restart the system to the inactive partition that contains the older version of the software using the switch-version option.

However, any configuration changes that you made since you upgraded the software will be lost, because the database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching back to the inactive partition.

Supported Upgrades

For supported upgrades, see the Cisco Emergency Responder Release Notes.

If Cisco Emergency Responder is using a secure JTAPI connection, the CTLfile.tlv, JtapiClientKeyStore, and JtapiServerKeyStore files may get deleted post the upgrade. The following alternative options can be used as a workaround:

- Copy the CTLfile.tlv, JtapiClientKeyStore, and JtapiServerKeyStore files from /partB//usr/local/CER/lib to /usr/local/CER/lib location and restart the Cisco Emergency Responder service.

Important You need access to the root account to copy the files.

- Regenerate the CAPF profile on Cisco Unified Communication Manager for the Cisco Emergency application user used for controlling route points and CTI ports.

Upgrade Cisco Unified Operating System

Note You must complete the items mentioned in the procedure before you perform any configuration tasks. You also must not make any configuration changes to Cisco Emergency Responder during an upgrade. Configuration changes include any changes that you make in Emergency Responder Administration or Serviceability pages. Any configuration changes that you make during an upgrade could be lost after the upgrade completes, and some configuration changes can cause the upgrade to fail.

Note Do not perform configuration tasks until the upgrade completes on both Emergency Responder publisher and subscriber until you have:

- switched the servers over to the upgraded partition.
- verified that database replication is functioning.

Procedure

Step 1 Stop all configuration tasks, including all configuration tasks in the various Emergency Responder-related GUIs or the CLI.

Step 2 Apply the required Upgrade Readiness COP Files (pre-upgrade). For example, `ciscocm.cer_preUpgradeCheck-X.k4.cop.sha512`.

Step 3 Upgrade the Emergency Responder publisher.

Note The upgraded system *will not* automatically reboot to the upgraded partition. Instead you are presented with two options: **Reboot to new partition** and **Do not reboot to new partition**. The latter is the default option and is considered the best practice. If you choose to reboot to a new partition, then steps 5 and 6 are not required.

Step 4 Upgrade the Emergency Responder subscriber.

Step 5 Switch over the Emergency Responder publisher to the upgraded partition.

Step 6 Switch over the Emergency Responder subscriber to the upgraded partition.

Step 7 Ensure that database replication is functioning between the Emergency Responder publisher and the Emergency Responder subscriber.

Step 8 Apply the required Upgrade Readiness COP Files (post-upgrade). For example, `ciscocm.cer_postUpgradeCheck-X.k4.cop.sha512`.

Step 9 When all other upgrade tasks are complete, you can perform any needed configuration tasks as required.

Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file by placing an order for Cisco Emergency Responder software. You must also download the appropriate cop file as needed from https://www.cisco.com/.

Note Do not rename the patch file before you install it because the system will not recognize it as a valid file.

Note Do not unzip or untar the upgrade file. If you do, the system cannot read the upgrade files.

You can access the upgrade file during the installation process from either a local DVD or from a remote FTP or SFTP server. Be aware that directory names and filenames that you enter to access the upgrade file are case-sensitive.

Install or Upgrade Software From DVD

You can install software from a DVD that is in the local disk drive and then start the upgrade process.

Note Be sure to back up your system data before starting the software upgrade process. For more information, see Configure Cisco Emergency Responder Disaster Recovery System chapter.

Procedure

Step 1 Order the appropriate upgrade file. You may choose to receive a physical DVD or download an disk image file through electronic software delivery.

Note If you download a disk image file, create the DVD by using the .iso file to burn a DVD. The .iso file contains the complete image of the original DVD disk. You *must not* copy the .iso file to the DVD. You must use your burner software to extract the files that are in the image and burn them on the DVD. This creates an exact replica of the DVD disk.

Step 2 Insert the DVD into the disk drive on the local server that is to be upgraded.

Step 3 From the CiscoUnifiedOS Administration web page, select **Software Upgrades > Install/Upgrade**. The Software Installation/Upgrade page appears.

Step 4 Choose **DVD/CD** from the Source list.

Step 5 Enter the path to the patch file on the DVD in the Directory field.

If the file is in the root directory, enter a slash (/).

Step 6 Click **Next** to continue the upgrade process.

Step 7 Choose the upgrade version that you want to install and click **Next**.

Step 8 On the next page, monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.

Step 9 Choose **Switch to new version after upgrade** to install the upgrade and automatically reboot to the upgraded partition. The system restarts on the upgraded software.

Install Software From Network Drive or Remote Server

Note Do not use your browser controls, such as Refresh/Reload, while accessing Cisco Unified Operating System Administration. Instead, you should use use the navigation controls on the interface.

Before you begin

Be sure to back up your system data before starting the software upgrade process. For more information, see Configure Cisco Emergency Responder Disaster Recovery System chapter.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Software Upgrades > Install/Upgrade**.

The **Software Installation/Upgrade** page appears.

Step 2 Choose **Remote Filesystem** from the **Source** list.

Step 3 Enter the path to the patch file on the remote system in the **Directory** field.

If the upgrade file is on a Linux or UNIX server, you must enter a forward slash at the beginning of the directory path you want to specify. For example, if the upgrade file is in the patches directory, you must enter **`/patches`**.

If the upgrade file is on a Windows server, remember that you are connecting to an FTP or SFTP server so use the appropriate syntax, including:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

Step 4 Enter the server name in the **Server** field.

Step 5 Enter your user name in the **User Name** field.

Step 6 Enter your password in the **User Password** field.

Step 7 Select the transfer protocol from the **Transfer Protocol** field.

Step 8 Click **Next** to continue the upgrade process.

Step 9 Choose the upgrade version that you want to install and click **Next**.

Step 10 On the next page, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

Step 11 When the download completes, verify the checksum value against the checksum for the file you that downloaded that is shown on Cisco.com.

Caution The two checksum values must match to ensure the authenticity and integrity of the upgrade file. If the checksum values do not match, download a fresh version of the file from Cisco.com and try the upgrade again.

Note If you lose your connection with the server or close your browser during the upgrade process, you may see following message when you try to access the **Software Upgrades** menu again:

```
Warning: Another session is installing software, click Assume
      Control to take over the installation.
```

Click **Assume Control** if you are sure you want to take over the session.

If Assume Control is not displayed, you can also monitor the upgrade with the Real Time Monitoring Tool.

Step 12 Choose **Reboot to upgraded partition** to install the upgrade and automatically reboot to the upgraded partition. The system restarts and runs the upgraded software.

Step 13 To install the upgrade and then manually reboot to the upgraded partition at a later time, do the following steps:

a) Choose **Do not reboot after upgrade**.
b) Click **Next**.
The **Upgrade Status** window displays the **Upgrade log**.
c) Click **Finish** when the installation completes, .

d) Choose **Settings** > **Version** to restart the system and activate the upgrade, then click **Switch Version**. The system restarts running the upgraded software.

Troubleshoot Stalled Upgrades

During a software upgrade, the software installation may stall. Check the upgrade log for new messages. If the upgrade log does not have any new log messages, then the installation may have stalled.

You must cancel the upgrade, disable I/O throttling, and restart the upgrade procedure. When you successfully complete the upgrade, you do not need to enable I/O throttling again.

- To disable I/O throttling, enter the CLI command **utils iothrottle disable**.
- To display the status of I/O throttling, enter the CLI command **utils iothrottle status**.
- To enable I/O throttling, enter the CLI command **utils iothrottle enable**. By default, I/O throttle remains enabled.

If the system does not respond to the cancellation, you must reboot the server, disable I/O throttling, and restart the upgrade process procedure.

If the software upgrade shows stalled at /partb rpm deletion in the logs, then stop the rpm -e process using the root to proceed further.

```
[root@<Hostname>]# ps -eaf | grep rpm

root      4925  4913  0 18:21 ?        00:00:00 rpm -e --nodeps master

root      7264     1  0 14:02 ?        00:00:00 /usr/local/os-services/sbin/arpmond

root     24359 24188  0 18:37 pts/3    00:00:00 grep
[root@<Hostname>]# kill -9 4925

[root@<Hostname>]# ps -eaf | grep rpm

root      7264     1  0 14:02 ?        00:00:00 /usr/local/os-services/sbin/arpmond

root     24652 24188  0 18:37 pts/3    00:00:00 grep rpm
```

What to do next

If the software upgrade continues to stall, then contact Cisco TAC for assistance.

Revert to Previous Version

After upgrading, you can revert to the software version that was running before the upgrade, by restarting your system and switching to the software version on the inactive partition.

Procedure

Step 1 Revert the publisher node.

For more information, see Revert Publisher Server to Previous Version , on page 23.

Step 2 Revert all backup subscriber nodes.

For more information, see Revert Subscriber Server to Previous Version , on page 23.

Revert Publisher Server to Previous Version

Procedure

Step 1 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

https://"server-name"/**cmplatform**

Server-name is the host name or IP address of the Emergency Responder server.

Step 2 Enter your Administrator username and password.

Step 3 Choose **Settings>Version**.
The Version Settings window displays.

Step 4 Click **Switch Versions**.

After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 5 Verify that the version switch was successful:

a) Log into Open Cisco Unified Communications Operating System Administration again.
b) Choose **Settings>Version**.
The **Version Settings** window displays.
c) Verify that the correct product version is now running on the active partition.
d) Verify that all activated services are running.
e) Log into Emergency Responder by entering the following URL and entering your user name and password:

https://"server-name"**/ccmadmin**

f) Verify that you can log in and that your configuration data exists.

Revert Subscriber Server to Previous Version

Procedure

Step 1 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

https://"server-name"/**cmplatform**

"server-name" is the host name or IP address of the Emergency Responder server.

Step 2 Enter your Administrator user name and password.

Step 3 Choose **Settings>Version**.
The Version Settings window displays.

Step 4 Click **Switch Versions**.

After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 5 Verify that the version switch was successful:

a) Log into Open Cisco Unified Communications Operating System Administration again.
b) Choose **Settings>Version**.
The Version Settings window displays.
c) Verify that the correct product version is now running on the active partition.
d) Verify that all activated services are running.

Upload Customized Logon Message

You can upload a text file that contains a customized logon message that appears in Cisco Unified Communications Operating System Administration, Unified CM Administration, and the CLI.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades > Customized Logon Message**.

The Customized Logon Message window displays.

Step 2 Click **Browse** to choose the text file that you want to upload.

Step 3 Click **Upload File**.

Note You cannot upload a file that is larger than 10 KB.

The system displays the customized logon message.

Step 4 Click **Delete** to revert to the default logon message.

Your customized logon message is deleted, and the system displays the default logon message.

Cisco Unified OS Services

The following sections describe how to use CiscoUnifiedOS services.

Ping Another System

The Ping Configuration page enables you to send ping requests to test if other systems are reachable over the network.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Services > Ping**.

The **Ping Configuration** page appears. For details about the **Ping Configuration** page, see Ping Configuration.

Step 2 Enter the IP address or network name for the system that you want to ping.

Step 3 Enter the ping interval in seconds.

Step 4 Enter the packet size.

Step 5 Enter the ping count, which is the number of times that you want to ping the system.

Note When you specify multiple pings, the **ping** command does not display the ping date and time in real time. The **ping** command displays the date and time once the ping count is completed.

Step 6 Choose if you want to validate IPsec or not.

Step 7 Click **Ping**.

The **Ping Results** text box displays the ping statistics.

Set Up Remote Support

From the **Remote Support** page, you can set up a remote account that Cisco support personnel can use to access the Emergency Responder system for a specified period of time.

1. The customer sets up a remote support account. This account includes a configurable time limit on how long Cisco personnel can access it.
2. When the remote support account is set up, a pass phrase gets generated.
3. The customer calls Cisco support and provides the remote support account name and pass phrase.
4. Cisco support enters the pass phrase into a decoder program that generates a password from the pass phrase.
5. Cisco support logs into the remote support account on the customer system by using the decoded password.
6. When the account time limit expires, Cisco support can no longer access the remote support account.

To set up remote support, follow these steps:

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Services > Remote Support**.
The **Remote Access Configuration** page appears.

Step 2 If no remote support account is configured, click **Add**.

Step 3 Enter an account name for the remote account and the account life in days.

Note Ensure the account name at least six-characters long and all lowercase, alphabetic characters.

Step 4 Click **Save**.
The **Remote Access Configuration** page redisplays. For descriptions of fields on the **Remote Access Configuration** page, see Table 2.

Step 5 To access the system by using the generated pass phrase, contact your Cisco TAC.