



CHAPTER 7

Configuring the Cisco Unified Operating System for Cisco Emergency Responder 2.0

The following topics describe how to configure and use the Cisco Unified Communications Operating System, which is bundled with Cisco Emergency Responder 2.0:

- [Displaying Cisco Unified OS Information, page 7-1](#)
- [Displaying and Modifying Cisco Unified OS Settings, page 7-3](#)
- [Restarting, Shutting Down, or Switching Software Versions, page 7-5](#)
- [Managing Security, page 7-6](#)
- [Performing Software Upgrades, page 7-13](#)
- [Using Cisco Unified OS Services, page 7-16](#)

Displaying Cisco Unified OS Information

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

- [Viewing ServerGroup Information, page 7-1](#)
- [Viewing Hardware Status, page 7-2](#)
- [Viewing Network Status, page 7-2](#)
- [Viewing Installed Software, page 7-2](#)
- [Viewing System Status, page 7-3](#)

Viewing ServerGroup Information

To view cluster information, follow these steps:

Procedure

-
- Step 1** From the main Cisco Unified OS Administration web page, select **Show>ServerGroup**. The ServerGroup page appears.

- Step 2** For descriptions of the fields on the ServerGroup page, see [Table C-1 on page C-2](#).
-

Viewing Hardware Status

To view the hardware status, follow these steps:

Procedure

- Step 1** From the main Cisco Unified OS 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 C-2 on page C-2](#).
-

Viewing 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.

To view the network status, follow these steps:

Procedure

- Step 1** From the Cisco Unified OS Administration web page, select **Show > Network**.
The Network Settings page appears.
- Step 2** See [Table C-3 on page C-3](#) for descriptions of the fields on the Network Settings page.
-

Viewing Installed Software

To view the software versions and installed software options, follow these steps:

Procedure

- Step 1** From the Cisco Unified OS 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 C-4 on page C-4](#).
-

Viewing System Status

To view the system status, follow these steps:

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Show > System**.
The System Status page appears.
- Step 2** See [Table C-5 on page C-4](#) for descriptions of the fields on the System Status page.
-

Displaying and Modifying Cisco Unified OS Settings

Use the Settings options to display and modifying IP settings, host settings, and Network Time Protocol (NTP) settings. These topics describe how to display and modify Cisco Unified OS settings:

- [Configuring Ethernet Settings, page 7-3](#)
- [Configuring NTP Servers, page 7-4](#)
- [Configuring SMTP Settings, page 7-5](#)
- [Configuring Time Settings, page 7-5](#)
- [Restarting, Shutting Down, or Switching Software Versions, page 7-5](#)

Configuring 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's 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.

To view or change the Ethernet settings, follow these steps:

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Settings > IP > Ethernet**.
The Ethernet Configuration page appears.
- Step 2** To modify the Ethernet settings, enter the new values in the appropriate fields. For a description of the fields on the Ethernet Configuration page, see [Table C-6 on page C-5](#).



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

Step 3 To preserve your changes, click **Save**.

Configuring 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 Cisco Unified OS Administration web page, select **Settings>NTP Servers**.
The NTP Server List page appears. For details on the NTP Server List page, see the [“NTP Server List” section on page C-6](#).
- 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.

Configuring SMTP Settings

To configure the SMTP host settings, follow these steps:

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Settings>SMTP**.
The SMTP Settings page appears. For details on the SMTP Settings page, see the [“SMTP Settings” section on page C-7](#).
- Step 2** Enter the hostname or IP address of the SMTP host.
- Step 3** Click **Save**.
-

Configuring Time Settings

To manually configure the time, follow these steps:



Note

Before you can manually configure the server time, you must delete any NTP servers that you have configured. See the [“Configuring NTP Servers” section on page 7-4](#) for information about deleting NTP servers.

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Settings>Time**. The Time Settings page appears. For details on the Time Settings page, see the [“Time Settings” section on page C-8](#).
- Step 2** Enter the date and time for the system.
- Step 3** Click **Save**.
-

Restarting, Shutting Down, or Switching Software Versions

To restart, shutdown, or switch Cisco ER software versions, follow these steps:

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Settings>Version**. The Version Settings page appears. For details on the Version Settings page, see the [“Version Settings” section on page C-8](#).
- Step 2** To restart the version running on the active partition, click **Restart**.



Caution

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

- Step 3** To shut down the system, click **Shutdown**.



Note The hardware does not power down automatically.



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

Step 4 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, click **Switch Versions**.



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 need to fall back to an earlier software version.

Managing Security

These topics describe how to perform security and IPSec management tasks:

- [Set Internet Explorer Security Options, page 7-6](#)
- [Managing Certificates and Certificate Trust Lists, page 7-7](#)
- [Managing IPSec, page 7-12](#)

Set Internet Explorer Security Options

To ensure that your Internet Explorer security settings are configured correctly so that you can download certificates from the server, follow these steps:

Procedure

- Step 1** Start Internet Explorer.
- Step 2** Navigate to **Tools>Internet Options**.
- Step 3** Click the **Advanced** tab.
- 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**.
-

Managing Certificates and Certificate Trust Lists

The following topics describe the functions you can perform using the Certificate Management menu options:

- [Displaying Certificates](#), page 7-7
- [Downloading a Certificate or CTL](#), page 7-7
- [Deleting and Regenerating a Certificate](#), page 7-8
- [Uploading a Certificate or Certificate Trust List](#), page 7-9
- [Using Third Party CA Certificates](#), page 7-10
- [Downloading a Certificate Signing Request](#), page 7-11
- [Monitoring Certificate Expiration Dates](#), page 7-11

Displaying Certificates

To display existing certificates, follow these steps:

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Security > Certificate Management**. The Certificate List page appears. For details on the Certificate List page, see the [“Certificate List” section on page C-9](#).
- Step 2** Use the Find controls to filter the certificate list.
- Step 3** To view details of a certificate or trust store, click the file name. The Certificate Configuration page displays information about the certificate.
- Step 4** To return to the Certificate List page, select Back To Find/List in the Related Links list, then click **Go**.
-

Downloading a Certificate or CTL

To download a certificate or CTL from Cisco ER to your local system, follow these steps:

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Security > Certificate Management**. The Certificate List page appears. Click the file name of the certificate or CTL.
- 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 **Download**.
- Step 5** In the File Download dialog box, click **Save**.
-

Deleting and Regenerating a Certificate

These sections describe deleting and regenerating a certificate:

- [Deleting a Certificate, page 7-8](#)
- [Regenerating a Certificate, page 7-8](#)

Deleting a Certificate

To delete a trusted certificate, follow these steps:

**Caution**

Deleting a certificate can affect your system operations.

Procedure

-
- Step 1** From the Cisco Unified OS 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**.
-

Regenerating a Certificate

To regenerate a certificate, follow these steps:

**Caution**

Regenerating a certificate can affect your system operations.

Procedure

-
- Step 1** From the Cisco Unified OS 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.
- Step 4** Click **Generate New**.
-

Uploading a Certificate or Certificate Trust List

**Caution**

Uploading a new certificate or certificate trust list (CTL) file can affect your system operations.

**Note**

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

These sections describe how to upload a CA root certificate, application certificate, or CTL file to the server:

- [Upload a Certificate, page 7-9](#)
- [Upload a Trusted Certificate, page 7-9](#)

Upload a Certificate

To upload a CA root certificate, application certificate, or CTL file to the server, follow these steps:

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Security > Certificate Management**.
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:
- In the **Upload File** text box, enter the path to the file.
 - Click the **Browse** button and navigate to the file; then, click **Open**.
- Step 6** To upload the file to the server, click the **Upload File** button.
-

Upload a Trusted Certificate

To upload a trusted certificate, follow these steps:

Procedure

-
- Step 1** From the Cisco Unified OS 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 the **Browse** button and navigate to the file; then, click **Open**.
- Step 6** To upload the file to the server, click the **Upload File** button.

Using Third Party CA Certificates

Cisco Unified OS supports certificates that a third party Certificate Authority (CA) issues with PKCS # 10 Certificate Signing Request (CSR). The following table provides an overview of this process, with references to additional documentation:

	Task	For More Information
Step 1	Generate a CSR on the server.	See the “Generating a Certificate Signing Request” section on page 7-10.
Step 2	Download the CSR to your PC.	See the “Downloading a Certificate Signing Request” section on page 7-11.
Step 3	Use the CSR to obtain an application certificate from a CA.	Get information about obtaining application certificates from your CA. See “Obtaining Third-Party CA Certificates” section on page 7-11 for additional notes.
Step 4	Obtain the CA root certificate.	Get information about obtaining a root certificate from your CA. See “Obtaining Third-Party CA Certificates” section on page 7-11 for additional notes.
Step 5	Upload the CA root certificate to the server.	See the “Uploading a Certificate or Certificate Trust List” section on page 7-9.
Step 6	Upload the application certificate to the server.	See the “Uploading a Certificate or Certificate Trust List” section on page 7-9.
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 Cisco Unified CM, restart the TFTP service. For information about restarting services, see the “Using the Control Center” section on page 6-1.

Generating a Certificate Signing Request

To generate a Certificate Signing Request (CSR), follow these steps:

Procedure

- Step 1** From the Cisco Unified OS 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**.
-

Downloading a Certificate Signing Request

To download a Certificate Signing Request, follow these steps:

Procedure

- Step 1** From the Cisco Unified OS Administration web page, select **Security > Certificate Management**.
The Download Certificate Signing Request 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** In the File Download dialog box, click **Save**.
-

Obtaining Third-Party CA Certificates

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

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

Cisco Unified OS generates certificates in DER and PEM encoding formats and generates CSRs in PEM encoding format. It accepts certificates in DER and DER encoding formats.

Cisco has verified third-party certificates that were obtained from Microsoft, Keon, and Verisign CAs. Certificates from other CAs might work but have not been verified.

Monitoring Certificate Expiration Dates

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

To view and configure the Certificate Expiration Monitor, follow these steps:



Note

In order to update information on the Certificate Expiration Monitor page, the Cisco Certificate Expiry Monitor service must be running.

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Security > Certificate Management**.
The Certificate Monitor page appears.
- Step 2** Enter the required configuration information. See [Table C-19 on page C-13](#) for a description of the Certificate Monitor Expiration fields.
- Step 3** To save your changes, click **Save**.
-

Managing IPSec

These topics describe how to manage IPSec:

- [Displaying or Changing an Existing IPSec Policy, page 7-12](#)
- [Setting Up a New IPSec Policy, page 7-13](#)

**Note**

IPSec does not get automatically set up between nodes in the cluster during installation.

Displaying or Changing an Existing IPSec Policy

To display or change an existing IPSec policy, follow these steps:

**Note**

Because any changes that you make to an IPSec policy during a system upgrade will get lost, do not modify or create IPSec policies during an upgrade.

**Caution**

IPSec, especially with encryption, will affect the performance of you system.

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Security > IPSEC Configuration**.
The IPSEC Policy Configuration page appears.

**Caution**

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

- Step 2** Click the Display Detail link. The Association Details page appears. For an explanation of the fields in this page, see [Table C-21 on page C-14](#).
-

Setting Up a New IPSec Policy

To set up a new IPSec policy and association, follow these steps:

**Note**

Because any changes you make to an IPSec policy during a system upgrade will get lost, do not modify or create IPSec policies during an upgrade.

**Caution**

IPSec, especially with encryption, will affect the performance of you system.

Procedure

- Step 1** From the Cisco Unified OS Administration web page, select **Security > IPSEC Management**.
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 on the IPSEC Policy Configuration page. For a description of the fields on this page, see [Table C-21 on page C-14](#).
- Step 5** To set up the new IPSec policy, click **Save**.

Performing Software Upgrades

This topic describes how to perform software upgrades:

- [Upgrading and Installing Software, page 7-13](#)

Upgrading and Installing Software

The Software Upgrade pages enable you to upgrade Cisco ER software from either a local or a remote source.

The software upgrade process also enables you to back out of an upgrade if problems occur. You install the software for the upgrade on the system's inactive partition and perform a restart to switch the system to the newer version of the software. During this process, the upgraded software becomes the active partition, and your current software becomes the inactive partition. 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. However, any configuration changes that you made since upgrading the software will be lost.

**Note**

When upgrading from Cisco ER 2.0 to a later version, the Publisher must be upgraded first, followed by the Subscriber.

Installing and Upgrading Software From a Local Source

You can install software from a DVD that is located in the local disc 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 the [“Configuring the Cisco Emergency Responder 2.0 Disaster Recovery System”](#) chapter.

To install or upgrade software from a DVD, follow these steps:

Procedure

Step 1 If you plan to download the upgrade file, create a DVD by performing these steps:

- a. Download the appropriate upgrade file from Cisco.com.

**Note**

Do not unzip or untar the file. If you do, the system may not be able to read the upgrade files.

- b. Copy the upgrade file to a writable DVD.

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

Step 3 From the Cisco Unified OS 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 To continue the upgrade process, click **Next**.

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 getting transferred.

Step 9 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.

Step 10 Choose whether you want the system to automatically reboot to the upgraded partition after installing the upgrade software:

- To install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**.

- To install the upgrade and then manually reboot to the upgraded partition at a later time, choose **Do not reboot after upgrade**.

Step 11 Click **Upgrade**.

The Upgrade Status page appears the Upgrade log.

Step 12 When the installation completes, click **Install Another**.

Step 13 To restart the system and activate the upgrade, choose **Settings>Versions**, then click **Restart**.

The system restarts running the upgraded software.

Installing and Upgrading Software From a Remote Source

To install software from a network drive or remote server, follow these steps:



Note

Be sure to back up your system data before starting the software upgrade process. For more information, see the [“Configuring the Cisco Emergency Responder 2.0 Disaster Recovery System”](#) chapter.

Procedure

Step 1 From the Cisco Unified OS 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 located 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 located on a Windows server, check with your system administrator for the correct directory path.

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 To continue the upgrade process, click **Next**.

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.

- Step 12** Choose whether you want the system to automatically reboot to the upgraded partition after installing the upgrade software:
- To install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**.
 - To install the upgrade and then manually reboot to the upgraded partition at a later time, choose **Do not reboot after upgrade**.
- Step 13** Click **Next**.
The Upgrade Status page displays the Upgrade log.
- Step 14** When the installation completes, click **Install Another**.
- Step 15** To restart the system and activate the upgrade, choose **Settings > Versions**, then click **Restart**.
The system restarts running the upgraded software.
-

Using Cisco Unified OS Services

These topics describe how to use Cisco Unified OS services:

- [Using the Ping Utility, page 7-16](#)
- [Setting Up Remote Support, page 7-17](#)

Using the Ping Utility

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

To ping another system, follow these steps:

Procedure

-
- Step 1** From the Cisco Unified OS Administration web page, select **Services > Ping**.
The Ping Configuration page appears. For details on the Ping Configuration page, see the [“Ping Configuration” section on page C-16](#).
- 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, 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. Be aware that the **ping** command displays the data after the number of pings that you specified complete.

- Step 6** Choose whether you want to validate IPsec.

Step 7 Click **Ping**.

The Ping Results text box displays the ping statistics.

Setting Up Remote Support

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

The remote support process works as follows:

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 Cisco Unified OS 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 redisplay. For descriptions of fields on the Remote Access Configuration page, see [Table C-25 on page C-18](#).

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