Cisco Unified Operating System Administration Web Interface

ServerGroup

The ServerGroup page appears when you choose **Show > ServerGroup**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the ServerGroup page to view information about the Emergency Responder servers in the server group.

The following table describes the ServerGroup page.

Table 1: ServerGroup Page

Field	Description
ServerGroup	
Hostname	Displays the name of the host.
IP Address	Displays the IP address of the host.
Alias	Displays the alias of the host
Type of Node	Displays the node type of the host.
Database Replication	Displays the name of the database which will either be a Publisher or Subscriber.

Related Topics

View Hardware Status

Hardware Status

The Hardware Status page appears when you choose **Show > Hardware**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Hardware Status page to view information about the Emergency Responder hardware.

The following table describes the Hardware Status page.

Table 2: Hardware Status Page

Field	Description
Hardware Resources	
Platform Type	Model identity of the platform server
Serial Number	Displays serial number of the virtual machine.

Field	Description
Virtual Hardware	Shows you the status as “Configured” if the hardware is a virtual machine.
Virtual Support	Shows you the status as “Supported” if the support is on a virtual machine.
Processor Speed	Speed of the processor
CPU Type	Type of processor in the platform server
Memory	Total amount of memory in Mbytes
Object ID	Object ID of the platform server
OS Version	Operating system version running on the platform server
RAID Details	Detailed summary of the platform hardware

Related Topics

View Hardware Status

Network Configuration

The Network Configuration page appears when you choose **Show > Network**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Network Configuration page to view information about the network settings.

Note The network status information that displays 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 displays for the network ports Ethernet 0, Ethernet 1, and Bond 0. If Network Fault Tolerance is not enabled, status information displays only for Ethernet 0.

The following table describes the Network Configuration page.

Table 3: Network Configuration Page

Field	Description
Ethernet Details	

Field	Description
DHCP Status	Indicates whether DHCP is enabled for Ethernet port 0.
Status	Indicates whether the port is Up or Down for Ethernet ports 0 and 1.
IP Address	Shows the IP address of Ethernet port 0 (and Ethernet port 1 if Network Fault Tolerance (NFT) is enabled).
IP Mask	Shows the IP mask of Ethernet port 0 (and Ethernet port 1 if NFT is enabled).
Link Detected	Indicates whether there is an active link.
Queue Length	Displays the length of the queue.
MTU	Displays the maximum transmission unit.
MAC Address	Displays the hardware address of the port.
RX Stats	Displays information about received bytes and packets.
TX Stats	Displays information about transmitted bytes and packets.
DNS Details	
Primary DNS	Displays the IP address of the primary domain name server.
Secondary DNS	Displays the IP address of the secondary domain name server.
Options	Displays the number of attempts and timeouts.
Domain	Displays the domain of the server.
Gateway	Displays the IP address of the network gateway on Ethernet port 0.

Related Topics

View Network Status

Software Packages

The Software Packages page appears when you choose **Show > Software**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Software Packages page to view the software versions and installed software options.

The following table describes the Software Packages page.

Table 4: Software Packages Page

Field	Description
Partition Versions	Displays the software version that is running on the active and inactive partitions.
Active Version Installed Software Options	Displays the versions of installed software options that are installed on the active version.
Inactive Version Installed Software Options	Displays the versions of installed software options that are installed on the inactive version.
Installed Software Options	Displays the cop file installed on the system.

Related Topics

View Installed Software

System Status

The System Status page appears when you choose **Show > System**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the System Status page to view the status of the Emergency Responder system.

The following table describes the System Status page.

Table 5: System Status Page

Field	Description
Host Name	Name of the Cisco UCS host where the Emergency Responder system is installed.
Date	Date and time based on the continent and region that were specified during operating system installation.
Time Zone	Time zone that was chosen during installation.
Locale	Locale of the system.
Product Version	Operating system version.

Field	Description
Uptime	Displays system uptime information.
CPU	Displays the percentage of CPU capacity that is idle, the percentage that is running system processes, and the percentage that is running user processes.
Memory	Displays information about memory usage, including the amount of total memory, free memory, and used memory in kilobytes.
Disk/active	Displays the amount of total, free, and used disk space on the active disk.
Disk/inactive	Displays the amount of total, free, and used disk space on the inactive disk.
Disk/logging	Displays the amount of total, free, and disk space that is used for disk logging.

Related Topics

View System Status

IP Preferences

The IP Preferences page appears when you choose **Show > IP Preferences**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the IP Preferences page to view a list of registered ports that can be used by the system. The following table describes the IP Preferences page.

Table 6: IP Preferences Page

Field	Description
Application	Name of the application using (listening on) the port.
Protocol	Protocol used on this port (TCP, UDP, and so on).
Port Number	Numeric port number.

Field	Description
Type	Type of traffic allowed on this port: • Public—All traffic allowed. • Translated—All traffic allowed but forwarded to a different port. • Private—Traffic only allowed from a defined set of remote servers, for example, other servers in the server group.
Translated Port	Traffic destined for this port get forwarded to the port listed in the Port Number column. This field applies to Translated type ports only.
Status	Status of port usage: • Enabled—In use by the application and opened by the firewall. • Disabled—Blocked by the firewall and not in use.
Description	Brief description of how the port is used.

Related Topics

View IP Preferences

Ethernet Configuration

The Ethernet Configuration page appears when you choose **Settings > IP > Ethernet**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Ethernet Configuration page to view or change Ethernet settings.

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.

The following table describes the Ethernet Configuration page.

Table 7: Ethernet Configuration Page

Field	Description
DHCP Information	

Field	Description
DHCP	Indicates whether DHCP is enabled or disabled and allows you to change the DHCP setting using the pull-down menu.
Host Information	
Hostname	Displays the server name (Display only—Cannot configure).
Port Information	
IP Address	Displays the IP address of the system. You can change the IP address by entering a new IP address in the text box.
Subnet Mask	Displays the IP subnet mask address. You can change the mask by entering a new subnet mask in the text box.
Gateway Information	
Default Gateway	Displays the IP address of the default network gateway. You can change the gateway IP address by entering a new IP address in the text box.
Save button or icon	Saves any changes made to the Ethernet Configuration page. **Caution** If you click **Save**, the machine reboots. Do not click **Save** unless you want to shut down and reboot your system. **Note** To recognize any new IP addresses, both servers in the server group must be manually rebooted.

Related Topics

Set Up Ethernet Settings

Ethernet IPv6 Configuration

Use the **Settings** > **IP** > **Enternet IPv6** menu to enable and configure IPv6 on the node.

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.

Table 8: Ethernet IPv6 Configuration Page

Field	Description
Enable IPv6	Check this check box to enable IPv6 on the node.
Router Advertisement	Choose one of the following IP address sources: • Router Advertisement • DHCP • Manual Entry The three IP address sources are mutually exclusive. **Note** Unless you specify Manual Entry, IPv6 Address, Prefix Length, and Default Gateway fields remain read only.
IPv6 Address	If you chose Manual Entry, enter the IPv6 address of the node. For example, fd6:2:6:96:21e:bff:fecc:2e3a.
Prefix Length	If you chose Manual Entry, enter the prefix length. For example, 64.
Default Gateway	If you chose Manual Entry, enter the default gateway. For example, fe80::3ece:73ff:fea9:c641.
Update with Reboot	If you want the system to reboot immediately after you click Save, check this check box. If you want to reboot later, leave the check box blank. **Note** If you check the Update with Reboot check box, the system reboots after you click Save. For the IPv6 settings to take effect, reboot the system.

Publisher Settings

The Publisher Settings page appears when you choose **Settings > IP > Publisher.**

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Publisher Settings page to view or change the Publisher hostname or IP address.

Note You can only view and change the publisher hostname IP address only on the Emergency Responder Subscriber, not on the Emergency Responder publisher itself. Changing these fields must be followed by an immediate reboot of the Subscriber.

Table 9: Publisher Settings Page

Field	Description
Hostname	Displays the hostnames of the Emergency Responder Publisher for this Subscriber. To change the hostname, enter the new hostname in the text box, and click **Save**.
IP Address	Displays the IP address of the Emergency Responder Publisher for this Subscriber. To change the IP address, enter the IP address in the text box, and click **Save**.
Save button or icon	Saves the information in the Publisher Configuration Settings page.

Related Topics

Change IP Addresses for Emergency Responder Servers

NTP Server List

The NTP Server List page appears when you choose **Settings > NTP Servers**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the NTP Server List page to add, modify, or delete an NTP server. You can only configure the NTP server settings on the Publisher.

Note Ensure that the external NTP server is stratum 9 or higher (1 to 9).

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.

Caution If you add, modify, or delete an NTP server, you must reboot both the Publisher and the Subscriber.

The following table describes the NTP Server List page.

Table 10: NTP Server List Page

Field	Description
Status	Displays how many configured NTP server were found.
NTP Server	
Hostname or IP Address field	Displays the hostnames or IP addresses of the configured NTP servers. To change a hostname or IP address, click it, enter the new hostname or IP address, and click **Save**.
Add New button or icon	Adds a new NTP server. After you click **Add New**, enter the hostname of IP address of the new NTP server and click **Save**.
Select All button or icon	Selects all NTP servers listed. When you click this button or icon, a check mark appears in the boxes to the left of each NTP hostname or IP address and to the left of the Hostname or IP Address column heading. **Note** The Select All button or icon is only visible if you have previously configured one or more NTP servers.
Clear All button or icon	Deselects all NTP servers listed. When you click this button or icon, all check marks disappear. **Note** The Clear All button or icon is only visible if you have previously configured one or more NTP servers.
Delete Selected button or icon	Deletes the selected NTP server. To delete an NTP server, you must first select it from the list of NTP servers. Click the box to the left of the NTP server name to select it. To select all listed NTP servers, click the box to the left of the Hostname or IP Address column heading or click **Select All**. **Note** The Delete Selected button or icon is only visible if you have previously configured one or more NTP servers.

The following table describes the NTP Server Configuration page.

Table 11: NTP Server Configuration Page

Field	Description
Status	Displays how many configured NTP server were found.
NTP Server Settings	
Hostname or IP Address field	Displays the hostnames or IP addresses of the configured NTP servers. To change a hostname or IP address, click it, enter the new hostname or IP address, and click **Save**.
Save button or icon	Saves the information about the new NTP server.

Related Topics

Set Up NTP Servers

SMTP Settings

The SMTP Settings page appears when you choose **Settings > SMTP**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the SMTP Settings page to manually configure the SMTP host.

The following table describes the SMTP Settings page.

Table 12: SMTP Settings Page

Field	Description
Status	Displays the status of the SMTP Settings page.
SMTP Host	
Hostname or IP Address	Enter the hostname or IP address of the SMTP server in the text box.
Host Status	Displays the status of the SMTP host server.
Save button or icon	Saves changes made to the SMTP Settings page.

Related Topics

Set Up SNMPv2

Time Settings

The Time Settings page appears when you choose **Settings > Time**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Time Settings page to manually configure the server time.

Note Before you can manually configure the server time, you must delete any NTP servers that you have configured. See NTP Server List, on page 10 for more information.

Caution If you change the server time, you must reboot both the Publisher and the Subscriber.

The following table describes the Time Settings page.

Table 13: Time Settings Page

Field	Description
Date	Allows you to set the month, day, year, hours, minutes, and seconds using the pull-down menus.
Save button or icon	Saves changes made to the Time Settings page.

Related Topics

NTP Server List, on page 10
Set Up NTP Servers
Set Up Time Settings

Version Settings

The Version Settings page appears when you choose **Settings > Version**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Version Settings page to restart or shutdown the system and to switch software versions.

Note You must have a different software version installed on the inactive partition to switch versions.

Caution Initiating this action causes the system to restart and become temporarily unavailable.

The following table describes the Version Settings page.

Table 14: Version Settings Page

Field	Description
Status	Displays the current status.
Installed Versions	
Active Version	Displays the version running on the active partition.
Inactive Version	Display the version on the inactive partition.
Restart button or icon	Restarts the system.
Shutdown button or icon	Shuts down the system.
Switch Versions button or icon	Actives the software version on the inactive partition. **Note** The Switch Versions button or icon is only visible if there is a software version installed on the inactive partition.

Related Topics

Manage Software Versions

Certificate List

The Certificate List page appears when you choose **Security > Certificate Management**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Certificate List page to do the following:

- Search for existing certificates
- Generate a new certificates
- Upload a certificate

- Upload a CTL
- Generate a CSR

The following table describes the Certificate List page.

Table 15: Certificate List Page

Field	Description
Status	Displays the current status.
Certificate List	
Find certificate list where	Enter search criteria for the certificate lists you want to find. To find all certificate lists by file name, select File Name from the pull-down menu and click **Find** without entering any criteria. To find all certificate lists by certificate name, select Certificate Name from the pull-down menu and click **Find** without entering any criteria. To narrow your search: • Select the search relationship (begins with, contains, and so on) from the pull-down menu, and enter the search string in the text box. • To search on a combination of fields, click the **Plus** icon **(+)** to add additional search parameters. Click the **Minus** icon (–) to remove search parameters. Click **Clear Filter** to remove all additional search parameters. • Use the Rows per Page pull-down menu to select how many rows are displayed per page. When you have entered all of the search parameters, click **Find**. If the search finds existing certificates, the information about the certificates (File Name, Certificate Name, and Certificate Type) displays in the Certificate List. Click the File Name link to display the Certificate Configuration page. See Table 21: Certificate Configuration Page , on page 18 for information about the Certificate Configuration Page.
Generate New button or icon	Allows you to generate a new certificate. When you click **Generate New**, the Generate Certificate page appears. See Table 16: Generate Certificate Page , on page 16 for a description of the Generate Certificate page.

Cisco Unified Operating System Administration Web Interface

Field	Description
Upload Certificate button or icon	Allows you to upload a certificate from a remote server. When you click **Upload Certificate**, the Upload Certificate page appears. See Table 17: Upload Certificate Page , on page 17 for a description of the Upload Certificate page.
Upload CTL button or icon	Allows you to upload a Certificate Trust List (CTL) from a remote server. When you click **Upload CTL**, the Upload Certificate Trust List page appears. See Table 18: Upload CTL Page , on page 17 for a description of the Upload Certificate Trust List page.
Generate CSR button or icon	Allows you to generate a new Certificate Signing Request (CSR). When you click **Generate CSR**, the Generate Certificate Signing Request page appears. See Table 19: Generate CSR Page , on page 17 for a description of the Generate New page.
Download CSR button or icon	Allows you to download a CSR. When you click **Download CSR**, the Download Certificate Signing Request page appears. See Table 20: Download CSR Page , on page 18 for a description of the Download Certificate Signing Request page.

The following table describes the Generate Certificate page.

Table 16: Generate Certificate Page

Field	Description
Status	Displays the current status of the Generate Certificate page.
Generate Certificate	
Certificate Name	Allows you to choose a certificate name from the pull-down menu.
Key Length	Allows you to choose 1024 or 2048 from the drop-down list.
Hash Algorithm	Allows you to choose SHA1 or SHA256 from the drop-down list.
Generate New button or icon	Generates a new certificate. You must first select a Certificate Name from the pull-down menu.
Close button or icon	Closes the Generate Certificate page.

The following table describes the Upload Certificate page.

Table 17: Upload Certificate Page

Field	Description
Status	Displays the current status of the Upload Certificate page.
Upload Certificate	
Certificate Name	Use the pull-down menu to select the name of the certificate to upload.
Root Certificate	Enter the name of the root certificate.
Upload File	Use the Browse button to select the file to be uploaded.
Upload File button or icon	Uploads the certificate file specified in the Upload Certificate section.
Close button or icon	Closes the Update Certificate page.

The following table describes the Upload CTL page.

Table 18: Upload CTL Page

Field	Description
Status	Displays the current status of the Upload CTL page.
Upload Certificate	
Certificate Name	Use the pull-down menu to select the name of the CTL file to upload.
Root Certificate	Enter the name of the root certificate.
Upload File	Use the Browse button to select the file to be uploaded.
Upload File button or icon	Uploads the certificate file specified in the Upload Certificate Trust List section.
Close button or icon	Closes the Update CTL page.

The following table describes the Generate CSR page.

Table 19: Generate CSR Page

Field	Description
Status	Displays the current status of the Generate CSR page.
Generate Certificate Signing Request	

Cisco Unified Operating System Administration Web Interface

Field	Description
Certificate Name	Use the pull-down menu to select the name of the CTL file to generate.
Generate CSR button or icon	Generates a new CSR.
Close button or icon	Close the Generate CSR page.

The following table describes the Download CSR page.

Table 20: Download CSR Page

Field	Description
Status	Displays the current status of the Download CSR page.
Download Certificate Signing Request	
Certificate Name	Use the pull-down menu to select the name of the CTL file to download.
Download CSR button or icon	Downloads the CSR specified in the Download Certificate Signing Request section.
Close button or icon	Closes the Download CSR page.

The following table describes the Certificate Configuration page.

Table 21: Certificate Configuration Page

Field	Description
Status	Displays the current status of the Certificate Configuration page.
Certificate Settings	Displays the following information about the certificate: • File Name • Certificate Name • Certificate Type • Certificate Group • Description
Certificate File Data	Displays the contents of the certificate file.
Delete button or icon	Deletes the current certificate.
Download button or icon	Downloads the certificate to your local system.

Related Topics

Certificate Management

Certificate Monitor

The Certificate Monitor page appears when you choose **Security > Certificate Monitor**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Certificate Monitor page to do the following:

- Specify the start time
- Specify the frequency
- Enable email notification and provide email addresses of those to be notified

The following table describes the Certificate Monitor page.

Table 22: Certificate Monitor Page

Field	Description
Status	Displays the current status of the Certificate Monitor page.
Certificate Monitor Configuration	
Notification Start Time	Enter the number of days before the certificate expires that you want to be notified.
Notification Frequency	Enter the notification frequency and click one of the radio buttons to indicate days or hours.
Enable Email Notification	Check the box to the enable email notification. **Note** For the system to send notifications, you must configure an SMTP host.
Email ID	Enter the email addresses of those to be notified in the text box. Enter multiple e-mail addresses by separating each address with a semicolon (;). There should be no spaces between the email addresses.
Save button or icon	Saves the information entered on the Certificate Monitor page.

Related Topics

Certificate Management

IPSec Policy List

The IPSec Policy List page appears when you choose **Security > IPSec Configuration**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the IPsec Policy List page to display existing IPsec policies, add an additional IPsec policy, or modify an existing IPsec policy.

The following table describes the IPsec Policy List page.

Table 23: IPSec Policy List Page

Field	Description
Status	Displays the current status of the IPsec Policy List page.
IPSec Policy List	Displays the currently configured IPsec policies. Click on the Policy Name link to IPsec Policy Configuration page for that policy.
Add New button or icon	Adds a new IPsec policy. When you click **Add New**, the IPsec Policy Configuration page appears. See Table 24: IPSec Policy Configuration Page, on page 20 for information about the IPsec Policy Configuration page.

The following table describes the IPSec Policy Configuration page in Non Federal Information Processing Standard (Non FIPS) Mode.

Table 24: IPSec Policy Configuration Page

Field	Description
Status	Displays the current status of the IPsec Policy Configuration page.
IPSec Policy Details	
Policy Group Name	Specifies the name of the IPsec policy group.
Policy Name	Specifies the name of the IPsec policy.

Field	Description
Authentication Method	Specifies the authentication method. The Authentication Method field has two options Preshared Key and Certificate. If Preshared Key is selected, the Preshared Key field is editable and the Peer Type and Certificate Name fields are disabled. If Certificate is selected, the Preshared Key field is disabled. The Peer Type and Certificate Name fields are enabled.
Preshared Key	Specifies the preshared key if you selected Pre-shared Key in the Authentication Method field.
Peer Type	Specifies that the peer type is different.
Certificate Name	Specifies the certificate name.
Destination Address	Specifies the IP address of the destination (FQDN is not supported).
Destination Port	Enter the port number at the destination.
Source Address	Specifies the IP address of the source (FQDN is not supported).
Source Port	Specifies the port number at the source.
Mode	Select the Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include: • 3DES • AES 128 • AES 256
Hash Algorithm	Specifies the hash algorithm: • SHA1 • SHA256

Cisco Unified Operating System Administration Web Interface

Field	Description
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices include: • 3DES • AES 128 • AES 256
Phase 1 DH Group	
Phase One Life Time	Specifies the lifetime for phase One, IKE negotiation, in seconds.
Phase One DH	From the drop-down list, choose the phase One DH value. Choices include: 2, 5, 14, 15, 16, 17, and 18.
Phase 2 DH Group	
Phase Two Life Time	Specifies the lifetime for phase Two, IKE negotiation, in seconds.
Phase Two DH	From the drop-down list, choose the phase Two DH value. Choices include: 2, 5, 14, 16, 17, and 18.
IPSec Policy Configuration	
Enable Policy	Check the check box to enable the policy.
Save button or icon	Saves the changes made to the IPsec Policy List page.

The following table lists the field names that are displayed when the system is in FIPS Mode or ESM Mode.

Table 25: IPSec Policy Configuration Page

Field	Description
Status	Displays the current status of the IPsec Policy Configuration page.
IPSec Policy Details	
Policy Group Name	Specifies the name of the IPsec policy group.
Policy Name	Specifies the name of the IPsec policy.
Authentication Method	Specifies the authentication method. By default, certificate is selected. **Note** Preshared key is not present in FIPS Mode.
Peer Type	Specifies the peer type is different.
Certificate Name	The name of the certificate.
Destination Address	Specifies the IP address or FQDN of the destination.

Field	Description
Destination Port	Enter the port number at the destination.
Source Address	Specifies the IP address or FQDN of the source.
Source Port	Specifies the port number at the source.
Mode	Specifies the Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include: • 3DES (default) • AES 128 • AES 256
Hash Algorithm	Specifies the hash algorithm: • SHA1 • SHA256
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices include: • 3DES (default) • AES 128 • AES 256
Phase 1 DH Group	
Phase One Life Time	Specifies the lifetime for phase One, IKE negotiation, in seconds.
Phase One DH	From the drop-down list, choose the phase One DH value. The choices are from 14 to 18.
Phase 2 DH Group	
Phase Two Life Time	Specifies the lifetime for phase Two, IKE negotiation, in seconds.
Phase Two DH	From the drop-down list, choose the phase Two DH value. The choices are from 14 to 18.
IPSec Policy Configuration	
Enable Policy	Check the check box to enable the policy.

Field	Description
Save button or icon	Saves the changes made to the IPsec Policy Configuration page.

Related Topics

IPsec Management

Bulk Certificate Management

To support the Extension Mobility Cross Cluster (EMCC) feature, the system allows you to execute a bulk import and export operation to and from a common SFTP server that is configured by the cluster administrator.

You can also use the Bulk Certificate Management window to import certificates that you have exported from other clusters. However, before the **Import** button displays, you must complete the following activities:

- Export the certificates from at least two clusters to the SFTP server.
- Consolidate the exported certificates.

Field	Description
IP Address	Enter the IP address of the common node where you want to export the certificates.
Port	Enter the port number. Default: 22
User ID	Enter the User ID you want to use to log into the node.
Password	Enter the appropriate password.
Directory	Enter a directory on the node where you want to save the certificates. Example: /users/cisco

Cipher Management

Cipher management gives the administrator the ability to control the set of security ciphers allowed for every TLS and SSH connection. Administrators can choose to enforce a minimum level of security by disabling weaker ciphers.

The Cipher Management feature only take effects once this page has been used to configure allowed ciphers. Additionally, certain weak ciphers will never be allowed, even if configured in the Cipher Management page.

For more details, see Cipher Restrictions, on page 30.

TLS Interfaces

The following table details the TLS interfaces fields:

Fields	Description
All TLS	The ciphers assigned in this field will apply on all server and client connections that support the TLS protocol.
HTTPS TLS	The cipher selection in this field will apply on all connections to Tomcat on ports 443 and 8443 that support the TLS protocol.
Cipher String	This field accepts an OpenSSL formatted cipher string that will apply to the designated interface. For more information about syntax, see the OpenSSL documentation at https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.
Cipher Expansion String	When you **Save** this page, this field shows the expansion of the configured ciphers in the field "Cipher String" for the respective interface.

For more details on how to configure the cipher string, see the "Cipher Management" section in the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

SSH Interfaces

The following table details the SSH interfaces fields:

Fields	Description
SSH Ciphers	The ciphers assigned in this field will apply to SSH connections.
Cipher String	This field accepts OpenSSH formatted cipher string. For more information about syntax, see the OpenSSH documentation at https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html.
Cipher Expansion String	This field shows the expansion of the configured cipher in the field "Cipher String" for the SSH interface.
SSH Key Exchange	Key exchange algorithm configured here will be associated with the SSH Key Exchange interface on Emergency Responder.

Fields	Description
Algorithm String	This field accepts OpenSSH formatted algorithm string. For more information about syntax, see the OpenSSH documentation at https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html.
Algorithm Expansion String	This field shows the expansion of the configured SSH Key algorithms in the field "Algorithm String" for the interface.
SSH MAC	MAC algorithm configured here will be associated with the SSH MAC interface on Emergency Responder.
Algorithm String	This field accepts OpenSSH formatted algorithm string. For more information about syntax, see the OpenSSH documentation at https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html.
Algorithm Expansion String	This field shows the expansion of the configured MAC algorithm in the field "Algorithm String" for the SSH interface.

For more details on how to configure the cipher string, see the "Cipher Management" section in the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Recommended Ciphers

Warning Ensure the ciphers configured include the recommended ciphers as listed below. Otherwise, you may encounter interoperability issues with other products over secure interfaces. For changes to take effect you must restart the affected services or reboot the server when the values on the **Cipher Management** page are changed.

Warning Configuring hmac-sha2-512 in SSH MAC interface affects the DRS and CDR functionality.

Configuring ciphers aes128-gcm@openssh.com, aes256-gcm@openssh.com in "SSH Cipher's" field or configuring only ecdh-sha2-nistp256 algorithm in "SSH KEX" will break the DRS and CDR functionalities.

We recommend the following cipher strings for the TLS and SSH interface configuration:

TLS

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:
```

```
ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA
```

SSH Ciphers

```
aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
```

SSH MAC

```
hmac-sha2-256,hmac-sha1
```

SSH KEX for FIPS

```
ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
```

SSH KEX for Non-FIPS

```
ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1,
diffie-hellman-group1-sha1,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1
```

Cipher Limitations

Although the **Cipher Management** configuration page allows you to configure any number of ciphers, each application has a list of ciphers it supports on its interfaces. For example, **All TLS** interfaces may show ECDHE or DHE or ECDSA based ciphers, but an application such as Emergency Responder may not support these ciphers because EC curves or DHE algorithms are not enabled for this application's interfaces. See the "Application Ciphers Support" section below for a list of ciphers supported by individual application interfaces.

Validation in GUI

The ciphers on the **Cipher Management** page are validated according to the OpenSSL guidelines. For example, if a cipher configured is ALL:BAD:!MD5, the cipher string will be considered as valid although "BAD" is not a recognized cipher suite. OpenSSL considers this as a valid string. If AES128_SHA is configured instead of AES128-SHA (using an underscore instead of a hyphen) however, OpenSSL will identify this as an invalid cipher suite.

Application Ciphers Support

The following table represents the application interfaces and the all corresponding ciphers and algorithms that are supported on TLS and SSH interfaces:

Cisco Unified Operating System Administration Web Interface

Table 26: Emergency Responder Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers
DRS	TCP / TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
Cisco Tomcat	TCP / TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA

Table 27: Cipher Support for SSH Ciphers

Service	Ciphers/Algorithms

SSH Server	• Ciphers: aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-gcm@openssh.com`
	`aes256-gcm@openssh.com`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp256`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

SSH Client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-gcm@openssh.com`
	`aes256-gcm@openssh.com`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp256`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

Service	Ciphers/Algorithms

DRS Client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

SFTP client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

Cipher Restrictions

Though the **Cipher Management** page allows configuration of any ciphers as supported by OpenSSL or OpenSSH, some of the ciphers are disabled internally based on the security standards of Cisco to avoid accidental exposure of critical data.

When you configure ciphers on the **Cipher Management** page, the following ciphers are disabled:

TLS Disabled Ciphers

```
EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:ADH-DES-CBC-SHA:
DES-CBC-SHA:KRB5-DES-CBC-SHA:KRB5-DES-CBC-MD5:EXP-EDH-RSA-DES-CBC-SHA:
EXP-EDH-DSS-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:
EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-DES-CBC-SHA:EXP-KRB5-RC2-CBC-MD5:EXP-KRB5-DES-CBC-MD5:
EXP-ADH-RC4-MD5:EXP-RC4-MD5:EXP-KRB5-RC4-SHA:EXP-KRB5-RC4-MD5:ADH-AES256-GCM-SHA384:
ADH-AES256-SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ADH-AES128-GCM-SHA256:ADH-AES128-SHA256:
ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ADH-DES-CBC3-SHA:ADH-RC4-MD5:
AECDH-AES256-SHA:AECDH-AES128-SHA:AECDH-DES-CBC3-SHA:AECDH-RC4-SHA:AECDH-NULL-SHA:
DES-CBC3-MD5:IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:
```

```
ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:KRB5-RC4-SHA:
KRB5-RC4-MD5:IDEA-CBC-SHA:KRB5-IDEA-CBC-SHA:KRB5-IDEA-CBC-MD5:DHE-RSA-SEED-SHA:
DHE-DSS-SEED-SHA:SEED-SHA:KRB5-DES-CBC3-MD5:NULL-MD5:PSK-AES256-CBC-SHA:
PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-NULL-SHA:ECDHE-ECDSA-NULL-SHA:
ECDH-RSA-NULL-SHA:ECDH-ECDSA-NULL-SHA:NULL-SHA256:NULL-SHA
```

SSH Disabled Ciphers

```
3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

SSH Disabled KEX Algorithms

```
curve25519-sha256@libssh.org,gss-gex-sha1-,gss-group1-sha1-,gss-group14-sha1-
```

SSH Disabled MAC Algorithms

```
hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

Software Installation/Upgrade

The Software Installation/Upgrade page appears when you choose **Software Upgrades > Install/Upgrade**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Software Installation/Upgrade page to install or upgrade software from a DVD/CD or from a file system on a remote server.

The following table describes the Software Installation/Upgrade page.

Table 28: Software Installation/Upgrade Page

Field	Description
Status	Displays the current status of the Software Installation/Upgrade page.
Software Location	
Source	Pull-down menu used to specify the source for the installation/upgrade. Options are **DVD/CD** or **Remote Filesystem**.

Field	Description
Directory	The name of the directory containing the files. **Note** If the upgrade file is on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path that 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, check with your system administrator for the correct directory path.
Server	The hostname or IP address of the remote server from which the software is downloaded.
User Name	The name of a user who is configured on the remote server.
User Password	Password that is configured for this user on the remote server.
Transfer Protocol	Pull-down menu used to specify which transfer protocol to use. Options are **ftp** or **sftp**. **Note** These options are available only if you selected **Remote Filesystem** from the **Source** pull-down menu. If you selected **DVD/CD**, this pull-down menu is grayed out.
Cancel Install button or icon	Cancels the installation or upgrade procedure.
Next button or icon	Continues with the installation or upgrade procedure.

TFTP File Management

You can upload files for use by the phones to the TFTP server. Files that you can upload include custom phone rings, callback tones, and backgrounds. This option uploads files only to the specific server to which you connected, and other nodes in the cluster do not get upgraded.

Files upload into the **`tftp`** directory by default. You can also upload files to a subdirectory of the **`tftp`** directory.

If you have two Cisco TFTP servers that are configured in the cluster, you must perform the following procedure on both servers. This process does not distribute files to all nodes, nor to both Cisco TFTP servers in a cluster.

Note If you want to modify a file that is already in the **tftp** directory, you can use the CLI command **file list tftp** to see the files in the TFTP directory and **file get tftp** to get a copy of a file in the TFTP directory.

Table 29: TFTP File Management Page

Field	Description
Upload File	Click **Browse** next to this field and then choose the file that you want to upload.
Directory	To upload the file to a subdirectory of the tftp directory, enter the subdirectory.

Device Load Management

You can delete unused firmware for selected or all endpoints to ensure that there is enough free disk space during an upgrade.

Note You must delete unused firmware separately for each server in the cluster.

After you specify search criteria and click **Find**, the firmware entries appear. You can select entries and delete them to free up disk space.

Branding

The **Branding** page appears when you choose **Software Upgrades** > **Branding**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

You can upload customized branding for Cisco Emergency Responder. Use the **Branding** page to upload the `branding.zip` folder which contains the " CER" directory.

Once the `branding.zip` folder is uploaded successfully, you can enable or disable Branding using either the command line or graphical user interface and then refresh the page for the changes to take effect. For more information, refer to the "Branding" chapter.

The following table describes the Branding page.

Table 30: Branding Page

Field	Description
Status	Displays status of the **Branding** page.
Upload Branding File	
Browse	Click the **Browse** button to locate the `branding.zip` folder on the server.
Upload File	Click the **Upload File** button to upload the file to the server. It uploads the file successfully after it validates the required contents of the `branding.zip` folder.
Enable Branding	After you have uploaded the `branding.zip` file, click this button to enable branding customizations on this Cisco Emergency Responder node. After you enable branding, refresh your browser.
Disable Branding	Click this button to disable customized branding from Cisco Emergency Responder.

Related Topics

Branding File Requirements
Enable Branding

Ping Configuration

The Ping Configuration page appears when you choose **Services > Ping**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

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

The following table describes the Ping Configuration page.

Table 31: Ping Configuration Page

Field	Description
Status	Displays the current status of the Ping Configuration page.
Ping Settings	
Hostname or IP Address	Text box into which you enter the IP address or network name for the system that you want to ping.

Field	Description
Ping Interval	Text box in which you enter the amount of time between ping requests, in seconds.
Packet Size	Text box into which you enter the packet size of the ping request.
Ping iterations	Pull-down menu that allows you to choose the number of times you want to send ping requests to the other system. Available options are 1, 5, 25, or 100 times **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 are complete.
Validate IPsec	Select the check box to have the system validate IPsec.
Ping Results	Text box in which the ping results are displayed.
Ping button or icon	Sends the ping request.

Related Topics

Ping Another System

Remote Access Configuration

The Remote Access Configuration page appears when you choose **Services > Remote Support**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Remote Access Configuration page to set up a remote account that Cisco support personnel can use to access the system for a specified period of time. If the account duration limit expires, Cisco support can not access the remote support account.

When you establish a remote account, the system generates a pass phrase.

Follow this procedure to complete the remote account setup:

1. Call Cisco support and provide them with the remote support account name and pass phrase.
2. Cisco support enters the pass phrase into a decoder program that generates a password from the pass phrase.
3. Cisco support logs into the remote support account on the customer system by using the decoded password.

Cisco Unified Operating System Administration Web Interface

If you have not already created a remote account, when you navigate to the Remote Access Configuration page you can create a new account.

The following table describes the Remote Access Configuration page.

Table 32: Remote Access Configuration Page

Field	Description
Status	Displays the current status of the Remote Access Configuration page.
Remote Access Account Information	
Account Name	Name for the new remote account. Account names must be at least six-characters long and consist of all lowercase, alphabetic characters
Account Duration	The amount of time that the remote account exists, in days.
Save button or icon	Creates a new remote account. You must provide the Account Name and Account Duration before you click **Add**. Remote Access Configuration page redisplays. See Table 33: Remote Access Configuration Page , on page 36 for a description of the fields on the Remote Access Configuration page.
Delete button or icon	Deletes the currently configured remote account. **Note** The Delete button or icon is only visible if there is an existing remote account.

If you have already created a remote account, when you navigate to the Remote Access Configuration page you view and delete the remote account.

The following table describes the Remote Access Configuration page.

Table 33: Remote Access Configuration Page

Field	Description
Remote Access Account Information	
Account Name	Displays the name of the remote support account.
Expiration	Displays the date and time when access to the remote account expires.
Passphrase	Displays the generated pass phrase.
Decode Version	Indicates the version of the decoder in use.
Delete button or icon	Deletes the remote access account information.

Related Topics

Set Up Remote Support

Cisco Unified Operating System Administration Web Interface