10

Device Management

This chapter describes how to maintain the configuration and firmware, reboot or reset the security appliance, manage the security license and digital certificates, and configure other features to help maintain the security appliance. It includes the following sections:

To access the Device Management pages, click **Device Management** in the left hand navigation pane.

Viewing System Status

This section describes how to view information for all running processes and the system's CPU and memory utilization. Refer to the following topics:

- Viewing Process Status, page 404
- Viewing Resource Utilization, page 404

Viewing Process Status

Use the Processes page to view information for all running processes. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

Device Management > System Status > Processes

Field	Description
Name	Name of the process that is running on the security appliance.
Description	Brief description for the running process.
Protocol	Protocol that is used by the socket.
Port	Port number of the local end of the socket.
Local Address	IP address of the local end of the socket.
Foreign Address	IP address of the remote end of the socket.

Viewing Resource Utilization

Use the Resource Utilization page to view information for the system's CPU and memory utilization.

Device Management > System Status > Resource Utilization

Field	Description
CPU Utilization	
CPU Usage by User	CPU resource currently used by user space processes, in percentage.

Field	Description
CPU Usage by Kernel	CPU resource currently used by kernel space processes, in percentage.
CPU Idle	CPU idle resource at current time, in percentage.
CPU Waiting for I/O	CPU resource currently waiting for I/O, in percentage.
Memory Utilization	
Total Memory	Total amount of memory space available on the security appliance.
Memory Used	Total amount of memory space currently used by the processes.
Free Memory	Total amount of memory space currently not used by the processes.
Cached Memory	Total amount of memory space currently used as cache.
Buffer Memory	Total amount of memory space currently used as buffers.

Administration

Use the Administration pages to modify the username and password for the default administrator account, configure the user session settings, centrally configure the email alert settings, and configure remote management and SNMP.

This section includes the following topics:

- **Configuring Administrator Settings, page 406**
- **Configuring Remote Administration, page 407**
- **Configuring Email Alert Settings, page 408**
- **Configuring SNMP, page 415**

Configuring Administrator Settings

Use the Administrator Settings page to modify the username and password for the default administrator account and configure the user session settings. The user session settings are applicable for all authentication methods.

NOTE At your first login, you must change the default administrator password for security purposes. The Administrator Settings page provides another approach to modify the username and password for the default administrator account, but not for the first login.

STEP 1 Click **Device Management > Administration > Administrator Settings**.

STEP 2 To update your password, enter the following information in the **Administrator Name and Password** area:

- **User Name:** Enter the current username of the default administrator account, or enter a new username if you want to change it.
- **Current Password:** Enter the current administrator password.
- **New Password:** Enter a new administrator password. Passwords are case sensitive.

  NOTE: A password requires a minimum of 8 characters, including at least three of these character classes: uppercase letters, lowercase letters, digits, and special characters. Do not repeat any password more than three times in a row. Do not set the password as the username or “cisco.” Do not capitalize or spell these words backwards.
- **Confirm New Password:** Enter the new password again for confirmation.

STEP 3 To modify the user session settings, enter the following information in the **Session** area:

- **Inactivity Timeout:** Enter the time in minutes that the user can be inactive before the session is disconnected. The default value is 15 minutes. A value of zero (0) indicates that the user is always active before the session is disconnected.
- **Limit Login Session for Web Logins:** Click **On** to limit the time that the user can be logged into the security appliance through a web browser. Enter the time in minutes in the **Login Session Limit** field. The default value is 10 minutes. A value of zero (0) indicates that there is no limit for web login sessions.

- **Web Server SSL Certificate:** Choose a certificate to authenticate users who try to access the Configuration Utility through a web browser by using HTTPS. By default, the web authentication server uses the default certificate for authentication. You can choose an imported certificate for authentication. The web authentication server will restart to load the selected certificate.
- **Management:** Check the box to enable access the configuration utility via HTTP or HTTPS. HTTP is enabled by default.

  NOTE: Unchecking both boxes will disable access to the configuration utility.
- **Allow Address:** Choose whether to allow access to the configuration utility from **Any** IP address or from a particular address or address range. The default setting is Any.

STEP 4 Click **Save** to apply your settings.

Configuring Remote Administration

You can enable Remote Administration to allow an administrator to connect to the configuration utility from a different network than the local network (LAN) of the security appliance. You can allow connections through HTTPS (HTTP over SSL) and HTTP.

When this feature is enabled, a user can access the configuration utility by launching a web browser and entering the protocol, the WAN IP address of the security appliance, and the specified Listen Port Number, as shown in this example: `https://209.165.201.1:8080`

NOTE To locally or remotely access the Configuration Utility from a PC running Windows Server 2008 and Internet Explorer 9 by using the HTTP protocol, add the URL (such as http://192.168.75.1:80/login.htm) as a trusted site. To add a trusted site in Internet Explorer 9, you can first open the browser and go to the Tools > Internet Options > Security page, and then select the **Trusted sites** zone and add your URL as a trusted site.

STEP 1 Click **Device Management > Administration > Remote Administration**.

STEP 2 Specify the following information:

- **Remote Administration:** Click **On** to enable remote management by using HTTPS, or click **Off** to disable it. We recommend that you use HTTPS for secure remote management.

- **HTTPS Listen Port Number:** If you enable remote management by using HTTPS, enter the port number. By default, the listen port number for HTTPS is 8080.
- **HTTP:** Click **On** to enable remote management by using HTTP, or click **Off** to disable it.
- **HTTP Listen Port Number:** If you enable remote management by using HTTP, enter the port number. By default, the listen port number for HTTP is 80.
- **Allow Address:** To specify the devices that can access the configuration utility through the WAN interface, choose an Address Object or enter an address.
  - **Address Objects:** These objects represent known IP addresses and address ranges, such as the GUEST VLAN and the DHCP pool. For details about the listed Address Objects, see the Networking > Address Management page.
  - **Create new address:** Choose this option to enter an IP address or address range. In the pop-up window, enter a **Name** and specify the **Type** (Host or Range). For a single host, enter the IP address. For a range, enter the **Starting IP Address** and the **Ending IP Address**.
- **Remote SNMP:** Click **On** to enable SNMP for the remote connection, or click **Off** to disable SNMP. Enabling SNMP allows remote users to use SNMP to manage the security appliance from the WAN side.

STEP 3 Click **Save** to apply your settings.

Configuring Email Alert Settings

Use the Email Alert page to centrally configure how to send the alert emails to the operator or administrator for specific events or behaviors that may impact the performance, operation, and security of your security appliance, or for debugging purposes.

When this feature is enabled, an alert is sent under these three conditions:

- The Web URL categories are changed.
- The Security Services application server status is No Authentication because the server is offline.

- DNS resolution of the Security Services application server name fails because the server is offline.

STEP 1 Click **Device Management > Administration > Email Alert**.

STEP 2 In the **Email Server** area, specify the SMTP email server that is used to send the alert emails.

- **SMTP Server:** Enter the IP address or Internet name of the SMTP server.
- **Port:** Enter the port for SMTP communication. The valid range of port numbers is 1~65535.
  - If you enter port 25 (the default setting), you can choose TLS (Transport Layer Security) or SSL (Secure Sockets Layer) for securing the SMTP communication, or choose None for an unsecured connection.
  - If you enter port 465, you can choose either TLS or SSL for securing the SMTP communication.
  - If you enter port 587, you can choose either TLS or SSL for securing the SMTP communication.
- **Secure Connectivity Method:** Choose either **TLS** or **SSL** for securing the SMTP communication, or choose **None** for an unsecured connection. If you choose TLS or SSL, SMTP Authentication will be enabled.
- **SMTP Authentication:** Click **On** if the SMTP server requires authentication before accepting the connections. Users must provide the SMTP account credentials for authentication.
- **Account:** Enter the username of the SMTP email account.
- **Password:** Enter the password of the SMTP email account.
- **From Email Address:** Enter the email address to send the alert emails.
- **To Email Address:** Enter the email address to receive the alert emails. This email address is used to receive all alert emails for all events. If you want to send the alert emails that belong to different events to different email addresses, uncheck **All Alerts** and then specify the email address for each event individually.

STEP 3 To verify the settings, click the **Test Connectivity to Email Server**. The results appear in a pop-up window.

STEP 4 In the **Event Alerts** area, specify the email alert settings for each event. When the relative events are detected, the alert emails are sent to the specified email address.

The following table provides information about how to enable the email alert feature for each event.

Event	Description
CPU Overload Alert	Sends an alert email if the CPU utilization is higher than the threshold over one minute and sends another alert email when the CPU utilization comes back down to normal for one minute. ▪ **CPU Threshold Setting:** Enter the value in the range 10% to 100% for CPU utilization threshold. The default value is 90%. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable CPU Overload Alert, you must complete the following tasks: ▪ Configure the email server settings used to send the alert emails. ▪ Check **CPU Overload Alert** in the **Enable** column and specify the CPU utilization threshold and the email address used to receive the alert emails.
New Firmware Alert	Sends an alert email to the specified email address if a newer firmware is detected on Cisco.com. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable New Firmware Alert, you must complete the following tasks: ▪ Configure the email server settings used to send the alert emails. ▪ Check **New Firmware Alert** in the **Enable** column and specify the email address used to receive the alert emails. **NOTE:** Make sure that you have an active WAN connection and a valid Cisco.com account to download the latest firmware image from Cisco.com and then install it on your security appliance. For complete details, see **Upgrading your Firmware from Cisco.com, page 436**.

Event	Description
License Expiration Alert	Sends an alert email a specified number of days before the security license expires. ▪ **days:** Enter the number of days before the license expires to send the alert email. The default value is 15 days. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable License Expiration Alert, you must complete the following tasks: ▪ Validate the security license on the security appliance in the Device Management > License Management page. See **Installing or Renewing Security License, page 441**. ▪ Configure the email server settings used to send the alert emails. ▪ Check **License Expiration Alert** in the **Enable** column, set the number of days before the license expires to send the alert emails, and specify the email address used to receive the alert emails.
Syslog Email	Sends the syslogs on schedule to the specified email address for troubleshooting purposes. ▪ **Send to Email Address:** Enter the email address to receive the syslog messages. To enable Syslog Email, you must complete the following tasks: ▪ Enable the Log feature and specify the subtitle in the syslog emails, the severity level of syslogs that you want to send, and the schedule when you want to send the syslogs in the Device Management > Logs > Log Settings page. See **Configuring Log Settings, page 444**. ▪ Enable the **Email Alert** feature for the facilities in the Device Management > Logs > Log Facilities page. The syslogs generated by the selected facilities can be sent to the specified email address. See **Configuring Log Facilities, page 447**. ▪ Configure the email server settings used to send the syslog messages. ▪ Check **Syslog Email** in the **Enable** column and specify the email address used to receive the syslog messages.

Event	Description
Site-to-Site VPN Up/Down Alert	Sends an alert email when a VPN tunnel is established, a VPN tunnel is down, or the VPN tunnel negotiation fails. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable Site-to-Site VPN Up/Down Alert, you must complete the following tasks: ▪ Enable the Site-to-Site VPN feature and specify the IPsec VPN policies used to establish the VPN tunnels in the VPN > Site-to-Site > IPsec Policies page. See Configuring a Site-to-Site VPN, page 340. ▪ Configure the email server settings used to send the alert emails. ▪ Check **Site-to-Site VPN Up/Down Alert** in the **Enable** column and specify the email address used to receive the alert emails.
WAN Up/Down Alert	Sends an alert email if the WAN link is up or down. ▪ **Alert Interval:** Specify how often, in minutes, that the security appliance sends the alert emails. Enter a value in the range 3 to 1440 minutes. The default value is 5 minutes. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable WAN Up/Down Alert, you must complete the following tasks: ▪ Configure the email server settings used to send the alert emails. ▪ Check **WAN Up/Down Alert** in the **Enable** column and specify the email address used to receive the alert emails.

Event	Description
Traffic Meter Alert	Sends an alert email when the traffic limit is reached, or before the traffic counter is reset. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable Traffic Meter Alert, you must complete the following tasks: ▪ Enable the Traffic Metering feature for both the primary WAN and the secondary WAN (if applicable) and specify the corresponding settings in the Networking > WAN > Traffic Metering pages. See Measuring and Limiting Traffic with the Traffic Meter, page 135. ▪ Configure the email server settings used to send the alert emails. ▪ Check **Traffic Meter Alert** in the **Enable** column and specify the email address used to receive the alert emails.
Anti-Virus Alert	Sends an alert email at the specified interval to a specified email address if viruses are detected. ▪ **Alert Interval:** Specify how often, in minutes, that the security appliance sends an alert email for virus events. Enter a value in the range 1 to 1440 minutes. The default value is 30 minutes. The security appliance will log the virus events between alert intervals and send them in an alert email to the specified email address. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable Anti-Virus Alert, you must complete the following tasks: ▪ Enable the Anti-Virus feature and specify the protocols to scan for viruses in the Security Services > Anti-Virus > General Settings page. See Configuring Anti-Virus, page 302. ▪ Configure the email server settings used to send the alert emails. ▪ Check **Anti-Virus Alert** in the **Enable** column, set the alert interval, and specify the email address used to receive the alert emails.

Event	Description
IPS Alert	Sends an alert email every 30 minutes to the specified email address if an attack is detected by the IPS service or if an application is blocked by the Application Control service. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable the IPS Alert feature, you must complete the following tasks: ▪ Enable IPS and configure the IPS settings. See Configuring Intrusion Prevention, page 321. ▪ Enable Application Control and configure the Application Control settings. See Configuring Application Control, page 309. ▪ Configure the email server settings used to send the alert emails. ▪ Check **IPS Alert** in the **Enable** column and specify the email address used to receive the alert emails.
Web URL Filtering Alert	Sends an alert email to the specified email address when Web URL categories have any changes. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable the Web URL Filtering Alert feature, you must complete the following tasks: ▪ Enable Web URL Filtering in the Security Services > Web URL Filtering > Policy to Zone Mapping page. See Configuring Web URL Filtering, page 327. ▪ Configure the email server settings used to send the alert emails. ▪ Check **Web URL Filtering Alert** in the **Enable** column and specify the email address used to receive the alert emails.

NOTE: If a global email address for receiving all alert emails is configured in the **To Email Address** field, it will be displayed in the **Send to Email Address** field for all categories.

STEP 5 Click **Save** to apply your settings.

Configuring SNMP

Simple Network Management Protocol (SNMP) is a network protocol used over User Datagram Protocol (UDP) that lets you monitor and manage the security appliance from a SNMP manager. SNMP provides a remote means to monitor and control the network devices, and to manage the configuration, statistics collection, performance, and security.

STEP 1 Click **Device Management > Administration > SNMP**.

STEP 2 Click **On** to enable SNMP, or click **Off** to disable SNMP. By default, SNMP is disabled.

STEP 3 If you enable SNMP, specify the SNMP version. The security appliance provides support for network monitoring using SNMP Versions 1, 2c, and 3. By default, SNMP Version 1 and 2 is selected.

STEP 4 After you enable SNMP and select the SNMP version, enter the following information:

- **System Contact:** Enter the name of the contact person for your security appliance.
- **Device:** Enter the device name for easy identification of your security appliance.
- **System Location:** Enter the physical location of your security appliance.
- **Security User Name:** Enter the name of the administrator account with the ability to access and manage the SNMP MIB objects. This is only available for SNMPv3.
- **Authentication Password:** Enter the password of the administrator account for authentication (the minimum length of password is 8 characters). This is only available for SNMPv3.
- **Encrypted Password:** Enter the password for data encryption (the minimum length of password is 8 characters). This is only available for SNMPv3.
- **SNMP Engine ID:** The engine ID of the SNMP entity. The engine ID is used as a unique identification between two SNMP entities. This is only available for SNMPv3.

STEP 5 To enable SNMP Trap, enter the following information:

- **SNMP Read-Only Community:** Enter the read-only community used to access the SNMP entity.

- **SNMP Read-Write Community:** Enter the read-write community used to access the SNMP entity.
- **Trap Community:** Enter the community that the remote trap receiver host receives the traps or notifications sent by the SNMP entity.
- **SNMP Trusted Host:** Enter the IP address or domain name of the host trusted by the SNMP entity. The trusted host can access the SNMP entity. Entering 0.0.0.0 in this field allows any host to access the SNMP entity.
- **Trap Receiver Host:** Enter the IP address or domain name of the remote host that is used to receive the SNMP traps.

STEP 6 Click **Save** to apply your settings.

Backing Up and Restoring a Configuration

Use the Device Management > Backup/Restore page to manage your configuration.

You can back up your current settings as a configuration file to your local PC or to a USB device if applicable. You can later restore the saved configuration if needed. You should always back up your configuration whenever you make any modifications to the device configuration or performing any firmware updates.

NOTE When saving the configuration to a file, the security license and self-signed certificates are not saved in the configuration file.

STEP 1 Click **Device Management > Backup/Restore**.

STEP 2 To back up the current settings to your local PC, perform the following steps:

a. In **Configuration Backup** area, select the **Save Configuration to PC** radio button and click **Backup**. The Encryption window opens.

b. If you want to encrypt the configuration, check **Encrypt** and enter the password in the **Key** field, and then click **OK**. Locate where you want to save the configuration file (configure.bin) and click **Save**.

c. If you do not want to encrypt the configuration, click **OK**. Locate where you want to save the configuration file (configure.xml) and click **Save**.

STEP 3 To back up the current settings on a USB device, perform the following steps:

a. Insert a USB device into the USB port on the back panel. Make sure that the USB Device Status shows "Device Attached." Click **Refresh** to refresh the status immediately.

b. In the **Configuration Backup** area, select the **Save Configuration to USB** radio button and click **Backup**. The Encryption window opens.

c. If you want to encrypt the configuration, check **Encrypt** and enter the password in the **Key** field, and then click **OK**. The current settings will be saved as a configuration file (configure.bin) to the USB device.

d. If you do not encrypt the configuration, click **OK**. The current settings will be saved as a configuration file (configure.xml) to the USB device.

NOTE: Set the password carefully and record it, otherwise you cannot upload the configuration file later without the correct password.

STEP 4 To restore the settings from a saved configuration file on your local PC, perform the following steps:

a. In **Configuration Restore** area, select the **Restore Configuration From PC** radio button.

b. Click **Browse** to select the saved configuration file from your local PC and click **Restore**.

c. If the selected configuration file is encrypted, the Encryption window opens. Enter the password in the **Key** field and click **OK**. The security appliance reboots with the saved settings of the selected configuration file.

STEP 5 To restore the settings from a saved configuration file on a USB device, perform the following steps:

a. Insert a USB device into the USB port on the back panel.

b. In the **Configuration Restore** area, select the **Restore Configuration from USB** radio button. Make sure that the USB Device Status shows "Device Attached." Click **Refresh** to refresh the status.

c. In the **Configuration files on USB device** area, all saved configuration files located on the USB device appear in the list. Select a configuration file and click **Restore**.

d. If the selected configuration file is encrypted, the Encryption window opens. Enter the password in the **Key** field and click **OK**. The security appliance reboots with the saved settings of the selected configuration file.

Managing Certificates for Authentication

Use the Certificate Management page to manage the certificates for authentication. You can perform the following tasks:

- View the certificate status and details. See **Viewing Certificate Status and Details, page 419**.
- To export a local certificate or a Certificate Signing Request (CSR) to your PC, check it and click the **Download** icon in the **Configure** column. See **Exporting Certificates to Your Local PC, page 420**.
- To export a local certificate or a CSR to a mounted USB device, check it and click the **Export to USB** icon in the **Configure** column. See **Exporting Certificates to a USB Device, page 421**.
- To import a CA certificate or a local certificate from your local PC, click **Import PC**. See **Importing Certificates from Your Local PC, page 421**.
- To import a CA certificate or a local certificate from a mounted USB device, click **Import USB**. See **Importing Certificates from a USB Device, page 422**.
- To generate a CSR, click **Request Signing**. See **Generating New Certificate Signing Requests, page 422**.
- To import a signed certificate for a CSR from your local PC, click the **Upload** icon in the **Configure** column. See **Importing Signed Certificate for CSR from Your Local PC, page 423**.
- To delete a certificate or a CSR, click the **Delete** (x) icon in the **Configure** column.
- To delete multiple certificates, check them and click **Delete**.

Viewing Certificate Status and Details

STEP 1 Click **Device Management > Certificate Management**.

The Certificate Management window opens. All existing certificates are listed in the table. The following certificate information is displayed:

- **Certificate:** The name of the certificate.
- **Type:** The type of the certificate. The security appliance supports three types of certificates:
  - **Certificate Signing Request:** A certificate request generated by your security appliance that needs to be sent to the Certificate Authority (CA) for signing. CSR contains all information required to create your digital certificate.
  - **Local Certificate:** The local certificate is issued by a trusted CA, and is involved in the applications like remote management and SSL VPN. To use a local certificate, you must first request a certificate from the CA and then import the certificate to your security appliance.
  - **CA Certificate:** The CA certificate is issued by intermediate certificate authorities, such as GoDaddy or VeriSign. The CA certificate is used to verify the validity of certificates generated and signed by the CA.

STEP 2 To view complete details for a certificate, click the **Detail** icon in the **Details** column.

Certificate Type	Details
CA Certificate or Local Certificate	▪ **Name:** Name used to identify this certificate. ▪ **Issuer:** Name of the CA that issued the certificate. ▪ **Subject:** Name which other organizations will see as the holder (owner) of this certificate. ▪ **Serial number:** Serial number maintained by the CA and used for identification purposes. ▪ **Valid from:** Date from which the certificate is valid. ▪ **Expires on:** Date on which the certificate expires. It is advisable to renew the certificate before it expires.
Certification Signing Request (CSR)	▪ **Name:** Name used to identify this CSR. ▪ **Subject:** Name which other organizations will see as the holder (owner) of this certificate.

Exporting Certificates to Your Local PC

You can export a local certificate or a CSR to your local PC. CA certificate is not allowed to export.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To export a local certificate or a CSR to your local PC, click the **Download** icon in the **Configure** column.

- If you are downloading a CSR, the Download Certificate Signing Request window opens. Click **Download**. The certificate file will be saved in .pem format.

- If you are downloading a local certificate, the Download Certificate window opens. Enter a password in the **Enter Export Password** field to protect the certificate file and click **Download**. The certificate file will be saved in .p12 format.

Exporting Certificates to a USB Device

To export a local certificate or a CSR to a USB device, you must first insert the USB device into the USB port on the back panel. CA certificate is not allowed to export.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To export a local certificate or a CSR to the USB device, click the **Export to USB** icon in the **Configure** column.

- If you are downloading a CSR, the Export Certificate Signing Request to USB window opens. Click **Export**. The CSR file will be saved on the USB device in .pem format.
- If you are downloading a local certificate, the Export Certificate to USB window opens. Enter a password in the **Enter Export Password** field to protect the certificate file and click **Export**. The certificate file will be saved on the USB device in .p12 format.

Importing Certificates from Your Local PC

You can import a local certificate or a CA certificate from your local PC.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To import a local certificate or a CA certificate from your local PC, click **Import PC**.

STEP 3 Enter the following information:

- **Import a local end-user certificate with private key from a PKCS#12 (.p12) encoded file:** If you choose this option, click **Browse** to locate and select a local certificate file from your local PC, enter the certificate name in the **Certificate Name** field and the protection password in the **Import Password** field, and then click **Import**.

- **Import a CA certificate from a PEM (.pem or .crt) encoded file:** If you choose this option, click **Browse** to locate and select a CA certificate file from your local PC and click **Import**.

Importing Certificates from a USB Device

To import local or CA certificates from a USB device, you must first insert the USB device into the USB port on the back panel.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To import a local certificate or a CA certificate from the USB device, click **Import USB**.

The Import Certificate window opens. All available local certificates and CA certificates appear in the list.

STEP 3 Check the certificate file, enter the certificate name in the **Certificate Name** field and the protection password in the **Import Password** field, and then click **Import**.

Generating New Certificate Signing Requests

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 Click **Request Signing** to generate a new certificate signing request.

The Generate Certificate Signing Request window opens.

STEP 3 Enter the following information:

- **Certificate Alias:** Enter an alias name for the certificate.
- **Country Name:** Choose the country from the drop-down list.
- **State or Province Name:** Enter the state or province name of your location.
- **Locality Name:** Enter the address of your location.
- **Organization Name:** Enter your organization name.
- **Organization Unit Name:** Enter your department name.

- **Common Name:** Enter the common name for the certificate.
- **E-mail Address:** Enter your email address.
- **Subject Distinguished Name:** After you enter the above information, the Distinguished Name (DN) is created in this field.
- **Subject Key Type:** Displays the signature algorithm (RSA) used to sign the certificate. RSA is a public key cryptographic algorithm used for encrypting data.
- **Subject Key Size:** Choose the length of the signature: 502 bits, 1024 bits, or 2048 bits.

STEP 4 Click **Generate** to create a certificate signing request file.

After you generate a certificate signing request file, you need to export this file to your local PC for submission to a Registration or CA. The CSR file will be saved in .pem format.

Importing Signed Certificate for CSR from Your Local PC

You can upload the signed certificate for a CSR from your local PC.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To import the signed certificate for a CSR from your local PC, click the **Upload** icon in the **Configure** column.

STEP 3 Click **Browse** to locate and select the signed certificate file for the CSR from your local PC, and then click **Upload**.

NOTE: The signed certificate file should be PEM (.pem or .crt) encoded.

Configuring Cisco Services and Support Settings

This section describes how to configure your Cisco.com account on the security appliance, enable or disable Cisco OnPlus, configure the remote support settings, and send the contents for system diagnosis. Refer to the following topics:

Configuring Cisco.com Account

Use the Cisco.com Account page to configure your Cisco.com account credentials on the security appliance.

A valid Cisco.com account is required to download the latest firmware image from Cisco.com and to check for signature updates from Cisco's signature server for IPS, Application Control, and Anti-Virus. If you do not have one, go to https://tools.cisco.com/RPF/register/register.do by clicking the **Create a Cisco.com Account** link on this page to register a Cisco.com account.

NOTE You can also configure your Cisco.com account credentials by using the Setup Wizard. See Configuring Cisco.com Account Credentials, page 37.

STEP 1 Click **Device Management > Cisco Services & Support > Cisco.com Account**.

The Cisco.com Account window opens.

STEP 2 Enter the following information:

- **User Name:** Enter the name of your Cisco.com account.
- **Password:** Enter the password of your Cisco.com account.

STEP 3 Click **Save** to apply your settings.

Configuring Cisco OnPlus

Use the Cisco OnPlus page to enable or disable Cisco OnPlus Advanced Security Service on the security appliance. Enabling Cisco OnPlus Advanced Security Service allows your security appliance to send security reporting and notification data through the OnPlus Service. If an OnPlus appliance is not present in your network, this setting will have no effect.

For example, you can back up and restore the configuration, upgrade the firmware, and view the network usage reports, WAN bandwidth reports, and device utilization of the security appliance through the OnPlus Service. The security appliance can initiate or accept HTTP or HTTPS connection with the agent.

To learn more information about Cisco OnPlus, go to www.cisco.com/go/onplus.

STEP 1 Click **Device Management > Cisco Services & Support > Cisco OnPlus**.

STEP 2 Check the box next to **Enable Cisco OnPlus Advanced Security Service** to enable Cisco OnPlus on your security appliance, or uncheck this box to disable it. By default, Cisco OnPlus is enabled. This setting is provided mainly for support and troubleshooting purposes. If you disable Cisco OnPlus on the security appliance, Cisco OnPlus Service will be unable to communicate with the security appliance and overall management, monitoring, and reporting will be impacted.

NOTE: The security appliance only starts collecting the session data when the OnPlus appliance is connected.

STEP 3 If Cisco OnPlus is enabled, we recommend that you enable the following discovery protocols on your security appliance for optimal device discovery and topology support via the OnPlus portal:

- **Cisco Discovery Protocol (CDP):** Shows if CDP is enabled or disabled. You can click the link to view or edit its settings. See **CDP Discovery, page 432**.
- **Bonjour Discovery Protocol:** Shows if Bonjour is enabled or disabled. You can click the link to view or edit its settings. See **Bonjour Discovery, page 432**.

STEP 4 Click **Save** to apply your settings.

Configuring Remote Support Settings

Use the Remote Support page to enable the SSHv2 server for debugging purposes. This feature allows the engineers to use a unique console root password to log in to the security appliance for debugging operations.

STEP 1 Click **Device Management > Cisco Services & Support > Remote Support**.

STEP 2 Enter the following information:

- **SSHv2 Server:** Click **On** to enable the SSHv2 server for debugging, or click **Off** to disable it.
- **Remote Support Password:** Enter the root password for remote support in this field. The root password expires in 24 hours, so you must request for a new password after it expires.

STEP 3 Click **Save** to apply your settings.

Sending Contents for System Diagnosis

Use the Send Diagnostics page to select the contents like the configuration file, the syslog file, and the system status data and compress them into one file in zip format, and then send the compressed file to the specified email address for system diagnosis. You can set a password to protect the compressed file for security purposes.

STEP 1 Click **Device Management > Cisco Services& Support > Send Diagnostics**.

STEP 2 In the **Content (compressed)** area, choose the contents that you want to use for diagnosing the system. The selected files are compressed into one file.

- **Configuration File:** Click **On** to compress the configuration for system diagnosis.
- **Syslog File:** Click **On** to compress the syslog messages for system diagnosis.
- **System Status:** Click **On** to compress the system status data for system diagnosis.

STEP 3 In the **Password Protection** area, you can set a password to secure the compressed file.

- **Password Protection:** Click **On** to enable the password protection, or click **Off** to disable it.
- **Password:** If you enable the password protection, enter the password in this field.

STEP 4 In the **Email** area, specify the email address to receive the compressed file.

- You can send the compressed file to the email address specified on the Email Alert page by selecting the first radio button.
- If you want to temporarily send the compressed file to a specific email address for system diagnosis without changing the email address settings on the Email Alert page, select the **Other Address** radio button and enter the email address in the field.

STEP 5 Click **Save** to apply your settings.

STEP 6 Click **Send Now** to send the compressed file to the specified email address immediately.

STEP 7 Click **Download** to save the compressed file to your local PC.

Configuring System Time

Use the Date and Time page to manually configure the system time, or to dynamically synchronize the system time with the Network Time Protocol (NTP) server.

STEP 1 Click **Device Management > Date and Time**.

STEP 2 Specify the time zone from the **Time zone** drop-down list.

STEP 3 Select the **Manually Set System Time** radio button to manually set the date and time. Enter the values in the **Date** and **Time** fields.

STEP 4 Select the **Dynamically Set System Time** radio button to automatically synchronize the date and time with the specified NTP server:

- **Daylight Saving Time Adjustment:** Click **On** to automatically adjust the time for Daylight Saving Time, or click **Off** to disable it.
- **Default NTP Servers:** Click this option to use the default NTP server.

- **Custom NTP Servers:** Click this option to use a custom NTP server. Enter the IP addresses or domain names of up to two custom NTP servers in the **Server 1 Name/IP Address** and **Server 2 Name/IP Address** fields. The server 1 is the primary NTP server and the server 2 is the secondary NTP server.
- **Current Time:** Displays the current date and time synchronized with the configured NTP server.

STEP 5 Click **Save** to apply your settings.

Configuring Device Properties

Use the Device Properties page to configure the host name and domain name to identify your security appliance on the network.

STEP 1 Click **Device Management > Device Properties**.

STEP 2 Enter the following information:

- **Host Name:** Enter the host name for your security appliance, which is displayed on the network to identify your device.
- **Domain Name:** Enter a unique domain name to identify your network.

STEP 3 Click **Save** to apply your settings.

Diagnostic Utilities

Use the following diagnostic utilities to access configuration of the security appliance and to monitor the overall network health.

- **Ping, page 429**
- **Traceroute, page 429**
- **DNS Lookup, page 430**
- **Packet Capture, page 430**

NOTE These features require an active WAN connection.

Ping

Use the Ping page to test the connectivity between the security appliance and a connected device on the network.

STEP 1 Click **Device Management > Diagnostic Utilities > Ping**.

The Ping window opens.

STEP 2 Enter the following information:

- **IP Address or URL:** Enter the IP address or URL to ping.
- **Packet Size:** Enter the packet size in the range 32 to 65500 bytes to ping. The security appliance will send the packet with the specified size to the destination.
- **Number of Pings:** Enter the times to ping. The security appliance will send the packet for specific times to check the connectivity with the destination.

STEP 3 Click **Start** to ping the IP address or the URL, or click **Stop** to stop pinging.

Traceroute

Use the Traceroute page to view the route between the security appliance and a destination.

STEP 1 Click **Device Management > Diagnostic Utilities > Traceroute**.

The Traceroute window opens.

STEP 2 Enter the following information:

- **IP Address or URL:** Enter the IP address or URL of the destination.
- **Maximum Number of Hops:** Choose the maximum hop number.

STEP 3 Click **Start** to trace the route of the IP address or URL, or click **Stop** to stop tracing.

DNS Lookup

Use the DNS Lookup page to retrieve the IP address of any server on the Internet.

STEP 1 Click **Device Management > Diagnostic Utilities > DNS Lookup**.

STEP 2 Enter the IP address or domain name that you want to look up in the **IP Address or Domain Name** field.

STEP 3 Click **Run** to query the server on the Internet. If the host or domain name exists, you will see a response with the IP address.

STEP 4 Click **Clear** to clean up the querying results.

Packet Capture

Use the Packet Capture page to capture all packets that pass through a selected interface.

STEP 1 Click **Device Management > Diagnostic Utilities > Packet Capture**.

STEP 2 Choose an interface or a network (such as DEFAULT VLAN) that you want to capture the packets from the **Network** drop-down list.

NOTE: Selecting WAN1 or WAN2 (if applicable) means capturing the packets through a logical interface. Selecting GEx means capturing the packets through a physical interface. If you choose a VLAN, only inter-VLAN traffic will be captured.

STEP 3 Click **Start** to start capturing the packets, click **Stop** to stop capturing, or click **Save** to save the captured packets.

Device Discovery Protocols

The security appliance supports the following protocols to discover the devices:

- **UPnP Discovery, page 431**
- **Bonjour Discovery, page 432**
- **CDP Discovery, page 432**

- LLDP Discovery, page 433

UPnP Discovery

UPnP (Universal Plug and Play) allows for automatic discovery of devices that can communicate with your security appliance. The UPnP Portmaps table displays the port mapping entries of the UPnP-enabled devices that accessed your security appliance.

STEP 1 Click **Device Management > Discovery Protocols > UPnP**.

STEP 2 Enter the following information:

- **Universal Plug-n-Play (UPnP):** Click **On** to enable UPnP, or click **Off** to disable UPnP. If UPnP is disabled, the security appliance will not allow for automatic device configuration.
- **LAN:** Choose an existing VLAN to which the UPnP information is broadcasted and listened on.
- **Advertisement Period:** Enter the value in seconds of how often the security appliance broadcasts its UPnP information to all devices within range. The default value is 1800 seconds.
- **Advertisement Time to Live:** Enter the value expressed in hops for each UPnP packet. This is the number of steps a packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range. The default value is 4.

STEP 3 Click **Save** to apply your settings.

STEP 4 After you enable UPnP, the information in the UPnP Portmaps table will be refreshed immediately. Click **Refresh** to manually refresh the data.

Bonjour Discovery

Bonjour is a service advertisement and discovery protocol. Bonjour only advertises the default services configured on the security appliance when Bonjour is enabled.

STEP 1 Click **Device Management > Discovery Protocols > Bonjour**.

STEP 2 Click **On** to enable Bonjour, or click **Off** to disable it. If you enable Bonjour, all default services such as CSCO-SB, HTTP, and HTTPS are enabled. You cannot disable a particular service. You can either enable Bonjour or disable it.

STEP 3 In the **VLAN Association** area, you can associate the VLANs for the default services. The default services will only be visible to the hosts that belong to the associated VLANs. By default, DEFAULT VLAN is the broadcasting domain.

- To associate a VLAN, choose a VLAN from the **VLAN** drop-down list and click **Apply**.
- To dissociate the VLANs from the default services, check the boxes next to the appropriate VLANs and click **Delete**.

STEP 4 Click **Save** to apply your settings.

CDP Discovery

Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco manufactured equipment. Each CDP enabled device sends periodic messages to a multicast address and also listens to the periodic messages sent by others in order to learn about neighboring devices and determine the status of these devices. See **CDP Discovery, page 432**.

STEP 1 Click **Device Management > Discovery Protocols > CDP**.

STEP 2 In the **CDP Configuration** area, enter the following information:

- **Cisco Discovery Protocol (CDP):** Control whether CDP will run on some, all, or none of Ethernet interfaces. Choose one of the following options:
  - **Enable All:** Enable CDP on all ports supported by the security appliance.
  - **Disable All:** Disable CDP on all ports.

  - **Per Port:** Configure CDP on selective ports. CDP per port is recommended.

- **CDP Timer:** Enter the value of the time interval between two successive CDP packets sent by the security appliance. The default value is 60 seconds.
- **CDP Hold Timer:** The hold timer is the amount of time the information sent in the CDP packet should be cached by the security appliance that receives the CDP packet, after which the information is expired. The default value is 180 seconds.

Note: The Voice VLAN ID is a read-only field. You can configure the Voice VLAN on the Networking > VLAN page. For more information, see Configuring a VLAN, page 137.

STEP 3 In the **Enable CDP** area, specify which interfaces will run CDP. Click **On** to enable CDP on an interface, or click **Off** to disable CDP. This is required if you choose **Per Port** from the **CDP** drop-down list.

STEP 4 Click **Save** to apply your settings.

LLDP Discovery

Link Layer Discovery Protocol (LLDP) enables network managers to troubleshoot and enhance network management by discovering and maintaining network topologies over multi-vendor environments. LLDP discovers network neighbors by standardizing methods for network devices to advertise themselves to other systems, and to store discovered information.

LLDP enables a device to advertise its identification, configuration, and capabilities to neighboring devices that store the data in a Management Information Base (MIB). The network management system models the topology of the network by querying these MIB databases.

STEP 1 Click **Device Management > Discovery Protocols > LLDP**.

STEP 2 Click **On** to enable LLDP, or click **Off** to disable it. If you enable LLDP, the LLDP neighbors appear in the LLDP Neighbors table.

STEP 3 To view the detail of a LLDP neighbor, check it and click **Details**.

STEP 4 To refresh the data in the LLDP Neighbors table, click **Refresh**.

STEP 5 Click **Save** to apply your settings.

Firmware Management

You can perform the following tasks to maintain the firmware:

- View the firmware status. See **Viewing Firmware Information, page 435**.
- Switch to the secondary firmware through the Configuration Utility. See **Using the Secondary Firmware, page 435**.
- Upgrade your firmware to the latest version from Cisco.com. See **Upgrading your Firmware from Cisco.com, page 436**.
- Upgrade your firmware from a firmware image on your local PC or on a USB device. See **Upgrading Firmware from a PC or a USB Device, page 437**.
- Automatically fall back to the secondary firmware. See **Firmware Auto Fall Back Mechanism, page 438**.
- Use the Rescue mode to recover the system. See **Using Rescue Mode to Recover the System, page 438**.

CAUTION During a firmware upgrade, do NOT close the browser window, navigate away from the upgrading page, turn off the device, shut down the PC, remove the cable, or interrupt the process in any way until the operation is complete. This process should take several minutes including the reboot process. Interrupting the upgrade process at specific points when the flash is being written to can corrupt the flash memory and render the security appliance unusable.

Viewing Firmware Information

STEP 1 Click **Device Management > Firmware**.

The Firmware window opens.

STEP 2 In the **Firmware Version** area, the following firmware information is displayed:

- **Primary Firmware Version:** The version of the primary firmware that you are using.
- **Secondary Firmware Version:** The version of the secondary firmware that you used previously.

Using the Secondary Firmware

If the primary firmware is not stable, you can manually set the secondary firmware that was in use as the primary firmware. The original primary firmware will then become the secondary firmware. We recommend that you back up your current settings for later use before you switch to the secondary firmware.

CAUTION Do not try to switch the firmware if a secondary firmware image is not present. Doing so can cause the security appliance to not boot up.

STEP 1 Click **Device Management > Firmware**.

The Firmware window opens.

STEP 2 In the **Firmware Version** area, click **Switch Firmware**.

A warning message appears saying “Preparing to reboot. Do you want to continue? WARNING: All current sessions will be closed and the system will be down for approximately 180 seconds.”

STEP 3 Click **Yes** to reboot the security appliance by using the secondary firmware image.

Upgrading your Firmware from Cisco.com

The security appliance automatically checks for firmware updates from Cisco.com every 24 hours. You can upgrade your firmware to the latest version if a newer firmware is available on Cisco.com. A valid Cisco.com account is required to download the firmware image from Cisco.com.

NOTE This feature requires an active WAN connection.

STEP 1 Click **Device Management > Firmware**.

The Firmware window opens.

STEP 2 In the **Upgrade Firmware** area, the following information will be displayed under the **Upgrade Firmware from Cisco.com** radio button:

- **Your firmware is up to date:** Displays this message if you are using the latest firmware. The **Upgrade Firmware from Cisco.com** radio button will be grayed out.
- **Last checked:** Displays the date and time for the last query.
- **Unable to check firmware status:** Displays this message if the security appliance cannot access Cisco's IDA server due to invalid WAN connection or any other reasons.
- **New Firmware Available:** Displays the version number of the latest firmware image on Cisco's IDA server if newer firmware is available after the query. The **Upgrade Firmware from Cisco.com** radio button will be activated.

STEP 3 If newer firmware is available on Cisco.com, select the **Upgrade Firmware from Cisco.com** radio button and then perform one of the following actions:

- To upgrade the firmware and keep using the current settings, click **Upgrade**.
- To upgrade the firmware and restore the factory default settings, click **Upgrade and Factory Reset**.

STEP 4 The Firmware Upgrade window opens. Follow the on-screen prompts to download and install the firmware on your security appliance. For complete details, see Upgrading your Firmware After your First Login, page 33.

Upgrading Firmware from a PC or a USB Device

This section describes how to manually upgrade the firmware from a firmware image on your local PC or on a USB device. You must first download the latest firmware image from Cisco.com and save it to your local PC or to a USB device.

STEP 1 Click **Device Management > Firmware**.

The Firmware window opens.

STEP 2 To manually upgrade the firmware from your local PC, perform the following steps:

a. In the **Upgrade Firmware** area, select the **Upgrade Firmware from PC** radio button.

b. Click **Browse** to locate and select the firmware image from your local PC.

c. To upgrade the firmware and keep using the current settings, click **Upgrade**.

d. To upgrade the firmware and restore the factory default settings, click **Upgrade and Factory Reset**.

STEP 3 To upgrade the firmware through a USB device, perform the following steps:

a. Insert the USB device with the firmware images into the USB port on the back panel.

b. In the **Upgrade Firmware** area, select the **Upgrade Firmware from USB** radio button. Make sure that the USB Device Status shows as “Device Attached.” Click **Refresh** to refresh the status.

c. In the **Firmware images on USB device** area, all firmware images located on the USB device appear in the list. Select a firmware image from the list to upgrade.

d. To upgrade the firmware and keep using the current settings, click **Upgrade**.

e. To upgrade the firmware and restore the factory default settings, click **Upgrade and Factory Reset**.

Firmware Auto Fall Back Mechanism

The security appliance includes two firmware images in the same NAND flash to provide an Auto Fall Back mechanism so that the security appliance can automatically switch to the secondary firmware when the primary firmware experiences a CRC error or cannot boot up successfully for five times.

- **CRC Error:** An error that the firmware cannot pass the CRC (Cyclic Redundancy Check) validation. Downloading an incomplete firmware or incompletely writing the firmware to the flash may cause the CRC error.
- **Boot Failure:** A failure that the firmware cannot boot up successfully for five times.

The Auto Fall Back mechanism operates as follows:

STEP 1 The security appliance first boots up with the primary firmware.

STEP 2 The bootloader checks the CRC for the primary firmware.

STEP 3 If the CRC error or the boot failure occurs for the primary firmware, the bootloader will switch to the secondary firmware.

STEP 4 The bootloader checks the CRC for the secondary firmware.

STEP 5 If the CRC error or the boot failure occurs for the secondary firmware, the Rescue mode starts up. In Rescue mode, the security appliance works as a TFTP server. You can use a TFTP client to upload the firmware image to upgrade the firmware. For more information about the Rescue mode, see **Using Rescue Mode to Recover the System, page 438**.

Using Rescue Mode to Recover the System

When the system has a booting problem, a device error occurs, or the system has a problem, the POWER/SYS light on the front panel is solid amber. Follow these steps to start up the Rescue mode directly and then recover the system.

STEP 1 Press and hold the **RESET** button on the back panel of the security appliance for more than 3 seconds and power the unit on simultaneously.

The Rescue mode starts up. The Status LED flashes green and then shines solid amber. In Rescue mode, the security appliance works as a TFTP server.

STEP 2 Remove all cables from the WAN and LAN ports.

STEP 3 Connect your PC to the LAN port.

STEP 4 Configure your PC with a static IP address of 192.168.75.100 and a subnet mask of 255.255.255.0.

STEP 5 On your PC, start your TFTP client, such as tftpd32. Specify the host IP address as 192.168.75.1 and transfer the ISA500 firmware file from your PC to the security appliance.

The security appliance will upgrade the firmware after you upload the image. This process should take several minutes including the reboot process.

IMPORTANT: During firmware upgrade, do not turn off the device, shut down the PC, interrupt the process, or remove the cable in any way until the operation is complete.

When the POWER/SYS light on the front panel is solid green, the system is operating normally.

Managing Security License

The security services are licensable. A valid security license is required to activate security services and to support SSLVPN with mobile devices such as smart phones and tablets. The Product Authorization Key (PAK) and a valid Cisco.com account are required to install the security license. You can find the license code from the paper license that is shipped with the unit.

Use the License Management page to manage the security license. Refer to the following topics:

- **Checking Security License Status, page 440**
- **Installing or Renewing Security License, page 441**

Checking Security License Status

You can view information for the security license, including the expiration date, the device credentials used to renew the license, and the email alert settings for license expiration events.

STEP 1 Click **Device Management > License Management**.

The License Management window opens. The following information is displayed.

- **Feature:** The name of the security license.
- **Status:** Shows if the security license is installed or not installed. The security license cannot be transferred or revoked once it is installed.
- **Expiration:** The date on which the security license expires.

STEP 2 Click **Credentials** to display the product ID and series number of the device and the device credentials. The device credentials may be requested by Cisco sales or support to complete or troubleshoot licensing.

STEP 3 Click **Email Alerts** to set up or view the email alert settings for license expiration events.

The Email Alerts window opens. The following information is displayed.

- **Email Alert:** Click **On** to enable email alerts for license expiration, or click **Off** to disable this feature.
- **From Email Address:** The email address to use as the sender of the alert emails.
- **Send to Email Address:** The email address where the alerts will be sent.
- **SMTP Server:** The IP address or Internet name of the SMTP server.
- **SMTP Authentication:** Click **On** to enable SMTP authentication, or click **Off** to disable this feature.
- **Alert when it is:** Enter a number to specify the time frame when the alert will be sent. For example, enter 14 to send the email two weeks before the license expires.

STEP 4 We recommend that you enable the License Expiration Alert feature so that the system can send an alert to remind you to renew the security license before it expires. Click the link on the page or go to the Device Management > Administration > Email Alert page to enable the License Expiration Alert feature

and configure the email server settings. See **Configuring Email Alert Settings, page 408**.

Installing or Renewing Security License

This section describes how to install the security license or renew the security license before it expires. A valid security license is required to activate security services and to support SSLVPN with mobile devices such as smart phones and tablets.

NOTE You can also validate the security license by using the Setup Wizard. See Validating Security License, page 39.

STEP 1 Contact your Cisco reseller to purchase a license. The series number, PID, and UDI of your device are required to apply for a license. You can find these information from the Status > Dashboard page or from the Device Management > License Management page.

STEP 2 Log in to the Configuration Utility.

STEP 3 Click **Device Management > License Management**.

STEP 4 To install the security license, click the **Install** icon. **Other option:** If the security license is installed, you can click the **Renew** icon to renew the security license before it expires. Choose the license type from the **License Type** drop-down list:

- **License Code (PAK) from Cisco.com:** Automatically retrieves and installs the license on the security appliance from the Cisco server. If you choose this option, enter the following information. These credentials are required for the security appliance to authenticate to the Cisco server.
  - **License Code:** Enter the license code (PAK).
  - **Cisco.com Login:** Enter the username of your Cisco.com account.
  - **Cisco.com Password:** Enter the password of your Cisco.com account.
  - **Email Address:** Enter the registered email address to receive the PAK.
- **License File download from Cisco.com:** Installs a security license that was previously downloaded to your PC. If you choose this option, click **Browse** to locate and select the license file from your PC.

  NOTE: Make sure that the security appliance is set to the current time, or the license will not install properly. See **Configuring System Time, page 427**.

STEP 5 Check the box of **Click here if you accept with SEULA** to accept the SEULA (Software End User License Agreement) requirements. You can click the **SEULA** link to see the detailed SEULA requirements on Cisco.com.

STEP 6 Click **Validate License** to validate the security license on your security appliance.

After the license is installed or renewed, the expiration date of the security license is updated immediately. The security services are activated by the security license.

Log Management

You can configure logs for various events that occur on your network. The event logs can be used for tracking potential security threats. A variety of events can be captured and logged for review. These logs can be saved to the local syslog daemon or to a specified remote syslog server, or be emailed to a specified email address.

This section describes how to view the event logs, and configure the log settings and the log facilities. Refer to the following topics:

- **Viewing Logs, page 442**
- **Configuring Log Settings, page 444**
- **Configuring Log Facilities, page 447**

Viewing Logs

Use the View Logs page to view the logs for specific severity level, log facility, or source and/or destination IP address, or to search the logs by keyword.

NOTE Make sure that you enable the Local Log feature before you view the logs. See **Configuring Log Settings, page 444**.

STEP 1 Click **Device Management > Logs > View Logs**.

STEP 2 Specify the logs to be viewed:

- **Log Severity:** Choose the severity level to filter the logs. For example: If you select Critical, all logs listed under the Critical, Emergency, and Alert categories are displayed.

- **Log Facility:** Choose the facility to filter the logs. All logs that belong to the selected facility and match the specified severity settings are displayed.
- **Keyword:** Enter the keyword to search the logs. All logs that contain the specified keyword are displayed.
- **Source IP Address:** Enter the source IP address to filter the firewall logs. All firewall logs that match this source IP address are displayed.
- **Destination IP Address:** Enter the destination IP address to filter the firewall logs. All firewall logs that match this destination IP address are displayed.

STEP 3 Click **Query**.

The query outputs appear in the **Logs** table. The following information is displayed.

- **Date:** The date of the event.
- **Severity:** The severity level of the event.
- **Facility:** The type of facility for the log.
- **Log Data:** A brief description for the event.
- **Source IP Address:** The source IP address for the firewall event.
- **Destination IP Address:** The source IP address for the firewall event.

STEP 4 You can optionally perform the following actions:

- Sort the log entries. The logs can be sorted by clicking the column header. By default, the logs are sorted by date and time in descending sequence. For example, if you click **Severity**, the logs are sorted by the severity level in ascending sequence. Double click **Severity**, the logs are sorted by the severity level in descending sequence.
- Navigate the log entries. When viewing large numbers of logs, you can specify how many logs are displayed in the table per page, or you can navigate these logs by using the navigation buttons if one page cannot show all logs.
- Click **Clear** to clean up all logs that are saved in the local syslog daemon.
- Click **Refresh** to refresh the log data.
- Click **Export** to export the logs to a defined destination for debugging purposes.

Configuring Log Settings

Use the Log Settings page to enable the Log feature and configure the log settings. You can set the log buffer size, log all unicast traffic or broadcast traffic destined to your device for troubleshooting purposes, specify which syslogs to be mailed to a specified email address on schedule, and set the severity level of the events that are logged. If you have a remote syslog server support, you can save logs to the remote syslog server.

STEP 1 Click **Device Management > Logs > Log Settings**.

STEP 2 In the **Log Settings** area, enter the following information:

- **Log:** Click **On** to enable the Log feature, or click **Off** to disable it.
- **Log Buffer:** If you enable the Log feature, specify the size for the local log buffer. The default value is 409600 bytes.

  NOTE: After you enable the Log feature and set the log buffer size, specify the severity level of the events that you want to log. These logs will be saved to the local log daemon. See **Step 7**.

STEP 3 In the **System Logs** area, if you want to monitor the security appliance with more traffic data, you can choose to log all unicast traffic and/or all broadcast or multicast traffic directed to your security appliance for troubleshooting purposes. The logs for unicast traffic and broadcast or multicast traffic are at the Information severity level.

- **Unicast Traffic:** Click **On** to log all unicast packets directed to the security appliance. Unicast traffic for all facilities will be logged, regardless of internal or external traffic.
- **Broadcast/Multicast Traffic:** Click **On** to log all broadcast or multicast packets directed to the security appliance. Broadcast or multicast traffic for all facilities will be logged, regardless of internal or external traffic.

  If both are unselected, the security appliance only logs the events based on your facility settings. The log facilities are used to log some interest events, such as wireless clients are associated, packets are blocked by firewall rules, viruses are detected by the Anti-Virus service, and so forth.

STEP 4 In the **Email Server** area, specify which syslogs to be mailed to a specified email address on schedule.

- **Email Alert:** Shows if the Syslog Email feature is enabled or disabled.
- **From Email Address:** The email address used to send the logs.

- **To Email Address:** The email address used to receive the logs.
- **SMTP Server:** The IP address or Internet name of the SMTP server.
- **SMTP Authentication:** Shows if the SMTP authentication is enabled or disabled.

  NOTE: The above email server settings are read only. You must enable the Syslog Email feature and configure the email server settings to send the syslog messages to a specified email address. You can click the **Set Email Alert** link or go to the Device Management > Administration > Email Alert page to do this. See **Configuring Email Alert Settings, page 408**.
- **Mail Subtitle:** Enter the subtitle that is displayed in the email. For example, if you set the device name as the subtitle, the email recipient can recognize quickly what device the logs or alerts are coming from.
- **Severity:** Choose the severity level for the logs that you want to send.

Severity Level	Description
Emergency (level 0, highest severity)	System unusable.
Alert (level 1)	Immediate action needed.
Critical (level 2)	Critical conditions.
Error (level 3)	Error conditions.
Warning (level 4)	Warning conditions.
Notification (level 5)	Normal but significant conditions.
Information (level 6)	Informational messages only.
Debug (level 7, lowest severity)	Debugging messages.

For example: If you select Critical, all logs listed under the Critical, Emergency, and Alert categories are sent.

STEP 5 In the **Email Schedule** area, specify the schedule to send the logs.

- **Frequency:** Choose the period of time that you want to send the logs.
  - **Hourly:** Send the logs on an hourly basis.

- **Daily:** Send the logs at a specific time of every day. If you choose this option, specify the time to send the logs in the **Time** field.
- **Weekly:** Send the logs on a weekly basis. If you choose this option, specify the day of the week in the **Day** field and the time in the **Time** field.

- **Day:** If the logs are sent on a weekly basis, choose the day of the week
- **Time:** Choose the time of day when the logs should be sent.

STEP 6 In the **Remote Logs** area, specify how to save the logs to a remote syslog server.

- **Remote Logs:** Click **On** to save the logs to the specified remote syslog server, or click **Off** to disable it.
- **Syslog Server:** Enter the IP address or domain name of the remote syslog server that runs a syslog daemon.
- **Severity:** Choose the severity level of the logs that you want to save to the remote syslog server.

  For example: If you select Critical, the logs listed under the Critical, Emergency, and Alert categories are saved to the remote syslog server.

STEP 7 In the **Local Log** area, choose the severity level for the events that you want to log. The logs will be saved to the local syslog daemon.

For example: If you select Critical, all log messages listed under the Critical, Emergency, and Alert categories are saved to the local syslog daemon.

STEP 8 Click **Save** to apply your settings.

NOTE Next steps:

- To specify which system messages are logged based on the facility, go to the Log Facilities page. See **Configuring Log Facilities, page 447**.
- (Optional) To enable the Syslog Email feature and configure the email server settings to send the syslog messages to a specified email address, go to the Device Management > Administration > Email Alert page. See **Configuring Email Alert Settings, page 408**.

Configuring Log Facilities

Use the Log Facilities page to specify which system messages are logged based on the facility and determine where to save the syslogs and whether to send the syslogs to a specified email address on schedule.

NOTE Before you configure the log facilities, make sure that you enable the Log feature, set the log buffer size, and specify the Email Alert, Remote Log, and Local Log settings. See **Configuring Log Settings, page 444**.

STEP 1 Click **Device Management > Logs > Logs Facilities**.

The Log Facilities window opens. All supported facilities are listed in the table.

STEP 2 Specify the following information:

- **Email Alert:** Check **Email Alert** to enable the email alert settings for all facilities, or check the box for a facility to enable the email alert settings for the selected facility.

  The events that belong to the selected facilities and match the specified severity level for Syslog Email are logged and the recorded syslogs are sent to the specified email address on schedule.

- **Remote Log:** Check **Remote Log** to enable the remote log settings for all facilities, or check the box of a facility to enable the remote log settings for the selected facility.

  The events that belong to the selected facilities and match the specified severity level for Remote Logs are logged and the recorded syslogs are saved to the specified remote syslog server.

- **Local Log:** Check **Local Log** to enable the local log settings for all facilities, or check the box of a facility to enable the local log settings for the selected facility.

  The events that belong to the selected facilities and match the specified severity level for Local Log are logged and the recorded syslogs are saved to the local syslog daemon.

  NOTE: For information on configuring the Email Alert, Remote Log, and Local Log settings, see **Configuring Log Settings, page 444**.

STEP 3 Click **Save** to apply your settings.

Rebooting and Resetting the Device

Use the Reboot/Reset page to reboot the security appliance or restore the security appliance to the factory default settings (if necessary) from the Configuration Utility. Refer to the following topics:

- **Restoring the Factory Default Settings, page 448**
- **Rebooting the Security Appliance, page 449**

Restoring the Factory Default Settings

To restore the security appliance to the factory default settings, you can press and hold the **RESET** button on the back panel for more than 3 seconds, or perform the **Reset to Factory Defaults** operation from the Configuration Utility.

CAUTION The Reset To Factory Defaults operation will wipe out the current settings used on the security appliance (including the imported certificates). We recommend that you back up your current settings before restoring the factory default settings.

STEP 1 Click **Device Management > Reboot/Reset**.

The Reboot/Reset window opens.

STEP 2 In the **Reset Device** area, click **Reset to Factory Defaults**.

A warning message appears saying “Preparing to restore the factory default settings. Do you want to continue? WARNING: The current configuration will be overwritten.”

STEP 3 Click **Yes** to reboot the security appliance with the factory default settings.

Rebooting the Security Appliance

To reboot the security appliance, you can press and release the **RESET** button on the back panel for less than 3 seconds, or perform the **Reboot** operation from the Configuration Utility.

STEP 1 Click **Device Management > Reboot/Reset**.

The Reboot/Reset window opens.

STEP 2 In the **Reboot Device** area, click **Reboot**.

A warning message appears saying “Preparing to reboot. Do you want to continue? WARNING: All current sessions will be closed and the system will be down for approximately 180 seconds.”

STEP 3 Click **Yes** to reboot the security appliance.

Configuring Schedules

The schedule specifies when the firewall rule or the application control policy is active. For example, if you want a firewall rule only to work on the weekend, you can create a schedule called “Weekend” that is only active on Saturday and Sunday.

STEP 1 Click **Device Management > Schedules**.

The Schedules window opens.

STEP 2 To create a new schedule, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Schedule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Schedule Name:** Enter the name for the schedule.

- **Schedule Days:** Schedules the firewall rule or the application control policy on all days or on specific days.
  - **All Days:** Choose this option if you want to keep the firewall rule or the application control policy always on.
  - **Specific Days:** Choose this option and then check the days that you want to keep the firewall rule or the application control policy active.
- **Schedule Time:** Schedules the firewall rule or the application control policy on all days or at a specific time of day.
  - **All Days:** Choose this option if you want to keep the firewall rule or the application control policy always on.
  - **Specific Times:** Choose this option if you want to keep the firewall rule or the application control policy active at specific times. Specify the **Start Time** and **End Time** by entering the hour and minute and choosing either AM or PM.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.