Perform System Administration Tasks

This chapter contains the following sections:

Overview of System Administration

The S-Series appliance provides a variety of tools for managing the system. Functionality on System Administration tab helps you manage the following tasks:

- Appliance configuration
- Feature keys
- Adding, editing, and removing user accounts
- AsyncOS software upgrades and updates
- System time

Saving, Loading, and Resetting the Appliance Configuration

All configuration settings within the Web Security appliance are managed using a single XML configuration file.

Viewing and Printing the Appliance Configuration

Step 1 Choose **System Administration > Configuration Summary.**

Step 2 View or print the Configuration Summary page as required.

Saving the Appliance Configuration File

Step 1 Choose **System Administration > Configuration File**.

Step 2 Complete the Configuration File options.

Option	Description
Specify a file-handling option	Choose how the generated configuration file is handled: • Download file to local computer to view or save. • **Save file to this appliance** (wsa_example.com). • **Email file to:** – provide one or more email addresses.
Specify a passphrase-handling option	• **Mask passphrases in the Configuration Files** – The original passphrases are replaced with "*****" in the exported or saved file. Please note that configuration files with masked passphrases cannot be loaded directly back into AsyncOS for Web. • **Encrypt passphrases in the Configuration Files** – If FIPS mode is enabled, this option is available. See Enabling or Disabling FIPS Mode , on page 24 for information about enabling FIPS mode.
Select a file-naming option	Choose how the configuration file is named: • **Use system-generated file name** • **Use user-defined file name**

Step 3 Click **Submit**.

Loading the Appliance Configuration File

Caution Loading configuration will permanently remove all of your current configuration settings. It is strongly recommended that you save your configuration before performing these actions.

Loading configurations from previous release to the latest is not recommended. You can retain the configuration settings by upgrading the paths.

Note If a compatible configuration file is based on an older version of the set of URL categories than the version currently installed on the appliance, policies and identities in the configuration file may be modified automatically.

Step 1 Choose **System Administration > Configuration File**.

Step 2 Choose Load Configuration options and a file to load. Note:

Note
- Files with masked passphrases cannot be loaded.
- Files must have the following header:

  `<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">`

  and a correctly formatted config section:

  `<config>` ... *your configuration information in valid XML* `</config>`

Step 3 Click **Load**.

Step 4 Read the warning displayed. If you understand the consequences of proceeding, click **Continue**.

Resetting the Appliance Configuration to Factory Defaults

You can choose whether or not to retain existing network settings when you reset the appliance configuration.

This action does not require a commit.

Before you begin

Save your configuration to a location off the appliance.

Step 1 Choose **System Administration > Configuration File**.

Step 2 Scroll down to view the **Reset Configuration** section.

Step 3 Read the information on the page and select options.

Step 4 Click **Reset**.

Working with Feature Keys

Feature keys enable specific functionality on your system.Keys are specific to the serial number of your appliance (you cannot re-use a key from one system on another system).

Displaying and Updating Feature Keys

Step 1 Choose **System Administration > Feature Keys**.

Step 2 To refresh the list of pending keys, click **Check for New Keys** to refresh the list of pending keys.

Step 3 To add a new feature key manually, paste or type the key into the Feature Key field and click **Submit Key**. If the feature key is valid, the feature key is added to the display.

Step 4 To activate a new feature key from the Pending Activation list, mark its "Select" checkbox and click **Activate Selected Keys**.

You can configure your appliance to automatically download and install new keys as they are issued. In this case, the Pending Activation list will always be empty. You can tell AsyncOS to look for new keys at any time by clicking the **Check for New Keys** button, even if you have disabled the automatic checking via the Feature Key Settings page.

Changing Feature Key Update Settings

The Feature Key Settings page is used to control whether your appliance checks for and downloads new feature keys, and whether or not those keys are automatically activated.

Step 1 Choose **System Administration > Feature Key Settings**.

Step 2 Click **Edit Settings**.

Step 3 Change the Feature Key Settings as required.

Option	Description
Automatic Serving of Feature Keys	Options to automatically check and download feature keys and to automatically activate downloaded feature keys. Automatic checks are normally performed once a month but this changes to once a day when a feature key is to expire in less than 10 days and once a day after key expiration, for up to one month. After a month, the expired key is no longer included in the list of expiring/expired keys.

Step 4 Submit and commit your changes.

Virtual Appliance License

The Cisco Web Security Virtual appliance requires an additional license to run the virtual appliance on a host.

For more information about virtual appliance licensing, see the *Cisco Content Security Virtual Appliance Installation Guide* , available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Note You cannot open a Technical Support tunnel before installing the virtual appliance license.

After the license expires, the appliance will continue to serve as a web proxy without security services for180 days. Security service updates do not occur during this period.

You can configure the appliance so you receive alerts about license expiration.

Related Topics

- Managing Alerts, on page 14

Installing a Virtual Appliance License

See the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

Enabling Remote Power Cycling

Before you begin

- Cable the dedicated Remote Power Cycle (RPC) port directly to a secure network. For information, see the hardware guide for your appliance model. For the location of this document, see Documentation Set.
- Ensure that the appliance is accessible remotely; for example, open any necessary ports through the firewall.
- This feature requires a unique IPv4 address for the dedicated Remote Power Cycle interface. This interface is configurable only via the procedure described in this section; it cannot be configured using the ipconfig command.
- In order to cycle appliance power, you will need a third-party tool that can manage devices that support the Intelligent Platform Management Interface (IPMI) version 2.0. Ensure that you are prepared to use such a tool.
- For more information about accessing the command-line interface, see Command Line Interface

The ability to remotely reset the power for the appliance chassis is available only on 80-series hardware.

If you want to be able to remotely reset appliance power, you must enable and configure this functionality in advance, using the procedure described in this section.

Step 1 Use SSH or the serial console port to access the command-line interface.

Step 2 Sign in using an account with Administrator access.

Step 3 Enter the following commands:

```
remotepower

setup
```

Step 4 Follow the prompts to specify the following:

- The dedicated IP address for this feature, plus netmask and gateway.
- The username and passphrase required to execute the power-cycle command.

  These credentials are independent of other credentials used to access your appliance.

Step 5 Enter `commit` to save your changes.

Step 6 Test your configuration to be sure that you can remotely manage appliance power.

Step 7 Ensure that the credentials that you entered will be available to you in the indefinite future. For example, store this information in a safe place and ensure that administrators who may need to perform this task have access to the required credentials.

What to do next

Related Topics

- Hardware Appliances: Remotely Resetting Appliance Power

Administering User Accounts

The following types of users can log into the appliance to manage it:

- **Local users.** You can define users locally on the appliance itself.
- **Users defined in an external system.** You can configure the appliance to connect to an external LDAP or RADIUS server to authenticate users logging into the appliance.

Note Any user you define can log into the appliance using any method, such as logging into the web interface or using SSH.

Related Topics

- Managing Local User Accounts, on page 7
- RADIUS User Authentication, on page 9
- Configuring External Authentication through an LDAP Server

Managing Local User Accounts

You can define any number of users locally on the Web Security appliance.

The default system admin account has all administrative privileges. You can change the admin account passphrase, but you cannot edit or delete this account.

Note If you have lost the admin user passphrase, contact your Cisco support provider.

Adding Local User Accounts

Before you begin

Define the passphrase requirements that all user accounts must follow. See Setting Passphrase Requirements for Administrative Users , on page 11.

Step 1 Choose **System Administration > Users.**

Step 2 Click **Add User**

Step 3 Enter a username, noting the following rules:

- Usernames can contain lowercase letters, numbers, and the dash (-) character, but cannot begin with a dash.
- Usernames cannot greater than 16 characters.
- Usernames cannot be special names that are reserved by the system, such as “operator” or “root.”
- If you also use external authentication, usernames should not duplicate externally-authenticated usernames.

Step 4 Enter a full name for the user.

Step 5 Select a user type.

User Type	Description
Administrator	Allows full access to all system configuration settings. However, the `upgradecheck` and `upgradeinstall` CLI commands can be issued only from the system defined “admin” account.
Operator	Restricts users from creating, editing, or removing user accounts. The operators group also restricts the use of the following CLI commands: • `resetconfig` • `upgradecheck` • `upgradeinstall` The operators group restricts the use of System Setup Wizard as well.

User Type	Description
Read-Only Operator	User accounts with this role: • Can view configuration information. • Can make and submit changes to see how to configure a feature, but they cannot commit them. • Cannot make any other changes to the appliance, such as clearing the cache or saving files. • Cannot access the file system, FTP, or SCP.
Guest	The guests group users can only view system status information, including reporting and tracking.

Step 6 Enter or generate a passphrase.

Step 7 Submit and commit your changes.

Deleting User Accounts

Step 1 Choose **System Administration > Users**.

Step 2 Click the trash can icon corresponding to the listed user name and confirm when prompted.

Step 3 Submit and commit your changes.

Editing User Accounts

Step 1 Choose **System Administration > Users**.

Step 2 Click the user name.

Step 3 Make changes to the user on the Edit User page as required.

Step 4 Submit and commit your changes.

Changing Passphrases

To change the passphrase of the account currently logged in, select **Options > Change Passphrase** from the top right-hand side of the window.

For other accounts, edit the account and change the passphrase in the Local User Settings page.

Related Topics

- Editing User Accounts, on page 8
- Setting Passphrase Requirements for Administrative Users , on page 11

RADIUS User Authentication

The Web Security appliance can use a RADIUS directory service to authenticate users that log in to the appliance using HTTP, HTTPS, SSH, and FTP. You can configure the appliance to contact multiple external servers for authentication, using either PAP or CHAP authentication. You can map groups of external users to different Web Security appliance user role types.

Sequence of Events For Radius Authentication

When external authentication is enabled and a user logs into the Web Security appliance, the appliance:

1. Determines if the user is the system-defined “admin” account.
2. If not, checks the first configured external server to determine if the user is defined there.
3. If the appliance cannot connect to the first external server, it checks the next external server in the list.
4. If the appliance cannot connect to any external server, it tries to authenticate the user as a local user defined on the Web Security appliance.
5. If the user does not exist on any external server or on the appliance, or if the user enters the wrong passphrase, access to the appliance is denied.

Enabling External Authentication Using RADIUS

Step 1 On the **System Administration > Users** page, click **Enable External Authentication**.

Step 2 Choose **RADIUS** as the Authentication Type.

Step 3 Enter the host name, port number, and Shared Secret passphrase for the RADIUS server. Default port is `1812`.

Step 4 Enter the number of seconds the appliance is to wait for a response from the server before timing out.

Step 5 Choose the authentication protocol used by the RADIUS server.

Step 6 (Optional) Click **Add Row** to add another RADIUS server. Repeat **Steps 1 – 5** for each RADIUS server.

Note You can add up to ten RADIUS servers.

Step 7 In the **External Authentication Cache Timeout** field, enter the number of seconds AsyncOS stores the external authentication credentials before contacting the RADIUS server again to re-authenticate. Default is zero.

Note If the RADIUS server uses one-time passphrases, for example passphrases created from a token, enter zero (0). When the value is set to zero, AsyncOS does not contact the RADIUS server again to authenticate during the current session.

Step 8 Configure Group Mapping—Select whether to map all externally authenticated users to the Administrator role or to different appliance-user role types.

Setting	Description
Map externally authenticated users to multiple local roles.	Enter a group name as defined in the RADIUS CLASS attribute, and choose an appliance Role type. You can add more role mappings by clicking Add Row. AsyncOS assigns RADIUS users to appliance roles based on the RADIUS CLASS attribute. CLASS attribute requirements: • three-character minimum • 253-character maximum • no colons, commas, or newline characters • one or more mapped CLASS attributes for each RADIUS user (With this setting, AsyncOS denies access to RADIUS users without a mapped CLASS attribute.) For RADIUS users with multiple CLASS attributes, AsyncOS assigns the most restrictive role. For example, if a RADIUS user has two CLASS attributes, which are mapped to the Operator and Read-Only Operator roles, AsyncOS assigns the RADIUS user to the Read-Only Operator role, which is more restrictive than the Operator role. These are the appliance roles ordered from most restrictive to least restrictive: • Administrator • Operator • Read-Only Operator • Guest
Map all externally authenticated users to the Administrator role.	AsyncOS assigns all RADIUS users to the Administrator role.

Step 9 Submit and commit your changes.

What to do next

Related Topics

- External Authentication
- Adding Local User Accounts, on page 7.

Defining User Preferences

Preference settings, such as reporting display formats, are stored for each user and are the same regardless from which client machine the user logs into the appliance.

Step 1 Choose **Options > Preferences**.

Step 2 On the User Preferences page, click **Edit Preferences**.

Step 3 Configure the preference settings as required.

Preference Setting	Description
Language Display	The language AsyncOS for Web uses in the web interface and CLI.
Landing Page	The page that displays when the user logs into the appliance.
Reporting Time Range Displayed (default)	The default time range that displays for reports on the Reporting tab.
Number of Reporting Rows Displayed	The number of rows of data shown for each report by default.

Step 4 Submit and commit your changes.

Configuring Administrator Settings

Setting Passphrase Requirements for Administrative Users

To set passphrase requirements for locally-defined administrative users of the appliance:

Step 1 Select **System Administration > Users**.

Step 2 In the **Passphrase Settings** section, click **Edit Settings**.

Step 3 Choose options:

Option	Description
List of words to disallow in passphrases	Create a .txt file with each forbidden word on a separate line, then select the file to upload it. Subsequent uploads overwrite previous uploads.

Option	Description
Passphrase Strength	You can display a passphrase-strength indicator when an administrative user enters a new passphrase. This setting does not enforce creation of strong passphrases, it merely shows how easy it is to guess the entered passphrase. Select the roles for which you wish to display the indicator. Then, for each selected role, enter a number greater than zero. A larger number means that a passphrase that registers as strong is more difficult to achieve. This setting has no maximum value, but a very high number makes it effectively impossible to enter a passphrase that evaluates as "good." Experiment to see what number best meets your requirements. Passphrase strength is measured on a logarithmic scale. Evaluation is based on the U.S. National Institute of Standards and Technology rules of entropy as defined in NIST SP 800-63, Appendix A. Generally, stronger passphrases: • Are longer • Include upper case, lower case, numeric, and special characters • Do not include words in any dictionary in any language. To enforce passphrases with these characteristics, use the other settings on this page.

Step 4 Submit and commit your changes.

Additional Security Settings for Accessing the Appliance

You can use the CLI command `adminaccessconfig` to configure the Web Security appliance to have stricter access requirements for administrators logging into the appliance.

Command	Description
`adminaccessconfig > banner`	Configures the appliance to display any text you specify when an administrator tries to log in. The custom log-in banner appears when an administrator accesses the appliance through any interface; for example, via the Web UI, CLI, or FTP. You can load the custom text either by pasting it into the CLI prompt, or by copying it from a text file located on the Web Security appliance. To upload the text from a file, you must first transfer the file to the configuration directory on the appliance using FTP.
`adminaccessconfig > welcome`	This is a post-log-in banner, displayed after successful administrator log-in. This text is added to the appliance configuration by the same means as the log-in `adminaccessconfig > banner` text.

Command	Description
`adminaccessconfig > ipaccess`	Controls from which IP addresses administrators access the Web Security appliance. Administrators can access the appliance from any machine, or from machines with an IP address from a list you specify. When restricting access to an allow list, you can specify IP addresses, subnets, or CIDR addresses. By default, when you list the addresses that can access the appliance, the IP address of your current machine is listed as the first address in the allow list. You cannot delete the IP address of your current machine from the allow list. This information also can be provided using the Web UI; see User Network Access, on page 13.
`adminaccessconfig > csrf`	Enable/disable Web UI cross-site request forgery protection, used to identify and protect against malicious or spoofed requests. For best security, it is recommended that CSRF protection be enabled.
`adminaccessconfig > hostheader`	Configure use of host header in HTTP requests. By default, the Web UI responds with the host header sent by the Web client in an HTTP request. For increased security, you can configure the Web UI to respond with only the appliance-specific host name; that is, the appliance's configured name (for example, `wsa_04.local`).
`adminaccessconfig > timeout`	Provide an inactivity time-out interval; that is, the number of minutes users can be inactive before being logged out. This value can be between five and 1440 minutes (24 hours); the default value is 30 minutes. This information also can be provided using the Web UI; see User Network Access, on page 13.
`adminaccessconfig > strictssl`	Configures the appliance so administrators log into the web interface on port 8443 using stronger SSL ciphers (greater than 56 bit encryption). When you configure the appliance to require stronger SSL ciphers, the change only applies to administrators accessing the appliance using HTTPS to manage the appliance. It does not apply to other network traffic connected to the Web Proxy using HTTPS.

User Network Access

You can specify how long a user can be logged into the appliance before AsyncOS logs the user out due to inactivity. You also can specify the type of user connections allowed.

The session timeout applies to all users, including administrators, logged into either the Web UI or the CLI. When AsyncOS logs a user out, the user is redirected to the appliance log-in page.

Note You also can use the CLI `adminaccessconfig > timeout` to set this time-out value.

Step 1 Choose **System Administration** > **Network Access**.

Step 2 Click **Edit Settings**.

Step 3 In the **Session Inactivity Timeout** field, enter the number of minutes users can be inactive before being logged out.

You can define a time-out interval between five and 1440 minutes (24 hours); the default value is 30 minutes.

Step 4 In the **User Access** section, you control users' system access: choose either **Allow Any Connection** or **Only Allow Specific Connections**.

If you choose **Only Allow Specific Connections**, define the specific connections as IP addresses, IP ranges, or CIDR ranges. Along with the client IP address, the appliance IP address is automatically added in the **User Access** section.

Step 5 Submit and commit your changes.

Resetting the Administrator Passphrase

Before you begin

- If you do not know the passphrase for the admin account, contact your customer support provider to reset the passphrase.
- Understand that changes to the passphrase take effect immediately and do not require you to commit the change.

Any administrator-level user can change the passphrase for the "admin" user.

Step 1 Select **Management Appliance** > **System Administration** > **Users**.

Step 2 Click the **admin** link in the Users list.

Step 3 Select **Change the passphrase**.

Step 4 Generate or enter the new passphrase.

Configuring the Return Address for Generated Messages

You can configure the return address for mail generated by AsyncOS for reports.

Step 1 Choose **System Administration > Return Addresses**.

Step 2 Click **Edit Settings**.

Step 3 Enter the display name, user name, and domain name.

Step 4 Submit and commit your changes.

Managing Alerts

Alerts are email notifications containing information about events occurring on the Cisco Web Security Appliance appliance. These events can be of varying levels of importance (or severity) from minor (Informational) to major (Critical) and pertain generally to a specific component or feature on the appliance.

Note To receive alerts and email notifications, you must configure the SMTP relay host that the appliance uses to send the email messages.

Alert Classifications and Severities

The information contained in an alert is determined by an alert classification and a severity. You can specify which alert classifications, at which severity, are sent to any alert recipient.

Alert Classifications

AsyncOS sends the following types of alert:

- System
- Hardware
- Updater
- Web Proxy
- Anti-Malware
- L4 Traffic Monitor
- External URL Categories
- Policy Expiration

Alert Severities

Alerts can be sent for the following severities:

- **Critical**: Requires immediate attention.
- **Warning**: Problem or error requiring further monitoring and potentially immediate attention.
- **Information**: Information generated in the routine functioning of this device.

Managing Alert Recipients

Note If you enabled AutoSupport during System Setup, the email address you specified will receive alerts for all severities and classes by default. You can change this configuration at any time.

Adding and Editing Alert Recipients

Step 1 Choose **System Administration > Alerts**.

Step 2 Click on a recipient in the Alert Recipients list to edit it, or click **Add Recipient** to add a new recipient.

Step 3 Add or edit the recipient's email address. You can enter multiple addresses, separated by commas.

Step 4 Select which alert severities to receive for each alert type.

Step 5 Submit and commit your changes.

Deleting Alert Recipients

Step 1 Choose **System Administration > Alerts**.

Step 2 Click the trash can icon corresponding to the alert recipient in the Alert Recipient listing and confirm.

Step 3 Commit your changes.

Configuring Alert Settings

Alert settings are global settings, meaning that they affect how all of the alerts behave.

Step 1 Choose **System Administration > Alerts**.

Step 2 Click **Edit Settings**.

Step 3 Configure the alert settings as required.

Option	Description
From Address to Use When Sending Alerts	The RFC 2822 compliant “Header From:” address to use when sending alerts. An option is provided to automatically generate an address based on the system hostname (“alert@<hostname>”)
Wait Before Sending a Duplicate Alert	Specifies the time interval for duplicate alerts. There are two settings: **Initial Number of Seconds to Wait Before Sending a Duplicate Alert**. If you set this value to 0, duplicate alert summaries are not sent and instead, all duplicate alerts are sent without any delay (this can lead to a large amount of email over a short amount of time). The number of seconds to wait between sending duplicate alerts (alert interval) is increased after each alert is sent. The increase is the number of seconds to wait plus twice the last interval. So a 5 second wait would have alerts sent at 5 seconds, 15, seconds, 35 seconds, 75 seconds, 155 seconds, 315 seconds, etc. **Maximum Number of Seconds to Wait Before Sending a Duplicate Alert**. You can set a cap on the number of seconds to wait between intervals via the maximum number of seconds to wait before sending a duplicate alert field. For example, if you set the initial value to 5 seconds, and the maximum value to 60 seconds, alerts would be sent at 5 seconds, 15 seconds, 35 seconds, 60 seconds, 120 seconds, etc

Option	Description
Cisco AutoSupport	Specifies whether to send Cisco the following support information: • a copy of all alert messages generated by the system • weekly reports noting the uptime of the system, the output of the status command, and the AsyncOS version used. Also specifies whether or not to send internal alert recipients a copy of every message sent to Cisco. This applies only to recipients that are set to receive System alerts at Information severity level.

Step 4 Submit and commit your changes.

Alert Listing

The following sections list alerts by classification. The table in each section includes the alert name (internally used descriptor), actual text of the alert, description, severity (critical, information, or warning) and the parameters (if any) included in the text of the message.

Feature Key Alerts

The following table contains a list of the various feature key alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
A "$feature" key was downloaded from the key server and placed into the pending area. EULA acceptance required.	Information.	**$feature:** Name of the feature.
Your "$feature" evaluation key has expired. Please contact your authorized sales representative.	Warning.	**$feature:** Name of the feature.
Your "$feature" evaluation key will expire in under $days day(s). Please contact your authorized sales representative.	Warning.	**$feature:** Name of the feature. **$days:** The number of days that will pass before the feature key will expire.

Hardware Alerts

The following table contains a list of the various hardware alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
A RAID-event has occurred: $error	Warning	**$error:** Text of the RAID error.

Logging Alerts

The following table contains a list of the various logging alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
$error.	Information.	**$error:** The traceback string of the error.
Log Error: Subscription $name: Log partition is full.	Critical.	**$name:** Log subscription name.
Log Error: Push error for subscription $name: Failed to connect to $ip: $reason.	Critical.	**$name:** Log subscription name. **$ip:** IP address of the remote host. **$reason:** Text describing the connect error
Log Error: Push error for subscription $name: An FTP command failed to $ip: $reason.	Critical.	**$name:** Log subscription name. **$ip:** IP address of the remote host. **$reason:** Text describing what went wrong.
Log Error: Push error for subscription $name: SCP failed to transfer to $ip:$port: $reason',	Critical.	**$name:** Log subscription name. **$ip:** IP address of the remote host. **$port:** Port number on the remote host. **$reason:** Text describing what went wrong.
Log Error: 'Subscription $name: Failed to connect to $hostname ($ip): $error.	Critical.	**$name:** Log subscription name. **$hostname:** Hostname of the syslog server. **$ip:** IP address of the syslog server. **$error:** Text of the error message.
Log Error: Subscription $name: Network error while sending log data to syslog server $hostname ($ip): $error	Critical.	**$name:** Log subscription name. **$hostname:** Hostname of the syslog server. **$ip:** IP address of the syslog server. **$error:** Text of the error message.

Message	Alert Severity	Parameters
Subscription $name: Timed out after $timeout seconds sending data to syslog server $hostname ($ip).	Critical.	**$name:** Log subscription name. **$timeout:** Timeout in seconds. **$hostname:** Hostname of the syslog server. **$ip:** IP address of the syslog server.
Subscription $name: Syslog server $hostname ($ip) is not accepting data fast enough.	Critical.	**$name:** Log subscription name. **$hostname:** Hostname of the syslog server. **$ip:** IP address of the syslog server.
Subscription $name: Oldest log file(s) were removed because log files reached the maximum number of $max_num_files. Files removed include: $files_removed.	Information.	**$name:** Log subscription name. **$max_num_files:** Maximum number of files allowed per log subscription. **$files_removed:** List of files that were removed.

Reporting Alerts

The following table contains a list of the various reporting alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	Critical.	Not applicable.
The reporting system is now able to handle new data.	Information.	Not applicable.
A failure occurred while building periodic report '$report_title'. This subscription should be examined and deleted if its configuration details are no longer valid.	Critical.	**$report_title:** Title of the report.
A failure occurred while emailing periodic report '$report_title'. This subscription has been removed from the scheduler.	Critical.	**$report_title:** Title of the report.

Message	Alert Severity	Parameters
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	Warning.	**$threshold:** Threshold value.
PERIODIC REPORTS: While building periodic report $report_title' the expected domain specification file could not be found at '$file_name'. No reports were sent.	Critical.	**$report_title:** Title of the report. **$file_name:** Name of the file.
Counter group "$counter_group" does not exist.	Critical.	**$counter_group:** Name of the counter_group.
PERIODIC REPORTS: While building periodic report $report_title' the domain specification file '$file_name' was empty. No reports were sent.	Critical.	**$report_title:** Title of the report. **$file_name:** Name of the file.
PERIODIC REPORTS: Errors were encountered while processing the domain specification file '$file_name' for the periodic report '$report_title'. Any line which has any reported problem had no report sent. $error_text	Critical.	**$report_title:** Title of the report. **$file_name:** Name of the file. **$error_text:** List of errors encountered.
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	Warning.	**$threshold:** Threshold value.
The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: $err_msg	Critical.	**$err_msg:** Error message text.

System Alerts

The following table contains a list of the various system alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
Startup script $name exited with error: $message	Critical.	**$name:** Name of the script. **$message:** Error message text.
System halt failed: $exit_status: $output',	Critical.	**$exit_status:** Exit code of the command. **$output:** Output from the command.
System reboot failed: $exit_status: $output	Critical.	**$exit_status:** Exit code of the command. **$output:** Output from the command.
Process $name listed $dependency as a dependency, but it does not exist.	Critical.	**$name:** Name of the process. **$dependency:** Name of the dependency that was listed.
Process $name listed $dependency as a dependency, but $dependency is not a wait_init process.	Critical.	**$name:** Name of the process. **$dependency:** Name of the dependency that was listed.
Process $name listed itself as a dependency.	Critical.	**$name:** Name of the process.
Process $name listed $dependency as a dependency multiple times.	Critical.	**$name:** Name of the process. **$dependency:** Name of the dependency that was listed.
Dependency cycle detected: $cycle.	Critical.	**$cycle:** The list of process names involved in the cycle.
An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider: Error: $error.	Warning.	**$error:** The error message associated with the exception.
There is an error with “$name”.	Critical.	**$name:** Name of the process that generated a core file.
An application fault occurred: “$error”	Critical.	**$error:** Text of the error, typically a traceback.

Message	Alert Severity	Parameters
Appliance: $appliance, User: $username, Source IP: $ip, Event: Account locked due to X failed login attempts. User $username is locked after X consecutive login failures. Last login attempt was from $ip.	Information.	**$appliance**: Identifier of the specific WSA. **$username**: Identifier of the specific user account. **$ip**: - IP address from which the login attempt occurred.
Tech support: Service tunnel has been enabled, port $port	Information.	**$port:** Port number used for the service tunnel.
Tech support: Service tunnel has been disabled.	Information.	Not applicable.
• The host at $ip has been added to the blacklist because of an SSH DOS attack. • The host at $ip has been permanently added to the ssh whitelist. • The host at $ip has been removed from the blacklist	Warning.	**$ip** - IP address from which a login attempt occurred. **Description:** IP addresses that try to connect to the appliance over SSH but do not provide valid credentials are added to the SSH blacklist if more than 10 failed attempts occur within two minutes. When a user logs in successfully from the same IP address, that IP address is added to the whitelist. Addresses on the whitelist are allowed access even if they are also on the blacklist. Entries are automatically removed from the blacklist after about a day.

Updater Alerts

The following table contains a list of the various updater alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.	Warning.	**$app:** Web Security appliance security service name. **$attempts:** Number of attempts tried.
The updater has been unable to communicate with the update server for at least $threshold.	Warning.	**$threshold:** Threshold value time.

Message	Alert Severity	Parameters
Unknown error occurred: $traceback.	Critical.	**$traceback:** Traceback information.

Anti-Malware Alerts

For information about alerts related to Advanced Malware Protection, see Ensuring That You Receive Alerts About Advanced Malware Protection Issues.

Policy Expiration Alerts

The following table contains a list of the various Policy Expiration alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
'$PolicyType': '$GroupName' has been disbaled due to expiry configuration.	Information	**$PolicyType:** Access policy / decryption policy based on the web policy type. **$GroupName:**Policy group name.
'$PolicyType' : '$GroupName' will expire in days : 3.	Information	**$PolicyType:** Access policy / decryption policy based on the web policy type. **$GroupName:** Policy group name.

FIPS Compliance

Federal Information Processing Standards (FIPS) specify requirements for cryptographic modules that are used by all government agencies to protect sensitive but unclassified information. FIPS help ensure compliance with federal security and data privacy requirements. FIPS, developed by the National Institute for Standards and Technology (NIST), are for use when no voluntary standards exist to meet federal requirements.

The WSA achieves FIPS 140-2 compliance in FIPS mode using Cisco Common Cryptographic Module (C3M). By default, FIPS mode is disabled.

Related Topics

- FIPS Mode Problems

FIPS Certificate Requirements

FIPS mode requires that all enabled encryption services on the Web Security appliance use a FIPS-compliant certificate. This applies to the following encryption services:

- HTTPS Proxy
- Authentication

- Identity Provider for SaaS
- Appliance Management HTTPS Service
- Secure ICAP External DLP Configuration
- Identity Services Engine
- SSL Configuration
- SSH Configuration

Note The Appliance Management HTTPS Service must be configured with a FIPS Complaint certificate before FIPS mode can be enabled. The other encryption services need not be enabled.

A FIPS-compliant certificate must meet these requirements:

Certificate	Algorithm	Signature Algorithm	Notes
X509	RSA	sha1WithRSAEncryption sha256WithRSAEncryption	Cisco recommends a bit key size of 1024 for best decryption performance and sufficient security. A larger bit size will increase security, but impact decryption performance.

FIPS Certificate Validation

When you enable FIPS mode, the appliance performs the following certificate checks:

- All certificates uploaded to the WSA, whether by means of the UI or the `certconfig` CLI command, are validated to comply strictly with CC standards. Any certificate without a proper trust path in the WSA's trust store cannot be uploaded.
- Certificate Signature with a trusted path validation; Certificate/Public Key tampering with `basicConstrains` and `CAFlag` set validated for all signer certificates.
- OCSP validation is available to validate a certificate against a revocation list. This is configurable using the `certconfig` CLI command.

See also Strict Certificate Validation, on page 27.

Enabling or Disabling FIPS Mode

Before you begin

- Make a back-up copy of the appliance configuration; see Saving the Appliance Configuration File, on page 2
- Ensure the certificates to be used in FIPS mode use FIPS 140-2 approved public key algorithms (see FIPS Certificate Requirements, on page 23).

Note

- Changing the FIPS mode initiates a reboot of the appliance.
- When you disable FIPS mode, the SSL and SSH settings—which were automatically made FIPS-compliant when FIPS mode was enabled—are not reset to their default values. You must explicitly change these settings if you wish to allow a client using weaker SSH/SSL settings to connect. See SSL Configuration , on page 26 for additional information.

Step 1 Choose **System Administration > FIPS Mode**.

Step 2 Click **Edit Settings**.

Step 3 Check **Enable FIPS Compliance** to enable FIPS compliance.

When you check Enable FIPS Compliance, the **Enable encryption of Critical Sensitive Parameters (CSP)** check box is enabled.

Step 4 Check **Enable encryption of Critical Sensitive Parameters (CSP)** to enable encryption of configuration data such as passwords, authentication information, certificates, shared keys, and so on.

Step 5 Click **Submit**.

Step 6 Click **Continue** to allow the appliance to reboot.

System Date and Time Management

Setting the Time Zone

Step 1 Choose **System Administration > Time Zone**.

Step 2 Click **Edit Settings**.

Step 3 Select your region, country, and time zone or select the GMT offset.

Step 4 Submit and commit the changes.

Synchronizing the System Clock with an NTP Server

Cisco recommends that you set your Web Security appliance to track the current date and time by querying a Network Time Protocol (NTP) server, not by manually setting the time on the appliance. This is especially true if your appliance integrates with other devices. All integrated devices should use the same NTP server.

Step 1 Choose **System Administration > Time Settings**.

Step 2 Click **Edit Settings**.

Step 3 Select **Use Network Time Protocol** as the Time Keeping Method.

Step 4 Enter the fully qualified hostname or IP address of the NTP server, clicking **Add Row** as needed to add servers.

Step 5 (Optional) Choose the routing table associated with an appliance network interface type, either Management or Data, to use for NTP queries. This is the IP address from which NTP queries should originate.

Note This option is only editable if the appliance is using split routing for data and management traffic.

Step 6 Submit and commit your changes.

SSL Configuration

For enhanced security, you can enable and disable SSL v3 and various versions of TLS for several services. Disabling SSL v3 for all services is recommended for best security. By default, all versions of TLS are enabled, and SSL is disabled.

Note You also can use the `sslconfig` CLI command to enable or disable these features. See Web Security Appliance CLI Commands.

Step 1 Choose **System Administration > SSL Configuration**.

Step 2 Click **Edit Settings**.

Step 3 Check the corresponding boxes to enable SSL v3 and TLS v1.x for these services:

- **Appliance Management Web User Interface** – Changing this setting will disconnect all active user connections.
- **Proxy Services** – Includes HTTPS Proxy and Credential Encryption for Secure Client. This section also includes:
  - **Cipher(s) to Use** – You can enter additional cipher suites to be used with Proxy Services communications. Use colons (:) to separate the suites. To prevent use of a particular cipher, add an exclamation point (!) to the front of that string. For example, `!EXP-DHE-RSA-DES-CBC-SHA` .

    Be sure to enter only suites appropriate to the TLS/SSL versions you have checked. Refer to https://www.openssl.org/docs/manmaster/man1/ciphers.html for additional information, and cipher lists.

    The default cipher for AsyncOS versions 9.0 and earlier is `DEFAULT:+kEDH` . For AsyncOS versions 9.1 and later, it the default cipher is

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
    !AES256-SHA:DHE-RSA-AES128-SHA
    ```

    In both cases, this may change based on your ECDHE cipher selections.

    Note However, regardless of version, the default cipher does not change when you upgrade to a newer AsyncOS version. For example, when you upgrade from an earlier version to AsyncOS 9.1, the default cipher is `DEFAULT:+kEDH` . In other words, following an upgrade, you must update the current cipher suite yourself; Cisco recommends updating to

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
    !AES256-SHA:DHE-RSA-AES128-SHA
    ```

- **Disable TLS Compression (Recommended)** – You can check this box to disable TLS compression; this is recommended for best security.

- **Secure LDAP Services** – Includes Authentication, External Authentication and Secure Mobility.
- **Secure ICAP Services (External DLP)** – Select the protocol(s) used to secure ICAP communications between the appliance and external DLP (data loss prevention) servers. See Configuring External DLP Servers for more information.
- **Update Service** – Select the protocol(s) used for communications between the appliance and available update servers. See AsyncOS for Web Upgrades and Updates, on page 31 for more information about update services.

Note Cisco's Update servers do not support SSL v3, therefore TLS 1.0 or above must be enabled for the Cisco Update service. However, SSL v3 can still be used with a local update server, if it is so configured—you must determine which versions of SSL/TLS are supported on that server.

Step 4 Click **Submit**.

Certificate Management

The appliance uses digital certificates to establish, confirm and secure a variety of connections. The Certificate Management page lets you view and update current certificate lists, manage trusted root certificates, and view blocked certificates.

Related Topics

- About Certificates and Keys, on page 28
- Certificate Updates, on page 29
- Managing Trusted Root Certificates, on page 28
- Viewing Blocked Certificates, on page 29

Strict Certificate Validation

With the release of the FIPS-mode updates in AsyncOS 10.5, all presented certificates are validated strictly to comply with Common Criteria (CC) standards before uploading, and OCSP validation is available to validate certificates against a revocation list.

You must ensure that proper, valid certificates are uploaded to the WSA, and that valid, secure certificates are configured on all related servers to facilitate smooth SSL handshakes with those servers.

Strict certificate validation is applied for the following certificate uploads:

- HTTPS Proxy (Security Services > HTTPS Proxy)
- File Analysis Server (Security Services > Anti-Malware and Reputation > Advanced Settings for File Analysis > File Analysis Server: Private Cloud & Certificate Authority: Use Uploaded Certificate Authority)
- Trusted Root Certificates (Network > Certificate Management)
- Global Authentication Settings (Network > Authentication > Global Authentication Settings)

- Identity Provider for SaaS (Network > Identity Provider for SaaS)
- Identity Services Engine (Network > Identity Services Engine)
- External DLP Servers (Network > External DLP Servers)
- LDAP & Secure LDAP (Network > Authentication > Realm)

See also FIPS Compliance, on page 23.

About Certificates and Keys

When a browser prompts its user to authenticate, the browser sends the authentication credentials to the Web Proxy using a secure HTTPS connection. By default, the Web Security appliance uses the "Cisco Web Security Appliance Demo Certificate" that comes with it to create an HTTPS connection with the client. Most browsers will warn users that the certificate is not valid. To prevent users from seeing the invalid certificate message, you can upload a certificate and key pair that your applications recognize automatically.

Related Topics

- Uploading or Generating a Certificate and Key, on page 29
- Certificate Signing Requests, on page 30
- Intermediate Certificates, on page 31

Managing Trusted Root Certificates

The Web Security appliance ships with and maintains a list of trusted root certificates. Web sites with trusted certificates do not require decryption.

You can manage the trusted certificate list, adding certificates to it and functionally removing certificates from it. While the Web Security appliance does not delete certificates from the master list, it allows you to override trust in a certificate, which functionally removes the certificate from the trusted list.

To add, override or download a trusted root certificate:

Step 1 Choose **Network** > **Certificate Management**.

Step 2 Click **Manage Trusted Root Certificates** on the Certificate Management page.

Step 3 To add a custom trusted root certificate with a signing authority not on the Cisco-recognized list:

Click **Import** and then browse to, select, and **Submit** the certificate file.

Step 4 To override the trust for one or more Cisco-recognized certificates:

a) Check the **Override Trust** checkbox for each entry you wish to override.
b) Click **Submit**.

Step 5 To download a copy of a particular certificate:

a) Click the name of the certificate in the Cisco Trusted Root Certificate List to expand that entry.
b) Click **Download Certificate**.

Certificate Updates

The Updates section lists version and last-updated information for the Cisco trusted-root-certificate and blacklist bundles on the appliance. These bundles are updated periodically.

Click **Update Now** on the Certificate Management page to update all bundles for which updates are available.

Viewing Blocked Certificates

To view a list of certificates which Cisco has determined to be invalid, and has blocked:

Click **View Blocked Certificates**.

Uploading or Generating a Certificate and Key

Certain AsyncOS features require a certificate and key to establish, confirm or secure a connection Identity Services Engine (ISE) and . You can either upload an existing certificate and key, or you can generate one when you configure the feature.

Uploading a Certificate and Key

A certificate you upload to the appliance must meet the following requirements:

- It must use the X.509 standard.
- It must include a matching private key in PEM format. DER format is not supported.

Step 1 Select **Use Uploaded Certificate and Key**.

Step 2 In the **Certificate** field, click Browse; locate the file to upload.

Note The Web Proxy uses the first certificate or key in the file. The certificate file must be in PEM format. DER format is not supported.

Step 3 In the **Key** field, click Browse; locate the file to upload.

Note The key length must be 512, 1024, or 2048 bits. The private key file must be in PEM format. DER format is not supported.

Step 4 If the key is encrypted, select **Key is Encrypted**.

Step 5 Click **Upload Files**.

Generating a Certificate and Key

Step 1 Select **Use Generated Certificate and Key**.

Step 2 Click **Generate New Certificate and Key**.

a) In the Generate Certificate and Key dialog box, enter the necessary generation information.

Note You can enter any ASCII character except the forward slash (/) in the Common Name field.

b) Click **Generate** in the Generate Certificate and Key dialog box.

When generation is complete, the certificate information is displayed in the Certificate section, along with two links: **Download Certificate** and **Download Certificate Signing Request**. In addition, there is a Signed Certificate option that is used to upload the signed certificate when you receive it from the Certificate Authority (CA).

Step 3 Click **Download Certificate** to download the new certificate for upload to the appliance.

Step 4 Click **Download Certificate Signing Request** to download the new certificate file for transmission to a Certificate Authority (CA) for signing. See Certificate Signing Requests, on page 30 for more information about this process.

a) When the CA returns the signed certificate, click Browse in the Signed Certificate portion of the Certificate field to locate the signed-certificate file, and then click Upload File to upload it to the appliance.

b) Ensure the CA's root certificate is present in the appliance's list of trusted root certificates. If it is not, add it. See Managing Trusted Root Certificates, on page 28 for more information.

Certificate Signing Requests

The Web Security appliance cannot generate Certificate Signing Requests (CSR) for certificates uploaded to the appliance. Therefore, to have a certificate created for the appliance, you must issue the signing request from another system. Save the PEM-formatted key from this system because you will need to install it on the appliance later.

You can use any UNIX machine with a recent version of OpenSSL installed. Be sure to put the appliance hostname in the CSR. Use the guidelines at the following location for information on generating a CSR using OpenSSL:

`http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28`

Once the CSR has been generated, submit it to a certificate authority (CA). The CA will return the certificate in PEM format.

If you are acquiring a certificate for the first time, search the Internet for "certificate authority services SSL server certificates," and choose the service that best meets the needs of your organization. Follow the service's instructions for obtaining an SSL certificate.

Note You can also generate and sign your own certificate. Tools for doing this are included with OpenSSL, free software from `http://www.openssl.org` .

Intermediate Certificates

In addition to root certificate authority (CA) certificate verification, AsyncOS supports the use of intermediate certificate verification. Intermediate certificates are certificates issued by a trusted root CA which are then used to create additional certificates. This creates a chained line of trust. For example, a certificate may be issued by example.com who, in turn, is granted the rights to issue certificates by a trusted root CA. The certificate issued by example.com must be validated against example.com's private key as well as the trusted root CA's private key.

Servers send a "certificate chain" in an SSL handshake in order for clients (for example, browsers and in this case the WSA, which is a HTTPS proxy) to authenticate the server. Normally, the server certificate is signed by an intermediate certificate which in turn is signed by a trusted root certificate, and during the handshake, the server certificate and the entire certificate chain are presented to the client. As the root certificate is typically present in the Trusted Certificate store of the WSA, verification of the certificate chain is successful.

However, sometimes when the end-point entity certificate is changed on the server, necessary updates for the new chain are not performed. As a result, going forward the server presents only the server certificate during the SSL handshake and the WSA proxy is unable to verify the certificate chain since the intermediate certificate is missing.

Previously, the solution was manual intervention by the WSA administrator, who would upload the necessary intermediate certificate to the Trusted Certificate store. Now you can use the CLI command `advancedproxyconfig > HTTPS > Do you want to enable automatic discovery and download of missing Intermediate Certificates?` to enable "intermediate certificate discovery," a process the WSA uses in an attempt to eliminate the manual step in these situations.

Intermediate certificate discovery uses a method called "AIA chasing": when presented with an untrusted certificate, the WSA examines it for an extension named "Authority Information Access." This extension includes an optional CA Issuers URI field, which can be queried for the Issuer Certificate used to sign the server certificate in question. If it is available, the WSA fetches the issuer's certificate recursively until the root CA certificate is obtained, and then tries to verify the chain again.

AsyncOS for Web Upgrades and Updates

Cisco periodically releases upgrades (new software versions) and updates (changes to current software versions) for AsyncOS for Web and its components.

Best Practices For Upgrading AsyncOS for Web

- Before you start the upgrade, save the XML configuration file off the Web Security appliance from the **System Administration > Configuration File** page or by using the saveconfig command.
- Save other files stored on the appliance, such as PAC files or customized end-user notification pages.
- When upgrading, do not pause for long amounts of time at the various prompts. If the TCP session times out during the download, the upgrade may fail.
- After the upgrade completes, save the configuration information to an XML file.

Related Topics

- Saving, Loading, and Resetting the Appliance Configuration, on page 2

Upgrading and Updating AsyncOS and Security Service Components

Downloading and Installing an Upgrade

Before you begin

Save the appliance configuration file (see Saving, Loading, and Resetting the Appliance Configuration, on page 2).

Note When downloading and upgrading AsyncOS in a single operation from a local server instead of from a Cisco server, the upgrade installs immediately while downloading. A banner is displayed for 10 seconds at the beginning of the upgrade process. While this banner is displayed, you can type Control-C to exit the upgrade process before downloading starts.

Note While performing an upgrade, if the secure authentication certificate is not FIPs-complaint, it will be replaced with the default certificate of the latest path to which your appliance is upgraded to. This happens only when the customer has used the default certificate before the upgrade.

You can download and install in a single operation, or download in the background and install later.

Step 1 Choose **System Administration** > **System Upgrade**.

Step 2 Click **Upgrade Options**.

Select upgrade options and an upgrade image:

Setting	Description
Choose an upgrade option	• **Download and install** – Download and install the upgrade in a single operation. If you have already downloaded an installer, you will be prompted to overwrite the existing download. • **Download only** – Download an upgrade installer, but do not install. If you have already downloaded an installer, you will be prompted to overwrite the existing download. The installer downloads in the background without interrupting service. An **Install** button is displayed when the download is complete; click to install a previously downloaded upgrade.
	Select an upgrade image to be downloaded, or downloaded and installed, from the **List of available upgrade images files at upgrade server**.

Setting	Description
Upgrade Preparation	• To save a back-up copy of the current configuration to the `configuration` directory on the appliance, check **Save the current configuration to the configuration directory before upgrading**. • If the **Save current configuration** option is checked, you can check **Mask passwords in the configuration file** to have all current-configuration passwords masked in the back-up copy. However, you cannot load a configuration file with masked passwords using the **Load Configuration** command, nor with the CLI `loadconfig` command. If FIPS mode is enabled, you can select **Encrypt passphrases in the Configuration Files**. These files can be reloaded. • If the **Save current configuration** option is checked, you can enter one or more email addresses into the **Email file to** field; a copy of the back-up configuration file is mailed to each address. Separate multiple addresses with commas.

Step 3 Click **Proceed**.

If you are installing:

a) Be prepared to respond to prompts during the process.
b) At the completion prompt, click **Reboot Now**.
c) After about 10 minutes, access the appliance again and log in.

If you feel you need to power-cycle the appliance to troubleshoot an upgrade issue, do not do so until at least 20 minutes have passed since you rebooted.

Viewing Status of, Canceling, or Deleting a Background Download

Step 1 Choose **System Administration** > **System Upgrade**.

Step 2 Click **Upgrade Options**.

Step 3 Choose an option:

To	Do This
View download status	Look in the middle of the page. If there is no download in progress and no completed download waiting to be installed, you will not see download status information.
Cancel a download	Click the **Cancel Download** button in the middle of the page. This option appears only while a download is in progress.
Delete a downloaded installer	Click the **Delete File** button in the middle of the page. This option appears only if an installer has been downloaded.

Step 4 (Optional) View the Upgrade Logs.

What to do next

Related Topics

- Local And Remote Update Servers, on page 35

Automatic and Manual Update and Upgrade Queries

AsyncOS periodically queries the update servers for new updates to all security service components, but not for new AsyncOS upgrades. To upgrade AsyncOS, you must manually prompt AsyncOS to query for available upgrades. You can also manually prompt AsyncOS to query for available security service updates. For more information, see Reverting to a Previous Version of AsyncOS for Web, on page 38.

When AsyncOS queries an update server for an update or upgrade, it performs the following steps:

1. Contacts the update server.

   Cisco allows the following sources for update servers:

   - **Cisco update servers.** For more information, see Updating and Upgrading from the Cisco Update Servers, on page 35.
   - **Local server.** For more information, see Upgrading from a Local Server, on page 36.

2. Receives an XML file that lists the available updates or AsyncOS upgrade versions. This XML file is known as the "manifest."
3. Downloads the update or upgrade image files.

Manually Updating Security Service Components

By default, each security service component periodically receives updates to its database tables from the Cisco update servers. However, you can manually update the database tables.

Note Some updates are available on demand from the GUI pages related to the feature.

Tip View a record of update activity in the updater log file. Subscribe to the updater log file on the **System Administration > Log Subscriptions** page.

Note Updates that are in-progress cannot be interrupted. All in-progress updates must complete before new changes can be applied.

Step 1 Choose **System Administration > Upgrade and Update Settings**.

Step 2 Click **Edit Update Settings**.

Step 3 Specify the location of the update files.

Step 4 Initiate the update using the Update Now function key on the component page located on the Security Services tab. For example, Security Services > Web Reputation Filters page.

The CLI and the Web application interface may be sluggish or unavailable during the update process.

Local And Remote Update Servers

By default, AsyncOS contacts the Cisco update servers for both update and upgrade images and the manifest XML file. However, you can choose from where to download the upgrade and update images and the manifest file. Using a local update server for the images or manifest file for any of the following reasons:

- **You have multiple appliances to upgrade simultaneously.** You can download the upgrade image to a web server inside your network and serve it to all appliances in your network.
- **Your firewall settings require static IP addresses for the Cisco update servers.** The Cisco update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for updates and AsyncOS upgrades. For more information, see Configuring a Static Address for the Cisco Update Servers, on page 35.

Note Local update servers do not automatically receive security service updates, only AsyncOS upgrades. After using a local update server for upgrading AsyncOS, change the update and upgrade settings back to use the Cisco update servers so the security services update automatically again.

Updating and Upgrading from the Cisco Update Servers

A Web Security appliance can connect directly to Cisco update servers and download upgrade images and security service updates. Each appliance downloads the updates and upgrade images separately.

Configuring a Static Address for the Cisco Update Servers

The Cisco update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for updates and AsyncOS upgrades.

Step 1 Contact Cisco Customer Support to obtain the static URL address.

Step 2 Navigate to the **System Administration** > **Upgrade and Update Settings** page, and click **Edit Update Settings**.

Step 3 On the Edit Update Settings page, in the “Update Servers (images)” section, choose **Local Update Servers** and enter the static URL address received in step 1.

Step 4 Verify that Cisco Update Servers is selected for the “Update Servers (list)” section.

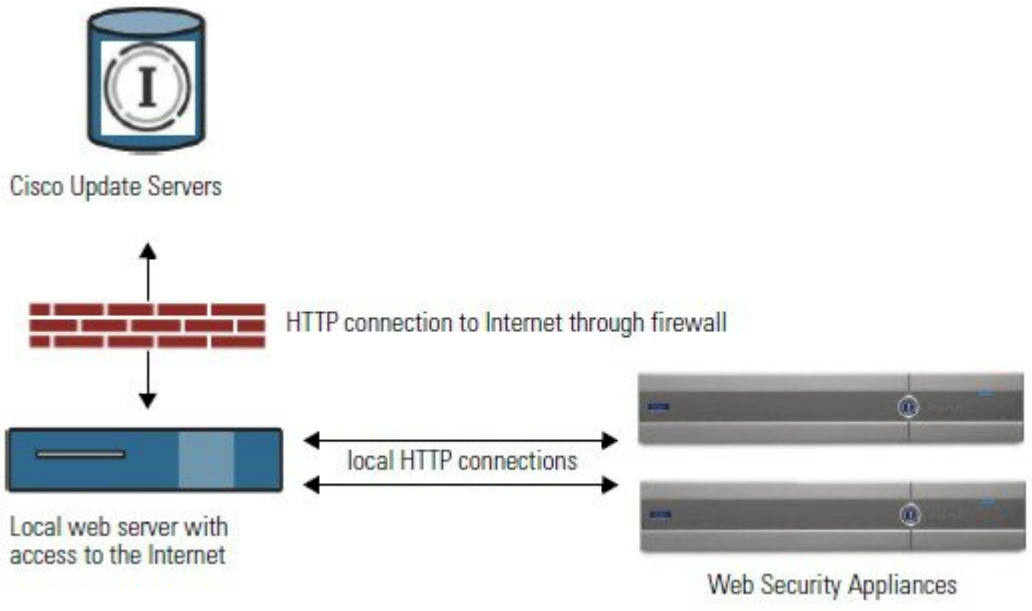
Step 5 Submit and commit your changes.

Upgrading from a Local Server

The Web Security appliance can download AsyncOS upgrades from a server within your network instead of obtaining upgrades directly from the Cisco update servers. When you use this feature, you download the upgrade image from Cisco once only, and then serve it to all Web Security appliances in your network.

The following figure shows how Web Security appliances download upgrade images from local servers.

Figure 1: Upgrading from a Local Server



Hardware and Software Requirements for Local Upgrade Servers

For *downloading* AsyncOS upgrade files, you must have a system in your internal network that has a web browser and Internet access to the Cisco update servers.

Note If you need to configure a firewall setting to allow HTTP access to this address, you must configure it using the DNS name and not a specific IP address.

For *hosting* AsyncOS upgrade files, a server on the internal network must have a web server, such as Microsoft IIS (Internet Information Services) or the Apache open source server, which has the following features:

- Supports the display of directory or filenames in excess of 24 characters.
- Has directory browsing enabled.
- Is configured for anonymous (no authentication) or Basic ("simple") authentication.
- Contains at least 350MB of free disk space for each AsyncOS upgrade image.

Configuring Upgrades from a Local Server

Note Cisco recommends changing the update and upgrade settings to use the Cisco update servers (using dynamic or static addresses) after the upgrade is complete to ensure the security service components continue to update automatically.

Step 1 Configure a local server to retrieve and serve the upgrade files.

Step 2 Download the upgrade zip file.

Using a browser on the local server, go to http://updates.ironport.com/fetch_manifest.html to download a zip file of an upgrade image. To download the image, enter your serial number (for a physical appliance) or VLN (for a virtual appliance) and the version number of the appliance. You will then be presented with a list of available upgrades. Click on the upgrade version that you want to download.

Step 3 Unzip the zip file in the root directory on the local server while keeping the directory structure intact.

Step 4 Configure the appliance to use the local server using the **System Administration > Upgrade and Update Settings** page or the updateconfig command.

Step 5 On the **System Administration > System Upgrade** page, click **Available Upgrades** or run the upgrade command.

Differences Between Local and Remote Upgrading Methods

The following differences apply when upgrading AsyncOS from a local server rather than from a Cisco update server:

- The upgrading installs immediately *while downloading* .
- A banner displays for 10 seconds at the beginning of the upgrade process. While this banner is displayed, you have the option to type Control+C to exit the upgrade process before downloading starts.

Configuring Upgrade and Service Update Settings

You can configure how the Web Security appliance downloads security services updates and AsyncOS for Web upgrades. For example, you can choose which network interface to use when downloading the files, configure the update interval or disable automatic updates.

Step 1 Choose **System Administration > Upgrade and Update Settings**.

Step 2 Click **Edit Update Settings**.

Step 3 Configure the settings, referencing the following information:

Setting	Description
Automatic Updates	Choose whether to enable automatic updates of the security components. If you choose automatic updates, enter the time interval. The default is enabled and the update interval is 5 minutes.

Setting	Description
Upgrade Notifications	Choose whether to display a notification at the top of the Web Interface when a new upgrade to AsyncOS is available. The appliance only displays this notification for administrators. For more information, see AsyncOS for Web Upgrades and Updates, on page 31.
Update Servers (list)	Whether to download the list of available upgrades and updates (the manifest XML file) from the Cisco update servers or a local web server. When you choose a local update server, enter the full path to the manifest XML file for the list including the file name and port number for the server. If you leave the port field blank, AsyncOS uses port 80. If the server requires authentication, you can also enter a valid user name and passphrase. • The URL for obtaining the manifest for hardware appliances is: https://update-manifests.ironport.com • The URL for obtaining the manifest for virtual appliances is: https://update-manifests.sco.cisco.com
Update Servers (images)	Whether to download upgrade and update images from the Cisco update servers or a local web server. When you choose a local update server, enter the base URL and port number for the server. If you leave the port field blank, AsyncOS uses port 80. If the server requires authentication, you can also enter a valid user name and passphrase.
Routing Table	Choose which network interface's routing table to use when contacting the update servers.
Proxy Server (optional)	If an upstream proxy server exists and requires authentication, enter the server information and user name and passphrase here.

Step 4 Submit and commit your changes.

What to do next

Related Topics

- Local And Remote Update Servers, on page 35
- Automatic and Manual Update and Upgrade Queries, on page 34
- Upgrading and Updating AsyncOS and Security Service Components, on page 32

Reverting to a Previous Version of AsyncOS for Web

AsyncOS for Web supports the ability to revert the AsyncOS for Web operating system to a previous qualified build for emergency uses.

Note You cannot revert to a version of AsyncOS for Web earlier than version 7.5.

Reverting AsyncOS on Virtual Appliances Impacts the License

If you revert to AsyncOS 8.0, there is no 180-day grace period during which the appliance processes web transactions without security features. License expiration dates are unaffected.

Configuration File Use in the Revert Process

Effective in version 7.5, when you upgrade to a later version, the upgrade process automatically saves the current system configuration to a file on the Web Security appliance. (However, Cisco recommends manually saving the configuration file to a local machine as a backup.) This allows AsyncOS for Web to load the configuration file associated with the earlier release after reverting to the earlier version. However, when it performs a reversion, it uses the current network settings for the management interface.

Reverting AsyncOS for an Appliance Managed by the SMA

You can revert AsyncOS for Web from the Web Security appliance. However, if the Web Security appliance is managed by a Security Management appliance, consider the following rules and guidelines:

- When Centralized Reporting is enabled on the Web Security appliance, AsyncOS for Web finishes transferring the reporting data to the Security Management appliance before it starts the reversion. If the files take longer than 40 seconds to transfer to the Security Management appliance, AsyncOS for Web prompts you to continue waiting to transfer the files, or continue the reversion without transferring all files.
- You must associate the Web Security appliance with the appropriate Configuration Master after reverting. Otherwise, pushing a configuration from the Security Management appliance to the Web Security appliance might fail.

Reverting AsyncOS for Web to a Previous Version

Caution Reverting the operating system on a Web Security appliance is a very destructive action and destroys all configuration logs and databases. Reversion also disrupts web traffic handling until the appliance is reconfigured. Depending on the initial Web Security appliance configuration, this action may destroy network configuration. If this happens, you will need physical local access to the appliance after performing the reversion.

Note If updates to the set of URL categories are available, they will be applied after AsyncOS reversion.

Before you begin

- Contact Cisco Quality Assurance to confirm that you can perform the intended reversion. (BS: this is a summary of the Available Versions section in the original chapter. Have asked if this is correct.)
- Back up the following information from the Web Security appliance to a separate machine:
  - System configuration file (with passphrases unmasked).
  - Log files you want to preserve.
  - Reports you want to preserve.
  - Customized end-user notification pages stored on the appliance.
  - PAC files stored on the appliance.

Step 1 Log into the CLI of the appliance you want to revert.

Note When you run the `revert` command in the next step, several warning prompts are issued. After these warning prompts are accepted, the revert action takes place immediately. Therefore, do not begin the reversion process until after you have completed the pre-reversion steps.

Step 2 Enter the `revert` command.

Step 3 Confirm twice that you want to continue with the reversion.

Step 4 Choose one of the available versions to revert to.

The appliance reboots twice.

Note The reversion process is time-consuming. It may take fifteen to twenty minutes before reversion is complete and console access to the appliance is available again.

The appliance should now run using the selected AsyncOS for Web version. You can access the web interface from a web browser.

Monitoring System Health and Status Using SNMP

The AsyncOS operating system supports system status monitoring via SNMP (Simple Network Management Protocol). (For more information about SNMP, see RFCs 1065, 1066, and 1067.)

Please note:

- SNMP is **off** by default.
- SNMP SET operations (configuration) are not implemented.
- AsyncOS supports SNMPv1, v2, and v3. For more information on SNMPv3, see RFCs 2571-2575.
- Message authentication and encryption are mandatory when enabling SNMPv3. Passphrases for authentication and encryption should be different. The encryption algorithm can be AES (recommended) or DES. The authentication algorithm can be SHA-1 (recommended) or MD5. The snmpconfig command “remembers” your passphrases the next time you run the command.
- The SNMPv3 username is: v3get.

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- If you use only SNMPv1 or SNMPv2, you must set a community string. The community string does not default to `public`.
- For SNMPv1 and SNMPv2, you must specify a network from which SNMP GET requests are accepted.
- To use traps, an SNMP manager (not included in AsyncOS) must be running and its IP address entered as the trap target. (You can use a host name, but if you do, traps will only work if DNS is working.)

MIB Files

MIB files are available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Use the latest version of each MIB file.

There are multiple MIB files:

- asyncoswebsecurityappliance-mib.txt — an SNMPv2 compatible description of the Enterprise MIB for Web Security appliances.
- ASYNCOS-MAIL-MIB.txt — an SNMPv2 compatible description of the Enterprise MIB for Email Security appliances.
- IRONPORT-SMI.txt — This "Structure of Management Information" file defines the role of the asyncoswebsecurityappliance-mib.

This release implements a read-only subset of MIB-II as defined in RFCs 1213 and 1907.

See https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html to know about monitoring CPU usage on the appliance using SNMP.

Enabling and Configuring SNMP Monitoring

To configure SNMP to gather system status information for the appliance, use the snmpconfig command in the command-line interface (CLI). After you choose and configure values for an interface, the appliance responds to SNMPv3 GET requests.

When you use SNMP monitoring, keep the following points in mind:

- These version 3 requests must include a matching passphrase.
- By default, version 1 and 2 requests are rejected.
- If enabled, version 1 and 2 requests must have a matching community string.

Hardware Objects

Hardware sensors conforming to the Intelligent Platform Management Interface Specification (IPMI) report information such as temperature, fan speed, and power supply status.

To determine the hardware-related objects available for monitoring (for example, the number of fans or the operating temperature range), see the hardware guide for your appliance model.

Related Topics

- Documentation Set

SNMP Traps

SNMP provides the ability to send traps, or notifications, to advise an administration application when one or more conditions have been met. Traps are network packets that contain data relating to a component of the system sending the trap. Traps are generated when a condition has been met on the SNMP agent (in this case, the Cisco Web Security Appliance appliance). After the condition has been met, the SNMP agent then forms an SNMP packet and sends it to the host running the SNMP management console software.

You can configure SNMP traps (enable or disable specific traps) when you enable SNMP for an interface.

To specify multiple trap targets: when prompted for the trap target, you may enter up to 10 comma separated IP addresses.

Related Topics

- About the connectivityFailure SNMP Trap , on page 42

About the connectivityFailure SNMP Trap

The connectivityFailure trap is intended to monitor your appliance's connection to the internet. It does this by attempting to connect and send an HTTP GET request to a single external server every 5 to 7 seconds. By default, the monitored URL is `downloads.ironport.com` on port 80.

To change the monitored URL or port, run the `snmpconfig` command and enable the connecivityFailure trap, even if it is already enabled. You will see a prompt to change the URL.

Tip To simulate connectivityFailure traps, you can use the `dnsconfig` CLI command to enter a non-working DNS server. Lookups for downloads.ironport.com will fail, and traps will be sent every 5-7 seconds. Be sure to change the DNS server back to a working server after completing your test.

CLI Example: snmpconfig

```
wsa.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP?
[Y]>

Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: wsa.example.com)
[1]>

Which port shall the SNMP daemon listen on interface "Management"?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
```

```
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 authentication passphrase.
[]>

Please enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>

Please enter the SNMPv3 privacy passphrase again to confirm.
[]>

Service SNMP V1/V2c requests?
[N]> Y

Enter the SNMP V1/V2c community string.
[ironport]> public

Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>

Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1

Enter the Trap Community string.
[ironport]> tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y

Do you want to disable any of these traps?
[Y]> n

Do you want to enable any of these traps?
[Y]> y
```

```
Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12

What threshold would you like to set for CPU utilization?
[95]>

What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>

What threshold would you like to set for memory utilization?
[95]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.
[snmp@localhost]> wsa-admin@example.com

Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: wsa-admin@example.com

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

wsa.example.com> commit

Please enter some comments describing your changes:
[]> Enable and configure SNMP

Changes committed: Fri Nov 06 18:13:16 2015 GMT
wsa.example.com>
```

Web Traffic Tap

Before You Begin: Enabling Web Traffic Tap feature will result in reduced transaction handling capacity (requests per second) for the appliance as appliance will need additional CPU cycles and memory to copy the messages to the tap interface.

Note For reducing the performance impact due to Web Traffic Tap feature, reduce the amount of traffic that gets tapped by setting appropriate Web Traffic Tap policies.

This feature is not supported on Amazon Web Services (AWS)

Web Traffic Tap feature allows you to tap the HTTP and HTTPS web traffic that passes through the appliance and copy it to a Web Security appliance interface in-line with the real time data traffic. You can select the Web Security appliance interface to which the tapped traffic data is sent. If the tapped traffic includes HTTPS data, the appliance decrypts them based on the decryption policies before sending them to the tap interface. See Decryption Policies.

The selected tap interface must be directly connected to an external security device for analysis, forensics, and archiving. Alternatively, it may be connected to a L2 switch on a dedicated VLAN.

Note The traffic mirrored on the tap interface is broadcast over Ethernet layer and not IP routable. Therefore a dedicated VLAN is required if connected to a L2 switch.

This feature also enables you to set Web Traffic Tap policies. Based on these customer defined policy filters, the appliance mirrors the web traffic that is available for the external security device. Web Traffic Tap feature provides visibility to the HTTPS traffic.

The term tapping refers to the reconstruction of complete TCP (Transmission Control Protocol) streams as if occurring between a directly connected client and server.

Virtual Web Security appliances support Web Traffic Tap feature.

Note The act of inspecting SSL traffic might be subject to corporate policy guidelines and/or national legislation. Cisco is not responsible for any legal obligations and it is your sole responsibility to ensure that your use of Web Traffic Tap feature on Web Security appliance is in accordance with any such legal or policy requirements.

You must perform the following procedures to tap the web traffic using the appliance:

1. Enable Web Traffic Tap feature
2. Configure Web Traffic Tap policies

Related Topics

- Enabling Web Traffic Tap, on page 45
- Configuring Web Traffic Tap Policies, on page 46

Enabling Web Traffic Tap

Before you begin

The Web Traffic Tap feature is disabled by default. You must enable the feature before you define the Web Traffic Tap policies using **Web Security Manager** > **Web Traffic Tap Policies**.

Note Decryption policies must be defined in order to tap HTTPS transactions. See Decryption Policies.

Step 1 Choose **Network** > **Web Traffic Tap**.

Step 2 Click **Edit Settings**.

Step 3 In the Edit Web Traffic Tap page, check the **Enable** check box to enable Web Traffic Tap feature.

Note To disable the Web Traffic Tap feature, uncheck the **Enable** check box. If you disable the Web Traffic Tap feature, you will not be able to view or edit the Web Traffic Tap policies. You must enable the feature again to view and edit the policies.

Step 4 From the Tap Interface drop-down list, choose the WSA interface to which the tapped traffic data is sent. The interface options are P1, P2, T1, and T2. See Connecting the Appliance to know about interfaces.

Note The selected tap interface must be directly connected to an external security device for analysis, forensics, and archiving. Alternatively, it may be connected to a L2 switch on a dedicated VLAN. The tap interface chosen should be connected and its status should be active; if not, mirroring of tapped traffic will fail.

Step 5 Click **Submit** and commit your changes.

Configuring Web Traffic Tap Policies

Step 1 Choose **Web Security Manager** > **Web Traffic Tap Policies**.

Step 2 Click **Add Policy**.

Follow the instructions in Creating a Policyto add a new Web Traffic Tap policy.

Note A Global Traffic Tap policy with no tapping set is available by default on the Web Traffic Tap Policies page (**Web Security Manager** > **Web Traffic Tap Policies**).

Step 3 Expand the Advanced section of the Policy Member Definition area to add the following additional group membership criteria for Web Traffic Tap.

- Protocols - Choose either HTTP or HTTPS protocol or both of them to create Web Traffic Tap Policy.

  Note You must define matching decryption policy (**Web Security Manager** > **Decryption Policies**) in order to tap HTTPS traffic.

  Web Traffic Tap policies do not support Native FTP and SOCKS protocols.

- Subnets
- URL Categories – Set **Tap** or **No Tap** for the URL Filtering categories as required. To set traffic tap for uncategorized URLs, choose **Tap** from the Uncategorized URLs drop-down list and click **Submit**.
- User Agents

See Creating a Policy to know more about defining additional group membership criteria.

Note The traffic that you want to tap must satisfy all the filter conditions that you have defined for the Web Traffic Tap policy.

You can also add URL categories from the URL Filtering table using **Web Security Manager** > **Web Traffic Tap Policies**.

Note If you have already added the URL categories in the Advanced section, you will see only those URL categories listed in the URL Filtering table (**Web Security Manager** > **Web Traffic Tap Policies**).

See Policy Order to know about the Web Traffic Tap policy order.