Introduction to the Product and the Release

This chapter contains the following sections:

- Introduction to the Web Security Appliance, on page 1
- What's New in AsyncOS 11.7, on page 2
- Related Topics, on page 4
- Using the Appliance Web Interface, on page 4
- Supported Languages, on page 7
- The Cisco SensorBase Network, on page 7

Introduction to the Web Security Appliance

The Cisco Web Security Appliance intercepts and monitors Internet traffic and applies policies to help keep your internal network secure from malware, sensitive data loss, productivity loss, and other Internet-based threats.

What's New in AsyncOS 11.7

Feature	Description
Improved Pre-classification Efficacy (Reducing File Uploads to Cisco AMP Threat Grid)	The File Analysis service in your appliance now supports all the file types supported by Cisco AMP Threat Grid. This has dual advantages. You can: • Upload files that only contain dynamic content for file analysis. This helps administrators to track the daily file upload limit. Previously, the on-box pre-classfication engine filtered the files with a limited scope before sending them for analysis. Now, a new cloud-based Threat Grid pre-classifcation engine is added to filter and remove low risk files. This improves efficacy by saving the submission limit for possible malicious files. • Reduce file uploads for file analysis. To configure this feature, see Enabling and Configuring File Reputation and Analysis Services. **Note** If you are using the private cloud file analysis server version 2.4 or an earlier version, it is recommended that you do not enable the new file types for file analysis. A new verdict – Low Risk is introduced when no dynamic content is found in a file after file analysis. You can view the verdict details in the Incoming Files Handed by AMP section of the Advanced Malware Protection report. **Note** The low risk files are not searchable in the File Analysis page in Reporting with their SHA because they are not sent for analysis to the AMP Threat Grid.

Feature	Description
ISE-PIC Integration	You can now configure your appliance to transparently identify users with ISE-PIC version 2.4 (with pxGrid version 2.0). ISE-PIC fetches user-identity information (user names and Active Directory groups) to allow transparent user identification in policies configured to use those profiles. **Note** • When you upgrade to AsyncOS 11.7 for Web Security appliances, you must reconfigure ISE for a successful integration. Any previously configured ISE functionality will not work until the ISE is reconfigured again. • AsyncOS 11.7 for Web Security appliances only supports ISE release 2.4. If the ISE versions in your deployment are older than ISE 2.4, continue to use AsyncOS releases for Web Security appliances earlier than 11.7. For more information, see Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service.
Encapsulated URL Protection	URL category filtering will be applied to all transactions that go through translate.google.com, further fortifying the ability to identify and take action on all transactions. You must enable the HTTPS proxy and choose to decrypt HTTPS requests.
Enhanced Web-based reputation score (WBRS) Engine	The WBRS engine is enhanced to improve the efficacy of web reputation and web category information for URLs.
Server Name Indication (SNI) Information in reports	The appliance now provides the SNI of pass-through HTTPS transactions, which enables you to search for transactions for a specific website in the Web Tracking page.
Support for 30 Feed Files in External Live Feed for Custom and External URL Categories	You can use up to 30 feed files with URL category definitions, with each file containing up to 5,000 entries. **Note** Increasing the number of external feed entries causes performance degradation.
Login History Configuration	A new subcommand **loginhistory** is added to the CLI command **adminaccessconfig** to configure the number of days for which the login history is retained. Default value is 1 day. This is available in FIPS and non-FIPS mode.

Feature	Description
Maximum Concurrent Login Sessions Configuration	A new subcommand **maxsessions** is added to the CLI command **adminaccessconfig** to configure the maximum number of concurrent sessions of the appliance through the Command Line Interface and web interface. Default value in FIPS mode is 3 and non-FIPS mode is 10.
Enhanced User Experience Using Walkthroughs	The appliance provides walkthroughs to assist you in accomplishing a particular configuration task. The following walkthroughs are supported in this release: • Authenticate end-users using Active Directory – NTLM • Authenticate end-users using Active Directory – Kerberos • Decrypt HTTPS traffic **Note** The list of walkthroughs is cloud updateable. Make sure that you clear your browser cache to view an updated version of the How-Tos widget and pop-up window. For information on how to enable the walkthroughs, see Additional Security Settings for Accessing the Appliance.
Support for Smart Software Licensing	Smart Software Licensing enables you to manage and monitor Cisco Web Security appliance licenses seamlessly. To activate Smart Software licensing, you must register your appliance with Cisco Smart Software Manager (CSSM), which is the centralized database that maintains the licensing details of all the Cisco products that you purchase and use. **Caution** After you enable the Smart Licensing feature on your appliance, you will not be able to roll back from Smart Licensing to Classic Licensing mode. For more information, see Smart Software Licensing.

Related Topics

- http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

Using the Appliance Web Interface

- Web Interface Browser Requirements, on page 5
- Enabling Access to the Web Interface on Virtual Appliances , on page 5
- Accessing the Appliance Web Interface, on page 5
- Committing Changes in the Web Interface, on page 7
- Clearing Changes in the Web Interface, on page 7

Web Interface Browser Requirements

To access the web interface, your browser must support and be enabled to accept JavaScript and cookies. It must be able to render HTML pages containing Cascading Style Sheets (CSS).

The Cisco Web Security Appliance follows the Target Environments set by YUI: http://yuilibrary.com/yui/environments/

Your session automatically times out after 30 minutes of inactivity.

Some buttons and links in the web interface cause additional windows to open. Therefore, you may need to configure the browser's pop-up blocking settings in order to use the web interface.

Note Only use one browser window or tab at a time to edit the appliance configuration. Also, do not edit the appliance using the web interface and the CLI at the same time. Editing the appliance from multiple places concurrently results in unexpected behavior and is not supported.

To access the GUI, your browser must support and be enabled to accept JavaScript and cookies, and it must be able to render HTML pages containing Cascading Style Sheets (CSS).

Conditional support is offered for Internet Explorer 6.0 and Opera 10.0.x on the Windows XP operating system and for Safari 3.1 on Mac OS X. Conditional support means that important functional bugs will be addressed, but minor or visual issues may not be corrected.

Browsers are supported only for operating systems officially supported by the browser.

You may need to configure your browser's pop-up blocking settings in order to use the GUI, because some buttons or links in the interface will cause additional windows to open.

Enabling Access to the Web Interface on Virtual Appliances

By default, the HTTP and HTTPS interfaces are not enabled on virtual appliances. To enable these protocols, you must use the command-line interface.

Step 1 Access the command-line interface. See Accessing the Command Line Interface.

Step 2 Run the `interfaceconfig` command.

Pressing Enter at a prompt accepts the default value.

Look for the prompts for HTTP and HTTPS and enable the protocol(s) that you will use.

Accessing the Appliance Web Interface

If you are using a virtual appliance, see Enabling Access to the Web Interface on Virtual Appliances , on page 5.

Step 1 Open a browser and enter the IP address (or hostname) of the Web Security appliance. If the appliance has not been previously configured, use the default settings:

`https://192.168.42.42:8443`

-or-

`http://192.168.42.42:8080`

where `192.168.42.42` is the default IP address, and `8080` is the default admin port setting for HTTP, and `8443` is default admin port for `HTTPS`.

Otherwise, if the appliance is currently configured, use the IP address (or host name) of the M1 port.

Note You must use a port number when connecting to the appliance (by default, port `8080`). Failing to specify a port number when accessing the web interface results in a default port 80, Proxy Unlicensed error page.

Step 2 [New Web Interface Only] Login to the legacy web interface and click **Web Security appliance is getting a new look. Try it!!** link to access the new web interface. When you click this link, it opens a new tab in your web browser and goes to `https://wsa_appliance.com:<trailblazer-https-port>/ng-login`, where `wsa_appliance.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

Note
- You must login to the legacy web interface of the appliance.
- Ensure that your DNS server can resolve the hostname of the appliance that you specified.
- By default, the new web interface needs TCP ports 6080, 6443 and 4431 to be operational. Ensure that these ports are not blocked in the enterprise firewall.
- The default port for accessing new web interface is 4431. This can be customized using `trailerblazerconfig` CLI command. For more information on the `trailblazerconfig` CLI command, see Web Security Appliance CLI Commands.
- The new web interface also needs AsyncOS API (Monitoring) ports for HTTP and HTTPS. By default these ports are 6080 and 6443. The AsyncOS API (Monitoring) ports can also be customized in the `interfaceconfig` CLI command. For more information on the `interfaceconfig` CLI command, see Web Security Appliance CLI Commands.
- If you change these default ports, then ensure that the customized ports for the new web interface too must not be blocked in the enterprise firewall.

Step 3 When the appliance login screen appears, enter your user name and passphrase to access the appliance.

By default, the appliance ships with the following user name and passphrase:

- User name: **admin**
- Passphrase: **ironport**

If this is the first time you have logged in with the default **admin** user name, you will be prompted to immediately change the passphrase.

Step 4 To view a listing of recent appliance access attempts, both successes and failures, for your user name, click the recent-activity icon (**i** or **!** for success or failure respectively) in front of the “Logged in as” entry in the upper right corner of the application window.

Committing Changes in the Web Interface

Step 1 Click the **Commit Changes** button.

Step 2 Enter comments in the Comment field if you choose.

Step 3 Click **Commit Changes**.

Note You can make multiple configuration changes before you commit all of them.

Clearing Changes in the Web Interface

Step 1 Click the **Commit Changes** button.

Step 2 Click **Abandon Changes**.

Supported Languages

AsyncOS can display its GUI and CLI in any of the following languages:

- German
- English
- Spanish
- French
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Chinese
- Taiwanese

The Cisco SensorBase Network

The Cisco SensorBase Network is a threat management database that tracks millions of domains around the world and maintains a global watch list for Internet traffic. SensorBase provides Cisco with an assessment of reliability for known Internet domains. The Web Security appliance uses the SensorBase data feeds to improve the accuracy of Web Reputation Scores.

SensorBase Benefits and Privacy

Participating in the Cisco SensorBase Network means that Cisco collects data and shares that information with the SensorBase threat management database. This data includes information about request attributes and how the appliance handles requests.

Cisco recognizes the importance of maintaining your privacy, and does not collect or use personal or confidential information such as usernames and passphrases. Additionally, the file names and URL attributes that follow the hostname are obfuscated to ensure confidentiality. When it comes to decrypted HTTPS transactions, the SensorBase Network only receives the IP address, web reputation score, and URL category of the server name in the certificate.

If you agree to participate in the SensorBase Network, data sent from your appliance is transferred securely using HTTPS. Sharing data improves Cisco's ability to react to web-based threats and protect your corporate environment from malicious activity.

Enabling Participation in The Cisco SensorBase Network

Note Standard SensorBase Network Participation is enabled by default during system setup.

Step 1 Choose **Security Services > SensorBase**.

Step 2 Verify that SensorBase Network Participation is enabled.

When it is disabled, none of the data that the appliance collects is sent back to the SensorBase Network servers.

Step 3 In the Participation Level section, choose one of the following levels:

- **Limited.** Basic participation summarizes server name information and sends MD5-hashed path segments to the SensorBase Network servers.
- **Standard.** Enhanced participation sends the entire URL with unobfuscated path segments to the SensorBase Network servers. This option assists in providing a more robust database, and continually improves the integrity of Web Reputation Scores.

Step 4 In the AnyConnect Network Participation field, choose whether or not to include information collected from clients that connect to the Web Security appliance using Cisco AnyConnect Client.

AnyConnect Clients send their web traffic to the appliance using the Secure Mobility feature.

Step 5 In the Excluded Domains and IP Addresses field, optionally enter any domains or IP addresses to exclude from traffic sent to the SensorBase servers.

Step 6 Submit and commit your changes.