Introduction

This topic contains the following sections:

About Secure Web Appliance

The Cisco Secure Web Appliance (SWA) 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. The Cisco Secure Web Appliance acts as a proxy server, intercepting web requests from users and scanning the requested web content for potential threats such as malware, viruses, and phishing attempts. It uses various security technologies such as URL filtering, antivirus scanning, reputation-based filtering, and advanced malware protection to ensure the security of web traffic. Overall, the Secure Web Appliance helps organizations secure their web traffic, enforce usage policies, and protect against web-based threats, contributing to a safer and more controlled web browsing environment for users.

What's New in AsyncOS 15.1

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>Mandatory Smart License for Secure Web Appliance</td><td>In AsyncOS 15.1 and later releases, Smart Software License is mandatory. Implementation of Smart License includes the following features:
Smart License is enabled by default when installing the Secure Web Appliance image from CCO.
You cannot upgrade to AsyncOS 15.1 build if the system administrator has not enabled the Smart Software License for the device.
The AsyncOS 15.1 and later releases do not support the classic license commands and UI options. These commands and UI options are not valid with the Cisco Smart License policy.
For more information, see Smart Software Licensing.</td></tr>
<tr><td>Cisco Secure Web Appliance integration with Cisco Umbrella</td><td>The integration of Cisco Umbrella and Cisco Secure Web Appliance facilitates deployment of common web policies from Umbrella to Secure Web Appliance. In addition, you can configure policies through the Umbrella dashboard and view logs.

When you configure the common web policies in the Umbrella Dashboard, the policies are pushed to Secure Web Appliance. The reporting data of those configured web policies are sent back to Umbrella and available on the Umbrella Dashboard. Reporting data includes information such as URLs browsed, their IP addresses, and whether the URL was permitted or blocked.

After successful integration, the following web policies get translated and pushed from Umbrella to Secure Web Appliance.
<table>
<tr><th>From Umbrella</th><th>To Secure Web Appliance</th></tr>
<tr><td>Ruleset Identities</td><td>Global Identification Profile</td></tr>
<tr><td>Destination Lists</td><td>Custom and External URL Categories</td></tr>
<tr><td>Web Policy (rules)</td><td>Access Policies</td></tr>
<tr><td>HTTPS Inspection</td><td>Decryption Policies</td></tr>
<tr><td>Microsoft 365 Compatibility</td><td>Custom and External URL Categories</td></tr>
<tr><td>Block Page settings in Ruleset</td><td>End-User Notification</td></tr>
<tr><td>Application Settings (CASI)</td><td>Applications Access Policies</td></tr>
</table>
For more information, see Integrate Cisco Secure Web Appliance with Cisco Umbrella.</td></tr>
</table>

Related Topics

- http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html
- https://docs.umbrella.com/umbrella-user-guide/docs/umbrella-integration-with-secure-web-appliance

Using the Appliance Web Interface

Web Interface Browser Requirements

Following are the requirements for accessing the web interface:

- Cookies and JavaScript must be supported and enabled by your browser.
- The browser must be able to render HTML pages that contain Cascading Style Sheets (CSS).
- The Cisco Secure Web 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 Use only 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).

Table 1: Supported Browsers and Releases

Browser	Windows 10	MacOS 10.6
Safari	—	7.0 and later
Google Chrome	Latest stable version	Latest stable version
Microsoft Internet Explorer	11.0	—

Browser	Windows 10	MacOS 10.6
Mozilla Firefox	Latest stable version	Latest stable version
Microsoft Edge	Latest stable version	Latest stable version

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.

You can access the legacy web interface of the appliance on any of the supported browsers.

The supported resolution for the new web interface of the appliance (AsyncOS 11.8 and later) is between 1280x800 and 1680x1050. The best viewed resolution for all supported browsers is 1440x900.

Note Cisco does not recommend viewing the new web interface of the appliance on higher resolutions.

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.

Press Enter at a prompt to accept the default value.

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

Look for the prompts for AsyncOS API (Monitoring) 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 4.

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

`ttps://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 **Secure Web 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 interface 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 Secure Web 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 Secure Web Appliance CLI Commands.

  Note The ports are enabled by default, but once these ports are disabled, they will be enabled again after the upgrade.

- 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 **Commit Changes**.

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 **Commit Changes**.

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 Cisco Secure Web 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 Cisco Secure Web 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.