



## 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 11.5, on page 1](#)
- [Related Topics, on page 3](#)
- [Using the Appliance Web Interface, on page 3](#)
- [Supported Languages, on page 5](#)
- [The Cisco SensorBase Network, on page 5](#)

## 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 11.5

Feature	Description
Cisco Cloudlock-specific Custom W3C Logs	<p>You can configure your appliance to send W3C access logs to the Cisco Cloudlock portal for analysis and reporting. These custom W3C logs provide better visibility into the SaaS usage of the customers. Cisco Cloudlock is a cloud-native CASB and cloud cybersecurity platform that protects users, data, and applications across Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service.</p> <p>See <a href="#">Configuring Cisco Cloudlock-specific Custom W3C Logs</a> for more information.</p>

Feature	Description
Cisco CTA-specific Custom W3C Logs Enhancements	<p>You can now configure and send the CTA-specific custom W3C logs to the CTA portal for analysis using the new Cisco Cognitive Threat Analytics page on the appliance's GUI.</p> <p>You can also choose to anonymize the user name, IP address, and user group field values of the log so that the client related information will not be disclosed to external systems like CTA to which the logs are pushed to.</p> <p>See <a href="#">Configuring Cisco CTA-specific Custom W3C Logs</a> for more information.</p>
Scheduled Policy Expiration	<p>You can now set the expiry time for Access and Decryption policies. The policies will be automatically disabled once they exceed the set expiry time. You will receive alerts 3 days prior to expiry and also on expiry.</p> <p>See <a href="#">Creating a Policy</a> and <a href="#">Policy Expiration Alerts</a> for more information.</p>
User Count Report	<p>The User Count page allows you to view information about the total number of authenticated and unauthenticated users of the appliance.</p> <p>See <a href="#">User Count Page</a> for more information.</p>
Anonymization and Deanonymization of W3C Log Fields	<p>You can now choose to anonymize the user name, IP address, and user group field values of the W3C logs so that the client related information will not be disclosed to external servers like CTA to which the logs are pushed to.</p> <p>If you want to view the actual values of the anonymized log field values, you must deanonymize the field values using the Deanonymization feature.</p> <p>See <a href="#">Adding and Editing Log Subscriptions</a> and <a href="#">Deanonymizing W3C Log Fields</a> for more information.</p>
AMP for Endpoints Console Integration	<p>You can now integrate your appliance with AMP for Endpoints console, and add your own blacklisted or whitelisted file SHAs.</p> <p>After the integration, when a file SHA is sent to the File Reputation server, the verdict obtained for the file SHA from the File Reputation Server is overridden by the verdict already available for the same file SHA in the AMP for Endpoints console.</p> <p>To integrate your appliance with AMP for Endpoints console, see <a href="#">Integrating the Appliance with AMP for Endpoints Console</a></p> <p>The Advanced Malware Protection Report page now includes a new section- <b>Malware Files by Category</b> to view the percentage of blacklisted file SHAs received from the AMP for Endpoints console. The threat name of a blacklisted file SHA is displayed as Simple Custom Detection in the Malware Threat Files section of the report. See <a href="#">File Reputation and File Analysis Report Pages</a></p>

Feature	Description
Advanced SSL Debugging	Cisco Web Security appliance now includes an OPENSSL command tool: <code>ssltool</code> . This command executes different OPENSSL commands from the appliance's CLI to troubleshoot SSL connections. The administrators can use this command to debug HTTPS/SSL/TLS issues.  See the <a href="#">Command Line Interface</a> chapter in the user guide or online help.

## 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 3
- [Enabling Access to the Web Interface on Virtual Appliances](#), on page 3
- [Accessing the Appliance Web Interface](#), on page 4
- [Committing Changes in the Web Interface](#), on page 4
- [Clearing Changes in the Web Interface](#), on page 5

## 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.

---

## 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 3.

---

**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** 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 3** 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.

---