# Introduction

This topic contains the following sections:



## About Web Security Appliance

## What's New in AsyncOS 11.8

| Feature | Description |
|---|---|
| ISE/ISE-PIC Integrations Enhancements | • You can construct access policies using Secure Group Tags and Active Directory groups.<br>• For users that fail transparent identification with ISE/ISE-PIC, you can configure fallback authentication with Active Directory based realms.<br>• You can configure authentication of users in Virtual Desktop Environments (Citrix, Microsoft shared/remote desktop services).<br>**Note** Fallback authentication for Virtual Desktop Environments (VDI) users is not supported.<br>For more information, see Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service. |

| Feature | Description |
|---|---|
| Domain Map | You can now configure the appliance to allow passthrough of specific HTTPS traffic without any modification to client requests and certificate checks of the destination servers.<br>For more information, see Domain Map.<br>For Domain Map feature, optional format specifiers for access logs and W3C logs are introduced. For more information, see Access Log Format Specifiers and W3C Log File Fields. |
| Rollback of Configuration of the appliance | A new CLI command `rollbackconfig` is added. Use this command to rollback to one of the previously committed 10 configurations. The rollback configuration feature is enabled by default.<br>For more information, see Web Security Appliance CLI Commands. |
| Automated Backup of the Appliance Configurations | A new log type 'Configuration History Logs' is added. Use this log type to subscribe for the configuration files and send them to a remotely located backup server through FTP or SCP.<br>For more information, see Log File Typesand Using Configuration History Logs. |
| Support for Exception List for External Feeds and O365 feeds | You can exclude sites and regular expressions from the feed file of the Custom and External URL categories. This is applicable only for External Live Feed Category.<br>For more information, see Creating and Editing Custom URL Categories. |
| Proxy Bypass Setting for O365 Web Services Feed | You can add the domain names or IP addresses of the Custom URL categories (O365 URLs) to the proxy bypass list. You do not need to add the domain names or the IP addresses of the Custom URL categories manually.<br>For more information, see Configuring Web Proxy Bypassing for Web Requests |
| Support for Cisco AMP Threat Grid Clustering for File Analysis | You can now add standalone or clustered Cisco AMP Threat Grid appliances for file analysis in the following way:<br>Security Services > File Reputation and Analysis page in the web interface.<br>For more information, seeEnabling and Configuring File Reputation and Analysis Services |

| Feature | Description |
|---|---|
| Configuring Threshold Settings for File Analysis | You can now set the upper threshold limit for the acceptable file analysis score.<br>The files that are blocked based on the Threshold Settings are displayed as Custom Threshold in the Incoming Malicious Threat Files section of the Advanced Malware Protection report.<br>For more information, see Enabling and Configuring File Reputation and Analysis Services |
| Configuring URL Filtering with Multiple Web Category | You can now configure the URL filtering engine with multiple URL categories. The multiple URL category feature is applicable only for access policies.<br>For more information, see Configuring the URL Filtering Engine |
| Support for New Threat Categories | The appliance now has new 22 threat categories. The list of the new threat categories is automatically updated in the appliance's new web interface whenever new categories are available.<br>For more information, see Release Notes for URL Category and Threat Category Updates for Cisco Web and Email Security Appliances'. |

| Feature | Description |
|---|---|
| New Web Interface for Monitoring and Tracking | The appliance now has a new web interface for Monitoring and Tracking reports.<br><br>In the **Monitoring** page, you can view reports classified under General reports and Threat reports.<br><br>In the **Tracking** page, you can search for messages or a group of messages depending on your search criteria in Tracking > Search page in the web interface. See "Tracking Messages" chapter in the User Guide.<br><br>**Note**<br>• You must login to the legacy web interface of the appliance.<br>• Ensure that your DNS server can resolve the hostname of the appliance that you specified.<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br><br>For more information, see Secure Appliance Reports on the New Web Interface.<br><br>To access the new web interface, see Accessing the Appliance Web Interface, on page 7 |

| Feature | Description |
|---|---|
| The `trailblazerconfig` CLI Command | You can use the `trailblazerconfig` command to route your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface.<br>**Note** By default, `trailblazerconfig` CLI command is enabled on your appliance. You can see the inline help by typing the command: `help trailblazerconfig`.<br>For more information, see Command Line Interface. |

# 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

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).

*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 | — |
| Mozilla Firefox | Latest Stable Version | Latest Stable Version |
| Microsoft Edge | Latest Stable Version | Latest Stable Version |

- Internet Explorer 11.0 (Windows 10 only)
- Safari (7 and later)
- Firefox (Latest Stable Version)
- Google Chrome (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 is 1440x900, for all the browsers.

**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.

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.

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 6.

**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:

`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 **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.
- 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.

  **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 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 Cisco 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 Cisco 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.