Release Notes for AsyncOS 14.6 for Cisco Secure Web Appliance with Hybrid SWG

First Published: 2023-05-11

Last Modified: 2023-08-02

About Secure Web Appliance

The Cisco Secure Web 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

What's New In AsyncOS 14.6.0-108—Limited Deployment

The following features are introduced for this release:

<table>
<tr><th>Feature</th><th colspan="2">Description</th></tr>
<tr><td rowspan="9">Cisco Umbrella</td><td colspan="2">AsyncOS Release 14.6 provides support for the integration of Cisco Umbrella with Cisco Secure Web Appliance. This integration facilitates the deployment of common web policies from Umbrella to Secure Web Appliance.
You cannot edit or delete Umbrella managed profiles on the Secure Web Appliance. You cannot create profiles or policies with names prefixed with 'umbrella <text>', for example ,abc.
The sequence of the policy rules in Umbrella are retained during policy translation to Secure Web Appliance.
The AD Users or AD Groups in Umbrella web policies should be configured in Secure Web Appliance policies as **Selected Groups and Users** in the **Policy Member Definition** section.
After successful integration, the following web policies get translated and pushed from Umbrella to Secure Web Appliance.</td></tr>
<tr><td>**From Umbrella**</td><td>**To Secure Web Appliance**</td></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 colspan="2">See Integrate Cisco Secure Web Appliance with Cisco Umbrella section in the user guide.</td></tr>
</table>

Prerequisites

Prerequisites for this release include:

- The Cisco Trusted Root Certificate Bundle: 2.2 must be updated on Secure Web Appliance to connect successfully to the Umbrella Hybrid service.
- The 107 URL categories should be updated for Secure Web Appliance to successfully configure policy pushes from the Umbrella service.
- The HTTPS protocol must be enabled manually in Secure Web Appliance.
- When AD is integrated with Umbrella, it is necessary to configure the AD realm manually in Secure Web Appliance.
- The Secure Web Appliance integration with the Hybrid Policy feature requires an active Umbrella Web Policy license.

Access the New Web Interface

The new web interface provides a new look for monitoring reports and tracking web services. To access the new web interface, do the following:

- Log in to the legacy web interface.
- Click **SecureWeb Appliance is getting a new look. Try it!!** that appears on the top of the UI.

This link opens a new tab in your web browser and directs you to `https://wsa01-enterprise.com:<trailblazer-https-port>/ng-login` , where `wsa01-enterprise.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance for accessing the new web interface.

Important!

- You must log in 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 by the enterprise firewall.
- The default port for accessing new web interface is 4431. This can be customized using the **trailblazerconfig** command. For more information about the **trailblazerconfig** command, see Command Line Interface.
- 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 using the **interfaceconfig** command. For more information about the **interfaceconfig** command, see Command Line Interface.
- If you change these default ports, ensure that the customized ports for the new web interface are not blocked by the enterprise firewall.
- The new web interface opens in a new browser window, and you must log in again to access it. If you want to log out of the appliance completely, you need to log out of both the new and legacy web interfaces of your appliance.
- For seamless navigation and rendering of HTML pages, Cisco recommends using the following browsers to access the new web interface of the appliance (AsyncOS 11.8 and later):
  - Google Chrome
  - Mozilla Firefox
- You can access the legacy web interface of the appliance with 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 1440 x 900, for all the browsers.

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

Release Classification

Each release is identified by the release type (ED - Early Deployment, GD - General Deployment, etc.) For an explanation of these terms, see http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdf.

Supported Hardware for This Release

The build is available for upgrade on all the existing supported platforms, whereas the enhanced performance support is available only for the following hardware models:

- Sx90/F
- Sx95/F

Virtual Models:

- S100v
- S300v

  The system CPU and memory requirements are changed from 12.5 release onwards. For more information, see Cisco Content Security Virtual Appliance Installation Guide.

- S600v
- S1000v

Note

- Use the Cisco SFPs which are shipped with the appliance.
- AsyncOS version 15.0 will be the last version supported on Sx90/F models.

Upgrade Paths

Upgrading to AsyncOS 14.6.0-108, on page 4

Upgrading to AsyncOS 14.6.0-108

You can upgrade to release 14.6.0-108 of AsyncOS for Cisco Web Security Appliance from the following versions:

Note While upgrading, do not connect any devices (keyboard, mouse, management devices (Raritan, etc.) to the USB ports of the appliance.

- 12.5.1-043
- 12.5.5-008
- 14.0.1-053
- 14.0.4-005
- 14.5.0-537
- 14.5.1-016
- 14.6.0-081

Post–Upgrade Requirements

If the Secure Web Appliance is not registered with Cisco Threat Response, you must perform the following steps after you upgrade to 14.6.0-108.

Procedure

Step 1 Create a user account in the Cisco Threat Response portal with admin access rights. To create a new user account, follow these steps.

- Go to Cisco Threat Response portal https://visibility.amp.cisco.com.
- Click **Create an Account**.

Note If you are unable to create a new user account, contact Cisco TAC for assistance.

Step 2 For registering your appliance with Security Services Exchange (SSE) cloud portal, generate token from SSE portal corresponding to your region.

While registering with SSE cloud portal, select the following FQDN based on your region from the web user interface of your appliance:

- AMERICAS (*api-sse.cisco.com*)
- EUROPE (*api.eu.sse.itd.cisco.com*)
- APJC (*api.apj.sse.itd.cisco.com*)

Step 3 Make sure that you enable Cisco Threat Response under Cloud Services on the Security Services Exchange portal. Ensure that you open HTTPS (In and Out) 443 port on the firewall for the FQDN *api-sse.cisco.com* (America) to register your appliance with the Security Services Exchange portal.

To deploy a virtual appliance, see Cisco Content Security Virtual Appliance Installation Guide

Compatibility

Compatibility with Cisco AsyncOS for Security Management

For compatibility between this release and AsyncOS for Cisco Content Security Management releases, see the compatibility matrix at: https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/web-compatibility/index.html.

IPv6 and Kerberos Not Available in Cloud Connector Mode

When the appliance is configured in Cloud Connector mode, unavailable options for IPv6 addresses and Kerberos authentication appear on pages of the web interface. Although the options appear to be available, they are not supported in Cloud Connector mode. Do not attempt to configure the appliance to use IPv6 addresses or Kerberos authentication when in Cloud Connector mode.

Functional Support for IPv6 Addresses

Features and functionality that support IPv6 addresses:

- Command line and web interfaces. You can access the appliance using http://[2001:2:2::8]:8080 or https://[2001:2:2::8]:8443
- Performing proxy actions on IPv6 data traffic (HTTP/HTTPS/SOCKS/FTP)
- IPv6 DNS Servers
- WCCP 2.01 (Cat6K Switch) and Layer 4 transparent redirection
- Upstream Proxies
- Authentication Services
    - Active Directory (NTLMSSP, Basic, and Kerberos)
    - LDAP
    - SaaS SSO
    - Transparent user identification through CDA (communication with CDA is IPv4 only)
    - Credential Encryption
- Web Reporting and Web Tracking
- External DLP Servers (communication between the appliance and DLP Server is IPv4 only)
- PAC File Hosting
- Protocols: NTP, RADIUS, SNMP, and Syslog over the management server

Features and functionality that require IPv4 addresses:

- Internal SMTP relay
- External Authentication
- Log subscription push methods: FTP, SCP, and Syslog
- NTP servers
- Local update servers, including proxy servers for updates
- Authentication services
- AnyConnect Security Mobility
- Novell eDirectory authentication servers
- Custom logo for end-user notification pages

- Communication between the Web Security Appliance and the Security Management Appliance
- WCCP versions prior to 2.01
- SNMP

Post–Upgrade Requirements

If the Secure Web Appliance is not registered with Cisco Threat Response, you must perform the following steps after you upgrade to 14.6.0-108.

Procedure

Step 1 Create a user account in the Cisco Threat Response portal with admin access rights. To create a new user account, follow these steps.

- Go to Cisco Threat Response portal https://visibility.amp.cisco.com.
- Click **Create an Account**.

Note If you are unable to create a new user account, contact Cisco TAC for assistance.

Step 2 For registering your appliance with Security Services Exchange (SSE) cloud portal, generate token from SSE portal corresponding to your region.

While registering with SSE cloud portal, select the following FQDN based on your region from the web user interface of your appliance:

- AMERICAS (*api-sse.cisco.com*)
- EUROPE (*api.eu.sse.itd.cisco.com*)
- APJC (*api.apj.sse.itd.cisco.com*)

Step 3 Make sure that you enable Cisco Threat Response under Cloud Services on the Security Services Exchange portal. Ensure that you open HTTPS (In and Out) 443 port on the firewall for the FQDN *api-sse.cisco.com* (America) to register your appliance with the Security Services Exchange portal.

To deploy a virtual appliance, see Cisco Content Security Virtual Appliance Installation Guide

Deploying a Virtual Appliance

To deploy a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available at http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Migrating from a Hardware Appliance to a Virtual Appliance

Procedure

Step 1 Set up your virtual appliance with this AsyncOS release using the documentation described in Post–Upgrade Requirements, on page 5 .

Note Ensure that the Security Services updates are successful

Step 2 Upgrade your hardware appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded hardware appliance.

Step 4 Load the configuration file from the hardware appliance onto the virtual appliance.

If your hardware and virtual appliances have different IP addresses, deselect Load Network Settings before loading the configuration file.

Step 5 Commit your changes.

Step 6 Go to **Network** > **Authentication** and join the domain again. Otherwise identities won't work.

Upgrade AsyncOS for Web

Before you begin

- Log in as administrator.
- Perform pr-eupgrade requirements, including updating the RAID controller firmware.

Procedure

Step 1 On the **System Administration** > **Configuration File** page, save the XML configuration file from the Secure Web Appliance.

Step 2 On the **System Administration** > **System Upgrade** page, click **Upgrade Options**.

Step 3 Select either **Download and install**, or **Download only** option.

Step 4 Select an upgrade from the available list.

Step 5 Click **Proceed**.

If you chose **Download only**, the upgrade will be downloaded to the appliance.

Step 6 If you chose **Download and install**, when the upgrade is complete, click **Reboot Now** to reboot the Secure Web Appliance.

Note To verify the browser loads the new online help content in the upgraded version of AsyncOS, you must exit the browser and then open it before viewing the online help. This clears the browser cache of any outdated content.

Important! Actions Required After Upgrading

In order to ensure that your appliance continues to function properly after upgrade, you must address the following items:

- Change the Default Proxy Services Cipher Suites to Cisco Recommended Cipher Suites
- Virtual Appliances: Required Changes for SSH Security Vulnerability Fix
- File Analysis: Required Changes to View Analysis Result Details in the Cloud
- File Analysis: Verify File Types To Be Analyzed
- Unescaped Dots in Regular Expressions

Change the Default Proxy Services Cipher Suites to Cisco Recommended Cipher Suites

From AsyncOS 9.1.1 onwards, the default cipher suites available for Proxy Services are modified to include only secure cipher suites.

However, if you are upgrading from AsyncOS 9.x.x and later releases, the default Proxy Services cipher suites are not modified. For enhanced security, Cisco recommends that you change the default Proxy Services cipher suites to the Cisco recommended cipher suites after the upgrade. Do the following:

Procedure

Step 1 Log in to your appliance using the web interface.

Step 2 Click **System Administration** > **SSL Configuration**.

Step 3 Click **Edit Settings**.

Step 4 Under **Proxy Services**, set the **Cipher(s) to Use** field to the following field:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:TLS_AES_256_GCM_SHA384
```

Caution Make sure that you paste the above string as a single string with no carriage returns or spaces.

Step 5 Submit and commit your changes.

You can also use the **sslconfig** command in CLI to perform the above steps.

Virtual Appliances: Required Changes for SSH Security Vulnerability Fix

Requirements in this section were introduced in AsyncOS 8.8.

The following security vulnerability will be fixed during upgrade if it exists on your appliance:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport.

Note This patch is required only for virtual appliance releases that were downloaded or upgraded before June 25, 2015.

If you did not patch this issue before upgrading, you will see a message during upgrade stating that it has been fixed. If you see this message, the following actions are required to return your appliance to full working order after upgrade:

- Remove the existing entry for your appliance from the known hosts list in your ssh utility. Once the new key has been created, connect to the appliance via ssh and accept the connection.
- Clear the old SSH host key for the appliance on the remote server if you are using SCP push to transfer logs to a remote server (including Splunk).
- If your deployment includes a Cisco Content Security Management Appliance, see important instructions in the Release Notes for that appliance.

File Analysis: Required Changes to View Analysis Result Details in the Cloud

If you have deployed multiple content security appliances (web, email, and/or management) and you want to view detailed file analysis results in the cloud for all files uploaded from any appliance in your organization, you must configure an appliance group on each appliance after upgrading. To configure appliance groups, see File Reputation Filtering and File Analysis.

File Analysis: Required Changes to View Analysis Result Details in the Cloud

If you have deployed multiple content security appliances (web, email, and/or management) and you want to view detailed file analysis results in the cloud for all files uploaded from any appliance in your organization, you must configure an appliance group on each appliance after upgrading. To configure appliance groups, see File Reputation Filtering and File Analysis.

File Analysis: Verify File Types To Be Analyzed

The File Analysis cloud server URL changed in AsyncOS 8.8, and as a result, the file types that can be analyzed may have changed after the upgrade. You should receive an alert if there are changes. To verify the file types selected for analysis, select **Security Services** > **Anti-Malware and Reputation** and look at the Advanced Malware Protection settings.

Unescaped Dots in Regular Expressions

Following upgrades to the regular-expression pattern-matching engine, you may receive an alert regarding unescaped dots in existing pattern definitions after updating your system. Any unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the Velocity pattern-matching engine, and an alert to that effect will be sent to you. You will continue to receive an alert following each update until you correct or replace the pattern. Generally, unescaped dots in a larger regular expression can be problematic and should be avoided.

Documentation Updates

The user guide in the website (www.cisco.com) may be more current than the online help. To obtain the user guide and other documentation for this product, click the **View PDF** button in the online help or visit the URL shown in Related Documentation, on page 13.

Known and Fixed Issues

- Lists of Known and Fixed Issues
- Finding Information about Known and Resolved Issues

Lists of Known and Fixed Issues

- Fixed Issues
- Known Issues

Finding Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find current information about known and resolved defects.

Before you begin

Register for a Cisco account if you do not have one. Go to https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 Log in with your Cisco account credentials.

Step 3 Click **Select from list** > **Security** > **Web Security** > **Cisco Web Security Appliance**, and click **OK**.

Step 4 In **Releases** field, enter the version of the release, for example, x.x.x.

Step 5 Depending on your requirements, do one of the following:

- To view the list of resolved issues, select **Fixed in these Releases** from the **Releases** drop-down.
- To view the list of known issues, select **Affecting these Releases** from the **Releases** drop-down and select **Open** from the **Status** drop-down.

Note If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool. There is also an interactive tour; to view it, click the link in the orange bar above the search fields.

Known Behavior

The following are known behavior of this release:

- By default, the Source interface in Secure Web Appliance (SWA) umbrella settings is set to **Management**. Changing the source interface to **Data** requires you to submit and commit the changes prior to enabling Hybrid Policy.
- Translation is supported for rule actions **Allow**, **Block**, and **Warn**.
- Translation is supported for Content Categories and Destination Lists.
- The translation of AD Users, AD Groups, and internal networks associated with public networks is supported.
- In SWA, one Global umbrella pushed identification profile will always be available.

- Policies configured by SWA admins will be shifted to top priority following the policy push from Umbrella.
- Policies configured in the umbrella will be pushed to all SWAs registered under the umbrella.
- The WBRS are disabled for Decryption Policies pushed by Umbrella.
- The decryption policies pushed by Umbrella are set to Decrypt action by default.
- The End-User Notification page will always be enabled in SWA as a global setting.
- In SWA, the End-User Notification page is configured only for the block page first selected in first ruleset of Umbrella.
- Changes in the selected block page appearance of the first ruleset will be translated every three hours.
- In the case of Umbrella pushed identification profiles and customer categories, admin configured policies will be disabled from the SWA side if these profiles or categories are deleted from the Umbrella.
- SWA registration with Umbrella ORG is limited to the number of seats assigned to a specific ORG, which can be seen in the following path of the umbrella user interface: **Admin** > **Licensing** > **Number of seats**.
- When SWA is registered with Umbrella ORG, SMA policies cannot be pushed to SWA.
- Umbrella cannot push profiles, policies, and custom URL categories to SWA if there is no internal network and AD integrated in Umbrella.
- If API keys that were used for registration and enabling hybrid service are expired, the connection will not be closed until you enable hybrid policy or registered SWA with Umbrella again.
- The following Rules are not supported for translation: Application Settings, Rules Scheduling, and Protected Bypass.
- The SMA policies pushed to SWA are not accepted if the SWA is managed by Umbrella.
- The Save and Load configuration feature will not work for umbrella settings.
- Translation is not supported for the following Ruleset settings:
  - Ruleset Identities - Chromebooks, G Suite OUs, G Suite Users, Tunnels, Roaming Computers, Internal Networks All Tunnels
  - Tenant Controls
  - File Analysis
  - File Type Control
  - HTTPS Inspection - only applications in Selective Decryption list
  - PAC File
  - SafeSearch
  - Ruleset Logging
  - SAML
  - Security Settings

Known Limitations

The following are known limitations of this release:

- The following scenarios do not trigger policy translation:
  - Change in the name of the Ruleset.
  - A Change in the name of the destination list selected in the Rule.
  - Change in name of the selective decryption list selected during HTTP inspection.
  - Adding or removing categories from the selective decryption list used for HTTPS inspection.
  - A selective decryption list containing only categories is selected in the HTTPs inspection.
  - Adding or removing AD users or groups from a Ruleset or a Rule.
  - Integrating or removing AD from the umbrella dashboard.
- When Ruleset identities are the same in multiple Rulesets, only the first Ruleset of the same identity will translate HTTPS inspection settings consistently.
- The format for the Redirect to Custom URL textbox for end-user notification supports only well-formed hostnames or IPV4 addresses. If we push other URL formats configured in the block page of Umbrella to SWA, the policy push fails with the following error message: '*An http/https URL must consist of a well-formed hostname or IPv4 address, may optionally include a port, but may not contain a querystring ('?...').'.", 'code': '400', 'explanation': '400 = Bad request syntax or unsupported method*.'
- In the case where AD groups are selected in rulesets but rules do not match, the access policy will not be created for that rule.
- The categories and domains selected in the Selective Decryption List are set to passthrough for decryption policies that are pushed from umbrella to Secure Web Appliance (SWA). For predefined and custom URL categories, no access policy will be applied in SWA, but rules will be applied to the same configuration in Umbrella.
- If Microsoft 365 compatibility is enabled in Umbrella, decryption policies that are pushed from Umbrella to Secure Web Appliance are set to passthrough. As a result, passthrough will be enabled for all categories of Microsoft 365 endpoints.
- When a trusted AD is not configured in Secure Web Appliance (SWA) but a group is selected for this AD at the umbrella level, an error message appears indicating that it needs to be configured at the SWA level.
- If networks with different masks are selected in Ruleset and Rule, translation is not supported.

Related Documentation

Documentation	Location
Cisco Secure Web Appliance User Guide	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Documentation	Location
Cisco Content Security Management Appliance User Guide	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
Virtual Appliance Installation Guide	https://www.cisco.com/c/en/us/support/security/email-securityappliance/products-installation-guides-list.html
Secure Web Appliance Release Notes, ISE Compatibility Matrix,and Ciphers	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html
Compatibility Matrix for Cisco Secure Email and Web Manager with Secure Web Appliance	https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/web-compatibility/index.html
API Guide	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-programming-reference-guides-list.html
Secure Web Appliance integration with Umbrella	https://docs.umbrella.com/umbrella-user-guide/docs/umbrella-integration-with-secure-web-appliance

Support

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco users.

Access the Cisco Support Community for web security and associated management:

https://supportforums.cisco.com/community/5786/web-security

Customer Support

Note To get support for virtual appliances, call Cisco TAC and have your Virtual License Number (VLN) number ready.

Cisco TAC: Visit http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html.

Support Site for legacy IronPort: Visit http://www.cisco.com/web/services/acquisitions/ironport.html.

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.