Release Notes for AsyncOS 15.0 for Cisco Secure Web Appliance

First Published: 2023-05-11

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 15.0.0-355—General Deployment, on page 1
- Changes in Behavior in AsyncOS 15.0.0-355 GD (General Deployment), on page 3
- Known Limitations, on page 3

What's New In AsyncOS 15.0.0-355—General Deployment

The following features are introduced for this release:

Feature	Description
Smart Software Licensing Enhancements	Following are the enhancements made to the Smart Software Licensing feature: • License Reservation—You can reserve licenses for features enabled in Secure Web Appliance without connecting to the Cisco Smart Software Manager (CSSM) portal. This is mainly beneficial for users that deploy Secure Web Appliance in a highly secured network environment with no communication to the Internet or external devices. For more information, see Overview of smart licensing and Reserving Feature Licenses" sections in the user guide. • Device Led Conversion—After you register Secure Web Appliance with smart licensing, all existing valid classical licenses are automatically converted to smart licenses using the Device Led Conversion (DLC) process. These converted licenses are updated in the virtual account of the CSSM portal. For more information, see Overview of smart licensing section in the user guide. **Note** • AsyncOS version 15.0 is the last release to support the Classic license. The next major release of AsyncOS will support only Smart Licenses.
Deeper bandwidth control	You can manage the traffic bandwidth by configuring the bandwidth value in quota profile and mapping the quota profile in decryption policy and access policy URL category or overall web activity quota. For more information, see Defining Time, Volume, and Bandwidth Quotas section in the user guide.
Clone policy	The clone policy feature allows you to copy or clone the existing configurations of a policy and to create a new policy. For more information, see Policy Configuration section in the user guide.
Application Discovery and Control (ADC) engine	Supports ADC engine, an acceptable use policy component which inspects web traffic to gain deeper understanding and control of web traffic used for applications. Starting with AsyncOS 15.0, you can use either AVC or ADC engine to monitor web traffic. By default, AVC is enabled. The ADC engine supports high performance mode. For more information, see Configuring the URL Filtering Engine and Policy Configuration sections in the user guide.

Feature	Description
REST API for ADC Configuration	You can now retrieve configuration information, and perform any changes (such as modify existing information, add a new information, or delete an entry) in the access policy configuration data of the appliance using REST APIs. For more information, see AsyncOS API 15.0 for Cisco Secure Web Appliance - Getting Started Guide.
Enhancements	
SNMP3 non-default username	Starting from AsyncOS 15.0, admin can opt to configure custom SNMPv3 username other than the default username *v3get*. For more information, see Monitoring System Health and Status using SNMP section in the user guide.
Custom header	The maximum length of the custom header is 16k. For more information, see Adding Custom Headers To Web Requests section in the user guide.
Option to chose the secure tunnel interface and remote access connection	Allows you to select the interface through which the tunnel and remote access connection will be established. For more information, see Enabling remote access to the appliance section in the user guide.
Platform upgrades	From AsyncOS 15.0, FreeBSD version has been upgraded to FreeBSD 13.0. The following has been upgraded: • Cisco SSL version 1.0.2 to Cisco SSL version 1.1.1. • Talos engines such as AVC, WBRSD, DCA, and Beaker have been upgraded. • Scanner engines such as Webroot and McAfee have been upgraded. **Note** FreeBSD 13.0 is compatible with Cisco SSL version 1.1.1 only. Only Cisco SSH compatible cipher, mac and kex algorithms, will be supported for SSH connectivity to FreeBSD 13.0.

Changes in Behavior in AsyncOS 15.0.0-355 GD (General Deployment)

The DCA feature in Secure Web Appliance will be disabled as part of the AsyncOS15.0 GD release and will no longer be supported in future releases. Hence, we DO NOT recommend enabling it.

Known Limitations

This release has the following limitations:

- The SNMPWALK/SNMPGET operations for SNMP OIDs for Proxy Malloc memory is not supported in the multi-prox SWAs (S690, S695, S1000V).

Accessing the New Web Interface

The new web interface provides a new look for monitoring reports and tracking web services. You can access the new web interface in the following way:

- Log in to the legacy web interface and click the **Secure Web Appliance is getting a new look. Try it!!** link. When you click this link, it opens a new tab in your web browser and goes 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 in the enterprise firewall.
- The default port for accessing new web interface is 4431. This can be customized using the **trailblazerconfig** CLI command. For more information about the **trailblazerconfig** CLI command, see "Command Line Interface" chapter in the user guide.
- 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** CLI command. For more information about the **interfaceconfig** CLI command, see "Command Line Interface" chapter in the user guide.

If you change these default ports, ensure that the customized ports for the new web interface are not blocked in 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 a 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 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.

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 15.0.0-355, on page 5

Upgrading to AsyncOS 15.0.0-355

Note

- While upgrading, do not connect any devices (keyboard, mouse, management devices (Raritan) etc.) to the USB ports of the appliance.
- We do not recommend upgrading to AsyncOS 15.0 with Federal Information Processing Standards (FIPS) mode enabled since AsyncOS 15.0 does not support FIPS mode.

You can upgrade to the release 15.0.0-322 of AsyncOS for Cisco Web Security appliances from the following versions:

- 11.8.0-453
- 11.8.1-023
- 11.8.3-021
- 11.8.4-004
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.3-503
- 12.0.4-002
- 12.0.5-011
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2.011
- 12.5.3-002
- 12.5.3-006
- 12.5.4-005
- 12.5.4-011
- 12.5.5-004
- 12.5.5-005
- 12.5.5-008
- 12.5.5-501
- 12.5.6-008
- 12.7.0-033
- 14.0.1-014
- 14.0.1-040
- 14.0.1-053
- 14.0.2-012
- 14.0.3-014
- 14.0.4-005
- 14.1.0-032
- 14.1.0-041
- 14.1.0-047
- 14.5.0-498
- 14.5.0-537
- 14.5.0-673
- 14.5.1-008
- 14.5.1-016
- 14.6.0-108
- 15.0.0-302
- 15.0.0-322

Post–Upgrade Requirements

After you upgrade to 15.0.0-322, you must perform the following steps if you have not registered your appliance with Cisco Threat Response:

Procedure

Step 1 Create a user account in the Cisco Threat Response portal with admin access rights.

To create a new user account, navigate to the Cisco Threat Response portal login page using the following URL- https://visibility.amp.cisco.com and click ‘Create a Cisco Security Account’. 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 the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Compatibility Details

- Compatibility with Cisco AsyncOS for Security Management, on page 7
- IPv6 and Kerberos Not Available in Cloud Connector Mode, on page 7
- Functional Support for IPv6 Addresses, on page 7
- Post–Upgrade Requirements, on page 6

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

Availability of Kerberos Authentication for Operating Systems and Browsers

You can use Kerberos authentication with these operating systems and browsers:

- Windows servers 2003, 2008, 2008R2, and 2012.
- Latest releases of Safari and Firefox browsers on Mac (OSX Version 10.5 and later)
- IE (Version 7 and later) and latest releases of Firefox and Chrome browsers on Windows 7 and later.

Kerberos authentication is not available with these operating systems and browsers:

- Windows operating systems not mentioned above

- Browsers not mentioned above
- iOS and Android

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 Follow the instructions provided in the Post–Upgrade Requirements, on page 6 to configure your virtual appliance using this AsyncOS release.

Note Verify that the Security Services updates have been successfully installed.

Step 2 Upgrade your hardware appliance to this version of AsyncOS.

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

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

If your virtual appliances and hardware have different IP addresses, unselect **Load Network Settings** before loading the configuration files.

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

- Bug Search Tool Requirements
- Lists of Known and Fixed Issues
- Finding Information about Known and Resolved Issues

Bug Search Tool Requirements

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

Lists of Known and Fixed Issues

- Known and Fixed Issues in Release 15.0.0-355, on page 12

Known and Fixed Issues in Release 15.0.0-355

- 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.

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
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

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. Have your Virtual License Number (VLN) number ready before you call TAC.

Cisco TAC:

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

Support site for legacy IronPort:

http://www.cisco.com/web/services/acquisitions/ironport.html.

For noncritical issues, you can also access customer support from the appliance. For instructions, see the Troubleshooting section of the Secure Web Appliance User Guide.