Release Notes for AsyncOS 14.1 for Cisco Web Security Appliances

First Published: 2021-06-09

Last Modified: 2021-11-30

About 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

- What's New in AsyncOS 14.1.0-047 LD (Limited Deployment)—Refresh, on page 1
- What's New in AsyncOS 14.1.0-041 LD (Limited Deployment)—Refresh, on page 1
- What's New In AsyncOS 14.1.0-032 LD (Limited Deployment), on page 1

What's New in AsyncOS 14.1.0-047 LD (Limited Deployment)—Refresh

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 14.1.0-047, on page 12 for additional information.

What's New in AsyncOS 14.1.0-041 LD (Limited Deployment)—Refresh

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 14.1.0-041, on page 12 for additional information.

What's New In AsyncOS 14.1.0-032 LD (Limited Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 14.1.0-032, on page 12 for additional information.

Feature	Description
Cisco Umbrella Seamless ID	The Cisco Umbrella Seamless ID feature enables the appliance to pass the user identification information to the Cisco Umbrella Secure Web Gateway (SWG) after successful authentication. The Cisco Umbrella SWG checks the user information in the Active Directory based on the authenticated identification information received from the Web Security Appliance. The Cisco Umbrella SWG considers the user as authenticated and provides access to the user based on the defined security policies. The Web Security Appliance passes the user identification information to the Cisco Umbrella SWG using the HTTP headers; X-USWG-PKH, X-USWG-SK, and X-USWG-Data. **Note** • The Cisco Umbrella Seamless ID headers overwrite the headers with the same names on the Web Security Appliance, if any. • The Cisco Umbrella Seamless ID feature supports authentication scheme with Active Directory only. This feature does not support LDAP, Cisco Identity Services Engine (ISE), and Cisco Context Directory Agent (CDA). • The Cisco Umbrella SWG does not support FTP and SOCKS traffic. • Ensure that the Web Security Appliance and the Cisco Umbrella SWG have the same timezone across enterprises. If the time difference between the Cisco Umbrella SWG and the Web Security Appliance is more than four minutes, the Umbrella Seamless ID headers are not configured on the Cisco Umbrella SWG. See "Cisco Umbrella Seamless ID" section in the user guide. **Prerequisites:** On the Cisco Umbrella SWG web user interface, perform the following tasks: • Register Web Security Appliance public IP address as network deployment. • Configure the access policies and access rules with users and groups (**Policies** > **Management** > **All Policies**). On the Web Security Appliance user interface, perform the following tasks: • Add the Cisco Umbrella SWG root certificate to Web Security Appliances trusted certificate (**Network** > **Certificate Management**). • Configure TCP Anycast IP (146.112.255.50) in Cisco Umbrella Seamless ID profile page (**Web Security Manager** > **Cisco Umbrella Seamless ID** > **Edit Settings**). • Configure routing policies (**Web Security Manager** > **Routing Policies**) with Cisco Umbrella Seamless ID profile with the appropriate port as upstream proxy group. • Enable AD Authentication in Web Security Appliance policies. • Enable decryption for Authentication.

The AsyncOS 14.1 for Cisco Web Security Appliance supports TLSv1.2 session resumption in client and server.

Changes in Behavior in AsyncOS 14.1.0-047 LD (Limited Deployment)–Refresh

Cisco Umbrella Seamless ID Enhancements	The Web Security Appliance retrieves the UPN value from the active directory for basic authentication of the users and sends the correct UPN value to Cisco Umbrella Seamless ID. For this functionality to work, you must assign all the active directory users with a default or customized UPN value. For a successful log in, the basic authentication log in should be done in the following format: DomainName\UserName.

Changes in Behavior in AsyncOS 14.1.0-041 LD (Limited Deployment)–Refresh

Cisco Umbrella Seamless ID Enhancements	The Web Security Appliance retrieves the UPN value for the authenticated user from the active directory and allows the Cisco Umbrella Seamless ID to apply the correct web policies for the users. For this functionality to work, you must assign all the active directory users with default or customized UPN values.

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

– Sx95/F models



Note The Sx80 models are not supported from AsyncOS version 14.0 onwards.

Virtual models:

– S100v

– S300v

– S600v

Upgrade Paths

- Upgrading to AsyncOS 14.1.0-047, on page 5
- Upgrading to AsyncOS 14.1.0-041, on page 5

• Upgrading to AsyncOS 14.1.0-032, on page 5

Upgrading to AsyncOS 14.1.0-047

You can upgrade to the release 14.1.0-047 of AsyncOS for Cisco Web Security appliances 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.

- 14.1.0-041
- 14.1.0-032

Upgrading to AsyncOS 14.1.0-041

You can upgrade to the release 14.1.0-041 of AsyncOS for Cisco Web Security appliances 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.

- 14.1.0-032

Upgrading to AsyncOS 14.1.0-032

You can upgrade to the release 14.1.0-032 of AsyncOS for Cisco Web Security appliances 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.

- 11.7.3-025
- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-511
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-021
- 11.8.3-501
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 14.0.0-467
- 14.0.1-014

Post–Upgrade Requirements

After you upgrade to 14.1.0-047, you must perform the following steps if you have not registered your appliance with Cisco Threat Response:



Note This procedure is not applicable if you have already 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
- IPv6 and Kerberos Not Available in Cloud Connector Mode
- Functional Support for IPv6 Addresses
- Post-Upgrade Requirements

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 Set up your virtual appliance with this AsyncOS release using the documentation described in Post-Upgrade Requirements.

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.

Upgrading AsyncOS for Web

Before you begin

- Perform preupgrade requirements, including updating the RAID controller firmware.
- Log in as Administrator.

Procedure

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

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

Step 3 You can select either **Download and install**, or **Download only**.

Choose from the list of available upgrades.

Step 4 Click **Proceed**.

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

Step 5 If you chose **Download and install**, when the upgrade is complete, click **Reboot Now** to reboot the Web Security 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.

Upgrade Guidelines

Important!

Following an upgrade, you must take the following steps to ensure that your appliance continues to function properly.

- 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 Go to **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:!EXPORT:!3DES:!RC2:!RC4:!IDEA:!SEED:!ECDSA:AES256-SHA:AES256-SHA256:AES128-SHA:TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256
```

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:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport%20



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: 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 and and other documentation for this product is available in Related Documentation.

Known and Fixed Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects in this release.

- 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 14.1.0-047, on page 12
- Known and Fixed Issues in Release 14.1.0-041, on page 12
- Known and Fixed Issues in Release 14.1.0-032, on page 12

Known and Fixed Issues in Release 14.1.0-047

- Fixed Issues
- Known Issues

Known and Fixed Issues in Release 14.1.0-041

- Fixed Issues
- Known Issues

Known and Fixed Issues in Release 14.1.0-032

- 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://bst.cloudapps.cisco.com/bugsearch/search.

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
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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2021 Cisco Systems, Inc. All rights reserved.