Release Notes for AsyncOS 14.5 for Cisco Secure Web Appliance

First Published: 2022-04-11

Last Modified: 2024-08-30

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 14.5.3-033 MD (Maintenance Deployment), on page 1
- What's New In AsyncOS 14.5.2-011 MD (Maintenance Deployment), on page 1
- What's New In AsyncOS 14.5.1-016 MD (Maintenance Deployment)—Refresh, on page 1
- What's New In AsyncOS 14.5.1-008 MD (Maintenance Deployment), on page 2
- What's New In AsyncOS 14.5.0-537 GD (General Deployment), on page 2
- What's New In AsyncOS 14.5.0-498 LD (Limited Deployment), on page 2

What's New In AsyncOS 14.5.3-033 MD (Maintenance Deployment)

Introduction of new CLI for Sophos malloc settings- Sophos engine scan may often get timed out and run out of memory when there is a huge traffic running through the engine. To resolve this issue, we have introuduced a new subcommand **sophos > malloc_setting** under **advancedproxyconfig > scanners** command. You can use this command to change the default sophos malloc setting.

For more details on the command, see "Secure Web Appliance CLI Commands" section in the user guide.

What's New In AsyncOS 14.5.2-011 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 14.5.2-011, on page 19 for additional information.

What's New In AsyncOS 14.5.1-016 MD (Maintenance Deployment)—Refresh

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 14.5.1-016, on page 19 for additional information.

What's New In AsyncOS 14.5.1-008 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 14.5.1-008, on page 19 for additional information.

What's New In AsyncOS 14.5.0-537 GD (General Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 14.5.0-537, on page 19 for additional information.

What's New In AsyncOS 14.5.0-498 LD (Limited Deployment)

The following features are introduced for this release:

<table>
<tr><th>Feature</th><th colspan="2">Description</th></tr>
<tr><td>Secure DNS</td><td colspan="2">The Secure Web Appliance can now validate the DNS response received from the DNS server using cryptographic signatures.
See "Editing DNS Settings" section in the user guide.</td></tr>
<tr><td>Maximum connections per client</td><td colspan="2">The Secure Web Appliance restricts the number of concurrent connections initiated by the client to a configured value.
See "Configuring Web Proxy Settings" section in the user guide.</td></tr>
<tr><td rowspan="3">Rebranding of Cisco Web Security Appliance to Cisco Secure Web Appliance</td><td colspan="2">Beginning with AsyncOS Release 14.5, Cisco Web Security Appliance has been rebranded to Cisco Secure Web Appliance in the web interface and all user documentation.</td></tr>
<tr><td>Former Terminology</td><td>Rebranded Terminology</td></tr>
<tr><td>Web Security Appliance</td><td>Secure Web Appliance</td></tr>
<tr><td rowspan="6">Product Rebranding</td><td>Former Terminology</td><td>Rebranded Terminology</td></tr>
<tr><td>AMP for Endpoints</td><td>Secure Endpoint</td></tr>
<tr><td>Advanced Malware Protection</td><td>Secure Endpoint</td></tr>
<tr><td>AMP</td><td>Secure Endpoint</td></tr>
<tr><td>Thread Grid</td><td>Malware Analytics</td></tr>
<tr><td colspan="2">Note
Instances of the rebranded terms present in this document do not correspond with the web interface. In the web interface, AMP for Endpoints, Advance Malware Protection, and AMP is referred as Malware Analytics. The web interface will be updated in the upcoming release.</td></tr>
<tr><td>Misclassification requests</td><td colspan="2">The misclassification request is sent over HTTPS and hence you do not receive security alert notifications.
See "Configuring On-Box End-User Notification Pages" section in the user guide.</td></tr>
</table>

Feature	Description
New accesslog decision tags	The accesslog decision tag in the Decrypt Policy group is appended with EUN (End user Notification) when the EUN page appears on the client web browser. See "ACL Decision Tags" 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. See "Policy Configuration" section in the user guide.
Deeper bandwidth control	You can manage the traffic bandwidth by configuring the bandwidth value in quota profile and mapping the quota profile in access policy URL category or overall web activity quota. See "Defining Time, Volume, and Bandwidth Quotas" section in the user guide.
REST API for configuring management policies, decryption policies, routing policies, IP spoofing policies, Anti-Malware and reputation, Authentication realms, Cisco Smart Software License, Cisco Umbrella Seamless ID, Identity services, and System setup	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 configuration data of the appliance using REST APIs. See the "AsyncOS API 14.5 for Cisco Secure Web Appliance - Getting Started Guide."
ISE-SXP integration	You can integrate ISE-SXP deployment with Cisco Secure Web Appliance for passive authentication. This allows you to get all defined mappings, including SGT-to-IP address mappings that are published through SXP. See "Configure ISE-SXP Integration" section in the user guide.

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 Secure Web Appliance. The Cisco Umbrella SWG considers the user as authenticated and provides access to the user based on the defined security policies. The Secure Web 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 Secure Web 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. See "Cisco Umbrella Seamless ID" section in the user guide.
Enhancements	
Samba upgrade	The Samba version has been upgraded to version 4.11.15. You can enable or disable the SMB1 protocol support for Samba version 4.11.15 using the *smbprotoconfig* command. By default, this support is disabled and can be enabled based on the authentication realm configuration. See "Secure Web Appliance CLI Commands" section in the user guide.

Note (For TAC only)

Due to the tiny CLI revert, the HTTPS proxy ports are disabled on virtual Secure Web Appliances. Enable HTTPS on the interface using the *interfaceconfig* command.

Changes in Behavior

- Changes in Behavior in AsyncOS 14.5.0-537 GD (General Deployment), on page 5
- Changes in Behavior in AsyncOS 14.5.0-498 LD (Limited Deployment), on page 5
- Changes in Behavior in AsyncOS 14.5.3-033 MD (Maintenance Deployment), on page 6

Changes in Behavior in AsyncOS 14.5.0-537 GD (General Deployment)

Clone Policy	The following policies with cloning option in Secure Web Appliance can also be managed by Cisco Secure Email and Web Manager (SMA). • Access • Identification profile • Decryption • Routing

Changes in Behavior in AsyncOS 14.5.0-498 LD (Limited Deployment)

SSL Configuration	TLSv1.2 is enabled by default for Appliance Management web user interface under **System Administrator** > **SSL Configuration** to support chrome browser version 98.0.4758.80 or later.
Session resumption	After an upgrade, session resumption will be disabled by default.
Context Directory Agent (CDA)	Context Directory Agent (CDA) is no longer supported. It is recommended to configure ISE/ISE-PIC for transparent user identification to achieve the same functionality. Options to configure CDA will not be available in future releases. For more information, see End-of-Sale and End-of-Life Announcement for the Cisco Context Directory Agent (CDA)
Interface selection for Smart License Registration	You can now choose between Data or Management interface from the **Test Interface** drop-down list. **Note** Ensure both the Data and Management interface are configured. After an upgrade, when split routing is enabled, the **Test Interface** for Smart License in the web interface will show as **Data Interface**. If the split routing is disabled, then the **Management Interface** is displayed.
HTTPS Proxy–Invalid Certificate Handling	On a fresh installation of AsyncOS 14.5, the **Expired** and **Mismatched Hostname** certificate configurations value in the HTTPS Proxy page will be selected by default as **Drop** instead of **Monitor**. **Note** This is applicable only for a new installation and not for an upgrade. Upgrading the appliance will retain the same configuration from the previous version.

networktuning	After an upgrade to Cisco AsyncOS 14.5, you will receive a prompt to restart the proxy process when you execute the *networktuning* command for the first time. **Note** For AsyncOS version earlier than 14.5, this prompt to restart the proxy process is not available. If the command was executed in any of the previous version before an upgrade, the prompt will not be triggered.

Changes in Behavior in AsyncOS 14.5.3-033 MD (Maintenance Deployment)

Telnet command	The **telnet** command for communicating with another host using TELNET protocol is removed from Secure Web Appliance due to a vulnerability. This command is no longer supported in Secure Web Appliance

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



Note AsyncOS version 14.5 will be the last supported release on Sx90/F models.

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.

Upgrade Paths

- Upgrading to AsyncOS 14.5.3-033, on page 8
- Upgrading to AsyncOS 14.5.2-011, on page 9
- Upgrading to AsyncOS 14.5.1-016, on page 10
- Upgrading to AsyncOS 14.5.1-008, on page 10
- Upgrading to AsyncOS 14.5.0-537, on page 11
- Upgrading to AsyncOS 14.5.0-498, on page 12

Upgrading to AsyncOS 14.5.3-033



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

You can upgrade to the release 14.5.3-033 of AsyncOS for Cisco Secure Web Appliance from the following versions:

11.8.0-453	12.0.1-334	14.0.0-467
11.8.1-023	12.0.2-004	14.0.1-014
11.8.1-028	12.0.2-012	14.0.1-040
11.8.1-511	12.0.3-005	14.0.1-053
11.8.1-604	12.0.3-007	14.0.2-012
11.8.1-702	12.0.4-002	14.0.3-007
11.8.2-702	12.0.5-011	14.0.3-014
11.8.3-021	12.5.1-011	14.1.0-032
11.8.3-501	12.5.1-035	14.1.0-041
11.8.4-004	12.5.1-043	14.1.0-047
	12.5.2-011	14.5.0-388
	12.5.3-002	14.5.0-455
	12.5.3-006	14.5.0-498
	12.5.4-005	14.5.0-537
	12.5.4-011	14.5.0-673
	12.5.5-004	14.5.1-008
	12.5.5-005	14.5.1-016

	12.5.5-008	14.5.1-607
	12.7.0-033	14.5.2-011

Upgrading to AsyncOS 14.5.2-011



Note Before upgrading to this release, save a copy of the appliance configuration file to a location other than the appliance.

You can upgrade to the release 14.5.2-011 of AsyncOS for Cisco Secure Web Appliance from the following versions:

11.8.0-453	12.0.1-334	14.0.0-467
11.8.1-023	12.0.2-004	14.0.1-014
11.8.1-028	12.0.2-012	14.0.1-040
11.8.1-511	12.0.3-005	14.0.1-053
11.8.1-604	12.0.3-007	14.0.2-012
11.8.1-702	12.0.3-503	14.0.3-007
11.8.3-021	12.0.4-002	14.0.3-014
11.8.3-501	12.0.5-011	14.1.0-032
11.8.4-004	12.5.1-011	14.1.0-041
	12.5.1-035	14.1.0-047
	12.5.1-043	14.5.0-388
	12.5.2-011	14.5.0-455
	12.5.3-002	14.5.0-498
	12.5.3-006	14.5.0-537
	12.5.4-005	14.5.0-673
	12.5.4-011	14.5.1-008
	12.5.5-004	14.5.1-016
	12.5.5-005	
	12.5.5-008	
	12.5.5-501	
	12.5.6-008	
	12.7.0-033	

Upgrading to AsyncOS 14.5.1-016



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

You can upgrade to the release 14.5.1-016 of AsyncOS for Cisco Secure Web Appliance from the following versions:

11.8.0-453	12.0.1-334	14.0.0-467
11.8.1-023	12.0.2-004	14.0.1-014
11.8.1-028	12.0.2-012	14.0.1-040
11.8.1-511	12.0.3-005	14.0.1-053
11.8.1-604	12.0.3-007	14.0.2-012
11.8.1-702	12.0.4-002	14.0.3-007
11.8.2-702	12.0.5-011	14.0.3-014
11.8.3-021	12.5.1-011	14.0.4-005
11.8.3-501	12.5.1-035	14.1.0-032
11.8.4-004	12.5.1-043	14.1.0-041
	12.5.2-011	14.1.0-047
	12.5.3-002	14.5.0-388
	12.5.3-006	14.5.0-455
	12.5.4-005	14.5.0-498
	12.5.4-011	14.5.0-537
	12.5.5-004	14.5.0-673
	12.5.5-005	14.5.1-008
	12.5.5-008	
	12.7.0-033	

Upgrading to AsyncOS 14.5.1-008



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

You can upgrade to the release 14.5.1-008 of AsyncOS for Cisco Secure Web Appliance from the following versions:

11.8.0-453	12.0.1-334	14.0.0-467
11.8.1-023	12.0.2-004	14.0.1-014
11.8.1-028	12.0.2-012	14.0.1-040
11.8.1-511	12.0.3-005	14.0.1-053
11.8.1-604	12.0.3-007	14.0.2-012
11.8.1-702	12.0.4-002	14.0.3-007
11.8.2-702	12.0.5-011	14.0.3-014
11.8.3-021	12.5.1-011	14.1.0-032
11.8.3-501	12.5.1-035	14.1.0-041
11.8.4-004	12.5.1-043	14.1.0-047
	12.5.2-011	14.5.0-388
	12.5.3-002	14.5.0-455
	12.5.3-006	14.5.0-498
	12.5.4-005	14.5.0-537
	12.5.4-011	14.5.0-673
	12.5.5-004	
	12.5.5-005	
	12.5.5-008	
	12.7.0-033	

Upgrading to AsyncOS 14.5.0-537



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

You can upgrade to the release 14.5.0-537 of AsyncOS for Cisco Secure Web Appliance from the following versions:

11.8.0-453	12.0.1-268	14.0.0-467
11.8.1-023	12.0.1-334	14.0.1-014
11.8.1-028	12.0.2-004	14.0.1-040

11.8.1-511	12.0.2-012	14.0.1-053
11.8.1-604	12.0.3-005	14.0.1-503
11.8.1-702	12.0.3-007	14.0.2-012
11.8.2-009	12.0.4-002	14.1.0-032
11.8.2-702	12.5.1-011	14.1.0-041
11.8.3-021	12.5.1-035	14.1.0-047
11.8.3-501	12.5.1-043	14.5.0-388
11.8.4-004	12.5.2-007	14.5.0-455
	12.5.2-011	14.5.0-498
	12.5.3-002	
	12.5.4-005	
	12.5.4-011	
	12.7.0-033	

Upgrading to AsyncOS 14.5.0-498



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

You can upgrade to the release 14.5.0-498 of AsyncOS for Cisco Secure Web Appliance from the following versions:

11.8.0-453	12.0.1-268	14.0.0-467
11.8.1-023	12.0.1-334	14.0.1-014
11.8.1-028	12.0.2-004	14.0.1-040
11.8.1-511	12.0.2-012	14.0.1-053
11.8.1-604	12.0.3-005	14.0.2-012
11.8.1-702	12.0.3-007	14.1.0-032
11.8.2-009	12.0.4-002	14.1.0-041
11.8.2-702	12.5.1-011	14.1.0-047
11.8.3-021	12.5.1-035	14.5.0-388
11.8.3-501	12.5.1-043	14.5.0-455
11.8.4-004	12.5.2-007	

12.5.2-011

12.5.3-002

12.7.0-033

Post–Upgrade Requirements

After you upgrade to 14.5.1-016, 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
- 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 management server

Features and functionality that require IPv4 addresses:

- Internal SMTP relay
- External Authentication
- Log subscriptions push method: 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 Secure Web 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, on page 13.

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 Secure Web 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 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:

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 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 20.

Known and Fixed Issues

- Bug Search Tool Requirements
- List 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 14.5.3-033, on page 19
- Known and Fixed Issues in Release 14.5.2-011, on page 19
- Known and Fixed Issues in Release 14.5.1-016, on page 19
- Known and Fixed Issues in Release 14.5.1-008, on page 19
- Known and Fixed Issues in Release 14.5.0-537, on page 19
- Known and Fixed Issues in Release 14.5.0-498, on page 19

Known and Fixed Issues in Release 14.5.3-033

Log in to Cisco Bug Search Tool using your Cisco account credentials to view the list of fixed bugs.

- Fixed Issues
- Known Issues

Known and Fixed Issues in Release 14.5.2-011

Log in to Cisco Bug Search Tool using your Cisco account credentials to view the list of fixed bugs.

- Fixed Issues
- Known Issues

Known and Fixed Issues in Release 14.5.1-016

- Fixed Issues
- Known Issues

Known and Fixed Issues in Release 14.5.1-008

- Fixed Issues
- Known Issues

Known and Fixed Issues in Release 14.5.0-537

- Fixed Issues
- Known Issues

Known and Fixed Issues in Release 14.5.0-498

- 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 Secure Web 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

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.

© 2024 Cisco Systems, Inc. All rights reserved.