Release Notes for AsyncOS 12.0 for Cisco Web Security Appliances

First Published: 2020-01-13

Last Modified: 2022-06-07

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 12.0.5-011 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Lists of Known and Fixed Issues in Release 12.0.5-011, on page 21 for additional information.

What's New In AsyncOS 12.0.4-002 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Lists of Known and Fixed Issues in Release 12.0.4-002, on page 21 for additional information.

What's New In AsyncOS 12.0.3-007 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Lists of Known and Fixed Issues in Release 12.0.3-007 for additional information.

New URL Categories Update notification	A new **URL Categories Update** notification is introduced in the banner. An email notification is also sent to the users about the upcoming URL category updates.

What's New In AsyncOS 12.0.3-005 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Lists of Known and Fixed Issues in Release 12.0.3-005 for additional information.

What's New In AsyncOS 12.0.2-012 MD (Maintenance Deployment)–Refresh

This release contains a number of bug fixes; see the Lists of Known and Fixed Issues in Release 12.0.2-012 and Changes in Behavior in Asyncos 12.0.2-012 for additional information.

What's New In AsyncOS 12.0.2-004 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Lists of Known and Fixed Issues in Release 12.0.2-004 for additional information.

Feature	Description
Deprecation of TLS 1.0/1.1	Use TLS 1.2 or later versions to connect the appliance to the AMP File Reputation server. AMERICAS (Legacy) cloud-sa.amp.sourcefire.com is removed from the AMP File Reputation server list, so AMERICAS (Legacy) cloud-sa.amp.sourcefire.com cannot be configured on the appliance. Before you upgrade the appliance to the 12.0.2 version, the following is recommended: • If the AMP services are enabled and the File Reputation server is configured as AMERICAS (Legacy) cloud-sa.amp.sourcefire.com, change the File Reputation server to AMERICAS (cloud-sa.amp.cisco.com). • After you upgrade the appliance, check if the File Reputation server is retained as AMERICAS (cloud-sa.amp.cisco.com). **Note** If you configure Europe or APJC as the File Reputation server before upgrading the appliance, the preceding conditions will not be applicable. For more information, see Decommissioning Legacy File Reputation Servers for Cisco Web Security Appliances.
Enhancements	
Support to configure maximum concurrent scans for AMP	A new option **Enter the number of concurrent scans to be supported by AMP** is added in the main CLI command `advancedproxyconfig > scanners > AMP`. Using the new CLI option, you can configure the number of concurrent scans supported by AMP. The default value for all the models is 250 which is the maximum limit.

Feature	Description
Support to change the scan verdict during the eviction of long running scans	A new CLI subcommand **eviction** is added in the main CLI command `advancedproxyconfig > scanners`. Using the new CLI subcommand, you can change the default **Unscannable** verdict of long running scan eviction to **Timeout** and vice-versa.

What's New In AsyncOS 12.0.1-334 GD (General Deployment)

This release contains a number of bug fixes; see the Lists of Known and Fixed Issues in Release 12.0.1-334 for additional information.

The subcommand **scanners** is added under **advancedproxyconfig** CLI command.

New Command Line Interface	Description
Support to exclude MIME types from being scanned by the AMP engine.	A new subcommand **scanners** is added under the main **advancedproxyconfig** command to exclude the MIME types from being scanned by the AMP engine. To use the **scanners** subcommand, you must disable the 'Adaptive Scanning' feature. Using the **scanners** subcommand, you can add the MIME types that need not be scanned by the AMP engine to increase the scanning performance. Default MIME type options are 'image/ALL and text/ALL'. To add the MIME types, you must append them after the default options. For example, if you want to add the video and audio MIME types, the format must be: 'image/ALL and text/ALL video/ALL audio/ALL'

What's New In AsyncOS 12.0.1-268 LD (Limited Deployment)

This release contains a number of bug fixes; see the Lists of Known and Fixed Issues in Release 12.0.1-268 for additional information for additional information.

The following features are introduced for this release:

Feature	Description
Support for High Performance	The Cisco AsyncOS 12.0 release provides Web Security Appliance with High Performance (HP) for platforms S680, S690, and S695. This increases the traffic handling performance of the existing high end appliances. The following scanning engines are replicated as 2 instances for S680 model and 3 instances for S690/S695 models, when the high performance mode is enabled on the appliance: • Sophos • Mcafee • Merlin • Firestone • AVC • Archive scan • AMP
Integrating the Web Security Appliance with Cisco Threat Response (CTR) Portal	You can integrate your appliance with the Cisco Threat Response portal, and perform the following actions in the Cisco Threat Response portal: • View the web tracking data from multiple appliances in your organization. • Identify, investigate, and remediate threats observed in the web tracking. • Resolve the identified threats rapidly and provide recommended actions to take against the identified threats. • Document the threats in the portal to save the investigation, and enable collaboration of information among other devices on the portal. See the "Intercepting with Cisco Threat Response Portal" chapter in the user guide.
TLS Version	The appliance supports TLSv1.3 version. Cipher 'TLS_AES_256_GCM_SHA384' is added to the default cipher list. By default, TLSv1.3 is enabled on the appliance. See the "Intercepting Web Requests" chapter in the user guide.
Enhancements	

Feature	Description
Web interface enhancements for configuration file backup	The configuration file backup feature is moved from the sub menu '*Log Subscriptions*' to '*Configuration File*' under *System Administration*.
ECDSA Certificate upload	The appliance now supports the uploading of ECDSA certificate for HTTPS proxy.

Note Before you upgrade to 12.0.1-268, disable the following features in order to avail the High Performance mode on the models (S680, S690, S695, S680F, S690F, and S695F.)

- Web Traffic Tap
- Volume and Time Quotas
- Overall Bandwidth Limits

The Web Security appliance with High Performance mode supports high rate of transaction handling. The time duration for holding the reporting and tracking data on the hard disk of Security Management appliance or the Web Security appliance will be reduced in High Performance mode due to the increased processing capacity.

Note If the Security Management appliance (SMA) model is 680, use SMA12.7 version to manage the Cisco Web Security appliance 12.0.

The following changes are made to the Command Line Interface for this release:

Command Line Interface	Description
highperformance	A new subcommand **highperformance** is added under the main **advancedproxyconfig** command to enable and disable the high performance mode.
proxyscannermap	A new diagnostic CLI **proxyscannermap** subcommand is added under `diagnostic > proxy`. The **proxyscannermap** subcommand displays PID mapping between each proxy and corresponding scanner process.
New option added under the CLI command **authcache**.	New option **searchdetails** is added under the CLI command **authcache**. This CLI is applicable to all appliances.

Command Line Interface	Description
New sub command **CTROBSERVABLE** under the CLI command **reportingconfig**	New sub command **CTROBSERVABLE** is added under the CLI command **reportingconfig**. You can use the sub command **CTROBSERVABLE** to enable or disable the CTR observable based indexing. When this is enabled, you can index the URLs accessed by users. It also provides granularity to search any URLs in the appliance tracking database.

The following new logs are introduced for this release:

- Separate `trackstat` log files for each proxy instance
- `replicatord` logs

Changes in Behavior

- Changes in Behavior in Asyncos 12.0.5-011, on page 6
- Changes in Behavior in Asyncos 12.0.2-012, on page 7

Changes in Behavior in Asyncos 12.0.5-011

SSL Configuration	Beginning Cisco AsyncOS 12.0.5 version, 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 to Cisco AsyncOS 12.0.5 version, session resumption will be disabled by default.
Context Directory Agent (CDA)	Beginning Cisco AsyncOS 12.0.5 version, the following message is added to indicate the end of support for CDA in the CDA configuration section: "*Context Directory Agent (CDA) has reached EOS. It is recommended configuring ISE/ISE-PIC for transparent user authentication instead of CDA*".

Changes in Behavior in Asyncos 12.0.2-012

Warning messages for proxy malloc memory utilization	The following alert messages are triggered on the web user interface of the appliance (**System Administration** > **Alerts** > **View Top Alerts**): • when the proxy malloc memory crosses 90% of proxy malloc memory limit *Proxy malloc memory reached to 90%, proxy will restart whenever max limit exceed* • when the proxy gets restarted on reaching 100% of malloc memory *Proxy malloc memory exceed the max limit, restarting proxy* In both the cases, an e-mail notification is sent to all 'Alert recipients' configured to receive 'Web Proxy' critical alerts. The critical logs messages are now included in proxy logs.

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 **Web Security 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:

- S680
- S690
- S695
- S680F
- S690F
- S695F

The build is available for upgrade on the following hardware and virtual models:

Hardware Models:

- x80
- x90
- x95

Virtual Models:

- S100v
- S300v

- S600v

The system CPU and memory requirements are changed from 12.0 release onwards. For more information, see Cisco Content Security Virtual Appliance Installation Guide.

Some hardware models require a memory upgrade before you can install or upgrade to this AsyncOS release. For more information, see http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html.

Upgrade Paths

Upgrading to AsyncOS 12.0.5-011

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 12.0.5-011 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.6.0-240
- 10.6.0-244
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018
- 11.8.3-021
- 11.8.3-501
- 11.8.4-004
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.4-002

Upgrading to AsyncOS 12.0.4-002

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 12.0.4-002 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.6.0-240
- 10.6.0-244
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018
- 11.8.3-021
- 11.8.3-501
- 11.8.4-004
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007

Upgrading to AsyncOS 12.0.3-007

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 12.0.3-007 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.5-037
- 10.5.6-024
- 10.6.0-240
- 10.6.0-244
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018
- 11.8.3-021
- 11.8.3-501
- 12.0.1-268
- 12.0.1-334
- 12.0.1-004
- 12.0.2-012
- 12.0.3-005

Upgrading to AsyncOS 12.0.3-005

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 12.0.3-005 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.5-037
- 10.5.6-024
- 10.6.0-240
- 10.6.0-244
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11-7-1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018
- 11.8.3-021
- 11.8.3-501
- 12.0.1-268
- 12.0.1-334
- 12.0.1-004
- 12.0.2-012

Upgrading to AsyncOS 12.0.2-012

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 12.0.2-012 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.4-017
- 10.1.5-004
- 10.1.5-034
- 10.1.5-037
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 10.5.6-022
- 10.5.6-024
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.1-706
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.5.3-504
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 12.0.1-268
- 12.0.1-334
- 12.0.1-004

Upgrading to AsyncOS 12.0.2-004

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 12.0.2-004 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.4-017
- 10.1.5-004
- 10.1.5-034
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 10.5.6-022
- 10.5.6-024
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.1-706
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.5.3-504
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.2-011
- 11.8.0-414
- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 12.0.1-268
- 12.0.1-334

Upgrading to AsyncOS 12.0.1-334

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 12.0.1-334 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.4-017
- 10.1.5-004
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 10.5.6-022
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.1-706
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.5.3-504
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.8.0-453
- 11.8.1-023
- 12.0.1-268

Upgrading to AsyncOS 12.0.1-268

You can upgrade to the release 12.0.1-268 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.4-017
- 10.1.5-004
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.5.3-504
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.8.0-348
- 11.8.0-414
- 11.8.0-429
- 11.8.0-440
- 11.8.0-446
- 11.8.0-450
- 11.8.0-453
- 12.0.1-005
- 12.0.1-161

Post–Upgrade Requirements

After you upgrade to 12.0.5-011, 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.

Note 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

For compatibility between this release and AsyncOS for Cisco Content Security Management releases, see the compatibility matrix at: http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

Note This release is not compatible with, and cannot be used with, the currently available Security Management releases. A compatible Security Management release will be available shortly.

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 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 off 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.

Note When you upgrade or reboot Cisco Web Security appliance S690F with Nexus 56128P Switch Interface, the 10G fiber interface link status shows 'down'. Perform the following procedure to resolve this issue:

a. Configure the ‘media’ of the appliance interface to **10Gbase-SR** using the CLI command `etherconfig > media`.

b. Commit and reboot the appliance.

Note Reboot the S695F Cisco Web Security appliance after every SFP swap made from 1G SFP to 10G SFP (or conversely) on a fiber interface. It ensures that the driver buffer settings adjust properly for the intended bandwidth change.

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. Then ssh to the appliance and accept the connection with the new key.
- If you use SCP push to transfer logs to a remote server (including Splunk): Clear the old SSH host key for the appliance from the remote server.
- 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 the "File Reputation Filtering and File Analysis" chapter in the user guide PDF. (This PDF is more current than the online help in AsyncOS 8.8.)

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 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, and you 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.

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

- Lists of Known and Fixed Issues in Release 12.0.5-011, on page 21
- Lists of Known and Fixed Issues in Release 12.0.4-002, on page 21
- Lists of Known and Fixed Issues in Release 12.0.3-007, on page 21
- Lists of Known and Fixed Issues in Release 12.0.3-005, on page 21

Lists of Known and Fixed Issues in Release 12.0.5-011

- Fixed Issues
- Known Issues

Lists of Known and Fixed Issues in Release 12.0.4-002

- Fixed Issues
- Known Issues

Lists of Known and Fixed Issues in Release 12.0.3-007

- Fixed Issues
- Known Issues

Lists of Known and Fixed Issues in Release 12.0.3-005

- Fixed Issues
- Known Issues

Lists of Known and Fixed Issues in Release 12.0.2-012

- Fixed Issues
- Known Issues

Lists of Known and Fixed Issues in Release 12.0.2-004

- Fixed Issues
- Known Issues

Lists of Known and Fixed Issues in Release 12.0.1-334

- Fixed Issues
- Known Issues

Lists of Known and Fixed Issues in Release 12.0.1-268

- 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 Web Security 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 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.