Release Notes for AsyncOS 11.8.x for Cisco Web Security Appliances

Published: July 22, 2019

Last Updated: July 28, 2021

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

What's New in AsyncOS 11.8.4-004 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 11.8.4-004, page 25 for additional information.

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

What's New in AsyncOS 11.8.3-021 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 11.8.3-021, page 25 and Changes in Behavior in Asyncos 11.8.3-021, page 7 for additional information.

What's New in AsyncOS 11.8.3-018 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 11.8.3-018, page 25 and Changes in Behavior in Asyncos 11.8.3-018, page 8 for additional information.

What's New in AsyncOS 11.8.2-009 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 11.8.2-009, page 26 for additional information.

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 11.8.2 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 https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/content_security_general/Decommissioning_Legacy_File_Reputation_Servers_for_Cisco_Web_Security_Appliance.pdf.

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

New Command Line	Description
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.
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 11.8.1-023 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 11.8.1-023, page 26 for additional information.

The release includes a new `scanners` subcommand under `advancedproxyconfig` CLI command.

Enhancement	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 11.8.0-453 GD (General Deployment) Refresh

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 11.8.0-453, page 26 for additional information.

What's New in AsyncOS 11.8.0-440 GD (General Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 11.8.0-440, page 26 for additional information.

What's New in AsyncOS 11.8.0-429 LD (Limited Deployment) Refresh

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 11.8.0-429, page 26 for additional information.

What's New in AsyncOS 11.8.0-414 LD (Limited Deployment)

Feature	Description
ISE/ISE-PIC Integrations Enhancements	• You can construct access policies using Secure Group Tags and Active Directory groups. • For users that fail transparent identification with ISE/ISE-PIC, you can configure fallback authentication with Active Directory based realms. • You can configure authentication of users in Virtual Desktop Environments (Citrix, Microsoft shared/remote desktop services). **Note** Fallback authentication for Virtual Desktop Environments (VDI) users is not supported. **Note** Ensure that the number of maximum remote desktop sessions is the same in the Cisco Terminal Services agent and Microsoft server settings. This prevents incorrect session information from being sent to the Web Security appliance from ISE, and avoids false authentication for new sessions. See the "Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service" topic in the user guide.
Domain Map	You can now configure the appliance to allow passthrough of specific HTTPS traffic without any modification to client requests and certificate checks of the destination servers. See the "Intercepting Web Requests" chapter in the user guide.
Rollback of Configuration of the appliance	A new CLI command `rollbackconfig` is added. Use this command to rollback to one of the previously committed 10 configurations. The rollback configuration feature is enabled by default. See the "Command Line Interface" chapter in the user guide.
Automated Backup of the Appliance Configurations	A new log type 'Configuration History Logs' is added. Use this log type to subscribe for the configuration files and send them to a remotely located backup server through FTP or SCP. See the "Monitor System Activity Through Logs" chapter in the user guide.
Support for Exception List for External Feeds and O365 Feeds	You can exclude sites and regular expressions from the feed file of the Custom and External URL categories. This is applicable only for External Live Feed Category. See the "Classify URLs for Policy Application" chapter in the user guide.

Feature	Description
Proxy Bypass setting for O365 Web Services Feed	You can add the domain names or IP addresses of the Custom URL categories (O365 URLs) to the proxy bypass list. You do not need to add the domain names or the IP addresses of the custom URL categories manually. See the "InterceptingWeb Requests" chapter in the user guide.
Support for Cisco AMP Threat Grid Clustering for File Analysis	You can now add standalone or clustered Cisco AMP Threat Grid appliances for file analysis in the following way: Security Services > File Reputation and Analysis page in the web interface. See the "File Reputation Filtering and File Analysis" chapter in the user guide.
Configuring Threshold Settings for File Analysis	You can now set the upper threshold limit for the acceptable file analysis score. The files that are blocked based on the Threshold Settings are displayed as **Custom Threshold** in the Incoming Malware Threat Files section of the Advanced Malware Protection report. See the "File Reputation Filtering and File Analysis" chapter in the user guide.
Configuring URL Filtering with Multiple Web Category	You can now configure the URL filtering engine with multiple URL categories. The multiple URL category feature is applicable only for access policies. See "Classify URLs for Policy Application" chapter in the user guide.
Support for New Threat Categories	The appliance now has new 22 threat categories. The list of the new threat categories is automatically updated in the new web interface of the appliance whenever new categories are available. See 'Release Notes for URL Category and Threat Category Updates for Cisco Web and Email Security Appliances'.
New Web Interface for Monitoring and Tracking	The appliance now has a new web interface for Monitoring and Tracking reports. In the **Monitoring** page, you can view reports classified under General reports and Threat reports. In the **Tracking** page, you can search for messages or a group of messages depending on your search criteria in Tracking > Search page in the web interface. See "Tracking Messages" chapter in the user guide. For more information, see "Web Security Appliance Reports on the New Web Interface" chapter in the user guide. To access the new web interface, see "Accessing the Appliance Web Interface" topic in the "Introduction to the Product and the Release" chapter in the user guide. Also, see Accessing the New Web Interface, page 10.

Note The Web Reputation Engine name is changed to Talos Intelligence Engine.

The current version of the Advanced Malware Protection pre-classification engine is 1.0.0-113. The Advanced Malware Protection pre-classification engine has been updated recently and the version is changed from 1.0.0-007 to 1.0.0-113.

Note The appliance supports only the following ports in the factory default mode:
- 8080
- 8443
- 22

Note Cisco Web Security Appliance is FIPS certified and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. # 2984).

Changes in Behavior

Changes in Behavior in Asyncos 11.8.3-021

Appliance certificates (FIPS Mode)	The appliance rejects the import and upload of signed appliance certificates if: • Any of the intermediate certificates is expired • OCSP validation is not successful for any of the intermediate certificates. The OCSP validation is applicable for a maximum of five levels in the certificate chain. You can view the reason for rejection in the audit logs.

Changes in Behavior in Asyncos 11.8.3-018

Log Subscriptions	Now, you can configure the log subscription only within the size limit of the disk capacity. The web user interface and the CLI of the appliance now display warning messages if there are pre-existing log subscriptions configured with a size limit that exceed the disk capacity. The messages are displayed when you try to: • Commit changes regarding log subscription through the web user interface • Login or connect to the web user interface on the **My Dashboard** page • Login or connect through CLI

Changes in Behavior in Asyncos 11.8.x

TLS Version	By default, the following essential services provided over the management/data plane will have the minimum version as TLS 1.1: • WSA WUI • Proxy services • Secure LDAP • RADSEC • Secure ICAP services • Update service **Note** By default TLS 1.0 is disabled after the appliance is upgraded to 11.8.x versions. **Note** The TLS compression feature is disabled by default for best security. To enable this feature, upgrade the appliance to 12.0 or later versions. Enabling TLS compression on previous versions may cause issue with the appliance function.
FTP Proxy Service	By default, the FTP proxy service is disabled. If the FTP proxy has been enabled on your appliance, it will remain as enabled even after the upgrade.
Audit log for Authorization Changes	The audit logs now show the changes that are made to the authorization policy. If the user has changed the rights and privileges in the authorization policy (System Administration > Users), the same will be shown in the audit logs.
Change in Default Certificate Validity Period	The appliance Default Certificate Validity period has been reduced from 10 years to 5 years.
Ciphers for SSH client and server services.	In FIPS mode, `ssh-rsa` is the only supported public key authentication cipher for SSH client and server services. The following ciphers are additionally supported for SSH client service in the FIPS mode: • `aes128-ctr` and `aes256-ctr` • `ecdh-sha2-nistp256`, `ecdh-sha2-nistp384`, and `ecdh-sha2-nistp521`.

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 **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 `trailerblazerconfig` CLI command. For more information on 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 on the `interfaceconfig` CLI command, see “Command Line Interface” chapter in the user guide.

If you change these default ports, then 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 (Latest Stable Version)
- Mozilla Firefox (Latest Stable Version)

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 following virtual models:
  - S100V
  - S300V
  - S600V
- The following hardware models:
  - x80
  - x90
  - x95

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 11.8.4-004 (MD - Maintenance Deployment), page 11
- Upgrading to AsyncOS 11.8.3-021 (MD - Maintenance Deployment), page 12
- Upgrading to AsyncOS 11.8.3-018 (MD - Maintenance Deployment), page 13
- Upgrading to AsyncOS 11.8.2-009 (MD - Maintenance Deployment), page 14
- Upgrading to AsyncOS 11.8.1-023 (MD - Maintenance Deployment), page 15
- Upgrading to AsyncOS 11.8.0-453 (GD - General Deployment) Refresh, page 15
- Upgrading to AsyncOS 11.8.0-440 (GD - General Deployment), page 16
- Upgrading to AsyncOS 11.8.0-429 (LD - Limited Deployment) - Refresh, page 16
- Upgrading to AsyncOS 11.8.0-414 (LD - Limited Deployment), page 17

Upgrading to AsyncOS 11.8.4-004 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 17 and Installation and Upgrade Notes, page 19.

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

You can upgrade to release 11.8.4-004 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

Upgrading to AsyncOS 11.8.3-021 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 17 and Installation and Upgrade Notes, page 19.

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

You can upgrade to release 11.8.3-021 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
- 11.5.1-115
- 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
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.2-011
- 11.7.3-025
- 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
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018

Note Upgrade from AsyncOS 11.8.3-021 to AsyncOS 12.0.x/12.5.x will be available from June 2021.

Upgrading to AsyncOS 11.8.3-018 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 17 and Installation and Upgrade Notes, page 19.

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

You can upgrade to release 11.8.3-018 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
- 11.5.1-115
- 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
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.2-011
- 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
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.2-009
- 11.8.2-702

Upgrading to AsyncOS 11.8.2-009 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 17 and Installation and Upgrade Notes, page 19.

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

You can upgrade to release 11.8.2-009 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
- 10.5.6-024
- 10.6.0-240
- 10.6.0-244
- 11.5.1-115
- 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
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.2-011
- 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
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604

Upgrading to AsyncOS 11.8.1-023 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 17 and Installation and Upgrade Notes, page 19.

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

You can upgrade to release 11-8-1-023 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
- 11.5.1-115
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 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

Upgrading to AsyncOS 11.8.0-453 (GD - General Deployment) Refresh

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 17 and Installation and Upgrade Notes, page 19.

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

You can upgrade to release 11-8-0-453 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

The SMA 12.5.0-683, SMA 13.6.2-058, and SMA 13.8.1-068 version is not compatible with WSA 11.8.0-453 version when you try to add the external feed in the Custom URL Category through the Configuration Master (CM) and apply the configurations to the Web Security Appliances with older versions.

You can upgrade the Web Security Appliance to 11.8.2-xxx version or later to address the compatibility limitation.

For more information, click here.

Upgrading to AsyncOS 11.8.0-440 (GD - General Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 17 and Installation and Upgrade Notes, page 19.

You can upgrade to release 11-8-0-440 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
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.8.0-348
- 11.8.0-414
- 11.8.0-429

Note While upgrading from AsyncOS 11.8.0-414 to 11.8.0-440, Web Security Appliance supports only 10G SFP for a 10G interface. In all previous versions of AsyncOS, 1000Base-SX SFP was supported for 10G interface.

Upgrading to AsyncOS 11.8.0-429 (LD - Limited Deployment) - Refresh

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 17 and Installation and Upgrade Notes, page 19.

You can upgrade to release 11-8-0-429 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
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.8.0-348
- 11.8.0-414

Upgrading to AsyncOS 11.8.0-414 (LD - Limited Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 17 and Installation and Upgrade Notes, page 19.

You can upgrade to release 11-8-0-414 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.4-017
- 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
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.8.0-348

Note After you upgrade to AsyncOS 11.8 for Cisco Web Security Appliances, your browser must be enabled for TLS v 1.1 to access the web user interface.

Pre-upgrade Requirements

AsyncOS 11.8 for Web Security appliances only supports ISE release 2.4.

Other requirements are:

- Upgrade from Earlier Versions of AsyncOS with CTA Log Subscription, to AsyncOS 11.5, page 17
- Upgrade from AsyncOS Earlier Versions with Cloudlock Log Subscription to AsyncOS 11.5, page 18
- Upgrade from AsyncOS 11.5.x or Earlier Versions to AsyncOS 11.8, page 18
- Check Post-upgrade Requirements Before Upgrading, page 18

Upgrade from Earlier Versions of AsyncOS with CTA Log Subscription, to AsyncOS 11.5

- Upgrade from AsyncOS 11.0 to 11.5, page 17
- Upgrade from AsyncOS Pre-11.0 Releases to 11.5, page 18

Upgrade from AsyncOS 11.0 to 11.5

The following conditions should be met, if you have already configured a CTA log in AsyncOS 11.0 version and want to upgrade to AsyncOS 11.5 version:

- The log name must be ‘cta_log’.
- Retrieval method for the log must be ‘scp_push’.

- The 'CTA Enable' checkbox must be checked. Only then it will be considered as a CTA log after upgrading to 11.5 version.
- In case, any of the above mentioned conditions is not met, the log will be considered as a standard log after upgrade.

Upgrade from AsyncOS Pre-11.0 Releases to 11.5

The following conditions must be met, if you have already configured a CTA log in AsyncOS pre-11.0 releases and want to upgrade to AsyncOS 11.5 version:

- The log name must be 'cta_log'.
- Retrieval method for the log must be 'scp_push'. Only then it will be considered as a CTA log after upgrading to 11.5 version.
- In case, any of the above mentioned conditions is not met, the log will be considered as a standard log after upgrade.

Upgrade from AsyncOS Earlier Versions with Cloudlock Log Subscription to AsyncOS 11.5

The following conditions must be met, if you have already configured a Cloudlock log in AsyncOS earlier releases and want to upgrade to AsyncOS 11.5 version:

- The log name must be 'cloudlock_log'.
- Retrieval method for the log must be 'scp_push'. Only then it will be considered as a Cloudlock log after upgrading to 11.5 version.
- In case, any of the above mentioned condition is not met, the log will be considered as a standard W3C log after upgrade.

Upgrade from AsyncOS 11.5.x or Earlier Versions to AsyncOS 11.8

The following conditions must be met before you upgrade from AsyncOS version 11.5.x or earlier to AsyncOS 11.8:

- If your appliance runs on AsyncOS 11.5.x or earlier versions, you must update all security engines on your appliance before upgrading to AsyncOS 11.8.
- If you are unable to update the security engines on your existing appliance with AsyncOS version 11.5.x or earlier, first upgrade your appliance to AsyncOS 11.7.0 and then to AsyncOS 11.8 version.

Note Contact Cisco TAC if you have disabled the WBRS engine on your appliance and upgraded to AsyncOS 11.8 from Async 11.5.x version directly. Ensure that the appliance is accessible remotely.

Check Post-upgrade Requirements Before Upgrading

Some existing functionality will not work after upgrade until you make changes. To minimize downtime, familiarize yourself with and prepare for those requirements before upgrading. See Important! Actions Required After Upgrading.

Installation and Upgrade Notes

- Compatibility Details
- Deploying a Virtual Appliance
- Demo Security Certificate Encryption Strength
- Post-upgrade Reboot

Compatibility Details

- Compatibility with Cisco AsyncOS for Security Management
- IPv6 and Kerberos Not Available in Cloud Connector Mode
- Functional Support for IPv6 Addresses
- Availability of Kerberos Authentication for Operating Systems and Browsers

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 functions 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 functions 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 from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Note The following are the limitations for virtual Web Security appliances (with FreeBSD 10.x) deployed on Microsoft Hyper-V generation 1 platform:

- It is not possible to modify the virtual appliance interfaces using the `etherconfig` CLI command.
- The `ifconfig` CLI command displays the virtual appliance interface status as Unknown or Simplex even though it runs on Duplex mode.

However, there is no impact on the performance of the appliance due to the above limitations.

Migrating from a Hardware Appliance to a Virtual Appliance

Step 1 Set up your virtual appliance with this AsyncOS release using the documentation described in Deploying a Virtual Appliance, page 21.

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 will not work.

Demo Security Certificate Encryption Strength

The encryption strength of the demo security certificate is 1024 bits both before and after upgrade to AsyncOS 8.5. With upgrade to AsyncOS 9.1.1, it is 2048 bits. With AsyncOS 10.5 and later, when FIPS mode is enabled, the demo security certificate strength is changed to 4096 bits.

Post-upgrade Reboot

You must reboot the Web Security appliance after you upgrade.

Upgrading AsyncOS for Web

Before You Begin

Perform preupgrade requirements. See Pre-upgrade Requirements, page 17.

Step 1 Log in as Administrator.

Step 2 On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.

Step 3 On the System Administration > System Upgrade page, click **Upgrade Options**

Step 4 Select **Download** or **Download and Install** as required.

Choose from the list of available upgrades.

Step 5 Click **Proceed** to start the upgrade or download. Answer the questions as they appear.

If you chose **Download only**, the AsyncOS upgrade image will be downloaded to the appliance and the administrator can choose to install the downloaded image later.

Step 6 (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.

New features are typically not enabled by default.

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:

1. Configure the ‘*media*’ of the appliance interface to **10Gbase-SR** using the CLI command `etherconfig` > `media`.
2. 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, page 23
- Virtual Appliances: Required Changes for SSH Security Vulnerability Fix, page 23
- File Analysis: Required Changes to View Analysis Result Details in the Cloud, page 24
- File Analysis: Verify File Types To Be Analyzed, page 24

- Unescaped Dots in Regular Expressions, page 24

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:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA
```

Caution Make sure you paste the preceding 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, page 27.

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, page 25
- Lists of Known and Fixed Issues, page 25
- Related Documentation, page 27

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 11.8.4-004

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=11.8.4-004&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=11.8.4&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 11.8.3-021

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=11.8.3-021&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=11.8&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 11.8.3-018

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=11.8.3-018&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=11.8&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 11.8.2-009

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.2-009&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 11.8.1-023

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.1-023&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.1&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 11.8.0-453

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0-453&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 11.8.0-440

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0-440&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 11.8.0-429

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0-429&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 11.8.0-414

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0-414&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0&sb=afr&sts=open&svr=3nH&bt=custV

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, 11.8.0

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 Show Bugs drop down.
- To view the list of known issues, select **Affecting these Releases** from the Show Bugs 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 for this product is available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html.

Documentation for virtual appliances is available from

https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html

Documentation for Cisco Content Security Management Appliances is available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html.

List of Ciphers for AsyncOS 11.5. for Cisco Web Security Appliances is available from

https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-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://community.cisco.com/t5/web-security/bd-p/5786-discussions-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.

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.