



# Release Notes for AsyncOS 11.7.x for Cisco Web Security Appliances

---

**Published: December 11, 2018**

**Revised: March 02, 2021**

## Contents

- [What's New, page 2](#)
- [Changes in Behavior, page 8](#)
- [Release Classification, page 8](#)
- [Supported Hardware for This Release, page 8](#)
- [Upgrade Paths, page 9](#)
- [Pre-upgrade Requirements, page 13](#)
- [Installation and Upgrade Notes, page 14](#)
- [Upgrading AsyncOS for Web, page 17](#)
- [Important! Actions Required After Upgrading, page 17](#)
- [Documentation Updates, page 19](#)
- [Known and Fixed Issues, page 19](#)
- [Related Documentation, page 22](#)
- [Support, page 22](#)




## What's New

- [What's New in AsyncOS 11.7.3-025 - MD \(Maintenance Deployment\), page 2](#)
- [What's New in AsyncOS 11.7.2-011 - MD \(Maintenance Deployment\), page 3](#)
- [What's New in AsyncOS 11.7.1-049 - MD \(Maintenance Deployment\), page 3](#)
- [What's New in AsyncOS 11.7.1-020 - MD \(Maintenance Deployment\) Refresh, page 3](#)
- [What's New in AsyncOS 11.7.1-006 - MD \(Maintenance Deployment\), page 3](#)
- [What's New in AsyncOS 11.7.0-418 - GD \(General Deployment\) Refresh, page 3](#)
- [What's New in AsyncOS 11.7.0-407 - GD \(General Deployment\) Refresh, page 4](#)
- [What's New in AsyncOS 11.7.0-406 - Deprovisioned, page 7](#)

### What's New in AsyncOS 11.7.3-025 - MD (Maintenance Deployment)

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 11.7.3-025, page 20](#) for additional information.

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

New Command Line	Description
Deprecation of TLS 1.0/1.1	<p>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.</p> <p>Before you upgrade the appliance to the 11.7.3 version, the following is recommended:</p> <ul style="list-style-type: none"> <li>• 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).</li> <li>• After you upgrade the appliance, check if the File Reputation server is retained as AMERICAS (cloud-sa.amp.cisco.com).</li> </ul>
	<p> <b>Note</b> If you configure Europe or APJC as the File Reputation server before upgrading the appliance, the preceding conditions will not be applicable.</p> <p>For more information, see <a href="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">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</a>.</p>

## What's New in AsyncOS 11.7.2-011 - MD (Maintenance Deployment)

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 11.7.2-011, page 20](#) for additional information.

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	<p>A new option <code>Enter the number of concurrent scans to be supported by AMP</code> is added in the main CLI command <code>advancedproxyconfig &gt; scanners &gt; AMP</code>.</p> <p>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.</p>
Support to change the scan verdict during the eviction of long running scans	<p>A new CLI subcommand <code>eviction</code> is added in the main CLI command <code>advancedproxyconfig &gt; scanners</code>.</p> <p>Using the new CLI subcommand, you can change the default <b>Unscannable</b> verdict of long running scan eviction to <b>Timeout</b> and vice versa.</p>

## What's New in AsyncOS 11.7.1-049 - MD (Maintenance Deployment)

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 11.7.1-049, page 20](#) for additional information.

## What's New in AsyncOS 11.7.1-020 - MD (Maintenance Deployment) Refresh

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 11.7.1-020, page 20](#) for additional information.


## What's New in AsyncOS 11.7.1-006 - MD (Maintenance Deployment)



This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 11.7.1-006, page 21](#) for additional information.



## What's New in AsyncOS 11.7.0-418 - GD (General Deployment) Refresh



This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 11.7.0-418, page 21](#) for additional information.

## What's New in AsyncOS 11.7.0-407 - GD (General Deployment) Refresh

Feature	Description
Secure Group Tags and Active Directory Groups Support in ISE Integrations	In ISE integrations, you can use Secure Group Tags (SGTs) and Active Directory Groups (AD Groups) information received from ISE to construct access policies.
Encapsulated URL Protection	<p>URL category filtering will be applied to all transactions that go through translate.google.com, further fortifying the ability to identify and take action on all transactions.</p> <p>You must enable the HTTPS proxy and choose to decrypt HTTPS requests.</p>
Enhanced Web-based reputation score (WBRS) Engine	The WBRS engine is enhanced to improve the efficacy of web reputation and web category information for URLs.
Support for 30 Feed Files in External Live Feed for Custom and External URL Categories	<p>You can use up to 30 feed files with URL category definitions, with each file containing up to 5,000 entries.</p> <p> <b>Note</b> The maximum entries you can use is 5000. Increasing the number of external feed entries causes performance degradation. For optimal performance, you can use 1500 entries for each feed file, or a combined total of 45,000 entries.</p>
Server Name Indication (SNI) Information in reports	The appliance now provides the SNI of pass-through HTTPS transactions, which enables you to search for transactions for a specific website in the Web Tracking page.

Feature	Description
ISE-PIC Integration	<p>You can now configure your appliance to transparently identify users with ISE-PIC version 2.4 (with pxGrid version 2.0). ISE-PIC fetches user-identity information (user names and Active Directory groups) to allow transparent user identification in policies configured to use those profiles.</p> <hr/> <p> <b>Note</b> When you upgrade to AsyncOS 11.7 for Web Security appliances, you must reconfigure ISE for a successful integration. Any previously configured ISE functionality will not work until the ISE is reconfigured again.</p> <hr/> <p> <b>Note</b> AsyncOS 11.7 for Web Security appliances only supports ISE release 2.4. If the ISE versions in your deployment are older than ISE 2.4, continue to use AsyncOS releases for Web Security appliances earlier than 11.7.</p> <hr/> <p>For more information, see the “Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service” topic in the user guide.</p>

Feature	Description
<p>Improved Pre-classification Efficacy (Reducing File Uploads to Cisco AMP Threat Grid)</p>	<p>The File Analysis service in your appliance supports all the file types supported by Cisco AMP Threat Grid.</p> <ul style="list-style-type: none"> <li>You can upload files that only contain dynamic content for file analysis. This helps administrators to track the daily file upload limit. Previously, the on-box pre-classification engine filtered the files with a limited scope before sending them for analysis. Now, a new cloud-based Threat Grid pre-classification engine is added to filter and remove low risk files. This improves efficacy by saving the submission limit for possible malicious files.</li> <li>You can reduce file uploads for file analysis.</li> </ul> <p>To configure this feature, see the ‘Enabling and Configuring File Reputation and Analysis Services’ topic in the user guide.</p> <p> <b>Note</b> If you are using the private cloud file analysis server version 2.4 or an earlier version, it is recommended that you do not enable the new file types for file analysis.</p> <p>A new verdict – Low Risk is introduced when no dynamic content is found in a file after file analysis. You can view the verdict details in the <b>Incoming Files Handled by AMP</b> section of the Advanced Malware Protection report.</p> <p> <b>Note</b> The low risk files are not searchable in the File Analysis page in Reporting with their SHA because they are not sent for analysis to the AMP Threat Grid.</p>
<p>Login History Configuration</p>	<p>A new subcommand <code>loginhistory</code> is added to the CLI command <code>adminaccessconfig</code> to configure the number of days for which the login history is retained.</p> <p>Default value is 1 day.</p> <p>This is available in FIPS and non-FIPS mode.</p>
<p>Maximum Concurrent Login Sessions Configuration</p>	<p>A new subcommand <code>maxsessions</code> is added to the CLI command <code>adminaccessconfig</code> to configure the maximum number of concurrent sessions of the appliance through the Command Line Interface and web interface.</p> <p>Default value in FIPS mode is 3 and non-FIPS mode is 10.</p> <p>This is available in FIPS and non-FIPS mode.</p>

Feature	Description
Support for Smart Software Licensing	<p>Smart Software Licensing enables you to manage and monitor Cisco Web Security appliance licenses seamlessly. To activate Smart Software licensing, you must register your appliance with Cisco Smart Software Manager (CSSM), which is the centralized database that maintains the licensing details of all the Cisco products that you purchase and use.</p> <p> <b>Caution</b> After you enable the Smart Licensing mode on your appliance, you will not be able to revert to the Classic Licensing mode.</p> <p>For more information, see the “Smart Software Licensing” topic in the user guide.</p>
Enhanced User Experience Using Walkthroughs	<p>The appliance provides walkthroughs to assist you in accomplishing a particular configuration task. The following walkthroughs are supported in this release:</p> <ul style="list-style-type: none"> <li>• Authenticate end-users using Active Directory – NTLM</li> <li>• Authenticate end-users using Active Directory – Kerberos</li> <li>• Decrypt HTTPS traffic</li> <li>• Configure Transparent User Identification using ISE or ISE-PIC</li> </ul> <p> <b>Note</b> The list of walkthroughs is cloud updateable. Make sure that you clear your browser cache to view an updated version of the How-Tos widget and pop-up window.</p> <p>For information on how to enable the walkthroughs, see the “Additional Security Settings for Accessing the Appliance” topic in the user guide.</p>
Disk size flexibility support for virtual appliances	<p>This release of AsyncOS supports disk size flexibility for virtual appliances.</p> <p>For more information, see the Cisco Content Security Virtual Appliance Installation Guide.</p>

## What's New in AsyncOS 11.7.0-406 - Deprovisioned

This release was deprovisioned on May 23, 2019.

## Changes in Behavior

- [Changes in Behavior in AsyncOS 11.7, page 8](#)

### Changes in Behavior in AsyncOS 11.7

Log Subscription Names	Non-ASCII characters and whitespaces in log subscription names are not supported. Upgrade will fail if the log subscription file names contain any non-supported characters.
Changes to the output of the <code>version</code> CLI command, specific to the Enhanced Web-based reputation score (WBRs) Engine	<p>The output of the <code>version</code> CLI command, specific to the Enhanced Web-based reputation score (WBRs) Engine will appear slightly different, but all functions and efficacy remain the same.</p> <p>Example output is shown below:</p> <pre>Cisco Web Usage Controls - Web Categorization Engine: 1.12.4.944 (Never Updated) Web Reputation IP Filters: 1529708330 (Never Updated) Web Reputation Rules: 1528401763 (Never Updated) Web Reputation URL Queries Database: 1529706637 (Never Updated) Web Reputation Engine: 1.12.4.944 (Never Updated)</pre> <p>The <code>Web Reputation URL Queries Database</code> line represents the <code>Reputation Prefix Filters</code> in versions earlier than 11.7.</p>

## 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 models:

- S000V
- S100V
- S300V
- S600V
- x90
- x80



# Upgrade Paths


**Note**

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


**Note**

Before you start the upgrade process, see [Pre-upgrade Requirements, page 13](#) and [Installation and Upgrade Notes, page 14](#).

- [Upgrade Paths for 11.7.3-025 - MD \(Maintenance Deployment\), page 9](#)
- [Upgrade Paths for 11.7.2-011 - MD \(Maintenance Deployment\), page 9](#)
- [Upgrade Paths for 11.7.1-049 - MD \(Maintenance Deployment\), page 11](#)
- [Upgrade Paths for 11.7.1-020 - MD \(Maintenance Deployment\) Refresh, page 11](#)
- [Upgrade Paths for 11.7.1-006 - MD \(Maintenance Deployment\), page 12](#)
- [Upgrade Paths for 11.7.0-418 - GD \(General Deployment\) Refresh, page 12](#)
- [Upgrade Paths for 11.7.0-407 - GD \(General Deployment\) Refresh, page 12](#)

## Upgrade Paths for 11.7.3-025 - MD (Maintenance Deployment)

You can upgrade to release 11.7.3-025 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
- 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
- 11.7.1-501
- 11.7.2-011

## Upgrade Paths for 11.7.2-011 - MD (Maintenance Deployment)

You can upgrade to release 11.7.2-011 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
- 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
- 11.7.1-049

## Upgrade Paths for 11.7.1-049 - MD (Maintenance Deployment)

You can upgrade to release 11.7.1-049 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
- 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

## Upgrade Paths for 11.7.1-020 - MD (Maintenance Deployment) Refresh

You can upgrade to release 11.7.1-020 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
- 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

## Upgrade Paths for 11.7.1-006 - MD (Maintenance Deployment)

You can upgrade to release 11.7.1-006 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.1-235
- 10.1.4-017
- 10.1.5-004
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 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

## Upgrade Paths for 11.7.0-418 - GD (General Deployment) Refresh

You can upgrade to release 11.7.0-418 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.1-235
- 10.1.4-017
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11-5-3-003
- 11.5.3-016
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407

## Upgrade Paths for 11.7.0-407 - GD (General Deployment) Refresh

You can upgrade to release 11.7.0-407 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.1-235
- 10.1.4-017
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11.7.0-334
- 11.7.0-406

**Note**

Upgrading to AsyncOS 11.7.0-407 release for virtual appliances is not supported due to a defect which might corrupt the reporting and web tracking database. A refresh release with this fix for the virtuals will be released before End of June 2019.

# Pre-upgrade Requirements

AsyncOS 11.7 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 13](#)
- [Upgrade from AsyncOS Earlier Versions with Cloudlock Log Subscription to AsyncOS 11.5, page 13](#)
- [Check Post-upgrade Requirements Before Upgrading, page 14](#)

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

- [Upgrade from AsyncOS 11.0 to 11.5, page 13](#)
- [Upgrade from AsyncOS Pre-11.0 Releases to 11.5, page 13](#)

### 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.

## 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 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 from

<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

- 
- Step 1** Set up your virtual appliance with this AsyncOS release using the documentation described in [Deploying a Virtual Appliance, page 16](#).
- 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.
- 

## 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 13](#).

- 
- 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.

---

## 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 18](#)
- [Virtual Appliances: Required Changes for SSH Security Vulnerability Fix, page 18](#)
- [File Analysis: Required Changes to View Analysis Result Details in the Cloud, page 19](#)
- [File Analysis: Verify File Types To Be Analyzed, page 19](#)
- [Unescaped Dots in Regular Expressions, page 19](#)

## 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 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](http://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 22](#).

## 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 19](#)
- [Lists of Known and Fixed Issues, page 20](#)
- [Related Documentation, page 22](#)

## 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 11.7.3-025](#), page 20
- [Known and Fixed Issues in Release 11.7.2-011](#), page 20
- [Known and Fixed Issues in Release 11.7.1-049](#), page 20
- [Known and Fixed Issues in Release 11.7.1-020](#), page 20
- [Known and Fixed Issues in Release 11.7.1-006](#), page 21
- [Known and Fixed Issues in Release 11.7.0-418](#), page 21
- [Known and Fixed Issues in Release 11.7.0-407](#), page 21

### Known and Fixed Issues in Release 11.7.3-025

<b>Fixed Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282941570&amp;rls=11.7.3-025&amp;sb=fr&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282941570&amp;rls=11.7.3-025&amp;sb=fr&amp;svr=3nH&amp;bt=custV</a>
<b>Known Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282941570&amp;rls=11.7&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282941570&amp;rls=11.7&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV</a>

### Known and Fixed Issues in Release 11.7.2-011

<b>Fixed Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.2-011&amp;sb=fr&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.2-011&amp;sb=fr&amp;svr=3nH&amp;bt=custV</a>
<b>Known Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.2&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.2&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV</a>

### Known and Fixed Issues in Release 11.7.1-049

<b>Fixed Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1-049&amp;sb=fr&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1-049&amp;sb=fr&amp;svr=3nH&amp;bt=custV</a>
<b>Known Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV</a>

### Known and Fixed Issues in Release 11.7.1-020

<b>Fixed Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1-020&amp;sb=fr&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1-020&amp;sb=fr&amp;svr=3nH&amp;bt=custV</a>
<b>Known Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1&amp;sb=af&amp;sts=open&amp;svr=3nH&amp;bt=custV</a>

## Known and Fixed Issues in Release 11.7.1-006

<b>Fixed Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1-006&amp;sb=fr&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1-006&amp;sb=fr&amp;svr=3nH&amp;bt=custV</a>
<b>Known Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1&amp;sb=fr&amp;sts=open&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.1&amp;sb=fr&amp;sts=open&amp;svr=3nH&amp;bt=custV</a>

## Known and Fixed Issues in Release 11.7.0-418

<b>Fixed Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.0-418&amp;sb=fr&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.0-418&amp;sb=fr&amp;svr=3nH&amp;bt=custV</a>
<b>Known Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.0&amp;sb=fr&amp;sts=open&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.0&amp;sb=fr&amp;sts=open&amp;svr=3nH&amp;bt=custV</a>

## Known and Fixed Issues in Release 11.7.0-407

<b>Fixed Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.0-407&amp;sb=fr&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.0-407&amp;sb=fr&amp;svr=3nH&amp;bt=custV</a>
<b>Known Issues</b>	<a href="https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.0&amp;sb=fr&amp;sts=open&amp;svr=3nH&amp;bt=custV">https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&amp;pf=prdNm&amp;pfVal=282521310&amp;rls=11.7.0&amp;sb=fr&amp;sts=open&amp;svr=3nH&amp;bt=custV</a>

## 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, 11.7.0
  - 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](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.

---

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: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1110R)

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

© 2021 Cisco Systems, Inc. All rights reserved.

