



Release Notes for AsyncOS 10.1.x for Cisco Web Security Appliances

Published: September 1, 2016

Revised: January 20, 2020

Contents

- [What's New, page 1](#)
- [Release Classification, page 10](#)
- [Supported Hardware for This Release, page 10](#)
- [Upgrade Paths, page 11](#)
- [Pre-upgrade Requirements, page 17](#)
- [Installation and Upgrade Notes, page 17](#)
- [Upgrading AsyncOS for Web, page 20](#)
- [Important! Actions Required After Upgrading, page 21](#)
- [Documentation Updates, page 23](#)
- [Known and Fixed Issues, page 24](#)
- [Related Documentation, page 27](#)
- [Support, page 27](#)

What's New

- [What's New In Cisco AsyncOS 10.1.5-034 MD \(Maintenance Deployment\), page 2](#)
- [What's New In Cisco AsyncOS 10.1.5-004 \(MD - Maintenance Deployment\), page 3](#)
- [What's New In Cisco AsyncOS 10.1.4-017 \(MD - Maintenance Deployment\), page 3](#)
- [What's New In Cisco AsyncOS 10.1.4-007 \(MD - Maintenance Deployment\), page 3](#)



- [What's New In Cisco AsyncOS 10.1.3-054 \(MD - Maintenance Deployment\)](#), page 3
- [Cisco AsyncOS 10.1.2-036 - Deprovisioned](#), page 4
- [What's New In Cisco AsyncOS 10.1.1-235 \(Maintenance Deployment\) Refresh](#), page 4
- [What's New In Cisco AsyncOS 10.1.1-234 \(Maintenance Deployment\)](#), page 4
- [What's New In Cisco AsyncOS 10.1.1-230 \(Maintenance Deployment\)](#), page 4
- [What's New In Cisco AsyncOS 10.1.0 \(General Deployment\)](#), page 5
- [What's New In Cisco AsyncOS 10.0.0 \(Limited Deployment\)](#), page 6

**Note**

For AsyncOS 10.1.x versions: After an upgrade, if the appliance is configured with Kerberos, the authentication processes will exhibit high CPU usage. We recommend reducing the number of concurrent Kerberos authentications, or using IP surrogates with surrogate timeouts above 15 minutes. This will prevent latency for end user web requests. For the traffic that cannot use IP surrogates, use an identification profile and session cookies-based authentication surrogates. Be aware that when you commit changes to Identification Profiles, end-users must re-authenticate.

What's New In Cisco AsyncOS 10.1.5-034 MD (Maintenance Deployment)

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 10.1.5-037](#), page 24 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 10.1.5-034 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.


What's New In Cisco AsyncOS 10.1.5-004 (MD - Maintenance Deployment)

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 10.1.5-004](#), [page 25](#) for additional information for additional information.

What's New In Cisco AsyncOS 10.1.4-017 (MD - Maintenance Deployment)

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 10.1.4-017](#) for additional information for additional information.

What's New In Cisco AsyncOS 10.1.4-007 (MD - Maintenance Deployment)

| Feature | Description |
|---------------------------------------|--|
| Enable or Disable Incremental Updates | You can use the CLI command <code>updateconfig > setup</code> to enable or disable incremental updates from the Web Reputation service. Even after you disable incremental updates, the appliance will continue to download the full updates from the Cisco server. |
| |  Note Disabling incremental updates will result in delays in receiving updated web reputation information on the appliance. |
| | For more information, see “Web Security Appliance CLI Commands” in the user guide. |

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 10.1.4-007](#) for additional information for additional information.

What's New In Cisco AsyncOS 10.1.3-054 (MD - Maintenance Deployment)

| Feature | Description |
|---|--|
| Configure the number of Kerberos authentication helpers | You can use the CLI command <code>modifyauthhelpers</code> to configure the number of Kerberos authentication helpers. |

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 10.1.3-054](#) for additional information for additional information.

Cisco AsyncOS 10.1.3-039 - Deprovisioned

This release was deprovisioned on July 12, 2018.

Cisco AsyncOS 10.1.2-050 - Deprovisioned

This release was deprovisioned on July 12, 2018.

Cisco AsyncOS 10.1.2-036 - Deprovisioned

This release was deprovisioned on December 14, 2017.

What's New In Cisco AsyncOS 10.1.1-235 (Maintenance Deployment) Refresh

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 10.1.1-235](#) for additional information.

What's New In Cisco AsyncOS 10.1.1-234 (Maintenance Deployment)

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 10.1.1-234](#) for additional information.

What's New In Cisco AsyncOS 10.1.1-230 (Maintenance Deployment)

This release contains a number of bug fixes; see the [Known and Fixed Issues in Release 10.1.1-230](#) for additional information.

What's New In Cisco AsyncOS 10.1.0 (General Deployment)

| Feature | Description |
|---|---|
| Archive Inspection | You can now Allow, Block, or Inspect specific types of “Inspectable Archives.” Inspectable Archives are archive or compressed files that the WSA can inflate to inspect each of the contained files in order to apply the file-type block policy. The Inspectable Archives list includes archive types such as ZIP, Microsoft CAB, RAR, and TAR. See “Access Policies: Blocking Objects” in the User Guide. |
| Centralized Upgrade Management | With this feature, you can simultaneously upgrade multiple WSAs using a single Security Management Appliance (SMA). You also can apply a different software upgrade for each WSA. |
| Dynamic TCP window sizing | The CLI command <code>networktuning</code> can be used to enable and disable dynamic sizing of the TCP send- and receive-space buffers based on system load and available resources. |
| Enable/disable TCP RST (reset) forwarding | You can use the “Do you want to forward TCP RST sent by server to client?” option, added to CLI <code>advancedproxyconfig > MISCELLANEOUS</code> , to enable and disable TCP RST (reset) forwarding. See “Web Security Appliance CLI Commands” in the User Guide. |
| S600V support | The S600V virtual appliance model is supported for OVF as well as KVM deployments. See the Cisco Content Security Virtual Appliance Installation Guide for more information. |
| New Europe region servers added for File Reputation and File Analysis | <p>Cisco has added two new servers in the Europe region for Advanced Malware Protection Services:</p> <p>File Reputation Server - EUROPE (cloud-sa.eu.amp.cisco.com)</p> <p>File Analysis Server - EUROPE (https://panacea.threatgrid.com)</p> <p>You can choose these servers for File Reputation and File Analysis. See the File Reputation Filtering and File Analysis chapter in the User Guide.</p> |

What's New In Cisco AsyncOS 10.0.0 (Limited Deployment)

| Feature | Description |
|----------------------------|---|
| <code>curl</code> command | <p>You can send a cURL request directly to a Web server, or to a Web server via proxy, with the request and response HTTP headers returned to let you determine why a Web page is failing to load. See “Web Security Appliance CLI Commands” in the User Guide.</p> <p>Note This command is for Administrator or Operator use only, under TAC supervision.</p> |
| Referrer Exceptions | <p>You can now define exceptions to the default actions configured for embedded/referred content. A Website may embed or refer to content that is categorized differently than the source page, or that is considered an application of a different type than the source. By default, embedded/referred content is blocked or monitored based on the action selected for its assigned category or application, regardless of how the source Website is categorized. See “Exceptions to Blocking for Embedded and Referred Content” in the User Guide.</p> |
| AMP Private Cloud | <p>A Cisco AMP Virtual Private Cloud appliance can now be deployed on-premises in “air-gap” mode to provide private file reputation filtering for connected WSAs. See “Enabling and Configuring the File Reputation and Analysis Services” in the User Guide.</p> |
| AMP Reporting enhancements | <p>The AMP-related report pages have been enhanced, including new reporting panels and displays, additional columns of information in existing reporting panels, as well as cross-links between certain reports.</p> <p>Retrospective alerts now provide additional information, including file name and total number of users infected. In addition, the formatting of retrospective alerts has been updated to make them more “readable.”</p> <p>A new log-entry field was added to the access logs; a file-verdict number appended to the end of the log entry, as follows:</p> <ul style="list-style-type: none"> 1 - UNKNOWN 2 - CLEAN 3 - MALICIOUS 4 - UNSCANNABLE |
| Updated User Agents list | <p>The list of available user agents available for selection during policy definition has been updated and expanded. This list is presented on the Advanced > Membership by User Agent page, which is accessed from a number of feature pages such as Identification Profiles, Routing Policies, and so on.</p> |

| Feature | Description |
|---------------------------|---|
| Intermediate Certificates | You can now use the CLI command <code>advancedproxyconfig > HTTPS</code> to enable “intermediate certificate discovery,” a process the WSA uses in an attempt to eliminate the need to manually locate and download the intermediate certificate store to prevent intermediate certificate verification failures. See “Web Security Appliance CLI Commands” in the User Guide. |
| Live (third-party) Feeds | You can define custom URL categories based on data feeds from an external server. These live-feed custom URL categories can be used in policy definition. See “Creating and Editing Custom URL Categories” in the User Guide. |

See the appropriate “Fixed Issues” search in [Known and Fixed Issues, page 24](#) for additional information.

Changes in Behavior

- [Changes in Behavior in Cisco AsyncOS 10.1.5 \(MD - Maintenance Deployment\), page 7](#)
- [Changes in Behavior in Cisco AsyncOS 10.1.3 \(MD - Maintenance Deployment\), page 7](#)
- [Changes in Behavior in Previous Releases, page 7](#)

Changes in Behavior in Cisco AsyncOS 10.1.5 (MD - Maintenance Deployment)

| | |
|------------------------|--|
| 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 in Behavior in Cisco AsyncOS 10.1.3 (MD - Maintenance Deployment)

| | |
|---|---|
| AMP compressed files processing | When AMP is enabled, and access policies set to block all HTTP transactions with a malicious verdict from AMP, MIME types are first detected before decompressing files to either block or allow the file to be sent. |
| Changes in configuring and Managing VLANs | You cannot edit VLANs with the <code>etherconfig > VLAN</code> command in the CLI. To edit a VLAN, you need to delete the VLAN and configure it. |
| Default value of the <code>Find web server by:</code> parameter | The default value for the parameter <code>Find web server by:</code> , for the command <code>advancedproxyconfig > DNS</code> in the CLI, is changed to: <code>0= Always use DNS answers in order.</code> |

Changes in Behavior in Previous Releases

This section describes changes in behavior from previous versions of AsyncOS for Web that may affect the appliance configuration after you upgrade to the latest version.

- [Default Cipher Suites for Proxy Services, page 8](#)
- [Special Characters No Longer Allowed in Regular Expressions, page 8](#)
- [Special Characters Allowed in Active Directory User Names, page 8](#)
- [Limit on Number of WCCP Dynamic Service Groups, page 8](#)
- [Limit on Number of Concurrent Sessions, page 8](#)
- [List of Available Upgrades, page 8](#)
- [Support Requests Require CCO ID and Support Contract, page 9](#)
- [New Certificate Management Page, page 9](#)
- [Exporting Web Tracking Data, page 9](#)
- [SNMP Monitoring, page 9](#)
- [X-Authenticated-Groups Header Format, page 9](#)
- [New CLI Option to Modify Web Tracking Query Timeout, page 9](#)

Default Cipher Suites for Proxy Services

From AsyncOS 9.1.1 onwards, the default cipher suites available for Proxy Services are modified to include only secure cipher suites. If you are upgrading to AsyncOS 10.x.x, see [Change the Default Proxy Services Cipher Suites to Cisco Recommended Cipher Suites, page 21](#).

Special Characters No Longer Allowed in Regular Expressions

You can no longer use “.” to begin or end a regular expression. You also cannot use “/” in a regular expression intended to match a URL, nor can you end such an expression with a dot.

Special Characters Allowed in Active Directory User Names

Prior to AsyncOS 9.0, attempts to join an Active Directory domain with a user name that included special characters would produce an error. Now the following special characters can be used in domain user names: ` ~ () { } ! # ^ _ \$ & (however, note that % is not yet supported).

Limit on Number of WCCP Dynamic Service Groups

You can configure no more than 15 WCCP service groups on the Web Security appliance.

Limit on Number of Concurrent Sessions

Beginning in AsyncOS 8.5, individual users are limited to a maximum of 10 concurrent sessions; this total includes both CLI and Web interface sessions.

List of Available Upgrades

Beginning in AsyncOS 8.5, all available releases appear in the list of available upgrades, including releases that would previously have been provisioned only to a limited number of customers as a limited release.

Each release in the list is identified by the release type (ED - Early Deployment, GD - General Deployment, MD - Maintenance 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>.

Support Requests Require CCO ID and Support Contract

Beginning in AsyncOS 8.5, in order to open a support request from the appliance, you must enter a CCO ID and a support contract ID.

New Certificate Management Page

Beginning in AsyncOS 8.5, certificate management functionality has been moved from the Security Services > HTTPS Proxy page to a new, stand-alone page: Network > Certificate Management.

Exporting Web Tracking Data

Previously, when exporting web tracking data as CSV, the data was sorted by timestamps. Beginning in AsyncOS 8.5, this data is not sorted.

SNMP Monitoring

Beginning in AsyncOS 8.5, the following functionality is different from previous implementations:

Message authentication and encryption are mandatory when enabling SNMPv3. Passwords for authentication and encryption should be different. The encryption algorithm can be AES (recommended) or DES. The authentication algorithm can be SHA-1 (recommended) or MD5.

X-Authenticated-Groups Header Format

Beginning in AsyncOS 8.5, if LDAP authentication and External Data Loss Prevention are configured on the appliance, AsyncOS sends the X-Authenticated-Groups header in this format:

`LDAP://(LDAP server name)/(groupname).`

Previously, the format was `LDAP://(groupname)`. This software change may require changes to policies or other automation relying on the X-Authenticated-Groups header. [Defect: CSCum91801]

New CLI Option to Modify Web Tracking Query Timeout

A new CLI option `webtrackingquerytimeout` is introduced under `reportingconfig` command to modify the web tracking query timeout.



Note

The default value for `webtrackingquerytimeout` is 120 seconds and can be modified from 120 seconds and above.

The following is an example to modify the web tracking query timeout to 150 seconds:

```
web.example.com > reportingconfig
```

Choose the operation you want to perform:

- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Web Tracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this appliance.

```
[>webtrackingquerytimeout
```

Timeout value for Web Tracking Queries (in Seconds)

```
[120]> 150
```

Choose the operation you want to perform:

- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Web Tracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.

```
[>
```

```
web.example.com > commit
```

Please enter some comments describing your changes:

```
[>
```

Changes committed: Fri May 05 13:18:18 2017 GMT

```
web.example.com >
```

Release Classification

Each release is identified by the release type (ED - Early Deployment, GD - General Deployment, and so.) 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

- All virtual appliance models.
- The following hardware models:
 - x70 (Cisco Web Security Appliance S170 is not supported for AsyncOS 10.5 and later)
 - x80
 - x90

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

Important! After an upgrade, on S190, S390, and S690 appliances which have read-only root partitions, the output of the ipcheck command may display the usage of the root partition as more than 100%. Please be advised that this normal, and will not have any functional impact.



Note

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

- [Upgrading to AsyncOS 10.1.5-037 \(MD - Maintenance Deployment\), page 11](#)
- [Upgrading to AsyncOS 10.1.5-034 \(MD - Maintenance Deployment\), page 12](#)
- [Upgrading to AsyncOS 10.1.5-004 \(MD - Maintenance Deployment\), page 12](#)
- [Upgrading to AsyncOS 10.1.5-004 \(MD - Maintenance Deployment\), page 12](#)
- [Upgrading to AsyncOS 10.1.4-017 \(MD - Maintenance Deployment\), page 12](#)
- [Upgrading to AsyncOS 10.1.4-007 \(MD - Maintenance Deployment\), page 14](#)
- [Upgrading to AsyncOS 10.1.3-054 \(MD - Maintenance Deployment Refresh\), page 14](#)
- [Upgrading to AsyncOS 10.1.1-235 \(MD - Maintenance Deployment - Refresh\), page 15](#)
- [Upgrading to AsyncOS 10.1.1-234 \(MD - Maintenance Deployment\), page 15](#)
- [Upgrading to AsyncOS 10.1.1-230 \(MD - Maintenance Deployment\), page 16](#)
- [Upgrading to AsyncOS 10.1.0-204 \(GD - General Deployment\), page 16](#)
- [Upgrading to AsyncOS 10.0.0-233 \(LD - Limited Deployment\), page 17](#)

Upgrading to AsyncOS 10.1.5-037 (MD - Maintenance Deployment)



Note

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.5-037 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.1-235 • 10.1.4-007 • 10.1.5-004
- 10.1.1-306 • 10.1.4-009 • 10.1.5-034
- 10.1.2-036 • 10.1.4-017
- 10.1.2-050
- 10.1.3-039
- 10.1.3-054

Upgrading to AsyncOS 10.1.5-034 (MD - Maintenance Deployment)

**Note**

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.5-034 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.1-235
- 10.1.1-306
- 10.1.2-036
- 10.1.2-050
- 10.1.3-039
- 10.1.3-054
- 10.1.4-007
- 10.1.4-009
- 10.1.4-017
- 10.1.5-004

Upgrading to AsyncOS 10.1.5-004 (MD - Maintenance Deployment)

**Note**

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.5-004 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.1-235
- 10.1.1-306
- 10.1.2-036
- 10.1.2-050
- 10.1.3-039
- 10.1.3-054
- 10.1.4-007
- 10.1.4-009
- 10.1.4-017

Upgrading to AsyncOS 10.1.4-017 (MD - Maintenance Deployment)

**Note**

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.4-017 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.1.1-235
- 10.1.1-306
- 10.1.2-036
- 10.1.2-050
- 10.1.3-039
- 10.1.3-054
- 10.1.4-007

Upgrading to AsyncOS 10.1.4-007 (MD - Maintenance Deployment)



Note

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.4-007 of AsyncOS for Cisco Web Security appliances from the following versions:

- 9.1.1-074 • 10.1.1-235
- 9.1.2-022 • 10.1.1-306
- 9.1.2-041 • 10.1.2-036
- 9.1.3-016 • 10.1.2-050
- 9.1.3-024 • 10.1.3-039
- 10.1.3-054

Upgrading to AsyncOS 10.1.3-054 (MD - Maintenance Deployment Refresh)



Note

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.3-054 of AsyncOS for Cisco Web Security appliances from the following versions:

- 9.1.1-074 • 10.1.1-235 • 8.5.3-901
- 9.1.2-022 • 10.1.1-306
- 9.1.2-041 • 10.1.2-036
- 9.1.3-016 • 10.1.2-050
- 9.1.3-024 • 10.1.3-039

Upgrading to AsyncOS 10.1.1-235 (MD - Maintenance Deployment - Refresh)



Note

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.1-235 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8.0.8-113
- 8.0.8-118
- 8.5.3-069
- 8.5.4-038
- 9.0.1-162
- 9.1.0-157
- 9.1.1-074
- 9.1.2-022
- 9.1.2-029
- 9.1.2-034
- 10.1.0-204
- 10.1.1-230
- 10.1.1-234

Upgrading to AsyncOS 10.1.1-234 (MD - Maintenance Deployment)



Note

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.1-234 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8.0.8-113
- 8.0.8-118
- 8.5.3-069
- 8.5.4-038
- 9.0.1-162
- 9.1.0-157
- 9.1.1-074
- 9.1.2-022
- 9.1.2-029
- 10.0.0-233
- 10.1.0-204
- 10.1.1-230

Upgrading to AsyncOS 10.1.1-230 (MD - Maintenance Deployment)



Note

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.1-230 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8.0.8-118 • 9.0.1-162 • 10.0.0-233
- 8.5.3-069 • 9.1.0-157 • 10.1.0-204
- 8.5.4-038 • 9.1.1-074
- 9.1.2-022

Upgrading to AsyncOS 10.1.0-204 (GD - General Deployment)



Note

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.1.0-204 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8.0.6-119 • 8.5.1-104 • 8.8.0-085 • 9.0.1-162 • 10.0.0-233
- 8.0.7-149 • 8.5.2-027 • 9.0.1-204
- 8.0.8-113 • 8.5.3-069 • 9.1.0-070
- 8.0.8-118 • 9.1.0-157
- 9.1.1-074
- 9.1.1-507
- 9.1.1-508
- 9.1.1-510
- 9.1.2-010

Upgrading to AsyncOS 10.0.0-233 (LD - Limited Deployment)



Note

Before you start the upgrade process, see [Pre-upgrade Requirements, page 17](#) and [Installation and Upgrade Notes, page 17](#).

You can upgrade to release 10.0.0-233 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8.0.6-119
- 8.0.7-149
- 8.0.8-118
- 8.5.1-104
- 8.5.2-027
- 8.5.2-103
- 8.5.2-105
- 8.5.3-069
- 8.8.0-085
- 9.0.1-162
- 9.0.1-203
- 9.1.0-157
- 9.1.1-074
- 10.0.0-188

Pre-upgrade Requirements

Update RAID Controller Firmware

Before upgrading the AsyncOS software, update the RAID controller firmware as described in *Cisco Update for RAID Controller Firmware (For S360/S370/S660/S670 only, reboot required) Release Notes*.

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](#)
- [Configuration Files](#)
- [Demo Security Certificate Encryption Strength](#)
- [Post-upgrade Reboot](#)
- [What's New In Cisco AsyncOS 10.0.0 \(Limited Deployment\)](#)

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>.

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 WSA 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 WSA and DLP Server is IPv4 only)
- PAC File Hosting

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+)
- IE (Version 7+) and latest releases of Firefox and Chrome browsers on Windows 7 and XP.

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 19](#).
- 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.

Configuration Files

When you upgrade AsyncOS for Web from the web interface or Command Line Interface (CLI), the configuration is saved to file in the `/configuration/upgrade` directory. You can access the upgrade directory using an FTP client. Each configuration file name is appended with the version number, and passwords in the configuration file are masked so they are not human readable.

Generally, configuration files from earlier AsyncOS releases are incompatible with later AsyncOS releases and vice-versa.

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, 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 AsyncOS for Web.

Upgrading AsyncOS for Web

Before You Begin

- Perform preupgrade requirements, including updating the RAID controller firmware. See [Pre-upgrade Requirements, page 17](#).
- Log in as Administrator.

-
- 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.

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 21](#)
- [Virtual Appliances: Required Changes for SSH Security Vulnerability Fix, page 22](#)
- [File Analysis: Required Changes to View Analysis Result Details in the Cloud, page 22](#)
- [File Analysis: Verify File Types To Be Analyzed, page 22](#)
- [Unescaped Dots in Regular Expressions, page 22](#)


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 to AsyncOS 10.x.x, 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>.

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

The requirement in this section was introduced in AsyncOS 8.8.

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 following information supplements information in the Online Help and/or User Guide for this release.

Sophos No Longer Scans Archive Files

As of AsyncOS 9.0, scanning of archive (.zip) files has been disabled in the Sophos scanner.

Adding JavaScript to End-user Notifications

If you need to add standard JavaScript to end-user notifications of any type, follow instructions in the user guide or online help for editing notification page HTML files. (JavaScript entered into the Custom Message box for notifications in the web user interface will be stripped out.) Be sure to test your script first in supported client browsers to ensure that it works as expected.

Which Files Can Have their Reputation Evaluated and Be Sent for Analysis?

The criteria for evaluating a file's reputation and for sending files for analysis may change at any time. Criteria are available only to registered Cisco customers. See *File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*, available from <http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html>.

In order to access this document, you must have a Cisco customer account with a support contract. To register, visit <https://tools.cisco.com/RPF/register/register.do>.

Viewing File Analysis Details in the Cloud

The most current instructions for configuring this functionality are in the user guide PDF, available from <http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html>.

Different Client "Hello" Behavior for Custom and Default Categories

When scanning packet captures, you may notice that the "Client Hello" handshake is sent at different times for custom category and default (Web) category HTTPS Decryption pass-through policies.

For an HTTPS page passed through via the default category, the Client Hello is sent before receipt of a Client Hello from the requestor, and the connection fails. For an HTTPS page passed through via a custom URL category, the Client Hello is sent after the Client Hello is received from the requestor, and the connection is successful.

As a remedy, you can create a custom URL category with a pass-through action for SSL 3.0-only-compatible Web pages.

Additional Information

The User Guide PDF may be more current than the online help. To obtain the User Guide PDF 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 24
- [Lists of Known and Fixed Issues](#), page 24
- [Finding Information about Known and Resolved Issues](#), page 26

Bug Search Tool Requirements

Register for a Cisco account if you do not have one. Go to <https://tools.cisco.com/RPF/register/register.do>.

Lists of Known and Fixed Issues

- [Known and Fixed Issues in Release 10.1.5-037](#), page 24
- [Known and Fixed Issues in Release 10.1.5-034](#), page 24
- [Known and Fixed Issues in Release 10.1.5-004](#), page 25
- [Known and Fixed Issues in Release 10.1.4-017](#), page 25
- [Known and Fixed Issues in Release 10.1.4-007](#), page 25
- [Known and Fixed Issues in Release 10.1.3-054](#), page 25
- [Known and Fixed Issues in Release 10.1.1-235](#), page 25
- [Known and Fixed Issues in Release 10.1.1-234](#), page 26
- [Known and Fixed Issues in Release 10.1.1-230](#), page 26
- [Known and Fixed Issues in Release 10.1.0-204](#), page 26
- [Known and Fixed Issues in Release 10.0.0-233](#), page 26

Known and Fixed Issues in Release 10.1.5-037

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=10.1.5-037&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=10.1&sb=afr&sts=open&svr=3nH&bt=custV |

Known and Fixed Issues in Release 10.1.5-034

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=10.1.5-037&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=10.1&sb=afr&sts=open&svr=3nH&bt=custV |

Known and Fixed Issues in Release 10.1.5-004

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.5-004&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.5&sb=af&sts=open&svr=3nH&bt=custV |

Known and Fixed Issues in Release 10.1.4-017

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.4-017&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.4&sb=af&sts=open&svr=3nH&bt=custV |

Known and Fixed Issues in Release 10.1.4-007

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.4-007&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.4&sb=af&sts=open&svr=3nH&bt=custV |

Known and Fixed Issues in Release 10.1.3-054

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.3-054&sb=fr&svr=2nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.3&sb=af&sts=open&svr=2nH&bt=custV This URL displays the list of all known issues with the status Open . In the Filter, change the Status to Other , to see issues not visible with the open status. |

Known and Fixed Issues in Release 10.1.1-235

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.1-235&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.1&sb=af&sts=open&svr=3nH&bt=custV |

Known and Fixed Issues in Release 10.1.1-234

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.1-234&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.1&sb=afr&sts=open&svr=3nH&bt=custV |

Known and Fixed Issues in Release 10.1.1-230

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.1-230&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.1&sb=afr&sts=open&svr=3nH&bt=custV |

Known and Fixed Issues in Release 10.1.0-204

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.0-204&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.0&sb=afr&sts=open&svr=3nH&bt=custV |

Known and Fixed Issues in Release 10.0.0-233

| | |
|---------------------|---|
| Fixed Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.0.0-233&sb=fr&svr=3nH&bt=custV |
| Known Issues | https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.0.0&sb=afr&sts=open&svr=3nH&bt=custV |

Finding Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find the most current information about known and resolved defects in shipping releases.

Before You Begin

Register for a Cisco account if you do not have one. Go to <https://tools.cisco.com/RPF/register/register.do>.

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, 10.1.

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 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>.

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.

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. 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.

© 2017-2019 Cisco Systems, Inc. All rights reserved.