Release Notes for AsyncOS 10.x for Cisco Content Security Management

Published: June 20, 2016
Revised: January 15, 2018

Contents

- New Features, page 1
- Upgrade Paths, page 7
- Content Security Release Terminology, page 8
- Compatibility with Email and Web Security Releases, page 8
- Changed Information, page 8
- Installation and Upgrade Notes, page 9
- Documentation Updates, page 11
- Known and Fixed Issues, page 11
- Related Documentation, page 12
- Service and Support, page 13

New Features

- New in Cisco AsyncOS 10.1.0-052 (MD - Maintenance Deployment), page 2
- New in Cisco AsyncOS 10.1.0-037 (GD - General Deployment), page 3
- New in Cisco AsyncOS 10.0.0-096 (MD - Maintenance Deployment), page 3
- New in Cisco AsyncOS 10.0.0-088 (MD - Maintenance Deployment), page 4
- New in Cisco AsyncOS 10.0.0-055, page 4
New in Cisco AsyncOS 10.1.0-052 (MD - Maintenance Deployment)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Support for new features in AsyncOS 10.5 for Cisco Web Security Appliances | • **WCCP weighted load balancing** – This release provides a weighting assignment parameter that lets you configure differential WCCP load balancing for each WSA based on its performance capability.  
• **FIPS mode updates** – You can enable FIPS mode and encryption of Critical Sensitive Parameters (CSP) such as shared secret keys, SNMP passwords, Active Directory credentials, and so on.  
In addition, certificates are validated strictly to comply with CC standards before uploading, and OCSP validation is available to validate certificates against a revocation list.  
Further, per CC requirements, all auditable events are now logged in the audit logs.  
• **Common Criteria certification** – This release is a candidate for CC certification.  
• **TLS versions** – Transport Layer Security v1.1 and v1.2 are now available for selection with management, updater, LDAPS, and other services. In FIPS mode, the services are auto-configured to use these protocols.  
• **Platform Upgrades** – AsyncOS has been upgraded to FreeBSD 10.1.  
Cisco SSL has been upgraded to ciscoss1-1.0.2f.6.0.3, with FIPS Object Module (FOM) 6.0 which is more secure and already FIPS compliant.  
Refer to the Release Notes for AsyncOS 10.x for Cisco Web Security Appliances for additional information about these new features. |
New in Cisco AsyncOS 10.1.0-037 (GD - General Deployment)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Support for new features in AsyncOS 10.0.1 for Cisco Email Security Appliances | Reporting support for the following new feature in AsyncOS 10.0.1 for Cisco Email Security Appliances:  
  - Macro Detection. Use this report page to view details such as:  
    - Top Incoming Macro-Enabled Attachments by File Type in graphical and tabular format.  
    - Top Outgoing Macro-Enabled Attachments by File Type in graphical and tabular format.  
  For details, search for the relevant terms in the email reporting chapter of the online help or user guide. |
| Support for new features in AsyncOS 10.1 for Cisco Web Security Appliances |  
  - **Archive Inspection** – 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.  
  - **Centralized Upgrade Management** – Simultaneously upgrade multiple WSAs using a single Security Management Appliance. You also can apply a different software upgrade for each WSA.  
  - **Dynamic TCP window sizing** – The CLI command `networktuning` 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 `advancedproxyconfig > MISCELLANEOUS`, to enable and disable TCP RST (reset) forwarding.  
  - **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.  
  Refer to the [Release Notes for AsyncOS 10.x for Cisco Web Security Appliances](#) for additional information about these new features. |

New in Cisco AsyncOS 10.0.0-096 (MD - Maintenance Deployment)

This is a maintenance release; no new features were added.
New in Cisco AsyncOS 10.0.0-088 (MD - Maintenance Deployment)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Support for new features in AsyncOS 10.0 for Cisco Web Security Appliances | - **Referrer Exceptions** – 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. You can now define exceptions to the default actions configured for embedded/referred content.  
  - **AMP Private Cloud** – 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.  
  - **AMP Reporting enhancements** – 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.  
  - **Updated User Agents list** – The list of available user agents available for selection during policy definition has been updated and expanded.  
  - **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. Refer to the Release Notes for AsyncOS 10.0.x for Cisco Web Security Appliances for additional information about these new features.                                                                                                                                                                                                                                                                 |

New in Cisco AsyncOS 10.0.0-055

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO Using SAML 2.0</td>
<td>Cisco Content Security Management appliance now supports SAML 2.0 SSO so that the end users can access the Spam Quarantine using the same credentials that are used to access other SAML 2.0 SSO enabled services within their organization. See the “Common Administrative Tasks” chapter in the user guide or online help.</td>
</tr>
<tr>
<td>Support for new hardware</td>
<td>This AsyncOS release supports the new M190, M390, and M690 hardware appliance models. Quick start and hardware installation guides with information for setting up your hardware are available from <a href="http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html">http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html</a>.</td>
</tr>
<tr>
<td>New Features</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Spam Quarantine Enhancement</strong></td>
<td>You can now send notifications to end users that list new quarantined messages without displaying the message subject. To view the message subject, end users must click the link and view the message in the spam quarantine. You can achieve this using the new notification variable <code>New Message Table without Subject</code>. See the “Spam Quarantine” chapter in the user guide or online help.</td>
</tr>
<tr>
<td><strong>Message Tracking Details for URLs in Messages</strong></td>
<td>Users can now view finer details about URLs caught by content and outbreak filters. Administrators can configure which users can see this information. See the “Tracking Email Messages” chapter in the user guide or online help.</td>
</tr>
</tbody>
</table>
| **Support for new features in AsyncOS 10.0 for Cisco Email Security Appliances** | Reporting and tracking support for the following features that are new in AsyncOS 10.0 for Cisco Email Security Appliances:  
  - **Forged Email Detection.** Use this report page to view details such as:  
    - The top ten users in the content dictionary that matched the forged From: header in the incoming messages.  
    - A list of all the users in the content dictionary that matched the forged From: header in the incoming messages and for a given user, the number of messages matched.  
  - **Mailbox Auto Remediation.** Use this report page to view details such as:  
    - A list of recipients for whom the mailbox remediation was successful or unsuccessful  
    - Remedial actions taken on messages  
    - The filenames associated with a SHA-256 hash For details, search for the relevant terms in the email reporting chapter of the online help or user guide. |
### Enhanced AMP Reports

**Advanced Malware Protection** page includes the following enhancements:

- A new graph that shows the incoming files handled by AMP in percentage based on the verdicts (Clean, Malicious, Unknown, Unscannable).
- A new table that shows the number of incoming files handled by AMP based on the verdicts (Clean, Malicious, Unknown, Unscannable). Click on the file count to view the related messages in Message Tracking.

**Incoming Malware Threat Files Report**

- Incoming Malware Threat Files report now shows the name of the file(s) associated with a SHA-256 hash.
- If you click on a SHA-256 hash, a new page that shows file reputation and analysis summary for the specified SHA-256 hash is displayed.
- Click on the number of infected messages to view the related messages in Message Tracking.

### File Analysis

**File Analysis** page includes the following enhancements:

- Completed Analysis Requests from This Appliance and Pending Analysis Requests from This Appliance reports include the following enhancements:
  - Reports now show the name of the file(s) associated with a SHA-256 hash.
  - Click on **Details** to view the related messages in Message Tracking.
Upgrade Paths

- Upgrading to Cisco AsyncOS 10.1.0-052 (MD - Maintenance Deployment), page 7
- Upgrading to Cisco AsyncOS 10.1.0-037 (GD - General Deployment), page 7
- Upgrading to Cisco AsyncOS 10.0.0-096 (MD - Maintenance Deployment), page 7
- Upgrading to Cisco AsyncOS 10.0.0-088 (MD - Maintenance Deployment), page 8
- Upgrading to Cisco AsyncOS 10.0.0-055, page 8

Upgrading to Cisco AsyncOS 10.1.0-052 (MD - Maintenance Deployment)

You can upgrade to release 10.1.0-052 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.6-039
- 9.1.1-005
- 9.1.1-702
- 9.5.2-023
- 9.5.2-033
- 9.6.0-051
- 9.6.0-066
- 9.6.1-019
- 9.6.1-027
- 10.0.0-013
- 10.0.0-055
- 10.0.0-088
- 10.0.0-096
- 10.1.0-037

Upgrading to Cisco AsyncOS 10.1.0-037 (GD - General Deployment)

You can upgrade to release 10.1.0-037 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.6-039
- 9.1.1-005
- 9.1.1-702
- 9.5.2-023
- 9.5.2-033
- 9.6.0-051
- 9.6.0-066
- 9.6.1-019
- 9.6.1-027
- 10.0.0-013
- 10.0.0-055
- 10.0.0-088
- 10.0.0-096

Upgrading to Cisco AsyncOS 10.0.0-096 (MD - Maintenance Deployment)

You can upgrade to release 10.0.0-096 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.6-039
- 9.1.1-005
- 9.1.1-702
- 9.5.2-023
- 9.5.2-033
- 9.6.0-051
- 9.6.0-066
- 9.6.1-019
- 10.0.0-013
- 10.0.0-055
- 10.0.0-088
Upgrading to Cisco AsyncOS 10.0.0-088 (MD - Maintenance Deployment)

You can upgrade to release 10.0.0-088 of AsyncOS for Cisco Content Security Management from the following versions:

- 9.1.2-013
- 9.5.2-023
- 9.5.2-033
- 9.6.1-019
- 10.0.0-055

Upgrading to Cisco AsyncOS 10.0.0-055

You can upgrade to release 10.0.0-055 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.6-039
- 9.1.1-005
- 9.1.1-702
- 9.5.2-023
- 9.5.2-033
- 9.6.0-051
- 9.6.1-019
- 10.0.0-013

Content Security Release Terminology

For an explanation of terms like LD, ED, GD, and MD that are used in labeling content security product releases, see https://supportforums.cisco.com/blog/12309231/content-security-release-terminology.

Compatibility with Email and Web Security Releases


Changed Information

In addition to the changes described in the New Features table above, the following functionality on your appliance has changed from previous releases and may require your attention.

| Advanced Malware Protection and File Analysis Reports Prior to the Upgrade | From AsyncOS 10.0 onwards, Advanced Malware Protection, File Analysis, and Verdict Updates reports are enhanced to display additional fields, graphs, and so on. The reports displayed after the upgrade do not include the reporting data prior to the upgrade. To view the reports prior to the upgrade, click on the hyperlink (click here to view reports prior to AsyncOS 10.0) at the top of the report page. |
Important Additional Reading

You should also review the release notes for your associated Email and Web security releases. For links to this information, see Related Documentation, page 12.

Virtual Appliance


Upgrading a Virtual Appliance

If your current Virtual Appliance release does not support more than 2TB of disk space, and you want to use more than 2 TB of disk space with this release, you cannot simply upgrade your virtual appliance. Instead, you must deploy a new virtual machine instance for this release.

When you upgrade a virtual appliance, the existing licenses remain unchanged.

Migrating From a Hardware Appliance to a Virtual Appliance

Step 1 Set up your virtual appliance using the documentation described in Virtual Appliance, page 9.

Step 2 Upgrade your physical appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded physical appliance.

<table>
<thead>
<tr>
<th>Change in Report Page Name</th>
<th>File Analysis report page is renamed to Advanced Malware Protection File Analysis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Quarantine Access for Administrator</td>
<td>After enabling SSO for Spam Quarantine, administrators will no longer be able to access the Spam Quarantine using the Spam Quarantine URL (http://&lt;appliance_hostname&gt;:&lt;port&gt;). Administrators can access the Spam Quarantine using the web interface (Email &gt; Message Quarantine &gt; Spam Quarantine).</td>
</tr>
</tbody>
</table>
Installation and Upgrade Notes

Step 4
Load the configuration file from the hardware appliance onto the virtual appliance. Be sure to select appropriate options related to disk space and network settings.

What To Do Next
If you will use your hardware appliance as a backup appliance, see information about backups in the user guide or online help. For example, you should ensure that the backup appliance does not pull data directly from managed email and web security appliances, or publish configurations to web security appliances.

Preupgrade Requirements

Perform the following important preupgrade tasks:

- Verify Associated Email and Web Security Appliance Versions, page 10
- Back Up Your Existing Configuration, page 10

Verify Associated Email and Web Security Appliance Versions

Before upgrading, verify that the Email Security appliances and Web Security appliances that you want to manage will run releases that are compatible. See the Compatibility with Email and Web Security Releases, page 8.

Back Up Your Existing Configuration

Before upgrading your Cisco Content Security Management appliance, save the XML configuration file from your existing Security Management appliance. Save this file to a location off the appliance. For important caveats and instructions, see the “Saving and Exporting the Current Configuration File” section in the user guide or online help.

IPMI Messages During Upgrade

If you are upgrading your appliance using the CLI, you may observe messages related to IPMI. You can ignore these messages. This is a known issue.

Defect ID: CSCuz33125

Upgrading to This Release

Step 1
Address all topics described in Preupgrade Requirements, page 10.

Step 2
Follow all instructions in the “Before You Upgrade: Important Steps” section in the user guide PDF for THIS release.

Step 3
Perform the upgrade:

Follow instructions in the “Upgrading AsyncOS” section of the “Common Administrative Tasks” chapter of the user guide PDF for your EXISTING release.
Step 4 After about 10 minutes, access the appliance again and log in.
Step 5 Follow instructions in the “After Upgrading” section of the user guide PDF for THIS release.
Step 6 If applicable, see Migrating From a Hardware Appliance to a Virtual Appliance, page 9.

Documentation Updates

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 12.

Information about other resources, including Tech Notes and the Cisco support community, is in the Additional Resources chapter in the online help and User Guide PDF.

Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware

Problem You receive an alert with subject “Battery Relearn Timed Out” for 380 or 680 hardware.
Solution This alert may or may not indicate a problem. The battery relearn timeout, in itself, does not mean there is any problem with the RAID controller. The controller can recover in the subsequent relearn. Please monitor your email for any other RAID alerts for the next 48 hours, to ensure that this is not the side-effect of any other problem. If you do not see any other RAID-related alerts from the system, then you can safely ignore this alert.

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 12]
- [Lists of Known and Fixed Issues, page 12]
- [Finding Information about Known and Resolved Issues, page 12]

Note Known issues on Cisco Email Security Appliances and Cisco Web Security Appliances may appear in or impact functionality of Cisco Content Security Management Appliances.

Known issues in previous content security management releases may also affect this release.
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

|--------------------|-------------------------------------------------------------------------------------------------|

Finding Information about Known and Resolved Issues

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Go to <a href="https://tools.cisco.com/bugsearch/">https://tools.cisco.com/bugsearch/</a>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log in with your Cisco account credentials.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Select from list &gt; Security &gt; Security Management &gt; Cisco Content Security Management Appliance, and click OK.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In Releases field, enter the version of the release, for example, 10.0.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Depending on your requirements, do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• To view the list of resolved issues, select Fixed in these Releases from the Show Bugs drop down.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

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

In addition to the main documentation in the following table, information about other resources, including the knowledge base and Cisco support community, is in the More Information chapter in the online help and User Guide PDF.
## Service and Support

**Note**

To get support for virtual appliances, call Cisco TAC and have your Virtual License Number (VLN) number ready.


For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

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.

© 2018 Cisco Systems, Inc. All rights reserved.