Release Notes for AsyncOS 9.6.x for Cisco Content Security Management

First Published: October 26, 2015
Last Updated: August 2, 2017

Contents

New Features

- New in Release 9.6.1, page 2
- New in Release 9.6.0, page 2

Cisco Systems, Inc.
www.cisco.com

New in Release 9.6.1

- New in Release 9.6.1-027, page 2

New in Release 9.6.1-027

Feature	Description
Web Security	
Support for new WSA release	Support for AsyncOS 9.1.2 for Cisco Web Security Appliances.

New in Release 9.6.0

Feature	Description
Ability to disable insecure SSLv3 protocol	The SSL v3 protocol is not secure and you should not use it. A new command, `sslconfig,` allows you to select which protocol to use for communicating with LDAPS and updater servers and for the web interface of the security management appliance. For details, see Communication Protocol, page 4.

Feature	Description
Web Security	
Support for new WSA release	Support for AsyncOS 8.5.3 for Cisco Web Security Appliances, for Cisco Content Security Management Appliances running on x70 or later hardware.
Email Security	
Reporting and tracking	This release reflects reporting and tracking changes in AsyncOS 9.7 for Cisco Email Security appliances.
LDAP	LDAP queries that return certain error codes such as Unavailable, Busy, or Operations Error, now fall back to a subsequent LDAP server listed for failover. Previously, failover occurred only if the connection to the LDAP server failed.
Non-spam Quarantines	You can now specify a retention time in minutes for all policy, virus, and outbreak quarantines including the File Analysis quarantine.

Supported Hardware

The following hardware is supported for this release:

- All virtual appliance models.
- The following hardware models:
  - M380 or M680
  - M170, M670 or M1070

Upgrade Paths

- Upgrading to Release 9.6.1-027 (GD - General Deployment), page 3
- Upgrading to Release 9.6.0-051 (GD - General Deployment), page 3

Upgrading to Release 9.6.1-027 (GD - General Deployment)

Note Before upgrading, see Supported Hardware, page 3 and Pre-upgrade Requirements, page 7.

You can upgrade to release 9.6.1-027 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.1.1-022
- 8.3.6-039
- 8.3.6-042
- 8.3.7-008
- 9.1.0-031
- 9.1.1-005
- 9.1.1-702
- 9.5.0-125
- 9.6.0-051

Upgrading to Release 9.6.0-051 (GD - General Deployment)

Note Before upgrading, see Supported Hardware, page 3 and Pre-upgrade Requirements, page 7.

You can upgrade to release 9.6.0-051 of AsyncOS for Cisco Content Security Management from the following versions:

- 9.5.1-009
- 9.5.0-125
- 9.5.0-034
- 9.1.1-005

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

Compatibility with AsyncOS for Email Security and AsyncOS for Web Security releases is detailed in the Compatibility Matrix available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

New and 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.

Communication Protocol

The following changes were introduced in Release 9.6.1:

- SSL v3 is not secure and you should not use it.
- You can choose the communication protocol to be used for each of the following:
  - Updater server
  - End-user access to the spam quarantine
  - Web-based administrative interface to the appliance
  - LDAPS
- If you are upgrading, protocol changes are *not* made automatically.
- To view the currently selected protocols and available options, or to change protocols, use the `sslconfig` command in the command-line interface.
- Cisco update servers do not support SSL v3.
- If you are using a local (remote) update server, and for all other services and web browsers, the protocol you choose must be supported by and enabled on the server and tools you are using.
- One of the available options must be enabled for each service you use.
- Changes made using the `sslconfig` command require a Commit.
- Affected services will be briefly interrupted after you commit changes made using the `sslconfig` command.

(Email Security) URL Filtering Report Change

This change was introduced in Release 9.6:

URLs that were formerly labeled “Suspicious” are now labeled “Neutral.” Only the labeling has changed; the underlying logic and processing have not changed.

(Email Security) Changes in Reporting of Marketing Messages

This change was introduced in Release 9.5.0.

With the introduction of graymail management in AsyncOS 9.5 for Cisco Email Security Appliances, reporting of marketing messages in the Overview report for email has changed.

Specifically, if Marketing Email Scanning under anti-spam settings was enabled on your Email Security appliances before upgrade, or is enabled on some Email Security appliances instead of the graymail feature:

- The number of marketing messages is the sum of marketing messages detected before and after upgrade, and those detected by both features.
- The total number of graymail messages does not include marketing messages detected before the upgrade or those detected on appliances that do not have the graymail feature enabled.
- The total number of attempted messages includes marketing messages detected before the upgrade and marketing messages detected by appliances running either feature.
- Marketing messages processed on appliances on which the graymail feature is not enabled are counted as clean messages.

Change When Saving a Configuration File During Upgrade (CLI)

This change was introduced in Release 9.5.0.

The presentation of the options for passwords when saving a configuration file during upgrades has changed slightly from previous releases. Please read the prompt carefully before making your selection.

(Web Security) Changes to Malware Categories and Malware Threats

Beginning in AsyncOS 9.6.1-019 for Cisco Content Security Management Appliances, the “Unknown” malware category and the “Unnamed” malware threat are no longer used. Thus, you can no longer filter web tracking results by “Unknown’ malware category or “Unnamed” malware threat.

However, some older malware data may still appear in reports as “Unnamed Malware Threat” and ‘Unknown Malware Category;” links to details in Web Tracking, and filtering within Web Tracking, are not available for these results.

(Web Security) Configuration Master Changes

- Appliances that were assigned to Configuration Master 8.5 or later (depending on the AsyncOS release that you are upgrading from) are assigned after upgrade to the Configuration Master associated with this release. Existing settings in the previous Configuration Master will be rolled automatically and seamlessly to the new configuration master.
- Beginning in Release 9.5.1, Configuration Masters 9.0 and 8.1 support the ability to configure access policies to control how range requests are applied.

(Web Security) Changes to the Web Reputation Filtering Report

These changes were introduced in Release 9.5.1.

- The “Web Reputation Threat Types by Blocked Transactions” chart is now called “Web Reputation Threat Types Blocked by WBRS.”

- The “Web Reputation Threat Types by Scanned Further Transactions" chart is now called “Threat Types Detected in Other Transactions.”

  Threats shown in this chart are color-coded to indicate the reason they were not blocked.

The new labels better describe the data shown in the charts. The documentation has also been updated to more accurately describe this data.

Installation and Upgrade Notes

- Important Additional Reading, page 6
- Virtual Appliance, page 6
- Pre-upgrade Requirements, page 7
- Upgrading to This Release, page 8
- Important! Requirements After Upgrade, page 8

Important Additional Reading

You should also review the release notes for:

- Your associated Email and Web security releases.
- Earlier releases of AsyncOS for Security Management, if you are upgrading from a release earlier than the immediate previous release. Information about upgrades to releases between your current release and this release may not be included in these release notes.

For links to this information, see Related Documentation, page 11.

Virtual Appliance

To set up a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html.

Upgrading a Virtual Appliance

If your current Virtual Appliance release does not support more than 2 TB 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 6.

Step 2 Upgrade your physical appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded physical appliance

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.

Pre-upgrade Requirements

Perform the following important pre-upgrade tasks:

- Prepare for the SSH Vulnerability Fix, page 7
- Verify Associated Email and Web Security Appliance Versions, page 7
- Back Up Your Existing Configuration, page 7

Prepare for the SSH Vulnerability Fix

Requirements when upgrading from a release earlier than AsyncOS 9.5.0-125.

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, you must perform certain actions after upgrade in order to return your appliance to full working order after upgrade. To simplify those tasks, note the following BEFORE upgrading:

- You will need appropriate credentials for managed appliances in order to re-establish connection to those appliances after installation.
- If you use centralized configuration management for Web Security appliances, you will need to reassign the configuration master to each appliance after installing the patch. Suggestion: Before you install the patch, take a screen shot of the list on the Web > Utilities > Configuration Masters > Edit Appliance Assignment List page.

For more information about the post-upgrade requirements for this issue, see Virtual Appliances: Required Changes for SSH Security Vulnerability Fix, page 8.

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 4.

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.

Upgrading to This Release

Step 1 Address all topics described in Pre-upgrade Requirements, page 7.

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.

Note Do not interrupt power to the appliance for any reason (even to troubleshoot an upgrade issue) until at least 20 minutes have passed since you rebooted. If you have a virtual appliance, do not use the hypervisor or host OS tools to reset, cycle, or power off the virtual machine.

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 Perform all tasks in Important! Requirements After Upgrade, page 8.

Step 7 If applicable, see Migrating From a Hardware Appliance to a Virtual Appliance, page 6.

Important! Requirements After Upgrade

Virtual Appliances: Required Changes for SSH Security Vulnerability Fix

These requirements apply when upgrading from a release earlier than AsyncOS 9.5.0-125.

As noted in Prepare for the SSH Vulnerability Fix, page 7, 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:

- If you are upgrading from AsyncOS 8.4.0-150:

  You will see an “Upgrade failure” message after running the upgrade, but the patch has installed correctly. However, you must reboot the appliance manually to complete the installation process:

  After you see “Upgrade failure,” the `upgrade` command options will reappear. Press <Enter> to exit the `upgrade` command, then enter the `reboot` command.

  You should also receive an alert about an application fault; ignore this.

- Retrieve the information you noted in Prepare for the SSH Vulnerability Fix, page 7.
- 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.
- Use the `logconfig > hostkeyconfig > delete` CLI command as many times as needed to clear the old key associated with each managed ESA and WSA virtual appliance.

- Re-establish the connection to each managed appliance and (if applicable) reassign each managed appliance to the appropriate configuration master:

  1. Go to Management Appliance > Centralized Services > Security Appliances and click the link for an appliance in the list.
  2. Click Establish Connection.
  3. (Managed WSAs only) If your appliance is configured for centralized configuration management, re-assign the Configuration Master to each managed WSA.
  4. Submit and commit your changes if applicable.
  5. Repeat for each managed appliance.

File Analysis: Required Changes to View Analysis Result Details in the Cloud

The requirement in this section applies to upgrades from releases earlier than AsyncOS 9.5.0-125.

In order to view detailed file analysis results in the cloud for all files uploaded from all email and web security appliances in your organization, you must configure an appliance group on each appliance after upgrading. To configure appliance groups on your content security management appliance, see the email or web reporting chapter in the user guide PDF for this release.

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 11.

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.

SNMP

AsyncOS supports system status monitoring via Simple Network Management Protocol (SNMP) versions v1, v2, and v3.

MIBs are available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html.

When setting up SNMP to monitor connectivity:

When entering the url-attribute while configuring a connectivityFailure SNMP trap, determine whether the URL is pointing at a directory or a file.

- If it is a directory, add a trailing slash (/)
- If it is a file, do not add a trailing slash

The following information applies beginning in AsyncOS 8.4:

The use of SNMPv3 with password authentication and DES Encryption is mandatory to enable this service. (For more information on SNMPv3, see RFCs 2571-2575.) You are required to set a SNMPv3 passphrase of at least 8 characters to enable SNMP system status monitoring. The first time you enter a SNMPv3 passphrase, you must re-enter it to confirm. The snmpconfig command "remembers" this phrase the next time you run the command.

Known and Fixed Issues

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

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, page 10
- Lists of Known and Fixed Issues, page 10
- Other Bug Searches, page 11

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

Note Issues that were open in previous releases may also be open in this release.

Known and Fixed Issues in Release 9.6.1

Known issues in this release	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=9.6.1&sb=anfr&sts=open&bt=empCustV
Fixed issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=9.6.1&sb=anfr&sts=fd&bt=custV

Known and Fixed Issues in Release 9.6.0

Known issues in this release	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=9.6.0&sb=anfr&sts=open&srtBy=byRel&bt=CustV
Fixed issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=9.6.0&sb=anfr&sts=fd&srtBy=byRel&bt=custV

Other Bug Searches

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 Log in with your Cisco account credentials.

Step 3 Enter search criteria.

For example, enter a bug number, or

a. Click **Select from list**, then navigate to and select your product:

`Cisco Email Security Appliance`

`Cisco Web Security Appliance`

`Cisco Content Security Management Appliance`

b. For **Releases**, enter the AsyncOS release number, such as `8.1.1`.

Step 4 If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool.

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.

Documentation For Cisco Content Security Products:	Is Located At:
Cisco Content Security Management appliances	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web Security appliances	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Email Security appliances	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html

Documentation For Cisco Content Security Products:	Is Located At:
Command Line Reference guide for content security products	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco Email Encryption	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

Service and Support

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

Cisco TAC: 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.

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

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.