Release Notes for AsyncOS 8.3.5 for Cisco Content Security Management

First Published: March 21, 2014

Contents

Cisco Systems, Inc.
www.cisco.com

What's New in This Release

What's New in Release 8.3.5

Feature	Description
Reporting and tracking support for Advanced Malware Protection features	This release supports centralized reporting and tracking for file reputation and filtering features on managed Email and Web Security appliances. In order to view File Analysis report details, your appliance must be able to communicate with the File Analysis server. See essential configuration instructions in File Analysis Reporting, page 8 and in the Advanced Malware Protection reporting sections in the online help or user guide.
Configuration Master support on Web Security appliances	This release includes configuration master changes to support file reputation and file analysis features.

What's New in Release 8.3.0

Feature	Description
New Features:	
Upgrade notification	A notification now appears at the top of the web interface when a new AsyncOS upgrade is available. See Upgrade Notifications, page 26.
Spam quarantine improvements	• You can now choose whether to require end users to log in when they access the end user quarantine via a link in a notification. For more information, see Notifying End Users About Quarantined Messages, page 23. • You have more flexibility in scheduling the frequency and timing of notifications sent to end users about possible spam they receive. For example, you can now send notifications any day or days of the week and any hour or hours of the day. • Administrators can now view, search, add, edit, and delete safelist and blocklist entries. For more information, see Adding Senders and Domains to Safelists and Blocklists (Administrators), page 13.
Enhancements:	
Reporting and Tracking enhancement	Click links in reports to view the Message Tracking data for messages that are included in the report. This enhancement will simplify identification of problems, investigation of patterns, and testing of system and configurations.

Feature	Description
Password security enhancements	You can set the following options for administrative user passwords: • Show a password strength indicator to a user entering a new password. (Password strength is enforced by the other password requirements that you specify.) • Disallow certain words in passwords. (You upload a list of forbidden words to the appliance.)
Support for new email security features	Reporting and tracking support is available for new features on the Email Security appliance, such as High Volume Mail, DMARC verification, and URL Filtering. You can also search for message events processed by a particular message filter.
Enhancements for cloud/hosted appliances	Administrators of cloud/hosted Security Management appliances can now: • Configure LDAP groups for external authentication. This allows distribution of administrative tasks to cloud administrators and external authentication of end users accessing the spam quarantine. • Access and configure scheduled reports • Access centralized email reporting and message tracking.

Upgrade Paths

You can upgrade to release 8.3.5-067 of AsyncOS for Cisco Content Security Management from the following versions:

- 8.3.0-356
- 8.2.0-238
- 8.1.1-013
- 8.0.0-710
- 8.0.0-404
- 7.9.1-102
- 7.9.0-107

Security Management Compatibility Matrix

Compatibility with AsyncOS for Email Security and AsyncOS for Web Security releases is detailed in the Compatibility Matrix available from http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html.

Important Notes

Sign Up to Receive Important Notifications

Sign up to receive notifications such as Security Advisories, Field Notices, End of Sale and End of Support announcements, and information about software updates and known issues.

You can specify options such as notification frequency and types of information to receive. You should sign up separately for notifications for each product that you use.

To sign up, visit the Cisco Notification Service page at http://www.cisco.com/cisco/support/notifications.html

A Cisco.com account is required. If you do not have one, visit https://tools.cisco.com/RPF/register/register.do.

Note This service replaces any previous email announcement service. You must sign up with the Cisco Notification Service to receive future announcements.

SNMP

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

New and Changed Information

The following functionality on your appliance has changed from previous releases.

Accessing the Sender Group Report

Beginning in AsyncOS 8.3.0, you can access the Sender Group report directly from the Email > Reporting menu; the link has been removed from the bottom of the Incoming Mail report page.

Installation and Upgrade Notes

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.

For links to this information, see Related Documentation, page 9.

Supported Browsers

Supported browsers are listed in the "Browser Requirements" section in the "Setup, Installation, and Basic Configuration" chapter of the user guide for your release.

Preupgrade Requirements

Perform the following important preupgrade tasks:

- Change the Protocol for Users and Log Subscriptions Configured to Use SSH 1, page 5
- Preserve Configuration Master 7.1 Settings, page 5
- Preserve Pre-Upgrade Data from the System Capacity Report, page 6
- Verify Associated Email and Web Security Appliance Versions, page 6
- Disk Space Reductions, page 6
- Back Up Your Existing Configuration, page 6

Change the Protocol for Users and Log Subscriptions Configured to Use SSH 1

This section applies if you are upgrading from a release earlier than AsyncOS 8.0 for Content Security Management:

Support for SSH 1 has been removed starting in AsyncOS release 8.0. Therefore, before upgrade, you should do the following:

- Any remote host keys which use SSH 1 should be changed to SSH 2. Use the `logconfig > hostkeyconfig` command in the CLI to make this change.
- For any log subscriptions that are configured to use SSH 1 as the protocol for SCP log push, choose SSH 2 instead.
- Change the access protocol or add a new SSH 2 key for any users configured to use only SSH 1. Use the `sshconfig` command in the CLI to make this change.
- Disable SSH 1 using the `sshconfig > setup` command in the CLI.

Preserve Configuration Master 7.1 Settings

Configuration Master 7.1 is not supported in this release and will be removed during upgrade. If you wish to preserve the settings in Configuration Master 7.1: If applicable, copy your 7.5 configuration into Configuration Master 7.7, then copy your 7.1 configuration into Configuration Master 7.5.

Web Security appliances assigned to Configuration Master 7.1 at upgrade will not be assigned to any Configuration Master after upgrade.

Preserve Pre-Upgrade Data from the System Capacity Report

This section applies if you are upgrading from a release earlier than AsyncOS 8.0 for Content Security Management.

Beginning in AsyncOS release 8.0 for Cisco Content Security Management, changes have been made to the CPU Usage by Function chart in the System Capacity report.

Specifically, Web Reputation and Web Categorization data in this chart have been combined into a single measure called "Acceptable Use and Reputation." As a result, CPU usage data for “Acceptable Use and Reputation” may not be valid for time ranges that include dates before the upgrade.

If you want to preserve pre-upgrade CPU usage data for Web Reputation and Web Categorization, export or save the data for the CPU Usage by Function chart as CSV or PDF before you upgrade.

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 Security Management Compatibility Matrix, page 3.

Disk Space Reductions

As a result of changes in disk space allocation, the maximum disk space available in this release may have changed from previous releases. Depending on your hardware and the AsyncOS version that you are upgrading from, the maximum disk space available may have increased or decreased. A decrease in available disk space may result in loss of the oldest data after upgrade, based on the amount of data on the appliance that exceeds the new maximum limit.

See Table 1-1 to determine the change that applies to your deployment.

Table 1-1 Maximum Disk Space Available for Different AsyncOS Releases and Hardware, in GB

Disk Space Available (GB)	**Hardware Platform**					
AsyncOS Version	**M160**	**M170**	**M660**	**M670**	**M1060**	**M1070**
8.x	165	165	681	681	1039	1407
7.9	165	165	681	681	1053	1409
7.8	180	180	450	700	800	1500
7.7	180	180	450	700	800	1500

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 Preupgrade Requirements, page 5.

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.

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 Requirements After Upgrade, page 7.

Requirements After Upgrade

Reallocate Disk Space

After upgrade, available disk space may have changed (see Disk Space Reductions, page 6.) However, the disk space allocations that existed before upgrade have not been changed. To allocate new amounts that fit the current disk space, go to **Management Appliance > System Administration > Disk Management**.

Until you do this, you will not be able to load configuration files that you have saved from the appliance.

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 9.

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

Online Help Updates

The following information has been updated in the User Guide PDF, but is not correct in the online help.

File Analysis Reporting

Email and Web Reporting

Complete information about opening firewall ports for File Analysis Details are as follows:

Default Port	Protocol	In/Out	Hostname	Purpose
443	TCP	Out	For web reports: As configured on your Web Security appliance on the Security Services > Anti-Malware and Reputation page, in the Advanced section. For email reports: As configured on your Email Security appliance on the Security Services > File Reputation and Analysis page, in the Advanced section.	Obtain File Analysis Details reporting data.

Email Reporting

The configuration requirements for File Analysis reporting in the Email reporting chapter erroneously give instructions for locating the File Analysis server address on the Web Security appliance. For correct information, see the table above.

Finding Current Information about Known and Fixed Issues

Use the Cisco Bug Search Tool to find the most current information about known and fixed 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 Enter search criteria.

For example, to find all issues fixed in a release:

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`.

c. For **Show Bugs**, select **Fixed in this release**.

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.

Step 4 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.

Documentation For:	Is Located At:
Cisco Content Security Management appliances	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
Cisco Email Security appliances	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Cisco Web Security appliances	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html
Cisco IronPort Encryption	http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html
CLI reference guide	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html

Service and Support

International: Visit http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site: Visit http://www.cisco.com/en/US/products/ps11169/serv_group_home.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.