Release Notes for AsyncOS 8.1.1 for Cisco Content Security Management

Published: October 31, 2013

Revised: December 4, 2013

Contents

- What’s New in This Release, page 2
- Upgrade Paths, page 3
- Security Management Compatibility Matrix, page 4
- Important Notes, page 4
- New and Changed Information, page 5
- Installation and Upgrade Notes, page 5
- Documentation Updates, page 7
- Resolved Issues, page 7
- Known Issues, page 9
- Current Information about Known and Fixed Issues, page 9
- Related Documentation, page 10
- Service and Support, page 11

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

What's New in This Release

Feature	Description
New Features in Release 8.1.1:	
Support for new hardware	This release supports the new M380 and M680 hardware.
Remote power management	This feature is available only on M380 and M680 hardware. You can now remotely reset the power to the appliance chassis. You must configure this feature in advance if you want it to be available when you need it. For more information, see "Enabling Remote Power Management" in the System Administration chapter and "Remotely Resetting Appliance Power" in the Troubleshooting chapter of the user guide or online help.
New Features in Release 8.1.0:	
Centralized policy, virus, and outbreak quarantines	The following quarantines can now be collectively centralized on a Cisco Content Security Management appliance: • anti-virus • outbreak • Policy quarantines used for messages that are caught by – message filters – content filters – data loss prevention policies Centralizing these quarantines offers the following benefits: • Administrators can manage quarantined messages from multiple Email Security appliances in one location. • Quarantined messages are stored behind the firewall instead of in the DMZ, reducing security risk. • Centralized quarantines can be backed up as part of the standard backup functionality on the Cisco Content Security Management appliance. For more information, see Chapter 27, "Quarantines."
My Favorites list	Add the pages you use most to a quick-access menu of your favorite pages. For more information, see Using Favorite Pages, page 58.
Download upgrades in the background	You can now download upgrades in the background and install them later, allowing you to minimize interruption of service. For more information, see Upgrading AsyncOS, page 18.
Roll back to a previous configuration	You can now set your current configuration to a previous configuration, rolling back all configuration changes since that configuration. For more information, see Rolling Back to a Previously Committed Configuration, page 52.

Feature	Description
View recent alerts	You can view a list of recent alerts in the application even if an alert email is not delivered or is deleted. For more information, see Viewing Recent Alerts, page 34.
Enhancements:	
Reporting enhancements	Reporting enhancements let you: • Create a custom report page with the charts and tables you reference most. For more information, see Custom Reports, page 7. • Click links in reports to view the Message Tracking data for messages that violate Data Loss Prevention or Content Filtering policies. This enhancement will simplify investigating patterns and root causes of such violations. In addition, a new Inbound SMTP Authentication report summarizes data for messages received using SMTP session authentication with client certificates, for organizations using a Common Access Card (CAC).
Message Tracking enhancements	• You can now search Message Tracking for: – Messages with UTF-8 encoded subjects – Messages in any quarantine – Messages caught by content filters • Message Tracking search results and message details now include links to the message details page for quarantines that the message resides in • If a Message Tracking query returns more than 1000 messages, you can now export up to 50,000 messages matching your query as a comma-separated values file, for analysis using other tools. • Message tracking includes data for messages received using SMTP session authentication with client certificates, for organizations using a Common Access Card (CAC).
Support for more flexible password lengths	Appliance passwords of any length, including zero characters, are now supported. For more information, see Setting Password and Login Requirements, page 12.
SNMP trap improvements	The linkUp and linkDown SNMP traps have been replaced with standard RFC implementations (RFC-3418).
Spam quarantine improvements	Spam quarantine search results are now easier to view.

Upgrade Paths

You can upgrade to release 8.1.1-013 of AsyncOS for Cisco Content Security Management from the following versions:

- 7.2.2-107
- 7.7.0-206
- 7.9.0-107
- 7.9.0-302

- 7.9.1-039
- 7.9.1-102
- 8.0.0-404
- 8.1.0-476

Security Management Compatibility Matrix

Compatibility with AsyncOS for Email Security Appliances and AsyncOS for Web Security Appliances 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, page 4
- SNMP, page 4

Sign Up to Receive Important Notifications

In order to receive Security Advisories, Field Notices, End of Sale and End of Support announcements, and information about software updates and known issues, you must sign up to receive notifications.

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

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.

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.

- Centralized Policy, Virus, and Outbreak Quarantines No Longer Require a Feature Key, page 5

Centralized Policy, Virus, and Outbreak Quarantines No Longer Require a Feature Key

In Release 8.1.1, the Centralized Policy, Virus, and Outbreak Quarantines feature no longer requires a feature key.

Installation and Upgrade Notes

- Supported Browsers, page 5
- Pre-Upgrade Requirements, page 5
- Upgrading to This Release, page 6
- Post-Upgrade Requirements, page 7

Supported Browsers

Supported browsers are listed in the "Browser Requirements" section in the Online Help and in the "Setup, Installation, and Basic Configuration" chapter of the *AsyncOS for Cisco Content Security Management User Guide*.

Pre-Upgrade Requirements

Perform the following important preupgrade tasks:

- Important Additional Reading, page 5
- Disk Space Reductions, page 6
- Back Up Your Existing Configuration, page 6

Important Additional Reading

If you are upgrading from a release earlier than the immediate previous release, you should carefully review the release notes for all releases between your release and this release. Information that affects those releases also applies to upgrades to this release.

Note Some releases include changes that can impact existing configurations. For example, old Configuration Masters (for managing Web Security Appliances) may be deleted.

For links to release notes for past releases, see Related Documentation, page 10.

Disk Space Reductions

As a result of changes in disk space allocation, the maximum disk space available in this release has changed. 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**	**M380**	**M650**	**M660**	**M670**	**M680**	**M1050**	**M1060**	**M1070**
8.1.1	165	165	968	—	681	681	1805	—	1039	1407
8.1.0	165	165	—	—	681	681	—	—	1039	1407
8.0	165	165	—	—	681	681	—	—	1039	1407
7.9	165	165	—	187	681	681	—	429	1053	1409
7.8	180	180	—	186	450	700	—	405	800	1500
7.7	180	180	—	186	450	700	—	405	800	1500
7.2	180	180	—	186	450	700	—	405	800	1500

Back Up Your Existing Configuration

Before upgrading your Cisco Content Security Management appliance, save the XML configuration file from your appliance to a volume other than the appliance. For important caveats and instructions, see the “Saving and Exporting the Current Configuration File” section in the *AsyncOS for Cisco Content Security Management User Guide* or the online help.

Upgrading to This Release

Before You Begin

Obtain the user guide PDFs for this release and for your current release, from http://www.cisco.com/en/US/products/ps10155/products_user_guide_list.html.

Step 1 Address all topics described in Pre-Upgrade Requirements, page 5.

Step 2 Follow all instructions in the “Before You Upgrade: Important Steps” section in the “Common Administrative Tasks” chapter of 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 PRE-UPGRADE release. Be sure to address any additional applicable prerequisites.

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 Address all topics in Post-Upgrade Requirements, page 7.

Post-Upgrade Requirements

Reallocate Disk Space

After upgrade, disk space will automatically be allocated for the centralized policy, virus, and outbreak quarantine feature. The amount of space allocated will be the smaller of:

- The default space allocated in new installations for centralized policy, virus, and outbreak quarantines, as described for each hardware model in the table in the Disk Management section of the User Guide.
- All remaining allocable disk space

If you do not plan to centralize policy, virus, and outbreak quarantines, you should reallocate disk space after upgrade.

Documentation Updates

Please note the following changes to the online help. These changes have been incorporated into the latest version of the user guide PDF.

Maximum Disk Space for Spam Quarantine on M380 and M680 Hardware

Correct values for maximum disk space allocable to the spam quarantine are:

- For M380: 150 GB
- For M680: 265 GB

Resolved Issues

Note

- The most current information about open and resolved issues is available via the Bug Search Tool. See Current Information about Known and Fixed Issues, page 9.
- If you are upgrading from a version other than the release immediately preceding this version, see also the Resolved Issues lists in the Release Notes for each version between your original release and this release.

- Issues in AsyncOS for Email and AsyncOS for Web that affected the Cisco Content Security Management appliance may be documented in the release notes for those products.

Resolved Issues in Release 8.1.1

Table 2 Resolved Issues in Release 8.1.1

Reference Number	Description
CSCuf52204	Tracking results with unusual UTF Subjects causes memory exceptions
CSCuf56294	Appfault occurs when try to select Authorized Groups on SOCKS Policy
CSCuf82028	SMA is unusably slow when using ICCM with lots of WSAs
CSCug69245	All centralized services show errors on System Status page after upgrade
CSCug76474	Decryption policy with global identity disabled on import to Configuration Master 7.7
CSCug90456	LDAPS is unusable after upgrade
CSCuh24749	Reflected Cross Site Scripting Vulnerability
CSCuh24755	Stored Cross Site Scripting
CSCuh38818	SMA with SSHv1 key loses connectivity to WSA/ESA after upgrade to 8.x
CSCui83063	SNMP sends incorrect OID values for traps
CSCzv28496	deleterecipients based on Centralized Policy Quarantines release host not working

Resolved Issues in Release 8.1.0

Table 3 Resolved Issues in Release 8.1.0

Old Defect ID	New Defect ID	Description
—	CSCzv81712	**Fixed: IronPort Spam Quarantine (ISQ) Denial of Service Vulnerability** A vulnerability in the appliance could have allowed an unauthenticated, remote attacker to cause multiple critical processes to become unresponsive, resulting in a denial of service condition. For more information, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-sma.
—	CSCzv78669	**Fixed: Management Graphical User Interface Denial of Service Vulnerability** A vulnerability in the appliance could have allowed an unauthenticated, remote attacker to cause multiple critical processes to become unresponsive, resulting in a denial of service condition. For more information, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-sma.
37638	CSCzv11562	**Fixed: Searches for UTF-8-encoded subjects are now supported in Message Tracking** For more information, see the New Features section.

Table 3 Resolved Issues in Release 8.1.0

Old Defect ID	New Defect ID	Description
84281	CSCzv18056	**Fixed: Large Number of Content Filter Matches May Result in PDF Report Error** Fixed an issue a printable PDF report for content filters may contain the error message "one of tables has too many columns" due to a large number of incoming or outgoing content filter matches. Now, the PDF report prints out correctly.
—	CSCuf57558	**Fixed: SNMP MIBs cannot be loaded into MIB browser** This issue applied only to MIBs downloaded from the appliance.
70279 87369	CSCzv56988	**Fixed: SNMP trap issues** Various issues with the link status (linkUp, linkDown) SNMP trap For example: • The snmp trap interface index incorrectly identified the interface • The link status sent from the appliance when the P1 or P2 port went up or down did not include information about the event. Now, the use of the linkUp and linkDown traps have been deprecated. Cisco recommends that you use the standardized traps in RFC-3418 instead.
49096	CSCzv18535	**Fixed: (External RADIUS Authentication) System takes into account just the first RADIUS Class attribute** Users with multiple class attributes are now supported. If a user is assigned multiple Class attributes that are mapped to custom user roles, the last class attribute on the list in the RADIUS server will be used. For details, see the user guide or online help.

Known Issues

Note

- Information about known issues in this release is available via the Bug Search Tool. See Current Information about Known and Fixed Issues, page 9.
- Some issues may also have been present in previous releases. These issues are described in previous release notes.
- Known issues in AsyncOS for Email and AsyncOS for Web that affect the Cisco Content Security Management appliance may be documented under those product names in the Bug Search Tool or in the release notes for those products.

Current Information about Known and Fixed Issues

Use the Cisco Bug Search Tool to find the most current information about known and fixed 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

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, search for "Cisco Content Security Management Appliance" and enter the AsyncOS version number.

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.

Related Documentation

The documentation set for Cisco content security products includes the following key documents and books. Not all types are available for all products and releases, and other documentation may also exist.

- Release Notes
- Quick Start Guides
- Hardware and virtual appliance installation guides
- User Guides (for administrators)
- Command-line interface (CLI) reference guide

Documentation is available at the following locations:

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

Use the following methods to obtain support:

U.S.: Call 1 (408) 526-7209 or toll-free 1 (800) 553-2447

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

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

You can also access customer support from the appliance. For instructions, see the User Guide or online help.

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.