Release Notes for Cisco IronPort AsyncOS 7.9.1 for Security Management

Published: June 27, 2013

Revised: September 13, 2013
Added newly qualified upgrade path.

Contents

What's New in Cisco IronPort AsyncOS 7.9 for Security Management

This section describes the new features and enhancements in release 7.9 of AsyncOS for Security Management.

Cisco Systems, Inc.
www.cisco.com

You might also find it useful to review release notes for earlier releases to see the features and enhancements that were previously added.

In addition, see the New Features list in the Release Notes for Cisco IronPort AsyncOS 7.6 for Email Security at http://www.cisco.com/en/US/products/ps10154/prod_release_notes_list.html.

Table 1 New Features for AsyncOS 7.9 for Security Management

Feature	Description
New Features:	
Reporting and Message Tracking support for new Email Security features	The following new features in AsyncOS 7.6 for for Email Security are supported in Centralized Reporting and/ or Centralized Message Tracking: • Support in Reporting, tracking, and Cisco IronPort Spam Quarantine for messages sent via IPv6. (All interfaces on the Security Management appliance continue to use IPv4 in this release.) • Reporting and Message Tracking support for Rate Limiting per sender. This includes a new centralized Rate Limits report, which lets you identify the top senders of mass email messages received by your organization. • Identification in Message Tracking for messages handled by the new "Quarantine a copy and deliver" feature, which allows you to monitor Data Loss Prevention violations without taking action on messages. For general information about the features underlying these reports, see the Release Notes for Cisco IronPort AsyncOS 7.6 for Email Security. See also Searching and the Interactive Email Report Pages and the Rate Limits Page in the Using Centralized Email Security Reporting chapter, and Searching for Email Messages in the Tracking Email Messages chapter.
Different server settings for upgrades and service updates	You can now specify separate download server settings for upgrades and for updates, for both image and list servers. For example, you can now specify a local server for AsyncOS upgrades and the Cisco IronPort update servers for service updates, giving you control over timing of upgrades while benefiting from service updates immediately. For more information, see the Configuring Upgrade and Service Update Settings section in the Common Administrative Tasks chapter.
Enhancements:	
Enhanced: More granular control over DLP Tracking Privileges	You can now restrict access to sensitive Data Loss Prevention information in Message Tracking by user role. For information, see Controlling Access to Sensitive DLP Information in Message Tracking in the Distributing Administrative Tasks chapter.
Enhanced: SNMP	Support for 64bit counters for high capacity interfaces is now available in SNMP. You can now obtain appliance status using ifXTable (COUNTER64), SNMP MIB OID.
Enhanced: Browser support on Windows 7	AsyncOS for Security Management now supports Internet Explorer 8 running on Windows 7.

Upgrade Paths

You can upgrade to release 7.9.1-102 of AsyncOS for Security Management from the following versions:

- 7.2.2-107
- 7.2.2-110
- 7.7.0-210
- 7.7.0-213
- 7.9.0-107
- 7.9.0-110
- 7.9.0-201
- 7.9.0-302
- 7.9.1-030
- 7.9.1-039

SMA Compatibility Matrix

For compatibility of AsyncOS for Security Management with AsyncOS for Email Security and AsyncOS for Web Security releases, see the separate compatibility matrix document at http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html.

Important Notes

- Sign Up to Receive Important Notifications, page 3

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 the existing email announcement service. You must sign up with the Cisco Notification Service to receive future announcements.

Installation and Upgrade Notes

Supported Browsers

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

Preupgrade Requirements

Perform the following important preupgrade tasks:

Upgrade to Compatible Email and Web Security Appliance Versions

Verify that the Email Security appliances and Web Security appliances that you want to manage will run releases that are compatible, and upgrade or retire any that are not. See the SMA Compatibility Matrix, page 3.

Note that a minor release (X.X.x) may be compatible where a major release (X.X) is not.

Important Changes in Centralized Configuration Management for Web Security

If your Security Management appliance is running a release earlier than AsyncOS 7.8 and you use centralized configuration management for Web Security appliances:

Before upgrading, carefully read the *Release Notes for Cisco IronPort AsyncOS 7.8 for Security Management* at http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html, as the changes described for that release also apply to upgrades to this release. Your existing Configuration Master settings may change upon upgrade, and you may need to make additional changes to those settings.

Disk Space Reduction

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 1-2 to determine the change that applies to your deployment.

Table 1-2 Maximum Disk Space Available for Different AsyncOS Releases and Hardware

Disk Space Available	Hardware Platform							
AsyncOS Version	**M160**	**M170**	**M650**	**M660**	**M670**	**M1050**	**M1060**	**M1070**
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
6.7.8	186	186	186	450	450	405	800	800
6.7.7	186	—	186	450	450	405	800	800
6.7.6	195	—	186	450	—	405	800	—

Upgrading to This Release

Caution If you are upgrading from AsyncOS 7.2.1 or earlier and you have M160 hardware:
You may need to upgrade the hard drive firmware before you upgrade the AsyncOS. To verify whether or not your M160 requires the firmware upgrade, run the **upgrade** command at the command line prompt. If the M160 requires the firmware upgrade, "Hard Drive Firmware upgrade (for C/M/S160 models only, build 002)" will be listed as an upgrade option. If listed, run the firmware upgrade, and then upgrade AsyncOS for Security Management.
See the *Cisco IronPort Hard Driver Firmware Upgrade for C160, S160, and M160 Appliances Release Notes* on Cisco.com for more information.

Additional information about upgrading is in the "Upgrading AsyncOS" section of the "Common Administrative Tasks" chapter of the *Cisco IronPort AsyncOS for Security Management User Guide*.

Step 1 Save the XML configuration file from the Security Management appliance:

On the Security Management appliance, click **Management Appliance > System Administration > Configuration File**. For complete information, see the documentation for your release of the Security Management appliance.

Step 2 If you are using the Safelist/Blocklist feature, export the list from the appliance:

On the Security Management appliance, click **Management Appliance > System Administration > Configuration File** and scroll down. For complete information, see the documentation for your release of the Security Management appliance.

Step 3 Perform the upgrade:

a. On the Security Management appliance, click **Management Appliance > System Administration > System Upgrade.**

b. Click **Available Upgrades**.

The page displays a list of available AsyncOS for Security Management upgrade versions.

c. Click **Begin Upgrade** to start the upgrade process.

Answer the questions as they appear.

d. When the upgrade is complete, click **Reboot Now** to reboot the Security Management appliance.

Note Before viewing the new online help after upgrade, exit the browser and then open it again. This clears the browser cache of any outdated content.

New and Changed Information

New End User License Agreement

The text of the End User License Agreement has changed in Release 7.9.1. You can read the new license agreement and supplement in the online help by scrolling to the bottom of the Contents section and clicking the relevant link.

Opening Support Cases Through the Appliance

If you open a support case using the appliance, the severity level is 3. Previously, you could set the severity level using the appliance.

To open a support case at a higher severity level, contact Customer Support.

Documentation Updates

Please note the following changes to the *Cisco IronPort AsyncOS 7.9 for Security Management User Guide*.

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

Reporting and Tracking

Distinction Between Second-Level Domains and Subdomains

In reporting and tracking searches, second-level domains (regional domains listed at http://george.surbl.org/two-level-tlds) are treated differently from subdomains, even though the two domain types may appear to be the same. For example:

- Reports will not include results for a two-level domain such as `co.uk`, but will include results for `foo.co.uk`. Reports include subdomains under the main corporate domain, such as `cisco.com`.
- Tracking search results for the regional domain `co.uk` will not include domains such as `foo.co.uk`, while search results for `cisco.com` will include subdomains such as `subdomain.cisco.com`.

Web Reporting and Tracking Data Availability for L4TM and Client Malware Risk

On the Web Tracking page, for L4TM information, only data that is added after upgrade to AsyncOS 7.8 or 7.9 for Security Management and AsyncOS 7.5 for Web is included in search results.

Tables on the L4 Traffic Monitor Page and the Client Malware Risk Page display the number of blocked and monitored connections to malware sites. For data that is collected after upgrade to AsyncOS 7.8 or 7.9 for Security Management and AsyncOS 7.5 for Web, you can click a number in the table to view details about the relevant individual connections. For pre-upgrade data, only the totals are available.

Filtering by port on the L4 Traffic Monitor Page is also not available for pre-upgrade data.

For more information about these pages, see the "Using Centralized Web Reporting" chapter in the *Cisco IronPort AsyncOS for Security Management User Guide*.

Supported Hardware

Any references in the Online Help or User Guide to M600 or M1000 appliances are no longer valid. This release of AsyncOS for Security Management is not supported on those appliances.

Resolved Issues

Table 3 Resolved Issues in This Release of AsyncOs 7.9.1 for Security Management

Old Defect ID	New Defect ID	Description
Resolved in Release 7.9.1-102		
—	CSCzv24579	**Fixed: Web Framework Authenticated Command Injection Vulnerability** A vulnerability in the appliance could have allowed an authenticated, remote attacker to execute arbitrary commands on the underlying operating system with elevated privileges. For more information, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-sma.

Table 3 Resolved Issues in This Release of AsyncOs 7.9.1 for Security Management (continued)

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.
—	CSCuf82028	**Fixed: SMA is unusably slow when using Centralized Configuration Management with many WSAs** The web interface was very slow when visiting pages like System Status and Web Appliance Status.
Resolved in Release 7.9.1-039		
92304	CSCzv12825	**Fixed: Newly quarantined messages are prevented or delayed from reaching the end-user spam quarantine** When this situation occurred, the tophost command in the SMA CLI showed many messages pending delivery to the spam quarantine. Messages with incorrectly formatted utf subjects could trigger this defect.
Resolved in Release 7.9.1-030		
85307	—	**Fixed: Loading a configuration file fails after resetting the appliance to the factory default or reverting to a previous release** Previously, a workaround was required in order to load a configuration file in these situations, if the Security Management appliance managed one or more Web Security appliances running AsyncOS 7.5.
85724	—	**Fixed: Proxy Server settings for upgrade server are incorrect when selected in CLI** The proxy server settings for the upgrade server are now correct.
87072	—	**Fixed: Delay in importing reporting archives from Email Security appliances** Previously, this caused a performance decrease when many Email Security appliances were associated with the Security Management appliance. This delay no longer occurs.
69125	—	**Fixed: resourceConservationMode SNMP trap is missing** This trap is now available via `snmpconfig` in the CLI.
84563	—	**Fixed: Client applications with user agent Firefox 10.x erroneously match Identity Policies configured for Firefox 1.x** Previously, client applications with user agent Firefox 10.x erroneously matched Identity Policies configured for Firefox 1.x. This no longer occurs.

Table 3 Resolved Issues in This Release of AsyncOs 7.9.1 for Security Management (continued)

Old Defect ID	New Defect ID	Description
85235	—	**Fixed: Search for "Internal Sender IP Address" does not work** Previously, searching for an internal sender IP address nearly always returned "No data was found in the selected time range". This issue also occurred when clicking on an IP address under the Incoming Mail -> IP Address and Outgoing Sender -> IP Address reports.
87246	—	**Fixed: Removing a hard disk does not generate an snmp trap** Removing a hard disk now generates the expected trap.
87098	—	**Fixed: Critical error alert is inappropriately sent when an LDAP-authenticated user logs in to End User Quarantine and the mail attribute for that account is empty** This situation now generates an appropriate error which is shown to the user, and an appropriate warning appears in the euqgui logs.
87613	—	**Fixed: Online Help for End User Quarantine page is not translated (Japanese)** The page has now been translated.
82858, 85887, 82202	—	**Fixed: Japanese translation errors in online help for End User Quarantine** Multiple translation errors have been fixed.
68125	—	**Fixed: resourceConservationMode SNMP trap is not available** This trap is now available again.
73467	—	**Fixed: Rebooting the appliance without proper shutdown sometimes causes irreparable damage to the appliance** This issue no longer occurs.
—86549	—	**Fixed: Attempts to generate a Web Tracking report in PDF format result in an application fault if the report data includes very long URLs** This issue no longer occurs.
76210	—	**Fixed: Traceback generated after technical support tunnel fails for reasons related to DNS** Previously, when attempting to establish a secure tunnel through which Cisco IronPort technical support can connect to the Appliance, if the tunnel attempt failed for reasons related to DNS, AsyncOS generated a traceback.
82866	—	**Fixed: End User Quarantine Advanced Search Page has Japanese translation errors** These translation errors have been fixed.
86807	—	**Fixed:Web Tracking search by User/Client IP address does not fetch any results** This issue has now been fixed.

Known Issues

Note Known issues in AsyncOS for Email Security and AsyncOS for Web may also affect functionality on the Security Management appliance. See also the release notes for those products.

Table 4 Known Issues in This Release

Old Defect ID	New Defect ID	Description
85567	CSCzv12107	**Privileges for custom web user roles in Configuration Masters disappear after upgrade** This issue has been fixed in release AsyncOS 8.0 for Security Management.
71470	CSCzv11245	**Loading, importing, or publishing an XML configuration file fails if the hostname specified in a SaaS Policy cannot be resolved** This failure can occur when doing any of the following: • Loading the configuration file directly on the Security Management Appliance or the Web Security Appliance. • Importing the configuration file into a Configuration Master on the Security Management Appliance. • Publishing the configuration file to the Web Security Appliance.
91441	CSCzv66810	**Alert about authentication error may not be sent when the SMA fails to establish an SSH connection to a new ESA or WSA** If you replace an Email or Web Security Appliance (for example, if you return an appliance with an RMA) you must re-authenticate the new machine from the SMA because the SSH host key has changed.
84281	CSCzv18056	**Content filters report PDF shows only an error message if there are many content filter matches** If there are many content filter matches in the Incoming/Outgoing content filter matches graph, the PDF generates but shows an error instead of the expected data.
84881	CSCzv43434	**Application fault occurs if centralized reporting is enabled but zero disk space is allocated for centralized reporting** The following application fault occurs if centralized reporting is enabled but zero disk space is allocated for centralized reporting: 'No such file or directory...'. To prevent this issue: Before you enable centralized email and/or web reporting, go to System Administration > Disk Management and ensure that at least 1 GB of disk space has been allocated for Centralized Reporting. To recover from this issue: Allocate disk space as described above, then reboot the appliance.
84778	CSCzv34188	**Issue Priority options on “Open a Technical Support Case” page are not translated** On the “Open a Technical Support Case” page under the Help and Support menu, the options for Issue Priority do not appear in the language currently selected in Preferences.
84595	CSCzv06303	**Scheduled reports in languages other than English are generated with DAT filename extension instead of PDF or CSV** Workaround: Change the filename extension to the intended format (CSV or PDF), then open the file.

Table 4 Known Issues in This Release (continued)

Old Defect ID	New Defect ID	Description
83979	CSCzv75331	**Some pre-upgrade reporting data is missing from Incoming Mail: IP Address report details** IP addresses in pre-upgrade data that are in the range 128.x.x.x to 255.x.x.x will be counted in the report summary, but will not be available in report details. This issue does not occur with new data entering the system after upgrade, and the discrepancy will disappear when the older data "ages out" of the system.
83348, 83623	CSCzv36110 CSCzv93649	**Languages that are read from right to left, such as Arabic or Hebrew, do not appear correctly in PDFs Generated from AsyncOS** PDFs generated from the appliance's interface, such as the Message Details page or the Printable PDF link in Message Tracking, do not display text of languages that are read from right to left, such as Arabic or Hebrew. This text displays as black boxes.
72405	CSCzv31977	**When searching for groups in external directory servers, if there are more than 500 matches, the SMA does not display all matching results** If the desired group is not found by directory search you may add it to the "Authorized Groups" list by entering it in the Directory search field and clicking the "add" button. These instructions have been documented in the pop-up "?" help available beside the directory search option on the Add Access Policy page.
81115	CSCzv96976	**SMTP Routes behavior is different on SMA than on ESA** On the Security Management appliance, SMTP Routes are used only for sending alerts and emailed reports (scheduled or generated on-demand). When multiple SMTP Routes are configured, the SMA provides failover only, not round-robin.
76201	CSCzv05651 (ESA bug)	**SMA Cannot Communicate with ESA after AsyncOS Reversion on the ESA** If your Email Security appliance is connected to a Security Management appliance, reverting the version of AsyncOS on the ESA to a previous version prevents the SMA from communicating with it. Workaround: Re-authenticate the SMA's connection to the ESA.

Related Documentation

The documentation set for Cisco IronPort appliances includes the following documents and books (not all types are available for all appliances and releases):

- Release Notes for all products
- The *Quick Start Guide* for the Security Management appliance
- *Cisco IronPort AsyncOS for Security Management User Guide*
- *Cisco IronPort AsyncOS for Web User Guide*
- Cisco IronPort AsyncOS for Email Security user guides:
  - *Cisco IronPort AsyncOS for Email Security Configuration Guide*
  - *Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*
  - *Cisco IronPort AsyncOS for Email Security Daily Management Guide*
- *Cisco IronPort AsyncOS CLI Reference Guide*

This and other documentation is available at the following locations:

Documentation For:	Is Located At:
Security Management appliances	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
Email Security appliances and the CLI reference guide	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
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

Service and Support

For support information, visit the following sites:

- http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html
- http://www.cisco.com/en/US/products/ps11169/serv_group_home.html