Release Notes for Cisco IronPort AsyncOS 7.7.1 for Security Management

Published: May 14, 2012

Revised: April 24, 2013

Contents

This document contains information for Cisco IronPort AsyncOS 7.7.1 for Security Management. This document includes the following sections:

What's New in Cisco IronPort AsyncOS 7.7 for Security Management

This section describes the new features and enhancements in AsyncOS 7.7 for Security Management. For more information about the release, see the complete documentation at:

http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html

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

You might also find it useful to review release notes for earlier releases to see the features and enhancements that were previously added. Release notes for all releases are available via the link above.

Table 1 summarizes the new features and enhancements that are included in this version of AsyncOS for Security Management.

Table 1 New Features for AsyncOS 7.7 for Security Management

Feature	Description
New Features:	
Custom Email User Roles for Delegated Administration	In AsyncOS 7.7, you can design custom user roles for administrative access to the following email security-related features on the Security Management appliance: • All email reports (optionally restricted by Reporting Group) • Mail policy reports (optionally restricted by Reporting Group) • DLP reports (optionally restricted by Reporting Group) • Message tracking • Spam quarantine Chapter 12, "Common Administrative Tasks."
Technician Role	New in AsyncOS 7.7, the predefined Technician role allows users to perform system upgrades, reboot the appliance, manage feature keys, and perform other tasks required to upgrade the Security Management appliance. Chapter 12, "Common Administrative Tasks."
DLP Tracking Privileges	AsyncOS 7.7 allows on-Administrator users to view content in Message Tracking that matches a DLP policy violation. You can enable or disable this access to control visibility of sensitive information. Chapter 12, "Common Administrative Tasks."
Restrictive User Accounts and Password Settings	AsyncOS 7.7 allows you to define user account and password restrictions to enforce organizational password policies. The available password restrictions include mandatory characters, password length, and password lifetime. You can also define how many failed login attempts cause the user to be locked out of the account. Chapter 12, "Common Administrative Tasks."
IP-Based Access	In AsyncOS 7.7, you can control from which IP addresses users access the Security Management appliance. Users can access the appliance from any machine with an IP address from an access list that you define. If your organization's network uses reverse proxy servers between remote users' machines and the Security Management appliance, AsyncOS 7.7 allows you to create an access list with the IP addresses of the proxies that can connect to the appliance. Chapter 12, "Common Administrative Tasks."
Web UI Session Timeout	AsyncOS 7.7 allows you to specify how long a user can be logged into the Security Management appliance's Web UI before AsyncOS logs the user out due to inactivity. This Web UI session timeout applies to all users, including admin, and it is used for both HTTP and HTTPS sessions. Chapter 12, "Common Administrative Tasks."

Table 1 New Features for AsyncOS 7.7 for Security Management (continued)

Feature	Description
Packet Capture	AsyncOS 7.7 provides packet capture controls, letting you intercept and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached. This feature can help you debug the network setup and to discover what network traffic is reaching or leaving the appliance. Chapter 2, "Setup and Installation."
Timezone Updates	Effective in AsyncOS 7.7, time zone files can be updated independently of AsyncOS upgrades. You can check for time zone file updates and update time zones manually on the Management Appliance > System Administration > Time Settings page. Chapter 12, "Common Administrative Tasks."
Enhancements:	
Virus Outbreak Filters Report	The Virus Outbreak Filters report has been enhanced and renamed to the Outbreak Filters Report. This report now also includes information on malware distribution, scams, and phishing attempts. Chapter 4, "Using Centralized Email Reporting."
PDF Reports Enhancements	New in AsyncOS 7.7, you can generate PDF reports in languages other than English and properly render all non-ASCII characters in PDF reports. PDF reports containing multiple reports now include links at the top of the PDF. Chapter 3, "Appliance Configuration."
Attachment Search	AsyncOS 7.7 allows you to search for messages by attachment name in Message Tracking. Chapter 6, "Tracking Email Messages."

Upgrade Paths

You can upgrade to release 7.7.1-039 from the following versions:

- 7.2.2-106
- 7.2.2-107
- 7.2.3-038
- 7.2.3-039
- 7.7.0-206
- 7.7.0-207

Compatibility Matrix

This section describes the compatibility between AsyncOS 7.7.1 for the Security Management appliance and the various AsyncOS releases for the Email Security appliance and the Web Security appliance. Additionally, it includes a table of supported configuration file versions.

Security Management Appliance Compatibility with AsyncOS for Email Security

This release of AsyncOS for Security Management is compatible with the following releases of AsyncOS for Email:

- 7.1.5
- 7.5.1
- 7.5.2

Security Management Appliance Compatibility with AsyncOS for Web Security

This release of AsyncOS for Security Management is compatible with the following releases of AsyncOS for Web:

Table 1-2 Security Management Appliance Compatibility with Web Security Appliances

Version	Centralized Reporting and Tracking	Publish a Configuration Master to Web Security appliances	Advanced File Publish to Web Security appliances
WSA 5.7	Feature not Available	Supported by 5.7 Configuration Master	Configuration file version must match target WSA version.
WSA 6.3	Feature not Available	Supported by 5.7 and 6.3 Configuration Master. 6.3 Configuration Master can publish to WSAs running 6.3.8 only.	Configuration file version must match target WSA version to three digits of specificity (for example 6.3.3.)
WSA 7.0	Feature not Available	Supported by 6.3 Configuration Master	Configuration file version must match target WSA version.
WSA 7.1	Support See limitation in Resolved Issue 79474, page 12.	Supported by 6.3 and 7.1 Configuration Master 7.1 Configuration Master can publish to WSAs running 7.1.4-053 only.	Configuration file version must exactly match target WSA version including build number (for example, 7.1.4-052).

Table 3 (Deployments with WSAs Only) Configuration Master Compatibility

Populate settings for Configuration Master version:	Populate settings by copying existing Configuration Master version:	Populate settings by importing a configuration file from Web Security appliance version:
5.7	Not applicable	Web Security appliance 5.7
6.3	Configuration Master 5.7	Web Security appliance 6.3.8
7.1	Configuration Master 6.3	Web Security appliance 7.1.4-053

Installation and Upgrade Notes

Preupgrade Notes

Be aware of the upgrade impacts and advisories discussed in the following topics.

Disk Space Reduction

This issue applies only to M160 hardware.

Some AsyncOS for Security Management releases prior to this release had more disk space available for data storage than is available in this release, as specified in Table 4:

Table 4 Total Maximum Disk Space on M160

Release	Total Maximum Disk Space in GB
AsyncOS 6.5.x	195
AsyncOS 6.7.x	186
AsyncOS 7.2.x	180
AsyncOS 7.7	180

When upgrading to AsyncOS 7.x, if your M160 has more than 180 GB of existing data, any data above this amount will be lost upon upgrade, starting with the oldest data.

Verify Associated Email and Web Security Appliance Releases

Before upgrading to AsyncOS 7.7, verify that the Email Security appliances and Web Security appliances that you want to manage are running releases that are compatible. See the Compatibility Matrix, page 4. Compatibility may change with each upgrade.

Configuration File Backup

Before upgrading your Security Management appliance, save the XML configuration file from your existing Security Management appliance. For instructions, see the "Managing the Configuration File" section in the *Cisco IronPort AsyncOS 7.8 for Security Management User Guide*.

Upgrading to the AsyncOS 7.7 Release

Warning **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.

To upgrade to AsyncOS 7.7 for Security Management:

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

On the Security Management appliance, click **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 **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 **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.

Important Notes

Signing 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.

Documentation Updates

Please note the following changes to the *Cisco IronPort AsyncOS 7.7 for Security Management User Guide*.

Requirements for Backups

In addition to the requirements already stated in the “Restrictions for Backups” section in the “Common Administrative Tasks” chapter of the user guide, note the following requirement:

The source and target Security Management appliances must be able to communicate using SSH. Therefore:

- Port 22 must be open on both appliances. By default, this port is opened when you run the System Setup Wizard.
- The Domain Name Server (DNS) must be able to resolve the host names of both appliances using both A records and PTR records.

Reporting and Tracking

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`.

Known Issues

Note Known issues in AsyncOS for Email Security and AsyncOS for Web Security are documented in the release notes for those products.

Table 5 describes the known issues for the Security Management appliance for this release.

Table 5 Known Issues in Cisco IronPort AsyncOS 7.7 for Security Management

Defect ID	Description
85389	**Error in some situations when importing 6.3 configuration to initialize a 6.3 Configuration Master** If you receive the error "Configuration conflict detected!" when trying to import a 6.3 configuration to initialize a Configuration Master, try the following workaround: Abandon the changes, then try importing the configuration again.
78045	**Compatibility issues with configuration files from AsyncOS 7.1.2 for Web Security** Advanced file publish cannot be used to publish a configuration file from AsyncOS 7.1.2 for Web Security to Web Security appliances running AsyncOS 7.1.0 or 7.1.1.
77609	**Active Sessions page and 'who' CLI command cannot identify active CLI users whose usernames contain 16 characters** Neither the `who` CLI command nor the Active Sessions page identify active CLI users whose user name is 16 characters long.
76201	**SMA Cannot Communicate with some managed appliances after AsyncOS Reversion** If your Email or Web security appliance is connected to a Security Management appliance, reverting the version of AsyncOS on the managed appliance to a previous version may prevent the SMA from communicating with it. Workaround: Re-authenticate the SMA's connection to the managed appliance.

Table 5 Known Issues in Cisco IronPort AsyncOS 7.7 for Security Management (continued)

Defect ID	Description
74336	**If a power loss occurs on the destination appliance while a backup is in progress, the backup cannot be restarted** The source appliance is unable to detect that the backup is no longer actually in progress and thus a new backup cannot be initiated.
73133	**Domain-Based executive summary report counts stopped by reputation filtering incorrect** The Stopped by Reputation Filtering results in the Domain-Based Executive Summary report on the Security Management appliance cannot be seen. **Workaround**: To see Stopped by Reputation Filtering results in your Domain-Based Executive Summary report on the Security Management appliance, you must have **hat_reject_info** enabled on both the Email Security appliance and the Security Management appliance. To enable the **hat_reject_info** on the Security Management appliance, run the **reportingconfig > domain > hat_reject_info** command. This information has been added to the user guide and online help.
72405	**When searching for groups in external directory servers, if there are more than 500 matches, the SMA does not display all matching results** **Workaround:** 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.
67749	**Initiation of multiple nearly-simultaneous immediate backup processes may be allowed** Rarely, it is possible to initiate multiple closely-overlapping immediate backups. However, in such cases, only one backup will run. This does not interfere with future backups, but you can use the `backupconfig > cancel` command to delete the extra backup process(es) from the list of scheduled backups.

Resolved Issues

Resolved in Release 7.7.1

Table 6 Resolved issues in Cisco IronPort AsyncOS 7.7.1 for Security Management

Defect ID	Description
83688	**Fixed: Cloud Admin accounts cannot access scheduled and archived reports** Users logged in as cloud administrators were not able to access scheduled and archived reports. This has now been fixed.
82692	**Fixed: CPU usage may unexpectedly run at maximum capacity** Previously, in rare circumstances, SNMP could drive CPU usage to %100. This problem has now been fixed.
83262	**Fixed: FreeBSD telnetd Remote Code Execution Vulnerability** Previously, there was a vulnerability that could have allowed a remote, unauthenticated attacker to execute arbitrary code with elevated privileges. This has now been fixed. For more information on the vulnerability, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120126-ironport
82513	**Fixed: SMA backups failing due to verbosity** Backups no longer fail for this reason, and the verbose logging option is now available only to support personnel.
82858	**Fixed: Japanese translation of EUQ Online help documentation for end users is incorrect** These translation errors have been corrected.
80938	**Fixed: More than one day's data displays in web report when Day is selected, and clicking a value in a table on the reporting page produces an error on the Web Tracking page** Previously, on the web report, Day appeared to be selected for the time range, but more than one day's data was displayed in the report. Clicking a value in a table on the web reporting page displayed the Web Tracking page, where the Time Range option displayed the error: "That value is not valid". This issue occurred if you selected Year for the time range for email reports, then viewed any web report without changing the time range. (Year is not a supported time range for web reports.) This issue has been fixed.
80601	**Fixed: Users from group "Email Administrators" cannot log in directly to the Spam Quarantine** Previously, after upgrade to release 7.7.0, users who attempted to access the Spam Quarantine without signing in first to the web interface of the Security Management appliance could not log in. This issue has bee fixed.

Table 6 Resolved issues in Cisco IronPort AsyncOS 7.7.1 for Security Management

Defect ID	Description
80493	**Fixed: (Japanese language only) Releasing a message from spam quarantine appears to delete it** When releasing a message from the spam quarantine, the GUI incorrectly stated that the message was deleted instead of released.
80938	**Fixed: More than one day's data displays in web report when Day is selected, and clicking a value in a table on the reporting page produces an error on the Web Tracking page** Formerly, on the web report, Day appeared to be selected for the time range, but more than one day's data was displayed in the report. Clicking a value in a table on the web reporting page displayed the Web Tracking page, where you saw the following error for the Time Range option: "That value is not valid". This issue occurred if you selected Year for the time range for email reports, then viewed any web report without changing the time range. (Year is not a supported time range for web reports.) This issue no longer occurs.
81046	**Fixed: Russia Daylight Saving Time** This version of AsyncOS for Web adopts the latest timezone rules for Russia that cancel Daylight Saving Time.
81189	**Fixed: After 3 days, all Radius-authenticated users may have full access privileges** Previously, when a user authenticated using Radius was configured with any role having limited access privileges, the user receivesd appropriately-restricted access only for the first three days. After that time, all Radius-authenticated users had full Administrator-level access. (If any Radius-authenticated user logged in during the three-day window, the three-day timer was reset.)
79929	**Fixed: Colons are converted to %3A when Web Tracking results are exported as .csv file** Colons now appear properly in CSV files.
77926	**Fixed: Publishing or copying Configuration Master 6.3 may change existing Access Policies** Previously, in the 'Web Reputation and Anti-Malware Filtering' settings for Access Policies, the action for the 'Other Malware' and 'Unscannable' categories changed from Block to Monitor when you did either of the following: • Published Configuration Master 6.3 to WSA 7.1.x or 7.5.0. • Copied Configuration Master 6.3 to Configuration Master 7.1 or 7.5 These actions no longer change existing Access Policies.
75101	**Fixed: Log process memory usage to determine cause of lockups due to excessive swapping** Process memory is now logged, which will help to determine the cause of lockups that occur as a result of excessive memory swapping.

Table 6 Resolved issues in Cisco IronPort AsyncOS 7.7.1 for Security Management

Defect ID	Description
74880	**Fixed: Backups and data flow from managed appliances may stop unexpectedly, which may result in data loss** If reporting data was actively flowing from managed appliances to the Security Management appliance and either you disabled centralized reporting, or a backup was in progress, the data flow as well as any backups in progress could stop. If this situation continued unnoticed, the outgoing queues on the appliances could overflow, causing data loss. This issue has been fixed.
73469	**Fixed: Appliance sends out a non-applicable critical alert email in some cases** Previously, the appliance sent out a non-applicable critical alert email with the following message: `Counter group "MAIL_SYSTEM_CAPACITY" does not exist.` This no longer occurs.
79127	**Fixed: Appliance can run out of swap memory and lock up** Publishing configurations to Web Security appliances would cumulatively trigger this issue over time. It has now been fixed.
74058	**Fixed: Displaying reports for a custom time range longer than about 9 months results in error** Previously, the error "An error occurred while retrieving the data." occurred when viewing report data covering more than about 9-10 months. This no longer occurs.
49662	**Fixed: Application fault occurs intermittently when releasing message from End-User Quarantine** Previously, this issue occurred intermittently; it has now been fixed.

Resolved in Release 7.7.0

Table 7 Resolved Issues in Cisco IronPort AsyncOS 7.7.0 for Security Management

Defect ID	Description
83262	**Fixed: FreeBSD telnetd Remote Code Execution Vulnerability** Previously, there was a vulnerability that could have allowed a remote, unauthenticated attacker to execute arbitrary code with elevated privileges. This has now been fixed. For more information on the vulnerability, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120126-ironport
77244	**Fixed: Critical alert sent in error when previously-connected ESA or WSA is unavailable** Previously, the following critical alert was being sent when in fact no problem existed: Critical: An application fault occurred: ('authentication/remote_connect.py __str__|24', "<type 'exceptions.AttributeError'>", "'SmadConnectError' object has no attribute 'error_message'", '[_coro.pyx coro._coro._wrap1 (coro/_coro.c:8442)|757] [authentication/auth_manager.py start|62] [authentication/remote_connect.py __str__|24]') Now, no alert is sent in this situation.
80493	**Fixed: (Japanese language only) Releasing a message from spam quarantine appears to delete it** When releasing a message from the spam quarantine, the GUI incorrectly states that the message was deleted instead of released.
79501	**Fixed: Modified end-user Spam Quarantine URL can disable the end-user quarantine for all users** Previously, if an end user attempted to modify a system-generated spam quarantine URL, all subsequent spam quarantine users would receive an error when attempting to access the quarantine. This problem no longer occurs.
81246	**Fixed: (Japanese language only) "Quarantine" is mistranslated** This mistranslation has been corrected.
80678	**Fixed: Infrequent race condition could lock up Security Management appliance** When this issue occurred, the Security Management appliance stopped communicating with associated Email and Web Security appliances, and stopped responding to input via GUI and CLI.
78648	**Fixed: showconfig shows incorrect amount of memory** Previously, the showconfig command incorrectly reported 0GB of memory. The correct amount now appears, matching the amount of RAM indicated correctly by the ipcheck command.

Table 7 Resolved Issues in Cisco IronPort AsyncOS 7.7.0 for Security Management (continued)

Defect ID	Description
79474	**Fixed: URLs are shown incorrectly on the Web Tracking page if data was generated on Web Security appliance 7.1.2 or later** For data from earlier Web Security appliances, URLs in simple view appear in Web Tracking results in the Security Management appliance as "http%3A". URLs in detail view precede the URL with "http%3A". If the Web Security appliance is running AsyncOS 7.1.2 or later, the Security Management appliance must be running AsyncOS 7.2.2 or later
77616	**Fixed: (M160, M660, M670, M1060, M1070 hardware only) Changing disk space quotas requires lowering spam quarantine allocation** For some hardware models, the maximum disk space allocation for spam quarantine in AsyncOS 6.7 was larger than the maximum allocation in AsyncOS 7.x. If you had more spam quarantine data at time of upgrade than the new maximum allowed, and you changed your disk space allocations after upgrade, you had to lower the quota for spam quarantine to the new maximum, resulting in loss of spam quarantine data over the new maximum amount. In AsyncOS 7.7, this problem will not occur because the maximum disk space allocations for Spam Quarantine now match those of previous releases for all hardware models. For specific quotas, see the "Maximum Disk Space Available" section of the *Cisco IronPort AsyncOS 7.7 for Security Management User Guide*.
76790	**Fixed: If 100% of available space in Disk Management was allocated before upgrade, all available disk space is not used after upgrade** Previously, if 100% of disk space was allocated in a previous release, less than 100% of disk space was allocated after upgrade to AsyncOS 7.x. Now, 100% of available disk space will still be allocated after upgrade. Allocation reductions will be spread evenly among all services to which you have allocated space in Disk Management, except Centralized Email Tracking, which is generally reduced only if 100% of disk space is allocated to it.
71406	**Fixed: Error Occurs When Using the Default Client or Server IP Address for the packetcapture Predefined Filter** Running a packet capture that specifies the default client or server IP address for the predefined filter now works successfully. Loading a saved configuration file with these characteristics now also works.
75568, 76084	**Fixed: Local users assigned the operator, read-only operator, help desk, or guest roles can access the Spam Quarantine after their authorization is removed in the Spam Quarantine settings** This issue no longer occurs. If a user is assigned a role both locally and in an external authentication source, the locally-assigned role takes precedence.

Table 7 Resolved Issues in Cisco IronPort AsyncOS 7.7.0 for Security Management (continued)

Defect ID	Description
76295	**Fixed: Users assigned to the helpdesk role or to a custom web user role without Publish privileges can access the CLI and run 'who' command** Users assigned to these roles no longer have access to the CLI.
73611	**Fixed: Reports have no data** Previously, this issue occurred if insufficient disk space was allocated for Centralized Reporting in Management Appliance > System Administration > Disk Management. Now, if a value greater than 0 is entered, at least 5 GB is required.
71976	**Fixed: (M160 and M170 Hardware only) Disk fails with RAID alert.** Software RAID robustness has been improved, making these disk failures less likely to occur.

Service and Support

To obtain support, use one of the following methods:

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

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

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

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.