Release Notes for Cisco IronPort AsyncOS 7.9.0 for Security Management

Published: April 2, 2012

Revised: January 17, 2013

Contents

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

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

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

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

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 7.9.0-107 of AsyncOS for Security Management from the following versions:

- 6.7.6-076
- 6.7.7-202
- 7.2.0-390
- 7.2.1-036
- 7.2.2-028
- 7.2.2-106
- 7.2.2-107
- 7.7.0-204
- 7.7.0-206
- 7.7.0-210
- 7.7.1-039
- 7.8.0-564
- 7.8.0-572

SMA Compatibility Matrix

This section describes the compatibility between this release of AsyncOS for Security Management 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.

Note (For Deployments with Web Security appliances) The Web Security appliance maintains backward compatibility of its configuration data for up to two previous major versions. It is important to remember though, that any upgrade may affect Security Management appliance functionality depending on what the software versions are on the source and destination appliances.

Table 2 Security Management Appliance Compatibility with the Email Security Appliance

Version	Reporting	Tracking	SafeList/ BlockedList	ISQ
ESA 6.3	No Support	No Support	No Support	Support
ESA 6.4	Support	Support	Support	Support
ESA 6.5	Support	Support	Support	Support
ESA 7.0	Support	Support	Support	Support
ESA 7.1	Support	Support	Support	Support
ESA 7.3	Support	Support	Support	Support

Version	Reporting	Tracking	SafeList/ BlockedList	ISQ
ESA 7.5	Support	Support	Support	Support
ESA 7.6	Support	Support	Support	Support

Table 3 Security Management Appliance Compatibility with Web Security Appliances

Version	Centralized Reporting and Tracking	ICCM Publish[1]	Advanced File Publish to the Web Security appliance
WSA 5.6	Feature not Available	No support	No support
WSA 5.7	Feature not Available	No support	Configuration file version must match target WSA version.
WSA 6.0	Feature not Available	No support	No support
WSA 6.3	Feature not Available	Support on 6.3 Configuration Master	Configuration file version must match target WSA version.
WSA 7.0	Feature not Available	Support on 6.3 Configuration Master	Configuration file version must match target WSA version.
WSA 7.1	Support	Support on 6.3 and 7.1 Configuration Master	Configuration file version must match target WSA version.
WSA 7.5	Support	Support on 6.3, 7.1, and 7.5 Configuration Master Configuration Master 7.5 is strongly recommended.	Configuration file version must match target WSA version.

1. **For ICCM Publish and Advanced File Publish rows in the table, the destination for the publish is a Web Security appliance.**

Table 4 (Deployments with WSAs Only) Configuration Master Compatibility

Target Configuration Master version:	Source Configuration Master version:	Source Configuration file from Web Security appliance version:
6.3	Not applicable	Web Security appliance 6.3
7.1	Configuration Master 6.3	Web Security appliance 7.1
7.5	Configuration Master 6.3 or 7.1	Web Security appliance 7.5

Important Notes

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*.

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:

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 SMA Compatibility Matrix, page 3.

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 1-5 to determine the change that applies to your deployment.

Table 1-5 Maximum Disk Space Available for Different AsyncOS Releases and Hardware

Disk Space Available	Hardware Platform									
AsyncOS Version	**M160**	**M170**	**M600**	**M650**	**M660**	**M670**	**M1000**	**M1050**	**M1060**	**M1070**
7.9	165	165	187	187	681	681	429	429	1053	1409
7.8	180	180	186	186	450	700	405	405	800	1500
7.7	180	180	186	186	450	700	405	405	800	1500
7.2	180	180	186	186	450	700	405	405	800	1500
6.7.8	186	186	186	186	450	450	405	405	800	800
6.7.7	186	—	186	186	450	450	405	405	800	800
6.7.6	195	—	186	186	450	—	405	405	800	—

Back Up Your Existing Configuration

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

Upgrading to This 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.

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.

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

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`.

Resetting the Configuration to the Factory Default

Information in this section applies only if the Security Management appliance manages one or more Web Security appliances running AsyncOS 7.5.

If you reset the appliance configuration to the factory default, either using the web interface (**Management Appliance > System Administration > Configuration File** page) or the `resetconfig` command:

After you reset the configuration, but before you load a configuration file, add a managed Web Security appliance to the Security Management appliance and allow the URL category set to update. Otherwise, the configuration file will fail to load.

Resolved Issues

Issues Resolved in AsyncOS 7.9

Table 6 Resolved Issues in AsyncOs 7.9 for Security Management

Defect ID	Description
84035	**Fixed: Backup fails if it overlaps with Spam Quarantine purging** Previously, backup failure occurred if the backup overlapped with a spam-quarantine purge triggered when the specified quota- or time-based purge-point was reached. (The following backup was likely to occur successfully.)
72587	**Fixed: Internet Explorer 8 issues on Windows 7** Internet Explorer 8 now runs without issues on Windows 7.

Table 6 Resolved Issues in AsyncOs 7.9 for Security Management (continued)

Defect ID	Description
75846	**Fixed: Feature key checks should use the same network path as update downloads** Previously, feature key checks were sometimes was made on a network port without a route to an external destination, so the automated feature key check feature could not be used. Now, feature key checks use the same interface (data or management) that is configured for downloading updates.
72770	**Fixed: DNS alternate authority domains are case sensitive but should not be** Previously, when defining an alternate DNS authority (for which authority for a realm is delegated to an alternate host via "dnsconfig"), the DNS entry was treated case-sensitively, but this is no longer the case. Lookups now match regardless of case.
82208	**Fixed: End User Spam Quarantine stops working if a user attempts to search for 2 MBs of text** Previously, when such a search occurred, the entire page became unresponsive until the search was completed. Now, search entries are limited to 1000 characters.
72743	**Fixed: OpenSSH vulnerability could expose plain text data** Previously, a remote attacker could have recovered certain plaintext data in an SSH session by exploiting OpenSSH CBC Mode Information Disclosure Vulnerability CVE-2008-5161. This vulnerability has been fixed.
77215	**Fixed: Non-English PDFs for various reports display some text in English** In addition, text in the report email was garbled. Now, all reports should display correctly and completely in the chosen language.
78916	**Fixed: The `%days_until_expire%` variable in the quarantine notification email does not work when the default language is Spanish** Previously, when the "Spam Quarantine Settings" default language was set to Spanish, the number of days before expiration did not replace the variable in the resulting notification.
81312	**Fixed: When exporting Message Tracking data as CSV, message subjects with non-English characters are gibberish** The readable non-English subject now appears in the CSV file.

Issues Resolved in AsyncOS 7.8

Table 7 Resolved Issues in Cisco IronPort AsyncOS 7.8 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. For more information about the vulnerability, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120126-ironport
79512	**Fixed: Web Tracking may unexpectedly stop functioning** To prevent this issue, extremely long URLs are now truncated in Web Tracking. To determine the full URL, note the Web Security appliance that hosted the transaction, then check the Accesslog on that appliance.
73706	**Fixed: Web Tracking details incorrectly display a web reputation score of 10.1 for Access Policies with blocked protocols or user agents** Previously, Web Tracking details incorrectly displayed a web reputation score of 10.1 for Access Policies with blocked protocols or user agents. This no longer occurs. Now, "No score" is displayed in these cases.
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.
77926	**Fixed: Publishing or copying Configuration Master 6.3 may change existing Access Policies** 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.
80601	**Fixed: Users from group "Email Administrators" cannot log in directly to the Spam Quarantine** After upgrade, 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. Users can now log in directly to the Spam Quarantine without first signing in to the Security Management appliance.
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.

Table 7 Resolved Issues in Cisco IronPort AsyncOS 7.8 for Security Management (continued)

Defect ID	Description
81189	**Fixed: After 3 days, all Radius-authenticated users may have full access privileges** Formerly, when a Radius-authenticated user was configured with any role having limited access privileges, the user received appropriately-restricted access only for the first three days. After that time, all Radius-authenticated users had full Administrator-level access. (However, if any Radius-authenticated user logged in during the three-day window, the three-day timer was reset.) Appropriate access restrictions now persist as expected.
81310	**Fixed: Publish history detail may generate an application fault error** Formerly, this error occurred when an Identity used NTLMSSP authentication provided by a sequence, and the Web Security appliance had a sequence with that name, but that sequence did not support NTLMSSP. This could happen if you deleted or modified a realm. This issue no longer occurs.
77726	**Fixed: Web reporting in the GUI may become sluggish** Previously, response to any action performed in the web reporting pages could become very slow until appliance reboot. This issue has been fixed.
74880	**Fixed: Backups and data flow from managed appliances may stop unexpectedly, which may result in data loss** Previously, 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 have overflowed, causing data loss. Now, this situation does not occur.
74487	**Fixed: Identities on Web Security appliance are erroneously set to "No Surrogate" when Credential Encryption is disabled on the Security Management appliance** Previously, when the Web Security appliance was enabled for Credential Encryption, and the configuration master was configured to disable Credential Encryption, Identities on the Web Security appliance were erroneously set to "No Surrogate" after publishing the configuration master. The workaround is no longer needed.
77609	**Fixed: Active Sessions page and 'who' CLI command cannot identify active CLI users whose usernames contain 16 characters** Previously, neither the `who` CLI command nor the Active Sessions page identified active CLI users whose user name was 16 characters long. Now these users are identified.
74336	**Fixed: If a power loss occurs on the destination appliance while a backup is in progress, the backup cannot be restarted** Previously, the source appliance was unable to detect that the backup was no longer actually in progress and thus a new backup could not be initiated. Now, the backup can be restarted if a power loss occurs on the destination appliance.
67749	**Fixed: Initiation of multiple nearly-simultaneous immediate backup processes may be allowed** Rarely, it was possible to initiate multiple closely-overlapping immediate backups. However, in such cases, only one backup would run. Now, the option to start a backup does not appear if a backup is currently running.

Table 7 Resolved Issues in Cisco IronPort AsyncOS 7.8 for Security Management (continued)

Defect ID	Description
37034	**Fixed: The Items per Page search is not functioning properly** Previously, when you selected the number of items per page to be displayed in a report on the Security Management appliance, an incorrect number of items was displayed. Now, the specified number of items appears.
69601	**Fixed: An extra column appears on overview report when switching to Daylight Savings Time (DST)** Previously, an extra column appeared on the Web > Reporting > Overview page when you changed the time to Daylight Savings Time (DST). This no longer occurs.
72432	**Fixed: The Web Tracking Printable PDF report does not contain Related Transactions information** Previously, when you clicked the Printable PDF link from the Web > Reporting > Web Tracking page, the report did not contain the Related Transactions information. Now, the report includes this information.

Issues Resolved in AsyncOS 7.7

Table 8 Resolved Issues in Cisco IronPort AsyncOS 7.7 for Security Management

Defect ID	Description
79501	**Fixed: Modified end-user Spam Quarantine URL can disable the end-user quarantine for all users** This no longer occurs.
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.
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

Table 8 Resolved Issues in Cisco IronPort AsyncOS 7.7 for Security Management (continued)

Defect ID	Description
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.
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.

Table 8 Resolved Issues in Cisco IronPort AsyncOS 7.7 for Security Management (continued)

Defect ID	Description
71976	**Fixed: (M160 Hardware only) Disk fails with RAID alert** Software RAID robustness has been improved, making these disk failures less likely to occur.

Known Issues

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

Table 9 Known Issues for Release 7.9

Defect ID	Description
86777	**Importing a Web Security appliance configuration file to Configuration Master 7.5 may fail** Importing a configuration file saved from AsyncOS 7.5.0-727 gives the following error: "Web Configuration File was not imported. Parse Error on element "wccp_debug_level" line number 4335 column 23 with value "5": Value must be an integer from 0 to 4." Workaround: Manually update the "wccp_debug_level" from "5" to "4". Save the configuration file and import the changed file.
84881	**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.
85059	**Error when importing a configuration file to a Configuration Master or using Advanced File Publish** This error occurs when managing Web Security appliances running AsyncOS 7.5.0. Importing a configuration file from AsyncOS 7.5.0 to a Configuration Master, or publishing a configuration to AsyncOS 7.5.0 using Advanced File Publish, will fail with the following error: `"Failure: ERROR: Element 'prox_etc_send_size' not allowed here at Unknown:3272:25 Text: 262144"` Workaround: Upgrade your Web Security appliance to a build later than 7.5.0-703. The build number appears in the Upgrade Paths section of the Release Notes for each release.
84778	**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.

Table 9 Known Issues for Release 7.9 (continued)

Defect ID	Description
84595	**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.
83979	**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	**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.

Table 10 Known Issues for Release 7.8

Defect ID	Description
81115	**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.
78045	**Compatibility issues with configuration files from AsyncOS 7.1.2 or 7.1.3 for Web** Advanced file publish cannot be used to publish a configuration file from AsyncOS 7.1.2 or 7.1.3 for Web to Web Security appliances running AsyncOS 7.1.0 or 7.1.1.
76201	**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

You can request our support by phone, email, or online 24 hours a day, 7 days a week.

During customer support hours (24 hours per day, Monday through Friday excluding U.S. holidays), an engineer will contact you within an hour of your request.

To report a critical issue that requires urgent assistance outside of our office hours, please contact IronPort using one of the following methods:

U.S. toll-free: 1(877) 641- 4766

International: `http://cisco.com/web/ironport/contacts.html`

Support Portal: `http://cisco.com/web/ironport/index.html`

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2012-2013 Cisco Systems, Inc. All rights reserved.