Release Notes for Cisco IronPort AsyncOS 7.8 for Security Management

Published: June 14, 2012

Revised: October 14, 2013 (Added additional upgrade path)

Contents

This document contains information for Cisco IronPort AsyncOS 7.8 for Security Management. This document includes the following sections:

What's New in Cisco IronPort AsyncOS 7.8 for Security Management

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

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 7.5 for Web Security at http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html.

Table 1 New Features for AsyncOS 7.8 for Security Management

Feature	Description
New Features:	
Support for new Web Security features	A new Configuration Master 7.5 supports new features in Cisco IronPort AsyncOS 7.5 for Web Security, including: • Transparent User Identification for Microsoft Active Directory • Adaptive Scanning (automatic selection of the most effective anti-malware tool for the situation) • Automatic updates to the set of URL categories used with Cisco IronPort Web Usage Controls For information about these features, see the Release Notes for Cisco IronPort AsyncOS 7.5 for Web Security. You will configure these features in the new Configuration Master the same way that you configure them in the Web Security appliance.
User preferences	Each user of the Security Management appliance can now specify language, landing page, and default report settings for time range and number of table rows to display.
Log rollover at specified time	You can now specify a time for logs to roll over.
Enhancements:	
Enhanced: L4 Traffic Monitor reporting and tracking	These enhancements improve your ability to determine whether blocking a site or a port is the more effective solution to a particular malware problem, or whether to take action specific to a particular client IP address that is at unusually high risk. • You can view a list of top client IP addresses accessing malware sites, and filter these results by port. • You can filter top malware sites by port. • You can click the data in a table in the report to view details for a suspect site, port, or client IP address. • You can perform multi-dimensional searches for malware risk areas, for example by hostname and port.
Enhanced: Backups	• You can now schedule multiple future backups and recurring backups at times and intervals that you choose. • You can back up just the features that you specify. • Backup information is now logged separately in a Backup Log to make it easier to locate, and backup start and end times are now logged.
Enhanced: Warning for triggers of proxy restart	When you publish configuration changes that will cause a Web Security proxy server restart, thus interrupting service to end-users, you now see a warning so that you can choose to make this change at a time of lower impact.

Table 1 New Features for AsyncOS 7.8 for Security Management (continued)

Feature	Description
Enhanced: Web reporting pages	Ability to choose which data to display as a graph for each report.
Enhanced: Web User Interface Protection	AsyncOS 7.8 for Security Management includes additional protection from cross-site request forgeries (CSRF) and other attacks on the web user interface.
Enhanced: Performance	Reporting data now appears more quickly than previously.

Upgrade Paths

You can upgrade to release 7.8.0-572 of AsyncOS for Security Management from the following versions:

6.x	7.2.x	7.7.x	7.8.x
• 6.7.3-229 • 6.7.6-076 • 6.7.7-202 • 6.7.8-009	• 7.2.0-390 • 7.2.1-036 • 7.2.2-028 • 7.2.2-106 • 7.2.2-107	• 7.7.0-202 • 7.7.0-204 • 7.7.0-206	• 7.8.0-564

SMA Compatibility Matrix

- Compatibility with Email Security Appliances, page 3
- Compatibility with Web Security Appliances, page 4

Compatibility with Email Security Appliances

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

- 7.1.5
- 7.5.1
- 7.5.2

Compatibility with Web Security Appliances

- Security Management Appliance Compatibility with Web Security Appliances
- Configuration Master Compatibility

Table 2 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 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 exactly 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 exactly 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 3 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

- AsyncOS 7.8 for Security Management Does Not Support FIPS, page 4
- Web Reporting and Tracking Data Availability for L4TM and Client Malware Risk, page 5

AsyncOS 7.8 for Security Management Does Not Support FIPS

Note that although AsyncOS 7.5 for Web supports FIPS, this release of the Security Management appliance does not support FIPS.

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 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 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 7.8 for Security Management User Guide*.

Installation and Upgrade Notes

- Important Information for Upgrades, page 5
- Preupgrade Requirements, page 6
- Upgrading to the AsyncOS 7.8 Release, page 7
- After Upgrading, page 8

Important Information for Upgrades

- End-of-Life Announcement, page 5
- Changes in Behavior, page 5

End-of-Life Announcement

Cisco has announced end-of-life for the IronPort URL Filters service, replacing it with Cisco IronPort Web Usage Controls. For more information about this migration, see: http://www.cisco.com/web/ironport/docs/IronPort_URL_Filtering_EoL.pdf.

After migration, you must edit Identities and policies in your Configuration Masters to use the new URL categories.

Changes in Behavior

- Changes to the Set of URL Categories Used in Policies and Identities, page 5
- Mobile User Security Feature is Renamed, page 6
- Supported Browsers, page 6

Changes to the Set of URL Categories Used in Policies and Identities

For deployments currently using Cisco IronPort Web Usage Controls:

The set of URL categories used in policies and Identities has changed in AsyncOS 7.5 for Web and AsyncOS 7.8 for Security Management. These changes are described in the Release Notes for AsyncOS 7.5 for Web.

For information about how these changes affect the Security Management appliance and for actions you should take, see all sections under "URL Category Set Updates and Centralized Configuration Management" in the "Managing Web Appliances" chapter in the *Cisco IronPort AsyncOS 7.8 for Security Management User Guide*.

Mobile User Security Feature is Renamed

Mobile User Security is now called AnyConnect Secure Mobility.

Supported Browsers

Support for Internet Explorer 6 has been dropped in this release. Supported browsers are listed in the "Browser Requirements" section in the "Setup, Installation, and Basic Configuration" chapter of the *Cisco IronPort AsyncOS 7.8 for Security Management User Guide*.

Preupgrade Requirements

Perform the following important preupgrade tasks:

- Verify Associated Email and Web Security Appliance Versions, page 6
- Prepare for Disk Space Reduction (M160 Hardware Only), page 6
- Back Up Your Existing Configuration, page 7
- Preserve Configuration Master 5.7 Settings, page 7
- Unassign Appliances From Configuration Master 5.7, page 7

Verify Associated Email and Web Security Appliance Versions

Before upgrading to AsyncOS 7.8, 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.

Prepare for Disk Space Reduction (M160 Hardware Only)

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

Table 4 Total Maximum Disk Space on M160 (continued)

Release	Total Maximum Disk Space in GB
AsyncOS 7.7	180
AsyncOS 7.8	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.

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 7.8 for Security Management User Guide*.

Preserve Configuration Master 5.7 Settings

Configuration Master 5.7 is not supported in this release and will be removed after upgrade. If you wish to preserve the settings in Configuration Master 5.7: Before you upgrade, copy your 5.7 configuration into Configuration Master 6.3. If necessary, first copy your 6.3 configuration into Configuration Master 7.1.

Unassign Appliances From Configuration Master 5.7

Configuration Master 5.7 is not supported in this release. If you have a Configuration Master 5.7 on your existing Security Management appliance, you cannot upgrade until you have unassigned all Web Security appliances from Configuration Master 5.7. Before you upgrade, preserve your Configuration Master 5.7 settings by importing them into Configuration Master 6.3. If your existing Security Management appliance already has a Configuration Master 6.3, first import the existing Configuration Master 6.3 settings into Configuration Master 7.1, then import the 5.7 settings into Configuration Master 6.3.

Upgrading to the AsyncOS 7.8 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 you see "Hard Drive Firmware upgrade (for C/M/S160 models only, build 002)" listed as an upgrade option, 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*.

To upgrade to AsyncOS 7.8 for Security Management:

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.

After Upgrading

If you are using centralized configuration management:

When you configure the new Configuration Master 7.5 to support the new features in AsyncOS 7.5 for Web, you must also enable the new features on the Security Services Display page. For more information, see information about enabling features in the “Managing Web Security Appliances” chapter in the *Cisco IronPort AsyncOS 7.8 for Security Management User Guide*.

Documentation Updates

Please note the following changes to the *Cisco IronPort AsyncOS 7.8 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`.

Resolved Issues

- Issues Resolved in AsyncOS 7.8, page 9
- Issues Resolved in AsyncOS 7.7, page 12

Issues Resolved in AsyncOS 7.8

Table 5 Resolved Issues in Cisco IronPort AsyncOS 7.8 for Security Management

Defect ID	Description
84905	**Fixed: Critical Application Fault after unsuccessful Configuration Master publish** Previously, application faults could occur when clicking Identities or Access policies in Configuration Master 7.5 after an unsuccessful publish.
85307	**Fixed: Loading a configuration file fails after reverting to AsyncOS 7.8.0-564** If the Security Management appliance manages one or more Web Security appliances running AsyncOS 7.5, a workaround was required in order to load a configuration file after reverting. The workaround is no longer required.
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.
83075	**Fixed: Web Tracking Search query generates out of memory error when tracking data contains large amounts of data** Previously, searching Web Tracking data generated an out of memory error when the tracking data contained large amounts of data. This no longer occurs. Now, when you click the Related Transactions link, the web interface displays up to 500 transaction and displays "[Omitted]" when it omits transactions. Also, extremely long URLs are truncated to 1000 characters, and "[truncated]" in the displayed URL.
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

Table 5 Resolved Issues in Cisco IronPort AsyncOS 7.8 for Security Management (continued)

Defect ID	Description
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	**(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.
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.

Table 5 Resolved Issues in Cisco IronPort AsyncOS 7.8 for Security Management (continued)

Defect ID	Description
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.
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.

Table 5 Resolved Issues in Cisco IronPort AsyncOS 7.8 for Security Management (continued)

Defect ID	Description
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 6 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
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*.

Table 6 Resolved Issues in Cisco IronPort AsyncOS 7.7 for Security Management (continued)

Defect ID	Description
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.
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 7 Known Issues for Release 7.8

Defect ID	Description
87193	**Remote Access page always shows "Not Connected" for tunnel status** If you have enabled an SSH tunnel for tech support access, the status of that tunnel is not reflected on the Remote Access page. Workaround: CLI shows correct status.
86558	**Appliance cannot establish a secure support tunnel when the appliance is not configured with working DNS settings.** The appliance does not try to connect using IP address when a secure support tunnel connection attempt using hostname fails. Workaround: Make sure the secure tunnel hostname is DNS resolvable.
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.
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.
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.
84035	**Backup fails if it overlaps with Spam Quarantine purging** Backup failure occurs if the backup overlaps with a spam-quarantine purge triggered when the specified quota- or time-based purge-point is reached. However, the next backup is likely to occur successfully.
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.

Table 7 *Known Issues for Release 7.8*

Defect ID	Description
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`

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.