Release Notes for *Cisco IronPort AsyncOS 7.3 for Email*

Published: September 17, 2010

OL-23626-01

Contents

These release notes contain information critical to upgrading and running Cisco IronPort AsyncOS 7.3 for Email, including hardware-specific information and known issues.

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

What's New in Cisco IronPort AsyncOS 7.3 for Email

This section describes the new features added in the Cisco IronPort AsyncOS 7.3 for Email release.

New Feature: FIPS Compliance

AsyncOS for Email 7.3 provides support for the Cisco IronPort Email Security appliance with a FIPS-compliant Hardware Security Module (HSM) card.

The Federal Information Processing Standard (FIPS) 140 is a publicly announced standard developed jointly by the United States and Canadian federal governments specifying requirements for cryptographic modules that are used by all government agencies to protect sensitive but unclassified information. The HSM offered with the Cisco IronPort C670 Email Security appliance is the CAVIUM Nitrox XL CN15xx-NFBE Cryptographic Module, which complies with the FIPS 140-2 Level 2 standard. This standard specifies additional protections for information used in cryptographic operations, including the use of a tamper-resistant hardware keystore for private keys.

The HSM card provides cryptographic processing for the appliance as well as storage for private keys. All cryptographic operations take place within the secure environment of the HSM card.

When the Email Security appliance includes the HSM card and uses AsyncOS 7.3, it offloads all cryptographic operations to the HSM card in a FIPS-compliant manner. AsyncOS for Email 7.3 also provides a FIPS management console to allow a FIPS Officer to configure the HSM card to manage certificates and private keys.

Software Notes

Please be aware of the following software impacts:

Security Management Appliances That Are Not FIPS Compliant

While you can use a Security Management appliance that does not have an HSM card to provide centralized services for an Email Security appliance running AsyncOS 7.3, this may bring the Email Security appliance's HSM card out of FIPS compliance.

FIPS Officer Password

To manage certificate/key pairs and signing keys on the Email Security appliance's HSM card, you must log into the Email Security appliance as an administrator and then provide the FIPS Officer password. You need the FIPS Officer password to access the FIPS Management console or to use the `fipsconfig` CLI command.

Warning **AsyncOS for Email keeps track of the total number of failed login attempts to the HSM card using the FIPS Officer password. On the third subsequent login failure, the HSM card is initialized, which clears its contents. There is no timeout between failed login attempts. Because the HSM card gets initialized, it loses the certificate and key for accessing the appliance web interface. If the HSM card initializes after the third unsuccessful login attempt, the browser displays a generic error message that it cannot display the web page.**

There is no way to retrieve the FIPS Officer password once it is set. If you forget the FIPS Officer password, the only way to access the HSM card is to initialize it, which wipes all certificates and keys it manages.

Configuration Files

When you save the appliance configuration to a file using AsyncOS 7.3, the certificate and keys that the HSM card manages are not included in the configuration file. Also, if you restore the appliance configuration from a file that erroneously includes certificate and key information, AsyncOS 7.3 ignores the certificate and key information in the file.

To back up the certificates and keys the HSM card manages:

Step 1 From the FIPS Mode menu, choose FIPS Backup/Restore.

The Backup and Restore page is displayed.

Step 2 Under the Backup Certificates and Keys section, choose the file name to use for the XML file that will contain the encrypted certificate and key pairs. You can define your own file name or AsyncOS can choose one for you.

Step 3 Click **Backup**.

Step 4 Choose to save the file, and click OK.

Navigate to the directory on the local machine to where you want to save the XML file, and click **Save**.

Note IronPort does not support the backward compatibility of configuration files with previous major releases.

Committing Changes in AsyncOS 7.3

When you log into the FIPS Management console, AysncOS automatically commits any uncommitted changes to the system. All changes accepted in the FIPS Management console are automatically committed.

Console Serial Port Timeout

If you are accessing an Email Security appliance running AsyncOS 7.3 via a serial connection, the session times out 30 minutes after the connection to the Serial Console port is terminated.

Security Management Appliances Discard Reporting Data for DLP and Marketing Mail

IronPort Security Management appliances running AsyncOS 6.7.3 or earlier do not support reporting data for the DLP and Marketing Mail features in AsyncOS 7.0 or later. If your IronPort Email Security appliance uses centralized reporting, the Security Management appliance discards the reporting data for those features.

If the Security Management appliance is running AsyncOS 6.7.0 or 6.7.3, it sends an alert once each time the reporting service begins, such as on a reboot, stating that the reporting service is receiving data that it cannot process.

Your Security Management appliance must be running AsyncOS 6.7.6 or later in order to use centralized reporting for the DLP and Marketing Mail features.

Email Authentication

For DKIM Authentication, IronPort currently supports version 8 of the Draft Specification of 'Authentication-Results:' header.

For SPF/SIDF verification, the `spf-passed` rule is no longer available in content filters. To maintain backwards compatibility, the `spf-passed` content filter rule will be accepted from XML configuration files but it will be converted to the `spf-status` rule with corresponding arguments. `spf-passed` will be changed to `spf-status == "Pass"` and NOT spf-passed to `spf-status != "Pass"`. You can, however, still use the `spf-passed` message filter.

Received Headers

When you configure AsyncOS to use received headers, you can specify that the header reflects one of the following hostnames:

- The hostname of the Virtual Gateway used for delivering the message
- The hostname of the interface the message is received on

You specify the hostname from the CLI command `listenerconfig-> setup`. You cannot configure the hostname from the GUI.

If you configure the received header to display the hostname of the interface the message is received on, a `strip-header` filter action configured to strip received headers will strip the received header inserted by AsyncOS. [Defect IDs: 16254, 25816]

Feature Keys

The AsyncOS appliance checks for and applies feature keys at one minute intervals. Therefore, when you add a feature key, it may take up to a minute to view the changes. [Defect ID: 29160]

Upgrading to the AsyncOS 7.3 Release

Appliances cannot be upgraded to the AsyncOS 7.3 for Email release.

Performance Advisory

RSA Email DLP - Enabling RSA Email DLP for outbound traffic on an appliance that is also running anti-spam and anti-virus scanning on inbound traffic can cause a performance decrease of less than 10%. Appliances that are only running outbound messages and are not running anti-spam and anti-virus may experience a significant performance decline.

DomainKeys - DomainKeys signing outgoing email can cause a decrease in the message throughput capacity.

SBNP - SenderBase Network Participation now uses the Context Adaptive Scanning Engine (CASE) to collect data to power IronPort Information Services. In some configurations customers may experience a moderate performance decline.

Virus Outbreak Filters - Virus Outbreak Filters now uses the Context Adaptive Scanning Engine to determine the threat level of a message and scores messages based on a combination of Adaptive Rules and Outbreak Rules. In some configurations, you may experience a moderate performance decline.

IronPort Spam Quarantine - Enabling the IronPort Spam Quarantine on-box for a C-Series or X-Series appliance causes a minimal reduction in system throughput for nominally loaded appliances. For appliances that are running near or at peak throughput, the additional load from an active quarantine may cause a throughput reduction of 10-20%. If your system is at or near capacity, and you desire to use the IronPort Spam Quarantine, consider migrating to a larger C-Series appliance or an M-Series appliance.

If you change your anti-spam policy from dropping spam to quarantining it (either on-box or off-box), then your system load will increase due to the need to scan additional spam messages for virus and content security. For assistance in properly sizing your installation please contact your authorized IronPort support provider.

Upgrade Paths

Version 7.3.0-051 is the AsyncOS 7.3 release of the Cisco IronPort AsyncOS for Email operating system.

There are no qualified upgrade paths to this release.

Fixed Issues

The following issues have been fixed in the AsyncOS 7.3 for Email release.

Table 1 Resolved Issues in Version 7.3

Defect ID	Description
71552	**Extra Spaces in DKIM Signature Causes App Fault.** Fixed an issue where several extra spaces in the `d` tag of a DKIM signature would cause an app fault.
70739	**Trailing Space in alt-mailhost Parameters for Policy or Filter Causes App Fault.** Previously, if any extra spaces were entered via in the alt-mailhost parameters for a policy or filter via the GUI, any messages that hit the policy or filter would cause an app fault and potentially the message would be lost. This issue has been resolved.
71151	**Internal Users Summary Report Causes App Fault When Run Over 200 Days.** Fixed an issue where running an Internal Users Summary Report over a range of more than 200 days caused an app fault.

Table 1 Resolved Issues in Version 7.3 (continued)

Defect ID	Description
69829	**Emails Exceeding the Maximum Size Do Not Timeout Properly.** Previously, there was an issue where the timeout for messages does not work properly if the message is larger than the configured maximum message size. A response wouldn't be sent back to the send and the logs incorrectly indicated that no data was sent. This issue has been resolved.
71152	**Loading a Configuration file from Previous Appliance to a C670, or X1070 Takes It Offline After Reboot.** Fixed an issue where a C670 or X1070 appliance that had configuration files imported from a previous generation IronPort appliance, such as a X1060 or C660, would go offline after a reboot. Please note that Cisco IronPort does not support the loading of a configuration file from one appliance model to another.
67137	**Messages Bounce If an LDAP Server in Chained Masquerade Query is Unreachable.** Previously, if you had a chained masquerade LDAP query configured and the second LDAP server was unreachable, the message was stuck in the queue in a partially masqueraded state. When the second LDAP server started to respond again, the appliance bounced any partially masqueraded messages stuck in the queue. This issue has been resolved.
55972	**TLS/SSL Man-in-the-Middle Vulnerability.** Previously, an industry-wide vulnerability that existed in the TLS protocol potentially impacted any Cisco product using any version of TLS /SSL. The vulnerability existed in how the protocol handles session re-negotiation and exposed users to a potential Man-in-the-middle attack. This issue has been fixed.
70522 55358	**DKIM Signing and Verification Create Memory Leak.** Fixed an issue where DKIM signing and verification created large amounts of unclaimed data in the appliance's RAM, which could have resulted in the appliance running out of memory.
69429	**CASE No Longer Updates After Hitting a Timeout.** Previously, AsyncOS stopped attempting to update the Context Adaptive Scanning Engine (CASE) after hitting an update timeout. No more CASE updates would arrive, even after trying to force an update via the CLI. This issue has been resolved. AsyncOS will continue to do further updates to CASE after a timeout.

Known Issues

The following list describes known issues in this release of AsyncOS for Email.

Clustering Issues

Table 2 Clustering Issues

Defect ID	Description
71712	**CLI Displays Host Key Error Messages During Cluster Creation.** When creating a cluster of appliances running AsyncOS 7.3, the CLI displays error messages stating that the `/etc/ssh/ssh_host_key.pub` and `/etc/ssh/ssh_host_dsa_key.pub` system host keys cannot be opened. These host keys listed do not exist on the appliance. Cisco IronPort advises you to ignore these error messages.
68368	**Reconnect Link in GUI Does Not Reconnect Machines.** The "reconnect" link in the GUI does not reconnect machines that were disconnected from a cluster unless the machines were disconnected from the cluster individually. Workaround: Use the `clusterconfig -> reconnect` command in the CLI to reconnect the machines.

DLP Issues

Table 3 DLP Issues

Defect ID	Description
68556	**Renaming Encryption Profile Doesn't Update DLP Policy.** If you rename an encryption profile that is being used by a DLP policy, AsyncOS does not automatically update the DLP policy with the updated encryption profile name. AsyncOS will bounce messages that match the DLP profile.

LDAP Issues

Table 4 DLP Issues

Defect ID	Description
71610	**Critical LDAP Alert Sent After Creating an LDAP Profile.** The Email Security appliance sometimes sends a critical alert after the user creates an LDAP profile using a configuration file. There is no loss in functionality when this occurs.

Other Issues

Table 5 Other Issues

Defect ID	Description
72144	**Connection Not Redirecting to HTTPS After Initialization.** Some SSH clients and web browsers automatically lose the SSH or HTTPS connection when the HSM initializes or when the wrong password is entered three times. If a user enters the wrong password three times via SSH, attempting to log back into the appliance via HTTP will result in an error message because the connection will not redirect to HTTPS. In these cases, the administrator must manually reboot the appliance by powering it off and on.
71994	**Host Key Cannot Be Updated For Individual Logs via the GUI.** Instead of updating the SSH host key for SCP push for an individual log, manually entering an SSH host key using a log subscription's GUI page actually updates the host key for all logs which are configured to SCP push to the given host.

Related Documentation

The documentation for the Cisco IronPort Email Security appliance includes the following books:

- *Cisco IronPort AsyncOS for Email Daily Management Guide*. This guide provides instructions for performing common, everyday tasks that system administrators use to manage and monitor the IronPort appliance, such as viewing email traffic using the Email Security Monitor, tracking email messages, managing system quarantines, and troubleshooting the appliance. It also provides reference information for features that system administrators interact with on a regular basis, including Email Security Monitor pages, AsyncOS logs, CLI support commands, and quarantines.
- *Cisco IronPort AsyncOS for Email Configuration Guide*. This guide is recommended for system administrators who are setting up a new IronPort appliance and want to learn about its email delivery features. It provides instructions on installing the appliance into an existing network infrastructure and setting it up as an email gateway appliance. It also includes reference information and configuration instructions for email delivery features such as the Email Pipeline, Virus Outbreak Filters, content filters, DLP, email encryption, anti-virus scanning, and anti-spam scanning.
- *Cisco IronPort AsyncOS for Email Advanced Configuration Guide*. This guide provides instructions configuring the advanced features of the IronPort appliance. Topics include configuring the appliance to work with LDAP, managing FIPS, creating message filters to enforce email policies, organizing multiple appliances into clusters, and customizing the listeners on the appliance. In addition to configuration, this guide provides reference material for advanced features such as message filter rules and actions, regular expressions used in content dictionaries and message filter rules, and LDAP query syntax and attributes.
- *IronPort AsyncOS CLI Reference Guide*. This guide provides a detailed list of the commands in the AsyncOS command line interface (CLI), as well as examples of the commands in use. System administrators can use this guide for reference when using the CLI on the IronPort appliance.

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 Cisco 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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.