Release Notes for *Cisco IronPort AsyncOS 7.0.1 for Email Security*

Revised: February 3, 2010, 423-0090 (B)

Contents

These release notes contain information critical to upgrading and running AsyncOS 7.0.1, 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 AysncOS 7.0.1* for Email Security

Fixed Issues

The following issues have been fixed in this release of AsyncOS 7.0.1.

- Fixed: Reporting Engine Stops Allocating Memory, Stops Processing Data, and Causes an Application Fault When the Housekeeper Thread Stops [Defect ID: 52048]

  Previously, the reporting engine stopped allocating memory, stopped processing data, and caused an application fault when the housekeeper thread stopped. This issue has been resolved.

- Fixed: Italian Translation Errors [Defect ID: 56181]

  Fixed Italian translation errors in the AsyncOS user interface.

- Fixed: TLS/SSL Man-in-the-Middle Vulnerability [Defect ID: 55972]

  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.

What's New in *Cisco IronPort AsyncOS 7.0 for Email Security*

New Feature: RSA Email Data Loss Prevention

New in AsyncOS 7.0, your IronPort Email Security appliance now secures your organization's data by providing the DLP scanning engine and email DLP policy templates from RSA Security, Inc. By enabling RSA Email DLP, your IronPort appliance allows you to protect your organization's sensitive information and enforce regulatory compliance and internal policies by preventing users from unintentionally emailing sensitive data. You can define what kind of data is allowed to be emailed by your employees.

The RSA Email DLP feature includes predefined DLP policy templates and content matching classifiers designed by RSA Security, Inc. AsyncOS 7.0 also includes a new set of reports for monitoring DLP incidents.

The RSA Email DLP feature is supported on all C-Series and X-Series appliances, except for the C10, C30, C60, C100, C300D, C350D, and C360D appliances.

New Feature: Unwanted Marketing Message Detection

In AsyncOS 7.0, IronPort Anti-Spam can distinguish between spam and marketing mail from a legitimate source. Even though marketing mail is not considered spam, your organization or end-users may not want to receive it. AsyncOS 7.0 provides the same actions for marketing mail that it does for spam.

Enhanced: Prioritized SMTP Routes

AsyncOS 7.0 allows you to prioritize the destination hosts for your SMTP routes. AsyncOS will attempt to deliver the message to a destination host in order based on priority. Destinations with identical priority will be used in a "round-robin" fashion.

Enhanced: Encryption Enhancements

AsyncOS 7.0 provides the following enhancements to IronPort Email Encryption:

- **Guaranteed Secure Delivery.** In content filters and DLP policies, you can set up your appliance to first attempt to send a message over a TLS connection before sending it encrypted, depending on the TLS settings in a domain's destination controls.
- **Encrypt on Delivery.** Content filters now have an option to encrypt a message on delivery. The message continues to the next stage of processing, allowing the appliance to scan the message at each stage of the workqueue before encrypting it.

- **Encrypt on Quarantine Exit.** The Quarantined Message page displays information on whether or not a message will be encrypted upon release from the quarantine due to the Encrypt on Delivery filter action.
- **Encryption Multi-Envelope Branding.** You can configure multiple encryption profiles for a hosted key service. If your organization has multiple brands, this allows you to reference different logos stored on the key server for the PXE envelopes.
- **PXE Engine Updates.** You can configure the IronPort appliance to automatically update the PXE engine using the Security Services > Service Updates page.

Enhanced: RADIUS Groups and Protocols for External Authentication

AsyncOS 7.0 allows you to assign user roles to groups in your RADIUS directory. You can also specify whether the appliance uses Password Authentication Protocol or Challenge Handshake Authentication Protocol to communicate with a RADIUS server.

Enhanced: Quarantined Message Attachments Enhancements

AsyncOS 7.0 provides the following enhancements for quarantined messages:

- You can download a message attachment by clicking the attachment's file name in the Matched Content or Message Parts section of Quarantine Message page. AsyncOS warns you of possible viruses when downloading a quarantined attachment.
- You can also download the message body by clicking `[message body]` in the Message Parts section of the Quarantine Message page.
- The Quarantine Message page displays the Image Analysis score for inappropriate image attachments.

Installation Notes

Preupgrade Notes

Please be aware of the following upgrade impacts:

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. 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.

Maximum Scanning Size Increases

AsyncOS 7.0 increases the maximum scanning size for message attachments to 25 MB. Use the `scanconfig` command to set the maximum scanning size.

Space Available for System Quarantines Increases

AsyncOS 7.0 increases the amount of storage space available for system quarantines. The following table displays the space available in AsyncOS 7.0 and previous versions.

Table 1-1 Comparison of Space Available for Quarantines on IronPort Appliances

IronPort Appliance	AsyncOS 6.5 Storage Space	AsyncOS 7.0 Storage Space
X1000/1050/1060	5GB	10GB
C600/650/660	5GB	10GB

Table 1-1 Comparison of Space Available for Quarantines on IronPort Appliances

IronPort Appliance	AsyncOS 6.5 Storage Space	AsyncOS 7.0 Storage Space
C300/350/360	2GB	4GB
C150/160	1GB	2.5GB

For more information on quarantine storage space, see the "Quarantines" chapter in the *IronPort AsyncOS for Email Daily Management Guide*.

New Scanned File Types for Attachments

AsyncOS 7.0 includes new file types for attachment scanning. The following file types have been added:

Attachment Group Name	Scanned File Types
Text	• `txt` • `html` • `xml`
Media	• `wma` • `wmv`

Re-enable SNMP

SNMP does not start when you boot the appliance after upgrading to AsyncOS 7.0. Use `snmpconfig` to enable it.

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.

Configuration Files

IronPort does not generally support the backward compatibility of configuration files with previous major releases. Minor release support is provided. Configuration files from previous versions may work with later releases; however, they may require modification to load. Check with IronPort Customer Support if you have any questions about configuration file support.

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 7.0.1 Release

For the AsyncOS 7.0.1 release, please use the following instructions to upgrade your Email Security appliance.

Step 1 Save the XML configuration file off the IronPort appliance.

Step 2 If you are using the Safelist/Blocklist feature, export the Safelist/Blocklist database off the IronPort appliance.

Step 3 Suspend all listeners.

Step 4 Wait for the queue to empty.

Step 5 From the System Administration tab, select the System Upgrade page.

Step 6 Click the **Available Upgrades** button. The page refreshes with a list of available AsyncOS upgrade versions.

Step 7 Click the **Begin Upgrade** button and your upgrade will begin. Answer the questions as they appear.

Step 8 When the upgrade is complete, click the **Reboot Now** button to reboot your IronPort appliance.

Step 9 Resume all listeners.

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. Using smaller signing keys (512 byte or 768 byte) can mitigate this.

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 7.0.1-010 is the AsyncOS 7.0.1 release of the IronPort AsyncOS for Email Security operating system.

The qualified upgrade paths to this release are:

- From: Version 6.5.1-005 To: Version 7.0.1-010.
- From: Version 6.5.2-101 To: Version 7.0.1-010.
- From: Version 6.5.3-007 To: Version 7.0.1-010.
- From: Version 6.5.3-009 To: Version 7.0.1-010.
- From: Version 6.5.3-013 To: Version 7.0.1-010.
- From: Version 6.5.3-014 To: Version 7.0.1-010.
- From: Version 6.6.0-202 To: Version 7.0.1-010.
- From: Version 6.6.1-016 To: Version 7.0.1-010.
- From: Version 7.0.0-702 To: Version 7.0.1-010.
- From: Version 7.0.1-009 To: Version 7.0.1-010.

Fixed Issues

The following issues have been fixed in this release of AsyncOS 7.0.

- Fixed: DKIM Does Not Use Sender: Header to Check Against Domain Profile [Defect ID: 43272]

Previously, for email authentication using DKIM, the IronPort Email Security appliance checked outbound messages for a From: header to see if a matching domain profile exists for DKIM signing. The appliance only used the Sender: header for DomainKeys profiles, not DKIM signing. Now, the IronPort appliance can use the Sender: header for DKIM signing.

- Fixed: $filenames and $filetypes Variables Return Confusing Information [Defect ID: 42391 and 51841]

  Fixed an issue where the `$filenames` and `$filetypes` variables returned inconsistent and confusing information for archive types such as .tar.gz, .zoo, and .ear. Now, the variables return the names of files and file types stored in the MIME structure of the archive.

- Fixed: Exported IP Address Search Results for Incoming Mail Shows “Last Sender Group” Twice [Defect ID: 43218]

  Fixed an issue where exporting IP address search results from the Incoming Mail page to a CVS report resulted in the “Last Sender Group” being displayed in the report twice.

- Fixed: IronPort Spam Quarantine Authentication Fails for Queries Configured to Use LDAP Referrals in Active Directory [Defect ID: 42011]

  Previously, when using an LDAP referral for an Active Directory server, the IronPort Spam Quarantine authentication query failed to bind the password and the query fails. This issue only occurred when performing authentication queries using LDAP referrals in Active Directory. This issue has been resolved.

- Fixed: The IronPort Spam Quarantine GUI Does Not Highlight Matched Content Containing Spaces [Defect ID: 44356]

  Previously, the IronPort Spam Quarantine GUI did not highlight certain content matched by the “ssn” Smart Identifier. This appeared to occur only when the matched nine-digit string contained spaces. This issue has been resolved.

- Fixed: Message Filters Cannot Reference Interface Groups for Clustered Appliances [Defect ID: 43467]

  Previously, in a clustered environment, message filters could not reference an IP interface group configured on the appliances. Message filters that referenced IP interface groups were automatically marked as invalid. This issue has been resolved.

- Fixed: Service Updates Page Displays Local Server URL After Changing to IronPort Update Servers [Defect ID: 45036]

  Previously, if you changed the appliance's service update settings from using a local server for updates to the IronPort Update Servers, the Service Updates page continued to display the local server for updates after submitting the changes. This issue has been resolved. Now, the Service Updates page displays "IronPort Update Servers" after submitting the changes.

- Fixed: Revert Does Not Reset Configuration Settings to the Default Values [Defect ID: 47153]

  Previously, user-defined settings were not reset to the predefined values if you reverted to a previous qualified build of AsyncOS for Security Management. This issue has been resolved.

- Fixed: TLS Connections Graph Does Not Include Unencrypted Connections to "TLS Preferred" Domains [Defect ID: 45792]

  Previously, AsyncOS did not report any message sent over an unencrypted connection to a recipient domain with a TLS delivery setting of "Preferred" or "Preferred (Verify)" in the "Outgoing TLS Connections Graph" and "Outgoing TLS Connections Summary" graphs.

  AsyncOS did report the unencrypted connection in the "Outgoing TLS Messages Summary" graph. This issue has been resolved.

Known Issues

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

DLP Issues

- Invalid Regular Expressions Halt RSA Email DLP Scanning [Defect ID: 67002]

  Entering an invalid regular expression for a RSA Email DLP policy causes an app fault that halts DLP scanning even if the regular expression is later corrected. While the AsyncOS GUI validates regular expressions, it may not catch all errors. There are two known regular expression errors that can cause this app fault:

  - the repeat construct, which is represented as brackets (`{}`), if the brackets are empty or contain something other than a single number or two numbers separated by a comma, and
  - a regular expression begins or ends with the "or" construct, which is represented as a vertical bar (`|`).

  Workaround: Fix the invalid regular expression and reboot the Email Security appliance.

- RSA Email DLP Performance

  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.

- False Positives with "Transmission of Contact Information" DLP Policy [Defect ID: 55289]

  A message signature containing the sender's contact information can result in a false positive from the "Transmission of Contact Information" DLP policy if a reply to the original message resulted in the sender's information appearing multiple times in the message body. Workaround: Adjust the policy's severity scale to increase the number of matches before triggering the policy's actions.

Reporting Issues

- Security Management Appliances Discard Reporting Data for DLP, Intelligent Multi-Scan 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. 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.

- The Email Security Monitor Overview Page Incorrectly Counts Quarantine Mails as “Virus” [Defect ID: 51960]

  When calculating the number of virus-positive messages, the Email Security Monitor Overview page includes messages that were quarantined by the anti-virus scanning engine due to the message being unscannable or encrypted. These messages are not included in the virus-positive report on the Virus Types pages.

LDAP Issues

- LDAP Test Query in Domain Assignment Fails If One or More Servers Defined in Domain Assignments Is Unreachable [Defect ID: 52308]

  When you run the test query from the Domain Assignment page, the query may erroneously tests other servers defined from the Domain Assignments page. If any server defined in the Domain Assignments page is unreachable, the query may fail.

- One or More Unavailable LDAP Servers Can Cause a Chain Query to Fail [Defect ID: 52444]

  One or more unavailable LDAP servers in a chain can cause the chain query to fail.

External Authentication Issues

- AsyncOS Does Not Support Multiple RADIUS Class Attributes [Defect ID: 49096]

  Currently, AsyncOS supports only one RADIUS class attribute per user. If a user has more than one class attribute defined, AsyncOS provides the user access to the GUI based on the first RADIUS class attribute only. Ensure that you carefully configure the RADIUS server to define the user's group in the first RADIUS class attribute.

- CLI Does Not Support Usernames Longer Than 16 Characters for Local and External Authentication [Defect ID: 49909]

  Currently, the CLI does not support usernames containing 17 characters or more. Workaround: Use a shorter username, or enter the username in the GUI, which has no such limitation if external authentication is configured.

- External Authentication Fails if the Group Name Contain Special Characters [Defect ID: 51185]

  External Active Directory LDAP users cannot long into the IronPort Email Security appliance if they belong to an LDAP group that has one of the following special characters in the group name: `# " < > , + \ ;`. Active Directory escapes these characters by prepending backslashes (\). This issue also affects LDAP group queries.

  Workaround: Manually escape these characters during configuration by adding the backslash character (\) before the special character. For example, if the LDAP group name is #Admin, enter `\#Admin` when mapping LDAP groups in AsyncOS.

Message Tracking Issues

- GUI Sometimes Displays Fewer Query Results Per Page Than Expected [Defect IDs: 55066, 37034]

  When you perform a query, sometimes the GUI displays fewer results per page than expected. For example, if you select to view 50 items of your query results per page, the GUI may display only 20 per page, even though the page may say "Displaying 1-50 of 120 items."

- Message Tracking Details Page Displays Masking Backslashes in Content Matching Classifiers Containing Single Quotation Marks [Defect ID: 52407]

  The DLP Matched Content tab on the Message Tracking Details page erroneously displays masking backslashes preceding single quotation marks in content matching classifiers. For example, `"b'lad"e '''"2"`' appears as `"b\'lad"e\'\'\'"2"\'`. Workaround: Use double quotation marks instead of single quotation marks in content matching classifiers.

Text Resources Issues

- Importing and Exporting Dictionaries Does Not Preserve the Match Whole Words and Case Sensitive Options [Defect ID: 54997]

  AsyncOS does not preserve the Match whole words and Case sensitive options when importing or exporting dictionaries. The dictionary file only includes a list of terms.

- Editing a Large Content Dictionary From the GUI Causes Browser to Hang [Defect ID: 51884]

  Attempting to edit a content dictionary that is larger than the recommended five thousand term limit from the GUI may sometimes cause the browser to hang.

  Workaround: If your content dictionary is larger than the five thousand term limit, export the file, edit it, and import it again from the CLI. Do not edit larger files in the GUI.

Other Known Issues

- Sender Groups Accept Whitespace as a Valid “ALL” Sender [Defect ID: 52355]

  The AsyncOS GUI accepts whitespace as a valid sender group name and commits it as an ALL sender group. This sender group cannot be deleted from the GUI. Workaround: You can delete the sender group from the CLI, as well as export, edit, and import the HAT.

- DKIM Only Uses “From” Header for Lookup [Defect ID: 43272]

In a previous release DKIM used only “From” address and never used “Sender” address to lookup for DKIM profile and subsequently for the signing key lookup. You now have the ability to use value “Sender:” header use for DKIM signing of the message.

- Non-ASCII Subject Displays as Plain Text on the Message Details Page [Defect ID: 37156]

  A non-ASCII subject displays as plain text on the Message Details page when you perform message tracking. This causes the subject to appear unreadable.

- Application Fault Occurs When Switching Cluster Levels in Encryption Profile [Defect ID: 55874]

  An application fault occurs when switching between different cluster levels on the Encryption Profile page in the GUI. Workaround: Change the cluster level in the CLI.

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, 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, 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 IronPort using one of the following methods:

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

International: `www.ironport.com/support/contact_support.html`

Support Portal: `www.ironport.com/support`

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

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.

♻ Printed in the USA on recycled paper containing 10% postconsumer waste.