Release Notes for *Cisco IronPort AsyncOS 7.1.5 for Email Release*

Revised: January 16, 2013

Note This release ships on certain hardware.

Contents

These release notes contain information critical to upgrading and running Cisco IronPort AsyncOS 7.1.5 for Email, including hardware-specific information and known issues.

What's New in Cisco IronPort AsyncOS 7.1.5 for Email

This section describes the new features and resolved issues in the Cisco IronPort AsyncOS 7.1.5 for Email release.

New License Agreement

The IronPort End User License Agreement has been replaced by the Supplemental End User License Agreement for Cisco Systems Email and Web Security Software.

Because the license agreement has changed, you may be required to accept the new agreement when you apply new feature keys after upgrading.

A copy of the new license agreement is included in the Online Help. To view it, choose **Help and Support > Online Help**, scroll down to the end of the the Contents list, and click the link for the license agreement.

Fixed Issues

Table 1   ***Resolved Issues in Version 7.1.5***

Defect ID	Description
83262	**Fixed: FreeBSD *telnetd* Remote Code Execution Vulnerability**
	This hot patch fixes a vulnerability in the Cisco IronPort Email Security appliance that could have allowed a remote, unauthenticated attacker to execute arbitrary code with elevated privileges.
	For more information on the vulnerability, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-2012 0126-ironport
81754	**Fixed: TLS Traffic Causing Email Processing to Restart or Become Unresponsive**
	The DigiNotar blacklist solution added in the previous 7.5.1 hot patch contained a defect that resulted in the email process restarting or becoming unresponsive due to certain types of TLS traffic. This issue has been resolved and the email process errors no longer occurs.
80810	**Fixed: Email Security appliance trusts DigiNotar as a root certificate authority**
	Previously, the Email Security appliance trusted DigiNotar as a root certificate authority. It also trusted DigiNotar's intermediate certificates issued by the State of Netherlands. This no longer occurs. The Email Security appliance no longer includes DigiNotar in the list of trusted certificate authorities. It has also blacklisted DigiNotar's intermediate certificates.
22164	**Fixed: Regular Expression that Exceeds Data Limit Invalidates Message Filter**
	Previously, if certain data caused a failure when evaluating a message filter's regular expression, an application fault occurred and the message filter became invalidated. This issue has been resolved. Now, the appliance skips the message filter for that message without invalidating the filter for subsequent messages.
74473	**Fixed: version Command Displays RAID Type as 'NA'**
	Fixed an issue where the `version` command would display the RAID type as `NA` due to improper RAID controller parsing heuristics. This issue affects the following areas: • CLI: the `version` command didn't display the correct RAID volume state. • SNMP: would mark all disks down at boot and fire notifications for all disks, due to an invalid state change.

Table 1   Resolved Issues in Version 7.1.5

Defect ID	Description
51946	**Fixed: LDAP Masquerade Query Cannot Process To: Headers that Do Not Conform to RFC 2047** Previously, an LDAP masquerade query would not be able to process a message with a non-English "To:" header where the email address is also encoded and does not conform to RFC 2047. The message would get stuck in the queue. This issue has been resolved. Now, the appliance decodes and re-encodes a non-compliant To: header and performs the correct LDAP masquerade query.
75798	**Fixed: End User Quarantine Always Uses Demo Certificate for LDAP Connections** Fixed an issue where the End User Quarantine always used the Demo Certificate for LDAP connections instead of the certificate that the user configured the appliance to use for LDAP connections.
72606	**Fixed: Excessive Memory Usage When Archiving Large Unscannable Messages** Previously, the appliance would run out of memory when it attempted to archive a very large message that could not be scanned by the anti-virus scanning engine. This issue has been resolved.
55358	**Fixed: Excessive Unclaimed Memory After DKIM Signing and Verification** Previously. the appliance would have unclaimed memory after performing DKIM signing or verification. Appliances performing frequent DKIM signing and verification would eventually run out of memory. This issue has been solved.
74972	**Fixed: Quarantined Messages with Older than Hard Bounce Timeout May be Bounced When Released** Previously, messages that stay in a system quarantine longer than the timeout for hard bounces would be bounced if the destination server was not available when a message was released. The appliance also bounced an older message if the destination queue had more than 5000 messages, even if the destination server was available. This issue has been resolved.
76664	**Fixed: Reporting Goes Out of Operation Due to Resources Leak** Fixed an issue where the Reporting feature goes out of operation due to a resources leak on the appliance when a report query errors out. The appliance would incorrectly display an error message stating that the maximum number of concurrent queries has been exceeded when this issue occurred.

Table 1   *Resolved Issues in Version 7.1.5*

Defect ID	Description
76292	**Fixed: STARTTLS Vulnerability**
	Previously, an industry-wide vulnerability that existed in the STARTTLS implementation in some versions of Postfix had the potential for impacting Email Security appliances under certain circumstances. This issue has been resolved.
76277	**Fixed: findevent Command Does Not Show Some Message ID Logs**
	Previously, when using the `findevent` command to display Message ID logs in the CLI, the command would not display a log if there is a colon after `MID <number>` in the log, yet the `grep` command would display the log. For example, the `findevent` command would not display the following log:
	`Wed Mar  9 21:39:44 2011 Warning: MID 55555555: scanning error (name=somewordfile.doc', type=document/doc): file is corrupt` The command `grep "MID 55555555" mail_logs`, however, would display this log. This issue has been resolved.
70598	**Fixed: Message Filter Does Not Modify Some Headers Properly**
	Fixed an issue where a message filter designed to modify message headers did not modify structured message headers such as To: and From: correctly. Mail user agents like Outlook, Thunderbird, Gmail, and Yahoo Mail could not decode these headers. This issue has been resolved.
72623	**Fixed: Message in End User Quarantine Displays Incorrect Date**
	Fixed an issue where occasionally a message in the end user quarantine would display the wrong age when you poll an appliance for the oldest messages in the end user quarantine.
76304	**Fixed: LDAP Failover Not Working**
	Fixed an issue where the LDAP failover functionality was not working when one of the LDAP servers was down.
31279	**Fixed: NIC Pairing and VLAN Not Supported by Packet Capture Feature**
	The Packet Capture feature in AsyncOS 7.1.5 now supports NIC Pairing and VLAN when configuring the feature using the CLI or GUI.

Table 1   *Resolved Issues in Version 7.1.5*

Defect ID	Description
49407	**Fixed: Message Tracking Not Updated for Time Zone Change** Previously, changing the time zone for an appliance did not update the time zone information for Message Tracking. Message Tracking continued to use times relative to the older time zone when performing searches. This issue has been resolved.
72684	**Fixed: netstat Command Restricts View of non-inet Interface** AsyncOS 7.1.5 removes the `-f inet` restriction built into the CLI's `netstat` command, allowing the user to view information on non-inet interfaces.
74547	**Fixed: Scanning Engine Restarts If It Exceeds Memory Limit** The content scanning engine in AsyncOS 7.1.5 for Email improved performance from previous versions but it would run out of memory when scanning certain types of vCard attachments. When it reached its memory limit, the engine restarted and the message and its attachment continued through the work queue. This issue has been resolved.

What's New in *Cisco IronPort AsyncOS 7.1.3 for Email*

This section describes the enhancements and resolved issues in the Cisco IronPort AsyncOS 7.1.3 for Email release.

Enhancement: New $AV_INFECTED_PARTS Variable for Anti-Virus Notifications

This release adds a new variable to the Anti-virus Notification Template: Infected Parts List (`$AV_INFECTED_PARTS`). This variable returns a comma-separated list of filenames for the files that contained a virus. To create an anti-virus notification template using the GUI, go to Mail Policies > Text Resources and click Add Text Resource. When creating the notification, select Anti-Virus Notification Template as the type of text resource.

For more instructions on creating a custom anti-virus notification template, see Anti-Virus Notifications in the Text Resources chapter of the *Cisco IronPort AsyncOS for Email Configuration Guide*.

This release also adds all of the anti-virus-related variables to the Notification Template used by content filters. The following variables can now be used in notifications:

- $AV_VIRUSES
- $AV_VIRUS_TABLE
- $AV_VERDICT
- $AV_DROPPED_TABLE
- $AV_REPAIRED_VIRUSES
- $AV_REPAIRED_TABLE
- $AV_DROPPED_PARTS
- $AV_REPAIRED_PARTS
- $AV_ENCRYPTED_PARTS
- $AV_UNSCANNABLE_PARTS
- $AV_INFECTED_PARTS

Fixed Issues

Table 2   *Resolved Issues in Version 7.1.3*

Defect ID	Description
73455	**Fixed: IP Address Logged for Successful and Unsuccessful Logins** AsyncOS 7.1.3 for Email now records a user's IP address for successful and unsuccessful system login attempts in the authentication log.
49958	**Fixed: Alert Sent When Oldest Log Record is Deleted** AsyncOS 7.1.3 adds an option to log subscriptions that sends an Information-level System alert when log records are removed due to the maximum number of records being exceeded. This option appears when creating or editing log subscriptions via the `logconfig` command in the CLI, and it can only be used with the FTP Poll retrieval method. This option cannot be set in the GUI.

Table 2   ***Resolved Issues in Version 7.1.3***

Defect ID	Description
72023	**Fixed: Messages Larger than Maximum Allowed Size Cause Excessive Memory Usage**
	The appliance more efficiently clears out memory used by messages exceeding the maximum allowed size. In addition, the order of the log lines have changed to ensure that oversized messages are always logged.
72006	**Fixed: CLI List of Certificates Incorrectly Shows Invalid Certificate**
	Previously, if you attempted to update an existing certificate in the CLI with a public certificate that did not match the private key, the CLI correctly displayed an error message but incorrectly displayed the invalid certificate in the list of the appliance's certificates. If you made any other changes without exiting the `certconfig` command, the system committed the invalid certificate and an application fault would occur the next time you ran the `certconfig` command. This issue has been resolved.
68903	**Fixed: DKIM z= Tag Signing Could Create a Header Too Long For RFC Compliance**
	Previously, when using the z= tag with DKIM signing, multiple recipients could cause the DKIM header to exceed the maximum length allowed by SMTP RFC. This could cause delivery issues. This issue has been resolved. The z= tag is now turned off by default.
71241	**Fixed: Multipart/Alternative Messages Result in Double DLP Score**
	Previously, when RSA Email DLP scanned a multipart/alternative type message, such as HTML messages with a alternative/plain text part, the system combined the classifier scores of both parts of the message to create the DLP score. This could result in a message that should have a "low severity" score to be rated as high or medium severity. This issue has been resolved.
72656	**Fixed: Messages with From Header Split Over Two Lines Cannot Be Encrypted**
	Fixed an issue where a message cannot be encrypted if its From header is split over two lines.
72708	**Fixed: Email Scanning Engine Hangs Up While Trying to Decode Invalid UTF-32 Data**
	Fixed an issue where the Email Scanning Engine would crash when attempting to process malformed UTF-32 payloads.

Table 2   *Resolved Issues in Version 7.1.3*

Defect ID	Description
69584	**Fixed: App Fault Occurs After Appliance with Centralized Reporting Enabled Starts Up** When the Email Security appliance starts up, it performs a scan for corrupted files. Previously, if the appliance had centralized reporting enabled, it was possible for an exception to occur due to the corruption scan not recognizing timestamp files and deleting them. This issue has been resolved. The corruption scan no longer deletes these timestamp files.
70468	**Fixed: Attachment Filenames Decrypted Incorrectly When the Filename is Split Across Multiple Words** Fixed an issue where the filename of an encrypted message's attachment was decoded incorrectly due to the filename being composed of multiple words. The decoded filename would contain an extra space. This could result in applications being unable to open the file. The filename now decodes correctly.
70111	**Fixed: SNMP Process Causes High CPU Usage** Fixed an issue where SNMP wasn't properly dealing with failover communicating with AsyncOS, creating 100% CPU usage scenarios.

What's New in *Cisco IronPort AsyncOS 7.1.2 for Email*

This section describes the issues resolved in the Cisco IronPort AsyncOS 7.1.2 for Email release.

Fixed Issues

Table 3   ***Resolved Issues in Version 7.1.2***

Defect ID	Description
71552	**Fixed: 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	**Fixed: 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.
69797	**Fixed: Generation of Virus Outbreak Filters Report When Virus Outbreak Filters is Disabled Causes App Fault**
	Previously, the user could generate a Virus Outbreak Filters report even if Virus Outbreak Filters were not enabled on the appliance. Doing so would result in an app fault. The Virus Outbreak Filters report was added during the System Setup Wizard. This issue has been resolved. If Virus Outbreak Filters are not enable on the appliance, the user cannot create a report for the feature during the System Setup Wizard.
70185	**Fixed: Submit Button Not Working When Using Message Tags in Email DLP Policy with IE 7 or 8**
	Previously, when creating an Email DLP policy using Internet Explorer 7 or 8, specifying a message tag for the policy would cause the **Submit** button not to work properly. Clicking the button failed to submit the Email DLP policy. This issue has been resolved.
55558	**Fixed: Non-ASCII Character in Recipient Address Causes App Fault**
	Fixed an issue where a non-ASCII character in the envelope recipient address caused an app fault.
71151	**Fixed: 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 3   Resolved Issues in Version 7.1.2 (continued)

Defect ID	Description
69829	**Fixed: 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.
69573	**Fixed: SSL Protocol Modified via sslconfig Does Not Take Effect** In versions 7.1.0 and 7.1.1, the Email Security appliance did not use the SSL protocol for mail delivery specified using the `sslconfig` CLI command. It continued to use the default protocol. This issue has been resolved.
71152	**Fixed: Loading a Configuration file from Previous Appliance to a C370, C670, or X1070 Takes It Offline After Reboot** Fixed an issue where a C370, C670, or X1070 appliance that had configuration files imported from a previous generation IronPort appliance, such as a C360 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	**Fixed: 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.

What's New in *Cisco IronPort AsyncOS 7.1.1 for Email*

This section describes the new features and enhancements added in the Cisco IronPort AsyncOS 7.1.1 for Email release.

Enhancement: New RSA Email DLP Policy Templates

AsyncOS 7.1.1 includes two new RSA Email DLP policy templates:

- **Massachusetts CMR-201**. Policies based on this template identify documents and transmissions that contain personally identifiable information regulated by Massachusetts CMR-201. Any person who owns, licenses, stores or maintains personal information about a resident of the Commonwealth of Massachusetts is required to protect against unauthorized access to or use of the information in a manner that creates risk of identity theft or fraud. The policy detects US Social Security numbers, global credit card numbers and US drivers license numbers.

- **Corporate Financials**. Policies based on this template identify documents and transmissions that contain financial information related to organizational accounting such as balance sheets, cash flow, income statements, key ratios, SEC information, and annual, quarterly, and transition reports.

Fixed Issues

The following issues have been fixed in the AsyncOS 7.1.1 for Email release.

Table 4   ***Resolved Issues in Version 7.1.1***

Defect ID	Description
68955	**Fixed: Robustness Fixes for Lockups on C160 Appliances** AsyncOS 7.1.1 includes a series of robustness fixes and logging enhancements to address lockups that have occurred on C160 appliances.
67312	**Fixed: Extra Spaces in Footer When Forwarding via Outlook** Fixed an issue where extra line spaces were inserted into footer text when emails were forwarded using Outlook

Table 4   *Resolved Issues in Version 7.1.1 (continued)*

Defect ID	Description
69456	**Fixed: Demo Certificate Becomes Default TLS Certificate After Upgrading** Previously, the Cisco Appliance Demo certificate became the default TLS certificate for LDAP, HTTPS, destination controls, and all listeners after upgrading the Email Security appliance to AsyncOS 7.1. This issue has been resolved. Custom certificates are not changed during the upgrade.
68615	**Fixed: Email Processing Delay When Trying to Drop Viral Attachments When Using McAfee** In AsyncOS 7.0 and 7.1, certain specific viral email attachments could cause delays in mail processing and queue backup issues, which could eventually lead to corruption of the email queue, if the appliance's mail policies used McAfee anti-virus scanning and the "Drop infected attachments if a virus is found and it could not be repair" option was enabled. This issue was resolved in AsyncOS 7.1.1.

What's New in *Cisco IronPort AsyncOS 7.1 for Email*

This section describes the new features and enhancements added in the Cisco IronPort AsyncOS 7.1 for Email release.

Enhancement: DLP Assessment Wizard

AsyncOS 7.1 provides a browser-based DLP Assessment Wizard to guide you through the three-step process of configuring popular DLP policies and enabling them in the default outgoing mail policy.

Enhancement: TLS Enhancements

AsyncOS 7.1 provides a number of enhancements to the TLS features on the Email Security appliance:

- **Certificates Management**. You can use the GUI and CLI to add trusted public certificates and create a self-signed certificate. You can also use the appliance to generate a certificate signing request.

- **Certificate Authorities Management.** You can import a custom list of trusted certificate authorities onto the appliance, as well as disable and export the default system list.

- **TLS per Listener.** You can assign a unique certificate per listener on the appliance for TLS connections. You can also assign a certificate to the HTTPS services on an IP interface, the LDAP interface, and all outgoing TLS connections.

- **Batch Management.** You can import and export a Destination Controls configuration file that defines multiple destination domains using the GUI and CLI.

- **Troubleshooting Tools.** AsyncOS 7.1 provides new troubleshooting tools for TLS:

  - The `hoststatus` command has been enhanced to display the reason why the last outgoing TLS connection failed.

  - The `tlsverify` command has been added to create a TLS connection on demand. This allows an administrator to pinpoint the exact step a TLS connection failure occurs.

  - AsyncOS 7.1 records information on why a TLS connection attempt failed in the mail logs.

New Feature: Administrative Access Control List

In AsyncOS 7.1, you can control from which IP addresses users access the Email Security appliance. Users can access the appliance from any machine with an IP address from an access list you define. You can create the list using the GUI or the `adminaccessconfig > ipaccess` command in the CLI.

New Feature: Login Banner

AsyncOS 7.1 allows you to display a customizable message called a "login banner" when a user attempts to log into the Email Security appliance through SSH, Telnet, FTP, or Web UI. The login banner appears above the login prompt in the CLI and to the right of the login prompt in the GUI. The login banner can only be created using the `adminaccessconfig > banner` command.

Enhancement: No Authentication Encryption Envelope

In AsyncOS 7.1 adds the option of a No Password Required security level to encryption profiles. This is the lowest level of encrypted message security. The recipient does not need to enter a password to open the encrypted message, but the read receipts, Secure Reply, Secure Reply All, and Secure Message Forwarding features will be unavailable to prevent another email user from sending a message on behalf of the original recipient.

Enhancement: Packet Capture

AsyncOS 7.1 provides packet capture controls. The packet capture feature provides the ability to intercept and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached. This feature can help you debug the network setup and to discover what network traffic is reaching the appliance or leaving the appliance. A `packetcapture` command has also been added to the CLI.

Enhancement: Rescan Messages Released from Outbreak Quarantine

AsyncOS 7.1 includes an enhancement to the Virus Outbreak Filters feature. If the appliance has the Virus Outbreak Filters feature and either the IronPort Anti-Spam or Intelligent Multi-Scan feature, the anti-spam filter scans every message released from the Outbreak quarantine based on the mail flow policy that applies to the message. A message released from the Outbreak quarantine may be sent to the IronPort Spam Quarantine if it discovered to be spam, suspected spam, or a marketing message.

Enhancement: Suspend and Resume Mail Operations in the GUI

AsyncOS 7.1 now allows you to suspend and resume message receiving and delivery in the GUI using the Shutdown/Suspend page (formerly the Shutdown/Reboot page) under the System Administration menu.

New Feature: signed-certificate() Filter Rule

The `signed-certificate` rule selects those S/MIME messages where the X.509 certificate issuer or message signer matches the given regular expression. This rule only supports X.509 certificates.

Enhancement: Unpacking Opaque-Signed Messages

The `scanconfig` CLI command now includes an option to convert the application/(x-)pkcs7-mime (opaque-signed) parts of a message to a multipart/signed (clear-signed) MIME entity in order to allow the IronPort Email Security appliance to scan the message's content.

Enhancement: Retry Delivery in the GUI

In AsyncOS 7.1, messages that are scheduled for later delivery can now be immediately retried by clicking the **Retry All Delivery** button on the Delivery Status page in the GUI. Retry All Delivery allows you to reschedule messages in the queue for immediate delivery. All domains that are marked down and any scheduled or soft bounced messages are queued for immediate delivery.

Enhancement: New Message and Content Filter Actions

AsyncOS 7.1 adds two new message and content filter actions:

- **Add Log Entry.** This new message and content filter action inserts customized text into the IronPort Text Mail logs at the INFO level. The text can include action variables. The log entry also appears in message tracking.

- **Add Message Tag.** This new message and content filter action inserts a custom term into a message to use with RSA Email DLP policy filtering. You can configure a RSA Email DLP policy to limit scanning to messages with the message tag. The message tag is not visible to recipients.

Enhancement: New SPF Control Options in the CLI

The AsyncOS 7.1 CLI supports new control settings for each SPF/SIDF conformance level. Based on the SPF/SIDF verdict, you now have the ability to accept or reject a message, in SMTP conversation, on a per listener basis. You can modify the SPF/SIDF settings when editing the default settings for a listener's Host Access Table using the `listenerconfig` command.

Installation Notes

Preupgrade Notes

Please be aware of the following upgrade impacts:

Hard Drive Firmware Upgrade for C160 Required Before Upgrading to AsyncOS 7.1.3

When you begin upgrading your C160 to AsyncOS 7.1.3, the appliance first checks for the Cisco IronPort Hard Drive Firmware Upgrade. If the firmware upgrade is pending, appliance prompts you to complete it prior to upgrading your C160 to AsyncOS 7.1.3. This firmware upgrade fixes a bug in the driver controller code on the hard drives used on C160 appliances that sometimes caused requests to timeout in certain conditions, which resulted in errors or the drive going offline. [Defect ID: 73406]

See the *Cisco IronPort Hard Driver Firmware Upgrade for C160, S160, and M160 Appliances Release Notes* on the Cisco.com support site for more information.

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.

Re-enable SNMP

SNMP does not start when you boot the appliance after upgrading to AsyncOS 7.1.1. Use `snmpconfig -> setup` and then `commit` 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. AsyncOS 7.1 does not support configuration files from AsyncOS 7.0.1 or earlier.

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 7.1.3 Release

For the AsyncOS 7.1.3 release, please use the following instructions to upgrade your Email Security appliance.

✎ **Note** If your C160 appliance does not have the latest hard drive firmware upgrade, you will be prompted to upgrade the firmware before upgrading to AysncOS 7.1.3. See Hard Drive Firmware Upgrade for C160 Required Before Upgrading to AsyncOS 7.1.3, page 17 for more information.

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

You cannot upgrade to release 7.1.5-102 from any previous version.

Fixed Issues

The following issues have been fixed in the AsyncOS 7.1 for Email release.

Table 5   ***Resolved Issues in Version 7.1***

Defect ID	Description
67002	**Fixed: Invalid Regular Expressions Halt RSA Email DLP Scanning** Previously, entering an invalid regular expression for a RSA Email DLP policy caused an application fault that halted DLP scanning even if the regular expression was later corrected. While the AsyncOS GUI validates regular expressions, it may not catch all errors. There were two known regular expression errors that could cause this application 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 (`|`). This issue has been resolved. The AsyncOS GUI now tests for the above regular expression errors.
52407	**Fixed: Message Tracking Details Page Displays Masking Backslashes in Content Matching Classifiers Containing Single Quotation Marks** Previously, 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"\'`. This issue has been resolved.

Table 5   Resolved Issues in Version 7.1 (continued)

Defect ID	Description
55874	**Fixed: Application Fault Occurs When Switching Cluster Levels in Encryption Profile** Previously, an application fault occurred when switching between different cluster levels on the Encryption Profile page in the GUI. This issue has been resolved.
37164	**Fixed: Corrupted Uuencoded Content Results in Warning and Skipped Filters** Previously, a message with a corrupted uuencoded attachment caused the Email Security appliance to skip message filters processing and record a warning in the mail logs. This issue has been resolved. Now, the appliance applies filters to messages with corrupted uuencoded content.

Known Issues

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

Anti-Virus Issues

Table 6   Anti-Virus Issues

Defect ID	Description
68899	**Sophos Anti-Virus Unable to Scan PDFs with Large Cross-Reference Tables** The most recent Sophos anti-virus scanning engine imposes a maximum limit to the number of entries in a PDF's cross-reference tables to avoid malformed files from using too much memory. The scanning engine returns "unscannable" for PDFs that exceed the maximum limit even if they are not malformed. Cisco IronPort is working with Sophos to resolve this issue in a future Sophos engine update.
77059	**Messages Altered by AsyncOS are Unscannable by Sophos** AsyncOS sometimes cleans bare CR and LF characters from messages, which results in Sophos flagging the messages as unscannable.

Clustering Issues

Table 7 *Clustering Issues*

Defect ID	Description
67341	**Cannot Save Regional Settings for IronPort Anti-Spam and IMS for Clustered Appliance** You cannot save changes to the Regional Settings for IronPort Ant-Spam or IronPort Intelligent Multi-Scan via the GUI when a clustered Email Security appliance is in cluster or group mode. Workaround: Set the Regional Settings for IronPort Anti-Spam or IMS using the CLI instead of the GUI.
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.
68527	**Misleading Message When Trying to Run DLP Assessment Wizard in Cluster Mode** The DLP Assessment Wizard cannot be run in a clustered environment. However, if you attempt to run the wizard when logged into a clustered appliance in any mode other than the login host mode, AsyncOS displays an error message stating that the wizard is only available in login host mode. If you switch to login host mode, AsyncOS displays an error message stating that the DLP Assessment Wizard cannot be run on a clustered machine. The machine must be removed from the cluster in order to run the wizard.

DLP Issues

Table 8   *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 Issue

Table 9   *DLP Issues*

Defect ID	Description
69838	**LDAP Doesn't Renew Connection After Certificate is Removed from Appliance** The Email Security appliance does not renew its connection to the LDAP server if the security certificate assigned to the LDAP interface is removed from the appliance after the connection was established. Workaround: Reboot the Email Security appliance to release the connection.
71610, 38606	**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.

Upgrading Issues

Table 10   *Upgrading Issues*

Defect ID	Description
74035	**Switching to the CLI after a Failed Upgrade in the GUI Could Result in an App Fault** If you attempt to upgrade your ESA appliance to AsyncOS 7.1.3 using the GUI and the upgrade attempt fails, attempting to upgrade the appliance again through using the upgrade command in the CLI may result in an application fault. You should try the upgrade again using the GUI.
66543	**Message Tracking Does Not Display Any Message Details After Upgrading and Changing the Time Zone** After upgrading the appliance to AsyncOS 7.0.1 or later and changing the time zone on the appliance, the Message Tracking page does not display any details when you click Show Details for a message. All message details values are blank or NA. Workaround: Use the Printable PDF option to view the message details.
67160	**Non-Default Administrator Can Reset Configuration Using System Setup Wizard** Any user assigned to the administrator user role can run the System Setup Wizard and reset the appliance's configuration. Only the admin user is expected to be able to run the System Setup Wizard.
68278	**Internet Explorer 7 Displays Error Messages for System Upgrade Page** When you open the System Upgrade page in Internet Explorer 7, IE7 displays an "Object Required" error in the status bar at the bottom of the browser window. If you select a version of AsyncOS and click Begin Upgrade, AsyncOS displays an "Upgrade failure" error message, but AsyncOS is actually upgrading the appliance and displays the upgrade progress below the error message. Workaround: Ignore the error messages and continue with the upgrade.

Other Issues

Table 11   *Other Issues*

Defect ID	Description
68337	**AsyncOS Saves Exported PKCS#12 Certificate with .cer Extension**
	When exporting a PKCS#12 certificate from the Certificates > Export Certificate page in the GUI, AsyncOS saves the certificate with the .cer extension instead of .p12.
71854	**Reboot Required to Show Message Tracking Data After resetconfig**
	No results are shown in Message Tracking after running `resetconfig` on an Email Security appliance running AsyncOS 7.1.2 for Email and using `loadconfig` to load a configuration file. To work around this issue, reboot the appliance. All message tracking details will appear correctly after the reboot.
71991	**Incorrect Certificate Warning Appears When Editing an IP Interface**
	When editing an IP interface that does not have custom certificates, the Email Security appliance incorrectly displays a warning message saying that the `https_cert` certificate does not exist anymore. This warning does not show after committing your changes. This issue occurs only after upgrading to version 7.1.2.
73306	**text/rfc822-headers Caused Scanning Engine to Time Out**
	The presence of text/rfc822-headers in a message may cause the message scanning engine to time out.
80539	**Incorrect Encryption File Size Information in Configuration Guide**
	The information in the Maximum Message Size for Encryption table in the AsyncOS for Email Configuration Guide is incorrect and should be ignored.

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, 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2011 Cisco Systems, Inc. All rights reserved.

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