Release Notes for Cisco IronPort AsyncOS 7.6.3 for Email

Revised: August 6, 2013

Contents

This document contains release information for Cisco IronPort AsyncOS 7.6.3 for the Email Security appliance, and includes the following sections:

What's New

This section describes the new features and enhancements that are introduced in Cisco IronPort AsyncOS 7.6 for Email releases.

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

Cisco IronPort AsyncOS 7.6.3 for Email

Enhancement: Reusable DLP Custom Classifiers

Prior to AsyncOS 7.6.3, a DLP custom classifier can only be created as part of a custom DLP policy and cannot be reused in other custom DLP policies. After upgrading to AsyncOS 7.6.3, you can:

- Create reusable DLP custom classifiers that can be used across multiple DLP policies.
- Reuse the previously configured DLP custom classifiers in other DLP policies.

After the upgrade, previously configured custom classifiers will be listed on the DLP Policy Customizations page. You can use this page to view, edit, or delete previously configured custom classifiers or add new custom classifiers. This page can be accessed by clicking **Mail Policies > DLP Policy Customizations**.

You cannot delete the DLP custom classifiers that are currently being used by a DLP policy. You must first remove the DLP custom classifier from all DLP policies that are using it before AsyncOS allows you to delete it.

Note The Delete button for any DLP custom classifiers that are currently being used by a DLP policy is disabled.

Cisco IronPort AsyncOS 7.6 for Email

New Feature: IPv6 Support

AsyncOS 7.6 adds Internet Protocol Version 6 (IPv6) address compatibility to your Email Security appliance. You can use both IPv4 and IPv6 addresses for your appliance's IP interfaces. IPv6 addresses are also an option for the following features:

- Gateways (default routers) and static routes.
- SMTP routes.
- SMTP Call Ahead.
- Trace.
- Senders for Host Access Tables.
- Recipients for Recipient Access Tables.
- Content Filter's Remote IP condition and Send to Alternate Destination Host action.
- Destination Controls, where you can specify whether IPv4 or IPv6 addresses are preferred.
- Outbreak Filters' Bypass Domain Scanning field.
- Report searches.

AsyncOS supports the following formats for IPv6 addresses:

- `2620:101:2004:4202::0-2620:101:2004:4202::ff`
- `2620:101:2004:4202::`
- `2620:101:2004:4202::23`
- `2620:101:2004:4202::/64`

New Feature: RSA Enterprise Manager Integration

AsyncOS 7.6's RSA Enterprise Manager Integration allows your organization to migrate an Email Security appliance's Data Loss Prevention policies to RSA Security's Enterprise Manager software in order to distribute those policies to all of your vectors enforcement. With RSA Enterprise Manager Integration, you can ensure consistent DLP policies across your enterprise and still have the option to manage policies on a local Email Security appliance when needed. For users of RSA's DLP Datacenter, RSA Enterprise Manager Integration also provides fingerprinting detection for scanning source code and documents to certain DLP policies.

Enterprise Manager is a third-party software offered by RSA Security, Inc. It is not a part of the Cisco IronPort Email Security appliance. This feature is compatible with version 9.0 of the Enterprise Manager software.

See the "Data Loss Prevention" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

As part of RSA Enterprise Manager Integration, AsyncOS now includes a User Distinguished Name LDAP query for LDAP profiles. This query returns a message sender's distinguished name for the Email Security appliance to include with all the other DLP incident data it sends to Enterprise Manager.

See the "LDAP Queries" chapter in the *Cisco IronPort AsyncOS Advanced Configuration Guide*

Enhancement: DLP Message Tracking Privileges By User Group

AsyncOS 7.6 allows you to choose which non-administrator user can view sensitive DLP-related information in Message Tracking by user role. See the "Common Administrative Tasks" chapter in the *Cisco IronPort AsyncOS for Email Daily Management Guide* for more information.

Enhancement: RSA Email DLP's "Quarantine a Copy and Deliver" Option

AsyncOS 7.6 provides an option to quarantine a copy of a message that violates a RSA Email DLP policy while still delivering the original message. See the "Data Loss Prevention" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

Enhancement: DLP Message Actions

Starting in AsyncOS 7.6, the primary and secondary actions performed by DLP policies are now defined as *message actions*. You create message actions using the Mail Policies > DLP Message Actions page in the GUI and then add the actions to your DLP policies. When updating from a previous version of AsyncOS, the system automatically generates new message actions based on the primary and secondary actions defined in your existing DLP policies.

See the "Data Loss Prevention" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

Enhancement: New and Updated RSA Email DLP Policy Templates

AsyncOS 7.6 includes some updated RSA Email DLP policy templates, which may affect the performance of existing DLP policies on your appliance. Please double-check your DLP policies to see if the classifiers have changed.

The following RSA Email DLP policy templates have been updated to require customization in AsyncOS 7.6:

- Georgia SB-230
- Hawaii SB-2290
- Illinois SB-1633
- Indiana HB-1101
- Kansas SB-196
- Maine LD-1671
- Montana HB-732
- Rhode Island HB-6191
- Vermont SB-284

The following templates have also been modified in AsyncOS 7.6:

- Suspicious Transmission - ZIP Files is now Suspicious Transmission - Archive Files
- HIPAA is now HIPAA and HITECH and uses the Healthcare Dictionaries, Patient Identification Numbers, US National Provider Identifier, and US Social Security Number classifiers

AsyncOS 7.6 includes these new DLP policy templates:

- HIPAA and HITECH Low Threshold
- PIPEDA (Personal Information Protection and Electronic Documents Act)
- Puerto Rico DACO 7207, 7336 and 7376
- Alaska HB-65
- Arkansas SB-1167
- Delaware HB-116
- District of Columbia CB 16-810
- Iowa SF-2308
- Maryland HB-208
- Michigan SB-309
- Mississippi HB-583
- Missouri HB-62
- Nebraska LB-876
- North Carolina SB-1048
- North Dakota SB-2251
- Oregon SB-583
- South Carolina SB-453
- Tennessee SB-2220
- U.S. Virgin Islands V.I. Code 2208
- Virginia SB-307
- West Virginia SB-340
- Wisconsin SB-164

- Wyoming WS 40-12-501 to 502
- Credit Card Numbers - By Issuer
- US Passport Numbers
- Confidential Documents
- Network Diagrams

Enhancement: SenderBase Reputation Service Requires an Anti-Spam Feature Key

Starting in AsyncOS 7.6, an Email Security appliance requires an anti-spam system feature key in order to use the SenderBase Reputation Service.

New Feature: DKIM Verification Profiles

AsyncOS 7.6 adds DKIM verification profiles, which are lists of parameters that the Email Security appliance's mail flow policies use for verifying DKIM signatures. For example, you can create two verification profiles, one that allows 30 seconds before a query times out and a second that allows only 3 seconds before a query times out. You can assign the second verification profile to the Throttled mail flow policy to prevent connection starvation in case of a DDoS.

See the "Email Authentication" chapter in the *Cisco IronPort AsyncOS Advanced Configuration Guide* for more information.

Enhancement: New Tags for DKIM Signing Profiles

AsyncOS 7.6 adds a new list of tags to include in DKIM message signatures. You select which tags you want to include in the signatures when creating a DKIM signing profile. The following tags are available:

- **"i" Tag.** The identity of the user or agent (e.g., a mailing list manager) on whose behalf the message is signed.
- **"q" Tag.** A comma-separated list of query methods used to retrieve the public key.
- **"t" Tag.** The timestamp of when the signature was created.
- **"x" Tag.** The expiration time of the signature, in seconds. (The option in include "x" tag information existed in previous versions of AsyncOS 7.6.)
- **"z" Tag.** A vertical bar-separated (i.e., |) list of header fields present when the message was signed.

See the "Email Authentication" chapter in the *Cisco IronPort AsyncOS Advanced Configuration Guide* for more information.

New Feature: DKIM Signing of System-Generated Messages

AsyncOS 7.6 allows you to choose whether to sign system-generated messages with a DKIM signature. The types of system-generated message that the Email Security appliance will sign include the following:

- Cisco IronPort Spam Quarantine notifications
- Content filter-generated notifications
- Configuration messages
- Support requests

See the "Email Authentication" chapter in the *Cisco IronPort AsyncOS Advanced Configuration Guide* for more information.

Enhancement: Skip DKIM Signing Action

In AsyncOS 7.6, content filters now include an action to skip DKIM signing. See the "Email Security Manager" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

Enhancement: Rate Limiting and Enforced TLS for Envelope Senders in Mail Flow Policies

AsyncOS 7.6 updates Mail Flow Policies with the option to limit number of recipients during a specified time period that a listener will receive from a unique envelope sender, based on the mail-from address. Each listener tracks its own rate limiting threshold; however, because all listeners validate against a single counter, it is more likely that the rate limit will be exceeded if messages from the same mail-from address are received by multiple listeners.

You can also make TLS connections mandatory for envelope senders from a certain domain or with a specific email address when the mail flow policy has a setting of Preferred for encryption over TLS.

You specify the domains and email addresses for these envelope senders using an address list.

AsyncOS also adds a Rate Limiting report that allows you to quickly identify individual senders of large numbers of messages. Use this report to help you to control spam from internal user accounts, identify compromised user accounts, limit out-of-control applications that use email, and avoid damaging your organization's online reputation and the attendant hassles resulting from this situation.

See the "Using Email Security Monitor" chapter in the *Cisco IronPort AsyncOS for Email Daily Management Guide* for more information.

Enhancement: Separate Update Servers for AsyncOS Upgrades and Other Service Updates

AsyncOS 7.6 allows you to specify a different update server for AsyncOS upgrades than the one used for other service updates, such as feature key updates, outbreak filters, and time zone rules. For example, you can specify a local server for downloading AsyncOS upgrades while using the Cisco IronPort update servers for the other service updates.

See the "System Administration" chapter in the *Cisco IronPort AsyncOS for Email Configuration Guide* for more information.

Enhancement: Message Size for Encryption

Starting in AsyncOS 7.6, the Email Security appliance can encrypt messages up to 10 MB in size. If the appliance attempts to encrypt a message larger than 10 MB, it will be send the message back to the sender.

Enhanced: Web User Interface Protection

AsyncOS 7.6 for Email includes additional protection from cross-site request forgeries (CSRF) and other attacks on the web user interface.

Upgrade Paths

You can upgrade to release 7.6.3-019 from the following versions:

- 7.1.5-102
- 7.1.5-104
- 7.1.5-106
- 7.5.2-101
- 7.5.2-203
- 7.5.9-004
- 7.6.1-022
- 7.6.1-025
- 7.6.1-101
- 7.6.2-014
- 7.6.2-103
- 7.6.2-201

Installation and Upgrade Notes

Read through and consider the installation and upgrade impacts listed in this section.

When you upgrade AsyncOS for Email from the web interface or Command Line Interface (CLI), the configuration is saved to file in the /configuration/upgrade directory. You can access the upgrade directory using an FTP client. Each configuration file name is appended with the version number, and passwords in the configuration file are masked so they are not human readable.

Note You must be logged in as the admin to upgrade. Also, you must reboot the appliance after upgrading.

Upgrading to the AsyncOS 7.6 Release

Caution The network configuration of your Email Security appliance will be lost if you upgrade AsyncOS for Email from version 7.5.2-203 to 7.6.3-019, and revert back to version 7.5.2-203. If the network configuration is lost, emails are not delivered until you reset the network configuration by physically accessing the Email Security appliance.

For the AsyncOS 7.6 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.

Resume all listeners.

Resolved Issues

This section describes the resolved issues for the Cisco IronPort AsyncOS 7.6 for Email releases.

Cisco IronPort AsyncOS 7.6.3 for Email

Table 1 describes the resolved issues in the Cisco IronPort AsyncOS 7.6.3 for Email release.

Table 1 Resolved Issues in AsyncOS 7.6.3 for Email

Defect ID	Description
CSCuf33132	**'Use SenderBase for Flow Control' not Rate Limiting as expected** Rate limiting is applied to each IP address instead of the full subnet. This results in the ESA accepting more emails than expected for the rate limiting settings. This issue occurs when 'Use SenderBase for Flow Control' is selected as the Flow Control method on AsyncOS 7.6 or later.
CSCzv15209	**SenderBase Reputation Service unable to retrieve data** Reputation engine restarts giving out "SBRS unable to retrieve" errors. This issue occurs with very high incoming connection rate leaving the mail processing engine in a state where every connection gets an "SBRS unable to retrieve."
CSCzv15563	**Sophos engine get expired after upgrade** Upgrade to latest AsyncOS which is having Expired Sophos engine will alert the user stating that it is expired. This issue occurs when user upgrades to latest available AsyncOS which has Expired Sophos Engine. An alert will be sent to user stating that the Sophos engine is expired.

Table 1 Resolved Issues in AsyncOS 7.6.3 for Email

Defect ID	Description
CSCzv44971	**DLP errors when certain content blades are enabled on custom policies** Customer may see slow outgoing mail flow and the following text within the mail logs: Warning: MID ###### '(no name)' DLP content scanning failed (unknown error). This issue occurs when you have a custom DLP Policy that is using one of the following content blades that requires additional information: • Group Insurance Numbers • Health Plan Beneficiary Numbers • Mergers and Acquisitions Codenames • Patient Identification Numbers • Custom Accounts • US Personal Identification Information • Medical Record Numbers • Confidential Documents • Student Identification Numbers
CSCzv50755	**External Auth against Cisco ACS stopped working after upgrading** External user authentication against Cisco ACS stopped working after upgrade of AsyncOS from 7.5.1-102 to 7.6.1-022 version.
CSCzv77030	**High connection rates result in no SBRS scores** SBRS scores are not retrievable due to high connection rates with high latency DNS responses. High number of incoming mail connections results in the mail flow engine not getting Sender Base Reputation Scores.
CSCzv81113	**Domain Profiles UI displays error on page and displays extra options** Domain Profiles UI displays error on page and displays extra options in Internet Explorer 8 in comparing to Firefox version 3.6.13. This issue is applicable only for Internet Explorer 8 on Windows 7.
CSCzv81592	**Using "Australia Business and Company Numbers" causes DLP to stop functioning** DLP stops functioning and scan messages when use "Australia Business and Company Numbers" DLP policy.
CSCzv25573	**IronPort Spam Quarantine (ISQ) Denial of Service Vulnerability** A vulnerability in the Cisco IronPort Email Security appliance that could have allowed an unauthenticated, remote attacker to cause multiple critical processes to become unresponsive, resulting in a denial of service condition. For more information on the vulnerability, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa.

Table 1 Resolved Issues in AsyncOS 7.6.3 for Email

Defect ID	Description
CSCzv44633	**Web Framework Authenticated Command Injection Vulnerability** A vulnerability in the Cisco IronPort Email Security appliance that could have allowed an authenticated, remote attacker to execute arbitrary commands on the underlying operating system 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-20130626-esa.
CSCzv63329	**Management Graphical User Interface Denial of Service Vulnerability** A vulnerability in the Cisco IronPort Email Security appliance that could have allowed an unauthenticated, remote attacker to cause multiple critical processes to become unresponsive, resulting in a denial of service condition. For more information on the vulnerability, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa.

Cisco IronPort AsyncOS 7.6.2 for Email

The following is a list of resolved issues in the Cisco IronPort AsyncOS 7.6.2 for Email release.

- **Log Injection Vulnerability.** This version of AsyncOS fixes a log injection vulnerability, where invalid entries could be added to the appliance's logs.
- **Damage Caused by Reboot Without Proper Shutdown.** Previously, rebooting the appliance without proper shutdown sometimes caused irreparable damage to the appliance.
- **Delivery Status Details Report Shows Error Message.** Fixed an issue where the Delivery Status Details report page for an IPv4 or IPv6 destination would show a "cannot concatenate 'str' and 'IPv6' (or IPv4) objects" error message.
- **Appliance Does Not Retry DNS Query.** Fixed an issue where the appliance would not retry a DNS query when it doesn't get a response when the appliance is configured to use root DNS or only multiple local DNS servers with the same priority level. A timeout has been added to allow the appliance to retry a DNS query if it does not receive a response.
- **Packet Capture Doesn't Capture Traffic On VLAN Interface When Filter is Used.** Fixed an issue where Packet Capture didn't capture traffic on a VLAN interface when a custom filter was used.
- **User Connects to Wrong Interface When Using telnet and the hostname.** Previously, if the user did not specify a network interface for telnet connections, attempting to telnet into the appliance using the hostname would result in the user connecting to the wrong network interface. This issue has been resolved. Now, using telnet and the appliance's hostname results in connecting to the appliance's default network interface.
- **DNS Queries Fail Because of AAAA Record Request.** Previously, the Email Security appliance would request AAAA records from an MX even if the dnshostpref and destconfig DNS preference require only IPv4 connections. If the MX returns a valid A record, but not an AAAA record, the mail delivery would fail. This issue has been resolved. Now, appliance only requests A records for IPv4 connections.
- **CPU Usage May Unexpectedly Run at Maximum Capacity.** Previously, in rare circumstances, SNMP could drive CPU usage to %100. This problem no longer occurs.

- **Traceback Generated After Technical Support Tunnel Tails for DNS-related Reasons.** Previously, when attempting to establish a secure tunnel through which Cisco IronPort technical support can connect to the appliance, if the tunnel attempt fails for reasons related to DNS, AsyncOS generates a traceback.
- **Large Number of Content Filter Matches May Result in PDF Report Error.** Fixed an issue a printable PDF report for content filters may contain the error message "one of tables has too many columns" due to a large number of incoming or outgoing content filter matches. Now, the PDF report prints out correctly.
- **Spam Digest Notification Email Does Not Display Correctly in Japanese.** Fixed an issue where the spam digest notification email did not display its information in Japanese correctly when localized.
- **telnet to Appliance that Does Not Have an A or AAAA Record Results in Traceback.** Fixed an issue where a traceback occurred when you attempt to telnet into an appliance that does not have an A or AAAA DNS record.
- **Outlook Improperly Displays Messages with Body and Footer Encoded Differently.** Footers added to messages by the appliance can be encoded as text/plain or text/html. Previously, if the message body and footer are not encoded the same way, Microsoft Outlook will only display the footer.This issue has been resolved. Now the message body and footer are properly displayed in Outlook.
- **resourceConservationMode SNMP Trap Missing.** Fixed an issue where the resourceConservationMode SNMP trap was not available on the appliance.

Cisco IronPort AsyncOS 7.6.1 for Email

The following is a list of resolved issues in the Cisco IronPort AsyncOS 7.6.1 for Email release.

- **Mail Delivery to Destination Goes Offline After Over 5000 Messages to the Same Destination Are Queued.** In the previous versions of AsyncOS 7.6, mail delivery to a destination may go offline if the appliance had to queue over 5000 messages for that destination before it could delivery them. This could happen, for example, if an organization's mail servers go offline for maintenance and the appliance has to queue messages until the servers are back online. When delivery resumed, the appliance may have only delivered a few messages. The remaining messages for that destination would not be delivered. This issue has been resolved and queued messages will be delivered.
- **Switching from RSA Enterprise Manager Mode to Local RSA Email DLP Mode Using Wizard Causes Errors.** In the AsyncOS 7.6.0 release, if you switched the appliance from RSA Enterprise Manager mode to the local RSA Email DLP mode and then used the DLP Assessment Wizard to create new policies, the multiple errors occur if Enterprise Manager did not send any DLP policies to the appliance before you switched the DLP modes.
- **Deleting Message Action Used in Existing DLP Policies Results in Application Fault.** In the AsyncOS 7.6.0 release, if you deleted a message action that was being used by one or more DLP policies, an application fault occurred when you committed the change without first reconfiguring the affected DLP policies with a new message action.
- **Some Pre-upgrade Reporting Data is Missing from Incoming Mail: IP Address Report Details.** When upgrading to AsyncOS 7.6.0, IP addresses in pre-upgrade data that are in the range 128.x.x.x to 255.x.x.x would be counted in the report summary, but would not be available in report details.
- **Errors in Japanese Localization of User Interface.** AsyncOS 7.6.1 fixes a number of translation errors in the Japanese localization of the user interface. These errors appeared on multiple spam quarantine pages and the end user quarantine online help.

- **Upgrade Request of Second Level TDLs (Regional Domains).** In the previous release, subdomains would not be listed in the Sender Profile section of regional domains on the Incoming Mail report. The same applied while searching for Regional domains. Example: "foo.mail.ru" will not be listed in the Sender Profile report for mail.ru.
- **Email Sent to Recipient with Only Periods in Domain Name Halts Message Processing.** Previously, if the Email Security appliance received an email sent to a recipient with only periods for the recipient's domain name (e.g., bob@.....), the email would result in the Email Security appliance halting message processing. The appliance would continue to accept messages, but could not process them.
- **IronPort Mail Merge Feature Missing.** Previously, 3xxD appliances upgraded to AsyncOS 7.5.0 or later lost the IronPort Mail Merge (IPMM) feature. Previously, appliances with a DPP feature key received the IPMM feature, too. This issue has been resolved. Appliances with a DPP feature key once again get the IPMM feature.
- **Changing Notification Schedule Sends Out Notification.** Fixed an issue where changing an email notification schedule results in the Email Security appliance automatically sends out email notifications once you commit the change.
- **Upgrading to AsyncOS 7.6.0 Changes Netmasks of IP Interfaces on a Single Physical Interface.** If you have assigned multiple IP interfaces with the same 255.255.255.0 netmask to a single physical interface, the Email Security appliance would automatically assign a netmask of 255.255.255.255 to one of the IP interfaces, making the other IP interface the source of all requests from the physical interface. Upgrading your appliance to AsyncOS 7.6.0 may have swapped the netmasks for those two interfaces, which could result in connection problems, depending on your configuration. This issue has been resolved. Upgrading to AsyncOS 7.6.1 does not change the netmasks of the IP interfaces.
- **Application Fault Occurs When Viewing Report on Incoming Messages with No Hostname.** Fixed an issue where viewing an Incoming Mail report on messages from an IP address with no domain record could result in an application error.
- **LDAP Using Invalid Interface on Clustered Machine Causes Application Fault.** Fixed an issue where if you change the name of an interface on a clustered machine, opening the System Administration > LDAP page in clustered mode would cause an application fault.
- **HAT Rescanning May Cause Application Fault if the Connection is Refused at TCP Level.** Fixed an issue where a the HAT rescanning feature may cause an application fault to occur on the appliance if, upon rescanning, the message's sender is moved to another sender group that has Directory Harvest Attack Prevention limits set and will refuse a connection at the TCP level.
- **Adding Footer to Uuencoded Messages Results in Outlook Rendering Messages Incorrectly.** Fixed an issue where adding a footer to a uuencoded message would result in Outlook displaying the message incorrectly by rendering its attachments inline. This was due to a MIME-version header being added to the message because of the footer. This issue has been resolved. Adding a footer no longer adds a MIME-version header to the uuencoded message.
- **Signing a Splintered Message Relayed Through Private Listener with DKIM Could Result in Dropped Message.** If you have configured a private listener on the appliance to sign a message using DKIM, it was possible in previous versions of AsyncOS that the appliance may not have delivered one of the messages if the original message was splintered. This would result in one of the splintered messages in being lost.
- **Injection Debug Log with Syslog Push Retrieval Method May Cause Work Queue to Crash.** Fixed an error where an injection debug log with Syslog Push as a retrieval method could cause the appliance's work queue to crash when work queue processing is restarted.

Cisco IronPort AsyncOS 7.6 for Email

The following is a list of resolved issues in the Cisco IronPort AsyncOS 7.6 for Email release.

- **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-20120126-ironport.
- **Email Security appliance trusts DigiNotar as a root certificate authority.** In previous versions of AsyncOS for Email, the Email Security appliance trusted DigiNotar as a root certificate authority. It also trusted DigiNotar's intermediate certificates issued by the State of Netherlands. These certificates are no longer accepted.
- **AsyncOS 7.6 Updated to Use OpenSSH 5.4.** AsyncOS 7.6 has been updated to use OpenSSH 5.4 in order to fix the CVE-2008-5161 vulnerability.
- **Disclaimers Cannot Be Added to Non-US-ASCII Message Body.** Previously, mail agents such as Outlook and Thunderbird displayed a disclaimer as an attachment and not inline with the message because the message body was not encoded as US-ASCII. This issue has been resolved. This disclaimer is now displayed inline with the message even if the message body is encoded in a format other than US-ASCII.
- **AsyncOS Upgrades and Service Updates Use Same Update Server.** In AsyncOS 7.5, AsyncOS upgrades used the same update server as all of the service updates, whether it was an IronPort update server or a local update server. This prevented users from using a local server for AsyncOS upgrades and an IronPort update server for all other service updates unless they configure the appliance to use a manifest on a local appliance for an AsyncOS upgrade and then re-configure the appliance to use an IronPort update server for the other services after the upgrade is complete. This issue has been resolved. AsyncOS 7.6 allows you to specify a different update server for AsyncOS upgrades than the one used for other service updates, such as feature key updates, outbreak filters, and time zone rules.
- **Using a Virtual Gateway Hostname for a Received Header May Prevent DKIM Signing.** Previously, AsyncOS for Email may not have signed outgoing messages using DKIM if the appliance uses a Virtual Gateway hostname in the received header.
- **GUI Sometimes Displays Fewer Query Results Per Page Than Expected.** Previously, when you performed a query, the GUI sometimes displayed fewer results per page than expected. For example, if you selected to view 50 items of your query results per page, the GUI may have displayed only 20 per page, even though the page may have said "Displaying 1-50 of 120 items."

Known Issues

Table 2 lists the known issues in this release of AsyncOS 7.6.3 for Email release.

Table 2 Known Issues for AsyncOS 7.6.3 for Email

Defect ID	Description
CSCzv54743	**Network configuration lost while reverting back after an AsyncOS for Email upgrade** You will lose the network configuration of your Email Security appliance if you are reverting back after an AsyncOS for Email upgrade. If you lose the network configuration, emails are not delivered until you reset the network configuration by physically accessing the Email Security appliance. This is observed when you upgrade AsyncOS for Email from version 7.5.2-203 to 7.6.3-019, and revert back to version 7.5.2-203.
CSCzv39735	**Appliance Misses Incoming Connections When Handling Large Messages** The Email Security appliance may not pick up an incoming connection when it's processing a very large message (e.g., greater than 30 MB).
CSCzv54420	**CLI Session is Lost if You Configure the Hostname as SNMP Trap Target** If you enter the appliance's hostname as a Trap Target when configuring SNMP, you will lose the CLI session to the appliance immediately after you enter the hostname and hit the Return key.
CSCzv41250	**Message Tracking Returning Messages with a High Number of Recipients Results in Excessive Memory Usage** The Email Security appliance may run out of memory if you run a Message Tracking query in the Web UI that returns messages that have a large number of recipients.
CSCzv44674	**Application Fault May Occur When RSA Enterprise Manager DLP is Enabled at Group or Cluster Level** Under rare conditions, configuring a clustered ESA to use RSA EM DLP at cluster or group level may lead to an application fault.
CSCzv18038	**SNMP Trap Cannot Use a URL That Has a Tilde (~) After a Slash (/)** SNMP will not generate an SNMP trap if you use a URL with a tilde (~) after a slash for the destination. Workaround: Make sure that the URL ends with a slash (/), otherwise the URL will be interpreted as a file instead of a directory.
CSCzv50959	**netstat > State of Network Interfaces CLI Command Shows Truncated IPv6 Addresses** If you use the netstat > State of Network Interfaces command in the CLI to view IPv6 addresses, the CLI truncates the IPv6 addresses shown
CSCzv22849	**Appliance Cannot Send Alerts to IPv6 Destinations** The Email Security appliance cannot send an alert to an IPv6 destination. It can only send an alert to an IPv4 destination.

Table 2 Known Issues for AsyncOS 7.6.3 for Email (continued)

Defect ID	Description
CSCzv31989	**Matched Content Displayed Incorrectly in Enterprise Manager** If you attempt to view matched content from messages with DLP violations in Enterprise Manager, Enterprise Manager displays random characters at the end of the message. If you download message's attachment using Enterprise Manager, the attachment may content random characters in it and may not open.
CSCzv71027	**Network Settings Not Saved When Reverting to Previous Version of AsyncOS** Due to the new IPv6 address feature, the appliance's network settings are not saved when you revert the appliance from AsyncOS 7.6 to an earlier version.
CSCzv63788	**Right-to-Left Languages Disabled for PDFs Generated from AsyncOS** AsyncOS 7.6 does not include right-to-left languages in PDFs generated from the appliance's interface, such as the Message Details page, due to issues displaying the languages properly. The PDFs display black squares instead.
CSCzv50968	**Application Fault Occurs if '&', '<', and '>' are in Name of DLP Policy** If you use the &, <, and > characters in the name of a DLP policy, an application fault occurs when the Email Security appliance receives an email that matches that DLP policy. Because of the application fault, the DLP violation will not be caught by the appliance.
CSCzv81127	**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.
CSCzv32026	**Modifying Certificate Re-initializes All Interfaces.** If you modify the HTTPS certificate on any interface, AsyncOS re-initializes all existing interfaces on the appliance. During the initialization, which is usually less than a second, network errors are seen while interfaces re-initialize and alerts are sent. Workaround: Cisco IronPort recommends suspending listeners and delivery on the appliance before modifying the HTTPS certificate on an interface, then resuming listeners and delivery.
CSCzv12305	**AsyncOS Does Not Log Out RADIUS User After Access Rights Change in CLI.** If a RADIUS external user changes the role mapped to their RADIUS group using the `userconfig` command in the CLI, AsyncOS does not forcibly log the user out or change their access rights during their session. The user continues to have the same access rights until they log out of the CLI.
CSCzv66064	**Improper Reboot May Cause CASE Corruption.** An improper reboot of the Email Security appliance may corrupt the CASE engine and cause emails to back up in the queue until the CASE engine is updated. Workaround: Use the `antispamupdate ironport force` command to force a CASE engine update.

Table 2 Known Issues for AsyncOS 7.6.3 for Email (continued)

Defect ID	Description
CSCzv32468	**Search Again Widget Not Displayed for Split Messages.** If you perform a Message Tracking search for a message that was split during processing, the Message Details page does not display the Search Again widget if the message has been quarantined, bounced, or dropped, but not delivered. The Message Details page does display the Search Again widget for split messages that have been delivered.
CSCzv86681	**User Can Import a Configuration File with Larger Disk Allocation Values than Possible** When you import a configuration file from a system running on a different hardware platform, there is a possibility to incorrectly configure the disk management so that the Email Security appliance is configured to use more space than is available.
CSCzv05651	**SMA Cannot Communicate with ESA after AsyncOS Reversion** 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.
CSCzv91885	**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.
CSCzv53919	**Active Sessions Page and who CLI Command Cannot Display Active CLI Usernames 16 Characters or Longer** Neither the `who` CLI command nor the Active Sessions page in the GUI can identify active CLI users with usernames 16 characters or longer.
CSCzv18352	**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.
CSCzv27454	**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.
CSCzv40745	**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.

Table 2 Known Issues for AsyncOS 7.6.3 for Email (continued)

Defect ID	Description
CSCzv18265	**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 7.6 for Email and using `loadconfig` to load a configuration file. Workaround: Reboot the Email Security appliance. All message tracking details will appear correctly after the reboot.
CSCzv85685	**The Email Security Monitor Overview Page Incorrectly Counts Quarantine Mails as "Virus."** 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.
CSCzv70453	**LDAP Test Query in Domain Assignment Fails If One or More Servers Defined in Domain Assignments Is Unreachable.** 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.
CSCzv95624	**One or More Unavailable LDAP Servers Can Cause a Chain Query to Fail.** One or more unavailable LDAP servers in a chain can cause the chain query to fail.
CSCzv66584	**False Positives with "Transmission of Contact Information" DLP Policy.** 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.
CSCzv95338	**AsyncOS Does Not Support Multiple RADIUS Class Attributes.** 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.
CSCzv25323	**CLI Does Not Support Usernames Longer Than 16 Characters for Local and External Authentication.** 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.
CSCzv59483	**External Authentication Fails if the Group Name Contain Special Characters.** 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.

Table 2 Known Issues for AsyncOS 7.6.3 for Email (continued)

Defect ID	Description
CSCzv31160	**Editing a Large Content Dictionary From the GUI Causes Browser to Hang.** 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.
CSCzv05911	**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.

Finding Information about Known and Fixed Issues

Use the Cisco Software Bug Toolkit to find the most current information about known and fixed defects.

Before You Begin

Register for a Cisco account if you do not have one. Go to https://tools.cisco.com/RPF/register/register.do.

Procedure

Step 1 Go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2 Log in with your Cisco account credentials.

Step 3 Enter information:

To	Do This
Search for a list of bugs for your product	1. For **Select Product Category**, select **Security**. 2. For **Select Products**, select **Cisco Email Security Appliance**. 3. (Optional) Scroll down and enter additional criteria. 4. Click **Search**.
Find information about a specific issue	• Choose the product category and product as described in the previous table row, then enter keywords related to the issue. Then click **Search**. • Enter a bug ID number that starts with CSC in the **Search for Bug ID** field, then click **Go**. **Note** The 5-digit bug numbers used for previous releases of content security software cannot be used with this tool.
• Save searches • Create bug groups • Sign up for notifications	• Click the **Help Page** link on the Bug Toolkit page, or • Visit http://www.cisco.com/web/applicat/cbsshelp/help.html#personalize.

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, 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

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.