Release Notes for *Cisco IronPort AsyncOS 7.5.2 for Email*

Revised: April 4, 2012

Contents

These release notes contain information critical to upgrading and running Cisco IronPort AsyncOS 7.5.2 for Email, including hardware-specific information and known issues.

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

What's New in Cisco IronPort AsyncOS 7.5.2 for Email

This section describes the resolved issues in Cisco IronPort AsyncOS 7.5.2 for Email.

Fixed Issues in Release 7.5.2

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

Table 1 Resolved Issues in Version 7.5.2

Defect ID	Description
72743	**Fixed: OpenSSH Vulnerability Could Expose Plain Text Data** Previously, a remote attacker could have recovered certain plaintext data in an SSH session by exploiting OpenSSH CBC Mode Information Disclosure Vulnerability CVE-2008-5161. This vulnerability has been fixed.
84068	**Fixed: Content Scanning Engine Stops Scanning Due to Memory Leak** Previously, the Email Security appliance's content scanning engine would go out of operation and stop scanning documents and attachments if it leaked memory and the leaked memory and memory usage reached 400 MB. The scanning engine would instead log, "no filter available for this file type." This issue has been resolved.
81190 83861	**Fixed: Office 2010 Files Detected as ZIP Files** Previously, the Email Security appliance detected Office 2010 .files as .zip files instead of document filetype. This affected DLP scanning and content filters. This issue has been resolved.
74457	**Fixed: Proxy Server Setting Erroneously Used for Feature Key Updates in Some Cases** Previously, when a proxy server was configured for the update settings and was then removed, AsyncOS still tried to connect through the proxy server when trying to retrieve feature key updates. This no longer occurs.

Table 1 Resolved Issues in Version 7.5.2 (continued)

Defect ID	Description
64885	**Email Security Appliance Now Uses AES-256 Encryption with CRES** The Email Security appliance now supports encrypting messages using the AES-256 algorithm when using CRES as a key server.
82139	**Email Security Appliance No Longer Trusts DigiCert Sdn. Bhd. as an Intermediate Certificate Authority** Previously, the Email Security appliance trusted intermediate CA certificates issued to "Digicert Sdn. Bhd" by Entrust and GTE CyberTrust. This no longer occurs. The Email Security appliance has blacklisted these intermediate certificates. For more information, see the following Cisco PSIRT article: http://tools.cisco.com/security/center/viewAlert.x?alertId=24031
80493 81246 82858 82866	**Fixed: Errors in Japanese Localization of User Interface** AsyncOS 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.
84104	**Upgrade Request of Second Level TDLs (Regional Domains)** Subdomains will not be listed in the Sender Profile section of regional domains on the Incoming Mail report. The same applies while searching for Regional domains. Example: "foo.mail.ru" will not be listed in the Sender Profile report for mail.ru.

What's New in Cisco IronPort AsyncOS 7.5.1 for Email

This section describes the resolved issues in Cisco IronPort AsyncOS 7.5.1 for Email.

Fixed Issues in Release 7.5.1

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

Table 2 Resolved Issues in Version 7.5.1

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-20120126-ironport
82012	**Fixed: Appliance may stop accepting new email messages** After reboot, an appliance upgraded to AsyncOS 7.5.1-026 may suspend all listeners, causing the appliance to stop accepting incoming email messages. If you suspect this issue, enter the `status detail` command in the CLI. If this issue has occurred, the Resource Conservation line will show 999.
78178	**Fixed: Appliance May Become Unresponsive** Previously, a C660, C670, X1060, or X1070 appliance would become unresponsive after processing a high amount of message traffic with large attachments over an extended period of time. This issue required the work queue, scanning engines, and other AsyncOS features to be handling a constant high level of traffic in order to create the excessive memory usage that caused the appliance to become unresponsive. This issue has been resolved.
80072	**Fixed: Feature Key Checks May Cause Slowdown** When processing a message, the Email Security appliance performs feature key checks when running certain filter rules. The performance of these feature key checks slowed down in AsyncOS 7.5.0 and caused a slowdown in processing messages through the email pipeline. This issue has been resolved.
80678	**Fixed: Infrequent Race Condition Could Lock Up Email Security Appliance** When this issue occurred, the Email Security appliance stopped communicating with associated Security Management appliances, and stopped responding to input via GUI and CLI.

Table 2 Resolved Issues in Version 7.5.1 (continued)

Defect ID	Description
79524	**Fixed: Excessive Memory Usage from Footer Stamping and Attachment Stripping** Fixed an issue where adding a footer to an outgoing message or stripping an outgoing message's attachment would result in excessive memory usage on the Email Security appliance.
74547	**Fixed: Scanning Engine Restarts If It Exceeds Memory Limit** The content scanning engine in AsyncOS 7.5.0 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.
76228	**Fixed: Large Messages Put Appliance into "Resource Conservation" Mode if Destination is Down** Previously, if the Email Security appliance tried delivering large messages to a destination that could not be reached, the message queue would fill up messages and stop accepting new messages. The queue would then force the appliance into "resource conservation" mode because the queue would not release the memory it was using, which prevented the appliance from running tasks like garbage collection. This issue has been resolved.
79854	**Fixed: Unable to Reply with Cisco Registered Envelope Service Encryption** Fixed an issue where a recipient was unable to reply to a message that had been encrypted using the Cisco Registered Envelope Service.
81079	**Fixed: Multiple Emails Sent to Mailing List Recipients** Previously, if a mailing list had email addresses with mixed cases, the Email Security appliance would send duplicate messages to the addresses with mixed cases if an LDAP routing query was enabled on the appliance. This issue has been resolved.
79501	**Fixed: Modified End-User Spam Quarantine URL Can Disable the End-User Quarantine for All Users** Previously, if an end user attempted to modify a system-generated spam quarantine URL, all subsequent spam quarantine users would receive an error when attempting to access the quarantine. This problem no longer occurs.

What's New in Cisco IronPort AsyncOS 7.5 for Email

This section describes the new features added in Cisco IronPort AsyncOS 7.5 for Email.

New Feature: Outbreak Filters

AsyncOS 7.5 updates the Virus Outbreak Filters feature, now Outbreak Filters, to protect your users from the growing trend of low-volume, targeted email attacks in addition to virus outbreaks. The messages used for these threats, such as phishing messages, scams, and malware distribution, are complex, evolving, and can be more difficult to detect than widespread spam, phishing, and virus outbreaks. The enhancements in the Outbreak Filters feature offer your users protection from these attacks and prevents them from downloading malware or distributing sensitive information. The Outbreak Filters feature can rewrite URLs in messages to protect recipients from browsing to malicious websites and add disclaimers to suspect messages to warn recipients.

As part of this update, the previous CLI commands for Virus Outbreak Filters have been renamed:

- **vofconfig** is now **outbreakconfig**
- **vofflush** is now **outbreakflush**
- **vofstatus** is now **outbreakstatus**
- **vofupdate** is now **outbreakupdate**

The Outbreak Filters feature also includes the updated Outbreak Filters report and new outbreak threat-related variables for disclaimer templates.

New Feature: Delegated Administration

AysncOS 7.5 provides more flexible control over users' access to the email security features on the appliance than the predefined user roles. You can design custom user roles and delegate specific responsibilities to users that align with their roles within your organization, allowing these *delegated administrators* access only to the email security features they are responsible for and not the system configuration features that are not related to their jobs. You can control the level of access that user groups have to the features on the appliance.

New Feature: Technician User Role

AsyncOS 7.5 adds a new predefined Technician role for users responsible for upgrading Cisco IronPort Email Security appliances. Users assigned to the technician role can perform system upgrades, reboot the appliance, manage feature keys, and perform other actions needed to upgrade an appliance.

Enhancement: Administrator Role

Starting in AsyncOS 7.5, administrators can perform system upgrades, create clusters, and join appliances to existing clusters.

New Feature: Password Policy Enforcement

In AsyncOS 7.5, you can define user account and password restrictions to enforce organizational password policies for local Email Security appliance users. These restrictions include:

- **Password rules.** You can define what kinds of passwords users can choose, such as which characters are optional or mandatory.
- **User account locking.** You can define how many failed login attempts cause the user to be locked out of the account.
- **Password lifetime rules.** You can define how long a password can exist before the user is required to change the password after logging in.

Enhancement: Large Message Scanning

AsyncOS 7.5 improves how anti-spam scanning handles large messages in order to optimize the throughput of your Email Security appliance while still being able to scan the increasing number of larger messages. You can define an *always scan* message size, where messages smaller than the defined size are completely scanned by IronPort Anti-Spam engine, delivering IronPort's industry-leading level of efficacy, and a *never scan* message size, where messages larger than the defined size are not scanned. For messages larger than the *always scan* size and smaller than the *never scan* size, the anti-spam engine performs a limited and faster scan.

New Feature: SMTP Call Ahead

AsyncOS 7.5 includes SMTP call-ahead recipient validation, which allows the Email Security appliance to perform recipient validation by querying an external SMTP server prior to accepting incoming mail for the recipient. SMTP call-ahead recipient validation is useful in cases where you might want to validate users but cannot use LDAP Accept or the Recipient Access Table (RAT) for recipient validation.

New Feature: Configuration History Logs

AsyncOS 7.5 include a configuration history log that consists of a configuration file with an additional section listing the name of the user, a description of where in the configuration the user made changes, and the comment the user entered when committing the change. Each time a user commits a change, a new log is created containing the configuration file after the change.

New Feature: HTML Disclaimers

With AsyncOS 7.5, you can create some text resources with both HTML-based and plain text messages. When the text resource is applied to an email message, the HTML-based text resource message is applied to the text/html part of the email message, and the plain text resource message is applied to the text/plain part of the email message.

Enhancement: Schedule Log Rollover

To prevent log files on the appliance from becoming too large, AsyncOS 7.5 performs a "rollover" and archives a log file when it reaches a user-specified maximum file size or time interval and creates a new file for incoming log data. For example, you can set up the appliance to perform rollovers every night at midnight to archive a day's worth of logs. You can configure rollovers to be performed hourly, daily, or on certain days of the week.

Enhancement: Manually Download Logs Using HTTP/HTTPS

With AsyncOS 7.5, you can now access log files at any time by clicking a link to the log directory on the Log Subscriptions page, then clicking the log file to access. Depending on your browser, you can view the file in a browser window or open or save it as a text file. This method uses the HTTP(S) protocol and is the default retrieval method.

Note Using this method, you cannot retrieve logs for any computer in a cluster, regardless of level (machine, group, or cluster), even if you specify this method in the CLI.

Enhancement: Service Updates Enhancements

The Email Security appliance now automatically updates to the following services:

- IronPort Anti-Spam and Intelligent Multi-Scan rules
- Sophos anti-virus definitions
- Time zone updates

You can manage the update settings using the Service Updates page.

Enhancement: IP-Based Access Through a Proxy

If your organization's network uses reverse proxy servers between remote users' machines and the Email Security appliance, AsyncOS 7.5 allows you create an access list with the IP addresses of the proxies that can connect to the appliance.

Enhancement: Web UI Session Timeout

In AsyncOS 7.5, you can specify how long a user can be logged into the Email Security appliance's Web UI before AsyncOS logs the user out due to inactivity. This Web UI session timeout applies to all users, including admin, and it is used for both HTTP and HTTPS sessions.

Note The Web UI Session Timeout does not apply to IronPort Spam Quarantine sessions.

Enhancement: Attachment Search Using Message Tracking

AsyncOS 7.5 now allows you to search for messages by attachment name in Message Tracking.

Enhancement: Reporting Enhancements

AsyncOS 7.5 includes enhanced reports that support selecting columns to display on tabular reports, selection of custom date ranges, and links in PDFs.

Enhancement: Internationalization of PDF Reports

New in AsyncOS 7.5, the Email Security appliance has the ability to generate localized PDF reports and properly render all non-ASCII/international symbols in PDF reports.

Enhancement: Default Availability of User Interface in Eleven Major Languages

AsyncOS 7.5 now allows you to select one of eleven major languages for the user interface of the GUI and CLI without the need for a feature key. The supported language are:

- English
- French
- Spanish
- German
- Italian

- Korean
- Japanese
- Portuguese (Brazil)
- Chinese (zh-cn and zh-tw)
- Russian

New and Updated CLI Commands

AsyncOS 7.5 adds new CLI commands and updates some existing ones. See the *Cisco IronPort AsyncOS CLI Reference Guide* for more information on these commands.

Table 1-3 New and Updated Commands

Command Name	Description
outbreakconfig	Configure Outbreak Filters (formerly `vofconfig`)
outbreakflush	Clear the cached Outbreak Rules (formerly `vofflush`)
outbreakstatus	Display current Outbreak Rules (formerly `vofstatus`)
outbreakupdate	Update Outbreak Filters rules (formerly `vofupdate`)
redirectrecipients	Redirect all messages to another relay host
showrecipients	Show messages from the queue
sievechar	Configure characters for Sieve Email Filtering
tzupdate	Update timezone rules
updatenow	Update all components

Installation Notes

Preupgrade Notes

Please be aware of the following upgrade impacts:

AsyncOS Upgrades and Service Updates Use Same Update Server

In previous versions of AsyncOS, AsyncOS upgrades, PXE Engine updates, and McAfee Anti-Virus definitions could use a different update server than services such as IronPort Anti-Spam rules and Feature Key rules. In AsyncOS 7.5.1, AsyncOS upgrades use the same update server as all of the service updates, whether it's an IronPort update server or a local update server. This will prevent you from using a local server for AsyncOS upgrades and an IronPort update server for all other service updates unless you configure the appliance to use a manifest on a local appliance to perform an AsyncOS upgrade and the re-configure the appliance to use an IronPort update server for the other services after the upgrade is complete.

Re-enable SNMP

SNMP does not start when you boot the appliance after upgrading to AsyncOS 7.5.1. Use **snmpconfig -> setup** and then **commit** to enable it.

SNMP Monitoring: More Open Files

If you are monitoring Email Security appliances using SNMP, the number of open files will increase to around 2500 after upgrading the appliance to AsyncOS 7.5.1.

Email Authentication

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

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

Configuration Files

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

Received Headers

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

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

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

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

Feature Keys

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

Upgrading to the AsyncOS 7.5.1 Release

For the AsyncOS 7.5.1 release, please use the following instructions to upgrade your Email Security appliance.

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

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

Step 3 Suspend all listeners.

Step 4 Wait for the queue to empty.

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

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

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

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

Step 9 Resume all listeners.

Performance Advisory

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

DomainKeys - DomainKeys signing outgoing email can cause a decrease in the message throughput capacity. Using smaller signing keys (512 byte or 768 byte) can mitigate this.

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

Outbreak Filters - Outbreak Filters 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 can upgrade to release 7.5.2-014 from the following versions:

- 7.1.5-101
- 7.5.1-102

Fixed Issues in Release 7.5

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

Table 4 Resolved Issues in Version 7.5

Defect ID	Description
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 has been resolved in AsyncOS 7.5.
67341	**Fixed: Cannot Save Regional Settings for IronPort Anti-Spam and IMS for Clustered Appliance.** Previously, you could not save changes to the Regional Settings for IronPort Ant-Spam or IronPort Intelligent Multi-Scan via the GUI when a clustered Email Security appliance was in cluster or group mode. This issue has been resolved. Now, you can save the Regional Settings for the appliance at the cluster, group, or machine level as well as standalone mode.
68527	**Fixed: Misleading Message When Trying to Run DLP Assessment Wizard in Cluster Mode.** Previously, AsyncOS displayed an incorrect error message when you attempted to run DLP Assessment Wizard a clustered environment, stating that the wizard must be run from the “login host” level. This error message has been corrected. The message now correctly states that the appliance must be removed from the cluster to run the DLP Assessment Wizard.
29829	**Fixed: updateconfig Command Does Not Allow User to Specify Interface for Certain Service Updates.** Previously, you could not correctly apply which of IP interfaces assigned to the same physical network interface to use when connecting to the update server. That was a reason of failed updates/upgrades. This issue has been resolved. Now, when you run the updateconfig -> setup command and choose which particular IP interface connects to the update server the selected IP interface is applied properly and updates/upgrades are always completed successfully.

Table 4 Resolved Issues in Version 7.5 (continued)

Defect ID	Description
71406	**Fixed: Error Occurs When Using the Default Client or Server IP Address for the packetcapture Predefined Filter.** Previously, configuring the client and server IPs addresses for the **packetcapture** feature's predefined filter could result in a configuration error. The error occurred if an IP address was specified for one of the client or server IP addresses and the default address was used for the other. For example, if your configuration specified an IP address for the client IP but used the default IP address for the server IP. In these cases, AsyncOS saved a comma-separated string value for the **packetcapture** configuration instead of a list, which resulted in a error message after saving. This issue has been resolved. When configuring packetcapture in AsyncOS 7.5, the system uses a comma-separated string for the client and server IP addresses. However, AsyncOS 7.5 cannot fix a broken, existing XML configuration as there is no single way to fix the broken packetcapture settings. These settings may let the loadconfig fail or result into loading inappropriate settings for client or server IP addresses. The packetcapture will fail to start with these settings and user will have to manually correct settings using `packetcapture -> setup` command.
52692	**Fixed: Cannot Reject Connections from localhost.** Previously, you could not configure the Host Access Table (HAT) to reject connections from the localhost. This issue has been resolved. You can now use **localhost** as a hostname in HAT and can configure HAT to reject connections from the localhost.
66543	**Fixed: Message Tracking Does Not Display Any Message Details After Upgrading and Changing the Time Zone.** After changing the time zone in previous versions of AsyncOS, the Message Tracking page did not display any details when you clicked Show Details for a message. All message details values were blank or **NA**. This issue has been resolved in AsyncOS 7.5.

Table 4 Resolved Issues in Version 7.5 (continued)

Defect ID	Description
68278	**Fixed: Internet Explorer 7 Displays Error Messages for System Upgrade Page.** When you opened the System Upgrade page of a previous version of AsyncOS in Internet Explorer 7, IE7 displayed an "Object Required" error in the status bar at the bottom of the browser window. If you selected a version of AsyncOS and click Begin Upgrade, AsyncOS displayed an "Upgrade failure" error message, but AsyncOS was actually upgrading the appliance and displayed the upgrade progress below the error message. This issue has been resolved. AsyncOS 7.5 does not display these incorrect error messages.
68337	**Fixed: AsyncOS Saves Exported PKCS#12 Certificate with .cer Extension.** Fixed an issue where exporting a PKCS#12 certificate from the Certificates > Export Certificate page saved the certificate with the .cer extension instead of .p12. Now, saving the certificate file using Firefox or Internet Explorer with the filename specified by the user and the content type of **application/x-pkcs12**. Saving the certificate using Safari automatically adds the .p12 extension.
76977	**Fixed: CLI displays "Unknown Command" Error When User Enters a Command for an Expired Feature** Previously, the CLI displayed an `Unknown command: [command name]` error message if a user entered a command for a feature that has an expired feature key. This message has been updated to state `Unknown command or missing feature key: [command name]` in order to notify the customer that either the command is missing or the key for this feature has expired.
38480	**Fixed: Batch Command Allows Multiple Domain Profiles with Same Users** In previous versions of AsyncOS for Email, you could using the `domainkeysconfig` batch command in the CLI to create multiple domain profiles with the same users. For example, running `domainkeysconfig profiles new new1 dk qa47.qa san all` followed by `domainkeysconfig profiles new new2 dk qa47.qa san all` would create two domain profiles, new1 and new2, with the same users. This issue has been resolved. AsyncOS now displays an error message if you attempt to create a domain profile with the same users as an existing profile.

Table 4 Resolved Issues in Version 7.5 (continued)

Defect ID	Description
76378	**Fixed: Configuration File Fails to Load Due to Domain Profiles Duplication** Previously, AysncOS for Email would not load a configuration file if multiple domain profiles used the "all" wildcard to specify the users assigned to the profiles. This issue existed due to issue 38480. The resolution of issue 38480 prevents this issue from occurring.
71976	**Fixed: Removing a Disk from C150, C160 or C170 RAID May Prevent Appliance from Rebooting** Previously, removing a disk from a RAID set in the C150, C160, or C170 and then reinstalling it may have prevented a C150, C160, or C170 appliance from rebooting after the RAID rebuild was completed. This issue no longer occurs.
72770	**Fixed: Alternate DNS Authority Entries Are Case-Sensitive** Fixed an issue where AsyncOS for Email treated the hostnames for alternate DNS authorities as case-sensitive. These entries are now treated as case-insensitive.

Known Issues

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

Table 5 Known Issues in AsyncOS 7.5.1

Defect ID	Description
78019	**AsyncOS Upgrades and Service Updates Use Same Update Server** In previous releases, AsyncOS upgrades, PXE Engine updates, and McAfee Anti-Virus definitions could use a different update server than services such as IronPort Anti-Spam rules and Feature Key rules. In AsyncOS 7.5, AsyncOS upgrades use the same update server as all of the service updates, whether it's an IronPort update server or a local update server. This will prevent you from using a local server for AsyncOS upgrades and an IronPort update server for all other service updates unless you configure the appliance to use a manifest on a local appliance to perform an AsyncOS upgrade and the re-configure the appliance to use an IronPort update server for the other services after the upgrade is complete.
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.
72847	**Modifying Certificate Reinitializes All Interfaces.** If you modify the HTTPS certificate on any interface, AsyncOS reinitializes all existing interfaces on the appliance. During the initialization, which is usually less than a second, network errors are seen while interfaces reinitialize and alerts are sent. Work around: Cisco IronPort recommends suspending listeners and delivery on the appliance before modifying the HTTPS certificate on an interface, then resuming listeners and delivery.
75458, 48023	**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.

Table 5 Known Issues in AsyncOS 7.5.1

Defect ID	Description
51884	**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.
72365	**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. Work around: Use the `antispamupdate ironport force` command to force a CASE engine update.
76151	**Commit Changes Button Highlighted After Upgrading from 7.0.0-702 and Uploading Config File.** The Commit Change button is highlighted after you upgrade the appliance to AsyncOS 7.5 from version 7.0.0-702 and then save and load the configuration file. Normally, you do not have to commit changes after loading the configuration file. In this case, Cisco IronPort recommends committing the changes after loading the configuration file.
75774	**Log Subscriptions Show Incorrect Hostname for Manual Log Retrieval.** The New and Edit Log Subscriptions pages in the GUI show the incorrect hostname for the “Manually download logs” retrieval method shows the hostname for which FTP is enabled, not the hostname for which HTTP is enabled.
71565	**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

Table 5 Known Issues in AsyncOS 7.5.1

Defect ID	Description
76201	**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.
75046	**Using a Virtual Gateway Hostname for a Received Header May Prevent DKIM Signing** AsyncOS for Email may not sign outgoing messages using DKIM if the appliance uses a Virtual Gateway hostname in the received header. The C300D, C350D, C360D, and C370D appliances use a Virtual Gateway hostname in the received header by default. Cisco recommends using the hostname of the interface that received the message in the received header to guarantee that the appliance signs messages using DKIM.
76940	**Using IronPort Mail Merge Variables in a Message May Prevent DKIM Signing** Using IronPort Mail Merge (IPMM) variables for outgoing messages may invalidate the DKIM signature for any signed messages that are altered by IPMM. IPMM is only used on C300D, C350D, C360D, and C370D appliances.
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.
77609	**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.

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

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.