Release Notes for *Cisco IronPort AsyncOS 7.3.2 for Email*

Published: March 26, 2012

Contents

These release notes contain information critical to upgrading and running Cisco IronPort AsyncOS 7.3.1 for Email, including hardware-specific information and known issues.

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

What's New in Cisco IronPort AsyncOS 7.3.2 for Email

This section describes the new features in Cisco IronPort AsyncOS 7.3.2 for Email release.

SMTP Session Authentication Using Client Certificates

AsyncOS 7.3.2 adds support for using client certificates to authenticate SMTP sessions between the Email Security appliance and users' mail applications. The Email Security appliance can request a client certificate from a user's mail application when it attempts to connect to the appliance to send messages. The certificate is sent to the appliance, which verifies that the certificate is valid, has not expired, and has not been revoked. If the certificate is valid, the Email Security appliance allows an SMTP connection from the mail application over TLS.

Organizations that require their users to use a Common Access Card (CAC) for their mail applications can use this feature to configure the Email Security appliance to request a certificate that the CAC and ActivClient middleware application then provides to the appliance.

You can configure the Email Security appliance to require users to provide a certificate it when sending mail, but still allow for special circumstances for certain users. For these users, you can configure the appliance to use the SMPT AUTH command to authenticate them, if you choose.

Users must configure their mail application to send messages through a secure connection (TLS) and accept a client certificate from the mail application.

This new feature includes the following updates:

- **Certificate Authentication LDAP Query.** This new LDAP query checks the validity of a client certificate in order to authenticate an SMTP session between the user's mail client and the Email Security appliance. When creating this query, you select a list of certificate fields for authentication, specify the User ID attribute (the default is `uid`), and enter the query string.

For example, a query string that searches for the certificate's common name and serial number may look like `(&(objectClass-posixAccount)(caccn={cn})(cacserial={sn})`. After you have created the query, you can use it in a Certificate SMTP Authentication Profile. This LDAP query supports OpenLDAP, Active Directory, and Oracle Directory.

- **SMTP Authentication LDAP Query.** AsyncOS 7.3.2 adds an Allowance Query String to this query type, which allows the Email Security appliance to check whether the user's mail application is allowed to use the SMTP AUTH command to connect to the appliance. This query string should check for the user's ID in the directory. You can also filter out results based on other attributes. For example, the query string `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))` checks to see if any of the following conditions are true for the user:
  - CAC is not issued to the user (`caccn=*`)
  - CAC is exempt (`cacexempt=*`)
  - the time period that a user may temporarily send mail without a CAC expires in the future (`cacemergency>={t}`)
- **SMTP Authentication Profile.** AsyncOS 7.3.2 adds a new Certificate type of SMTP authentication profile. This profile type allows the Email Security appliance to authenticate an SMTP connection over TLS using a client certificate. When creating the profile, you select the Certificate Authentication LDAP query to use for verifying the certificate. You can also specify whether the Email Security appliance falls back to the SMTP AUTH command to authenticate the user if a client certificate isn't available.
- **Mail Flow Policies.** A new TLS parameter has been added to mail flow policies: Verify Client Certificate. Selecting this option directs the Email Security appliance to verify that the user has a client certificate. If you select this option for the TLS Preferred setting, the appliance still allows a connection if the user doesn't have a certificate, but rejects the connection if the user has an invalid certificate. For the TLS Required setting, selecting this option requires the user to have a valid certificate in order for the appliance to allow the connection.
- **CRL Sources.** The Email Security appliance checks a list of revoked certificates (called a Certificate Revocation List) as part of its certificate verification to make sure that the user's certificate hasn't been revoked. To

configure this option, specify the name and filetype of the Certificate Revocation List, the URL of the server hosting the file, and a schedule for when the appliance will download the latest version of the file.

- **Inbound SMTP Authentication Report.** This new report displays information on the number of connections with client certificates and the SMTP AUTH command and the number of authenticated and non-authenticated messages sent.

Authenticating a User's SMTP Session With a Client Certificate

Step 1 Go to **System Administration > LDAP** to configure an LDAP server profile.

Step 2 Define a certificate query for the LDAP profile.

a. Enter the query name.

b. Choose the certificate fields to authenticate, such as the serial number and common name.

c. Enter the query string. For example, `(&(caccn={cn})(cacserial={sn}))`.

d. Enter the user ID field, such as `uid`.

e. Submit your changes.

Step 3 Go to **Network > SMTP Authentication** to configure a Certificate SMTP authentication profile.

a. Enter the profile name.

b. Select the certificate LDAP query you want to use.

c. Do not select the option to allow the SMTP AUTH command if a client certificate is not available.

d. Submit your changes.

Step 4 Go to **Network > Listeners** to configure a listener to use the certificate SMTP authentication profile that you created.

Step 5 Modify the RELAYED mail flow policy to require TLS and a client certificate, as well as require SMTP authentication.

Note Although SMTP authentication is required, the Email Security appliance will not use the SMTP AUTH command because it is using certificate authentication. The Email Security appliance will require a client certificate from the mail application to authenticate the user.

Step 6 Submit and commit your changes.

Authenticating a User's SMTP Session with the SMTP AUTH Command

The Email Security appliance can use the SMTP AUTH command to authenticate a user's SMTP session instead of a client certificate. If you user is not allowed to use SMTP AUTH for their connection, you can select whether the appliance rejects the connection or temporarily allows it while logging all activity.

Step 1 Go to **System Administration > LDAP** to configure an LDAP server profile.

Step 2 Define an SMTP authentication query for the LDAP profile.

- **a.** Enter the query name.
- **b.** Enter the query string. For example, `(uid={u})`.
- **c.** Select LDAP Bind for the authentication method.
- **d.** Enter an allowance query string. For example, `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t}))).`
- **e.** Submit your changes.

Step 3 Go to **Network > SMTP Authentication** to configure an LDAP SMTP authentication profile.

- **a.** Enter the profile name.
- **b.** Select the SMTP authentication LDAP query you want to use.
- **c.** Select the Check with LDAP if user is allowed to use SMTP AUTH Command and choose to monitor and report the user's activity.
- **d.** Submit your changes.

Step 4 Go to **Network > Listeners** to configure a listener to use the LDAP SMTP authentication profile that you created.

Step 5 Modify the RELAYED mail flow policy to require TLS and SMTP authentication.

Step 6 Submit and commit your changes.

Authenticating a User's SMTP Session with Either a Client Certificate or SMTP AUTH

This configuration requires the Email Security appliance to ask for a client certificate from users with a client certificate while allowing SMTP AUTH for users without one, or who cannot use one for sending email.

Any attempt to use the SMTP AUTH command by a user who is not allowed will be prohibited.

Step 1 Go to **System Administration > LDAP** to configure an LDAP server profile.

Step 2 Define an SMTP authentication query for the profile.

- **a.** Enter the query name.
- **b.** Enter the query string. For example, `(uid={u})`.
- **c.** Select LDAP Bind for the authentication method.
- **d.** Enter an allowance query string. For example, `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t}))).`

Step 3 Define a certificate query for the LDAP profile.

- **a.** Enter the query name.
- **b.** Choose the client certificate fields to authenticate, such as the serial number and common name.
- **c.** Enter the query string. For example, `(&(caccn={cn})(cacserial={sn}))`.
- **d.** Enter the user ID field, such as `uid`.
- **e.** Submit your changes.

Step 4 Go to **Network > SMTP Authentication** to configure an LDAP SMTP authentication profile.

- **a.** Enter the profile name.
- **b.** Select the SMTP authentication LDAP query you want to use.

c. Select the Check with LDAP if user is allowed to use SMTP AUTH Command and choose to reject the connection.

d. Enter a custom SMTP AUTH response. For example, `525, "Dear user, please use your CAC to send email."`

e. Submit your changes.

Step 5 Configure a Certificate SMTP authentication profile.

a. Enter the profile name.

b. Select the certificate LDAP query you want to use.

c. Select the option to allow the SMTP AUTH command if a client certificate is not available.

d. Select your LDAP SMTP authentication profile for the appliance to use if the user does not have a client certificate.

e. Submit your changes.

Step 6 Go to **Network > Listeners** to configure a listener to use the certificate SMTP authentication profile you created.

Step 7 Modify the RELAYED mail flow policy to select the following options:

- TLS Preferred
- SMTP authentication required
- Require TLS for SMTP Authentication

Step 8 Submit and commit your changes.

Retrieving a Certificate Revocation List

Step 1 Go to **Network > CRL Sources**.

Step 2 Under Global Settings, enable CRL checking for inbound SMTP TLS connections.

Step 3 Click Add CRL Source:

Step 4 Enter a name for the CRL source.

Step 5 Select the file type. This can be either ASN.1 or PEM.

Step 6 Enter the URL for the primary source for the file, including the filename. For example, `https://crl.example.com/certs.crl`

Step 7 Optionally, enter the URL for a secondary source in case the appliance cannot contact the primary source.

Step 8 Specify a schedule for downloading the CRL source.

Step 9 Enable the CRL source.

Step 10 Submit and commit your changes.

What's New in Cisco IronPort AsyncOS 7.3.1 for Email

This section describes the issues resolved in the Cisco IronPort AsyncOS 7.3.1 for Email release.

Fixed Issues

Table 1 Fixed Issues in Version 7.3.1

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
75758, 75761	**Fixed: FIPS-Compliant Appliance Only Partially Resets After Third Failed Login Attempt** Fixed an issue where a FIPS-compliant Email Security appliance was only partially reset after the third failed login attempt from an SSH connection to the CLI and the appliance was not accessible by SSH or HTTPS. This issue has been resolved. Now, after the third failed login attempt in a row, the appliance deletes its certificates, resets the HSM card, and schedules a system reboot before closing the SSH connection.
81754	**Fixed: TLS Traffic Causing Email Processing to Restart or Become Unresponsive** The DigiNotar blacklist solution added in the previous release 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.
74547	**Fixed: Scanning Engine Restarts If It Exceeds Memory Limit** Fixed an issue where the Email Security appliance's content scanning engine ran 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 no longer occurs.

Table 1 Fixed Issues in Version 7.3.1 (continued)

Defect ID	Description
75324	**Fixed: Fiber IP Interfaces Disappear after Revert** Fixed an issue where the IP interfaces for the ports on the appliance's fiber card disappeared after you reverted the appliance to an earlier version of the software.
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.
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.
22164, 67958	**Fixed: Regular Expression that Exceeds Data Limit Invalidates Message Filter** Previously, if certain header 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.
69693	**Fixed: External User Authentication Fails Because Appliance Sends Demo Certificate to LDAP Server** Previously, if you configure the appliance to connect to an LDAP server using SSL in order to authenticate external users, the appliance would send the LDAP server AsyncOS's demo certificate instead of a certificate you uploaded to the appliance. 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.

Table 1 Fixed Issues in Version 7.3.1 (continued)

Defect ID	Description
31279	**Fixed: NIC Pairing and VLAN Not Supported by Packet Capture Feature** The Packet Capture feature in AsyncOS 7.3.1 now supports NIC Pairing and VLAN when configuring the feature using the CLI or GUI.
72977	**Fixed: Application Fault Occurs When Adding a FIPS Log Using Web UI** Fixed an issue where an application fault occurred when adding a FIPS log subscription using the Log Subscriptions page in the Web UI.
72658	**Fixed: Content Scanning Engine Times Out When Scanning Corrupted PDFs** The content scanning engine in previous versions of AsyncOS would time out when scanning certain corrupted PDFs. This no longer occurs. AysncOS 7.3.1 includes an updated version of the content scanning engine that returns an error message when it scans a corrupted PDF.
44537	**Fixed: Unable to Detect .exe files Embedded in Microsoft Excel 1997 Documents** Previously, when .exe files were embedded in Microsoft Excel 1997 documents, the content scanning engine was unable to detect the .exe attachment using the attachment-filetype == "Executable" filter condition. This issue has been resolved.
43951	**Fixed: Content Scanning Engine Does Not Detect Microsoft Office 2007 Documents as Password-Protected** Previously, the scanning engine was unable to detect Microsoft Office 2007 attachments as password-protected using the attachment-protected filter condition. This issue has been resolved.
73306	**Fixed: text/rfc822-headers Caused Scanning Engine to Time Out** Fixed an issue in which the presence of text/rfc822-headers in a message sometimes caused the message scanning engine to time out.
74482	**Fixed: CLI Can be used to Access Machine-level Prompt.** Fixed an issue in which users in certain groups were able to access a machine-level command prompt.
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 1 Fixed Issues in Version 7.3.1 (continued)

Defect ID	Description
67268	**Fixed: Scanning Engine Unable to Scan OpenOffice .odt files** Fixed an issue in which a content filter with a body scanning condition defined in the dictionary was unable to match the term in OpenOffice .odt files. This issue has been addressed.
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.
75582	**Fixed: "Legacy mailflow report" setting is not retained in saved configuration files** The "Legacy mailflow report" setting is now retained in the configuration file and this setting will now be correctly set when the configuration file is loaded.
74268	**Fixed: Use of persistent cookies by the web interface creates a security vulnerability** Persistent cookies stored on the user's hard disk included a session identifier and whether or not the user was logged in. The Email Security appliance web user interface now uses temporary (session) cookies for this information, which do not present the same risk.
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.
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.

Table 1 Fixed Issues in Version 7.3.1 (continued)

Defect ID	Description
45990	**Fixed: PDF with no document open password triggers attachment-protected rule in message filter** If a message filter was set up to catch messages with attachments that require a password in order to open them, messages with PDF attachments that did not include password protection, but may have included other restrictions, were caught by the filter. This no longer occurs.
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.

What's New in Cisco IronPort AsyncOS 7.3 for Email Hot Patch Release

This section describes the issues resolved in the Cisco IronPort AsyncOS 7.3 for Email hot patch release.

Fixed Issues

Table 2 Resolved Issues in Version 7.3.1 Hot Patch Release

Defect ID	Description
73455	**Fixed: IP Address Logged for Successful and Unsuccessful Logins** AsyncOS 7.3 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 7.3 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.

What's New in Cisco IronPort AsyncOS 7.3 for Email

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

New Feature: FIPS Compliance

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

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

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

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

Software Notes

Please be aware of the following software impacts:

Security Management Appliances That Are Not FIPS Compliant

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

FIPS Officer Password

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

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

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

Configuration Files

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

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

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

The Backup and Restore page is displayed.

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

Step 3 Click **Backup**.

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

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

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

Committing Changes in AsyncOS 7.3

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

Console Serial Port Timeout

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

Security Management Appliances Discard Reporting Data for DLP and Marketing Mail

IronPort Security Management appliances running AsyncOS 6.7.3 or earlier do not support reporting data for the DLP and Marketing Mail features in AsyncOS 7.0 or later. If your IronPort Email Security appliance uses centralized reporting, the Security Management appliance discards the reporting data for those features. If the Security Management appliance is running AsyncOS 6.7.0 or 6.7.3, it sends an alert once each time the reporting service begins, such as on a reboot, stating that the reporting service is receiving data that it cannot process.

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

Email Authentication

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

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

Received Headers

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

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

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

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

Feature Keys

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

Upgrading to the AsyncOS 7.3 Release

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

Performance Advisory

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

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

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

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

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

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

Upgrade Paths

You can upgrade to release 7.3.2-023 from the following versions:

- 7.3.1-101
- 7.3.2-017

Fixed Issues

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

Table 3 Resolved Issues in Version 7.3

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.
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.
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.
71152	**Fixed: Loading a Configuration file from Previous Appliance to a C670, or X1070 Takes It Offline After Reboot.** Fixed an issue where a C670 or X1070 appliance that had configuration files imported from a previous generation IronPort appliance, such as a X1060 or C660, would go offline after a reboot. Please note that Cisco IronPort does not support the loading of a configuration file from one appliance model to another.
67137	**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.

Table 3 Resolved Issues in Version 7.3 (continued)

Defect ID	Description
55972	**Fixed: TLS/SSL Man-in-the-Middle Vulnerability.** Previously, an industry-wide vulnerability that existed in the TLS protocol potentially impacted any Cisco product using any version of TLS /SSL. The vulnerability existed in how the protocol handles session re-negotiation and exposed users to a potential Man-in-the-middle attack. This issue has been fixed.
70522 55358	**Fixed: DKIM Signing and Verification Create Memory Leak.** Fixed an issue where DKIM signing and verification created large amounts of unclaimed data in the appliance's RAM, which could have resulted in the appliance running out of memory.
69429	**Fixed: CASE No Longer Updates After Hitting a Timeout.** Previously, AsyncOS stopped attempting to update the Context Adaptive Scanning Engine (CASE) after hitting an update timeout. No more CASE updates would arrive, even after trying to force an update via the CLI. This issue has been resolved. AsyncOS will continue to do further updates to CASE after a timeout.

Known Issues

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

Table 4 Known Issues in AsyncOS 7.3

Defect ID	Description
84647	**False Warning for LDAP Certificate** If you upgrade the appliance from version 7.3.1-101, the LDAP page in the GUI incorrectly displays a warning message saying that the system has reverted the certificate settings for LDAP to System Default because the previous certificate was deleted. This message is incorrect. The previous certificate was not deleted from the system, but you will need to commit and save.
85006	**Verify Client Certificate Checkbox Disabled in Non-Default Mail Flow Policy** If TLS is set to Preferred or Required in the default mail flow policy and if a non-default mail flow policy is set to Use Default for TLS, you will not be able to check the Verify Client Certificate checkbox as it will be disabled. However, the Email Security appliance will verify the client certificate even though the checkbox is disabled.
84826	**Some GUI Controls Not Selectable in Internet Explorer 8** Internet Explorer 8 does not render some GUI controls properly on a few pages. These controls are supposed to become "enabled" after you select a check box, but in IE 8, these controls remain disabled. These controls are: • **Network > SMTP Authentication > LDAP-Based SMTP Authentication Profile.** The **Monitor** and **Reject** options and **Specify a custom SMTP response to be used when a SMTP AUTH command is disallowed** check box are not enabled when you select **Check with LDAP if user is allowed to use SMTP AUTH Command**. • **Network > SMTP Authentication > Certificate-Based SMTP Authentication Profile.** The **Specify LDAP or Forward Type SMTP Auth Profile** dropdown list is not enabled when you select **Allow SMTP AUTH command if client certificate is not available**. • **Network > CRL Sources**. The options to schedule the CRL download are not enabled when you select **Enable Scheduled auto update of CRL file**.

Table 4 Known Issues in AsyncOS 7.3

Defect ID	Description
72144	**Connection Not Redirecting to HTTPS After Initialization.** Some SSH clients and web browsers automatically lose the SSH or HTTPS connection when the HSM initializes or when the wrong password is entered three times. If a user enters the wrong password three times via SSH, attempting to log back into the appliance via HTTP will result in an error message because the connection will not redirect to HTTPS. In these cases, the administrator must manually reboot the appliance by powering it off and on.
79296	**Appliance May Become Unresponsive** A C660, C670, X1060, or X1070 appliance may become unresponsive after processing a high amount of message traffic with large attachments over an extended period of time. This issue requires 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 causes the appliance to become unresponsive.
71994	**Host Key Cannot Be Updated For Individual Logs via the GUI.** Instead of updating the SSH host key for SCP push for an individual log, manually entering an SSH host key using a log subscription's GUI page actually updates the host key for all logs which are configured to SCP push to the given host.
71712	**CLI Displays Host Key Error Messages During Cluster Creation.** When creating a cluster of appliances running AsyncOS 7.3, the CLI displays error messages stating that the `/etc/ssh/ssh_host_key.pub` and `/etc/ssh/ssh_host_dsa_key.pub` system host keys cannot be opened. These host keys listed do not exist on the appliance. Cisco IronPort advises you to ignore these error messages.
68368	**Reconnect Link in GUI Does Not Reconnect Machines.** The "reconnect" link in the GUI does not reconnect machines that were disconnected from a cluster unless the machines were disconnected from the cluster individually. Workaround: Use the `clusterconfig -> reconnect` command in the CLI to reconnect the machines.
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.

Table 4 Known Issues in AsyncOS 7.3

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.
71712	**CLI Displays Host Key Error Messages During Cluster Creation.** When creating a cluster of appliances running AsyncOS 7.3, the CLI displays error messages stating that the `/etc/ssh/ssh_host_key.pub` and `/etc/ssh/ssh_host_dsa_key.pub` system host keys cannot be opened. These host keys listed do not exist on the appliance. Cisco IronPort advises you to ignore these error messages.
68368	**Reconnect Link in GUI Does Not Reconnect Machines.** The "reconnect" link in the GUI does not reconnect machines that were disconnected from a cluster unless the machines were disconnected from the cluster individually. Workaround: Use the `clusterconfig -> reconnect` command in the CLI to reconnect the machines.
79555	**Scanning Engine Does Not Recognize Some Password-Protected PDFs** The Email Security appliance's content scanning engine may not recognize password-protected PDFs created using the Linux version of Open Office.

Related Documentation

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

- *Cisco IronPort AsyncOS for Email Daily Management Guide*. This guide provides instructions for performing common, everyday tasks that system administrators use to manage and monitor the IronPort appliance, such as viewing email traffic using the Email Security Monitor, tracking email messages, managing system quarantines, and troubleshooting the appliance. It also provides reference information for features that system administrators interact with on a regular basis, including Email Security Monitor pages, AsyncOS logs, CLI support commands, and quarantines.

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

Service and Support

You can request our support by phone, email, or online 24 hours a day, 7 days a week.

During customer support hours (24 hours per day, Monday through Friday excluding U.S. holidays), an engineer will contact you within an hour of your request.

To report a critical issue that requires urgent assistance outside of our office hours, please contact Cisco IronPort using one of the following methods:

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

International: http://cisco.com/web/ironport/contacts.html

Support Portal: http://cisco.com/web/ironport/index.html

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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