



Release Notes for *Cisco IronPort AsyncOS 7.1.1 for Email*

Published: May 20, 2010

Revised: June 9, 2010, OL-22161-02

Contents

These release notes contain information critical to upgrading and running Cisco IronPort AsyncOS 7.1.1 for Email, including hardware-specific information and known issues.

- [What's New in Cisco IronPort AsyncOS 7.1.1 for Email, page 2](#)
- [What's New in Cisco IronPort AsyncOS 7.1 for Email, page 3](#)
- [Installation Notes, page 7](#)
- [Upgrade Paths, page 10](#)
- [Fixed Issues, page 11](#)
- [Known Issues, page 12](#)
- [Related Documentation, page 14](#)
- [Service and Support, page 15](#)



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

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

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

Enhancement: New RSA Email DLP Policy Templates

AsyncOS 7.1.1 includes two new RSA Email DLP policy templates:

- **Massachusetts CMR-201.** Policies based on this template identify documents and transmissions that contain personally identifiable information regulated by Massachusetts CMR-201. Any person who owns, licenses, stores or maintains personal information about a resident of the Commonwealth of Massachusetts is required to protect against unauthorized access to or use of the information in a manner that creates risk of identity theft or fraud. The policy detects US Social Security numbers, global credit card numbers and US drivers license numbers.
- **Corporate Financials.** Policies based on this template identify documents and transmissions that contain financial information related to organizational accounting such as balance sheets, cash flow, income statements, key ratios, SEC information, and annual, quarterly, and transition reports.

Fixed Issues

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

- **Robustness Fixes for Lockups on C160 Appliances [Defect ID: 68955]**
AsyncOS 7.1.1 includes a series of robustness fixes and logging enhancements to address lockups that have occurred on C160 appliances.
- **Fixed: Extra Spaces in Footer When Forwarding via Outlook [Defect ID: 67312]**

Fixed an issue where extra line spaces were inserted into footer text when emails were forwarded using Outlook.

- Fixed: Demo Certificate Becomes Default TLS Certificate After Upgrading [Defect ID: 69456]

Previously, the Cisco Appliance Demo certificate became the default TLS certificate for LDAP, HTTPS, destination controls, and all listeners after upgrading the Email Security appliance to AsyncOS 7.1. This issue has been resolved. Custom certificates are not changed during the upgrade.

- Fixed: Email Processing Delay When Trying to Drop Viral Attachments When Using McAfee [Defect ID: 68615]

In AsyncOS 7.0 and 7.1, certain specific viral email attachments could cause delays in mail processing and queue backup issues, which could eventually lead to corruption of the email queue, if the appliance's mail policies used McAfee anti-virus scanning and the "Drop infected attachments if a virus is found and it could not be repair" option was enabled. This issue was resolved in AsyncOS 7.1.1.

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

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

Enhancement: DLP Assessment Wizard

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

Enhancement: TLS Enhancements

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

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

- **Certificate Authorities Management.** You can import a custom list of trusted certificate authorities onto the appliance, as well as disable and export the default system list.
- **TLS per Listener.** You can assign a unique certificate per listener on the appliance for TLS connections. You can also assign a certificate to the HTTPS services on an IP interface, the LDAP interface, and all outgoing TLS connections.
- **Batch Management.** You can import and export a Destination Controls configuration file that defines multiple destination domains using the GUI and CLI.
- **Troubleshooting Tools.** AsyncOS 7.1 provides new troubleshooting tools for TLS:
 - The `hoststatus` command has been enhanced to display the reason why the last outgoing TLS connection failed.
 - The `tlsverify` command has been added to create a TLS connection on demand. This allows an administrator to pinpoint the exact step a TLS connection failure occurs.
 - AsyncOS 7.1 records information on why a TLS connection attempt failed in the mail logs.

New Feature: Administrative Access Control List

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

New Feature: Login Banner

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

Enhancement: No Authentication Encryption Envelope

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

Enhancement: Packet Capture

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

Enhancement: Rescan Messages Released from Outbreak Quarantine

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

Enhancement: Suspend and Resume Mail Operations in the GUI

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

New Feature: signed-certificate() Filter Rule

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

Enhancement: Unpacking Opaque-Signed Messages

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

Enhancement: Retry Delivery in the GUI

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

Enhancement: New Message and Content Filter Actions

AsyncOS 7.1 adds two new message and content filter actions:

- **Add Log Entry.** This new message and content filter action inserts customized text into the IronPort Text Mail logs at the `INFO` level. The text can include action variables. The log entry also appears in message tracking.
- **Add Message Tag.** This new message and content filter action inserts a custom term into a message to use with RSA Email DLP policy filtering. You can configure a RSA Email DLP policy to limit scanning to messages with the message tag. The message tag is not visible to recipients.

Enhancement: New SPF Control Options in the CLI

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

Installation Notes

Preupgrade Notes

Please be aware of the following upgrade impacts:

Security Management Appliances Discard Reporting Data for DLP and Marketing Mail

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

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

Re-enable SNMP

SNMP does not start when you boot the appliance after upgrading to AsyncOS 7.1.1. Use `snmpconfig -> setup` and then `commit` to enable it.

Email Authentication

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

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

Configuration Files

IronPort does not generally support the backward compatibility of configuration files with previous major releases. AsyncOS 7.1 does not support configuration files from AsyncOS 7.0.1 or earlier.

Custom Notification Templates

If you previously used a custom notification template, headers were included by default. When you upgrade to AsyncOS version 5.0 or later, notification templates do not include headers by default. To include headers, you can add the `$allheaders` message filter action variable. [Defect ID: 27710]

Received Headers

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

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

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

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

Feature Keys

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

Upgrading to the AsyncOS 7.1.1 Release

For the AsyncOS 7.1.1 release, please use the following instructions to upgrade your Email Security appliance.

-
- Step 1** Save the XML configuration file off the IronPort appliance.
 - Step 2** If you are using the Safelist/Blocklist feature, export the Safelist/Blocklist database off the IronPort appliance.
 - Step 3** Suspend all listeners.
 - Step 4** Wait for the queue to empty.
 - Step 5** From the System Administration tab, select the System Upgrade page.
 - Step 6** Click the **Available Upgrades** button. The page refreshes with a list of available AsyncOS upgrade versions.
 - Step 7** Click the **Begin Upgrade** button and your upgrade will begin. Answer the questions as they appear.
 - Step 8** When the upgrade is complete, click the **Reboot Now** button to reboot your IronPort appliance.
 - Step 9** Resume all listeners.

Performance Advisory

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

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

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

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

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

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

Upgrade Paths

Version 7.1.1-012 is the AsyncOS 7.1.1 release of the Cisco IronPort AsyncOS for Email operating system.

The qualified upgrade paths to this release are:

- From: Version 6.5.3-014 to Version 7.1.1-012.
- From: Version 6.6.1-016 to Version 7.1.1-012.
- From: Version 7.0.0-702 to Version 7.1.1-012.
- From: Version 7.0.1-010 to Version 7.1.1-012.
- From: Version 7.0.1-013 to Version 7.1.1-012.

- From: Version 7.0.1-101 to Version 7.1.1-012.
- From: Version 7.0.1-102 to Version 7.1.1-012.
- From: Version 7.0.2-007 to Version 7.1.1-012.
- From: Version 7.1.0-104 to Version 7.1.1-012.
- From: Version 7.1.1-011 to Version 7.1.1-012.

Fixed Issues

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

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

Previously, entering an invalid regular expression for a RSA Email DLP policy caused an application fault that halted DLP scanning even if the regular expression was later corrected. While the AsyncOS GUI validates regular expressions, it may not catch all errors. There were two known regular expression errors that could cause this application fault:

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

This issue has been resolved. The AsyncOS GUI now tests for the above regular expression errors.

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

Previously, the DLP Matched Content tab on the Message Tracking Details page erroneously displays masking backslashes preceding single quotation marks in content matching classifiers. For example, "b'lād"e ' ' '2" appears as "b\lād"e\ ' \ '2\ ". This issue has been resolved.

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

Previously, an application fault occurred when switching between different cluster levels on the Encryption Profile page in the GUI. This issue has been resolved.

- Fixed: Corrupted Uuencoded Content Results in Warning and Skipped Filters [Defect ID: 37164]

Previously, a message with a corrupted uuencoded attachment caused the Email Security appliance to skip message filters processing and record a warning in the mail logs. This issue has been resolved. Now, the appliance applies filters to messages with corrupted uuencoded content.

Known Issues

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

Anti-Virus Issues

- Sophos Anti-Virus Unable to Scan PDFs with Large Cross-Reference Tables [Defect ID: 68899]

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.

Clustering Issues

- Cannot Save Regional Settings for IronPort Anti-Spam and IMS for Clustered Appliance [Defect ID: 67341]

You cannot save changes to the Regional Settings for IronPort Ant-Spam or IronPort Intelligent Multi-Scan via the GUI when a clustered Email Security appliance is in cluster or group mode. Workaround: Set the Regional Settings for IronPort Anti-Spam or IMS using the CLI instead of the GUI.

- Reconnect Link in GUI Does Not Reconnect Machines [Defect ID: 68368]

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.

- Misleading Message When Trying to Run DLP Assessment Wizard in Cluster Mode [Defect ID: 68527]

The DLP Assessment Wizard cannot be run in a clustered environment. However, if you attempt to run the wizard when logged into a clustered appliance in any mode other than the login host mode, AsyncOS displays an error message stating that the wizard is only available in login host mode. If you switch to login host mode, AsyncOS displays an error message stating that the DLP Assessment Wizard cannot be run on a clustered machine. The machine must be removed from the cluster in order to run the wizard.

DLP Issues

- Renaming Encryption Profile Doesn't Update DLP Policy [Defect ID: 68556]

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.

Workaround: After you rename the encryption profile, go to the DLP Policy manager and open the DLP policy. Select the renamed encryption profile. Submit the DLP policy and commit the changes. If you do not submit the DLP policy, AsyncOS will not update it with the renamed encryption profile.

Upgrading Issues

- Message Tracking Does Not Display Any Message Details After Upgrading and Changing the Time Zone [Defect ID: 66543]

After upgrading the appliance to AsyncOS 7.0.1 or later and changing the time zone on the appliance, the Message Tracking page does not display any details when you click Show Details for a message. All message details values are blank or NA. Workaround: Use the Printable PDF option to view the message details.

- Non-Default Administrator Can Reset Configuration Using System Setup Wizard [Defect ID: 67160]

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.

- Internet Explorer 7 Displays Error Messages for System Upgrade Page [Defect ID: 68278]

When you open the System Upgrade page in Internet Explorer 7, IE7 displays an "Object Required" error in the status bar at the bottom of the browser window. If you select a version of AsyncOS and click Begin Upgrade, AsyncOS displays an "Upgrade failure" error message, but AsyncOS is actually upgrading the appliance and displays the upgrade progress below the error message. Workaround: Ignore the error messages and continue with the upgrade.

Other Issues

- AsyncOS Saves Exported PKCS#12 Certificate with .cer Extension [Defect ID: 68337]

When exporting a PKCS#12 certificate from the Certificates > Export Certificate page in the GUI, AsyncOS saves the certificate with the .cer extension instead of .p12.

- LDAP Doesn't Renew Connection After Certificate is Removed from Appliance [Defect ID: 69838]

The Email Security appliance does not renew its connection to the LDAP server if the security certificate assigned to the LDAP interface is removed from the appliance after the connection was established. Workaround: Reboot the Email Security appliance to release the connection.

Related Documentation

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

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

Service and Support

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

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

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

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

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

Support Portal: www.ironport.com/support


This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

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

© 2009 Cisco Systems, Inc. All rights reserved.

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