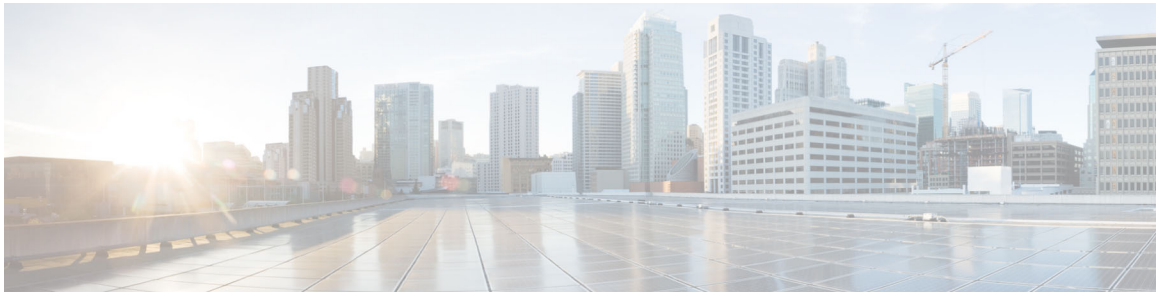

Release Notes for AsyncOS 11.0.2 for Cisco Email Security Appliances

Published: June 14, 2017
Revised: October 30, 2018

Contents

What's New In This Release

Cisco Systems, Inc.
www.cisco.com

What's New in AsyncOS 11.0.2

Feature	Description
Ability to categorize IP addresses as persistent whitelist or blacklist	You can categorize the IP address that you use to access the appliance using SSH as a persistent whitelist or blacklist. If the appliance or the `ipblockd` service is restarted, the IP address in the persistent blacklist or whitelist is retained. You can use the `sshconfig > accesscontrol` command in the CLI to categorize the IP address as a persistent whitelist or blacklist. For more information, see the *sshconfig* section of the *CLI Reference Guide for AsyncOS 11.0 for Email Security Appliances*.
New datacenter added in APJC region for File Reputation service	Cisco has added the following new datacenter in the APJC region for the File Reputation service: *APJC (cloud-sa.apjc.amp.cisco.com)* You can configure your Email Security appliances to use the new File Reputation service. For more information, see the "File Reputation Filtering and File Analysis" chapter in the user guide or the online help.

What's New in AsyncOS 11.0

Feature	Description
FIPS Certification	Cisco Email Security Appliance will be FIPS certified and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #1643). See the "FIPS Management" chapter in the user guide or online help.
New Data Loss Prevention (DLP) solution	RSA has announced End of Life (EOL) for RSA Data Loss Prevention Suite. For more information, see https://community.rsa.com/docs/DOC-59316. Cisco now provides an alternative DLP solution that allows seamless migration of all the existing DLP policies created in RSA DLP to the new DLP engine. After the upgrade, you can view or modify the migrated DLP policies in **Mail Policies > DLP Policy Manager** page in the web interface. For more information, see the "Data Loss Prevention" chapter in the user guide. **Note** There is no support for RSA Enterprise Manager Integration in Async0S 11.0 and later. If you have DLP policies created in RSA Enterprise Manager, you must recreate those policies in your appliance after the upgrade.

Support for Two-Factor Authentication	Cisco Email Security appliance now supports two-factor authentication that ensures secure access when you log into your appliance. You can configure two-factor authentication for your appliance through any standard RADIUS server that complies with standard RFC. You can enable two-factor authentication in one of the following ways: • System Administration > Users page in the web interface. See the "Distributing Administrative Tasks" chapter in the user guide. • `userconfig > twofactorauth` command in the CLI. See the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances.* If you have enabled two-factor authentication on your appliance, you can join it to a cluster machine using pre-shared keys. Use the `clusterconfig > prepjoin` command in the CLI to configure this setting. See the "Centralized Management Using Clusters" chapter in the user guide
Manually Rollback to a Previous Version of the Service Engine	You can now manually roll back to a previous version of the current engine when: • The engine update is defective. • The engine is not functioning properly. Currently, you can perform an engine rollback for the following engines: • McAfee • Sophos • Graymail You can perform an engine rollback only at the machine level and not at the cluster level. You can use the Security Services > Services Overview page in the web interface to perform: • Rollback to a previous version of the service engine. • Manually update the service engines to the required version. For more information, see the "System Administration" chapter in the user guide.

Handling incoming mail connections and incoming or outgoing messages from different geographic locations	Cisco Email Security appliance can now handle incoming mail connections and incoming or outgoing messages from specific geolocations and perform appropriate actions on them, for example: • Prevent email threats coming from specific geographic regions. • Allow or disallow emails coming from specific geographic regions. You can use this feature in the following ways: • **SMTP Connection Level.** You can now configure sender groups to handle incoming mail connections from specific geolocations using one of the following ways: – Mail Policies > HAT Overview > Add Sender Group > Submit and Add Senders > **Geolocation** option in the web interface. – `listenerconfig > hostaccess > country` command in the CLI. For more information, see the "Defining Which Hosts Are Allowed to Connect Using the Host Access Table (HAT)" chapter in the user guide or the *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances.* You can use the **Geo Distribution** report to view the details of incoming mail connections from specific geolocations based on the sender's country of origin. For more information, see the "Using Email Security Monitor" chapter in the user guide. • **Content or Message Filter Level**: You can now create a content or a message filter to handle incoming or outgoing messages from specific geolocations and perform appropriate actions on such messages. Content and message filters include the following new options: – A new content filter condition - **Geolocation** – A new message filter rule - `geolocation-rule()`. For more information, see the "Content Filters" or "Using Message Filters to enforce Email Policies" chapter in the user guide. You can use the Content Filters and Message Filters reports to view the details of incoming or outgoing messages from specific geolocations that are detected by the content or message filter. For more information, see the "Using Email Security Monitor" chapter in the user guide. You can use Message Tracking to search for incoming messages from specific geolocations detected by the content or message filter. Use the **Geolocation** filter for the Message Event option in the Advanced section of Message Tracking. The geolocation list of countries is cloud updateable.

Scanning Outgoing Messages using the AMP engine	You can now configure the appliance to scan outgoing messages using the AMP engine. You can use this feature to: • Prevent users from sending malicious messages from the organization's network, which can lead to low IP or domain reputation. • Track users who are sending outbound messages with malicious attachments and perform appropriate actions on them. You can configure the outgoing mail policy of your appliance to allow scanning of messages by the AMP engine in one of the following ways: • Mail Policies > Outgoing Mail Policies page in the web interface. See the "File Reputation Filtering and File Analysis" chapter in the user guide. • `policyconfig` command in the CLI. The following reports have been enhanced to show details of outgoing messages scanned by the AMP engine: Advanced Malware Protection • AMP File Analysis • AMP Verdict Updates • Overview Page • Outgoing Destinations • Outgoing Senders • Internal Users See the "Using Email Security Monitor" chapter in the user guide. You can use the **Mail Flow Direction** filter in the Message Tracking > Message Event > Advanced Malware Protection option to search for incoming and outgoing messages that are scanned by the AMP engine.
Enable or Disable Automatic Updates	You can now enable or disable automatic updates in the Global Settings page for the following service engines: • McAfee • Sophos • Graymail You can now receive periodic alerts when automatic updates are disabled for a specific service engine. You can change the existing alert interval in one of the following ways: • Security Services > Service Updates > Alert Interval for Disabled Automatic Engine Updates option in the web interface. See the "System Administration" chapter in the user guide. • `updateconfig` command in the CLI.

Performing additional actions on attachments detected by Advanced Malware Protection in Mail Policy	You can perform the following additional actions, if an attachment is considered 'malicious', 'unscannable', or 'sent for file analysis' in the Advanced Malware Protection section for Incoming or Outgoing Mail Policies: • Modifying the message recipient • Sending the message to an alternate destination host. For more information, see the "File Reputation Filtering and File Analysis" chapter in the user guide.
Improved AMP Engine Logs	Information about the following scenarios are now logged in the AMP engine logs: • File that is not uploaded to the File Analysis server. • File that is skipped for file analysis because the appliance exceeded the daily file upload limit to the File Analysis server. • File that is marked as unscannable.
Supported Archive File Formats for Content Scanning	The Content Scanner in your appliance can perform content scanning on the following archive file formats: • ACE Archive • ALZ Archive • Apple Disk Image • ARJ Archive • bzip2 Archive • EGG Archive • GNU Zip • ISO Disk Image • Java Archive • LZH • Microsoft Cabinet Archive • RAR Multi-Part File • RedHat Package Manager Archive • Roshal Archive (RAR) • Unix AR Archive • UNIX Compress Archive • UNIX cpio • UNIX Tar • XZ Archive • Zip Archive • 7-Zip

Macro Detection Enhancement	You can now detect macros in the following files: • Javascript macros in Adobe Acrobat Portable Document Format (PDF) files. • Visual Basic for Applications (VBA) macros in Microsoft Office Files (Open XML) and OLE files. For more information, see the "Content Filters" or "Using message Filters to Enforce Email Policies" chapter in the user guide.
CRL Check for web interface login	You can configure CRL check for web interface login using one of the following ways: • Network > CRL Sources > Edit Settings > CRL check for WebUI option in the web interface. See the "Authenticating SMTP Sessions Using Client Certificates" chapter in the user guide. • `certconfig > crl` command in the CLI If you enable this option and the certificate is revoked: • You will receive an alert indicating that the certificate is revoked. • You will not be able to access the web interface of your appliance. However, you can still log in to your appliance using the CLI. You must import and configure a valid certificate through the CLI to be able to access the web interface of your appliance. See *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*.
Configuring Cache Expiry Period for File Reputation disposition values.	You can configure the cache expiry period for File Reputation disposition values in one of the following ways: • Security Services > File Reputation and Analysis > Cache Settings page in the web interface. • `ampconfig > cachesettings > modifytimeout` command in the CLI.
New datacenter added in European region for File Reputation and File Analysis services	Cisco has added a new datacenter in the European region for the File Reputation and File Analysis services: • *EUROPE (cloud-sa.eu.amp.cisco.com)* for File Reputation server • *EUROPE (https://panacea.threatgrid.eu)* for File Analysis server You can configure your Email Security appliance to use the new File Reputation and File Analysis services. For more information, see the "File Reputation Filtering and File Analysis" chapter in the user guide.

Changes in Behavior

Changes in Behavior in AsyncOS 11.0.2

Changes in configuring Domain Keys/DKIM Verification	Prior to this release, if your appliance is on FIPS mode, you could only use 2048-bit DKIM keys to verify incoming messages. After you upgrade to this release, if your appliance is in FIPS mode, you can verify your incoming messages using 1024, 1536, or 2048-bit DKIM keys.
DMARC Aggregate Report Changes	You can now use the `dmarcconfig` command in the CLI to configure the maximum limit of DMARC aggregate reports that can be generated per day. The default value for the number of DMARC aggregate reports generated per day is 1000, and the maximum value is 50K. It is recommended that you schedule the generation of DMARC aggregate reports during non-peak hours to avoid impact on mail flow. If you generate a higher number of DMARC aggregate reports, you might experience a slight delay in email delivery during non-peak hours for a longer duration.
Changes in Threshold Value for Memory Page Swapping	Prior to this release, the default threshold level for memory page swapping was measured based on the number of pages. After you upgrade to this release, you can now configure your appliance to measure the threshold value for memory page swapping in percentage. The default threshold value for memory page swapping is set to 10%.

Changes in Behavior in AsyncOS 11.0

No Support for RSA Enterprise Manager	After you upgrade to this release, there is no support for RSA Enterprise Manager. If you have DLP policies created in RSA Enterprise Manager, you must recreate those policies in your appliance after the upgrade.
DLP updates performed at machine level only	Prior to this release, DLP updates were performed at the level that DLP was configured. For example, if DLP was configured at cluster level, DLP updates were also performed at that level. After you upgrade to this release, DLP updates are only performed at the machine level, irrespective of whether DLP is configured at the cluster, machine, or group level.
Unable to rollback to a previous version of DLP engine and content matching classifiers	Prior to this release, you could rollback to a previous version of DLP engine and content matching classifiers on the appliance. After you upgrade to this release, you cannot rollback to a previous version of DLP engine and content matching classifiers on the appliance.

Changes in US Drivers License classifier	Prior to this release, you could view the US Drivers License classifier field in Mail Policies > DLP Policy Manager > Advance Settings page in the web interface. You could use this classifier to select or deselect particular US states to match a DLP policy that you create. After you upgrade to this release, the US Drivers License classifier field is not available in Mail Policies > DLP Policy Manager > Advance Settings page in the web interface. You cannot select or deselect particular US states to match a DLP policy that you create. By default, the US Drivers License classifier now searches for all driver licenses issued in the US.
Changes in default Severity Scale values	Prior to this release, all policies had the same default Severity Scale values that you could adjust for each policy. After you upgrade to this release, the default Severity Scale values differ for each policy.
Changes in resetting the passphrase	The admin (user) can now reset the passphrase for a locked user account through the serial console port. All locked administrative (user) accounts can be unlocked after the passphrase is changed by the admin (user) only.
New Syntax for adding Regular Expressions	You can now use the Perl Compatible Regular Expression (PCRE) syntax to add regular expressions for content matching classifiers or the DLP policy templates.
Validating LDAP server certificate	You can validate the LDAP server certificate in one of the following ways: • System Administration > LDAP > Edit LDAP Settings page in the web interface • `ldapconfig > setup` command in the CLI.
Cloud Domain parameter Changes	Prior to this release, you could configure the Cloud Domain parameter through the web interface or the CLI. After you upgrade to this release, you cannot configure the Cloud Domain parameter through the web interface or the CLI.
Configuring maximum HTTP header size	You can use the `adminaccessconfig > maxhttpheaderfieldsize` command in CLI to configure the maximum HTTP header size of an HTTP request sent to the appliance. The default value for the HTTP header field size is 4096 (4 KB) and the maximum value is 33554432 (32 MB).
Change in host key verifications during cluster communication.	During cluster communication, host key verifications are now performed based on SSH-RSA only. For more information, see SSH-RSA Keys for Cluster Communication and SCP Push, page 16.
Ability to select Alert Severities for Anti-Virus and Advanced Malware Protection alert types separately	You can now select the alert severities for Anti-Virus and Advanced Malware Protection alert types separately on the web interface or CLI.

New default Message Scanning threshold values for Anti-Spam	The following are the new default threshold values to scan messages through the Anti-Spam engine: • Messages that are smaller than 1 MB size are scanned by the Anti-Spam engine. • Messages that are larger than 2 MB size are not scanned by the Anti-Spam engine.
Username Length Changes	Prior to this release, the username length was limited to 16 characters. After you upgrade to this release, the username length is limited to 32 characters.
Content Scanning Changes	The Content Scanner in your appliance now performs partial scanning of Microsoft Excel attachments when the Content Scanner exceeds the memory usage allocated for full content scan. A partial scan skips the scanning of numbers, dates, and duplicate contents in Microsoft Excel attachments. A **`X-Attachment-Scan = Partial`** header is added to the scanned message to indicate the partial scan. To perform appropriate actions on such messages, use a message filter or a content filter that detects the **`X-Attachment-Scan = Partial`** header. The following example shows how a message filter is used to detect and quarantine partially scanned messages. *`PartialContentScan: if (header("X-Attachment-Scan") == "^partial$") {quarantine("Policy");}`*
Forged Email Detection Changes	Prior to this release, the name of the user and the user ID in the From: header of the message was used to detect forged messages. After you upgrade to this release, only the name of the user in the From: header of the message is used to detect forged messages. In the following example, only the name of the user (Jim Ross) is used to detect forged messages: Jim Ross <jimr@example.com> If the message contains only the email address (jimr@example.com) in the From: header, the user ID (jimr) is used to detect forged messages.

Upgrade Paths

Upgrading to Release 11.0.2-044 - MD (Maintenance Deployment) Refresh

You can upgrade to release 11.0.2-044 from the following versions:

- 9.1.2-053
- 9.8.1-021
- 9.8.1-015
- 11.0.1-027
- 11.0.1-301
- 11.0.2-037
- 11.0.2-038

Upgrading to Release 11.0.2-037 - MD (Maintenance Deployment)

You can upgrade to release 11.0.2-037 from the following versions:

- 9.1.2-053
- 9.7.2-145
- 9.8.1-021
- 9.8.1-015
- 10.0.3-003
- 11.0.0-274
- 11.0.1-027
- 11.0.1-030
- 11.0.1-301
- 11.0.1-401
- 11.0.1-505

Upgrading to Release 11.0.0-274 - GD (General Deployment) Refresh

You can upgrade to release 11.0.0-274 from the following versions:

- 9.7.2-145
- 10.0.1-103
- 10.0.2-020
- 10.0.3-003
- 11.0.0-264
- 11.0.0-272

Upgrading to Release 11.0.0-260 - LD (Limited Deployment) Refresh

You can upgrade to release 11.0.0-260 from the following versions:

- 9.1.1-038
- 9.1.2-036
- 9.7.1-066
- 9.7.2-065
- 9.7.2-131
- 9.7.2-148
- 10.0.0-203
- 10.0.1-103
- 10.0.2-020
- 11.0.0-074
- 11.0.0-105
- 11.0.0-255

Upgrading to Release 11.0.0-105 - LD (Limited Deployment)

You can upgrade to release 11.0.0-105 from the following versions:

- 9.1.1-038
- 9.1.2-036
- 9.7.1-066
- 9.7.2-065
- 9.7.2-131
- 9.7.2-148
- 10.0.0-203
- 10.0.1-103

Installation and Upgrade Notes

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

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

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

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models:
  - C380, C390, C680, or C690
  - C170 or C190
  - Some C370, C370D, C670 or X1070 appliances

    To determine whether your appliance is supported, and to remedy the situation if it is not currently compatible, see http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html.

The following hardware is NOT supported for this release:

C160, C360, C660, and X1060

Deploying or Upgrading a Virtual Appliance

If you are deploying or upgrading a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.

Upgrading a Virtual Appliance

If your current Virtual Appliance release does not support more than 2TB of disk space, and you want to use more than 2 TB of disk space with this release, you cannot simply upgrade your virtual appliance.

Instead, you must deploy a new virtual machine instance for this release.

When you upgrade a virtual appliance, the existing licenses remain unchanged.

Migrating from a Hardware Appliance to a Virtual Appliance

Step 1 Set up your virtual appliance with this AsyncOS release using the documentation described in Deploying or Upgrading a Virtual Appliance, page 13.

Step 2 Upgrade your hardware appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded hardware appliance

Step 4 Load the configuration file from the hardware appliance onto the virtual appliance.

Be sure to select an appropriate option related to network settings.

Getting Technical Support for Virtual Appliances

Requirements for obtaining technical support for your virtual appliance are described in the *Cisco Content Security Virtual Appliance Installation Guide* available from http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html.

See also Service and Support, page 20, below.

Provisioning and Activating Cisco Registered Envelope Service Administrator from Virtual Appliances

Please contact Cisco TAC for information required to provision your virtual appliance.

Pre-upgrade Notes

Before upgrading, review the following:

No Support for RSA DLP Suite and RSA Enterprise Manager

RSA has announced End of Life (EOL) for RSA Data Loss Prevention Suite (DLP). Cisco now provides an alternative DLP solution that allows seamless migration of all the existing DLP policies created in RSA DLP to the new DLP engine. After the upgrade, you can view or modify the migrated DLP policies in Security Services > Data Loss Prevention page in the web interface. For more information, see the “Data Loss Prevention” chapter in the user guide.

There is no support for RSA Enterprise Manager Integration in Async0S 11.0 and later. If you have DLP policies created in RSA Enterprise Manager, you must recreate those policies in your appliance after the upgrade.

Performance Degradation on C170 and C100V Models

After you upgrade to AsyncOS 11.0 on C170 or C100V models, you might experience a performance degradation in certain configurations. For more details, see

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCve27500

FIPS Compliance

AsyncOS 11.0 GD will be FIPS certified and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #1643).

Reverting to Previous AsyncOS Versions

The following AsyncOS versions are affected by the Internal Testing Interface Vulnerability (http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa):

- 9.1.2-023
- 9.1.2-028
- 9.1.2-036
- 9.7.2-046
- 9.7.2-047
- 9.7-2-054
- 10.0.0-124
- 10.0.0-125

If you upgrade to AsyncOS 11.0.0-264 from one of the above versions, you cannot revert to any of the previous versions.

Upgrading Deployments with Centralized Management (Clustered Appliances)

If a cluster includes C160, C360, C660, or X1060 hardware appliances, remove these appliances from the cluster before upgrading.

All machines in a cluster must be running the same version of AsyncOS, and x60 hardware cannot be upgraded to this release. If necessary, create a separate cluster for your x60 appliances.

Upgrading From a Release Other Than the Immediate Previous Release

If you are upgrading from a major (AsyncOS X.0) or minor (AsyncOS X.x) release other than the release immediately preceding this release, you should review the Release Notes for major and minor releases between your current release and this release.

Maintenance releases (AsyncOS X.x.x) include only bug fixes.

Configuration Files

Cisco 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 Cisco Customer Support if you have any questions about configuration file support.

IPMI Messages During Upgrade

If you are upgrading your appliance using CLI, you may observe messages related to IPMI. You can ignore these messages. This is a known issue.

Defect ID: CSCuz28415

SSH-RSA Keys for Cluster Communication and SCP Push

Cluster Communication

During cluster communication, host key verifications are now performed based on SSH-RSA only. If you do not add the SSH-RSA keys to your appliance, your cluster communication will fail after you upgrade to AsyncOS 11.0.

SCP Push

If you configure SCP Push to periodically push log files to the SCP server on a remote computer that does not have a SSH-RSA key, the SCP Push will fail after you upgrade to AsyncOS 11.0.

Add SSH-RSA Keys to Your Appliance (Cluster Communications)

Before You Begin

Make sure that all your appliances are connected to the cluster.

Procedure

Step 1 Log in to one of the appliances using the CLI.

Step 2 Enter the following batch command:

logconfig ssh hostkey scan **<hostname_or_IP_address>**

Example: Adding SSH-RSA Keys Using an IP Address

```
Cluster cluster_example)> logconfig ssh hostkey scan 10.1.1.1

Adding key type rsa for host 10.1.1.1:
10.1.1.1 ssh-rsa AAB3Nx34TAQA...
Adding key type dsa for host 10.1.1.1:
10.1.1.1.1 ssh-dss AAB3NzaC1kc3AAcbAOY…
```

Example: Adding SSH-RSA Keys Using a Hostname

```
(Cluster cluster_example)> logconfig ssh hostkey scan mail1.example.com

Adding key type rsa for mail1.example.com:
mail1.example.com ssh-rsa ADFTghYAB……

Adding key type dsa for host mail1.example.com:
mail1.example.com ssh-dss AB3NzaC1kc3MAA…
```

Step 3 On the same appliance, repeat Step 2 using the hostname or IP address of all the other appliances in the cluster.

Step 4 Commit your changes.

Upgrading to This Release

Before You Begin

- Review the Known and Fixed Issues, page 19 and Installation and Upgrade Notes, page 12.
- If you are upgrading a virtual appliance, see Upgrading a Virtual Appliance, page 13.

Procedure

Use the following instructions to upgrade your Email Security appliance.

Step 1 Save the XML configuration file off the appliance.

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

Step 9 Resume all listeners.

What To Do Next

- After the upgrade, review your SSL configuration to ensure that you have selected the correct GUI HTTPS, Inbound SMTP, and Outbound SMTP methods to use. Use the **System Administration > SSL Configuration** page or the `sslconfig` command in CLI. For instructions, see the "System Administration" chapter in the User Guide or the online help.
- Review the Performance Advisory, page 18.

Post-Upgrade Notes

Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 11.x

After upgrading to AsyncOS 11.x, if your appliances are in the cluster mode and DLP is configured, inconsistency in the DLP settings is seen when you run the `clustercheck` command using the CLI.

To resolve this inconsistency, force the entire cluster to use the DLP configuration of any of the other machines in the cluster. Use the following prompt "`How do you want to resolve this inconsistency?`" in the `clustercheck` command as shown in the following example:

```
(Cluster)> clustercheck
Checking DLP settings...
```

```
Inconsistency found!
DLP settings at Cluster test:
mail1.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
mail2.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
How do you want to resolve this inconsistency?
1. Force the entire cluster to use the mail1.example.com version.
2. Force the entire cluster to use the mail2.example.com version.
3. Ignore.
[3]>
```

Performance Advisory

DLP

- Enabling DLP for outbound messages on an appliance that is already having anti-spam and anti-virus scanning running on inbound messages can cause a performance degradation of less than 10%.
- Enabling DLP on an appliance that is only running outbound messages and is not running anti-spam and anti-virus can cause higher performance degradation as compared to the previous scenario.

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 support provider.

Known and Fixed Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects in this release.

Bug Search Tool Requirements

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

Lists of Known and Fixed Issues

Known Issues	**AsyncOS 11.0.2**	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.2*&sb=afr&bt=custV
	AsyncOS 11.0.1	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.1-027&sb=afr&bt=custV
	AsyncOS 11.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.0&sb=afr&bt=custV

Fixed Issues	**AsyncOS 11.0.2**	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.2-044&sb=fr&bt=custV
	AsyncOS 11.0.1	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.1-027&sb=fr&bt=custV
	AsyncOS 11.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.0&sb=fr&bt=custV

Finding Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find the most current information about known and resolved defects.

Before You Begin

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

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 Log in with your Cisco account credentials.

Step 3 Click **Select from list > Security > Email Security > Cisco Email Security Appliance**, and click **OK**.

Step 4 In Releases field, enter the version of the release, for example, 11.0.2

Step 5 Depending on your requirements, do one of the following:

- To view the list of resolved issues, select **Fixed in these Releases** from the Show Bugs drop down.
- To view the list of known issues, select **Affecting these Releases** from the Show Bugs drop down and select **Open** from the Status drop down.

Note If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool. There is also an interactive tour; to view it, click the link in the orange bar above the search fields.

Related Documentation

Documentation For Cisco Content Security Products	Location
Hardware and virtual appliances	See the applicable product in this table.
Cisco Content Security Management	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Web Security	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Email Security	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
CLI reference guide for Cisco Content Security appliances	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort Encryption	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

Service and Support

Note To get support for virtual appliances, have your Virtual License Number (VLN) number ready when you call Cisco TAC.

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site for legacy IronPort: http://www.cisco.com/web/services/acquisitions/ironport.html

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.

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