Release Notes for AsyncOS 14.2 for Cisco Secure Email Gateway - GD (General Deployment)

Published: May 26, 2022
Revised: November 14, 2023

Contents

What's New In This Release

Feature	Description
Sender Maturity	In this release, the legacy Sender Domain Reputation (SDR) Domain Age functionality is replaced with Sender Maturity. Sender Maturity is an important feature to establish sender reputation. Sender Maturity is automatically generated for spam classification based on multiple sources of information and can differ from "Whois-based domain age."
	Sender Maturity represents the Cisco Talos view of how mature a domain is as an email sender. The maturity value is tuned to enable threat detection regarding emails and generally does not reflect the domain age represented in "Whois-based domain age."
	Sender Maturity is set to a limit of 30 days, and beyond this limit, a domain is considered mature as an email sender, and no further details is provided.
	✎ **Note** From this release onwards, the 'SDR Domain Age' configured filters are automatically updated to the 'SDR Sender Maturity' filters. The filters with an invalid value for Sender Maturity are marked as 'inactive' after the upgrade. Make sure you review and modify the message and content filters accordingly.
	Sender Maturity is used to calculate the sender reputation. Immature domains are assigned lower reputation. Cisco Talos recommends you rely on sender reputation only for determining policy actions. Sender Maturity is exposed to fine-tune filters for specific, non-standard scenarios.
	✎ **Note** Cisco Talos does not manually adjust maturity for domains but relies on automated systems and sensors to determine the most appropriate value.
	For more information, see the "Sender Domain Reputation Filtering" chapter in the user guide.
Sender Domain Reputation Filtering Improvements	In this release, the user experience and overall quality of the Sender Domain Reputation (SDR) service is enhanced with performance improvements, increased availability, and deployment of SDR.

New Sender Domain Reputation Verdicts	From this release onwards, the Sender Domain Reputation (SDR) verdicts are updated to accurately reflect the intended meaning and recommended usage.
	During the upgrade, the system automatically updates the Sender Domain Reputation message or content filter configurations to reflect the new verdicts. Make sure you review and configure the message or content filters accordingly.
	For more information about the recommended actions, you can take for each new SDR verdict, see the "SDR Verdicts" section in the "Sender Domain Reputation Filtering" chapter of the user guide.
	After you upgrade to AsyncOS 14.2.x release, the legacy SDR verdicts in the content or message filters, reporting, and message tracking are replaced with the new SDR verdicts as follows:
	• Untrusted
	• Questionable
	• Neutral
	• Favorable
	• Trusted
	• Unknown
	Note The SDR Reporting and Tracking AsyncOS APIs are updated to reflect the new SDR Threat Levels and Category structure.
	Note The SDR Mail and Tracking Logs are updated to reflect the new SDR Threat Levels and Sender Maturity details.
	Note From this release onwards, an additional Sender Domain Reputation check is performed after the sender header of the message is received. Messages with a Threat Level that matches the configured SDR reject level (in your email gateway) are rejected,
	For more information, see the:
	• "Sender Domain Reputation Filtering" chapter in the user guide.
	• "Sender Domain Reputation Filtering" section in the "The Commands: Reference Examples" chapter of the CLI reference guide.

Enhancements on Grouping Appliances for File Analysis Reporting	The email gateway now uses the Smart Account ID to group appliances in your organization and to view the file analysis result of all appliances. When Smart Licensing is enabled on your email gateway, and you configure the appliance group for file analysis reporting, the system automatically registers Smart Account ID as the Appliance Group ID. You can change the Appliance Group ID at any time, and the change takes effect immediately without a Commit action. ✎ **Note** You must upgrade the email gateway and Secure Email and Web Manager to the 14.2 version for this feature to work. For more information, see the: • "(Public Cloud File Analysis Services Only) Configuring Appliance Groups" section in the "File Reputation Filtering and File Analysis" chapter of the user guide. • "(Public Cloud File Analysis Services Only) Configuring Appliance Groups" section in the "The Commands: Reference Examples" chapter of the CLI reference guide.

Smart Software Licensing Enhancements	Following are the enhancements made to the Smart Software Licensing feature:
	
	• **License Reservation**: You can reserve licenses for features enabled in your email gateway without connecting to the Cisco Smart Software Manager (CSSM) portal. This is mainly beneficial for covered users that deploy the email gateway in a highly secured network environment with no communication to the Internet or external devices. The feature licenses can be reserved in any one of the following modes:
	
	    – **Specific License Reservation (SLR)** – use this mode to reserve licenses for individual features (for example, 'Mail Handling') for a given time-period.
	
	    – **Permanent License Reservation (PLR)** – use this mode to reserve licenses for all features permanently.
	
	• **Device Led Conversion**: After you register your email gateway with smart licensing, all existing, valid classical licenses are automatically converted to smart licenses using the Device Led Conversion (DLC) process. These converted licenses are updated in the virtual account of the CSSM portal.
	
	For more information, see the:
	
	• "Overview and Reserving Feature Licenses"sections in the "File System Administration" chapter of the user guide.
	
	• "Smart Software Licensing" section in the "The Commands: Reference Examples" chapter of the CLI reference guide.

TLS Certificate Enhancement for Destination Control	You can now choose a different certificate other than the certificate configured in the 'Default' destination control entry for specific domains.
	You can choose a different certificate in any one of the following ways:
	• Edit the corresponding destination control entry and select a different certificate using the TLS certificate option in the web interface.
	• Use the `destconfig` > `new` or `edit` sub commands in the CLI to select a certificate when you create or edit a destination control entry.
	For more information, see "Controlling TLS" section in the "Configuring Routing and Delivery Features" chapter of the user guide.
Modification of Classic Licensing - Expiration Date in Web Interface and CLI	From this release onwards, the existing 'Expiration Date' column header in the web interface and CLI for classic licensing is modified as follows – "Expiration Date (including grace period)" to indicate that the grace period is included in the expiration date.
	Note All alert messages and mail logs are modified to display the expiration date, including the grace period for a feature key.
Detecting Smart Identifier with or without Prefix	The email gateway now detects a smart identifier with or without the keyword ('credit,' 'ssn,' 'cusip,' or 'aba') added as a prefix in the message content.
	You can configure the content filter condition or message filter rule to detect the smart identifier with or without the keyword added as a prefix in the following ways:
	• Use the **Contains smart identifier prefix** option in the content filter condition for Message Body, Message Body or Attachment, and Attachment Content. For more information, see the 'Content Filter Condition' section in the 'Content Filter' chapter of the user guide.
	• Use the `prefix` syntax in the message filter rule. For more information, see the 'Smart Identifier Syntax' section in the 'Using Message Filters to Enforce Email Policies' chapter of the user guide.

Caching for Syslog Push Log Subscriptions	You can now configure a local disk buffer for a syslog push log subscription to allow email gateway to cache log events when the remote syslog server is unavailable. When the syslog server becomes available, the email gateway sends all the data in the buffer for that log subscription to the syslog server.
	You can configure the disk buffer parameters in the following ways:
	• **System Administration** > **Log Subscription** page in web interface. For more information, see 'Log Retrieval Methods' section in the 'Logging' chapter of the user guide.
	• `logconfig` command in CLI. For more information, see 'Logging and Alerts' section in the 'The Commands: Reference Examples' chapter of the CLI Reference Guide.
	Note The disk buffer parameter configuration is only applicable for the TCP protocol.
Configuring Maximum Number of Content Dictionaries in Email Gateway	You can now configure a maximum number of 150 content dictionaries in your email gateway.
	Note By default, you can configure a maximum of 100 content dictionaries in your email gateway.
	Use the `dictionaryconfig` > `dictionarylimits` sub command in the CLI to to modify the default limits.
	Note When you use content dictionaries extensively with 'Message Body or Attachments' content filter condition or 'Body Scanning' or 'Attachment Scanning' message filter rules, it may degrade system performance.
	For more information see the 'Policy Enforcement' section in 'The Commands: Reference Examples' chapter of the CLI reference guide associated with this release.

Changes in Behavior

No Support for `sdrstatus` and `sdrupdate` CLI commands	From this release onwards, the `sdrstatus` and `sdrupdate` CLI commands are no longer supported. You can now use the following CLI commands to configure the functionalities of `sdrstatus` and `sdrupdate` CLI commands: • `talosstatus` – to view the current version of the SDR component. • `talosupdate` - to manually update the SDR component.
FQDN Validation Changes	From this release onwards, when you validate a peer certificate or import a certificate, FQDN validation checks whether the SAN extension is critical when the subject name (common name) field is not available in the certificate that you import or in the server certificate. **Note** This behavior change is applicable only when you enable FQDN Validation during a certificate import or peer certificate validation.
Updater Server CA Certificate Changes	Following are the updater server CA certificate behavior changes made in this release: • FQDN validation is performed when you add the updater server CA certificate in your email gateway. A new statement - "`Do you want to check if Common Name or SAN:dNSName or both are in Fully Qualified Domain Name(FQDN) format?`" is added in the `updateconfig` > `trusted_certificates` > `add` sub command in the CLI to perform the FQDN validation. • CA certificate validation is performed when you add an updater CA certificate in your email gateway. **Note** The email gateway allows you to add the updater CA certificate if the root CA certificate and the other certificates in the chain are trusted
Web UI Inactivity Timeout Value Changes	Following are the 'Web UI Inactivity Timeout' value behavior changes made in this release: • [Applicable for new AsyncOS install only]: The default value for ' Web UI Inactivity Timeout ' option is changed from 30 to 5 minutes. You can modify the value if required. • [Applicable for AsyncOS upgrade only]: On upgrade, the 'Web UI Inactivity Timeout' option retains the same value configured before the upgrade.
FQDN Validation Changes for Peer Certificate	From this release onwards, if the Common Name (CN) or SAN: DNS Name fields in the peer certificate have a resolvable domain, the FQDN validation for the peer certificate is successful.

AWS S3 Push Configuration Changes	Prior to this release, when you configured the 'AWS S3 Push' log retrieval method, you could only enter the AWS (S3) Bucket name in the 'S3 Bucket Name' field in the 'System Administration > Log Subscription > Add Log Subscription' page to transfer the consolidated event logs
	From this release onwards, when you configure the 'AWS S3 Push' log retrieval method, you can now enter the AWS (S3) Bucket name along with any directory path within the AWS (S3) Bucket, in the 'S3 Bucket' field in the 'System Administration > Log Subscription > Add Log Subscription' page to transfer the consolidated event logs.
	For Example, if you enter 'test1esa/dir1' in the S3 Bucket field, then 'test1esa' is the AWS S3 Bucket name and 'dir1' is the directory path within the 'test1esa' bucket.
Mail Policy Entry Changes	From this release onwards, the email gateway does not allow you to:
	• Add duplicate users for a mail policy through the CLI or when you load an XML configuration file in the email gateway.
	• Edit a mail policy to add a duplicate user to the mail policy.
	✎
	Note The users of a mail policy must be unique.
Web UI Session Timeout Changes	Prior to this release, if you set the default value for the Web UI Inactivity Timeout option to more than 12 hours, you would not get logged out of the new web interface of your email gateway after 12 hours. You could still access the new web interface after 12 hours.
	After you upgrade to this release, if you set the default value for the Web UI Inactivity Timeout option to more than 12 hours, you are now automatically logged out of the new web interface of the email gateway after 12 hours.
Syslog Disk Buffer Size Configuration Changes	Prior to this release, the maximum disk buffer size allowed for a syslog push log subscription was 10 GB.
	After you upgrade to this release, the maximum disk buffer size allowed for a syslog push log subscription is 1GB.
	[Applicable for AsyncOS upgrade only]: During the upgrade, the system automatically reduces the maximum disk buffer size value to 1GB if the existing configured value is more than 1 GB before the upgrade.
	✎
	Note During the upgrade, if the allocated miscellaneous disk quota exceeds the configured limit, then you need to reduce the maximum disk buffer size value (if the existing configured value is more than 1 GB) to free up the allocated miscellaneous disk quota space to continue the upgrade process.

CA Certificates Validation During System Upgrade	From this release onwards, when you upgrade your email gateway, the existing CA certificate is upgraded only if the CA certificate is active (not expired) and the CA flag in the certificate is set to true. The email gateway rejects expired certificates and the CA certificate with the CA flag set to false during system upgrade. Also, when you load configuration file on your email gateway, the CA certificate with CA flag set to false and expired certificates are removed.
Mail Logs and Tracking Logs Changes	Prior to this release, the information in the subject of 'Mail Logs' and 'Tracking Logs' was not enclosed in quotes.
	After you upgrade to this release, the information in the subject of the 'Mail Logs' and 'Tracking Logs' is now enclosed in double quotes.
Certificate Validation Changes in Non-FIPS Mode	From this release onwards, if your email gateway is in the non-FIPS mode, and you add or upload a self-signed or signed certificate, the email gateway now validates the required certificate.
Mail Policy Configuration Changes for Anti-Spam:	From this release onwards, if the Anti-Spam configuration is defined at a particular level and then moved to another level (for example, cluster to machine level), you can configure mail policies for Anti-Spam only at the moved level (for example, machine level).
Text Resource Name Changes	Prior to this release, you could add a name to text resource with blank spaces.
	After you upgrade to this release, you cannot enter text resource names with blank spaces. Text Resource name must start with a letter or underscore, followed by any number of letters, numbers, underscores, or hyphens.
	Note Blank space is not allowed.
	When you upgrade to this release, the text resources from previous release versions are upgraded in the same format to the new release version.
	Note After you upgrade, it is recommended to rename the text resources that have blank spaces.
System Health API Changes	Prior to this release (applicable to AsyncOS 13.5.x and 13.7 release versions only), a sample response of the System Health API contained details of the Delivery Status and System Status APIs.
	From this release onwards, the details of the Delivery Status and System Status APIs are removed from the System Health API response. You can now view these details in the corresponding responses of the Delivery Status and System Status APIs.

Changes in uploading HTML and Octet-stream Files for File Analysis	[Before this release]: The email gateway could only upload HTML and Octet-stream files (mime type - application/octet-stream and text/html) to the File Analysis server if the file extensions were selected for file analysis.
	[From this release onwards]: The email gateway can now upload the HTML and Octet-stream files to the File Analysis server for file analysis, even if the file extensions are not selected for file analysis.
	Note As the number of files uploaded to the File Analysis server may increase, the email gateway could potentially reach the file upload limit of the file analysis server quickly.
Changes in uploading Archived Files for File Analysis	[Before this release]: When the AMP engine failed to extract the archive files (including password-protected archived attachments) from a message, the attachments would not be uploaded to the File Analysis server.
	[From this release onwards]: When the AMP engine fails to extract the archive files (including password-protected archived attachments) from a message, the attachments are now uploaded to the File Analysis server for file analysis.
	Note As the number of files uploaded to the File Analysis server may increase, the email gateway could potentially reach the file upload limit of the file analysis server quickly.

Upgrade Paths

You can upgrade to release 14.2.0-620 from the following versions:

- 13.5.1-277
- 13.5.2-036
- 13.7.0-093
- 14.0.0-480
- 14.0.0-657
- 14.0.0-692
- 14.0.0-698
- 14.0.1-033
- 14.0.1-103
- 14.0.2-020
- 14.0.2-228
- 14.0.2-606
- 14.2.0-102
- 14.2.0-468

- 14.2.0-524
- 14.2.0-616

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 a user with administrator privileges to upgrade. Also, you must reboot the email gateway after upgrading.

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models:
    - C190
    - C195
    - C390
    - C395
    - C690
    - C695
    - C695F

Note [For C695 and C695F models only]: Before you upgrade or restart the appliance, disable LLDP on the connected fiber switch port interface. This automatically disables the FCoE traffic.

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
- C170, C370, C370D, C670 and X1070
- C380 and C680 appliances

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 email gateway.

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

When you upgrade a virtual email gateway, 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 11.

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 22, below.

Provisioning and Activating Cisco Registered Envelope Service Administrator from Virtual Appliances

Contact Cisco TAC for information required to provision your virtual appliance.

Pre-upgrade Notes

Before upgrading, review the following:

- Features Configurable using IDN Domains in Email Gateway, page 13
- New Categories and New Names for Existing URL Reputation Verdicts, page 14
- Firewall Settings to Access Cisco Talos Services, page 15
- Firewall Settings to Access Cisco Advanced Phishing Protection Cloud Service, page 15
- Enabling Service Logs on Email Gateway, page 16
- Upgrading Intelligent Multi-Scan and Graymail Configurations at Cluster Levels, page 16
- FIPS Compliance, page 16
- Reverting to Previous AsyncOS Versions, page 16

Features Configurable using IDN Domains in Email Gateway

Prerequisites:

Make sure you have met the following prerequisites before you use the Internationalized Domain Names (IDN) feature:

- All incoming messages must have IDNs encoded in UTF-8.
  For Example: An MTA that sends messages to the email gateway must support IDNs and make sure the domains in the messages are in the UTF-8 format.

- All outgoing messages must have IDNs encoded in UTF-8, and the destination server must accept and support IDNs accordingly.
  For Example: An MTA that accepts messages from the email gateway must support IDNs and domains encoded in the UTF-8 format.

- In all applicable DNS records, IDNs must be configured using the Punycode format.
  For Example: When you configure an MX record for an IDN, the domain in the DNS record must be in the Punycode format.

For this release, you can **only** configure the following features using IDN domains in your email gateway:

- **SMTP Routes Configuration Settings**:

  - Add or edit IDN domains.

  - Export or import SMTP routes using IDN domains.

- **DNS Configuration Settings**: Add or edit the DNS server using IDN domains.

- **Listener Configuration Settings:**

  - Add or edit IDN domains for the default domain in inbound or outbound listeners.

  - Add or edit IDN domains in the HAT or RAT tables.

  - Export or import HAT or RAT tables using IDN domains.

- **Mail Policies Configuration Settings**:

  - Add or edit domains using IDN domains for senders ('Following Senders' or 'Following Senders are not'options) and recipients ('Following Recipients' or 'Recipients are not'options) in Incoming Mail Policies.

  - Add or edit domains using IDN domains for senders ('Following Senders' or 'Following Senders are not'options) and recipients ('Following Recipients' or 'Recipients are not'options) in Outgoing Mail Policies.

  - Find senders or recipients using IDN domains in Incoming or Outgoing Mail Policies

  - Define Sender Verification Exception table using IDN domains.

  - Create an address list using IDN domains.

  - Add or edit the destination domain using IDN domains for destination controls.

- **Bounce Profiles Configuration Settings** - Add or edit the alternate email address using IDN domains.

- **Sender Domain Reputation Configuration Settings**: Define sender domain reputation scores for IDN domains.

- **IP Reputation Configuration Settings**: Define IP reputation scores for IDN domains.

- **LDAP Configuration Settings**: Create LDAP group queries, accept queries, routing queries, and masquerade queries for incoming and outgoing messages using IDN domains.

- **Reporting Configuration Settings:** View IDN data - usernames, email addresses, and domains) in the reports.

- **Message Tracking Configuration Settings**: View IDN data- usernames, email addresses, and domains) in message tracking.

- **Policy, Virus, and Outbreak Quarantine Configuration Settings:**

  - View messages with IDN domains that may be transmitting malware, as determined by the anti-virus engine.

  - View messages with IDN domains caught by Outbreak Filters as potentially being spam or malware.

  - View messages with IDN domains caught by message filters, content filters, and DLP message actions.

- **Spam Quarantine Configuration Settings**:

  - View messages with IDN domains detected as spam or suspected spam.

  - Add email addresses with IDN domains to the safelist and blocklist categories.

  > ✎
  >
  > **Note**   Currently, recipients with IDN domains can access the End-User Quarantine only if the end-user authentication method is set to 'None' under the 'End-User Quarantine Access' section in the 'Spam Quarantine' settings page.

- **SPF Configuration Settings**: Perform SPF verification of messages using IDN domains.

- **DKIM Configuration Settings**: Perform DKIM signing and verification of messages using IDN domains.

- **DMARC Configuration Settings**: Perform DMARC verification of messages using IDN domains.

New Categories and New Names for Existing URL Reputation Verdicts

The following table details the new categories and new names for the existing URL Reputation verdicts in your email gateway:

Current URL Reputation Verdict Name	New Cisco Talos URL Reputation Verdict Name	Score Range	Description
Clean	Trusted	+6.0 to +10.0	Displays a behavior that indicates exceptional safety.

Current URL Reputation Verdict Name	New Cisco Talos URL Reputation Verdict Name	Score Range	Description
Neutral	Favorable	+0.1 to +5.9	Displays a behavior that indicates a level of safety.
	Neutral	-3.0 to 0.0	Does not display a positive or negative behavior. However, this verdict has been evaluated.
	Questionable	-5.9 to -3.1	Displays a behavior that may indicate risk, or undesirable.
Malicious	Untrusted	-10.0 to -6.0	Displays a behavior that is exceptionally bad, malicious, or undesirable.
No Score	Unknown	No score	The verdict has not been previously evaluated or lacks the capability to assert a threat level verdict.

Firewall Settings to Access Cisco Talos Services

You need to open HTTPS (Out) 443 port on the firewall for the following hostnames or IP addresses (refer to the table below) to connect your email gateway to Cisco Talos services.

✎
Note   The HTTPS updater proxy configuration is used to connect to Cisco Talos services.

Hostname	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:ffff::/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04:e4c7:fffe::/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

For more information, see the "Firewall" chapter of the user guide.

Firewall Settings to Access Cisco Advanced Phishing Protection Cloud Service

You need to open HTTPS (Out) 443 port on the firewall for the following hostnames to connect your email gateway to Cisco Advanced Phishing Protection cloud service.

- kinesis.us-west-2.amazonaws.com
- sensor-provisioner.ep.prod.agari.com
- houston.sensor.prod.agari.com

For more information, see the "Firewall" chapter of the user guide.

Enabling Service Logs on Email Gateway

The Service Logs are used to collect personal data based on the Cisco Email Security Appliance Data Sheet guidelines.

The Service Logs are sent to the Cisco Talos Cloud service to improve Phishing detection.

Cisco Secure Email Gateway collects limited personal data from customer emails and offers extensive useful threat detection capabilities that can be coupled with dedicated analysis systems to collect, trend, and correlate observed threat activity. Cisco uses the personal data to improve your email gateway capabilities to analyze the threat landscape, provide threat classification solutions on malicious emails, and to protect your email gateway from new threats such as spam, virus, and directory harvest attacks.

During the upgrade process, you can choose to enable Service Logs on your email gateway in any one of the following ways:

- Select the **I Agree** option for Service Logs in the System Administration > System Upgrade page of the web interface.

- Type **Yes** for the *Do you agree to proceed with Service Logs being enabled by default? [y]>* statement in the upgrade CLI command.

For more information, see the "Improving Phishing Detection Efficacy using Service Logs" chapter of the user guide.

Upgrading Intelligent Multi-Scan and Graymail Configurations at Cluster Levels

Before you upgrade to AsyncOS 14.2, ensure that the Intelligent Multi-Scan and Graymail configurations are at the same cluster level. If not, you must review the Intelligent Multi-Scan and Graymail settings after the upgrade.

FIPS Compliance

AsyncOS 14.2 release is not a FIPS compliant release. If you have enabled FIPS mode on your email gateway, you must disable it before upgrading to AsyncOS 14.2.

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

■ **Release Notes for AsyncOS 14.2 for Cisco Secure Email Gateway - GD (General Deployment)**

16

Upgrading Deployments with Centralized Management (Clustered Appliances)

If a cluster includes C160, C360, C660, X1060, C170, C370, C670, C380, C680, or X1070 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, x70, and x80 hardware cannot be upgraded to this release. If necessary, create a separate cluster for your x60, x70, and x80 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 email gateway using CLI, you may observe messages related to IPMI. You can ignore these messages. This is a known issue.

Defect ID: CSCuz28415

Upgrading to This Release

Before You Begin

- Clear all the messages in your workqueue. You cannot perform the upgrade without clearing your work queue.
- Review the Known Issues, page 8 and Installation and Upgrade Notes, page 11.
- If you are upgrading a virtual email gateway, see Upgrading a Virtual Appliance, page 12.

Procedure

Use the following instructions to upgrade your email gateway:

Step 1 Save the XML configuration file off the email gateway.

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

Step 3 Suspend all listeners.

Step 4 Wait for the work 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 email gateway.

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 20.

- If you have changed the SSH key, re-authenticate the connectivity between the email gateway and Cisco Secure Email and Web Manager after the upgrade.

Post-Upgrade Notes

Monitoring Status of IP Reputation Service

After you upgrade, you may see the following IP address - 172.0.0.2 in the IP Reputation Debug logs.

The 172.0.0.2 IP address is mainly used to check the availability of the IP Reputation cloud service. This IP address is used internally to check the connectivity of the IP Reputation cloud service and your email gateway. The IP address has no relation to the incoming/outgoing messages or the user network.

DLP Service Status Check

After you upgrade to this release, you might experience an issue with the DLP service.

Solution: Check the status of the DLP service on your email gateway using the `diagnostic` > `services` > `DLP` > `status` sub command in the CLI. If the DLP service is not running, refer to the 'Workarounds' section of the CSCvy08110 defect available in the Known Issues list. For more information on how to view the Known Issues, see Lists of Known and Fixed Issues, page 20.

Scanning Password-Protected Attachments in Email Gateway

When you configure the Content Scanner in your email gateway to scan the password-protected attachments, there may be a performance impact if your email traffic contains a high percentage of password-protected attachments.

[Smart Licensing users only] Unable to Connect Email Gateway to Cisco Talos Services

If your email gateway is in the Smart Licensing mode and the system time is behind GMT, your email gateway might experience connectivity issues to Cisco Talos Services.

Solution: Make sure that you configure your email gateway to use the NTP server in time settings.

Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 13.x

After upgrading to AsyncOS 13.x, if your email gateways 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]>
```

Intelligent Multi-Scan and Graymail Global Configuration Changes

The following are the changes to the global settings configuration for Intelligent Multi-Scan (IMS) and Graymail after you upgrade to AsyncOS 14.0:

- If the global settings of IMS and Graymail are configured at different cluster levels, the email gateway copies the global settings to the lowest configuration level. For example, if you configure IMS at the cluster level and Graymail at the machine level, the email gateway copies the IMS global settings to the machine level.

- If the maximum message size and timeout values for scanning messages are different, the email gateway uses the maximum timeout and maximum message size values to configure the IMS and Graymail global settings. For example, if the maximum message size values for IMS and Graymail are 1M and 2M respectively, the appliance uses 2M as the maximum message size value for both IMS and Graymail.

Performance Advisory

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 appliance causes a minimal reduction in system throughput for nominally loaded appliances. For email gateways 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 want 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://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

Lists of Known and Fixed Issues

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=14.2.0&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=14.2.0-620&prdNam=Cisco%20Secure%20Email%20Gateway

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://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

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 Secure Email Gateway**, and click **OK**.

Step 4 In Releases field, enter the version of the release, for example, 14.2

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.

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 Secure Email and Web Manager	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 Secure Email Gateway	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 email gateway. For instructions, see the User Guide or online help.