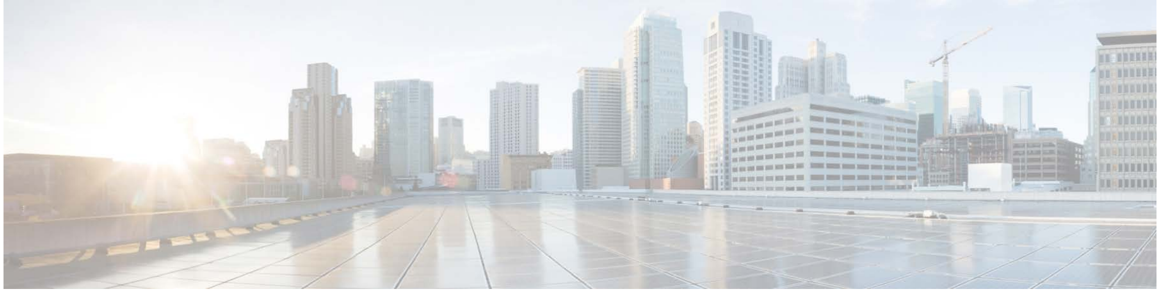

Release Notes for AsyncOS 14.0.1 for Cisco Secure Email Gateway

Published: March 22, 2021
Revised: January 8, 2024

Contents

Cisco Systems, Inc.
www.cisco.com

What’s New In This Release

What’s New in AsyncOS 14.0.1

Feature	Description
URL Filtering Advanced Configuration Settings	You can now configure the following advanced URL filtering parameters in the web interface of your email gateway: • URL Lookup Timeout value • Maximum number of URLs in the message body • Maximum number of URLs in message attachments • Rewrite URL text and HREF in the message • URL details in Mail Logs and Message Tracking For more information, see the 'Enable URL Filtering' section in the "Protecting Against Malicious or Undesirable URLs" chapter of the user guide associated with this release.
Reregistering Email Gateway with Cisco Cloud Services Portal	You can reregister your email gateway with the Cisco Cloud Services portal based on any one of the following scenarios: • If you are unable to view or manage the devices added to the Cisco Cloud Services portal when you automatically register your email gateway with the Cisco Cloud Services portal. • If your Smart Account and Cisco Cloud Services Account are not linked when you automatically register your email gateway with the Cisco Cloud Services portal. You can reregister your email gateway with the Cisco Cloud Services portal using any one of the following ways: • Network > Cloud Service Settings page in the web interface. • `cloudserviceconfig` > `reregister` sub command in the CLI. For more information, see: • ’Reregistering Email Gateway with Cisco Cloud Services Portal' section in the 'Integrating with Cisco SecureX Threat Response" chapter of the user guide associated with this release. • 'Configuring Cisco Cloud Service Portal Settings and Usage' section in 'The Commands: Reference Examples' chapter of the CLI reference guide associated with this release.

New Parameters for Syslog Push - Log Retrieval Method	Following are the new parameters that you need to use to configure the Syslog Push log retrieval method in your email gateway: • Port number of the remote Syslog server. • Maximum size of the log message in bytes that is sent to the remote Syslog server. • [For TCP protocol only]: TLS connection between email gateway and the remote Syslog server. You can configure the new parameters for the Syslog Push log retrieval method using any one of the following ways: • System Administration > Log Subscriptions page in the web interface • `logconfig` command in the CLI. For more information, see: • 'Log Retrieval Methods' section in the 'Logging' chapter of the user guide associated with this release. • 'Logging and Alerts' section in 'The Commands: Reference Examples' chapter of the CLI Reference Guide associated with this release.
Performing SMTP Call-Ahead Recipient Validation using TLS	You can now configure your email gateway to perform SMTP call-ahead recipient validation using TLS. The SMTP call-ahead recipient validation uses the same TLS version selected in the 'Other TLS Client Services' option in the SSL Configuration page in your email gateway. You can enable TLS support for SMTP call-ahead recipient validation using any one of the following ways: • Network > SMTP Call-Ahead page in the web interface • `callaheadconfig` command in the CLI For more information, see: • 'SMTP Call-Ahead Server Profile Settings' section in the 'Validating Recipients Using an SMTP Server' chapter of the user guide associated with this release. • 'SMTP Services Configuration' section in 'The Commands: Reference Examples' chapter of the CLI reference guide associated with this release.

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.
ESXi 7.0 Qualification on Secure Email Gateway	Cisco Secure Email Virtual Gateway can now be deployed on VMware vSphere Hypervisor (ESXi) 7.0. For more information, see the Cisco Content Security Virtual Appliance Installation Guide, at https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html
Configuring Email Gateway to consume SecureX Threat Response Feeds	You can configure your email gateway to consume threat feeds from the Cisco SecureX Threat Response portal. The Cisco SecureX Threat Response portal allows you to create custom feeds for the continuous gathering of observables and to consume them in your email gateway using the feed URL. A feed is a simple list of observables in JSON format. The feeds are created and managed in the **Intelligence** > **Feeds** page in the SecureX Threat Response portal. For more information, see: • “How to Configure Email Gateway to Consume External Threat Feeds” and “Configuring SecureX Threat Response Feeds Source" sections in the "Configuring Email Gateway to Consume External Threat Feeds" chapter of the user guide associated with this release. • “Configuring Email Gateway to Consume External Threat Feeds” section in “The Commands: Reference Examples” chapter of the CLI reference guide associated with this release.

What's New in AsyncOS 14.0

Feature	Description
Integrating Email Gateway with Cisco Secure Awareness Cloud Service	The Cisco Secure Awareness cloud service allows you to effectively deploy phishing simulations, awareness training, or both to measure and report results. It empowers the security operations team to focus on real-time threats and not end-user mitigation. The Cisco Secure Awareness cloud service provides reports of repeat clickers - users who repeatedly click on any URL or attachment in messages. These users are identified via a phishing simulation campaign defined by the Cisco Secure Awareness cloud service. You can integrate your email gateway with the Cisco Secure Awareness cloud service to: • Improve end-user awareness towards real-world phishing attacks. • Allow email administrators to configure stringent policies for end users identified as repeat clickers. For more information, see the "Integrating Cisco Email Gateway with Cisco Secure Awareness Cloud Service" chapter in the user guide or online help.
Simple Network Management Protocol (SNMP) Enhancements	The following are the enhancements made to the SNMP configuration settings: • Added new SNMP MIBs for additional monitoring. • Support for SNMPv3 traps: – SNMPv3 supports all the three security levels – noAuthNoPriv, authNoPriv, and authPriv. – When both SNMPv3 and SNMPv2 are enabled, you need to select the required version for traps. – A new option is added under `snmpconfig` CLI command to select the trap version when both SNMPv2 and SNMPv3 are enabled. For more information, see the "Managing and Monitoring Using the CLI" chapter in the user guide or online help.

Improved Phishing Detection in Email Gateway	The following are the enhancements made to improve phishing detection in your email gateway: • Sender Domain Reputation Filtering Enhancement • Default Scanning of URLs in Message Attachments **Sender Domain Reputation Filtering Enhancement**: You can configure your email gateway to block messages based on the Sender Domain Reputation (SDR) verdict at the SMTP conversation level. You can enable or disable SDR verification using the Mail Flow Policy configuration settings. **Note** By default, SDR verification is enabled for incoming mail flow policies and disabled for outgoing mail flow policies. **Note** By default, your email gateway blocks all incoming messages if the SDR verdict is "Awful." **Default Scanning of URLs in Message Attachments**: By default, the email gateway scans URLs in message attachments for any malicious content early in the email pipeline (before the Anti-Spam engine.) The ability to block messages based on the SDR verdict at the SMTP conversation level and default scanning of URLs in message attachments helps an organization to: • Improve efficacy detection in phishing and domain spoofing. • Detect phishing attacks early in the email pipeline based on the default action taken on the SDR reputation verdict. For more information, see the "Sender Domain Reputation Filtering" and "Defining Which Hosts Are Allowed to Connect Using the Host Access Table" chapters in the user guide or online help.

Scanning Password-protected Attachments in Messages	You can configure the Content Scanner in your email gateway to scan the contents of password-protected attachments in incoming or outgoing messages. The ability to scan password-protected message attachments in the email gateway helps an organization to: • Detect phishing campaigns that use malware as attachments in messages with password-protection to target limited cyber-attacks. • Analyze messages that contain password-protected attachments for malicious activity and data privacy. The following languages are supported for this feature - English, Italian, Portuguese, Spanish, German, and French. You can create user-defined passphrases to open password-protected attachments in incoming or outgoing messages in any one of the following ways: • Security Services > Scan Behavior page in the web interface. • `scanconfig > protectedattachmentconfig` sub command in the CLI. In this release, the Content Scanner can scan the contents of password-protected attachments for the following file types only: • Adobe Portable Document Format (PDF) files. • MS Office file types: – Word - .doc file format that supports 2002 to 2004 version and .docx file format that supports 2007 to 2016 version. – Excel - .xls and .xlsx file formats that support 2007 to 2016 version. – PowerPoint - .ppt or .pptx file formats that support 2007 to 2016 version. • Archive file types - .zip format. For more information, see the "Using Message Filters to Enforce Email Policies” chapter in the user guide and the *CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*.
New report for mail policy details	A new report – **Mail Policy Details** is added in the new web interface of your email gateway. Use this report to view the number of messages that match a configured mail policy. For more information, see the “Using Email Security Monitor” chapter in the user guide or online help.
New Message Tracking Filter for mail policy details	A new message tracking filter - **Mail Policy** is added in the Message Tracking > Advanced Search > Message Event option in the new web interface of your email gateway. Use this option to search for incoming or outgoing messages that match the configured mail policy name entered in the ‘Mail Policy Name’ field.

Enhanced Overview and Incoming Mail reporting pages	The following are the enhancements made to the Overview and Incoming Mail reporting pages in the legacy web interface of your email gateway: **Overview** report page: • Added new message category – Stopped by Domain Reputation Filtering in the Incoming Mail Summary section. • Changed Stopped by Reputation Filtering message category name to Stopped by IP Reputation Filtering in the Incoming Mail Summary section. **Incoming Mail** report page: • Added new column – Stopped by Domain Reputation Filtering in the Incoming Mail Details section. • Changed Stopped by Reputation Filtering column name to Stopped by IP Reputation Filtering in the Incoming Mail Details section. For more information, see the "Using Email Security Monitor" chapter in the user guide or online help.
Enhanced Mail Flow Summary and Mail Flow Details reporting pages	The following are the enhancements made to the Mail Flow Summary and Mail Flow Details reporting pages in the new web interface of your email gateway: **Mail Flow Summary** report page: • Added new category – Stopped by Domain Reputation Filtering in the Threat Messages graph section. • Changed Stopped by Reputation Filtering category name to Stopped by IP Reputation Filtering in the Threat Messages graph section. • Added new column – Stopped by Domain Reputation Filtering in the Threat Detection Summary section. • Changed Stopped by Reputation Filtering column name to Stopped by IP Reputation Filtering in the Threat Detection Summary section. **Mail Flow Details** report page: • Added new column – Stopped by Domain Reputation Filtering in the Incoming Mails section for IP Addresses, Domains, and Network Owners. • Changed Stopped by Reputation Filtering column name to Stopped by IP Reputation Filtering in the Incoming Mails section for IP Addresses, Domains, and Network Owners. For more information, see the "Using Email Security Monitor" chapter in the user guide or online help.

Support for New Content Matching Classifiers - National Identification Numbers for Southeast Asian countries	You can create a DLP policy using any one of the following new content matching classifiers - National Identification Numbers for Southeast Asian countries: • Indonesia KTP • Malaysia MyKad • Thailand ID • Philippines UMID • Singapore NRIC You can select the new content matching classifiers in the following pages of the web interface in your email gateway: • Go to Mail Policies > DLP Policy Manager > Add Custom Policy page > Predefined Custom Classifiers > **Policy Matching Details** option. • Go to Mail Policies > DLP Policy Manager > Add Custom Policy page > Create Custom Classifier > **Entity rule** option. • Go to Mail Policies > DLP Policy Manager >Add DLP Policy page > **Privacy Protection** template option. • Go to Mail Policies > DLP Policy Customizations > Add Custom Classifier page > **Entity** rule option.
New Remediation Report Status Widget	A new widget - ’Remediation Report Status’ is added when you search and remediate messages in the Message Tracking page of the new web interface of your email gateway. Use this widget to check the status of the Remediation Report generation. For more information, see the "Remediating Messages in Mailboxes" chapter in the user guide or online help.
Performing Remedial Actions on Messages in Cisco SecureX Threat Response	In Cisco SecureX Threat Response, you can now investigate and apply the following remedial actions on messages processed by your email gateway: • Delete • Forward • Forward and Delete For more information, see the “Integrating with Cisco SecureX Threat Response"chapter in the user guide or online help.
AMP Upstream Proxy Settings for File Analysis	You can now configure an upstream proxy for file analysis. For more information, see Enabling and Configuring File Reputation and Analysis Services section in the “File Reputation Filtering and File Analysis” chapter in the user guide or online help.

Content Filter - Attachment File Info condition and Strip by Attachment File Info action Enhancements	A new option - **File Hash List** is added in the Content Filters - "Attachment File Info" condition and "Strip by Attachment File Info" action. Use this option to configure a content filter to take action on message attachments that match a specific file SHA-256 value in the selected file hash list. **Note** You can also configure this functionality using message filters. For more information, see "Content Filter Conditions" and "Content Filter Actions" sections in the "Content Filters" chapter in the user guide or online help.
Smart Software Licensing Enhancements	AsyncOS 14.0 includes the following smart software licensing enhancements: • In a clustered configuration, you can now enable smart software licensing and register all the machines simultaneously with the Cisco Smart Software Manager. • After you enabled smart software licensing and registered your email gateway with the Cisco Smart Software Manager, the Cisco Cloud Services portal is automatically enabled and registered on your email gateway. • You can view details of the smart account created in the Cisco Smart Software Manager portal using the `smartaccountinfo` command in the CLI. • If the Cisco Cloud Services certificate is expired, you can now download a new certificate from the Cisco Talos Intelligence Services portal using the `cloudserviceconfig` > `fetchcertificate` sub command in the CLI. For more information, see: • "Smart Licensing in Cluster Mode" and "Registering the Email Gatewaywith Cisco Smart Software Manager" sections in the "System Administration" chapter of the user guide or online help. • "Smart Software Licensing" and "Configuring Cisco Cloud Service Portal Settings and Usage" sections of the *CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*.
Security Enhancements	AsyncOS 14.0 includes the following security enhancements: • The email gateway now sends the Cisco Technical Support requests over TLS. If your SMTP server is not using TLS, the requests are sent as plain text. • You can now configure your email gateway to send alerts over TLS. Use the following subcommand in the CLI to configure this functionality: `alertconfig > SETUP > Do you want to enable TLS support to send alert messages`?. For more information, see "Example: Sending Alerts over TLS" section of the *CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*.

Support for Internationalized Domain Name (IDN)	Cisco Secure Email Gateway can now receive and deliver messages with email addresses that contain IDN domains. Currently, your email gateway provides support of IDN domains for the following languages only: • **Indian Regional Languages**: Hindi, Tamil, Telugu, Kannada, Marati, Punjabi, Malayalam, Bengali, Gujarati, Urdu, Assamese, Nepali, Bangla, Bodo, Dogri, Kashmiri, Konkani, Maithili, Manipuri, Oriya, Sanskrit, Santali, Sindhi, and Tulu. • **European and Asian Languages**: French, Russian, Japanese, German, Ukrainian, Korean, Spanish, Italian, Chinese, Dutch, Thai, Arabic, and Kazakh. For this release, you can only configure few features using IDN domains in your email gateway. For more information, see Features Configurable using IDN Domains in Email Gateway, page 28.
No Support for Sender Domain Age functionality post AsyncOS 14.0 Release	There will be no support for the Sender Domain Age functionality post the AsyncOS 14.0 release. The Sender Domain Age functionality will be replaced with the Sender Maturity feature. 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 90 days, and beyond this limit, a domain is considered mature as an email sender, and no further details is provided. 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.
Alert or Notification Banner for End-of-Life (EOL) or End-of-Service (EOS) AsyncOS Version or Hardware Model	You will now receive an alert or notification banner message on your email gateway web interface or CLI, if your email gateway is running on an End-of-Life (EOL) or End-of-Service (EOS) AsyncOS version or hardware model.
Virtual Email Gateway Support for Amazon Web Services (AWS)	You can deploy Cisco Secure Email Virtual Gateway on Amazon Elastic Compute Cloud (EC2) on Amazon Web Services (AWS). Contact your Cisco sales representative with your AWS account details (username and region) to provision an AMI image.
Support for Cloud Connector Logging	The email gateway now supports a new type of log subscription - **Cloud Connector Logs**. Use this log subscription to view information about Web Interaction Tracking data from Cisco Aggregator Server. Most of the information is present at the Info or Warning Level.

Enhancement for Request Retry Method of File Reputation Service	You can now set the reputation query timeout value within the range of 20–30 seconds while configuring the file reputation and analysis services (Security Services > File Reputation and Analysis). The default value is 20, which is the minimum value. During the configured query timeout, the email gateway sends the file reputation queries to the AMP server. If the email gateway fails to receive response from the AMP server, it retries by sending the query again to the AMP server. The query timeout includes the time taken for the first query request and the retry request. The retry method enables the email gateway to receive responses when there are network latencies, issues related to the AMP server, and so on.
New Cisco Talos Email Status Portal	The Cisco Talos Email Status Portal replaces the legacy Cisco Email Submission and Tracking Portal. The Cisco Talos Email Status Portal is a web-based tool for monitoring the status of email submissions from end-users. **Important:** • Users of the legacy portal can still access their previous submissions in the new portal. • You will not be able to submit samples of spam, phish, ham, marketing or non-marketing emails that may have been misidentified by your email gateway in the new portal. For more information on how to submit email samples, see the How to Submit Email Messages to Cisco document at https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214133-how-to-submit-email-messages-to-cisco.html# For more information, see the "Managing Spam and Graymail" chapter in the user guide or online help.
Authentication Logs Enhancement	You can now view the user privilege role details (for example, 'admin,', 'operator,' and so on) of the logged-in user in the authentication logs.
Office 365 or Hybrid (Graph API) Remediation Account Profile Configuration Enhancement	You can now validate the client credentials for the Office 365 or Hybrid (Graph API) remediation account profile using the Client Secret value of the application generated on the Azure Management Portal. For more information, see the "Remediating Messages in Mailboxes" chapter in the user guide or online help.
New Passphrase Rule for defining login passphrases	A new passphrase rule is added in your email gateway to define your login passphrase: `Avoid usage of passphrases that contain three or more repetitive or sequential characters, (for example, 'AAA@124,' 'Abc@123,' and so on.)` You can configure this passphrase rule in any one of the following ways: • System > Administration > Users > Local User Account & Passphrase Settings > **Reject three or more repetitive or sequential characters in passphrases** check box in the web interface. • `userconfig > POLICY > PASSWORDSTRENGTH > Reject passphrases that contain three or more repetitive or sequential characters? [Y]>` command in the CLI

Creating system-generated passphrases	In addition to creating a login passphrase manually, you can now also create a system-generated passphrase to log in to your email gateway. You can configure the system-generated passphrase in any one of the following ways: • Options > Change Passphrase page in the web interface. • System Administration > System Setup Wizard page in the web interface. • System Administration > Users > Add Local User page in the web interface. • `passphrase` or `passwd` commands in the CLI.
Performing FQDN Validation for Certificates	You can configure your email gateway to perform FQDN validation for certificates in the following scenarios: • Importing a custom certificate. • Creating a self-signed S/MIME certificate. • Creating a self-signed certificate. • Importing a custom Certificate Authority (CA) list. **Note** You can also perform FQDN validation for email gateway certificates that contain IDN domains. For more information, see "S/MIME Security Services" and "Encrypting Communication with Other MTAs" chapters in the user guide.
Performing FQDN Validation for Peer Certificate during SSL Communication	You can configure your email gateway to perform FQDN validation for peer certificate in System Administration > SSL Configuration page in the web interface. The FQDN validation is applicable for the following services: • Outbound SMTP • LDAP • Updater • Alert over TLS **Note** You can perform FQDN validation for peer certificates that contain IDN domains for the 'Outbound SMT'P services only. For more information, see the “System Administration” chapter in the user guide.

Performing x509 Validation for Peer Certificate during SSL Communication	You can configure your email gateway to perform x509 validation for peer certificate in System Administration > SSL Configuration page in the web interface. The x509 validation is applicable for the following services: • Outbound SMTP • LDAP • Updater • Alert over TLS For more information, see the "System Administration" chapter in the user guide.

Consolidated Event Logs Enhancement	Following are the enhancements made to the 'Consolidated Event Logs' log type:
	• A new log field - **Message Size** is added in the 'Consolidated Event Logs' log type to view the message size in the single log line output.
	• You can now view the size of the attachment in the message in a single log line output.
	Steps:
	a. Select the 'File(s) Details' log field when configuring the log subscription for the Consolidated Event Logs.
	b. Configure a message filter rule as follows:
	`Custom_ Log_Entry: if (true) {`
	`log-entry("$filesizes");`
	OR
	Configure the **Add Log Entry** content filter action by adding the customized text as '`$filesizes`.'

Configuring Email Gateway to consume SecureX Threat Response Feeds	You can configure your email gateway to consume threat feeds from the Cisco SecureX Threat Response portal. The Cisco SecureX Threat Response portal allows you to create custom feeds for the continuous gathering of observables and to consume them in your email gateway using the feed URL. A feed is a simple list of observables in JSON format. The feeds are created and managed in the **Intelligence** > **Feeds** page in the SecureX Threat Response portal. For more information, see: • "How to Configure Email Gateway to Consume External Threat Feeds" and "Configuring SecureX Threat Response Feeds Source" sections in the "Configuring Email Gateway to Consume External Threat Feeds" chapter of the user guide associated with this release. • "Configuring Email Gateway to Consume External Threat Feeds" section in "The Commands: Reference Examples" chapter of the CLI reference guide associated with this release.

<table>
<tr><td>Rebranded Product and Related Documentation</td><td>We have rebranded the product and related documentation as follows:
<table>
<tr><th>Old Terminology</th><th>Rebranded Terminology</th></tr>
<tr><td>Cisco Email Security Appliance</td><td>Cisco Secure Email Gateway</td></tr>
<tr><td>Cisco Cloud Email Security Appliance</td><td>Cisco Secure Email Cloud Gateway</td></tr>
<tr><td>Cisco Content Security Management Appliance</td><td>Cisco Secure Email and Web Manager</td></tr>
</table></td></tr>
<tr><td>Bias-Free Terminology Usage in Product and Related Documentation</td><td>We have removed all bias terms in the product and related documentation.
The following table shows the list of bias terms replaced with the new bias-free terms:
<table>
<tr><th>Bias Terms</th><th>Bias-Free Terms</th></tr>
<tr><td>whitelist</td><td>allowed list</td></tr>
<tr><td>blacklist</td><td>blocked list</td></tr>
<tr><td>master</td><td>primary</td></tr>
<tr><td>slave</td><td>secondary</td></tr>
<tr><td>blackhole</td><td>sink hole</td></tr>
</table></td></tr>
</table>

Changes in Behavior

- Changes in Behavior in AsyncOS 14.0.1, page 15
- Changes in Behavior in AsyncOS 14.0, page 18

Changes in Behavior in AsyncOS 14.0.1

Changes in Appliance Grouping for File Analysis	Prior to this release, if you configured an appliance group in your email gateway, you could not modify the group. After you upgrade to this release, you can now use the `ampconfig > setup` sub command in the CLI to modify the appliance group.
Sender Domain Reputation (SDR) Verification Changes on Mail Flow Policy	Before the upgrade, if you configured a mail flow policy with the relay connection behavior on a public listener and the Sender Domain Reputation Verification option turned on by default in your email gateway. On upgrade, the Sender Domain Reputation Verification option is turned off automatically in the mail flow policy. You need to manually enable the Sender Domain Reputation Verification option for the mail flow policy in the web interface of your email gateway.

URL Filtering Changes	Prior to this release, you could only configure the advanced URL filtering settings at the machine level using the `websecurityadvancedconfig` command in the CLI. After you upgrade to this release, you can now configure the advanced URL filtering settings at the machine level and cluster level using the `websecurityadvancedconfig` command in the CLI. **Note** Suppose you have configured different advanced URL filtering settings for each machine in a cluster. On upgrade, the system configures the maximum value for each advanced URL filtering setting for all machines at the cluster level.
URL Logging Changes	Prior to this release, you could only enable logging of URL-related information in your email gateway using the `outbreakconfig` command in the CLI. After you upgrade to this release, you can only enable logging of URL-related information in your email gateway in any one of the following ways: • `websecurityadvancedconfig` command in the CLI • Security Services > URL Filtering page in the web interface. For more information, see the: • 'Enable URL Filtering' section in the 'Protecting Against Malicious or Undesirable URLs' chapter of the user guide associated with this release. • 'URL Filtering' section in 'The Commands: Reference Examples' chapter of the CLI Reference Guide associated with this release.
Mail Processing Changes in Email Gateway	Prior to this release if you enabled the 'Action for unscannable messages due to RFC Violations' option, the email gateway would not mark messages that do not contain a "From:" header field or contain multiple "From:" header fields as "unscannable" due to RFC violation. After you upgrade to this release, if you enable the 'Action for unscannable messages due to RFC Violations' option, the email gateway now marks messages that do not contain a "From:" header field or contain multiple "From:" header fields as "unscannable" due to RFC violation.
New Help Text for Other TLS Client Services option	A new help text is added for the Other TLS Client Services option in the following web pages of your email gateway: • System Administration > SSL Configuration page • System Administration > SSL Configuration > Edit SSL Configuration page The help text message details the list of services used for the TLS method you select for the 'Other TLS Client Services' option.

Certificate Expiry Alert Changes	Prior to this release, the email gateway would send a system alert when device certificates and custom CA certificates are about to expire, and the Custom List option was disabled in the Network > Certificate > Edit Settings page. After you upgrade to this release, the email gateway now sends a system alert when • Custom CA certificates are about to expire, and the Custom List option is enabled in the Network > Certificate> Edit Settings page. • Device certificates are about to expire. The following is an example of a system alert generated when a custom CA certificate is about to expire: `Your certificate "Cisco" expires in 3 days, 4:45:20 hour(s). Use the certconfig -> certauthority -> custom -> delete. sub command in the CLI to delete any unused custom CA certificates in the CA list.`
SSL Cipher Changes for LDAP Profile	Prior to this release, if you selected the 'Use SSL' option for the LDAP profile and switched from a non- FIPS mode to the FIPS mode, the same SSL ciphers available in the non-FIPS mode would be displayed for the LDAP profile in the FIPS mode. After you upgrade to this release, if you select the 'Use SSL' option for the LDAP profile and switch from a non- FIPS mode to the FIPS mode, the SSL ciphers are displayed as 'FIPS' in the LDAP profile. Also, if you switch back to the non-FIPS mode with the 'Use SSL' option already selected for the LDAP profile, the following default SSL ciphers are displayed in the LDAP profile: `ECDHE-RSA:ECDHE-ECDSA:DHE-DSS-AES:AES128:AES256:!DHE-RSA-AE256-SHA:!ECDHE-ECDSA-AES256-SHA:!DHE-DSS-AES256-SHA:!DH-RSA-AES128-SHA:!DH-DSS-AES128-SHA:!DH-RSA-AES256-SHA256:!DH-DSS-AES256-SHA256:!DH-RSA-AES256-SHA:!DH-DSS-AES256-SHA:!aNULL`
Unsupported SSL Cipher Changes in LDAP Profile	Prior to this release, if you already selected the 'Use SSL' option and configured non-supported SSL ciphers for the LDAP profile. On upgrade to Secure Email version 14.0.1, the unsupported SSL ciphers are replaced with the following default SSL ciphers: `ECDHE-RSA:ECDHE-ECDSA:DHE-DSS-AES:AES128:AES256:!DHE-RSA-AES256-SHA:!ECDHE-ECDSA-AES256-SHA:!DHE-DSS-AES256-SHA:!DH-RSA-AES128-SHA:!DH-DSS-AES128-SHA:!DH-RSA-AES256-SHA256:!DH-DSS-AES256-SHA256:!DH-RSA-AES256-SHA:!DH-DSS-AES256-SHA:!aNULL.`
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 Behavior in AsyncOS 14.0

URL Reputation Verdict Name Changes in Cisco Secure Email Gateway	Cisco Talos has introduced new categories and new names for the existing URL Reputation verdicts. Currently, there are no configuration or reporting changes needed on the Cisco Secure Email Gateway. See the following table in New Categories and New Names for Existing URL Reputation Verdicts, page 30 to view the new categories and new names for the existing URL Reputation verdicts in your email gateway. For more information, see the Cisco Talos blog at https://blog.talosintelligence.com/2019/09/new-cisco-talos-web-reputation-verdicts.html
Anti-Spam Configuration Changes	Metadata analysis and other language-agnostic features used in CASE machine learning systems have minimized the efficacy differences between the Chinese regional and the global scanning profiles in the Anti-Spam configuration settings of your email gateway. You can now use the global scanning profile instead of the Chinese regional scanning profile for faster detection of threats that provides better efficacy to organizations situated in China, Taiwan, and Hong Kong.
No Support for `threatresponseconfig` and `csnconfig` CLI commands	From AsyncOS 14.0 release onwards, the `threatresponseconfig` and `csnconfig` CLI commands are no longer supported. You can now use the `cloudserviceconfig` CLI command to configure the functionalities of `threatresponseconfig` and `csnconfig` CLI commands. For more information, see the "Configuring Cisco Cloud Service Portal Settings and Usage" section of the *CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*.
Integrating Email Gateway with Cisco SecureX Threat Response Changes	Prior to this release, you needed to enable and register your email gateway with Cisco SecureX Threat Response to complete the integration. After you upgrade to this release, you need to enable and register your email gateway with the Cisco Cloud Services portal and then enable Cisco SecureX Threat Response on your email gateway to complete the integration. **Note** If you have enabled smart software licensing and registered your email gateway with the Cisco Smart Software Manager, the Cisco Cloud Services portal is automatically enabled and registered on your email gateway. You only need to manually enable Cisco SecureX Threat Response on your email gateway to complete the integration. For more information, see the "Integrating with Cisco SecureX Threat Response"chapter of the user guide.

Changes in Logging Details	From this release onwards, all sensitive data such as 'passphrases,' 'registration tokens,' and so on are no longer displayed in the CLI and Mail logs generated by the email gateway. **Note** By default, all sensitive data is replaced by generic customized messages
No Async0S version details in Secure Email Gateway Swagger page	From this release onwards, you will no longer see the AsyncOS version details in the Secure Email Gateway API Swagger page.
AMP Engine Logs Changes	From this release onwards, the SHA-256 value is displayed in text format in the AMP Engine logs.
Encrypting Sensitive Data in Email Gateway in FIPS or Non-FIPS mode	A new CLI sub command - `encryptconfig` is added under the `fipsconfig` CLI command to encrypt sensitive data in your email gateway, irrespective of FIPS or non-FIPS mode
Email Gateway Certificate Changes for FIPS mode only	From this release onwards, you will no longer be able to import, edit, or paste an email gateway certificate, if the intermediate certificate expires or fails the CRL validation.
Registering Email Gateway with Cisco Talos Email Status Portal Changes	You must now obtain a registration ID from the new Cisco Talos Email Status Portal before you register your email gateway with the new portal. For more information, see “Managing Spam and Graymail” chapter in the user guide or online help.
File Reputation Query Timeout Changes	The email gateway now adds extra buffer time of 2 seconds to the total timeout period during the file reputation query process.
Message Tracking- Show Details Page Changes	From this release onwards, you can view a maximum of 20000 records of message processing details for a single MID in the Message Tracking > Search > Show Details page.
Host Header Configuration Changes	Prior to this release, you could enable your email gateway to respond to HTTP requests using the configured base hostname only. After you upgrade to this release, if you enable the `hostheader` option under `adminaccessconfig` CLI command, you can configure your email gateway to respond to HTTP requests using: • Configured base host name. • (Optional) Hosts added to the allowed host list.
Changes in 'Filtering by Sender and Recipients field for DLP Policy Matching	From this release onwards, when you configure a DLP policy in your email gateway, entries for users (sender or recipient) in the 'Filtering by Sender and Recipients' fields are case-insensitive. For example, if you enter the recipient Joe@ for a user, a message sent to joe@example.com will match based on the configured DLP policy.

System Health Check Changes	Prior to this release, the system health check was done automatically during the upgrade process. After you upgrade to this release, you can perform the system health check manually in any one of the following ways: • Go to System Administration > System Health > Run System Health Check option in the web interface. See the “System Administration” chapter in the user guide. • Use the `healthcheck` command in the CLI. See the *“CLI Reference Guide for AsyncOS for Cisco Email Security Appliances.”*
Disclaimer Changes during Decoding Errors	If the disclaimer added to the footer or header of the message generates a decoding error, the disclaimer or message body is split into separate message attachment.
SSH Server Configuration Changes	The following SSH server configuration changes are only applicable when you install AsyncOS 14.0 for Cisco Secure Email Gateway for the first time: The following cipher algorithm and MAC methods are disabled in your email gateway by default: • **Cipher Algorithm** - `3des-cbc` • **MAC Methods**: – `mac-md5` – `umac-64@openssh.com` – `hmac-ripemd160` – `hmac-ripemd160@openssh.com` – `hmac-sha1-96` – `hmac-md5-96` If you want to enable the above cipher algorithm and MAC methods., use the `sshconfig` > `SSHD` > `setup` sub command in the CLI. [**FIPS Mode only**] Before you enable FIPS mode on your email gateway, make sure to remove the following cipher algorithms that are not supported for FIPS mode: • `aes192-ctr` • `rijndael-cbc@lysator.liu.se` Use the `sshconfig` > `SSHD` > `setup` sub command in the CLI to remove the above-mentioned cipher algorithms in your email gateway.

File Reputation Service Configuration Changes	There is no option to enable or disable SSL communication when you configure the File Reputation service in your email gateway. The email gateway uses the SSL protocol by default to communicate with the File Reputation service using firewall port 443 only. The following options to configure SSL communication settings for the File Reputation service in your email gateway are removed: • The **Use SSL (Port 443)** checkbox in Security Services > File Reputation and Analysis page in the web interface of your email gateway. • The `Do you want to enable SSL communication (port 443) for file reputation? [Y]>` statement in `ampconfig` > `advanced` sub command in the CLI.
External Threat Feeds - File Hash Configuration Changes	The email gateway now detects file hashes categorized as malicious by the External Threat Feeds (ETF) engine, irrespective of the letter case (uppercase or lowercase) and applies appropriate configured actions on the message.
Notification Email Changes	Prior to this release, if you had configured a content filter action to send notification emails to certain recipients, the email gateway would send a single notification mail to all the recipients of the original message. After you upgrade to this release, the email gateway now sends the notification mail only to the recipients defined in the content filter action.

Certificate Authority Configuration Changes	The Certificate Authority (CA) configuration changes are applicable in any one of the following scenarios: • Upgrade from a lower AsyncOS version to AsyncOS 14.0 version and later. • Install AsyncOS 14.0 for Cisco Secure Email Gateway for the first time. The following changes are made to the Certificate Authorities list: • You can view the count and details of custom and system CA certificates in your email gateway. Use the **Managed Trusted Root Certificates** option in Network > Certificates > page to view the custom or system CA certificate details. • You can upload, delete, or append the custom CA certificate in your email gateway. • You will not be able to upload duplicate custom CA certificates to your email gateway. • [**Applicable for new AsyncOS install only**]: You can update the existing system CA certificate bundle to the latest available version. Use the **Update Now** option in Network > Certificates page in the web interface or the `updatenow` CLI command to update the existing system CA certificate bundle. • [**Applicable for AsyncOS upgrade only**]: – During upgrade, you can choose to append the valid CA certificates from the system CA bundle (of the current AsyncOS build) to the custom CA bundle of the upgraded AsyncOS build. **Note** The backup of the current system CA bundle is stored in the following location - `/data/pub/systemca.old/trustedca.old.pem` – After upgrade, the system CA certificate bundle of the current AsyncOS build is updated to the latest version automatically.

SSL Cipher Configuration Changes	The following SSL cipher configuration changes are only applicable when you install AsyncOS 14.0 for Cisco Secure Email Gateway for the first time: • The TLS_DHE_RSA_WITH_AES_256_CBC_SHA cipher suite is no longer supported for TLS 1.2 client and server services (HTTPS GUI, SMTP Outbound, and SMTP Inbound). • The following cipher suites are no longer supported for TLS 1.2 client services (HTTPS GUI, SMTP Outbound, and SMTP Inbound): – TLS_DHE_RSA_WITH_AES_256_CBC_SHA – TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA – TLS_DHE_DSS_WITH_AES_256_CBC_SHA – TLS_DH_RSA_WITH_AES_128_CBC_SHA – TLS_DH_DSS_WITH_AES_128_CBC_SHA – TLS_DH_RSA_WITH_AES_256_CBC_SHA256 – TLS_DH_DSS_WITH_AES_256_CBC_SHA256 – TLS_DH_RSA_WITH_AES_256_CBC_SHA – TLS_DH_DSS_WITH_AES_256_CBC_SHA The following SSL configuration change is applicable in any one of the following scenarios: • Upgrade from a lower AsyncOS version to AsyncOS 14.0 version and later. • Install AsyncOS 14.0 for Cisco Secure Email Gateway for the first time. [Only if X509 validation is enabled] The following signature algorithms for Peer Certificates (such as LDAP, SMTP Outbound, Updater, and Alert Receivers) are no longer supported: 'sha1withrsaencryption', 'sha224withrsaencryption', 'ecdsa-with-sha1', 'ecdsa-with-sha224', 'md2withrsaencryption', 'md4withrsaencryption', 'md5withrsaencryption', 'ripemd128withrsaencryption', 'ripemd160withrsaencryption', 'ripemd256withrsaencryption', 'secp224r1', 'secp192r1', 'brainpoolP160r1', 'brainpoolP192r1', 'secp160r1', 'secp160r2', 'secp192k1', 'secp224k1', 'secp256k1', 'sect163k1', 'sect163r2', 'sect193r1', 'sect193r2', 'sect233k1', 'sect233r1', 'sect239k1', 'sect283k1', 'sect283r1', 'sect409k1', 'sect409r1', 'sect571k1', 'sect571r1'

Client Certificate Changes	From this release onwards, the following client certificate changes are applicable when you enable the FIPS mode in your email gateway: • If the root Certificate Authority (CA) that signed the client certificate has expired, you will now not be able to import or edit the client certificate in the email gateway. • If the intermediate CA that signed the client certificate has expired or revoked, you will now not be able to import or edit the client certificate in the email gateway. **Solution**: Make sure you perform any one of the following actions to manage the client certificate: • Sign your client certificate with a valid root CA and upload it to the email gateway. • Sign your client certificate with an intermediate CA that is valid or not revoked and upload it to the email gateway.
Mail Logs and Tracking Logs Changes	Prior to this release the information in the subject of the Mail Logs and Tracking Logs was enclosed in quotes. After you upgrade to this release, the information in the subject of the Mail Logs and Tracking Logs is now not enclosed in quotes.
Smart Identifier Changes	Prior to this release, the email gateway would detect a smart identifier in the message, irrespective of the keyword added before the smart identifier. After you upgrade to this release, the email gateway now detects a smart identifier, only if the message contains the keyword ('credit,' 'ssn,' 'cusip,' or 'aba') added before the smart identifier. For Example: If a message contains a Social Security number (XXX-XX-XXXX'), the email gateway detects the Social Security number as a smart identifier only if there is a keyword - 'ssn' added before the Social Security number ('ssn XXX-XX-XXXX,' 'ssn: XXX-XX-XXXX,' and so on.)
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.

Upgrade Paths

Upgrading to Release 14.0.1-033 - MD (Maintenance Deployment)

You can upgrade to release 14.0.1-033 from the following versions:

- 12.5.3-035
- 12.5.3-107
- 13.0.0-392
- 13.0.1-030
- 13.0.2-030
- 13.5.1-277
- 13.5.2-036
- 13.5.3-010
- 13.5.4-020
- 13.7.0-093
- 14.0.0-698
- 14.0.1-032

Upgrading to Release 14.0.0-698 - GD (General Deployment) Refresh

You can upgrade to release 14.0.0-698 from the following versions:

- 12.5.1-037
- 12.5.2-011
- 12.5.3-035
- 13.0.0-392
- 13.0.1-030
- 13.0.2-030
- 13.5.1-277
- 13.5.2-036
- 13.5.2-103
- 13.5.2-204
- 13.5.3-010
- 13.7.0-093
- 13.7.0-094
- 14.0.0-484
- 14.0.0-657
- 14.0.0-692

Upgrading to Release 14.0.0-692 - GD (General Deployment)

You can upgrade to release 14.0.0-692 from the following versions:

- 12.5.1-037
- 12.5.2-011
- 12.5.3-035
- 13.0.0-392
- 13.0.1-030
- 13.0.2-030
- 13.5.1-277
- 13.5.2-036
- 13.5.2-103
- 13.5.3-010
- 13.7.0-093
- 14.0.0-484
- 14.0.0-657

Upgrading to Release 14.0.0-484 - LD (Limited Deployment)

You can upgrade to release 14.0.0-484 from the following versions:

- 12.5.3-035
- 13.0.0-392
- 13.0.2-030
- 13.5.1-277
- 13.5.3-010
- 13.7.0-093
- 14.0.0-450

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 27.

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 37, 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 28
- New Categories and New Names for Existing URL Reputation Verdicts, page 30
- Firewall Settings to Access Cisco Talos Services, page 30
- Firewall Settings to Access Cisco Advanced Phishing Protection Cloud Service, page 31
- Enabling Service Logs on Email Gateway, page 31
- Upgrading Intelligent Multi-Scan and Graymail Configurations at Cluster Levels, page 31
- FIPS Compliance, page 32
- Reverting to Previous AsyncOS Versions, page 32
- Upgrading Deployments with Centralized Management (Clustered Appliances), page 32
- Upgrading From a Release Other Than the Immediate Previous Release, page 32
- Configuration Files, page 32
- IPMI Messages During Upgrade, page 32

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.
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 14.0, 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 14.0.1 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 14.0.1.

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

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 26.
- If you are upgrading a virtual email gateway, see Upgrading a Virtual Appliance, page 27.

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 35.
- 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

- Scanning Password-Protected Attachments in Email Gateway, page 34
- [Smart Licensing users only] Unable to Connect Email Gateway to Cisco Talos Services, page 34
- Inconsistency in DLP Settings at Cluster Level after Upgrading to AsyncOS 13.x, page 34
- Intelligent Multi-Scan and Graymail Global Configuration Changes, page 34

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, page 35
- Lists of Known and Fixed Issues, page 35
- Related Documentation, page 36

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 and Fixed Issues for 14.0.1, page 35
- Known and Fixed Issues for 14.0, page 36

Known and Fixed Issues for 14.0.1

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=14.0.1&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=14.0.1-033&prdNam=Cisco%20Secure%20Email%20Gateway

Known and Fixed Issues for 14.0

Known Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=14.0.0&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=14.0.0-698&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, 14.0.1

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 Secure Web Appliance	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

Documentation For Cisco Content Security Products	Location
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 Secure Email Encryption Service	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.

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.