



Customer Notification for AsyncOS 15.5 Release for Cisco Secure Email Gateway - New Features and Behavior Changes

Published Date: March 12, 2024

Contents

- [Release Date, page 1](#)
- [New Features, page 2](#)
- [Behavior Changes, page 6](#)
- [Service and Support, page 8](#)

Release Date



Release Date: March 20, 2024





Cisco Systems, Inc.
www.cisco.com

New Features

Feature	Description
Configuring Threat Scanner for Threat Detection	<p>In the AsyncOS 15.0 release, the Threat Scanner feature was introduced to detect threats on incoming messages. In this release, you could not directly configure Threat Scanner to detect threats and it was configured in the back end.</p> <p>From this release onwards, you can configure Threat Scanner to detect incoming threats on your email gateway. You can enable or disable Threat Scanner for each incoming mail policy. When you enable Threat Scanner, it scans the incoming messages and influences the Anti-Spam verdict.</p> <p>Prerequisite: You must enable Graymail Global Settings to enable Threat Scanner.</p> <p>You can configure Threat Scanner per policy in the following ways:</p> <ul style="list-style-type: none"> • Web Interface: Navigate to Mail Policies > Incoming Mail Policies and click the link under the Anti-Spam column of the mail policy to open the Mail Policies: Anti-Spam page. You can check or uncheck the Enable Threat Scanner check box. • CLI: Use the <code>policyconfig</code> command. <p>Install and Upgrade Scenarios</p> <p>When you install or upgrade your email gateway from AsyncOS 15.0 or earlier versions to AsyncOS 15.5 release, Threat Scanner will be disabled by default.</p> <p>For more information, see the "Defining Anti-Spam Policies" section in the "Managing Spam and Graymail" chapter of the <i>User Guide for AsyncOS 15.5 for Secure Email Gateway</i>.</p> <p>For more information on configuring Threat Scanner using CLI, see the "Configuring Threat Scanner Per Policy" section in the "The Commands: Reference Examples" chapter of <i>CLI Reference Guide for AsyncOS 15.5 for Cisco Secure Email Gateway</i>.</p>


Including Additional Attributes for Improved Efficacy of SDR Service	<p>Your email gateway now includes the Additional Attributes (Display name and the complete email address - Username, and Domain) by default as part of telemetry data sent to Cisco TAC for reputation analysis to enhance the efficacy of the Sender Domain Reputation (SDR) service.</p> <p>When the administrator logs into the email gateway, you will receive a warning message informing that the Include Additional Attributes option in SDR is enabled by default so that telemetry data includes the processing of personal data.</p>  <p>Note The Include Additional Attributes option is enabled by default only when you enable Sender Domain Reputation Filtering.</p> <p>If you want to disable the Include Additional Attributes option:</p> <ol style="list-style-type: none"> 1. Navigate to Security Services > Domain Reputation 2. Click Edit Global Settings and uncheck the Include Additional Attributes check box. <p>For more information, see "Enabling Sender Domain Reputation Filtering on Email Gateway" section in "Sender Domain Reputation Filtering" chapter of the <i>User Guide for AsyncOS 15.5 for Secure Email Gateway</i>.</p>
C5 Nitro-Instance Support for AWS	<p>From the AsyncOS 15.5 release onwards, your email gateway supports c5.4xlarge EC2 instance type for the C600V model deployed through AWS.</p> <p>For more information, see Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual on AWS EC2 Installation Guide.</p>
Mandatory Usage of Cisco Smart Software Licensing for On-Premises Users	<p>The Cisco Smart Software Licensing usage is mandatory from this release (all releases post AsyncOS 15.0 release) for Cisco Secure Email Gateway.</p>  <p>Note From AsyncOS 15.5 onwards, there will be no support for classic licensing for On-Premises users. You will no longer be able to order new feature licenses or renew existing feature licenses in the Classic Licensing mode.</p> <p>Prerequisite: Make sure you create a smart account in the Cisco Smart Software Manager portal and enable Cisco Smart Software Licensing on your email gateway. For more information, see the "Smart Software Licensing" section in the "System Administration" chapter of the <i>User Guide for AsyncOS 15.5 for Secure Email Gateway</i>.</p> <p>After you enable Cisco Smart Software Licensing, you can upgrade your email gateway to this release and continue to use the existing feature licenses in the Smart Licensing mode.</p>

Configure Threat Defense Connector for individual incoming mail policies	<p>You can now configure Threat Defense Connector for each incoming mail policy. To use this feature, you must have configured and enabled the Threat Defense Connector in your Secure Email Gateway.</p> <p>Go to Mail Policies > Incoming Mail Policies to enable or disable Threat Defense Connector for individual mail policies.</p> <p>For more information, see "Integrating Secure Email Gateway with Threat Defense" chapter of the <i>User Guide for AsyncOS 15.5 for Secure Email Gateway</i>.</p>
Support of Large Key Size Values for DKIM Verification	<p>You can use the following large key size values for DKIM verification in your email gateway:</p> <ul style="list-style-type: none"> • 3072 key bits size • 4096 key bits size <p>You can select the new, large key size values for DKIM verification in the following ways:</p> <ul style="list-style-type: none"> • Web Interface: Go to <i>Mail Policies > Verification Profiles > Add Profile</i> or <i>Default</i> and select 3072 or 4096 from the 'Smallest Key to be Accepted:' or 'Largest Key to be Accepted:' drop down list fields. • CLI: Use <code>domainkeysconfig > keys > new or edit > Enter the smallest key to be accepted or Enter the largest key to be accepted</code> options and enter the required value that corresponds to 3072 or 4096 for a specific DKIM Verification profile.
No Support for 512 and 768 Key Size Values in New DKIM Verification profile	<p>From this release onwards, the 512 and 768 key bits size values are no longer supported when you create a new DKIM verification profile.</p> <div>  <p>Note The existing DKIM verification profiles created with 512 and 768 key size values are still supported on upgrade to this release.</p> </div>
TLS 1.3 Support for SSL Services	<p>You can now configure TLS 1.3 for the following TLS services in your email gateway:</p> <ul style="list-style-type: none"> • GUI HTTPS • Inbound SMTP • Outbound SMTP <p>The email gateway only supports the following TLS ciphers when you configure TLS 1.3 for the “GUI HTTPS,” “Inbound SMTP,” and “Outbound SMTP” TLS services:</p> <ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 <div>  <p>Note The email gateway does not allow you to modify the ciphers used for TLS 1.3.</p> </div> <p>After you configure TLS 1.3, you can use it for TLS communication across the legacy or new web interfaces of your email gateway and the API services.</p>

Obtaining File Hash Lists, RAT, SMTP Routes, Save and Load Configuration, Address List, and Incoming Mail Policy Users Information using AsyncOS APIs	<p>You can now obtain information about File Hash Lists, Recipient Access Table (RAT) entries, SMTP Routes, Save and Load Configuration, Address List, and Incoming Mail Policy Users information in your email gateway using AsyncOS APIs.</p> <p>For more information, see the “Configuration APIs” section of the <i>AsyncOS 15.5 API for Cisco Secure Email Cloud Gateway - Getting Started Guide</i>.</p>
Enforcing TLS for Outgoing Messages at Sender or Recipient Level	<p>The existing Destination Controls configuration allows you to override the TLS modes (such as TLS Mandatory, TLS Preferred, and so on) on a per-domain basis.</p> <p>If you need to enforce TLS for outgoing messages based on additional conditions such as – senders, recipients, and so on, you can now use the <code>X-ESA-CF-TLS-Mandatory</code> header.</p> <p>You can configure the “Content Filter – Add/Edit Header” action to add the <code>X-ESA-CF-TLS-Mandatory</code> header in the “Header Name:” field based on any content filter conditions and attach the content filter to an outgoing mail policy.</p>
Scanning Password-Protected Attachments in Messages	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>The following languages are supported for this feature - English, Italian, Portuguese, Spanish, German, French, Japanese, and Korean.</p> <p>For more information, see "Using Message Filters to Enforce Email Policies" in the <i>User Guide for AsyncOS 15.5 for Secure Email Gateway</i>.</p>
Region-based Polling for URL Retrospective Service	<p>You can configure the URL Retrospective Service region to which the Secure Email Gateway connects for verdict updates. The Secure Email Gateway ESA can update the Retrospective Service regions and associated end-point URLs.</p> <p>For more information, see the "Setting Up URL Filtering" section in the <i>User Guide for AsyncOS 15.5 for Secure Email Gateway</i>.</p>
File Analysis Server Region Enhancement	<p>From this release onwards, the File Analysis Server region supports two new regions - Australia and Canada.</p> <p>You can configure File Analysis Server region in the following ways:</p> <ul style="list-style-type: none"> • Web Interface: Navigate to Security Services > File Reputation and Analysis and click Edit Global Settings. • CLI: Use the <code>anpconf ig > ADVANCED</code> command. <p>For more information, see the "Enabling and Configuring File Reputation and Analysis Services" section in the "File Reputation Filtering and File Analysis" chapter of the <i>User Guide for AsyncOS 15.5 for Secure Email Gateway</i>.</p>

Behavior Changes

Application SSH Client Algorithm Support	<p>The following application SSH client algorithms are supported when you add an email gateway to a cluster.</p> <p>[Non-FIPS Mode]</p> <p>The following cipher algorithm, MAC method, and KEX algorithm are added to your Secure Email and Web Manager by default in addition to the existing algorithms:</p> <ul style="list-style-type: none"> • Cipher algorithms - aes128-ctr • MAC methods - hmac-sha2-256 • KEX algorithms - diffie-hellman-group14-sha256 <p>[FIPS Mode]</p> <p>The following cipher algorithm and MAC method are added to your Secure Email and Web Manager by default in addition to the existing algorithms:</p> <ul style="list-style-type: none"> • Cipher algorithms - aes128-ctr • MAC methods - hmac-sha2-256
Archive or Compressed File Processing by Advanced Malware Protection Engine	<p>From this release onwards, Secure Email Gateway sends the entire archive file to Cisco Secure Malware Analytics if one or more constituent files qualify for File Analysis. The entire archive file is marked malware if any constituent files are found malicious.</p> <p>If the Secure Email Gateway fails to extract a compressed or archive file, it will be uploaded to Secure Malware Analytics for analysis.</p>

<p>Prompt Statement Changes - FIPS Mode</p>	<p>From this release onwards, the prompt statements that you receive, when you enable FIPS mode, and when you enable MINIMIZEDATA in FIPS mode, are modified to include only SMTP instead of SMTP DANE. These statements are modified as the MINIMIZEDATA option under FIPS configuration is not specific to SMTP DANE and is common for SMTP.</p> <p>Modified Prompt Statement - Enabling FIPS Mode</p> <p><i>Do you want to minimize FIPS restriction on SMTP in the email gateway ? [N]></i></p> <p>Modified Prompt Statement - Enabling MINIMIZEDATA in FIPS Mode</p> <p><i>FIPS restriction is currently enforced for SMTP in the email gateway.</i></p> <p><i>When you change FIPS restriction, the email gateway reboots immediately. No commit is required.</i></p> <p><i>Do you want to minimize FIPS restriction on SMTP in the email gateway ? [N]></i></p>
<p>No Support for aes192- cbc Cipher in FIPS Mode</p>	<p>From this release onwards, the aes192- cbc cipher is not supported for both the SSH server and client in the FIPS mode. If you want to enable FIPS mode in AsynOS 15.5, you must remove the aes192- cbc cipher using the sshconf i g->SSH-D subcommand in the CLI.</p> <div data-bbox="719 959 764 999"></div> <p>Note If your email gateway is in FIPS mode and it is upgraded to the AsynOS 15.5 release, the aes192- cbc cipher is removed by default.</p>

Service and Support

**Note**

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2024 Cisco Systems, Inc. All rights reserved.