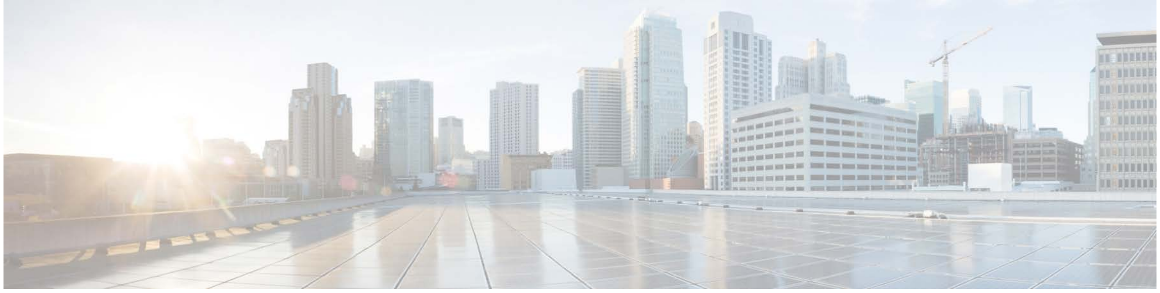

Release Notes for AsyncOS 15.5.1 for Cisco Secure Email Cloud Gateway - GD (General Deployment)

Published: April 30, 2024

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
Monitoring Vault Service and Sending Alerts	Your email gateway now monitors the Vault service and keeps track of its status, whether it is initialized or not. It also sends appropriate alert messages and logs status information into error_logs. You can access the alert logs using one of the following ways: • Navigate to **System Administration** > **Alerts** page on the web interface, and click the **View Top Alerts** button. • Use the `displayalerts` command in the CLI. If the Vault service fails to initialize due to any issues, you receive alert messages (in the mail, on the web interface, and in the CLI) to indicate that the Vault service is down, and you have to execute the Vault Recovery process to restore the Vault service. **Note** If the upgrade fails while upgrading to AsyncOS 15.5.1, then you should check for the Vault service error in upgrade_logs. If a Vault service error is identified, then you must restore the Vault service or proceed with the upgrade process without saving the configuration. You will receive alert messages in the following scenarios: • If the Vault service fails to initialize after you upgrade to AsyncOS 15.5.1, you receive alert messages through the mail, on the web interface, and in the CLI. • If any of the services of your email gateway use the Vault service that fails to initialize, you receive alert messages through the mail, on the web interface, and in the CLI. The alert messages sent depend on the encryption status. You can check the encryption status using the `fipsconfig` > `encryptconfig` subcommand. The Vault monitoring mechanism checks the Vault service every 75 minutes. If it is down, then it sends alert messages until the Vault service is restored. For information on an example of a successful vault health check and initialization log entry, see "Successful Vault Health Check and Initialization" section in "Logging" chapter of *User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway*.

	To restore the Vault service, you have to execute the Vault Recovery process. ⚠ **Caution** If the encryption (CLI > `fipsconfig` > `encryptconfig`) is enabled, ensure that you always save and keep a copy of email gateway's configuration to avoid data loss. For more information on how to save the email gateway's configuration, see Saving Email Gateway's Configuration, page 9. For information on how to execute the Vault Recovery process, see Executing Vault Recovery Process to Resolve Vault Issues, page 9.
Identifying Messages that Violate End-Of-Message RFC Standard	Your email gateway now identifies and filters the messages that violate the end-of-message RFC standard (that is, <CRLF.CRLF>) to detect threats. When email gateway receives a message with an invalid end-of-message sequence, it adds an **X-Ironport-Invalid-End-Of-Message** Extension Header (X-Header) to all message IDs (MIDs) within that connection until a message that complies with the end-of-message RFC standard is received. You can configure policies in content filters to perform necessary actions on these messages. For more information on configuring the CR and LF Handling field, see the "Listening for Connection Requests by Creating a Listener Using Web Interface" section of *User Guide for AsyncOS 15.5.1 for Secure Email Gateway.*
Restarting API Server through CLI	You can now restart the API server using a new CLI subcommand - `API_SERVER`. You can use the `API_SERVER` subcommand to restart and view the status of the API server. The `API_SERVER` subcommand is added under the `diagnostic` > `SERVICES` subcommand. For more information on the diagnostic command and the subcommands, see the "diagnostic" section in the "The Commands: Reference Examples" chapter of *CLI Reference Guide for AsyncOS 15.5.1 for Cisco Secure Email Gateway*.

Configuring Threat Scanner for Threat Detection	In the AsynOS 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. 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. **Prerequisite**: You must enable **Graymail Global Settings** to enable Threat Scanner. You can configure Threat Scanner per policy in the following ways: • **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 `policyconfig` command. **Install and Upgrade Scenarios** When you install or upgrade your email gateway from AsyncOS 15.0 or earlier versions to AsyncOS 15.5.1 release, Threat Scanner will be disabled by default. For more information, see the "Defining Anti-Spam Policies" section in the"Managing Spam and Graymail" chapter of the *User Guide for AsyncOS 15.5.1 for Secure Email Gateway*. 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 *CLI Reference Guide for AsyncOS 15.5.1 for Cisco Secure Email Gateway.*

Including Additional Attributes for Improved Efficacy of SDR Service	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. 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. **Note** The **Include Additional Attributes** option is enabled by default only when you enable Sender Domain Reputation Filtering. If you want to disable the Include Additional Attributes option: 1. Navigate to **Security Services** > **Domain** Reputation 2. Click **Edit Global Settings** and uncheck the **Include Additional Attributes** check box. For more information, see "Enabling Sender Domain Reputation Filtering on Email Gateway" section in "Sender Domain Reputation Filtering" chapter of the *User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway*.
Configure Threat Defense Connector for individual incoming mail policies	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. Go to **Mail Policies** > **Incoming Mail Policies** to enable or disable Threat Defense Connector for individual mail policies. For more information, see "Integrating Secure Email Gateway with Threat Defense" chapter in the *User Guide for AsyncOS 15.5.1 for Cisco Secure Email Cloud Gateway*.
Support of Large Key Size Values for DKIM Verification	You can use the following large key size values for DKIM verification in your email gateway: • 3072 key bits size • 4096 key bits size You can select the new, large key size values for DKIM verification in the following ways: • **Web Interface**: Go to *Mail Policies* > *Verification Profiles* > *Add Profile* or *Default* and select **3072** or **4096** from the *'Smallest Key to be Accepted:'* or *'Largest Key to be Accepted:'* drop down list fields. • **CLI**: Use `domainkeysconfig` > `keys` > `new` or `edit` > `Enter the smallest key to be accepted` or `Enter the largest key to be accepted` 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	From this release onwards, the 512 and 768 key bits size values are no longer supported when you create a new DKIM verification profile. **Note** The existing DKIM verification profiles created with 512 and 768 key size values are still supported on upgrade to this release.
TLS 1.3 Support for SSL Services	You can now configure TLS 1.3 for the following TLS services in your email gateway: • GUI HTTPS • Inbound SMTP • Outbound SMTP 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: • `TLS_AES_128_GCM_SHA256` • `TLS_AES_256_GCM_SHA384` • `TLS_CHACHA20_POLY1305_SHA256` **Note** The email gateway does not allow you to modify the ciphers used for TLS 1.3. 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.
Obtaining File Hash Lists, RAT, SMTP Routes, Save and Load Configuration, Address List, and Incoming Mail Policy Users Information using AsyncOS APIs	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. For more information, see the "Configuration APIs" section of the *AsyncOS 15.5.1 API for Cisco Secure Email Cloud Gateway - Getting Started Guide*.
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, French, Japanese, and Korean. For more information, see "Using Message Filters to Enforce Email Policies" in the *User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway*.

Enforcing TLS for Outgoing Messages at Sender or Recipient Level	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. 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 `X-ESA-CF-TLS-Mandatory` header. You can configure the "Content Filter – Add/Edit Header" action to add the `X-ESA-CF-TLS-Mandatory` header in the "Header Name:" field based on any content filter conditions and attach the content filter to an outgoing mail policy.
Synchronizing Configuration Changes between Machines in Different Clusters Simultaneously	You can synchronize configuration changes made to a logged-in machine in one cluster to all machines in a remote cluster simultaneously. The synchronization process occurs only when both clusters are in the same or different data centers of the same region. **Note** You can only synchronize configuration changes between machines at the cluster level and not at the group or machine level. **Note** You must move the machine to the group level to avoid the SPAM Quarantine IP configuration being synchronized over the intercluster. To enable this feature, contact your Cisco account manager. **Prerequisite**: Before you request your Cisco account manager to enable this feature, ensure the configuration is the same in all machines across the clusters. After the synchronization process is complete, if you make a configuration change in one machine, the same configuration is automatically replicated to all machines across the clusters. You can view the same in the System Logs. For more information see, the "Logging" chapter in the *User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway*. **Note** You must not modify the cluster name after the inter-cluster connection process is complete. Make sure to have a unique name for the cluster.
Region-based Polling for URL Retrospective Service	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. For more information, see the "Setting Up URL Filtering" section in the *User Guide for AsyncOS 15.5.1 for Secure Email Cloud Gateway*.

Changes in Behavior

Application SSH Client Algorithm Support	The following application SSH client algorithms are supported when you add an email gateway to a cluster. [**Non-FIPS Mode**] 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: • Cipher algorithms - `aes128-ctr` • MAC methods - `hmac-sha2-256` • KEX algorithms - `diffie-hellman-group14-sha256` [**FIPS Mode**] The following cipher algorithm and MAC method are added to your Secure Email and Web Manager by default in addition to the existing algorithms: • Cipher algorithms - `aes128-ctr` • MAC methods - `hmac-sha2-256`
Archive or Compressed File Processing by Advanced Malware Protection Engine	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. If the Secure Email Gateway fails to extract a compressed or archive file, it will be uploaded to Secure Malware Analytics for analysis.
No Support for `aes192-cbc` Cipher in FIPS Mode	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 15.5.1, you must remove the `aes192-cbc` cipher using the `sshconfig`->`SSHD` subcommand in the CLI. **Note** If your email gateway is in FIPS mode and it is upgraded to the AsynOS 15.5.1 release, the `aes192-cbc` cipher is removed by default.

Upgrade Paths

You can upgrade to release 15.5.1-055 from the following versions:

• 15.5.1-001	• 15.5.0-048	• 15.0.1-105
• 15.0.1-030	• 15.0.0-104	• 15.0.0-097
• 14.3.0-209	• 14.3.0-032	• 14.3.0-020
• 14.2.3-102	• 14.2.3-031	• 14.2.3-027
• 14.2.2-004	• 14.2.1-020	• 14.2.0-620

Supported VMs for this Release

The following VMs are supported for this release:

- C100V
- C300V
- C600V

Pre-Upgrade Notes

Before upgrading, review the following:

- Saving Email Gateway's Configuration, page 9
- Executing Vault Recovery Process to Resolve Vault Issues, page 9
- System Upgrade Blocked due to Disk Space Shortage, page 11
- Prerequisites for File Reputation Service Activation - Secure Endpoint Private Cloud, page 11

Saving Email Gateway's Configuration

If encryption is enabled on your email gateway, we recommend you save a copy of your email gateway's configuration before or after you upgrade to AsyncOS 15.5.1.

You can load the saved email gateway's configuration to restore the previous configuration of your device after you execute the Vault Recovery process to restore the Vault service.

You can save the device’s configuration using the following ways:

- Navigate to **System Administration** > **Configuration File** and **select Encrypt passphrases in the configuration files**.
- Use the `saveconfig` command in the CLI and type **2** to select the **Encrypt passphrases** option.

Executing Vault Recovery Process to Resolve Vault Issues

If your email gateway (on Hardware, On Premises, CES, AWS, KVM, Azure, or Hyper-V) encounters Vault-related issues before or after you upgrade to AsyncOS 15.5.1, then you must execute Vault Recovery process to resolve these issues. Perform the following steps to execute the Vault Recovery process:

1. Log in to your email gateway through a direct SSH connection using the following credentials:

username: **enablediag**

password: **admin user's password**

2. Execute the `recovervault` command.
3. Enter the following sequence of subcommands, when prompted:
   a. `yes`
   b. `1 (encryption enabled) or 2 (encryption disabled)`
4. Log in to your email gateway with administrator user credentials and reboot the device after the Vault Recovery process is complete.
5. [**Only for Cluster Setup**] Rejoin the email gateway to the cluster after the Vault recovers and the device reboot is complete.
6. [**Only If Encryption is Enabled**] Load a copy of the device's configuration that you had saved earlier to restore previous configuration.
7. Monitor your email gateway for a couple of hours for any Vault service alerts.

Your email gateway recovers, and the vault is reinitialized. Now, you can connect to the device without any issues.

Note **Encryption Disabled**

In this scenario, all the system configuration settings are retained.

Encryption Enabled

In this scenario, the following encrypted variables are reset to their default factory values:

- Certificate private keys
- RADIUS passwords
- LDAP bind passwords
- Local users' password hashes
- SNMP password
- DK/DKIM signing keys
- Outgoing SMTP authentication passwords
- PostX encryption keys
- PostX encryption proxy password
- FTP Push log subscriptions' passwords
- IPMI LAN password
- Updater server URLs
- Authentication APIs client credentials
- AMP proxy password
- SAML certificate passphrase

If you want to restore the previous configuration, you must load the previously saved configuration file.

Note The client credentials for the Authentication APIs are not saved in the configuration file and therefore you have to create new client credentials by calling the APIs.

Logs (for enablediag user):

```
Available Commands:
help -- View this text.
quit -- Log out.
service -- Enable or disable access to the service system.
network -- Perform emergency configuration of the diagnostic network interface.
clearnet -- Resets configuration of the diagnostic network interface.
ssh -- Configure emergency SSH daemon on the diagnostic network interface.
clearssh -- Stop emergency SSH daemon on the diagnostic network interface.
tunnel -- Start up tech support tunnel to IronPort.
print -- Print status of the diagnostic network interface.
recovervault -- Recover vault, it will only restore the encrypted variables to factory
values, will not touch anything related to configurations if encryption is disabled .
resetappliance -- Reset appliance reverts the appliance to chosen build with factory
default settings with default IP. No network configuration would be preserved.
reboot -- Reboot the appliance.

S/N 42189A47B0D50A645948-CEC55115B364
Service Access currently ENABLED (0 current service logins)
esa1.hc303-10.smtpi.com> recovervault

Are you sure you want to recover vault?  [N]> y
Encryption is enabled [1]>
Encryption is not enabled [2]>
```

System Upgrade Blocked due to Disk Space Shortage

Your system upgrade to AsyncOS 15.0 version is blocked because the machine has a next root partition of less than 4GB disk space. You must deploy a new virtual appliance with a next root partition of 4 GB disk space. For more information on how to deploy a new virtual appliance with a next root partition of 4 GB disk space, see the Field Notice (FN) at *https://www.cisco.com/c/en/us/support/docs/field-notices/722/fn72230.html*

Prerequisites for File Reputation Service Activation - Secure Endpoint Private Cloud

Before you upgrade to this release, make sure you have met the following prerequisites for File Reputation service activation:

- Upgraded the Secure Endpoint Private Cloud to 3.8.1 or higher version
- Provided the Secure Endpoint - ’Console Hostname’ and ’Activation Code’ details when prompted during the upgrade process.

Post-Upgrade Notes

Activating File Reputation Service for Secure Endpoint Private Cloud

Follow any one of the given steps based on your system setup to activate the File Reputation Service:

- [**For Cluster mode**]: Connect to the email gateway that is already configured with the new File Reputation service.
- [**For Standalone mode**]: Perform the following steps:

  1. Navigate to the **Security Services** > **File Reputation and Analysis** page on the web interface,

  2. Click the **Edit Global Settings** button.

  3. Click the **Advanced Settings for File Reputation** panel,

  4. Select the **Private reputation cloud** option from the “File Reputation Server” drop-down list.

  5. Enter the console hostname and activation code in the given fields.

  6. Click **Submit** and commit your changes.

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 Known and Fixed Issues, page 14.

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 15.0:

- 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 14
- Lists of Known and Fixed Issues, page 14
- Related Documentation, page 16

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=15.5.0,15.5.1&prdNam=Cisco%20Secure%20Email%20Gateway
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=15.5.1-055&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, 15.5.1-055

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.

Software Lifecycle Support Statement

For information about software time-based release model and software release support timelines, see Software Lifecycle Support Statement.

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
Cisco Secure Email Cloud Gateway	https://www.cisco.com/c/en/us/support/security/cloud-email-security/products-user-guide-list.html
CLI Reference Guide for Cisco Secure Email Gateway	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.