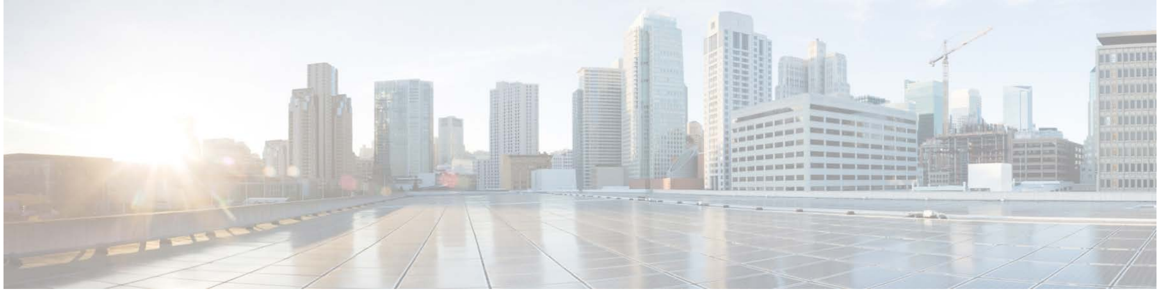

Release Notes for AsyncOS 15.0 for Cisco Secure Email and Web Manager - MD (Maintenance Deployment)

Published: August 10, 2023

Revised: January 18, 2024

Contents

Note You must ensure that you provide your email identifier with the domain name while you login the spam quarantine portal.

Note If you already have a Cisco SecureX account that is managed by different administrator login, Cisco recommends that you register your devices with SSE first before you perform smart licensing registration. You must not perform smart licensing registration without registering your device with SSE first. This is a known issue- Defect ID- CSCvy10226.

Cisco Systems, Inc.
www.cisco.com

What's New in this Release

What's New in AsynOS 15.0.0-413

This release focuses specifically on IOPS optimization. For more information, see Changes in Behavior in AsyncOS 15.0.0-413, page 8.

What's New in AsynOS 15.0.0-334

Feature	Description
FIPS Compliance	Cisco Secure Email and Web Manager is FIPS compliant and has integrated the following FIPS 140-2 approved cryptographic module: Cisco Common Crypto Module (FIPS 140-2 Cert. #4036). **Note** The Cisco Secure Email and Web Manager FIPS Certification only applies to email gateway integration and not to Secure Web Appliance integration. **Note** There is no support for the TLS v1.0 method if your Secure Email and Web manager is in the FIPS mode.

	SSH Server and Client Configuration The following SSH Server and Client Configuration are supported when you install AsyncOS 15.0 for Cisco Secure Email and Web Manager for the first time and when FIPS mode is enabled: [**SSH Server Configuration**] The following Cipher, Host key, KEX algorithms, and MAC methods are supported in Secure Email and Web Manager by default: • **Cipher algorithms** - `aes128-ctr`, `aes256-ctr`, `aes128-cbc`, `aes192-cbc`, and `aes256-cbc` • **Host key algorithms** - `rsa-sha2-256` • **KEX algorithms** - `diffie-hellman-group14-sha1`, `ecdh-sha2-nistp256`, `ecdh-sha2-nistp384`, and `ecdh-sha2-nistp521` • **MAC methods** - `hmac-sha1`
	[SSH Client Configuration] The following Cipher, Host key, KEX algorithms, and MAC methods are supported in Secure Email and Web Manager by default: • **Cipher algorithms** - `aes128-ctr`, `aes192-ctr`, `aes256-ctr`, `aes128-cbc`, `aes192-cbc`, `aes256-cbc`, `aes128-gcm@openssh.com`, and `aes256-gcm@openssh.com` • **Host key algorithms** - `rsa-sha2-256` • **KEX algorithms** - `diffie-hellman-group14-sha1`, `ecdh-sha2-nistp256`, `ecdh-sha2-nistp384`, and `ecdh-sha2-nistp521` • **MAC methods** - `hmac-sha1` For more information on this feature, see "FIPS Management" chapter of the user guide.
Single Log Line (SLL)	The SLL feature creates, indexes, and stores the email tracking data as a single log line or a flattened model. Therefore, you can execute a query and get a response quickly. This feature boosts the tracking query or search performance through fast response, low memory, and CPU usage. This feature is only applicable to post-upgrade email tracking data.

Configuring CRL Sources	The Secure Email and Web Manager checks a list of revoked certificates called a Certificate Revocation List (CRL) as part of its certificate verification to ensure that the user's certificate has not been revoked. You need to keep an up-to-date version of this list on a server, and the Secure Email and Web Manager downloads it on a schedule you create. You can manually update the list too. You can configure CRL sources using the following ways: • Navigate to **Network** > **CRL Sources** > **Add CRL Source** > **Add CRL (Certificate Revocation Lists) Source** window in the legacy web interface. • Use the `Certconfig` > `CRL` subcommand in the CLI. For more information on Configuring CRL Sources, see "Configuring CRL Sources" section in the "Common Administrative Tasks" chapter of the user guide.

Removal of Old Splunk Data	When you upgrade to Secure Email and Web Manager 15.0 and later, and if email tracking data is contained in the Splunk database, the system will delete the Splunk database and binaries if you proceed with the upgrade. **Note** From the Secure Email and Web Manager 13.6.2 release onwards, the Splunk database is no longer used for storing email tracking data. All new email tracking data is stored in the Lucene database. After you upgrade to Secure Email and Web Manager 15.0, all tracking data before the upgrade to Secure Email and Web Manager 13.6.2 will be removed and cannot be recovered. During the upgrade to Secure Email and Web Manager 15.0 and later, a warning message indicating that the system will delete the Splunk database is displayed in the CLI or on the web interface of your Secure Email and Web Manager. **Sample Warning Message** *"From the Secure Email and Web Manager 13.6.2 version onwards, we have moved to a newer storage system for email tracking data. Generally, the old data is replaced with new data in the new storage system automatically. However, in some scenarios (for example, late upgrades, low mail flow and tracking data, and so on), there could be traces of old data still present in the old storage system that is no longer supported.* *In your case, it is 19 MB, which was last updated on 11 Aug 2022.* *You can take a back up of the email tracking data (if required). You can use the backupconfig command in the CLI to perform the backup action. For more information, see the 'Scheduling Single or Recurring Backups' section in the 'Common Administrative Tasks' chapter of the user guide.* *If you proceed with this upgrade process, your Splunk email tracking data will be deleted.* *You can choose to proceed with the upgrade or abort the upgrade.* *Do you agree to proceed with this upgrade? [Y]"* **Note** The warning message is only displayed for on-premises admin users.

	Note The **`debug`** submenu used to collect debug information for the Splunk database will be removed from the `Diagnostic` > `Tracking` subcommand in the CLI.
Resetting the Network Configuration to the Initial Manufacturer Value	A new subcommand `Reload Status` that displays the status of the execution of the last Reload subcommand (that resets the network configuration) is added to the `Diagnostic` command. For more information on this command, See the "Diagnostic - Reload command" and "Diagnostic - Reload Status command" sections in the "Common Administrative Tasks" chapter of the user guide.
Performing X.509 Validation for Peer Certificate during TLS Communication	You can configure your Secure Email and Web Manager to perform X.509 validation for peer certificates. The X.509 validation is applicable for the following services: • Outbound SMTP • LDAP • Updater • Alert over TLS • Syslog Server • Smart Licensing Server • SSE Connector • SSE Server You can configure X.509 validation for Peer Certificate using the following ways: • Navigate to **System Administration** > **SSL Configuration** > **SSL Configuration** page on the web interface. • Execute the `sslconfig` command in the CLI. For more information, see the "X.509" section of the "Common Administrative Tasks" chapter in the user guide.
New RAM Value for Secure Email and Web Manager Virtual Appliance Model	From AsyncOS 15.0 release onwards, there is a new RAM value for the M600V Secure Email and Web Manager virtual appliance model deployed through KVM or VMWare ESXi. For more information on the new RAM value applicable for the virtual appliance model, see Cisco Content Security Virtual Appliance Installation Guide.

Microsoft Hyper-V Server 2019 Support	Secure Email and Web Manager 15.0 supports the Microsoft Hyper-V Server 2019.
Generation 2 Deployment Support for Hyper-V	From AsyncOS 15.0 release onwards, Secure Email and Web Manager supports only Generation 2 deployment for Hyper-V. **Note** The supported model for Hyper-V Generation 2 deployment is **M600V** only. For more information on Generation 2 deployment support for Hyper-V, see Cisco Content Security Virtual Appliance Installation Guide.
Generation 2 Deployment Support on Azure Platform	From AsyncOS 15.0 release onwards, Secure Email and Web Manager supports Generation 2 deployments on Azure platform. **Note** The supported model for Azure Generation 2 deployment is **M600V** only. **Note** The Generation 2 image does not boot after the deployment on Azure platform. You must reboot the virtual machine after the Generation 2 image is deployed. For more information on Generation 2 deployment on Azure platform, see Cisco Secure Email Virtual Gateway and Cisco Secure Email and Web Manager Virtual on Microsoft on Azure Deployment Guide.
Supported Model for AWS Deployment	From AsyncOS 15.0 release onwards, the supported model for AWS deployment is **M600V** only. For more information, see Deploying Cisco Secure Email Gateway, Secure Web, and Secure Email and Web Manager Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services Guide.

Changes in Behavior

Changes in Behavior in AsyncOS 15.0.0-413

IOPS Optimization	As part of ongoing performance improvements, the Secure Email and Web Manager is optimized to perform the I/O (read and write) operations efficiently. There are no functional changes made in this release.

Changes in Behavior in AsyncOS 15.0.0-334

SSH Server and Client Configuration Changes	[**Upgrade Scenario**] The following SSH Server and Client Configuration changes are applicable when you upgrade your Secure Email and Web Manager from a lower AsyncOS version to AsyncOS 15.0 version and later. [**For Non-FIPS mode only**]: The following SSH Server and Client Configuration changes are applicable when your Secure Email and Web Manager is not in the FIPS mode: **[SSH Server Configuration Changes]** • The following cipher algorithms, MAC methods, KEX algorithms, and host key algorithm are removed from your Secure Email and Web Manager by default: – **Cipher algorithms** - `rijndael-cbc@lysator.liu.se`, `3des-cbc`, `blowfish-cbc`, `cast128-cbc`, `arcfour`, `arcfour128`, and `arcfour256` – **MAC methods** - `hmac-md5`, `umac-64@openssh.com`, `hmac-ripemd160`, `hmac-ripemd160@openssh.com`, `hmac-sha1-96`, `hmac-md5-96` – **KEX algorithms** - `diffie-hellman-group-exchange-sha256`, `diffie-hellman-group-exchange-sha1`, `diffie-hellman-group1-sha1` – **Host key algorithm** - `rsa1` • The "Minimum Server Key Size" option is removed from the CLI of your Secure Email and Web Manager by default. • The host key algorithm - `rsa-sha2-256` is added to your Secure Email and Web Manager by default. [**SSH Client Configuration Changes**] • The following cipher algorithms - `aes128-gcm@openssh.com`, and `aes256-gcm@openssh.com` are added to your Secure Email and Web Manager by default. • The host key algorithm - `rsa-sha2-256` is added to your Secure Email and Web Manager by default.

	[**SCP Push Changes**] Before this release, when you configured SCP Push through **System Administration** -> **Log Subscription** page, the system generated the `ssh-dss` key. The `ssh-dss` key was configured in the remote server to push the logs to the remote server. After you upgrade to this release and enable FIPS mode, when you configure SCP Push through **System Administration** -> **Log Subscription** page, the system generates the `ssh-rsa` key. The `ssh-rsa` key must be configured in the remote server to push the logs to the remote server. **Note** After you upgrade to Secure Email and Web Manager 15.0 and enable FIPS mode, you must subscribe to one of the logs again to get the new `ssh-rsa` key and configure the `ssh-rsa` key in the remote server. For more information on log subscription, see the "Configuring Log Subscriptions" section of the "Logging" chapter of the User Guide. [**Banner Text Changes**] In the System Upgrade banner text, a note is added that informs you that the system will remove weak algorithms in Ciphers, Keys, Kex, and MAC after the upgrade process.

[**New Install Scenario**]

The following SSH server configuration changes are only applicable when you install AsyncOS 15.0 for Cisco Secure Email and Web Manager for the first time.

[**For non-FIPS mode only**]: The following cipher algorithms, MAC method, and host key algorithms are supported in your Secure Email and Web Manager:

- **Cipher algorithms** - `aes128-ctr`, `aes192-ctr, aes256-ctr`, `aes128-cbc`, `aes192-cbc`, and `aes256-cbc`
- **MAC method** - `hmac-sha1`
- **Host key algorithms** - `rsa-sha2-256`, `ssh-rsa`, and `ssh-dss` (disabled by default)

  Note You need to manually enable the `ssh-dss` cipher algorithm using the `sshconfig` > `sshd` > `setup` subcommand in the CLI.

- **KEX algorithms** - `diffie-hellman-group14-sha1`, `ecdh-sha2-nistp256`, `ecdh-sha2-nistp384`, and `ecdh-sha2-nistp521`

[**For FIPS mode only**]: To enable FIPS mode, make sure you first disable the following cipher and host key algorithms that are non-FIPS compliant using the `sshconfig` > `sshd` > `setup` subcommand in the CLI.

- Cipher algorithms - `aes192-ctr`
- Host key algorithm - `ssh-rsa`

Note The host key algorithm - `rsa-sha2-256` is newly added and is enabled by default on your Secure Email and Web Manager.

X.509 Certificates Changes	[**Upgrade Scenario**] When you upgrade to Secure Email and Web Manger 15.0 and later versions, the system prompts you to delete or retain less secure X.509 certificates. **Notification Message** *From Secure Management Appliance 15.0.x and later versions, we will go ahead and delete x509 certificates that have less secure signature algorithm if any configured. These x509 certificates can be configured from Network-> Certificates from GUI page and via certconfig from CLI page.* *Note: You can still choose to skip deletion of these less secure x509 certificates but it is not recommended. Do you want to proceed with the upgrade?[y]/[n]* *y* *Do you wish to skip the deletion of x509 certificates with less secure signature algorithm if any configured?[n]/[y]:* *N* *Processing configuration... cert-1: Thu Dec 22 13:48:08 2022 getCertDb: Caught exception IOError or OSError* *Processing configuration... cert* *WARNING: The following x509 certificates are deleted because their signature algorithm is less secure. : ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP']*
	[**New Install Scenario**] The following signature algorithm changes for X.509 certificates are only applicable when you install AsyncOS 15.0 for Cisco Secure Email and Web Manager for the first time: • The following signature algorithms for x509 certificates are no longer supported - `sha1withrsaencryption`, `dsawithsha1`, `sha224withrsaencryption`, `ecdsa-with-sha1`, `ecdsa-with-sha224`, `md2withrsaencryption`, `md4withrsaencryption`, `md5withrsaencryption`, `ripemd128withrsaencryption`, `ripemd160withrsaencryption`, and `ripemd256withrsaencryption`. • The following curves for x509 certificates having ECDSA signature algorithms are not supported - `secp224r1`, `secp192r1`, `brainpoolP160r1`, `brainpoolP192r1`, `secp160r1`, `secp160r2`, `secp192k1`, `secp224k1`, `secp256k1`, `sect163k1`, `sect163r2`, `sect193r1`, `sect193r2`, `sect233k1`, `sect233r1`, `sect239k1`, `sect283k1`, `sect283r1`, `sect409k1`, `sect409r1`, `sect571k1`, and `sect571r1`.

X.509 Certificates Changes	[**Upload Certificate Scenario**] When you upload X.509 certificates with the less secure signature algorithm, you will receive an error message stating the X.509 certificates with the ABC algorithm are less secure. **Error Message** *Error: The x509 certificates with ripemd160WithRSA digest are less secure.*
	[**Loading configuration file Scenario]** **Loading configuration file using CLI** When you load a configuration file through CLI, the system warns you that the X.509 certificates with a less secure signature algorithm are deleted. **Warning Message** *WARNING: The following x509 certificates are deleted because their signature algorithm is less secure: ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP'].* **Loading configuration file using GUI** When you load a configuration file through GUI, the system warns you that the X.509 certificates with a less secure signature algorithm are deleted. **Warning Message** *Warnings: The following x509 certificates are deleted because their signature algorithm is less secure: ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP'].*
Resetting the Network Configuration to the Initial Manufacturer Value	Before this release, the `Diagnostic` > `Reload` subcommand was used to remove all user settings and reset the entire device. After you upgrade to this release, along with the previous functionality, this subcommand resets the network configuration to the initial manufacturer value.
JWT token - error message changes	Before this release, when you used JSON Web Token (JWT) token to make any API request, and if the JWT token was expired, the expired token error message was displayed. After you upgrade to this release, when you use the JWT token to make any API request, if the JWT token used is older than 12 hours, an invalid token or expired token error message is displayed. The expired token error message is displayed only up to 12 hours from token generation.

Modifications to the SPoG feature	When you enable or disable SPoG, the session of all the users concurrently logged into the new web interface becomes invalid, and a new request to the server logs them out. The users must log in again. Also, if a Secure Email and Web Manager is added to SPoG, and you are currently logged into the new web interface of the same Secure Email and Web Manager, then you will be logged out due to a change in the flow of JWT validation. **Note** The SPoG feature works only if all the Secure Email and Web Manager under the SPoG cluster have the same version.
Message Tracking - Remediation Action Changes	Before this release, you could enter a-z, A-Z, 0-9, and any special characters for the Remediation Batch Name and Description fields in the Confirm Remediation dialog box. From this release onwards, you can only enter a-z, A-Z, 0-9, _, -, and spaces for the Remediation Batch Name and Description fields in the Confirm Remediation dialog box. Any other special characters are not allowed.
No support for TLSv1.0 for communicatoin between Secure Email and Web Manager and syslog server	Before this release, the Secure Email and Web Manager used TLSv1.0 to communicate with the syslog server irrespective of the TLS version enabled on the syslog server. From this release onwards, the Secure Email and Web Manager uses the highest TLS version enabled on the syslog server. For example, if the highest TLS version on the syslog server is 1.2, then Secure Email and Web Manager uses TLSv1.2 to communicate with syslog server. **Note** TLSV1.0 is not supported now as it is an insecure TLS method.
Warning Message for Syslog Disk Buffer Size	From this release onwards, when you upgrade from Secure Email and Web Manager 14.2 release to Secure Email and Web Manager 15.0 release if the syslog disk buffer size is set to 10 GB and the size of the syslog disk buffer data exceeds 1 GB, the Secure Email and Web Manager displays a warning message in the CLI and on the web interface. You can ignore the warning message and continue the upgrade process or abort the upgrade. If you abort the upgrade process, you can connect the Secure Email and Web Manager to the syslog server, drain the syslog disk buffer data, and then perform the upgrade process.

Notification Message for Phase 2 Backup Process	Before this release, if any service task in the phase 2 backup process was in progress and exceeded 2 hours to complete, a notification message was not sent to the administrator. After you upgrade to this release, if any service task in the phase 2 backup process is in progress and exceeds 2 hours to complete, a notification message is sent to the administrator informing the status of the backup process along with the service name that is taking longer to complete.
Time Zone -> **Country** field changes	From this release onwards, the United States option available in the **Time Zone ->Country** field is modified to the United States of America.

Accessing the New Web Interface

Note Next generation user interface is best experienced with trailblazer being enabled. Therefore, we recommend that you access the new interface with trailblazer enabled.

The new web interface provides a new look for monitoring reports, quarantines, and searching for messages.

Note The new web interface of your appliance uses AsyncOS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the `trailblazerconfig` command in the CLI to configure the trailblazer HTTPS ports. Make sure that the trailblazer HTTPS port is opened on the firewall.

You can access the new web interface in any one of the following ways:

- When `trailblazerconfig` CLI command is enabled, use the following URL - `https://example.com:<trailblazer-https-port>/ng-login`

  where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

  By default, `trailblazerconfig` is enabled on the appliance.

  – Make sure that the configured HTTPS port is opened on the firewall. The default HTTPS port is 4431.

  – Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.

- When `trailblazerconfig` CLI command is disabled, use the following URL - `https://example.com:<https-port>/ng-login`

  where `example.com` is the appliance host name and `<https-port>` is the HTTPS port configured on the appliance.

Note If the trailblazerconfig CLI command is disabled, you may need to add multiple certificates for API ports for certain browsers.

- Log into the appliance and click **Security Management Appliance is getting a new look. Try it !** to navigate to the new web interface.

The new web interface opens in a new browser window and you must log in again to access it. If you want to log out of the appliance completely, you need to log out of both the new and legacy web interfaces of your appliance.

For a seamless navigation and rendering of HTML pages, Cisco recommends using the following browsers to access the new web interface of the appliance (AsyncOS 12.0 and later):

- Google Chrome (Latest Stable Version)
- Mozilla Firefox (Latest Stable Version)
- Safari (Latest Stable Version)

You can access the legacy web interface of the appliance on any of the supported browsers.

The supported resolution for the new web interface of the appliance (AsyncOS 12.0 and later) is between 1280x800 and 1680x1050. The best viewed resolution is 1440x900, for all the browsers.

Note Cisco does not recommend viewing the new web interface of the appliance on higher resolutions.

The end-users can now access the spam quarantine on the new web interface in any one of the following ways:

- When `trailblazerconfig` CLI command is enabled, use the following URL - `https://example.com:<trailblazer-https-port>/euq-login`.

  where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

- When `trailblazerconfig` CLI command is disabled, use the following URL - `https://example.com:<https-port>/euq-login`.

  where `example.com` is the appliance host name and `<https-port>` is the HTTPS port configured on the appliance.

Note Make sure that the HTTP/HTTPS and the AsyncOS API ports are opened on the firewall.

Upgrade Paths

Upgrading to Release 15.0.0-413 - MD (Maintenance Deployment)

You can upgrade to release 15.0.0-413 from the following versions:

- 15.0.0-405
- 15.0.0-334
- 15.0.0-333
- 14.3.0-124
- 14.3.0-120
- 14.2.0-241
- 14.2.0-224
- 14.2.0-217
- 14.2.0-212
- 14.2.0-203

Upgrading to Release 15.0.0-334 - GD (General Deployment)

You can upgrade to release 15.0.0-334 from the following versions:

- 15.0.0-333
- 14.3.0-120
- 14.3.0-124
- 14-3-0-126
- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224

Upgrading to Release 15.0.0-333 - LD (Limited Deployment) Refresh

You can upgrade to release 15.0.0-333 from the following versions:

- 15.0.0-317
- 14.3.0-120
- 14.3.0-124

- 14-3-0-126
- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224

Upgrading to Release 15.0.0-317 - LD (Limited Deployment)

You can upgrade to release 15.0.0-317 from the following versions:

- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224
- 14.3.0-120
- 14.3.0-124
- 14.3.0-126
- 15.0.0-281

Installation and Upgrade Notes

- Important Additional Reading, page 17
- Virtual Appliance, page 18
- Pre-Upgrade Requirements, page 18
- IPMI Messages During Upgrade, page 19
- Upgrading to This Release, page 20
- Post-Upgrade Requirements, page 21

Important Additional Reading

You should also review the release notes for your associated Email and Web security releases.

For links to this information, see Related Documentation, page 24.

Virtual Appliance

To set up a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html.

Note Fiber Network Interface Cards on virtual appliances are not compatible with AsyncOS versions 12.5 and later. This is a known issue. Defect ID: CSCvr26218

Note The RAM size of M600V virtual appliance is increased from 8 GB to 16 GB. You will receive an alert if your virtual appliance does not meet this requirement.

Upgrading a Virtual Appliance

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

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

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

Migrating From a Hardware Appliance to a Virtual Appliance

Step 1 Set up your virtual appliance using the documentation described in Virtual Appliance, page 18.

Step 2 Upgrade your physical appliance to this AsyncOS release.

Step 3 Save the configuration file from your upgraded physical appliance

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

Be sure to select appropriate options related to disk space and network settings.

What To Do Next

If you will use your hardware appliance as a backup appliance, see information about backups in the user guide or online help. For example, you should ensure that the backup appliance does not pull data directly from managed email and web security appliances, or publish configurations to web security appliances.

Pre-Upgrade Requirements

Perform the following important pre-upgrade tasks:

- Verify Associated Email and Web Security Appliance Versions, page 19
- Back Up Your Existing Configuration, page 19
- Centralized Policy, Virus, and Outbreak Quarantine Certificate Settings in FIPS Mode, page 19
- Back Up Your Existing Databases, page 19

Verify Associated Email and Web Security Appliance Versions

Before upgrading, verify that the Email Security appliances and Web Security appliances that you want to manage will run releases that are compatible. See the Installation and Upgrade Notes, page 17.

Back Up Your Existing Configuration

Before upgrading your Cisco Secure Email and Web Manager, save the XML configuration file from your existing Security Management appliance. Save this file to a location off the appliance. For important caveats and instructions, see the “Saving and Exporting the Current Configuration File” section in the user guide or online help.

Centralized Policy, Virus, and Outbreak Quarantine Certificate Settings in FIPS Mode

After upgrading your managed Email Security appliance in FIPS mode to AsyncOS 15.0 or later, the Centralized Policy, Virus, and Outbreak Quarantine is disabled. From AsyncOS 13.0 onwards, Email Security appliances in FIPS mode uses a certificate of 2048 bits to enable Centralized Policy, Virus, and Outbreak Quarantines. The earlier AsyncOS versions have certificates of size 1024 bits.

Follow these steps to enable the Centralized Policy, Virus, and Outbreak Quarantines:

Step 1 Upgrade the Cisco Secure Email and Web Manager to AsyncOS 15.0.

Step 2 Upgrade your Cisco Email Security appliance to the latest supported version.

After the upgrade, the Centralized Policy, Virus and Outbreak Quarantines setting will be disabled.

Step 3 On the upgraded Cisco Secure Email and Web Manager, run the `updatepvocert` command on the CLI.

The CA certificate for Centralized Policy, Virus, and Outbreak Quarantines is updated to 2048 bits.

Step 4 On the upgraded Cisco Email Security appliance, verify if the Centralized Policy, Virus, and Outbreak Quarantines is enabled. For more information, see the *Cisco Secure Email and Web Manager User Guide*.

Back Up Your Existing Databases

Before you upgrade your Secure Email and Web Manager, back up the existing databases of your Secure Email and Web Manager.

For information on disaster recovery of the Secure Email and Web Manager, see Backing Up Security Management Appliance section in Common Administrative Tasks chapter of the user guide. For detailed steps to schedule a backup process, see Scheduling Single or Recurring Backups section in Common Administrative Tasks chapter of the user guide.

IPMI Messages During Upgrade

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

Defect ID: CSCuz33125

Upgrading to This Release

Step 1 Address all topics described in Pre-Upgrade Requirements, page 18.

Step 2 Follow all instructions in the “Before You Upgrade: Important Steps” section in the user guide PDF for THIS release.

Step 3 Perform the upgrade:

Follow instructions in the “Upgrading AsyncOS” section of the “Common Administrative Tasks” chapter of the user guide PDF for your EXISTING release.

Note Do not interrupt power to the appliance for any reason (even to troubleshoot an upgrade issue) until at least 20 minutes have passed since you rebooted. If you have a virtual appliance, do not use the hypervisor or host OS tools to reset, cycle, or power off the virtual machine.

Step 4 After about 10 minutes, access the appliance again and log in.

Step 5 Follow instructions in the “After Upgrading” section of the user guide PDF for THIS release.

Step 6 If applicable, see Migrating From a Hardware Appliance to a Virtual Appliance, page 18.

Important! After you upgrade to this release, you can try any one of the following steps to make the navigation in your browser seamless:

- Accept the certificate used by the web interface and use the following URL syntax: `https://hostname.com:<https_api_port>` (for example, `https://some.example.com:6443`) in a new browser window and accept the certificate. Here `<https_api_port>` is the AsyncOS API HTTPS port configured in **Network > IP Interfaces**. Also, ensure that the API ports (HTTP/HTTPS) are opened on the firewall.
- By default, `trailblazerconfig` CLI command is enabled on your appliance. Make sure that the HTTPS port is opened on the firewall. Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.

  If the `trailblazerconfig` CLI command is disabled, you can run the `trailblazerconfig` > `enable` command using the CLI to avoid the following issues:

  - Requiring to add multiple certificates for API ports in certain browsers.
  - Redirecting to the legacy web interface when you refresh the spam quarantine, Safelist or Blocklist page.
  - Metrics bar on the Advanced Malware Protection report page does not contain any data.

  For more information, see section "The trailblazerconfig Command" of the user guide.

Note Reboot your appliance or clear your browser cache if you are unable to access the web interface. If the problem persists, contact Cisco Customer Support.

Post-Upgrade Requirements

Perform the following important post-upgrade tasks:

- Executing Vault Recovery Script to Resolve Vault Issues, page 21
- Spam Notification URL Changes, page 22
- Mandatory Usage of Cisco Smart Software Licensing in Next AsyncOS Release, page 22

Executing Vault Recovery Script to Resolve Vault Issues

If your Secure Email and Web Manager (on Hardware, On Premises, AWS, KVM, Azure, or Hyper-V) encounters vault-related issues and if encryption is **disabled**, then you must execute Vault Recovery Script to resolve these issues. Perform the following steps to execute the Vault Recovery Script:

1. Log in to your Secure Email and Web Manager 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. `encryption disable [2]`

   c. `reboot`

   Your Secure Email and Web Manager recovers, and the vault is reinitialized.

   Now, you can connect to the system without any issues, and all the system configuration settings are retained.

If your Secure Email and Web Manager (on Hardware, On Premises, AWS, KVM, Azure, or Hyper-V) encounters vault-related issues and if encryption is **enabled**, then you must execute Vault Recovery Script to resolve these issues. Perform the following steps to execute the Vault Recovery Script:

1. Log in to your Secure Email and Web Manager through **console** 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. `encryption enable [1]`

   c. `reboot`

   Your Secure Email and Web Manager recovers, and the vault is reinitialized.

   Now, you can connect to the system without any issues.

Note 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
- FTP Push log subscriptions' passwords
- IPMI LAN password
- Updater server URLs
- SAML certificate passphrase

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

Spam Notification URL Changes

After you upgrade to Secure Email and Web Manager 15.0, if you cannot log in using the saved spam notification URL, use the new URL mentioned in the spam notification mail.

Mandatory Usage of Cisco Smart Software Licensing in Next AsyncOS Release

The Cisco Smart Software Licensing usage is mandatory from the next AsyncOS release (all releases post AsyncOS 15.0 release) for Cisco Secure Email and Web Manager.

Note There will be no support for classic licensing from the next AsyncOS release. You will no longer be able to order new feature licenses or renew existing feature licenses in the Classic Licensing mode.

Prerequisite: Make sure you create a smart account in the Cisco Smart Software Manager portal and enable Cisco Smart Software Licensing on your Secure Email and Web Manager. For more information, see the "Smart Software Licensing" section of the "Common Administrative Tasks" chapter of the user guide.

Result: After you enable Cisco Smart Software Licensing, you can upgrade your Secure Email and Web Manager from AsyncOS 15.0 to the next AsyncOS release seamlessly and continue to use the existing feature licenses in the Smart Licensing mode.

Supported Hardware for this Release

Supported Hardware:

- M190
- M195
- M390
- M395
- M690
- M695

Supported VMs:

- M100V
- M300V

- M600V

Known and Fixed Issues

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

- Bug Search Tool Requirements, page 23
- Lists of Known and Fixed Issues, page 23
- Finding Information about Known and Resolved Issues, page 23

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?kw=*&pf=prdNm&rls=15.0.0&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.0.0&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

Finding Information about Known and Resolved Issues

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

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://bst.cloudapps.cisco.com/bugsearch/.

Step 2 Log in with your Cisco account credentials.

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

Step 4 In **Releases** field, enter the version of the release, for example, 15.0.

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

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

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

Related Documentation

In addition to the main documentation in the following table, information about other resources, including the knowledge base and Cisco support community, is in the More Information chapter in the online help and user guide.

Documentation For Cisco Secure Products:	Is Located At:
Cisco Secure Email and Web Manager Appliances	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 Security appliances	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Command Line Reference guide for content security products	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco Email Encryption	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

Service and Support

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

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

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

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

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

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.