

Release Notes for AsyncOS 14.0 for Cisco Secure Email and Web Manager -MD (Maintenance Deployment)

First Published: 05 July 2021

Revised: November 27, 2023

Contents

- [What's New in this Release, page 2](#)
- [Changes in Behavior, page 8](#)
- [Accessing the New Web Interface, page 10](#)
- [Upgrading to AsyncOS 14.0, page 11](#)
- [Installation and Upgrade Notes, page 12](#)
- [Supported Hardware for this Release, page 16](#)
- [Known and Fixed Issues, page 16](#)
- [Related Documentation, page 17](#)
- [Service and Support, page 18](#)



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.




What's New in this Release

Feature	Description
Header Rewrite	You can configure custom header profiles for HTTP requests and can create multiple headers under a header rewrite profile. The header rewrite profile feature enables the appliance to pass the user and group information to another upstream device after successful authentication. The upstream proxy considers the user as authenticated, bypasses further authentication, and provides access to the user based on the defined access policies. See the User Guide for AsyncOS 14.0 for Cisco Secure Web Appliance .
Support for XAuthentication: Appliance to Consume X-Authenticates User/Group Headers and Apply Policies	You can now configure the Header Based Authentication scheme for an active directory. The client and the Web Security Appliance consider the user as authenticated and do not prompt again for authentication or user credentials. The X-Authenticated feature works when the Web Security Appliance acts as an upstream device. See the User Guide for AsyncOS 14.0 for Cisco Secure Web Appliance .
New System Health Status Dashboard	In AsyncOS 14.0, you can now view the current status and configuration of the Web Security appliance in a page. You must choose Monitoring > System Health to monitor the system status of the Web security appliances. See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager .
New report for mail policy details	A new report – Mail Policy Details is added in the new web interface of your appliance. Use this report to view the number of messages that match a configured mail policy. See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager .
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 appliance. Use this option to search for incoming or outgoing messages that match the configured mail policy name entered in the 'Mail Policy Name' field. See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager .
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 appliance: Overview report page: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager .

Enhanced Mail Flow Summary and Mail Flow Details reporting pages	<p>The following are the enhancements made to the Mail Flow Summary and Mail Flow Details reporting pages in the new web interface of your appliance:</p> <p>Mail Flow Summary report page:</p> <p>The following are the enhancements made to the Mail Flow Summary and Mail Flow Details reporting pages in the new web interface of your appliance:</p> <p>Mail Flow Summary report page:</p> <ul style="list-style-type: none"> • 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. <p>Mail Flow Details report page:</p> <ul style="list-style-type: none"> • 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. <p>See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager.</p>
Performing Remedial Actions on Messages in Cisco Threat Response	<p>In Cisco Threat Response, you can now investigate and apply the following remedial actions on messages processed by your appliance:</p> <ul style="list-style-type: none"> • Delete • Forward • Forward and Delete <p>See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager.</p>

<p>Support for Internationalized Domain Name (IDN)</p>	<p>AsyncOS 14.0 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:</p> <ul style="list-style-type: none"> • 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. <p>For this release, you can only configure few features using IDN domains in your content security gateway.</p> <ul style="list-style-type: none"> • SMTP Routes Configuration Settings: <ul style="list-style-type: none"> – 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. • 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – View messages with IDN domains detected as spam or suspected spam. – Add email addresses with IDN domains to the safelist and blocklist categories. <p>See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager.</p>
--	---

Smart Licensing	<p>Cloud Service will be enabled and Appliance will be registered automatically when smart licensing is enabled and registered.</p> <ul style="list-style-type: none"> To enable or disable Cisco SecureX and Cisco Threat response, the option is introduced under the generalconfig command. The command threstresponseconfig will display the warning message “Enter general config command to Enable/Disable of Cisco SecureX/ Threat Response feature”. The command smartaccountinfo is introduced for getting the Smart account information. When you enable CloudServices, Cisco SecureX will be enabled automatically and Cisco SecureX will be disabled when CloudServices is disabled. <p>See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager.</p>
Passphrases	<p>A new passphrase rule is added in your Email and Web Manager to define your login passphrase:</p> <p>Avoid usage of passphrases that contain three or more repetitive or sequential characters, (for example, 'AAA@124,' 'Abc@123,' and so on.).</p> <p>You can now also create a system-generated passphrase to log in to your Cisco Secure Email and Web Manager.</p> <p>See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager.</p>
FQDN	<p>For a X509 certificate, the FQDN validation validates the common name field (CN) of that certificate's subject distinguished name and the subjectAltName extension of type dNSName (SAN:dNSName).</p> <p>See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager.</p>
SPAM Notification	<p>A new field Custom Logo Position is included that enables you to add the same logo to the SPAM notification email at the given position.</p> <p>See the User Guide for AsyncOS 14.0 for Cisco Secure Email and Web Manager.</p>

<p>Certificate Authority Configuration Changes</p>	<p>The Certificate Authority (CA) configuration changes are applicable in any one of the following scenarios:</p> <ul style="list-style-type: none"> • Upgrade from a lower AsyncOS version to AsyncOS 14.0 version and later. • Install AsyncOS 14.0 for Cisco Secure Email and Web Manager for the first time. <p>The following changes are made to the Certificate Authorities list:</p> <ul style="list-style-type: none"> • You can view the count and details of custom and system CA certificates in your email gateway. <p>Use the Managed Trusted Root Certificates option in Network > Certificates > page to view the custom or system CA certificate details.</p> <ul style="list-style-type: none"> • Certificate chain will be validated while uploading Custom Intermediate CA. Intermediate CA will be rejected if the issuer (Trusted Root CA) is not found in the appliance. • You can upload, delete, or append the custom CA certificate in your Cisco Secure Email and Web Manager. • You will not be able to upload an expired custom CA certificate to your Cisco Secure Email and Web Manager. • You will not be able to upload duplicate custom CA certificates to your Cisco Secure Email and Web Manager. • You will not be able to upload custom CA with No CAFlag or CAFlag set to False to your Cisco Secure Email and Web Manager • [Applicable from new AsyncOS 14.0 install only]: You can update the existing system CA certificate bundle to the latest available version. • Cisco Secure Email and Web Manager validates the certificate chain while uploading custom intermediate CA, and the intermediate CA will be rejected if the CA is uploaded before you upload the Trusted Root CA in the appliance. <p>Use the Update Now option in Network > Certificates page in the web interface or the <code>updatenow</code> CLI command to update the existing system CA certificate bundle.</p> <ul style="list-style-type: none"> • [Applicable from AsyncOS 14.0 upgrade only]: <p>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. There is no certificate append prompt given in GUI upgrade flow but it happens automatically.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p> Note The backup of the current system CA bundle is stored in the following location -</p> <p style="text-align: center;"><code>/data/pub/systemca.old/trustedca.old.pem</code></p> </div> <ul style="list-style-type: none"> - After upgrade, the system CA certificate bundle of the current AsyncOS build is updated to the latest version automatically.
--	---

Peer Certificate Validation for Subject name	<p>For a X509 certificate, the Cisco Secure Email and Web Manager validates if the common name field (CN) of that certificate's subject distinguished name or the subjectAltName extension of type dNSName (SAN:dNSName) has peer's Hostname.</p> <p>The Subject name validation is applicable for the following services:</p> <ul style="list-style-type: none">• LDAP• Updater• Alert over TLS
Rebranded Product and Related Documentation	<p>We have rebranded the product, and related documentation from “Cisco Content Security Management” to “Cisco Secure Email and Web Manager.”</p>

Changes in Behavior

SPAM Quarantine Portal	In AsyncOS 14.0, only HTTPS will be enabled by default in the SPAM quarantine portal. We recommend that you do not enable HTTP alone for services as HTTP can be deprecated in future.
Smart Licensing - SSE Integration feature	<p>Cloud Service will be enabled and Appliance will be registered automatically when smart licensing is enabled and registered.</p> <ul style="list-style-type: none"> To enable or disable Cisco SecureX and Cisco Threat response, the option is introduced under the generalconfig command. The command <code>threatresponseconfig</code> will display the warning message “Enter general config command to Enable/Disable of Cisco SecureX/ Threat Response feature”. The command <code>smartaccountinfo</code> is introduced for getting the Smart account information. When you enable CloudServices, Cisco SecureX will be enabled automatically and Cisco Securex will be disabled when CloudServices is disabled.
Removal of <code>tcpdump</code> command	In AsyncOS 14.0, the CLI command <code>tcpdump</code> has been deprecated.
Sub configuration master gets overwritten and incorrectly pushed with secondary configuration master.	When you select the sub configuration master and make changes and another user switches changes to the secondary configuration master without a commit, the first configuration is a success and an error identifiers are displayed for the second user. Ideally, you must not concurrently switch or modify sub configuration masters. Additionally, you must not perform a configuration master push while changes are happening.
Upgrade Scenario	After you perform an upgrade to Cisco Secure Email and Web Manager 14.0.0 - 404, you cannot revert to the older version.
CA bundle while upgrade	While performing a GUI upgrade, by default old system CA bundles are appended to the target build only in the first upgrade. You will not be able to append the old system CA certificates if the base builds are 14.0.0 - 250 or more.
Smart Licensing - SSE Integration feature	SSE Connector refers the CA certificate available in the appliance and services are restarted every time there is a change in the Trusted CA bundle.

SSL Cipher Support changes	<p>The following SSL cipher configuration changes are only applicable when you install AsyncOS 14.0 for Cisco Secure Email and Web Manager for the first time:</p> <ul style="list-style-type: none"> • "The TLS_DHE_RSA_WITH_AES_256_CBC_SHA cipher suite is no longer supported for TLS <= 1.2 server services: • "The following cipher suites are no longer supported for TLS <= 1.2 client services: <ul style="list-style-type: none"> - 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
SSH algorithms support changes	<p>The following SSH server configuration changes are only applicable when you install AsyncOS 14.0 for Email and Web Manager for the first time:</p> <p>The following cipher algorithm and MAC methods are disabled in your Email and Web Manager by default:</p> <ul style="list-style-type: none"> • Cipher Algorithm - 3des-cbc • MAC Methods: <ul style="list-style-type: none"> - hmac-md5 - umac-64@openssh.com - hmac-ripemd160 - hmac-ripemd160@openssh.com - hmac-sha1-96 - hmac-md5-96 • Key Exchange Algorithm - diffie-hellman-group1-sha1 <p>If you want to enable the above cipher algorithm, MAC methods and Key Exchange algorithm, use the <code>sshconfig > SSHD > setup</code> sub command in the CLI.</p>
Reporting Database	<p>When reports receive back log reporting archive files, it occurs that the reports gets deleted and the content get copied into the directory. When this occurs, the appliance displays an error <i>Directory not empty</i>. To avoid this scenario, an INFO log is generated every time this occurs.</p>
Removal of NG link when EOL notification is displayed	<p>In AsyncOs 14.0, as per EOL implementation, NG link is removed from the banner when EOL notification is shown, as EOL takes precedence.</p>

Accessing the New Web Interface

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.

Upgrading to AsyncOS 14.0

- [Upgrading to AsyncOS 14.0 - 418 MD \(Maintenance Deployment\)](#)
- [Upgrading to AsyncOS 14.0 - 404 LD \(Limited Deployment\)](#)
- [Upgrading to AsyncOS 14.0 - 359 LD \(Limited Deployment\)](#)

Upgrading to AsyncOS 14.0 - 418 MD (Maintenance Deployment)

You can upgrade to the release 14.0.0 - 418 build number from the following versions:

- 14.0.0 - 416
- 14.0.0 - 404
- 14.0.0 - 359
- 14.0.0 - 217
- 13.8.1 - 074
- 13.8.1 - 068
- 13.6.2 - 078
- 13.0.0 - 277
- 12.8.1 - 002
- 12.5.0 - 683
- 12.0.2 - 005
- 12.0.1 - 011

Upgrading to AsyncOS 14.0 - 404 LD (Limited Deployment)

You can upgrade to the release 14.0.0 - 404 build number from the following versions:

- 14.0.0 - 359

- 14.0.0 - 217
- 13.8.1 - 068
- 13.6.2 - 058
- 13.0.0 - 249
- 12.8.1 - 002
- 12.5.0 - 683
- 12.0.2 - 005
- 12.0.1 - 011

Upgrading to AsyncOS 14.0 - 359 LD (Limited Deployment)

You can upgrade to the release 14.0.0 - 359 from the following versions:

- 14.0.0 - 217
- 13.8.1 - 052
- 13.8.0 - 344
- 13.6.2 - 058
- 13.5.0 - 117
- 13.0.0 - 249
- 12.8.0 - 026
- 12.5.0 - 683
- 12.5.0 - 678
- 12.5.0 - 636
- 12.5.0 - 633
- 12-0-2 - 005
- 12-0-1 - 011
- 12.0.0 - 478
- 11.5.1 - 115
- 11.5.0 - 110
- 11.4.0 - 823
- 11.0.1 - 161
- 11.0.0 - 136

Installation and Upgrade Notes

- [Important Additional Reading, page 13](#)
- [Virtual Appliance, page 13](#)
- [Pre-Upgrade Requirements, page 13](#)
- [IPMI Messages During Upgrade, page 14](#)

- [Upgrading to This Release, page 15](#)

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 17](#).

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

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 13](#).
 - 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 14](#)

- [Back Up Your Existing Configuration, page 14](#)
- [Centralized Policy, Virus, and Outbreak Quarantine Certificate Settings in FIPS Mode, page 14](#)

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 12](#).

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 14.0 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 appliance to AsyncOS 14.0.
 - 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 Security Content Management appliance, 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 Security Content Management Appliance 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 13](#).
- 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 13](#).
-

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.

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 defects in this release.

- [Bug Search Tool Requirements](#), page 16
- [Lists of Known and Fixed Issues](#), page 16
- [Finding Information about Known and Resolved Issues](#), page 17

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=14.0.0&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=14.0.0&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 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://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, 14.0.
- 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 PDF.

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.

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.

© 2021 Cisco Systems, Inc. All rights reserved.