

Release Notes for AsyncOS 14.2 for Cisco Secure Email and Web Manager - MD (Maintenance Deployment)

Published: May 26, 2022

Revised: March 09, 2023

Contents

- [What's New in this Release, page 2](#)
- [Changes in Behavior, page 7](#)
- [Upgrade Paths, page 10](#)
- [Installation and Upgrade Notes, page 10](#)
- [Supported Hardware for this Release, page 14](#)
- [Known and Fixed Issues, page 14](#)
- [Related Documentation, page 15](#)
- [Service and Support, page 16](#)



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
<p>PVO Quarantine Threshold Alert</p>	<p>Secure Email and Web Manager sends an alert to the recipient when the number of PVO quarantine messages exceeds a user-defined threshold value set for a specific time duration and PVO quarantine.</p> <p>Secure Email and Web Manager ensures that you receive the alerts you set as an email.</p> <p>You can configure PVO quarantine threshold alerts, using the following ways:</p> <ul style="list-style-type: none"> • Email > Message Quarantine > Policy Virus and Outbreak Quarantines page in the legacy web interface • <code>quarantineconfig</code> command in the CLI <p>For more information, see “PVO Quarantine Threshold Alert” section in the “Centralized Policy, Virus, and Outbreak Quarantines” chapter of the user guide.</p>
<p>Configuring End-User Quarantine for Shared Mailbox</p>	<p>You can now access the End-User Quarantine (EUQ) of the Shared Mailbox and perform any actions on the spam quarantined messages when an administrator enables single sign-on to access EUQ and you have delegated access to that Shared Mailbox. It reduces the workload on administrators and assists in the timely delivery of quarantined messages.</p> <p>You can access EUQ to search the spam quarantine messages of the Shared Mailbox if you can log into EUQ through SAML 2.0 authentication. You can view the spam quarantined messages of your Primary Mailbox, and you can now add the Shared Mailbox to which you have access and view the spam quarantined messages of that Shared Mailbox.</p> <p>EUQ allows you to add multiple Shared Mailboxes and provides an option to view, search, release, release and add to safelist, and delete the spam quarantined messages.</p> <p>You can access the Shared Mailbox in the following ways:</p> <ul style="list-style-type: none"> • Click your email quarantine or View All Quarantined Messages link provided in the spam quarantine notification mail. • Log in to Secure Email and Web Manager EUQ using spam quarantine portal. <p>For more information, see “Configuring End-User Quarantine for Shared Mailbox” section in the “Spam Quarantine” chapter of the user guide.</p> <hr/> <p> Note You can use this feature if you are an Office 365 user. This feature uses Microsoft Azure Active Directory API to provide access to End User Quarantine associated with shared mailboxes.</p>

Managing Data Storage Time for Centralized Email Tracking Service

You can now configure your Secure Email and Web Manager to store the messages (data) in the Centralized Email Tracking database based on the number of days.

You can configure this feature in any one of the following ways:

- Use the **Apply Data Storage Time** option in **System Administration > Disk Management > Edit Data Disk Management** page of the legacy web interface.
- Use the `Manage data based on the storage time` statement in `diskquotaconfig > edit > Centralized Email Tracking` sub command in the CLI.





Important: From Secure Email and Web Manager 13.6.2 version, the Splunk database is no longer used for email tracking data. All new email tracking data is stored in the Lucene database. When you use this feature, the Splunk database that contains the email tracking data gets deleted automatically.



Action: Make sure you take a backup 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 “Scheduling Single or Recurring Backups” section in the “Common Administrative Tasks” chapter of the user guide.





Note If your organization network has only one Secure Email and Web Manager, you need to deploy a new Virtual Machine (VM) in the network. For more information on how to deploy a virtual Secure Email and Web Manager, see [Cisco Secure Email and Web Virtual Appliance Installation Guide](#).


For more information, see “Managing Data Storage Time” section in the “Common Administrative Tasks” chapter of the user guide.



<p>Enhancements on Grouping Appliances for File Analysis Reporting</p>	<p>Cisco Secure Email and Web Manager now uses the Smart Account ID to group appliances in your organization and to view the file analysis result of all appliances.</p> <p>When Smart Licensing is enabled on Cisco Secure Email and Web Manager, and you configure the appliance group for file analysis reporting, the system automatically registers Smart Account ID as the Appliance Group ID. You can change the Appliance Group ID at any time, and the change takes effect immediately without a Commit action.</p> <hr/> <p> Note You must upgrade the email gateway and Secure Email and Web Manager to the 14.2 version for this feature to work.</p> <hr/> <p>For more information, see the “(Cloud File Analysis) Configure the Management Appliance to Display Detailed File Analysis Results” section in the “Using Centralized Email Security Reporting” chapter of the user guide.</p> <hr/> <p> Note This feature is only available for on-premises admin users.</p>
<p>New Sender Domain Reputation Verdicts</p>	<p>The Sender Domain Reputation (SDR) verdicts are updated in this release to accurately reflect the intended meaning and recommended usage.</p> <p>After you upgrade to AsyncOS 14.2.x release, the legacy SDR verdicts in the reporting and message tracking are replaced with the new SDR verdicts as follows:</p> <ul style="list-style-type: none"> • Untrusted • Questionable • Neutral • Favorable • Trusted • Unknown <p>The SDR reporting and message tracking results are updated with the new verdicts accordingly on upgrade. Make sure that you also upgrade your email gateway(s) to the latest 14.2 version that contains the new SDR verdicts.</p> <hr/> <p> Note The SDR Reporting and Tracking AsyncOS APIs are updated to reflect the new SDR Threat Level and Category structure.</p> <hr/> <p> Note The SDR Tracking Logs are updated to reflect the new SDR Threat Levels and Sender Maturity details.</p>

Support for new feature in AsyncOS 14.2 for Cisco Secure Email Cloud Gateway	<p>URL Retrospection Report page - This report page shows URLs processed by the URL Retrospective Service. This page lists the malicious URLs, date and time when verdict is received from the URL Retrospective Service, and the remediation status of impacted messages.</p> <p> Note The URL Retrospection Report data is only available for Cloud admin users.</p> <p>For more information, see the “URL Retrospection Report Page” section of the “Using Centralized Email Security Reporting” chapter of the user guide.</p>
Smart Software Licensing Enhancements	<p>Following are the enhancements made to the Smart Software Licensing feature:</p> <p>License Reservation: You can reserve licenses for features enabled in Secure Email and Web Manager without connecting to the Cisco Smart Software Manager (CSSM) portal. This is mainly beneficial for users that deploy Secure Email and Web Manager in a highly secured network environment with no communication to the Internet or external devices.</p> <p>For more information, see “Overview” and “Reserving Feature Licenses” sections of “Common Administrative Tasks” chapter of the user guide.</p> <p>Device Led Conversion: After you register Secure Email and Web Manager with smart licensing, all existing, valid classical licenses are automatically converted to smart licenses using the Device Led Conversion (DLC) process. These converted licenses are updated in the virtual account of the CSSM portal.</p> <p>For more information, see the “Overview” section of the “Common Administrative Tasks” chapter of the user guide.</p>
Modification of Classic Licensing - Expiration Date in Web Interface and CLI	<p>From this release onwards, the existing ‘Expiration Date’ column header in the web interface and CLI for classic licensing is modified as follows – “Expiration Date (including grace period)” to indicate that the grace period is included in the expiration date.</p> <p> Note All alert messages and mail logs are modified to display the expiration date, including the grace period for a feature key.</p>

<p>New Parameter for Syslog Push - Syslog Disk Buffer</p>	<p>[Applicable for TCP protocol only]: Syslog Disk Buffer parameter enables you to configure a local disk buffer for a syslog push log subscription to allow Secure Email and Web Manager to cache log events when the remote syslog server is unavailable. When the syslog server becomes available, the Secure Email and Web Manager begins to send all the data in the buffer for that log subscription to the syslog server.</p> <p>For more information, see the “Log Retrieval” section of the “Logging” chapter of the user guide.</p>
<p>No Support of Splunk database for Email Tracking Data</p>	<p>When you log in to Secure Email and Web Manager through the web interface or the CLI, you may see the following message if you are using the Splunk database for email tracking data:</p> <p><i>“You have x GB of email tracking data in the Splunk database. From Secure Email and Web Manager 13.6.2 version, the Splunk database is no longer used for email tracking data. All new email tracking data is stored in the Lucene database. There will be no support of the Splunk database for email tracking data in the future General Availability (GA) release of Secure Email and Web Manager.”</i></p> <p>Action: Make sure you take a backup of the email tracking data (if required). You can use the <code>backupconfig</code> command in the CLI to perform the backup action. For more information, see “Scheduling Single or Recurring Backups” section in the “Common Administrative Tasks” chapter of the user guide.</p> <hr/> <p> Note If your organization network has only one Secure Email and Web Manager, you need to deploy a new Virtual Machine (VM) in the network. For more information on how to deploy a virtual Secure Email and Web Manager, see Cisco Secure Email and Web Virtual Appliance Installation Guide.</p> <hr/> <p> Note This behaviour is only applicable for on-premises Secure Email and Web Manager.</p>

Changes in Behavior

JWT token - error message changes	<p>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.</p> <p>From this release onwards, 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.</p>
SPoG Feature Modifications	<p>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.</p> <p>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.</p> <p> Note The SPoG feature works only if all the Secure Email and Web Manager under the SPoG cluster have the same version.</p>
New Command Introduced - <code>wsaupdatesconfig</code>	<p>From this release onwards, Secure Email and Web Manager supports a new <code>wsaupdatesconfig</code> command. The <code>wsaupdatesconfig</code> command forces update of WBRs, AVC, or both WBRs and AVC data on Secure Email and Web Manager.</p>
Absolute Timeout Modifications	<p>Prior to this release, if you set the default Web UI Inactivity Timeout field to more than 12 hours, the new web interface of Secure Email and Web Manager did not log you out after 12 hours, and you could access the options available on the interface.</p> <p>After you upgrade to this release, if you set the default Web UI Inactivity Timeout field to more than 12 hours, the new web interface of Secure Email and Web Manager logs you out after 12 hours.</p>
Reporting Calendar Modifications	<p>Prior to this release, in the new web interface, you could select the date for the reporting data that was already aggregated by month, but wrong results were displayed for the date as you can only view monthly data if data has been aggregated by month.</p> <p>After you upgrade to this release, you can now select only the first day of every month, and complete reporting data for that month is displayed.</p>
Mail Logs Changes	<p>Prior to this release, the information in the subject of the Mail Logs was not enclosed in quotes.</p> <p>After you upgrade to this release, the information in the subject of Mail Logs is now enclosed in double quotes.</p>

<p>FQDN Validation Changes</p>	<p>From this release onwards, when you validate a peer certificate or import a certificate, FQDN validation checks whether the SAN extension is critical when the subject name (common name) field is not available in the certificate that you import or in the server certificate.</p> <p> Note This behavior change is applicable only when you enable FQDN Validation during a certificate import or peer certificate validation.</p>
<p>Updater Server CA Certificate Changes</p>	<p>Following are the updater server CA certificate behavior changes made in this release:</p> <ul style="list-style-type: none"> • FQDN validation is performed when you add the updater server CA certificate in your Secure Email and Web Manager. A new statement - <i>"Do you want to check if Common Name or SAN:dNSName or both are in Fully Qualified Domain Name(FQDN) format?"</i> is added in the <code>updateconfig > trusted_certificates > add</code> sub command in the CLI to perform the FQDN validation. • CA certificate validation is performed when you add an updater CA certificate in your Secure Email and Web Manager. <p> Note The Secure Email and Web Manager allows you to add the updater CA certificate if the root CA certificate and the other certificates in the chain are trusted.</p>
<p>CA Certificates Validation During System Upgrade</p>	<p>From this release onwards, when you upgrade your Secure Email and Web Manager, the existing CA certificate is upgraded only if the CA certificate is active (not expired) and the CA flag in the certificate is set to true. The Secure Email and Web Manager rejects expired certificates and the CA certificate with the CA flag set to false during system upgrade. Also, when you load configuration file on your Secure Email and Web Manager, the CA certificate with CA flag set to false and expired certificates are removed.</p>

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

You can upgrade to release 14.2.0-224 MD (Maintenance Deployment) from the following versions:

- 13.8.1-052
- 13.8.1-068
- 13.8.1-074
- 13.8.1-090
- 13.8.1-101
- 13.8.1-102
- 13.8.1-108
- 14.0.0-404
- 14.0.0-418
- 14.1.0-199
- 14.1.0-227
- 14.1.0-239
- 14.1.0-250
- 14.2.0-203
- 14.2.0-206
- 14.2.0-212
- 14.2.0-217

Installation and Upgrade Notes

- [Important Additional Reading, page 11](#)
- [Virtual Appliance, page 11](#)
- [Pre-Upgrade Requirements, page 11](#)
- [IPMI Messages During Upgrade, page 12](#)
- [Upgrading to This Release, page 12](#)
- [Post-Upgrade Requirements, page 13](#)

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 15](#).

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 11](#).
 - 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 12](#)
- [Back Up Your Existing Configuration, page 12](#)
- [Centralized Policy, Virus, and Outbreak Quarantine Certificate Settings in FIPS Mode, page 12](#)

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 10](#).

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 14.2 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 14.2.
 - 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 11](#).
 - 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 11](#).

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

Spam Notification URL Changes

After you upgrade to Secure Email and Web Manager 14.2, if you cannot log in using the saved spam notification URL, use the new URL mentioned in the spam notification mail.

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 14
- [Lists of Known and Fixed Issues](#), page 14
- [Finding Information about Known and Resolved Issues](#), page 15

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/search?kw=*&pf=prdNm&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20IronPort%20Security%20Management%20Appliance%20Software&rls=14.2.0
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20IronPort%20Security%20Management%20Appliance%20Software&rls=14.2.0

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, 14.2.0
- 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.

Cisco Secure Products	Location
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.

© 2023 Cisco Systems, Inc. All rights reserved.