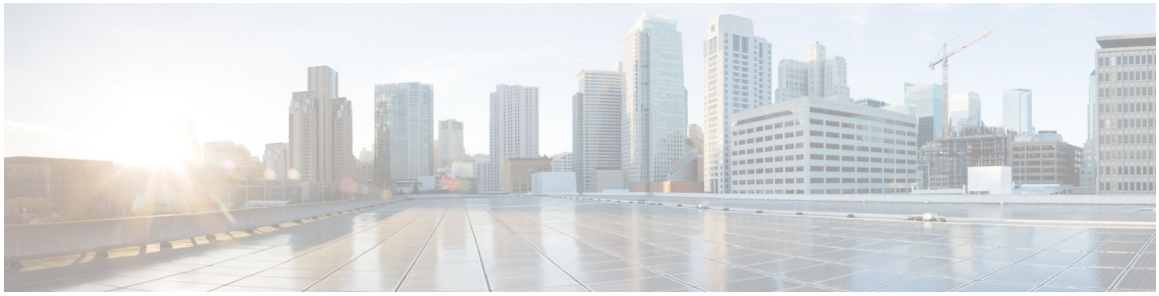

Release Notes for AsyncOS 12.0 for Cisco Content Security Management Appliances

Published: February 18, 2019
Revised: April 25, 2019

Contents

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

Feature	Description
New Web Interface for Reporting, Quarantine and Tracking	The appliance now has a new web interface to search and view: • **Email Reports.** You can now view email reports from the Reports drop-down based on the following categories: – Email Threat Reports – File and Malware Reports – Connection and Flow Reports – User Reports – Filter Reports For more information, see the "Using Centralized Email Security Reporting on the New Web Interface" chapter in the user guide. • **Spam Quarantine** – You can now view and search for spam and suspected spam messages in **Quarantine > Spam Quarantine > Search** page in the web interface. – You can view, add, and search for domains added in the safelist and blocklist in **Quarantine > Spam Quarantine > Safelist** or **Blocklist** page in the web interface. For more information, see the "Spam Quarantine" chapter in the user guide. • **Policy, Virus and Outbreak Quarantines.** You can view and search for policy, virus and outbreak quarantines in Quarantine > Other Quarantine > Search page in the web interface. For more information, see the "Centralized Policy, Virus, and Outbreak Quarantines" chapter in the user guide. • **Message Tracking.** You can search for messages or a group of messages depending on your search criteria in Tracking > Search page in the web interface. For more information, see the "Tracking Messages" chapter in the user guide. **Important!** • Make sure that you have enabled AsyncOS API 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. • If `trailblazerconfig` is disabled, the AsycnOS API ports configured in **Management Appliance > Network > IP Interfaces** must be opened on the firewall. The default AsyncOS API HTTP/HTTPS port is 6080/6443. For more information, see Accessing the New Web Interface, page 12.

Encrypting sensitive information on the appliance	You can use the `adminaccessconfig > encryptconfig` sub command in the CLI to configure encryption of sensitive information on your appliance. **Note** By default, the encryption is disabled on the appliance.
Message Tracking Enhancement	You can now search for messages based on the "`Reply-To`" header of the message. For more information, see "Tracking Messages" chapter of the user guide or the online help.
The `trailblazerconfig` CLI Command	You can use the `trailblazerconfig` command to route your incoming and outgoing connections through HTTPS ports on the new web interface. **Note** By default, `trailblazerconfig` CLI command is enabled on your appliance. You can see the inline help by typing the command: `help trailblazerconfig`. For more information, see "The trailblazerconfig CLI Command" section of the user guide.
Support for new features in AsyncOS 12.0 for Cisco Email Security Appliances	You can now view the following reports on the Reporting page of the Security Management appliance: • **External Threat Feeds** • **Sender Domain Reputation** For more information, see the "Using Centralized Email Security Reporting" chapter in the user guide. You can now view outgoing TLS connections summary for DANE Success and DANE Failure scenarios. For more information, see "SMTP DNS-based Authentication of Named Entities" section of the user guide or online help for *AsyncOS 12.0 for Cisco Email Security Appliances*. You can now use the following message events to search for messages on the Message Tracking page of the Security Management appliance: • **External Threat Feeds** • **Sender Domain Reputation** • **DANE Failure**
Metrics Bar Widget	The Metrics Bar widget enables you to view the real time data of the file analysis done by the Cisco Threat Grid appliance on the Advanced Malware Protection report page. For more information, see "Advanced Malware Protection Page" section of the user guide.

Advanced Malware Protection Report Enhancement	The Advanced Malware Protection Report page has the following enhancements: • A new section - **Incoming Malware Files by Category** to view the percentage of blacklisted file SHAs received from the AMP for Endpoints console that are categorized as **Custom Detection**. The threat name of a blacklisted file SHA obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report. • A new section - **Incoming Malware Files by Category** to view the percentage of blacklisted file SHAs based on the threshold settings that are categorised as **Custom Threshold**. • You can click on the link in the More Details section of the report to view the file trajectory details of a blacklisted file SHA in the AMP for Endpoints console. • A new verdict - **Low Risk** is introduced when no dynamic content is found in a file after file analysis. You can view the verdict details in the Incoming Files Handed by AMP section of the report. For more information, see the "Using Centralized Email Security Reporting on the New Web Interface" chapter in the user guide.
New Web Interface for Web Reporting and Tracking	The appliance now has a new web interface to search and view: • **Web Reports** You can now view web based reports from the Reports drop-down based on the following categories: – General Reports – Threats Reports • **Web Tracking** You can search for web transactions depending on your search criteria. On your Security Management appliance , click on the **Web** dropdown and choose **Tracking > Web Tracking Search** page. For more information on web reports and web tracking, see "Using Centralized Web Reporting and Tracking" chapter of the user guide. **Important!** • Make sure that you have enabled AsyncOS API 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. • If `trailblazerconfig` is disabled, the AsycnOS API ports configured in **Management Appliance > Network > IP Interfaces** must be opened on the firewall. The default AsyncOS API HTTP/HTTPS port is 6080/6443. For more information, see Accessing the New Web Interface, page 12.

HTTPS Reports Page	You can now view the overall aggrgation of the HTTP/HTTPS traffic and the summary of the ciphers based on the client and server side connection for each HTTP/HTTPS traffic, on the HTTPS Reports report page. For more information, see "Using Centralized Web Reporting and Tracking" chapter of the user guide.
Support for Smart Software Licensing	Smart Software Licensing enables you to manage and monitor Cisco Email Security appliance licenses seamlessly. To activate Smart Software licensing, you must register your appliance with Cisco Smart Software Manager (CSSM) which is the centralized database that maintains the licensing details about all the Cisco products that you purchase and use. **Caution** After you enable the Smart Licensing mode on your appliance, you may not be able to rollback to the Classic Licensing mode. For more information, see the "Common Administrative Tasks" chapter in the user guide.
Integrating the Appliance with Cisco Threat Response Portal	You can integrate your appliance with Cisco Threat Response portal, and perform the following actions in Cisco Threat Response portal: • View the message tracking data from multiple appliances in your organization. • Identify, investigate and remediate threats observed in the message tracking. • Resolve the identified threats rapidly and provide recommended actions to take against the identified threats. • Document the threats in the portal to save the investigation, and enable collaboration of information among other devices on the portal. For more information, see the "Assigning Network and IP Addresses" chapter in the user guide.

Support for the Office 365 Web Service External URL Categories feature in AsyncOS 11.5.1-124 for Cisco Web Security Appliances	This release supports the Office 365 Web Service External URL Categories feature in AsyncOS 11.5.1-124 for Cisco Web Security Appliances. For more information, see the "Using Centralized Web Reporting and Tracking" chapter in the user guide.
Web Traffic Tap Policies for web	Cisco Content Security Management appliance now allows you to set Web Traffic Tap Policies. You can define the Web Traffic Tap Policies based on which web traffic that passes through the Web Security appliance will be tapped. You must enable the Web Traffic Tap feature in Web Security appliance to set the Web Traffic policies in the Security Management appliance. Four new sections are included in the Overview report page. The sections are: • Web Traffic Tap Status • Web Traffic Tap Summary • Tapped HTTP/HTTPS Traffic • Tapped Traffic Summary For more information about the report, see the "Using Centralized Web Reporting and Tracking" chapter in the user guide.

Changes in Behaviour

Change in Report Pages	The following reports are changed on the new web interface, in this release: • Overview report page is renamed to Mail Flow Summary. • Outbreak Filters report page is renamed to Outbreak Filtering. • Virus Types report page is renamed to Virus Filtering. • Advanced Malware Protection, AMP File Analysis, AMP Verdict Updates and Mailbox Auto Remediation report pages are merged as Advanced Malware Protection. • Incoming Mail and Outgoing Senders report pages are merged as Mail Flow Details. • TLS Connections report page is renamed to TLS Encryption. • Geo-Distribution report page is renamed to Connection by Country. • Internal Users report page is renamed to User Mail Summary. • Web Interaction Tracking report page is renamed to Web Interaction. For more information, see "Understanding the Email Reporting Pages" section in the user guide
Encrypting Passphrases	After you upgrade to this release, you can encrypt the user's passphrases when updating the configuration files on the appliance. To encrypt the passphrase, do one of the following: • On the **System Administration > Configuration File** page, select the **Encrypt passphrases in the Configuration Files** checkbox. • Use the `saveconfig` command in the CLI to encrypt the passphrase.

Changes in Accessing the Spam Quarantine	• The administrative users can now access the Spam Quarantine page on the new web interface of the appliance. You can navigate to **Quarantine > Spam Quarantine > Search** page on the new web interface to access the Spam Quarantine page. • The end-users can now access the Spam Quarantine portal on the new web interface, For more information, see Accessing the New Web Interface, page 12. **Important!** Only end users can log in to the end-user spam quarantine portal. Local and externally-authenticated users cannot log in to the end-user spam qurantine portal. • You will now recieve spam notification with a link to view the quarantined messages on the new web interface. Make sure that you have enabled AsyncOS API HTTP/HTTPS ports and HTTPS service on the appliance. • If you are using spam quarantine on the any other interface (Data 1), then you must set it as the default interface. **Important!** If the `trailblazerconfig` is enabled, then you must enable the AsyncOS API ports (HTTP/HTTPS) and HTTP/HTTPS service on the (Data 1) interface. If the `trailblazerconfig` is disabled, then you must enable the AsyncOS API ports (HTTP/HTTPS) on the (Data 1) interface.
Changing the User's Password After Expiry	Users are prompted to change the password after the user account is expired. For more information, see "Changing the User's Password After Expiry" section in the user guide.
Changes in Demo Certificates	Prior to this release, the appliance was pre-configured with a demonstration certificate to enable the TLS connections. After you upgrade to this release, the appliance generates a unique certificate to enable TLS connection. The existing demonstration certificate that is used in the following configurations are replaced with the new certificate: • Mail Delivery • LDAP • Networking • URL Filtering • SMTP Services

Comparison of Web Interfaces, AsyncOS 12.0 vs. Previous Releases

Web Interface Page or Element	AsyncOS 12.0	Previous Releases
Landing Page	After you log in to the Security Management appliance, the Mail Flow Summary page is displayed.	After you log in to the appliance, the System Status page is displayed.
Product Drop-down	You can switch between the Email Security Appliance and the Web Security Appliance from the Product drop-down.	You can use the Email or Web tab to switch between the Email Security Appliance and the Web Security Appliance.
Reports Drop-down	You can view reports for your Email and Web Security Appliances from the Reports drop-down.	You can view reports for your Email and Web Security Appliances from the Reporting drop-down menu.
Management Appliance Tab	Click ⚙ on the Security Management appliance to access the Management Appliance tab.	You can enable and configure reporting, message tracking and quarantines, as well as configure network access, and monitor system status.
My Reports Page	Click ⚙ on the Security Management appliance and choose **Email > Reporting > My Reports** to access the My Reports page.	You can customize your reports dashboard by assembling charts (graphs) and tables from existing report pages.
Reporting Data Availability Page	Click ⚙ on the Security Management appliance and choose **Email > Reporting > Reporting Data Availability** to access the Reporting Data Availability page.	You can view, update and sort data to provide real-time visibility into resource utilization and email traffic trouble spots.
Scheduling & Archiving Reports	Click ⚙ on the Security Management appliance and choose **Email > Reporting > Scheduled Reports** to schedule your reports. Click ⚙ on the Security Management appliance and choose **Email > Reporting > Archive Reports** to archive your reports.	You can schedule reports using the **Email > Reporting > Scheduled Reports** page, and archive your reports using the **Email > Reporting > Archived Report** page of the Security Management appliance.

Web Interface Page or Element	AsyncOS 12.0	Previous Releases
Reporting Overview Page	The Email Reporting Overview page on the Security Management appliance has been redesigned as Mail Flow Summary page in the new web interface. The Mail Flow Summary page includes trend graphs and summary tables for incoming and outgoing messages.	The Email Reporting Overview page on the Security Management appliance provides a synopsis of the email message activity from your Email Security appliances. The Overview page includes graphs and summary tables for the incoming and outgoing messages.
Advanced Malware Protection Report Pages	The following sections are available on the **Advanced Malware Protection** report page of the Reports menu: • Summary • AMP File Reputation • File Analysis • File Retrospection • Mailbox Auto Remediation	The **Email > Reporting** drop-down menu of the Security Management appliance has the following Advanced Malware Protection report pages: • Advanced Malware Protection • AMP File Analysis • AMP Verdict Updates • Mailbox Auto Remediation
Outbreak Filters Page	The Past Year Virus Outbreaks and Past Year Virus Outbreak Summary are not available in the Outbreak Filtering report page of the new web interface.	The **Email > Reporting Outbreak Filters** page displays the Past Year Virus Outbreaks and Past Year Virus Outbreak Summary.
Spam Quarantine (Admin and End-User)	Click **Quarantine > Spam Quarantine > Search** on the new web interface to access the Spam Quarantine page. For more information on the end-users access to the Spam Quarantine portal on the new web interface, see Accessing the New Web Interface, page 12.	-
Policy, Virus and Outbreak Quarantines	Click **Quarantine > Other Quarantine** on the new web interface. You can only view Policy, Virus and Outbreak Quarantines on the Security Management appliance.	You can view, configure and modify the Policy, Virus and Outbreak Quarantines on the appliance.
Select All action for Messages in Quarantine	You can select multiple (or all) messages in a quarantine and perform a message action, such as, delete, delay, release, move, etc.	You cannot select multiple messages in a quarnatine and perform a message action.

Web Interface Page or Element	AsyncOS 12.0	Previous Releases
Maximum Download Limit for Attachments	The maximum limit for downloading attachments of a quarantined message is restricted to 25 MB.	-
Rejected Connections	To search for rejected connections, click **Tracking > Search > Rejected Connection** tab on the Security Management appliance.	-
Query Settings	The **Query Settings** field of the Message Tracking feature is not available on the Security Management appliance.	You can set the query timeout in the Query Settings field of the Message Tracking feature.
Message Tracking Data Availability	Click ⚙ on the on the Security Management appliance and choose **Email > Message Tracking > Message Tracking Data Availability** to access Message Tracking Data Availability page.	You can view the missing-data intervals for your appliance.
Verdict Charts and Last State Verdicts	Verdict Chart displays information of the various possible verdicts triggered by each engine in your appliance. Last State of the message determines the final verdict triggered after all the possible verdicts of the engine.	Verdict Charts and Last State Verdicts of the messages are not available.
Message Attachments and Host Names in Message Details	Message attachments and host names are not displayed in the Message Details section of the message on the Security Management appliance.	Message attachments and host names are displayed in the Message Details section of the message.
Sender Groups, Sender IP, SBRS Score and Policy Match in Message Details	Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is displayed in the Message Details section of the message on the Security Management appliance.	Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is not available in the Message Details section of the message.
Direction of the Message (Incoming or Outgoing)	Direction of the messages (incoming or outgoing) is displayed in the message tracking results page on the Security Management appliance.	Direction of the messages (incoming or outgoing) is not displayed in the message tracking results page.

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.
- 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.
- 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)

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:

Note The end-users cannot log in to the Spam Quarantine portal on the new web interface using the interface ports 82/83.

- 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 12.0.0-478 - MD (Maintenance Deployment)

You can upgrade to release 12.0.0-478 from the following version:

- 11.4.0-800
- 11.5.1-115
- 11.5.1-121
- 12.0.0-452
- 12.0.0-457
- 12.0.0-476

Note This release is compatible with AsyncOS 12.x for Cisco Email Security Appliances and AsyncOS 11.7.0 for Cisco Web Security Applainces.

Upgrading to Release 12.0.0-322 - LD (Limited Deployment)

You can upgrade to release 12.0.0-322 from the following version:

- 11.0.0-136
- 11.4.0-812
- 11.5.0-110
- 11.5.1-115
- 12.0.0-225
- 12.0.0-305

Note This release is compatible with AsyncOS 12.0.0 for Cisco Email Security Appliances and AsyncOS 11.7.0 for Cisco Web Security Applainces.

Compatibility with Email and Web Security Releases

Compatibility with AsyncOS for Email Security and AsyncOS for Web Security releases is detailed in the Compatibility Matrix available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

Installation and Upgrade Notes

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 18.

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.

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 14.

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 preupgrade tasks:

- Verify Associated Email and Web Security Appliance Versions, page 15
- Back Up Your Existing Configuration, page 15

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 Compatibility with Email and Web Security Releases, page 14.

Back Up Your Existing Configuration

Before upgrading your Cisco Content Security Management appliance, 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.

IPMI Messages During Upgrade

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

Defect ID: CSCuz33125

Upgrading to This Release

Step 1 Address all topics described in Pre-Upgrade Requirements, page 15.

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 14.

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 cerificate 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.

Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware

Problem You receive an alert with subject "Battery Relearn Timed Out" for 380 or 680 hardware.

Solution This alert may or may not indicate a problem. The battery relearn timeout, in itself, does not mean there is any problem with the RAID controller. The controller can recover in the subsequent relearn. Please monitor your email for any other RAID alerts for the next 48 hours, to ensure that this is not the side-effect of any other problem. If you do not see any other RAID-related alerts from the system, then you can safely ignore this alert.

Post-Upgrade Notes

Traceback Issue after Upgrading

After upgrading to AsyncOS 11.0.0-115 version from AsyncOS 11.0.0-112 on M190 and M170 models, if you run the `etherconfig > media` command using the CLI, a Traceback error is displayed. Contact TAC to assist you in resolving this issue.

Supported Hardware for This Release

- All virtual appliance models.
- The following hardware models - M380, M680, M190, M390, or M690.

  To determine whether your appliance is supported, and to remedy the situation if it is not currently compatible, see https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-field-notices-list.html

The following hardware is NOT supported for this release:

- M160, M360, M660, and M1060
- M170, M370, M370D, M670 and M1070 appliances

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 17
- Lists of Known and Fixed Issues, page 17
- Finding Information about Known and Resolved Issues, page 18

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&pfVal=282509131&rls=12.0.0&sb=anfr&sts=open&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=12.0.0&sb=anfr&sts=fd&bt=custV

Finding Information about Known and Resolved Issues

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

Before You Begin

Register for a Cisco account if you do not have one. Go to https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 Log in with your Cisco account credentials.

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

Step 4 In **Releases** field, enter the version of the release, for example, 11.1

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 downand 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 Content Security Products:	Is Located At:
Security Management appliances	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web Security appliances	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
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.