Release Notes for Management Console for Cisco Cloud Email Security (AsyncOS 11.4) - LD (Limited Deployment)

Published: March 29, 2018

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 "Using Centralized Email Security Reporting on the Cloud Email Security Management Console" chapter of the user guide or online help. • Policy, Virus and Outbreak Quarantines For more information, see "Centralized Policy, Virus, and Outbreak Quarantines" chapter of the user guide or online help. • Message Tracking For more information, see "Tracking Messages" chapter of the user guide or online help.

To enable and configure reporting, message tracking, quarantines, network access, and monitor system status, you must access the legacy web interface. Click the gear ⚙ icon on the Cloud Email Security Management Console, to navigate to the legacy web interface.

The legacy 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.

Changes in Behavior

Changes in Report Names	The following reports are changed in this release: • Overview report page is renamed to Mail Flow Summary. • 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 meged into Advanced Malware Protection. • Incoming Mail and Outgoing Senders report page is merged into 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 or online help.
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 or online help.

Comparison of Web Interfaces, AsyncOS 11.4 vs. Previous Releases

Web Interface Page or Element	AsyncOS 11.4	Previous Releases
Landing Page	After you log in to the Cloud Email Security Management Console, the Mail Flow Summary page is displayed.	After you log in to the appliance, the System Status page is displayed.
Management Appliance Tab	Click ⚙ on the Cloud Email Security Management Console 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 Cloud Email Security Management Console 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.

Web Interface Page or Element	AsyncOS 11.4	Previous Releases
Reporting Data Availability Page	Click ⚙ on the Cloud Email Security Management Console 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 Cloud Email Security Management Console and choose **Email > Reporting > Scheduled Reports** to schedule your reports. Click ⚙ on the Cloud Email Security Management Console 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.
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.
Report Drill-down	You cannot perform drill-down in reports in the new web interface.	You can perform a drill-down in the following reports: • Incoming Mail • Internal Users • Content Filters • Web Interaction Tracking • System Capacity
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

Web Interface Page or Element	AsyncOS 11.4	Previous Releases
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 or End-User Quarantines	To access Spam Quarantine on the Cloud Email Security Management Console, click **Quarantine > Spam Quarantine**. The Spam Quarantine page is displayed in a new browser window.	-
Policy, Virus and Outbreak Quarantines	You can only view Policy, Virus and Outbreak Quarantines on the Cloud Email Security Management Console. To configure or modify the policy, virus and outbreak quarantines on the Cloud Email Security Management Console, click **Quarantine > Other Quarantine > View >** +.	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.
Maximum Download Limit for Attachments	The maximum limit for downloading attachments of a quarantined message is restricted to 25 MB.	-
Message Details	Click ⚙ on the Cloud Email Security Management Console and choose **Email > Message Quarantine > Policy, Virus and Outbreak Quarantine** to track quarantined messages.	You can perform message tracking of quarantined messages using the Message Details section of the quarantines.
Rejected Connections	To search for rejected connections, click **Tracking > Search > Rejected Connection** tab on the Cloud Email Security Management Console.	-
Query Settings	The Query Settings field of the Message Tracking feature is not available on the Cloud Email Security Management Console.	You can set the query timeout in the Query Settings field of the Message Tracking feature.

Web Interface Page or Element	AsyncOS 11.4	Previous Releases
Message Tracking Data Availability	Click ☼ on the on the Cloud Email Security Management Console 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 Cloud Email Security Management Console.	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 Cloud Email Security Management Console.	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 Cloud Email Security Management Console.	Direction of the messages (incoming or outgoing) is not displayed in the message tracking results page.

Accessing the Cloud Email Security Management Console

The Cloud Email Security Management Console provides a new look for monitoring reports, quarantines and searching for email messages.

Step 1 Log in to the appliance. For more information, see "Accessing the Web Interface" section of the user guide or online help.

Step 2 Click **Cloud Email Security is getting a new look. Try it !** to navigate to the Cloud Email Security Management Console.

Step 3 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.

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 7
- List of Known and Fixed Issues, page 7
- Finding Information about Known and Resolved Issues, page 7

Note Known issues on Cisco Email Security Appliances may appear in or impact functionality of Cisco Content Security Management Appliances.

Known issues in previous content security management releases may also affect this release.

Bug Search Tool Requirements

Register for a Cisco account if you do not have one. Go to https://tools.cisco.com/RPF/register/register.do.

List of Known and Fixed Issues

Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.4.0&sb=anfr&sts=open&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=11.4.0&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://tools.cisco.com/RPF/register/register.do.

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 > Security Management > Cisco Content Security Management Appliance**, and click **OK**.

Step 4 In Releases field, enter the version of the release, for example, 11.4.

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.

Content Security Release Terminology

For an explanation of terms like LD, ED, GD, and MD that are used in labeling content security product releases, see https://supportforums.cisco.com/blog/12309231/content-security-release-terminology.

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
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.