Release Notes for AsyncOS 13.6.1 for Cisco Content Security Management Appliances

Published: June 2, 2020
Revised: June 23, 2020

Contents

Cisco Systems, Inc.
www.cisco.com

What's New in this Release

Feature	Description
Cisco Advanced Phishing Protection Reporting and Tracking	**Reporting**: You can use the Advanced Phishing Protection report page to view the following: • The total number of messages that your email security gateway attempted to forward to the Cisco Advanced Phishing Protection cloud service. • The summary of messages that your email security gateway forwarded to the Cisco Advanced Phishing Protection cloud service. **Message Tracking**: You can use the Message Tracking to view the message details based on whether your email security gateway was able to forward the messages to the Cisco Advanced Phishing Protection cloud service. For more information, see "Advanced Phishing Protection (APP) Report Page" topic of the user guide.
Monitoring Mailbox Remediation Results	You can now monitor the remediation results for Mailbox Auto Remediation and Mailbox Search and Remediate using the Remediation Report. This report provides a summary of: • Total number of messages attempted for remediation using Mailbox Auto Remediation and Mailbox Search and Remediate. • Number of messages successfully remediated for a configured remedial action. • Number of messages for which the remediation failed. Click the Mailbox Auto Remediation and Mailbox Search and Remediate tabs in the report to view details about the messages for which the remediation was attempted. For more information, see "Remediation Reports Page" topic of the user guide.
Manual searching and remediating messages in the mailbox and filtering it in tracking	You can now configure your appliance to remediate the messages manually using the Search and Remediate feature. The Search and Remediate feature provides the capability to search for the messages using the Message Tracking filter and apply remedial action on the messages. You can view the report based on the search criteria that displays the filtered messages delivered to the user mailbox. For more information, see "Remediating Messages in Mailboxes" topic of the user guide.

New web interface of the appliance in Dark Mode	Dark Mode is a reversed color scheme that utilizes light-colored typography, UI elements, and iconography on dark backgrounds. You can now use dark mode on the new web interface of your appliance. For more information, see "Accessing the New Web Interface on Dark Mode" topic of the user guide.
Cisco Threat Response Enhancements	• You can now connect to the Cisco Threat Response Server through a proxy. Use the `threatresponseconfig >enable_proxy` command in the CLI. • You can now choose the "APJC data center - APJC (`api.apj.sse.itd.cisco.com`)" to connect your appliance to the Cisco Threat Response portal. For more information, see the"Integrating the Appliance with Cisco Threat Response" and "Integrating the Appliance with Cisco Threat Response using CLI" topics of the user guide.
Monitoring Service Status on the New Web Interface of the Appliance	You can perform the following on the New Web Interface of the appliance: • Configure Centralized Email Reporting • Configure Centralized Email Tracking • Configure Spam Quarantine: – Edit Spam Quarantine Settings – Edit Safelist/Blocklist Settings For more information, see "Enabling Centralized Email Tracking on the New Web Interface of the Appliance", "Enabling Centralized Email Reporting on the New Web Interface of the Appliance", "Enabling Safelist/Blocklist on the New Web Interface" and "Enabling and Configuring Spam Quarantine on the New Web Interface" topics of the user guide.
Enable or disable the next generation web interface banner	You can use the `adminaccessconfig > NGUIBANNER` command in the CLI to enable or disable the banner link that redirects to the new web interface of the appliance. For more information, see "Enabling and Disabling Message Banners for Administrative Users" topic of user guide.

Changes in Behavior

Changes in URL Search	After you upgrade to this release, if you want to search for a URL in the message tracking of the new web interface, you must use "*" before and/or after the search string for retrieving the results. For example, if you are searching for https://www.cisco.com, you can use *cisco.com* or https://cis* to retrieve the search results.

Comparison of Web Interfaces, New vs. Legacy Web Interface

Web Interface Page or Element	New Web Interface	Legacy Web Interface
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 Service Status tab of the Security Management appliance to manage centralized services.	You can enable and configure reporting, message tracking and quarantines, as well as configure network access, and monitor system status.
Favorites Reports Page	Select **Email** from the Product drop-down and choose **My Favorite Reports** from the Reports drop-down.	You can view the My Reports page from **Email > Reporting > My Reports**.
Reporting Data Availability Page	Select **Email** from the Product drop-down and choose **Reporting Data Availability** from the Reports drop-down.	You can view the My Reports page from **Email > Reporting > Reporting Data Availability**.
Scheduling & Archiving Reports	Select **Email** from the Product drop-down and choose Monitoring > **Schedule & Archive** from the Reports drop-down.	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	New Web Interface	Legacy Web Interface
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 7.	-
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	New Web Interface	Legacy Web Interface
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 gear icon on SecurityManagement 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.

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

  - Make sure that the configured HTTPS port is opened on the firewall. The default HTTPS port is 4431.
  - Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.
- When `trailblazerconfig` CLI command is disabled, use the following URL - `https://example.com:<https-port>/ng-login`

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Upgrade Paths

Upgrading to Release 13.6.1-201 - GD (General Deployment)

You can upgrade to release 13.6.1-201 from the following versions:

- 11.0.0-136
- 11.0.1-161
- 11.4.0-823
- 11.5.0-110
- 11.5.1-115
- 12.0.0-478
- 12.0.1-011
- 12.0.2-007
- 12.5.0-670
- 12.5.0-658
- 13.0.0-249
- 13.5.0-117
- 13.6.0-157
- 13.6.1-118
- 13.6.1-193

Upgrading to Release 13.6.1-193 - LD (Limited Deployment)

You can upgrade to release 13.6.1-193 from the following versions:

- 11.0.0-136
- 11.0.1-161
- 11.4.0-823
- 11.5.0-110
- 11.5.1-115
- 12.0.0-478
- 12.0.1-011
- 12.0.2-007
- 12.5.0-658
- 13.0.0-249
- 13.5.0-117
- 13.6.0-157
- 13.6.1-118

Note This release is compatible with AsyncOS 13.5.1 for Cisco Email Security Appliances.

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 14.

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 10.

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 10
- Back Up Your Existing Configuration, page 11
- Centralized Policy, Virus, and Outbreak Quarantine Certificate Settings in FIPS Mode, page 11

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 9.

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.

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

After upgrading your managed Email Security appliance in FIPS mode to AsyncOS 13.0 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 Security Content Management appliance to AsyncOS 13.6.1.

Step 2 Upgrade your Cisco Email Security appliance to AsyncOS 13.5.1.

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 Cisco Security Content ManagementAppliance User Guide.

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

Note While upgrading, do not connect any devices (keyboard, mouse, management devices (Raritan) etc.) to the USB ports of the appliance.

Step 1 Address all topics described in Pre-Upgrade Requirements, page 10.

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 10.

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.

Supported Hardware for this Release

All virtual appliance models.

- The following hardware models - M190, M195, M390, M395, M690, and M695.

  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/docs/field-notices/639/fn63931.html.

The following hardware is NOT supported for this release:

- M160, M360, M660, and X1060
- M170, M370, M370D, M670 and X1070

- M380 and M680 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 13
- Lists of Known and Fixed Issues, page 13
- Finding Information about Known and Resolved Issues, page 13

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=13.6.0,13.6.1&sb=afr&sts=open&svr=3nH&bt=custV
Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509131&rls=13.6.1&sb=fr&sts=fd&svr=3nH&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://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, 12.5

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 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.