Release Notes for AsyncOS 12.5 for Cisco Content Security Management Appliances

Published: July 22, 2019
Revised: December 16, 2019

Contents

- What’s New In This Release, page 2
- Changes in Behaviour, page 3
- Comparison of Web Interfaces, New Web Interface vs. Legacy Web Interface, page 4
- Upgrade Paths, page 8
- Compatibility with Email and Web Security Releases, page 10
- Installation and Upgrade Notes, page 10
- Supported Hardware for this Release, page 13
- Known and Fixed Issues, page 13
- Related Documentation, page 14
- Service and Support, page 14
## What’s New In This Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Support for new hardware models              | The AsyncOS 12.5.0 release for Cisco Content Security Management appliance now supports the following hardware models in addition to the x80 and x90 series:  
  - M195  
  - M395  
  - M695  
| Managing Multiple Subset of Configuration Masters | You can now configure subsets of a particular version of a Configuration Master to centrally manage the different policy configurations of your Web Security appliance.  
  For more information, see the "Managing Web Security Appliances" chapter of the user guide or online help. |
| Performing Threat Analysis using Casebooks    | The Cisco Content Security Management appliance now includes the casebook and pivot menu widgets.  
  **Note**  
  If you are using the Microsoft Internet Explorer browser to access your appliance, you will not be able to use the casebook widget.  
  You can perform the following actions in your appliance using the casebook and pivot menu widgets:  
  - Add an observable to a casebook to investigate for any threat analysis.  
  - Pivot an observable to a new case, an existing case, or other devices registered in the Cisco Threat Response portal (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on) to investigate for threat analysis.  
  For more information, see the "Integrating with Cisco Threat Response Server" chapter of the user guide or online help. |
| Ability to choose Cisco Threat Response server when registering appliance with Cisco Threat Response portal | When registering your appliance with the Cisco Threat Response portal, you can now choose a Cisco Threat Response server to connect your appliance to the Cisco Threat Response portal.  
  The following are the Cisco Threat Response servers that are supported for this release:  
  - **AMERICAS** (api-sse.cisco.com)  
  - **EUROPE** (api.eu.sse.itd.cisco.com)  
  For more information, see "Integrating with Cisco Threat Response Server" chapter of the user guide or online help. |
## Changes in Behaviour

<table>
<thead>
<tr>
<th>Change Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing favorite reports on the New Web Interface</td>
<td>You can create a custom report page by assembling charts (graphs) and tables from all your existing email security reports on the new web interface of your appliance. For more information, see the &quot;Working with Reports on the New Web Interface&quot; chapter of the user guide or online help.</td>
</tr>
<tr>
<td>Configuring Policy, Virus and Outbreak Quarantine on the New Web Interface</td>
<td>You can now configure Policy, Virus or Outbreak Quarantine from the new web interface of your appliance. For more information, see &quot;Centralized Policy, Virus and Outbreak Quarantines&quot; chapter of the user guide or online help.</td>
</tr>
<tr>
<td>Managing APIs using Swagger UI</td>
<td>Swagger is a set of open-source tools built around the OpenAPI Specification. Swagger UI helps you to design and manage AsyncOS API resources on a web interface. For more information, see the &quot;Setup, Installation and Basic Configuration&quot; chapter of the user guide or online help.</td>
</tr>
<tr>
<td>Improving User Experience by Collecting Feature Usage Statistics</td>
<td>The Cisco Content Security Management appliance now collects feature/interface usage statistics on the new web interface of the appliance that helps Cisco improve overall user experience. All data collected is anonymized. If you want to opt-out of this feature, navigate to <strong>Management Appliance &gt; System Administration &gt; General Settings &gt; Usage Analytics</strong> page of the web interface to disable it. For more information, see section &quot;Monitoring Web Usage Analytics&quot; section in the user guide or online help.</td>
</tr>
<tr>
<td>Improving user experience by collecting web interface usage statistics of the appliance</td>
<td>The Cisco Content Security Management appliance can now collect the web interface usage statistics of the appliance using the Usage Analytics feature. This feature is used to collect and analyze the web interface usage data and provide insight to improve user experience of the appliance. For more information, see “Monitoring Web Usage Analytics” section in the user guide or online help.</td>
</tr>
</tbody>
</table>

## Changes in Behaviour

<table>
<thead>
<tr>
<th>Change Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changes in generating passphrase</td>
<td>After you upgrade to this release, you cannot choose to generate system passphrase on your appliance.</td>
</tr>
<tr>
<td>Downloading message attachment for Policy, Virus and Outbreak Quarantines</td>
<td>Prior to this release, message attachments detected and quarantined by the Policy, Virus and Outbreak Quarantines engine were displayed on the new browser window. After you upgrade to this release, you can download message attachments that are detected and quarantined by the Policy, Virus and Outbreak Quarantines engine.</td>
</tr>
</tbody>
</table>
# Comparison of Web Interfaces, New Web Interface vs. Legacy Web Interface

<table>
<thead>
<tr>
<th>Web Interface Page or Element</th>
<th>New Web Interface</th>
<th>Legacy Web Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Landing Page</td>
<td>After you log in to the Security Management appliance, the Mail Flow Summary page is displayed.</td>
<td>After you log in to the appliance, the System Status page is displayed.</td>
</tr>
<tr>
<td>Product Drop-down</td>
<td>You can switch between the Email Security Appliance and the Web Security Appliance from the Product drop-down.</td>
<td>You can use the Email or Web tab to switch between the Email Security Appliance and the Web Security Appliance.</td>
</tr>
<tr>
<td>Reports Drop-down</td>
<td>You can view reports for your Email and Web Security Appliances from the Reports drop-down.</td>
<td>You can view reports for your Email and Web Security Appliances from the Reporting drop-down menu.</td>
</tr>
<tr>
<td>Management Appliance Tab</td>
<td>Click  🐦 on the Security Management appliance to access the Management Appliance tab.</td>
<td>You can enable and configure reporting, message tracking and quarantines, as well as configure network access, and monitor system status.</td>
</tr>
<tr>
<td>My Reports Page</td>
<td>Select Email from the Product drop-down and choose My Reports from the Reports drop-down.</td>
<td>You can view the My Reports page from Email &gt; Reporting &gt; My Reports.</td>
</tr>
<tr>
<td>Reporting Data Availability Page</td>
<td>Click  🐦 on the Security Management appliance and choose Email &gt; Reporting &gt; Reporting Data Availability to access the Reporting Data Availability page.</td>
<td>You can view, update and sort data to provide real-time visibility into resource utilization and email traffic trouble spots.</td>
</tr>
<tr>
<td>Scheduling &amp; Archiving Reports</td>
<td>Click  🐦 on the Security Management appliance and choose Email &gt; Reporting &gt; Scheduled Reports to schedule your reports. Click  🐦 on the Security Management appliance and choose Email &gt; Reporting &gt; Archive Reports to archive your reports.</td>
<td>You can schedule reports using the Email &gt; Reporting &gt; Scheduled Reports page, and archive your reports using the Email &gt; Reporting &gt; Archived Report page of the Security Management appliance.</td>
</tr>
</tbody>
</table>
### Comparison of Web Interfaces, New Web Interface vs. Legacy Web Interface

<table>
<thead>
<tr>
<th>Web Interface Page or Element</th>
<th>New Web Interface</th>
<th>Legacy Web Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting Overview Page</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 quarantine and perform a message action. |
### Comparison of Web Interfaces, New Web Interface vs. Legacy Web Interface

<table>
<thead>
<tr>
<th>Web Interface Page or Element</th>
<th>New Web Interface</th>
<th>Legacy Web Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Download Limit for Attachments</td>
<td>The maximum limit for downloading attachments of a quarantined message is restricted to 25 MB.</td>
<td>-</td>
</tr>
<tr>
<td>Rejected Connections</td>
<td>To search for rejected connections, click <strong>Tracking &gt; Search &gt; Rejected Connection</strong> tab on the Security Management appliance.</td>
<td>-</td>
</tr>
<tr>
<td>Query Settings</td>
<td>The <strong>Query Settings</strong> field of the Message Tracking feature is not available on the Security Management appliance.</td>
<td>You can set the query timeout in the Query Settings field of the Message Tracking feature.</td>
</tr>
<tr>
<td>Message Tracking Data Availability</td>
<td>Click 📪 on the on the Security Management appliance and choose <strong>Email &gt; Message Tracking &gt; Message Tracking Data Availability</strong> to access Message Tracking Data Availability page.</td>
<td>You can view the missing-data intervals for your appliance.</td>
</tr>
<tr>
<td>Verdict Charts and Last State Verdicts</td>
<td>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.</td>
<td>Verdict Charts and Last State Verdicts of the messages are not available.</td>
</tr>
<tr>
<td>Message Attachments and Host Names in Message Details</td>
<td>Message attachments and host names are not displayed in the Message Details section of the message on the Security Management appliance.</td>
<td>Message attachments and host names are displayed in the Message Details section of the message.</td>
</tr>
<tr>
<td>Sender Groups, Sender IP, SBRS Score and Policy Match in Message Details</td>
<td>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.</td>
<td>Sender Groups, Sender IP, SBRS Score, and Policy Match details of the message is not available in the Message Details section of the message.</td>
</tr>
<tr>
<td>Direction of the Message (Incoming or Outgoing)</td>
<td>Direction of the messages (incoming or outgoing) is displayed in the message tracking results page on the Security Management appliance.</td>
<td>Direction of the messages (incoming or outgoing) is not displayed in the message tracking results page.</td>
</tr>
</tbody>
</table>
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 -
  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 12.5.0-658 - MD (Maintenance Deployment), page 8
- Upgrading to Release 12.5.0-655 - MD (Maintenance Deployment), page 9
- Upgrading to Release 12.5.0-643 - MD (Maintenance Deployment), page 9
- Upgrading to Release 12.5.0-636 - MD (Maintenance Deployment), page 9
- Upgrading to Release 12.5.0-633 - GD (General Deployment), page 9

**Upgrading to Release 12.5.0-658 - MD (Maintenance Deployment)**

You can upgrade to release 12.5.0-658 from the following versions:

- 11.0.1-161
- 11.4.0-823
- 11.5.1-121
- 12.0.0-478
- 12.0.1-011
- 12.0.2-001
- 12.5.0-613
- 12.5.0-633
- 12.5.0-636
- 12.5.0-655

**Note** This release is compatible with AsyncOS 12.5 for Cisco Email Security Appliances and AsyncOS 11.8 for Cisco Web Security Appliances.
Upgrading to Release 12.5.0-655 - MD (Maintenance Deployment)

You can upgrade to release 12.5.0-655 from the following versions:

- 11.1.0-065
- 11.1.0-088
- 12.0.0-478
- 12.5.0-633
- 12.5.0-636
- 12.5.0-648

Note
This release is compatible with AsyncOS 12.5 for Cisco Email Security Appliances and AsyncOS 11.8 for Cisco Web Security Appliances.

Upgrading to Release 12.5.0-643 - MD (Maintenance Deployment)

You can upgrade to release 12.5.0-643 from the following versions:

- 11.1.0-088
- 12.0.0-478

Note
This release is compatible with AsyncOS 12.5 for Cisco Email Security Appliances and AsyncOS 11.8 for Cisco Web Security Appliances.

Upgrading to Release 12.5.0-636 - MD (Maintenance Deployment)

You can upgrade to release 12.5.0-636 from the following versions:

- 11.4.0-823
- 12.5.0-633

Note
This release is compatible with AsyncOS 12.5 for Cisco Email Security Appliances and AsyncOS 11.8 for Cisco Web Security Appliances.

Upgrading to Release 12.5.0-633 - GD (General Deployment)

You can upgrade to release 12.5.0-633 from the following versions:

- 11.1.0-077
- 11.1.0-083
- 11.4.0-800
- 11.5.1-121
- 12.0.0-457
Compatibility with Email and Web Security Releases


Installation and Upgrade Notes

- Important Additional Reading, page 10
- Virtual Appliance, page 10
- Pre-Upgrade Requirements, page 11
- IPMI Messages During Upgrade, page 11
- Upgrading to This Release, page 12

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


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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set up your virtual appliance using the documentation described in Virtual Appliance, page 10.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Upgrade your physical appliance to this AsyncOS release.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Save the configuration file from your upgraded physical appliance</td>
</tr>
<tr>
<td>Step 4</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 11
- Back Up Your Existing Configuration, 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 10.

**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 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.
Supported Hardware for this Release

All virtual appliance models.

- The following hardware models - M190, M195, M380, M390, M395, M680, M690, and M695.

To determine whether your appliance is supported, and to remedy the situation if it is not currently compatible, see


The following hardware is NOT supported for this release:

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

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

|----------------------|--------------------------------------------------------------------------------------------------|

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.

<table>
<thead>
<tr>
<th>Documentation For Cisco Content Security Products:</th>
<th>Is Located At:</th>
</tr>
</thead>
</table>

Service and Support

Note  To get support for virtual appliances, call Cisco TAC and have your Virtual License Number (VLN) number ready.


For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.