Release Notes for AsyncOS 8.2 for Cisco Content Security Management

First Published: February 14, 2014
Last Updated: February 26, 2014

Contents

• What’s New in This Release, page 2
• Upgrade Paths, page 3
• Security Management Compatibility Matrix, page 3
• Important Notes, page 3
• Installation and Upgrade Notes, page 4
• Finding Current Information about Known and Fixed Issues, page 7
• Related Documentation, page 7
• Service and Support, page 8
## What’s New in This Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Features:</strong></td>
<td></td>
</tr>
<tr>
<td>Support for AsyncOS 8.0 for Web</td>
<td>A new Configuration Master 8.0 replaces the old Configuration Master 7.1. It supports new features in AsyncOS 8.0 for Web Security appliances.</td>
</tr>
<tr>
<td>Support for IPv6 addresses in reporting, web tracking, and Configuration Masters</td>
<td>Transactions that involve servers that have IPv6 addresses are reflected in reporting and web tracking. Settings on the Web Security appliance that support IPv6 are also configurable with IPv6 when using Configuration Master 8.0. For information about these settings, see the Web Security documentation.</td>
</tr>
<tr>
<td>Identities support Kerberos authentication scheme</td>
<td>Identities in Configuration Master 8.0 support the Kerberos authentication scheme for publishing to Web Security appliances running AsyncOS 8.0. For essential information, see the &quot;Before You Publish a Configuration Master&quot; topic in the User Guide or Online Help for this release.</td>
</tr>
</tbody>
</table>
| Ability to reorder identities and policies by dragging and dropping them | You can now reorder identities and certain policies in Configuration Master 8.0 by dragging and dropping them. This applies to the following policies:  
  - Identities  
  - Decryption Policies  
  - Routing Policies  
  - Access Policies  
  - Data Security Policies  
  - External DLP Policies  
  - Outbound Malware Scanning Policies  
  - SOCKS Policies |
| Web Tracking enhancement | You can now click to expand individual URLs in Web Tracking search results to view more details for an individual transaction. |
Upgrade Paths

You can upgrade to release 8.2.0-238 of AsyncOS for Cisco Content Security Management from the following versions:

<table>
<thead>
<tr>
<th>Release 7.9.0</th>
<th>Release 7.9.1</th>
<th>Release 8.0</th>
<th>Release 8.1.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.9.0-107</td>
<td>7.9.1-030</td>
<td>8.0.0-402</td>
<td>8.1.0-428</td>
</tr>
<tr>
<td>7.9.0-110</td>
<td>7.9.1-040</td>
<td>8.0.0-404</td>
<td>8.1.0-476</td>
</tr>
<tr>
<td>7.9.0-201</td>
<td>7.9.1-102</td>
<td>8.0.0-710</td>
<td>8.1.1-013</td>
</tr>
<tr>
<td>7.9.0-302</td>
<td>7.9.1-110</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security Management Compatibility Matrix


Important Notes

- Sign Up to Receive Important Notifications, page 3
- SNMP, page 3

Sign Up to Receive Important Notifications

Sign up to receive notifications such as Security Advisories, Field Notices, End of Sale and End of Support announcements, and information about software updates and known issues.

You can specify options such as notification frequency and types of information to receive. You should sign up separately for notifications for each product that you use.

To sign up, visit the Cisco Notification Service page at http://www.cisco.com/cisco/support/notifications.html

A Cisco.com account is required. If you do not have one, visit https://tools.cisco.com/RPF/register/register.do.

Note

This service replaces any previous email announcement service. You must sign up with the Cisco Notification Service to receive future announcements.

SNMP

When setting up SNMP to monitor connectivity:
When entering the url-attribute while configuring a connectivityFailure SNMP trap, determine whether the URL is pointing at a directory or a file.

- If it is a directory, add a trailing slash (/)
- If it is a file, do not add a trailing slash

# Installation and Upgrade Notes

- Additional Reading, page 4
- Supported Browsers, page 4
- Preupgrade Requirements, page 4
- Upgrading to This Release, page 6
- Requirements After Upgrade, page 6

## Additional Reading

You should also review the release notes for:

- Your associated Email and Web security releases.
- Earlier releases of AsyncOS for Security Management, if you are upgrading from a release earlier than the immediate previous release.

For links to this information, see Related Documentation, page 7.

## Supported Browsers

Supported browsers are listed in the “Browser Requirements” section in the “Setup, Installation, and Basic Configuration” chapter of the user guide for your release.

## Preupgrade Requirements

Perform the following important preupgrade tasks:

- Change the Protocol for Users and Log Subscriptions Configured to Use SSH 1, page 4
- Preserve Configuration Master 7.1 Settings, page 5
- Preserve Pre-Upgrade Data from the System Capacity Report, page 5
- Verify Associated Email and Web Security Appliance Versions, page 5
- Disk Space Reductions, page 5
- Back Up Your Existing Configuration, page 6

## Change the Protocol for Users and Log Subscriptions Configured to Use SSH 1

This section applies if you are upgrading from a release earlier than AsyncOS 8.0 for Content Security Management:
Support for SSH 1 has been removed starting in AsyncOS release 8.0. Therefore, before upgrade, you should do the following:

- Any remote host keys which use SSH 1 should be changed to SSH 2. Use the `logconfig > hostkeyconfig` command in the CLI to make this change.
- For any log subscriptions that are configured to use SSH 1 as the protocol for SCP log push, choose SSH 2 instead.
- Change the access protocol or add a new SSH 2 key for any users configured to use only SSH 1. Use the `sshconfig` command in the CLI to make this change.
- Disable SSH 1 using the `sshconfig > setup` command in the CLI.

**Preserve Configuration Master 7.1 Settings**

Configuration Master 7.1 is not supported in this release and will be removed during upgrade. If you wish to preserve the settings in Configuration Master 7.1: If applicable, copy your 7.5 configuration into Configuration Master 7.7, then copy your 7.1 configuration into Configuration Master 7.5.

Any Web Security appliances assigned to Configuration Master 7.1 at upgrade will not be assigned to any Configuration Master after upgrade.

**Preserve Pre-Upgrade Data from the System Capacity Report**

This section applies if you are upgrading from a release earlier than AsyncOS 8.0 for Content Security Management.

Beginning in AsyncOS release 8.0 for Cisco Content Security Management, changes have been made to the CPU Usage by Function chart in the System Capacity report.

Specifically, Web Reputation and Web Categorization data in this chart have been combined into a single measure called "Acceptable Use and Reputation." As a result, CPU usage data for “Acceptable Use and Reputation” may not be valid for time ranges that include dates before the upgrade.

If you want to preserve pre-upgrade CPU usage data for Web Reputation and Web Categorization, export or save the data for the CPU Usage by Function chart as CSV or PDF before you upgrade.

**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 Security Management Compatibility Matrix, page 3.

**Disk Space Reductions**

As a result of changes in disk space allocation, the maximum disk space available in this release may have changed from previous releases. Depending on your hardware and the AsyncOS version that you are upgrading from, the maximum disk space available may have increased or decreased. A decrease in available disk space may result in loss of the oldest data after upgrade, based on the amount of data on the appliance that exceeds the new maximum limit.

See Table 1-1 to determine the change that applies to your deployment.
### 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.

### Upgrading to This Release

1. **Step 1** Address all topics described in Preupgrade Requirements, page 4.
2. **Step 2** Follow all instructions in the “Before You Upgrade: Important Steps” section in the user guide PDF for THIS release.
3. **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.
4. **Step 4** After about 10 minutes, access the appliance again and log in.
5. **Step 5** Follow instructions in the “After Upgrading” section of the user guide PDF for THIS release.
6. **Step 6** Perform all tasks in Requirements After Upgrade, page 6.

### Requirements After Upgrade

#### Reallocate Disk Space

After upgrade, available disk space may have changed (see Disk Space Reductions, page 5.) However, the disk space allocations that existed before upgrade have not been changed. To allocate new amounts that fit the current disk space, go to Management Appliance > System Administration > Disk Management.

Until you do this, you will not be able to load configuration files that you have saved from the appliance.

---

### Table 1-1 Maximum Disk Space Available for Different AsyncOS Releases and Hardware, in GB

<table>
<thead>
<tr>
<th>Disk Space Available (GB)</th>
<th>Hardware Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>AsyncOS Version</td>
<td>M160</td>
</tr>
<tr>
<td>8.x</td>
<td>165</td>
</tr>
<tr>
<td>7.9</td>
<td>165</td>
</tr>
<tr>
<td>7.8</td>
<td>180</td>
</tr>
</tbody>
</table>
Finding Current Information about Known and Fixed Issues

Use the Cisco Bug Search Tool to find the most current information about known and fixed defects in shipping releases.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Go to https://tools.cisco.com/bugsearch/.
| 2    | Log in with your Cisco account credentials.
| 3    | Enter search criteria. 

For example, to find all issues fixed in a release:

a. Click Select from list, then navigate to and select your product:
   - Cisco Email Security Appliance
   - Cisco Web Security Appliance
   - Cisco Content Security Management Appliance

b. For Releases, enter the AsyncOS release number, such as 8.1.1.

c. For Show Bugs, select Fixed in this release.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4    | 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

The documentation set for Cisco content security products includes the following major documents and books (not all types are applicable to or available for all products and releases):

- Release Notes
- Quick Start Guides
- Hardware and virtual appliance installation guides
- User Guides (for administrators)
- Command-line interface (CLI) reference guide

This and other documentation is available at the following locations:
Service and Support

You can also access customer support from the appliance. For instructions, see the User Guide or online help.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.