Release Notes for AsyncOS 9.2.x for Cisco Web Security Appliances

Published: January 27, 2016
Revised: August 31, 2016

Contents

- What’s New, page 1
- About Policy Application from Cloud Web Security, page 2
- WSA Functionality Not Available in Hybrid Mode, page 3
- Release Classification, page 3
- Supported Hardware for This Release, page 3
- Upgrade Paths, page 4
- Known and Fixed Issues, page 5
- Related Documentation, page 7
- Support, page 7

What’s New

- What’s New in Cisco AsyncOS 9.2, page 1

What’s New in Cisco AsyncOS 9.2

Note
This release is intended primarily for installing Hybrid Web Security on a device that has never been configured. Do not install or upgrade to this version unless you plan to operate the appliance in Hybrid mode.
• What’s New in Cisco AsyncOS 9.2.0-809 (GD), page 2
• What’s New in Cisco AsyncOS 9.2.0-796, page 2
• What’s New in Cisco AsyncOS 9.2.0-083 (GD), page 2
• What’s New in Cisco AsyncOS 9.2.0-075, page 2

What’s New in Cisco AsyncOS 9.2.0-809 (GD)

This is an upgrade release; no new features were added.

What’s New in Cisco AsyncOS 9.2.0-796

• Translation of both default and user-defined CWS policies to WSA policies has been expanded and optimized; very few CWS rules are not converted.
• Upgrades to the AsyncOS software are now downloaded automatically whenever available. Downloaded upgrades are then installed during the Time Windows specified on the Upgrade and Update Settings page.

What’s New in Cisco AsyncOS 9.2.0-083 (GD)

This is an upgrade release; no new features were added.

What’s New in Cisco AsyncOS 9.2.0-075

Hybrid Web Security mode provides unified cloud and on-premise policy enforcement and threat defense, using policies defined in Cisco ScanCenter—the administrative portal to Cloud Web Security—which are automatically downloaded to the Web Security appliance.

About Policy Application from Cloud Web Security

Please note these points regarding download, conversion and application of CWS policies/filters/rules to WSA policies:
• Translation of both default and user-defined CWS policies to WSA policies is not a one-to-one conversion; however, the action that results from application of a particular policy in both environments is the same. In other words, the Block or Allow decision is always consistent, regardless of the sequence of rules “fired” in both cases. This allows rule evaluation in the proxy to be optimized for better performance without compromising consistent behavior.
• Supported anti-malware scanning services are not the same on both platforms; they will remain independent. The WSA provides an option to choose scanning services, and at least one must be enabled.
• In Hybrid mode, the WSA does not support the following items; these will not be downloaded:
  – Any rule assigned the Authenticate or Warn action. (Warn was supported in an earlier version of Hybrid mode for URL categories; this is no longer the case.)
  – Outbound filters. Any rule using a filter that contains any Keyword, Outbound File Type, Preconfigured ID, or Regular Expression. Inbound Extensions are also not supported.
WSA Functionality Not Available in Hybrid Mode

The following WSA features are not available in Hybrid mode:

- Time and Volume Quotas
- External DLP
- SaaS Policies
- L4TM
- Upstream Proxy support
- ISE integration
- Range Requests
- Native FTP & SOCKS protocol support
- SNMP
- HTTPS rules assigned the Drop action

Release Classification

Each release is identified by the release type (ED - Early Deployment, GD - General Deployment, etc.) For an explanation of these terms, see http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdf.

Supported Hardware for This Release

This release supports these virtual appliances on KVM and ESXi 5.0:

- S000v
- S100v
- S300v

This release supports the following hardware models:

- S170
- S370
- S670
- S380
- S680
Upgrade Paths

Before you start the upgrade process, see Related Documentation, page 7.

- Upgrading to AsyncOS 9.2.0-809 (GD), page 4
- Upgrading to AsyncOS 9.2.0-796 (Beta), page 4
- Upgrading to AsyncOS 9.2.0-083 (GD), page 4
- Upgrading to AsyncOS 9.2.0-075 (ED), page 5

Upgrading to AsyncOS 9.2.0-809 (GD)

You can upgrade to release 9.2.0-809 for AsyncOS for Cisco Web Security appliances from the following versions:

- 9.0.0-485
- 9.0.1-162
- 9.2.0-070
- 9.2.0-075
- 9.2.0-083
- 9.2.0-070
- 9.2.0-795
- 9.2.0-796

Note

If you are upgrading from an earlier version, you may encounter a “400 Bad Request” error (bug CSCva83169). Perform a WSA configuration reset via the UI or CLI and attempt registration again.

Upgrading to AsyncOS 9.2.0-796 (Beta)

You can upgrade to release 9.2.0-796 for AsyncOS for Cisco Web Security appliances from the following version:

- 9.2.0-083

Upgrading to AsyncOS 9.2.0-083 (GD)

You can upgrade to release 9.2.0-083 for AsyncOS for Cisco Web Security appliances from the following versions:

Some hardware models require a memory upgrade before you can install or upgrade to this AsyncOS release. For more information, see
Upgrading to AsyncOS 9.2.0-075 (ED)

You can upgrade to release 9.2.0-075 for AsyncOS for Cisco Web Security appliances from the following versions:

- 8.5.0-497
- 9.0.0-485
- 9.2.0-070
- 9.2.0-075

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 5
- Lists of Known and Fixed Issues, page 5
- Finding Information about Known and Resolved Issues, page 6

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.

Lists of Known and Fixed Issues

- Known and Fixed Issues in Release 9.2.0-809 (GD), page 5
- Known and Fixed Issues in Release 9.2.0-796 (Beta), page 6
- Known and Fixed Issues in Release 9.2.0-083 (GD), page 6
- Known and Fixed Issues in Release 9.2.0-075 (ED), page 6

Known and Fixed Issues in Release 9.2.0-809 (GD)

<table>
<thead>
<tr>
<th>Fixed Issues</th>
<th>Known Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Link]</td>
<td>[Link]</td>
</tr>
</tbody>
</table>
Known and Fixed Issues in Release 9.2.0-796 (Beta)

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

Known and Fixed Issues in Release 9.2.0-083 (GD)

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

Known and Fixed Issues in Release 9.2.0-075 (ED)

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

Finding Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find the most current information about known and resolved 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>
<tbody>
<tr>
<td>Step 1</td>
<td>Go to <a href="https://tools.cisco.com/bugsearch/">https://tools.cisco.com/bugsearch/</a>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log in with your Cisco account credentials.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Select from list &gt; Security &gt; Web Security &gt; Cisco Web Security Appliance, and click OK.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In Releases field, enter the version of the release, for example, 8.8.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Depending on your requirements, do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• To view the list of resolved issues, select Fixed in these Releases from the Show Bugs drop down.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
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


### Support

#### Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco users.


#### Customer Support

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.

---

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](http://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.

© 2016 Cisco Systems, Inc. All rights reserved.