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

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

Contents

What's New

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.

Cisco Systems, Inc.
www.cisco.com

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.

  - Whitelisting sets of domains and URLS to bypass Sypware/Web Reputation scanning at the global level is not supported.
  - Anonymize. Any CWS rule that has the action set to Anonymize.
  - SearchAhead
  - WSA does not incorporate the concept of delegated administration. CWS will send the merged policy configuration.

WSA Functionality Not Available in Hybrid Mode

The following WSA features are not available in Hybrid mode:

- Time and Volume Quotas
- External DLP
- SaaS Polices
- 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 ESXiv5.0:

- S000v
- S100v
- S300v

This release supports the following hardware models:

- S170
- S370
- S670
- S380
- S680

Some hardware models require a memory upgrade before you can install or upgrade to this AsyncOS release. For more information, see http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html

Upgrade Paths

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

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:

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

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

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

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)

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.2.0-809&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.2.0&sb=anfr&sts=open&bt=custV

Known and Fixed Issues in Release 9.2.0-796 (Beta)

Fixed Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.2.0-796&sb=fr&svr=3nH&bt=custV
Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.2.0&sb=anfr&sts=open&bt=custV

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

Fixed Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.2.0-083&sb=fr&svr=3nH&bt=custV
Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.2.0&sb=anfr&sts=open&bt=custV

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

Fixed Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.2.0-075&sb=fr&svr=3nH&bt=custV
Known Issues	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=9.2.0&sb=afr&sts=open&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 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

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 > Web Security > Cisco Web Security Appliance**, and click **OK**.

Step 4 In Releases field, enter the version of the release, for example, 8.8.

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

Documentation for this product is available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html.

Documentation for Cisco Cloud Web Security is available from http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html.

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.

Access the Cisco Support Community for web security and associated management:

https://supportforums.cisco.com/community/5786/web-security

Customer Support

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

Cisco TAC: Visit 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.