Release Notes for AsyncOS 15.5 Hot Patch 1 for Cisco Secure Web Appliances

First Published: 2026-05-26

About Secure Web Appliance

The Cisco Secure Web Appliance intercepts and monitors internet traffic and applies policies to help keep your internal network secure from malware, sensitive data loss, productivity loss, and other internet-based threats. It acts as a proxy server, intercepting web requests from users and scanning the requested web content for potential threats such as malware, viruses, and phishing attempts. Cisco Secure Web Appliance uses various security technologies such as URL filtering, antivirus scanning, reputation-based filtering, and advanced malware protection to ensure the security of web traffic.

Build Number and Release Date

Build Number: 15.5.0-816

Release Date: May 27, 2026

New Features in AsyncOS 15.5.0-816

The following features are introduced for this release:

Feature	Description
Talos URS	Talos URS (URL Rating Service) is a URL categorization service fully integrated into the Cisco Secure Web Appliance (SWA). When the Beaker web reputation engine encounters a URL that is not yet categorized during web traffic inspection, it forwards the query to Talos URS for classification. If Talos URS has the URL pre-classified in its cache, it immediately returns the category and score to the proxy, which then enforces the configured policies accordingly. If the URL is not found in the Talos URS cache, the uncategorized domains are uploaded to the Service Request (SR). In the backend, outside of the SWA, these domains are categorized using Talos intelligence and subsequently delivered to the SWA through notification updates. The Cisco Secure Web Appliance (SWA) retrieves the latest notification update during its next scheduled update cycle. Following this update, URLs that were previously uncategorized are categorized and subject to policy enforcement. This integration ensures timely and accurate URL categorization to support effective web filtering and security policy application within the Cisco Secure Web Appliance environment. New/modified commands: **talosursconfig** **Note** Changes made through the **talosursconfig** CLI command take effect immediately without requiring an explicit commit. However, these changes do not persist through or after a software upgrade of the Secure Web Appliance (SWA). You must reapply any desired configuration changes using **talosursconfig** after the appliance has completed the upgrade and is back online.

Changes in Behavior in AsyncOS 15.5.1-816

- **Route Configuration Engine Update**–The interface and route configuration architecture has been refactored to support an idempotent reconciliation engine utilizing PF_ROUTE sockets, providing an alternative to the legacy flush-and-rebuild method. The legacy flush-and-rebuild approach remains the default configuration. To transition to the new PF_ROUTE socket-based engine, use the **diagnostic** > **routeengine** command. Changes made via this command take effect immediately and do not require an explicit commit.

  This configuration is not retained across software upgrades. If you choose to use the new engine, you must reapply the **diagnostic** > **routeengine** command following any software upgrade of the SWA.

Upgrade Paths



Note Before upgrading to this release, save copy of the appliance configuration file to a location other than the appliance.

You can upgrade to the 15.5.0-816 HP1 release from the following versions:

- 15.5.0-710
- 15.0.1-004

Known and Fixed Issues

Log in to the Cisco Bug Search Tool using your Cisco account credentials to view the list of fixed bugs.

- Fixed Issues
- Known Issues

Related Documentation

Documentation	Location
Cisco Secure Web Appliance User Guide	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Content Security Management Appliance User Guide	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
Virtual Appliance Installation Guide	https://www.cisco.com/c/en/us/support/security/email-securityappliance/products-installation-guides-list.html
Compatibility Matrix for Cisco Secure Email and Web Manager with Secure Web Appliance	https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/web-compatibility/index.html
API Guide	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-programming-reference-guides-list.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. Have your Virtual License Number (VLN) number ready before you call TAC.

Cisco TAC:

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html.

Support site for legacy IronPort:

http://www.cisco.com/web/services/acquisitions/ironport.html.

For noncritical issues, you can also access customer support from the appliance. For instructions, see the Troubleshooting section of the Secure Web Appliance User Guide.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

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.

© 2026 Cisco Systems, Inc. All rights reserved.