Release Notes for AsyncOS 16.0 for Cisco Secure Web Appliance

First Published: 2026-06-09

Last Modified: 2026-09-16

What's New

- What's New in AsyncOS 16.0.0-399 (General Deployment), on page 2
- What's New in AsyncOS 16.0.0-359 (Limited Deployment), on page 3
- Changes in Behavior in AsyncOS 16.0.0-399 (General Deployment), on page 4
- Known Behavior, on page 5
- Known Limitations, on page 7

What's New in AsyncOS 16.0.0-399 (General Deployment)

Feature	Description
Health Check APIs	AsyncOS 16.0 introduces REST APIs for performing health checks on key appliance services, network connectivity, and system resources. These APIs enable administrators to programmatically retrieve health information and troubleshoot connectivity and system-related issues. The following health check APIs are available: • **External DLP Health Check**—Tests ICAP connectivity to configured External DLP servers and provides connection status and response-time information. • **Network Interface Health Check**— Tests IPv4 and IPv6 gateway reachability for configured network interfaces and provides packet-loss and round-trip-time information. • **NTP Health Check**—Reports the health of the NTP service, including process and readiness status, recent service start information, time adjustments, and error or warning messages. • **DNS Lookup Health Check**—Tests configured DNS servers by performing forward and reverse DNS lookups and reports DNS resolution and server responsiveness. • **System Health Check**—Provides appliance health and resource metrics, including RAM and disk utilization, proxy CPU usage, disk usage, RAID status, proxy bandwidth, and proxy connection information. You can retrieve information for all applicable components or, where supported, query a specific server, network interface, or system metric. These APIs can be used for automated health monitoring and troubleshooting of the appliance. For more information, see AsyncOS API 16.0 for Cisco Secure Web Appliance–Getting Started Guide The health check APIs are supported only with the **REST API v3.0** endpoint.

What's New in AsyncOS 16.0.0-359 (Limited Deployment)

Feature	Description
Single Sign-On using SAML	The Secure Web Appliance now supports Single Sign-On (SSO) using SAML. This enables users to log in to the appliance's web interface with the same credentials they use for other SAML SSO-enabled services within their organization. By configuring the appliance as a SAML Service Provider (SP) and integrating with a SAML Identity Provider (IdP) such as Microsoft ADFS, users can authenticate once and gain seamless access to all authorized services without repeated logins. **Note** This feature is unsupported in the Secure Web Appliance NGUI. NGUI access is unavailable after SSO login. **New/Modified Screens**: **Network** > **SSO**, **System Administration** > **Users** > **External Authentication**
Configuration Audit Logs	The Configuration Audit log is a monitoring page designed to track and log all configuration changes made to the Secure Web Appliance throughout its lifecycle. Previously, there was no dedicated page to monitor these changes, making it difficult to track modifications. **New/Modified Screens**: **Reporting** > **Configuration Audit**
KyberKEM (Post-Quantum Cryptography)	KyberKEM is integrated into the Secure Web Appliance as a Post-Quantum Cryptography (PQC) feature to secure communications against future quantum computing threats. Its primary purpose is to establish a shared secret between two communicating parties while remaining resistant to attackers within the transmission system. **Note** • By default the feature is disbaled. • KyberKEM is only supported on TLS version 1.3. • CiscoSSL_PQC 3.3.3.8.3.39 based on OpenSSL 3.3.3 library is introduced for this feature. **New/Modified CLI**: `wsa` > `advancedproxyconfig` > `HTTPS`

Feature	Description
Generative AI Visibility and Control for ADC	Secure Web Appliance now provides enhanced visibility and granular control over Generative AI applications through the Applications Discovery and Control (ADC) engine. This update addresses the security risks associated with Shadow IT and potential data leakage by expanding the ADC database from 4 to over 1,200 Generative AI applications, including tools such as ChatGPT, Claude, Midjourney, and GitHub Copilot. By integrating with Cisco's Cloud App Security Intelligence (CASI), administrators can now accurately identify, monitor, and apply access policies to a wide range of AI-powered content creation, coding, and productivity tools.

Changes in Behavior in AsyncOS 16.0.0-399 (General Deployment)

- **Real-time monitoring of access and PACD logs when syslog push is enabled**—When syslog push is configured, access log (`.c`) and PACD log (`.log`) files are created on the Secure Web Appliance. You can use the `tail` command to monitor these log files in real time.
- **Increased maximum number of retained log files**—When SCP, FTP, or syslog push is configured, you can now configure the maximum number of retained log files up to 999.

  Previously, the default maximum number of retained files was 100 for SCP and FTP, and this value could not be customized for syslog push.
- **Increased syslog buffer limit**—The upper limit of the syslog buffer has been increased from 512 KB to a larger, model-specific capacity measured in GB.
- **Maximum number of files available as a separate Field**—The **Maximum Number of Files** option is now available as a separate field for all the logs. You can use this field to configure number of files to be rotated.

  Previously, this option was available only when **FTP** or **None** was selected as the log retrieval method.
- **Log Rollover and file settings available with syslog push**—When syslog push is enabled, you can now customize the **Rollover by File Size**, **Rollover by Time**, **Log Compression**, and **File Name** settings for all log types.

  Previously, these settings were disabled when syslog push was enabled.
- **PACD and access log processes restart after manual log rollover**—When you perform a manual log rollover, the PACD and access log processes restart automatically.
- **Changes to log file naming and rotation**—The `.c`, `.s`, and `.current` log files are no longer used for PACD logs. The current log is stored in a `.log` file.

  For size-based rollover, rotated log files use the `.log.1`, `.log.2`, and subsequent naming convention. For time-based rollover, rotated log files use the `.log.<timestamp>` naming convention.
- **Log file retention when SCP or FTP push is enabled**—When SCP or FTP push is enabled, log files are not retained on the appliance. Only one rotated log file, `.log.1`, is retained for transfer.

  If there is no interruption to the `swa_logd` process, subsequent log files are not retained after transfer.

- **Begin and End log file messages removed**—The Begin log file and End log file messages are no longer included in the PACD logs.
- **Time-based Log Rollover occurs after a new log message**—When time-based rollover is configured, the log file does not rotate immediately after the configured time interval is reached. The rollover occurs when a new log message is received after the configured interval.

Known Behavior

The following are known behaviors of this release:

PACD Configuration Resets After Upgrade When FIPS Is Enabled with CSP—When FIPS is enabled with CSP, upgrading the appliance resets the PACD configuration to the default values in the backend. However, the existing PACD settings continue to appear correctly in the web interface. To synchronize and retain the existing PACD settings in the backend, modify any PACD logging configuration in the web interface and commit the changes.

Secure Web Appliance AVC or ADC Engine known behavior—When an application is configured to be blocked under ADC/AVC, every sub-category under the application will also be blocked. A specific sub-category can be blocked using fine and gain control feature, however this feature is limited to certain apps like smugmug, facebook, linkedin, etc.

Secure Web Appliance integration with Umbrella - Hybrid Policies known behavior

- By default, the source interface in Secure Web Appliance Umbrella settings is set to **Management**. Changing the source interface to **Data** requires you to submit and commit the changes before enabling Hybrid Policy.
- Hybrid policies support translation for rule actions **Allow**, **Block**, and **Warn**.
- There is support for translation of **Content Categories**, **Destination Lists**, and **Applications**.
- The translation of AD Users, AD Groups, and internal networks that are associated with public networks is supported.
- In Secure Web Appliance, one Global Umbrella pushed identification profile will always be available.
- Policies that are configured by Secure Web Appliance administrator are prioritized following the policy push from Umbrella.
- When policy push is enabled in the registered appliance page, policies configured in the Umbrella are pushed to all Secure Web Appliances registered under Umbrella.
- The WBRS are disabled for Decryption Policies pushed by Umbrella.
- The decryption policies pushed by Umbrella are set to Decrypt action by default.
- The End-User Notification page will always be enabled in Secure Web Appliance as a global setting.
- In Secure Web Appliance, the End-User Notification page is configured only for the block page first selected in first ruleset of Umbrella.
- Changes in the selected block page appearance of the first ruleset will be translated every three hours.
- In the case of Umbrella pushed identification profiles and customer categories, admin configured policies will be disabled from the Secure Web Appliance side if these profiles or categories are deleted from the Umbrella.

- Secure Web Appliance registration with Umbrella ORG is limited to the number of seats assigned to a specific ORG, which can be seen in the following path of the Umbrella user interface: **Admin** > **Licensing** > **Number of seats**.
- SMA policies cannot be pushed to Secure Web Appliance when it is registered with Umbrella ORG.
- Umbrella cannot push profiles, policies, and custom URL categories to Secure Web Appliance if there is no internal network and AD integrated in Umbrella.
- If API keys that were used for registration and enabling hybrid service are expired, the connection will not be closed until you enable hybrid policy or registered Secure Web Appliance with Umbrella again.
- The following Umbrella Rules configuration are not supported for hybrid policy push: Rules Scheduling and Protected Bypass.
- The SMA policies pushed to Secure Web Appliance are not accepted if the Secure Web Appliance is managed by Umbrella.
- The Save and Load configuration feature will not work for Umbrella settings.
- Translation is not supported for the following Ruleset settings:
    - Ruleset Identities - Chromebooks, G Suite OUs, G Suite Users, Tunnels, Roaming Computers, Internal Networks All Tunnels
    - Tenant Controls
    - File Analysis
    - File Type Control
    - HTTPS Inspection - only applications in Selective Decryption list
    - PAC File
    - SafeSearch
    - Ruleset Logging
    - SAML
    - Security Settings
- The changes made to the HTTPS proxy or AD realm on the Secure Web Appliance does not affect the umbrella policy.
- Application Settings (CASI) Translation
    - Application Settings selected in Rules are translated and pushed to Secure Web Appliance's Access Policy only when ADC is enabled under **Security Services** > **Acceptable Use Control** in Secure Web Appliance.
    - When the Application is selected in the Rule, a Custom URL category containing the domains of the selected application will be pushed to that Rule. This same category of Custom URLs is selected under the URL Filtering section of the Access Policy, with **Monitor** as the action.
    - The application available in Secure Web Appliance but not in Umbrella inherits the global settings action. The application available in Umbrella but not in Secure Web Appliance are ignored.
    - In Secure Web Appliance, applications that are not selected within Rules inherit the global settings.

- Selective Policy Psuh
  - Umbrella web policies are pushed to registered Secure Web Appliances only if the Hybrid Policy state is **Active** and Policy Push is enabled.
- Umbrella UI Error Message
  - The error message for the last policy push failure can be seen on the **Registered Appliance** page, which has a maximum character limit of 1024.
- Cleanup of Umbrella Pushed Policies
  - After the Umbrella pushed policies are cleaned up, all admin configured policies will be disabled.

Secure Web Appliance integration with Umbrella - Hybrid Reporting known behavior

- The hybrid reporting feature of Secure Web Appliance can only be enabled if a hybrid policy is enabled.
- The Secure Web Appliance sends Umbrella configured policies reporting data to the Umbrella dashboard.
- Approximately 25% of the local reporting disk space is used to store hybrid reporting data, which is then pushed to Umbrella.
- When Secure Web Appliance does not push the reporting data to Umbrella, it stores only those reporting data on disk for later debugging.
- The Secure Web Appliance continues to send reporting data evaluated by Umbrella policies, even after selective policy push is disabled for that SWA. The Umbrella policy reporting dashboard may display deleted rules for those records if the rule has been deleted from the Umbrella policy.

Known Limitations

The following are known limitations of this release:

Log file configuration:

- You cannot configure both size-based and time-based rollover for the same log file. If both rollover options are configured, time-based rollover takes precedence.
- When you reduce the **Maximum Number of Files** value, existing log files that exceed the newly configured limit are not automatically deleted. The files remain in the existing log file path.

Sophos engine known limitation—Sophos cannot scan a file which is multi-encoded with Deflate/Brotli encoding types. Sophos displays a SAVI_CORRUPT error and the file gets blocked by default

MIME type library—The MIME type library is now upgraded from 5.11 to 5.39 and the MIME type for certain file types are changed. As a result of this, there might be a change in behaviour to the allowed/blocked MIME types in SWA. You can modify the MIME type with respect to the latest library to avoid the behaviour change.

Secure Web Appliance integration with Umbrella - Hybrid Policies known Limitations

- The following scenarios do not trigger policy translation:
  - Change in the name of the Ruleset.
  - Change in the name of the destination list selected in the Rule.

  - Change in the name of the application list selected in the Rule.
  - Change in name of the selective decryption list selected during HTTP inspection.
  - Adding or removing categories from the selective decryption list used for HTTPS inspection.
  - A selective decryption list containing only categories is selected in the HTTPs inspection.
  - Adding or removing AD users or groups from a Ruleset or a Rule.
  - Integrating or removing AD from the Umbrella dashboard.

- When Ruleset identities are the same in multiple Rulesets, only the first Ruleset of the same identity will translate HTTPS inspection settings consistently.
- The format for the Redirect to Custom URL textbox for end-user notification supports only well-formned hostnames or IPV4 addresses. If we push other URL formats configured in the block page of Umbrella to Secure Web Appliance, the policy push fails with the error message stating: '*An http/https URL must consist of a well-formed hostname or IPv4 address, may optionally include a port, but may not contain a querystring ('?...').'", 'code': '400', 'explanation': '400 = Bad request syntax or unsupported method*.'
- In the case where AD groups are selected in rulesets but rules do not match, the access policy will not be created for that rule.
- The categories and domains selected in the Selective Decryption List are set to passthrough for decryption policies that are pushed from Umbrella to Secure Web Appliance. For predefined and custom URL categories, no access policy will be applied in Secure Web Appliance, but rules will be applied to the same configuration in Umbrella.
- If Microsoft 365 compatibility is enabled in Umbrella, decryption policies that are pushed from Umbrella to Secure Web Appliance are set to passthrough. As a result, passthrough will be enabled for all categories of Microsoft 365 endpoints.
- When a trusted AD is not configured in Secure Web Appliance but a group is selected for this AD at the Umbrella level, an error message appears indicating that it needs to be configured at the Secure Web Appliance level.
- If networks with different masks are selected in Ruleset and Rule, translation is not supported.
- When a large number of applications are selected across Rules, Secure Web Appliance performance is affected.
- To avoid redundant configuration, we recommend using application list rather than selecting individual application in Rules.

Secure Web Appliance integration with Umbrella - Hybrid Reporting known Limitations

- If the user is not included in Umbrella policies, the mapping of AD User to Umbrella origin ID is not possible. Events of this type will be identified by Secure Web Appliance's origin ID.
- Filtering support
  - Only external IP addresses are supported by Secure Web Appliance based filtering.
  - Secure Web Appliances from the same Org (different locations) having the same management IP address will result in combined reporting data.

    - For LDAP/ISE/Guest-based identities, Secure Web Appliance AD user-based identities are not supported.

- In some cases, the system may see duplicates or lost reporting entries.
- Upon enabling or disabling hybrid reporting, an application fault occurs in the reported helper.

Accessing the New Web Interface

The new web interface provides a new look for monitoring reports and tracking web services. You can access the new web interface in the following way:

- Log in to the legacy web interface and click the **Secure Web Appliance is getting a new look. Try it!!** link. When you click this link, it opens a new tab in your web browser and goes to `https://wsa01-enterprise.com:<trailblazer-https-port>/ng-login`, where `wsa01-enterprise.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance for accessing the new web interface.

Important!

- You must log in to the legacy web interface of the appliance.
- Ensure that your DNS server can resolve the hostname of the appliance that you specified.
- By default, the new web interface needs TCP ports 6080, 6443, and 4431 to be operational. Ensure that these ports are not blocked in the enterprise firewall.
- The default port for accessing new web interface is 4431. This can be customized using the **trailblazerconfig** CLI command. For more information about the **trailblazerconfig** CLI command, see “Command Line Interface” chapter in the user guide.
- The new web interface also needs AsyncOS API (Monitoring) ports for HTTP and HTTPS. By default, these ports are 6080 and 6443. The AsyncOS API (Monitoring) ports can also be customized using the **interfaceconfig** CLI command. For more information about the **interfaceconfig** CLI command, see “Command Line Interface” chapter in the user guide.

If you change these default ports, ensure that the customized ports for the new web interface are not blocked in the enterprise firewall.

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 11.8 and later):

- Google Chrome
- Mozilla Firefox

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 11.8 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.

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

The build is available for upgrade on all the existing supported platforms, whereas the enhanced performance support is available only for the following hardware models:

- Sx95/F
- Sx96/F

Virtual Models:

- S100v
- S300v

  The system CPU and memory requirements are changed from 12.5 release onwards. For more information, see Cisco Content Security Virtual Appliance Installation Guide.
- S600v
- S1000v

Upgrade Paths

- Upgrading to AsyncOS 16.0.0-399, on page 10
- Upgrading to AsyncOS 16.0.0-359, on page 11

Upgrading to AsyncOS 16.0.0-399

Note
- TLSv1.0 and TLSv1.1 are no longer supported in any SSL configuration. You must change the TLS version to TLSv1.2 or later before upgrading your AsyncOS.
- While upgrading, do not connect any devices (keyboard, mouse, management devices (Raritan) and so on.) to the USB ports of the appliance.

You can upgrade to the AsyncOS 16.0.0-399 version from the following versions:

- 14.5.1-016
- 14.5.1-607
- 14.5.2-011
- 14.5.3-033
- 15.0.0-355
- 15.0.1-004
- 15.1.0-287
- 15.2.0-116
- 15.2.0-164
- 15.2.1-011
- 15.2.2-009
- 15.2.3-007
- 15.2.3-505
- 15.2.4-022
- 15.2.5-013
- 15.5.0-566
- 15.5.0-574
- 15.5.0-710
- 15.5.1-002
- 16.0.0-359

Upgrading to AsyncOS 16.0.0-359



Note

- TLSv1.0 and TLSv1.1 are no longer supported in any SSL configuration. You must change the TLS version to TLSv1.2 or later before upgrading your AsyncOS.
- While upgrading, do not connect any devices (keyboard, mouse, management devices (Raritan) and so on.) to the USB ports of the appliance.

You can upgrade to the AsyncOS 16.0.0-359 version from the following versions:

- 14.5.1-016
- 14.5.1-607
- 14.5.2-011
- 14.5.3-033
- 15.0.0-355
- 15.0.1-004
- 15.1.0-287
- 15.2.0-116
- 15.2.0-164
- 15.2.1-011
- 15.2.2-009
- 15.2.3-007
- 15.2.3-505
- 15.2.4-022
- 15.2.5-013
- 15.5.0-566
- 15.5.0-574
- 15.5.0-710
- 15.5.1-002

Deploying a Virtual Appliance

To deploy a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available at http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Migrating from a Hardware Appliance to a Virtual Appliance

Procedure

Step 1 Follow the instructions provided in *Cisco Content Security Virtual Appliance Installation Guide* to configure your virtual appliance.

Note
Verify that the Security Services updates have been successfully installed.

Step 2 Upgrade your hardware appliance to this version of AsyncOS.

Step 3 Save the configuration file for your upgraded hardware appliance.

Step 4 Load the configuration file from the hardware appliance onto the virtual appliance.

If your virtual appliances and hardware have different IP addresses, unselect **Load Network Settings** before loading the configuration files.

Step 5 Commit your changes.

Step 6 Go to **Network** > **Authentication** and join the domain again. Otherwise, identities won't work.

Upgrade AsyncOS for Web

Before you begin

- TLSv1.0 and TLSv1.1 protocols are no longer supported in any SSL configuration other than the proxy configuration. You must change the TLS version to TLSv1.2 or later before upgrading your AsyncOS.
- Log in as administrator.
- Perform pr-eupgrade requirements, including updating the RAID controller firmware.

Procedure

Step 1 On the **System Administration** > **Configuration File** page, save the XML configuration file from the Secure Web Appliance.

Step 2 On the **System Administration** > **System Upgrade** page, click **Upgrade Options**.

Step 3 Select either **Download and install**, or **Download only** option.

Step 4 Select an upgrade from the available list.

Step 5 Click **Proceed**.

If you chose **Download only**, the upgrade will be downloaded to the appliance.

Step 6 If you chose **Download and install**, when the upgrade is complete, click **Reboot Now** to reboot the Secure Web Appliance.

Note
To verify the browser loads the new online help content in the upgraded version of AsyncOS, you must exit the browser and then open it before viewing the online help. This clears the browser cache of any outdated content.

Important Actions Required After Upgrading

In order to ensure that your appliance continues to function properly after upgrade, you must address the following items:

- Change the Default Proxy Services Cipher Suites to Cisco Recommended Cipher Suites
- Virtual Appliances: Required Changes for SSH Security Vulnerability Fix
- File Analysis: Required Changes to View Analysis Result Details in the Cloud
- File Analysis: Verify File Types To Be Analyzed
- Unescaped Dots in Regular Expressions

Change the Default Proxy Services Cipher Suites to Cisco Recommended Cipher Suites

From AsyncOS 9.1.1 onwards, the default cipher suites available for Proxy Services are modified to include only secure cipher suites.

However, if you are upgrading from AsyncOS 9.x.x and later releases, the default Proxy Services cipher suites are not modified. For enhanced security, Cisco recommends that you change the default Proxy Services cipher suites to the Cisco recommended cipher suites after the upgrade. Do the following:

Procedure

Step 1 Log in to your appliance using the web interface.

Step 2 Click **System Administration** > **SSL Configuration**.

Step 3 Click **Edit Settings**.

Step 4 Under **Proxy Services**, set the **Cipher(s) to Use** field to the following field:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:TLS_AES_256_GCM_SHA384
```

Caution
Make sure that you paste the above string as a single string with no carriage returns or spaces.

Step 5 Submit and commit your changes.

You can also use the **sslconfig** command in CLI to perform the above steps.

Virtual Appliances: Required Changes for SSH Security Vulnerability Fix

Requirements in this section were introduced in AsyncOS 8.8.

The following security vulnerability will be fixed during upgrade if it exists on your appliance:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport%20

Note This patch is required only for virtual appliance releases that were downloaded or upgraded before June 25, 2015.

If you did not patch this issue before upgrading, you will see a message during upgrade stating that it has been fixed. If you see this message, the following actions are required to return your appliance to full working order after upgrade:

- Remove the existing entry for your appliance from the known hosts list in your ssh utility. Once the new key has been created, connect to the appliance via ssh and accept the connection.
- Clear the old SSH host key for the appliance on the remote server if you are using SCP push to transfer logs to a remote server (including Splunk).
- If your deployment includes a Cisco Content Security Management Appliance, see important instructions in the Release Notes for that appliance.

File Analysis: Required Changes to View Analysis Result Details in the Cloud

If you have deployed multiple content security appliances (web, email, and/or management) and you want to view detailed file analysis results in the cloud for all files uploaded from any appliance in your organization, you must configure an appliance group on each appliance after upgrading. To configure appliance groups, see File Reputation Filtering and File Analysis.

File Analysis: Required Changes to View Analysis Result Details in the Cloud

If you have deployed multiple content security appliances (web, email, and/or management) and you want to view detailed file analysis results in the cloud for all files uploaded from any appliance in your organization, you must configure an appliance group on each appliance after upgrading. To configure appliance groups, see File Reputation Filtering and File Analysis.

File Analysis: Verify File Types To Be Analyzed

The File Analysis cloud server URL changed in AsyncOS 8.8, and as a result, the file types that can be analyzed may have changed after the upgrade. You should receive an alert if there are changes. To verify the file types selected for analysis, select **Security Services** > **Anti-Malware and Reputation** and look at the Advanced Malware Protection settings.

Unescaped Dots in Regular Expressions

Following upgrades to the regular-expression pattern-matching engine, you may receive an alert regarding unescaped dots in existing pattern definitions after updating your system. Any unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the Velocity pattern-matching engine, and an alert to that effect will be sent to you. You will continue to receive an alert following each update until you correct or replace the pattern. Generally, unescaped dots in a larger regular expression can be problematic and should be avoided.

Documentation Updates

The user guide in the website (www.cisco.com) may be more current than the online help. To obtain the user guide and other documentation for this product, click the **View PDF** button in the online help or visit the URL shown in Related Documentation, on page 16.

Known and Fixed Issues

- Bug Search Tool Requirements
- List of Known and Fixed Issues
- Finding Information about Known and Resolved Issues

Lists of Known and Fixed Issues

- Known and Fixed Issues in Release 16.0.0-399, on page 15
- Known and Fixed Issues in Release 16.0.0-359, on page 16

Known and Fixed Issues in Release 16.0.0-399

- Fixed Issues

- Known Issues

Known and Fixed Issues in Release 16.0.0-359

- Fixed Issues
- Known Issues

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.

Finding Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find 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/search.

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, x.x.x.

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 **Releases** drop-down.
- To view the list of known issues, select **Affecting these Releases** from the **Releases** 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	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

Documentation	Location
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
Secure Web Appliance Release Notes, ISE Compatibility Matrix,and Ciphers	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-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.