Release Notes for AsyncOS 10.5.x for Cisco Web Security Appliances

Published: September 1, 2016
Revised: August 11, 2020

Contents

Cisco Systems, Inc.
www.cisco.com

What's New

Cisco AsyncOS 10.5.6-024 - MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 10.5.6-024 for additional information for additional information.

Cisco AsyncOS 10.5.6-022 - MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 10.5.6-022 for additional information for additional information.

Cisco AsyncOS 10.5.5-005 - MD (Maintenance Deployment)

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 10.5.5-005 for additional information for additional information.

Cisco AsyncOS 10.5.4-018 - MD (Maintenance Deployment)

Feature	Description
Enable or Disable Incremental Updates	You can use the CLI command `updateconfig > setup` to enable or disable incremental updates from the Web Reputation service. If you disable incremental updates, the appliance will continue to download the full updates from the Cisco server. **Note** Disabling incremental updates will result in delays in receiving updated web reputation information on the appliance. For more information, see the "Web Security Appliance CLI Commands" topic in the user guide.

Cisco AsyncOS 10.5.3-025 - MD (Maintenance Deployment) Refresh

Feature	Description
Support for Outbound ACL on the management port	A new subcommand OUTBOUNDACL is added to the CLI command `fipsconfig` to restrict IP addresses on the management port. Using this subcommand, you can configure IP addresses to which you want to restrict the appliance from making any outbound connections. This subcommand is available only in FIPS mode. You can perform the following actions using the subcommand OUTBOUNDACL: • Add New • Edit • Delete • Clear
Support to configure login history	A new subcommand LOGINHISTORY is added to the CLI command `adminaccessconfig` to configure the number of days for which the login history is retained. Default value is 1 day. This is available in both FIPS and non-FIPS mode.
Support to configure maximum concurrent login sessions	A new subcommand MAXSESSIONS is added to the CLI command `adminaccessconfig` to configure the maximum number of concurrent sessions of the appliance through the Command Line Interface and web interface. Default value in FIPS mode is 3 and non-FIPS mode is 10. This is available in both FIPS and non-FIPS mode.

Feature	Description
WBRS enhancement	Currently when the WBRS update fails, it will revert to factory default settings. The new WBRS enhancement ensures that if the WBRS update fails or downloading the files fail during the update process, the WBRS reverts to the previous version. It will not revert to factory default settings.
Office 365 Web Service External URL Categories	You can configure your appliance with Microsoft Office 365 web service's external live feed which serves URLs and IPs. The web service URL must not contain a *ClientRequestId*, and must have JSON as the format.

Cisco AsyncOS 10.5.3-024 - Deprovisioned

This release was deprovisioned on November 22, 2018

What's New In Cisco AsyncOS 10.5.2-072 - GD (General Deployment Refresh)

Note

- The L4 Traffic Monitor functionality is unavailable in this release due to the change in the way Free BSD 10.1 handles bridging.
- Web proxy bypassing, or blocking of domains or hostnames based on DNS IP snooping, dependent on L4 Traffic Monitor, is unavailable in this release.

Feature	Description
Kerberos support for high availability clusters	While creating or editing an Active Directory realm, you can use the **Use keytab authentication** option in the Kerberos High Availability section, to enable Kerberos authentication for all appliances in high availability clusters. See the "Creating an Active Directory Realm for Kerberos Authentication Scheme", and "Creating a Service Account in Windows Active Directory for Kerberos Authentication in High Availability Deployments" topics in the user guide for more information.
Configure the number of Kerberos authentication helpers	You can use the CLI command `modifyauthhelpers` to configure the number of Kerberos authentication helpers.
List of Ciphers for AsyncOS for Cisco Web Security Appliances	A new document that lists the supported and unsupported ciphers (SSL and SSH) for AsyncOS for Cisco Web Security Appliances is available now. See https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

Feature	Description
SSH configuration	The following subcommands are added to the CLI command `sshconfig:` • `Incomplete SSH session timeout (in secs)` Default value is 60. • `Unsuccessful SSH login attempts allowed` Default value is 3.
FIPS mode update	The maximum number of password retry attempts permitted for access to the appliance through SSH is now 3.

This release contains a number of bug fixes; see the Known and Fixed Issues in Release 10.5.2-072 for additional information for additional information.

Cisco AsyncOS 10.5.2-061 - Deprovisioned

This release was deprovisioned on August 20, 2018.

Cisco AsyncOS 10.5.2-042 - Deprovisioned

This release was deprovisioned on August 20, 2018.

What's New In Cisco AsyncOS 10.5.2-034 - LD (Limited Deployment)

Note

- The L4 Traffic Monitor functionality is unavailable in this release due to the change in the way Free BSD 10.1 handles bridging.
- Web proxy bypassing, or blocking of domains or hostnames based on DNS IP snooping, dependent on L4 Traffic Monitor, is unavailable in this release.

Feature	Description
Two-factor authentication	Cisco Web Security appliance now supports two-factor authentication that ensures secure access when you log into your appliance. You can configure two-factor authentication for your appliance through any standard RADIUS server that complies with a standard RFC. You can enable two-factor authentication through the web interface or the CLI: • System Administration > Users page in the web interface. See the Perform System Administration Tasks chapter in the user guide or online help. • `userconfig` > `twofactorauth` command in the CLI. See the Command Line Interface chapter in the user guide or online help. **Note** If your appliance is managed by a Security Management appliance, add the pre-shared keys in the Security Management and Web Security appliances using the `smaconfig` command in the CLI.
Network Time Protocol (NTP) updates	• You can now configure the query interval and sync up delay time for NTP queries. You can enable authentication for NTP responses and requests sent and received between the appliance and NTP servers. MD5 and SHA1 are supported. You configure these settings through the web interface or the CLI: – System Administration > Time Settings page in the web interface. See the Perform System Administration Tasks chapter in the user guide or online help. – `ntpconfig` command in the CLI. See the Command Line Interface chapter in the user guide or online help.
FIPS mode updates	You can enable automatic shutdown of the appliance when logging of critical information fails. See the Perform System Administration Tasks chapter in the user guide or online help.
Logo support for the administrator login banner	You can use the `adminaccessconfig` > `logo` CLI to select a logo for the administrator login banner. See the Command Line Interface chapter in the user guide or online help.
User login status display for administrative user login	You can now see a list of successful and unsuccessful logins made through various protocols, independent of source IP addresses. This is displayed in the web interface and CLI, only for administrative users after logging in.
Forced re-authentication for non-administrative users after user type change	Users will be asked to re-authenticate after any user type changes made by an administrator. This change in user type will be displayed in the web interface, after the user re-authenticates. See the Perform System Administration Tasks chapter in the user guide or online help.

Samba upgrade	Samba version has been upgraded to version 4.5.8.
SMB v2 and v3 support	SMB v2 and v3 protocols are now supported.

What's New in Cisco AsyncOS 10.5.1-296 GD (General Deployment)

Note

- The L4 Traffic Monitor functionality is unavailable in this release due to the change in the way Free BSD 10.1 handles bridging.
- Web proxy bypassing, or blocking of domains or hostnames based on DNS IP snooping, dependent on L4 Traffic Monitor, is unavailable in this release.

This release contains a number of bug fixes; see Known and Fixed Issues in Release 10.5.1-296 for additional information.

What's New In Cisco AsyncOS 10.5.1 - LD (Limited Deployment)

Note

- The L4 Traffic Monitor functionality is unavailable in this release due to the change in the way Free BSD 10.1 handles bridging.
- Web proxy bypassing, or blocking of domains or hostnames based on DNS IP snooping, dependent on L4 Traffic Monitor, is unavailable in this release.

Feature	Description
Certificate-based authentication	Administrative users can use digital certificates to login to the appliance's web interface. Configure the CLI login separately with password-based authentication (LDAP, and RADIUS with TLS or UDP are supported). See the "Enabling Certificate Based Authentication for Administrative Users" topic in the user guide or online help.
RADIUS with TLS for authentication and authorization of administrative users	You can use RADIUS over Transport Layer Security (TLS) to authenticate and authorize administrative users. See the "Enabling External Authentication Using RADIUS" topic in the user guide or online help.
Platform Upgrades	Cisco SSL has been upgraded to 6.1.21, with FIPS Object Module (FOM) 6.0, 1.0.2h openSSL, which is more secure and already FIPS compliant.
WCCP weighted load balancing	The Cisco-developed Web Cache Communication Protocol (WCCP) is a content-routing technology that enables transparent redirection of content requests. It provides a weighting assignment parameter that lets you configure differential WCCP load balancing for each WSA based on its performance capability. See the "About WCCP Load Balancing" topic in the user guide or online help.

Feature	Description
FIPS mode updates	You can enable FIPS mode and encryption of Critical Sensitive Parameters (CSP) such as shared secret keys, SNMP passwords, Active Directory credentials, and so on. All auditable events are now logged in the audit logs. **Note** When upgrading to AsyncOS 10.5 for Web Security Appliances, disable FIPS mode (**System Administration** > **FIPS Mode)** before upgrading, and re-enable it after the appliance has restarted.
TLS v1.2 support for appliance management web interfaces, and audit logs	You can use Transport Layer Security v1.2 (along with TLS v1.1) for appliance management, updater, LDAPS, and other services. This is available in the non-FIPS mode. In FIPS mode, services are auto-configured to use these protocols. See the "SSL Configuration" topic in the user guide or online help.

What's New In Cisco AsyncOS 10.5.0 LD (Limited Deployment)

Note

- The L4 Traffic Monitor functionality is unavailable in this release due to the change in the way Free BSD 10.1 handles bridging.
- Web proxy bypassing, or blocking of domains or hostnames based on DNS IP snooping, dependent on L4 Traffic Monitor, is unavailable in this release.

Feature	Description
WCCP weighted load balancing	The Cisco-developed Web Cache Communication Protocol (WCCP) is a content-routing technology that enables transparent redirection of content requests. This release provides a weighting assignment parameter that lets you configure differential WCCP load balancing for each WSA based on its performance capability. The CLI command `wccpstat` is available with two options: • `all` – Displays details of all WCCP (Web Cache Communication Protocol) service groups. • `servicegroup` – Displays details of a specific WCCP service group.
FIPS mode updates	You can enable FIPS mode and encryption of Critical Sensitive Parameters (CSP) such as shared secret keys, SNMP passwords, Active Directory credentials, and so on. For example, when FIPS mode is enabled, all Administration access features are FIPS 140-2 compliant, swap disk space is encrypted, and configuration files can be saved and loaded with passwords encrypted. In addition, certificates are validated strictly to comply with CC standards before uploading, and OCSP validation is available to validate certificates against a revocation list. Further, per CC requirements, all auditable events are now logged in the audit logs. **Notice** When upgrading to AsyncOS 10.5 for Web Security Appliances, disable FIPS mode (**System Administration > FIPS Mode)** before upgrading, and then re-enable after the system has restarted.
Common Criteria certification	This release is a candidate for CC certification.
TLS versions	Transport Layer Security v1.1 and v1.2 are now available for selection with management, updater, LDAPS, and other services. In FIPS mode, the services are auto-configured to use these protocols.
Platform Upgrades	AsyncOS has been upgraded to FreeBSD 10.1. Cisco SSL has been upgraded to ciscossl-1.0.2f.6.0.3, with FIPS Object Module (FOM) 6.0 which is more secure and already FIPS compliant.

Changes in Behavior

- Change in Behavior in Cisco AsyncOS 10.5.5-005 - MD (Maintenance Deployment), page 10
- Changes in Behavior in Cisco AsyncOS 10.5.2-072 - GD (General Deployment), page 10
- Changes in Behavior in Cisco AsyncOS 10.5.2-034 - LD (Limited Deployment), page 10
- Change in Behavior in Cisco AsyncOS 10.5.1 - GD (General Deployment), page 10
- Change in Behavior in Cisco AsyncOS 10.5.0 - LD (Limited Deployment), page 11
- Changes in Behavior in Previous Releases, page 12

Change in Behavior in Cisco AsyncOS 10.5.5-005 - MD (Maintenance Deployment)

Log Subscription Names	Non-ASCII characters and whitespaces in log subscription names are not supported. Upgrade will fail if the log subscription file names contain any non-supported characters.

Changes in Behavior in Cisco AsyncOS 10.5.2-072 - GD (General Deployment)

AMP compressed files processing	When AMP is enabled, and access policies set to block all HTTP transactions with a malicious verdict from AMP, MIME types are first detected before decompressing files to either block or allow the file to be sent.
Verification of secure authentication certificate	While performing an upgrade, if the secure authentication certificate is not FIPs-complaint, it will be replaced with the default certificate of the latest path to which the appliance is upgraded to. This happens only when the customer has used the default certificate before the upgrade.
FIPS mode update	• The maximum number of concurrent sessions allowed for FIPS mode is 3. • The maximum number of concurrent sessions allowed for non-FIPS mode is 10.

Changes in Behavior in Cisco AsyncOS 10.5.2-034 - LD (Limited Deployment)

Web Reputation Filtering and URL categorization	URL categorization relies on Web Reputation Filtering being enabled. If Web Reputation Filtering is disabled globally, URL categorization will not function optimally.
Web proxy custom headers	Web proxy custom headers character limit is increased to 998.

Change in Behavior in Cisco AsyncOS 10.5.1 - GD (General Deployment)

FIPS mode update	The maximum number of password retry attempts permitted for access to the appliance through SSH is now 3.

sshconfig CLI command enhancements	The sshconfig > sshd > setup command in the CLI now supports configuring the duration of the incomplete SSH session timeout and the number of unsuccessful SSH login attempts allowed.
Unsupported ciphers	The following ciphers are not supported: • Port 8443 (management interface) - RC4-MD5, RC4-SHA for SSL V 3.0 and TLS 1.0 • Port 22 (SSH port) - arcfour256, arcfour128, blowfish-cbc, arcfour

Change in Behavior in Cisco AsyncOS 10.5.0 - LD (Limited Deployment)

tail command	Displays the end of a log file. Command accepts log file name as parameter. Example 1 example.com> tail Currently configured logs: 1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll 2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll … … Enter the number of the log you wish to tail. []> 9 Press Ctrl-C to stop scrolling, then `q` to quit. ~ ~ Thu Dec 14 10:03:07 2017 Info: Begin Logfile ~ ~ … … “CTRL-C” + “q” Example 2 example.com> tail system_logs Press Ctrl-C to stop scrolling, then `q` to quit. ~ ~ Thu Dec 14 09:59:10 2017 Info: Begin Logfile … … “CTRL-C” + “q”

Changes in Behavior in Previous Releases

This section describes changes in behavior from previous versions of AsyncOS for Web that may affect the appliance configuration after you upgrade to the latest version.

Strict Certificate Validation

With the release of the FIPS-mode updates in AsyncOS 10.5, all presented certificates are validated strictly to comply with Common Criteria (CC) standards before uploading, and OCSP validation is available to validate certificates against a revocation list.

You must ensure that proper, valid certificates are uploaded to the WSA, and that valid, secure certificates are configured on all related servers to facilitate smooth SSL handshakes with those servers.

Strict certificate validation is applied for the following certificate uploads:

- HTTPS Proxy (Security Services > HTTPS Proxy)
- File Analysis Server (Security Services > Anti-Malware and Reputation > Advanced Settings for File Analysis > File Analysis Server: Private Cloud & Certificate Authority: Use Uploaded Certificate Authority)
- Trusted Root Certificates (Network > Certificate Management)
- Global Authentication Settings (Network > Authentication > Global Authentication Settings)
- Identity Provider for SaaS (Network > Identity Provider for SaaS)
- Identity Services Engine (Network > Identity Services Engine)
- External DLP Servers (Network > External DLP Servers)
- LDAP & Secure LDAP (Network > Authentication > Realm)

Default Cipher Suites for Proxy Services

From AsyncOS 9.1.1 onwards, the default cipher suites available for Proxy Services are modified to include only secure cipher suites. If you are upgrading to AsyncOS 10.x.x, see Change the Default Proxy Services Cipher Suites to Cisco Recommended Cipher Suites, page 25.

Special Characters No Longer Allowed in Regular Expressions

You can no longer use “.*” to begin or end a regular expression. You also cannot use “./” in a regular expression intended to match a URL, nor can you end such an expression with a dot.

Special Characters Allowed in Active Directory User Names

Prior to AsyncOS 9.0, attempts to join an Active Directory domain with a user name that included special characters would produce an error. Now the following special characters can be used in domain user names: ` ~ ( ) { } ! # ^ _ $ & (however, note that % is not yet supported).

Limit on Number of WCCP Dynamic Service Groups

You can configure no more than 15 WCCP service groups on the Web Security appliance.

WCCP Behavior Changes

The WSA sends a WCCP “here I am” (HIA) message to the specified WCCP-enabled routers every 10 seconds. The appliance’s WCCP daemon also sends a proxy health check message (xmlrpc client request) to the xmlrpc server running on the Web proxy every 10 seconds.

If the proxy is up and running, the WCCP service receives a response from the proxy. If the WCCP service doesn’t receive a reply from the proxy, then HIA messages are not sent to the WCCP routers.

After a WCCP router misses three consecutive HIA messages, the router removes the WSA from its service group and traffic is no longer forwarded to the WSA. [CSCzv19247]

Limit on Number of Concurrent Sessions

Beginning in AsyncOS 8.5, individual users are limited to a maximum of 10 concurrent sessions; this total includes both CLI and Web interface sessions.

List of Available Upgrades

Beginning in AsyncOS 8.5, all available releases appear in the list of available upgrades, including releases that would previously have been provisioned only to a limited number of customers as a limited release.

Each release in the list is identified by the release type (ED - Early Deployment, GD - General Deployment, MD - Maintenance 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.

Support Requests Require CCO ID and Support Contract

Beginning in AsyncOS 8.5, in order to open a support request from the appliance, you must enter a CCO ID and a support contract ID.

New Certificate Management Page

Beginning in AsyncOS 8.5, certificate management functionality has been moved from the Security Services > HTTPS Proxy page to a new, stand-alone page: Network > Certificate Management.

Exporting Web Tracking Data

Previously, when exporting web tracking data as CSV, the data was sorted by timestamps. Beginning in AsyncOS 8.5, this data is not sorted.

SNMP Monitoring

Beginning in AsyncOS 8.5, the following functionality is different from previous implementations:

Message authentication and encryption are mandatory when enabling SNMPv3. Passwords for authentication and encryption should be different. The encryption algorithm can be AES (recommended) or DES. The authentication algorithm can be SHA-1 (recommended) or MD5.

X-Authenticated-Groups Header Format

Beginning in AsyncOS 8.5, if LDAP authentication and External Data Loss Prevention are configured on the appliance, AsyncOS sends the X-Authenticated-Groups header in this format:

LDAP://(*LDAP server name*)/(*groupname*).

Previously, the format was LDAP://(*groupname*). This software change may require changes to policies or other automation relying on the X-Authenticated-Groups header. [Defect: CSCum91801]

New CLI Option to Modify Web Tracking Query Timeout

A new CLI option `webtrackingquerytimeout` is introduced under `reportingconfig` command to modify the web tracking query timeout.

Note The default value for `webtrackingquerytimeout` is 120 seconds and can be modified from 120 seconds and above.

The following is an example to modify the web tracking query timeout to 150 seconds:

```
web.example.com > reportingconfig

Choose the operation you want to perform:
- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Web Tracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this appliance.
```

```
[]> webtrackingquerytimeout

Timeout value for Web Tracking Queries (in Seconds)
[120]> 150

Choose the operation you want to perform:
- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Web Tracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
[]>
web.example.com > commit

Please enter some comments describing your changes:
[]>
Changes committed: Fri May 05 13:18:18 2017 GMT

web.example.com >
```

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

- All virtual appliance models.
- The following hardware models:
  - x70 (Cisco Web Security Appliance S170 is not supported for AsyncOS 10.5 and later)
  - x80
  - x90

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

Important! After an upgrade, on S190, S390, and S690 appliances which have read-only root partitions, the output of the ipcheck command may display the usage of the root partition as more than 100%. Please be advised that this normal, and will not have any functional impact.

Note While upgrading, do not connect any devices (keyboard, mouse, management devices (Raritan) etc.) to the USB ports of the appliance.

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21 and Installation and Upgrade Notes, page 21.

- Upgrading to AsyncOS 10.5.6-024 (MD - Maintenance Deployment), page 16
- Upgrading to AsyncOS 10.5.6-022 (MD - Maintenance Deployment), page 17
- Upgrading to AsyncOS 10.5.5-005 (MD - Maintenance Deployment), page 17
- Upgrading to AsyncOS 10.5.4-018 (MD - Maintenance Deployment), page 18
- Upgrading to AsyncOS 10.5.3-025 (MD - Maintenance Deployment) Refresh, page 19
- Upgrading to AsyncOS 10.5.2-072 (GD - General Deployment Refresh), page 19
- Upgrading to AsyncOS 10.5.2-034 (LD - Limited Deployment), page 20
- Upgrading to AsyncOS 10.5.1-296 (GD - General Deployment), page 20
- Upgrading to AsyncOS 10.5.1-270 (LD - Limited Deployment), page 20
- Upgrading to AsyncOS 10.5.0-358 (LD - Limited Deployment), page 21

Upgrading to AsyncOS 10.5.6-024 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21, and Installation and Upgrade Notes, page 21. Review the list of known issues, see Known and Fixed Issues.

You can upgrade to release 10.5.6-022 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10-1-4-017
- 10-5-1-296
- 10-5-1-508
- 10-5-2-061
- 10-5-2-072
- 10-5-3-025
- 10-5-3-503
- 10-5-4-018
- 10-5-5-005
- 10-5-6-022

Upgrading to AsyncOS 10.5.6-022 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21, and Installation and Upgrade Notes, page 21. Review the list of known issues, see Known and Fixed Issues.

You can upgrade to release 10.5.6-022 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10-1-4-017
- 10-5-1-296
- 10-5-1-508
- 10-5-2-061
- 10-5-2-072
- 10-5-3-025
- 10-5-3-503
- 10-5-4-018
- 10-5-5-005

Upgrading to AsyncOS 10.5.5-005 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21, and Installation and Upgrade Notes, page 21. Review the list of known issues, see Known and Fixed Issues.

You can upgrade to release 10.5.5-005 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10-1-1-235
- 10-1-1-307
- 10-1-3-036
- 10-1-3-039
- 10-1-3-054
- 10-1-4-017
- 10-5-1-296
- 10-5-1-508
- 10-5-2-072
- 10-5-3-025
- 10-5-3-503
- 10-5-4-018

Upgrading to AsyncOS 10.5.4-018 (MD - Maintenance Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21, and Installation and Upgrade Notes, page 21. Review the list of known issues, see Known and Fixed Issues.

You can upgrade to release 10.5.4-018 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10-1-1-235
- 10-1-1-307
- 10-1-2-050
- 10-1-3-036
- 10-1-3-039
- 10-1-3-054
- 10-1-4-007
- 10-1-4-017
- 10-5-1-296
- 10-5-1-503
- 10-5-1-508
- 10-5-2-034
- 10-5-2-072
- 10-5-2-504
- 10-5-3-025
- 10-5-3-503

Upgrading to AsyncOS 10.5.3-025 (MD - Maintenance Deployment) Refresh

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21, and Installation and Upgrade Notes, page 21. Review the list of known issues, see Known and Fixed Issues.

You can upgrade to release 10.5.3-025 of AsyncOS for Cisco Web Security appliances from the following versions:

- 9-1-2-022
- 9-1-2-029
- 9-1-2-041
- 9-1-3-016
- 9-1-3-024
- 10-1-1-235
- 10-1-2-050
- 10-1-3-036
- 10-1-3-039
- 10-1-3-054
- 10-1-4-007
- 10-5-1-296
- 10-5-1-503
- 10-5-1-508
- 10-5-2-034
- 10-5-2-504
- 10-5-2-072
- 10-5-3-024

Upgrading to AsyncOS 10.5.2-072 (GD - General Deployment Refresh)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21, and Installation and Upgrade Notes, page 21. Review the list of known issues, see Known and Fixed Issues.

You can upgrade to release 10.5.2-072 of AsyncOS for Cisco Web Security appliances from the following versions:

- 9-1-2-022
- 9-1-2-041
- 9-1-3-016
- 9-1-3-024
- 10-1-1-235
- 10-1-2-050
- 10-1-3-039
- 10-1-3-054
- 10-5-1-296
- 10-5-1-503
- 10-5-2-034
- 10-5-2-042
- 10-5-2-061

Upgrading to AsyncOS 10.5.2-034 (LD - Limited Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21, and Installation and Upgrade Notes, page 21. Upgrade is not recommended for appliances managed by SMA version 10.1.0.Review the list of known issues, see Known and Fixed Issues.

You can upgrade to release 10.5.2-034 of AsyncOS for Cisco Web Security appliances from the following versions:

- 10.5.1-296
- 10.5.2-031

Upgrading to AsyncOS 10.5.1-296 (GD - General Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21, and Installation and Upgrade Notes, page 21. Upgrade is not recommended for appliances managed by SMA version 10.1.0.Review the list of known issues, see Known and Fixed Issues.

You can upgrade to release 10.5.1-296 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8.5.3-069
- 8.5.4-038
- 9.0.1-162
- 9.1.1-074
- 9.1.2-022
- 9.1.2-029
- 9.1.2-033
- 9.1.2-034
- 10.0.0-233
- 10.1.0-204
- 10.1.1-234
- 10.1.1-235
- 10.5.0-358
- 10.5.1-270
- 10.5.1-292

Upgrading to AsyncOS 10.5.1-270 (LD - Limited Deployment)

Note Before you start the upgrade process, see Pre-upgrade Requirements, page 21, and Installation and Upgrade Notes, page 21. Upgrade is not recommended for appliances managed by SMA version 10.1.0. Review the list of known issues, see Known and Fixed Issues.

You can upgrade to release 10.5.1-270 of AsyncOS for Cisco Web Security appliances from the following versions:

- 9.1.1-074
- 9.1.2-022
- 10.1.1-234
- 10.5.0-358

Upgrading to AsyncOS 10.5.0-358 (LD - Limited Deployment)

> **Note** Before you start the upgrade process, see Pre-upgrade Requirements, page 21 and Installation and Upgrade Notes, page 21.

You can upgrade to release 10.5.0-358 of AsyncOS for Cisco Web Security appliances from the following versions:

- 8.5.3-069
- 9.0.1-162
- 9.1.1-074
- 9.1.2-010
- 10.0.0-233
- 10.1.0-204
- 10.1.1-234

Pre-upgrade Requirements

- Update RAID Controller Firmware, page 21
- FIPS Mode, page 21
- Check Post-upgrade Requirements Before Upgrading, page 21

Update RAID Controller Firmware

Before upgrading the AsyncOS software, update the RAID controller firmware as described in *Cisco Update for RAID Controller Firmware (For S360/S370/S660/S670 only, reboot required) Release Notes*.

FIPS Mode

Prior to upgrading to AsyncOS 10.5, make a back-up copy of the current configuration, and then disable FIPS mode if it is currently enabled (System Administration > FIPS Mode).

Check Post-upgrade Requirements Before Upgrading

Some existing functionality will not work after upgrade until you make changes. To minimize downtime, familiarize yourself with and prepare for those requirements before upgrading. See Important! Actions Required After Upgrading.

Installation and Upgrade Notes

- Compatibility Details
- Deploying a Virtual Appliance
- Configuration Files
- Demo Security Certificate Encryption Strength

- Post-upgrade Reboot
- Changes in Behavior

Compatibility Details

- Compatibility with Cisco AsyncOS for Security Management
- IPv6 and Kerberos Not Available in Cloud Connector Mode
- Functional Support for IPv6 Addresses
- Availability of Kerberos Authentication for Operating Systems and Browsers

Compatibility with Cisco AsyncOS for Security Management

For compatibility between this release and AsyncOS for Cisco Content Security Management releases, see the compatibility matrix at: http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

IPv6 and Kerberos Not Available in Cloud Connector Mode

When the appliance is configured in Cloud Connector mode, unavailable options for IPv6 addresses and Kerberos authentication appear on pages of the web interface. Although the options appear to be available, they are not supported in Cloud Connector mode. Do not attempt to configure the appliance to use IPv6 addresses or Kerberos authentication when in Cloud Connector mode.

Functional Support for IPv6 Addresses

Features and functionality that support IPv6 addresses:

- Command line and web interfaces. You can access WSA using http://[2001:2:2::8]:8080 or https://[2001:2:2::8]:8443
- Performing Proxy actions on IPv6 data traffic (HTTP/HTTPS/SOCKS/FTP)
- IPv6 DNS Servers
- WCCP 2.01 (Cat6K Switch) and Layer 4 transparent redirection
- Upstream Proxies
- Authentication Services
  - Active Directory (NTLMSSP, Basic, and Kerberos)
  - LDAP
  - SaaS SSO
  - Transparent User Identification through CDA (communication with CDA is IPv4 only)
  - Credential Encryption
- Web Reporting and Web Tracking
- External DLP Servers (communication between WSA and DLP Server is IPv4 only)
- PAC File Hosting

Features and functionality that require IPv4 addresses:

- Internal SMTP relay
- External Authentication
- Log subscriptions push method: FTP, SCP, and syslog
- NTP servers
- Local update servers, including Proxy Servers for updates
- Authentication services
- AnyConnect Security Mobility
- Novell eDirectory authentication servers
- Custom logo for end-user notification pages
- Communication between the Web Security appliance and the Security Management appliance
- WCCP versions prior to 2.01
- SNMP

Availability of Kerberos Authentication for Operating Systems and Browsers

You can use Kerberos authentication with these operating systems and browsers:

- Windows servers 2003, 2008, 2008R2 and 2012
- Latest releases of Safari and Firefox browsers on Mac (OSX Version 10.5+)
- IE (Version 7+) and latest releases of Firefox and Chrome browsers on Windows 7 and XP.

Kerberos authentication is not available with these operating systems and browsers:

- Windows operating systems not mentioned above
- Browsers not mentioned above
- iOS and Android

Deploying a Virtual Appliance

To deploy a virtual appliance, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from 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

Step 1 Set up your virtual appliance with this AsyncOS release using the documentation described in Deploying a Virtual Appliance, page 23.

Step 2 Upgrade your hardware appliance to this AsyncOS release.

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

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

If your hardware and virtual appliances have different IP addresses, deselect Load Network Settings before loading the configuration file.

Step 5 Commit your changes.

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

Configuration Files

When you upgrade AsyncOS for Web from the web interface or Command Line Interface (CLI), the configuration is saved to file in the `/configuration/upgrade` directory. You can access the upgrade directory using an FTP client. Each configuration file name is appended with the version number, and passwords in the configuration file are masked so they are not human readable.

Generally, configuration files from earlier AsyncOS releases are incompatible with later AsyncOS releases and vice-versa.

Demo Security Certificate Encryption Strength

The encryption strength of the demo security certificate is 1024 bits both before and after upgrade to AsyncOS 8.5. With upgrade to AsyncOS 9.1.1, it is 2048 bits. With AsyncOS 10.5, when FIPS mode is enabled, the demo security certificate strength is changed to 4096 bits.

Post-upgrade Reboot

You must reboot the Web Security appliance after you upgrade AsyncOS for Web.

Upgrading AsyncOS for Web

Before You Begin

- Perform preupgrade requirements, including updating the RAID controller firmware. See Pre-upgrade Requirements, page 21.
- Log in as Administrator.

Step 1 On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.

Step 2 When upgrading to AsyncOS 10.5 for Web Security Appliances, disable FIP mode (**System Administration** > **FIPS Mode)** before upgrading, and then re-enable after the system has restarted.

Step 3 On the System Administration > System Upgrade page, click **Upgrade Options**.

Step 4 You can select either **Download and install**, or **Download only**.

Choose from the list of available upgrades.

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 Web Security 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.

New features are typically not enabled by default.

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, page 25
- Virtual Appliances: Required Changes for SSH Security Vulnerability Fix, page 26
- File Analysis: Required Changes to View Analysis Result Details in the Cloud, page 26
- File Analysis: Verify File Types To Be Analyzed, page 26
- Unescaped Dots in Regular Expressions, page 26

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 to AsyncOS 10.x.x, 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:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECD
HE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES12
8-SHA
```

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: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport.

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. Then ssh to the appliance and accept the connection with the new key.
- If you use SCP push to transfer logs to a remote server (including Splunk): Clear the old SSH host key for the appliance from the remote server.
- 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

The requirement in this section was introduced in AsyncOS 8.8.

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 the “File Reputation Filtering and File Analysis” chapter in the user guide PDF. (This PDF is more current than the online help in AsyncOS 8.8.)

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 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, and you 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 following information supplements information in the Online Help and/or User Guide for this release.

Sophos No Longer Scans Archive Files

As of AsyncOS 9.0, scanning of archive (.zip) files has been disabled in the Sophos scanner.

Adding JavaScript to End-user Notifications

If you need to add standard JavaScript to end-user notifications of any type, follow instructions in the user guide or online help for editing notification page HTML files. (JavaScript entered into the Custom Message box for notifications in the web user interface will be stripped out.) Be sure to test your script first in supported client browsers to ensure that it works as expected.

Which Files Can Have their Reputation Evaluated and Be Sent for Analysis?

The criteria for evaluating a file's reputation and for sending files for analysis may change at any time. Criteria are available only to registered Cisco customers. See *File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html.

In order to access this document, you must have a Cisco customer account with a support contract. To register, visit https://tools.cisco.com/RPF/register/register.do.

Viewing File Analysis Details in the Cloud

The most current instructions for configuring this functionality are in the user guide PDF, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html.

Different Client "Hello" Behavior for Custom and Default Categories

When scanning packet captures, you may notice that the "Client Hello" handshake is sent at different times for custom category and default (Web) category HTTPS Decryption pass-through policies.

For an HTTPS page passed through via the default category, the Client Hello is sent before receipt of a Client Hello from the requestor, and the connection fails. For an HTTPS page passed through via a custom URL category, the Client Hello is sent after the Client Hello is received from the requestor, and the connection is successful.

As a remedy, you can create a custom URL category with a pass-through action for SSL 3.0-only-compatible Web pages.

Additional Information

The User Guide PDF may be more current than the online help. To obtain the User Guide PDF and other documentation for this product, click the **View PDF** button in the online help or visit the URL shown in Related Documentation, page 32.

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 28
- Lists of Known and Fixed Issues, page 28
- Finding Information about Known and Resolved Issues, page 31

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 10.5.6-024, page 29
- Known and Fixed Issues in Release 10.5.6-022, page 29
- Known and Fixed Issues in Release 10.5.5-005, page 29
- Known and Fixed Issues in Release 10.5.4-018, page 29
- Known and Fixed Issues in Release 10.5.3-025, page 29
- Known and Fixed Issues in Release 10.5.2-072, page 29
- Known and Fixed Issues in Release 10.5.2-034, page 30
- Known and Fixed Issues in Release 10.5.1-296, page 30
- Known and Fixed Issues in Release 10.5.1-270, page 30
- Known and Fixed Issues in Release 10.5.0-358, page 30

Known and Fixed Issues in Release 10.5.6-024

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.6-024&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.6&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.6-022

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.6-022&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.6&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.5-005

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.5-005&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.5&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.4-018

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.4-018&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.4&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.3-025

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.3-025&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.3&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.2-072

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.2-072&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.2&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.2-034

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.2-034&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.2&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.1-296

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.1-296&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.1&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.1-270

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.1-270&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.1&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.0-358

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.0&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.0&sb=afr&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.2-072

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.2-072&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.2&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.2-034

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.2-034&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.2&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.1-296

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.1-296&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.1&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.1-270

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.1-270&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.1&sb=afr&sts=open&svr=3nH&bt=custV

Known and Fixed Issues in Release 10.5.0-358

Fixed Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.0&sb=fr&svr=3nH&bt=custV
Known Issues	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.5.0&sb=afr&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, 10.5.

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 Content Security Management Appliances is available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/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://community.cisco.com/t5/web-security/bd-p/5786-discussions-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.

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.