Release Notes for Cisco IronPort AsyncOS 7.7.0 for Web

Published: July 15, 2013

Contents

This document contains release information for running Cisco IronPort AsyncOS 7.7.0 for the Web Security appliance, and includes the following sections:

What's New in Cisco IronPort AsyncOS 7.7 for Web

Table 1-1 describes the new features and enhancements that have been added in the Cisco IronPort AsyncOS 7.7 for Web release. It references where you can find more details in the *Cisco IronPort AsyncOS for Web User Guide*. You can view these chapters in the PDF or the online help. You might also find it useful to review release notes from earlier releases.

Cisco Systems, Inc.
www.cisco.com

Table 1-1 New Features for AsyncOS 7.7 for Web

Feature	Description
New Features	
Multi-Forest NTLM	Configure the Web Security Appliance to authenticate users from Multiple untrusted NTLM realms. Sometimes creating trust relationships between distinct NTLM realms is not practical. You can now support these configurations using the same WSA without expending the cost and effort associated with enabling NTLM trust. Authenticate users from multiple NTLM realms if those realms posses a trust relationship. Create multiple identity policies using these untrusted NTLM realms and then configure user and group policies associated with these identities. See Authenticating Users Against Multiple Active Directory Domains in the user guide or online help.
Software-based FIPS Level 1 Compliance	The Federal Information Processing Standard (FIPS) 140-2 is a publicly announced standard developed jointly by the United States and Canadian federal governments specifying requirements for cryptographic modules that are used by all government agencies to protect sensitive but unclassified information. With AsyncOS 7.7 for Web, FIPS 140-2 Level 1 compliance can be enabled via a few simple steps in the Web Security Appliance GUI. This feature utilizes the Cisco Common Crypto Module (C3M) rather than the previously used Hardware Security Module (HSM) for all cryptographic operations and it will be available via AsyncOS 7.7 for Web running on all currently supported hardware models. See FIPS Compliance in the user guide or online help.
SOCKS Proxy	Support for SOCKS-based applications, including Bloomberg Terminals. Define SOCKS-specific user and group policies as well as specific TCP and UDP destination ports. SOCKS logs and reports allow you to track and analyze SOCKS proxy usage. See Overview of SOCKS Proxy Services in the user guide or online help.
Custom Header Insertion	Insert custom request headers. Certain websites such as YouTube for Schools require that web requests to their domains be appended with customized header strings. In the case of YouTube for Schools, an account-specific string must be sent with each request to YouTube's domains so that YouTube can recognize users from a Schools account and serve content accordingly. This function allows you to utilize the CLI to specify the custom header string and the domains for which requests will be appended. See "Custom Headers" in the in the user guide or online help.
OCSP	Use the Online Certificate Status Protocol (OCSP) to provide revocation status updates for X.509 certificates. OCSP provides a more timely means of validation for certificates than the alternative Certificate Revocation Lists (CRL). Currently, the administrator can configure the invalid certificate handling policies under the HTTPS Proxy page. Enable/disable OCSP and configure new OCSP policies using the Web UI. Configure timeout values, and select a configured upstream proxy group. Configure a list of exempt servers that WSA will connect to directly without using the upstream proxy. See Enabling Real-Time Revocation Status Checking in the user guide or online help.

Table 1-1 New Features for AsyncOS 7.7 for Web (continued)

Feature	Description
Certificate Trust Store Management	Greater management control of certificates and certificate authorities. View all of the Cisco-bundled certificates, remove trust of any Cisco-trusted root certificate authorities, and view the Cisco-published blacklist. This will provide more flexibility in making your own decisions with regards to acceptable and unacceptable certificates used by the WSA. Within the Web UI, import your own trusted certificates and add them to the trusted root certificate list. View current Cisco-trusted root certificates and select an option to override each individual certificate, removing trust by the WSA for that certificate. View Cisco's intermediate certificate blacklist. Due to real-life incidents where certain intermediate CA's were compromised, the WSA was given a hard-coded list of blacklisted intermediate certificates that was previously transparent to administrators. This now becomes a viewable list. See Adding Certificates to the Trusted List and Removing Certificates from the Trusted List in the user guide or online help.
Encrypted Private Keys	Use encrypted, password-protected private keys. Upload encrypted private keys and provide a password for the WSA to decrypt them. The WSA then stores these private keys by obfuscating/encrypting them with a password that is unknown to the user. When configurations are exported to a file, private keys remain obfuscated and unreadable to the user. The WSA can decrypt them when the configuration is loaded onto a WSA. See Uploading a Root Certificate and Key in the user guide or online help.
Enhancements	
SNI extension for Transparent SSL Handshake	Access the Server Name Indication (SNI) extension to parse the destination server name. This is useful when making requests to virtual servers hosting multiple HTTPS websites such as youtube.com and google.com. [Defect Number: 74969, CSCzv50011]

Upgrade Paths

You can upgrade to release 7.7.0-608 from the following version:

- coeus-7-5-0-703
- coeus-7-5-0-727
- coeus-7-5-0-810
- coeus-7-5-0-833
- coeus-7-5-0-834
- coeus-7-5-0-836
- coeus-7-5-0-838
- coeus-7-5-1-074
- coeus-7-5-1-079
- coeus-7-5-1-201
- coeus-7-5-2-113

- coeus-7-7-0-223
- coeus-7-7-0-327
- coeus-7-7-0-487
- coeus-7-7-0-499
- coeus-7-7-0-500

To ensure a successful upgrade, prepare for the upgrade process as described in Installation and Upgrade Notes, page 5.

Pre-Upgrade Requirements

Note IMPORTANT: During testing of AsyncOS 7.7.0, Cisco observed performance changes ranging from + 33% to - 16%, depending on the model and configuration. Performance degradation risk is limited to S160 & S360 models and models S370 and S660 that are running the web proxy without security services. If you experience performance degradation with AsyncOS 7.7.0, Cisco recommends that you revert to AsyncOS 7.5.x.

Warning **Model S160: Before installing AsyncOS for Web on some S160 appliances, install the hard drive firmware upgrade on the appliance. To verify whether your S160 requires the firmware upgrade, run the "upgrade" CLI command. If the S160 requires the firmware upgrade, "Hard Drive Firmware upgrade (for C/M/S160 models only, build 002)" will be listed as an upgrade option. If listed, run the firmware upgrade, and then upgrade AsyncOS for Web to the current version.**

Preserve Pre-Upgrade Data from the System Capacity Report

Pre-upgrade data for CPU usage for Web Reputation and Web Categorization (as shown in the CPU Usage by Function chart on the System Capacity report page) will not be available after upgrade. If you need to preserve this historic data, export or save the data for the CPU Usage by Function chart as CSV or PDF before you upgrade.

In this release, Web Reputation and Web Categorization data have been combined into a single collation called "Acceptable Use and Reputation."

Current Users of IronPort URL Filters: Upgrade to Cisco IronPort Web Usage Controls

Cisco has announced end-of-life for the IronPort URL Filters service, replacing it with Cisco IronPort Web Usage Controls. This release of AsyncOS for Web no longer supports IronPort URL Filters nor will it receive updates.

If the Web Security appliance currently uses IronPort URL Filters, we advise you to migrate to Cisco IronPort Web Usage Controls. To migrate, you must first obtain a license key for it **before upgrading** to the current version. If you do not yet have a license for Cisco IronPort Web Usage Controls, contact your Cisco sales representative or reseller. After migrating and upgrading, you might need to edit existing policies to use the new URL categories as necessary.

For more information about migrating and obtaining a license, read the following announcement:

http://www.cisco.com/web/ironport/docs/IronPort_URL_Filtering_EoL.pdf

Current Users of Cisco IronPort Web Usage Controls: Prepare for URL Filtering Changes

Note Note There are no changes if the appliance used IronPort URL Filters before upgrading.

The set of URL categories for Cisco IronPort Web Usage Controls changed in AsyncOS 7.5 for Web. If you are upgrading from a pre-7.5 version, these changes may modify or disable existing policies. To understand, prepare for, control, and respond to these changes, see "Managing Updates to the Set of URL Categories" in the "URL Filters" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.

See the 7.5 release notes for a table listing the changes to the set of URL categories that will occur when you upgrade to AsyncOS 7.7 for Web from a pre-7.5 version. For descriptions of the new categories, see the "URL Category Descriptions" section in the "URL Filters" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.

Change the Protocol for Users and Log Subscriptions Configured to Use SSH 1

Support for SSH 1 has been removed for this release. Therefore, before upgrade, you should do the following:

Any remote host keys which use SSH 1 should be changed to SSH 2. Use the logconfig > hostkeyconfig command in the CLI to make this change.

For any log subscriptions that are configured to use SSH 1 as the protocol for SCP log push, choose SSH 2 instead.

Change the access protocol or add a new SSH 2 key for any users configured to use only SSH 1. Use the sshconfig command in the CLI to make this change.

Disable SSH 1 using the sshconfig > setup command in the CLI.

Reporting Data Erasure

When you upgrade from a version of AsyncOS for Web *before* version 7.1, all historical data stored on the Web Security appliance for the on-box reports **will be erased**. To retain this historical data, you must export each report to PDF before upgrading.

Known Issues

Familiarize yourself with known issues and limitations before you upgrade AsyncOS for Web using these resources:

- Current Information about Known and Resolved Issues, page 10
- Known Issues, page 13

Installation and Upgrade Notes

- Post-Upgrade Reboot
- Sending Customer Support Requests through the Appliance, page 6
- Configuration Files
- Compatibility with IronPort AsyncOS for Security Management

- Changes in Behavior

Post-Upgrade Reboot

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

New License Agreement

A copy of the new license agreement is included in the Online Help. To view it, choose **Help and Support > Online Help**, scroll down to the end of the Contents list, and click the link for the license agreement.

Because the license agreement has changed, you may be required to accept the new agreement when you apply new feature keys after upgrading.

Sending Customer Support Requests through the Appliance

A change to Cisco IronPort Customer Support contact methods is currently in a transitional stage. When requested by CSE to send a support request through the Web Security Appliance to open or edit a case, include customercare@ironport.com in the Other Recipients field to ensure your communication is received.

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.

IronPort does not generally support the backward compatibility of configuration files with previous major releases. Minor release support is provided. Configuration files from previous versions may work with later releases; however, they may require modification to load. Check with IronPort Customer Support if you have any questions about configuration file support.

Compatibility with IronPort AsyncOS for Security Management

Features on AsyncOS 7.7 for Web are supported by AsyncOS for Security Management version 8.0. For more information about compatibility between the Web Security appliance and Security Management appliance, see the compatibility matrix in the release notes for the Security Management appliance posted on the Cisco products web site:
http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html

Changes in Behavior

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.

advancedproxyconfig Command

proxystat and rate Commands

The proxystat and rate commands now display the percent of CPU used by the web proxy instead of the percent of CPU being used by all processes.

Defect: 90186, CSCzv71295

Send Buffer Size

AsyncOS now dynamically adjusts the size of the send buffer for the client-side socket. AsyncOS no longer includes the option of the MISCELLANEOUS subcommand of the **advancedproxyconfig** command to configure the size of this buffer.

Defect 90684, CSCzv99595

wccp Command

The advancedproxyconfig>wccp command has been removed from the CLI. See Logging Command Replaced with Web Interface Support, page 8 for more information.

Defect: 85003, CSCzv21217

Opening Support Cases Through the Appliance

When opening a support case using the appliance, the severity level is 3. Previously, users were able to set the severity level using the appliance, either through the CLI command, supportrequest, or through the GUI. To open a support case at a higher severity level, call Customer Support. See Support, page 17.

Defect: 87828, CSCzv13413; 87830, CSCzv25201

Use NTLMSSP Option

For any sequence that contains an NTLM realm, in the Identities GUI, the All Realms and Sequences setting no longer includes the “Use NTLMSSP” option because it is not a valid option. For any sequence that contains an NTLM realm, the GUI now displays only these options for All Realms and Sequences:

- Use Basic or NTLMSSP (default)
- Use Basic

Defect: 92048, CSCzv27778

FTP Proxy Authentication

A third formatting option, No Proxy Authentication, for use when communicating with FTP clients allows for more formatting flexibility. The FTP Proxy now supports the following three formats for proxy authentication:

- **Check Point.** Uses the following formats:
  - User: ftp_user@proxy_user@remote_host
  - Password: ftp_password@proxy_password

- **Raptor.** Uses the following formats:
  - User: ftp_user@remote_host proxy_user
  - Password: ftp_password
  - Account: proxy_password"
- **No Proxy Authentication.** Uses the following formats:
  - User: ftp_user@remote_host
  - Password: ftp_password

Defect: 90467, CSCzv69205

Certificate Error Category Changes

Certificate error categories have changed:

Old Category	New Category	Description
Unrecognized Root Authority	Unrecognized Root Authority/Issuer	Either the root authority or an intermediate certificate authority is unrecognized.
—	Invalid Signing Certificate	There was a problem with the signing certificate, for example, a failure to verify or decrypt the signature. Previously, these errors were included in the “Other Error” category.
—	Invalid Leaf Certificate	There was a problem with the leaf certificate, for example, a rejection, decoding, or mismatch problem. Previously, these errors were included in the “Other Error” category.

Access Log Changes

Access logs now include these entries:

- FTP_CONNECT
- FTP_TUNNEL

See information about enhancements to the Native FTP Proxy in New Features for AsyncOS 7.7 for Web.

Logging and Reporting Changes

Logging Command Replaced with Web Interface Support

The **advancedproxyconfig > wccp** command has been removed, and more robust logging is now available through the web interface. Now, the wccp command has been removed and you can set WCCP logging using logconfig command in the CLI or using Log Subscriptions page in the web user interface. You can use the following log levels:

- Warning. Lists errors.

- Info. Adds configuration information to the level above.
- Debug. Describes flow information in addition to the level above.
- Trace. Describes the current state and state changes in addition to the level above.

Defect: 85003, CSCzv21217

Reporting and Tracking for SOCKS

New support for the SOCKS protocol includes a new SOCKS Proxy report and a new SOCKS Proxy tab in Web Tracking. Read about support for SOCKS Proxy in New Features for AsyncOS 7.7 for Web.

Upgrading AsyncOS for Web

Before You Begin

- Read Pre-Upgrade Requirements, page 4
- Upgrade the appliance to AsyncOS version 7.5.x before upgrading to AsyncOS version 7.7.0.
- If you have limited administrator access based on IP addresses (at System Administration > Network Access), make sure that the list of allowed connections includes the appliance's Management interface IP address.
- Login to the administrator account.

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

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

The page refreshes with a list of available AsyncOS for Web upgrade versions.

Step 3 Click **Begin Upgrade** to start the upgrade process. Answer the questions as they appear.

Step 4 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.

Post-Upgrade Requirement for FIPS Appliances

Upon upgrading from 6.5 or 7.5 on FIPS appliances, AsyncOS generates new host keys. The first attempt to access the appliance via ssh will fail if the old host key remains in the known_hosts file.

Before connecting to the appliance after upgrade, remove the old host key from the known_hosts file. Then, when attempting to connect, accept the new host key.

Defect: 88140, CSCzv77236

Current Information about Known and Resolved Issues

Use the Cisco Software Bug Toolkit to find current information about known and fixed defects.

Before You Begin

Register for a Cisco account if you do not have one: https://tools.cisco.com/RPF/register/register.do.

Procedure

Step 1 Go to http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2 Log in with your Cisco account credentials.

Step 3 (Optional) Query the database for Web Security appliance bugs:

For	Enter This
Product Category	Security
Product(s)	Cisco Web Security Appliance

Step 4 (Optional) Enter a Bug ID number in the "Search for Bug ID" field. Example: CSCzv79153

Note The 5-digit bug numbers used in previous AsyncOS releases cannot be used with this tool.

Step 5 (Optional) Click the Help link on the Bug Toolkit page or visit http://www.cisco.com/web/applicat/cbsshelp/help.html#personalize for information about performing these tasks:

- Save searches
- Create bug groups
- Sign up for notifications

Resolved Issues

Security Vulnerabilities Addressed

Cisco AsyncOS for Web version 7.7.0-608 addresses the security vulnerabilities detailed in this security alert: http://www.cisco.com/en/US/products/csa/cisco-sa-20130626-wsa.html.

Other Resolved Issues

Previous Defect ID	Bug Toolkit ID	Description
90699	CSCzv79153	After uploading a custom root CA, AsyncOS did not recognize the uploaded certificate until the web proxy was restarted. This is fixed.
90467	CSCzv69205	AsyncOS was sending incorrect usernames to the FTP server when all of these conditions were met: • Authentication configured and enabled in Identities • Native FTP exempted from authentication • Username for FTP connection either included the backslash character (\) or it was used to escape a special character in the username. AsyncOS now provides a third formatting option to fix this defect. See FTP Proxy Authentication, page 7.
88970	CSCzv25023	The login banner was failing to appear in the appliance GUI. This is fixed.
87864	CSCzv21851	Decryption failed when connecting to particular sites. This is fixed.
87643	CSCzv21222	When sending non-SSL traffic over SSL port 443, the web proxy sometimes ran out of memory and crashed or restarted. This is fixed.
87314	CSCzv97159	Users who had previously submitted authentication credentials were later unable to access HTTPS websites and were not prompted to authenticate. Conditions: • Decryption enabled • Authentication required • Transparent redirection • IP session caching This is fixed.
86556	CSCzv57040	The Appliance sometimes responded to an HTTPS file upload request with a 504 Gateway Timeout. Conditions: • The HTTPS proxy was enabled • The upload file included this header: "Transfer-encoding: chunked" This is fixed.
86549	CSCzv43726	Attempts to generate a Web Tracking report in PDF format resulted in an application fault if the report data included very long URLs. This is fixed.
86529	CSCzv94982	Time zone setting updates updated components unrelated to time zone.Clicking the **Update Now** button in the Time Zone File Updates section of the System Administration > Time Settings page updated all components (WBRS, Sophos, etc.), not just the time zone settings. This issue also occurred when using the tzupdate command in the CLI. This is fixed.
86394	CSCzv59884	Using the **authcache - list** command was resulting in an application fault when the username included non-ascii characters. This is fixed.
86109	CSCzv21811	SSH 1 is an obsolete and nonsecular protocol and is no longer an option for SCP push on the Log Subscriptions page or in the CLI logconfig command. SSH2 is the default protocol.

Previous Defect ID	Bug Toolkit ID	Description
85964	CSCzv91287	Download time for Web Tracking data in CSV format was excessive when specifying a custom time range for the report. This is fixed.
85383	CSCzv21238	Although support for Secure Sockets Layer (SSL) version 2 was removed from AsyncOS, client to proxy communication still allowed for SSL version 2. Client to proxy requests using SSL version 2 now fail, which is the expected behavior. This is fixed.
85085	CSCzv56404	The Status command was reporting incorrect system resource values. This is fixed.
84195	CSCzv73908	Transaction requests were sometimes resulting in HTTP 503 errors due to DNS caching problems. This is fixed.
83666	CSCzv68184	With Safe Search enabled, for URLs that included a question mark (?) in the first position after the domain name, for example, "example.com/?abc", transaction requests were resulting in an HTTP 404 error message. This is fixed.
83479	CSCzv78744	When the disk reported a high temperature, AsyncOS was sending out frequent, redundant alerts. This is fixed.
82946	CSCzv27807	Non-UTF-8 characters in transaction header fields were resulting in unnecessary UTF-8 errors on the appliance. This is fixed.
82857	CSCzv85035	External authentication failed with a Juniper SBR RADIUS server when RADIUS users were mapped to different Web Security appliance user role types using a RADIUS CLASS attribute. This is fixed.
82809	CSCzv44630	Host Header spoofing in HTTP and HTTPS Requests was not prevented. Now, there is a CLI option in `adminaccessconfig` to allow only hostnames/IP addresses of existing interfaces. This allows restricting specific machines to a specific domain name. By default, this option is disabled.
82780	CSCzv58956	Expired certificates were sometimes not detected by the appliance due to the order in which AsyncOS checked for errors and different actions assigned to different types of errors. AsyncOS now checks for all errors and applies the most restrictive action that applies.
82662	CSCzv27661	SNMP erroneously returned appliance information from the previous version of AsyncOS after upgrading. This is fixed.
82415	CSCzv95909	Large Objects were taking too long to load in some cases when the client made a universal range request. This is fixed.
81661	CSCzv78679	On Appliances using WebRoot scanning, requests for web pages that included javascript were sometimes taking too long. This is fixed.
81156	CSCzv95258	Attempting to navigate from Web Security Manager to the Outbound Malware Scanning page was, in rare cases, producing an application fault. This is fixed.
81055	CSCzv50828	Processing client requests sometimes took too long after updating new anti-malware rules.This is fixed.
77935	CSCzv40418	The Dynamic Content Analysis engine was erroneously overwriting the effective category used in policy decisions for new requests. This is fixed.
76250	CSCzv13897	**Requires change to the user guide -- the new mask functionality. Network>Transparent Redirection> WCCP> Service > Advanced > Load Balancing.**
73467	CSCzv63552	Rebooting the appliance without proper shutdown sometimes caused irreparable damage to the appliance. This is fixed.

Previous Defect ID	Bug Toolkit ID	Description
71012	CSCzv42816	**Fixed: Clients cannot connect to HTTPS servers that do not support TLS Hello during the SSL handshake.** Previously, clients could not connect to HTTPS servers that did not support TLS Hello during the SSL handshake. This is fixed.
70224	CSCzv66892	Added CLI command: date.
42512	CSCzv83549	**Fixed: Web Proxy cannot process server responses with extremely large HTTP headers** Previously, the Web Proxy could not process server responses with extremely large HTTP headers. This no longer occurs.

Known Issues

Bug Toolkit ID	Description
CSCuf34778	AsyncOS fails to proxy HTTP, HTTPS, FTP-Over-HTTP requests under these conditions: • Credential Encryption enabled AND • Basic authentication AND • Identity: All protocols, no surrogates, authentication required Workaround: “Edit” the Identity without actually changing it. Submit and commit.
CSCuf51391	AsyncOS allows the Security Management appliance to publish an Identity with SOCKS policies configured to the Web Security appliance when SOCKS is disabled on the Web Security appliance. Workaround: Match the SOCKS enabled/disabled setting on the Security Management appliance with those on the Web Security appliance.
CSCuf51729	Surrogate settings for Global Identity are disabled after publishing Configuration Master 7.7. This issue occurs when there is a mismatch in SOCKS proxy configurations on WSAs and SMA. Workaround: Disable/enable SOCKS Proxy on SMA to match settings on WSAs before publishing configurations.
CSCuf56258	An application fault occurs under these conditions: • On the SOCKS Policy Edit Page, a user selects Authorized Groups or Users AND • The SOCKS Policy is based on an Identity with custom or predefined URL Categories.

Bug Toolkit ID	Description
CSCuf85838	AsyncOS fails to decrypt HTTPS traffic from specific sites under these conditions: • The HTTPS Server asks for the client certificate AND • The Server Certificate is invalid AND • The appliance is configured to decrypt traffic when the server certificate is invalid AND • The appliance is configured to pass through traffic when the HTTPS Server asks for a client certificate. Workaround: Add the site to a custom URL category, and set the action to pass through.
CSCzv79284	For SOCKS UDP transactions, CPU usage may increase to 100% if DNS cannot resolve the domain name to a valid IP address.
CSCzv07140	AsyncOS fails to prevent the creation of invalid identities in under these conditions: • SOCKS Proxy is disabled on the Web Security appliance • SOCKS Proxy is enabled on the Security Management appliance • User creates a custom identity using the Security Management appliance that defines members based only on the SOCKS protocol. The custom identity is invalid.
CSCzv59181	The SCP push command fails with the message "invalid characters in scp command!" under these conditions: • scponly shell • filename includes the "@" character Workaround: Use a different shell to run the SCP push command.
CSCzv87357	SNMP - AsyncOS returns wrong interface speed (ifSpeed) value when Auto negotiation is used. Workaround: Set fixed speed and duplex values for affected interface using the command line interface: etherconfig>media>edit.
CSCzv80840	Upgrading to AsyncOS version 7.5 and above removes administrator IP address restrictions that were previously configured using the adminaccessconfig>ipaccess CLI command. After upgrade, all IP addresses are allowed for administrator access. Workaround: After upgrading, use the adminaccessconfig>ipaccess CLI command to reconfigure administrator IP address access constrictions.
CSCzv08939	After upgrading to 7.5.1, you may not be able to see, add, or edit excluded custom categories in the URL Filtering column of the Access Policies page. Workaround: 1. Navigate to Web Security Manager>Identities. 2. Click the link for the related identity. 3. Submit and commit without making changes.

Bug Toolkit ID	Description
CSCzv15210	After upgrading to this release, clicking on **Security Services > Acceptable Use Controls** may result in continual page refreshing. Workaround: Clear the browser cache. Use CTRL+R/Command+R to refresh the page.
CSCzv90385	Reverting to an older version of AsyncOS results in the loss of realm membership to the domain. Workaround: After reverting the software version, join the realm to the domain again.
CSCzv95795	Rarely, AsyncOS stops performing normal operations. For example, it may stop logging activities, may stop accepting new connections, and it may not allow logins. Workaround: Reboot the appliance.
CSCzv87294	Attempt to send dig SSH command to TTY triggers a traceback. This issue occurs when including a dig command directly in the SSH login string. Workaround: Use -t in the string. For example: user1$ ssh -t admin@192.0.2.0 'dig @198.51.100.0 www.yahoo.com'
CSCzv30028	These reportingconfig > counters settings are not preserved after upgrading or after using saveconfig, resetconfig, and loadconfig: • 2. Minimally Limited Reporting Data. • 3. Moderately Limited Reporting Data.
CSCzv84704	AsyncOS does not display End User Acknowledgements (EUAs) or End User Notifications (EUNs) that are larger than 16K. Workaround: Reduce the size of EUAs and EUNs to less than 16K.
CSCzv32093	When Adaptive Scanning is enabled, access logs that use the custom field %:<s provide an incorrect value for the time it takes to receive the verdict from the Web Proxy anti-spyware process.
CSCzv25707	Upgrading AsyncOS on the appliance using the web interface results in an application fault if the list of allowed connections does not include the appliance's Management interface IP address. Workaround: Go to **System Administration > Network Access** and add the appliance's Management interface IP address to the list of allowed connections.
CSCzv18801	Attempting to modify the time range for an access policy results in an application fault if Acceptable Use Control is disabled. Workaround: Enable Acceptable Use Control and then modify the time range for the Access Policy.
CSCzv87130	Creating a domain and then failing to join the domain causes a daemon to restart repeatedly, which results in repeated logging of the daemon restart event, which results in log files filling up and rolling over. Workaround: Either join the domain or delete the domain.
CSCzv27676	Attempt to join a domain fails if AsyncOS cannot resolve the name of the Active Directory server to which you are trying to connect, and the AsyncOS error message does not clearly identify the problem. Workaround: Add both the fully qualified domain name and the IP address for the Active Directory server to which you are trying to connect.

Bug Toolkit ID	Description
CSCzv39361	The index feature in online help for Cisco Security Appliances is not intuitive. As you type a term in the index field, the online help software highlights the first matching term in the list of index terms; pressing Enter does not take you directly to the related topic in the book. Instead it pops up an instruction to click on the highlighted term to go to the topic in the book. Workaround: In the list of index terms, click on a term to go to the related topic in the book.
CSCzv86403	With Transparent User Identification (TUI) and Active Directory agent, users who have recently authenticated may need to re-authenticate at frequent intervals.
CSCzv06278	The online help index does not work properly in Safari browsers. Searching the index results in a pop-up box that cannot be permanently dismissed using the Enter key. Workaround: Dismiss the pop-up box with a mouse click or use a different browser.
CSCzv86357	AsyncOS fails to authenticate users through LDAP if UTF-8 characters are used in the Bind DN or Base DN.
CSCzv58857	The SOCKS proxy does not support SaaS single sign-on. Workaround: Send SaaS traffic through the HTTP or HTTPS proxy.
CSCzv95175	Web interface stops responding after entering some regular expressions with trailing context patterns in a custom URL category. This is a known issue with the Flex, the application that AsyncOS for Web uses to analyze regular expressions. For more information on this limitation, go here: http://flex.sourceforge.net/manual/Limitations.html#Limitations
CSCzv03044	When the appliance is configured to warn end-users about explicit content, AsyncOS displays an End-User Notification warning about explicit content for sites that allow explicit content even if the site does not actually include explicit content. While this feature is working as designed, it may be a confusing outcome because the text in the web interface for the appliance implies that AsyncOS will only display an End-User Notification warning for explicit content if the site actually includes explicit content. In fact, end-users receive the warning if the site allows explicit content.
CSCzv46190	Attempting to delete a PAC file may result in misidentification of the file as the default PAC file. This can happen if the name of the default PAC file includes special characters. Workaround: Don't use special characters in PAC file names.
CSCzv17778	AsyncOS and some browsers determine the root CA for each site using different processes, which may result in discrepancies. Discrepancies may lead to unexpected results when attempting to black list sites.
CSCzv50704	Web Security appliance performance is affected when the Default Proxy Logs are configured at debug or trace logging level. Workaround: Change the logging level of the Default Proxy Logs to something higher than Debug, such as Information.
CSCzv36346	Running logconfig from the CLI and choosing 'Request Debug Logs' causes logging and reporting to fail.
CSCzv36740	Occasionally, network traffic moves faster than AsyncOS can accept the packets, and the network adapter drops some packets.

Bug Toolkit ID	Description
CSCzv56650	Overriding the application type bandwidth limit for a particular application does not work . When you define a bandwidth limit for an application type and then override that limit by choosing no bandwidth for a particular application in that application type, the Web Proxy erroneously still applies the defined bandwidth limits to the application.
CSCzv69285	In deployments using WCCP, users who exceed the maximum number of entries allowed for Ports to Proxy experience failures with IPFW rules and do not receive an alert from the appliance. The maximum number of port entries is 30 for HTTP, HTTPS, and FTP ports combined. Workaround: Reduce the number of port entries to fewer than 30 for HTTP, HTTPS, and FTP ports combined.
CSCzv60471	Certain browsers, including Firefox version 3 and Internet Explorer version 8, may display their native error page instead of displaying the End-User Acknowledgement or End-User Notification page configured through the appliance. Conditions: • Protocol is HTTPS • Decryption is not enabled on the appliance. Workaround: Enable decryption.

Related Documentation

The documentation for the Cisco IronPort Web Security appliance includes the following books:

- *Cisco IronPort AsyncOS for Web User Guide*

Support

Knowledge Base

You can access the Cisco IronPort Knowledge Base on the Cisco IronPort Customer Support site at the following URL:

http://www.cisco.com/web/ironport/knowledgebase.html

Note You need a Cisco.com User ID to access the site. If you do not have a Cisco.com User ID, you can register for one here: https://tools.cisco.com/RPF/register/register.do

The Knowledge Base contains a wealth of information on topics related to Cisco IronPort products.

Articles generally fall into one of the following categories:

- **How-To.** These articles explain how to do something with a Cisco IronPort product. For example, a how-to article might explain the procedures for backing up and restoring a database for an appliance.

- **Problem-and-Solution.** A problem-and-solution article addresses a particular error or issue that you might encounter when using a Cisco IronPort product. For example, a problem-and-solution article might explain what to do if a specific error message is displayed when you upgrade to a new version of the product.
- **Reference.** Reference articles typically provide lists of information, such as the error codes associated with a particular piece of hardware.
- **Troubleshooting.** Troubleshooting articles explain how to analyze and resolve common issues related to Cisco IronPort products. For example, a troubleshooting article might provide steps to follow if you are having problems with DNS.

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 and Cisco IronPort users.

Access the Cisco Support Community at the following URL:

- For web security and associated management:

  https://supportforums.cisco.com/community/netpro/security/web

Customer Support

Use the following methods to obtain support:

U.S.: 1 (408) 526-7209 or Toll-free 1 (800) 553-2447

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

Support Site: http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.