Release Notes for Cisco IronPort AsyncOS for Web 7.5.2-118

Published: September 30, 2013

Contents

This document contains release information for running Cisco IronPort AsyncOS 7.5.2 for the Web Security appliance, and includes the following sections:

Upgrade Paths

You can upgrade to release 7.5.2-118 from the following versions:

- 6.3.0-604
- 6.3.1-025
- 6.3.3-015
- 6.3.5-015
- 6.3.8-005
- 7.0.0-819
- 7.1.0-306
- 7.1.0-307

Cisco Systems, Inc.
www.cisco.com

- 7.1.1-027
- 7.1.1-038
- 7.1.2-080
- 7.1.3-014
- 7.1.3-021
- 7.1.3-031
- 7.1.3-033
- 7.1.4-053
- 7.1.4-101
- 7.5.0-703
- 7.5.0-833
- 7.5.0-838
- 7.5.1-079
- 7.5.1-085
- 7.5.1-201
- 7.5.1-230
- 7.5.2-113

Note Version 7.5.2 is not compatible with Web Security Appliances with FIPS hardware. Do not upgrade your Web Security Appliance with FIPS hardware to this version.

To ensure a successful upgrade, before installing this update, read the "Installation and Upgrade Notes" section on page 2.

Installation and Upgrade Notes

Read through and consider the installation and upgrade impacts listed in this section.

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.

Note You must be logged in as the admin to upgrade. Also, you must reboot the Web Security appliance after you upgrade AsyncOS for Web.

Warning **Before installing AsyncOS for Web on some S160 appliances, you must install the hard drive firmware upgrade on the appliance. To verify whether or not 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.**

Security Vulnerabilities Addressed

Cisco AsyncOS for Web version 7.5.2-118 addresses the security vulnerabilities detailed in this security alert: http://www.cisco.com/en/US/products/csa/cisco-sa-20130626-wsa.html.

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.

End-of-Life Announcement

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 on migrating and obtaining a license, read the following announcement:

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

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

Review the known issues associated with this release. See "Finding Current Information about Known and Fixed Issues: Bug Search Tool" section on page 22.

Configuration Files

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

Compatibility with AsyncOS for Security Management

Features on AsyncOS 7.5.2-118 for Web are only supported by AsyncOS for Security Management version 7.9.1 HP3 and above. The reverse is also true: AsyncOS for Security Management version 7.9.1 HP3 is only compatible with AsyncOS 7.5.2-126. 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

New Features

Caching for Syslog Push Log Subscriptions

You can now use the logconfig command to configure a local disk buffer for a syslog push log subscription to allow AsyncOS to cache log events when the remote syslog server is unavailable. When the syslog server becomes available, AsyncOS begins sending all the data in the buffer for that log subscription to the syslog server.

Before You Begin

- Create the syslog push log subscription (use TCP for transport) if it does not already exist.
- Ensure the syslog server is running before starting this procedure to avoid log data loss.
- Determine the size of the local disk buffer, allowing enough space to accomodate the maximum expected period of down time for the syslog server. This avoids loss of log data.
- If you have a secondary log subscription for local retention, Cisco recommends you cancel the secondary subscription to allow space for the local disk buffer for the primary subscription.
- Be aware that AsyncOS may not be able to cache the first several seconds of log data after loss of connection to the syslog server. This is due to characteristics of syslog over TCP.
- Allow a buffer initialization period of 10 minutes per 50 GB of disk buffer size before sending data to the Web Security Appliance.

Step 1 Use the logconfig CLI command to edit the syslog push log subscription:

```
mail3.example.com> logconfig

Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- HOSTKEYCONFIG - Configure SSH host keys.

[]>edit
```

Step 2 Identify the log subscription by number.

Step 3 Accept the existing values for these options:

- Log name
- Log style
- HTTP Error Status Codes

- Method to retrieve the logs (Syslog Push is the only applicable method)
- Hostname to deliver the logs

Step 4 Change the transfer protocol to TCP if it is set to UDP. Otherwise accept TCP.

Step 5 Accept the existing value for these options:

- Send facility

Step 6 Enable the disk buffer:

Enable syslog disk buffer (yes/no)

[no]> yes

Step 7 Set the syslog disk buffer size (in bytes, in multiples of 1024) or accept the default value of 100M:

Syslog disk buffer size (in bytes)

[100M]>

Example values: 10G, 10485760, 20M

Step 8 Commit your changes.

Related Documentation

- AsyncOS CLI Reference Guide

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.

Webroot Body Scanning

You can now disable Webroot body scanning using the advancedproxyconfig scanning subcommand.

Defect: CSCzv78679

WCCP Related Commands

In AsyncOS for Web 7.5, the advancedproxyconfig > wccp command no longer exists. Now, you use the web interface to change the logging level of the WCCP Module Logs. 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: 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 Customer Support, page 23.

Defect: CSCzv13413, CSCzv25201

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: CSCzv71295

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: CSCzv69205

Send Buffer Size

AsyncOS now dynamically adjusts the size of the send buffer for TCP connections. This is the new default behavior. There is an option to disable this behavior and use static TCP send buffer size for all connections, which is available under the CLI advancedproxyconfig command.

To disable dynamic adjustment of the send buffer size, respond “no” to this advancedproxyconfig command question: Would you like proxy to perform dynamic adjustment of TCP send window size?

Defect: CSCzv99595

Upgrading AsyncOS for Web

.**Before You Begin**

- 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.

Step 1 Login to the appliance using an administrator account.

Step 2 On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.

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

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

Step 4 Click **Begin Upgrade** to start the upgrade process. Answer the questions as they appear.

Step 5 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.

Resolved Issues in This Release

Table 1 Resolved Issues in This Release

Reference Number	Description
CSCuf35134	Access Log Subscription with Syslog Push not buffering data (See Caching for Syslog Push Log Subscriptions, page 4)
CSCug04470	Proxy (and every other) watchdog timer is a one time only event
CSCug17048	Upgrade from 7.5 to 7.7 fails with certain configuration
CSCug35548	WSA not extracting correct client IP from XFF header
CSCug43543	W3C log field %Y incorrectly logging HTTP version
CSCug67323	HTTPS certificate expiry alerts not generated correctly
CSCug74881	High bit characters in PAC file breaks GUI
CSCug80134	Proxy crashes when we try to use 2nd realm set up in Authentication/TUI
CSCug85543	SNMP sends incorrect OID values for traps
CSCuh01348	Proxy crashes in UDS RPC code: Transparent User Identification
CSCuh56403	DNS Application Fault with unresponsive local DNS server
CSCui45649	Upload performance degrades on upgrading from 7.5.0
CSCui48172	SNMP - upstreamProxyFailure trap is unusable - incomplete WSA AsyncOS MIB
CSCzv24465	Adaptive scanning is unusable by some customers

Table 1 Resolved Issues in This Release (continued)

Reference Number	Description
CSCzv37800	Scanning performance issues when Adaptive Scanning is enabled
CSCzv57081	WSA not failing over to active mode if FTP servers reply with private IP
CSCzv58669	WSA - Management GUI Denial of Service Vulnerability
CSCzv69294	Authenticated Command Injection Vulnerability
CSCzv69390	Designated web-cache constantly sends RA when 2 or more WSAs in WCCP
CSCzv75642	KeyInfo missing in SAMLResponse
CSCzv78978	SNMP fan alerts on 7.5
CSCzv79153	Uploaded custom root CA not recognized until proxy is restarted
CSCzv80840	adminaccessconfig -> ipaccess settings are lost on upgrade
CSCzv85726	Authenticated command injection vulnerabilities on GUI pages
CSCzv85727	WSA incorrectly throws away requests with a redirect when name begins with a digit
CSCzv91509	WSA sending alerts about updater application faults
CSCzv91837	WSA is failing to apply wbrs updates after upgrade

Known Issues in This Release

New Issues

Issues discovered recently are available using the process described in Finding Current Information about Known and Fixed Issues: Bug Search Tool, page 22.

Legacy Issues

Issues discovered in previous releases that also occur in this release:

Table 2 Known Issues for AsyncOS 7.5.2 for Web

Legacy Defect ID	New Defect ID	Description
	CSCui79449	AsyncOS my display an erroneous Application Fault alert while while making syslog related changes to logs. This can include changing the buffer size, disabling the buffering feature, or switching the log retrieval method from syslog to a different method. This erroneous alert is characterized by the presence of this string toward the end of the message: _buffer_reader. You can safely ignore this alert.
—	CSCui45649	Upload performance in this release is slower than upload performance in 7.5.0 Upload performance in 7.5.2 is better than upload performance in 7.5.1, but is still slower than upload performance in 7.5.0.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
91280	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.
91277	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.
91072	CSCzv18769	AsyncOS does not log HTTP 307 requests in the access logs if all of these conditions are met: 1. Transparent user identification (TUI) 2. Transparent redirection 3. Authentication required with no guest access 4. Active Directory agent fails to identify the transaction. These unlogged transactions are also not included in the statistics returned by the rate command. Note: The end client receives the 307 redirect.
91054	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.
90361	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.
89987	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'
89756	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.
89724	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.
88960	CSCzv81174	Client session may stall if an HTTP response includes an incorrect value in the content-length header.(The header may report the uncompressed size of a compressed file, for example.)
88753	CSCzv86403	With Transparent User Identification (TUI) and Active Directory agent, users who have recently authenticated may need to re-authenticate at frequent intervals.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
87282	CSCzv76331	Backing up and restoring the certificates and keys using the FIPS management console does not work as expected under the following conditions: • A certificate and key pair to access the web interface is uploaded to the HMS card. • The SaaS Single Sign On certificate and key pair is uploaded to the HMS card. • Back up and restore the certificates and keys stored on the HMS card. When the certificates and keys are restored, the web interface certificate and key is replaced with the SaaS Single Sign On certificate and key. Workaround: After restoring the certificates and keys, upload the correct certificate and key to access the web interface using the `certconfig` CLI command.
86620	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
86558	CSCzv42050	The appliance cannot establish a secure support tunnel when the secure tunnel host name is not DNS resolvable. Workaround: Make sure the secure tunnel hostname is DNS resolvable.
86326	CSCzv81635	The FTP Proxy prematurely closes an FTP control connection under the following circumstances: • Cisco IronPort Data Security Filters is disabled. • An FTP client uploads a file that is blocked by an Outbound Malware Scanning policy due to the presence of malware. This may be a problem if a script attempts to upload multiple files using native FTP using a single control connection. Workaround: Enable Cisco IronPort Data Security Filters. Or, only upload a single file per control connection.
84487	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.
84304	CSCzv36346	Running logconfig from the CLI and choosing 'Request Debug Logs' causes logging and reporting to fail.
84178	CSCzv95787	When the HTTPS Proxy is enabled, transparent HTTPS traffic is always logged as decrypted when authentication is required and a Routing Policy applies. Note that the HTTPS traffic is passed through, decrypted, or dropped as configured.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
83098	CSCzv91782	Users may get prompted to enter authentication credentials when transparent user identification is enabled and a client application sends invalid user credentials in a Proxy-Authorization HTTP header in its initial transaction request. These unsolicited user credentials are sent before the Web Proxy requests authentication information. When a client sends unsolicited user credentials, the Web Proxy uses the credentials in the Proxy-Authorization HTTP header instead of using transparent user identification to obtain the identity. If the credentials in the HTTP header are invalid, users are prompted to enter credentials instead of being identified transparently.
82857	CSCzv85035	External authentication fails with a Juniper SBR RADIUS server when RADIUS users are mapped to different Web Security appliance user role types using a RADIUS CLASS attribute. Workaround: When using a Juniper SBR RADIUS server, use the "Map all externally authenticated users to the Administrator role" option to map all RADIUS users to the Administrator user role type on the Web Security appliance.
82852	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.
82244	—	Users who make uploads (POST requests) in Internet Explorer with cookies used as the authentication surrogate see an Internet redirection message in the web browser notifying them that they are being redirected to a different site. This is because the Web Proxy must redirect explicit connections to the Web Proxy itself using a 307 HTTP response in order to set the cookie as the authentication surrogate. This is a known issue with Internet Explorer. Workaround: Users can click Yes in the redirection message window to continue and they will be directed to the originally requested website after the Web Proxy sets the cookie. Or, to prevent users from seeing the redirection message, you can configure Internet Explorer to not show a message in this circumstance by disabling the "Warn if POST submittal is redirected to a zone that does not permit posts" option. Typically, this option is found in Tools > Internet Options > Advanced.
82093	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.
82082	CSCzv36389	The ERR_SAML_PROCESSING notification page does not use variables correctly. If you customize the ERR_SAML_PROCESSING on-box notification page, you can only use the variable %s to represent the username and %E to represent the logo.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
81667	—	Identity Provider Signing Certificate and Key are not restored in the FIPS management console after reverting to a previous release of AsyncOS for Web in some cases. The configured Identity Provider Signing Certificate and Key does not restore when you complete the following steps: 1. In the FIPS management console, you upload an Identity Provider Signing Certificate and Key. 2. You back up the certificates and keys in the FIPS management console. 3. You upgrade AsyncOS for Web. 4. After upgrading, you revert AsyncOS for Web to the previous version. 5. You restore the certificates and keys in the FIPS management console. Workaround: In the FIPS management console, upload the Identity Provider Signing Certificate and Key again.
81243	CSCzv57964	Users cannot access HTTPS sites under the following conditions: • The Web Proxy is deployed in explicit forward mode. • Credential Encryption is enabled. • The authentication surrogate is IP address. • Users access an HTTPS site before any HTTP site using Internet Explorer 7 or a later version.
80638	—	Users cannot re-authenticate as a different user when blocked by URL category using Internet Explorer in some cases. When a user is blocked by URL category and clicks the re-authentication link on the end-user notification page to log in as a different user, the web browser does not prompt to enter user credentials under the following conditions: • The Web Proxy is deployed in explicit forward mode. • The web browser used is Internet Explorer. • The proxy server port configured on Internet Explorer is a port other than port 80. Instead, Internet Explorer displays an error message saying the page cannot be displayed. Workaround: Edit either the Redirect Hostname configured on the appliance or the proxy server information in Internet Explorer so that they use different values. They should reference the Web Security appliance, but use slightly different hostname values. For example, you can use the fully qualified domain name in Internet Explorer, but just use the hostname for the Redirect Hostname on the appliance.
79535	CSCzv21565	System Capacity reports and logs may show CPU activity for Web Reputation and Web Categorization when those features are disabled. This is because these measures also include activity related to other services.
79488	—	When you include the %k format specifier as a custom field in the Access logs, the access log entry displays 255.255.255.255 when the object was served from the cache.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
78517	—	Some FTP clients may time out and close the connection with the FTP Proxy early when uploading very large files and IronPort Data Security Policies are enabled. This results when the FTP Proxy requires more time to upload the file to the FTP server and the connection between the FTP client and the FTP Proxy has been idle for more than the configured time on the FTP client. Note that the FTP Proxy correctly uploads the file to the FTP server even if the FTP client closes its connection with the FTP Proxy. Workaround: Increase the appropriate idle timeout value on the FTP client.
77286	—	Cannot change directory using a relative path with native FTP in some cases. When you enter a maximum path size for the FTP server directory that is less than 1024 (using `advancedproxyconfig > nativeftp` command), users cannot change the directory using a relative path such as "cd .." . Workaround: Use the `advancedproxyconfig > nativeftp` CLI command and change the maximum path size for an FTP server directory to a value equal to or greater than 1024. Or, to go to the desired directory, specify the absolute path in the FTP client.
76210	—	Traceback generated after technical support tunnel fails for reasons related to DNS. When attempting to establish a secure tunnel through which Cisco technical support can connect to the Appliance, if the tunnel attempt fails for reasons related to DNS, AsyncOS generates a traceback.
73151	—	The Web Proxy erroneously returns the "Policy: URL Filtering" end-user notification page instead of the "DNS Failure" page when there is a DNS failure and uncategorized URLs are set to Block.
72798	—	Clients are continually prompted to authenticate when using Internet Explorer to access servers that require authentication when NTLM authentication is enabled on the appliance. This is a known issue with Internet Explorer. Workaround: Read the following Microsoft support article for more information: `http://support.microsoft.com/?scid=kb;en-us;820780&x=6&y=10` Or, use Internet Explorer 9 on Windows 7.
72332	—	The Filter by User-Requested Transactions option on Web Tracking report erroneously includes transactions that were not requested by the user. Workaround: Ignore the results in the Filter by User-Requested Transactions option. In a future release, this filter will no longer be available.
71992	—	PAC file hosting does not work with a configured VLAN. When a VLAN is configured on the P1 network interface, and you host a PAC file on the Web Security appliance, AsyncOS only listens for PAC file requests on the P1 interface IP address, not the VLAN IP address.
71912	—	Google Talk clients cannot successfully log into Google Talk under the following conditions: • The Web Proxy is deployed in explicit forward mode. • The HTTPS Proxy decrypts the Google Talk traffic. • The Access Policy applied to the Google Talk transaction is not configured to use port 5222 as an HTTP CONNECT Port. Workaround: Edit the Access Policy that applies to Google Talk transactions and add port 5222 as an HTTP CONNECT Port.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
71012	—	Clients cannot connect to HTTPS servers that do not support TLS Hello during the SSL handshake. Workaround: If the Web Proxy is deployed in transparent mode, use the proxy bypass list to bypass the Web Proxy for these websites. If the Web Proxy is deployed in explicit forward mode, use a custom URL category and a Decryption Policy to pass through traffic to these websites, and verify the option "Would you like to block tunneling of non-SSL transactions on SSL Ports?" is disabled.
70370	—	Users cannot log into MSN Messenger from Mac OS X when the Web Proxy is deployed in explicit forward mode.
70369	—	Users cannot log into MSN Messenger from Mac OS X when decryption is enabled.
70038	—	Data does not fit in table cell in reports exported to PDF in some cases. When you display all columns in a report and print the report to PDF, the data in some columns do not fit in the table cell.
69379	—	The Policy Trace feature erroneously lists "Global Access Policy" instead of "Global Routing Policy" when the transaction matches Global Routing policy.

68993	—	The Web Proxy erroneously processes some URLs in client requests as the SaaS single sign-on (SSO) URL under the following conditions:
		• The URL in the client request matches the SSO URL of a configured SaaS Application Authentication Policy, but contains extra characters at the end.
		• The URL in the client request matches the SSO URL of a configured SaaS Application Authentication Policy, but some characters in the URL after "SSOURL/" use a different case than the application name in the configured policy. For example, the client request URL is "http://idp.example.com/SSOURL/WebEx" and the application name in the policy group is "webex".
		When users try to navigate to the wrong URLs, they are directed to a page with the following error message:
		`Error response`
		`Error code 404.`
		`Message: Not Found.`
		`Reason: None.`
		Workaround: Ensure all users trying to access SaaS applications using the SSO URL use the correct URL with the correct case and with no additional characters.

68988	—	Disabled SaaS Application Authentication Policy is erroneously editable when disabled in some cases. When you disable a SaaS Application Authentication Policy using Internet Explorer 7, some fields are still configurable instead of being grayed out.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
68555	—	Web Proxy does not handle POST requests properly with authentication required in some cases. When the user's first client request is a POST request and the user still needs to authenticate, the POST body content is not passed to the web server. When users need to authenticate, the client is redirected to the Web Proxy for authentication purposes. However, during this process, the POST body content is lost. This might be a problem when the POST request is for a SaaS application with the SaaS Access Control single sign-on feature in use. Workaround: Verify users request a different URL through the browser and authenticate with the Web Proxy before connecting to the web server. Or, you can bypass authentication for the server domain name. When working with SaaS Access Control, you can bypass authentication for the Assertion Consumer Service (ACS) URL configured in the SaaS Application Authentication Policy.
68411	—	AsyncOS is unable to join an Active Directory domain when an embedded special character is in the short domain name.
68246	—	Users cannot connect to WebEx Connect with HTTPS decryption enabled. When the HTTPS Proxy decrypts WebEx Connect traffic, users cannot log into WebEx Connect. Workaround: Pass through traffic intended for ".webexconnect.com" using a custom URL category.
67460	—	Web interface does not show changed update server settings in some cases. When you use the `updateconfig` CLI command to change the update server, the new server does not appear in the web interface on the System Administration > Upgrade and Update Settings page. Workaround: Ignore the value in the web interface, and instead use the CLI to view and edit the settings.
55958	—	When an Access Policy is configured to block Microsoft Office files by MIME type, the Web Proxy does not block Microsoft Office 2007 files.
55005	—	FTP clients create a zero byte file on the server machine when the FTP Proxy blocks an upload due to outbound anti-malware scanning.
54636	—	Users cannot access FTP servers that require server authentication using FTP over HTTP with Internet Explorer. This is a known issue with Internet Explorer when communicating with web proxies. This is due to Internet Explorer never prompting users to enter the server authentication credentials. Workaround: To access FTP servers that require server authentication, use one of the following workarounds: • Use a different browser, such as FireFox or Chrome, to access the FTP server. • Use an FTP client that uses native FTP to access the FTP server. • If users must use Internet Explorer, they can prepend the username and password into the URL. For example: ftp://USERNAME:PASSWORD@ftp.example.com
53869	—	Not all data in a native FTP transfer is uploaded with external DLP enabled in some cases. When uploading a 2 GB file using native FTP with external DLP enabled, not all data is uploaded to the server when the external DLP server is Vontu Web Prevent version 9.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
51514	—	Deleting directories on the appliance causes errors when saving or loading a configuration file or when upgrading AsyncOS for Web. Errors occur under the following circumstances: • An administrator connects to the Web Security appliance using FTP and deletes some directories, such as directories that exist for holding log files. • The configuration is saved or loaded, or AsyncOS for Web is upgraded. Workaround: Recreate all missing directories on the appliance before saving or loading the configuration file and before upgrading AsyncOS for Web.
51433	—	The Web Security appliance sends the authenticated user name (X-Authenticated-User value) to external DLP servers in a format that is not compliant with the ICAP RFC. For some DLP vendors, such as Vontu, this may adversely affect reports or user name based policies.
50219, 50995	—	IronPort Data Security scanning is bypassed under the following circumstances: • The client machine uses Adobe Flash version 10 and the client browser is configured to explicitly forward transactions to the Web Security appliance. • Users upload files to some websites, such as Flickr and Gmail (attachments), and the total upload size exceeds the minimum scanning threshold. This is a problem with Adobe Flash. Flash version 10 allows these websites to ignore the configured proxy settings in the browser and instead causes transaction to bypass the Web Proxy. Workaround: Deploy the Web Security appliance in transparent mode, or deploy the Web Security appliance in explicit forward mode and disallow direct access to port 80 on the firewall.
49677	—	Web interface does correctly validate some IronPort Data Security Policies values in some cases. When the minimum request body size for the IronPort Data Security Filters is set to a value other than the default value of 4 KB, the web interface erroneously performs the following: • Prevents you from defining a maximum file size in the IronPort Data Security Policies less than 4 KB when the minimum request body size is less than 4 KB. • Allows you to define a maximum file size in the IronPort Data Security Policies with a value that is less than the minimum request body size when the minimum request body size is greater than 4 KB.
49593	—	FTP clients create a zero byte file on the client machine when the FTP Proxy blocks a download due to anti-malware scanning.
49505	—	Upload requests of 1 GB and greater are not blocked in some cases. When an IronPort Data Security Policy is configured to block HTTP or FTP upload requests of 1 GB or greater, upload requests of 1 GB or greater are not blocked. Instead, they are successfully upload either fully or partially. Workaround: To block upload requests of 1 GB or later, configure the IronPort Data Security Policies to block HTTP and FTP requests at a size less than 1 GB.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
49335	—	The access logs sometimes show inconsistent ACL decision tags for tunneled HTTPS traffic when HTTPS proxy is disabled. Some access log entries might show "OTHER-NONE" and some might show "DEFAULT_CASE" at the beginning of each ACL decision tag for tunneled HTTPS transactions. "OTHER-NONE" indicates that the Web Proxy did not make a final ACL decision when the transaction ended.
49152	—	Authentication fails with Microsoft Internet Explorer version 7 when the Web Security appliance is configured for persistent cookie-based authentication and the surrogate time out value is less than 799 seconds. This is a known issue with Internet Explorer version 7. Workaround: Increase the surrogate time value on the Network > Authentication page to a value greater than 799 seconds.
48963	—	Users not copied in the Customer Support ticket system automatically. When you create a support request from the Web Security appliance and add users in the "CC" field, those users are not added in the "CC" field in the Customer Support ticket system automatically.
48675	—	The end-user acknowledgement page appears twice under the following circumstances: • An Identity group exists that is defined by IP address and requires authentication. • Another Identity group based on a custom URL category and does not require authentication exists below the IP-based Identity group. • A client makes a request from the IP address in the first Identity group to a URL in the custom URL category in the second Identity group. The client is presented with the end-user acknowledgement page, and when the user clicks the link, the client is prompted for authentication. After entering valid authentication credentials, the client is presented with the end-user acknowledgement page again. After clicking the link the user is presented with the correct website content.
48378	—	Log files are not automatically recreated after deletion. When log files or the directory containing them are deleted from the Web Security appliance (for example, by using an FTP client), AsyncOS does not automatically create them again once new data is available to be logged. Workaround: Rollover the missing log file in the web interface or using the `rollovernow` CLI command.
47184	—	IronPort data security policies configured to block files based on file size do not block very large files, such as greater than 30 MB. Workaround: Contact Customer Support to change the value of an internal setting.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
46430	—	A valid user is erroneously treated as a guest user under the following conditions: • An identity group uses authentication and is configured for "Basic and NTLMSSP" authentication scheme. • The identity allows guest privileges. • A browser that supports NTLMSSP prompts the user for authentication credentials. • The user enters valid Basic authentication credentials. In this case, the Basic authentication credentials fail against the NTLM authentication realm. The Web Proxy treats the user as someone who has failed authentication and grants the user guest access as configured in the identity and access policy groups. The Web Proxy does not prompt the user to enter NTLM credentials. Workaround: Configure the identity group to use NTLMSSP only or Basic only.
45760	—	Authenticated users can erroneously access websites because they are not authenticated again in some cases. When the Web Security appliance is deployed in transparent mode, authenticated users can access a website they should not be able to access under the following conditions: • The user successfully authenticates as a member of an authentication realm. • That authentication realm and a custom URL category are used as membership criteria in an Identity group. The user accesses a website using an Access Policy using that Identity group. • Another Identity group exists that uses a different authentication realm and a different custom URL category. • The user keeps the *same* browser session open (uses a persistent connection) and accesses a website used in the custom URL category specified in the other Identity group. The user is not authenticated in the other authentication realm (and is not a member of it) and therefore should not have access to sites in the other custom URL category.
44089	—	Internet Explorer prompts for authentication multiple times under the following circumstances: • The Surrogate Timeout global authentication setting is configured, and the Surrogate Type is set to cookie. (In explicit forward mode, you can configure the surrogate timeout when you enable secure client authentication or from the `advancedproxyconfig > authentication` CLI command.) • A user views a file that includes links to objects coming from multiple domains. • The surrogate used to store the authentication credentials has expired. Workaround: Enter the user name and password each time, or use Firefox.
44023	—	External authentication does not fail over to the next configured RADIUS server when DNS fails to resolve the first RADIUS server. Instead, the appliance tries to authenticate the user as a local user defined on the Web Security appliance.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
42806	—	Access log entries and some reports do not list Windows domain for requests authenticated using NTLM Basic authentication in some cases. When a user is authenticated using NTLM Basic authentication and the user does not include the domain when prompted for authentication, the access log entry for that request and the Client Web Activity and Client Malware Risk reports do not show the Windows domain along with the user name. The access logs and reports display *user_name@realm_name* instead of *domain_name/user_name@realm_name*.
41942	—	Need to verify Authentication Transparent Redirect Hostname after any interface host name change. If any interface hostname (the M1 or P1 interface, for example) is changed, the administrator must verify that the transparent redirect hostname is set correctly to reflect the change.
40872	—	Cannot create a computer object on an Active Directory server using the createcomputerobject CLI command in some cases. The `createcomputerobject` CLI command does not successfully create a computer object on an Active Directory server when the security mode is set to "domain." The command returns the following error: Error: Unable to retrieve NTLM Authentication Realm settings. Check the realm name ''*realm_name*'' Workaround: Use the web interface to create the computer object for the NTLM authentication realm by joining the domain. Or, you can set the security mode to "ADS."

40363	—	Web Security appliance fails to join Active Directory domain under the following conditions:
		• The Web Security appliance is in Standard time, such as Pacific Standard Time (PST).
		• The Active Directory server is in Daylight Savings time, such as Pacific Daylight Time (PDT).
		The two machines might be in different time modes if the Active Directory server does not have the daylight time patch applied that fixes the change in Daylight Savings time starting in 2008. When you try to join the Active Directory domain, the web interface displays the following misleading message:
		`Error - Computer Account creation failed.`
		`Failure: Error while joining WSA onto server 'vmw038-win04.wga' : Failed to join domain: Invalid credentials`
		Workaround: Apply the appropriate patch to the Active Directory server.

39853	—	Microsoft Windows activation fails when authentication is enabled on the Web Security appliance. This is a known issue with Microsoft Windows activation. Workaround: For more information on how to work around this issue, see the following articles: • http://support.microsoft.com/kb/921471 • http://support.microsoft.com/kb/816897

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
38468	—	The Web Security appliance cannot pass HTTPS traffic and users gets a gateway timeout error under the following circumstances: • HTTPS scanning is enabled and the HTTPS decryption policy determines to decrypt the traffic • The web server requests a client certificate Workaround: Configure the appliance so it passes through HTTPS traffic to these web servers instead of decrypting the traffic.
37455	—	LDAP authentication fails when all of the following conditions are true: • The LDAP authentication realm uses an Active Directory server. • The Active Directory server uses an LDAP referral to another authentication server. • The referred authentication server is unavailable to the Web Security appliance. Workaround: Either specify the Global Catalog server (default port is 3268) in the Active Directory forest when you configure the LDAP authentication realm in the appliance, or use the `advancedproxyconfig > authentication` CLI command to disable LDAP referrals. LDAP referrals are disabled by default.
36229	—	The Web Security appliance does not create a computer account in the specified location on the Active Directory server under the following conditions: 1. You define the location for the computer account in the NTLM authentication realm and join the domain. The appliance successfully creates the computer account in the Active Directory server. 2. You change the location for the computer account in the NTLM authentication realm and then try to join the domain again. The appliance does not create the computer account even though it displays a message informing you that it successfully created the computer account. The computer account still exists in the old location.
35652	—	Clients running older versions of Java VM cannot load certain Java applets when NTLM authentication is enabled. When clients run Java version 1.5 and the Web Security appliance uses NTLM authentication, some Java applets fail to load. Workaround: Upgrade Java to version 1.6_03 on the client machines.
34159, 40097	—	Custom URL categories set to Monitor do not appear in access log entries in some cases. When a web access policy group has a custom URL category set to Monitor and some other component, such as the Web Reputation Filters or the DVS engine, makes the final decision to allow or block a request for a URL in the custom URL category, then the access log entry for the request shows the predefined URL category instead of the custom URL category.
34496	—	NTLM authentication does not work in some cases when the Web Security appliance is connected to a WCCP v2 capable device. When a user makes a request with a highly locked down version of Internet Explorer that does not do transparent NTLM authentication correctly and the appliance is connected to a WCCP v2 capable device, the browser defaults to Basic authentication. This results in users getting prompted for their authentication credentials when they should not get prompted. Workaround: In Internet Explorer, add the Web Security appliance redirect hostname to the list of trusted sites in the Local Intranet zone (Tools > Internet Options > Security tab).

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
34405	—	LDAP group authentication does not work with posixGroups. When you configure an LDAP authentication realm and enter a custom group filter query as objectclass=posixGroup, the appliance does not query memberUid objects correctly.
33285	—	Web Security appliance does not support Group Authorization against predefined Active Directory groups for LDAP authentication realms. When the Web Security appliance has a web access policy group using LDAP authentication and policy membership is defined by authentication groups using a predefined Active Directory group, such as "Domain Users" or "Cert Publishers," then no transactions match this policy group. Transactions from users in the predefined Active Directory group typically match the Global Policy Group instead. Workaround: Specify a user defined Active Directory group.
31935	—	Blocking DOS executable object types blocks updates for Windows OneCare. When you configure the Web Security appliance to block DOS executable object types, the appliance also blocks updates for Windows OneCare.
30703	—	Using Internet Root DNS servers for DNS lookups fails to resolve local hostnames. When you configure the Web Security appliance to use Internet Root DNS servers for DNS lookups, it fails to resolve machine names for local hostnames, such as the appliance or Active Directory server host names. Workaround: Fix the DNS or add the appropriate static entries to the local DNS using the Command Line Interface.
30255	—	NTLM authentication settings might not save correctly. When NTLM Basic authentication is configured and then disabled in a web access policy group, settings are saved and you do not have to repeat the setup if you re-enable. Currently, the appliance fails to save the authentication scheme and the setting defaults to "Use NTLMSSP."
29868	—	Changing NTLM non-admin user credentials requires AD server configuration. When changing the non-admin user credentials for the Active Directory server on the appliance, the credentials used to join the Active Directory domain must also be configured on the Active Directory server. The new credentials must have at least the following permissions on the "Computers" container in the "Active Directory Users and Computers" MMC applet: Create Computer Objects, and Delete Computer Objects.
28958	—	Issue with temperature alerts. The system health daemon fails to send alerts when the environmental temperature reaches critical levels. To prevent disk failure due to high temperatures, power down the appliance before the ambient air temperature reaches 95 degrees Fahrenheit.
28821	—	System reports false hard disk failure. Transient reports of hard disk failures might be erroneous. Performing a same drive hot swap resets the RAID firmware and likely resolves this issue.
27887	—	No alerts for failed authentication servers. The Web Security appliance does not currently support alert messaging for failed authentication servers. To manage the appliance during such an event, use the advanced authentication settings to specify an action if the authentication server becomes unavailable. This option is located on the Network > Authentication page.

Table 2 Known Issues for AsyncOS 7.5.2 for Web (continued)

Legacy Defect ID	New Defect ID	Description
23480, 23483, 26979, 37384	—	Partial messaging for denied HTTP CONNECT requests. Some browsers truncate HTTP data that is sent in response to a CONNECT request. This means that if the Web Security appliance denies a CONNECT request, the "page cannot be displayed: Access Denied" error message might be incomplete.
N/A	—	Specifying port 8080 is required to access the administration interface. To access the Web Security appliance management interface, you must connect using the appliance IP address and port number, `http://192.168.42.42:8080`. Failing to specify a port number when accessing the web interface results in a default port 80, Proxy Unlicensed error page.
N/A	—	LDAP uses M1 management interface. Currently, all LDAP traffic is restricted to the M1 management interface. For this limitation, and any other LDAP-related issue, please contact Customer Support.

Finding Current Information about Known and Fixed Issues: Bug Search Tool

Use the Cisco Software Bug Search tool to find the most current information about known and fixed defects.

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 Enter search criteria. The search begins as soon as you enter the first criterion.

Finding Current Information About Known and Fixed Issues: Bug Toolkit

If you do not find what you are looking for using the Bug Search Tool, try using Bug Toolkit at the following URL: http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Related Documentation

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

- *Cisco IronPort AsyncOS for Web User Guide*

Customer Support

Use the following methods to obtain support:

U.S.: Call 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.