Release Notes for Cisco IronPort AsyncOS 7.5.7 for Web

Contents

This document contains release information for running Cisco IronPort AsyncOS 7.5.7 for the Web Security appliance, and includes the following sections:

What's New in Cisco IronPort AsyncOS 7.5.7 for Web

Table 1 describes the new features and enhancements that have been added in the Cisco IronPort AsyncOS 7.5.7 for Web release. It references where you can find more details in the *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.

Table 1　　　*New Features for AsyncOS 7.5.7 for Web*

Feature	Description
Cloud Web Security Connector	The 7.5.7 release introduces a new configuration mode, which allows you to connect to and direct traffic to Cisco Cloud Web Security for policy enforcement and threat defense. Documentation for the Cloud Connector is in Chapter 7, "Cloud Web Security Connector". To put the Web Security appliance in Cloud Connector mode, begin with Configuring the Cloud Connector.
	✎
	Note　After upgrading to AsyncOS 7.5.7, if you plan to use the appliance in Cloud Connector mode, do not put the appliance into Standard mode using the System Setup Wizard. Put the appliance directly into Cloud Connector mode. See Known Issue CSCuh97153 for more information.

Documentation

Cisco IronPort AsyncOS 7.5.7 for Web User Guide includes documentation for all features. For customers who will run 7.5.7 in Cloud Connector mode, the following documentation will be most useful to you:

- Chapter 7, "Cloud Web Security Connector" in the *Cisco IronPort AsyncOS 7.5.7 for Web User Guide*.
- *Cisco ScanCenter Administrator Guide*, which is available from www.cisco.com: http://www.cisco.com/en/US/docs/security/web_security/scancenter/sc5200a/Administration.html

Upgrade Paths

You can upgrade to release 7.5.7-048 from the following versions:

- 7.1.3-031
- 7.5.0-833
- 7.5.1-079
- 7.5.1-201
- 7.5.2-118
- 7.5.2-303
- 7.5.7-040

To ensure a successful upgrade, you must complete some steps before you start the upgrade process. For detailed information about these prerequisites, see "Installation and Upgrade Notes" section on page 3.

Installation and Upgrade Notes

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

When you upgrade AsyncOS for Web, the software saves the configuration to a 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.

Known Limitations

User Authentication and Policy Application for HTTPS Sites

When all of these conditions are present, AsyncOS will allow access to HTTPS sites without authentication, preventing Cisco Cloud Web Security from applying username/group-based policies:

- Cloud Connector mode
- Traffic transparently redirected to Cisco Cloud Web Security
- User's first authentication attempt is at an HTTPS web site

Workaround: The user can authenticate at an HTTP site before accessing the HTTPS site.

Known Issues

Verify you read the list of known issues and limitations before you upgrade AsyncOS for Web. For a list of all known issues, see "Known Issues" section on page 6.

Configuration Files

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

AsyncOS for Security Management does not support AsyncOS 7.5.7 for Web.

Upgrading AsyncOS for Web

Step 1 In the web interface, navigate to **System Administration > System Upgrade**.

Step 2   Click **Available Upgrades**.

Step 3   Select the appropriate upgrade.

Step 4   Deselect **Mask passwords in the Configuration Files**.

Step 5   Click **Begin Upgrade**.

Step 6   Answer the questions as they appear.

Step 7   Click **Reboot Now**.

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 Found During Beta

The following bug was reported by beta testers during AsyncOS 7.5 beta and was fixed during beta:

- 89694: In Cloud Connector mode with HTTPS traffic, AsyncOS did not send the username or usergroup to the cloud with the transaction. Therefore, for HTTPS traffic coming from the Web Security appliance, Cisco Cloud Web Security could not apply HTTPS inspection policies to transactions based on username or usergroup. This is fixed.

Finding Information about Known and Fixed Issues

Use the Cisco Software Bug Toolkit 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 http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2   Log in with your Cisco account credentials.

Step 3   Enter information:

To	Do This

Search for a list of bugs for your product	1. For **Select Product Category**, select **Security**.
	
	2. For **Select Products**, select one of the following:
	  – Cisco Content Security Management Appliance
	  – Cisco IronPort Security Management Appliance Software
	  – Cisco Email Security Appliance
	  – Cisco IronPort Email Security Appliance Software
	  – Cisco Web Security Appliance
	  – Cisco IronPort Web Security Appliance Software
	
	3. (Optional) Scroll down and enter additional criteria.
	
	4. Click **Search**.

Find information about a specific issue	• Choose the product category and product as described in the previous table row, then enter keywords related to the issue. Then click **Search**. • Enter a bug ID number that starts with CSC in the **Search for Bug ID** field, then click **Go**. **Note** The 5-digit bug numbers used for previous releases of content security software cannot be used with this tool.
• Save searches • Create bug groups • Sign up for notifications	• Click the **Help Page** link on the Bug Toolkit page, or • Visit http://www.cisco.com/web/applicat/cbsshelp/help.html#personalize.

Questions About Using Bug Toolkit?

See:

- http://www.cisco.com/web/applicat/cbsshelp/help.html#personalize
- https://supportforums.cisco.com/community/netpro/online-tools/bugs

Known Issues

Table 2 lists the known issues in this release of AsyncOS for Web.

Table 2 *Known Issues for AsyncOS 7.5.7 for Web*

Defect ID	Description
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.
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.
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.
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.
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.
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.
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."
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.

Table 2   Known Issues for AsyncOS 7.5.7 for Web (continued)

Defect ID	Description
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.
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.
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).
35652	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.
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.
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.

Table 2   Known Issues for AsyncOS 7.5.7 for Web (continued)

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.
39853	MS 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

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.

40872	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."
41942	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.
42584	Some mobile devices that use ActiveSync cannot synchronize when authentication is enabled and the device sends an OPTIONS HTTP request. This is because ActiveSync cannot respond to an NTLM_CHALLENGE for an OPTIONS HTTP request.

Table 2   Known Issues for AsyncOS 7.5.7 for Web (continued)

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*.
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.
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.
45558, 89308	AsyncOS includes both active and inactive RAM in its report of RAM usage, excluding only unused RAM. Because inactive RAM is still available to AsyncOS, RAM usage reports may indicate a high level that may be misleading.
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.

Table 2 **Known Issues for AsyncOS 7.5.7 for Web (continued)**

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.
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.
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.
48963	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 IronPort Customer Support ticket system automatically.
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.

Table 2   Known Issues for AsyncOS 7.5.7 for Web (continued)

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.
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.
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.
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
67460	The Web interface does not always show changed update server settings. 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.
68411	AsyncOS is unable to join an Active Directory domain when an embedded special character is in the short domain name.

Table 2 ***Known Issues for AsyncOS 7.5.7 for Web (continued)***

Defect ID	Description
68555	Web Proxy may not handle POST requests properly with authentication required.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.
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.
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.
73467	Rebooting an appliance without a proper shutdown sometimes causes irreparable damage to the appliance.
79488	When including the %k format specifier as a custom field in the Access logs, when an object is served from the cache, the access log entry displays 255.255.255.255.
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.
82415	Large objects take too long to load in some cases when the client makes a universal range request.

Table 2   Known Issues for AsyncOS 7.5.7 for Web (continued)

Defect ID	Description
82662	SNMP erroneously returns appliance information from the previous version of AsyncOS after upgrading.
82857	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.
84178	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.
84195	Transaction requests sometimes result in HTTP 503 errors due to DNS caching problems.
84304	Running **logconfig** from the command line interface and choosing 'Request Debug Logs' causes logging and reporting to fail.
84487	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.
86394	Using the **authcache - list** command results in an application fault when the username includes non-ascii characters.
86556	The Appliance sometimes responds to an HTTPS file upload request with a 504 Gateway Timeout. Conditions: • The HTTPS proxy is enabled • The upload file includes this header: "Transfer-encoding: chunked"
86558	The appliance cannot establish a secure support tunnel when the secure tunnel host name is not DNS resolvable. Workaround: Ensure the secure tunnel hostname is DNS resolvable.
86620	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
87314	Users who have previously submitted authentication credentials are later unable to access HTTPS websites and are not prompted to authenticate. Conditions: • Decryption enabled • Authentication required • Transparent redirection • IP session caching
88970	The login banner fails to appear in the appliance web interface.

Table 2   Known Issues for AsyncOS 7.5.7 for Web (continued)

Defect ID	Description
89293	In Cloud Connector mode, if the cloud routing policy allows direct connection to the internet, AsyncOS does not cache FTP over HTTP downloads.
89348	In Cloud Connector mode using transparent requests, it is not possible to bypass the tower to connect directly to HTTPS web sites using custom URL categories. Workaround: Bypass the Web Security appliance for these requests using a router or switch.
89987	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'
91054	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.
CSCuh97153	Changing deployment mode from Standard to Cloud Connector results in AsyncOS sending feature key expiration notifications that are not applicable in Cloud Connector mode.

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.