Release Notes for Cisco IronPort AsyncOS 7.5.0 for Web

Published: August 06, 2012

Revised: January 2, 2013

Contents

This document contains release information for running Cisco IronPort AsyncOS 7.5.0 for the Web Security appliance, and includes the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

What's New in Cisco IronPort AsyncOS 7.5 for Web

Table 1 describes the new features and enhancements that have been added in the Cisco IronPort AsyncOS 7.5 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.

Table 1 New Features for AsyncOS 7.5 for Web

Feature	Description
New Features	
Adaptive Scanning	AsyncOS for Web 7.5 introduces the Adaptive Scanning feature to improve efficacy by identifying high-risk content and automatically selecting the best combination of available anti-malware services. Adaptive Scanning is a logic layer that associates web reputation and the content type and decides based on the current threat profile which anti-malware scanning engine will process the web request. Enabling Adaptive Scanning increases efficacy for filtering out malware, but causes a slight decrease in appliance performance. To use Adaptive Scanning, you must enable Web Reputation Filters. For more information, see the "Understanding Adaptive Scanning" section in the "Configuring Security Services" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.
Transparent User Identification for Active Directory	In AsyncOS for Web 7.5, you can identify users by an authenticated user name transparently when using Active Directory with an NTLM authentication realm. Previously, you could only identify users transparently when using Novell eDirectory with an LDAP authentication realm. When users are identified transparently, they are not prompted to enter user credentials. Active Directory does not record user login event information in a method that is easily queried by other servers, such as the Web Security appliance. However, Cisco offers the Cisco Active Directory Agent that queries the Active Directory security event logs to maintain an IP address to user name mapping of users authenticated with Active Directory. The Active Directory agent acts as a sort of identity repository. You must install the Active Directory Agent on a machine on the network that the appliance can communicate with. For more information, see the "Transparent User Identification with Active Directory" section in the "Identities" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 54973]

Table 1 New Features for AsyncOS 7.5 for Web (continued)

Feature	Description
AsyncOS Reversion	AsyncOS for Web 7.5 supports the ability to revert the AsyncOS for Web operating system to a previous qualified build for emergency uses. However, you cannot revert to a version of AsyncOS for Web earlier than version 7.5. Also, effective in version 7.5, when you upgrade to a later version, the upgrade process automatically saves the current system configuration to a file on the Web Security appliance. (However, Cisco recommends manually saving the configuration file to a local machine as a backup.) This allows AsyncOS for Web to load the configuration file associated with the earlier release after reverting to the earlier version. However, when it performs a reversion, it uses the current network settings with the earlier configuration file. To revert AsyncOS for Web to a previous version, use the `revert` CLI command. For more information, see the "Reverting to a Previous Version of AsyncOS for Web" section in the "System Administration" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 40414]
URL Category Updates for URL Filtering	The predefined set of URL categories for Cisco IronPort Web Usage Controls has been updated to accommodate new web trends and evolving usage patterns, and the system now allows Web Security appliances to automatically download additional changes. Category set changes in this release are designed to provide an optimal balance between simplicity and flexibility when configuring usage policies. Additionally, the new set of URL categories associated with this release matches the Cisco ScanSafe URL category list, simplifying management for Cisco ScanSafe customers. For more information, see URL Filtering Changes, page 11 and the "Managing Updates to the Set of URL Categories" section in the "URL Filters" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.
User System Preferences	In AsyncOS for Web 7.5, local users can define preference settings, such as language, specific to each account. These settings apply by default when the user first logs into the appliance. Users can change these settings during the appliance management session, but the settings revert to the default values when they log in again. The preference settings are stored for each user and are the same regardless from which client machine the user logs into the appliance. For more information, see the "Defining User Preferences" section in the "System Administration" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 71739]

Table 1 New Features for AsyncOS 7.5 for Web (continued)

Feature	Description
FIPS Compliance	AsyncOS for Web 7.5 provides support for the FIPS-compliant version of the Cisco IronPort S670 Web Security appliance. The Federal Information Processing Standard (FIPS) 140 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. The Cisco IronPort S670 Web Security appliance is now offered in a configuration that complies with the FIPS 140-2 Level 2 standard. This standard specifies additional protections for information used in cryptographic operations, including the use of a tamper-resistant hardware keystore for private keys. The FIPS version of the S670 includes a Hardware Security Module (HSM). The HSM provides cryptographic processing for the appliance as well as storage for private keys. All cryptographic operations take place within the secure environment of the HSM. AsyncOS for Web 7.5 provides support for using the HSM for all cryptographic operations performed by the appliance. It also provides a FIPS management console to allow an administrator to configure the HSM for use in a clustered environment and manage certificates and private keys. For more information, see the "FIPS Management" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.
Identifying Clients by IP Address in the XFF Header	In AsyncOS for Web 7.5, when the appliance has been deployed as an upstream proxy, you identify clients using the IP address specified in the X-Forwarded-For header instead of the IP address from the downstream proxy. Use the "Use Received Headers" section when you configure the Web Proxy or the `advancedproxyconfig > miscellaneous` CLI command. For more information, see the "Configuring the Web Proxy" section in the "Web Proxy Services" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 74303]
AsyncOS Upgrades Notification	AsyncOS for Web 7.5 displays a message at the top of the web interface notifying you when an upgrade to AsyncOS is available for the appliance. AsyncOS displays this notification for any administrator logged into the appliance. Hover over the notification with your mouse cursor to view the number of upgrades available for the appliance and the version and build number of the latest available upgrade. You can choose to dismiss the message and the appliance will not display another notification until a new upgrade becomes available. For more information, see the "Available Upgrade Notifications" section in the "System Administration" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 74267]

Table 1 ***New Features for AsyncOS 7.5 for Web (continued)***

Feature	Description
Rolling Over Log Subscriptions by Time of Day	AsyncOS for Web 7.5 allows you to roll over log subscriptions by time as day. Previously, AsyncOS for Web rolled over log subscriptions based on the first user-specified limit reached, either maximum file size or maximum time. You can roll over log subscriptions daily, weekly, or using a custom time interval. For more information, see the "Rolling Over Log Subscriptions" section in the "Logging" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 779]
Proxy Restart Warning Before Commit	In AsyncOS for Web 7.5, when you commit changes in the web interface or the CLI, AsyncOS for Web displays a warning that the Web Proxy will restart as a result of the commit. You can then choose to schedule to commit your configuration changes for a time when the Web Proxy processes fewer user transactions, such as overnight. For more information, see the "Checking for Web Proxy Restart on Commit" section in the "Using the Web Security Appliance" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 48941]
Read-Only Operator User	AsyncOS for Web 7.5 includes the Read-Only Operator local user. User accounts with this role can view configuration information and make and commit changes, but they cannot commit changes. For more information, see the "Managing Local Users" section in the "System Administration" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 39732]
Certificate Signing Request Support	When you generate a certificate and key on the Web Security appliance, AsyncOS for Web 7.5 allows you to download the Certificate Signing Request (CSR) so you can submit it to a certificate authority (CA). After you receive a signed certificate from the CA, you can upload it to the appliance. You do this in the web interface using the Download Certificate Signing Request link that appears after you generate a certificate and key when you configure the HTTPS Proxy or configure the Web Security appliance as an identity provider. For more information, see the "Enabling the HTTPS Proxy" section in the "Decryption Policies" chapter and the "Configuring the Appliance as an Identity Provider" section in the "Controlling Access to SaaS Applications" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 37984]

Table 1 New Features for AsyncOS 7.5 for Web (continued)

Feature	Description
Global Policy Default Action	AsyncOS for Web 7.5 allows you to block or monitor all web traffic by default after the System Setup Wizard completes. When you choose to block all traffic, the Global Access Policy blocks all proxied protocols, such as HTTP, HTTPS, and FTP. When you choose monitor, no proxied protocols are blocked. You can change this behavior later by editing the Protocols and User Agents settings for the Global Access Policy. Do this using the Global Policy Default Action on the Security tab of the System Setup Wizard. You might want to block all traffic with the Global Access Policy until you can define appropriately restrictive user-defined Access Policies and then edit the Global Access Policy as necessary. [Defect ID: 41113]
Enhancements	
Enhanced: Native FTP Proxy	AsyncOS for Web 7.5 includes several enhancements to native FTP functionality. • You can use spaces and the @ character in FTP user names and passwords. However, you must precede these characters with a backslash character (\). [Defect IDs: 52183 and 55380] • FTP clients can specify any TCP port for the control connection as long as they use proper formatting (hostname:port). [Defect ID: 55044] • Regardless of which mode the FTP client uses to connect to the FTP Proxy, the FTP Proxy first attempts to use passive mode to connect to the FTP server. However, if the FTP server does not allow passive mode, the FTP Proxy uses active mode. [Defect ID: 51308] • The FTP notification message defined on the appliance is displayed to native FTP clients when the FTP Proxy cannot establish a connection with the FTP server for any reason, such as an error with FTP Proxy authentication or a bad reputation for the server domain name. Previously, it was only displayed when there was an error with FTP Proxy authentication. • Access logs now include entries for when users first start a native FTP session. Search the access log file for “FTP_CONNECT” (explicit forward connections) and “FTP_TUNNEL” (transparent connections). • The following FTP commands are now supported: – XMKD, XRMD, XPWD, XCUP [Defect ID: 67985] – REST, APPE [Defect ID: 70135] – STOU • The ports defined for the Active Mode Data Port Range now apply to FTP over HTTP transactions as well as native FTP transactions. • The FTP Proxy now supports Trivial Virtual File Store (TVFS) FTP extensions.

Table 1 New Features for AsyncOS 7.5 for Web (continued)

Feature	Description
Enhanced: L4 Traffic Monitor Reporting and Tracking	In AsyncOS for Web 7.5, enhancements have been made to the L4 Traffic Monitor report to improve your ability to determine whether blocking a site or a port is the more effective solution to a particular malware problem, or whether to take action specific to a particular client IP address that is at unusually high risk. • You can view a list of top client IP addresses accessing malware sites, and filter these results by port. • You can filter top malware sites by port. • You can click the data in a table in the report to view details for a suspect site, port, or client IP address. • You can perform multi-dimensional searches for malware risk areas, for example by hostname and port. For more information, see the "L4 Traffic Monitor Page" section in the "Web Security Appliance Reports" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 75140, 70289]
Enhanced: External Authentication	In AsyncOS for Web 7.5, when using external authentication, you can map all RADIUS users to the Administrator user role type or you can map RADIUS users to different Web Security appliance user role types. To map RADIUS users to different Web Security appliance user role types, you assign a role type, such as Administrator and Operator, to a RADIUS CLASS attribute. Mapping different role types lets you specify the authorization level for each RADIUS user. For more information, see the "Using External Authentication" section in the "System Administration" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 41790, 70470]
Enhanced: End-User Acknowledgement Page	AsyncOS for Web 7.5 can track users who have accepted the end-user acknowledgement page by session cookie or IP address when no username is available. Previously, it could only track users by IP address when no username was available. Also, AsyncOS for Web now remembers when a user accepted the end-user acknowledgement page even after the Web Proxy restarts. For more information, see the "End-User Acknowledgement Page" section in the "Notifying End Users" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 46682, 48066]
Enhanced: WCCP	AsyncOS for Web 7.5 has enhanced WCCP robustness. For example, deploying a new configuration does not cause the Web Proxy to renegotiate WCCP communication. [Defect ID: 68342]
Enhanced: Syslog Support	AsyncOS for Web 7.5 supports Syslog Push for access logs. [Defect ID: 33010]

Table 1 New Features for AsyncOS 7.5 for Web (continued)

Feature	Description
Enhanced: Authentication	In AsyncOS for Web 7.5, you can configure Web Proxy to automatically restart the internal authentication process that communicates with Active Directory servers when it becomes unresponsive, but is still running. Do this using the `advancedproxyconfig > authentication` CLI command. [Defect ID: 35038]
Enhanced: On-Box End-User Notification Pages	AsyncOS for Web 7.5 has updated the look and feel of the default on-box end-user notification pages to make them more clear and easier to read. Customized on-box end-user notification pages are not affected.
Enhanced: SNMP MIB	AsyncOS for Web 7.5 uses 64-bit values for many counters in the SNMP MIB file instead of 32-bit values. This reduces the likelihood that the values will roll over when the appliance is under heavy load. [Defect ID: 72555] Additionally, the SNMP MIB file includes the cacheCpuUsage OID that provides the average Web Proxy CPU usage every 10 seconds. Note that in previous versions, the cacheCpuUsage OID reported the Web Proxy CPU usage since the Web Proxy started. [Defect ID: 81881]
Enhanced: PAC File Hosting	AsyncOS for Web 7.5 includes improvements to hosting PAC files on the Web Security appliance. • You can now replace an existing PAC file with a new version of the file with the same name. When you upload a PAC file that has the same name of an already uploaded PAC file, the GUI asks if you want to replace the current file with the new file. • You can also delete existing PAC files using the Delete button icon. • When you add a new row in the Hostnames for Serving PAC Files Directly section, the default PAC file is the first file uploaded to the appliance. [Defect ID: 78598]
Enhanced: Authentication with Machine Credentials	In AsyncOS for Web 7.5, you can configure a timeout value to use when it processes machine credentials for authentication from Windows machines that uses NCSI. Windows 7 and Windows Vista machines have a feature called Network Connectivity Status Indicator (NCSI). When clients on your network use NCSI and the Web Security appliance uses NTLMSSP authentication, you should configure the appliance so it uses a relatively small timeout value for machine credentials. Do this using the `advancedproxyconfig > authentication` CLI command: For more information, see the "Working with Windows 7 and Windows Vista" section in the "Authentication" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. [Defect ID: 75073]

Table 1 New Features for AsyncOS 7.5 for Web (continued)

Feature	Description
Enhanced: Web User Interface Protection	AsyncOS for Web 7.5 includes additional protection from cross-site request forgeries (CSRF) and other attacks on the web user interface. [Defect ID: 66682]
Fixed Known Limitations	Many previous known limitations have been fixed in this release. For more information, see Resolved Issues, page 17.

Upgrade Paths

You can upgrade to release 7.5.0-833 from the following versions:

- coeus-6-3-0-604
- coeus-6-3-1-025
- coeus-6-3-1-028
- coeus-6-3-3-015
- coeus-6-3-5-015
- coeus-6-3-5-024
- coeus-6-3-7-018
- coeus-6-3-8-005
- coeus-6-5-0-093
- coeus-7-0-0-819
- coeus-7-0-0-825
- coeus-7-1-0-297
- coeus-7-1-0-306
- coeus-7-1-0-307
- coeus-7-1-1-027
- coeus-7-1-1-038
- coeus-7-1-2-080
- coeus-7-1-2-405
- coeus-7-1-2-409
- coeus-7-1-3-006
- coeus-7-1-3-011
- coeus-7-1-3-013
- coeus-7-1-3-014
- coeus-7-1-3-019
- coeus-7-1-3-021
- coeus-7-1-3-022

- coeus-7-1-3-024
- coeus-7-1-3-025
- coeus-7-1-3-028
- coeus-7-1-4-052
- coeus-7-1-4-053
- coeus-7-1-4-055
- coeus-7-1-4-056
- coeus-7-1-4-062
- coeus-7-5-0-517
- coeus-7-5-0-586
- coeus-7-5-0-703
- coeus-7-5-0-727
- coeus-7-5-0-805
- coeus-7-5-0-810
- coeus-7-5-0-825
- coeus-7.5.0-826

To ensure a successful upgrade, you must complete some steps before you start the upgrade process. For details on these prerequisites, see "Installation and Upgrade Notes" section on page 10.

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.**

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

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 30.

URL Filtering Changes

As described in What's New in Cisco IronPort AsyncOS 7.5 for Web, page 2, the set of URL categories for Cisco IronPort Web Usage Controls has changed.

These changes may modify or disable existing policies.

To understand, prepare for, control, and respond to these changes, see the "Managing Updates to the Set of URL Categories" section in the "URL Filters" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.

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

Table 2 describes the changes to the set of URL categories that will occur when you upgrade to AsyncOS 7.5 for Web.

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*.

Table 2 URL Category Changes

Change	Old Categories	New Categories
Categories added	—	• Astrology • Auctions • Digital Postcards • Dynamic and Residential • Entertainment • Fashion • Humor • Illegal Downloads • Non-Governmental Organizations • Organizational Email • Parked Domains • Personal Sites • Photo Searches and Images • Politics • Professional Networking • Religion • SaaS and B2B
Categories renamed	Arts and Entertainment	Arts
	Infrastructure	Infrastructure and Content Delivery Networks
	Lottery and Sweepstakes	Lotteries
	Sex Ed and Abortion	Sex Education
	Porn	Pornography
	Child Porn	Child Abuse Content
Categories deleted	• Cults • Paranormal and Occult • Spiritual Healing • Tattoos	—
Categories split	• Alcohol and Tobacco	• Alcohol • Tobacco
	• Streaming Media	• Streaming Audio • Streaming Video

Table 2 URL Category Changes

Change	Old Categories	New Categories
Categories merged	• Instant Messaging • Web-based Chat	• Chat and Instant Messaging
	• Tasteless and Obscene • Violence	• Extreme

Configuration Files

IronPort does not generally s1upport 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 7.5 for Web are supported by AsyncOS for Security Management version 7.8.

End-User Notification Pages

This section describes changes to the On-box End User Notification pages.

Additional Notification Pages

Effective in AsyncOS for Web 7.5, the IronPort Notification pages have been renamed On-box End User Notification pages.

AsyncOS for Web 7.5 includes a new On-box End User Notification page. If the On-box End User Notification pages on the Web Security appliance were edited and customized by your organization in the previous version, you might want to make similar edits in the new On-box End User Notification page.

The following page is added in version 7.5:

- ERR_ADAPTIVE_SECURITY

Also, all default On-box End User Notification pages have been modified to change the look and feel. Any customized On-box End User Notification pages have not been modified.

For a list of all On-box End User Notification pages, see the “Notification Page Types” section in the “Notifying End Users” chapter of the *Cisco IronPort AsyncOS for Web User Guide*.

Unused Notification Pages

The Web Security appliance `eun` directory contains On-box End User Notification pages not used by AsyncOS for Web. You can ignore these pages. The following notification pages will be removed in a future release:

- ERR_AUTH

- ERR_ACCESS_FORBIDDEN
- ERR_BLOCK_SRC
- ERR_ONLY_IF_CACHED_NOT_IN_CACHE
- ERR_MISS_ACCESS_FORBIDDEN
- ERR_MALWARE_GENERAL

Defect ID: 82013

The following page is not used and has been removed in version 7.5:

- ERR_SOCKS_FAIL

Defect ID: 82011

Web Reporting and Tracking Data Availability for L4TM and Client Malware Risk

On the Web Tracking page, for L4TM information, only data that is added after upgrading to AsyncOS 7.8 for Security Management and AsyncOS 7.5 for Web is included in search results. Tables on the L4 Traffic Monitor Page and the Client Malware Risk Page display the number of blocked and monitored connections to malware sites. For data that is collected after upgrading to AsyncOS 7.8 for Security Management and AsyncOS 7.5 for Web, you can click a number in the table to view details about the relevant individual connections. For pre-upgrade data, only the totals are available.

Filtering by port on the L4 Traffic Monitor Page is also not available for pre-upgrade data.

For more information about these pages, see the “Using Centralized Web Reporting” chapter in the *Cisco IronPort AsyncOS for Security Management User Guide*, version 7.8.

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.

Handling Client Certificates

In AsyncOS for Web 7.5, how the HTTPS Proxy handles SSL connections that require client certificates has changed. You can now choose how the HTTPS Proxy responds to an HTTPS server when it asks for a client certificate during the SSL handshake negotiation. You can pass through the transaction or reply to the server that the client certificate is unavailable. You can choose which behavior to use with the `advancedproxyconfig > https` CLI command. Previously, the HTTPS Proxy always passed through the transaction.

When you upgrade to version 7.5 or install version 7.5 on a new appliance, the default is to reply to the HTTPS server that the client certificate is unavailable. Note that when upgrading, this is a change in behavior since previously, the HTTPS Proxy passed through the transaction.

When the HTTPS server requests a client certificate after the SSL session is already established, the behavior is different. Previously, the HTTPS Proxy dropped the transaction. In AsyncOS for Web 7.5, the HTTPS Proxy informs the server that the client certificate is unavailable. The HTTPS server determines whether or not the transaction is allowed to proceed.

[Defect ID: 71882]

FTP Functionality

AsyncOS for Web 7.5 includes several enhancements to native FTP functionality. Some of these enhancements include changes from previous behavior. For more information, see the description for the FTP enhancements in What's New in Cisco IronPort AsyncOS 7.5 for Web, page 2.

Configuring Custom Log Fields in the Access Logs

In AsyncOS for Web 7.5, the web interface validates the syntax of custom fields in the access log subscription and only allows you to enter custom fields using the proper syntax. The proper syntax includes a space between each format specifier and any descriptive text, such as "client_IP %a body_bytes %b".

If you upgrade from a previous version that uses improper custom field syntax, such as "%a%b" then the access log file works as it did previously. However, if after upgrading you try to change the custom fields in the access log subscription, you must correct the syntax so that it follows the proper format before you can submit the changes.

[Defect ID: 72714]

Configuring Language Setting

In AsyncOS for Web 7.5, how you define the language to view in the web interface and CLI has changed. You can now define the default language to display per local user account, regardless from which machine the user logs into the appliance. Define user preference settings on the Options > User Preferences page.

DNS Domain Search List

In AsyncOS for Web 7.5, how AsyncOS uses the configured domain search list has changed. Previously, it only added the domains in the domain search list (Network > DNS page) to hostnames when the hostnames did not contain a dot (.) character before doing a DNS match.

Now, when AsyncOS for Web cannot resolve a request with the DNS server, it appends the domains in the domain search list to all hostnames, whether or not they contain a dot.

[Defect ID: 77747]

advancedproxyconfig Command Changes

This section contains important information if your organization uses the `advancedproxyconfig` CLI command.

Transparent User Identification Related Commands

In AsyncOS for Web 7.5, the CLI commands you use to configure transparent user identification for Novell eDirectory have changed. Previously, you used an `advancedproxyconfig > authentication` command. Now, you use the `tuiconfig` and `tuistatus` CLI commands.

For more information on these commands, see the "Using the CLI to Configure Transparent User Identification" section in the "Identities" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.

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.

Access Log Changes

ACL Decision Tag Changes

In AsyncOS for Web 7.5, the ACL decision tag of SSO_EDIR has been replaced with SSO_TUI. The SSO_TUI ACL decision tag indicates that the user name was obtained by matching the client IP address to an authenticated user name using transparent user identification (using either Novell eDirectory or Active Directory).

Additionally, when the end-user acknowledgement page is displayed to a user, the access log entry for that transaction now shows OTHER as the ACL decision tag. This is because the originally requested URL was blocked, and instead the user was shown the end-user acknowledgement page. Previously, the ACL decision tag was BLOCK_ADMIN.

Anti-Malware Scanning Verdicts

The anti-malware verdicts are now written as integers instead of a string. This means the values are no longer enclosed in quotation marks. The anti-malware verdicts are position 3, 8, and 14 in the scanning verdict information section of each access log file entry.

[Defect ID: 73065]

Web Interface Name Changes

Effective in AsyncOS for Web 7.5, some web interface pages have changed names. The following table compares the previous page names to the current page names.

Previous Page	New Page
Web Security Manager > IronPort Data Security	Web Security Manager > Cisco IronPort Data Security
Security Services > Anti-Malware	Security Services > Web Reputation and Anti-Malware
Security Services > Web Reputation Filters	Security Services > Web Reputation and Anti-Malware
Security Services > Mobile User Security	Security Services > AnyConnect Secure Mobility
Security Services > SenderBase	Security Services > SensorBase

Upgrading AsyncOS for Web

Use the following instructions to upgrade the AsyncOS for Web version.

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.

Resolved Issues

This section includes the following topics:

- Resolved Issues in Version 7.5.0, page 17

Resolved Issues in Version 7.5.0

Table 3 lists the issues that were resolved in version 7.5.0 of AsyncOS for Web.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web

Defect ID	Description
83817	**Fixed:After upgrade, secondary aggregation fails to upload data from WSA to SMA.** Previously, with secondary aggregation enabled, after upgrading to version 7.5.0, AsyncOS failed to upload secondary data from the Web Security Appliance to the Security Management Appliance. Secondary data now uploads properly.
85053	**Fixed: Web Proxy generates a core file when the server sends data faster than the Web Proxy can scan it** Previously, the Web Proxy generated a core file when the server sent data faster than the Web Proxy could scan it. This no longer occurs. Now, the Web Proxy adapts to receive incoming data at the rate at which it can scan it.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
85730	**Fixed: Multiple HTTPS passthrough requests cause the WSA to run out of free memory resources, causing users to be unable to use the web** This issue could also cause the proxy to restart or core. Previously, this occurred because these connections were kept open even when no data was passing through them. This no longer occurs.
86307	**Fixed: Decreased performance when Safe Search and Content Rating are enabled in the Global Policy on a WSA with a complex configuration** Performance no longer degrades when Safe Search and Content Rating are enabled in the Global Policy.
86797	**Fixed: Use of FTP over HTTP in FireFox and Internet Explorer browsers results in the display of an incorrect directory listing.** Previously, the use of FTP over HTTP in FireFox and Internet Explorer browsers resulted in the display of an incorrect directory listing. The directory listing now displays correctly.
86906	**Fixed: Delayed response to HTTP HEAD requests causes the appliance to appear as offline** The appliance now responds immediately, avoiding the unexpected offline appearance.
86968	**Fixed: FTP over HTTP CONNECT fails while connecting to FTP sites using MLSD** Connections to FTP sites using MLSD are now successful.
87371	**Fixed: The WSA trusts some intermediate Certificate Authority certificates revoked by Microsoft in June 2012** The compromised intermediate certificates have been added to the proxy certificate blacklist and connections using those certificates are blocked.
88082	**Fixed: Appliance producing core files characterized by XFF invalid entries in the proxy logs.** Previously, the appliance was producing core files. These core files were characterized by XFF invalid entries in the proxy logs. This is fixed.
88822	**Fixed: Cannot revert after upgrade.** Previously, customers who upgraded to version 7.5.0 were unable to revert to an older version. Now customers can revert to older versions after upgrade.
73867	**Fixed: WSA incorrectly resets the connection to the Management HTTP port is unexpectedly reset if the same port is being used for Data traffic in split mode** You can now use the same port (i.e. 80) for the Management HTTP port and for proxying traffic on Data interface.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
72072	**Fixed: Client applications get "sec_error_reused_issuer_and_serial" error when accessing an HTTPS server that uses a certificate with the same serial number as a different server's certificate in some cases** Previously, client applications got a "sec_error_reused_issuer_and_serial" error when accessing an HTTPS server under the following conditions: • The HTTPS server uses a certificate with the same serial number as a different server's certificate that the client application has already encountered. • Decryption is enabled and the connection is decrypted. This no longer occurs. Now, the HTTPS Proxy creates a unique serial number when it mimics the server certificate when communicating to the client application in a decrypted connection.
73535	**Fixed: Web Proxy erroneously stops reading the entire uploaded object in a POST request when it sends an HTTP 407 status code due to authentication being required** Previously, the Web Proxy erroneously stopped reading the entire uploaded object in a POST request when it sent an HTTP 407 status code due to authentication being required. Many web browsers treat this behavior as an error. This no longer occurs. Now, the Web Proxy finishes reading the uploaded content before sending the 407 status code to the client.
75106	**Fixed: Web Proxy erroneously stops reading the entire uploaded object in a POST request when it sends an HTTP 307 status code due to authentication being required in transparent mode** Previously, the Web Proxy was in transparent mode, it erroneously stopped reading the entire uploaded object in a POST request when it sent an HTTP 307 status code due to authentication being required. Web browsers treated this as an error and did not redirect the page to allow authentication to occur. This no longer occurs. Now, the Web Proxy finishes reading the uploaded content before sending the 407 status code to the client.
75296	**Fixed: WCCP load balancing negotiation fails when the port numbers are not in the same order in the same WCCP service ID on multiple Web Security appliances** Previously, WCCP load balancing negotiation failed when the port numbers were not in the same order in the same WCCP service ID on multiple Web Security appliances. This no longer occurs. Now, the web interface sorts the ports in the WCCP service ID before saving the port numbers internally.
75351	**Fixed: Web Proxy erroneously sends only one cookie to the destination server when a client request contains multiple cookies** Previously, when a client request contained multiple cookies, the Web Proxy erroneously sent only one cookie to the destination server. This no longer occurs.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
76529	**Fixed: Web Proxy erroneously returns 400 Bad Request HTTP status code to DELETE requests that contain body content** Previously, the Web Proxy erroneously returned 400 Bad Request HTTP status code to DELETE requests that contain body content. This no longer occurs. Now, it processes the DELETE request as expected.
79929	**Fixed: Colons are erroneously converted to %3A when Web Tracking results are exported as .csv file** Previously, Colons were erroneously converted to %3A when Web Tracking results were exported as .csv file. This no longer occurs. Now, colons appear properly in CSV files.
80745	**Fixed: AsyncOS does not serve some PAC files stored on the appliance** Previously, AsyncOS did not serve some PAC files stored on the appliance because it did not correctly save some PAC file configuration information. This no longer occurs.
83039	**Fixed: Web Proxy generates a core file when non-HTTP data is transparently redirected and sent over a secure SSL tunnel on port 443** Previously, the Web Proxy generated a core file when non-HTTP data was transparently redirected and sent over a secure SSL tunnel on port 443. This no longer occurs.
83075	**Fixed: Web Tracking Search query generates out of memory error when tracking data contains large amounts of data** Previously, searching Web Tracking data generated an out of memory error when the tracking data contained large amounts of data. This no longer occurs. Now, when you click the Related Transactions link, the web interface displays up to 500 transaction and displays “[Omitted]” when it omits transactions. Also, extremely long URLs are truncated to 1000 characters, and “[truncated]” in the displayed URL.
85307	**Fixed: Loading a configuration file fails after reverting to some versions of AsyncOS for Web** Previously, loading a configuration file failed after reverting to some versions of AsyncOS for Web. This no longer occurs.
86521	**Fixed: Access logs erroneously include no information for the MIME type in some cases** Previously, the access logs erroneously included no information for the MIME type instead of a hyphen when the server returned either no Content-Type header, or a Content-Type header with an empty value. This no longer occurs. Now, the access logs include a hyphen (-) when the server includes no MIME type information.
42512	**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.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
80479	**Fixed: Web Proxy generates a core file when trying to** keep a persistent connection to a server in some cases Previously, the Web Proxy generated a core file when trying to keep a persistent connection to a server that unexpectedly returned a resource temporarily unavailable error and the Web Proxy continued to try to write to the server. This no longer occurs.
82692	**Fixed: CPU usage may unexpectedly run at maximum capacity** Previously, in rare circumstances, SNMP could drive CPU usage to %100. This problem no longer occurs.
84528	**Fixed: Web Proxy lags in some network environments** Previously, the Web Proxy lagged when a large number of clients connect to the Web Proxy with a slow network connection. Workaround: Contact Cisco IronPort Customer Support to determine the best value to use for the send buffer client-side sockets using the `advancedproxyconfig > miscellaneous` CLI command.
84563	**Fixed: Client applications with user agent Firefox 10.x erroneously match Identity Policies configured for Firefox 1.x** Previously, client applications with user agent Firefox 10.x erroneously matched Identity Policies configured for Firefox 1.x. This no longer occurs.
84718	**Fixed: Web Proxy performance is very slow after upgrading to version 7.5 for some very complicated configurations** Previously, Web Proxy performance was very slow after upgrading to version 7.5 for some very complicated configurations, such as ones with a very large number of custom URL categories. This no longer occurs.
84855	**Fixed: Web Proxy generates a core file attempting to send a POST request to some web servers** Previously, the Web Proxy generated a core file attempting to send a POST request to some web servers. This no longer occurs.
39535, 73610	**Fixed: Application error occurs in the L4 Traffic Monitor when loading or reading the DNS cache in some cases** Previously, an application error occurred in the L4 Traffic Monitor when loading misformatted entries in the DNS cache and when reading a DNS cache with misformatted entries. This no longer occurs. Now, the L4 Traffic Monitor no longer enters misformatted entries, nor does it result in an application fault when it reads misformatted entries.
68501	**Fixed: Incorrect cache state logged in the access logs for native FTP transactions** Previously, native FTP upload and download transactions were logged in the access logs with “NONE” as the cache state. This no longer occurs. Now, they are logged similarly to HTTP transactions. For example, “TCP_MISS” is logged when the FTP object is downloaded from the FTP server instead of from the web cache.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
73706	**Fixed: Web Tracking details incorrectly display a web reputation score of 10.1 for Access Policies with blocked protocols or user agents** Previously, Web Tracking details incorrectly displayed a web reputation score of 10.1 for Access Policies with blocked protocols or user agents. This no longer occurs. Now, “No score” is displayed in these cases.
79512	**Fixed: Web Tracking unexpectedly stops functioning when processing extremely long URLs** Previously, Web Tracking unexpectedly stopped functioning when processing extremely long URLs. This no longer occurs. Now, extremely long URLs are truncated in Web Tracking. For the full URL, check the access log.
81001	**Fixed: Web Proxy performance slows down on S160 hardware models in some cases** Previously, Web Proxy performance slowed down on S160 hardware models due to too many internal watchdog processes that monitor anti-malware scanning using too many CPU resources. This no longer occurs. Now, these internal watchdog processes are created less frequently thus causing them to take up fewer CPU resources.
70395	**Fixed: RAM usage on the System Status report** The RAM usage on the System Status report may appear unnaturally high when the appliance experiences a light load. The *Cisco IronPort AsyncOS for Web User Guide* has been updated to explain that this is expected and should not cause undue concern.
72824	**Fixed: Some streaming media client transactions fail in some cases** Previously, some streaming media client transactions failed when the HTTP GET request included a non-HTTP compliant range request header. This no longer occurs.
80076	**Fixed: Cannot host a PAC file on the appliance using a single word hostname** Previously, when the appliance hosted a PAC file, clients could not reach it when the appliance hostname was a single word. This no longer occurs.
80930	**Fixed: Cannot fetch feature keys after upgrading in some cases** Previously, when a feature key was in a pending state and then the appliance was upgraded, the appliance could not fetch new feature keys from the Cisco IronPort server. This no longer occurs.
81068	**Fixed: Application fault occurs in the web interface when trying to preview Reports by User Location > Users in some cases** Previously, an application fault occurred in the web interface using Spanish localization when trying to preview the Reports by User Location > Users section with all table columns included. This no longer occurs.
81405	**Fixed: Cannot modify the DNS time to live (TTL) parameter** Previously, you could not modify the DNS time to live (TTL) parameter the Web Security appliance used. This no longer occurs. You can now modify this value using the `dnsconfig > setup` CLI command.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
81488	**Fixed: No results are returned when searching by network ranges in the User/Client IP field on the Web Tracking page** Previously, no results were returned when you searched for a network range in the User/Client IP field on the Web Tracking page. This no longer occurs.
81544	**Fixed: Number of applications is different on the Access Policies page** Previously, the number of applications listed in the Applications column of the Access Policies page was different than the total number of applications listed on the Access Policies > Applications Visibility and Control > *policy_name* page. This no longer occurs.
71303	**Fixed: Cannot remove guest users from the authentication cache** Previously, The `authcache` CLI command did not allow administrators to remove guest users from the authentication cache. This no longer occurs.
77790	**Fixed: Web Proxy generates a core file when sending concurrent POST requests and it receives an early server response** Previously, the Web Proxy generated a core file when sending concurrent POST requests and it received an early server response. This no longer occurs.
39620	**Fixed: HTTPS Proxy does not update the spoofed server certificate when the server certificate changes in some cases** Previously, the HTTPS Proxy did not update the spoofed server certificate when the server certificate changed and when the spoofed certificate was found in the certificate cache. This no longer occurs.
44247	**Fixed: Application fault occurs in the web interface after committing changes in some cases** Previously, an application fault occurred in the web interface after clicking **Submit** and then waiting at least 30 minutes before clicking **Commit**. This no longer occurs.
44810	**Fixed: SCP Push method does not work when the log file name or directory contains a space** Previously, SCP Push method did not work when the log file name or directory contained a space. This no longer occurs.
49508	**Fixed: Loading a previously saved configuration file fails in some cases** Previously, loading a previously saved configuration file failed when the update interval for updates and upgrades was greater than one hour. This no longer occurs.
53853	**Fixed: Anti-malware scanning error occurs trying to download a Microsoft Windows update executable with heuristic scanning enabled** Previously, an anti-malware scanning error occurred when trying to download a Microsoft Windows update executable when heuristic scanning was enabled. This no longer occurs.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
69457	**Fixed: Redirected explicit transactions always get redirected to port 80 even if port 80 is not an HTTP proxy port** Previously, redirected explicit transactions, such as redirecting for authentication purposes, always get redirected to port 80 even if port 80 is not an HTTP proxy port. This no longer occurs. Now, the requests are redirect to the port on which they were received.
70818	**Fixed: Web Proxy does not send user credentials to upstream proxy** Previously, the Web Proxy did not send user credentials to an upstream proxy. This no longer occurs.
71942	**Fixed: Logging data is recorded on Web Security appliance after enabling Centralized Reporting** Previously, when Centralized Reporting was enabled on the Web Security appliance, AsyncOS for Web recorded information in the Web Security appliance logging database as well as collected information for centralized reporting on the Security Management appliance. This no longer occurs.
72794	**Fixed: Application fault occurs when processing and If-Modified-Since header in a PAC file request** Previously, an application fault occurred when processing and If-Modified-Since header in a PAC file request. This no longer occurs.
73441	**Fixed: Policy trace feature does not work with an LDAP authentication realm in some cases** Previously, the policy trace feature did not work with an LDAP authentication realm that was configured to use “UserObject” for group-authorization. This no longer occurs.
73527	**Fixed: SNMP memory percentage (.1.3.6.1.4.1.15497.1.1.1.1.0) always displays “1”** Previously, the SNMP memory percentage (.1.3.6.1.4.1.15497.1.1.1.1.0) always displayed “1” instead of the percentage. This no longer occurs.
73972	**Fixed: Authentication is skipped for explicit Native FTP requests when cookie surrogates are used** Previously, authentication was skipped for explicit Native FTP requests when cookie surrogates were used. This no longer occurs.
74084	**Fixed: FTP Proxy process leaks memory when processing PASV and PORT FTP commands** Previously, the FTP Proxy process leaked memory when processing PASV and PORT commands. This no longer occurs.
74457	**Fixed: Proxy server setting erroneously used for feature key updates in some cases** Previously, when a proxy server was configured for the update settings and was then removed, AsyncOS still tried to connect through the proxy server when trying to retrieve feature key updates. This no longer occurs.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
74491	**Fixed: Cannot use non-alphanumeric characters for group authorization in LDAP authentication realms** Previously, you could not use non-alphanumeric characters for group authorization in LDAP authentication realms. This no longer occurs.
74590	**Fixed: Appliance does not automatically incorporate new Application Visibility and Control engine updates in some cases** Previously, the appliance did not automatically incorporate new Application Visibility and Control engine updates in some cases. This no longer occurs.
74905	**Fixed: S160 hardware models erroneously send out watchdog timeout messages when reporting lags a little bit under normal operation** Previously, S160 hardware models erroneously sent out watchdog timeout messages when reporting lagged a little bit under normal operation. This no longer occurs.
75303	**Fixed: FTP clients time out when the connection between the FTP Proxy and FTP server is slow in some cases** Previously, FTP clients timed out when the file took too long to upload to the FTP server due to a slow connection between the appliance and FTP server. This no longer occurs.
75597	**Fixed: HTTPS requests for uncategorized URLs erroneously succeed when uncategorized URLs are configured to block or warn** Previously, HTTPS requests for uncategorized URLs erroneously succeeded when uncategorized URLs were configured to block or warn. This no longer occurs.
75735	**Fixed: Web Proxy generates a core file when customized on-box notification pages use the %K variable** Previously, the Web Proxy generated a core file when customized on-box notification pages used the %K variable. This no longer occurs.
75851	**Fixed: Policy trace feature erroneously uses the appliance IP address as the client source IP address when the Web Proxy is deployed in explicit forward mode** Previously, the Policy trace feature erroneously used the appliance IP address as the client source IP address when the Web Proxy is deployed in explicit forward mode. This no longer occurs.
75953	**Fixed: Some URLs are erroneously categorized by the Cisco IronPort Web Usage Controls URL filtering engine when the Dynamic Content Analysis engine is disabled** Previously, some URLs were erroneously categorized using the Dynamic Content Analysis engine even when the Dynamic Content Analysis engine was disabled.
76368	**Fixed: Application fault occurs in the web interface when clicking a second link on the Web Tracking page** Previously, an application fault occurred in the web interface when clicking a second link on the Web Tracking page. This no longer occurs.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
76440	**Fixed: Critical email alert for logging occurs when the Data Security log subscription uses Syslog Push in some cases** Previously, a critical email alert for logging was sent when the Data Security log subscription used Syslog Push with UDP as the protocol and local5 as the Facility. This no longer occurs.
76632	**Fixed: Web Tracking report does not show POST requests blocked by Cisco IronPort Data Security Filters** Previously, the Web Tracking report did not show POST requests blocked by Cisco IronPort Data Security Filters. This no longer occurs.
76959	**Fixed: Value for CPU usage in proxystat CLI command is divided by 100** Previously, the value for the CPU usage in the `proxystat` CLI command was divided by 100. This no longer occurs.
77726	**Fixed: Web reporting in the GUI may become sluggish** Previously, response to any action performed in the web reporting pages could become very slow until the appliance rebooted. This issue has been fixed.
77799	**Fixed: Valid feature keys appear invalid in some cases** Previously, when installing a new valid feature key on an appliance where the feature was disabled, the new feature key appeared invalid. This no longer occurs.
77943	**Fixed: Web Proxy generates a core file when it tries to process a malformed authentication URL** Previously, the Web Proxy generated a core file when it tried to process a malformed authentication URL. This no longer occurs.
77962	**Fixed: Hard disk fills up with temporary files when the appliance restarts while Sophos scans large files** Previously, the appliance hard disk filled up with temporary files when the appliance restarted while Sophos was scanning large files. This no longer occurs. Now, the appliance deletes the temporary files when they are no longer needed.
78408	**Fixed: Appliance becomes unusable when it cannot reach the update server for a full day** Previously, the appliance became unusable when it could not reach the update server for a full day. This no longer occurs.
78793	**Fixed: Web Proxy generates a core file after leaking numerous connection objects due to processing range requests in some cases** Previously, the Web Proxy generated a core file after leaking numerous connection objects due to processing range requests for objects already contained in the web cache. This no longer occurs.
80429	**Fixed: Web Proxy leaks memory and eventually generates a core file in some cases** Previously, the Web Proxy leaked memory and eventually generated a core file when an internal process leaked memory processing authentication surrogates. This no longer occurs.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
71976, 67473	**Fixed: (S160 and S170 Hardware only) Disk fails with RAID alert** Software RAID robustness has been improved, making these disk failures less likely to occur.
74487, 71794, 71747	**Fixed: Identities have incorrect authentication surrogate settings after upgrading from a previous version in some cases** Previously, after upgrading from a previous version in explicit forward mode, Identities had incorrect authentication surrogate settings when no authentication surrogates were configured in the Identity. This no longer occurs. Now, authentication surrogate settings are retained correctly.
76136	**Fixed: Self signed certificates erroneously not recognized as an invalid certificate when the server requests a client certificate** Previously, the HTTPS Proxy did not treat self signed certificates from an HTTPS server as an invalid certificate (Unrecognized Root Authority) when the server requested a client certificate. For example, if the HTTPS Proxy was configured to drop transactions to servers that use certificates with an unrecognized root authority, it did not drop those transactions if the server requested a client certificate. This no longer occurs. Now, the HTTPS Proxy evaluates the server certificate validity before proceeding to the next step in the SSL handshake negotiation. See also how the Web Security appliance handles servers that request a client certificate. For more information, see Handling Client Certificates, page 14.
77225	**Fixed: Authentication compatibility issues with Active Directory 2008** To improve compatibility with Active Directory 2008, the Web Security appliance no longer uses TCP port 139 to communicate to the Active Directory server. It now uses port 445 exclusively.
77926	**Fixed: Some anti-malware settings are changed after upgrading from a previous version** Previously, when you upgraded from a previous version, the “Other Malware” and “Unscannable” settings on the Access Policies > Web Reputation and Anti-Malware Settings page were changed from their original settings. This no longer occurs.
78620	**Fixed: PAC file hosting erroneously appears disabled after loading a configuration file** Previously, when you enabled PAC file hosting on the appliance, saved the configuration, and then loaded the configuration, PAC file hosting appeared disabled on the Security Services > Proxy Auto-Configuration File Hosting page. (However, the appliance was correctly configured and served PAC files to clients as necessary.) This no longer occurs.
70914	**Fixed: Policy Trace feature does not use the Dynamic Content Analysis engine when performing a trace** Previously, the Policy Trace feature did not use the Dynamic Content Analysis engine when categorizing a URL when performing a trace. This no longer occurs.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
72238	**Fixed: Dynamic Content Analysis engine does not categorize web pages that contain NULL characters** Previously, the Dynamic Content Analysis engine did not categorize web pages that included characters containing NULL bytes. This might happen for web pages whose contents are UTF-16 encoded. This no longer occurs.
74872	**Fixed: WCCP negotiation with some Cisco 7600 routers fails** Previously, WCCP negotiation with some Cisco 7600 routers failed. This no longer occurs.
76000	**Fixed: Native FTP connections fail when the configured welcome banner for the FTP Proxy exceeds 1024 characters** Previously, native FTP connections failed when the configured welcome banner for the FTP Proxy exceeded 1024 characters. This no longer occurs.
76207	**Fixed: Application fault occurs in the web interface when trying to download an uploaded Identity Provider signing certificate** Previously, an application fault occurred in the web interface when trying to download an uploaded Identity Provider signing certificate. This no longer occurs.
76472	**Fixed: Application fault occurs in the web interface when clicking the Schedule Reports link on the Next Steps page of the System Setup Wizard** Previously, an application fault occurred in the web interface when clicking the Schedule Reports link on the Next Steps page of the System Setup Wizard. This no longer occurs.
76916	**Fixed: The %g variable in customized end-user notification pages sometimes erroneously displays the wrong value** Previously, when you customized the end-user notification pages stored on the appliance and included the %g variable, sometimes the variable correctly displayed the custom URL category, and sometimes it displayed a predefined URL category. This no longer occurs.
77271	**Fixed: Browsers cannot access PAC files stored on the appliance when the port is changed in some cases** Previously, browsers could not access PAC files stored on the appliance when the port was changed from the current value and when browsers tried to access the PAC file using only the hostname specified in the Hostnames for Serving PAC Files Directly section on the Security Services > Proxy Auto-Configuration File Hosting page. This no longer occurs.
75040	**Fixed: Application error occurs trying to generate a PDF from the Reports by User Location page in some cases** Previously, an application error occurred when you changed the web interface language using the Options menu and then clicked the **Printable (PDF)** link on the Reports by User Location page. This no longer occurs.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
76185	**Fixed: Files greater than the maximum allowed file size are erroneously uploaded using FTP in some cases** Previously, files greater than the maximum allowed file size were erroneously uploaded when an IronPort Data Security policy was configured to block FTP transactions greater than a specified size. The access logs showed that the file was blocked, but in reality the file was successfully transferred to the FTP server. This no longer occurs.
73339	**Fixed: Log file timestamps and log file headers show incorrect time after changing the time zone in some cases** Previously, when you changed the time zone on the appliance, the time zone change was not propagated to the internal logging process. As a result, the timestamps in the log filename and the offset in the log file headers were incorrect. (However, the log entries in the log files correctly used the new time zone.) This no longer occurs.
72834	**Fixed: An application fault occurs in the internal reporting process when you change the system time or time zone on the appliance in some cases** Previously, an application fault occurred in the internal reporting process when you changed the system time or time zone on the appliance after it had processed traffic. Additionally, for some appliances, data was not aggregated properly (for example, hourly data was not aggregated into the daily data). This no longer occurs.
72835	**Fixed: Export link is missing on the Reports By User Location report page for the “Suspect Transactions Detected” charts** Previously, the Export link was missing on the Reports By User Location report page for the “Suspect Transactions Detected” charts for both Remote and Local users. This no longer occurs.
72432	**Fixed: PDF file of Web Tracking report does not include related transactions information** Previously, when you displayed the related transactions in a Web Tracking report and then printed to PDF, the PDF file did not contain the related transactions information. This no longer occurs.
70537	**Fixed: Web Proxy erroneously does not recognize some root authorities** Previously, by default, the Web Proxy erroneously did not recognize the “VeriSign Class 3 Secure Server CA” root certificate. The Web Proxy did not recognize the root authority of websites that use this root certificate to establish its trust relationship. Depending on how the HTTPS Proxy was configured to handle invalid certificates, client requests to these sites may have been dropped. This no longer occurs.

Table 3 Resolved Issues in AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
69388	**Fixed: Policy Trace erroneously matches some transactions with the Global Access policy in some cases** Previously, the Policy Trace feature erroneously matched transactions with the Global Access policy under the following circumstances: • An Identity included authenticated users in the "Domain Local" group in Active Directory, and an Access Policy group used that Identity. • In the Policy Trace tool you entered a user in the "Domain Local" group. Instead of matching the Access Policy that uses the Identity configured above, users matched the Global Access Policy in the Policy Trace. (However, the Web Proxy assigned the correct Access Policy to users accessing the Internet.) This no longer occurs.
56418	**Fixed: Exported URL Categories Report does not show all information** Previously, when you clicked the Export link on the Monitor > URL Categories page, the exported .csv file did not contain any information in the "bandwidth saved by blocking" column. This no longer occurs.
56418	**Fixed: Exported URL Categories Report does not show all information** Previously, when you clicked the Export link on the Monitor > URL Categories page, the exported .csv file did not contain any information in the "bandwidth saved by blocking" column. This no longer occurs.
44031	**Fixed: Policy trace feature does not display a web reputation score when authentication is enabled** Previously, the policy trace feature did not display a web reputation score when authentication was enabled.

Known Issues

Table 4 lists the known issues in this release of AsyncOS for Web.

Table 4 Known Issues for AsyncOS 7.5.0 for Web

Defect ID	Description
82852	**Choosing no bandwidth limit for a particular application does not work as expected** When a bandwidth limit is applied to an application type, and then you configure a particular application in that type to have no bandwidth limit, the bandwidth limits are still applied to that application.
84487	**Web Security appliance performance is affected when Default Proxy Logs are configured at debug or trace level** 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.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
86396	**HTTPS requests are erroneously not dropped when Adaptive Scanning is enabled in some cases** Requests to HTTPS servers that have a web reputation score that indicates to drop the request are not dropped when Adaptive Scanning is enabled.
86558	**Appliance cannot establish a secure support tunnel when the secure tunnel host name is not DNS resolvable** 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.
87282	**Backing up and restoring the certificates and keys the HSM card manages using the FIPS management console does not work as expected in some cases** 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.
54636	**Users cannot access FTP servers that require server authentication using FTP over HTTP with Internet Explorer** 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
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.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
71912	Google Talk clients cannot successfully log into Google Talk when the HTTPS Proxy decrypts traffic in some cases. 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.
73469	**Appliance sends out a non-applicable critical alert email in some cases** The Web Security appliance sometimes sends out a non-applicable critical alert email with the following message: `Counter group "MAIL_SYSTEM_CAPACITY" does not exist.`
76210	**Traceback generated after technical support tunnel fails for reasons related to DNS.** When attempting to establish a secure tunnel through which Cisco IronPort technical support can connect to the Appliance, if the tunnel attempt fails for reasons related to DNS, AsyncOS generates a traceback.
79535	**System Capacity reports and logs show CPU activity for some features that are disabled** 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.
81408	**First web reputation database incremental update after upgrading AsyncOS for Web fails in some cases** The first web reputation database incremental update after upgrading AsyncOS for Web fails depending on the Web Proxy load and time of day. Workaround: Wait until the next full web reputation database update which will occur in less than 24 hours.
82852	**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.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
85307	**Loading a configuration file fails after reverting to AsyncOS 7.8.0-564** If the Security Management appliance manages one or more Web Security appliances running AsyncOS for Web 7.5, you must do the following after the reversion is complete, but before you load a configuration file: Allow the Web Security appliance to connect to the update server and update the URL category set. Wait a few minutes to allow any URL category set updates to be downloaded to the Web Security appliance. Reverting to the current release will not require this workaround.
85843	**Access log file erroneously records FTP over HTTP transaction with a "200 OK" HTTP status when the transfer fails due to no space available on the FTP server** Access log file erroneously records FTP over HTTP transaction with a "200 OK" HTTP status when the transfer fails due to no space available on the FTP server.
86326	**FTP Proxy prematurely closes an FTP control connection with Cisco IronPort Data Security Filters disabled in some cases** 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.
86620	**Web interface stops responding after entering some regular expressions in a custom URL category** 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
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.
82093	**Web interface erroneously does not limit the number of ports to proxy** The web interface erroneously does not prevent you from entering more than 30 ports in the HTTP Ports to Proxy and HTTPS Ports to Proxy fields combined. The total number of ports in both fields must be 30 or less.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
82244	**Users making web uploads see an Internet redirection message in Internet Explorer in some cases** 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.
82662	**SNMP erroneously returns appliance information from the previous version of AsyncOS after upgrading** An internal SNMP configuration file fails to update after upgrading from a previous version. SNMP still works, but it returns appliance information from the previous version of AsyncOS. For example, SNMP returns the previous AsyncOS version number. Workaround: Use the `snmpconfig` CLI command to disable SNMP and commit the changes, and then use `snmpconfig` to enable SNMP.
82857	**External authentication fails with a Juniper SBR RADIUS server in some cases** 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.
83098	**Users may get prompted to enter authentication credentials when transparent user identification is enabled in some cases** 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.
84178	**Transparent HTTPS traffic is always logged as decrypted when authentication is required and a Routing Policy applies** 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 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
84293	**Native FTP client transaction may hang indefinitely when uploading a file and the connection to the FTP server is reset in some cases** Native FTP client transaction may hang indefinitely when uploading a file and the connection to the FTP server is reset, perhaps by a firewall. Workaround: Close the FTP transaction from the FTP client and start the upload again.
82480	**Web Proxy generates a core file when it receives a connection reset from the FTP server when downloading an object using FTP over HTTP in some cases** The Web Proxy generates a core file (and may restart) when it receives a connection reset from the FTP server when downloading an object using FTP over HTTP. This may occur due to network connection issues or firewall settings, for example.
76803	**AsyncOS erroneously allows administrators to configure the same ports for different services** AsyncOS erroneously allows administrators to configure the same ports for different proxy services related to the Web Proxy, HTTPS Proxy, and FTP Proxy. For example, neither the web interface nor CLI prevent you from entering the same TCP ports for the HTTP ports to proxy and the active and passive mode data port ranges for FTP. Workaround: Ensure that you enter unique ports and port ranges for each field when configuring the different proxy services.
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.
82082	**ERR_SAML_PROCESSING notification page does not use variables correctly** 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.
55958	**Web Proxy does not block Microsoft Office 2007 files** When an Access Policy is configured to block Microsoft Office files by MIME type, the Web Proxy does not block Microsoft Office 2007 files.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
71012	**Clients cannot connect to HTTPS servers that do not support TLS Hello during the SSL handshake** 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.
71912	**Google Talk clients cannot successfully log into Google Talk when the HTTPS Proxy decrypts traffic in some cases** 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.
72798	**Clients are continually prompted to authenticate when accessing some servers that require authentication and when NTLM authentication is enabled on the appliance in some cases** 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.
79488	**Custom format specifier %k in the Access logs returns 255.255.255.255 for all cached objects** 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 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
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.
81055	**Processing client requests may take too long after updating new anti-malware rules in some cases** Processing client requests may take too long after updating new anti-malware rules. Too many internal watchdog processes are created which use a lot of CPU resources. On some Web Security appliance machines under certain web traffic conditions, this may cause a lag when processing client requests. Workaround: Restart the appliance.
81243	**Cannot access HTTPS with Credential Encryption enabled in explicit forward mode in some cases** 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.
81416	**Cannot access FTP servers using Internet Explorer 7 in some cases** Users cannot access FTP servers using Internet Explorer 7 under the following conditions: • The “Enable FTP folder view (outside of Internet Explorer)” checkbox is enabled on the Tools > Internet options > Advanced page of Internet Explorer 7. • Internet Explorer 7 is configured to use passive mode for FTP transactions. • The Web Proxy is deployed in transparent mode. Workaround: You can either configure Internet Explorer to use active mode for FTP transactions, or you can enable IP spoofing for FTP transactions using the `advancedproxyconfig > nativeftp CLI` command.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

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** 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.
73151	**Web Proxy erroneously returns the "Policy: URL Filtering" notification page instead of the "DNS Failure" page in some cases** 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.
75322	**Access logs erroneously show "ns" as the Web Reputation filters score for DNS lookup failures** The access logs erroneously show "ns" as the Web Reputation filters score for DNS lookup failures instead of "dns."
75793	**Access logs erroneously record the ACL decision tag as DECRYPT instead of PASSTHROUGH in some cases** The access logs erroneously record the ACL decision tag as DECRYPT instead of PASSTHROUGH when the HTTPS server requests a client certificate. However, these transactions are passed through to the HTTPS server and are not decrypted.
72637	**Cannot upgrade from version 6.3 using Internet Explorer 6** When you use Internet Explorer 6 to access the appliance to upgrade AsyncOS for Web from version 6.3, the System Upgrade page does not display the Continue button which prevents the upgrade from processing completely. Workaround: Use a different browser or browser version to access the web interface for upgrading.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
72332	**Filter by User-Requested Transactions option on Web Tracking report erroneously includes extra transactions** 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.
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.
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.
68411	**AsyncOS is unable to join Active Directory domain with an embedded special character in short domain name** AsyncOS is unable to join an Active Directory domain when an embedded special character is in the short domain name.
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.

68993	**Web Proxy erroneously processes some URLs in client requests as the SaaS single sign-on URL**
	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.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
70369	**Cannot log into MSN Messenger from Mac OS X with decryption enabled** Users cannot log into MSN Messenger from Mac OS X when decryption is enabled.
70370	**Cannot log into MSN Messenger from Mac OS X in explicit forward mode** Users cannot log into MSN Messenger from Mac OS X when the Web Proxy is deployed in explicit forward mode.
66309	**Web Proxy erroneously drops CONNECT requests to ports other than port 443 in some cases** When you add a port other than port 443 to the Transparent HTTPS Ports field on the Security Services > HTTPS Proxy page, the Web Proxy erroneously drops CONNECT requests to that port. Workaround: After adding the port to the Transparent HTTPS Ports field, edit any Access Policy and submit and commit the changes.
69379	**Policy Trace erroneously lists “Global Access Policy” instead of “Global Routing Policy”** The Policy Trace feature erroneously lists “Global Access Policy” instead of “Global Routing Policy” when the transaction matches Global Routing policy.
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** FTP clients create a zero byte file on the server machine when the FTP Proxy blocks an upload due to outbound anti-malware scanning.
56045, 46555	**Decrypted connections to buggy HTTPS servers fail in some cases** Decrypted connections to some buggy HTTPS servers that use AES cipher fail after the SSL handshake completes. Workaround: Create a policy to pass through connections to the buggy server.
68269	**NTLMSSP authentication fails using Firefox 3.6 on Windows in some cases** Explicit forward requests from Firefox 3.6 on Windows fail NTLMSSP authentication. The client is repeatedly prompted for authentication credentials. This is due to a known limitation with Firefox 3.6. Workaround: Use a previous version of Firefox, such as version 3.5.x, or use Internet Explorer.
68288	**Loading some config files fail with an HTTPS redirect port error** When you upgrade AsyncOS for Web from a previous version and then export the configuration file and load it, the load configuration fails with the following error: `Configuration File was not loaded. Parse Error on element “prox_etc_auth_redirect_port” line number 3769 column 34 with value “443”: Authentication HTTPS redirect Port has to be a valid port number thats not a standard proxy port.` Workaround: Edit the configuration file so the <prox_etc_auth_redirect_port> values do not conflict with any values for <prox_etc_port>.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

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.
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.
51433	**Web Security appliance sends authenticated user name to external DLP servers in incorrect format** 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.
50632	**Default actions for global Decryption Policy URL categories are incorrect after upgrading from version 5.5.1** Default actions for global Decryption Policy URL categories are incorrect after upgrading from AsyncOS for Web version 5.5.1 when in the previous version Decryption Policies were not enabled. Each global Decryption Policy URL category action is set to the action configured for the global Access Policy URL category. Workaround: After upgrading, edit the global Decryption Policy URL category actions, submit, and commit.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
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.
49335	**Access logs sometimes show inconsistent ACL decision tags for tunneled HTTPS traffic when HTTPS proxy is disabled** 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.
50219, 50995	**IronPort Data Security scanning is bypassed for some websites** 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.
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.
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.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
48675	**End-user acknowledgement page appears twice in some cases** 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	**Users not copied in the IronPort 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 IronPort Customer Support ticket system automatically.
49152	**Authentication fails with Internet Explorer 7 in some cases** 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.
49593	**FTP clients create a zero byte file on the client machine when the FTP Proxy blocks a download due to anti-malware scanning** FTP clients create a zero byte file on the client machine when the FTP Proxy blocks a download due to anti-malware scanning.
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.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
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.
44023	**External authentication does not fail over to the next configured RADIUS server when DNS fails to resolve the first RADIUS server** 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.
46044	**Refreshing a website in Internet Explorer 6 causes the browser to hang in some cases** Internet Explorer 6 (version 6.0.2900.2180.xpsp_sp2_gdr.080814-1233) hangs under the following conditions: • The Web Security appliance is deployed in explicit forward mode. • Authentication and credential encryption are enabled. • The Internet Explorer 6 user clicks the Refresh button in the browser for content that already exists in the browser's cache. Workaround: Use a different version of Internet Explorer or a different browser. This is a known issue with Internet Explorer 6.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
46430	**Valid user is erroneously treated as a guest user in some cases** 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.
47184	**IronPort data security policies do not block very large files in some cases** 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.
44071	**Firefox version 3 does not display websites with embedded links correctly with decryption enabled in some cases** When Firefox version 3 explicitly forwards an HTTPS request, it does not display the website correctly when decryption is enabled and the website contains embedded links. This is due to stricter certificate trust changes in Firefox version 3. Workaround: Install the Web Security appliance root certificate as a trusted authority on all instances of Firefox 3.
44089	**Internet Explorer prompts for authentication multiple times when viewing files with multiple links in some cases** 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.
39947	**The loadconfig CLI command fails when the configuration file contains a webcache ignore list from a version before 5.2.1** The `loadconfig` CLI command fails when the configuration file contains a list of URLs or domains to not cache when the configuration file was saved from a version before 5.2.1.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
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."
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.
42584	**Some mobile devices that use ActiveSync cannot synchronize when authentication is enabled in some cases** 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.
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*.
39570	**Basic authentication fails when the password contains characters that are not 7-bit ASCII** Basic authentication fails when the password contains characters that are not 7-bit ASCII.
37455	**LDAP Authentication fails with LDAP referrals in some cases** 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 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description

40363	**Web Security appliance fails to join Active Directory domain and displays an erroneous message when the Active Directory server is in a different time mode**
	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** 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
39221	**Users cannot log in to AOL Instant Messenger server when the Web Security appliance decrypts traffic in some cases** When users try to connect to AOL Instant Messenger using client version 5.9 or later, they cannot log in when the Web Security appliance is configured to decrypt the traffic. This problem occurs even when you add the appliance's root certificate to the client machine as a trusted root certificate authority. Versions 5.9 and later of the AOL Instant Messenger client do not use the same repository of trusted root certificate authorities as other client applications, nor does it allow users to import trusted root certificates. Workaround: Create an HTTPS decryption policy that passes through traffic destined for the server AOL Instant Messenger uses to sign in, or use a previous version of AOL Instant Messenger client.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
39247	**Unable to join some Active Directory domains when the security setting for NTLM authentication is set to Domain mode** Joining an Active Directory domain in an NTLM authentication realm fails under the following conditions: • The `setntlmsecuritymode` CLI command is used to change the security setting to "domain." • The Active Directory domain requires "Network Security:Client Signing Required." Workaround: Use the `setntlmsecuritymode` CLI command to change the security settings to ADS mode.
39001	**Web Proxy generates a core file after upgrading the Web Security appliance without rebooting the appliance** The Web Proxy generates a core file after you upgrade the Web Security appliance, but before you reboot it. Workaround: Reboot the appliance. [Defect ID:]
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.
38468	**Web Security appliance cannot pass HTTPS traffic when the web server requests a client certificate in some cases** 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.
40097, 34159	**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.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
36280	**Upgrading from version 5.1 loses WBRS scores in some cases** When you changed the default WBRS score thresholds and upgrade from version 5.1, the Web Security appliance uses the changed (non-default) WBRS score for the Global Policy Group, but uses the default WBRS score for each user-defined web access policy group. Workaround: Edit each web access policy group and define the WBRS score as desired.
36229	**Web Security appliance does not create a computer account in the specified location on the Active Directory server if the computer account already exists in a different location** 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.
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).

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
36151	**NTLM authentication does not work after upgrading from a version prior to 5.2 in some cases** When you upgrade a pre-5.2 version Web Security appliance that uses NTLM authentication to version 5.2, NTLM authentication does not work when the account used to join the domain was not in the Administrator group. Workaround: Delete the old computer account in Active Directory. Next, edit the NTLM authentication realm and join the domain by entering a user name and password for a user that has the proper permissions.
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.
29133	**Load config functionality is inconsistent** Functionality on the System Administration tab > Configuration File page that allows you to save an appliance configuration file (`saveconfig`), or load a complete or partial configuration (`loadconfig`) might fail to commit a particular change in settings. For example, if you initially configure root DNS servers and then configure an authoritative DNS server, reloading the initial configuration does not configure root DNS.
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.”
32114	**Issue with manual updates and WCCP** Manual updates fail to download when the appliance is configured as a WCCP transparent proxy with IP spoofing enabled. The manual update succeeds when IP spoofing is disabled.
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.
25069, 28629, 31966	**Response message for manual updates might be inconsistent** The result code for manually updated components is always “Success — Component was successfully updated.” In some instances, update status and descriptive messaging might not reflect actual activity.

Table 4 Known Issues for AsyncOS 7.5.0 for Web (continued)

Defect ID	Description
37384, 26979, 23483, 23480	**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.
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 IronPort Customer Support.
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.
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.
32127	**Changing system time on Web Security appliance causes blank reports** When you change the time or date on the System Administration > Time Settings page and then view the Monitor > Overview page, the reports display "No data was found in the selected time range." Workaround: Reboot the Web Security appliance.

Related Documentation

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

- *Cisco IronPort AsyncOS for Web User Guide*

Service and Support

You can request our support by phone, email, or online 24 hours a day, 7 days a week.

During customer support hours (24 hours per day, Monday through Friday excluding U.S. holidays), an engineer will contact you within an hour of your request.

To report a critical issue that requires urgent assistance outside of our office hours, please contact IronPort using one of the following methods:

U.S. toll-free: 1(877) 641- 4766

International: http://cisco.com/web/ironport/contacts.html

Support Portal: http://cisco.com/web/ironport/index.html

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

♲ Printed in the USA on recycled paper containing 10% postconsumer waste.