Release Notes for Cisco IronPort AsyncOS 7.1.3 for Web

Published: November 9, 2011

Contents

This document contains release information for running Cisco IronPort AsyncOS AsyncOS 7.1.3 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 7.1 for Web

This section includes the following topics:

New Features in Version 7.1

Table 1 describes the new features and enhancements that have been added in the Cisco IronPort AsyncOS 7.1 for Web release.

Table 1 New Features for AsyncOS 7.1 for Web

Feature	Description
New Features	
Web Reporting and Web Tracking	AsyncOS for Web 7.1 supports advanced web reporting and web tracking. Web reporting and tracking aggregates information from individual security components as well as acceptable use enforcement components and records data that can be used to monitor your web traffic patterns and security risks. Web reporting and tracking gives managers visibility and insight into current operational data to help them refine policies, plan infrastructure, and measure productivity. You can run reports in real time to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals. You can also export raw data to a file. To use web reporting and tracking, use the Reporting > Web Tracking page. For more information, see the "Web Tracking Page" section in the "Web Security Appliance Reports" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Table 1 New Features for AsyncOS 7.1 for Web (continued)

Feature	Description
Centralized Reporting	AsyncOS for Web 7.1 includes the Centralized Reporting feature which, when the Web Security appliance is managed by a Security Management appliance, allows you to configure the Web Security appliance so that the Security Management appliance maintains the reports. You might want to enable Centralized Reporting when the Security Management appliance manages multiple Web Security appliances. This gives you a centralized view of web traffic across all Web Security appliances on the Security Management Appliance dashboard. When you enable Centralized Reporting, only the System Capacity and System Status reports are available on the Web Security appliance. To view the other reports, connect to the Security Management appliance. The Web Security appliance no longer stores data for the other reports. For more information, see the "Enabling Centralized Reporting" section in the "Reporting" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.
Anonymized Usernames on Reporting Pages	AsyncOS for Web 7.1 allows you to make usernames unrecognizable in all reports. Configure this on the Security Services > Reporting page using the **Anonymize usernames in reports** setting. However, administrators always see usernames.
Enhancements	
Enhanced: Reports	AsyncOS for Web 7.1 includes the following new reports: • Users • Web Sites • Web Tracking It also includes updated information for many existing reports. Due to all the reporting changes, when you upgrade to AsyncOS 7.1 for Web, all historical data stored on the Web Security appliance for the on-box reports **will be erased**. For more information, see Reporting Data Erasure, page 13. For more information, see the "Monitoring" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.
Fixed Known Limitations	Many previous known limitations have been fixed in this release. For more information, see Resolved Issues, page 21.

New Features in Version 7.0

Table 2 describes the new features and enhancements that have been added in the Cisco IronPort AsyncOS 7.0 for Web release.

Table 2 New Features for AsyncOS 7.0 for Web

Feature	Description
New Features	
New Feature: Cisco AnyConnect Secure Mobility	AsyncOS for Web 7.0 includes support for Cisco AnyConnect Secure Mobility which extends the network perimeter to remote endpoints, enabling the seamless integration of web filtering services offered by the Web Security appliance. AnyConnect Secure Mobility is a collection of features across multiple Cisco products that restores security and control in borderless networks. The Cisco products that work with AnyConnect Secure Mobility are the Cisco IronPort Web Security appliance, Cisco ASA 5500 series adaptive security appliance, and Cisco AnyConnect secure mobility client. Using AnyConnect Secure Mobility, mobile and remote users have a seamless experience and are always protected from risks as if they were local users connected within the network. When AnyConnect Secure Mobility is enabled on the Web Security appliance, you can distinguish remote users from local users. This allows you to perform the following tasks: • Create Identities and other policies for remote users. • View reports for remote traffic. • Enable single sign-on (SSO) for remote users. To protect remote users using always-on security, first you must enable the AnyConnect Secure Mobility feature on the Web Security appliance. When AnyConnect Secure Mobility is enabled, you can distinguish between remote users from local users when creating Identities. For more information, see the "Achieving Secure Mobility" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Table 2 New Features for AsyncOS 7.0 for Web (continued)

Feature	Description
New Feature: Application Visibility and Control	AsyncOS for Web 7.0 enhances the Cisco IronPort Web Usage Controls platform to include the Application Visibility and Control engine (AVC engine) which enables administrators to apply deeper controls to particular application types. The AVC engine is an acceptable use policy component that inspects web traffic to gain deeper understanding and control of web traffic used for applications. Application control gives you more granular control over web traffic than just URL filtering. For example, you can block streaming media from sports sites, but not news sites. To control applications using the AVC engine, enable the AVC engine when you enable Cisco IronPort Web Usage Controls, and then define application control settings in the Access Policies. For more information, see the "Understanding Application Visibility and Control" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Table 2 New Features for AsyncOS 7.0 for Web (continued)

Feature	Description
New Feature: Safe Search and Site Content Rating Enforcement	AsyncOS for Web 7.0 uses the AVC engine to filter adult content from some web searches and websites. You might want to do this to allow access to these sites, such as google.com and youtube.com, while still restricting potentially unsafe content from reaching users. AsyncOS for Web offers the following features to filter adult content: • **Enforce safe searches.** Most search engines allow the safe search feature to be enabled and disabled by end users. You can configure the Web Security appliance so that outgoing search requests appear to search engines as safe search requests. This gives the control to an administrator on the network instead of the end user. You might want to do this to prevent users from bypassing acceptable use policies using search engines. • **Enforce site content ratings.** Many content sharing sites that serve user-generated photos and videos classify some of their content as adult. They allow users to restrict their own access to the adult content on these sites by either enforcing their own safe search feature or blocking access to adult content, or both. This classification feature is commonly called content ratings. To enforce safe searches and site content ratings, configure the URL filtering settings for an Access Policy. For more information, see the "Controlling Instant Messaging Traffic" section in the "URL Filters" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.
New Feature: Bandwidth Control for Streaming Media	AsyncOS for Web 7.0 uses the AVC engine to control the amount of bandwidth used for streaming media applications. You can define an overall bandwidth limit and per user bandwidth limits. When both the overall limit and user limit applies to a transaction, the most restrictive option applies. For more information, see the "Controlling Bandwidth" section in the "Understanding Application Visibility and Control" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Table 2 New Features for AsyncOS 7.0 for Web (continued)

Feature	Description
New Feature: HTTP Instant Messaging Controls	AsyncOS for Web 7.0 uses the AVC engine to apply control settings to some instant messenger (IM) traffic that runs on top of HTTP. You can block or monitor the IM traffic, and depending on the IM service, you can block particular activities (also known as application behaviors) in an IM session. For example, you can allow an IM session with a particular IM service provider, but block file transfers within that session. You control IM traffic by configuring Instant Messenger application settings on the Applications Visibility and Control page of Access Policies. For more information, see the "Controlling Instant Messaging Traffic" section in the "Understanding Application Visibility and Control" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.
New Feature: SaaS Access Control	AsyncOS for Web 7.0 includes the SaaS Access Control feature which provides IT administrators with seamless, secure controls necessary for managing access to Software as a Service (SaaS) applications and enforcing security policies. SaaS Access Control allows IT administrators to easily control authentication and authorization for users who need to access SaaS applications. When you enable Cisco SaaS Access Control, users log into the configured SaaS applications using their network authentication user credentials. That means they use the same user name and password for all SaaS applications as well as network access. You can choose whether users are transparently signed in (single sign-on functionality) or prompted to enter their authentication user name and password. The SaaS Access Control solution uses the Security Assertion Markup Language (SAML) to authorize access to SaaS applications. It works with SaaS applications that are compliant with SAML version 2.0. To enable SaaS Access Control, you must configure settings on both the Web Security appliance and the SaaS application. It is very important that the settings you configure on the appliance and SaaS application match each other appropriately. For more information, see the "Controlling Access to SaaS Applications" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Table 2 New Features for AsyncOS 7.0 for Web (continued)

Feature	Description
New Feature: Sophos Anti-Virus Scanning	AsyncOS for Web 7.0 adds the Sophos scanning engine to the list of possible Web Security appliance on-box anti-malware scanning engines. The Sophos engine offers award-winning protection against known and unknown threats using their Genotype and Behavioral Genotype Protection. The Sophos Genotype virus detection technology proactively blocks families of viruses, and Behavioral Genotype Protection automatically guards against zero-day threats by analyzing the behavior of the code before it executes—offering protection from new and existing viruses, trojans, worms, spyware, adware, and other potentially unwanted applications (PUAs). For more information, see the "Anti-Malware Services" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.
New Feature: Transparent User Identification for Novell eDirectory	AsyncOS for Web 7.0 allows you to configure the Web Security appliance so that it identifies users by an authenticated user name transparently—that is, without prompting the end user. You might want to do this to: • Create a single sign-on environment so users are not aware of the presence of a proxy on the network. • Use authentication based policies to apply to transactions coming from client applications that are incapable of displaying the authentication prompt to end users. To identify users transparently, you must define at least one LDAP authentication realm that supports Novell eDirectory. For more information, see the "Identifying Users Transparently" section in the "Identities" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Table 2 New Features for AsyncOS 7.0 for Web (continued)

Feature	Description
New Feature: Outbound Malware Scanning	AsyncOS for Web 7.0 includes protects data and objects leaving the network by providing outbound malware scanning. The IronPort Dynamic Vectoring and Streaming (DVS) engine scans transaction requests as they leave the network in real-time. By working with the IronPort DVS engine, the Web Security appliance allows you to prevent users from unintentionally uploading malicious data. To restrict malicious data from leaving the network, the Web Security appliance provides the Outbound Malware Scanning policy groups. You define which uploads are scanned for malware, which anti-malware scanning engines to use for scanning, and which malware types to block. For more information, see the "Outbound Malware Scanning" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.
New Feature: Application Scanning Bypass	AsyncOS for Web 7.0 allows administrators to easily bypass certain web applications from being scanned by the Web Proxy by checking a checkbox. This can prevent integration issues with web applications that do not interact well with proxies. In version 7.0, you can bypass scanning for Cisco Webex. For more information, see the "Bypassing Application Scanning" section in the "Web Proxy Services" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.
New Feature: Allow User One Login at a Time	AsyncOS for Web 7.0 allows administrators to control whether or not an authenticated user can access the Internet from multiple machines simultaneously. You might want to restrict access to one machine to prevent users from sharing their authentication credentials with non-authorized users. When a user is prevented from logging at a different machine, an end-user notification page appears. You can choose whether or not users can click a button to login as a different username. To restrict an authenticated user from accessing the Internet from a different machine, configure the User Session Restrictions settings on the Network > Authentication page. For more information, see the "Configuring Global Authentication Settings" section in the "Authentication" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Table 2 New Features for AsyncOS 7.0 for Web (continued)

Feature	Description
New Feature: WBRS Threat Details	AsyncOS for Web 7.0 now provides additional details on the threat which caused a site to have a low reputation. This information is included in end-user notification pages when a user is blocked due to low reputation, as well as the access logs. There is also a new report which displays information on how many transactions have been blocked due to each threat type.
New Feature: What's New In This Release	AsyncOS for Web 7.0 now provides a way to easily view which features are new or enhanced in the current version of AsyncOS. To do this, choose New in this Release from the Support and Help menu.
Enhancements	
Enhanced: Per Identity Authentication Settings	AsyncOS for Web 7.0 now allows you to define authentication surrogate type settings (either cookie or IP address) per Identity instead of globally for all Identities. You might want to define different surrogate types for different Identities if you want to use IP addresses for almost all users, but use cookie surrogates on systems like kiosks which are shared among many users. For more information, see the "Creating Identities" section in the "Identities" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.
Enhanced: PAC File Hosting	Effective in AsyncOS for Web 7.0, you can use any port to serve PAC files stored on the Web Security appliance. In previous versions, you could only specify ports for serving PAC files that were not listed as an HTTP port to proxy on the Security Services > Proxy Settings page. However, for PAC files to be served through HTTP proxy ports, such as port 80, you must explicitly configure the hostnames that should serve PAC files and choose a default PAC file for each hostname. Do this when you upload the PAC file to the Web Security appliance using the Security Services > Proxy Auto-Configuration File Hosting page. For more information, see the "Adding PAC Files to the Web Security Appliance" section in the "Web Proxy Services" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Table 2 New Features for AsyncOS 7.0 for Web (continued)

Feature	Description
Enhanced: Reports	AsyncOS for Web 7.0 includes the following new reports: • Application Visibility • Mobile User Security • System Capacity It also includes updated information for many existing reports. For more information, see the "Monitoring" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Table 2 New Features for AsyncOS 7.0 for Web (continued)

Feature	Description
Enhanced: Advancedproxy-config CLI Command	AsyncOS for Web 7.0 includes many new commands for fine tuning the Web Proxy and how it handles transactions. For example, you can configure the Web Proxy so that matching LDAP usernames is not case sensitive when matching policy groups to a transaction. For more information, see the "Advanced Proxy Configuration" section in the "Web Proxy Services" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.
Enhanced: Logging	AsyncOS 7.0 for Web includes the following new types of log files: • **AVC Engine Logs.** Records debug messages from the AVC engine. • **AVC Engine Framework Logs.** Records messages related to communication between the Web Proxy and the AVC engine. • **Mobile User Security Daemon Logs.** Records the interaction between the Web Security appliance and the AnyConnect client, including the status check. • **SaaS Auth Logs.** Records messages related to the SaaS Access Control feature. • **Sophos Logs.** Records the status of anti-malware scanning activity from the Sophos scanning engine. • **Sophos Integration Framework Logs.** Records messages related to communication between the Web Proxy and the Sophos scanning engine. • **UDS Logs.** Records data about how the Web Proxy discovers the user name without doing actual authentication. It includes information about interacting with the Cisco adaptive security appliance for the AnyConnect Secure Mobility as well as integrating with the Novell eDirectory server for transparent user identification. Also, new log fields are available in the access logs and W3C access logs for AVC engine and WBRS threat details.

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 7.1.1 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 version 7.1.1.**

Reporting Data Erasure

When you upgrade to AsyncOS 7.1 for Web, 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 54.

Configuration Files

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

Compatibility with IronPort AsyncOS for Security Management

Features on AsyncOS 7.1.2 for Web and later are supported by AsyncOS for Security Management version 7.2.2.

IronPort Notification Pages

AsyncOS for Web 7.0 includes new IronPort Notification pages. If the IronPort 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 IronPort Notification pages.

The following pages are added in version 7.0:

- ERR_ADULT_CONTENT
- ERR_AVC
- ERR_MALWARE_SPECIFIC_OUTGOING
- ERR_PROXY_PREVENT_MULTIPLE_LOGIN
- ERR_SAAS_AUTHENTICATION
- ERR_SAAS_AUTHORIZATION
- ERR_SAML_PROCESSING
- ERR_WBRS

Note Effective in AsyncOS for Web 7.0, users are shown ERR_WBRS instead of ERR_MALWARE_GENERAL when users are blocked due to web reputation filtering. The ERR_WBRS page includes more specific information, such as the threat type and threat reason.

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

Changes in Behavior

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

Reporting Changes

In AsyncOS for Web 7.1, several enhancements and changes have been made to most reports. In addition, the Monitor menu has changed to the Reporting menu, and the reports have been reorganized under the Reporting menu.

Reports that display data in table format have interactive column headings that can be configured to sort the data in each column specific to your needs for viewing data on that page. You can also choose which columns to display in a table.

In addition, the following reports have been removed:

- The Monitor > Client Web Activity report has been replaced with Reporting > Users.
- The Monitor > Web Site Activity report has been replaced with Reporting > Web Sites.

Supported SSL Versions

In AsyncOS for Web 7.0, the HTTPS Proxy also works with HTTPS websites that support SSL version 3 only. Additionally, it no longer works with HTTPS websites that only support SSL version 2.

Authentication Surrogate Type

In AsyncOS for Web 7.0, where you configure the authentication surrogate type settings has changed. Previously, you configured the authentication surrogate type globally on the Network > Authentication page. Now, you configure the authentication surrogate type per Identity group.

When you upgrade, each existing Identity group inherits the previously configured global setting.

After upgrading, when you create a new Identity group, the default surrogate type depends on the Web Proxy deployment mode. In transparent mode, the default surrogate type is IP address, not cookie.

Anti-Malware Logging and Reporting Changes

In AsyncOS for Web 7.0, how the access logs report malware based on the URL request has changed. Previously, when an anti-malware scanning engine blocked or monitored a transaction based on the URL in the client request, the ACL decision tag in the access logs was BLOCK_AMW_REQ or MONITOR_AMW_REQ.

Now, BLOCK_AMW_REQ and MONITOR_AMW_REQ are used to indicate an Outbound Malware Scanning Policy blocked or monitored an upload request because the body produced a positive malware verdict. Two new ACL decision tags have been introduced to report when an anti-malware scanning engine blocked or monitored a transaction based on the URL in the client request: BLOCK_AMW_RESP_URL and MONITOR_AMW_RESP_URL.

The following table describes each of these ACL decision tags in version 7.0:

ACL Decision Tag	Current Description and Behavior
BLOCK_AMW_REQ	The Web Proxy blocked the request based on the Anti-Malware settings for the Outbound Malware Scanning Policy group. The request body produced a positive malware verdict.
BLOCK_AMW_RESP_URL	The Web Proxy suspects the URL in the HTTP request might not be safe, so it blocked the transaction at request time based on the Anti-Malware settings for the Access Policy group.

ACL Decision Tag	Current Description and Behavior
MONITOR_AMW_REQ	The Web Proxy scanned the request based on the Anti-Malware settings for the Outbound Malware Scanning Policy group. The request body produced a positive malware verdict, but the Web Proxy did not block the transaction.
MONITOR_AMW_RESP_URL	The Web Proxy suspects the URL in the HTTP request might not be safe, but it monitored the transaction based on the Anti-Malware settings for the Access Policy group.

Malware Scanning Verdict Logging Changes

In AsyncOS for Web 7.1, how malware scanning verdict values are recorded in the access logs has changed. Previously in AsyncOS for Web 7.0, they were recorded as string values, such as "Phishing URL." Now, they are recorded as integers. The current behavior is consistent with AsyncOS for Web versions before version 7.0.

Also, effective in AsyncOS for Web 7.0, the numeric values for each malware scanning verdict has changed. For a list of values, see the "Malware Scanning Verdict Values" section in the "Logging" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.

Before upgrading, it is recommended that you save a PDF of the hour, day, week, and 30 day reports for any malware reports you want to preserve. For example, you might want to save the Overview, Web Site Activity, Client Malware Risk, and Anti-Malware reports.

LDAP User Name Matching

In AsyncOS for Web 7.0, how LDAP user names are match has changed. Previously, LDAP user name matching was case sensitive. When a user entered "JSmith" as her user name, she would match all configured policies for "JSmith" and would not match any policy configured for "jsmith."

Now, the following behavior occurs:

- When you receive a new Web Security appliance with version 7.0 already installed, LDAP user name matching is case insensitive. That is, user "JSmith" matches all policies configured for both "JSmith" and "jsmith."
- When you upgrade a previous version, the previous behavior is retained such that LDAP user name matching is case sensitive.

You can choose whether or not the Web Proxy should ignore case when matching user names against the policy groups using the `advancedproxyconfig > authentication` CLI command.

Web Interface Name Changes

Effective in AsyncOS for Web 7.1, some web interface pages have changed names. The Monitor menu has changed to the Reporting menu.

Effective in AsyncOS for Web 7.0, some web interface pages have changed names. The following table compares the previous page names to the current page names.

Previous Page	New Page
Monitor > Malware Risk	Reporting > Client Malware Risk
Web Security Manager > IronPort Data Security Policies	Web Security Manager > IronPort Data Security
Web Security Manager > External DLP Policies	Web Security Manager > External Data Loss Prevention
Web Security Manager > Time Ranges	Web Security Manager > Defined Time Ranges
Web Security Manager > Proxy Bypass	Web Security Manager > Bypass Settings
Security Services > Proxy Settings	Security Services > Web Proxy
Security Services > FTP Proxy Settings	Security Services > FTP Proxy

In addition to these changes, some columns in the Access Policies table on the Web Security Manager > Access Policies page have changed.

- The "Applications" column is now called "Protocols and User Agents."

- A new column exists called Applications. It allows you to configure which web applications and application types, such as streaming media, to block or limit.
- The summarized text in the Access Policies table for each column has been shortened and simplified. The summarized text now only shows items that are blocked, limited, and/or in use.

advancedproxyconfig Command Changes

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

End-User Notification Pages Related Commands

In AsyncOS for Web 7.0, the CLI command you use to edit the content of the IronPort Notification pages stored on the Web Security appliance has changed. Previously, you used an `advancedproxyconfig > miscellaneous` command. Now, you use the `advancedproxyconfig > eun` CLI command.

DNS Related Commands

In AsyncOS for Web 7.0, some DNS related commands have changed. Previously, the `advancedproxyconfig > DNS` CLI commands below existed, but the values you configured had no effect. Now, they have been removed in version 7.0.

- Enter the time to cache successful DNS results if DNS does not provide TTL (in seconds).
- Enter the time to cache results of DNS errors (negative DNS caching) (in seconds).

The Web Proxy applies the default values used by the DNS server configured.

Logging Custom Fields in the Access Logs

In AsyncOS for Web 7.0, the web interface strictly enforces the correct syntax when entering format specifiers in the Access logs. Previously, the web interface allowed you to enter static text next to format specifiers with no spaces in between. Now, you must include spaces between static text and the format specifiers. This improves logging performance.

When you upgrade from a previous version that includes static text and format specifiers, validation of the custom fields fails, but logging of the Access logs succeeds.

Access Log Changes

In AsyncOS for Web 7.0, the data recorded in the access logs has changed. Now, the scanning verdict information (located in angled brackets at the end of each access log entry) contains additional fields. In addition, there are new possible values for the ACL decision tags. If you use any third party software to process the access logs you need to change your configuration to process the new format.

For more information on the current access log format, see the "Access Log File" section in the "Logging" chapter of the *Cisco IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

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.

Upgrade Paths

You can upgrade to release 7.1.3-019 from the following versions:

- 6.3.3-015
- 6.3.7-018
- 7.1.0-307
- 7.1.1-027
- 7.1.1-038
- 7.1.2-080
- 7.1.3-014

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 13.

Resolved Issues

This section includes the following topics:

Resolved Issues in Version 7.1.3

Table 3 lists the issues that were resolved in version 7.1.3 of AsyncOS for Web.

Table 3 Resolved Issues in AsyncOS 7.1.3 for Web

Defect ID	Description
75098	**Fixed: Web Proxy performance is slow on some hardware models in some networks** Previously, in some network conditions the Web Proxy would eventually run out of chunk memory resources on the S370 and S670 hardware models and Web Proxy performance would slow down. This no longer occurs.
77926	**Fixed: Some anti-malware category actions change after upgrading** Previously, after upgrading from a previous version the configured action for some anti-malware categories changed. This no longer occurs.
81046	**Fixed: Russia Daylight Saving Time** This version of AsyncOS for Web adopts the latest timezone rules for Russia that cancel Daylight Saving Time.
81294	**Fixed: Uploading files takes a long time with IronPort Data Security enabled in some cases** Previously, uploading files to some web servers took a long time when IronPort Data Security was enabled because the Web Proxy would eventually run out of chunk of memory. This no longer occurs.
80810	**Fixed: Web Security appliance trusts DigiNotar as a root certificate authority** Previously, the Web Security appliance trusted DigiNotar as a root certificate authority. It also trusted DigiNotar's intermediate certificates issued by the State of Netherlands. This no longer occurs. The Web Security appliance no longer includes DigiNotar in the list of trusted certificate authorities. It has also blacklisted DigiNotar's intermediate certificates. You can configure how the appliance handles HTTPS traffic (drop, decrypt, or monitor) when it encounters an unknown root certificate authority (such as DigiNotar's) when you configure the HTTPS Proxy.

Table 3 Resolved Issues in AsyncOS 7.1.3 for Web (continued)

Defect ID	Description
80231	**Fixed: Web Proxy generates a core file when serving cached responses with no body content and no Content-Length HTTP header** Previously, the Web Proxy generated a core file when serving cached responses that contained no body content and no Content-Length HTTP header. This no longer occurs.
79612	**Fixed: Cannot connect to some HTTPS sites with decryption enabled and set to pass through connections in some cases** Previously, clients could not connect to the following types of HTTPS servers: • Server uses non-SSL compliant traffic, such as Skype • Server only supports TLS and not SSL. • Server ties to negotiate SSL or TLS options that the Web Proxy cannot understand. Under the following conditions: • The Web Proxy received client requests on configured SSL ports. • Decryption was enabled, and the Decryption Policy was configured to pass through connections. • The Web Proxy was configured to allow non-SSL traffic on SSL ports. (`advancedproxyconfig > miscellaneous` CLI command) This no longer occurs. Now, the Web Proxy always handles these connections according to how it is configured to treat non-SSL traffic on SSL ports.
76193	**Fixed: Cannot connect to some web servers when they send a non-HTTP response** Previously, clients could not connect to some web servers when they sent a non-HTTP response. This no longer occurs.
49207	**Fixed: File system corruption on S160** Previously, the file system on S160 hardware models would get corrupt when the appliance lost power in some cases. This no longer occurs.

Table 3 Resolved Issues in AsyncOS 7.1.3 for Web (continued)

Defect ID	Description
69544	**Fixed: Upgrading AsyncOS for Web on S160 appliances takes longer than usual and produces errors in some cases** Previously, upgrading AsyncOS for Web on S160 appliances took longer than usual to complete and produced errors when internal processes were writing a lot of data to disk. This issue has been resolved. However, the improved upgrade time will be observed when upgrading from AsyncOS for Web 7.1.3 to a later version.
70014	**Fixed: Web Proxy becomes unresponsive for several minutes while processing WBRS updates on S160 appliances** Previously, the Web Proxy became unresponsive for several minutes while processing WBRS updates on S160 appliances. This no longer occurs.
75836, 75960, 76921, 76978, 77684	**Fixed: Hard drive and RAID issues on S160 appliances** 7.1.3 introduces a new RAID driver for the S160 platform, providing faster disk I/O than the previous version. In addition to addressing the specific issues noted in these Defect IDs, this new driver provides an increase in overall system performance as compared to previous releases.
76131, 70679	**Fixed: Web Proxy generates a core file when clients use FTP over HTTP to access some FTP servers** Previously, the Web Proxy generated a core file when clients used FTP over HTTP to access some FTP servers. This no longer occurs.
77849	**Fixed: Web Proxy erroneously stops sending upload requests to the external DLP server in some cases** Previously, the Web Proxy erroneously stopped sending upload requests to the external DLP server when it incorrectly counted the number of simultaneous ICAP request connections and then reached the maximum number of connections allowed. This no longer occurs.

Resolved Issues in Version 7.1.2

Table 4 lists the issues that were resolved in version 7.1.2 of AsyncOS for Web.

Table 4 Resolved Issues in AsyncOS 7.1.2 for Web

Defect ID	Description
50248	**Fixed: Web Proxy generates a core file when it encounters memory management issues** Previously, the Web Proxy generated a core file when it encountered internal memory management issues. This no longer occurs.
71187	**Fixed: Invalid HTTPS certificate handling** Previously, when the HTTPS Proxy encountered a destination server using a certificate with multiple errors (such as unrecognized root authority), the HTTPS Proxy performed the configured action for unrecognized root authority before all other types of certificate errors. This no longer occurs. Now, the HTTPS Proxy performs the action specified for the error that has a higher ranking using the following ranking: • Expired certificates • Unrecognized root authority • All other errors • Mismatched hostname
71202	**Fixed: FTP Proxy generates a core file when the FTP client closes a connection very early** Previously, the FTP Proxy generated a core file when the FTP client closed a connection before the Web Proxy could accept it. This no longer occurs.
72382	**Fixed: Web Security appliance locks up and then automatically reboots when a large number of SSH connections are made to the management interface** Previously, the Web Security appliance locked up and then automatically rebooted when a large number of SSH connections were made to the management interface, such as from automated scripts. This no longer occurs. Now, only 100 concurrent SSH sessions are allowed.

Table 4 Resolved Issues in AsyncOS 7.1.2 for Web (continued)

Defect ID	Description
72849	**Fixed: Uploading a zero byte file using FTP causes the FTP session to remain open until the FTP server times out the connection** Previously, uploading a zero byte file using FTP caused the FTP session to remain open until the FTP server timed out the connection. This no longer occurs.
73499	**Fixed: Internal reporting process encounters an error and automatically restarts multiple times when rolling up daily data in the database tables** Previously, the internal reporting process encountered an error and automatically restarted multiple times when rolling up daily data in the database tables. This no longer occurs.
73808	**Fixed: Web Proxy stops processing client requests after upgrading in some cases** Previously, the Web Proxy stopped processing client requests after upgrading from a previous version that has the Web Proxy listening for traffic on port 8081. This no longer occurs.
73888	**Fixed: Some data on some HTTPS web pages does not appear when the server is decrypted** Previously, some data, such as graphics, did not appear on some HTTPS pages when the server was decrypted. This no longer occurs.
74075	**Fixed: Native FTP client connections erroneously reach a very high number in some cases** Previously, native FTP client connections erroneously reached a very high number when processing an unscannable file. This no longer occurs.
74537	**Fixed: Application fault occurs in the authcache > list CLI command in some cases** Previously, an application fault occurred in the `authcache > list` CLI command when the authentication cache contained a large number of entries. This no longer occurs.
74594	**Fixed: Web Tracking report does not include all data in some cases** Previously, the Web Tracking report did not include all data from client applications that do not URL encode URLs in HTTP requests. This no longer occurs.

Table 4 Resolved Issues in AsyncOS 7.1.2 for Web (continued)

Defect ID	Description
74814	**Fixed: Web Proxy erroneously returns an internal error notification page instead of the Gateway Timeout page** Previously, the Web Proxy erroneously returned the "Internal Error" end-user notification page instead of the "Gateway Timeout" page when it could not connect to servers in some cases. This no longer occurs.
75013	**Fixed: System Capacity report with custom dates erroneously shows data for the wrong date range** Previously, the System Capacity report with custom dates erroneously showed data for the wrong date range. This no longer occurs.
75111	**Fixed: FTP Proxy generates a core file when changing the current directory in an FTP client with a very large path** Previously, the FTP Proxy generated a core file when changing the current directory in an FTP client with a very large path. This no longer occurs. Now, the maximum allowed FTP server path size is 1024 by default. You can configure the maximum allowed FTP server path size using the `advancedproxyconfig > nativeftp` CLI command.
75245	**Fixed: proxystat CLI command leaks memory and eventually causes the appliance to reboot** Previously, when you enabled the `proxystat` CLI command, it leaked memory and eventually caused the appliance to reboot. This no longer occurs.
75305	**Fixed: W3C log field "time" erroneously records local time instead of Coordinated Universal Time (UTC) time** Previously, the W3C log field "time" erroneously recorded the local time instead of the Coordinated Universal Time (UTC) time. This no longer occurs.
75451	**Fixed: grep CLI command erroneously does not accept an empty regular expression string** Previously, the `grep` CLI command erroneously did not accept an empty regular expression string. This no longer occurs.
75542	**Fixed: Very large CONNECT uploads take too long to process and use too many CPU cycles** Previously, very large CONNECT uploads took too long to process and used too many CPU cycles. This no longer occurs.

Table 4 Resolved Issues in AsyncOS 7.1.2 for Web (continued)

Defect ID	Description
75751	**Fixed: Exported Web Tracking report does not include client IP address data** Previously, when you exported a Web Tracking report to a CSV file, the exported file did not include client IP address data. This no longer occurs.
75791	**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 the "Apply same surrogate settings to explicit forward requests" setting in the Identity groups was disabled. This no longer occurs.
76501	**Fixed: Exported Web Site report does not include the "Web Site" column in some cases** Previously, when you exported the Web Site Detail report to a CSV file, the URL Categories Matched table in the exported file did not include the "Web Site" column. This no longer occurs.
76682	**Fixed: Fraudulent certificates issued by Comodo** AsyncOS for Web 7.1.2 checks for fraudulent certificates issued by the Comodo root authority. This prevents the Web Security appliance from accepting any of the fraudulent certificates issued by Comodo.
76825	**Fixed: Dynamic Content Analysis engine does not work correctly after the Web Proxy reboots in some cases** Previously, the Dynamic Content Analysis engine did not work correctly after the Web Proxy rebooted in some cases. This no longer occurs.
76919	**Fixed: Web Proxy restarts after processing several streaming transactions in some cases** Previously, when the Web Proxy was handling streaming data on a constrained network, it would eventually run out of chunk memory resources, become unresponsive, and would restart due to an internal watchdog process. This no longer occurs.
77310	**Fixed: Web Tracking report includes the incorrect IP address for users who log in from multiple computers** Previously, the Web Tracking report included the incorrect IP address for users who logged in from multiple computers. This no longer occurs.

Resolved Issues in Version 7.1.1

Table 5 lists the issues that were resolved in version 7.1.1 of AsyncOS for Web.

Table 5 Resolved Issues in AsyncOS 7.1.1 for Web

Defect ID	Description
77757	**Fixed: Web Proxy stops processing client traffic after receiving a forged DNS request in some cases** Previously, when the Web Proxy received a forged DNS request in a UDP packet with a source IP address of 127.x.x.x, it stopped processing DNS requests and was unable to process client traffic. This no longer occurs.
72227	**Fixed: Web Proxy generates a core file when processing multiple simultaneous connections to a web server that returns a malformed response** Previously, the Web Proxy generated a core file when processing multiple simultaneous connections to a web server that does not include a blank end of header line in its response. This no longer occurs.
75668	**Fixed: LDAP authentication intermittently fails when using group authorization in some cases** Previously, LDAP authentication intermittently failed when using group authorization due to leaked LDAP connections. This no longer occurs.
72380, 75545	**Fixed: Web Proxy generates a core file when processing an explicit POST request to a hostname that is unresolvable by DNS** Previously, the Web Proxy generated a core file when processing an explicit POST request to a hostname that is unresolvable by DNS. This no longer occurs.
75167	**Fixed: Web Proxy begins to fail some requests while processing simultaneous large downloads on S160 models** Previously, the Web Proxy began to fail some requests while processing simultaneous large downloads on S160 models. The Proxy logs included an error message saying "Out of memory blocks in DataChunk_Alloc." This no longer occurs.
74073	**Fixed: Web Proxy generates a core file when processing a POST request to a domain name that does not resolve in some cases** Previously, the Web Proxy generated a core file when processing a POST request to a domain name that did not resolve in some cases. This no longer occurs.

Table 5 Resolved Issues in AsyncOS 7.1.1 for Web (continued)

Defect ID	Description
75077, 75129	**Fixed: FTP Proxy erroneously closes native FTP connections prematurely when processing active requests from some FTP clients** Previously, the FTP Proxy erroneously closed native FTP connections prematurely when processing active requests from some FTP clients. This no longer occurs.
74445	**Fixed: Web Proxy generates a core file when processing some transparent upload requests to some servers** Previously, the Web Proxy generated a core file when processing some transparent upload requests to some servers. This no longer occurs.
74539, 74500	**Fixed: Web Proxy under heavy load could become unresponsive when running scheduled reports on some models in some cases** Previously, the Web Proxy under heavy load could become unresponsive when running scheduled reports due to memory usage issues. When this occurred on some models, the Web Proxy did not automatically reboot. This no longer occurs. Now, the memory issues have been addressed so that the Web Proxy is less likely to become unresponsive, and if it does encounter this state, all models reboot automatically.
74482	**Fixed: CLI can erroneously be used to access the machine-level prompt** Previously, the CLI could erroneously be used to access the machine-level prompt. This no longer occurs.
31853	**Fixed: Symbolic links are broken when viewing FTP directory in a browser** Previously, when you used a web browser to access an FTP directory that contained symbolic links, access was broken to the subdirectory or file where the symbolic link pointed. This no longer occurs.
44445	**Fixed: NTLM authentication fails after a period of time when a policy group uses many authorization groups** Previously, NTLM authentication failed after a period of time when a policy group used many authorization groups from an NTLM authentication realm, such as over 100 groups. When the list of all group IDs approached 6 KB, an internal process started to leak memory and failed to authenticate users against the Active Directory server. This no longer occurs. Now, when the list of group IDs approaches 300 or more groups (14 KB), users may fail to authenticate, but no memory leak occurs.

Table 5 Resolved Issues in AsyncOS 7.1.1 for Web (continued)

Defect ID	Description
55752	**Fixed: Application fault occurs in the web interface when disabling object blocking for the global Access Policy** Previously, an Application fault occurred in the web interface when disabling object blocking for the global Access Policy. This no longer occurs.
69830	**Fixed: Web Proxy erroneously removes HOST headers from server responses** Previously, when the destination server includes a HOST header in its response, the Web Proxy removes the header before sending the response to the client. This no longer occurs.
71284	**Fixed: Web interface does not allow an empty value for the Base DN property in LDAP authentication realms** Previously, the web interface did not allow an empty value for the Base DN property in LDAP authentication realms. This no longer occurs.
71931, 72018	**Fixed: Native FTP transactions are delayed when using an upstream proxy in some cases** Previously, when the appliance used an upstream proxy server and an FTP client sent multiple native FTP transactions in succession, the transactions were delayed due to the appliance mismanaging connections to the proxy server and to the client. This no longer occurs.
71986	**Fixed: Some users are erroneously prompted for authentication after being transparently identified using Novell eDirectory in some cases** Previously, some users were erroneously prompted for authentication after being transparently identified using Novell eDirectory when the NetworkAddress attribute value in eDirectory was in some formats. This no longer occurs.
72211	**Fixed: Clients cannot access files with the "#" character in the filename using FTP over HTTP** Previously, clients could not access files with the "#" character in the filename using FTP over HTTP because the Web Proxy did not URL encode the "#" character. This no longer occurs. Now, the Web Proxy URL encodes the "#" character when returning the FTP directory list to the client application.

Table 5 Resolved Issues in AsyncOS 7.1.1 for Web (continued)

Defect ID	Description
72254	**Fixed: An internal process runs out of memory and generates a core file when creating time-based Decryption Policies in some cases** Previously, an internal process ran out of memory and generated a core file when creating multiple time-based Decryption Policies. This no longer occurs.
72596, 73142	**Fixed: Predefined URL categories are not displayed in policy groups using Microsoft Internet Explorer in some cases** Previously, predefined URL categories were not displayed in access and decryption policy groups using some versions of Microsoft Internet Explorer when a custom URL category was defined. This no longer occurs.
72796	**Fixed: An application fault occurs when rebooting the appliance very soon after upgrading from a previous version in some cases** Previously, an application fault occurred with the internal logging process when you upgraded AsyncOS from a previous version and rebooted the appliance and then rebooted the appliance again within a few minutes after the upgrade and reboot complete.
73157	**Fixed: Access logs in Apache format erroneously include quotes around the date** Previously, access logs in Apache format erroneously included quotes around the date. This no longer occurs. Now, the date is surrounded by brackets only in the Apache formatted access logs.
73209	**Fixed: Web Proxy returns "200 OK" instead of "200 Connection established" for successful CONNECT requests** Previously, Web Proxy returned "200 OK" instead of "200 Connection established" for successful CONNECT requests. This change in behavior breaks some non-compliant client applications that depend on the "200 Connection established" phrase. This no longer occurs.
73262	**Fixed: System Capacity > Bandwidth Out (Bytes) report displays data in bits, not bytes** Previously, the System Capacity > Bandwidth Out (Bytes) report displayed data in bits, not bytes. This no longer occurs. Now, it displays data in bytes.

Table 5 Resolved Issues in AsyncOS 7.1.1 for Web (continued)

Defect ID	Description
73476	**Fixed: W3C access logs stop logging data when it contains some fields in some cases** Previously, the W3C access logs stopped logging data when it contained the x-resultcode-httpstatus or x-hierarchy-origin fields in some cases. This no longer occurs.
73615	**Fixed: Web Proxy no longer includes the Content-Length header in server responses that cannot contain body content** Previously, the Web Proxy stopped including the Content-Length header in server responses that cannot contain body content, such as HTTP 204 responses. This breaks client applications that are not HTTP compliant. This no longer occurs. Now, the Web Proxy includes the Content-Length header when the destination server includes it in the response even if the response body cannot contain body data.
73729	**Fixed: Web Proxy erroneously responds with a 503 Service Unavailable response for responses with a Content-Length header value of 0 in some cases** Previously, the Web Proxy erroneously responded with a 503 Service Unavailable response when the response contained a Content-Length header value of 0 and the destination server ended the transmission using an atypical method. This no longer occurs. Now, the Web Proxy returns all data from the server to the client and returns the response code given by the server.
73998	**Fixed: Web Proxy does not follow servers that respond with a 302 Moved Temporarily HTTP response** Previously, the Web Proxy did not follow servers that responded with a 302 Moved Temporarily HTTP response. This no longer occurs. Now, the Web Proxy redirects client applications to the new URL specified in the 302 response.

Resolved Issues in Version 7.1

Table 6 lists the issues that were resolved in version 7.1 of AsyncOS for Web.

Table 6 Resolved Issues in AsyncOS 7.1 for Web

Defect ID	Description
74076	**Fixed: Webroot definition file** In a previous build of AsyncOS for Web version 7.1.0, AsyncOS did not download the latest Webroot definition file. This no longer occurs.
72428	**Fixed: Web Proxy generates a core file when accessing HTTPS servers with AVC enabled in some cases** Previously, the Web Proxy generated a core file when processing a transparent request to an HTTPS server without a CN in the server certificate and when AVC was enabled. This no longer occurs.
72485	**Fixed: Global policies are erroneously assigned to native FTP transaction when authentication is used in some cases** Previously, the Global Access and Global Routing Policies were assigned to native FTP transactions instead of the proper user-defined Access and Routing Policies when the assigned Identity used authentication and IP address surrogates. This no longer occurs.
72535	**Fixed: Client requests stall and time out when upgrading from a previous version with an expired Webroot feature key in some cases** Previously, after upgrading from a previous version that had an expired Webroot feature key and an Access Policy that enabled the Webroot scanning engine, client requests stalled for about a minute and then failed with a 403 Forbidden response. This no longer occurs.
72670	**Fixed: Some client applications cannot communicate with the Web Proxy with NTLMSSP authentication enabled** Previously, some client applications could not communicate with the Web Proxy when NTLMSSP authentication was enabled. This no longer occurs.
73015	**Fixed: FTP directory listing appears corrupt when using native FTP** Previously, when a client application accessed an FTP server using native FTP and the FTP Proxy was enabled, the directory listing appeared corrupt . This no longer occurs.

Table 6 Resolved Issues in AsyncOS 7.1 for Web (continued)

Defect ID	Description
30070	**Fixed: Reporting engine does not work and contains corrupt data after the appliance shut down improperly** Previously, the reporting engine did not work and contained corrupt data after the appliance shut down improperly. This no longer occurs.
71985	**Fixed: Application fault occurs when applying the Web Proxy feature key in the web interface** Previously, an application fault occurred when applying the Web Proxy feature key in the web interface. This no longer occurs.
72682	**Fixed: Access log entries are not written when custom fields use incorrect syntax** Previously, when the access log subscription was configured to use format specifiers with incorrect syntax, no entries were written to the access log file. This no longer occurs. For a description of the correct syntax, see the "Logging" chapter in the *Cisco IronPort AsyncOS for Web User Guide*.

Resolved Issues in Version 7.0

Table 7 lists the issues that were resolved in version 7.0 of AsyncOS for Web.

Table 7 Resolved Issues in AsyncOS 7.0 for Web

Defect ID	Description
71776	**Fixed: Web Proxy runs out of memory and generates a core file when uploading very large files in some cases** Previously, the Web Proxy ran out of memory and generated a core file when uploading very large files to servers that sent an early HTTP 200 Ok response. This no longer occurs.
71900	**Fixed: Web Proxy processes requests very slowly due to a memory issue** Previously, the Web Proxy could get into a state where it processed requests very slowly. This was due to a memory allocation issue. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
71947	**Fixed: Web Proxy does not properly tunnel CONNECT requests in some cases** Previously, when the HTTPS Proxy was disabled and a client application initiated an SSL CONNECT request over port 443, the Web Proxy tunneled the connection, but did not return the server data to the client. This no longer occurs.
71619	**Fixed: Web Proxy generates a core file with explicit requests from Google Chrome in some cases** Previously, the Web Proxy generated a core file when processing explicit forward requests to HTTPS servers from the Google Chrome browser with NTLMSSP authentication.
56254	**Fixed: WCCP Module Logs contain no information** Previously, the WCCP Module Logs contained no information. This no longer occurs.
52556	**Fixed: Web Security appliance sends HTTPS transactions to external DLP servers in obscure format** Previously, the Web Security appliance sent HTTPS transactions to external DLP servers in a format that did not make it clear it was an HTTPS transaction instead of HTTP. This no longer occurs. Now, it sends HTTPS transactions as "https://*uri*" instead of sending the URI only.
54571	**Fixed: Very large native FTP downloads appear in the access logs as "Scanning Error" when McAfee is enabled** Previously, the access logs displayed "Scanning Error" in the McAfee name field under the following conditions: • McAfee is enabled. • A file is downloaded using native FTP, and the file is larger than the "Max. Object Size" field on the Security Settings > Anti-Malware page. This no longer occurs. Now, the access logs display "Skipped." The file still downloads successfully.
54683	**Fixed: Cannot compress access logs using the web interface** Previously, the web interface did not allow you to compress the access log subscription. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
54884	**Fixed: Web interface cannot load authentication groups from Lotus Domino Server** Previously, the web interface could not load authentication groups from Lotus Domino Server. As a result, the Test Authentication feature for the LDAP authentication realm gave an error when group authentication was configured, and when creating non-Identity policies, no LDAP groups were displayed. However, group authentication with Lotus Domino Server worked as expected. This no longer occurs. Now, the Test Authentication feature works as expected and LDAP groups are displayed when creating non-Identity policies.
54891	**Fixed: Access logs erroneously show a 4 GB FTP file download in some cases** Previously, the access logs erroneously showed a 4 GB FTP file download when a user tried to use FTP to download a non-existent file. This no longer occurs.
55087	**Fixed: Web interface erroneously allows underscores (_) in authentication realm and sequence names** Previously, the web interface erroneously allowed underscore characters (_) in authentication realm and sequence names. This no longer occurs.
55628	**Fixed: Policy trace feature does not work when accessing servers that require the User-Agent HTTP header** Previously, the policy trace feature did not work when accessing servers that require the User-Agent HTTP header. This no longer occurs.
55731	**Fixed: Date and time custom format specifiers (%v and %V) do not work** Previously, the date (%v) and time (%V) custom format specifiers did not work. When these were added to an access log subscription, no date or time values were displayed in the access log file. This no longer occurs. [Defect ID:]
50706	**Fixed: LDAP searches do not work in some cases** Previously, LDAP searches did not work when AsyncOS used old LDAP connections that did not have sufficient privileges.
51811	**Fixed: Application fault occurs in the web interface when accessing the Network > Internal SMTP Relay page in some cases** Previously, an application fault occurred in the web interface when accessing the Network > Internal SMTP Relay page if the SMTP relay was configured to use a deleted network interface. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
51822	**Fixed: Incorrect response size value recorded in the access logs for FTP over HTTP transactions when the transaction times out** Previously, an incorrect response size value was recorded in the access logs for FTP over HTTP transactions when the transaction timed out. This no longer occurs.
52184	**Fixed: Cannot enter text in some Identity fields using Safari 4.0.x** Previously, when you used the Safari browser version 4.0.x to access the web interface, you could not enter text in the Description or Define Members by Subnet fields for Identity groups under some circumstances. This no longer occurs.
53866	**Fixed: Access logs erroneously display a negative value for the custom format specifier %q in some cases** Previously, the access logs erroneously displayed a negative value for the custom format specifier %q for uploads greater than 2 GB. This no longer occurs.
53867	**Fixed: Web Proxy generates a core when uploading 2 GB files with external DLP enabled in some cases** Previously, the Web Proxy generated a core when uploading 2 GB files with external DLP enabled using Vontu Web Prevent version 9. This no longer occurs.
53868, 53870	**Fixed: Not all data is uploaded with external DLP enabled in some cases** Previously, when uploading a 2 GB file using HTTP POST or FTP over HTTP with external DLP enabled, not all data was uploaded to the server when the external DLP server is Vontu Web Prevent version 9.
50971	**Fixed: Web Proxy generates a core file when changing the IP Spoofing setting when FTP downloads are occurring** Previously, the Web Proxy generated a core file when a user was downloading a file using FTP and an administrator changed the IP Spoofing setting on the Security Services > Proxy Settings page from “For All Connections” to “For Transparent Connections Only.” This no longer occurs.
49501	**Fixed: Timestamp field in the Data Security Logs shows time in GMT instead of local timezone** Previously, the timestamp field in the Data Security Logs showed time in the Greenwich Mean Time (GMT) timezone instead of the Web Security appliance local timezone. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
52237	**Fixed: Web Proxy generates a core file when processing multiple native FTP sessions in some cases** Previously, The Web Proxy generated a core file when processing multiple native FTP sessions to some FTP servers.
69094	**Fixed: Web Proxy stops responding to servers and generates a core file in some cases** Previously, the Web Proxy stopped responding to servers and generated a core file when the server certificate was expired. This no longer occurs.
69724	**Fixed: McAfee erroneously marks some files as unscannable** Previously, McAfee erroneously marked some archive files containing character special members as unscannable. This no longer occurs.
69792	**Fixed: DLP fails when both external DLP and IP spoofing are configured** Previously, when the Web Security appliance was configured for both External DLP and IP spoofing, the appliance used the spoofed IP address to connect to the DLP server. This caused the connection to fail and prevented a DLP verdict from being generated. This no longer occurs.
69793	**Fixed: Cannot access some HTTPS servers with decryption enabled** Previously, users could not access some HTTPS servers intermittently when decryption was enabled. This no longer occurs.
69794	**Fixed: Users are erroneously blocked before being prompted for authentication with IronPort Data Security Filters enabled in some cases** Previously, users were erroneously blocked before being prompted for authentication when IronPort Data Security Filters enabled and only one Identity and Access Policy group were defined. This no longer occurs.
69902	**Fixed: Web Proxy generates a core file accessing some websites** Previously, the Web Proxy generated a core file due to leaked memory when accessing some websites. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
70141	**Fixed: Uploads fail and the Web Proxy generates a core with upstream proxy servers in some cases** Previously, uploads to web servers going through an upstream proxy server failed and the Web Proxy generated a core when the web server issued a 304 “Not Modified” response in some cases. This no longer occurs.
70375	**Fixed: Native FTP downloads fail using the MGET command on some FTP servers** Previously, Native FTP downloads failed using the MGET command on some FTP servers. This no longer occurs.
70547	**Fixed: Gateway Timeout errors occur for certain websites when HTTPS Proxy is enabled** Previously, when the HTTPS proxy was enabled, if an HTTPS website spontaneously closed an HTTPS connection, gateway timeout errors sometimes occurred. This no longer occurs.
70742	**Fixed: Web Proxy improperly terminates chunked encoded downloads in some cases** Previously, the Web Proxy improperly terminated chunked encoded downloads when the last packet is completely full. This no longer occurs.
70833	**Fixed: Web Proxy leaks memory and generates a core file when processing multiple NLST FTP commands** Previously, the Web Proxy leaked memory and generated a core file when processing multiple NLST FTP commands. This no longer occurs.
70951	**Fixed: AsyncOS for Web generates a core file when making configuration changes in the web interface in some cases** Previously, AsyncOS for Web generated a core file when changing the HTTPS Proxy configuration. This no longer occurs.
70997	**Fixed: Uploads hang when the server replies with a 500 Internal Server Error response in some cases** Previously, uploads hung when the server replied with a 500 Internal Server Error response because the Web Proxy never sends the 500 response to the client. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
71211	**Fixed: Web Proxy does not forward to clients server responses to POST requests in some scenarios** Previously, the Web Proxy did not forward to clients server responses to POST requests in some scenarios. This no longer occurs.
71236	**Fixed: Uploads to some servers fail** Previously, uploads failed when the web server sent a response body too early. This no longer occurs. [Defect ID: 71236]
41568	**Fixed: URIs do not match custom URL categories containing a large number of regular expressions** URIs do not match custom URL categories containing a large number of regular expressions. Workaround: Only include up to 200 regular expressions in a custom URL category.
45494	**Fixed: HTML tag missing on the Custom URL Categories page after adding a custom URL** Previously, when you added a custom URL category to the Web Security Manager > Custom URL Categories page and then save the page to an HTML file, the HTML file was missing a <tr> tag. This no longer occurs.
49758	**Fixed: Web Proxy creates invalid cookies for requests to hostnames belonging to some particular top-level domains in some cases** Previously, the Web Proxy created invalid cookies for requests to hostnames belonging to some particular top-level domains (TLDs) where only third-level sub-domains are allowed, such as TLD .au. This no longer occurs.
54676	**Fixed: Application fault occurs when accessing an Access Policy with a non-existent Identity** Previously, an application fault occurred when accessing an Access Policy that erroneously used a non-existent Identity. This no longer occurs. Now, Access Policies do not erroneously use a non-existent Identity.
67090	**Fixed: Upload fails when the client sends a second upload before the first upload finishes** Previously, an upload failed when the client sent a second upload before the first upload finished. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
68059	**Fixed: Web Proxy stops sending requests to the external DLP server after uploading several files using FTP in some cases** Previously, the Web Proxy stopped sending requests to the external DLP server after successfully blocking FTP upload requests that exceeded the maximum number of simultaneous connections configured for the external DLP server. This no longer occurs.
68075	**Fixed: Policy trace cannot fetch authentication groups when proceeding group uses non-ASCII characters** Previously, the policy trace feature could not fetch authentication groups when the proceeding group used non-ASCII characters. This no longer occurs. Now, it displays all groups that only use ASCII characters.
68314	**Fixed: HTTPS Proxy incorrectly decrypts or passes through HTTPS transactions to custom URL categories configured to Monitor** Previously, the HTTPS Proxy incorrectly decrypted or passed through HTTPS transactions to custom URL categories configured to Monitor. This no longer occurs.
68332	**Fixed: AsyncOS does not send compressed access logs to a remote server using FTP or SCP** Previously, AsyncOS did not send compressed access logs to a remote server using FTP or SCP. This no longer occurs.
68575	**Fixed: Web Proxy generates a core file and restarts when the data connection for a native FTP session receives a RESET from the server** Previously, the Web Proxy generated a core file and restarted when the data connection for a native FTP session received a RESET from the server. This no longer occurs.
68907	**Fixed: Configuration Summary page does not list all configured interfaces** Previously, the System Administration > Configuration Summary page did not list all configured interfaces. This no longer occurs.
68937	**Fixed: Some websites take awhile to load with the Dynamic Content Analysis engine enabled in some cases** Previously, accessing websites with a malformed compressed file would take a long time to scan when the Dynamic Content Analysis engine was enabled. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
69119	**Fixed: cs-byte field for W3C access logs is not available** Previously, you could not specify the "cs-byte" field in a W3C access log subscription. This no longer occurs.
69128	**Fixed: Web Proxy in transparent mode generates a core file when authenticating multiple users simultaneously in some cases** Previously, when the Web Proxy was in transparent mode, configured with a large surrogate timeout value, and configured to use cookie-based authentication, it generated a core file when authenticating multiple users simultaneously. This no longer occurs.
69188	**Fixed: Native FTP STOR requests fail with external DLP enabled in some cases** Previously, native FTP STOR requests in active mode to Microsoft Windows servers failed with external DLP enabled. This no longer occurs.
69397	**Fixed: Web Proxy generates a core file connecting to some HTTPS servers** Previously, the Web Proxy generated a core file connecting to some HTTPS servers. This no longer occurs.
69646	**Fixed: authcache > flushuser CLI command does not work when the authentication realm name or username has whitespaces in it** Previously, the `authcache > flushuser` CLI command does not work when the authentication realm name or username has whitespaces in it. This no longer occurs.
69647	**Fixed: Web Proxy returns 504 Gateway Timeout errors to clients accessing unresponsive HTTPS servers in some cases** Previously, when the HTTPS Proxy was enabled, the Web Proxy in transparent mode returned 504 Gateway Timeout errors to clients accessing HTTPS sites after several requests were made to unresponsive HTTPS servers. This no longer occurs.
66458	**Fixed: FTP Proxy does not spoof the IP address of the FTP server for active mode connections** Previously, the FTP Proxy did not spoof the IP address of the FTP server for active mode connections. This no longer occurs. Now, the FTP Proxy spoofs the IP address of FTP servers for both active and passive mode connections.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
51315	**Fixed: Web interface erroneously allows some invalid regular expressions in some cases** Previously, the web interface erroneously allowed some invalid regular expressions when defining custom URL categories. This no longer occurs. For more information on the valid syntax to use when using regular expressions in custom URL categories, see the "Regular Expressions" section in the URL Filters chapter of the *Cisco IronPort AsyncOS for Web User Guide*.
54925	**Fixed: Decrypting HTTPS traffic to SSLv3 only websites fails** Previously, decrypting HTTPS websites that only support SSLv3 or TLSv1 failed. This no longer occurs. Now, the Web Proxy no longer works with HTTPS websites that only support SSLv2.
54929	**Fixed: CPU usage can get very high with a very large number of authentication groups** Previously, the Web Proxy downloaded the entire list of authentication groups, and when the number of groups was very large, such as over 250,000 groups, the CPU usage was close to 100%. This no longer occurs. Now, the Web Proxy limits downloads up to 500 authentication groups at a time.
55387	**Fixed: Browsers erroneously encounter certificate errors for some websites with decryption enabled in some cases** Previously, browsers erroneously encounter certificate errors with decryption enabled when users visit a website that uses a server certificate file that contains duplicate entries. This no longer occurs.
66600	**Fixed: Application fault occurs when running logconfig CLI command in some cases** Previously, an application fault occurred when running the `logconfig` CLI command after upgrading with McAfee Framework Integration logs enabled. This no longer occurs.
66647	**Fixed: Application fault occurs when configuring an LDAP authentication realm as supporting Novell eDirectory in some cases** Previously, an application fault occurred when configuring an LDAP authentication realm as supporting Novell eDirectory when the configured authentication server is not a Novell eDirectory server. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
66944	**Fixed: Chunked responses larger than the maximum scanning size are erroneously logged as a scanning error with McAfee enabled** Previously, chunked responses larger than the maximum scanning size were erroneously logged as a scanning error with McAfee enabled. This no longer occurs. Now, they are logged as skipped.
66956	**Fixed: Testing the authentication settings times out when retrieving a large number of authentication groups** Previously, testing the authentication settings timed out when retrieving a large number of authentication groups defined by user attributes. This no longer occurs.
67198	**Fixed: Application fault occurs in the web interface when enabling external authentication after changing the admin password** Previously, an application fault occurred in the web interface when enabling external authentication after changing the admin password. This no longer occurs.
67620	**Fixed: Welcome Page Acknowledgement logs record the incorrect expiration time** Previously, the Welcome Page Acknowledgement logs recorded the incorrect expiration time. This no longer occurs.
67816, 52504	**Fixed: Uploading data to servers using a POST command fails in some cases** Previously, using a POST command to upload data to a server that sent an error code failed. This no longer occurs.
67917	**Fixed: Web interface erroneously does not allow some LDAP custom query filters** Previously, the web interface erroneously did not allow LDAP custom query filters that included multiple conditions, such as in the form `(&(object=value)(object=value))`. This no longer occurs.
68044	**Fixed: Editing an Identity erroneously affects other Identities in an Access Policy** Previously, when an Access Policy includes multiple Identities with URL categories defined and one of the Identities changes, all other Identities in the Access Policy are excluded from the Access Policy. This no longer occurs. Now, only the applicable Identity is affected.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
68122	**Fixed: Configurations with too many custom URL categories in an IronPort Data Security Policy fail to load** Previously, configurations with too many custom URL categories in an IronPort Data Security Policy failed to load. This no longer occurs.
68202	**Fixed: Web Proxy generates a core file after a native FTP STOR request in some cases** Previously, the Web Proxy generated a core file after processing a native FTP STOR request from some non-compliant FTP clients. This no longer occurs.
68306	**Fixed: Web interface erroneously allows more than 32 router IP addresses in a WCCP service** Previously, the web interface erroneously allowed more than 32 router IP addresses in a WCCP service. This no longer occurs. Now, it allows a maximum of 32 router IP addresses.
68316	**Fixed: Web reputation returns the incorrect value in some cases** Previously, the web reputation filters returned the incorrect value for host names and IP addresses which resulted in some pages being unnecessarily blocked. This no longer occurs.
68407	**Fixed: Custom URL categories intermittently not matching URLs included in the category** Previously, Custom URL categories intermittently did not match URLs included in the category. This no longer occurs.
68443	**Fixed: Changing the "Retrieval Method" setting for the access log subscription in the web interface disables the "Maximum Time Interval Between Transferring" setting** Previously, changing the "Retrieval Method" setting for the access log subscription in the web interface disabled the "Maximum Time Interval Between Transferring" setting. This no longer occurs.
68710	**Fixed: Access logs erroneously include a URL category for some uncategorized websites** Previously, the access logs erroneously included a URL category for some uncategorized websites. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
68817	**Fixed: LDAP authentication does not work correctly when an asterisk (*) is entered as the user name** Previously, LDAP authentication did not work correctly when an asterisk (*) was entered as the user name. This no longer occurs.
69110	**Fixed: FTP Proxy erroneously returns cached data to Filezilla clients using the control connection, causing garbled data** Previously, the FTP Proxy erroneously returned cached data to Filezilla clients using the control connection, causing garbled data. This no longer occurs.
54894	**Fixed: Web Proxy generates a core file when downloading large files in some cases** Previously, the Web Proxy generated a core file when downloading large files from servers that served data faster than the client application could read it. This no longer occurs.
39942	**Fixed: Application fault occurs in the web interface when the web browser refreshes the page multiple times** Previously, an application fault occurred in the web interface when the web browser refreshed the page multiple times. This no longer occurs.
41304	**Fixed: Erroneous error message when deleting a route that does not exist on the Web Security appliance** Previously, when deleting a route that did not exist on the Web Security appliance, the System Logs showed the following warning message: Warning: The following update to the interface failed: setfib -1 route -n delete *route* Reason: route: writing to routing socket: No such process This no longer occurs.
43057	**Fixed: Policy Trace feature does not accept spaces in authenticated username field** Previously, the Policy Trace feature did not accept spaces in authenticated username field. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
47048	**Fixed: Web interface cannot be accessed using HTTPS on port 443** Previously, when the Web Security appliance management interface was configured to listen for requests on port 443, administrators could not access the management web interface using HTTPS on port 443. This no longer occurs. However, to access the web interface on port 443, you must not enable the HTTPS Proxy.
48360	**Fixed: Loading a configuration file takes a long time in some cases** Previously, loading a configuration file took a long time. This no longer occurs. Now, loading these configuration files is quicker.
49472	**Fixed: Web Security appliance cannot establish connection with WCCP router in some cases** Previously, the Web Security appliance could not establish a connection with some WCCP routers. This no longer occurs.
50652	**Fixed: Upgrading from a previous version removes the certificate and key pair uploaded for credential encryption** Previously, if credential encryption (also known as "secure client authentication") was enabled in a previous version and then you upgraded AsyncOS for Web to the current version, any certificate and key pair previously uploaded for credential encryption was removed. This no longer occurs.
50901	**Fixed: Policy Trace feature works incorrectly with IP spoofing enabled** Previously, the Policy Trace feature worked incorrectly when IP spoofing was enabled and the client IP address was not provided in the Policy Trace feature. This no longer occurs. Now, the Policy Trace feature succeeds with IP spoofing enabled when no client IP address is provided.
51048	**Fixed: GMT time zones incorrectly set in some cases** Previously, when configuring the GMT time zones in the web interface, some time zones were off from the correct value by an hour. This happened for time zones with a half hour increment to GMT, such as Caracas, Venezuela. This no longer occurs.
51864	**Fixed: Web Proxy erroneously adds its domain name as a DNS search domain in some cases** Previously, when a client explicitly forwarded a request for a URL hostname that could not be resolved, the Web Proxy appended its own name domain to the URL and tried the DNS lookup again. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
51873	**Fixed: Policy Trace feature does not override the MIME type in some cases** Previously, when using the Policy Trace and a response detail override was configured for the MIME type, the MIME type was not overridden. This no longer occurs.
51933	**Fixed: Changing the name of the Web Security appliance host name does not take effect immediately** Previously, changing the name of the Web Security appliance host name did not take effect immediately. This no longer occurs.
52022	**Fixed: Changing the default gateway does not display the new IP address in the web interface immediately** Previously, when you changed the default gateway and clicked **Submit**, the Network > Routes page did not immediately display the new IP address for the default gateway after clicking **Submit**. This no longer occurs.
52378	**Fixed: Web Proxy erroneously replies with HTTP 1.1 to HTTP 1.0 requests** Previously, the Web Proxy erroneously replied with HTTP 1.1 to HTTP 1.0 requests. This no longer occurs.
52487	**Fixed: Web interface does not display uploaded PAC files in some cases** Previously, uploaded PAC files were not listed in the PAC Files Hosted field on the Security Services > PAC File Hosting page in view mode. This no longer occurs.
52509	**Fixed: Updates and upgrades do not work due to incorrect routing tables configured after upgrading from AsyncOS for Web 5.6.4** Previously, after upgrading from AsyncOS for Web 5.6.4, the Routing Table for AsyncOS update and upgrade settings was erroneously set to “Data” instead of “Management” when the previous version was configured to use the P1 network interface for component updates (`updateconfig` CLI command) and the “Restrict M1 port to appliance management services only” setting was disabled. This caused updates and upgrades to not work. This no longer occurs. Now, the routing table for update and upgrade settings is upgraded to “Data” only when the P1 network interface was configured for component updates and the “Restrict M1 port to appliance management services only” setting was *enabled*.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
52515	**Fixed: FTP Proxy generates a core file uploading files using native FTP in some cases** Previously, the FTP Proxy generated a core file uploading files using native FTP in some cases. This no longer occurs.
52523	**Fixed: Configuring the FTP Proxy passive mode data port range makes the Web Security appliance inaccessible in some cases** Previously, configuring the FTP Proxy passive mode data port range to values other than the default values made the Web Security appliance inaccessible. This no longer occurs.
53811	**Fixed: Web Proxy incorrectly interprets "%2F" in FTP over HTTP URIs in some cases** Previously, the Web Proxy incorrectly interpreted "%2F" in FTP over HTTP URIs. This no longer occurs. Now, when the FTP URI starts with "%2F" (the URL encoded slash character), the Web Proxy interprets it correctly as part of the path on the remote FTP server.
53826	**Fixed: Web Proxy refuses connections with the authentication cache is set to a very large value** Previously, the Web Proxy refused connections with the authentication cache was set to a very large value. This no longer occurs. Now, the web interface only allows values between 1,000 and 32,000 bytes.
53937	**Fixed: Backed up configuration files do not mask all passwords** Previously, when you backed up a configuration file, not all passwords in the file were masked even when "Mask passwords in the Configuration Files" was enabled. This no longer occurs.
54600, 54720	**Fixed: Web Proxy performance is slow with some complex configurations** Previously, Web Proxy performance was slow with some complex configurations. This no longer occurs.
54681	**Fixed: Guest users cannot change their password in the web interface** Previously, Guest users could not change their password on the Options > Change Password page. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
54808, 51570, 47998	**Fixed: Transparently redirected HTTPS transactions do not match Identities configured for "All protocols"** Previously, transparently redirected HTTPS transactions did not match Identities configured for "All protocols." This no longer occurs.
55010	**Fixed: Web Proxy fails to generate a core file when it restarts due to some errors** Previously, the Web Proxy failed to generate a core file when it restarted due to some errors. This no longer occurs.
55163	**Fixed: Application fault occurs when browsers send a malformed request to the PAC server port on the Web Security appliance** Previously, an application fault occurred when browsers sent a malformed request containing NULL bytes to the PAC server port on the Web Security appliance. This no longer occurs.
55189	**Fixed: Enabling the end-user acknowledgement page breaks the Policy Trace feature** Previously, enabling the end-user acknowledgement page broke the Policy Trace feature. This no longer occurs.
55350	**Fixed: Cannot join Active Directory domain after changing Web Security appliance hostname in some cases** Previously, joining the Active Directory domain did not work under the following steps were applied: • Configure the Web Security appliance hostname to a value that does not resolve to the appliance itself. • Create an NTLM authentication realm and try to join the Active Directory domain. The Computer Account creation fails with the error message "Unknown hostname." • Change the Web Security appliance hostname to a value that *does* resolve to itself, and then try to join the domain again. AsyncOS for Web used the previous hostname to try and join the domain, so the Computer Account creation failed again. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
55634	**Fixed: Access policies show incorrect value for "HTTP/HTTPS Max Download Size" setting in some cases** Previously, Access Policies showed the incorrect value for the "HTTP/HTTPS Max Download Size" setting when it used the global policy values for the Object settings and the Global Access policy was configured for a value other than the default value. However, the Access Policies blocked transactions appropriately as configured in the Global Access policy. This no longer occurs.
55671	**Fixed: Loading route tables with spaces in the file name fails** Previously, loading route tables with spaces in the file name failed. This no longer occurs.
55694	**Fixed: Deleting a custom URL category erroneously disabled some Access Policies** Previously, deleting a custom URL category disabled Access Policies that were configured to perform an action on the custom URL category when the policy membership was not defined by the custom URL category. This no longer occurs. Now, Access Policies are disabled only when their policy membership is defined by a custom URL category that is deleted.
56338	**Fixed: Webroot returns a scanning error for some configurations** Previously, Webroot returned a scanning error when the "Domain Levels for Malware Request Detection" proper was set to a value less than 10. This no longer occurs.
56386	**Fixed: Accessing some web servers fails when an upstream proxy server is configured** Previously, accessing some web servers failed when an upstream proxy server was configured. This no longer occurs.
65977	**Fixed: Web Proxy does not query all LDAP groups in some cases** Previously, the Web Proxy did not query all LDAP groups, causing some requests to erroneously fall into the Global Access Policy. This no longer occurs.

Table 7 Resolved Issues in AsyncOS 7.0 for Web (continued)

Defect ID	Description
66231	**Fixed: Web Proxy erroneously returns HTTP status code 416 to clients when the web server returns HTTP status code 302 in some cases** Previously, the Web Proxy erroneously returned HTTP status code 416 to clients when the web server returned HTTP status code 302 when the object was cached and the client made a range request. This no longer occurs.
67029	**Fixed: Web Proxy does not query all LDAP groups when group membership attribute is not a DN** Previously, the Web Proxy did not query all LDAP groups when group membership attribute was not a DN. This no longer occurs.

Known Issues

Table 8 lists the known issues in this release of AsyncOS for Web.

Table 8 Known Issues for AsyncOS 7.1 for Web

Defect ID	Description

78754	**RAID state change erroneously creates an alert message in some cases**
	When the RAID on the S170 appliances change state in some cases, the appliance sends an alert message with the following message:
	`A RAID-event has occurred:`
	`RAID states changed from “OPTIMAL” to “SUBOPTIMAL”`
	or
	`A RAID-event has occurred:`
	`RAID states changed from “SUBOPTIMAL” to “OPTIMAL”`
	The change in state is usually the result of the appliance powering off without being shut down from the web interface or CLI.
	Workaround: This change in state is benign. You can ignore these alert messages.

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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
78620	**PAC file hosting erroneously appears disabled after loading a configuration file** When you enable PAC file hosting on the appliance, save the configuration, and then load the configuration, PAC file hosting is disabled on the Security Services > Proxy Auto-Configuration File Hosting page. Note, the appliance is correctly configured and serves PAC files to clients as necessary. Workaround: Navigate to the Security Services > Proxy Auto-Configuration File Hosting page, and click **Enable and Edit Settings**. Verify the Enable Proxy Auto-Configuration File Hosting Settings option is checked, and submit your changes. You do not need to commit the changes to fix this problem in the web interface.
70914	**Policy Trace feature does not use the Dynamic Content Analysis engine when performing a trace** The Policy Trace feature does not use the Dynamic Content Analysis engine when categorizing a URL when performing a trace.
72238	**Dynamic Content Analysis engine does not categorize web pages that contain NULL characters** The Dynamic Content Analysis engine does not categorize web pages that include characters containing NULL bytes. This might happen for web pages whose contents are UTF-16 encoded.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
74487, 71794	**Identities have incorrect authentication surrogate settings after upgrading from a previous version in some cases** After upgrading from a previous version, Identities have incorrect authentication surrogate settings under the following conditions: • The Web Proxy was deployed in explicit forward mode in the previous version. • An Identity was configured to use authentication but no authentication surrogates in the previous version. • After upgrading, the Identity's authentication surrogate is set to IP address in the web interface, but does not work correctly. After upgrading, the Identity's authentication surrogate is not retained as No Surrogate. Workaround: After upgrading, edit the Identity, choose No Surrogate, and click **Submit** and **Commit**.
74872	**WCCP negotiation with some Cisco 7600 routers fails** WCCP negotiation with some Cisco 7600 routers fails. Workaround: Contact Cisco IronPort Customer Support.
75953	**Some URLs are erroneously categorized by the Cisco IronPort Web Usage Controls URL filtering engine when the Dynamic Content Analysis engine is disabled** Some URLs are erroneously categorized using the Dynamic Content Analysis engine even when the Dynamic Content Analysis engine is disabled.
76000	**Native FTP connections fail when the configured welcome banner for the FTP Proxy exceeds 1024 characters** Native FTP connections fail when the configured welcome banner for the FTP Proxy exceeds 1024 characters. Workaround: Edit the Welcome Banner Custom Message setting on the Security Services > FTP Proxy page and ensure it uses less than 1025 characters.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
76207	**Application fault occurs in the web interface when trying to download an uploaded Identity Provider signing certificate** An application fault occurs in the web interface when trying to download an uploaded Identity Provider signing certificate.
76472	**Application fault occurs in the web interface when clicking the Schedule Reports link on the Next Steps page of the System Setup Wizard** An application fault occurs in the web interface when clicking the Schedule Reports link on the Next Steps page of the System Setup Wizard. Workaround: To view the scheduled reports, log into the web interface again and choose Reporting > Schedule Reports.
76916	**The %g variable in customized end-user notification pages sometimes erroneously displays the wrong value** When you customize the end-user notification pages stored on the appliance and include the %g variable, sometimes the variable correctly displays the custom URL category, and sometimes it displays a predefined URL category.
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.
77271	**Browsers cannot access PAC files stored on the appliance when the port is changed in some cases** Browsers cannot access PAC files stored on the appliance when the port is changed from the current value and when browsers try 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. Workaround: Reboot the appliance. Or, to avoid restarting the appliance, you can make any change to any Access Policy and then submit and commit the change. For example, you can create an Access Policy, submit and commit the change, and then delete the policy and submit and commit your change again.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.
75040	**Application error occurs trying to generate a PDF from the Reports by User Location page in some cases** An application error occurs when you change the web interface language using the Options menu and then click the **Printable (PDF)** link on the Reports by User Location page. Workaround: Navigate to another report page, return to the Reports by User Location report page, and then click the **Printable (PDF)** link.
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.
76185	**Files greater than the maximum allowed file size are erroneously uploaded using FTP in some cases** Files greater than the maximum allowed file size are erroneously uploaded when an IronPort Data Security policy is configured to block FTP transactions greater than a specified size. The access logs show that the file was blocked, but in reality the file is successfully transferred to the FTP server.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
73339	**Log file timestamps and log file headers show incorrect time after changing the time zone in some cases** When you change the time zone on the appliance, the time zone change is not propagated to the internal logging process. As a result, the timestamps in the log filename and the offset in the log file headers are incorrect. However, the log entries in the log files correctly use the new time zone. Workaround: Reboot the appliance after changing the time zone setting.
72834	**An application fault occurs in the internal reporting process when you change the system time or time zone on the appliance in some cases** An application fault occurs in the internal reporting process when you change the system time or time zone on the appliance after it has processed traffic. Additionally, for some appliances, data is not aggregated properly (for example, hourly data is not aggregated into the daily data). This may result in performance degradation, and eventually, into data retention issues. Workaround: Contact Cisco IronPort Customer Support to disable and then enable the reporting process.
72835	**Export link is missing on the Reports By User Location report page for the "Suspect Transactions Detected" charts** The Export link is missing on the Reports By User Location report page for the "Suspect Transactions Detected" charts for both Remote and Local users. Workaround: Export data from the Suspect Transactions Summary charts instead.
71942	**Logging data is recorded on Web Security appliance after enabling Centralized Reporting** When you enable Centralized Reporting on the Web Security appliance, AsyncOS for Web records information in the Web Security appliance logging database as well as collects information for centralized reporting on the Security Management appliance. Workaround: After enabling Centralized Reporting on the Web Security appliance, reboot the Web Security appliance.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.
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.
72432	**PDF file of Web Tracking report does not include related transactions information** When you display the related transactions in a Web Tracking report and then print to PDF, the PDF file does not contain the related transactions information.
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.
71747	**Web Proxy enters a redirect loop with credential encryption enabled in explicit forward mode in some cases** The Web Proxy enters a redirect loop under the following circumstances: • The Web Proxy is configured in explicit forward mode. • An Identity is configured to use authentication and no authentication surrogates. • Credential encryption is enabled after configuring the Identity. Workaround: Edit the Identity, make no changes, and click **Submit** and **Commit**.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.

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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.
70537	**Web Proxy erroneously does not recognize some root authorities** By default, the Web Proxy erroneously does not recognize the "VeriSign Class 3 Secure Server CA" root certificate. The Web Proxy does not recognize the root authority of websites that use this root certificate to establish its trust relationship. Depending on how the HTTPS Proxy is configured to handle invalid certificates, client requests to these sites may be dropped. Workaround: Import the "VeriSign Class 3 Secure Server CA" root certificate as a custom root authority certificate on the Security Services > HTTPS Proxy page.
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
69388	**Policy Trace erroneously matches some transactions with the Global Access policy in some cases** The Policy Trace feature erroneously matches transactions with the Global Access policy under the following circumstances: • An Identity includes authenticated users in the "Domain Local" group in Active Directory, and an Access Policy group uses that Identity. • In the Policy Trace tool you enter a user in the "Domain Local" group. Instead of matching the Access Policy that uses the Identity configured above, users match the Global Access Policy in the Policy Trace. However, the Web Proxy assigns the correct Access Policy to users accessing the Internet.
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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>.
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.
56418	**Exported URL Categories Report does not show all information** When you click the Export link on the Monitor > URL Categories page, the exported .csv file does not contain any information in the "bandwidth saved by blocking" column.
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description

56116	**Cannot import an AsyncOS 6.3.1 for Web Security configuration file to Configuration Master 6.3**
	
	Attempting to import an AsyncOS 6.3.1 for Web Security configuration file to Configuration Master 6.3 results in error messages.
	
	Workaround: Prior to import, delete the following three lines from the configuration file:
	
	`<prox_config_http_port_tunneling_enabled>1 </prox_config_http_port_tunneling_enabled>`
	
	`<prox_etc_allow_wild_card_in_group_name>1 </prox_etc_allow_wild_card_in_group_name>`
	
	`<prox_etc_basic_auth_charset>ISO-8859-1</prox_etc_basic_auth_charset>`

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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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 8 Known Issues for AsyncOS 7.1 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 8 Known Issues for AsyncOS 7.1 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.
44031	**Policy trace feature does not display a web reputation score when authentication is enabled** The policy trace feature does not display a web reputation score when authentication is enabled.
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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 8 Known Issues for AsyncOS 7.1 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

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.
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:]

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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).
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.
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.

Table 8 Known Issues for AsyncOS 7.1 for Web (continued)

Defect ID	Description
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.