IRONPORT™

IronPort AsyncOS™ 6.5

RELEASE NOTES

for Web Security Appliances

COPYRIGHT

Part Number: 423-0101(B)

Revision Date: September 1, 2010

IRONPORT SYSTEMS® , INC.

IronPort Systems, Inc.
950 Elm Ave.
San Bruno, CA 94066

CONTACTING IRONPORT CUSTOMER SUPPORT

If you have purchased support directly from IronPort Systems, you can request our support by phone, email or online 24 hours a day, 7 days a week. During our office hours (24 hours per day, Monday through Friday excluding US holidays), one of our engineers will contact you within an hour of your request. To report a critical issue that requires urgent assistance outside of our office hours, please call us immediately at the numbers below.

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

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

Support Portal:
`http://www.cisco.com/cisco/web/support/index.html`

If you have purchased support through a reseller or another entity, please contact them for support of your IronPort products.

IronPort AsyncOS 6.5 for Web Release Notes

The IronPort S-Series Web Security appliance is the industry's first and only secure web gateway to combine traditional URL filtering, reputation filtering, malware filtering and data security on a single platform to address the web-based risks. By combining innovative technologies, the IronPort S-Series helps organizations address the growing challenges of both securing and controlling web traffic. Customers enjoy low total cost of ownership (TCO), as these powerful applications are integrated and managed on a single appliance. Robust management and reporting tools deliver ease of administration, flexibility and control, as well as complete visibility into policy- and threat-related activities.

This document includes the following software product information:

Qualified Upgrade Paths

There are no qualified upgrade paths for the IronPort AsyncOS 6.5 for Web operating system.

To ensure a successful upgrade, you must complete some steps before you start the upgrade process. For details on these prerequisites, see "Upgrading the Web Security Appliance" on page 10.

IronPort Web Security Appliance Support Portal

You can use the following URL to access Web Security appliance product information online:

`http://www.ironport.com/support/login.html`

The support portal contains the most recent publications including the *IronPort S-Series Quick Start Guide*, *IronPort AsyncOS for Web User Guide*, and other useful product information.

WHAT'S NEW IN THIS RELEASE

This section describes new features and enhancements added in the AsyncOS 6.5 for Web release.

New Feature: FIPS Compliance

AsyncOS for Web 6.5 provides support for the new FIPS-compliant version of the Cisco IronPort S670 Web Security appliance.

The Federal Information Processing Standard (FIPS) 140 is a publicly announced standard developed jointly by the United States and Canadian federal governments specifying requirements for cryptographic modules that are used by all government agencies to protect sensitive but unclassified information. The Cisco IronPort S670 Web Security appliance is now offered in a configuration that complies with the FIPS 140-2 Level 2 standard. This standard specifies additional protections for information used in cryptographic operations, including the use of a tamper-resistant hardware keystore for private keys.

The FIPS version of the S670 includes a Hardware Security Module (HSM). The HSM provides cryptographic processing for the appliance as well as storage for private keys. All cryptographic operations take place within the secure environment of the HSM.

AsyncOS for Web 6.5 provides support for using the HSM for all cryptographic operations performed by the appliance. It also provides a FIPS management console to allow an administrator to configure the HSM for use in a clustered environment and manage certificates and private keys.

For more information, see the "FIPS Management" chapter of the *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 "Bugs Fixed in 6.3.4" on page 15, "Bugs Fixed in 6.3.3" on page 18, "Bugs Fixed in 6.3.1" on page 22, "Bugs Fixed in 6.3.0" on page 25 and "Bugs Fixed in 6.0.0" on page 34.

WHAT'S NEW IN VERSION 6.3

This section describes new features and enhancements added in the AsyncOS 6.3 for Web release.

New Feature: Rich Acceptable Use Controls with URL Filtering

AsyncOS for Web 6.3 introduces a new platform, Cisco IronPort Web Usage Controls, for rich acceptable use controls to address the challenge of current day Web traffic. The new platform includes a new and improved URL filtering engine with dynamic categorization capabilities for the uncategorized traffic. Subsequent releases will build on this new platform to include additional capabilities for application control and bandwidth management.

Cisco IronPort Web Usage Controls includes the Dynamic Content Analysis engine, a highly sophisticated technology on the appliance for real-time analysis of uncategorized sites. This engine improves URL filtering by categorizing some of the uncategorized traffic in real-time, and is especially effective for commonly blocked categories containing objectionable content. This addresses the challenge posed by thousands of sites being added to the Web every few minutes. URL databases have difficulty keeping up with this volume and they take time to update.

The new URL filtering engine has more granular categories. Efficacy for the new URL filtering engine is supported by a combination of sophisticated backend tools, processes, and a global team of categorization experts to provide continuous automatic updates to the URL database on customers' Web Security appliances. This also results in a huge improvement in our responsiveness for categorization or re-categorization requests.

For more information, see the "URL Filters Overview" section of the "URL Filters" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

WHAT'S NEW IN VERSION 6.0

This section describes new features and enhancements added in the AsyncOS 6.0 for Web release.

New Feature: IronPort Data Security

AsyncOS for Web 6.0 includes the IronPort Data Security Filters to provide you visibility and control over data leaving your network via the web and FTP. This feature allows you to create policies and take actions based on relevant parameters like the source (user), destination (URL categories and web reputation), and file metadata (file name, file type, and file size). For example, you can enforce the following business policies using IronPort Data Security:

- Do not allow members in the Finance department to send Excel files.
- Do not allow attachments in outgoing web-based emails to exceed 100 KB.

Additionally, IronPort Data Security logs all the upload transactions so that you can retain the record for HR investigations if a data loss incident is reported.

To use IronPort Data Security, first you enable the IronPort Data Security Filters, and then you create Data Security policies to create the business policies you want to enforce.

For more information, see the "Data Security and External DLP Policies" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

New Feature: External Data Loss Prevention

AsyncOS for Web 6.0 interoperates with leading Data Loss Prevention (DLP) vendors for advanced web DLP. The Web Security appliance sends the outbound traffic to the configured third party external DLP server, and enforces the verdict returned by the DLP server. This allows you to use content scanning, dictionaries, file fingerprinting and other techniques to satisfy advanced web DLP use cases like regulatory compliance and case management.

To use data loss prevention, first you define external DLP servers on the Web Security appliance, and then you create External DLP policies.

Even when the appliance uses External DLP policies, IronPort recommends that you also use IronPort Data Security in parallel because this combination has better performance than using External DLP policies alone. IronPort Data Security policies can block uploaded content sooner than External DLP policies in many cases. For example, you might use the IronPort Data Security policies to block data uploads to websites with a low reputation score. This way, the data is never sent to the External DLP system for a deep content scan, which improves overall performance. Content that needs deeper inspection can be selectively passed to the External DLP server for content analysis.

For more information, see the "Data Security and External DLP Policies" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

New Feature: Native FTP

Prior to AsyncOS for Web 6.0, the Web Security appliance supported FTP over HTTP in addition to HTTP and HTTPS.

With AsyncOS for Web 6.0, the Web Security appliance supports traffic sent over native FTP. This allows you to control and secure the native FTP traffic in your organization, in addition to HTTP and HTTPS traffic. For example, you can control users who are allowed to download or upload documents over FTP. You can also scan content downloaded over FTP with the IronPort DVS engine and the anti-malware scanning engines.

For more information, see the "Working with FTP Connections" section of the "Web Proxy Services" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

New Feature: Multiple Identities in a Policy Group

In AsyncOS for Web 6.0, you can add multiple identities to a single non-identity policy group. This allows you to keep identities as granular as required, and then either associate them all with a single policy group or with different policy groups. This can be useful after a merger, when you need to keep the identities of the merged companies separate because they use different authentication realms, but use both these identities together in a single uniform policy.

For more information, see the "Configuring Identities in Other Policy Groups" section in the "Identities" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

New Feature: Warning Users Before Continuing

With AsyncOS for Web 6.0, you can warn users that a site does not meet the organization's acceptable use policies and allow them to continue if they choose. To warn users and allow them to continue, configure the URL categories for an access policy group.

When users access a URL that is configured to warn and continue, they initially see an IronPort notification page with a warning about accessing sites of this category. The end-user URL category warning page includes a "continue" hypertext link to the originally requested URL. With this continue option, the end-user can review the company's acceptable use policy and, if desired, continue accessing the blocked site. End-user actions are appropriately logged.

For more information, see the "Warning Users and Allowing Them to Continue" section in the "URL Filters" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Enhanced: Authentication

AsyncOS 6.0 for Web includes several changes and enhancements to authentication.

Re-Authentication

In AsyncOS for Web 6.0, it is possible for a user to re-authenticate when blocked from accessing a web site due to restrictive URL filtering. Users can enter different authentication credentials that allow broader access. To do this, enable the "Enable Re-Authentication Prompt If End User Blocked by URL Category" global authentication setting. This is useful in many situations including, for example, authenticating users on a shared workstation, or allowing a teacher to enter higher privileged credentials to provide access to restricted websites to students for a limited time.

For more information, see the "Allowing Users to Re-Authentication" section in the "Authentication" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Guest Access (Failed Authentication)

Sometimes, users do not have an account in an organization's user directory. Examples of such users include visitors, contractors, interns, and students pursuing a short course. AsyncOS for Web 6.0 allows you to define policies for these users who fail authentication due to invalid credentials. Users who fail authentication and are granted access are logged in as guests, and their activities are logged by user name (as entered by the user) or IP address with a tag indicating the user was not authenticated.

To grant guest access to users who fail authentication, you create an identity that requires authentication, but also allows guest privileges. Then you create another policy using that identity and apply that policy to the guest users. When users have guest access, they can access the resources defined in the policy group that specifies guest access for that identity. Typically, guest policies allow for limited access to web resources.

For more information, see the "Allowing Guest Access to Users Who Fail Authentication" section in the "Identities" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

NTLM Authentication Caching

In previous versions, when the Web Security appliance used cookie-based NTLMSSP authentication, users were authenticated against the Active Directory server every time they made a request to a new domain. Now in AsyncOS for Web 6.0, the Web Security appliance uses authentication caching to reduce the load on the Active Directory server. It does this by adding a master cookie to the request when the user is authenticated for the first time. Subsequent requests get authenticated by validating the cookie, and frequent requests to the Active Directory server are avoided, improving overall authentication performance.

Active Directory 2008 Support

AsyncOS for Web 6.0 supports Active Directory 2008, without requiring a domain controller running Windows Server 2003 or older versions in the network.

Surrogates in Explicit Forward Mode

In previous versions, you could configure authentication surrogates for tracking users in transparent mode or when secure client authentication (now known as credential encryption)

was enabled. Authentication surrogates allow you to associate transactions with a user either by IP address or cookie after the user has been authenticated successfully.

In AsyncOS for Web 6.0, you can configure authentication surrogates for both transparent and explicit forward deployments whether or not credential encryption is enabled.

For more information, see the "Configuring Global Authentication Settings" section in the "Authentication" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

LDAP User Attribute Based Group Authorization

AsyncOS for Web 6.0 supports LDAP schema which stores user group memberships in group objects or user objects. In previous versions, AsyncOS for Web only supports LDAP schema which stores user group memberships in group object.

For more information, see the "LDAP Group Authorization" section in the "Authentication" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Enhanced: Logging

AsyncOS 6.0 for Web includes several changes and enhancements to Web Security appliance logging to help you troubleshoot issues more easily.

W3C Standard Extended Log File Format Access Logs

In AsyncOS for Web 6.0, the Web Security appliance supports the W3C standard extended log file format (ELFF) for access log information. The W3C access log subscriptions record Web Proxy transaction history in a format that is readable by generic analysis tools. The extended log file format is self-describing, so your analysis tool can read the log fields in use and present them in an understandable format.

You can create multiple W3C access log subscriptions and define the data to include in each. You might want to create one W3C access log that includes all information your organization typically needs, and other, specialized W3C access logs that can be used for troubleshooting purposes or special analysis. For example, you might want to create a W3C access log for an HR manager that only needs access to certain information.

For more information, see the "W3C Compliant Access Logs" section in the "Logging" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Enhanced HTTPS Logging

AsyncOS for Web 6.0 includes enhanced logging of HTTPS transaction for easier troubleshooting. To view more HTTPS transaction details, increase the HTTPS log level detail to either Debug or Trace. With this feature, the HTTPS logs show various SSL handshake phases, such as establishing capabilities, server authentication and key exchange, client key exchange, and finalizing of the SSL handshake. Additionally, session information like server certificate, client certificate, certificate chain, key size, cipher used, and certificate verification message is also logged.

New Log File Types

AsyncOS 6.0 for Web includes the following new types of log files:

- **Data Security Logs.** Records client history for upload requests that are evaluated by the IronPort Data Security Filters.
- **Data Security Module Logs.** Records messages related to the IronPort Data Security Filters. The Data Security Module Logs are one of the Web Proxy module log types containing more detailed information for troubleshooting purposes.
- **FTP Proxy Logs.** Records error and warning messages related to the FTP Proxy. The FTP Proxy Logs are one of the Web Proxy module log types containing more detailed information for troubleshooting purposes.
- **W3C Access Logs.** Records Web Proxy client history in a W3C compliant format.

For more information, see the "Log File Types" section in the "Logging" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

Enhanced: Accelerated AsyncOS Upgrades

In AsyncOS 6.0 for Web, the IronPort update servers have a distributed architecture so customers can quickly download AsyncOS upgrades wherever in the world they are located. When configuring your system for AsyncOS upgrades, you can choose to stream upgrades directly to your IronPort appliances or set up a local server to host upgrades.

For more information, see the "Upgrading the System Software" and "Configuring Upgrade and Service Update Settings" sections in the "System Administration" chapter of the *IronPort AsyncOS for Web User Guide*. You can view this chapter in the PDF or the online help.

UPGRADING THE WEB SECURITY APPLIANCE

Read through and consider the upgrade impacts listed in this section. Some upgrade impacts were introduced in AsyncOS for Web 6.0 and some in version 6.3.

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.

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 and Limitations" on page 46.

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 for Web 6.5 are not supported by IronPort Centralized Configuration Manager (ICCM) or AsyncOS for Security Management.

W3C Log Custom Log Fields

AsyncOS for Web 6.3 has changed the syntax of some of the custom log fields for the W3C Logs, and it has removed some log fields for both the W3C logs and access logs.

Table 1-1 lists the old and new syntax for some of the W3C log fields.

Table 1-1 Changed W3C Log Field Syntax

Previous W3C Log Field Syntax	New W3C Log Field Syntax
cs(MIME_type)	cs-mime-type
sc(response-size)	sc-body-size
x-decoded-wbrs-value	x-wbrs-score
x-decoded-web-category-code-abbreviation	x-webcat-code-abbr

Table 1-1 Changed W3C Log Field Syntax (Continued)

Previous W3C Log Field Syntax	New W3C Log Field Syntax
x-decoded-web-category-code-full-name	x-webcat-code-full
x-DVS-Threat_name	x-dvs-threat-name
x-mcafee-filename-yielding-verdict	x-mcafee-filename
x-mcafee-av_detecttype	x-mcafee-av-detecttype
x-mcafee-av_scanerror	x-mcafee-av-scanerror
x-mcafee-av_virustype	x-mcafee-av-virustype

Table 1-2 lists the log fields that were removed in the W3C logs and access logs.

Table 1-2 Obsolete Log Fields

Obsolete W3C Log Field	Obsolete Access Log Field
N/A	%r
N/A	%T
x-asw-option-switchboard	%X
x-raw-numeric-wbrs-score	N/A
x-raw-web-category-code	N/A
N/A	%:

IronPort Notification Pages

This section contains important information if your organization uses customized IronPort notification pages.

New IronPort Notification Pages

AsyncOS for Web 6.0 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.

Customized IronPort Notification Pages

In previous versions of AsyncOS for Web, you could edit the IronPort Notification pages stored on the Web Security appliance to customize the look and content of each page.

In AsyncOS for Web 6.0, there is a new feature that allows users to re-authenticate when blocked from accessing a web site due to restrictive URL filtering. For re-authentication to work, users click on a link embedded in an IronPort end-user notification page. The following IronPort notification pages use the re-authentication link:

- ERR_BLOCK_DEST
- ERR_WEBCAT

However, when you upgrade to AsyncOS for Web 6.0, any customized IronPort notification page does not automatically inherit the re-authentication link. If the pages listed above were customized in the previous version, you need to edit them to take advantage of the new re-authentication feature. Edit the HTML files and add the following text:

```
<td>
%?R
<div align="left">
<form name="ReauthInput" action="%r" method="GET">
<input name="Reauth" type="button" OnClick="document.location='%r'"
id="Reauth" value="Login as different user...">
</form>
</div>
%#R
</td>
```

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.

Identities and Access Policies

In AsyncOS for Web 6.0, the way AsyncOS for Web evaluates Identities and Access Policies has changed. Previously, both policy types were evaluated in parallel. Now, Identities are always evaluated before Access Policies. In some configurations, this might result in different transactions being assigned to different Identities.

Update and Upgrade Settings

In AsyncOS for Web 6.0, the way you upgrade the system software and update security components has changed. This involves the following changes:

- Now, you configure upgrade and update settings in one location, the System Administration > Upgrade and Update Settings page, and using only one CLI command, `updateconfig`. The settings you configure, such as a proxy server on the network, apply to both updates and upgrades.
- The URL for downloading upgrades has changed. Therefore, if you have any existing firewall rules allowing download of legacy upgrades from `upgrades.ironport.com` ports such as 22, 25, 80, 4766, they must be removed and/or replaced with revised firewall rules.

- The System Administration > Upgrade Settings and System Administration > Component Updates pages no longer exist. Use the System Administration > Upgrade and Update Settings page for both types of settings.
- The `upgradeconfig` CLI command no longer exists. Use the `updateconfig` command.
- When you upgrade from a previous version, some settings from the update settings (Component Updates pages) are preserved instead of the proxy server settings from the upgrade settings (Upgrade Settings page). For example, the proxy server and network interfaces settings are preserved from the update settings. After you upgrade to AsyncOS for Web 6.0, check the settings on the System Administration > Upgrade and Update Settings page and verify they are correct for your environment.

For more information, see "Configuring Upgrade and Service Update Settings" and "Upgrading the System Software" in the System Administration chapter.

Routing Tables

In AsyncOS for Web 6.0, the routing tables you can select for different Internet-facing services, such as DNS and service updates, have changed slightly. Previously, you configured a particular network interface to specify the routing table. You could choose M1, P1, P2, or "Auto." Now, you can choose "Management" or "Data."

The settings get upgraded according to the following mappings:

- "Auto" gets upgraded to Management.
- P1 and P2 gets upgraded to Data.
- M1 gets upgraded to Management.

Custom URL Categories

In previous versions of AsyncOS for Web, custom URL categories were "included" in policy URL filtering by default. If you did not want the IronPort URL Filters to evaluate the URL in a transaction against a custom URL category in an access or decryption policy, you had to explicitly exclude the custom URL category for that policy group.

Now, in AsyncOS for Web 6.0, custom URL categories are excluded by default when you create a new access or decryption policy. If you want to include a custom URL category in a new access or decryption policy, you must explicitly include it in the policy group. When you upgrade to AsyncOS for Web 6.0, existing policy groups retain their custom URL category settings.

"Proxy-Authorization" Header

In previous versions of AsyncOS for Web, by default, the Web Proxy did not pass the "Proxy-Authorization" header to the next server (including proxy servers) if the Web Proxy used the information in the header. Also, the Web Proxy could be configured to always pass the "Proxy-Authorization" header to the next server.

Now, in AsyncOS for Web 6.0, by default, the Web Proxy *never* passes the "Proxy-Authorization" header to the next server. You can configure this option using the

`advancedproxyconfig > authentication` CLI command, and select from any of the following settings:

- **Never.** The Web Proxy never passes the "Proxy-Authorization" header to the next server. This is the default. After upgrading to AsyncOS for Web 6.0, this becomes the default when the setting was previously configured to sometimes pass the header.
- **Always.** The Web Proxy always passes the "Proxy-Authorization" header to the next server.
- **Only if not used by the WSA.** The Web Proxy only passes the "Proxy-Authorization" header to the next server if the Web Proxy does not use the information in the header.

If an upstream proxy server requires the "Proxy-Authorization" header, you might need to change the `advancedproxyconfig > authentication` CLI command to "Always" or "Only if not used by the WSA."

Access Logs

In previous versions of AsyncOS for Web, some string fields in the access logs were enclosed in double quotes ("") if the value contained a space. However, the fields were not always enclosed in double quotes.

In AsyncOS for Web 6.0, the string fields that may contain spaces are always enclosed in double quotes. This includes, for example, authenticated user name and the user agent, if added. Also, all fields (format specifiers) entered in the Custom Fields field are enclosed in double quotes. For a list of all fields enclosed in double quotes, see the "Logging" chapter of the *IronPort AsyncOS for Web User Guide*.

The access logs also include the following additions:

- The ACL decision tag includes more components for the new policy groups introduced in AsyncOS for Web 6.0.
- The Web Reputation filtering and Anti-Malware scanning information section (inside the angled brackets (<>)) includes two new verdicts, one for the Data Security Policy scanning verdict and one for the External DLP Policy scanning verdict.

Upgrading AsyncOS for Web

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

1. On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.
2. On the System Administration > System Upgrade page, click **Available Upgrades**.

   The page refreshes with a list of available AsyncOS for Web upgrade versions.
3. Click **Begin Upgrade** to start the upgrade process. Answer the questions as they appear.
4. When the upgrade is complete, click **Reboot Now** to reboot the Web Security appliance.

BUGS FIXED IN 6.3.4

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. [Defect ID: 69793]

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. [Defect ID: 69902]

Fixed: Web Proxy restarts and generates a core file when serving a range of PDF content from the web cache

Previously, the Web Proxy restarted and generated a core file when serving a range of PDF content from the web cache. This no longer occurs. [Defect ID: 70142]

Fixed: Web Proxy restarts and generates a core file with decryption enabled in some cases

Previously, the Web Proxy restarted and generated a core file when decryption was enabled and the HTTPS server returned a 503 Service Unavailable response. This no longer occurs. [Defect ID: 70182]

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. [Defect ID: 54894]

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. [Defect ID: 54929]

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. [Defect ID: 65977]

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. [Defect ID: 66458]

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. [Defect ID: 66944]

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. [Defect ID: 67029]

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. [Defect ID: 67816, 52504]

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. [Defect ID: 67917]

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. [Defect ID: 68044]

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. [Defect ID: 68059]

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. [Defect ID: 68202]

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. [Defect ID: 68817]

Fixed: Web Proxy in transparent mode generates a core file when authenticating multiple users simultaneously in some cases

Previously, the Web Proxy in transparent mode generated a core file when authenticating multiple users simultaneously and it was configured with a large surrogate timeout value and to use cookie-based authentication. This no longer occurs. [Defect ID: 69128]

BUGS FIXED IN 6.3.3

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. [Defect ID: 52515]

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. [Defect ID: 69647]

Fixed: Decrypting some HTTPS fails in some cases

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. [Defect ID: 54925]

Fixed: Web Proxy generates a core file when a request is being served from the web cache in some cases

Previously, the Web Proxy generated a core file when a request was being served from the web cache in memory and writing the response to the client failed in some cases. This no longer occurs. [Defect ID: 67860]

Fixed: HTTPS Proxy generates a core file and stops decrypting transactions in some cases

Previously, the HTTPS Proxy generated a core file and stopped decrypting transactions when HTTPS transactions were reset frequently. This no longer occurs. [Defect ID: 68430]

Fixed: FTP Proxy returns incorrect IP address when replying to the PASV command in some cases

Previously, the FTP Proxy returned the incorrect network interface IP address when replying to the PASV command when both the M1 and P1 network interfaces were configured for data traffic. This no longer occurs. [Defect ID: 51768]

Fixed: Transparently tunneling non-HTTP traffic does not work

Previously, transparent tunneling of non-HTTP traffic did not work. This no longer occurs. [Defect ID: 56336]

Fixed: FTP Proxy generates a core file when a client FTP connection is interrupted

Previously, the FTP Proxy generated a core file when a client FTP connection was interrupted. This no longer occurs. [Defect ID: 67685]

Fixed: Appliance may lock up or reboot when tailing access logs in some cases

Previously, the Web Security appliance would lock up and reboot when viewing the access logs with the `tail` CLI command on some versions of the hardware. This no longer occurs. [Defect ID: 42438]

Fixed: HTTPS Proxy root certificate and key pair is erroneously overwritten when using the Security Management appliance in some cases

Previously, when you used the Security Management appliance to load a configuration onto a Web Security appliance, the HTTPS Proxy root certificate and key pair was erroneously overwritten. This no longer occurs. [Defect ID: 42636]

Fixed: hostkeyconfig CLI command erroneously returns a traceback in some cases

Previously, using the `hostkeyconfig` CLI command erroneously returned a traceback instead of listing the available subcommands when the appliance contained some invalid SSH keys. This no longer occurs. [Defect ID: 48748]

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. [Defect ID: 52504]

Fixed: Web Proxy erroneously returns some objects from the web cache instead of from the web server in some cases

Previously, the Web Proxy erroneously returned some objects from the web cache regardless of the "Accept-Encoding" HTTP header, ignoring the information given in the "Vary" HTTP header. This no longer occurs. [Defect ID: 54474]

Fixed: Native FTP downloads fail with McAfee enabled in some cases

Previously, McAfee failed to scan some native FTP downloads with logs showing "Scanning Error" error. This no longer occurs. [Defect ID: 54572]

Fixed: Cannot join the Active Directory domain in some cases

Previously, the Web Security appliance could not join the Active Directory domain due to some Kerberos errors. This happened when the Active Directory server did not return the expected reply to AsyncOS's kinit request. The web interface displayed the following error message:

"Error while fetching Kerberos Ticket from server '*servername*':

This no longer occurs. [Defect ID: 54854]

Fixed: Compressed log files are not pushed to configured SCP or FTP servers

Previously, compressed log files were not pushed to configured SCP or FTP servers. This no longer occurs. [Defect ID: 54944]

Fixed: Web Proxy generates a core file when HTTPS Proxy and secure client authentication are disabled in some cases

Previously, the Web Proxy generated a core file when the HTTPS Proxy and secure client authentication were disabled and a CONNECT request was made to the "Redirect Hostname" configured on the appliance. This no longer occurs. [Defect ID: 55352]

Fixed: Native FTP using Raptor format authentication fails when proxy authentication is not required

Previously, native FTP using the Raptor format authentication failed when proxy authentication was not required. This no longer occurs. [Defect ID: 55379]

Fixed: Cannot restrict M1 network interface to management only when VLANS are configured in some cases

Previously, you could not restrict the M1 port to management only when VLANS were configured on the P1 network interface. This no longer occurs. [Defect ID: 55893]

Fixed: TLS/SSL Man-in-the-Middle Vulnerability

Previously, an industry-wide vulnerability that existed in the TLS protocol potentially impacted any Cisco product using any version of TLS /SSL. The vulnerability existed in how the protocol handled session re-negotiation and exposed users to a potential Man-in-the-middle attack. This issue has been fixed. [Defect ID: 55972]

Fixed: Web Proxy erroneously sends two requests to a server instead of one in some cases

Previously, the Web Proxy erroneously sent two requests to a server instead of one when the requested object existed in the web cache, but had expired. The Web Proxy always returned the object to the client as retrieved from the server in the second request. This no longer occurs. Now, the Web Proxy returns the object from the web cache if the server indicates the object has not been modified, or it returns the object from the server if it has been modified. [Defect ID: 55973]

Fixed: Web Proxy erroneously includes duplicate HTTP headers to web servers in some cases

Previously, the Web Proxy erroneously included duplicate "Connection: keep-alive" HTTP headers to web servers when requesting expired cached objects. This caused some web servers to not properly service the request. This no longer occurs. [Defect ID: 55974]

Fixed: Web Proxy stops authenticating users when the Active Directory server is unavailable in some cases

Previously, the Web Proxy stopped authenticating users when the Active Directory server was shut down either for long periods of time or multiple times. This caused an internal process to leak sockets and no longer respond to authentication requests until the Web Proxy restarted. This no longer occurs. [Defect ID: 56207]

Fixed: Access logs erroneously omit log entries for some transactions

Previously, the access logs erroneously omitted log entries for server responses that contained a space in some header fields, such as the Content-Type header. This no longer occurs. [Defect ID: 56227]

Fixed: Web Proxy returns incomplete web pages from objects in the web cache in some cases

Previously, the Web Proxy returned incomplete web pages from objects in the web cache when the cached objects contain HTTP headers with an extra space at the end of the header. Some web servers, such as facebook.com, erroneously include an extra space in some HTTP headers. This no longer occurs. [Defect ID: 66076]

Fixed: IronPort Data Security Filters erroneously block all upload requests in some cases

Previously, the IronPort Data Security Filters erroneously blocked all upload requests after the Web Security appliance rebooted. This no longer occurs. [Defect ID: 66286]

BUGS FIXED IN 6.3.1

Fixed: Web Proxy generates a core file when uploading a file using FTP in some cases

Previously, the Web Proxy generated a core file when a client uploaded a file to an FTP server and the server encountered an unexpected error, such as running out of space for new files. This no longer occurs. [Defect ID: 49837]

Fixed: Authentication issues observed with some LDAP servers

Previously, various authentication problems were encountered with some LDAP servers due to how AsyncOS managed connections with the LDAP server. Some issues observed were clients being authenticated with the wrong (cached) user name, and user group based policies not matching transactions correctly. This no longer occurs. Now, AsyncOS manages connections with LDAP servers correctly. [Defect ID: 50706]

Fixed: End-user URL category warning page hypertext link does not work with virtual IP addresses in some cases

Previously, the end-user URL category warning page hypertext link sometimes erroneously used the Web Security appliance's IP address instead of the hostname. When clients on the network accessed the appliance using a virtual IP address, the hypertext link in the warning page did not work. This no longer occurs. [Defect ID: 51440]

Fixed: status CLI command displays incorrect value for a setting in some cases

Previously, the `status` CLI command displayed the incorrect value for the "Total server connections" setting when users used native FTP. This no longer occurs. [Defect ID: 51995]

Fixed: FTP clients do not work with FTP servers that support MLSD

Previously, FTP clients did not work with FTP servers that support MLSD. This was due to the FTP Proxy claiming the FTP server supported MLSD even though the FTP Proxy did not support MLSD. Clients would try to use MLSD, but the transaction failed. This no longer occurs. Now, the FTP Proxy no longer claims that the FTP server supports MLSD, so FTP clients no longer try to use it. [Defect ID: 52216]

Fixed: Explicit forward requests to non-standard ports are redirected to port 80 in some cases

Previously, explicit forward requests to non-standard ports were redirected to port 80 when the authentication settings required the Web Proxy to use a 307 HTTP response to redirect the client to the Web Proxy for authentication purposes. This no longer occurs. Now, the authentication redirect URL preserves the non-standard port. [Defect ID: 52427]

Fixed: HTTPS requests fail with the end-user acknowledgement page enabled in some cases

Previously, HTTPS requests failed when the assigned Decryption Policy decrypted the transaction, and the assigned Access Policy caused the end-user acknowledgement page to

display. The end-user acknowledgement page appeared, but when the user clicked the acknowledgement link, the request timed out. This no longer occurs. [Defect ID: 52522]

Fixed: Web Security appliance spontaneously reboots due to a slow memory leak when clients used NTLMv1 authentication in some cases

Previously, the Web Security appliance spontaneously rebooted due to a slow memory leak when clients used NTLMv1 authentication and policy groups defined users by authentication user groups. This no longer occurs. [Defect ID: 52548]

Fixed: HTTPS requests fail when an upstream proxy uses NTLMSSP authentication in some cases

Previously, HTTPS requests failed when the Web Security appliance did not require authentication, but an upstream proxy used NTLMSSP authentication. This no longer occurs. [Defect ID: 52574]

Fixed: Access logs erroneously list policy group name as "NONE" in some cases

Previously, the Access logs erroneously listed policy group name as "NONE" when the browser included the If-Modified-Since HTTP header. This no longer occurs. [Defect ID: 53766]

Fixed: Webroot scanning engine stops working when downloading some .cab files

Previously, the Webroot scanning engine stopped working when downloading some .cab files. This no longer occurs. [Defect ID: 53793]

Fixed: Web Proxy generates a core file after a client sends a POST request to a server that returns a 503 "Service Unavailable" message in some cases

Previously, the Web Proxy generated a core file after a client sent a POST request to a server that returned a 503 "Service Unavailable" message when the IronPort Data Security Filters are disabled. This no longer occurs. [Defect ID: 54019]

Fixed: HTTP responses are erroneously blocked when content encoded

Previously, HTTP responses were erroneously blocked when the HTTP server encoded the response as indicated by the Content-Encoding header. This no longer occurs. [Defect ID: 54225]

Fixed: Proxy logs show large number of "Could not find record of closed connection" warning messages in some cases

Previously, the Proxy logs showed a large number of "Could not find record of closed connection" warning messages due to mishandling of server connections. This no longer occurs. [Defect ID: 54362]

Fixed: Web interface erroneously shows 100% CPU utilization when rate is lower

Previously, the web interface erroneously showed 100% CPU utilization when the true rate was lower. This no longer occurs. [Defect ID: 54767]

Fixed: Web Proxy generates a core file and restarts in some cases

Previously, the Web Proxy generated a core file and restarted due to leaked connections. This no longer occurs. [Defect ID: 54890]

Fixed: Web Proxy generates a core file with the error message "NFTPReturnProxyRespMessage"

Previously, the Web Proxy generated a core file with the error message "NFTPReturnProxyRespMessage". This no longer occurs. [Defect ID: 55354]

Fixed: Web Proxy generates a core file and restarts after processing some HTTPS requests in some cases

Previously, the Web Proxy generated a core file and restarted after a memory leak. This no longer occurs. [Defect ID: 55407]

BUGS FIXED IN 6.3.0

Fixed: Vulnerability in Secure Sockets Layer (SSL) certificates

A vulnerability in Secure Sockets Layer (SSL) certificates has been fixed. The vulnerability allowed attackers to substitute imposter SSL certificates in place of trusted ones when clients used an affected browser. This no longer occurs. [Defect ID: 55278]

Fixed: Web Proxy erroneously returns a 504 "Gateway Timeout" status to clients accessing HTTPS sites in some cases

Previously, the Web Proxy erroneously returned a 504 "Gateway Timeout" status to clients accessing HTTPS sites due to leaking memory. This no longer occurs. [Defect ID: 41794]

Fixed: Web Proxy cannot communicate with FTP servers in some cases

Previously, the Web Proxy could not communicate with FTP servers under the following circumstances:

- The Web Proxy received a transparently redirected FTP request (either native FTP or FTP over HTTP) in passive mode.
- IP spoofing was enabled on the Security Services > Proxy Settings page.

This no longer occurs. [Defect ID: 47571]

Fixed: "Get Groups" button in the Policy Trace tool does not return all groups in some cases

Previously, the **Get Groups** button in the Policy Trace tool did not return all groups for a user in an NTLM authentication realm when the Active Directory server returned group names with different capitalization than the authorized group names listed in the applicable policy group. This no longer occurs. [Defect ID: 49292]

Fixed: Web Proxy generates a core file when it receives a transparent native FTP request with proxy authentication required and an upstream proxy is used

Previously, the Web Proxy generated a core file when it received a transparent native FTP request and the Identity required authentication for native FTP transactions and a Routing Policy directed the transaction to an upstream proxy. Authentication is not supported for transparent native FTP requests, however, the Web Proxy should not have generated a core file. This no longer occurs. [Defect ID: 49997]

Fixed: Web Proxy generates a core file when persistent server connections are used in some cases

Previously, the Web Proxy generated a core file when persistent server connections were used and clients uploaded large requests. This no longer occurs. [Defect ID: 50334]

Fixed: McAfee scanning engine stops working after a feature key is updated in some cases resulting in latency

Previously, the McAfee scanning engine stopped scanning transactions when the McAfee feature key expired and then was updated. This resulted in slow response times for transactions. This no longer occurs. Now, McAfee scanning works after the feature key is updated after expiration and no latency is observed. [Defect ID: 50591]

Fixed: Web Proxy stops processing transactions after upgrading from a version with an invalid configuration in some cases

Previously, the Web Proxy stopped processing transactions and the proxy logs showed error messages saying, "Couldn't determine available system storage." This happened after upgrading from a previous version that had a custom URL category that was deleted, but the configuration file still had some residual references to the deleted custom URL category. This no longer occurs. [Defect ID: 50839]

Fixed: Web Proxy does not start when it fails nslookups on its own IP address

Previously, the Web Proxy did not start when it failed nslookups on its own IP address. This no longer occurs. [Defect ID: 50853]

Fixed: Web Proxy generates a core file when processing very long URIs in some cases

Previously, the Web Proxy generated a core file when processing very long URIs after an internal failure. This no longer occurs. [Defect ID: 50986]

Fixed: Wrong action taken on upload requests with IronPort Data Security Policies and custom URL categories in some cases

Previously, when an upload request was matched to an IronPort Data Security Policy, and the URL in the request matched a custom URL category set to Monitor, the Web Proxy applied the action defined for the applicable predefined URL category instead. This no longer occurs. [Defect ID: 51027]

Fixed: HTTP requests fail when the request header is slightly smaller than 16K in size

Previously, HTTP requests failed when the request header was slightly smaller than 16K in size. This no longer occurs. [Defect ID: 51083]

Fixed: CPU utilization rate is very high with a large number of policies

Previously, the CPU utilization rate was very high with a large number of policies. This no longer occurs. [Defect ID: 51362]

Fixed: Application fault occurs in the CLI when creating a new Request Debug log

Previously, an application fault occurred in the CLI when creating a new Request Debug log using the `logconfig` CLI command. This no longer occurs. [Defect ID: 51406]

Fixed: Web interface shows incorrect WBRS setting for Decryption Policies in some cases

Previously, the web interface showed the incorrect WBRS setting for Decryption Policies when the setting was changed so the Drop value was between -10.0 and 0.0. This no longer occurs. [Defect ID: 51421]

Fixed: Some image files are erroneously allowed to download

Previously, when an Access Policy was configured to block image files, such as image/gif, some images were erroneously downloaded from servers that erroneously report the Content Type. This no longer occurs. Now, all images are always blocked according to their actual type. [Defect ID: 51450]

Fixed: Web Proxy leaks memory and eventually generates a core file after processing upload requests in some cases

Previously, the Web Proxy leaked memory and eventually generated a core file after attempting to upload data to servers that were not responding. This no longer occurs. [Defect ID: 51850]

Fixed: NTLM proxy authentication against Windows 2008 Server R2 does not work

Previously, NTLM proxy authentication against Windows 2008 Server R2 did not work. This no longer occurs. Effective in AsyncOS for Web 6.3, NTLM proxy authentication works and is supported against generally available versions of Windows 2008 Server including version R2. [Defect ID: 52047]

Fixed: Access Policies do not correctly match transactions when the authentication realm used in the associated Identity contains a space

Previously, access Policies did not correctly match transactions when the authentication realm used in the associated Identity contained a space. This no longer occurs. [Defect ID: 52070]

Fixed: Blocking the "Java Program" object type also erroneously blocks javascript

Previously, blocking the "Java Program" object type in Access Policies also erroneously blocked javascript. This no longer occurs. Now, only java programs are blocked. [Defect ID: 52083]

Fixed: Access logs do not contain entries for requests from users with spaces in the user name

Previously, access logs did not contain entries for requests from users with spaces in the user name. This no longer occurs. [Defect ID: 52092]

Fixed: Downloads greater than 4 GB fail

Previously, when a client tried to download a file through the Web Proxy that was greater than 4 GB, the file failed to completely download. This no longer occurs. [Defect ID: 52353]

Fixed: Web Proxy sends incorrectly formatted requests to upstream proxy servers that require NTLM authentication

Previously, the Web Proxy sent incorrectly formatted requests to upstream proxy servers that required NTLM authentication. This no longer occurs. [Defect ID: 52369]

Fixed: URL category "Transportation" is misspelled

Previously, the URL category "Transportation" is misspelled as "Transporation." This no longer occurs. [Defect ID: 50599]

Fixed: Policy groups appear to lose authentication groups after upgrading from version 5.6

Previously, policy groups, such as Access Policies, appeared to lose the configured authentication user groups after upgrading from AsyncOS for Web version 5.6 under the following circumstances:

- In the previous version, the global Identity group was configured to use authentication and no user defined Identity groups were defined.
- A policy group using the global Identity defined specific authentication user groups.

The upgrade process erroneously created a new Identity group that used authentication and configured the global Identity to not use authentication. This no longer occurs. Now, the Access Policies use the global Identity group and no new Identities are created. [Defect ID: 50973]

Fixed: Deleting a custom category erroneously disables all Access Policies that define membership by any custom URL category

Previously, deleting a custom category erroneously disabled all Access Policies that defined membership by any custom URL category. This no longer occurs. Now, deleting a custom category only disables Access Policies that include the deleted custom URL category in its membership criteria. [Defect ID: 47543]

Fixed: Web Proxy does not spoof client IP address in the data channel for FTP over HTTP in passive mode even with IP spoofing enabled

Previously, when IP spoofing was enabled and a client sent an FTP over HTTP transaction in passive mode, the Web Proxy did not spoof the client IP address in the data channel. This no longer occurs. [Defect ID: 47562]

Fixed: Web Proxy unavailable for a couple seconds after some configuration changes

Previously, the Web Proxy erroneously restarted and was unavailable for a couple seconds and refused some connections after some configuration changes. This no longer occurs. [Defect ID: 48868]

Fixed: Packet capture feature fails to include some packets

Previously, the packet capture feature failed to include packets sent to the Web Security appliance using GRE. This made it more difficult for Customer Support to assist customers. This no longer occurs. [Defect ID: 48971]

Fixed: End-user acknowledgement page link contains client IP instead of Web Security appliance IP after DNS failure

Previously, the link included in the end-user acknowledgement page contained the client IP address instead of Web Proxy IP address after DNS failure. This no longer occurs. [Defect ID: 49114]

Fixed: Some FTP over HTTP requests erroneously time out when the network connection is slow

Previously, some FTP over HTTP requests mishandled server responses and erroneously timed out client connections when the network connection was slow. This no longer occurs. [Defect ID: 49142]

Fixed: Configuration file erroneously references deleted custom URL categories in some cases

Previously, when a custom URL category was deleted and the Web Security appliance configuration was saved, the configuration file included references to the deleted category if the category was used in a time-based Access Policy. This no longer occurs. [Defect ID: 49416]

Fixed: Access logs and FTP logs do not include entries for blocked native FTP transactions that require authentication when the client provided no credentials

Previously, the access logs and FTP did not include entries for blocked native FTP transactions that required authentication when the client provided no credentials. This no longer occurs. [Defect ID: 49859]

Fixed: Cannot access URL Categories page from the Advanced section of Access Policies using Internet Explorer 7

Previously, when you clicked the URL Categories link in the Advanced section of an Access Policy using Internet Explorer 7, the page showing the authentication groups appeared instead of the URL Categories page. This no longer occurs. [Defect ID: 50152]

Fixed: Web Proxy generates a core file when processing some transparent authentication requests

Previously, the Web Proxy generated a core file when processing some transparent authentication requests. This no longer occurs. [Defect ID: 50198]

Fixed: Web Proxy generates a core file when a client application uses HTTP pipelining

Previously, the Web Proxy generated a core file when a client application used HTTP pipelining (multiple HTTP requests are written out to a single socket without waiting for the corresponding responses) due to internal memory management issues. This no longer occurs. [Defect ID: 50248]

Fixed: Web Proxy generates a core file and restarts multiple times a day when fetching content from the memory cache

Previously, the Web Proxy generated a core file and restarted multiple times a day when fetching content from the memory cache. This no longer occurs. [Defect ID: 50405]

Fixed: Slow response times experienced after McAfee license expires

Previously, users experienced slow response times after the McAfee license expired on the Web Security appliance. This no longer occurs. [Defect ID: 50449]

Fixed: Web Proxy generates a core file when processing some malformed HTTP requests

Previously, the Web Proxy generated a core file when processing malformed HTTP requests that tried to connect to the non-existent port 0 on the server. This no longer occurs. [Defect ID: 51084]

Fixed: Application fault occurs when trying to specify subnets for Access Policy membership with no Identity selected

Previously, an application fault occurred when trying to specify subnets for Access Policy membership when no Identity was selected. This no longer occurs. [Defect ID: 51123]

Fixed: DNS lookups fail when using the routing table on the Data network interface

Previously, DNS lookups failed when using the routing table on the Data network interface. This no longer occurs. [Defect ID: 51139, 51140]

Fixed: Cannot enable End-User Misclassification Reporting in some cases

Previously, administrators could not change the state (to enabled or disabled) of the End-User Misclassification Reporting field on the Security Services > End-User Notification page. The GUI made it appear as if the change took effect, but the Web Security appliance configuration did not change. This no longer occurs. [Defect ID: 48886]

Fixed: Application fault occurs in an internal process and an alert is sent after deleting a time range in some cases

Previously, an application fault occurred in an internal process and an alert was sent after the following steps were taken:

- The global Access Policy was configured to take action on a predefined URL category based on a time range.
- The time range used by the global Access Policy was deleted.

- You went to the URL Categories page for the global Access Policy and clicked **Submit** and **Commit** without making any changes.

This no longer occurs. [Defect ID: 49916]

Fixed: Custom URL categories cannot be included in the global Access Policy after deleting a time range in some cases

Previously, custom URL categories could not be included in the global Access Policy after the following steps were taken:

- A custom URL category was included in the global Access Policy and the category action was time-based using a defined time range.
- The time range used in the custom URL category that was included in the global Access Policy was deleted.
- You went to the URL Categories page for the global Access Policy and clicked **Submit** and **Commit** without making any changes.

When you navigated to the URL Categories page for the global Access Policy again, the custom URL category edited previously did not appear in the list of custom URL categories.

This no longer occurs. [Defect ID: 49919]

Fixed: Upload requests fail to match IronPort Data Security and External DLP Policies that use group authorization in some cases

Previously, upload requests failed to match IronPort Data Security and External DLP Policies that used group authorization when another policy type, such as an Access Policy, did not define its membership by the same group authorization requirements. This no longer occurs. [Defect ID: 49720]

Fixed: AsyncOS lists the incorrect McAfee scanning engine version in some cases

AsyncOS listed the incorrect McAfee scanning engine version (version 5200) instead of 5300 in the web interface and CLI under the following circumstances:

- You received a Web Security appliance with AsyncOS 6.0 already installed.
- You had an existing Web Security appliance with McAfee scanning engine updated to version 5300 and then upgraded AsyncOS to version 6.0.
- A Web Security appliance running AsyncOS 6.0 updated the McAfee scanning engine to version 5300 and sometime after, an administrator reset the configuration on the Web Security appliance.

This no longer occurs. The correct McAfee scanning engine version is still updated and in use and is now displayed correctly. [Defect ID: 49360]

Fixed: Web Proxy continually restarts when regular expressions are used in IronPort Data Security Policies in some cases

Previously, the Web Proxy continually restarted when an IronPort Data Security Policy contained regular expressions with some special characters for file names to block. This no longer occurs. [Defect ID: 45785]

Fixed: Application fault occurs when a Web Security appliance user full name includes some special characters

Previously, an application fault occurred when a Web Security appliance user full name included some special characters. This no longer occurs. Now, when the full name of the appliance user contains one of the following characters, it displays a warning message instead:

```
: @ !
```

[Defect ID: 47888]

Fixed: Native FTP requests with FTP Proxy authentication enabled erroneously allowed in some cases

Previously, when FTP Proxy authentication was enabled, native FTP requests from the Filezilla FTP client were erroneously allowed even when the user supplied no or incorrect authentication credentials. This no longer occurs. [Defect ID: 49087]

Fixed: IronPort Data Security Filters does not block upload requests to some sites

Previously, IronPort Data Security Filters did not block upload requests to sites that include the path with the file name in the upload request, such as Virgin Mail. This no longer occurs. Now, the upload requests are blocked as configured in the IronPort Data Security Policies. [Defect ID: 49326]

Fixed: Web Proxy generates a core file when an FTP client issues the QUIT command in some cases

Previously, the Web Proxy generated a core file when an FTP client issued the QUIT command after being idle for awhile. This no longer occurs. [Defect ID: 49469]

Fixed: VCS and ICS files are erroneously recognized as the “application/x-awk” MIME type

Previously, the calendar file types of VCS and ICS were erroneously recognized as the “application/x-awk” MIME type. This no longer occurs. Now, these file types are recognized and matched as the “text/x-vcalendar” MIME type. [Defect ID: 49639]

Fixed: Requests are erroneously matched against an incorrect policy group with some global authentication setting values

Previously, requests were erroneously matched against an incorrect policy group when the Basic Authentication Token TTL value was less than the Surrogate Timeout value. This no longer occurs. [Defect ID: 49708]

Fixed: Validation error erroneously occurs in the web interface when editing a policy group with All Identities in some cases

Previously, the web interface displayed an error message saying "Error — Errors have occurred. Please see below for details" under the following conditions:

- You created an Access, Decryption, IronPort Data Security, or External DLP Policy group with All Identities, and defined a single authorized user for the policy group.
- You submitted and committed the changes, and then opened the policy group to edit its membership.

This no longer occurs. [Defect ID: 49781]

BUGS FIXED IN 6.0.0

Fixed: Some web pages take several minutes to load when a web page component returns a 5xx response

Previously, some web pages took several minutes to load when a web page component returned a 5xx response due to the Web Proxy sending the body content twice. This no longer occurs. Now, web pages load normally and the Web Proxy sends the body content once. [Defect ID: 52020]

Fixed: Web Proxy generates a core file when uploading data with persistent connections and IronPort Data Security Filters enabled in some cases

Previously, the Web Proxy generated a core file when a transaction uploaded data using a persistent connection and the data was scanned by the IronPort Data Security Filters. This happened quite often with Adobe Flash applications. This no longer occurs. [Defect ID: 51813]

Fixed: Alerts fail to get sent when the Web Security appliance is configured to use separate networks for Management and Data traffic in some cases

Previously, alerts failed to get sent when the Web Security appliance was configured to use separate networks for Management and Data traffic and the SMTP server used for sending the alerts was not accessible from the Data network interface. This no longer occurs. [Defect ID: 51693]

Fixed: Web Proxy generates a core file when a client application uses HTTP pipelining

Previously, the Web Proxy generated a core file when a client application used HTTP pipelining (multiple HTTP requests are written out to a single socket without waiting for the corresponding responses) due to internal memory management issues. This no longer occurs. [Defect ID: 50248]

Fixed: HTTP requests fail when the request header is slightly smaller than 16K in size

Previously, HTTP requests failed when the request header was slightly smaller than 16K in size. This no longer occurs. [Defect ID: 51083]

Fixed: Web Proxy generates a core file when processing some malformed HTTP requests

Previously, the Web Proxy generated a core file when processing malformed HTTP requests that tried to connect to the non-existent port 0 on the server. This no longer occurs. [Defect ID: 51084]

Fixed: Web Proxy generates a core file serving a very large cached response in some cases

Previously, the Web Proxy generated a core file when trying to satisfy a range request with an invalid range for a large object served from cache. This no longer occurs. [Defect ID: 43813]

Fixed: Web Proxy generates a core file when an idle native FTP client issues a QUIT command

Previously, the Web Proxy generated a core file when an idle native FTP client issued a QUIT command. This no longer occurs. [Defect ID: 49469]

Fixed: Security vulnerability in OpenSSL

A security vulnerability, CVE-2009-0590, was identified in OpenSSL that affected the IronPort Web Security appliance. Due to this vulnerability, a user who browsed to a web server hosting a carefully crafted SSL server certificate could cause a denial of service. This issue has been fixed. [Defect ID: 49624]

Fixed: Web Proxy generates a core file when processing some transparent authentication requests

Previously, the Web Proxy generated a core file when processing some transparent authentication requests. This no longer occurs. [Defect ID: 50198]

Fixed: Web Proxy generates a core file and restarts multiple times a day when fetching content from the memory cache

Previously, the Web Proxy generated a core file and restarted multiple times a day when fetching content from the memory cache. This no longer occurs. [Defect ID: 50405]

Fixed: Slow response times experienced after McAfee license expires

Previously, users experienced slow response times after the McAfee license expired on the Web Security appliance. This no longer occurs. [Defect ID: 50449]

Fixed: Policy trace feature does not list matching policy when the request fails to authenticate

Previously, when you used the policy trace feature without entering a user name and the request matched policies requiring authentication, the policy trace feature properly showed that the request was blocked due to failed authentication, but it did not list which policies matched the request. This no longer occurs. [Defect ID: 40493]

Fixed: Policy trace feature does not display correct policies when policies lists authorized users in an authorization group

Previously, the policy trace feature did not display the correct policies when the policies listed authorized users in an authorization group. The policy trace listed either “None” or the global policy. However, the policy trace feature works when the policies list specific authorized users. This no longer occurs. Now, the policy trace feature displays the correct policies. [Defect ID: 43078]

Fixed: Preview pages in the web interface do not appear using Safari

Previously, when you clicked a link in the web interface to preview a page, such as the “Preview Custom URL,” the HTML page did not appear when using the Safari browser with

the pop-up blocker enabled. This no longer occurs. Now, a popup message appears informing users that pop-up blocking is enabled and they may need to disable it for the page to appear. [Defect ID: 35487]

Fixed: Web Security appliance becomes unconfigurable when it contains a large number of custom URL categories

Previously, the Web Security appliance became unconfigurable when it contained a large number of custom URL categories. This no longer occurs. [Defect ID: 41097]

Fixed: Application fault occurs on Access Policies page after upgrading in some cases

Previously, an application fault occurred on the Access Policies page after upgrading from a previous version when the previous configuration contained policy groups that referenced non-existent Identities. This no longer occurs.

Now, when you upgrade a configuration from a previous version that contained policy groups that referenced non-existent Identities, the policy groups are disabled and specify All Identities. [Defect ID: 46173]

Fixed: Some Russian end-user notification pages do not display correctly

Previously, some Russian end-user notification pages did not display correctly because they were not encoded using UTF-8. [Defect ID: 46815]

Fixed: Requests do not match NTLM based policies that separate the domain from users and groups using "\\"

Previously, requests did not match NTLM based policies that separated the domain from users and groups using "\\". This no longer occurs. Now, AsyncOS removes the extra slash character when it stores the authorized user or group in the policy group configuration. [Defect ID: 47117]

Fixed: AsyncOS does not fetch new HTTPS server certificate when the cached certificate has expired

Previously, AsyncOS did not fetch a new HTTPS server certificate when a cached certificate had expired. This no longer occurs. [Defect ID: 47454]

Fixed: Monitor > Anti-Malware page erroneously shows "Unnamed Malware" for some transactions when the McAfee scanning engine is overloaded

Previously, the Monitor > Anti-Malware page erroneously showed "Unnamed Malware" for some transactions when the McAfee scanning engine was overloaded. [Defect ID: 47601]

Fixed: FTP downloads fail when using anonymous login when FTP server does not require password for anonymous users

Previously, FTP downloads failed when using anonymous login when the FTP server did not require password for anonymous users. This no longer occurs. [Defect ID: 48173]

Fixed: Web Proxy does not serve ranges for cached content even if rangerequestdownload is enabled

Previously, the Web Proxy did not serve ranges for cached content even if rangerequestdownload was enabled. In some cases, this broke client applications that expected only part of the response in a range instead of the entire response. This no longer occurs. [Defect ID: 48394]

Fixed: Application error occurs in Japanese web interface when downloading a root certificate for the HTTPS Proxy

Previously, an application error occurred in the Japanese localized web interface when downloading a root certificate for the HTTPS Proxy. This no longer occurs. [Defect ID: 48624]

Fixed: Some client applications do not work with the Web Proxy

Previously, the Web Proxy did not forward some client headers to the destination server, breaking some client applications that used those headers. This no longer occurs. Now, the Web Proxy forwards those headers. [Defect ID: 49139]

Fixed: On-box reports incorrectly display requests that match custom URL categories

Previously, the on-box reports incorrectly displayed requests that matched custom URL categories. This no longer occurs. [Defect ID: 49257]

Fixed: Web Proxy leaks cache memory and slows down when processing large chunked transactions

Previously, the Web Proxy leaked cache memory and slowed down when processing large chunked transactions. This no longer occurs. [Defect ID: 49322]

Fixed: Web Reputation Filters returns “err” as the web reputation score for some HTTPS websites

Previously, when an HTTPS server used a security certificate containing an asterisk (*) in the Common Name (CN) field, the Web Reputation Filters returned “err” as the web reputation score instead of its true score. This no longer occurs. [Defect ID: 49394]

Fixed: Some URLs are miscategorized

Previously, some URL were miscategorized. This no longer occurs. Now, these URLs are correctly categorized. [Defect ID: 46203]

Fixed: End-user acknowledgement page times out after some configuration changes

Previously, the end-user acknowledgement page timed out after some configuration changes, prompting users to acknowledge the page again. This no longer occurs. However, it still times out after the Web Proxy restarts, as documented. [Defect ID: 47925]

Fixed: Cannot retrieve Active Directory groups for the configured user in the policy trace tool

Previously, clicking the Get Groups button in the policy trace tool did not retrieve the Active Directory groups for the configured user. This no longer occurs. Now, it returns the groups the user is a member of. [Defect ID: 48056]

Fixed: Accessing some buggy servers causes HTTP requests to hang in some cases

Previously, when the Web Proxy sent an If-Modified-Since request to a web server, it included a "Pragma: no-cache" header which caused some buggy web servers to not properly process the request. This no longer occurs. Now, the Web Proxy does not include the "Pragma: no-cache" header in If-Modified-Since requests. [Defect ID: 42124]

Fixed: Policy Trace does not show URL category when the Identity requires authentication

Previously, the Policy Trace feature did not show the applicable URL category when the Identity required authentication. This no longer occurs. [Defect ID: 44134]

Fixed: Web Proxy navigates to the incorrect directory on FTP servers in some cases

Previously, when a user opened a URL such as ftp://ftp.example.com/, the Web Proxy did not go to the home directory. Instead, it changed the working directory to the / directory. This no longer occurs. Now, the Web Proxy navigates to the correct directory on the FTP server. [Defect ID: 44686]

Fixed: Mcafee status on Configuration Summary page always shows disabled when locale is set to "Traditional Chinese"

Previously, the Mcafee status on the Configuration Summary page always showed disabled when the locale was set to "Traditional Chinese." This no longer occurs. Now, it correctly shows the status as either enabled or disabled. [Defect ID: 44798]

Fixed: Upstream proxy servers erroneously considered offline in some cases

Previously, upstream proxy servers were erroneously considered offline when the Web Proxy decrypted a request and failed the HTTPS handshake with an HTTPS server. This no longer occurs. [Defect ID: 46399]

Fixed: Web interface shows a misleading error message when the "Redirect Hostname" field is left blank

Previously, the web interface showed a misleading error message when the "Redirect Hostname" field was left blank. This no longer occurs. Now, the error message says "The value cannot be blank."' [Defect ID: 47042]

Fixed: Multiple entries for alternate DNS servers disappears from the web interface

Previously, when you added multiple entries for a alternate DNS servers and then edited the DNS server settings again, the second entry for the same domain disappeared from the web interface. This no longer occurs. Now, all entries remain. [Defect ID: 47430]

Fixed: testauthconfig CLI command fails for NTLM authentication realms in some cases

Previously, the `testauthconfig` CLI command failed when an NTLM authentication realm was created and deleted, and then a new NTLM authentication realm was created with a domain name that was a substring of the previous domain name. This no longer occurs. [Defect ID: 47431]

Fixed: Web Proxy erroneously sends "403 Unauthorized" instead of "403 Forbidden" when blocking sites

Previously, the Web Proxy erroneously sent "403 Unauthorized" instead of "403 Forbidden" when blocking sites. This no longer occurs. Now, it correctly describes the 403 HTTP status code as "Forbidden." [Defect ID: 47756]

Fixed: Policy trace with authentication fails when authentication realm name contains a space

Previously, the policy trace feature failed when it used authentication and the authentication realm name contained a space. This no longer occurs. [Defect ID: 47834]

Fixed: FTP PUT command fails using FTP over HTTP when using the CWD command

Previously, the PUT method using FTP over HTTP failed with certain FTP servers. This no longer occurs. [Defect ID: 47880]

Fixed: Changing the admin password on the Web Security appliance removes any SSH public key added

Previously, when you changed the admin password on the Web Security appliance in the web interface, the process removed any SSH public key added in the CLI. This no longer occurs. [Defect ID: 47906]

Fixed: Application fault occurs in the web interface when creating a PDF of the Monitor > Anti-Malware page

Previously, an application fault occurred in the web interface when creating a PDF of the Monitor > Anti-Malware page using the "Printable (PDF)" link. This no longer occurs. [Defect ID: 47972]

Fixed: An application fault occurs in the web interface when navigating to the Network > Authentication page using a Japanese locale

Previously, an application fault occurred in the web interface when navigating to the Network > Authentication page using a Japanese locale. This no longer occurs. [Defect ID: 46058]

Fixed: logconfig CLI command gives a misleading error message when entering in invalid value

Previously, when you used the `logconfig` CLI command to change the Log Rollover Interval to a value greater than 12 days, such as 13 days ("13d"), it returned a misleading error message saying the value cannot exceed "1,000,000." This no longer occurs. Now, the error message very clearly states what values are allowed and not allowed. The Log Rollover Interval still cannot exceed 12 days. [Defect ID: 47488]

Fixed: FTP transfers fail when the FTP transfer type is included in the URL

Previously, FTP transfers failed when the FTP transfer type was included in the URL. This no longer occurs. [Defect ID: 40265]

Fixed: Some web pages do not open after requesting a web page from a buggy web server in some cases

Previously, when a user opened a web page from a buggy web server using the Authorization header and then navigated to a different website using the same browser session, the other website did not open. This no longer occurs. [Defect ID: 45584]

Fixed: End-user notification pages do not display correctly because they do not contain UTF-8 encoding information

Previously, end-user notification pages did not display correctly because they did not contain UTF-8 encoding information. Some non-7-bit ASCII characters did not display. This no longer occurs. [Defect ID: 32009]

Fixed: webcache CLI command allows duplicate entries

Previously, the `webcache` CLI command allowed users to enter duplicate entries. This no longer occurs. [Defect ID: 34493]

Fixed: Range requests use too much bandwidth in some cases

Previously, range requests used too much bandwidth when the request was served from the destination server instead of the web cache. This happened because the Web Proxy downloaded more bytes from the server than was specified in the range request. This no longer occurs. [Defect ID: 39944]

Fixed: SNMP service is disabled after upgrading

Previously, after you upgraded to the latest version of AsyncOS, the SNMP service was disabled if it was enabled before upgrading. This no longer occurs. [Defect ID: 41927]

Fixed: Incorrect value shown for Bandwidth Used in reports

Previously, an incorrect large negative value was shown for the "Bandwidth Used" field in some reports. This no longer occurs. [Defect ID: 42431]

Fixed: Web interface erroneously allows proxy group names with the underscore (_) character

Previously, when creating a proxy group, the web interface erroneously allowed you to include the underscore (_) character in proxy group name. This no longer occurs. [Defect ID: 42485]

Fixed: Some applications have difficulty downloading access logs from the Web Security appliance

Previously, some applications, such as Webspy Vantage, have difficulty downloading access logs from the Web Security appliance. This no longer occurs. [Defect ID: 42632]

Fixed: Loading a configuration file using the loadconfig CLI command fails when a string parameter contains certain characters

Previously, loading a configuration file using the `loadconfig` CLI command failed when a string parameter contained the following characters:

```
< > /
```

This no longer occurs. [Defect ID: 42891]

Fixed: A 502 "Bad Gateway" error is erroneously displayed instead of a 504 "Gateway Timeout" error for HTTPS transactions in some cases

Previously, when an HTTPS server times out a decrypted HTTPS session, the Web Proxy displayed 502 "Bad Gateway" instead of 504 "Gateway Timeout. This no longer occurs. [Defect ID: 42913]

Fixed: Web interface erroneously displays Active Directory distribution groups

Previously, the web interface erroneously displayed Active Directory distribution groups when it looked up Active Directory groups in a policy group. This no longer occurs. [Defect ID: 42943]

Fixed: An application fault intermittently occurs in the L4 Traffic Monitor

Previously, an application fault intermittently occurred in the L4 Traffic Monitor. This no longer occurs. [Defect ID: 43574]

Fixed: The log rollover interval setting for a log subscription is removed after editing the log subscription in the web interface

Previously, the log rollover interval setting for a log subscription was removed after editing the log subscription in the web interface. This no longer occurs. [Defect ID: 43787]

Fixed: dnsconfig CLI command erroneously only allows one IP address for an alternate DNS server

Previously, the `dnsconfig` CLI command erroneously only allowed one IP address for one set of domains. This no longer occurs. Now, when you configure alternate DNS servers using

the `dnsconfig` command, it allows you to configure multiple IP addresses for one set of domains. [Defect ID: 43852]

Fixed: Web Proxy generates a core file when downloading very large files with no Content-Length header

Previously, the Web Proxy generated a core file when downloading very large files with no Content-Length header. This no longer occurs. [Defect ID: 44026]

Fixed: All CONNECT requests are blocked when access policies block HTTPS

Previously, all CONNECT requests were blocked when access policies blocked HTTPS. This no longer occurs. Now, only HTTPS requests are blocked. [Defect ID: 44197]

Fixed: HTTPS connections break when client certificates are required when the Web Security appliance is deployed in transparent mode

Previously, HTTPS connections broke when client certificates were required by the HTTPS server when the Web Security appliance was deployed in transparent mode. This no longer occurs. [Defect ID: 44706]

Fixed: SCP Push method does not work when the log file name or directory contains a space

Previously, SCP Push method did not work when the log file name or directory contained a space. This no longer occurs. [Defect ID: 44810]

Fixed: Traceback occurs and the user is logged out when using the setgateway CLI command

Previously, when users implemented the `setgateway` CLI command, they received an error, were logged out of the CLI, and a tracebook occurred. This no longer occurs. [Defect ID: 44940, 47008]

Fixed: Web interface is slow displaying the Identities page when there are more than 20 identity groups

Previously, the web interface was slow displaying the Identities page when there were more than 20 identity groups. This no longer occurs. [Defect ID: 45124]

Fixed: Russian characters are not displayed in the web interface when viewing authentication groups

Previously, Russian characters did not display in the web interface when viewing authentication groups. This no longer occurs. [Defect ID: 45279]

Fixed: Authentication is bypassed for HTTPS sites when using cookie authentication surrogates

Previously, authentication was bypassed for HTTPS sites when using cookie based authentication surrogates. This no longer occurs. Now, when using cookie surrogates and

explicitly accessing an HTTPS website (or using an explicitly forwarded CONNECT request), the Web Proxy replies to the client with a 407 HTTP response "Proxy Authentication Required." This status informs the client that it must supply valid authentication credentials to access the server. [Defect ID: 45285]

Fixed: Access logs show authentication sequence name instead of the authentication realm name when the identity uses the All Realms sequence

Previously, the access logs showed the user's authentication sequence name instead of the authentication realm name when the identity used the All Realms sequence. This no longer occurs. [Defect ID: 45289]

Fixed: AsyncOS for Web sends a misleading response when a browser requests the PAC file stored on the appliance in some cases

Previously, when a web browser had a copy of the PAC file hosted on the Web Security appliance and then sent an If-Modified-Since request to the appliance for the PAC file, AsyncOS for Web sent 304 "Not Modified" responses to the browser with a "Transfer-Encoding: chunked" header instead of a "Content-Length: 0" header. This no longer occurs. [Defect ID: 45445]

Fixed: Previously deleted authentication realm reappears after upgrade

Previously, previously deleted authentication realm reappeared after upgrade. This no longer occurs. [Defect ID: 45495]

Fixed: Web Security appliance MIB shows different value for CPU utilization than the web interface

Previously, when using the Web Security appliance MIB to view the CPU utilization, the value in the MIB was different than the value shown on the Monitor > System Status page in the web interface. This no longer occurs. [Defect ID: 45638]

Fixed: NTLM users are blocked after changing the NTLM authentication realm name

Previously, when an access policy used an identity that used an NTLM authentication realm that changed name, users that matched that access policy were blocked because the access policy did not show the new NTLM authentication realm name. This no longer occurs. [Defect ID: 45652]

Fixed: An application fault occurs in the Web Reputation Filters causing the filters to stop working after accessing a buggy website

Previously, an application fault occurred in the Web Reputation Filters causing the filters to stop working after accessing a buggy website. This no longer occurs. [Defect ID: 45699]

Fixed: Files get truncated when uploaded in a CONNECT tunnel using FTP

Previously, files were truncated when they were uploaded in a CONNECT tunnel using FTP. This no longer occurs. [Defect ID: 45703]

Fixed: Web Security appliance spontaneously reboots due to a slow memory leak when using NTLM authentication in some cases

Previously, the Web Security appliance spontaneously rebooted due to a slow memory leak when using NTLM authentication. This no longer occurs. [Defect ID: 45765]

Fixed: WMA files are not blocked in some cases

Previously, WMA files were not blocked when the Content-Type header contained the wrong value. This no longer occurs. [Defect ID: 45767]

Fixed: Web Proxy cannot communicate with upstream proxy servers in some cases

Previously, when the Web Proxy was deployed in transparent mode and IP spoofing was enabled, it could not communicate with upstream proxy servers when the upstream proxy server did not use port 80 or 3128. This no longer occurs. [Defect ID: 45854]

Fixed: Deleting custom URL categories does not remove them from the Web Security Manager > Access Policies page

Previously, when a custom URL category was deleted, it still was counted and listed in the total count of URL categories on the Web Security Manager > Access Policies page. This no longer occurs. [Defect ID: 46202, 46970]

Fixed: Scheduled WBRS report generates an email with an error message instead of the report content

Previously, a Scheduled WBRS report generated an email with an error message instead of the report content itself. This no longer occurs. [Defect ID: 46214]

Fixed: Web Proxy uses the Proxy-Connection header instead of the Connection header, causing problems with some user agents

Previously, the Web Proxy used the Proxy-Connection header instead of the Connection header when communicating with user agents with explicit forward requests. Because of this, some user agents, such as Real Player, did not work as expected. This no longer occurs. Now, the Web Proxy replies to the client using the Connection header in addition to the Proxy-Connection header. [Defect ID: 46515]

Fixed: Web Proxy in transparent mode does not include the port in the URI when forwarding requests to an upstream proxy

Previously, when Web Proxy was deployed in transparent mode, it did not include the port in the URI when forwarding requests to an upstream proxy. This no longer occurs. [Defect ID: 46783]

Fixed: An application fault occurs in the web interface on the Web Security Manager > Access Policies page after upgrading

Previously, an application fault occurred in the web interface on the Web Security Manager > Access Policies page after upgrading to AsyncOS for Web 5.6.2. This no longer occurs. [Defect ID: 47365]

Fixed: Access logs do not log policies correctly when using custom URL categories in some cases

Previously, the access logs showed the wrong policy names when two custom URL categories existed with the same URL in each, and two identities existed using each custom URL category. This no longer occurs. Now, the access logs show the correct identity and custom URL category for each transaction. [Defect ID: 41992]

Fixed: Upgrading loses language setting for end-user notification pages

Previously, when you upgraded to the latest version of AsyncOS, the language setting for end-user notification pages defaulted to English depending on the previous version of AsyncOS. This no longer occurs. [Defect ID: 44433]

Fixed: Access policy application settings erroneously list HTTPS as a blocked protocol when HTTPS scanning is enabled in some cases

Access policy application settings erroneously listed HTTPS as a blocked protocol when HTTPS scanning was enabled in some cases. This no longer occurs. [Defect ID: 43009]

Fixed: CLI allows you to create multiple duplicate access log subscriptions

Previously, the command line interface (CLI) allowed you to create multiple access log subscriptions even though each one was identical to the others. The web interface only allowed you to create one access log subscription. This no longer occurs. Now, you can create multiple access logs in the CLI and the web interface. However, IronPort recommends creating only one access log subscriptions for performance reasons. [Defect ID: 43123]

Fixed: Web Proxy spoofs client IP address for explicit forward requests when deployed in transparent mode

Previously, when the Web Security appliance was deployed in transparent mode with IP spoofing enabled and a client explicitly forwarded a request to the appliance, the Web Proxy always used the client source IP address for the request instead of using the appliance IP address. This no longer occurs. Now you can configure whether or not to spoof the client source IP address for explicitly forwarded connections. By default, the Web Proxy spoofs the client source IP address for transparent connections only. [Defect ID: 38637, 30914]

KNOWN ISSUES AND LIMITATIONS

Certificate and key for web interface is lost after loading a configuration in some cases

When you upload a certificate and key for the web interface using the `fipsconfig > certconfig` CLI command, then save the appliance configuration, and load the configuration, the previously uploaded certificate and key are lost. Instead, the appliance uses the "IronPort Appliance FIPS Demo Certificate."

Workaround: Upload the desired certificate and key again. [Defect ID: 72541]

NTLM authentication fails after a period of time when a policy group uses many authorization groups

NTLM authentication fails after a period of time when a policy group uses many authorization groups from an NTLM authentication realm, such as over 100 groups. When the list of all group IDs approaches 2 KB, an internal process starts to leak memory and fails to authenticate users against the Active Directory server. [Defect ID: 44445]

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. [Defect ID: 66309]

Some DNS related CLI commands do not have any effect

The following `advancedproxyconfig > DNS` CLI commands do not have any effect:

- 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 currently ignores the values you enter for these commands and applies the default values used by the DNS server configured. [Defect ID: 55329]

WCCP Module Logs contain no information

The WCCP Module Logs contain no information.

Workaround: Read the Default Web Proxy Logs and search for the string "wccp" for information related to WCCP. [Defect ID: 56254]

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. [Defect ID: 56418]

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. [Defect ID: 67460]

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>
```

[Defect ID: 56116]

Erroneous error message when deleting a route that does not exist on the Web Security appliance

When deleting a route that does not exist on the Web Security appliance, the System Logs show 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

You can ignore this message. [Defect ID: 41304]

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. [Defect ID: 51433]

Web Security appliance sends HTTPS transactions to external DLP servers in obscure format

The Web Security appliance sends HTTPS transactions to external DLP servers in a format that does not make it clear it is an HTTPS transaction instead of HTTP. Instead of sending HTTPS transactions as "https://*uri*" it sends them as the URI only. This may cause some DLP vendors,

such as Vontu, to incorrect identify the transaction as HTTP instead of HTTPS. [Defect ID: 52556]

Very large native FTP downloads appear in the access logs as "Scanning Error" when McAfee is enabled

The access logs display "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.

The file downloads successfully. You can ignore the scanning error value in the access logs. [Defect ID: 54571]

Cannot compress access logs using the web interface

The web interface does not allow you to compress the access log subscription. It allows you to compress other log subscriptions.

Workaround: Use the `logconfig` CLI command to compress the access logs. [Defect ID: 54683]

Web interface cannot load authentication groups from Lotus Domino Server

The web interface cannot load authentication groups from Lotus Domino Server. As a result, the Test Authentication feature for the LDAP authentication realm gives an error when group authentication is configured, and when creating non-Identity policies, no LDAP groups are displayed. However, group authentication with Lotus Domino Server works as expected.

Workaround: When creating non-Identity policies, manually enter user groups where necessary. [Defect ID: 54884]

Access logs erroneously show a 4 GB FTP file download in some cases

The access logs erroneously show a 4 GB FTP file download when a user tries to use FTP to download a non-existent file. You can ignore the file object size in the access logs. [Defect ID: 54891]

Web interface erroneously allows underscores (_) in authentication realm and sequence names

Web interface erroneously allows underscore characters (_) in authentication realm and sequence names. Because AsyncOS for Web stores the authentication realm and sequence names with spaces using underscores, this erroneously allows you to create two authentication realms or sequences with the same name.

Workaround: Do not use underscore characters in authentication realm and sequence names. [Defect ID: 55087]

Cannot join Active Directory domain after changing Web Security appliance hostname in some cases

Joining the Active Directory domain does not work under the following circumstances:

- 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 uses the previous hostname to try and join the domain, so the Computer Account creation fails again.

Workaround: Reboot the Web Security appliance. [Defect ID: 55350]

Policy trace feature does not work when accessing servers that require the User-Agent HTTP header

The policy trace feature does not work when accessing servers that require the User-Agent HTTP header. Instead, it reports a gateway timeout error. [Defect ID: 55628]

Access policies show incorrect value for "HTTP/HTTPS Max Download Size" setting in some cases

Access policies show the incorrect value for the "HTTP/HTTPS Max Download Size" setting when it uses the global policy values for the Object settings and the Global Access policy is configured for a value other than the default value. However, the Access Policies block transactions appropriately as configured in the Global Access policy.

Workaround: Ignore the value displayed in the user defined Access Policy and instead look at the value displayed for the Global Access policy. [Defect ID: 55634]

Date and time custom format specifiers (%v and %V) do not work

The date (%v) and time (%V) custom format specifiers do not work. When these are added to an access log subscription, no date or time values are displayed in the access log file. [Defect ID: 55731]

LDAP searches do not work in some cases

LDAP searches do not work when AsyncOS uses old LDAP connections that do not have sufficient privileges. [Defect ID: 50706]

Application fault occurs in the web interface when accessing the Network > Internal SMTP Relay page in some cases

An application fault occurs in the web interface when accessing the Network > Internal SMTP Relay page if the SMTP relay is configured to use a deleted network interface.

Workaround: Use the `smtprelay` CLI command to configure an SMTP relay host. [Defect ID: 51811]

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. [Defect ID: 51514]

Incorrect response size value recorded in the access logs for FTP over HTTP transactions when the transaction times out

An incorrect response size value is recorded in the access logs for FTP over HTTP transactions when the transaction times out. The value should be zero (0) for the response size when a transaction times out, but instead, the value appears as a large positive or negative number. You can ignore the value stored in the access logs for the response size. [Defect ID: 51822]

Web Proxy erroneously adds its domain name as a DNS search domain in some cases

When a client explicitly forwards a request for a URL that does not exist, the Web Proxy appends its own name domain to the URL and tries the DNS lookup again. For example, the Web Security appliance host name is wsa.example.com, and a client sends a request to http://myhost.mysite. The original DNS lookup fails to find http://myhost.mysite, so the Web Proxy tries another DNS lookup for http://myhost.mysite.example.com.

Workaround: Configure the appliance to use transparent mode and transparently redirect client requests to the Web Proxy. [Defect ID: 51864]

Changing the name of the Web Security appliance host name does not take effect immediately

Changing the name of the Web Security appliance host name does not take effect immediately.

Workaround: Restart AsyncOS for Web, or contact Customer Support to restart the Web Proxy only. [Defect ID: 51933]

Changing the default gateway does not display the new IP address in the web interface immediately

When you change the default gateway and click **Submit**, the Network > Routes page does not immediately display the new IP address for the default gateway after clicking **Submit**.

Workaround: Reload the page in the browser and the correct default gateway address appears. [Defect ID: 52022]

Cannot enter text in some Identity fields using Safari 4.0.x

When you use the Safari browser version 4.0.x to access the web interface, you cannot enter text in the Description or Define Members by Subnet fields for Identity groups under the following circumstances:

- Create an Identity and leave the Description or Define Members by Subnet fields empty. Submit and commit the changes.
- Disable the Identity, and commit the changes.
- Enable the Identity. You cannot enter text into the Description or Define Members by Subnet fields.

Workaround: Resize the Description or Define Members by Subnet fields, and then enter text into either field. [Defect ID: 52184]

Web interface does not display all uploaded PAC files in some cases

Uploaded PAC files are not listed in the PAC Files Hosted field on the Security Services > PAC File Hosting page in view mode.

Workaround: Click **Edit Settings** and the Web Interface displays all uploaded PAC Files. [Defect ID: 52487]

Updates and upgrades do not work due to incorrect routing tables configured after upgrading from AsyncOS for Web 5.6.4

After upgrading from AsyncOS for Web 5.6.4, the Routing Table for AsyncOS update and upgrade settings is 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 causes updates and upgrades to not work.

Workaround: On the System Administration > Upgrade and Update Settings page, configure the Routing Table setting to use "Management." [Defect ID: 52509]

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. [Defect ID: 50632]

Access logs erroneously display a negative value for the custom format specifier %q in some cases

The access logs erroneously display a negative value for the custom format specifier %q for uploads greater than 2 GB. [Defect ID: 53866]

Web Proxy generates a core when uploading 2 GB files with external DLP enabled in some cases

The Web Proxy generates a core when uploading 2 GB files with external DLP enabled using Vontu Web Prevent version 9. [Defect ID: 53867]

Not all data is uploaded with external DLP enabled in some cases

When uploading a 2 GB file with external DLP enabled, not all data is uploaded to the server when the external DLP server is Vontu Web Prevent version 9. [Defect ID: 53868, 53869, 53870]

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. [Defect ID: 49335]

Web interface erroneously allows some invalid regular expressions in some cases

Web interface erroneously allows some invalid regular expressions when defining custom URL categories. 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 *IronPort AsyncOS for Web User Guide*. [Defect ID: 51315]

End-user URL category warning page hypertext link does not work with virtual IP addresses in some cases

The end-user URL category warning page hypertext link sometimes erroneously uses the Web Security appliance's IP address instead of the hostname. When clients on the network access the appliance using a virtual IP address, the hypertext link in the warning page does not work. [Defect ID: 51440]

Web Proxy generates a core file when changing the IP Spoofing setting when FTP downloads are occurring

The Web Proxy generates a core file when a user is downloading a file using FTP and an administrator changes the IP Spoofing setting on the Security Services > Proxy Settings page from "For All Connections" to "For Transparent Connections Only." [Defect ID: 50971]

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. [Defect ID: 50219, 50995]

Upgrading from a previous version removes the certificate and key pair uploaded for credential encryption

If credential encryption (also known as "secure client authentication") was enabled in a previous version and then you upgrade AsyncOS for Web to the current version, any certificate and key pair previously uploaded for credential encryption is removed. [Defect ID: 50652]

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. [Defect ID: 49505]

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.

[Defect ID: 49677]

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. [Defect ID: 46555]

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. [Defect ID: 48675]

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. [Defect ID: 48963]

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. [Defect ID: 49152]

Timestamp field in the Data Security Logs shows time in GMT instead of local timezone

The timestamp field in the Data Security Logs shows time in the Greenwich Mean Time (GMT) timezone instead of the Web Security appliance local timezone. [Defect ID: 49501]

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. [Defect ID: 49593]

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. [Defect ID: 48378]

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. [Defect ID: 45760]

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. [Defect ID: 44023]

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. [Defect ID: 46044]

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. [Defect ID: 46430]

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. [Defect ID: 47184]

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. [Defect ID: 44031]

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. [Defect ID: 44071]

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. [Defect ID: 44089]

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. [Defect ID: 39947]

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." [Defect ID: 40872]

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. [Defect ID: 41942]

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. [Defect ID: 41568]

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. [Defect ID: 42584]

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*. [Defect ID: 42806]

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. [Defect ID: 39570]

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. [Defect ID: 37455]

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. [Defect ID: 40363]

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

[Defect ID: 39853]

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. [Defect ID: 39221]

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. [Defect ID: 39247]

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: 39001]

Opera does not pass NTLM authentication credentials after an NTLMSSP_CHALLENGE response from HTTPS servers

When an HTTPS server sends an NTLMSSP_CHALLENGE response to an Opera web browser, Opera does not send the NTLM authentication credentials. [Defect ID: 38821]

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. [Defect ID: 35652]

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. [Defect ID: 38468]

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. [Defect ID: 40097, 34159]

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. [Defect ID: 36280]

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. [Defect ID: 36229]

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. [Defect ID: 33285]

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. [Defect ID: 34405]

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). [Defect ID: 34496]

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. [Defect ID: 36151]

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.

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. [Defect ID: 29133]

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." [Defect ID: 30255]

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. [Defect ID: 32114]

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. [Defect ID: 29868]

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. [Defect IDs: 25069, 28629, 31966]

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. [Defect ID: 37384, 26979, 23483, 23480]

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. [Defect ID: 27887]

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. [Defect ID: 28821]

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. [Defect ID: 28958]

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.

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. [Defect ID: 30703]

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. [Defect ID: 31935]

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. [Defect ID: 32127]

CONTACTING IRONPORT CUSTOMER SUPPORT

If you have purchased support directly from IronPort, you can request our support by phone, email or online 24 hours a day, 7 days a week. During our office hours (24 hours per day, Monday through Friday excluding U.S. holidays), one of our engineers will contact you within an hour of your request.

To report a critical issue that requires urgent assistance outside of our office hours, use the following contact information:

Toll-Free Customer Support: 1-877-641-IRON (4766)
International: `http://www.ironport.com/support/contact_support.html`
Support Portal: `http://www.ironport.com/support`