Release Notes for Cisco IronPort AsyncOS 7.7.5 for Web

Published: November 7, 2013

Revised: January 7, 2014

Contents

Cisco Systems, Inc.
www.cisco.com

What's New in Cisco IronPort AsyncOS 7.7.5 for Web

Table 1 New Features in Cisco AsyncOS for Web Security 7.7.5

Feature	Description
New Features:	
Cisco Web Security Virtual Appliance	Cisco offers the Cisco Web Security appliance as a virtual machine that you can host on your own network. The virtual appliance requires a separate license for the virtual appliance purchased from Cisco and a Cisco UCS Server (Blade or Rack-Mounted) hardware platform running VMware ESXi. The *Cisco Content Security Virtual Appliance Installation Guide* includes more information on the requirements for the virtual appliance. The new Web Security virtual appliance models and configurations are: • S000V (250 GB disk space, 50 GB cache space, 1 core, 4 GB memory) • S100V (250 GB disk space, 50 GB cache space, 2 cores, 6 GB memory) • S300V (1024 GB disk space, 200 GB cache space, 4 cores, 8 GB memory) This feature includes the following changes to AsyncOs for Web: • The Web Security virtual appliance license allows you to clone and run multiple virtual appliances on your network. • The `loadlicense` CLI command for installing the virtual appliance license. You can use the same license for multiple virtual appliances. • Feature keys are included as part of the virtual appliance license. The feature keys will expire at the same time as the license. Purchasing new feature keys will require downloading and installing a new virtual appliance license. • Due to feature keys being included in the virtual appliance license, there are no 30-day evaluations for AsyncOS features. • You cannot open a Technical Support tunnel before installing the virtual appliance license. • The `version`, `ipcheck`, and `supportrequest` CLI commands have also been updated to included virtual appliance information. • There are new alerts and logs for misconfigured virtual appliances.

What's New in Cisco IronPort AsyncOS 7.7.0 for Web

Table 2 New Features for AsyncOS 7.7 for Web

Feature	Description
New Features	
Multi-Forest NTLM	Configure the Web Security Appliance to authenticate users from Multiple untrusted NTLM realms. Sometimes creating trust relationships between distinct NTLM realms is not practical. You can now support these configurations using the same WSA without expending the cost and effort associated with enabling NTLM trust. Authenticate users from multiple NTLM realms if those realms posses a trust relationship. Create multiple identity policies using these untrusted NTLM realms and then configure user and group policies associated with these identities. See Authenticating Users Against Multiple Active Directory Domains in the user guide or online help.
Software-based FIPS Level 1 Compliance	The Federal Information Processing Standard (FIPS) 140-2 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. With AsyncOS 7.7 for Web, FIPS 140-2 Level 1 compliance can be enabled via a few simple steps in the Web Security Appliance GUI. This feature utilizes the Cisco Common Crypto Module (C3M) rather than the previously used Hardware Security Module (HSM) for all cryptographic operations and it will be available via AsyncOS 7.7 for Web running on all currently supported hardware models. See FIPS Compliance in the user guide or online help.
SOCKS Proxy	Support for SOCKS-based applications, including Bloomberg Terminals. Define SOCKS-specific user and group policies as well as specific TCP and UDP destination ports. SOCKS logs and reports allow you to track and analyze SOCKS proxy usage. See Overview of SOCKS Proxy Services in the user guide or online help.
Custom Header Insertion	Insert custom request headers. Certain websites such as YouTube for Schools require that web requests to their domains be appended with customized header strings. In the case of YouTube for Schools, an account-specific string must be sent with each request to YouTube's domains so that YouTube can recognize users from a Schools account and serve content accordingly. This function allows you to utilize the CLI to specify the custom header string and the domains for which requests will be appended. See "Custom Headers" in the in the user guide or online help.
OCSP	Use the Online Certificate Status Protocol (OCSP) to provide revocation status updates for X.509 certificates. OCSP provides a more timely means of validation for certificates than the alternative Certificate Revocation Lists (CRL). Currently, the administrator can configure the invalid certificate handling policies under the HTTPS Proxy page. Enable/disable OCSP and configure new OCSP policies using the Web UI. Configure timeout values, and select a configured upstream proxy group. Configure a list of exempt servers that WSA will connect to directly without using the upstream proxy. See Enabling Real-Time Revocation Status Checking in the user guide or online help.

Table 2 New Features for AsyncOS 7.7 for Web (continued)

Feature	Description
Certificate Trust Store Management	Greater management control of certificates and certificate authorities. View all of the Cisco-bundled certificates, remove trust of any Cisco-trusted root certificate authorities, and view the Cisco-published blacklist. This will provide more flexibility in making your own decisions with regards to acceptable and unacceptable certificates used by the WSA. Within the Web UI, import your own trusted certificates and add them to the trusted root certificate list. View current Cisco-trusted root certificates and select an option to override each individual certificate, removing trust by the WSA for that certificate. View Cisco's intermediate certificate blacklist. Due to real-life incidents where certain intermediate CA's were compromised, the WSA was given a hard-coded list of blacklisted intermediate certificates that was previously transparent to administrators. This now becomes a viewable list. See Adding Certificates to the Trusted List and Removing Certificates from the Trusted List in the user guide or online help.
Encrypted Private Keys	Use encrypted, password-protected private keys. Upload encrypted private keys and provide a password for the WSA to decrypt them. The WSA then stores these private keys by obfuscating/encrypting them with a password that is unknown to the user. When configurations are exported to a file, private keys remain obfuscated and unreadable to the user. The WSA can decrypt them when the configuration is loaded onto a WSA. See Uploading a Root Certificate and Key in the user guide or online help.
Enhancements	
SNI extension for Transparent SSL Handshake	Access the Server Name Indication (SNI) extension to parse the destination server name. This is useful when making requests to virtual servers hosting multiple HTTPS websites such as youtube.com and google.com. [Defect Number: 74969, CSCzv50011]

Upgrade Paths

You can upgrade to AsyncOS 7.7.5-194 from the following version:

- 7.7.5-190

Installation and Upgrade Notes

Compatible Hardware

This release runs only on virtual appliances as described in Cisco UCS Servers and VMware ESXi 4.x and 5.0, page 5. It does not run on any S-Series physical hardware appliance.

Configuration Files

AsyncOS for Web 7.7.5 does not directly support backward compatibility with configuration files from previous versions of AsyncOS for Web, such as 7.5.1 or 7.7.0.

However, a Configuration Migration Tool is available to convert a configuration file from select versions of AsyncOS into a new file that can be uploaded to a virtual appliance.

For details, see the *Release Notes for the Configuration Migration Tool for Cisco Content Security Virtual Appliances* at http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html.

Essential Cisco Web Security Virtual Appliance Installation Instructions

Instructions for installing the Cisco Web Security virtual appliance are available in the *Cisco Content Security Virtual Appliance Installation Guide* at http://www.cisco.com/en/US/products/ps10164/prod_installation_guides_list.html.

Note It is extremely important to configure time and synchronization settings on your virtual machine in order to prevent random failures on your Cisco Web Security Virtual Appliance. Specific instructions are in the "Important! Preventing Random Failures" section of the Install Guide and must be followed precisely.

Cisco UCS Servers and VMware ESXi 4.x and 5.0

Cisco UCS servers (blade or rack-mounted) are the only supported hardware platform for the virtual appliance. **VMware ESXi version 4.x and 5.0** are the only supported virtualization hypervisors. Any other hardware platform or VMware hypervisor will be supported on a "Best Effort" basis: we will try to help you, but it may not be possible to reproduce all problems, and we cannot guarantee a solution. No other virtualization hypervisor is supported.

Cisco recommends that the server hosting your virtual appliances have the minimum requirement of two 64-bit x86 processors of at least 1.5 GHz each, 8 GB of physical RAM, and a 10k RPM SAS hard drive disk.

VMware ESXi 4 File System Settings

VMware ESXi version 4.x comes with a file system that has a default block-size of 4 MB, which supports a virtual disk image of up to 1 TB. However, the larger Cisco virtual security appliances (e.g., S300V) require more than 1 TB of disk space. In order to run these models, you will need to create a new datastore and format it with an 8 MB or larger block size.

For information on block size and instructions on how to create a new datastore, seeVMware's technical documentation at http://kb.vmware.com/selfservice/microsites/search.do? .

Compatibility with IronPort AsyncOS for Cisco Content Security Management

Features on AsyncOS 7.7.5 for Web are supported by AsyncOS for Cisco Content Security Management version 8.0. Note that there is no virtual Cisco Security Management appliance.

Compatibility of this release with AsyncOS for Cisco Content Security Management releases is detailed in the Compatibility Matrix available from http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html.

Opening Support Cases Through the Appliance

When opening a support case using the appliance, the severity level is 3. Previously, users were able to set the severity level using the appliance, either through the CLI command, `supportrequest`, or through the GUI. To open a support case at a higher severity level, call Customer Support.

Defect: 87828, CSCzv13413; 87830, CSCzv25201

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.

Certificate Error Category Changes

Certificate error categories have changed:

Old Category	New Category	Description
Unrecognized Root Authority	Unrecognized Root Authority/Issuer	Either the root authority or an intermediate certificate authority is unrecognized.
—	Invalid Signing Certificate	There was a problem with the signing certificate, for example, a failure to verify or decrypt the signature. Previously, these errors were included in the “Other Error” category.
—	Invalid Leaf Certificate	There was a problem with the leaf certificate, for example, a rejection, decoding, or mismatch problem. Previously, these errors were included in the “Other Error” category.

Access Log Changes

Access logs now include these entries:

- FTP_CONNECT
- FTP_TUNNEL

See information about enhancements to the Native FTP Proxy in New Features for AsyncOS 7.7 for Web.

Logging and Reporting Changes

Logging Command Replaced with Web Interface Support

The **advancedproxyconfig > wccp** command has been removed, and more robust logging is now available through the web interface. See defect number 85003 in Resolved Issues in Release 7.7.0, page 8.

Reporting and Tracking for SOCKS

New support for the SOCKS protocol includes a new SOCKS Proxy report and a new SOCKS Proxy tab in Web Tracking. Read about support for SOCKS Proxy in New Features for AsyncOS 7.7 for Web.

Upgrading AsyncOS for Web

Before You Begin

Save your configuration to a location off the appliance.

Step 1 On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.

Step 2 On the System Administration > System Upgrade page, click **Available Upgrades**.

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

Step 3 Click **Begin Upgrade** to start the upgrade process. Answer the questions as they appear.

Step 4 When the upgrade is complete, click **Reboot Now** to reboot the Web Security appliance.

Note To verify the browser loads the new online help content in the upgraded version of AsyncOS, you must exit the browser and then open it before viewing the online help. This clears the browser cache of any outdated content.

Resolved Issues

Resolved Issues in Release 7.7.5-194

Bug ID	Description
CSCug24726	Content rich sites slow on 7.7 when AS disabled & some AVC apps blocked
CSCug43789	PAC file hosting on port 80 does not work after upgrade to 7.7
CSCug74881	High bit characters in PAC file breaks GUI
CSCug87703	Proxy crashes on POST when using external DLP

Bug ID	Description
CSCui45649	Upload performance degrades on upgrading from 7.5.0
CSCzv03132	HTTP Response Header Last-Modified field uses UTC not GMT
CSCzv58669	WSA - Management GUI Denial of Service Vulnerability

Resolved Issues in Release 7.7.0

Previous Defect ID	Bug Toolkit ID	Description
90699	CSCzv79153	After uploading a custom root CA, AsyncOS did not recognize the uploaded certificate until the web proxy was restarted. This is fixed.
90467	CSCzv69205	AsyncOS was sending incorrect usernames to the FTP server when all of these conditions were met: • Authentication configured and enabled in Identities • Native FTP exempted from authentication • Username for FTP connection either included the backslash character (\) or it was used to escape a special character in the username. AsyncOS now provides a third formatting option to fix this defect.
88970	CSCzv25023	The login banner was failing to appear in the appliance GUI. This is fixed.
87864	CSCzv21851	Decryption failed when connecting to particular sites. This is fixed.
87643	CSCzv21222	When sending non-SSL traffic over SSL port 443, the web proxy sometimes ran out of memory and crashed or restarted. This is fixed.
87314	CSCzv97159	Users who had previously submitted authentication credentials were later unable to access HTTPS websites and were not prompted to authenticate. Conditions: • Decryption enabled • Authentication required • Transparent redirection • IP session caching This is fixed.
86556	CSCzv57040	The Appliance sometimes responded to an HTTPS file upload request with a 504 Gateway Timeout. Conditions: • The HTTPS proxy was enabled • The upload file included this header: "Transfer-encoding: chunked" This is fixed.
86549	CSCzv43726	Attempts to generate a Web Tracking report in PDF format resulted in an application fault if the report data included very long URLs. This is fixed.
86529	CSCzv94982	Time zone setting updates updated components unrelated to time zone.Clicking the **Update Now** button in the Time Zone File Updates section of the System Administration > Time Settings page updated all components (WBRS, Sophos, etc.), not just the time zone settings. This issue also occurred when using the **tzupdate** command in the CLI. This is fixed.

Previous Defect ID	Bug Toolkit ID	Description
86394	CSCzv59884	Using the **authcache - list** command was resulting in an application fault when the username included non-ascii characters. This is fixed.
86109	CSCzv21811	SSH 1 is an obsolete and nonsecular protocol and is no longer an option for SCP push on the Log Subscriptions page or in the CLI logconfig command. SSH2 is the default protocol.
85964	CSCzv91287	Download time for Web Tracking data in CSV format was excessive when specifying a custom time range for the report. This is fixed.
85383	CSCzv21238	Although support for Secure Sockets Layer (SSL) version 2 was removed from AsyncOS, client to proxy communication still allowed for SSL version 2. Client to proxy requests using SSL version 2 now fail, which is the expected behavior. This is fixed.
85085	CSCzv56404	The Status command was reporting incorrect system resource values. This is fixed.
84195	CSCzv73908	Transaction requests were sometimes resulting in HTTP 503 errors due to DNS caching problems. This is fixed.
83666	CSCzv68184	With Safe Search enabled, for URLs that included a question mark (?) in the first position after the domain name, for example, "example.com/?abc", transaction requests were resulting in an HTTP 404 error message. This is fixed.
83479	CSCzv78744	When the disk reported a high temperature, AsyncOS was sending out frequent, redundant alerts. This is fixed.
82946	CSCzv27807	Non-UTF-8 characters in transaction header fields were resulting in unnecessary UTF-8 errors on the appliance. This is fixed.
82857	CSCzv85035	External authentication failed with a Juniper SBR RADIUS server when RADIUS users were mapped to different Web Security appliance user role types using a RADIUS CLASS attribute. This is fixed.
82809	CSCzv44630	Host Header spoofing in HTTP and HTTPS Requests was not prevented. Now, there is a CLI option in `adminaccessconfig` to allow only hostnames/IP addresses of existing interfaces. This allows restricting specific machines to a specific domain name. By default, this option is disabled.
82780	CSCzv58956	Expired certificates were sometimes not detected by the appliance due to the order in which AsyncOS checked for errors and different actions assigned to different types of errors. AsyncOS now checks for all errors and applies the most restrictive action that applies.
82662	CSCzv27661	SNMP erroneously returned appliance information from the previous version of AsyncOS after upgrading. This is fixed.
82415	CSCzv95909	Large Objects were taking too long to load in some cases when the client made a universal range request. This is fixed.
81661	CSCzv78679	On Appliances using WebRoot scanning, requests for web pages that included javascript were sometimes taking too long. This is fixed.
81156	CSCzv95258	Attempting to navigate from Web Security Manager to the Outbound Malware Scanning page was, in rare cases, producing an application fault. This is fixed.
81055	CSCzv50828	Processing client requests sometimes took too long after updating new anti-malware rules.This is fixed.
77935	CSCzv40418	The Dynamic Content Analysis engine was erroneously overwriting the effective category used in policy decisions for new requests. This is fixed.
76250	CSCzv13897	Requires change to the user guide -- the new mask functionality. Network>Transparent Redirection> WCCP> Service > Advanced > Load Balancing.

Previous Defect ID	Bug Toolkit ID	Description
73467	CSCzv63552	Rebooting the appliance without proper shutdown sometimes caused irreparable damage to the appliance. This is fixed.
71012	CSCzv42816	**Fixed: Clients cannot connect to HTTPS servers that do not support TLS Hello during the SSL handshake.** Previously, clients could not connect to HTTPS servers that did not support TLS Hello during the SSL handshake. This is fixed.
70224	CSCzv66892	Added CLI command: date.
42512	CSCzv83549	**Fixed: Web Proxy cannot process server responses with extremely large HTTP headers** Previously, the Web Proxy could not process server responses with extremely large HTTP headers. This no longer occurs.

Known Issues

Known Issues in Release 7.7.5-194

Table 3 Known Issues for AsyncOS 7.7.5 for Web

Defect ID	Description
N/A	**Local Updates Currently Not Supported for Virtual Appliances** Currently, you cannot download a local update image from http://updates.ironport.com/fetch_manifest.html for your virtual appliance. The site does not accept the virtual license numbers that virtual appliances use in place of serial numbers
CSCzv91509	**Redundant Application Fault Alerts** AsyncOS sends redundant alerts about application faults when it is unable to connect to the Cisco Updater Servers or the servers are down. Workaround: Restore the connection to the Cisco Updater Servers, and run the **tzupdate force** command in the command line interface to force all updates.
CSCug25134	**Online Help Contains Incorrect Information on the S000V Appliance** The “What’s New” section of the AsyncOS for Web 7.7.5 online help incorrectly states that the S000V appliance is for evaluation purposes only. You can use the S000V appliance in production.

Known Issues in Release 7.7.0

Bug Toolkit ID	Description
CSCuf66424	**WSA reboots unexpectedly** when changing the default gateway for Management or Data interfaces This can occur whether using the CLI or Web interface. Cisco recommends taking the appliance out of production use before changing default gateways.
CSCuf34778	AsyncOS fails to proxy HTTP, HTTPS, FTP-Over-HTTP requests under these conditions: • Credential Encryption enabled AND • Basic authentication AND • Identity: All protocols, no surrogates, authentication required Workaround: "Edit" the Identity without actually changing it. Submit and commit.
CSCuf51391	AsyncOS allows the Security Management appliance to publish an Identity with SOCKS policies configured to the Web Security appliance when SOCKS is disabled on the Web Security appliance. Workaround: Match the SOCKS enabled/disabled setting on the Security Management appliance with those on the Web Security appliance.
CSCuf51729	Surrogate settings for Global Identity are disabled after publishing Configuration Master 7.7. This issue occurs when there is a mismatch in SOCKS proxy configurations on WSAs and SMA. Workaround: Disable/enable SOCKS Proxy on SMA to match settings on WSAs before publishing configurations.
CSCuf56258	An application fault occurs under these conditions: • On the SOCKS Policy Edit Page, a user selects Authorized Groups or Users AND • The SOCKS Policy is based on an Identity with custom or predefined URL Categories.
CSCuf85838	AsyncOS fails to decrypt HTTPS traffic from specific sites under these conditions: • The HTTPS Server asks for the client certificate AND • The Server Certificate is invalid AND • The appliance is configured to decrypt traffic when the server certificate is invalid AND • The appliance is configured to pass through traffic when the HTTPS Server asks for a client certificate. Workaround: Add the site to a custom URL category, and set the action to pass through.
CSCzv79284	For SOCKS UDP transactions, CPU usage may increase to 100% if DNS cannot resolve the domain name to a valid IP address.

Bug Toolkit ID	Description
CSCzv07140	AsyncOS fails to prevent the creation of invalid identities in under these conditions: • SOCKS Proxy is disabled on the Web Security appliance • SOCKS Proxy is enabled on the Security Management appliance • User creates a custom identity using the Security Management appliance that defines members based only on the SOCKS protocol. The custom identity is invalid.
CSCzv59181	The SCP push command fails with the message "invalid characters in scp command!" under these conditions: • scponly shell • filename includes the "@" character Workaround: Use a different shell to run the SCP push command.
CSCzv87357	SNMP - AsyncOS returns wrong interface speed (ifSpeed) value when Auto negotiation is used. Workaround: Set fixed speed and duplex values for affected interface using the command line interface: etherconfig>media>edit.
CSCzv95795	Rarely, AsyncOS stops performing normal operations. For example, it may stop logging activities, may stop accepting new connections, and it may not allow logins. Workaround: Reboot the appliance.
CSCzv87294	Attempt to send dig SSH command to TTY triggers a traceback. This issue occurs when including a dig command directly in the SSH login string. Workaround: Use -t in the string. For example: user1$ ssh -t admin@192.0.2.0 'dig @198.51.100.0 www.yahoo.com'
CSCzv84704	AsyncOS does not display End User Acknowledgements (EUAs) or End User Notifications (EUNs) that are larger than 16K. Workaround: Reduce the size of EUAs and EUNs to less than 16K.
CSCzv32093	When Adaptive Scanning is enabled, access logs that use the custom field %:<s provide an incorrect value for the time it takes to receive the verdict from the Web Proxy anti-spyware process.
CSCzv18801	Attempting to modify the time range for an access policy results in an application fault if Acceptable Use Control is disabled. Workaround: Enable Acceptable Use Control and then modify the time range for the Access Policy.
CSCzv87130	Creating a domain and then failing to join the domain causes a daemon to restart repeatedly, which results in repeated logging of the daemon restart event, which results in log files filling up and rolling over. Workaround: Either join the domain or delete the domain.
CSCzv27676	Attempt to join a domain fails if AsyncOS cannot resolve the name of the Active Directory server to which you are trying to connect, and the AsyncOS error message does not clearly identify the problem. Workaround: Add both the fully qualified domain name and the IP address for the Active Directory server to which you are trying to connect.

Bug Toolkit ID	Description
CSCzv39361	The index feature in online help for Cisco Security Appliances is not intuitive. As you type a term in the index field, the online help software highlights the first matching term in the list of index terms; pressing Enter does not take you directly to the related topic in the book. Instead it pops up an instruction to click on the highlighted term to go to the topic in the book. Workaround: In the list of index terms, click on a term to go to the related topic in the book.
CSCzv86403	With Transparent User Identification (TUI) and Active Directory agent, users who have recently authenticated may need to re-authenticate at frequent intervals.
CSCzv06278	The online help index does not work properly in Safari browsers. Searching the index results in a pop-up box that cannot be permanently dismissed using the Enter key. Workaround: Dismiss the pop-up box with a mouse click or use a different browser.
CSCzv86357	AsyncOS fails to authenticate users through LDAP if UTF-8 characters are used in the Bind DN or Base DN.
CSCzv58857	The SOCKS proxy does not support SaaS single sign-on. Workaround: Send SaaS traffic through the HTTP or HTTPS proxy.
CSCzv95175	Web interface stops responding after entering some regular expressions with trailing context patterns in a custom URL category. This is a known issue with the Flex, the application that AsyncOS for Web uses to analyze regular expressions. For more information on this limitation, go here: http://flex.sourceforge.net/manual/Limitations.html#Limitations
CSCzv03044	When the appliance is configured to warn end-users about explicit content, AsyncOS displays an End-User Notification warning about explicit content for sites that allow explicit content even if the site does not actually include explicit content. While this feature is working as designed, it may be a confusing outcome because the text in the web interface for the appliance implies that AsyncOS will only display an End-User Notification warning for explicit content if the site actually includes explicit content. In fact, end-users receive the warning if the site allows explicit content.
CSCzv46190	Attempting to delete a PAC file may result in misidentification of the file as the default PAC file. This can happen if the name of the default PAC file includes special characters. Workaround: Don't use special characters in PAC file names.
CSCzv17778	AsyncOS and some browsers determine the root CA for each site using different processes, which may result in discrepancies. Discrepancies may lead to unexpected results when attempting to black list sites.
CSCzv50704	Web Security appliance performance is affected when the Default Proxy Logs are configured at debug or trace logging level. Workaround: Change the logging level of the Default Proxy Logs to something higher than Debug, such as Information.
CSCzv36346	Running logconfig from the CLI and choosing 'Request Debug Logs' causes logging and reporting to fail.
CSCzv36740	Occasionally, network traffic moves faster than AsyncOS can accept the packets, and the network adapter drops some packets.

Bug Toolkit ID	Description
CSCzv56650	Overriding the application type bandwidth limit for a particular application does not work . When you define a bandwidth limit for an application type and then override that limit by choosing no bandwidth for a particular application in that application type, the Web Proxy erroneously still applies the defined bandwidth limits to the application.
CSCzv69285	In deployments using WCCP, users who exceed the maximum number of entries allowed for Ports to Proxy experience failures with IPFW rules and do not receive an alert from the appliance. The maximum number of port entries is 30 for HTTP, HTTPS, and FTP ports combined. Workaround: Reduce the number of port entries to fewer than 30 for HTTP, HTTPS, and FTP ports combined.
CSCzv60471	Certain browsers, including Firefox version 3 and Internet Explorer version 8, may display their native error page instead of displaying the End-User Acknowledgement or End-User Notification page configured through the appliance. Conditions: • Protocol is HTTPS • Decryption is not enabled on the appliance. Workaround: Enable decryption.

Finding Current Information about Known and Fixed Issues

Use the Cisco Bug Search Tool to find the most current information about known and fixed defects in shipping releases.

Before You Begin

Register for a Cisco account if you do not have one. Go to https://tools.cisco.com/RPF/register/register.do.

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 Log in with your Cisco account credentials.

Step 3 Enter search criteria.

For example, search for “Cisco Web Security Appliance” and enter the AsyncOS version number.

Related Documentation

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

- *Cisco Content Security Virtual Appliance Installation Guide*
- *Cisco IronPort AsyncOS for Web User Guide*

Documentation For Cisco Content Security Products	Location
Hardware and virtual appliances	See the applicable product in this table.
Cisco Web Security	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html
Cisco Email Security	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Cisco Content Security Managment	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
CLI reference guide for Cisco Content Security appliances	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Cisco IronPort Encryption	http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html

Service and Support

Knowledge Base

You can access the Cisco IronPort Knowledge Base on the Cisco IronPort Customer Support site at the following URL:

`http://www.cisco.com/web/ironport/knowledgebase.html`

Note You need a Cisco.com User ID to access the site. If you do not have a Cisco.com User ID, you can register for one here: `https://tools.cisco.com/RPF/register/register.do`

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco and Cisco IronPort users.

Access the Cisco Support Community at the following URL:

- For web security and associated management:

  https://supportforums.cisco.com/community/netpro/security/web

Customer Support

Use the following methods to obtain support:

International: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site: http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

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