Release Notes for Cisco IronPort AsyncOS 7.7.0 for Web (All Builds After Build 725)

This document is cumulative for all FCS and GA releases of AsyncOS 7.7.0 for Cisco Web Security appliances since release 7.7.0-725.

Published: July 11, 2014

Revised: October 13, 2014

Contents

New Features in Cisco IronPort AsyncOS 7.7 for Web

Tip You might also find it useful to review release notes from earlier releases.

Cisco Systems, Inc.
www.cisco.com

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.

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

Upgrading to Release 7.7.0-761 (GD - General Deployment)

Note **For S380 and S680 hardware only:** At least one fix in this release also requires a RAID firmware upgrade. For details, see Resolved Issues in Release 7.7.0-761, page 11.

To ensure a successful upgrade, prepare for the upgrade process as described in Pre-Upgrade Requirements, page 5 and Installation and Upgrade Notes, page 6.

You can upgrade to release 7.7.0-761 from the following versions:

- 7-5-0-703
- 7-5-0-727
- 7-5-0-810
- 7-5-0-833
- 7-5-0-834
- 7-5-0-836
- 7-5-0-838
- 7-5-0-840
- 7-5-0-850
- 7-5-1-074
- 7-5-1-079
- 7-5-1-085
- 7-5-2-107
- 7-5-2-202
- 7-5-2-303
- 7-5-2-304
- 7-5-2-306
- 7-5-2-332
- 7-7-0-500
- 7-7-0-608
- 7-7-0-614
- 7-7-0-710
- 7-7-0-725
- 7-7-0-734
- 7-7-0-736
- 7-7-0-744
- 7-7-0-745
- 7-7-0-753
- 7-7-0-757
- 7-7-0-760

Upgrading to Release 7.7.0-760 (Deprovisioned 9/22/2014)

It is no longer possible to upgrade to this build.

Upgrading to Release 7.7.0-757 (GA Release)

You can upgrade to release 7.7.0-757 from the following versions:

7.5.0-703	7.5.1-074	7.5.2.107	7.7.0-500
7.5.0-727	7.5.1-079	7.5.2-202	7.7.0-608
7.5.0-810	7.5.1-085	7.5.2-303	7.7.0-614
7.5.0-833		7.5.2-304	7.7.0-710
7.5.0-834		7.5.2-306	7.7.0-725
7.5.0-836		7.5.2-332	7.7.0-734
7.5.0-838			7.7.0-736
7.5.0-840			7.7.0-744
7.5.0-850			7.7.0-745
			7.7.0-753

Upgrading to Release 7.7.0-753 (GA Release)

Note To ensure a successful upgrade, prepare for the upgrade process as described in Pre-Upgrade Requirements, page 5 and Installation and Upgrade Notes, page 6.

You can upgrade to release 7.7.0-753 from the following versions:

- 7.5.0-703
- 7.5.0-727
- 7.5.0-810
- 7.5.0-833
- 7.5.0-834
- 7.5.0-836
- 7.5.0-838
- 7.5.0-840
- 7.5.0-850
- 7.5.1-074
- 7.5.1-079
- 7.5.1-085
- 7.5.2-107
- 7.5.2-202
- 7.5.2-303
- 7.5.2-304
- 7.5.2-332
- 7.7.0-500
- 7.7.0-608
- 7.7.0-614
- 7.7.0-710
- 7.7.0-725
- 7.7.0-734
- 7.7.0-736
- 7.7.0-744
- 7.7.0-745

Pre-Upgrade Requirements

Note IMPORTANT: During testing of AsyncOS 7.7.0, Cisco observed performance changes ranging from + 33% to - 16%, depending on the model and configuration. Performance degradation risk is limited to S160 & S360 models and models S370 and S660 that are running the web proxy without security services. If you experience performance degradation with AsyncOS 7.7.0, Cisco recommends that you revert to AsyncOS 7.5.x.

Warning **Model S160: Before installing AsyncOS for Web on some S160 appliances, install the hard drive firmware upgrade on the appliance. To verify whether your S160 requires the firmware upgrade, run the "upgrade" CLI command. If the S160 requires the firmware upgrade, "Hard Drive Firmware upgrade (for C/M/S160 models only, build 002)" will be listed as an upgrade option. If listed, run the firmware upgrade, and then upgrade AsyncOS for Web to the current version.**

Preserve Pre-Upgrade Data from the System Capacity Report

Pre-upgrade data for CPU usage for Web Reputation and Web Categorization (as shown in the CPU Usage by Function chart on the System Capacity report page) will not be available after upgrade. If you need to preserve this historic data, export or save the data for the CPU Usage by Function chart as CSV or PDF before you upgrade.

In this release, Web Reputation and Web Categorization data have been combined into a single collation called "Acceptable Use and Reputation."

Current Users of IronPort URL Filters: Upgrade to Cisco IronPort Web Usage Controls

Cisco has announced end-of-life for the IronPort URL Filters service, replacing it with Cisco IronPort Web Usage Controls. This release of AsyncOS for Web no longer supports IronPort URL Filters nor will it receive updates.

If the Web Security appliance currently uses IronPort URL Filters, we advise you to migrate to Cisco IronPort Web Usage Controls. To migrate, you must first obtain a license key for it **before upgrading** to the current version. If you do not yet have a license for Cisco IronPort Web Usage Controls, contact your Cisco sales representative or reseller. After migrating and upgrading, you might need to edit existing policies to use the new URL categories as necessary.

For more information about migrating and obtaining a license, read the following announcement:

http://www.cisco.com/web/ironport/docs/IronPort_URL_Filtering_EoL.pdf

Current Users of Cisco IronPort Web Usage Controls: Prepare for URL Filtering Changes

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

The set of URL categories for Cisco IronPort Web Usage Controls changed in AsyncOS 7.5 for Web. If you are upgrading from a pre-7.5 version, these changes may modify or disable existing policies. To understand, prepare for, control, and respond to these changes, see "Managing Updates to the Set of URL Categories" in the "URL Filters" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.

See the 7.5 release notes for a table listing the changes to the set of URL categories that will occur when you upgrade to AsyncOS 7.7 for Web from a pre-7.5 version. For descriptions of the new categories, see the "URL Category Descriptions" section in the "URL Filters" chapter of the *Cisco IronPort AsyncOS for Web User Guide*.

Change the Protocol for Users and Log Subscriptions Configured to Use SSH 1

Support for SSH 1 has been removed for this release. Therefore, before upgrade, you should do the following:

Any remote host keys which use SSH 1 should be changed to SSH 2. Use the logconfig > hostkeyconfig command in the CLI to make this change.

For any log subscriptions that are configured to use SSH 1 as the protocol for SCP log push, choose SSH 2 instead.

Change the access protocol or add a new SSH 2 key for any users configured to use only SSH 1. Use the sshconfig command in the CLI to make this change.

Disable SSH 1 using the sshconfig > setup command in the CLI.

Known Issues

Familiarize yourself with known issues and limitations before you upgrade AsyncOS for Web using these resources:

- Other Bug Searches, page 12
- Known Issues, page 12

Installation and Upgrade Notes

- Upgrading from a Version Earlier Than AsyncOS 7.5.0
- Post-Upgrade Reboot

Upgrading from a Version Earlier Than AsyncOS 7.5.0

If you upgrade to this release from a version earlier than 7.5.0, you must upgrade in steps. You should read the Release notes for each release between your version and this version.

Caveats such as the following may apply: Erasure of Reporting Data, page 7.

Erasure of Reporting Data

When you upgrade from a version of AsyncOS for Web *before* version 7.1, all historical data stored on the Web Security appliance for the on-box reports **will be erased**. To retain this historical data, you must export each report to PDF before upgrading.

Post-Upgrade Reboot

You must reboot the Web Security appliance after you upgrade AsyncOS for Web.

New License Agreement

A copy of the new license agreement is included in the Online Help. To view it, choose **Help and Support > Online Help**, scroll down to the end of the Contents list, and click the link for the license agreement.

Because the license agreement has changed, you may be required to accept the new agreement when you apply new feature keys after upgrading.

Sending Customer Support Requests through the Appliance

A change to Cisco IronPort Customer Support contact methods is currently in a transitional stage. When requested by CSE to send a support request through the Web Security Appliance to open or edit a case, include customercare@ironport.com in the Other Recipients field to ensure your communication is received.

Configuration Files

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.

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

For compatibility between Web Security appliance releases and Security Management appliance releases, see the compatibility matrix at: http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

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.

advancedproxyconfig Command

proxystat and rate Commands

The proxystat and rate commands now display the percent of CPU used by the web proxy instead of the percent of CPU being used by all processes.

Defect: 90186, CSCzv71295

Send Buffer Size

AsyncOS now dynamically adjusts the size of the send buffer for the client-side socket. AsyncOS no longer includes the option of the MISCELLANEOUS subcommand of the **advancedproxyconfig** command to configure the size of this buffer.

Defect 90684, CSCzv99595

wccp Command

The advancedproxyconfig>wccp command has been removed from the CLI. See Logging Command Replaced with Web Interface Support, page 10 for more information.

Defect: 85003, CSCzv21217

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. See Support, page 13.

Defect: 87828, CSCzv13413; 87830, CSCzv25201

Use NTLMSSP Option

For any sequence that contains an NTLM realm, in the Identities GUI, the All Realms and Sequences setting no longer includes the "Use NTLMSSP" option because it is not a valid option. For any sequence that contains an NTLM realm, the GUI now displays only these options for All Realms and Sequences:

- Use Basic or NTLMSSP (default)
- Use Basic

Defect: 92048, CSCzv27778

FTP Proxy Authentication

A third formatting option, No Proxy Authentication, for use when communicating with FTP clients allows for more formatting flexibility. The FTP Proxy now supports the following three formats for proxy authentication:

- **Check Point.** Uses the following formats:
  - User: ftp_user@proxy_user@remote_host
  - Password: ftp_password@proxy_password
- **Raptor.** Uses the following formats:
  - User: ftp_user@remote_host proxy_user
  - Password: ftp_password
  - Account: proxy_password"
- **No Proxy Authentication.** Uses the following formats:
  - User: ftp_user@remote_host
  - Password: ftp_password

Defect: 90467, CSCzv69205

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 in Cisco IronPort AsyncOS 7.7 for Web, page 1.

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. Now, the wccp command has been removed and you can set WCCP logging using logconfig command in the CLI or using Log Subscriptions page in the web user interface. You can use the following log levels:

- Warning. Lists errors.
- Info. Adds configuration information to the level above.
- Debug. Describes flow information in addition to the level above.
- Trace. Describes the current state and state changes in addition to the level above.

Defect: 85003, CSCzv21217

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 in Cisco IronPort AsyncOS 7.7 for Web, page 1.

Upgrading AsyncOS for Web

Before You Begin

- Read Pre-Upgrade Requirements, page 5
- Upgrade the appliance to AsyncOS version 7.5.x before upgrading to AsyncOS version 7.7.0.
- If you have limited administrator access based on IP addresses (at System Administration > Network Access), make sure that the list of allowed connections includes the appliance's Management interface IP address.
- Login to the administrator account.

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.

Post-Upgrade Requirement for FIPS Appliances

Upon upgrading from 6.5 or 7.5 on FIPS appliances, AsyncOS generates new host keys. The first attempt to access the appliance via ssh will fail if the old host key remains in the known_hosts file.

Before connecting to the appliance after upgrade, remove the old host key from the known_hosts file. Then, when attempting to connect, accept the new host key.

Defect: 88140, CSCzv77236

Known and Fixed Issues

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

Requirements for the Bug Search Tool

In order to use the Bug Search Tool, you must have a Cisco account. If you do not have one, register at https://tools.cisco.com/RPF/register/register.do.

Resolved Issues

Resolved Issues in Release 7.7.0-761

For a list of issues resolved in build 7.7.0-761, see https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=7.7.0-761&sb=fr&svr=3nH&srtBy=byRel&bt=custV.

Important: See also Resolved Issues in Release 7.7.0-760, page 12.

Resolved Issues in Release 7.7.0-760

For a list of issues resolved in build 7.7.0-760, see https://tools.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282521310&rls=7.7.0-760&sb=fr&svr=3nH&srtBy=byRel&bt=custV.

For S380 and S680 hardware only: This release, in conjunction with the required firmware upgrade described in Field Notice 63877, prevents an issue that can cause the appliance to become permanently inaccessible. If this issue occurs, the only solution is to RMA the appliance; there is no workaround. This issue does not affect any other S-Series hardware model.

For complete information, see:

- Field Notice 63877 at http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63877.html.
- Bug CSCup88211 in the Bug Search Tool at https://tools.cisco.com/bugsearch/bug/CSCup88211.
- Release Notes for the S380/S680 RAID firmware update at http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html.

Resolved Issues in Release 7.7.0-757

https://tools.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282521310&rls=7.7.0-757&sb=fr&srtBy=byRel&bt=custV

Resolved Issues in Release 7.7.0-753

https://tools.cisco.com/bugsearch/search?kw=&pf=sr&pfVal=282521310&rls=7.7.0-753&sb=fr&srtBy=svr&bt=custV

Known Issues

Known Issues in Release 7.7.0

https://tools.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282521310&rls=7.7.0&sb=afr&sts=open&svr=3nH&srtBy=byRel&bt=custV

Other Bug Searches

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, to find all issues fixed in a release:

a. Click **Select from list**, then navigate to and select your product:

```
Cisco Email Security Appliance
```

```
Cisco Web Security Appliance
Cisco Content Security Management Appliance
```

b. For **Releases**, enter the AsyncOS release number, such as `8.1.1`.

Step 4 If you have questions or problems, click the **Help** or **Feedback** links at the top right side of the tool. There is also an interactive tour; to view it, click the link in the orange bar above the search fields.

Related Documentation

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

- *Cisco IronPort AsyncOS for Web User Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Support

Knowledge Base

You can access the Knowledge Base for this product at:

https://ironport.custhelp.com/app/answers/list

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

Access the Cisco Support Community at the following URL:

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/web/services/acquisitions/ironport.html#~Support

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