Release Notes for Cisco IronPort AsyncOS for Web 7.5.2-303

Published: December 3, 2013

Contents

This document contains release information for running Cisco IronPort AsyncOS 7.5.2 for the Web Security appliance, and includes the following sections:

Upgrade Paths

You can upgrade to release 7.5.2-303 from the following versions:

- 6.3.0-604
- 6.3.1-025
- 6.3.3-015
- 6.3.5-015
- 6.3.8-005
- 7.0.0-819
- 7.1.0-306
- 7.1.0-307
- 7.1.1-027
- 7.1.1-038

Cisco Systems, Inc.
www.cisco.com

- 7.1.2-080
- 7.1.3-014
- 7.1.3-021
- 7.1.3-031
- 7.1.3-033
- 7.1.4-053
- 7.1.4-101
- 7.5.0-703
- 7.5.0-833
- 7.5.0-838
- 7.5.1-079
- 7.5.1-085
- 7.5.1-201
- 7.5.1-230
- 7.5.2-113
- 7.5.2-118

Note Version 7.5.2 is not compatible with Web Security Appliances with FIPS hardware. Do not upgrade your Web Security Appliance with FIPS hardware to this version.

To ensure a successful upgrade, before installing this update, read the "Installation and Upgrade Notes" section on page 2.

Installation and Upgrade Notes

Read through and consider the installation and upgrade impacts listed in this section.

When you upgrade AsyncOS for Web from the web interface or Command Line Interface (CLI), the configuration is saved to file in the /configuration/upgrade directory. You can access the upgrade directory using an FTP client. Each configuration file name is appended with the version number, and passwords in the configuration file are masked so they are not human readable.

Note You must be logged in as the admin to upgrade. Also, you must reboot the Web Security appliance after you upgrade AsyncOS for Web.

Warning **Before installing AsyncOS for Web on some S160 appliances, you must install the hard drive firmware upgrade on the appliance. To verify whether or not your S160 requires the firmware upgrade, run the "upgrade" CLI command. If the S160 requires the firmware upgrade, "Hard Drive Firmware upgrade (for C/M/S160 models only, build 002)" will be listed as an upgrade option. If listed, run the firmware upgrade, and then upgrade AsyncOS for Web to the current version.**

Security Vulnerabilities Addressed

Cisco AsyncOS for Web version 7.5.2-118 addresses the security vulnerabilities detailed in this security alert: http://www.cisco.com/en/US/products/csa/cisco-sa-20130626-wsa.html.

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.

End-of-Life Announcement

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

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

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

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

Reporting Data Erasure

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

Known Issues

Review the known issues associated with this release. See "Finding Information about Known and Fixed Issues" section on page 7.

Configuration Files

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

Compatibility with AsyncOS for Security Management

Features on AsyncOS 7.5.2-118 for Web are only supported by AsyncOS for Security Management version 7.9.1 HP3 and above. The reverse is also true: AsyncOS for Security Management version 7.9.1 HP3 is only compatible with AsyncOS 7.5.2-126. For more information about compatibility between the Web Security appliance and Security Management appliance, see the compatibility matrix in the release notes for the Security Management appliance posted on the Cisco products web site: http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html

New Features

Caching for Syslog Push Log Subscriptions

You can now use the logconfig command to configure a local disk buffer for a syslog push log subscription to allow AsyncOS to cache log events when the remote syslog server is unavailable. When the syslog server becomes available, AsyncOS begins sending all the data in the buffer for that log subscription to the syslog server.

Before You Begin

- Create the syslog push log subscription (use TCP for transport) if it does not already exist.
- Ensure the syslog server is running before starting this procedure to avoid log data loss.
- Determine the size of the local disk buffer, allowing enough space to accomodate the maximum expected period of down time for the syslog server. This avoids loss of log data.
- If you have a secondary log subscription for local retention, Cisco recommends you cancel the secondary subscription to allow space for the local disk buffer for the primary subscription.
- Be aware that AsyncOS may not be able to cache the first several seconds of log data after loss of connection to the syslog server. This is due to characteristics of syslog over TCP.
- Allow a buffer initialization period of 10 minutes per 50 GB of disk buffer size before sending data to the Web Security Appliance.

Step 1 Use the logconfig CLI command to edit the syslog push log subscription:

```
mail3.example.com> logconfig

Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- HOSTKEYCONFIG - Configure SSH host keys.

[]>edit
```

Step 2 Identify the log subscription by number.

Step 3 Accept the existing values for these options:

- Log name
- Log style
- HTTP Error Status Codes

- Method to retrieve the logs (Syslog Push is the only applicable method)
- Hostname to deliver the logs

Step 4 Change the transfer protocol to TCP if it is set to UDP. Otherwise accept TCP.

Step 5 Accept the existing value for these options:

- Send facility

Step 6 Enable the disk buffer:

Enable syslog disk buffer (yes/no)

[no]> yes

Step 7 Set the syslog disk buffer size (in bytes, in multiples of 1024) or accept the default value of 100M:

Syslog disk buffer size (in bytes)

[100M]>

Example values: 10G, 10485760, 20M

Step 8 Commit your changes.

Related Documentation

- AsyncOS CLI Reference Guide

Changes in Behavior

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

Webroot Body Scanning

You can now disable Webroot body scanning using the advancedproxyconfig scanning subcommand.

Defect: CSCzv78679

WCCP Related Commands

In AsyncOS for Web 7.5, the advancedproxyconfig > wccp command no longer exists. Now, you use the web interface to change the logging level of the WCCP Module Logs. You can use the following log levels:

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

Defect: 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 Customer Support, page 8.

Defect: CSCzv13413, CSCzv25201

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: CSCzv71295

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: CSCzv69205

Send Buffer Size

AsyncOS now dynamically adjusts the size of the send buffer for TCP connections. This is the new default behavior. There is an option to disable this behavior and use static TCP send buffer size for all connections, which is available under the CLI advancedproxyconfig command.

To disable dynamic adjustment of the send buffer size, respond “no” to this advancedproxyconfig command question: Would you like proxy to perform dynamic adjustment of TCP send window size?

Defect: CSCzv99595

Upgrading AsyncOS for Web

.Before You Begin

- 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.

Step 1 Login to the appliance using an administrator account.

Step 2 On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.

Step 3 On the System Administration > System Upgrade page, click **Available Upgrades**.

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

Step 4 Click **Begin Upgrade** to start the upgrade process. Answer the questions as they appear.

Step 5 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.

Finding Information about Known and Fixed Issues

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

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, 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`.

c. For **Show Bugs**, select **Fixed in this release**.

Note Known issues on Cisco Email Security Appliances and Cisco Web Security Appliances may appear in or impact functionality of Cisco Content Security Management Appliances.

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*

Customer Support

Use the following methods to obtain support:

U.S.: Call 1 (408) 526-7209 or Toll-free 1 (800) 553-2447

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

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

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