



Cisco IronPort URL Filters Upgrade for S-Series Web Security Appliances

Published: February 02, 2012

Revised: February 03, 2012

Contents

These release notes contain important information about installing the IronPort URL Filters upgrade for all S-Series Web Security appliances. This update fixes an issue with IronPort URL Filters. Note that there are two URL filtering engines available on the Web Security appliance, IronPort URL Filters and Cisco IronPort Web Usage Controls. You only need to install this update if the appliances uses IronPort URL Filters. To verify which URL filtering engine is currently in use, go to [Pre-installation Requirements, page 2](#).

This document contains the following sections:

- **Supported Versions for the Upgrade.** See [Supported Versions for the IronPort URL Filters Upgrade, page 1](#).
- **Fixed Issues.** See [Fixed Issues, page 2](#).
- **Installation Instructions.** See [Upgrade Installation Instructions, page 2](#)
- **Related Documentation.** See [Related Documentation, page 3](#).
- **Service and Support.** See [Service and Support, page 3](#).

Supported Versions for the IronPort URL Filters Upgrade

To install the IronPort URL Filters upgrade on S-Series appliances, you must be on or above AsyncOS for Web 6.3.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Fixed Issues

This section describes the issues fixed by this upgrade.

Fixed: IronPort URL filtering engine returns uncategorized for all URLs

A bug in the IronPort URL filtering engine caused its license to expire on January 31, 2012. As a result, the IronPort URL filtering engine returns uncategorized for all transactions. This issue does *not* affect Cisco IronPort Web Usage Controls.

[Defect ID: 83864]

Upgrade Installation Instructions

You can install the IronPort URL Filters upgrade patch from either the CLI or web interface.

After you run the IronPort URL Filters upgrade, the “Cisco IronPort URL Filtering License Update” will display in the list of available upgrades even after a successful installation. The presence of this package does *not* indicate a failed upgrade.



Note

If you upgrade the appliance to a later version or build after you run the IronPort URL Filters upgrade, you must run the IronPort URL Filters upgrade again.

Pre-installation Requirements

Before you perform the IronPort URL Filters upgrade installation, perform the following steps:

- Step 1** Verify the Web Security appliance uses IronPort URL Filters instead of Cisco IronPort Web Usage Controls. In the web interface, navigate to the Security Services > Acceptable Use Controls page and verify IronPort URL Filters is selected.



Note

If Cisco IronPort Web Usage Controls is selected, you do not need to run this upgrade.

- Step 2** Navigate to the System Administration > Configuration File page and save the XML configuration file off the Web Security appliance.

Installing the Upgrade from the CLI

- Step 1** Access the CLI interface.
- For information on accessing the CLI, see the “Using the Web Security Appliance” chapter in the *Cisco IronPort AsyncOS for Web User Guide*.
- Step 2** From the CLI, enter **upgrade**.
- A list of available upgrades is displayed.

The IronPort URL Filters upgrade package is provisioned *only* for appliances that require the upgrade. If you do not see “Cisco IronPort URL Filtering License Update” in the list of available upgrades, you can assume that your appliance does not require the upgrade and you can skip any further upgrade steps.

Step 3 Select the package “Cisco IronPort URL Filtering License Update”.

Step 4 You will be prompted to proceed with the upgrade. Click **Yes**.

In about one minute the IronPort URL filtering engine will start processing transactions. To verify that the upgrade has run successfully, read the access log to read the URL category verdicts.

Installing the Upgrade from the Web Interface

Step 1 Access the web interface.

For information on accessing the web interface, see the “Using the Web Security Appliance” chapter in the *Cisco IronPort AsyncOS for Web User Guide*.

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

The Available Upgrades page is displayed.

The IronPort URL Filters upgrade package is provisioned *only* for appliances that require the upgrade. If you do not see “Cisco IronPort URL Filtering License Update” in the list of available upgrades, you can assume that your appliance does not require the upgrade and you can skip any further upgrade steps.

Step 3 Select the package “Cisco IronPort URL Filtering License Update” and click **Begin Upgrade** to start the upgrade process. Answer the questions as they appear.



Note Even though the Overall Progress bar shows 0%, the upgrade process is complete when the web interface displays “Upgrade is complete.”

In about one minute the IronPort URL filtering engine will start processing transactions. To verify that the upgrade has run successfully, read the access log to read the URL category verdicts.

Related Documentation

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

- *Cisco IronPort AsyncOS for Web User Guide*

Service and Support

You can request our support by phone, email, or online 24 hours a day, 7 days a week.

During customer support hours (24 hours per day, Monday through Friday excluding U.S. holidays), an engineer will contact you within an hour of your request.

To report a critical issue that requires urgent assistance outside of our office hours, please contact IronPort using one of the following methods:

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

International: <http://cisco.com/web/ironport/contacts.html>

Support Portal: <http://cisco.com/web/ironport/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.

 Printed in the USA on recycled paper containing 10% postconsumer waste.