Cisco IronPort Update for BIOS Firmware for Content Security Appliances

Published: October 31, 2012

Contents

These release notes contain important information about installing the update for BIOS firmware for Cisco IronPort Content Security appliances:

- **Appliances covered by the Update for BIOS firmware.** This section lists the appliances covered by this firmware upgrade. See Appliances Covered by the Update for BIOS Firmware, page 1.
- **Supported Versions for the Update for BIOS firmware**. This section describes the supported versions for this firmware upgrade. See Supported Versions for the Update for BIOS Firmware, page 2.
- **Fixed Issues**. This section describes the issues fixed by the update for BIOS firmware. See Fixed Issues, page 2.
- **Patch Installation Instructions**. This section provides hard drive upgrade installation instructions. See Update for BIOS Firmware Installation Instructions, page 2
- **Service and Support**. This section provides information on obtaining service and support for your Cisco IronPort Appliances. See Service and Support, page 4.

Appliances Covered by the Update for BIOS Firmware

- **Email Security appliances:**
  - C370
  - C670
  - X1070
  - X1070-F

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

- **Content Security Management appliances:**
  - M670
  - M1070
- **Web Security Appliances:**
  - S370
  - S670

Supported Versions for the Update for BIOS Firmware

To install the firmware patch, you must be on or above the following AsyncOS versions. You may need to perform an upgrade before you can install the firmware patch:

- **Cisco IronPort Email Security Appliance**:
  - 7.1.5
  - 7.3.1
  - 7.3.2
  - 7.5.1 and higher
- **Cisco IronPort Content Security Management Appliance**:
  - 7.2.2 or higher
- **Cisco IronPort Web Security Appliance**:
  - 6.3.3 or higher

Fixed Issues

This section describes the issues fixed by this firmware upgrade.

Fixed: Instances of performance degradation on the Security Appliance with BIOS firmware version 2.2.12C

Due to a problem with BIOS firmware version 2.2.12C, full CPU processing power was not enabled on some appliances.

The update for BIOS firmware fixes this problem.

[Defect ID:86614]

Update for BIOS Firmware Installation Instructions

Follow the instructions below to obtain and install the update for BIOS firmware patch.

Pre-installation Requirements

Before you install the update for BIOS firmware, save the configuration file to a location off of the appliance:

Step 1 In the graphical user interface, navigate to **System Administration > Configuration File**.

Step 2 Select **Download file to local computer to view or save**.

Step 3 Click **Submit**.

Installation Steps

Step 1 Access the CLI interface. For details on accessing the CLI, see Accessing the CLI.

Note For the upgrade to run correctly, you *must* run it from the CLI.

Step 2 From the CLI, enter *upgrade*.

Step 3 A list of available upgrades will display.

The update for BIOS firmware package is provisioned *only* for appliances that require the upgrade. If you do not see the Update for BIOS firmware package 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 4 Select the package *Update for BIOS firmware*.

Step 5 You will be prompted to reboot your machine. Click **Yes**.

Step 6 Wait approximately fifteen minutes.

Step 7 Your machine should automatically reboot after approximately fifteen minutes.

Warning **If your machine does not automatically reboot in fifteen minutes, contact customer support. Do not attempt to reboot your machine again.**

Note After you run the firmware upgrade, the firmware upgrade package will display in the list of available upgrades even after a successful installation. The presence of this package does *not* indicate a failed upgrade.

Step 8 To verify that the upgrade has run successfully, you can run the upgrade script again after the machine has rebooted. If the upgrade was successful, the upgrade script will indicate that the appliance does not require upgrading.

Accessing the CLI

To run this upgrade, you must access the CLI. The instructions below provide information on accessing the CLI.

Access to the CLI varies depending on the management connection method chosen while setting up the appliance. Initially, only the admin user account has access to the CLI. You can add other users with differing levels of permission after you have accessed the command line interface for the first time via the admin account. The system setup wizard asks you to change the password for the admin account. The password for the admin account can also be reset directly at any time using the password command. To connect via Ethernet: Start an SSH or Telnet session with the factory default IP address 192.168.42.42. SSH is configured to use port 22. Telnet is configured to use port 23.

To connect via a Serial connection: Start a terminal session with the communication port on your personal computer that the serial cable is connected to. See the "Setup and Installation" chapter in the *Cisco IronPort AsyncOS Configuration Guide* for more information. Enter the user name and password below.

Factory Default User name and Password

• Username: `admin`

• Password: `ironport`

Service and Support

You can request our support by phone, email, or online 24 hours a day, 7 days a week. Cisco IronPort Customer Support service level agreement details are available on the Support Portal.

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-IRON (4766)
- International: www.ironport.com/support/contact_support.html
- Support Portal: www.ironport.com/support

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

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