



Cisco IronPort Hard Drive Firmware Upgrade for C160, S160, and M160 Appliances

Published: July 22, 2010

Contents

These release notes contain important information about installing the hard drive firmware upgrade for C160, S160, M160 appliances:

- **Supported Versions for the Hard Drive Firmware Upgrade.** This section describes the supported versions for this firmware upgrade. See [Supported Versions for the Hard Drive Firmware Upgrade, page 1](#).
- **Fixed Issues.** This section describes the issues fixed by the hard drive firmware upgrade. See [Fixed Issues, page 2](#).
- **Patch Installation Instructions.** This section provides hard drive upgrade installation instructions. See [Hard Drive Firmware Upgrade 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](#).

Supported Versions for the Hard Drive Firmware Upgrade

To install the firmware patch on C160, S160, and M160 appliances, 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**- version 6.5.0 or higher
- **Cisco IronPort Security Management Appliance** - version 6.5.0 or higher
- **Cisco IronPort Web Security Appliance** - version 6.0 or higher



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 firmware upgrade.

Fixed: Error In Driver Controller Causes Requests to Timeout Under Certain Conditions

A bug in the driver controller code on the hard drives used on the C160, S160, and M160 appliances sometimes caused requests to timeout in certain conditions, which resulted in errors or the drive going offline.

The hard drive firmware upgrade fixes this problem.

[Defect ID:71333]

Hard Drive Firmware Upgrade Installation Instructions

Follow the instructions below to obtain and install the hard drive firmware upgrade patch.

Pre-installation Requirements

Before you perform the hard drive firmware patch installation, complete the following steps:

- **For the Cisco IronPort Web Security Appliance:** On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.
- **For the Cisco IronPort Email Security Appliance.** Take the following precautions before performing the firmware patch installation:
 - Save the XML configuration file off the IronPort appliance.
 - If you are using the Safelist/Blocklist feature, export the Safelist/Blocklist database off the IronPort appliance.
 - Suspend all listeners.
 - Wait for the queue to empty before you run the firmware patch.
- **For the Cisco IronPort Security Management Appliance.** Take the following precautions before performing the firmware patch installation:
 - On the Security Management appliance, click System Administration > Configuration File. Save the XML configuration file off the Security Management appliance.
 - If you are using the Safelist/Blocklist feature, export the list off the appliance.

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 hard drive firmware upgrade package is provisioned *only* for appliances that require the upgrade. If you do not see the Hard Drive Firmware Upgrade 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 *Hard Drive Firmware upgrade*.
- 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. The machine will then automatically reboot a second time.

**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 no disks 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: <http://www.cisco.com/web/ironport/contacts.html>
- Support Portal: <http://www.cisco.com/web/ironport/index.html>

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0807R)

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.

© 2010 Cisco Systems, Inc. All rights reserved.