



# Release Notes for RAID Firmware Upgrade for S380/S680 Cisco Content Security Appliances

---

**Published: September 10, 2014**

**Revised: September 10, 2014**

- [Appliance Models Requiring This Firmware Upgrade, page 1](#)
- [AsyncOS Software Versions That Support This Firmware Upgrade, page 2](#)
- [Issues Resolved in This Firmware Upgrade, page 2](#)
- [Upgrade Instructions, page 2](#)
- [Accessing the CLI, page 2](#)
- [Support, page 3](#)

## Appliance Models Requiring This Firmware Upgrade

- S380
- S680



# AsyncOS Software Versions That Support This Firmware Upgrade

The **Known Fixed Releases** list at the following URLs shows the AsyncOS versions that support this firmware upgrade:

Cisco Web Security Appliances	<a href="https://tools.cisco.com/bugsearch/bug/CSCup88211">https://tools.cisco.com/bugsearch/bug/CSCup88211</a>
-------------------------------	---



**Note**

A Cisco account is required to view this information. To obtain an account, visit <https://tools.cisco.com/RPF/register/register.do>.

## Issues Resolved in This Firmware Upgrade

This upgrade 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.

For complete information about this issue, see Field Notice 63877 at <http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63877.html>.

## Upgrade Instructions

You must upgrade both AsyncOS and the RAID firmware to install this fix.

See important instructions in Field Notice 63877 at <http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63877.html>.

## 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*

# Support

## Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco and Cisco IronPort users.

Access the Cisco Support Community at the following URL:

- For web security and associated management:  
<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](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](http://www.cisco.com/en/US/products/ps11169/serv_group_home.html)

