



ASA for FirePOWER Services Local Management Update Notes

Version 6.0

First Published: November 11, 2015

This document provides instructions for updating Cisco ASA with FirePOWER Services from Version 5.4.1 to Version 6.0 using the local ASA FirePOWER module user interface through ASDM.

For more information on Version 6.0, including supported platforms, new and changed features and functionality, management platform-managed device compatibility, and known and resolved issues, see the *Firepower System Release Notes*, Version 6.0. If you want to update your ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X using the Firepower Management Center instead, refer to those notes. They contain detailed information on prerequisites, warnings, and specific installation instructions for updating the Firepower Management Center and the devices it manages.

Even if you are familiar with the update process, make sure you thoroughly read and understand these release notes. They contain detailed information on prerequisites, warnings, and specific update instructions for the following appliances:

- Cisco ASA with FirePOWER Services on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X

These release notes are valid for Version 6.0 of the ASA FirePOWER module.

Caution: These notes specifically address how to update when you are locally managing the ASA FirePOWER module through ASDM. If you are managing the ASA FirePOWER module using a Firepower Management Center, refer to the *Firepower System Release Notes* for information on updating the module using the Firepower Management Center rather than following the procedure in these notes.

For more information, see the following sections:

- [Updating the ASA FirePOWER Module Using Local Management, page 1](#)
- [For Assistance, page 5](#)

Updating the ASA FirePOWER Module Using Local Management

For more information, see the following sections:

- [Before You Begin: Important Update and Compatibility Notes, page 1](#)
- [Installing the Update, page 3](#)

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 6.0, you should familiarize yourself with the behavior of the system during the update process, as well as with any compatibility issues or required pre- or post-update configuration changes.

Updating the ASA FirePOWER Module Using Local Management

For more information, see the following sections:

- [Configuration and Event Backup Guidelines, page 2](#)
- [Traffic Flow and Inspection During the Update, page 2](#)
- [Version Requirements for Updating to Version 6.0, page 2](#)
- [Time and Disk Space Requirements for Updating to Version 6.0, page 2](#)

Configuration and Event Backup Guidelines

Before you begin the update, Cisco strongly recommends that you delete or move any backup files that reside on your appliance, then back up current event and configuration data to an external location.

Use the ASA FirePOWER module user interface through ASDM to back up event and configuration data for itself and the devices it manages. For more information on using the backup and restore feature prior to update, see the *ASA FirePOWER Module User Guide, Version 5.4.1*.

Note: The module purges locally stored backups from previous updates. To retain archived backups, store the backups externally.

Traffic Flow and Inspection During the Update

The update process reboots the ASA FirePOWER module. Depending on how your module is configured and deployed, the following capabilities are affected:

- traffic inspection, including application awareness and control, URL filtering, Security Intelligence, intrusion detection and prevention, and connection logging
- traffic flow, including switching, routing, NAT, VPN, and related functionality (on the ASA device)
- link state

Traffic Inspection and Link State

In an inline deployment, your ASA FirePOWER module can affect traffic flow via application control, user control, URL filtering, Security Intelligence, and intrusion prevention.

Version Requirements for Updating to Version 6.0

To update to Version 6.0, an ASA FirePOWER module must be running at least Version 5.4.1 of ASA for FirePOWER Services. If you are running an earlier version, you can obtain updates from the Support site.

Time and Disk Space Requirements for Updating to Version 6.0

The table below provides disk space and time guidelines for the Version 6.0 update.

Caution: Do **not** restart the update or reboot your appliance at any time during the update process. Cisco provides time estimates as a guide, but actual update times vary depending on the appliance model, deployment, and configuration. Note that the system may appear inactive during the pre-checks portion of the update and after rebooting; this is expected behavior.

If you encounter issues with the progress of your update, contact Support.

Installing the Update

Table 1 Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Cisco ASA with FirePOWER Services	32 MB	7644 MB	1.2 GB	41 minutes

You can locally update ASA FirePOWER modules to Version 6.0 on the following ASA platforms running version 9.5(1.5):

- ASA 5506-X
- ASA 5506H-X
- ASA 5506W-X
- ASA 5508-X
- ASA 5516-X

Installing the Update

Before you begin the update, you must thoroughly read and understand these release notes, especially [Before You Begin: Important Update and Compatibility Notes, page 1](#).

Caution: Do **not** reboot or shut down your appliances during the update until you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.

Installation Method

Use the ASA FirePOWER module's web interface, via ASDM, to perform the update.

After the Installation

After you perform the update, you **must** redeploy device configuration and access control policies. Deploying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.0*.

There are several additional post-update steps you should take to ensure that your deployment is performing properly. These include:

- verifying that the update succeeded
- making sure that all appliances in your deployment are communicating successfully
- optionally, updating your intrusion rules and vulnerability database (VDB) and redeploying your access control policies

The next sections include detailed instructions not only on performing the update, but also on completing any post-update steps. Make sure you complete all of the listed tasks.

ASA FirePOWER modules using local management do not require Firepower Management Centers to update.

Note: Before updating an ASA FirePOWER module to Version 6.0, you must update to ASA version 9.5(1.5) and ASDM 7.5.1.

For the Version 6.0 update, all devices reboot.

Installing the Update

Caution: Before you update a device, reapply the appropriate access control policy.

To update ASA FirePOWER modules on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X locally via ASDM:

1. Read these release notes and complete any required pre-update tasks.

For more information, see [Before You Begin: Important Update and Compatibility Notes, page 1](#).

2. Update the ASA software on the devices running ASA FirePOWER module to ASA version 9.5(1.5) and ASDM 7.5.1. For more information, see the *Release Notes for the Cisco ASA Series, 9.5(x)* and the *Release Notes for Cisco ASDM, 7.5(x)*.

3. Download the update from the Beta site:

- for ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X devices:

```
Cisco_Network_Sensor_-6.0.0-1002.sh
```

Note: Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted.

4. Select **Configuration > ASA FirePOWER Configuration > Updates**.

5. Click **Upload Update**.

6. Click **Choose File** to navigate to and select the update.

7. Click **Upload**.

8. Select **Monitoring > ASA FirePOWER Monitoring > Task Status** to view the task queue and make sure that there are no jobs in process.

Tasks that are running when the update begins are stopped and cannot be resumed; you must manually delete them from the task queue after the update completes. The task queue automatically refreshes every 10 seconds. You must wait until any long-running tasks are complete before you begin the update.

9. Select **Configuration > ASA FirePOWER Configuration > Updates**.

10. Click the install icon next to the update you uploaded.

The update process begins. How you monitor the update depends on whether the update is a major or minor update. For major updates, you can begin monitoring the update's progress in the task queue. However, after the ASA FirePOWER module completes its necessary pre-update checks, you are locked out of the module interface.

11. After the update finishes, reconnect ASDM to the ASA device.

12. Access the ASA FirePOWER module interface and refresh the page. Otherwise, the interface may exhibit unexpected behavior. If you are the first user to access the interface after a major update, the End User License Agreement (EULA) may appear. You must review and accept the EULA to continue.

13. If the intrusion rule update available on the Support site is newer than the rules on your ASA FirePOWER module, import the newer rules. Do not auto-apply the imported rules when working with Version 6.0.

For more information, see the *Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.0*.

14. If the VDB available on the Support Site is newer than the most recently installed VDB, install the latest VDB.

Installing a VDB update causes a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.0*.

15. Redeploy policies.

Deploying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Cisco ASA with FirePOWER Services Local Management Configuration Guide*, Version 6.0.

For Assistance

Thank you for choosing the Firepower System.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

If you have any questions or require assistance, please contact Cisco Support:

- Visit the Cisco Support site at <http://support.cisco.com/>.
- Email Cisco Support at tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.

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.

© 2015 Cisco Systems, Inc. All rights reserved.

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

For Assistance