



Firepower System Release Notes for Version 6.0.0 Pre-Install

First Published: January 27, 2016

Last Updated: June 27, 2018

The Version 6.0.0 Pre-Install must be installed on Firepower Management Centers and managed devices that have STIG enabled via prior to updating your system to Version 6.0.0. This Pre-Install optimizes the update procedure for Firepower Management Centers updating to Version 6.0.0 and decreases the time the update takes to complete. Once you install the Version 6.0.0 Pre-Install, update the system to Version 6.0.0. For more information, see the *Firepower System Release Notes Version 6.0.0*.

These notes provide installation instructions and a summary of the caveats resolved by the Firepower System Version 6.0.0 Pre-Install.

For more information, see the following sections:

- [Before You Begin: Important Update Notes, page 1](#)
- [Installing the Update, page 2](#)
- [Updating the Firepower Management Center, page 3](#)
- [Updating Managed Devices, page 4](#)
- [Updating ASA FirePOWER modules locally via ASDM, page 4](#)
- [Uninstalling the Pre-Install from the Firepower Management Center, page 5](#)

Before You Begin: Important Update Notes

Apply the Pre-Install to appliances running the following versions:

- Firepower Management Centers running Version 5.4.1.1, Version 5.4.1.2, Version 5.4.1.3, Version 5.4.1.4, or Version 5.4.1.5

Note: The Version 6.0.0 Pre-Install optimizes updating Firepower Management Centers to Version 6.0.0 and decreases the time the update takes to complete.

- Series 3 devices running Version 5.4.0.2, Version 5.4.0.3, Version 5.4.0.4, Version 5.4.0.5, or Version 5.4.0.6
- ASA FirePOWER modules (ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and the ASA5585-X-SSP-60) running Version 5.4.0.2, Version 5.4.0.3, Version 5.4.0.4, Version 5.4.0.5, or Version 5.4.0.6
- ASA FirePOWER modules (ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, and ASA5516-X) running Version 5.4.1.1, Version 5.4.1.2, Version 5.4.1.3, Version 5.4.1.4, or Version 5.4.1

Note: The Version 6.0.0 Pre-Install and Version 6.0.0 and later do not support Series 2 devices.

Installing the Update

The Pre-Install is not required on appliances running the following versions:

- Firepower Management Centers running Version 5.4.1.6 or later

Note: While the Version 6.0.0 Pre-Installation package is not required, we strongly recommend you install prior to updating to Version 6.0 to decrease the time the update takes to complete.

- Series 3 devices running Version 5.4.0.7 or later
- ASA FirePOWER modules (ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and the ASA5585-X-SSP-60) running Version 5.4.0.7 or later
- ASA FirePOWER modules (ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, and ASA5516-X) running Version 5.4.1.6 or later

Installing the Update

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

You can update Firepower Management Centers running at least Version 5.4.1.1 of the Firepower System to Version 6.0.0 Pre-Install.

Note that updating to the Version 6.0.0 Pre-Install does **not** change the listed version of the Firepower Management Center's About page (**Help > About**).

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.

When to Perform the Update

Because the update process may affect traffic inspection, traffic flow, and link state, Cisco strongly recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

Installation Method

Use the Firepower Management Center's web interface to perform the update.

Order of Installation

Update your Firepower Management Centers before updating the devices they manage. Once the system is running Version 6.0.0. Pre-Install, update the system to Version 6.0.0.

Break Firepower Management Center High Availability Prior to Upgrade

Version 6.0.0 does not support Firepower Management Centers in a high availability pair. In order to update Firepower Management Centers in a high availability environment, you must break the pair and update each Firepower Management Center individually. Before updating to Version 6.0.0, you must break the high availability pair.

After the Installation

After you perform the update on the Firepower Management Center, you must reapply device configuration and access control policies. Applying 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 *Firepower Management Center Configuration Guide*. 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

Updating the Firepower Management Center

- reapplying your access control policies

After installing the Pre-Install on the Firepower Management Center and reapplying device configuration, update the system to Version 6.0.0. 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.

Updating the Firepower Management Center

You **must** install the Version 6.0.0 Pre-Install to your Firepower Management Center prior to updating your system to Version 6.0.0 if STIG is enabled,

1. Download the pre-installation file (Sourcefire_6.0.0_Pre-install-build_4.tar) from the [Cisco Support site](#).

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

2. On the system that will be used to upload the Version 6.0.0 Pre-Install to the Firepower Management Center, extract the file:
 - for Series 3 and virtual Firepower Management Center

Sourcefire_3D_Defense_Center_S3_6.0.0_Pre-install-5.4.1.999-21.sh

Note: An application capable of extracting tarballs (.tar or .tar.gz) will be needed for this task. (Due to a significant number of reported file corruption issues upon extraction, we recommend against using WinZip to handle the file extraction.) To reduce the possibility of file corruption or alteration during transfer, do not extract the hotfix file (.sh) on a different system, and/or transfer the hotfix file via email. We advise comparing the checksum (sha512) of the extracted hotfix file against the respective checksum provided in the hotfix archive file to ensure a match.

3. Using a web browser on the same system, log into the web user interface of the Firepower Management Center.
4. Select **System > Updates**.
5. Upload the file to the Firepower Management Center by clicking **Upload Update**.
6. Click **Choose File** in the Updates box, select the file from the local file system, then click **Upload** to upload the file to the Firepower Management Center.

The Product Updates sub-tab will then appear again.

7. Take note of the Reboot column for each file to be installed.
8. Click the Install icon for the file.
9. Select the device(s) to which to install the file.
10. Click **Install** to begin installing the file.
11. Confirm on the System Status tab page (**Tasks > System Status**) the progress of the installation, until the installation is complete.

Note: The Firepower Management Center does not reboot.

Caution! Updating a Firepower Management Center that manages devices running Version 5.4.0.6, Version 5.4.1.5, or earlier to Version 6.0.0 may cause traffic outages and system issues. To avoid traffic disruption, you **must** disable the **Retry URL cache miss lookup** option in the Advanced Options section of the Access Control page prior to deploying configuration to managed devices running Version 5.4.0.6, Version 5.4.1.5, or earlier. For more information after you update the Firepower Management Center to Version 6.0.0, see the [Preventing URL Cache Miss Lookup Retries](#) section of the *Firepower System Version 6.0.0 Release Notes*.

Updating Managed Devices

You must install the Version 6.0.0 Pre-Install to managed devices that have STIG enabled via your Firepower Management Center prior to updating your system to Version 6.0.0.

1. Download the Version 6.0.0 Pre-install (Sourcefire_3D_Defense_Center_S3_6.0.0_Pre-install-5.4.1.999-4.sh) from the [Cisco Support site](#).

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

2. On the system that will be used to upload the file to the managed device, extract the file:
 - for Series 3 devices

```
Sourcefire_3D_Device_S3_6.0.0_Pre-install-5.4.0.999-2.sh
```

- for virtual managed devices

```
Sourcefire_3D_Device_Virtual64_VMware_6.0.0_Pre-install-5.4.0.999-2.sh
```

3. Upload the update to the Firepower Management Center by selecting **System > Updates**, then clicking **Upload Update** on the Product Updates tab. Browse to the update and click **Upload**.
4. Click the install icon next to the update you are installing.
5. Select the devices where you want to install the update.
6. Click **Install**. Confirm that you want to install the update and reboot the devices. The update process begins.
7. The update process begins. To view the task status, click the System Status icon, then click on the Tasks tab.

Updating ASA FirePOWER modules locally via ASDM

You must install the Version 6.0.0 Pre-Install to ASA FirePOWER modules that have STIG enabled via ASDM.

1. Download the Version 6.0.0 Pre-Install (Cisco_Network_Sensor_6.0.0_Pre-install-5.4.0.999-2.sh) from the [Cisco Support site](#).

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

2. Log into ASDM.
3. Select **Configuration > ASA FirePOWER Configuration > Updates**.
4. Upload the Pre-Install to the ASA FirePOWER module via ASDM by clicking **Upload Update**.
5. Click **Choose File**, select the Pre-Install from the local file system, then click **Upload** to upload the file to the ASA FirePOWER device.
6. Click the Install icon for the file.
7. Select the device(s) to which to install the file.
8. Click **Install** to begin installing the file.
9. To view the installation status, click the System Status icon, then click on the Tasks tab.

Uninstalling the Pre-Install from the Firepower Management Center

If you need to uninstall the Version 6.0.0 Pre-Install from a Firepower Management Center, you must uninstall updates locally.

Use the following procedure to uninstall the Version 6.0.0 Pre-Install from Firepower Management Centers.

Uninstalling the Version 6.0.0 Pre-Install update results in a Firepower Management Center running the version the appliance updated from. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

1. Log into the device as admin via SSH or through the virtual console.
2. At the bash shell prompt, type **sudo su -**.
3. Type the admin password to continue the process with root privileges.
4. At the prompt, enter the following on a single line:

```
install_update.pl --detach  
/var/sf/updates/Sourcefire_3D_Defense_Center_S3_6.0.0_Pre-install_Uninstaller-5.4.1.999-21.s  
h
```

The uninstallation process begins.

Caution: If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Support.

5. After the uninstallation finishes, log into the managing Firepower Management Center and select **Devices > Device Management**. Confirm that the device where you uninstalled the update has the version the appliance updated from as the correct software version.
6. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Resolved Caveats

You can track defects resolved in this release using the Cisco Bug Search Tool (<https://tools.cisco.com/bugsearch/>). A Cisco account is required. The pre-install addresses the following issues:

- Resolved an issue where, if you enable STIG compliance on a system running 5.4.x and upgrade the system to Version 6.0.0, the upgrade failed. (CSCux23487)
- Resolved an issue where, if you created an access control policy referencing an SSL policy containing a network object with multiple entries on a managed Firepower appliance running Version 5.4 or later and you updated the Firepower Management Center to Version 6.0.0, policy apply failed. (CSCux31618)
- Resolved an issue where, in some cases, the system database integrity check failed and you could not upgrade the system to Version 6.0.0. (CSCux52218)
- Resolved a rare issue where, if you saved an intrusion policy on a Firepower Management Center running Version 6.0.0 that previously ran a version prior to Version 5.4, the saved intrusion policy corrupted. (CSCux57697)
- Detects whether or not a system updated from Version 5.2 is missing configuration in the system policy which would prevent access to the user interface after update to Version 6.0.0 and causes update to Version 6.0.0 to fail while that condition exists. If your update to Version 6.0.0 fails for this reason, configure the default **Browser SessionTimeout** to a larger value and perform the update to Version 6.0.0 again. (CSCux61503)
- Improved Firepower Management Center performance when rebooting during the update. (CSCuz23081)
- Optimized the automated process to check available disk space. (CSCuz71421)

For Assistance

- Improved troubleshoot generation. (CSCuz71430, CSCva71569)
- Improved the automated database update process. (CSCuz71453)
- Optimized the update to skip enterprise objects that do not need conversion or integrity checks. (CSCuz71471, CSCuz71485)
- Improved the SQL update process. (CSCuz71492)
- Improved the update process for main database tables and large amounts of scan data from network maps. (CSCuz98801)
- Resolved an issue where, if you updated a system from Version 5.4.0.X or later to the Version 6.0.0 Pre-Installation package and then updated to Version 6.0.0 or later, the system experienced a variety of issues such as update failure or Firepower Management Center login failure. (CSCvb27923)
- Resolved an issue where updating an ASA FirePOWER module from Version 5.4.1.8 or later to Version 6.0.0 or if you uninstall Version 5.4.1.8 or later on a ASA FirePOWER module to Version 5.4.1.7 and attempt to update the device to Version 6.0.0 failed. (CSCvb62987)
- Removed the file system integrity check during the update. (CSCvb64157)
- Resolved an issue where, under some circumstances, updating a Firepower Management Center from Version 5.4.0 to Version 6.0.0 failed. (CSCvc36969)
- Resolved an issue where, if you updated a managed device running Version 5.4.0.9 to Version 6.0.0, the appliance experienced an error and the update failed. (CSCvc96251)
- Resolved an issue where the Version 6.0.0 pre-install incorrectly stopped the update when the pre-install script checked Defense Centers for exactly 8G RAM. (CSCvc98418)

For Assistance

Thank you for choosing the Firepower System.

Cisco Support

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about Cisco ASA devices, 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 with Cisco ASA devices, 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.

© 2016 Cisco Systems, Inc. All rights reserved.

For Assistance

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

For Assistance