



Uninstall Version 6.2.0.x

You must uninstall updates locally. You *cannot* use a Firepower Management Center to uninstall the update from a managed device.

To monitor the uninstallation process, access the device through the shell and navigate to the `/var/log/sf/<uninstaller file name folder>` directory, then execute the `tail -f main_upgrade_script.log` shell command. Once the uninstallation process is complete, the system generates a upgrade completed message in the file `main_upgrade_script.log`.

Order of Uninstallation

Uninstall the update in the reverse order that you installed it. That is, first uninstall the update from managed devices, then from Firepower Management Centers.

Uninstall the Update from Firepower Threat Defense Devices in High Availability

Firepower Threat Defense devices in high availability pairs must run the same Firepower version.

You cannot uninstall Firepower Threat Defense devices in high availability. Before you uninstall, you *must* break the high availability. Uninstall each device independently, then reform the high availability pair.

Uninstall the Update from Clustered Firepower Threat Defense Devices

Verify the Firepower Threat Defense devices within the cluster are healthy and operating normally. Determine which member of the cluster is the master and which member is the slave. Uninstall the update from each slave unit one at a time and then uninstall the master unit to avoid dropping traffic. While the slave unit uninstalls, the other slave units and the master unit continue to process traffic. While the master unit uninstalls, one of the slave units becomes the master and continues to process traffic. Once the uninstall completes on the master unit, the temporary master unit returns to the slave state and reforms the cluster.

Uninstall the Update from Clustered 7000 and 8000 Series Devices

Clustered devices must run the same Firepower version. Although the uninstallation process triggers an automatic failover, appliances in mismatched pairs or clusters do not share configuration information, nor do they install or uninstall updates as part of their synchronization. If you need to uninstall an update from redundant appliances, plan to perform the uninstallations in immediate succession.

To ensure continuity of operations, uninstall the update from clustered devices one at a time. First, uninstall the update from the secondary appliance. While the secondary appliance uninstalls, the active appliance continues to forward traffic to the Firepower Management Center. Wait until the uninstallation process is complete, then immediately uninstall the update from the active appliance. While the active appliance uninstalls, the secondary appliance temporarily becomes active and continues to forward traffic to the Firepower Management Center. Once the uninstall completes, the secondary appliances returns and the appliances reform the cluster.

Uninstall the Update from Stacked Devices

All devices in a stack must run the same Firepower version. Uninstalling the update from any of the stacked devices causes the devices in that stack to enter a limited, mixed-version state.

To minimize impact on your deployment, we recommend you uninstall an update from stacked devices simultaneously. The stack resumes normal operation when the uninstallation completes on all devices in the stack.

Uninstall the Update from Devices Deployed Inline

Managed devices do not perform traffic inspection, switching, routing, or related functions while the update is being uninstalled. Depending on how your devices are configured and deployed, the uninstallation process may also affect traffic flow and link state. See [Preupdate Configuration and Event Backups](#) for more information.

Uninstall the Update from Firepower Management Centers in High Availability

Firepower Management Centers in high availability pairs must run the same Firepower version. Although the uninstallation process triggers an automatic failover, appliances in mismatched pairs or clusters do not share configuration information, nor do they install or uninstall updates as part of their synchronization. If you need to uninstall an update from redundant appliances, plan to perform the uninstallations in immediate succession.

To ensure continuity of operations, uninstall the update from paired Firepower Management Centers one at a time. First, pause high availability synchronization and uninstall the update from the secondary Firepower Management Center. Wait until the uninstallation process is complete, then immediately uninstall the update from the primary Firepower Management Center. Once the primary Firepower Management Center uninstallation completes, resume high availability synchronization. At this point, both Firepower Management Centers exist in split brain. Click **Make Me Active** for the Firepower Management Center you want to act as the primary. The Firepower Management Center you do not make active automatically switches to standby mode. Communication between the Firepower Management Center pairs automatically restarts.



Note If the uninstallation process on Firepower Management Centers in a high availability pair fails, do not restart the uninstall or change configurations on its peer. Instead, contact Cisco TAC.

After the Uninstall

After you uninstall the update, there are several steps you should take to ensure that your deployment is performing properly. These include verifying that the uninstall succeeded and that all appliances in your deployment are communicating successfully.

Confirm that uninstalling devices with Firepower software and ASA Firepower or FXOS versions, such as devices running Firepower Threat Defense or ASA Firepower Services, uninstalls both the Firepower and the ASA or FXOS version.

Clustered, stacked, or paired devices reform after the uninstall. Verify the cluster, stack, or paired devices experience healthy activity and communication before deploying any new policies.

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

- [Uninstall 7000 and 8000 Series Managed Devices](#), on page 3
- [Uninstall Firepower NGIPSv Devices](#), on page 3
- [Uninstall ASA FirePOWER Modules Managed By Firepower Management Center](#), on page 4

- [Uninstall Firepower Threat Defense Devices and Firepower Threat Defense Virtual Managed By Firepower Management Center](#), on page 5
- [Uninstall Firepower Management Centers](#), on page 5
- [Uninstall ASA FirePOWER Modules Managed By ASDM](#), on page 6
- [Uninstall from Firepower Threat Defense Devices Managed by Firepower Device Manager](#), on page 7

Uninstall 7000 and 8000 Series Managed Devices

Uninstalling the update results in a device running the previous version. For information on uninstalling a previous version, see to the [Firepower System Release Notes](#) for that version.

Uninstalling the update reboots the device. Appliances do *not* perform traffic inspection, switching, routing, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see [Preupdate Configuration and Event Backups](#).

Step 1 Read and understand "Order of Installation" at [Uninstall Version 6.2.0.x](#).

Step 2 Log into the device as **admin**, through SSH or the virtual console.

Step 3 At the CLI prompt, enter **expert** to access the bash shell.

Step 4 At the bash shell prompt, type **sudo su -**.

Step 5 Type the admin password to continue the process with root privileges.

Step 6 At the prompt, enter the following on a single line: **install_update.pl --detach/var/sf/updates/filename_Patch_Uninstaller-[version]-[build].sh**
The uninstallation process begins.

Note If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.

Step 7 After the uninstallation finishes, the device reboots.

Step 8 Log into the managing Firepower Management Center and choose **Devices > Device Management**. Confirm that the device where you uninstalled the update reflects the software version previous to the one you just uninstalled..

Step 9 Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall Firepower NGIPSv Devices

Uninstalling the update results in a device running the previous version. For information on uninstalling a previous version, see to the [Firepower System Release Notes](#) for that version.

Uninstalling the update reboots the device. Appliances do *not* perform traffic inspection, switching, routing, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see [Preupdate Configuration and Event Backups](#).

Step 1 Read and understand "Order of Installation" at [Uninstall Version 6.2.0.x](#).

- Step 2** Log into the device as **admin**, through SSH or the virtual console.
- Step 3** At the CLI prompt, enter **expert** to access the bash shell.
- Step 4** At the bash shell prompt, type **sudo su -**.
- Step 5** Type the admin password to continue the process with root privileges.
- Step 6** At the prompt, enter the following on a single line: **install_update.pl --detach/var/sf/updates/filename_Patch_Uninstaller-[version]-[build].sh**
The uninstallation process begins.
- Note** If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.
- Step 7** After the uninstallation finishes, the device reboots.
- Step 8** Log into the managing Firepower Management Center and choose **Devices > Device Management**. Confirm that the device where you uninstalled the update reflects the software version previous to the one you just uninstalled..
- Step 9** Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall ASA FirePOWER Modules Managed By Firepower Management Center

Uninstalling the update results in a device running the previous version. For information on uninstalling a previous version, see to the [Firepower System Release Notes](#) for that version.

Uninstalling the update reboots the device. Appliances do *not* perform traffic inspection, switching, routing, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see [Preupdate Configuration and Event Backups](#).

- Step 1** Read and understand "Order of Installation" at [Uninstall Version 6.2.0.x](#).
- Step 2** Log into the device as **admin**, through SSH or the virtual console.
- Step 3** At the CLI prompt, type **session sfr console**.
- Step 4** At the CLI prompt, enter **expert** to access the bash shell.
- Step 5** At the bash shell prompt, type **sudo su -**.
- Step 6** Type the admin password to continue the process with root privileges.
- Step 7** At the prompt, enter the following on a single line: **install_update.pl /var/sf/updates/filename_Patch_Uninstaller-[version]-[build].sh**
The uninstallation process begins.
- Note** If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.
- Step 8** After the uninstallation finishes, the device reboots.
- Step 9** Log into the managing Firepower Management Center and choose **Devices > Device Management**. Confirm that the device where you uninstalled the update reflects the software version previous to the one you just uninstalled..

- Step 10** Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.
-

What to do next

Uninstall Firepower Threat Defense Devices and Firepower Threat Defense Virtual Managed By Firepower Management Center

Uninstalling the update results in a device running the previous version. For information on uninstalling a previous version, see to the [Firepower System Release Notes](#) for that version.

Uninstalling the update reboots the device. Appliances do *not* perform traffic inspection, switching, routing, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see [Preupdate Configuration and Event Backups](#).

- Step 1** Read and understand "Order of Installation" at [Uninstall Version 6.2.0.x](#).
- Step 2** Log into the device as **admin**, through SSH or the virtual console.
- Step 3** For Firepower 4100 Series devices and Firepower 9300 Security Appliances, type **connect module <slot number> console** and then **connect ftd** .
- Step 4** At the CLI prompt, enter **expert** to access the bash shell.
- Step 5** At the bash shell prompt, type **sudo su -**.
- Step 6** Type the admin password to continue the process with root privileges.
- Step 7** At the prompt, enter the following on a single line: **install_update.pl /var/sf/updates/filename_Patch_Uninstaller-[version]-[build].sh**
The uninstallation process begins.
- Note** If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.
- Step 8** After the uninstallation finishes, the device reboots.
- Step 9** Log into the managing Firepower Management Center and choose **Devices > Device Management**. Confirm that the device where you uninstalled the update reflects the software version previous to the one you just uninstalled..
- Step 10** Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.
-

Uninstall Firepower Management Centers

Uninstalling the update results in a device running the previous version. For information on uninstalling a previous version, see to the [Firepower System Release Notes](#) for that version.

-
- Step 1** Read and understand "Order of Installation" at [Uninstall Version 6.2.0.x](#).
- Step 2** On the managing Firepower Management Center, make sure that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.
- Step 3** On the managed device, click the system status icon and view the Tasks tab in the Message Center to make sure there are no tasks in progress.
- Tasks that are running when the uninstallation begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the Tasks tab after the uninstallation completes.
- Step 4** Choose **System > Updates**.
- Step 5** Click the install icon next to the uninstaller that matches the update you want to remove, then confirm that you want to uninstall the update.
- You can monitor the uninstallation progress in the Tasks tab of the Message Center.
- Note** Do *not* use the UI to perform any other tasks until the uninstallation is complete and the device reboots. Before the uninstallation completes, the web interface may become unavailable and the device may log you out. This is expected behavior; log in again to view the Tasks tab. If the uninstallation is still running, do *not* use the web interface until the uninstallation is complete. If you encounter issues with the uninstallation (for example, if the Tasks tab indicates that the update has failed or if the Tasks tab shows no progress for several minutes), do *not* restart the uninstallation. Instead, contact Cisco TAC.
- Step 6** After the uninstallation is complete, the appliance reboots.
- Step 7** Clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.
- Step 8** Log in to the device.
- Step 9** Choose **Help > About** and confirm that the version number reflects the software version previous to the one you just uninstalled.
- Step 10** On the managing Firepower Management Center, verify that the appliances in your deployment successfully communicate with the Firepower Management Center and that there are no issues reported by the health monitor.
-

Uninstall ASA FirePOWER Modules Managed By ASDM

Uninstalling the update results in a device running the previous version. For information on uninstalling a previous version, see to the [Firepower System Release Notes](#) for that version.

Uninstalling the update reboots the device. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see [Preupdate Configuration and Event Backups](#).

- Step 1** Read and understand "Order of Installation" at [Uninstall Version 6.2.0.x](#).
- Step 2** Log into the device as **admin**, through SSH or the virtual console.
- Step 3** At the CLI prompt, type **expert** to access the bash shell.
- Step 4** At the bash shell prompt, type **sudo su -**.
- Step 5** Type the admin password to continue the process with root privileges.

Step 6 At the prompt, enter the following on a single line: **install_update.pl**
/var/sf/updates/filename_Patch_Uninstaller-6.1.0.X-57xxx.sh

The uninstallation process begins.

Note If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.

Step 7 After the uninstallation finishes, the device reboots.

Step 8 Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall from Firepower Threat Defense Devices Managed by Firepower Device Manager

You cannot uninstall Firepower Threat Defense devices managed by Firepower Device Manager. You must reimage the appliance. See the [Firepower Threat Defense Command Reference Guide](#) for more information.

