



Uninstall a Version 6.5.0.x Patch

You can uninstall Firepower patches from:

- FMCs and their managed devices
- ASA FirePOWER modules managed by ASDM

Uninstalling a patch results in an appliance running the version you upgraded from.



Note You *cannot* uninstall a patch from an FTD device managed by FDM. You also cannot uninstall a major version of the Firepower software from any appliance. In those cases, you must freshly install.

For more information, see:

- [Guidelines and Limitations for Uninstalling, on page 1](#)
- [Uninstall Order for HA/Scalability Deployments, on page 3](#)
- [Uninstall Instructions, on page 5](#)
- [Uninstall Packages, on page 10](#)

Guidelines and Limitations for Uninstalling

These important guidelines and limitations apply to uninstall.

Verify Uninstall is Supported for Your Patch

Uninstalling specific patches can cause issues on Firepower appliances, including:

- Inability to deploy configuration changes after uninstall.
- Incompatibilities between the operating system and the Firepower software.
- FSIC (file system integrity check) failure when the appliance reboots, if you patched with security certifications compliance enabled (CC/UCAPL mode).

**Caution**

If security certifications compliance is enabled and the FSIC fails, Firepower software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.

In these cases, if you need to revert to an earlier patch, we recommend you reimage and then upgrade.

The following table lists situations where you should not uninstall.

Table 1: Version 6.5.0.x Patches with Subsequent Issues on Uninstall

Platforms	Uninstalling From	If Upgraded From
FMC/FMCv	6.5.0.1	6.5.0

Uninstall from Devices First, Using the Shell

In FMC deployments, uninstall patches from managed devices first. We recommend that FMCs run a higher version than their managed devices.

To uninstall a device patch, you must use the Linux shell, also called expert mode. This means that you uninstall from devices both *individually* and *locally*. In other words:

- You cannot batch-uninstall patches from clustered, stacked, or high availability (HA) Firepower devices, or from clustered or failover ASA with FirePOWER Services devices. To plan an uninstall order that minimizes disruption, see [Uninstall Order for HA/Scalability Deployments, on page 3](#).
- You cannot use an FMC, ASDM, or FDM to uninstall a patch from a device, nor can you use the local web interface on a 7000/8000 series device.
- You cannot use an FMC user account to log into and uninstall the patch from one of its managed devices. Firepower appliances maintain their own user accounts.
- You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. If you disabled shell access, you cannot uninstall device patches. Contact Cisco TAC to reverse the device lockdown.

Uninstall from FMCs After Devices

Uninstall patches from FMCs after you uninstall from their managed devices. As with upgrade, you must uninstall from high availability FMCs one at a time; see [Uninstall Order for HA/Scalability Deployments, on page 3](#).

We recommend you use the FMC web interface to uninstall FMC patches. You must have Administrator access. If you cannot use the web interface, you can use the Linux shell as either the `admin` user for the shell, or as an external user with shell access. If you disabled shell access, contact Cisco TAC to reverse the FMC lockdown.

Verify NTP Synchronization

Before you uninstall, make sure Firepower appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause uninstall failure. In FMC deployments, the Time Synchronization Status health module does alert if clocks are out of sync by more than 10 seconds, but you should still check manually.

To check time:

- FMC: Choose **System > Configuration > Time**.
- Devices: Use the **show time** CLI command.

Appliance Access

Firepower devices can stop passing traffic during the uninstall (depending on interface configurations), or if the uninstall fails. Before you uninstall a patch from a Firepower device, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In Firepower Management Center deployments, you should also be able to access the FMC management interface without traversing the device.

Disable ASA REST API on ASA FirePOWER Devices

Before you uninstall an ASA FirePOWER patch, make sure the ASA REST API is disabled. Otherwise, the uninstall could fail. From the ASA CLI: `no rest api agent`. You can reenable after the uninstall: `rest-api agent`.

Unresponsive Uninstalls

Do *not* deploy changes to or from, manually reboot, or shut down an uninstalling appliance. Do *not* restart an uninstall in progress. The uninstall process may appear inactive at times; this is expected. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

A failed uninstall may require a reimage, which returns most settings to factory defaults. For this reason, we *strongly* recommend you back up event and configuration data to an external location before you reimage.

Traffic Flow, Inspection, and Device Behavior

Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. We *strongly* recommend performing any uninstall in a maintenance window or at a time when any interruption will have the least impact on your deployment. For more information, see [Traffic Flow, Inspection, and Device Behavior](#).

Uninstall Order for HA/Scalability Deployments

You uninstall patches from Firepower appliances individually, even those that you upgraded as a unit. Especially in high availability (HA) and scalability deployments, you should plan an uninstall order that minimizes disruption. Unlike upgrade, the system does not do this for you. The tables below outline uninstall order for HA/scalability deployments.

Note that in most cases, you will:

- Uninstall from the secondary/standby/slave units first, then the primary/active/master.
- Uninstall one at a time. Wait until the patch has fully uninstalled from one unit before you move on to the next unit.

Table 2: Uninstall Order for FMCs in HA

FMC Deployment	Uninstall Order
FMC high availability	<p>With synchronization paused, which is a state called <i>split-brain</i>, uninstall from FMC peers one at a time. Do not make or deploy configuration changes while the pair is split-brain.</p> <ol style="list-style-type: none"> 1. Pause synchronization (enter split-brain). 2. Uninstall from the standby. 3. Uninstall from the active. 4. Restart synchronization (exit split-brain).

Table 3: Uninstall Order for FTD devices in HA or Clusters

FTD Deployment	Uninstall Order
FTD high availability	<p>You cannot uninstall a patch from FTD devices configured for high availability. You must break high availability first.</p> <ol style="list-style-type: none"> 1. Break high availability. 2. Uninstall from the former standby. 3. Uninstall from the former active. 4. Reestablish high availability.
FTD cluster	<p>Uninstall from one unit at a time, leaving the master unit for last. Clustered units operate in maintenance mode while the patch uninstalls.</p> <ol style="list-style-type: none"> 1. Uninstall from the slave modules one at a time. 2. Make one of the slave modules the new master module. 3. Uninstall from the former master.

Table 4: Uninstall Order for ASA with FirePOWER Services Devices in ASA Failover Pairs/Clusters

ASA Deployment	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	<p>Always uninstall from the standby.</p> <ol style="list-style-type: none"> 1. Uninstall from the ASA FirePOWER module on the standby ASA device. 2. Fail over. 3. Uninstall from the ASA FirePOWER module on the new standby ASA device.

ASA Deployment	Uninstall Order
ASA active/active failover pair, with ASA FirePOWER	<p>Make both failover groups active on the unit you are not uninstalling.</p> <ol style="list-style-type: none"> 1. Make both failover groups active on the primary ASA device. 2. Uninstall from the ASA FirePOWER module on the secondary ASA device. 3. Make both failover groups active on the secondary ASA device. 4. Uninstall from the ASA FirePOWER module on the primary ASA device.
ASA cluster, with ASA FirePOWER	<p>Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the master unit for last.</p> <ol style="list-style-type: none"> 1. On a slave unit, disable clustering. 2. Uninstall from the ASA FirePOWER module on that unit. 3. Reenable clustering. Wait for the unit to rejoin the cluster. 4. Repeat for each slave unit. 5. On the master unit, disable clustering. Wait for a new master to take over. 6. Uninstall from the ASA FirePOWER module on the former master. 7. Reenable clustering.

Uninstall Instructions

The following sections explain how to uninstall Firepower patches from eligible appliances.

Uninstall from a Standalone FMC

Use this procedure to uninstall a patch from a standalone Firepower Management Center, including Firepower Management Center Virtual.

Before you begin

Uninstall patches from managed devices. We recommend that FMCs run a higher version than their managed devices.

Step 1 Deploy to managed devices whose configurations are out of date.

Deploying before you uninstall reduces the chance of failure.

Step 2 Perform prechecks.

- Check health: Use the Message Center on the FMC (click the System Status icon on the menu bar). Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

- Running tasks: Also in the Message Center, make sure essential tasks are complete. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 3 Choose **System > Updates**.

Step 4 Click the Install icon next to the uninstall package for the FMC, then choose the FMC.

If you do not have the correct uninstall package, contact Cisco TAC.

Step 5 Click **Install** to begin the uninstall.

Confirm that you want to uninstall and reboot the FMC.

Step 6 Monitor progress in the Message Center until you are logged out.

Do not make configuration changes or deploy to any device while the patch is uninstalling. Even if the Message Center shows no progress for several minutes or indicates that the uninstall has failed, do *not* restart the uninstall or reboot the FMC. Instead, contact Cisco TAC.

Step 7 Log back into the FMC after the patch uninstalls and the FMC reboots.

Step 8 Verify success.

Choose **Help > About** to display current software version information.

Step 9 Use the Message Center to recheck deployment health.

Step 10 Redeploy configurations.

Uninstall from High Availability FMCs

Use this procedure to uninstall a patch from a Firepower Management Center in a high availability pair.

You uninstall from peers one at a time. With synchronization paused, first uninstall from the standby, then the active. When the standby FMC starts the uninstall, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade and uninstall. Do *not* make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization.

Before you begin

Uninstall patches from managed devices. We recommend that FMCs run a higher version than their managed devices.

Step 1 On the active FMC, deploy to managed devices whose configurations are out of date.

Deploying before you uninstall reduces the chance of failure.

Step 2 Use the Message Center to check deployment health before you pause synchronization.

Click the System Status icon on the FMC menu bar to display the Message Center. Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 3 Pause synchronization.

a) Choose **System > Integration**.

- b) On the **High Availability** tab, click **Pause Synchronization**.

Step 4 Uninstall the patch from the FMCs one at a time—first the standby, then the active.

Follow the instructions in [Uninstall from a Standalone FMC, on page 5](#), but omit the initial deploy, and stop after you verify update success on each FMC. In summary, for each FMC:

- Perform prechecks (health, running tasks).
- On the **System > Updates** page, uninstall the patch.
- Monitor progress until you are logged out, then log back in when you can.
- Verify uninstall success.

Do *not* make or deploy configuration changes while the pair is split-brain.

Step 5 On the FMC you want to make the active peer, restart synchronization.

- Choose **System > Integration**.
- On the **High Availability** tab, click **Make-Me-Active**.
- Wait until synchronization restarts and the other FMC switches to standby mode.

Step 6 Use the Message Center to recheck deployment health.

Step 7 Redeploy configurations.

Uninstall from Any Device (FMC Managed)

Use this procedure to uninstall a patch from a *single* managed device in a Firepower Management Center deployment. This includes physical and virtual devices, security modules, and ASA FirePOWER modules.

Before you begin

- Make sure you are uninstalling from the correct device, especially in HA/scalability deployments. See [Uninstall Order for HA/Scalability Deployments, on page 3](#).
- For ASA FirePOWER modules, make sure the ASA REST API is disabled. From the ASA CLI: `no rest api agent`. You can reenable after the uninstall: `rest-api agent`.

Step 1 If the device's configurations are out of date, deploy now from the FMC.

Deploying before you uninstall reduces the chance of failure.

Exception: Do not deploy to mixed-version stacks, clusters, or HA pairs. In an HA/scalability deployment, deploy before you uninstall from the first device, but then not again until you have uninstalled the patch from all members.

Step 2 Perform prechecks.

- Check health:** Use the Message Center on the FMC (click the System Status icon on the menu bar). Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
- Running tasks:** Also in the Message Center, make sure essential tasks are complete. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

- Step 3** Access the Firepower CLI on the device. Log in as `admin` or another Firepower CLI user with configuration access. You can either SSH to the device's management interface (hostname or IP address) or use the console. If you use the console, some devices default to the operating system CLI, and require an extra step to access the Firepower CLI.

Firepower 1000/2100 series	<code>connect ftd</code>
Firepower 4100/9300 chassis	<code>connect module <i>slot_number</i> console, then connect ftd</code> (first login only)
ASA FirePOWER	<code>session sfr</code>

- Step 4** At the Firepower CLI prompt, use the `expert` command to access the Linux shell.

- Step 5** Run the `uninstall` command, entering your password when prompted.

```
sudo install_update.pl --detach /var/sf/updates/uninstall_package_name
```

The package name varies by platform; see [Uninstall Packages, on page 10](#). Do not untar signed (.tar) packages.

Unless you are running the `uninstall` from the console, use the `--detach` option to ensure the `uninstall` does not stop if your user session times out. Otherwise, the `uninstall` runs as a child process of the user shell. If your connection is terminated, the process is killed, the check is disrupted, and the appliance may be left in an unstable state.

Caution The system does *not* ask you to confirm that you want to uninstall. Entering this command starts the `uninstall`, which includes a device reboot. Interruptions in traffic flow and inspection during an `uninstall` are the same as the interruptions that occur during an upgrade. Make sure you are ready.

- Step 6** Monitor the `uninstall`.

If you did not detach the `uninstall`, progress is displayed on the console or terminal. If you did detach, you can use `tail` or `tailf` to display logs:

- FTD devices: `tail /ngfw/var/log/sf/update.status`
- All other devices: `tail /var/log/sf/update.status`

- Step 7** Verify success.

After the patch uninstalls and the device reboots, confirm that the device has the correct software version. On the FMC, choose **Devices > Device Management**.

- Step 8** Use the Message Center to recheck deployment health.

- Step 9** Redeploy configurations.

Exception: In a HA/scalability deployment, do *not* deploy to mixed-version stacks, clusters, or HA pairs. Deploy only after you repeat this procedure for all members.

What to do next

- For HA/scalability deployments, repeat this procedure for each device in your planned sequence. Then, make any final adjustments. For example, in an FTD HA deployment, reestablish HA after you `uninstall` from both peers.

- For ASA FirePOWER modules, reenable the ASA REST API if you disabled it earlier. From the ASA CLI: `rest-api agent`.

Uninstall from ASA FirePOWER (ASDM Managed)

Use this procedure to uninstall a patch from a locally managed ASA FirePOWER module. If you manage ASA FirePOWER with an FMC, see [Uninstall from Any Device \(FMC Managed\)](#), on page 7.

Before you begin

- Make sure you are uninstalling from the correct device, especially in ASA failover/cluster deployments. See [Uninstall Order for HA/Scalability Deployments](#), on page 3.
- Make sure the ASA REST API is disabled. From the ASA CLI: `no rest api agent`. You can reenable after the uninstall: `rest-api agent`.

Step 1 If the device's configurations are out of date, deploy now from ASDM.

Deploying before you uninstall reduces the chance of failure.

Step 2 Perform prechecks.

- System status: Choose **Monitoring** > **ASA FirePOWER Monitoring** > **Statistics** and make sure everything is as expected.
- Running tasks: Choose **Monitoring** > **ASA FirePOWER Monitoring** > **Tasks** and make sure essential tasks are complete. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 3 Access the Firepower CLI on the ASA FirePOWER module. Log in as `admin` or another Firepower CLI user with configuration access.

You can either SSH to the module's management interface (hostname or IP address) or use the console. If you use the console, note that ASA 5585-X series devices have a dedicated ASA FirePOWER console port. On other ASA models, the console port defaults to the ASA CLI and you must use the `session sfr` command to access the Firepower CLI.

Step 4 At the Firepower CLI prompt, use the `expert` command to access the Linux shell.

Step 5 Run the uninstall command, entering your password when prompted.

```
sudo install_update.pl --detach
/var/sf/updates/Cisco_Network_Sensor_Patch_Uninstaller-version-build.sh.REL.tar
```

Do not untar signed (.tar) packages.

Unless you are running the uninstall from the console, use the `--detach` option to ensure the uninstall does not stop if your user session times out. Otherwise, the uninstall runs as a child process of the user shell. If your connection is terminated, the process is killed, the check is disrupted, and the appliance may be left in an unstable state.

Caution The system does *not* ask you to confirm that you want to uninstall. Entering this command starts the uninstall, which includes a device reboot. Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. Make sure you are ready.

Step 6 Monitor the uninstall.

If you did not detach the uninstall, progress is displayed on the console or terminal. If you did detach, you can use `tail` or `tailf` to display logs:

```
tail /var/log/sf/update.status
```

Do not deploy configurations to the device while the patch is uninstalling. Even if the log shows no progress for several minutes or indicates that the uninstall has failed, do not restart the uninstall or reboot the device. Instead, contact Cisco TAC.

Step 7 Verify success.

After the patch uninstalls and the module reboots, confirm that the module has the correct software version. Choose **Configuration > ASA FirePOWER Configurations > Device Management > Device**.

Step 8 Redeploy configurations.

What to do next

- For ASA failover/cluster deployments, repeat this procedure for each device in your planned sequence.
- For ASA FirePOWER modules, reenable the ASA REST API if you disabled it earlier. From the ASA CLI: `rest-api agent`.

Uninstall Packages

When you patch a Firepower appliances, the uninstaller for that patch is automatically created in the upgrade directory:

- `/ngfw/var/sf/updates` on FTD devices
- `/var/sf/updates` on the FMC and all other devices (7000/8000 series, ASA FirePOWER, NGIPSv)

If the package is not in the upgrade directory (for example, if you manually deleted it) contact Cisco TAC. Do not untar signed (.tar) packages.

Platform	Package
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Patch_Uninstaller- <i>version-build</i> .sh.REL.tar
Firepower 1000 series	Cisco_FTD_SSP_FP1K_Patch_Uninstaller- <i>version-build</i> .sh.REL.tar
Firepower 2100 series	Cisco_FTD_SSP_FP2K_Patch_Uninstaller- <i>version-build</i> .sh.REL.tar
Firepower 4100/9300 chassis	Cisco_FTD_SSP_Patch_Uninstaller- <i>version-build</i> .sh.REL.tar
ASA 5500-X series with FTD ISA 3000 with FTD FTDv	Cisco_FTD_Patch_Uninstaller- <i>version-build</i> .sh.REL.tar

Platform	Package
Firepower 7000/8000 series	Cisco_Firepower_NGIPS_Appliance_Patch_Uninstaller- <i>version-build</i> .sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Patch_Uninstaller- <i>version-build</i> .sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Patch_Uninstaller- <i>version-build</i> .sh.REL.tar

