

Uninstall a Patch

In Firepower Management Center and ASDM deployments, you can uninstall most patches. Uninstalling returns you to the version you upgraded from, and does not change configurations.

Uninstall is not supported for Firepower Device Manager. Do not attempt to uninstall a hotfix. Instead, contact Cisco TAC.

- Patches That Support Uninstall, on page 1
- Guidelines for Uninstalling Patches, on page 2
- Uninstall Order for HA/Scalability Deployments, on page 2
- Uninstall Instructions, on page 4
- Uninstall Packages, on page 9

Patches That Support Uninstall

Uninstalling specific patches can cause issues, *even when the uninstall itself succeeds*. These issues include:

- Inability to deploy configuration changes after uninstall.
- Incompatibilities between the operating system and the 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, the 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.

Version 6.7.0/6.7.x Patches That Support Uninstall

Uninstall is currently supported for all 6.7.0/6.7.x patches.

Guidelines for Uninstalling Patches

Uninstall from Devices First, Using the Shell

The Firepower Management Center must run the *same or newer* version as its managed devices. This means that in FMC deployments, uninstall patches from managed devices first.

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 devices in high availability/scalability deployments. To plan an uninstall order that minimizes disruption, see Uninstall Order for HA/Scalability Deployments, on page 2.
- You cannot use the FMC or ASDM to uninstall a patch from a device.
- You cannot use FMC user accounts to log into and uninstall the patch from one of its managed devices. Devices 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 the FMC After Devices

Uninstall patches from the FMC after you uninstall from 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 2.

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.

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

Table 1: Uninstall Order for FMCs in HA

Deployment	Uninstall Order
FMC high availability	With synchronization paused, which is a state called *split-brain*, uninstall from peers one at a time. Do not make or deploy configuration changes while the pair is split-brain. **1.** Pause synchronization (enter split-brain). **2.** Uninstall from the standby. **3.** Uninstall from the active. **4.** Restart synchronization (exit split-brain).

Table 2: Uninstall Order for FTD devices in HA or Clusters

Deployment	Uninstall Order
Device high availability	You cannot uninstall a patch from devices configured for high availability. You must break high availability first. **1.** Break high availability. **2.** Uninstall from the former standby. **3.** Uninstall from the former active. **4.** Reestablish high availability.
Device cluster	Uninstall from one unit at a time, leaving the control unit for last. Clustered units operate in maintenance mode while the patch uninstalls. **1.** Uninstall from the data modules one at a time. **2.** Make one of the data modules the new control module. **3.** Uninstall from the former control.

Table 3: 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	Always uninstall from the standby. **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	Make both failover groups active on the unit you are not uninstalling. **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	Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the control unit for last. **1.** On a data 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 data unit. **5.** On the control unit, disable clustering. Wait for a new control unit to take over. **6.** Uninstall from the ASA FirePOWER module on the former control unit. **7.** Reenable clustering.

Uninstall Instructions

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 4, but omit the initial deploy, and stop after you verify update success on each FMC. In summary, for each FMC:

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

a) Choose **System** > **Integration**.
b) On the **High Availability** tab, click **Make-Me-Active**.
c) 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 2.

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 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 series	`connect ftd`
Firepower 2100 series	`connect ftd`
Firepower 4100/9300	`connect module` *`slot_number`* `console`, then `connect ftd` (first login only)
ASA FirePOWER	`session sfr`

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/uninstaller_name
```

When you patch a Firepower appliance, an easily identifiable uninstaller for that patch is automatically created in the upgrade directory; see Uninstall Packages, on page 9.

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 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.

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 6.

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 2.

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. Note that 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.

Uninstall Packages

Patch uninstallers are named like upgrade packages, but have 'Patch_Uninstaller' instead of 'Patch' in the file name. When you patch a Firepower appliance, the uninstaller for that patch is automatically created in the upgrade directory:

- `/ngfw/var/sf/updates` on Firepower Threat Defense devices
- `/var/sf/updates` on the Firepower Management Center and NGIPS devices (ASA FirePOWER, NGIPSv)

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