Revert or Uninstall the Upgrade

If an upgrade succeeds but the system does not function to your expectations, you may be able to revert or uninstall:

- Revert is supported for major and maintenance upgrades to threat defense.
- Uninstall is supported for patches to threat defense and to the management center.

If this will not work for you and you still need to return to an earlier version, you must reimage.

Revert Threat Defense

Reverting threat defense returns the software to its state just before the last major or maintenance upgrade. Reverting after patching necessarily removes patches as well. You must enable revert when you upgrade the device, so the system can save a revert snapshot.

About Reverting Threat Defense

Reverted Configurations

Configurations that are reverted include:

- Snort version.
- Device-specific configurations.

  General device settings, routing, interfaces, inline sets, DHCP, SNMP — anything you configure on the **Devices** > **Device Management** page.
- Objects used by your device-specific configurations.

  These include access list, AS path, key chain, interface, network, port, route map, and SLA monitor objects. If you edited these objects after you upgraded the device, the system creates new objects or configure object overrides for the reverted device to use. This allows your other devices to continue handling traffic according to their current configuration.

After a successful revert, we recommend you examine the objects used by the reverted device and make any necessary adjustments.

Configurations Not Reverted

Configurations that are not reverted include:

- Shared policies that can be used by multiple devices; for example, platform settings or access control policies.

  A successfully reverted device is marked out-of-date and you should redeploy configurations.

- For the Firepower 4100/9300, interface changes made using the Secure Firewall chassis manager or the FXOS CLI.

  Sync interface changes after a successful revert.

- For the Firepower 4100/9300, FXOS and firmware.

  If you are required to run the recommended combination of FXOS and threat defense, you may need a full reimage; see Revert Guidelines for Threat Defense, on page 2.

Revert Guidelines for Threat Defense

System Requirements

Reverting threat defense requires Version 7.1+ on the device and the management center. For example, even though a Version 7.1 management center can manage a device as far back as Version 6.5, and even though you can use that Version 7.1 management center to upgrade a device to intermediate versions (6.6, 6.7, 7.0), revert is not supported until you upgrade the device to Version 7.1.

Revert is not supported for:

- Patches and hotfixes
- Threat defense container instances
- Management centers

Reverting High Availability or Clustered Devices

When you use the management center web interface to revert threat defense, you cannot select individual high availability units or clustered nodes.

Revert is more successful when all units/nodes are reverted simultaneously. When you initiate revert from the management center, the system automatically does this. If you need to use the device CLI, do this manually—open sessions with all units/nodes, verify that revert is possible on each, then start the processes at the same time. Simultaneous revert means that interruptions to traffic flow and inspection depend on interface configurations only, as if every device were standalone.

Note that revert is supported for fully and partially upgraded groups. In the case of a partially upgraded group, the system removes the upgrade from the upgraded units/nodes only. Revert will not break high availability or clusters, but you can break a group and revert its newly standalone devices.

Revert Does Not Downgrade FXOS

For the Firepower 4100/9300, major threat defense versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of threat defense, you may be running a non-recommended version of FXOS (too new).

Although newer versions of FXOS are backwards compatible with older threat defense versions, we do perform enhanced testing for the recommended combinations. You cannot manually downgrade FXOS, so if you find yourself in this situation and you want to run a recommended combination, you will need a full reimage.

Scenarios Preventing Revert

If you attempt to revert in any of these situations, the system displays an error.

Table 1: Scenarios Preventing Revert

Scenario	Solution
Revert snapshot is not available because: • You did not enable revert when you upgraded the device. • You deleted the snapshot from either the management center or the device, or it expired. • You upgraded the device with a different management center.	None. If you think you might need to revert after a successful upgrade, use **System** (⚙) > **Updates** to upgrade threat defense. This is the only way to set the **Enable revert after successful upgrade** option, and is in contrast to our usual recommendation to use the threat defense upgrade wizard. The revert snapshot is saved on the management center *and* the device for thirty days, after which it is automatically deleted and you can no longer revert. You can manually delete the snapshot from either appliance to save disk space, but this removes your ability to revert.
Last upgrade failed.	Return the device to its pre-upgrade state by canceling the upgrade. Or, fix the issues and try again. Revert is for situations where the upgrade succeeds, but the upgraded system does not function to your expectations. Reverting is not the same as canceling a failed or in-progress upgrade. If you cannot revert or cancel, you will have to reimage.
Management access interface changed since the upgrade.	Switch it back and try again.
Clusters where the units were upgraded from different versions.	Remove units until all match, reconcile cluster members, then revert the smaller cluster. You may also be able to revert the newly standalone units.
Clusters where one or more units were added to the cluster after upgrade.	Remove the new units, reconcile cluster members, then revert the smaller cluster. You may also be able to revert the newly standalone units.
Clusters where the management center and FXOS identify a different number of cluster units.	Reconcile cluster members and try again, although you may not be able to revert all units.

Revert Threat Defense with Management Center

You must use the management center to revert the device, unless communications between the management center and device are disrupted. In those cases, you can use the **upgrade revert** CLI command on the device. To see what version the system will revert to, use **show upgrade revert-info**.

Caution Reverting from the CLI can cause configurations between the device and the management center to go out of sync, depending on what you changed post-upgrade. This can cause further communication and deployment issues.

Threat Defense History:

- 7.1: Initial support.

Before you begin

- Make sure revert is supported. Read and understand the guidelines.
- Back up to a secure external location. A failed revert may require a reimage, which returns most settings to factory defaults.

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device you want to revert, click **More** (⋮) and select **Revert Upgrade**.

With the exception of high availability pairs and clusters, you cannot select multiple devices to revert.

Step 3 Confirm that you want to revert and reboot.

Interruptions to traffic flow and inspection during revert depend on interface configurations only, as if every device were standalone. This is because even in high availability/scalability deployments, the system reverts all units simultaneously.

Step 4 Monitor revert progress.

In high availability/scalability deployments, traffic flow and inspection resume when the first unit comes back online. If the system shows no progress for several minutes or indicates that the revert has failed, contact Cisco TAC.

Step 5 Verify revert success.

After the revert completes, choose **Devices** > **Device Management** and confirm that the devices you reverted have the correct software version.

Step 6 (Firepower 4100/9300) Sync any interface changes you made to threat defense logical devices using the chassis manager or the FXOS CLI.

On the management center, choose **Devices** > **Device Management**, edit the device, and click **Sync**.

Step 7 Complete any other necessary post-revert configuration changes.

For example, if you edited objects used by device-specific configurations after you upgraded the device, the system creates new objects or configures object overrides for the reverted device to use. We recommend you examine the objects used by the reverted device and make any necessary adjustments.

Step 8 Redeploy configurations to the devices you just reverted.

A successfully reverted device is marked out-of-date. Because the device will be running an older version, newer configurations may not be supported even after a successful deploy.

Uninstall a Patch

Uninstalling a patch returns you to the version you upgraded from, and does not change configurations. Because the management center must run the same or newer version as its managed devices, uninstall patches from devices first. Uninstall is not supported for hotfixes.

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 7.3 Patches That Support Uninstall

Uninstall is currently supported for all Version 7.3 patches.

Version 6.7 Patches That Support Uninstall

Uninstall is currently supported for all Version 6.7 patches.

Uninstall Order for High Availability/Scalability

In high availability/scalability deployments, minimize disruption by uninstalling from one appliance at a time. Unlike upgrade, the system does not do this for you. Wait until the patch has fully uninstalled from one unit before you move on to the next.

Table 2: Uninstall Order for Management Center High Availability

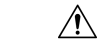
Configuration	Uninstall Order
Management Center high availability	With synchronization paused, which is a state called *split-brain*, uninstall from peers one at a time. Do not make or deploy configuration changes while the pair is split-brain. **1.** Pause synchronization (enter split-brain). **2.**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

Table 3: Uninstall Order for Threat Defense High Availability and Clusters

Configuration	Uninstall Order
Threat Defense 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.
Threat Defense 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.

Uninstall Threat Defense Patches

Use the Linux shell (*expert mode*) to uninstall patches. You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. You cannot use a management center user account. If you disabled shell access, contact Cisco TAC to reverse the lockdown.



Caution Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

Before you begin

- Break threat defense high availability pairs; see Uninstall Order for High Availability/Scalability, on page 5.
- Make sure your deployment is healthy and successfully communicating.

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

Deploying before you uninstall reduces the chance of failure. Make sure the deployment and other essential tasks 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 2 Access the threat defense CLI on the device. Log in as `admin` or another 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 threat defense CLI, as listed in the following table.

Firepower 1000 series	`connect ftd`
Firepower 2100 series	`connect ftd`
Secure Firewall 3100 series	`connect ftd`
Firepower 4100/9300	`connect module` *`slot_number`* `console`, then `connect ftd` (first login only)

Step 3 Use the `expert` command to access the Linux shell.

Step 4 Verify the uninstall package is in the upgrade directory.

```
ls /var/sf/updates
```

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch a device, the uninstaller for that patch is automatically created in the upgrade directory. If the uninstaller is not there, contact Cisco TAC.

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

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

Caution The system does *not* ask you to confirm. 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. Note that using the `--detach` option ensures the uninstall process is not killed if your SSH session times out, which can leave the device in an unstable state.

Step 6 Monitor the uninstall until you are logged out.

For a detached uninstall, use `tail` or `tailf` to display logs:

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

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

After the uninstall completes, confirm that the devices have the correct software version. On the management center, choose **Devices** > **Device Management**.

Step 8 In high availability/scalability deployments, repeat steps 2 through 6 for each unit.

For clusters, never uninstall from the control unit. After you uninstall from all the data units, make one of them the new control, then uninstall from the former control.

Step 9 Redeploy configurations.

Exception: Do not deploy to mixed-version high availability pairs or device clusters. Deploy before you uninstall from the first device, but not again until you have uninstalled the patch from all group members.

What to do next

- For high availability, reestablish high availability.
- For clusters, if you have preferred roles for specific devices, make those changes now.

Uninstall Standalone Management Center Patches

We recommend you use the web interface to uninstall management center patches. 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 lockdown.

Caution Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

Before you begin

- If uninstalling will put the management center at a lower patch level than its managed devices, uninstall patches from the devices first.
- Make sure your deployment is healthy and successfully communicating.

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

Deploying before you uninstall reduces the chance of failure.

Step 2 Under Available Updates, click the **Install** icon next to the uninstall package, then choose the management center.

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch the management center, the uninstaller for that patch is automatically created. If the uninstaller is not there, contact Cisco TAC.

Step 3 Click **Install**, then confirm that you want to uninstall and reboot.

You can monitor uninstall progress in the Message Center until you are logged out.

Step 4 Log back in when you can and verify uninstall success.

If the system does not notify you of the uninstall's success when you log in, choose **Help** > **About** to display current software version information.

Step 5 Redeploy configurations to all managed devices.

Uninstall High Availability Management Center Patches

We recommend you use the web interface to uninstall management center patches. 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 lockdown.

Uninstall from high availability peers one at a time. With synchronization paused, first uninstall from the standby, then the active. When the standby 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.

Caution Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization. Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

Before you begin

- If uninstalling will put the management centers at a lower patch level than their managed devices, uninstall patches from the devices first.
- Make sure your deployment is healthy and successfully communicating.

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

Deploying before you uninstall reduces the chance of failure.

Step 2 On the active management center, pause synchronization.

a) Choose **Integration** > **Other Integrations**.
b) On the **High Availability** tab, click **Pause Synchronization**.

Step 3 Uninstall the patch from peers one at a time — first the standby, then the active.

Follow the instructions in Uninstall Standalone Management Center Patches , on page 8, but omit the initial deploy, stopping after you verify uninstall success on each peer. In summary, for each peer:

a) On the **System** > **Updates** page, uninstall the patch.
b) Monitor progress until you are logged out, then log back in when you can.
c) Verify uninstall success.

Step 4 On the management center you want to make the active peer, restart synchronization.

a) Choose **Integration** > **Other Integrations**.
b) On the **High Availability** tab, click **Make-Me-Active**.

c) Wait until synchronization restarts and the other management center switches to standby mode.

Step 5 Redeploy configurations to all managed devices.