Revert Firewall Threat Defense

If an upgrade succeeds but the system does not function to your expectations, you may be able to return to the previous version.

Revert vs Uninstall

Whether you revert or uninstall depends on the release type.

Table 1: Revert vs Uninstall

	Revert	Uninstall
Releases	First-digit (major), second-digit (major or minor), and third-digit (maintenance) upgrades to Version 7.2.x–10.0.x. **Note** Before Version 10.0, second-digit releases are called *major* releases. In Version 10.0+ they are called *minor* releases. Third-digit releases are always maintenance releases. You can revert all of these, regardless of label.	Patches (fourth-digit upgrades) to Version 10.0 and earlier.
Details	Returns the software to its state just before the last upgrade (a *snapshot*). For details, see Reverted Configurations, on page 4.	Returns the software to the version you patched from. Does not change configurations.
Restrictions	Not supported for container instances or the Secure Firewall 200. For more scenarios that prevent revert, see Scenarios Preventing Revert, on page 3.	For scenarios where uninstall is not supported or recommended, see the Uninstall Guidelines, on page 6.
Revert/Uninstall From	Use **Devices** > **Device Management** to revert Firewall Threat Defense upgrades.	Use expert mode (CLI) on the device to uninstall Firewall Threat Defense patches.

Example: Revert vs Uninstall

Reverting after patching also removes the patch. For example:

1. Upgrade Firewall Threat Defense from Version 7.2.0 → 7.2.5.
2. Patch from Version 7.2.5 → 7.2.5.2.
3. You can now either:
   - Uninstall the patch to go back to Version 7.2.5.

     This removes the patch only.
   - Revert the upgrade to go back to Version 7.2.0.

     This removes the patch and the maintenance release.

Revert Firewall Threat Defense Upgrades

Revert Guidelines

This section discusses general guidelines for revert. To check for version-specific revert issues, see the release notes: https://cisco.com/go/fmc-ftd-release-notes.

Reverting High Availability or Clustered Devices

When you use the Cloud-Delivered Firewall Management Center web interface to revert Firewall 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 Cloud-Delivered Firewall 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 only on interface configurations, as if every device were standalone.

Revert is supported for fully and partially upgraded high availability pairs and clusters. In the case of partial upgrade, the upgraded units/nodes are reverted. Revert will not break high availability or clusters, but you can do it manually and revert the newly standalone devices.

Revert is supported only for high availability pairs and clusters whose members were upgraded as a unit (or where upgrade was attempted as a unit) by the current Cloud-Delivered Firewall Management Center. For example, you cannot upgrade standalone devices, form a high availability pair, and then revert the pair. Similarly, you cannot revert a cluster until all units match (that is, all active cluster units were upgraded as a cluster, together).

Reverting the Firepower 4100/9300

For the Firepower 4100/9300, reverting Firewall Threat Defense does not revert the chassis (FXOS). In multi-instance mode, revert is not supported for container instances.

Major Firewall Threat Defense versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of Firewall Threat Defense, you may be running a non-recommended version of FXOS (too new).

Although newer versions of FXOS are backwards compatible with older Firewall 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.

Reverting the Secure Firewall 3100/4200

For the Secure Firewall 3100/4200 in multi-instance mode, revert is not supported for container instances, so there is no need to revert the chassis. In appliance mode, revert is fully supported.

Scenarios Preventing Revert

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

Table 2: Scenarios Preventing Revert

Scenario	Solution
Lower-memory devices: • Container instances • Secure Firewall 200	None. Some devices do not have enough memory to store a revert snapshot, so revert is not supported.
Revert snapshot is not available because: • You did not enable revert when you upgraded the device. • You deleted the snapshot from either the Cloud-Delivered Firewall Management Center or the device, or it expired. • You upgraded the device with a different Cloud-Delivered Firewall Management Center. • You reverted to the version you are running now (you are trying to perform multiple reverts in succession).	None. The revert snapshot is saved on the Cloud-Delivered Firewall Management Center and the device for 30 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. The system only saves one snapshot. You cannot revert more than once, that is: • Supported: A → B → C → B • Not supported: A → B → C → B → A
Last upgrade failed.	Return the device to its pre-upgrade state by canceling the upgrade. Or, fix the issues and try again. Use revert when an upgrade succeeds but the upgraded device does not function as expected. This 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.

Scenario	Solution
High availability pair formed after either device, or both devices, were upgraded.	Break high availability and revert the newly standalone units, if possible.
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. This includes newly formed clusters using upgraded devices.	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 Cloud-Delivered Firewall 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.

Reverted Configurations

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 Firewall Threat Defense, you may need a full reimage; see Revert Guidelines, on page 2.

Revert a Firewall Threat Defense Upgrade

You must use the Cloud-Delivered Firewall Management Center to revert the device.

Note If communications between the Cloud-Delivered Firewall Management Center and the device are disrupted, use the device CLI to delete the device from management (**configure manager delete**), then revert (**upgrade revert**). Deleting the manager does invalidate the device configuration, but this can still save time over a reimage. You should also use the Cloud-Delivered Firewall Management Center web interface to unregister the stale device. After the revert completes, you can re-register and deploy configurations. To see what version the system will revert to, use **show upgrade revert-info**.

Before you begin

- Make sure revert is supported. Read and understand the guidelines.
- Revisit the Planning Your Upgrade chapter. In general, prepare for reverting an upgrade in the same way you prepared for installing it. It is especially important that you back up to a secure external location. A failed revert may require a reimage, which returns most settings to factory defaults.

Procedure

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/clustered deployments, the system reverts all units simultaneously.

Step 4 Monitor revert progress.

In high availability/clustered 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 Firewall Threat Defense logical devices using the Firewall Chassis Manager or the FXOS CLI.

On the Cloud-Delivered Firewall 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 Firewall Threat Defense Patches

Uninstall Guidelines

This topic discusses general guidelines for uninstall. To check for version-specific uninstall issues, see the upgrade guidelines in the release notes: https://cisco.com/go/fmc-ftd-release-notes.

Uninstalling from High Availability or Clustered Devices

Minimize disruption by uninstalling from one device 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.

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.

Clusters: 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.

Scenarios Preventing or Restricting Uninstall

If you attempt to uninstall in any of these situations, you may have significant issues.

Table 3: Scenarios Preventing or Restricting Uninstall

Scenario	Solution
The release notes say that a specific patch does not support or recommend uninstall.	Uninstalling a patch applies only to the software. After uninstalling a patch that updates the operating system or other components not reversed by the uninstall, you may be unable to deploy configuration changes, or you may experience other incompatibilities between the newer components and the older software. In these cases, we recommend you do not uninstall. Because patches are cumulative, and because uninstalling a patch returns the software to the version you started from, we also recommend against uninstalling later patches if it will take you to a version earlier than the affected patch. For example, if Patch 5 updates the operating system, do not uninstall Patch 5, but also do not uninstall Patch 6+ if you started at Patch 4 or earlier (including the base version). Specific patches that you should not uninstall due to this or any other reason are listed in the release notes. If you need to uninstall one of these patches, contact Cisco TAC.
You are in Security Certifications Compliance (CC/UCAPL) mode.	If a patch updates the operating system and security certifications compliance is enabled, FSIC (file system integrity check) fails when the appliance reboots. The software does not start, remote SSH access is disabled, and you can access the appliance only via local console. Uninstall is not recommended in security certifications compliance mode. If you need to do this, contact Cisco TAC.
You need to uninstall a hotfix or a hotfixed patch.	You must uninstall hotfixes and patches in the exact reverse order from their installation (last in, first out). For example: • Install: Patch A → Hotfix B → Hotfix C → Patch D → Hotfix E • Uninstall: Hotfix E → Patch D → Hotfix C → Hotfix B → Patch A To view your update history, use expert mode: **`cat /etc/sf/patch_history`**. Uninstall is not recommended for hotfixes and hotfixed patches. If you need to do this, contact Cisco TAC.
You reverted to the version you are running now.	None. Upgrading to a major or maintenance release deletes upgrade packages and uninstallers that do not apply to the new version.

Uninstall a Firewall Threat Defense Patch

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 Cloud-Delivered Firewall 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

- Make sure uninstall is supported. Read and understand the guidelines.
- Revisit the Planning Your Upgrade chapter. In general, you should prepare for uninstalling a patch in the same way you prepared for installing it.
- Break high availability pairs.

Procedure

Step 1 If the device's configurations are out of date, deploy now from the Cloud-Delivered Firewall 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 Firewall 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 Firewall Threat Defense CLI, as follows.

ASA 5500-X series ISA 3000	—
Firewall Threat Defense Virtual	—
Firepower 4100/9300	`connect module` *`slot_number`* `console`, then `connect ftd` (first login only)
All other models	`connect ftd`

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 device has the correct software version. On the Cloud-Delivered Firewall Management Center, choose **Devices** > **Device Management**.

Step 8 In high availability and clustered deployments, repeat steps 2 through 7 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.