Revert Threat Defense

If a threat defense upgrade succeeds but the system does not function to your expectations, you may be able to revert. If this will not work for you and you still need to return to an earlier version, you must reimage. You cannot revert the management center.

About Reverting Threat Defense

Reverting threat defense returns the software to its state just before the last upgrade. You must enable revert when you upgrade the device, so the system can save a revert snapshot.

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A successfully reverted device is marked out-of-date and you should redeploy configurations.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

Revert is supported for major and maintenance threat defense upgrades.

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. 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.