# Troubleshooting and Reference



# Troubleshooting High Availability Threat Defense Upgrade

***Table 1: Troubleshooting High Availability Threat Defense Upgrade***

| Issue | Solution |
|---|---|
| Upgrade will not begin without deploying uncommitted changes. | If you get an error message stating that you must deploy all uncommitted changes even though there are none, log into the active unit (remember, you should be upgrading the standby), create some minor change, and deploy. Then, undo the change, redeploy, and try the upgrade again on the standby.<br><br>If this does not work, and the units are running different software versions against recommendations, switch roles to make the standby unit active, then suspend high availability. Deploy from the active/suspended unit, resume high availability, then switch roles to make the active unit the standby again. Upgrade should then work. |
| Deployment from active unit fails during standby upgrade, or causes an application synchronization error. | This can happen if you deploy from the active unit while the standby is upgrading, which is not supported. Proceed with the upgrade despite the error. After you upgrade both units, make any required configuration changes and deploy from the active unit. The error should resolve.<br><br>To avoid these issues, do not make or deploy configuration changes on one unit while the other is upgrading, or to a mixed version pair. |
| Configuration changes made during upgrade are lost. | If you absolutely must make and deploy changes to a mixed version pair, you must make the changes to both units or they will be lost after you upgrade the down-level active unit. |

| Issue | Solution |
|---|---|
| High availability is suspended after upgrade. | After the post-upgrade reboot, high availability is briefly suspended while the system performs some final automated tasks, such as updating libraries and restarting Snort. You are most likely to notice this if you log into the CLI *very* shortly after upgrade. If high availability does not resume on its own after the upgrade fully completes and device manager is available, do it manually:<br>**1.** Log into both the active device and the standby device and check the task lists. Wait until all tasks are finished running on both devices. If you resume high availability too soon, you may have a future issue where failover causes an outage.<br>**2.** Select **Device** > **High Availability**, then select **Resume HA** from the gear menu (⚙). |
| Failover does not occur with a mixed version pair. | Although an advantage of high availability is that you can upgrade your deployment without traffic or inspection interruptions, failover is disabled during the entire upgrade process. That is, not only is failover necessarily disabled when one device is offline (because there is nothing to fail over to—you are essentially already failed over), but failover is also disabled with mixed version pairs. During upgrade is the only time where mixed version pairs are (temporarily) allowed. Schedule upgrades during maintenance windows when they will have the least impact if something goes wrong, and make sure you have enough time to upgrade both devices in that window. |
| Upgrade failed on only one device, or one device was reverted. The pair is now running mixed versions. | Mixed version pairs are not supported for general operations. Either upgrade the down-version device or revert the higher version device. For patches, because revert is not supported, if you cannot successfully upgrade the down-version device you must break high availability, reimage one or both devices, then re-establish high availability. |

# Unresponsive and Failed Threat Defense Upgrades

⚠

**Caution** Do not reboot or shut down at any point during upgrade, even if the system appears inactive. You could place the system in an unusable state and require a reimage.

***Table 2: Unresponsive and Failed Threat Defense Upgrades***

| Issue | Solution |
|---|---|
| Cannot reach the device. | Devices can stop passing traffic during the upgrade or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. |
| Upgrade or patch appears hung/device appears inactive. | If device upgrade status has stopped updating but there is no report of upgrade failure, you can try canceling the upgrade; seeCancel or Retry Threat Defense Upgrades. If you cannot cancel or canceling does not work, contact Cisco TAC. |

| Issue | Solution |
|---|---|
| Upgrade failed. | If an upgrade fails and:<br>• The device reverted to its pre-upgrade state (auto-cancel is enabled), correct any issues and try again from the beginning.<br>• The device is still in maintenance mode, correct any issues and resume the upgrade. Or, cancel and try again later.<br>For more information, see Cancel or Retry Threat Defense Upgrades. If you cannot retry or cancel, or if you continue to have issues, contact Cisco TAC. |
| Patch failed. | You cannot cancel in-progress or failed patches. However, if a patch fails early, for example, during validation stages, the device may remain up and running normally. Simply correct any issues and try again. If a patch fails after the device has entered maintenance mode, contact Cisco TAC. |
| I want to cancel an upgrade. | Canceling reverts the device to its pre-upgrade state. You can cancel failed and in-progress upgrades on the upgrade status page that automatically appears during upgrade. You can also use the **upgrade cancel** CLI command. You cannot cancel patches.<br>If you cannot cancel or canceling does not work, contact Cisco TAC. |
| I want to retry (resume) a failed upgrade. | You can resume an upgrade on the upgrade status page that automatically appears during upgrade. You can also use the **upgrade retry** CLI command.<br>If you continue to have issues, contact Cisco TAC. |
| I want to change what happens when upgrade fails. | Part of the upgrade process is choosing what happens if it fails. This is done with the **Automatically cancel on upgrade failure...** (auto-cancel) option:<br>• Auto-cancel enabled (default): If upgrade fails, the upgrade cancels and the device automatically reverts to its pre-upgrade state. This returns you to normal operations as quickly as possible while you regroup and try again.<br>• Auto-cancel disabled: If upgrade fails, the device remains as it is. This allows you to correct any issues and resume the upgrade.<br>For high availability devices, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. |

# Traffic Flow and Inspection

Schedule maintenance windows when upgrade will have the least impact, considering any effect on traffic flow and inspection.

# Traffic Flow and Inspection for Threat Defense Upgrades

### Software Upgrade

Traffic is dropped while you upgrade. In a high availability deployment, you can minimize disruption by upgrading devices one at a time.

For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.

### Software Revert (Major/Maintenance Releases)

Traffic is dropped while you revert. In a high availability deployment, revert is more successful when you revert both units simultaneously. Traffic flow and inspection resume when the first unit comes back online.

# Traffic Flow and Inspection for Chassis Upgrades

Upgrading FXOS reboots the chassis. For FXOS upgrades to Version 2.14.1+ that include firmware upgrades, the device reboots twice—once for FXOS and once for the firmware.

Even in high availability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time; see Upgrade Order for Threat Defense with Chassis Upgrade and High Availability.

***Table 3: Traffic Flow and Inspection: FXOS Upgrades***

| Threat Defense Deployment | Traffic Behavior | Method |
|---|---|---|
| Standalone | Dropped. | — |
| High availability | Unaffected. | **Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby. |
| | Dropped until one peer is online. | Upgrade FXOS on the active peer before the standby is finished upgrading. |

# Traffic Flow and Inspection when Deploying Configurations

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

# Time and Disk Space

## Time to Upgrade

We recommend you track and record your own upgrade times so you can use them as future benchmarks. The following table lists some things that can affect upgrade time.

**Caution** Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive and Failed Threat Defense Upgrades, on page 2.

*Table 4: Upgrade Time Considerations*

| Consideration | Details |
|---|---|
| Versions | Upgrade time usually increases if your upgrade skips versions. |
| Models | Upgrade time usually increases with lower-end models. |
| Virtual appliances | Upgrade time in virtual deployments is highly hardware dependent. |
| High availability | In a high availability configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair, therefore, takes longer than upgrading a standalone device. |
| Configurations | Upgrade time can increase with the complexity of your configurations and whether/how they are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer. |
| Components | You may need additional time to perform operating system or virtual hosting upgrades, upgrade package transfers, readiness checks, VDB and intrusion rule (SRU/LSP) updates, configuration deployment, and other related tasks. |

## Disk Space to Upgrade

To upgrade, the upgrade package must be on the device. Readiness checks should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails. To check disk space, use the **show disk** CLI command.

# Upgrade Feature History

*Table 5: Version 7.0.0 Features*

| Feature | Details |
|---|---|
| Upgrade readiness check for device manager-managed devices. | You can run an upgrade readiness check on an uploaded threat defense upgrade package before attempting to install it. The readiness check verifies that the upgrade is valid for the system, and that the system meets other requirements needed to install the package. Running an upgrade readiness check helps you avoid failed installations.<br>A link to run the upgrade readiness check was added to the **System Upgrade** section of the **Device** > **Updates** page. |

*Table 6: Version 6.7.0 Features*

| Feature | Details |
|---|---|
| Ability to cancel a failed threat defense software upgrade and to revert to the previous release. | If an threat defense major software upgrade fails or is otherwise not functioning correctly, you can revert to the state of the device as it was when you installed the upgrade.<br>We added the ability to revert the upgrade to the System Upgrade panel in FDM. During an upgrade, the FDM login screen shows the upgrade status and gives you the option to cancel or revert in case of upgrade failure. In the threat defense API, we added the CancelUpgrade, RevertUpgrade, RetryUpgrade, and UpgradeRevertInfo resources.<br>In the threat defense CLI, we added the following commands: **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**. |

*Table 7: Version 6.2.0 Features*

| Feature | Details |
|---|---|
| Upgrade threat defense software through device manager. | You can install software upgrades through device manager. Select **Device** > **Updates**. |