

Reference

- Traffic Flow and Inspection, on page 1
- Time and Disk Space, on page 2
- Upgrade Feature History, on page 3

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 Firewall 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 chassis 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.

Table 1: Traffic Flow and Inspection: FXOS Upgrades

Firewall 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 Troubleshooting Threat Defense Upgrades.

Table 2: 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.

Consideration	Details
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 3: Device Upgrade Feature History

Feature	Minimum Threat Defense	Details
Pre-upgrade readiness check.	7.0.0	You can run a readiness check before upgrade. 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. A link to run the upgrade readiness check was added to the **System Upgrade** section of the **Device** > **Updates** page.

Feature	Minimum Threat Defense	Details
Cancel and revert a failed upgrade.	6.7.0	If a 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. 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 Firewall Threat Defense API, we added the CancelUpgrade, RevertUpgrade, RetryUpgrade, and UpgradeRevertInfo resources. In the Firewall 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**.
Upgrade with Firewall Device Manager.	6.2.0	You can install software upgrades through Firewall Device Manager. Select **Device** > **Updates**.