Upgrade the Software

This chapter provides critical and release-specific information.

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 22.

Table 1: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up the software. Back up FXOS on the Firepower 4100/9300. Back up ASA for ASA FirePOWER.

Planning Phase	Includes
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Check disk space. Deploy configurations. Run readiness checks. Check running tasks. Check deployment health and communications.

Minimum Version to Upgrade

You can upgrade directly to Version 6.3.0 as follows. You do not need to be running any specific patch level.

Table 2: Minimum Version to Upgrade to Version 6.3.0

Platform	Minimum Version
Firepower Management Center	6.1.0
Firepower devices with FMC: • Firepower 2100 series • ASA 5500-X series • ISA 3000 • FTDv • Firepower 7000/8000 series • ASA FirePOWER • NGIPSv	6.1.0

Platform	Minimum Version
Firepower devices with FMC: • Firepower 4100/9300	6.2.3 on FXOS 2.3.1.73 or later build (recommended) 6.1.0 on FXOS 2.4.1.214 or later build (required) If you are running Version 6.1.0 and need to upgrade directly to Version 6.3.0, see Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade, on page 9. However, if you plan to upgrade "past" 6.3.0, we recommend you use Version 6.2.3 on FXOS 2.3.1 as the intermediate version. From Version 6.2.3, you can upgrade as far as Version 6.6.x.
Firepower devices with FDM	6.2.0
ASA FirePOWER with ASDM	6.2.0

New Upgrade Guidelines for Version 6.3.0

This checklist contains upgrade guidelines that are new or specific to Version 6.3.0.

Table 3: Version 6.3.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Renamed Upgrade and Installation Packages, on page 4	FMC Firepower 7000/8000 series NGIPSv	Any	6.3.0+
	Reimaging to Version 6.3+ Disables LOM on Most Appliances, on page 5	FMC (physical) Firepower 7000/8000 series	Any	6.3.0+
	Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 6	FMC Firepower 7000/8000 series NGIPSv	6.2.3 through 6.2.3.4 6.2.2 through 6.2.2.4 6.2.1 6.2.0 through 6.2.0.6 6.1.0 through 6.1.0.6	6.3.0+
	Reporting Data Removed During FTD/FDM Upgrade, on page 6	FTD with FDM	6.2.0 through 6.2.3.x	6.3.0 only
	RA VPN Default Setting Change Can Block VPN Traffic, on page 6	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	TLS/SSL Hardware Acceleration Enabled on Upgrade, on page 7	Firepower 2100 series Firepower 4100/9300	6.1.0 through 6.2.3.x	6.3.0 only
	Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER, on page 7	FMC ASA FirePOWER with ASDM	6.1.0 through 6.2.3.x	6.3.0 only
	Security Intelligence Enables Application Identification, on page 7	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 8	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 8	Any	6.1.0 through 6.2.3.x	6.3.0+
	Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade, on page 9	Firepower 4100/9300	6.1.0.x	6.3.0 only

Renamed Upgrade and Installation Packages

Deployments: FMC, 7000/8000 series, NGIPSv

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3+

The naming scheme (that is, the first part of the name) for upgrade, patch, hotfix, and installation packages changed starting with Version 6.3.0, on select platforms.

Note This change causes issues with reimaging older *physical* appliances: DC750, 1500, 2000, 3500, and 4000, as well as 7000/8000 series devices and AMP models. If you are currently running Version 5.x and need to freshly install Version 6.3.0 or 6.4.0 on one of these appliances, rename the installation package to the "old" name after you download it from the Cisco Support & Download site.

Table 4: Naming Schemes: Upgrade, Patch, and Hotfix Packages

Platform	Naming Schemes
FMC	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_3D_Defense_Center_S3
Firepower 7000/8000 series	**New:** Cisco_Firepower_NGIPS_Appliance **Old:** Sourcefire_3D_Device_S3

Platform	Naming Schemes
NGIPSv	**New:** Cisco_Firepower_NGIPS_Virtual **Old:** Sourcefire_3D_Device_VMware **Old:** Sourcefire_3D_Device_Virtual64_VMware

Table 5: Naming Schemes: Installation Packages

Platform	Naming Schemes
FMC (physical)	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_Defense_Center_M4 **Old:** Sourcefire_Defense_Center_S3
FMCv: VMware	**New:** Cisco_Firepower_Mgmt_Center_Virtual_VMware **Old:** Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	**New:** Cisco_Firepower_Mgmt_Center_Virtual_KVM **Old:** Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 series	**New:** Cisco_Firepower_NGIPS_Appliance **Old:** Sourcefire_3D_Device_S3
NGIPSv	**New:** Cisco_Firepower_NGIPSv_VMware **Old:** Cisco_Firepower_NGIPS_VMware

Reimaging to Version 6.3+ Disables LOM on Most Appliances

Deployments: Physical FMCs, 7000/8000 series devices

Reimaging from: Version 6.0+

Directly to: Version 6.3+

Freshly installing Version 6.3+ now automatically deletes Lights-Out Management (LOM) settings on most appliances, for security reasons. On a few older FMC models, you have the option of retaining LOM settings along with your management network settings.

If you delete network settings during a Version 6.3+ reimage, you *must* make sure you have physical access to the appliance to perform the initial configuration. You cannot use LOM. After you perform the initial configuration, you can reenable LOM and LOM users.

Table 6: Reimage Effect on LOM Settings

Platform	Reimage to Version 6.2.3 or earlier	Reimage to Version 6.3+
MC1600, 2600, 4600 MC1000, 2500, 4500 MC2000, 4000	Never deleted	Always deleted

Platform	Reimage to Version 6.2.3 or earlier	Reimage to Version 6.3+
MC750, 1500, 3500	Deleted if you delete network settings	Deleted if you delete network settings
7000/8000 series	Always deleted	Always deleted

Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv

Deployments: FMC, 7000/8000 series devices, NGIPSv

Upgrading from: Version 6.1.0 through 6.1.0.6, Version 6.2.0 through 6.2.0.6, Version 6.2.1, Version 6.2.2 through 6.2.2.4, and Version 6.2.3 through 6.2.3.4

Directly to: Version 6.3.0+

You cannot run the readiness check on the listed models when upgrading from one of the listed Firepower versions. This occurs because the readiness check process is incompatible with newer upgrade packages.

Table 7: Patches with Readiness Checks for Version 6.3.0+

Readiness Check Not Supported	First Patch with Fix
6.1.0 through 6.1.0.6	6.1.0.7
6.2.0 through 6.2.0.6	6.2.0.7
6.2.1	None. Upgrade to Version 6.2.3.5+.
6.2.2 through 6.2.2.4	6.2.2.5
6.2.3 through 6.2.3.4	6.2.3.5

Reporting Data Removed During FTD/FDM Upgrade

Deployments: Firepower Device Manager

Upgrading from: Version 6.2.x

Directly to: Version 6.3 only

Reporting data for short time periods are removed during the Version 6.3 upgrade. After the upgrade, if you try to query short time ranges on days that fall before the upgrade, the system adjusts your query to match the available data. For example, if you query 1-3 PM for a date, and the system only has 24-hour data, the system reports on the entire day.

RA VPN Default Setting Change Can Block VPN Traffic

Deployments: Firepower Threat Defense configured for remote access VPN

Upgrading from: Version 6.2.x

Directly to: Version 6.3+

Version 6.3 changes the default setting for a hidden option, **sysopt connection permit-vpn**. Upgrading can cause your remote access VPN to stop passing traffic. If this happens, use either of these techniques:

- Create a FlexConfig object that configures the **sysopt connection permit-vpn** command. The new default for this command is **no sysopt connection permit-vpn**.

  This is the more secure method to allow traffic in the VPN, because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic.

- Create access control rules to allow connections from the remote access VPN address pool.

  This method ensures that VPN traffic is inspected and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network.

TLS/SSL Hardware Acceleration Enabled on Upgrade

Deployments: Firepower 2100 series, Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3.0 only

The upgrade process automatically enables TLS/SSL hardware acceleration (sometimes called *TLS crypto acceleration*) on eligible devices. When it was introduced in Version 6.2.3, this feature was disabled by default on Firepower 4100/9300 chassis, and was not available on Firepower 2100 series devices.

Using TLS/SSL hardware acceleration on a managed device that is not decrypting traffic can affect performance. In Version 6.3.0.x, we recommend you disable this feature on devices that are not decrypting traffic.

To disable, use this CLI command:

```
system support ssl-hw-offload disable
```

Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER

Deployments: Firepower Management Center, ASA FirePOWER (locally managed)

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3.0-83

Some Firepower Management Centers and locally (ASDM) managed ASA FirePOWER modules experienced upgrade failures with Version 6.3.0, build 83. This issue was limited to a subset of customers who upgraded from Version 5.4.x. For more information, see CSCvn62123 in the Cisco Bug Search Tool.

A new upgrade package is now available. If you downloaded the Version 6.3.0-83 upgrade package, do not use it. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

Security Intelligence Enables Application Identification

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

In Version 6.3, Security Intelligence configurations enable application detection and identification. If you disabled discovery in your current deployment, the upgrade process may enable it again. Disabling discovery if you don't need it (for example, in an IPS-only deployment) can improve performance.

To disable discovery you must:

- Delete all rules from your network discovery policy.
- Use only simple network-based conditions to perform access control: zone, IP address, VLAN tag, and port. Do not perform any kind of application, user, URL, or geolocation control.
- **(NEW)** Disable network and URL-based Security Intelligence by deleting all whitelists and blacklists from your access control policy's Security Intelligence configuration, including the default Global lists.
- **(NEW)** Disable DNS-based Security Intelligence by deleting or disabling all rules in the associated DNS policy, including the default Global Whitelist for DNS and Global Blacklist for DNS rules.

Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

Upgrading from: Version 6.1.0 through 6.2.3.x, with VDB 299+

Directly to: Version 6.3.0+

If you upgrade while using vulnerability database (VDB) 299 or later, an issue with the upgrade process prevents you from using CIP detection post-upgrade. This includes every VDB released from June 2018 to now, even the latest VDB.

Although we always recommend you update the vulnerability database (VDB) to the latest version after you upgrade, it is especially important in this case.

To check if you are affected by this issue, try to configure an access control rule with a CIP-based application condition. If you cannot find any CIP applications in the rule editor, manually update the VDB.

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

For network variables in an intrusion variable set, any IP addresses you *exclude* must be a subset of the IP addresses you *include*. This table shows you examples of valid and invalid configurations.

Valid	Invalid
Include: 10.0.0.0/8 Exclude: 10.1.0.0/16	Include: 10.1.0.0/16 Exclude: 172.16.0.0/12 Exclude: 10.0.0.0/8

Before Version 6.3.0, you could successfully save a network variable with this type of invalid configuration. Now, these configurations block deploy with the error: `Variable set has invalid excluded values`.

If this happens, identify and edit the incorrectly configured variable set, then redeploy. Note that you may have to edit network objects and groups referenced by your variable set.

Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade

Deployments: Firepower 4100/9300 with FTD

Upgrading from: Version 6.1.x on FXOS 2.0.1, 2.1.1, or 2.3.1

Directly to: Version 6.3.0 on FXOS 2.4.1

If your Firepower Management Center is running Version 6.2.3+, we strongly recommend you copy (*push*) Firepower upgrade packages to managed devices before you upgrade. This helps reduce the length of your upgrade maintenance window. For Firepower 4100/9300 with FTD, best practice is to copy before you begin the required companion FXOS upgrade.

Note We recommend that you not upgrade from Version 6.1.0 → 6.3.0. If you are running Version 6.1.0, we recommend upgrading to Version 6.2.3 on FXOS 2.3.1, and proceeding from there. If you do choose to perform this Version 6.1.0 → 6.3.0 upgrade, a push from the FMC before you upgrade FXOS is *required*.

This is because upgrading FXOS to Version 2.4.1 while still running Firepower 6.1.0 causes the device management port to flap, which in turn causes intermittent communication problems between the device and the FMC. Until you upgrade the Firepower software, you may continue to experience management port flaps. You may see 'sftunnel daemon exited' alarms, and any task that involves sustained communications—such as pushing a large upgrade package—may fail.

To upgrade Firepower 4100/9300 with FTD, always follow this sequence:

1. Upgrade the FMC to the target version.
2. Obtain the device upgrade package from the Cisco Support & Download site and upload it to the FMC.
3. Use the FMC to push the upgrade package to the device.
4. After the push completes, upgrade FXOS to the target version.
5. Immediately, use the FMC to upgrade the Firepower software on the device.

Previously Published Upgrade Guidelines

This checklist contains older upgrade guidelines.

Table 8: Version 6.3.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Can Unregister FTD/FDM from CSSM, on page 10	FTD with FDM	6.2.0 through 6.2.2.x	6.2.3 through 6.4.0

✓	Guideline	Platforms	Upgrading From	Directly To
	Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 10	FTD clusters	6.1.0.x	6.2.3 through 6.4.0
	Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 10	FTD with FDM	6.2.0 only	6.2.2 through 6.4.0
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 11	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 11	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0

Upgrade Can Unregister FTD/FDM from CSSM

Deployments: FTD with FDM

Upgrading from: Version 6.2 through 6.2.2.x

Directly to: Version 6.2.3 through 6.4.0

Upgrading a Firepower Threat Defense device managed by Firepower Device Manager may unregister the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 If the device is not registered, click **Register Device**.

Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade

Deployments: Firepower Threat Defense clusters

Upgrading from: Version 6.1.x

Directly to: Version 6.2.3 through 6.4.0

Firepower Threat Defense Version 6.1.x clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in Version 6.2.0).

If you deployed or redeployed a Version 6.1.x cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, remove the site ID (set to `0`) on each unit in FXOS before you upgrade. Otherwise, the units cannot rejoin the cluster after the upgrade.

If you already upgraded, remove the site ID from each unit, then reestablish the cluster. To view or change the site ID, see the Cisco FXOS CLI Configuration Guide.

Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0

Deployments: FTD with FDM, running on a lower-memory ASA 5500-X series device

Upgrading from: Version 6.2.0

Directly to: Version 6.2.2 through 6.4.0

If you are upgrading from Version 6.2.0, the upgrade may fail with an error of: `Uploaded file is not a valid system upgrade file`. This can occur even if you are using the correct file.

If this happens, you can try the following workarounds:

- Try again.
- Use the CLI to upgrade.
- Upgrade to 6.2.0.1 first.

Access Control Can Get Latency-Based Performance Settings from SRUs

Deployments: FMC

Upgrading from: 6.1.x

Directly to: 6.2.0+

New access control policies in Version 6.2.0+ *by default* get their latency-based performance settings from the latest intrusion rule update (SRU). This behavior is controlled by a new **Apply Settings From** option. To configure this option, edit or create an access control policy, click **Advanced**, and edit the Latency-Based Performance Settings.

When you upgrade to Version 6.2.0+, the new option is set according to your current (Version 6.1.x) configuration. If your current settings are:

- Default: The new option is set to **Installed Rule Update**. When you deploy after the upgrade, the system uses the latency-based performance settings from the latest SRU. It is possible that traffic handling could change, depending on what the latest SRU specifies.
- Custom: The new option is set to **Custom**. The system retains its current performance settings. There should be no behavior change due to this option.

We recommend you review your configurations before you upgrade. From the Version 6.1.x FMC web interface, view your policies' Latency-Based Performance Settings as described earlier, and see whether the **Revert to Defaults** button is dimmed. If the button is dimmed, you are using the default settings. If it is active, you have configured custom settings.

'Snort Fail Open' Replaces 'Failsafe' on FTD

Deployments: FTD with FMC

Upgrading from: Version 6.1.x

Directly to: Version 6.2+

In Version 6.2, the Snort Fail Open configuration replaces the Failsafe option on FMC-managed Firepower Threat Defense devices. While Failsafe allows you to drop traffic when Snort is busy, traffic automatically passes without inspection when Snort is down. Snort Fail Open allows you to drop this traffic.

When you upgrade an FTD device, its new Snort Fail Open setting depends on its old Failsafe setting, as follows. Although the new configuration should not change traffic handling, we still recommend that you consider whether to enable or disable Failsafe before you upgrade.

Table 9: Migrating Failsafe to Snort Fail Open

Version 6.1 Failsafe	Version 6.2 Snort Fail Open	Behavior
Disabled (default behavior)	**Busy**: Disabled **Down**: Enabled	New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down.
Enabled	**Busy**: Enabled **Down**: Enabled	New and existing connections pass without inspection when the Snort process is busy or down.

Note that Snort Fail Open requires Version 6.2 on the device. If you are managing a Version 6.1.x device, the FMC web interface displays the Failsafe option.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or 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, contact Cisco TAC.

Traffic Flow and Inspection

Interruptions in traffic flow and inspection can occur when you:

- Reboot a device.
- Upgrade the device software, operating system, or virtual hosting environment.
- Uninstall the device software.
- Move a device between domains.
- Deploy configuration changes (Snort process restarts).

Device type, high availability/scalibility configurations, and interface configurations determine the nature of the interruptions. We *strongly* recommend performing these tasks in a maintenance window or at a time when any interruption will have the least impact on your deployment.

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300

FXOS Upgrades

Upgrade FXOS on each chassis independently, even if you have inter-chassis clustering or high availability pairs configured. How you perform the upgrade determines how your devices handle traffic during the FXOS upgrade.

Table 10: Traffic Behavior: FXOS Upgrades

Deployment	Method	Traffic Behavior
Standalone	—	Dropped.
High availability	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.	Unaffected.
	Upgrade FXOS on the active peer before the standby is finished upgrading.	Dropped until one peer is online.
Inter-chassis cluster (6.2+)	**Best Practice:** Upgrade one chassis at a time so at least one module is always online.	Unaffected.
	Upgrade chassis at the same time, so all modules are down at some point.	Dropped until at least one module is online.
Intra-chassis cluster (Firepower 9300 only)	Hardware bypass enabled: **Bypass: Standby** or **Bypass-Force**. (6.1+)	Passed without inspection.
	Hardware bypass disabled: **Bypass: Disabled**. (6.1+)	Dropped until at least one module is online.
	No hardware bypass module.	Dropped until at least one module is online.

Software Upgrades for Standalone Devices

Devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

Table 11: Traffic Behavior: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (6.1+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (6.1+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled** (6.1+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices.

- FTD with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.

  For clusters, the data security module or modules upgrade first, then the control module. During the control security module upgrade, although traffic inspection and handling continues normally, the system stops logging events. Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the upgrade is completed. However, if the logging downtime is significant, the system may prune the oldest events before they can be logged.

- FTD with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

Note Upgrading an inter-chassis cluster from Version 6.2.0, 6.2.0.1, or 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster. Upgrading high availability or clustered devices from Version 6.0.1 through 6.2.2.x may have additional upgrade path requirements; see the upgrade path information in the planning chapter of the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an

uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

- FTD with FDM: Not supported.

Deploying Configuration Changes

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 12: Traffic Behavior: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled (6.0.1–6.1).	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Firepower Threat Defense Upgrade Behavior: Other Devices

Software Upgrades for Standalone Devices

Devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

Table 13: Traffic Behavior: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (Firepower 2100 series, 6.3+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (Firepower 2100 series, 6.3+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled** (Firepower 2100 series, 6.3+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability devices.

- Firepower Threat Defense with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.
- Firepower Threat Defense with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.
- FTD with FDM: Not supported.

Deploying Configuration Changes

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 14: Traffic Behavior: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled (6.0.1–6.1).	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Firepower 7000/8000 Series Upgrade Behavior

The following sections describe device and traffic behavior when you upgrade Firepower 7000/8000 series devices.

Standalone 7000/8000 Series: Firepower Software Upgrade

Interface configurations determine how a standalone device handles traffic during the upgrade.

Table 15: Traffic Behavior During Upgrade: Standalone 7000/8000 Series

Interface Configuration	Traffic Behavior
Inline, hardware bypass enabled (**Bypass Mode: Bypass**)	Passed without inspection, although traffic is interrupted briefly at two points: • At the beginning of the upgrade process as link goes down and up (flaps) and the network card switches into hardware bypass. • After the upgrade finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces.
Inline, no hardware bypass module,or hardware bypass disabled (**Bypass Mode: Non-Bypass**)	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected
Routed, switched	Dropped

7000/8000 Series High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading devices (or device stacks) in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

Which peer upgrades first depends on your deployment:

- Routed or switched: Standby upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.
- Access control only: Active upgrades first. When the upgrade completes, the active and standby maintain their old roles.

8000 Series Stacks: Firepower Software Upgrade

In an 8000 series stack, devices upgrade simultaneously. Until the primary device completes its upgrade and the stack resumes operation, traffic is affected as if the stack were a standalone device. Until all devices complete the upgrade, the stack operates in a limited, mixed-version state.

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all devices, including those configured

for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 16: Traffic Behavior During Deployment: 7000/8000 Series

Interface Configuration	Traffic Behavior
Inline, **Failsafe** enabled or disabled	Passed without inspection A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
Inline, tap mode	Egress packet immediately, copy bypasses Snort
Passive	Uninterrupted, not inspected
Routed, switched	Dropped

ASA FirePOWER Upgrade Behavior

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during the Firepower software upgrade, including when you deploy certain configurations that restart the Snort process.

Table 17: Traffic Behavior During ASA FirePOWER Upgrade

Traffic Redirection Policy	Traffic Behavior
Fail open (**sfr fail-open**)	Passed without inspection
Fail closed (**sfr fail-close**)	Dropped
Monitor only (**sfr {fail-close}|{fail-open} monitor-only**)	Egress packet immediately, copy not inspected

Traffic Behavior During ASA FirePOWER Deployment

Traffic behavior while the Snort process restarts is the same as when you upgrade the ASA FirePOWER module.

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection. Your service policies determine whether traffic drops or passes without inspection during the interruption.

NGIPSv Upgrade Behavior

This section describes device and traffic behavior when you upgrade NGIPSv.

Firepower Software Upgrade

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 18: Traffic Behavior During NGIPSv Upgrade

Interface Configuration	Traffic Behavior
Inline	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 19: Traffic Behavior During NGIPSv Deployment

Interface Configuration	Traffic Behavior
Inline, **Failsafe** enabled or disabled	Passed without inspection A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
Inline, tap mode	Egress packet immediately, copy bypasses Snort
Passive	Uninterrupted, not inspected

Time and Disk Space Tests

For reference purposes, we provide reports of in-house time and disk space tests for the FTD and FMC software.

Time Tests

We report the *slowest* tested time of all software upgrades tested on a particular platform/series. Your upgrade will likely take longer than the provided times for multiple reasons, as explained in the following table. We recommend you track and record your own upgrade times so you can use them as future benchmarks.

Caution Even if the system appears inactive, do not manually reboot, shut down, or 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, contact Cisco TAC.

Table 20: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for FTD upgrades are from tests in a FMC deployments. Raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
Versions	For major and maintenance releases, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version. Upgrade time usually increases if your upgrade skips versions.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual appliances	We test with the default settings for memory and resources. However, note that upgrade time in virtual deployments is highly hardware dependent.
High availability/scalability	Unless otherwise noted, we test on standalone devices. In a high availability or clustered 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 or entire cluster, therefore, takes longer than upgrading a standalone device.
Configurations	We test on appliances with minimal configurations and traffic load. Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how those things 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	We report times for the software upgrade itself and the subsequent reboot *only*. This does not include time for operating system upgrades, transferring upgrade packages, readiness checks, VDB and intrusion rule (SRU/LSP) updates, or deploying configurations.

Disk Space Tests

We report the *most* disk space used of all software upgrades tested on a particular platform/series. This includes the space needed to copy the upgrade package to the device.

We also report the space needed on the FMC (in /var) for the device upgrade package. If you are using FDM, ignore those values.

When we report disk space estimates for a particular location (for example, /var or /ngfw), we are reporting the disk space estimate for the partition mounted in that location. On some platforms, these locations may be on the same partition.

Table 21: Checking Disk Space

Platform	Command
FMC	Choose **System** > **Monitoring** > **Statistics** and select the FMC. Under Disk Usage, expand the By Partition details.
FTD with FMC	Choose **System** > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.
FTD with FDM	Use the **show disk** CLI command.

Version 6.3.0 Time and Disk Space

Table 22: Version 6.3.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	12.7 GB	29 MB	—	47 min
FMCv: VMware	12.7 GB	29 MB	—	29 min
Firepower 2100 series	13 MB	8.8 GB	930 MB	20 min
Firepower 4100/9300	10 MB	7.6 GB	930 MB	6 min
ASA 5500-X series with FTD	7.9 GB	100 KB	1.1 GB	25 min
FTDv: VMware	7.3 GB	100 KB	1.1 GB	12 min
Firepower 7000/8000 series	7.0 GB	19 MB	920 MB	32 min
ASA FirePOWER	11.3 GB	22 MB	1.2 GB	63 min
NGIPSv	5.7 GB	19 MB	810 MB	16 min

Upgrade Instructions

The release notes do not contain upgrade instructions. After you read the guidelines and warnings in these release notes, see one of the following documents.

Table 23: Firepower Upgrade Instructions

Task	Guide
Upgrade in Firepower Management Center deployments.	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

Task	Guide
Upgrade Firepower Threat Defense with Firepower Device Manager.	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager See the *System Management* chapter in the guide for the Firepower Threat Defense version you are currently running—not the version you are upgrading to.
Upgrade FXOS on a Firepower 4100/9300 chassis.	Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
Upgrade ASA FirePOWER modules with ASDM.	Cisco ASA Upgrade Guide
Upgrade the ROMMON image on the ISA 3000, ASA 5508-X, and ASA 5516-X.	Cisco ASA and Firepower Threat Defense Reimage Guide See the *Upgrade the ROMMON Image* section. You should always make sure you have the latest image.