Upgrade Guidelines

This document provides critical and release-specific upgrade guidelines for Version 6.2.3.

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 appropriate upgrade or configuration guide.

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 configurations and events. Back up FXOS on the Firepower 4100/9300. Back up ASA for ASA FirePOWER.
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.

Planning Phase	Includes
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

Minimum Version to Upgrade

Minimum Version to Upgrade

You can upgrade directly to Version 6.2.3 as follows.

Table 2: Minimum Version to Upgrade to Version 6.2.3

Platform	Minimum Version
FMC	6.1
FTD	6.1 with FMC 6.2 with FDM FXOS 2.3.1.73 is required for the Firepower 4100/9300. In most cases, we recommend you use the latest FXOS build in each major version. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.3(1). **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+.
Firepower 7000/8000 series	6.1

Platform	Minimum Version
ASA with FirePOWER Services	6.1 with FMC 6.2 with ASDM See Device Platforms for ASA requirements for your model. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues. To help you decide, see the Cisco Secure Firewall ASA Release Notes.
NGIPSv	6.1

Minimum Version to Patch

Patches change the fourth digit *only*. You cannot upgrade directly to a patch from a previous major or maintenance release.

Upgrade Guidelines for Version 6.2.3

These checklists provide new and/or previously published upgrade guidelines that may apply to you.

Table 3: Upgrade Guidelines for FTD with FMC Version 6.2.3

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 2	Any	Any	Any
	Cisco Secure Firewall Management Center New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Bugs, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 9	Firepower 4100/9300	Any	Any
	Patches That Support Uninstall	Any	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure, on page 5	FTD	6.2.3 through 6.2.3.9	6.2.3.10

✓	Guideline	Platforms	Upgrading From	Directly To
	Version 6.2.3.3 FTD Device Cannot Switch to Local Management, on page 5	FTD	6.2.3 through 6.2.3.2	6.2.3.3
	Hotfix Before Upgrading Version 6.2.3-88 FMCs, on page 6	FMC	6.2.3-88	6.2.3.1 through 6.2.3.3
	Remove Site IDs from Version 6.1.x Firepower Threat Defense Clusters Before Upgrade, on page 6	FTD clusters	6.1.0.x	6.2.3+
	Edit/Resave Access Control Policies After Upgrade, on page 7	Any	6.1.0 through 6.2.2.x	6.2.3 only
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 8	FMC	6.1.0.x	6.2+
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 8	FTD	6.1.0.x	6.2+

Table 4: Upgrade Guidelines for FTD with FDM Version 6.2.3

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 2	Any	Any	Any
	Cisco Secure Firewall Device Manager New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Bugs, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 9	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Version 6.2.3.3 FTD Device Cannot Switch to Local Management, on page 5	Any	6.2.3 through 6.2.3.2	6.2.3.3
	Upgrade Can Unregister FDM from CSSM, on page 6	Any	6.2.3 through 6.2.3.1	6.2.3.2 through 6.2.3.5

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Can Unregister FDM from CSSM, on page 6	Any	6.2.0 through 6.2.2.x	6.2.3+
	Upgrade Failure: Firepower 2100 Series from Version 6.2.2.5, on page 7	Firepower 2100 series	6.2.2.5	6.2.3 only
	Edit/Resave Realms After FTD/FDM Upgrade, on page 7	Any	6.2.0 through 6.2.2.x	6.2.3 only
	Edit/Resave Access Control Policies After Upgrade, on page 7	Any	6.1.0 through 6.2.2.x	6.2.3 only
	Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 7	Any	6.2.0 only	6.2.2+

Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure

Deployments: Firepower Threat Defense

Upgrading from: Version 6.2.3 through 6.2.3.9

Directly to: Version 6.2.3.10 only

Known issue: CSCvo39052

Upgrading an FTD device to Version 6.2.3.10 with CC mode enabled causes a FSIC (file system integrity check) failure when the device reboots.

Caution If security certifications compliance is enabled and the FSIC fails, the software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.

If your FTD deployment requires security certifications compliance (CC mode), we recommend you upgrade directly to Version 6.2.3.13+. For Firepower 4100/9300 devices, we also recommend that you upgrade to FXOS 2.3.1.130+.

Version 6.2.3.3 FTD Device Cannot Switch to Local Management

Deployments: FTD wth FMC

Upgrading from: Version 6.2.3 through Version 6.2.3.2

Directly to: Version 6.2.3.3 only

In Version 6.2.3.3, you cannot switch Firepower Threat Defense device management from FMC to FDM. This happens even if you uninstall the Version 6.2.3.3 patch. If you want to switch to local management at that point, either freshly install Version 6.2.3, or contact Cisco TAC.

As a workaround, switch management before you upgrade to Version 6.2.3.3. Or, upgrade to the latest patch. Keep in mind that you lose device configurations when you switch management.

Note that you can switch management from FDM to FMC in Version 6.2.3.3.

Hotfix Before Upgrading Version 6.2.3-88 FMCs

Deployments: FMC

Upgrading from: Version 6.2.3-88

Directly to: Version 6.2.3.1, Version 6.2.3.2, or Version 6.2.3.3

Sometimes Cisco releases updated builds of Firepower upgrade packages. Version 6.2.3-88 has been replaced by a later build. If you upgrade an FMC running Version 6.2.3-88 to Version 6.2.3.1, Version 6.2.3.2, or Version 6.2.3.3, the SSE cloud connection continuously drops and generates errors. Uninstalling the patch does not resolve the issue.

If you are running Version 6.2.3-88, install Hotfix T before you upgrade.

Remove Site IDs from Version 6.1.x Firepower Threat Defense 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 Can Unregister 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

Note Upgrades from 6.2.3 and 6.2.3.1 directly to 6.2.3.2 through 6.2.3.5 are also affected.

Upgrading FTD with FDM 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**.

Upgrade Failure: Firepower 2100 Series from Version 6.2.2.5

Deployments: Firepower 2100 series with FTD, managed by FDM

Upgrading from: Version 6.2.2.5

Directly to: Version 6.2.3 only

If you change the DNS settings on a Firepower 2100 series device running Version 6.2.2.5, and then upgrade to Version 6.2.3 without an intermediate deployment, the upgrade fails. You must deploy or execute an action that triggers a deployment, such as an SRU update, before you upgrade the device.

Edit/Resave Realms After FTD/FDM Upgrade

Deployments: FTD with FDM

Upgrading from: Version 6.2.0 through Version 6.2.2.x

Directly to: Version 6.2.3 only

Before Version 6.2.3, users were not automatically logged out after 24 hours of inactivity. After you upgrade Firepower Threat Defense to Version 6.2.3 when using Firepower Device Manager, if you are using identity policies with active authentication, update your realm before you deploy configurations. Choose **Objects** > **Identity Realm**, edit the realm (no changes are needed), and save it. Then, deploy.

Edit/Resave Access Control Policies After Upgrade

Deployments: Any

Upgrading from: Version 6.1 through 6.2.2.x

Directly to: Version 6.2.3 only

If you configured network or port objects that are used *only* in intrusion policy variable sets, deploying associated access control policies after the upgrade fails. If this happens, edit the access control policy, make a change (such as editing the description), save, and redeploy.

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 5: 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.

Version 6.1 Failsafe	Version 6.2 Snort Fail Open	Behavior
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.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

For the Firepower 4100/9300, major FTD upgrades also require a chassis upgrade (FXOS and firmware). Maintenance release and patches rarely require this, but you may still want to upgrade to the latest build to take advantage of resolved issues.

Table 6: Upgrade Guidelines for the Firepower 4100/9300 Chassis

Guideline	Details
FXOS upgrades.	FXOS 2.3.1.73+ is required to run threat defense Version 6.2.3 on the Firepower 4100/9300. **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+. You can upgrade to any later FXOS version from as far back as FXOS 2.2.2. For critical and release-specific upgrade guidelines, new and deprecated features, and open and resolved bugs, see the Cisco Firepower 4100/9300 FXOS Release Notes.
Firmware upgrades.	FXOS 2.14.1+ upgrades include firmware. If you are upgrading to an earlier FXOS version, see the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
Time to upgrade.	Chassis upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see Traffic Flow and Inspection for Chassis Upgrades, on page 12.

Unresponsive Upgrades

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

Uninstall a Patch

In FMC and ASDM deployments, you can uninstall most patches. If you need to return to an earlier major release, you must reimage. For guidelines, limitations, and procedures, see Uninstall a Patch in the FMC upgrade guide or Uninstall ASA FirePOWER Patches with ASDM, on page 10 in these release notes.

Uninstall ASA FirePOWER Patches with ASDM

Use the Linux shell (*expert mode*) to uninstall device 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. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

For ASA failover pairs and clusters, minimize disruption by uninstalling from one appliance at a time. Wait until the patch has fully uninstalled from one unit before you move on to the next.

Table 7: Uninstall Order for ASA with FirePOWER Services in ASA Failover Pairs/Clusters

Configuration	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	Always uninstall from the standby. **1.** Uninstall from the ASA FirePOWER module on the standby ASA device. **2.** Fail over. **3.** Uninstall from the ASA FirePOWER module on the new standby ASA device.
ASA active/active failover pair, with ASA FirePOWER	Make both failover groups active on the unit you are not uninstalling. **1.** Make both failover groups active on the primary ASA device. **2.** Uninstall from the ASA FirePOWER module on the secondary ASA device. **3.** Make both failover groups active on the secondary ASA device. **4.** Uninstall from the ASA FirePOWER module on the primary ASA device.
ASA cluster, with ASA FirePOWER	Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the control unit for last. **1.** On a data unit, disable clustering. **2.** Uninstall from the ASA FirePOWER module on that unit. **3.** Reenable clustering. Wait for the unit to rejoin the cluster. **4.** Repeat for each data unit. **5.** On the control unit, disable clustering. Wait for a new control unit to take over. **6.** Uninstall from the ASA FirePOWER module on the former control unit. **7.** Reenable clustering.

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

- In ASA failover/cluster deployments, make sure you are uninstalling from the correct device.
- Make sure your deployment is healthy and successfully communicating.

Step 1 If the device's configurations are out of date, deploy now from ASDM.

Deploying before you uninstall reduces the chance of failure. Make sure the deployment and other essential tasks are completed. 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 Firepower CLI on the ASA FirePOWER module. Log in as `admin` or another Firepower CLI user with configuration access.

You can either SSH to the module's management interface (hostname or IP address) or use the console. Note that the console port defaults to the ASA CLI and you must use the `session sfr` command to access the Firepower CLI.

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 module has the correct software version. Choose **Configuration** > **ASA FirePOWER Configurations** > **Device Management** > **Device**.

Step 8 Redeploy configurations.

What to do next

In ASA failover/cluster deployments, repeat this procedure for each unit in your planned sequence.

Traffic Flow and Inspection

Device upgrades (software and operating system) affect traffic flow and inspection. Schedule maintenance windows when this will have the least impact.

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/clustered deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time.

Table 8: Traffic Flow and Inspection: FXOS Upgrades

FTD 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.
Inter-chassis cluster	Unaffected.	**Best Practice:** Upgrade one chassis at a time so at least one module is always online.
	Dropped until at least one module is online.	Upgrade chassis at the same time, so all modules are down at some point.
Intra-chassis cluster (Firepower 9300 only)	Passed without inspection.	Hardware bypass enabled: **Bypass: Standby** or **Bypass-Force**.
	Dropped until at least one module is online.	Hardware bypass disabled: **Bypass: Disabled**.
	Dropped until at least one module is online.	No hardware bypass module.

Traffic Flow and Inspection for FTD Upgrades with FMC

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 9: Traffic Flow and Inspection: 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. For bridge group interfaces on the ISA 3000 only, you can use a FlexConfig policy to configure hardware bypass for power failure. This causes traffic to drop during software upgrades but pass without inspection while the device completes its post-upgrade reboot.
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force**	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby**	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**	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. 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.

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)

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.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption. 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.

Table 10: Traffic Flow and Inspection: 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.	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.	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled.	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Traffic Flow and Inspection for FTD Upgrades with FDM

Software Upgrades

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.

Deploying Configuration Changes

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.

Traffic Flow and Inspection for ASA FirePOWER Upgrades

Software Upgrades

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during software upgrade.

Table 11: Traffic Flow and Inspection: ASA FirePOWER Upgrades

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

Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In ASA failover/cluster 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.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection. Traffic behavior while the Snort process restarts is the same as when you upgrade ASA FirePOWER. 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.

Traffic Flow and Inspection for NGIPSv Upgrades with FMC

Software Upgrades

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 12: Traffic Flow and Inspection: NGIPSv Upgrades

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

Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection. Interface configurations determine whether traffic drops or passes without inspection during the interruption. 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.

Table 13: Traffic Flow and Inspection: Deploying Configuration Changes

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 FMC and device software upgrades.

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 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.

Table 14: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for device 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 either /Volume or /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.

Without enough free disk space, the upgrade fails.

Table 15: 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 6.2.3.18 Time and Disk Space

Table 16: Time and Disk Space for Version 6.2.3.18

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	3.4 GB	290 MB	—	40 min	9 min
FMCv: VMware	3.5 GB	250 MB	—	24 min	4 min
Firepower 2100 series	—	2.7 GB	600 MB	13 min	12 min
Firepower 4100 series	—	1.8 GB	400 MB	6 min	6 min
Firepower 9300	—	1.7 GB	400 MB	5 min	9 min
ASA 5500-X series with FTD	2.1 GB	200 MB	420 MB	15 min	53 min
FTDv: VMware	2.0 GB	200 MB	420 MB	8 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	650 MB	10 min	83 min
ASA FirePOWER	3.8 GB	59 MB	580 MB	74 min	59 min
NGIPSv	2.3 GB	180 MB	480 MB	6 min	4 min

Version 6.2.3.17 Time and Disk Space

Table 17: Time and Disk Space for Version 6.2.3.17

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	3.4 GB	300 MB	—	32 min	7 min
FMCv: VMware	4.1 GB	230 MB	—	23 min	5 min
Firepower 2100 series	—	2.7 GB	600 MB	12 min	12 min
Firepower 4100 series	—	1.7 GB	390 MB	5 min	6 min
Firepower 9300	—	1.7 GB	390 MB	5 min	7 min
ASA 5500-X series with FTD	2.1 GB	200 MB	420 MB	18 min	37 min
FTDv: VMware	2.1 GB	190 MB	420 MB	7 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	640 MB	10 min	15 min
ASA FirePOWER	3.8 GB	58 MB	580 MB	72 min	61 min
NGIPSv	2.5 GB	180 MB	480 MB	5 min	4 min

Version 6.2.3.16 Time and Disk Space

Table 18: Time and Disk Space for Version 6.2.3.16

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	3.6 GB	250 MB	—	40 min	9 min
FMCv: VMware	3.3 GB	220 MB	—	25 min	4 min
Firepower 2100 series	—	2.6 GB	620 MB	11 min	12 min
Firepower 4100 series	—	1.7 GB	410 MB	5 min	5 min
Firepower 9300	—	1.8 GB	410 MB	5 min	9 min
ASA 5500-X series with FTD	2.0 GB	200 MB	430 MB	18 min	33 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FTDv: VMware	2.0 GB	190 MB	430 MB	8 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	670 MB	31 min	14 min
ASA FirePOWER	3.8 GB	58 MB	600 MB	74 min	77 min
NGIPSv	2.3 GB	180 MB	500 MB	6 min	4 min

Version 6.2.3.15 Time and Disk Space

Table 19: Time and Disk Space for Version 6.2.3.15

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	4.7 GB	260 MB	—	50 min
FMCv: VMware	4.7 GB	210 MB	—	Hardware dependent
Firepower 2100 series	—	2.3 GB	590 MB	27 min
Firepower 4100 series	—	1.7 GB	390 MB	10 min
Firepower 9300	—	2.4 GB	390 MB	11 min
ASA 5500-X series with FTD	2.0 GB	190 MB	410 MB	38 min
FTDv: VMware	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.5 GB	210 MB	640 MB	19 min
ASA FirePOWER	3.9 GB	56 MB	580 MB	100 min
NGIPSv	2.7 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.14 Time and Disk Space

Table 20: Time and Disk Space for Version 6.2.3.14

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	4.5 GB	260 MB	—	58 min
FMCv: VMware	4.7 GB	190 MB	—	Hardware dependent
Firepower 2100 series	—	1.9 GB	590 MB	23 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
Firepower 4100 series	—	1.7 GB	390 MB	11 min
Firepower 9300	—	1.7 GB	390 MB	10 min
ASA 5500-X series with FTD	2.0 GB	200 MB	410 MB	32 min
FTDv: VMware	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.4 GB	200 MB	630 MB	19 min
ASA FirePOWER	3.7 GB	53 MB	560 MB	106 min
NGIPSv	2.6 GB	190 MB	470 MB	Hardware dependent

Version 6.2.3.13 Time and Disk Space

Table 21: Time and Disk Space for Version 6.2.3.13

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	4.7 GB	290 MB	—	50 min
FMCv: VMware	4.6 GB	190 MB	—	Hardware dependent
Firepower 2100 series	—	2.6 GB	590 MB	25 min
Firepower 4100 series	—	1.7 GB	390 MB	11 min
Firepower 9300	—	1.8 GB	390 MB	11 min
ASA 5500-X series with FTD	2.4 GB	190 MB	410 MB	32 min
FTDv: VMware	2.3 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.8 GB	190 MB	620 MB	18 min
ASA FirePOWER	3.7 GB	51 MB	560 MB	105 min
NGIPSv	2.6 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.12 Time and Disk Space

Table 22: Time and Disk Space for Version 6.2.3.12

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	3.9 GB	220 MB	—	49 min
FMCv: VMware	4.6 GB	160 MB	—	Hardware dependent
Firepower 2100 series	—	1.9 GB	390 MB	21 min
Firepower 4100 series	—	970 MB	190 MB	14 min
Firepower 9300	—	1.7 GB	190 MB	11 min
ASA 5500-X series with FTD	1.4 GB	96 MB	210 MB	30 min
FTDv: VMware	2.4 GB	200 MB	210 MB	Hardware dependent
Firepower 7000/8000 series	3.6 GB	160 MB	540 MB	19 min
ASA FirePOWER	3.5 GB	31 MB	480 MB	104 min
NGIPSv	2.6 GB	130 MB	400 MB	Hardware dependent

Version 6.2.3.11 Time and Disk Space

Table 23: Time and Disk Space for Version 6.2.3.11

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	4.5 GB	250 MB	—	39 min
FMCv: VMware	4.6 GB	35 MB	—	Hardware dependent
Firepower 2100 series	—	2.8 GB	590 MB	40 min
Firepower 4100 series	—	2.0 GB	380 MB	10 min
Firepower 9300	—	1.6 GB	380 MB	11 min
ASA 5500-X series with FTD	1.8 GB	230 MB	410 MB	33 min
FTDv: VMware	2.2 GB	230 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.3 GB	170 MB	600 MB	23 min
ASA FirePOWER	3.6 GB	50 MB	530 MB	110 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
NGIPSv	2.6 GB	130 MB	450 MB	Hardware dependent

Version 6.2.3.10 Time and Disk Space

Table 24: Time and Disk Space for Version 6.2.3.10

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	4.2 GB	200 MB	—	40 min
FMCv	4.5 GB	230 MB	—	Hardware dependent
Firepower 2100 series	—	1.8 GB	390 MB	21 min
Firepower 4100/9300	—	1.3 GB	190 MB	11 min
ASA 5500-X series with FTD	1.3 GB	140 MB	210 MB	25 min
FTDv	1.6 GB	140 MB	210 MB	Hardware dependent
Firepower 7000/8000 series	3.2 GB	190 MB	560 MB	25 min
ASA FirePOWER	3.4 GB	31 MB	480 MB	100 min
NGIPSv	2.1 GB	160 MB	400 MB	Hardware dependent

Version 6.2.3.9 Time and Disk Space

Table 25: Time and Disk Space for Version 6.2.3.9

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	3630 MB	190 MB	—	35 min
FMCv	3596 MB	172 MB	—	Hardware dependent
Firepower 2100 series	—	1677 MB	385 MB	21 min
Firepower 4100/9300	—	779 MB	184 MB	9 min
ASA 5500-X series with FTD	1105 MB	130 MB	206 MB	12 min
ISA 3000 with FTD	1071 MB	130 MB	206 MB	25 min
FTDv	1094 MB	130 MB	206 MB	Hardware dependent

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
Firepower 7000/8000 series	2975 MB	161 MB	538 MB	30 min
ASA FirePOWER	3211 MB	27 MB	462 MB	38 min
NGIPSv	1883 MB	146 MB	378 MB	Hardware dependent

Version 6.2.3.8 Time and Disk Space

Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. If you are running this version, we recommend you upgrade.

Version 6.2.3.7 Time and Disk Space

Table 26: Time and Disk Space for Version 6.2.3.7

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	2909 MB	137 MB	—	25 min
FMCv	3972 MB	211 MB	—	Hardware dependent
Firepower 2100 series	—	1668 MB	384 MB	19 min
Firepower 4100/9300	—	795 MB	183 MB	8 min
ASA 5500-X series with FTD	1067 MB	130 MB	205 MB	9 min
ISA 3000 with FTD	1080 MB	130 MB	205 MB	20 min
FTDv	1146 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	3300 MB	136 MB	477 MB	20 min
ASA FirePOWER	2291 MB	26 MB	411 MB	80 min
NGIPSv	1588 MB	121 MB	327 MB	Hardware dependent

Version 6.2.3.6 Time and Disk Space

Table 27: Time and Disk Space for Version 6.2.3.6

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	2524 MB	47 MB	—	30 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMCv	2315 MB	101 MB	—	Hardware dependent
Firepower 2100 series	—	1673 MB	383 MB	10 min
Firepower 4100/9300	—	790 MB	182 MB	17 min
ASA 5500-X series with FTD	1220 MB	130 MB	205 MB	21 min
ISA 3000 with FTD	1087 MB	130 MB	205 MB	21 min
FTDv	1133 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	1196 MB	17 MB	204 MB	30 min
ASA FirePOWER	1844 MB	16 MB	226 MB	106 min
NGIPSv	364 MB	17 MB	142 MB	Hardware dependent

Version 6.2.3.5 Time and Disk Space

Table 28: Time and Disk Space for Version 6.2.3.5

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	1566 MB	24 MB	—	28 min
FMCv	2266 MB	80 MB	—	Hardware dependent
Firepower 2100 series	—	1001MB	257 MB	20 min
Firepower 4100/9300	—	370 MB	56 MB	7 min
ASA 5500-X series with FTD	587 MB	130 MB	78 MB	20 min
ISA 3000 with FTD	379 MB	130 MB	78 MB	20 min
Firepower 7000/8000 series	806 MB	17 MB	78 MB	22 min
ASA FirePOWER	1465 MB	15 MB	100 MB	70 min
NGIPSv	120 MB	17 MB	16 MB	Hardware dependent

Version 6.2.3.4 Time and Disk Space

Table 29: Time and Disk Space for Version 6.2.3.4

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	2191 MB	107 MB	—	80 min
FMCv	1760 MB	35 MB	—	Hardware dependent
Firepower 2100 series	—	1014 MB	261 MB	17 min
Firepower 4100/9300	—	334 MB	59 MB	7 min
ASA 5500-X series with FTD	411 MB	128 MB	82 MB	20 min
ISA 3000 with FTD	393 MB	128 MB	82 MB	20 min
FTDv	411 MB	128 MB	82 MB	Hardware dependent
Firepower 7000/8000 series	800 MB	17 MB	82 MB	23 min
ASA FirePOWER	1385 MB	15 MB	103 MB	25 min
NGIPSv	191 MB	17 MB	20 MB	Hardware dependent

Version 6.2.3.3 Time and Disk Space

Table 30: Time and Disk Space for Version 6.2.3.3

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	1879 MB	88 MB	—	26 min
FMCv	2093 MB	90 MB	—	Hardware dependent
Firepower 2100 series	—	987 MB	255 MB	15 min
Firepower 4100/9300	—	313 MB	54 MB	5 min
ASA 5500-X series with FTD	553 MB	128 MB	77 MB	16 min
ISA 3000 with FTD	307 MB	90 MB	77 MB	15 min
FTDv	307 MB	90 MB	77 MB	Hardware dependent
Firepower 7000/8000 series	825 MB	17 MB	77 MB	15 min
ASA FirePOWER	634 MB	16 MB	98 MB	40 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
NGIPSv	102 MB	17 MB	77 MB	Hardware dependent

Version 6.2.3.2 Time and Disk Space

Table 31: Time and Disk Space for Version 6.2.3.2

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	1743 MB	27 MB	—	24 min
FMCv	1976 MB	70 MB	—	Hardware dependent
Firepower 2100 series	—	977 MB	252 MB	17 min
Firepower 4100/9300	—	374 MB	51 MB	4 min
ASA 5500-X series with FTD	585 MB	126 MB	73 MB	16 min
ISA 3000 with FTD	676 MB	126 MB	73 MB	17 min
FTDv	585 MB	126 MB	73 MB	Hardware dependent
Firepower 7000/8000 series	688 MB	11 MB	76 MB	13 min
ASA FirePOWER	1440 MB	15 MB	98 MB	40 min
NGIPSv	96 MB	17 MB	14 MB	Hardware dependent

Version 6.2.3.1 Time and Disk Space

Table 32: Time and Disk Space for Version 6.2.3.1

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	1361.8 MB	59.67 MB	—	25 min
FMCv	1240.8 MB	40.8 MB	—	Hardware dependent
Firepower 2100 series	—	948.3 MB	246 MB	81 min
Firepower 4100/9300	—	278 MB	45 MB	8 min
ASA 5500-X series with FTD	275.5 MB	89.9 MB	68 MB	16 min
ISA 3000 with FTD	343.4 MB	127.5 MB	68 MB	15 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FTDv	275.5 MB	89.9 MB	67 MB	Hardware dependent
Firepower 7000/8000 series	99.8 MB	36 MB	10 MB	19 min
ASA FirePOWER	867.9 MB	15.45 MB	32 MB	60 min
NGIPSv	101.9 MB	17.18 MB	9 MB	Hardware dependent

Version 6.2.3 Time and Disk Space

Table 33: Time and Disk Space for Version 6.2.3

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	From 6.1.0: 7415 MB From 6.2.0: 8863 MB From 6.2.1: 8263 MB From 6.2.2: 11860 MB	From 6.1.0: 17 MB From 6.2.0: 24 MB From 6.2.1: 23 MB From 6.2.2: 24 MB	—	From 6.1.0: 38 min From 6.2.0: 43 min From 6.2.1: 37 min From 6.2.2: 37 min
FMCv	From 6.1.0: 7993 MB From 6.2.0: 9320 MB From 6.2.1: 11571 MB From 6.2.2: 11487 MB	From 6.1.0: 23 MB From 6.2.0: 28 MB From 6.2.1: 24 MB From 6.2.2: 24 MB	—	Hardware dependent
Firepower 2100 series	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	1000 MB	From 6.2.1: 15 min From 6.2.2: 15 min
Firepower 4100/9300	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	795 MB	From 6.1.0: 10 min From 6.2.0: 12 min From 6.2.2: 15 min
ASA 5500-X series with FTD	From 6.1.0: 4322 MB From 6.2.0: 6421 MB From 6.2.2: 6450 MB	From 6.1.0: .088 MB From 6.2.0: .092 MB From 6.2.2: .088 MB	1000 MB	From 6.1.0: 54 min From 6.2.0: 53 min From 6.2.2: 50 min
FTDv	From 6.1.0: 4225 MB From 6.2.0: 5179 MB From 6.2.2: 6450 MB	From 6.1.0: .076 MB From 6.2.0: .092 MB From 6.2.2: .092 MB	1000 MB	Hardware dependent

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
Firepower 7000/8000 series	From 6.1.0: 5145 MB From 6.2.0: 5732 MB From 6.2.2: 6752 MB	From 6.1.0: 18 MB From 6.2.0: 18 MB From 6.2.2: 18 MB	840 MB	From 6.1.0: 29 min From 6.2.0: 31 min From 6.2.2: 31 min
ASA FirePOWER	From 6.1.0: 7286 MB From 6.2.0: 7286 MB From 6.2.2: 10748 MB	From 6.1.0: 16 MB From 6.2.0: 16 MB From 6.2.2: 16 MB	From 6.1.0: 1200 MB From 6.2.0: 1200 MB	From 6.1.0: 94 min From 6.2.0: 104 min From 6.2.2: 96 min
NGIPSv	From 6.1.0: 4115 MB From 6.2.0: 5505 MB From 6.2.2: 5871 MB	From 6.1.0: 18 MB From 6.2.0: 19 MB From 6.2.2: 19 MB	741 MB	Hardware dependent