Upgrade Firepower 7000/8000 Series and NGIPSv

Upgrade Checklist: Firepower 7000/8000 Series and NGIPSv with FMC

Complete this checklist before you upgrade Firepower 7000/8000 series and NGIPSv devices.

Note At all times during the process, make sure you maintain deployment communication and health. Do *not* restart a device upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 1:

✓	Action/Check
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths.

✓	Action/Check
	Read *all* upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with the release notes, which contain critical and release-specific information, including upgrade warnings, behavior changes, new and deprecated features, and known issues.
	Check appliance access. Devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

Table 2:

✓	Action/Check
	Upload the upgrade package to the FMC. See Upload to the Firepower Management Center.
	Copy the upgrade package to the device. If your FMC is running Version 6.2.3+, we recommend you copy (*push*) packages to managed devices before you initiate the device upgrade. See Copy to Managed Devices.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.

Caution We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 3:

✓	Action/Check
	Back up 7000/8000 series devices. Use the FMC to back up 7000/8000 series devices. Backups are not supported for NGIPSv. Back up before and after upgrade: • Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly. • After upgrade: This creates a snapshot of your freshly upgraded deployment. In FMC deployments, we recommend you back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 4:

✓	Action/Check
	Upgrade virtual hosting. If needed, upgrade the hosting environment for any virtual appliances. If this is required, it is usually because you are running an older version of VMware and are performing a major device upgrade.

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 5:

✓	Action/Check
	Check configurations. Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.

✓	Action/Check
	Check NTP synchronization. Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually. To check time: • FMC: Choose **System** > **Configuration** > **Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Deploy configurations. Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In FMC high availability deployments, you only need to deploy from the active peer. When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Run readiness checks. If your FMC is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade. See Firepower Software Readiness Checks.
	Check running tasks. Make sure essential tasks on the device are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them.

Upgrade Firepower 7000/8000 and NGIPSv with FMC

Use this procedure to upgrade Firepower 7000/8000 series and NGIPSv devices. You can upgrade multiple devices at once if they use the same upgrade package. You must upgrade the members of device stacks and high availability pairs at the same time.

Before you begin

Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.

Step 1 (Optional) Switch the active/standby roles of your high availability device pairs that perform switching/routing.

If your high availability pairs are deployed to perform access control *only*, the active upgrades first. When the upgrade completes, the active and standby maintain their old roles.

However, in a routed or switched deployment, the 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.

Choose **Devices** > **Device Management**, click the **Switch Active Peer** icon next to the pair, and confirm your choice.

Step 2 Choose **System** > **Updates**.

Step 3 Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

Note We *strongly* recommend upgrading no more than five devices simultaneously from the System Update page. You cannot stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 4 Click **Install**, then confirm that you want to upgrade and reboot the devices.

Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.

Step 5 Monitor upgrade progress.

Caution Do *not* deploy changes to, manually reboot, or shut down an upgrading device. Do *not* restart a device upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Step 6 Verify upgrade success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 7 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 8 Complete any post-upgrade configuration changes described in the release notes.

Step 9 Redeploy configurations to the devices you just upgraded.