Upgrade Firepower Management Centers

Upgrade Checklist: Firepower Management Center

Complete this checklist before you upgrade an FMC, including FMCv. If you are upgrading a high availability pair, complete the checklist for each peer.

Note At all times during the process, make sure you maintain deployment communication and health. Do *not* restart an FMC 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 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. In FMC high availability deployments, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to HA synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization. See Upload to the Firepower Management Center.

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. 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. If this is required, it is usually because you are running an older version of VMware and are performing a major FMC 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 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. **Note** In some deployments, upgrades automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. This feature is currently supported for FMCs running Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. Note that this feature is supported for all upgrades *from* a supported version. This feature is not supported for upgrades *to* a supported version from an unsupported version.

Upgrade a Standalone Firepower Management Center

Use this procedure to upgrade a standalone Firepower Management Center, including Firepower Management Center Virtual.

Caution Do *not* make or deploy configuration changes, manually reboot, or shut down while you are upgrading the FMC. Do *not* restart an 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.

Before you begin

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

Step 1 Choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade package you want to use, then choose the FMC.

Step 3 Click **Install** to begin the upgrade.

Confirm that you want to upgrade and reboot.

Step 4 Monitor precheck progress until you are logged out. Do not make configuration changes during this time.

Step 5 Log back in when you can.

- Minor upgrades (patches and hotfixes): You can log in after the upgrade and reboot are completed.
- Major and maintenance upgrades: You can log in before the upgrade is completed. The system displays a page you can use to monitor the upgrade's progress and view the upgrade log and any error messages. You are logged out again when the upgrade is completed and the system reboots. After the reboot, log back in again.

Step 6 If prompted, review and accept the End User License Agreement (EULA).

Step 7 Verify upgrade success.

If the system does not notify you of the upgrade's success when you log in, choose **Help** > **About** to display current software version information.

Step 8 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 9 Complete any post-upgrade configuration changes described in the release notes.

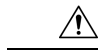
Step 10 Redeploy configurations.

Redeploy to *all* managed devices. If you do not deploy to a device, its eventual upgrade may fail and you may have to reimage it.

Upgrade High Availability Firepower Management Centers

Use this procedure to upgrade the Firepower software on FMCs in a high availability pair.

You upgrade peers one at a time. With synchronization paused, first upgrade the standby, then the active. When the standby starts prechecks, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade. Do *not* make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization.



Caution Do *not* make or deploy configuration changes, manually reboot, or shut down while you are upgrading the FMC. Do *not* restart an 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.

Before you begin

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

Step 1 Pause synchronization.

a) Choose **System** > **Integration**.
b) On the **High Availability** tab, click **Pause Synchronization**.

Step 2 Upload the upgrade package to the standby.

In FMC high availability deployments, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to HA synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization.

Step 3 Upgrade peers one at a time — first the standby, then the active.

Follow the instructions in Upgrade a Standalone Firepower Management Center, on page 5, stopping after you verify update success on each peer. In summary, for each peer:

a) On the **System** > **Updates** page, install the upgrade.
b) Monitor progress until you are logged out, then log back in when you can (this happens twice for major upgrades).
c) Verify upgrade success.

Do *not* make or deploy configuration changes while the pair is split-brain.

Step 4 Restart synchronization.

a) Log into the FMC that you want to make the active peer.
b) Choose **System** > **Integration**.
c) On the **High Availability** tab, click **Make-Me-Active**.
d) Wait until synchronization restarts and the other FMC switches to standby mode.

Step 5 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 6 Complete any post-upgrade configuration changes described in the release notes.

Step 7 Redeploy configurations.

Redeploy to *all* managed devices. If you do not deploy to a device, its eventual upgrade may fail and you may have to reimage it.