Upgrade the FMC

This chapter explains how to upgrade a customer-deployed FMC from Version 7.1 to a later version.

If you are using the cloud-delivered management center, you do not need this chapter. In that case, we take care of management center feature updates, and you can upgrade your devices using the latest released version of the Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center.

Upgrade Checklist for FMC

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

✓	Action/Check	Details
	Assess your deployment.	Understanding where you are determines how you get to where you want to go. In addition to current version and model information, determine if your deployment is configured for high availability/scalability, if your devices are deployed as an IPS or as firewalls, and so on.
	Plan your upgrade path.	This is especially important for large deployments, multi-hop upgrades, and situations where you need to upgrade operating systems or hosting environments. See: • Upgrade Path for FMC, on page 4 • Upgrade Paths for FTD • Upgrade Paths for FXOS

✓	Action/Check	Details
	Read 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 these: • Software Upgrade Guidelines, for critical and release-specific upgrade guidelines. • 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. • CiscoFirepower Release Notes, in the *Open and Resolved Bugs* chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool. • Cisco Firepower 4100/9300 FXOS Release Notes, for FXOS upgrade guidelines for the Firepower 4100/9300.
	Check bandwidth.	Make sure your management network has the bandwidth to perform large data transfers. Whenever possible, upload upgrade packages ahead of time.
	Schedule maintenance windows.	Schedule maintenance windows when they will have the least impact, especially considering the time the upgrade is likely to take. Consider the tasks you must perform in the window, and those you can perform ahead of time. SeeTime and Disk Space Tests.

Backups

We *strongly* recommend you back up to a secure remote location and verify transfer success, both 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. Back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.

✓	Action/Check	Details
	Back up configurations and events.	See the *Backup/Restore* chapter in the Firepower Management Center Administration Guide.

✓	Action/Check	Details
	Back up FXOS on the Firepower 4100/9300.	Use the Firepower Chassis Manager or the FXOS CLI to export chassis configurations, including logical device and platform configuration settings. See the *Configuration Import/Export* chapter in the Cisco Firepower 4100/9300 FXOS Configuration Guide.

Upgrade Packages

Uploading upgrade packages to the system before you begin upgrade can reduce the length of your maintenance window.

✓	Action/Check	Details
	Download the upgrade package from Cisco and upload it to the FMC.	Upgrade packages are available on the Cisco Support & Download site. You may also be able to use the FMC to perform a direct download. For FMC high availability, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to 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 Upgrade Packages for FMC, on page 7.

Associated Upgrades

We recommend you perform hosting environment upgrades in a maintenance window.

✓	Action/Check	Details
	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 upgrade.

Final Checks

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

✓	Action/Check	Details
	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	Details
	Check NTP synchronization.	Make sure all appliances are synchronized with any NTP server you are using to serve time. Although the health monitor alerts if clocks are out of sync by more than 10 seconds, you should still check manually. Being out of sync can cause upgrade failure. To check time: • FMC: Choose **System > Configuration > Time**. • FTD: Use the **show time** CLI command.
	Deploy configurations.	Deploying configurations before you upgrade reduces the chance of failure. Deploying can affect traffic flow and inspection; see Traffic Flow and Inspection for FTD Upgrades.
	Run readiness checks.	Passing compatibility and readiness checks reduce the chance of upgrade failure. See Run Readiness Checks for FMC, on page 7.
	Check disk space.	Readiness checks include a disk space check. Without enough free disk space, the upgrade fails. To check the disk space available on the management center, choose **System** (⚙) > **Monitoring** > **Statistics** and select the FMC. Under Disk Usage, expand the By Partition details.
	Check running tasks.	Make sure essential tasks are complete, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Upgrades from Version 6.6.3+ automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. If you do not want this to happen (or if you are upgrading from an earlier version), check for tasks that are scheduled to run during the upgrade and cancel or postpone them.

Upgrade Path for FMC

This table provides the upgrade path for customer-deployed FMCs.

Remember that a customer-deployed FMC must run the same or newer version as its managed devices. You cannot upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

Note that if your current FTD/FMC version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

Table 1: FMC Direct Upgrades

Current Version	Target Version
7.3	→ Any later 7.3.x release
7.2	Any of: → 7.3.x → Any later 7.2.x release
7.1	Any of: → 7.3.x → 7.2.x → Any later 7.1.x release
7.0 Last support for FMC 1000, 2500, and 4500.	Any of: → 7.3.x → 7.2.x → 7.1.x → Any later 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+.
6.7	Any of: → 7.2.x → 7.1.x → 7.0.x → Any later 6.7.x release

Current Version	Target Version
6.6 Last support for FMC 2000 and 4000.	Any of: → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Any later 6.6.x release **Note** Due to datastore incompatibilities, you cannot upgrade the FMC from Version 6.6.5+ to Version 6.7.0. We recommend you upgrade directly to Version 7.0+.
6.5	Any of: → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 Last support for FMC 750, 1500, and 3500.	Any of: → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Any of: → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3	Any of: → 6.6.x → 6.5 → 6.4 → 6.3

Upload Upgrade Packages for FMC

Use this procedure to manually upload upgrade packages to the FMC.

Tip Select upgrade packages become available for direct download some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors. If the FMC has internet access, you can click the **Download Updates** button to immediately download the latest VDB, latest maintenance release, and the latest critical patches for the FMC and all managed devices.

Upgrade packages are signed tar archives (.tar). After you upload a signed package, the System Updates page on the FMC can take extra time to load as the package is verified. To speed up the display, delete unneeded upgrade packages. Do not untar signed packages.

Before you begin

If you are upgrading the standby FMC in a high availability pair, pause synchronization.

For FMC high availability, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to 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 1 Download the upgrade package from the Cisco Support & Download site: https://www.cisco.com/go/firepower-software.

You use the same software upgrade package for all models in a family or series. To find the correct one, select or search for your model, then browse to the software download page for the appropriate version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads.

Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), software version, and build, like this:

```
Cisco_Firepower_Mgmt_Center_Upgrade-7.1-999.sh.REL.tar
```

Step 2 On the FMC, choose **System** (⚙) > **Updates**.

Step 3 Click **Upload Update**.

Step 4 For the **Action**, click the **Upload local software update package** radio button.

Step 5 Click **Choose File**.

Step 6 Browse to the package and click **Upload**.

Run Readiness Checks for FMC

Use this procedure to run FMC readiness checks.

Readiness checks assess preparedness for major and maintenance upgrades. If you fail readiness checks, you cannot upgrade until you correct the issues. The time required to run a readiness check varies depending on model and database size. Do not manually reboot or shut down during readiness checks.

Before you begin

Upload the upgrade package to the FMC.

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

Step 2 Under Available Updates, click the **Install** icon next to the upgrade package, then choose the FMC.

Step 3 Click **Check Readiness**.

You can monitor readiness check progress in the Message Center.

What to do next

On **System** (⚙) > **Updates**, click **Readiness Checks** to view readiness check status for your whole deployment, including checks in progress and failed checks. You can also use this page to easily re-run checks after a failure.

Upgrade the FMC: Standalone

Use this procedure to upgrade a standalone FMC.

⚠

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.

Before you begin

Complete the pre-upgrade checklist. Make sure your deployment is healthy and successfully communicating.

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

Step 2 Under Available Updates, click the **Install** icon next to the upgrade package, then choose the FMC.

Step 3 Click **Install**, then confirm that you want to upgrade and reboot.

You can monitor precheck progress in the Message Center until you are logged out.

Step 4 Log back in when you can.

- 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.
- Patches and hotfixes: You can log in after the upgrade and reboot are completed.

Step 5 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 6 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 7 Complete any required post-upgrade configuration changes.

Step 8 Redeploy configurations to all managed devices.

Upgrade the FMC: High Availability

Upgrade high availability FMCs one at a time. With synchronization paused, first upgrade the standby, then the active. When the standby starts the upgrade, 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 (and patch uninstall).

Caution Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization. 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.

Before you begin

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

Step 1 On the active FMC, pause synchronization.

a) Choose **System** > **Integration**.

b) On the **High Availability** tab, click **Pause Synchronization**.

Step 2 Upload the upgrade package to the standby.

For FMC high availability, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to 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 the FMC: Standalone, on page 8, 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 may happen twice).

c) Verify upgrade success.

Step 4 On the FMC you want to make the active peer, restart synchronization.

a) Choose **System** > **Integration**.
b) On the **High Availability** tab, click **Make-Me-Active**.
c) 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 required post-upgrade configuration changes.

Step 7 Redeploy configurations to all managed devices.