Freshly Install Version 6.2.3

If you are unable to upgrade a Firepower appliance, or are disinclined to follow the required upgrade path, you can freshly install major Firepower releases.

Deciding to Freshly Install

Use this table to identify scenarios where you need to freshly install. In all of these scenarios—including switching device management between local and remote—*you will lose device configurations*.

Note *Always* address licensing concerns before you reimage or switch management of a Firepower appliance. If you are using Cisco Smart Licensing, you may need to manually unregister from the Cisco Smart Software Manager to avoid accruing orphan entitlements. If you do not manually unregister, you may not be able to register a device if it is still registered with smart licensing

Table 1: Scenarios: Do You Need a Fresh Install?

Scenario	Solution	Licensing
Upgrade FMC-managed devices from an older Firepower version (5.x, 6.0.x).	The upgrade path from older versions includes intermediate versions. Especially in larger deployments where you must alternate FMC and device upgrade, this multi-step process can be time consuming. To save time, you can reimage older devices instead of upgrading: **1.** Remove the devices from the FMC. **2.** Upgrade the FMC only (5.x → 6.0 → 6.0.1 → 6.1 → 6.2.3+). **3.** Reimage the devices. **4.** Re-add the devices to the FMC.	Removing devices from the FMC unregisters them. Reassign licenses after you re-add the devices.
Change FTD management from FDM to FMC (local to remote).	Use the **configure manager** CLI command; see Command Reference for Firepower Threat Defense.	Unregister the device before you switch management. Reassign its license after you add it to the FMC.
Change FTD management from FMC to FDM (remote to local).	Use the **configure manager** CLI command; see Command Reference for Firepower Threat Defense. **Exception:** The device is running or was upgraded from Version 6.0.1. In this case, fresh install.	Remove the device from the FMC to unregister it. Reregister using FDM.
Change ASA FirePOWER management between ASDM and FMC.	Start using the other management method.	Contact Sales for new Classic licenses. ASA FirePOWER licenses are associated with a specific manager.
Replace ASA FirePOWERwith FTD on the *same* physical device.	Fresh install.	Convert Classic to Smart licenses; see the Firepower Management Center Configuration Guide.
Replace NGIPSv with FTDv.	Fresh install.	Contact Sales for new Smart licenses.

Guidelines and Limitations for Fresh Installs

Careful planning and preparation can help you avoid missteps. Even if you are familiar with Firepower releases and have previous experience reimaging Firepower appliances, make sure you read these guidelines and limitations, as well as the instructions linked in Installation Instructions, on page 5.

Back Up Event and Configuration Data

We *strongly* recommend backing up event and configuration data to an external location. Reimaging returns most settings to factory defaults, including the system password (Admin123).

Note, however, if you are reimaging so that you don't have to upgrade, you cannot use a backup to import your old configurations. You can restore a backup only from an appliance of the same model *and Firepower version*.

Remove Devices from the Firepower Management Center

Always remove devices from remote management before you reimage. If you are:

- Reimaging the FMC, remove all its devices from management.
- Reimaging a single device or switching from remote to local management, remove that one device.

Address Licensing Concerns

Before you reimage *any* Firepower appliance, address licensing concerns. You may need to unregister from the Cisco Smart Software Manager, or you may need to contact Sales for new licenses. See Deciding to Freshly Install to determine what you need to do, depending on your scenario.

For more information on licensing, see:

- Cisco Firepower System Feature Licenses Guide
- Frequently Asked Questions (FAQ) about Firepower Licensing
- The licensing chapter in your *Configuration Guide*.

Appliance Access During and After Reimage

Reimaging returns most settings to factory defaults.

If you do not have physical access to an appliance, the reimage process lets you keep management network settings. This allows you to connect to the appliance after you reimage to perform the initial configuration. If you delete network settings, you *must* have physical or Lights-Out Management (LOM) access to the appliance. Note that LOM is only supported on select appliances and must be already configured.

For devices, 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.

Reimaging Firepower 2100 Devices to Earlier Major Versions

We recommend that you perform a *complete* reimage if you need to revert a Firepower 2100 series device to an earlier major version. If you use the erase configuration method, FXOS may not revert along with the Firepower Threat Defense software. This can cause failures, especially in high availability deployments.

For more information, see the Reimage Procedures chapter of the *Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series Running Firepower Threat Defense*.

Unregistering Smart Licenses

Firepower Threat Defense devices, whether locally (Firepower Device Manager) or remotely (Firepower Management Center) managed, use Cisco Smart Licensing. To use licensed features, you must register with Cisco Smart Software Manager (CSSM). Before you reimage or switch management, you must manually unregister to avoid accruing orphan entitlements.

Unregistering removes an appliance from your virtual account, and also releases associated licenses so they can be can be reassigned. When you unregister an appliance, it enters Enforcement mode. Its current configuration and policies continue to work as-is, but you cannot make or deploy any changes.

Unregister from CSSM before you:

- Reimage a Firepower Management Center that manages FTD devices.
- Reimage a Firepower Threat Defense device that is locally managed by FDM.
- Switch a Firepower Threat Defense device from FDM to FMC management.

Do not unregister from CSSM when you:

- Reimage a Firepower Threat Defense device that is managed by an FMC.
- Switch a Firepower Threat Defense device from FMC to FDM management.

In these two cases, removing the device from the FMC automatically unregisters the device. You do not have to unregister manually as long as you remove the device from the FMC.

Tip Classic licenses for NGIPS devices are associated with a specific manager (ASDM/FMC), and are not controlled using CSSM. If you are switching management of a Classic device, or if you are migrating from an NGIPS deployment to an FTD deployment, contact Sales.

Unregister a Firepower Management Center

Unregister a Firepower Management Center from the Cisco Smart Software Manager before you reimage the FMC. This also unregisters any managed Firepower Threat Defense devices.

If the FMC is configured for high availability, licensing changes are automatically synchronized. You do not need to unregister the other FMC.

Step 1 Log into the Firepower Management Center.

Step 2 Choose **System** > **Licenses** > **Smart Licenses**.

Step 3 Next to Smart License Status, click the stop sign (●).

Step 4 Read the warning and confirm that you want to unregister.

Unregister an FTD Device Using FDM

Unregister locally managed Firepower Threat Defense devices from the Cisco Smart Software Manager before you either reimage or switch to remote (FMC) management.

Step 1 Log into the Firepower Device Manager.

Step 2 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 3 Select **Unregister Device** from the gear drop-down list.

Step 4 Read the warning and confirm that you want to unregister.

Installation Instructions

The release notes do not contain installation instructions. Instead, see one of the following documents. Installation packages are available on the Cisco Support & Download site.

Table 2: Firepower Management Center Installation Instructions

FMC Platform	Guide
FMC 750, 1500, 2000, 3500, 4000	Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500, and 4000 — Restoring a Firepower Management Center to Factory Defaults
FMC 1000, 2500, 4500	Cisco Firepower Management Center Getting Started Guide for Models 1000, 2500, and 4500 — Restoring a Firepower Management Center to Factory Defaults
FMCv	Cisco Firepower Management Center Virtual Deployment Guide

Table 3: Firepower Threat Defense Installation Instructions

FTD Platform	Guide
Firepower 2100 series	Reimage the Cisco ASA or Firepower Threat Defense Device *and* Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series Running Firepower Threat Defense
Firepower 4100/9300 chassis	Cisco Firepower 4100/9300 FXOS Configuration Guides — Image Management chapters
ASA 5500-X series ISA 3000	Reimage the Cisco ASA or Firepower Threat Defense Device
FTDv: VMware, with FMC	Cisco Firepower Threat Defense Virtual for VMware Deployment Quick Start Guide
FTDv: VMware, with FDM	Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for VMware Deployment Quick Start Guide
FTDv: KVM, with FMC	Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide
FTDv: KVM, with FDM	Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for KVM Deployment Quick Start Guide
FTDv: AWS	Cisco Firepower Threat Defense Virtual Quick Start Guide for the AWS Cloud

FTD Platform	Guide
FTDv: Azure	Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

Table 4: Firepower 7000/8000 Series, NGIPSv, and ASA FirePOWER Installation Instructions

NGIPS Platform	Guide
Firepower 7000 series	Cisco Firepower 7000 Series Getting Started Guide — Restoring a Device to Factory Defaults
Firepower 8000 series	Cisco Firepower 8000 Series Getting Started Guide — Restoring a Device to Factory Defaults
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware
ASA FirePOWER	Reimage the Cisco ASA or Firepower Threat Defense Device *and* ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide — Managing the ASA FirePOWER Module