

Install the Software

If you cannot or do not want to upgrade to Version 7.0, you can freshly install major and maintenance releases. This is also called *reimaging*. We do not provide installation packages for patches. To run a particular patch, install the appropriate major or maintenance release, then apply the patch.

- Installation Guidelines, on page 1
- Installation Guides, on page 3

Installation Guidelines

These guidelines can prevent common reimage issues, but are not comprehensive. For detailed checklists and procedures, see the appropriate installation guide.

Backups

Before you reimage, we *strongly* recommend you back up to a secure remote location and verify transfer success. Reimaging returns most settings to factory defaults, including the system password. It deletes any backups left on the appliance.

Note If you want to reimage so that you don't have to upgrade, due to version restrictions you cannot use a backup to import your old configurations. You must recreate your configurations manually.

Appliance Access

If you do not have physical access to an appliance, reimaging to the current major or maintenance release lets you keep management network settings. This allows you to connect to the appliance after you reimage to perform the initial configuration. Note that if you delete network settings or if you reimage to an earlier release, you must have physical access to the appliance. You cannot use Lights-Out Management (LOM).

For devices, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In Firewall Management Center deployments, you should also able to access the Firewall Management Center's management interface without traversing the device.

Unregistering from Smart Software Manager

Before you reimage any appliance or switch device management, you may need to unregister from the Cisco Smart Software Manager (CSSM). This is to avoid accruing orphan entitlements, which can prevent you from reregistering.

Unregistering removes an appliance from your virtual account, unregisters it from the cloud and cloud services, and 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.

If you plan to restore from backup, do not unregister before you reimage and do not remove devices from the Firewall Management Center. Instead, manually revert any licensing changes made since you took the backup. After the restore completes, reconfigure licensing. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.

Table 1: Scenarios for Unregistering from CSSM (Not Restoring from Backup)

Scenario	Action
Reimage the Firewall Management Center.	Unregister manually.
Model migration for the Firewall Management Center.	Unregister manually, before you shut down the source Firewall Management Center.
Reimage Firewall Threat Defense with Firewall Management Center.	Unregister automatically, by removing the device from the Firewall Management Center.
Reimage Firewall Threat Defense with Firewall Device Manager.	Unregister manually.
Switch Firewall Threat Defense from Firewall Management Center to Firewall Device Manager.	Unregister automatically, by removing the device from the Firewall Management Center.
Switch Firewall Threat Defense from device manager to Firewall Management Center.	Unregister manually.

Removing Devices from the Firewall Management Center

In Firewall Management Center deployments, if you plan to manually configure the reimaged appliance, remove devices from the Firewall Management Center before you reimage either. If you plan to restore from backup, you do not need to do this.

Table 2: Scenarios for Removing Devices from the Firewall Management Center (Not Restoring from Backup)

Scenario	Action
Reimage the Firewall Management Center.	Remove all devices from management.
Reimage Firewall Threat Defense.	Remove the one device from management.
Switch Firewall Threat Defense from Firewall Management Center to Firewall Device Manager.	Remove the one device from management.

Fully Reimaging Firewall Threat Defense Hardware to Downgrade FXOS

For Firewall Threat Defense hardware models that use the FXOS operating system, reimaging to an earlier software version may require a full reimage, regardless of whether FXOS is bundled with the software or upgraded separately.

Table 3: Scenarios for Full Reimages

Model	Details
Firepower 1000 series Firepower 2100 series	If you use the **erase configuration** method to reimage, FXOS may not downgrade along with the software. This can cause failures, especially in high availability deployments. We recommend that you perform full reimages of these devices.
Firepower 4100/9300	Reverting Firewall Threat Defense does not downgrade FXOS. Major Firewall Threat Defense versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of Firewall Threat Defense, you may be running a non-recommended version of FXOS (too new). Although newer versions of FXOS are backwards compatible with older Firewall Threat Defense versions, we do perform enhanced testing for the recommended combinations. You cannot manually downgrade FXOS, so if you find yourself in this situation and you want to run a recommended combination, you will need a full reimage.

Installation Guides

Table 4: Installation Guides

Platform	Guide
Firewall Management Center	
FMC 1600, 2600, 4600	*Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide*
FMC 1000, 2500, 4500	*Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide*
Firewall Management Center Virtual	*Cisco Secure Firewall Management Center Virtual Getting Started Guide*
Firewall Threat Defense	
Firepower 1000/2100 series	*Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide* *Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense*

Platform	Guide
Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Configuration Guides: *Image Management* chapters *Cisco Firepower 4100 Getting Started Guide* *Cisco Firepower 9300 Getting Started Guide*
ASA 5500-X series	*Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*
ISA 3000	*Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*
Firewall Threat Defense Virtual	Secure Firewall Threat Defense Virtual getting started guides
ASA FirePOWER/NGIPSv	
ASA FirePOWER	*Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide* ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware