Install the Software

If you cannot or do not want to upgrade to Version 7.3, 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

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

Reimaging the Secure Firewall 3100 to Version 7.3+

Reimage Impact.

In Version 7.3, we combined the threat defense install and upgrade package for the Secure Firewall 3100, as follows:

- Version 7.1–7.2 install package: cisco-ftd-fp3k.*version*.SPA
- Version 7.1–7.2 upgrade package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar
- Version 7.3+ combined package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar

Although you can upgrade threat defense without issue, you cannot reimage from older threat defense and ASA versions directly to threat defense Version 7.3+. This is due to a ROMMON update required by the new image type. To reimage from those older versions, you must "go through" ASA 9.19+, which is supported with the old ROMMON but also updates to the new ROMMON. There is no separate ROMMON updater.

To get to threat defense Version 7.3+, your options are:

- Upgrade from threat defense Version 7.1 or 7.2 — use the normal upgrade process.

  See the appropriate Upgrade Guide.

- Reimage from threat defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to threat defense Version 7.3+.

See *Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100* and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

- Reimage from ASA 9.17 or 9.18 — upgrade to ASA 9.19+ first, then reimage to threat defense Version 7.3+.

  See the Cisco Secure Firewall ASA Upgrade Guide and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

- Reimage from threat defense Version 7.3+ — use the normal reimage process.

  See *Reimage the System with a New Software Version* in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense.

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 management center deployments, you should also able to access the 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 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 management center.	Unregister manually.
Model migration for the management center.	Unregister manually, before you shut down the source management center.
Reimage threat defense with management center.	Unregister automatically, by removing the device from the management center.
Reimage threat defense with device manager.	Unregister manually.
Switch threat defense from management center to device manager.	Unregister automatically, by removing the device from the management center.
Switch threat defense from device manager to management center.	Unregister manually.

Removing Devices from the Management Center

In management center deployments, if you plan to manually configure the reimaged appliance, remove devices from the 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 Management Center (Not Restoring from Backup)

Scenario	Action
Reimage the management center.	Remove all devices from management.
Reimage threat defense.	Remove the one device from management.
Switch threat defense from management center to device manager.	Remove the one device from management.

Fully Reimaging Threat Defense Hardware to Downgrade FXOS

For 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 Secure Firewall 3100 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.

Model	Details
Firepower 4100/9300	Reverting threat defense does not downgrade FXOS. For the Firepower 4100/9300, major threat defense versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of threat defense, you may be running a non-recommended version of FXOS (too new). Although newer versions of FXOS are backwards compatible with older 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
Management Center	
FMC 1600, 2600, 4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
Management Center Virtual	Cisco Secure Firewall Management Center Virtual Getting Started Guide
Threat Defense	
Firepower 1000/2100 series Secure Firewall 3100 series	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense
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
ISA 3000	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide
Threat Defense Virtual	Cisco Secure Firewall Threat Defense Virtual Getting Started Guide