Getting Started

Is this Guide for You?

This guide explains how to prepare for and complete a successful upgrade of **Secure Firewall Threat Defense** with **Secure Firewall device manager** currently running **Version 7.2**.

Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. We also may provide hotfixes, which are minor updates that address particular, urgent issues.

Additional Resources

If you are upgrading a different platform/component, upgrading to/from a different version, or are using a cloud-based manager, see one of these resources.

Table 1: Upgrading Management Center

Current Management Center Version	Guide
Cloud-delivered management center (no version)	None. We take care of updates.
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version.
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1.
7.0 or earlier	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Table 2: Upgrading Threat Defense with Management Center

Current Management Center Version	Guide
Cloud-delivered management center (no version)	The latest released version of the Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center.
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version.
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1.
7.0 or earlier	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Table 3: Upgrading Threat Defense with Device Manager

Current Threat Defense Version	Guide
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager for your version.
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1.
7.0 or earlier	*System Management* in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for your version. For the Firepower 4100/9300, also see the FXOS upgrade instructions in the Cisco Firepower 4100/9300 Upgrade Guide, FTD 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1.
Version 6.4+, with CDO	*Onboard Devices and Services* in Managing FDM Devices with Cisco Defense Orchestrator.

Table 4: Upgrading Other Components

Version	Component	Guide
Any	ASA logical devices on the Firepower 4100/9300	Cisco Secure Firewall ASA Upgrade Guide.
Latest	BIOS and firmware for management center	Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes.
Latest	Firmware for the Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide
Latest	ROMMON image for the ISA 3000	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the upgrade chapters.

Table 5: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up the software. Back up FXOS on the Firepower 4100/9300.
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300.
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

Feature History

Table 6: Version 7.0.0 Features

Feature	Description
Upgrade readiness check for device manager-managed devices.	You can run an upgrade readiness check on an uploaded threat defense upgrade package before attempting to install it. The readiness check verifies that the upgrade is valid for the system, and that the system meets other requirements needed to install the package. Running an upgrade readiness check helps you avoid failed installations. A link to run the upgrade readiness check was added to the **System Upgrade** section of the **Device** > **Updates** page.

Table 7: Version 6.7.0 Features

Feature	Description
Ability to cancel a failed threat defense software upgrade and to revert to the previous release.	If an threat defense major software upgrade fails or is otherwise not functioning correctly, you can revert to the state of the device as it was when you installed the upgrade. We added the ability to revert the upgrade to the System Upgrade panel in FDM. During an upgrade, the FDM login screen shows the upgrade status and gives you the option to cancel or revert in case of upgrade failure. In the threat defense API, we added the CancelUpgrade, RevertUpgrade, RetryUpgrade, and UpgradeRevertInfo resources. In the threat defense CLI, we added the following commands: **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**.

Table 8: Version 6.2.0 Features

Feature	Description
Upgrade threat defense software through device manager.	You can install software upgrades through device manager. Select **Device** > **Updates**.

For Assistance

Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco software and to troubleshoot and resolve technical issues.

- Documentation: http://www.cisco.com/go/threatdefense-72-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts