

# Why You Shouldn't Fear Your Firewall Upgrade

The Evolution and How-to Guide

John Payne  
Technical Marketing Engineer

**CISCO** Live !

# Cisco Webex App

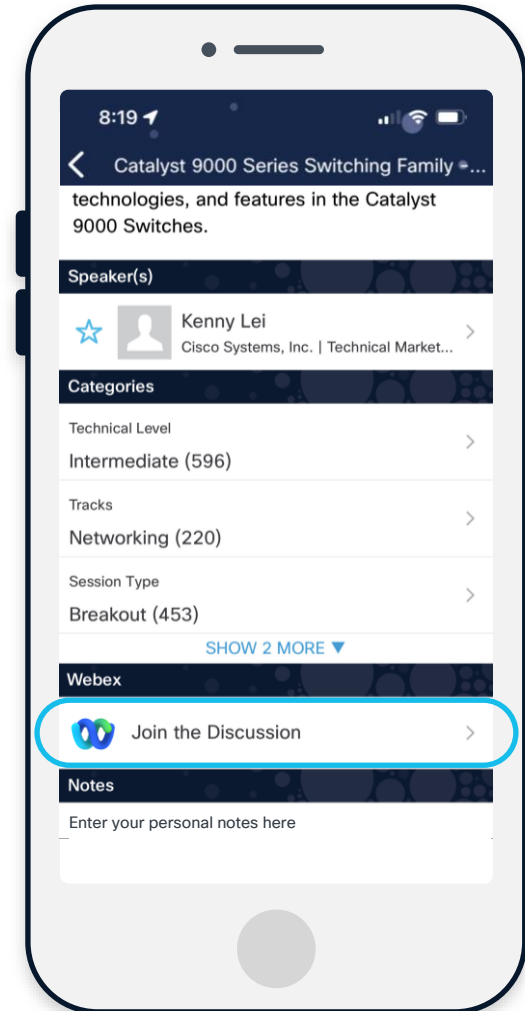
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

**Webex spaces will be moderated by the speaker until June 13, 2025.**



# About Me...

- 2018 – CCNA
  - 2020 – CCNP Security
  - 2019 – 2021 – Cisco POC Lab Lead
  - 2022 – 2025 – Technical Marketing Engineer, Secure Firewall
- 
- Have 2 Miniature Dachshunds
  - Avid Golfer
  - Originally from New Jersey and moved to North Carolina



New Jersey to North Carolina



# Agenda

- 01 Why Upgrade?
- 02 Where We Came From
- 03 Upgrade Planning & Preparation
- 04 Upgrade Steps – What actually happens?
- 05 Upgrade Steps – How to
- 06 Where We Are Going
- 07 Best Practices



AI generated image

# Reminder

## Firewall Platforms



Firepower 2110  
Firepower 2120  
Firepower 2130  
Firepower 2140



Firepower 4110  
Firepower 4120  
Firepower 4140  
Firepower 4150

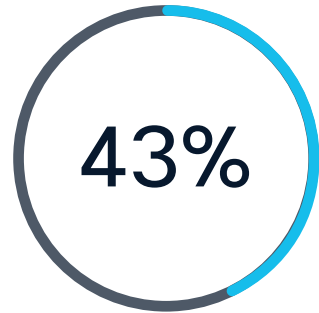


Firepower 9300: SM-24  
Firepower 9300: SM-36  
Firepower 9300: SM-44

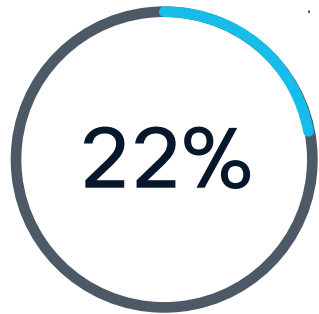


# Why Upgrade?

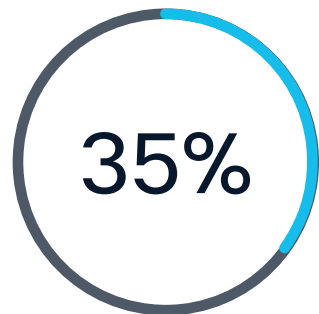
# Release Adoption



Running Threat Defense Code  
0 - 2 years



Running Threat Defense Code  
older than 3 years



Running Threat Defense Code  
older than 4 years

Low adoption prevents you from benefiting from the latest features and increased risk of potential quality and security issues.

# New Features!

## Encrypted Visibility Engine

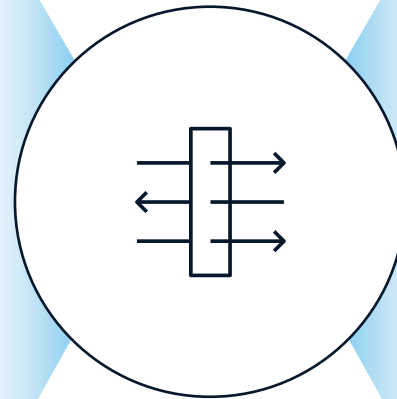
AI/ML-driven detection of apps and malware in encrypted traffic, without decrypting

## AI Assistant for Firewall

Enables quick discovery of policies with fast, rich data responses on-demand

## SnortML

Deep neural network engine to detect exploits, trained on malicious and benign traffic



## Firewall

## Intelligent Decryption Bypass

Risk-based intelligent decryption bypass, powered by the Encrypted Visibility Engine and Talos Server Reputation

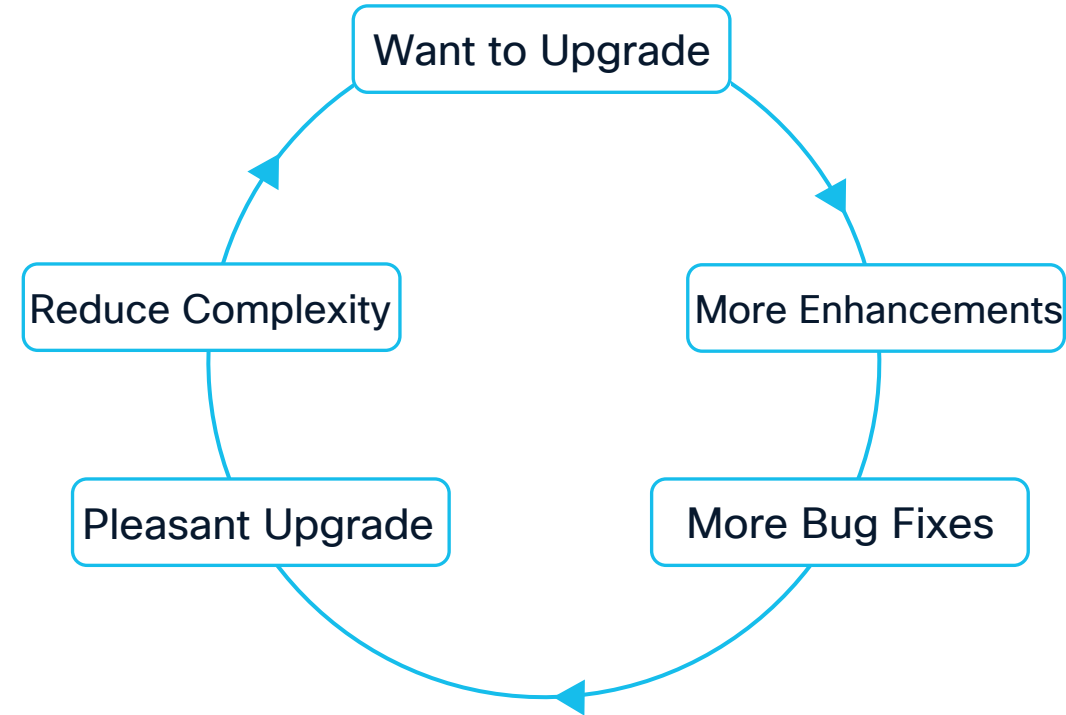
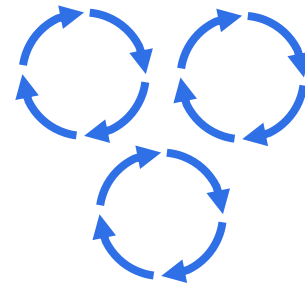
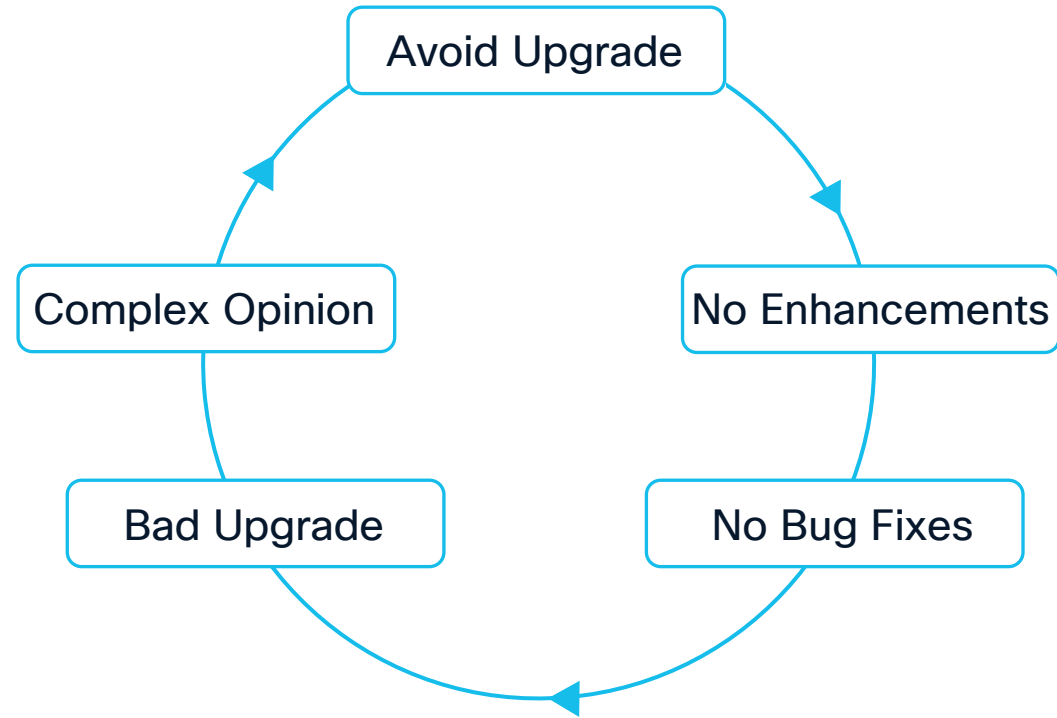
## Bulk Branch Pre-Provisioning

Apply pre-provisioned configurations to many devices at the time of registration

## Geolocation-based RAVPN

Manage remote access VPN connections of users based on their geolocation

# Don't fall into a trap...



# Where We Came From...

# Upgrade Enhancements Over Releases



7.0 ————— • 7.2 ————— • 7.4 ————— • 7.6 ————— • 7.7

- Fleet Upgrade Improvements
- Requirement for devices to pass Compatibility Check

- Package Management for FMC & FTD (7.2.6/7.4.1)
- Peer-to-peer Sync for Upgrade Packages
- Unattended FTD Upgrades (7.2.6)
- Upgrade-related Defects

- Reduced backup time
- FMC: New Upgrade Wizard for FTD & FMC (7.2.6/7.4.1)
- FMC: In product notifications for suggested releases
- FMC: Automatically generate configuration change report post-FMC upgrade

- FMC HA Upgrade Simplification – Eliminates manual upgrade needs on both Management Center peers
- Upgrade Optimizations – Reduce failures
- Reduce Upgrade time to 23 minutes

- Start FTD Upgrades without upgrade package – devices automatically obtain package from the internet
- Readiness check optimization
- Upgrade times reduced by 33%
- User input reduced by 50%

# Firewall Upgrades in Version 6.x to 7.x

The image shows a sequence of four overlapping screenshots from the Cisco Firepower Management Center (FMC) interface, illustrating the steps to upgrade firewalls from version 6.x to 7.x.

**Step 1: Product Updates**  
The first screenshot shows the 'Product Updates' page. A callout box labeled 'Upload Update' points to the 'Upload Update' button in the top right corner.

**Step 2: Device Upgrade**  
The second screenshot shows the 'Device Upgrade' page. The 'Upgrade to:' dropdown is set to '7.x'. The 'Device Selection' section shows '2 devices selected'.

**Step 3: Device Selection**  
The third screenshot shows the 'Device Selection' page. The 'Upgrade to:' dropdown is set to '7.0.5-72'. The 'Device Selection' table shows '2 devices ready for upgrade to Version 7.0.5-72'. The 'Upgrade Failure Preferences' section has the checkbox 'Automatically cancel on upgrade failure and roll back to the previous version.' checked.

**Step 4: Upgrade**  
The fourth screenshot shows the 'Upgrade' page. The 'Device Details' table shows '2 devices ready for upgrade'. The 'Start Upgrade' button is highlighted. A callout box labeled 'Upgrade!' points to this button.

Device	Model	Details
ftd01 Version 6.4.0.16	FTDv for VMware	Ready for upgrade. Compatibility and readines...
ftd02 Version 6.4.0.16	FTDv for VMware	Ready for upgrade. Compatibility and readines...

# Upgrade Planning & Preparation

# Deployment Assessment



# FMC to Device Compatibility

FMC Version	Device Version											
	7.7	7.6.x	7.4.x	7.3.x	7.2.x	7.1.x	7.0.x	6.7.x	6.6.0	6.5.0	6.4.0	
7.7	Yes	Yes	Yes	Yes	Yes	-	-	-	-	-	-	-
7.6.x	-	Yes	Yes	Yes	Yes	Yes	-	-	-	-	-	-
7.4.x	-	-	Yes	Yes	Yes	Yes	Yes	-	-	-	-	-
7.3.x	-	-	-	Yes	Yes	Yes	Yes	Yes	-	-	-	-
7.2.x	-	-	-	-	Yes	Yes	Yes	Yes	Yes	-	-	-
7.1.x	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	-
7.0.x	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes
6.7.x	-	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes
6.6.x	-	-	-	-	-	-	-	-	Yes	Yes	Yes	Yes
6.5.0	-	-	-	-	-	-	-	-	-	Yes	Yes	Yes
6.4.0	-	-	-	-	-	-	-	-	-	-	-	Yes

# Supported Upgrade Paths

Current Version	Target Version
7.7.x	Any later 7.7.x release (future)
7.6.x	Any later 7.6.x release (future)
7.4.x	Any later 7.4.x release + 7.6.x + 7.7.x
7.3.x	Any later 7.3.x release + 7.4.x + 7.6.x + 7.7.x
<b>7.2.x</b>	Any later 7.2.x release + 7.3.x + + 7.4.x + 7.6.x + 7.7.x
7.1.x	Any later 7.1.x release + 7.2.x + 7.3.x + 7.4.x + 7.6.x
<b>7.0.x</b>	Any later 7.0.x release + 7.1.x + <b>7.2.x</b> + 7.3.x + 7.4.x
6.6.x	Any later 6.6.x release + 6.7.x + 7.0.x + 7.1.x + 7.2.x
6.5	6.6.x + 6.7.x + 7.0.x + 7.1.x
<b>6.4.x</b>	6.5 + 6.6.x + 6.7.x + <b>7.0.x</b>

# Upgrade Checklist

- Plan upgrade path.
- Ensure no more than 2 DNS servers are configured for **FDM-Managed Devices**.
- Check disk space.
- Confirm connectivity to remote back up servers (if applicable) and back up FTD and FMC configurations.
- Upload FMC and FTD upgrade packages to an Internal Server or FMC.
- Check bandwidth.
- Schedule maintenance window(s).
- Check configurations.
- Upgrade FXOS. (For Firepower 4100/9300)
- Run FMC Readiness Checks.
- Upgrade Standalone or High-Availability FMC(s).
- Redeploy configurations to managed devices.
- Run FTD Readiness Checks.
- Upgrade Standalone or High-Availability FTD.
- Redeploy configurations to upgraded devices.

# Upgrade Steps – Step by Step

# FMC Upgrade Flow

Image Download

- Start on the Standby Unit first
- User triggers download action using the Product Upgrades page

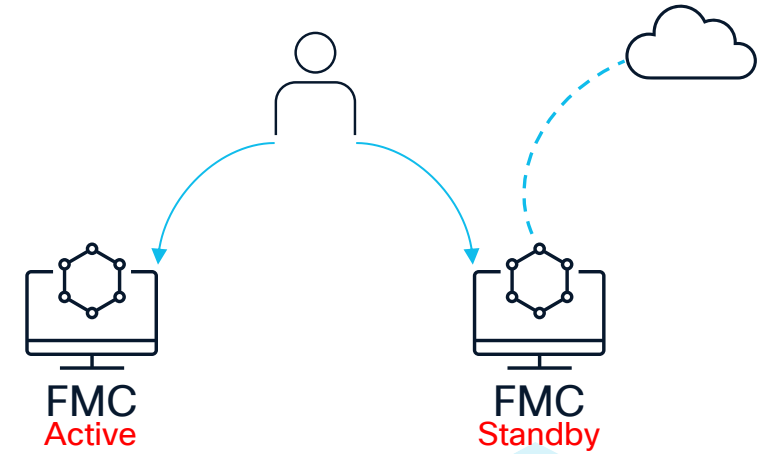
Launch Upgrade Wizard

FMC Selected for Upgrade

Run Readiness Check

Start Upgrade

Next Steps



**Product Upgrades**

**System Overview**

Management Center: 7.6.0-113  
New upgrade available: 7.7.0-91  
Last upgrade performed: 7.4.0-118 – 7.6.0-113

Threat Defense: 1 device  
Visit Device Management to view your devices.

**Available Upgrade Packages**

These are the downloadable upgrades that apply to your current deployment, and the upgrade packages you have manually uploaded or configured. [Upgrade Guide](#)

Upgrade	Release Date	Required Minimum Version	Availability	Actions
> 7.7.0-91	2025-03-14	7.2.0	Available for download @	Download
> 7.6.0-113	2024-09-13	7.1.0	Downloaded	...
> 7.4.2.2-28	2025-02-28	7.4.2	Available for download	Download
> 7.4.2.1-30	2024-10-05	7.4.2	Available for download	Download

Available package list last retrieved May 11, 2025 1:37 AM EDT

[Add Upgrade Package](#)

# FMC Upgrade Flow

Image Download



Launch Upgrade Wizard

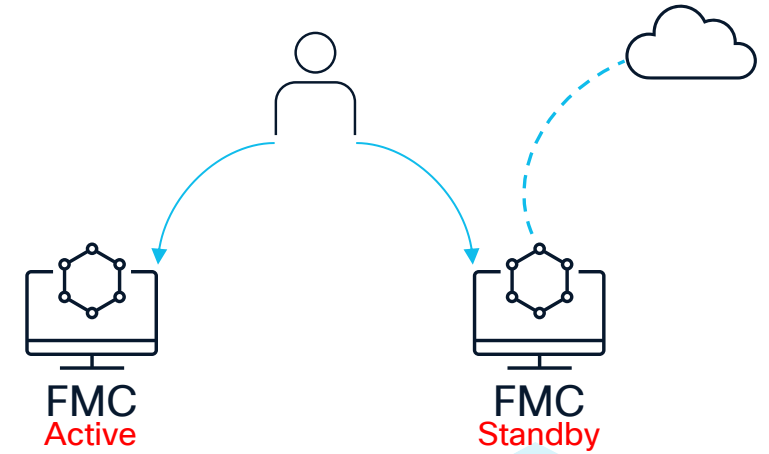
- Choose your target version
- Prechecks are ran automatically; Disk space & Compatibility
- Run Readiness Check

FMC Selected for Upgrade

Run Readiness Check

Start Upgrade

Next Steps



Firewall Management Center  
System / Product Upgrades

System Overview

Management Center: 7.6.0-113  
New upgrade available: 7.7.0-91  
Last upgrade performed: 7.4.0-118 - 7.6.0-113

Threat Defense: 1 device  
Visit Device Management to view your devices.

Available Upgrade Packages

These are the downloadable upgrades that apply to your current deployment, and the upgrade packages you have manually uploaded or configured.

Upgrade	Release Date	Required Minimum Version	Availability	Actions
> 7.7.0-91	2025-03-14	7.2.0	Downloaded for all devices	Upgrade
> 7.6.0-113	2024-09-13	7.1.0	Downloaded	...
> 7.4.2.2-28	2025-02-28	7.4.2	Available for download	Download
> 7.4.2.1-30	2024-10-05	7.4.2	Available for download	Download

Available package list last retrieved May 11, 2025 1:37 AM EDT

# FMC Upgrade Flow

Image Download



Launch Upgrade Wizard



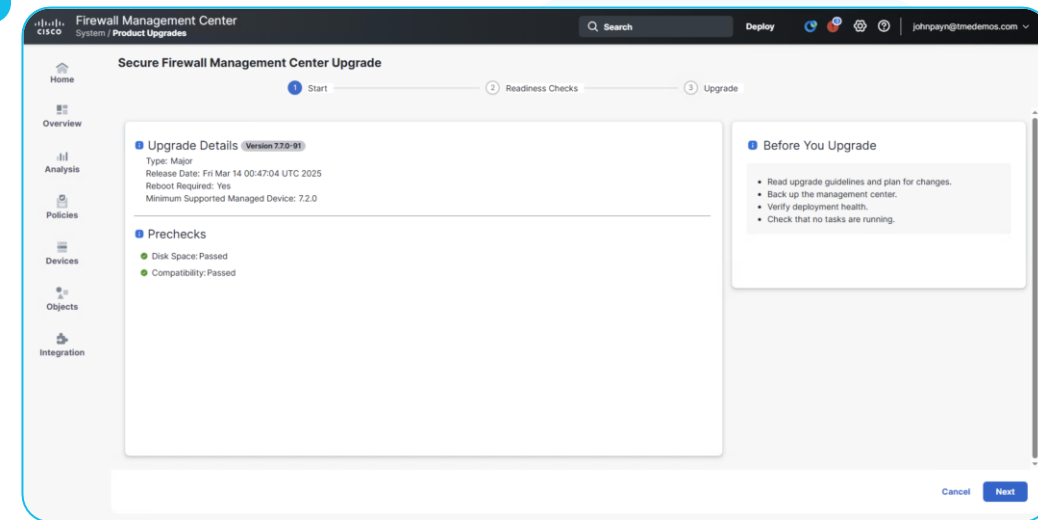
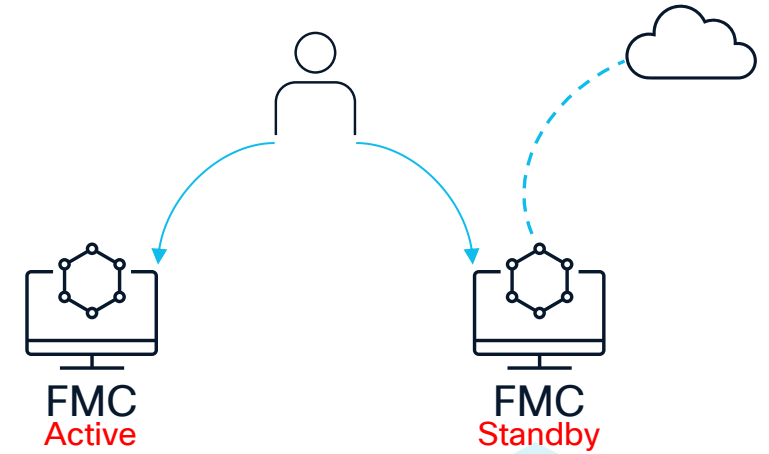
FMC Selected for Upgrade

- Target version selected
- Ensure Green check marks next to Prechecks

Run Readiness Check

Start Upgrade

Next Steps



# FMC Upgrade Flow

Image Download



Launch Upgrade Wizard



FMC Selected for Upgrade

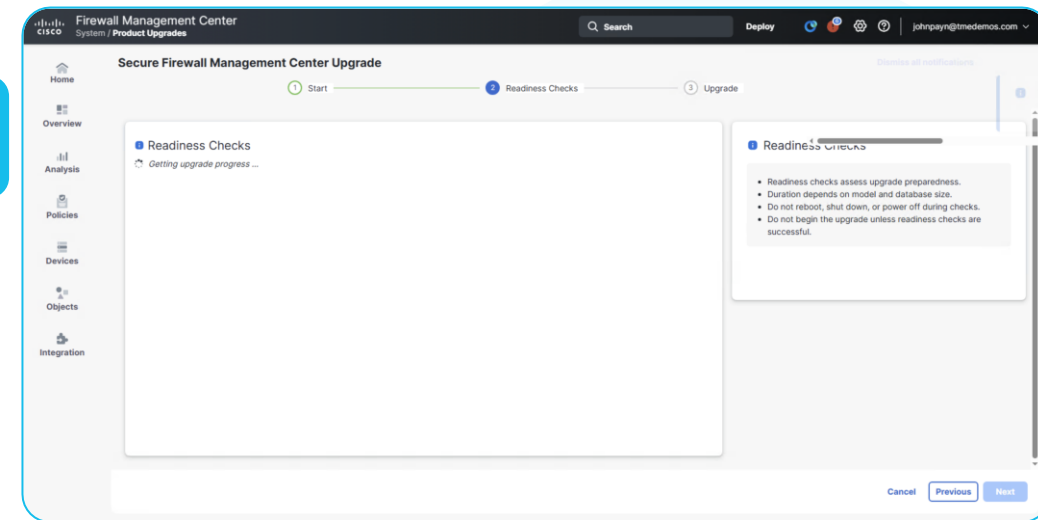
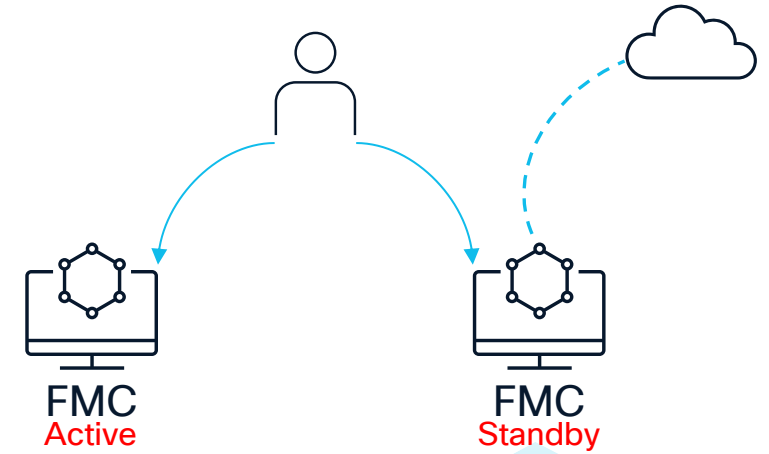


Run Readiness Check

- Assess Upgrade preparedness
- Ensure Green check marks next to Prechecks

Start Upgrade

Next Steps



# FMC Upgrade Flow

Image Download



Launch Upgrade Wizard



FMC Selected for Upgrade



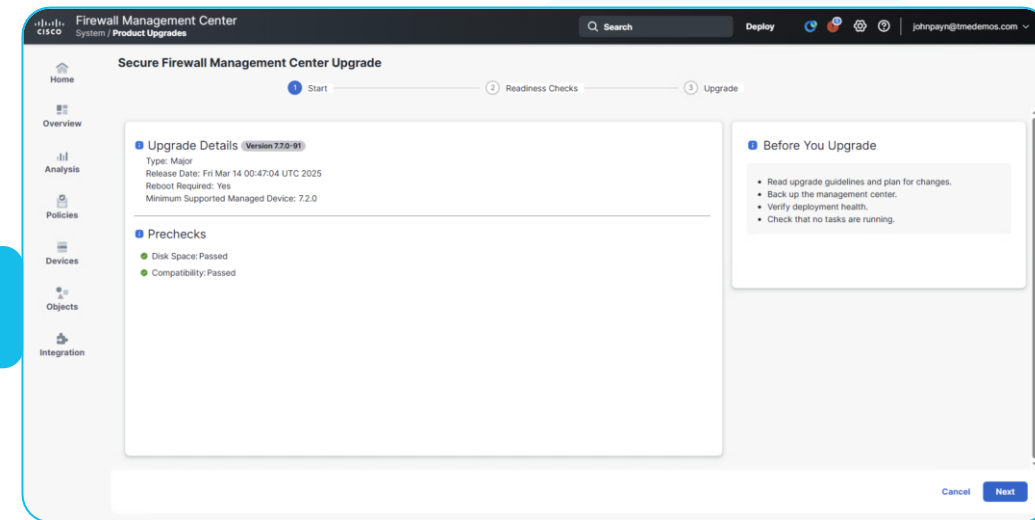
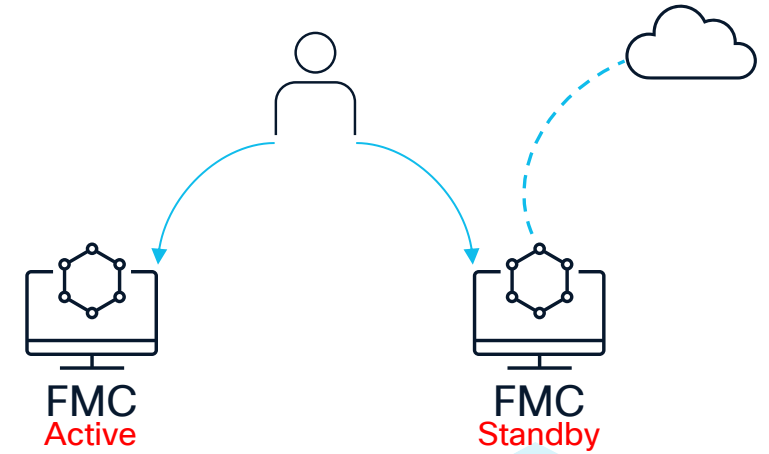
Run Readiness Check



Start Upgrade

- Install FMC version with a single click
- Perform actions on standby before moving to active FMC

Next Steps



# FMC Upgrade Flow

Image Download



Launch Upgrade Wizard



FMC Selected for Upgrade



Run Readiness Check

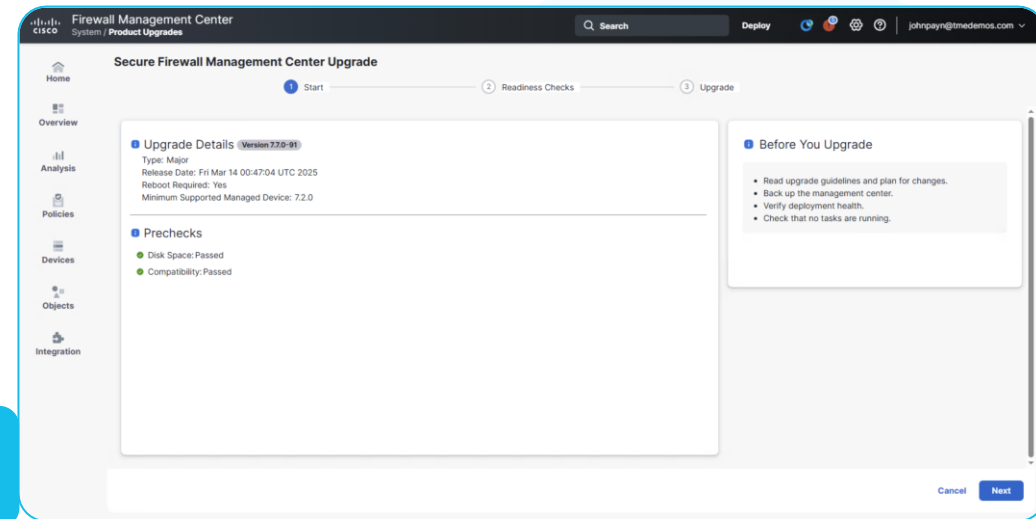
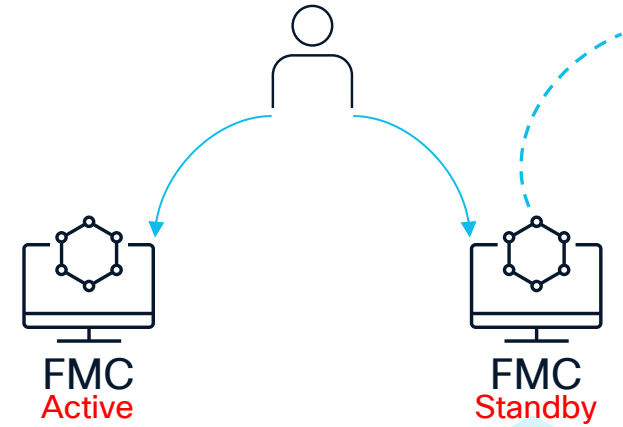


Start Upgrade



Next Steps

- Upgrade Active FMC
- Upgrade the managed devices



# FTD Upgrade Architecture

# FTD Upgrade Flow

## Image Download

- User triggers download action using the Product Upgrades page
- Image directly pulled from software repository

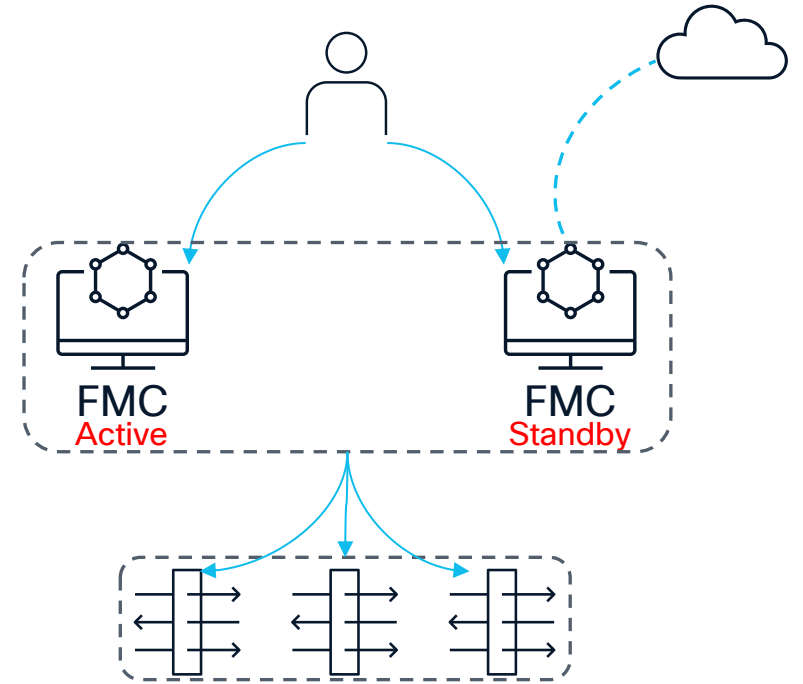
## Launch Upgrade Wizard

## Select Devices for Upgrade

## Copy Packages and Run Readiness

## Start Upgrade

## Next Steps



# FTD Upgrade Flow

Image Download



Launch Upgrade Wizard

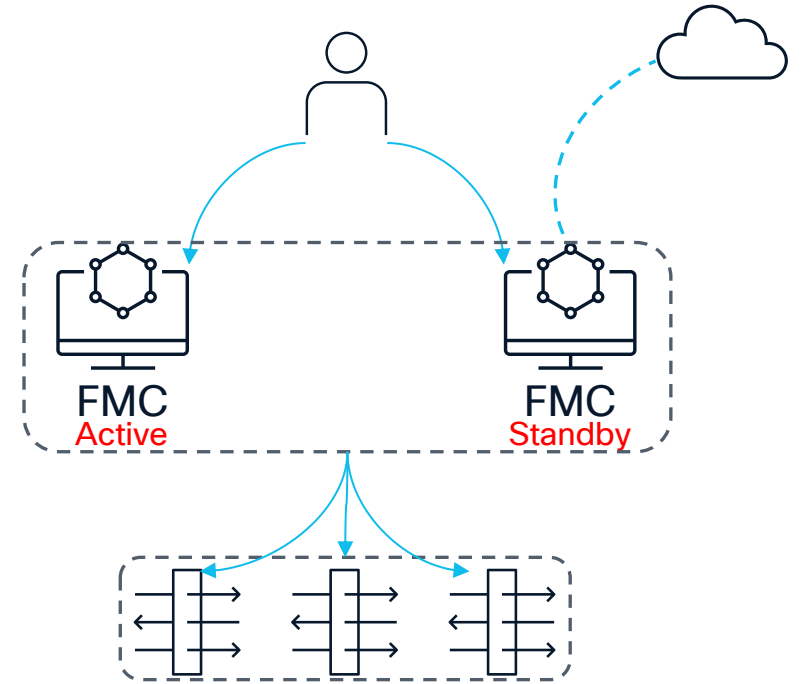
- Select target version next to Threat Defense
- Select devices from Device Selection pane

Select Devices for Upgrade

Copy Packages and Run Readiness

Start Upgrade

Next Steps



# FTD Upgrade Flow

Image Download



Launch Upgrade Wizard



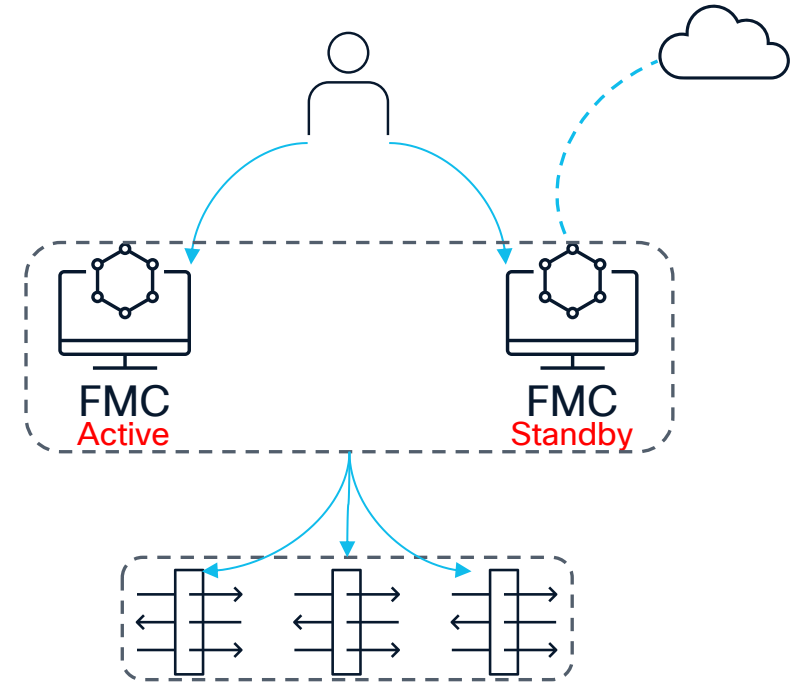
Select Devices for Upgrade

- Use device links to toggle device details
- Some devices may be ineligible for upgrades

Copy Packages and Run Readiness

Start Upgrade

Next Steps



# FTD Upgrade Flow

Image Download



Launch Upgrade Wizard



Select Devices for Upgrade

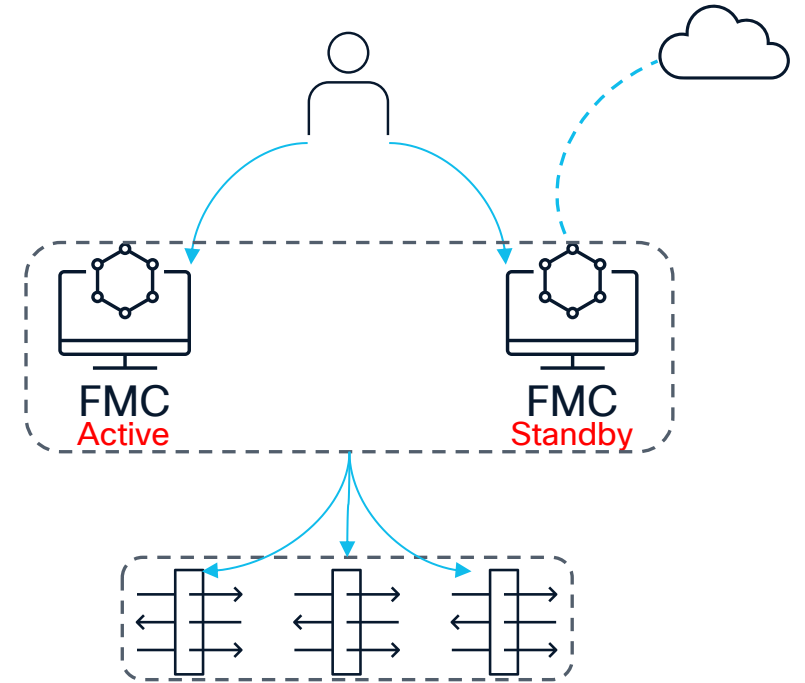


Copy Packages and Run Readiness

- Upgrade packages must be present on the device
- Passing readiness checks reduces the chance of upgrade failure
- Contact TAC if the readiness check exposes any issues

Start Upgrade

Next Steps



# FTD Upgrade Flow

Image Download



Launch Upgrade Wizard



Select Devices for Upgrade



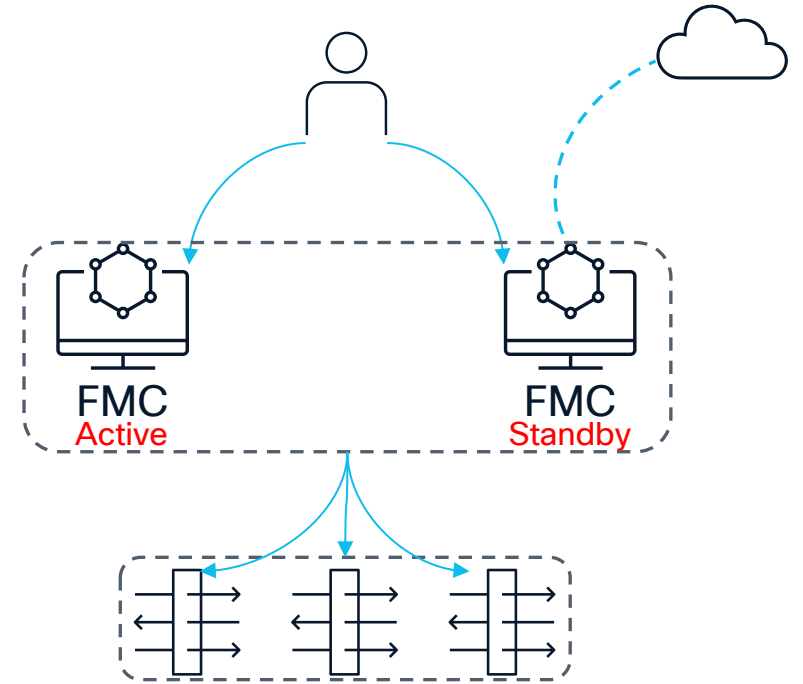
Copy Packages and Run Readiness



Start Upgrade

- Wizard shows overall upgrade process
- For high availability devices, the standby unit occurs first and then the active unit is upgrade. A failover does occur.

Next Steps



# FTD Upgrade Flow

Image Download



Launch Upgrade Wizard



Select Devices for Upgrade



Copy Packages and Run Readiness

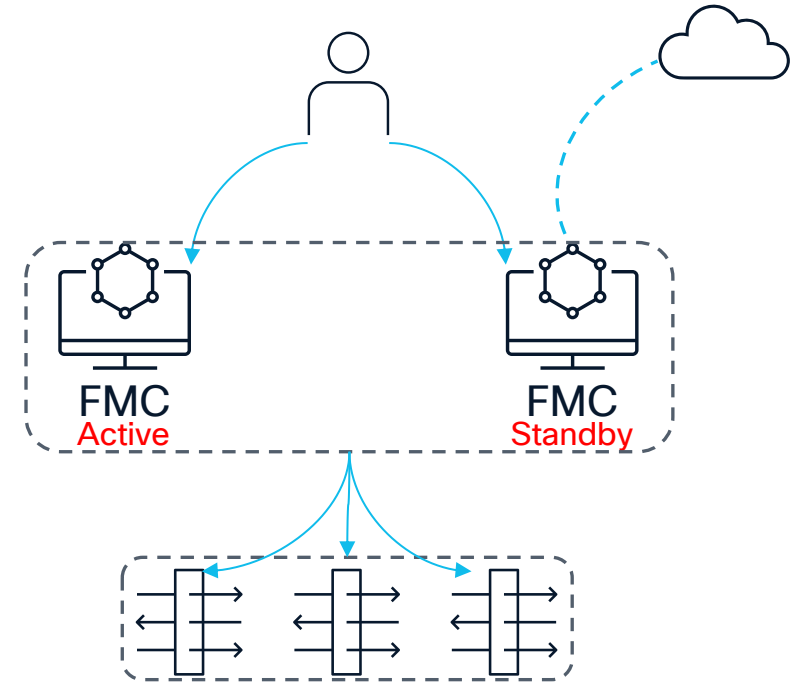


Start Upgrade



Next Steps

- Verify success
- For high availability devices, ensure device roles are correct
- Update intrusion rules, VDB, and deploy post-upgrade



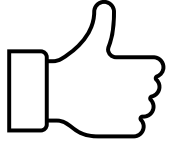
# Upgrade Steps – How to

**Demo**



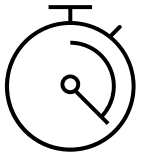
**Where We Are Going...**

# Future of Firewall Upgrades



Simple

Less than 10 clicks from anywhere in the UI to a fully upgraded environment. Including running a backup, executing the upgrade and final deployment.



Swift

Less than 1 hour to upgrade entire environment, from wanting to execute the upgrade to being able to arriving at the UI of new release and completing tasks.



Error-free

Users will no encounter failures during the upgrade process, including back up and deployment

# Upgrade Workflow Layout – Step Navigation

The screenshot shows the 'Threat Defense Upgrade' page in the Cisco Firewall Management Center. The page title is 'Threat Defense Upgrade' and the breadcrumb is 'Devices / Upgrade / Threat Defense Upgrade'. The user is logged in as 'admin'. The page features a progress bar with four steps: 1. Select Devices, 2. Prepare for Upgrade, 3. Start Upgrade, and 4. Monitor Upgrade. The current step is 'Prepare for Upgrade', which is highlighted in blue. A blue callout bubble labeled 'Upgrade Step' points to this step. Below the progress bar, there are tabs for 'Check for Compatibility and Readiness (1 + 1)', 'In Progress (1 + 1)', and 'Ready to Upgrade (0)'. The 'In Progress' tab is selected. A search bar is present to the right of these tabs. Below the tabs is a table with columns: Device, Version, Model, and Details. The table contains one main entry for 'auto\_bwasniak\_ftd' with version 7.4.1, and a sub-entry for 'HA2025 High Availability' with two members: 'auto\_bwasniak\_ftd2 (Primary)' and 'auto\_bwasniak\_ftd3 (Secondary - Active)'. A blue callout bubble labeled 'Filter Tabs' points to the tabs. Another blue callout bubble labeled 'Selected Devices' points to the 'Device' column. A third blue callout bubble labeled 'Device Details' points to the 'Details' column. At the bottom of the page, there are 'Reset', 'Previous', and 'Next' buttons. A status message at the bottom left says '1 device and 1 cluster/HA pair are running readiness checks.'

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Search Deploy 1

## Threat Defense Upgrade

1 Select Devices — 2 Prepare for Upgrade — 3 Start Upgrade — 4 Monitor Upgrade

Upgrade to: 7.7.0-89 In Progress (1 device and 1 cluster/HA pair) Unattended Mode

Check for Compatibility and Readiness (1 + 1) In Progress (1 + 1) Ready to Upgrade (0) Search Advanced Settings

Device	Version	Model	Details
auto_bwasniak_ftd	7.4.1	Firewall Threat Defense for VMware	Not ready for upgrade. Compatibility check passed. Readiness check in progress.
HA2025 High Availability			
1 auto_bwasniak_ftd2 (Primary)	7.4.1	Firewall Threat Defense for VMware	Not ready for upgrade. Compatibility check passed. Readiness check in progress. High availability status: Standby.
2 auto_bwasniak_ftd3 (Secondary - Active)	7.4.1	Firewall Threat Defense for VMware	Not ready for upgrade. Compatibility check passed. Readiness check in progress. High availability status: Active.

1 device and 1 cluster/HA pair are running readiness checks.

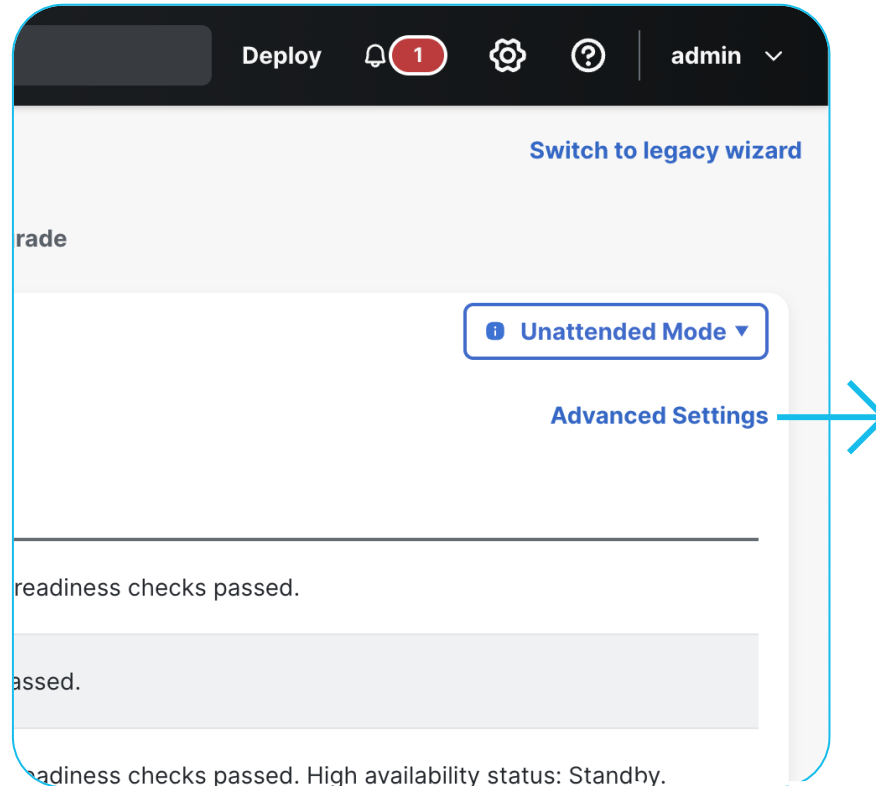
Reset Previous Next

# Upgrade Workflows - Advanced Settings

Click on 'Advanced Settings' in the towards the upper right to open Advanced Settings on the right side (like a drawer).

Clicking on an option will change the setting immediately.

To close the "drawer", click away from it.



## Advanced Settings

### Compatibility and Readiness Checks

- Require passing compatibility and readiness checks.

### Upgrade Failure

- Automatically cancel on upgrade failure and roll back to the previous version.

### Enable Revert ⚠️

- Enable revert after successful upgrade. ⓘ

### Upgrade Snort ⚠️

- Convert eligible devices from Snort 2 to Snort 3. ⓘ

# Upgrading FTDs – Monitor Upgrade

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Search Deploy 1 admin

## Threat Defense Upgrade

Switch to legacy wizard

1 Select Devices — 2 Prepare for Upgrade — 3 Start Upgrade — 4 Monitor Upgrade

**i** Upgrade of selected devices started 2025-03-24 18:10:33 EDT.  
Use the [Message Center](#) to view overall upgrade status. This page (until you clear it) and [Device Management](#) have detailed upgrade status. [Clear Upgrade Information](#)

Upgrade to: **7.7.0-89**

[Upgrade Initiated \(1 + 1\)](#) [In Progress \(1 + 1\)](#)

Device	Version	Model	Status
auto_bwasniak_ftd	7.4.1	Firewall Threat Defense for VMware	In progress <div style="width: 14%;"></div> 14% <a href="#">Detailed Status</a> <small>Preparing to upgrade...</small>
HA2025 High Availability			
1 auto_bwasniak_ftd3 (Secondary)	7.4.1	Firewall Threat Defense for VMware	In progress <div style="width: 14%;"></div> 14% <a href="#">Detailed Status</a> <small>Preparing to upgrade...</small>
2 auto_bwasniak_ftd2 (Primary – Active)	7.4.1	Firewall Threat Defense for VMware	Pending <a href="#">Detailed Status</a> <small>Waiting to start...</small>

Upgrade initiated for 1 + 1 devices.

[Reset](#) [Previous](#)

**Monitor Device Upgrades from Single-pane**

# Best Practices

# What to keep in mind...

- Understand how the upgrade process works
- Always make sure to verify your upgrade path prior to kicking off an upgrade
- Effective planning and preparation is essential for a successful upgrade
- Upgrading your firewall not only enhances stability, but also improves performance enabling you to leverage the latest feature-set
- Always schedule a maintenance window

# Call to Action

- Don't allow fears to overshadow your motivation for the upgrade. Start planning for the upgrade now!
- Embrace the recommended best practices for the upgrade.

# Reference

- Secure Firewall Essentials  
<https://secure.cisco.com/secure-firewall/>
- Secure Firewall YouTube Channel  
<https://www.youtube.com/@CiscoNetSec/videos>
- Upgrade Threat Defense Guide  
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/upgrade/management-center/770/upgrade-management-center-77.html>
- Secure Firewall Management Center – New Features by Release  
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/roadmap/management-center-new-features-by-release.html>

# Complete your session evaluations



**Complete** a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



**Earn** 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



**Level up** and earn exclusive prizes!



**Complete your surveys** in the Cisco Live mobile app.

# Continue your education



**Visit** the Cisco Showcase for related demos



**Book** your one-on-one Meet the Engineer meeting



**Attend** the interactive education with DevNet, Capture the Flag, and Walk-in Labs



**Visit** the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)

**Contact me at: Webex room**

**Thank you**

**CISCO** Live !

