# Upgrade FTD HA via CLI Managed by FMC

## Contents

## Introduction

This document describes a detailed procedure to upgrade Cisco Firepower Threat Defense (FTD) devices via the Command Line Interface (CLI).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Management Center v7.2.8

- Cisco Firepower Threat Defense for VMWare v7.2.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

Specific requirements for this document include:

- Cisco Secure Firewall Threat Defense running version 7.2 or higher
- Cisco Secure Firewall Management Center running version 7.2 or higher

# Configure

Upgrading a pair of FTD devices via CLI requires the upgrade package file to be present on the device. It is essential to have no pending deployments as a prerequisite for a successful upgrade via CLI.

# Preparing for Upgrade

**Warning**: Check the upgrade order, Standby / Active to avoid any traffic outages.

1. Begin with the device configured as Standby.

2. Access the CLI in expert mode by entering **expert** followed by **sudo su** in the clish mode. Confirm the device password to elevate privileges and enter expert mode.

```
Copyright 2004-2022, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 1104)
Cisco Firepower Threat Defense for VMware v7.2.2 (build 54)

> expert
admin@firepower:~$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
root@firepower:/home/admin#
root@firepower:/home/admin# cd
root@firepower:~#
root@firepower:~#
```

# Check Failover Status

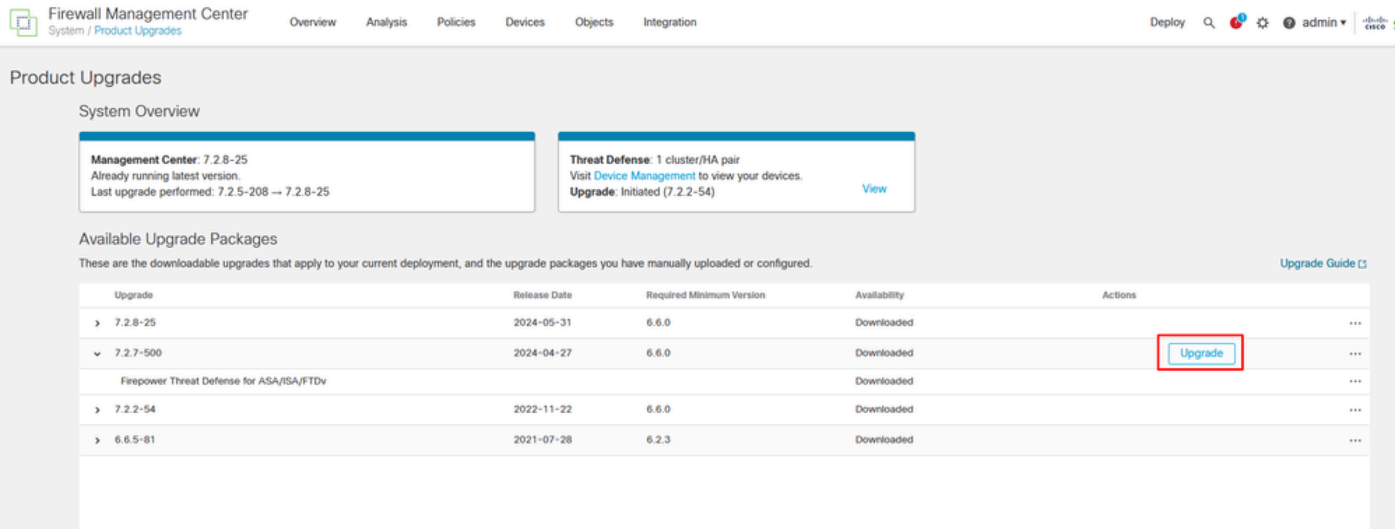
Verify the failover status to ensure that the steps are applied to the Secondary FTD, which can be displayed as Secondary and Standby Ready.

```
firepower#
firepower# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None

====Configuration State===
        Sync Done - STANDBY
====Communication State===
        Mac set

firepower#
firepower#
```

## Upload the Upgrade Package

Upload the upgrade package to both devices through the FMC by navigating to **Settings** > **Updates** > **Product Updates** > **Upload local software update package**. Choose the previously downloaded package from software.cisco.com and select **Upload**.

Once you have uploaded Firepower package on the FMC, continue with **Upgrade button**.



Product Upgrades

System Overview

**Management Center**: 7.2.8-25
Already running latest version.
Last upgrade performed: 7.2.5-208 → 7.2.8-25

**Threat Defense**: 1 cluster/HA pair
Visit Device Management to view your devices.
**Upgrade**: Initiated (7.2.2-54) View

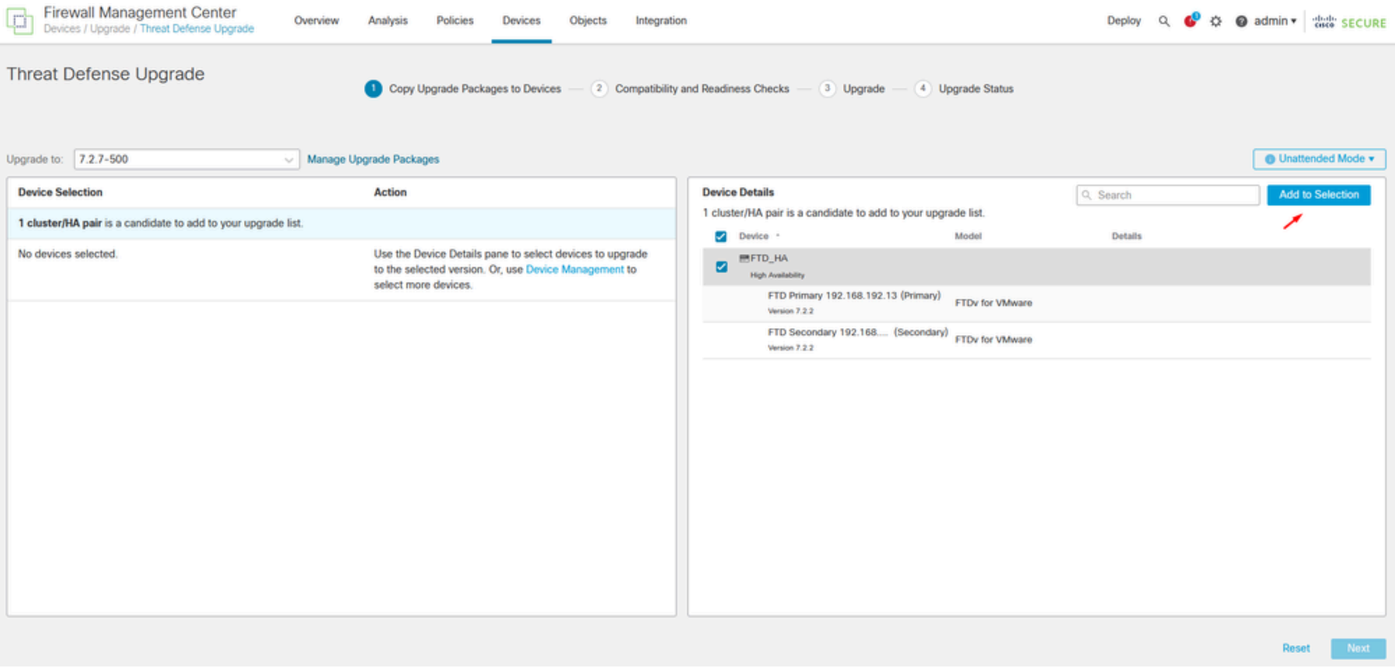
Available Upgrade Packages

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 |
|---|---|---|---|---|
| › 7.2.8-25 | 2024-05-31 | 6.6.0 | Downloaded | ··· |
| ⌄ 7.2.7-500 | 2024-04-27 | 6.6.0 | Downloaded | Upgrade ··· |
| Firepower Threat Defense for ASA/ISA/FTDv | | | Downloaded | ··· |
| › 7.2.2-54 | 2022-11-22 | 6.6.0 | Downloaded | ··· |
| › 6.6.5-81 | 2021-07-28 | 6.2.3 | Downloaded | ··· |

*Upgrade Button*

On the upgrade wizard you need to select the **FTD HA** devices, then select the devices, and click **Add to Selection**.


Firewall Management Center
Devices / Upgrade / Threat Defense Upgrade
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE

Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Manage Upgrade Packages Unattended Mode ▾

| Device Selection | Action |
|---|---|
| **1 cluster/HA pair** is a candidate to add to your upgrade list. | |
| No devices selected. | Use the Device Details pane to select devices to upgrade to the selected version. Or, use Device Management to select more devices. |

Device Details

Search Add to Selection

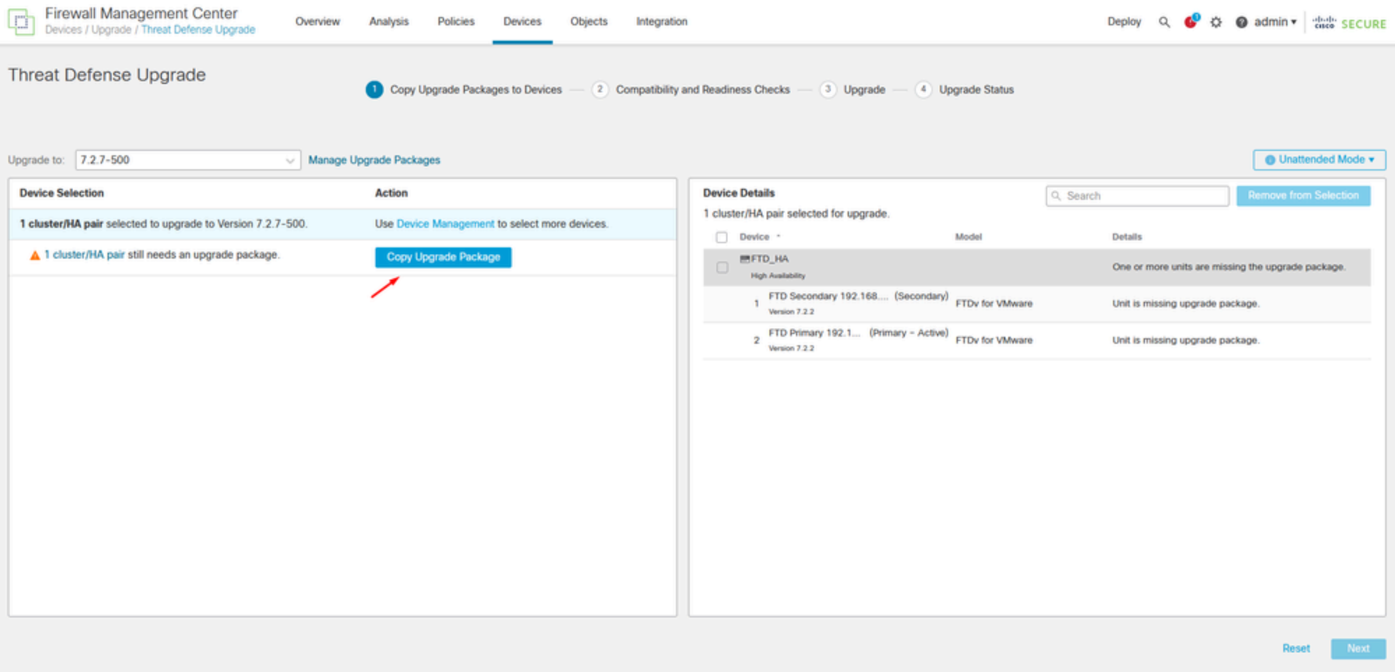
1 cluster/HA pair is a candidate to add to your upgrade list.

| ☑ Device | Model | Details |
|---|---|---|
| ☑ FTD_HA<br>High Availability | | |
| FTD Primary 192.168.192.13 (Primary)<br>Version 7.2.2 | FTDv for VMware | |
| FTD Secondary 192.168.... (Secondary)<br>Version 7.2.2 | FTDv for VMware | |

Reset Next

*Add to Selection*

Then, you can copy the upgrade Package on the devices, a message appears to continue Upgrade Packages.



Threat Defense Upgrade

Upgrade to: 7.2.7-500

| Device Selection | Action |
|---|---|
| **1 cluster/HA pair** selected to upgrade to Version 7.2.7-500. | Use Device Management to select more devices. |
| ⚠ 1 cluster/HA pair still needs an upgrade package. | Copy Upgrade Package |

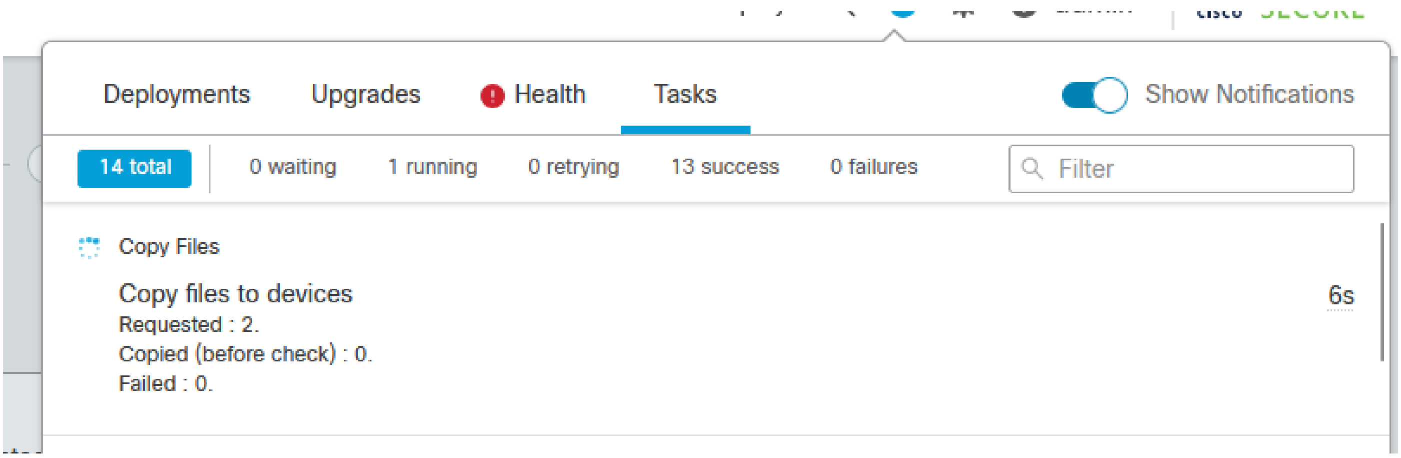
**Device Details**

1 cluster/HA pair selected for upgrade.

| | Device | Model | Details |
|---|---|---|---|
| □ | FTD_HA<br>High Availability | | One or more units are missing the upgrade package. |
| 1 | FTD Secondary 192.168.... (Secondary)<br>Version 7.2.2 | FTDv for VMware | Unit is missing upgrade package. |
| 2 | FTD Primary 192.1... (Primary - Active)<br>Version 7.2.2 | FTDv for VMware | Unit is missing upgrade package. |

*Copy Upgrade Package Button*

On the Notification task, you can find the job copying the files to device When the task is finished, it is completed and successful.



Copy Files

Copy files to devices 6s

Requested : 2.
Copied (before check) : 0.
Failed : 0.

*Task Copying Files to Devices*

You can verify the package is uploaded to the devices on this path:

```
root@firepower:/ngfw/var/sf/updates#
root@firepower:/ngfw/var/sf/updates# ls -l
total 2181772
-rw-r--r-- 1 root root 1110405120 Jul 18 01:08 Cisco_FTD_Upgrade-7.2.2-54.sh.REL.tar
-rw-r--r-- 1 root root        815 Jul 18 01:23 Cisco_FTD_Upgrade-7.2.2-54.sh.REL.tar.METADATA
-rw-r--r-- 1 root root 1123706880 Jul 18 02:36 Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
-rw-r--r-- 1 root root        854 Jul 18 02:37 Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar.METADATA
root@firepower:/ngfw/var/sf/updates#
```

## Readiness Check

Execute the readiness check from the CLI on the secondary device using the command:

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach --readiness-check /ngfw/var/sf/updates/
```

Here is an example:

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach --readiness-check /ngfw/var/sf/updates/
ARGV[0] = --detach
ARGV[1] = --readiness-check
ARGV[2] = /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
bundle_filepath: /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
[Readiness-Info]filename : /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar  at /usr/local/sf/lib
This was not run through the SF::System APIs at /usr/local/sf/lib/perl/5.24.4/SF/System/Wrappers.pm lin
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_FTD_Upgrade_Readiness-7.2.7-500.
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm l
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_FTD_Upgrade_Readiness-7.2.7-500.sh at /usr/local/
root@firepower:/ngfw/var/sf/updates#
```

Monitor the readiness check process at this path:

**root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness**

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness# cat upgrade_readiness_status
TIMESTAMP:Thu Jul 18 02:43:05 UTC 2024 PERCENT: 0%  MESSAGE:Running script 000_start/000_00_run_cli_kic
TIMESTAMP:Thu Jul 18 02:43:05 UTC 2024 PERCENT: 5%  MESSAGE:Running script 000_start/000_check_platform
TIMESTAMP:Thu Jul 18 02:43:06 UTC 2024 PERCENT:10%  MESSAGE:Running script 000_start/100_start_messages
TIMESTAMP:Thu Jul 18 02:43:06 UTC 2024 PERCENT:14%  MESSAGE:Running script 000_start/101_run_pruning.pl
TIMESTAMP:Thu Jul 18 02:43:41 UTC 2024 PERCENT:19%  MESSAGE:Running script 000_start/105_check_model_nu
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:24%  MESSAGE:Running script 000_start/106_check_HA_state
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:29%  MESSAGE:Running script 000_start/107_version_check.
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:33%  MESSAGE:Running script 000_start/108_clean_user_sta
TIMESTAMP:Thu Jul 18 02:43:43 UTC 2024 PERCENT:38%  MESSAGE:Running script 000_start/110_DB_integrity_c
TIMESTAMP:Thu Jul 18 02:43:47 UTC 2024 PERCENT:43%  MESSAGE:Running script 000_start/113_EO_integrity_c
TIMESTAMP:Thu Jul 18 02:43:50 UTC 2024 PERCENT:48%  MESSAGE:Running script 000_start/250_check_system_f
TIMESTAMP:Thu Jul 18 02:43:50 UTC 2024 PERCENT:52%  MESSAGE:Running script 000_start/410_check_disk_spa
TIMESTAMP:Thu Jul 18 02:43:55 UTC 2024 PERCENT:57%  MESSAGE:Running script 200_pre/001_check_reg.pl...
TIMESTAMP:Thu Jul 18 02:43:55 UTC 2024 PERCENT:62%  MESSAGE:Running script 200_pre/002_check_mounts.sh.
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:67%  MESSAGE:Running script 200_pre/004_check_deploy_pac
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:71%  MESSAGE:Running script 200_pre/005_check_manager.pl
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:76%  MESSAGE:Running script 200_pre/006_check_snort.sh..
TIMESTAMP:Thu Jul 18 02:43:57 UTC 2024 PERCENT:81%  MESSAGE:Running script 200_pre/007_check_sru_instal
TIMESTAMP:Thu Jul 18 02:43:57 UTC 2024 PERCENT:86%  MESSAGE:Running script 200_pre/009_check_snort_prep
TIMESTAMP:Thu Jul 18 02:43:58 UTC 2024 PERCENT:90%  MESSAGE:Running script 200_pre/011_check_self.sh...
TIMESTAMP:Thu Jul 18 02:43:58 UTC 2024 PERCENT:95%  MESSAGE:Running script 200_pre/015_verify_rpm.sh...
TIMESTAMP:Thu Jul 18 02:44:00 UTC 2024 PERCENT:100%  MESSAGE:Readiness Check completed successfully.
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness#
```

If readiness check fails, contact Cisco TAC.

# Upgrade Installation

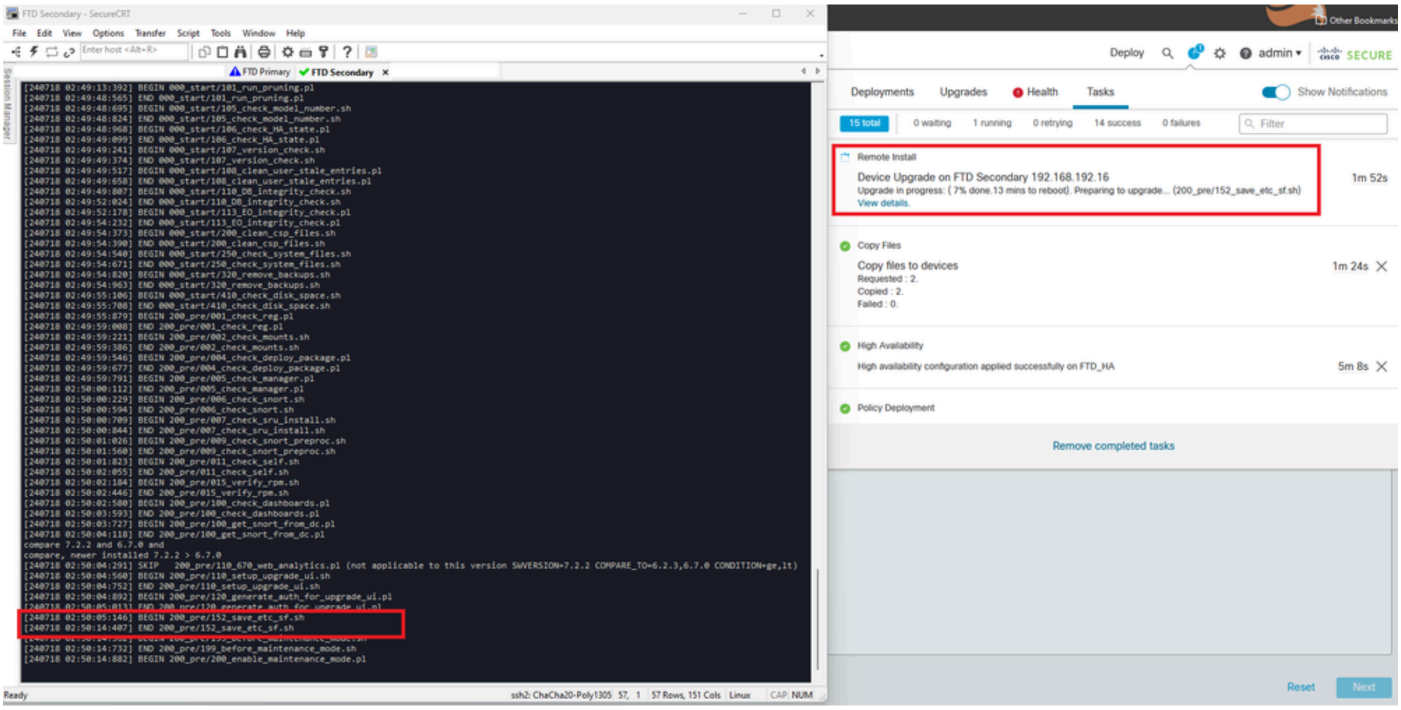
Proceed with the upgrade installation on the Secondary FTD. Navigate to the folder containing the upgrade file and execute the installation command:

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach <FTD_Upgrade_Package.sh.REL.tar>
```

Once the upgrade has been executed, there is going to be an output like the next example:

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
ARGV[0] = Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
bundle_filepath: Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
updated absolute bundle_filepath: /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_FTD_Upgrade-7.2.7-500.sh at /usr
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm l
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_FTD_Upgrade-7.2.7-500.sh at /usr/local/sf/lib/perl
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value $in_container in string eq at /usr/local/sf/lib/perl/5.24.4/SF/Update/Status
Verifying archive integrity... All good.
Uncompressing Cisco FTD Upgrade / Sat Apr 27 04:09:29 UTC 2024.........................................
Entering is_fmc_managed
Device is FMC Managed
[240718 02:48:13:868] Found original ftd upgrade file /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.RE
[240718 02:48:16:990] MAIN_UPGRADE_SCRIPT_START
[240718 02:48:17:006] #####################################
[240718 02:48:17:007] # UPGRADE  STARTING
[240718 02:48:17:008] #####################################
compare 7.2.2 and 6.2.3 and
compare, newer installed 7.2.2 > 6.2.3
Entering create_upgrade_status_links...
Create upgrade_status.json and upgrade_status.log link in /ngfw/var/sf/sync/updates_status_logs
Running [ln -f /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json /ngfw/var/sf/sync/updates_st
Link to JSON upgrade status file /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json created i
Running [ln -f /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/var/sf/sync/updates_sta
Link to log upgrade status file /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log created in
[240718 02:48:17:229] BEGIN 000_start/000_00_run_cli_kick_start.sh
[240718 02:48:18:421] END 000_start/000_00_run_cli_kick_start.sh
[240718 02:48:18:525] BEGIN 000_start/000_00_run_troubleshoot.sh
```

On the FMC, there is a task running the upgrade on the Secondary device:



FTD Secondary - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
FTD Primary
FTD Secondary
Session Manager

```
[240718 02:49:13:392] BEGIN 000_start/101_run_pruning.pl
[240718 02:49:48:565] END 000_start/101_run_pruning.pl
[240718 02:49:48:695] BEGIN 000_start/105_check_model_number.sh
[240718 02:49:48:824] END 000_start/105_check_model_number.sh
[240718 02:49:48:968] BEGIN 000_start/106_check_HA_state.pl
[240718 02:49:49:099] END 000_start/106_check_HA_state.pl
[240718 02:49:49:241] BEGIN 000_start/107_version_check.sh
[240718 02:49:49:374] END 000_start/107_version_check.sh
[240718 02:49:49:517] BEGIN 000_start/108_clean_user_stale_entries.pl
[240718 02:49:49:658] END 000_start/108_clean_user_stale_entries.pl
[240718 02:49:49:807] BEGIN 000_start/110_DB_integrity_check.sh
[240718 02:49:52:024] END 000_start/110_DB_integrity_check.sh
[240718 02:49:52:178] BEGIN 000_start/113_EO_integrity_check.pl
[240718 02:49:54:232] END 000_start/113_EO_integrity_check.pl
[240718 02:49:54:373] BEGIN 000_start/200_clean_csp_files.sh
[240718 02:49:54:390] END 000_start/200_clean_csp_files.sh
[240718 02:49:54:540] BEGIN 000_start/250_check_system_files.sh
[240718 02:49:54:671] END 000_start/250_check_system_files.sh
[240718 02:49:54:820] BEGIN 000_start/320_remove_backups.sh
[240718 02:49:54:963] END 000_start/320_remove_backups.sh
[240718 02:49:55:106] BEGIN 000_start/410_check_disk_space.sh
[240718 02:49:55:708] END 000_start/410_check_disk_space.sh
[240718 02:49:55:879] BEGIN 200_pre/001_check_reg.pl
[240718 02:49:59:008] END 200_pre/001_check_reg.pl
[240718 02:49:59:221] BEGIN 200_pre/002_check_mounts.sh
[240718 02:49:59:386] END 200_pre/002_check_mounts.sh
[240718 02:49:59:546] BEGIN 200_pre/004_check_deploy_package.pl
[240718 02:49:59:677] END 200_pre/004_check_deploy_package.pl
[240718 02:49:59:791] BEGIN 200_pre/005_check_manager.pl
[240718 02:50:00:112] END 200_pre/005_check_manager.pl
[240718 02:50:00:229] BEGIN 200_pre/006_check_snort.sh
[240718 02:50:00:594] END 200_pre/006_check_snort.sh
[240718 02:50:00:709] BEGIN 200_pre/007_check_sru_install.sh
[240718 02:50:00:844] END 200_pre/007_check_sru_install.sh
[240718 02:50:01:026] BEGIN 200_pre/009_check_snort_preproc.sh
[240718 02:50:01:560] END 200_pre/009_check_snort_preproc.sh
[240718 02:50:01:823] BEGIN 200_pre/011_check_self.sh
[240718 02:50:02:055] END 200_pre/011_check_self.sh
[240718 02:50:02:184] BEGIN 200_pre/015_verify_rpm.sh
[240718 02:50:02:446] END 200_pre/015_verify_rpm.sh
[240718 02:50:02:580] BEGIN 200_pre/100_check_dashboards.pl
[240718 02:50:03:593] END 200_pre/100_check_dashboards.pl
[240718 02:50:03:727] BEGIN 200_pre/100_get_snort_from_dc.pl
[240718 02:50:04:118] END 200_pre/100_get_snort_from_dc.pl
compare 7.2.2 and 6.7.0 and
compare, newer installed 7.2.2 > 6.7.0
[240718 02:50:04:291] SKIP   200_pre/110_670_web_analytics.pl (not applicable to this version SWVERSION=7.2.2 COMPARE_TO=6.2.3,6.7.0 CONDITION=ge,lt)
[240718 02:50:04:560] BEGIN 200_pre/110_setup_upgrade_ui.sh
[240718 02:50:04:752] END 200_pre/110_setup_upgrade_ui.sh
[240718 02:50:04:892] BEGIN 200_pre/120_generate_auth_for_upgrade_ui.pl
[240718 02:50:05:013] END 200_pre/120_generate_auth_for_upgrade_ui.pl
[240718 02:50:05:146] BEGIN 200_pre/152_save_etc_sf.sh
[240718 02:50:14:407] END 200_pre/152_save_etc_sf.sh
[240718 02:50:14:[illegible]] BEGIN 200_pre/199_before_maintenance_mode.sh
[240718 02:50:14:732] END 200_pre/199_before_maintenance_mode.sh
[240718 02:50:14:882] BEGIN 200_pre/200_enable_maintenance_mode.pl
```

Remote Install

Device Upgrade on FTD Secondary 192.168.192.16
Upgrade in progress: ( 7% done.13 mins to reboot). Preparing to upgrade... (200_pre/152_save_etc_sf.sh)
View details.
1m 52s

Copy Files

Copy files to devices
Requested : 2.
Copied : 2.
Failed : 0.
1m 24s

High Availability

High availability configuration applied successfully on FTD_HA
5m 8s

Policy Deployment

*Task Running on FMC*

Monitor the upgrade status using this path:

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-X.X.X# tail -f upgrade_status.log
```

Here is an example of the output:

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7# tail -f upgrade_status.log
TIMESTAMP:Thu Jul 18 02:50:25 UTC 2024 PERCENT: 7%  MESSAGE:Running script 200_pre/202_disable_syncd.sh
TIMESTAMP:Thu Jul 18 02:50:26 UTC 2024 PERCENT: 7%  MESSAGE:Running script 200_pre/400_restrict_rpc.sh.
TIMESTAMP:Thu Jul 18 02:50:26 UTC 2024 PERCENT: 7%  MESSAGE:Running script 200_pre/500_stop_system.sh..
TIMESTAMP:Thu Jul 18 02:50:53 UTC 2024 PERCENT:14%  MESSAGE:Running script 200_pre/501_recovery.sh... T
TIMESTAMP:Thu Jul 18 02:50:53 UTC 2024 PERCENT:14%  MESSAGE:Running script 200_pre/505_revert_prep.sh..
TIMESTAMP:Thu Jul 18 02:51:46 UTC 2024 PERCENT:14%  MESSAGE:Running script 200_pre/999_enable_sync.sh..
TIMESTAMP:Thu Jul 18 02:51:46 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/001_verify_bundle.sh.
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/002_set_auto_neg.pl..
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/060_fix_fstab.sh... T
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14%  MESSAGE:Running script 300_os/100_install_Fire_Linu
```

When the Upgrade on the Secondary device has finished, you see this message:

```
240718 13:40:58:872] Attempting to remove upgrade lock
[240718 13:40:58:873] Success, removed upgrade lock
Upgrade lock /ngfw/tmp/upgrade.lock removed successfully.
[240718 13:40:58:882]
[240718 13:40:58:883] ##################################################
[240718 13:40:58:885] # UPGRADE  COMPLETE  #
[240718 13:40:58:887] ##################################################
```

```
Entering create_upgrade_status_links...
Create upgrade_status.json and upgrade_status.log link in /ngfw/Volume/root/ngfw/var/sf/sync/updates_st
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json /ngfw/Volu
Link to JSON upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_stat
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/Volum
Link to log upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_statu
Process 10677 exited.I am going away.
RC: 0
Update package reports success: almost finished...
Scheduling a reboot to occur in 5 seconds...
Process 12153 exited.I am going away.
root@firepower:/ngfw/var/sf/updates#
Broadcast message from root@firepower (Thu Jul 18 13:41:05 2024):

The system is going down for reboot NOW!
```

After the upgrade from the Standby device is completed, the device is going to be rebooted. Once the devices comes up, check the failover status to ensure everything remains as initially configured.

On the Active FTD you can find:

```
firepower# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             13:24:46 UTC Jul 18 2024

====Configuration State===
        Sync Done
====Communication State===
        Mac set

firepower#
```

On Standby FTD, you find this:

```
firepower#
firepower# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Standby Ready  None
Other host -   Primary
               Active         None

====Configuration State===
        Sync Skipped - STANDBY
====Communication State===
        Mac set

firepower#
```

There is going to be a message showing that the versions are not the same.

```
firepower#
************WARNING****WARNING****WARNING********************************
   Mate version 9.18(4)201 is not identical with ours 9.18(2)200
************WARNING****WARNING****WARNING********************************
```

Perform the failover manually via CLI using the command **failover active** on Standby Device. Now the Standby device become Active.

**Warning**: At this point there is going a brief traffic interruption when failover happens.

```
firepower#
firepower# failover active

        Switching to Active
firepower#
```

```
firepower#
firepower# sh fail
firepower# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Active         None
Other host -   Primary
               Standby Ready  None

====Configuration State===
        Sync Skipped
====Communication State===
        Mac set

firepower#
```

Once the failover has been completed, you can proceed upgrading the other device. Use the same steps described at the beginning of the document for the device that was previously Active and now is Standby.

Now both devices are upgraded. You can see with the command **show version** on Lina side. For the Primary Device:

```
firepower#
firepower# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Standby Ready  None
Other host -   Secondary
               Active         None

====Configuration State===
        Sync Skipped - STANDBY
====Communication State===
        Mac set

firepower#
```

For the Secondary Device:

```
firepower#
firepower# sh failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
               Active         None
Other host -   Primary
               Standby Ready  Comm Failure             14:03:06 UTC Jul 18 2024

====Configuration State===
        Sync Skipped
====Communication State===
        Mac set
```

```
firepower#
```

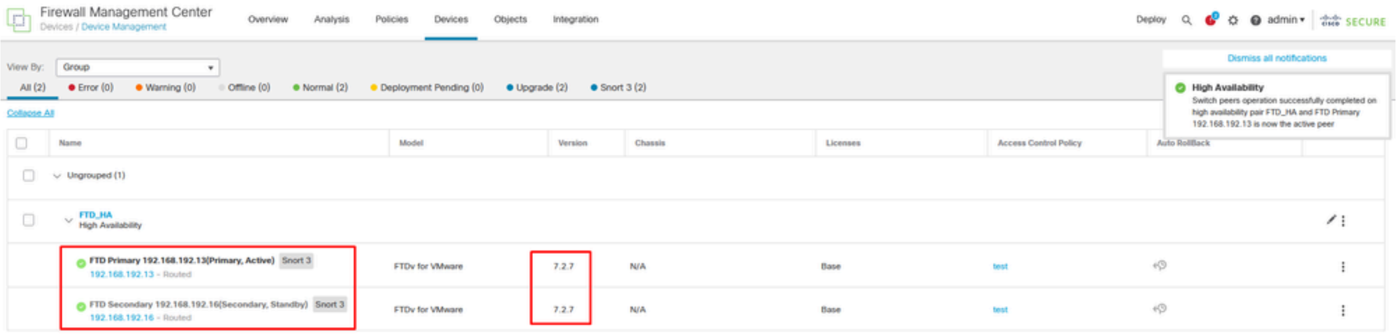
At this point, you can switch over the devices from FMC like it was at the beginning.

# Verify

After successfully upgrading both devices, verify the status within the FMC and on both FTDs using the command **show version**.

```
firepower# show version
-------------------[ firepower ]--------------------
Model                        : Cisco Firepower Threat Defense for VMware (75) Version 7.2.7 (Build 500)
UUID                         : 0edf9f22-78e6-11ea-8ed0-e0e5abf334e2
LSP version                  : lsp-rel-20240306-2015
VDB version                  : 353
----------------------------------------------------
```

On the FMC, you can see the version update and are ready to switch over as you had it at the beginning.



High Availability
Switch peers operation successfully completed on high availability pair FTD_HA and FTD Primary 192.168.192.13 is now the active peer

| Name | Model | Version | Chassis | Licenses | Access Control Policy | Auto RollBack |
|---|---|---|---|---|---|---|
| Ungrouped (1) | | | | | | |
| FTD_HA<br>High Availability | | | | | | |
| FTD Primary 192.168.192.13(Primary, Active) Snort 3<br>192.168.192.13 - Routed | FTDv for VMware | 7.2.7 | N/A | Base | test | |
| FTD Secondary 192.168.192.16(Secondary, Standby) Snort 3<br>192.168.192.16 - Routed | FTDv for VMware | 7.2.7 | N/A | Base | test | |

*Switched Peers from FMC*