

# Upgrade FTD HA Managed by FMC

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Overview](#)

### [Background Information](#)

### [Configure](#)

[Step 1. Upload Upgrade Package](#)

[Step 2. Check Readiness](#)

[Step 3. Upgrade FTD in High Availability](#)

[Step 4. Switch Active Peer \(Optional\)](#)

[Step 5. Final Deploy](#)

### [Validate](#)

---

## Introduction

This document describes the upgrade process for a Cisco Secure Firewall Threat Defense in High Availability managed by a Firewall Management Center.

## Prerequisites

### Requirements

Cisco recommends you have knowledge of these topics:

- High Availability (HA) concepts and configuration
- Secure Firewall Management Center (FMC) configuration
- Cisco Secure Firewall Threat Defense (FTD) configuration

### Components Used

The information in this document is based on:

- Virtual Firewall Management Center (FMC), version 7.2.4
- Virtual Cisco Firewall Threat Defense (FTD), version 7.0.1

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.

### Overview

The way the FMC works is to upgrade one peer at a time. First the Standby, then the Active, doing a failover

before the Active upgrade gets completed.

## Background Information

Upgrade package must be downloaded from [software.cisco.com](https://software.cisco.com) before the upgrade.

On CLI clish, run the **show high-availability config** command in the Active FTD to check the status of the High Availability.

```
> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: FAILOVER_LINK GigabitEthernet0/0 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1285 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(2)5, Mate 9.16(2)5
Serial Number: Ours 9AJJSEGJS2T, Mate 9AVLW3FSSK8
Last Failover at: 00:37:48 UTC Jul 20 2023
```

```
    This host: Secondary - Standby Ready
      Active time: 4585 (sec)
      slot 0: ASAv hw/sw rev (/9.16(2)5) status (Up Sys)
        Interface INSIDE (10.10.153.2): Normal (Monitored)
        Interface diagnostic (0.0.0.0): Normal (Waiting)
        Interface OUTSIDE (10.20.153.2): Normal (Monitored)
      slot 1: snort rev (1.0) status (up)
      slot 2: diskstatus rev (1.0) status (up)
```

```
    Other host: Primary - Active
      Active time: 60847 (sec)
      Interface INSIDE (10.10.153.1): Normal (Monitored)
      Interface diagnostic (0.0.0.0): Normal (Waiting)
      Interface OUTSIDE (10.20.153.1): Normal (Monitored)
      slot 1: snort rev (1.0) status (up)
      slot 2: diskstatus rev (1.0) status (up)
```

### Stateful Failover Logical Update Statistics

```
Link : FAILOVER_LINK GigabitEthernet0/0 (up)
Stateful Obj  xmit      xerr      rcv        rerr
General      9192        0        10774      0
sys cmd      9094        0        9092       0
...
Rule DB B-Sync  0          0          0          0
Rule DB P-Sync  0          0          204        0
Rule DB Delete  0          0          1          0
```

### Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	9	45336
Xmit Q:	0	11	11572

If no errors are visible, then proceed with upgrade.

## Configure

### Step 1. Upload Upgrade Package

- Upload the FTD upgrade package to the FMC using the graphical user interface (GUI). This has to be previously downloaded from the Cisco Software site based on the FTD model and desire version.



**Warning:** Ensure that the FMC version is higher or equal than the new FTD version to upgrade.

---

**System > Updates**

Configuration

Users

Domains

Updates

Licenses

Smart Licenses

Classic Licenses

Health

Monitor

Policy

Events

Exclude

Monitor Alerts

Monitoring

Audit

Syslog

Statistics

Tools

Backup/Restore

Scheduling

Import/Export

Data Purge

- Select **Upload Update**.

Firewall Management Center  
System / Updates / Product Updates



Overview Analysis Policies Devices Objects Integration Deploy Q 1 ⚙️ ? admin ▾ CISCO SECURE

Product Updates Rule Updates Geolocation Updates

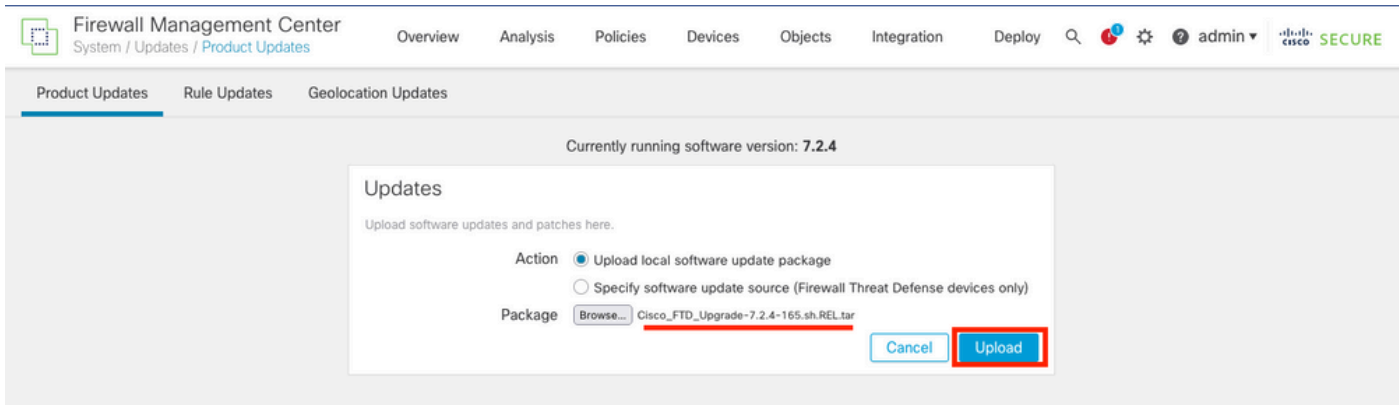
Download Updates Upload Update

Currently running software version: 7.2.4  
Currently installed VDB version: build 353 ( 2022-03-07 22:13:19 )

Available Updates Readiness History

Type	Version	Date	Reboot	
Cisco Secure FW Mgmt Center Upgrade	7.2.4-169	Wed May 10 12:48:58 UTC 2023	Yes	 

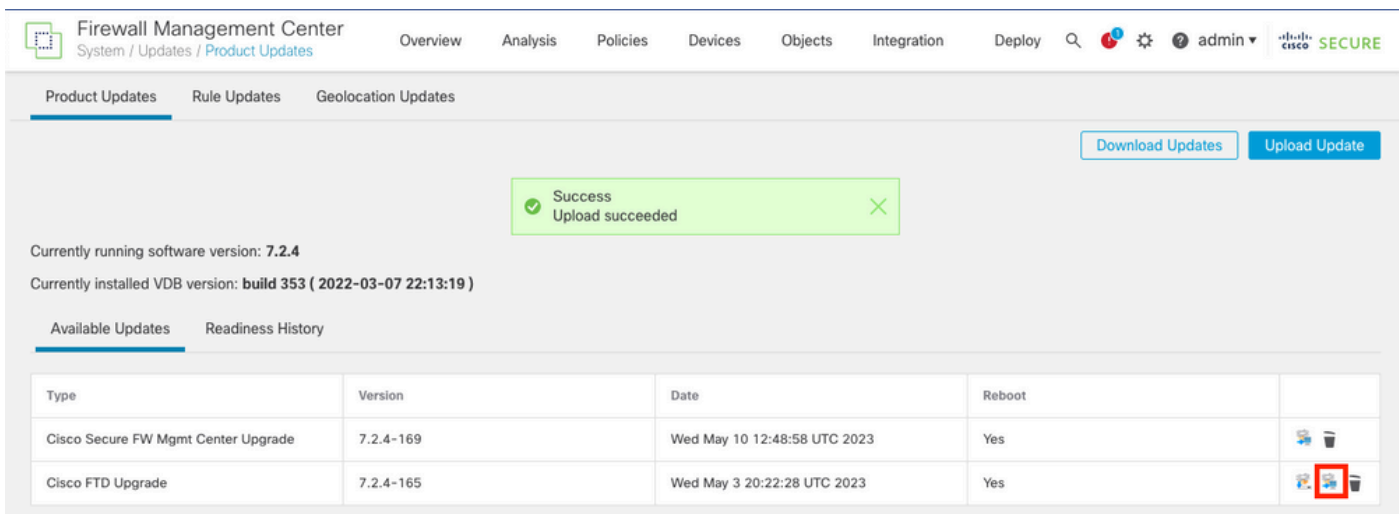
- Browse for the previously downloaded image, then select **Upload**.



## Step 2. Check Readiness

Readiness checks confirm if appliances are ready to proceed with upgrade.

- Select the **Install** option in the correct upgrade package.



Select the upgrade you prefer. In this case, the selection is for:

- Automatically cancel on upgrade failure and roll back to previous version.
- Enable revert after successful upgrade.
- Upgrade Snort 2 to Snort 3.
- Select the HA group of FTDs and click **Check Readiness**.

Product Updates   Rule Updates   Geolocation Updates

Currently running software version: **7.2.4**

**Selected Update**

Type	Cisco FTD Upgrade
Version	7.2.4-165
Date	Wed May 3 20:22:28 UTC 2023
Reboot	Yes

Automatically cancel on upgrade failure and roll back to the previous version (Applies to individual units in HA or Clusters)

Enable revert after successful upgrade

**Upgrade Snort 2 to Snort 3**

After the software upgrade, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom Intrusion or Network Analysis Policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. [Learn more](#)

By Group ▾

	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
<input checked="" type="checkbox"/> Ungrouped (1 total)						
<input checked="" type="checkbox"/> <b>FTD_HA</b> Cisco Firepower Threat Defense for VMware Cluster						
<input checked="" type="checkbox"/> <b>FTD_A (active)</b> 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	✔ Compatibility check passed. Proceed with			N/A	10 min	⬇
<input checked="" type="checkbox"/> <b>FTD_B</b> 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	✔ Compatibility check passed. Proceed with			N/A	10 min	⬇

The progress can be checked in the message center **Messages > Tasks**.

Policies   Devices   Objects   Integration   Deploy   🔍   🔔   ⚙️   ? admin ▾   CISCO SECURE

Deployments   Upgrades   ! Health   **Tasks**    Show Notifications

20+ total   0 waiting   0 running   0 retrying   20+ success   0 failures   🔍 Filter

✔ Remote Readiness Check

Checking Cisco FTD Upgrade 7.2.4-165 on [ FTD\_HA ] 2m 11s ✕

10.4.11.86: Success. OK to upgrade to 7.2.4-165 version.

10.4.11.87: Success. OK to upgrade to 7.2.4-165 version.

When the readiness check completes in both FTD and result is Success, the upgrade can be done.

By Group ▾

	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
<input type="checkbox"/> Ungrouped (1 total)						
<input type="checkbox"/> <b>FTD_HA</b> Cisco Firepower Threat Defense for VMware Cluster						
<input type="checkbox"/> <b>FTD_A (active)</b> 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	✔ Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min	⬇
<input type="checkbox"/> <b>FTD_B</b> 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	✔ Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min	⬇

### Step 3. Upgrade FTD in High Availability

- Select the **HA Pair** and click **Install**.

Firewall Management Center  
System / Updates / Upload Update

Overview Analysis Policies Devices Objects Integration Deploy

Product Updates Rule Updates Geolocation Updates

**Warnings**

- Version 7.2.0 onwards, the Intelligent Application Bypass (IAB) setting is deprecated for ... [See More](#)
- Version 7.2.0 onwards, the port\_scan inspector is deprecated for Snort 3 ... [See More](#)

Currently running software version: **7.2.4**

**Selected Update**

Type	Cisco FTD Upgrade
Version	7.2.4-165
Date	Wed May 3 20:22:28 UTC 2023
Reboot	Yes

Automatically cancel on upgrade failure and roll back to the previous version (Applies to individual units in HA or Clusters)


Enable revert after successful upgrade

Upgrade Snort 2 to Snort 3  
After the software upgrade, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom Intrusion or Network Analysis Policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. [Learn more](#)

By Group ▾

<input checked="" type="checkbox"/>	Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Snort 3	Estimated Upgrade Time	
<input checked="" type="checkbox"/>	FTD_HA Cisco Firepower Threat Defense for VMware Cluster						
<input checked="" type="checkbox"/>	FTD_A (active) 10.4.11.87 - Cisco Firepower Threat Defense for VMware v7.0.1	Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min	↓
<input checked="" type="checkbox"/>	FTD_B 10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1	Compatibility check passed. Proceed with	Success	2023-07-20 14:33:00	N/A	10 min	↓

Warning to continue with upgrade, the system reboots to complete upgrade. Select **OK**.


 **10.88.243.115:43092**

Update installation will reboot the system(s). Are you sure you want to continue?

The progress can be checked in the message center **Messages > Tasks**.

Deployments Upgrades **Health** **Tasks**  Show Notifications

20+ total | 0 waiting | 1 running | 0 retrying | 20+ success | 0 failures

 Remote Install

**Apply Cisco FTD Upgrade 7.2.4-165 to FTD\_HA** 8m 57s

FTD\_B : Upgrade in progress: (14% done.12 mins to reboot). Updating Operating System...  
(300\_os/100\_install\_Fire\_Linux\_OS\_aquila.sh (in background: 200\_pre/600\_ftd\_onbox\_data\_export.sh))

firepower: View details.

If you click on **firepower: View details**, the progress is shown in a graphical way and the logs of status.log.



# Upgrade in Progress



## FTD\_B

10.4.11.86

Cisco Firepower Threat Defense for VMware (Version: 7.0.1-84)

**Version:** 7.2.4-165 | **Size:** 1.04 GB | **Build Date:** May 3, 2023 8:22 PM UTC

**Initiated By:** admin | **Initiated At:** Jul 20, 2023 2:58 PM EDT



14% Completed (12 minutes left)

### Upgrade In Progress...

Updating Operating System... (300\_os/100\_install\_Fire\_Linux\_OS\_aquila.sh (in background: 200\_pre/600\_ftd\_onbox\_data\_export.sh))

- Upgrade will automatically cancel on failure and roll back to the previous version.

### Log Details



```
Thu Jul 20 18:56:51 UTC 2023 7% Running script 200_pre/202_disable_syncd.sh... 13 mins
Thu Jul 20 18:56:51 UTC 2023 7% Running script 200_pre/400_restrict_rpc.sh... 13 mins
Thu Jul 20 18:56:51 UTC 2023 7% Running script 200_pre/500_stop_system.sh... 13 mins
Thu Jul 20 18:57:17 UTC 2023 7% Running script 200_pre/501_recovery.sh... 13 mins rema
Thu Jul 20 18:57:18 UTC 2023 14% Running script 200_pre/505_revert_prep.sh... 12 mins
Thu Jul 20 18:58:05 UTC 2023 14% Running script 200_pre/999_enable_sync.sh... 12 mins
Thu Jul 20 18:58:05 UTC 2023 14% Running script 300_os/001_verify_bundle.sh... 12 mins
Thu Jul 20 18:58:06 UTC 2023 14% Running script 300_os/002_set_auto_neg.pl... 12 mins
Thu Jul 20 18:58:06 UTC 2023 14% Running script 300_os/060_fix_fstab.sh... 12 mins re
Thu Jul 20 18:58:06 UTC 2023 14% Running script 300_os/100_install_Fire_Linux_OS_aqui
```

Cancel Upgrade

Close

---

**Note:** Upgrade takes around 20 min per FTD.

---

On CLI, progress can be checked in upgrade folder `/ngfw/var/log/sf`; move to **expert mode** and enter **root access**.

```
> expert
admin@firepower:~$ sudo su
Password:
root@firepower:/home/admin# cd /ngfw/var/log/sf

root@firepower:/ngfw/var/log/sf# ls
Cisco_FTD_Upgrade-7.2.4

root@firepower:/ngfw/var/log/sf# cd Cisco_FTD_Upgrade-7.2.4

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.4# ls
000_start AQ_UUID DBCheck.log finished_kickstart.flag flags.conf main_upgrade_script.log status.1

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.4# tail -f status.log
state:running
```

```
ui:Upgrade has begun.
ui: Upgrade in progress: ( 0% done.14 mins to reboot). Checking device readiness... (000_start/000_00_r
...
ui: Upgrade in progress: (64% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com
ui: Upgrade complete
ui: The system will now reboot.
ui: System will now reboot.
```

Broadcast message from root@firepower (Thu Jul 20 19:05:20 2023):

System will reboot in 5 seconds due to system upgrade.

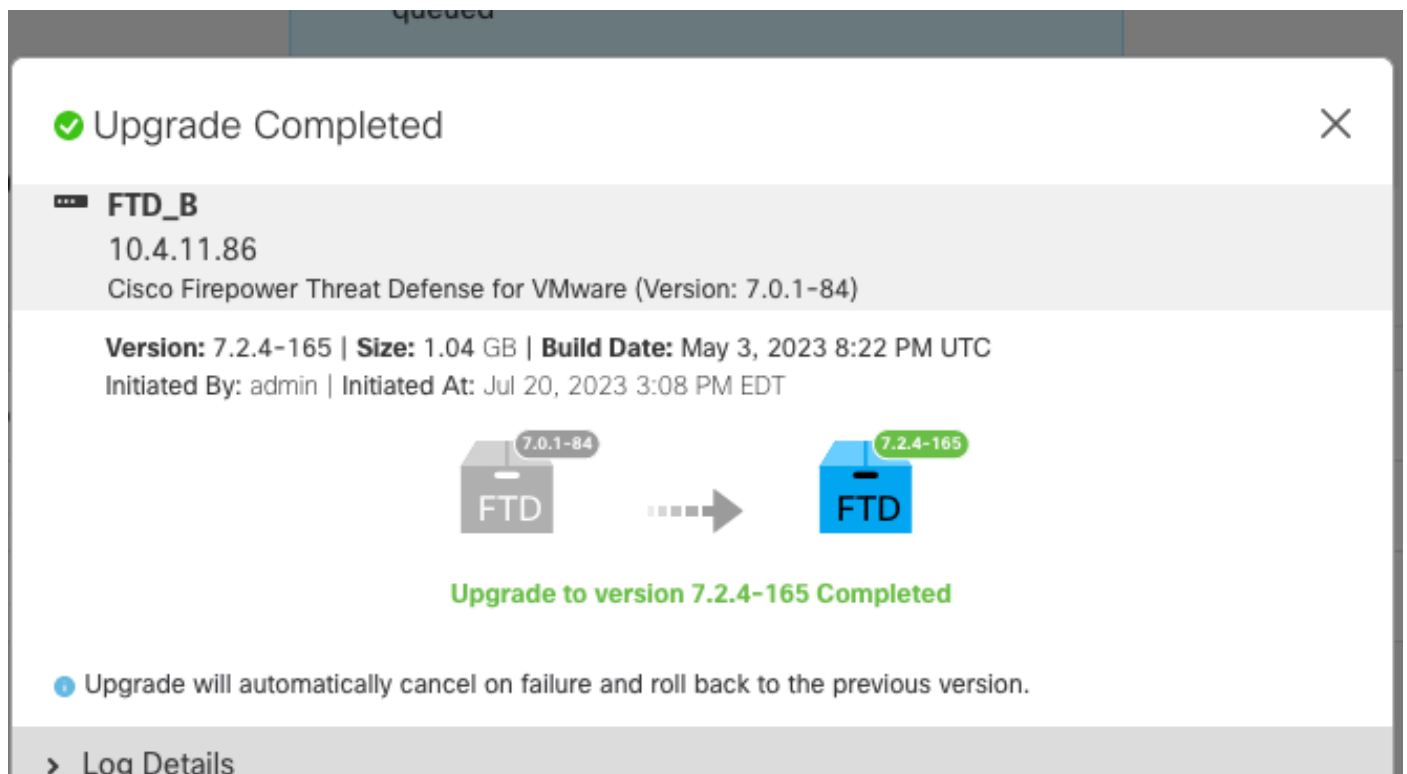
Broadcast message from root@firepower (Thu Jul 20 19:05:25 2023):

System will reboot now due to system upgrade.

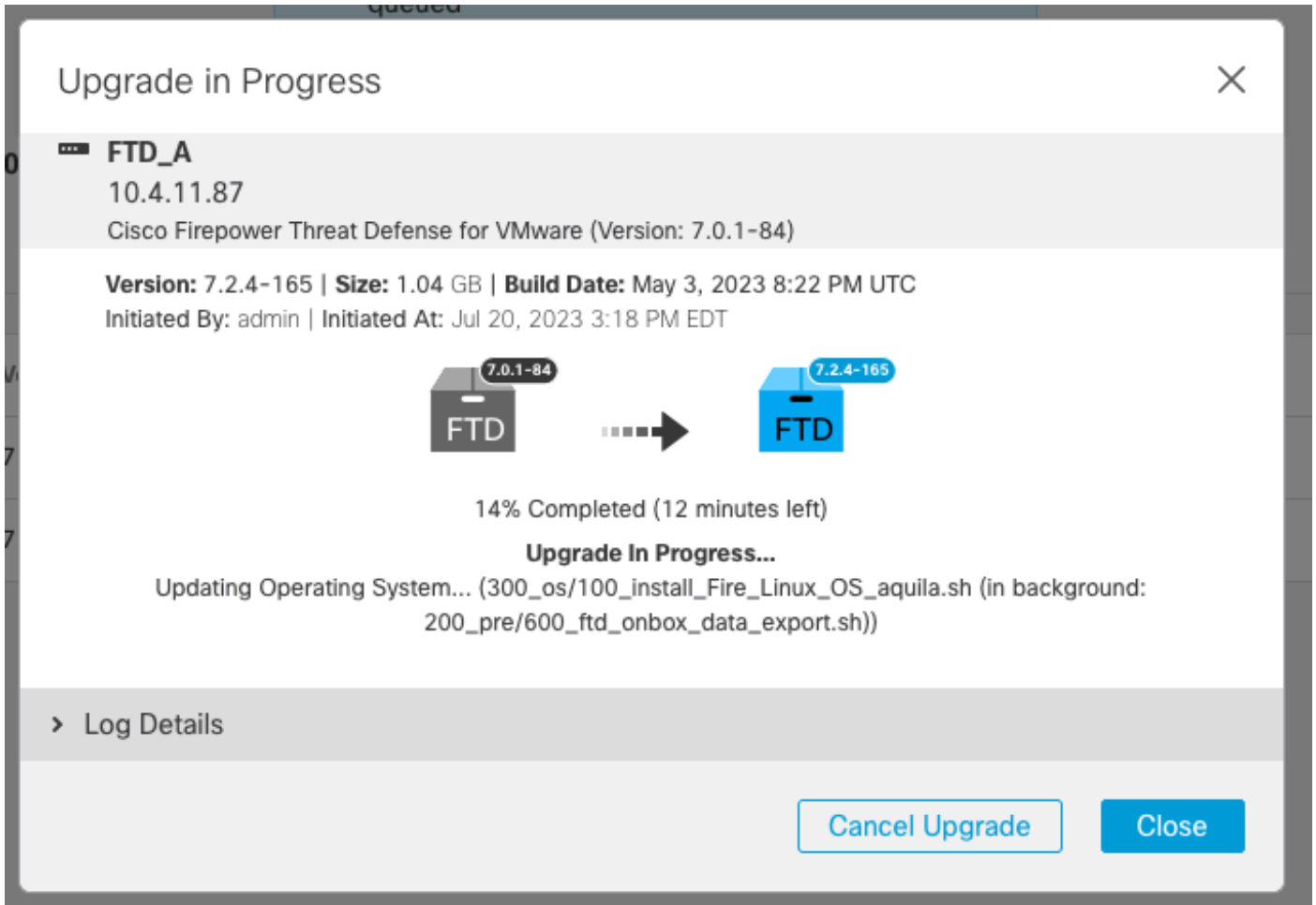
Broadcast message from root@firepower (Thu Jul 20 19:05:34 2023):

The system is going down for reboot NOW!

Upgrade status is marked as completed on GUI, and shows the next steps.



After the upgrade is completed in the Standby device, it starts in the Active device.



On CLI, move to LINA (system support diagnostic-cli) and check the failover state on the Standby FTD using command **show failover state**.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password:
firepower# show 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#
Switching to Active
```



**Note:** The failover occurs automatically as part of the upgrade. Before Active FTD reboots and complete the upgrade.

---

When the upgrade completes, a reboot is needed:

## ✔ Upgrade Completed



FTD\_A

10.4.11.87

Cisco Firepower Threat Defense for VMware (Version: 7.0.1-84)

**Version:** 7.2.4-165 | **Size:** 1.04 GB | **Build Date:** May 3, 2023 8:22 PM UTC

**Initiated By:** admin | **Initiated At:** Jul 20, 2023 3:28 PM EDT



Upgrade to version 7.2.4-165 Completed

> Log Details

Close

### Step 4. Switch Active Peer (Optional)



**Note:** If Secondary device as Active, it does not have any operational impact.  
Having Primary device as Active and Secondary as Standby is a best practice that helps tracking any failover that can occur.

---

In this case, the FTD Active is now Standby, a manual failover can be used to set it back to Active.

- Navigate to the three dots next to the edit sign.

View By:  Deployment History

All (2) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (2) ● Deployment Pending (1) ● Upgrade (2) ● Snort 3 (2) 🔍 Search Device Add ▾

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD_HA High Availability							
<span style="color:green">●</span>	FTD_A(Primary, Standby) 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮
<span style="color:green">●</span>	FTD_B(Secondary, Active) 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮

- **Select Switch Active Peer.**

View By:  Deployment History

All (2) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (2) ● Deployment Pending (1) ● Upgrade (2) ● Snort 3 (2) 🔍 Search Device Add ▾

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD_HA High Availability							
<span style="color:green">●</span>	FTD_A(Primary, Standby) 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮
<span style="color:green">●</span>	FTD_B(Secondary, Active) 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↶	⋮

Switch Active Peer

Break

Force refresh node status

Delete

Revert Upgrade

Health Monitor

Troubleshoot Files

- **Select YES** to confirm the failover.



# Switch Active Peer

Are you sure you want to make "FTD\_A" the active peer?

No

Yes

Validation of High Availability status at the end of upgrade and failover done.

## Devices > Device Management

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (1) Upgrade (2) Snort 3 (2)

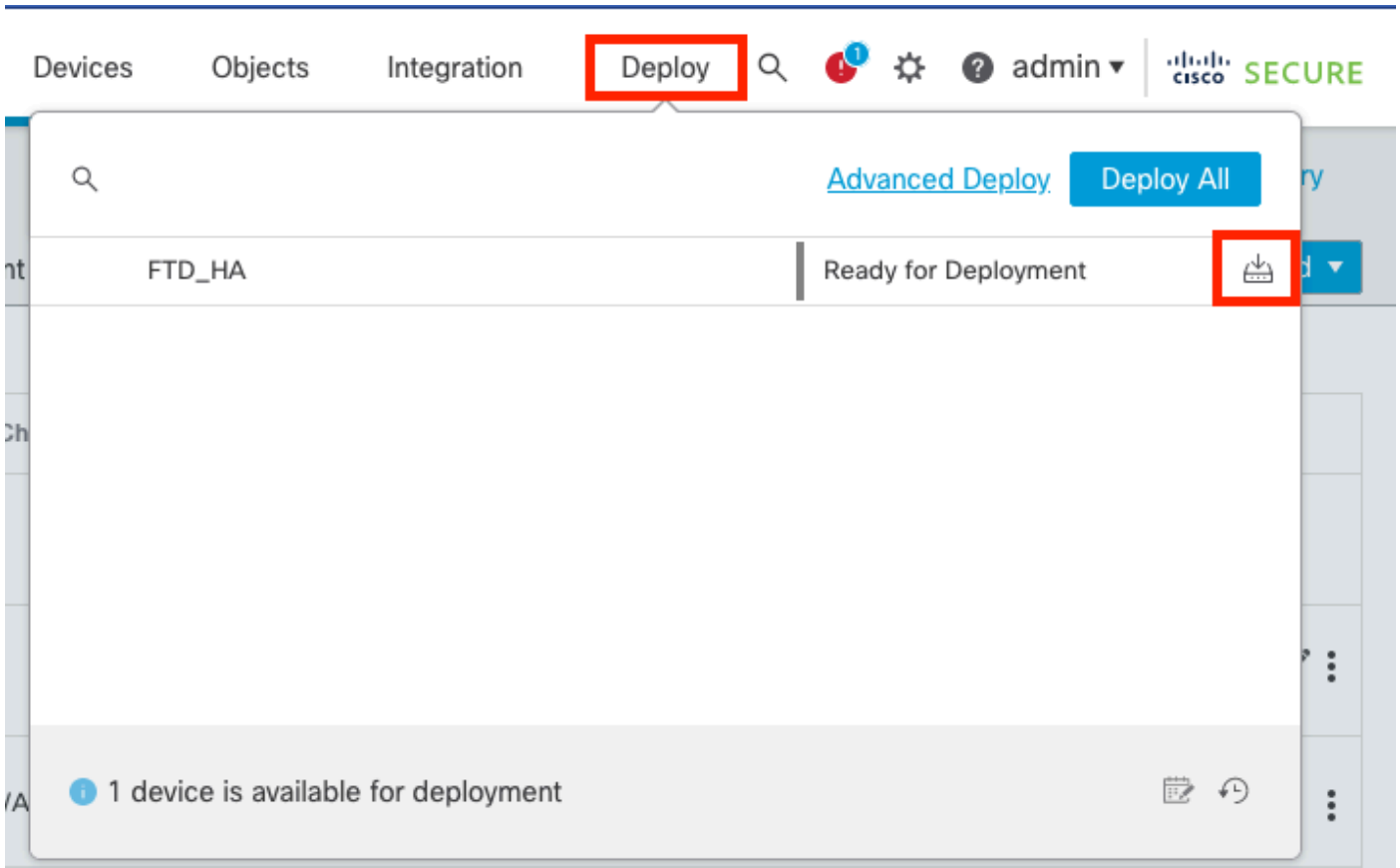
Search Device Add

Collapse All

Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FTD_HA High Availability						
FTD_A(Primary, Active) 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	
FTD_B(Secondary, Standby) 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	

## Step 5. Final Deploy

- Deploy a policy to devices **Deploy > Deploy to this device.**



## Validate

To validate High Availability status and upgrade are complete, you need to confirm the status:

Primary: Active

Secondary: Standby Ready

Both are under the version that is the recently changed one (7.2.4 in this example).

- In FMC GUI, navigate to **Devices > Device Management**.

The screenshot shows the 'Device Management' page in the Cisco FMC GUI. The table below displays the status of devices in a High Availability configuration.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FTD_HA High Availability						
FTD_A(Primary, Active) Snort 3 10.4.11.87 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↺
FTD_B(Secondary, Standby) Snort 3 10.4.11.86 - Routed	FTDv for VMware	7.2.4	N/A	Base, Threat (1 more...)	policy_lab	↺

- Over CLI clish, check the failover state using command **show failover state** and **show failover** for a more detailed information.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 499)  
Cisco Firepower Threat Defense for VMware v7.2.4 (build 165)

> show failover state

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

====Configuration State====

====Communication State====

Mac set

> show failover

Failover On

Failover unit Primary

Failover LAN Interface: FAILOVER\_LINK GigabitEthernet0/0 (up)

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 1285 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(3)39, Mate 9.18(3)39

Serial Number: Ours 9AVLW3FSSK8, Mate 9AJJSEGJS2T

Last Failover at: 19:56:41 UTC Jul 20 2023

This host: Primary - Active

Active time: 181629 (sec)

slot 0: ASAv hw/sw rev (/9.18(3)39) status (Up Sys)

Interface INSIDE (10.10.153.1): Normal (Monitored)

Interface OUTSIDE (10.20.153.1): Normal (Monitored)

Interface diagnostic (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Other host: Secondary - Standby Ready

Active time: 2390 (sec)

Interface INSIDE (10.10.153.2): Normal (Monitored)

Interface OUTSIDE (10.20.153.2): Normal (Monitored)

Interface diagnostic (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics

Link : FAILOVER\_LINK GigabitEthernet0/0 (up)

Stateful Obj	xmit	xerr	rcv	rerr
--------------	------	------	-----	------

General	29336	0	24445	0
---------	-------	---	-------	---

sys cmd	24418	0	24393	0
---------	-------	---	-------	---

...

Logical Update Queue Information

	Cur	Max	Total
--	-----	-----	-------

Recv Q:	0	11	25331
---------	---	----	-------

Xmit Q:	0	1	127887
---------	---	---	--------

If both FTDs are on the same version and high availability status is healthy, then the upgrade is complete.