

# Aggiorna FTD HA gestito da FMC

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica](#)

[Premesse](#)

[Configurazione](#)

[Passaggio 1. Carica pacchetto di aggiornamento](#)

[Passaggio 2. Verifica preparazione](#)

[Passaggio 3. Aggiorna FTD in alta disponibilità](#)

[Passaggio 4. Switch Active Peer \(opzionale\)](#)

[Passaggio 5. Installazione finale](#)

[Convalida](#)

---

## Introduzione

In questo documento viene descritto il processo di aggiornamento di Cisco Secure Firewall Threat Defense in High Availability gestito da un centro di gestione dei firewall.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Concetti e configurazione dell'alta disponibilità (HA, High Availability)
- Configurazione di Centro gestione firewall sicuro
- Configurazione Cisco Secure Firewall Threat Defense (FTD)

### Componenti usati

Le informazioni fornite in questo documento si basano su:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Panoramica

Il funzionamento del CCP prevede l'aggiornamento di un peer alla volta. Prima lo standby, quindi lo stato Attivo, eseguendo un failover prima del completamento dell'aggiornamento Attivo.

## Premesse

Il pacchetto di aggiornamento deve essere scaricato da [software.cisco.com](https://software.cisco.com) prima dell'aggiornamento.

Dalla CLI, eseguire il comando `show high-availability config` nel file FTD attivo per controllare lo stato dell'elevata disponibilità.

```
> 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 |

Se non sono visibili errori, procedere con l'aggiornamento.

## Configurazione

### Passaggio 1. Carica pacchetto di aggiornamento

- Caricare il pacchetto di aggiornamento FTD nel FMC utilizzando l'interfaccia utente grafica (GUI).

Questa versione deve essere precedentemente scaricata dal sito del software Cisco in base al modello FTD e alla versione desiderata.

---

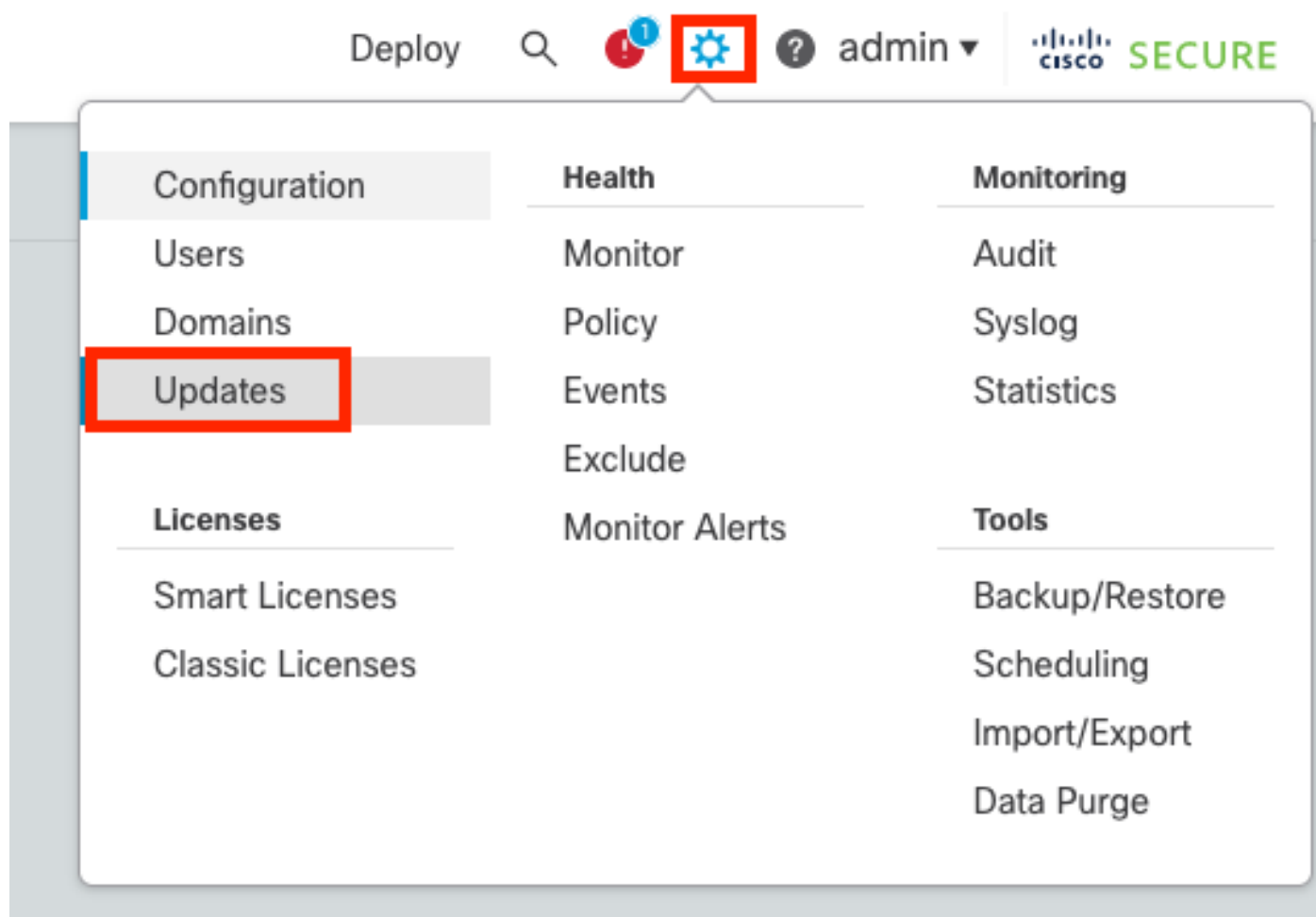


Avviso: verificare che la versione del FMC sia successiva o uguale alla nuova versione del

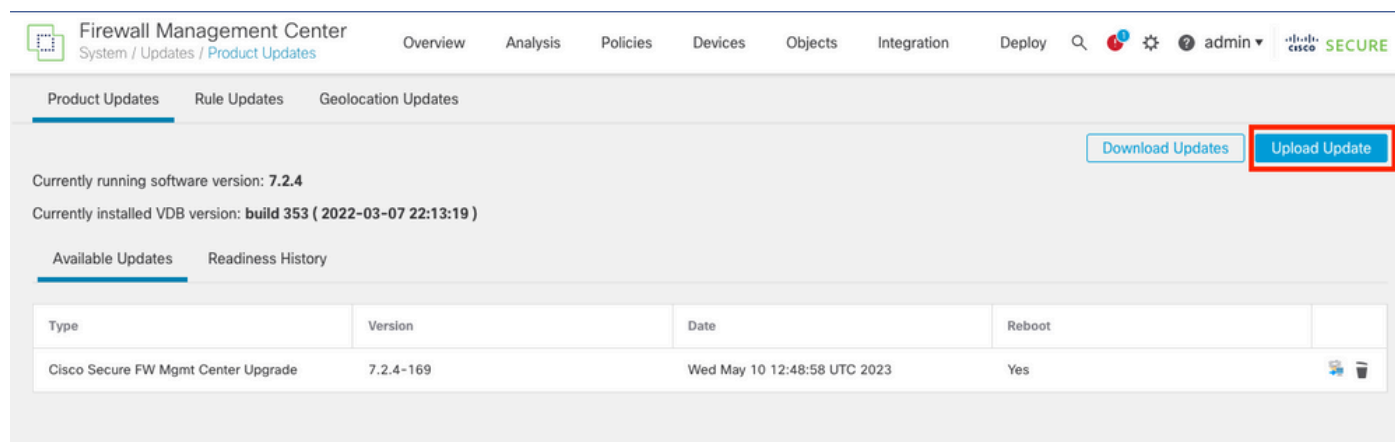
---

FTD da aggiornare.

Sistema > Aggiornamenti



- Selezionare Upload Update.



- Cercare l'immagine scaricata in precedenza, quindi selezionare Upload (Carica).

Firewall Management Center  
System / Updates / Product Updates

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin

Product Updates Rule Updates Geolocation Updates

Currently running software version: 7.2.4

Updates

Upload software updates and patches here.

Action  Upload local software update package  
 Specify software update source (Firewall Threat Defense devices only)

Package  Cisco\_FTD\_Upgrade-7.2.4-165.sh.REL.tar

## Passaggio 2. Verifica preparazione

I controlli di idoneità confermano se gli accessori sono pronti per l'aggiornamento.

- Selezionare l'opzione Install (Installa) nel pacchetto di aggiornamento corretto.

Firewall Management Center  
System / Updates / Product Updates

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin

Product Updates Rule Updates Geolocation Updates

✔ Success  
Upload succeeded

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    |  |
| Cisco FTD Upgrade                   | 7.2.4-165 | Wed May 3 20:22:28 UTC 2023  | Yes    |  |

Selezionare l'aggiornamento desiderato. In questo caso, la selezione è per:

- Annulla automaticamente in caso di errore di aggiornamento e ripristina la versione precedente.
- Abilitare il ripristino dopo l'aggiornamento.
- Aggiornare Snort 2 a Snort 3.
- Selezionare il gruppo HA di FTD e fare clic su Verifica preparazione.

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><br>Cisco Firepower Threat Defense for VMware Cluster                     |  |                         |                           |         |                        |   |
| <input checked="" type="checkbox"/> <b>FTD_A (active)</b><br>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><br>10.4.11.86 - Cisco Firepower Threat Defense for VMware v7.0.1          | ✔ Compatibility check passed. Proceed with |                         |                           | N/A     | 10 min                 | ⬇ |

Back Check Readiness Install

L'avanzamento può essere controllato nel centro messaggi **Messaggi > Attività**.

Policies   Devices   Objects   Integration   Deploy   🔍   📢   ⚙️   ? admin ▼   **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.

Quando il controllo di fattibilità viene completato sia in FTD che in caso di esito positivo, è possibile eseguire l'aggiornamento.

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><br>Cisco Firepower Threat Defense for VMware Cluster                     |  |                         |                           |         |                        |   |
| <input type="checkbox"/> <b>FTD_A (active)</b><br>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><br>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                 | ⬇ |

Passaggio 3. Aggiorna FTD in alta disponibilità

- Selezionare la coppia HA e fare clic su Installa.

Firewall Management Center  
System / Updates / Upload Update

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin

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<br>Cisco Firepower Threat Defense for VMware Cluster                     |   |                         |                           |         |                        |    |
| <input checked="" type="checkbox"/> | FTD_A (active)<br>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<br>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                 | ⬇️ |

Avviso per continuare l'aggiornamento. Il sistema si riavvia per completare l'aggiornamento. Selezionare OK.


 10.88.243.115:43092

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

L'avanzamento può essere controllato nel centro messaggi Messaggi > Attività.

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.

Se si fa clic su firepower: Visualizza dettagli, l'avanzamento viene visualizzato graficamente e i log di 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

---

Nota: l'aggiornamento richiede circa 20 minuti per FTD.

---

Dalla CLI, lo stato può essere controllato nella cartella di aggiornamento `/ngfw/var/log/sf`; passare alla modalità Expert e accedere alla directory principale.

```
> 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.log

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.

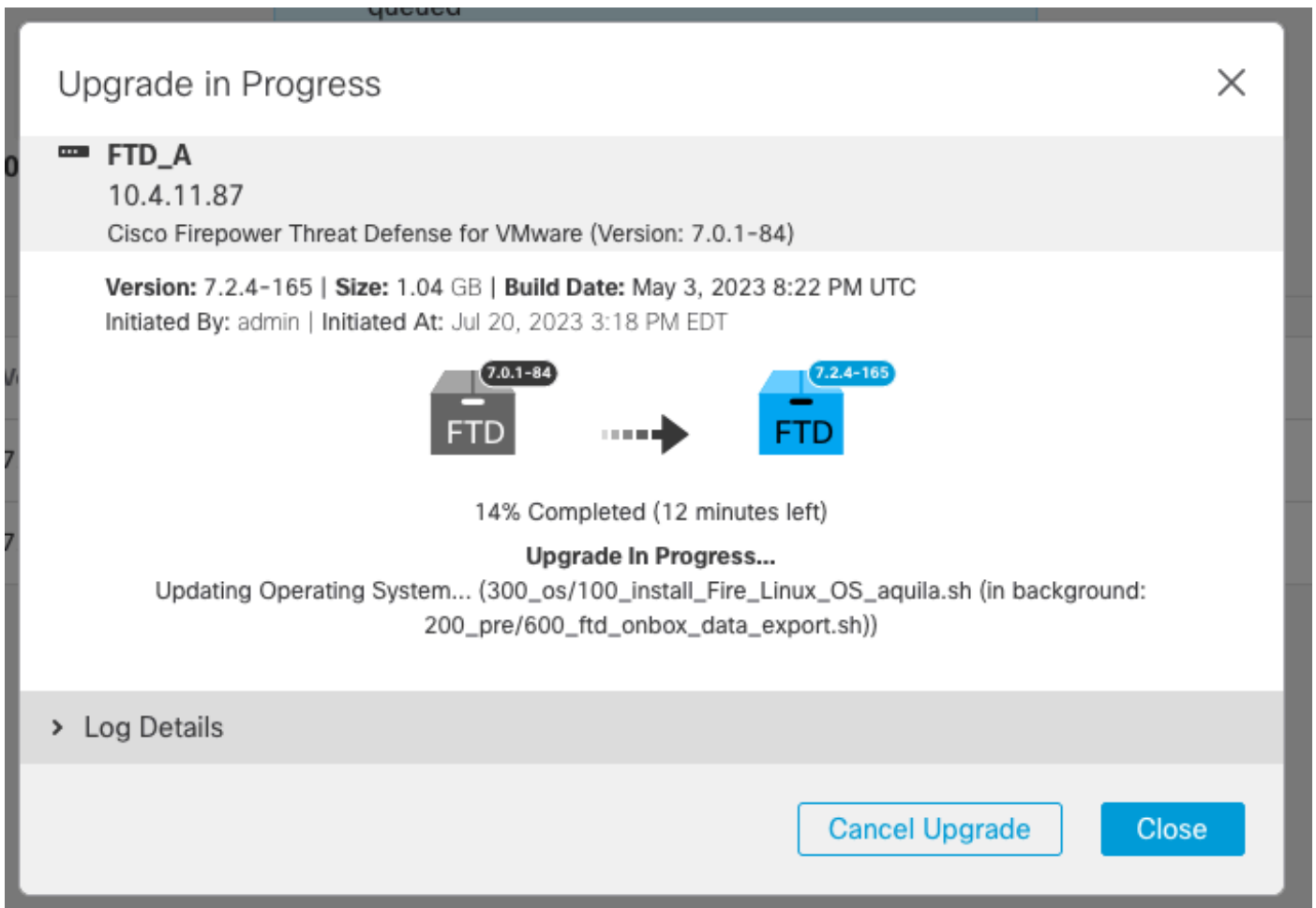
Broadcast message from root@firepower (Thu Jul 20 19:05:34 2023):

The system is going down for reboot NOW!

Lo stato dell'aggiornamento è contrassegnato come completato sulla GUI e mostra i passaggi successivi.



Al termine dell'aggiornamento nel dispositivo di standby, l'aggiornamento viene avviato nel dispositivo attivo.



Dalla CLI, passare a LINA (system support diagnostic-cli) e controllare lo stato di failover sull'FTD in standby usando il comando 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

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

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

firepower#
      Switching to Active
```



Nota: il failover viene eseguito automaticamente durante l'aggiornamento. Prima del riavvio di Active FTD e completare l'aggiornamento.

---

Al termine dell'aggiornamento, è necessario riavviare il sistema:

✔ 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

Passaggio 4. Switch Active Peer (opzionale)



Nota: se il dispositivo secondario è attivo, non ha alcun impatto operativo.  
La disponibilità di un dispositivo primario attivo e di un dispositivo secondario in standby è una procedura consigliata che consente di tenere traccia di qualsiasi failover che può verificarsi.

---

In questo caso, l'FTD attivo è ora Standby e può essere utilizzato un failover manuale per reimpostarlo su Attivo.

- Passare ai tre punti accanto al segno di modifica.

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

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](#)

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

- Selezionare Switch Active Peer.

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

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](#)

| <input type="checkbox"/>             | Name  | Model           | Ver... | Chassis | Licenses                 | Access Control Policy | Auto RollBack |   |
|--------------------------------------|---|-----------------|--------|---------|--------------------------|-----------------------|---------------|---|
| <input type="checkbox"/>             | Ungrouped (1)                                   |                 |        |         |                          |                       |               |   |
| <input type="checkbox"/>             | FTD_HA<br>High Availability                     |                 |        |         |                          |                       |               |   |
| <span style="color: green;">●</span> | FTD_A(Primary, Standby)<br>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)<br>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

- Selezionare YES per confermare il failover.



# Switch Active Peer

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

No

Yes

Convalida dello stato di elevata disponibilità al termine dell'aggiornamento e del failover.  
Dispositivi > Gestione dispositivi

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)

Deployment History

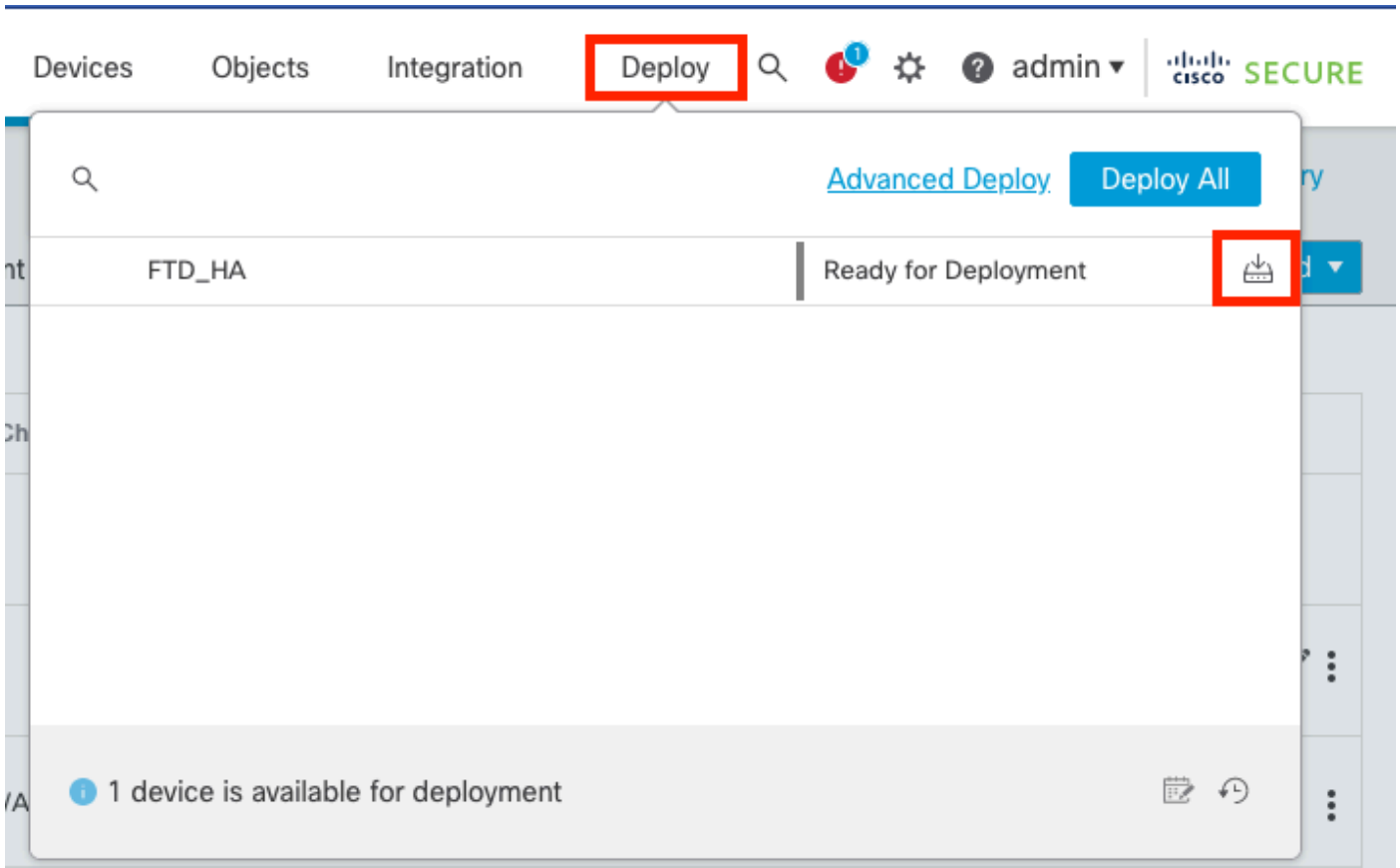
Search Device Add

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<br>High Availability                      |                 |        |         |                          |                       |               |  |
| <input checked="" type="checkbox"/> | FTD_A(Primary, Active)<br>10.4.11.87 - Routed    | FTDv for VMware | 7.2.4  | N/A     | Base, Threat (1 more...) | policy_lab            | ↺             |  |
| <input checked="" type="checkbox"/> | FTD_B(Secondary, Standby)<br>10.4.11.86 - Routed | FTDv for VMware | 7.2.4  | N/A     | Base, Threat (1 more...) | policy_lab            | ↺             |  |

## Passaggio 5. Installazione finale

- Distribuisci un criterio ai dispositivi Distribuisci > Distribuisci al dispositivo.



## Convalida

Per convalidare lo stato dell'alta disponibilità e il completamento dell'aggiornamento, è necessario confermare lo stato:

Primario: attivo

Secondario: Pronto per standby

Entrambi si trovano nella versione modificata di recente (7.2.4 in questo esempio).

- Nell'interfaccia utente di FMC, selezionare Devices > Device Management (Dispositivi > Gestione dispositivi).

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy Search Settings Help admin

View By: Group

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

Deployment History Search Device Add

Collapse All

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

- Dalla CLI, controllare lo stato del failover usando il comando show failover state e show failover per informazioni più dettagliate.

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 |

Se entrambi gli FTD si trovano nella stessa versione e lo stato di elevata disponibilità è integro, l'aggiornamento è completato.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).