

# Upgrade von FMC-verwaltetem FTD HA-Workflow mit Version 7.4.2

## Problem

Das Hauptproblem besteht in den Arbeitsabläufen und technischen Anforderungen für die Durchführung eines Hochverfügbarkeits-Upgrades auf Cisco FirePOWER Threat Defense (FTD)-Geräten (insbesondere FPR1120), die von einem FirePOWER Management Center (FMC) 4700 mit Version 7.4.2 verwaltet werden. In diesem Artikel werden die vorbereitenden Schritte, Best Practices und Überlegungen für eine erfolgreiche FTD HA-Aktualisierung beschrieben.

## Umwelt

- Technologie: Cisco Secure Firewall FirePOWER 7.4
- Subtechnologie: Firepower Threat Defense (FTD) - Software-Update/Sicherheits-Update/Neuzuordnung/Migration/Sicherung und Wiederherstellung
- Produktfamilie: FPRLOW (einschließlich FPR1120)
- Firepower Threat Defense (FTD) in Hochverfügbarkeitspaar
- Verwaltet vom FirePOWER Management Center (FMC) 4700
- FMC-Softwareversion: 7.4.2
- Geplante Upgrade-Aktivitäten innerhalb eines definierten Wartungsfensters

## Auflösung

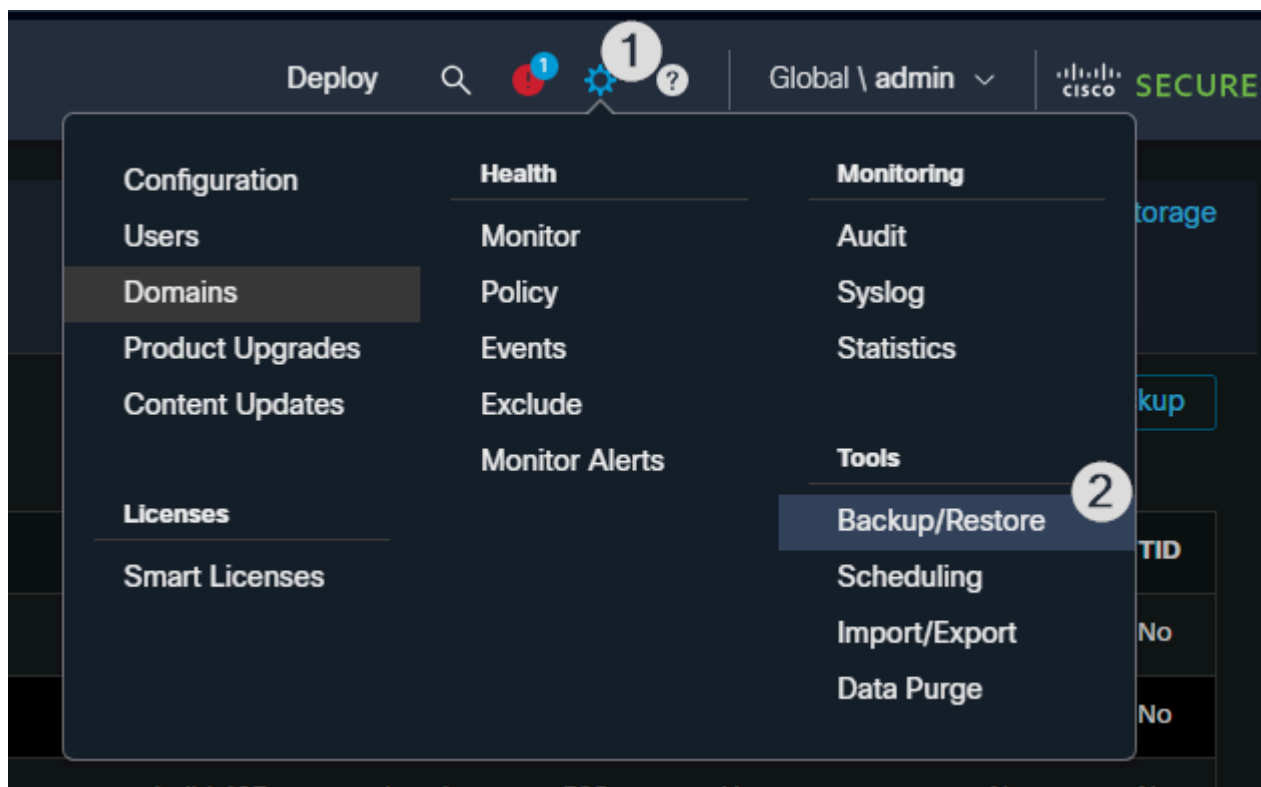
Befolgen Sie diesen detaillierten Workflow, um sicherzustellen, dass ein erfolgreiches Upgrade der von FMC verwalteten FTD HA-Paare durchgeführt wird:

### Schritt 1: Vorbereitung auf das Upgrade

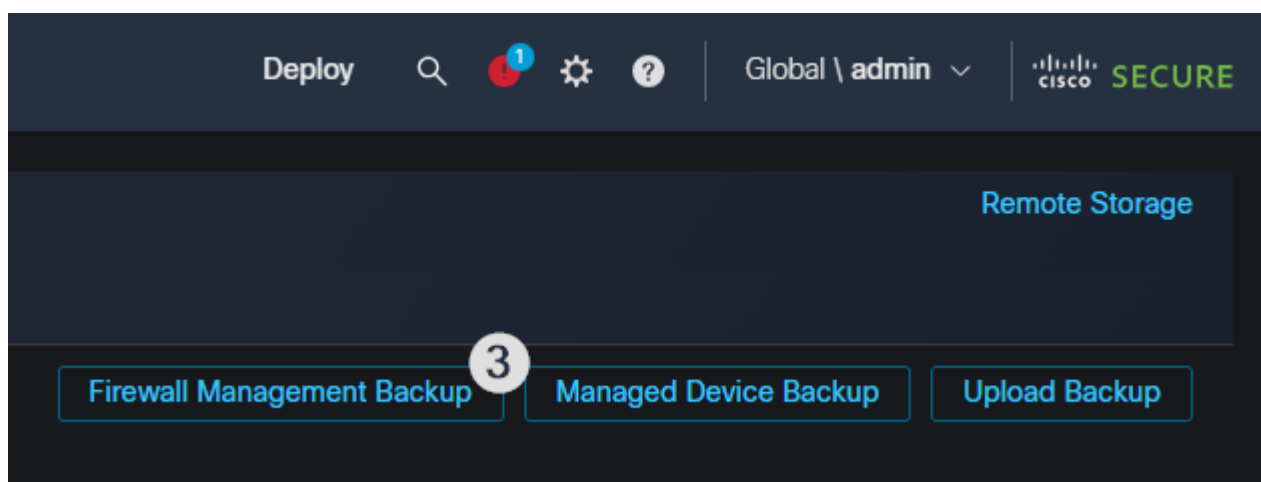
Vor Beginn des Upgrade-Vorgangs ist es wichtig, Konfigurations-Backups sowohl der FTD HA-Geräte als auch des FMC zu erstellen und zu speichern. Dadurch wird sichergestellt, dass

Konfigurationen bei einem Upgrade-Fehler oder einem unerwarteten Problem wiederhergestellt werden können.

So sichern Sie die FMC-Konfiguration: Navigieren Sie zu System > Tools: Backup/Restore (System > Extras: Sicherung/Wiederherstellung in der FMC-Benutzeroberfläche), und klicken Sie auf die Schaltfläche Firewall Management Backup (Firewall-Management-Sicherung):



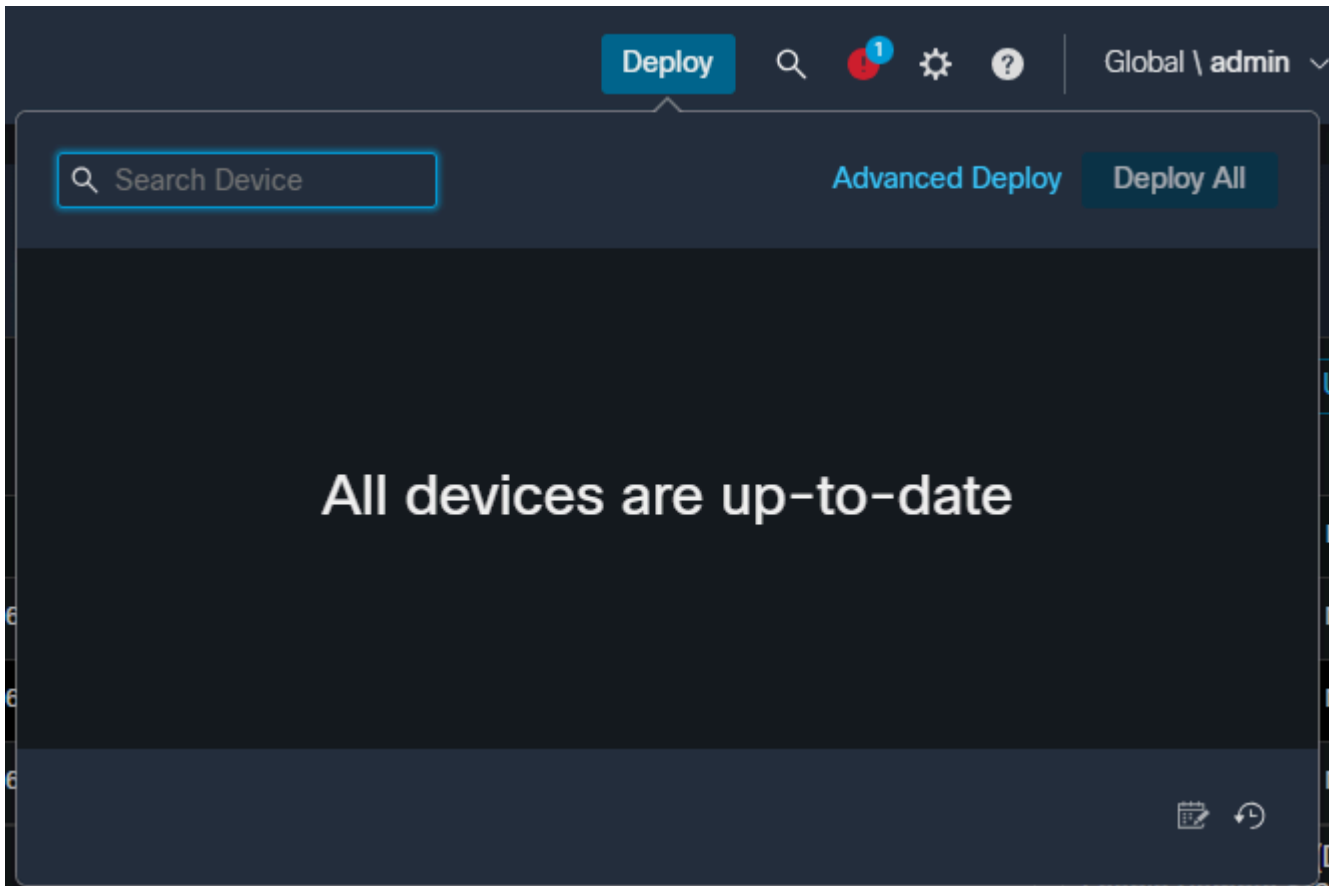
inline\_image\_0.png



inline\_image\_1.png

Klicken Sie auf die Schaltfläche Managed Device Backup (verwaltetes Gerätebackup), um das FTD HA-Paar zu sichern.

Um sicherzustellen, dass der Konfigurationsstatus des FTD-Geräts erhalten bleibt, stellen Sie sicher, dass die letzte Konfigurationsbereitstellung vom FMC für beide HA-Peers abgeschlossen wurde:



inline\_image\_2.png

## Schritt 2: Überprüfen des aktuellen Status des FTD HA-Paars

Überprüfen Sie den HA-Status, um sicherzustellen, dass beide Peers fehlerfrei und synchronisiert sind, bevor Sie mit dem Upgrade fortfahren. Verwenden Sie diesen Befehl in der FTD-CLI, um den Gerätestatus zu überprüfen:

```
> Failover-Status anzeigen
```

Beispiel:

```
Status Datum/Uhrzeit des letzten Fehlers Grund
```

```
Dieser Host - primär
```

```
Aktiv Keine
```

Anderer Host - Sekundär

Standby-fähig Keine

====Konfigurationsstatus====

Synchronisierung übersprungen

====Kommunikationsstatus====

### Mac setSchritt 3: Wartungsfenster planen und kommunizieren

Stellen Sie sicher, dass das Wartungsfenster klar definiert ist und alle Beteiligten informiert sind. Für diesen Workflow wurde die Wartung entsprechend geplant:

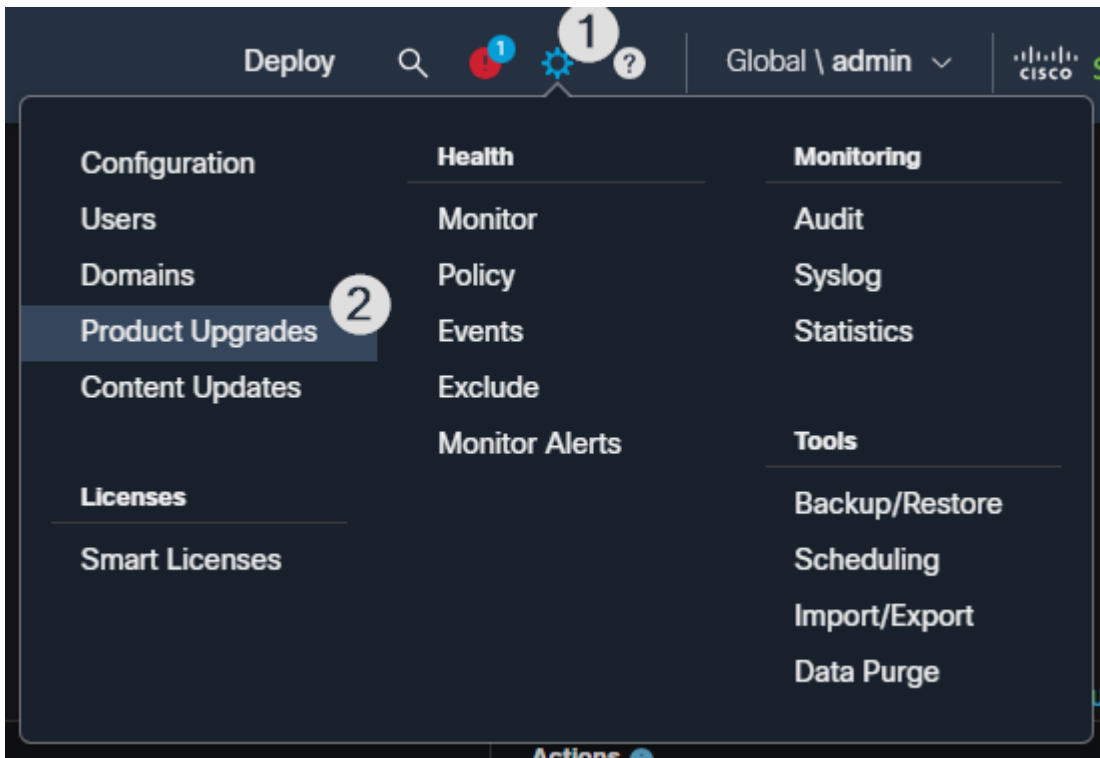
- Startzeit: 18.11.2025 12:00:00 (UTC -3 Argentina/Buenos\_Aires)
- Endzeit: 18.11.2025 14:00:00 (UTC -3 Argentinien/Buenos\_Aires)

### Schritt 4: FTD HA-Upgrade starten

Starten Sie das Upgrade vom FMC aus, und achten Sie dabei darauf, dass Sie die von Cisco empfohlene Vorgehensweise für das Upgrade von FTD HA-Paaren einhalten. Während des Upgrade-Vorgangs wird das Upgrade in der Regel automatisch im Wechsel durchgeführt:

1. FTD im Standby-Modus aktualisieren
2. Failover auf die neu aktualisierte FTD und Aktivierung.
3. Aktualisieren Sie die andere FTD jetzt im Standby-Modus.

Navigieren Sie in der FMC-GUI zu System > Product Upgrades (System > Produkt-Upgrades), und wählen Sie die Zielversion für das Upgrade aus.



inline\_image\_3.png

## Schritt 5: Überwachen des Upgrade-Prozesses

Überwachen Sie den Fortschritt des Upgrades für beide Einheiten genau. Verwenden Sie den Abschnitt für die Überwachung von FMC-GUI-Aufträgen oder die CLI für Statusaktualisierungen. So überprüfen Sie den Fortschritt des Upgrades in der CLI:

> Aktualisierungsstatus anzeigen

Beispiel:

Upgrade wird auf Standby-Gerät durchgeführt...

Upgrade auf Standby-Gerät abgeschlossen.

Failover wird initiiert...

Aktualisierung wird für aktive Einheit durchgeführt...

Die Aktualisierung wurde auf beiden Geräten abgeschlossen.

HA-Paar ist synchronisiert. Schritt 6: Überprüfung nach dem Upgrade

Überprüfen Sie nach Abschluss des Upgrades Folgendes:

- Auf beiden FTD-Geräten wird die beabsichtigte Softwareversion ausgeführt.
- Der HA-Status meldet beide Einheiten als fehlerfrei und synchronisiert.
- Alle beabsichtigten Services und Netzwerkflüsse werden erwartungsgemäß ausgeführt.

> Version anzeigen

Beispiel:

-----[ Feuerkraft ]-----

Modell: Cisco Firepower Threat Defense für VMware (75) Version 7.4.2.4 (Build 9)

UUID: bc9d31e8-0517-11f0-9c89-c358b8259f96

LSP-Version: lsp-rel-20260128-1954

VDB-Version: 404

-----

> Failover anzeigen

Beispiel:

> Failover anzeigen

Failover ein

Failover-Einheit Primär

Failover LAN-Schnittstelle: Failover-Status GigabitEthernet0/7 (aktiv)

Timeout für erneute Verbindung 0:00:00

Abfragehäufigkeit 1 Sekunden, Haltezeit 15 Sekunden

Interface-Abfragehäufigkeit 5 Sekunden, Haltezeit 25 Sekunden

Schnittstellenrichtlinie 1

Überwachte Schnittstellen 4 von maximal 361

Das Intervall für die Benachrichtigung über die Verschiebung der MAC-Adresse ist nicht festgelegt.

Failover-Replikation http

Version: Unsere Version 9.20(2)121, Partner 9.20(2)121

Seriennummer: Unsere SERIAL, Mate SERIAL

Letztes Failover um: 14:29:08 UTC 31. Dez. 2025

Dieser Host: Primär - Aktiv

Aktive Zeit: 3418340 (Sek.)

Steckplatz 0: ASAv hw/sw rev (/9.20(2)121) status (Up Sys)

EXTERNE Schnittstelle (IPADDRESS): Normal (überwacht)

Interface INSIDE (IPADDRESS): Normal (überwacht)

Schnittstelle DMZ (IPADDRESS): Normal (überwacht)

Schnittstellenverwaltung (IPADDRESS): Normal (überwacht)

Steckplatz 1: Status "Snort Rev (1.0)" (aktiv)

Steckplatz 2: Status der Festplattenaktualisierung (1.0) (aktiv)

Anderer Host: Sekundär - Standby-fähig

Aktive Zeit: 0 (Sek.)

EXTERNE Schnittstelle (IPADDRESS): Normal (überwacht)

Interface INSIDE (IPADDRESS): Normal (überwacht)

Schnittstelle DMZ (IPADDRESS): Normal (überwacht)

Schnittstellenverwaltung (IPADDRESS): Normal (überwacht)

Steckplatz 1: Status "Snort Rev (1.0)" (aktiv)

Steckplatz 2: Status der Festplattenaktualisierung (1.0) (aktiv)

## Schritt 7: Sicherstellen, dass die Backups auf dem neuesten Stand sind

Erstellen Sie nach dem Upgrade neue Backups von FMC und FTD, um den aktuellen, aktualisierten Konfigurationsstatus zu erfassen.

Wiederholen Sie den Sicherungsvorgang wie in Schritt 1 beschrieben.

## Ursache

None. Dies ist ein Standard-Upgrade-Workflow für Cisco FTD HA, der von FMC verwaltet wird.

## Verwandte Inhalte

- [Technischer Support und Downloads von Cisco](#)
- [FTD HA-Upgrade von FMC verwaltet](#)
- [Fehlerbehebung bei FirePOWER-Verfahren zur Dateigenerierung](#)
- [Versionshinweise](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.