

# Upgrade des FirePOWER Extensible Operating System (FXOS) mit dem FirePOWER Chassis Manager

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Vorbereitungen](#)

[Konfigurieren](#)

[Validierung](#)

## Einleitung

Dieses Dokument beschreibt ein Beispiel für ein Upgrade der FXOS-Version (Firepower Extensible Operating System) mit dem FXOS-Chassis-Manager.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Für diesen Leitfaden gibt es keine spezifischen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FirePOWER 4125
- FirePOWER Chassis Manager (FCM) Version 2.12 (0.484)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Spezifische Anforderungen für dieses Dokument:

- Verbindung zur Management-IP des Chassis
- Das FXOS-Installationspaket (.SPA), die zuvor vom Cisco Software-Portal heruntergeladen wurden

Dieses Upgrade-Verfahren wird auf folgenden Appliances unterstützt:

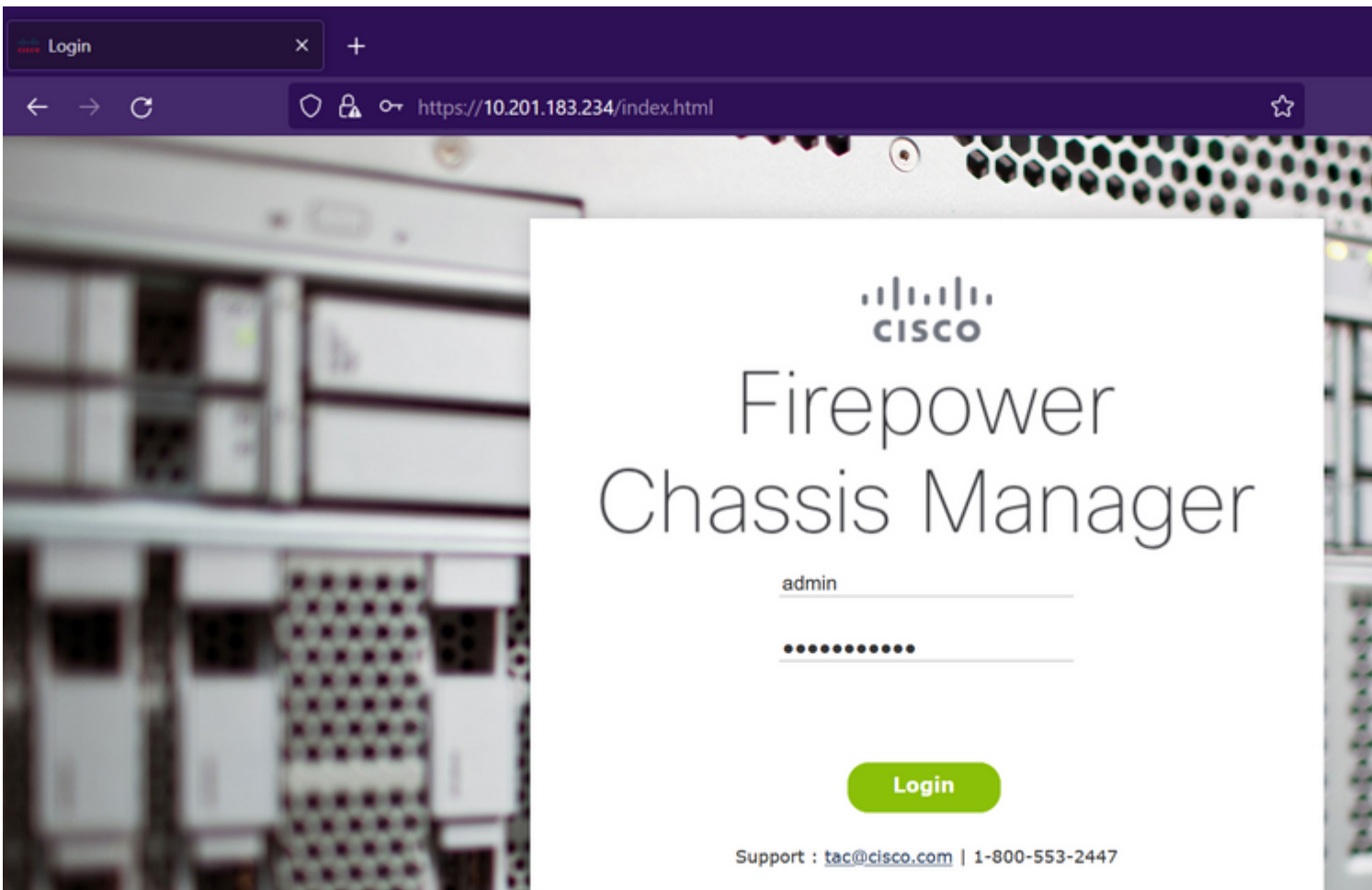
- Cisco Firepower 4100-Serie
- Cisco Firepower 9300-Serie

## Vorbereitungen

1. Überprüfen Sie, ob das Modell mit diesem Verfahren kompatibel ist.
2. Sichern der FXOS- und logischen Gerätekonfigurationen
3. Planen Sie ein Wartungsfenster, um dieses Verfahren durchzuführen.

## Konfigurieren

**Schritt 1:** Melden Sie sich bei Firepower Chassis Manager an:



**Vorsicht:** Um sich bei FCM anzumelden, müssen Sie die Management-IP-Adresse des Chassis verwenden. Beachten Sie, dass sich diese IP von der Management-IP-Adresse des logischen Geräts (FTD oder ASA) unterscheidet.

**Schritt 2:** Navigieren Sie zu **System > Updates** , um die Aktualisierungsseite im Firepower Chassis Manager aufzurufen:

## Available Updates

Image Name	Type	Version	Status	Build Date	Image
fxos-k9.2.12.0.484.SPA	platform-bundle	2.12(0.484)	Installed	04/06/2023	✓ Verif
cisco-ftd.7.2.4.165.csp	ftd	7.2.4.165	Installed	05/03/2023	Verifie

**Schritt 3:** Laden Sie das Installationspaket auf den Firepower Chassis Manager hoch:

- I. Klicken Sie auf die Schaltfläche **Bild hochladen**.
- II. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie im Datei-Explorer Ihr Installationspaket aus.
- III. Wählen Sie die Schaltfläche **Hochladen**, um das Hochladen des Pakets zu starten.

Overview Interfaces Logical Devices Security Engine Platform Settings

### Available Updates

Image Name	Type	Version	Status	Build Date	Image
fxos-k9.2.12.0.484.SPA	platform-bundle	2.12(0.484)	Installed	04/06/2023	✓ Verified
cisco-ftd.7.2.4.165.csp	ftd	7.2.4.165	Installed	05/03/2023	Verified

**Upload Image** [?] [X]

Select File:

fxos-k9.2.13.0.212.SPA

11 Successful Login in last 24 hrs - [View Details](#) | Tue Jul 18 2023 at 22:56:05 from - console

Beispiel für eine Fortschrittsleiste zum Hochladen:

Overview Interfaces Logical Devices Security Engine Platform Settings

### Available Updates

Image Name	Type	Version	Status	Build Date	Image
fxos-k9.2.12.0.484.SPA	platform-bundle	2.12(0.484)	Installed	04/06/2023	✓ Verified
cisco-ftd.7.2.4.165.csp	ftd	7.2.4.165	Installed	05/03/2023	Verified

**Upload Image** [?] [X]

Uploading fxos-k9.2.13.0.212.SPA

11 Successful Login in last 24 hrs - [View Details](#) | Tue Jul 18 2023 at 22:56:05 from - console


**Schritt 4:** Klicken Sie im Popup-Fenster auf **OK**, um zur Seite "Updates" zurückzukehren:

Overview Interfaces Logical Devices Security Engine Platform Settings

Available Updates

Image Name	Type	Version	Status	Build Date	Image
fxos-k9.2.13.0.212.SPA	platform-bundle	2.13(0.212)	Not-Installed	02/07/2023	✓ Verif
fxos-k9.2.12.0.484.SPA	platform-bundle	2.12(0.484)	Installed	04/06/2023	✓ Verif
cisco-ftd.7.2.4.165.csp	ftd	7.2.4.165	Installed	05/03/2023	Verified

**Success**

 fxos-k9.2.13.0.212.SPA  
Successfully Uploaded

OK

11 Successful Login in last 24 hrs - [View Details](#) | Tue Jul 18 2023 at 22:56:05 from - console

**Schritt 5:** Klicken Sie auf die Schaltfläche **Upgrade**, um die Installation zu starten:

Overview Interfaces Logical Devices Security Engine Platform Settings

Available Updates

Image Name	Type	Version	Status	Build Date	Image
fxos-k9.2.13.0.212.SPA	platform-bundle	2.13(0.212)	Not-Installed	02/07/2023	✓ Verif
fxos-k9.2.12.0.484.SPA	platform-bundle	2.12(0.484)	Installed	04/06/2023	✓ Verif
cisco-ftd.7.2.4.165.csp	ftd	7.2.4.165	Installed	05/03/2023	Verified

11 Successful Login in last 24 hrs - [View Details](#) | Tue Jul 18 2023 at 22:56:05 from - console

**Schritt 6:** Wählen Sie **Ja**, um das Upgrade zu bestätigen:

Overview Interfaces Logical Devices Security Engine Platform Settings

### Available Updates

Image Name	Type	Version	Status	Build Date	Image
fxos-k9.2.13.0.212.SPA	platform-bundle	2.13(0.212)	Not-Installed	02/07/2023	✓ Verified
fxos-k9.2.12.0.484.SPA	platform-bundle	2.12(0.484)		02/07/2023	✓ Verified
cisco-ftd.7.2.4.165.csp	ftd	7.2.4.165		02/07/2023	✓ Verified

#### Update Bundle Image

ⓘ Please ensure Application configuration is saved. All existing sessions will be terminated and FCM will not be accessible during the process. It may take several minutes. Chassis will reboot after upgrade, please re-login to FCM after upgrade completes.

Selected version 2.13(0.212) will be installed. Do you want to proceed?

Yes No

11 Successful Login in last 24 hrs - [View Details](#) | Tue Jul 18 2023 at 22:56:05 from - console

**Vorsicht:** Dieser Upgrade-Prozess dauert bis zu 45 Minuten. Beachten Sie, dass das Chassis während des Upgrades neu gestartet wird.

## Validierung

Überprüfen Sie den Upgrade-Prozess mit einer FXOS-CLI-Sitzung:

- I. Erstellen Sie eine SSH-Sitzung mit der Management-IP des Chassis.
- II. Überprüfen Sie den Fortschritt des FXOS-Upgrades auf der Firmware-Überwachung.
  - A. Wechseln Sie mit dem Command-Scope-System zum Systembereich.
  - B. Um den Fortschritt des Upgrades anzuzeigen, verwenden Sie den Befehl **show firmware monitor**

Beispiel für die vorgeschlagenen Verfahren:

```

B-09-FPR4125-NGFW-K9-18# scope system
B-09-FPR4125-NGFW-K9-18 /system # show firmware monitor
FPRM:
  Package-Vers: 2.12(0.484)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.12(0.484)
  Upgrade-Status: Upgrading

Chassis 1:
  Server 1:
    Package-Vers: 2.12(0.484)
    Upgrade-Status: Ready

B-09-FPR4125-NGFW-K9-18 /system # █

```

**Vorsicht:** Wenn das Upgrade abgeschlossen ist, müssen Sie alle Komponenten im Status "**Ready**" (**Bereit**) sehen. Wenn Sie feststellen, dass sich eine Komponente im Status "**Failed**" (**Fehlgeschlagen**) befindet, wenden Sie sich an das TAC.

Nach Abschluss des Upgrades können Sie sich beim Firepower Chassis Manager anmelden, um die aktuelle Version zu überprüfen. Dies finden Sie im Überblick-Dashboard:

**Overview** Interfaces Logical Devices Security Engine Platform Settings

**B-09-FPR4125-NGFW-K9-18** 10.201.183.234  
 Model: Cisco Firepower 4125 Security Appliance | **Version: 2.13(0.212)** | Operational State: Operable

CONSOLE MGMT USB  
 Power 1 - Running Power 2 - Running

Network Module 1 Network Module 2

**FAULTS** 0(1) CRITICAL 0(1) MAJOR  
**INTERFACES** 13 DOWN 3 UP  
**INSTANCES** 0 DOWN 0 UP  
**LICENSE** Smart Agent REGISTERED  
**INVENTORY** 1(1) Security Engine

Severity	Description	Cause	Occurrence
WARNING	Overall: CPU usage exceeded 90%	cpu-usage-high	2
INFO	[FSM:FAILED]: import configuration(FSM:sam:dme:MgmtImporterImport)	fsm-failed	1
CLEARED	ether port 1/7 on fabric interconnect A oper state: sfp-not-present	configuration-applying	1
CLEARED	ether port 1/8 on fabric interconnect A oper state: sfp-not-present	configuration-applying	1
CLEARED	ether port 1/4 on fabric interconnect A oper state: sfp-not-present	configuration-applying	1

3 Successful Login in last 24 hrs - View Details | Tue Jul 18 2023 at 18:34:36 from - 10.152.202.111

Um Validierungen von FXOS-Upgrades über die CLI durchzuführen, gehen Sie wie folgt vor:

- I. Erstellen Sie eine SSH-Sitzung mit der Management-IP des Chassis.
- II. Verwenden Sie den Befehl **show version**, um die aktuelle Version auf Ihrem Chassis zu überprüfen.
- III. Überprüfen Sie den Betriebszustand der Steckplätze am Chassis:
  - A. Wechseln Sie mit dem Befehl **scope ssa** zum ssa-Bereich.
  - B. Überprüfen Sie den aktuellen Status der Steckplätze mit dem Befehl **steckplatz anzeigen**.
- IV. Sie können den Befehl **show app-instance** verwenden, um den Status des logischen Geräts nach dem Upgrade zu überprüfen.

Beispiel für die vorgeschlagenen Verfahren:

```

B-09-FPR4125-NGFW-K9-18# scope ssa
B-09-FPR4125-NGFW-K9-18 /ssa # show slot
slot:
  Slot ID      Log Level Admin State Oper State
  -----
  1            Info      Ok          Online
B-09-FPR4125-NGFW-K9-18 /ssa # show app-instance
App Name      Identifier Slot ID      Admin State Oper State      Running Version Startup Version Deploy Type Turbo Mode Profile
  -----
ftd           FTD          1              Enabled      Online          7.2.4.165      7.2.4.165      Native      No
B-09-FPR4125-NGFW-K9-18 /ssa #

```



## 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.