

# Upgrade des aktiven/Standby-ASA-Failover-Paars für die sichere Firewall

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfen der Voraussetzungen](#)

[Upgrade über die Kommandozeile](#)

[Upgrade mit ASDM](#)

[Überprüfung](#)

[Über CLI](#)

[Über ASDM](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie Sie ASA für Failover-Bereitstellungen für die sichere Firewall 1000, 2100 im Appliance-Modus und die sichere Firewall 3100/4200 aktualisieren.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall Threat Defense:
- Konfiguration der Cisco Adaptive Security Appliance (ASA).

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Softwareversionen:

- Cisco Adaptive Security Appliance Software Version 9.14(4)
- Cisco Adaptive Security Appliance Software Version 9.16(4)

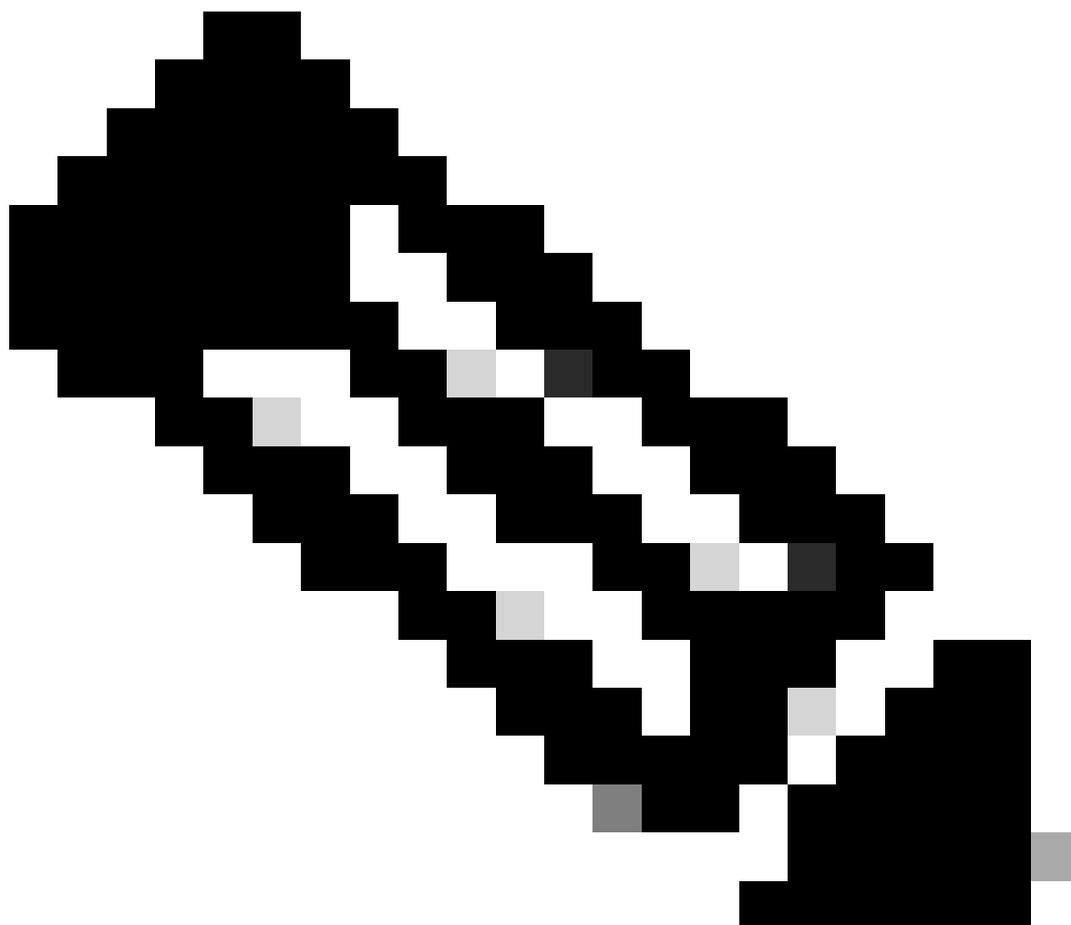
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

# Konfigurieren

## Überprüfen der Voraussetzungen

Schritt 1: Führen Sie den Befehl `show fxos mode` aus, um zu überprüfen, ob sich das Gerät im Appliance-Modus befindet.

---



Hinweis: Für die sichere Firewall 21XX In Version 9.13 und früheren Versionen wird nur der Plattformmodus unterstützt. In Version 9.14 und höher ist der Appliance-Modus der Standard.

---

```
<#root>
```

```
ciscoasa#
```

```
show fxos mode
```

```
Mode is currently set to appliance
```

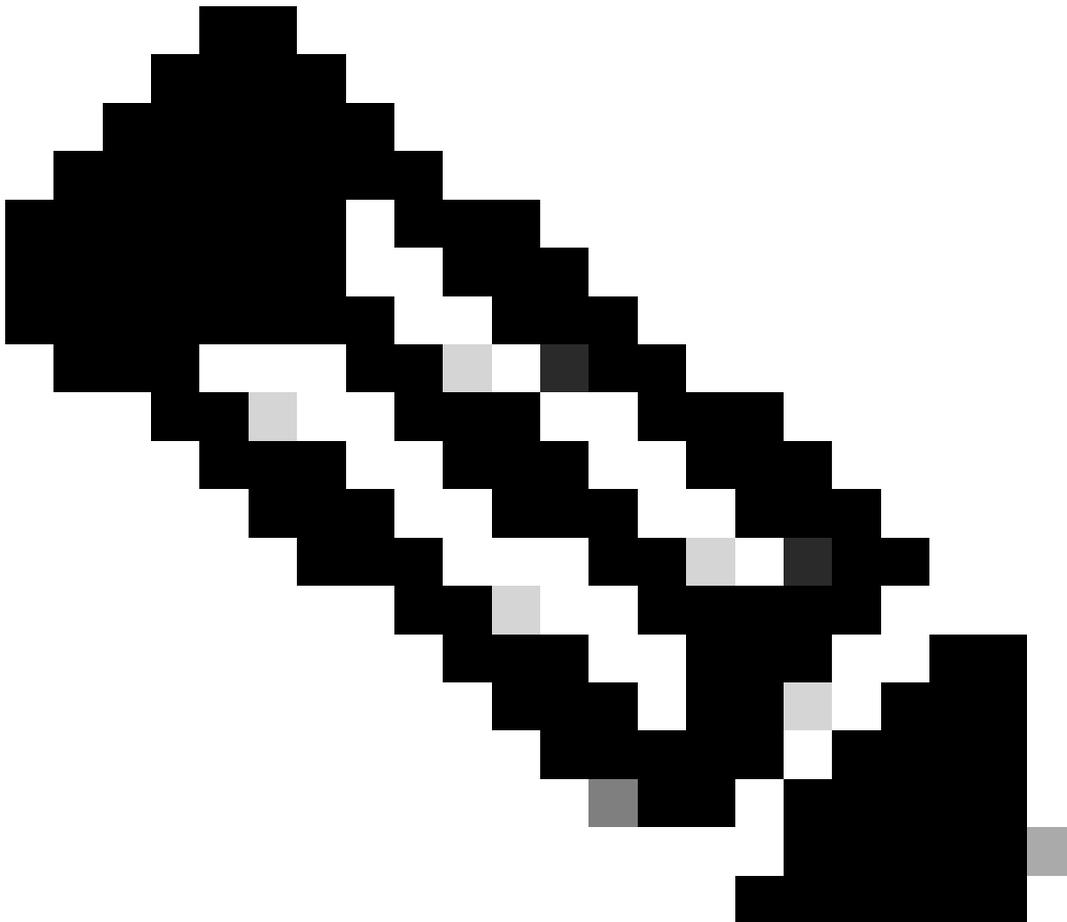
## Schritt 2: Überprüfen der Kompatibilität

Lesen Sie das Dokument zur ASA-Kompatibilität der Cisco Secure Firewall, um die Kompatibilität zwischen der FTD-Hardwareplattform und der ASA-Software der Secure Firewall zu überprüfen. Siehe

[Cisco Secure Firewall ASA-Kompatibilität](#)

Schritt 3: Laden Sie das Upgrade-Paket von [Cisco Software Central herunter](#).

---



Hinweis: Für die sichere Firewall 1000/2100 und die sichere Firewall 3100/4200 können Sie ASA oder FXOS nicht separat installieren; beide Images sind Teil eines Pakets.

---

Im entsprechenden Titel erfahren Sie mehr über die ASA- und FXOS-Versionen, die Teil des Pakets sind. Siehe [Secure Firewall 1000/2100 und 3100/4200 ASA und FXOS-Paketversionen](#) .

Upgrade über die Kommandozeile

Schritt 1: ASDM-Image zurücksetzen.

Stellen Sie im globalen Konfigurationsmodus eine Verbindung zur primären Einheit her, und führen Sie die folgenden Befehle aus:

```
<#root>
```

```
ciscoasa(config)#
```

```
asdm image disk0:/asdm.bin
```

```
ciscoasa(config)# exit
```

```
ciscoasa#
```

```
copy running-config startup-config
```

```
Source filename [running-config]?
```

```
Cryptochecksum: 6beb01d1 b7a3c30f 5e8eb557 a8ebb8ca
```

```
12067 bytes copied in 3.780 secs (4022 bytes/sec)
```

Schritt 2: Laden Sie das Software-Image auf die primäre Einheit hoch.



```
Writing file disk0:/cisco-asa-fp2k.9.16.4.SPA...
474475840 bytes copied in 843.230 secs (562842 bytes/sec)
```

Schritt 3: Laden Sie das Software-Image auf die sekundäre Einheit hoch.

Führen Sie den Befehl auf der primären Einheit aus.

```
<#root>
```

```
ciscoasa#
```

```
failover exec mate copy /noconfirm ftp://calo:calo@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA disk0:/cisco-asa
```

```
Accessing ftp://calo :<password>@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying file disk0:/cisco-asa-fp2k.9.16.4.SPA...
```

```
Writing file disk0:/cisco-asa-fp2k.9.16.4.SPA...
474475840 bytes copied in 843.230 secs (562842 bytes/sec)
```

Schritt 4: Überprüfen Sie, ob mit dem `show running-config boot system` Befehl ein aktuelles Boot-Image konfiguriert wurde.



**Hinweis:** Möglicherweise haben Sie kein Bootsystem konfiguriert.

---

<#root>

ciscoasa(config)#

show running-config boot system

```
boot system disk0:/cisco-asa-fp2k.9.14.4.SPA
```

**Schritt 5 (optional).** Falls Sie ein Boot-Image konfiguriert haben, müssen Sie es entfernen.

**Keine Boot-System-Diskette:/asa\_image\_name**

**Beispiel:**

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp2k.9.14.4.SPA
```

**Schritt 6:** Wählen Sie das zu bootende Image aus.

```
<#root>
```

```
ciscoasa(config)#
```

```
boot system disk0:/cisco-asa-fp2k.9.16.4.SPA
```

The system is currently installed with security software package 9.14.4, which has:

- The platform version: 2.8.1.172
- The CSP (asa) version: 9.14.4

Preparing new image for install...

!!!!!!!!!!!!!!

Image download complete (Successful unpack the image).

Installation of version 9.16.4 will do the following:

- upgrade to the new platform version 2.10.1.217
- upgrade to the CSP ASA version 9.16.4

After installation is complete, ensure to do write memory and reload to save this config and apply the  
Finalizing image install process...

Install\_status: ready.....

Install\_status: validating-images....

Install\_status: upgrading-npu

Install\_status: upgrading-system.

Install\_status: update-software-pack-completed

**Schritt 7. Speichern Sie die Konfiguration mit dem Befehl `copy running-config startup-config`.**

**Schritt 8:** Laden Sie die Sekundäreinheit neu, um die neue Version zu installieren.

```
<#root>
```

```
ciscoasa(config)#
```

```
failover reload-standby
```

Warten Sie, bis die Sekundäreinheit geladen ist.

**Schritt 9.** Sobald das Standby-Gerät neu geladen wurde, ändern Sie den Status des primären Geräts vom aktiven in den Standby-Status.

```
<#root>
```

```
ciscoasa#
```

```
no failover active
```

**Schritt 10.** Laden Sie das neue Standby-Gerät neu, um die neue Version zu installieren. Sie müssen eine Verbindung mit der neuen aktiven Einheit herstellen.

```
<#root>
```

ciscoasa(config)#

failover reload-standby

Sobald das neue Standby-Gerät geladen wurde, ist das Upgrade abgeschlossen.

## Upgrade mit ASDM

**Schritt 1:** Mit ASDM an die Sekundäreinheit anschließen

The screenshot shows the Cisco ASDM interface for a Cisco ASA device. The main content area is divided into several sections:

- Device Information:** Host Name: ciscoasa, ASA Version: 7.8(1)152, Firewall Mode: Routed, Total Flash: Not Applicable, FIPS Mode: Appliance, Device Uptime: 0d 0h: 43m 12s, Device Type: FPR-2120, Context Mode: Single, Total Memory: 6588 MB.
- Interface Status:** A table showing interface management with IP Address/Mask 10.88.15.59/24, Line up, Link up, and 13bps.
- Failover Status:** This Host: SECONDARY (Standby Ready), Other Host: PRIMARY (Active).
- Traffic Status:** Two line graphs showing Connections Per Second Usage and Management Interface Traffic Usage (kbps).
- System Resources Status:** A bar chart showing Memory Usage (MB) over time.
- Latest ASDM Syslog Messages:** A section for viewing system logs.

At the bottom, there is a message: "ASDM logging is disabled. To enable ASDM logging with informational level, click the button below." with an "Enable Logging" button.

**Schritt 2:** Gehen Sie zu Extras > Software von Lokaler Computer aktualisieren.

Cisco ASDM 7.18(1)152 for ASA - 10.88.15.59

File View **Tools** Wizards Window Help

Home

Device List

Find: 10.88.15.53

- Command Line Interface...
- Show Commands Ignored by ASDM on Device
- Packet Tracer...
- Ping...
- Traceroute...
- File Management...
- Check for ASA/ASDM Updates...
- Upgrade Software from Local Computer...**
- Backup Configurations
- Restore Configurations
- System Reload...
- Administrator's Alert to Clientless SSL VPN Users...
- Migrate Network Object Group Members...
- Preferences...
- ASDM Java Console...

Back Forward Help

all Dashboard

Device Uptime: **0d 0h 44m**

Device Type: **FPR-2120**

Context Mode: **Single**

Total Memory: **6588 MB**

less SSL VPN: **0** AnyConnect Client(SSL,TLS,DTLS):

Total Memory Usage Total CPU Usage Core Usage Details

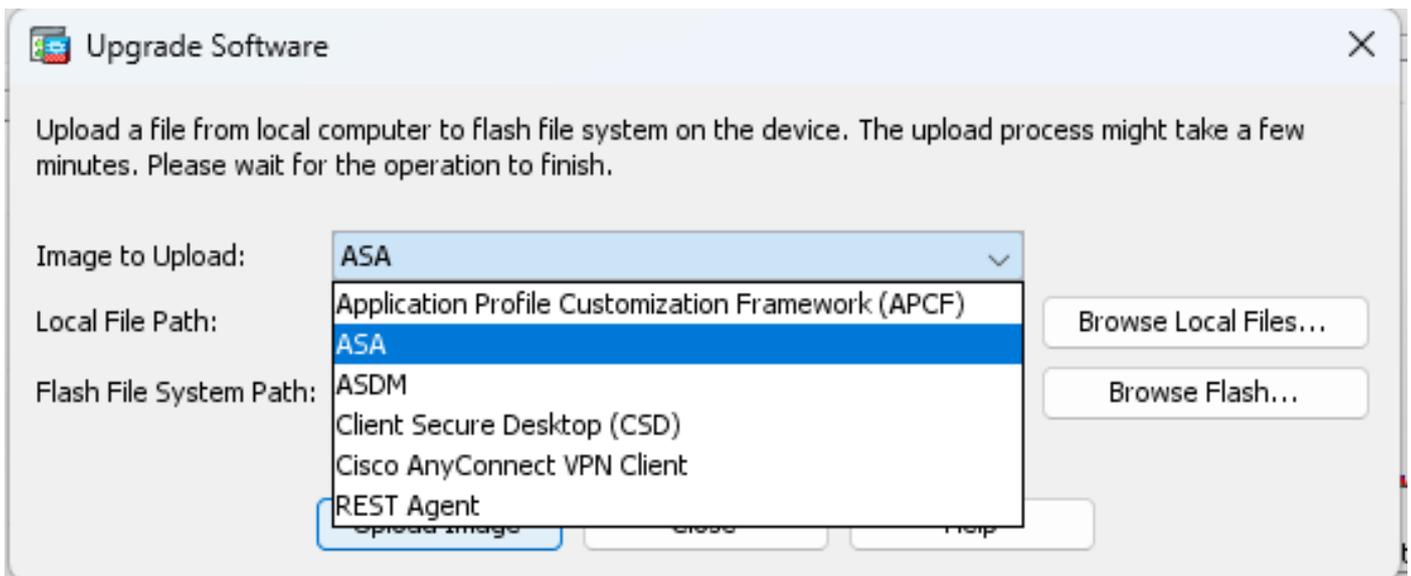
Memory Usage (MB)

Time	Memory Usage (MB)
22:59:53	965

Latest ASDM Syslog Messages

Device configuration loaded successfully.

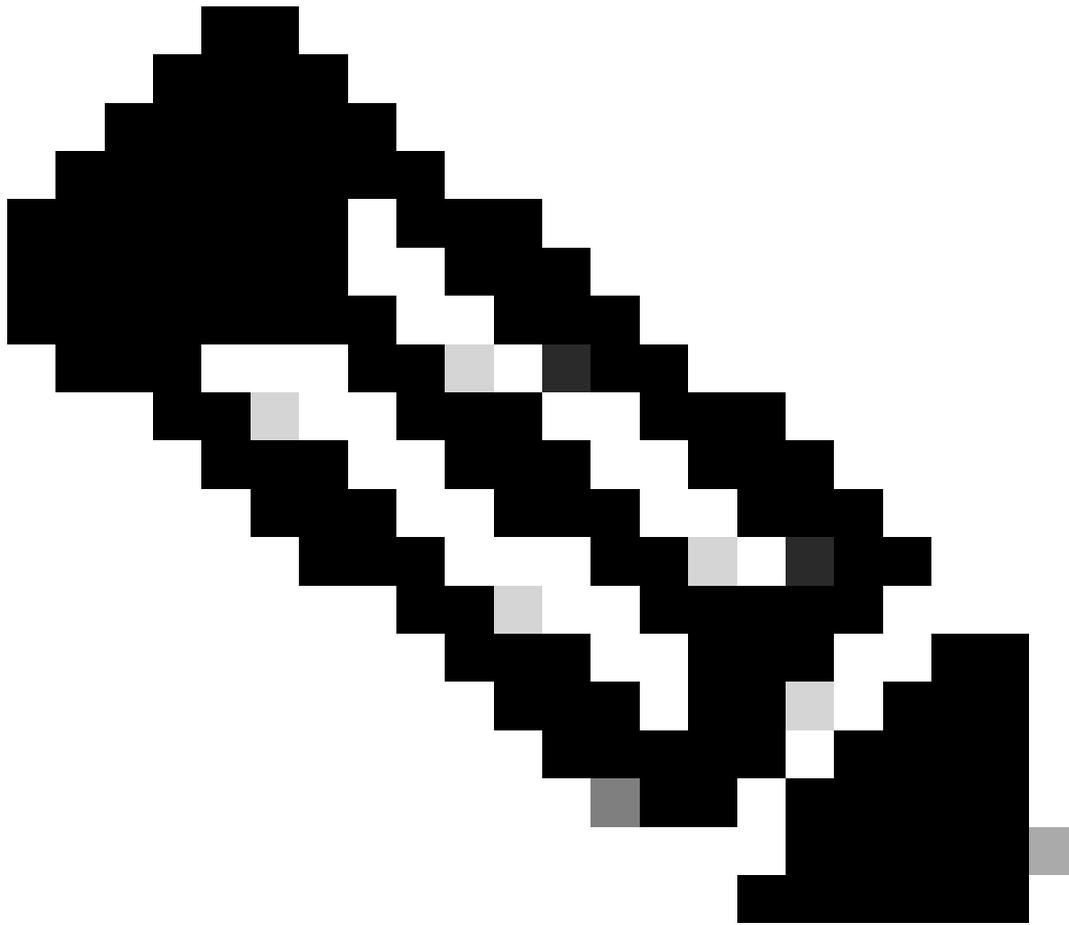
**Schritt 3:** Wählen Sie **ASA** aus der Dropdown-Liste aus.



**Schritt 4:** Klicken Sie im Fenster **Upgrade Software** (**Software** aktualisieren) auf **Browse Local Files** (**Lokale Dateien durchsuchen**), um das Software-Image auf die sekundäre Einheit hochzuladen.

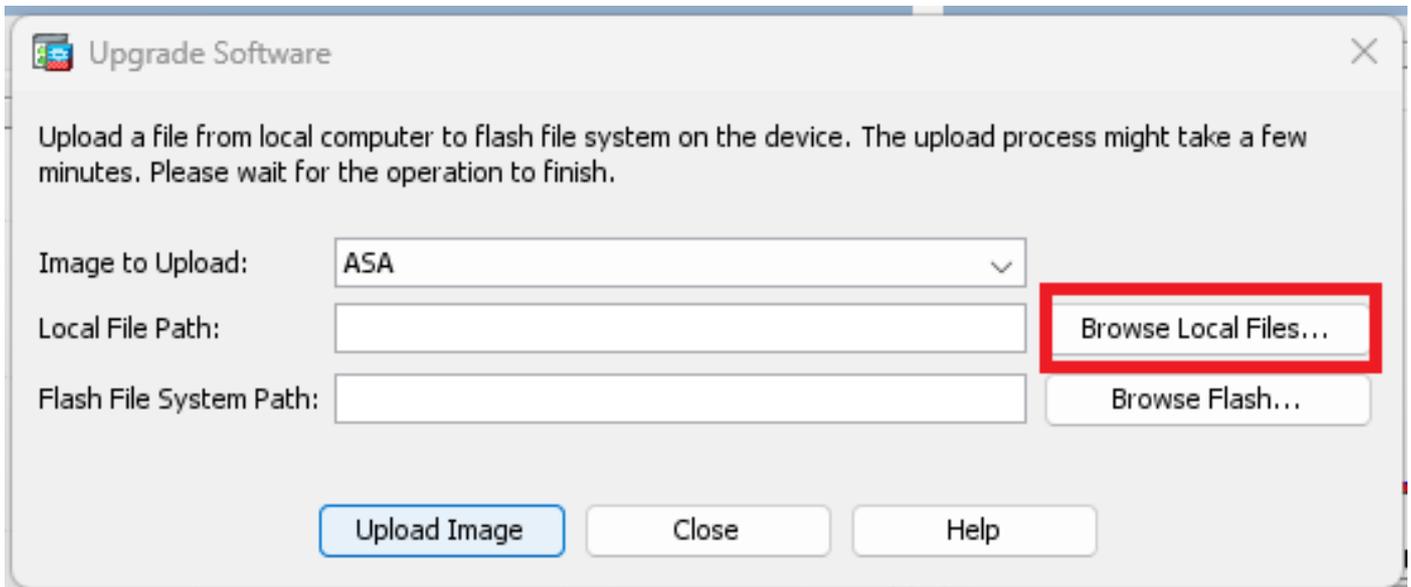
---

---

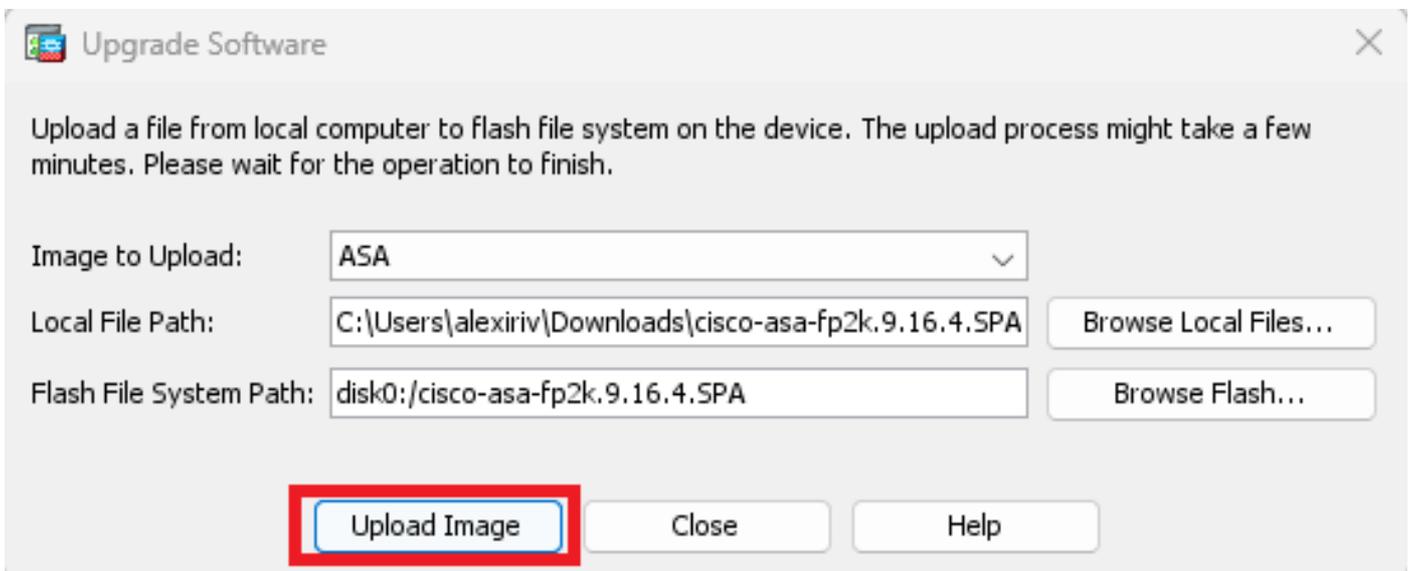


**Hinweis:** Standardmäßig ist der **Flash File System Path** disk0; um ihn zu ändern, klicken Sie auf **Flash durchsuchen** und wählen den neuen Pfad aus.

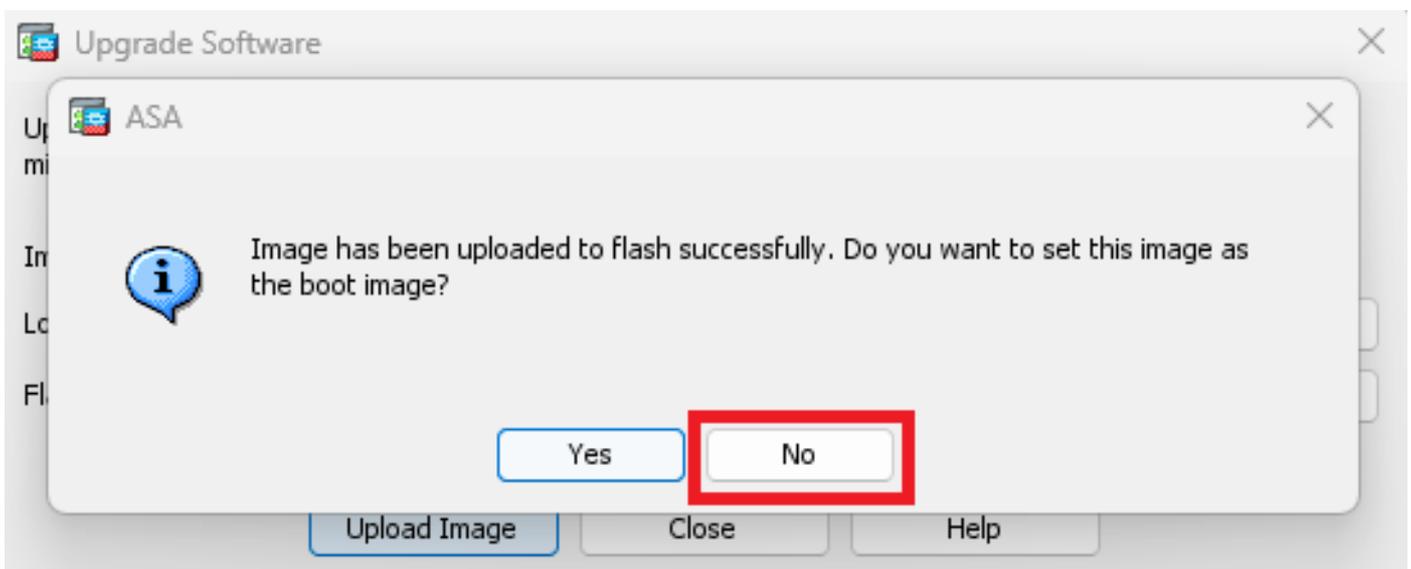
---



Klicken Sie auf **Bild hochladen**.



Wenn Sie das Bild hochgeladen haben, klicken Sie auf **Nein**.



**Schritt 5:** Setzen Sie das ASDM-Image zurück.

Stellen Sie mit ASDM eine Verbindung zur primären Einheit her, und gehen Sie zu **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration**.

Geben Sie in **ASDM Image File Path (ASDM-Image-Dateipfad)** den Wert **disk0:/asdm.bin** ein, und wenden Sie ihn an.

The screenshot shows the Cisco ASDM interface for ASA version 7.18(1)152. The breadcrumb navigation at the top indicates the current path: Configuration > Device Management > System Image/Configuration > Boot Image/Configuration. The left sidebar shows the 'Device Management' tree with 'System Image/Configuration' and 'Boot Image/Configuration' highlighted. The main content area displays the 'Boot Configuration' section, which includes a table for boot images and a text input field for the 'ASDM Image File Path'.

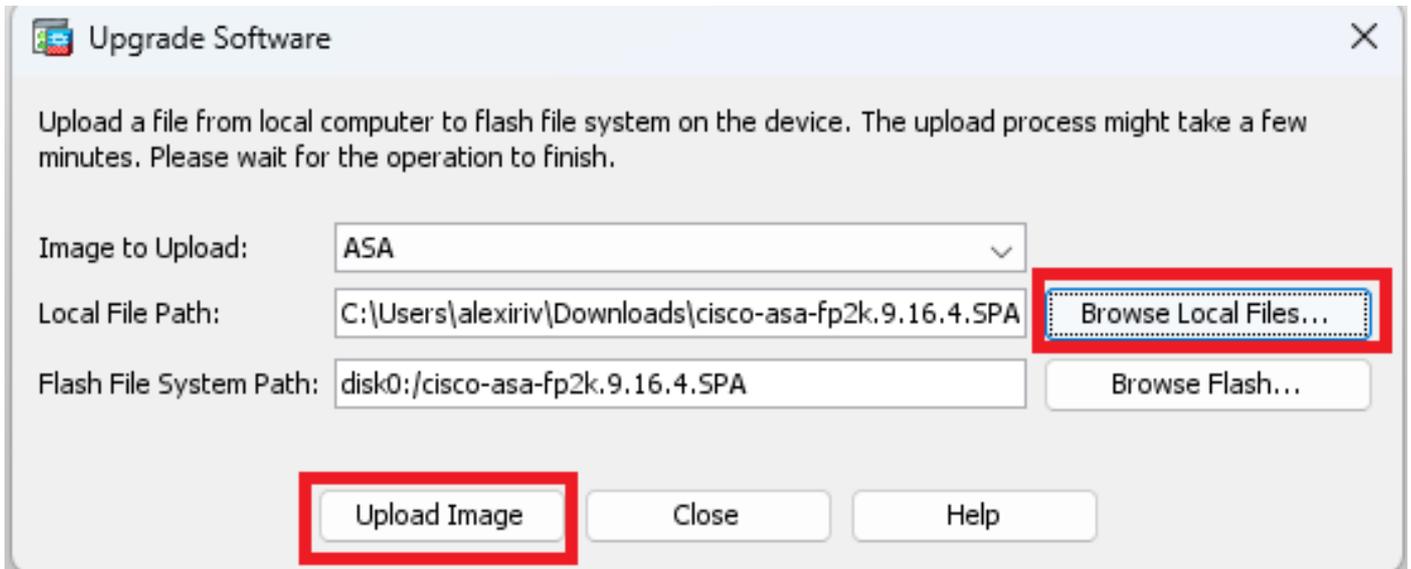
Boot Order	Boot Image Location
1	disk0:/cisco-asa-fp

ASDM Image File Path:

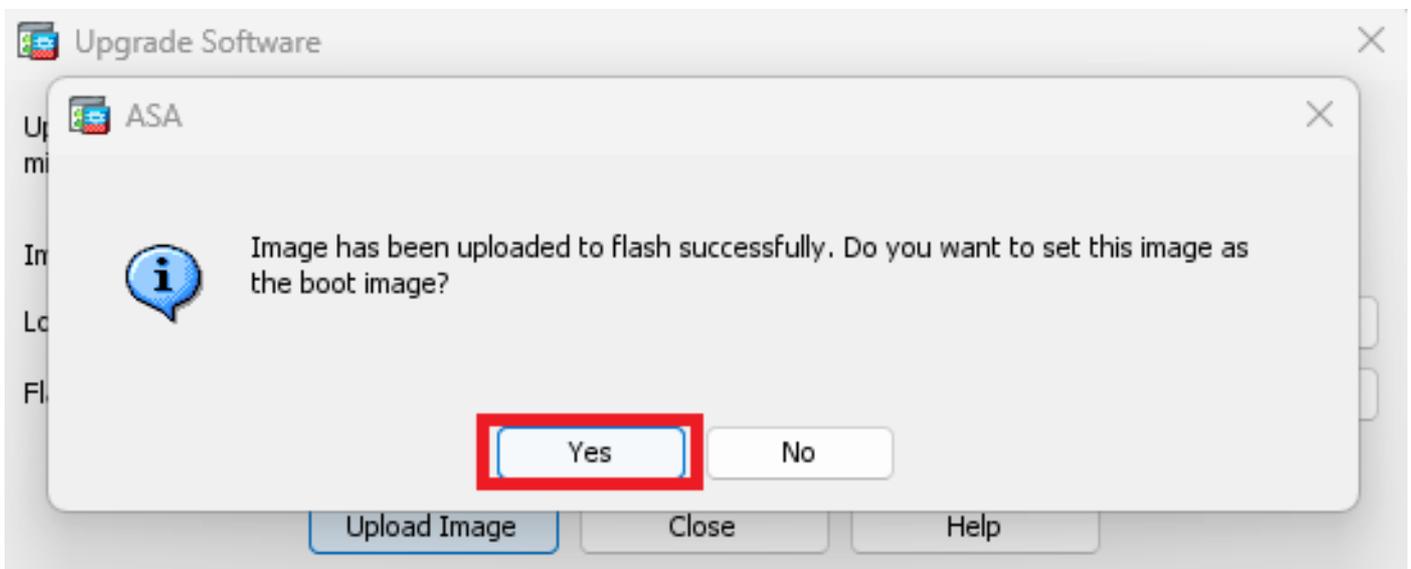
**Schritt 6:** Laden Sie das Software-Bild auf die primäre Einheit hoch.

Klicken Sie auf **Lokale Dateien durchsuchen**, und wählen Sie das Upgrade-Paket auf Ihrem Gerät aus.

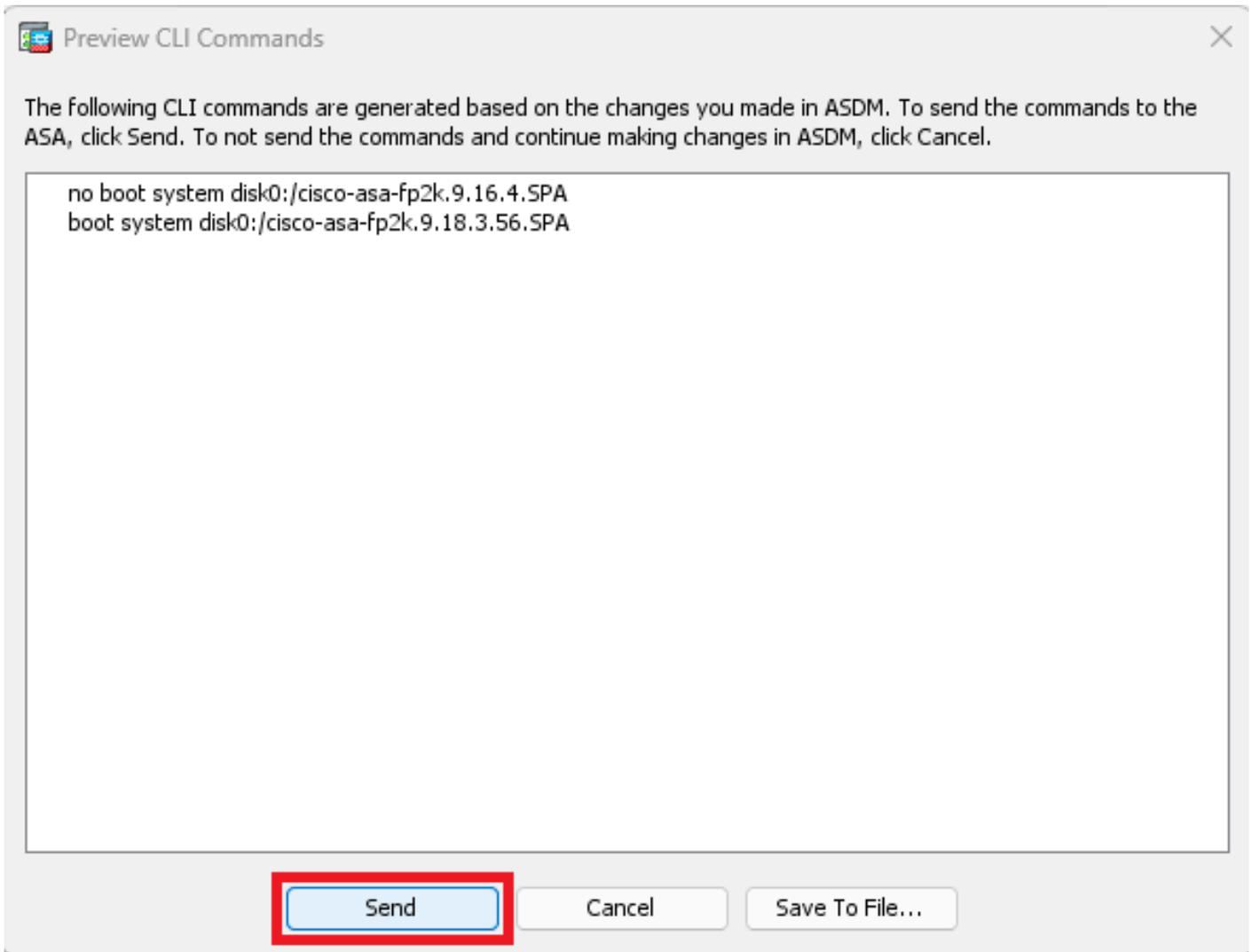
Klicken Sie auf **Bild hochladen**.



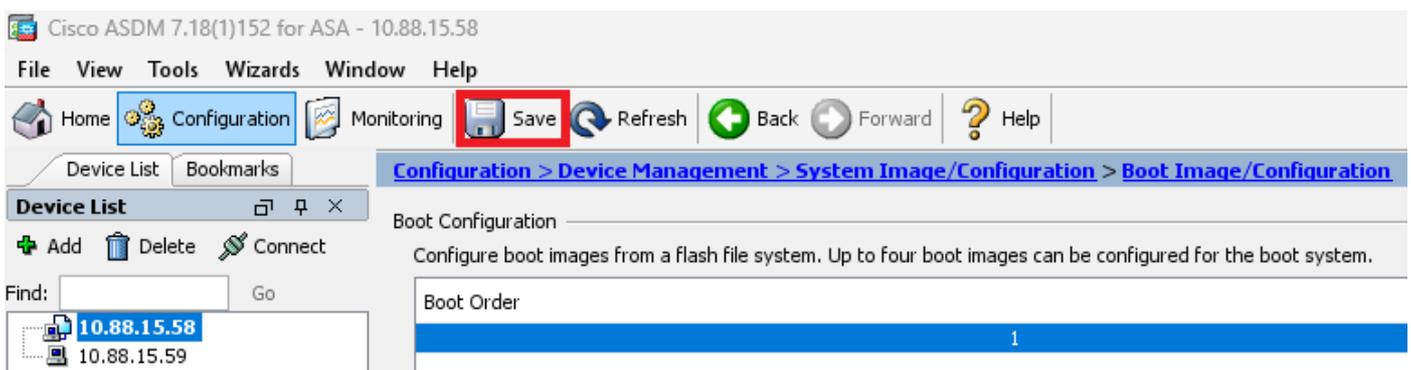
Klicken Sie nach dem Hochladen auf **Ja**.



Klicken Sie in den Vorschaufenstern auf die Schaltfläche **Senden**, um die Konfiguration zu speichern.



**Schritt 7.** Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.



**Schritt 8:** Laden Sie die Sekundäreinheit neu, um die neue Version zu installieren.

Gehen Sie zu Monitoring > **Properties** > **Failover** > **Status** und klicken Sie auf **Reload Standby (Standby neu laden)**.

Cisco ASDM 7.18(1)152 for ASA - 10.88.15.58

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List Bookmarks Monitoring > Properties > Failover > Status

Device List

Add Delete Connect

Find: 10.88.15.58 10.88.15.59 Go

Properties

- AAA Servers
- Device Access
- AAA Local Locked Out Users
- Authenticated Users
- ASDM/HTTPS/Telnet/SSH
- Connection Graphs
  - Perfmon
  - Xlates
- CRL
- DNS Cache
- Failover
  - Status**
  - History
  - Graphs
- Identity
  - AD Agent
  - Groups
  - Memory Usage
  - Users
- Identity by TrustSec
  - PAC
  - Environment Data
  - SXP Connections
  - IP Mappings
- IP Audit
- System Resources Graphs
  - Blocks
  - CPU
  - Memory
- WCCP

Interfaces

VPN

Routing

Properties

Logging

Failover state of the system:

```
Failover On
Failover unit Primary
Failover LAN Interface: folink Ethernet1/1 (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 1 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.16(4), Mate 9.16(4)
Serial Number: Ours JAD25430R73, Mate JAD25430RGG
Last Failover at: 22:45:48 UTC Jan 31 2024
This host: Primary - Active
Active time: 5781 (sec)
slot 0: FPR-2120 hw/sw rev (1.5/9.16(4)) status (Up_Sys)
```

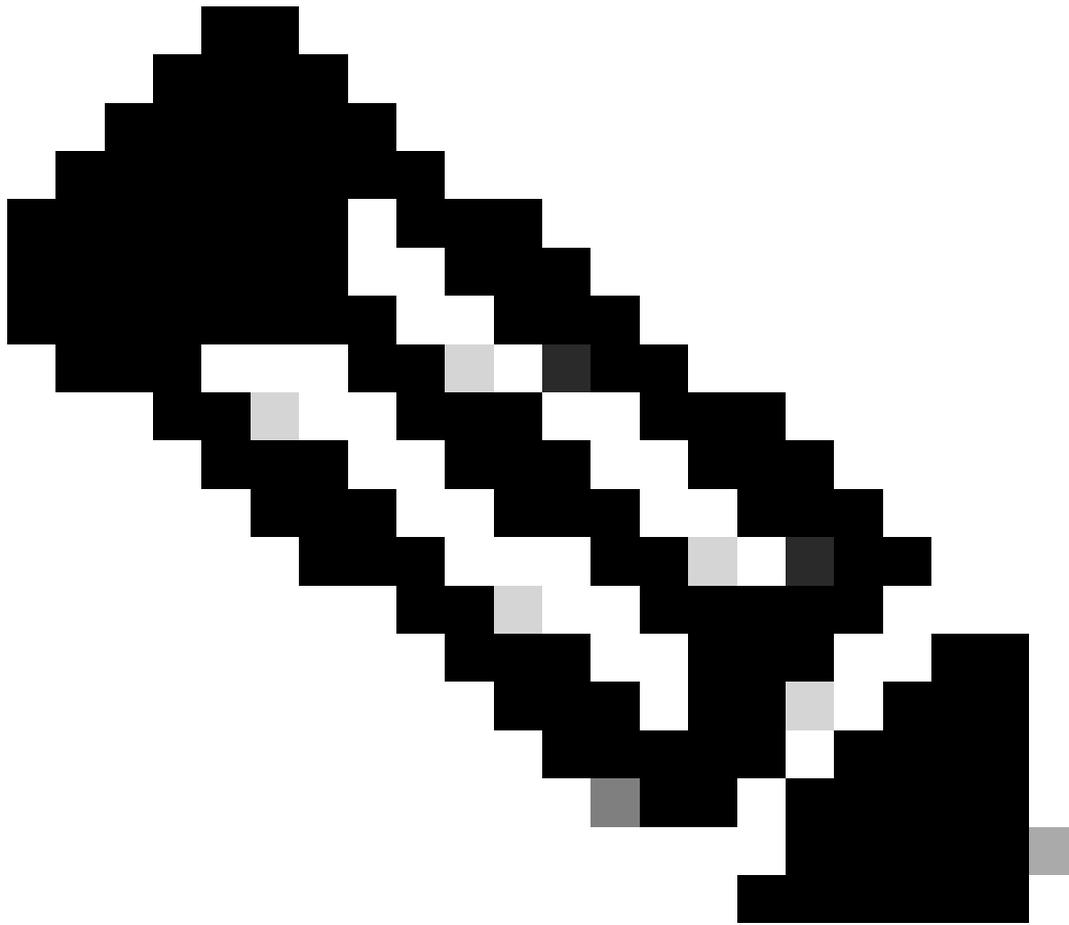
Make Active Make Standby Reset Failover **Reload Standby**

Refresh

Warten Sie, bis das Standby-Gerät geladen ist.

**Schritt 9.** Sobald das Standby-Gerät neu geladen wurde, ändern Sie den Status des primären Geräts in den Standby-Status.

Gehen Sie zu Monitoring > **Properties** > **Failover** > **Status** und klicken Sie auf **Make Standby (Standby machen)**.



**Hinweis:** ASMD stellt automatisch eine Verbindung zur neuen aktiven Einheit her.

---

Cisco ASDM 7.18(1)152 for ASA - 10.88.15.58

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List Bookmarks Monitoring > Properties > Failover > Status

Device List

Add Delete Connect

Find: 10.88.15.58 10.88.15.59

Properties

- AAA Servers
- Device Access
- AAA Local Locked Out Users
- Authenticated Users
- ASDM/HTTPS/Telnet/SSH
- Connection Graphs
  - Perfmon
  - Xlates
- CRL
- DNS Cache
- Failover
  - Status
  - History
  - Graphs
- Identity
  - AD Agent
  - Groups
  - Memory Usage
  - Users
- Identity by TrustSec
  - PAC
  - Environment Data
  - SXP Connections
  - IP Mappings
- IP Audit
- System Resources Graphs
  - Blocks
  - CPU
  - Memory
- WCCP

Interfaces

VPN

Routing

Properties

Logging

Failover state of the system:

```
Failover On
Failover unit Primary
Failover LAN Interface: folink Ethernet1/1 (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 1 of 128 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.16(4), Mate 9.16(4)
Serial Number: Ours JAD25430R73, Mate JAD25430RCG
Last Failover at: 22:45:48 UTC Jan 31 2024
This host: Primary - Active
Active time: 5781 (sec)
slot 0: FPR-2120 hw/sw rev (1.5/9.16(4)) status (Up_Sys)
```

Make Active **Make Standby** Reset Failover Reload Standby

Refresh

**Schritt 10.** Laden Sie das neue Standby-Gerät neu, um die neue Version zu installieren.

Gehen Sie zu Monitoring > Properties > Failover > Status und klicken Sie auf **Reload Standby (Standby neu laden)**.

Cisco ASDM 7.18(1)152 for ASA - 10.88.15.58

File View Tools Wizards Window Help

Home Configuration **Monitoring** Save Refresh Back Forward Help

Device List Bookmarks **Monitoring > Properties > Failover > Status**

**Device List**

Find: 10.88.15.58 10.88.15.59

**Properties**

- AAA Servers
- Device Access
  - AAA Local Locked Out Us
  - Authenticated Users
  - ASDM/HTTPS/Telnet/SSH
- Connection Graphs
  - Perfmon
  - Xlates
  - CRL
  - DNS Cache
- Failover**
  - Status**
  - History
  - Graphs
- Identity
  - AD Agent
  - Groups
  - Memory Usage
  - Users
- Identity by TrustSec
  - PAC
  - Environment Data
  - SXP Connections
  - IP Mappings
- IP Audit
- System Resources Graphs
  - Blocks
  - CPU
  - Memory
- WCCP

Interfaces

VPN

Routing

**Properties**

Logging

Failover state of the system:

```

Failover On
Failover unit Secondary
Failover LAN Interface: foLink Ethernet1/1 (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 1 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.18(3)56, Mate 9.16(4)
Serial Number: Ours JAD25430RCG, Mate JAD25430R73
Last Failover at: 00:53:34 UTC Feb 1 2024
This host: Secondary - Active
Active time: 3 (sec)
slot 0: FPR-2120 hw/sw rev (1.5/9.18(3)56) status (Up Sys)
  
```

Make Active Make Standby Reset Failover Reload Standby

Refresh

Sobald das neue Standby-Gerät geladen wurde, ist das Upgrade abgeschlossen.

## Überprüfung

Um zu überprüfen, ob das Upgrade auf beiden Geräten abgeschlossen wurde, überprüfen Sie das Upgrade über die CLI und ASDM.

### Über CLI

```
<#root>
```

```
ciscoasa#
```

show failover

Failover On  
Failover unit Primary  
Failover LAN Interface: folink Ethernet1/1 (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 1 of 1292 maximum  
MAC Address Move Notification Interval not set

Version: Ours 9.16(4), Mate 9.16(4)

Serial Number: Ours JAD25430R73, Mate JAD25430RCG  
Last Failover at: 22:45:48 UTC Jan 31 2024  
This host: Primary - Active  
Active time: 45 (sec)  
slot 0: FPR-2120 hw/sw rev (1.5/9.16(4)) status (Up Sys)  
Interface management (10.88.15.58): Normal (Monitored)  
Other host: Secondary - Standby Ready  
Active time: 909 (sec)  
slot 0: FPR-2120 hw/sw rev (1.5/9.16(4)) status (Up Sys)  
Interface management (10.88.15.59): Normal (Monitored)

Stateful Failover Logical Update Statistics

Link : folink Ethernet1/1 (up)  
Stateful Obj xmit xerr rcv rerr  
General 27 0 29 0  
sys cmd 27 0 27 0  
up time 0 0 0 0  
RPC services 0 0 0 0  
TCP conn 0 0 0 0  
UDP conn 0 0 0 0  
ARP tbl 0 0 1 0  
Xlate\_Timeout 0 0 0 0  
IPv6 ND tbl 0 0 0 0  
VPN IKEv1 SA 0 0 0 0  
VPN IKEv1 P2 0 0 0 0  
VPN IKEv2 SA 0 0 0 0  
VPN IKEv2 P2 0 0 0 0  
VPN CTCP upd 0 0 0 0  
VPN SDI upd 0 0 0 0  
VPN DHCP upd 0 0 0 0  
SIP Session 0 0 0 0  
SIP Tx 0 0 0 0  
SIP Pinhole 0 0 0 0  
Route Session 0 0 0 0  
Router ID 0 0 0 0

User-Identity 0 0 1 0  
CTS SGTNAME 0 0 0 0  
CTS PAC 0 0 0 0  
TrustSec-SXP 0 0 0 0  
IPv6 Route 0 0 0 0  
STS Table 0 0 0 0  
Umbrella Device-ID 0 0 0 0

### Logical Update Queue Information

Cur Max Total  
Recv Q: 0 10 160  
Xmit Q: 0 1 53

## Über ASDM

Gehen Sie zu **Monitoring > Properties > Failover > Status**, hier wird die ASA-Version für beide Geräte angezeigt.

The screenshot shows the Cisco ASDM interface for ASA 10.88.15.58. The breadcrumb navigation is **Monitoring > Properties > Failover > Status**. The left sidebar shows the 'Properties' tree with 'Failover' > 'Status' selected. The main content area displays the following failover state information:

```
Failover state of the system:

Failover On
Failover unit Primary
Failover LAN Interface: folink Ethernet1/1 (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 1 of 1292 maximum
MAC Address Move Notification Interval not set
Version: Curs 9.16(4), Mate 9.16(4)
Serial Number: Curs JAD26430R73, Mate JAD26430RCC
Last Failover at: 22:45:48 UTC Jan 31 2024
  This host: Primary - Active
    Active time: 5781 (sec)
    slot 0: FPR-2120 hw/sw rev (1.5/9.16(4)) status (Up Sys)
```

Below the text are four buttons: **Make Active**, **Make Standby**, **Reset Failover**, and **Reload Standby**. A **Refresh** button is located at the bottom center of the main content area.

## Zugehörige Informationen

- 

[Cisco Secure Firewall ASA-Kompatibilität](#)

- 

[Cisco Secure Firewall ASA Upgrade-Leitfaden](#)

## 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.