

# Kennwortwiederherstellung für SFTD/ASA-Instanz über FXOS-CLI

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Vorgehensweise](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie Sie das Kennwort für eine SFTD- oder ASA-Instanz über die FXOS-CLI wiederherstellen.

## Voraussetzungen

### Anforderungen

SFTD- oder ASA-Instanzen über die Secure Firewall-Serie FP41XX oder FP93XX.

Cisco empfiehlt, dass Sie über Kenntnisse in diesem Thema verfügen:

- Cisco FirePOWER Extensible Operating System (FXOS) Command Line Interface (CLI)

### Verwendete Komponenten

- Sichere Cisco Firewall 4110
- Cisco Secure Firewall ASA

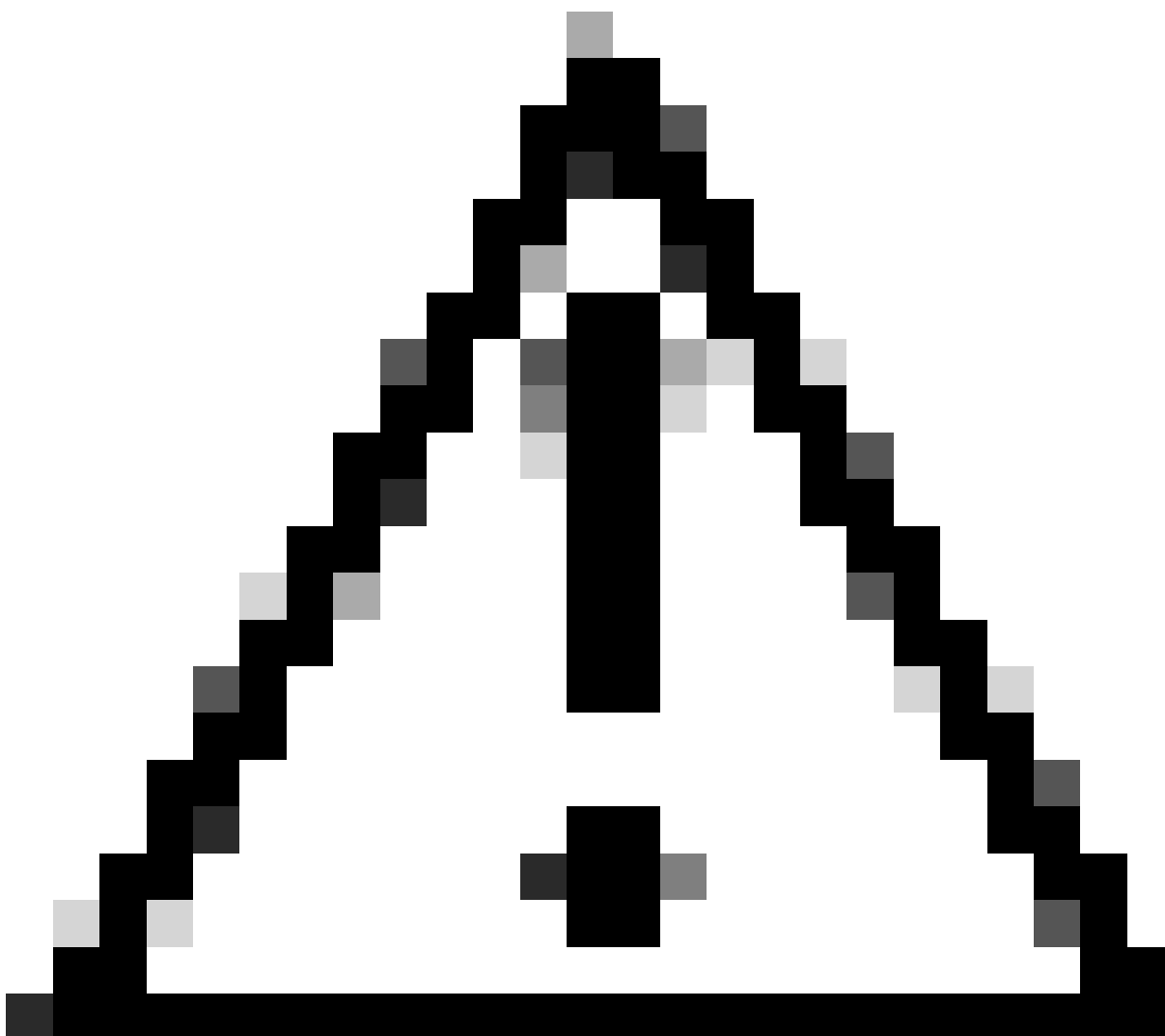
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

## Hintergrundinformationen

Es gibt Szenarien, in denen das Kennwort für ein Gerät verloren geht und wiederhergestellt werden muss, und die Verwendung des FXOS-FirePOWER-Chassis-Managers ist keine Option. Bei SFTD- oder ASA-Instanzen über die Secure Firewall-Serie FP41XX oder FP93XX kann die

Kennwortwiederherstellung über die FXOS-CLI erfolgen.

---



Achtung: Dieser Prozess erfordert einen Neustart der Instanz, was zu einem Ausfall des Datenverkehrs führen kann.

---

## Konfigurieren

### Vorgehensweise

Schritt 1: Melden Sie sich mit den Anmeldeinformationen für die Administratorrechte bei der FXOS-CLI an.

Schritt 2: Rufen Sie die Informationen zu Anwendungsname, Kennung und Steckplatz-ID ab.

Scopessa

App-Instanz anzeigen

Beispiel:

<#root>

```
FPR4110-K9-1# scope ssa
FPR4110-K9-1 /ssa # show app-instance
```

```
App Name Identifier Slot ID
```

```
Admin State Oper State   Running Version Startup Version Deploy Type Turbo Mode Profile Name Cluster St
-----
asa          ASA          1
Enabled      Online      9.16.3(14)   9.16.3(14)   Native      No          Not Appl
```

Schritt 3: Geben Sie das neue Admin- und Aktivierungskennwort ein, und speichern Sie die Änderungen.

Bereichskennung für logisches Gerät

```
scope mgmt-bootstrap app_name
```

```
scope bootstrap-key-secret PASSWORD
```

Sollwert

Geben Sie einen Wert ein: password

Bestätigen Sie den Wert: password

Commit-Puffer

beenden

beenden

Beispiel:

```
FPR4110-K9-1 /ssa # scope logical-device ASA
FPR4110-K9-1 /ssa/logical-device # scope mgmt-bootstrap asa
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap # scope bootstrap-key-secret PASSWORD
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret # set value
```

Enter value:

Confirm the value:

Warning: Bootstrap changes are not automatically applied to app-instances. To apply the changes, please

```
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* #commit-buffer
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret # exit
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap # exit
```

Schritt 4: Löschen Sie den Management-Bootstrap, und speichern Sie die Änderungen.

Scope-Steckplatz\_ID

Bereichsinstanz app\_name bezeichner

Clear-Mgmt-Bootstrap

Commit-Puffer

Beispiel:

```
FPR4110-K9-1 /ssa # scope slot 1
```

```
FPR4110-K9-1 /ssa/slot # scope app-instance asa ASA
```

```
FPR4110-K9-1 /ssa/slot/app-instance # clear-mgmt-bootstrap
```

```
Warning: Clears the application management bootstrap. Application needs to be restarted for this action
```

```
FPR4110-K9-1 /ssa/slot/app-instance* # commit-buffer
```

Schritt 5: Starten Sie die Instanz neu.

Neustart

Commit-Puffer

Beispiel:

```
FPR4110-K9-1 /ssa/slot/app-instance # restart
```

```
FPR4110-K9-1 /ssa/slot/app-instance* # commit-buffer
```



Hinweis: Die Instanz wird neu gestartet, sobald die Änderungen gespeichert wurden.

---

Schritt 6: Melden Sie sich mit den neuen Anmeldeinformationen über SSH bei der SFTD/ASA-Instanz an.

## 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.