

Konfigurieren mehrerer Instanzen in der Secure Firewall der Serie 3100

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration für Version 7.4.1+](#)

Einleitung

In diesem Dokument wird die Konfiguration von Multi-Instant in der Secure Firewall der Serie 3100 mit Version 7.4+ beschrieben.

Voraussetzungen

Kenntnisse der grafischen Benutzeroberfläche (GUI) von Firewall eXtensible Operating System (FXOS) und Firewall Management Center (FMC)

Anforderungen

Zugriff auf:

- Konsolenzugriff auf die sichere Firewall der Serie 3100
- FMC-GUI-Zugriff

Verwendete Komponenten

- Cisco Secure Firewall Management Center mit mehr als 7.4
- Cisco Secure Firewall der Serie 3100
 - Ausgenommen 3105*

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

Im Multi-Instance-Modus können Sie mehrere Container-Instanzen auf einem einzigen Chassis

bereitstellen, die als vollständig unabhängige Geräte fungieren.

Konfiguration für Version 7.4.1+

Schritt 1: Verbindung zum Konsolenport des Chassis

Der Konsolen-Port wird mit der FXOS-CLI verbunden.

Schritt 2: Melden Sie sich mit dem Benutzernamen admin und dem Kennwort admin123 an.

Sie werden aufgefordert, das Kennwort zu ändern, wenn Sie sich das erste Mal bei FXOS anmelden.

 Hinweis: Wenn das Kennwort bereits geändert wurde und Sie es nicht kennen, müssen Sie ein neues Image auf dem Gerät erstellen, um das Kennwort auf den Standardwert zurückzusetzen. Informationen [zum Bildverfahren](#) finden Sie [im](#) [FXOS-Fehlerbehebungshandbuch](#).

Schritt 3: Überprüfen Sie Ihren aktuellen Modus, Nativ oder Container. Wenn der Modus Nativ ist, können Sie mit dieser Prozedur fortfahren, um in den Multi-Instance (Container)-Modus zu konvertieren.

firepower# Systemdetails anzeigen

Beispiel:

```
firepower# show system detail
```

```
Systems:
```

```
  Name: firepower
```

```
  Mode: Stand Alone
```

```
  System IP Address: 0.0.0.0
```

```
  System IPv6 Address: ::
```

```
  System Owner:
```

```
  System Site:
```

```
  Deploy Mode: Native
```

```
  Description for System:
```

Mehrinstanzstatus anzeigen

Schritt 4: Stellen Sie eine Verbindung zur Threat Defence-CLI her.

```
firepower# connect ftd
```

Beispiel:

```
firepower# connect ftd  
>
```

Anschluss an FTD

Schritt 5: Wenn Sie sich das erste Mal beim Schutz vor Bedrohungen anmelden, werden Sie aufgefordert, die Endbenutzer-Lizenzvereinbarung (EULA) zu akzeptieren. Anschließend wird das CLI-Setup-Skript angezeigt.

Mit dem Setup-Skript können Sie die IP-Adresse der Management-Schnittstelle und andere Einstellungen festlegen. Wenn Sie jedoch in den Multi-Instance-Modus konvertieren, werden nur die folgenden Einstellungen beibehalten.

- Administratorkennwort (das Sie bei der erstmaligen Anmeldung festgelegt haben)
- DNS-Server
- Domänen durchsuchen

Sie setzen die Management-IP-Adresse und das Gateway als Teil des Befehls für den Multi-Instance-Modus zurück. Nach der Konvertierung in den Multi-Instance-Modus können Sie die Management-Einstellungen in der FXOS-CLI ändern. [Siehe Ändern der Chassis-Verwaltungseinstellungen in der FXOS-CLI.](#)

Schritt 6: Aktivieren Sie den Multi-Instance-Modus, legen Sie die Schnittstelleneinstellungen für das Chassis-Management fest, und identifizieren Sie das Management Center. Sie können IPv4 und/oder IPv6 verwenden. Nachdem Sie den Befehl eingegeben haben, werden Sie aufgefordert, die Konfiguration zu löschen und einen Neustart durchzuführen. Geben Sie ERASE (alle Großbuchstaben) ein. Das System wird neu gestartet, und beim Ändern des Modus wird die Konfiguration mit Ausnahme der Management-Netzwerkeinstellungen, die Sie im Befehl und im Admin-Kennwort festgelegt haben, gelöscht. Der Chassis-Hostname ist auf "firepower-model" festgelegt.

IPv4:

konfigurieren Sie das Netzwerk mit mehreren Instanzen

```
ipv4ip_addressNetzwerk_maskgateway_ip_addressManager_name {hostname | IPv4-Adresse | DONTRESOLVE} registration_keynat_id
```

IPv6:

konfigurieren Sie das Netzwerk mit mehreren Instanzen

```
ipv6ipv6_addressPräfix_lengthGateway_ip_addressManager_name {hostname | IPv6-Adresse | DONTRESOLVE} registration_keynat_id
```

Siehe folgende Managerkomponenten:

- {hostname | IPv4-Adresse | DONTRESOLVE} - Gibt entweder den FQDN oder die IP-Adresse des Management Centers an. Mindestens eines der Geräte, entweder das Management-Center oder das Chassis, muss über eine erreichbare IP-Adresse verfügen, um den bidirektionalen, SSL-verschlüsselten Kommunikationskanal zwischen den beiden Geräten einzurichten. Wenn Sie in diesem Befehl keinen Manager-Hostnamen oder keine IP-Adresse angeben, geben Sie DONTRESOLVE ein. In diesem Fall muss das Chassis eine erreichbare IP-Adresse oder einen erreichbaren Hostnamen aufweisen, und Sie müssen thenat_id angeben.
- registration_key: Geben Sie einen einmaligen Registrierungsschlüssel Ihrer Wahl ein, den Sie bei der Registrierung des Chassis auch in Management Center angeben. Der Registrierungsschlüssel darf maximal 37 Zeichen lang sein. Gültige Zeichen sind alphanumerische Zeichen (A-Z, a-z, 0-9) und Bindestrich (-).
- nat_id - Gibt eine eindeutige, einmalige Zeichenfolge Ihrer Wahl an, die Sie auch im

Management-Center angeben, wenn Sie das Chassis registrieren, wenn eine Seite keine erreichbare IP-Adresse oder keinen Hostnamen angibt. Sie ist erforderlich, wenn Sie keine Manager-Adresse oder keinen Hostnamen angeben. Wir empfehlen jedoch, dass Sie die NAT-ID auch dann festlegen, wenn Sie einen Hostnamen oder eine IP-Adresse angeben. Die NAT-ID darf maximal 37 Zeichen lang sein. Gültige Zeichen sind alphanumerische Zeichen (A-Z, a-z, 0-9) und Bindestrich (-). Diese ID kann nicht für andere Geräte verwendet werden, die sich beim Management Center registrieren.

Um den Modus wieder in den Appliance-Modus zu ändern, müssen Sie die FXOS-CLI verwenden und das Enscope-System und den nativen Bereitstellungsmodus festlegen. [Siehe Ändern der Chassis-Verwaltungseinstellungen in der FXOS-CLI.](#)

Beispiel:

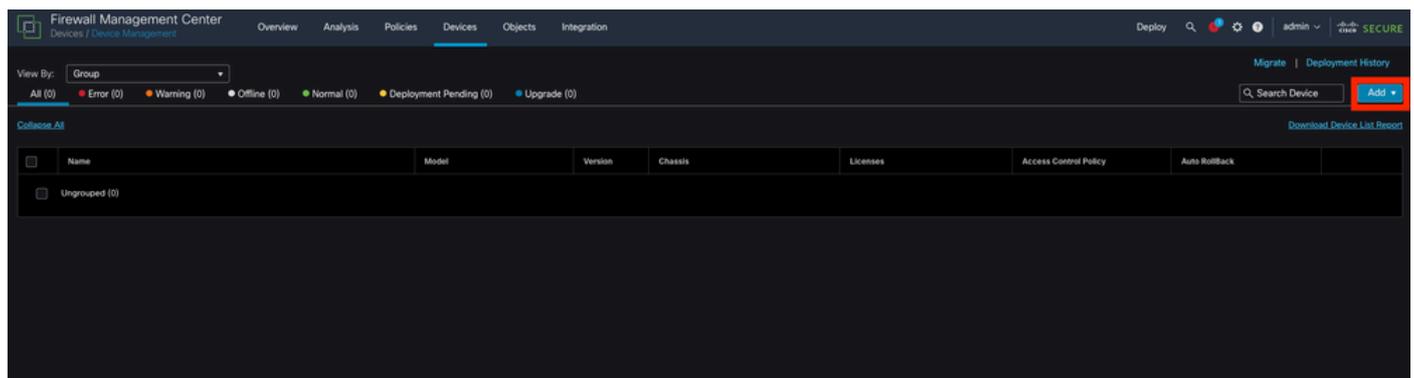
```
> configure multi-instance network ipv4 10.88.146.203 255.255.255.0 10.88.146.1
manager fmc1 10.88.243.100 cisco123 natid1
WARNING: This command will discard any FTD configuration (except admin's credentials). Make sure you backup your content
. All previous content will be lost. System is going to be re-initialized. Type ERASE to confirm:ERASE
Continue...
Validation check...
Checking startup version and csp file ...
Converting to MI mode, device will be rebooted and re-initialized...
>
Broadcast message from root@firepower (Sun Jan 22 00:10:14 2023):
All shells being terminated due to system /sbin/reboot
Broadcast message from root@firepower (Sun Jan 22 00:10:15 2023):
System is restarted due to deploy mode changed
```

Wechseln in den Multi-Instance-Modus

 Hinweis: Fügen Sie das Multi-Instance-Chassis dem Management Center hinzu. Das Management Center und das Chassis verwenden eine separate Management-Verbindung über die Chassis-MGMT-Schnittstelle. Mit dem Management Center können Sie alle Chassis-Einstellungen sowie Instanzen konfigurieren. Der Secure Firewall-Chassis-Manager oder die Konfiguration in der FXOS-CLI wird nicht unterstützt.

Schritt 7. Fügen Sie im Management Center das Chassis mit der IP-Adresse oder dem Hostnamen für das Chassis-Management hinzu.

- Wählen Sie Devices (Geräte) Device Management (Geräteverwaltung) und dann Add (Hinzufügen) Chassis.



Add Chassis ? ×

i This operation is only supported on 3100, 4100 & 9300 chassis

Hostname/IP Address†

Chassis name

Registration key*

Device Group

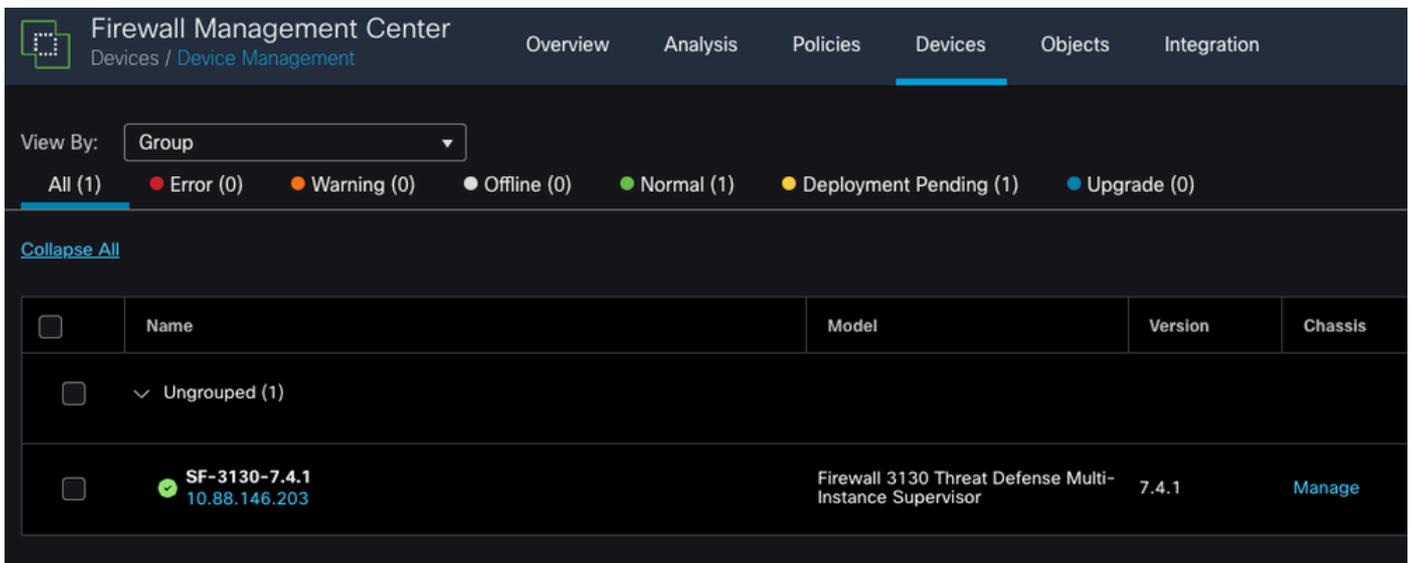
 ▼

Unique NAT ID†

† Either host or NAT ID is required. Cancel Submit

Setup-Parameter des Chassis

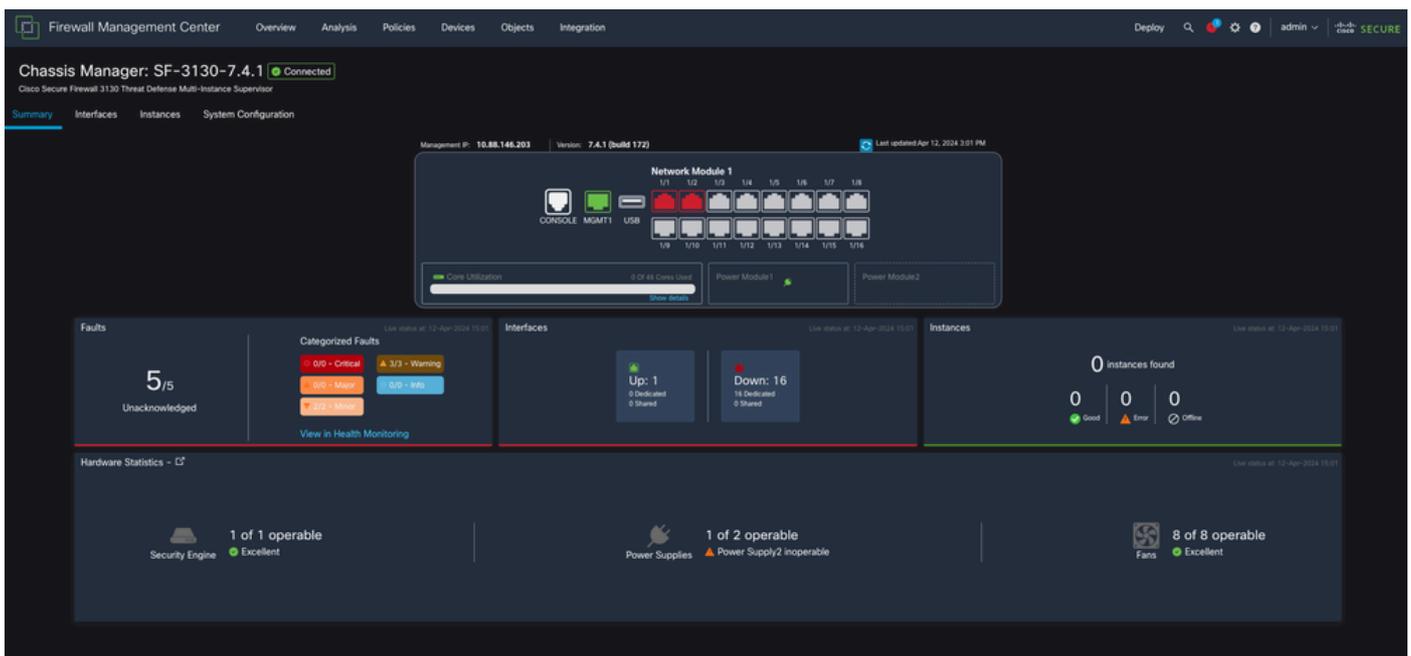
- Sobald das Chassis dem FMC hinzugefügt wurde, sehen Sie sich das Gerät in der Liste der Geräte im FMC an.



Chassis im FMC hinzugefügt

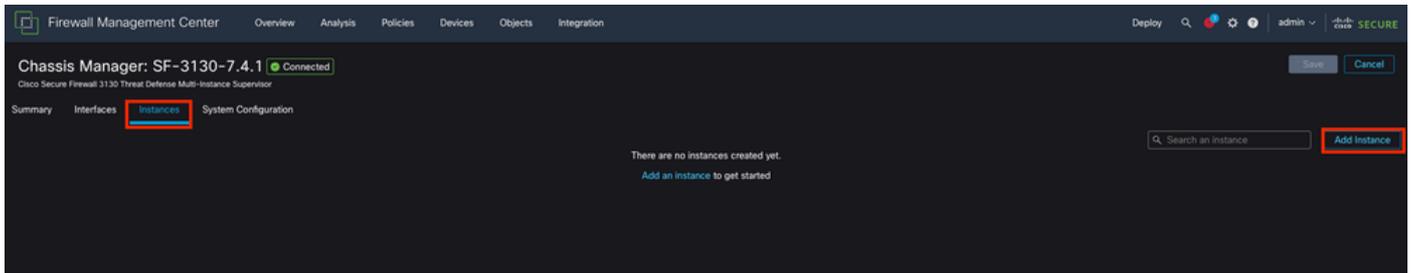
Schritt 8: Um das Chassis anzuzeigen und zu konfigurieren, klicken Sie in der Spalte Chassis auf Manage (Verwalten), oder klicken Sie auf Edit(✎).

Die Seite Chassis-Manager wird geöffnet, und das Chassis wird auf die Seite Zusammenfassung geleitet.



Chassis-Management

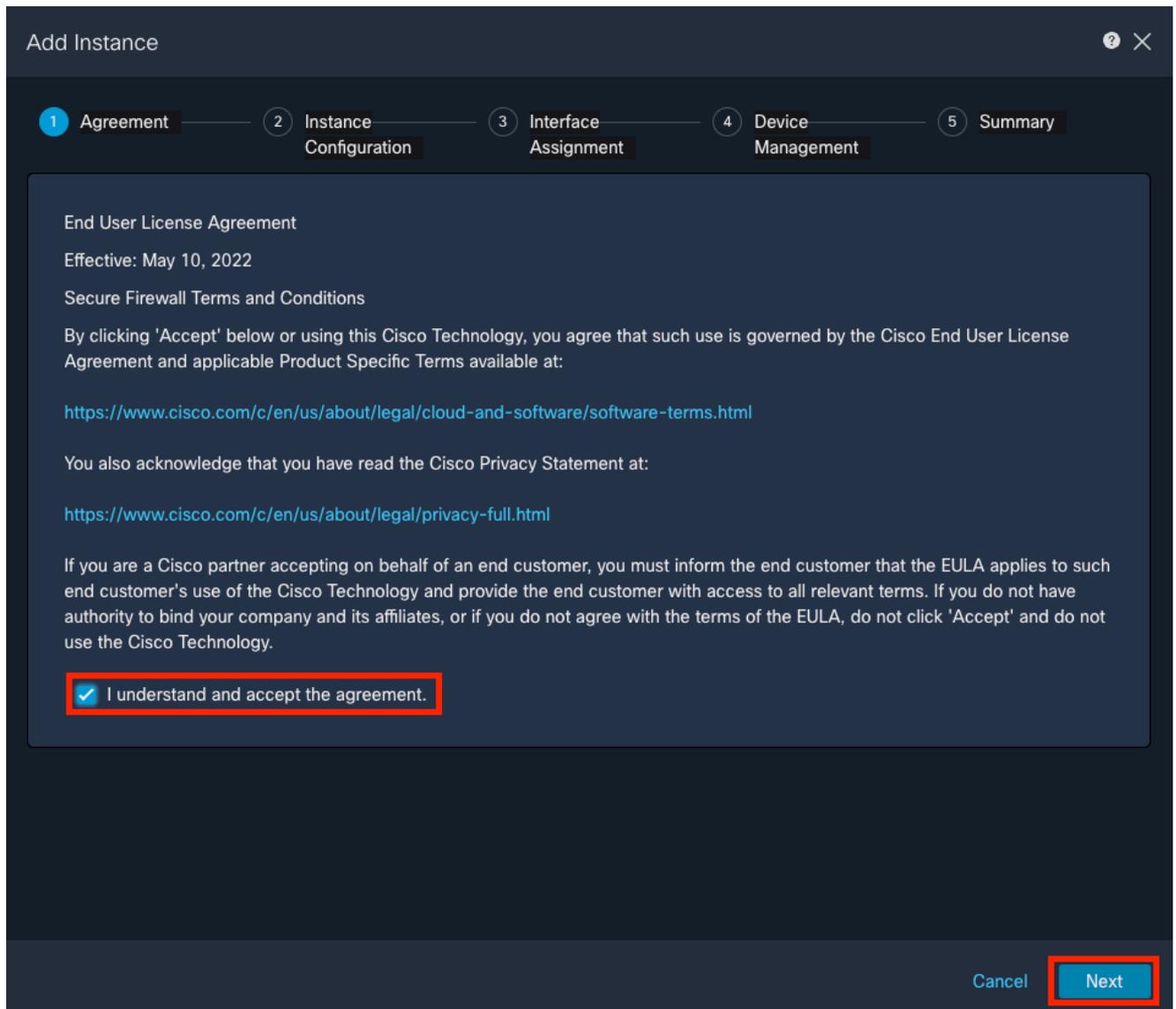
Schritt 9. Wählen Sie die Schaltfläche Instances (Instanzen) und dann Add Instance (Instanz hinzufügen), um eine neue Instanz im Chassis zu erstellen.



Erstellen einer Instanz

Schritt 10. Folgen Sie dem Assistenten, um die Installation der Instanz abzuschließen.

1. Akzeptieren Sie die Vereinbarung



Vereinbarung akzeptieren

2. Konfigurieren der Instanzparameter

Add Instance ? ×

1 Agreement — 2 Instance Configuration — 3 Interface Assignment — 4 Device Management — 5 Summary

Display Name*
SF-3130-741-Instance

Device Version*
7.4.1.172

Resource Profile*
Default-Medium +

Permit Expert mode for CLI

IPv4 IPv6 Both

IPv4

Management IP*
10.88.146.198

Network Mask*
255.255.255.0

Network Gateway*
10.88.146.1

Search Domain

FQDN

Firewall Mode*
Routed

DNS Servers
172.18.108.34

Device SSH Password*
.....

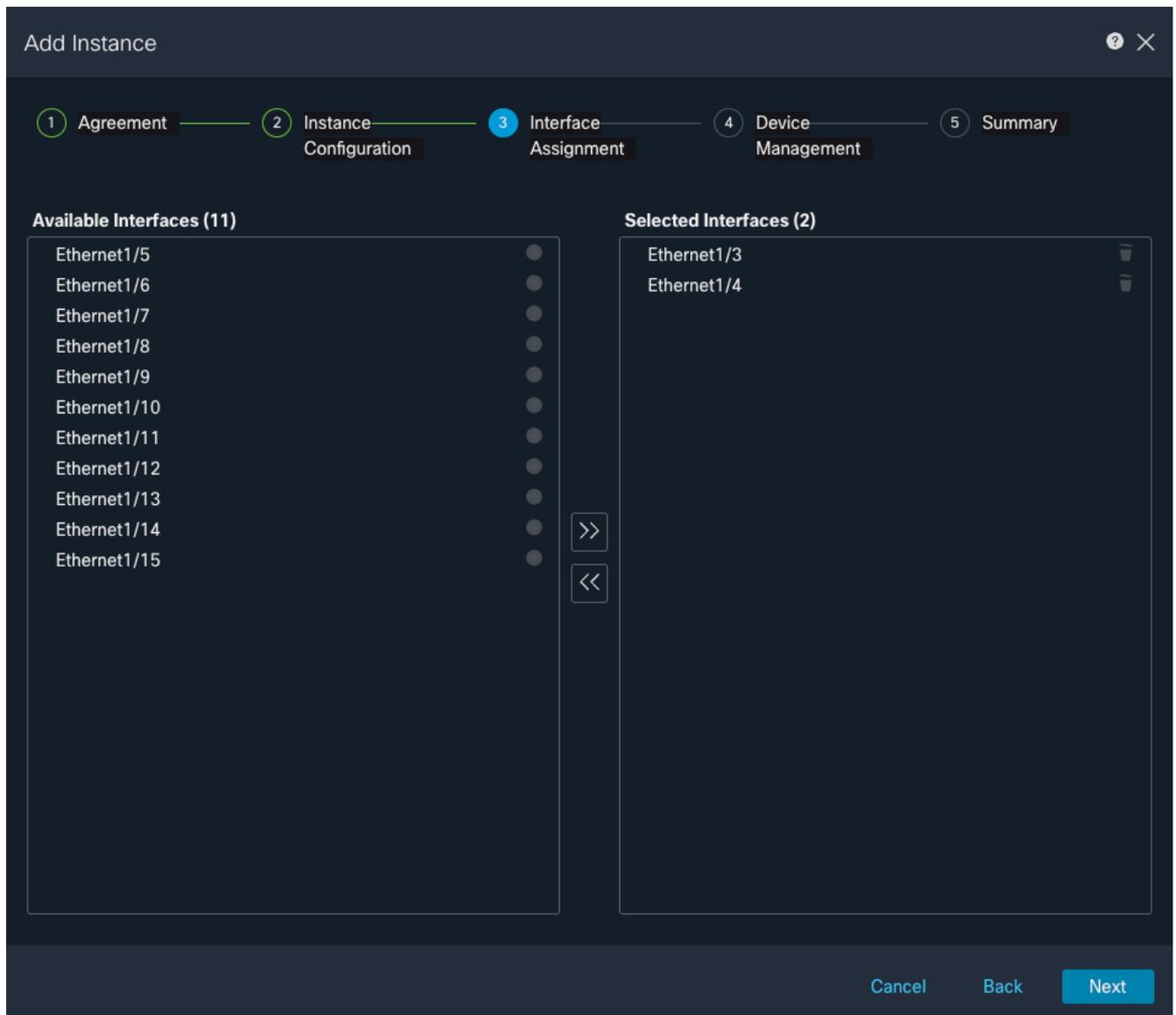
Confirm Password*
.....

Show Password

Cancel Back **Next**

Instanzparameter

3. Schnittstellenauswahl.



Schnittstellenzuweisung

4. Gerätemanagement:

Add Instance ? ×

1 Agreement — 2 Instance Configuration — 3 Interface Assignment — 4 Device Management — 5 Summary

Device Group
Select... ▾

Access Control Policy*
ACP ▾ +

Platform Settings
Instance x ▾ +

Smart Licensing

- Carrier
- Malware Defense
- IPS
- URL

Cancel Back **Next**

Gerätemanagement

5. Zusammenfassung

Add Instance



- 1 Agreement
- 2 Instance Configuration
- 3 Interface Assignment
- 4 Device Management
- 5 Summary

Instance Configuration

Name: asdvav
Version: 7.4.1.172
Resource Profile: Default-Small
IP: 10.88.243.13
Mask: 255.255.255.0
Gateway: 10.88.243.1
Mode: routed
Password: *****
FQDN:
DNS Servers:
Search Domain:
Expert Mode: disabled

Device Management - This info is required only during instance creation.

Access Policy: ACP
Device Group:
Platform Policy: Instance
Licenses: Carrier, Malware Defense, IPS, URL

Interface Assignment - 2 dedicated and 0 shared interfaces attached [Show All](#)

Cancel

Back

Save

Zusammenfassung der Instanz

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.