Configure Multi-Instance in Secure Firewall 3100 Series

Contents

Introduction

This document describes how to configure Multi-Instacne in Secure Firewall 3100 Series running version 7.4+.

Prerequisites

Knowledge of Firewall eXtensible Operating System (FXOS) and Firewall Management Center (FMC) Graphical User Interface (GUI).

Requirements

Access to:

- Console access to the Secure Firewall 3100 Series
- FMC GUI Access

Components Used

- Cisco Secure Firewall Management Center running 7.4+
- Cisco Secure Firewall Series 3100
  - Except 3105*

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In multi-instance mode, you can deploy multiple container instances on a single chassis that act as completely independent devices.

Configure for 7.4.1+ Version

Step 1.Connect to the chassis console port.

The console port connects to the FXOS CLI.

Step 2. Log in with the username **admin**and the password**Admin123**.

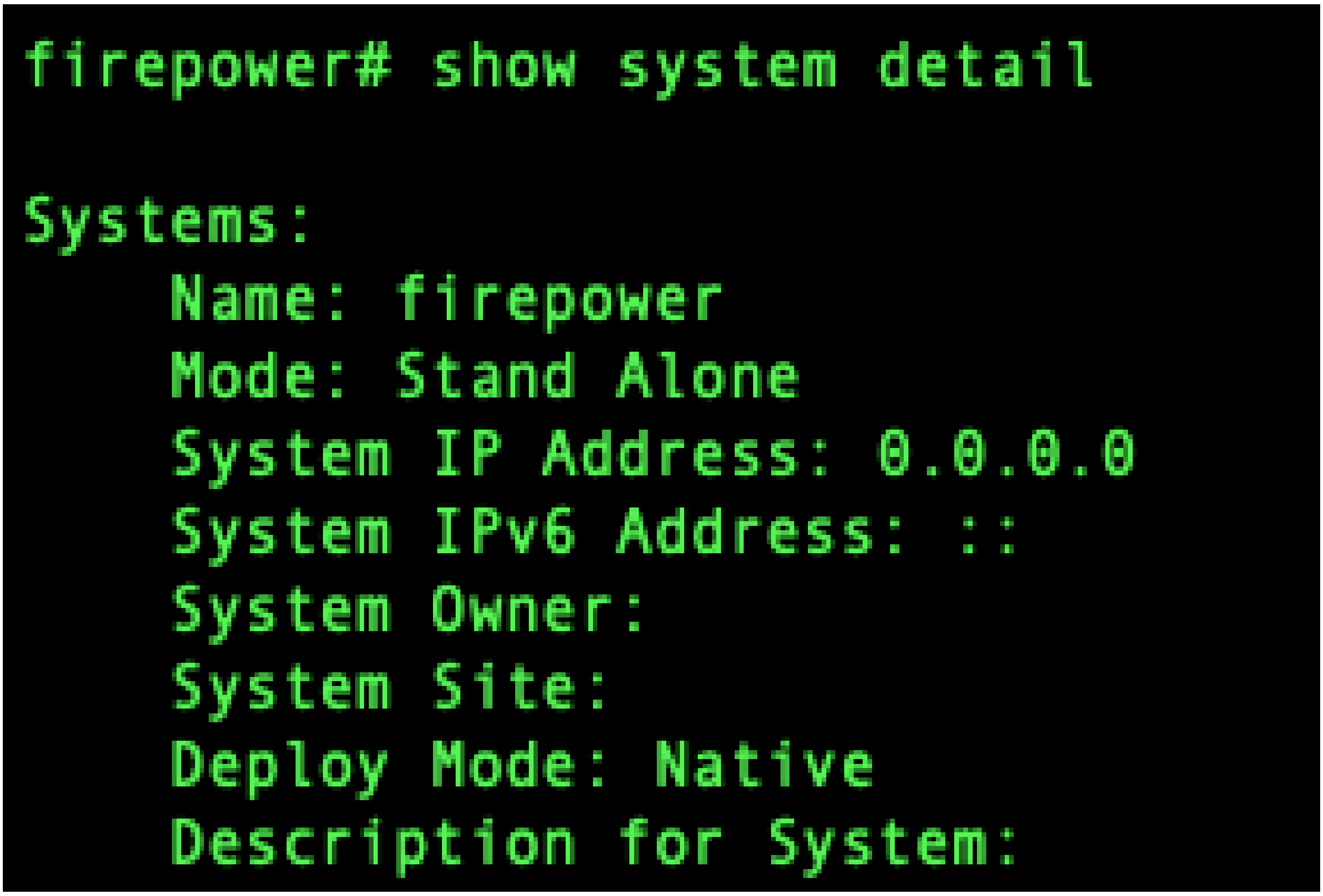
You are prompted to change the password the first time you log in to FXOS.

Note: If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See theFXOStroubleshooting guidefor thereimage procedure.

Step 3. Check your current mode, Native or Container. If the mode is Native, you can continue with this procedure to convert to multi-instance (Container) mode.

firepower# **show system detail**

Example:



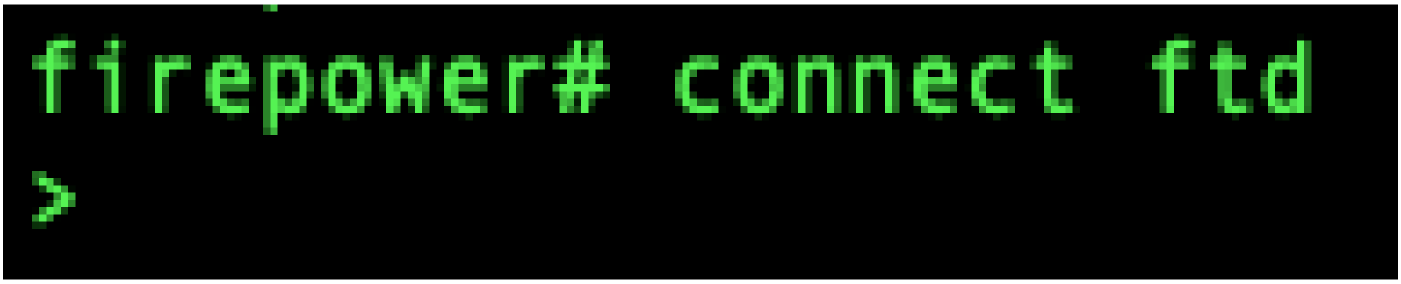
```
firepower# show system detail

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:
```

Show multi-instance state

Step 4. Connect to theTthreat Defense CLI.

firepower# **connect ftd**

Example:



```
firepower# connect ftd
>
```

Connecting to FTD

Step 5. The first time you log in to the threat defense, you are prompted to accept the End User License Agreement (EULA). You are then presented with the CLI setup script.

The setup script lets you set the Management interface IP address and other settings. However, when you convert to multi-instance mode, the only settings that are retained are the following.

- Admin password (that you set at initial login)
- DNS servers
- Search domains

You reset the Management IP address and gateway as part of the multi-instance mode command. After you convert to multi-instance mode, you can change Management settings at the FXOS CLI. SeeChange Chassis Management Settings at the FXOS CLI.

Step 6. Enable multi-instance mode, set the chassis management interface settings, and identify themanagement center. You can use IPv4 and/or IPv6. After you enter the command,you are prompted to erase the configuration and reboot. EnterERASE(all caps). The system reboots and, as part of changing the mode, erases the configuration with the exception of the Management network settings you set in the command and the admin password. The chassis hostname is set to "firepower-*model*."

IPv4:

configure multi-instance network ipv4*ip_addressnetwork_maskgateway_ip_address*manager*manager_name* {*hostname* | *ipv4_address* | DONTRESOLVE} *registration_keynat_id*

IPv6:

configure multi-instance network ipv6*ipv6_addressprefix_lengthgateway_ip_address*manager*manager_name* {*hostname* | *ipv6_address* | DONTRESO

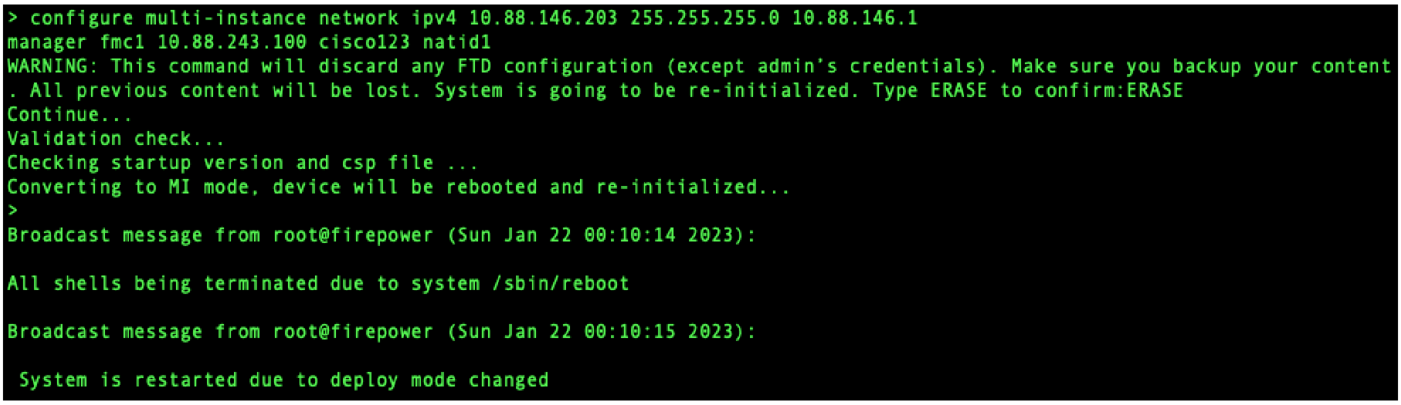
See these managercomponents:

- {*hostname* | *ipv4_address* | DONTRESOLVE} —Specifies either the FQDN or IP address of themanagement center. At least one of the devices, either themanagement centeror the chassis, must have a reachable IP address to establish the two-way, SSL-encrypted communication channel between the two devices. If you do not specify a manager hostname or IP address in this command, then enterDONTRESOLVE; in this case, the chassis must have a reachable IP address or hostname, and you must specify the*nat_id*.
- *registration_key*—Enter a one-time registration key of your choice that you also specify on themanagement centerwhen you register the chassis. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

- *nat_id*—Specifies a unique, one-time string of your choice that you also also specify on themanagement centerwhen you register the chassis when one side does not specify a reachable IP address or hostname. It is required if you do not specify a manager address or hostname, however, we recommend that you always set the NAT ID even when you specify a hostname or IP address. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to themanagement center.

To change the mode back to appliance mode, you must use the FXOS CLI and enterscope systemand thenset **deploymode native**. SeeChange Chassis Management Settings at the FXOS CLI.

Example:



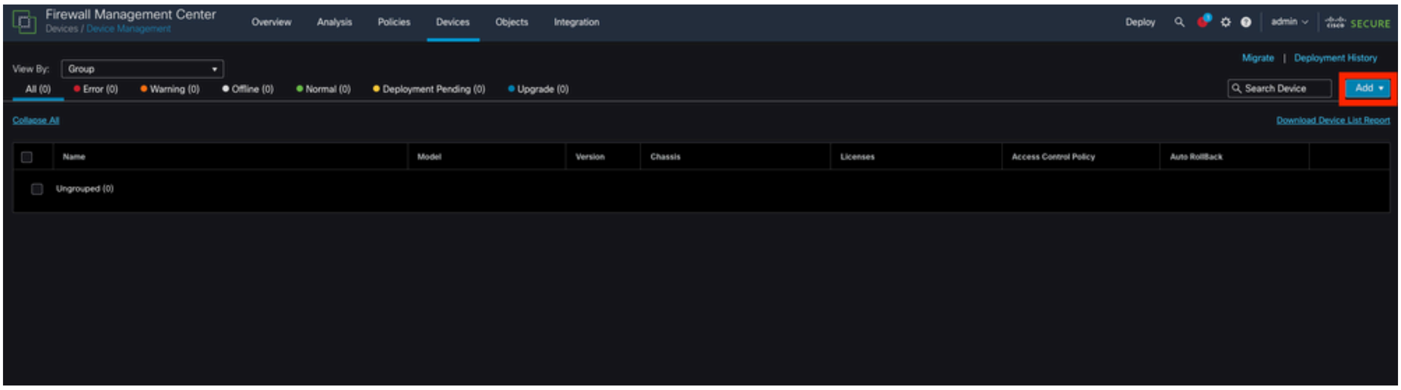
```
> configure multi-instance network ipv4 10.88.146.203 255.255.255.0 10.88.146.1
manager fmc1 10.88.243.100 cisco123 natid1
WARNING: This command will discard any FTD configuration (except admin's credentials). Make sure you backup your content
. All previous content will be lost. System is going 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
```

Changing to Multi-Instance Mode

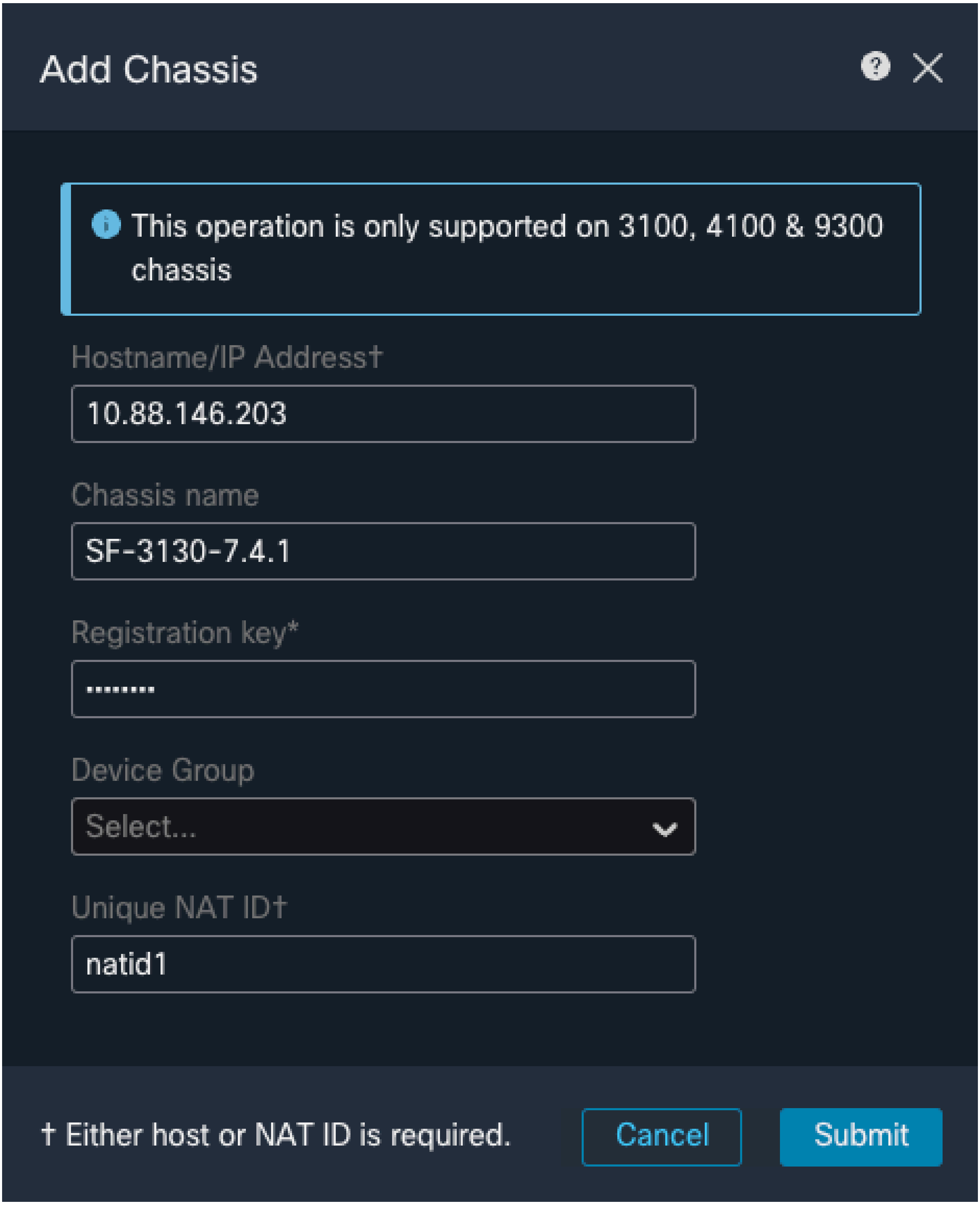
Note: Add the multi-instance chassis to the management center. The management center and the chassis share a separate management connection using the chassis MGMT interface. You can use the management center to configure all chassis settings as well as instances. The Secure Firewall chassis manager or configuration at the FXOS CLI is not supported.

Step 7. In the management center, add the chassis using the chassis management IP address or hostname.

- Choose **Devices**>**Device Management**, and then **Add**>**Chassis**.



Adding the Chassis to the FMC



Add Chassis

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

Hostname/IP Address†

10.88.146.203

Chassis name

SF-3130-7.4.1

Registration key*

•••••••••

Device Group

Select...

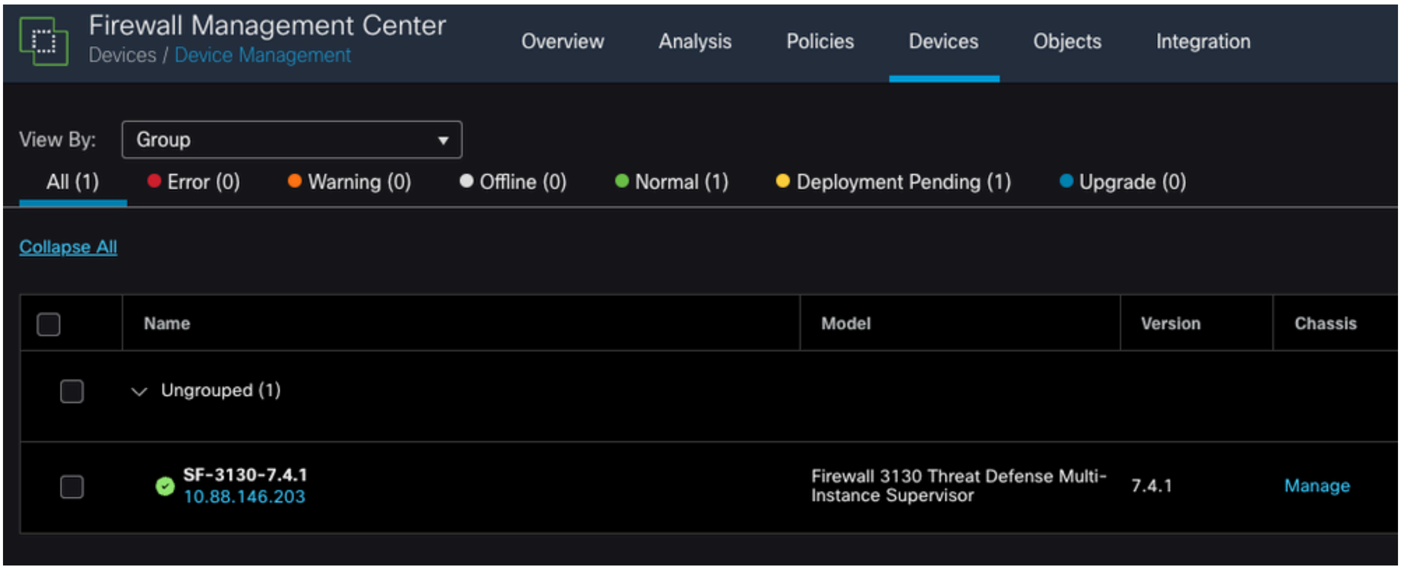
Unique NAT ID†

natid1

† Either host or NAT ID is required.

Setup parameters of the Chassis

- Once the Chassis is added to the FMC, see the device in the list of the devices on the FMC.



View By: Group

All (1) | ● Error (0) | ● Warning (0) | ● Offline (0) | ● Normal (1) | ● Deployment Pending (1) | ● Upgrade (0)

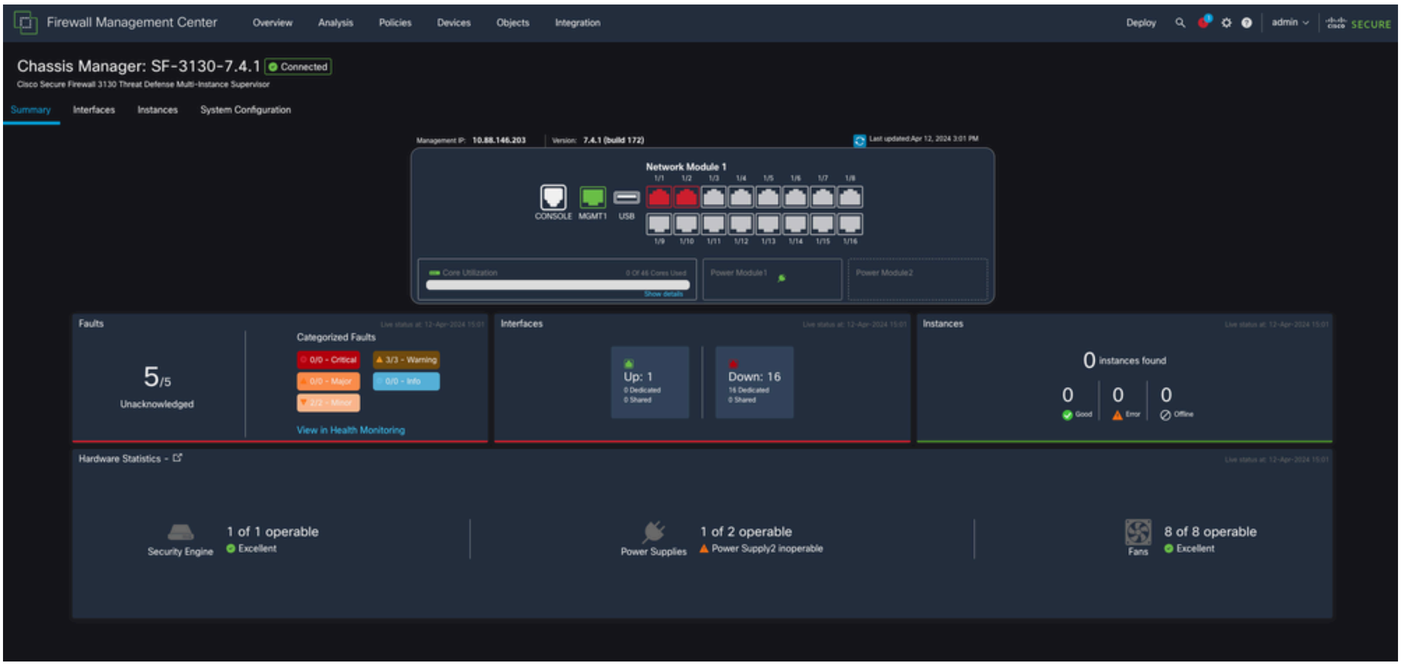
Collapse All

□	Name	Model	Version	Chassis
□	Ungrouped (1)			
□	SF-3130-7.4.1 10.88.146.203	Firewall 3130 Threat Defense Multi-Instance Supervisor	7.4.1	Manage

Chassis added in the FMC

Step 8. To view and configure the chassis, click **Manage** in the Chassis column, or click Edit(✎).

The Chassis Manager page opens for the chassis to the Summary page.



Chassis Manager: SF-3130-7.4.1 Connected

Cisco Secure Firewall 3130 Threat Defense Multi-Instance Supervisor

Management IP: 10.88.146.203 | Version: 7.4.1 (build 172)

Last updated:Apr 12, 2024 3:01 PM

Core Utilization 0 Of 46 Cores Used

Faults — Live status at: 12-Apr-2024 15:01

5/5 Unacknowledged

Categorized Faults: 0/0 - Critical; 3/3 - Warning; 0/0 - Major; 0/0 - Info; 2/2 - Minor

Interfaces — Live status at: 12-Apr-2024 15:01

Up: 1 (0 Dedicated, 0 Shared)

Down: 16 (16 Dedicated, 0 Shared)

Instances — Live status at: 12-Apr-2024 15:01

0 instances found

0 Good | 0 Error | 0 Offline

Hardware Statistics — Live status at: 12-Apr-2024 15:01

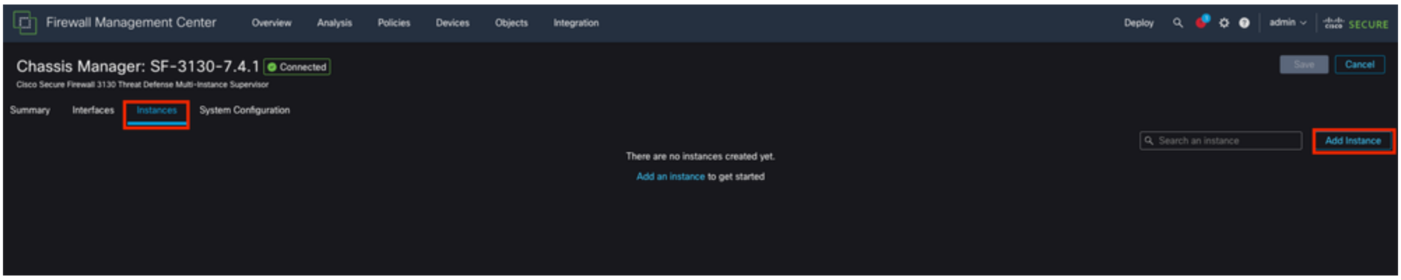
Security Engine: 1 of 1 operable, Excellent

Power Supplies: 1 of 2 operable, Power Supply2 inoperable

Fans: 8 of 8 operable, Excellent

Chassis Management

Step 9. Select the **Instances** button and then **Add Instance** to create a new Instance in the chassis.



Chassis Manager: SF-3130-7.4.1 Connected

Cisco Secure Firewall 3130 Threat Defense Multi-Instance Supervisor

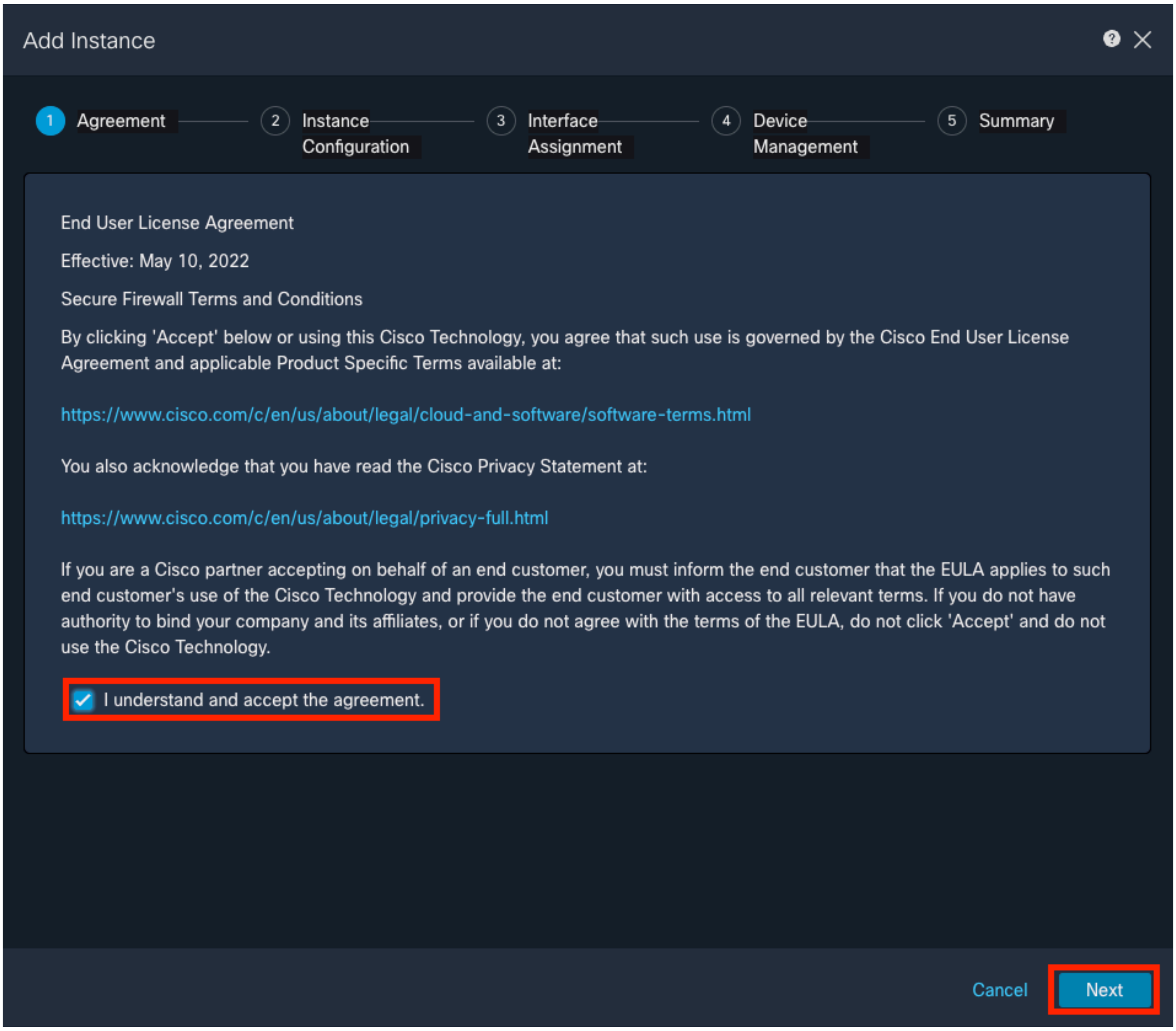
There are no instances created yet.

Add an instance to get started

Creating an Instance

Step 10. Follow the wizard to finish the installation of the Instance.

1. Accept the agreement



End User License Agreement

Effective: May 10, 2022

Secure Firewall Terms and Conditions

By clicking 'Accept' below or using this Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and applicable Product Specific Terms available at:

https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html

You also acknowledge that you have read the Cisco Privacy Statement at:

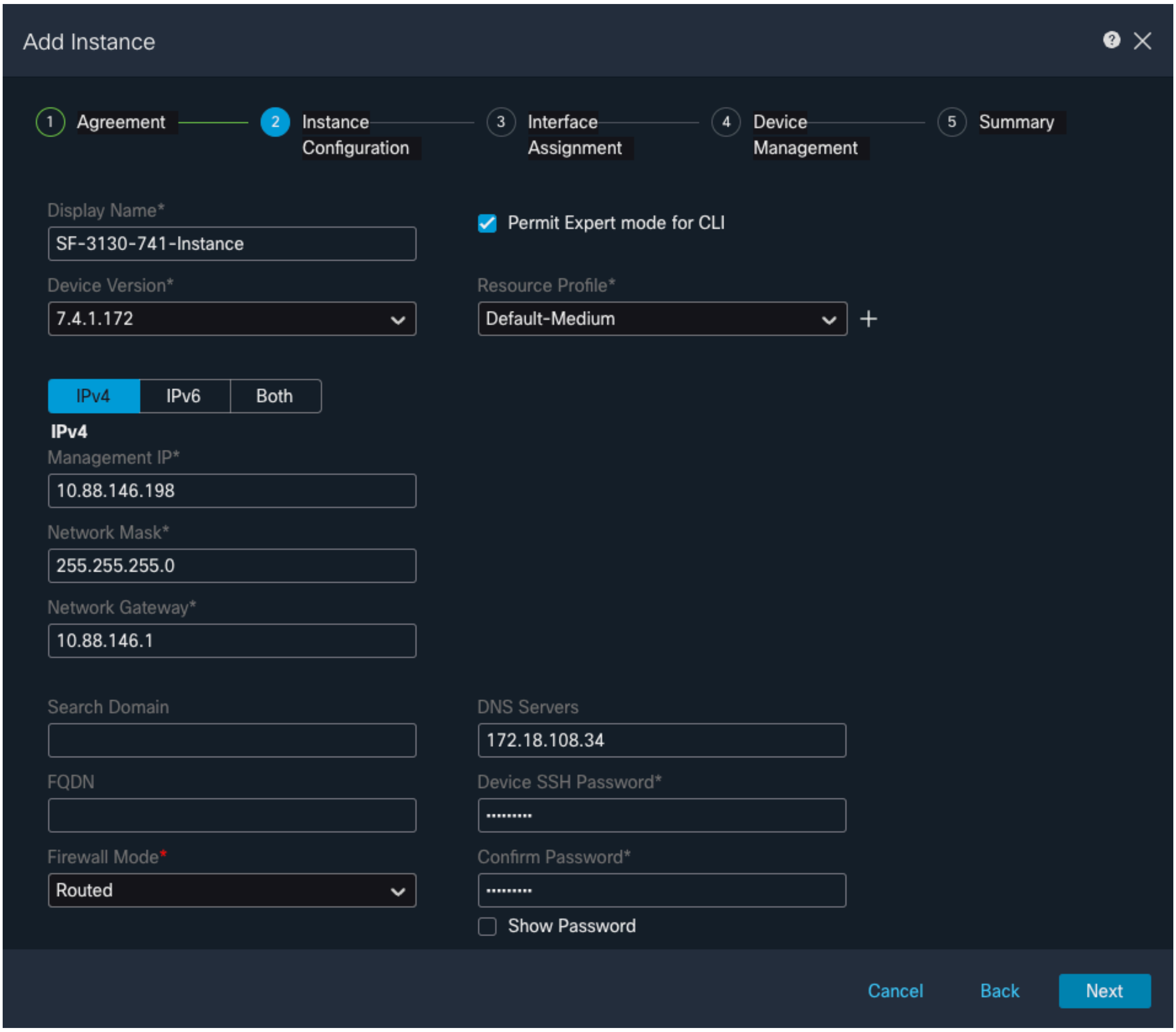
https://www.cisco.com/c/en/us/about/legal/privacy-full.html

If you are a Cisco partner accepting on behalf of an end customer, you must inform the end customer that the EULA applies to such end customer's use of the Cisco Technology and provide the end customer with access to all relevant terms. If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'Accept' and do not use the Cisco Technology.

☑ I understand and accept the agreement.

Accept agreement

2. Configure the Instance parameters



Display Name*: SF-3130-741-Instance

☑ Permit Expert mode for CLI

Device Version*: 7.4.1.172

Resource Profile*: Default-Medium

IPv4

Management IP*: 10.88.146.198

Network Mask*: 255.255.255.0

Network Gateway*: 10.88.146.1

Search Domain:

DNS Servers: 172.18.108.34

FQDN:

Device SSH Password*: •••••••••

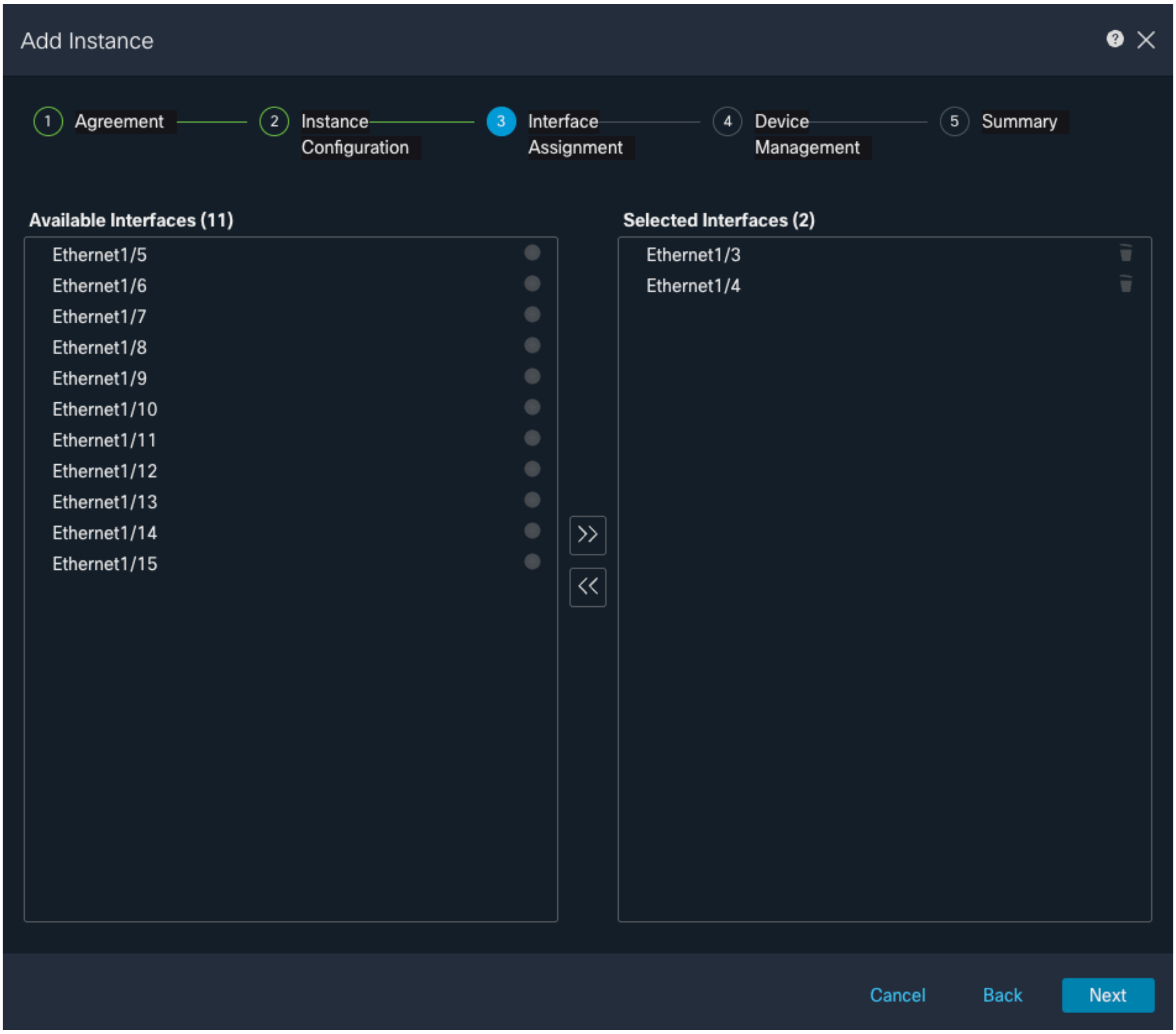
Firewall Mode*: Routed

Confirm Password*: •••••••••

□ Show Password

Instance Parameters

3. Interface Selection.



Add Instance

Available Interfaces (11)

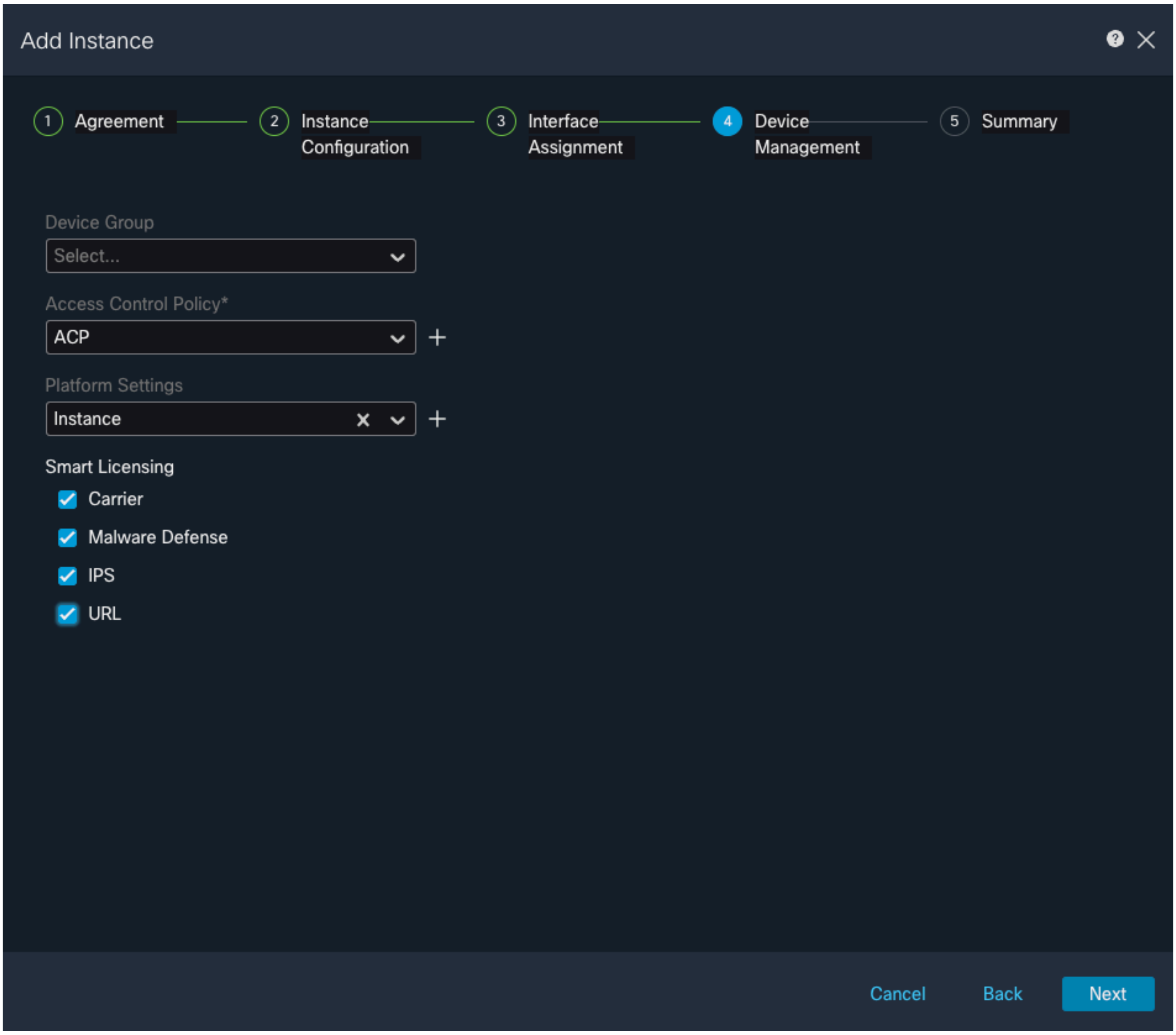
- Ethernet1/5
- Ethernet1/6
- Ethernet1/7
- Ethernet1/8
- Ethernet1/9
- Ethernet1/10
- Ethernet1/11
- Ethernet1/12
- Ethernet1/13
- Ethernet1/14
- Ethernet1/15

Selected Interfaces (2)

- Ethernet1/3
- Ethernet1/4

Interface Assigment

4. Device Management.



Device Group: Select...

Access Control Policy*: ACP

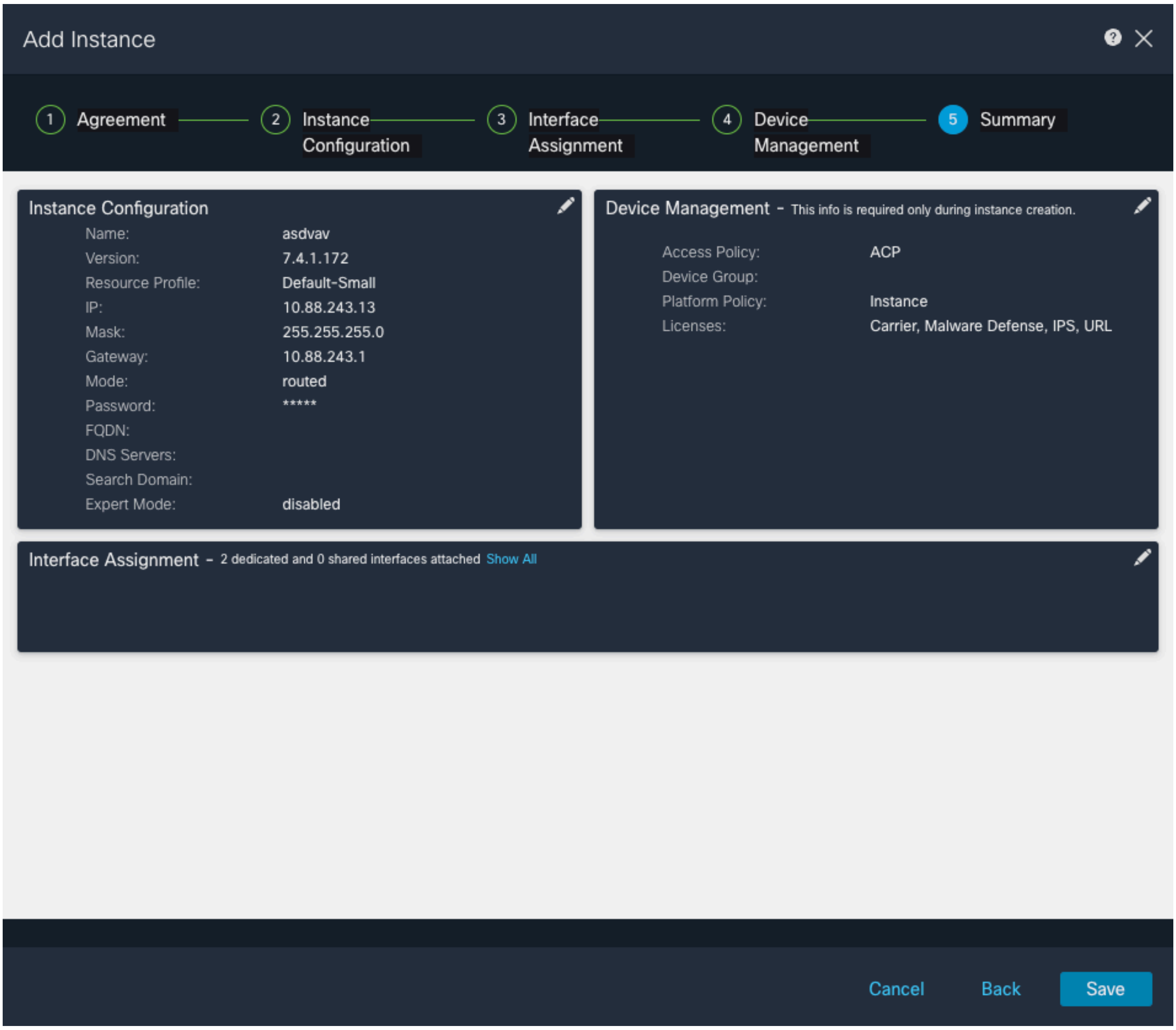
Platform Settings: Instance

Smart Licensing

- ☑ Carrier
- ☑ Malware Defense
- ☑ IPS
- ☑ URL

Device Management

5. Summary



Add Instance

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

Summary of the Instance