Configurazione di più istanze in Secure Firewall serie 3100

Sommario

Introduzione

In questo documento viene descritto come configurare Multi-Instance in Secure Firewall serie 3100 con versione 7.4+.

Prerequisiti

Conoscenza dell'interfaccia grafica utente (GUI) del sistema operativo estendibile (FXOS) e del centro di gestione dei firewall (FMC).

Requisiti

Accesso a:

- Accesso da console a Secure Firewall serie 3100
- Accesso all'interfaccia utente di FMC

Componenti usati

- Cisco Secure Firewall Management Center con versione 7.4+
- Cisco Secure Firewall serie 3100
  - Eccetto 3105*

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In modalità a più istanze, è possibile distribuire più istanze del contenitore su un singolo chassis

che fungono da dispositivi completamente indipendenti.

Configurazione per la versione 7.4.1+

Passaggio 1. Collegarsi alla porta della console dello chassis.

La porta della console si connette alla CLI di FXOS.

Passaggio 2. Accedere con il nome utente admin e la passwordAdmin123.

Al primo accesso a FXOS viene richiesto di modificare la password.

Nota: se la password è già stata cambiata e non la si conosce, è necessario ricreare l'immagine del dispositivo per ripristinare la password predefinita. Vedere la guida alla risoluzione dei problemi di FXOS per la procedura relativa all'immagine.

Passaggio 3. Controllare la modalità corrente, Nativa o Contenitore. Se la modalità è Nativa, è possibile continuare con questa procedura per passare alla modalità a più istanze (Contenitore).

firepower# mostra dettagli sistema

Esempio:

```
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:
```

Mostra stato a più istanze

Passaggio 4. Connettersi alla CLI di Threat Defense.

firepower#connect ftd

Esempio:

Connessione a FTD

Passaggio 5. La prima volta che si accede alla difesa contro la minaccia, viene richiesto di accettare il Contratto di Licenza con l'utente finale (EULA). Viene quindi visualizzato lo script di impostazione della CLI.

Lo script di impostazione consente di impostare l'indirizzo IP dell'interfaccia di gestione e altre impostazioni. Tuttavia, quando convertite in modalità multi-istanza, le uniche impostazioni che vengono mantenute sono le seguenti.

- Password amministratore (impostata al primo accesso)
- Server DNS
- Cerca domini

L'indirizzo IP di gestione e il gateway vengono reimpostati come parte del comando modalità a più istanze. Dopo la conversione in modalità a più istanze, è possibile modificare le impostazioni di gestione nella CLI di FXOS. Vedere Modifica delle impostazioni di gestione dello chassis nella CLI di FXOS.

Passaggio 6. Abilitare la modalità multi-istanza, impostare le impostazioni dell'interfaccia di gestione dello chassis e identificare il centro di gestione. È possibile utilizzare IPv4 e/o IPv6. Dopo aver immesso il comando, viene richiesto di cancellare la configurazione e riavviare il sistema. EnterERASE(tutto maiuscole). Il sistema si riavvia e, come parte della modifica della modalità, cancella la configurazione ad eccezione delle impostazioni di rete di gestione impostate nel comando e della password di amministratore. Il nome host dello chassis è impostato su "firepower-model".

IPv4:

configurare la rete a più istanze
ipv4ip_addressnetwork_maskgateway_ip_addressmanagermanager_name
{hostname | indirizzo_ipv4 | DONTRESOLVE} id_chiave_registrazione

IPv6:

configurare la rete a più istanze
ipv6ipv6_addressprefix_length_gateway_ip_addressmanagermanager_name
{hostname | indirizzo_ipv6 | DONTRESOLVE} id_chiave_registrazione

Vedere i seguenti componenti di gestione:

- {nome host | indirizzo_ipv4 | DONTRESOLVE}} - Specifica il nome di dominio completo (FQDN) o l'indirizzo IP del centro di gestione. Almeno uno dei dispositivi, il centro di gestione o lo chassis, deve avere un indirizzo IP raggiungibile per stabilire il canale di comunicazione bidirezionale crittografato con SSL tra i due dispositivi. Se non si specifica un nome host o un indirizzo IP del manager in questo comando, immettereDONTRESOLVE; in questo caso, lo chassis deve avere un indirizzo IP o un nome host raggiungibile ed è necessario specificare thenat_id.

- registration_key: immettere una chiave di registrazione unica di propria scelta che si specifica anche sul management centre quando si registra lo chassis. La chiave di registrazione non deve superare i 37 caratteri. I caratteri validi includono caratteri alfanumerici (A-Z, a-z, 0-9) e il trattino (-).

- nat_id - Specifica una stringa univoca e temporanea a scelta che viene specificata anche nel management centre quando si registra lo chassis quando un lato non specifica un indirizzo IP o un nome host raggiungibile. È obbligatorio se non si specifica l'indirizzo o il nome host di un manager. Tuttavia, si consiglia di impostare sempre l'ID NAT anche quando si specifica un nome host o un indirizzo IP. L'ID NAT non deve superare i 37 caratteri. I caratteri validi includono caratteri alfanumerici (A-Z, a-z, 0-9) e il trattino (-). Questo ID non può essere utilizzato per nessun altro dispositivo che si registra nel centro di gestione.

Per ripristinare la modalità accessorio, è necessario utilizzare la CLI di FXOS e il sistema enterscope e quindi impostare la modalità di distribuzione nativa. Vedere Modifica delle impostazioni di gestione dello chassis nella CLI di FXOS.

Esempio:

```
> 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
```

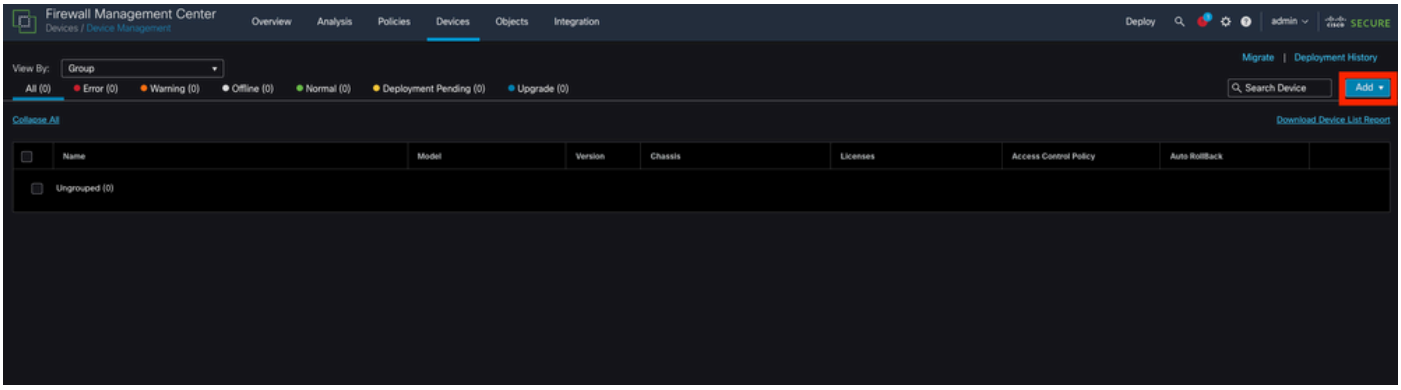
Passaggio alla modalità a più istanze

Nota: aggiungere lo chassis a più istanze al centro di gestione. Il centro di gestione e lo chassis condividono una connessione di gestione separata tramite l'interfaccia di gestione dello chassis. È possibile utilizzare il centro di gestione per configurare tutte le impostazioni

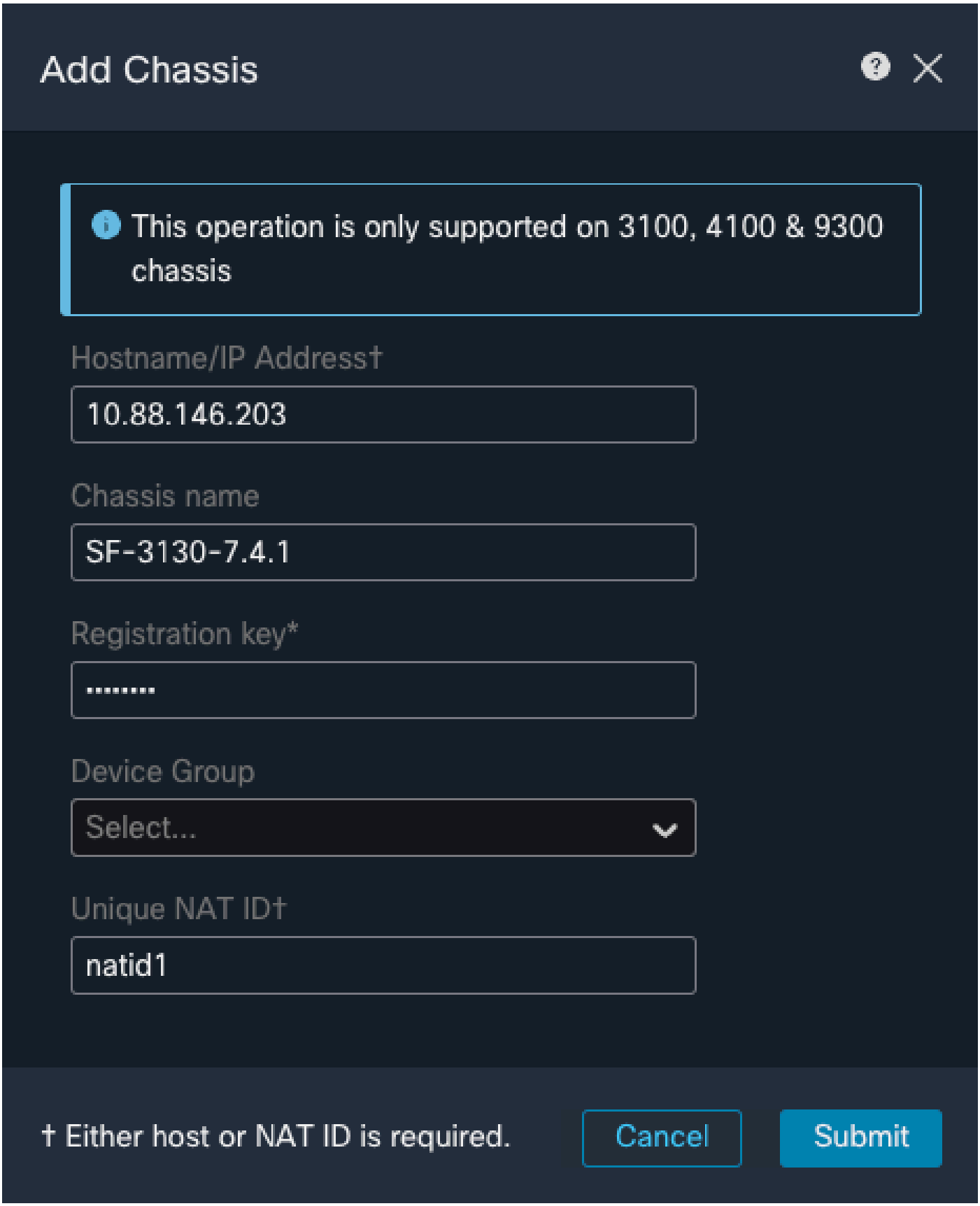
dello chassis e le istanze. La configurazione o il gestore dello chassis Secure Firewall nella CLI di FXOS non è supportato.

Passaggio 7. Nel centro di gestione, aggiungere lo chassis utilizzando l'indirizzo IP o il nome host di gestione dello chassis.

- Scegliere Dispositivi>Gestione dispositivi, quindi Aggiungi>Chassis.

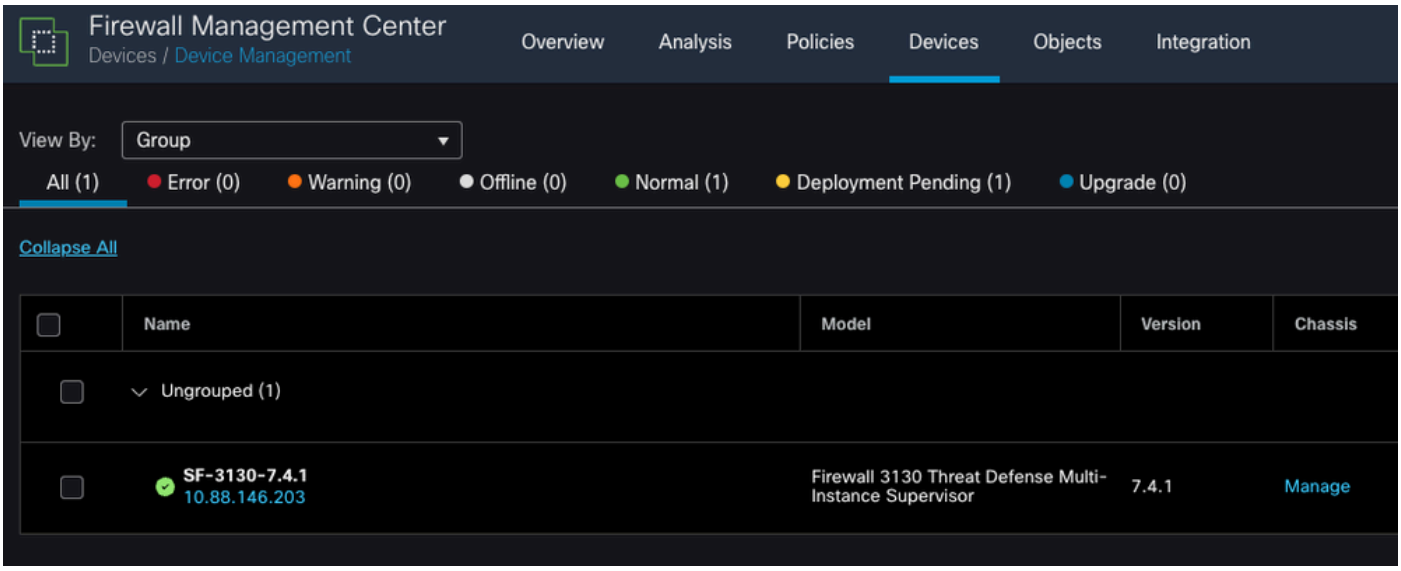


Aggiunta dello chassis al FMC



Parametri di configurazione dello chassis

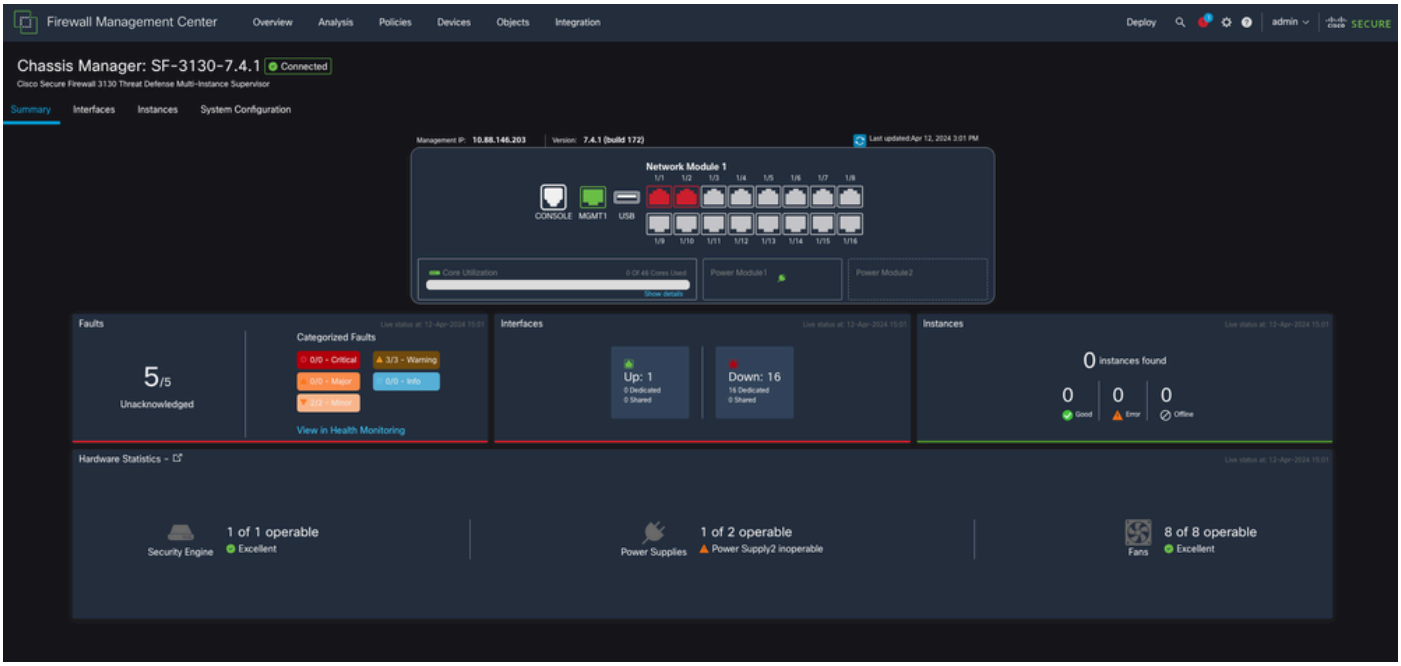
- Una volta aggiunto lo chassis al CCP, vedere il dispositivo nell'elenco dei dispositivi del CCP.



Chassis aggiunto nel FMC

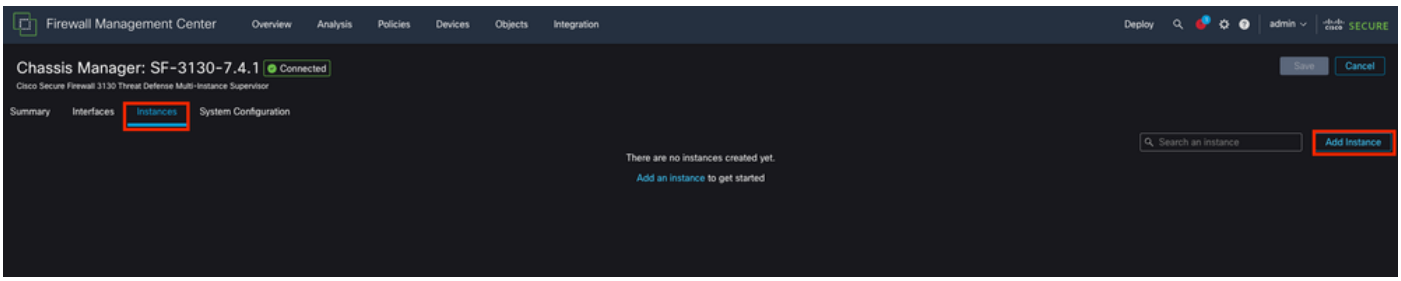
Passaggio 8. Per visualizzare e configurare lo chassis, fare clic su Gestisci nella colonna Chassis oppure fare clic su Modifica(✎).

Viene visualizzata la pagina Chassis Manager per passare alla pagina Summary.



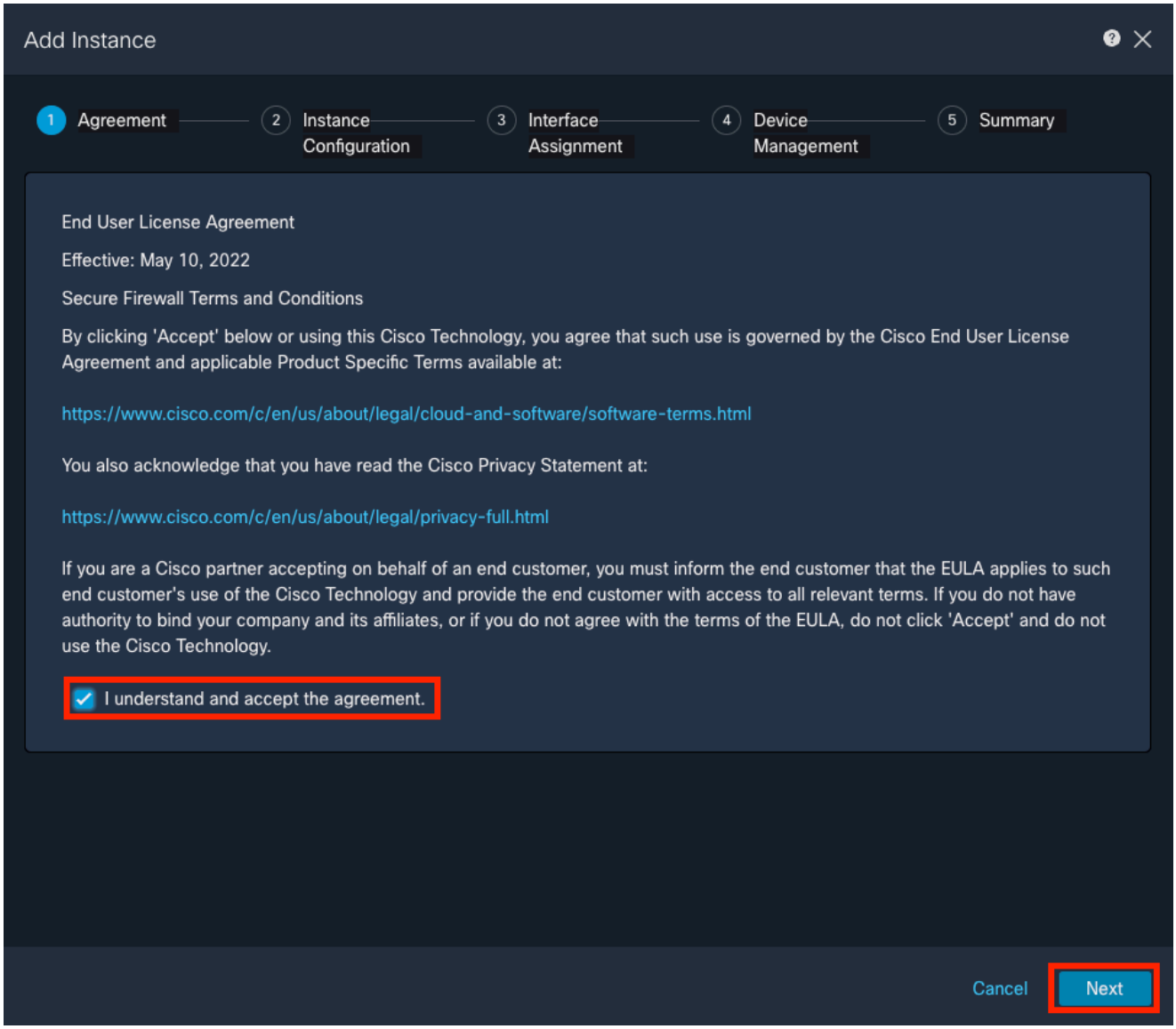
Gestione dello chassis

Passaggio 9. Selezionare il pulsante Istanze, quindi Aggiungi istanza per creare una nuova istanza nello chassis.



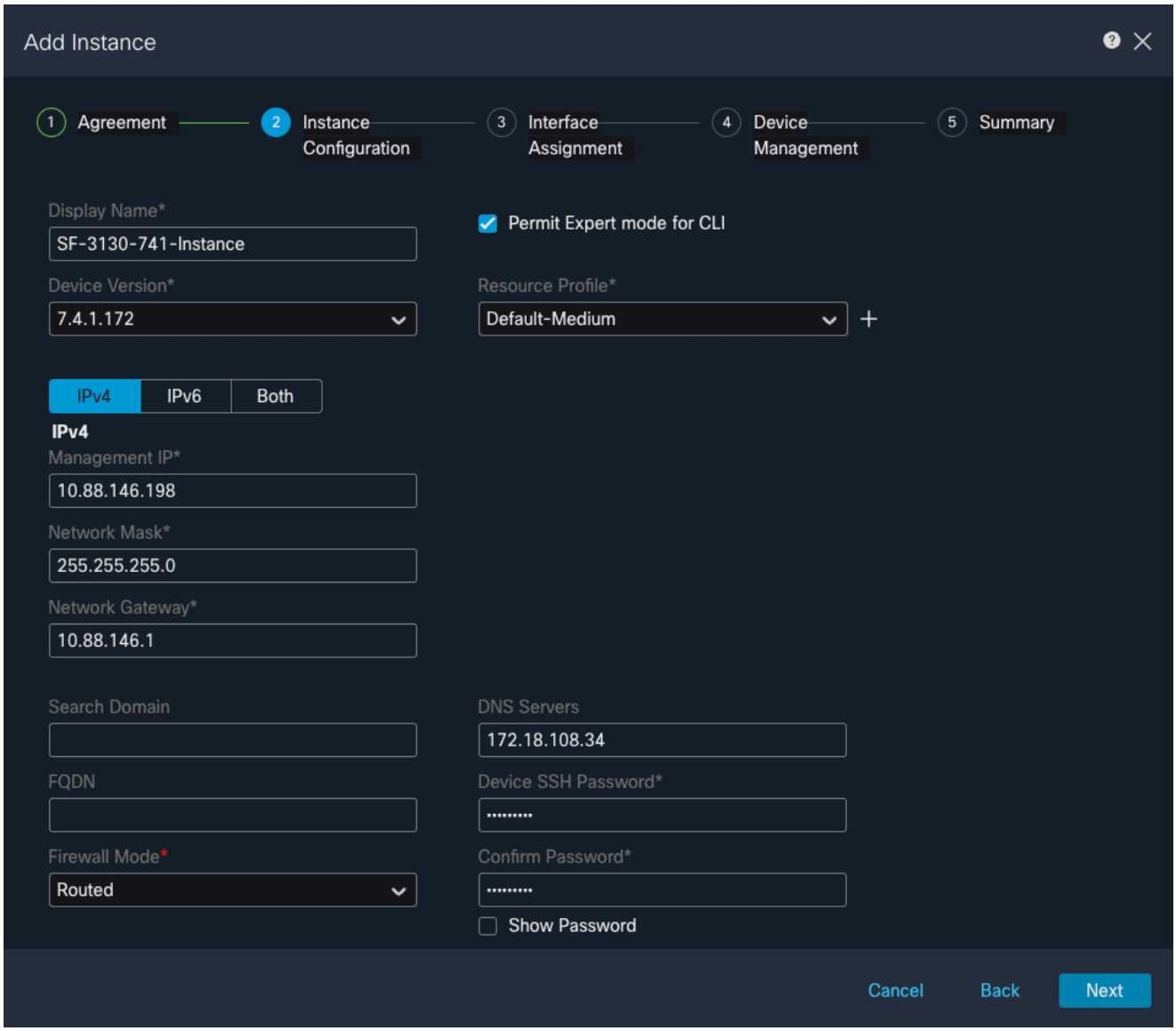
Passaggio 10. Seguire la procedura guidata per completare l'installazione dell'istanza.

1. Accettare il contratto



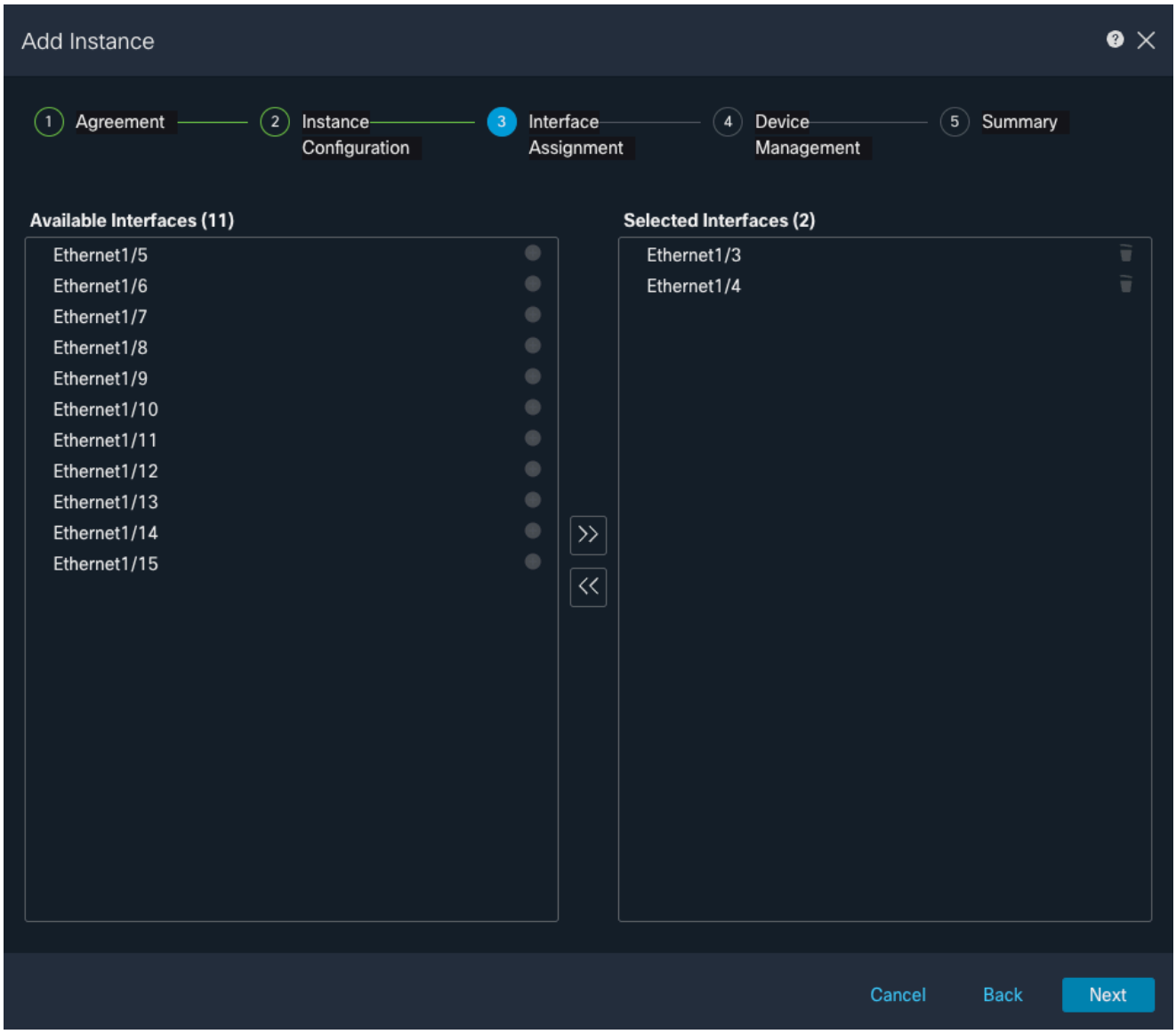
Accetta contratto

2. Configurare i parametri dell'istanza



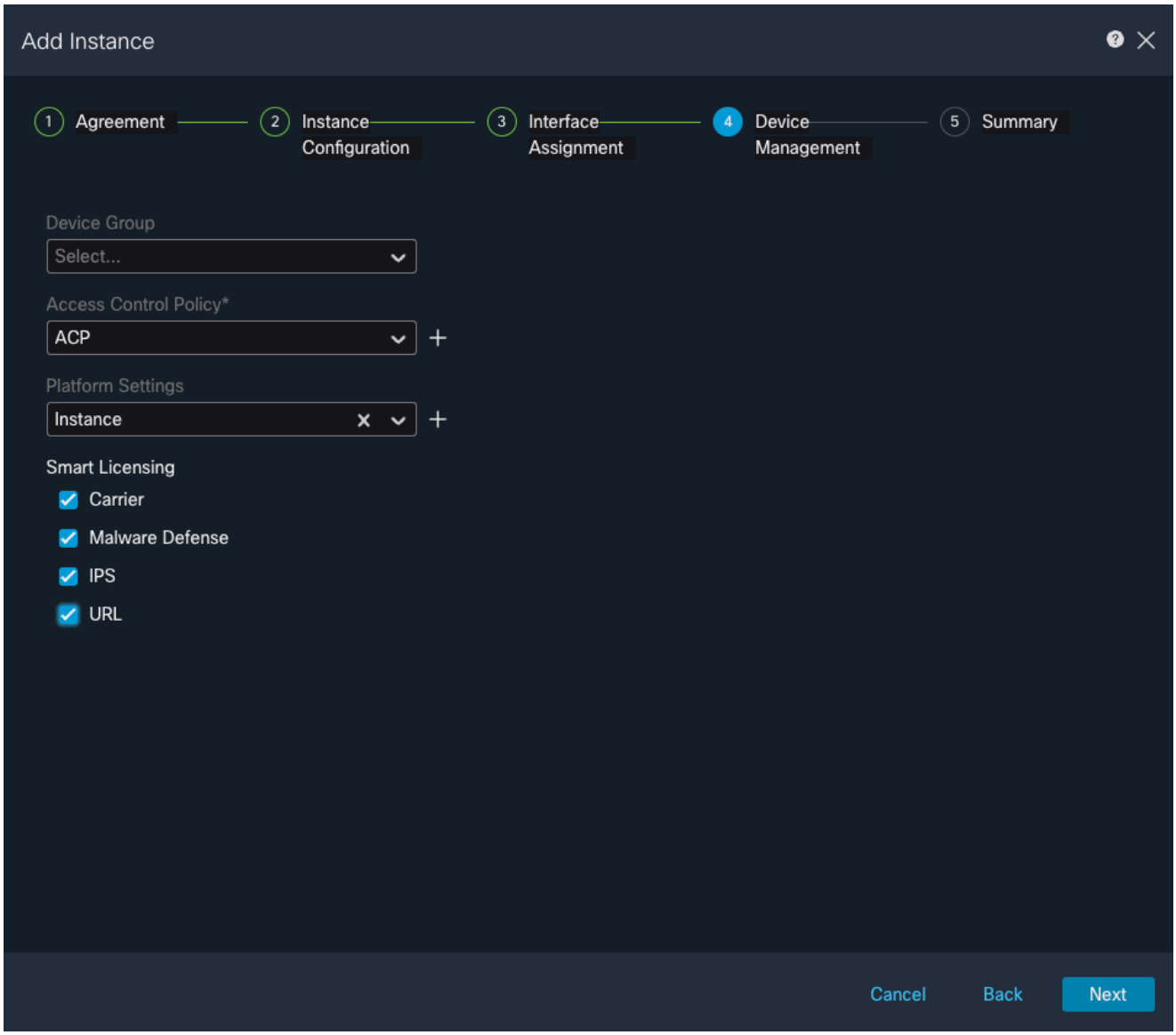
Parametri istanza

3. Selezione interfaccia.



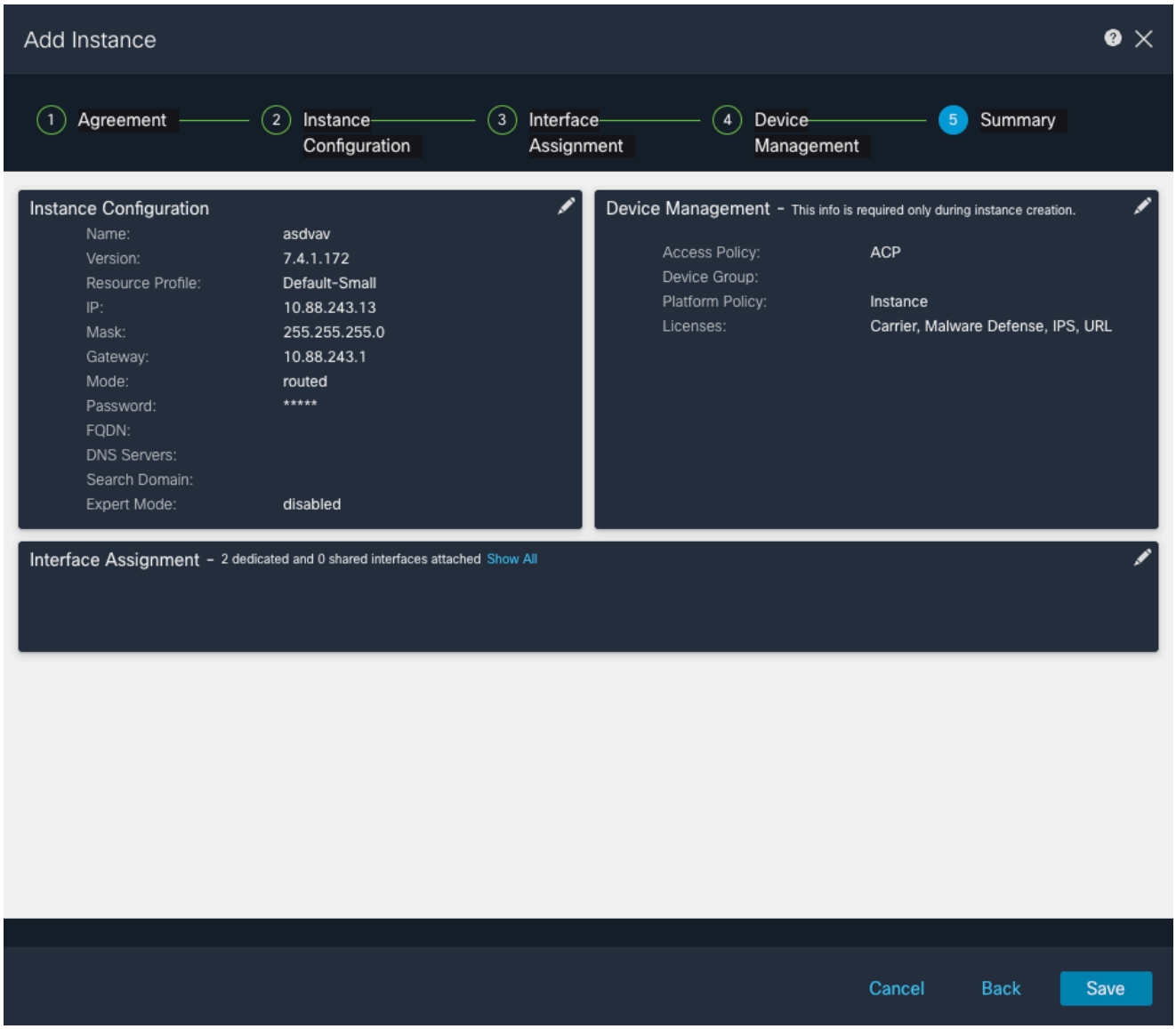
Assegnazione interfaccia

4. Gestione dispositivi.



Gestione dispositivi

5. Riepilogo



Riepilogo dell'istanza

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).