

Configuration de plusieurs instances dans la gamme Secure Firewall 3100

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer pour la version 7.4.1+](#)

Introduction

Ce document décrit comment configurer Multi-Instance dans Secure Firewall 3100 Series exécutant la version 7.4+.

Conditions préalables

Connaissance de Firewall eXtensible Operating System (FXOS) et de l'interface utilisateur graphique de Firewall Management Center (FMC).

Exigences

Accès à :

- Accès par console au pare-feu sécurisé 3100
- Accès à la GUI FMC

Composants utilisés

- Cisco Secure Firewall Management Center version 7.4+
- Pare-feu sécurisé Cisco 3100
 - Sauf 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

En mode multi-instance, vous pouvez déployer plusieurs instances de conteneur sur un seul châssis qui agissent comme des périphériques complètement indépendants.


Configurer pour la version 7.4.1+

Étape 1. Connectez-vous au port de console du châssis.

Le port de console se connecte à l'interface CLI FXOS.

Étape 2. Connectez-vous avec le nom d'utilisateur admin et le mot de passe Admin123.

Vous êtes invité à modifier le mot de passe lors de votre première connexion à FXOS.

 Remarque : si le mot de passe a déjà été modifié et que vous ne le connaissez pas, vous devez réinstaller l'image du périphérique pour réinitialiser le mot de passe par défaut. Reportez-vous [au](#) guide de [dépannage FXOS](#) pour [la procédure de réinstallation](#).

Étape 3. Vérifiez votre mode actuel, Natif ou Conteneur. Si le mode est Native, vous pouvez poursuivre cette procédure pour passer en mode multi-instance (conteneur).

```
firepower# show system detail
```

Exemple :

```
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:
```

Afficher l'état de plusieurs instances

Étape 4. Connectez-vous à la CLI Threat Defense.

firepower# connect ftd

Exemple :



```
firepower# connect ftd
>
```

Connexion à FTD

Étape 5. La première fois que vous vous connectez à la défense contre les menaces, vous êtes invité à accepter le Contrat de licence de l'utilisateur final (CLUF). Le script de configuration de l'interface de ligne de commande s'affiche.

Le script de configuration vous permet de définir l'adresse IP de l'interface de gestion et d'autres paramètres. Cependant, lorsque vous passez en mode multi-instance, les seuls paramètres conservés sont les suivants.

- Mot de passe admin (défini lors de la connexion initiale)
- Serveurs DNS
- Domaines de recherche

Vous réinitialisez l'adresse IP et la passerelle de gestion dans le cadre de la commande du mode multi-instance. Une fois la conversion en mode multi-instance effectuée, vous pouvez modifier les paramètres de gestion dans l'interface de ligne de commande de FXOS. [Voir Modifier les paramètres de gestion du châssis dans l'interface de ligne de commande FXOS.](#)

Étape 6. Activez le mode multi-instance, définissez les paramètres de l'interface de gestion du châssis et identifiez le centre de gestion. Vous pouvez utiliser IPv4 et/ou IPv6. Après avoir entré la commande, vous êtes invité à effacer la configuration et à redémarrer. EnterERASE (toutes les majuscules). Le système redémarre et, dans le cadre du changement de mode, efface la configuration, à l'exception des paramètres réseau de gestion que vous avez définis dans la commande et du mot de passe admin. Le nom d'hôte du châssis est défini sur « firepower-model ».

IPv4:

configuration du réseau à instances multiples

```
ipv4ip_addressnetwork_maskgateway_ip_addressmanagermanager_name  
{hostname | adresse_ipv4 | DONTRESOLVE} registration_keynat_id
```

IPv6 :

configuration du réseau à instances multiples

ipv6ipv6_addressprefix_lengthgateway_ip_addressmanagermanager_name
{hostname | adresse_ipv6 | DONTRESOLVE} registration_keynat_id

Reportez-vous aux composants de gestion suivants :

- {nom de l'hôte | adresse_ipv4 | DONTRESOLVE} : spécifie le nom de domaine complet ou l'adresse IP du centre de gestion. Au moins un des périphériques, soit le centre de gestion ou le châssis, doit avoir une adresse IP accessible pour établir le canal de communication bidirectionnel chiffré SSL entre les deux périphériques. Si vous ne spécifiez pas de nom d'hôte ou d'adresse IP de gestionnaire dans cette commande, alors entrez DONTRESOLVE ; dans ce cas, le châssis doit avoir une adresse IP ou un nom d'hôte accessible, et vous devez spécifier thenat_id.
- registration_key : saisissez une clé d'enregistrement unique de votre choix que vous spécifiez également sur le centre de gestion lorsque vous enregistrez le châssis. La clé d'enregistrement ne doit pas dépasser 37 caractères. Les caractères valides sont les caractères alphanumériques (A-Z, a-z, 0-9) et le trait d'union (-).
- nat_id : spécifie une chaîne unique et unique de votre choix que vous spécifiez également sur le centre de gestion lorsque vous enregistrez le châssis lorsqu'un côté ne spécifie pas d'adresse IP ou de nom d'hôte accessible. Elle est obligatoire si vous ne spécifiez pas d'adresse de gestionnaire ou de nom d'hôte. Toutefois, nous vous recommandons de toujours définir l'ID NAT même si vous spécifiez un nom d'hôte ou une adresse IP. L'ID NAT ne doit pas dépasser 37 caractères. Les caractères valides sont les caractères alphanumériques (A-Z, a-z, 0-9) et le trait d'union (-). Cet ID ne peut pas être utilisé pour d'autres périphériques s'enregistrant auprès du centre de gestion.

Pour repasser en mode appliance, vous devez utiliser l'interface de ligne de commande de FXOS et le système enterscope, puis définir le mode de déploiement natif. [Voir Modifier les paramètres de gestion du châssis dans l'interface de ligne de commande FXOS.](#)

Exemple :


```
> 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
```

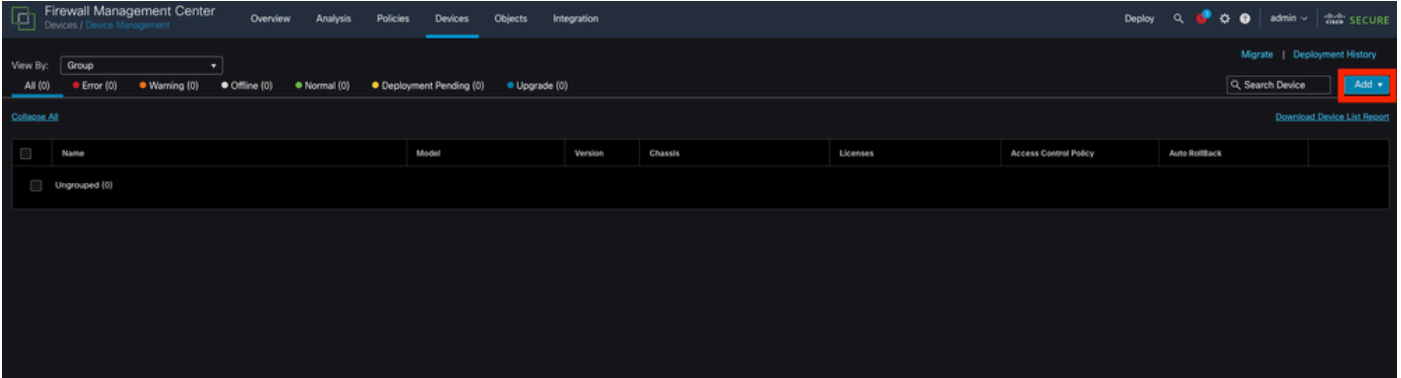
Passage en mode multi-instance

 Remarque : ajoutez le châssis multi-instance au centre de gestion. Le centre de gestion et le châssis partagent une connexion de gestion séparée à l'aide de l'interface de gestion du châssis. Vous pouvez utiliser le centre de gestion pour configurer tous les paramètres du

 châssis ainsi que les instances. Le gestionnaire de châssis Secure Firewall ou la configuration de l'interface de ligne de commande FXOS n'est pas pris en charge.

Étape 7. Dans le centre de gestion, ajoutez le châssis en utilisant l'adresse IP ou le nom d'hôte de gestion du châssis.

- Choisissez Périphériques>Gestion des périphériques, puis Ajouter>Châssis.



The screenshot shows the Firewall Management Center (FMC) interface. The 'Devices' tab is selected in the top navigation bar. The main area displays a table of devices with columns for Name, Model, Version, Chassis, Licenses, Access Control Policy, and Auto Rollback. The table currently shows one entry: 'Ungrouped (0)'. A red box highlights the 'Add' button in the top right corner of the device management area.

Ajout du châssis au contrôleur FMC

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†

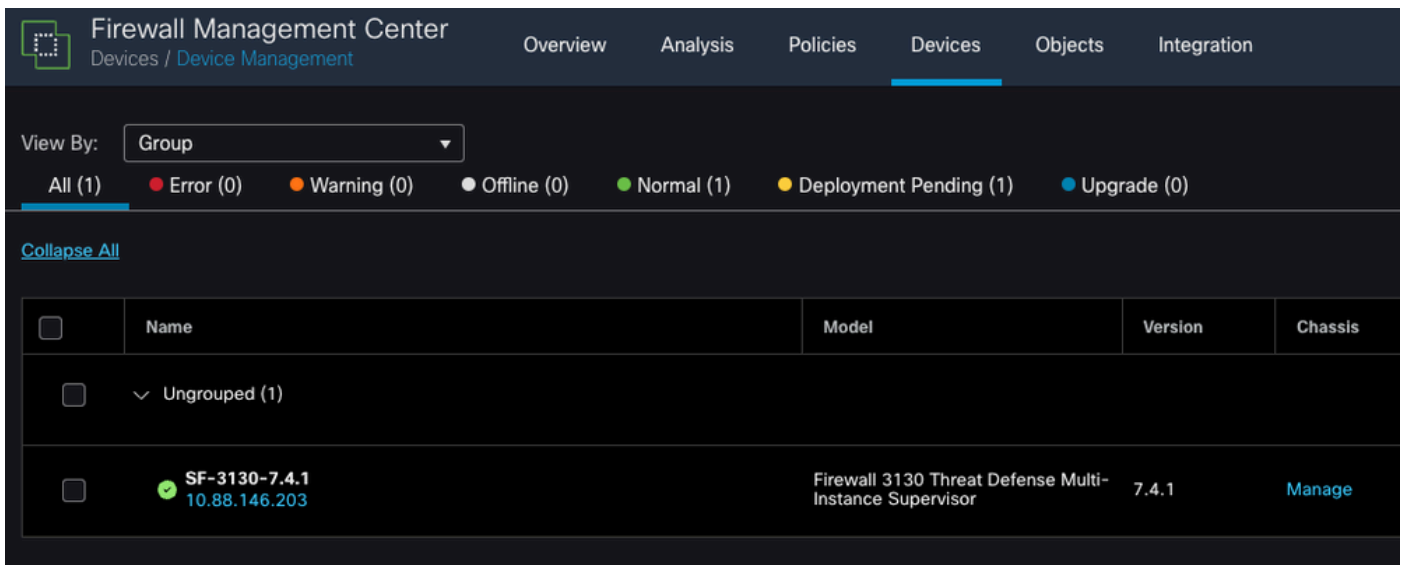
† Either host or NAT ID is required.

Cancel

Submit

Paramètres de configuration du châssis

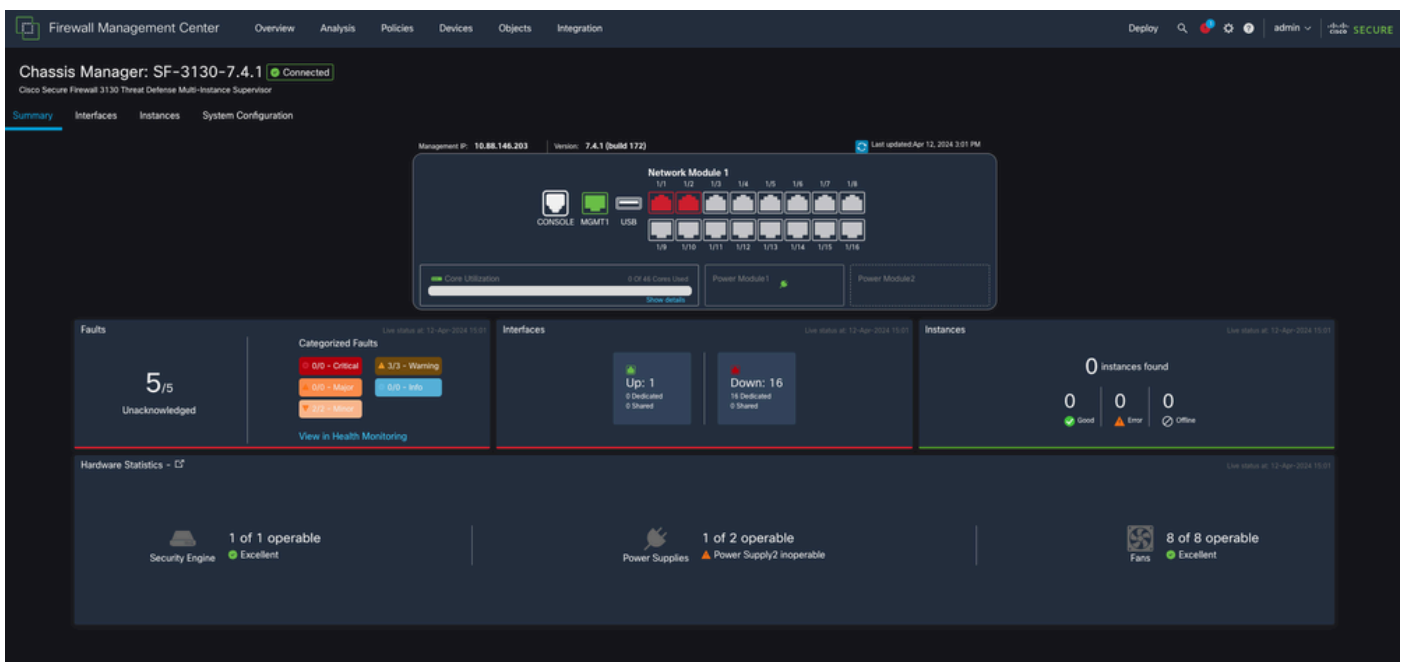
- Une fois le châssis ajouté au FMC, consultez le périphérique dans la liste des périphériques sur le FMC.



Châssis ajouté dans le FMC

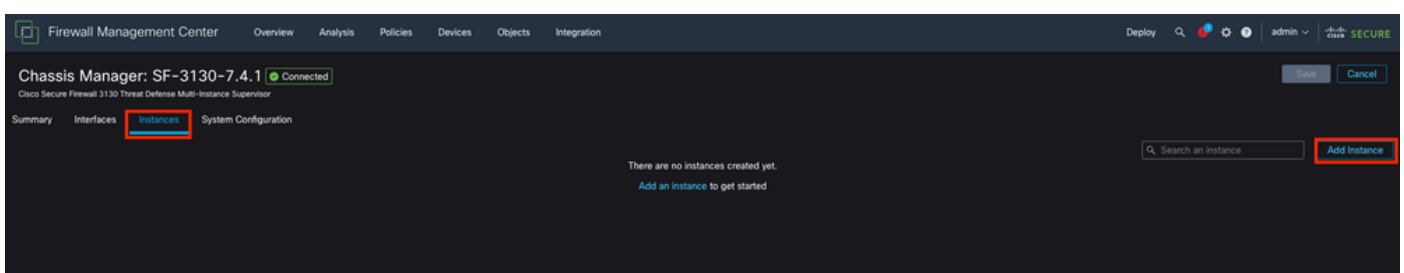
Étape 8. Pour afficher et configurer le châssis, cliquez sur **Gérer** dans la colonne **Châssis**, ou cliquez sur **Modifier** (✎).

La page **Chassis Manager** s'ouvre pour le châssis et affiche la page **Summary**.



Gestion du châssis

Étape 9. Cliquez sur le bouton **Instances**, puis sur **Add Instance** pour créer une instance dans le châssis.



Étape 10. Suivez les instructions de l'assistant pour terminer l'installation de l'instance.

1. Accepter le contrat

Add Instance

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

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.

Cancel Next

Accepter le contrat

2. Configurer les paramètres d'instance

Add Instance ? X

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*
.....

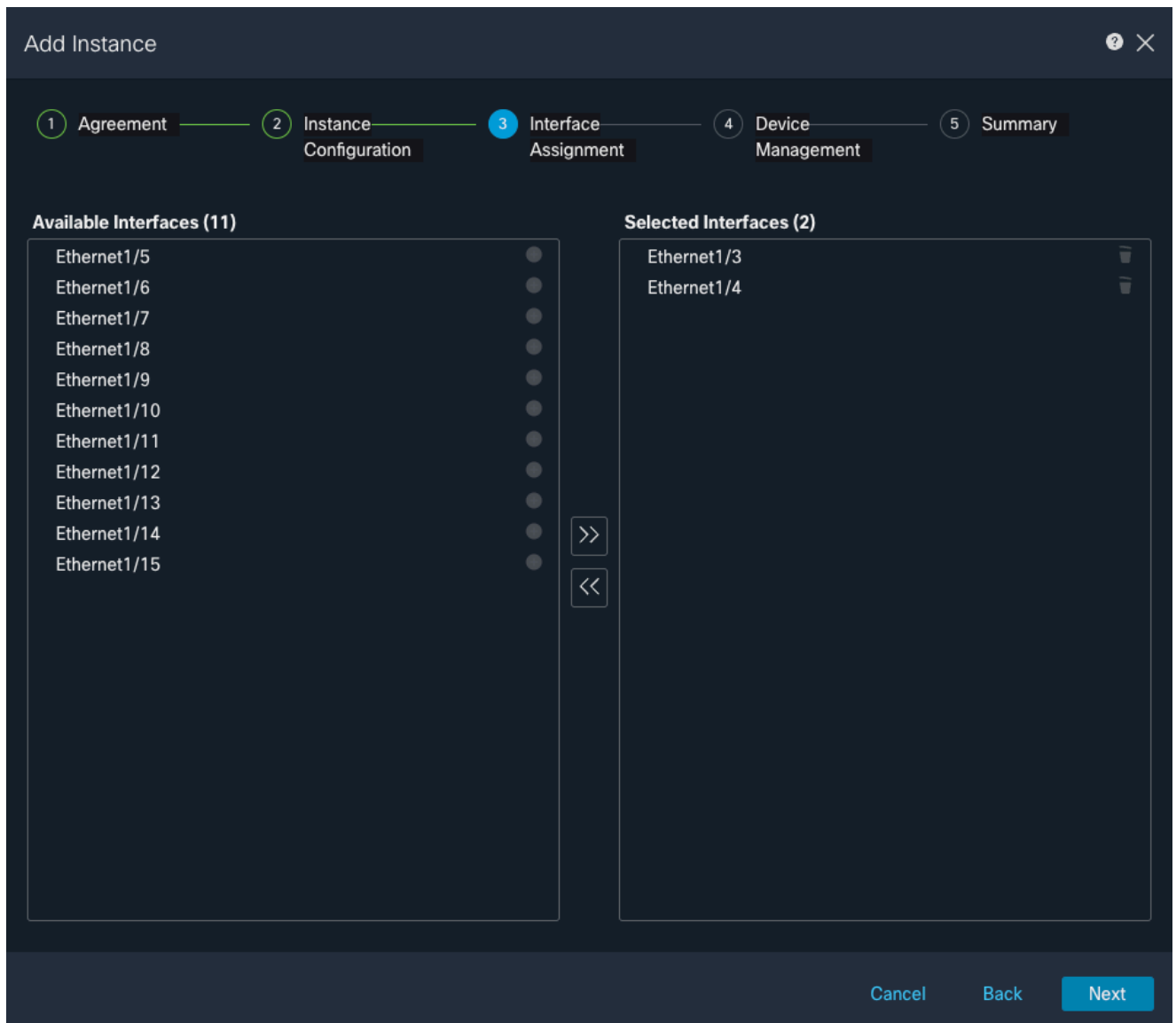
Confirm Password*
.....

Show Password

Cancel Back **Next**

Paramètres d'instance

3. Sélection d'interface.



Attribution d'interface

4. Gestion des périphériques.

Add Instance ? X

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**

Gestion des périphériques

5. Résumé

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

Résumé de l'instance

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.