Approvisionnement de pare-feu ASA sécurisé vers CSM

Table des matières

Introduction

Ce document décrit le processus de provisionnement de l'appliance de sécurité adaptatif (ASA) de pare-feu sécurisé sur Cisco Security Manager (CSM).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pare-feu sécurisé ASA
- CSM

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu sécurisé ASA version 9.18.3
- CSM version 4.28

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

CSM permet l'application cohérente des politiques et le dépannage rapide des événements de sécurité, en proposant des rapports récapitulatifs sur l'ensemble du déploiement de la sécurité. Grâce à son interface centralisée, les entreprises peuvent évoluer efficacement et gérer un large éventail de périphériques de sécurité Cisco avec une visibilité améliorée.

Configurer

Dans l'exemple suivant, un ASA virtuel est provisionné sur un CSM pour une gestion centralisée.

Configurations

Configurer ASA pour la gestion HTTPS

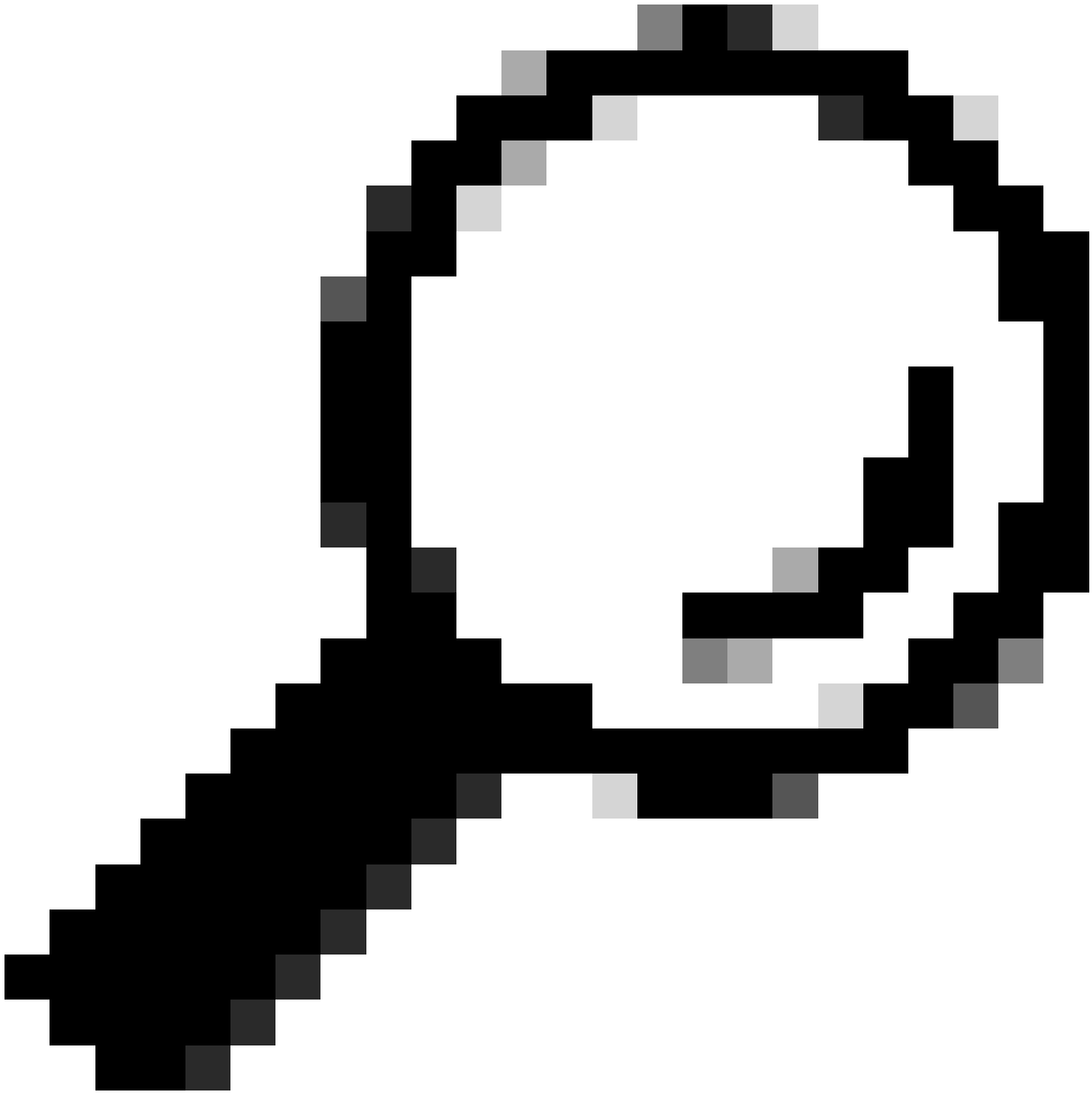
Étape 1. Créez un utilisateur avec tous les privilèges.

Syntaxe de ligne de commande (CLI) :

```
configure terminal
username < user string > password < password > privilege < level number >
```

Ceci se traduit par l'exemple de commande suivant, qui a l'utilisateur csm-user et le mot de passe cisco123 comme suit :

```
ciscoasa# configure terminal
ciscoasa(config)# username csm-user password cisco123 privilege 15
```



Conseil : les utilisateurs authentifiés en externe sont également acceptés pour cette intégration.

Étape 2. Activez le serveur HTTP.

Syntaxe de ligne de commande (CLI) :

```
configure terminal
http server enable
```

Étape 3. Autorisez l'accès HTTPS pour l'adresse IP du serveur CSM.

Syntaxe de ligne de commande (CLI) :

```
configure terminal
http < hostname > < netmask > < interface name >
```

Ceci se traduit par l'exemple de commande suivant, qui permet à n'importe quel réseau d'accéder à l'ASA via HTTPS sur l'interface externe (GigabitEthernet0/0) :

```
ciscoasa# configure terminal
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

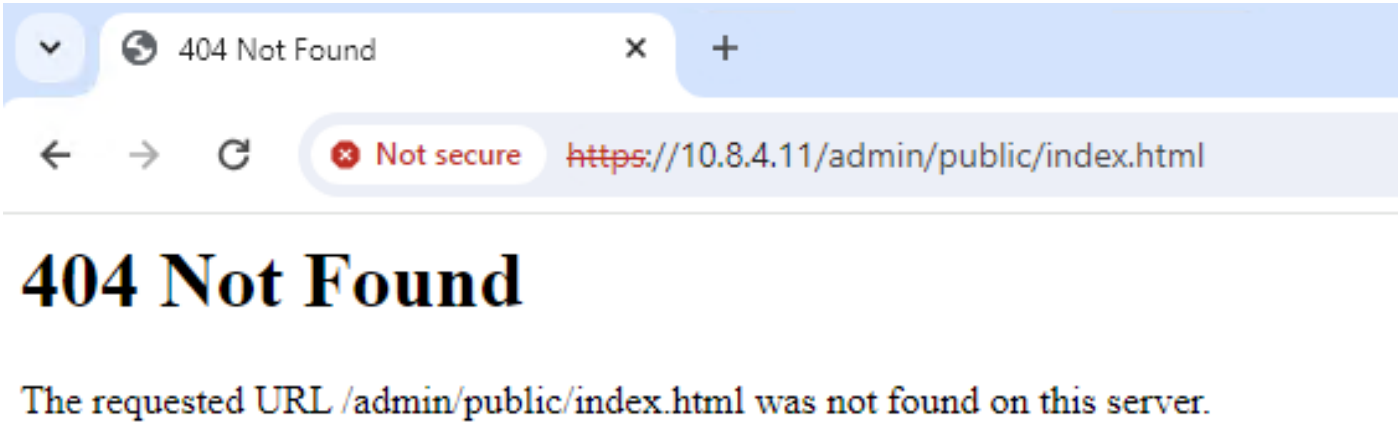
Étape 4. Vérifiez que HTTPS est accessible à partir du serveur CSM.

Ouvrez un navigateur Web et entrez la syntaxe suivante :

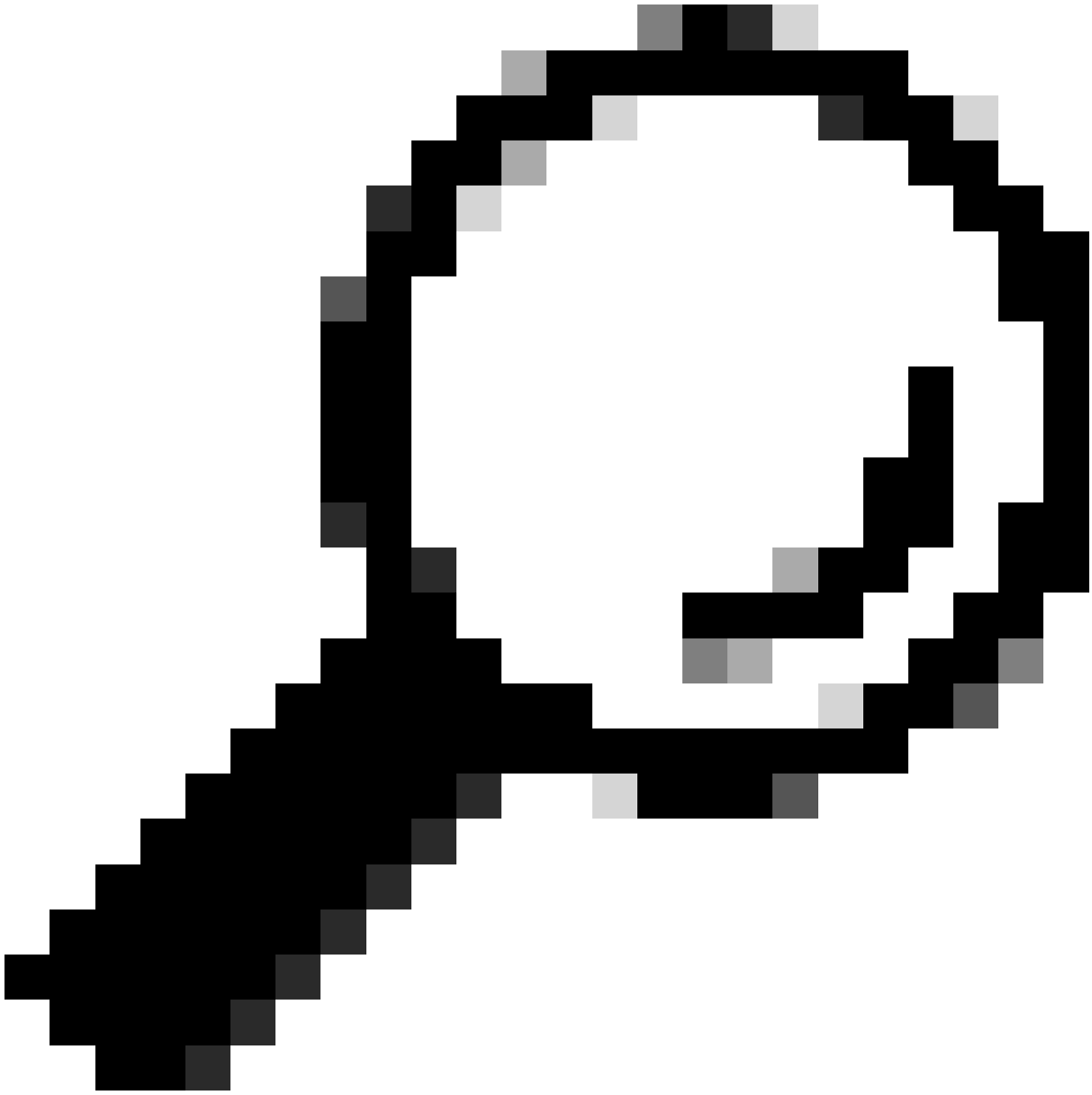
```
https://< ASA IP address >/
```

Cela se traduit par l'exemple suivant pour l'adresse IP de l'interface externe qui était autorisée pour l'accès HTTPS à l'étape précédente :

```
https://10.8.4.11/
```



Réponse HTTPS ASA



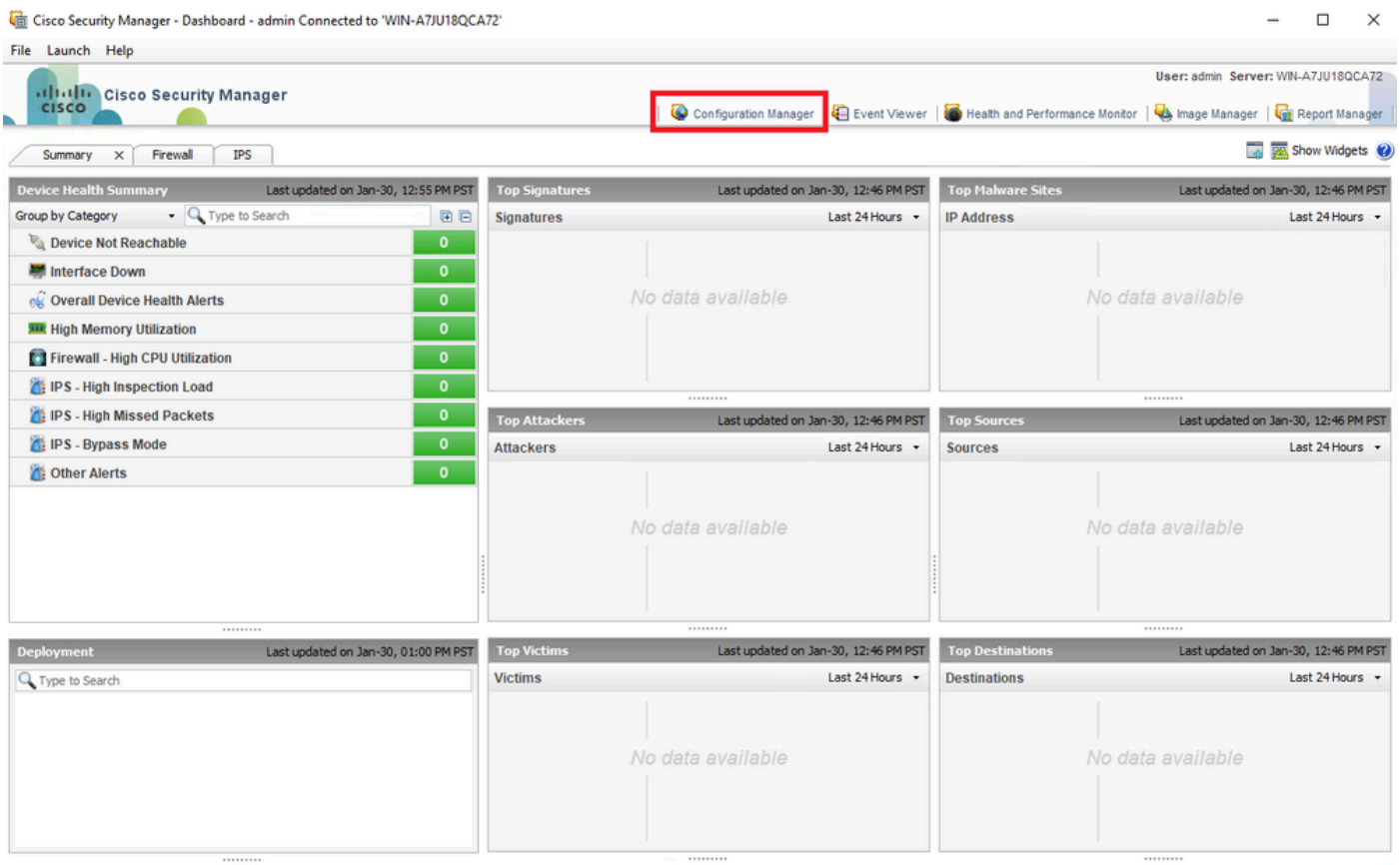
Conseil : l'erreur 404 Not Found est attendue à cette étape, car Cisco Adaptive Security Device Manager (ASDM) n'est pas installé sur cet ASA, mais la réponse HTTPS est présente car la page redirige vers l'URL /admin/public/index.html.

Approvisionnement de pare-feu ASA sécurisé vers CSM

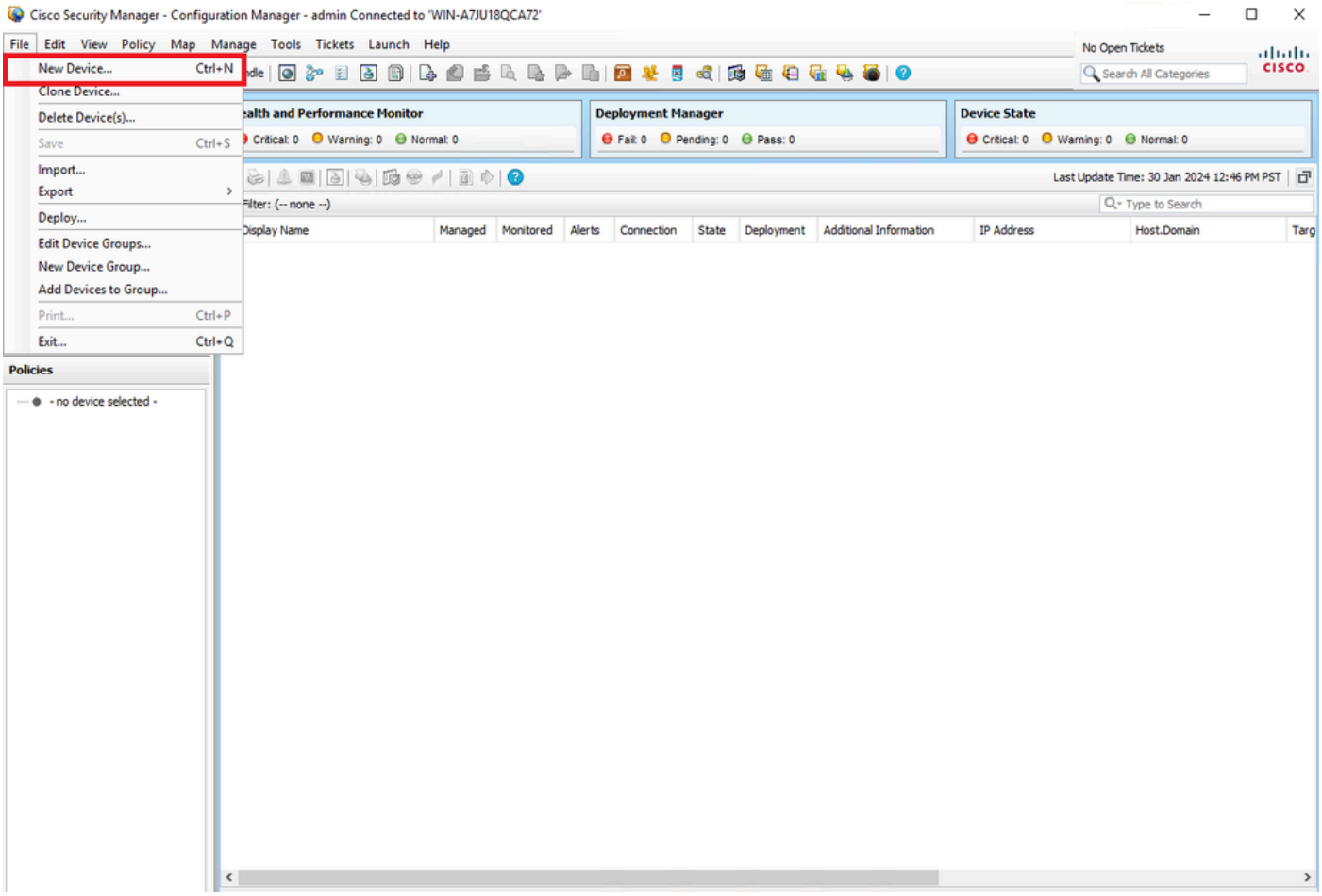
Étape 1. Ouvrez et connectez-vous au client CSM.

Connexion du client CSM

Étape 2. Ouvrez le Gestionnaire de configuration.

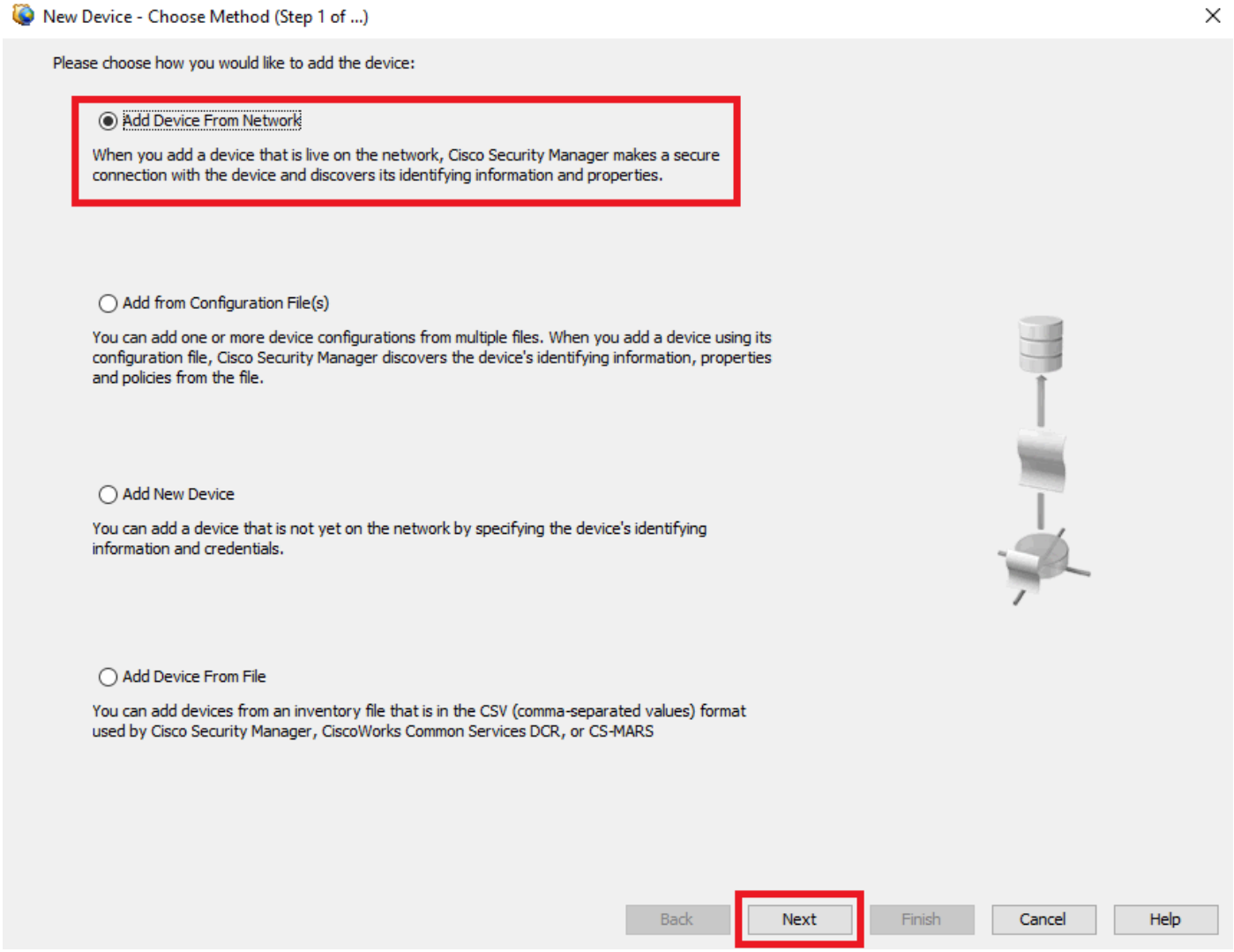


Étape 3. Accédez à Périphériques > Nouveau périphérique.



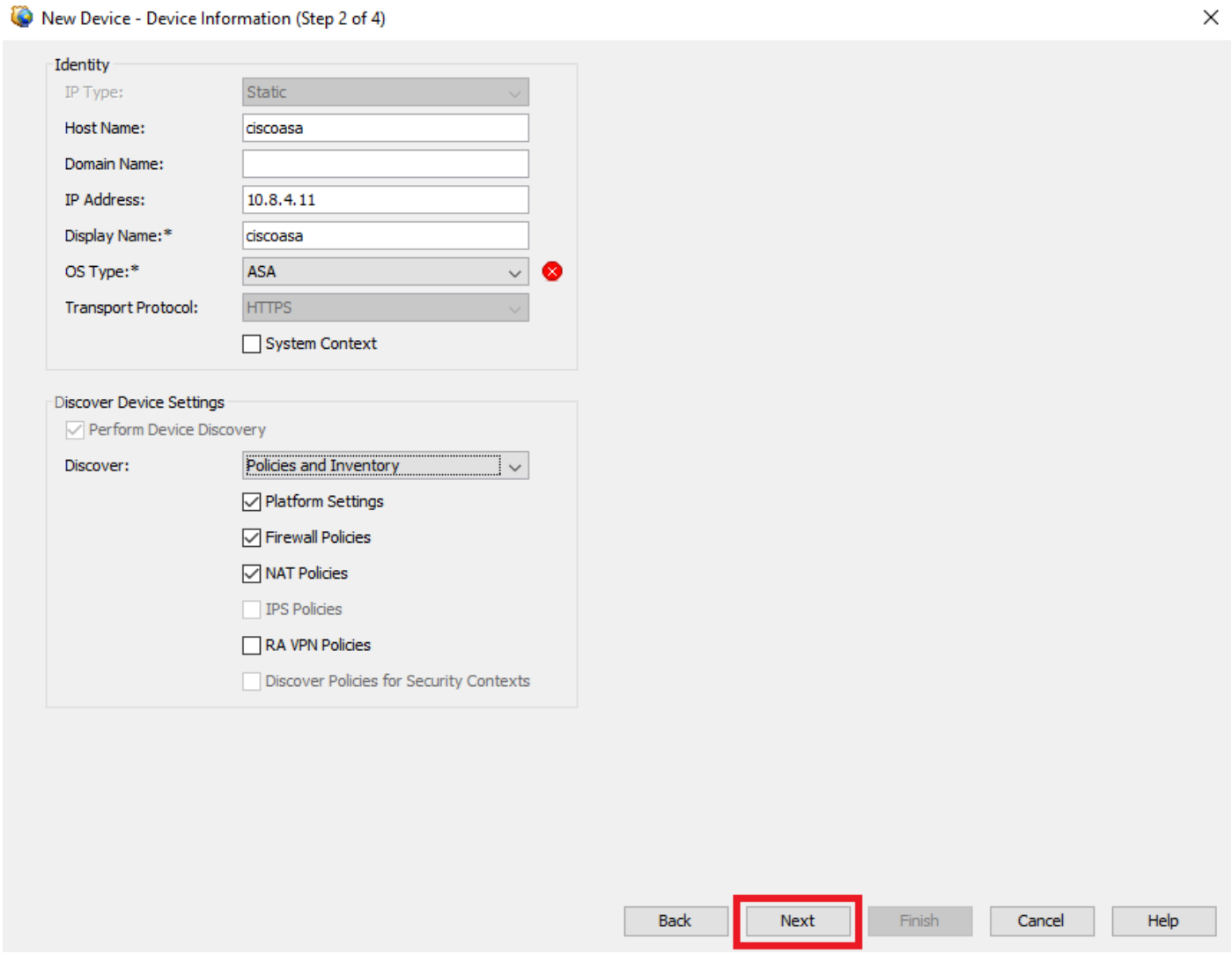
Gestionnaire de configuration CSM

Étape 4. Sélectionnez l'option d'ajout qui répond au besoin en fonction du résultat souhaité. Comme l'ASA configuré est déjà configuré dans le réseau, la meilleure option pour cet exemple est **Add Device From Network** et cliquez sur **Next**.



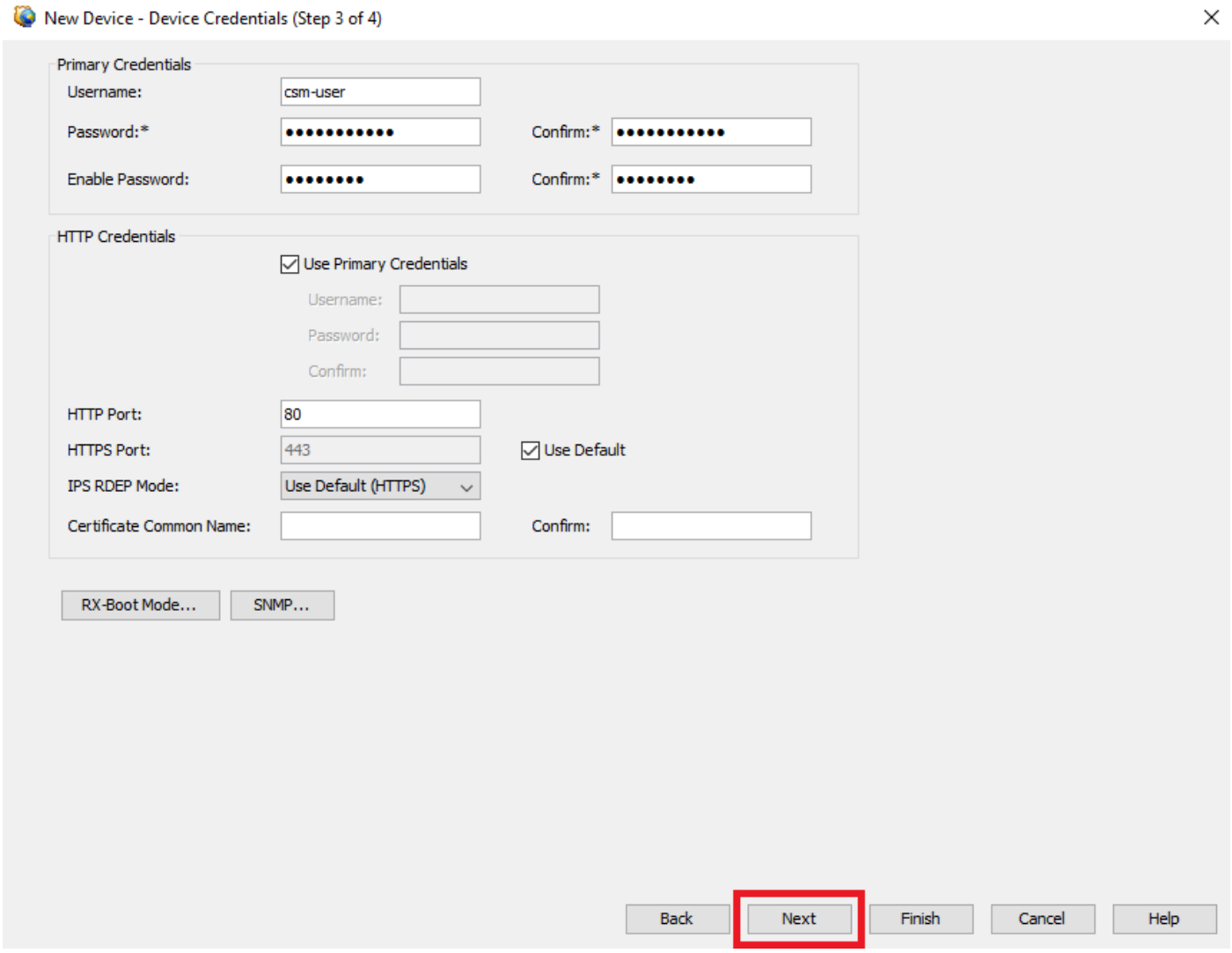
Device Add, méthode

Étape 5. Complétez les données requises en fonction de la configuration du pare-feu ASA sécurisé et des paramètres de détection. Cliquez ensuite sur **Next**.



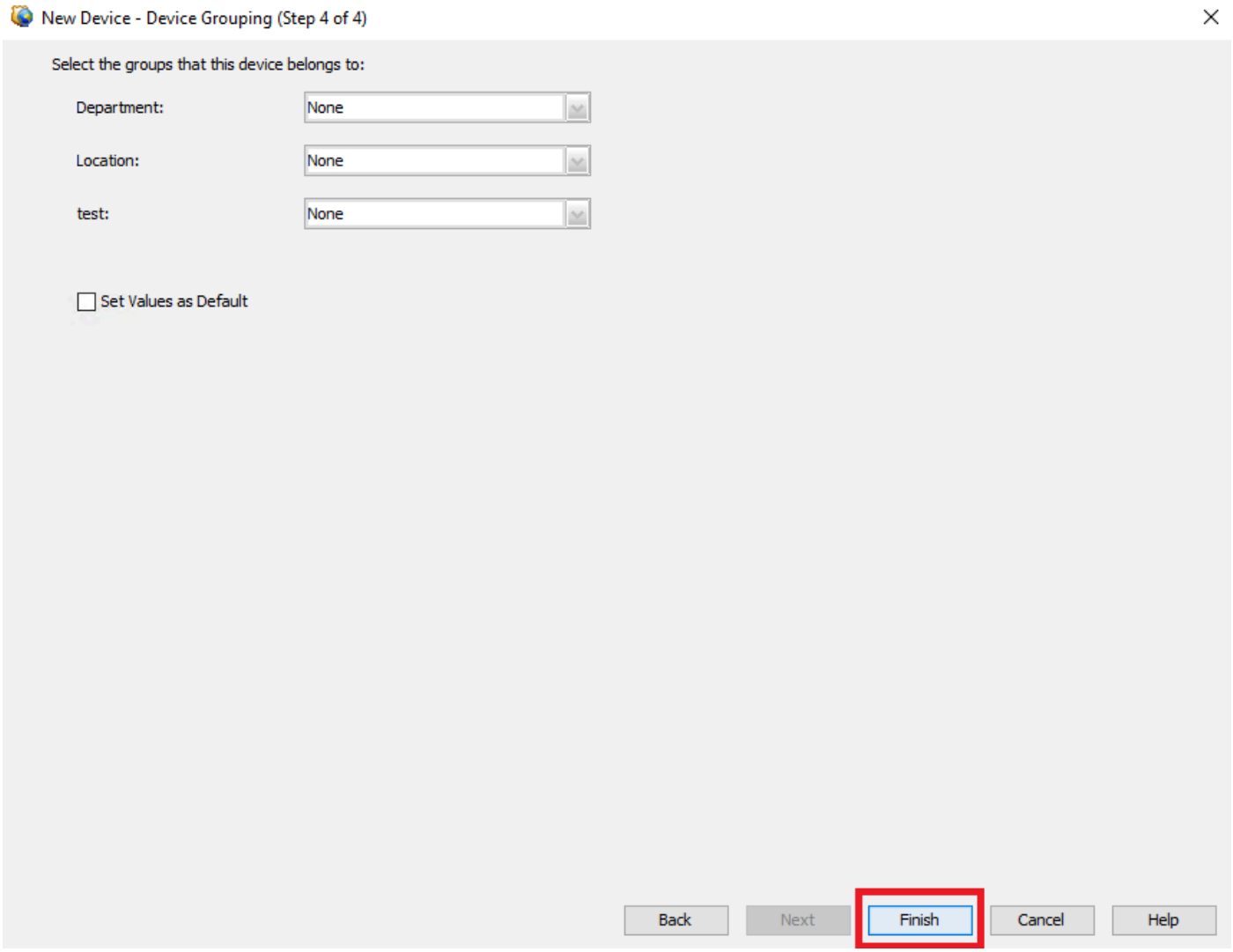
Paramètres ASA

Étape 6. Remplissez les informations d'identification requises à la fois de l'utilisateur CSM configuré sur ASA et du mot de passe **enable**.



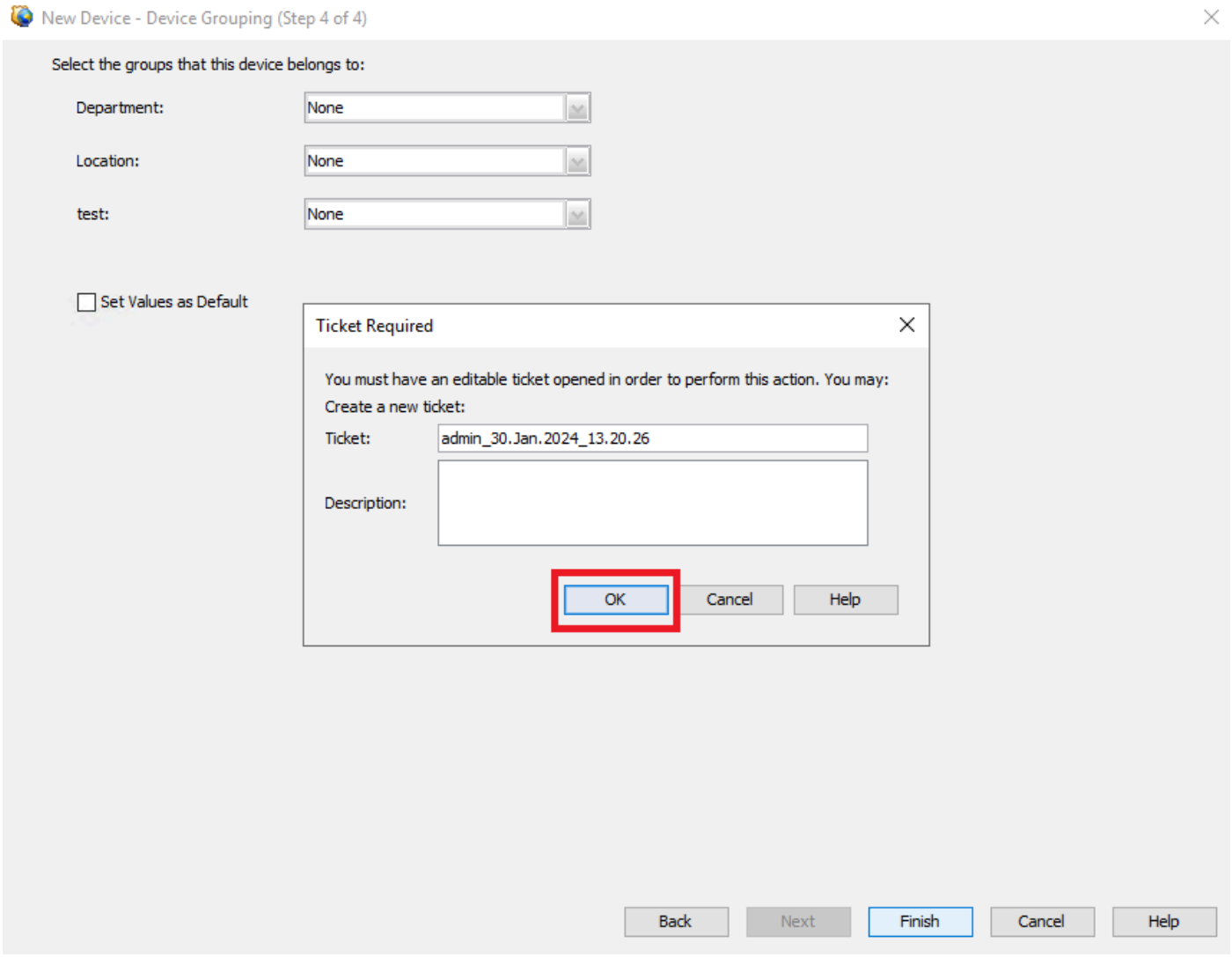
Identifiants ASA

Étape 7. Sélectionnez les groupes souhaités ou ignorez cette étape si aucune n'est requise et cliquez sur **Terminer**.



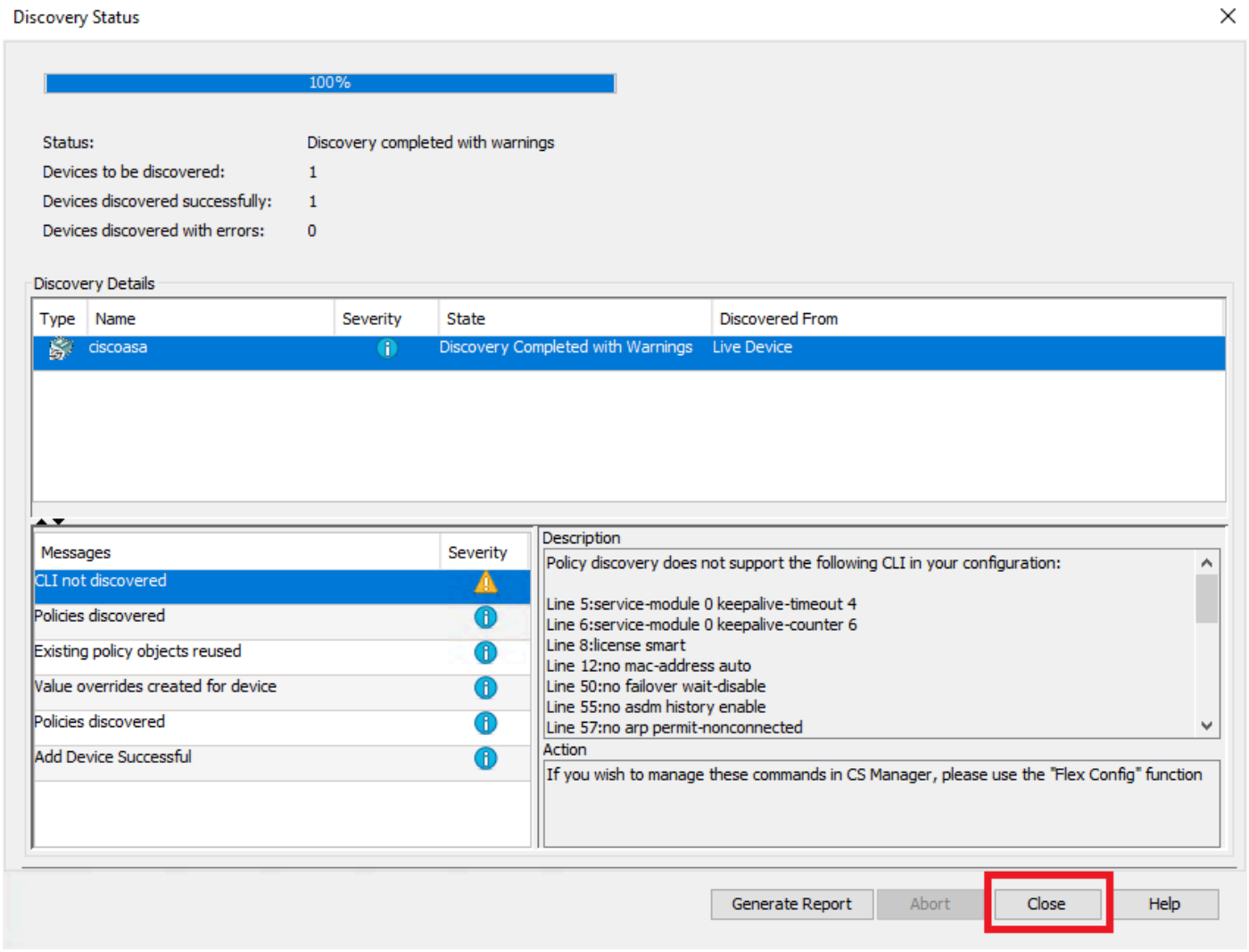
Sélection de groupe CSM

Étape 8. Une demande de ticket est générée à des fins de contrôle, cliquez sur **OK**.

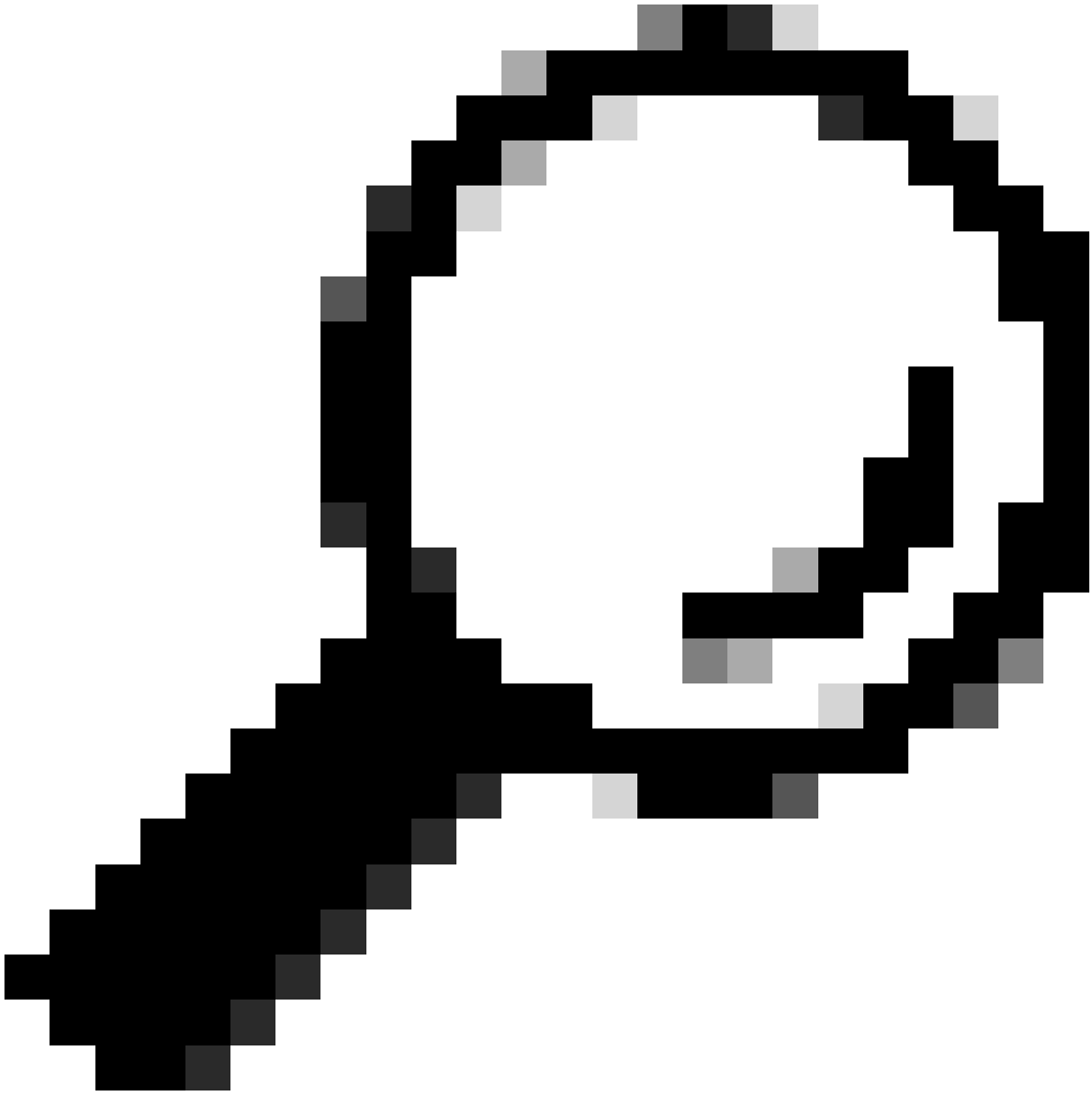


Création de tickets CSM

Étape 9. Vérifiez que la détection se termine sans erreurs et cliquez sur **Close**.

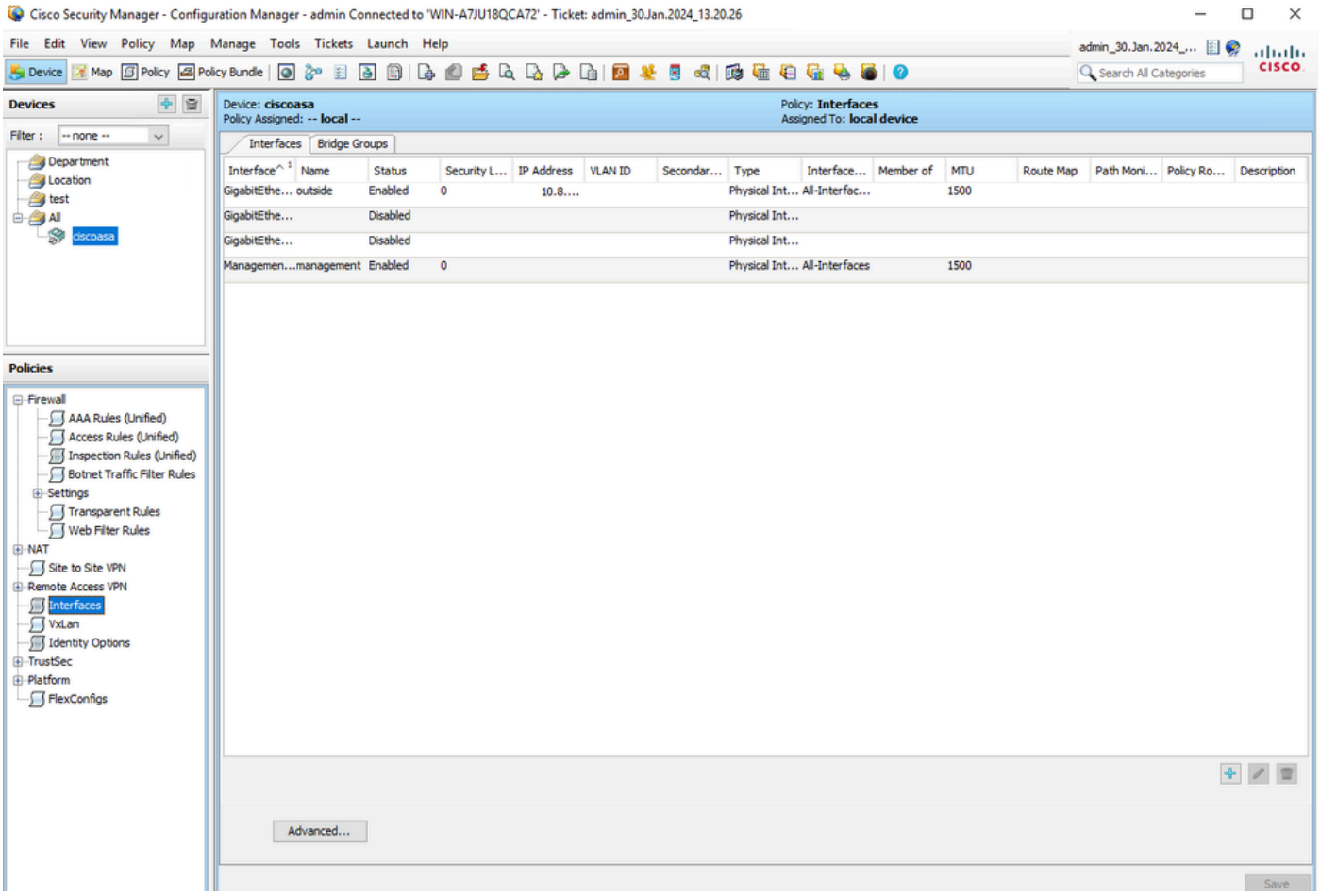


Détection ASA



Conseil : les avertissements sont acceptés comme résultats positifs, car toutes les fonctionnalités ASA ne sont pas prises en charge par CSM.

Étape 10. Vérifiez que l'ASA apparaît désormais comme enregistré sur le client CSM et affiche les informations correctes.



Informations ASA enregistrées

Vérifier

Un débogage HTTPS est disponible sur ASA à des fins de dépannage. La commande suivante est utilisée :

```
debug http
```

Voici un exemple de débogage réussi d'inscription CSM :

```
ciscoasa# debug http debug http enabled at level 1. ciscoasa# HTTP: processing handoff to legacy admin
```

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.