Configurer l'authentification externe sur Catalyst Center à l'aide de Windows Server

Table des matières

Introduction

Ce document décrit comment configurer l'authentification externe dans Cisco DNA Center à l'aide de Network Policy Server (NPS) dans Windows Server en tant que RADIUS.

Conditions préalables

Exigences

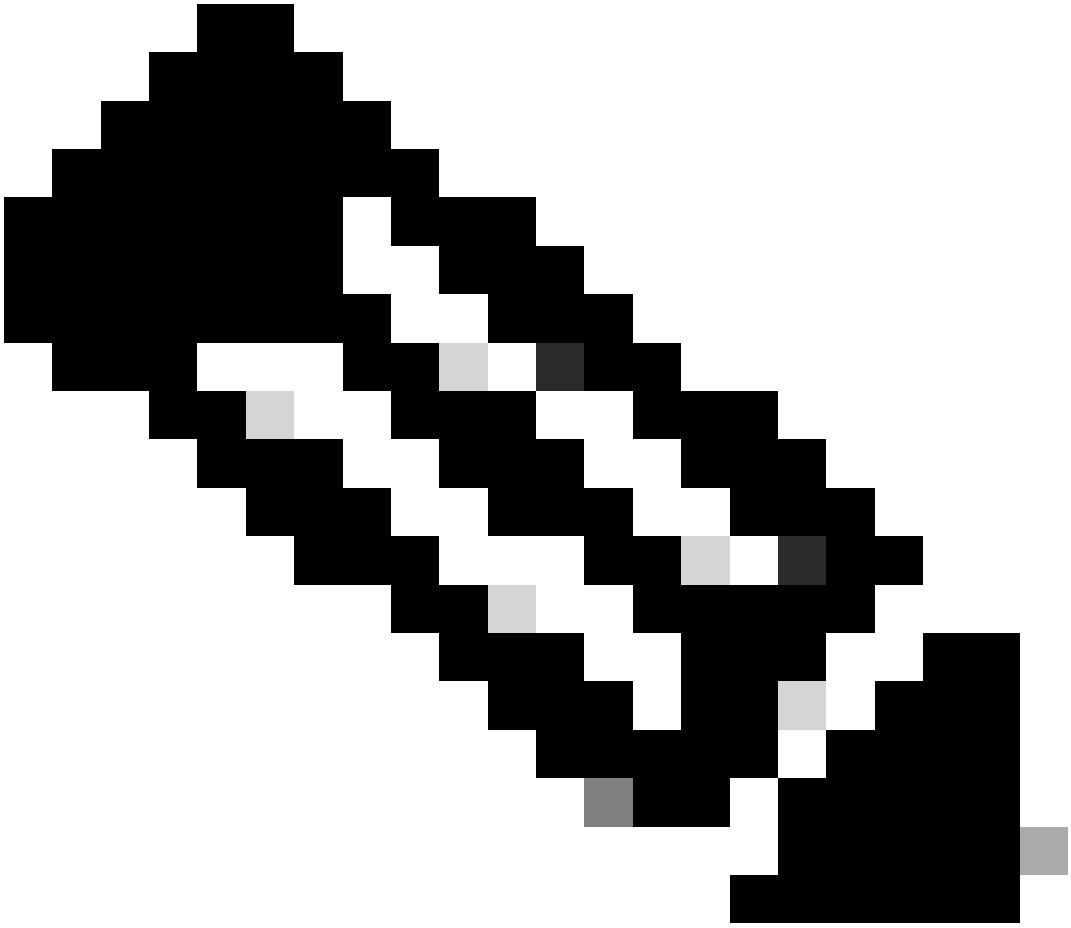
Connaissances de base sur :

- Utilisateurs et rôles de Cisco DNA Center
- Serveur de stratégie réseau Windows Server, RADIUS et Active Directory

Composants utilisés

- Cisco DNA Center 2.3.5.x
- Microsoft Windows Server Version 2019 agissant comme contrôleur de domaine, serveur DNS, NPS et Active Directory

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.

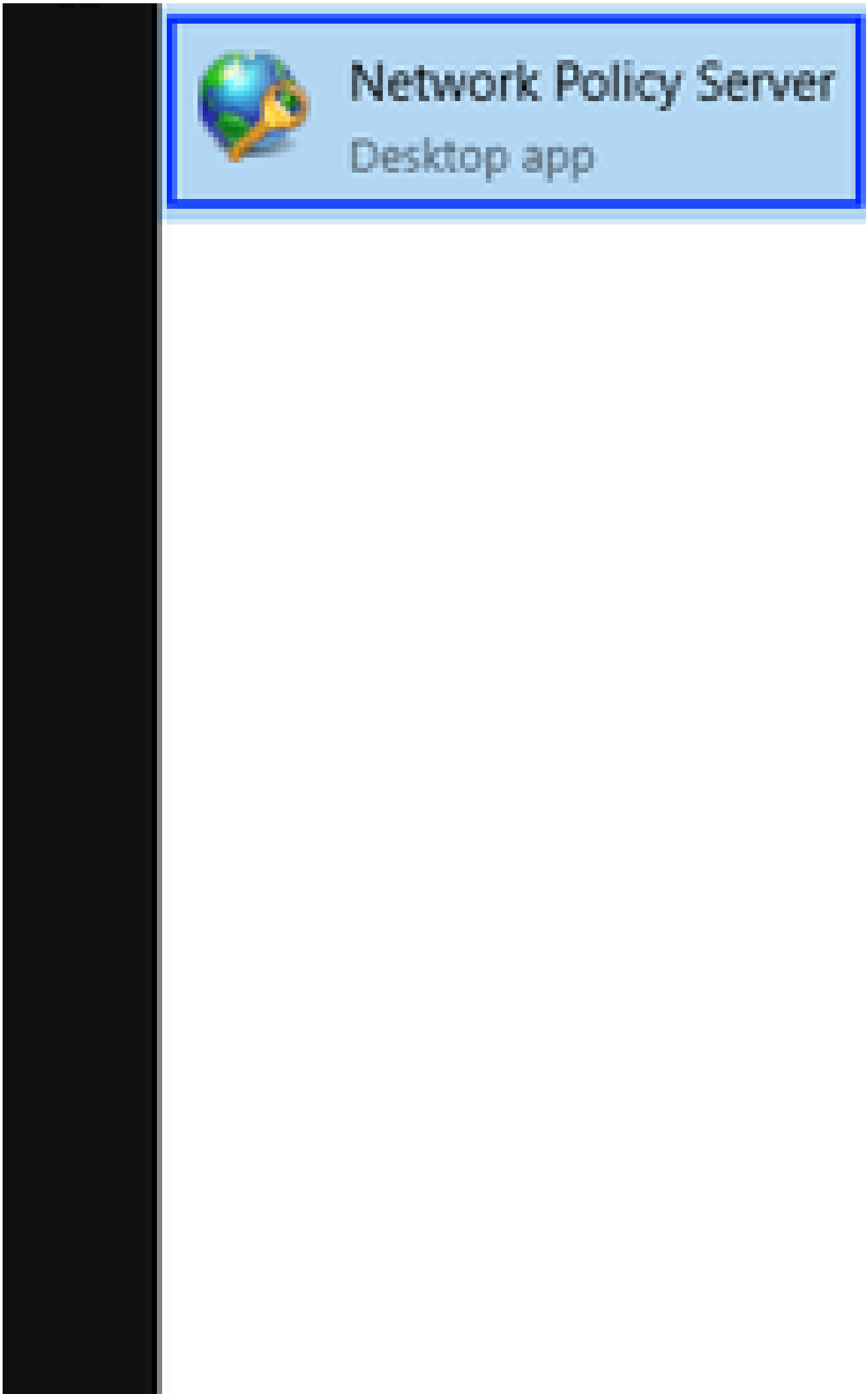


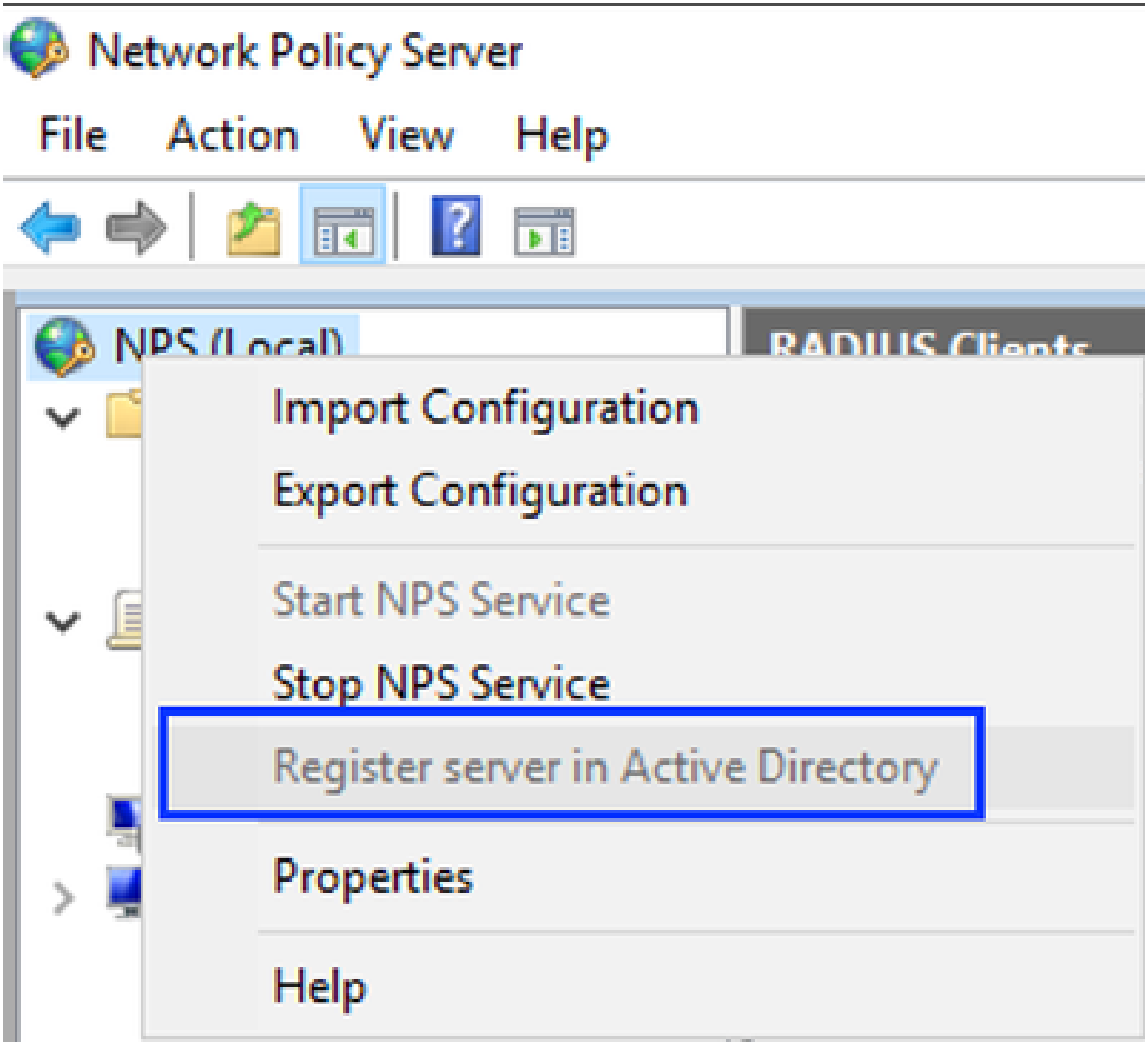
Remarque : le centre d'assistance technique Cisco (TAC) ne fournit pas d'assistance technique pour Microsoft Windows Server. Si vous rencontrez des problèmes avec la configuration de Microsoft Windows Server, contactez le support technique de Microsoft pour obtenir une assistance technique.

Configurer

Stratégie de rôle Admin

1. Cliquez sur dans le menu Démarrer de Windows et recherchez NPS. Sélectionnez ensuite Network Policy Server :

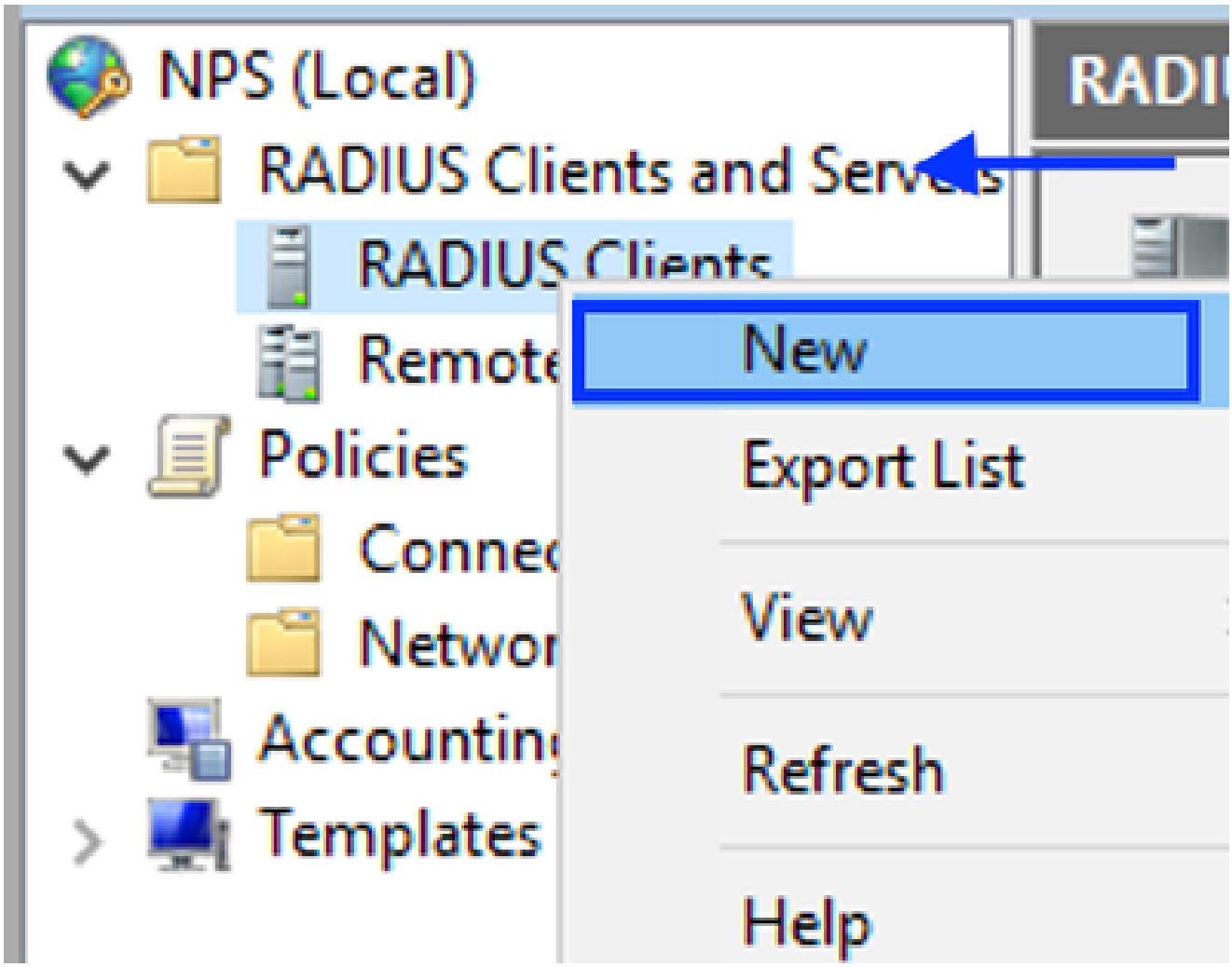

Network Policy Server
Desktop app



Service de stratégie réseau Windows

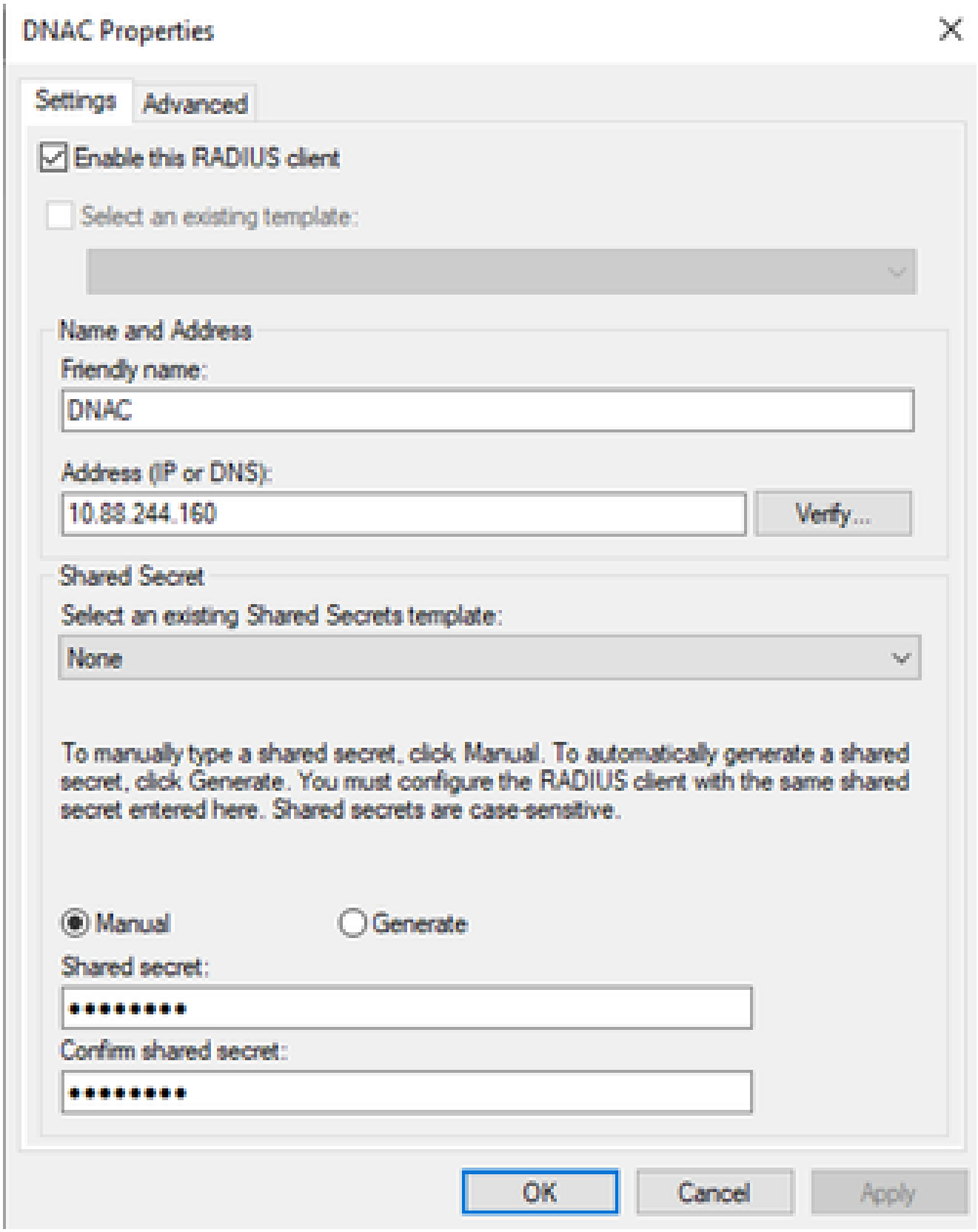
3. Cliquez sur OK deux fois.

4. Développez Clients et serveurs RADIUS, cliquez avec le bouton droit sur Clients RADIUS, puis sélectionnez Nouveau :



Ajouter un client RADIUS

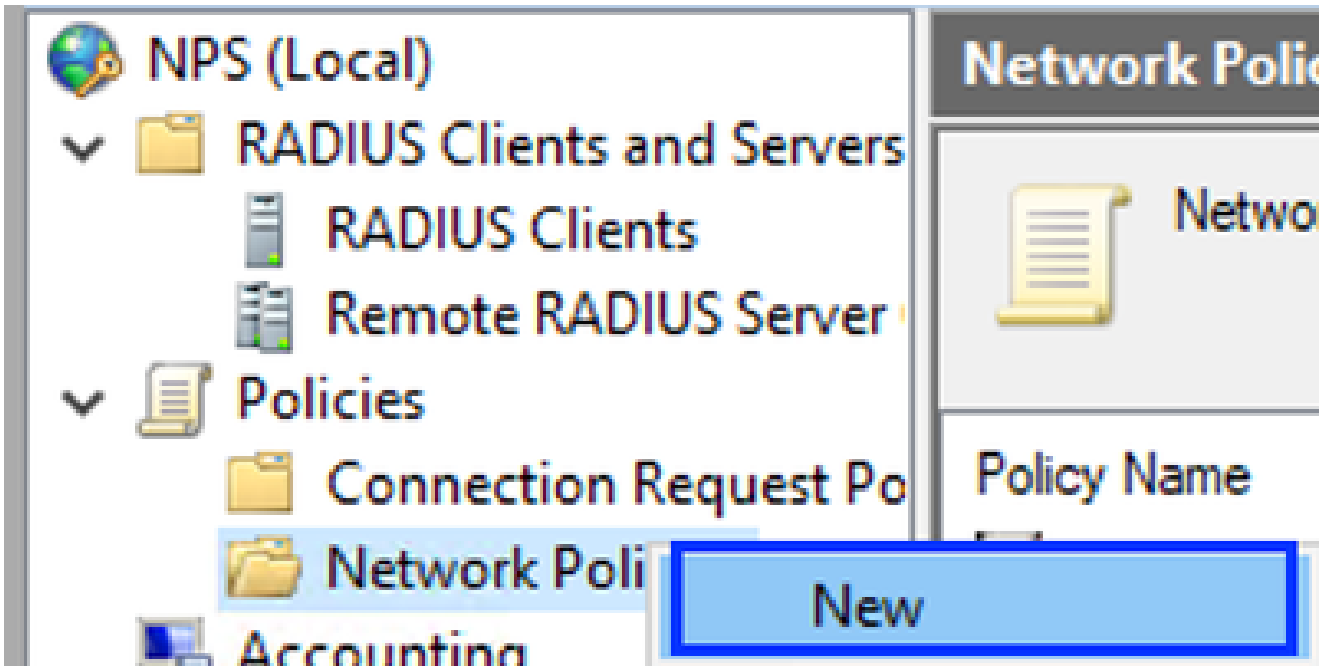
5. Saisissez le nom convivial, l'adresse IP de gestion de Cisco DNA Center et un secret partagé (ceci peut être utilisé ultérieurement) :



Configuration du client Radius

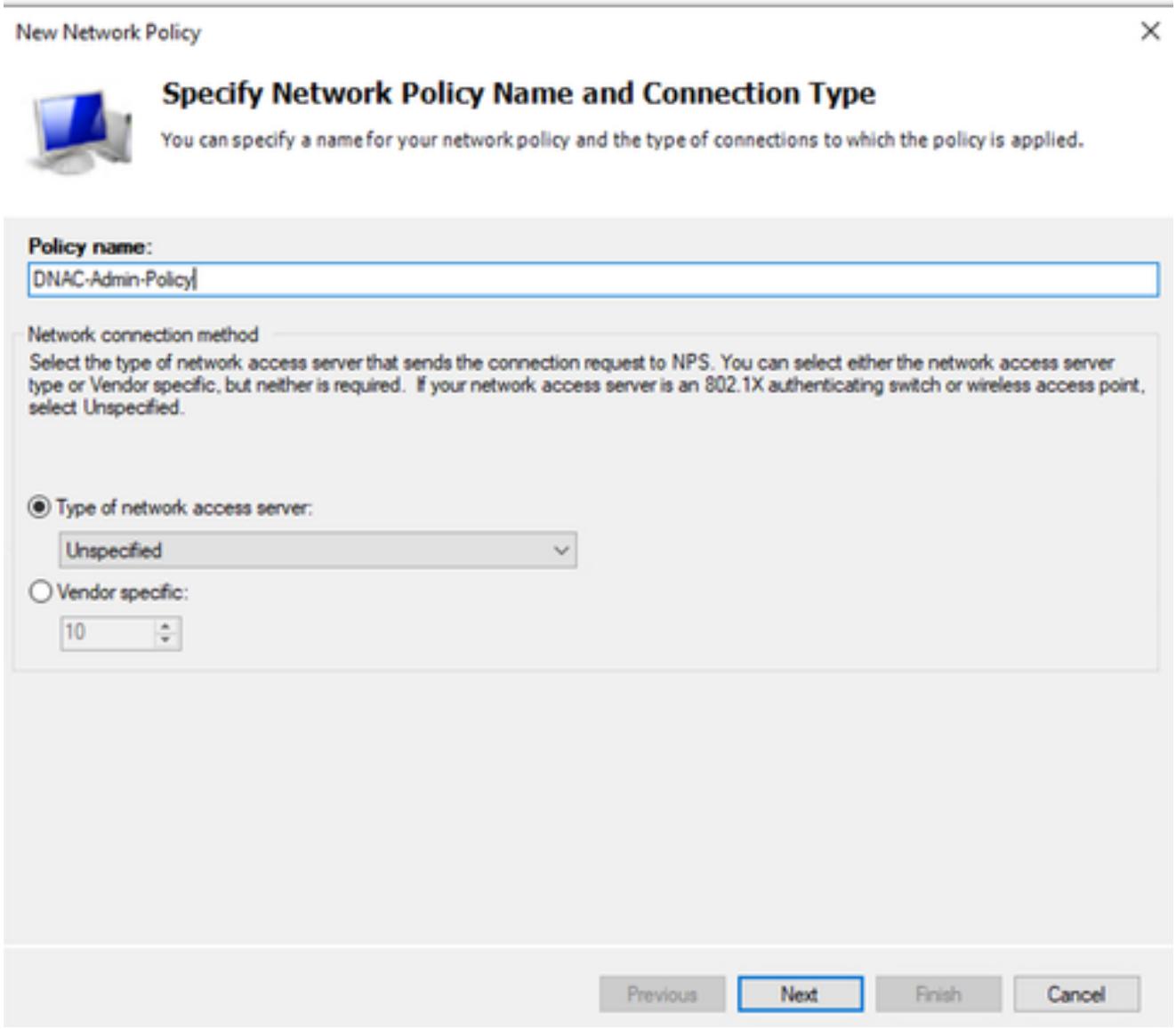
6. Cliquez sur OK pour l'enregistrer.

7. Développez Stratégies, cliquez avec le bouton droit sur Stratégies réseau et sélectionnez Nouveau :



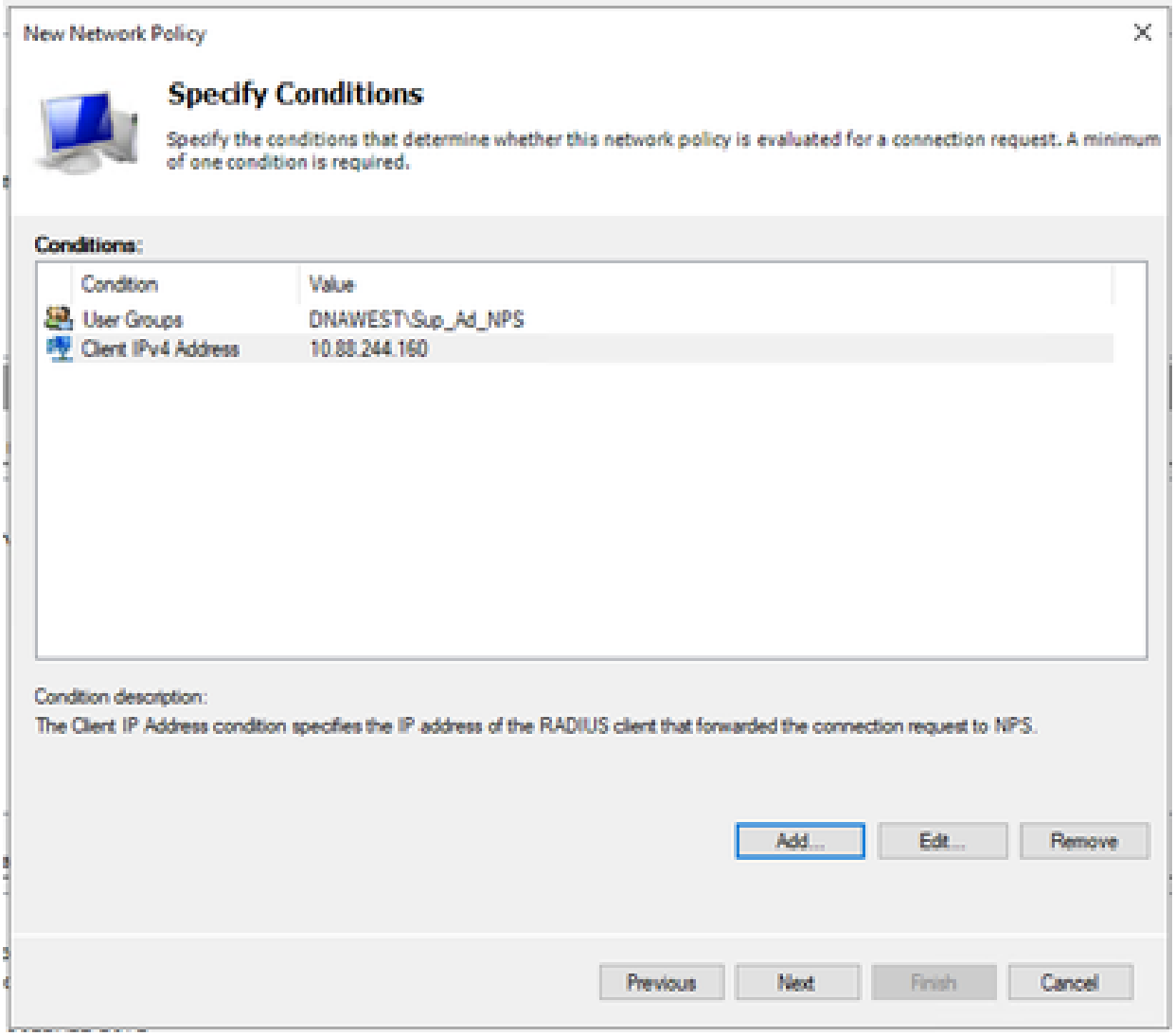
Ajouter une nouvelle politique de réseau

8. Entrez un nom de stratégie pour la règle et cliquez sur Suivant :



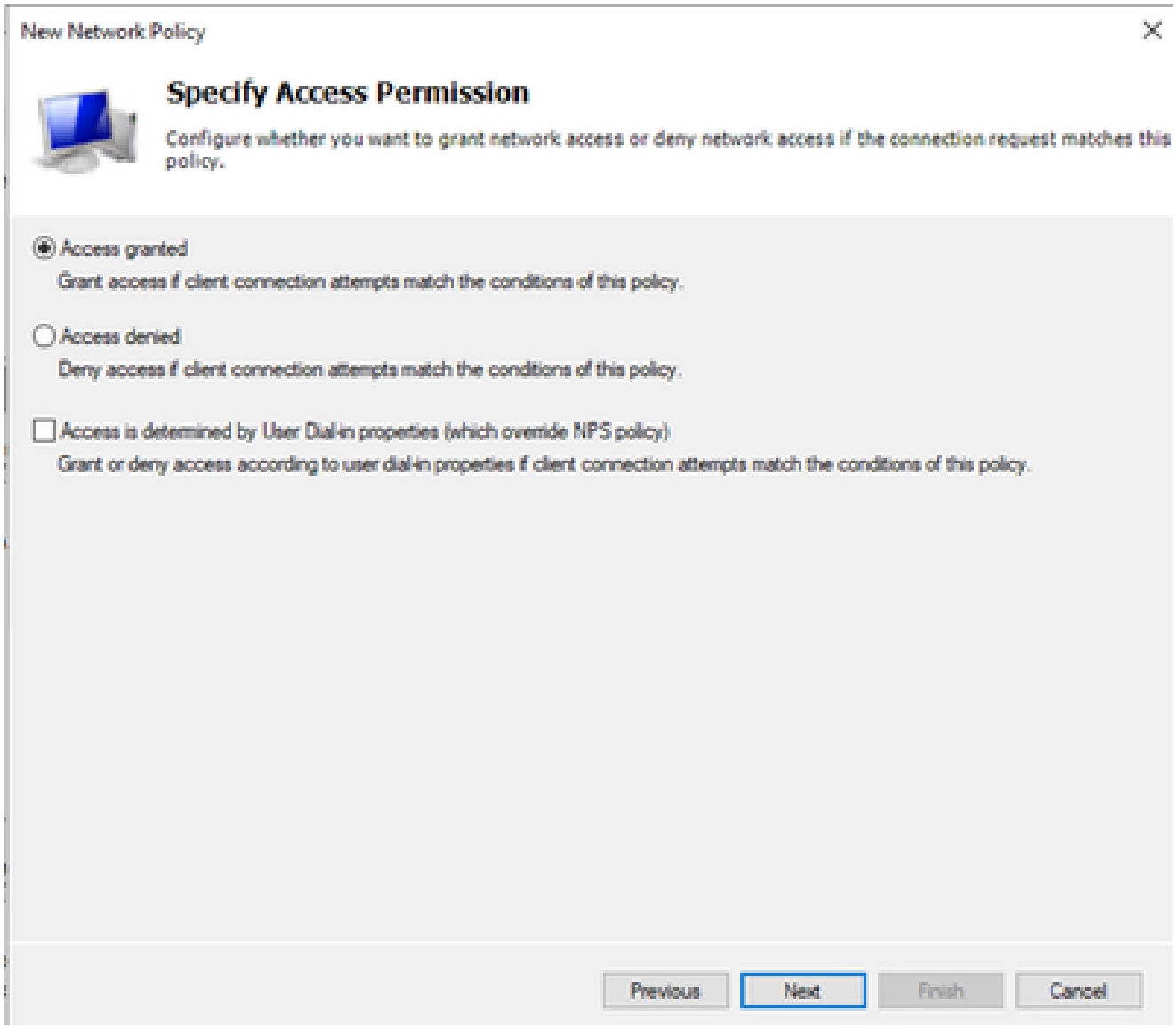
Nom de stratégie

9. Pour autoriser un groupe de domaines spécifique, ajoutez ces deux conditions et cliquez sur Suivant :
    - Groupe d'utilisateurs - Ajoutez votre groupe de domaines pouvant avoir un rôle d'administrateur sur Cisco DNA Center (pour cet exemple, le groupe Sup_Ad_NPS est utilisé).
    - ClientIPv4Address : ajoutez votre adresse IP de gestion Cisco DNA Center.



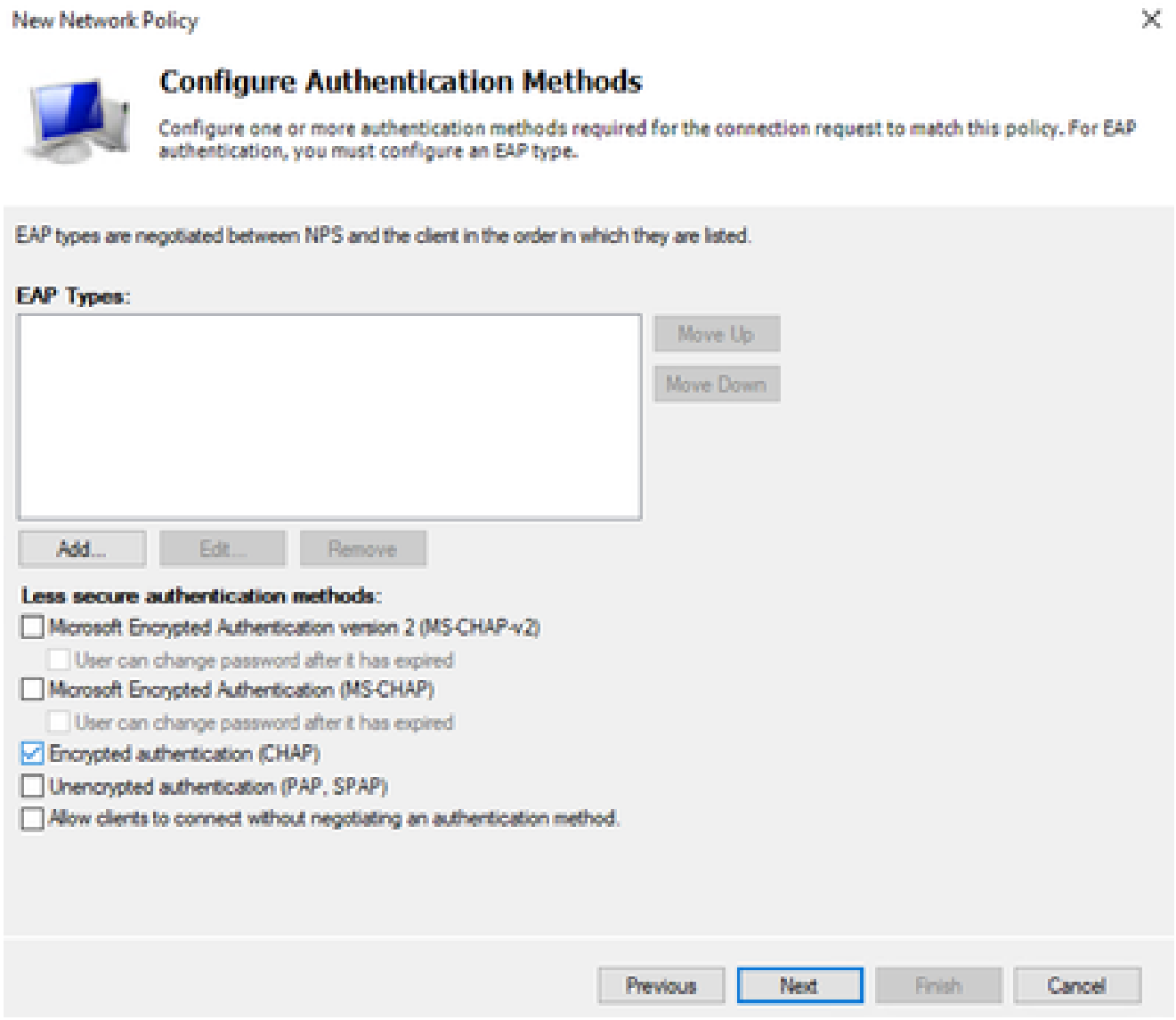
Conditions de stratégie

10. Sélectionnez Accès accordé et cliquez sur Suivant :



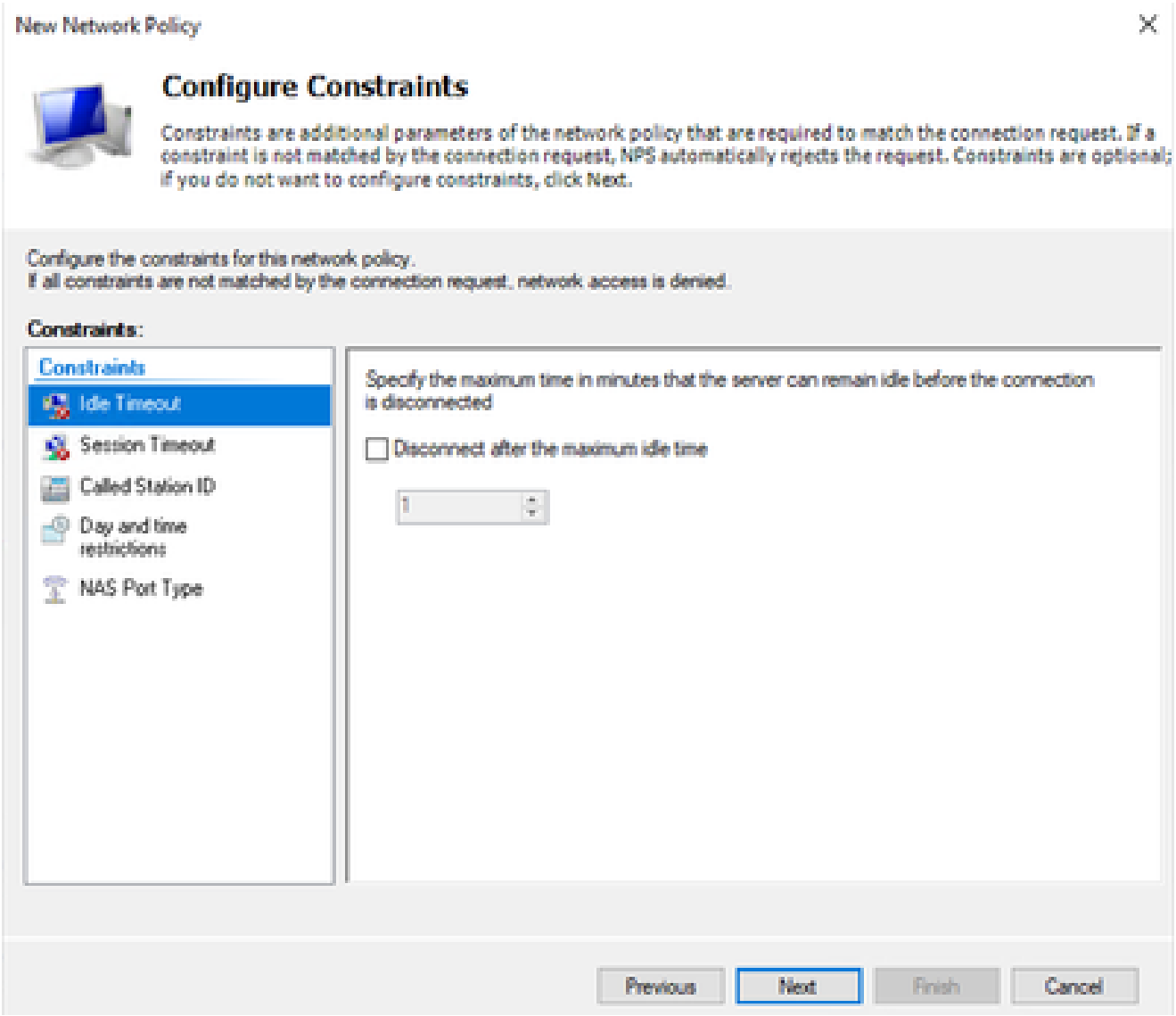
Utiliser l'accès accordé

11. Sélectionnez uniquement Authentification non chiffrée (PAP, SPAP) :



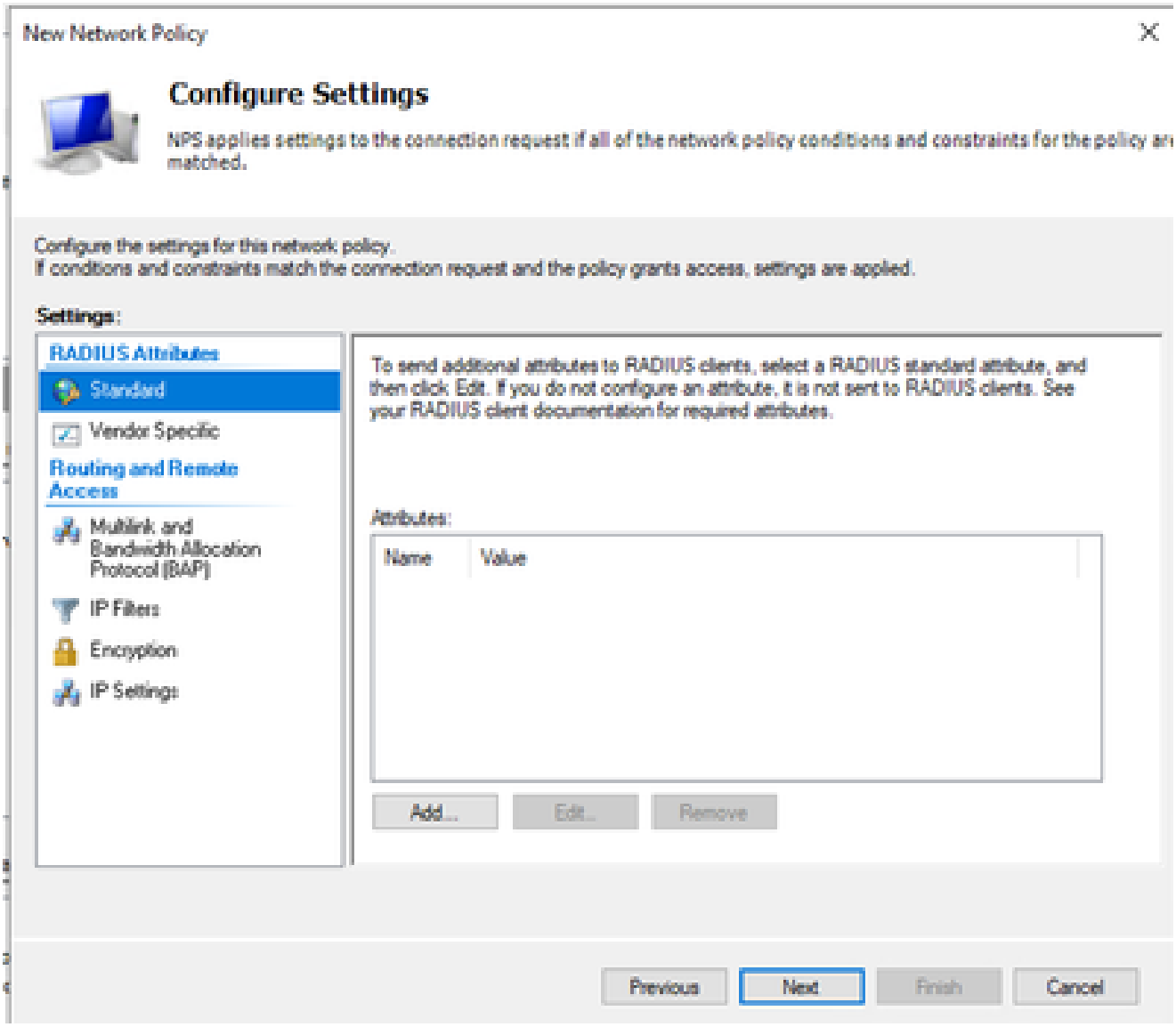
Sélectionnez Authentification non chiffrée

12. Sélectionnez Next puisque les valeurs par défaut sont utilisées :



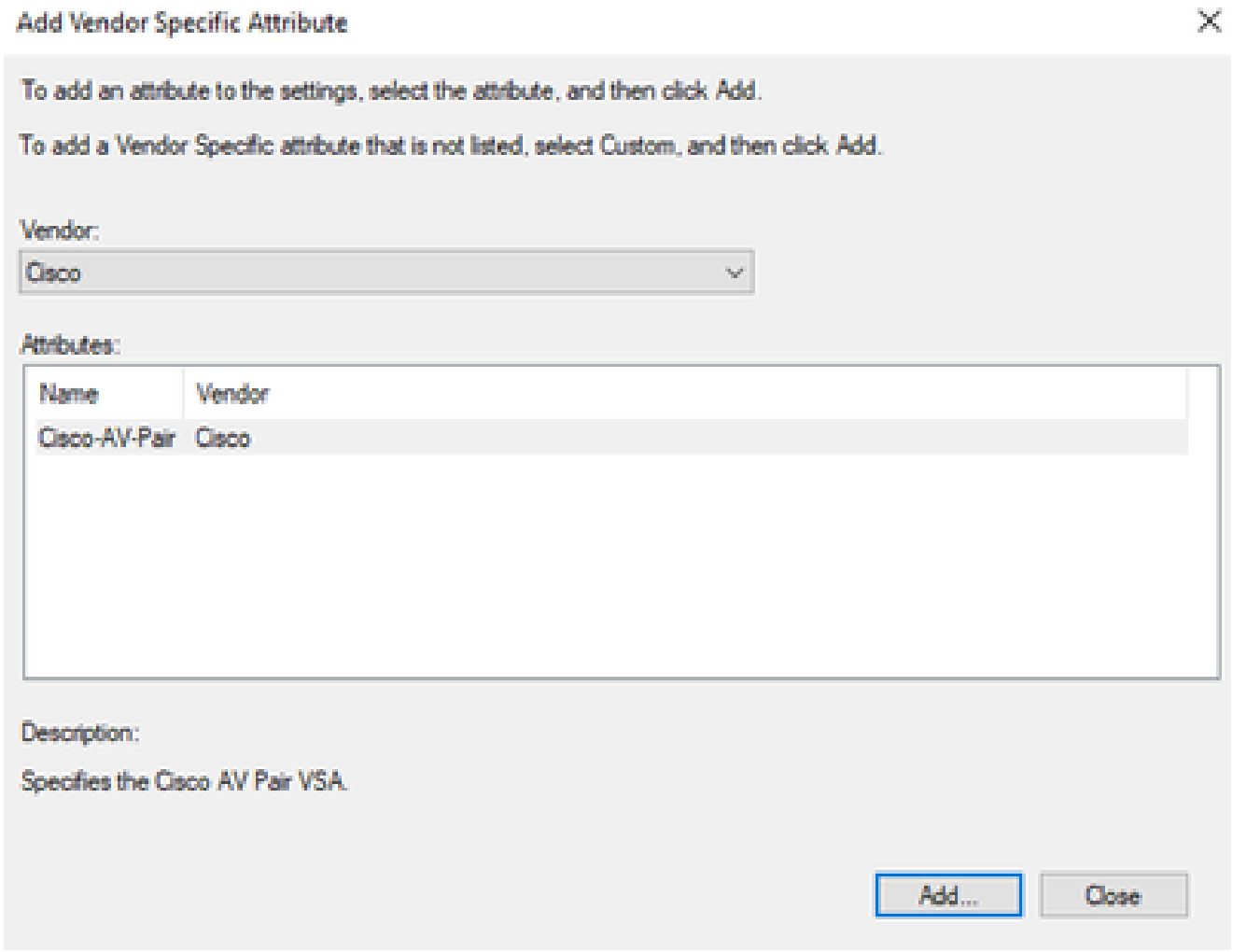
Fenêtre Configurer la contrainte

13. Supprimer les attributs standard :



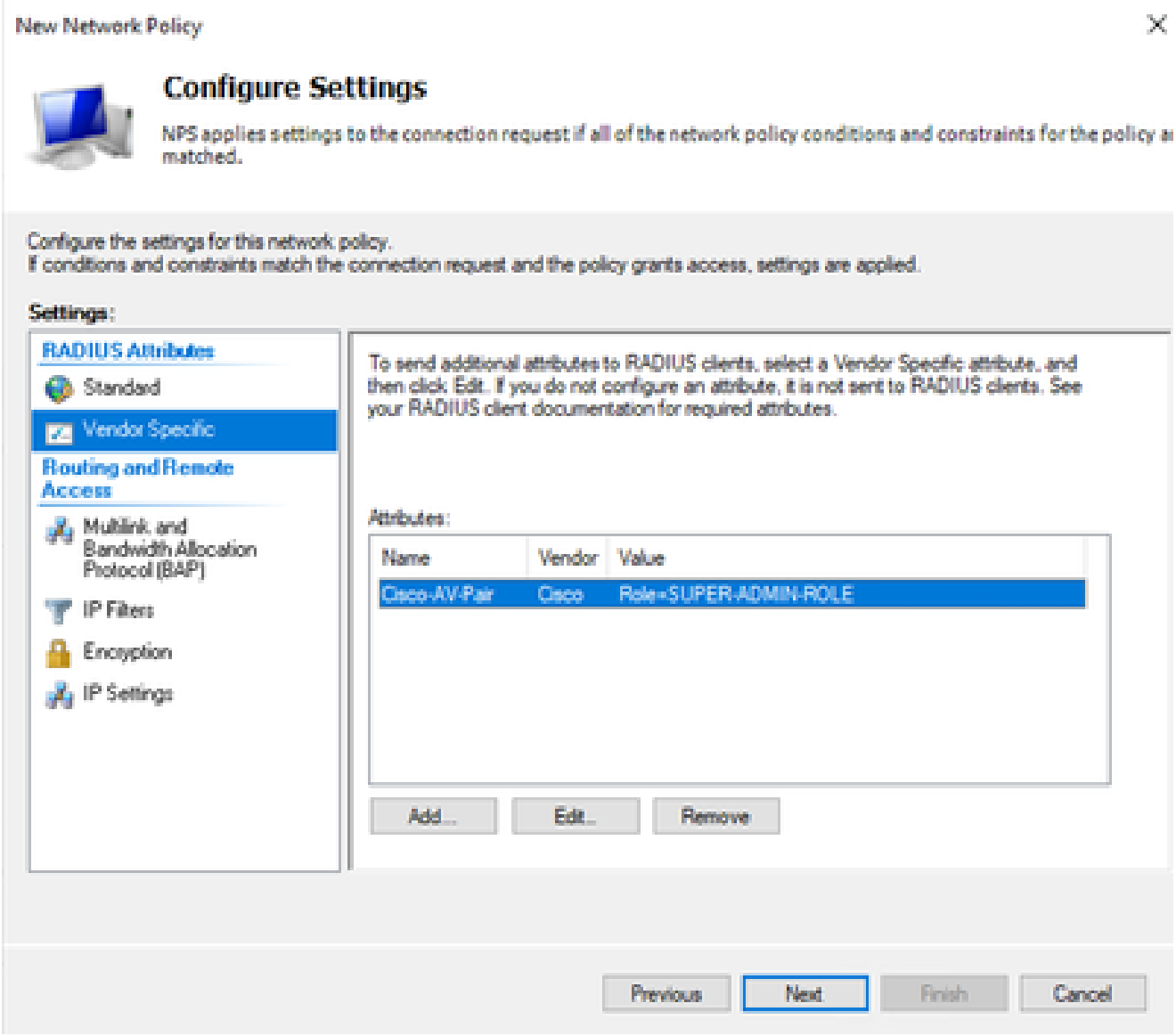
Définir les attributs à utiliser

14. Dans RADIUS Attributes, sélectionnez Vendor Specific, puis cliquez sur Add, sélectionnez Cisco as a Vendor, et cliquez sur Add :



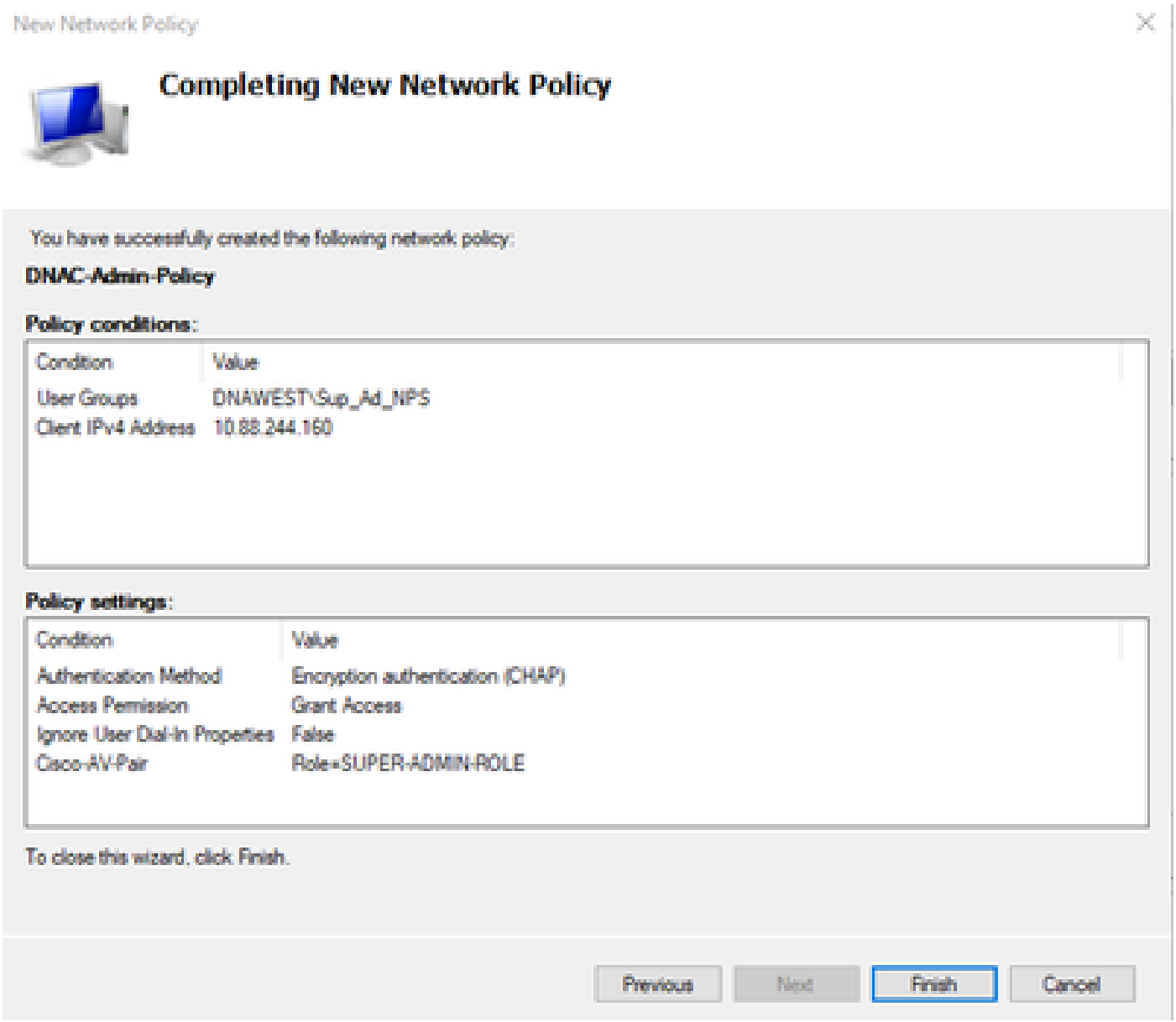
Ajouter une paire AV Cisco

15. Cliquez sur Add, écrivez Role=SUPER-ADMIN-ROLE et cliquez sur OK deux fois :



Attribut de paire AV Cisco ajouté

16. Sélectionnez Fermer, puis Suivant.
17. Vérifiez vos paramètres de stratégie et sélectionnez Terminer pour l'enregistrer.



Récapitulatif des stratégies

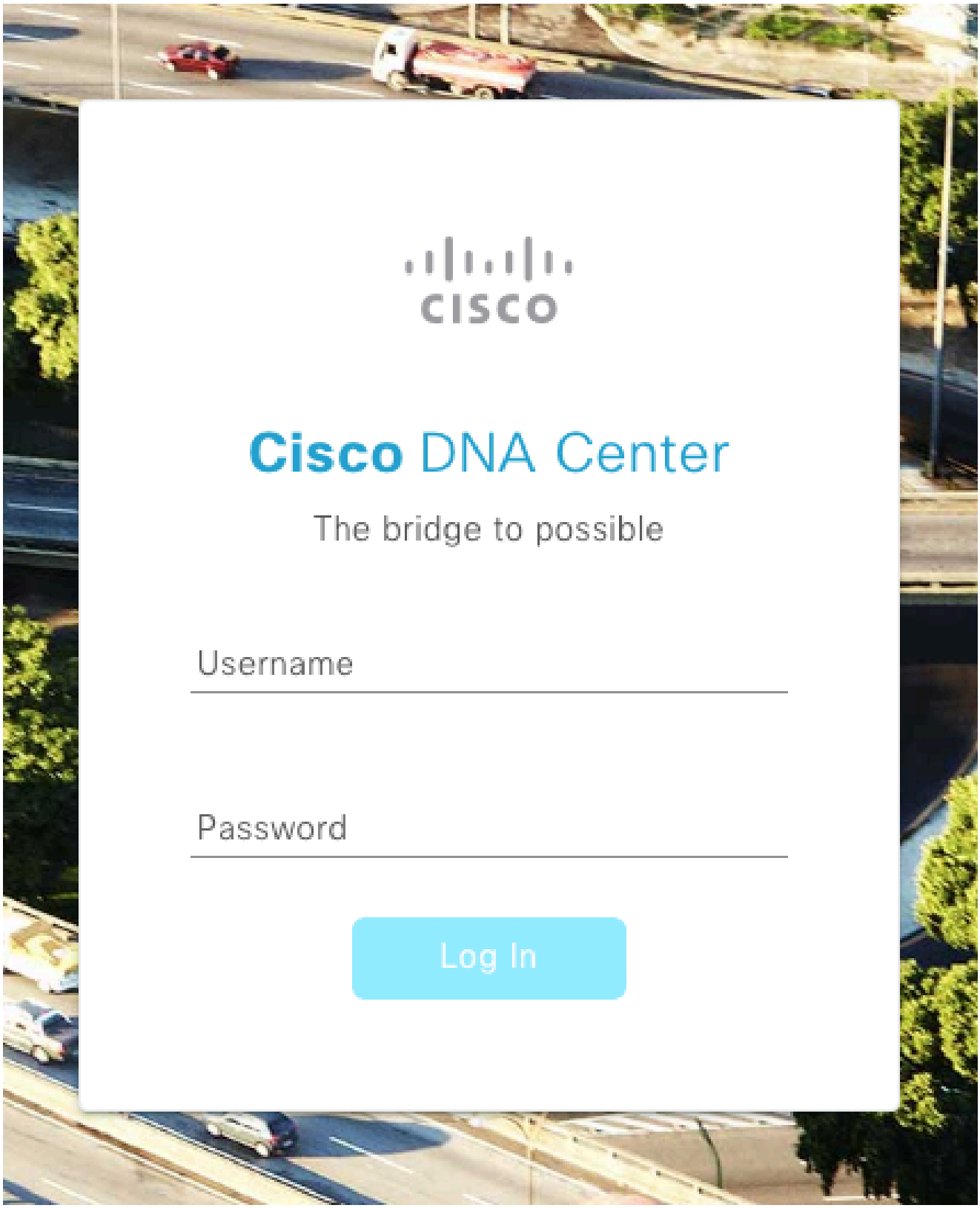
Politique de rôle Observateur.

1. Cliquez sur dans le menu Démarrer de Windows et recherchez NPS. Sélectionnez ensuite Network Policy Server.
2. Dans le volet de navigation sur le côté gauche, effectuez un clic droit dans l'option NPS (Local) et sélectionnez Register server in Active Directory.
3. Cliquez sur OK deux fois.
4. Développez RADIUS Clients and Servers, cliquez avec le bouton droit sur RADIUS Clients, puis sélectionnez New.
5. Saisissez un nom convivial, l'adresse IP de gestion de Cisco DNA Center et un secret partagé (ceci peut être utilisé ultérieurement).
6. Cliquez sur OK pour l'enregistrer.

7. Développez Stratégies, cliquez avec le bouton droit sur Stratégies réseau, puis sélectionnez Nouveau.
8. Entrez un nom de stratégie pour la règle et cliquez sur Next.
9. Pour autoriser un groupe de domaines spécifique, vous devez ajouter ces deux conditions et sélectionner Next.
    - Groupe d'utilisateurs - Ajoutez votre groupe de domaines afin d'attribuer un rôle d'observateur sur Cisco DNA Center (Pour cet exemple, le groupe Observer_NPS est utilisé).
    - ClientIPv4Address : ajoutez votre adresse IP de gestion Cisco DNA Center.
10. Sélectionnez Accès accordé, puis Suivant.
11. Sélectionnez uniquement Authentification non cryptée (PAP, SPAP).
12. Sélectionnez Next puisque les valeurs par défaut sont utilisées.
13. Supprimez les attributs Standard.
14. Dans Attributs RADIUS, sélectionnez Vendor Specific, puis cliquez sur Add, sélectionnez Cisco as a Vendor, et cliquez sur Add.
15. Sélectionnez Add, write ROLE=OBSERVER-ROLE, et OK deux fois.
16. Sélectionnez Fermer, puis Suivant.
17. Vérifiez vos paramètres de stratégie et sélectionnez Terminer pour l'enregistrer.

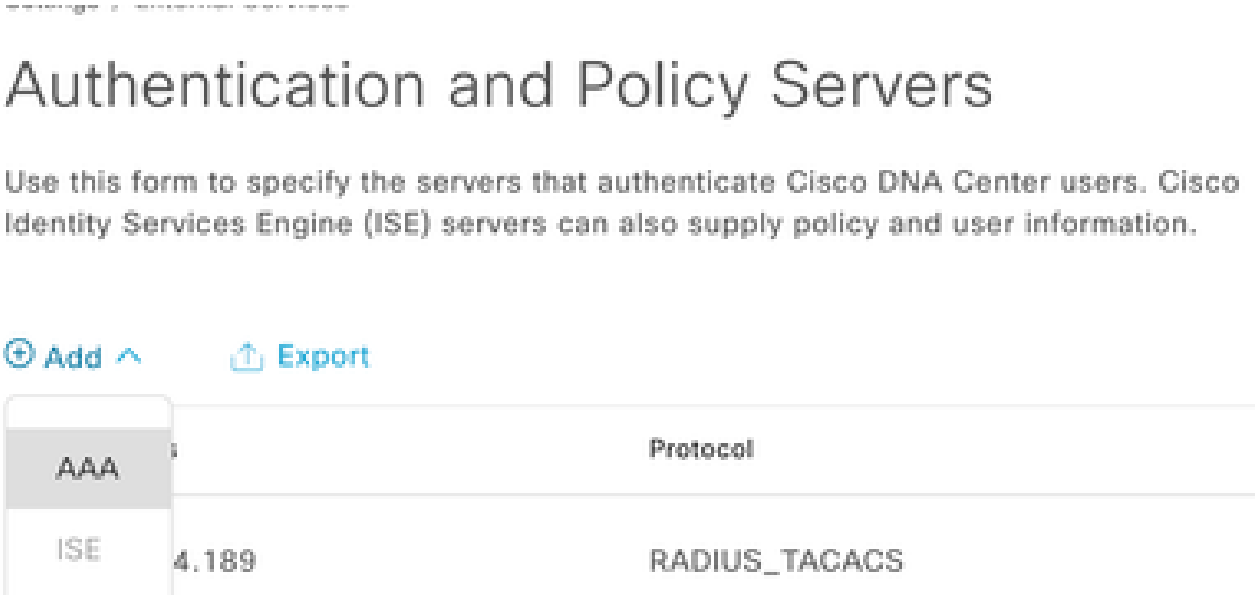
Activer l'authentification externe

1. Ouvrez l'interface utilisateur graphique de Cisco DNA Center dans un navigateur Web et connectez-vous à l'aide d'un compte d'administrateur privilégié :



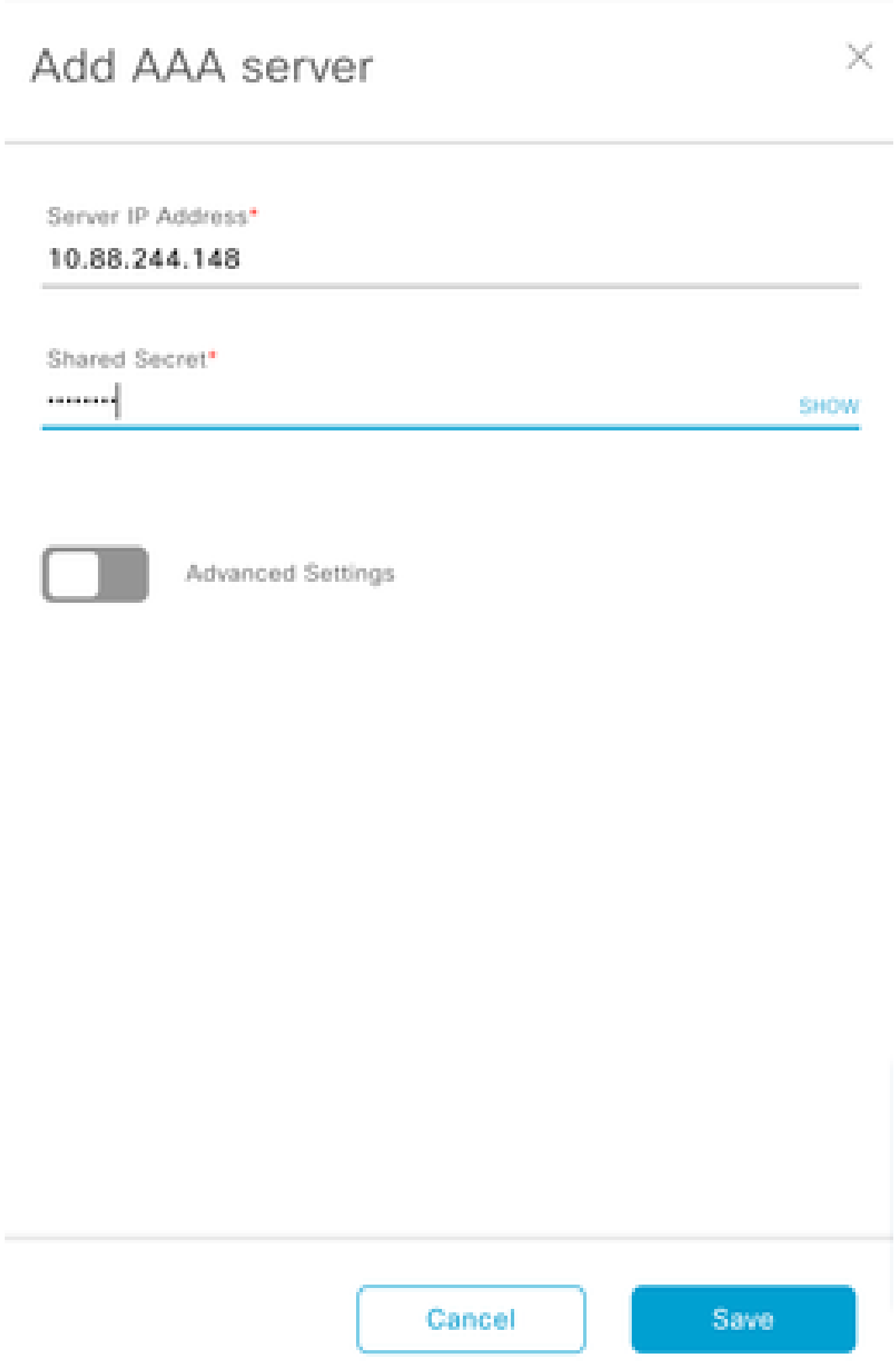
Page de connexion à Cisco DNA Center

2. Accédez à Menu > System > Setting > Authentication and Policy Servers et sélectionnez Add > AAA :



Ajouter un serveur Windows

3. Tapez votre adresse IP Windows Server et le secret partagé utilisé dans les étapes précédentes et cliquez sur Save :

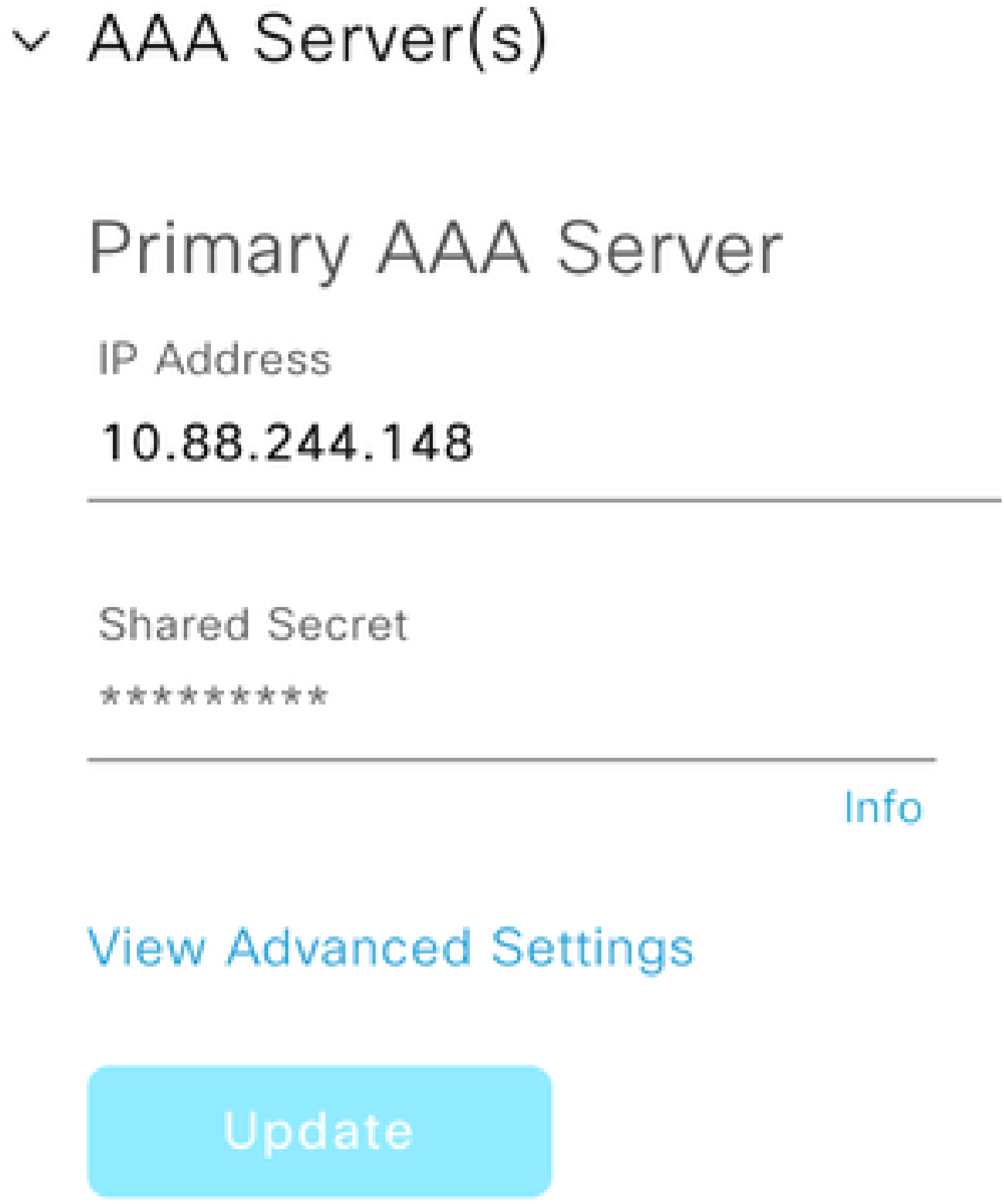


Valeurs de Windows Server

4. Vérifiez que votre état Windows Server est Actif :

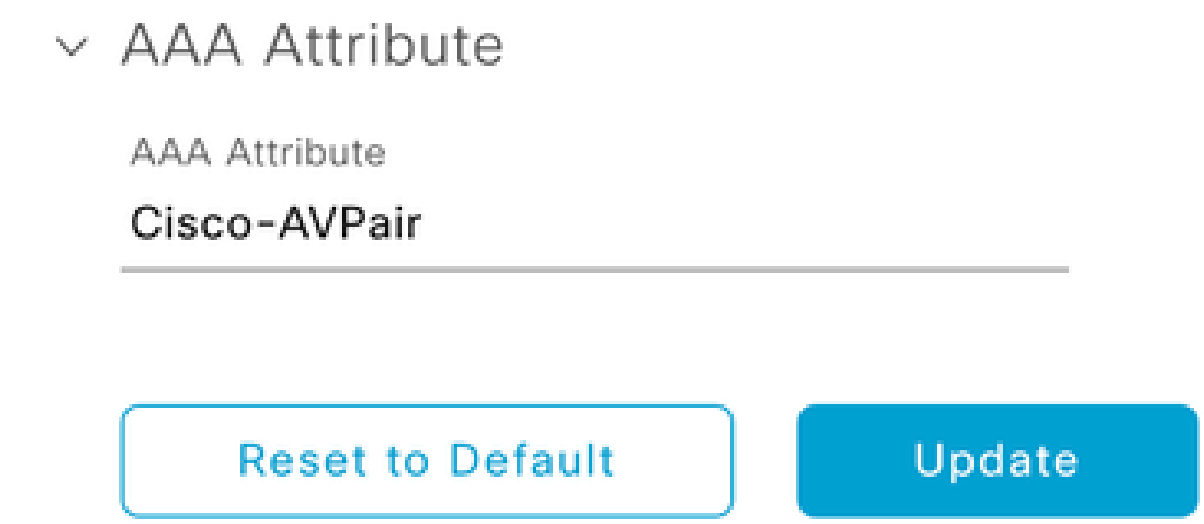
Résumé de Windows Server

5. Accédez à Menu > System > Users & Roles > External Authentication et sélectionnez votre serveur AAA :



Windows Server comme serveur AAA

6. Tapez Cisco-AVPair comme attribut AAA et cliquez sur Update:

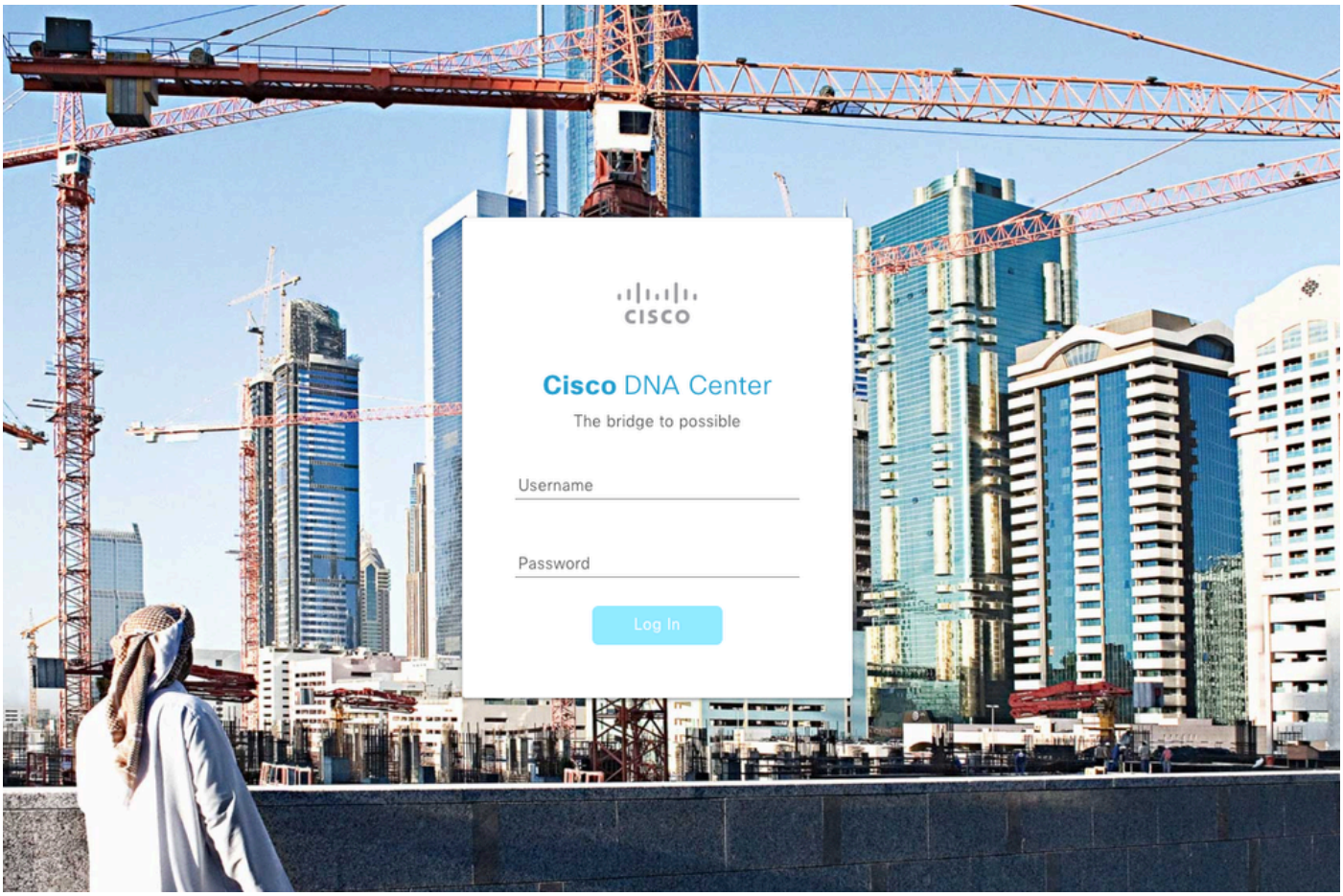


Paire AV sur utilisateur externe

7. Cochez la case Enable External User pour activer l'authentification externe :

Vérifier

Vous pouvez ouvrir l'interface utilisateur graphique (GUI) de Cisco DNA Center dans un navigateur Web et vous connecter avec un utilisateur externe configuré dans le serveur Windows pour valider que vous pouvez vous connecter avec succès à l'aide de l'authentification externe.



Page de connexion à Cisco DNA Center

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.