Windows Serverを使用したCatalyst Centerでの外部認証の設定

内容

はじめに

このドキュメントでは、Windows Serverのネットワークポリシーサーバ(NPS)をRADIUSとして使用して、Cisco DNA Center(DNA Center)で外部認証を設定する方法について説明します。

前提条件

要件

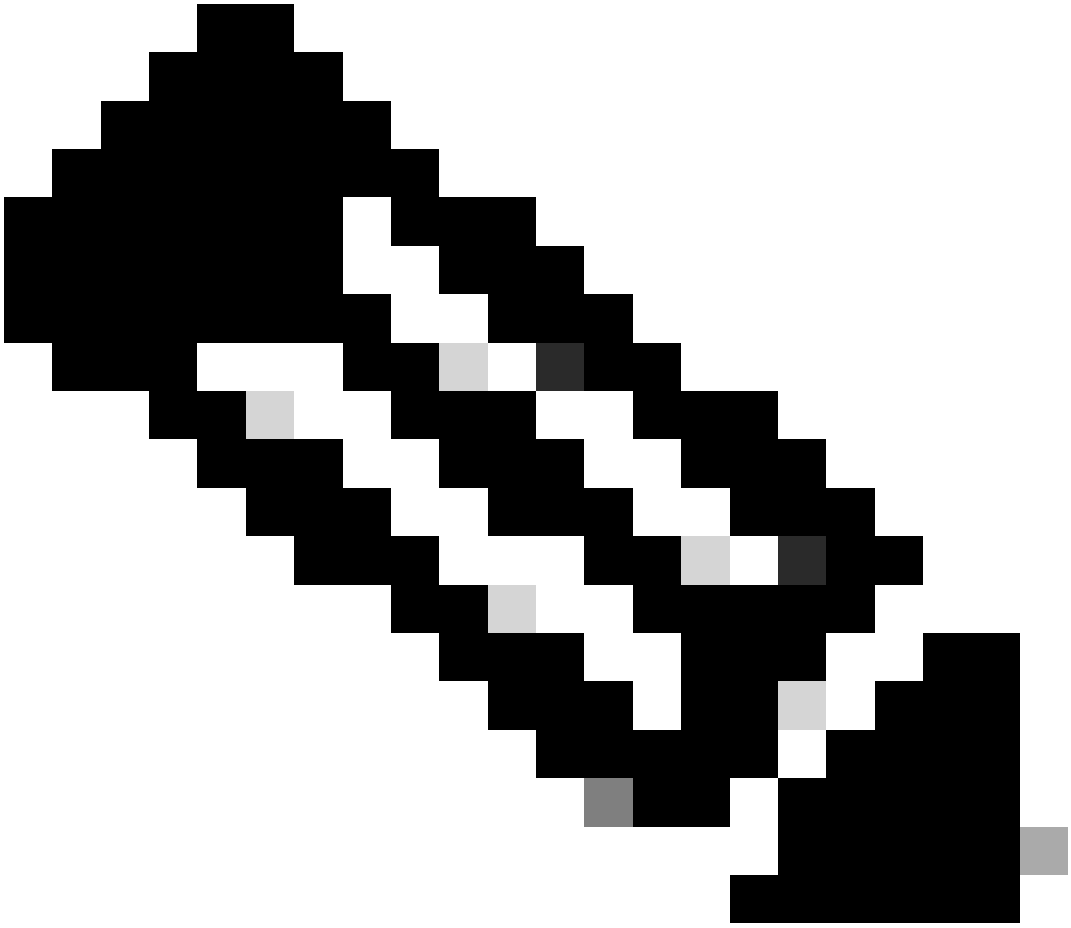
次の項目に関する基礎知識

- Cisco DNA Centerのユーザとロール
- Windows Serverネットワークポリシーサーバ、RADIUSおよびActive Directory

使用するコンポーネント

- Cisco DNA Center 2.3.5.x
- ドメインコントローラ、DNSサーバ、NPS、およびActive Directoryとして機能するMicrosoft Windows Serverバージョン2019

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

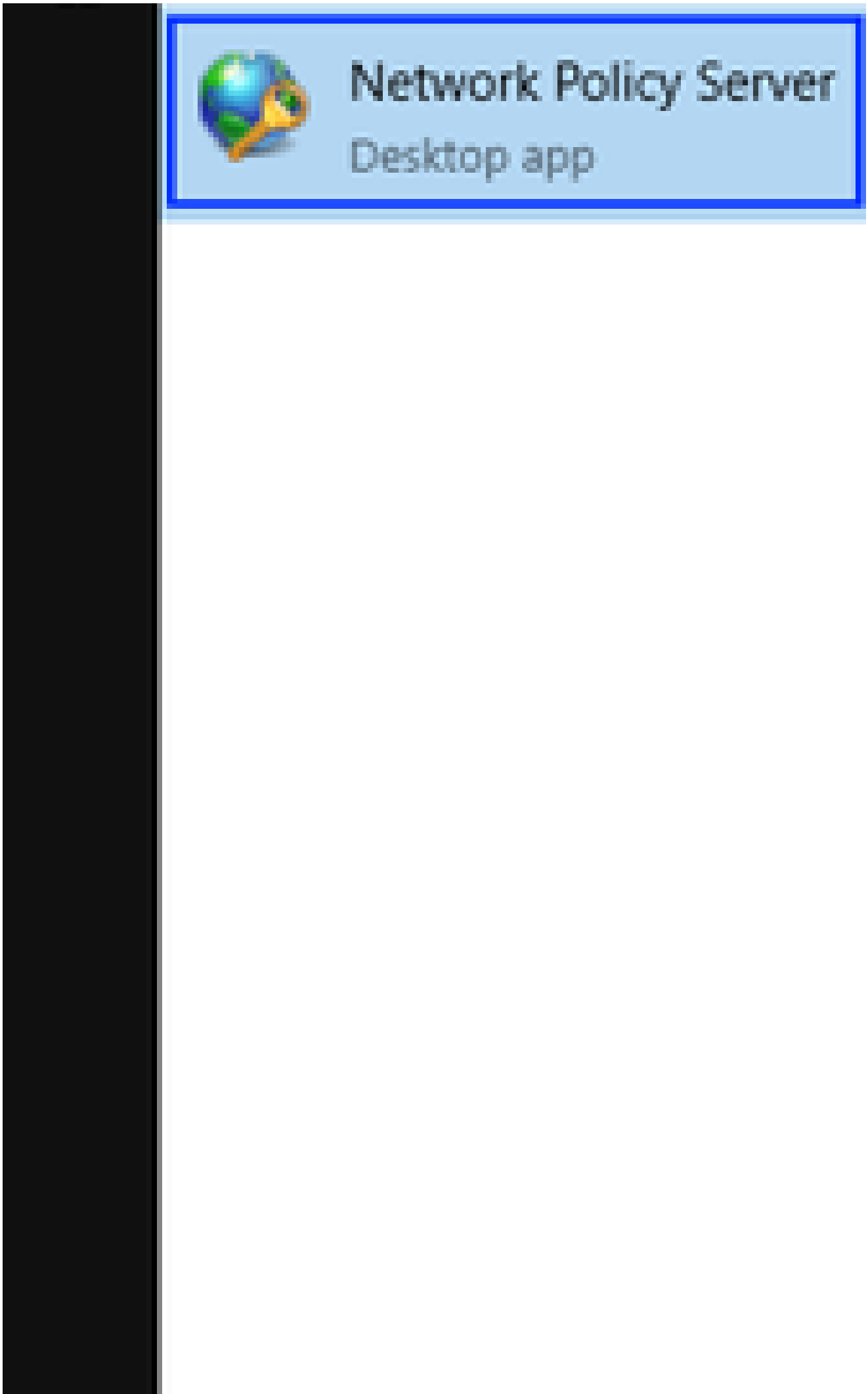


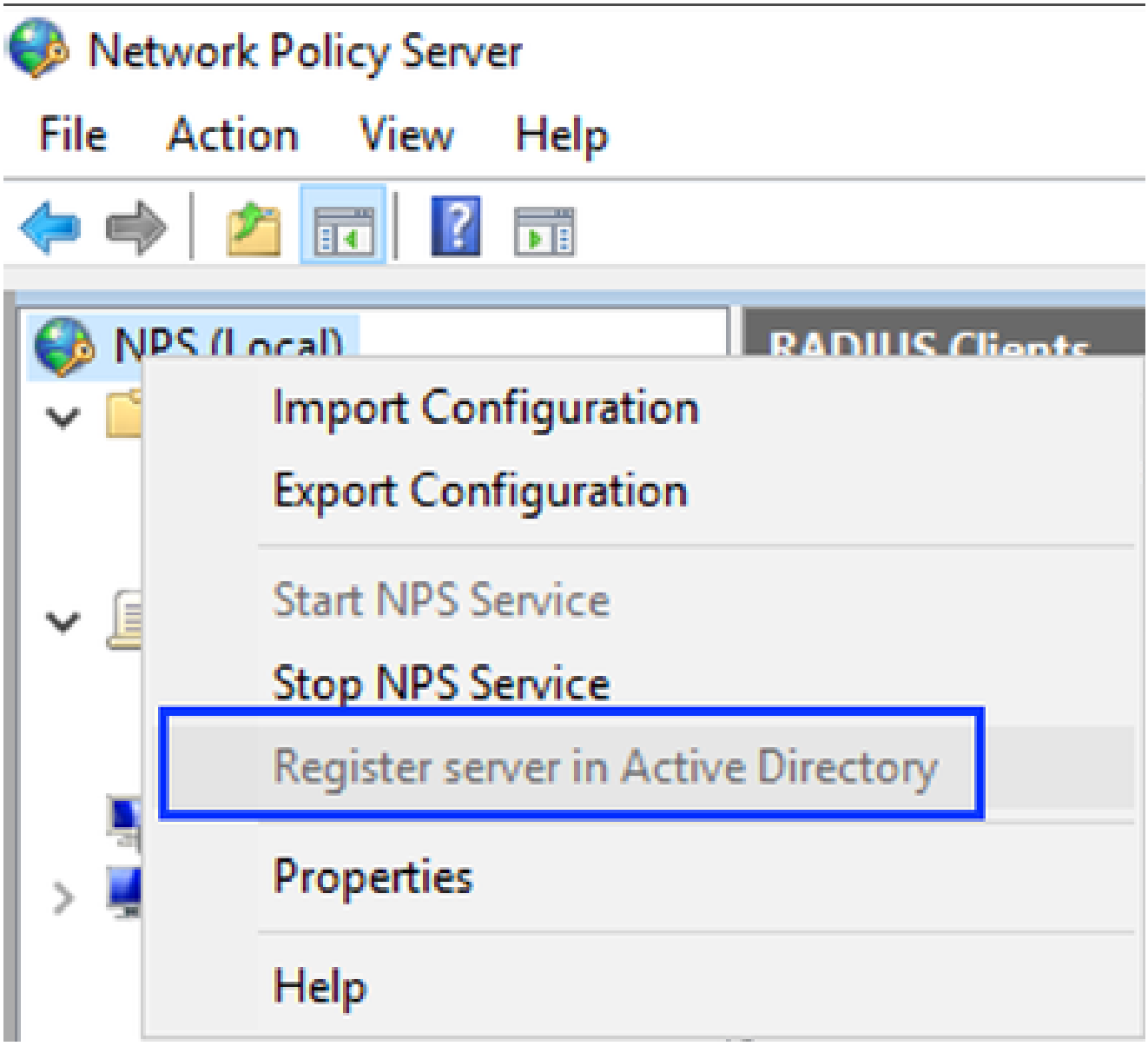
注:Cisco Technical Assistance Center(TAC)は、Microsoft Windows Serverに対するテクニカルサポートを提供しません。 Microsoft Windows Serverの設定に関する問題が発生した場合は、Microsoftサポートにテクニカルサポートを要請してください。

設定

管理者ロールポリシー

1. WindowsのStartメニューをクリックして、NPSを検索します。次に、Network Policy Serverを選択します。

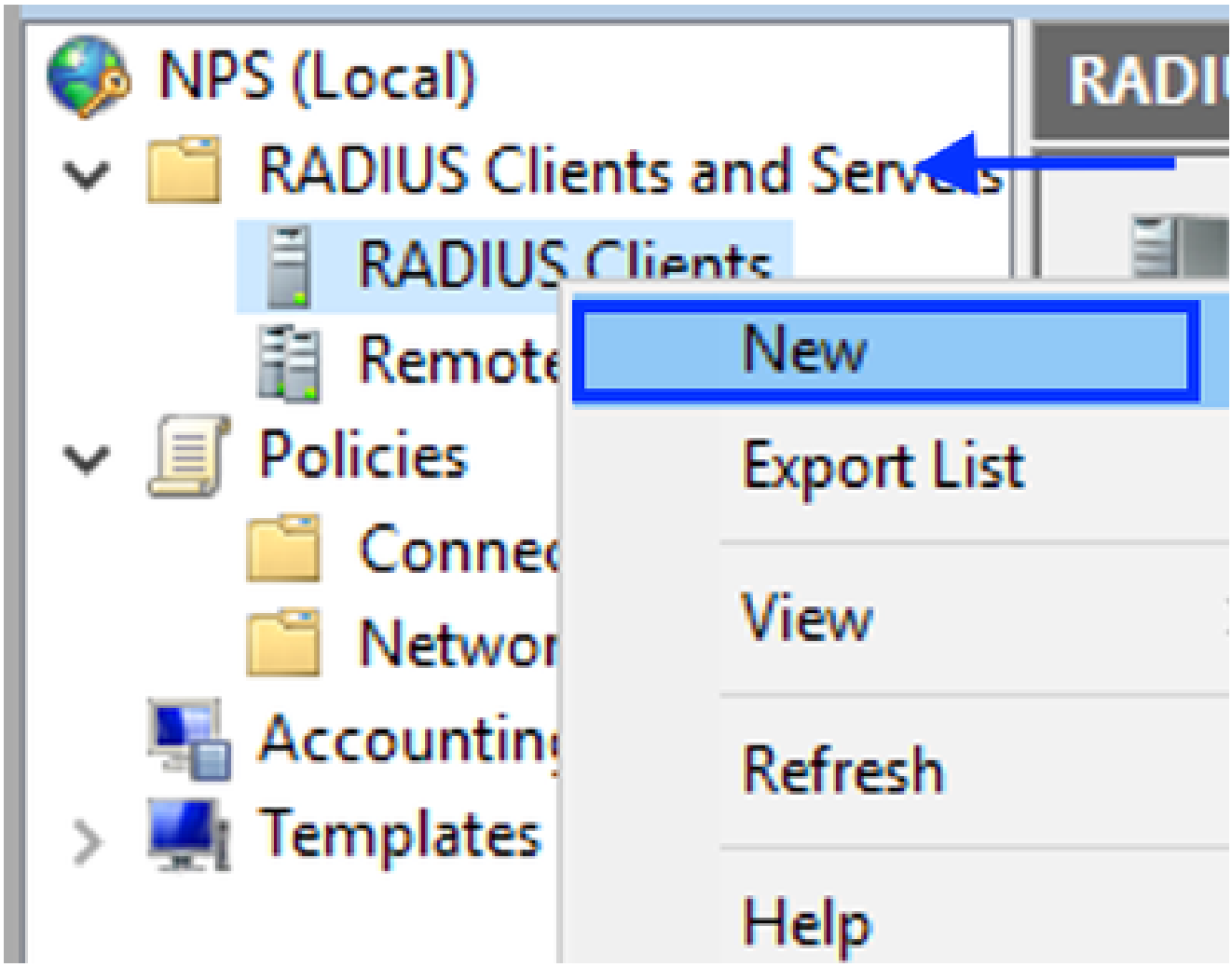

Network Policy Server
Desktop app



Windowsネットワークポリシーサービス

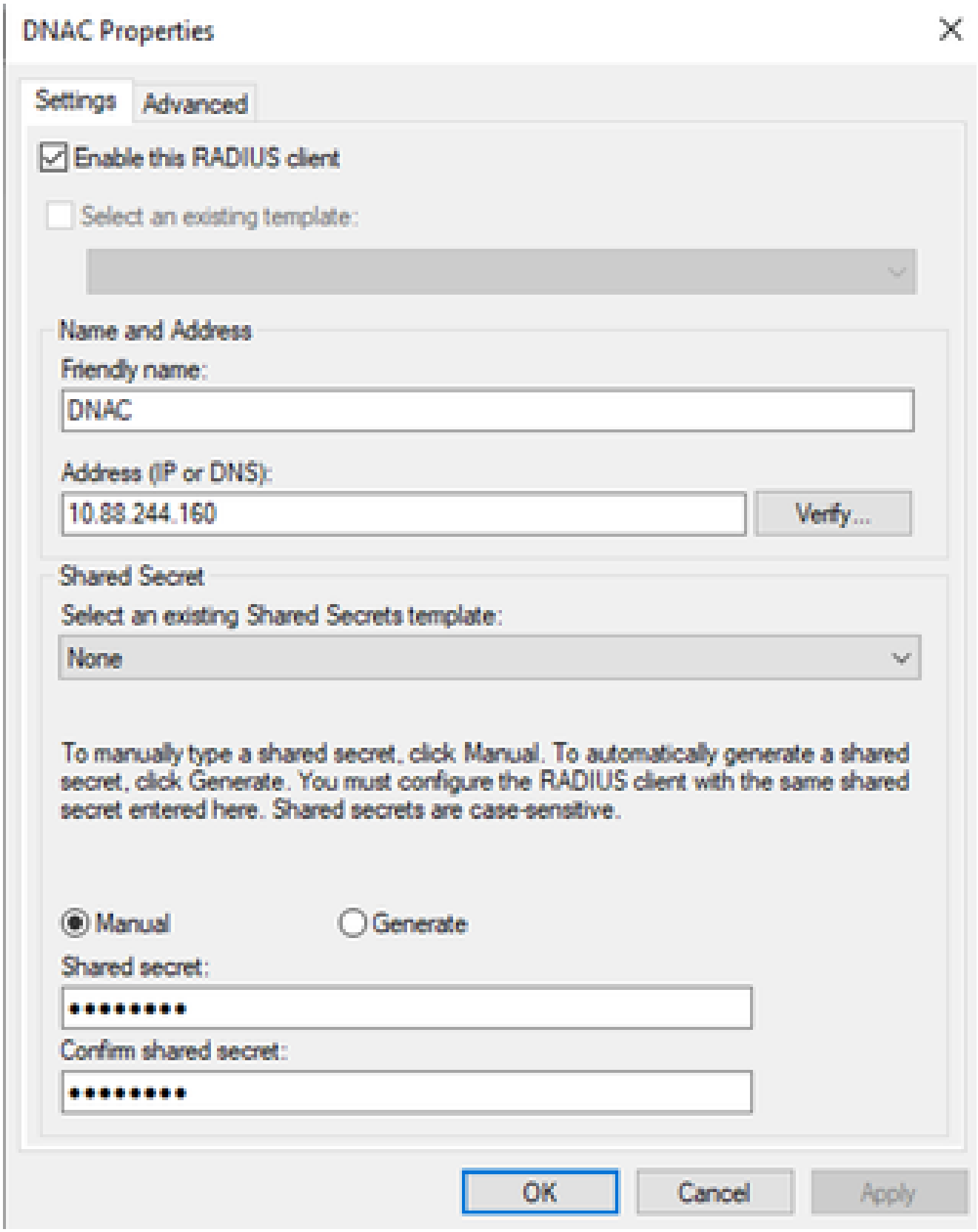
3. OKを2回クリックします。

4. RADIUS Clients and Serversを展開し、RADIUS Clientsを右クリックして、Newを選択します。



RADIUSクライアントの追加

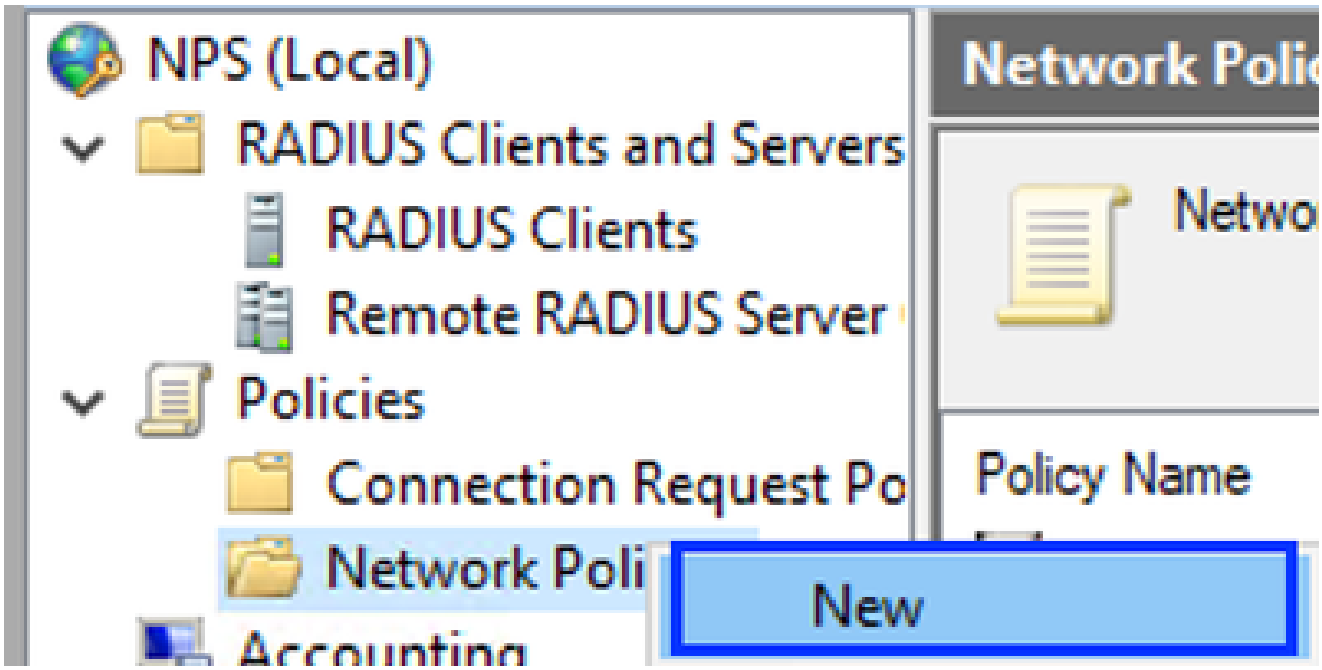
5. フレンドリ名、Cisco DNA Center管理IPアドレス、および共有秘密を入力します（これは後で使用できます）。



Radiusクライアントの設定

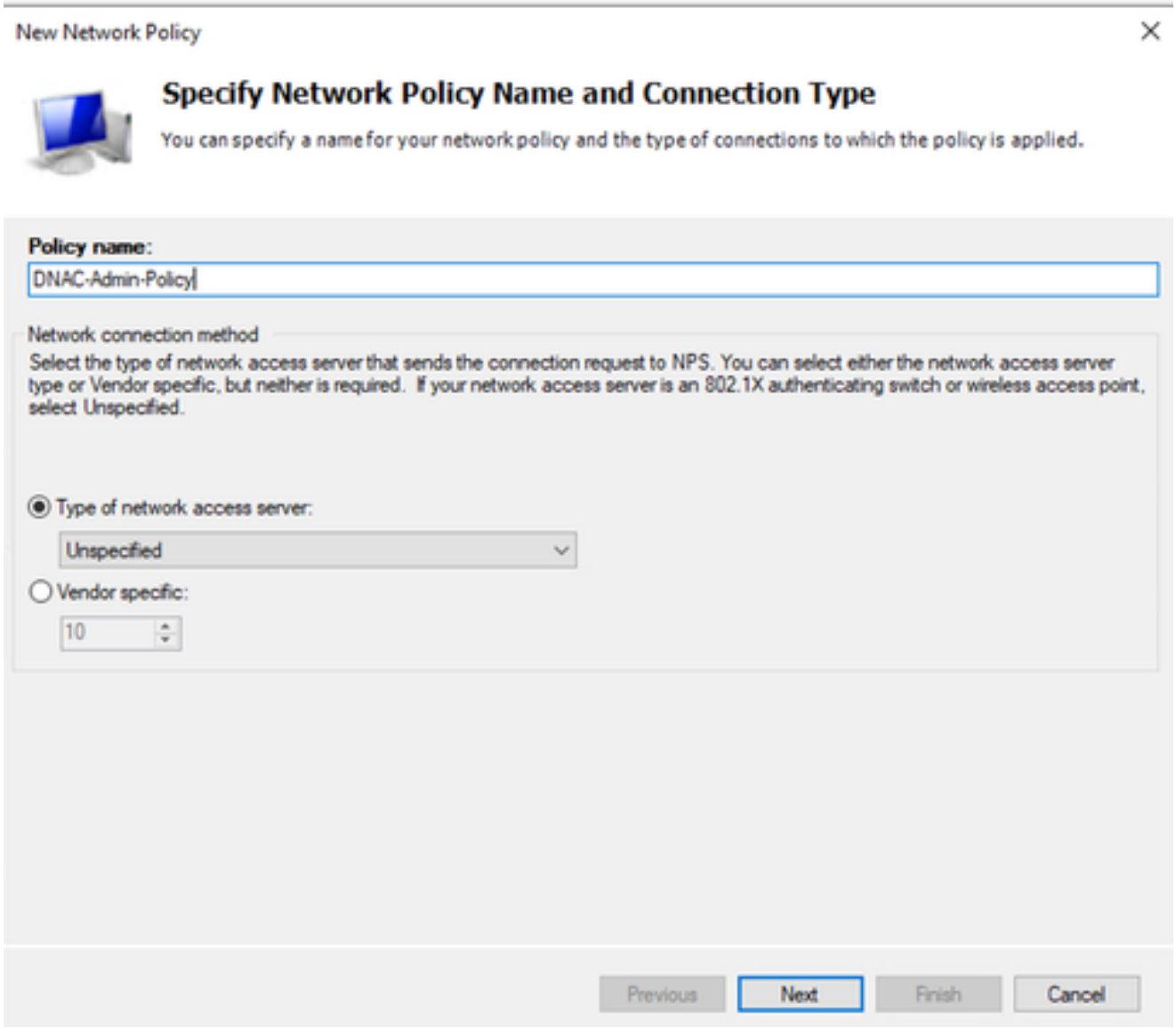
6. OKをクリックして保存します。

7. Policiesを展開して、Network Policiesを右クリックし、Newを選択します。



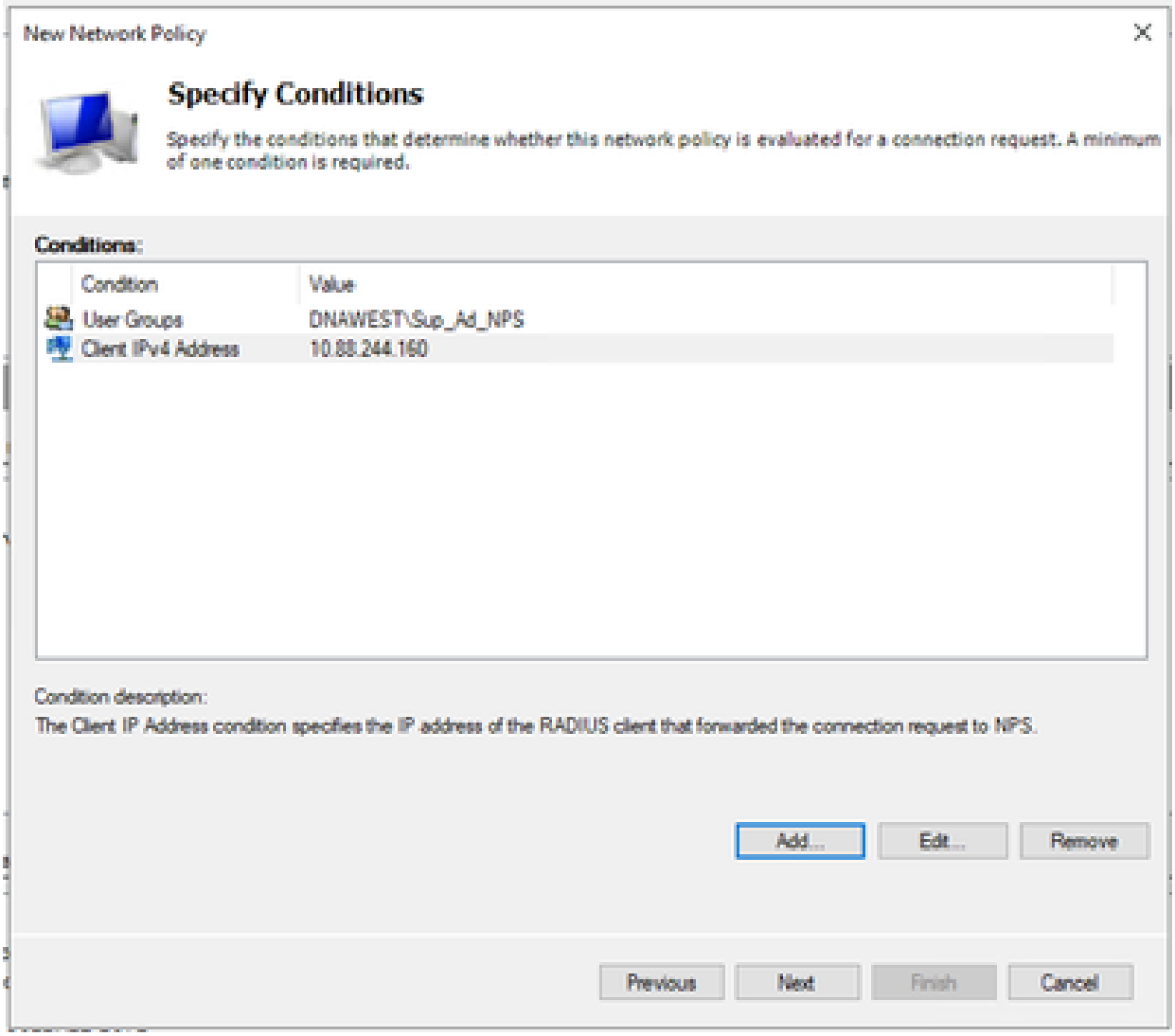
新しいネットワークポリシーの追加

8. ルールのポリシー名を入力し、Nextをクリックします。



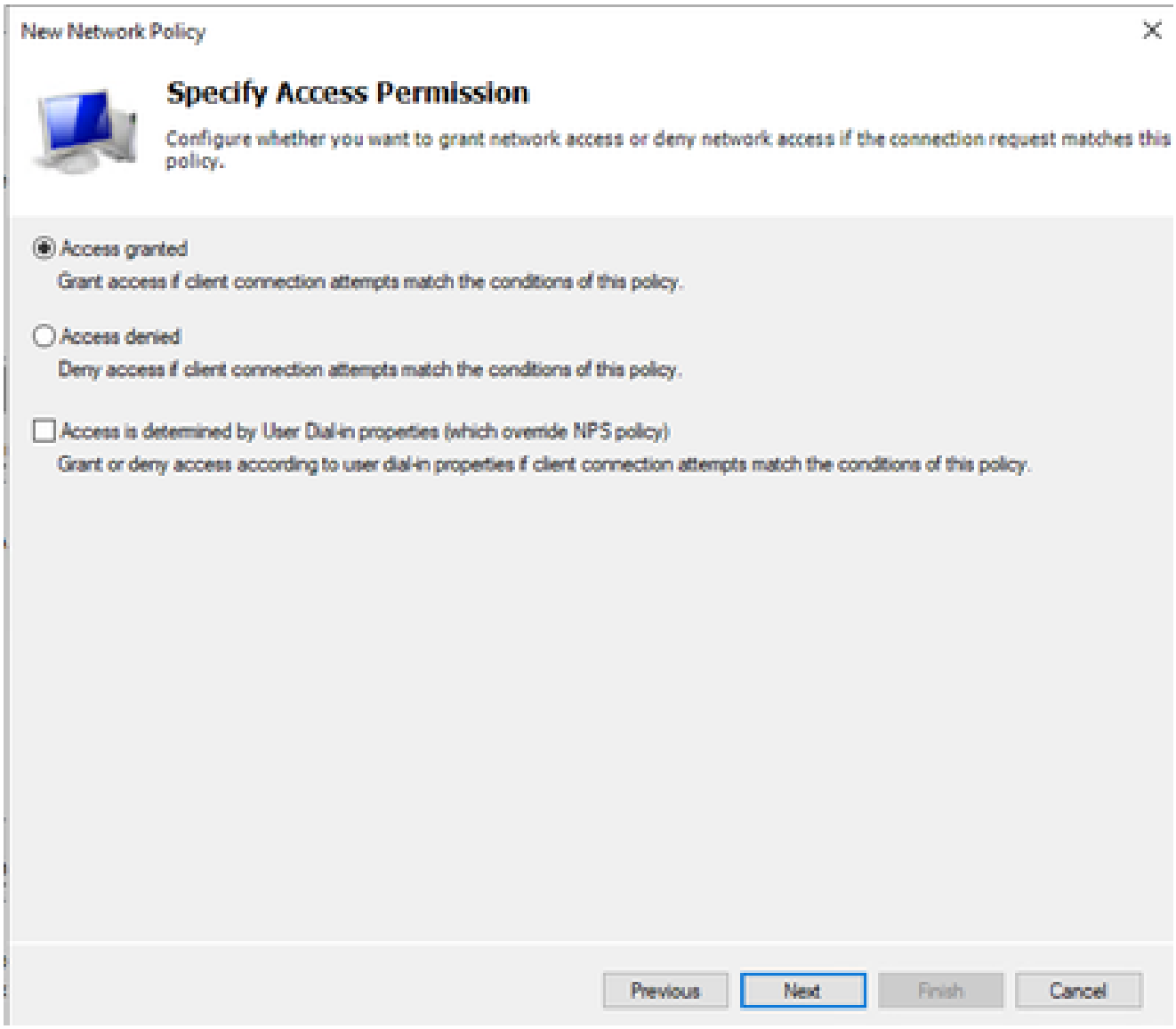
ポリシー名

9. 特定のドメイングループを許可するには、次の2つの条件を追加してNextをクリックします。
   - ユーザグループ:Cisco DNA Centerで管理者ロールを持つことができるドメイングループを追加します（この例では、Sup_Ad_NPSグループを使用）。
   - ClientIPv4Address:Cisco DNA Center管理IPアドレスを追加します。



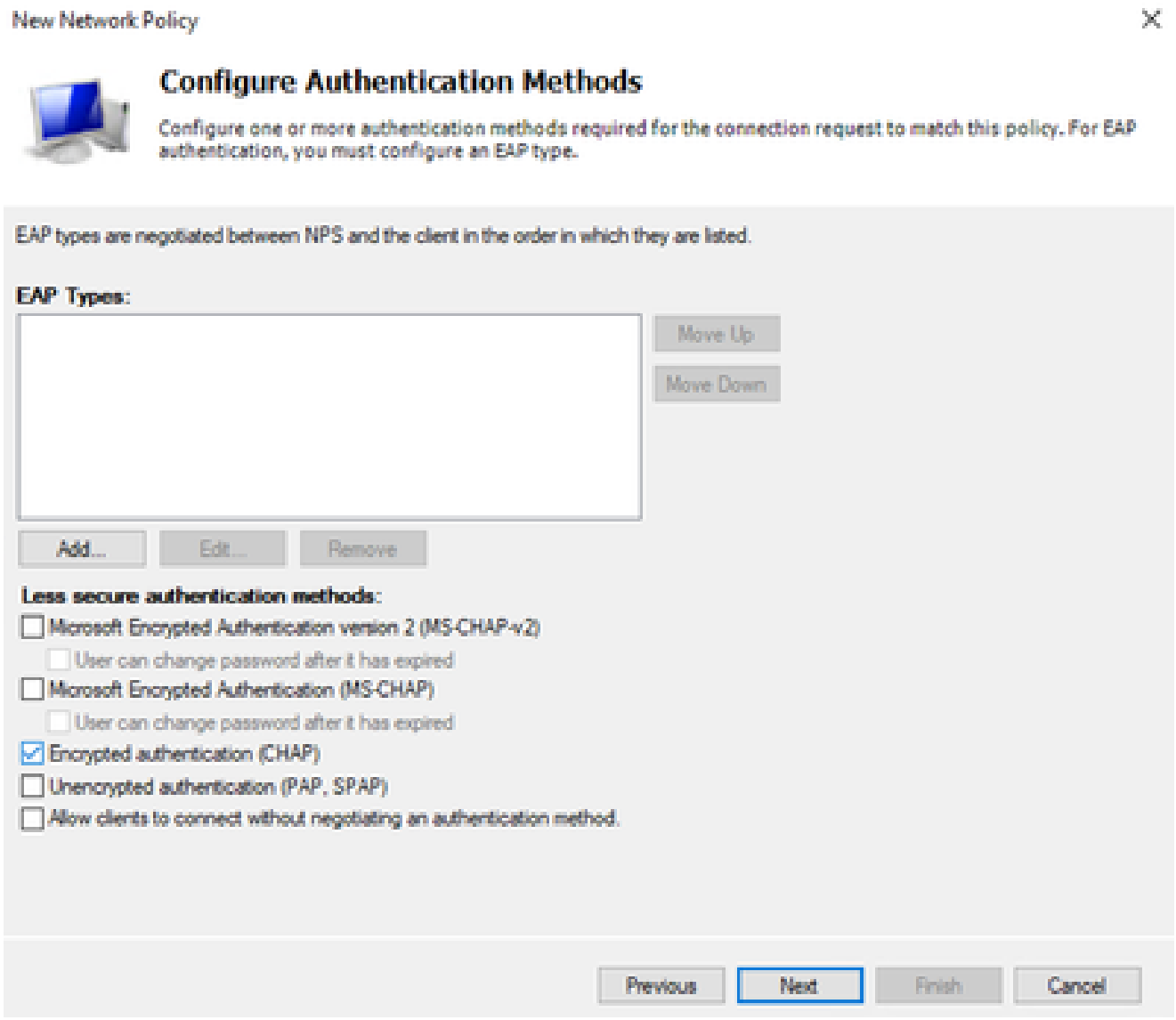
ポリシーの条件

10. Access Grantedを選択し、Nextをクリックします。



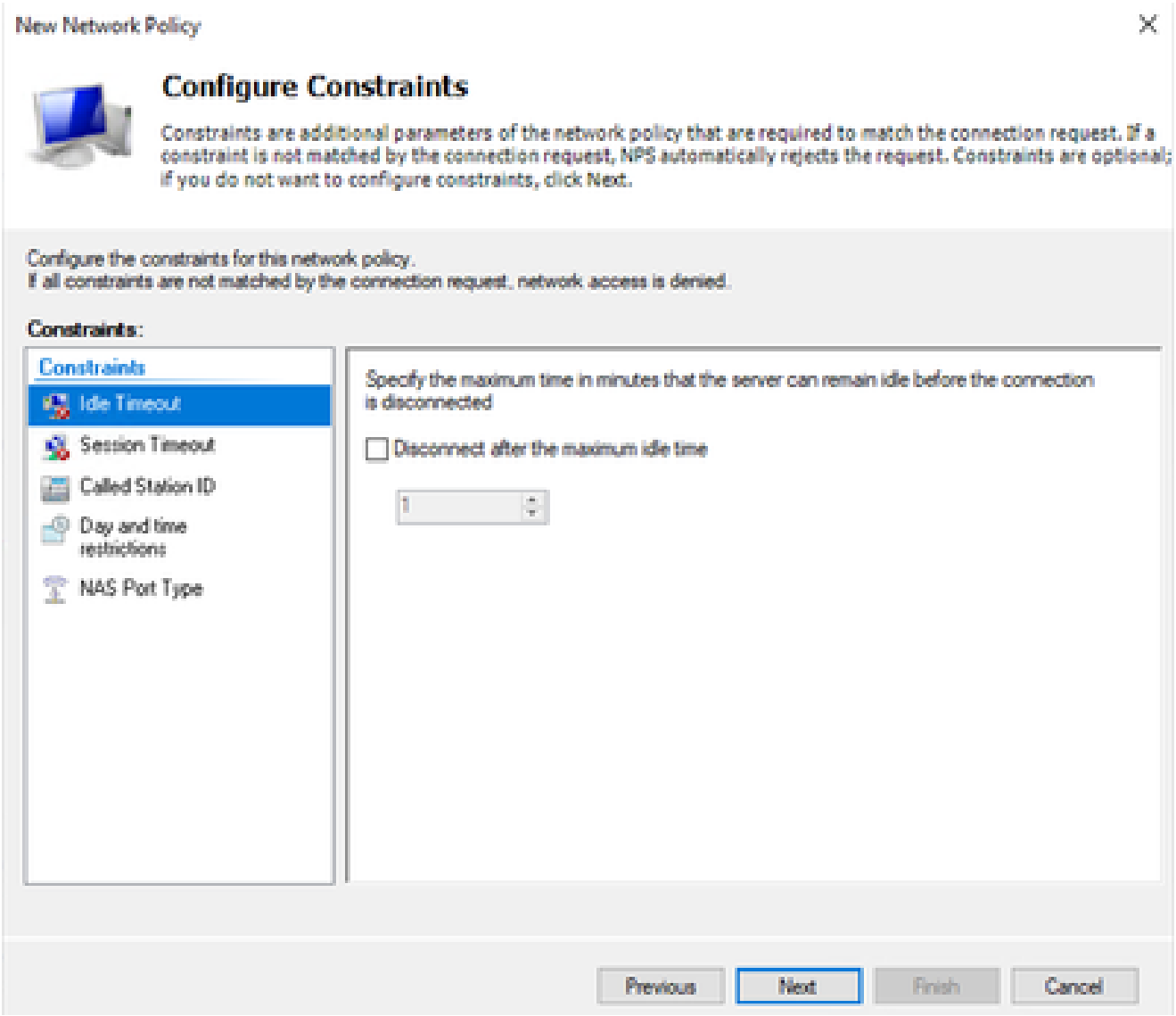
使用アクセス権の付与

11. Unencrypted authentication (PAP, SPAP)のみを選択します。



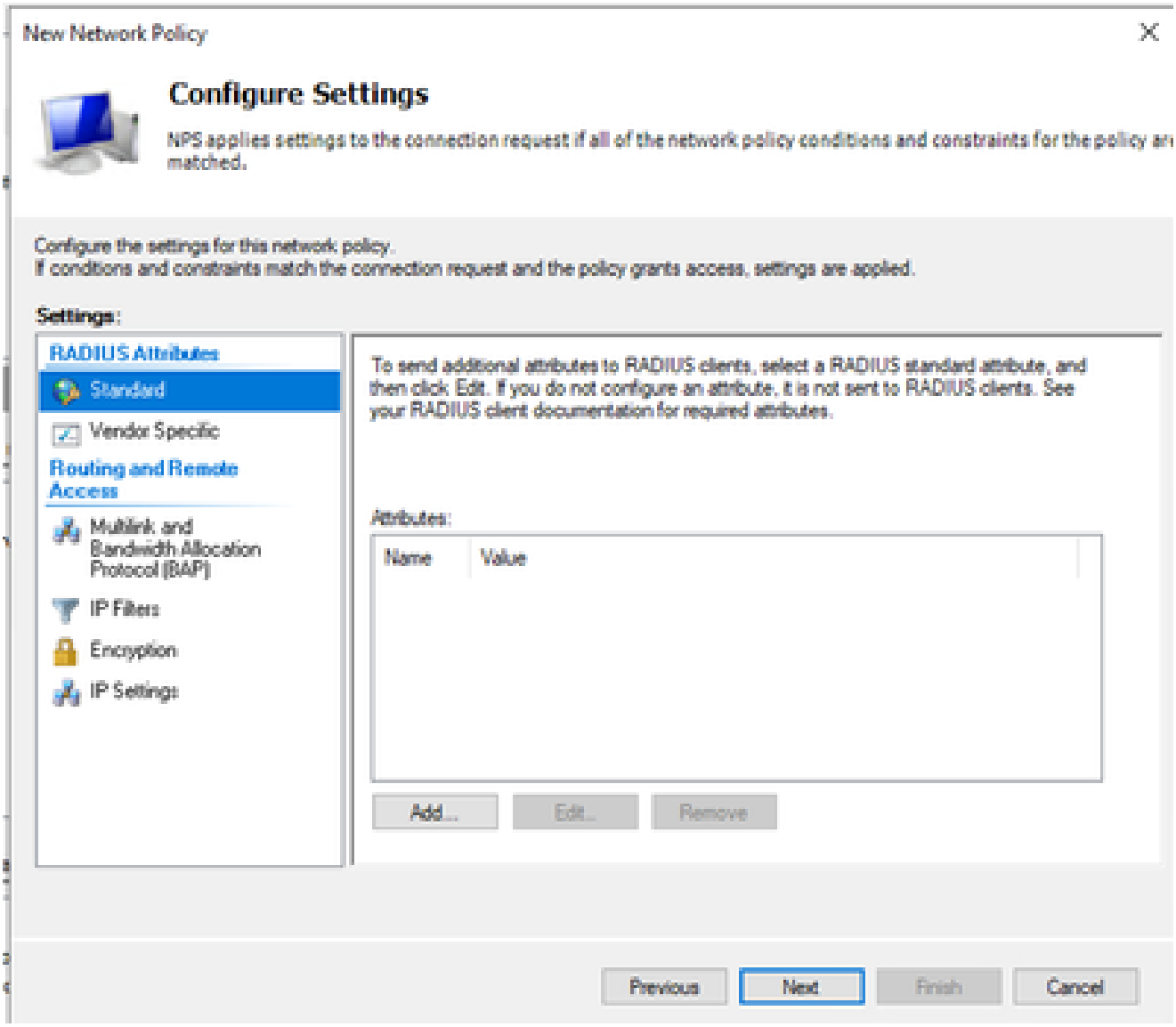
Unencrypted authenticationを選択します

12. デフォルト値が使用されるため、Nextを選択します。



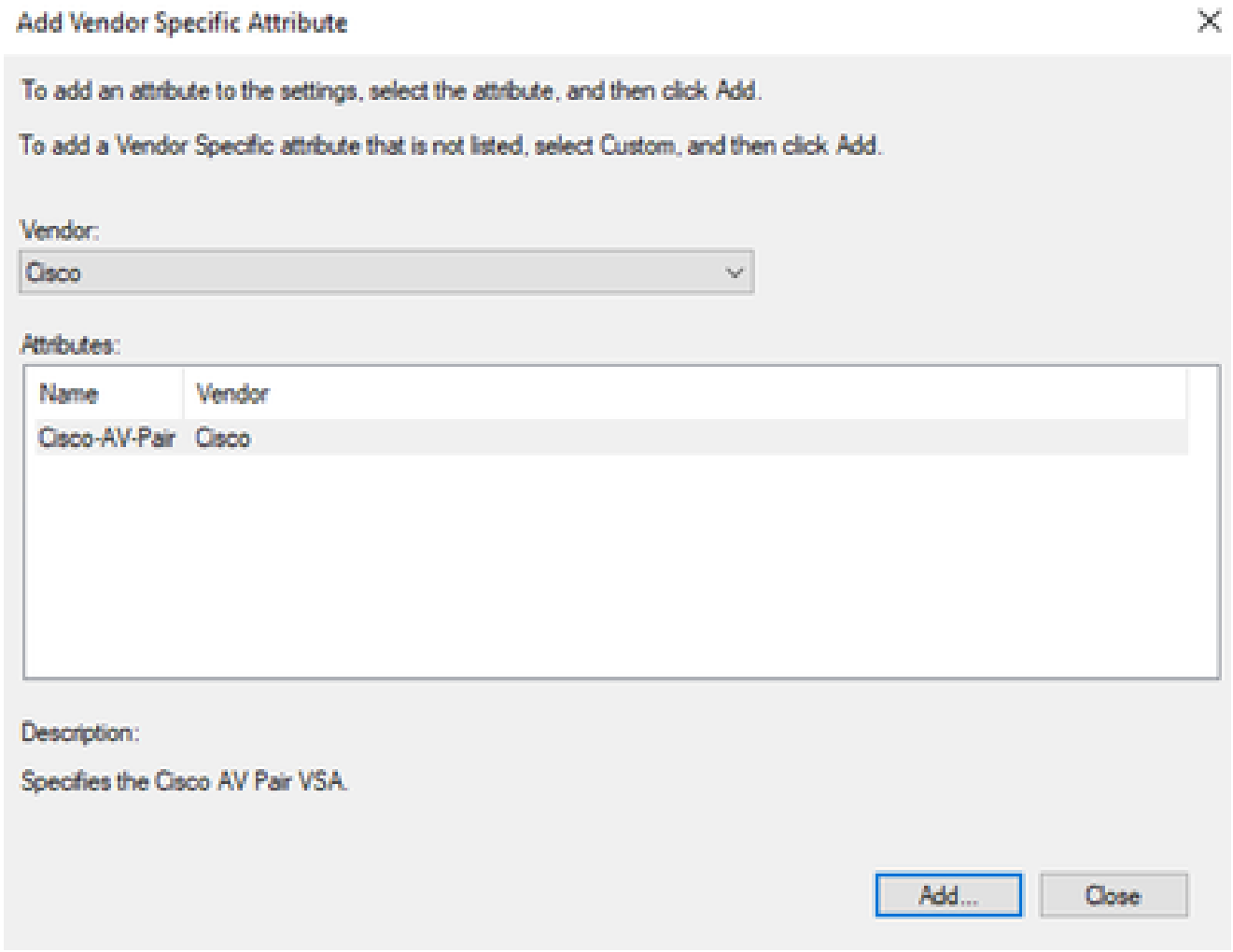
Configure Constraintウィンドウ

13. 標準属性を削除：



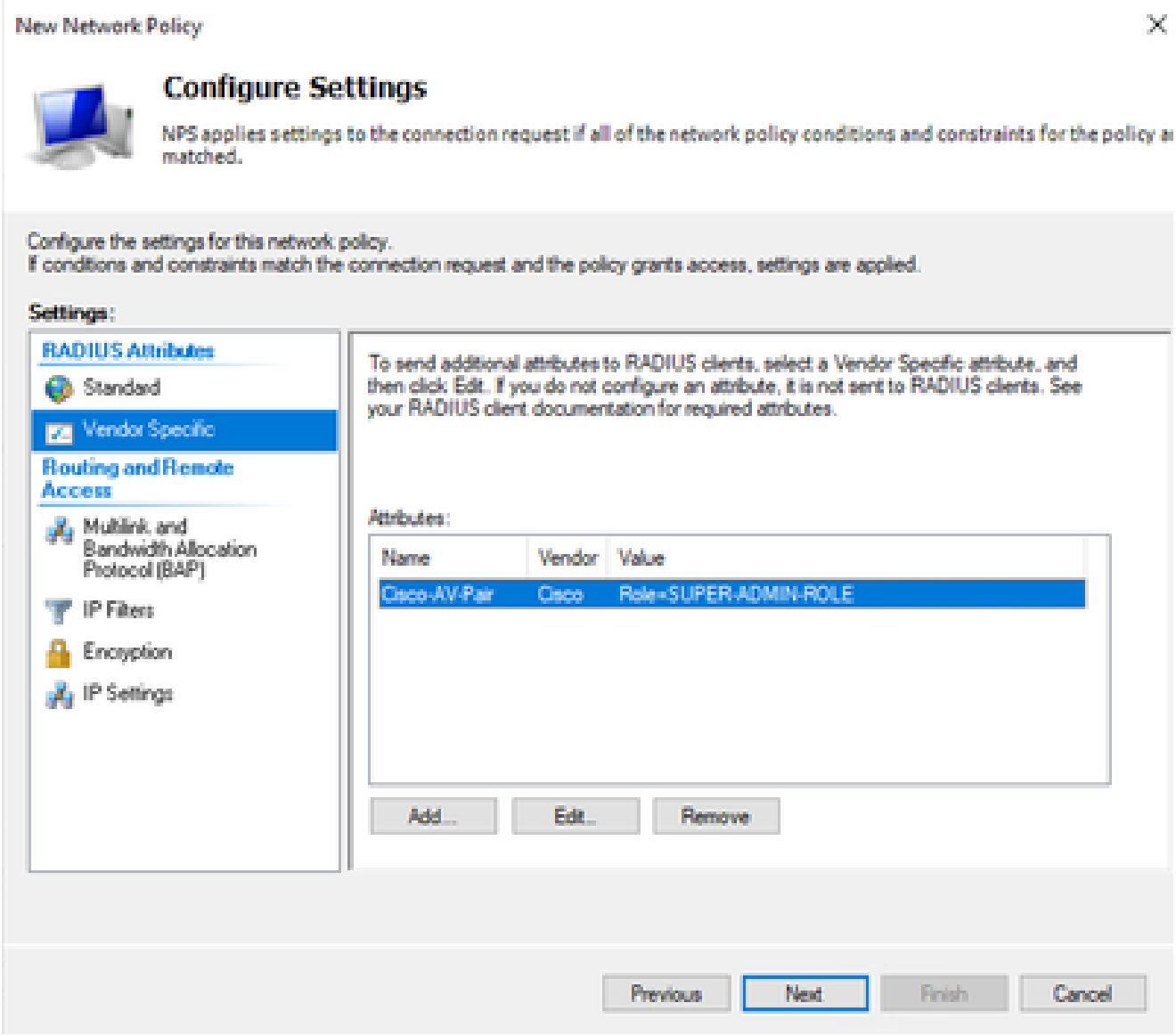
使用する属性の定義

14. RADIUS Attributesで、Vendor Specificを選択し、Addをクリックし、Ciscoをベンダーとして選択し、Addをクリックします。



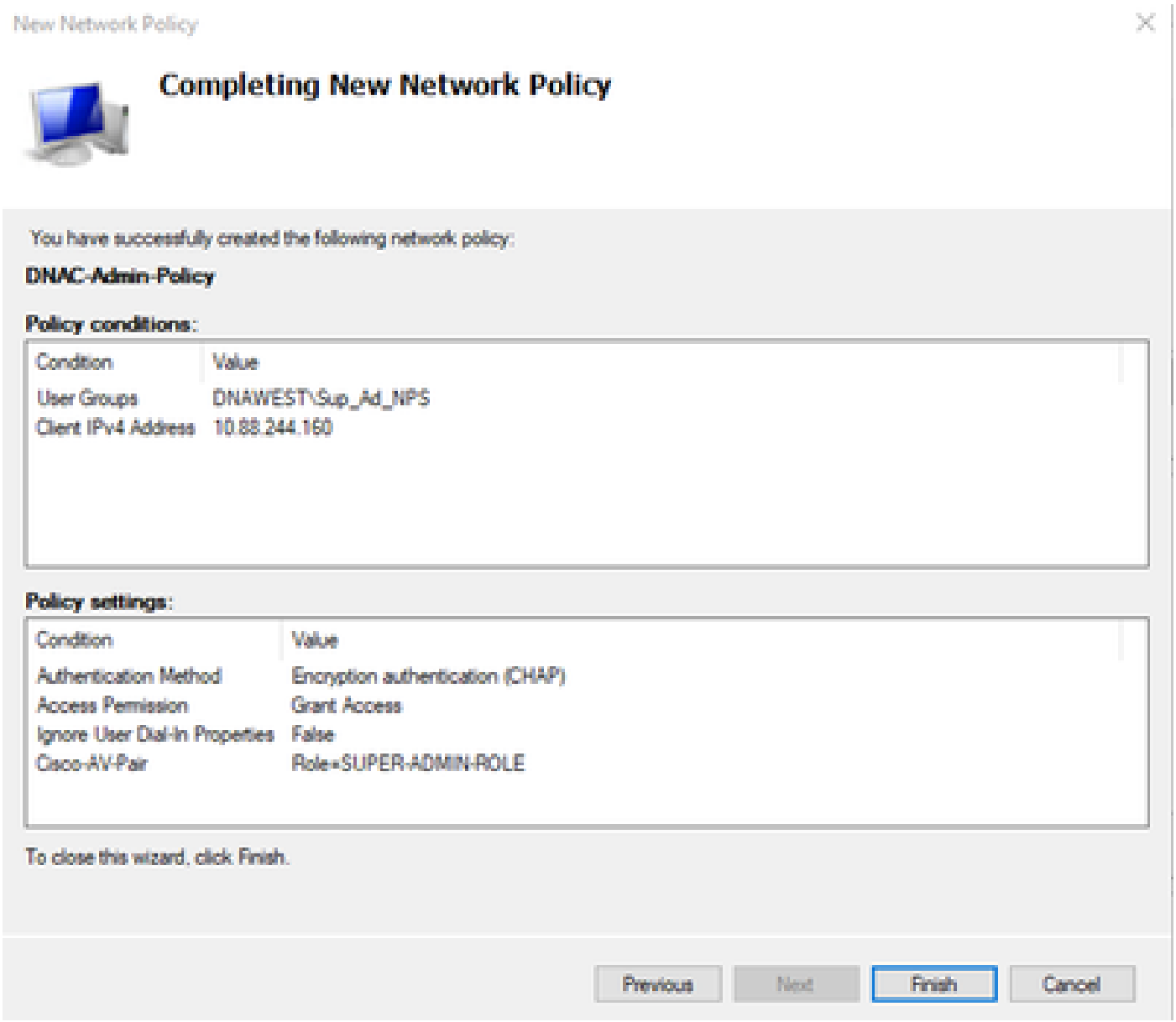
Cisco AVペアの追加

15. Addをクリックし、Role=SUPER-ADMIN-ROLEと入力して、OKを2回クリックします。



Cisco AVペア属性が追加されました

16. Closeを選択してからNextを選択します。
17. ポリシー設定を確認し、Finishを選択して保存します。



ポリシーの概要

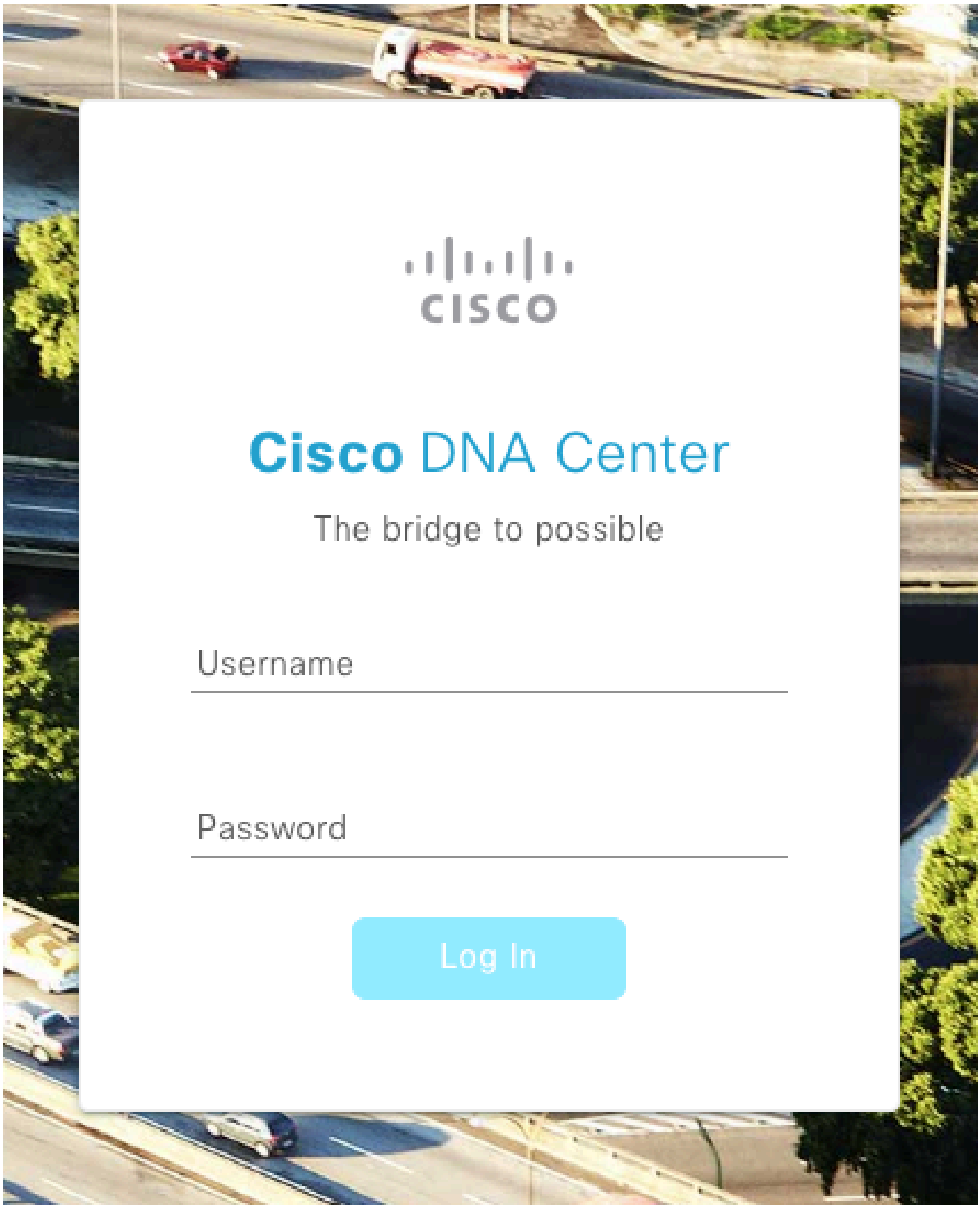
オブザーバロールポリシー。

1. WindowsのStartメニューをクリックして、NPSを検索します。次に、Network Policy Serverを選択します。
2. 左側のナビゲーションパネルで、NPS（ローカル）オプションを右クリックし、Register server in Active Directoryを選択します。
3. OKを2回クリックします。
4. RADIUS Clients and Serversを展開して、RADIUS Clientsを右クリックし、Newを選択します。
5. フレンドリ名、Cisco DNA Center管理IPアドレス、および共有秘密を入力します（これは後で使用できます）。
6. OKをクリックして保存します。

7. Policiesを展開して、Network Policiesを右クリックし、Newを選択します。
8. ルールのポリシー名を入力し、Nextをクリックします。
9. 特定のドメイングループを許可するには、次の2つの条件を追加してNextを選択します。
    - User Group:Cisco DNA Centerでオブザーバロールを割り当てるために、ドメイングループを追加します（この例ではObserver_NPSグループを使用）。
    - ClientIPv4Address:Cisco DNA Center管理IPを追加します。
10. Access Grantedを選択してからNextを選択します。
11. Unencrypted authentication (PAP, SPAP)だけを選択します。
12. デフォルト値が使用されるため、Nextを選択します。
13. Standard属性を削除します。
14. RADIUS Attributesで、Vendor Specificを選択し、Addをクリックし、ベンダーとしてCiscoを選択し、Addをクリックします。
15. Addを選択し、ROLE=OBSERVER-ROLEと入力して、OKを2回押します。
16. Close、Nextの順に選択します。
17. ポリシー設定を確認し、Finishを選択して保存します。

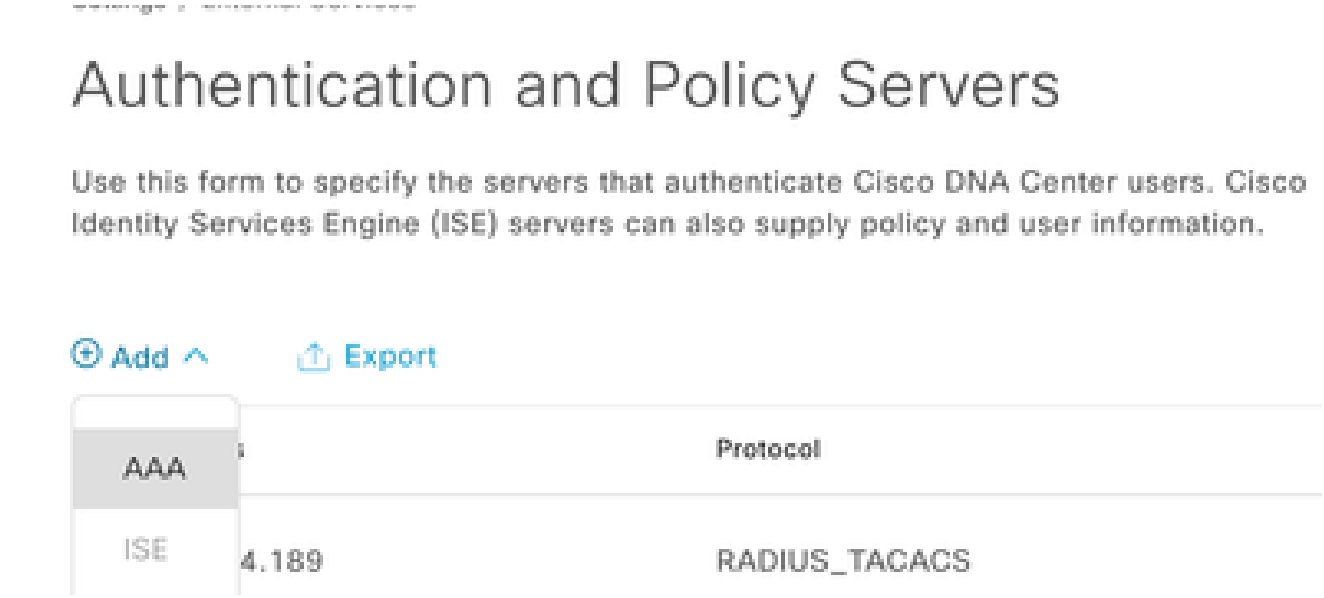
外部認証の有効化

1. WebブラウザでCisco DNA Centerのグラフィカルユーザインターフェイス(GUI)を開き、admin特権アカウントを使用してログインします。



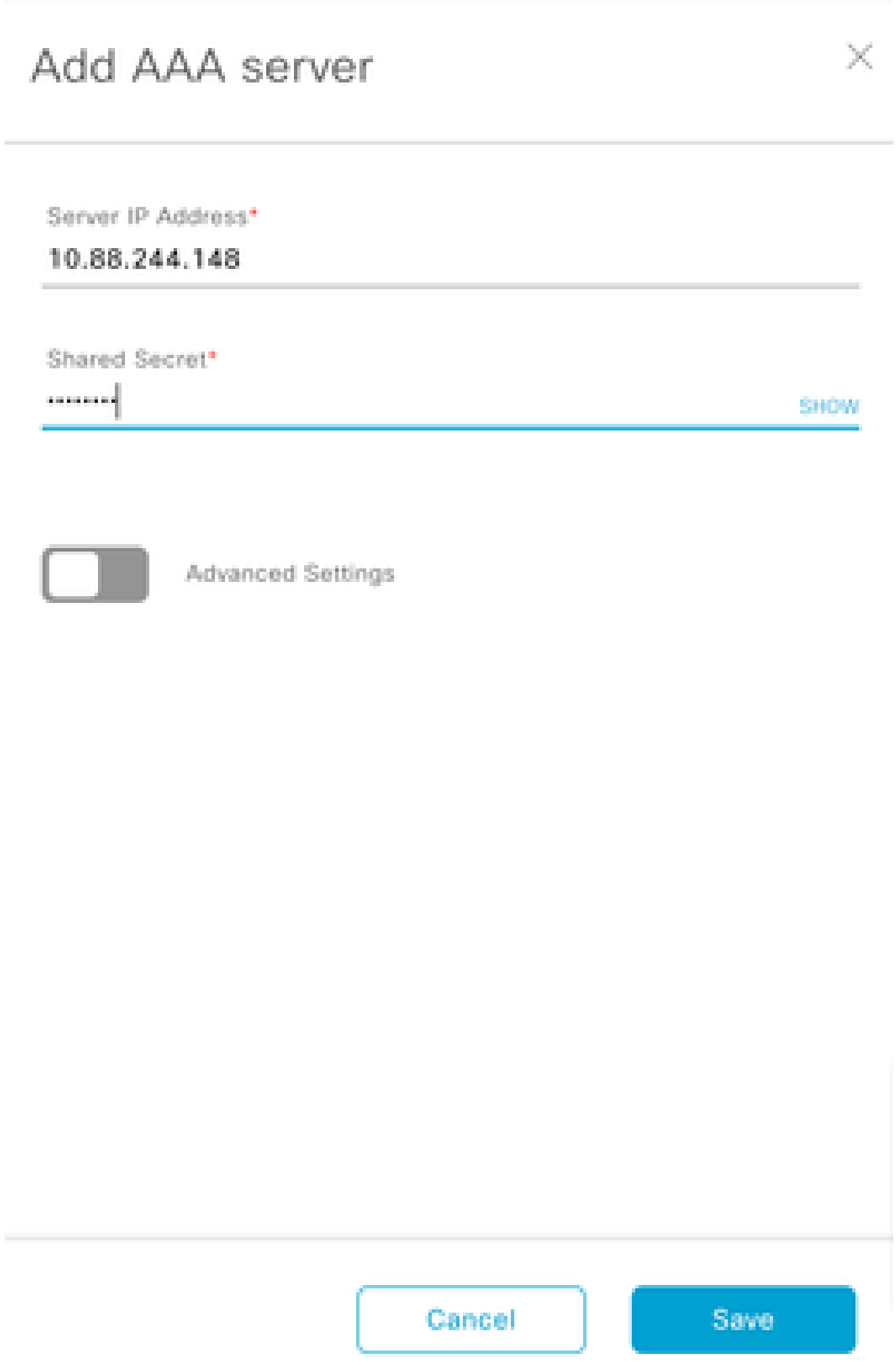
Cisco DNA Centerログインページ

2. Menu > System > Setting > Authentication and Policy Serversの順に移動し、Add > AAAの順に選択します。



Windows Serverの追加

3. Windows ServerのIPアドレスと前の手順で使用した共有秘密を入力し、Saveをクリックします。

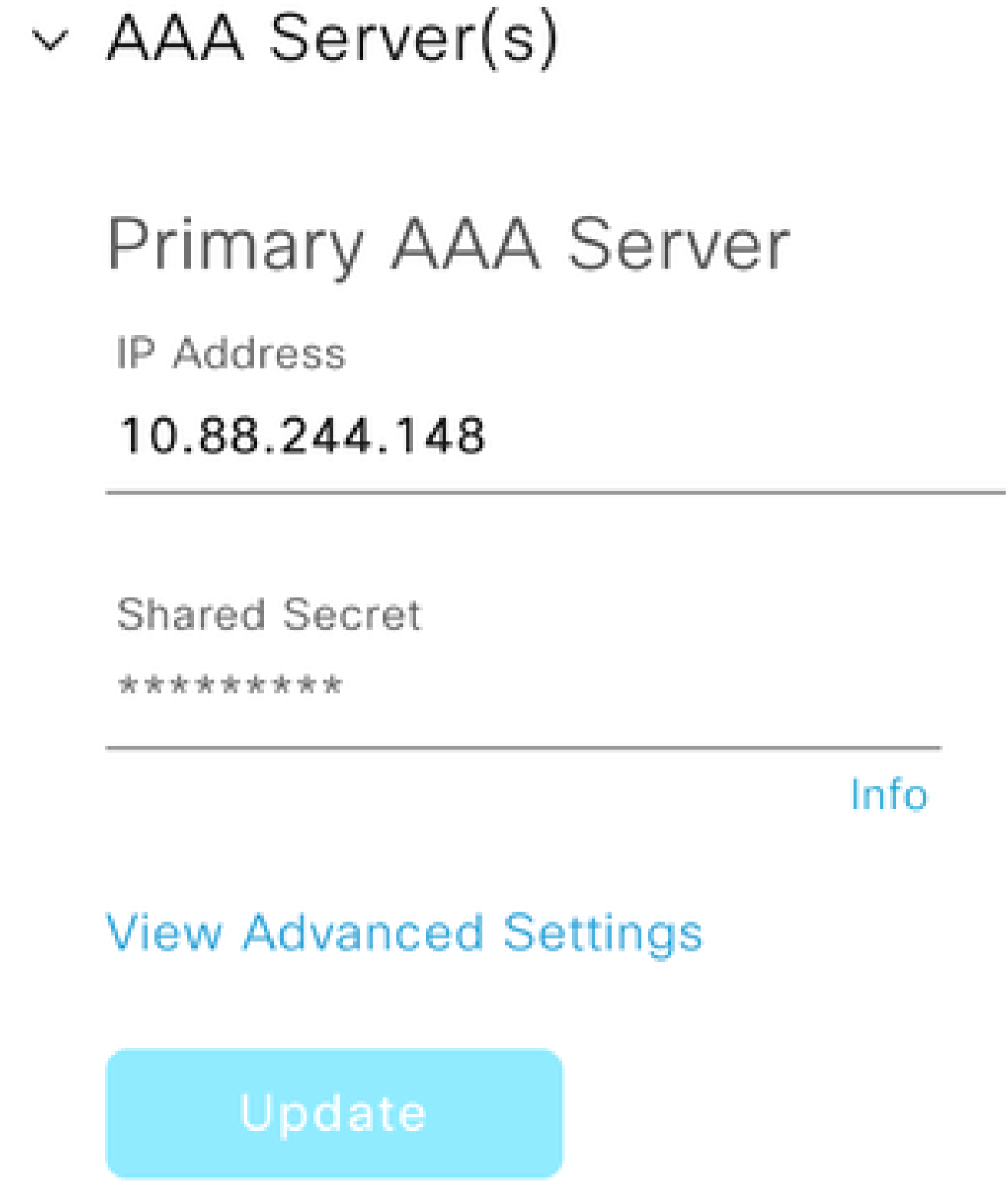


Windows Serverの値

4. Windows Serverのステータスがactiveであることを確認します。

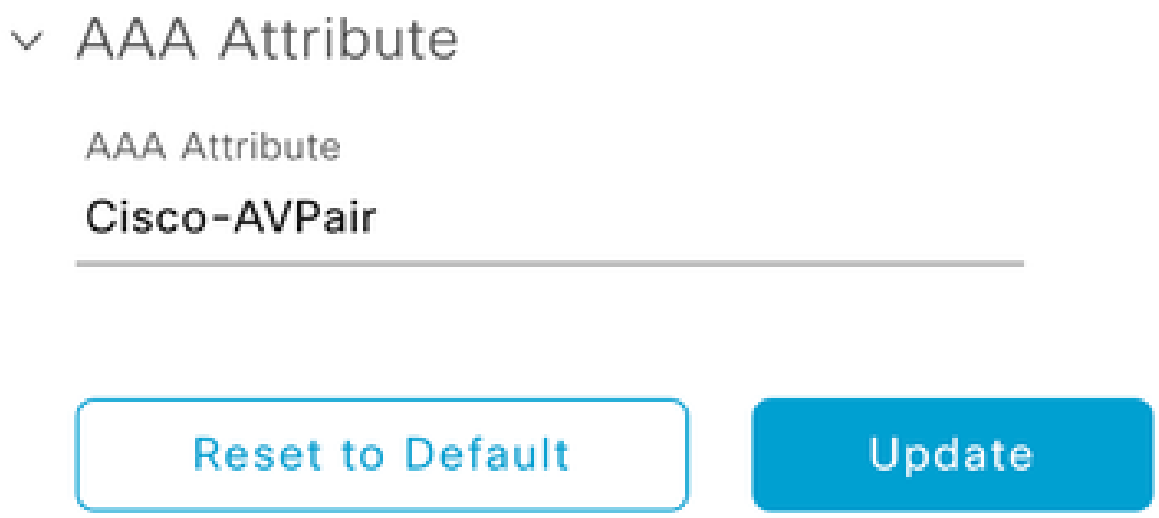
Windows Serverの概要

5. Menu > System > Users & Roles > External Authenticationの順に移動し、AAAサーバを選択します。



AAAサーバとしてのWindowsサーバ

6. AAA属性としてCisco-AVPairと入力し、Updateをクリックします。

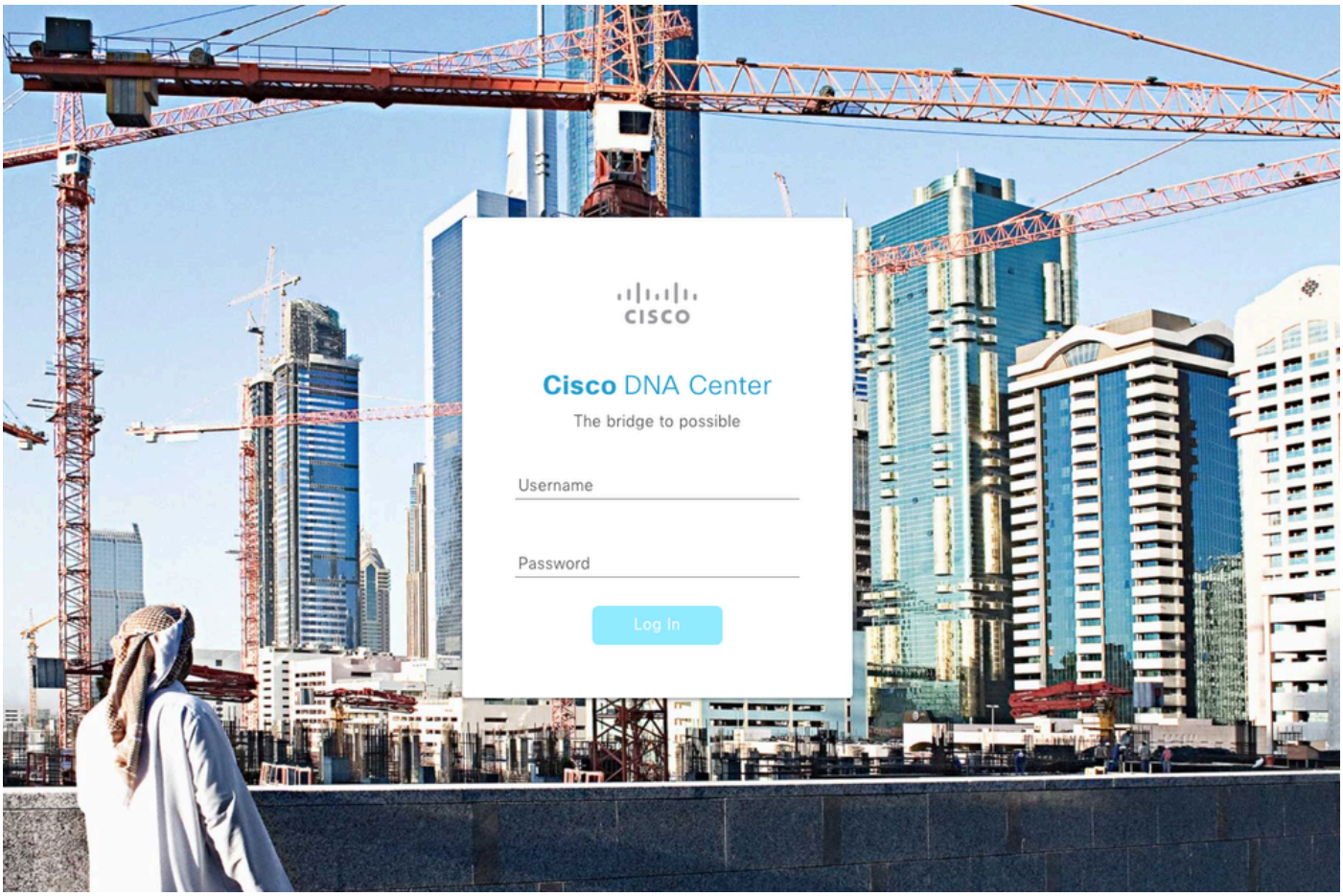


外部ユーザのAVペア

7. Enable External Userチェックボックスをクリックして、外部認証を有効にします。

確認

Cisco DNA Centerのグラフィカルユーザインターフェイス(GUI)をWebブラウザで開き、Windowsサーバで設定した外部ユーザでログインして、外部認証を使用して正常にログインできることを確認できます。



Cisco DNA Centerログインページ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。