

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

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[管理者ロールポリシー](#)

[オブザーバロールポリシー。](#)

[外部認証の有効化](#)

[確認](#)

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。

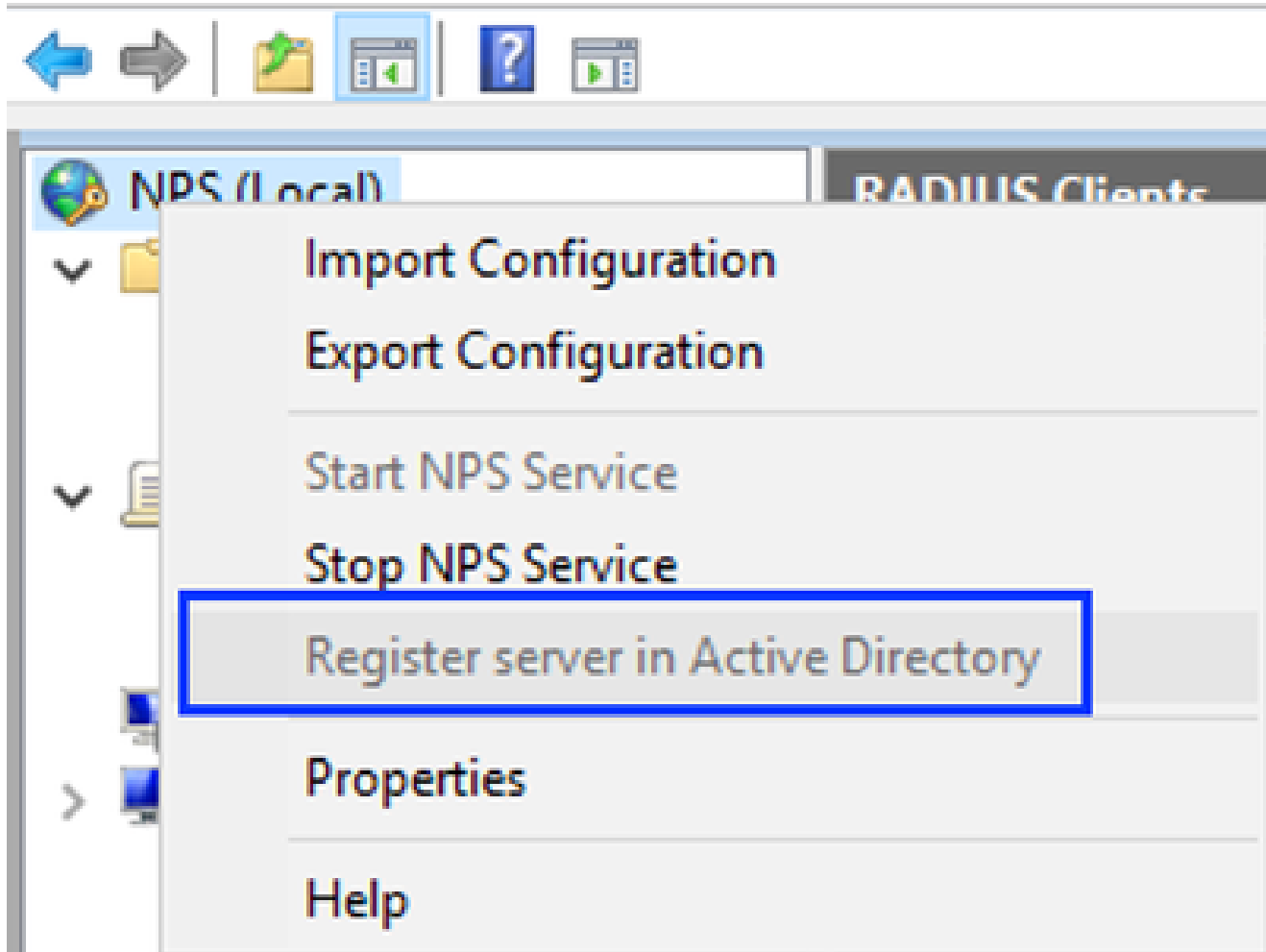


Network Policy Server

Desktop app

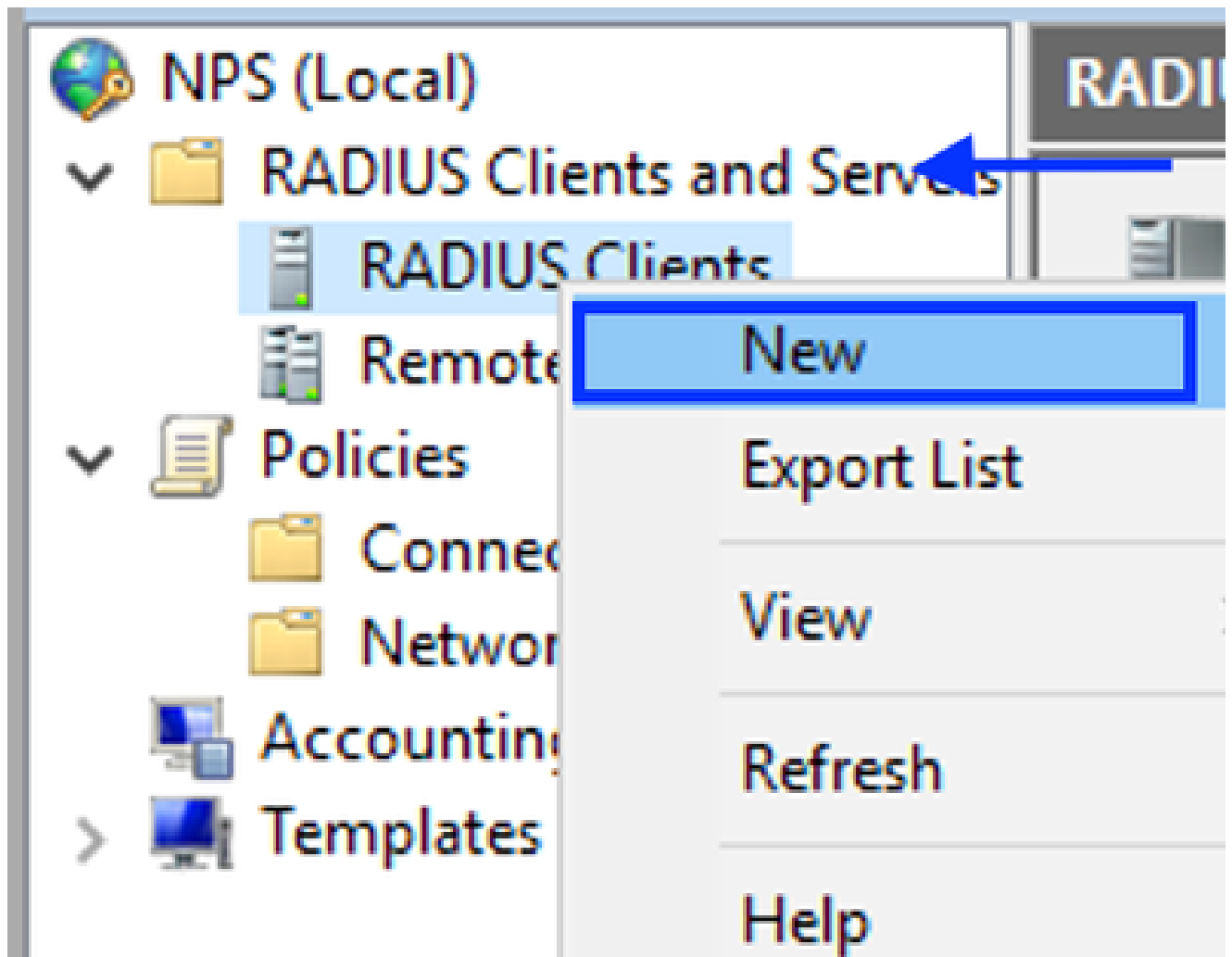
Network Policy Server

File Action View Help



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）。

DNAC Properties X

Settings **Advanced**

Enable this RADIUS client

Select an existing template:

Name and Address

Friendly name:

Address (IP or DNS):

Shared Secret

Select an existing Shared Secrets template:

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

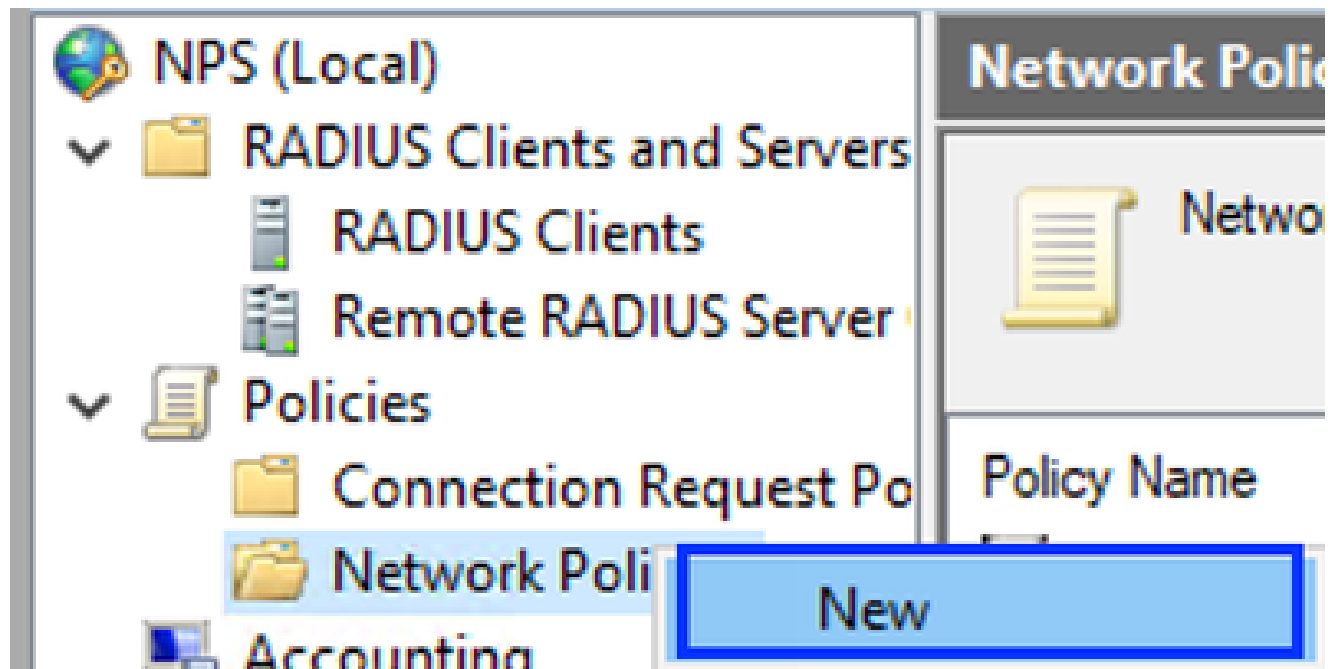
Manual Generate

Shared secret:

Confirm shared secret:

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。



Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
DNAC-Admin-Policy

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

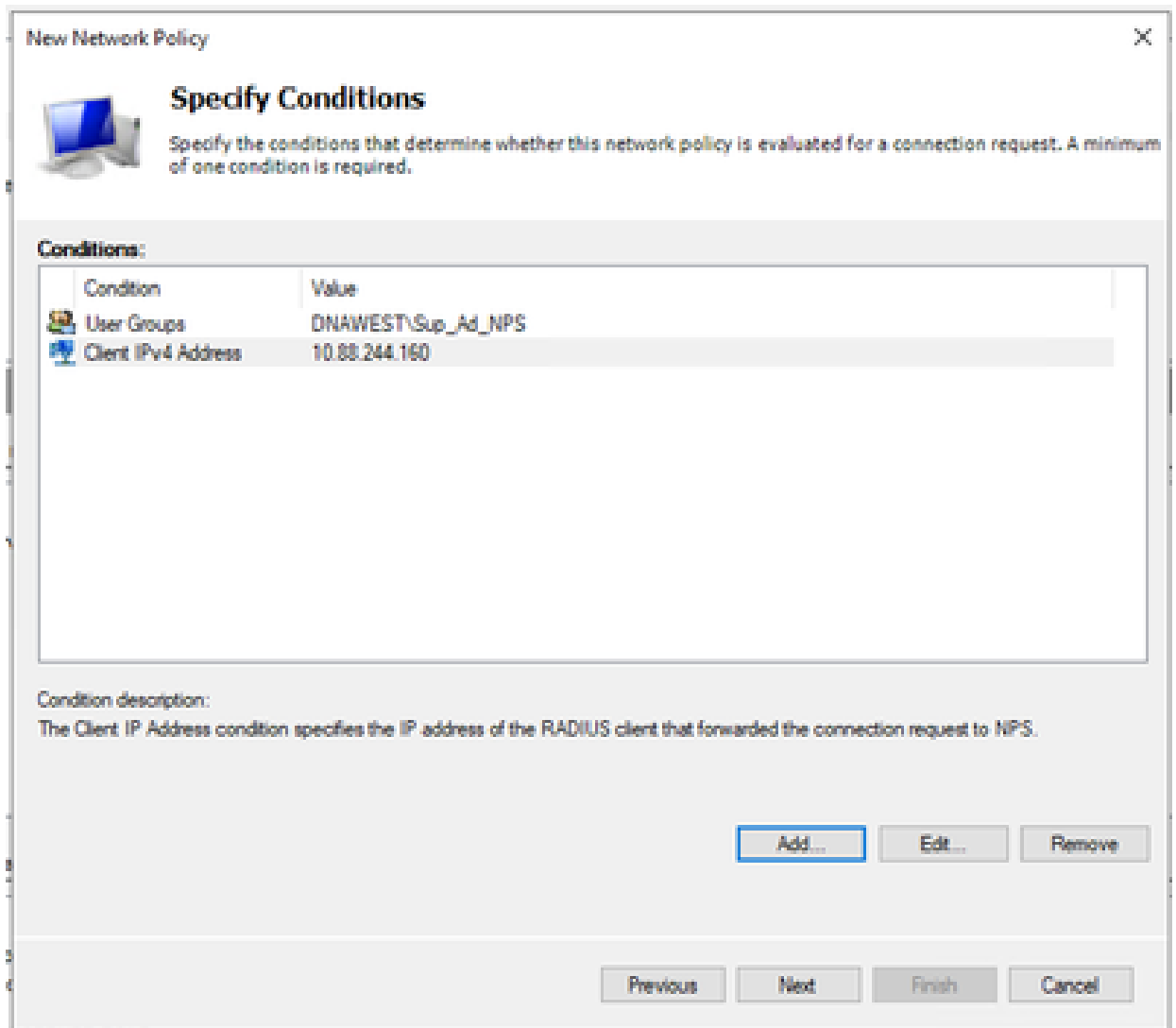
Type of network access server:
Unspecified

Vendor specific:
10

Previous Next Finish Cancel

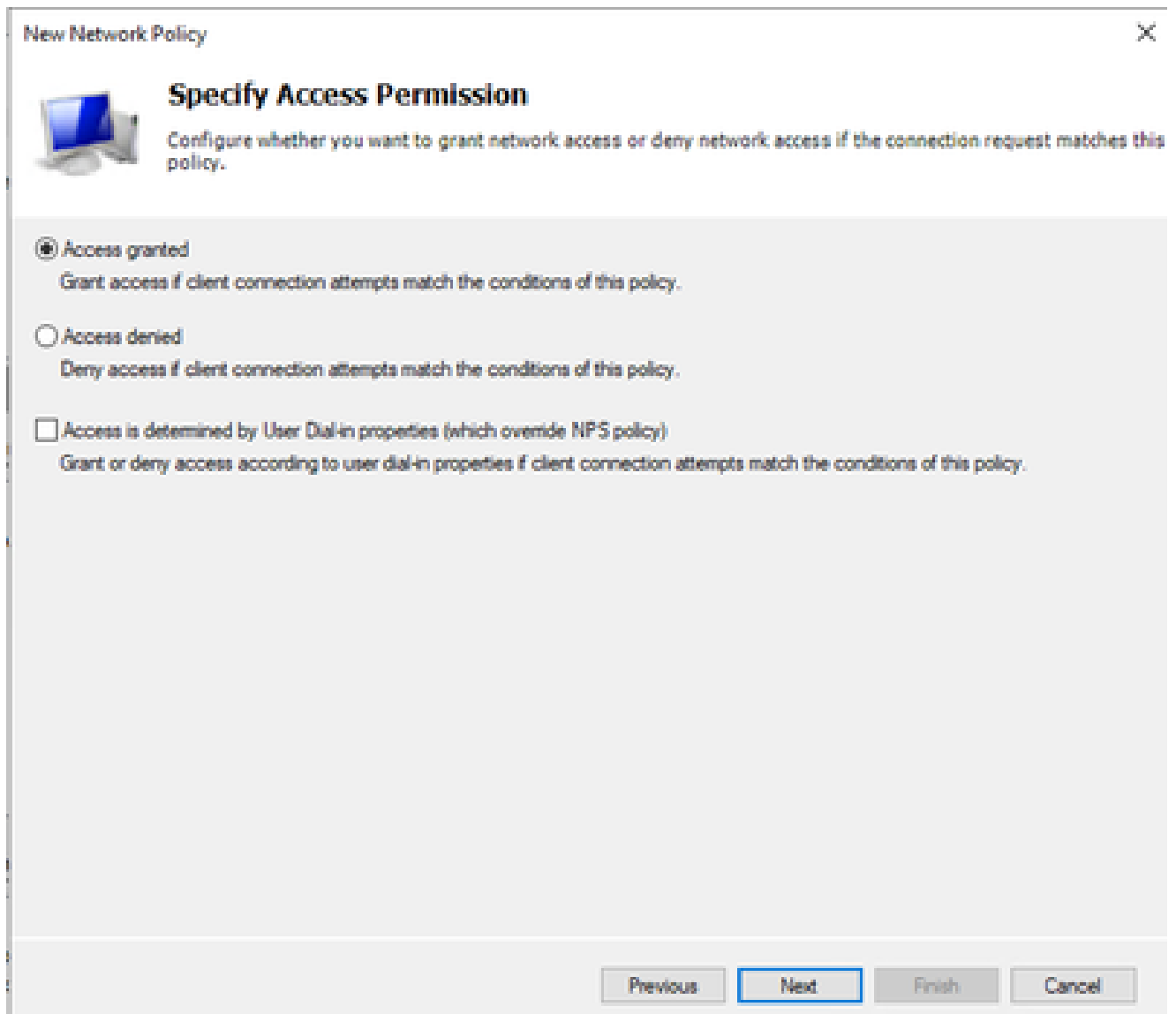
ポリシー名

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。



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up

Move Down

Add...

Edit...

Remove

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
 - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.

Previous

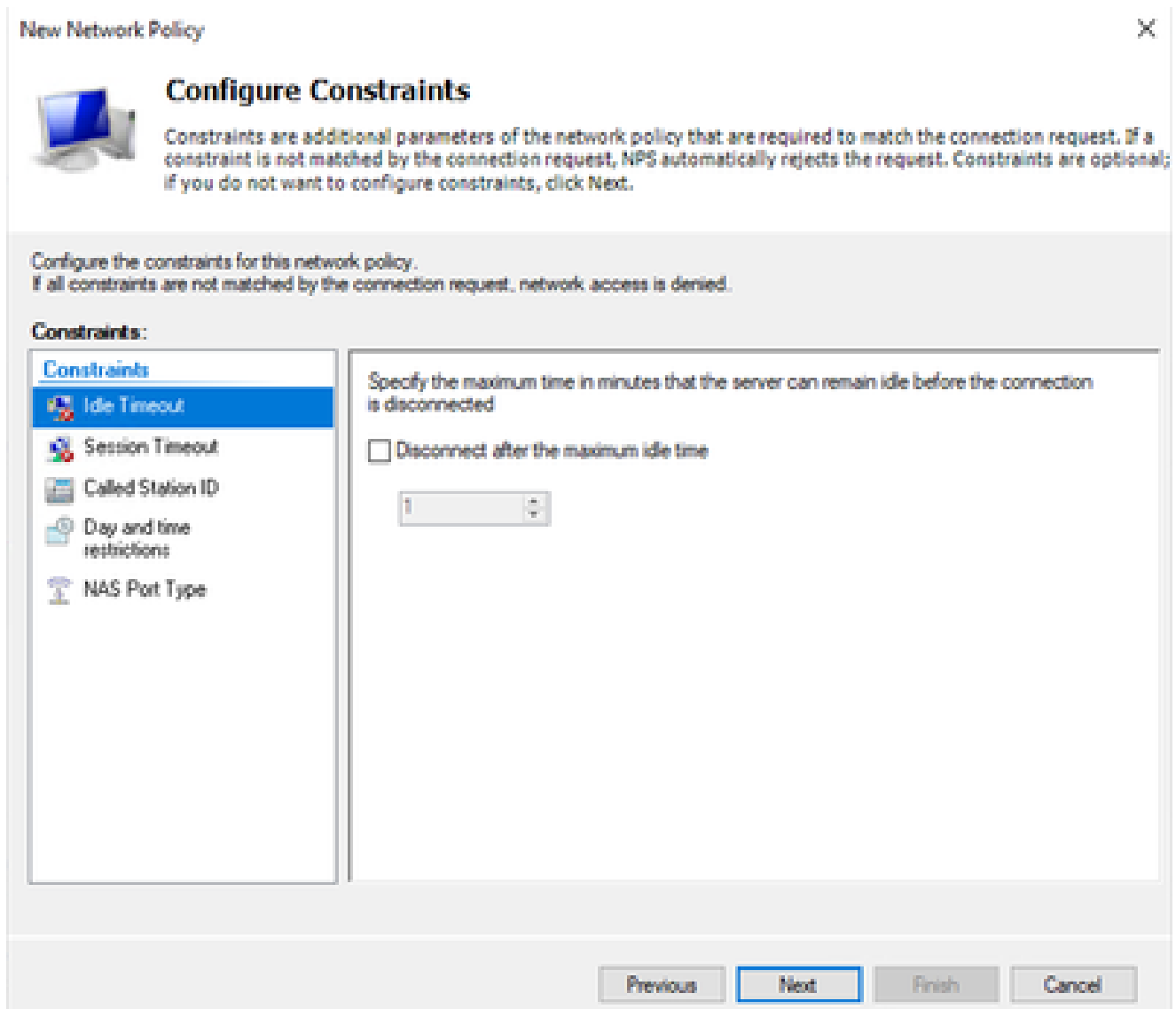
Next

Finish

Cancel

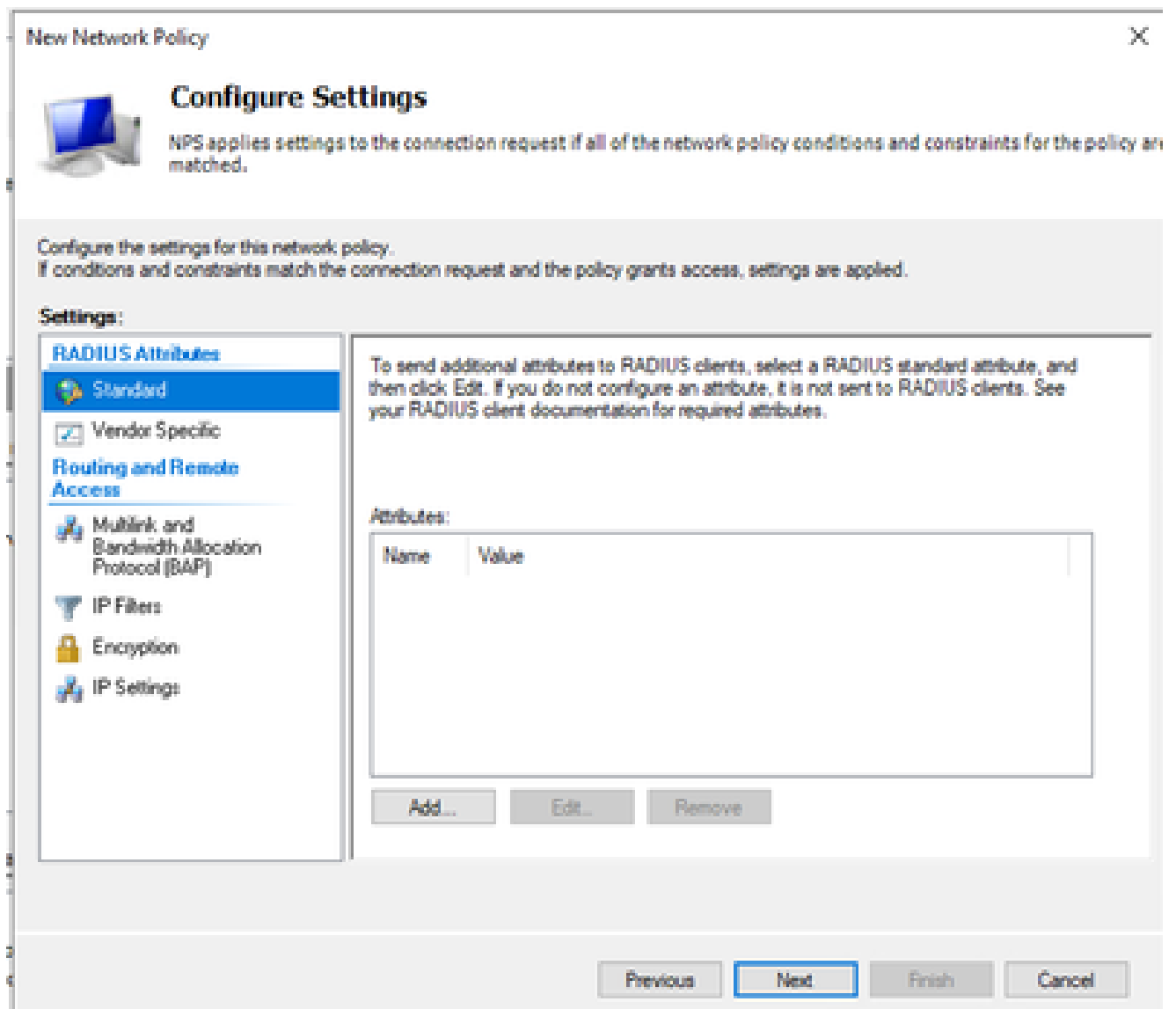
Unencrypted authenticationを選択します

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。

Add Vendor Specific Attribute



To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:

Disco

Attributes:

Name	Vendor
Cisco-AV-Pair	Cisco

Description:

Specifies the Cisco AV Pair VSA.

Add...

Close

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。



Configure Settings

NPS applies settings to the connection request if **all** of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.

If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

Standard

Vendor Specific

Routing and Remote Access

Multilink and Bandwidth Allocation Protocol (BAP)

IP Filters

Encryption

IP Settings

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Cisco-AV-Pair	Cisco	Role=SUPER-ADMIN-ROLE

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

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。



Completing New Network Policy

You have successfully created the following network policy:

DNAC-Admin-Policy

Policy conditions:

Condition	Value
User Groups	DNAWEST\Sup_Ad_NPS
Client IPv4 Address	10.88.244.160

Policy settings:

Condition	Value
Authentication Method	Encryption authentication (CHAP)
Access Permission	Grant Access
Ignore User Dial-In Properties	False
Cisco-AV-Pair	Role=SUPER-ADMIN-ROLE

To close this wizard, click Finish.

Previous

Next

Finish

Cancel

ポリシーの概要

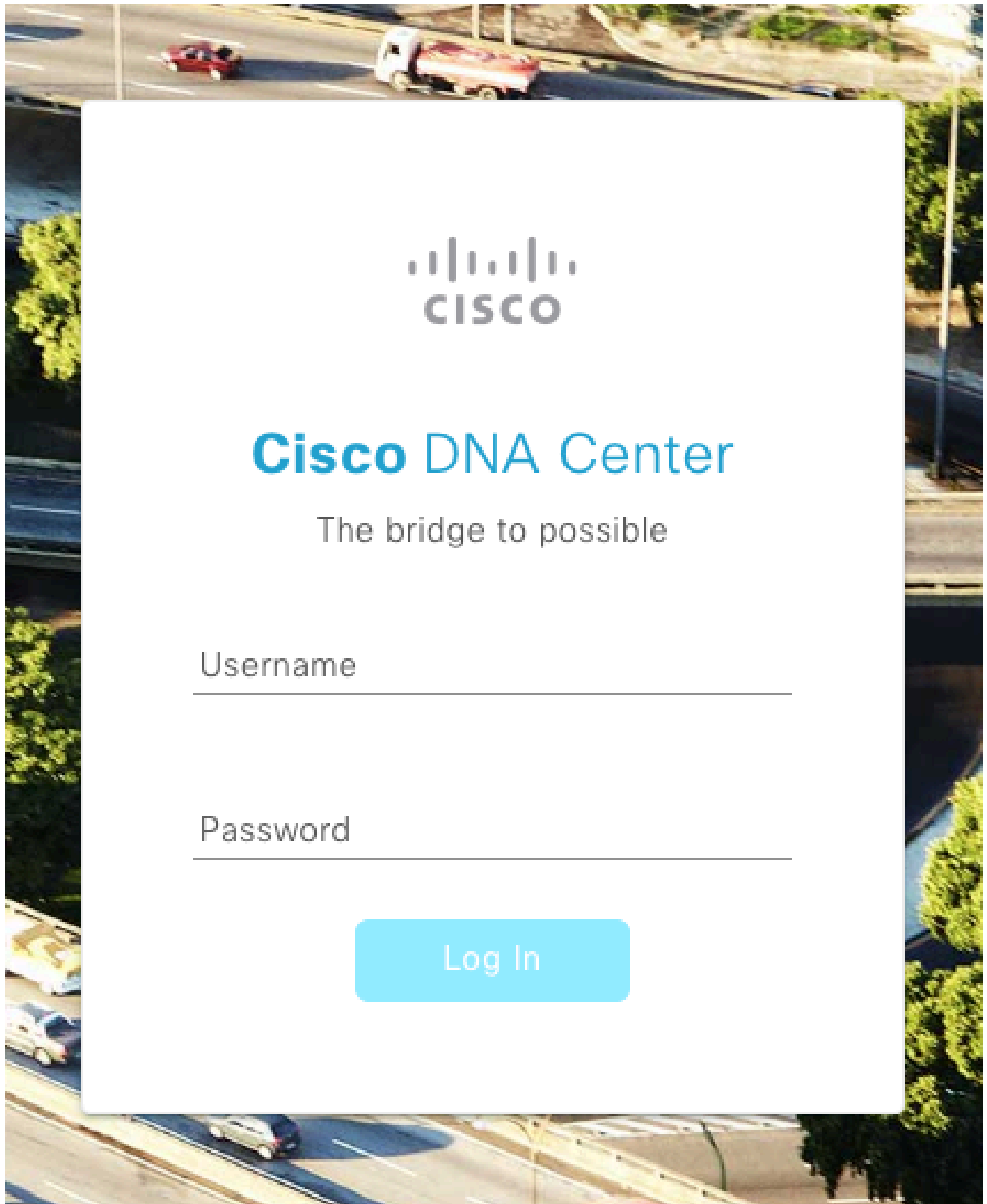
オブザーバロールポリシー。

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。

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

⊕ Add ^ ↑ Export

AAA	Protocol
ISE 4.189	RADIUS_TACACS

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。

Add AAA server



Server IP Address*

10.88.244.148

Shared Secret*

.....|

[SHOW](#)



Advanced Settings

Cancel

Save

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

10.88.244.148

RADIUS

AAA

ACTIVE



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 Server(s)

Primary AAA Server

IP Address

10.88.244.148

Shared Secret

[Info](#)

[View Advanced Settings](#)

Update

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。

▼ AAA Attribute

AAA Attribute

Cisco-AVPair

Reset to Default

Update

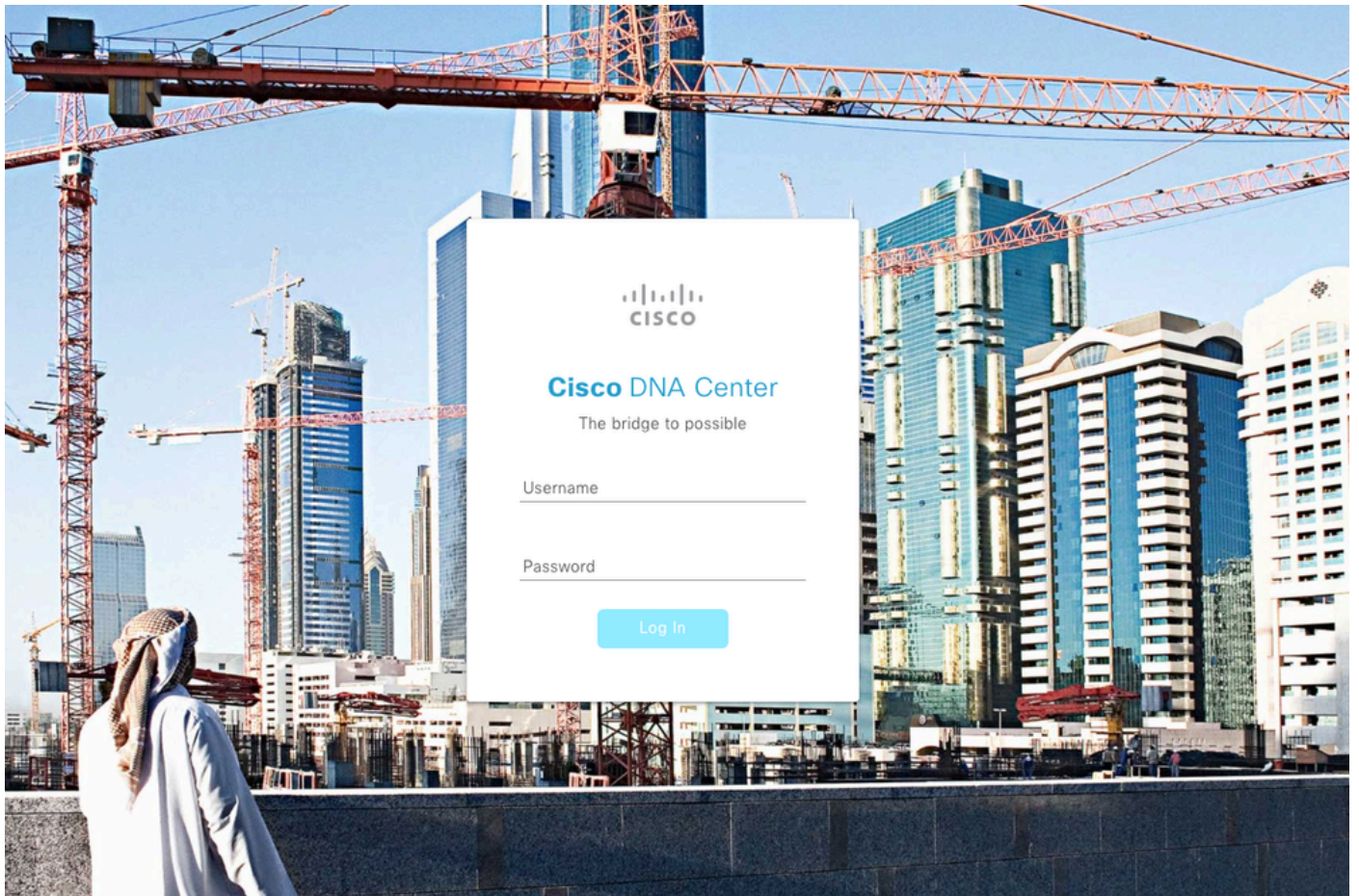
外部ユーザのAVペア

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。

Enable External User 

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。