Configure External Authentication on Catalyst Center using Windows Server

Contents

Introduction

This document describes how to configure External Authentication in Cisco DNA Center using Network Policy Server (NPS) in Windows Server as RADIUS.

Prerequisites

Requirements

Basic Knowledge on:

- Cisco DNA Center Users & Roles
- Windows Server Network Policy Server, RADIUS and Active Directory

Components Used

- Cisco DNA Center 2.3.5.x
- Microsoft Windows Server Version 2019 acting as Domain Controller, DNS Server, NPS and Active Directory

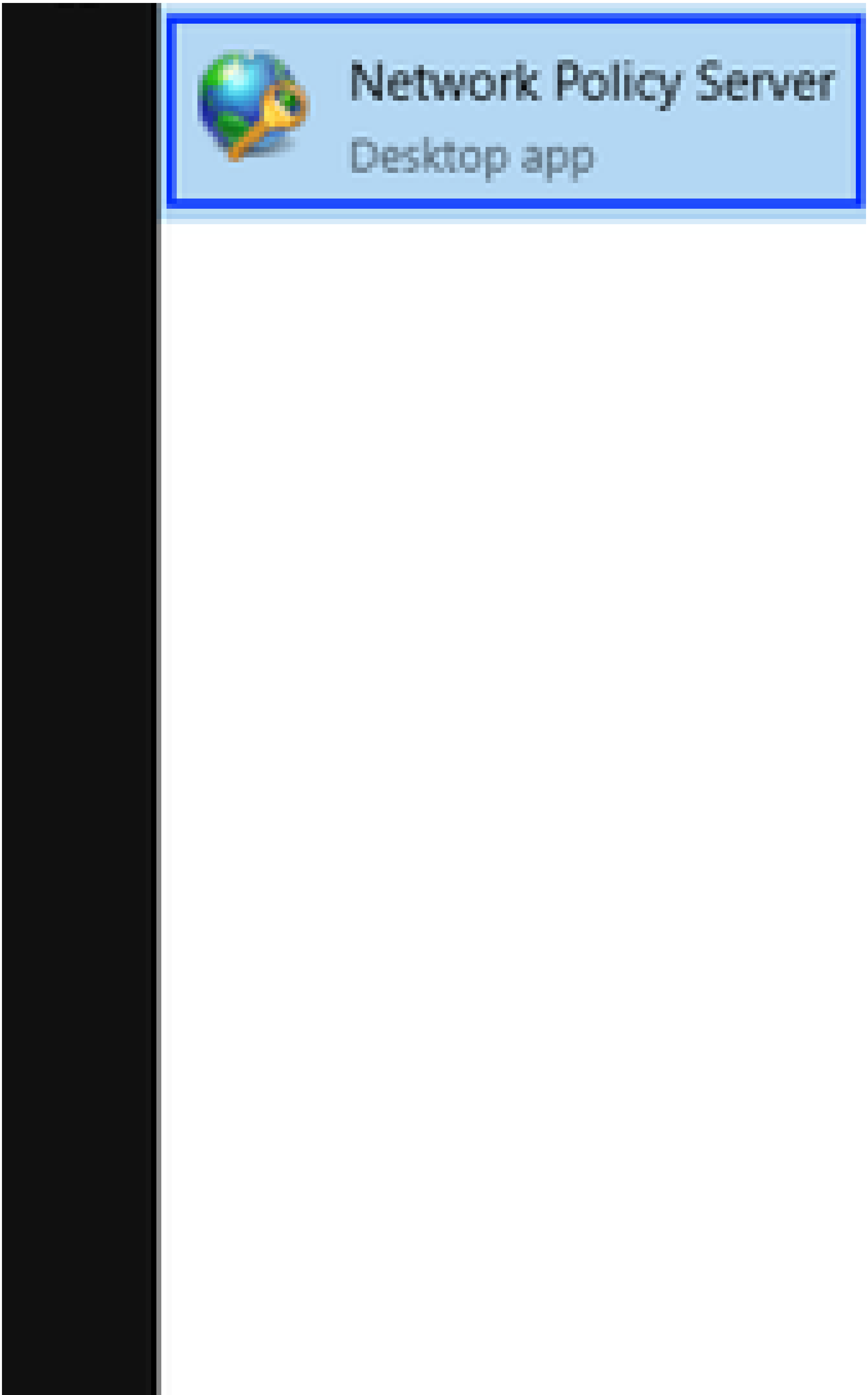
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Note: The Cisco Technical Assistance Center (TAC) does not provide technical support to the Microsoft Windows Server. If you experience issues with the Microsoft Windows Server configuration, please contact Microsoft Support for technical assistance.

Configure

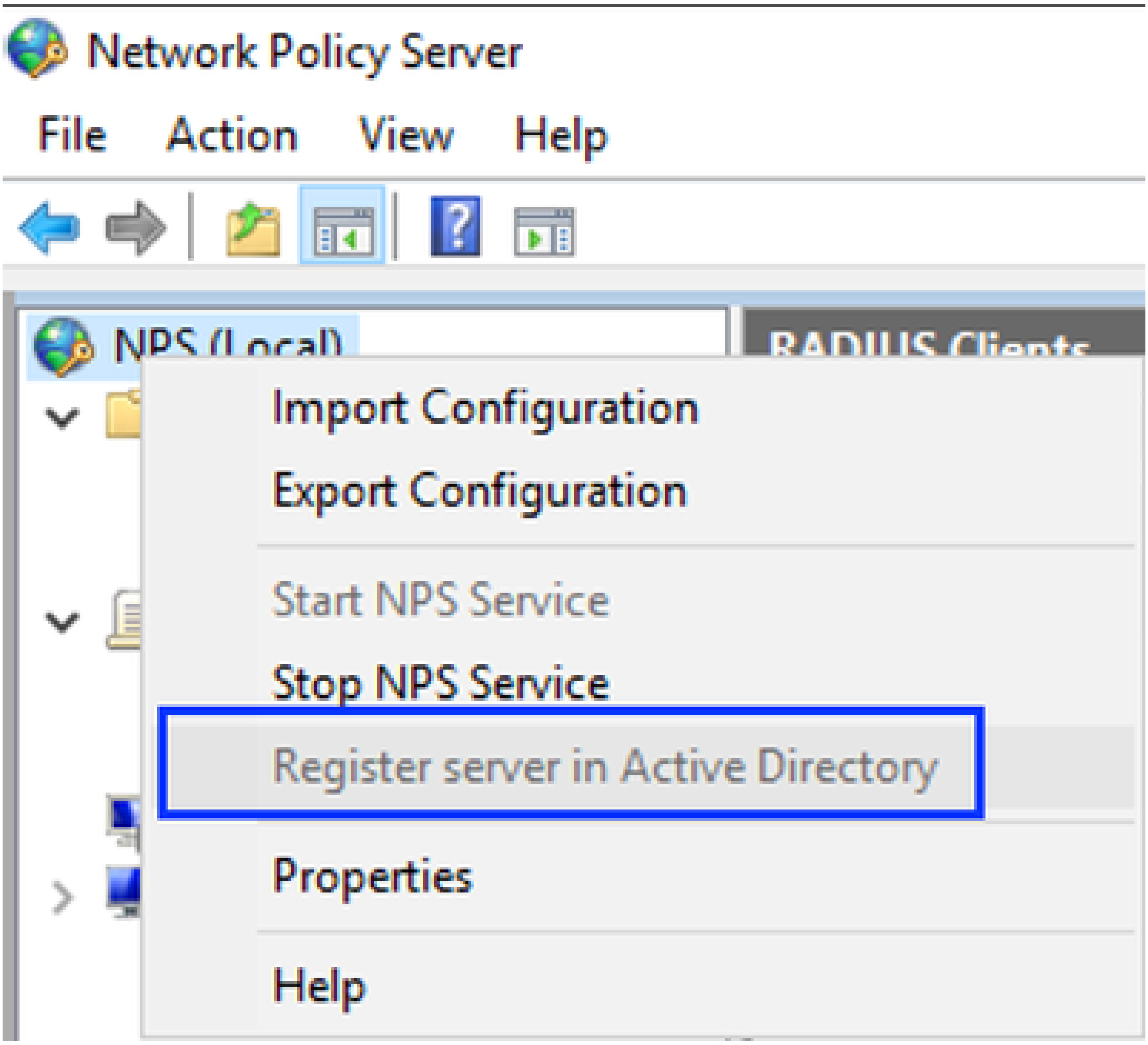
Admin Role Policy

1. Click in the **Windows Start** menu and search for **NPS**. Then select **Network Policy Server**:



Network Policy Server

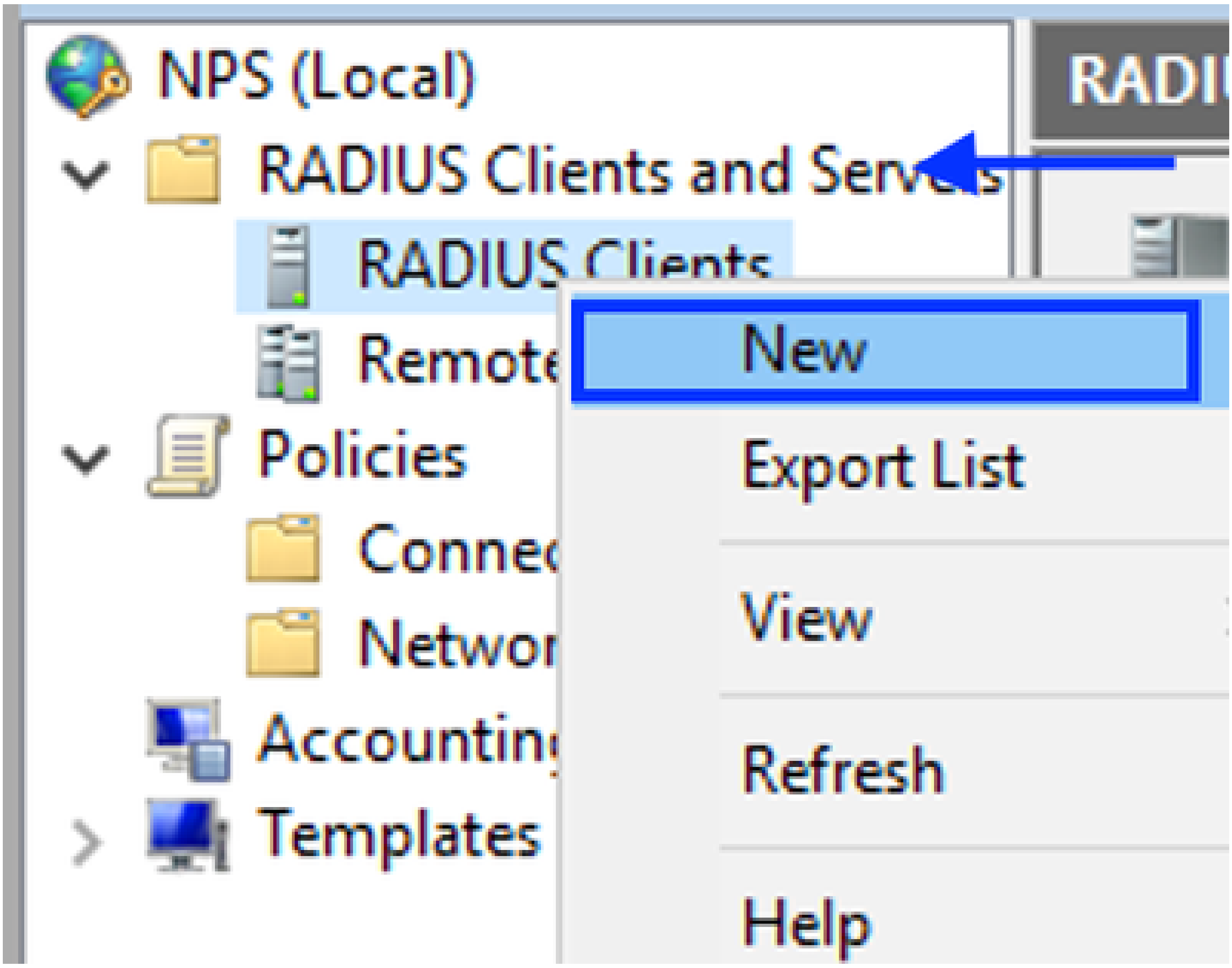
Desktop app



Windows Network Policy Service

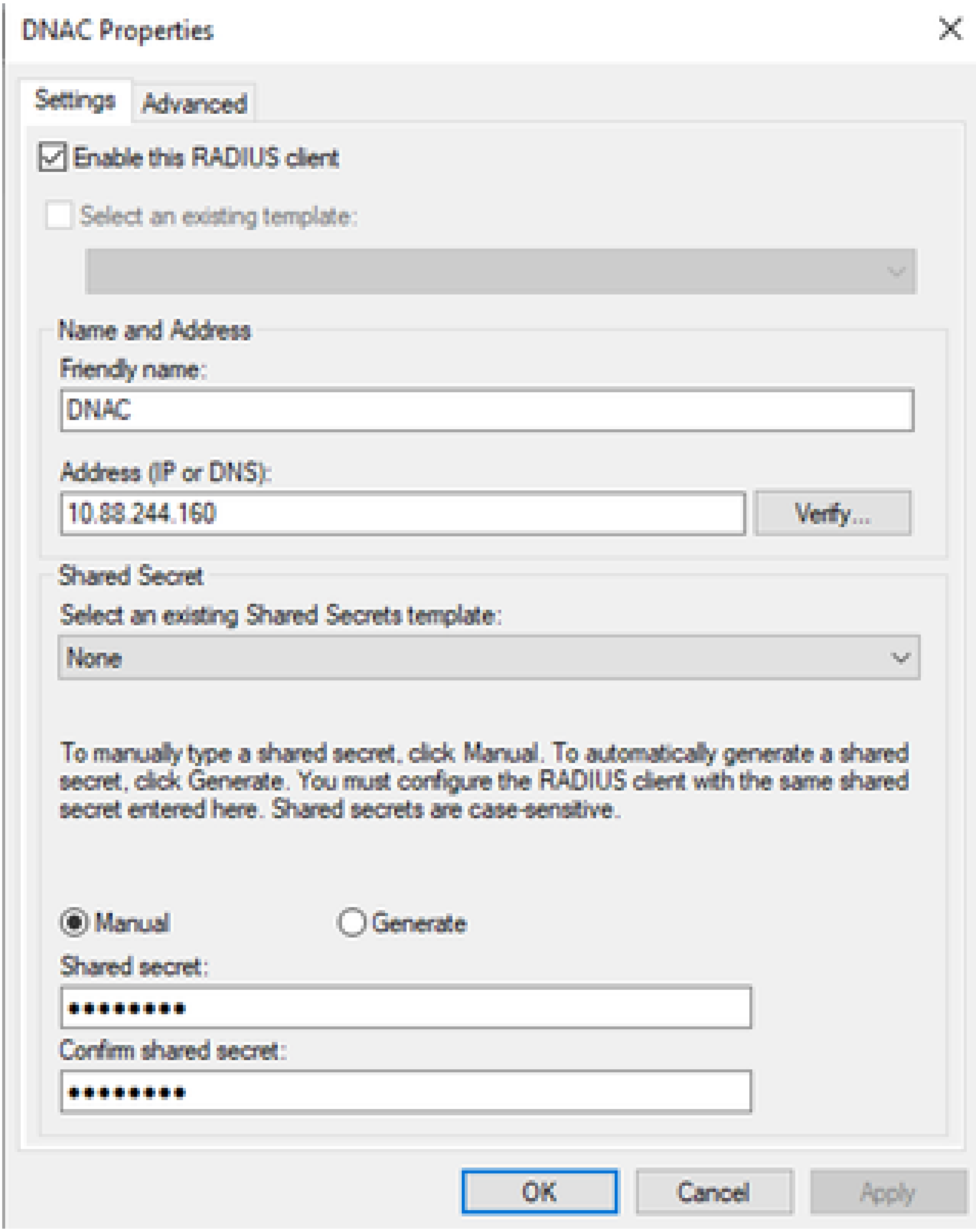
3. Click on **OK** twice.

4. Expand **RADIUS Clients and Servers**, right-click **RADIUS Clients**, and select **New**:



Add RADIUS Client

5. Enter the **Friendly name**, the Cisco DNA Center management IP address, and a shared secret (This can be used later):



DNAC Properties

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: DNAC

Address (IP or DNS): 10.88.244.160

Shared Secret

Select an existing Shared Secrets template: None

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

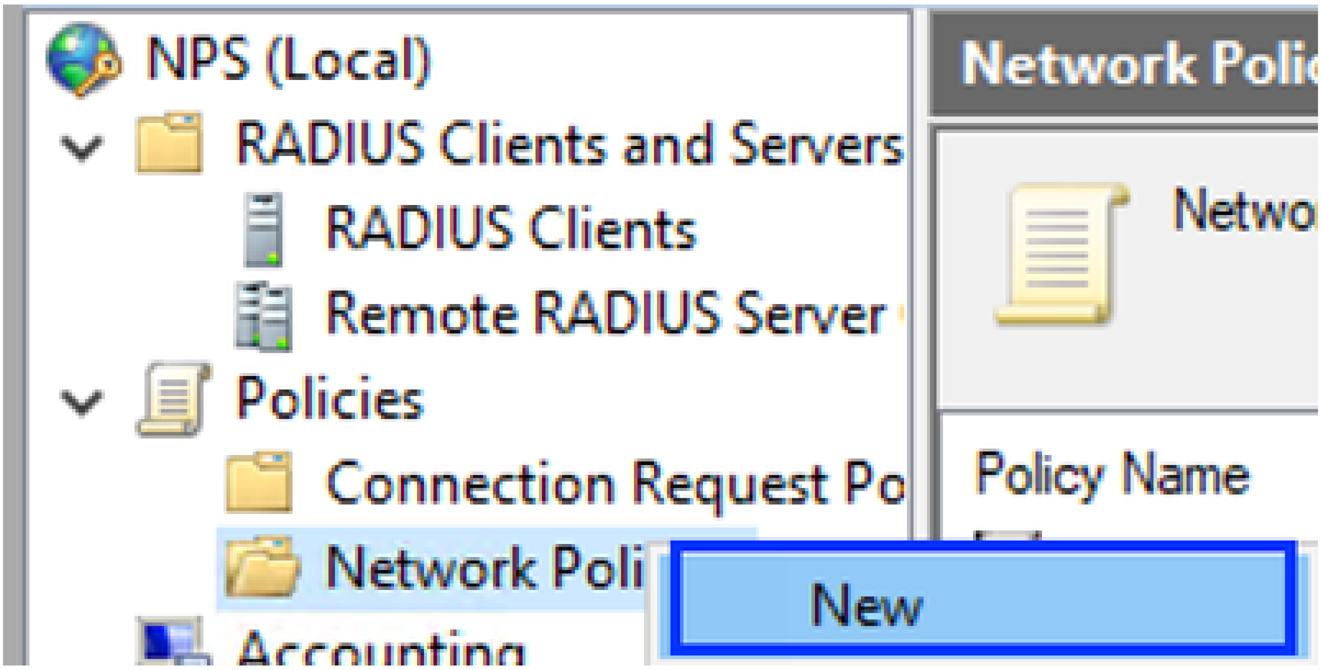
Shared secret: ••••••••

Confirm shared secret: ••••••••

Radius Client Configuration

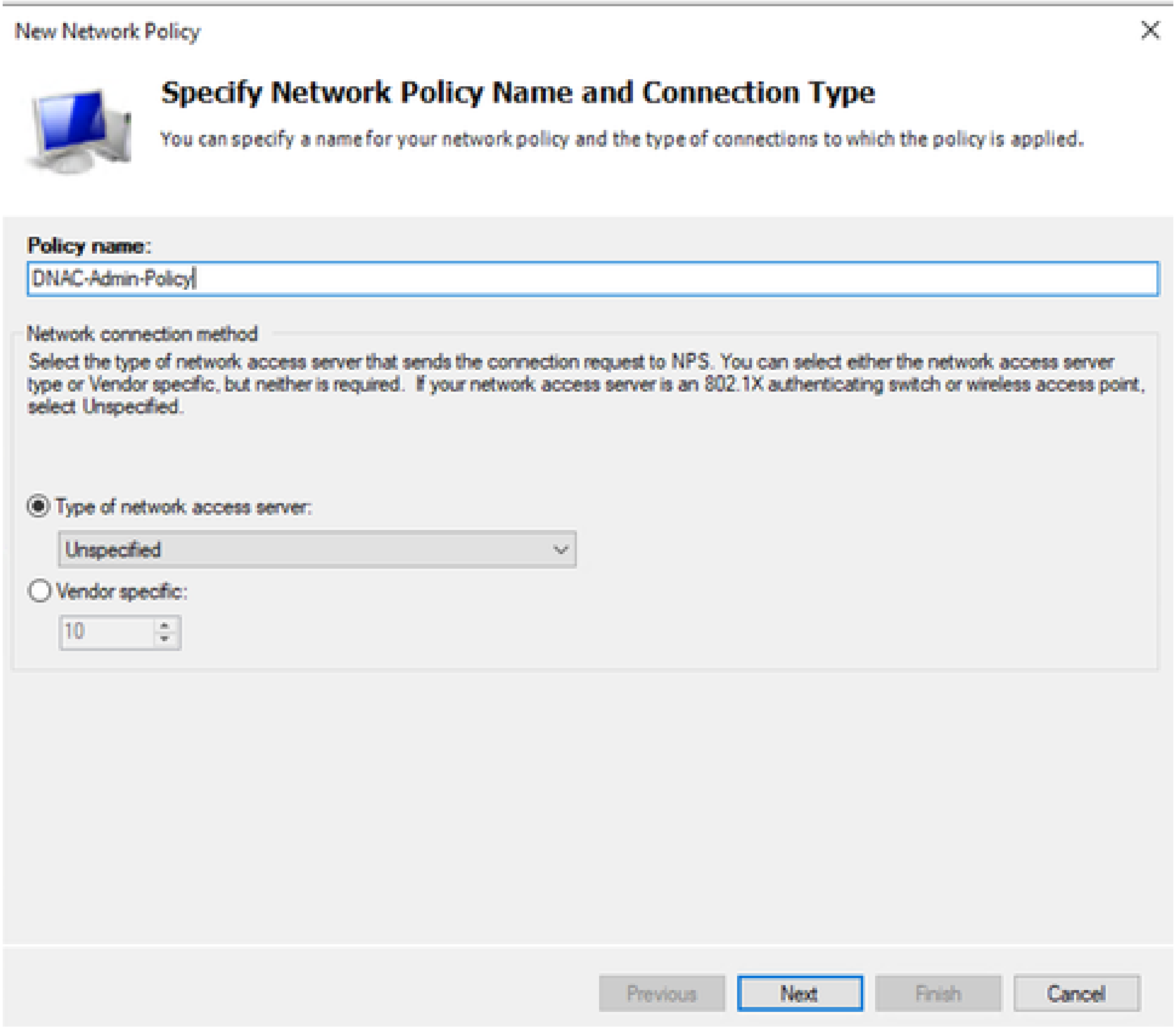
6. Click **OK** to save it.

7. Expand **Policies**, right-click **Network Policies** and select **New**:



Add New Network Policy

8. Enter a policy name for the rule and click **Next**:



New Network Policy

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

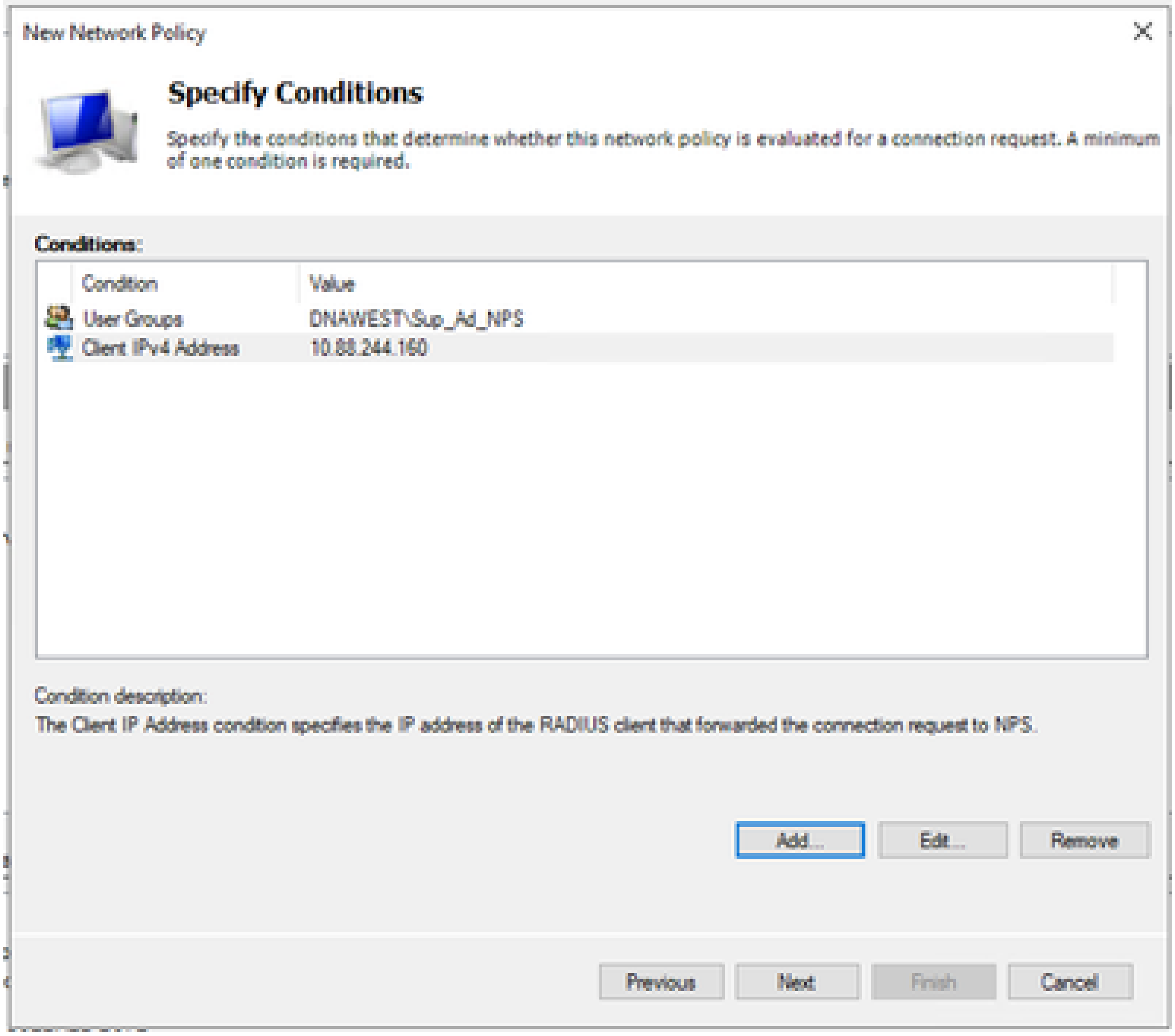
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server: Unspecified

○ Vendor specific: 10

Policy Name

9. To allow a specific domain group, add these two conditions and click **Next**:
    - **User Group –** Add your domain group that can have an Admin Role on Cisco DNA Center (For this example Sup_Ad_NPS group is used).
    - **ClientIPv4Address –** Add your Cisco DNA Center management IP address.



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

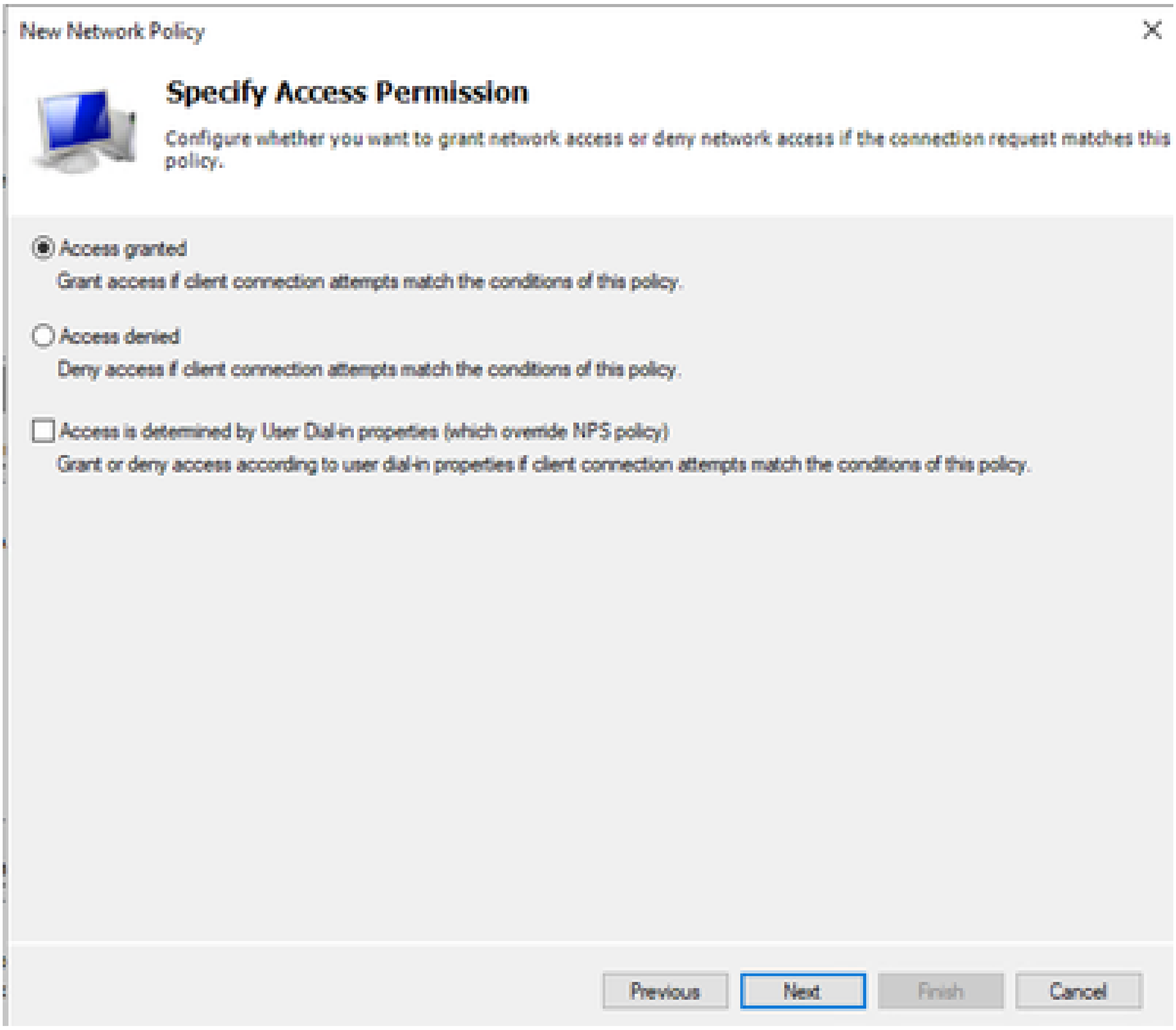
Conditions:

Condition	Value
User Groups	DNAWEST\Sup_Ad_NPS
Client IPv4 Address	10.88.244.160

Condition description:
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.

Policy Conditions

10. Select **Access Granted** and click **Next**:


New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

● Access granted

Grant access if client connection attempts match the conditions of this policy.

○ Access denied

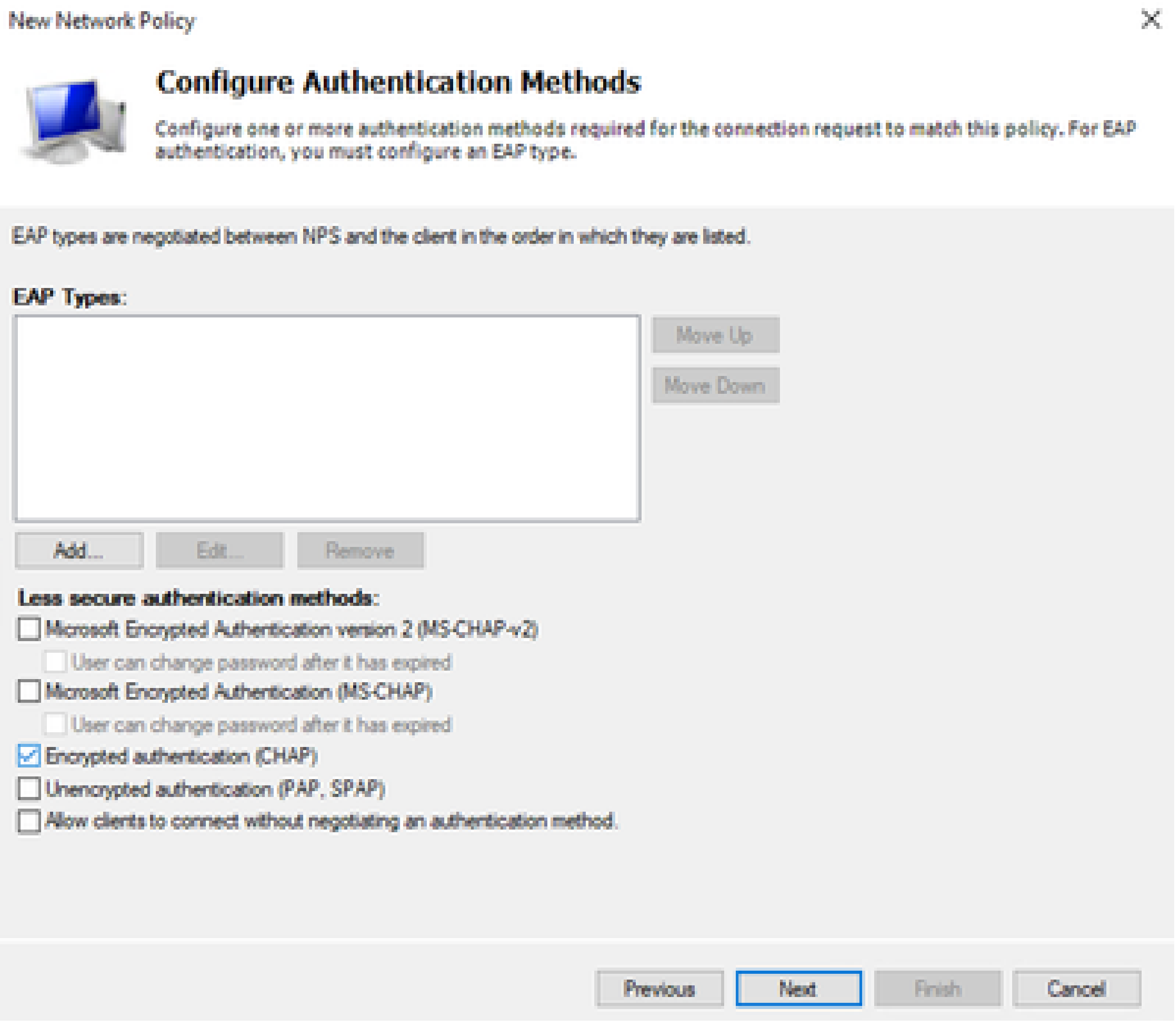
Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)

Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Use Access Granted

11. Only select **Unencrypted authentication (PAP, SPAP)**:



New Network Policy

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.

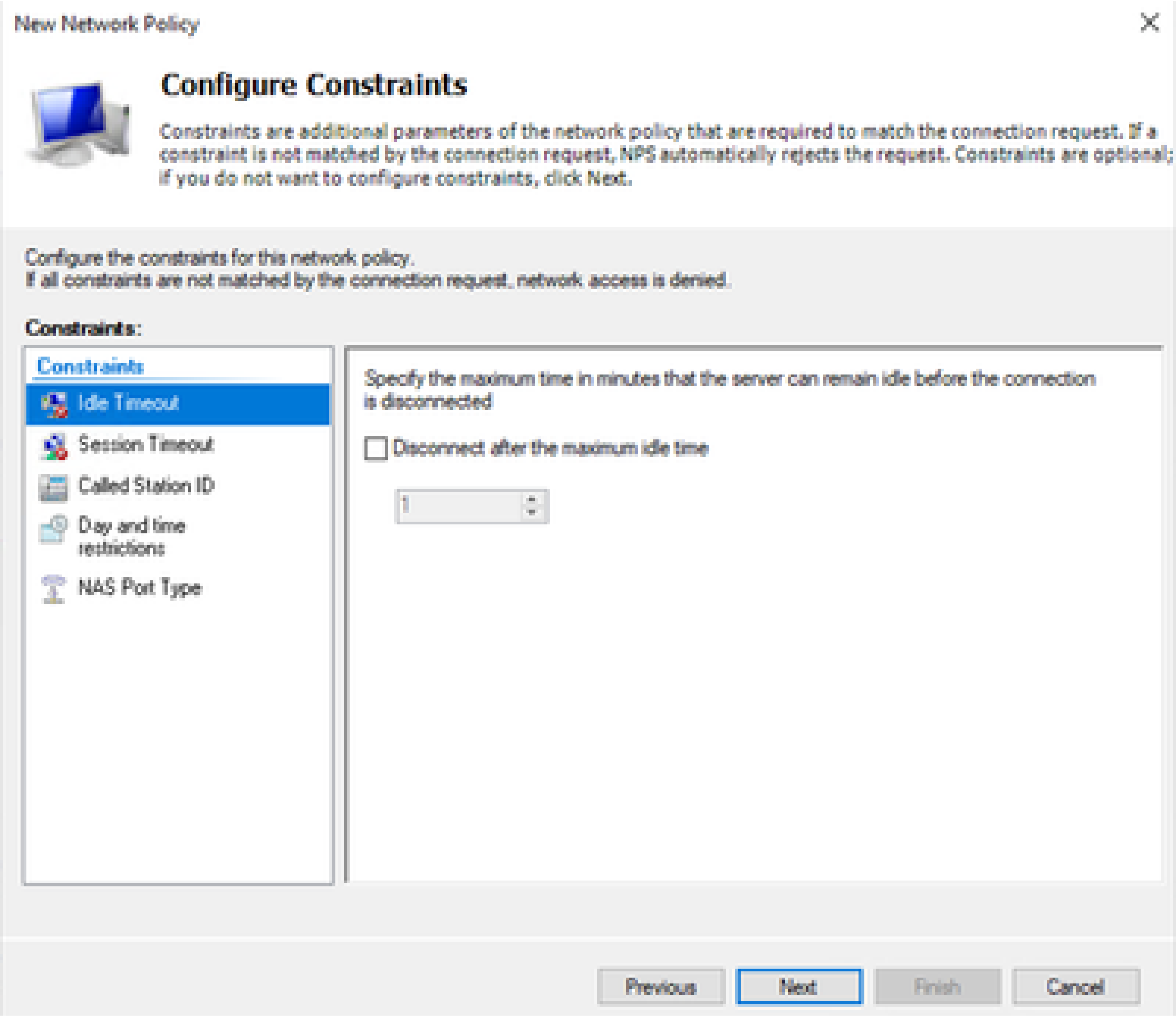
EAP Types:

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.

Select Unencrypted authentication

12. Select **Next** since default values are used:



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

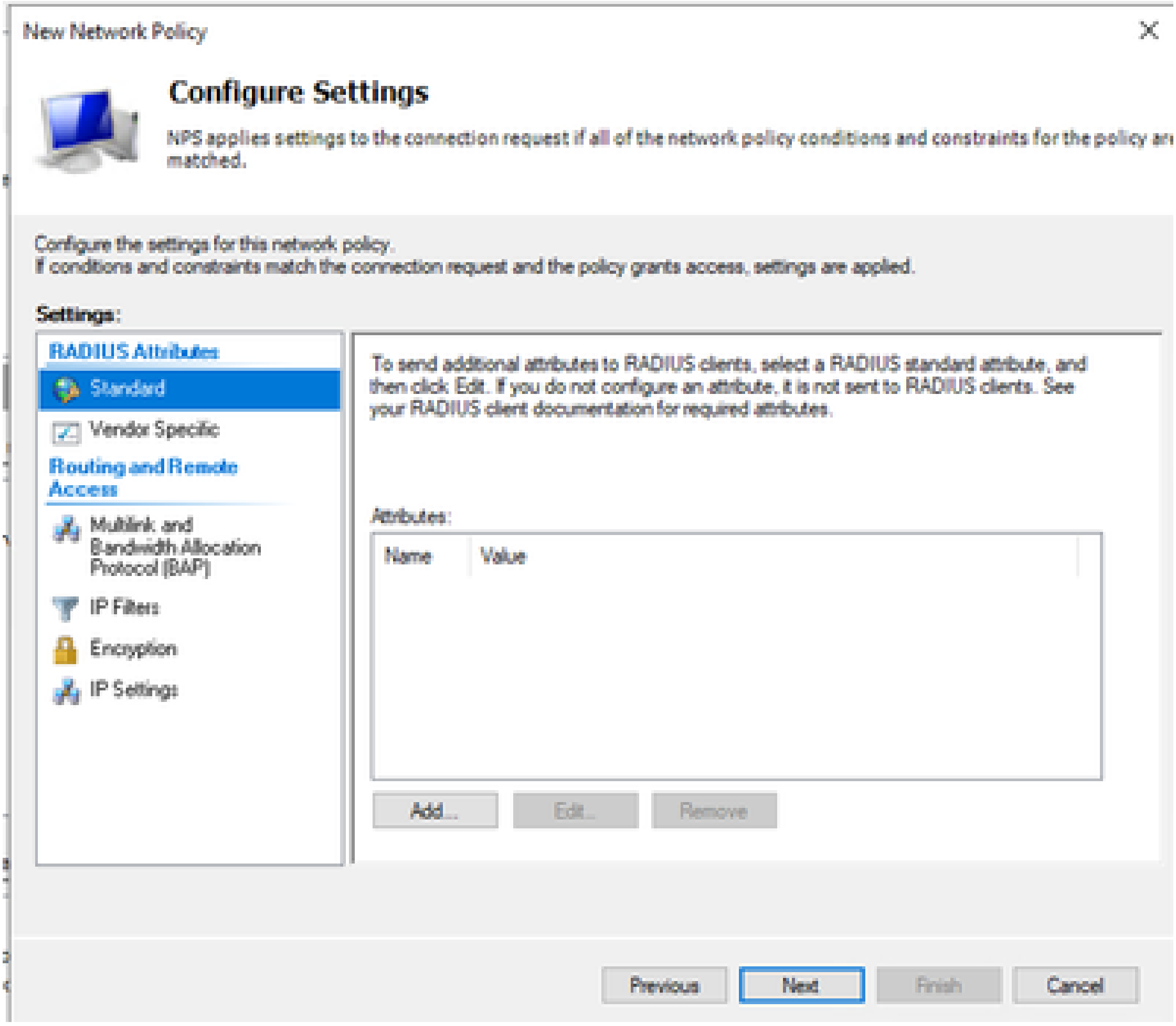
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

□ Disconnect after the maximum idle time

1

Configure Constraint Window

13. Remove Standard attributes:



New Network Policy

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

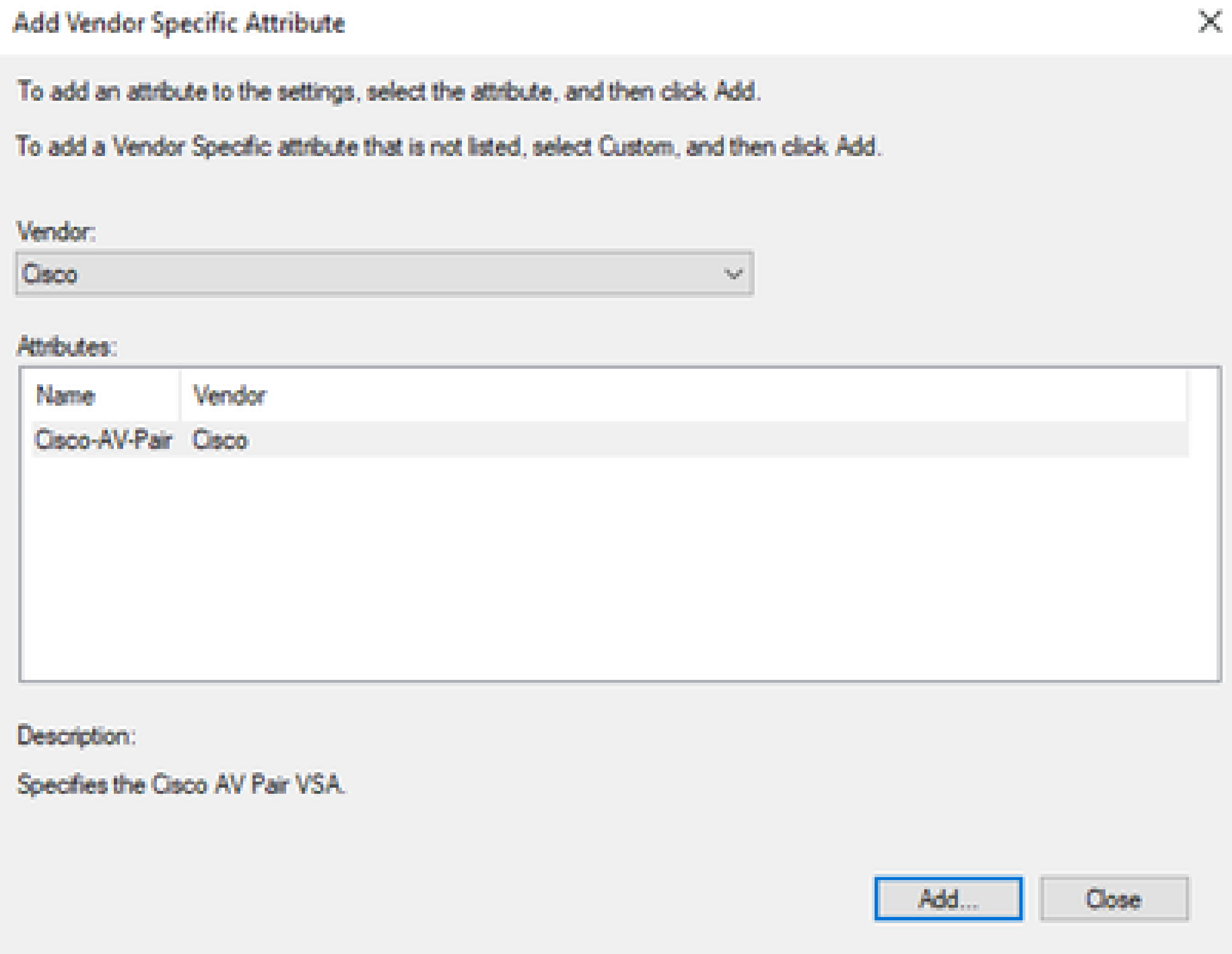
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value

Define Attributes to use

14. On RADIUS Attributes select Vendor Specific, then Click **Add**, select **Cisco** as a Vendor, and click **Add**:



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: Cisco

Attributes:

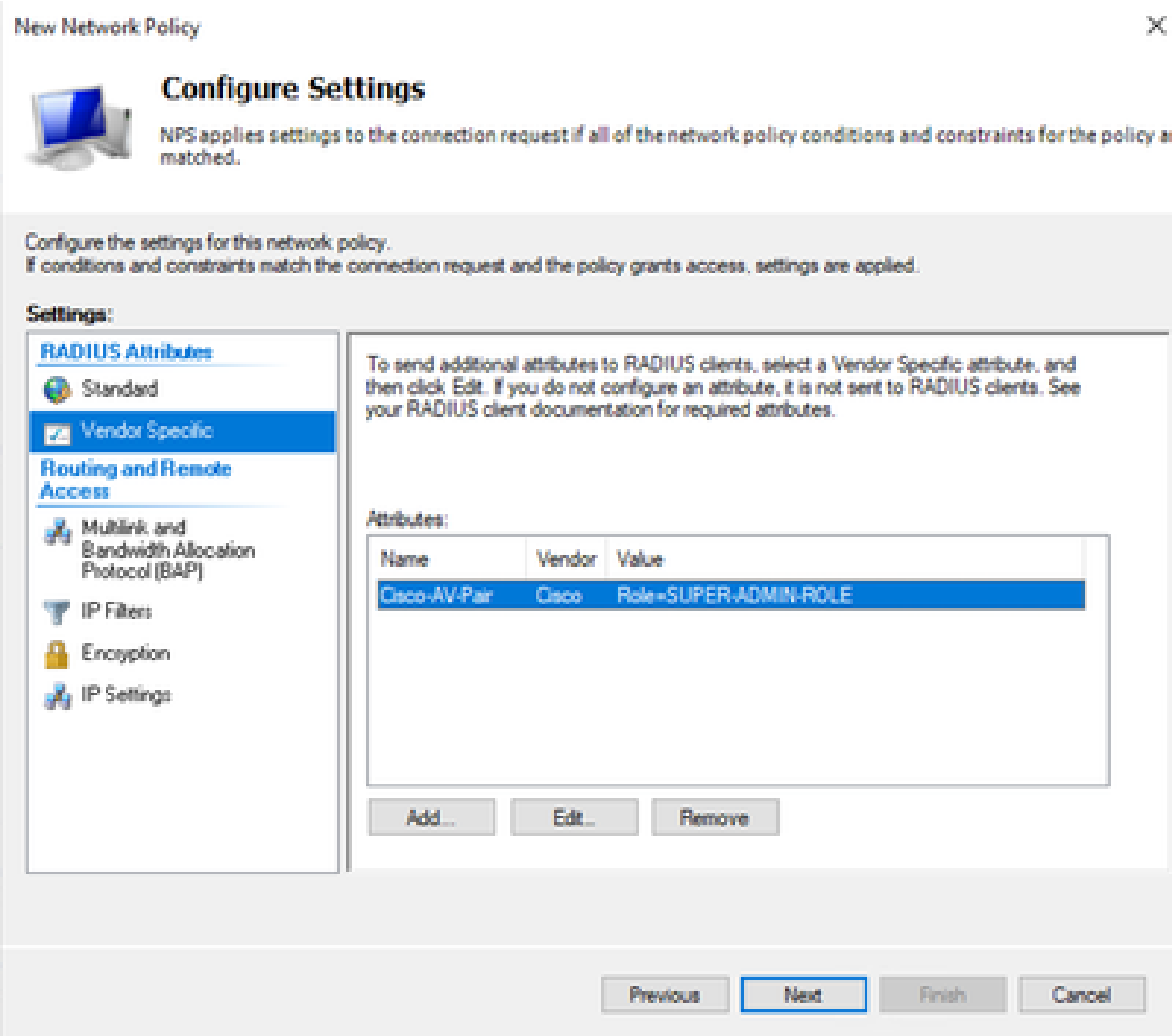
Name	Vendor
Cisco-AV-Pair	Cisco

Description:

Specifies the Cisco AV Pair VSA.

Add Cisco AV-Pair

15. Click **Add**, write **Role=SUPER-ADMIN-ROLE** and click **OK** twice:



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy a 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:

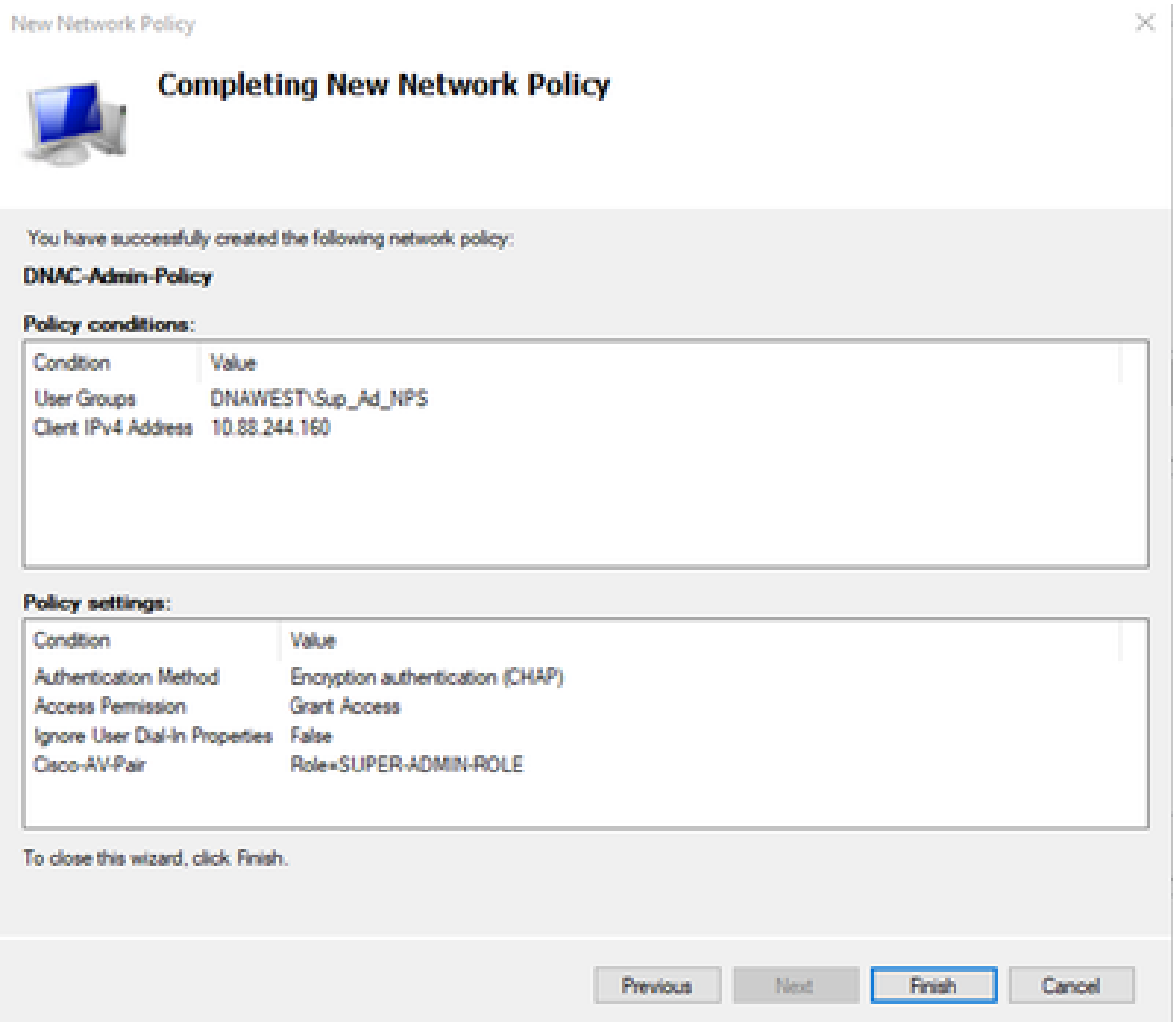
To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

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

Cisco AV-Pair Attribute added

16. Select **Close**, then select **Next**.
17. Review your policy settings and Select **Finish** to save it.



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.

Policy Summary

Observer Role Policy.

1. Click in the **Windows Start** menu and search for **NPS**. Then select **Network Policy Server**.
2. From the navigation panel in the left side, perform a Right-click in the **NPS (Local)** option and select **Register server in Active Directory**.
3. Click on **OK** twice.
4. Expand **RADIUS Clients and Servers**, right-click **RADIUS Clients**, and select **New**.
5. Enter a **Friendly name**, the Cisco DNA Center management IP address, and a shared secret (This can be used later).
6. Click **OK** to save it.
7. Expand **Policies**, right-click **Network Policies**, and select **New**.
8. Enter a policy name for the rule and click **Next**.
9. To allow a specific domain group, you need to add these two conditions and select **Next**.
   - **User Group –** Add your domain group in order to assign an Observer Role on Cisco DNA

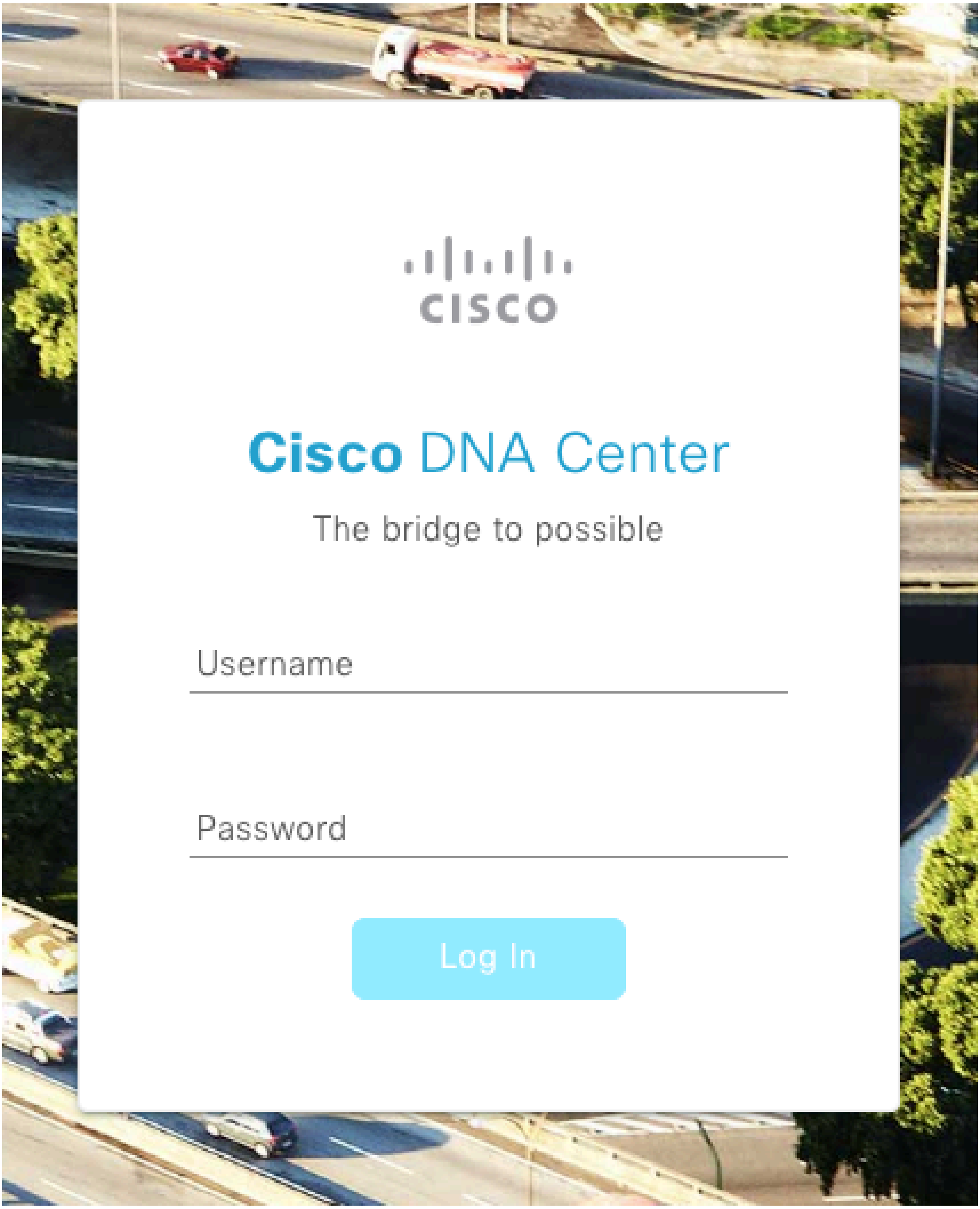
Center (For this example Observer_NPS group is used).

- **ClientIPv4Address –** Add your Cisco DNA Center management IP.

10. Select **Access Granted** and then select **Next**.
11. Only select **Unencrypted authentication (PAP, SPAP)**.
12. Select **Next** since default values are used.
13. Remove **Standard** attributes.
14. On RADIUS Attributes select **Vendor Specific**, then Click Add, select **Cisco** as a Vendor, and click **Add**.
15. Select **Add**, write **ROLE=OBSERVER-ROLE,** and **OK** twice.
16. Select **Close**, then **Next**.
17. Review your policy settings and select **Finish** to save it.

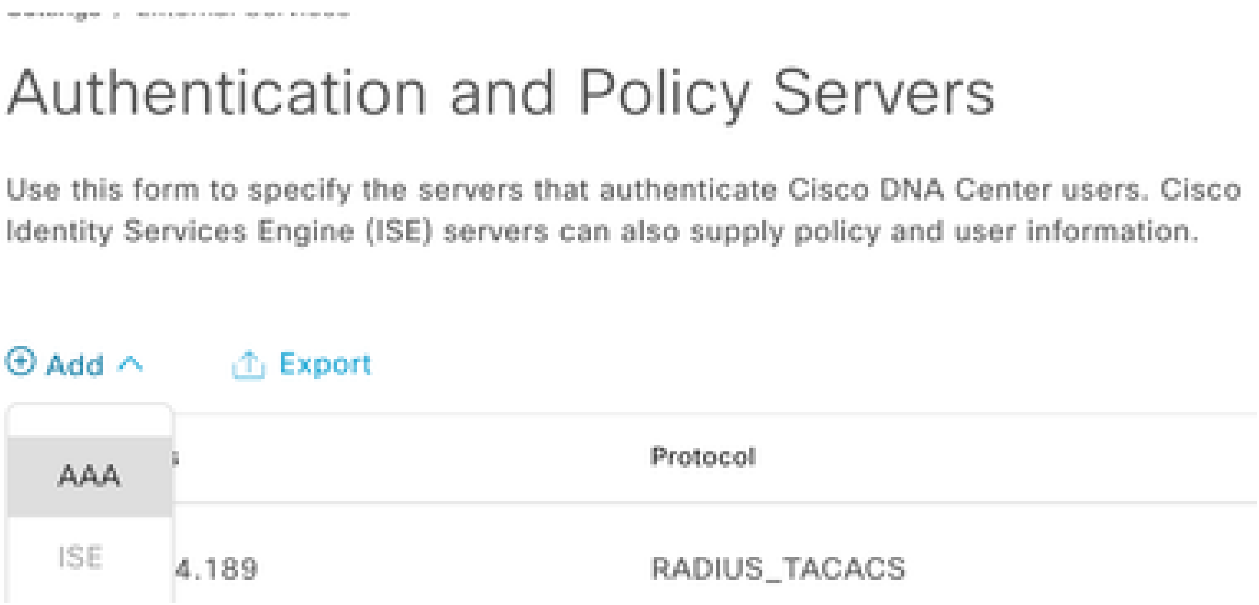
Enable External Authentication

1. Open the Cisco DNA Center Graphical User Interface (GUI) in a web browser and Log in using an admin privileged account:



Cisco DNA Center Login Page

2. Navigate to **Menu** > **System** > **Setting** > **Authentication and Policy Servers** and select **Add** > **AAA**:

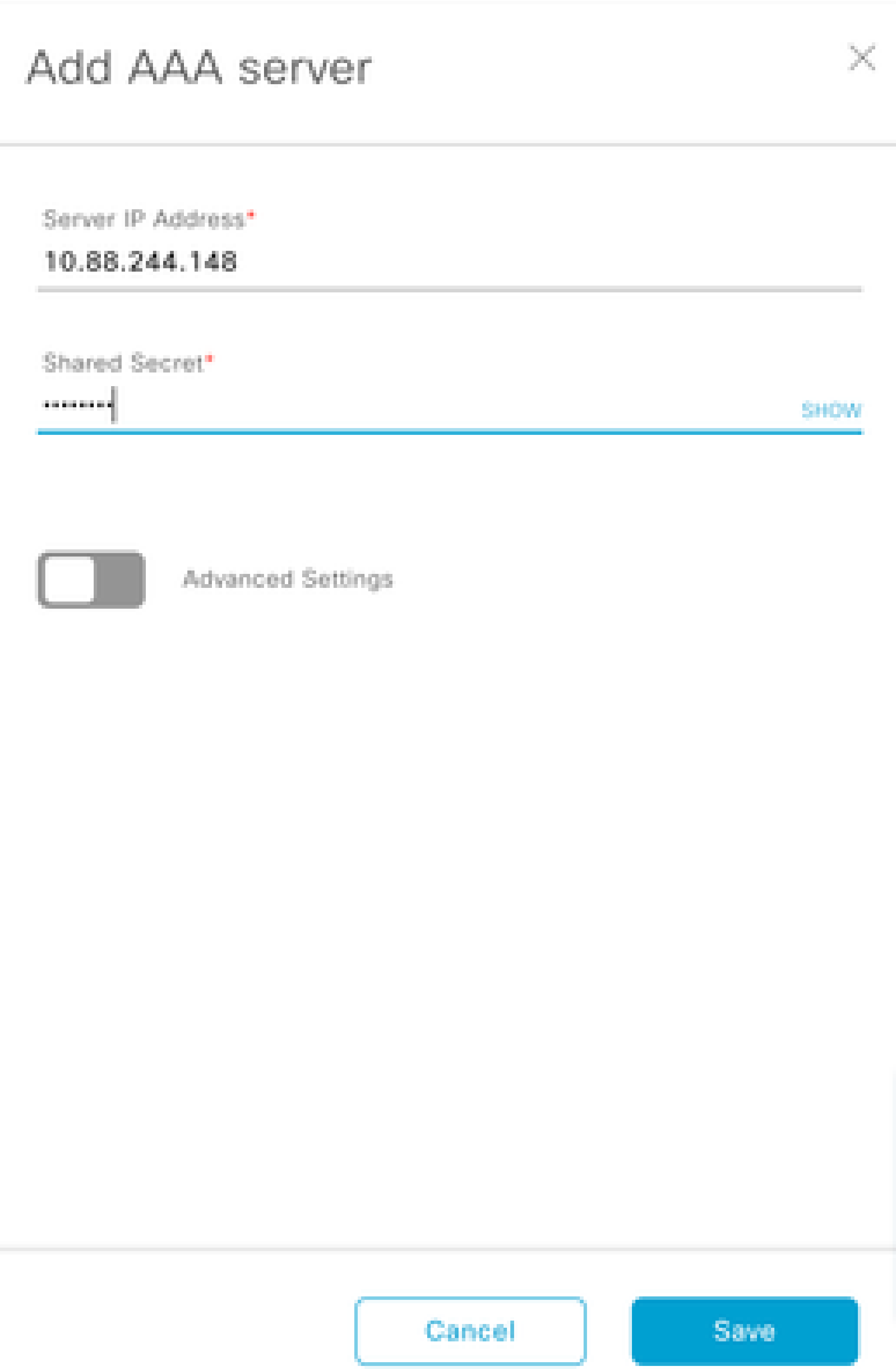


Authentication and Policy Servers

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 Windows Server

3. Type your Windows Server IP address and the Shared Secret used in the previous steps and Click **Save**:



Add AAA server

Server IP Address*

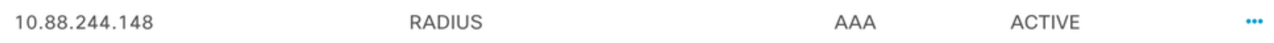
10.88.244.148

Shared Secret*

••••••••

Windows Server Values

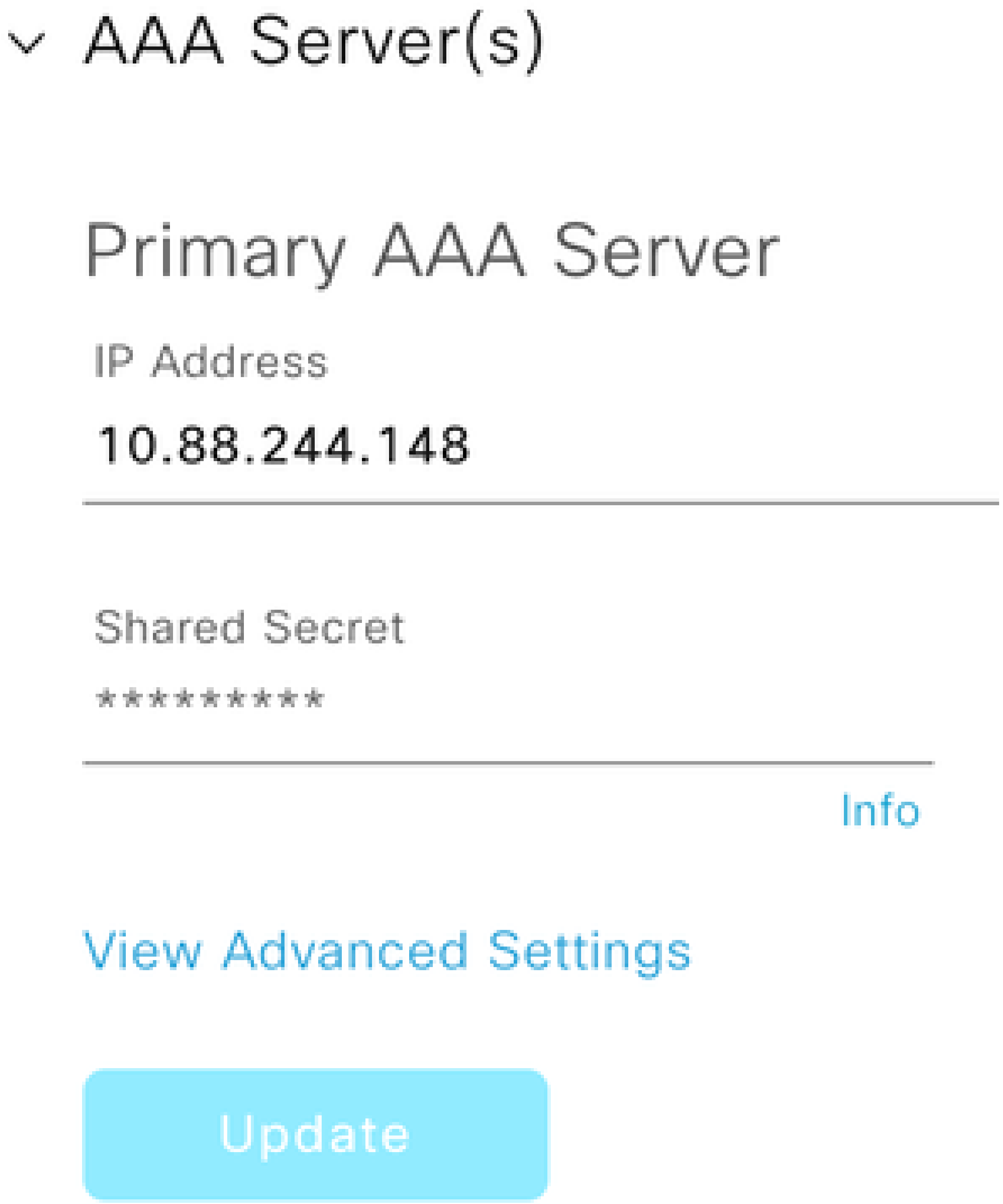
4. Validate that your Windows Server status is **Active**:



10.88.244.148	RADIUS	AAA	ACTIVE	•••

Windows Server Summary

5. Navigate to **Menu** > **System** > **Users & Roles** > **External Authentication** and select your AAA server:

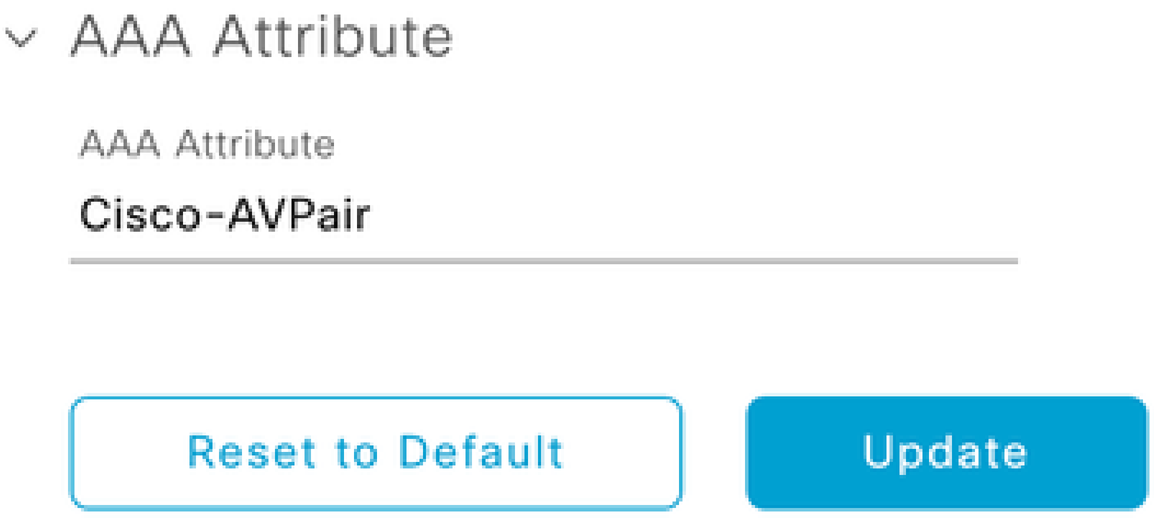


IP Address
10.88.244.148

Shared Secret
****

Windows Server as AAA Server

6. Type **Cisco-AVPair** as the AAA attribute and click **Update**:



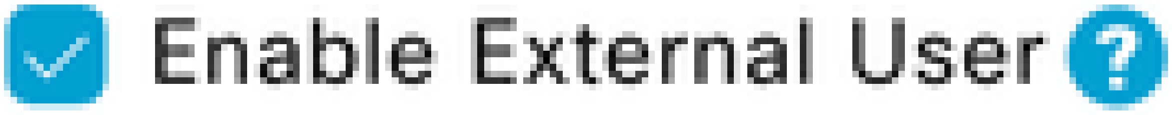
⌄ AAA Attribute

AAA Attribute

Cisco-AVPair

AV-Pair on External User

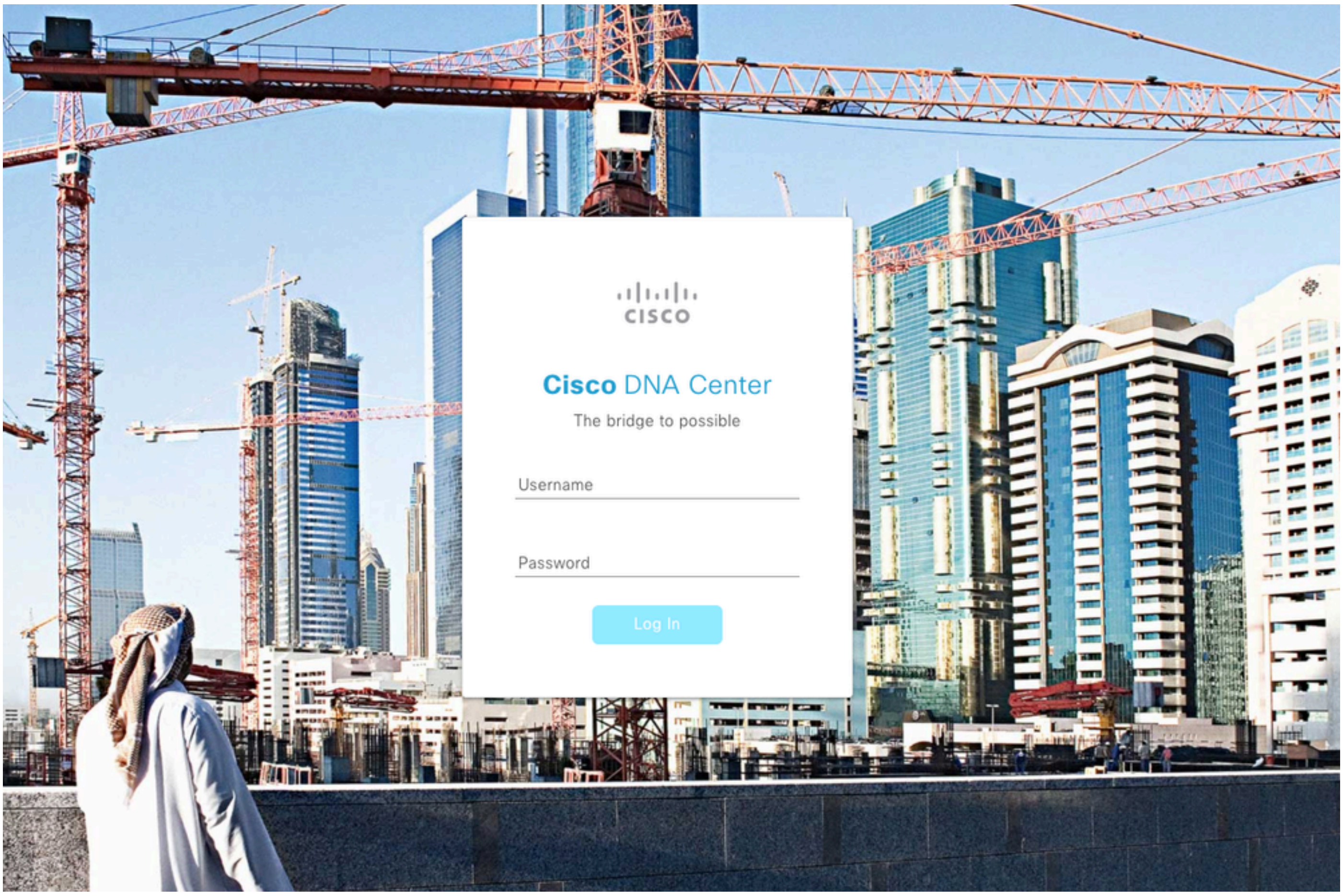
7. Click in the check-box **Enable External User** to enable External Authentication:



☑ Enable External User

Verify

You can open the Cisco DNA Center Graphical User Interface (GUI) in a web browser and Log in with an external user configured in the Windows Server to validate that you can Log in successfully using External Authentication.



Cisco DNA Center Login Page