使用Windows Server在Catalyst Center上配置外部身份验证

目录

简介

本文档介绍如何在Cisco DNA Center中使用Windows Server中的网络策略服务器(NPS)作为RADIUS来配置外部身份验证。

先决条件

要求

基本知识：

- Cisco DNA Center用户和角色
- Windows Server网络策略服务器、RADIUS和Active Directory

使用的组件

- 思科DNA Center 2.3.5.x
- Microsoft Windows Server Version 2019充当域控制器、DNS服务器、NPS和Active Directory

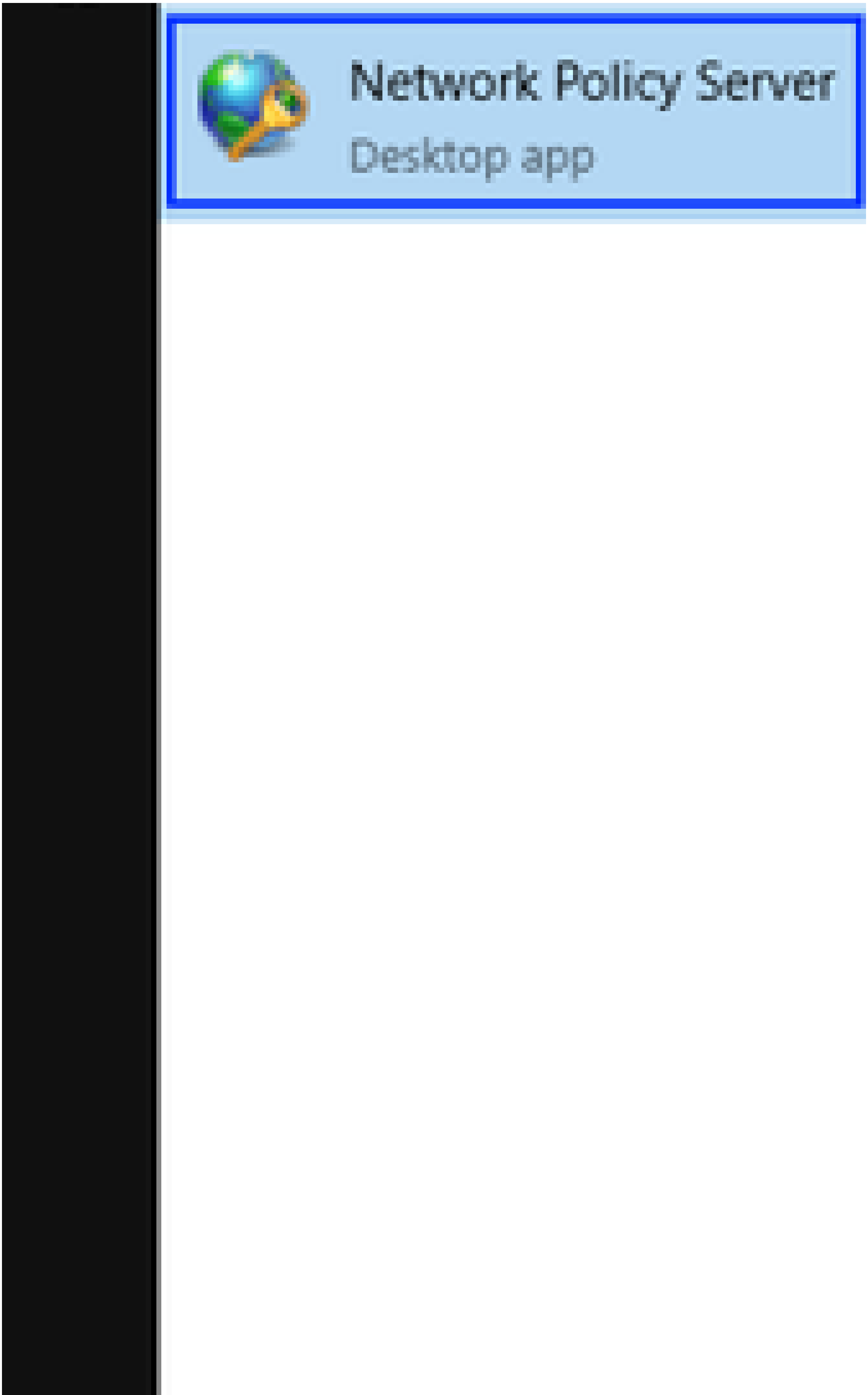
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

注意：思科技术支持中心(TAC)不为Microsoft Windows Server提供技术支持。 如果Microsoft Windows Server配置遇到问题，请与Microsoft支持联系以获取技术支持。

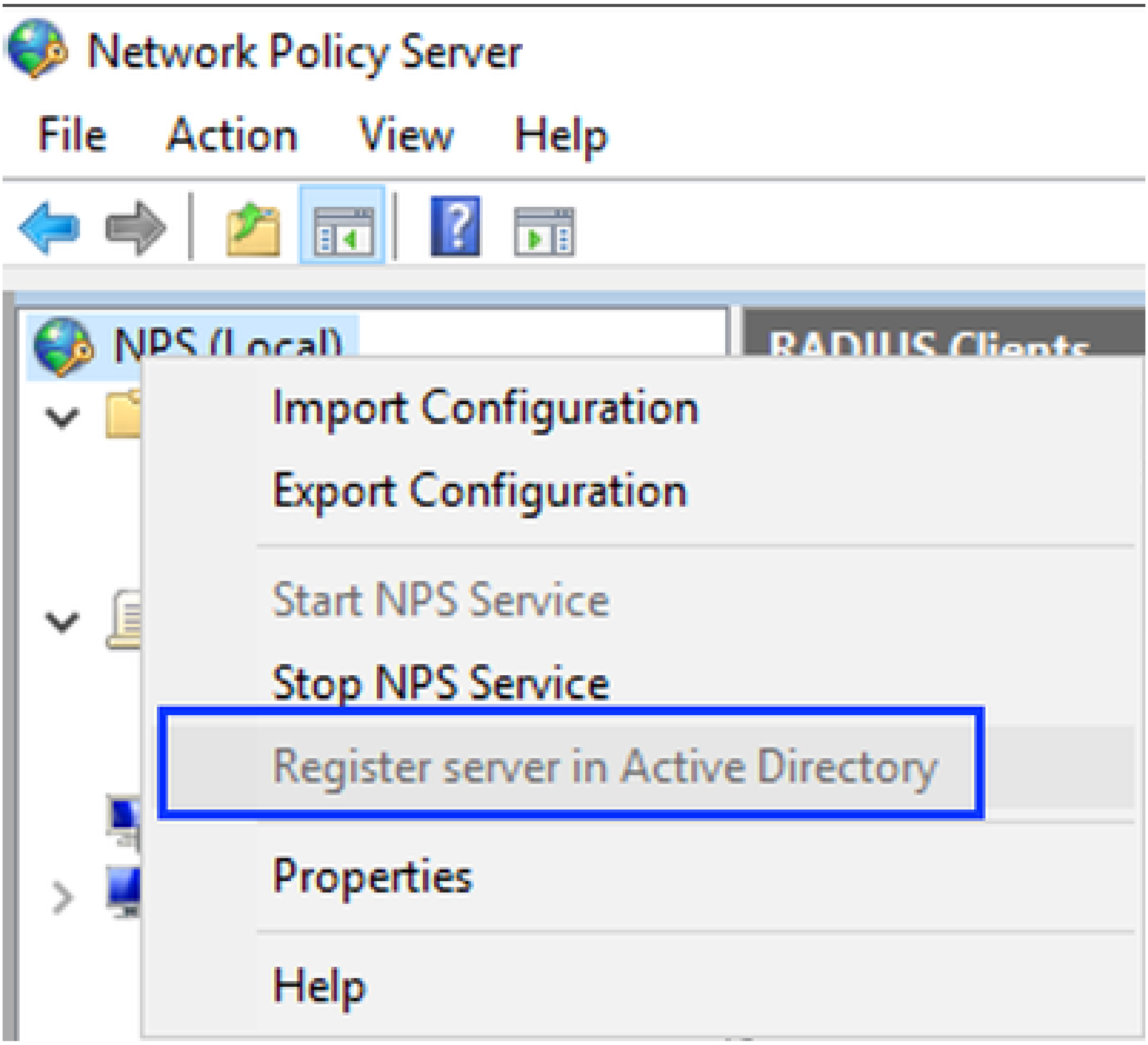
配置

管理员角色策略

1. 单击Windows Start菜单并搜索NPS。然后选择Network Policy Server：



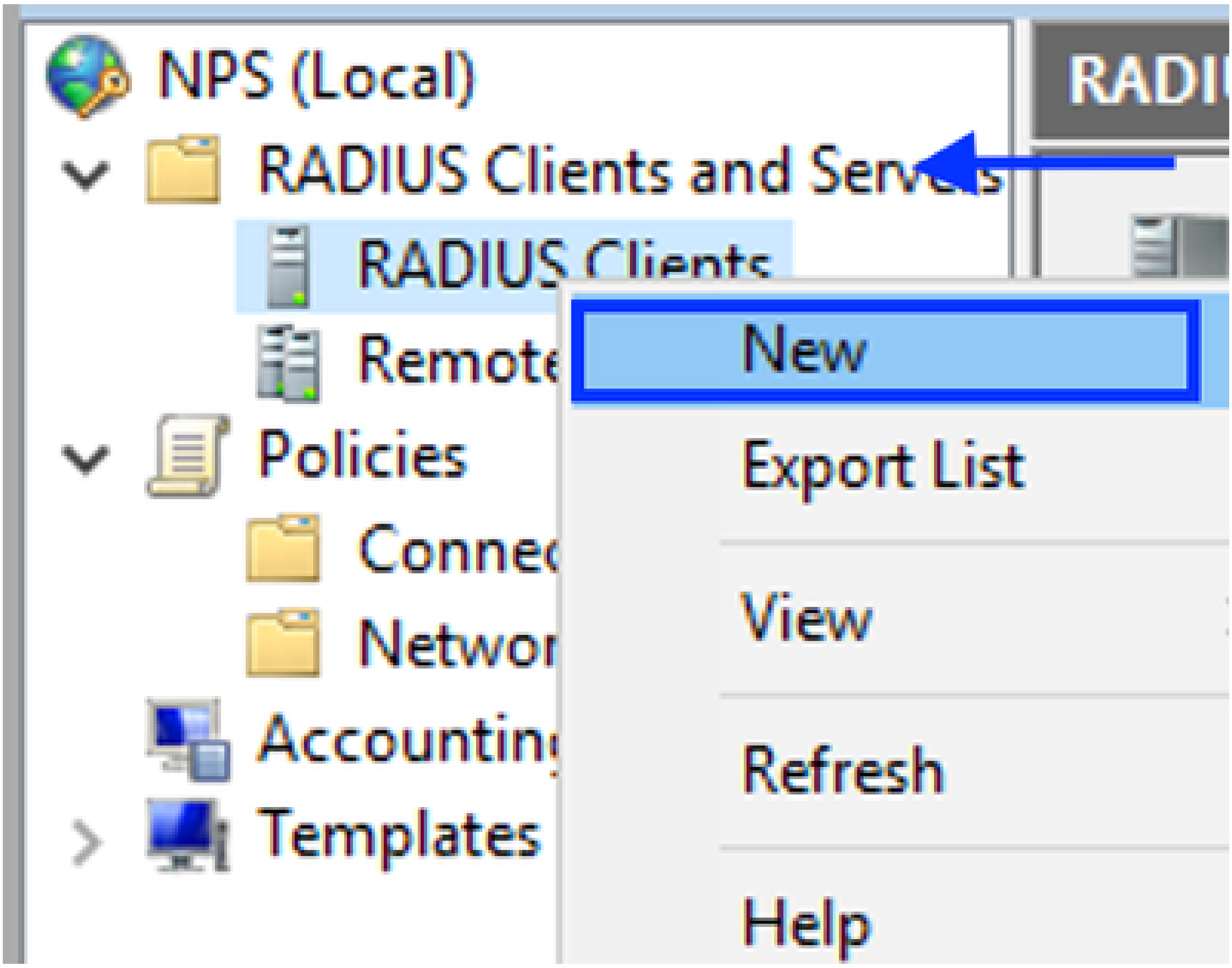
Network Policy Server
Desktop app



Windows网络策略服务

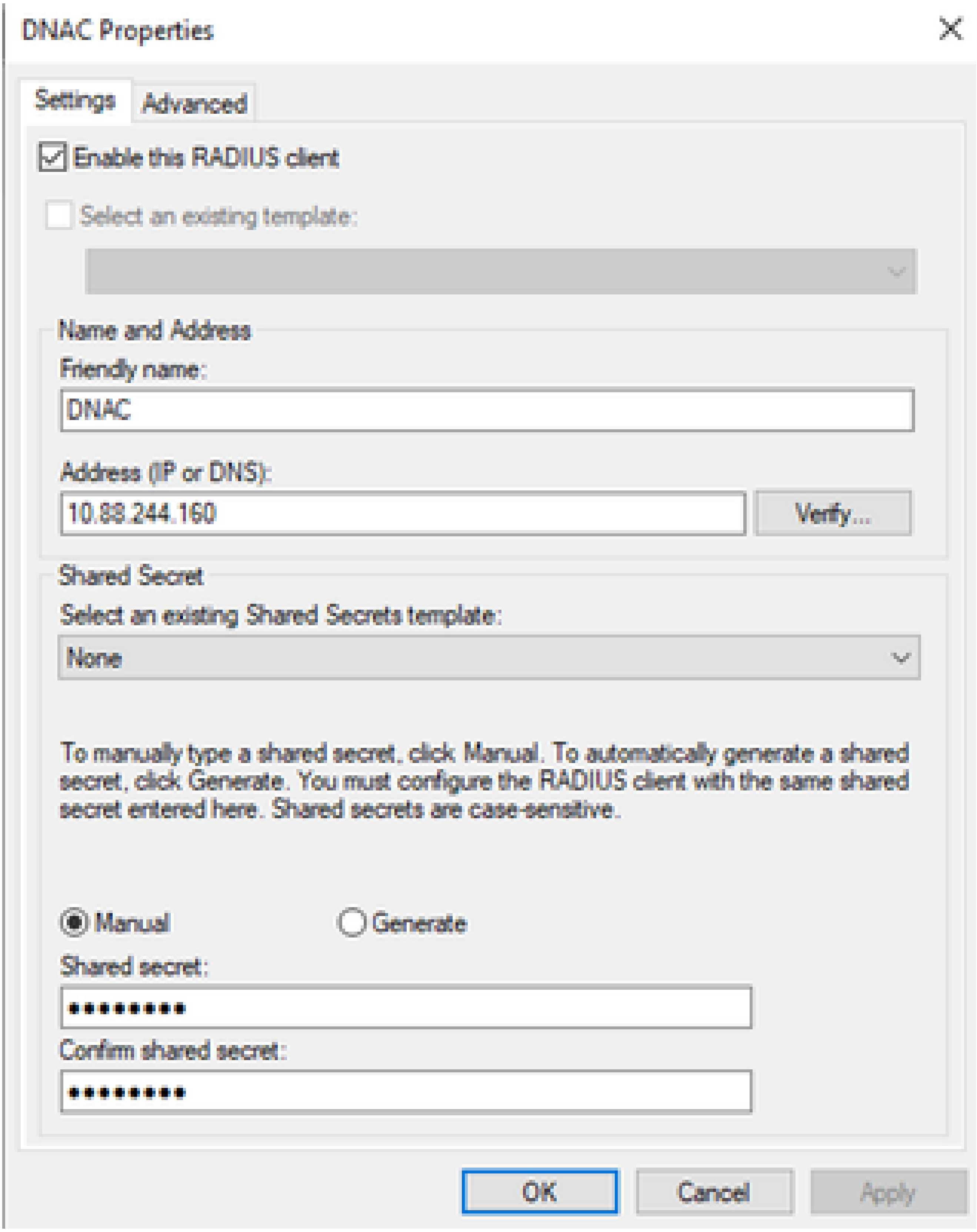
3. 单击OK两次。

4. 展开RADIUS Clients and Servers，右键单击RADIUS Clients，然后选择New：



添加RADIUS客户端

5. 输入友好名称、Cisco DNA中心管理IP地址和共享密钥（这一点可在以后使用）：



DNAC Properties

Settings | Advanced

☑ 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

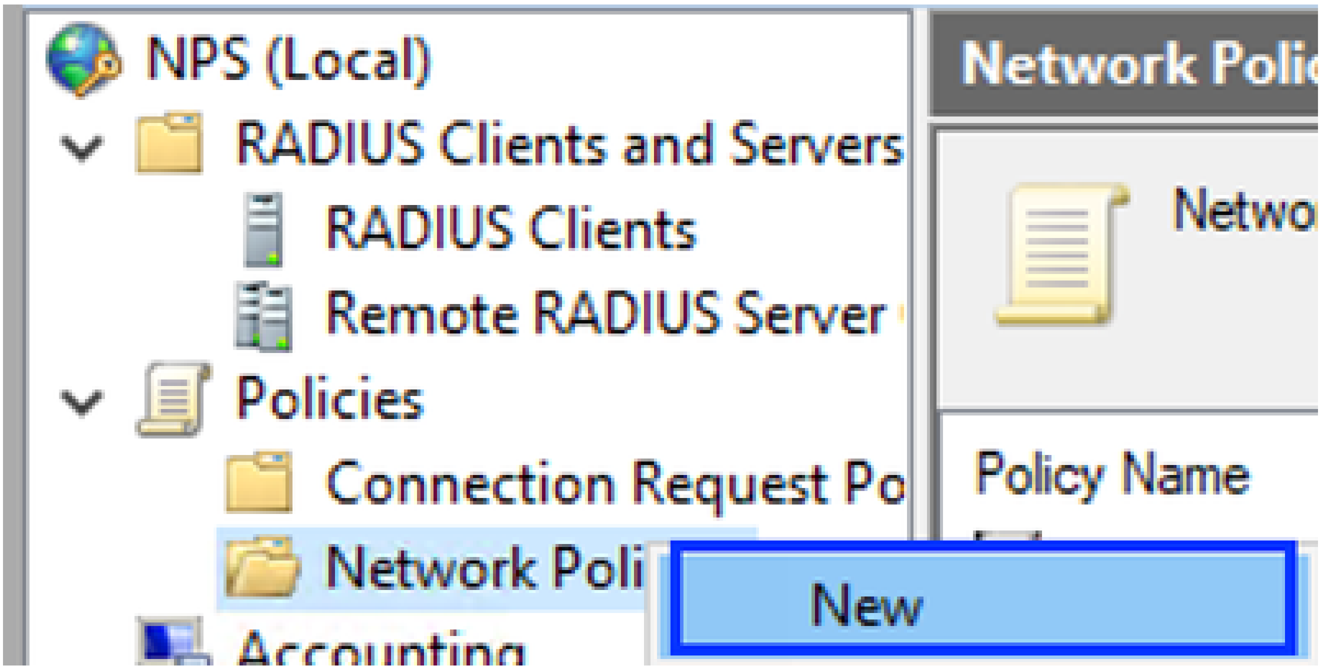
Shared secret: ●●●●●●●●●

Confirm shared secret: ●●●●●●●●●

Radius客户端配置

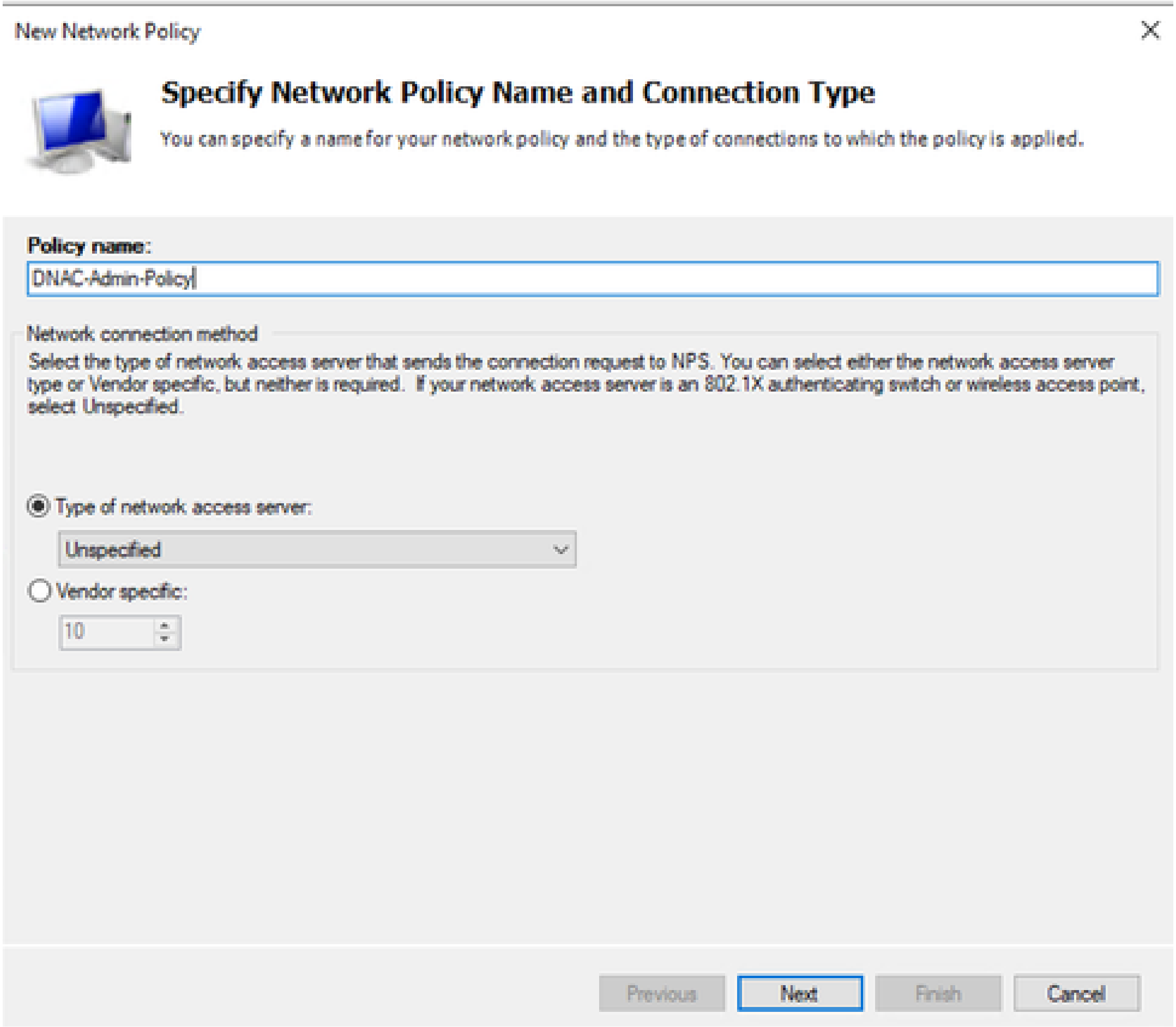
6. 单击OK保存它。

7. 展开Policies，右键单击Network Policies并选择New：



添加新网络策略

8. 为规则输入策略名称，然后点击下一步：



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:

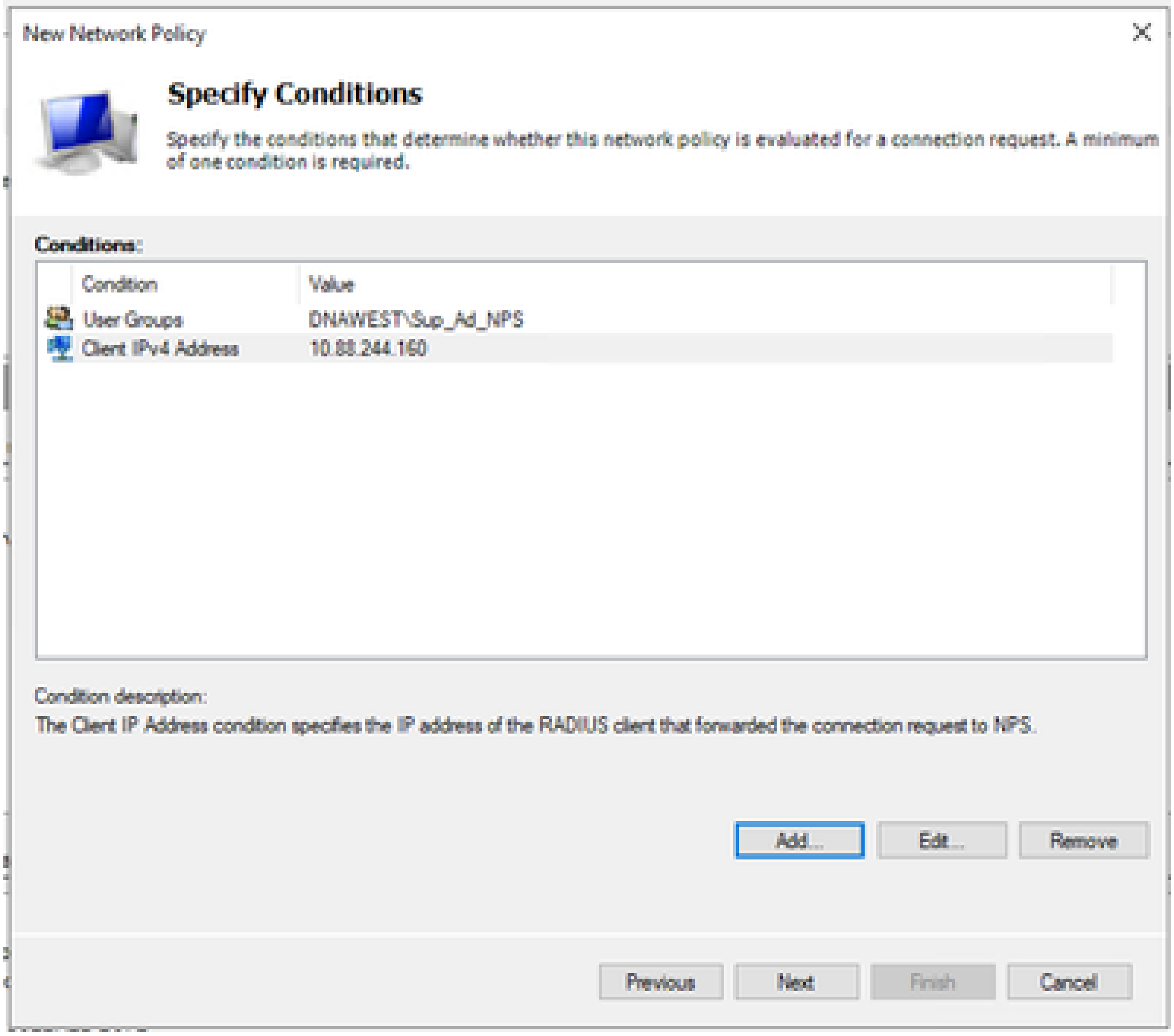
Unspecified

○ Vendor specific:

10

策略名称

9. 要允许特定域组，请添加以下两个条件并单击Next：
   - User Group -添加您的在Cisco DNA Center上可以具有管理员角色的域组（例如，使用Sup_Ad_NPS组）。
   - ClientIPv4Address -添加您的Cisco DNA Center管理IP地址。



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.

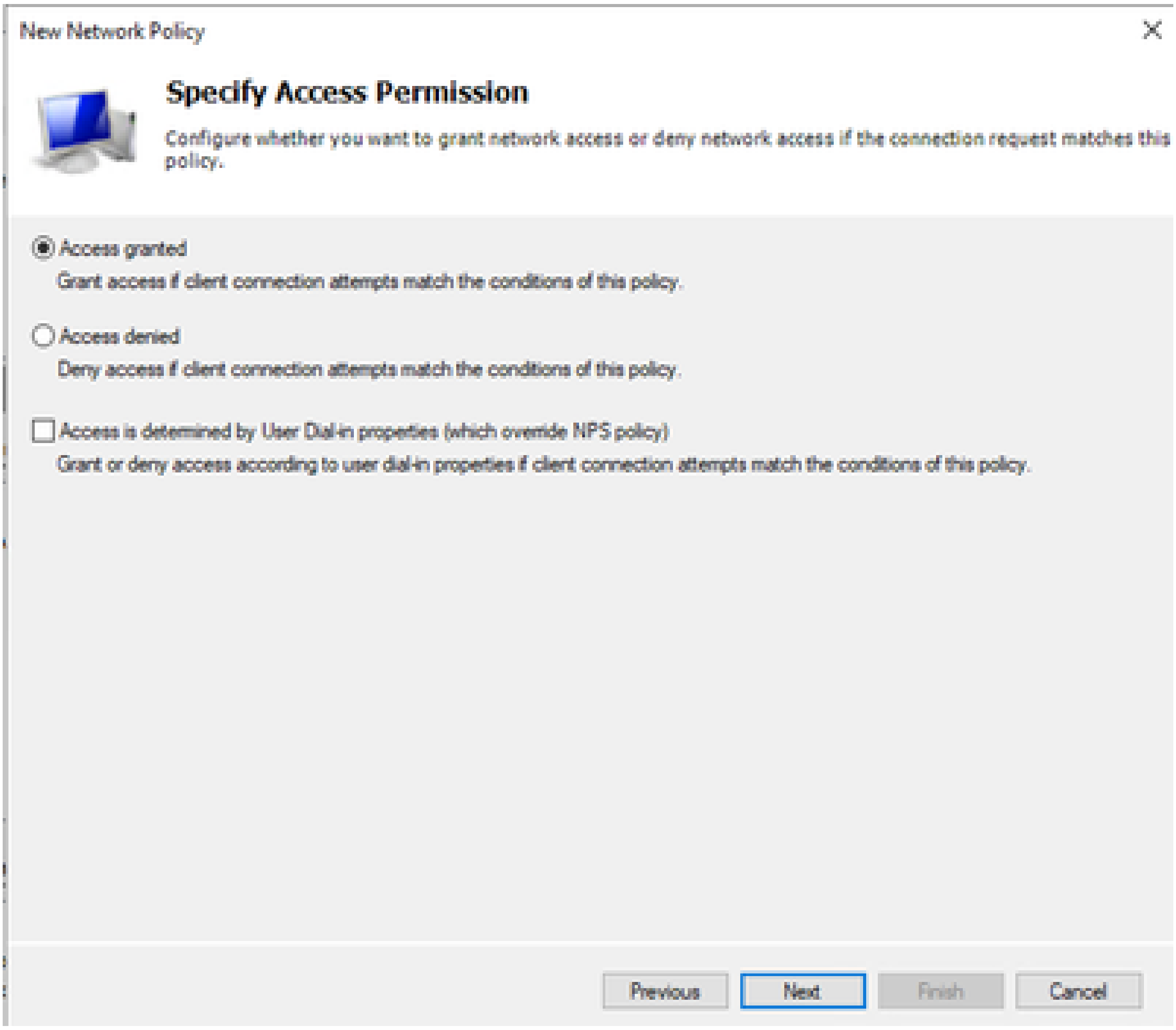
Conditions:

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.

策略条件

10. 选择Access Granted并单击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

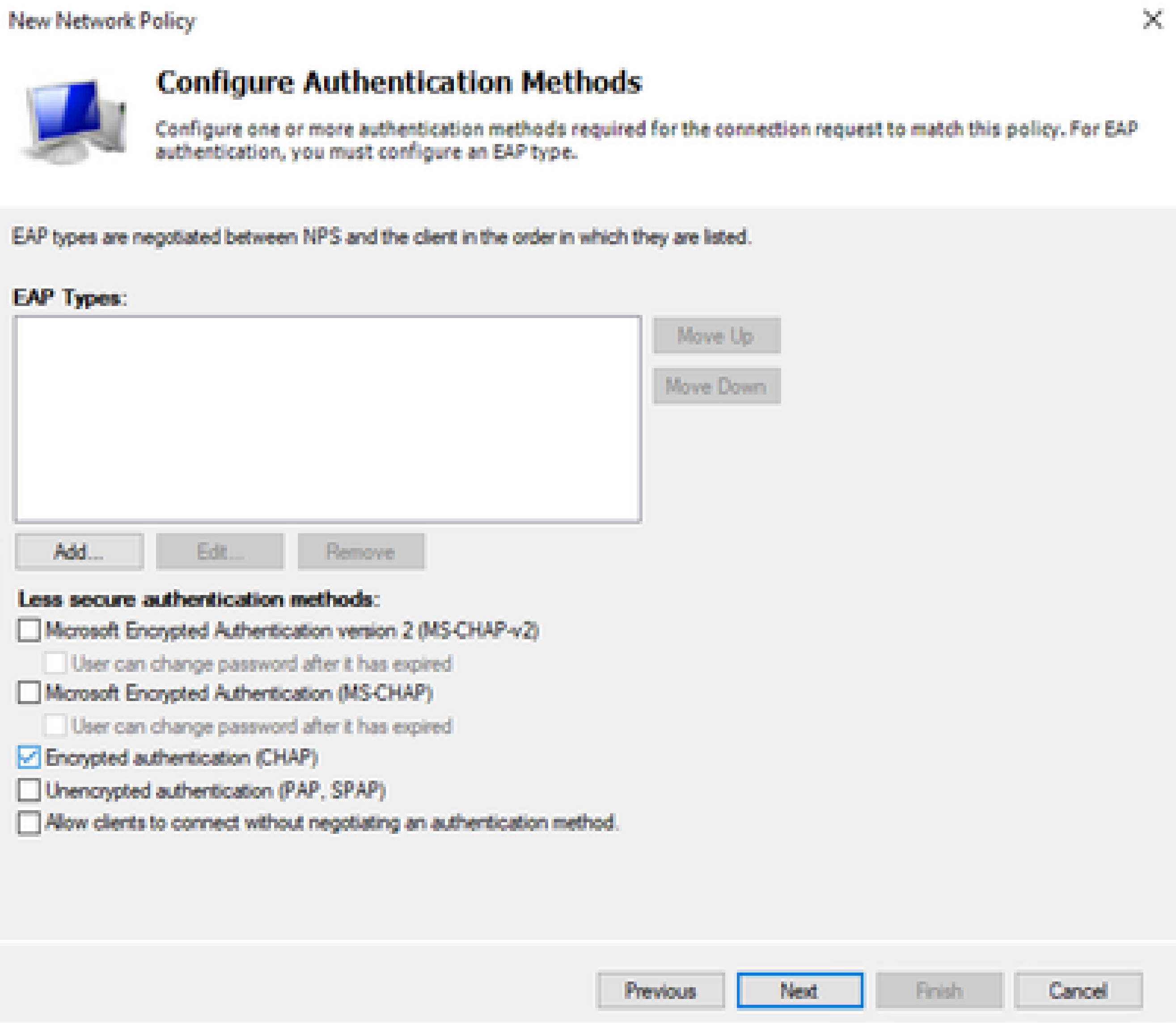
Deny access if client connection attempts match the conditions of this policy.

□ 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.

使用授予的访问权限

11. 仅选择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

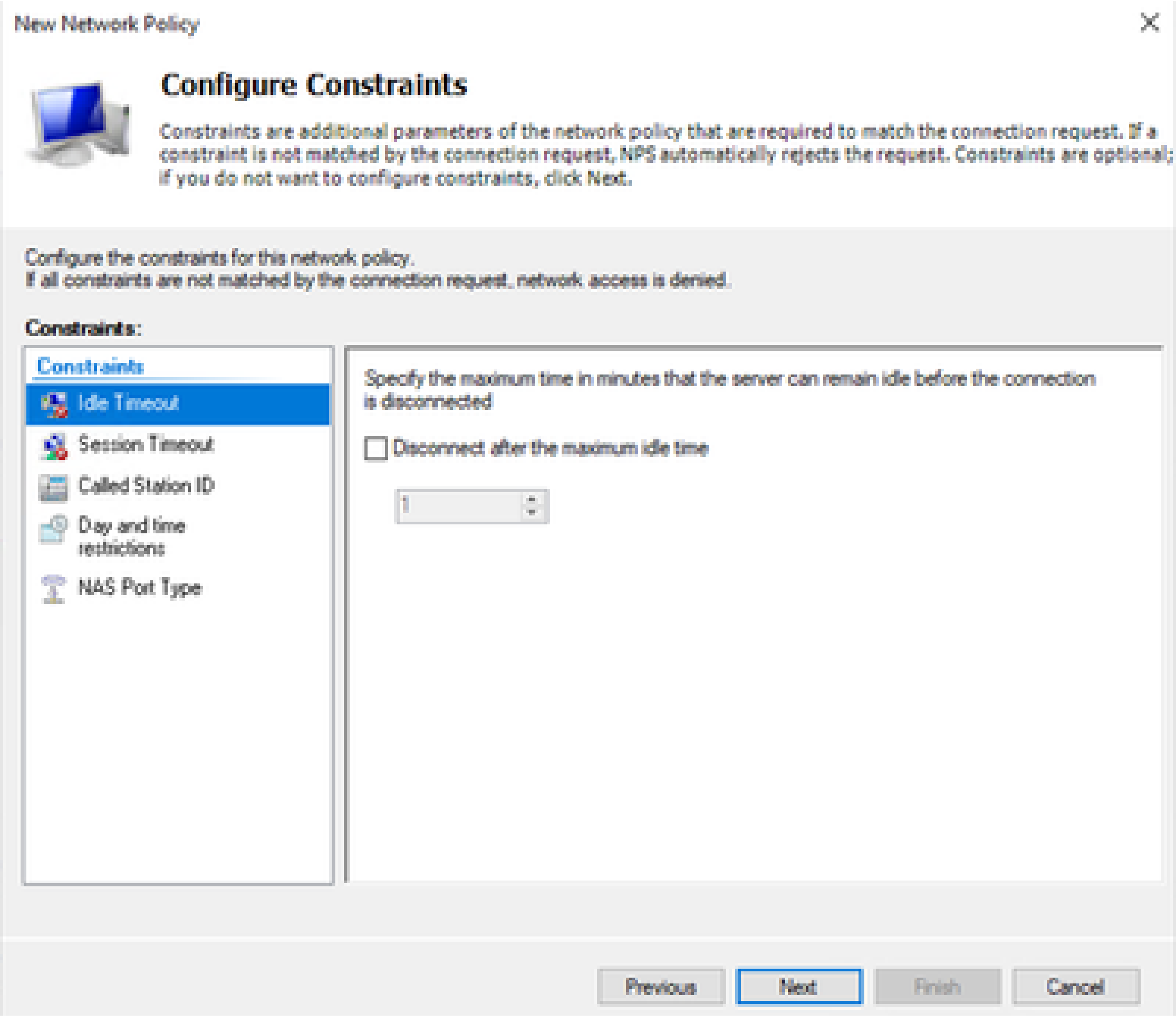
☑ Encrypted authentication (CHAP)

□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.

选择未加密的身份验证

12. 由于使用了默认值，请选择Next：



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:

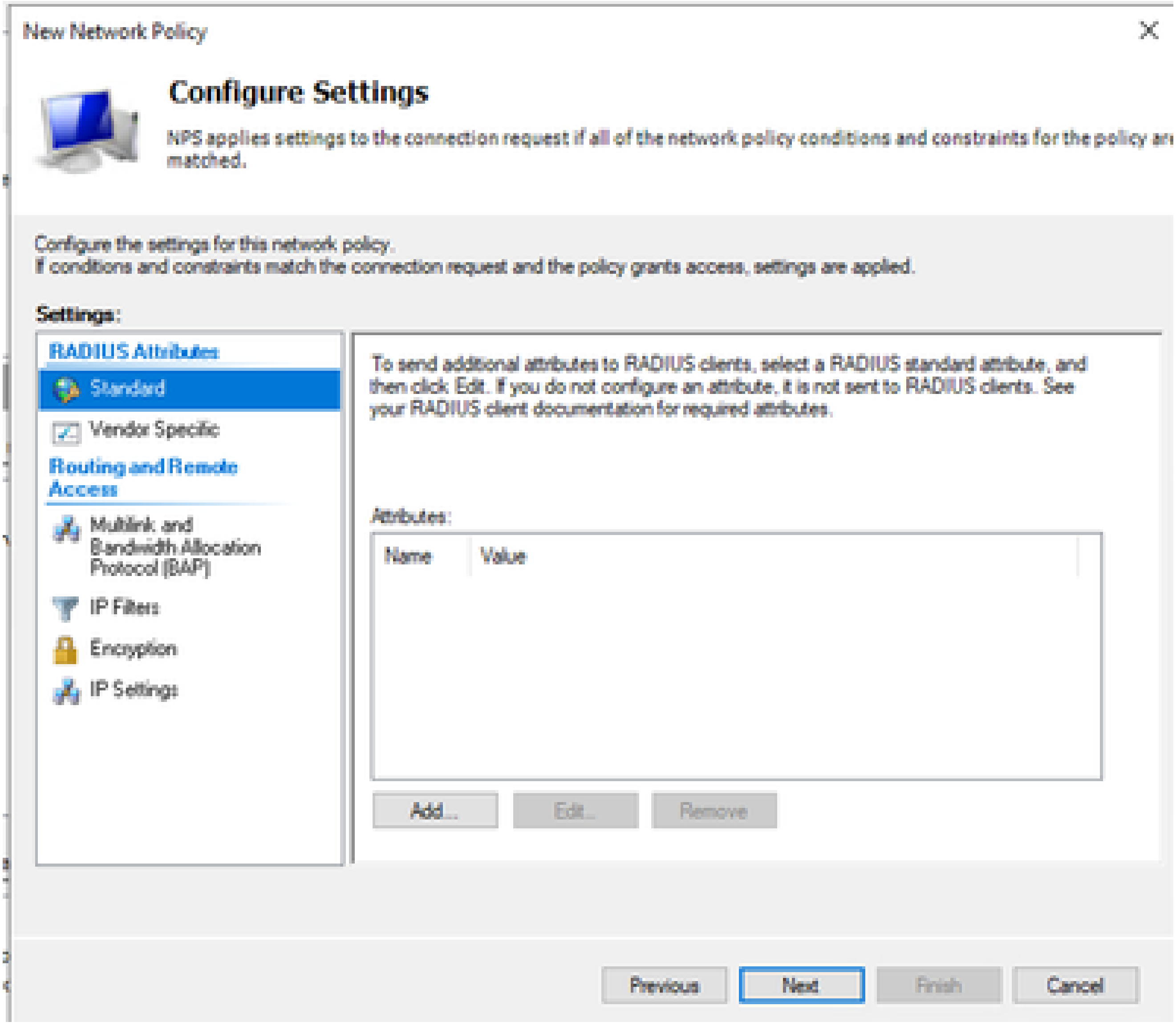
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

配置约束窗口

13. 删除标准属性：



New Network Policy

Configure Settings

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

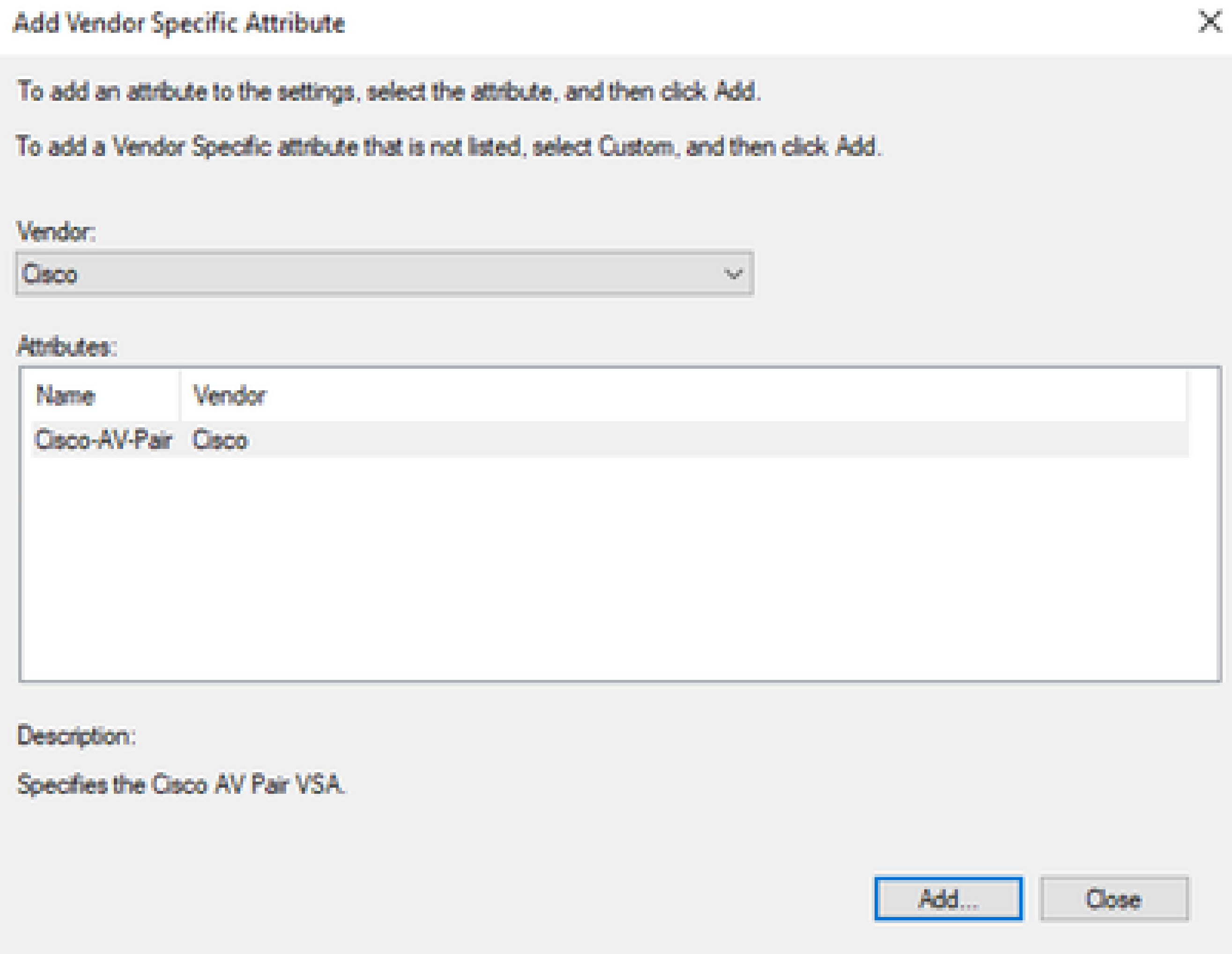
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value

定义要使用的属性

14. 在RADIUS属性上，选择Vendor Specific，然后点击Add，选择Cisco作为供应商，然后点击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:

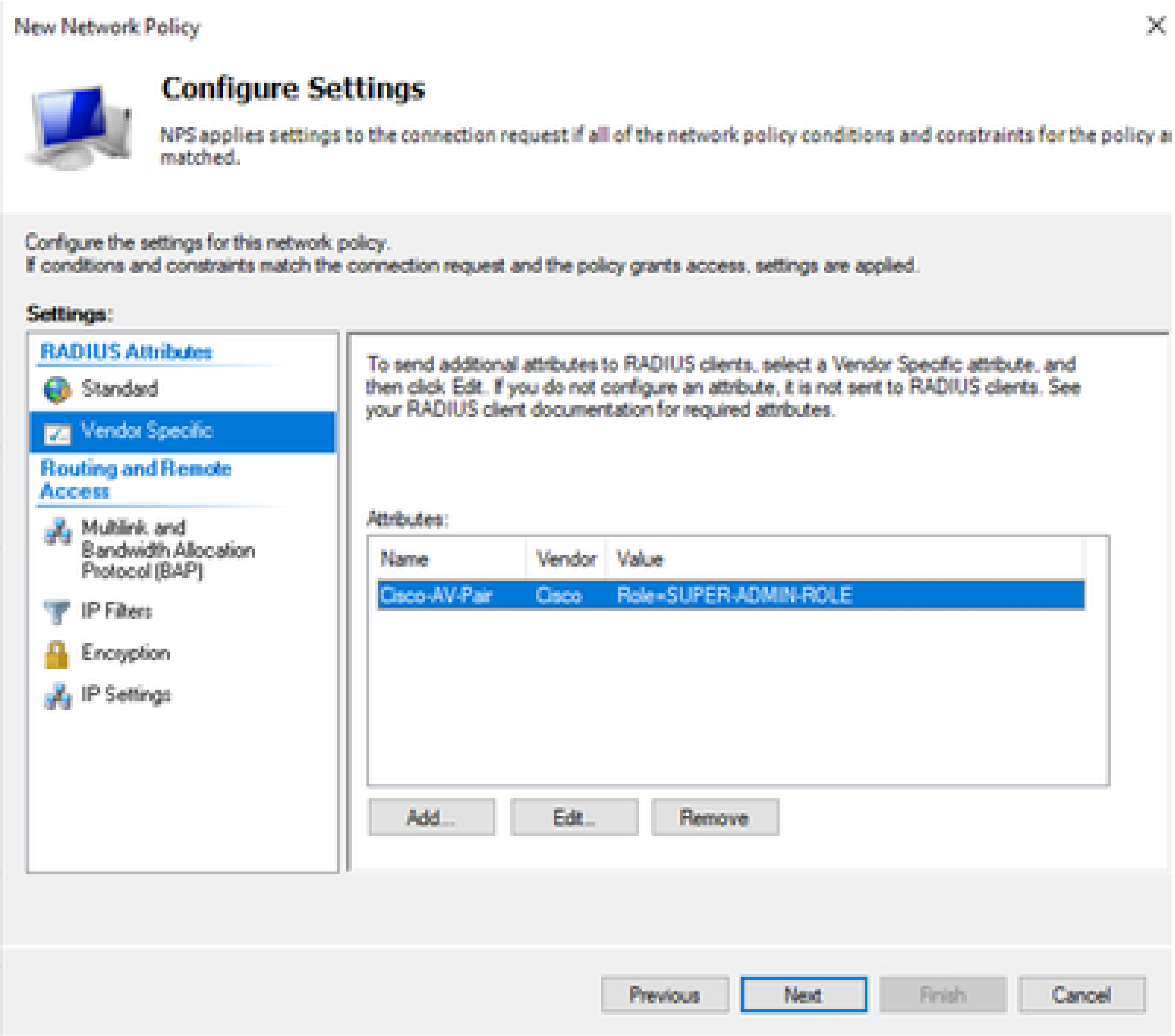
Name	Vendor
Cisco-AV-Pair	Cisco

Description:

Specifies the Cisco AV Pair VSA.

添加思科AV对

15. 单击Add，写入Role=SUPER-ADMIN-ROLE，然后单击OK两次：


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:

RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings

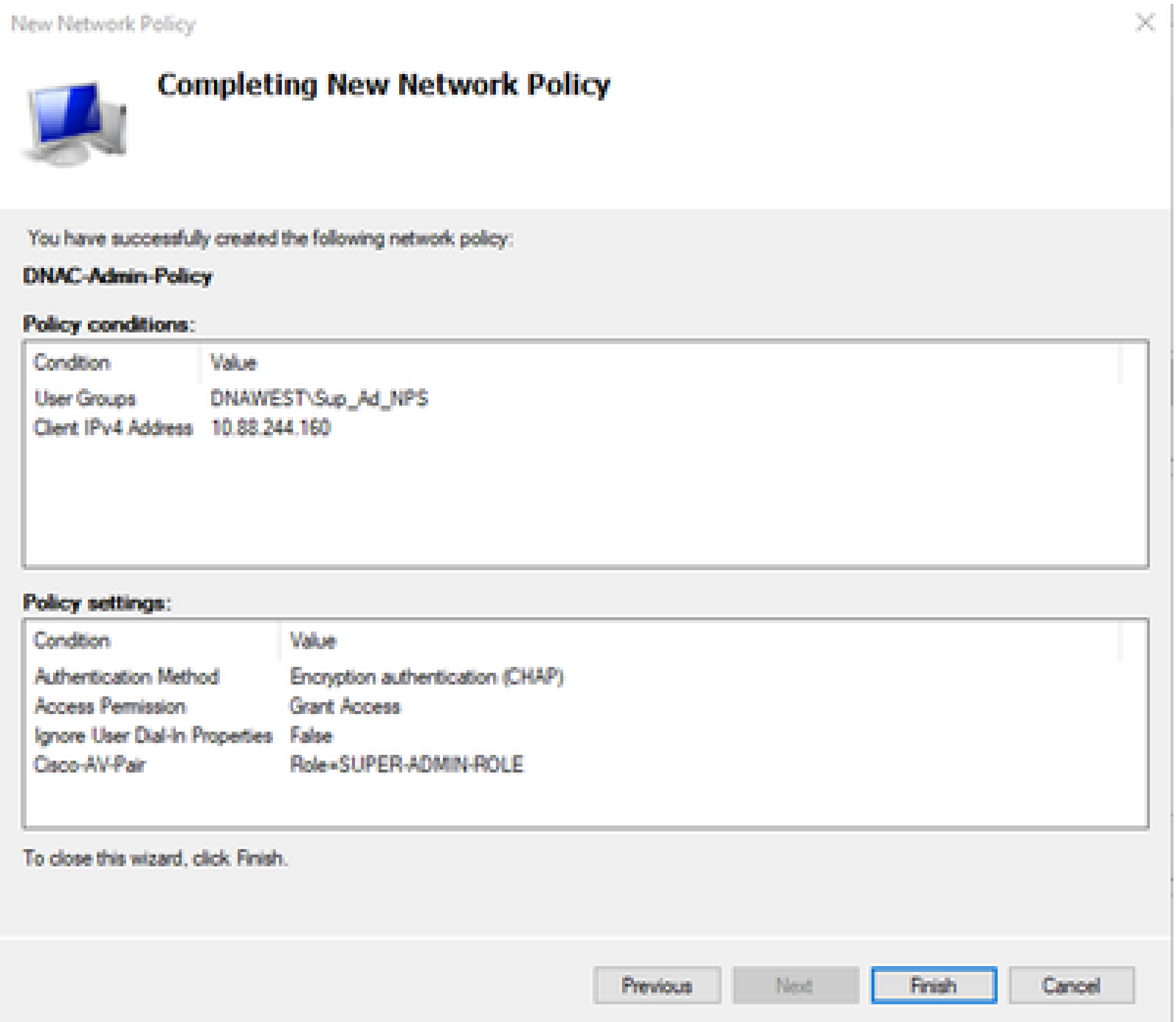
To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

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

添加了Cisco AV-Pair属性

16. 选择关闭，然后选择下一步。
17. 检查策略设置，然后选择完成保存策略。



New Network Policy

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.

策略摘要

观察者角色策略。

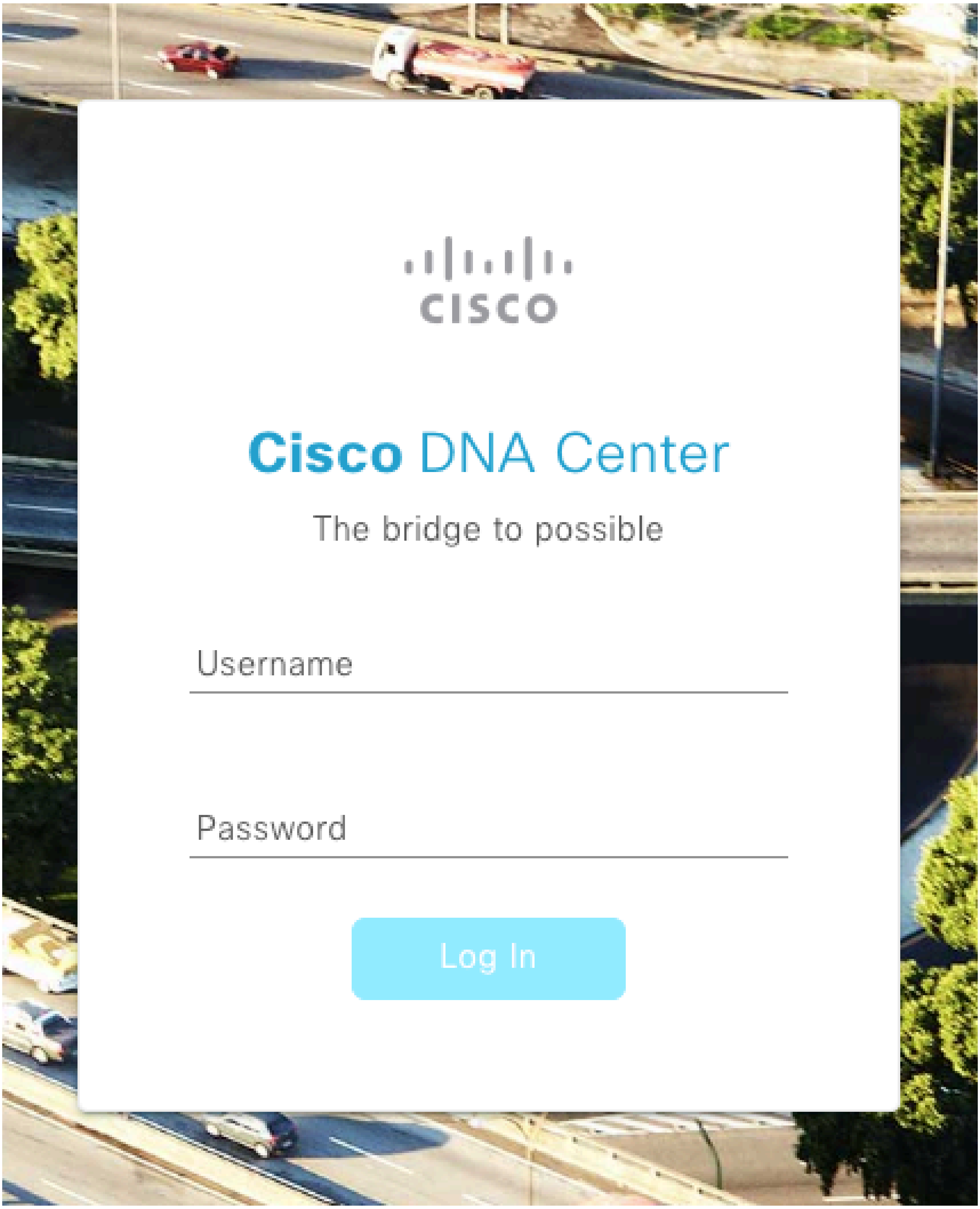
1. 单击Windows Start菜单并搜索NPS。然后选择Network Policy Server。
2. 从左侧的导航面板中，在NPS (Local) 选项中执行右键单击，然后选择Register server in Active Directory。
3. 单击OK两次。
4. 展开RADIUS Clients and Servers，右键单击RADIUS Clients，然后选择New。
5. 输入友好名称、Cisco DNA中心管理IP地址和共享密钥（这一点可以在以后使用）。
6. 单击OK保存它。
7. 展开Policies，右键单击Network Policies，然后选择New。
8. 为规则输入策略名称，然后单击Next。
9. 要允许特定域组，需要添加这两个条件并选择Next。

- 用户组- 添加您的域组以在Cisco DNA Center上分配观察者角色（例如，使用Observer_NPS组）。
- ClientIPv4Address -添加您的Cisco DNA Center管理IP。

10. 选择Access Granted，然后选择Next。
11. 仅选择Unencrypted authentication (PAP， SPAP)。
12. 由于使用了默认值，请选择Next。
13. 删除Standard属性。
14. 在RADIUS属性上，选择Vendor Specific，然后单击Add，选择Cisco作为供应商，然后单击Add。
15. 选择Add，写入ROLE=OBSERVER-ROLE，然后OK两次。
16. 选择关闭，然后选择下一步。
17. 检查策略设置并选择Finish保存设置。

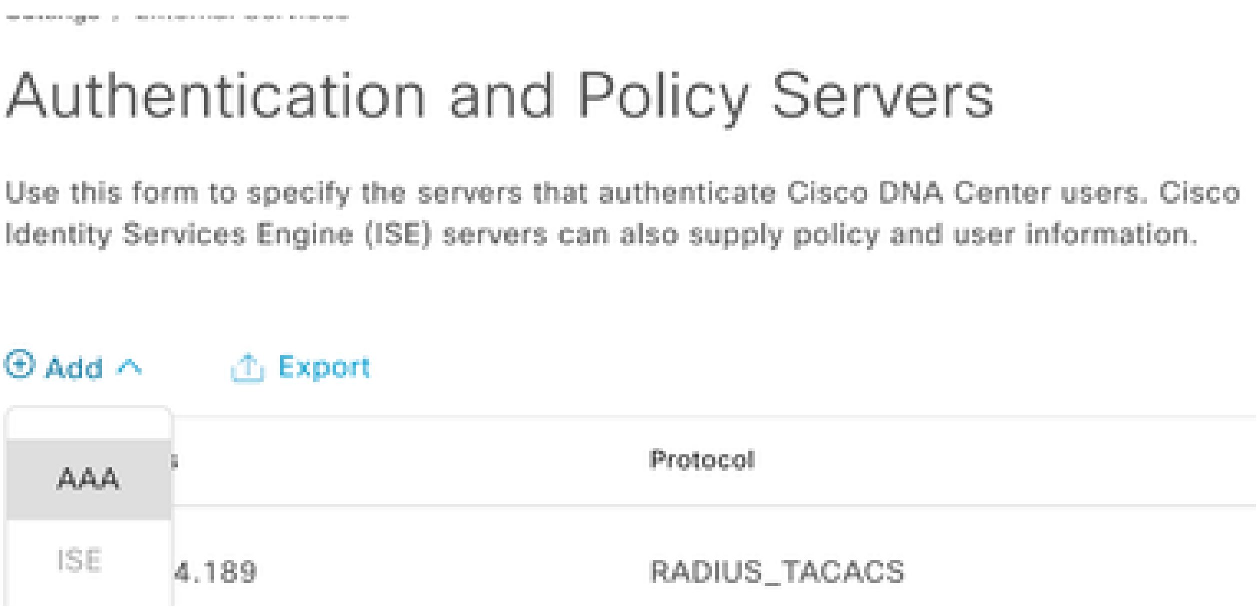
启用外部身份验证

1. 在Web浏览器中打开Cisco DNA Center图形用户界面(GUI)，然后使用管理员特权帐户登录：



Cisco DNA Center登录页

2. 导航到菜单>系统>设置> 身份验证和策略服务器，然后选择添加> AAA：



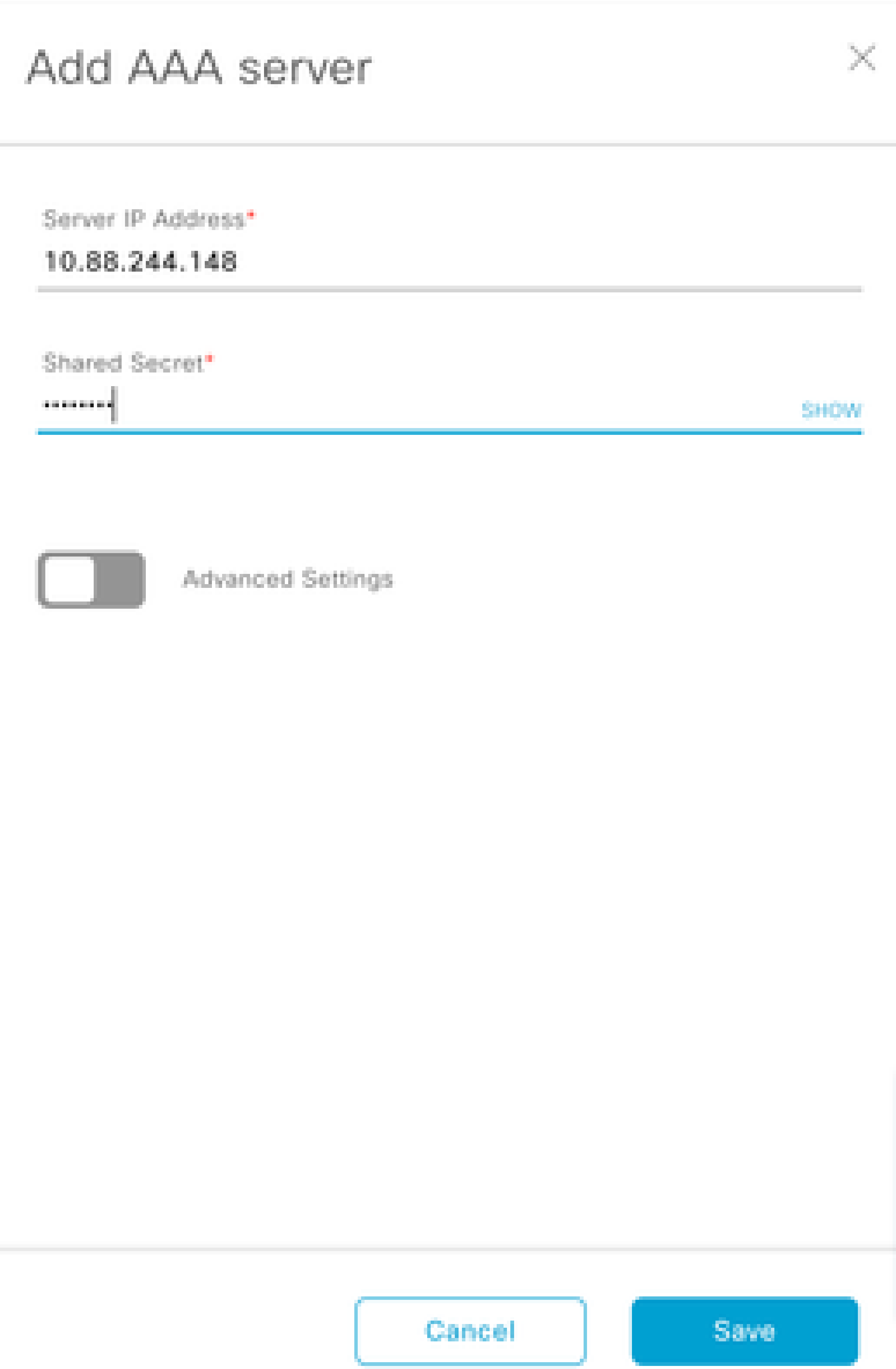
Authentication and Policy Servers

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.

	Protocol
4.189	RADIUS_TACACS

添加Windows服务器

3. 键入您在前面的步骤中使用的Windows Server IP地址和共享密钥，然后单击Save：



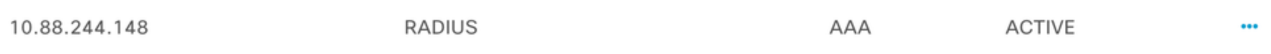
Add AAA server

Server IP Address*
10.88.244.148

Shared Secret*
••••••••

Windows服务器值

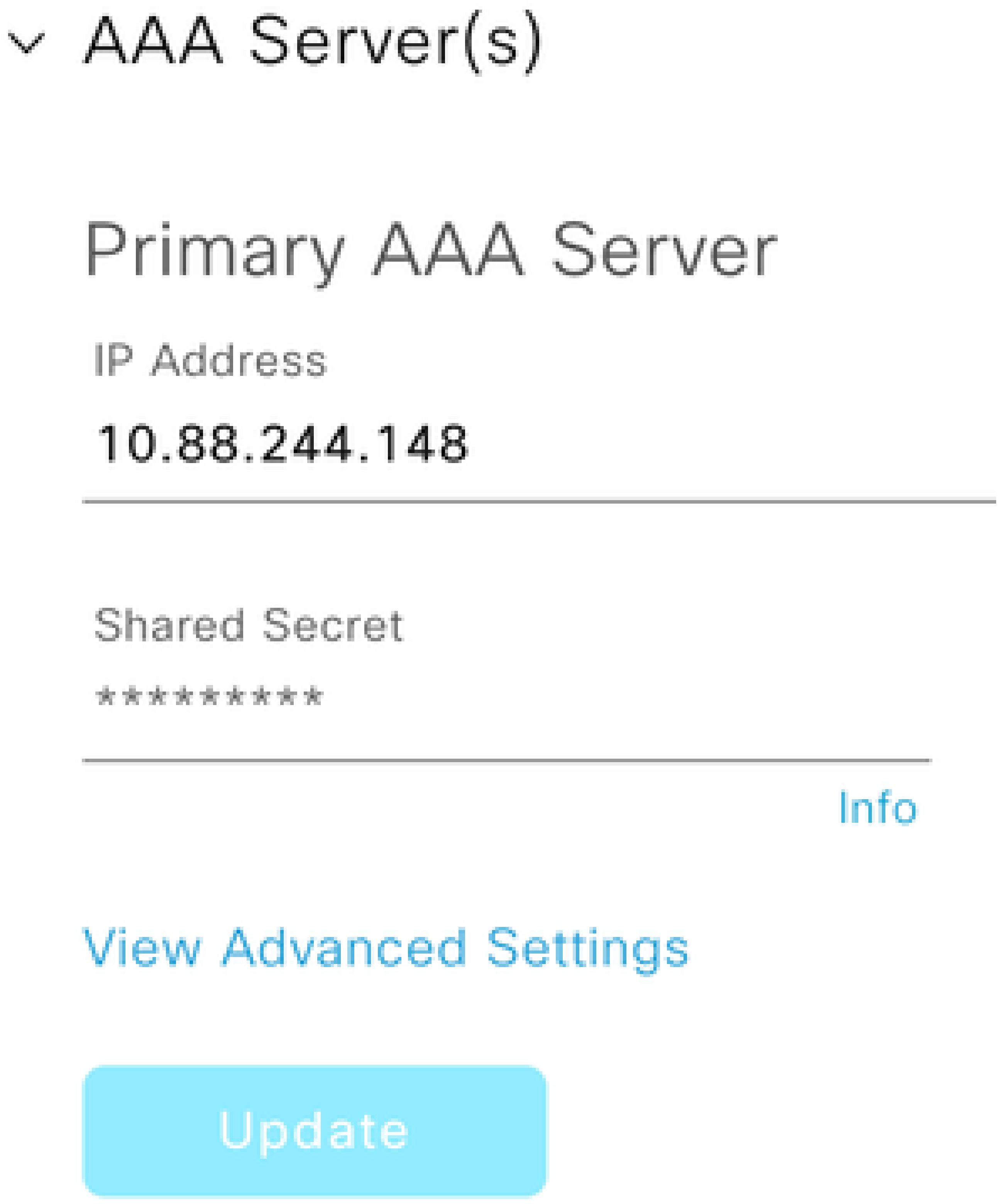
4. 验证您的Windows Server状态为Active：



10.88.244.148	RADIUS	AAA	ACTIVE	•••

Windows Server摘要

5. 导航到菜单 > 系统 > 用户和角色 > 外部身份验证，然后选择AAA服务器：



AAA Server(s)

Primary AAA Server

IP Address

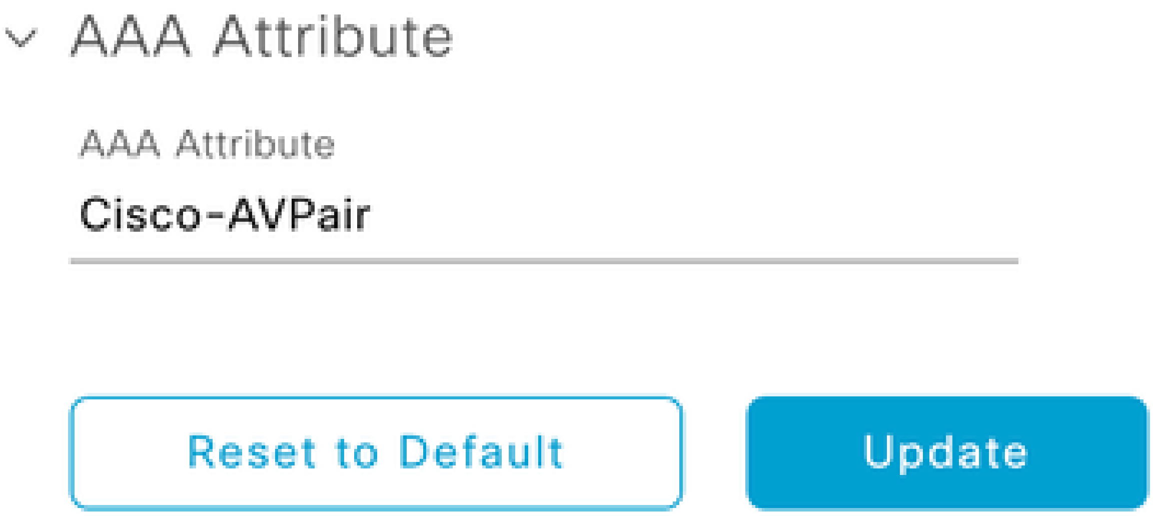
10.88.244.148

Shared Secret

****

Windows Server作为AAA服务器

6. 键入Cisco-AVPair作为AAA属性，然后单击Update：



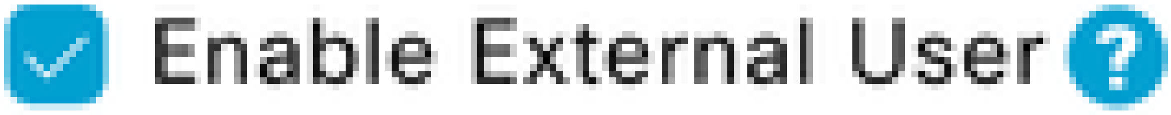
AAA Attribute

AAA Attribute

Cisco-AVPair

外部用户上的AV对

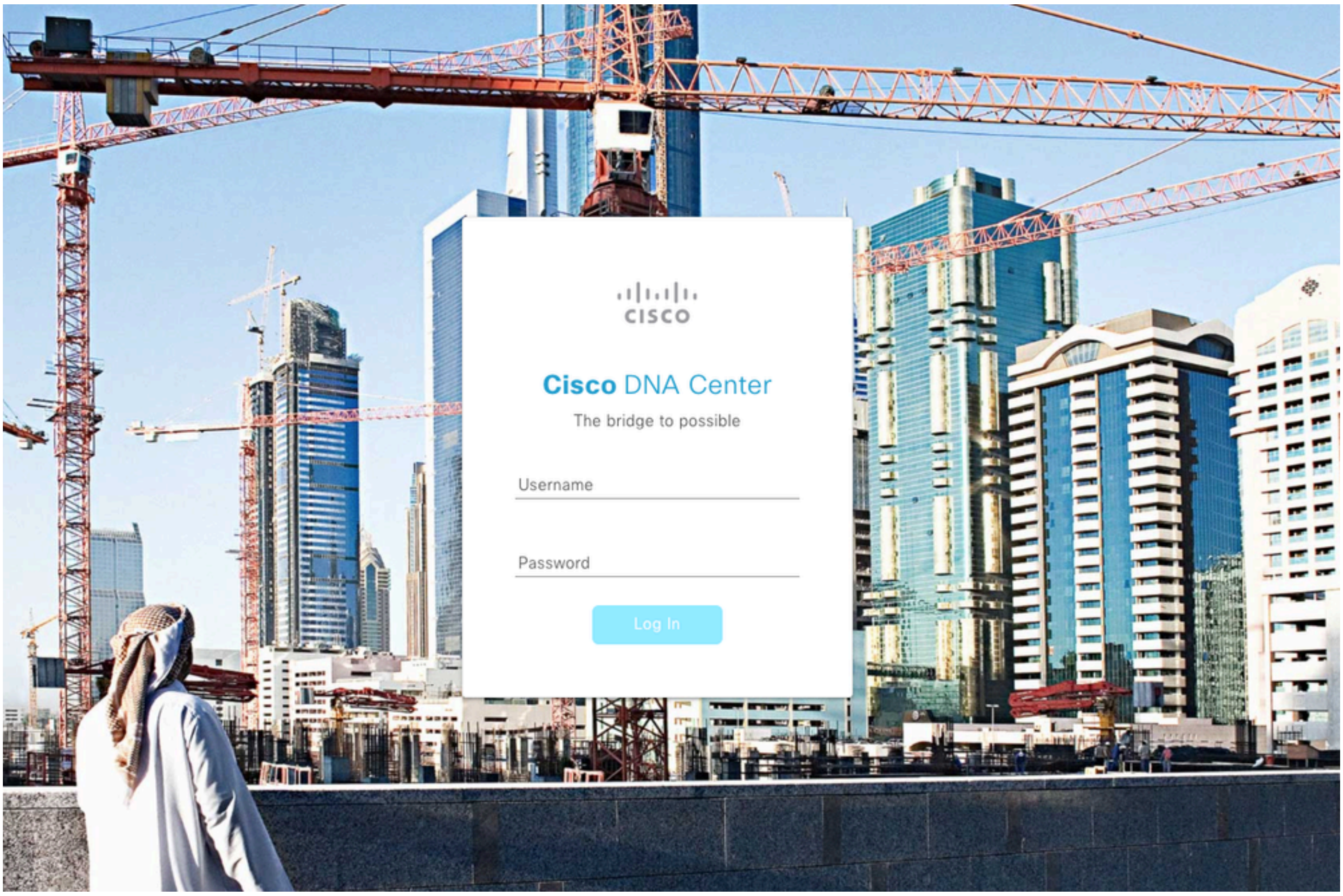
7. 单击Enable External User 复选框以启用外部身份验证：



☑ Enable External User

验证

您可以在Web浏览器中打开Cisco DNA Center Graphical User Interface (GUI)，并使用Windows Server中配置的外部用户登录，以验证您可以使用外部身份验证成功登录。



Cisco DNA Center

The bridge to possible

Username

Password

Cisco DNA Center登录页

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。