

# Windows Server를 사용하여 Catalyst Center에서 외부 인증 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[관리자 역할 정책](#)

[Observer Role Policy\(관찰자 역할 정책\)](#)

[외부 인증 사용](#)

[다음을 확인합니다.](#)

---

## 소개

이 문서에서는 Windows Server의 NPS(Network Policy Server)를 RADIUS로 사용하여 Cisco DNA Center에서 외부 인증을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

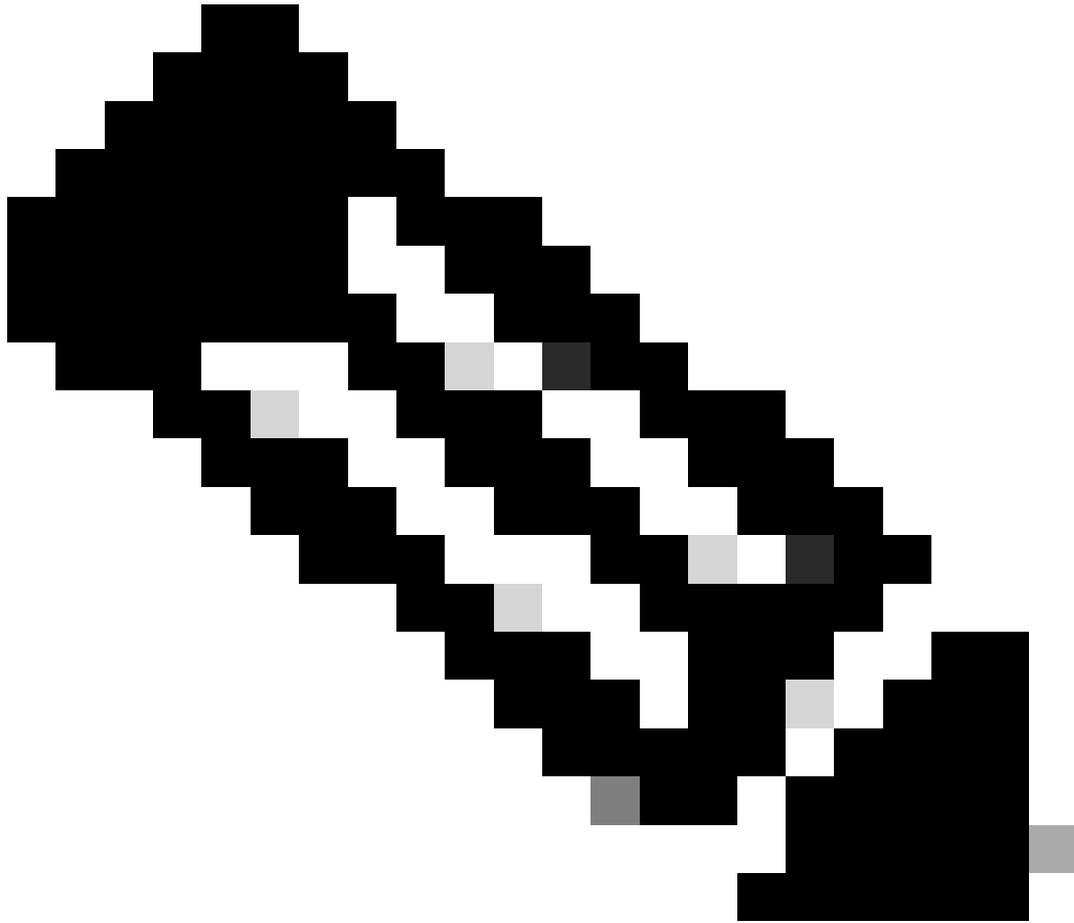
기본 지식:

- Cisco DNA Center 사용자 및 역할
- Windows Server 네트워크 정책 서버, RADIUS 및 Active Directory

### 사용되는 구성 요소

- Cisco DNA Center 2.3.5.x
- 도메인 컨트롤러, DNS 서버, NPS 및 Active Directory 역할을 하는 Microsoft Windows Server 버전 2019

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.



참고: Cisco TAC(Technical Assistance Center)에서는 Microsoft Windows Server에 대한 기술 지원을 제공하지 않습니다. Microsoft Windows Server 구성에 문제가 있으면 Microsoft 지원에 기술 지원을 요청하십시오.

---

## 구성

### 관리자 역할 정책

1. Windows 시작 메뉴를 클릭하고 NPS를 검색합니다. 그런 다음 Network Policy Server(네트워크 정책 서버)를 선택합니다.

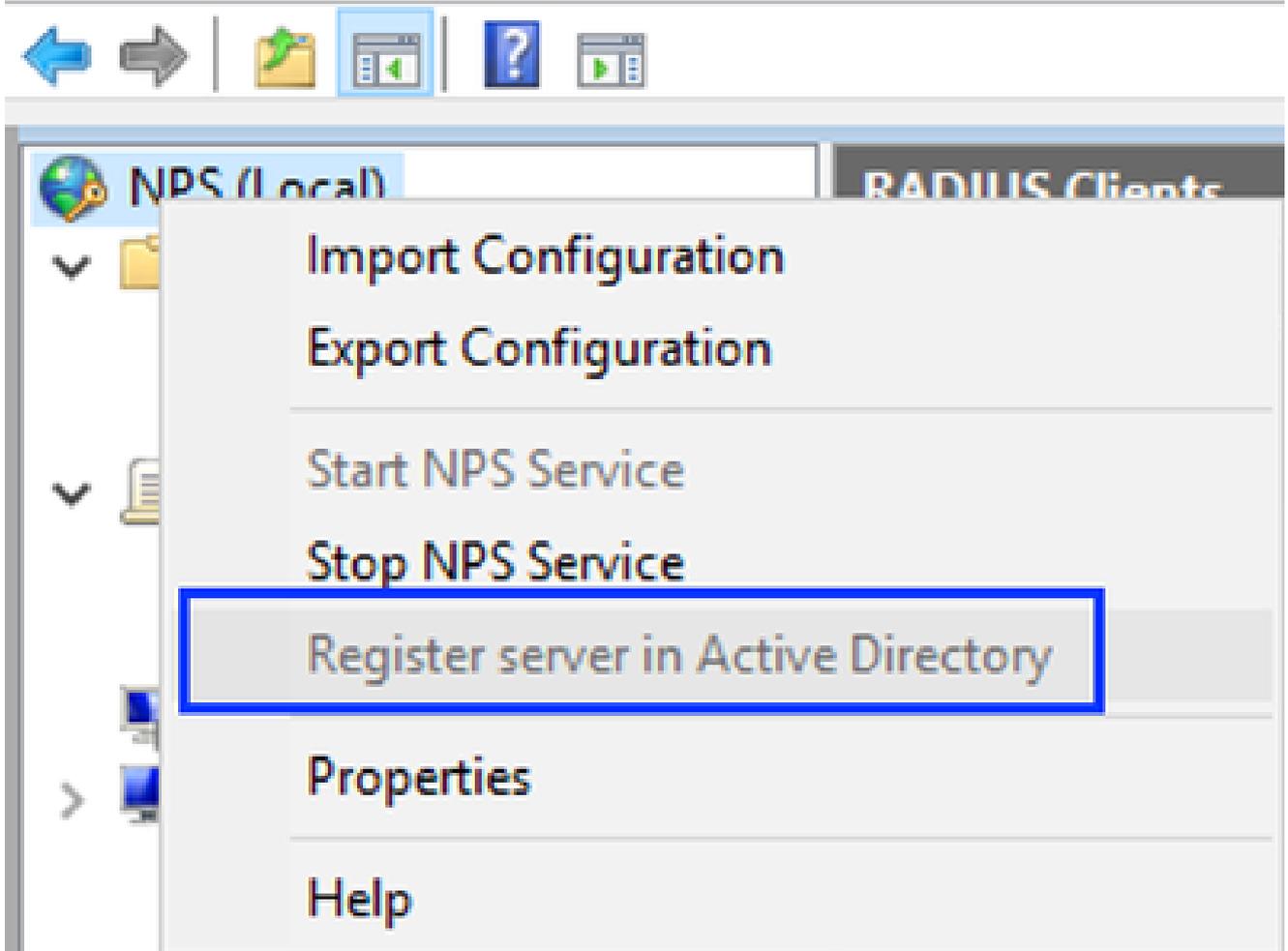


# Network Policy Server

Desktop app

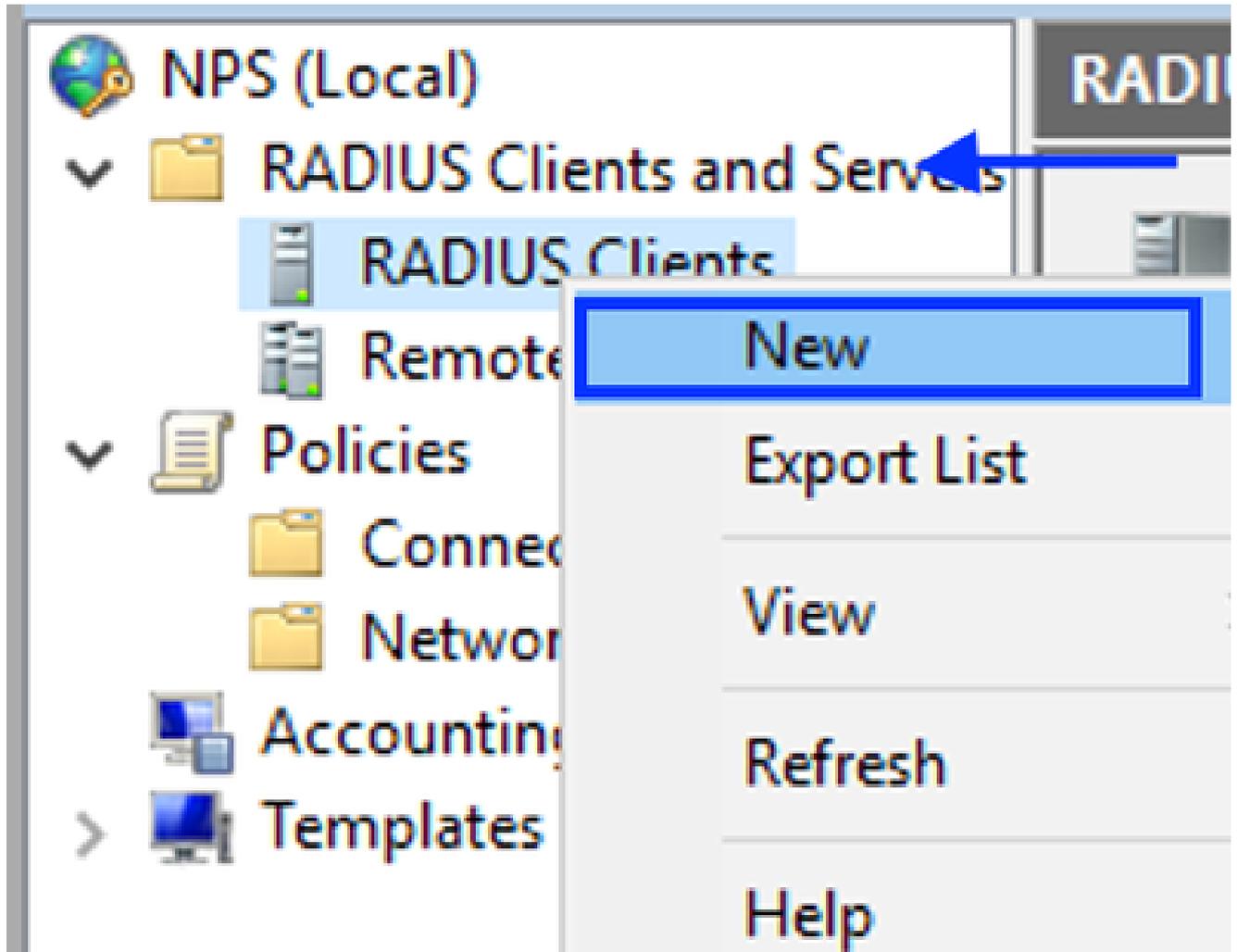
## Network Policy Server

File Action View Help



Windows 네트워크 정책 서비스

3. OK(확인)를 두 번 클릭합니다.
4. RADIUS Clients and Servers(RADIUS 클라이언트 및 서버)를 확장하고 RADIUS Clients(RADIUS 클라이언트)를 마우스 오른쪽 버튼으로 클릭한 다음 New(새로 만들기)를 선택합니다.



RADIUS 클라이언트 추가

5. 식별 이름, Cisco DNA Center 관리 IP 주소 및 공유 암호를 입력합니다(나중에 사용 가능).

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.

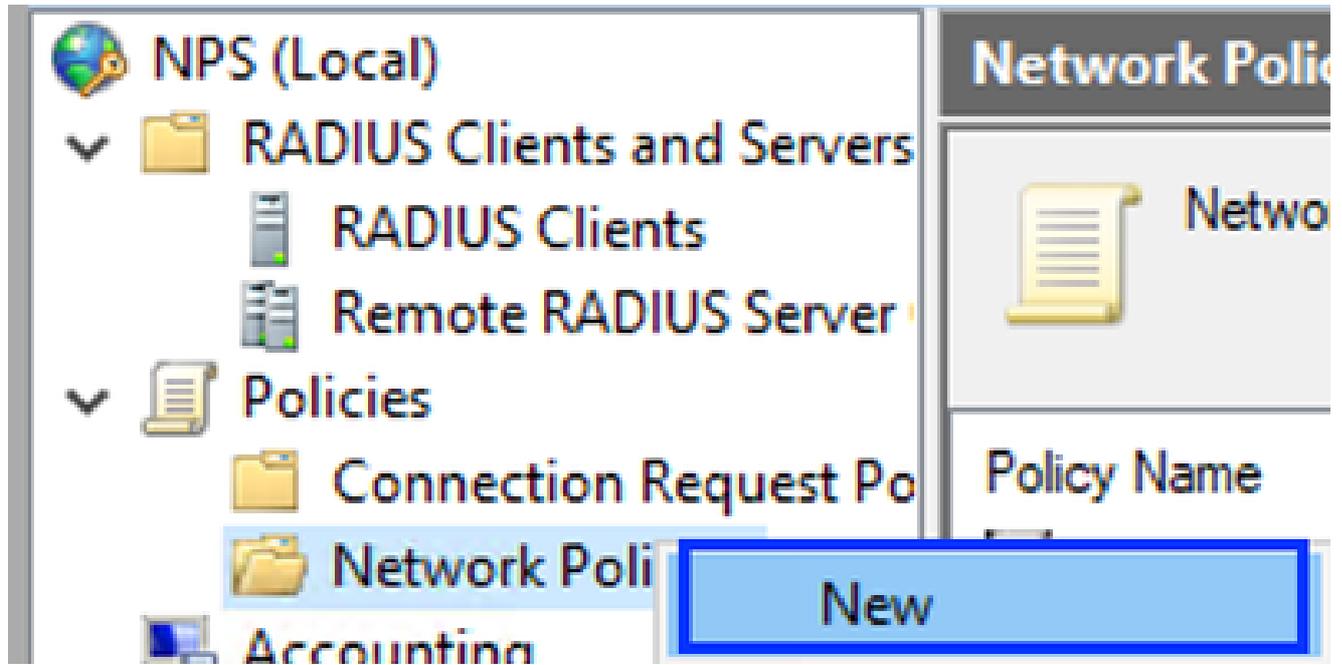
Manual       Generate

Shared secret:

Confirm shared secret:

Radius 클라이언트 컨피그레이션

6. OK(확인)를 클릭하여 저장합니다.
7. Policies(정책)를 확장하고 Network Policies(네트워크 정책)를 마우스 오른쪽 버튼으로 클릭한 다음 New(새로 만들기)를 선택합니다.



새 네트워크 정책 추가

8. 규칙의 정책 이름을 입력하고 Next(다음)를 클릭합니다.



## 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.

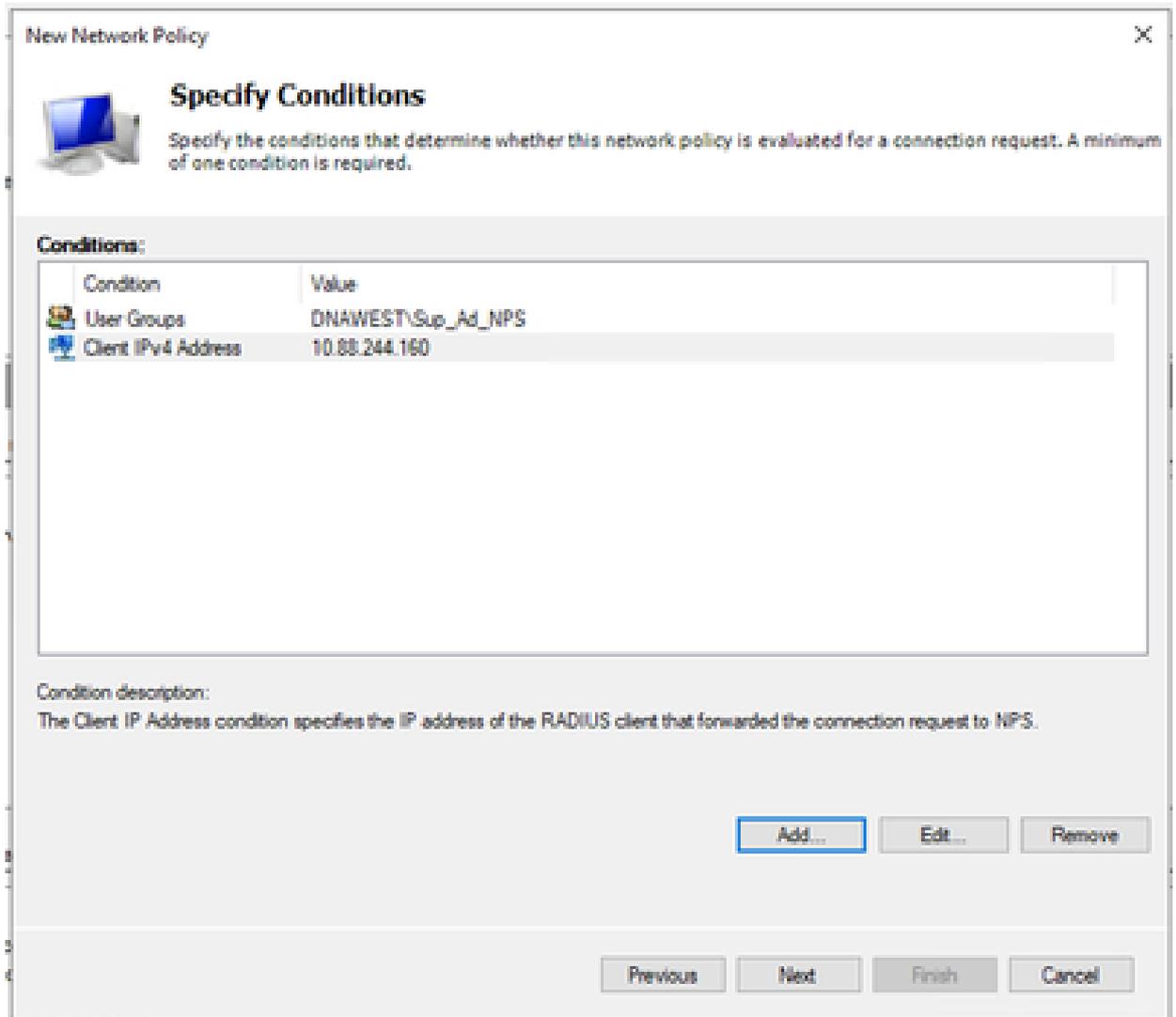
Type of network access server:  
Unspecified

Vendor specific:  
10

Previous Next Finish Cancel

정책 이름

- 특정 도메인 그룹을 허용하려면 다음 두 조건을 추가하고 다음을 클릭합니다.
  - 사용자 그룹 - Cisco DNA Center에서 관리자 역할을 가질 수 있는 도메인 그룹을 추가합니다(이 예에서는 Sup\_Ad\_NPS 그룹이 사용됨).
  - ClientIPv4Address - Cisco DNA Center 관리 IP 주소를 추가합니다.



정책 조건

10. Access Granted를 선택하고 Next(다음)를 클릭합니다.

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.

Previous Next Finish Cancel

부여된 액세스 사용

11. Unencrypted authentication (PAP, SPAP)만 선택합니다.



## 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

암호화되지 않은 인증 선택

12. 기본값이 사용되므로 다음을 선택합니다.



## 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:

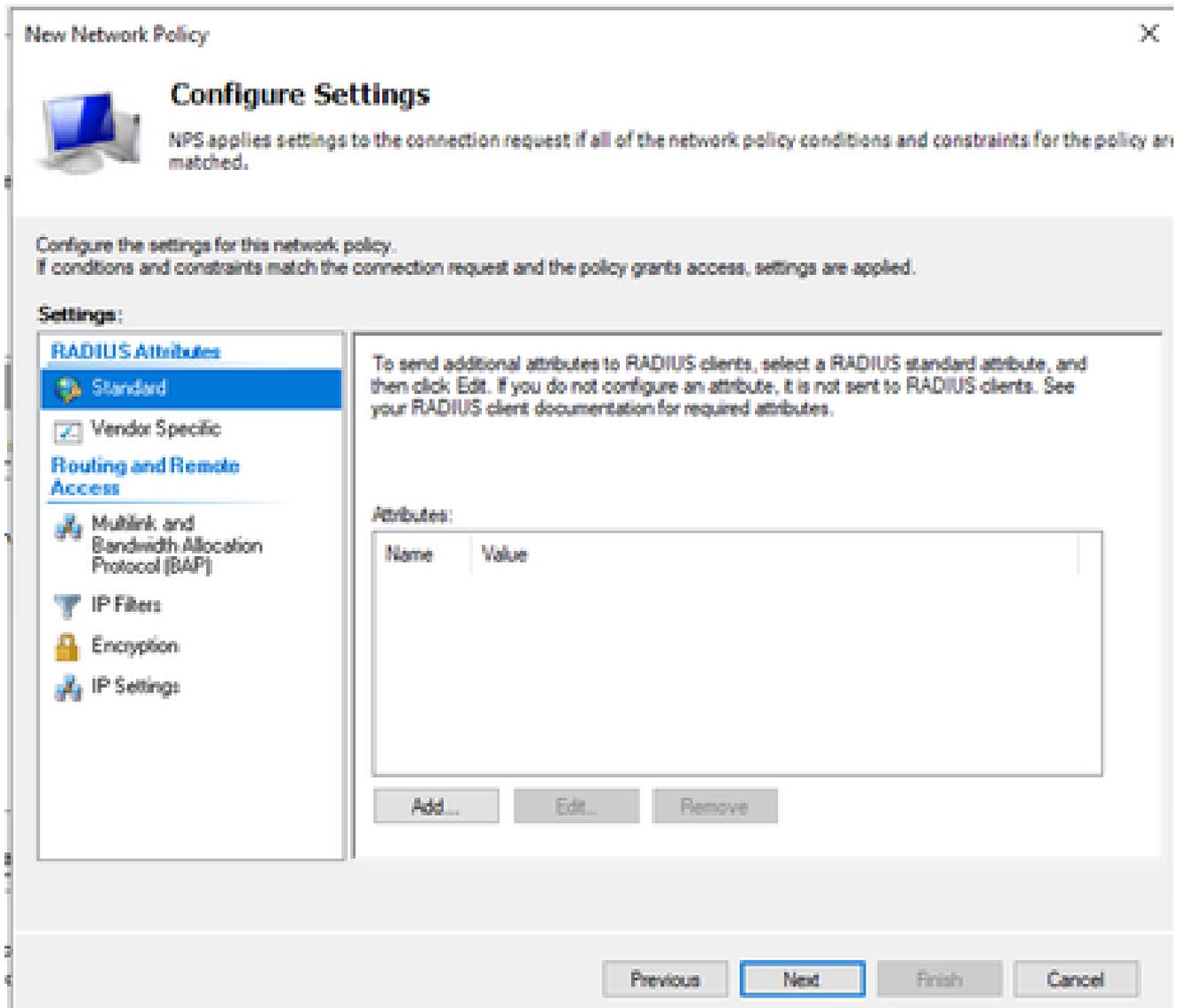
Constraints	
Idle Timeout	Specify the maximum time in minutes that the server can remain idle before the connection is disconnected <input type="checkbox"/> Disconnect after the maximum idle time <input type="text" value="1"/>
Session Timeout	
Called Station ID	
Day and time restrictions	
NAS Port Type	





제약 조건 구성 창

### 13. 표준 속성 제거:



사용할 특성 정의

14. RADIUS Attributes(RADIUS 특성)에서 Vendor Specific(벤더별)을 선택한 다음 Add(추가)를 클릭하고 Cisco as a Vendor(공급업체로 Cisco)를 선택한 다음 Add(추가)를 클릭합니다.

## 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 쌍 추가

15. Add(추가)를 클릭하고 Role=SUPER-ADMIN-ROLE을 쓴 다음 OK(확인)를 두 번 클릭합니다.



## 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 쌍 특성 추가됨

16. 달기를 선택한 다음 다음을 선택합니다.

17. 정책 설정을 검토하고 Finish(마침)를 선택하여 저장합니다.



## 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.





정책 요약

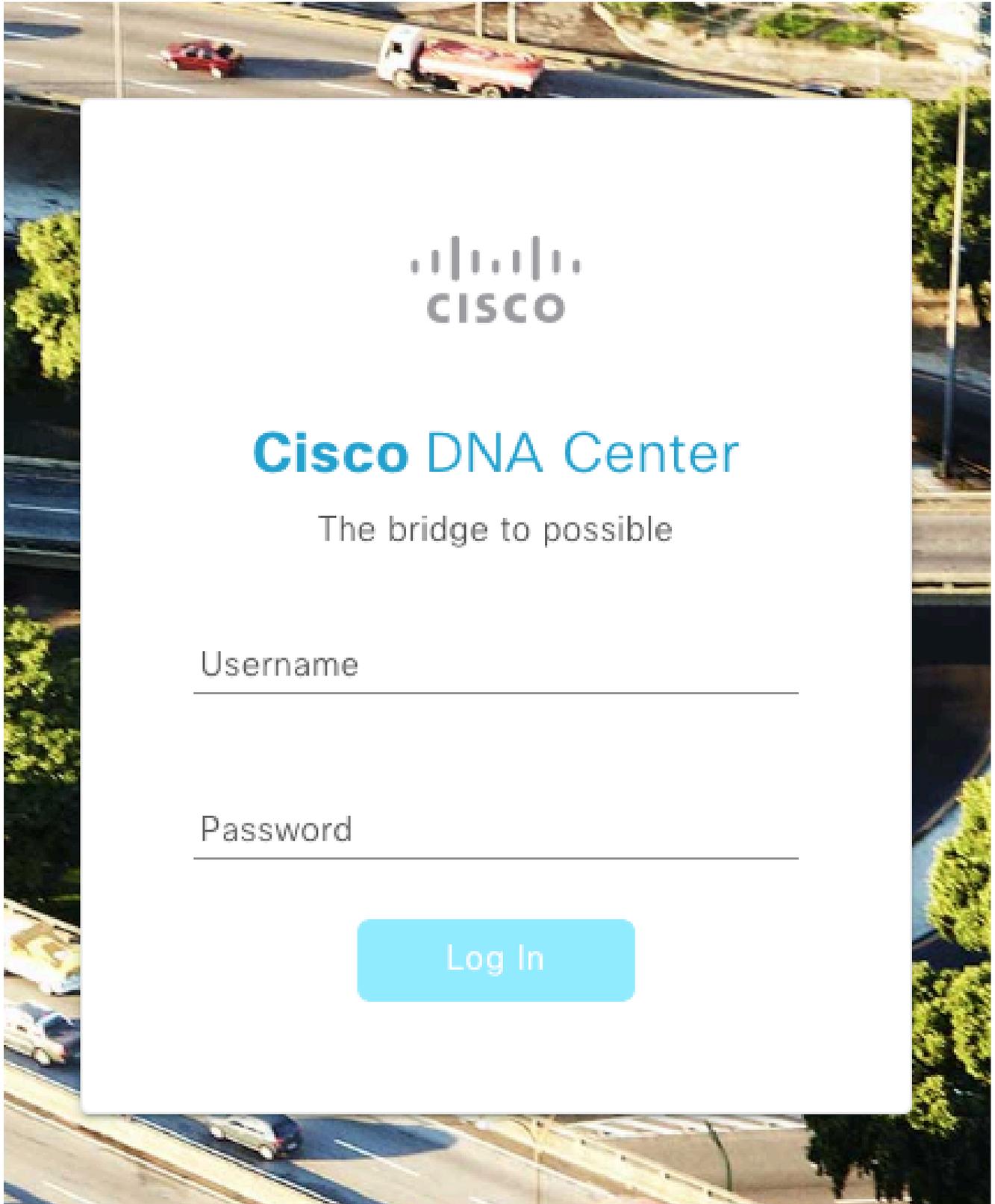
## Observer Role Policy(관찰자 역할 정책)

1. Windows 시작 메뉴를 클릭하고 NPS를 검색합니다. 그런 다음 Network Policy Server를 선택합니다.
2. 왼쪽의 탐색 패널에서 NPS (Local) 옵션에서 마우스 오른쪽 버튼을 클릭하고 Active Directory에서 서버 등록을 선택합니다.
3. OK(확인)를 두 번 클릭합니다.
4. RADIUS Clients and Servers(RADIUS 클라이언트 및 서버)를 확장하고 RADIUS Clients(RADIUS 클라이언트)를 마우스 오른쪽 버튼으로 클릭한 다음 New(새로 만들기)를 선택합니다.
5. 이름, Cisco DNA Center 관리 IP 주소 및 공유 암호를 입력합니다(나중에 사용 가능).
6. OK(확인)를 클릭하여 저장합니다.

7. Policies(정책)를 확장하고 Network Policies(네트워크 정책)를 마우스 오른쪽 버튼으로 클릭한 다음 New(새로 만들기)를 선택합니다.
8. 규칙의 정책 이름을 입력하고 Next(다음)를 클릭합니다.
9. 특정 도메인 그룹을 허용하려면 이 두 조건을 추가하고 다음을 선택해야 합니다.
  - 사용자 그룹 - Cisco DNA Center에서 관찰자 역할을 할당하려면 도메인 그룹을 추가합니다(이 예에서는 Observer\_NPS 그룹이 사용됨).
  - ClientIPv4Address - Cisco DNA Center 관리 IP 추가
10. Access Granted(액세스 허용)를 선택하고 Next(다음)를 선택합니다.
11. Unencrypted authentication (PAP, SPAP)만 선택합니다.
12. 기본값이 사용되므로 다음을 선택합니다.
13. 표준 특성을 제거합니다.
14. RADIUS Attributes(RADIUS 특성)에서 Vendor Specific(벤더별)을 선택한 다음 Add(추가)를 클릭하고 Cisco as a Vendor(공급업체로 Cisco)를 선택한 다음 Add(추가)를 클릭합니다.
15. Add(추가), write ROLE=OBSERVER-ROLE(역할 쓰기=OBSERVER-ROLE) 및 OK(확인)를 두 번 선택합니다.
16. Close(닫기), Next(다음)를 차례로 선택합니다.
17. 정책 설정을 검토하고 Finish를 선택하여 저장합니다.

## 외부 인증 사용

1. 웹 브라우저에서 Cisco DNA Center GUI(Graphical User Interface)를 열고 관리자 권한 계정을 사용하여 로그인합니다.



Cisco DNA Center 로그인 페이지

2. Menu(메뉴) > System(시스템) > Setting(설정) > Authentication and Policy Servers(인증 및 정책 서버)로 이동하고 Add(추가) > AAA를 선택합니다.

# 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 추가

- 이전 단계에서 사용한 Windows Server IP 주소와 공유 암호를 입력하고 Save(저장)를 클릭합니다.

# Add AAA server



Server IP Address\*

10.88.244.148

Shared Secret\*

.....|

[SHOW](#)



Advanced Settings

Cancel

Save

4. Windows Server 상태가 활성인지 확인합니다.

10.88.244.148

RADIUS

AAA

ACTIVE



Windows Server 요약

5. Menu(메뉴) > System(시스템) > Users & Roles(사용자 및 역할) > External Authentication(외부 인증)으로 이동하여 AAA 서버를 선택합니다.

## ▼ AAA Server(s)

### Primary AAA Server

IP Address

10.88.244.148

---

Shared Secret

\*\*\*\*\*

---

[Info](#)

[View Advanced Settings](#)

Update

Windows Server(AAA 서버)

6. AAA 특성으로 Cisco-AVPair를 입력하고 Update(업데이트)를 클릭합니다.

## ▼ AAA Attribute

AAA Attribute

Cisco-AVPair

---

Reset to Default

Update

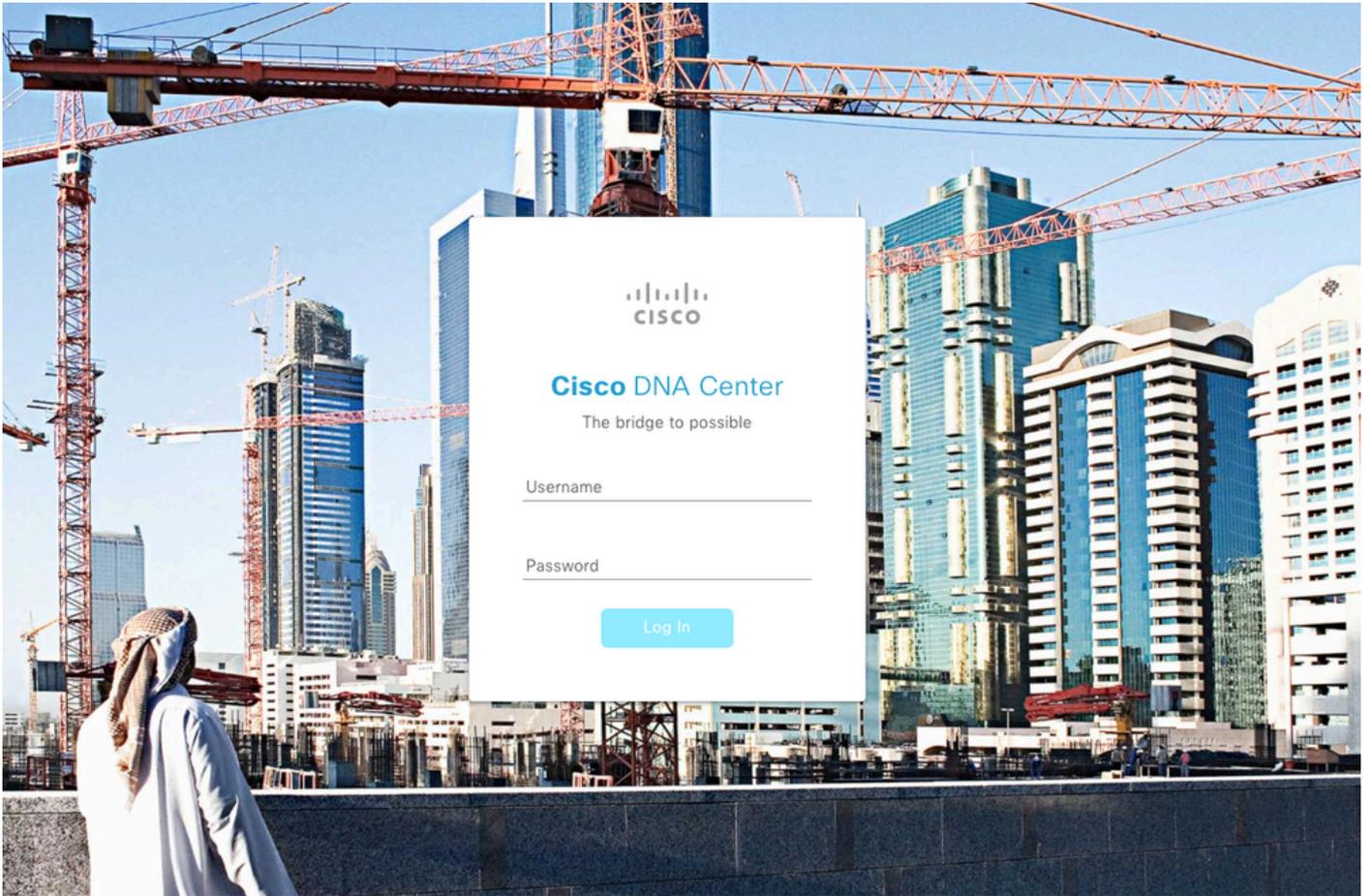
외부 사용자의 AV 쌍

7. 외부 인증을 활성화하려면 Enable External User(외부 사용자 활성화) 확인란을 클릭합니다.

**Enable External User** 

다음을 확인합니다.

웹 브라우저에서 Cisco DNA Center GUI(Graphical User Interface)를 열고 Windows Server에 구성된 외부 사용자로 로그인하여 외부 인증을 사용하여 성공적으로 로그인할 수 있는지 확인할 수 있습니다.



Cisco DNA Center 로그인 페이지

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.