

DNA Center 및 ISE 3.1에서 RADIUS 외부 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[다음을 확인합니다.](#)

[추가 역할](#)

소개

이 문서에서는 3.1 릴리스를 실행하는 Cisco ISE 서버를 사용하여 Cisco DNA Center에서 RADIUS 외부 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco DNA Center와 Cisco ISE는 이미 통합되었으며 통합이 활성화 상태입니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco DNA Center 2.3.5.x 릴리스.
- Cisco ISE 3.1 릴리스.

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.

구성

1단계. Cisco DNA Center GUI에 로그인하고 System > Settings > Authentication and Policy Servers로 이동합니다.

RADIUS 프로토콜이 구성되어 있고 ISE 유형 서버의 ISE 상태가 Active(활성)인지 확인합니다.

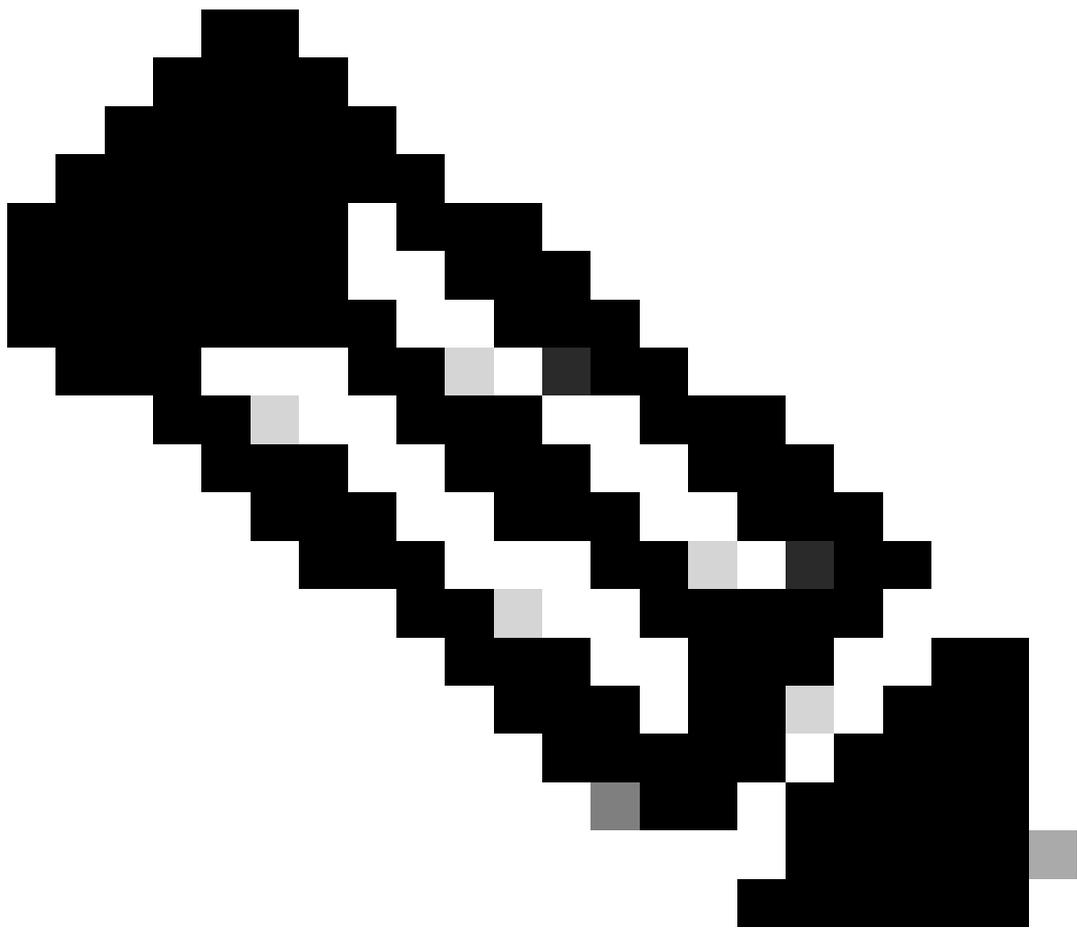
Authentication and Policy Servers

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](#)

As of: Jul 19, 2023 4:38 PM [Refresh](#)

IP Address	Protocol	Type	Status	Actions
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...
[REDACTED]	RADIUS	ISE	ACTIVE	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...



참고: RADIUS_TACACS 프로토콜 유형은 이 문서에 대해 작동합니다.



경고: ISE 서버가 활성 상태가 아닌 경우 먼저 통합을 수정해야 합니다.

2단계. ISE Server(ISE 서버)에서 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동하고, Filter(필터) 아이콘을 클릭하고 Cisco DNA Center IP Address(Cisco DNA Center IP 주소)를 작성한 다음 항목이 있는지 확인합니다. 그럴 경우 3단계로 진행합니다.

항목이 없으면 사용 가능한 데이터 없음 메시지가 표시되어야 합니다.

Network Devices

Selected 0 Total 0  

 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

이 경우 Cisco DNA Center용 네트워크 디바이스를 생성해야 하므로 Add(추가) 버튼을 클릭합니다.

Network Devices

Selected 0 Total 0

Edit + Add Duplicate Import Export Generate PAC Delete Quick Filter

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

Cisco DNA Center에서 이름, 설명 및 IP 주소(또는 주소)를 구성합니다. 다른 모든 설정은 기본값으로 설정되며 이 문서에서는 필요하지 않습니다.

Network Devices

* Name

Description

 IP Address / 

* Device Profile

Model Name

Software Version

* Network Device Group

Location	<input type="text" value="All Locations"/>	<input type="button" value="Set To Default"/>
IPSEC	<input type="text" value="Is IPSEC Device"/>	<input type="button" value="Set To Default"/>
Device Type	<input type="text" value="All Device Types"/>	<input type="button" value="Set To Default"/>

아래로 스크롤하여 해당 확인란을 클릭하여 RADIUS 인증 설정을 활성화하고 공유 암호를 구성합니다.



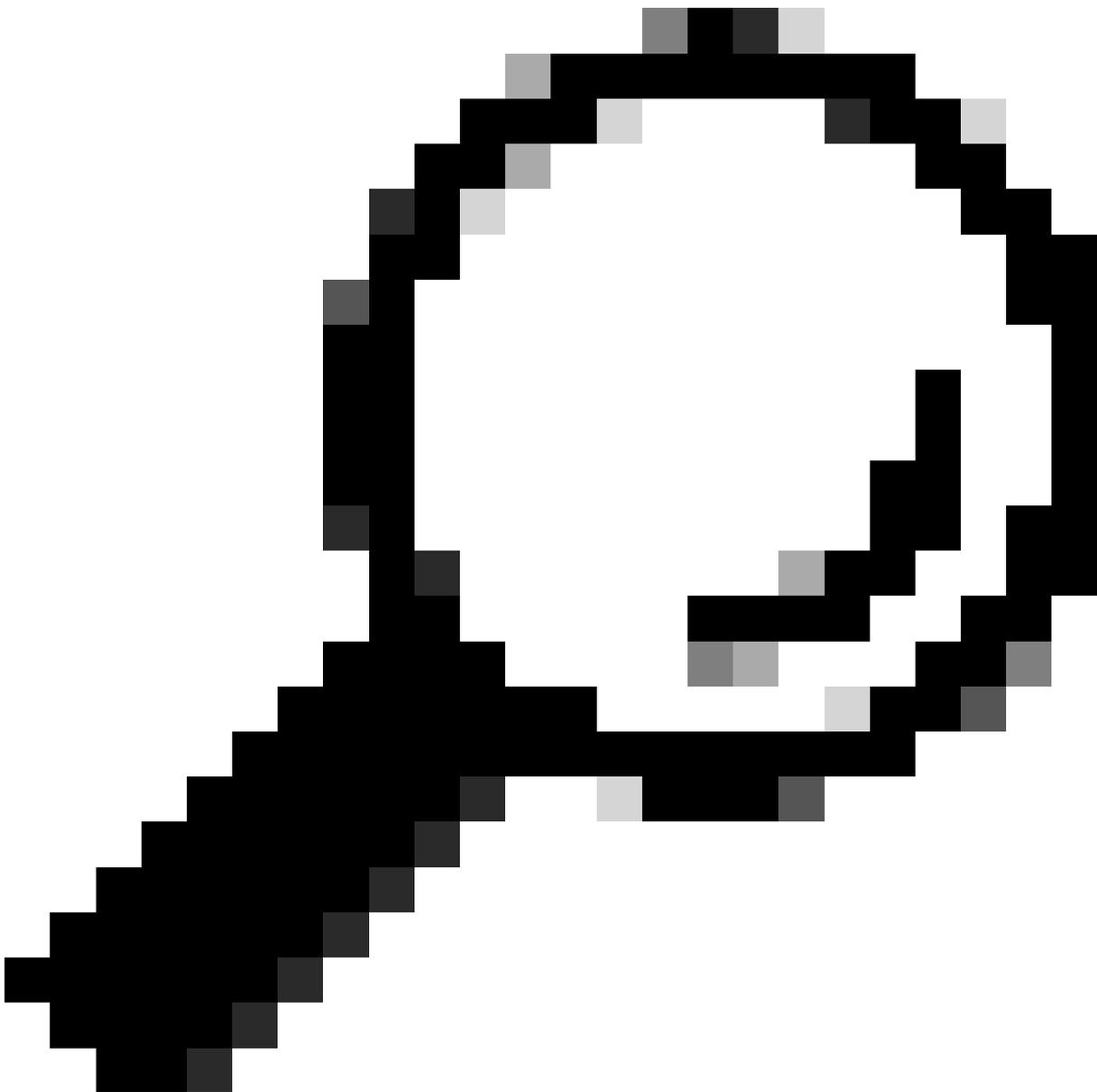
✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Show

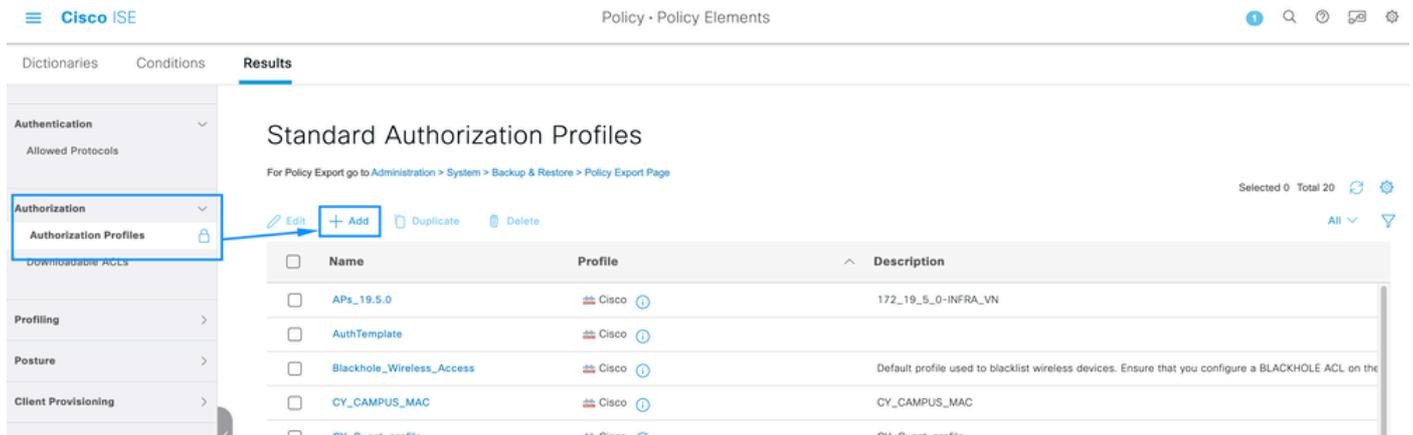


팁: 이 공유 암호는 나중에 필요하므로 다른 곳에 저장하십시오.

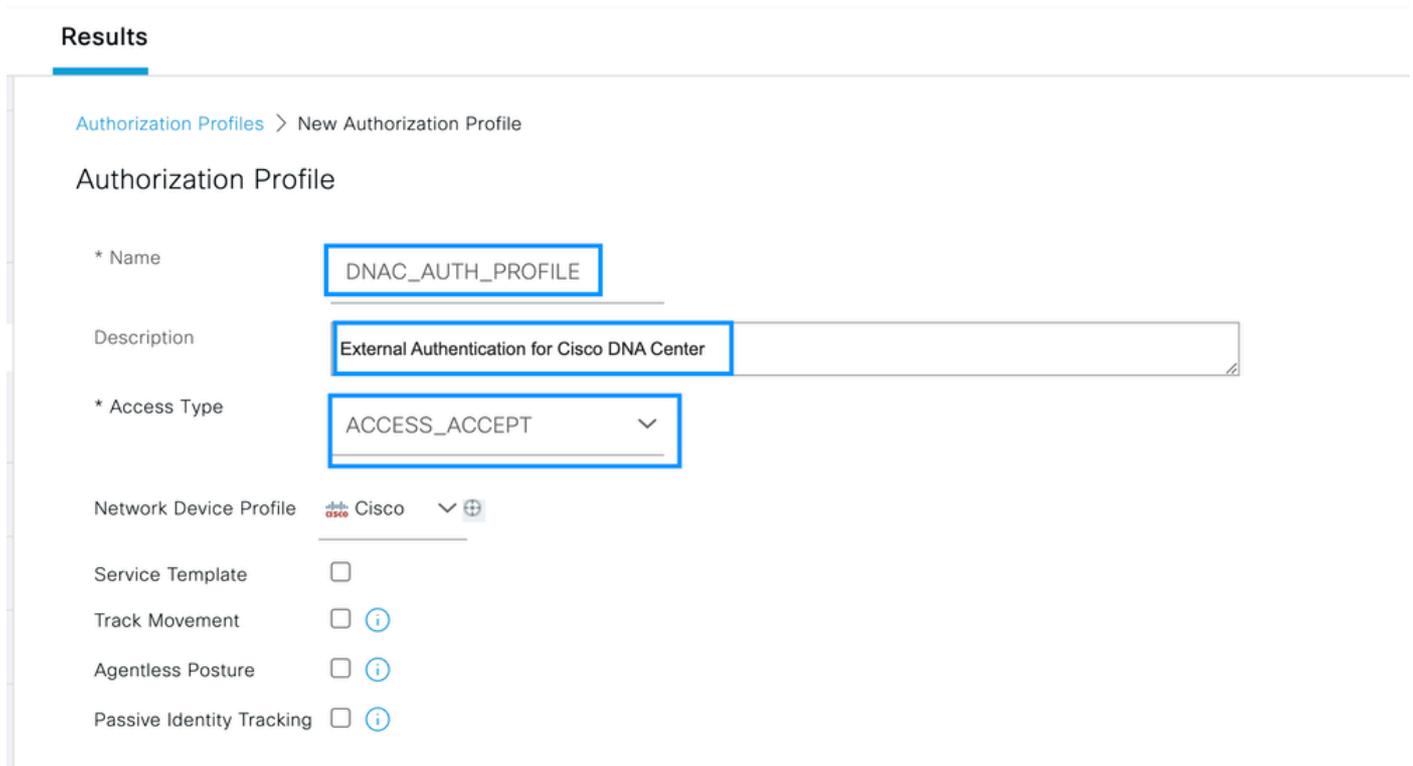
그런 다음 Submit(제출)을 클릭합니다.

3단계. ISE 서버에서 Policy(정책) > Policy Elements(정책 요소) > Results(결과)로 이동하여 권한 부여 프로필을 생성합니다.

Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일) 아래에 있는지 확인한 다음 Add(추가) 옵션을 선택합니다.



이름을 구성하고 설명을 추가하여 새 프로파일의 기록을 유지하고 액세스 유형이 ACCES_ACCEPT로 설정되었는지 확인합니다.



아래로 스크롤하여 Advanced Attributes Settings(고급 특성 설정)를 구성합니다.

왼쪽 열에서 cisco-av-pair 옵션을 검색하고 선택합니다.

오른쪽 열에 Role=SUPER-ADMIN-ROLE을 수동으로 입력합니다.

아래 이미지와 같으면 Submit(제출)을 클릭합니다.

Advanced Attributes Settings

☰ Cisco:cisco-av-pair = Role=SUPER-ADMIN-ROLE +

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = Role=SUPER-ADMIN-ROLE

4단계. ISE 서버에서 Work Centers(작업 센터) > Profiler(프로파일러) > Policy Sets(정책 집합)로 이동하여 인증 및 권한 부여 정책을 구성합니다.

기본 정책을 식별하고 파란색 화살표를 클릭하여 구성합니다.

The screenshot shows the Cisco ISE interface for configuring Policy Sets. The table below lists the available policy sets:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
⊗	Wire-dot1x		Wired_802.1X	internal_user	0	⚙️	➡️
⊗	MAB		Wired_MAB	Default Network Access	0	⚙️	➡️
✅	Default	Default policy set		Default Network Access	180517	⚙️	➡️

A blue box highlights the 'Default' policy set, and a blue arrow points to its 'View' button. The 'Save' button at the bottom right is also highlighted.

Default Policy Set(기본 정책 집합)에서 Authentication Policy(인증 정책)를 확장하고 Default(기본) 섹션에서 Options(옵션)를 확장하고 아래 컨피그레이션과 일치하는지 확인합니다.

Cisco ISE Work Centers - Profiler

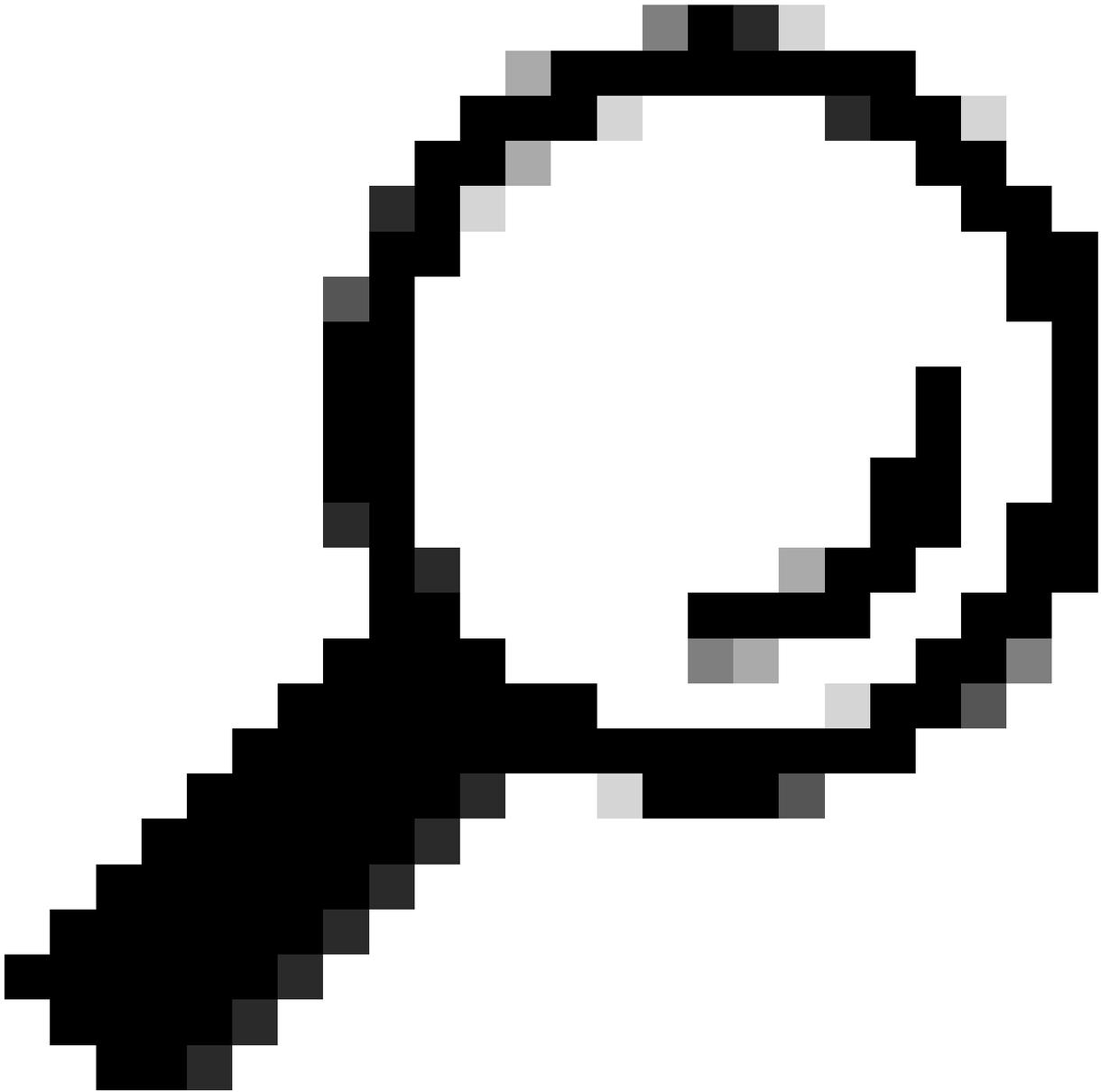
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	4556	⚙️
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙️
✓	Default		All_User_ID_Stores Options If Auth fail REJECT If User not found REJECT If Process fail DROP	62816	⚙️



팁: REJECT는 3가지 옵션에서도 사용할 수 있습니다.

Default Policy Set(기본 정책 집합) 내에서 Authorization Policy(권한 부여 정책)를 확장하고 Add(추가) 아이콘을 선택하여 새 권한 부여 조건을 생성합니다.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies **More**

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)
 > Authorization Policy - Local Exceptions
 > Authorization Policy - Global Exceptions
 ▾ Authorization Policy (25)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
⊕						

Rule Name(규칙 이름)을 구성하고 Add(추가) 아이콘을 클릭하여 Condition(조건)을 구성합니다.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies **More**

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)
 > Authorization Policy - Local Exceptions
 > Authorization Policy - Global Exceptions
 ▾ Authorization Policy (26)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
●	DNAC-SUPER-ADMIN-ROLE		Select from list	Select from list		

조건을 일부로 이를 2단계에서 구성한 네트워크 디바이스 IP 주소에 연결합니다.

Conditions Studio

Library

Search by Name



- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- CY_Campus
- CY_CAMPUS_MAC
- CY_Campus_voice
- CY_Guest
- EAP-MSCHAPv2
- ...

Editor

Network Access-Device IP Address

Equals 10.88.244.151

Set to 'Is not'

Duplicate Save

NEW | AND | OR

Close

Use

Save(저장)를 클릭합니다.

새 라이브러리 조건으로 저장하고 원하는 대로 이름을 지정합니다. 이 경우 이름이DNAC로 지정됩니다.



Save condition

Save as existing Library Condition (replaces current version and impact all policies that use this condition)

Select from list ▼

Save as a new Library Condition

DNAC

Description (optional)

Condition Description

Close

Save

마지막으로, 3단계에서 생성된 프로파일을 구성합니다.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617
> Authentication Policy (3) > Authorization Policy - Local Exceptions > Authorization Policy - Global Exceptions > Authorization Policy (25)					

Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
✓	DNAC-SUPER-ADMIN-ROLE	DNAC	DNAC_AUTH_PROFILE	Select from list			

Save(저장)를 클릭합니다.

5단계. Cisco DNA Center GUI에 로그인하고 System(시스템) > Users & Roles(사용자 및 역할) > External Authentication(외부 인증)으로 이동합니다.

Enable External User(외부 사용자 활성화) 옵션을 클릭하고 AAA Attribute(AAA 특성)를 Cisco-

AVPair로 설정합니다.

User Management

Role Based Access Control

External Authentication

External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user choo it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisc attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

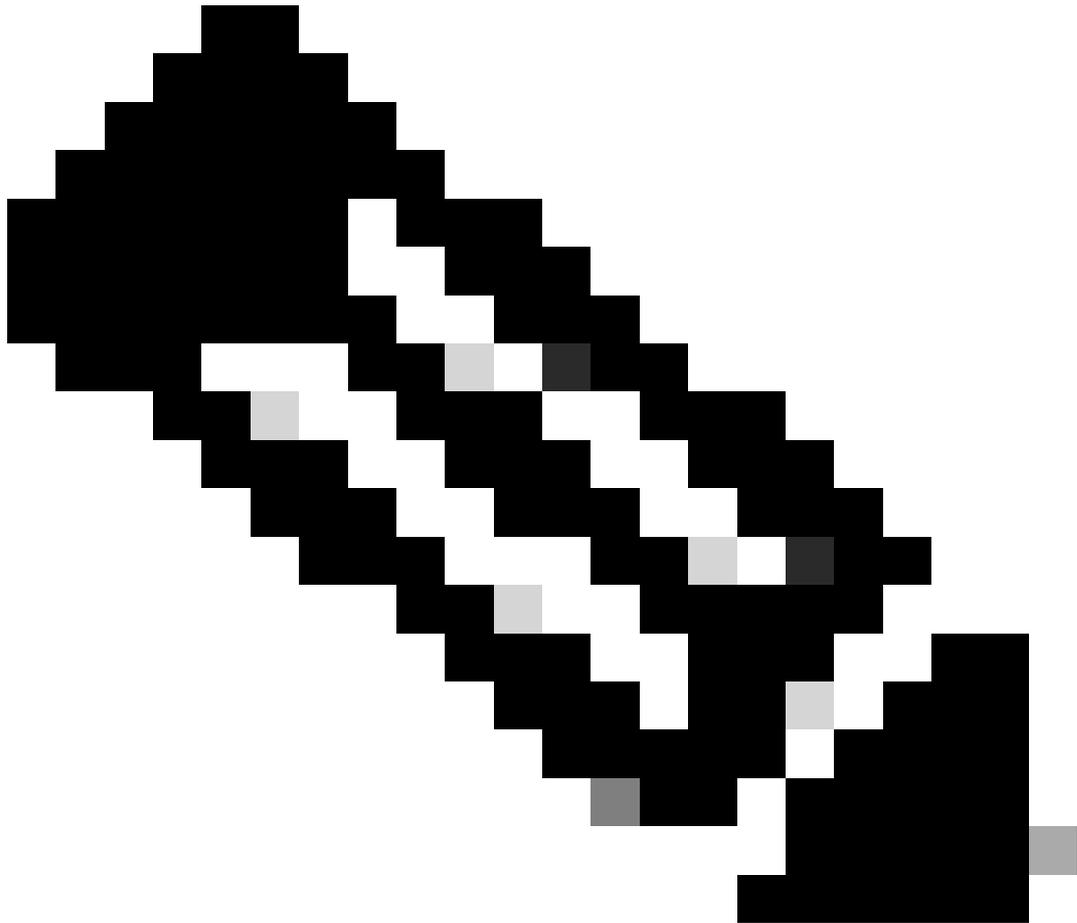
Enable External User ?

AAA Attribute

AAA Attribute
Cisco-AVPair

Reset to Default

Update



참고: ISE 서버는 백엔드에서 Cisco-AVPair 특성을 사용하므로 3단계의 컨피그레이션이 유효합니다.

아래로 스크롤하여 AAA Server(s) 컨피그레이션 섹션을 확인합니다. 1단계에서 ISE 서버의 IP 주소와 3단계에서 구성한 공유 암호를 구성합니다.

그런 다음 View Advanced Settings(고급 설정 보기)를 클릭합니다.

▼ AAA Server(s)

Primary AAA Server

IP Address

10.10.10.10



Shared Secret

SHOW

Info

View Advanced Settings

Update

Secondary AAA Server

IP Address

10.10.10.10



Shared Secret

SHOW

Info

View Advanced Settings

Update

RADIUS 옵션이 선택되어 있는지 확인하고 두 서버에서 Update(업데이트) 버튼을 클릭합니다.

▼ AAA Server(s)

Primary AAA Server

IP Address

██████████



Shared Secret

SHOW

Info

Hide Advanced Settings

RADIUS

TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

Timeout (seconds)

4

Secondary AAA Server

IP Address

██████████



Shared Secret

SHOW

Info

Hide Advanced Settings

RADIUS

TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

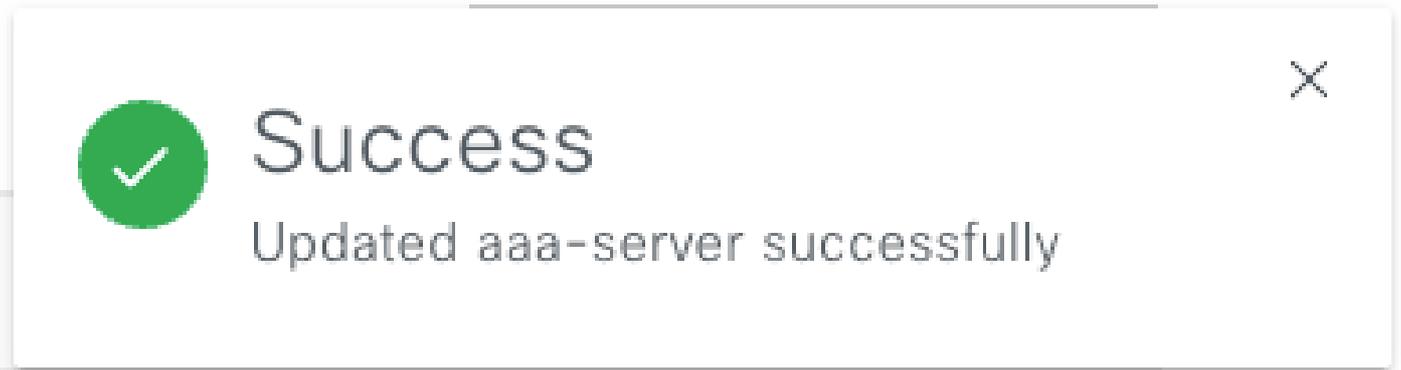
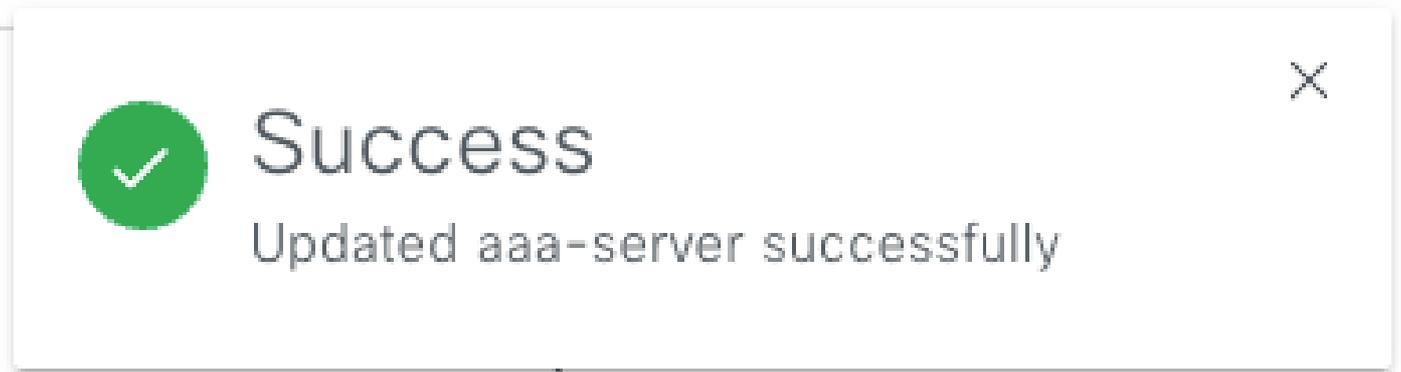
Timeout (seconds)

4

Update

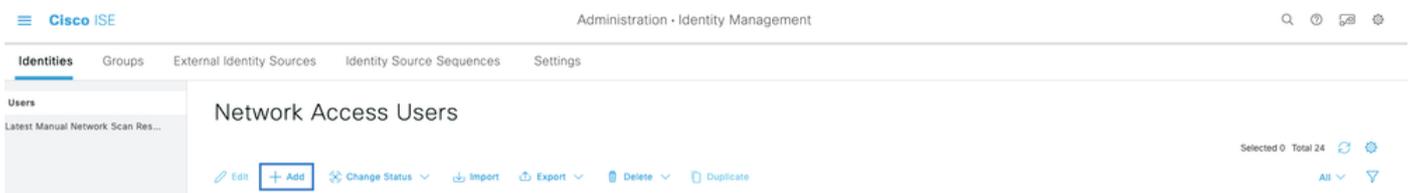
Update

각각에 대해 성공 메시지가 표시되어야 합니다.



이제 ISE 메뉴 > 관리 > ID 관리 > ID > 사용자 아래에서 생성한 ISE ID로 로그인할 수 있습니다.

생성된 항목이 없는 경우 ISE에 로그인하고 위 경로로 이동한 다음 새 네트워크 액세스 사용자를 추가합니다.



다음을 확인합니다.

Cisco DNA Center GUI 로드 ISE ID에서 사용자로 로그인합니다.



Cisco DNA Center

The bridge to possible

✓ Success!

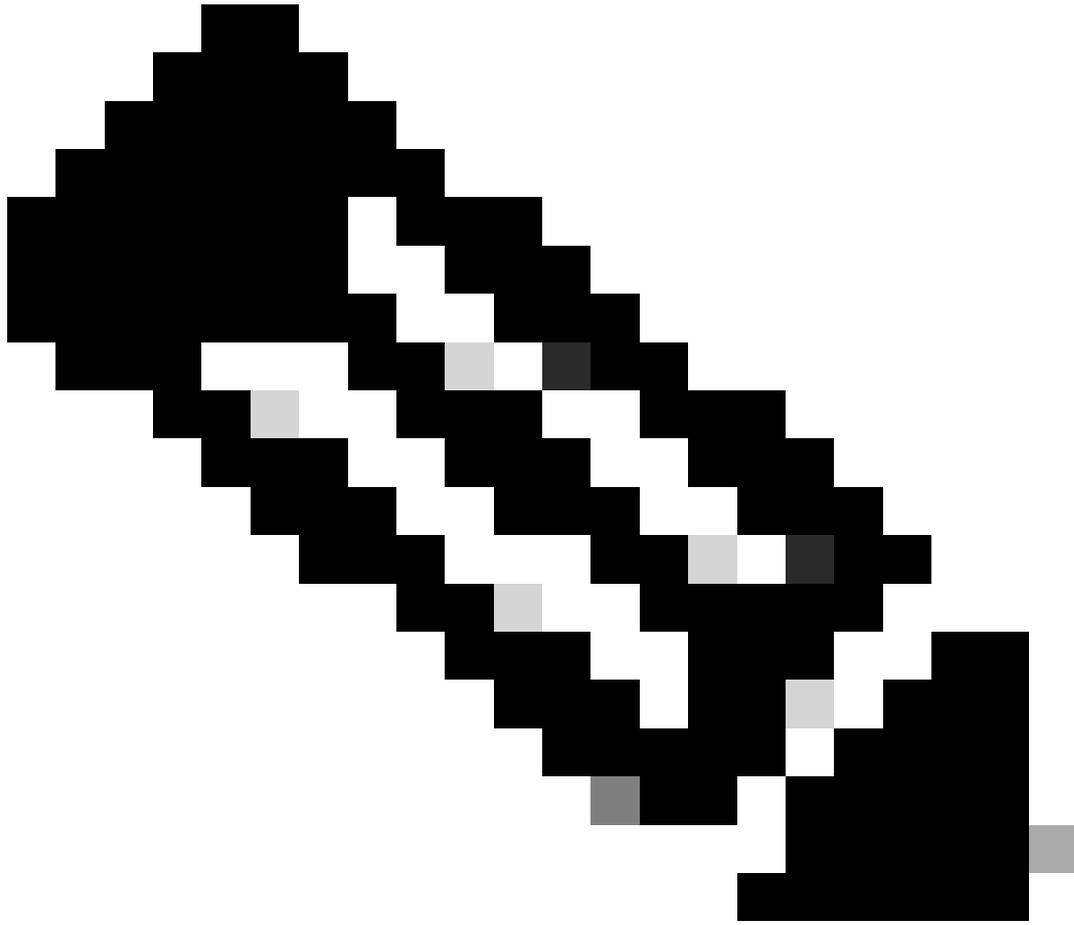
Username

test

Password

.....

Log In



참고: ISE ID의 모든 사용자가 지금 로그인할 수 있습니다. ISE 서버의 인증 규칙에 더 세분화된 정보를 추가할 수 있습니다.

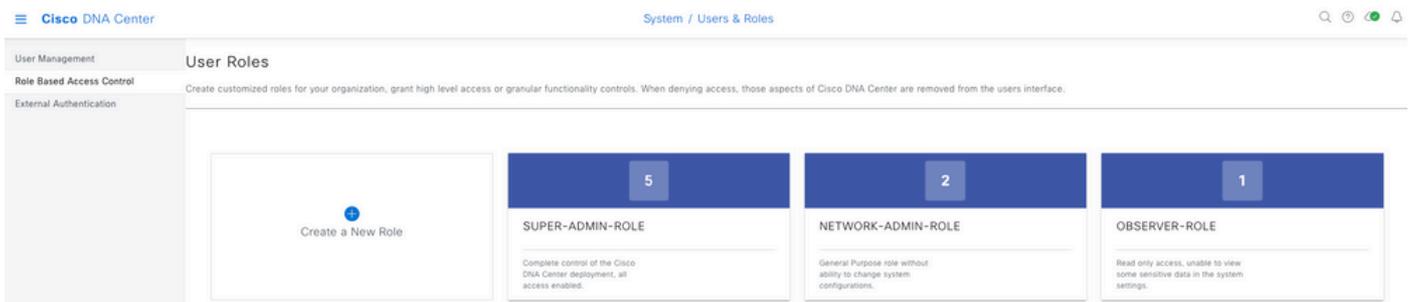
로그인 성공 후 Cisco DNA Center GUI에 사용자 이름이 표시됩니다

Welcome, test

시작 화면

추가 역할

Cisco DNA Center의 모든 역할에 대해 이러한 단계를 반복할 수 있습니다. 기본적으로 SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE 및 OBSERVER-ROLE이 있습니다.



이 문서에서는 SUPER-ADMIN-ROLE 역할 예를 사용하지만 Cisco DNA Center의 모든 역할에 대해 ISE에서 하나의 권한 부여 프로파일을 구성할 수 있습니다. 단, 3단계에서 구성된 역할이 Cisco DNA Center의 역할 이름과 정확히 일치해야 합니다(대/소문자 구분).

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.