

ISE를 사용하여 RA-VPNaaS 상태 평가를 위한 보안 액세스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[구성](#)

[보안 액세스 컨피그레이션](#)

[IP 풀에서 Radius 그룹 구성](#)

[ISE를 사용하도록 VPN 프로파일 구성](#)

[일반 설정](#)

[인증, 권한 부여 및 계정 관리\(AAA\)](#)

[트래픽 조정](#)

[Cisco Secure Client 컨피그레이션](#)

[ISE 컨피그레이션](#)

[네트워크 디바이스 목록 구성](#)

[그룹 구성](#)

[로컬 사용자 구성](#)

[정책 집합 구성](#)

[정책 집합 인증 및 권한 부여 구성](#)

[Radius 로컬 또는 Active Directory 사용자 구성](#)

[ISE Posture 구성](#)

[상태 조건 구성](#)

[상태 요구 사항 구성](#)

[상태 정책 구성](#)

[클라이언트 프로비저닝 구성](#)

[클라이언트 프로비저닝 정책 구성](#)

[권한 부여 프로파일 생성](#)

[상태 정책 집합 구성](#)

[다음을 확인합니다.](#)

[상태 검증](#)

[컴퓨터의 연결](#)

[ISE에서 로그를 수집하는 방법](#)

[규정 준수](#)

[비준수](#)

[보안 액세스 및 ISE 통합의 첫 단계](#)

[문제 해결](#)

[ISE Posture 디버그 로그를 다운로드하는 방법](#)

[보안 액세스 원격 액세스 로그를 확인하는 방법](#)

[보안 클라이언트에서 DART 번들 생성](#)

소개

이 문서에서는 ISE(Identity Service Engine) 및 보안 액세스를 통해 원격 액세스 VPN 사용자를 위한 상태 평가를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

- [사용자 프로비저닝 구성](#)
- 터널을 통해 보안 액세스에 연결된 Cisco ISE

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- [ISE\(Identity Service Engine\)](#)
- [보안 액세스](#)
- [Cisco 보안 클라이언트](#)
- ISE 상태
- 인증, 권한 부여 및 계정 관리(AAA)

사용되는 구성 요소

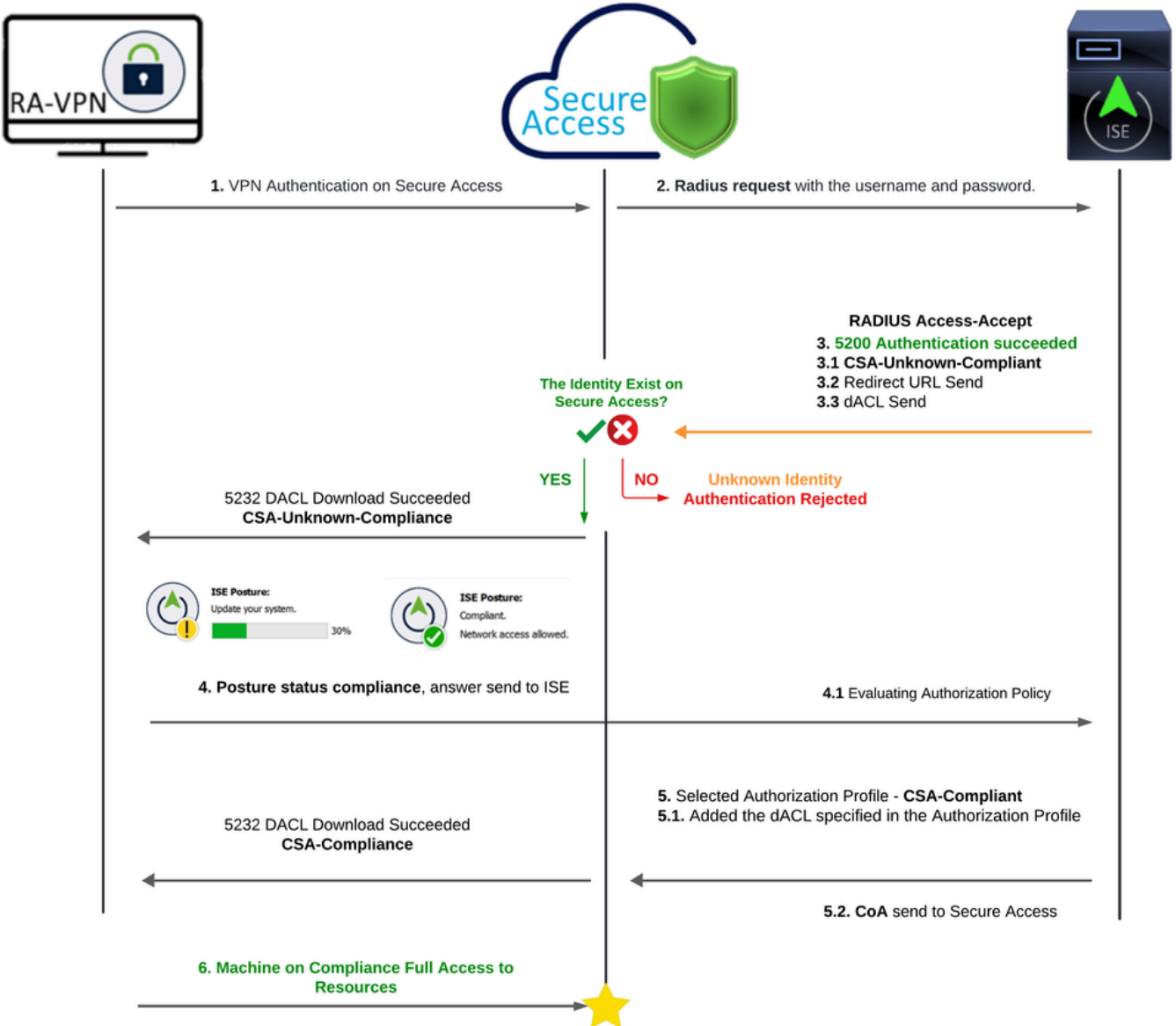
이 문서의 정보는 다음을 기반으로 합니다.

- ISE(Identity Service Engine) 버전 3.3 패치 1
- 보안 액세스
- Cisco Secure Client - Anyconnect VPN 버전 5.1.2.42

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.

배경 정보

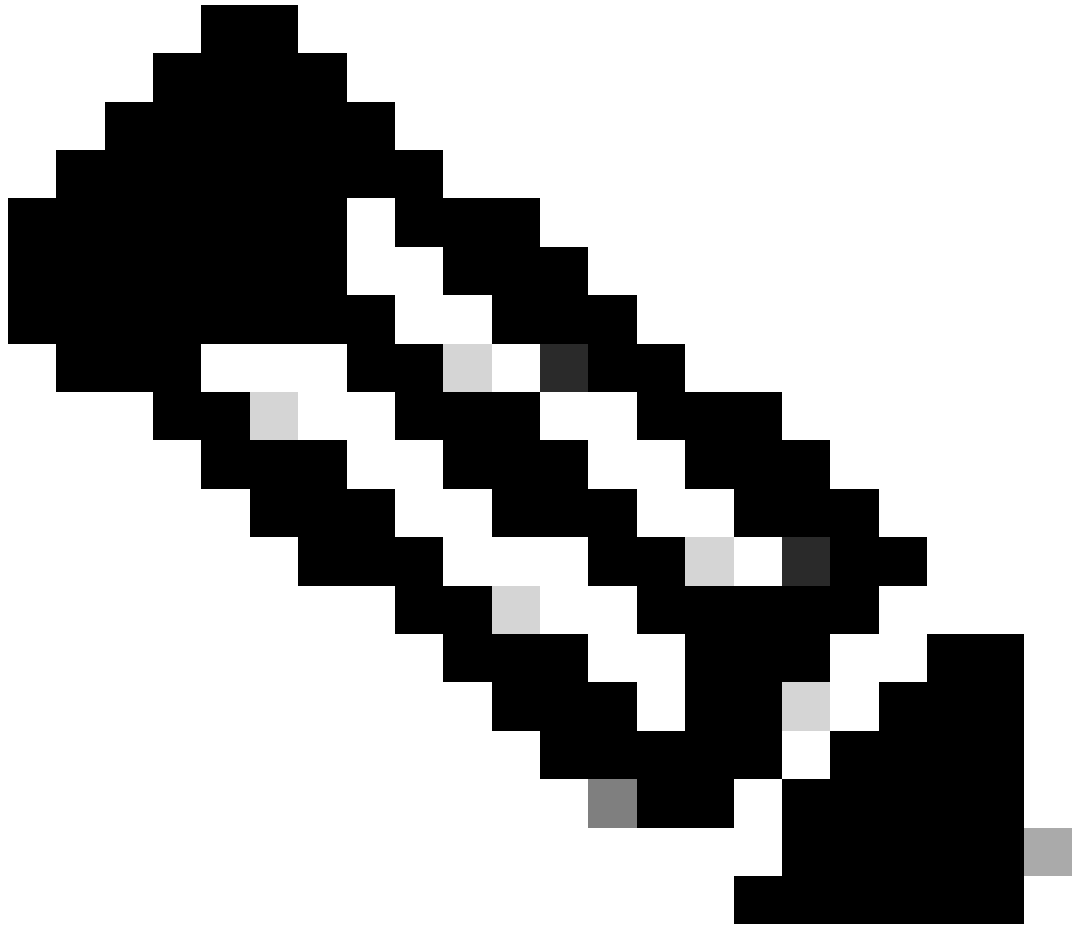
vpnuser@ciscosst.es



보안 액세스 - ISE - 다이어그램

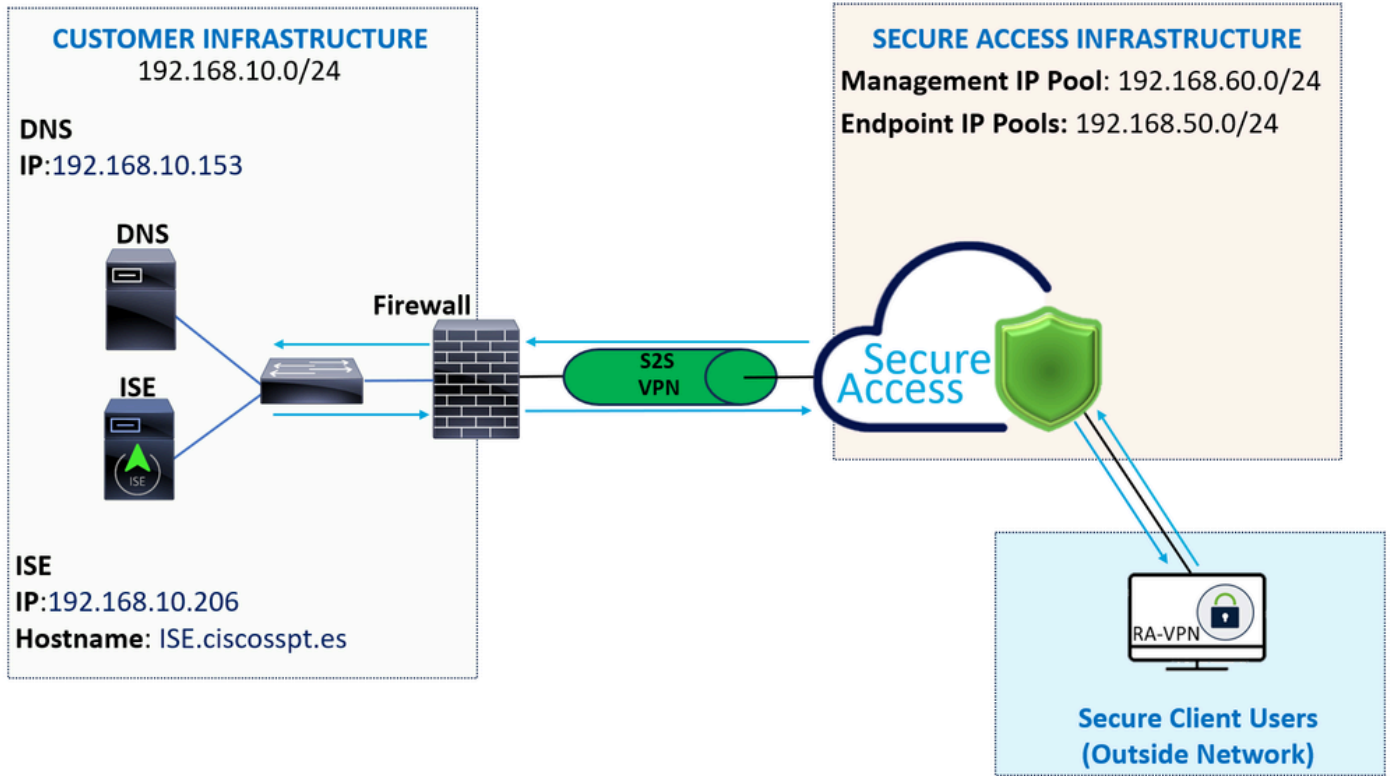
Cisco Secure Access를 ISE(Identity Services Engine)와 통합하면 MS-CHAPv2를 비롯한 다양한 인증 프로토콜을 활용하여 연결을 보호하는 포괄적인 보안 접근 방식이 제공됩니다. 고급 SSE(Security Service Edge) 솔루션을 갖춘 Cisco Secure Access는 ISE 기능을 사용하여 보호할 수 있는 VPNaaS(VPN as a Service) 기능을 제공하여 초분산 환경에서 보안 연결을 강화합니다.

이러한 통합을 통해 원활하고 안전한 액세스 환경을 제공하여 사용자가 어디서든 최적화된 성능과 보안을 통해 모든 애플리케이션에 연결할 수 있도록 합니다. Posture Assessment와 같은 Cisco ISE 고급 기능을 활용하면 액세스를 허용하기 전에 내부 사용자 정책에 대한 PC의 컴플라이언스를 평가함으로써 이 보안 모델을 더욱 강화합니다. 이렇게 하면 조직의 보안 요구 사항을 충족하는 장치만 네트워크 리소스에 액세스할 수 있으므로 취약성의 위험이 줄어듭니다.

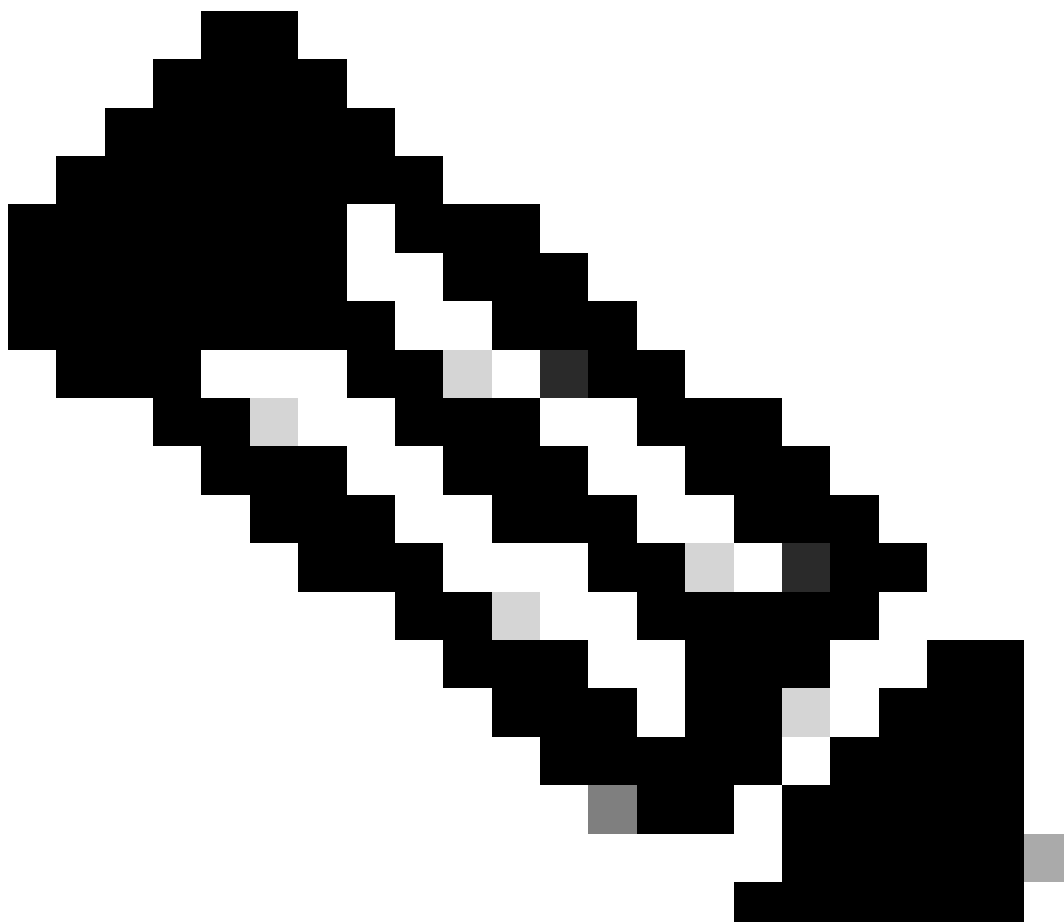


참고: RADIUS 통합을 구성하려면 두 플랫폼 간에 통신이 이루어졌는지 확인해야 합니다.

네트워크 다이어그램



구성



참고: 컨피그레이션 프로세스를 시작하기 전에 [Secure Access 및 ISE 통합의 첫 번째 단계를 완료해야 합니다.](#)

보안 액세스 컨피그레이션

IP 풀에서 Radius 그룹 구성

Radius를 사용하여 VPN 프로파일을 구성하려면 다음 단계를 진행합니다.

Secure [Access Dashboard](#)([보안 액세스 대시보드](#))로 이동합니다.



- **클릭** **Connect > Enduser Connectivity > Virtual Private Network**
- Pool Configuration(풀 컨피그레이션) **Manage IP Pools**아래에서Manage

Manage IP Pools

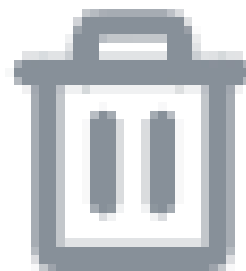
Manage

2 Regions mapped

- 를 IP Pool Region 선택하고 Radius Server

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	 

- 편집할 연필 클릭



- 이제 아래의 IP Pool(IP 풀) 섹션 configuration(컨피그레이션) 드롭다운 목록에서 **Radius Group (Optional)**
- 클릭 Add RADIUS Group

RADIUS Groups (optional)

Associate one RADIUS group per AAA method to this IP pool.



No RADIUS groups created

Add RADIUS Group

← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA ×

+ Add

#	Server Name	IP Address	
1	ISE_CSA	192.168.10.206	

통합의 이름 구성

- **AAA method**

- **Authentication:** 확인란을 선택하고 포트 **Authentication** 를 선택합니다(기본값: 1812).

- 인증에 확인란을 Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2) 표시해야 하는 경우

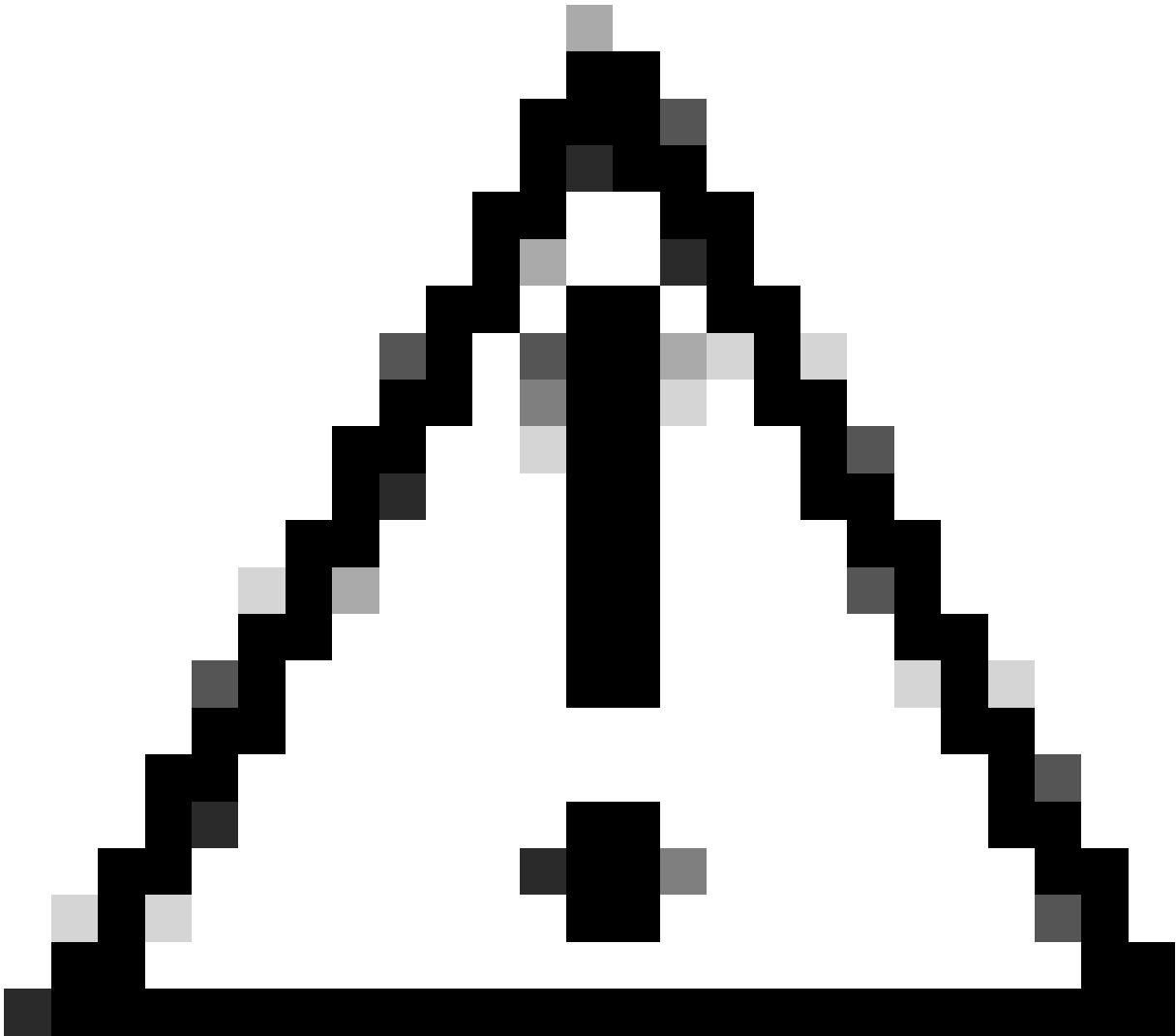
- **Authorization:** 확인란을 선택하고 Authorization 포트를 선택합니다(기본값: 1812).

- ISE에서 상태 및 **Authorization mode Only Change of Authorization (CoA) mode** 변경을 허용하려면 및의 확인란을 선택합니다

- **Accounting:** Authorization(권한 부여) 확인란을 선택하고 기본적으로 포트를 1813으로 선택합니다.

- 선택 **Single or Simultaneous** (단일 모드에서는 어카운팅 데이터가 하나의 서버로만 전송됩니다. 동시 모드에서는 그룹의 모든 서버에 대한 어카운팅 데이터)

- RADIUS interim- **Accounting update** accounting-update 메시지의 주기적인 생성을 활성화하려면 의 확인란을 선택합니다.



주의: Authentication 및 Authorization 메서드 모두 동일한 포트를 사용해야 합니다.

-
- 그런 다음 섹션에서 AAA를 통해 인증하는 데 사용되는 **RADIUS Servers (ISE)**를 구성해야 **RADIUS Servers**합니다.
 - 클릭 + Add

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

+ Add

#	Server Name	IP Address
---	-------------	------------

- 그런 다음 다음 옵션을 구성합니다.

Add RADIUS Server

Server name

IP Address

Password type

Secret Key

Show

Password

Show

Cancel

Save & Add server

Save

- **Server Name:** ISE 서버를 식별하기 위한 이름을 구성합니다.
 - **IP Address:** 보안 액세스를 통해 연결 할 수 있는 Cisco ISE 장치의 IP를 설정 한다
 - **Secret Key:** RADIUS 비밀 키 구성
 - **Password:** Radius 비밀번호를 구성합니다.
- 을 **Save** 클릭하고 옵션 아래에서 Radius 서버를 Assign Server 할당한 다음 ISE 서버를 선택합니다.

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

^

ISE_CSA

[+ Add](#)

- 완료된 모든 컨피그레이션을 저장하려면 **Save** 다시 클릭합니다.

← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA ×

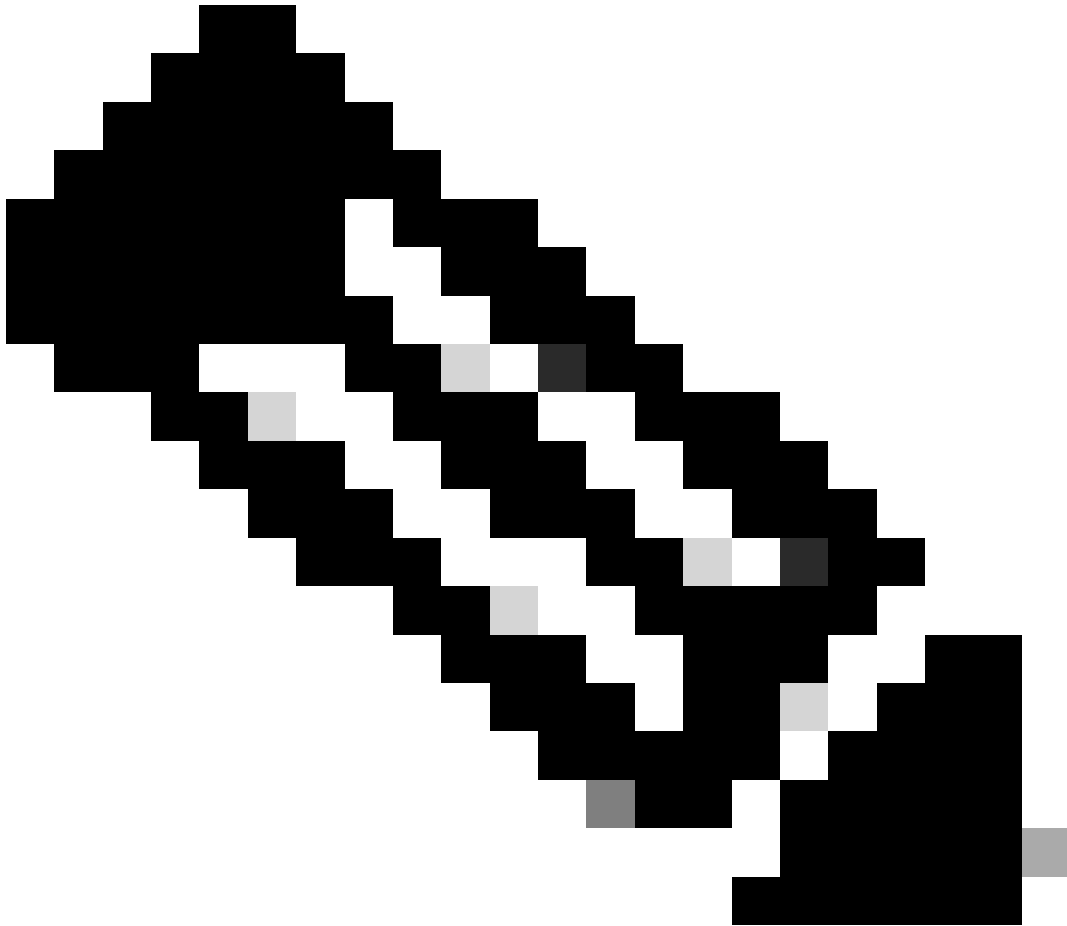
+ Add

#	Server Name	IP Address	
1	ISE_CSA	192.168.10.206	

◦ **Protocols: 선택 Radius**

• **Map authentication groups to regions: 지역을 선택하고 Radius Groups**

• **클릭 Next**



참고: 여러 영역이 있는 경우 모든 영역을 선택하고 반지름 그룹을 선택해야 합니다. 이렇게 하지 않으면 단추가 **Next** 회색으로 표시됩니다.

모든 인증 부품을 구성한 후 권한 부여를 진행하십시오.

Authorization(권한 부여)

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication **Authorization** Accounting

Enable Radius Authorization
Use defaults or customize groups to map to regions

Select one group for all regions + Group

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)

< Cancel Back Next

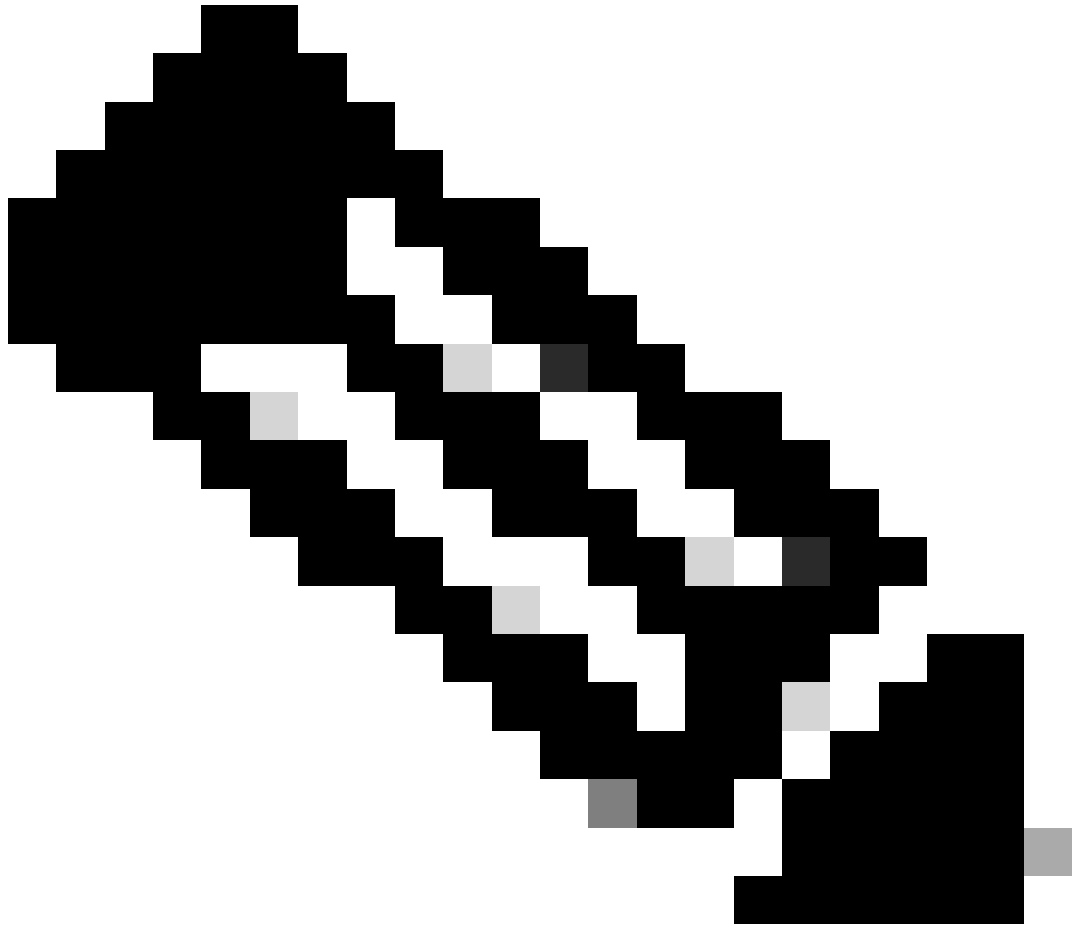
- **Authorization**

- **Enable Radius Authorization:** radius Authorization(radius 권한 부여)을 활성화하려면 확인란을 선택합니다.

- **모든 영역에 대해 그룹 하나 선택:** 모든 원격 액세스 - RA-VPN(Virtual Private Network) 풀에 대해 하나의 특정 RADIUS 서버를 사용하도록 확인란을 선택하거나 각 풀에 대해 개별적으로 정의합니다

- **클릭 Next**

모든 부품을 구성한 **Authorization** 후 를 계속 진행하십시오 **Accounting**.



참고: 활성화하지 않으면 포스터 **Radio Authorization**가 작동하지 않습니다.

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication Authorization Accounting

Enable Radius Accounting
Use defaults or customize groups to map to regions

Select one group for all regions + Group

ISE_CSA ▼

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA ▼
RA VPN 1	192.168.60.0/24	ISE_CSA (default) ▼



Cancel

Back

Next

- **Accounting**
 - **Map Authorization groups to regions:** 지역을 선택하고 **Radius Groups**

- 클릭 Next

After you have done configured the Authentication, Authorization and Accounting 을(를) 계속하십시오Traffic Steering.

트래픽 조정

트래픽 조정에서 Secure Access를 통한 통신 유형을 구성해야 합니다.

Tunnel Mode

Connect to Secure Access

All traffic is steered through the tunnel.



Tunnel Mode

Bypass Secure Access

All traffic is steered outside the tunnel.



- 선택하는 경우 **Connect to Secure Access** 모든 인터넷 트래픽이 **Secure Access**

Connect to Secure Access

All traffic is steered through the tunnel.



Add Exceptions

Destinations specified here will be steered OUTSIDE the tunnel.

+ Add

Destinations

Exclude Destinations

Actions

proxy-
 8195126.zpc.sse.cisco.com,
 ztna.sse.cisco.com,acme.sse.
 cisco.com,devices.api.umbrell
 a.com,sseposture-routing-
 commercial.k8s.5c10.org,sse
 posture-routing-
 commercial.posture.duosecuri
 ty.com,data.eb.thousandeyes.

-

-

Cancel

Back

Next

인터넷 도메인 또는 IP에 대한 제외를 추가하려면 버튼을 클릭한 다음 + Add 을 클릭하십시오Next.

- 모든 인터넷 트래픽 **Bypass Secure Access**은 인터넷 보호가 아닌 Secure Access 인터넷 공급자를 통해 전달됩니다

Tunnel Mode

Bypass Secure Access ▼

All traffic is steered outside the tunnel.



Add Exceptions

Destinations specified here will be steered **INSIDE** the tunnel.

[+ Add](#)

Destinations

Exclude Destinations

Actions

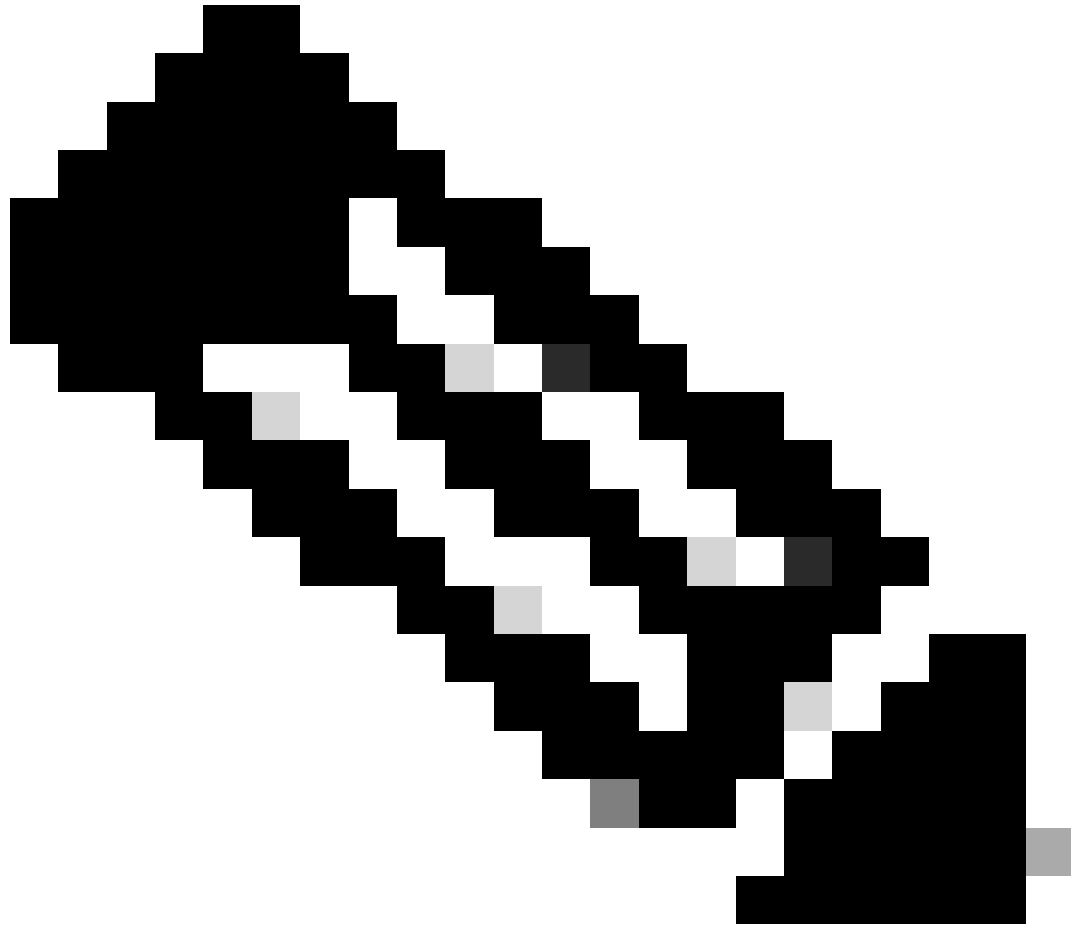


No matches found

[Cancel](#)

[Back](#)

[Next](#)



참고: ISE Postureenroll.cisco.com 를 선택할 때 추가하십시오 **Bypass Secure Access.**

이 단계에서는 VPN을 통해 액세스하려는 모든 프라이빗 네트워크 리소스를 선택합니다. 이렇게 하려면 을 클릭한 + **Add** 다음 모든 리소스를 추가한 **Next** 경우 을 클릭합니다.

Cisco Secure Client 컨피그레이션

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings **3** Client Settings **13** Client Certificate Settings **2** [Download XML](#)

Banner Message
Require user to accept a banner message post authentication

Session Timeout
 days

Session Timeout Alert
 minutes before

Maximum Transmission Unit ⓘ

[Cancel](#) [Back](#) [Save](#)

이 단계에서는 모든 항목을 기본값으로 유지하고 **Save**를 클릭할 수 있지만, 컨피그레이션을 더 사용자 지정하려면 [Cisco Secure Client Administrator Guide](#)를 확인하십시오.

ISE 컨피그레이션

네트워크 디바이스 목록 구성


Cisco ISE를 통해 인증을 구성하려면 Cisco ISE에 쿼리할 수 있는 허용된 디바이스를 구성해야 합니다.

- 탐색 **Administration > Network Devices**
- 클릭 + **Add**

Network Devices

Name CSA

Description _____

IP Address * IP : 192.168.60.0 / 24 


Device Profile  Cisco 

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret [Show](#)

Use Second Shared Secret 

Second Shared Secret _____ [Show](#)

CoA Port 1700 [Set To Default](#)

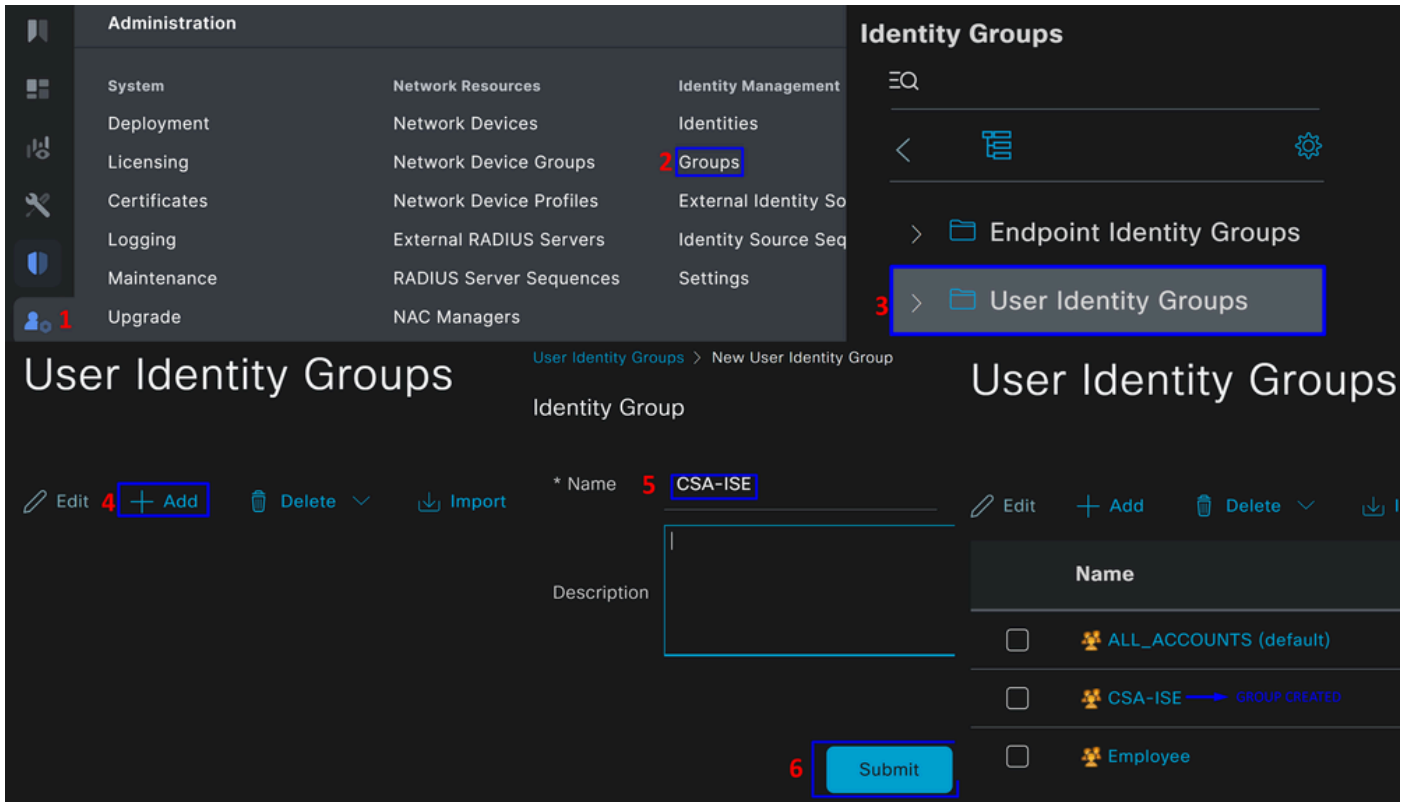
- **Name:** 이름을 사용하여 보안 액세스 식별
- **IP Address:** [IP 풀](#) Management Interface 영역 단계의 [를 구성합니다.](#)
- **Device Profile:** Cisco 선택
 - **Radius Authentication Settings**
 - Shared Secret: 비밀키 단계에서 구성한 것과 동일한 공유 [비밀 구성](#)
 - **CoA Port:** 기본값으로 듭니다. 1700은 Secure Access에서도 사용됩니다.

그런 다음 을 **Save**클릭하여 통합이 제대로 작동하는지 확인하려면 통합 확인을 위한 로컬 사용자 만들기를 진행합니다.

그룹 구성

로컬 사용자와 함께 사용하도록 그룹을 구성하려면 다음 단계를 진행합니다.

- 클릭 **Administration > Groups**
- 클릭 **User Identity Groups**
- 클릭 + Add
- 그룹에 Name대한 을 생성하고 **Submit**



로컬 사용자 구성

로컬 사용자가 통합을 확인하도록 구성하려면

- 탐색 **Administration > Identities**
- 클릭 **Add +**

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Passwords

Password Type: ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

	Password	Re-Enter Password	
* Login	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ
Enable	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ

▼ User Groups

⋮
CSA-ISE ▼
🗑️
+

- **Username:** Secure Access에서 알려진 UPN 프로비저닝을 사용하여 사용자 이름을 구성합니다. 이 단계는 사전 요구 사항 단계를 기반으로 [합니다](#).
- **Status:** 활성
- **Password Lifetime:** 사용자 **With Expiration** 에 따라 구성할 수도 Never Expires 있고
- **Login Password:** 사용자에게 대한 비밀번호를 생성합니다.
- **User Groups:** Configure a Group(그룹 구성) 단계에서 생성된 [그룹을 선택합니다](#).

참고: UPN 기반 인증은 Secure Access의 향후 버전에서 변경되도록 설정됩니다.

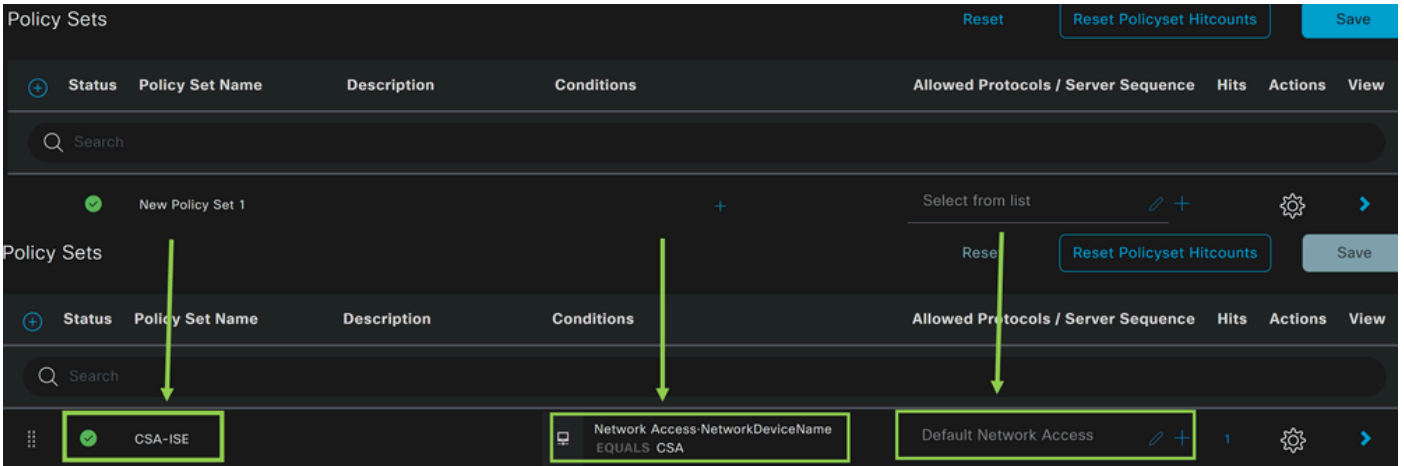
그런 다음 컨피그레이션 **Save** 을 수행하고 단계를 계속할 수 있습니다 **Configure Policy Set**.

정책 집합 구성

정책 집합에서 인증 및 권한 부여 중에 ISE가 수행하는 작업을 구성합니다. 이 시나리오에서는 사용자 액세스를 제공하기 위해 간단한 정책을 구성하는 활용 사례를 보여줍니다. 먼저 ISE는 RADIUS 인증의 출처를 확인하고 액세스를 제공하기 위해 ISE 사용자 데이터베이스에 ID가 있는지 확인합니다

해당 정책을 구성하려면 Cisco ISE 대시보드로 이동합니다.

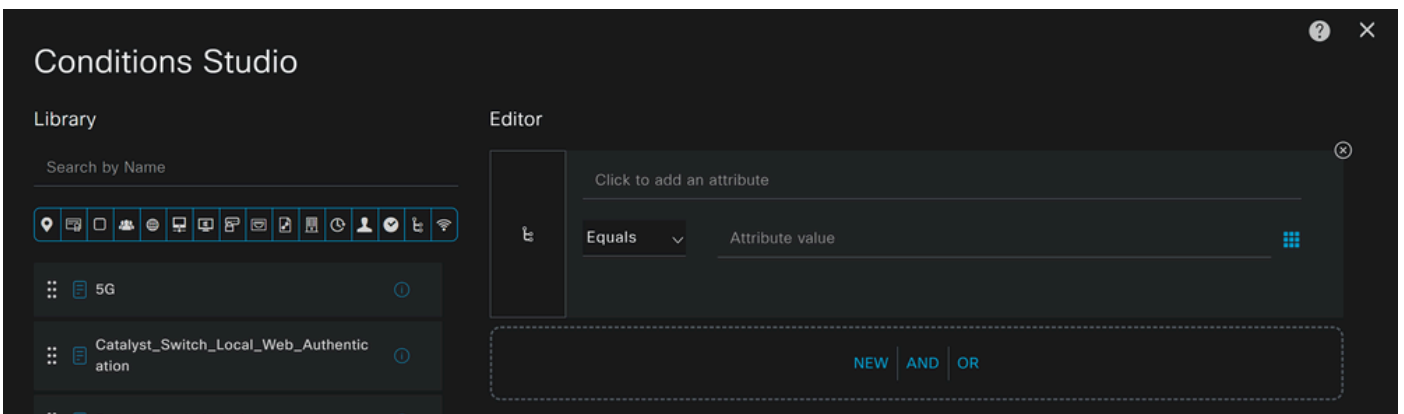
- 클릭 Policy > Policy Sets
- 새 정책 세트+ 를 추가하려면 클릭



이 경우 기본 정책 집합에서 작업하는 대신 새 정책 집합을 생성합니다. 그런 다음 해당 정책 집합에 따라 인증 및 권한 부여를 구성합니다. 구성된 정책은 [네트워크 디바이스 목록 구성 단계](#)에 정의된 네트워크 디바이스에 대한 액세스를 허용하여 이러한 인증이 [다음](#)과 같이 정책으로 CSA Network Device List 들어오는지 확인할 수 **Conditions** 있습니다. 마지막으로 허용되는 프로토콜도 **Default Network Access** 있습니다.

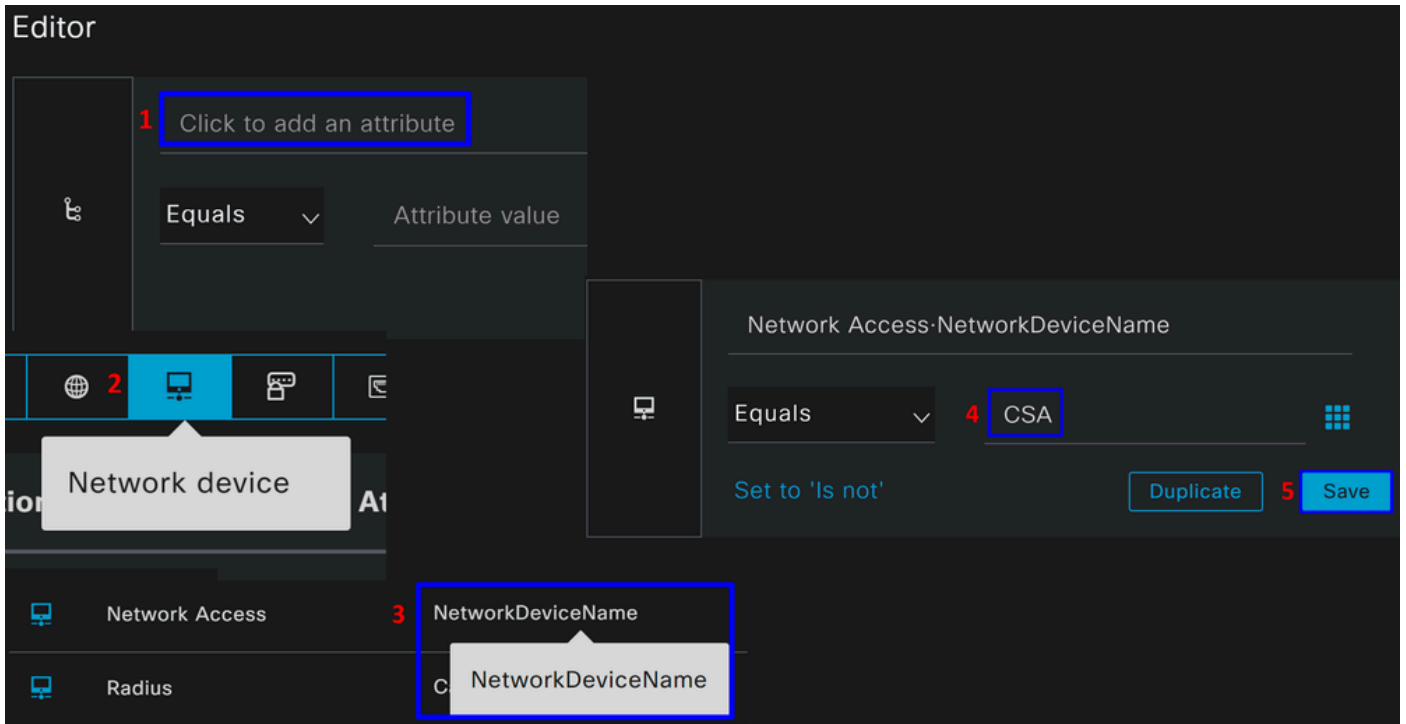
정책 집합과 일치하는 **condition** 을 생성하려면 다음 지침을 진행합니다.

- 클릭 +
- 에서 **Condition Studio** 제공되는 정보는 다음과 같습니다.



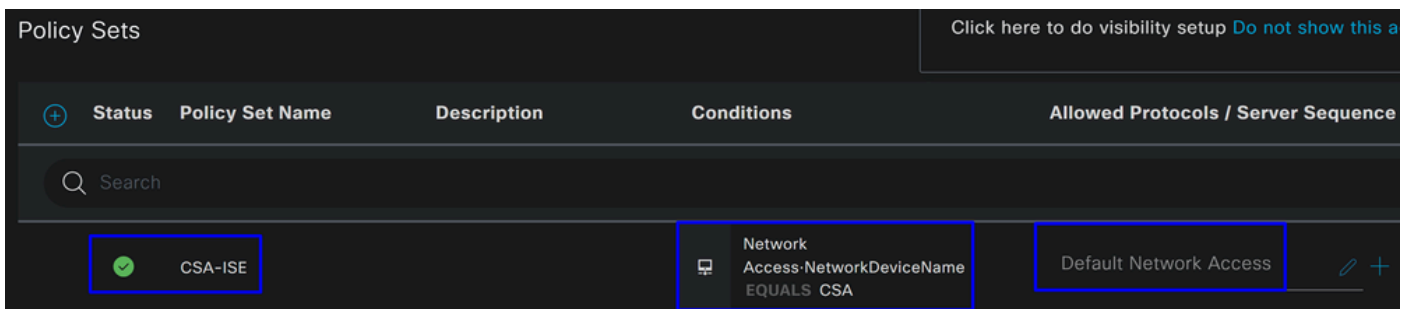
- 조건을 생성하려면 다음을 클릭합니다. Click to add an attribute
- 버튼을 **Network Device** 클릭합니다
- 뒤의 옵션에서 **Network Access** - 옵션을 **Network Device Name** 클릭합니다

- Equals(같음) 옵션에서 [네트워크 디바이스 목록 구성](#) Network Device 단계에 의 이름을 기록합니다
- 클릭 Save
CSA

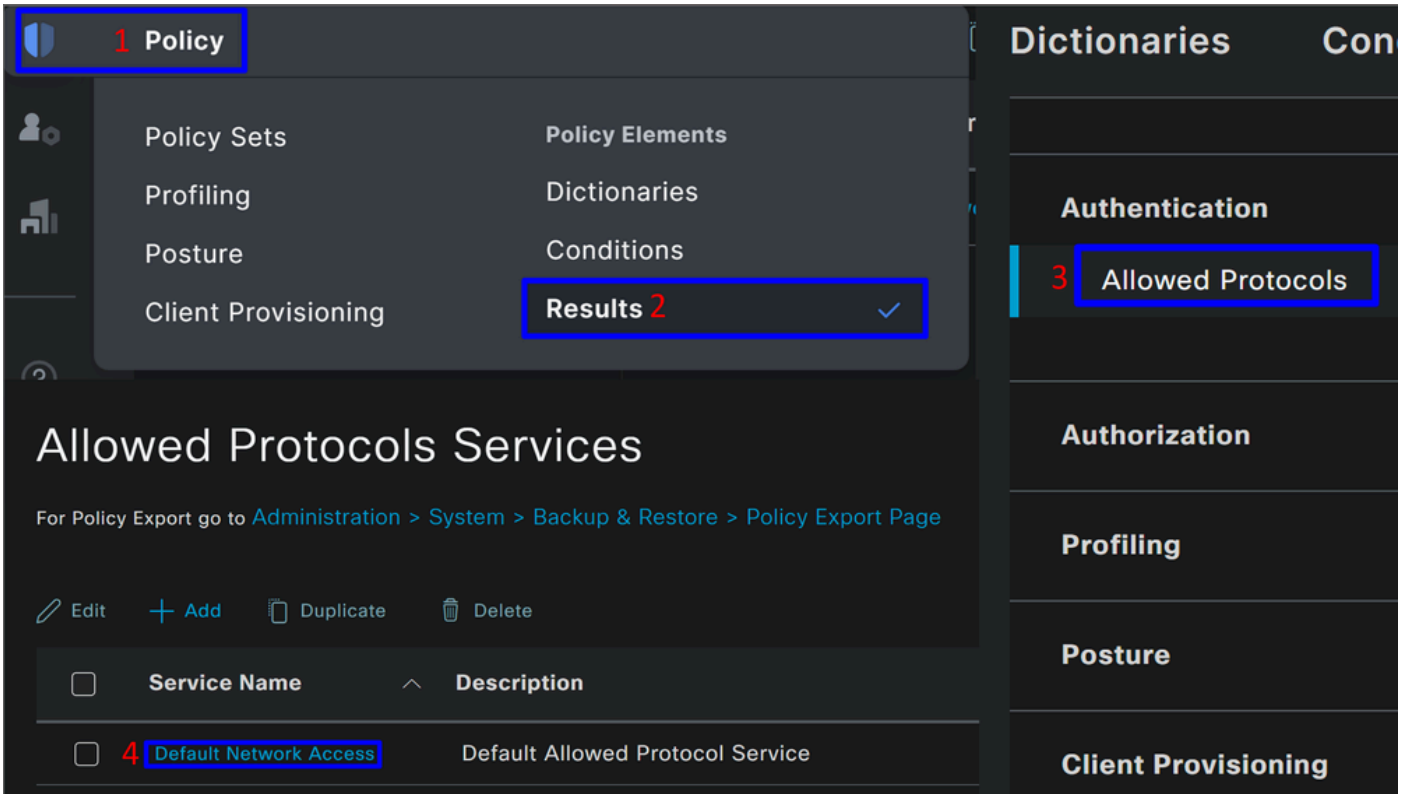


이 정책은 정책 세트에서 **Authentication** 및 **Authorization** 설정을 계속하기 위한 소스의 요청만 **CSA-ISE**을 승인하며, 허용되는 프로토콜에 **Default Network Access** 대해 를 기반으로 허용된 프로토콜도 확인합니다.

정의된 정책의 결과는 다음과 같아야 합니다.



- 허용되는 을 **Default Network Access Protocols** 확인하려면 다음 지침을 진행합니다.
 - 클릭 Policy > Results
 - 클릭 **Allowed Protocols**
 - 클릭 **Default Network Access**

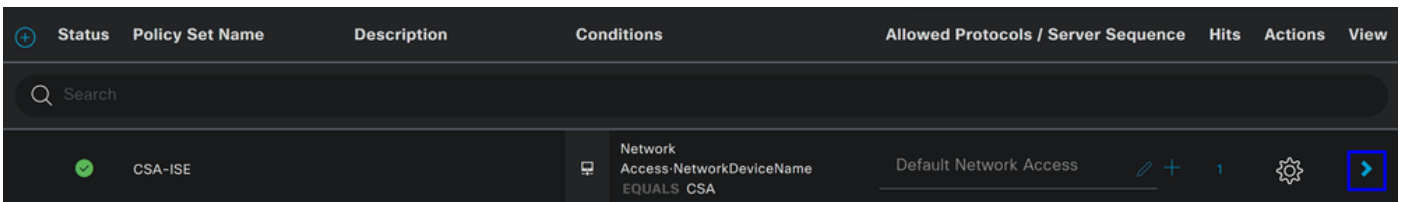


- 그런 다음, Firepower Threat Defense에서 **Default Network Access**

정책 집합 인증 및 권한 부여 구성

에서 Authentication 및 **Authorization** 정책을 생성하려면 **Policy Set** 다음 단계를 진행합니다.

- 클릭 >



- 그런 다음 및 정책이 Authentication **Authorization** 표시됩니다.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
🟢	CSA-ISE		Network Access:NetworkDeviceName EQUALS CSA	Default Network Access
> Authentication Policy(2)				
> Authorization Policy - Local Exceptions				
> Authorization Policy - Global Exceptions				
> Authorization Policy(2)				

인증 정책

인증 정책의 경우 여러 가지 방법으로 구성할 수 있습니다. 이 경우, [네트워크 디바이스 목록 구성 단계](#)에서 정의된 디바이스에 대한 정책을 확인하고 특정 기준에 따라 인증을 확인합니다.

- 를 통해 인증된 사용자 **Network Device CSA** 는 인증에 성공했거나 거부되었습니다.

Authentication Policy(2)				
+ Status	Rule Name	Conditions	Use	
🟢	Authentication Secure Access	Network Access:NetworkDeviceName EQUALS CSA	Internal Users	Options

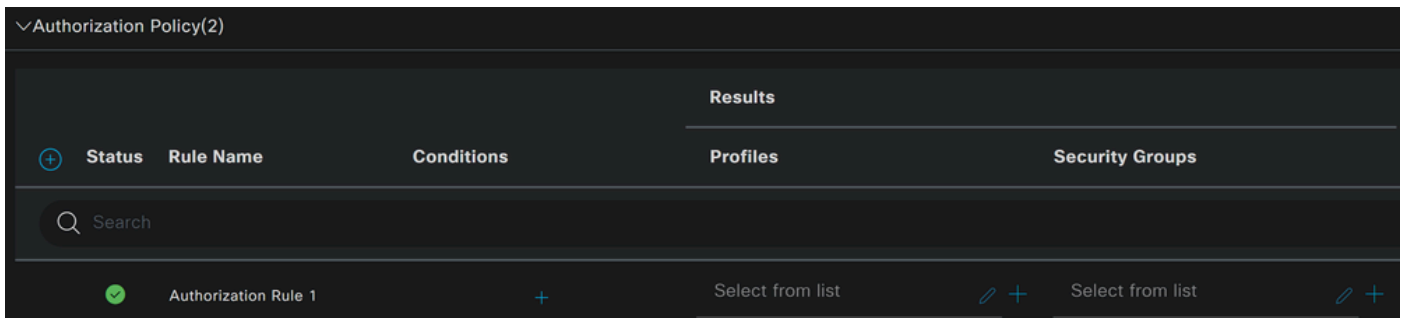
정책은 Configure Policy [Set](#)(정책 집합 구성) 단계에 정의된 [것과 동일합니다](#).

권한 부여 정책

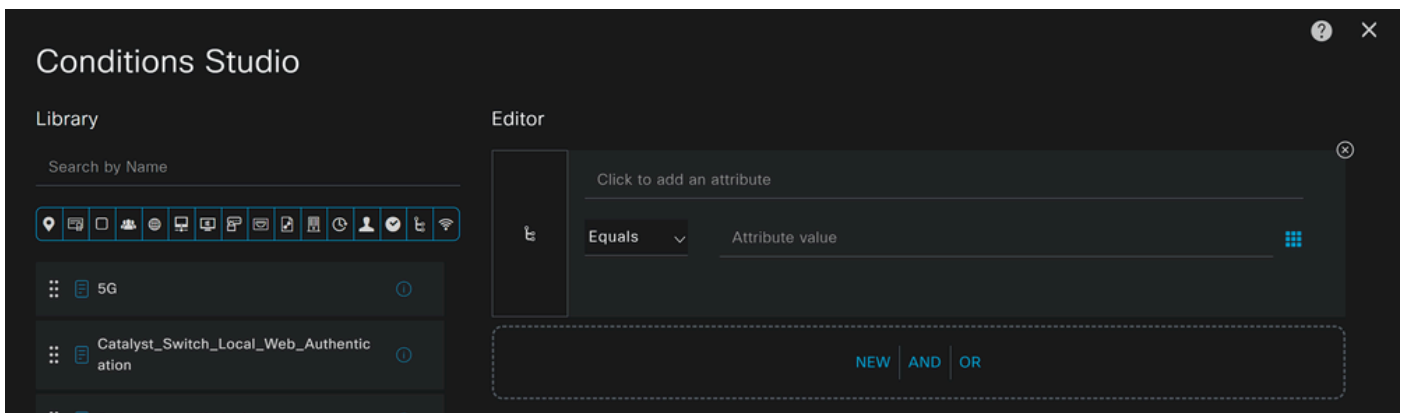
여러 가지 방법으로 권한 부여 정책을 구성할 수 있습니다. 이 경우 그룹 구성 단계에 정의된 그룹의 사용자만 권한을 부여합니다. 권한 부여 정책을 구성하려면 다음 예를 참조하십시오.

Authorization Policy(2)				
+ Status	Rule Name	Conditions	Profiles	Security Groups
🟢	Authorization Rule 1		Select from list	Select from list
🟢	Authorization Secure Access	InternalUser:IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list

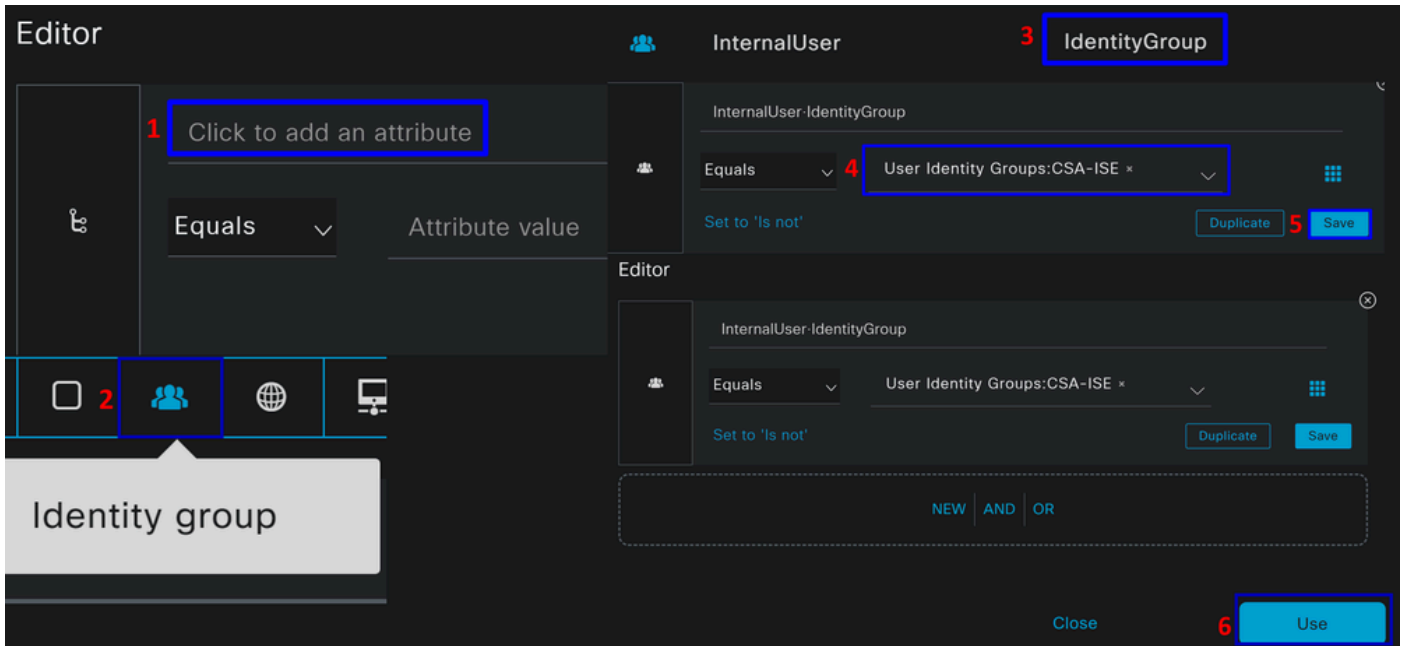
- 클릭 **Authorization Policy**
- 다음과 같이 권한 부여+ 를 위한 정책을 정의 하려면 클릭 합니다.



- 다음 단계로 Rule Name, Conditions 및 Profiles
- 권한 부여 정책을 쉽게 Name 식별하기 위해 를 구성하는 경우
- 을(를) **Condition**구성하려면 +
- 에서 **Condition Studio**다음 정보를 찾을 수 있습니다.

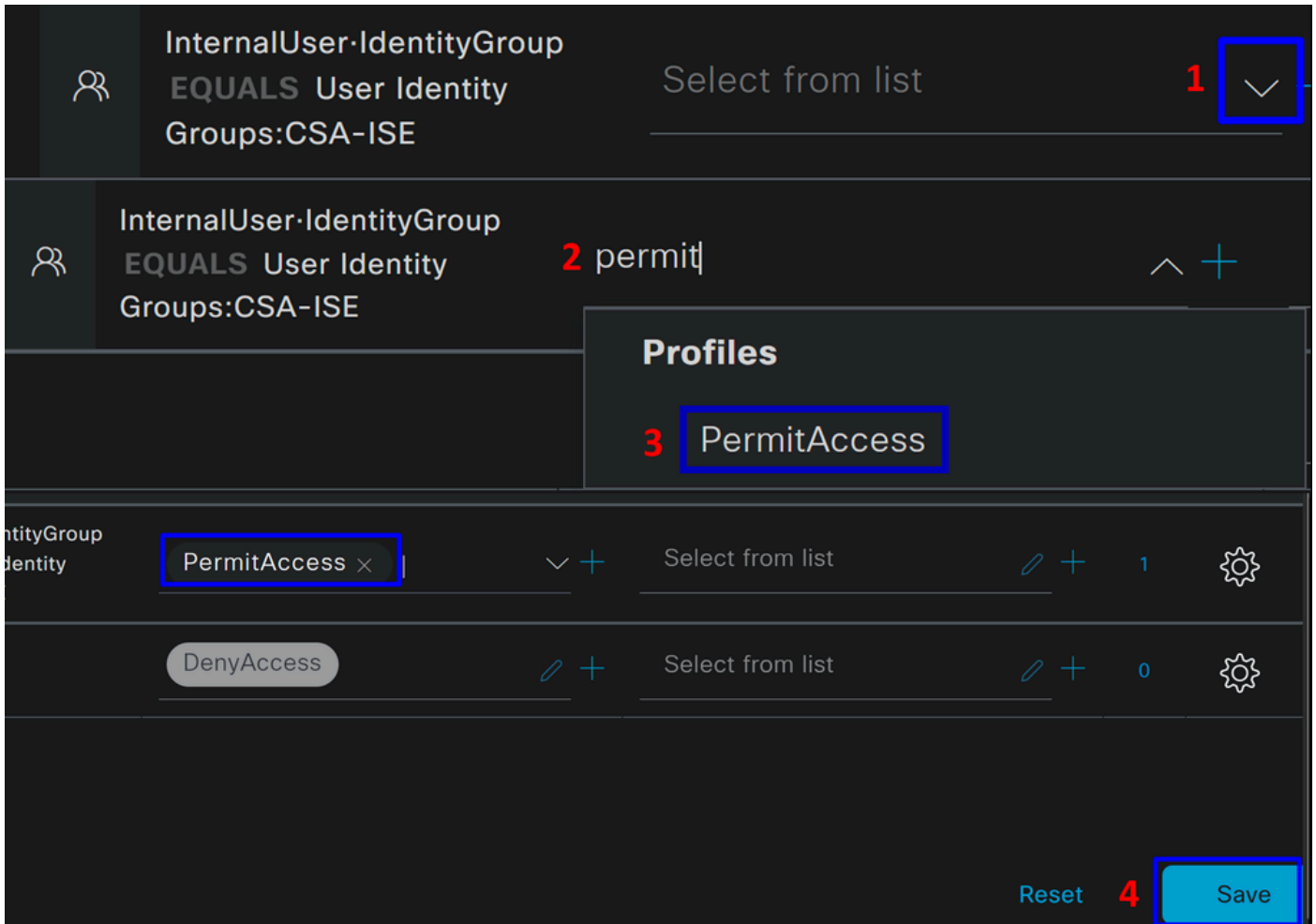


- 조건을 생성하려면 다음을 클릭합니다. Click to add an attribute
- 버튼을 **Identity Group** 클릭합니다
- 뒤의 옵션에서 **Internal User - IdentityGroup** 옵션을 클릭합니다.
- 옵션에서 **Equals** 드롭다운을 사용하여 **Group** 승인된 인증을 찾습니다(그룹 [구성](#)).
- 클릭 **Save**
- 클릭 **Use**



그런 다음 **Profiles**, which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- 에서 **Authorization Policy** 드롭다운 버튼을 클릭합니다. **Profiles**
- 허용 검색
- 선택 **PermitAccess**
- 클릭 Save



그런 다음 **Authentication Authorization** 및 정책을 정의했습니다. 사용자가 문제 없이 연결하는지 여부와 Secure Access 및 ISE에서 로그를 볼 수 있는지 여부를 확인하기 위해 인증합니다.

VPN에 연결하려면 Secure Access에서 생성된 프로파일을 사용하고 Secure Client를 통해 ISE 프로파일을 사용하여 연결할 수 있습니다.

- 인증이 승인될 때 Secure Access에서 로그는 어떻게 표시됩니까?
 - [Secure Access Dashboard\(보안 액세스 대시보드\)](#)로 이동합니다.
 - 클릭 **Monitor > Remote Access Log**

28 Events

User	Connection Event	Event Details	Internal IP Address	Public IP Address	VPN Profile
vpn user (vpnuser@ciscosst.es)	Connected		192.168.50.2	151.248.21.152	ISE_CSA

- 인증이 승인되면 ISE에 로그가 어떻게 표시됩니까?

- 탐색: Cisco ISE Dashboard

- 클릭 Operations > Live Logs

Status	Details	Identity	Authentication Policy	Authorization Policy
✕	∨	Identity	Authentication Policy	Authorization Policy
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access

Radius 로컬 또는 Active Directory 사용자 구성

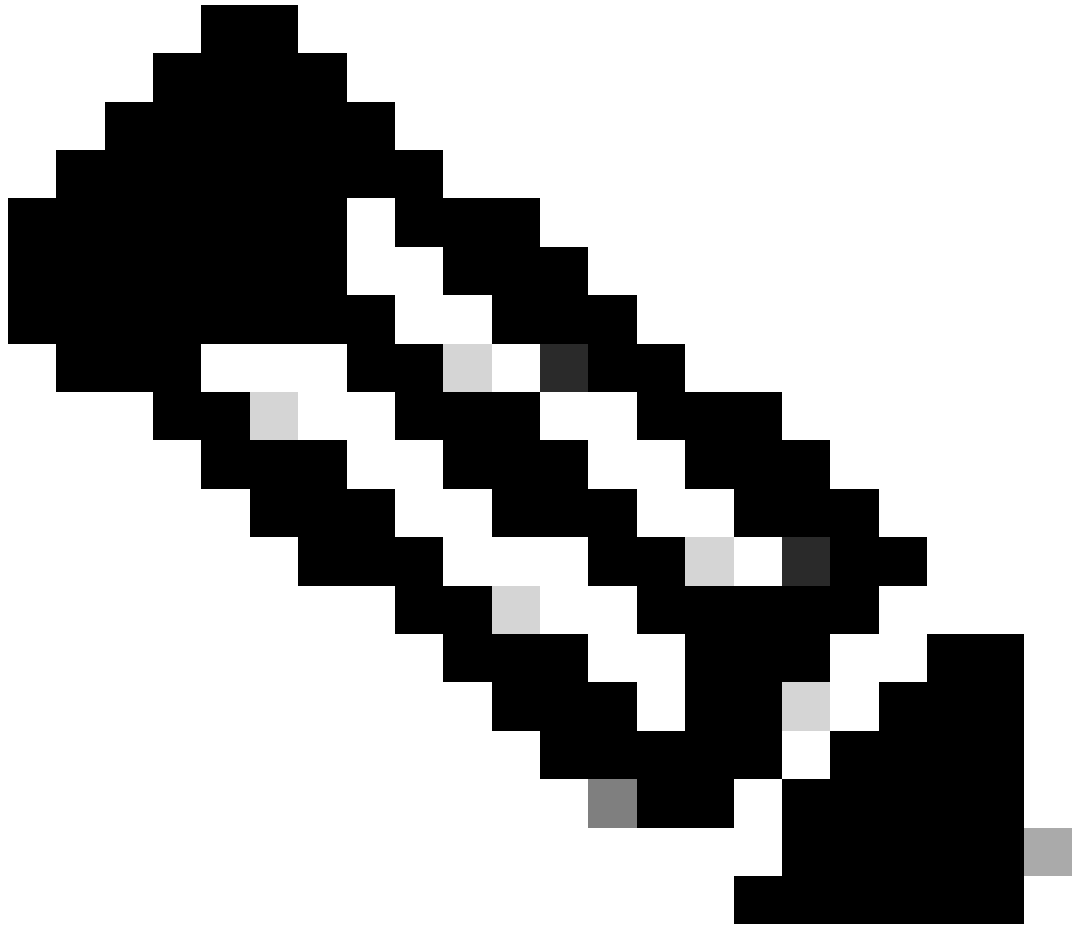
ISE Posture 구성

이 시나리오에서는 내부 리소스에 대한 액세스 권한을 부여하거나 거부하기 전에 엔드포인트 규정 준수를 확인하기 위한 컨피그레이션 생성합니다.

이를 구성하려면 다음 단계를 진행합니다.

상태 조건 구성

- ISE 대시보드로 이동
- 클릭 Work Center > Policy Elements > Conditions
- 클릭 Anti-Malware



참고: 여기에는 디바이스의 상태를 확인하고 내부 정책을 기반으로 올바른 평가를 수행할 수 있는 여러 옵션이 있습니다.

Conditions



Anti-Malware

Anti-Spyware

Anti-Virus

Application

Compound

Dictionary Compound

Dictionary Simple

Disk Encryption

External DataSource

File

Firewall

모듈을 장착하도록 클라이언트 프로비저닝을 구성합니다. 이렇게 하면 에이전트가 설치되면 더신 상태를 확인할 수 있습니다. 이 프로세스를 계속하려면 다음 단계를 수행하십시오.

ISE 대시보드로 이동합니다.










- 클릭 **Work Center > Client Provisioning**
- 선택 **Resources**

클라이언트 프로비저닝 아래에서 구성해야 하는 세 가지 사항이 있습니다.

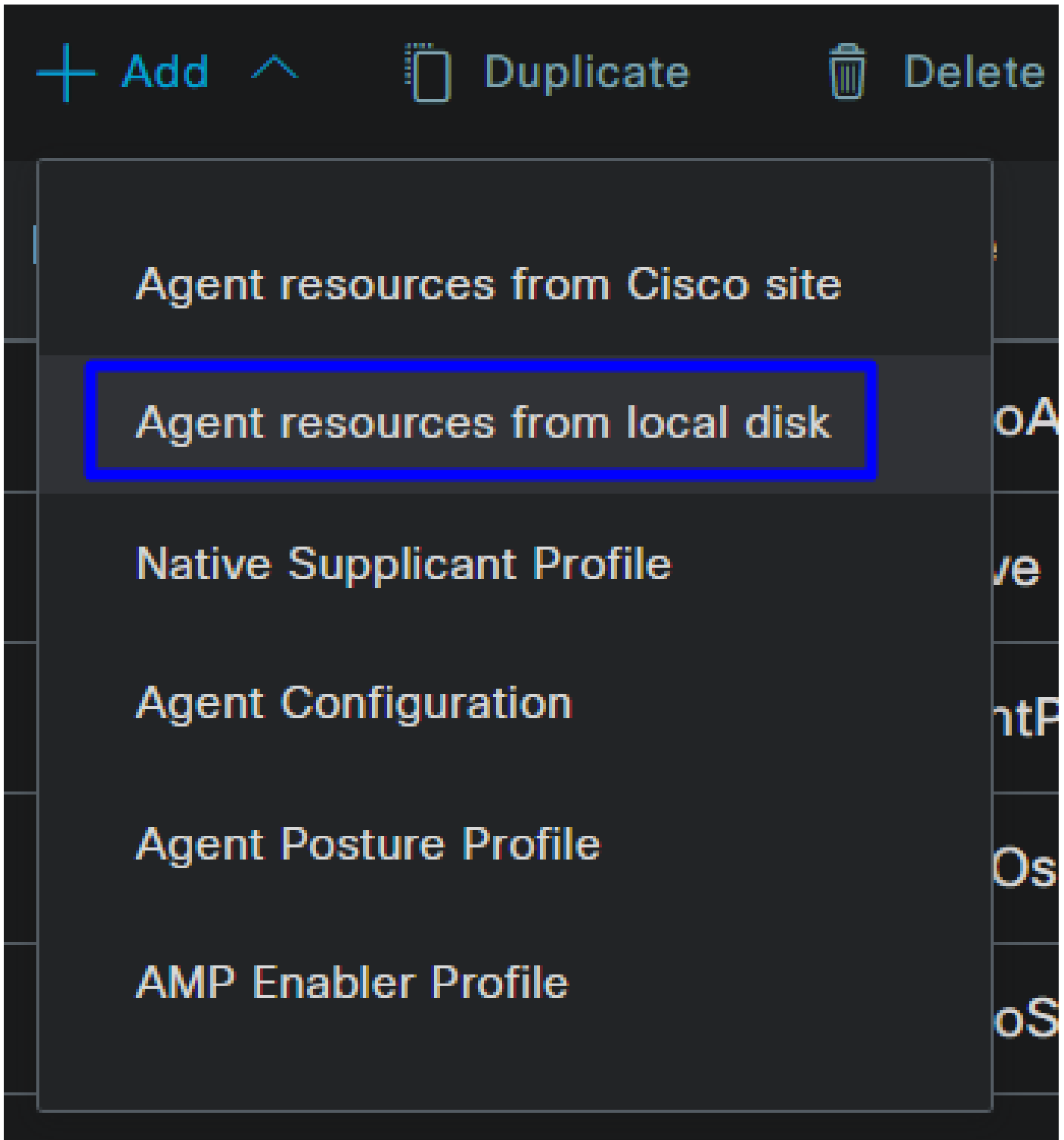
구성할 리소스	설명
1. Agent Resources	보안 클라이언트 웹 프로비저닝 패키지
2 . Compliance Module	Cisco ISE 규정 준수 모듈
3 . Agent Profile	프로비저닝 프로파일 제어.
3 . Agent Configuration	프로비저닝 포털을 설정하고 에이전트 프로파일 및 에이전트 리소스를 사용하여 프로비저닝할 모듈을 정의합니다.

Step 1 에이전트 리소스 다운로드 및 업로드

- 새 에이전트 리소스를 추가하려면 [Cisco Download Portal\(Cisco 다운로드 포털\)](#)로 이동하여 웹 배포 패키지를 다운로드합니다. 웹 배포 파일은 .pkg 형식이어야 합니다.

Cisco Secure Client Headend Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	58.06 MB	  
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	111.59 MB	  
Cisco Secure Client Headend Deployment Package (Mac OS) - Administrator rights or managed device required for install or upgrade. See Administrator Guide and Release Notes for details. cisco-secure-client-macos-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	118.88 MB	  

- 를 클릭하고 + Add > Agent resources from local disk 패키지를 업로드합니다.



Step 2 규정 준수 모듈 다운로드

- 클릭 + Add > Agent resources from Cisco Site



Add



Duplicate



Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- 필요한 모든 규정 준수 모듈에 대한 확인란을 선택하고 Save

Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3064.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3104.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3432.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3472.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3940.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3980.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3940....	Cisco Secure Client WindowsARM64 Compliance
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3980....	Cisco Secure Client WindowsARM64 Compliance

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save

Step 3 에이전트 프로파일 구성

- 클릭 + Add > Agent Posture Profile

+ Add ^

☰ Duplicate

🗑️ Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- 에 Name 대한 을(를) 만듭니다. Posture Profile

Agent Posture Profile

Name *



Description:

- Server name rules(서버 이름 규칙)에서 * 입력하고 그 Save 다음 을 클릭합니다

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com*
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Step 4 에이전트 컨피그레이션 구성

- 클릭 + Add > Agent Configuration

+ Add ^

☰ Duplicate

🗑 Delete

Agent resources from Cisco site

Agent resources from local disk


Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile


- 그런 다음 다음 매개변수를 구성합니다.

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

* Configuration Name:

Description:

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleWi 

Cisco Secure Client Module Selection

ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input type="checkbox"/>

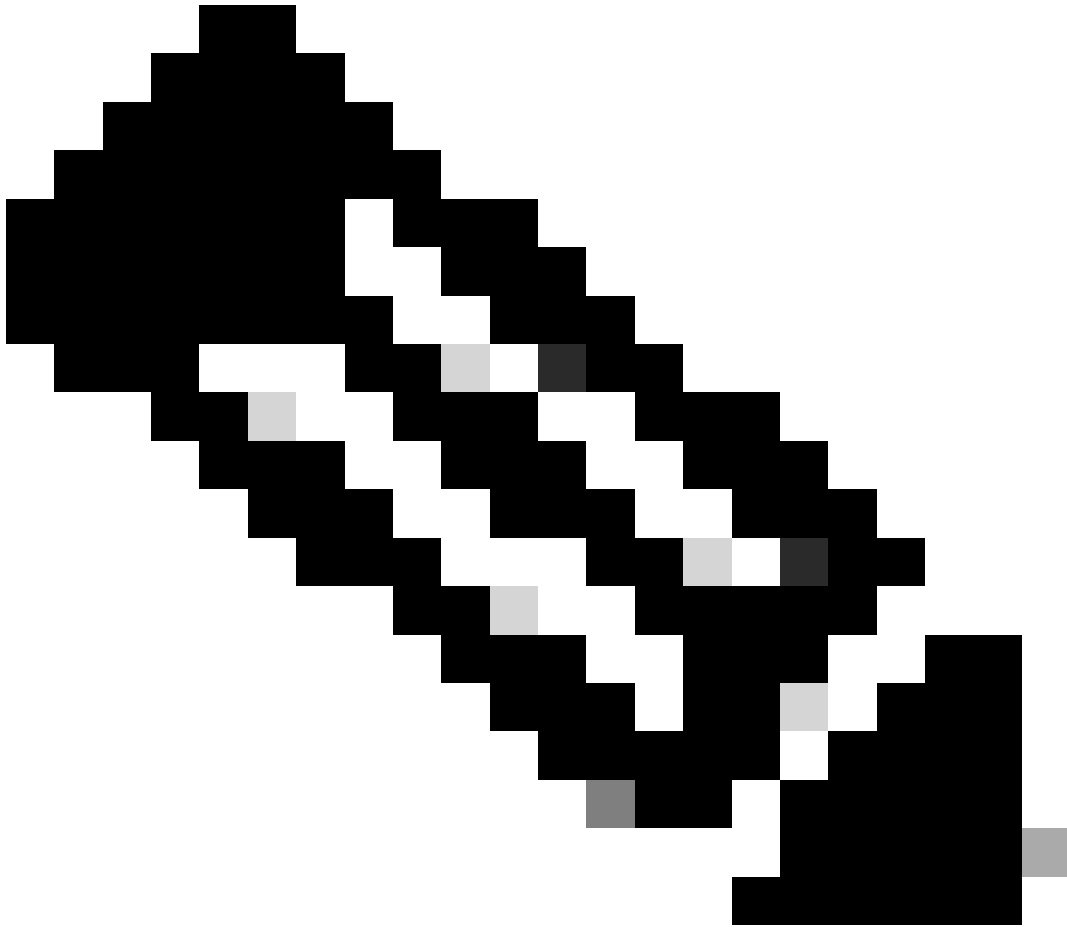
Profile Selection

* ISE Posture	1.CSA_PROFILE	▼
VPN		▼

- Select Agent Package : [1단계 Download and Upload Agent Resources\(에이전트 리소스 다운로드 및 업로드\)](#)에 업로드된 패키지를 선택합니다.
- **Configuration Name:** 인식할 이름을 선택합니다. **Agent Configuration**
- **Compliance Module:** [2단계에서 다운로드한 Compliance Module\(규정 준수 모듈 다운로드\)](#)을 선택합니다.
- Cisco Secure Client Module Selection
 - **ISE Posture:** 확인란을 선택합니다.
- **Profile Selection**

◦ ISE Posture: [3단계 에이전트](#) 프로필 구성에 구성된 [ISE 프로필을 선택합니다](#)

- 클릭 Save

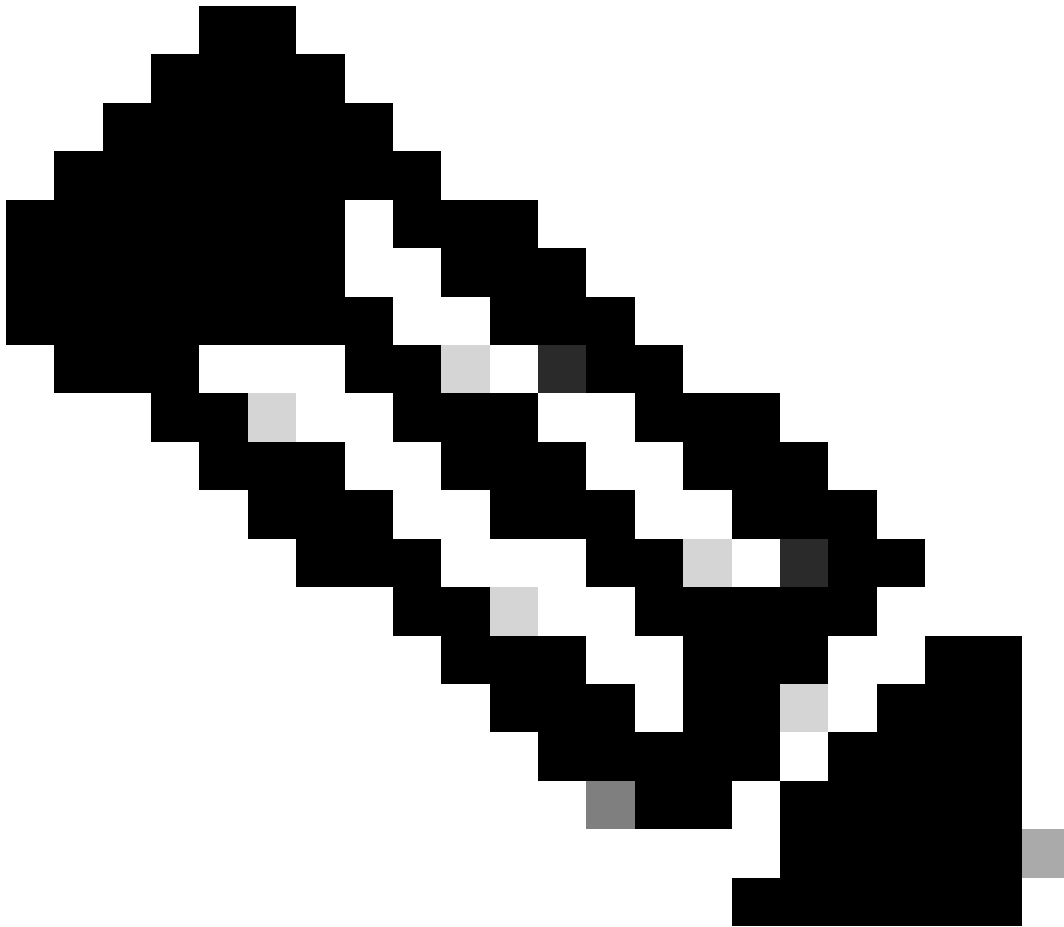


참고: 각 운영 체제, Windows, Mac OS 또는 Linux에는 하나의 클라이언트 구성이 독립적인 것이 좋습니다.

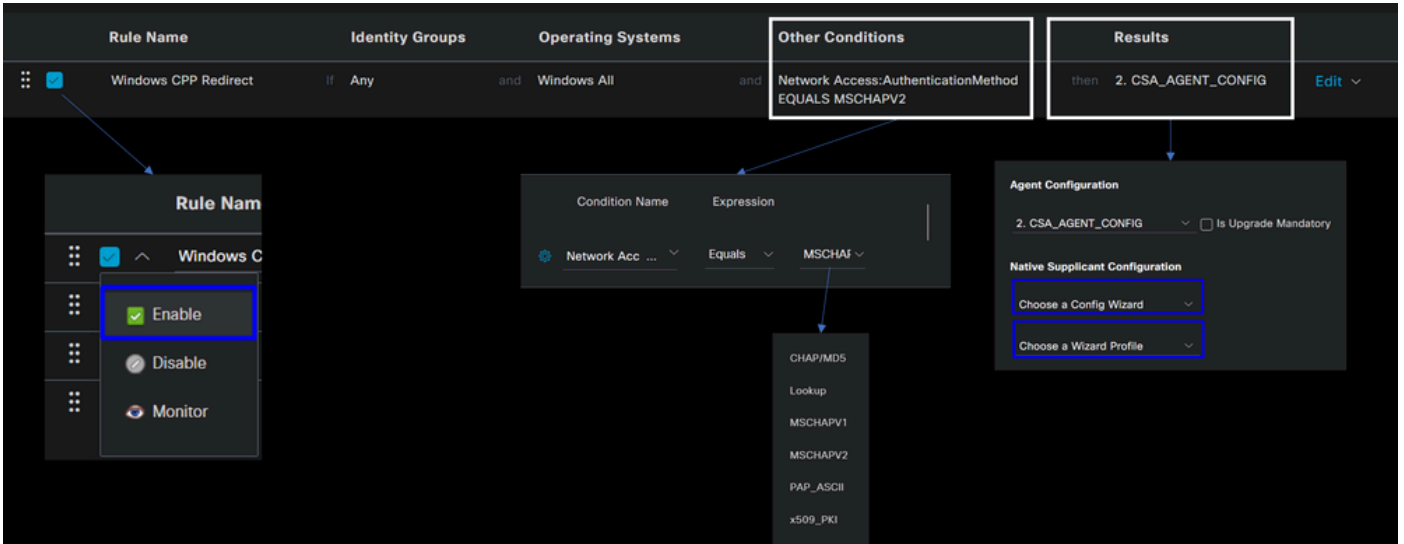
클라이언트 프로비저닝 정책 구성

ISE 상태 및 마지막 단계에서 구성된 모듈의 프로비저닝을 활성화하려면 프로비저닝을 수행할 정책을 구성해야 합니다.

- ISE 대시보드로 이동
 - 클릭 **Work Center > Client Provisioning**
-



참고: 각 운영 체제, Windows, Mac OS 또는 Linux에는 하나의 클라이언트 컨피그레이션 정책이 있는 것이 좋습니다.



- **Rule Name:** 각 정책을 쉽게 식별할 수 있도록 장치 유형 및 ID 그룹 선택에 따라 정책의 이름을 구성합니다
 - **Identity Groups:** 정책에서 평가할 ID를 선택합니다.
 - **Operating Systems:** 에이전트 패키지 선택 단계에서 선택한 에이전트 패키지를 기반으로 운영 체제를 [선택합니다.](#)
 - **Other Condition:** 단계Network Access 에 구성된 **Authentication Method**EQUALS 방법에 따라 RADIUS [그룹](#) 추가를 [선택하거나](#) 공백으로 둘 수 있습니다.
 - **Result:** [4단계](#) 에이전트 컨피그레이션 구성에서 [구성된 에이전트 컨피그레이션을 선택합니다](#)
 - **Native Supplicant Configuration:** 선택 Config Wizard 및 Wizard Profile
- 정책이 확인란에 enabled(활성화됨)로 나열되지 않은 경우 해당 정책을 enabled(활성화됨)로 표시합니다.

권한 부여 프로파일 생성

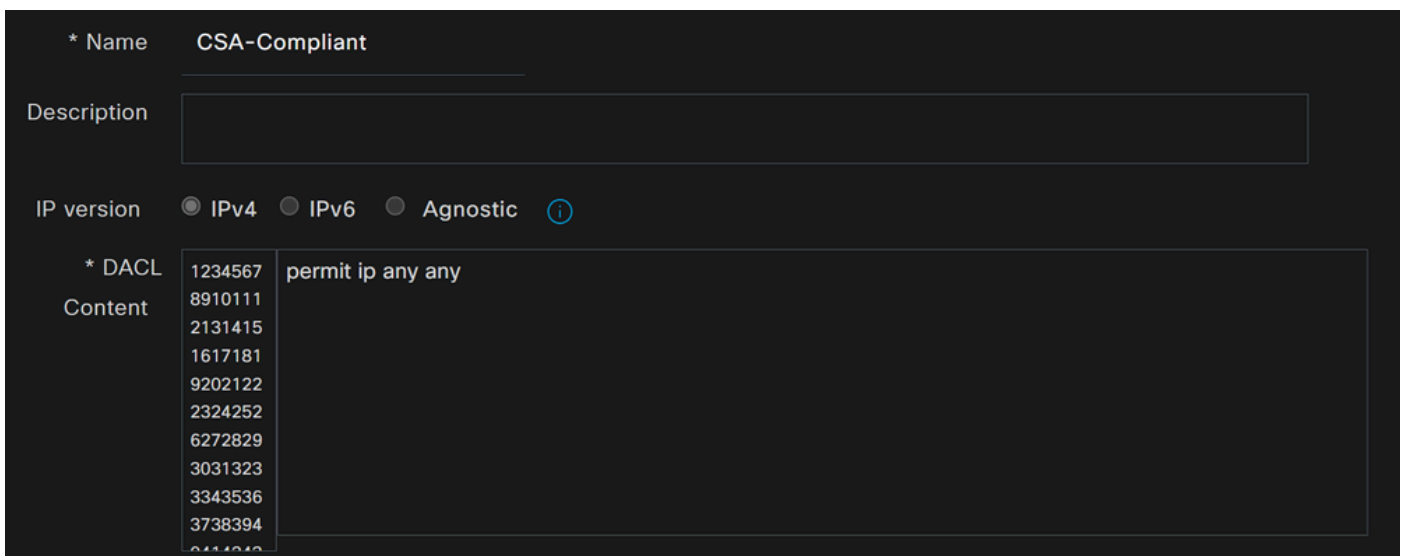
권한 부여 프로파일은 인증 통과 후 사용자 상태에 따라 리소스에 대한 액세스를 제한합니다. 사용자가 포스터를 기반으로 액세스할 수 있는 리소스를 결정하려면 권한 부여를 확인해야 합니다.

권한 부여 프로파일	설명
규정 준수	사용자 준수 - 설치된 에이전트 - 상태 확인됨
알 수 없는	User Unknown Compliant(사용자 알 수 없는 규정 준수) - 리디렉션하여 에이전트 설

규격	치 - Posture Pending to be verified(확인 보류 상태)
액세스 거부	사용자 비준수 - 액세스 거부

DAACL을 구성하려면 ISE 대시보드로 이동합니다.

- 클릭 **Work Centers > Policy Elements > Downloadable ACLs**
- 클릭 **+Add**
- Create(생성) **Compliant DAACL**



- **Name:** DAACL-Compliant를 참조하는 이름을 추가합니다.
- **IP version:** 선택 **IPv4**
- **DAACL Content:** 네트워크의 모든 리소스에 대한 액세스 권한을 제공하는 다운로드 가능한 DAACL(Access Control List)을 만듭니다.

<#root>

permit ip any any

Unknown Compliance DAACL(알 수 없는 규정 준수 DAACL)을 **Save** 클릭하고 생성합니다.

- 클릭 Work Centers > Policy Elements > Downloadable ACLs
- 클릭 +Add
- Create(생성) Unknown Compliant DACL

* Name **CSA_Redirect_To_ISE**

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content	
1234567	permit udp any any eq 67
8910111	permit udp any any eq 68
2131415	permit udp any any eq 53
1617181	permit tcp any host 192.168.10.206 eq 8443
9202122	permit tcp any any eq 80
2324252	
6272829	
3031323	
3343536	
3738394	

✓ Check DACL Syntax

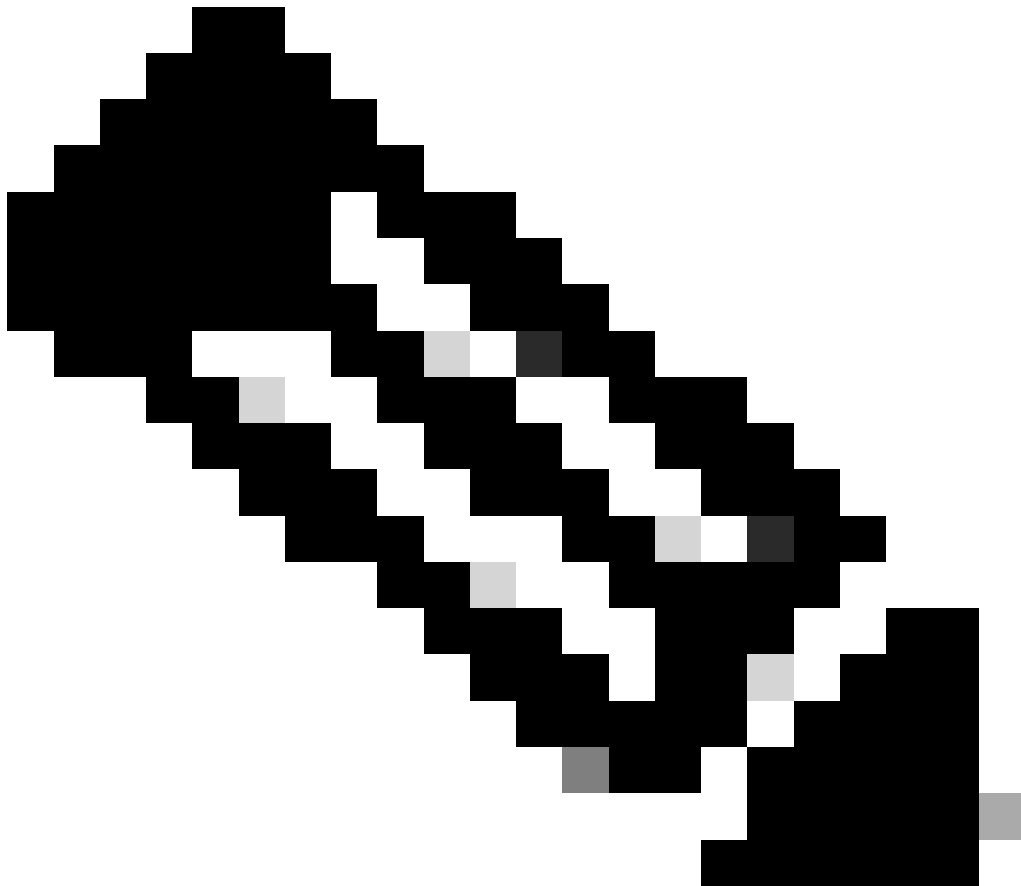
- **Name:** DACL-Unknown-Compliant를 참조하는 이름을 추가합니다
- **IP version:** 선택 IPv4
- **DACL Content:** 포트 8443을 통해 네트워크, DHCP, DNS, HTTP 및 프로비저닝 포털에 제한된 액세스를 제공하는 DACL을 생성합니다

```

permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any any eq 80

```

```
permit tcp any host 192.168.10.206 eq 8443
```



참고: 이 시나리오에서 IP 주소 192.168.10.206은 Cisco ISE(Identity Services Engine) 서버에 해당하며, 포트 8443은 프로비저닝 포털에 지정됩니다. 즉, 포트 8443을 통해 IP 주소 192.168.10.206에 대한 TCP 트래픽이 허용되어 프로비저닝 포털에 대한 액세스가 촉진됩니다.

이때 권한 부여 프로파일을 생성하는 데 필요한 DACL이 있습니다.

권한 부여 프로파일을 구성하려면 ISE 대시보드로 이동합니다.

- 클릭 Work Centers > Policy Elements > Authorization Profiles
- 클릭 +Add
- Create(생성) Compliant Authorization Profile

Authorization Profile

* Name

CSA-Compliant

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile



Cisco



Service Template

Track Movement



Agentless Posture



Passive Identity Tracking



Common Tasks

DACL Name

CSA-Compliant

IPv6 DACL Name

ACL

ACL IPv6 (Filter ID)

- **Name:** 호환 권한 부여 프로파일을 참조하는 이름을 만듭니다.
- **Access Type:** 선택 **ACCESS_ACCEPT**








- **Common Tasks**


- **DACL NAME:** Compliant DACL(규정 준수 DACL) 단계에 구성된 [DACL을 선택합니다](#)


을 **Save** 클릭하고 Unknown Authorization Profile

- 클릭 **Work Centers > Policy Elements > Authorization Profiles**
- 클릭 **+Add**

- Create(생성) Unknown Compliant Authorization Profile

* Name	CSA-Unknown-Compliant
Description	<input type="text"/>
* Access Type	ACCESS_ACCEPT 
Network Device Profile	 Cisco  
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> 
Agentless Posture	<input type="checkbox"/> 
Passive Identity Tracking	<input type="checkbox"/> 

 Common Tasks

<input checked="" type="checkbox"/> DACL Name	CSA_Redirect_To_ISE 
---	---

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) ▾ ACL redirect

Value Client Provisioning Portal (... ▾

- **Name:** 알 수 없는 호환 권한 부여 프로파일을 참조하는 이름을 만듭니다.
- Access Type: 선택 **ACCESS_ACCEPT**

- **Common Tasks**

- **DACL NAME:** Unknown Compliant DACL(알 수 없는 호환 DACL) 단계에 구성된 [DACL을 선택합니다.](#)

- **Web Redirection (CWA,MDM,NSP,CPP)**

- 선택 **Client Provisioning (Posture)**

- **ACL:** 이어야 합니다. redirect

- **Value:** 기본 프로비저닝 포털을 선택합니다. 다른 포털을 정의한 경우 기본 프로비저닝 포털을 선택합니다.
-
-

참고: 모든 구축의 보안 액세스에 대한 리디렉션 ACL의 이름은 **redirect**입니다.

이러한 값을 모두 정의한 후에는 아래에 비슷한 내용이 있어야 합니다Attributes Details.

```
Attributes Details
Access Type = ACCESS_ACCEPT
DAACL = CSA_Redirect_To_ISE
cisco-av-pair = url-redirect-acl=redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=
&action=cpp
```

컨피그레이션Save 을 종료하고 다음 단계로 진행하려면 클릭합니다.

상태 정책 집합 구성

생성하는 이 세 가지 정책은 구성된 권한 부여 프로파일을 기반으로 합니다. **DenyAccess** 즉, 다른 정책을 생성할 필요가 없습니다.

정책 설정 - 권한 부여	권한 부여 프로파일
규정 준수	권한 부여 프로파일 - 규정 준수
알 수 없는 규격	권한 부여 프로파일 - 알 수 없는 규격
비준수	액세스 거부

ISE 대시보드로 이동

- [클릭 Work Center > Policy Sets](#)

- 생성한 정책> 에 액세스하려면 를 클릭합니다

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
🟢	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	370	⚙️	➡️

- 다음을 클릭합니다. Authorization Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
🟢	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	370
> Authentication Policy(2)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
> Authorization Policy(4)					

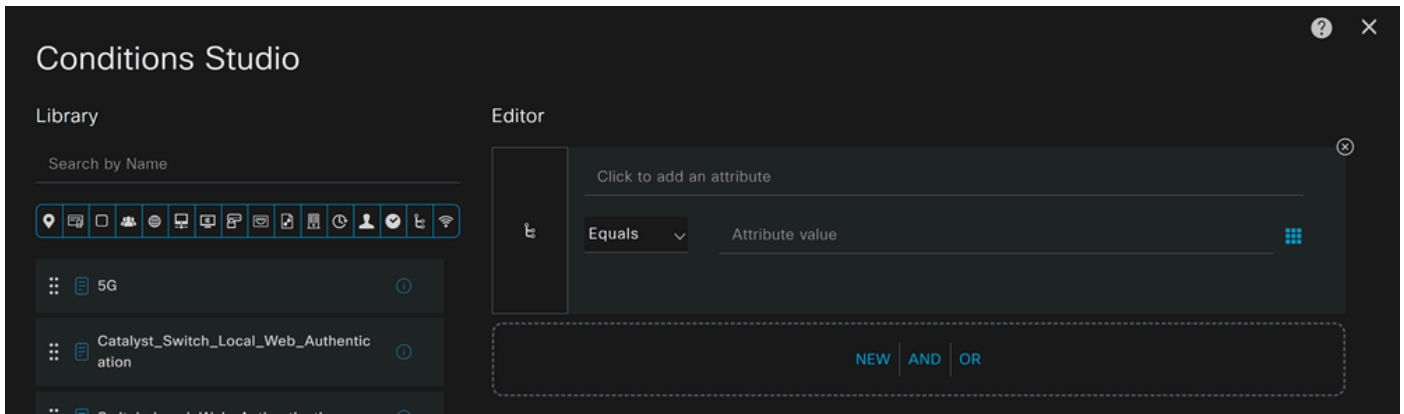
- 다음 순서로 다음 세 가지 정책을 생성합니다.

✓	CSA-Compliant	AND	<ul style="list-style-type: none"> Compliant_Devices Network_Access_Authentication_Passed InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE 	CSA-Post-Compliant
✓	CSA-Unknown-Compliant	AND	<ul style="list-style-type: none"> Network_Access_Authentication_Passed Compliance_Unknown_Devices InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE 	CSA-Unknown-Compliant
✓	CSA-Non-Compliant	AND	<ul style="list-style-type: none"> Non_Compliant_Devices Network_Access_Authentication_Passed InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE 	DenyAccess

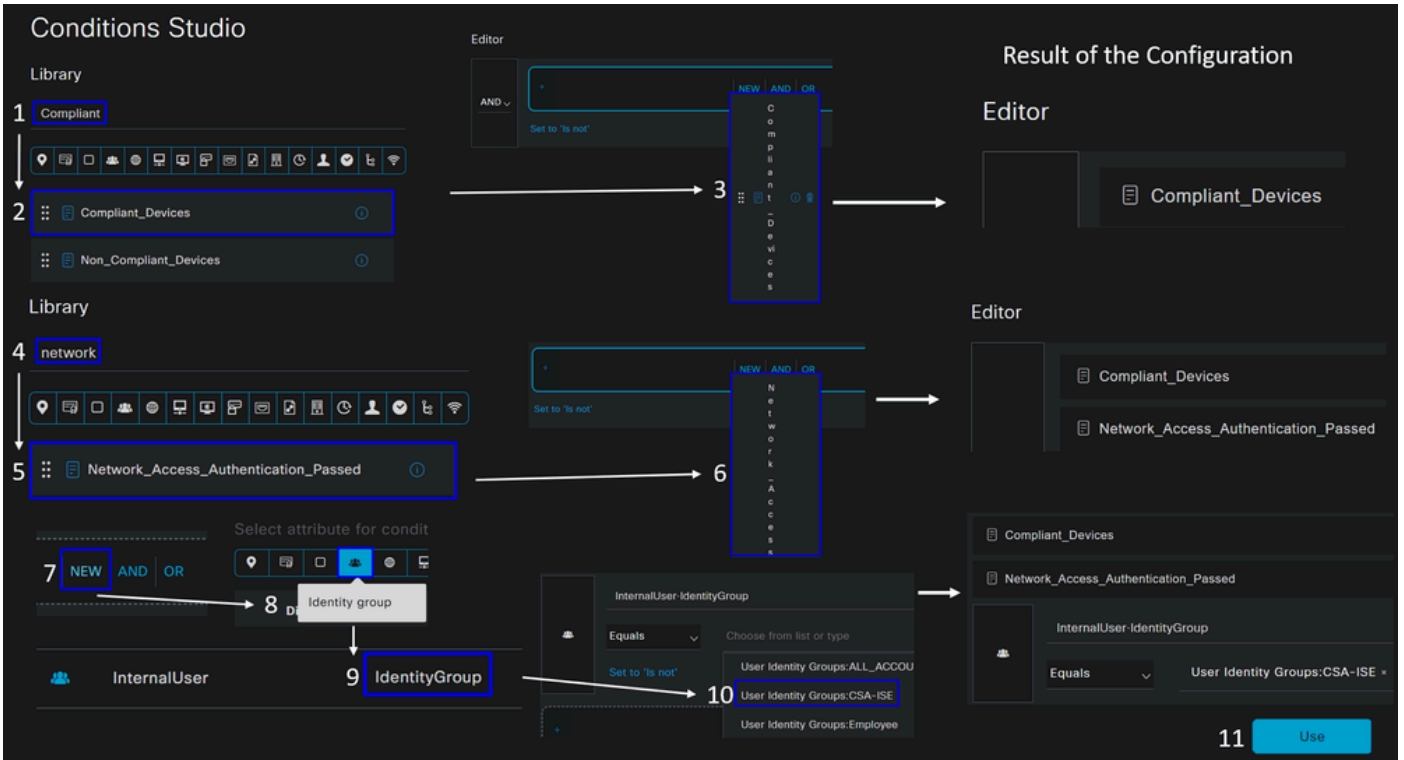
- 정책을 + 정의하려면 를 **CSA-Compliance** 클릭합니다.

				Results	
+ Status	Rule Name	Conditions		Profiles	Security Groups
<input type="text" value="Search"/>					
✓	Authorization Rule 1	+		Select from list	Select from list

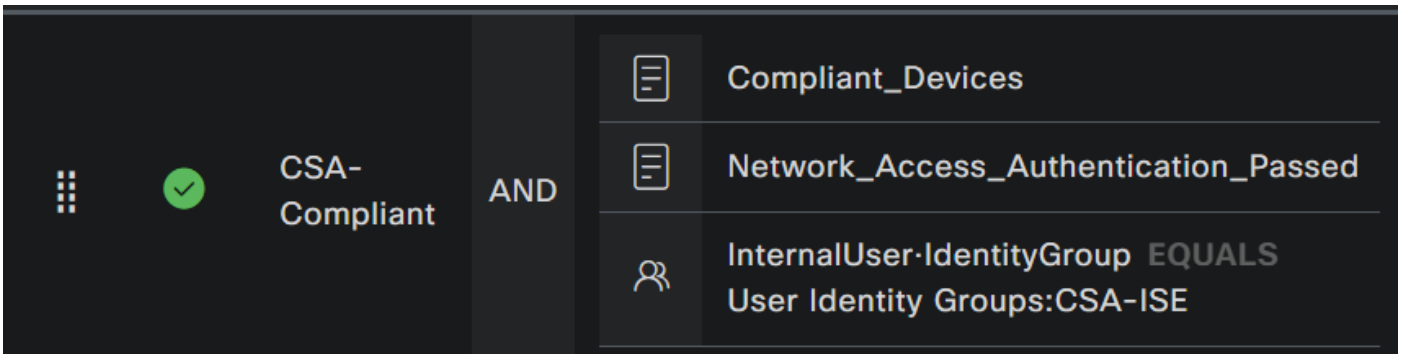
- 다음 단계로 Rule Name, Conditions 및 Profiles
- 구성 이름을 Name 다음으로 설정할 경우 **CSA-Compliance**
- 을(를) **Condition** 구성하려면 +
- 에서 **Condition Studio** 다음 정보를 찾을 수 있습니다.



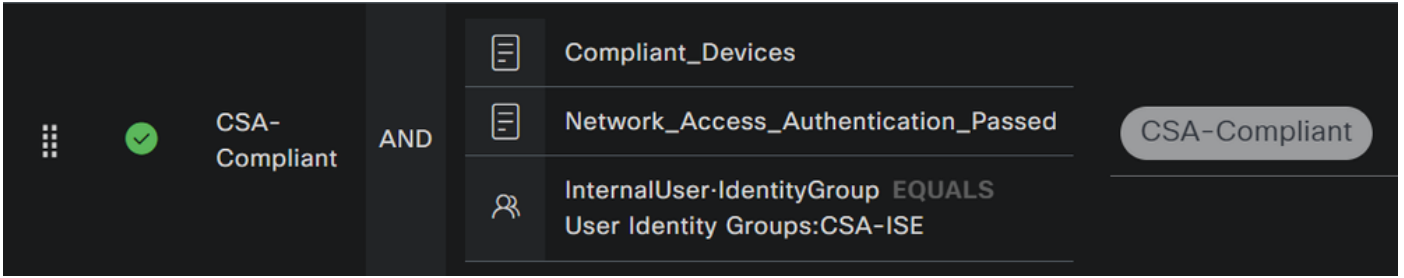
- 조건을 생성하려면 다음을 검색합니다. **compliant**
- 이(가) Compliant_Devices
- 끌어서 놓기 **Editor**
- 두 번째 조건을 생성하려면 다음을 검색합니다. **network**
- 이(가) Network_Access_Authentication_Passed
- 끌어서 놓기 **Editor**
- 의 아래를 Editor 클릭합니다. **New**
- 아이콘을 **Identity Group** 클릭합니다
- 선택 **Internal User Identity Group**
- 에서 **Equals** 일치시킬 **User Identity Group** 을 선택합니다
- 클릭 **Use**



- 그 결과, 다음 이미지가 생성됩니다

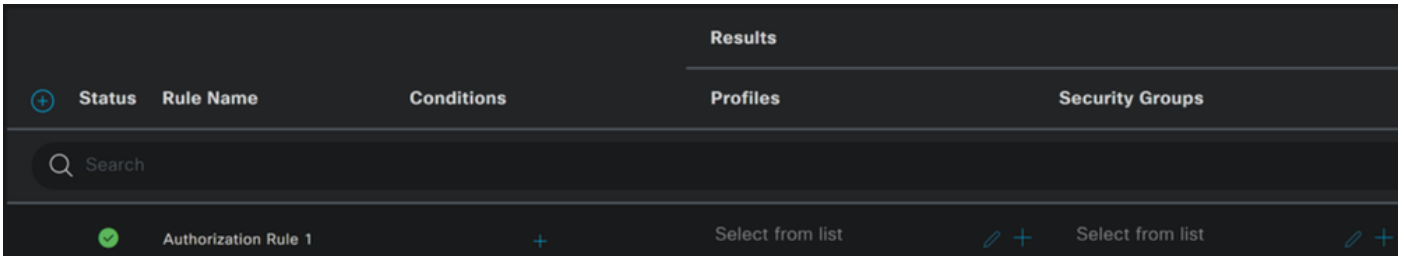


- 드롭다운 **Profile** 버튼 아래를 클릭하고 Compliant Authorization Profile(규정 준수 권한 부여 프로파일) 단계에서 구성된 Complaint Authorization [프로파일을 선택합니다](#)

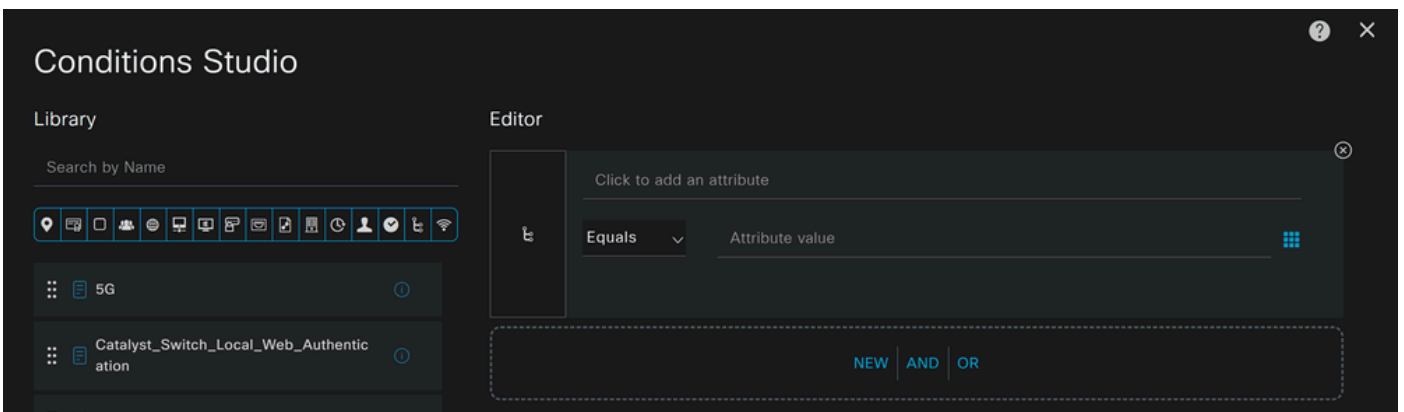


이제 을(를) **Compliance Policy Set** 구성했습니다.

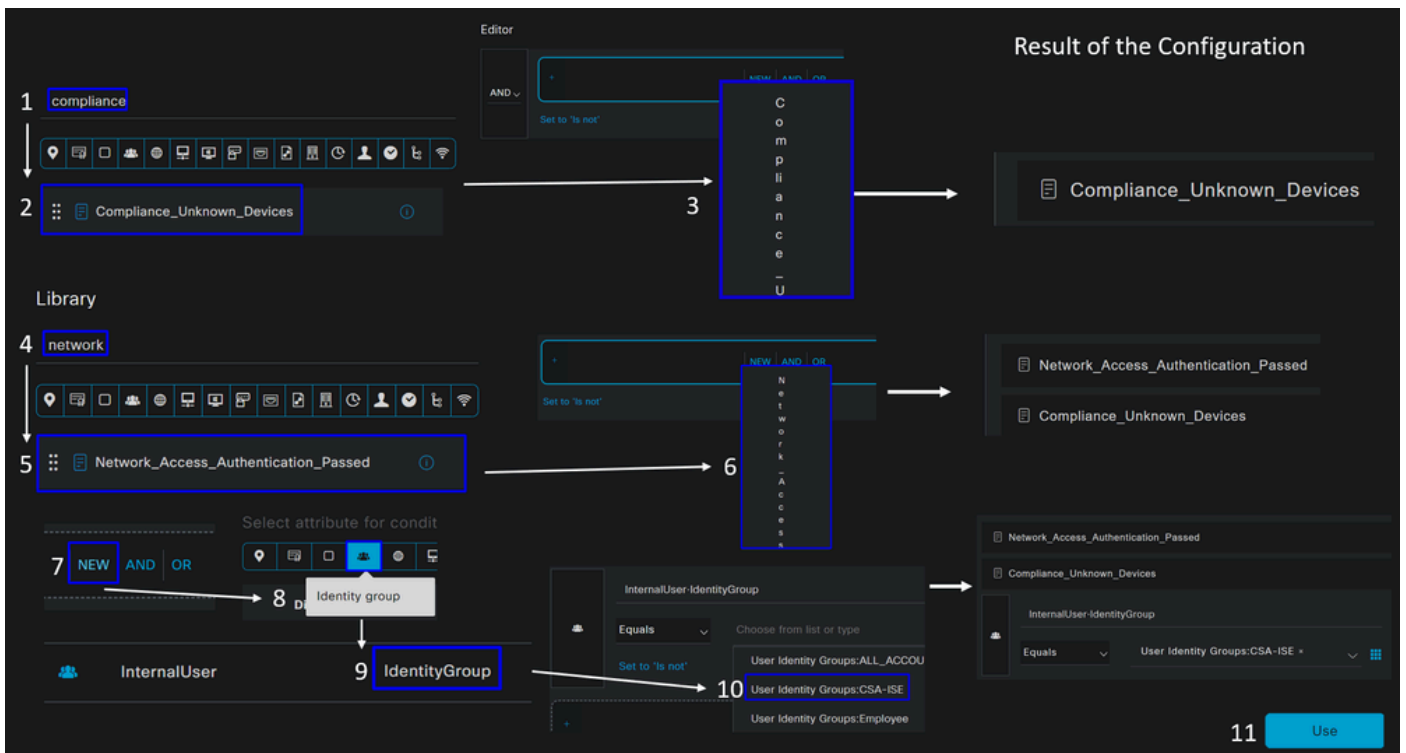
- 정책을 + 정의하려면 를 **CSA-Unknown-Compliance** 클릭합니다.



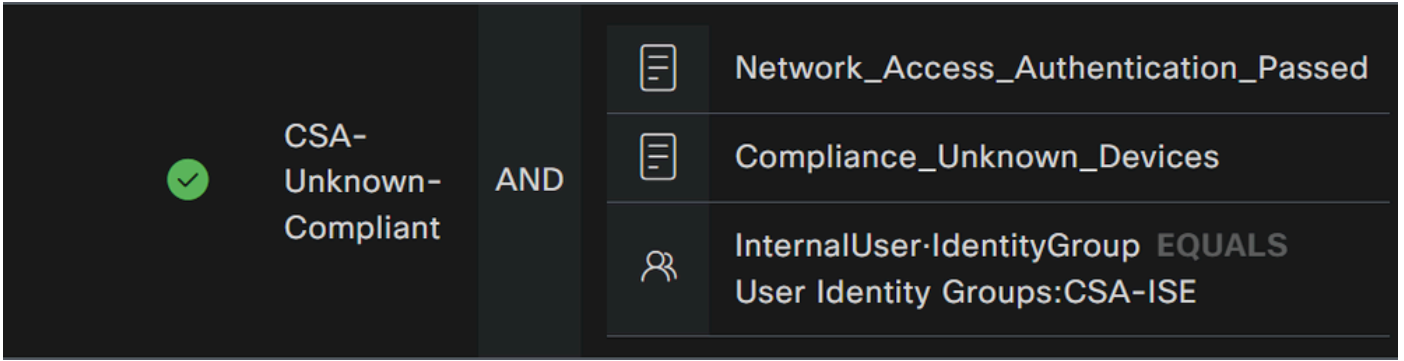
- 다음 단계로 Rule Name, Conditions 및 Profiles
- 구성 이름을 Name 다음으로 설정할 경우 **CSA-Unknown-Compliance**
- 을(를) **Condition** 구성하려면 +
- 에서 **Condition Studio** 다음 정보를 찾을 수 있습니다.



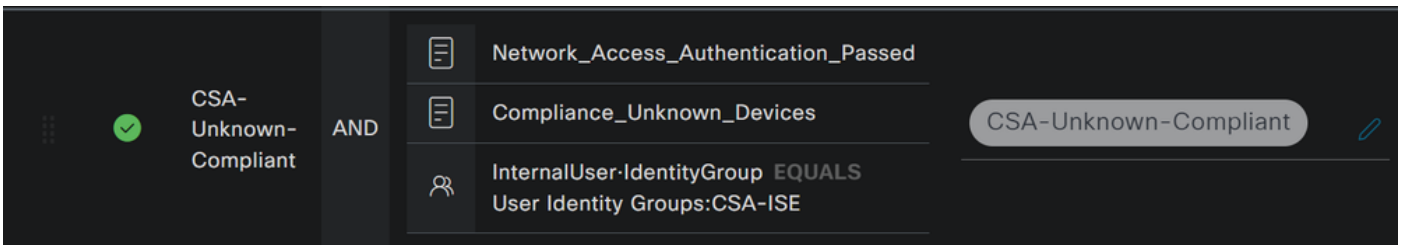
- 조건을 생성하려면 다음을 검색합니다. **compliance**
- 이(가) Compliant_Unknown_Devices
- 끌어서 놓기 **Editor**
- 두 번째 조건을 생성하려면 다음을 검색합니다. **network**
- 이(가) Network_Access_Authentication_Passed
- 끌어서 놓기 **Editor**
- 의 아래를 Editor 클릭합니다. **New**
- 아이콘을 **Identity Group** 클릭합니다
- 선택 **Internal User Identity Group**
- 에서 **Equals** 일치시킬 **User Identity Group** 을 선택합니다
- 클릭 **Use**



- 그 결과, 다음 이미지가 생성됩니다

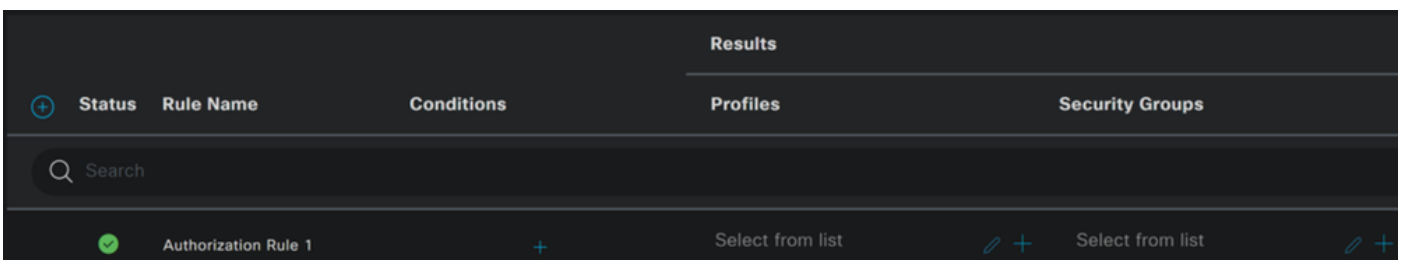


- 드롭다운 **Profile** 버튼 아래를 클릭하고 Unknown Compliant Authorization Profile(알 수 없는 호환 권한 부여 프로파일) 단계에서 구성된 [Compliant 권한 부여 프로파일을 선택합니다](#)



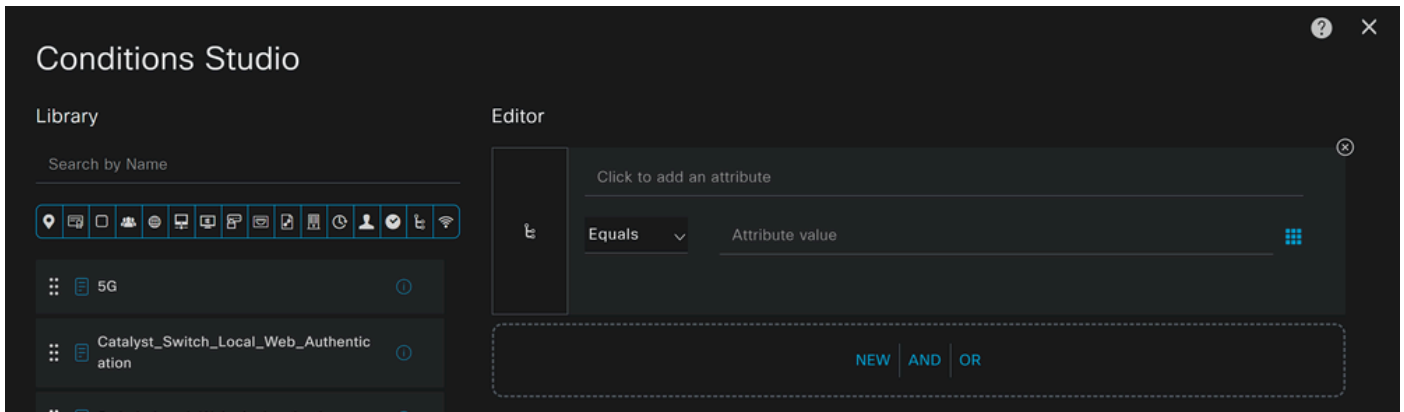
이제 을(를) **Unknown Compliance Policy Set**구성했습니다.

- 정책을 + 정의하려면 를 **CSA- Non-Compliant** 클릭합니다.

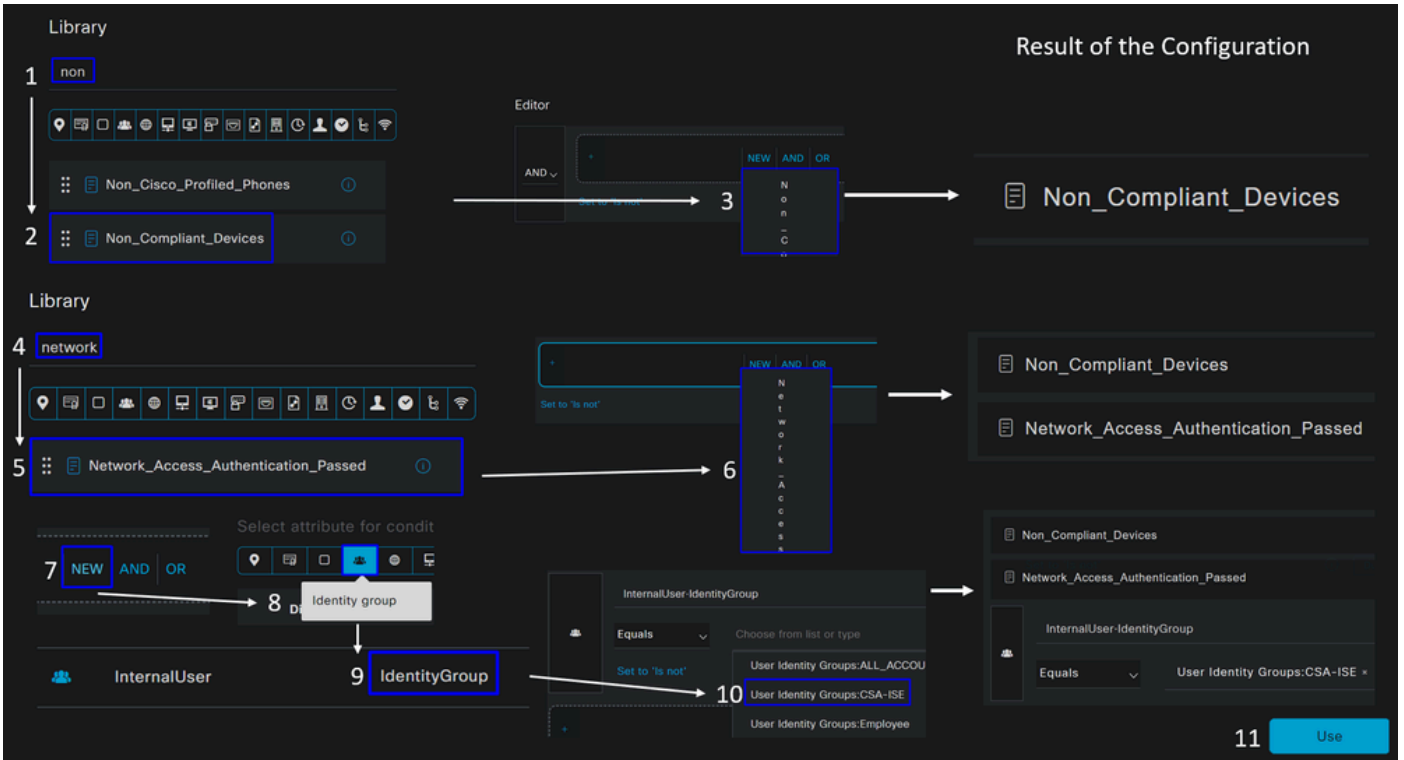


- 다음 단계로 Rule Name, Conditions 및 Profiles
- 구성 이름을 Name 다음으로 설정할 경우 **CSA-Non-Compliance**
- 을(를) **Condition**구성하려면 +

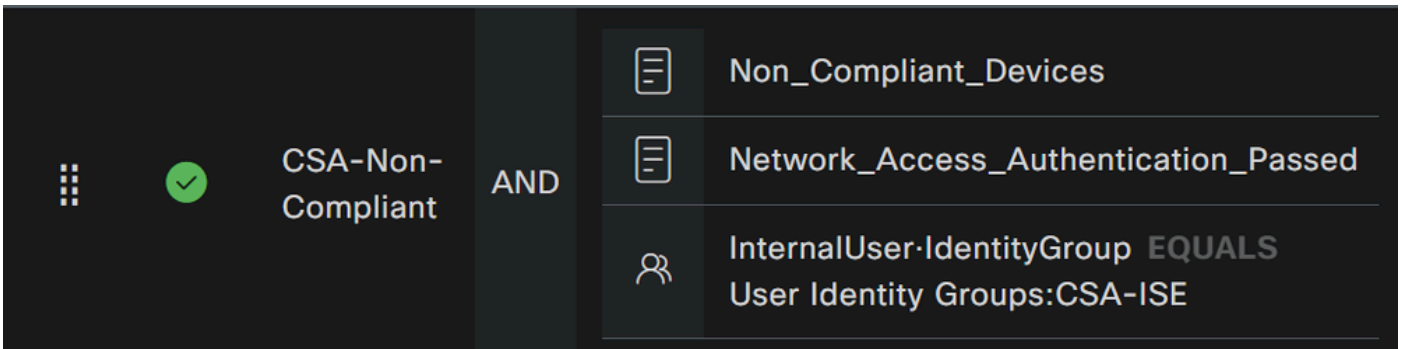
- 에서 **Condition Studio** 다음 정보를 찾을 수 있습니다.



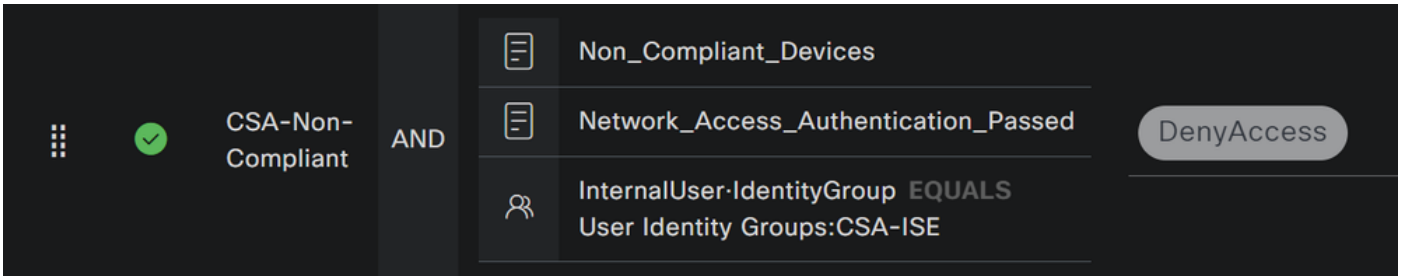
- 조건을 생성하려면 다음을 검색합니다. **non**
- 이(가) Non_Compliant_Devices
- 끌어서 놓기 **Editor**
- 두 번째 조건을 생성하려면 다음을 검색합니다. **network**
- 이(가) Network_Access_Authentication_Passed
- 끌어서 놓기 **Editor**
- 의 아래를 Editor 클릭합니다. **New**
- 아이콘을 **Identity Group** 클릭합니다
- 선택 **Internal User Identity Group**
- 에서 **Equals** 일치시킬 **User Identity Group** 을 선택합니다
- 클릭 Use



- 그 결과, 다음 이미지가 생성됩니다



- 드롭다운 **Profile** 버튼 아래를 클릭하고 불만 승인 프로필을 선택합니다 **DenyAccess**



세 가지 프로파일의 컨피그레이션을 종료하면 포스처와의 통합을 테스트할 준비가 됩니다.

다음을 확인합니다.

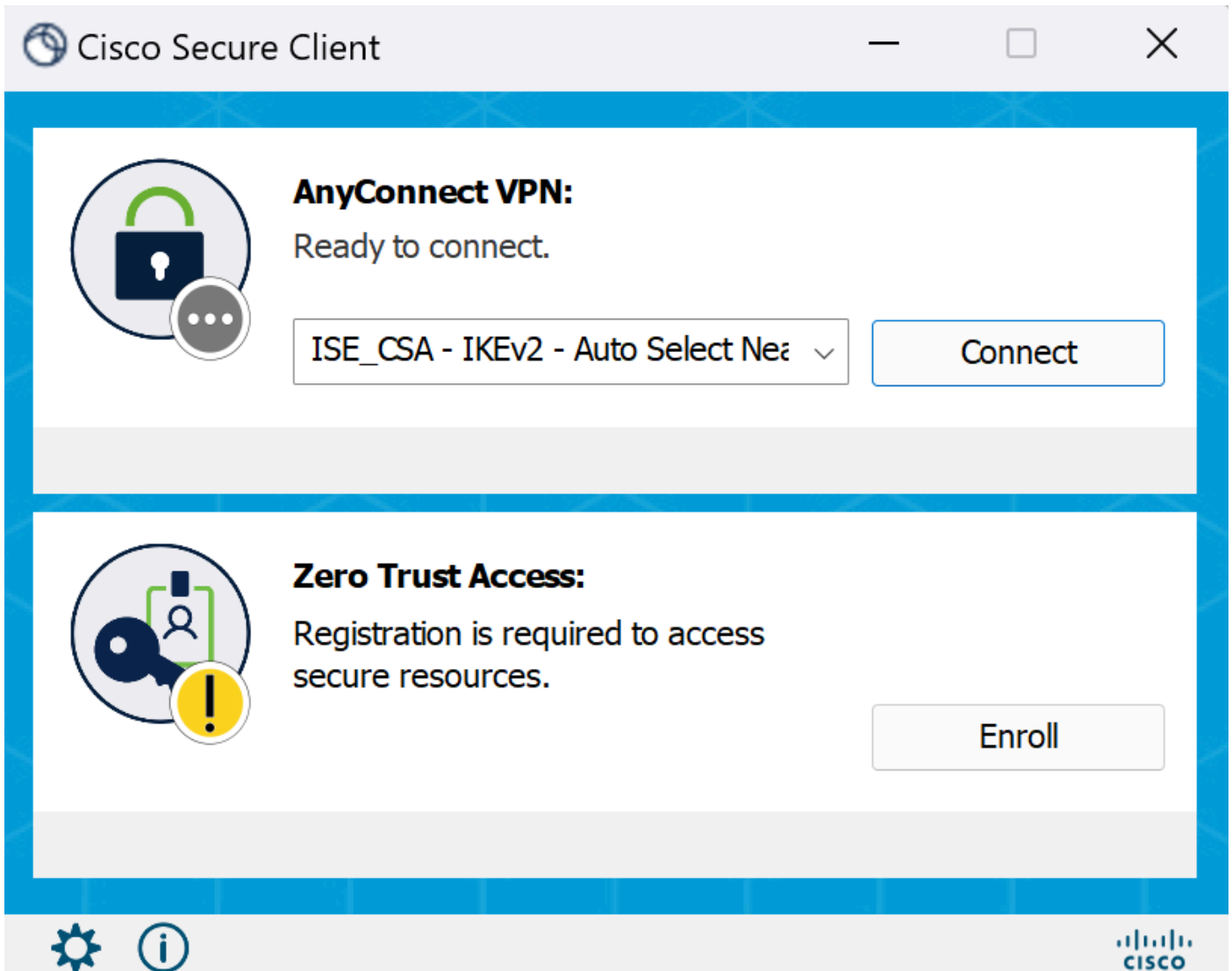
상태 검증

컴퓨터의 연결

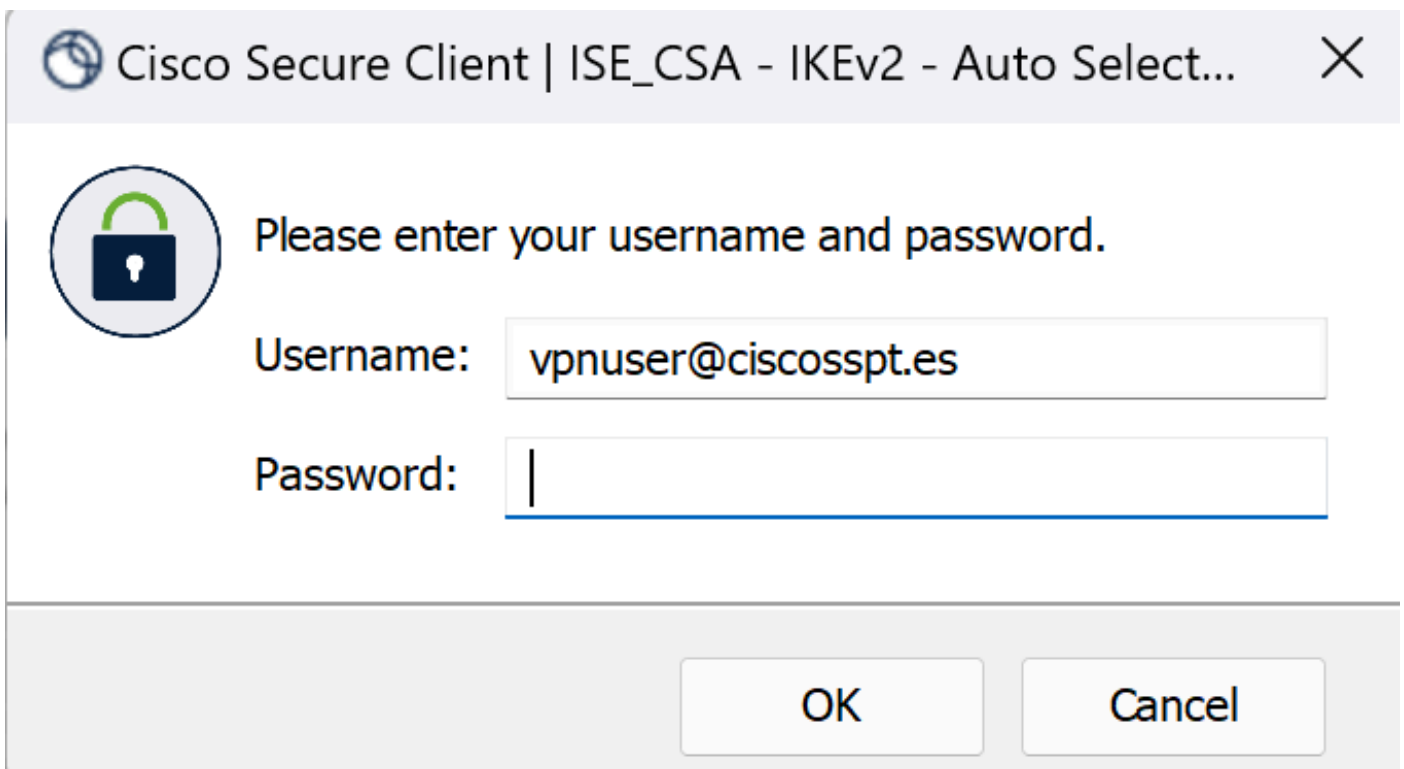
Secure Client를 통해 Secure Access에 제공된 FQDN RA-VPN 도메인에 연결합니다.

참고: 이 단계에서는 ISE 모듈을 설치하지 않아도 됩니다.

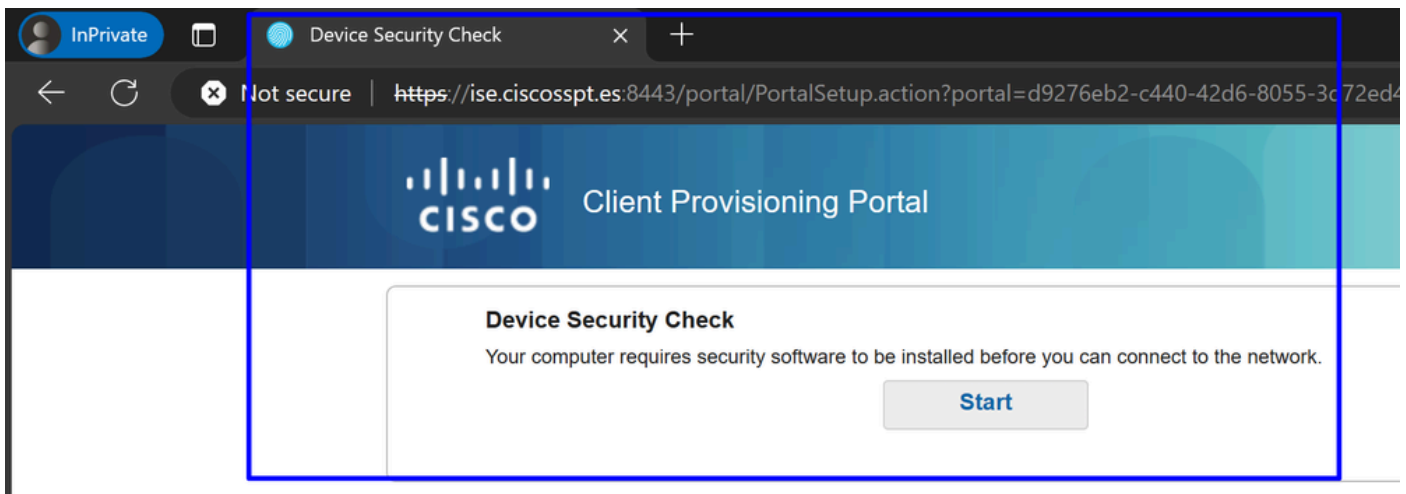
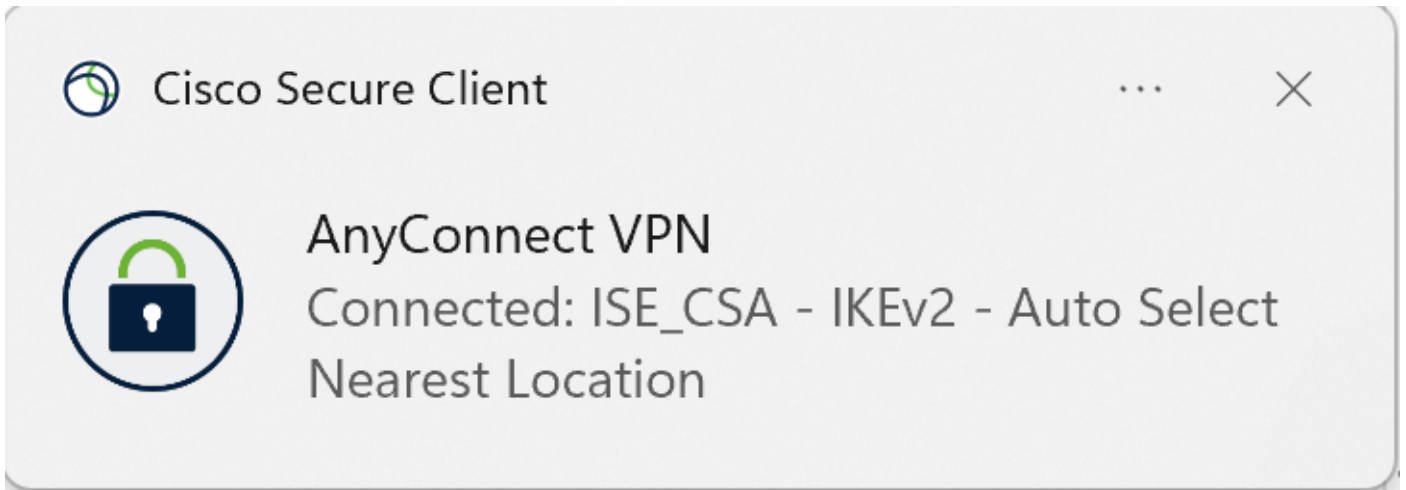
1. 보안 클라이언트를 사용하여 연결합니다.



2. 인증하려면 자격 증명을 제공합니다.



3. 이 시점에서 VPN에 연결되며 대부분 ISE로 리디렉션됩니다. 그렇지 않은 경우 로 이동할 수 [http:1.1.1.1](http://1.1.1.1)있습니다.





참고: 이 시점에서 권한 부여 - 정책 설정 [CSA-Unknown-Compliance](#)에 해당하게 됩니다. 시스템에 ISE Posture Agent가 설치되어 있지 않고 ISE 프로비저닝 포털로 리디렉션되어 에이전트를 설치할 수 있기 때문입니다.

4. [시작]을 클릭하여 에이전트 프로비저닝을 진행합니다.

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

9 Detecting if Agent is installed and running...

5. 클릭합니다+ **This is my first time here.**

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect Posture Agent

+ + This is my first time here


+ + Remind me what to do next

6. 클릭 Click here to download and install agent

+ This is my first time here

1. You must install Agent to check your device before accessing the network. [Click here to download and install Agent](#)
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.

 You have 4 minutes to install and for the compliance check to complete

7. 에이전트 설치

Downloads



cisco-secure-client-ise...aBf8STpS5Nr1nzotleQ.exe

[Open file](#)

[See more](#)

Network Setup Assistant



Network Setup Assistant



Installation is completed.

Quit

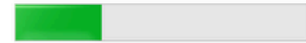
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

8. 에이전트를 설치하면 ISE Posture에서 시스템의 현재 상태를 확인하기 시작합니다. 정책 요구 사항이 충족되지 않으면 규정 준수를 안내하는 팝업이 나타납니다.



ISE Posture

1 Update(s) Required



30%

Time Remaining:

3 Minutes



Action Required to Enable Access

Updates are needed on your device before you can join the network.

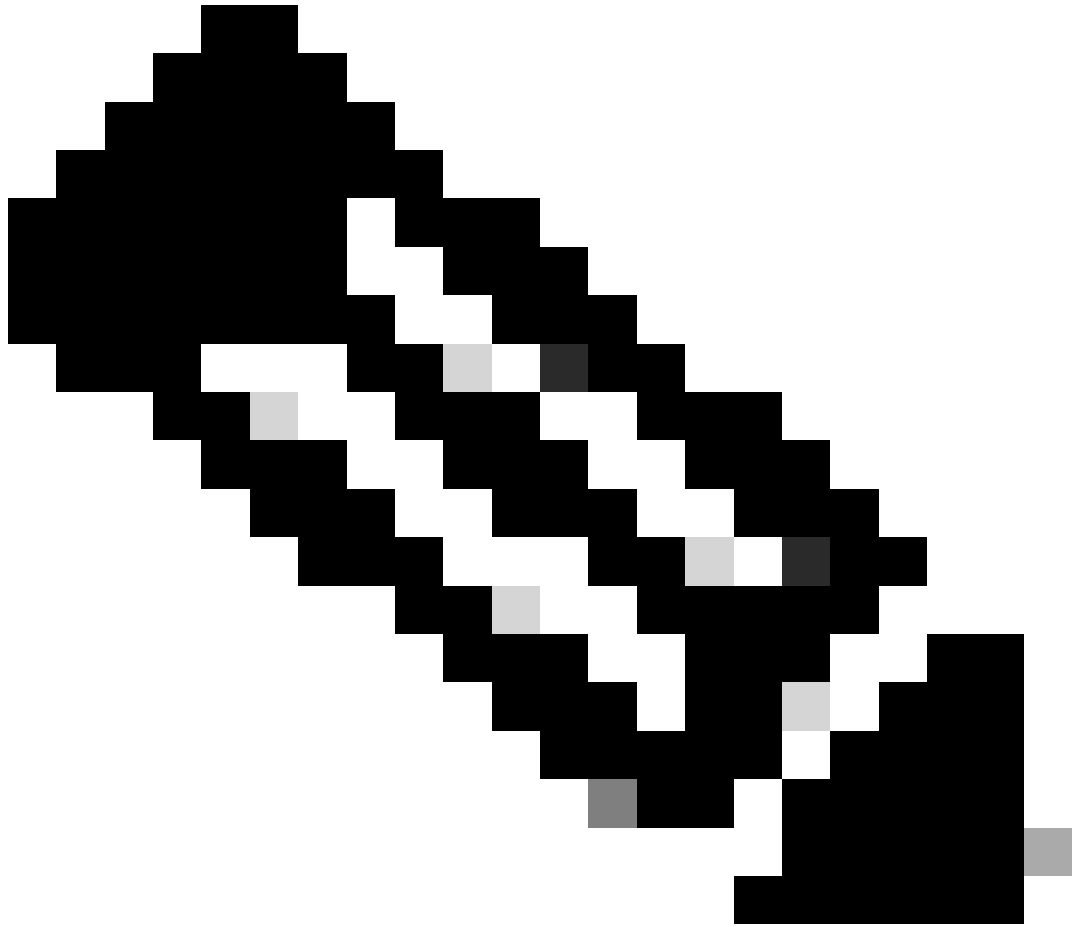
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

More Details



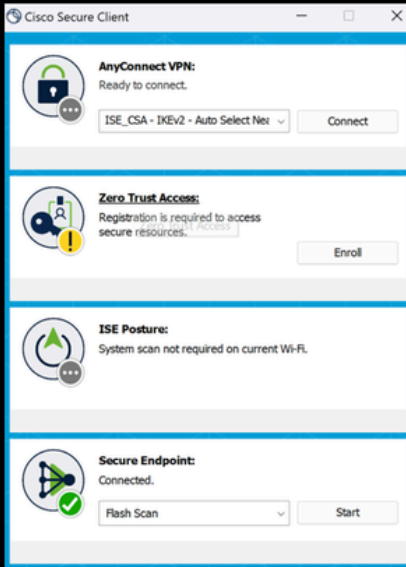
Cancel



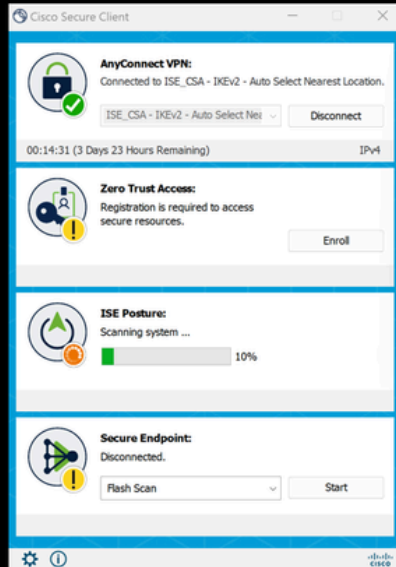
참고: 사용자Cancel 또는 나머지 시간이 종료되면 자동으로 비준수 상태가 되고 권한 부여 정책 집합 [CSA-Non-Compliance에 해당되며](#) 즉시 VPN에서 연결이 끊깁니다.

9. Secure Endpoint Agent를 설치하고 VPN에 다시 연결합니다.

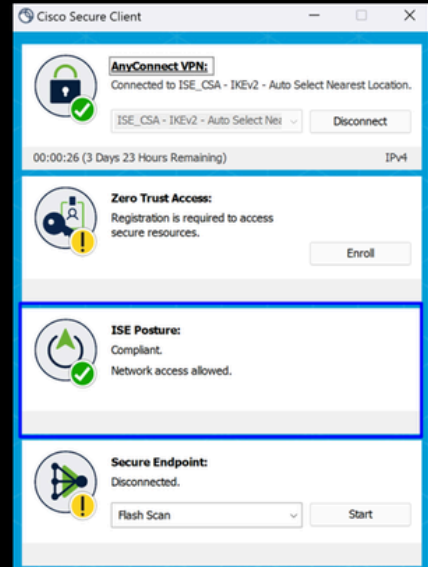
Secure Endpoint Installed



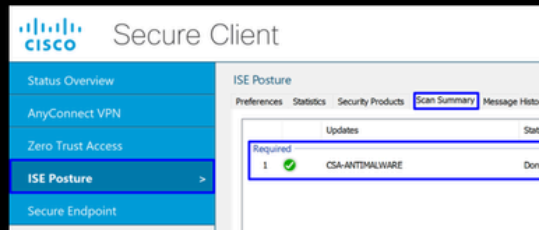
Agent Scanning



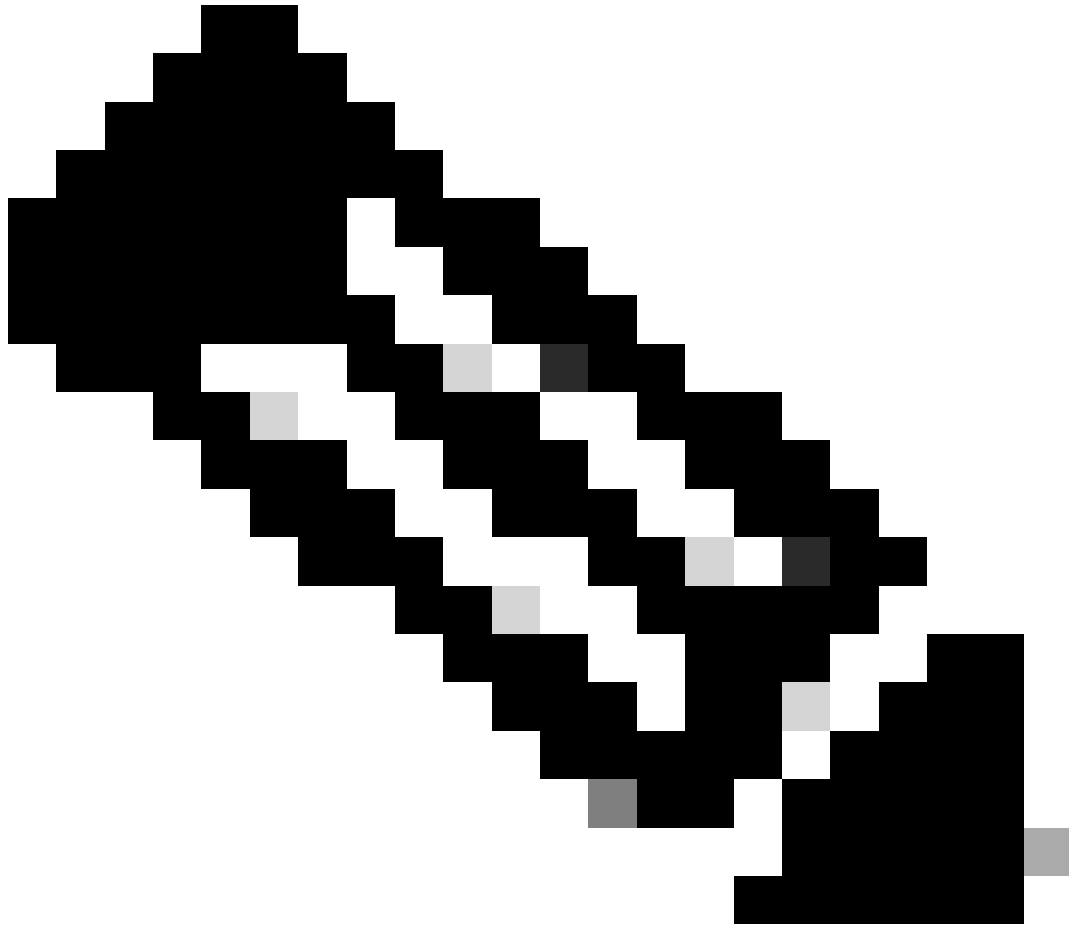
ISE Posture Successful validated



Scan Summary - Compliance



10. 상담원이 시스템이 규정 준수 상태인지 확인한 후, 상태가 불만 사항으로 변경되고 네트워크의 모든 리소스에 대한 액세스 권한을 부여합니다.



참고: 규정을 준수하면 [CSA-Compliance](#) 권한 부여 정책 집합에 해당되며, 즉시 모든 네트워크 리소스에 액세스할 수 있습니다.

ISE에서 로그를 수집하는 방법

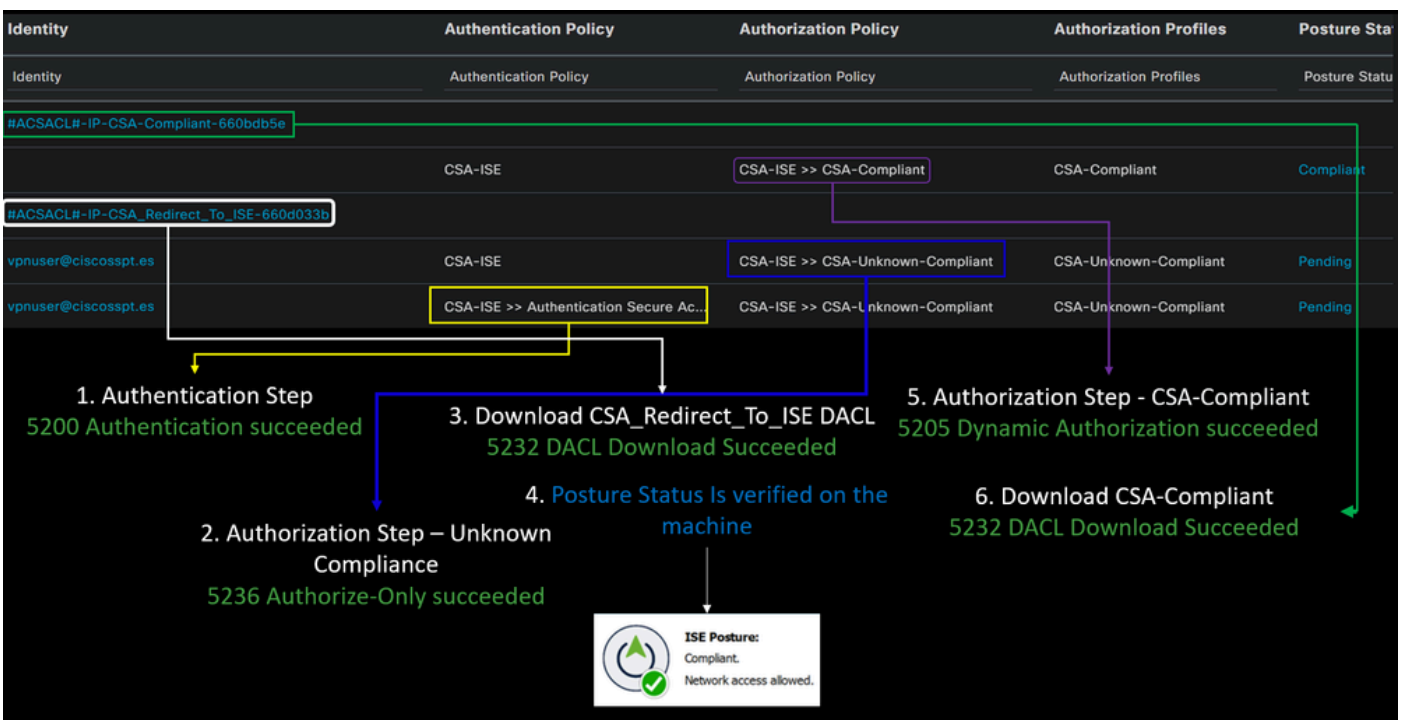
사용자에 대한 인증 결과를 확인하려면 두 가지 규정 준수 및 비준수 예를 사용합니다. ISE에서 검토하려면 다음 지침을 따르십시오.

- ISE 대시보드로 이동
-

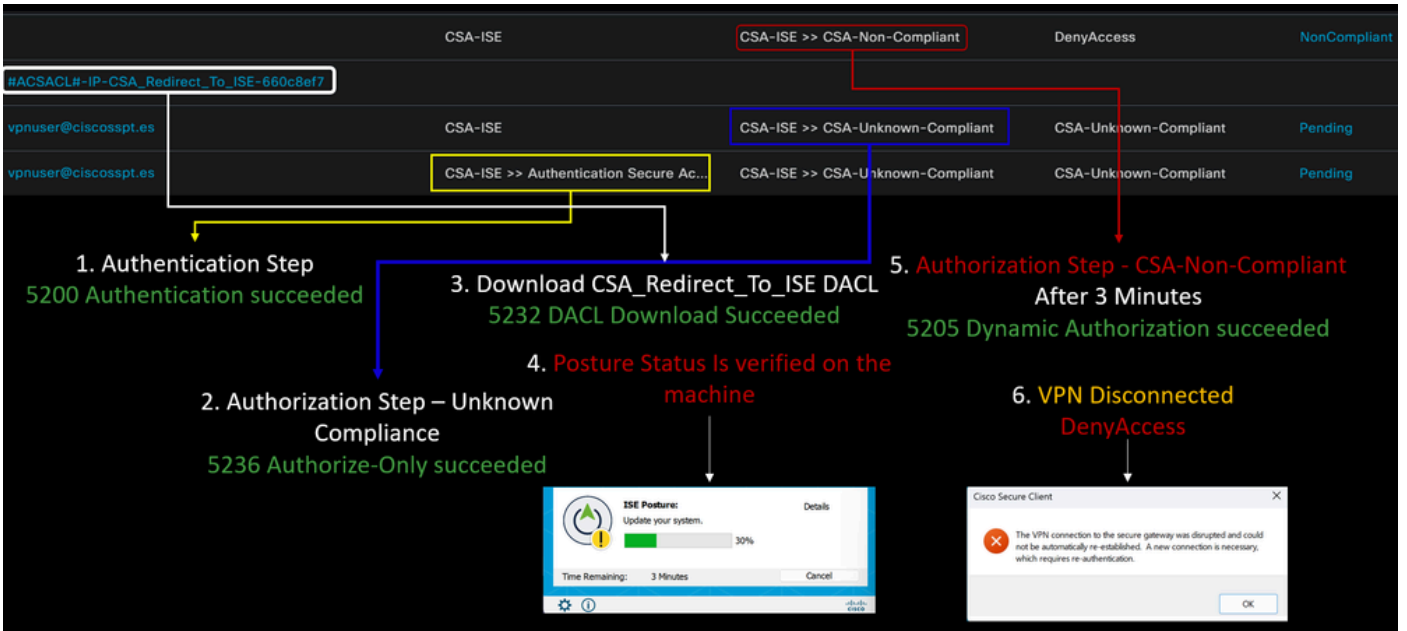
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter	
0	0	0	0	0	
Refresh Never		Show Latest 50 records		Within Last 24 hours	
Reset Repeat Counts		Export To		Filter	
Time	Status	Details	Identity	Authentication Policy	Authorization Policy
Apr 03, 2024 07:00:27.7...	✓		Identity	Authentication Policy	Authorization Policy
Apr 03, 2024 06:56:15.4...	✓		#ACSACL#-IP-CSA_Redirect_To_ISE-660d033b	CSA-ISE	CSA-ISE >> CSA-Non-Compla
Apr 03, 2024 06:56:15.3...	✓		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> CSA-Unknown-Co
Apr 03, 2024 06:56:15.2...	✓		vpnuser@ciscospt.es	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> CSA-Unknown-Co

다음 세 번째 시나리오에서는 성공적인 규정준수 및 비규정준수 이벤트가 다음 아래에 어떻게 표시되는지 **Live Logs**보여줍니다.

규정 준수



비준수



보안 액세스 및 ISE 통합의 첫 단계

다음 예에서 Cisco ISE는 네트워크 192.168.10.0/24에 있으며 터널을 통해 연결 가능한 네트워크의 컨피그레이션을 터널 컨피그레이션에 추가해야 합니다.

Step 1: 터널 컨피그레이션을 확인합니다.

이를 확인하려면 [Secure Access](#) Dashboard로 [이동하십시오](#).

- 클릭 **Connect > Network Connections**
- Your Tunnel(터널)을 **Network Tunnel Groups** 클릭합니다.

HomeFTD	Connected	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1
---------	-----------	------------------	---------------	---	---------------

- 요약에서 터널이 Cisco ISE가 있는 주소 공간을 구성했는지 확인합니다.

Summary



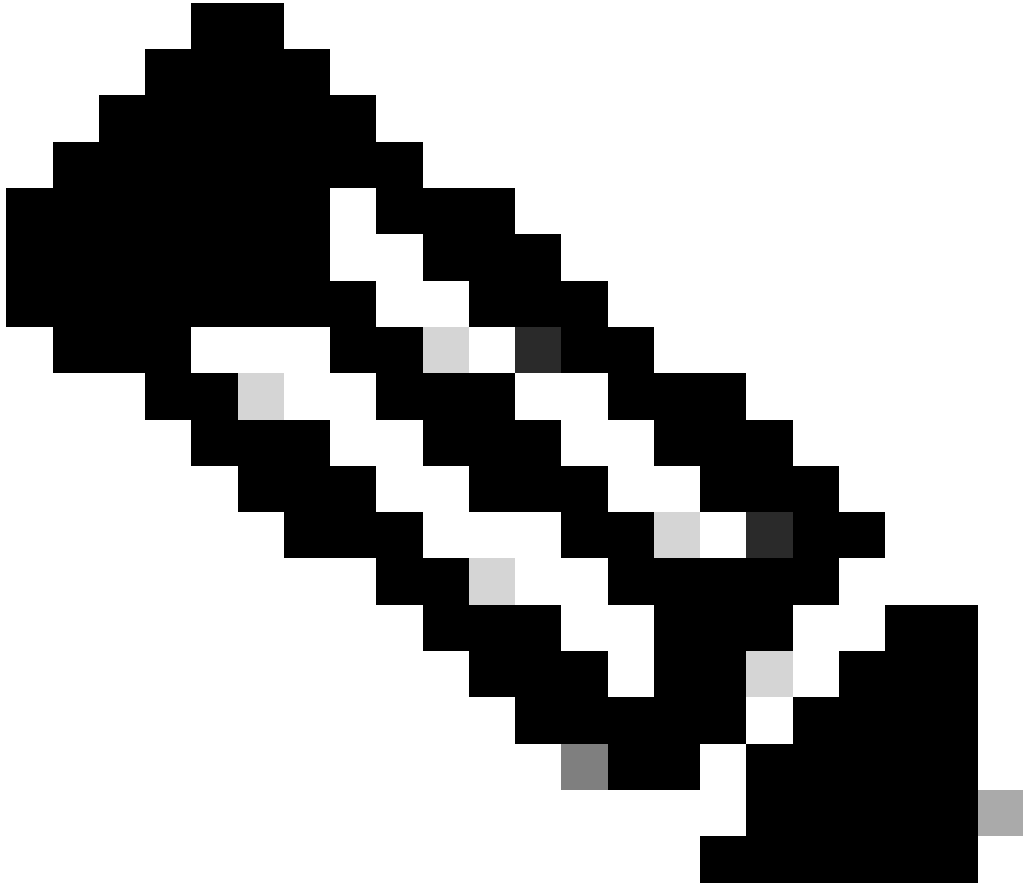
Connected

Region	Europe (Germany)
Device Type	FTD
Routing Type	Static Routing
IP Address Range	192.168.10.0/24
Last Status Update	Mar 19, 2024 11:13 AM

Step 2: 방화벽의 트래픽을 허용합니다.

Secure Access가 ISE 디바이스를 Radius 인증에 사용하도록 허용하려면 필요한 Radius 포트를 사용하여 Secure Access에서 네트워크에 대한 규칙을 구성해야 합니다.

규칙	소스	대상	Destination Port(대상 포트)
ISE에서 보안 액세스 관리 풀	ISE_서버	관리 IP 풀(RA-VPN)	COA UDP 1700(기본 포트)
ISE에 대한 보안 액세스 관리 IP 풀	관리 IP 풀	ISE_서버	인증, 권한 부여 UDP 1812(기본 포트) 어카운팅 UDP 1813(기본 포트)
ISE에 대한 보안 액세스 엔드포인트 IP 풀	엔드포인트 IP 풀	ISE_서버	프로비저닝 포털 TCP 8443(기본 포트)
DNS 서버에 대한 보안 액세스 엔드포인트 IP 풀	엔드포인트 IP 풀	DNS 서버	DNS



참고: ISE와 관련된 추가 포트를 확인하려면 [User Guide - Port Reference\(사용 설명서 - 포트 참조\)](#)를 확인하십시오.



참고: ISE가 ise.ciscosspt.es와 같은 이름을 통해 검색되도록 구성한 경우 DNS 규칙이 필요합니다.

관리 풀 및 엔드포인트 IP 풀

관리 및 엔드포인트 IP 풀을 확인하려면 [Secure Access](#) Dashboard로 [이동합니다](#).

- 클릭 **Connect > End User Connectivity**
- 클릭 **Virtual Private Network**

- 아래 **Manage IP Pools**
- **클릭 Manage**

EUROPE						1	^
Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups		
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	ISE_CSA		

3단계: ISE가 Private Resources(프라이빗 리소스)에 구성되어 있는지 확인합니다.

VPN을 통해 연결된 사용자가 탐색할 수 있도록 하려면 **ISE Provisioning Portal** VPN을 통해 의 자동 프로비저닝을 허용하는 데 사용되는 액세스를 제공하는 전용 리소스로 디바이스를 ISE Posture Module 구성해야 합니다.

ISE가 올바르게 구성되어 있는지 확인하려면 [Secure Access Dashboard](#)([보안 액세스 대시보드](#))로 이동합니다.

- **클릭 Resources > Private Resources**
- ISE 리소스를 클릭합니다

Private Resource Name

CiscoISE

Description (optional)

Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address.

[Help](#)

Internally reachable address

(FQDN, Wildcard FQDN, IP Address, CIDR)



Protocol

Port / Ranges

[+ Protocol & Port](#)

192.168.10.206

TCP - (HTTP/HTTPS)

Any

[+ IP Address or FQDN](#)

VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN.

필요한 경우 프로비저닝 포털 포트(8443)로 규칙을 제한할 수 있습니다.

참고: VPN 연결에 대한 확인란을 선택했는지 확인하십시오.

4단계: 액세스 정책에서 ISE 액세스 허용

VPN을 통해 연결된 사용자가 탐색할 수 있도록 **ISE Provisioning Portal**하려면 해당 규칙에 따라 구성된 사용자가 **Access Policy** 에 구성된 Private Resource에 액세스할 수 있도록 를 구성해야 합니다Step3.

ISE가 올바르게 구성되어 있는지 확인하려면 [Secure Access Dashboard](#)([보안 액세스 대시보드](#))로 이동합니다.



- 클릭 **Secure > Access Policy**

- VPN 사용자에게 ISE에 대한 액세스를 허용하도록 구성된 규칙을 클릭합니다

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)


Action

<p> Allow Allow specified traffic if security requirements are met.</p>	<p> Block Block specified traffic.</p>
---	--


<p>From Specify one or more sources.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> CSA (ciscospt.es\CSA) × × </div> <p><small>Information about sources, including selecting multiple sources. Help</small></p>	<p>To Specify one or more destinations.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> CiscoISE × × </div> <p><small>Information about destinations, including selecting multiple destinations. Help</small></p>
--	--

Endpoint Requirements

For VPN connections:

 End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ⓘ
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:

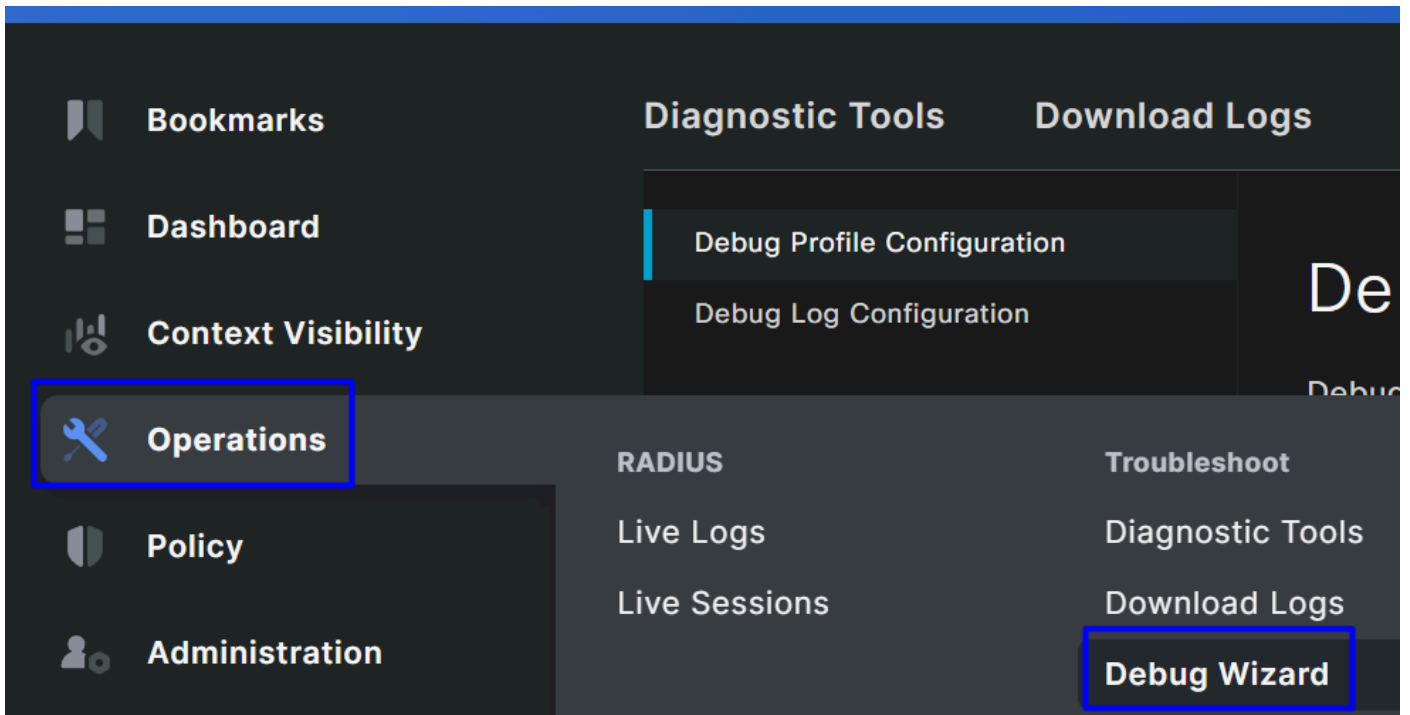
 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

문제 해결

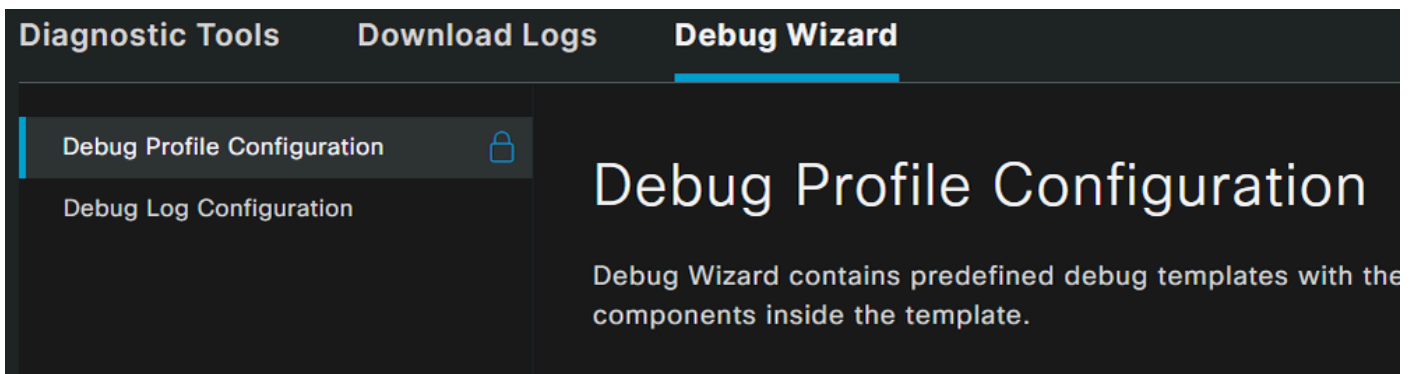
ISE Posture 디버그 로그를 다운로드하는 방법

ISE 로그를 다운로드하여 포스터와 관련된 문제를 확인하려면 다음 단계를 진행하십시오.

- ISE 대시보드로 이동
- 클릭 Operations > Troubleshoot > Debug Wizard



- 클릭 Debug Profile Configuration



- 확인란을 선택합니다. Posture > Debug Nodes



Add



Edit



Remove 2



Debug Nodes



Name

Des



802.1X/MAB

802



Active Directory

Acti



Application Server Issues

App



BYOD portal/Onboarding

BYO



Context Visibility

Con



Guest portal

Gue



Licensing

Lice



MnT

MnT

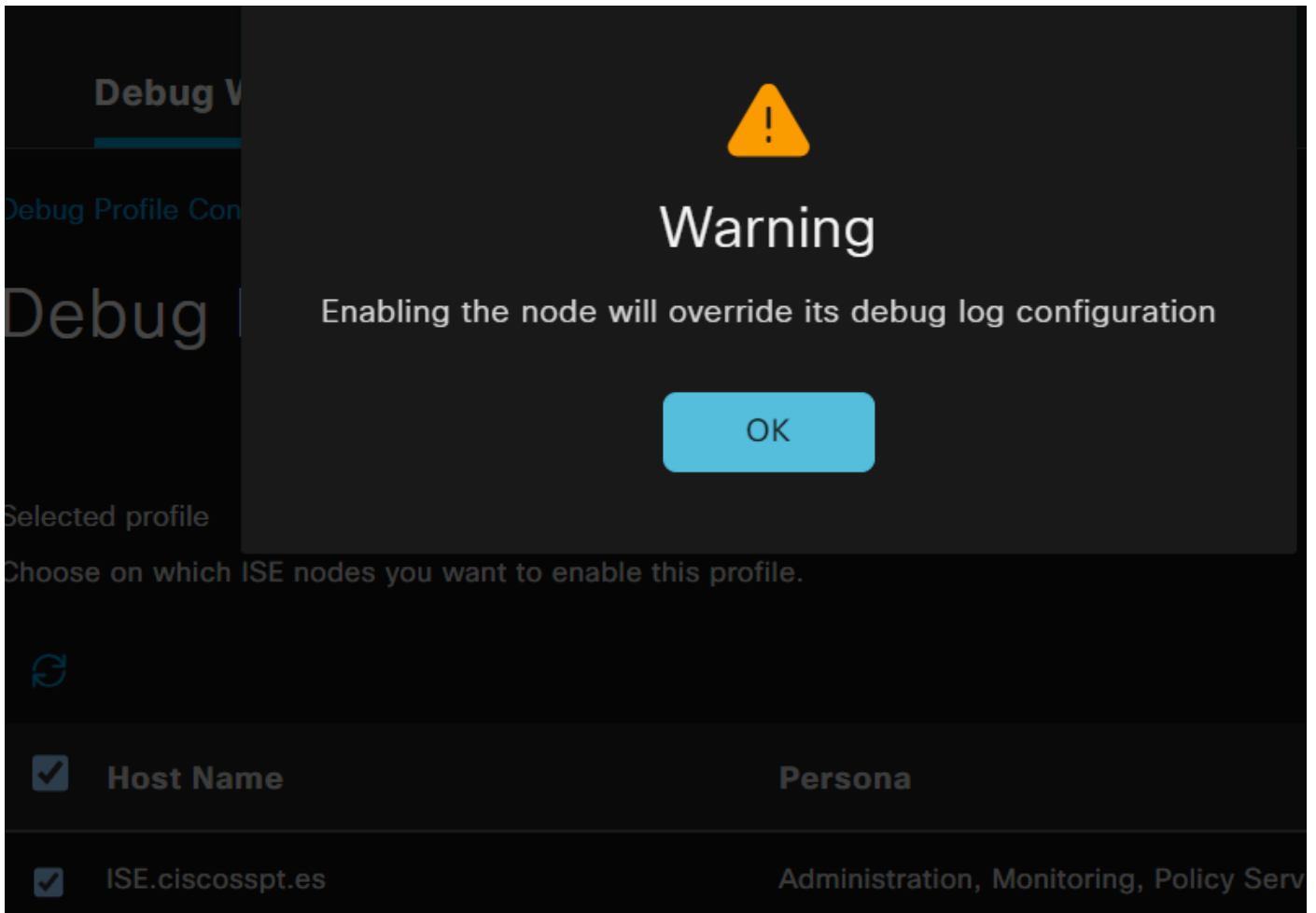
1



Posture

Pos

- 문제를 해결하기 위해 디버그 모드를 활성화할 ISE 노드의 확인란을 선택합니다



The image shows a warning dialog box overlaid on a configuration interface. The dialog box has a dark background and a yellow warning triangle icon at the top center. The text inside the dialog box reads: "Warning" in large white font, followed by "Enabling the node will override its debug log configuration" in smaller white font. At the bottom of the dialog box is a blue button with the text "OK".

Debug V

Debug Profile Con

Debug

Selected profile

Choose on which ISE nodes you want to enable this profile.

Host Name Persona

ISE.ciscosspt.es Administration, Monitoring, Policy Serv

- 클릭 Save

Debug Nodes

Selected profile Posture

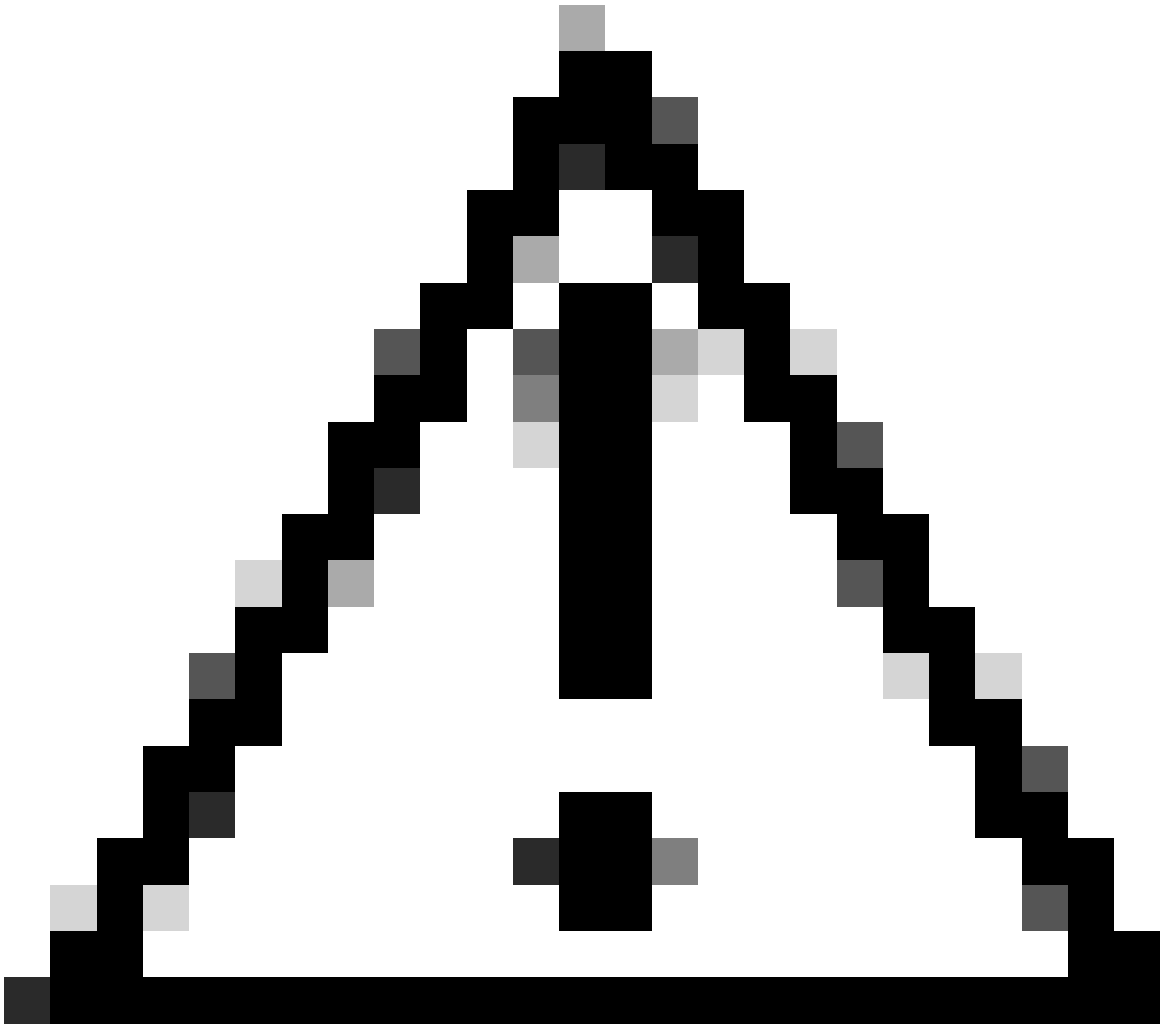
Choose on which ISE nodes you want to enable this profile.

 Filter  

<input checked="" type="checkbox"/> Host Name	Persona	Role
<input checked="" type="checkbox"/> ISE.ciscosppt.es	Administration, Monitoring, Policy Service	STANDALONE

Cancel

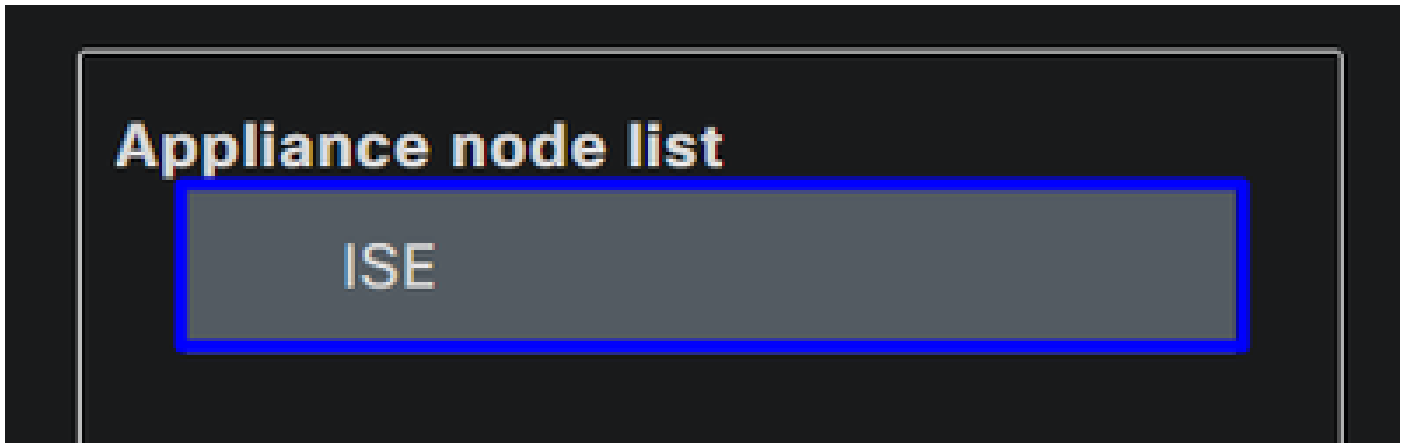
Save



주의: 이 시점 이후에는 문제를 재현해야 합니다. **the debug logs can affect the performance of your device.**

문제를 재현한 후 다음 단계를 진행합니다.

- 클릭 Operations > Download Logs
- 로그를 가져올 노드를 선택합니다



- 에서 **Support Bundle** 다음 옵션을 선택합니다.

Support Bundle

Debug Logs

- Include full configuration database ⓘ
- Include debug logs ⓘ
- Include local logs ⓘ
- Include core files ⓘ
- Include monitoring and reporting logs ⓘ
- Include system logs ⓘ
- Include policy configuration ⓘ
- Include policy cache ⓘ

From Date

(mm/dd/yyyy)

To Date

(mm/dd/yyyy)

* Note: Output from the 'show tech-support' CLI command will be included along with the selected entries.

Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

* Encryption key ⓘ

* Re-Enter Encryption key

Create Support Bundle

- Include debug logs
- 아래 **Support Bundle Encryption**
 - **Shared Key Encryption**
 - 채우기 **Encryption key** 및 **Re-Enter Encryption key**

- 클릭 Create Support Bundle
- 클릭 Download

Support Bundle - Last Generated

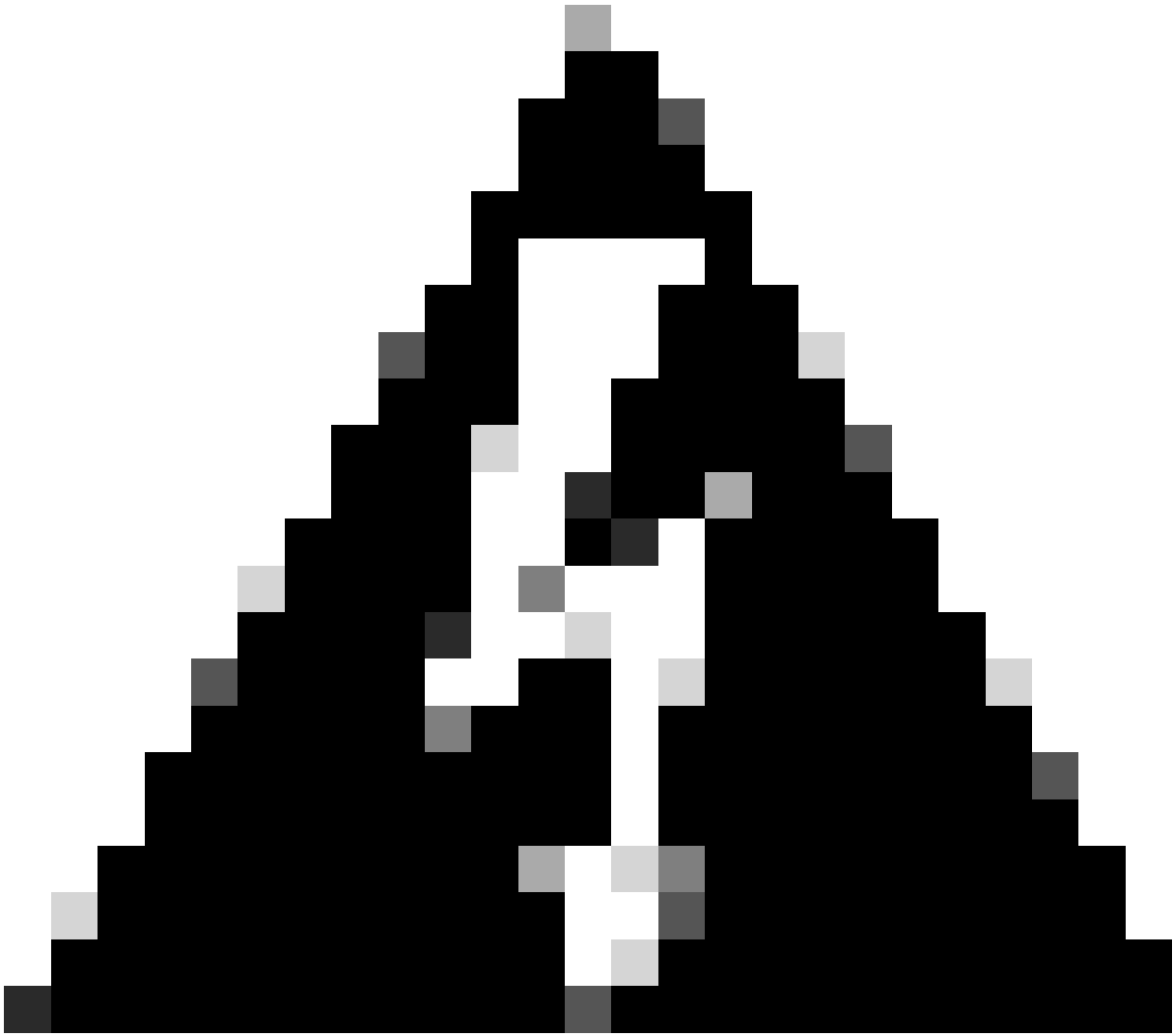
File Name: ise-support-bundle-ISE-admin-04-04-2024-14-27.tar.gpg

Time: Thu, 04 Apr 2024 14:35:35 UTC

Size(KB): 52165.0

Download

Delete


















경고: 디버그 프로필 컨피그레이션 단계에서 활성화된 디버그 [모드를 비활성화합니다.](#)

보안 액세스 원격 액세스 로그를 확인하는 방법

Secure Access Dashboard로 이동합니다.

- 클릭 Monitor > Remote Access Logs

100 Events

User	Connection Event	Event Details	Internal IP Address
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.1
<i>Unknown Identity</i>	 Failed	AUTHORIZATION-CHECK	

보안 클라이언트에서 DART 번들 생성

시스템에서 DART 번들을 생성하려면 다음 문서를 확인하십시오.

[Cisco Secure Client Diagnostic and Reporting Tool\(DART\)](#)



참고: 문제 해결 섹션에 나와 있는 로그를 수집했으면 와 함께 케이스TAC 를 열어 정보 분석을 진행하십시오.

관련 정보

- [Cisco 기술 지원 및 다운로드](#)
- [Secure Access 설명서 및 사용 설명서](#)

- [Cisco Secure Client Software 다운로드](#)
- [Cisco Identity Services Engine 관리자 가이드, 릴리스 3.3](#)

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.