FlexVPN 원격 사용자에 대한 RADIUS 특성 매핑 구성

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)를 사용하여 ID를 확인하고 특성 그룹 매핑을 수행하도록 FlexVPN을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CLI를 통해 Cisco IOS® XE 라우터에서 IKEV2/IPsec 컨피그레이션을 사용하는 RAVPN(Remote Access Virtual Private Network)
- Cisco ISE(Identity Services Engine) 컨피그레이션
- CSC(Cisco Secure Client)
- RADIUS 프로토콜

사용되는 구성 요소

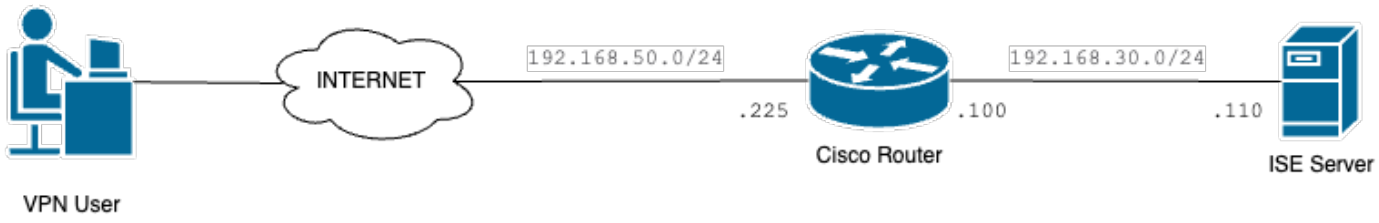
이 문서는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco CSR1000V(VXE) - 버전 17.03.04a
- Cisco ISE(Identity Services Engine) - 3.1
- CSC(Cisco Secure Client) - 버전 5.0.05040
- Windows 11

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

네트워크 다이어그램



기본 네트워크 다이어그램

설정

라우터 컨피그레이션

1단계. 디바이스에서 인증 및 로컬 권한 부여를 위해 RADIUS 서버를 구성합니다.

```
aaa new-model
aaa group server radius FlexVPN-Authentication-Server
server-private 192.168.30.110 key Cisco123
aaa authentication login FlexVPN-Authentication-List group FlexVPN-Authentication-Server
aaa authorization network FlexVPN-Authorization-List local
```

aaa authentication login <list_name> 명령은 RADIUS 서버를 정의하는 AAA(authentication, authorization, and accounting) 그룹을 참조합니다.

aaa authorization network <list_name> local 명령은 로컬로 정의된 사용자/그룹을 사용한다고 말합니다.

2단계. 라우터 인증서를 저장할 신뢰 지점을 구성합니다. 라우터의 로컬 인증은 RSA 유형이므로 디바이스에서 다음과 같이 인증서를 사용하여 서버를 인증해야 합니다.

```
crypto pki trustpoint FlexVPN-TP
enrollment url http://192.168.50.230:80
subject-name CN=192.168.50.225
```

```
revocation-check none
rsakeypair FlexVPN_KEY
```

3단계. 서로 다른 각 사용자 그룹에 대한 IP 로컬 풀을 정의합니다.

```
ip local pool group1 172.16.10.1 172.16.10.50
ip local pool group2 172.16.20.1 172.16.20.50
```

4단계. 로컬 권한 부여 정책을 구성합니다.

```
crypto ikev2 authorization policy FlexVPN-Local-Policy
```

인증 서버는 사용자가 속한 그룹을 기반으로 관련 값(DNS, 풀, 보호 경로 등)을 전송하므로 권한 부여 정책에 대한 컨피그레이션이 필요하지 않습니다. 그러나 로컬 권한 부여 데이터베이스에서 사용자 이름을 정의 하도록 구성 되어야 합니다.

5단계(선택 사항) IKEv2 제안서 및 정책을 생성합니다(구성되지 않은 경우 스마트 기본값이 사용됨).

```
crypto ikev2 proposal IKEv2-prop
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy IKEv2-pol
 proposal IKEv2-prop
```

6단계(선택 사항) 변형 집합을 구성합니다(구성되지 않은 경우 스마트 기본값이 사용됨).

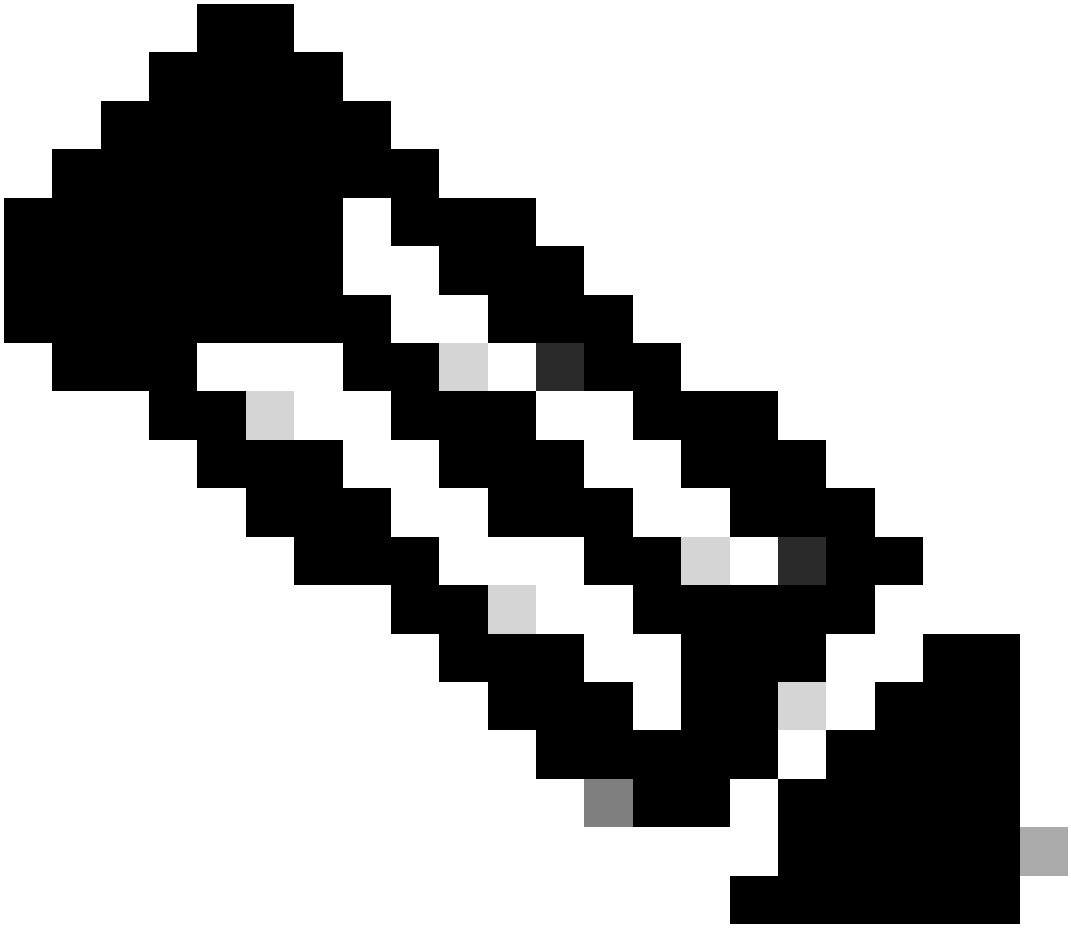
```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel
```

7단계. 연결에 사용되는 적절한 로컬 및 원격 ID, 인증 방법(로컬 및 원격), 신뢰 지점, AAA 및 가상 템플릿 인터페이스를 사용하여 IKEv2 프로필을 구성합니다.

```
crypto ikev2 profile FlexVPN-IKEv2-Profile
match identity remote key-id cisco.example
```

```
identity local dn
authentication local rsa-sig
authentication remote eap query-identity
pki trustpoint FlexVPN-TP
aaa authentication eap FlexVPN-Authentication-List
aaa authorization group eap list FlexVPN-Authorization-List FlexVPN-Local-Policy
aaa authorization user eap cached
virtual-template 100
```

aaa authorization user eap cached 명령은 EAP 인증 중에 받은 특성을 캐시하도록 지정합니다. 이 명령이 없으면 인증 서버에서 보낸 데이터가 사용되지 않아 연결에 실패하기 때문에 이 명령은 컨피그레이션에 필수적입니다.



참고: 원격 key-id는 XML 파일의 key-id 값과 일치해야 합니다. XML 파일에서 수정되지 않은 경우 기본값(*$AnyConnectClient$*)이 사용되며 IKEv2 프로파일에서 구성해야 합니다.

8단계. IPsec 프로필을 구성하고 변형 집합 및 IKEv2 프로필을 할당합니다.

```
crypto ipsec profile FlexVPN-IPsec-Profile
set transform-set TS
set ikev2-profile FlexVPN-IKEv2-Profile
```

9단계. 루프백 인터페이스를 구성합니다. 가상 액세스 인터페이스는 다음에서 IP 주소를 차입합니다.

```
interface Loopback100
ip address 10.0.0.1 255.255.255.255
```

10단계. 다른 가상 액세스 인터페이스를 생성하는 데 사용할 가상 템플릿을 생성하고 8단계에서 생성한 IPSec 프로필을 연결합니다.

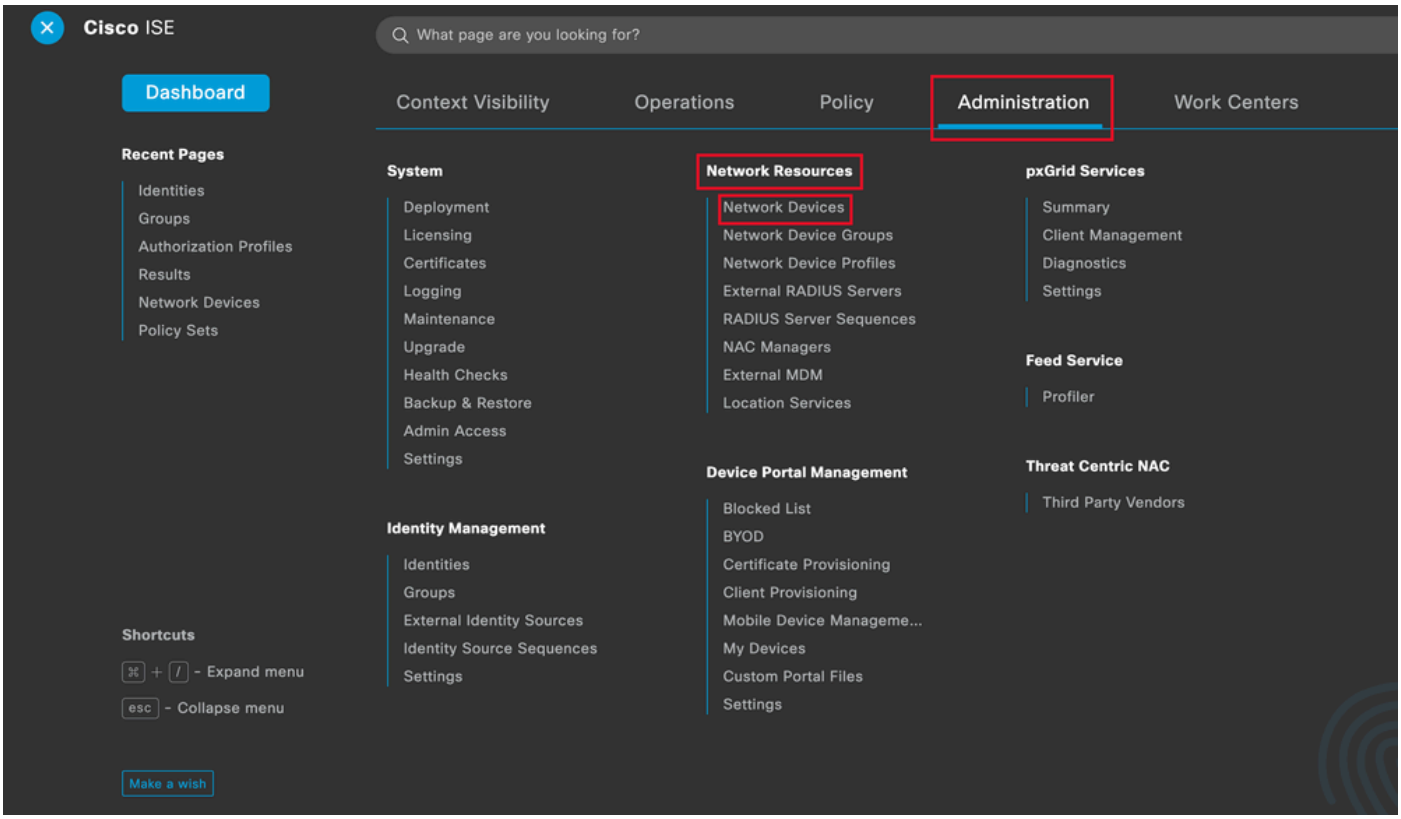
```
interface Virtual-Template100 type tunnel
ip unnumbered Loopback100
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

11단계. 라우터에서 HTTP-URL 기반 인증서 조회 및 HTTP 서버를 비활성화합니다.

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

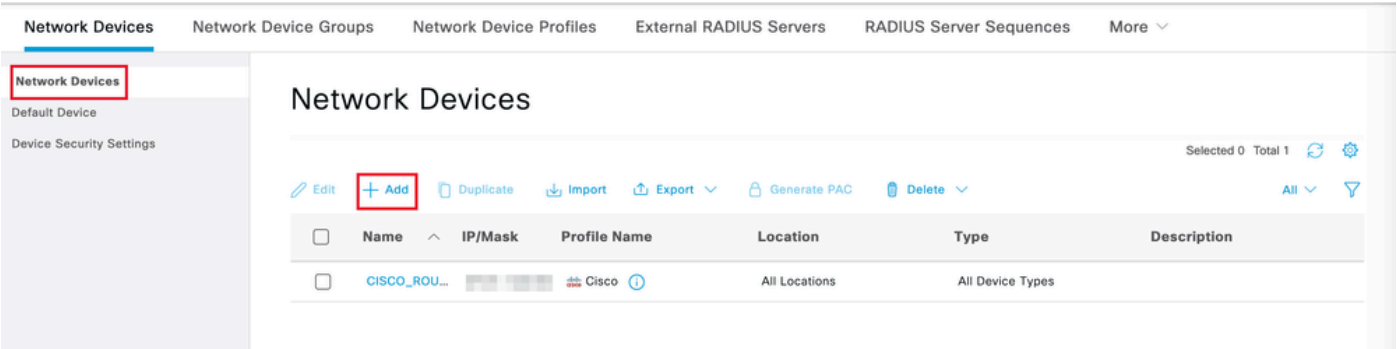
ISE(Identity Services Engine) 컨피그레이션

1단계. ISE 서버에 로그인하고 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다.



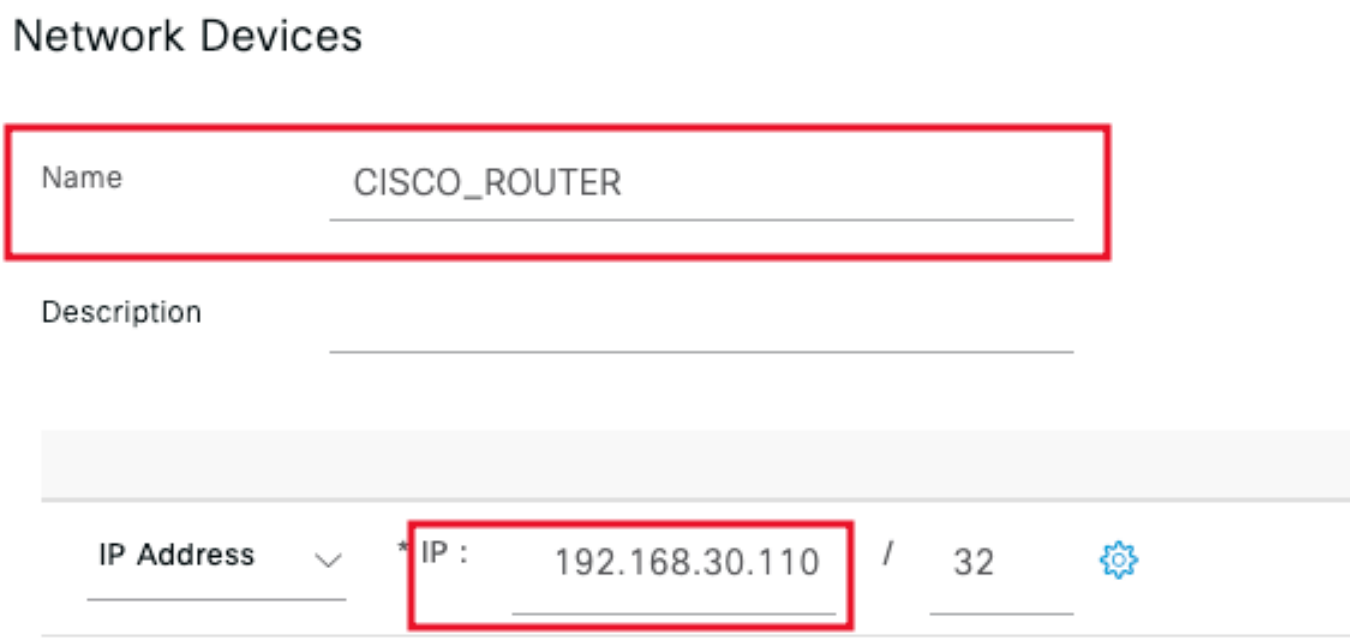
ISE 일반 메뉴

2단계. 라우터를 AAA 클라이언트로 구성하려면 Add(추가)를 클릭합니다.

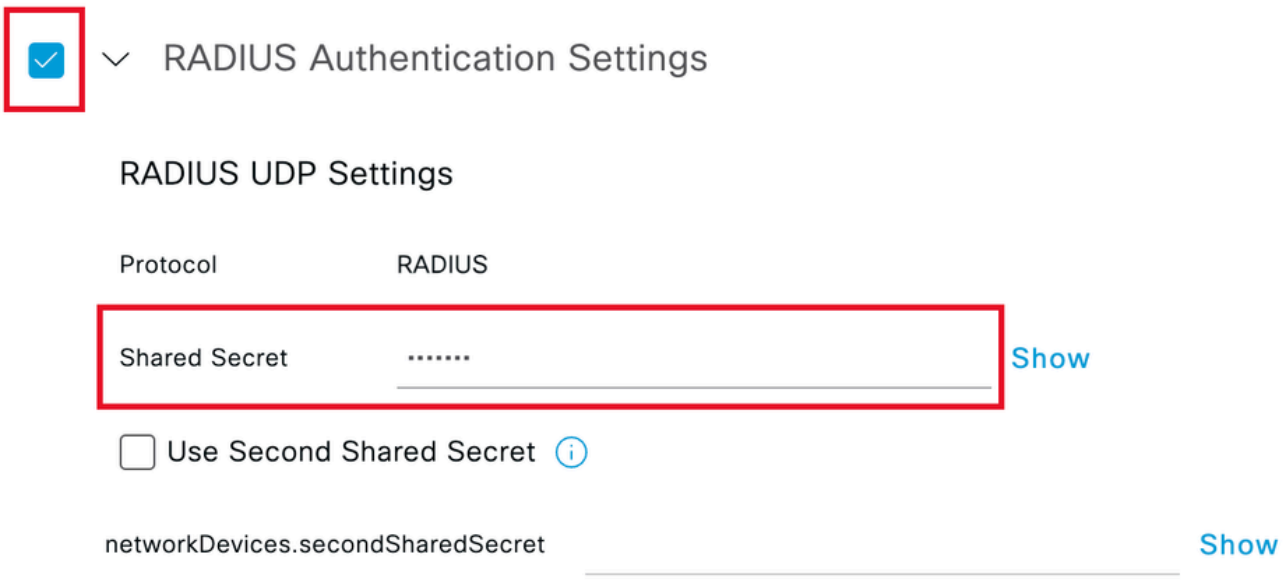


새 네트워크 디바이스 추가

네트워크 디바이스 이름 및 IP 주소 필드를 입력한 다음 RADIUS 인증 설정 상자를 선택하고 공유 암호를 추가합니다. 이 값은 라우터의 RADIUS 서버 개체를 만들 때 사용된 값과 같아야 합니다.



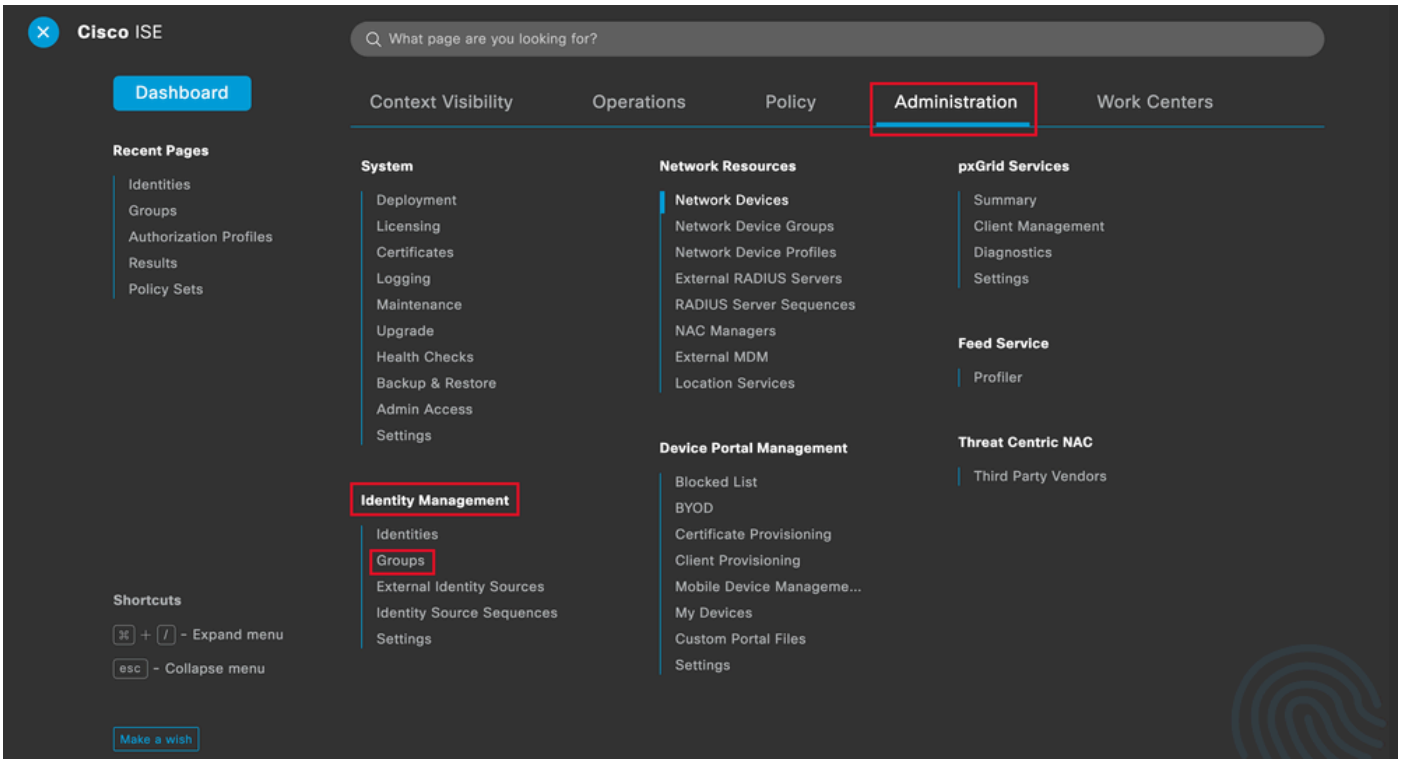
이름 및 IP 주소



Radius 비밀번호

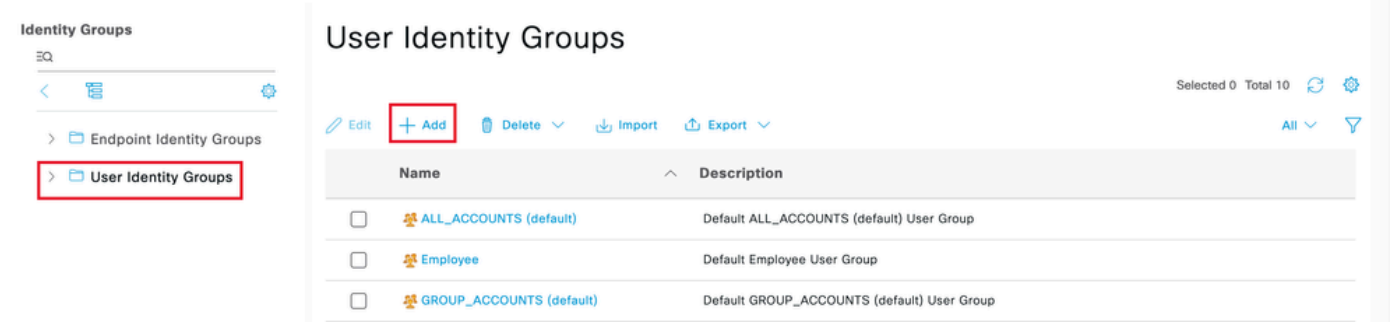
저장을 클릭합니다.

3단계. Administration(관리) > Identity Management(ID 관리) > Groups(그룹)로 이동합니다.



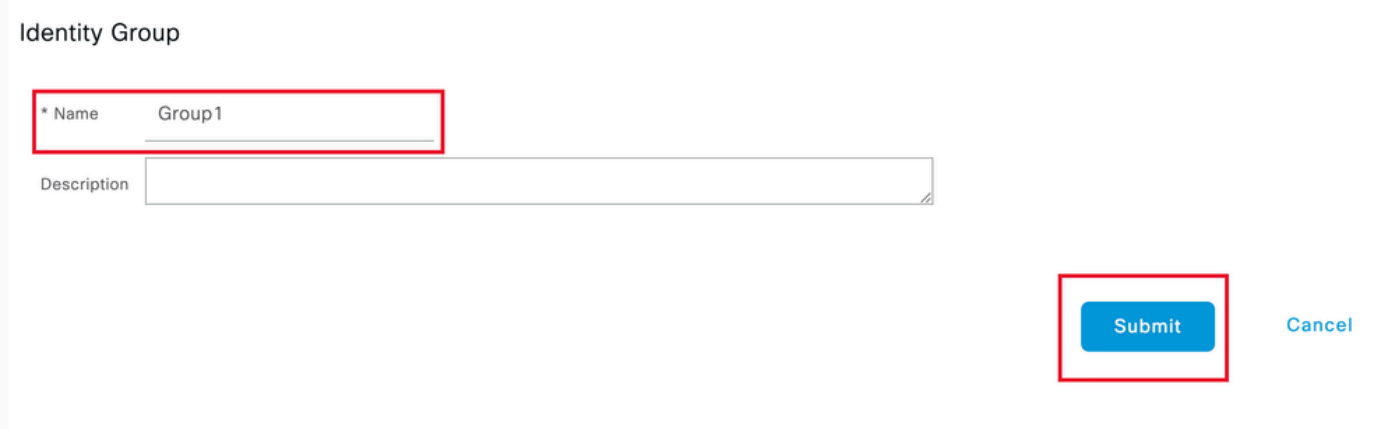
ISE 일반 메뉴

4단계. User Identity Groups(사용자 ID 그룹)를 클릭한 다음 Add(추가)를 클릭합니다.

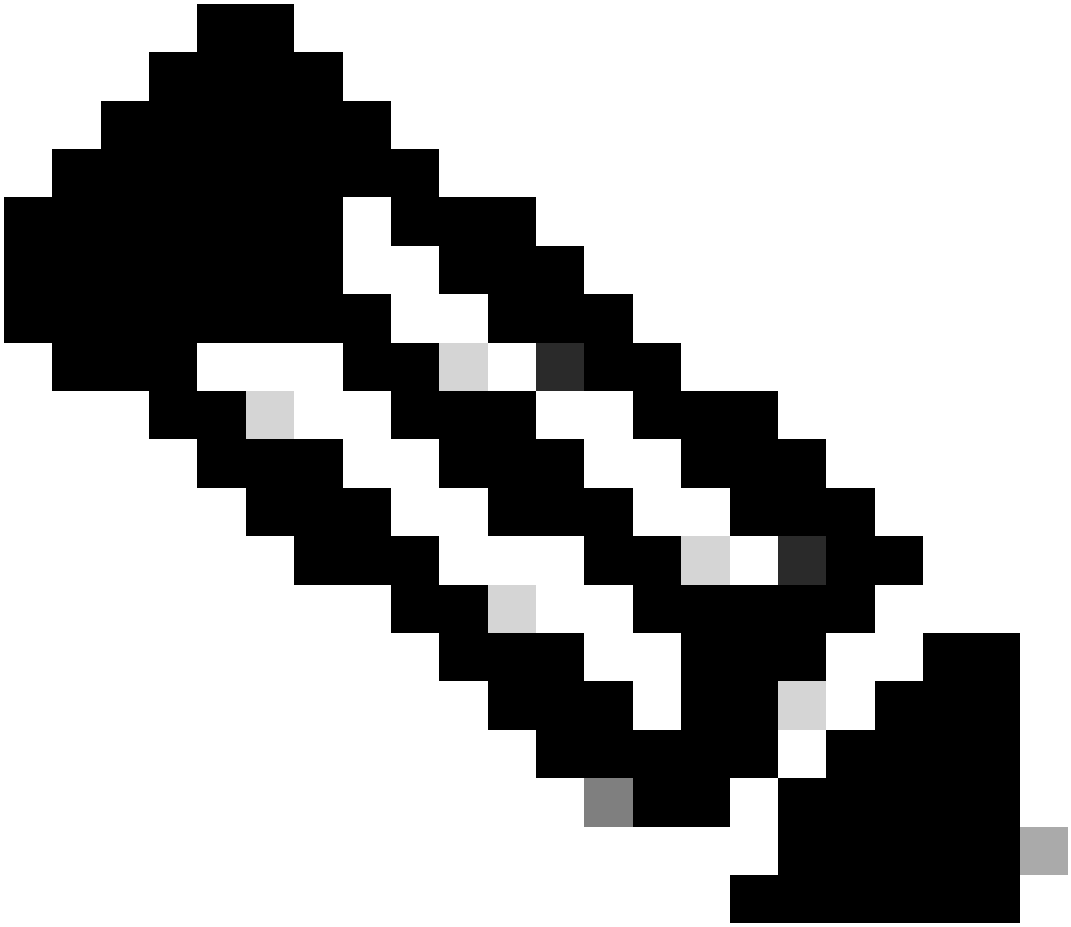


새 그룹 추가

그룹 이름을 입력하고 Submit(제출)을 클릭합니다.

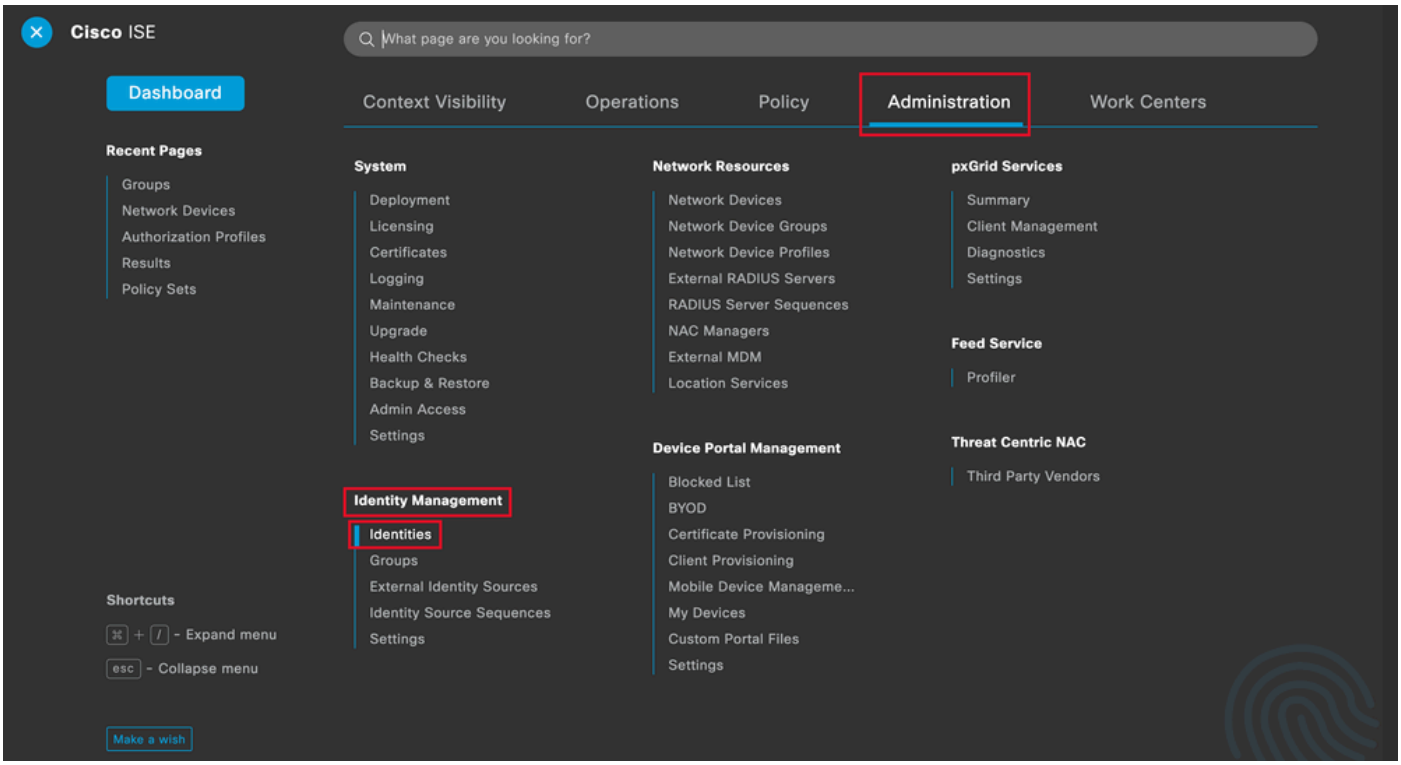


그룹 정보



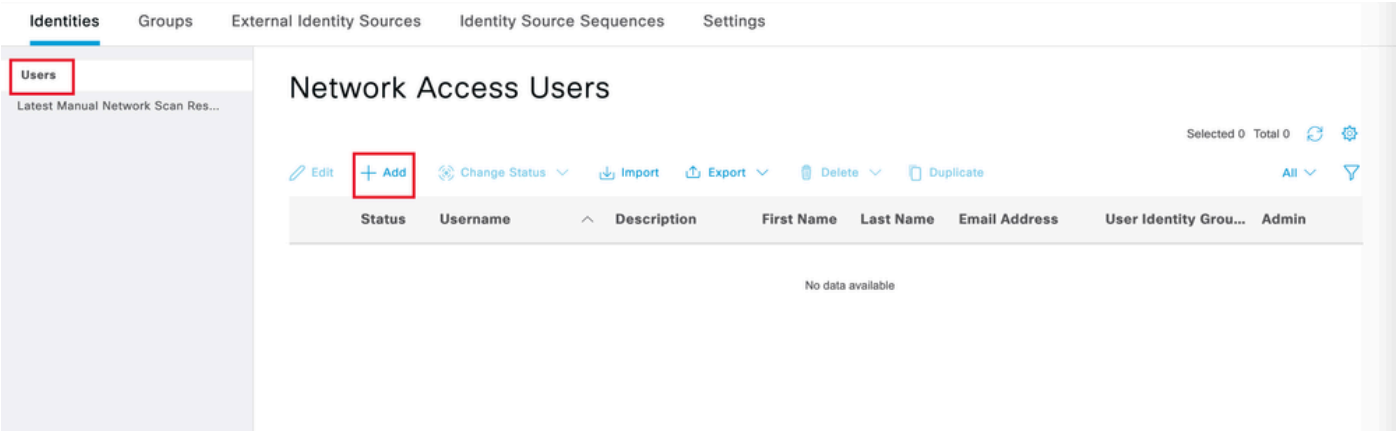
참고: 3단계와 4단계를 반복하여 필요한 만큼 그룹을 생성합니다.

5단계. Administration(관리) > Identity Management(ID 관리) > Identities(ID)로 이동합니다.



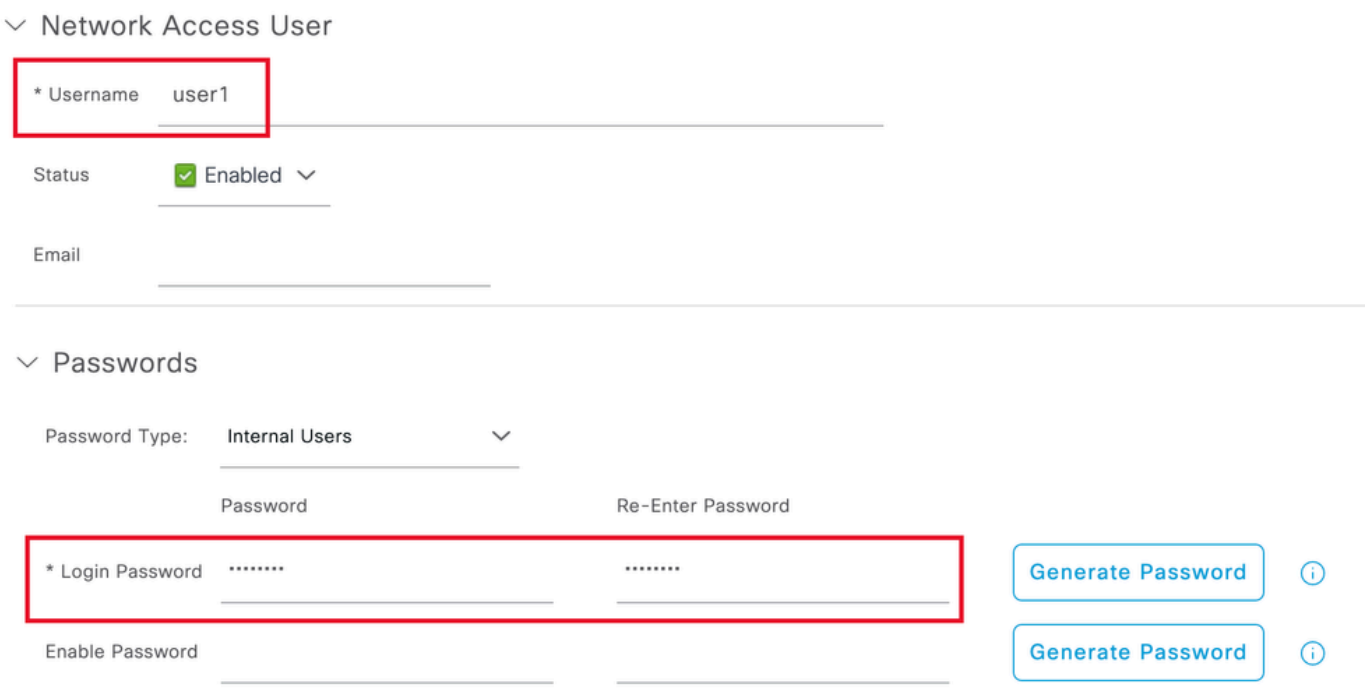
ISE 일반 메뉴

6단계. 서버 로컬 데이터베이스에서 새 사용자를 만들려면 Add(추가)를 클릭합니다.

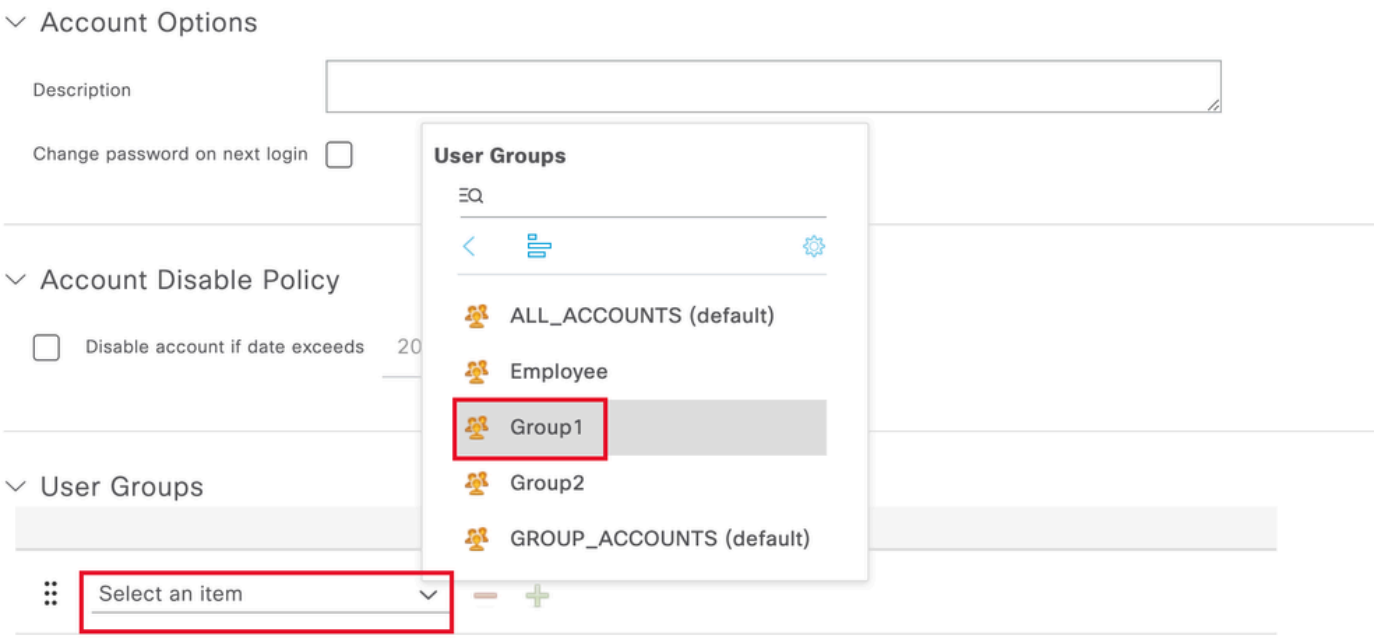


사용자 추가

사용자 이름 및 로그인 비밀번호를 입력합니다. 그런 다음 이 페이지의 끝으로 이동하여 사용자 그룹을 선택합니다.

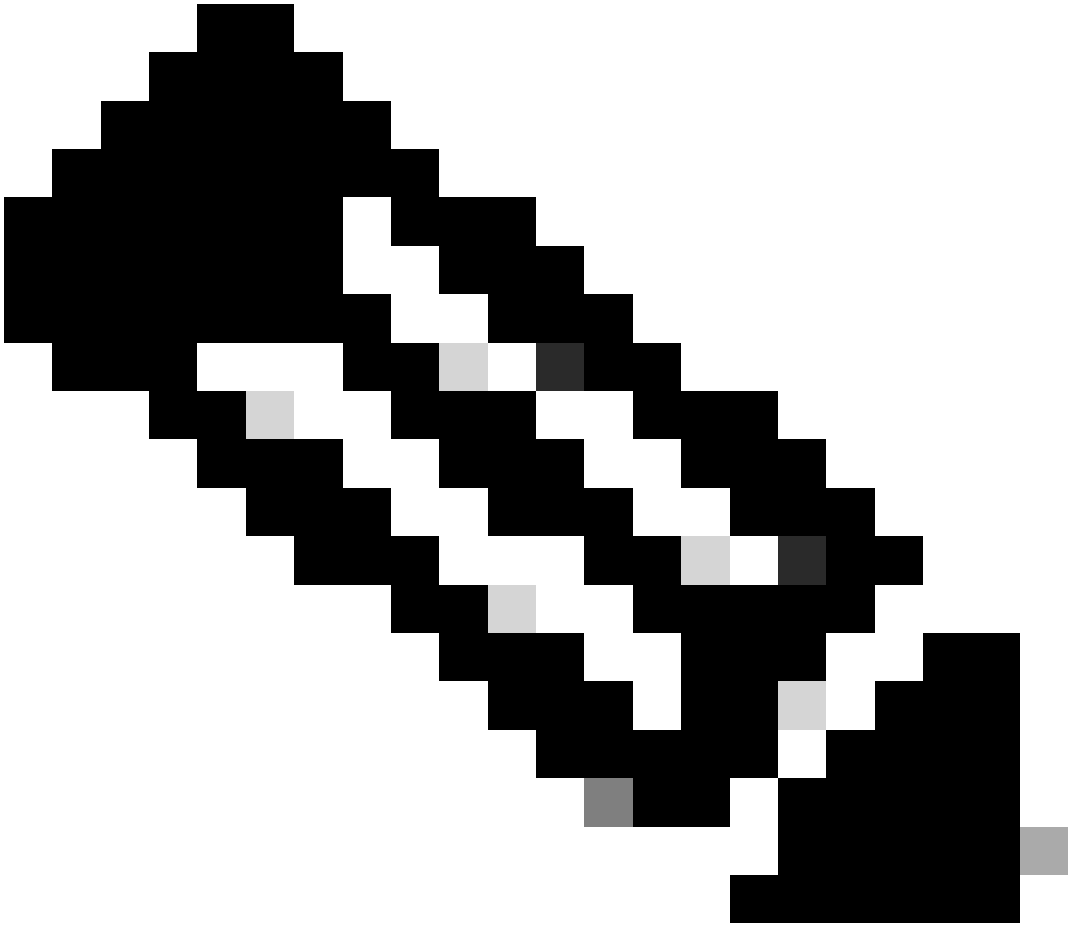


사용자 이름 및 비밀번호



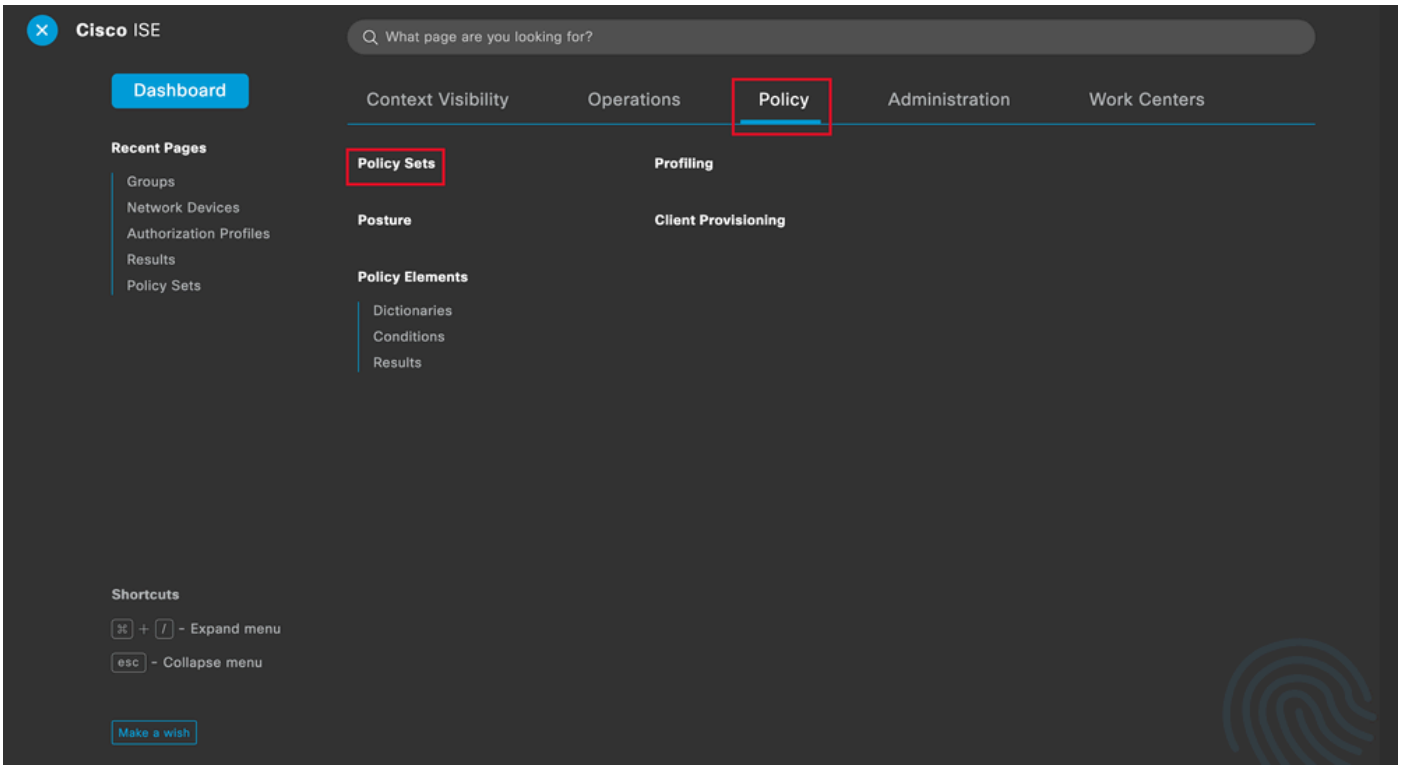
사용자에게 올바른 그룹 할당

저장을 클릭합니다.



참고: 5단계와 6단계를 반복하여 필요한 사용자를 생성하고 해당 그룹에 할당합니다.

7단계. Policy(정책) > Policy Sets(정책 집합)로 이동합니다.

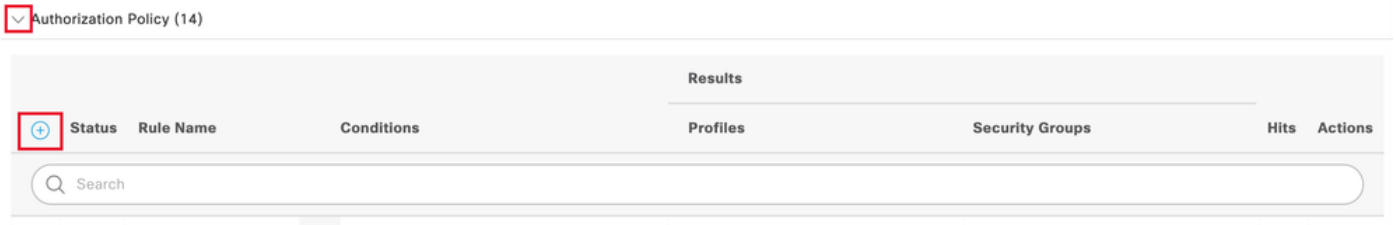


ISE 일반 메뉴

화면 오른쪽 화살표를 클릭하여 기본 권한 부여 정책을 선택합니다.

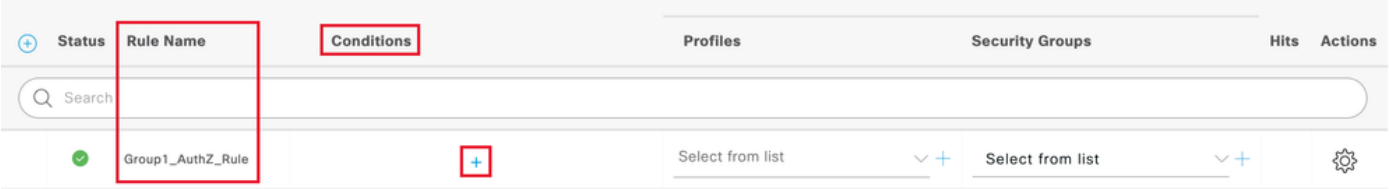
권한 부여 정책 선택

8단계. 권한 부여 정책 옆의 드롭다운 메뉴 화살표를 클릭하여 확장합니다. 새 규칙을 추가하려면 add(+) 아이콘을 클릭합니다.



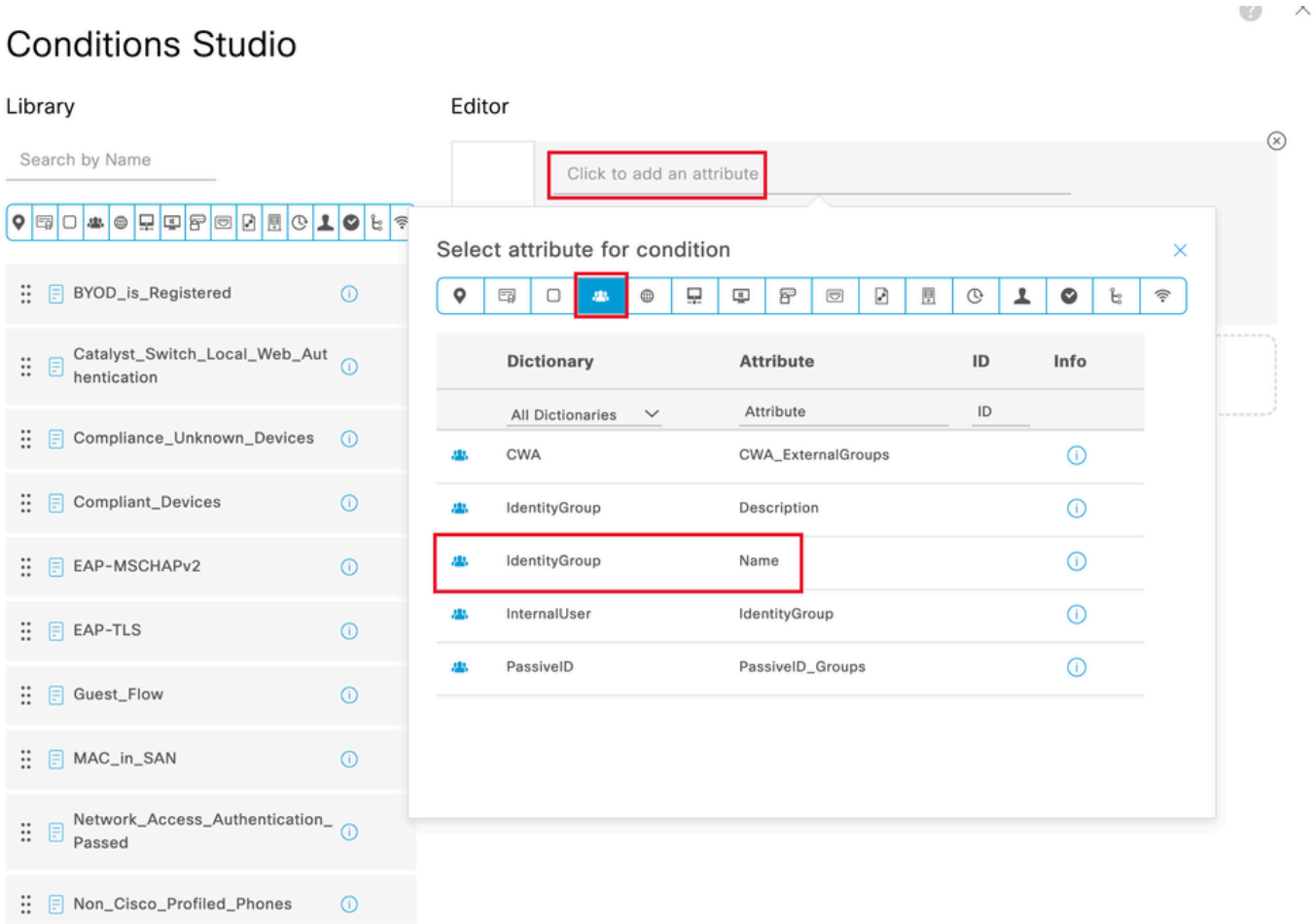
새 권한 부여 규칙 추가

규칙의 이름을 입력하고 Conditions(조건) 열에서 add(+) 아이콘을 선택합니다.



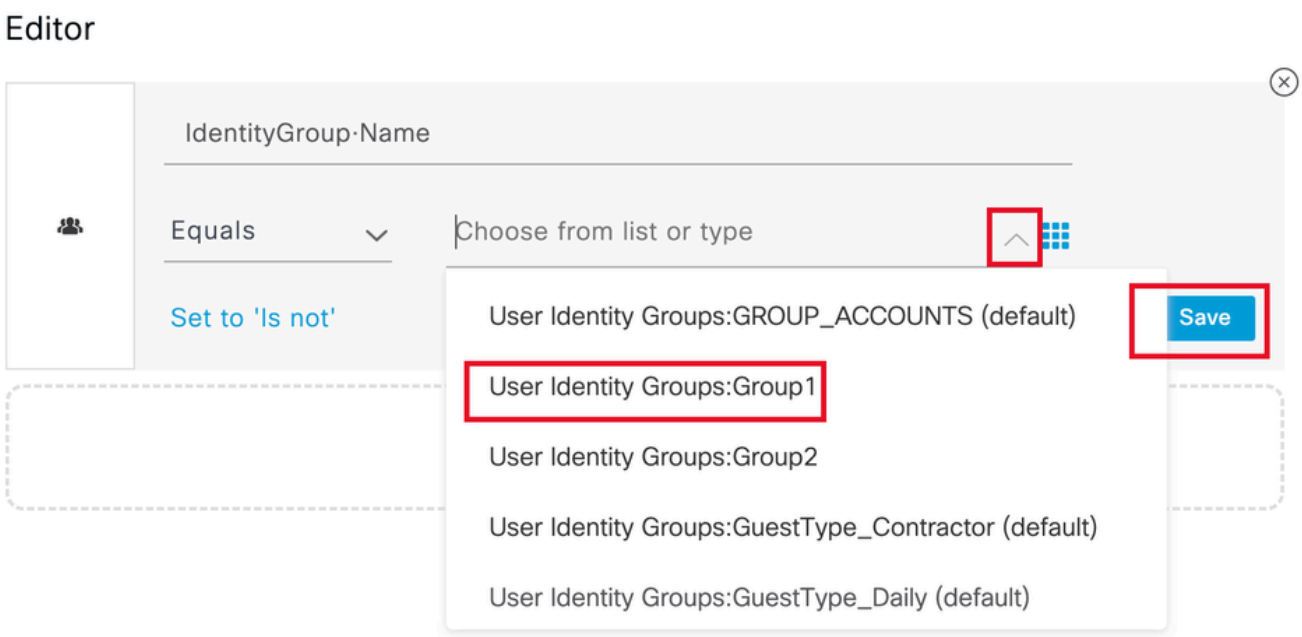
조건 추가

9단계. 속성 편집기 텍스트 상자를 클릭하고 ID 그룹을 클릭합니다. ID 그룹 - 이름 특성을 선택합니다.



조건 선택

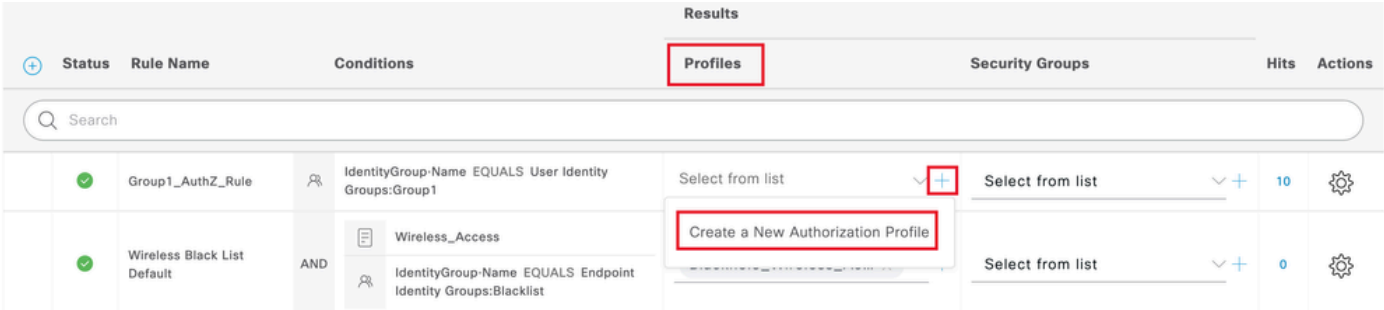
Equalas(같음)를 선택한 다음 드롭다운 메뉴 화살표를 클릭하여 사용 가능한 옵션을 표시하고 User Identity Groups:<GROUP_NAME>을 선택합니다.



그룹 선택

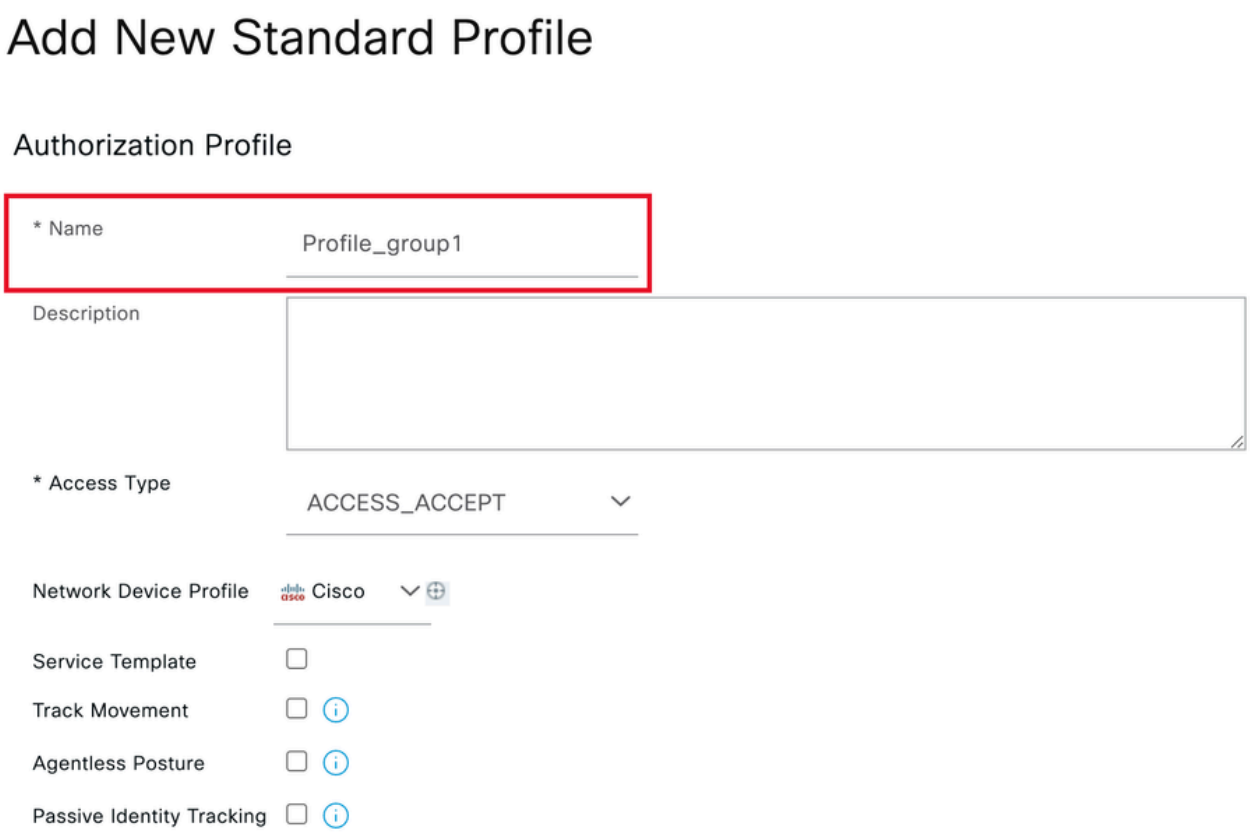
저장을 클릭합니다.

10단계. Profiles(프로파일) 열에서 추가(+) 아이콘을 클릭하고 Create a New Authorization Profile(새 권한 부여 프로파일 생성)을 선택합니다.



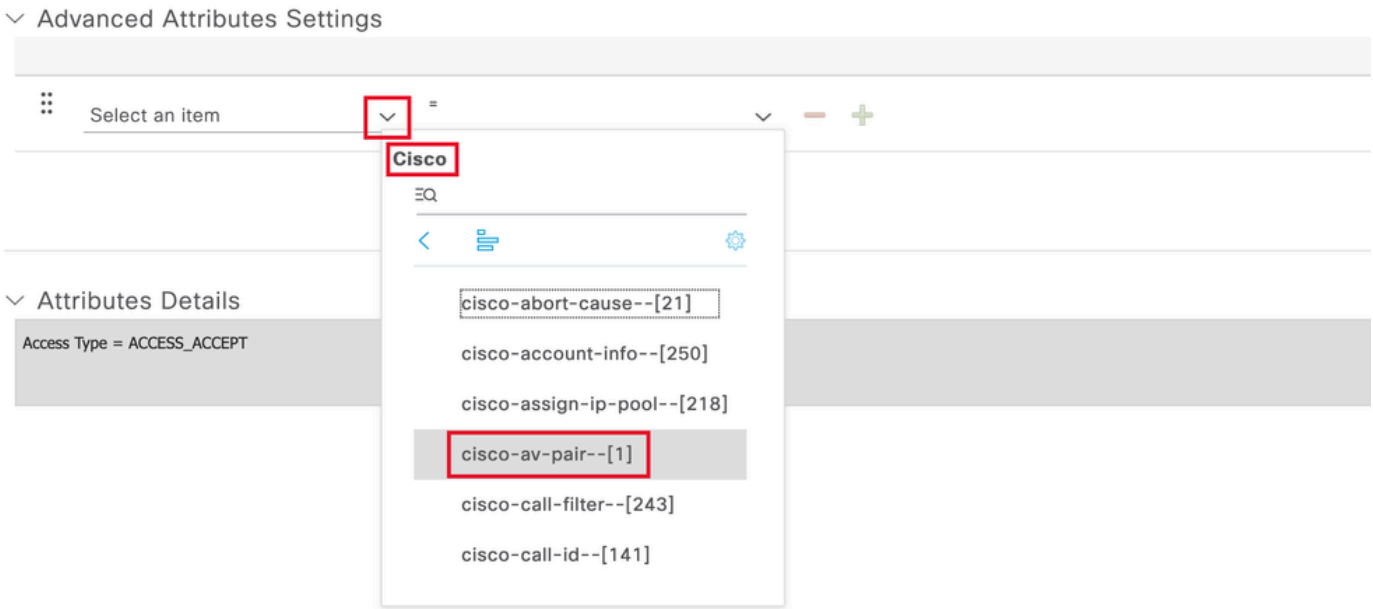
권한 부여 프로파일 생성

프로파일 이름 입력



프로필 정보

이 페이지의 끝으로 이동하여 고급 속성 설정을 찾아 드롭다운 메뉴 화살표를 클릭합니다. 그런 다음 Cisco를 클릭하고 cisco-av-pair—[1]을 선택합니다.

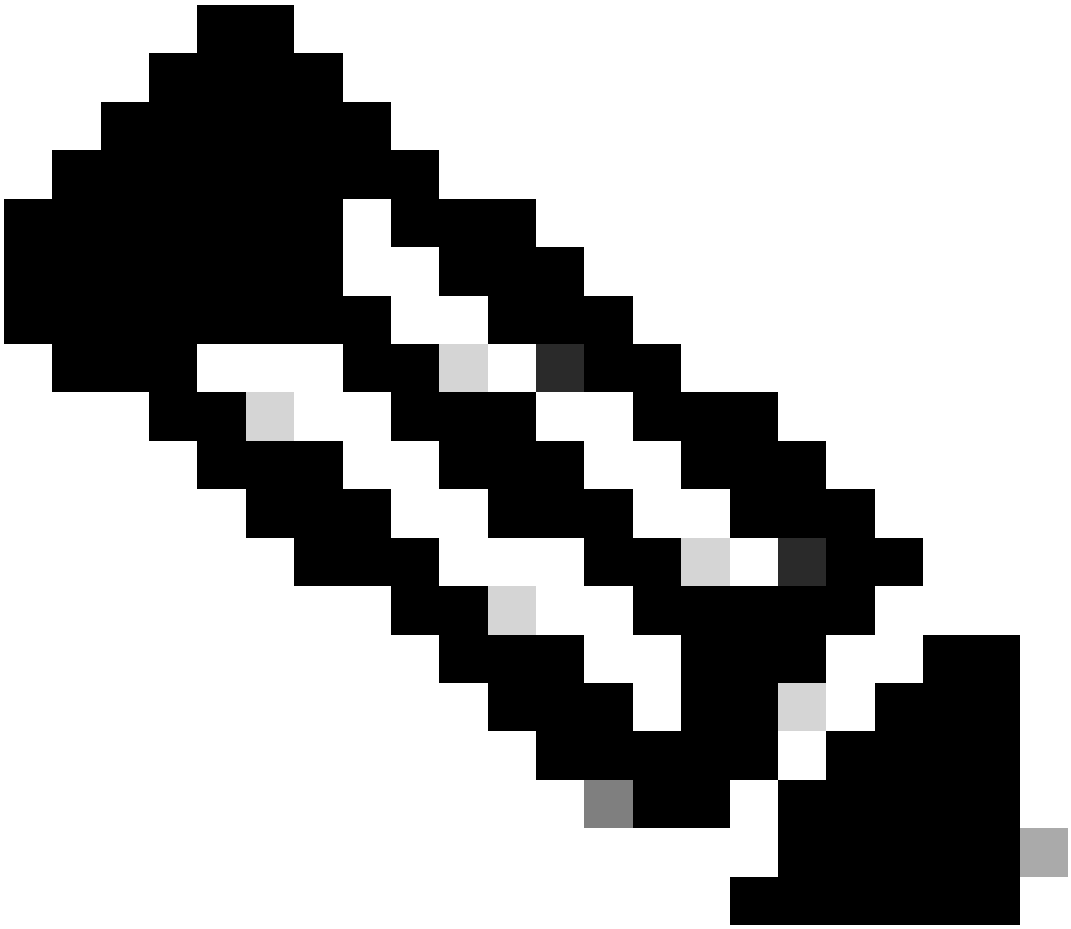


Attribute Type(특성 유형)을 선택합니다

.

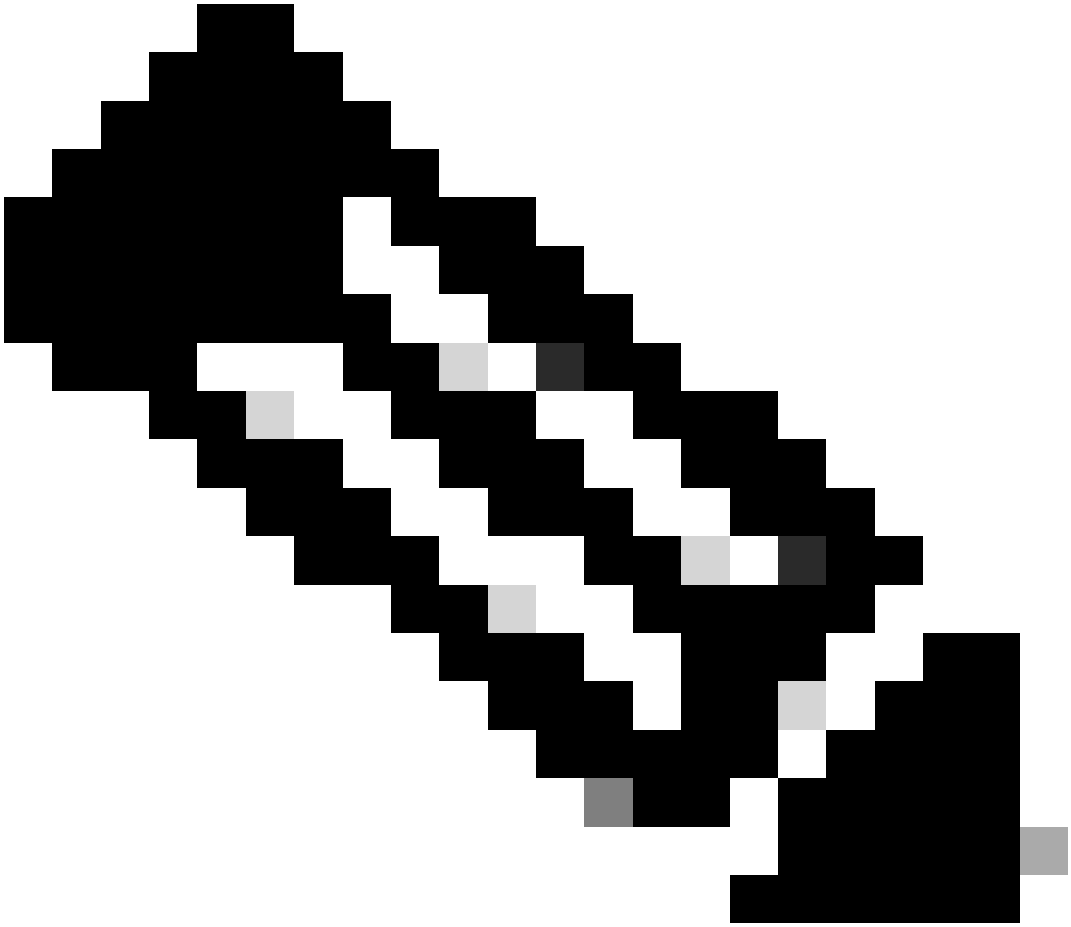
구성할 cisco-av-pair 특성을 추가하고 추가 (+) 아이콘을 클릭하여 다른 특성을 추가합니다.

특성 구성



참고: 특성 사양(이름, 구문, 설명, 예 등)은 FlexVPN RADIUS 특성 컨피그레이션 가이드를 참조하십시오.

[FlexVPN 및 인터넷 키 교환 버전 2 컨피그레이션 가이드, Cisco IOS XE Fuji 16.9.x - 지원되는 RADIUS 특성]

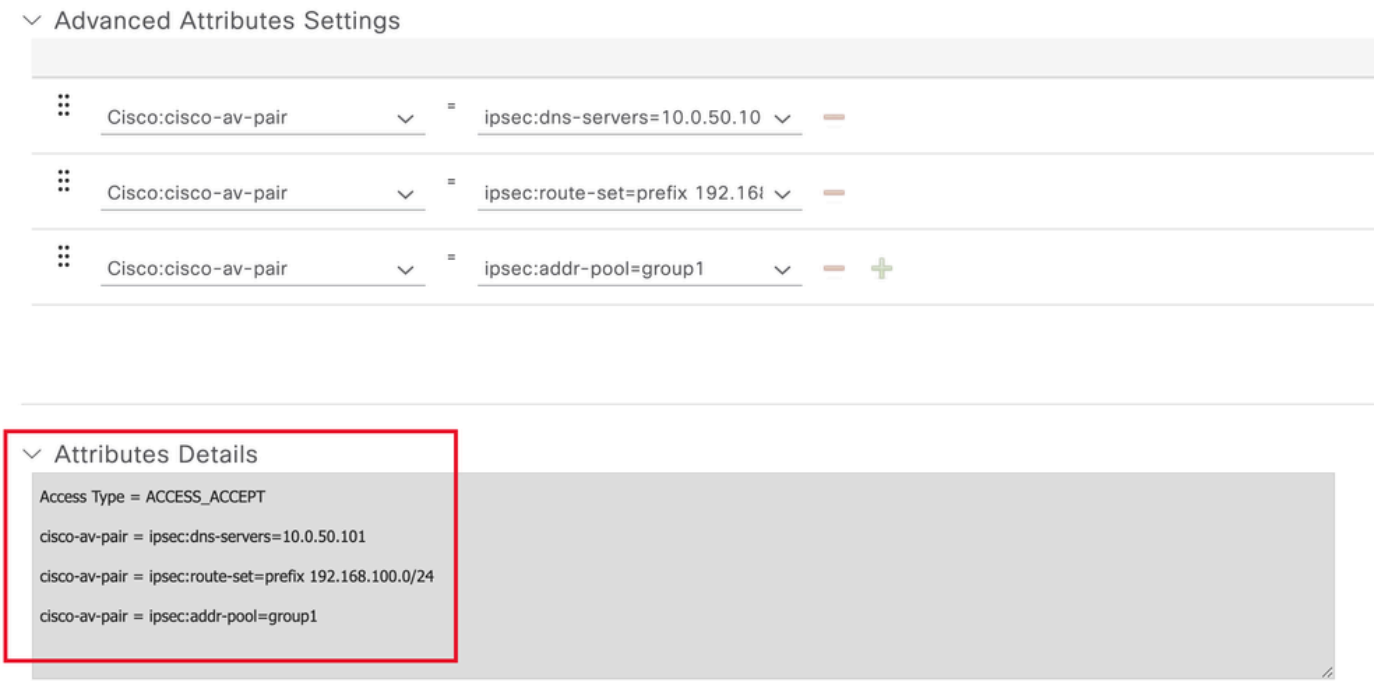


참고: 이전 단계를 반복하여 필요한 속성을 생성합니다.

저장을 클릭합니다.

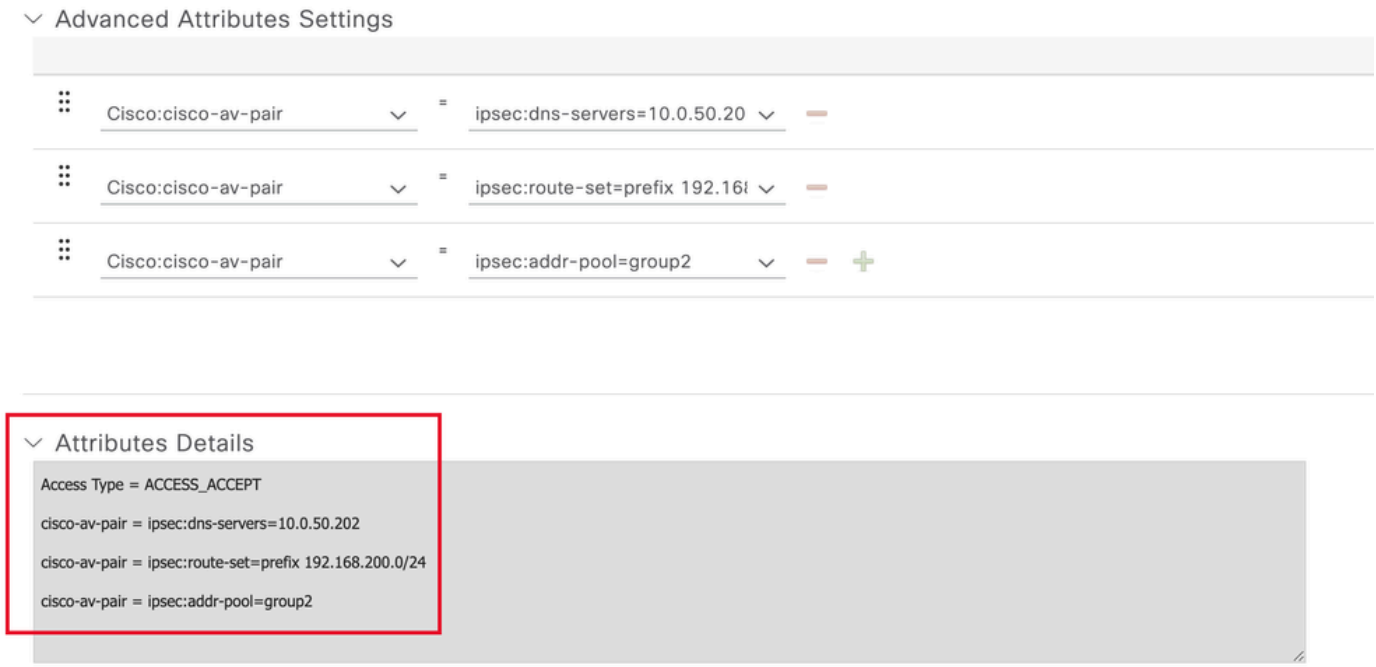
다음에 오는 속성이 각 그룹에 할당되었습니다.

- 그룹 1 특성:



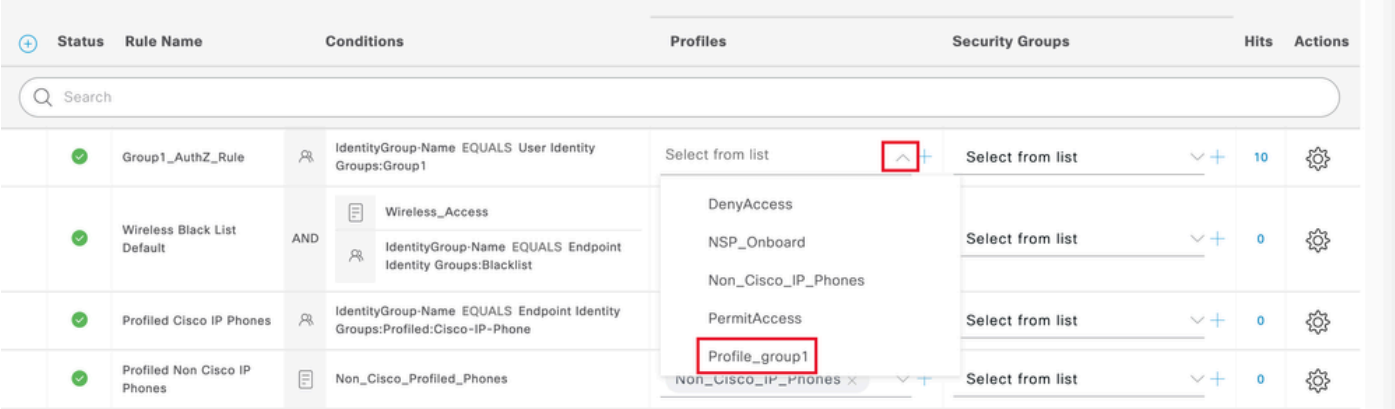
Group1 특성

- 그룹 2 특성:



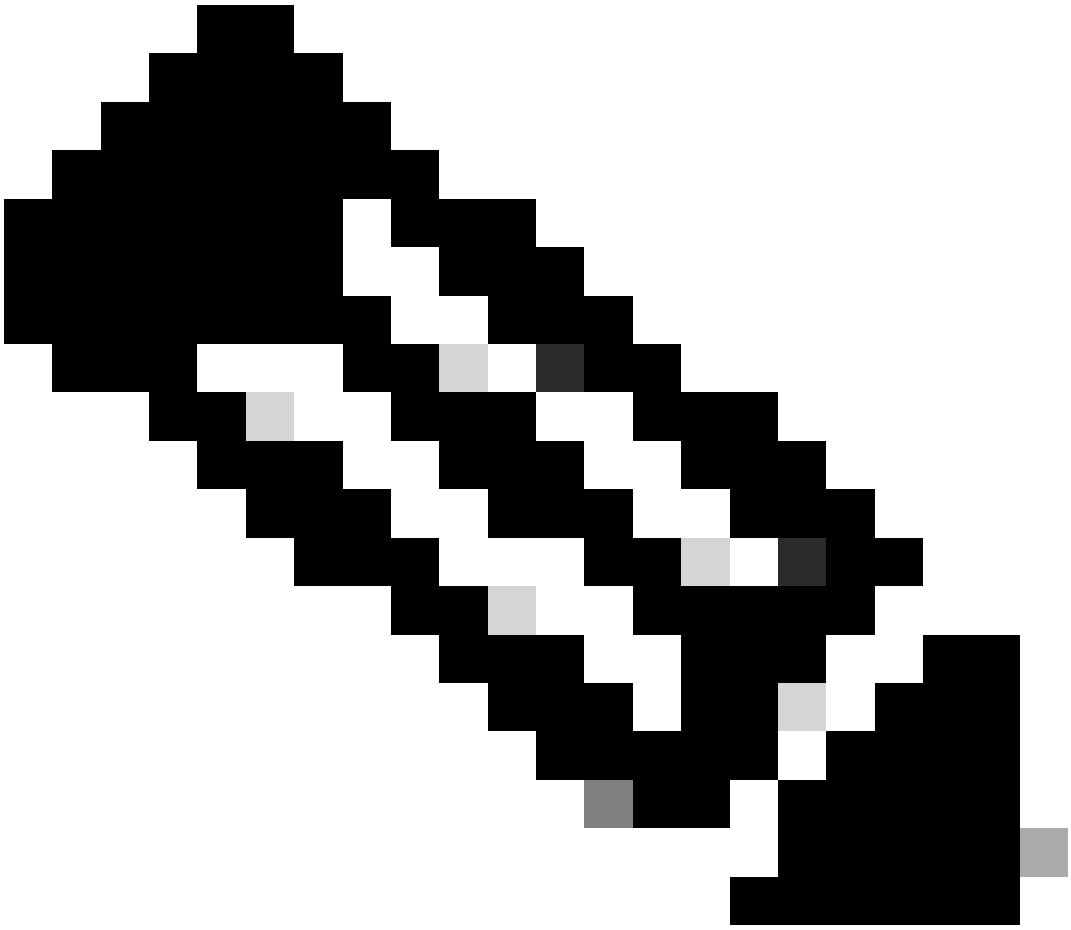
그룹 2 특성

11단계. 드롭다운 메뉴 화살표를 클릭하고 10단계에서 생성한 권한 부여 프로파일을 선택합니다.



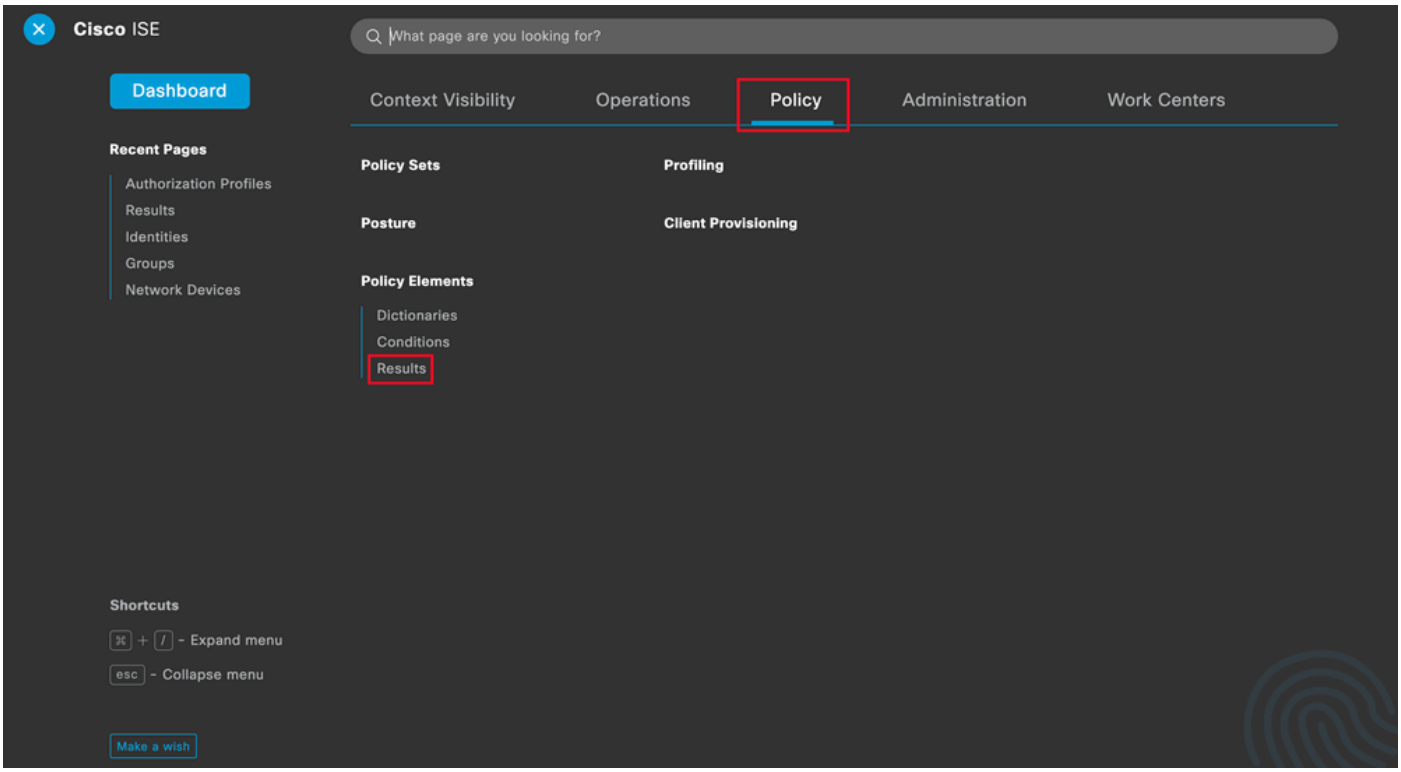
권한 부여 프로파일 할당

저장을 클릭합니다.



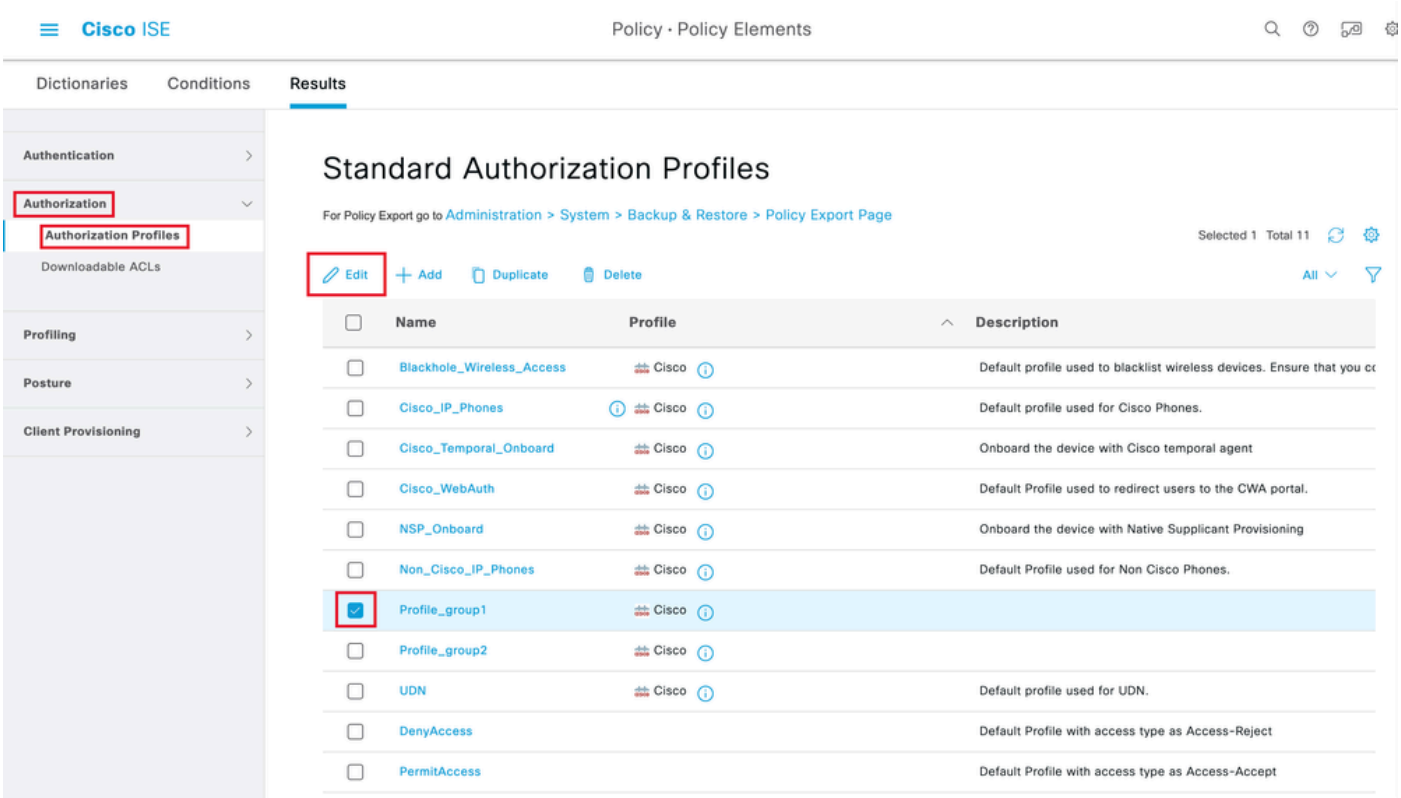
참고: 8~11단계를 반복하여 각 그룹에 필요한 권한 부여 규칙을 생성합니다.

12단계(선택 사항) 권한 부여 프로파일을 편집해야 하는 경우 Policy > Results로 이동합니다.



ISE 일반 메뉴

Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동합니다. 수정할 프로파일의 확인란을 클릭한 다음 Edit를 클릭합니다.



권한 부여 프로파일 편집

클라이언트 컨피그레이션

1단계. XML 프로파일 편집기를 사용하여 XML 프로파일을 생성합니다. 이 예는 이 문서를 작성하는 데 사용되는 예입니다.

<#root>


```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreLinux>All</CertificateStoreLinux>
<CertificateStoreOverride>true</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">
true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">
Disable
<PPPExclusionServerIP UserControllable="false"/>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">
false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false </RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>
```


FlexVPN HUB


```
</HostName>
<HostAddress>
```


192.168.50.225

```
</HostAddress>
<PrimaryProtocol>
```

IPsec

```
<StandardAuthenticationOnly>
true
<AuthMethodDuringIKENegotiation>
```

EAP-MD5

```
</AuthMethodDuringIKENegotiation>
<IKEIdentity>
```

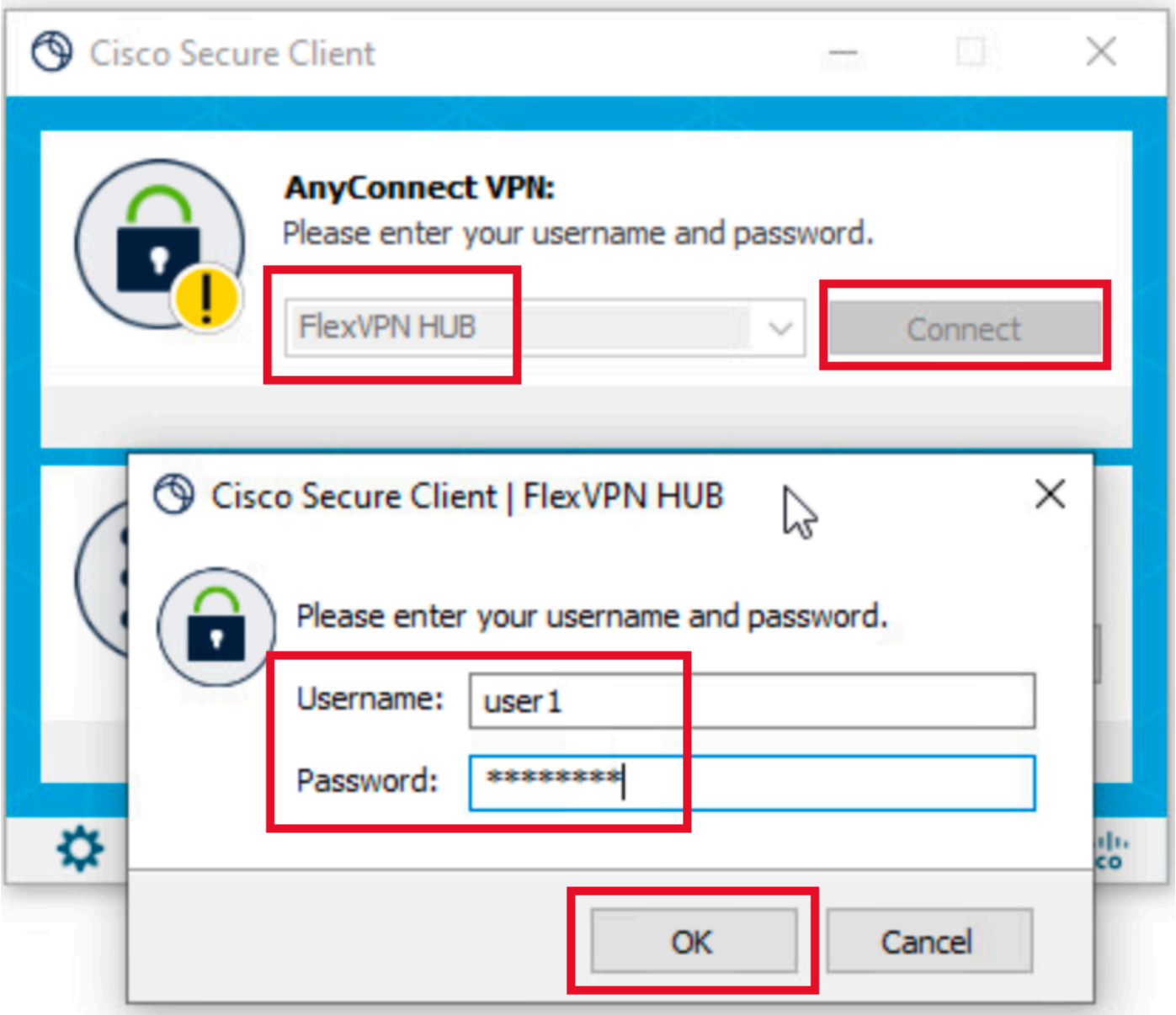
cisco.example

```
</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

- **<HostName>** - 호스트, IP 주소 또는 FQDN(Full-Qualified Domain Name)을 참조하는 데 사용되는 별칭입니다. CSC 상자에 표시됩니다.
- **<HostAddress>** - FlexVPN 허브의 IP 주소 또는 FQDN
- **<PrimaryProtocol>** - 클라이언트가 SSL 대신 IKEv2/IPsec을 사용하도록 강제하려면 IPsec으로 설정해야 합니다.
- **<AuthMethodDuringIKENegotiation>** - EAP 내에서 EAP-MD5를 사용하도록 설정해야 합니다. 이는 ISE 서버에 대한 인증에 필요합니다.
- **<IKEIdentity>** - 이 문자열은 클라이언트가 ID_GROUP 유형 ID 페이로드로 전송합니다. 이는 클라이언트를 허브의 특정 IKEv2 프로파일과 일치시키는 데 사용할 수 있습니다.

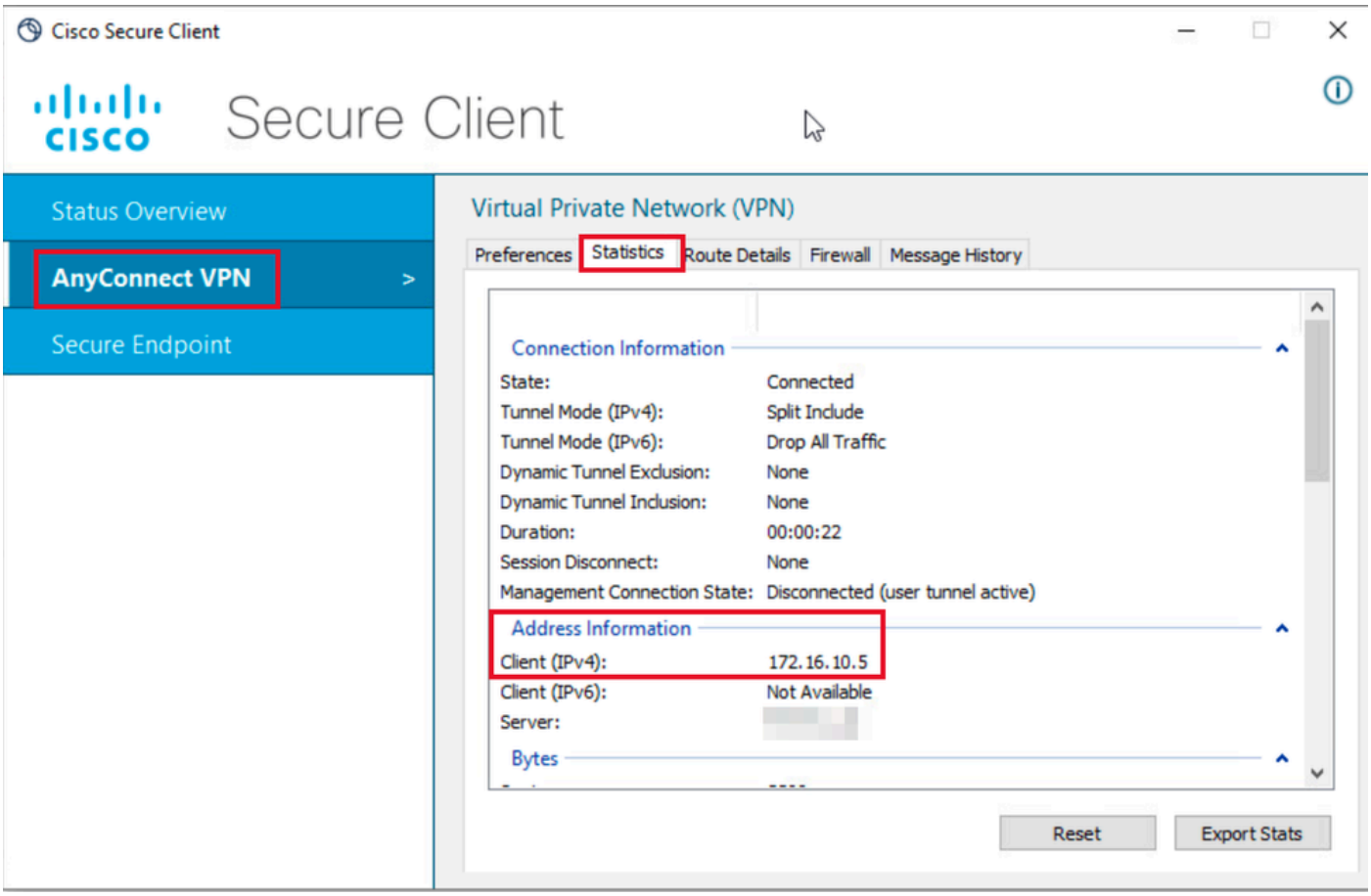
다음을 확인합니다.

1단계. CSC가 설치된 클라이언트 시스템으로 이동합니다. FlexVPN 허브에 연결하고 user1 자격 증명을 입력합니다.



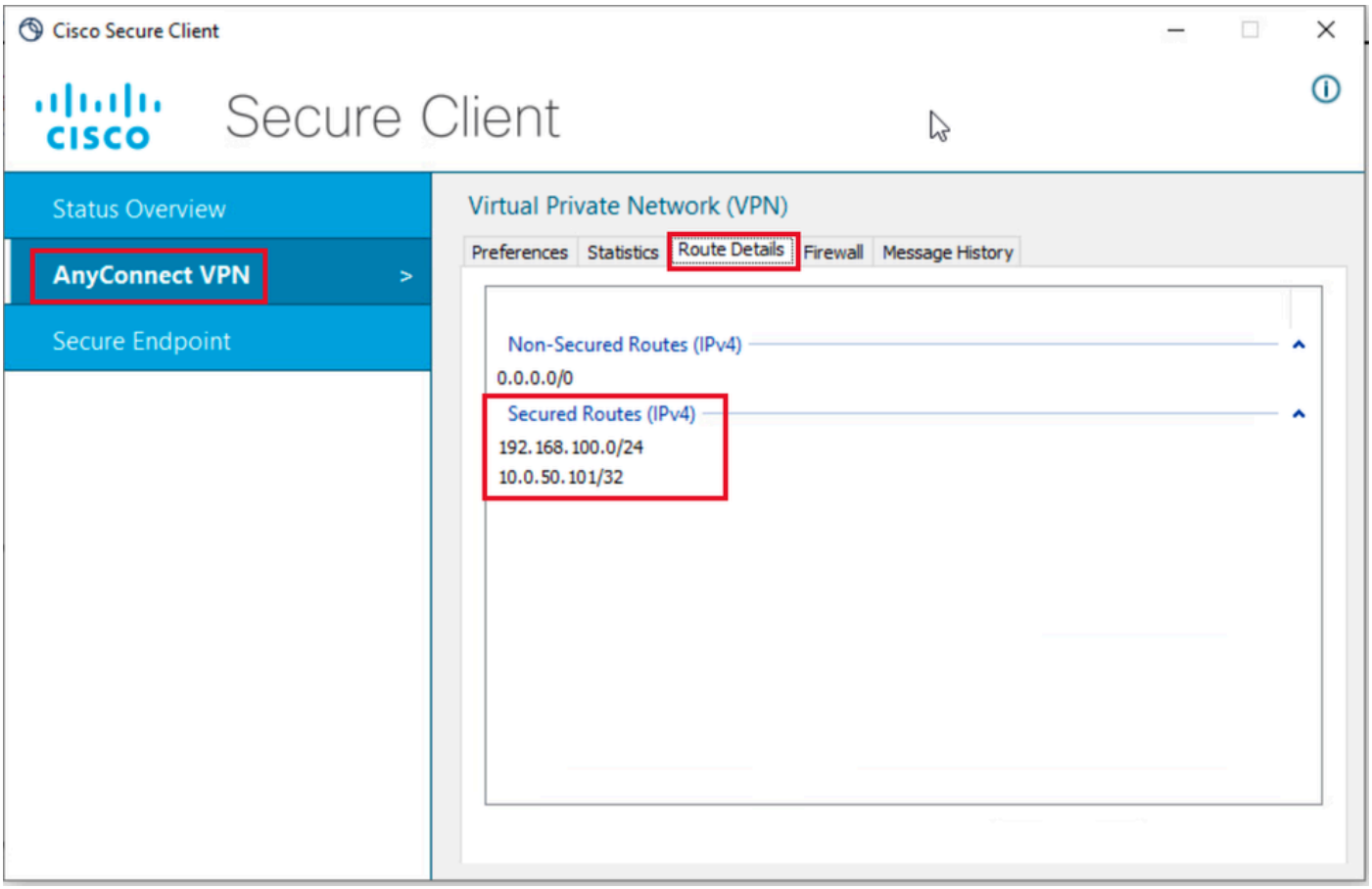
사용자1 자격 증명

2단계. 연결이 설정되면 기어 아이콘(왼쪽 하단 모서리)을 클릭하고 AnyConnectVPN > Statistics로 이동합니다. Address Information(주소 정보) 섹션에서 할당된 IP 주소가 group1에 대해 구성된 풀에 속하는지 확인합니다.



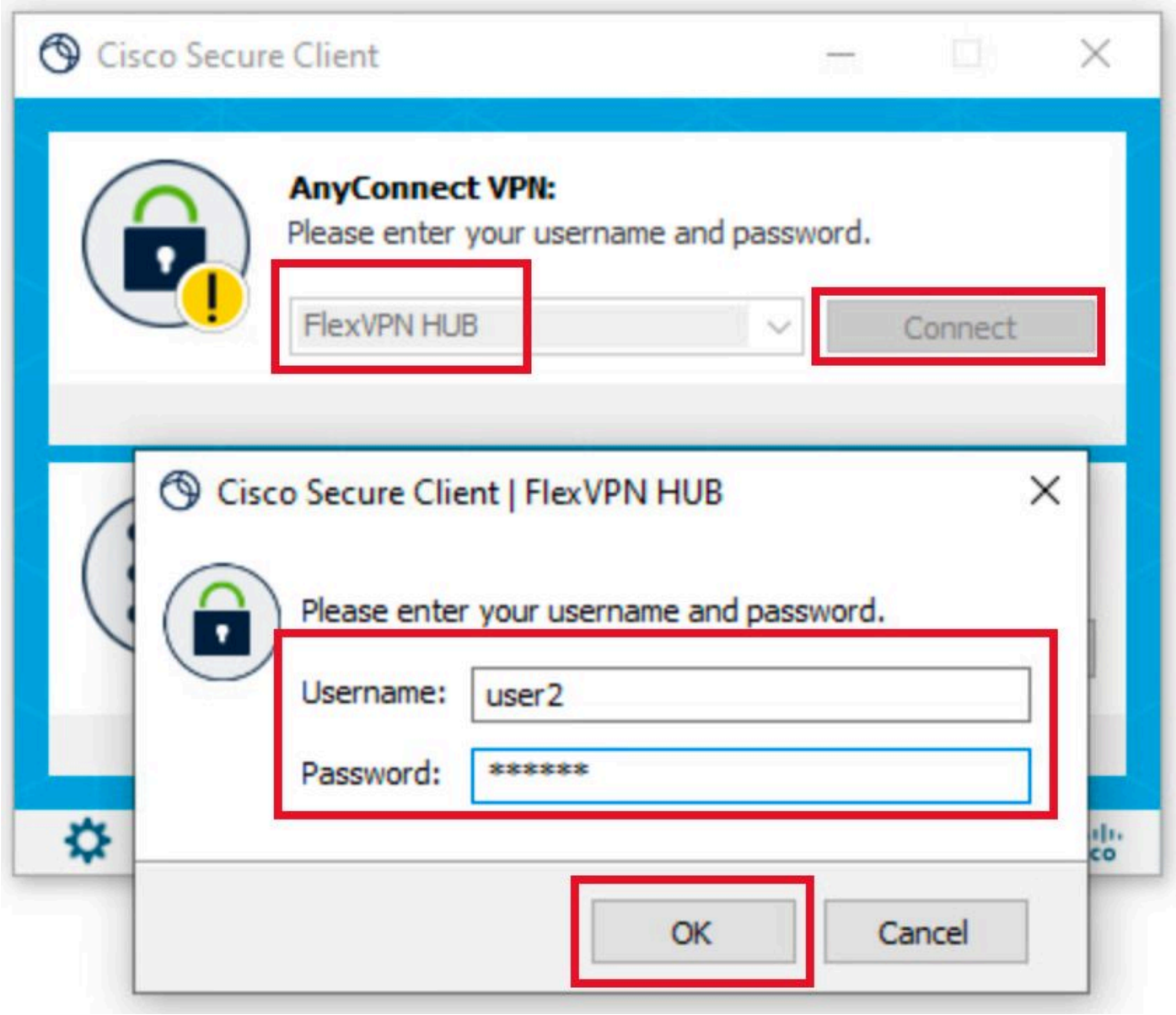
User1 통계

AnyConnectVPN > Route details(경로 세부사항)로 이동하고 표시된 정보가 group1에 대해 구성된 보안 경로 및 DNS에 해당하는지 확인합니다.

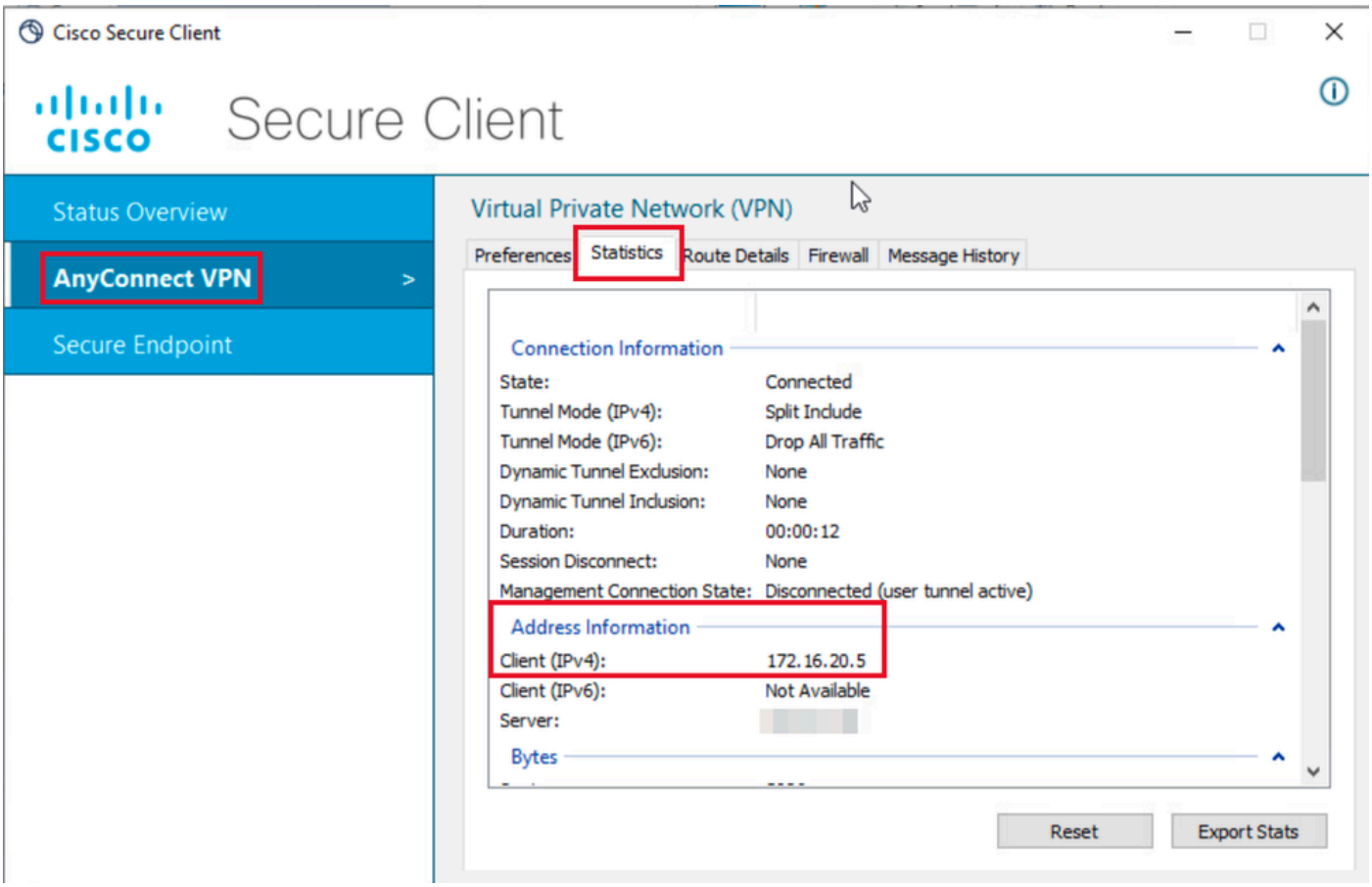


User1 경로 세부 정보

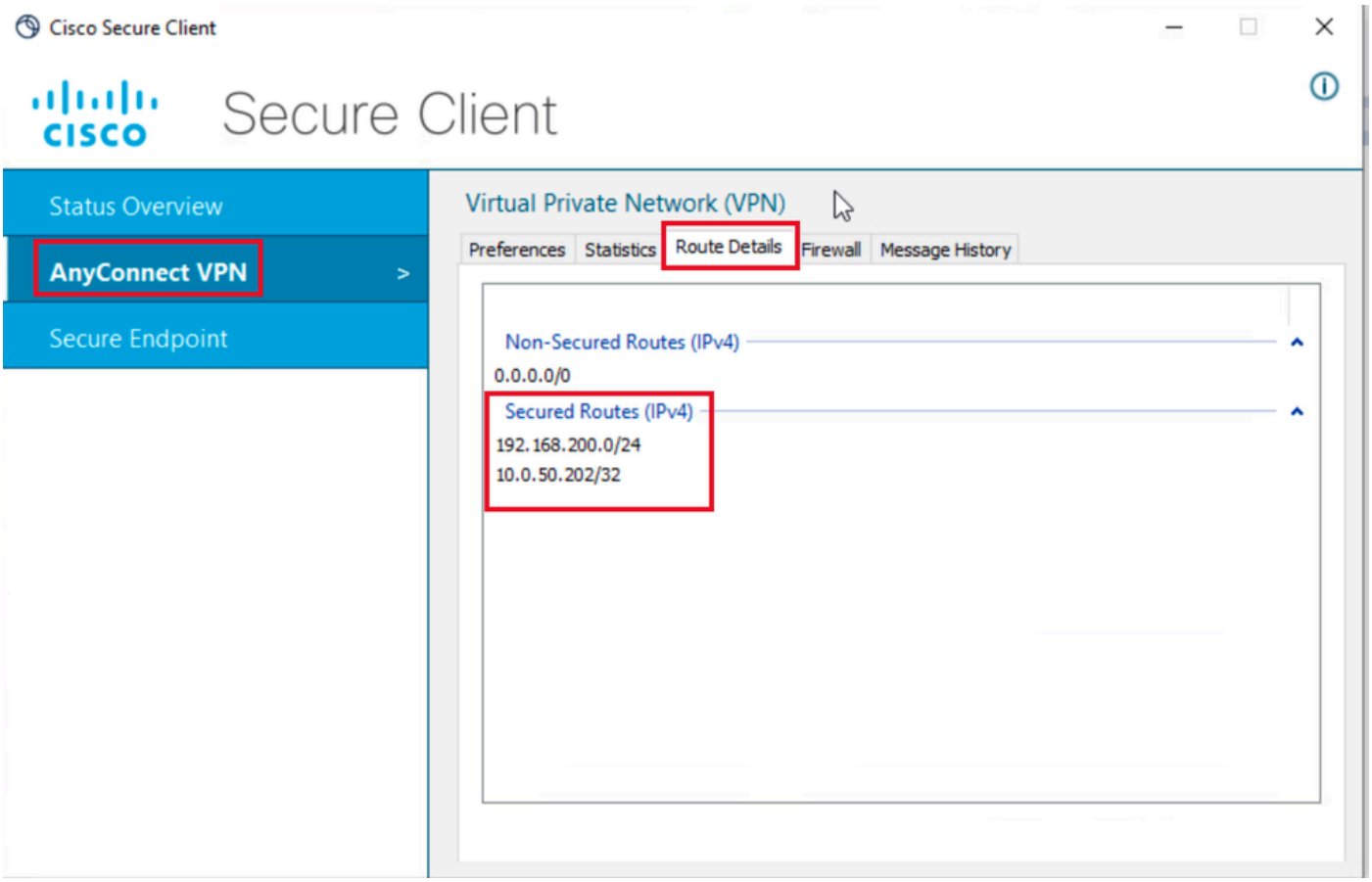
3단계. user2 자격 증명으로 1단계와 2단계를 반복하여 이 그룹에 대한 ISE 권한 부여 정책에 구성된 값과 일치하는 정보를 확인합니다.


Cisco Secure Client
AnyConnect VPN:
Please enter your username and password.
FlexVPN HUB
Connect
Cisco Secure Client | FlexVPN HUB
Please enter your username and password.
Username:
user2
Password:
******
OK
Cancel

사용자2 자격 증명



사용자2 통계



사용자2 경로 세부 정보

문제 해결

디버그 및 로그

Cisco 라우터:

1. IKEv2 및 IPSec 디버그를 사용하여 헤드엔드와 클라이언트 간의 협상을 확인합니다.

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

2. AAA 디버그를 사용하여 로컬 및/또는 원격 특성 할당을 확인합니다.

```
debug aaa authorization
debug aaa authentication
debug radius authentication
```

ISE의 경우:

- RADIUS 라이브 로그

작업 시나리오

다음 출력은 성공적인 연결의 예입니다.

- User1 디버그 출력:

<#root>

```
Jan 30 02:57:21.088: AAA/BIND(000000FF): Bind i/f
Jan 30 02:57:21.088: AAA/AUTHEN/LOGIN (000000FF):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.088: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.088: idb is NULL
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IPv6: ::
Jan 30 02:57:21.089: RADIUS/ENCODE(000000FF): acct_session_id: 4245
Jan 30 02:57:21.089: RADIUS(000000FF): sending
```

```
Jan 30 02:57:21.089: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.089: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.089: RADIUS(000000FF):
```

Send Access-Request to 192.168.30.110:1645 id 1645/85, len 229

```
RADIUS: authenticator C9 82 15 29 AF 4B 17 61 - 27 F4 5C 27 C2 C3 50 34
Jan 30 02:57:21.089: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 26
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 36
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 02:57:21.089: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 64
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194CAE2Z
Jan 30 02:57:21.089: RADIUS: User-Name [1] 7
```

"user1"

```
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 21
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 02:57:21.089: RADIUS: EAP-Message [79] 12
RADIUS: 02 3B 00 0A 01 75 73 65 72 31 [ ;user1]
Jan 30 02:57:21.089: RADIUS: Message-Authenticato[80] 18
RADIUS: E7 22 65 E0 DC 03 3A 49 0B 01 49 2A D5 3F AD 4F [ "e:II*?O]
Jan 30 02:57:21.089: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 02:57:21.089: RADIUS(000000FF): Sending a IPv4 Radius Packet
Jan 30 02:57:21.090: RADIUS(000000FF): Started 5 sec timeout
Jan 30 02:57:21.094: RADIUS:
```

Received from id 1645/85 192.168.30.110:1645, Access-Challenge, len 137

```
RADIUS: authenticator 67 2B 9D 9C 4D 1F F3 E8 - F6 EC 9B EB 8E 49 C8 A5
Jan 30 02:57:21.094: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.094: RADIUS: EAP-Message [79] 8
RADIUS: 01 52 00 06 0D 20 [ R ]
Jan 30 02:57:21.094: RADIUS: Message-Authenticato[80] 18
RADIUS: 38 8A B1 31 72 62 06 40 4F D4 58 48 E8 36 E7 80 [ 81rb@OXH6]
Jan 30 02:57:21.094: RADIUS(000000FF): Received from id 1645/85
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
Jan 30 02:57:21.097: AAA/AUTHEN/LOGIN (000000FF):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.097: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.097: idb is NULL
Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IPv6: ::
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): acct_session_id: 4245
```

```
Jan 30 02:57:21.097: RADIUS(000000FF): sending
Jan 30 02:57:21.097: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.097: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.097: RADIUS(000000FF):
```

Send Access-Request to 192.168.30.110:1645 id 1645/86, len 316

```
RADIUS: authenticator 93 07 42 CC D1 90 31 68 - 56 D0 D0 5A 35 C3 67 BC
Jan 30 02:57:21.097: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 02:57:21.097: RADIUS: Vendor, Cisco [26] 26
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 36
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 02:57:21.098: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 64
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194CAE2Z
Jan 30 02:57:21.098: RADIUS: User-Name [1] 7
```

"user1"

```
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 21
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 02:57:21.098: RADIUS: EAP-Message [79] 8
RADIUS: 02 52 00 06 03 04 [ R]
Jan 30 02:57:21.098: RADIUS: Message-Authenticato[80] 18
RADIUS: E0 67 24 D3 BB CF D9 E0 EE 44 98 8A 26 64 AC C9 [ g$D&d]
Jan 30 02:57:21.098: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.098: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 02:57:21.098: RADIUS(000000FF): Sending a IPv4 Radius Packet
Jan 30 02:57:21.099: RADIUS(000000FF): Started 5 sec timeout
Jan 30 02:57:21.101: RADIUS:
```

Received from id 1645/86 192.168.30.110:1645, Access-Challenge, len 161

```
RADIUS: authenticator 42 A3 5F E0 92 13 51 13 - B2 80 56 A3 91 36 BD A1
Jan 30 02:57:21.101: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.101: RADIUS: EAP-Message [79] 32
RADIUS: 01 53 00 1E 04 10 D7 61 AE 69 3B 88 A1 83 E4 EC 0F B6 EF 68 58 16 49 53 45 2D 44 49 41 4E [ Sai
Jan 30 02:57:21.101: RADIUS: Message-Authenticato[80] 18
RADIUS: 3E C9 C1 E1 F2 3B 4E 4C DF CF AC 21 AA E9 C3 F0 [ >;NL!]
Jan 30 02:57:21.101: RADIUS(000000FF): Received from id 1645/86
RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes
Jan 30 02:57:21.103: AAA/AUTHEN/LOGIN (000000FF):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.103: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.104: idb is NULL
Jan 30 02:57:21.104: RADIUS(000000FF): Config NAS IPv6: ::
Jan 30 02:57:21.104: RADIUS/ENCODE(000000FF): acct_session_id: 4245
Jan 30 02:57:21.104: RADIUS(000000FF): sending
Jan 30 02:57:21.104: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.104: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.104: RADIUS(000000FF):
```

Send Access-Request to 192.168.30.110:1645 id 1645/87, len 332

```
RADIUS: authenticator 89 35 9C C5 06 FB 04 B7 - 4E A3 B2 5F 2B 15 4F 46
Jan 30 02:57:21.104: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 26
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 36
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 02:57:21.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 64
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194CAE2Z
Jan 30 02:57:21.104: RADIUS: User-Name [1] 7
```

"user1"

```
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 21
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 02:57:21.104: RADIUS: EAP-Message [79] 24
RADIUS: 02 53 00 16 04 10 B0 BB 3E D5 B1 D6 01 FC 9A B7 4A DB AB F7 2F B6 [ S>J/]
Jan 30 02:57:21.104: RADIUS: Message-Authenticato[80] 18
RADIUS: 79 43 97 A7 26 17 3E 3B 54 B4 90 D4 76 0F E0 14 [ yC&>;Tv]
Jan 30 02:57:21.104: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 02:57:21.105: RADIUS(000000FF): Sending a IPv4 Radius Packet
Jan 30 02:57:21.105: RADIUS(000000FF): Started 5 sec timeout
Jan 30 02:57:21.170: RADIUS:
```

Received from id 1645/87 192.168.30.110:1645, Access-Accept, len 233

```
RADIUS: authenticator 75 F6 05 85 1D A0 C3 EE - F8 81 F9 02 38 AC C1 B6
Jan 30 02:57:21.170: RADIUS: User-Name [1] 7
```

"user1"

```
Jan 30 02:57:21.170: RADIUS: Class [25] 68
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6ZO2L42F2F016FZH]
RADIUS: 31 31 39 34 43 41 45 32 5A 4E 31 46 3A 49 53 45 [1194CAE2ZN1F:ISE]
```

```
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 32 39 [ 29]
Jan 30 02:57:21.170: RADIUS: EAP-Message [79] 6
RADIUS: 03 53 00 04 [ S]
Jan 30 02:57:21.170: RADIUS: Message-Authenticato[80] 18
RADIUS: 8A A9 CC 07 61 A2 6D BA E4 EB B5 B7 73 0E EC 28 [ ams(]
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 37
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 31
```

"ipsec:dns-servers=10.0.50.101"

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 47
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 41
```

"ipsec:route-set=prefix 192.168.100.0/24"

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 30
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 24
```

"ipsec:addr-pool=group1"

```
Jan 30 02:57:21.171: RADIUS(000000FF): Received from id 1645/87
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 02:57:21.175: AAA/BIND(00000100): Bind i/f
Jan 30 02:57:21.175: AAA/AUTHOR (0x100):
```

Pick method list 'FlexVPN-Authorization-List'

```
Jan 30 02:57:21.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to
Jan 30 02:57:21.192: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
Jan 30 02:57:21.376: %LINEPROTO-5-UPDOWN:
```

Line protocol on Interface Virtual-Access1, changed state to up

- User2 디버그 출력:

<#root>

```
Jan 30 03:28:58.102: AAA/BIND(00000103): Bind i/f
Jan 30 03:28:58.102: AAA/AUTHEN/LOGIN (00000103):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.103: idb is NULL
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.103: RADIUS(00000103): sending
Jan 30 03:28:58.103: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.103: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.103: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/88, len 229

```
RADIUS: authenticator 71 99 09 63 19 F7 D7 0B - 1D A9 4E 64 28 6F A5 64
Jan 30 03:28:58.103: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.103: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 03:28:58.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194E444Z
Jan 30 03:28:58.104: RADIUS: User-Name [1] 7
```

"user2"

```
Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.104: RADIUS: EAP-Message [79] 12
RADIUS: 02 3B 00 0A 01 75 73 65 72 32 [ ;user2]
Jan 30 03:28:58.104: RADIUS: Message-Authenticato[80] 18
RADIUS: 12 62 2F 51 12 FC F7 EC F0 87 E0 34 1E F1 AD E5 [ b/Q4]
Jan 30 03:28:58.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.104: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.105: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.109: RADIUS:
```

Received from id 1645/88 192.168.30.110:1645, Access-Challenge, len 137

```
RADIUS: authenticator 98 04 01 EA CD 9B 1E A9 - DC 6F 2F 17 1F 2A 5F 43
Jan 30 03:28:58.109: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.110: RADIUS: EAP-Message [79] 8
RADIUS: 01 35 00 06 0D 20 [ 5 ]
Jan 30 03:28:58.110: RADIUS: Message-Authenticato[80] 18
RADIUS: E3 A6 88 B1 B6 3D 93 1F 39 B3 AE 9E EA 1D BB 15 [ =9]
Jan 30 03:28:58.110: RADIUS(00000103): Received from id 1645/88
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
Jan 30 03:28:58.112: AAA/AUTHEN/LOGIN (00000103):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 03:28:58.112: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.112: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.112: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.112: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.113: idb is NULL
Jan 30 03:28:58.113: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.113: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.113: RADIUS(00000103): sending
Jan 30 03:28:58.113: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.113: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.113: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/89, len 316

```
RADIUS: authenticator 56 BD F0 9A 4B 16 5C 6C - 4E 41 00 56 8D C0 3A 8C
Jan 30 03:28:58.113: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 03:28:58.113: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194E444Z
Jan 30 03:28:58.113: RADIUS: User-Name [1] 7
```

"user2"

```
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.113: RADIUS: EAP-Message [79] 8
RADIUS: 02 35 00 06 03 04 [ 5]
Jan 30 03:28:58.113: RADIUS: Message-Authenticato[80] 18
RADIUS: 47 1F 36 A7 C3 9B 90 6E 03 2C B8 D7 FE A7 13 44 [ G6n,D]
Jan 30 03:28:58.113: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.114: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.114: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.114: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.116: RADIUS:
```

Received from id 1645/89 192.168.30.110:1645, Access-Challenge, len 161

```
RADIUS: authenticator 84 A3 30 3D 80 BC 71 42 - 1B 9B 49 EF 0B 1B 02 02
Jan 30 03:28:58.116: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.116: RADIUS: EAP-Message [79] 32
RADIUS: 01 36 00 1E 04 10 EB 9F A5 AC 70 1F 4D D6 48 05 9D EC 1F 29 67 AE 49 53 45 2D 44 49 41 4E [ 6pM
Jan 30 03:28:58.116: RADIUS: Message-Authenticato[80] 18
RADIUS: 08 5E BC EF E5 38 50 CD FB 3C B3 E9 99 0A 51 B3 [ ^8P<Q]
Jan 30 03:28:58.116: RADIUS(00000103): Received from id 1645/89
RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes
Jan 30 03:28:58.118: AAA/AUTHEN/LOGIN (00000103):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.118: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.118: idb is NULL
```

```
Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.118: RADIUS(00000103): sending
Jan 30 03:28:58.118: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.119: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.119: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/90, len 332

```
RADIUS: authenticator A1 62 1A FB 18 58 7B 47 - 5C 8A 64 FA B7 23 9B BE
Jan 30 03:28:58.119: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 03:28:58.119: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194E444Z
Jan 30 03:28:58.119: RADIUS: User-Name [1] 7
```

"user2"

```
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.119: RADIUS: EAP-Message [79] 24
RADIUS: 02 36 00 16 04 10 73 B7 F2 42 09 5B AB 21 D8 77 96 A2 F7 C7 83 AD [ 6sB[!w]
Jan 30 03:28:58.119: RADIUS: Message-Authenticato[80] 18
RADIUS: B1 68 3C 25 9E FE 52 13 10 69 E6 BB 17 67 6F 18 [ h<?Rigo]
Jan 30 03:28:58.119: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.119: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.119: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.119: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.186: RADIUS: Received from id 1645/90 192.168.30.110:1645, Access-Accept, len 233
RADIUS: authenticator 48 A5 A0 11 ED B8 C2 87 - 35 30 17 D5 6D D7 B4 FD
Jan 30 03:28:58.186: RADIUS: User-Name [1] 7
```

"user2"

```
Jan 30 03:28:58.186: RADIUS: Class [25] 68
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6ZO2L42F2F016FZH]
RADIUS: 31 31 39 34 45 34 34 34 5A 4E 32 30 3A 49 53 45 [1194E444ZN20:ISE]
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 33 30 [ 30]
Jan 30 03:28:58.186: RADIUS: EAP-Message [79] 6
RADIUS: 03 36 00 04 [ 6]
Jan 30 03:28:58.186: RADIUS: Message-Authenticato[80] 18
RADIUS: 9E A6 D9 56 40 C8 EB 08 69 8C E1 35 35 53 18 83 [ V@i55S]
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 37
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 31
```

"ipsec:dns-servers=10.0.50.202"

```
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 47
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 41
```

"ipsec:route-set=prefix 192.168.200.0/24"

```
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 30
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 24
```

"ipsec:addr-pool=group2"

```
Jan 30 03:28:58.187: RADIUS(00000103): Received from id 1645/90
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 03:28:58.190: AAA/BIND(00000104): Bind i/f
Jan 30 03:28:58.190: AAA/AUTHOR (0x104):
```

Pick method list 'FlexVPN-Authorization-List'

```
Jan 30 03:28:58.192: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to
Jan 30 03:28:58.209: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
Jan 30 03:28:58.398: %LINEPROTO-5-UPDOWN:
```

Line protocol on Interface Virtual-Access2, changed state to up

관련 정보

- Cisco 기술 지원 및 다운로드