ISE 3.2 및 Windows에서 유선 Dot1x 문제 해결

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

구성

- 네트워크 다이어그램

소개

이 문서에서는 ISE(Identity Services Engine) 3.2 및 Windows 기본 신청자에 대한 기본 802.1X PEAP 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- PEAP(Protected Extensible Authentication Protocol)
- PEAP 802.1x

사용되는 구성 요소

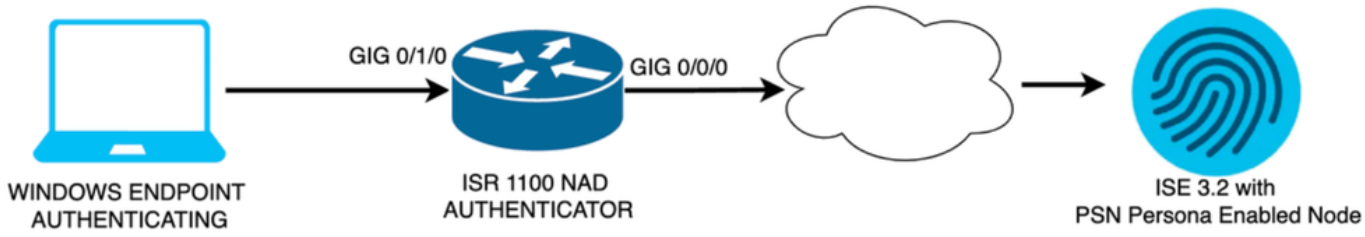
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE(Identity Services Engine) 버전
- Cisco C1117 Cisco IOS® XE Software, 버전 17.12.02
- Windows 10을 사용하는 랩톱

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



네트워크 다이어그램

설정

다음 단계를 수행하여 구성합니다.

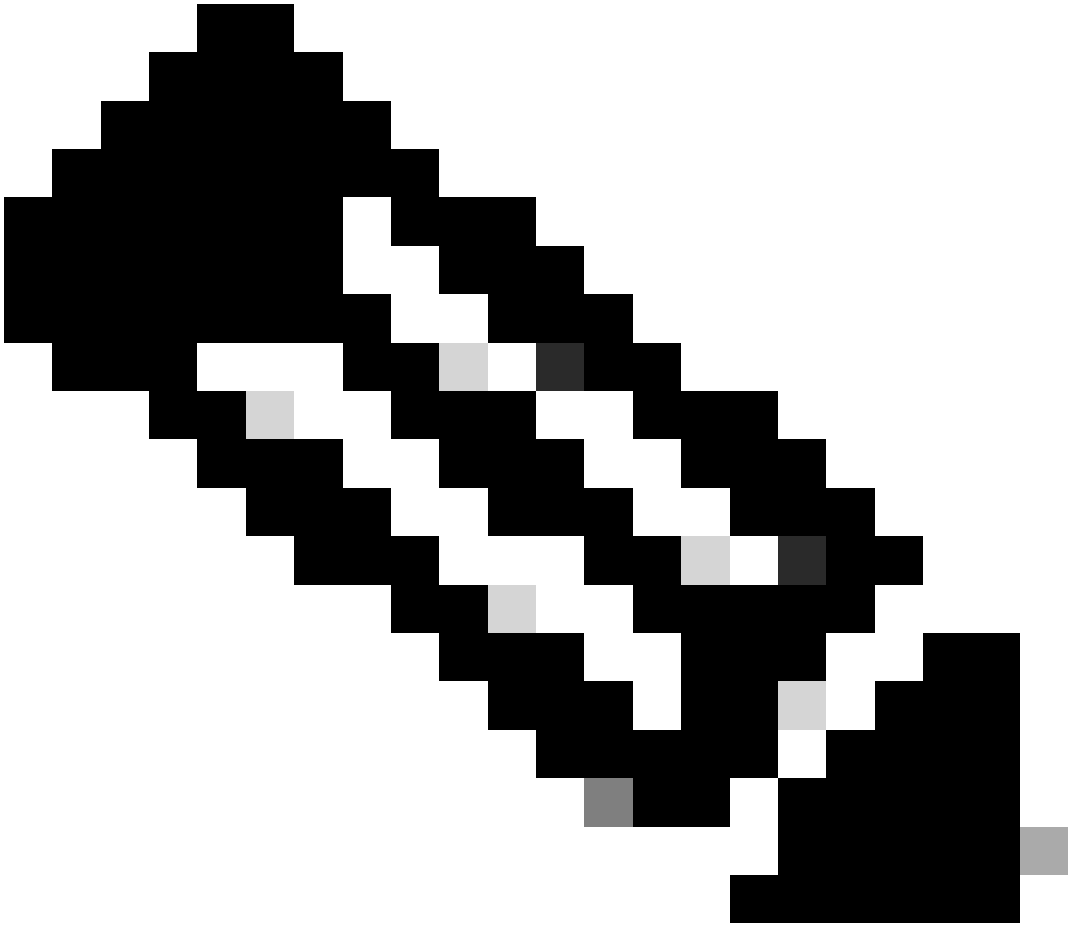
1단계. ISR 1100 라우터를 구성합니다.

2단계. Identity Service Engine 3.2를 구성합니다.

3단계. Windows 네이티브 서 플리 컨 트를 구성 합니다.

1단계. ISR 1100 라우터 구성

이 섹션에서는 dot1x를 작동시키기 위해 최소한 NAD에 있어야 하는 기본 컨피그레이션에 대해 설명합니다.



참고: 다중 노드 ISE 구축의 경우 PSN 페르소나가 활성화된 노드의 IP를 구성합니다. Administration(관리) > System(시스템) > Deployment(구축) 탭 아래에서 ISE로 이동할 경우 이 기능을 활성화할 수 있습니다.

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
 client A.B.C.D server-key  <Your shared secret>
!
!
radius server  ISE-PSN-1
 address ipv4 A.B.C.D auth-port 1645 acct-port 1646
 timeout 15
 key <Your shared secret>
```

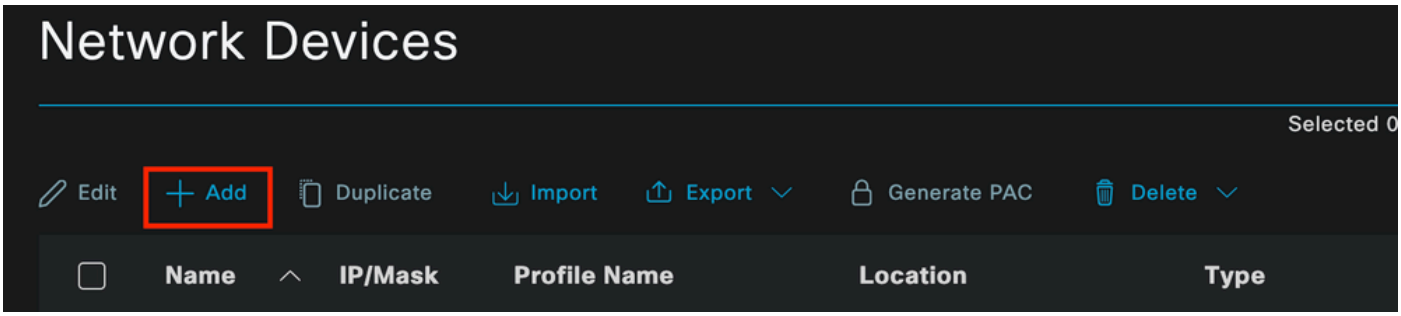
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

2단계. Identity Service Engine 3.2를 구성합니다.

2. a. 인증에 사용할 네트워크 장치를 구성하고 추가합니다.

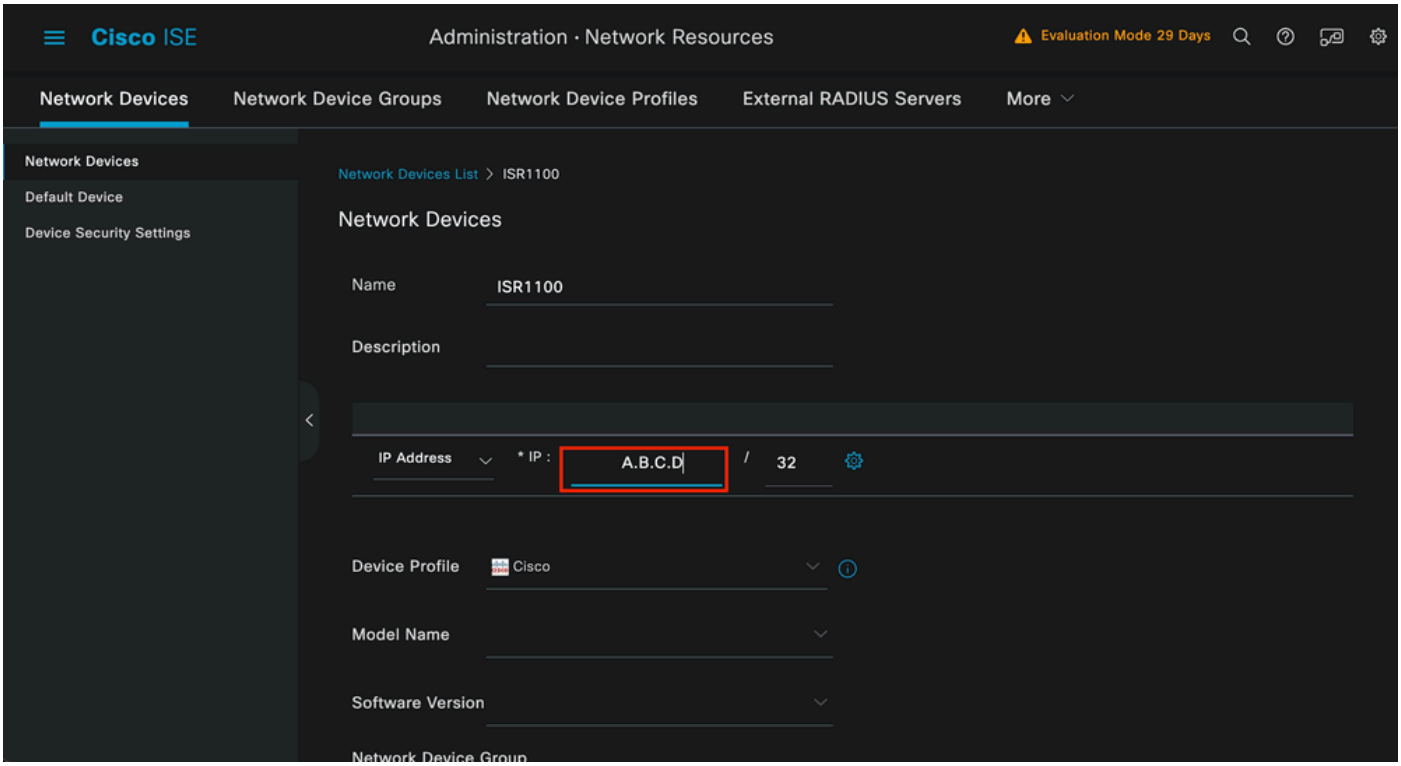
Network Device to ISE Network Devices(ISE 네트워크 디바이스에 네트워크 디바이스 추가) 섹션을 추가합니다.

시작하려면 Add(추가) 버튼을 클릭합니다.



ISE 네트워크 디바이스

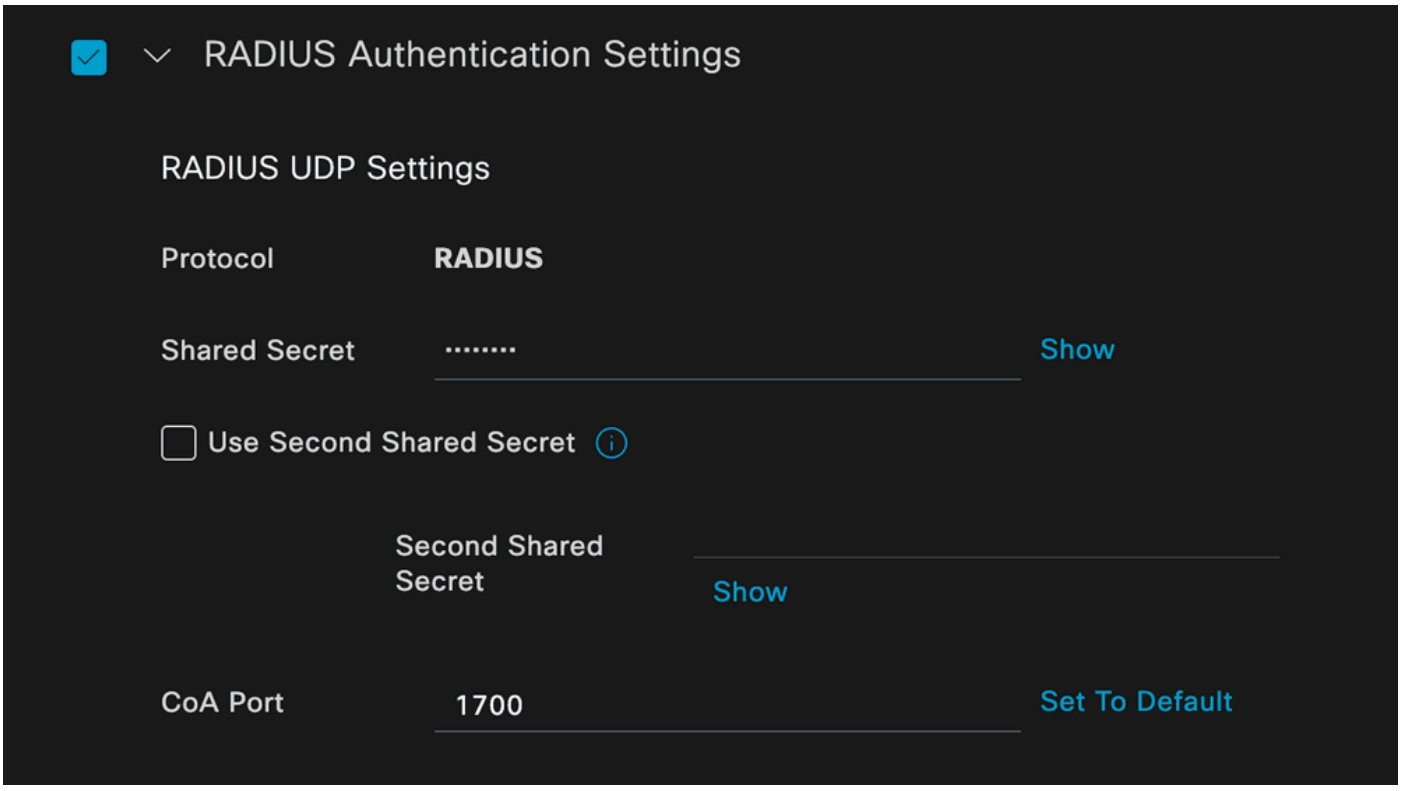
값을 입력하고 생성 중인 NAD에 이름을 할당한 다음 네트워크 디바이스가 ISE에 연결하는 데 사용하는 IP를 추가합니다.



네트워크 디바이스 생성 페이지

이 페이지에서 아래로 스크롤하여 Radius 인증 설정을 찾습니다. 다음 그림과 같이.

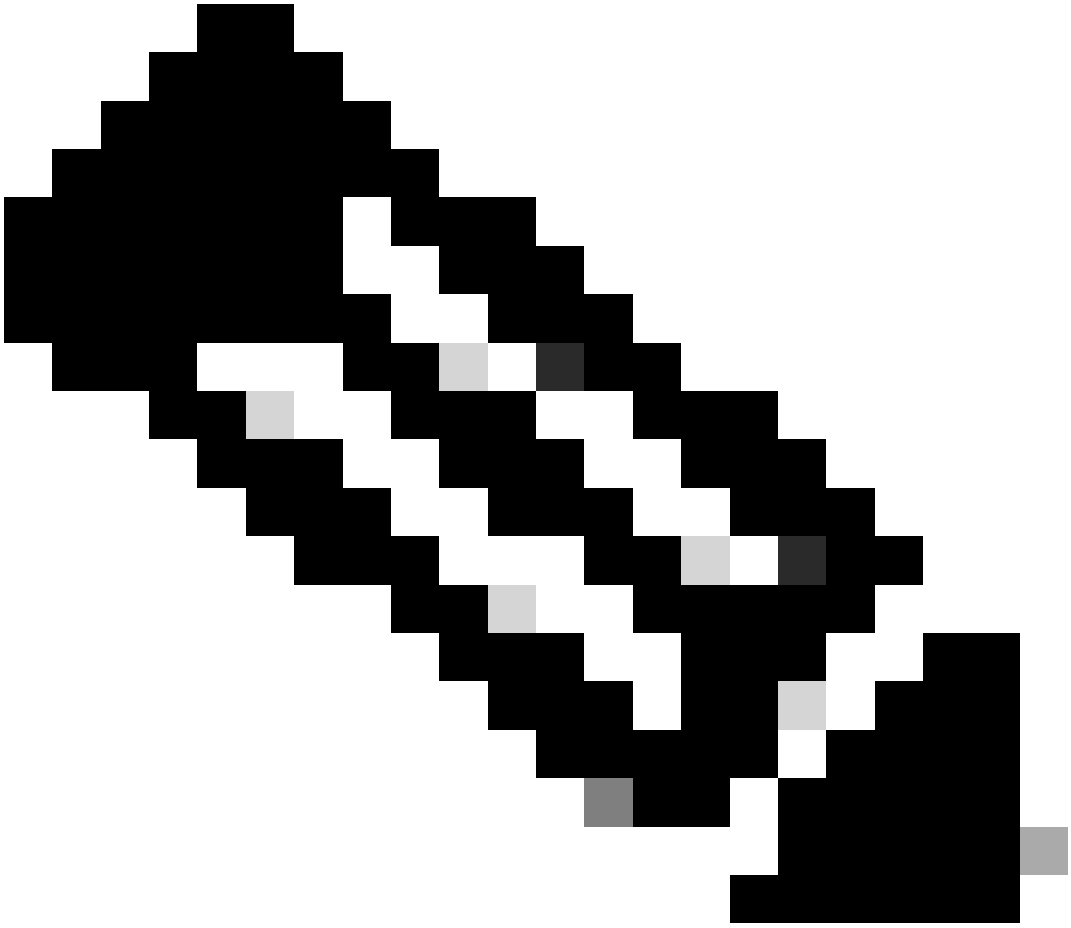
NAD 컨피그레이션에서 사용한 공유 암호를 추가합니다.



Radius 컨피그레이션

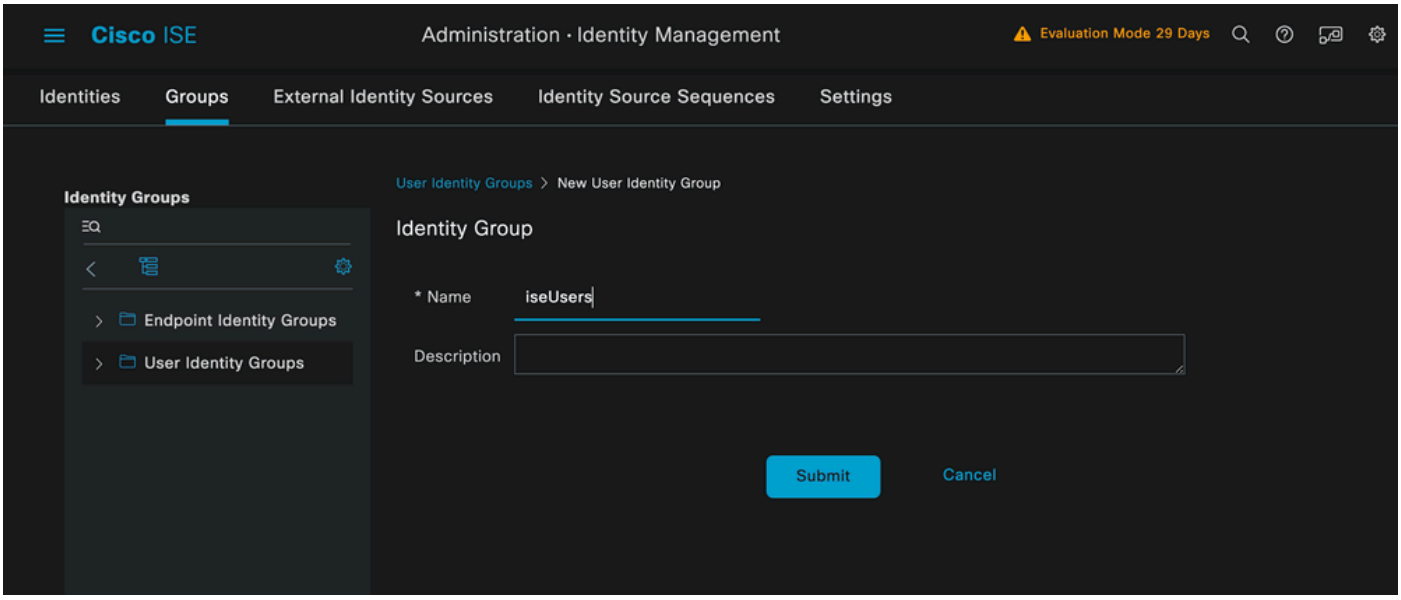
변경 사항을 저장합니다.

2. b. 엔드포인트를 인증하는 데 사용되는 ID를 구성합니다.



참고: 이 컨피그레이션을 유지하려면 간단한 ISE 로컬 인증이 사용됩니다.

Administration(관리) > Identity Management(ID 관리) > Groups(그룹) 탭으로 이동합니다. 그룹 및 ID를 생성합니다. 이 데모에 대해 생성된 그룹은 iseUsers입니다.

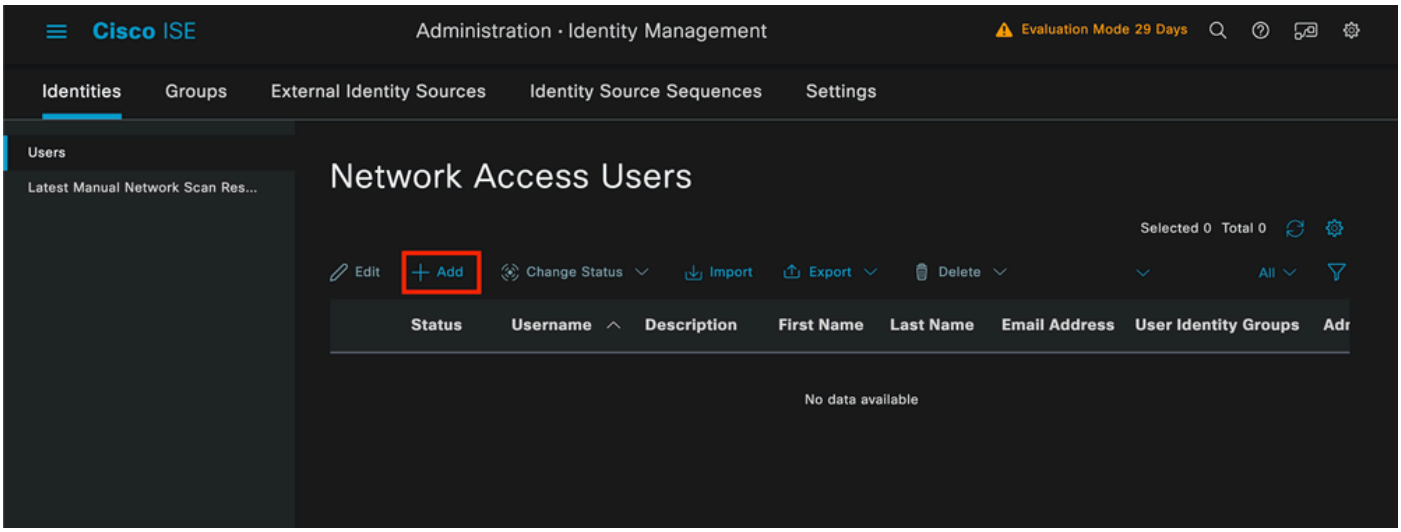


ID 그룹 생성 페이지

Submit(제출) 버튼을 클릭합니다.

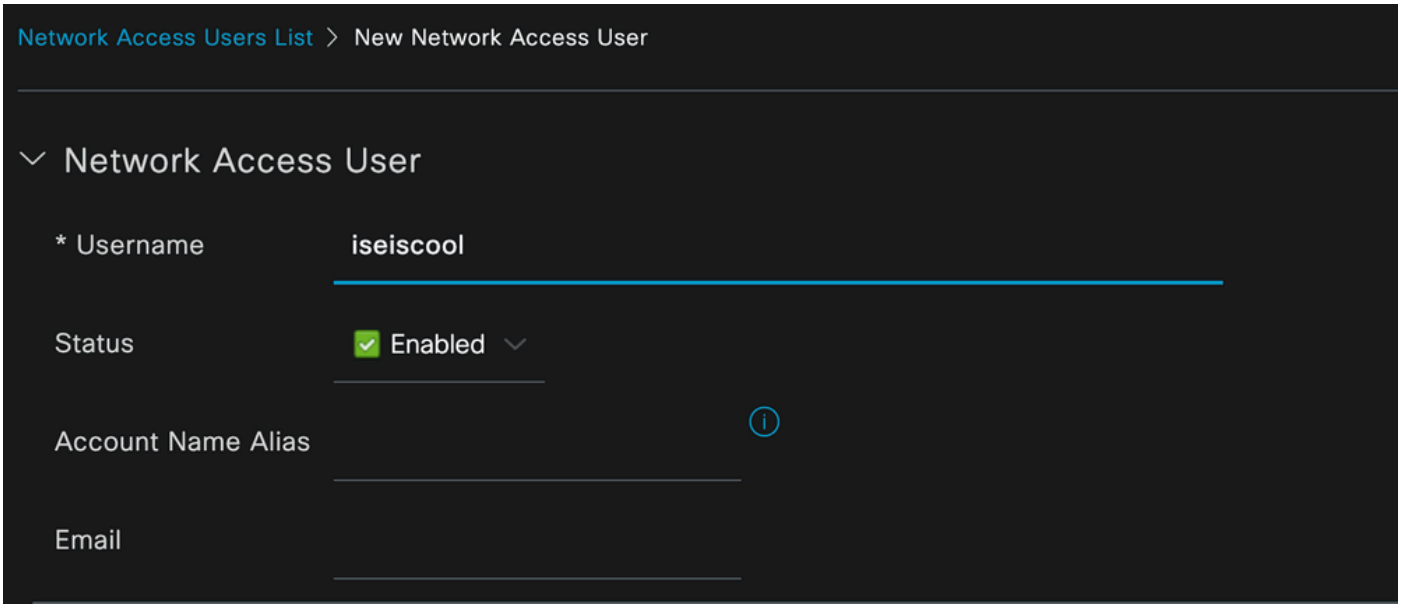
다음으로, Administration(관리) > Identity Management(ID 관리) > Identity(ID) 탭으로 이동합니다.

Add를 클릭합니다.



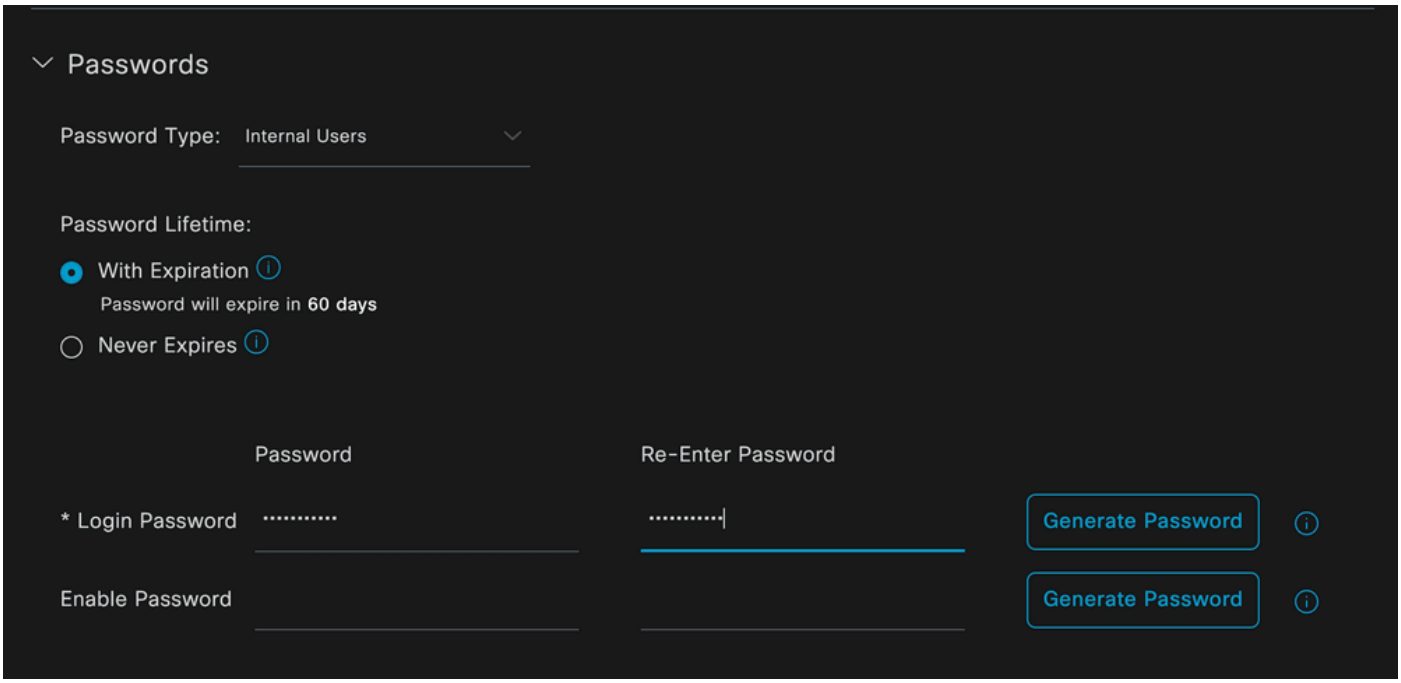
사용자 생성 페이지

필수 필드의 일부로 사용자 이름으로 시작합니다. 사용자 이름 iseiscool이 이 예에서 사용됩니다.



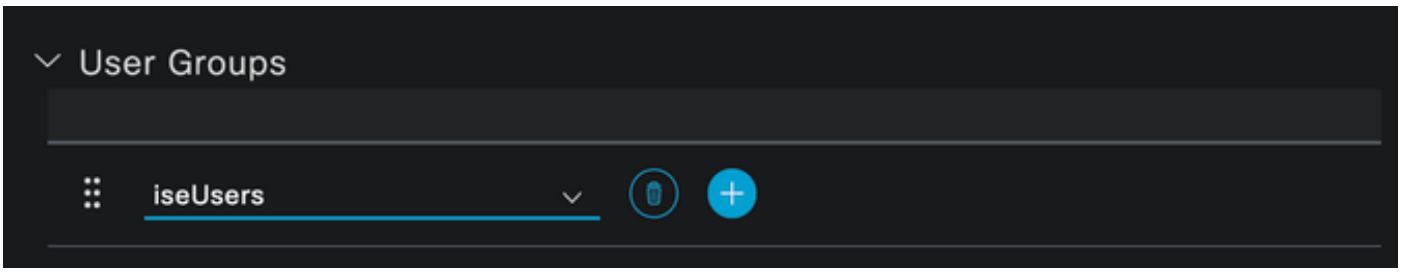
사용자 이름에 할당된 이름

다음 단계는 생성된 사용자 이름에 비밀번호를 할당하는 것입니다. 이 데모에서는 VainillaISE97이 사용됩니다.



비밀번호 생성

iseUsers 그룹에 사용자를 할당합니다.



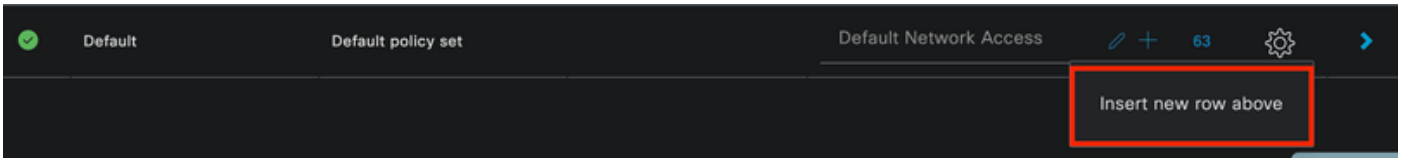
사용자 그룹 할당

2. c. 정책 집합 구성

ISE Menu(ISE 메뉴) > Policy(정책) > Policy Sets(정책 집합)로 이동합니다.

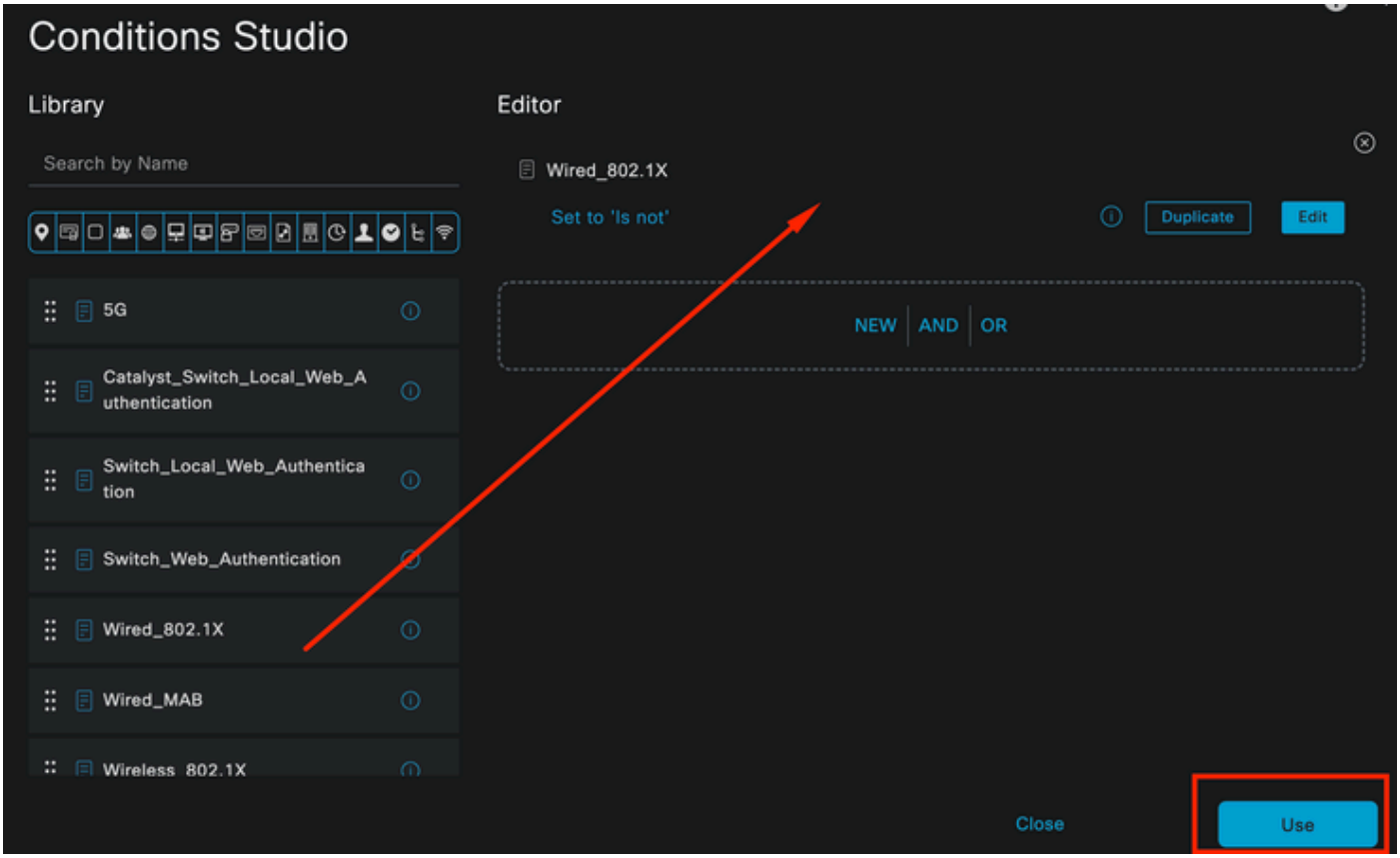
기본 정책 집합을 사용할 수 있습니다. 그러나 이 예에서는 정책 집합이 생성되고 이를 Wired라고 합니다. 정책 집합을 분류하고 차별화하면 문제 해결,

추가 또는 더하기 아이콘이 표시되지 않으면 정책 세트의 톱니바퀴 아이콘을 클릭할 수 있습니다. 기어 아이콘을 선택한 다음 위에 새 행 삽입을 선택합니다.



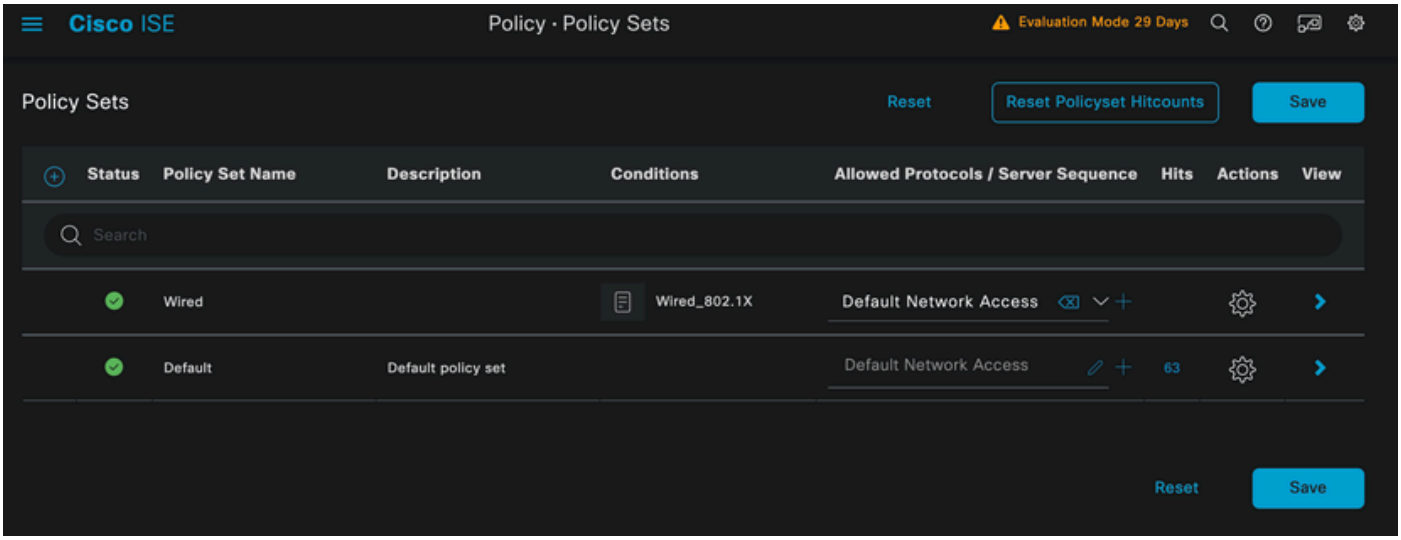
정책 생성

이 예에서 구성된 조건은 유선 8021x이며 ISE 신규 구축에서 미리 구성된 조건입니다. 드래그한 다음 Use(사용)를 클릭합니다.



조건 스튜디오

마지막으로, Default Network Access preconfigured allowed protocols service(기본 네트워크 액세스 사전 구성된 프로토콜 서비스)를 선택합니다.

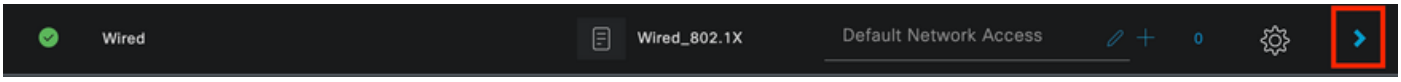


정책 설정 보기

저장을 클릭합니다.

2. d. 인증 및 권한 부여 정책을 구성합니다.

방금 생성한 정책 세트의 오른쪽에 있는 화살표를 클릭합니다.



유선 정책 집합

Authentication Policy(인증 정책)를 펼칩니다

+아이콘을 클릭합니다.

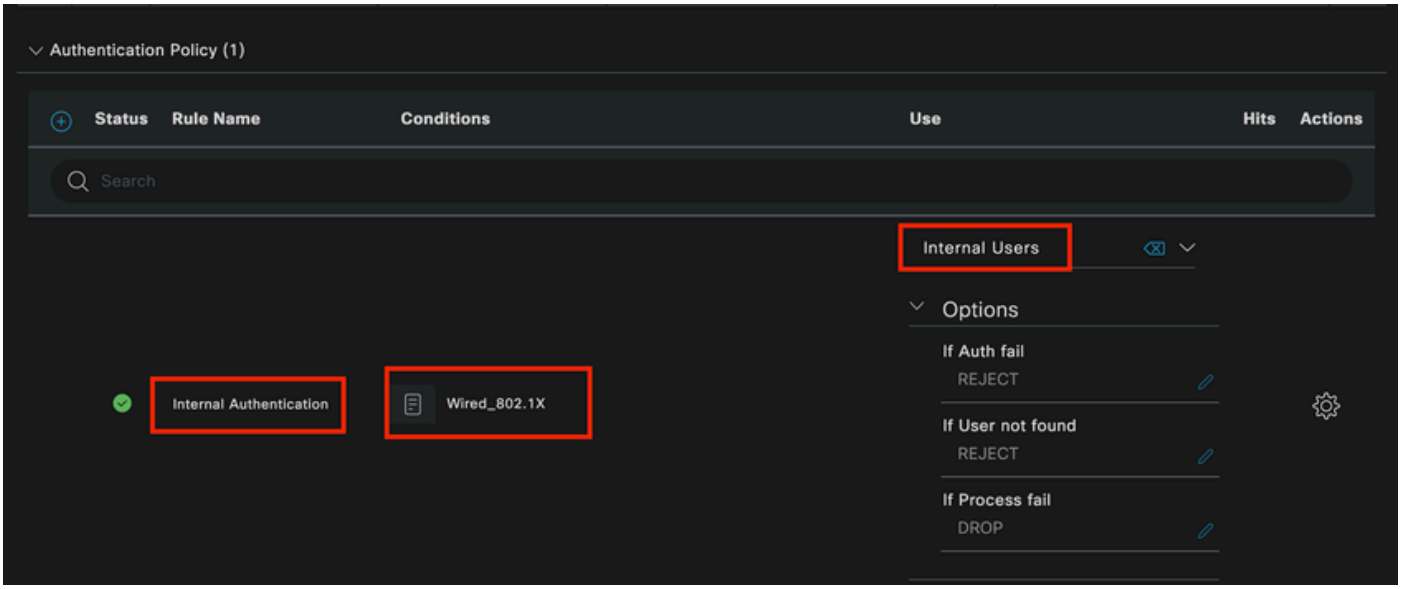
인증 정책 추가

인증 정책에 이름을 할당합니다. 예를 들어 내부 인증이 사용됩니다.

이 새 인증 정책의 조건 열에 있는 + 아이콘을 클릭합니다.

Wired Dot1x ISE와 함께 제공되는 사전 구성된 조건을 사용할 수 있습니다.

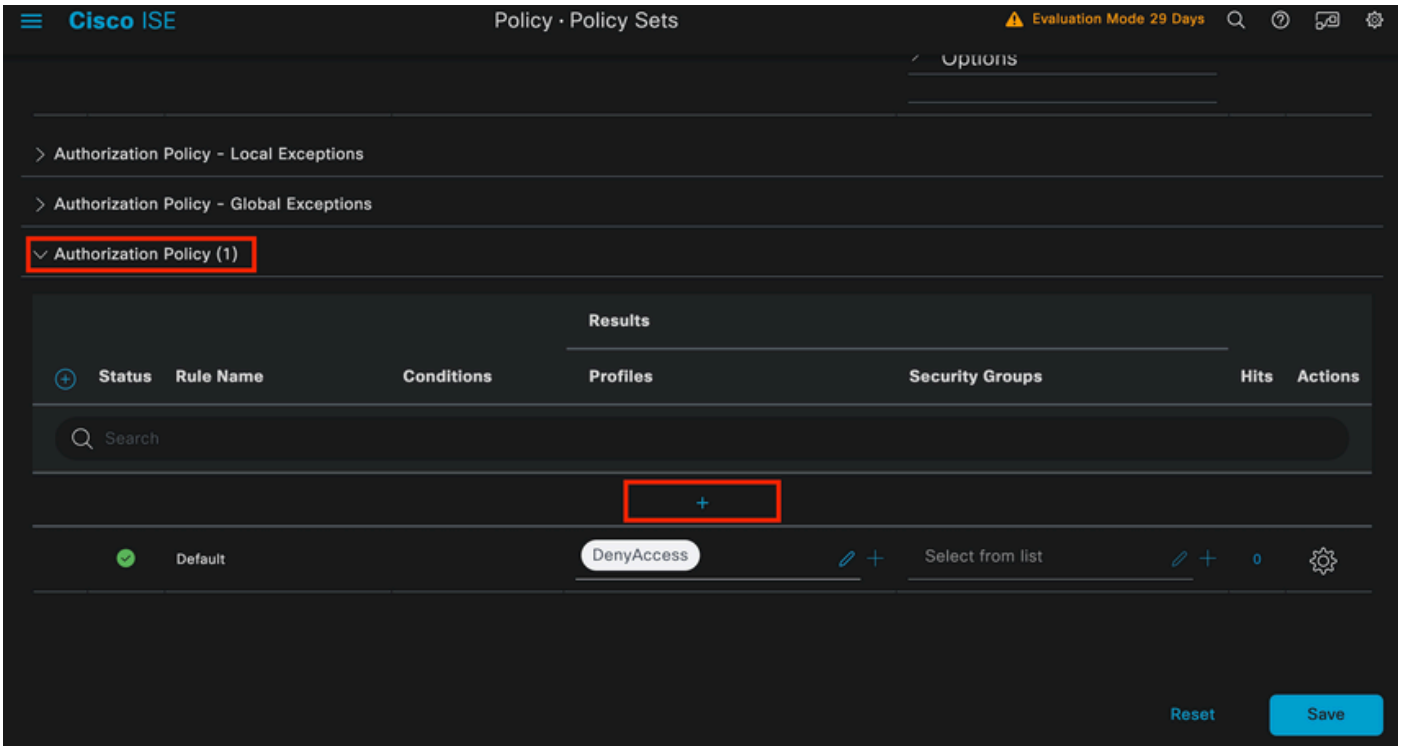
마지막으로 Use(사용) 열의 드롭다운 목록에서 Internal Users(내부 사용자)를 선택합니다.



인증 정책

권한 부여 정책

권한 부여 정책 섹션은 페이지 하단에 있습니다. 확장한 다음 + 아이콘을 클릭합니다.



권한 부여 정책

방금 추가한 권한 부여 정책의 이름을 지정합니다. 이 컨피그레이션에서는 Internal ISE Users라는 이름이 사용됩니다.

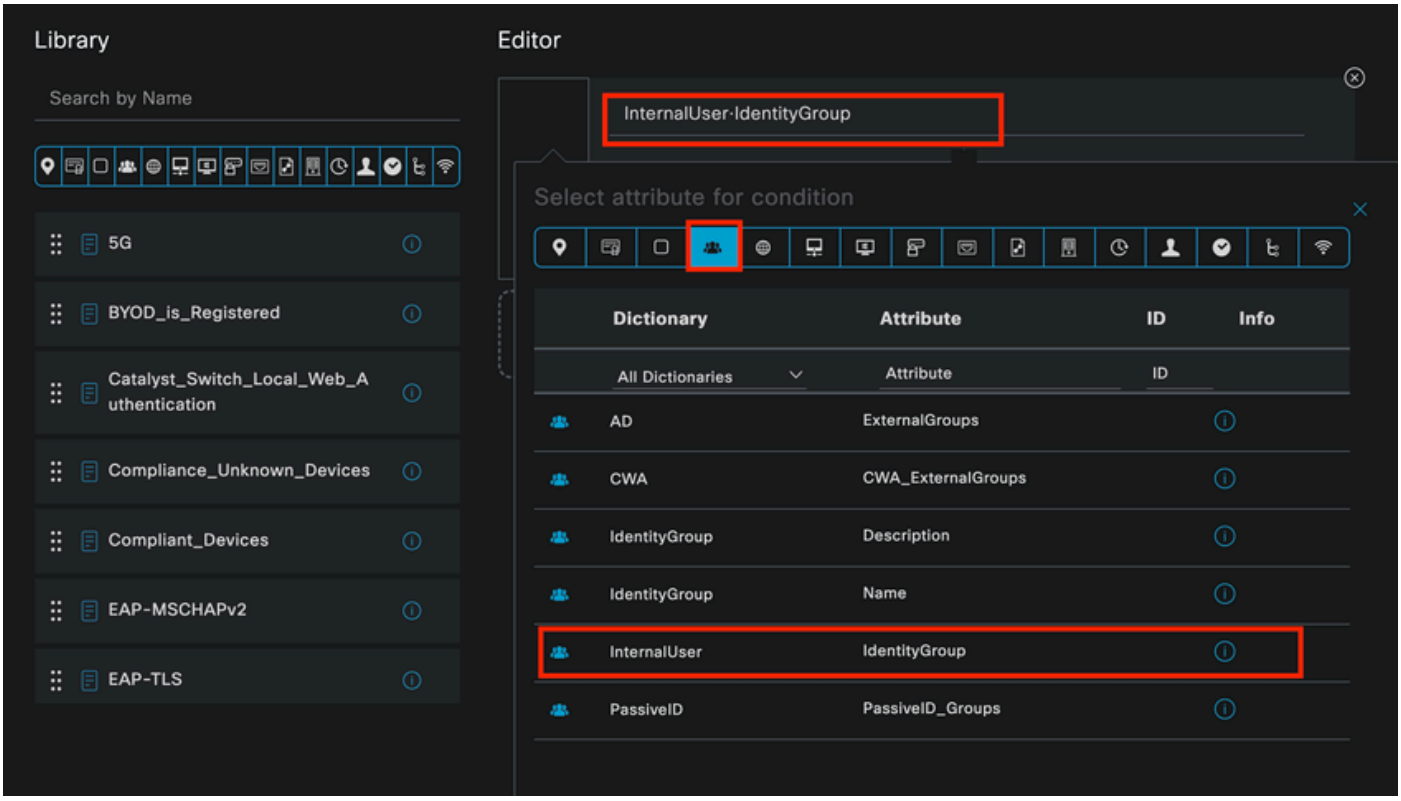
이 권한 부여 정책에 대한 조건을 생성하려면 Conditions(조건) 열에서 + 아이콘을 클릭합니다.

이전에 생성한 사용자는 IseUsers 그룹의 일부입니다.

편집기에서 Click to add an attribute 섹션을 클릭합니다.

ID 그룹 아이콘을 선택합니다.

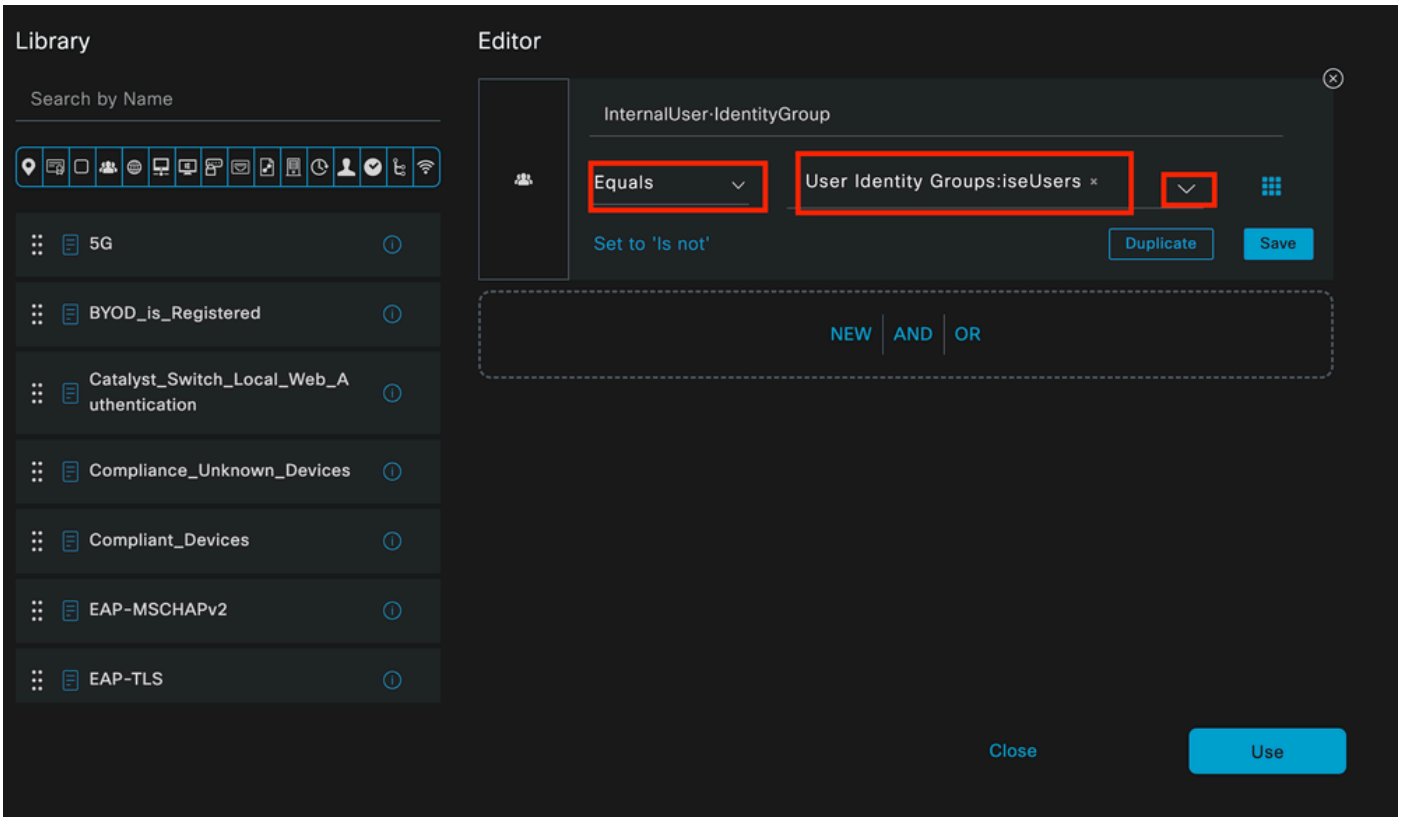
사전에서 ID 그룹 특성과 함께 제공되는 InternalUser 사전을 선택합니다.



권한 부여 정책에 대한 조건 Studio

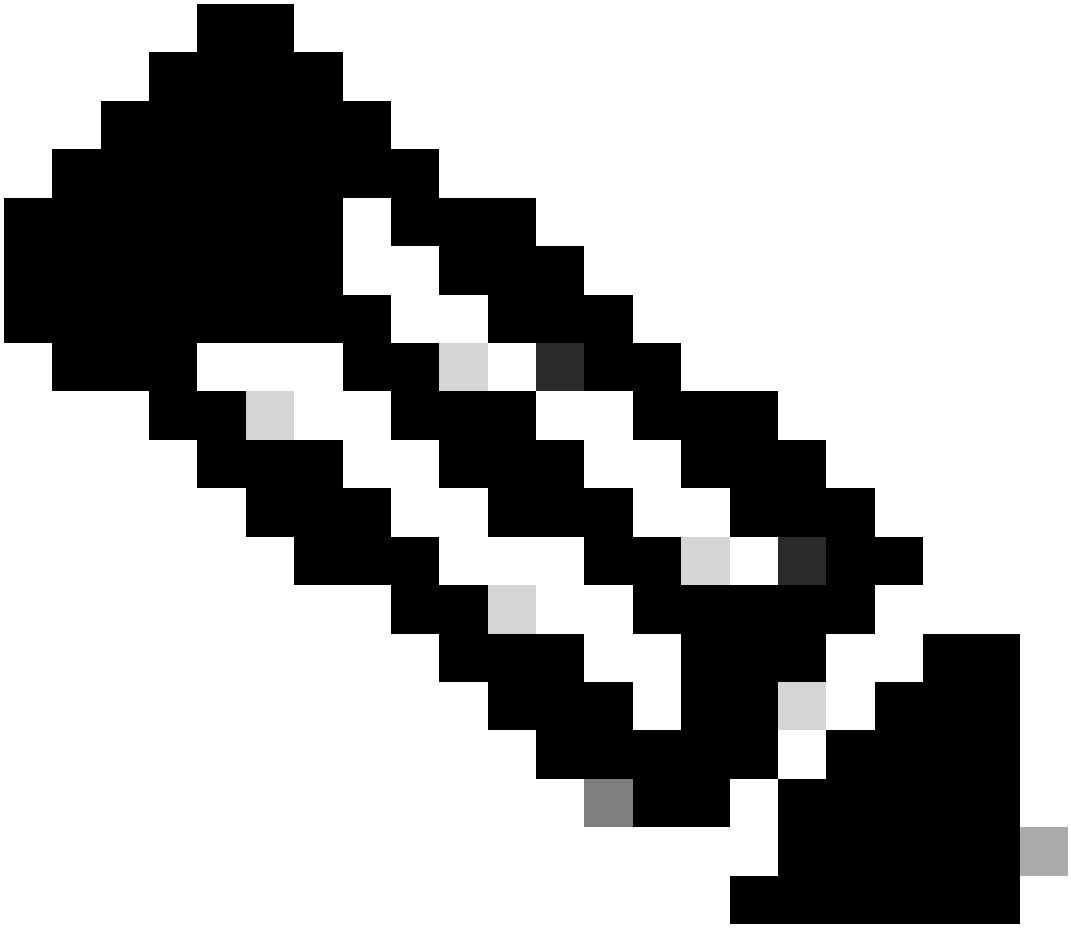
Equals(같음) 연산자를 선택합니다.

User Identity Groups(사용자 ID 그룹) 드롭다운 목록에서 그룹 IseUsers를 선택합니다.



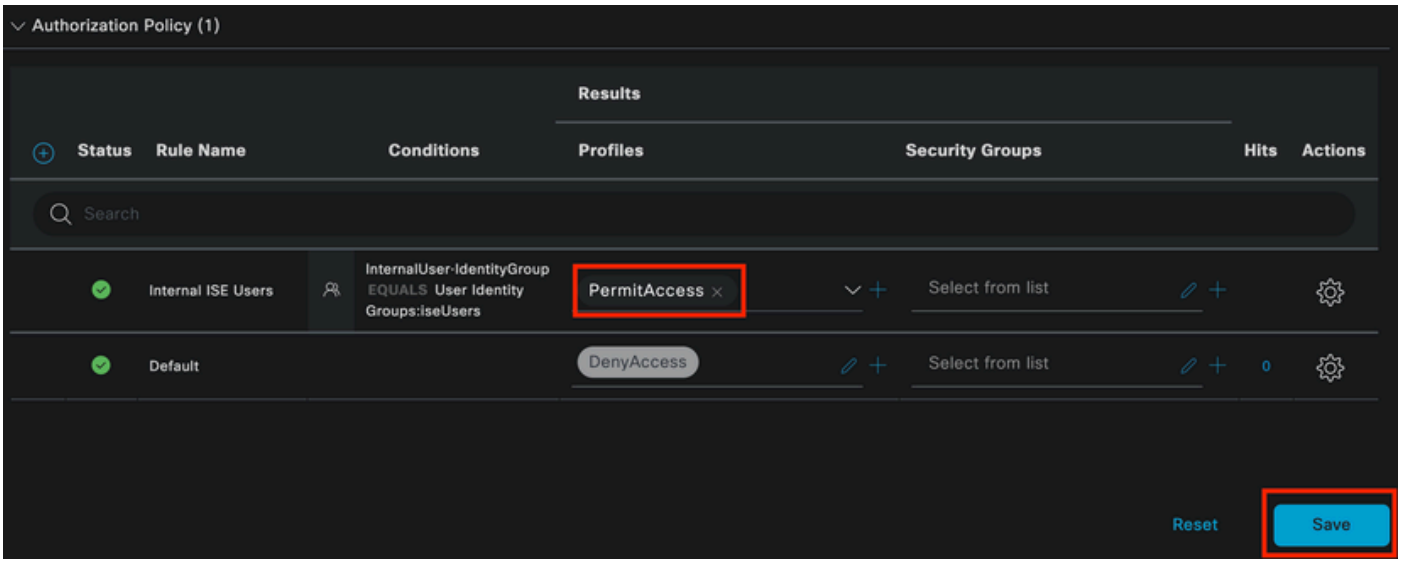
Use(사용)를 클릭합니다.

마지막으로, 이 ID 그룹의 인증 부분을 받는 결과 권한 부여 프로파일을 선택합니다.



> 참고: ISE로 인증 이 사용자 ID 그룹 ISEUsers의 일부가 아닌 이 유선 Dot1x 정책 집합에 적중이 이제 기본 권한 부여 정책을 적중 합니다. 프로필 결과 DenyAccess가 있습니다.

ISE는 Permit Access(액세스 허용) 프로필로 사전 구성됩니다. 선택합니다.



권한 부여 정책 완료

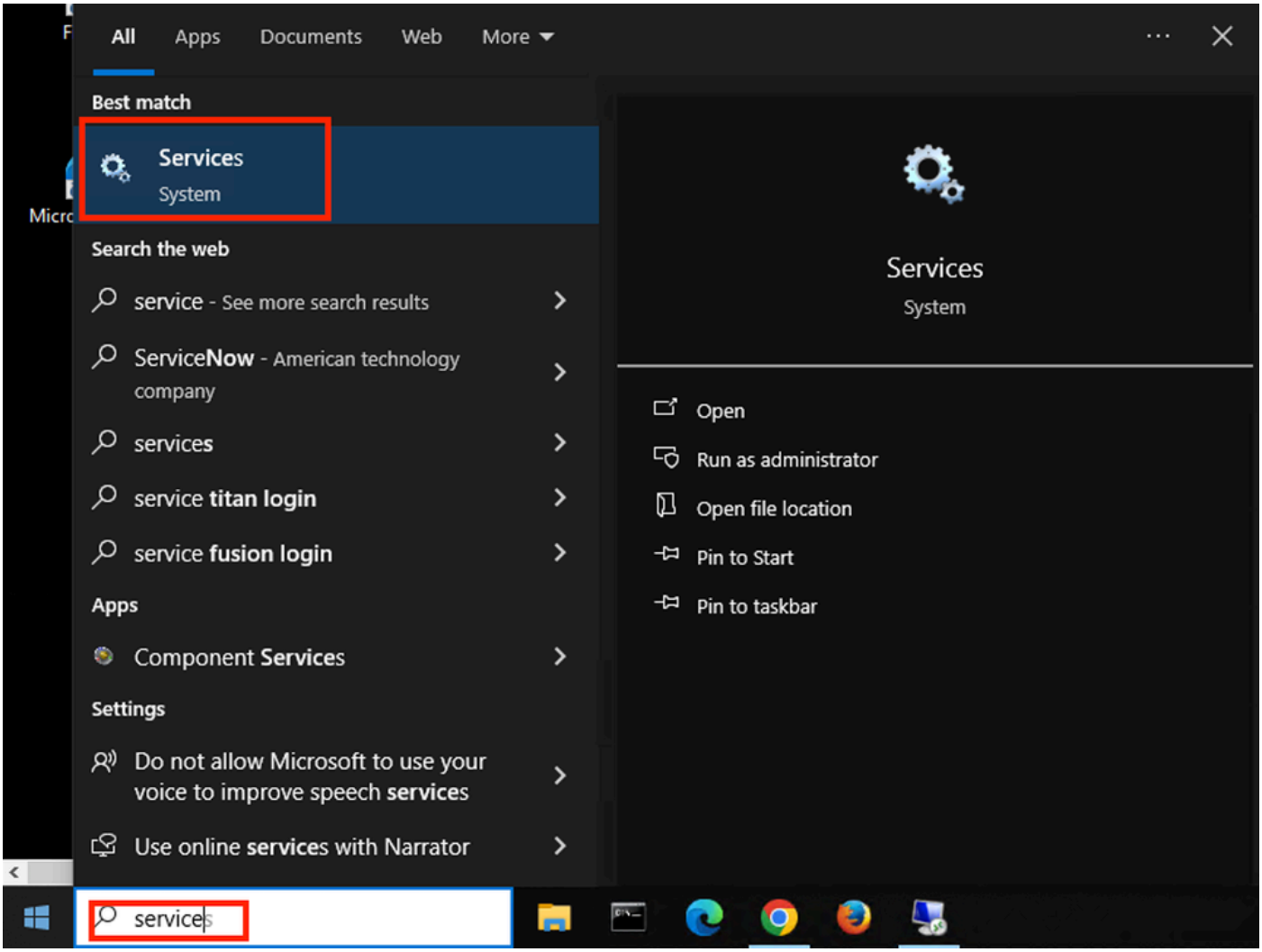
저장을 클릭합니다.

ISE에 대한 컨피그레이션이 완료되었습니다.

3단계. Windows 네이티브 서 플리 컨 트 구성

3. a. Windows에서 유선 dot1x를 사용하도록 설정합니다.

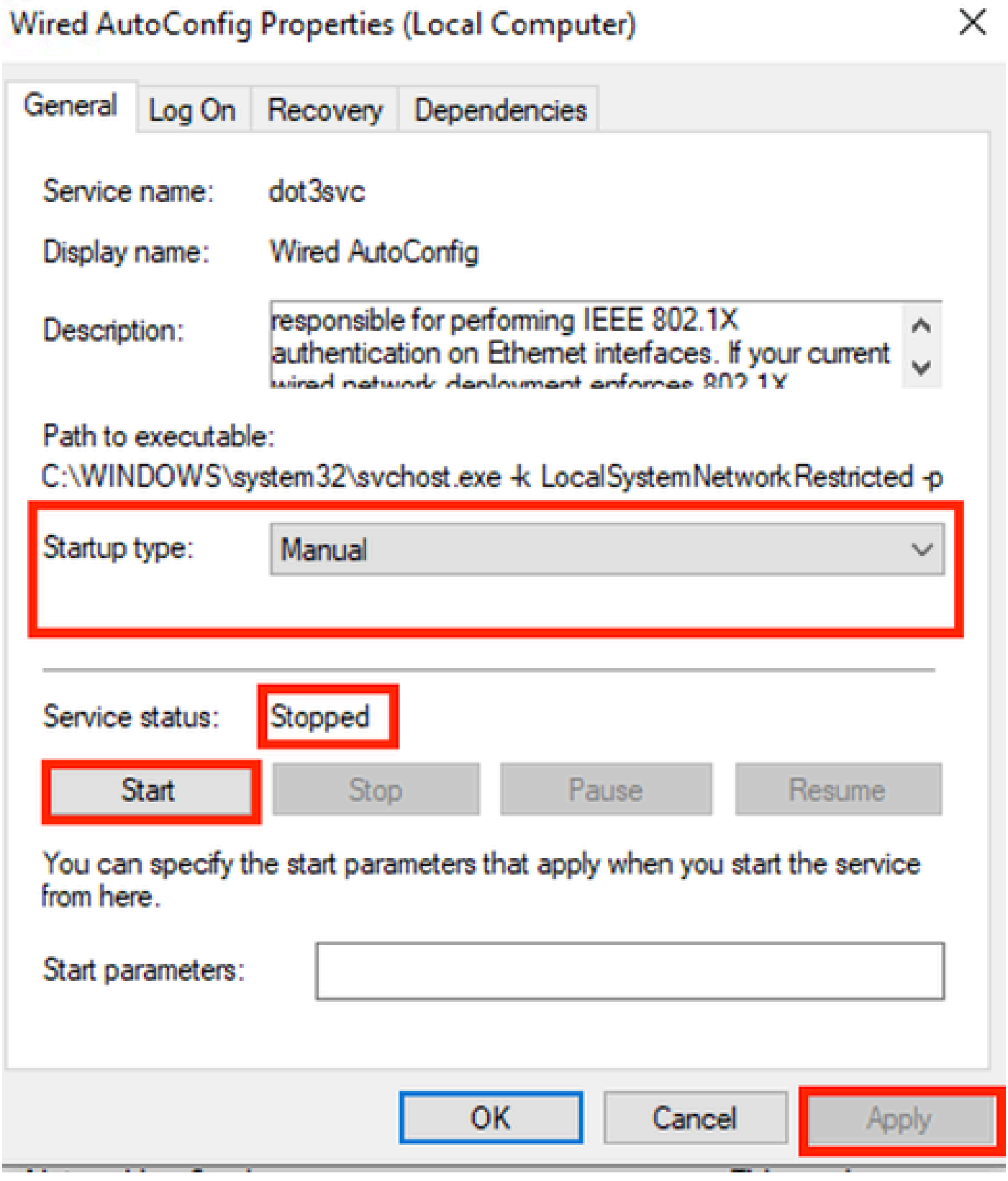
Windows 검색 표시줄에서 서비스를 엽니다.



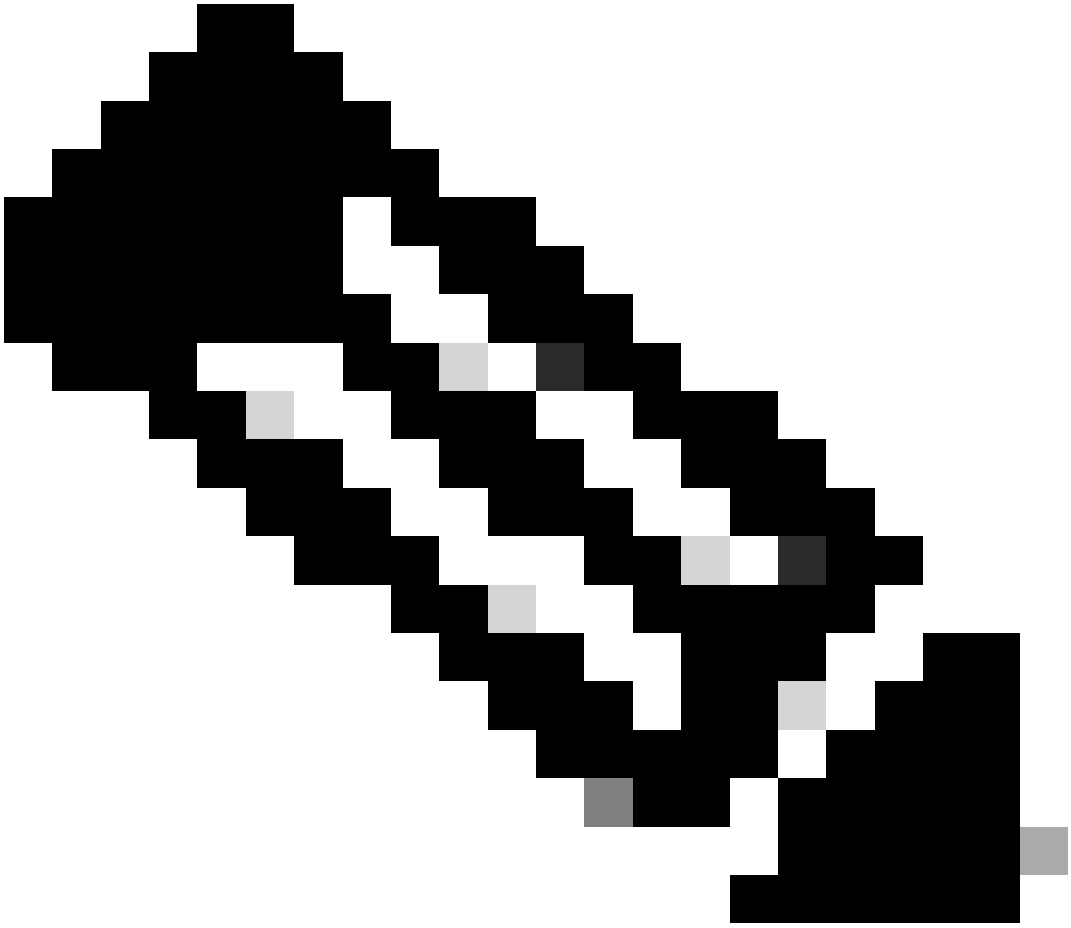
Windows 검색 표시줄

Services(서비스) 목록 하단에서 Wired Autoconfig(유선 자동 컨피그레이션)를 찾습니다.

Wired AutoConfig(유선 자동 구성)를 마우스 오른쪽 버튼으로 클릭하고 Properties(속성)를 선택합니다.


Wired AutoConfig Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
dot3svc
Display name:
Wired AutoConfig
Description:
responsible for performing IEEE 802.1X
authentication on Ethernet interfaces. If your current
Path to executable:
C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p
Startup type:
Manual
Service status:
Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service
from here.
Start parameters:
OK
Cancel
Apply

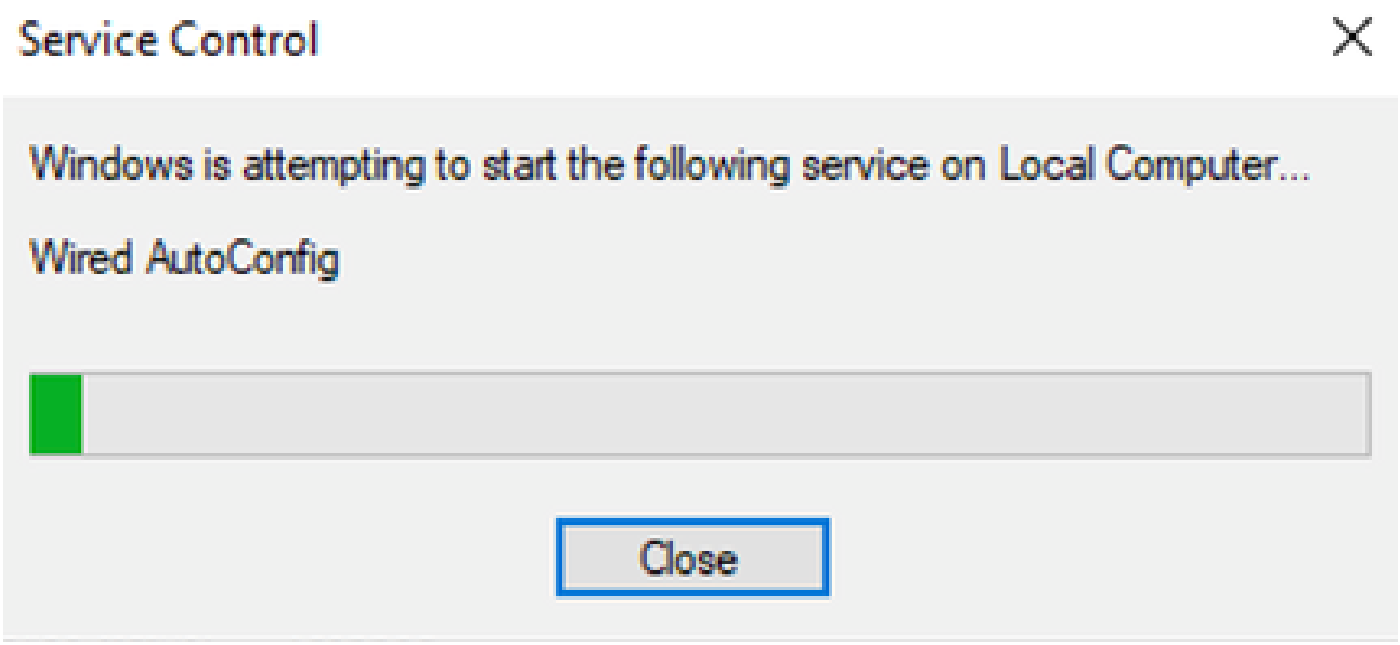
속성 창



참고: DOT3SVC(Wired AutoConfig) 서비스는 이더넷 인터페이스에서 IEEE 802.1X 인증을 수행합니다.

수동 시작 유형이 선택됩니다.

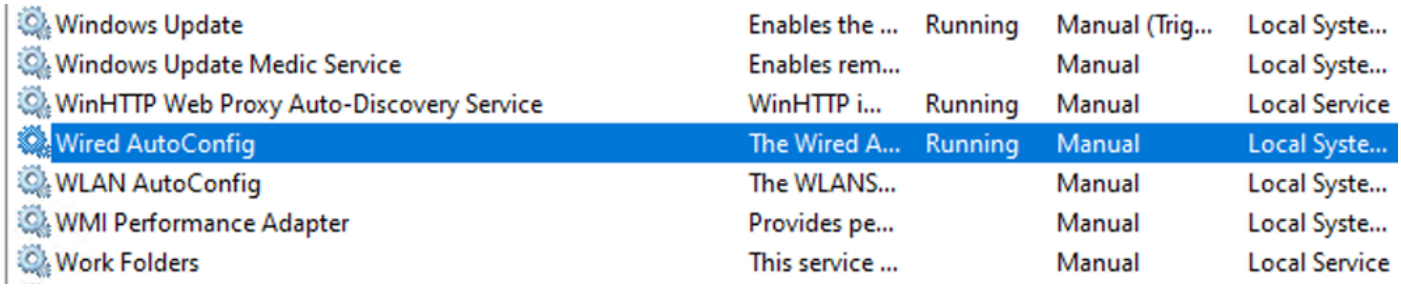
서비스 상태가 Stopped(중지됨)이므로. 시작을 클릭합니다.



서비스 제어

그런 다음 확인을 클릭합니다.

이 후에 서비스가 실행됩니다.



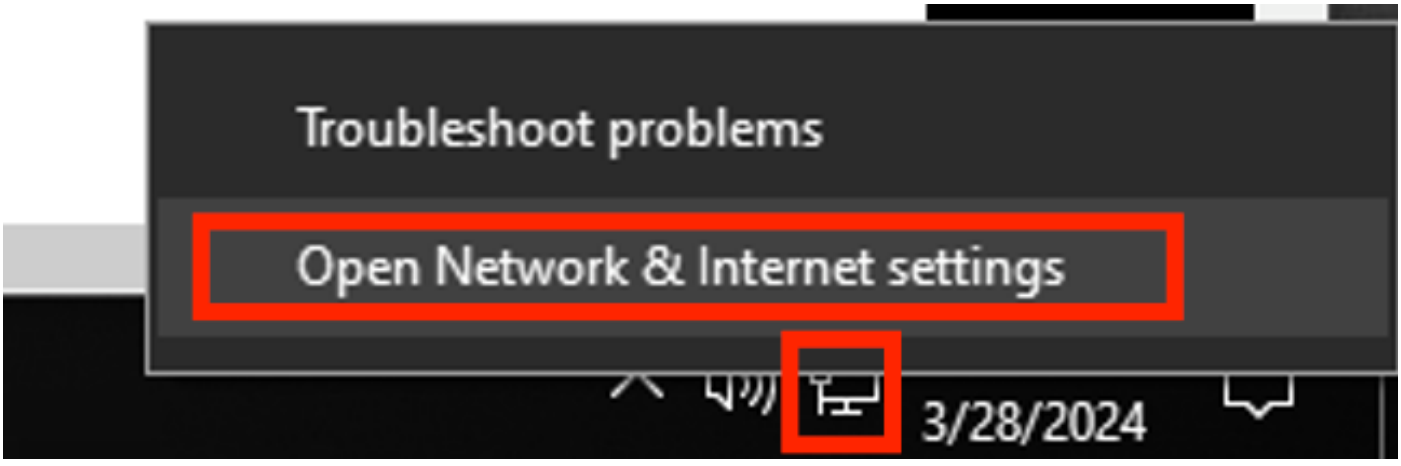
유선 자동 구성 서비스

3. b. NAD 인증자에 연결된 Windows 랩톱 인터페이스를 구성합니다(ISR 1100).

작업 표시줄에서 오른쪽 모서리를 찾은 다음 컴퓨터 아이콘을 사용합니다.

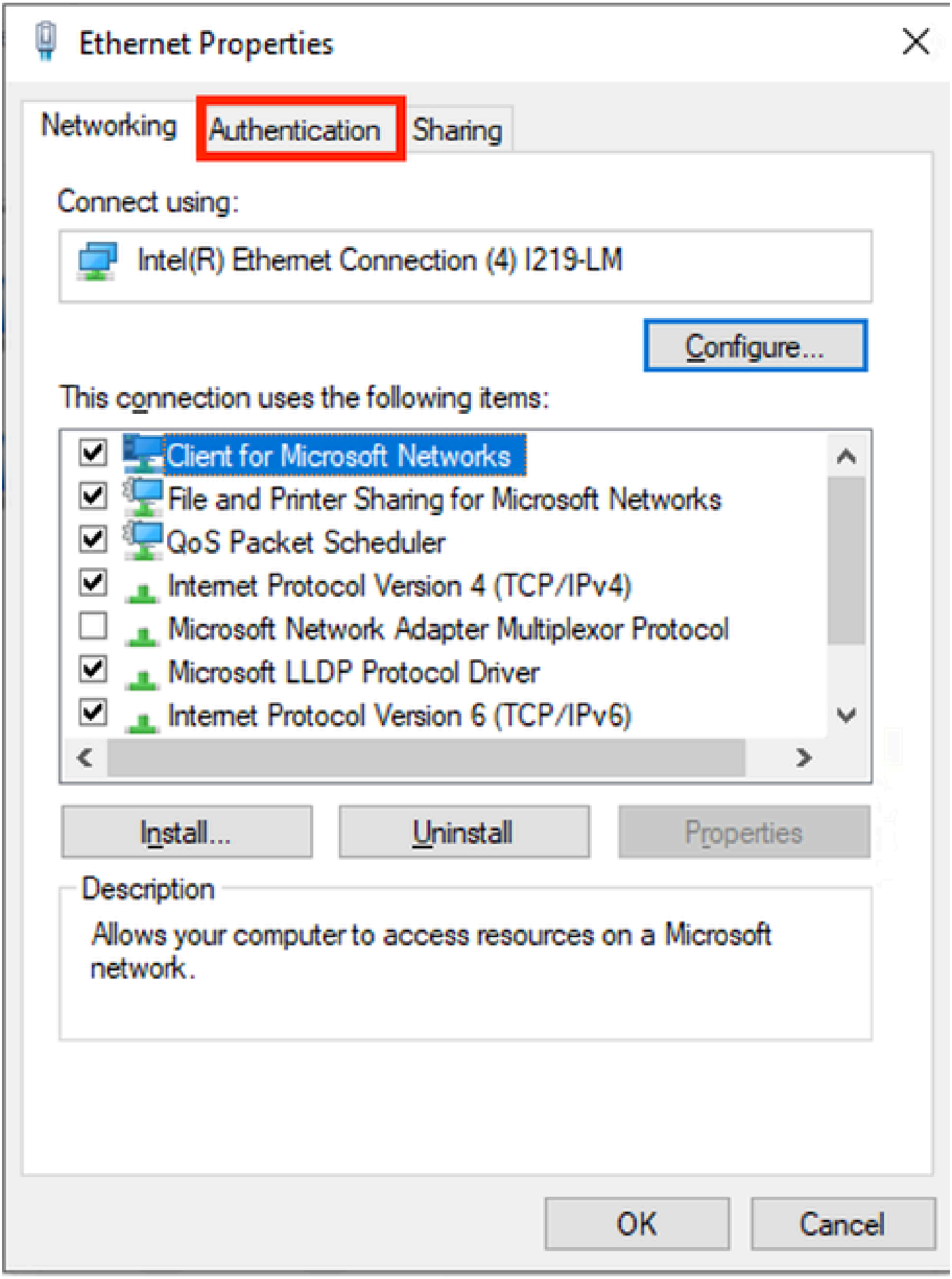
컴퓨터 아이콘을 두 번 클릭합니다.

네트워크 및 인터넷 설정 열기를 선택합니다.



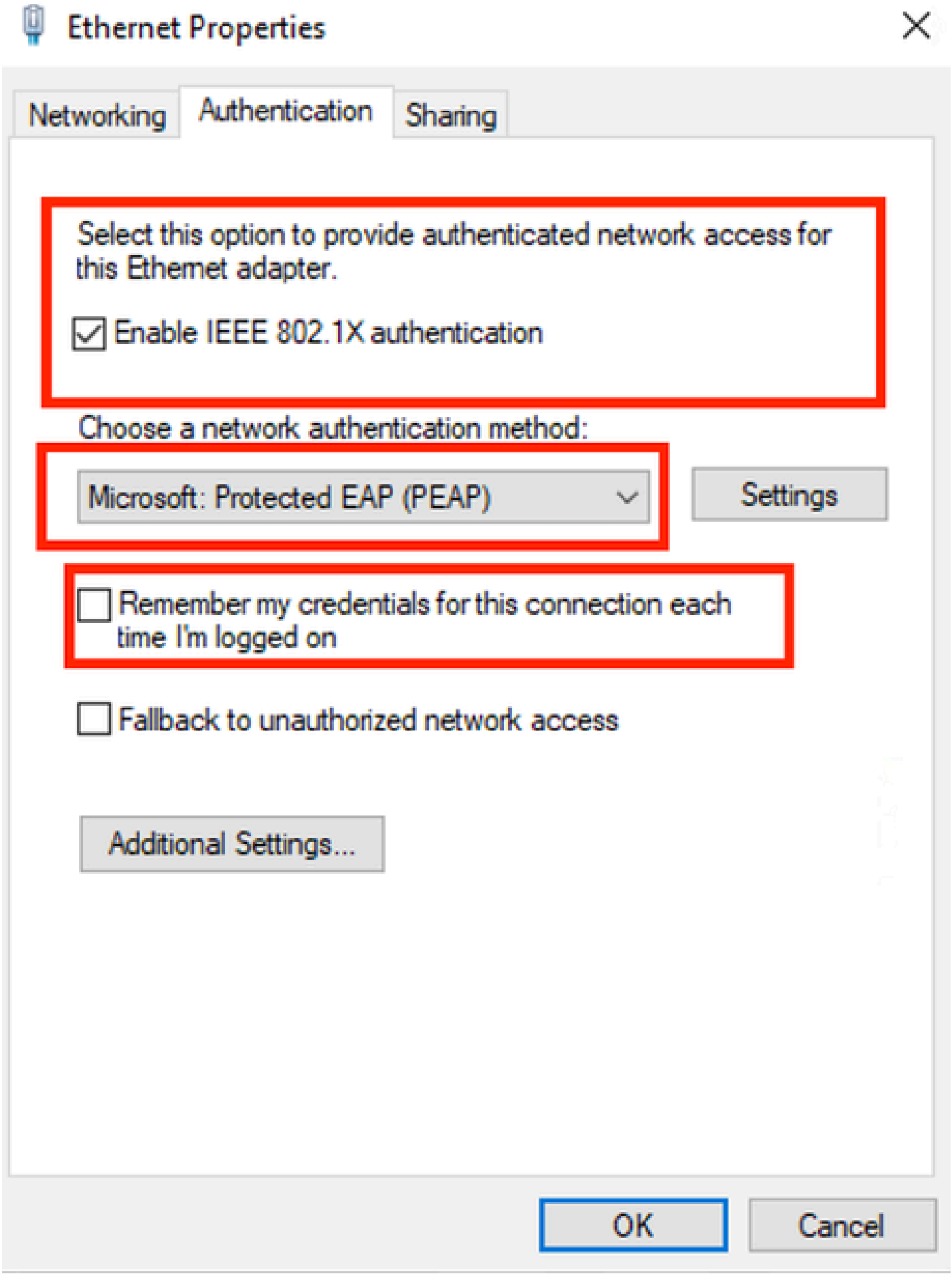
Network Connections(네트워크 연결) 창이 열리면 ISR Gig 0/1/0에 연결된 이더넷 인터페이스를 마우스 오른쪽 버튼으로 클릭합니다. Properties(속성) 옵션을 클릭합니다.

Authentication(인증) 탭을 클릭합니다.



인터페이스 이더넷 속성

Enable IEEE 802.1X authentication(IEEE 802.1X 인증 활성화) 확인란을 선택합니다.

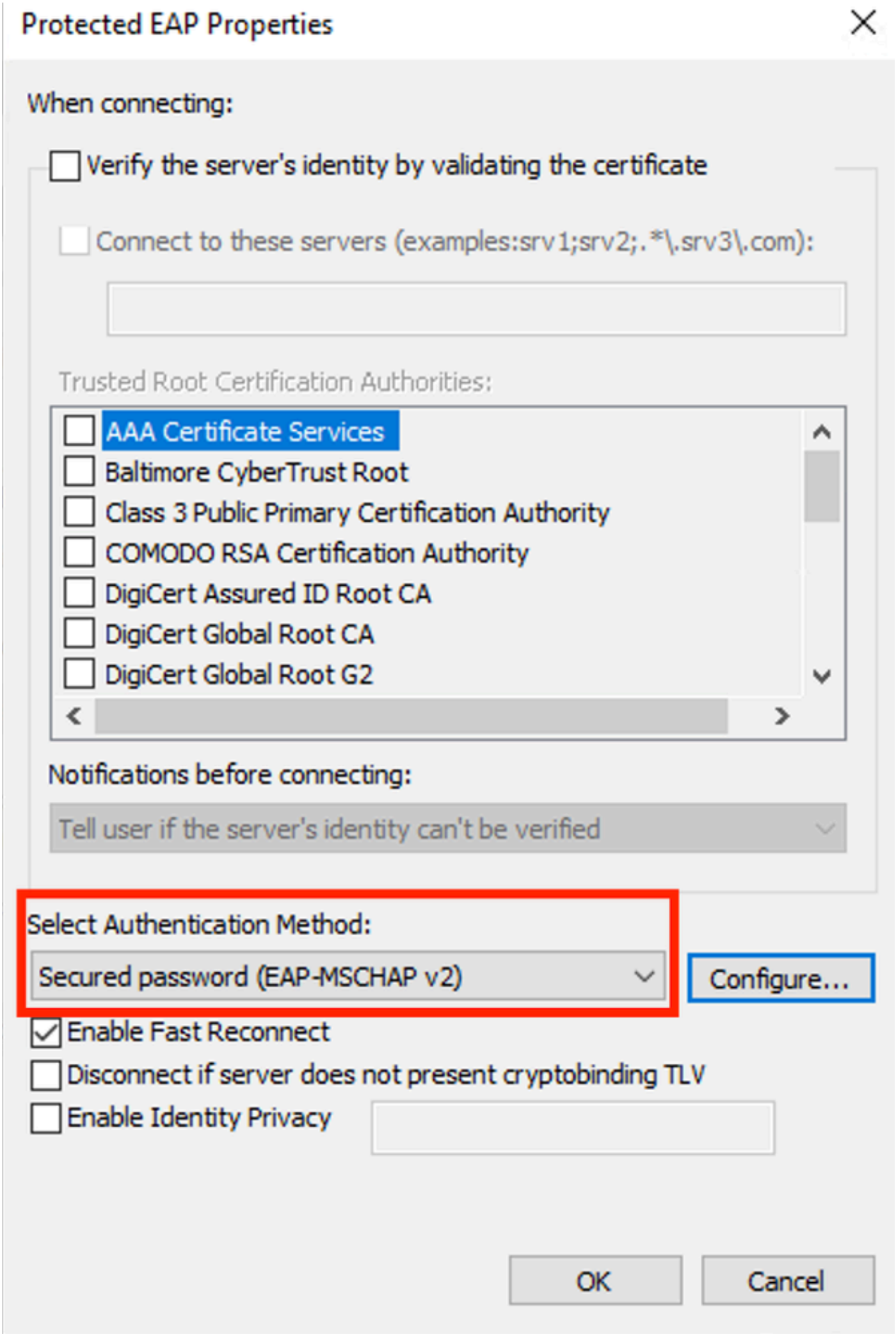

Ethernet Properties
Networking
Authentication
Sharing
Select this option to provide authenticated network access for this Ethernet adapter.
Enable IEEE 802.1X authentication
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Fallback to unauthorized network access
Additional Settings...
OK
Cancel

인증 이더넷 속성

PEAP(Protected EAP)를 선택합니다.

로그온할 때마다 이 연결에 대한 내 자격 증명 기억 옵션을 선택 취소합니다.

Settings(설정)를 클릭합니다.


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AAA Certificate Services
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert Global Root G2
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

PEAP 속성

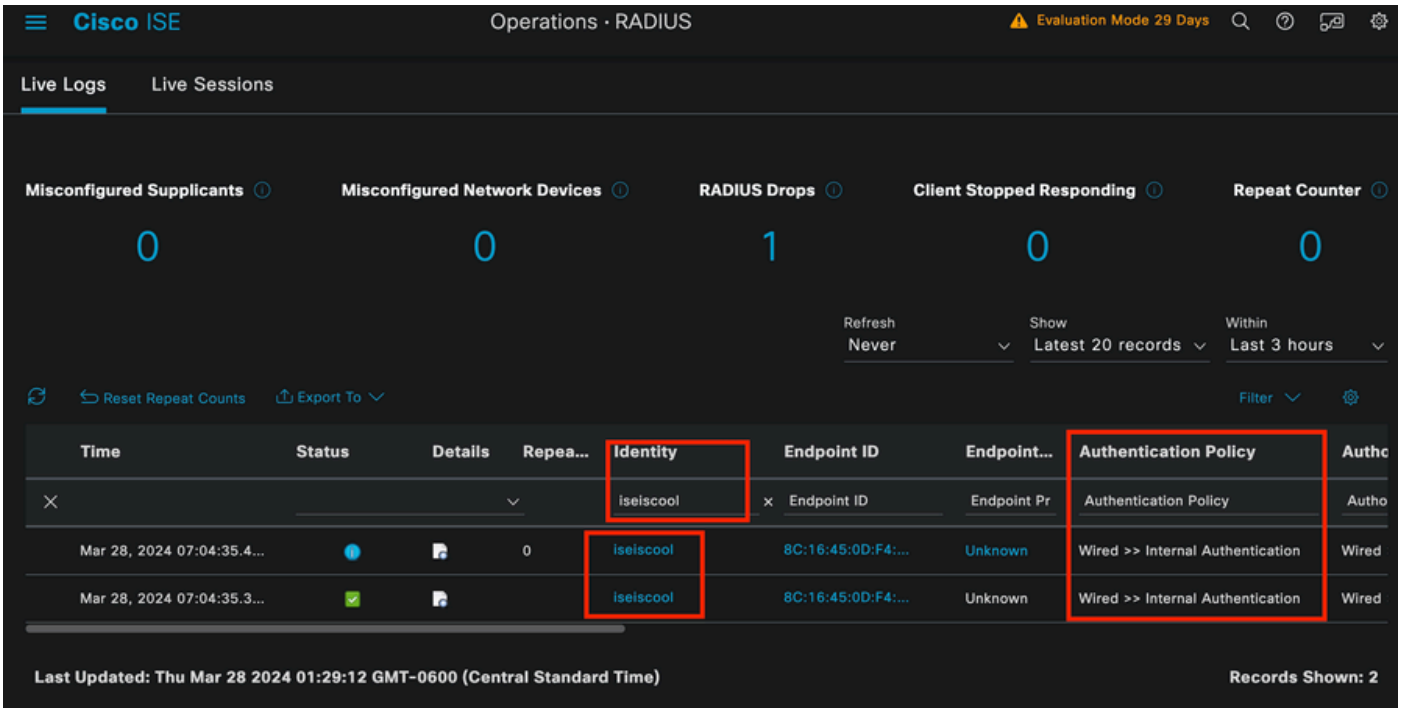
```
            Interface:  GigabitEthernet0/1/0
                IIF-ID:  0x08767C0D
           MAC Address:  8c16.450d.f42b
          IPv6 Address:  Unknown
          IPv4 Address:  Unknown
             User-Name:  iseiscool <--------- The username configured for Windows Native Supplicant
                Status:  Authorized <--------- An indication that this session was authorized by the PSN
                Domain:  DATA
        Oper host mode:  multi-auth
      Oper control dir:  both
       Session timeout:  N/A
     Common Session ID:  22781F0A0000000C83E28461
       Acct Session ID:  0x00000003
                Handle:  0xc6000002
        Current Policy:  POLICY_Gi0/1/0

Local Policies:
         Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
       Security Policy:  Should Secure

Server Policies:


Method status list:
       Method           State
         dot1x          Authc Success <--------- An indication that dot1x is used for this authenticati
```

```
Router#
```

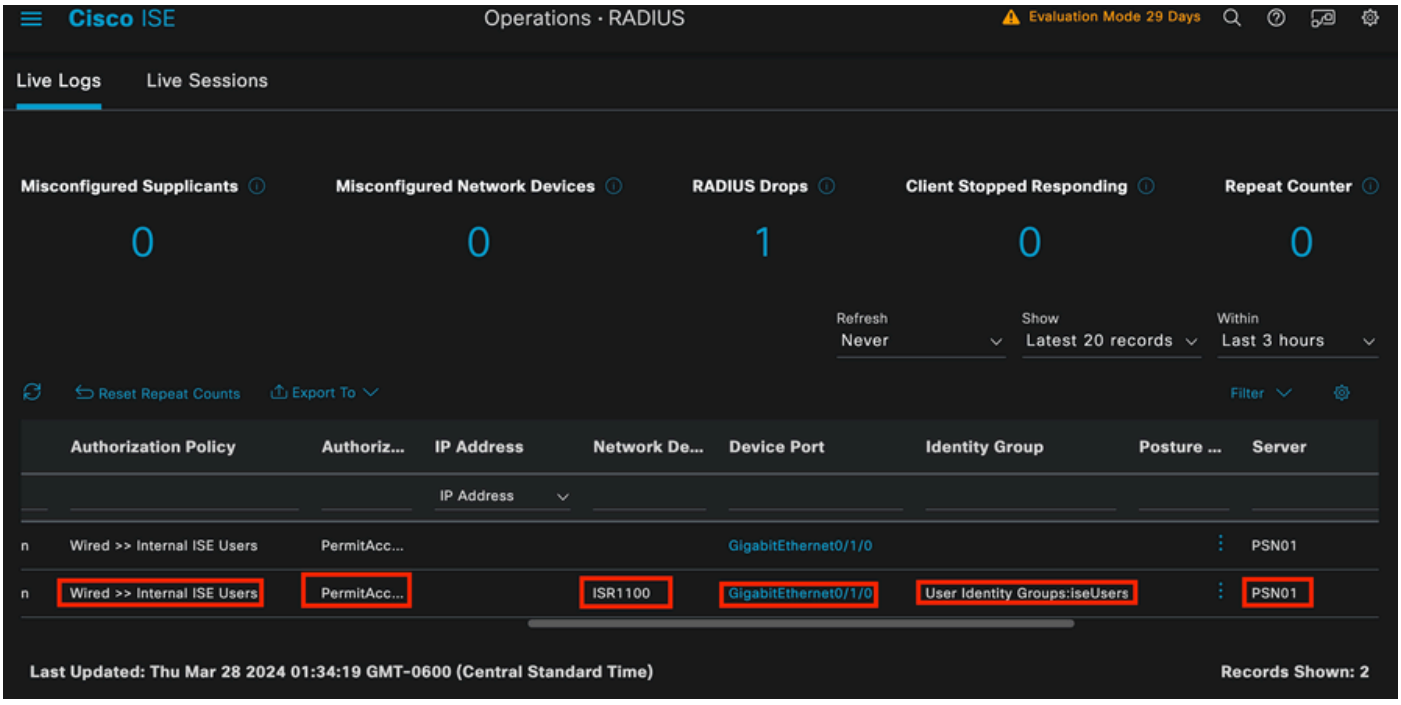
ISE 로그

Operations(운영) > Radius > Live logs(라이브 로그) 탭으로 이동합니다.

사용자 이름 ID로 필터링합니다. 이 예에서는 사용자 이름 iseiscool이 사용됩니다.



ISE 리벨로그



ISE 리벨로그

이 빠른 보기에서 라이브 로그는 다음과 같은 주요 정보를 제공합니다.

- 인증의 타임스탬프.
- 사용된 ID.
- 엔드포인트 mac 주소.
- 적중된 정책 설정 및 인증 정책.
- 적중된 정책 설정 및 권한 부여 정책.
- 인증 프로파일 결과.
- ISE에 Radius 요청을 전송하는 네트워크 디바이스입니다.
- 엔드포인트가 연결되는 인터페이스.
- 인증된 사용자의 ID 그룹입니다.
- 인증을 처리한 PSN(Policy Server Node)

문제 해결

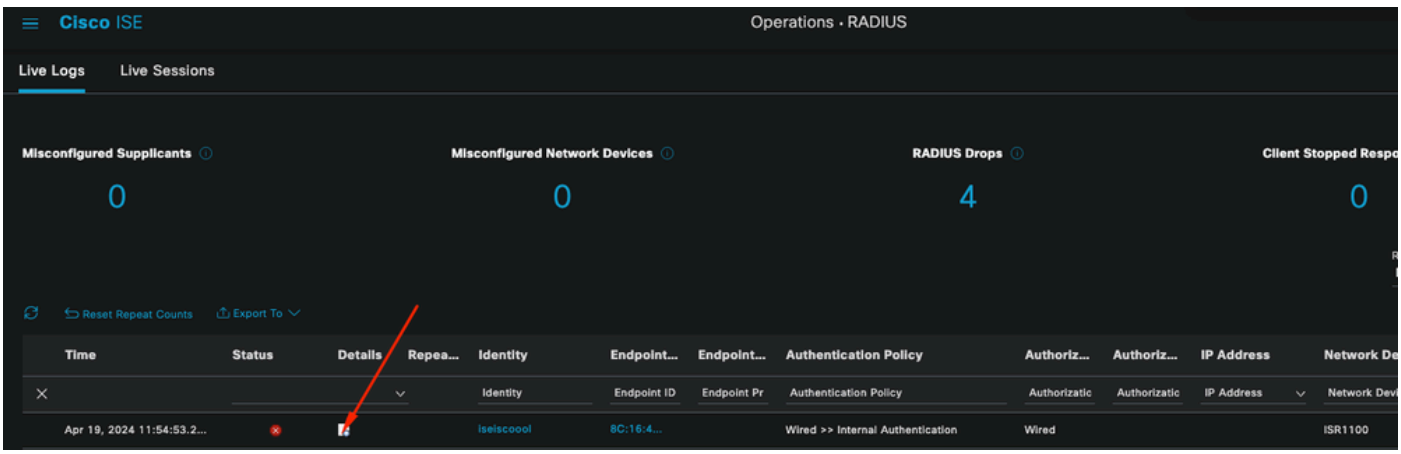
1 - ISE 라이브 로그 세부 정보 읽기

Operations(운영) > Radius > Live logs(라이브 로그) 탭으로 이동하여 Filter by Auth status: Failed(인증 상태: 실패)로 이동하거나, 사용자 이름을 사용하여 필터링하거나, MAC 주소를 사용하여 필터링하거나, 사용된 네트워크 액세스 디바이스를 사용하여 필터링합니다.

Operations(작업) > Radius > Live logs(라이브 로그) > Desired authentication(원하는 인증) > Live log details(라이브 로그 세부사항)에 액세스합니다.

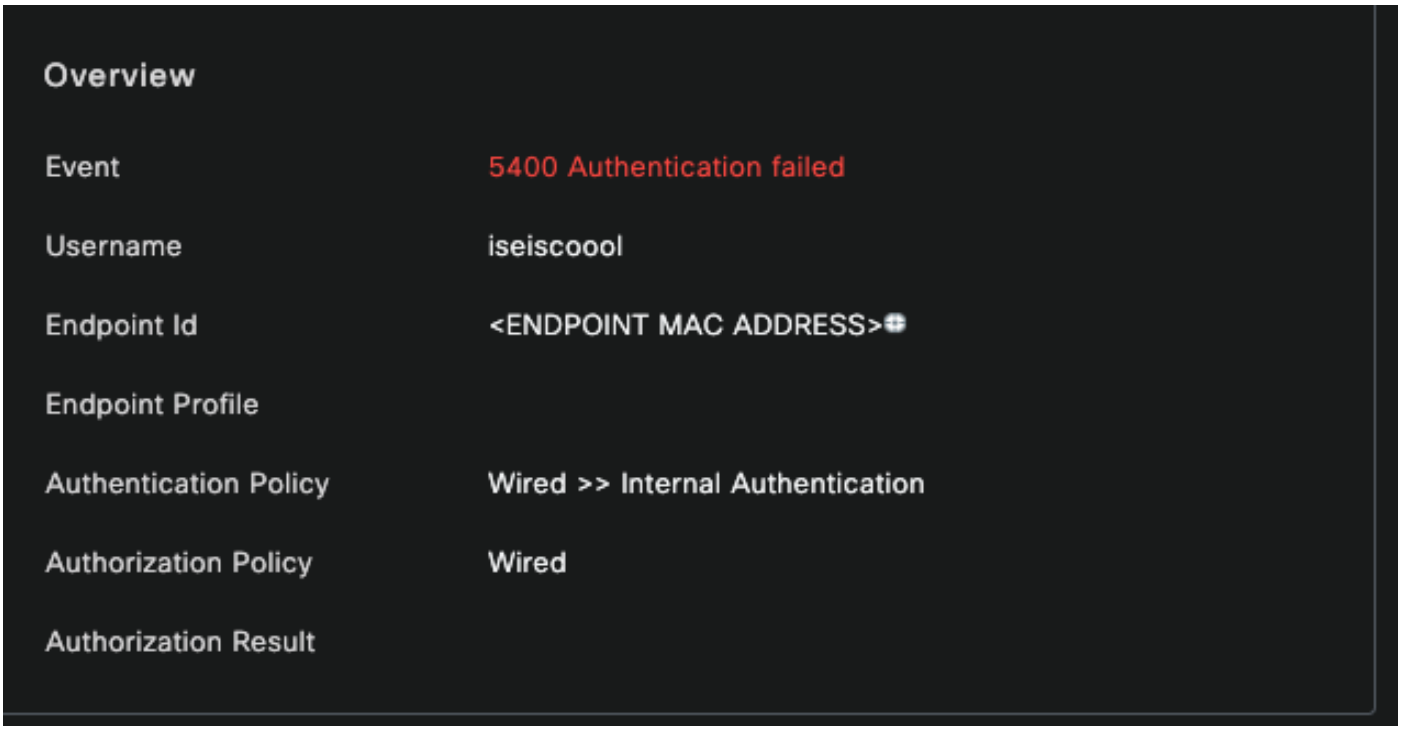
동일한 페이지에서 인증이 필터링되면 검색 아이콘을 클릭합니다.

첫 번째 시나리오: 사용자가 오타를 사용하여 사용자 이름을 입력합니다.



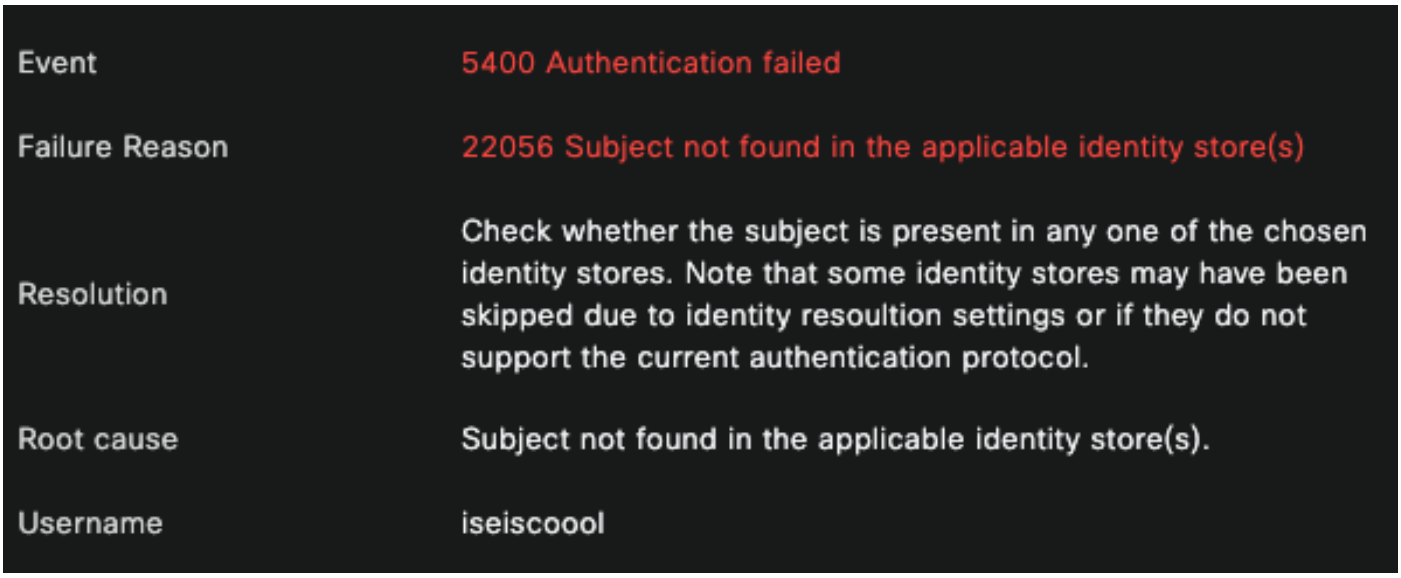
라이브 로그 세부 정보 열기

라이브 로그 세부 정보가 열리면 인증에 실패하고 사용된 사용자 이름도 나열된 것을 확인할 수 있습니다.



개요 섹션

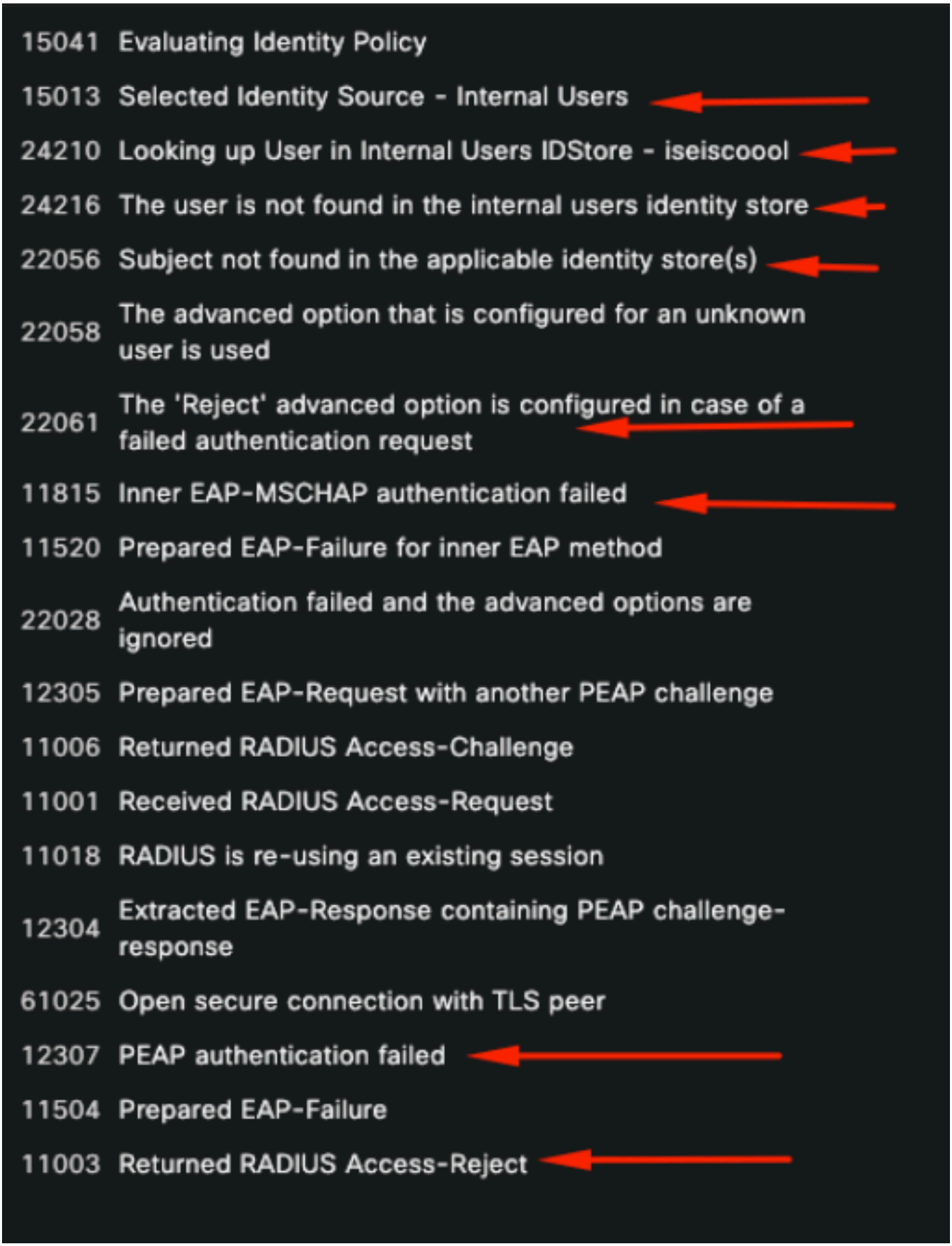
그런 다음 Authentication Details(인증 세부사항) 섹션에서 동일한 라이브 로그 세부사항에서 실패 사유, 근본 원인 및 오류 해결을 찾을 수 있습니다.



인증 세부 정보

이 시나리오에서 인증에 실패하는 이유는 사용자 이름에 오타가 있기 때문입니다. 그러나 사용자가 ISE에서 생성되지 않았거나 ISE에서 사용자가 다른 ID 저장소(예: LDAP 또는 AD)에 있는지 검증할 수 없는 경우 동일한 오류가 표시됩니다.

단계 섹션



라이브 로그 세부 정보 단계 섹션

단계 섹션에서는 RADIUS 대화 중에 ISE가 실행된 프로세스에 대해 자세히 설명합니다.

다음과 같은 정보를 여기에서 찾을 수 있습니다.

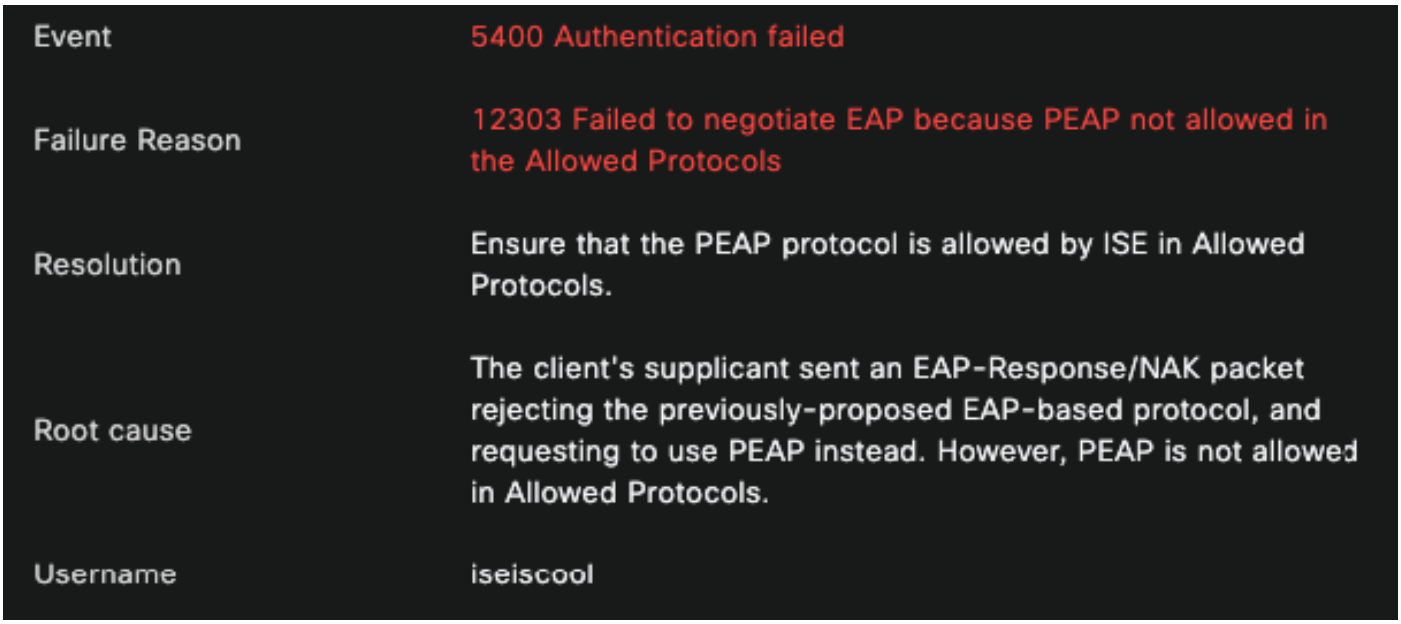
- 대화를 시작한 방법입니다.
- SSL 핸드셰이크 프로세스.
- 협상된 EAP 방법입니다.
- EAP 방법 프로세스.

이 예에서는 ISE가 이 인증을 위해 내부 ID를 방금 체크 인했음을 확인할 수 있습니다. 사용자를 찾을 수 없으므로 ISE에서 Access-Reject(액세스 거부)에 대한 응답으로 보냈습니다.

두 번째 시나리오: ISE 관리자가 Policy Set Allowed 프로토콜에서 PEAP를 비활성화했습니다.

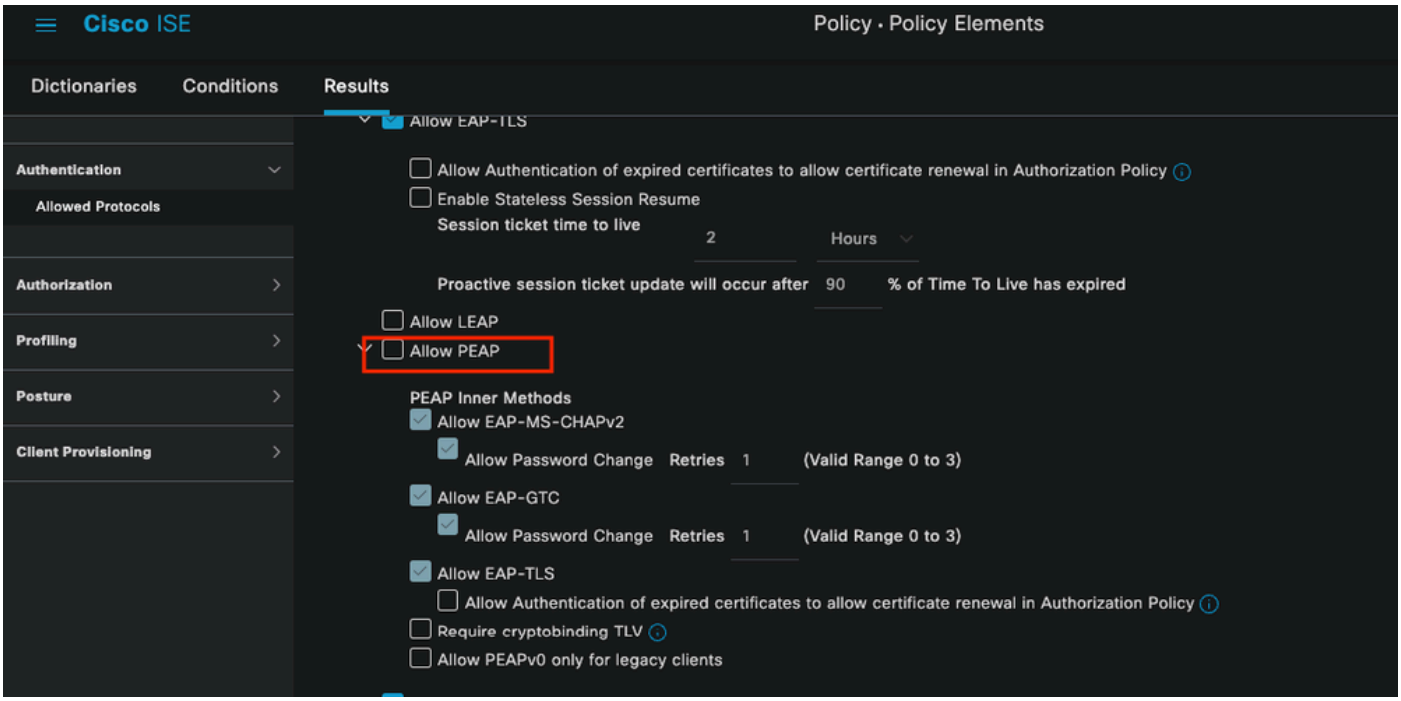
2 - 비활성화된 PEAP

실패한 세션의 라이브 로그 세부사항이 열리면 "PEAP는 허용되는 프로토콜에서 허용되지 않습니다."라는 오류 메시지가 표시됩니다.



라이브 로그 세부 정보 보고서

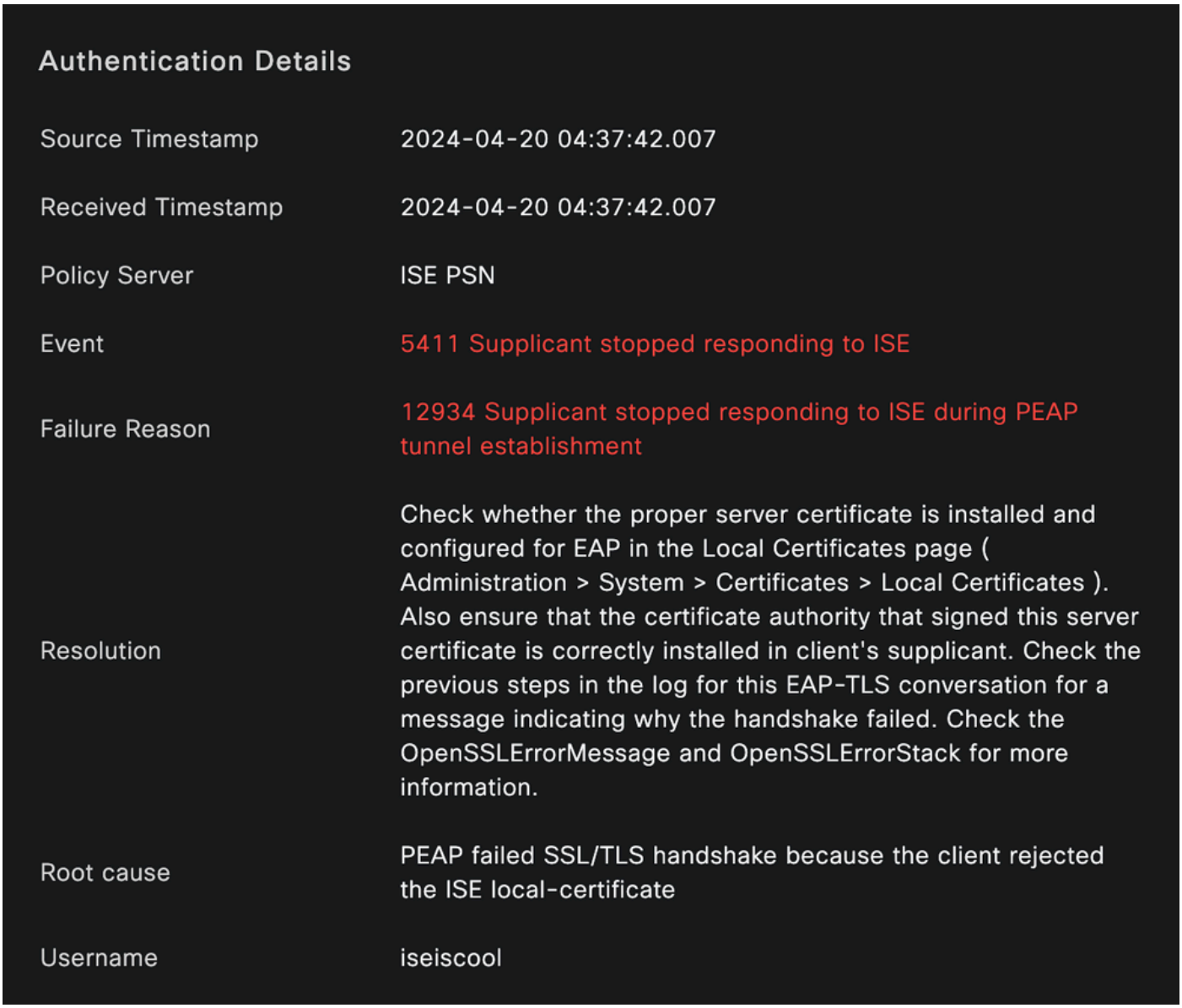
이 오류는 쉽게 해결할 수 있습니다. 해결 방법은 Policy(정책) > Policy Elements(정책 요소) > Authentication(인증) > Allowed Protocols(허용된 프로토콜)로 이동하는 것입니다. Allow PEAP(PEAP 허용) 옵션이 비활성화되었는지 확인합니다.



허용된 포털 섹션

세 번째 시나리오: 엔드포인트가 ISE 인증서를 신뢰하지 않으므로 인증이 실패합니다.

라이브 로그 세부 정보로 이동합니다. 실패한 인증에 대한 레코드를 찾아 라이브 로그 세부 정보를 확인합니다.

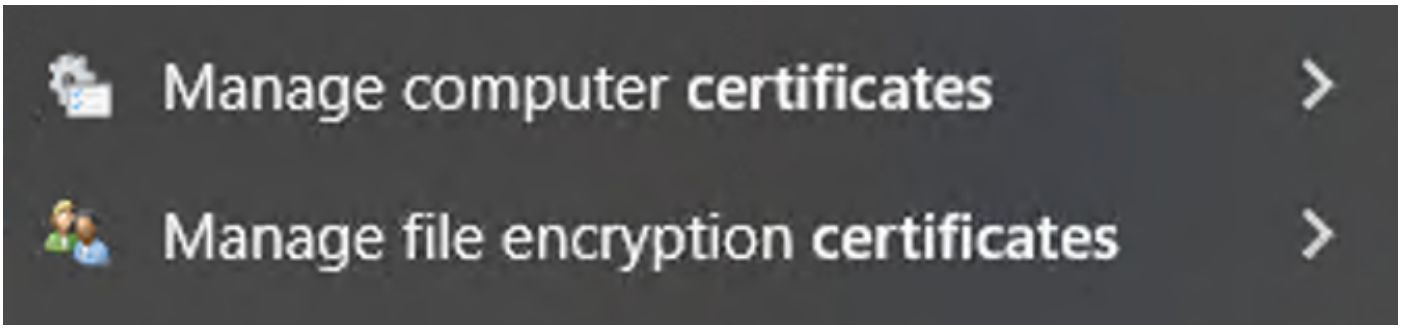


라이브 로그 세부 정보

엔드포인트가 PEAP 터널 설정에 사용된 인증서를 거부합니다.

이 문제를 해결하려면 문제가 있는 Windows 엔드포인트에서 ISE 인증서를 서명한 CA 체인이 Windows 섹션 Manage User Certificates(사용자 인증서 관리) > Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) 또는 Manage Computer Certificates(컴퓨터 인증서 관리) > Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관)에 있는지 확인합니다.

Windows 검색 표시줄에서 검색하여 Windows 디바이스에서 이 컨피그레이션 섹션에 액세스할 수 있습니다.

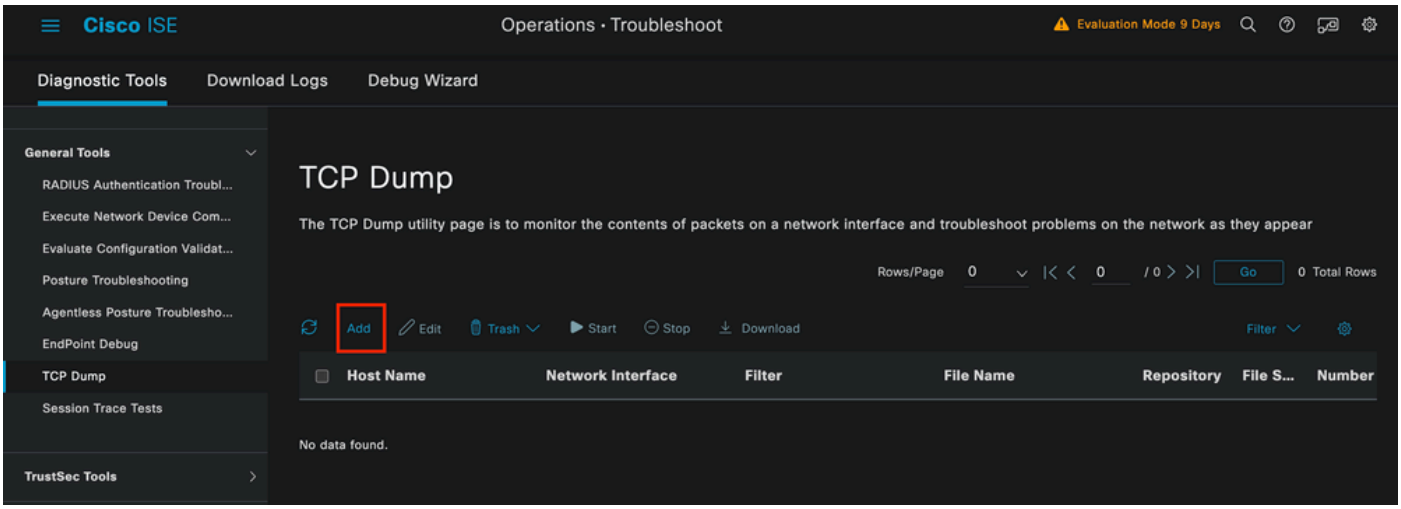


Windows 검색 창 결과

3 - ISE TCP 덤프 도구(패킷 캡처)

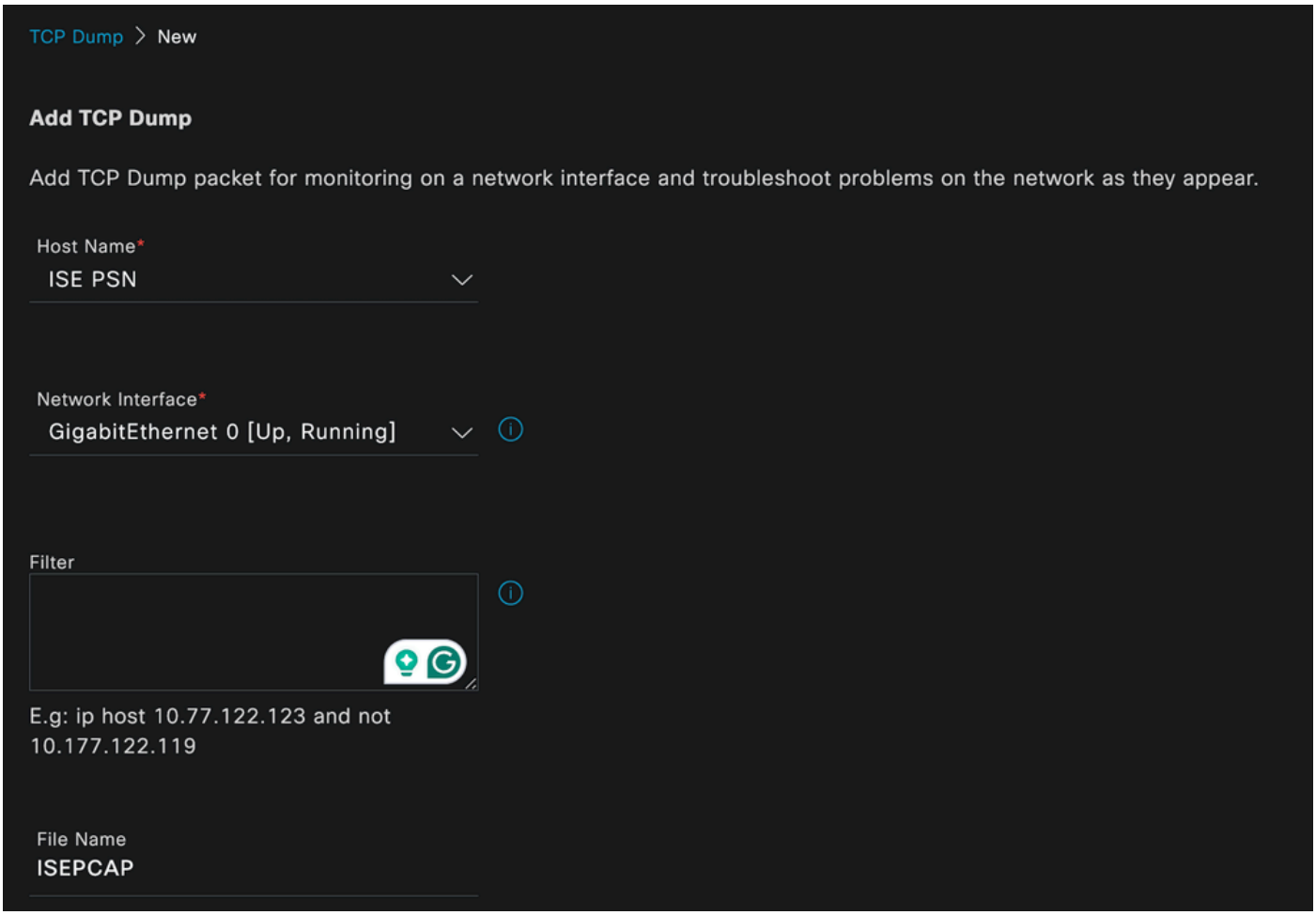
문제 해결 시 패킷 캡처 분석이 필수적입니다. ISE 패킷 캡처에서 직접 모든 노드 및 노드의 인터페이스에서 가져올 수 있습니다.

이 도구에 액세스하려면 Operations(운영) > Diagnostic Tools(진단 도구) > General Tools(일반 도구) > TCP Dump(TCP 덤프)로 이동합니다.

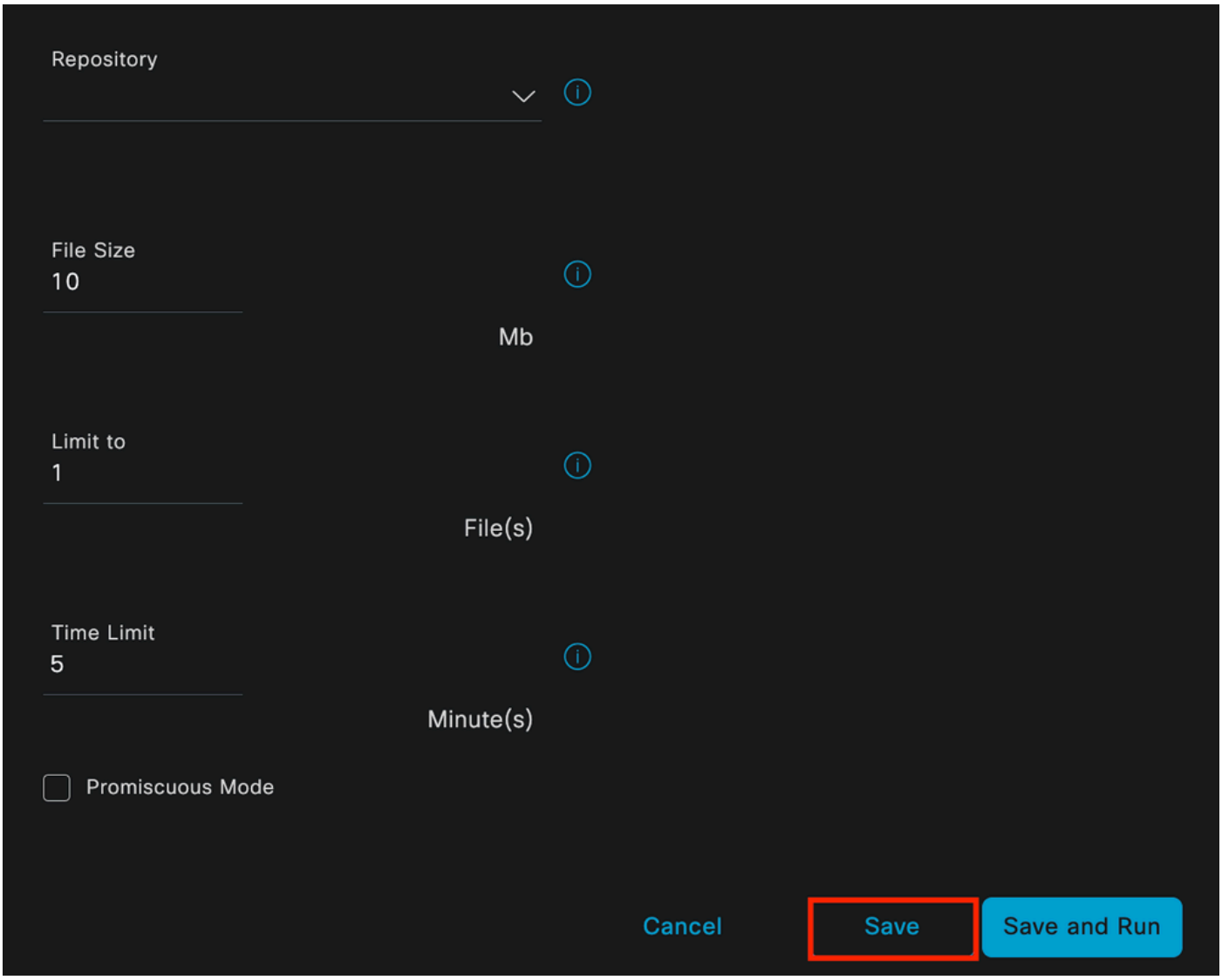


TCP 덤프 섹션

Add(추가) 버튼을 클릭하여 pcap 구성을 시작합니다.


TCP Dump > New
Add TCP Dump
Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.
Host Name*
ISE PSN
Network Interface*
GigabitEthernet 0 [Up, Running]
Filter
E.g: ip host 10.77.122.123 and not 10.177.122.119
File Name
ISEPCAP

TCP 덤프 생성

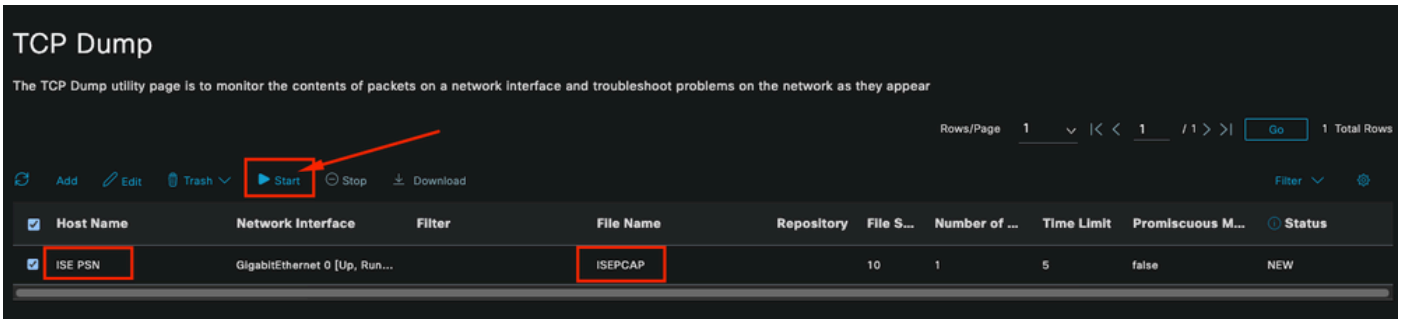


TCP 덤프 섹션

ISE에서 pcap를 생성하려면 다음을 입력해야 하는 데이터입니다.

- pcap를 가져와야 하는 노드를 선택합니다.
- pcap에 사용되는 ISE 노드 인터페이스를 선택합니다.
- 특정 트래픽을 캡처해야 하는 경우 필터를 사용하면 ISE에서 몇 가지 예를 제공합니다.
- pcap의 이름을 지정합니다. 이 시나리오에서는 ISEPCAP를 사용했습니다.
- 리포지토리를 선택하면, 선택된 리포지토리가 없으면 캡처는 ISE 로컬 디스크에 저장되며 GUI에서 다운로드할 수 있습니다.
- 또한 필요한 경우 pcap 파일 크기를 수정합니다.
- 필요한 경우 둘 이상의 파일을 사용합니다. 따라서 pcap가 파일 크기를 초과하면 나중에 새 파일이 생성됩니다.
- 필요한 경우 pcap에 대한 트래픽 캡처 시간을 연장합니다.

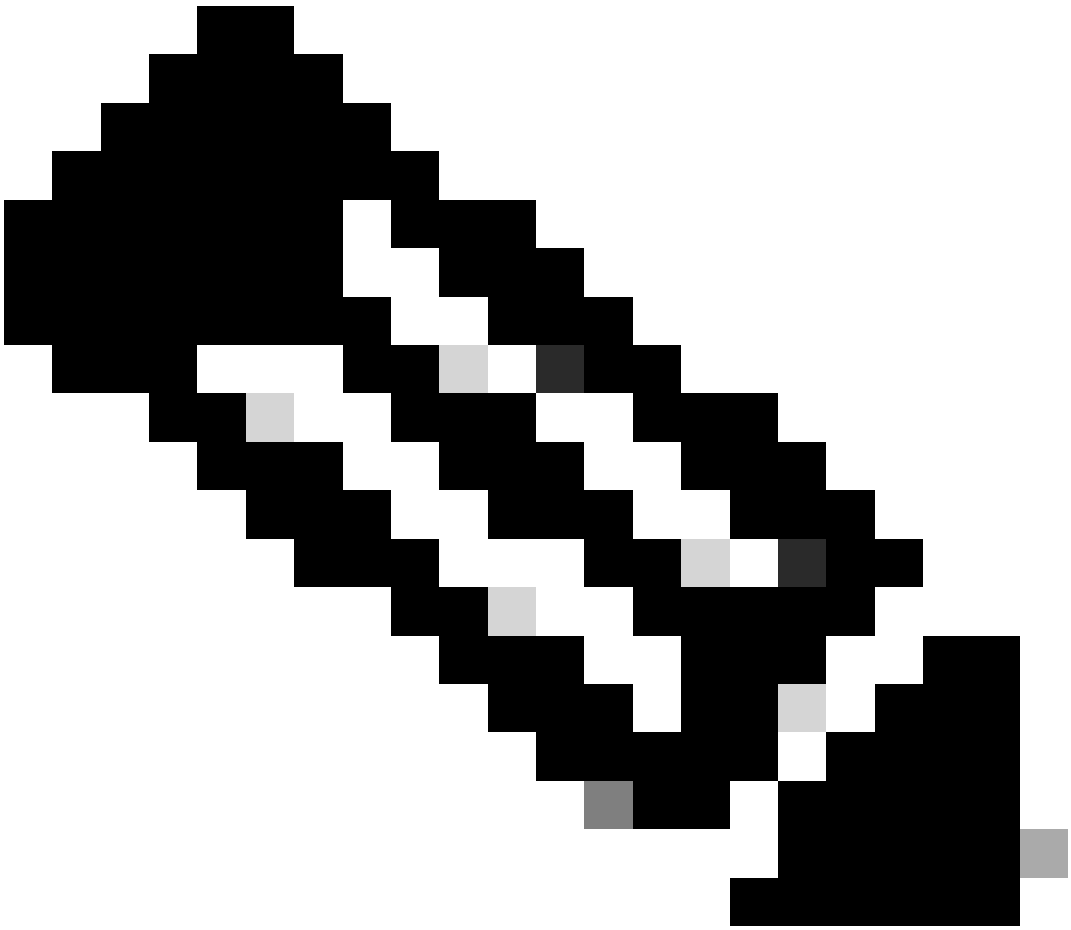
마지막으로 Save(저장) 버튼을 클릭합니다.



TCP 덤프 섹션

그런 다음 준비가 되면 pcap를 선택하고 Start(시작) 버튼을 클릭합니다.

Start(시작)를 클릭하면 Status(상태) 열이 RUNNING(실행 중) 상태로 변경됩니다.



참고: PCAP가 RUNNING 상태인 동안 실패한 시나리오 또는 캡처해야 하는 동작을 복제합니다. 완료되면 RADIUS, 대화의 세부 정보가 PCAP에 표시됩니다.

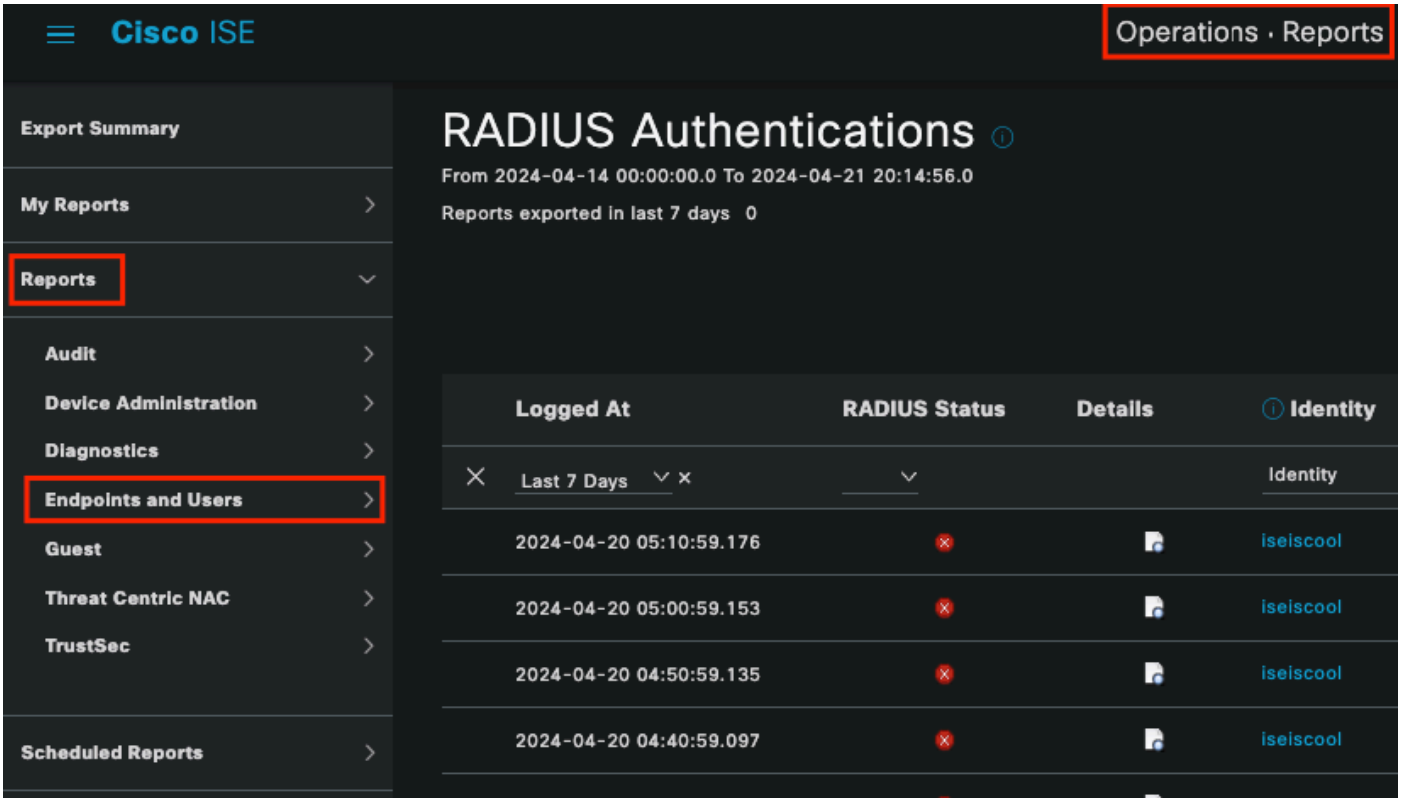
PCAP가 실행되는 동안 필요한 데이터가 캡처되면 pcap 수집을 완료합니다. 다시 선택하고 중지를

클릭합니다.

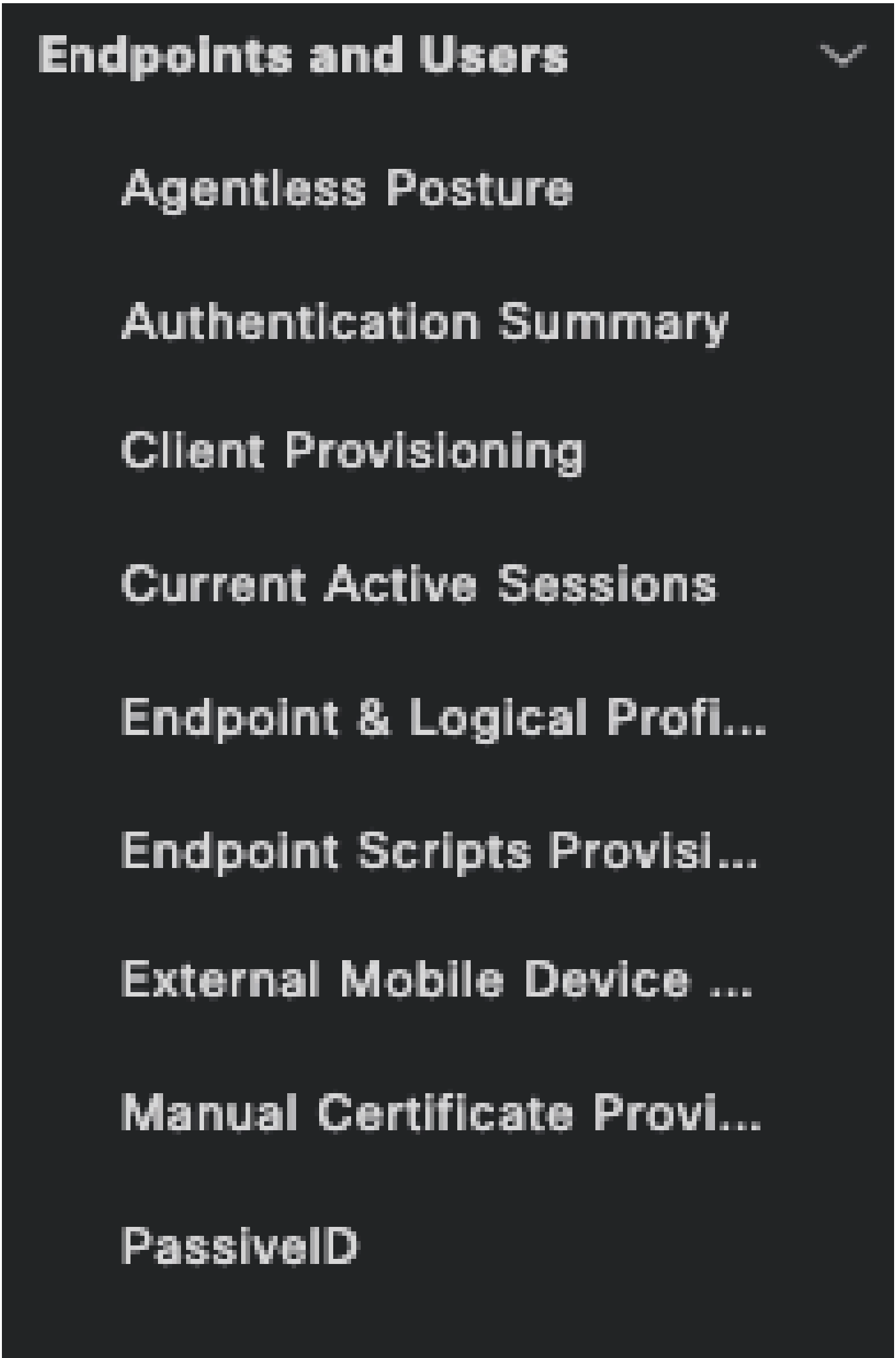
3 - 1 ISE 보고서

심층적인 분석이 필요한 경우 ISE는 과거 이벤트를 조사할 수 있는 유용한 보고서를 제공합니다.

이를 찾으려면 Operations(운영) > Reports(보고서) > Reports(보고서) > Endpoints and Users(엔드포인트 및 사용자)로 이동합니다

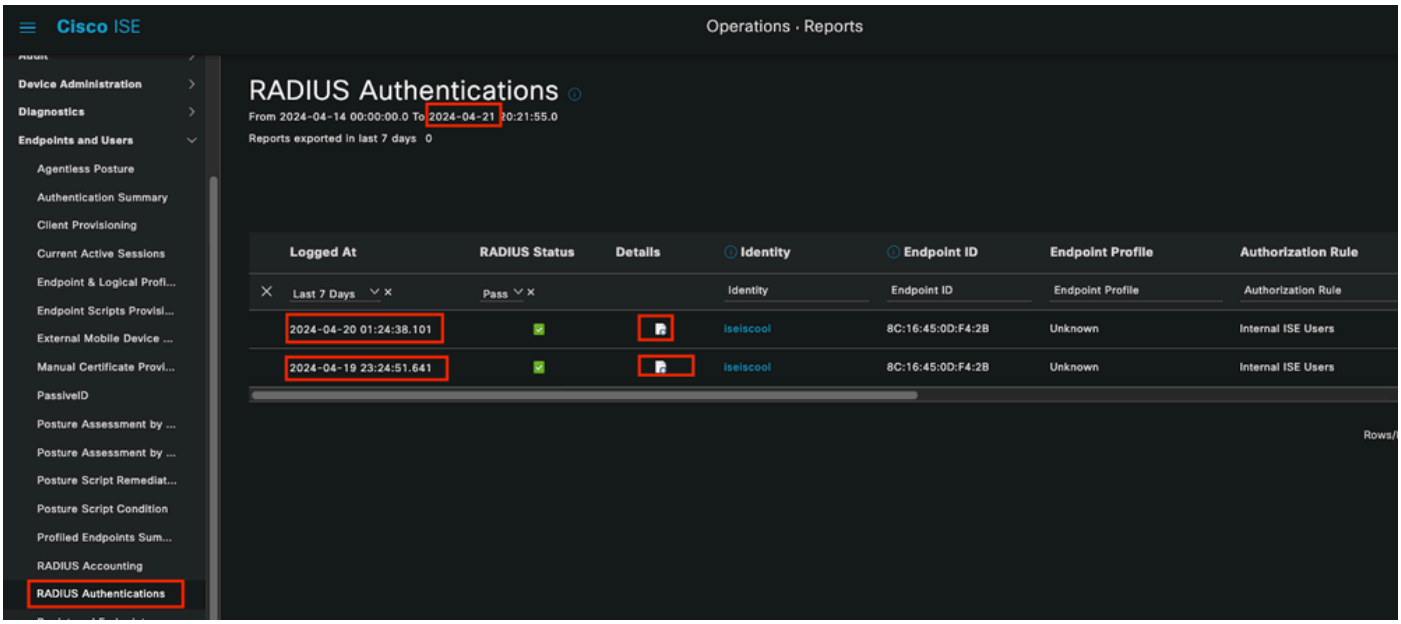


ISE 보고서 섹션


Endpoints and Users
Agentless Posture
Authentication Summary
Client Provisioning
Current Active Sessions
Endpoint & Logical Profi...
Endpoint Scripts Provisi...
External Mobile Device ...
Manual Certificate Provi...
PassiveID

라이브 로그) 섹션에서 최대 24시간의 과거 데이터를 선택할 수 있습니다. 때때로 이전 인증이 필요합니다. 과거에 정상적으로 작동하던 인증이 갑자기 실패하기 시작하면, 실제 작동하지 않는 인증과 이전에 작동하던 인증을 비교해야 합니다. Radius Authentication Report(RADIUS 인증 보고서)를 사용하여 이를 수행할 수 있습니다.

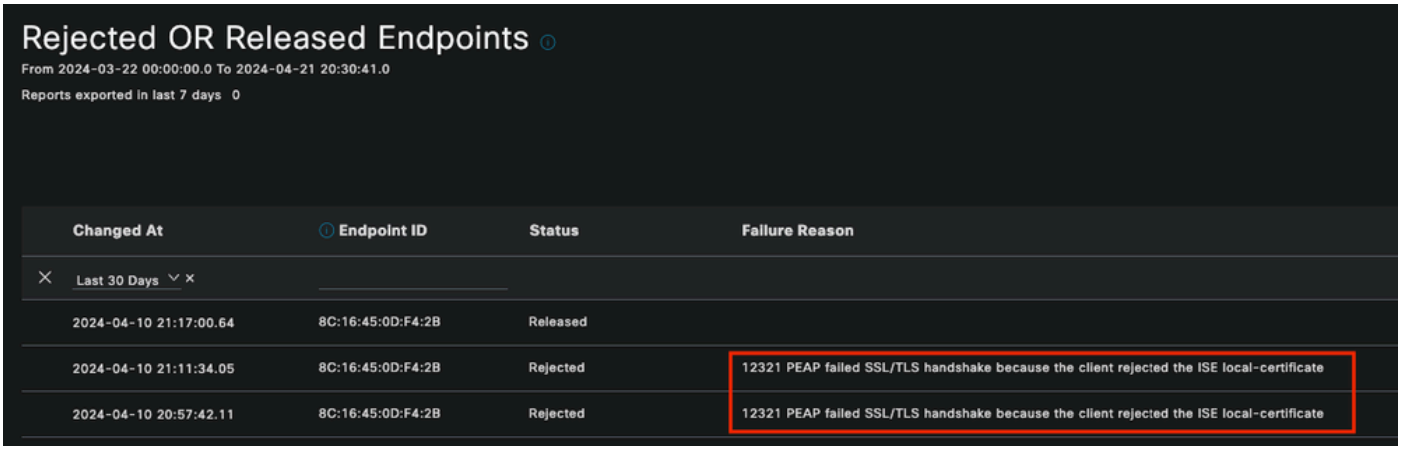
이 보고서에서는 최대 이전 30일의 시간 범위를 선택할 수 있습니다. 또한 각 인증에 대한 라이브 로그 세부사항 보고서를 유지합니다.



인증 보고서

3-3 거부되거나 릴리스된 엔드포인트

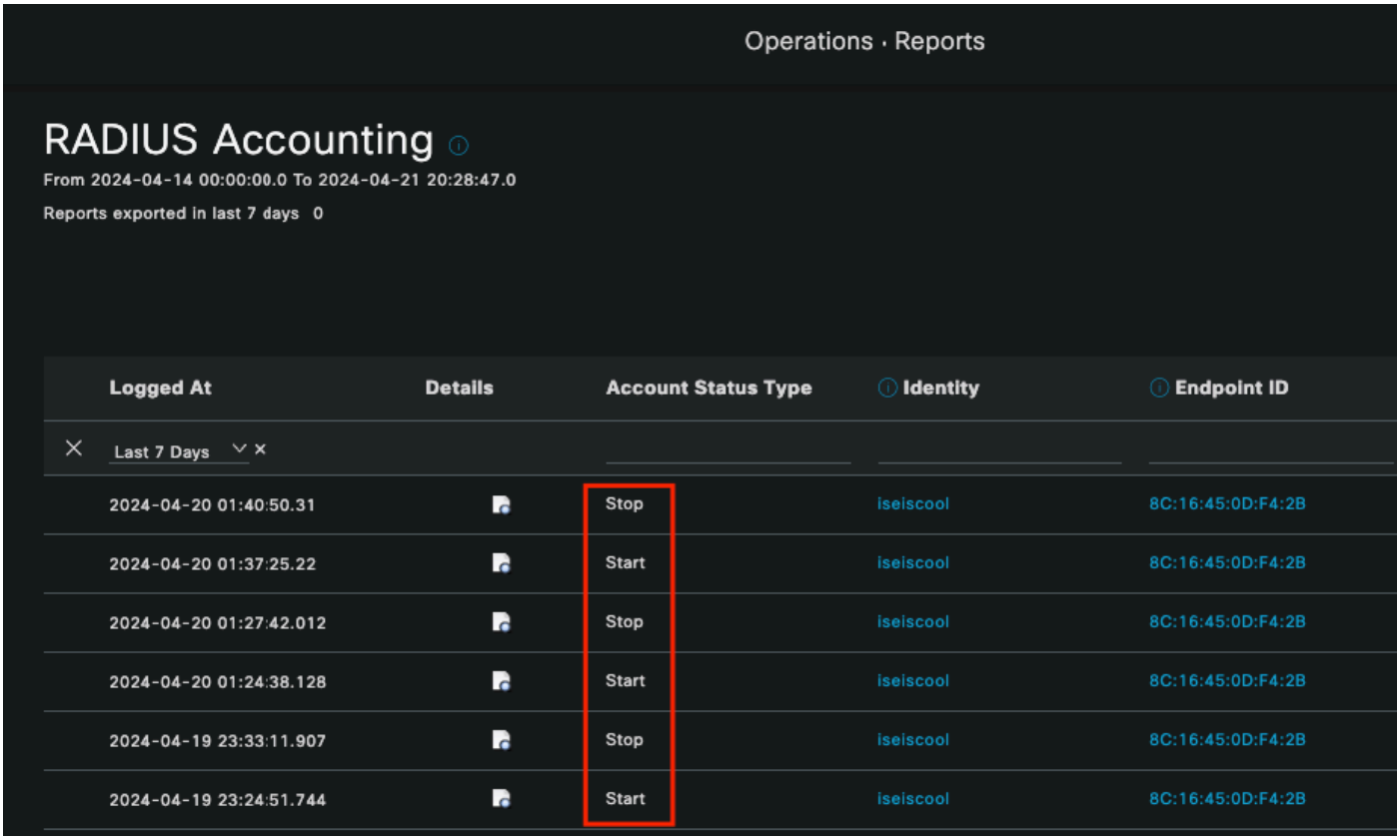
거부된 엔드포인트에 대한 실패 사유가 무엇인지 확인합니다. Rejected OR Released Endpoints(거부 또는 릴리스된 엔드포인트) 보고서를 확인할 수 있습니다. ISE 구축의 모든 PSN 노드에서 EAP 인증서가 업데이트된 다음 PEAP 인증이 전체 영역에서 실패하기 시작하는 시나리오에서 이 보고서를 확인할 수 있으며 라이브 로그 세부사항을 확인하지 않으면 클라이언트가 ISE 인증서를 거부하고 신뢰하지 않는다는 것을 알 수 있습니다.



거부된 엔드포인트 보고서

3-4 RADIUS 계정 관리 보고서

이는 과도한 라이센스 소비 문제가 발생하는 경우 자주 사용됩니다. 이러한 시나리오에서 ISE는 세션 완료 여부를 확인할 수 없기 때문에 라이센스를 릴리스하지 않습니다. ISE는 네트워크 디바이스가 보내는 어카운팅 패킷을 사용하여 이를 결정합니다. 어카운팅이 네트워크 디바이스에서 ISE로 올바르게 공유될 때 표시되는 방식은 다음과 같습니다.



RADIUS 계정 관리 보고서

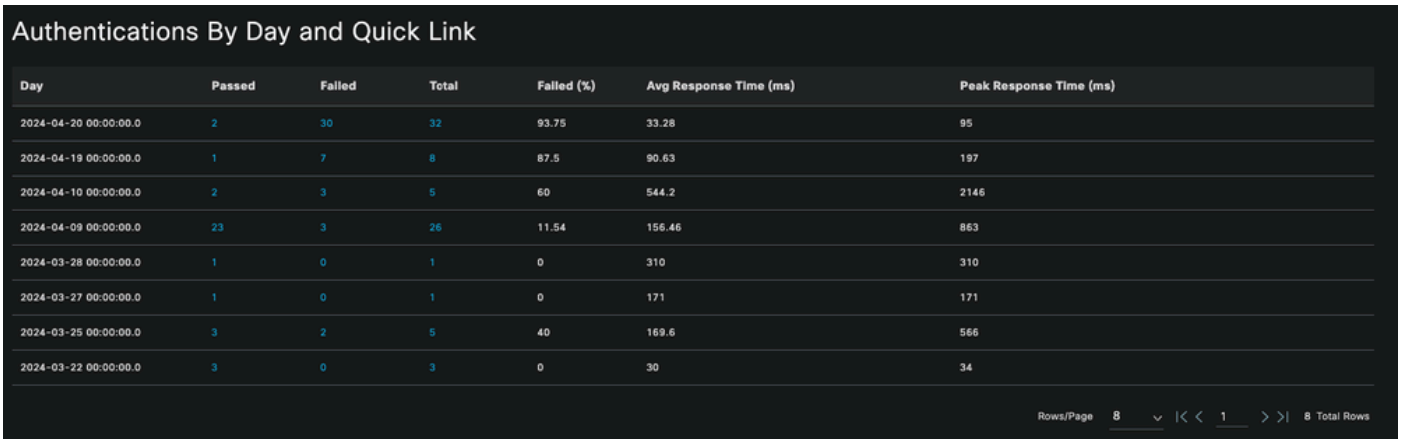
3-5 인증 요약 보고서

이는 ISE에서 제공하는 자주 사용되는 유용한 보고서입니다. 최대 30일의 이전 데이터를 선택할 수 있습니다. 이 보고서에서 다음과 같은 정보를 볼 수 있습니다.

- 일별 통과 및 실패 인증의 백분율입니다.

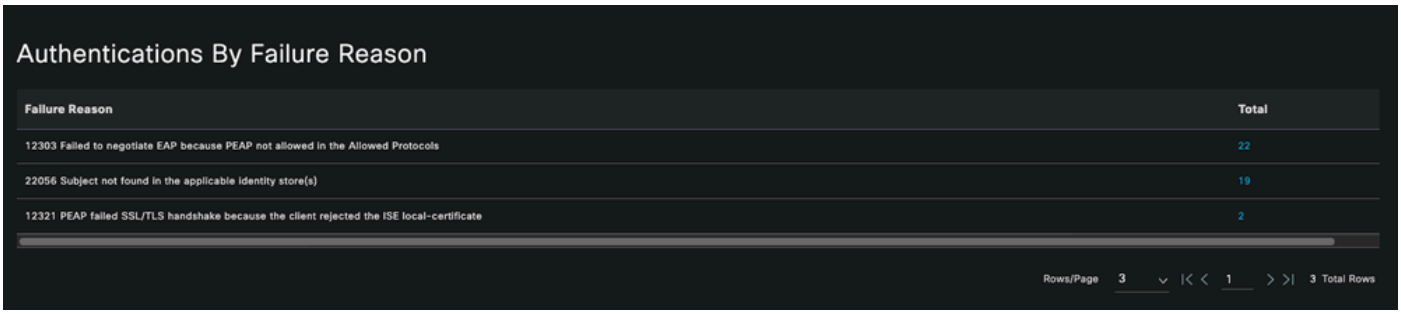
차트: 일별 전달 인증

- 데이터를 자세히 보기 위해 파란색 값을 클릭하는 옵션과 함께 차트의 하루 인증 횟수입니다.



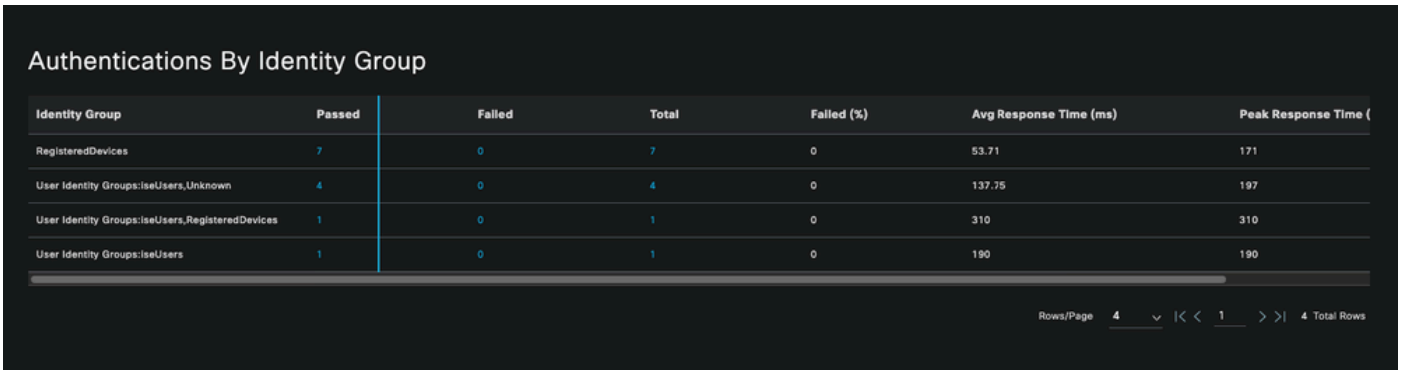
일별 인증 및 빠른 링크

- 실패 사유에 의한 인증 - 맨 위 목록에 나열되고, 가장 많이 반복된 항목부터 덜 반복된 항목까지 모두 포함합니다.



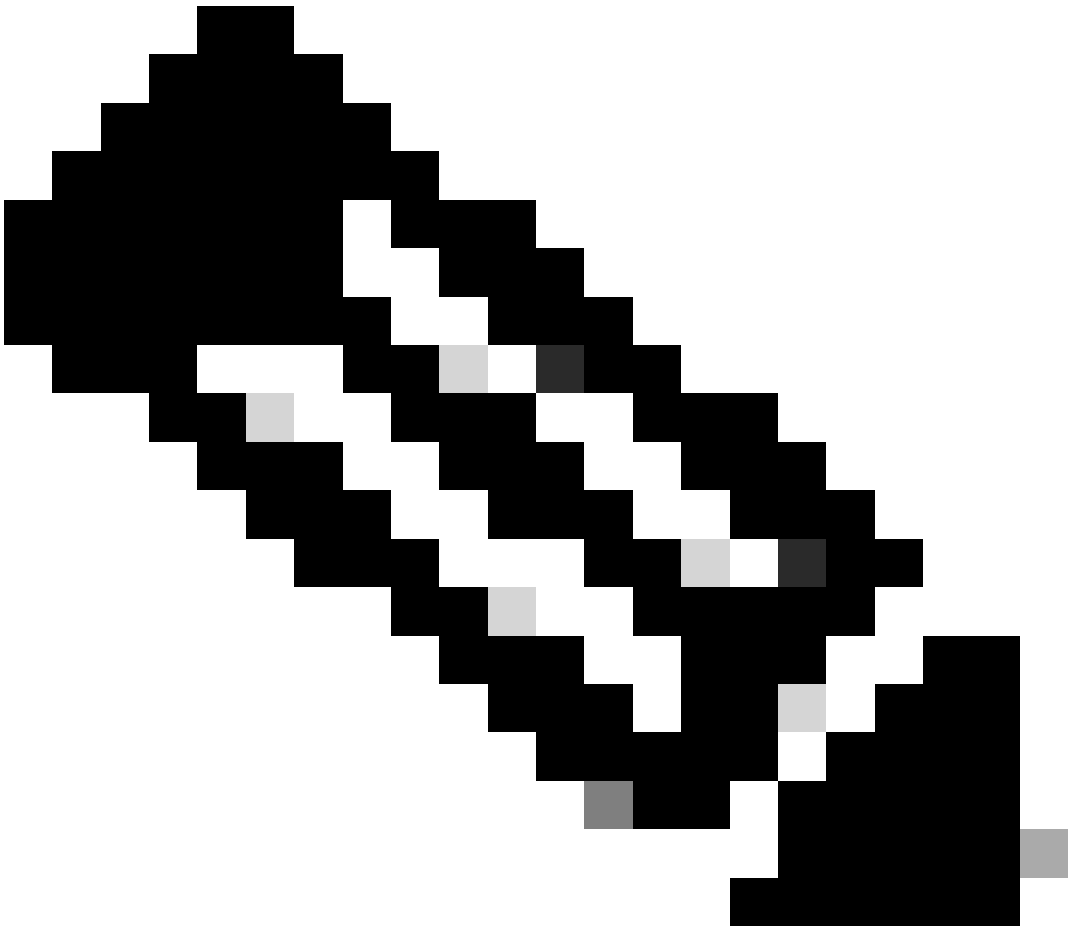
실패 사유별 인증

- 구축 인증에 일반적으로 사용 되는 ID 그룹을 확인 하는 옵션.

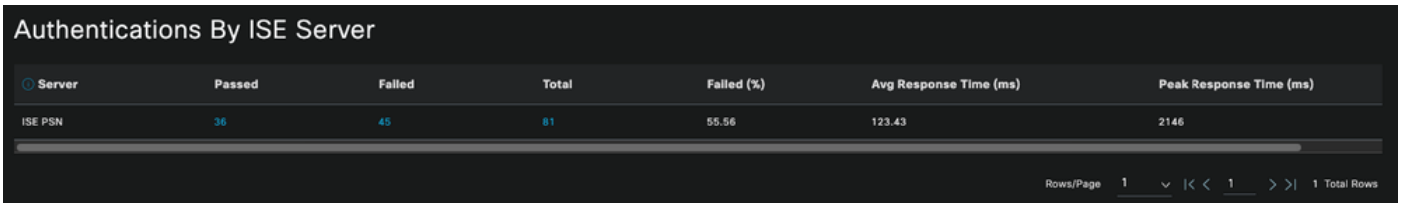


ID 그룹별 인증

- 어떤 PSN이 더 많은 인증을 받는지 확인합니다.



참고: 이 문서에 사용된 배포에서는 PSN이 하나만 사용되었지만 대규모 배포의 경우 이 데이터는 로드 밸런싱이 필요한지 여부를 확인하는 데 유용합니다.



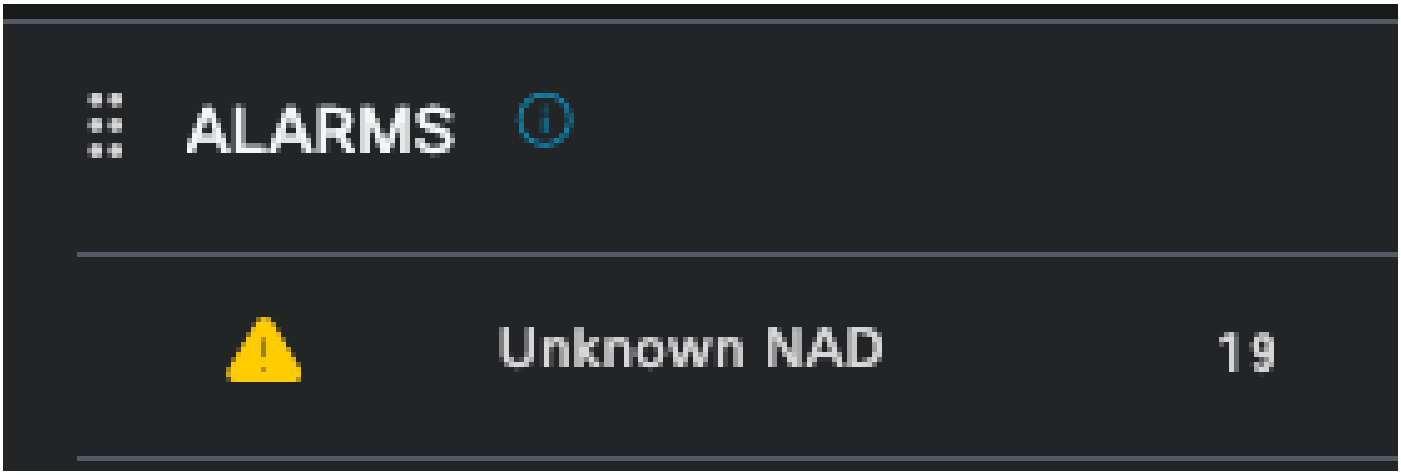
ISE 서버별 인증

4 - ISE 경보

ISE Dashboard(ISE 대시보드)에서 Alarms(경보) 섹션에 구축 문제가 표시됩니다.

다음은 트러블슈팅에 도움이 되는 몇 가지 ISE 알람입니다.

알 수 없는 NAD — 이 경보는 엔드 포인트를 인증 하고 ISE에 도달 하는 네트워크 장치가 있을 때 표시 됩니다. 그러나 ISE는 이를 신뢰하지 않으며 RADIUS 연결을 끊습니다. 가장 일반적인 이유는 네트워크 디바이스가 생성되지 않았거나 네트워크 디바이스가 사용 중인 IP가 ISE가 등록한 것과 동일하지 않기 때문입니다.

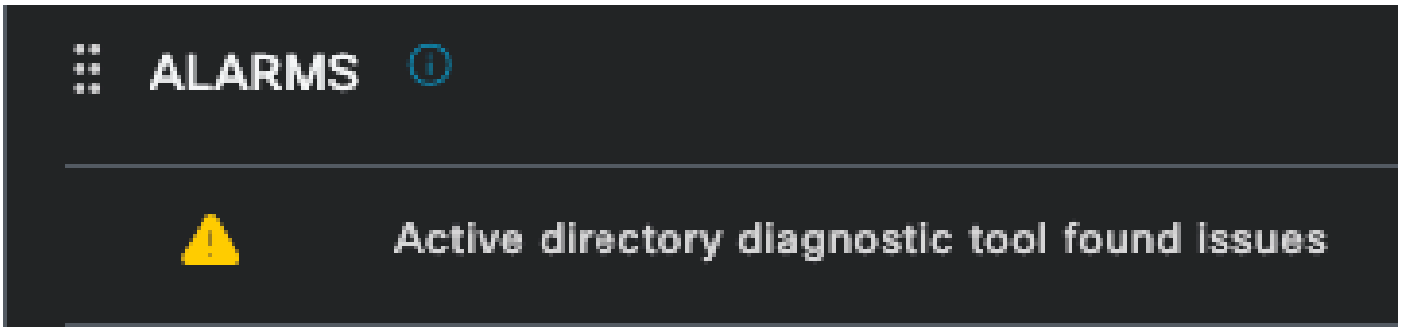


알 수 없는 NAD

서 플리 컨 트가 응답을 중지 한 서 플리 컨 트 통신에 문제가 있을 때 이 경보는 엔드 포인트 측에서 확인 하고 조사 해야 하는 서 플리 컨 트의 잘못된 구성 때문에 발생 합니다.

서 플리 컨 트가 응답을 중지

Active Directory 진단 도구에서 문제 발견 — Active Directory를 사용하여 사용자 ID를 검증하는 경우, 통신 프로세스에 문제가 발생하기 시작하거나 연결이 끊어지면 이 경보가 표시됩니다. 그러면 ID가 AD에 존재하는 인증이 실패하는 이유를 알 수 있습니다.



AD 진단 실패

COA(Change of Authorization) 실패 - ISE의 여러 플로우에서 CoA를 사용합니다. 이 알람은 CoA 포트 통신 중에 네트워크 디바이스에 문제가 발생한 경우 알려줍니다.

Coa 실패

5 - ISE 디버그 컨피그레이션 및 로그 수집

인증 프로세스 세부 정보를 계속하려면 mab 및 dot1x 문제에 대해 DEBUG에서 다음 구성 요소를 활성화해야 합니다.

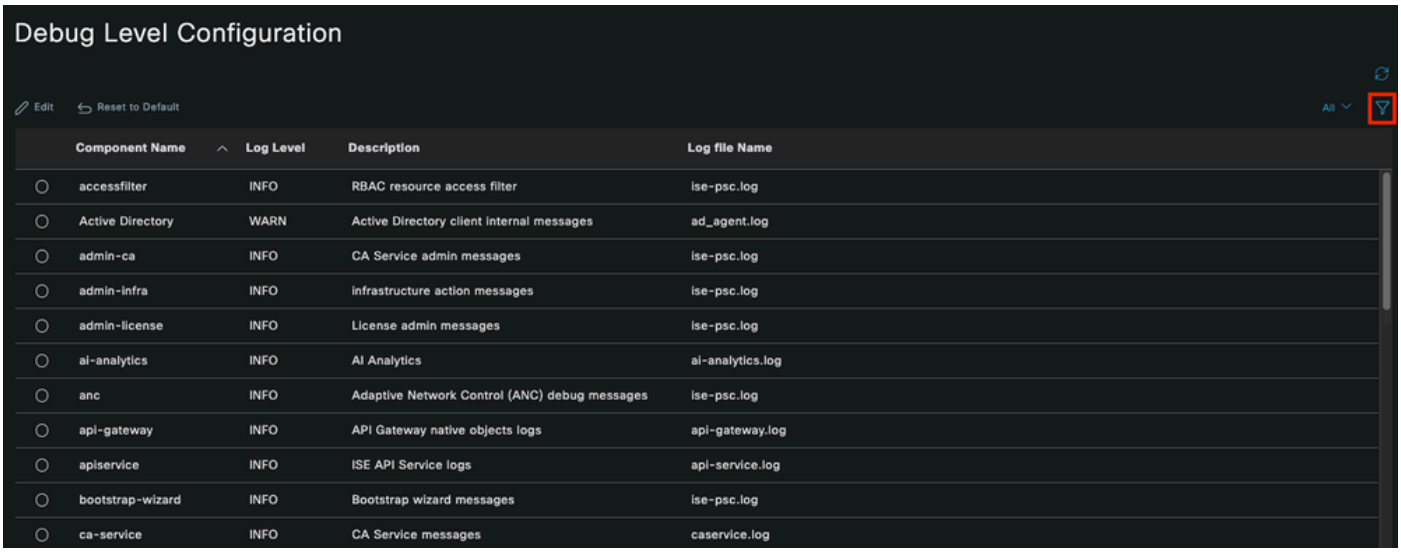
문제: dot1x/mab

디버그 수준으로 설정할 특성.

- 런타임 AAA(prrt-server.log)
- nsf(ise-psc.log)
- nsf-session(ise-psc.log)

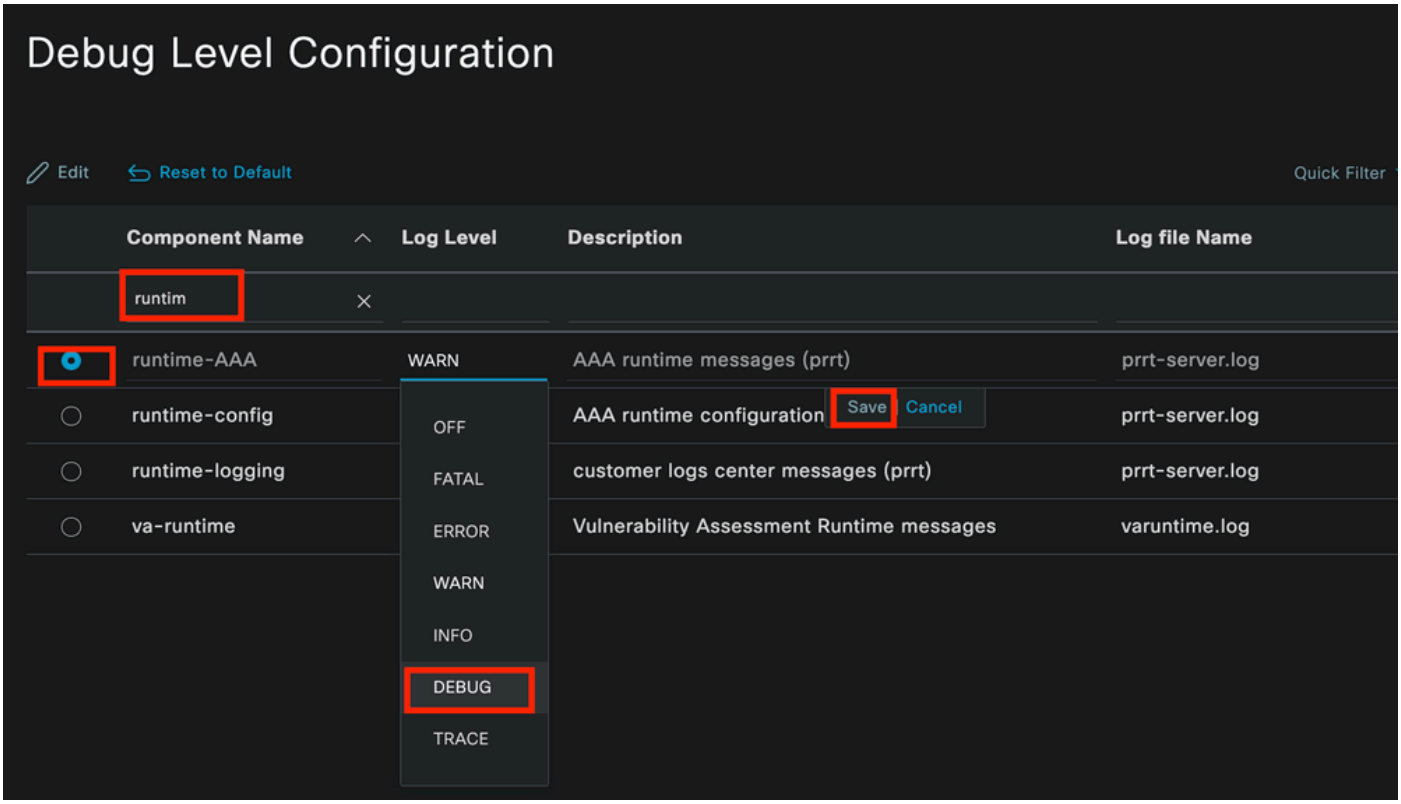
구성 요소를 DEBUG 수준으로 설정하려면 먼저 실패 중이거나 조사해야 하는 인증을 받는 PSN을 식별해야 합니다. 라이브 로그에서 이 정보를 가져올 수 있습니다. 그런 다음 ISE 메뉴 > 문제 해결 > 디버그 마법사 > 디버그 로그 구성 > PSN을 선택하고 > 편집 버튼을 클릭해야 합니다.

다음 메뉴가 표시됩니다. 필터 아이콘을 클릭합니다.



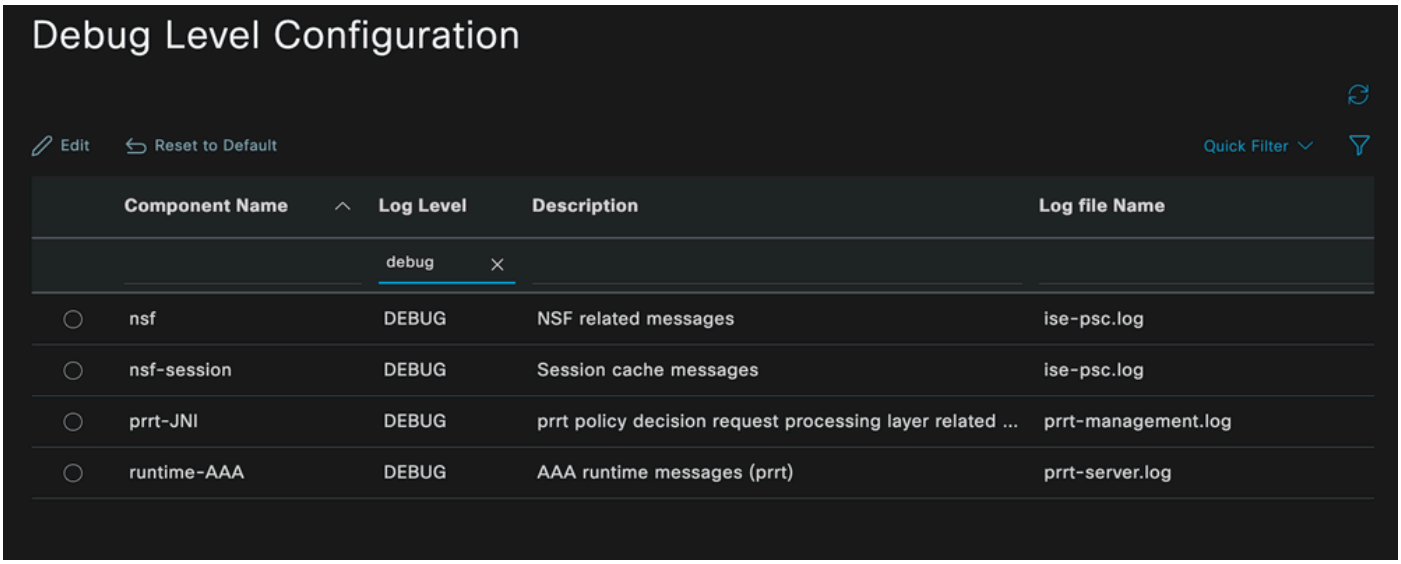
디버그 로그 컨피그레이션

구성 요소 이름 열에서 이전에 나열된 속성을 검색합니다. 각 로그 레벨을 선택하고 DEBUG로 변경합니다. 변경 사항을 저장합니다.



런타임 AAA 구성 요소 설정

각 구성 요소의 구성을 마쳤으면 모든 구성 요소가 올바르게 구성되었는지 확인할 수 있도록 DEBUG로 필터링합니다.

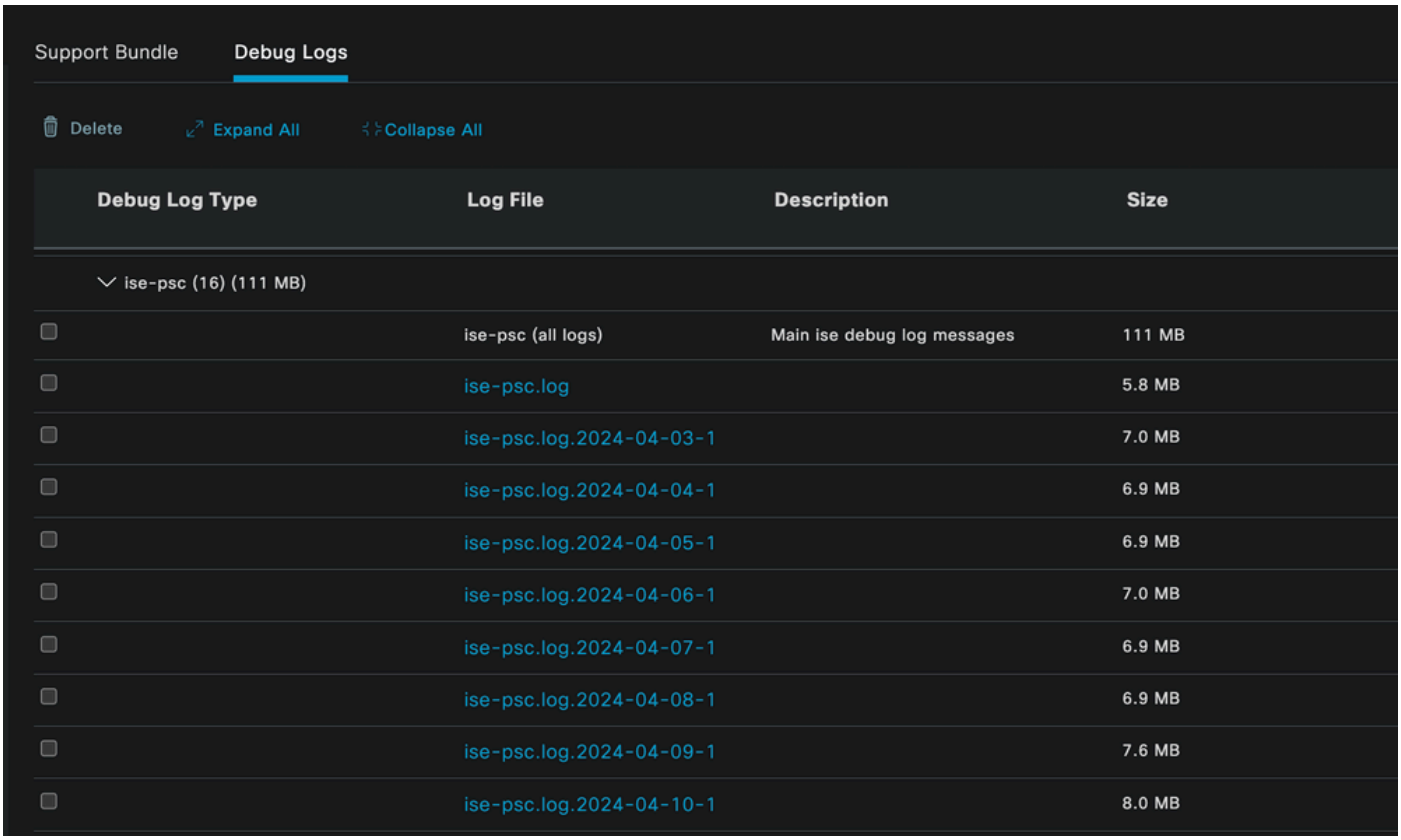


디버그 로그 컨피그레이션

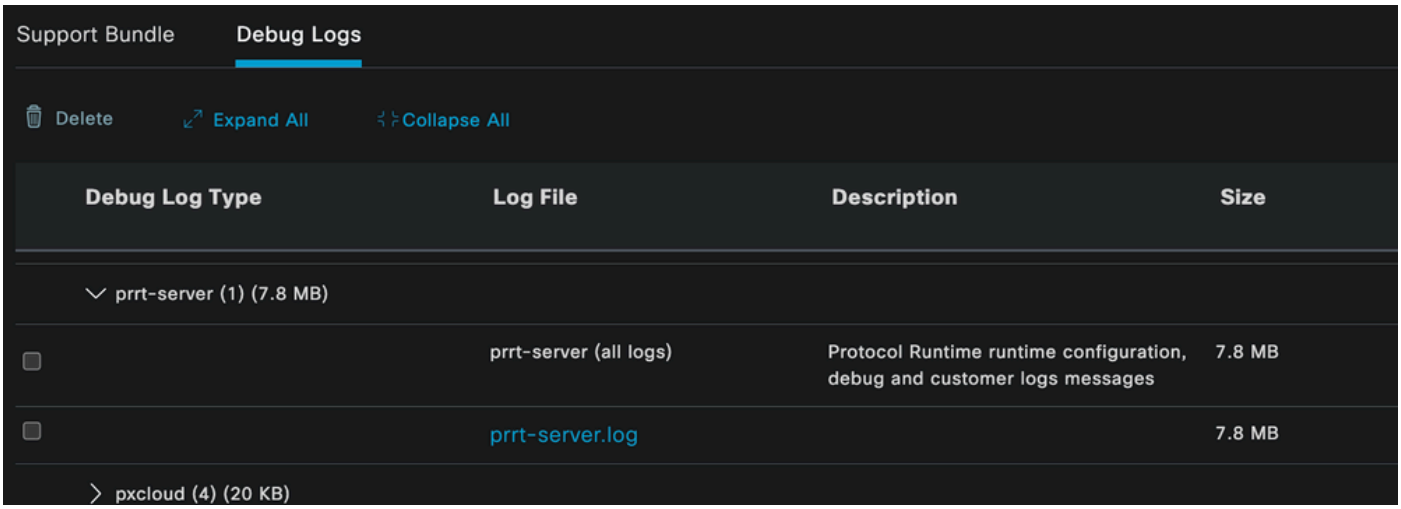
로그를 즉시 분석해야 하는 경우 ISE 메뉴 > 작업 > 문제 해결 > 로그 다운로드 > 어플라이언스 노드 목록 > PSN으로 이동하여 로그를 다운로드하고 DEBUGS > 디버그 로그를 활성화할 수 있습니다.

이 경우 port-server.log 및 ise-psc.log에서 dot1x 및 mab 문제를 다운로드해야 합니다. 다운로드해야 하는 로그는 마지막 테스트 날짜가 포함된 로그입니다.

이 이미지에 표시된 로그 파일을 클릭하고 다운로드합니다(파란색 텍스트로 표시됨).



PSN 노드의 디버그 로그

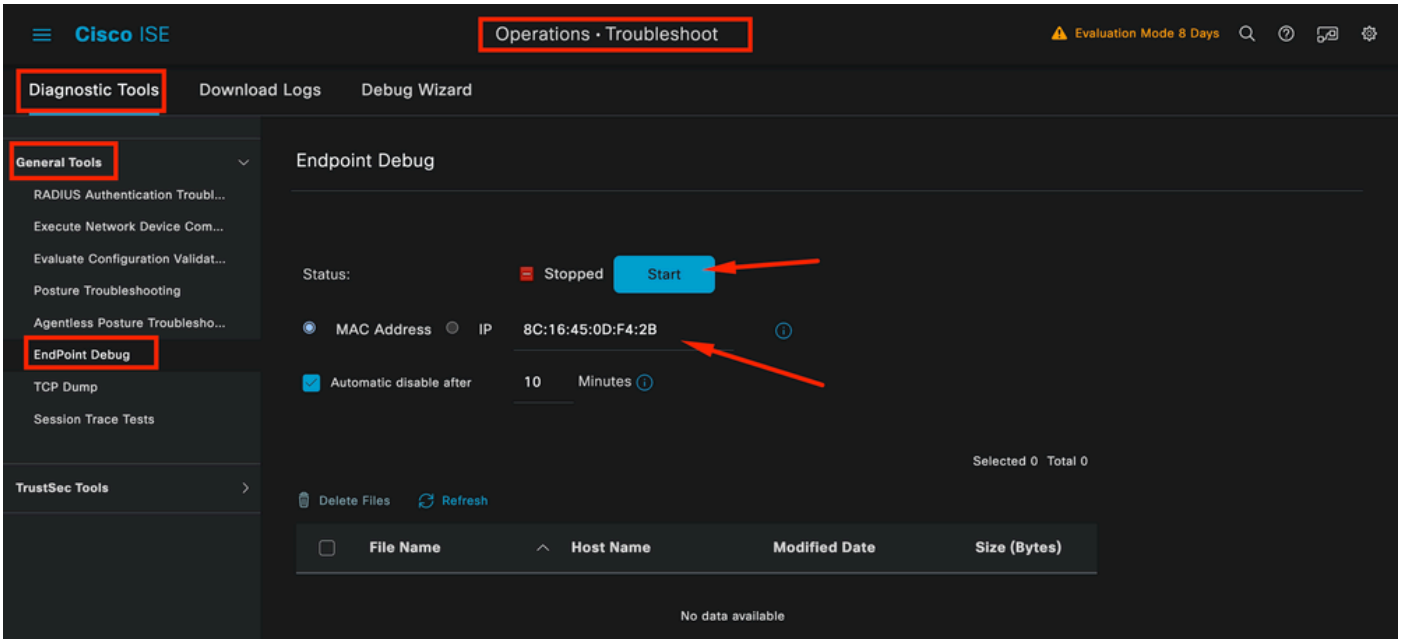


디버그 로그 섹션

6 - 엔드포인트당 ISE 디버그

또한 mac 주소 또는 IP에 따라 엔드포인트 디버그 로그별로 디버그 로그를 가져오는 다른 옵션도 있습니다. 엔드포인트 디버그 ISE 툴을 사용할 수 있습니다.

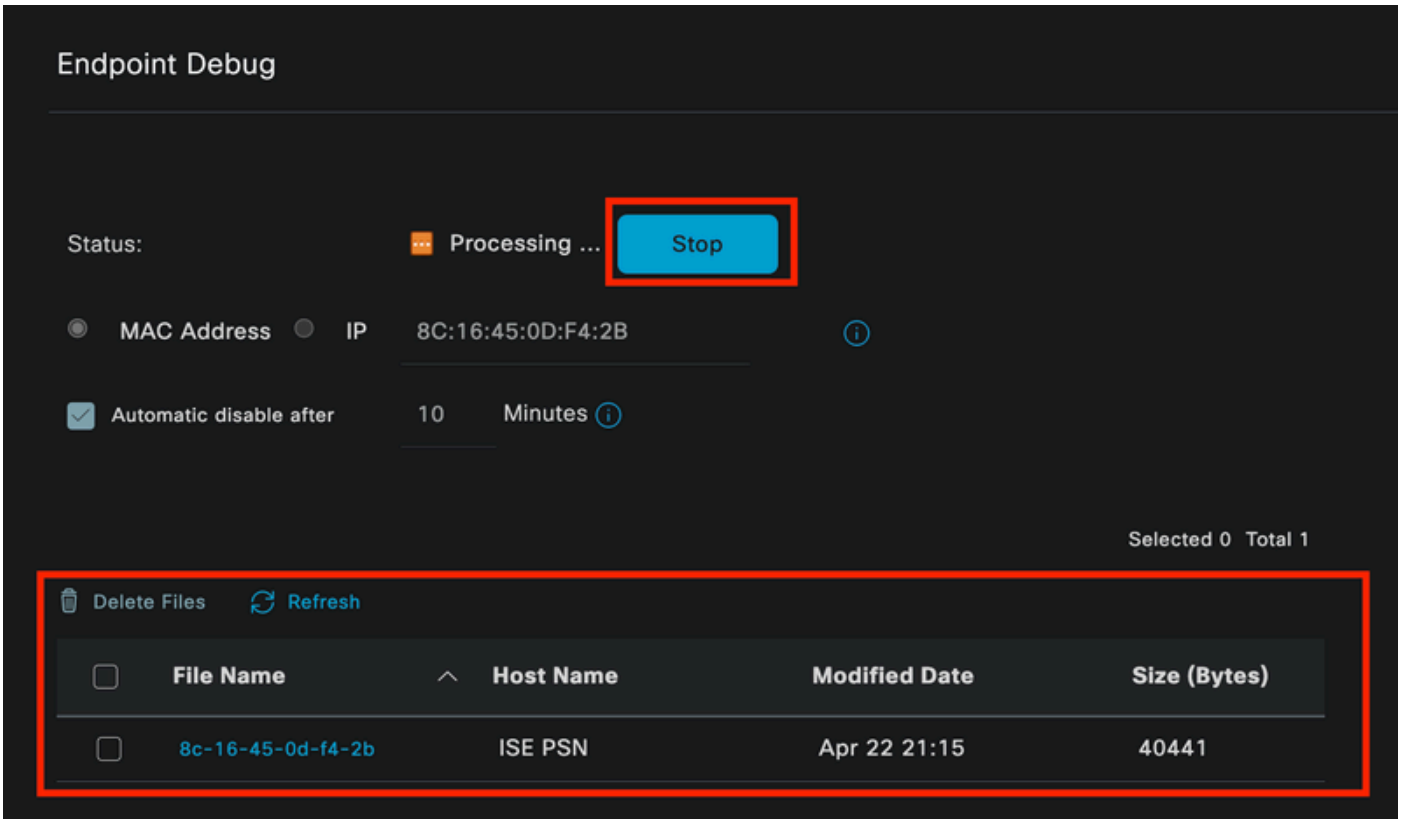
ISE Menu(ISE 메뉴) > Operations(운영) > Troubleshoot(문제 해결) > Diagnostic Tools(진단 도구) > General Tools(일반 도구) > Endpoint Debug(엔드포인트 디버그)로 이동합니다.



엔드포인트 디버그

그런 다음 원하는 엔드포인트 정보를 입력하여 로그 캡처를 시작합니다. 시작을 클릭합니다.

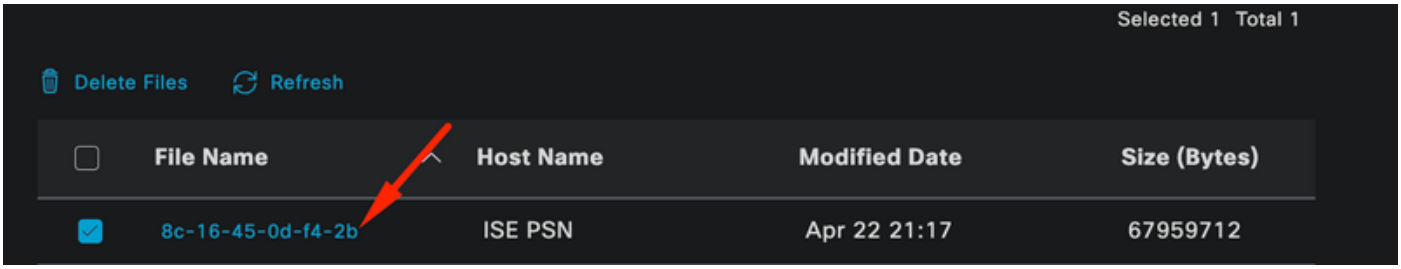
그런 다음 경고 메시지에서 Continue(계속)를 클릭합니다.



엔드포인트 디버그

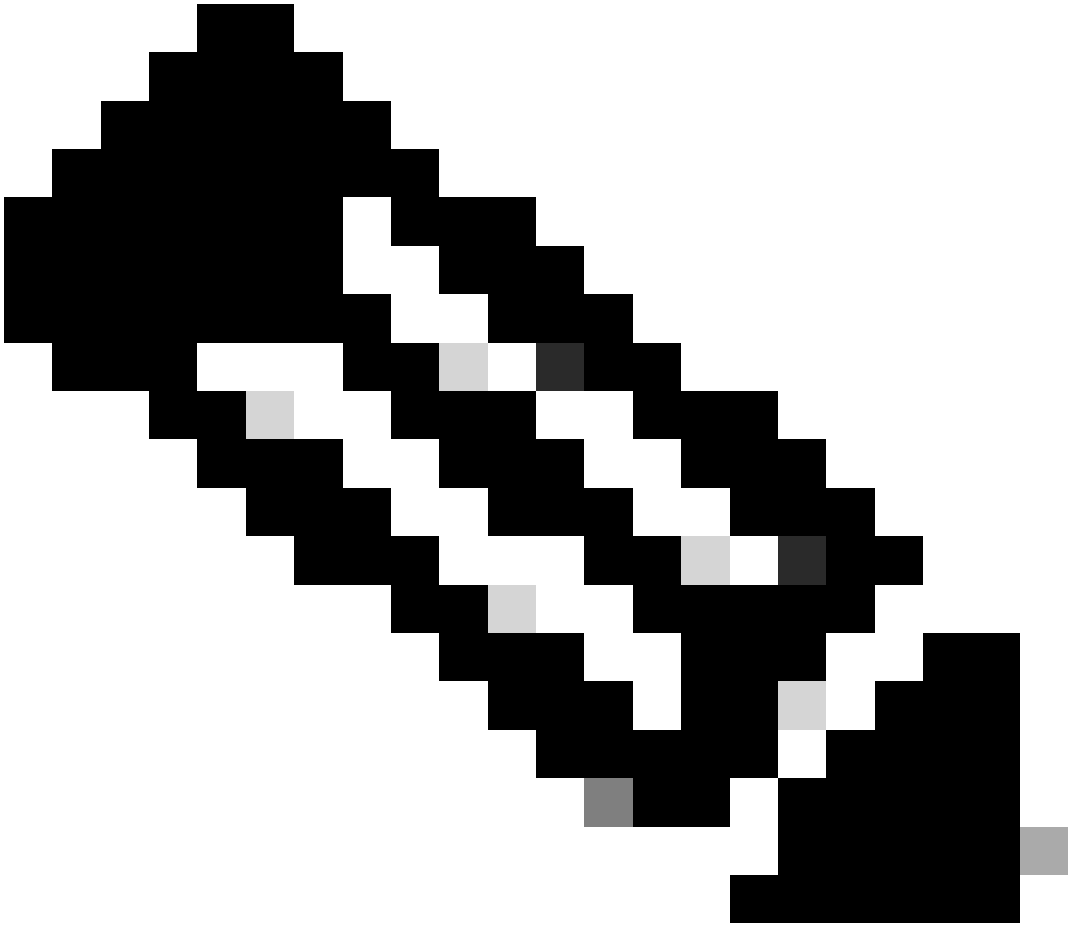
정보가 캡처되면 중지를 클릭합니다.

이 이미지에서 파란색으로 표시된 파일 이름을 클릭합니다.



엔드포인트 디버그

디버그 로그 컨피그레이션에서 직접 활성화하지 않고 DEBUG 로그로 인증 로그를 볼 수 있어야 합니다.

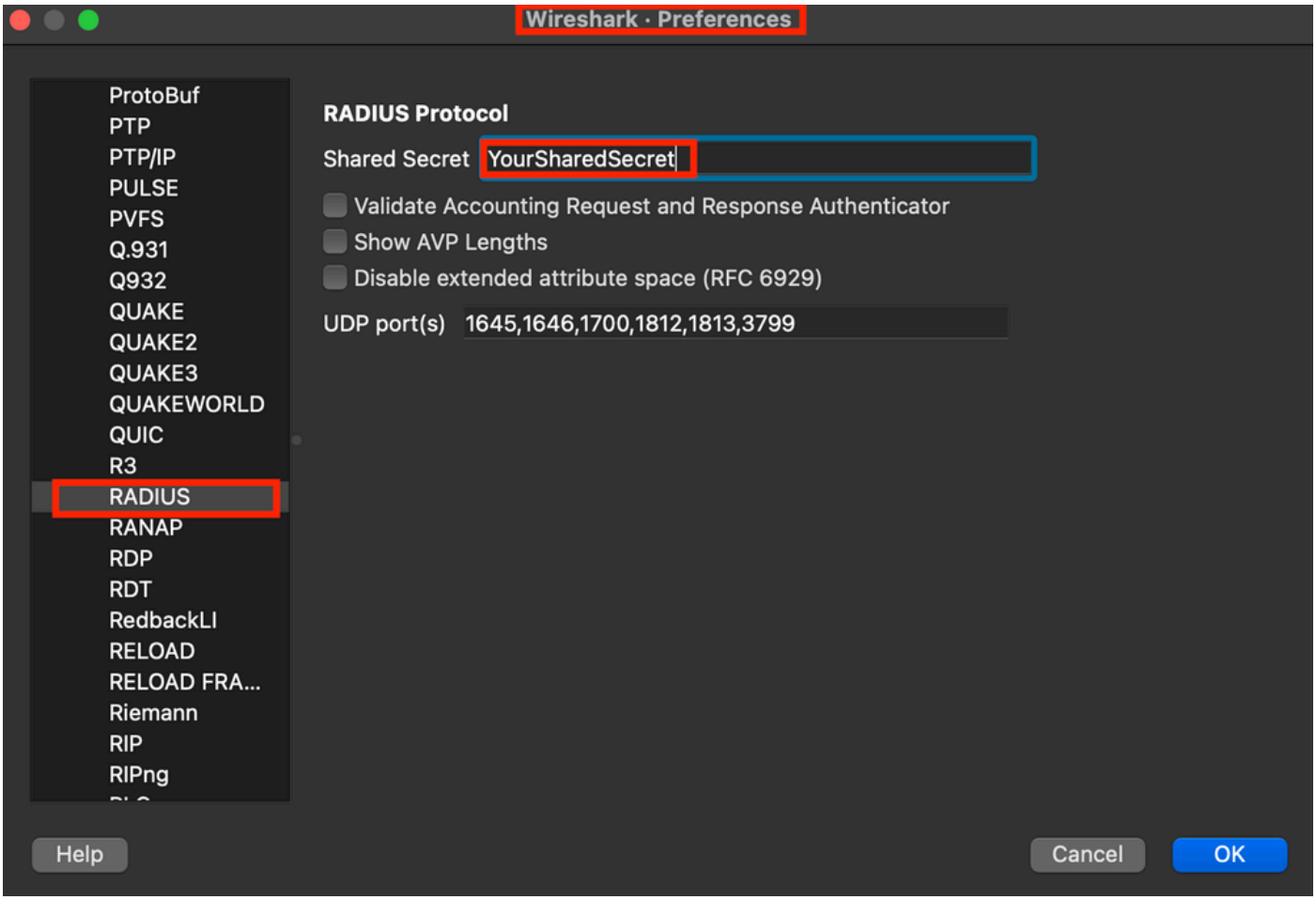


참고: 엔드포인트 디버그 출력에서 일부 항목이 생략될 수 있으므로, 디버그 로그 컨피그레이션으로 이를 생성하고 필요한 모든 파일에서 필요한 모든 로그를 다운로드하는 더욱 완벽한 로그 파일을 얻을 수 있습니다. 이전 ISE 디버그 컨피그레이션 및 로그 수집 섹션에서 설명한 대로.

---

7 - RADIUS 패킷 암호 해독

Radius 패킷은 사용자 암호 필드를 제외하고 암호화되지 않습니다. 그러나 전송된 비밀번호를 확인해야 합니다. Wireshark > Preferences > Protocols > RADIUS로 이동한 다음 ISE 및 네트워크 디바이스에서 사용하는 RADIUS 공유 키를 추가하여 사용자가 보낸 패킷을 볼 수 있습니다. 그런 다음 RADIUS 패킷이 암호 해독된 상태로 표시됩니다.



Wireshark Radius 옵션

8 - 네트워크 디바이스 트러블슈팅 명령

다음 명령은 ISR 1100 또는 유선 NAD 장치에서 문제를 해결할 때 유용합니다.

8 - 1 AAA 서버 또는 ISE가 사용 가능하고 네트워크 디바이스에서 연결 가능한지 확인하려면 show aaa servers를 사용합니다.

```
Router>show aaa servers

RADIUS: id 1, priority 1, host 10.88.240.80, auth-port 1645, acct-port 1646, hostname
     State: current UP, duration 2876s, previous duration 0s
     Dead: total time 0s, count 0

     Platform State from SMD: current UP, duration 2876s, previous duration 0s
     SMD Platform Dead: total time 0s, count 0

     Platform State from WNCD (1) : current UP, duration 3015s, previous duration 0s
     Platform State from WNCD (2) : current UP, duration 3015s, previous duration 0s
     Platform State from WNCD (3) : current UP, duration 3015s, previous duration 0s
     Platform State from WNCD (4) : current UP, duration 3015s, previous duration 0s
     Platform State from WNCD (5) : current UP, duration 3015s, previous duration 0s
     Platform State from WNCD (6) : current UP, duration 3015s, previous duration 0s
     Platform State from WNCD (7) : current UP, duration 3015s, previous duration 0s
     Platform State from WNCD (8) : current UP, duration 3015s, previous duration 0s

     WNCD Platform Dead: total time 0s, count 0UP
```

```
Quarantined: No

Authen: request 11, timeouts 0, failover 0, retransmission 0

        Response: accept 1, reject 0, challenge 10
        Response: unexpected 0, server error 0, incorrect 0, time 33ms
        Transaction: success 11, failure 0
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
        Dot1x transactions:

        Response: total responses: 11, avg response time: 33ms
        Transaction: timeouts 0, failover 0
        Transaction: total 1, success 1, failure 0

        MAC auth transactions:
        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0

Author: request 0, timeouts 0, failover 0, retransmission 0
        Response: accept 0, reject 0, challenge 0
        Response: unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction: success 0, failure 0

        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
        MAC author transactions:

        Response: total responses: 0, avg response time: 0ms
        Transaction: timeouts 0, failover 0
        Transaction: total 0, success 0, failure 0

Account: request 6, timeouts 4, failover 0, retransmission 3
        Request: start 1, interim 0, stop 0
        Response: start 1, interim 0, stop 0

        Response: unexpected 0, server error 0, incorrect 0, time 27ms
        Transaction: success 2, failure 1
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0

Elapsed time since counters last cleared: 47m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0

Consecutive Response Failures: total 0
        SMD Platform : max 0, current 0 total 0
        WNCD Platform: max 0, current 0 total 0
        IOSD Platform : max 0, current 0 total 0

Consecutive Timeouts: total 3
        SMD Platform : max 0, current 0 total 0
        WNCD Platform: max 0, current 0 total 0
        IOSD Platform : max 3, current 0 total 3

Requests per minute past 24 hours:
        high - 0 hours, 47 minutes ago: 4
```

```
            low  - 0 hours, 45 minutes ago: 0
            average: 0

Router>
```

8-2 포트 상태, 세부 정보, 세션에 적용된 ACL, 인증 방법 및 자세한 정보를 보려면 명령 show authentication sessions interface <interface where the laptop attached> 세부 정보를 사용하십시오
.

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
Interface: GigabitEthernet0/1/0
IIF-ID: 0x01D9BEFB
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781F0A0000000C0777AECD
Acct Session ID: 0x00000003
Handle: 0x0a000002
Current Policy: POLICY_Gi0/1/0


Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure

Server Policies:


Method status list:
Method State
dot1x Authc Success

Router#
```

8-3 글로벌 컨피그레이션에서 aaa에 대한 모든 필수 명령이 있는지 확인하려면 show running-config aaa를 실행합니다.

```
Router#sh run aaa
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
client <A.B.C.D> server-key Cisc0123
!
!
```

```
radius server COHVSRADISE01-NEW
address ipv4 <A.B.C.D> auth-port 1645 acct-port 1646
timeout 15
key Cisc0123
!
!
aaa group server radius ISE-CLUSTER
server name COHVSRADISE01-NEW
!
!
!
!
aaa new-model
aaa session-id common
!
!

Router#
```

8-4 또 다른 유용한 명령은 테스트 aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy입니다.

```
Router#test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy
User was successfully authenticated.

Router#
```

9 - 네트워크 장치 관련 디버깅

- debug dot1x all - 모든 dot1x EAP 메시지를 표시합니다.
- debug aaa authentication - AAA 애플리케이션의 인증 디버그 정보를 표시합니다.
- debug aaa authorization - AAA 권한 부여에 대한 디버그 정보를 표시합니다.
- debug radius authentication - 단지 인증을 위한 프로토콜 수준 활동에 대한 자세한 정보를 제공합니다.
- debug radius - 프로토콜 수준 활동에 대한 자세한 정보를 제공합니다.

관련 정보

- Cisco 기술 지원 및 다운로드

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.