Windows 및 ISE 3.2를 사용하여 Dot1x용 보안 클라이언트 NAM 구성

목차

소개

이 문서에서는 Windows에서 Secure Client NAM(Network Analysis Module)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RADIUS 서 플리 컨 트에 대한 기본 적 인 이해
- 점1x

- PEAP
- 피키

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Windows 10 Pro 버전 22H2 빌드 19045.3930
- ISE 3.2
- Cisco C1117 Cisco IOS® XE Software, 버전 17.12.02
- Active Directory 2016

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

이 문서에서는 Windows에서 보안 클라이언트 NAM을 구성하는 방법에 대해 설명합니다. dot1x 인증을 수행하기 위한 사전 구축 옵션 및 프로파일 편집기가 사용됩니다. 또한, 이것이 어떻게 달성되는지에 대한 몇 가지 예들이 제공된다.

네트워킹에서 신청자는 포인트-투-포인트 LAN 세그먼트의 한 쪽 끝에 있는 엔티티로, 해당 링크의 다른 쪽 끝에 연결된 인증자가 인증하려고 합니다. IEEE 802.1X 표준에서는 서 플리 컨 트라는 용어를 사용하여 하드웨어 또는 소프트웨어를 나타냅니다. 실제로 서 플리 컨 트는 최종 사용자 컴퓨터에 설치 된 소프트웨어 응용 프로그램입니다. 사용자는 신청자를 호출하고 컴퓨터를 보안 네트워크에 연결하기 위한 자격 증명을 제출합니다. 인증이 성공하면 인증자는 일반적으로 컴퓨터가 네트워크에 연결하도록 허용합니다.

Network Access Manager 정보

Network Access Manager는 정책에 따라 보안 레이어 2 네트워크를 제공하는 클라이언트 소프트웨어입니다. 최적의 레이어 2 액세스 네트워크를 탐지 및 선택하고 유무선 네트워크 모두에 액세스하기 위한 디바이스 인증을 수행합니다. Network Access Manager는 사용자 및 디바이스 ID와 보안 액세스에 필요한 네트워크 액세스 프로토콜을 관리합니다. 엔드 유저가 관리자가 정의한 정책을 위반하는 연결을 하지 않도록 지능적으로 작동합니다.

Network Access Manager는 싱글 홈(single-homed)으로 설계되어 한 번에 하나의 네트워크 연결만 허용합니다. 또한 유선 연결은 무선보다 우선순위가 높으므로 유선 연결로 네트워크에 연결하면 IP 주소가 없는 무선 어댑터가 비활성화됩니다.

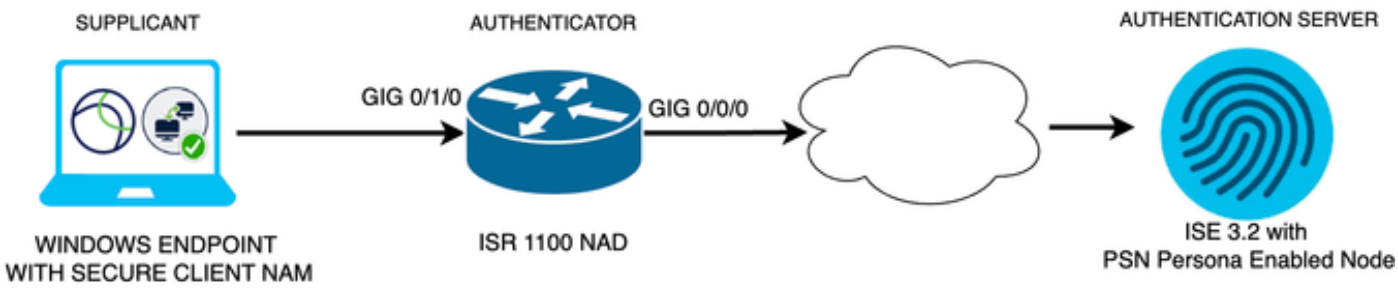
구성

네트워크 다이어그램

dot1x 인증에는 dot1x를 수행할 수 있는 신청자, RADIUS 내에서 dot1x 트래픽을 캡슐화하는 프록시 역할을 하는 NAS/NAD라고도 하는 인증자, 인증 서버 등 3가지 부분이 필요하다는 것을 이해하

는 것이 중요합니다.

이 예에서는 서 플리 컨 트가 서로 다른 방식으로 설치 및 구성 됩니다. 나중에 네트워크 디바이스 컨피그레이션 및 인증 서버의 시나리오가 표시됩니다.



네트워크 다이어그램

설정

1. Secure Client NAM(Network Access Manager)을 다운로드하고 설치합니다.

2. Secure Client NAM 프로파일 편집기를 다운로드하고 설치합니다.
3. 일반 기본 컨피그레이션
4. 시나리오 1: PEAP(MS-CHAPv2) 사용자 인증을 위한 보안 클라이언트 NAM 신청자를 구성합니다.
5. 시나리오 2: 사용자 및 머신 인증이 구성된 대로 EAP-FAST용 보안 클라이언트 NAM 신청자를 동시에 구성합니다.
6. 시나리오 3 1부: EAP-TLS용 보안 클라이언트 NAM 신청자를 구성합니다.
7. 시나리오 3 2부: NAD 및 ISE 데모를 구성합니다.

1. Secure Client NAM(Network Access Manager) 다운로드 및 설치

Cisco 소프트웨어 다운로드

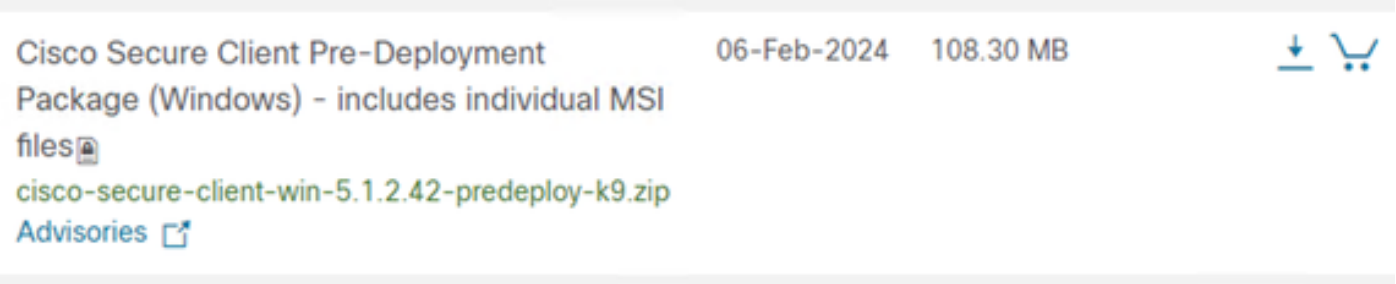
제품 이름 검색 표시줄에 Secure Client 5를 입력합니다.

Downloads Home(홈) > Security(보안) > VPN and Endpoint Security Clients(VPN 및 엔드포인트 보안 클라이언트) > Secure Client(AnyConnect 포함) > Secure Client 5(보안 클라이언트 5) > AnyConnect VPN Client Software(AnyConnect VPN 클라이언트 소프트웨어)를 선택합니다.

이 컨피그레이션 예에서는 버전 5.1.2.42가 사용됩니다.

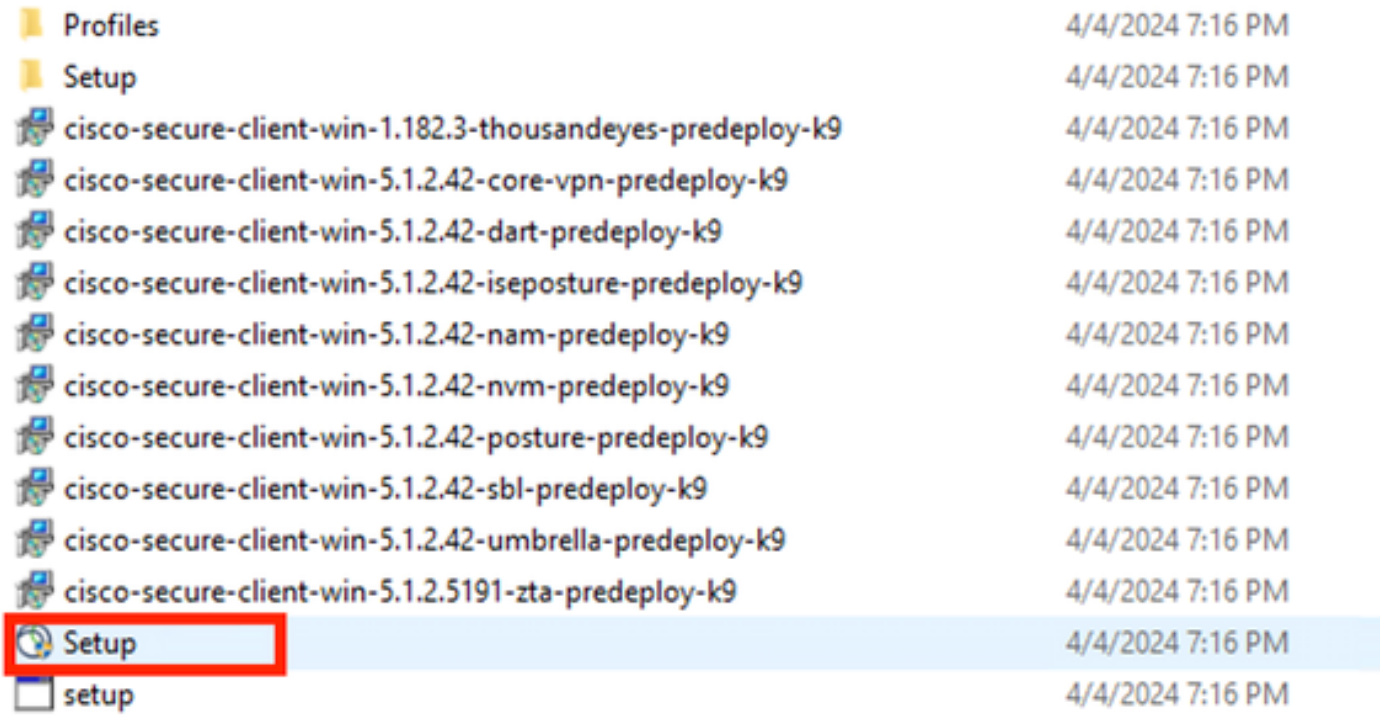
SCCM, ID 서비스 엔진, VPN 헤드엔드에서 Secure Client를 Windows 디바이스에 구축하는 방법에는 여러 가지가 있습니다. 다만, 이 글에서는 사용하는 설치 방법이 사전 구축 방법이다.

페이지에서 Cisco Secure Client Headend Deployment Package(Windows) 파일을 검색합니다.



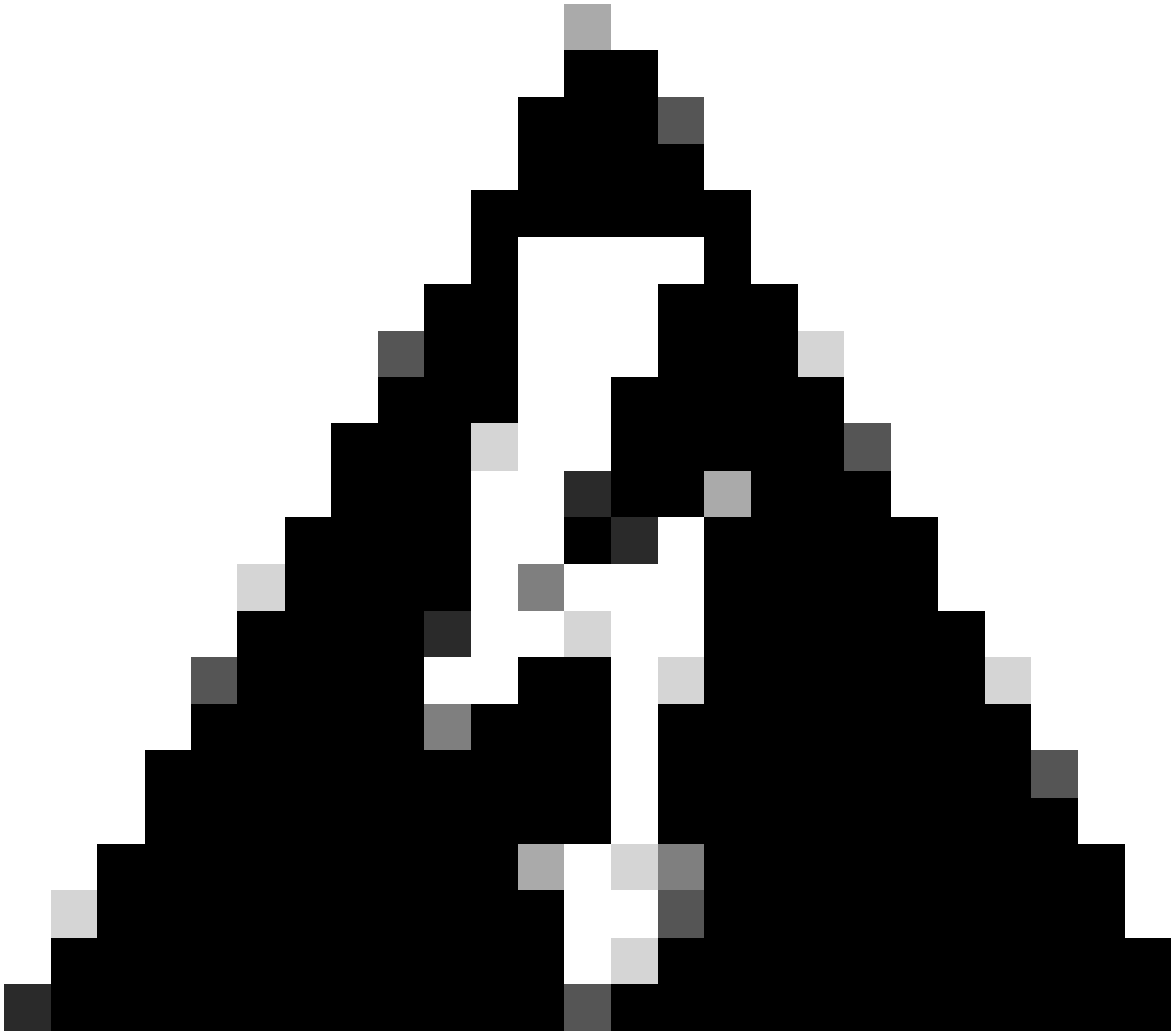
Msi zip 파일

다운로드하고 압축을 풀면 Setup(설정)을 클릭합니다.

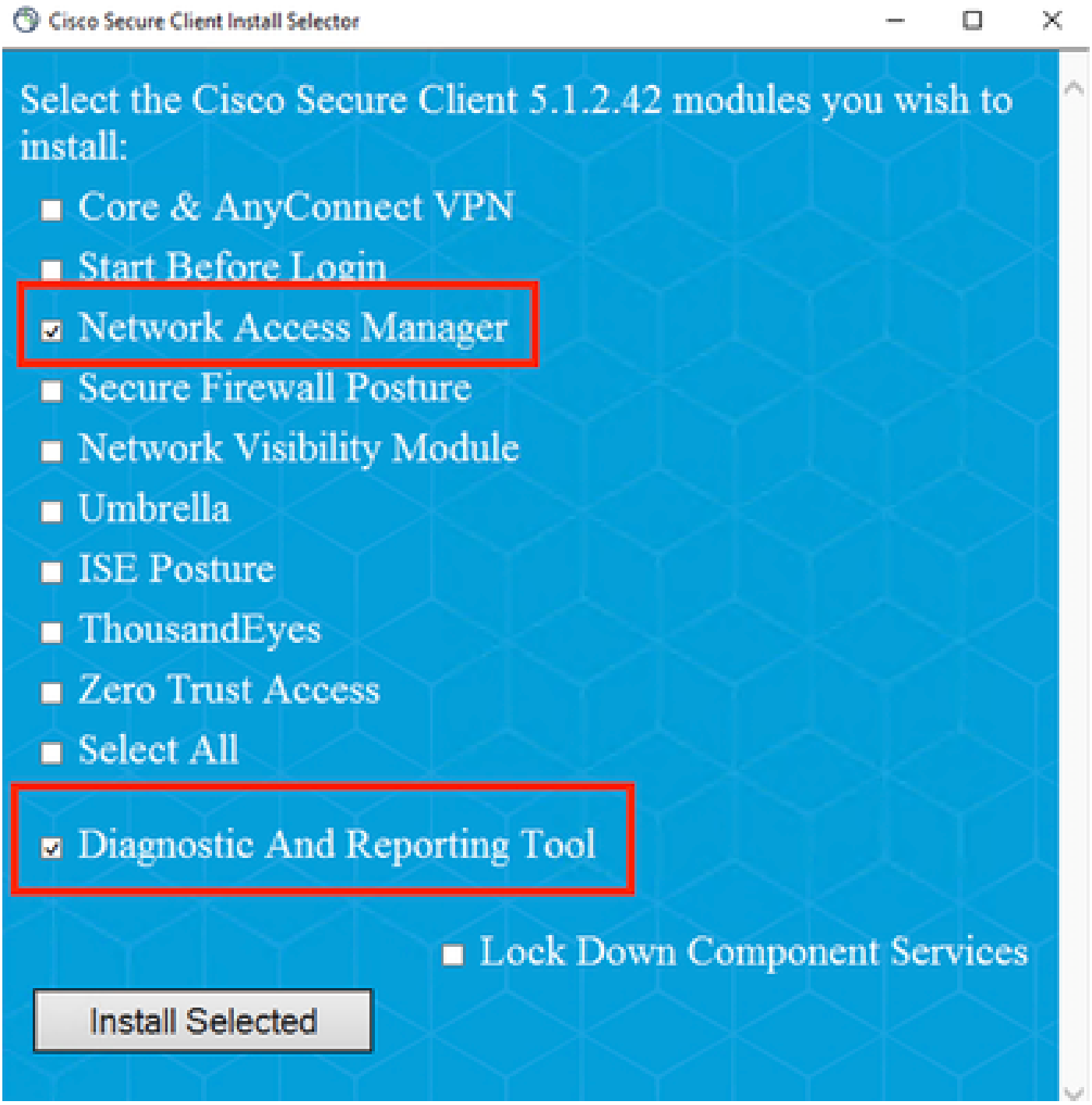


보안 클라이언트 파일

Network Access Manager 및 진단 및 보고 도구 모듈을 설치합니다.



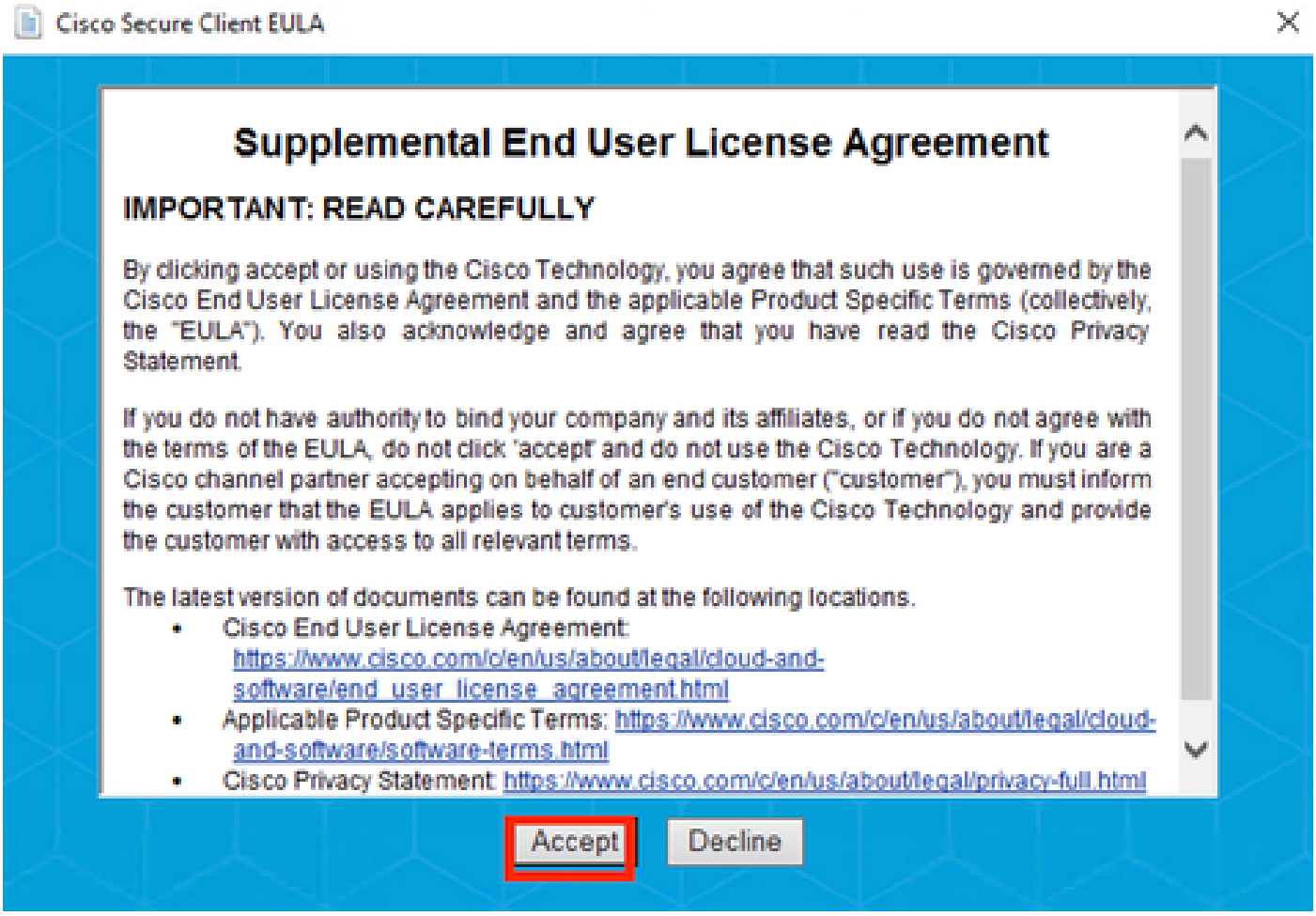
경고: Cisco Secure Client Wizard를 사용하는 경우 VPN 모듈이 자동으로 설치되고 GUI에서 숨겨집니다. VPN 모듈이 설치되어 있지 않으면 NAM이 작동하지 않습니다. 개별 MSI 파일 또는 다른 설치 방법을 사용하는 경우 VPN 모듈을 설치해야 합니다.



설치 선택기

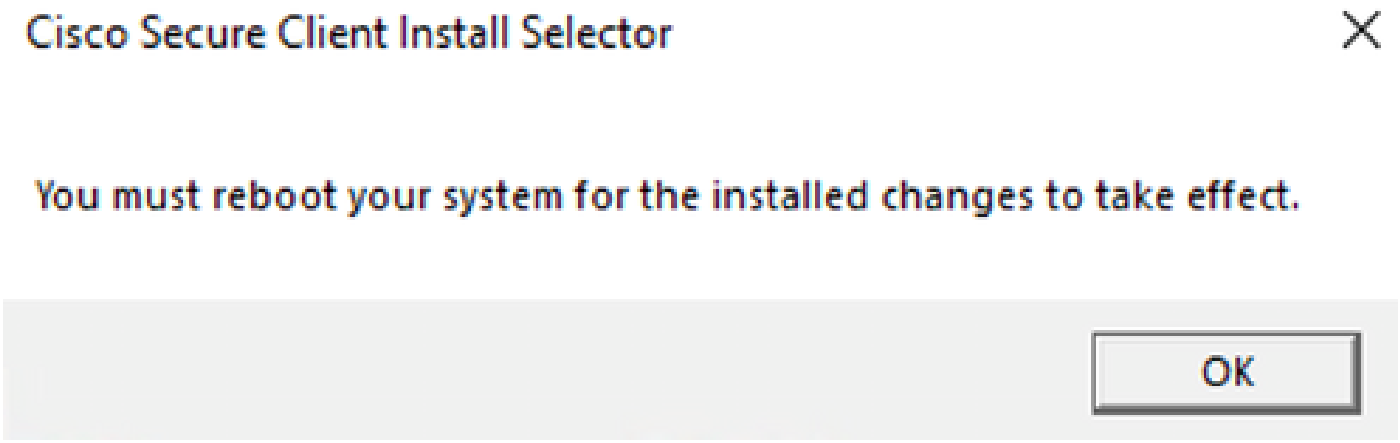
Install Selected(선택 항목 설치)를 클릭합니다.

EULA에 동의합니다.



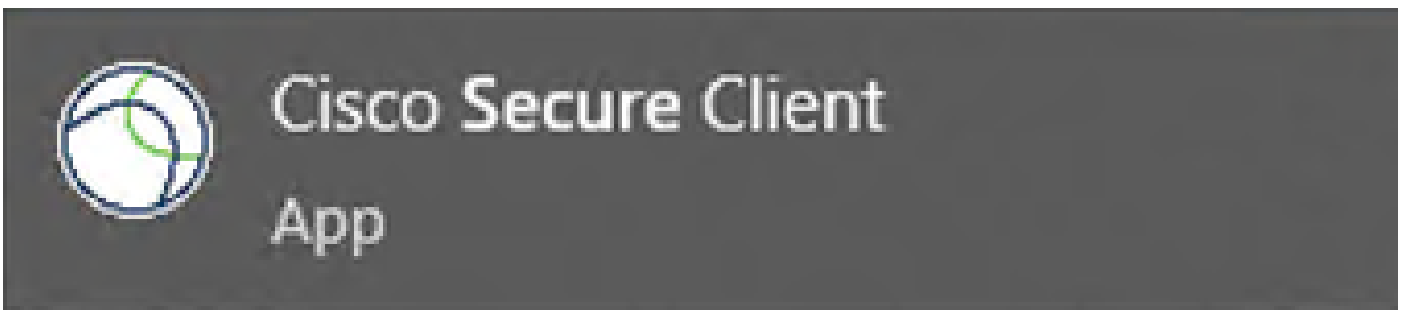
EULA 창

NAM 설치 후 다시 시작해야 합니다.



재부팅 요구 사항 창

설치한 후에는 Windows 검색 표시줄에서 이를 찾아 열 수 있습니다.



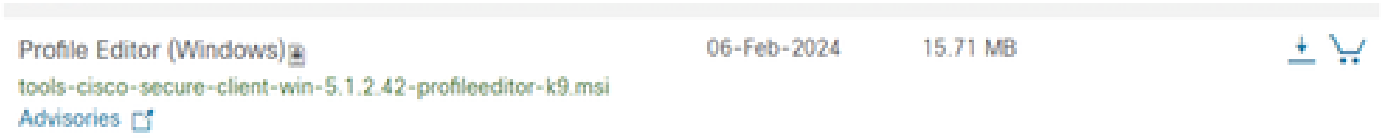
Secure Client 프로그램

2. Secure Client NAM 프로파일 편집기를 다운로드하고 설치합니다.

Dot1x 기본 설정을 구성하려면 Cisco Network Access Manager 프로파일 편집기가 필요합니다.

Secure Client가 다운로드되는 동일한 페이지에서 Profile Editor 옵션이 나타납니다.

이 예에서는 버전 5.1.2.42의 옵션을 사용합니다.



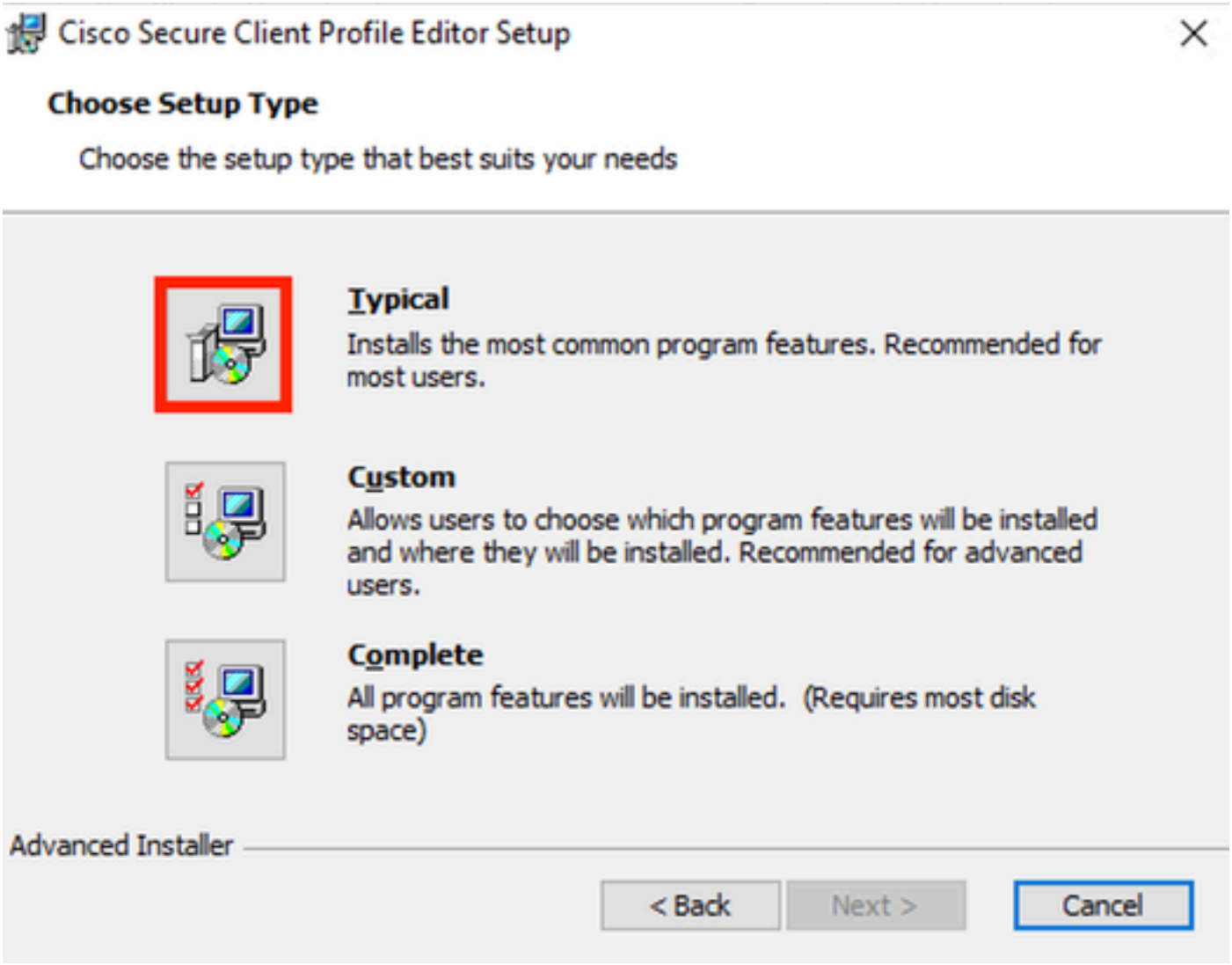
프로파일 편집기

다운로드한 후 설치를 진행합니다.

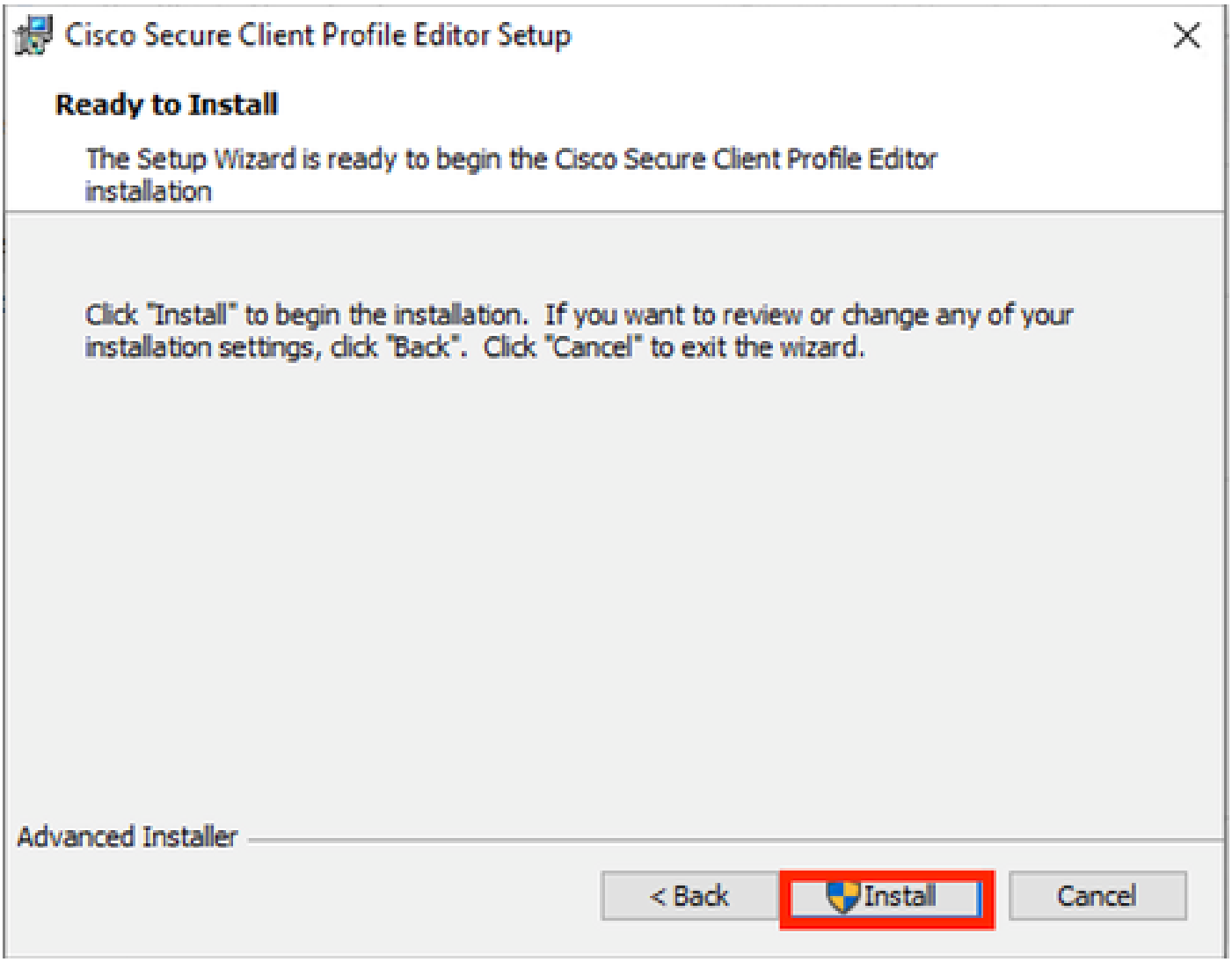
msi 파일을 실행합니다.

프로파일 편집기 설정 창

Typical setup 옵션을 사용합니다.

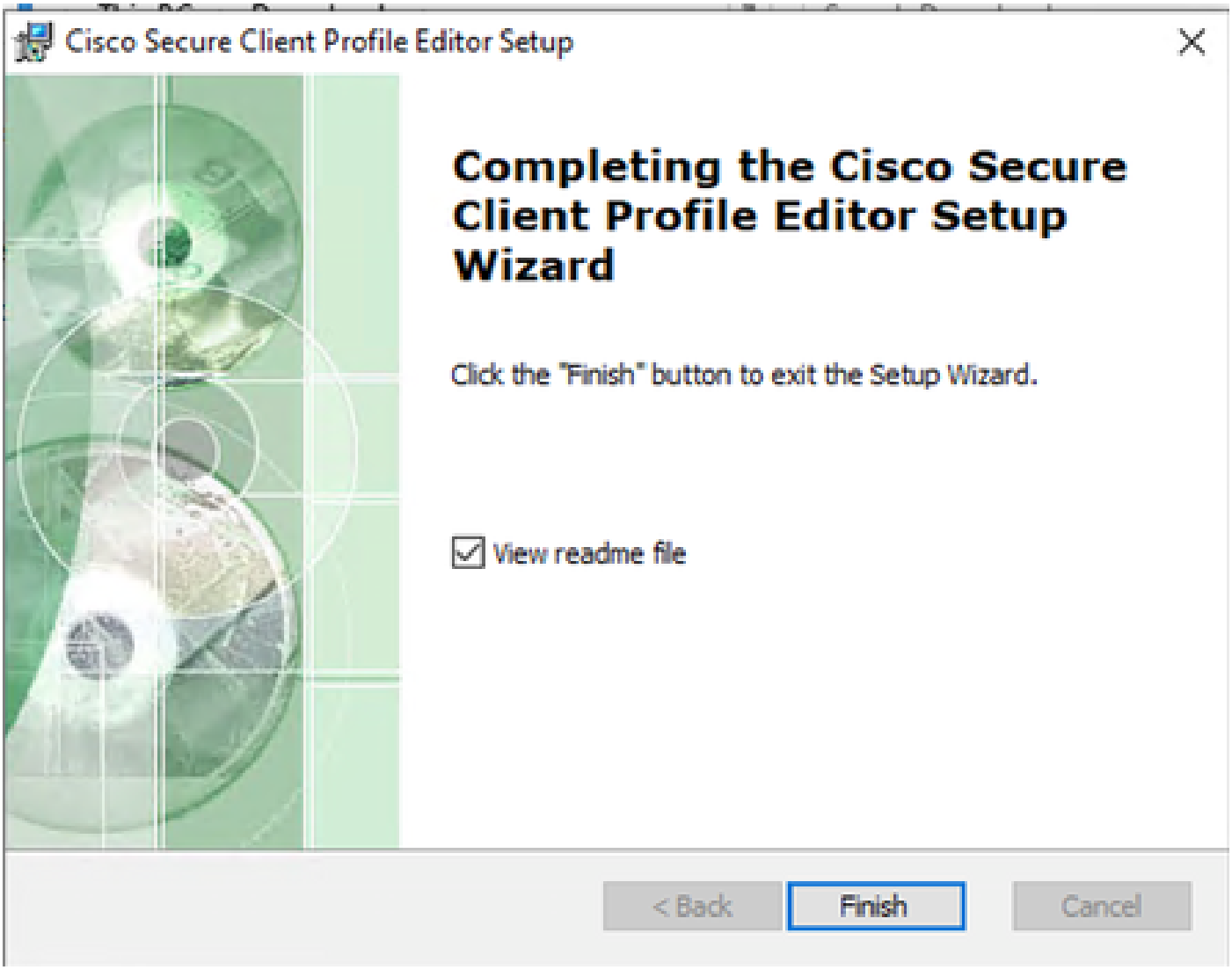


프로파일 편집기 설정



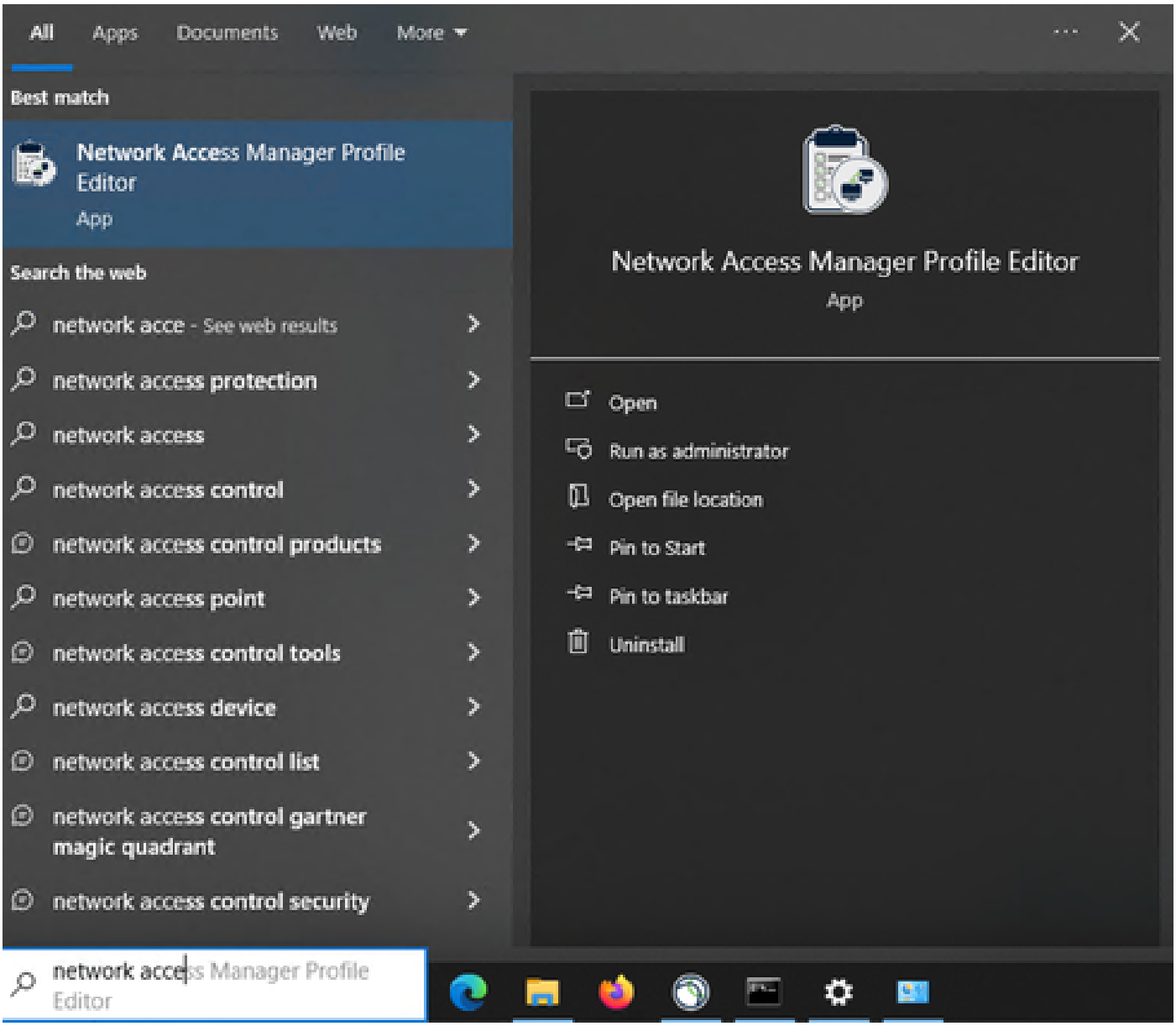
설치 창

Finish(마침)를 클릭합니다.



프로파일 편집기 설정 종료

설치가 완료되면 검색 표시줄에서 Network Access Manager 프로파일 편집기를 엽니다.



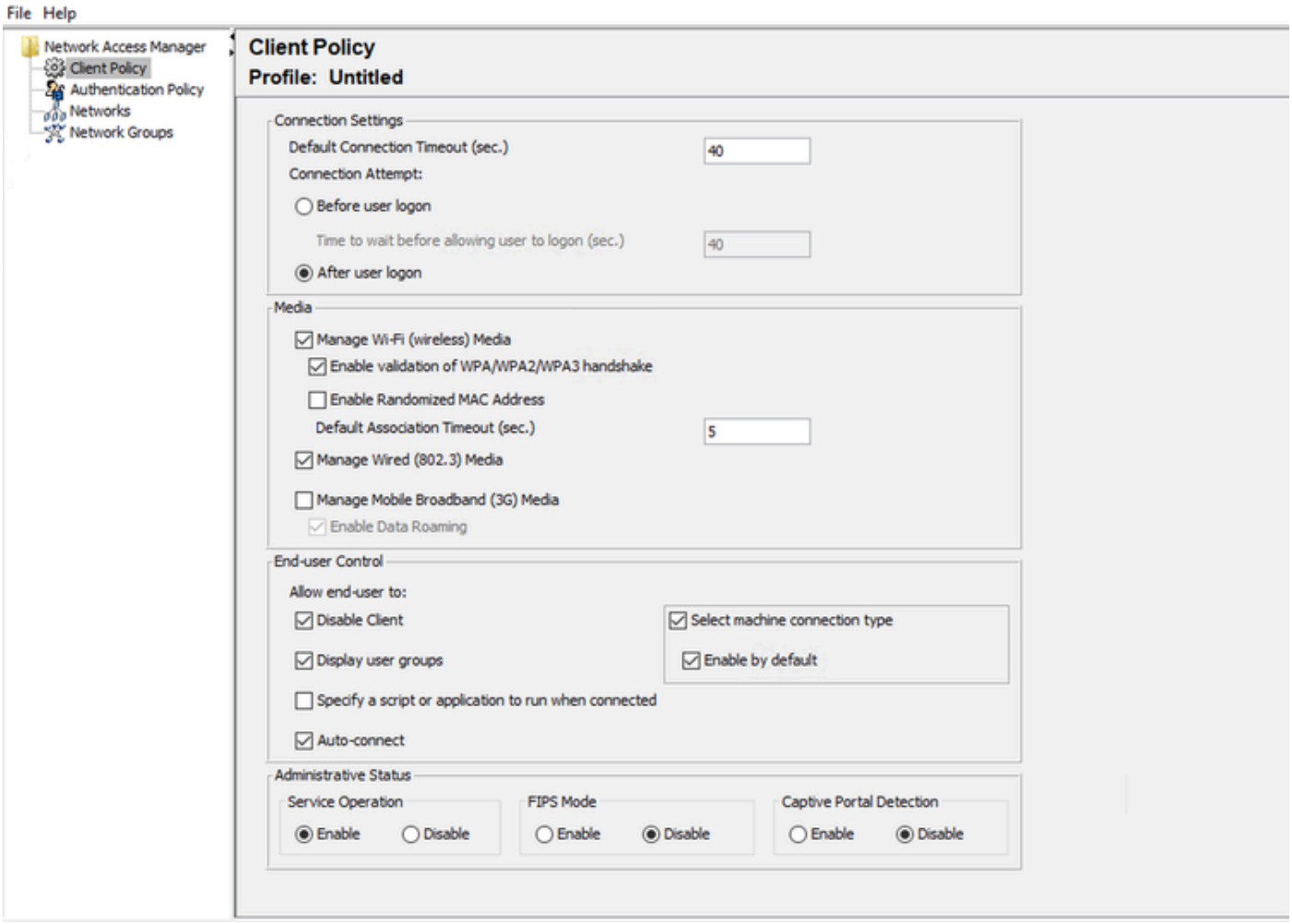
검색 막대의 NAM용 프로파일 편집기

Network Access Manager 및 프로파일 편집기 설치가 완료되었습니다.

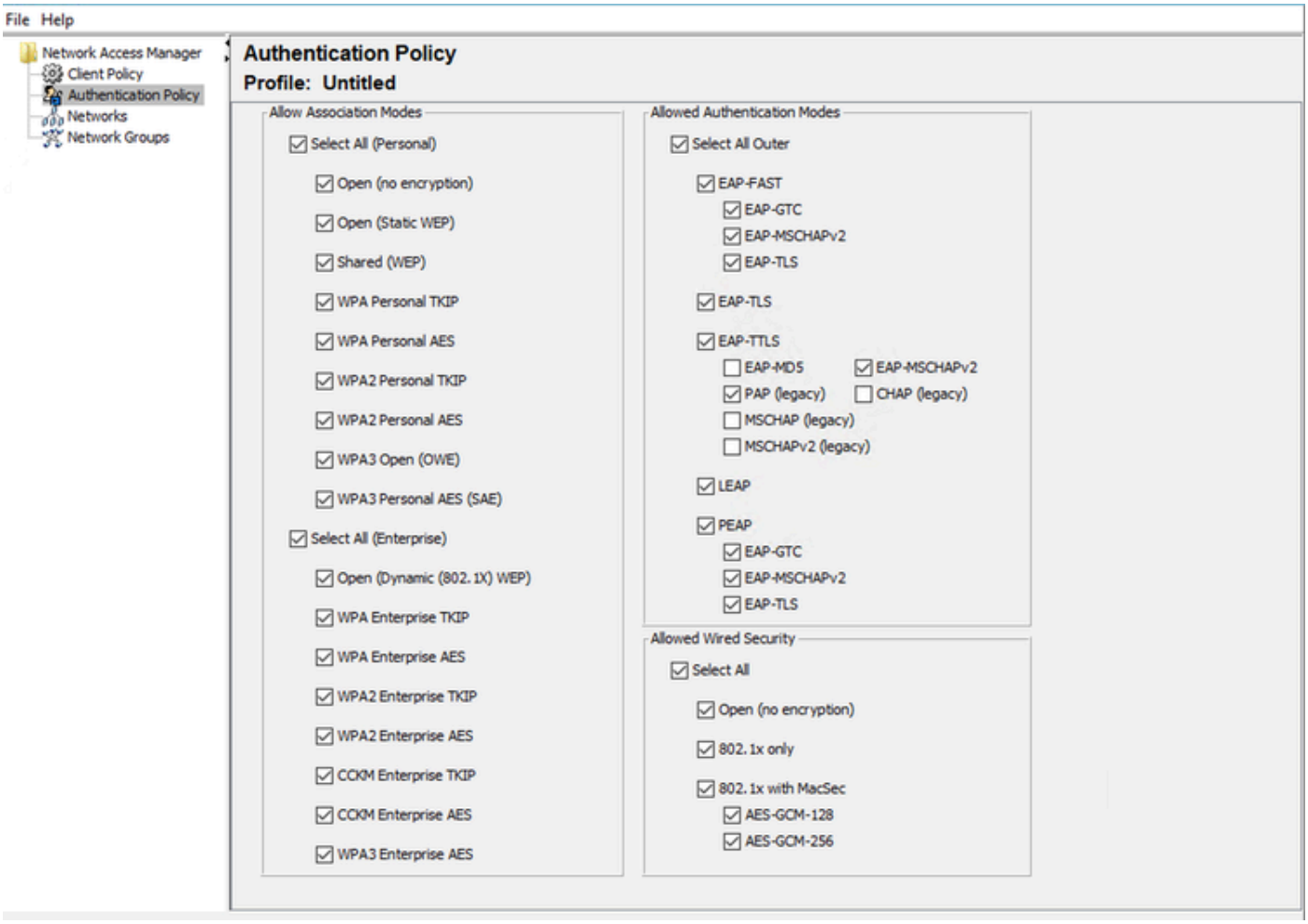
3. 일반 기본 구성

이 문서에 제시된 모든 시나리오에는 다음에 대한 구성이 포함되어 있습니다.

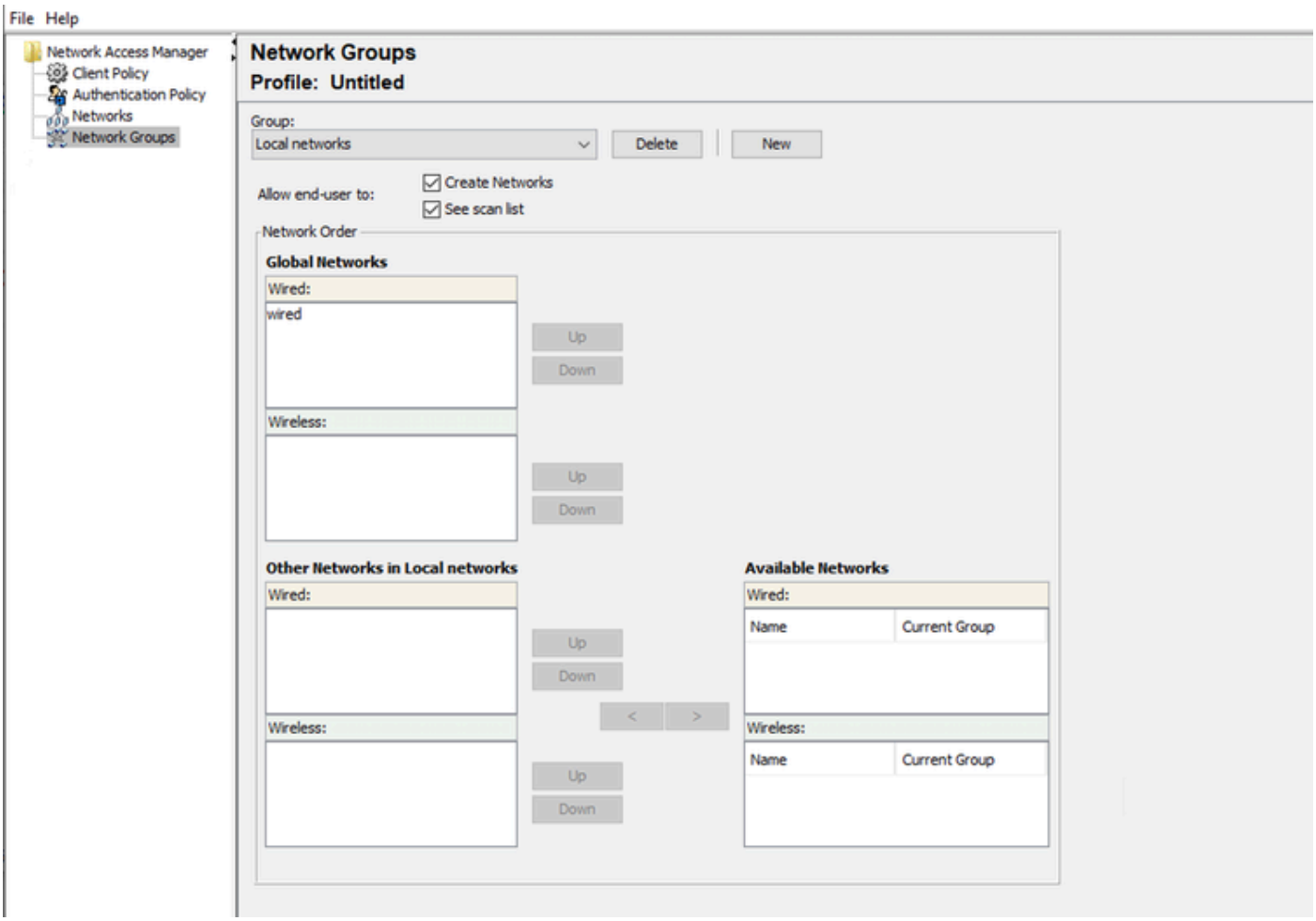
- 클라이언트 정책
- 인증 정책
- 네트워크 그룹



NAM 프로파일 편집기 클라이언트 정책



NAM 프로파일 편집기 인증 정책



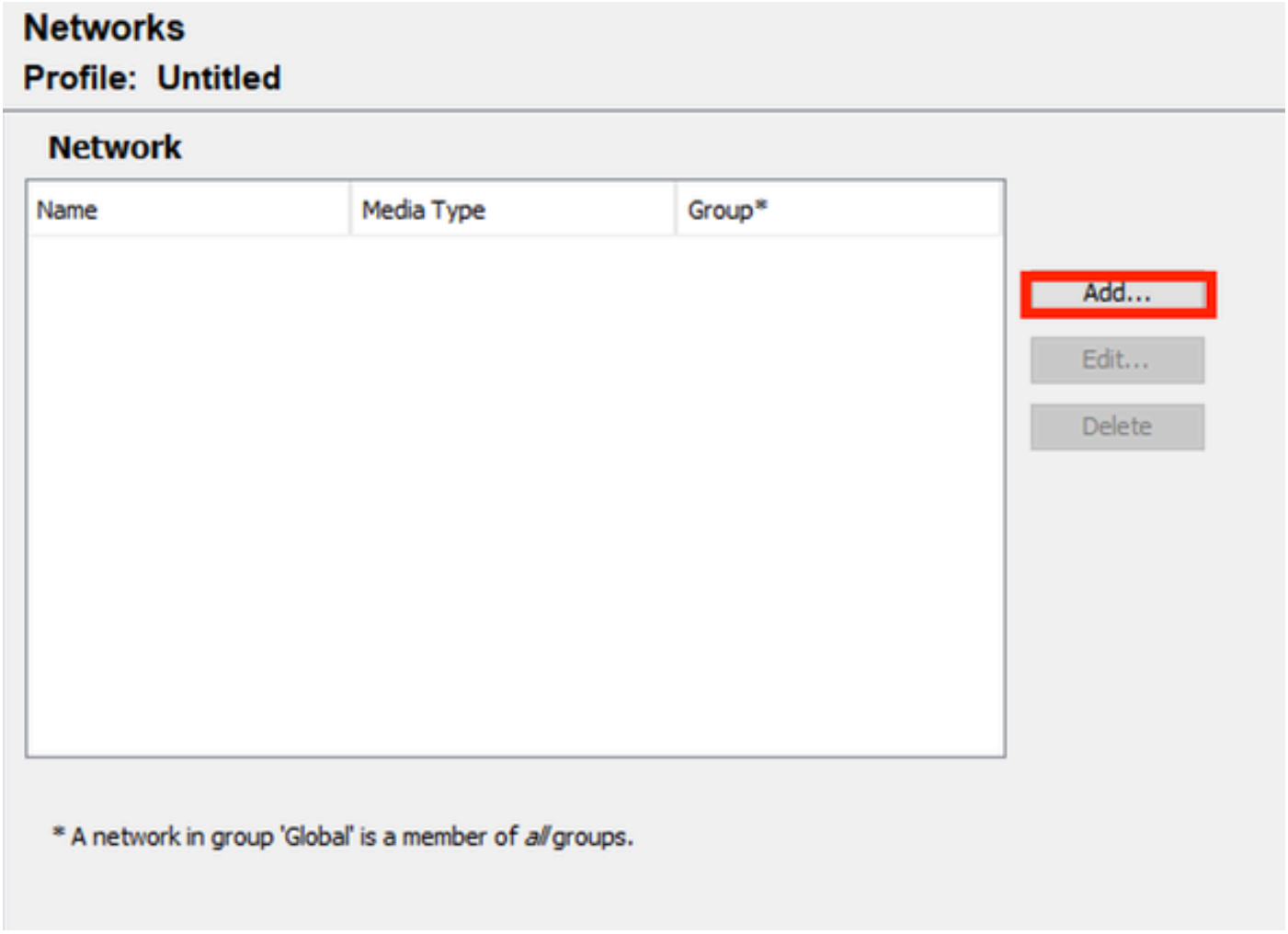
네트워크 그룹 탭

4. 시나리오 1: PEAP(MS-CHAPv2) 사용자 인증을 위한 보안 클라이언트 NAM 신청자 구성

네트워크 섹션으로 이동합니다.

기본 네트워크 프로필을 삭제할 수 있습니다.

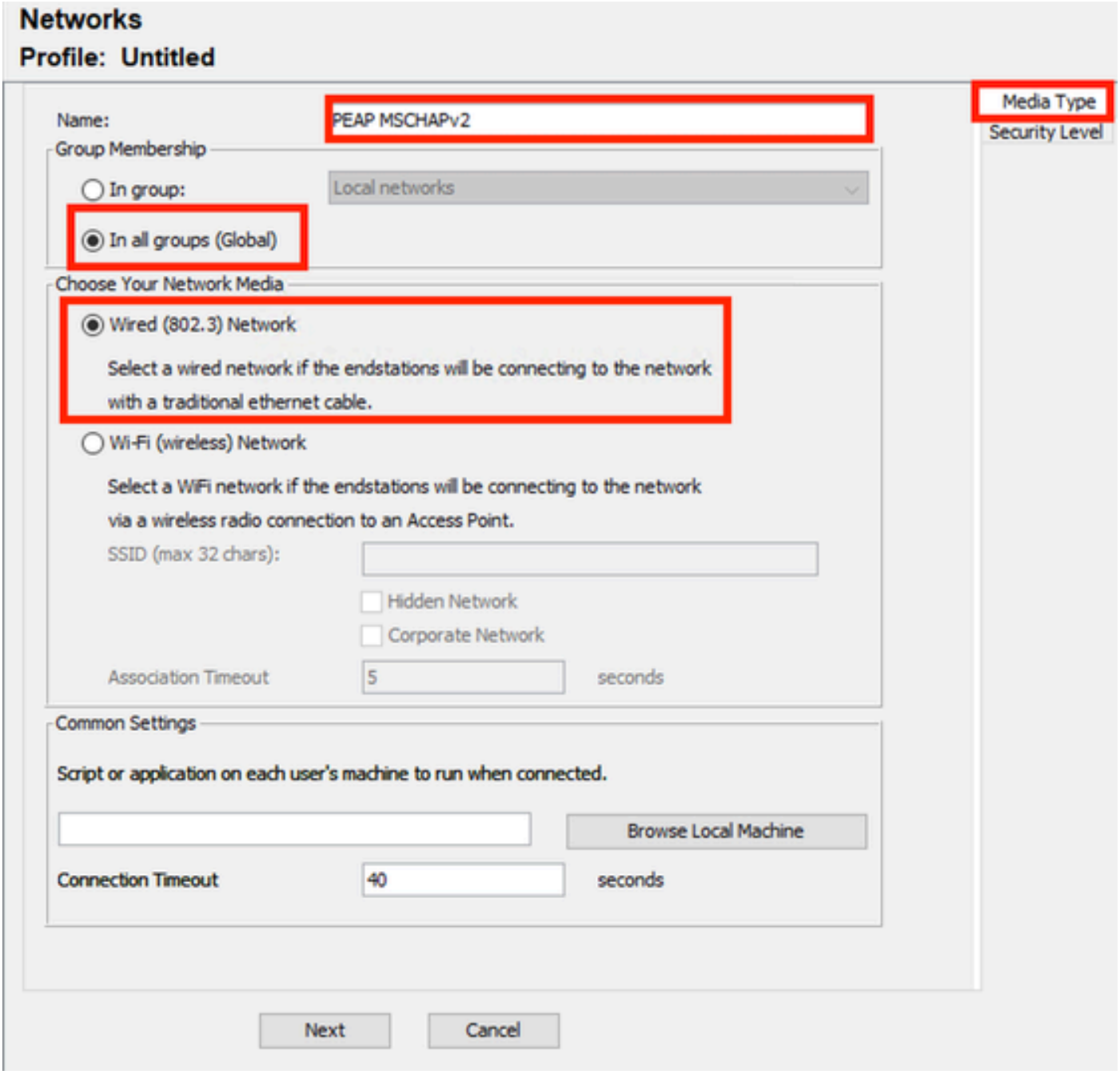
Add(추가)를 클릭합니다.



네트워크 프로파일 생성

네트워크 프로필의 이름을 지정합니다.

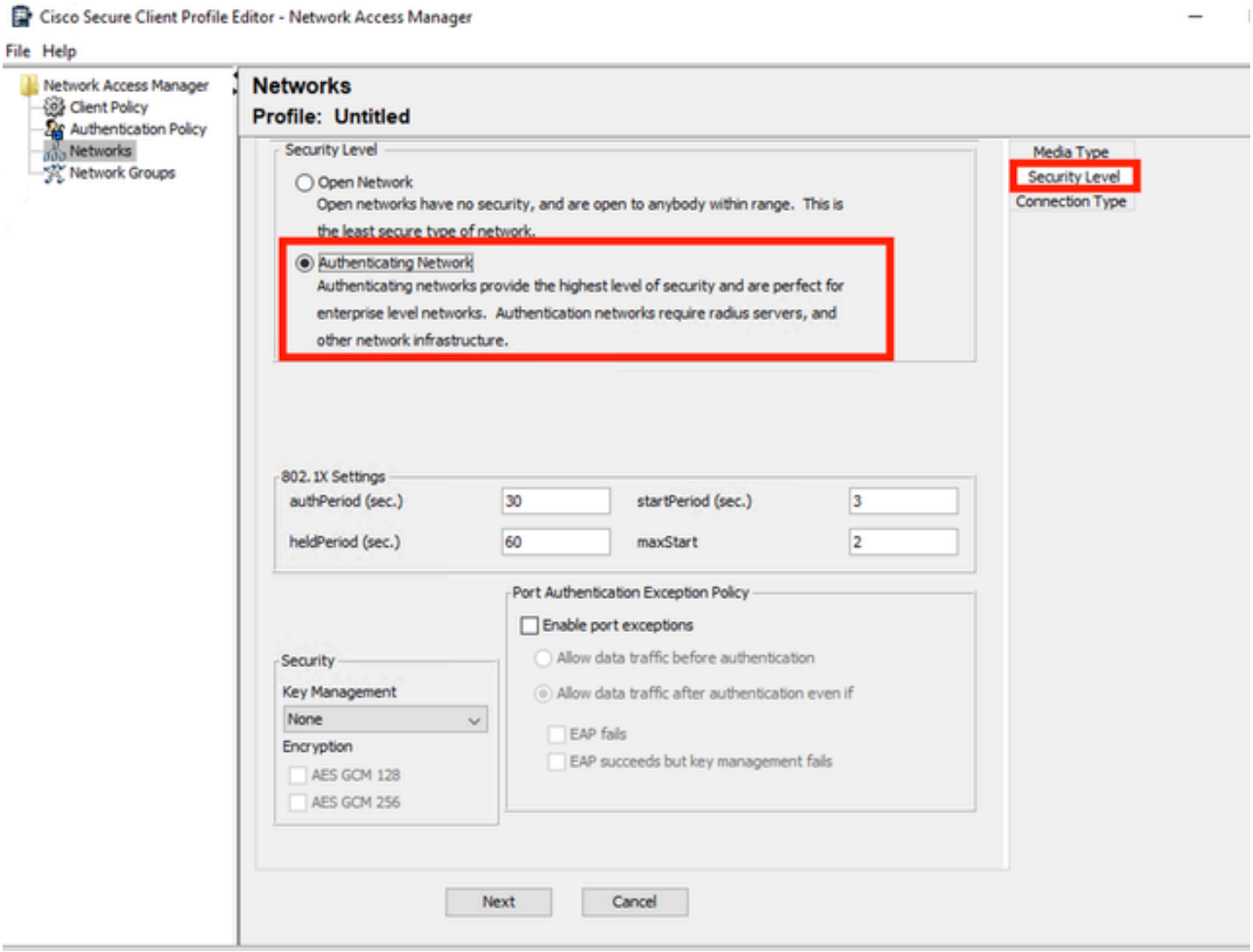
그룹 멤버십에 대해 Global을 선택합니다. Wired Network 미디어를 선택합니다.



네트워크 프로파일 미디어 유형 섹션

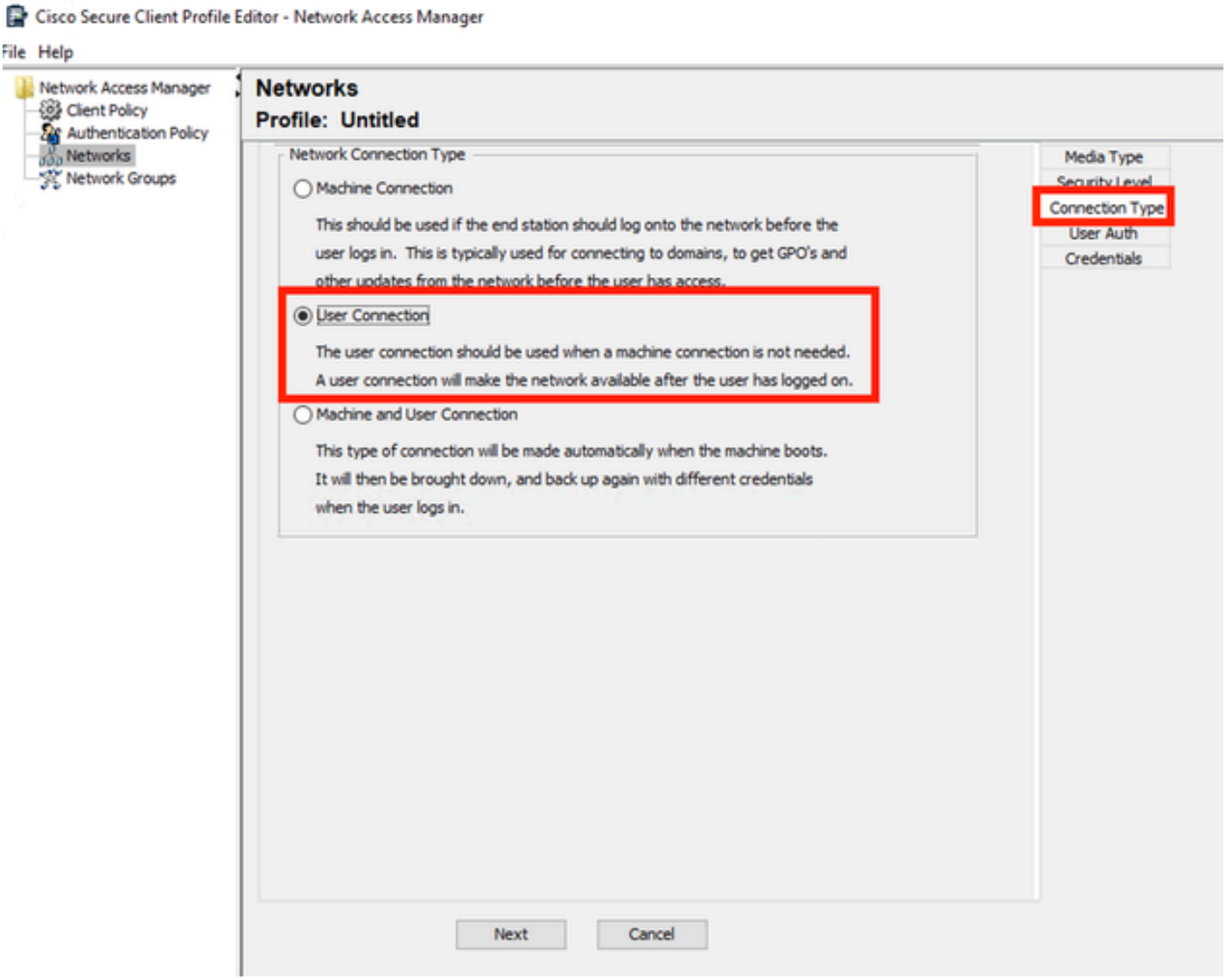
Next(다음)를 클릭합니다.

인증 네트워크를 선택하고 보안 레벨 섹션의 나머지 옵션에 대해 기본값을 사용합니다.



네트워크 프로파일 보안 레벨

Next(다음)를 클릭하여 Connection Type(연결 유형) 섹션을 계속합니다.

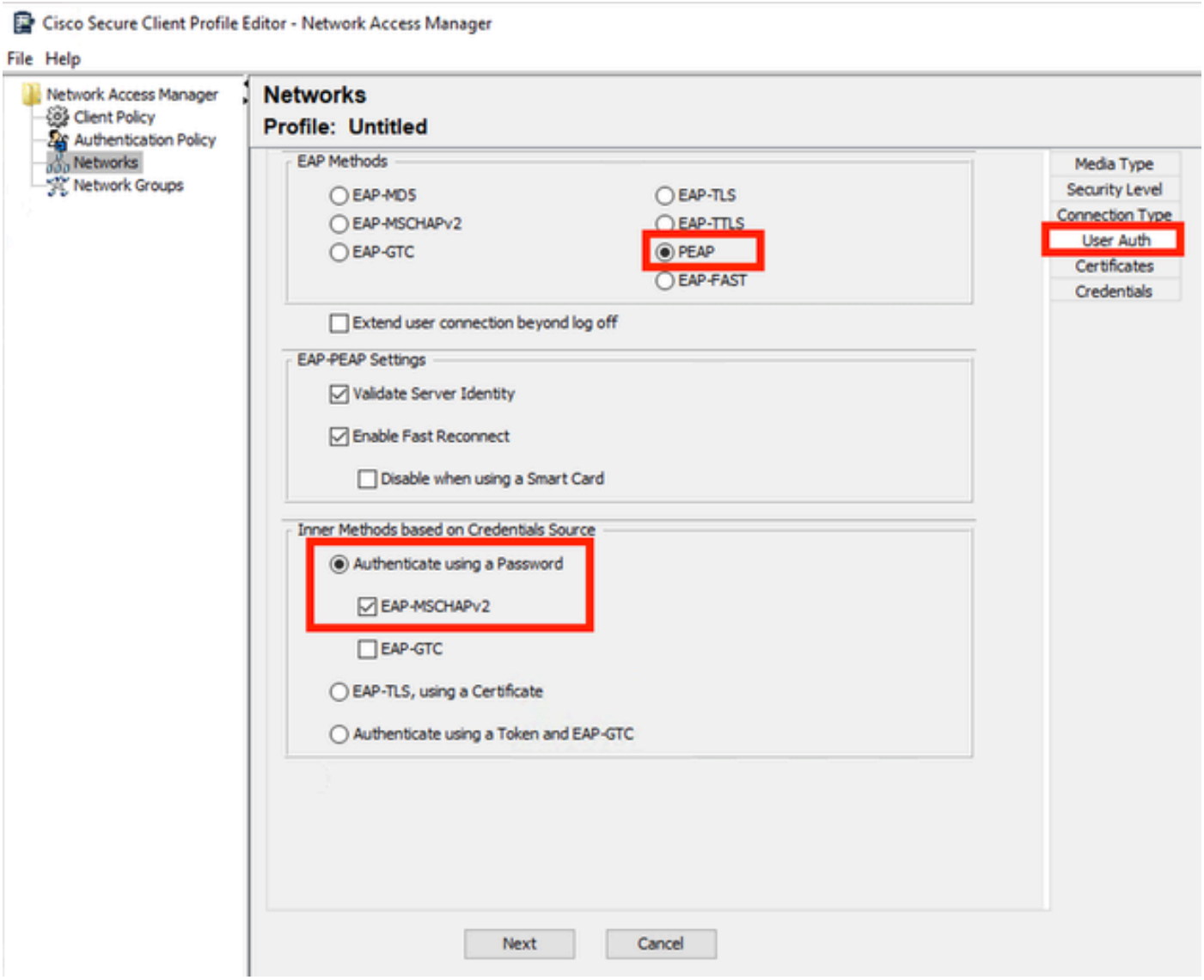


네트워크 프로파일 연결 유형

사용자 연결 연결 유형을 선택합니다.

Next(다음)를 클릭하여 현재 사용 가능한 User Auth(사용자 인증) 섹션을 계속합니다.

일반 EAP 방법으로 PEAP를 선택합니다.



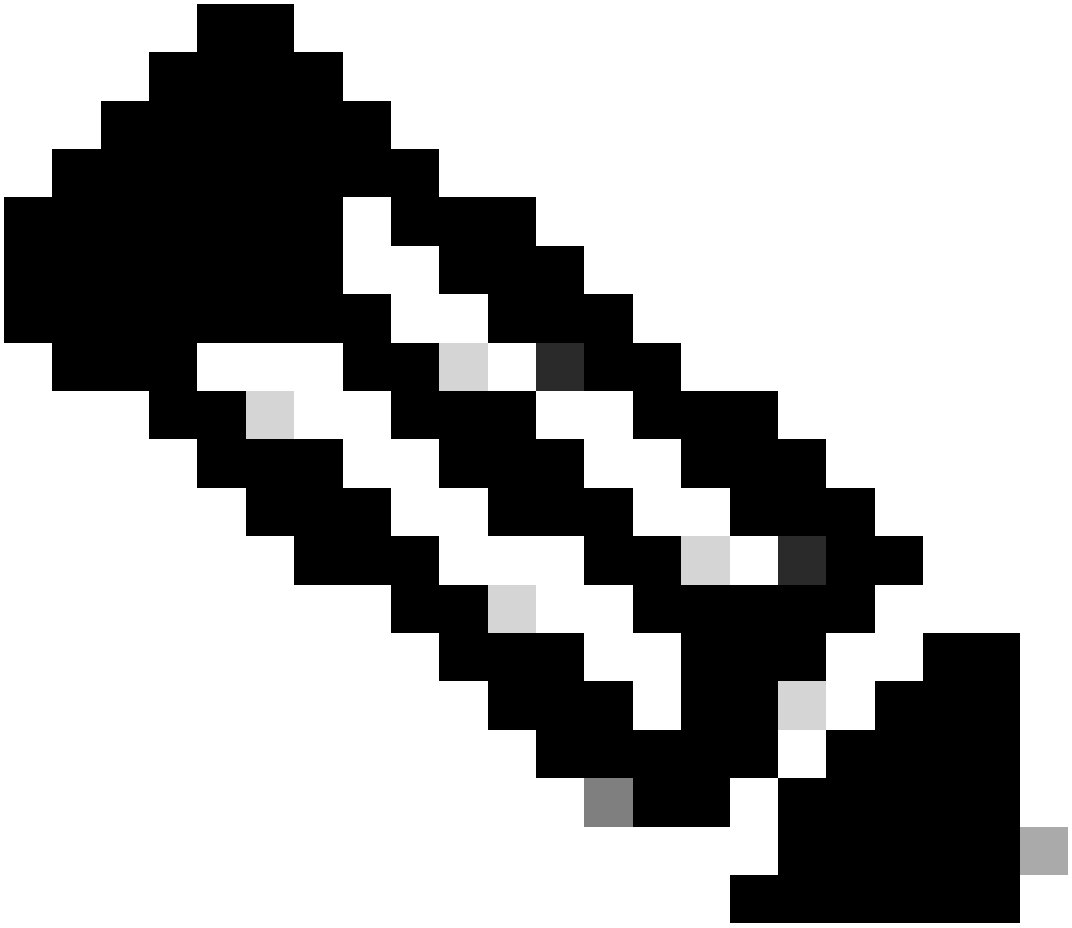
네트워크 프로파일 사용자 인증

EAP-PEAP 설정에서 기본값을 변경하지 마십시오.

Inner Methods based on Credentials Source 섹션을 계속합니다.

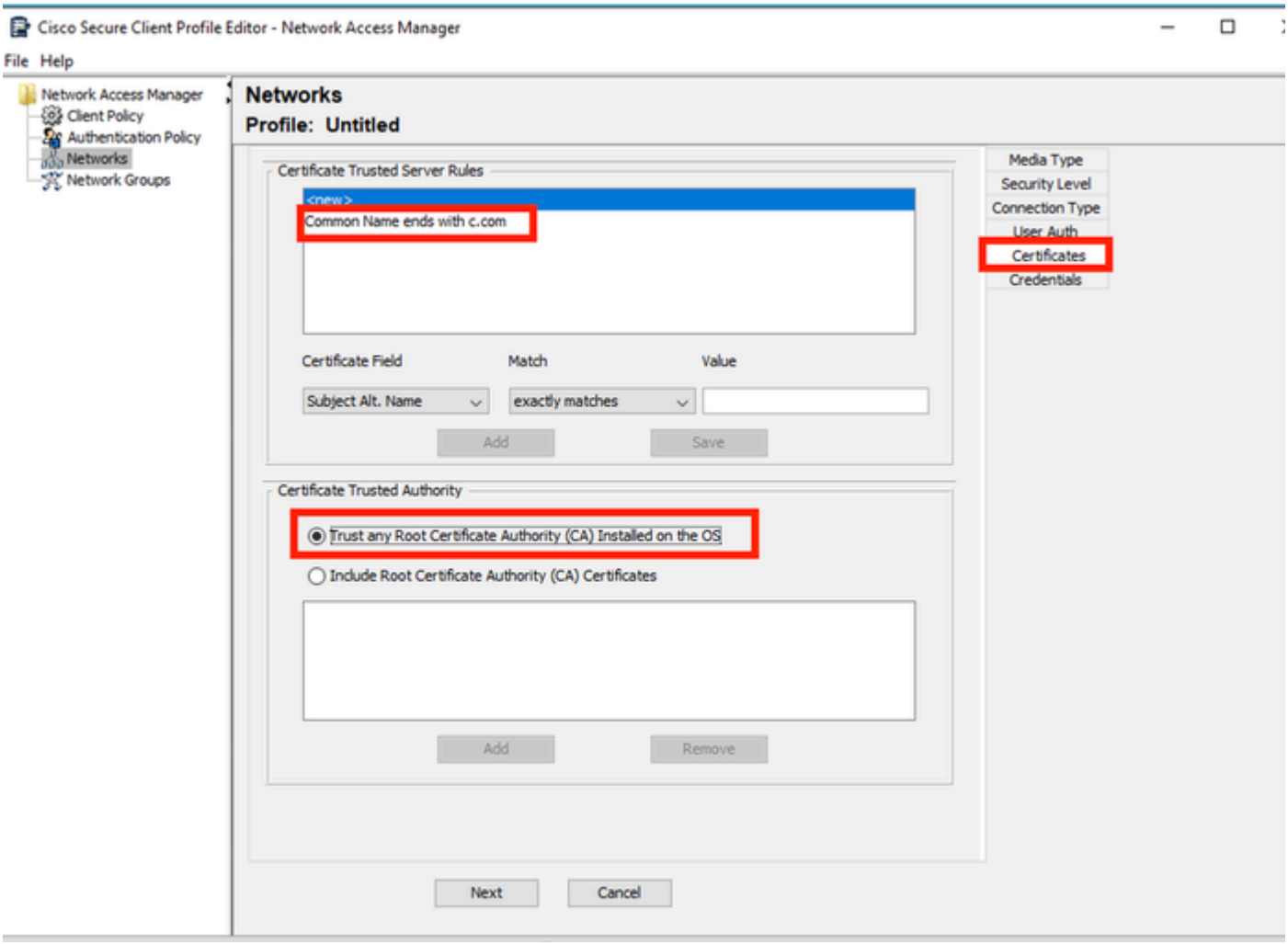
EAP PEAP에 대해 존재하는 여러 내부 방법에서 Authenticate using a Password(비밀번호를 사용하여 인증)를 선택하고 EAP-MSCHAPv2를 선택합니다.

Next(다음)를 클릭하여 Certificate(인증서) 섹션으로 이동합니다.



참고: EAP-PEAP 설정에서 서버 ID 검증 옵션이 선택되었으므로 Certificate(인증서) 섹션이 표시됩니다. EAP PEAP의 경우 서버 인증서를 사용하여 캡슐화를 수행합니다.

Certificates(인증서) 섹션의 Certificate Trusted Server Rules(인증서 신뢰 서버 규칙)에서 Common Name end with c.com(공통 이름 끝은)가 사용됩니다. 컨피그레이션의 이 섹션에서는 EAP PEAP 흐름 중에 서버가 사용하는 인증서를 참조합니다. 사용자 환경에서 ISE(Identity Service Engine)를 사용하는 경우 정책 서버 노드 EAP 인증서의 일반 이름을 사용할 수 있습니다.

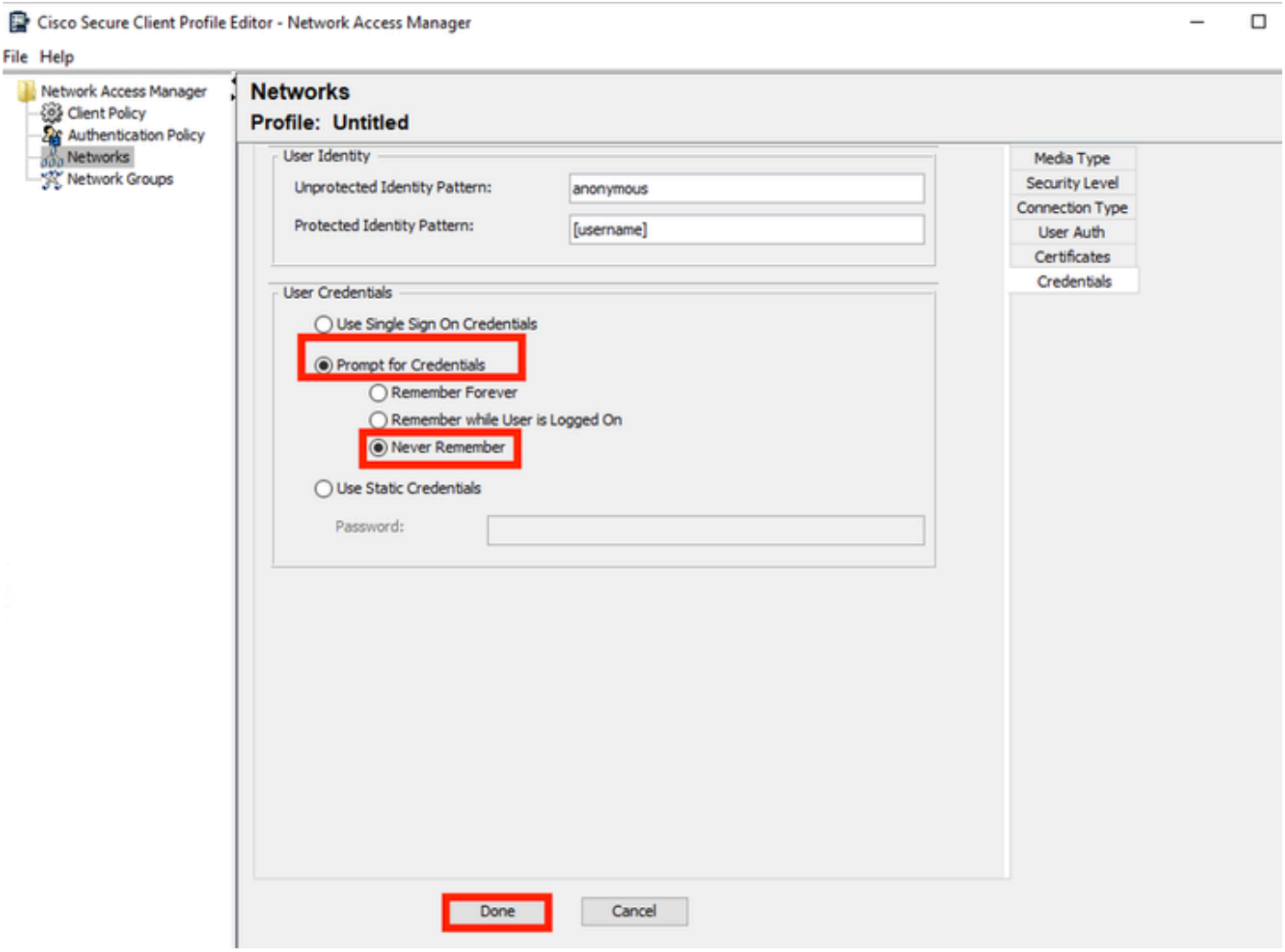


네트워크 프로파일 인증서 섹션

Certificate Trusted Authority에서 두 옵션을 선택할 수 있습니다. 이 시나리오에서는 RADIUS EAP 인증서를 서명한 특정 CA 인증서를 추가하는 대신 Trust any Root Certificate Authority (CA) Installed on the OS(OS에 설치된 모든 루트 CA 신뢰) 옵션이 사용됩니다.

이 옵션을 사용하면 Windows 디바이스는 Manage User Certs(사용자 인증서 관리) 프로그램 인증서 — Current User(현재 사용자) > Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) > Certificates(인증서)에 포함된 인증서에 의해 서명된 모든 EAP 인증서를 신뢰합니다.

Next(다음)를 클릭합니다.



네트워크 프로파일 자격 증명 섹션

Credentials(자격 증명) 섹션에서 User Credentials(사용자 자격 증명) 섹션만 변경됩니다.

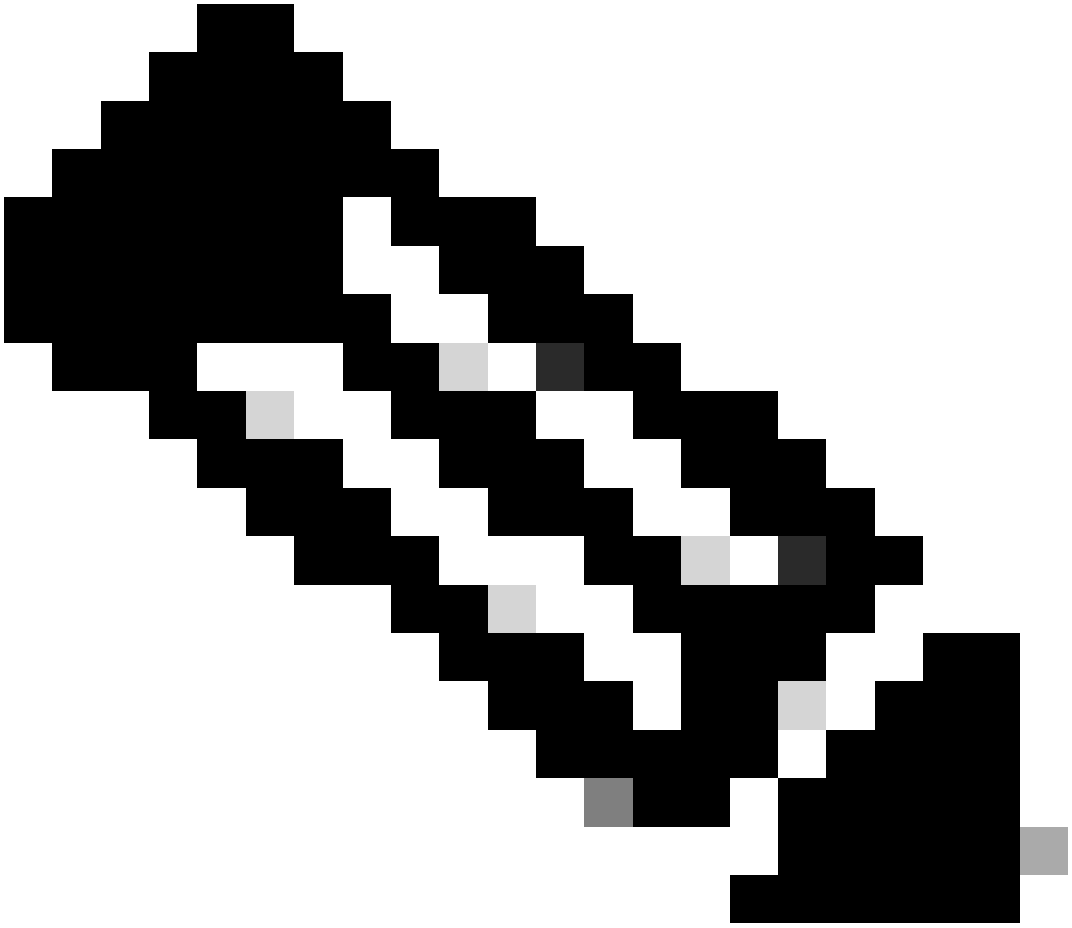
Prompt for Credentials(자격 증명 프롬프트) > Never Remember(기억하지 않음) 옵션이 선택되어 있으므로 각 인증에서 인증을 수행하는 사용자가 자격 증명을 입력해야 합니다.

완료를 클릭합니다.

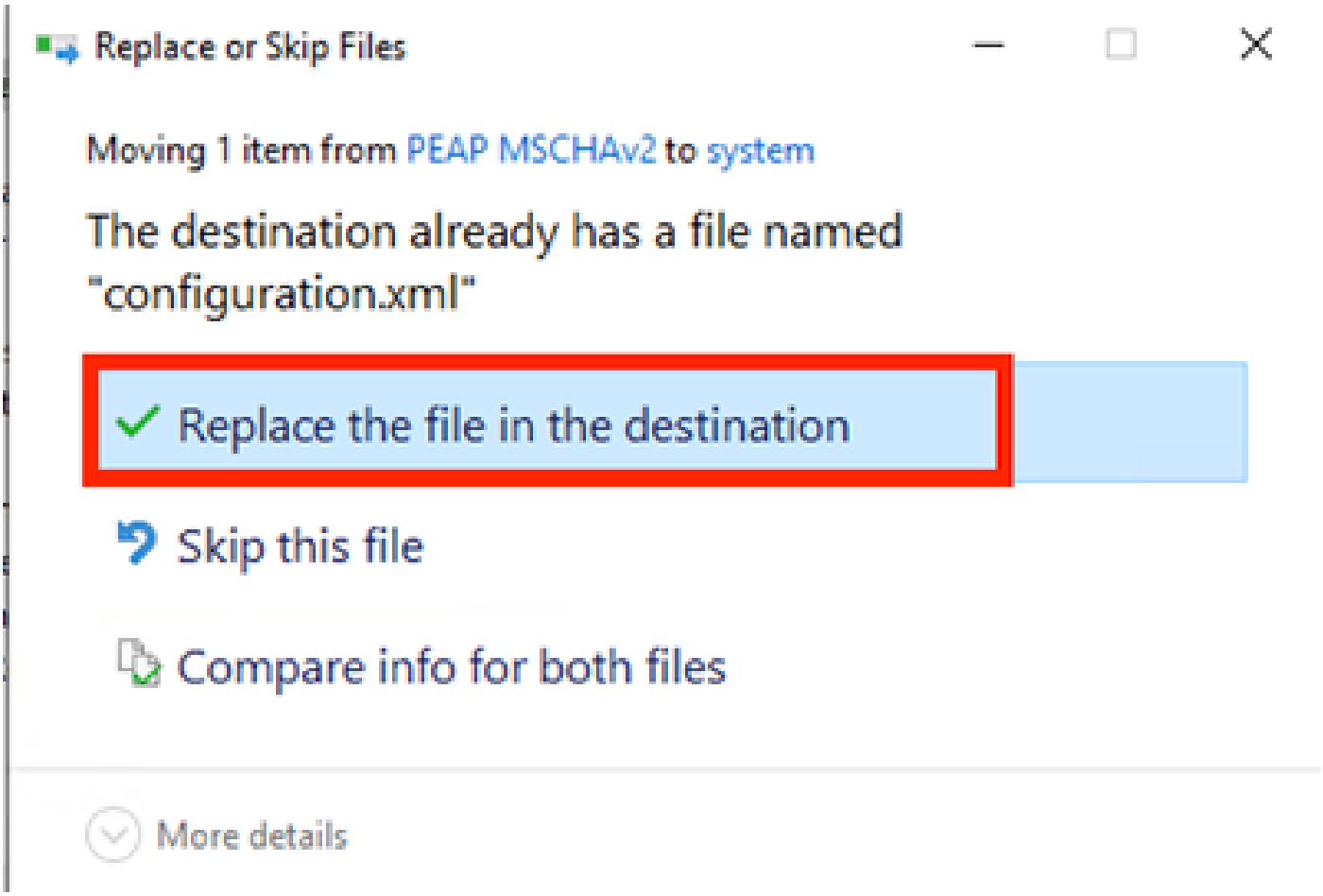
Secure Client Network Access Manager 프로파일을 configuration.xml로 File(파일) > Save As(다른 이름으로 저장) 옵션과 함께 저장합니다.

Secure Client Network Access Manage(보안 클라이언트 네트워크 액세스 관리)에서 방금 만든 프로필을 사용하도록 하려면 다음 디렉터리의 configuration.xml 파일을 새 디렉터리로 바꿉니다.

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



참고: 파일의 이름은 configuration.xml이어야 합니다. 그렇지 않으면 파일이 작동하지 않습니다.

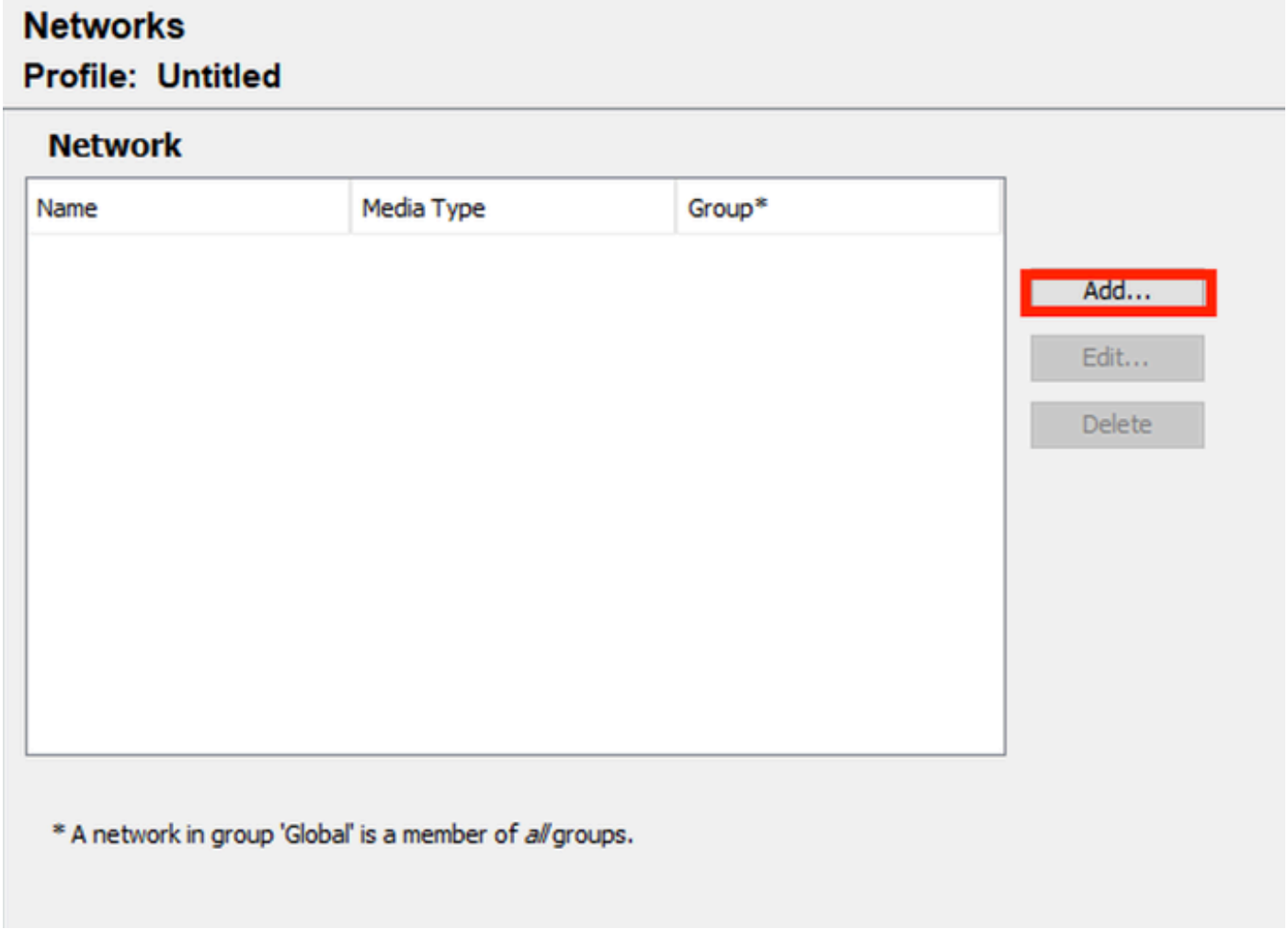


파일 섹션 바꾸기

5. 시나리오 2: EAP-FAST 동시 사용자 및 머신 인증을 위한 보안 클라이언트 NAM 신청자 구성

NAM 프로파일 편집기를 열고 네트워크 섹션으로 이동합니다.

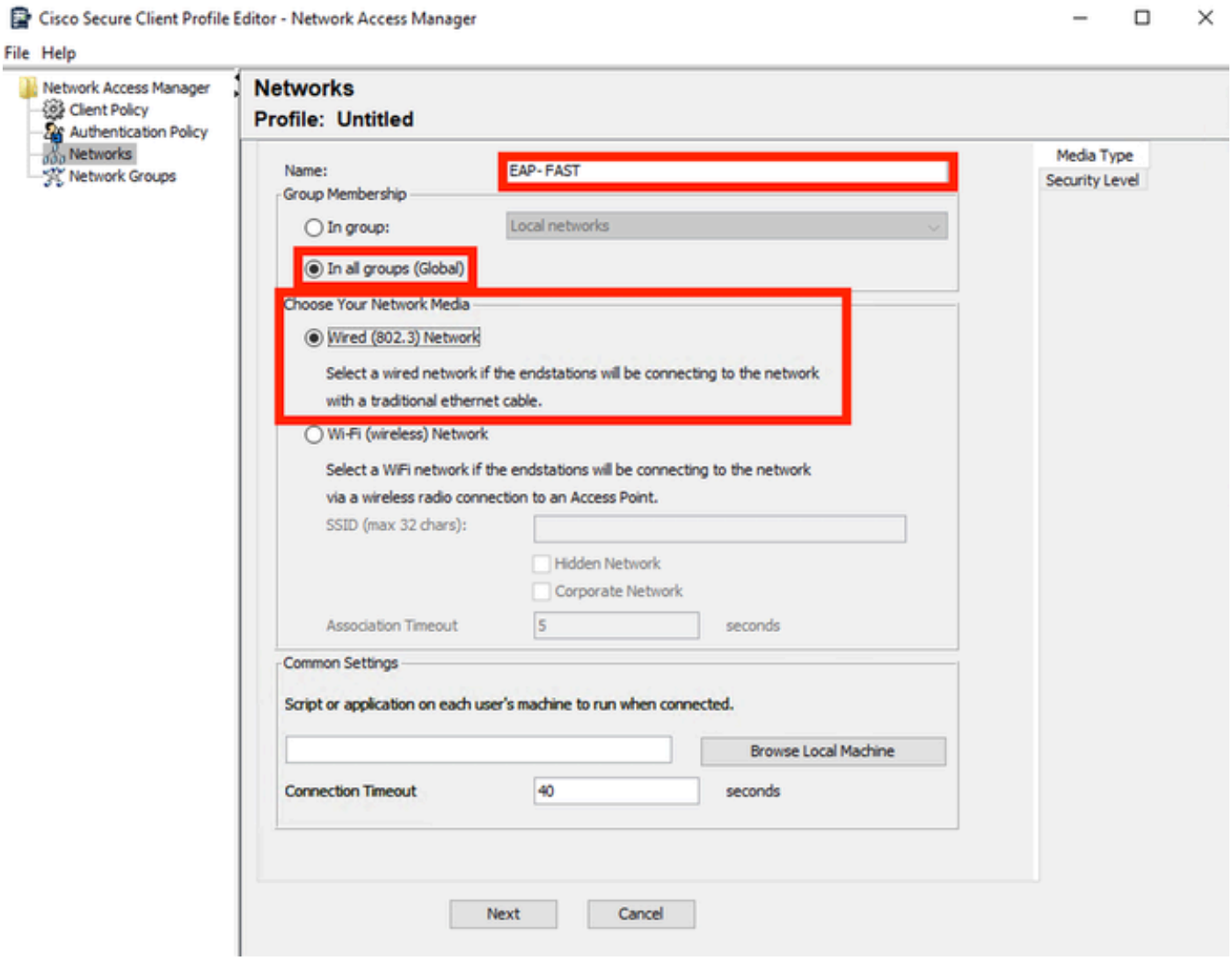
Add(추가)를 클릭합니다.



NAM 프로파일 편집기 네트워크 탭

네트워크 프로필에 이름을 입력합니다.

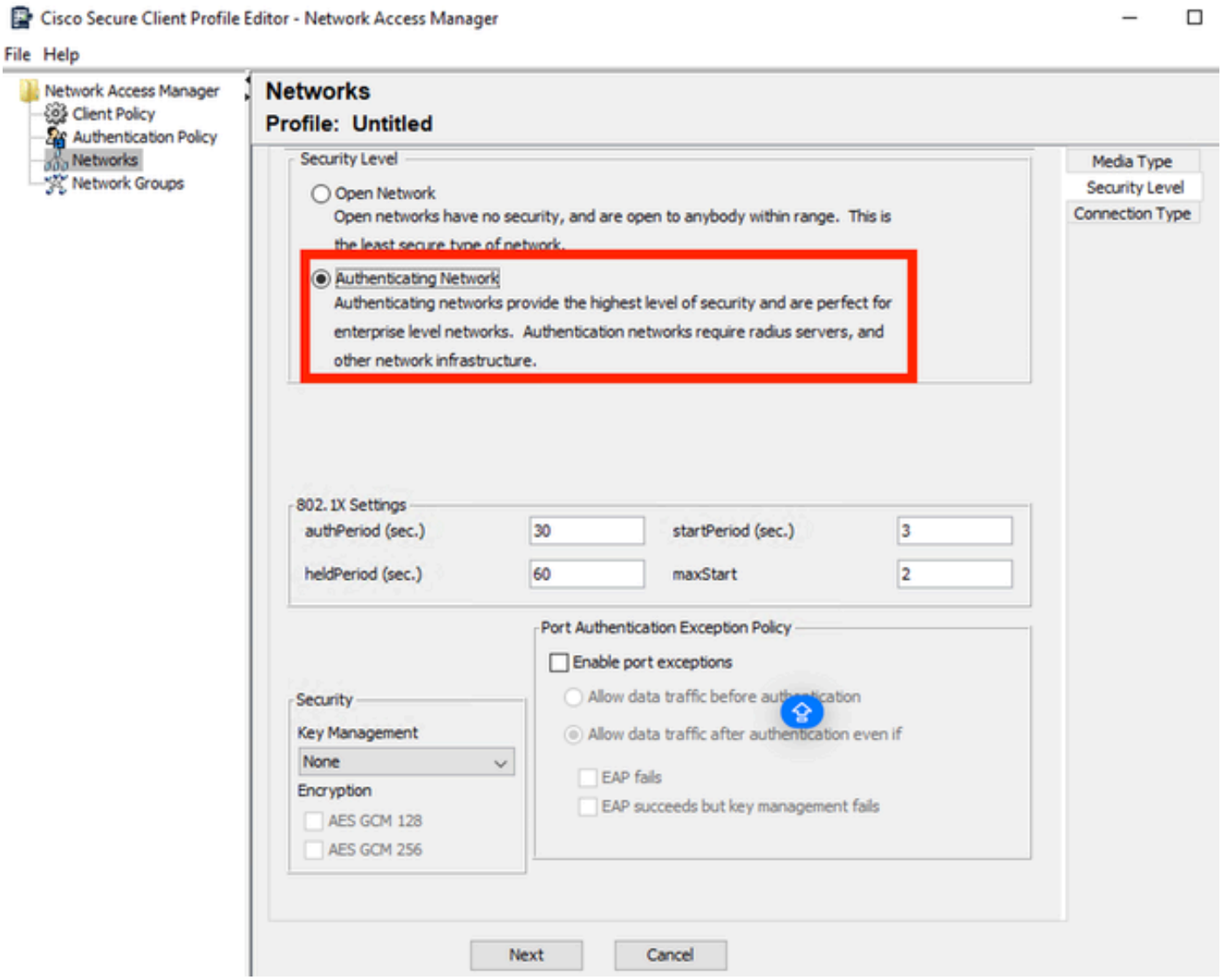
그룹 멤버십에 대해 Global을 선택합니다. Wired(유선)Network Media(네트워크 미디어)를 선택합니다.



미디어 유형 섹션

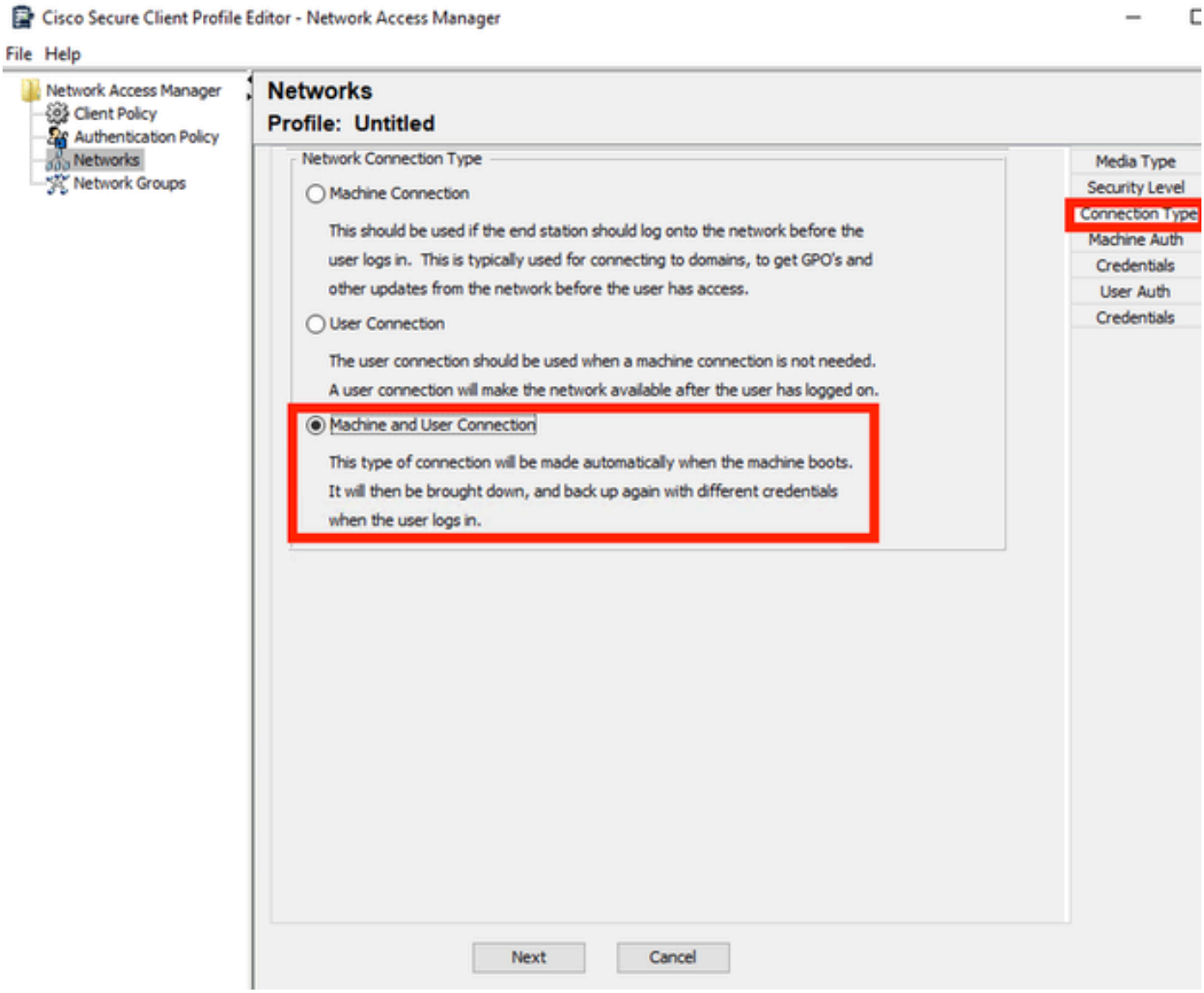
Next(다음)를 클릭합니다.

인증 네트워크를 선택하고 이 섹션의 나머지 옵션에 대한 기본값을 변경하지 마십시오.



보안 레벨 프로파일 편집기 섹션

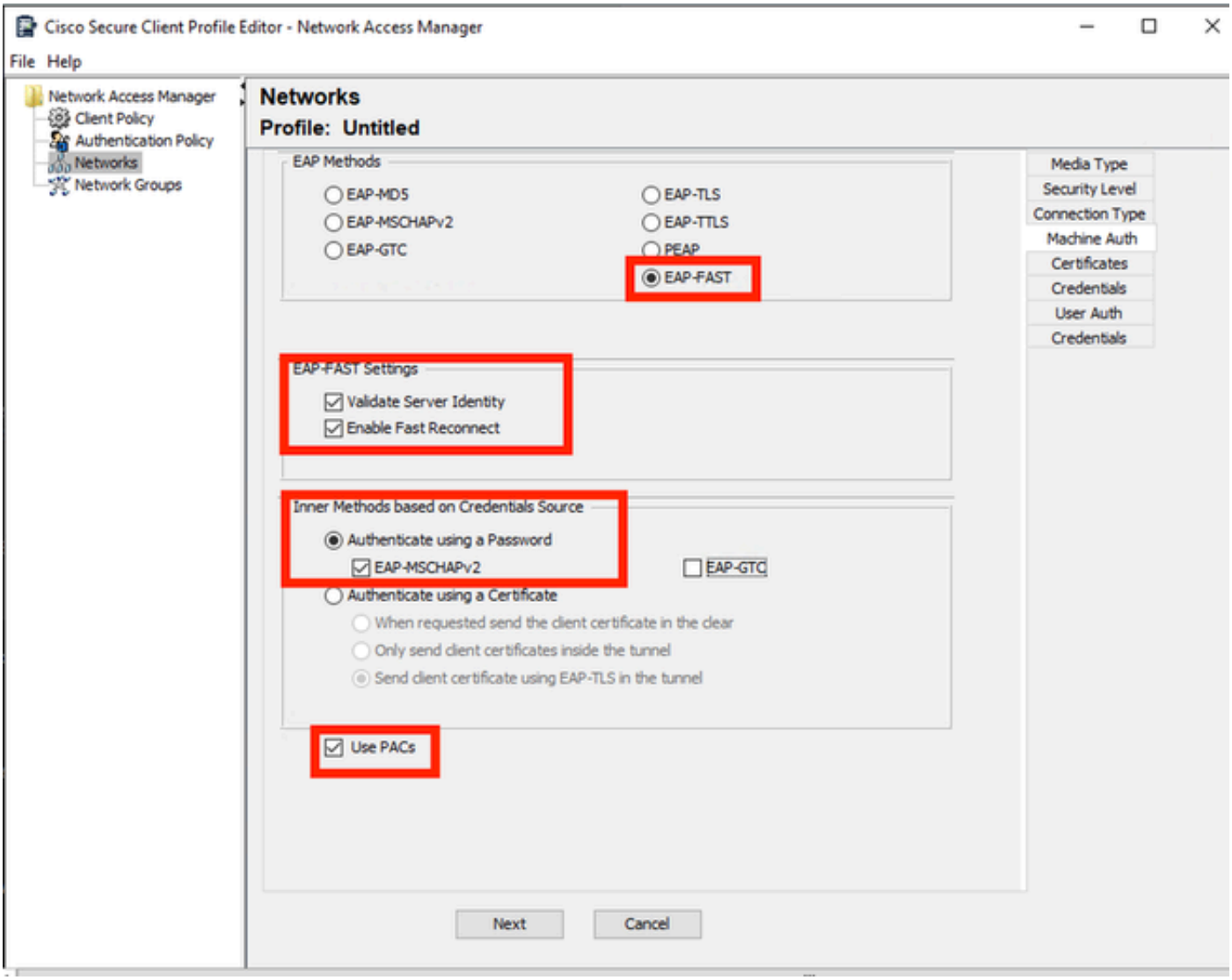
Next(다음)를 클릭하여 Connection Type(연결 유형) 섹션을 계속합니다.



연결 유형 섹션

세 번째 옵션을 선택하여 사용자 및 머신 인증을 동시에 구성합니다.

Next(다음)를 클릭합니다.

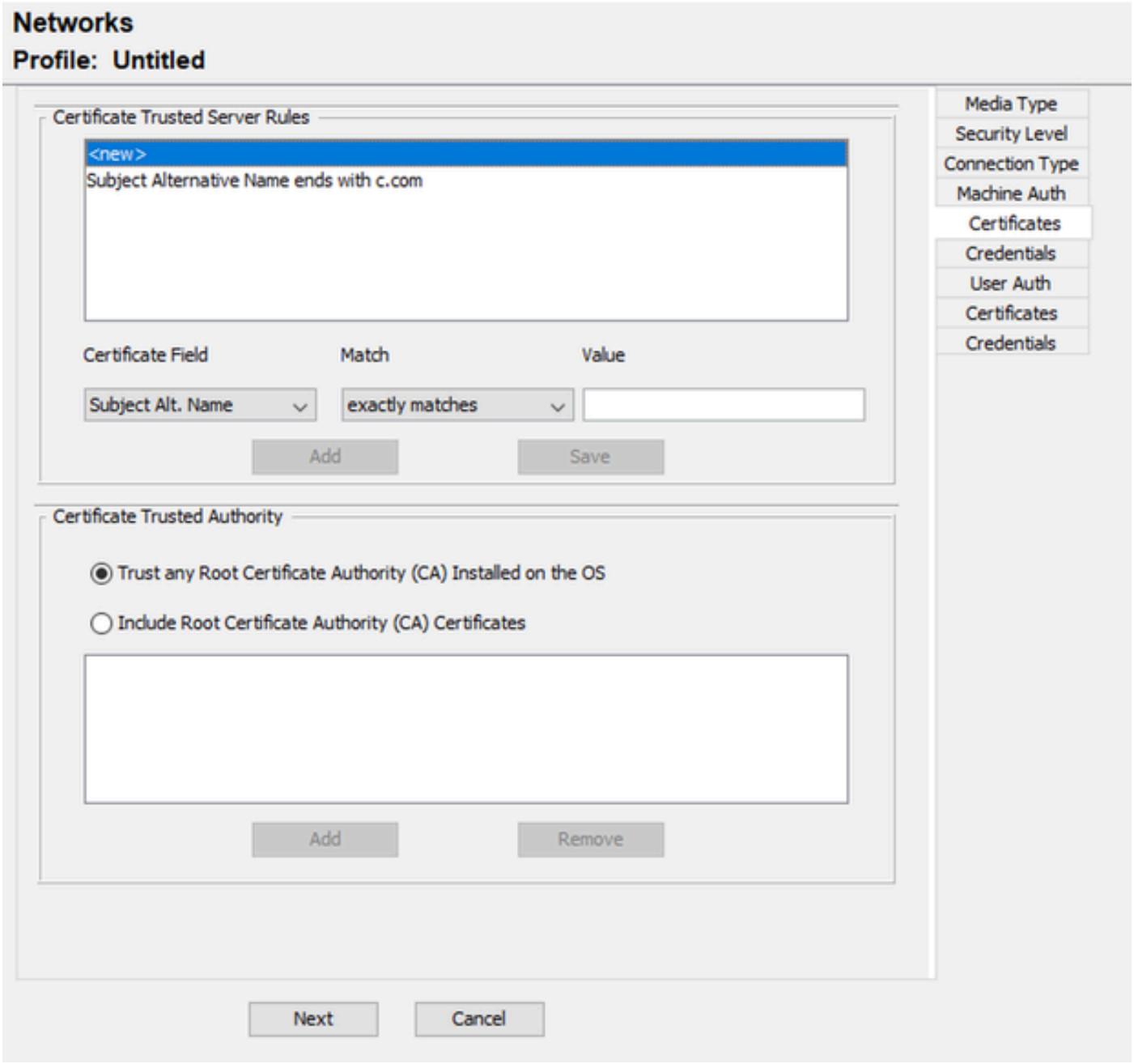


머신 인증 섹션

Machine Auth(머신 인증) 섹션에서 EAP 방법으로 EAP-FAST를 선택합니다. EAP FAST 설정 기본값을 변경하지 마십시오. Inner methods based on Credentials Source(자격 증명 소스 기반 내부 방법) 섹션에서 Authenticate using a Password(비밀번호를 사용하여 인증) 및 EAP-MSCHAPv2(EAP-MSCHAPv2를 방법으로 선택합니다. 그런 다음 Use PACs(PAC 사용) 옵션을 선택합니다.

Next(다음)를 클릭합니다.

Certificates(인증서) 섹션의 Certificate Trusted Server Rules(인증서 신뢰 서버 규칙)에서 규칙 일반 이름은 c.com으로 끝납니다. 이 섹션은 서버가 EAP PEAP 흐름 중에 사용하는 인증서를 나타냅니다. 사용자 환경에서 ISE(Identity Service Engine)를 사용하는 경우 정책 서버 노드 EAP 인증서의 일반 이름을 사용할 수 있습니다.

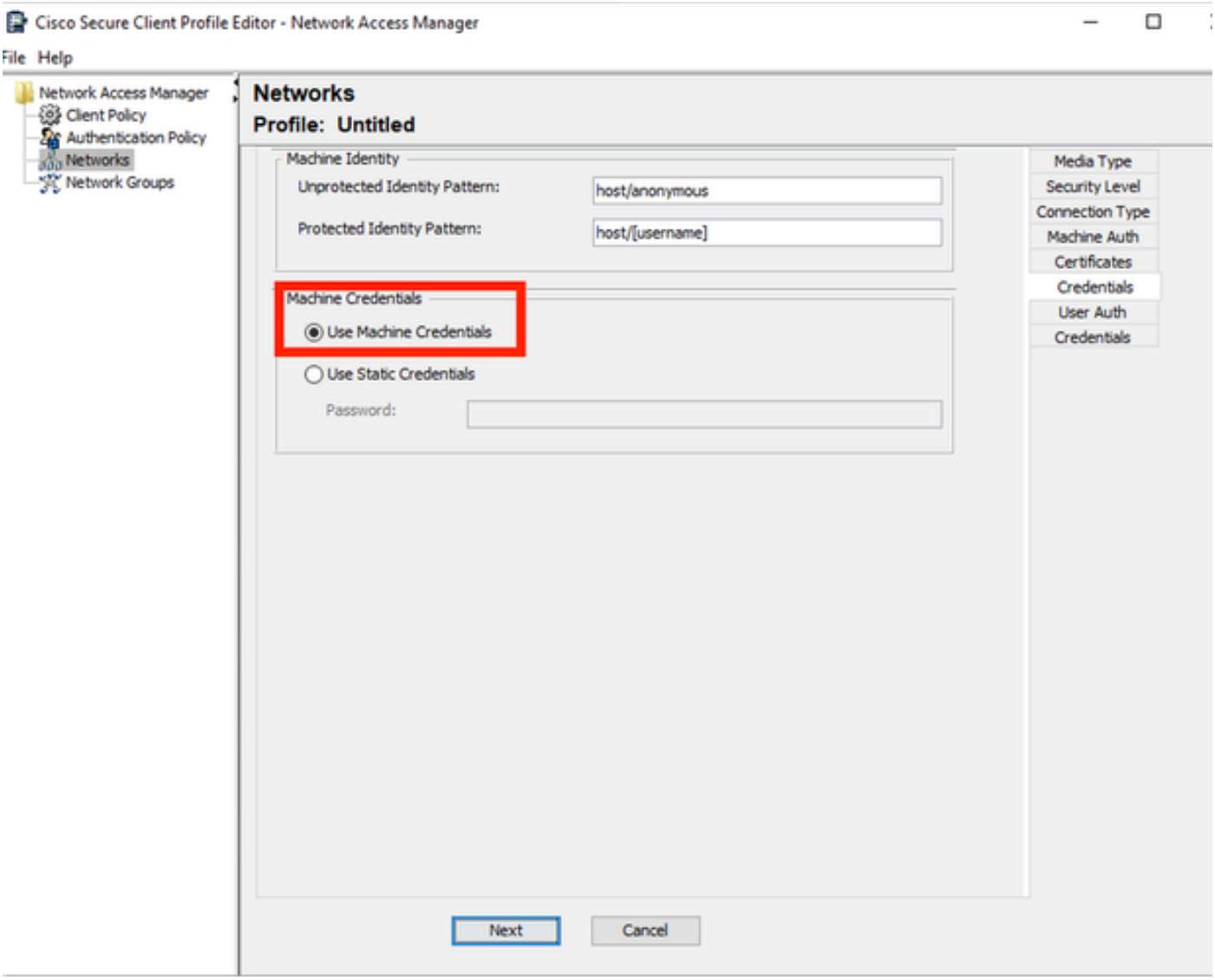


머신 인증 서버 인증서 신뢰 섹션

Certificate Trusted Authority에서 두 옵션을 선택할 수 있습니다. 이 시나리오에서는 RADIUS EAP 인증서를 서명한 특정 CA 인증서를 추가하는 대신 Trust any Root Certificate Authority (CA) Installed on the OS(OS에 설치된 모든 루트 CA 신뢰) 옵션을 사용합니다.

이 옵션을 사용하면 Windows는 Manage User Certs(사용자 인증서 관리) 프로그램에 포함된 인증서에서 서명한 모든 EAP 인증서를 신뢰합니다(Current User(현재 사용자) > Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) > Certificates(인증서)).

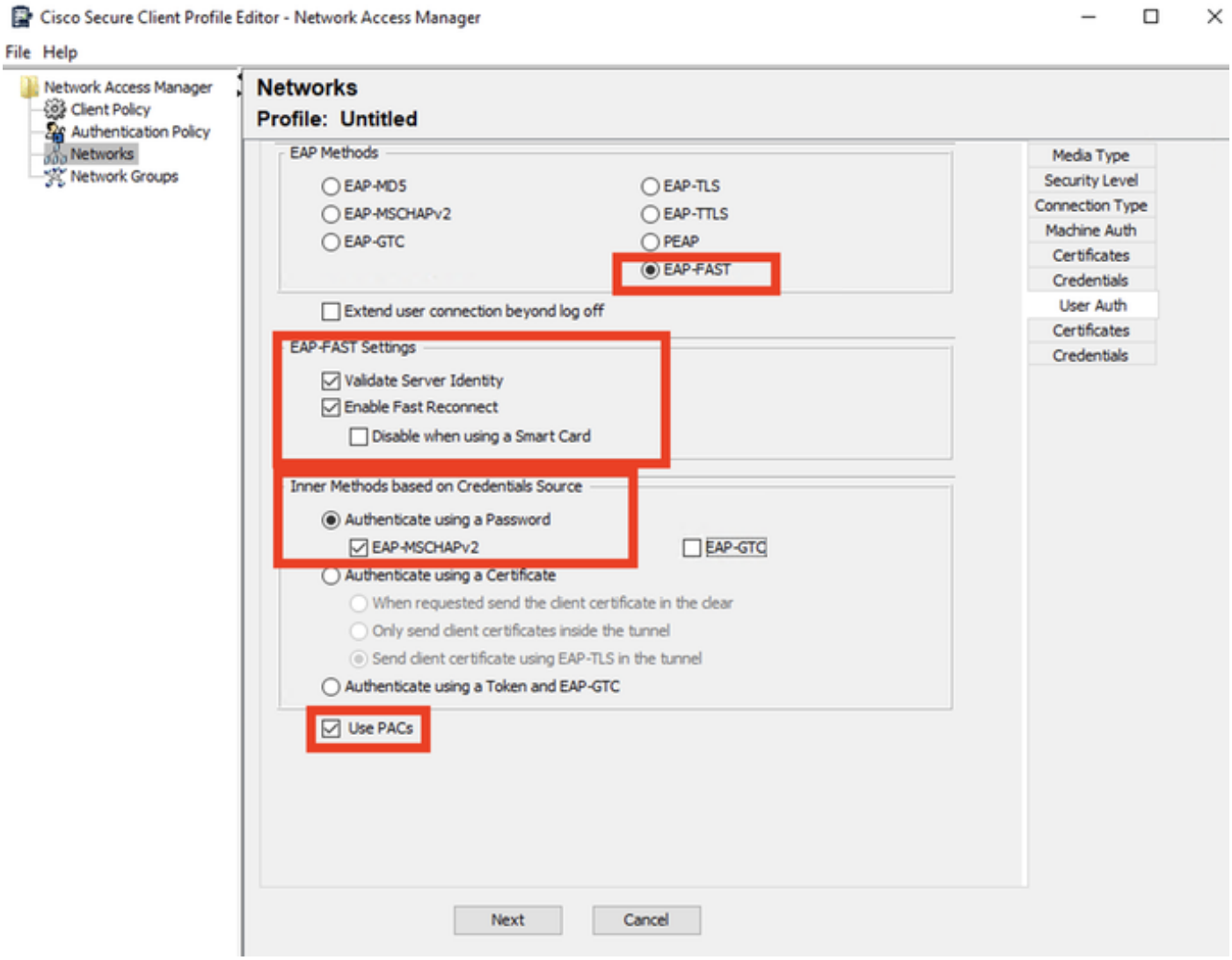
Next(다음)를 클릭합니다.



머신 인증 자격 증명 섹션

Machine Credentials(머신 자격 증명) 섹션에서 Use Machine Credentials(머신 자격 증명 사용)를 선택합니다.

Next(다음)를 클릭합니다.



사용자 인증 섹션

사용자 인증의 경우 EAP 방법으로 EAP-FAST를 선택합니다.

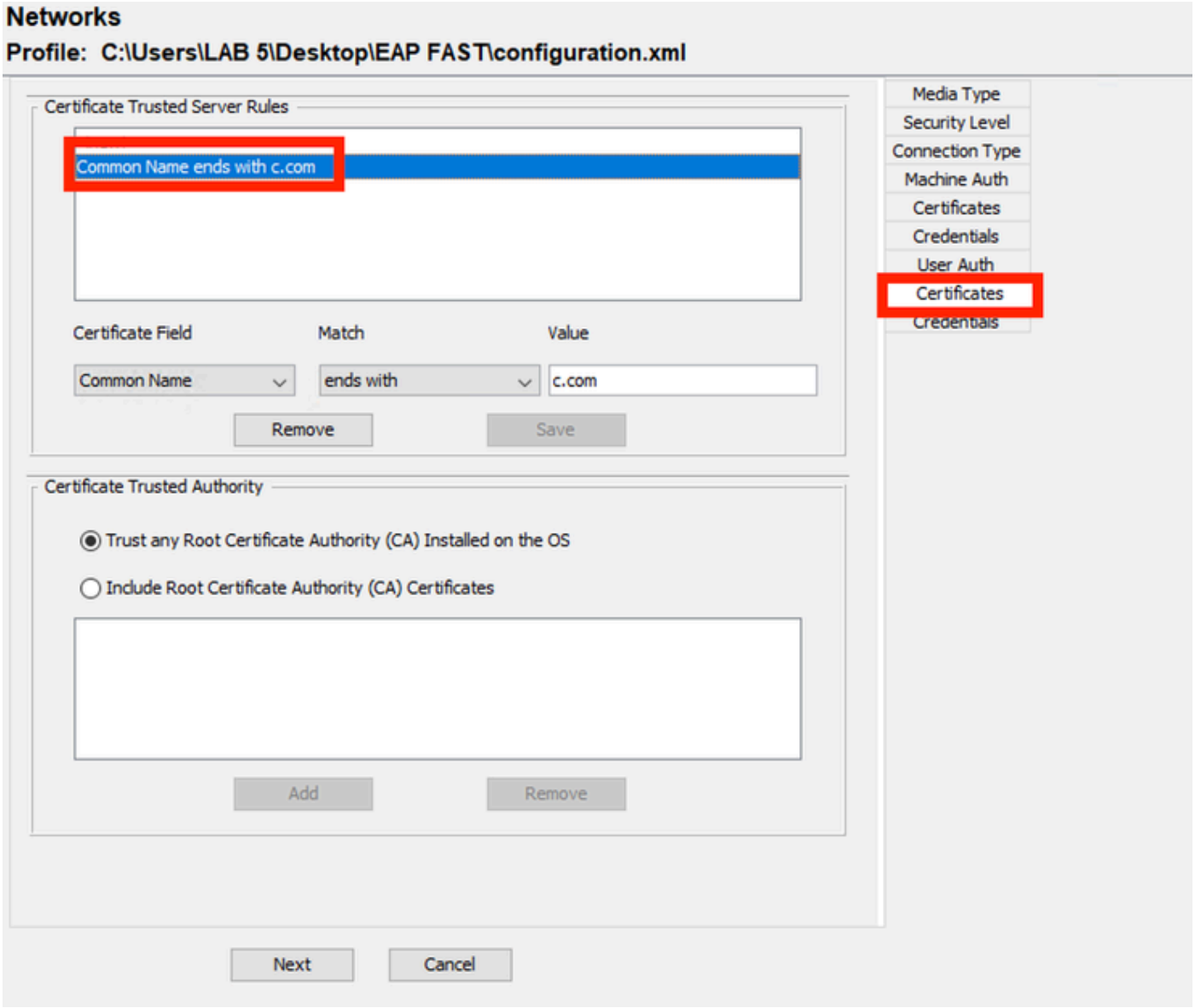
EAP-FAST 설정 섹션에서 기본값을 변경하지 마십시오.

Inner Method based on credentials source(자격 증명 소스 기반 내부 방법) 섹션의 경우 Authenticate using a Password(비밀번호를 사용하여 인증) 및 EAP-MSCHAPv2(EAP-MSCHAPv2를 방법으로 선택합니다.

Use PACs(PAC 사용)를 선택합니다.

Next(다음)를 클릭합니다.

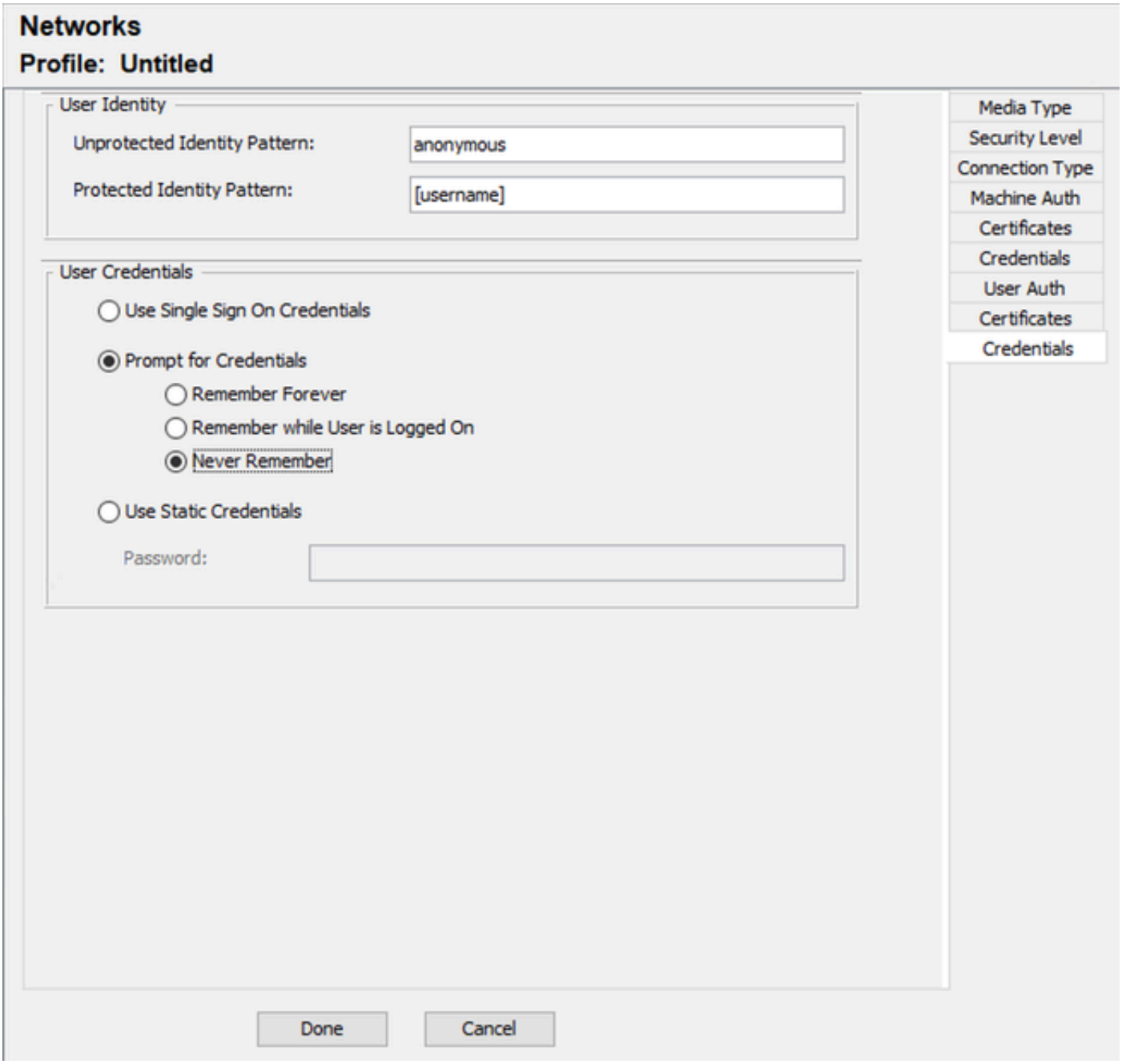
Certificates(인증서) 섹션의 Certificate Trusted Server Rules(인증서 신뢰 서버 규칙)에서 규칙은 Common Name(공통 이름)이 c.com으로 끝납니다. 이러한 컨피그레이션은 EAP PEAP 흐름 동안 서버가 사용하는 인증서에 사용됩니다. 사용자 환경에서 ISE를 사용하는 경우 정책 서버 노드 EAP 인증서의 일반 이름을 사용할 수 있습니다.



사용자 인증 서버 인증서 신뢰 섹션

Certificate Trusted Authority에서 두 옵션을 선택할 수 있습니다. 이 시나리오에서는 RADIUS EAP 인증서를 서명한 특정 CA 인증서를 추가하는 대신 Trust any Root Certificate Authority (CA) Installed on the OS(OS에 설치된 모든 루트 CA 신뢰) 옵션이 사용됩니다.

Next(다음)를 클릭합니다.



사용자 인증 자격 증명

Credentials(자격 증명) 섹션에서 User Credentials(사용자 자격 증명) 섹션만 변경됩니다.

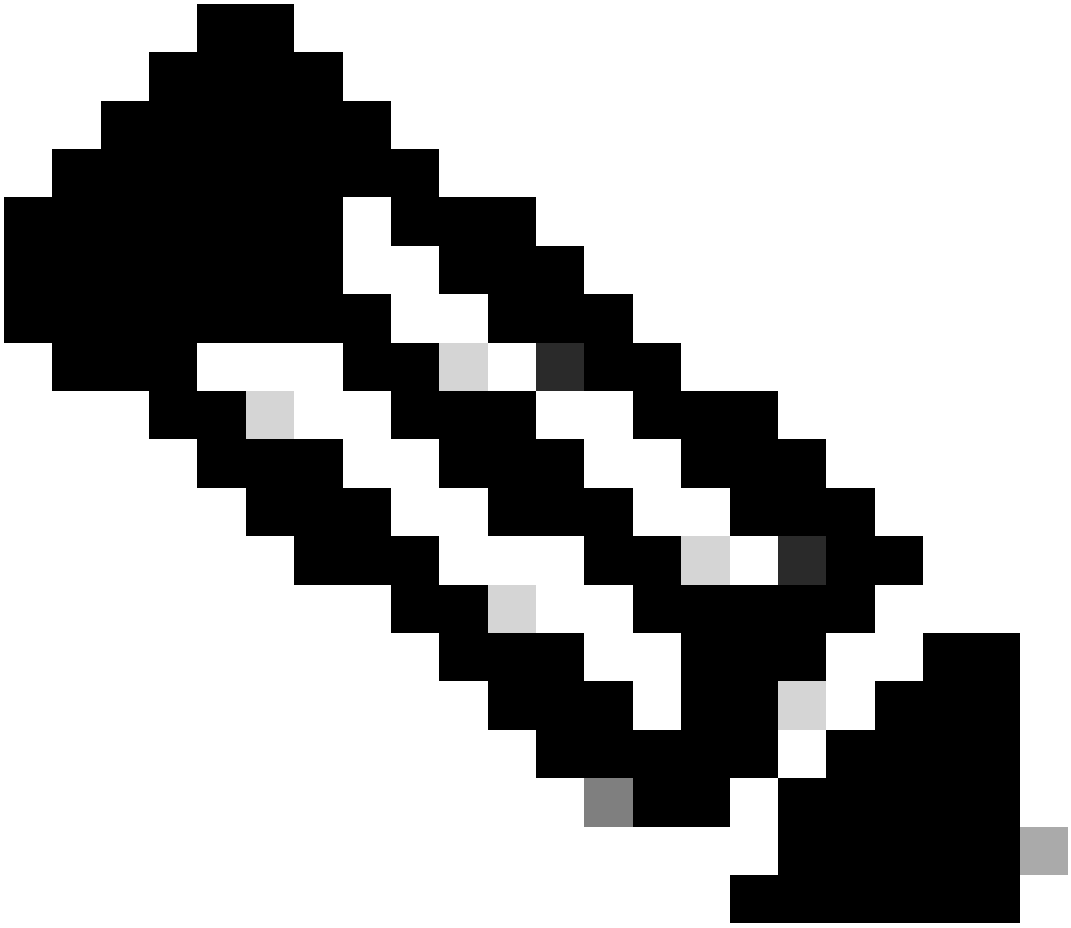
Prompt for Credentials(자격 증명 프롬프트) > Never Remember(기억 안 함) 옵션이 선택됩니다. 따라서 각 인증에서 사용자 인증은 자격 증명을 입력해야 합니다.

Done(완료) 버튼을 클릭합니다.

File(파일) > Save as(다른 이름으로 저장)를 선택하고 Secure Client Network Access Manager 프로파일을 configuration.xml로 저장합니다.

Secure Client Network Access Manager에서 방금 만든 프로파일을 사용하도록 하려면 다음 디렉토리의 configuration.xml 파일을 새 디렉토리로 바꿉니다.

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



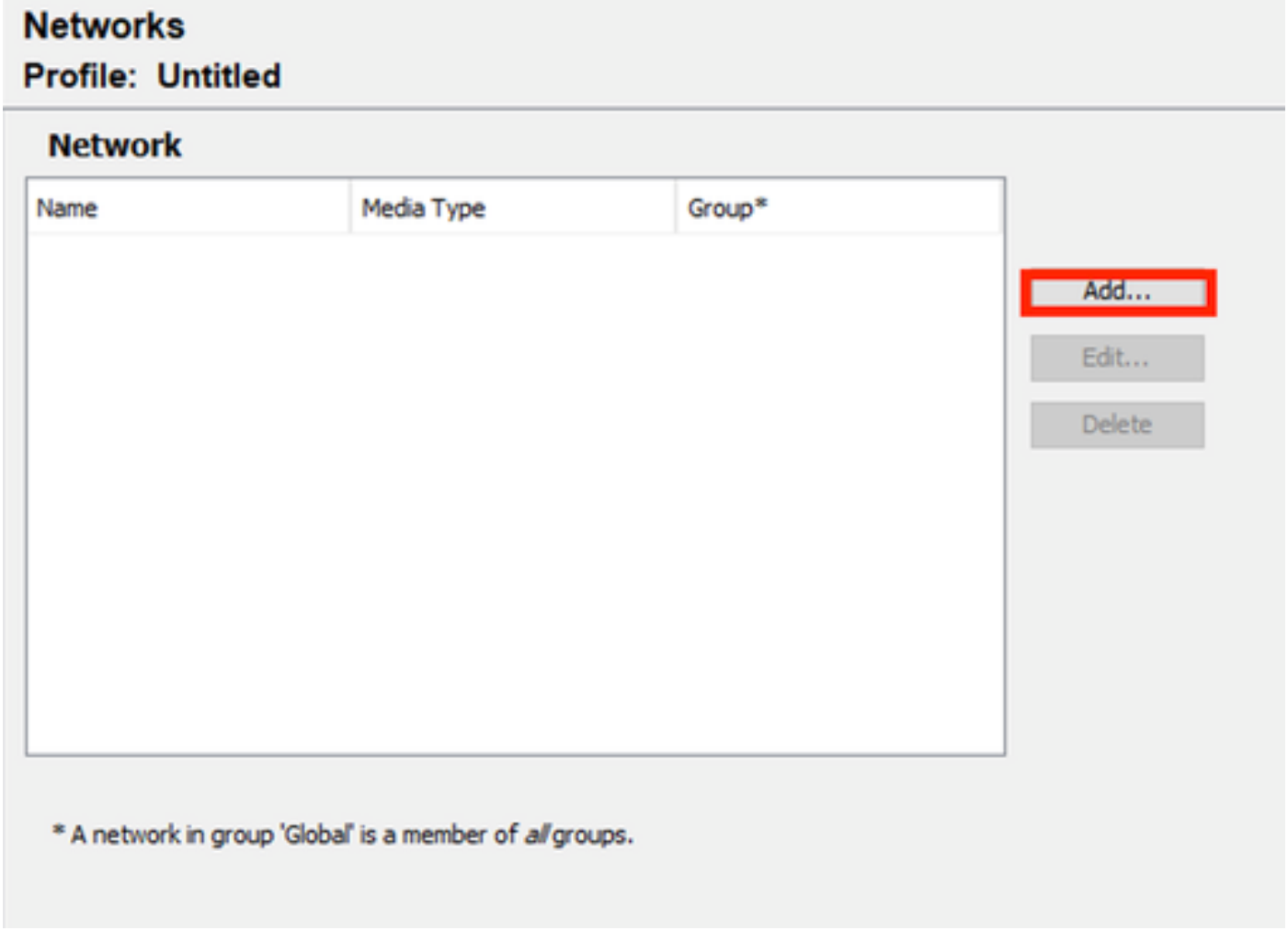
참고: 파일의 이름은 configuration.xml이어야 합니다. 그렇지 않으면 파일이 작동하지 않습니다.

---

6. 시나리오 3: EAP TLS 사용자 인증서 인증을 위한 보안 클라이언트 NAM 신청자 구성

NAM 프로파일 편집기를 열고 네트워크 섹션으로 이동합니다.

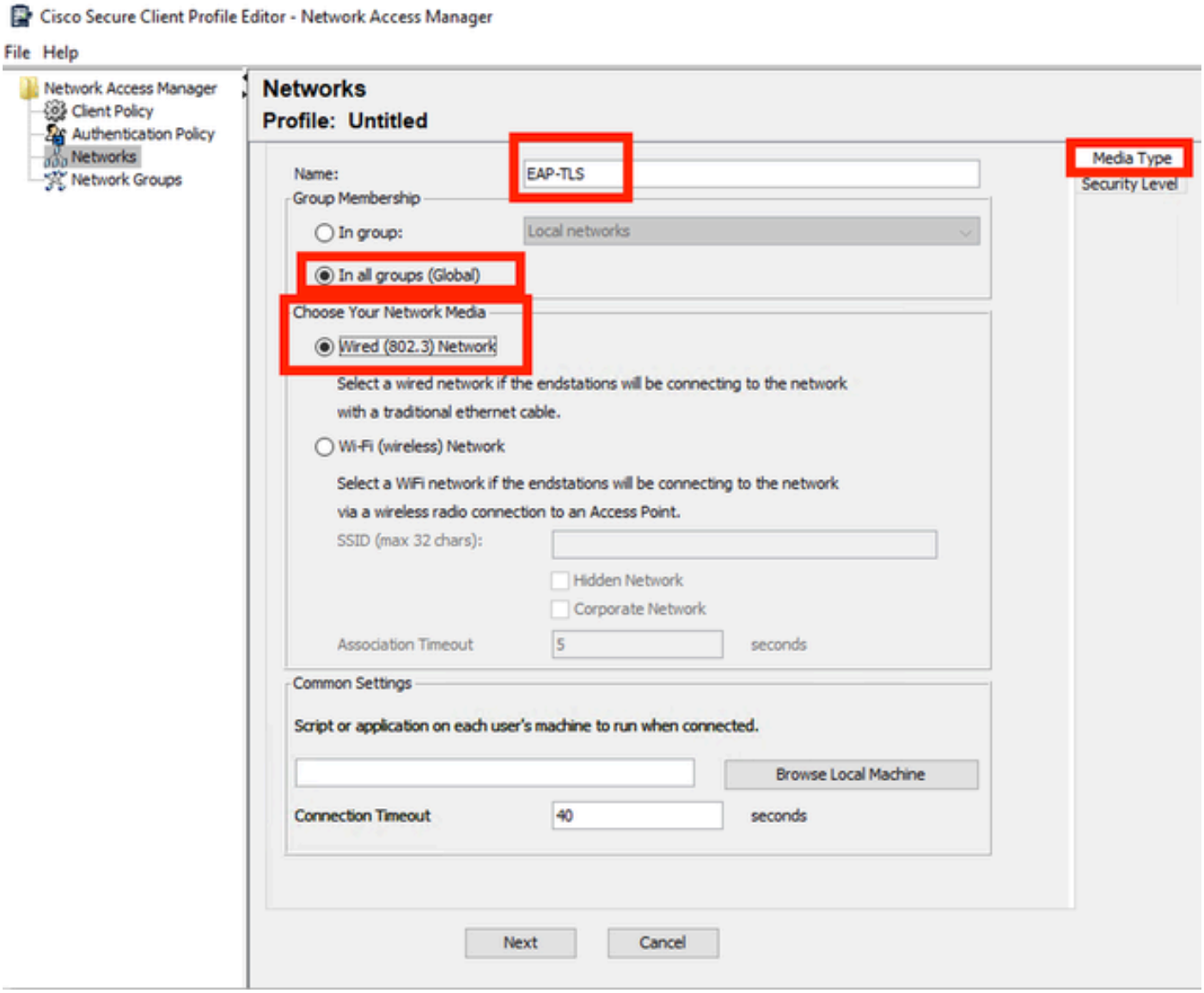
Add(추가)를 클릭합니다.



네트워크 생성 섹션

네트워크 프로필의 이름을 지정합니다. 이 경우 명명된 이름은 이 시나리오에 사용된 EAP 프로토콜과 함께 지정됩니다.

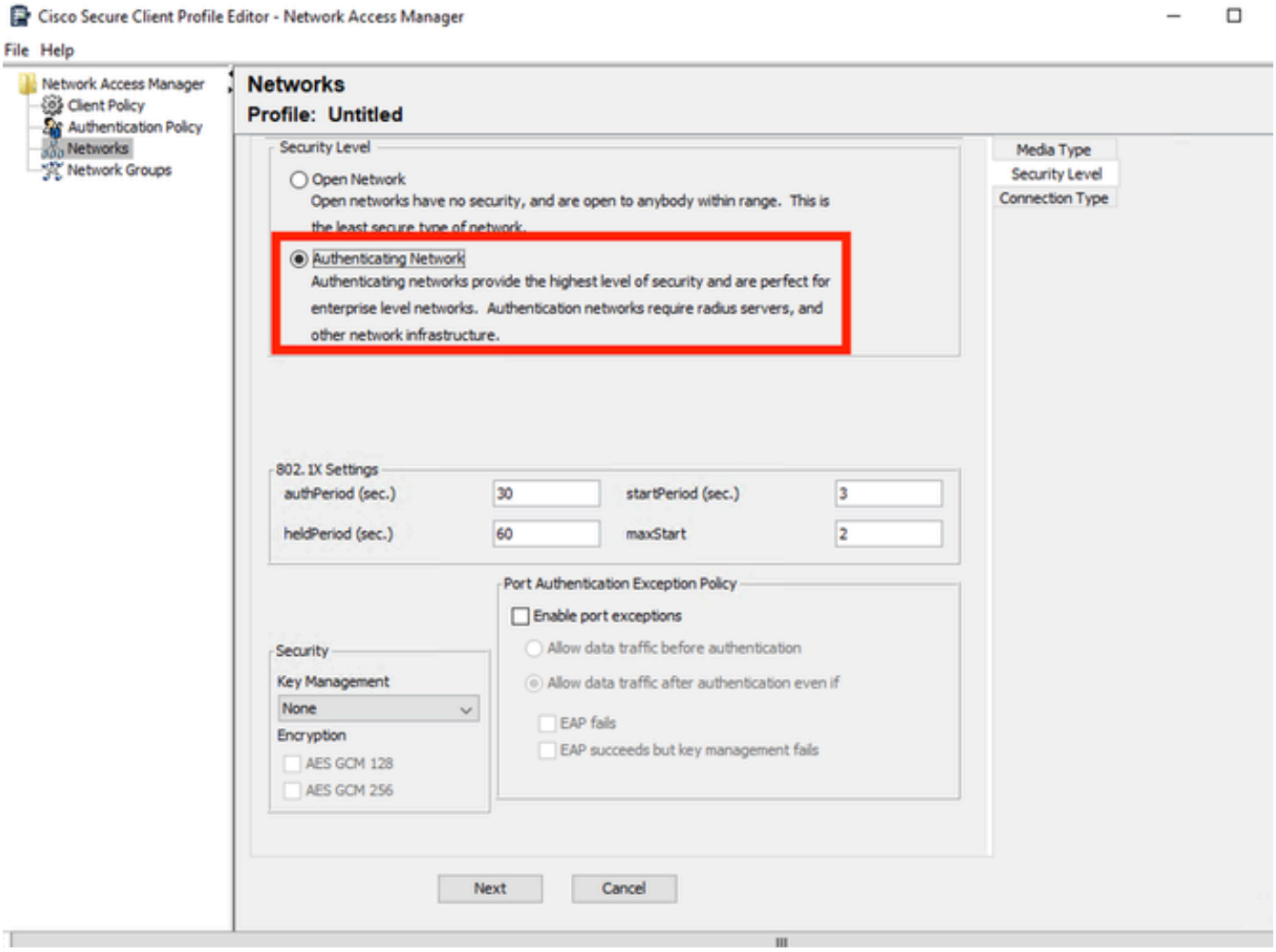
그룹 멤버십에 대해 Global을 선택합니다. 그리고 유선 네트워크 미디어.



미디어 유형 섹션

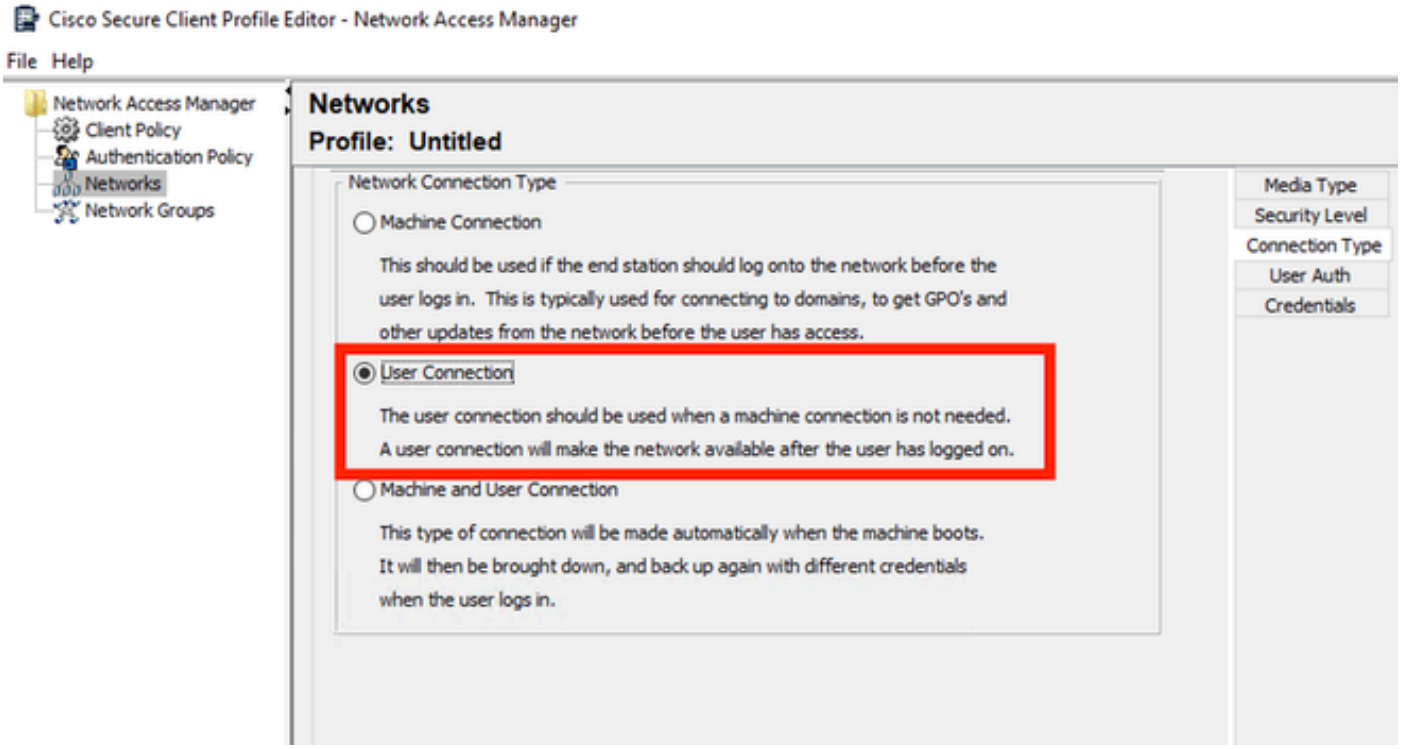
Next(다음)를 클릭합니다.

인증 네트워크를 선택하고 보안 레벨 섹션의 나머지 옵션에 대한 기본값을 변경하지 마십시오.



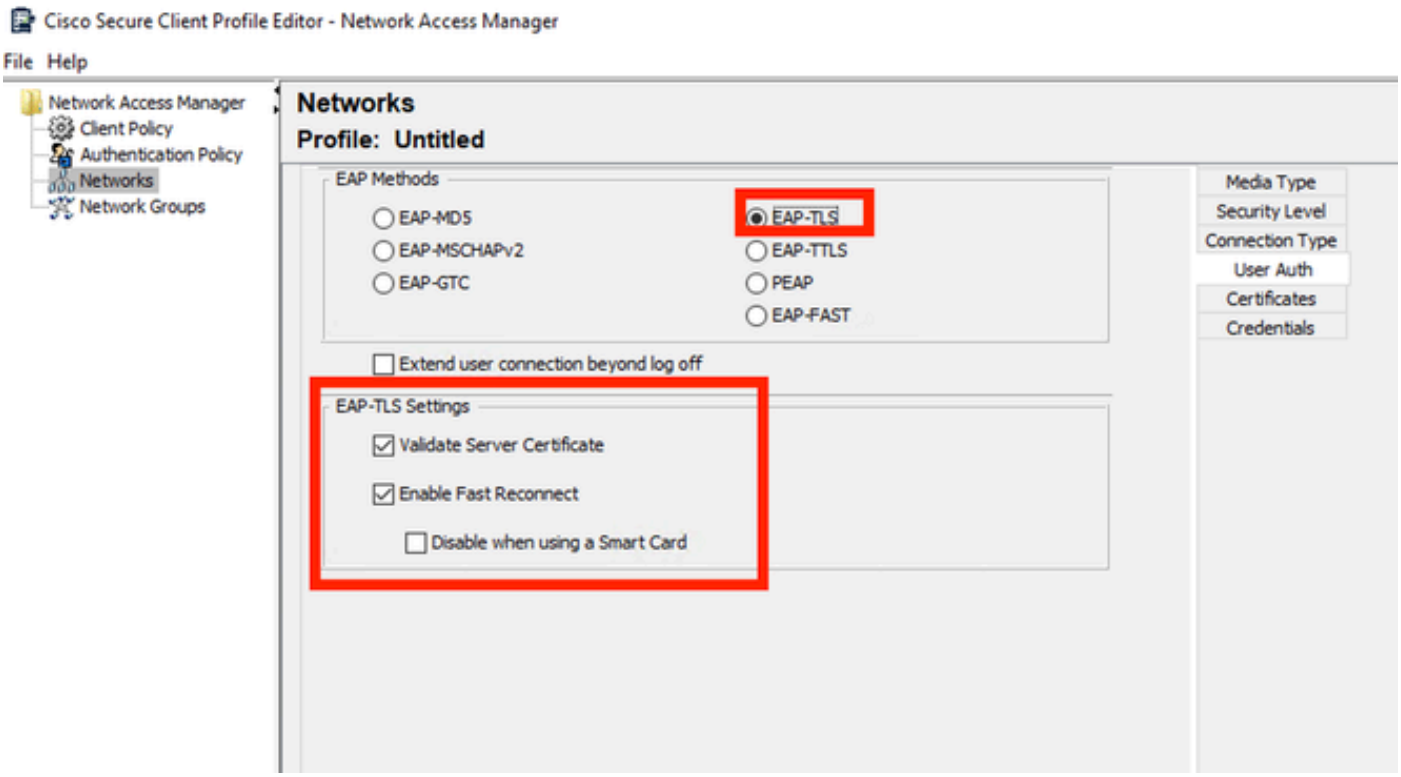
보안 수준

이 시나리오는 인증서를 사용하는 사용자 인증을 위한 것입니다. 따라서 User Connection(사용자 연결) 옵션이 사용됩니다.



연결 유형

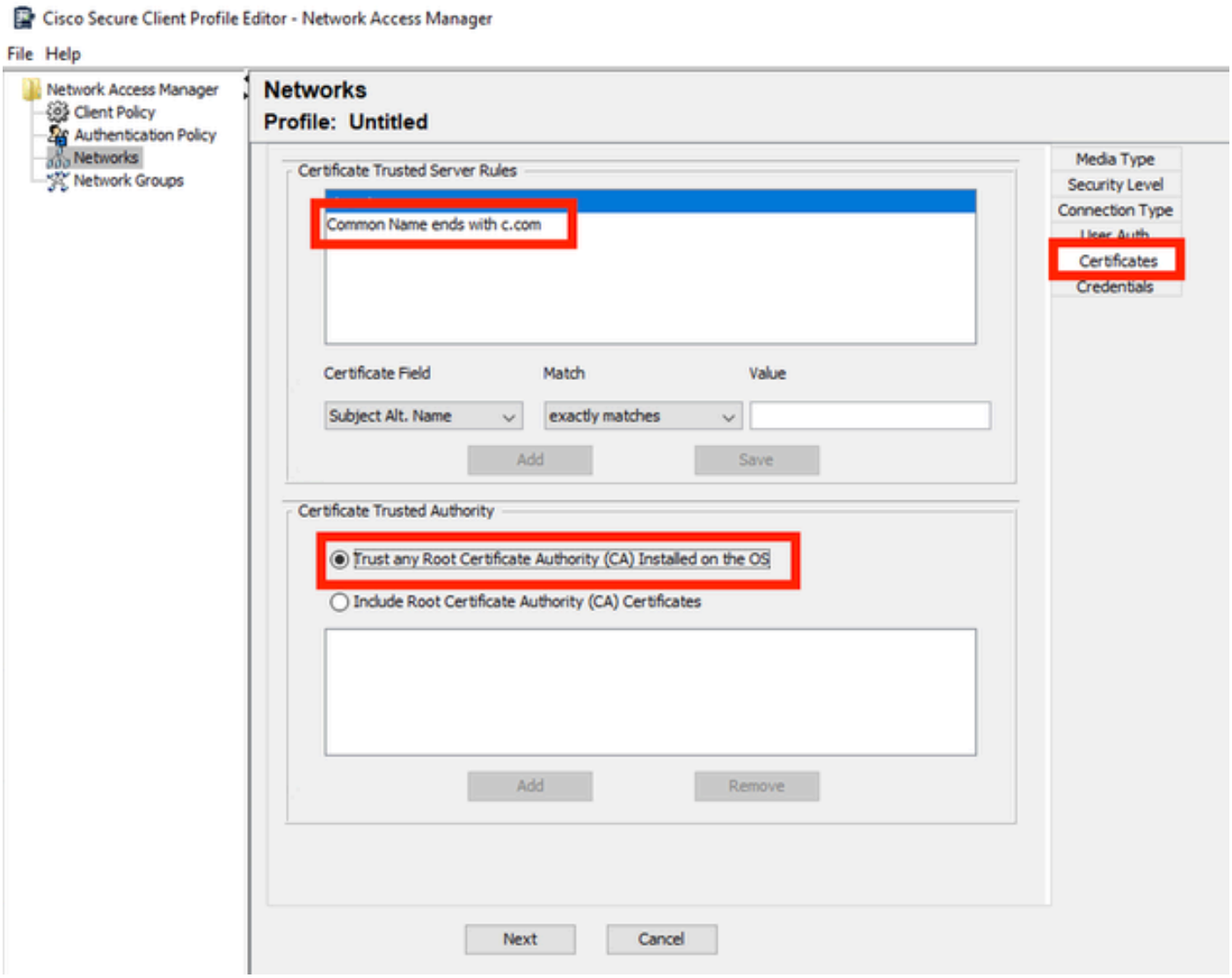
EAP 방법으로 EAP-TLS를 구성합니다. EAP-TLS 설정 섹션에서 기본값을 변경하지 마십시오.



사용자 인증 섹션

Certificates 섹션에서 AAA EAP-TLS 인증서와 일치하는 규칙을 생성합니다. ISE를 사용 중인 경우 Administration(관리) > System(시스템) > Certificates(인증서) 섹션에서 이 규칙을 찾습니다.

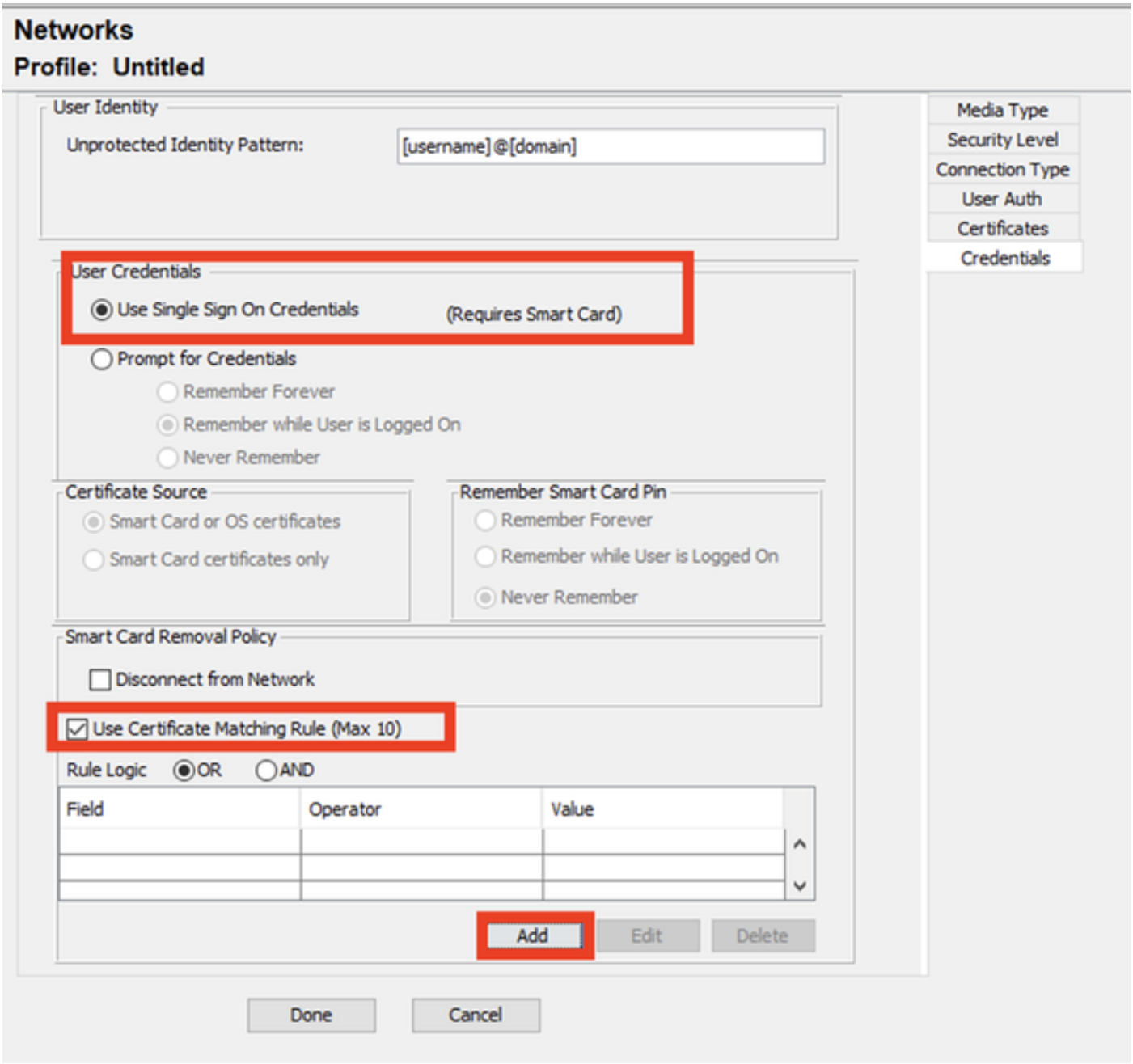
Certificate Trusted Authority(인증서 신뢰 기관) 섹션에서 OS에 설치된 모든 루트 CA(Certificate Authority) 신뢰를 선택합니다.



사용자 인증 서버 인증서 신뢰 설정

Next(다음)를 클릭합니다.

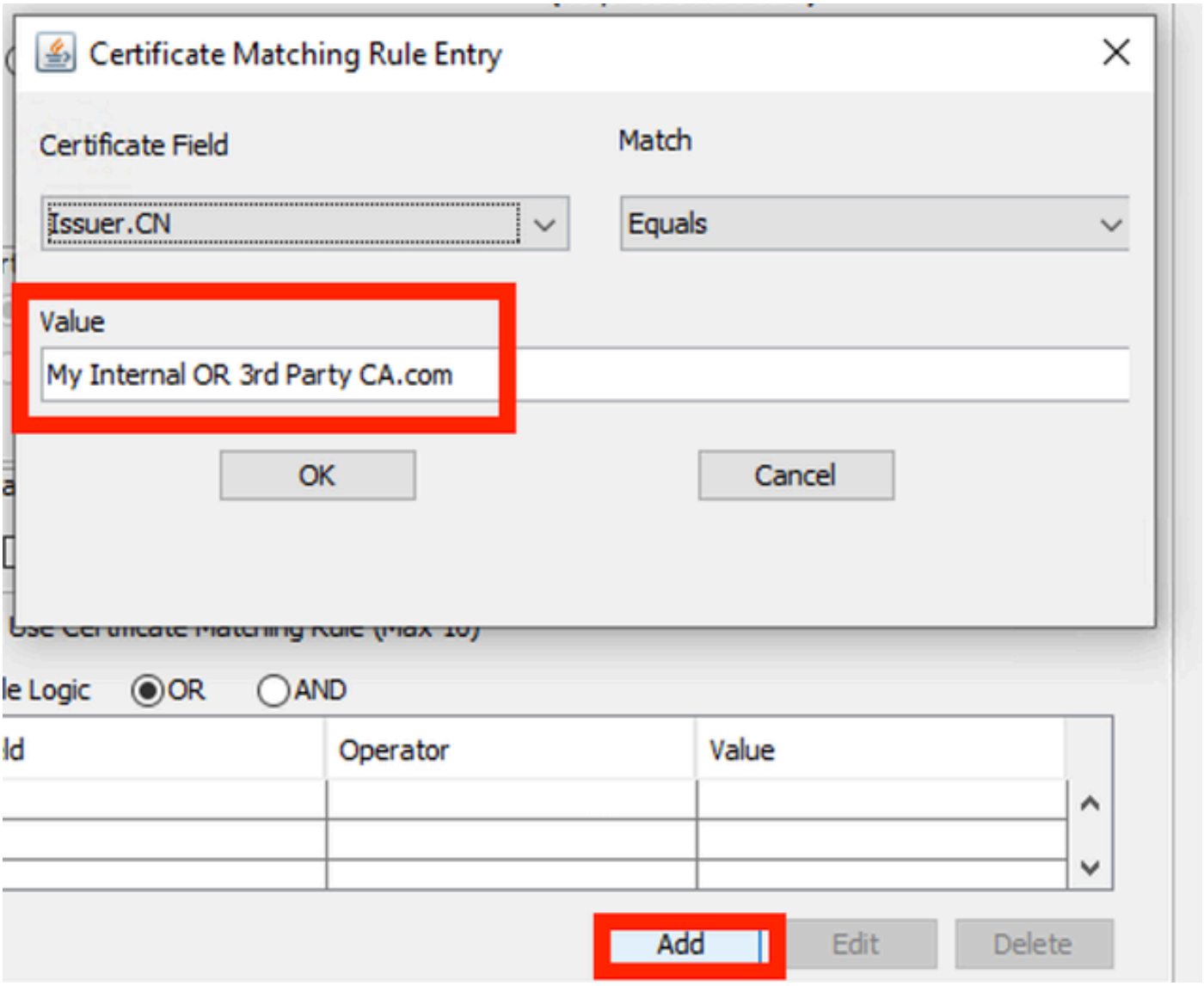
User Credentials(사용자 자격 증명) 섹션의 경우 첫 번째 부분의 기본값을 변경하지 마십시오.



사용자 인증 자격 증명 섹션

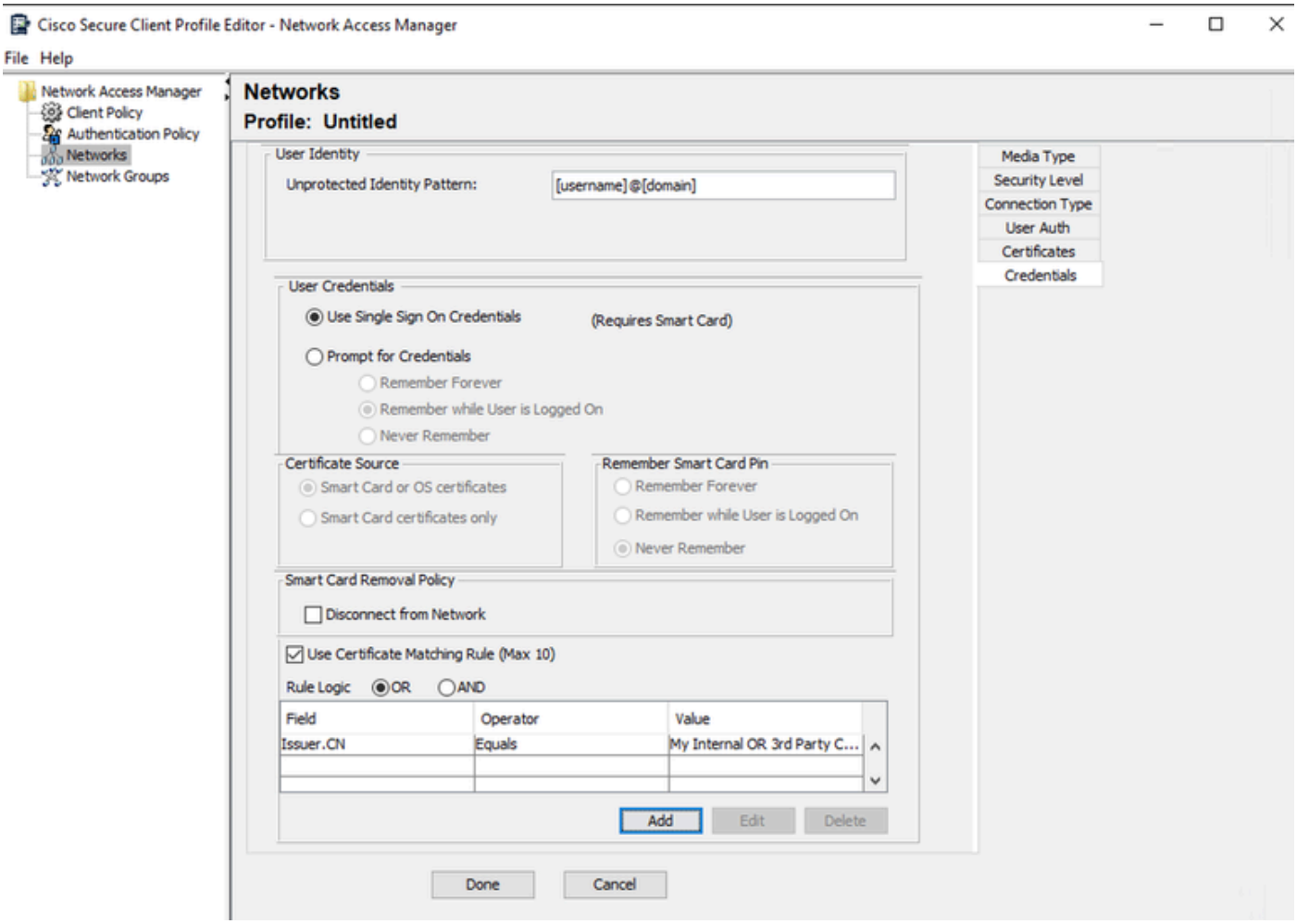
EAP TLS 프로세스 중에 사용자가 보내는 ID 인증서와 일치하는 규칙을 구성하는 것이 중요합니다. 이렇게 하려면 Use Certificate Matching Rule (Max 10)(인증서 일치 규칙 사용(최대 10)) 옆에 있는 확인란을 클릭합니다.

Add(추가)를 클릭합니다.



인증서 일치 규칙 창

My Internal 또는 서드파티 CA.com 문자열 값을 사용자 인증서의 CN으로 바꿉니다.



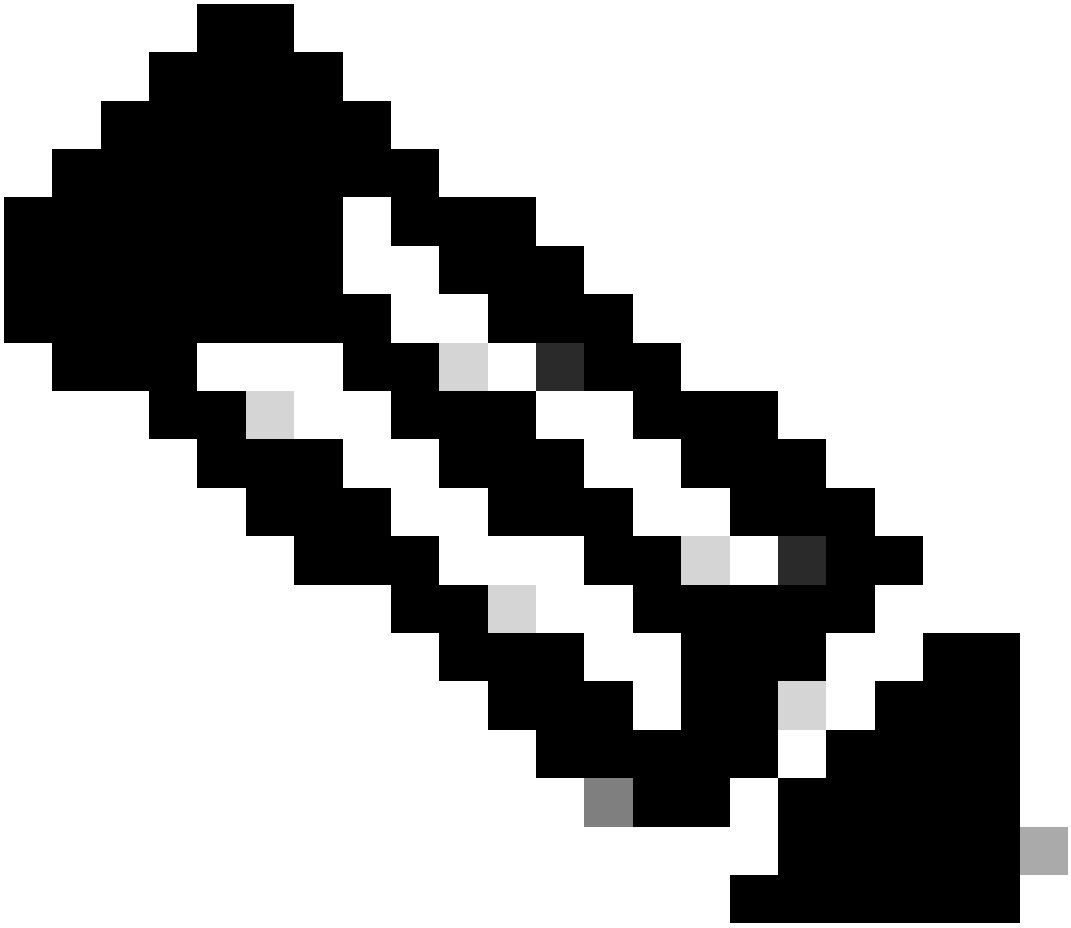
사용자 인증 인증서 자격 증명 섹션

Done(완료)을 클릭하여 컨피그레이션을 완료합니다.

Secure Client Network Access Manager 프로파일을 configuration.xml로 저장하려면 File(파일) > Save as(다른 이름으로 저장)를 선택합니다.

Secure Client Network Access Manager에서 방금 만든 프로파일을 사용하도록 하려면 다음 디렉토리의 configuration.xml 파일을 새 디렉토리로 바꿉니다.

C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\system



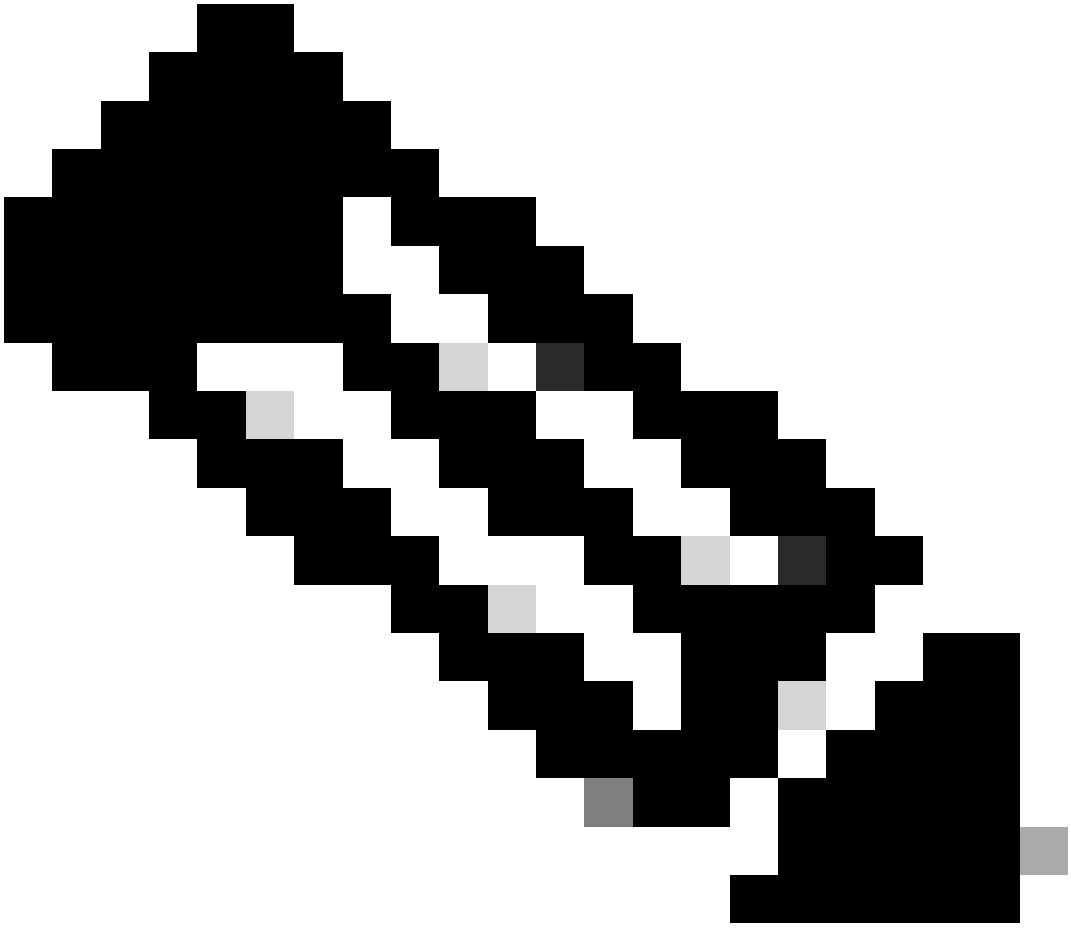
참고: 파일의 이름은 configuration.xml이어야 합니다. 그렇지 않으면 파일이 작동하지 않습니다.

---

7. 시나리오 1 PEAP MSCHAPv2를 기반으로 인증을 허용하도록 ISR 1100 및 ISE를 구성합니다

ISR 1100 라우터를 구성합니다.

이 섹션에서는 NAD가 dot1x를 작동하게 하기 위해 갖추어야 하는 기본 컨피그레이션에 대해 설명합니다.



참고: 다중 노드 ISE 구축의 경우 정책 서버 노드 페르소나가 활성화된 노드를 가리킵니다. 이는 Administration(관리) > System(시스템) > Deployment(구축) 탭에서 ISE로 이동하여 확인할 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>
```

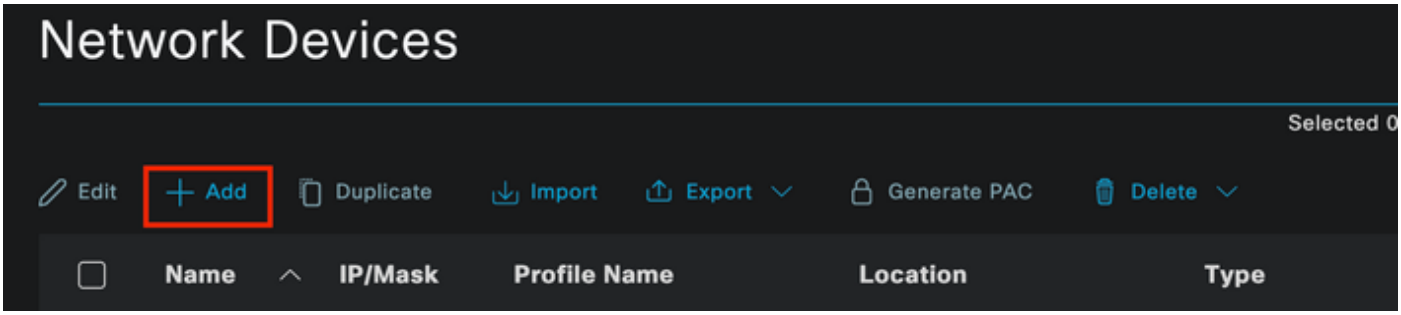
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication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

Identity Service Engine 3.2를 구성합니다.

네트워크 디바이스를 구성합니다.

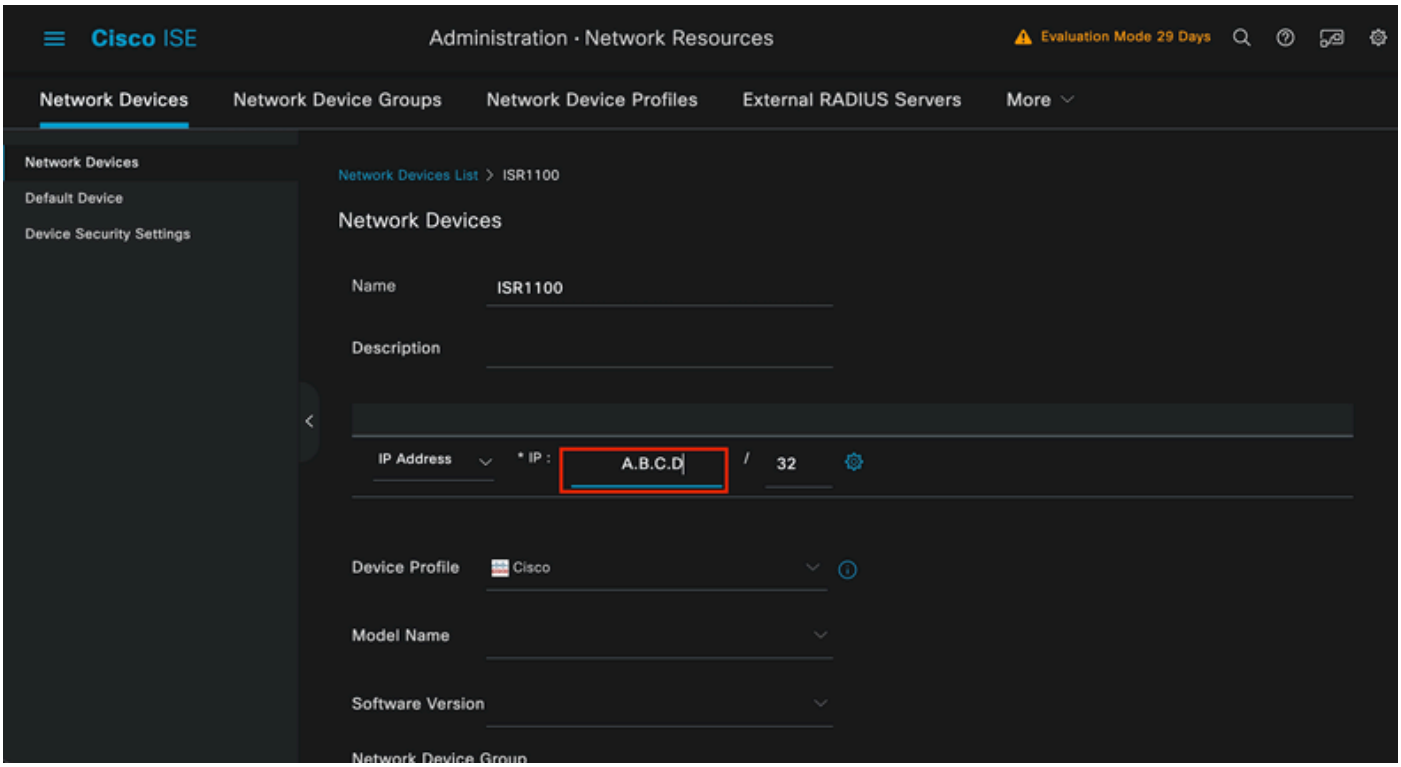
ISR NAD를 ISE Administration(ISE 관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)에 추가합니다.

Add(추가)를 클릭합니다.



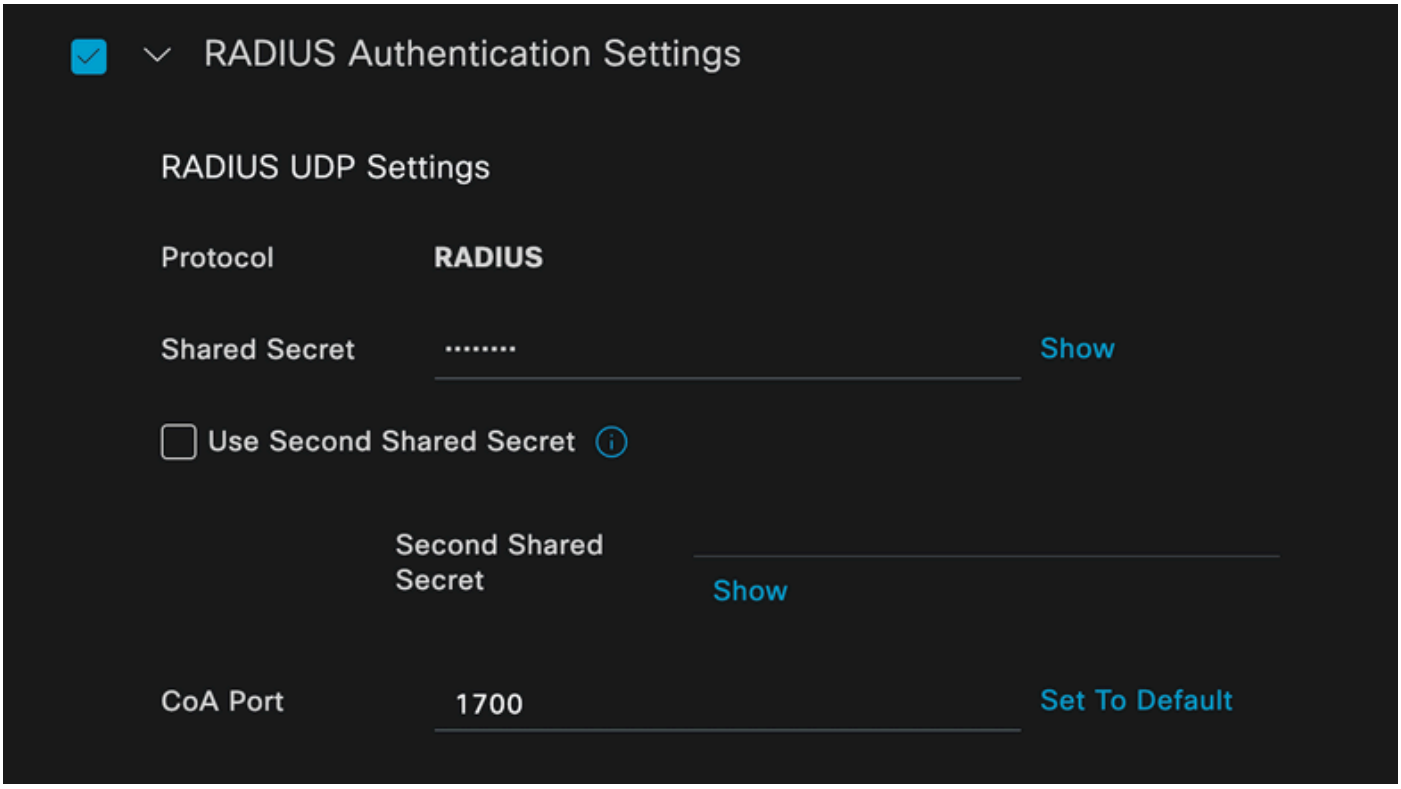
네트워크 장치 섹션

생성 중인 NAD에 이름을 할당합니다. 네트워크 디바이스 IP를 추가합니다.



네트워크 디바이스 생성

같은 페이지의 하단에서 네트워크 디바이스 컨피그레이션에서 사용한 것과 동일한 공유 암호를 추가합니다.



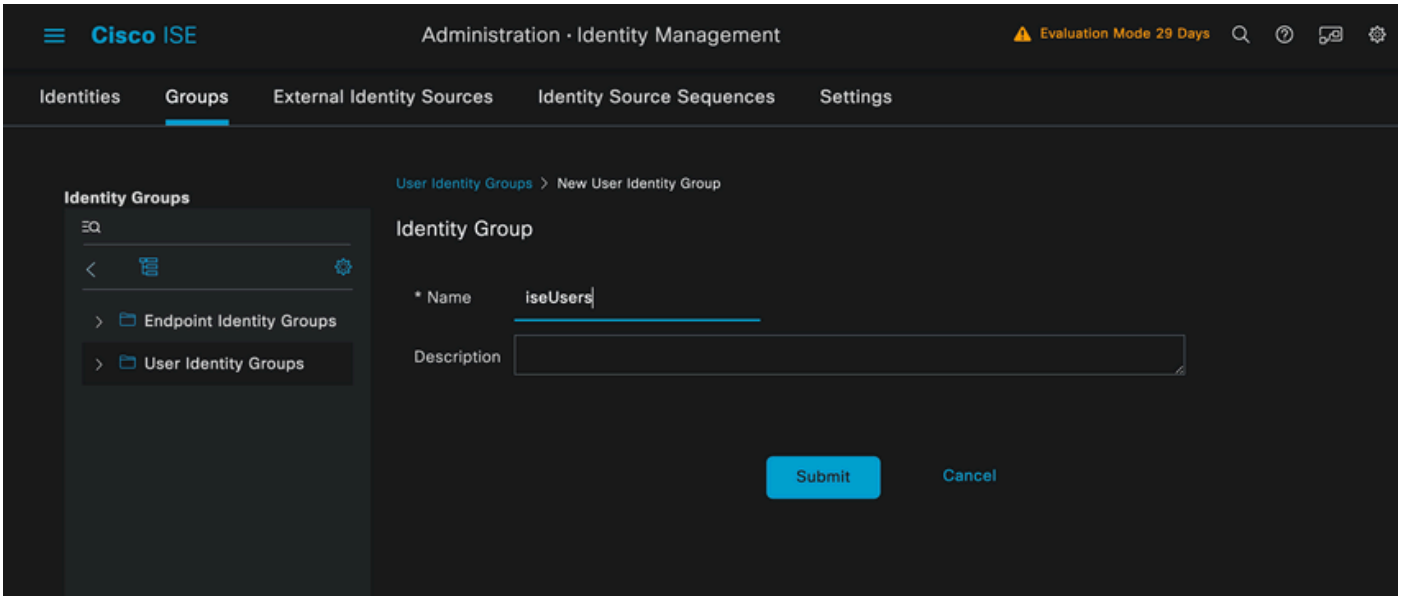
네트워크 디바이스 *Radius* 설정

변경 사항을 저장합니다.

엔드포인트를 인증하는 데 사용되는 ID를 구성합니다.

ISE 로컬 인증이 사용됩니다. 이 문서에서는 외부 ISE 인증에 대해 설명하지 않습니다.

Administration(관리) > Identity Management(ID 관리) > Groups(그룹) 탭으로 이동하여 사용자가 속한 그룹을 생성합니다. 이 데모를 위해 생성된 ID 그룹은 iseUsers입니다.

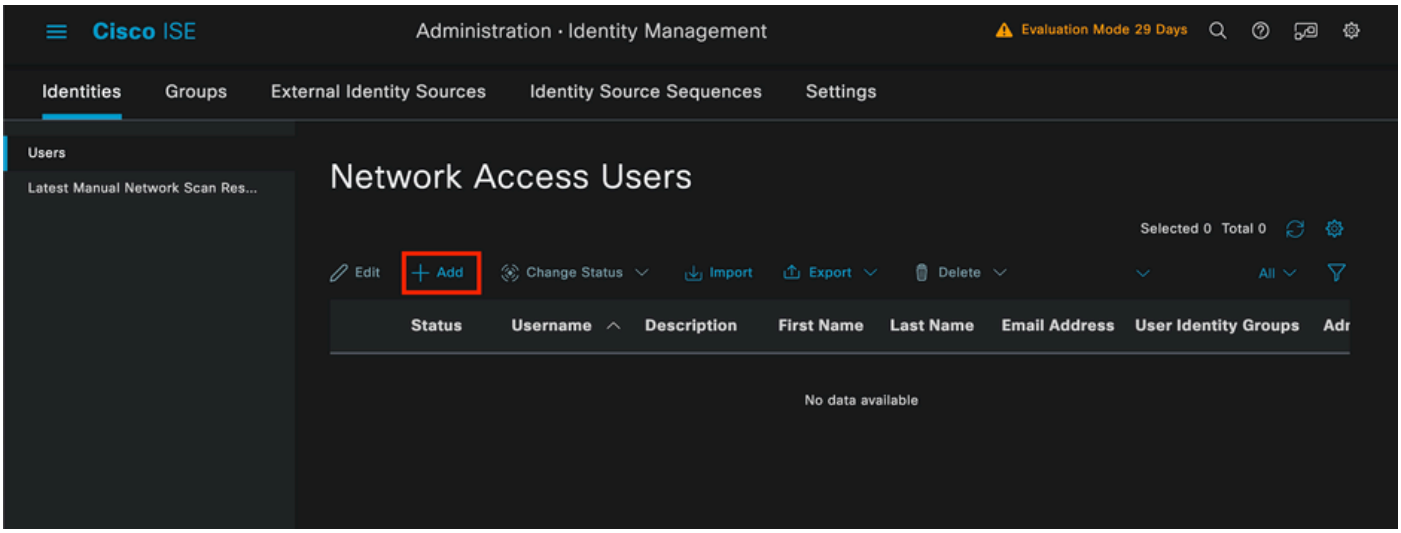


ID 그룹 생성

Submit(제출)을 클릭합니다.

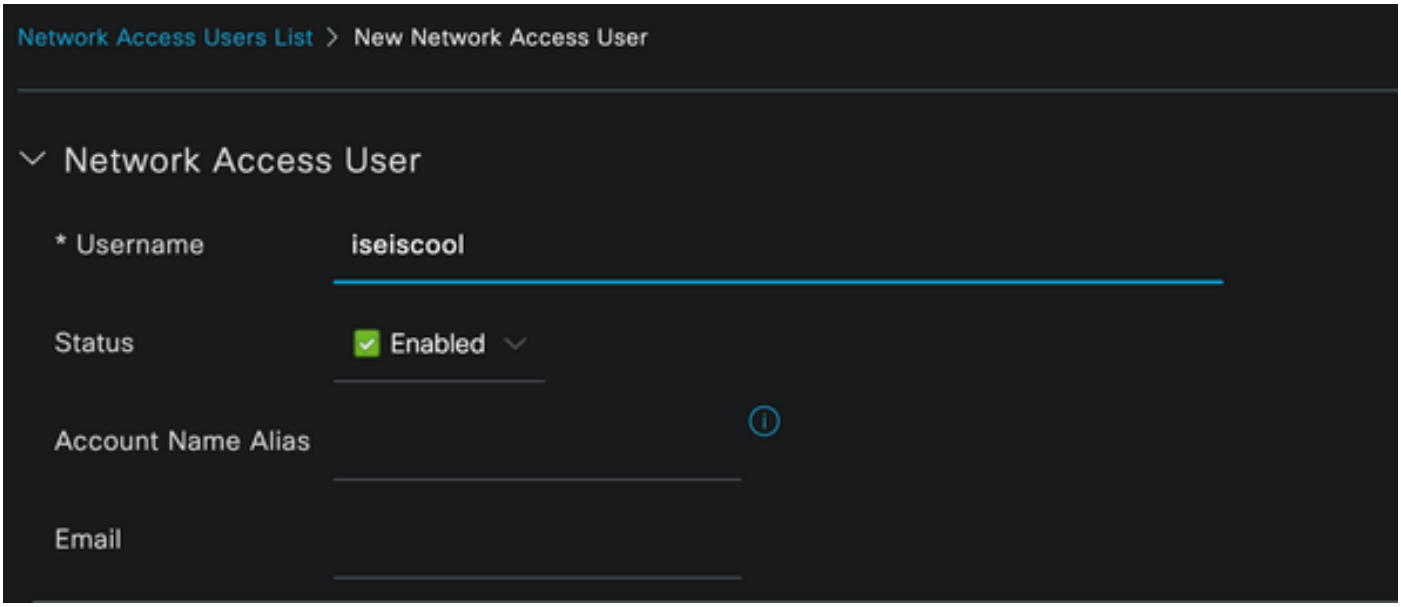
Administration(관리) > Identity Management(ID 관리) > Identity(ID) 탭으로 이동합니다.

Add(추가)를 클릭합니다.



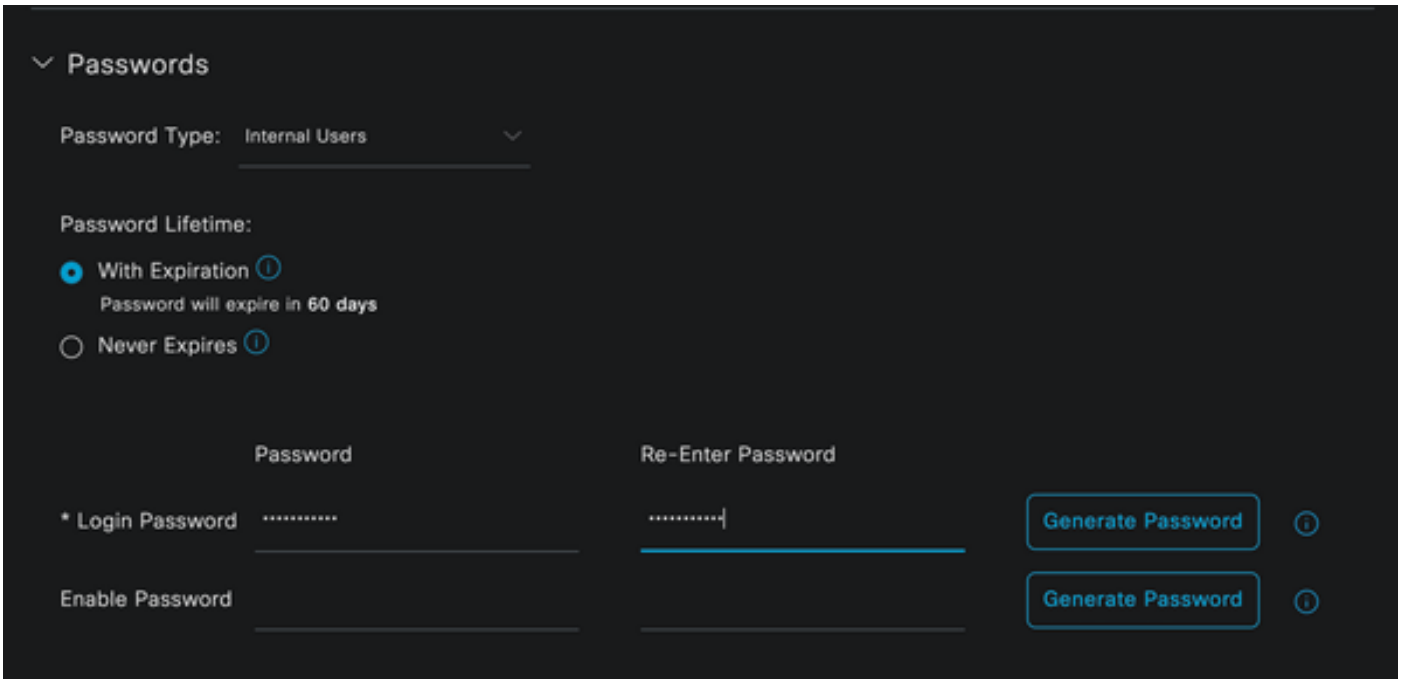
네트워크 액세스 사용자 섹션

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



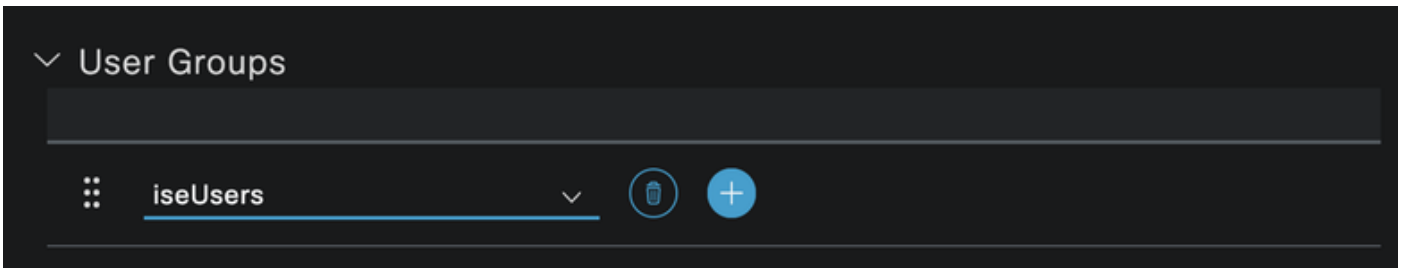
네트워크 액세스 사용자 생성

사용자에게 비밀번호를 할당합니다. VainillaISE97이 사용됩니다.



사용자 생성 비밀번호 섹션

사용자를 그룹 iseUsers에 할당합니다.

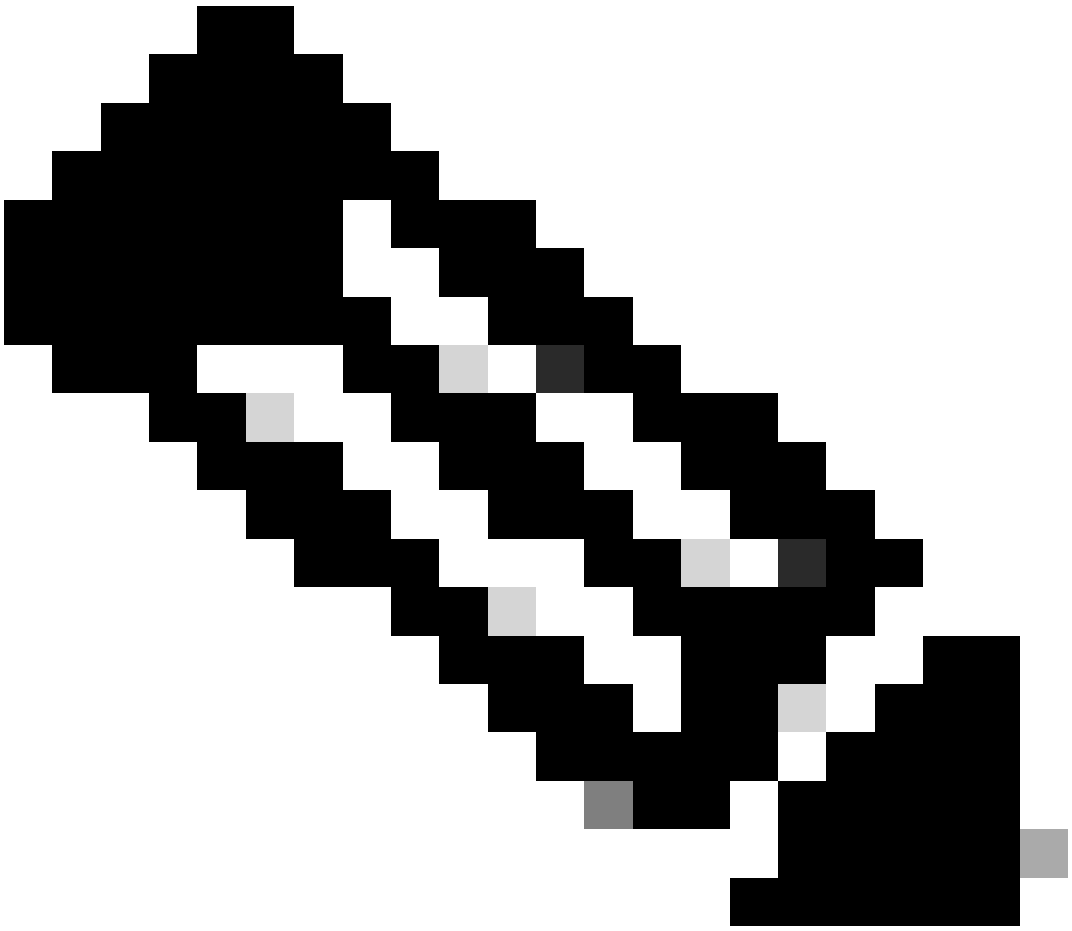


사용자 그룹 할당

정책 집합을 구성합니다.

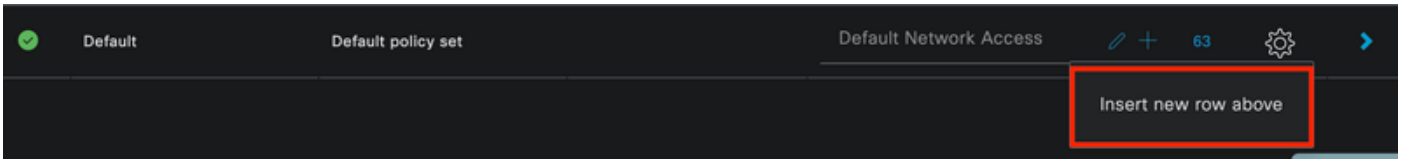
ISE Menu(ISE 메뉴) > Policy(정책) > Policy Sets(정책 집합)로 이동합니다.

기본 정책 집합을 사용할 수 있습니다. 그러나 이 예에서는 Wired라는 이름이 생성됩니다.



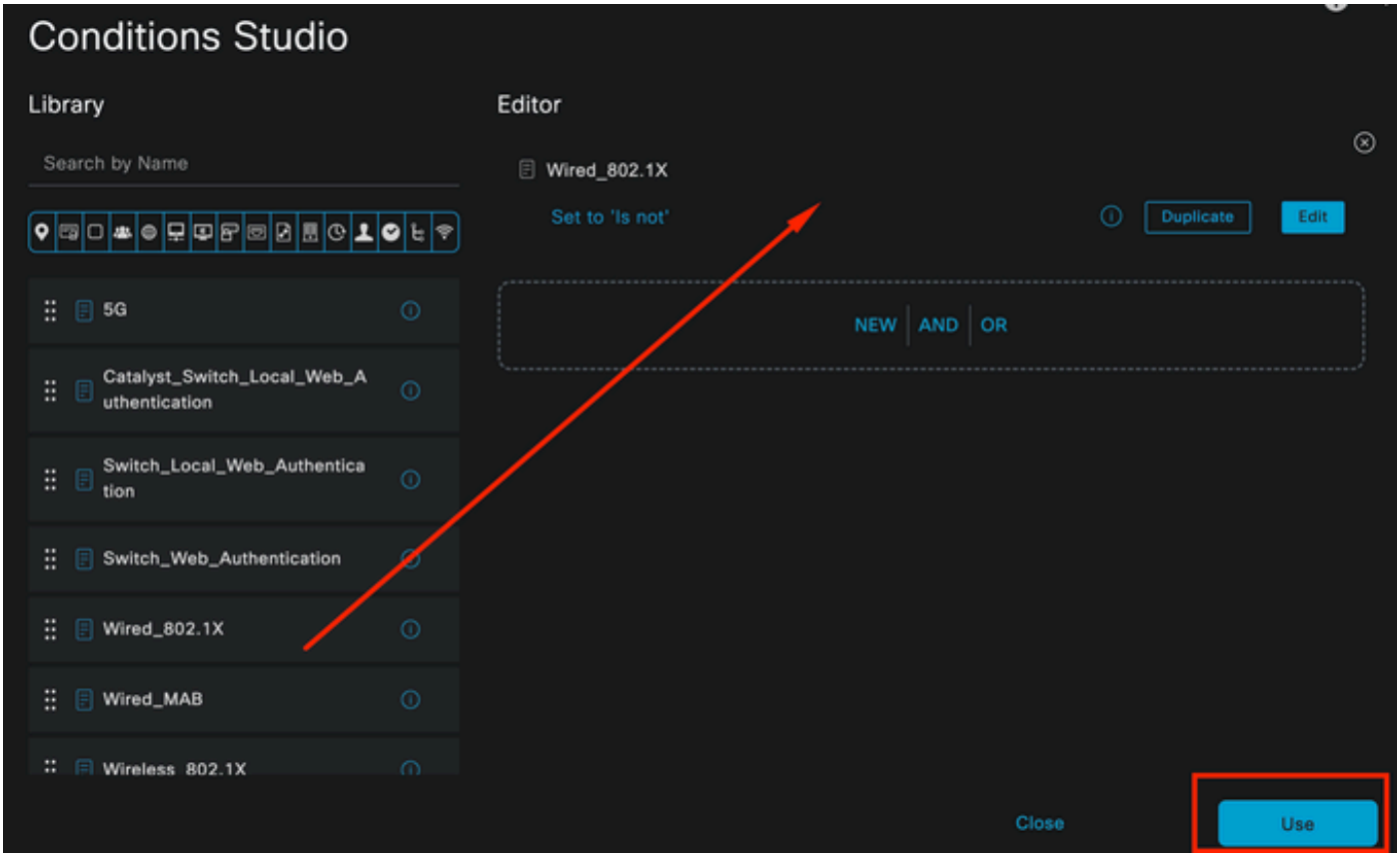
참고: 정책 집합을 분류하고 구분하는 것이 문제 해결에 도움이 됩니다.

참고: 추가 또는 더하기 아이콘이 표시되지 않으면 정책 세트의 톱니바퀴 아이콘을 클릭한 다음 위에 새 행 삽입을 선택할 수 있습니다.



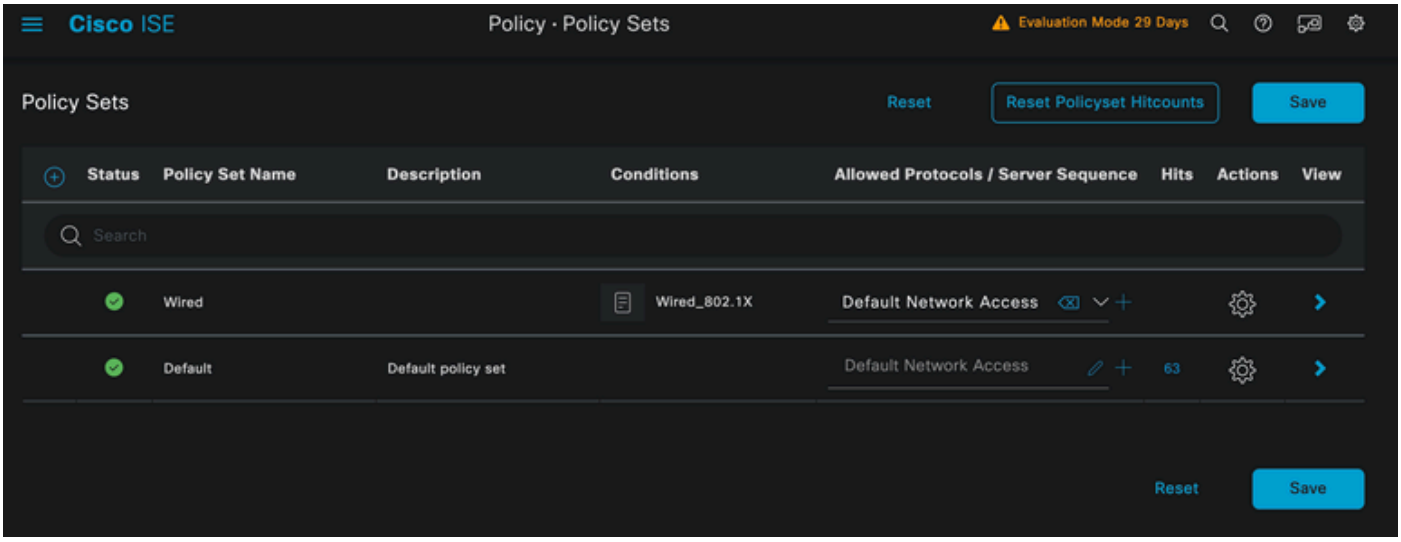
기어 아이콘 옵션

사용된 조건은 유선 8021x입니다. 드래그한 다음 Use(사용)를 클릭합니다.



Authentication Policy Condition Studio

Allowed Protocols 섹션에서 Default Network Access를 선택합니다.

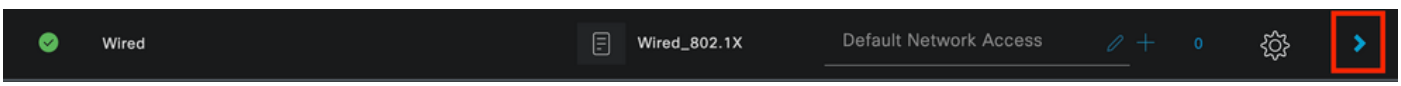


정책 집합 일반 보기

저장을 클릭합니다.

2일 인증 및 권한 부여 정책을 구성합니다.

>아이콘을 클릭합니다.



유선 정책 집합

Authentication Policy(인증 정책) 섹션을 확장합니다.

+아이콘을 클릭합니다.

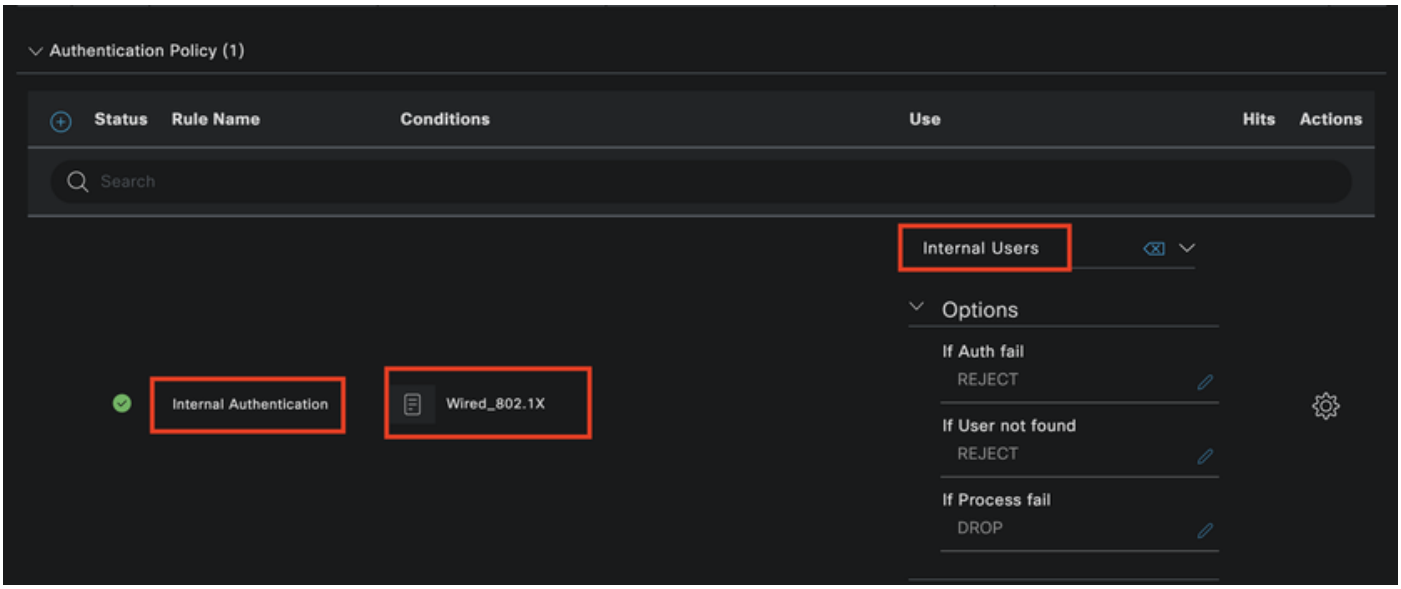
인증 정책

인증 정책에 이름을 할당합니다. 이 예에서는 내부 인증이 사용됩니다.

이 새 인증 정책에 대한 조건 열에서 + 아이콘을 클릭합니다.

미리 구성된 조건 Wired Dot1x가 사용됩니다.

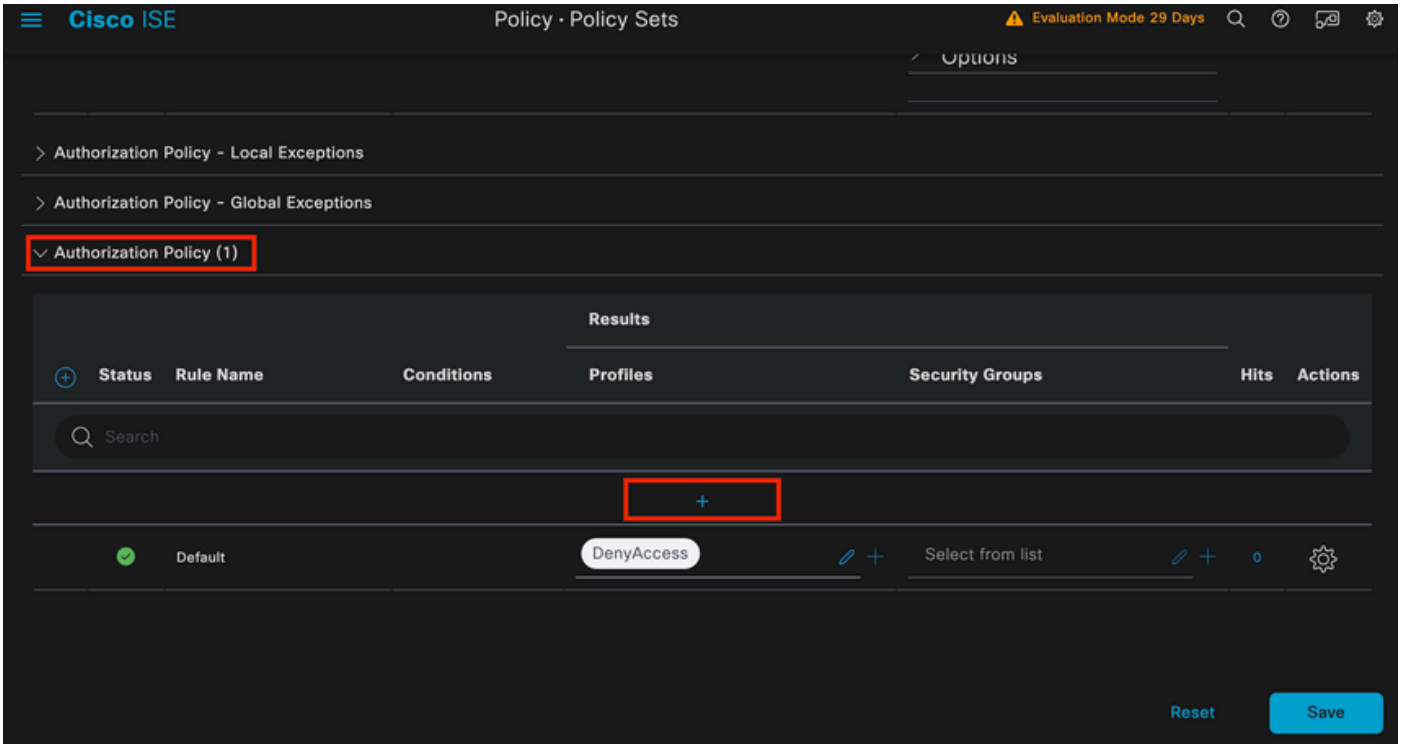
마지막으로 사용 열에서 내부 사용자를 선택합니다.



인증 정책

권한 부여 정책.

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



권한 부여 정책

최근에 생성한 권한 부여 정책의 이름을 지정합니다. 이 컨피그레이션에서는 이름 Internal ISE Users가 사용됩니다.

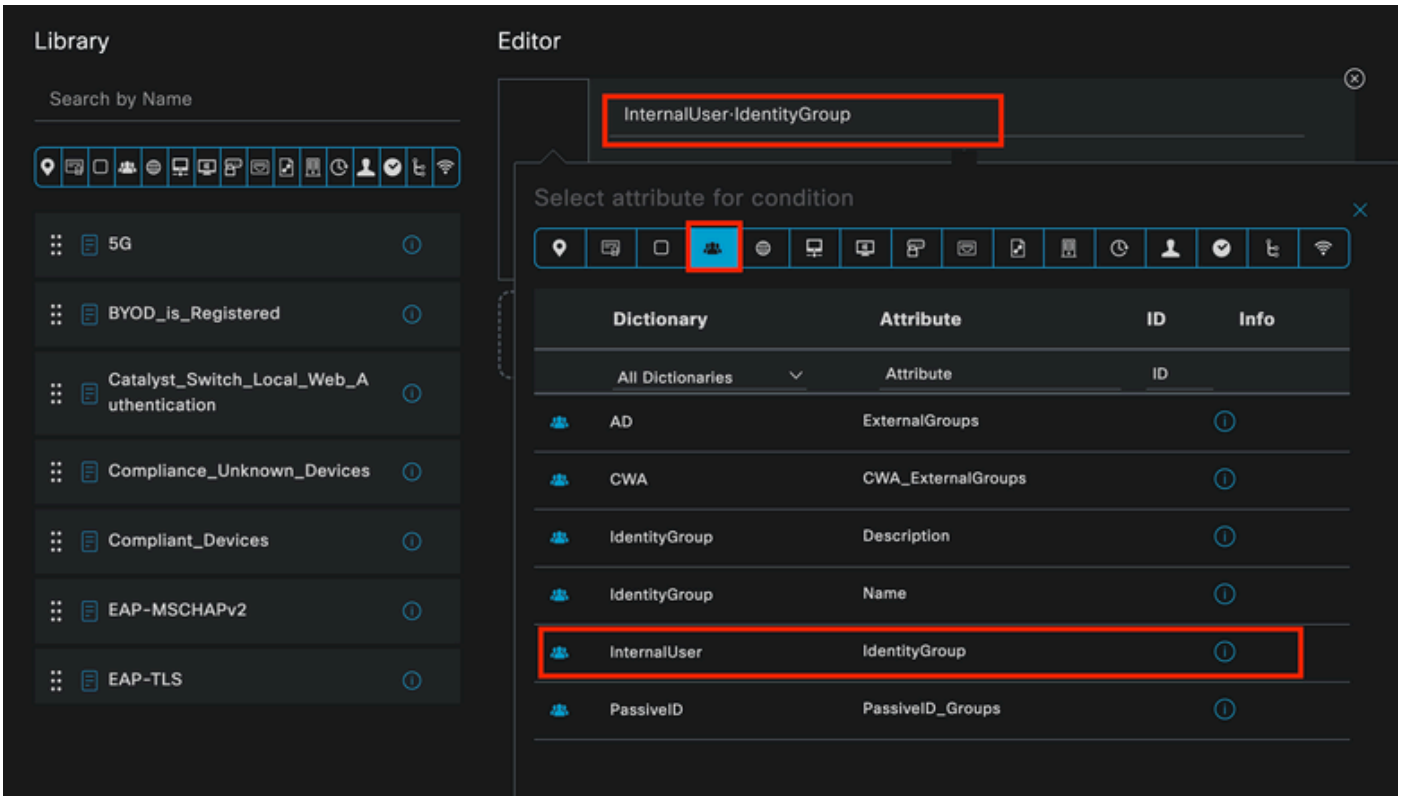
이 권한 부여 정책에 대한 조건을 생성하려면 Conditions(조건) 열에서 + 아이콘을 클릭합니다.

그룹 IseUsers가 사용됩니다.

Attribute(특성) 섹션을 클릭합니다.

IdentityGroup 아이콘을 선택합니다.

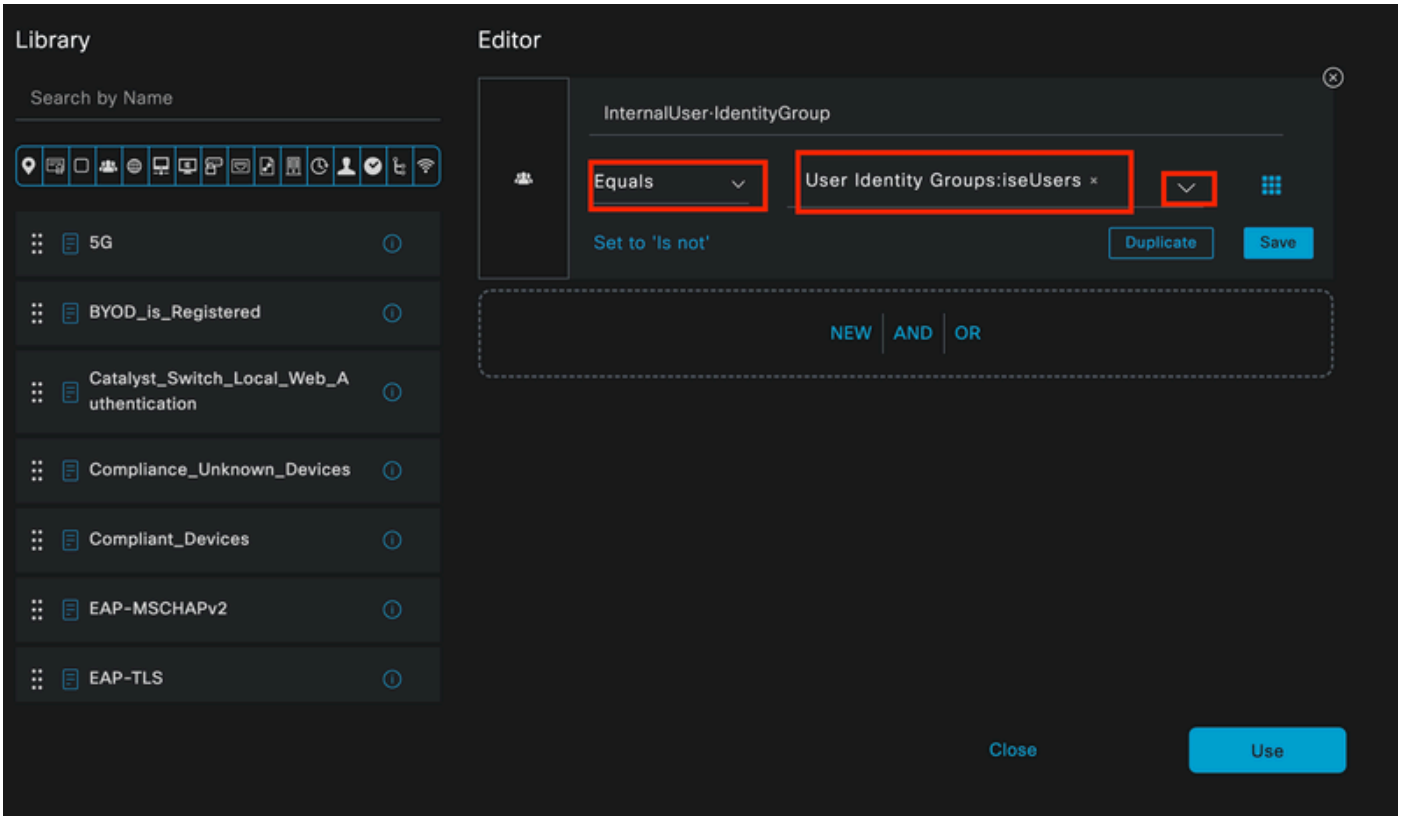
사전에서 IdentityGroup 특성과 함께 제공되는 InternalUser 사전을 선택합니다.



조건 생성

Equals(같음) 연산자를 선택합니다.

User Identity Groups(사용자 ID 그룹)에서 그룹 IseUsers를 선택합니다.

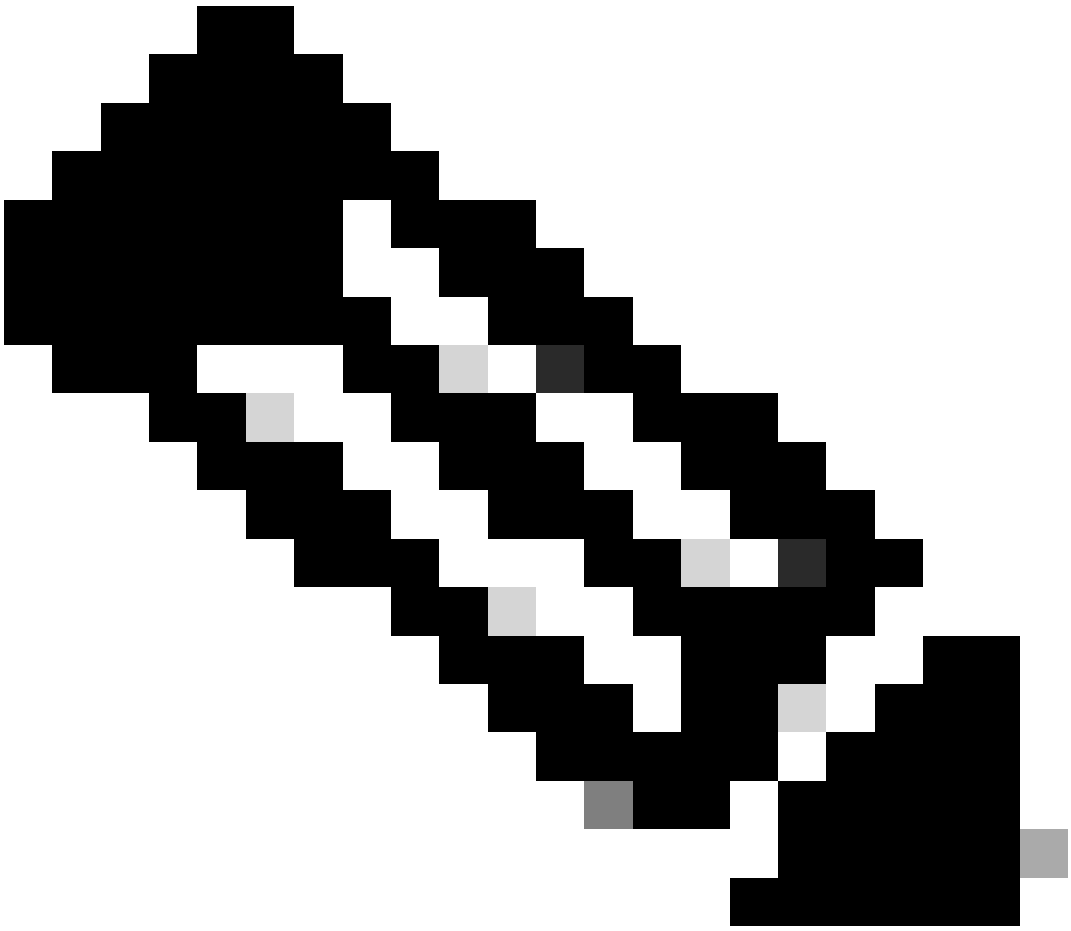


조건 생성

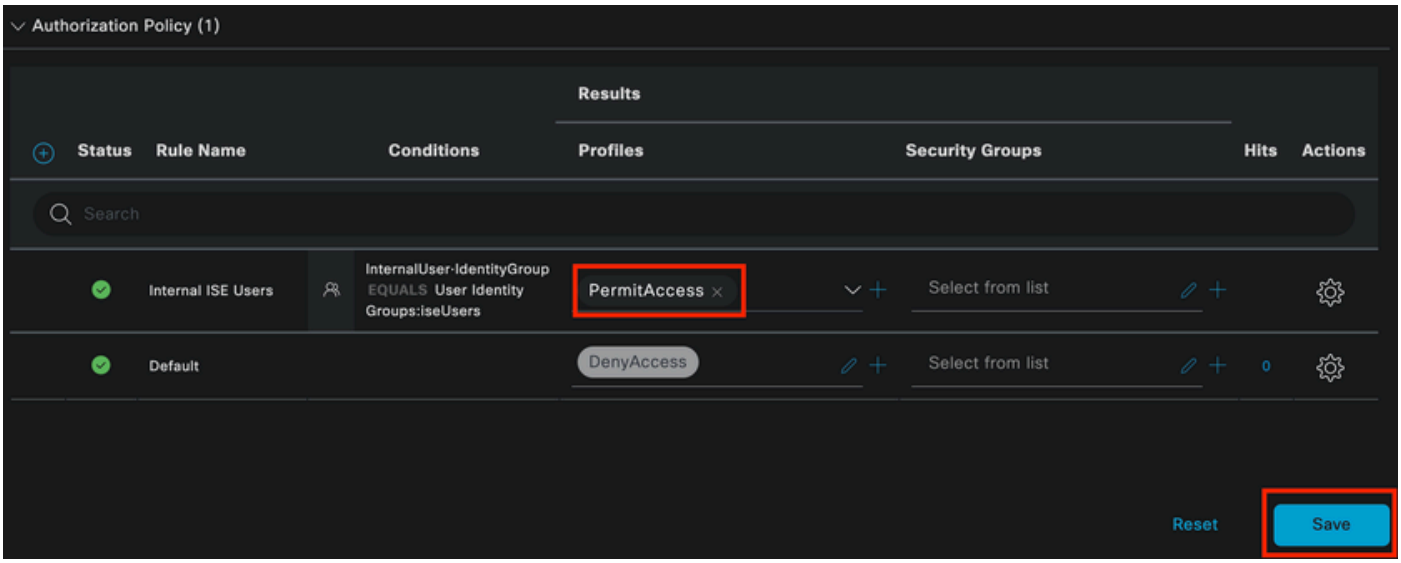
Use(사용)를 클릭합니다.

결과 권한 부여 프로파일을 추가합니다.

사전 구성된 프로파일 Permit Access가 사용됩니다.



참고: ISE로 들어오는 인증이 사용자 ID 그룹 ISEUsers의 일부가 아닌 이 유선 Dot1x 정책 집합을 적중하면 기본 권한 부여 정책을 적중하고 DenyAccess가 발생합니다.



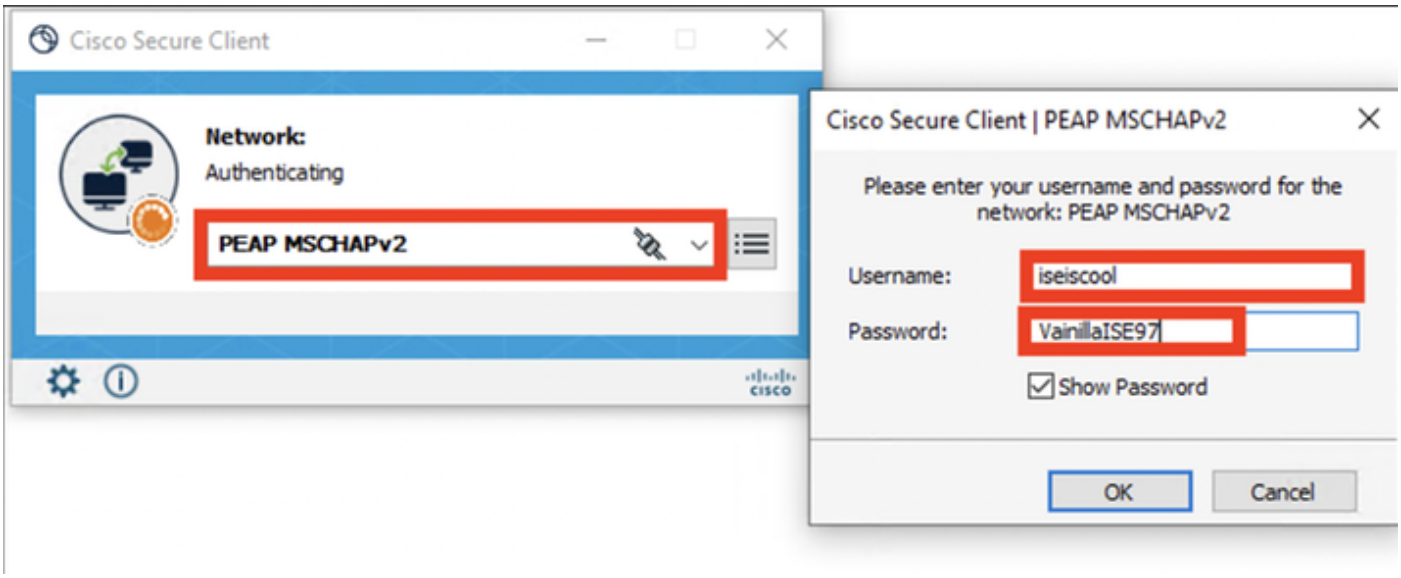
권한 부여 정책

저장을 클릭합니다.

다음을 확인합니다.

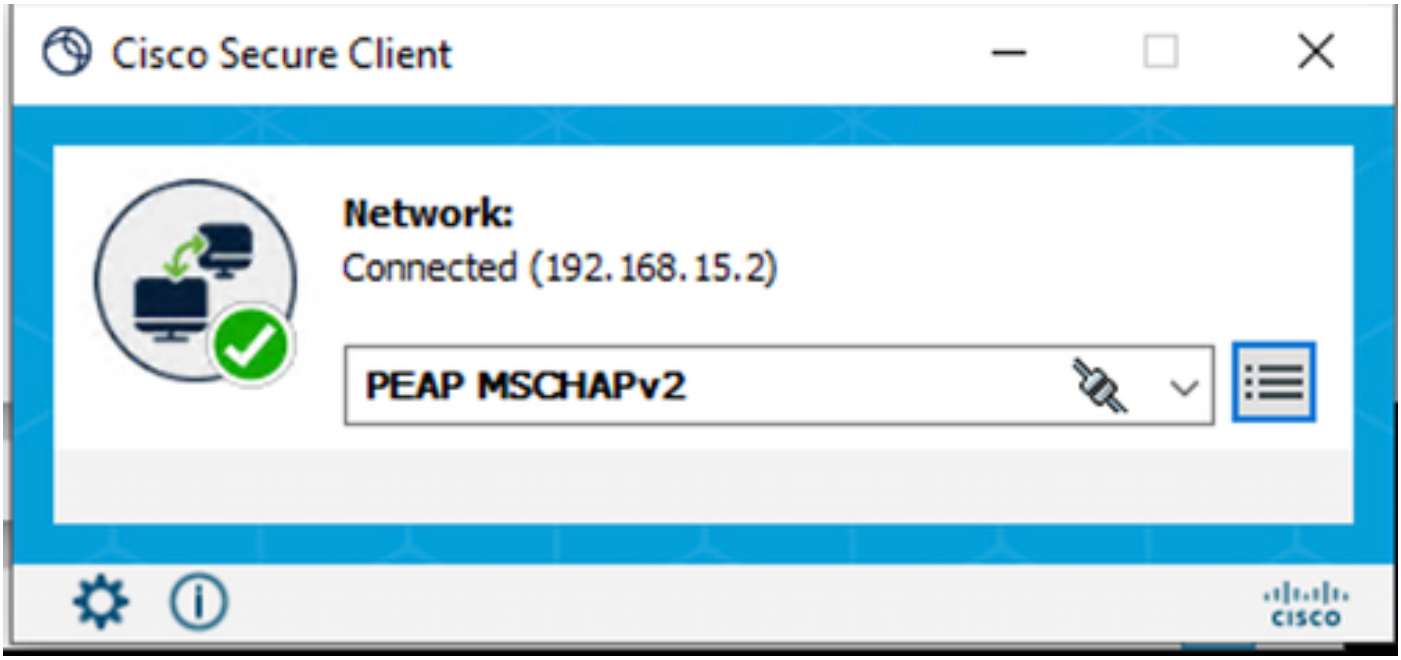
컨피그레이션이 완료되면 Secure Client는 자격 증명을 묻는 프롬프트를 표시하고 PEAP MSCHAPv2 프로파일의 사용을 지정합니다.

이전에 생성한 자격 증명이 입력됩니다.



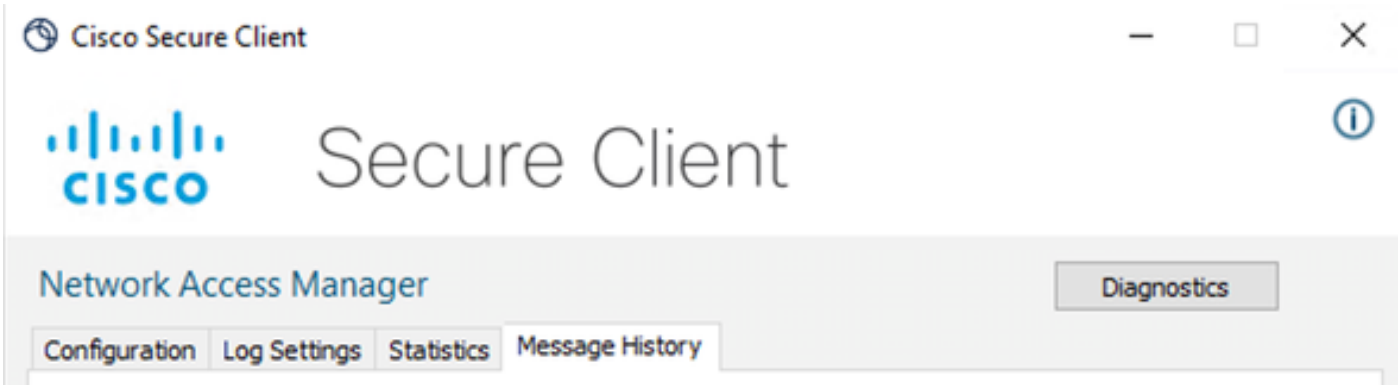
보안 클라이언트 *NAM*

엔드포인트가 올바르게 인증되는 경우 NAM은 연결되어 있음을 표시합니다.

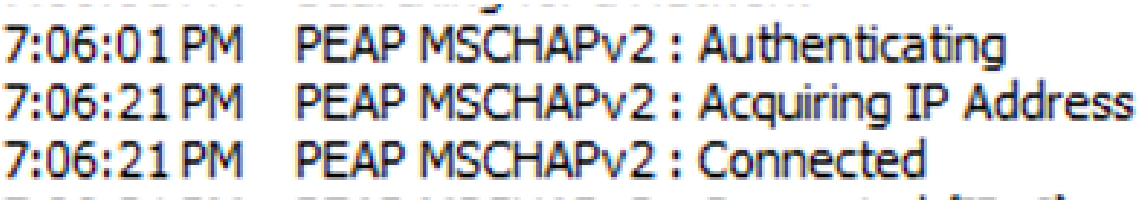


보안 클라이언트 *NAM*

정보 아이콘을 클릭하고 Message History(메시지 기록) 섹션으로 이동하면 NAM이 수행한 모든 단계의 세부 정보가 표시됩니다.



보안 클라이언트 메시지 기록



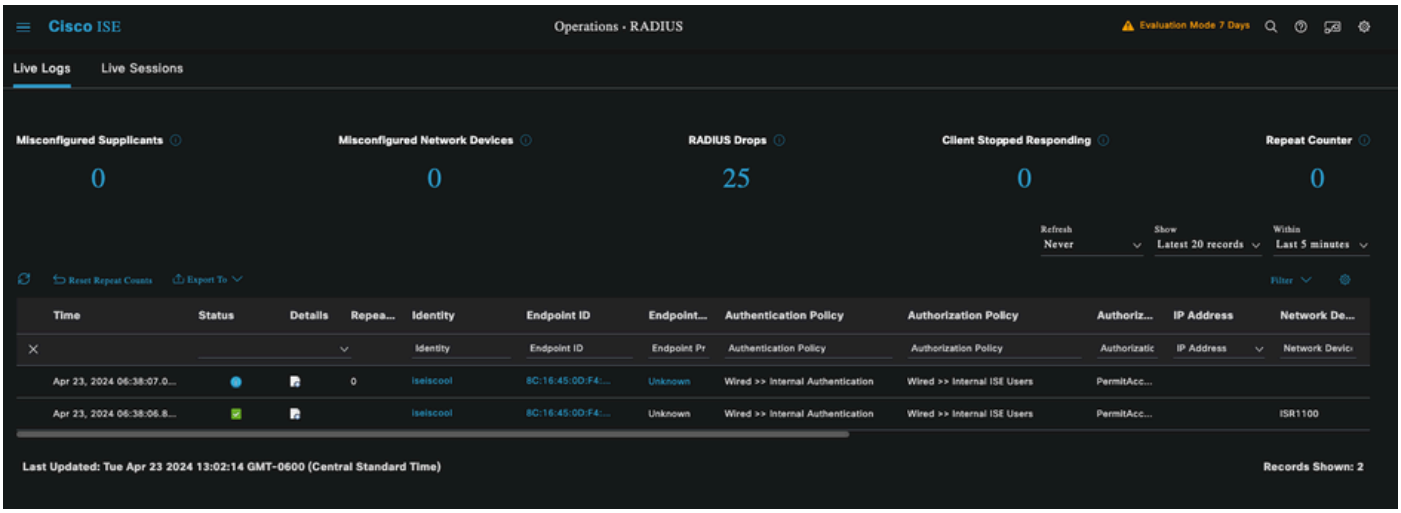
보안 클라이언트 메시지 기록

ISE에서 Operations(작업) > Radius LiveLogs(RADIUS 라이브 로그)로 이동하여 인증의 세부 정보를 확인합니다. 다음 그림에서 볼 수 있듯이 사용된 사용자 이름이 표시됩니다.

기타 세부 사항:

- 타임스탬프입니다.
- MAC 주소.
- 정책 집합이 사용되었습니다.
- 인증 정책.

- 권한 부여 정책.
- 기타 관련 정보



ISE RADIUS 라이브 로그

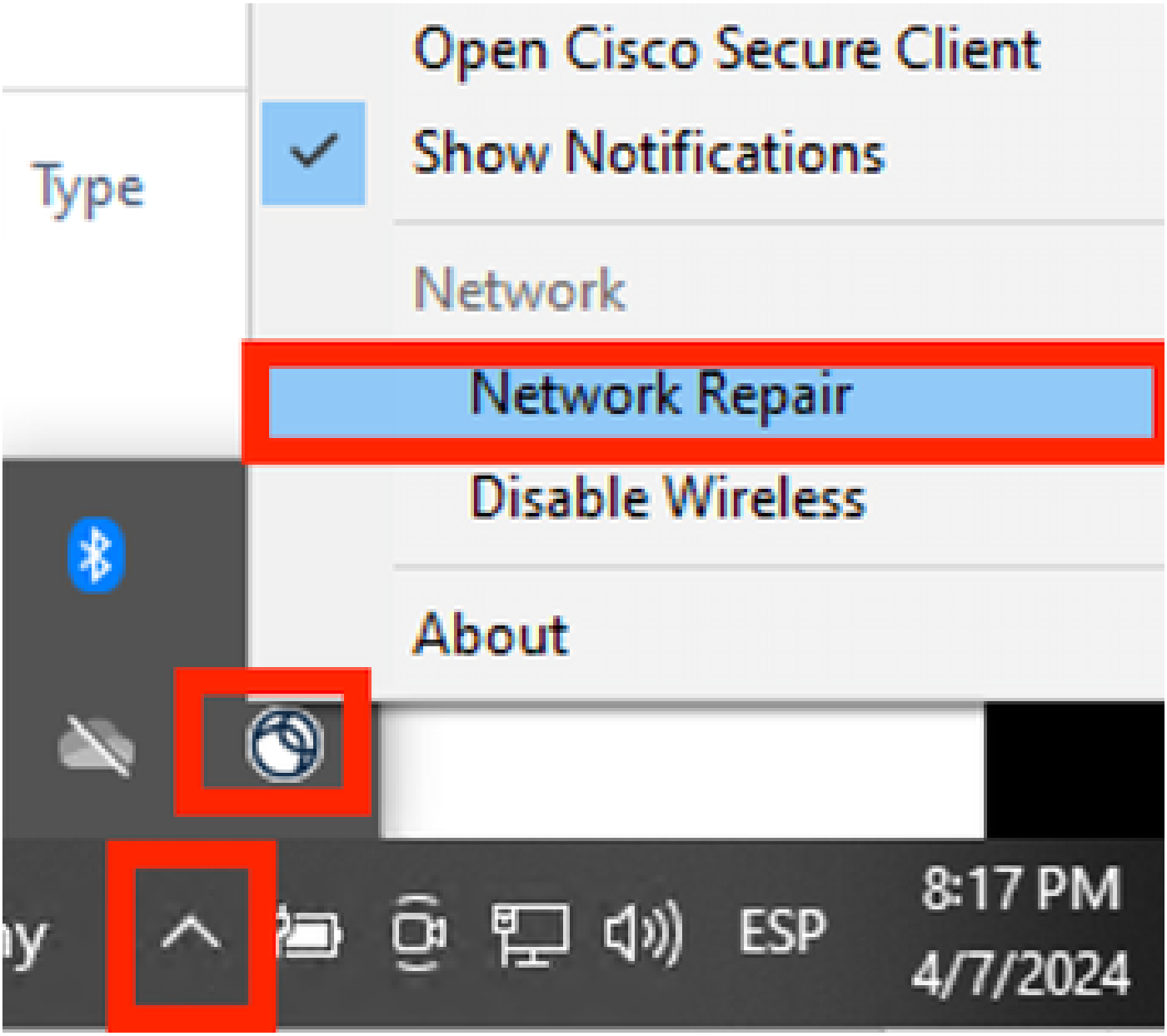
올바른 정책에 도달하고 그 결과가 인증 성공 상태임을 알 수 있으므로 컨피그레이션이 올바른 것으로 판단됩니다.

문제 해결

문제: 보안 클라이언트에서 NAM 프로필을 사용하지 않습니다.

프로파일 편집기에서 생성된 새 프로파일을 NAM이 사용하지 않는 경우 Secure Client에 대해 Network Repair 옵션을 사용합니다.

Windows 표시줄 > Circumflex 아이콘 클릭 > 마우스 오른쪽 단추 클릭 보안 클라이언트 아이콘 > 네트워크 복구 클릭으로 이동하여 이 옵션을 찾을 수 있습니다.



네트워크 복구 섹션

문제 2: 추가 분석을 위해 로그를 수집해야 합니다.

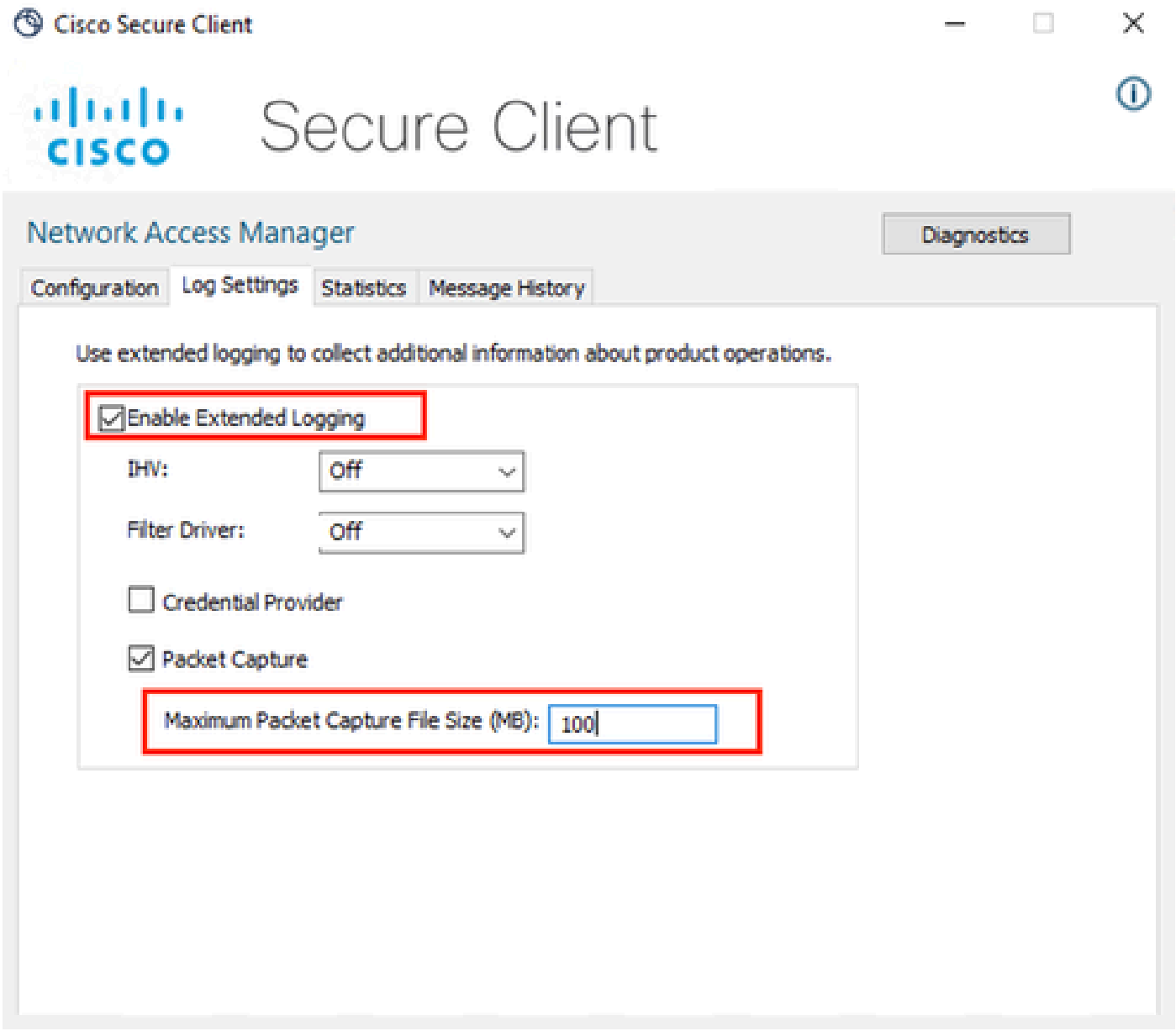
1. NAM 확장 로깅 사용

NAM을 열고 톱니바퀴 모양 아이콘을 클릭합니다.

NAM 인터페이스

Log Settings(로그 설정) 탭으로 이동합니다. Enable Extended Logging(확장 로깅 활성화) 확인란을 선택합니다.

패킷 캡처 파일 크기를 100MB로 설정합니다.



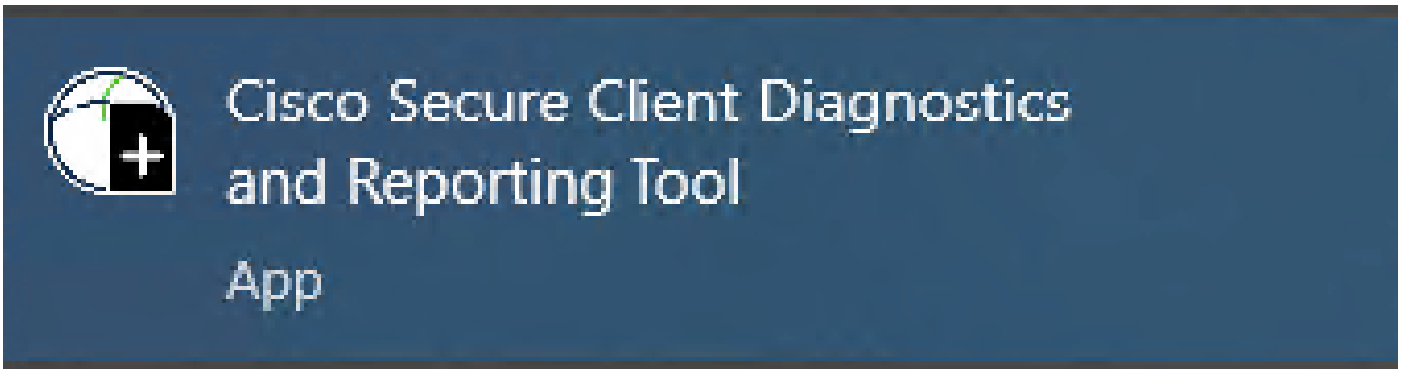
보안 클라이언트 NAM 로그 설정

2. 문제를 재현합니다.

확장 로깅을 활성화하면 로그가 생성되고 트래픽이 캡처되도록 문제를 여러 번 재현합니다.

3. 보안 클라이언트 DART 번들 수집

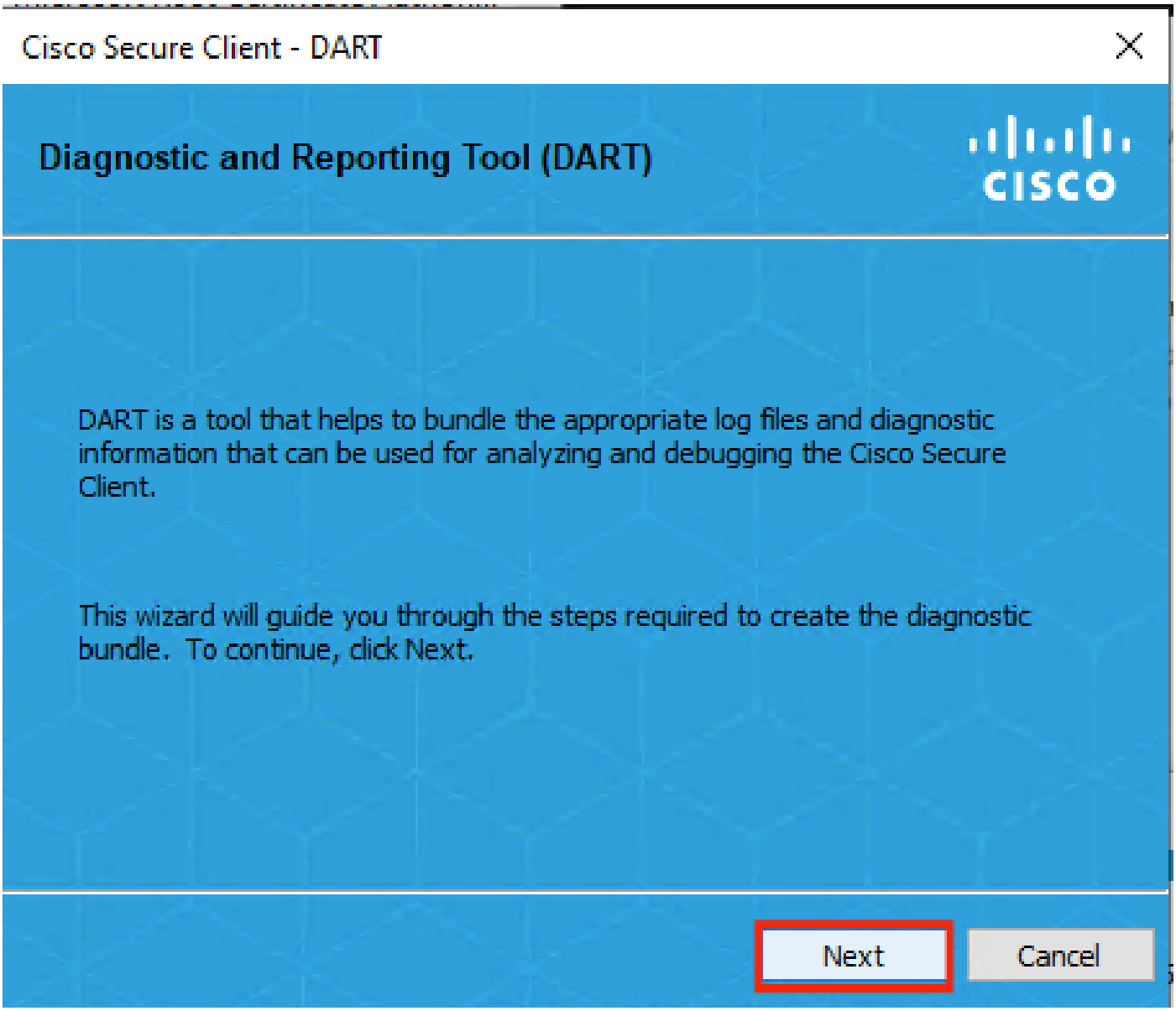
Windows에서 검색 표시줄로 이동하고 Cisco Secure Client Diagnostics and Reporting Tool을 입력합니다.



DART 모듈

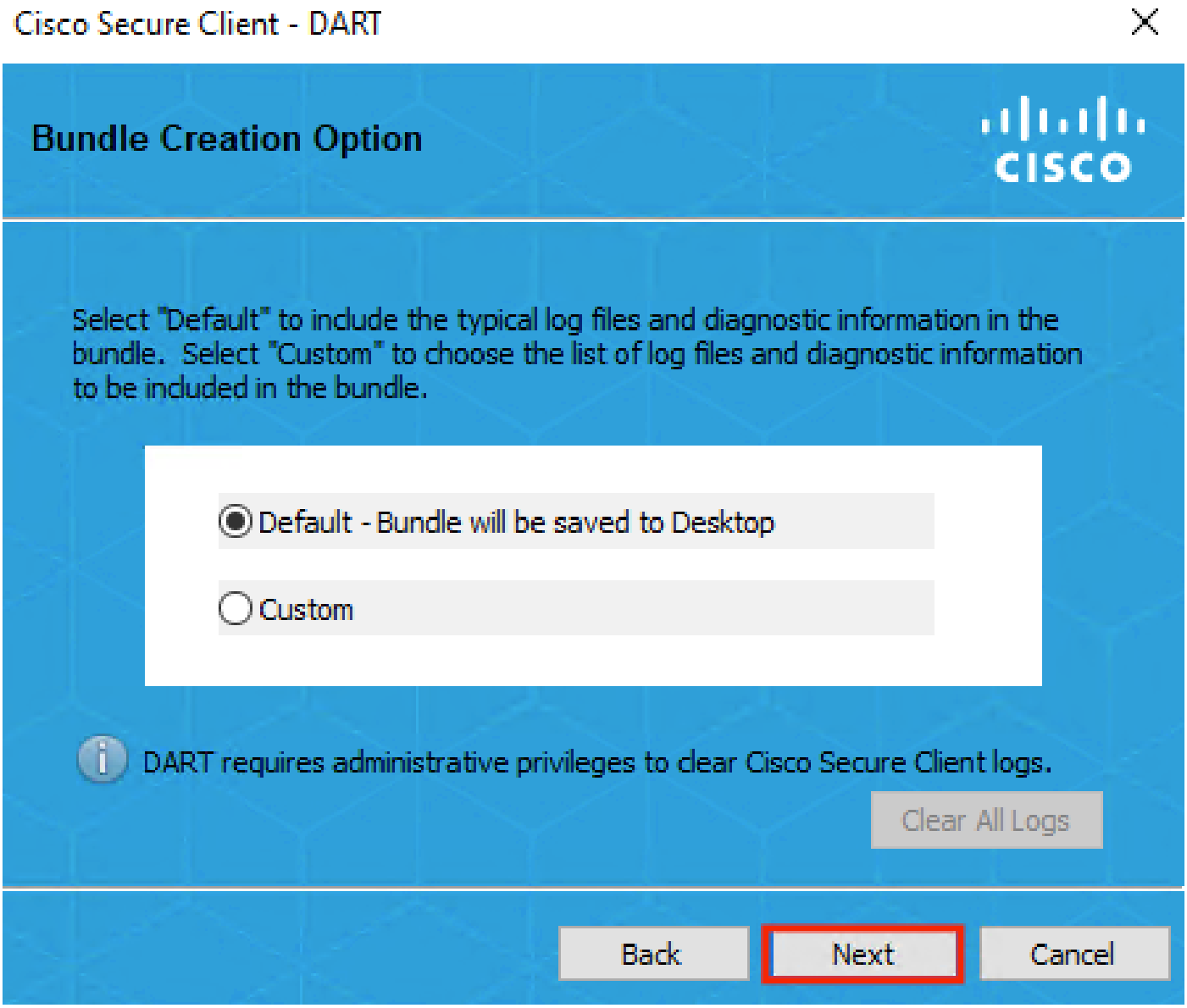
설치 과정에서 이 모듈도 설치했습니다. 로그 및 관련 dot1x 세션 정보를 수집하여 문제 해결 프로세스 중에 도움이되는 도구입니다.

첫 번째 창에서 Next(다음)를 클릭합니다.



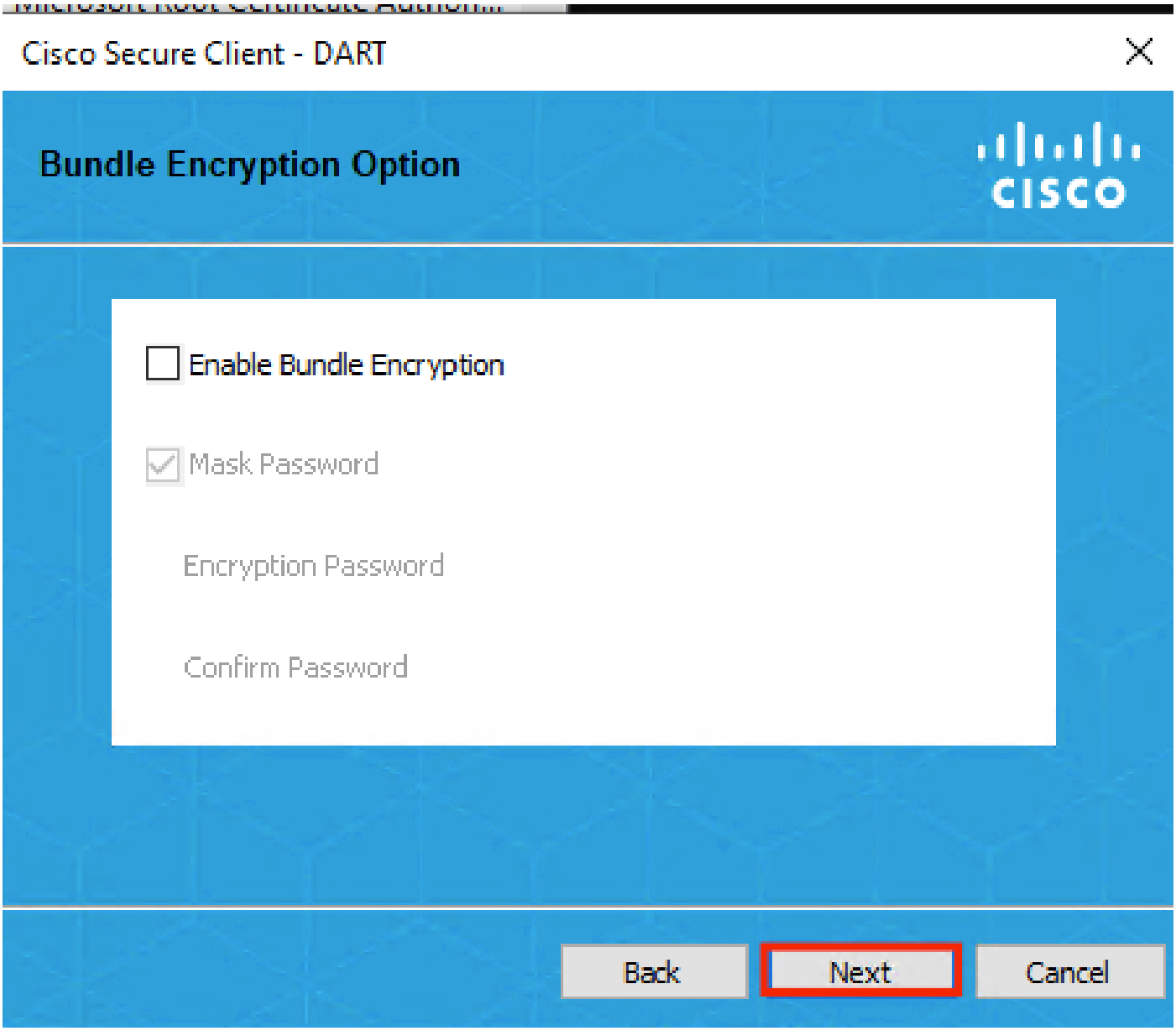
DART 모듈

다시 한 번 Next(다음)를 클릭하여 로그 번들을 데스크톱에 저장할 수 있습니다.



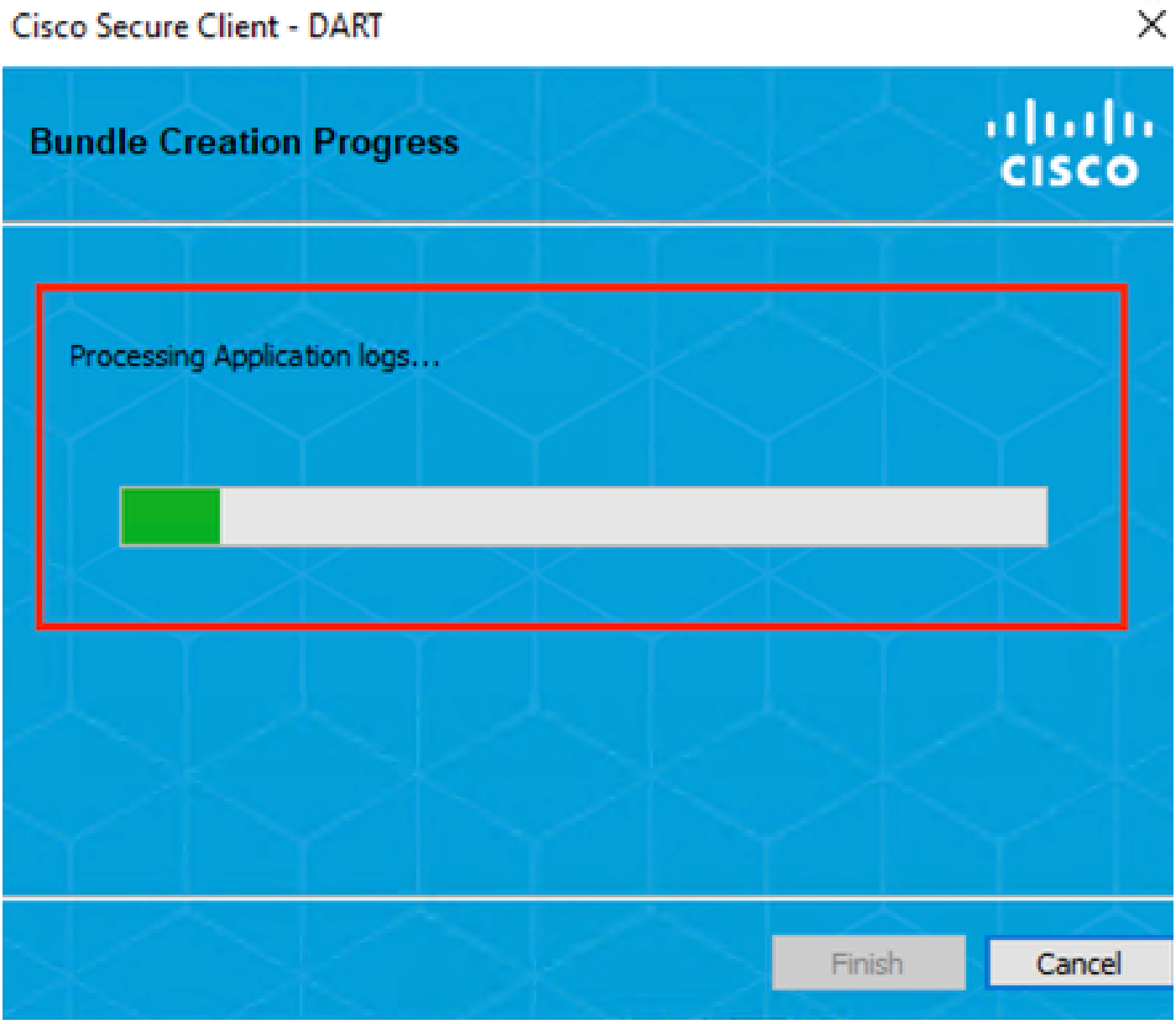
DART 모듈

필요한 경우 Enable Bundle Encryption(번들 암호화 활성화) 확인란을 선택합니다.



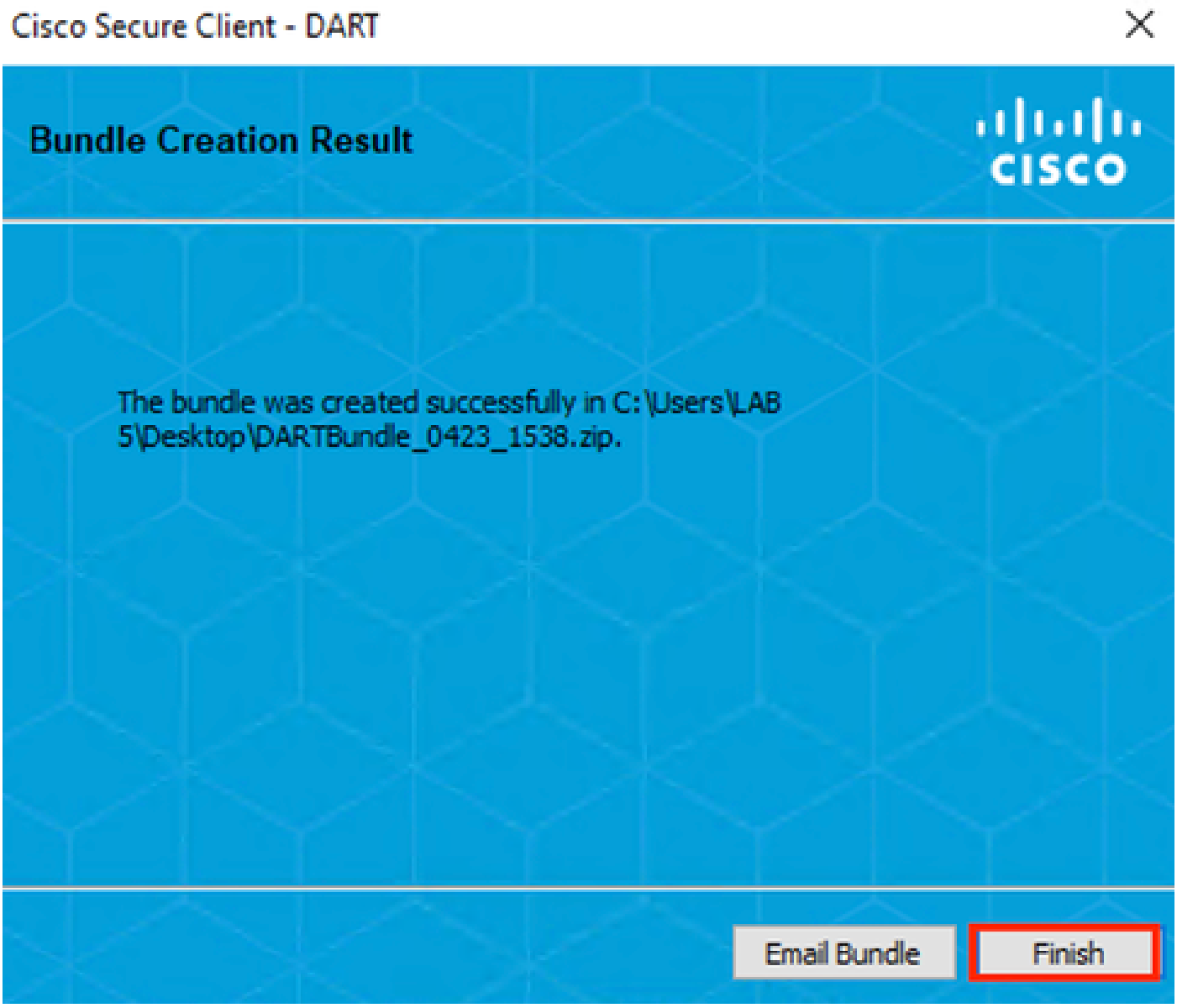
DART 모듈

DART 로그 수집이 시작됩니다.



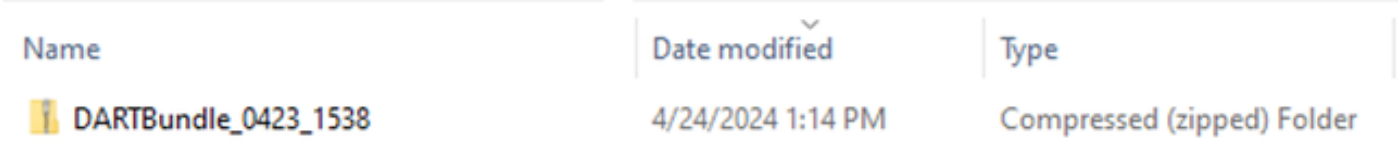
DART 로그 수집

프로세스가 완료될 때까지 10분 이상 걸릴 수 있습니다.



DART 번들 생성 결과

DART 결과 파일은 데스크톱 디렉토리에서 찾을 수 있습니다.



DART 결과 파일

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.