EAP-TTLS로 머신 및 사용자 인증 구성

목차

소개

이 문서에서는 보안 클라이언트 NAM 및 Cisco ISE에서 EAP-TTLS(EAP-MSCHAPv2)를 사용하여 머신 및 사용자 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이 구축을 진행하기 전에 다음 항목에 대해 미리 알고 있는 것이 좋습니다.

- Cisco ISE(Identity Services Engine)
- Secure Client NAM(Network Analysis Module)
- EAP 프로토콜

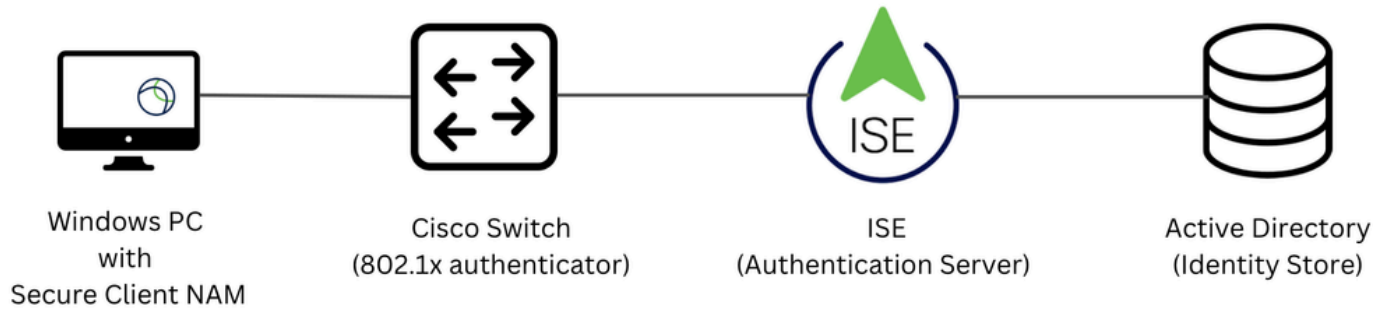
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE(Identity Services Engine) 버전 3.4
- C9300 스위치와 Cisco IOS® XE Software, 버전 16.12.01
- Windows 10 Pro 버전 22H2 빌드 19045.3930

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.

네트워크 토폴로지



네트워크 토폴로지

구성

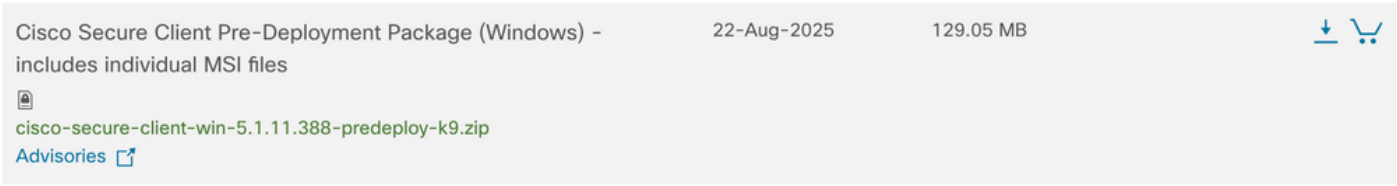
설정

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

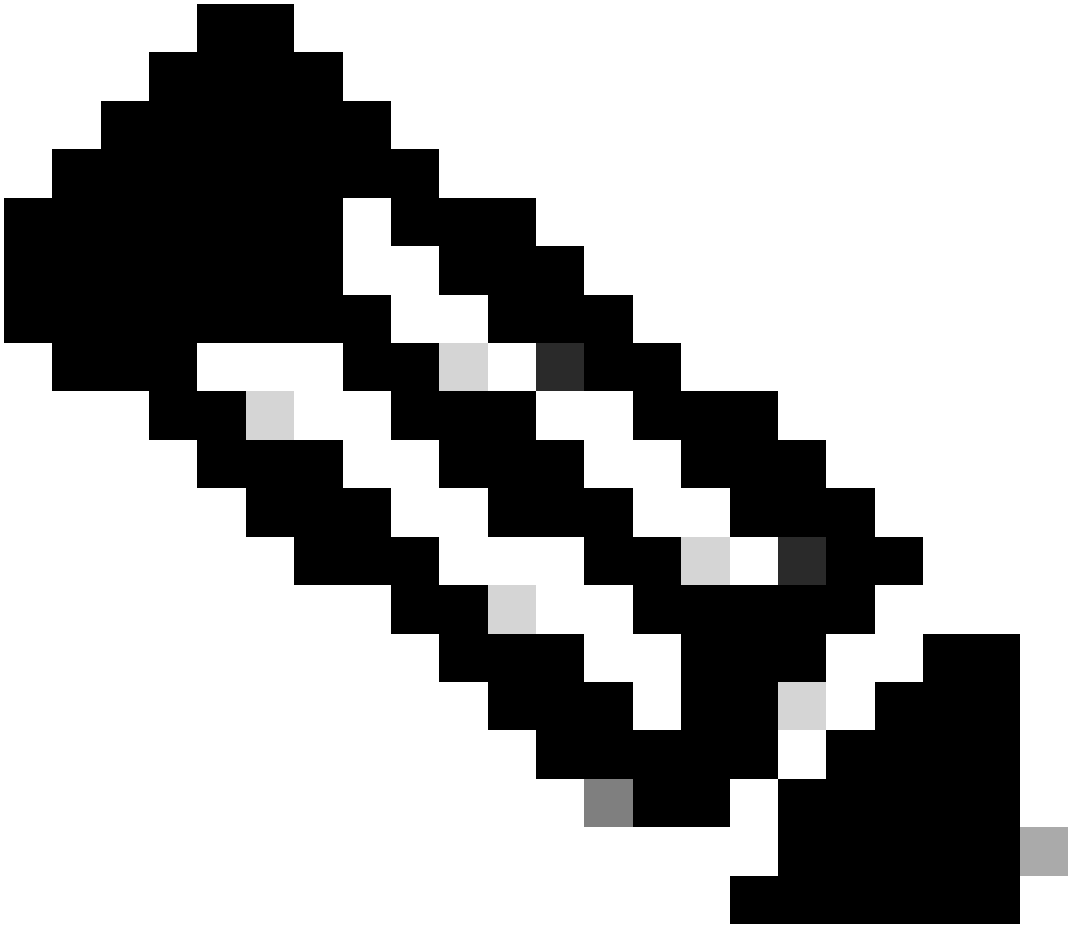
1단계. Cisco Software Download(Cisco 소프트웨어 다운로드)로 이동합니다. 제품 검색 표시줄에 Secure Client 5를 입력합니다.

이 컨피그레이션 예에서는 버전 5.1.11.388을 사용합니다. 설치는 사전 구축 방법을 사용하여 수행됩니다.

다운로드 페이지에서 Cisco Secure Client Pre-Deployment Package(Windows)를 찾아 다운로드합니다.

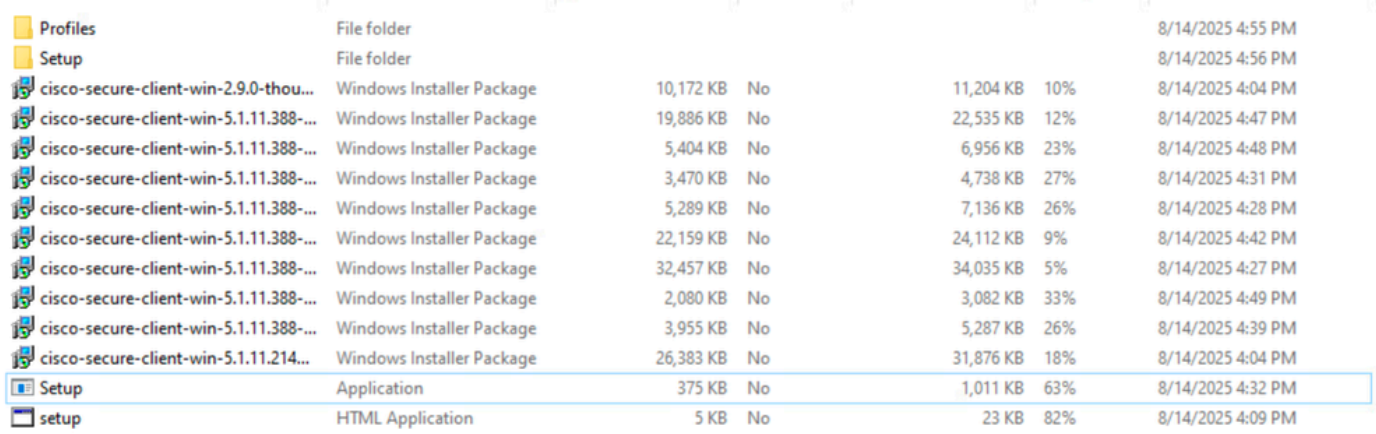


사전 구축 zip 파일



참고: Cisco AnyConnect는 더 이상 사용되지 않으며 Cisco 소프트웨어 다운로드 사이트에서 더 이상 사용할 수 없습니다.

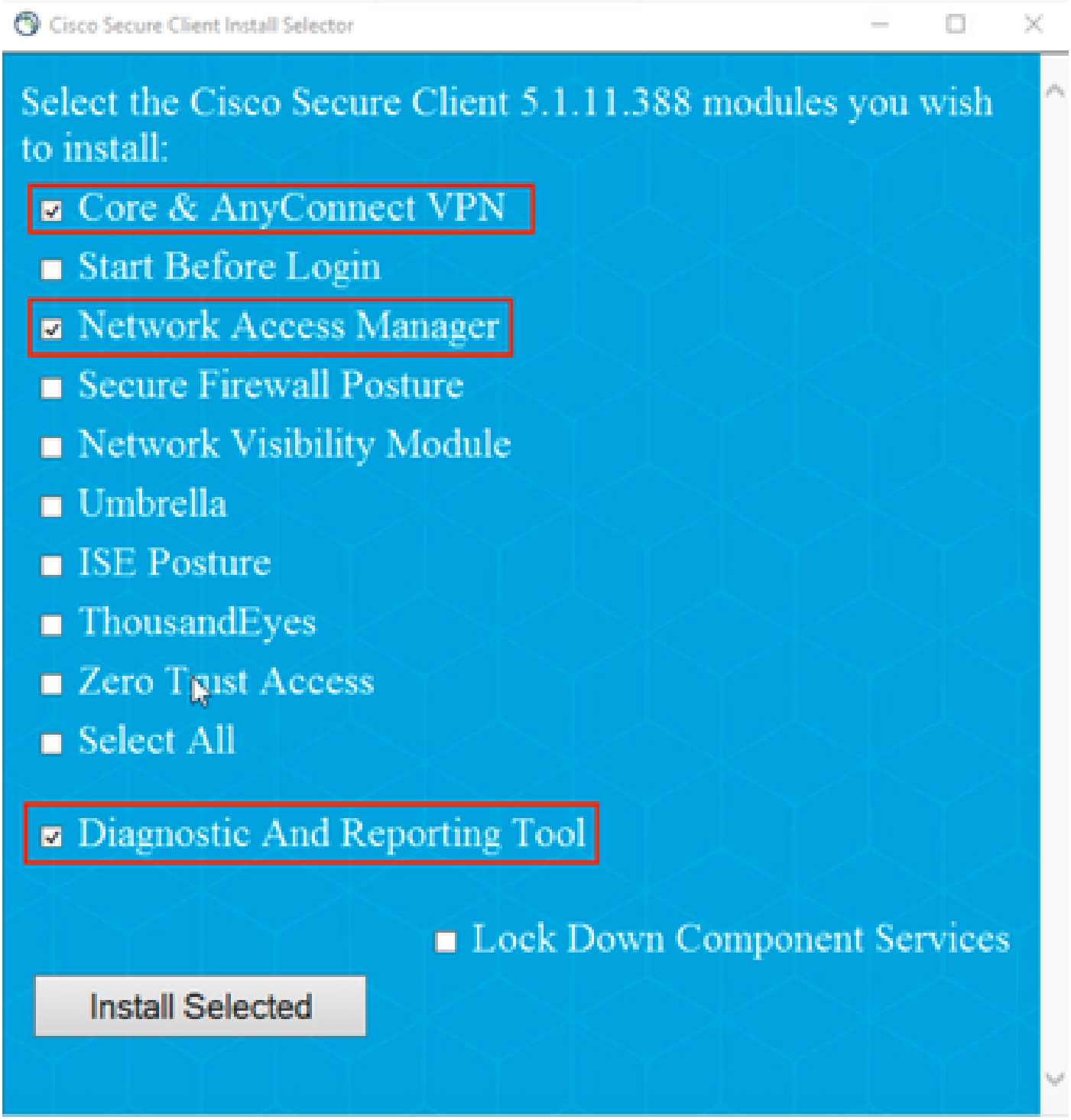
2단계. 다운로드하고 압축을 풀면 Setup(설정)을 클릭합니다.



Profiles	File folder					8/14/2025 4:55 PM
Setup	File folder					8/14/2025 4:56 PM
cisco-secure-client-win-2.9.0-thou...	Windows Installer Package	10,172 KB	No	11,204 KB	10%	8/14/2025 4:04 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	19,886 KB	No	22,535 KB	12%	8/14/2025 4:47 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,404 KB	No	6,956 KB	23%	8/14/2025 4:48 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,470 KB	No	4,738 KB	27%	8/14/2025 4:31 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	5,289 KB	No	7,136 KB	26%	8/14/2025 4:28 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	22,159 KB	No	24,112 KB	9%	8/14/2025 4:42 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	32,457 KB	No	34,035 KB	5%	8/14/2025 4:27 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	2,080 KB	No	3,082 KB	33%	8/14/2025 4:49 PM
cisco-secure-client-win-5.1.11.388-...	Windows Installer Package	3,955 KB	No	5,287 KB	26%	8/14/2025 4:39 PM
cisco-secure-client-win-5.1.11.214...	Windows Installer Package	26,383 KB	No	31,876 KB	18%	8/14/2025 4:04 PM
Setup	Application	375 KB	No	1,011 KB	63%	8/14/2025 4:32 PM
setup	HTML Application	5 KB	No	23 KB	82%	8/14/2025 4:09 PM

사전 구축 Zip 파일

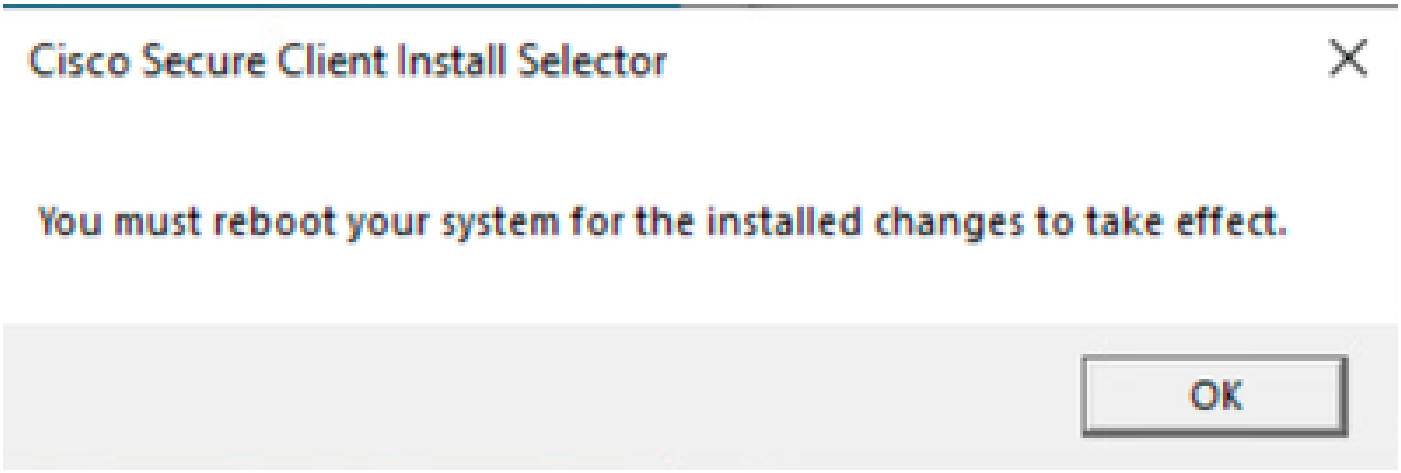
3단계. Core 및 AnyConnect VPN, Network Access Manager, 진단 및 보고 툴 모듈을 설치합니다.



보안 클라이언트 설치 프로그램

Install Selected(선택 항목 설치)를 클릭합니다.

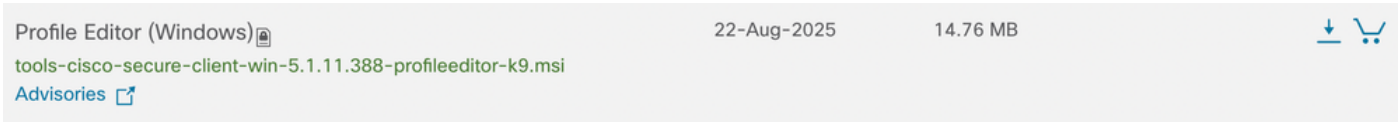
4단계. 설치 후 재부팅해야 합니다. OK(확인)를 클릭하고 디바이스를 다시 시작합니다.



Reboot Required 팝업

2부: Secure Client NAM 프로파일 편집기 다운로드 및 설치

1단계. 프로파일 편집기는 보안 클라이언트와 동일한 다운로드 페이지에서 찾을 수 있습니다. 이 구성 예에서는 버전 5.1.11.388을 사용합니다.



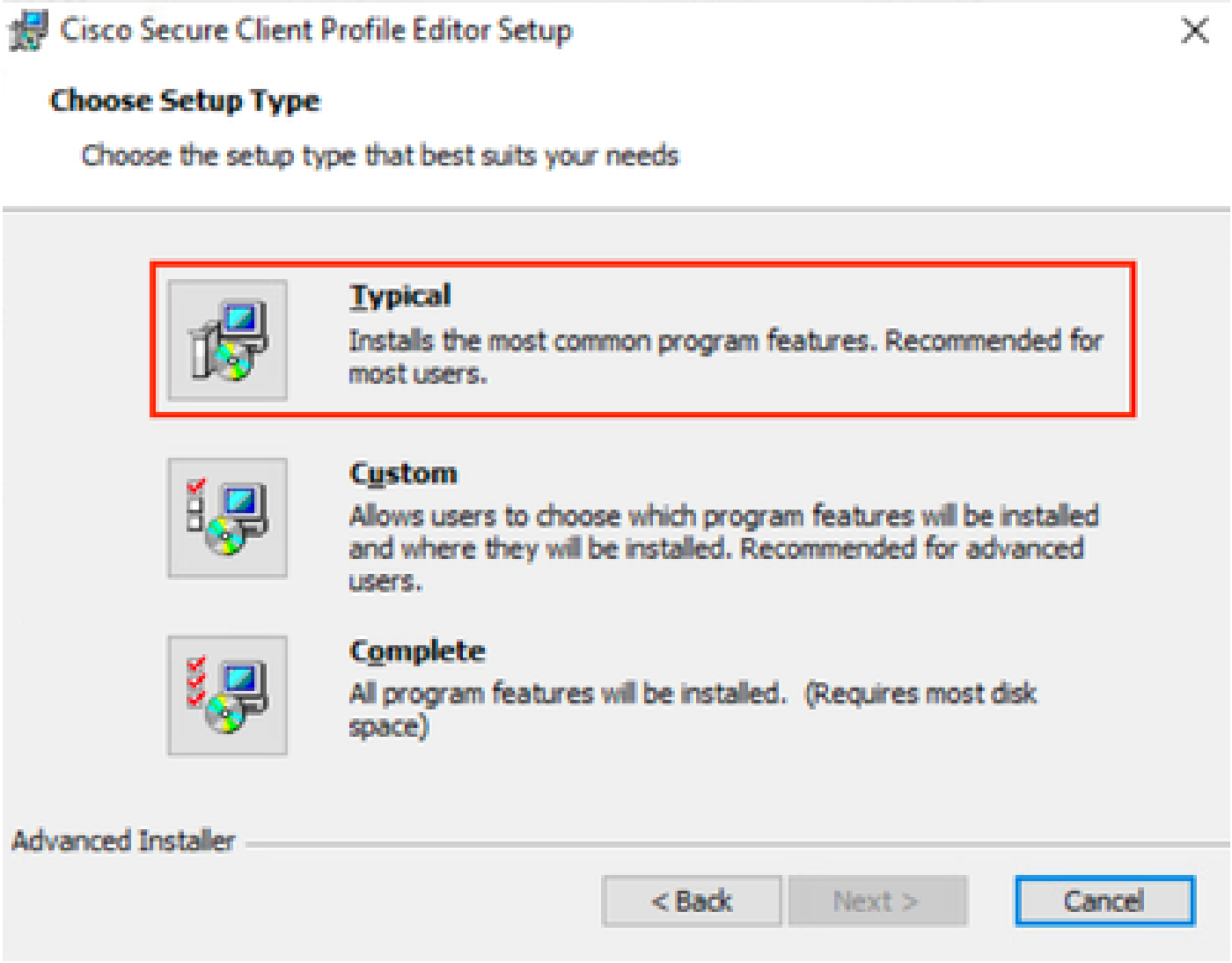
프로파일 편집기

프로파일 편집기를 다운로드하여 설치합니다.

2단계. MSI 파일을 실행합니다.

프로파일 편집기 설정 시작

3단계. Typical setup 옵션을 사용하고 NAM 프로파일 편집기를 설치합니다.

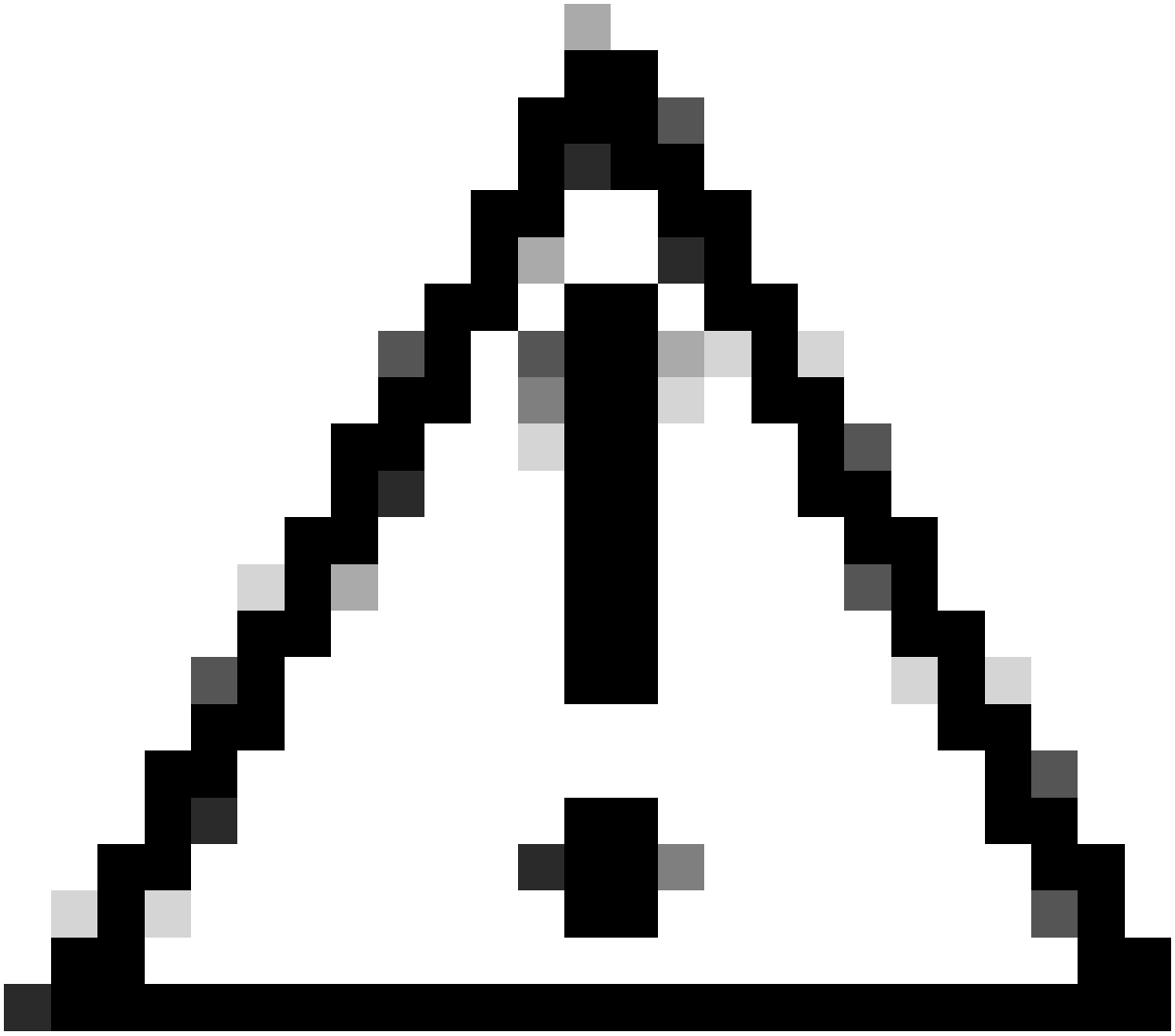


프로파일 편집기 설정

3부: NAM이 Windows 캐시 자격 증명에 액세스할 수 있도록 허용

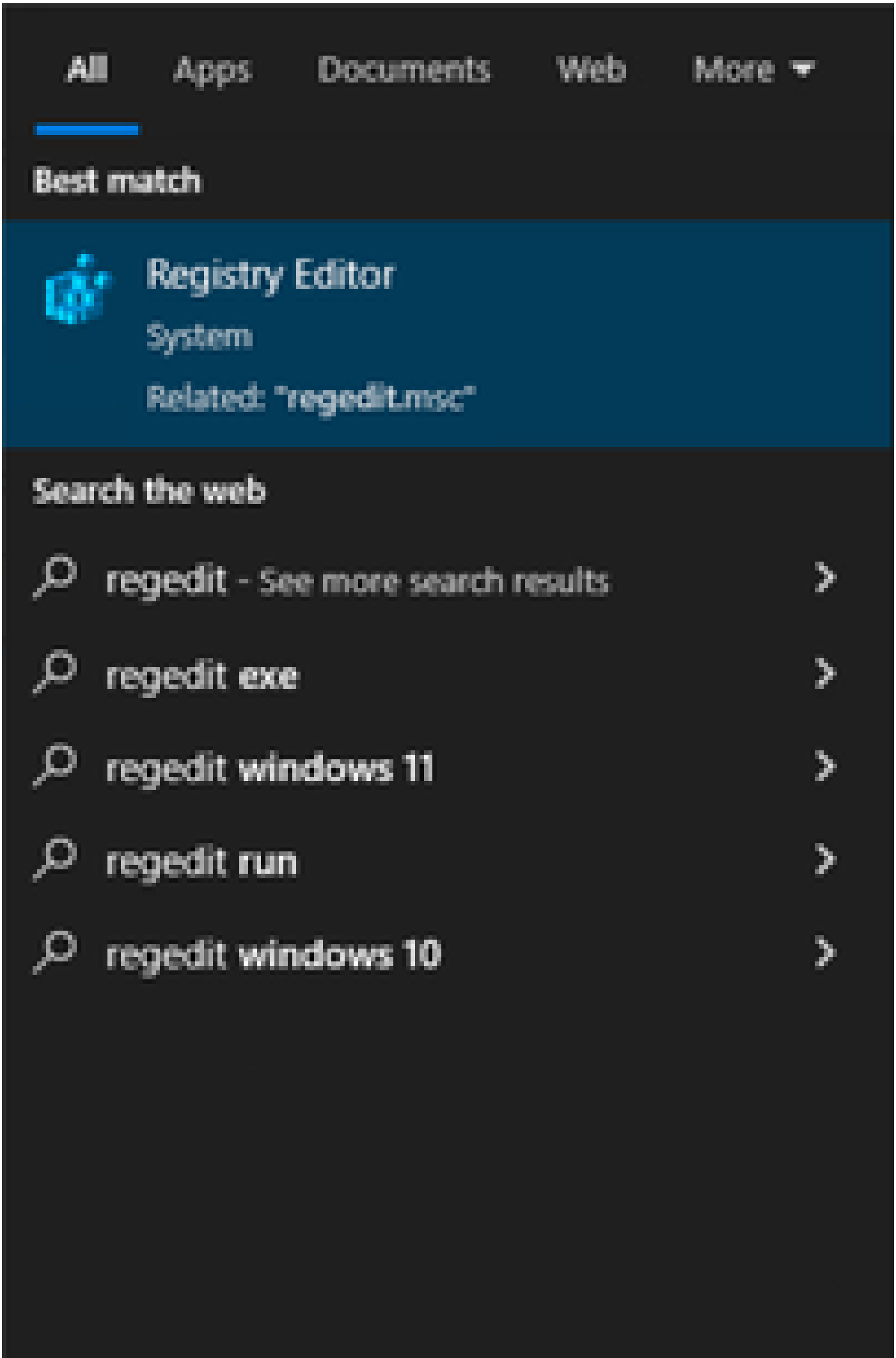
기본적으로 Windows 10, Windows 11 및 Windows Server 2012에서는 운영 체제에서 NAM(Network Access Manager)이 머신 인증에 필요한 머신 비밀번호를 검색하지 못하도록 합니다. 그 결과, 시스템 암호를 사용하는 시스템 인증은 레지스트리 수리가 적용되지 않는 한 작동하지 않습니다.

NAM이 머신 자격 증명에 액세스할 수 있게 하려면 클라이언트 데스크톱에 Microsoft KB 2743127 수정을 적용합니다.



주의: Windows 레지스트리를 잘못 편집하면 심각한 문제가 발생할 수 있습니다. 변경하기 전에 레지스트리를 백업해야 합니다.

1단계. Windows 검색 표시줄에서 regedit를 입력한 다음 레지스트리 편집기를 클릭합니다.

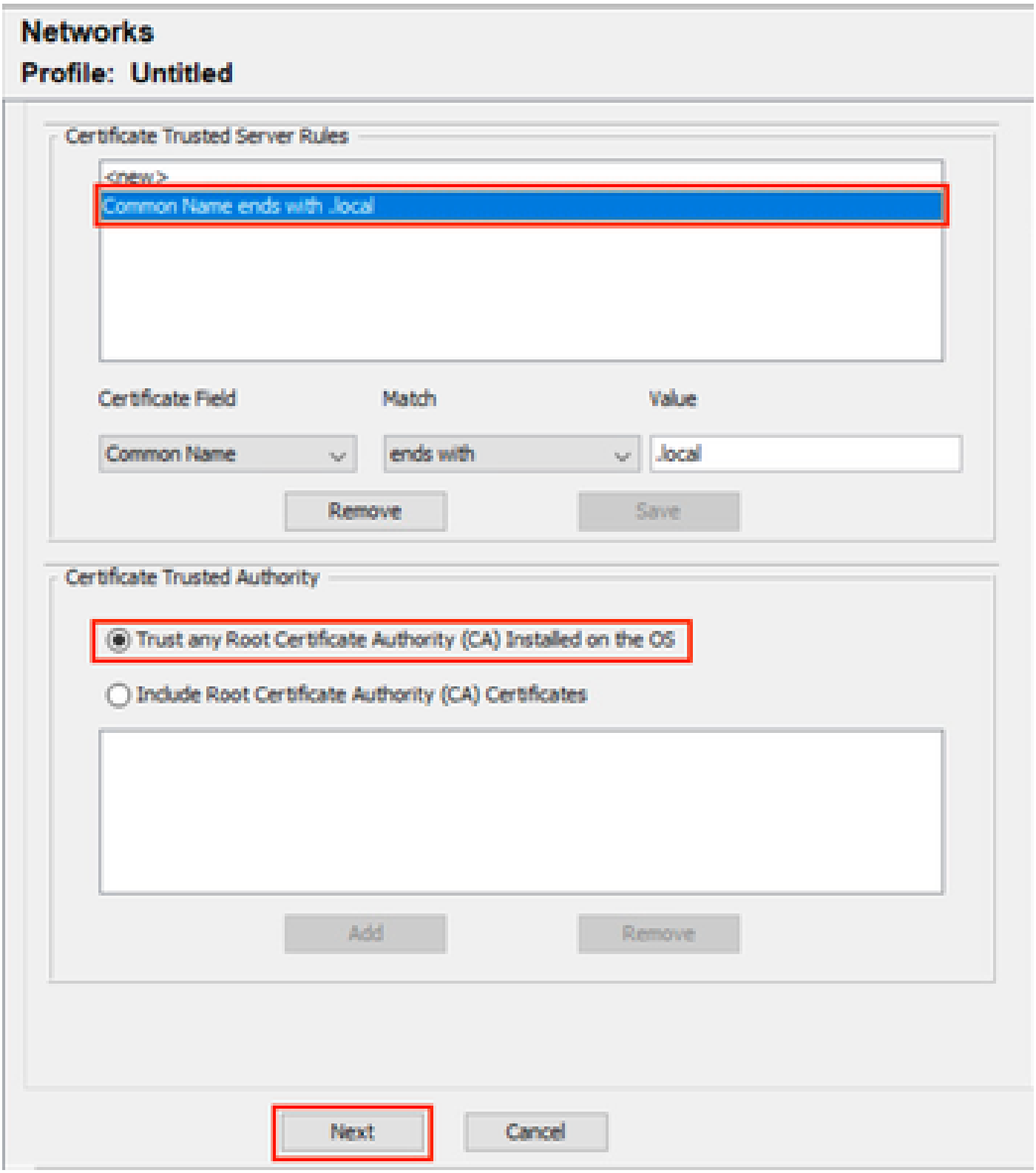

All
Apps
Documents
Web
More
Best match
Registry Editor
System
Related: "regedit.msc"
Search the web
regedit - See more search results
regedit exe
regedit windows 11
regedit run
regedit windows 10

이 예에서는 PSN 노드 인증서가 varshaah.varshaah.local에 의해 발급됩니다. 따라서 Common Name ends with .local 규칙이 사용됩니다. 이 규칙은 EAP-TTLS 흐름 중에 서버가 제공하는 인증서를 검증합니다.

또한 PSN(Policy Service Node) EAP 인증 인증서의 공통 이름을 지정할 수 있습니다.

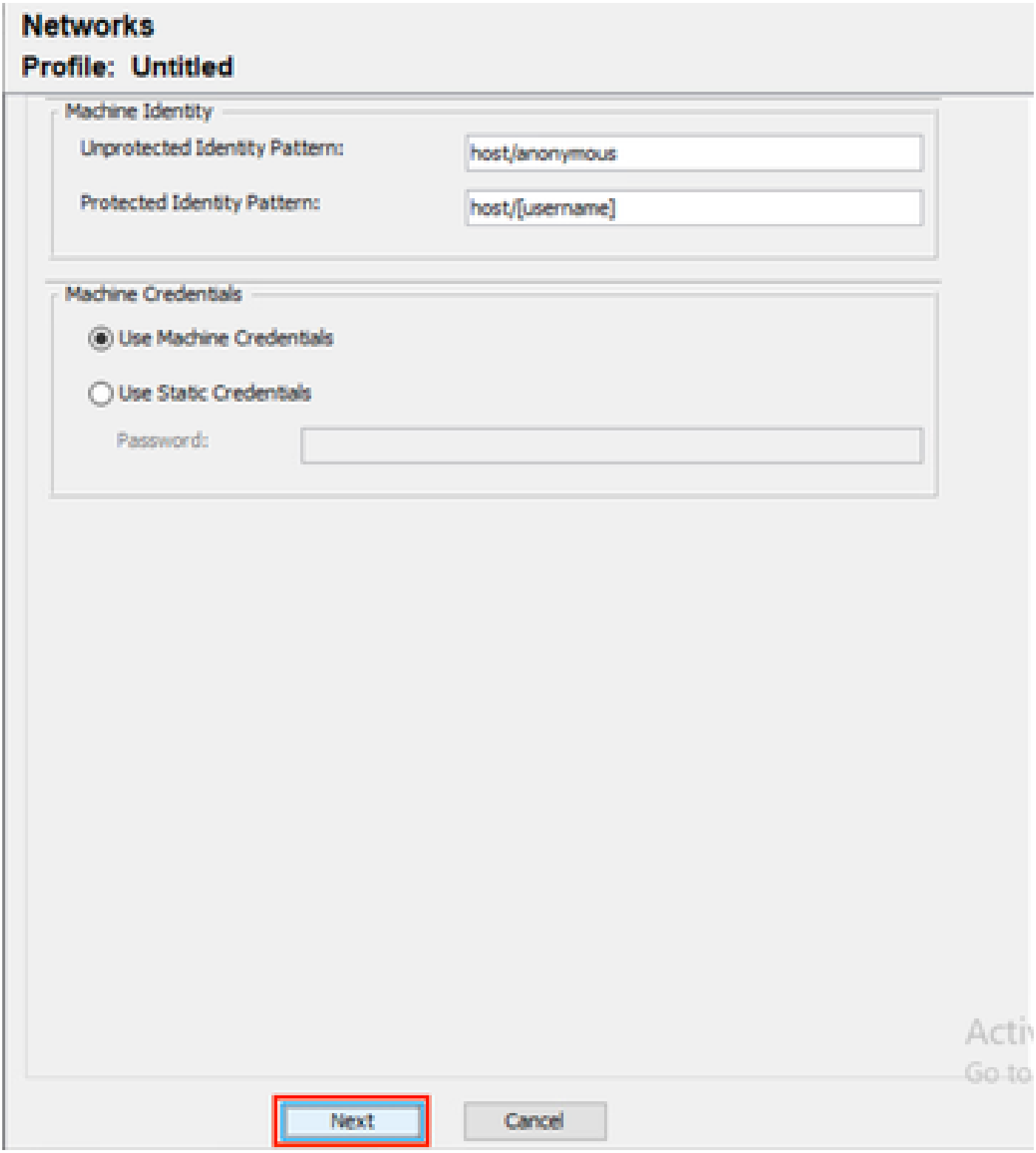
- Certificate Trusted Authority(인증서 신뢰 기관)에서 두 가지 옵션을 사용할 수 있습니다. 이 시나리오에서는 특정 CA 인증서를 추가하는 대신 OS에 설치된 Trust any Root Certificate Authority(CA) 옵션이 사용됩니다.

  이 옵션을 사용하면 Windows 디바이스는 Certificates(인증서) - Current User(현재 사용자) > Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) > Certificates(운영 체제에서 관리)에 포함된 인증서에 의해 서명된 모든 EAP 인증서를 신뢰합니다.
- 계속하려면 다음을 클릭합니다.



NAM 프로파일 편집기 인증서

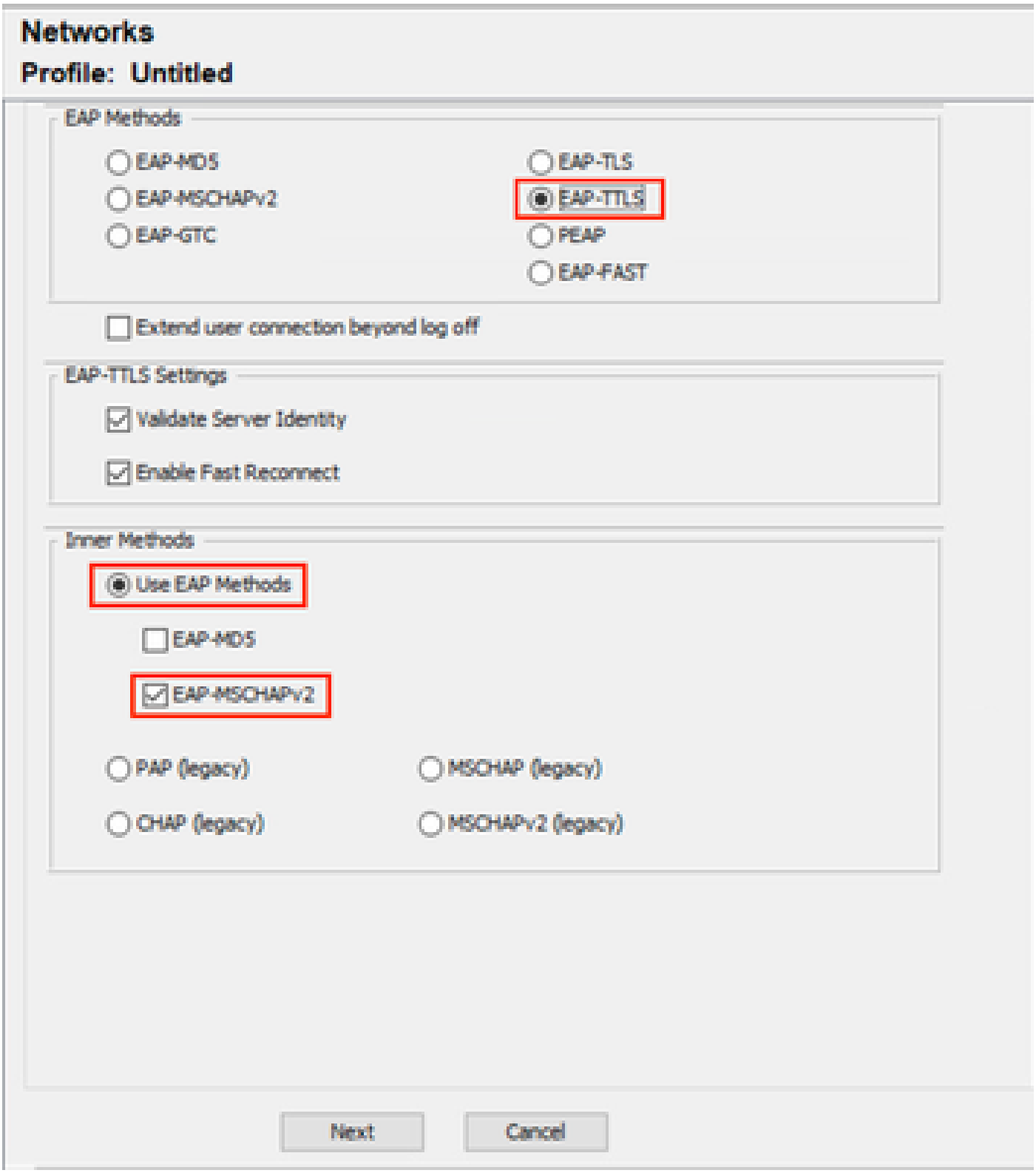
6단계. [머신 자격 증명] 섹션에서 [머신 자격 증명 사용]을 선택하고 [다음]을 클릭합니다.



NAM 프로파일 편집기 자격 증명

7단계. 사용자 인증 섹션을 구성합니다.

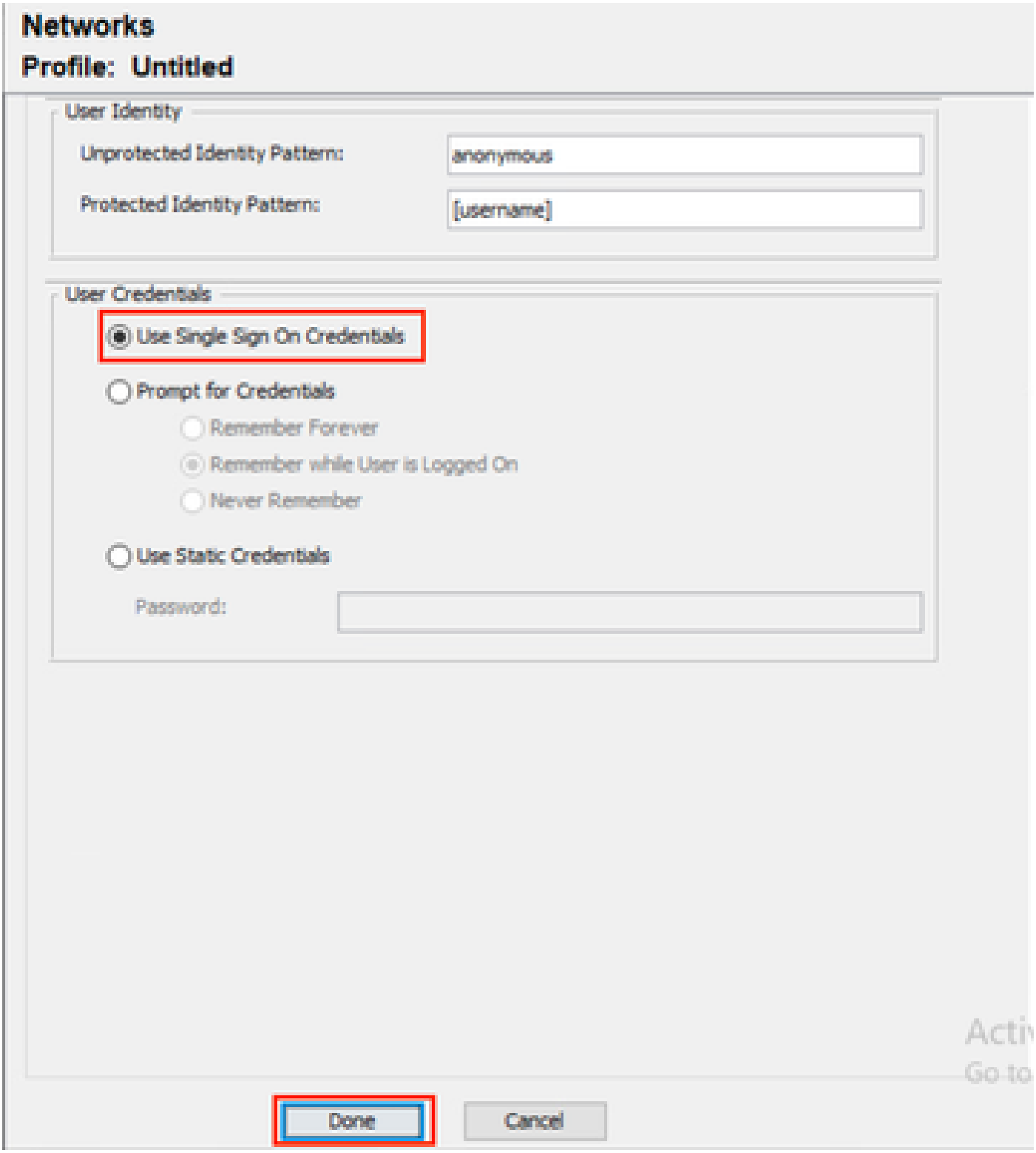
- EAP Methods(EAP 방법) 아래에서 EAP-TTLS를 선택합니다.
- Inner Methods(내부 방법) 아래에서 Use EAP Methods(EAP 방법 사용)를 선택하고 EAP-MSCHAPv2를 선택합니다.
- Next(다음)를 클릭합니다.



NAM 프로파일 편집기 사용자 인증

8단계. Certificates(인증서)에서 5단계에 설명된 것과 동일한 인증서 검증 규칙을 구성합니다.

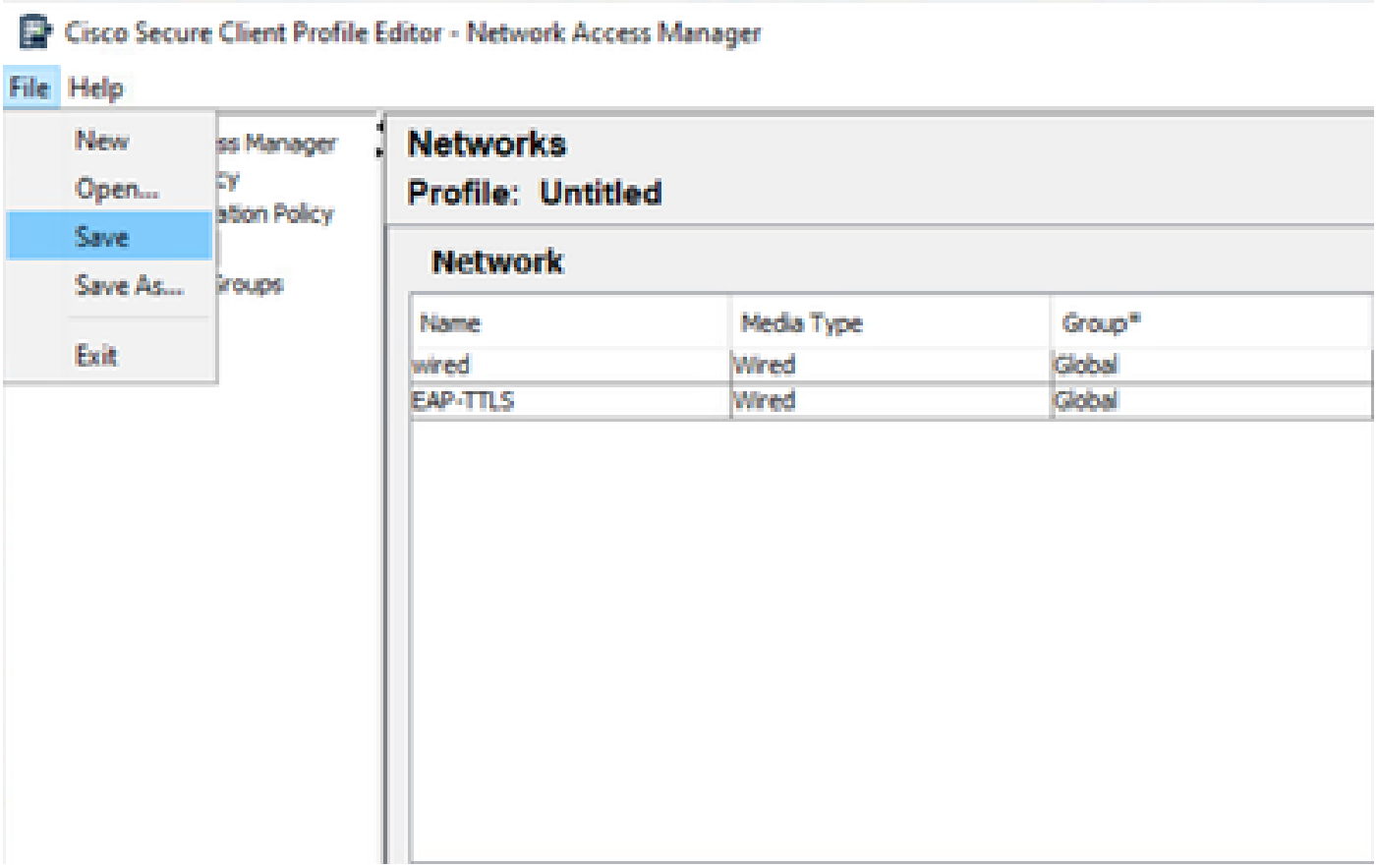
9단계. User Credentials(사용자 자격 증명)에서 Use Single Sign-On Credentials(단일 로그인 자격 증명 사용)를 선택한 다음 Done(완료)을 클릭합니다.



NAM 프로파일 편집기 사용자 자격 증명

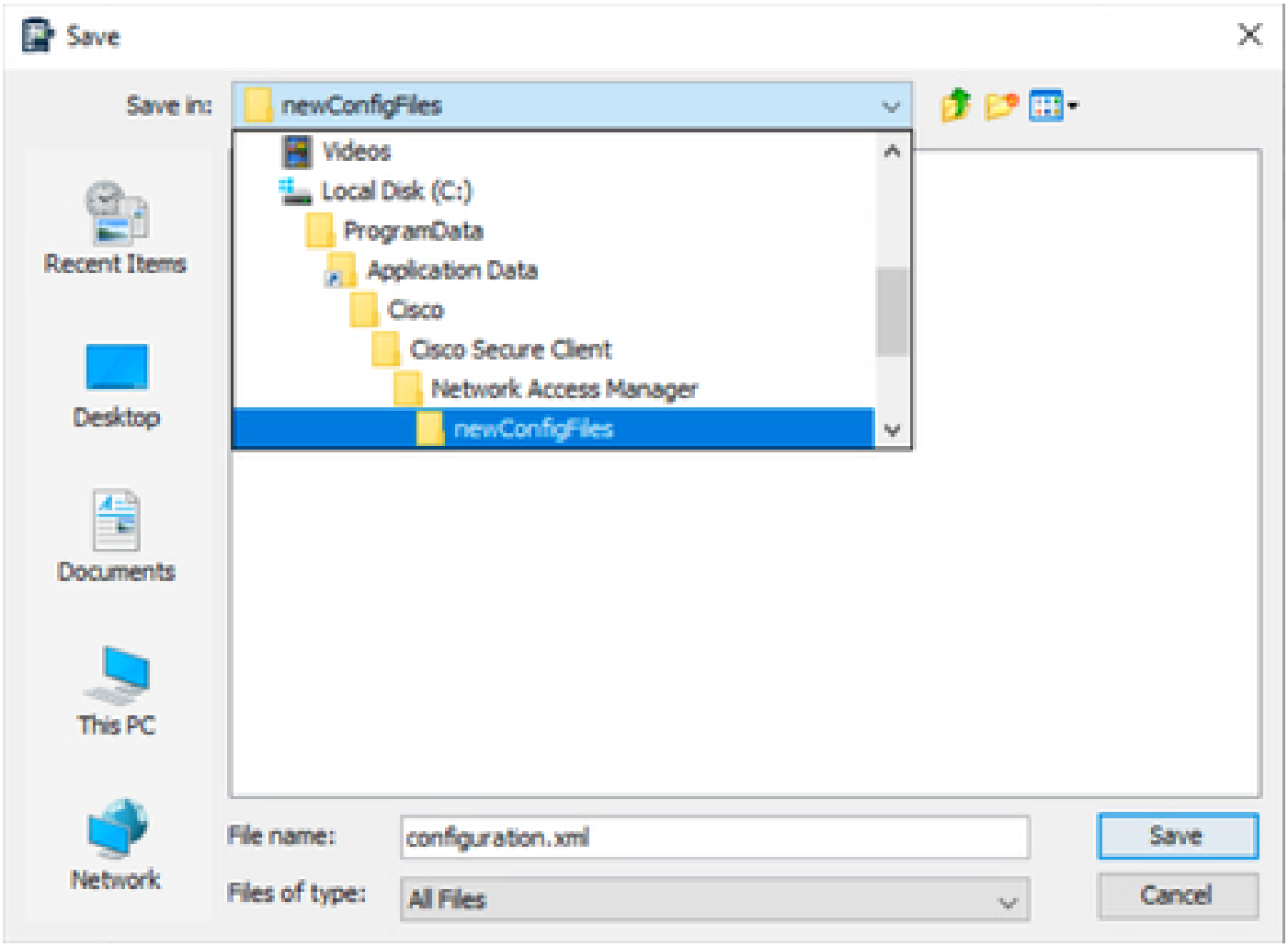
6부: 네트워크 컨피그레이션 파일 저장

1단계. File(파일) > Save(저장)를 클릭합니다.



NAM 프로파일 편집기 네트워크 컨피그레이션 저장

2단계. 새 ConfigFiles 폴더에 configuration.xml로 파일을 저장합니다.

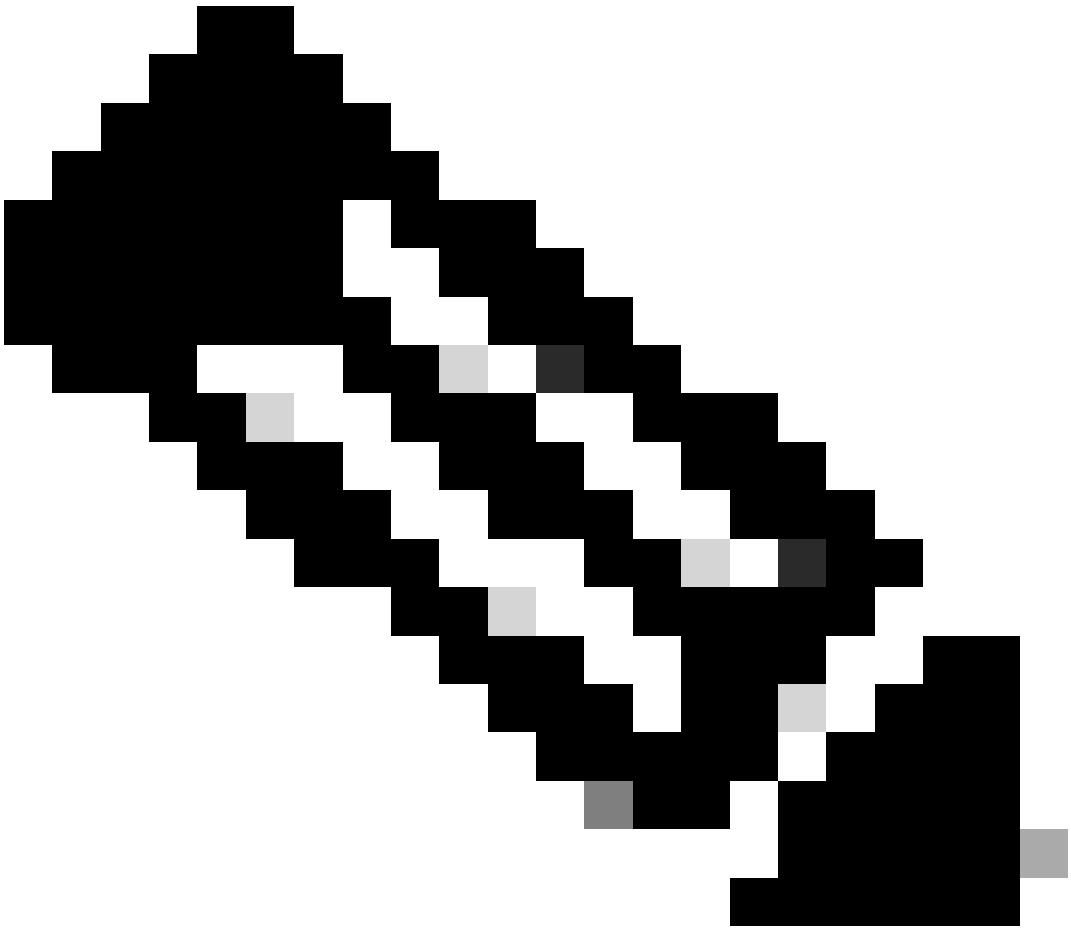


네트워크 컨피그레이션 저장

7부: 스위치에 AAA 구성

```
C9300-1#sh run aaa
!
aaa authentication dot1x default group labgroup
aaa authorization network default group labgroup
aaa accounting dot1x default start-stop group labgroup
aaa accounting update newinfo periodic 2880
!
!
!
!
aaa server radius dynamic-author
 client 10.76.112.135 server-key cisco
!
!
radius server labserver
 address ipv4 10.76.112.135 auth-port 1812 acct-port 1813
 key cisco
!
!
aaa group server radius labgroup
 server name labserver
!
```

```
!
!
!
aaa new-model
aaa session-id common
!
!



C9300-1(config)#dot1x system-auth-control
```



참고: dot1x system-auth-control 명령은 show running-config 출력에 나타나지 않지만 802.1X를 전역적으로 활성화해야 합니다.

802.1X용 스위치 인터페이스를 구성합니다.

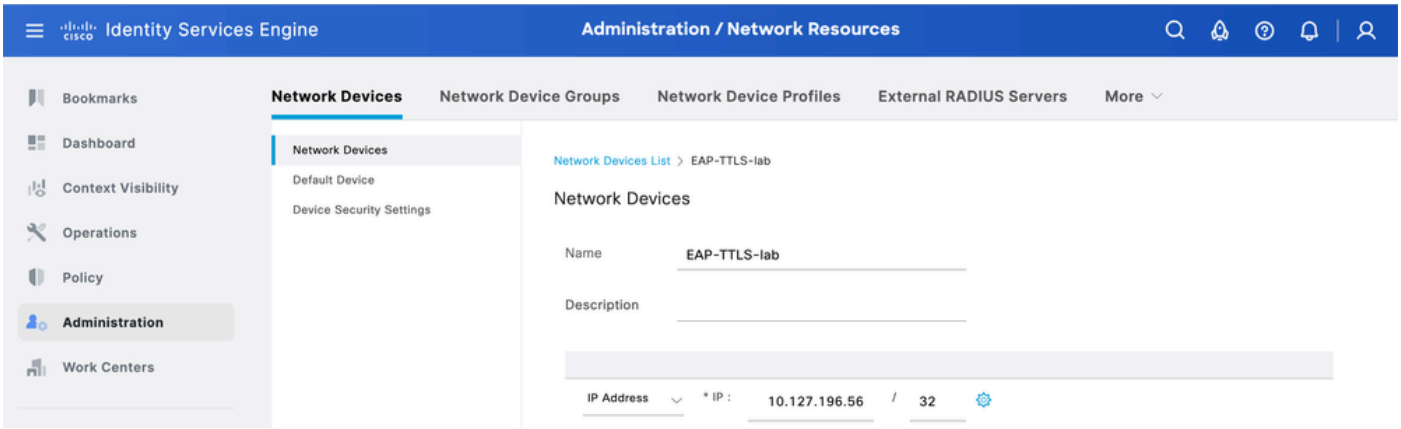
```
C9300-1(config)#do sh run int gig1/0/44
Building configuration...

Current configuration : 242 bytes
!
interface GigabitEthernet1/0/44
 switchport access vlan 96
 switchport mode access
 device-tracking
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-auth
 authentication periodic

 mab
 dot1x pae authenticator
end
```

8부: ISE 컨피그레이션

1단계. ISE에서 스위치를 구성합니다.

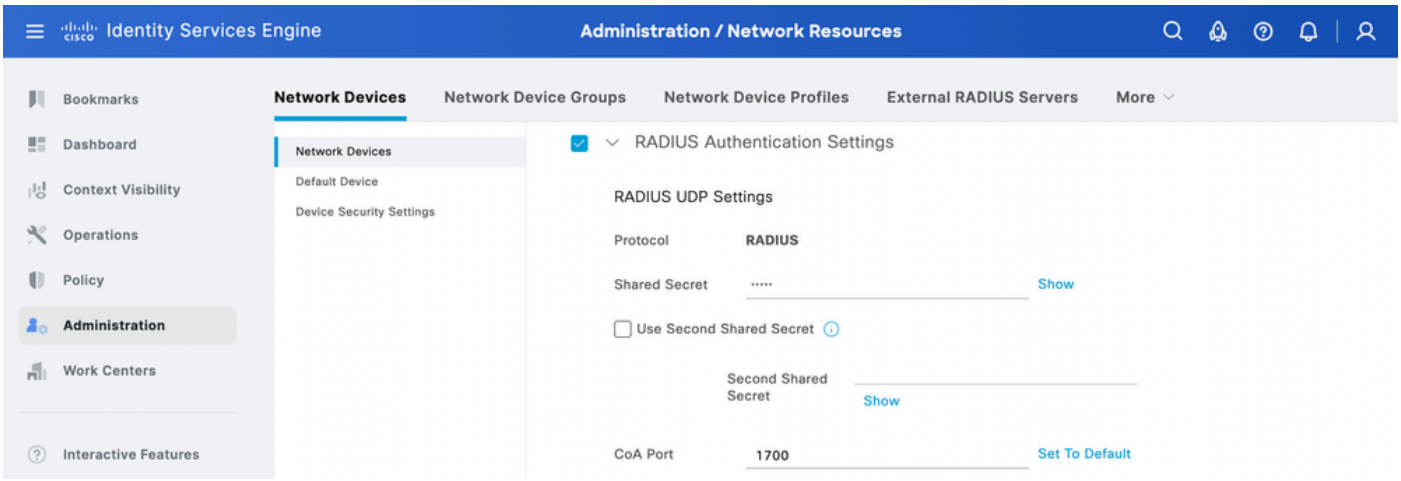
Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동하고 Add(추가)를 클릭합니다.

여기에 스위치 이름과 IP 주소를 입력합니다.



네트워크 디바이스 ISE 추가

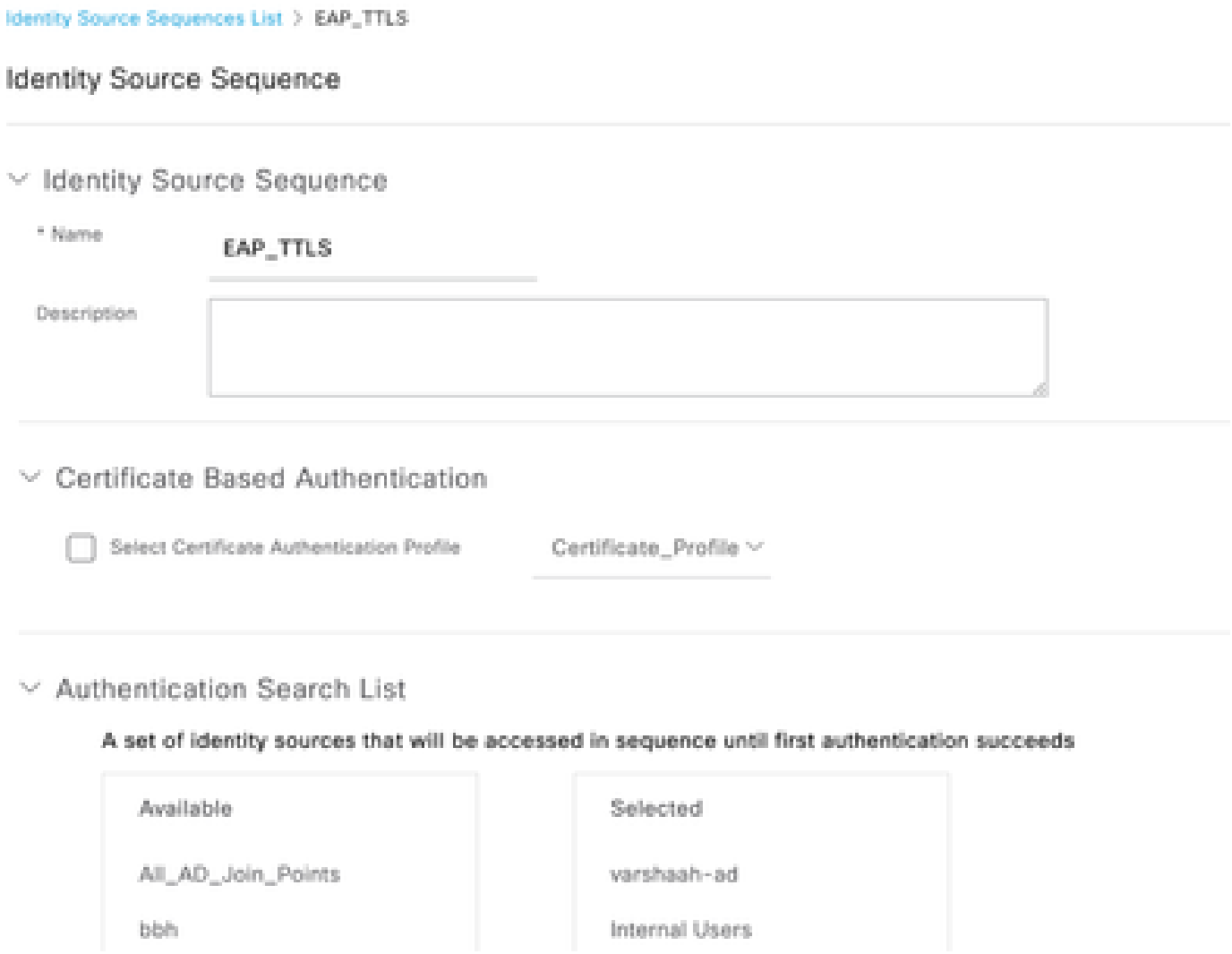
스위치에 이전에 구성한 것과 동일한 RADIUS 공유 암호를 입력합니다.



RADIUS 공유 암호 ISE

2단계. ID 소스 순서를 구성합니다.

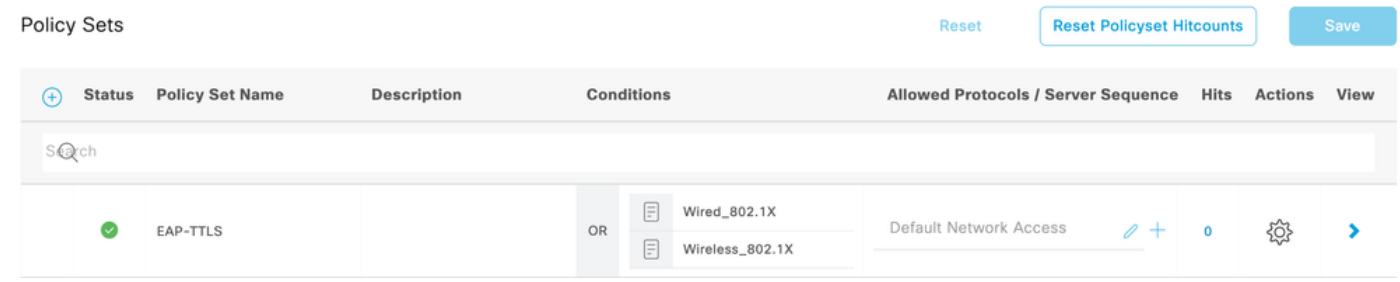
- Administration(관리) > Identity Management(ID 관리) > Identity Source Sequences(ID 소스 시퀀스)로 이동합니다.
- Add(추가)를 클릭하여 새 ID 소스 시퀀스를 생성합니다.
- Authentication Search List(인증 검색 목록)에서 ID 소스를 구성합니다.



ISE ID 소스 시퀀스

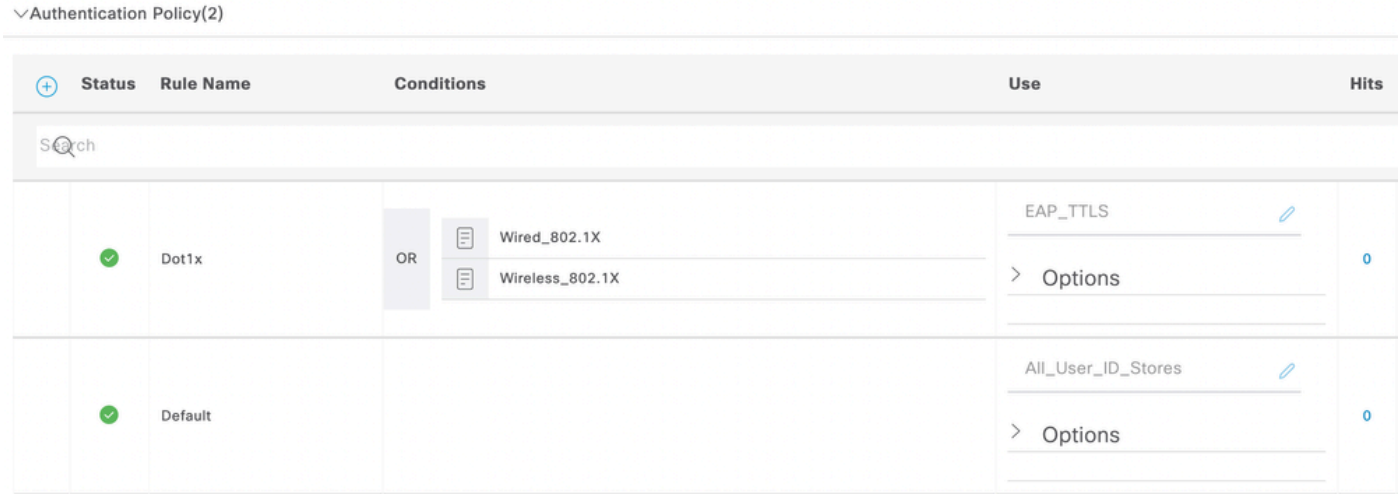
3단계. 정책 집합을 구성합니다.

Policy(정책) > Policy Sets(정책 집합)로 이동하여 새 정책 집합을 생성합니다. 조건을 Wired_802.1x 또는 Wireless_802.1x로 구성합니다. Allowed Protocols(허용되는 프로토콜)에서 Default Network Access(기본 네트워크 액세스)를 선택합니다.



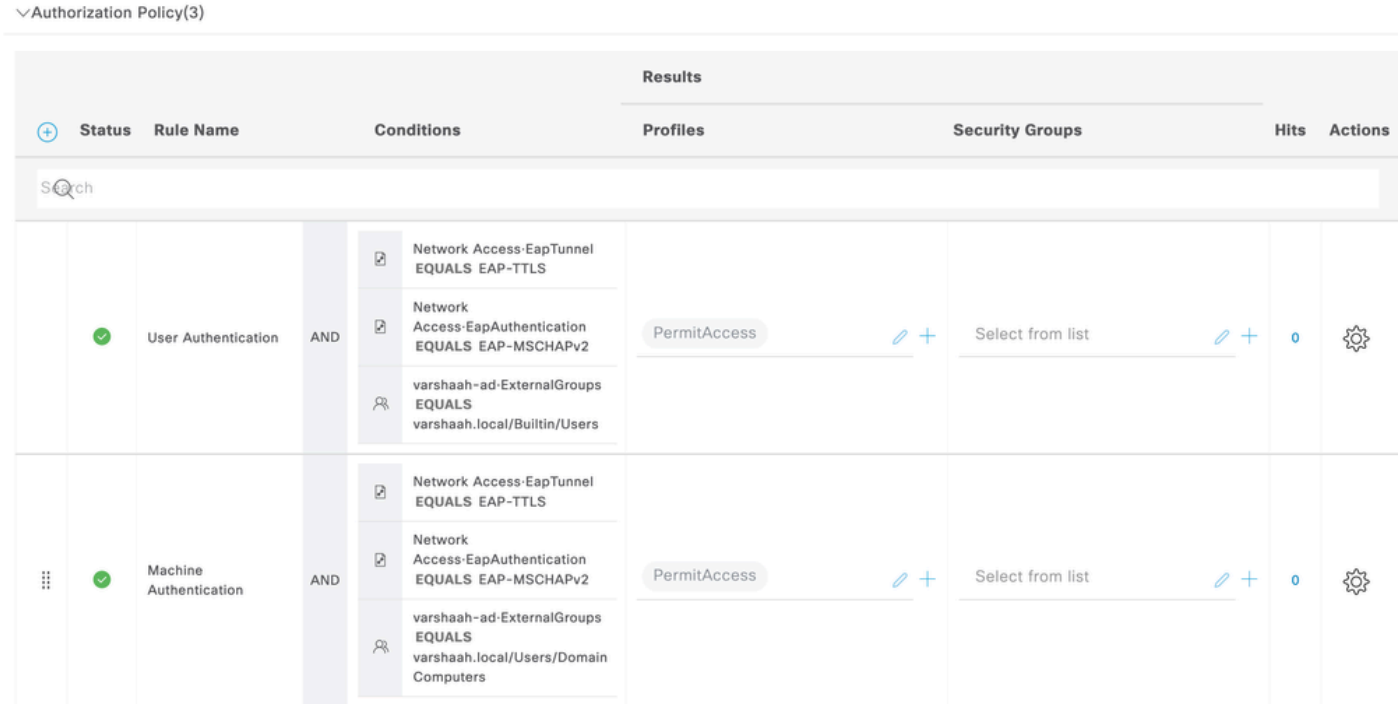
EAP-TTLS 정책 집합

dot1x에 대한 인증 정책을 만들고 4 단계에서 생성 된 ID 소스 시퀀스를 선택 합니다.



EAP-TTLS 인증 정책

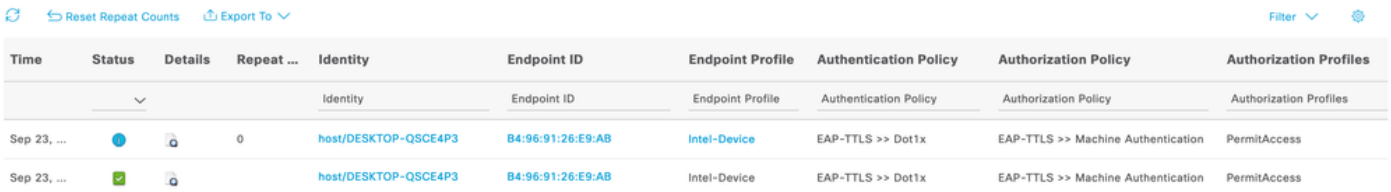
권한 부여 정책의 경우 3가지 조건으로 규칙을 생성합니다. 첫 번째 조건은 EAP-TTLS 터널이 사용되는 조건을 확인합니다. 두 번째 조건은 EAP-MSCHAPv2가 내부 EAP 방법으로 사용되는지 확인합니다. 세 번째 조건은 각각의 AD 그룹을 확인합니다.



Dot1x 권한 부여 정책

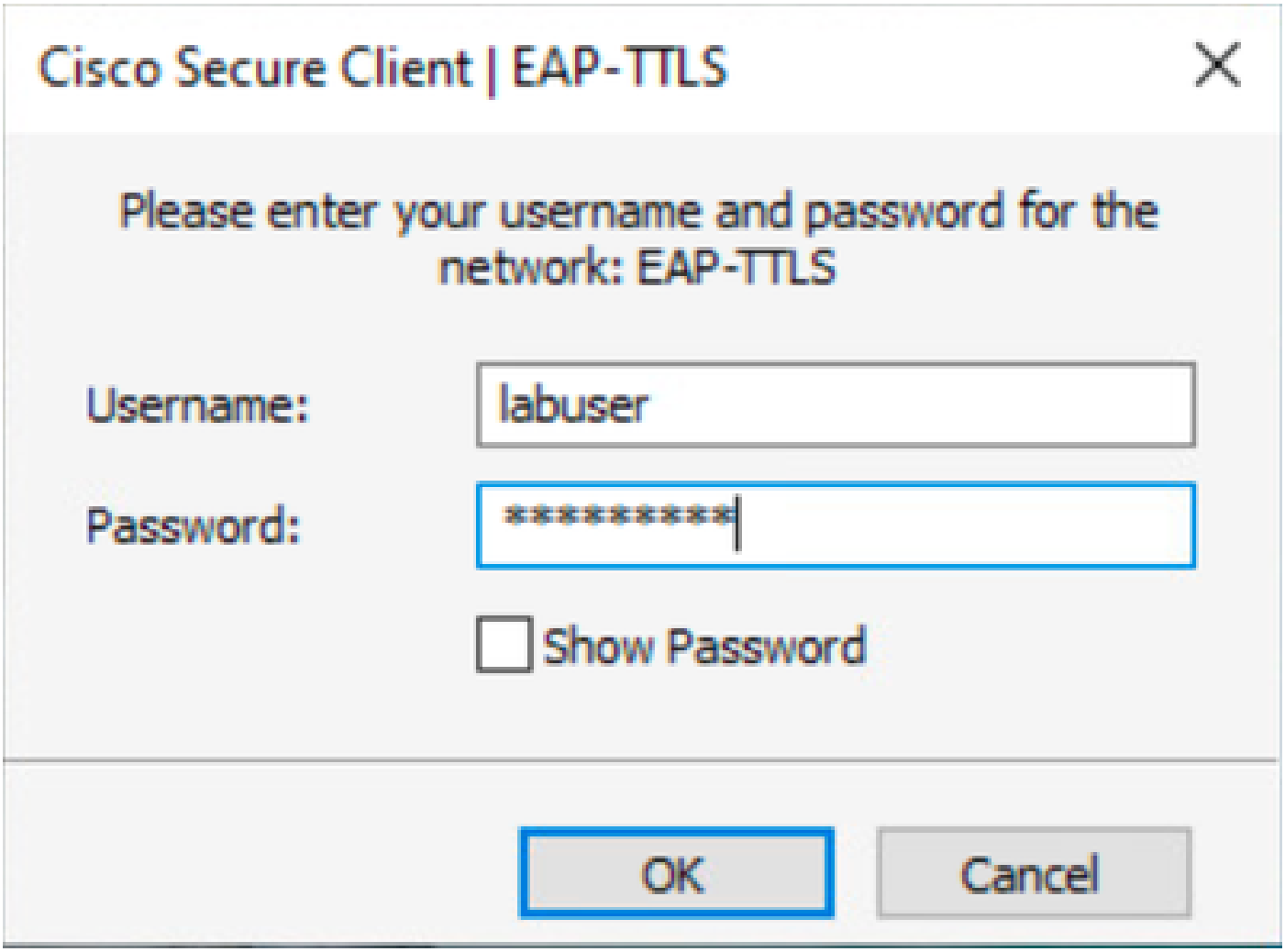
다음을 확인합니다.

Windows 10 시스템을 다시 부팅하거나 로그아웃한 다음 로그인할 수 있습니다. Windows 로그인 화면이 표시될 때마다 머신 인증이 트리거됩니다.

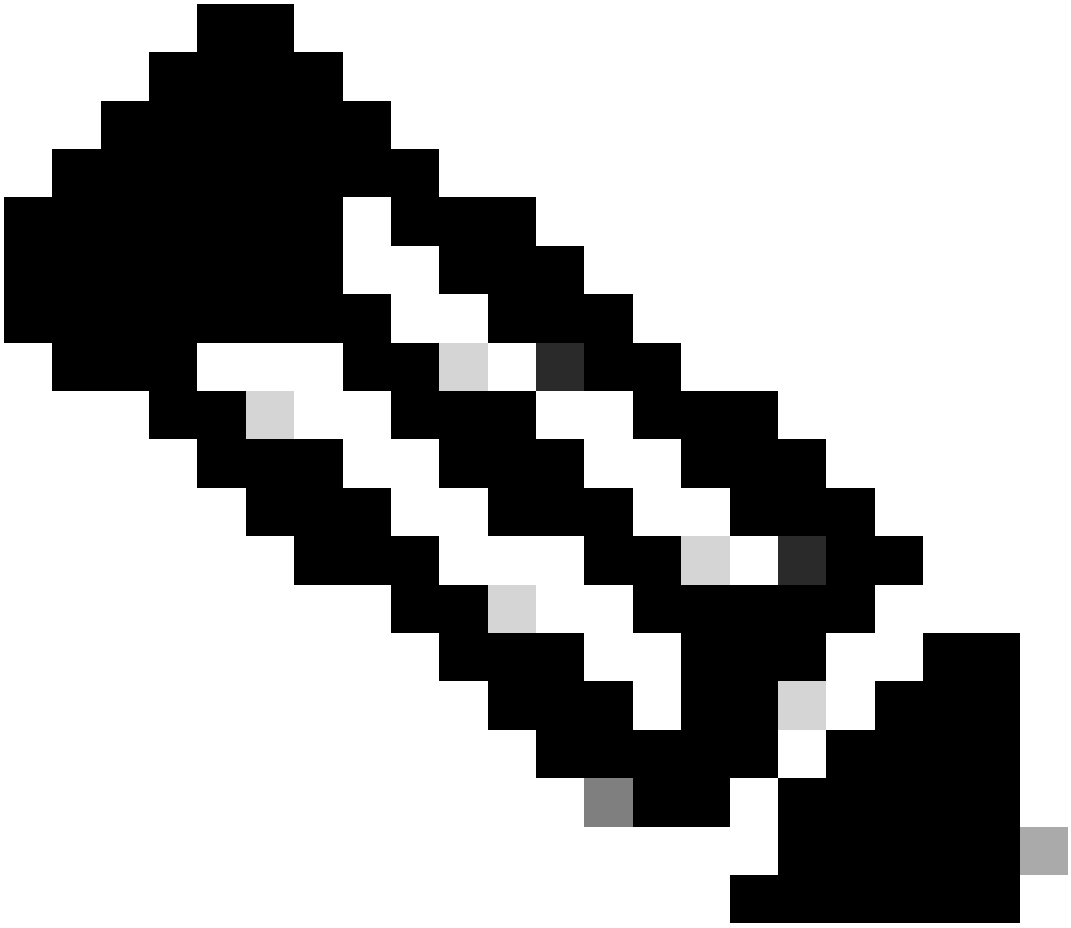


라이브 로그 시스템 인증

자격 증명을 사용하여 PC에 로그인하면 사용자 인증이 트리거됩니다.

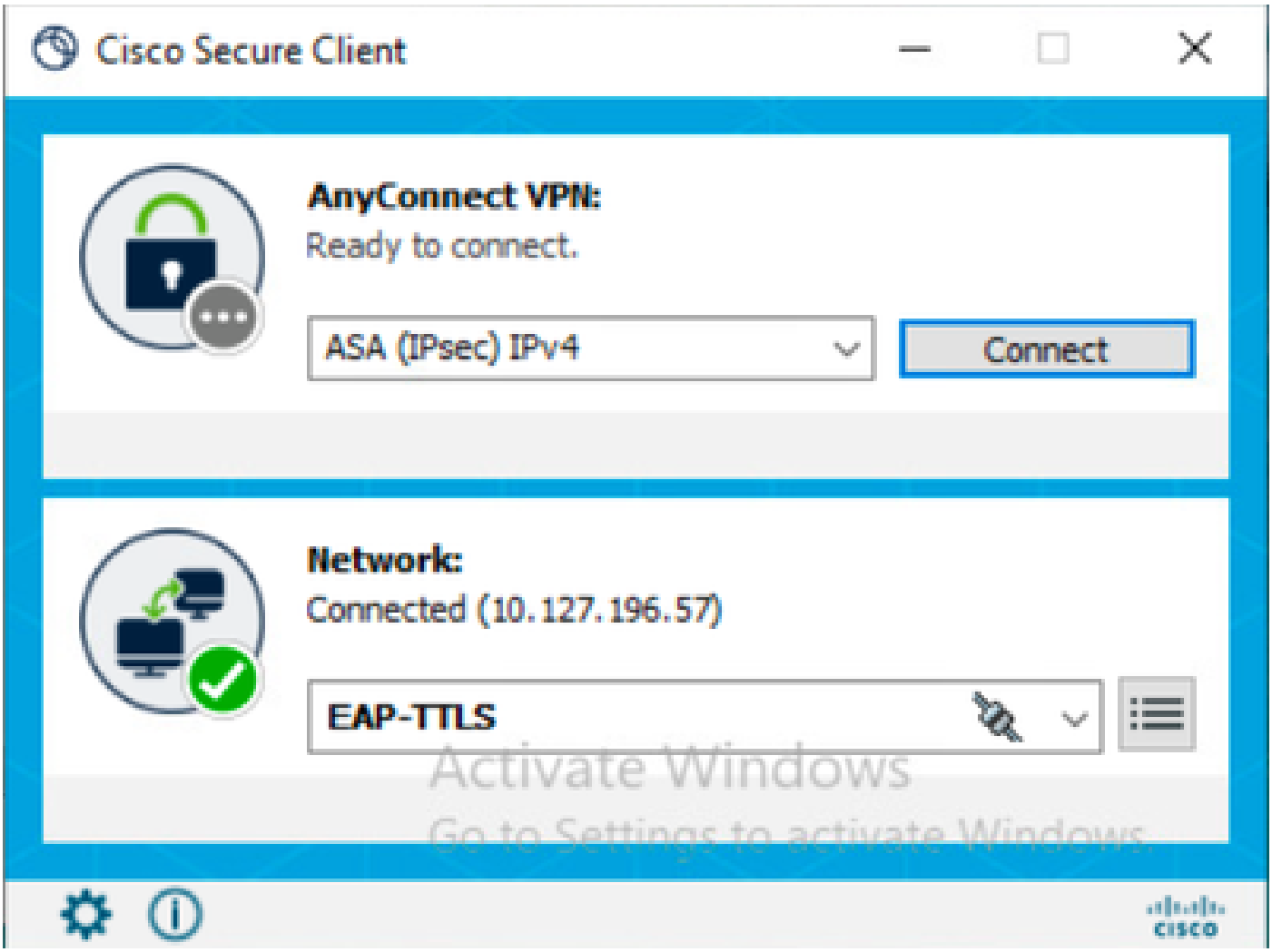


사용자 인증 자격 증명

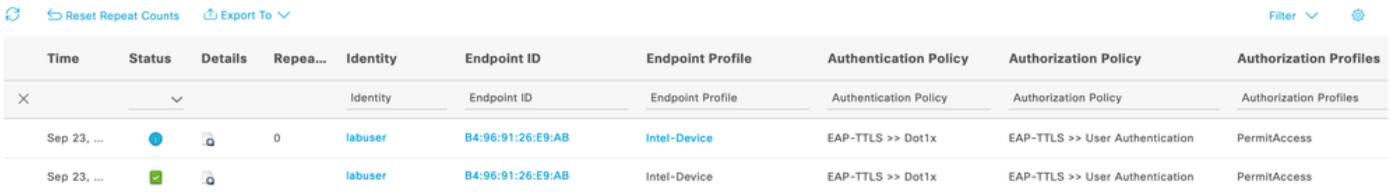


참고: 이 예에서는 인증에 Active Directory 사용자 자격 증명을 사용합니다. 또는 Cisco ISE에서 내부 사용자를 생성하고 로그인에 해당 자격 증명을 사용할 수 있습니다.

자격 증명을 입력하고 성공적으로 확인하면 엔드포인트가 사용자 인증을 통해 네트워크에 연결됩니다.



EAP-TTLS 연결됨



Reset Repeat Counts | Export To | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
				Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
Sep 23, ...			0	labuser	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> User Authentication	PermitAccess
Sep 23, ...				labuser	B4:96:91:26:E9:AB	Intel-Device	EAP-TTLS >> Dot1x	EAP-TTLS >> User Authentication	PermitAccess

라이브 로그 사용자 인증

ISE RADIUS 라이브 로그 분석

이 섹션에서는 성공적인 머신 및 사용자 인증을 위한 RADIUS 라이브 로그 항목을 보여줍니다.

머신 인증

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message 12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** **11806**

Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24431 Authenticating machine against Active Directory - varshaah-ad 24325 Resolving identity - host/DESKTOP-QSCE4P3 ... ... 24343 RPC Logon request succeeded - DESKTOP-QSCE4P3$@varshaah.local **24470 Machine authentication against Active Directory is successful - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - host/DESKTOP-QSCE4P3 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

사용자 인증

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message 12804 Extracted TLS Finished message 12801 Prepared TLS ChangeCipherSpec message 12802 Prepared TLS Finished message **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - labuser@varshaah.local ... ... 24343 RPC Logon request succeeded - labuser@varshaah.local **24402 User authentication against Active Directory succeeded - varshaah-ad** 22037 Authentication Passed ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method **12975 EAP-TTLS authentication succeeded** ... ... 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore - labuser 24211 Found Endpoint in Internal Endpoints IDStore 15048 Queried PIP - Network Access.Device IP Address 15048 Queried PIP - Network Access.EapTunnel **15016 Selected Authorization Profile - PermitAccess** ... ... 11002 Returned RADIUS Access-Accept

NAM 로그 분석

NAM 로그는, 특히 확장 로깅을 활성화한 후, 대량의 데이터를 포함하며, 대부분은 관련이 없으며 무시될 수 있습니다. 이 섹션에서는 NAM이 네트워크 연결을 설정하는 각 단계를 보여 주는 디버그 행을 나열합니다. 로그를 통해 작업할 때 이러한 핵심 구는 문제와 관련된 로그의 일부를 찾는 데 도움이 될 수 있습니다.

머신 인증

```
2160: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: 80
```

클라이언트는 네트워크 스위치로부터 EAP-TTLS 패킷을 수신하여 EAP-TTLS 세션을 시작합니다. 머신 인증 터널의 시작 지점입니다.

```
2171: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: EA
2172: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
2173: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11812][comp=SAE]: CER
```

클라이언트는 ISE에서 Server Hello를 수신하고 서버 인증서의 유효성 검사를 시작합니다 (CN=varshaah.varshaah.local). 인증서는 클라이언트의 신뢰 저장소에 있으며 유효성 검사를 위해 추가됩니다.

```
2222: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Validating th
2223: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.696 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Server certif
```

서버 인증서가 성공적으로 검증되어 TLS 터널 설정이 완료되었습니다.

```
2563: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2564: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11812][comp=SAE]: NE
2565: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.789 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

클라이언트는 인증이 통과되었음을 알립니다. 인터페이스가 차단 해제되고 내부 상태 머신이 USER_T_NOT_DISCONNECTED로 전환되며, 머신이 이제 트래픽을 전달할 수 있음을 나타냅니다 .

```
2609: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2610: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2611: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2612: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2613: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
2614: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11824][comp=SAE]: NE
2615: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.821 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11768]: Network EAP-
```

어댑터에서 인증된 것으로 보고하고 NAM AccessStateMachine이 ACCESS_AUTHENTICATED로 전환됩니다. 그러면 시스템이 성공적으로 인증을 완료했으며 전체 네트워크 액세스 권한을 갖게 됩니다.

사용자 인증

```
100: DESKTOP-QSCE4P3: Sep 25 2025 14:01:26.669 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Network EAP-TT
```

NAM 클라이언트가 EAP-TTLS 연결 프로세스를 시작합니다.

```
195: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Binding adapte
198: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
```

NAM은 물리적 어댑터를 EAP-TTLS 네트워크에 바인딩하고 ACCESS_ATTACHED 상태로 이동하여 어댑터가 인증할 준비가 되었음을 확인합니다.

```
204: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3252]: Network EAP-TT
247: DESKTOP-QSCE4P3: Sep 25 2025 15:09:11.780 +0900: %csc_nam-7-DEBUG_MSG: %[tid=3680][comp=SAE]: STAT
```

클라이언트가 ATTACHED에서 CONNECTING으로 전환되고 802.1X Exchange가 시작됩니다.

```
291: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.388 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
```

클라이언트는 인증 프로세스를 트리거하기 위해 EAPOL-Start를 전송합니다.

```
331: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: PORT
332: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: 8021
340: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.435 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6644][comp=SAE]: EAP
```

스위치가 ID를 요청하면 클라이언트는 외부 ID로 응답할 준비를 합니다.

```
402: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9580]: EAP-CB: creden
422: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: processin
460: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.685 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

NAM이 외부 ID를 전송합니다. 기본적으로 이는 익명으로, 교환이 사용자 인증(시스템 아님)을 위한 것임을 나타냅니다.

```
488: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP sugges
489: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-6-INFO_MSG: %[tid=6088]: EAP: EAP reques
490: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: EAP metho
```

```
491: DESKTOP-QSCE4P3: Sep 25 2025 13:15:36.497 +0900: %csc_nam-7-DEBUG_MSG: %[tid=6088]: EAP: credentia
```

클라이언트와 서버 모두 EAP-TTLS를 외부 방법으로 사용하는 데 동의합니다.

```
660: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
661: DESKTOP-QSCE4P3: Sep 25 2025 14:01:27.185 +0900: %csc_nam-7-DEBUG_MSG: %[tid=8296][comp=SAE]: EAP
```

클라이언트는 Client Hello를 전송하고 Server Hello를 수신하며, 여기에는 ISE 인증서가 포함됩니다.

```
706: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: 802
717: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
718: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.967 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
719: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-6-INFO_MSG: %[tid=11932][comp=SAE]: CERT
726: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
```

서버 인증서가 표시됩니다. 클라이언트는 CN varshaah.varshaah.local을 조회하고 일치 항목을 찾은 다음 인증서를 검증합니다. X.509 인증서가 점검되는 동안 핸드셰이크가 일시 중지됩니다.

```
729: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EAP
730: DESKTOP-QSCE4P3: Sep 25 2025 13:04:31.983 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EAP
1110: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1111: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.044 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

터널이 설정됩니다. 이제 NAM은 내부 인증을 위해 보호된 ID와 자격 증명을 요청하고 준비합니다.

```
1527: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1528: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.169 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11916][comp=SAE]: EA
1573: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1574: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
1575: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.184 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: EA
```

TLS 핸드셰이크가 완료되었습니다. 이제 내부 인증을 위해 보안 터널이 설정됩니다.

```
1616: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-6-INFO_MSG: %[tid=9664]: Protected iden
1620: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
1689: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9664]: Auth[EAP-TTLS
```

보호된 ID(사용자 이름)는 ISE에서 전송 및 수락됩니다.

```
1708: DESKTOP-QSCE4P3: Sep 25 2025 14:01:46.277 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9456][comp=SAE]: EAP
1738: DESKTOP-QSCE4P3: Sep 25 2025 13:01:44.758 +0900: %csc_nam-6-INFO_MSG: %[tid=11768]: Protected pas
1741: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.200 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
```

ISE에서 비밀번호를 요청합니다. NAM은 TLS 터널 내에서 보호된 비밀번호를 전송합니다.

```
1851: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1852: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1853: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=9644]: Auth[EAP-TTLS
1854: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
1855: DESKTOP-QSCE4P3: Sep 25 2025 13:04:42.262 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11932][comp=SAE]: STA
```

ISE는 비밀번호를 검증하고 EAP-Success를 전송하고 NAM이 AUTHENTICATED로 전환됩니다. 이때 사용자 인증이 완료되고 클라이언트는 네트워크 액세스가 허용됩니다.

문제 해결

Cisco ISE 및 스위치 통합과 관련된 NAM(Network Access Manager) 문제를 트러블슈팅할 때 세 가지 구성 요소 모두에서 로그를 수집해야 합니다. NAM(Secure Client), Cisco ISE 및 스위치.

NAM(Secure Client) 로그

1. 다음 단계를 수행하여 NAM 확장 로깅을 활성화합니다.
2. 문제를 재현합니다. 네트워크 프로필이 적용되지 않을 경우 보안 클라이언트에서 네트워크 복구를 실행합니다.
3. DART(Diagnostics and Reporting Tool)를 사용하여 DART 번들을 수집합니다.

Cisco ISE 로그

인증 및 디렉토리 상호 작용을 캡처하기 위해 ISE에서 다음 디버그를 활성화합니다.

- 런타임 AAA
- nsf
- nsf 세션

스위치 로그

기본 디버그

```
request platform software trace rotate all
set platform software trace smd switch active R0 radius debug
set platform software trace smd switch active R0 aaa debug
set platform software trace smd switch active R0 dot1x-all debug
set platform software trace smd switch active R0 eap-all debug
debug radius all
```

고급 디버깅(필요한 경우)

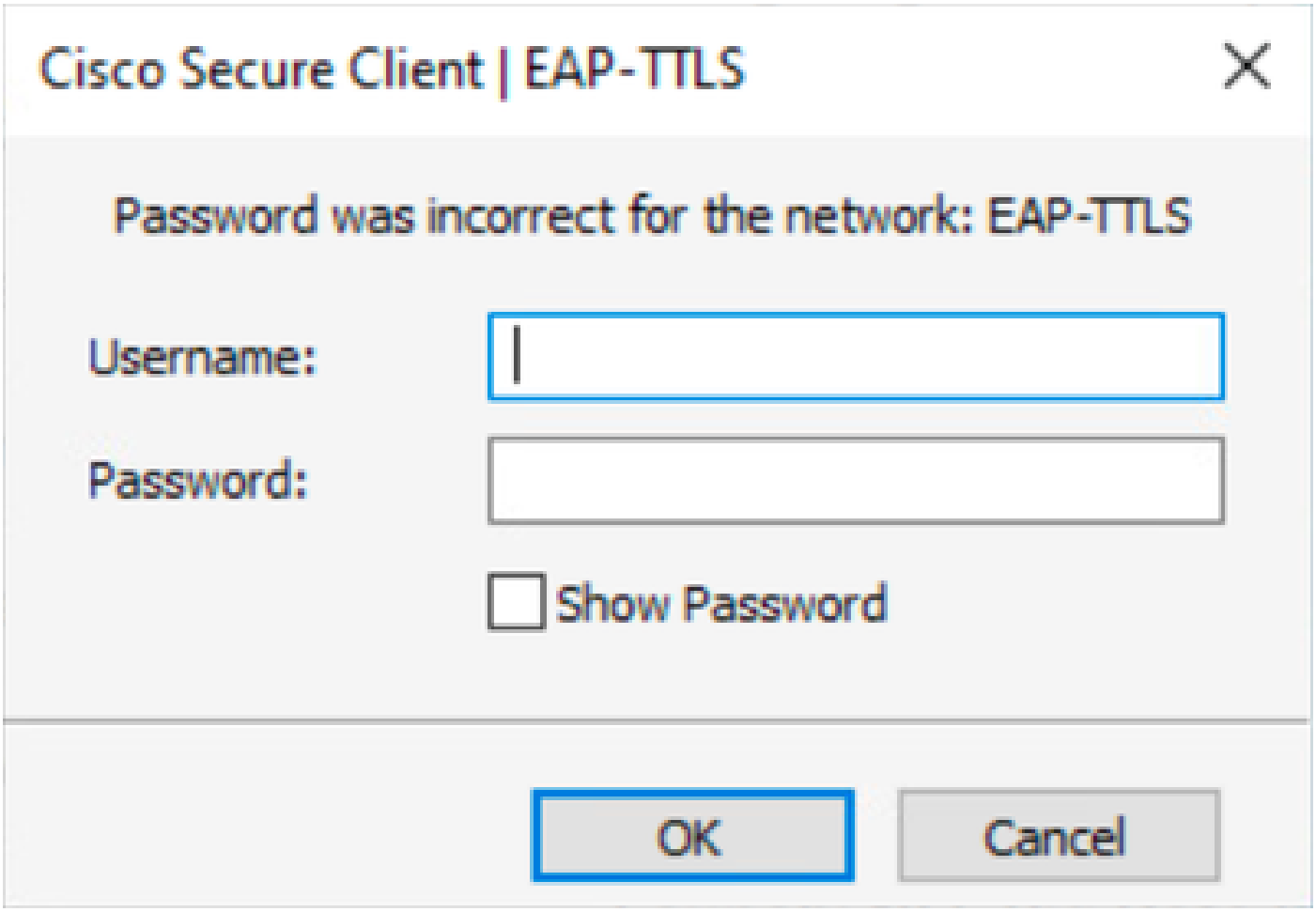
```
set platform software trace smd switch active R0 epm-all debug
set platform software trace smd switch active R0 pre-all debug
```

Show 명령

```
show version
show debugging
show running-config aaa
show authentication session interface gix/x details
show dot1x interface gix/x
show aaa servers
show platform software trace message smd switch active R0
```

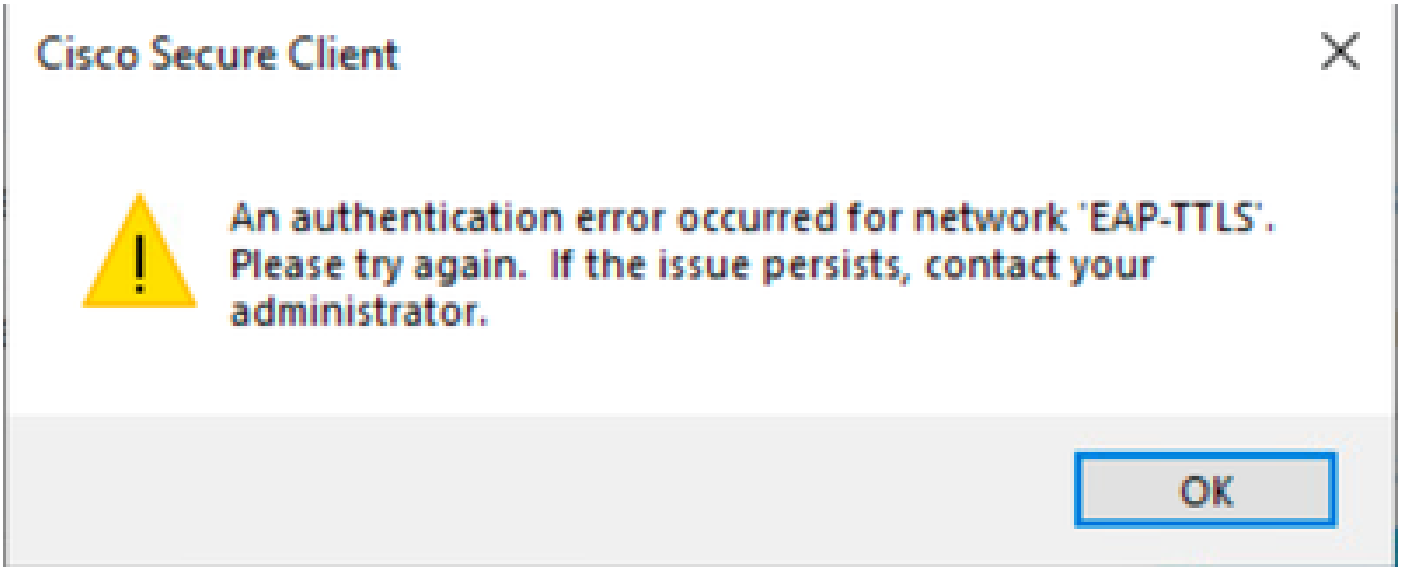
잘못된 자격 증명으로 인한 사용자 인증 실패

사용자가 잘못된 자격 증명을 입력하면 Secure Client는 네트워크에 대해 일반 비밀번호가 올바르지 않음을 표시합니다. EAP-TTLS 메시지입니다. 화면 오류는 잘못된 사용자 이름 또는 암호로 인해 발생한 문제인지 여부를 지정하지 않습니다.



잘못된 암호 오류

인증이 두 번 연속으로 실패할 경우 보안 클라이언트에서는 다음 메시지를 표시합니다. 'EAP-TTLS' 네트워크에 대해 인증 오류가 발생했습니다. 다시 시도하여 주십시오. 문제가 계속되면 관리자에게 문의하십시오.



사용자 인증 문제

원인을 확인하려면 NAM 로그를 검토하십시오.

1. 잘못된 암호:

사용자가 잘못된 비밀번호를 입력하면 NAM 로그에 이 출력과 유사한 항목이 표시됩니다.

```
3775: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3776: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.921 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3777: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.922 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
```

Cisco ISE 라이브 로그에서 해당 이벤트는 다음과 같이 나타납니다.

Event	5400 Authentication failed
Failure Reason	24408 User authentication against Active Directory failed since user has entered the wrong password
Resolution	Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Root cause	User authentication against Active Directory failed since user has entered the wrong password

잘못된 암호

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity 10 **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge 0** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 0 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response 0 **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - varshaah-ad 0 24430 Authenticating user against Active Directory - varshaah-ad 0 24325 Resolving identity - labuser@varshaah.local 4 24313 Search for matching accounts at join point - varshaah.local 0 24319 Single matching account found in forest - varshaah.local 0 24323 Identity resolution detected single matching account 0 **24344 RPC Logon request failed - STATUS_WRONG_PASSWORD, ERROR_INVALID_PASSWORD, labuser@varshaah.local 20 24408 User authentication against Active Directory failed since user has entered the wrong password - varshaah-ad 1** ... ... 11823 EAP-MSCHAP authentication attempt failed ... ... 11815 Inner EAP-MSCHAP authentication failed 0 ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11003 Returned RADIUS Access-Reject

2. 잘못된 사용자 이름:

사용자가 잘못된 사용자 이름을 입력하면 NAM 로그에 이 출력과 유사한 항목이 표시됩니다.

```
3788: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300][comp=SAE]: EA
3789: DESKTOP-QSCE4P3: Oct 02 2025 15:29:39.923 +0900: %csc_nam-7-DEBUG_MSG: %[tid=11300]: EAP-CB: EAP
```

Cisco ISE 라이브 로그에서 해당 이벤트는 다음과 같이 나타납니다.

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resoultion settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).

잘못된 사용자 이름

11001 Received RADIUS Access-Request 11017 RADIUS created a new session ... ... 11507 Extracted EAP-Response/Identity **12983 Prepared EAP-Request proposing EAP-TTLS with challenge** ... ... **12978 Extracted EAP-Response containing EAP-TTLS challenge-response and accepting EAP-TTLS as negotiated** 12800 Extracted first TLS record; TLS handshake started ... ... 12810 Prepared TLS ServerDone message ... ... 12812 Extracted TLS ClientKeyExchange message 12803 Extracted TLS ChangeCipherSpec message ... ... **12816 TLS handshake succeeded** ... ... **11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge** 12985 Prepared EAP-Request with another EAP-TTLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request ... ... 12971 Extracted EAP-Response containing EAP-TTLS challenge-response **11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated** ... ... 15013 Selected Identity Source - All_AD_Join_Points 24430 Authenticating user against Active Directory - varshaah-ad 24325 Resolving identity - user@varshaah.local 24313 Search for matching accounts at join point - varshaah.local ... ... 24352 Identity resolution failed - ERROR_NO_SUCH_USER **24412 User not found in Active Directory - varshaah-ad** ... ... 15013 Selected Identity Source - Internal Users 24210 Looking up User in Internal Users IDStore - user **24216 The user is not found in the internal users identity store** ... ... 22056 Subject not found in the applicable identity store(s) 22058 The advanced option that is configured for an unknown user is used 22061 The 'Reject' advanced option is configured in case of a failed authentication request **11823 EAP-MSCHAP authentication attempt failed** ... ... **11815 Inner EAP-MSCHAP authentication failed** ... ... 12976 EAP-TTLS authentication failed 0 ... ... 11504 Prepared EAP-Failure 1 **11003 Returned RADIUS Access-Reject**

알려진 결함

버그 ID	설명
Cisco 버그 ID 63395	서비스를 다시 시작한 후 ISE 3.0에서 REST ID 저장소를 찾을 수 없습니다.

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.