Machine- en gebruikersverificatie configureren met EAP-TTLS

Inhoud

Inleiding

In dit document wordt beschreven hoe u machine- en gebruikersverificatie configureert met EAP-TTLS (EAP-MSCHAPv2) op Secure Client NAM en Cisco ISE.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen voordat u doorgaat met deze implementatie:

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

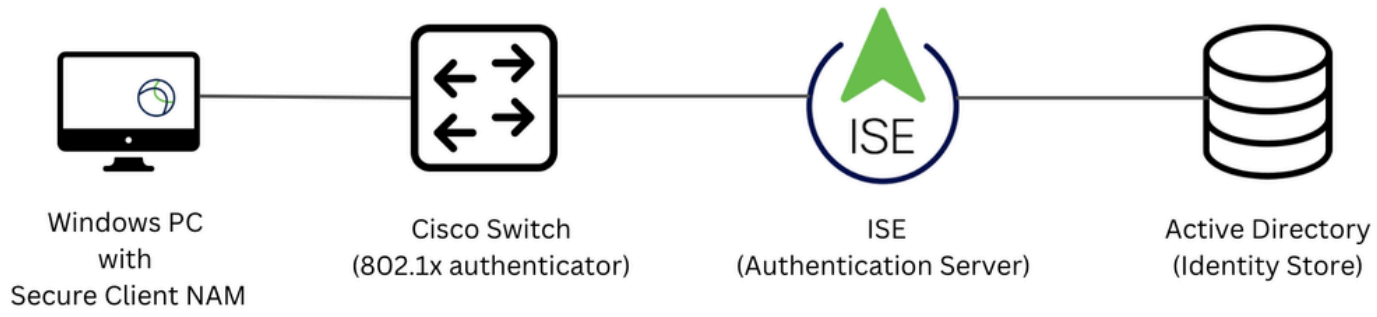
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine (ISE) versie 3.4
- C9300-switch met Cisco IOS® XE-software, versie 16.12.01
- Windows 10 Pro versie 22H2 gebouwd 19045.3930

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerktopologie



Netwerktopologie

Configureren

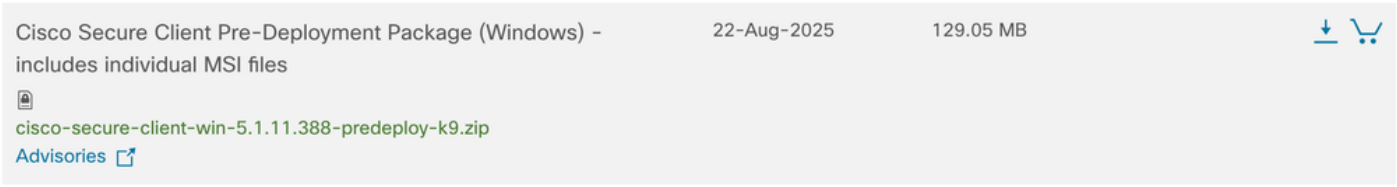
Configuraties

Deel 1: Download en installeer Secure Client NAM (Network Access Manager)

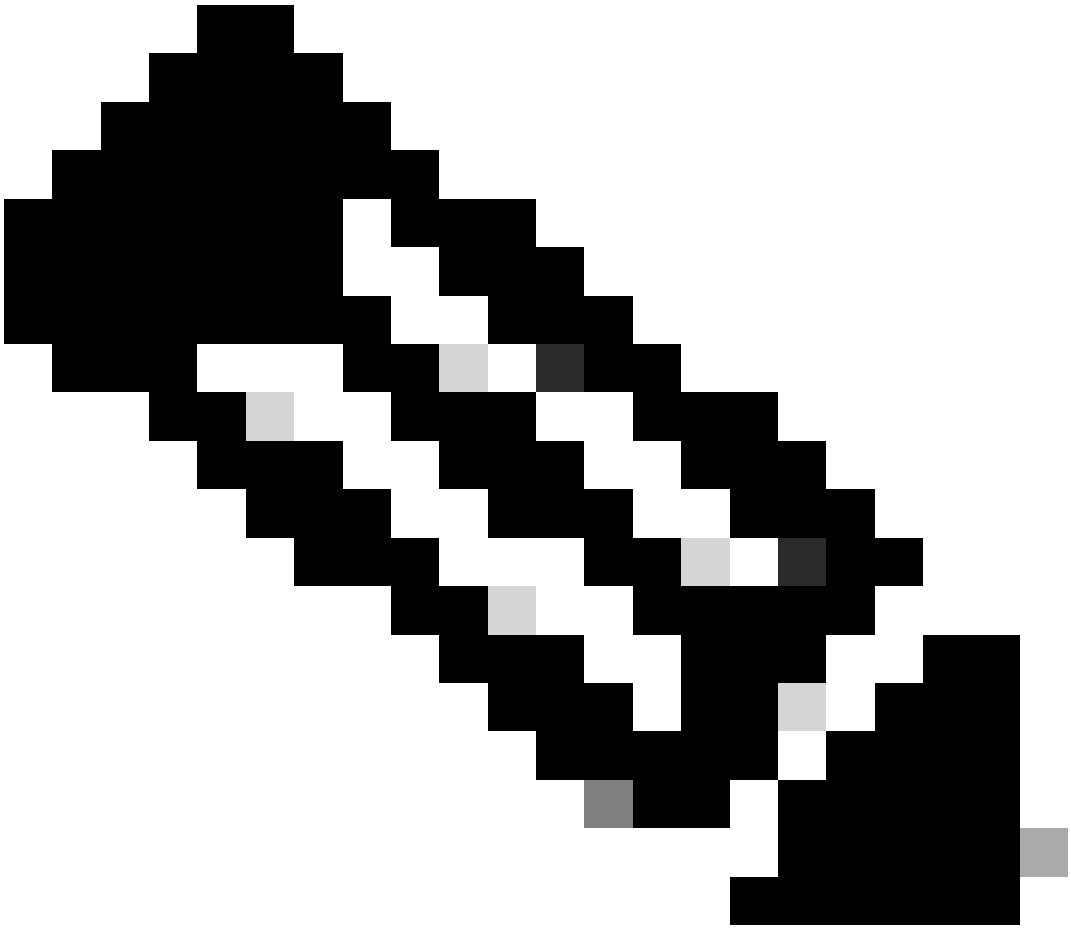
Stap 1. Ga naar Cisco Software Download. Voer in de zoekbalk van het product Secure Client 5 in.

Dit configuratievoorbeeld gebruikt versie 5.1.11.388. De installatie wordt uitgevoerd met behulp van de methode vóór implementatie.

Zoek en download op de downloadpagina het Cisco Secure Client Pre-Deployment Package (Windows).

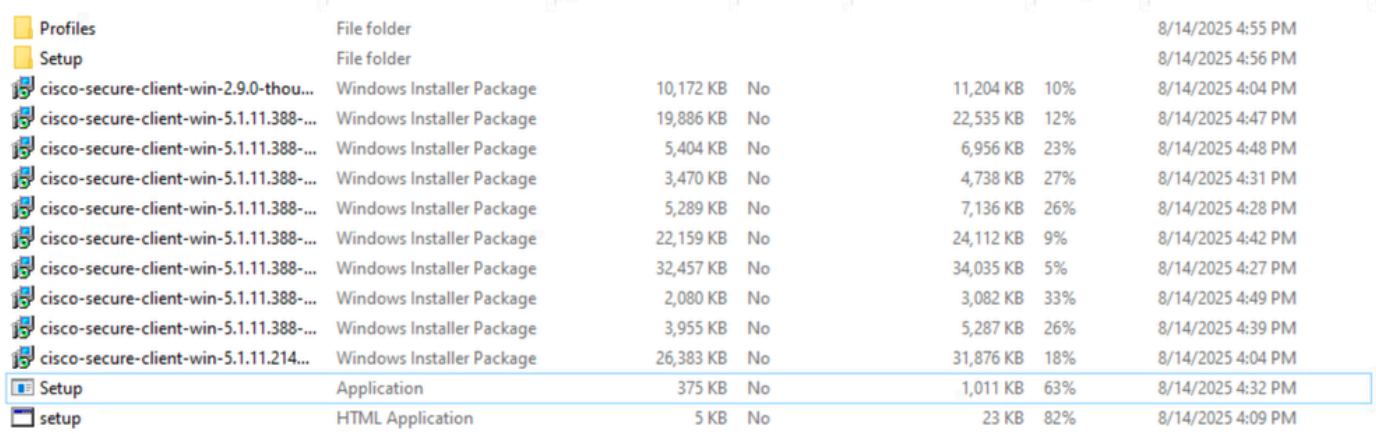


Postbestand vóór implementatie



> Opmerking: Cisco AnyConnect is verouderd en is niet meer beschikbaar op de downloadsite voor Cisco-software.

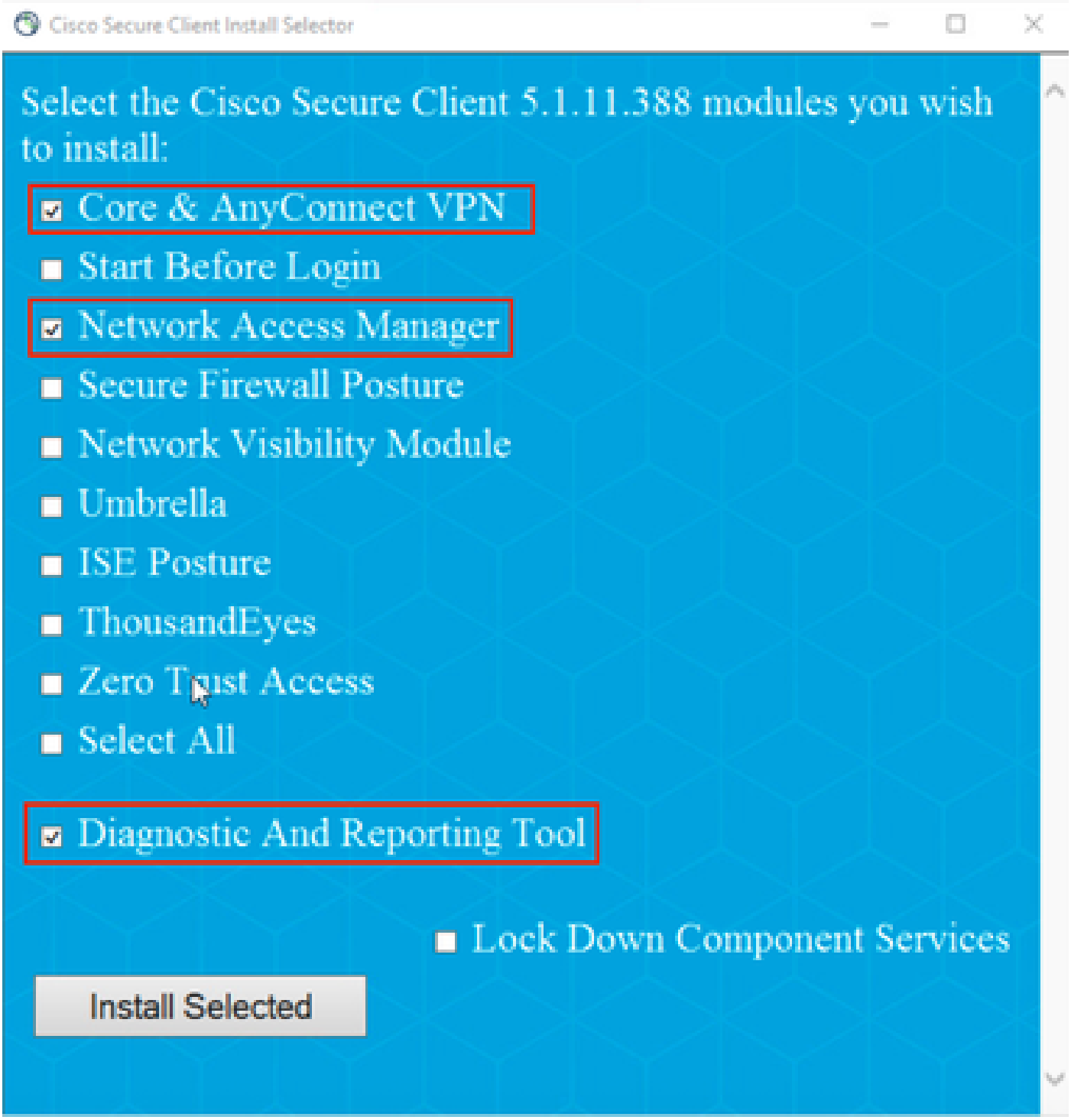
Stap 2. Klik op Setup als u het bestand hebt gedownload en uitgepakt.



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

Zip-bestand vóór implementatie

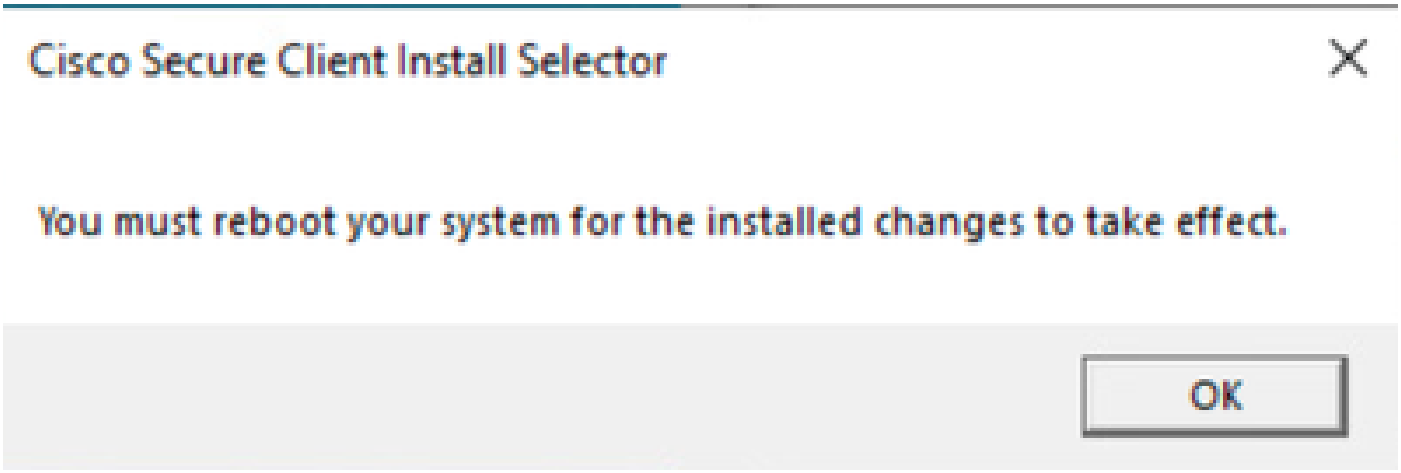
Stap 3. Installeer de Core & AnyConnect VPN, Network Access Manager, en de diagnostische en rapportage toolmodules.



Secure Client Installer

Klik op Install Selected (Selectie installeren).

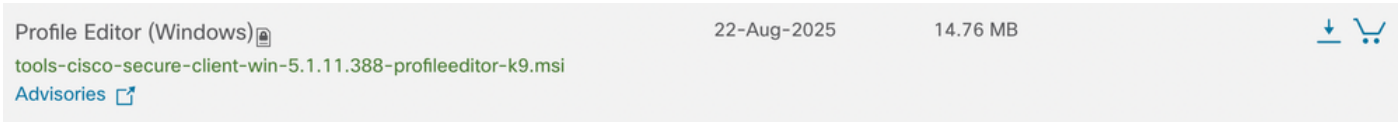
Stap 4. Na de installatie moet opnieuw worden opgestart. Klik op OK en start het apparaat opnieuw op.



Pop-upvenster Opnieuw opstarten vereist

Deel 2: Secure Client NAM Profile Editor downloaden en installeren

Stap 1. De profieleditor is te vinden op dezelfde downloadpagina als de beveiligde client. Dit configuratievoorbeeld gebruikt versie 5.1.11.388.



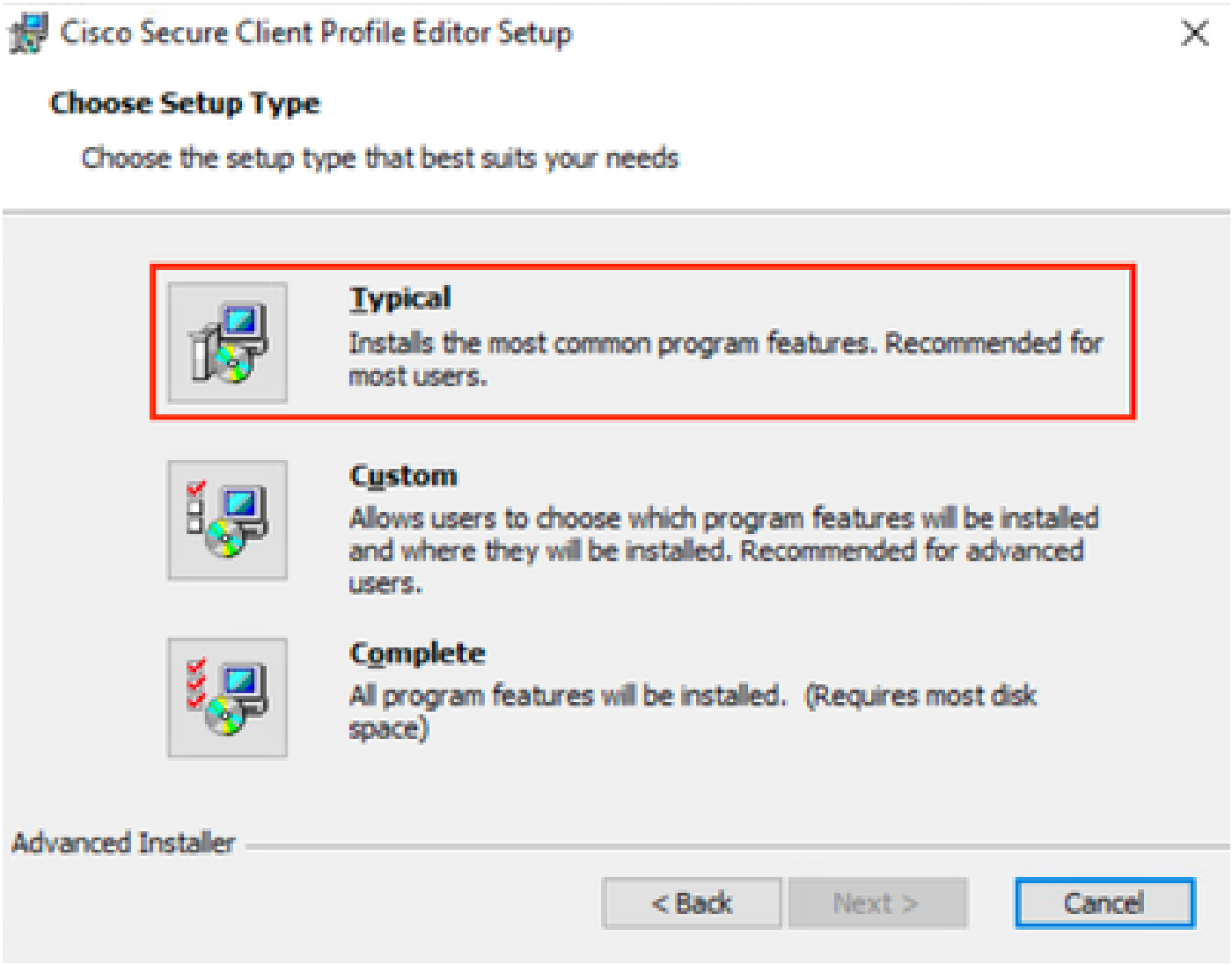
Profieleditor

Download en installeer de profieleditor.

Stap 2. Voer het MSI-bestand uit.

Instellingen voor profieleditor starten

Stap 3. Gebruik de optie Typische installatie en installeer de NAM Profile Editor.

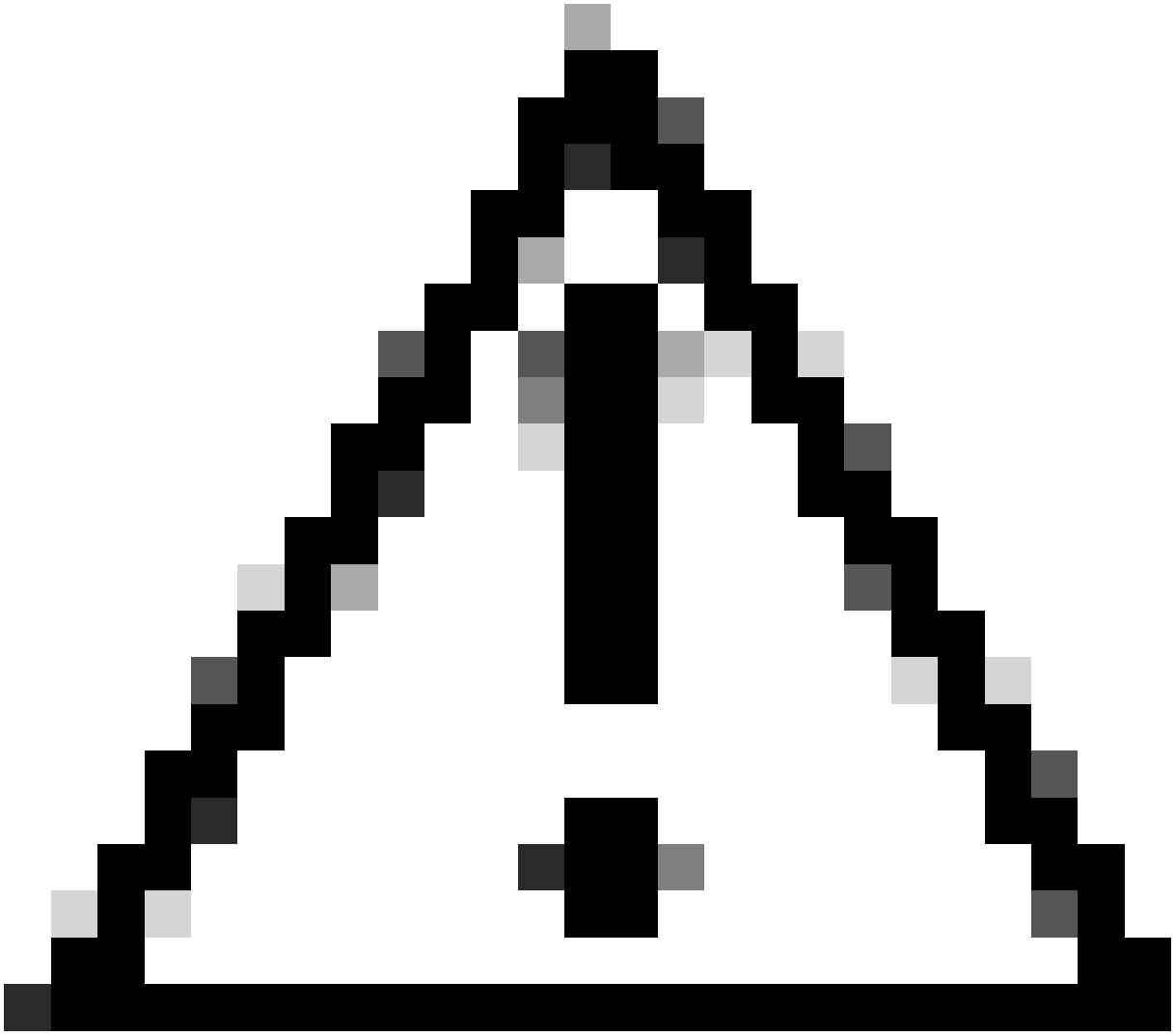


Profieleditor instellen

Deel 3: Toestaan dat aanmeldingsgegevens voor Windows-cache worden geopend door de NAM

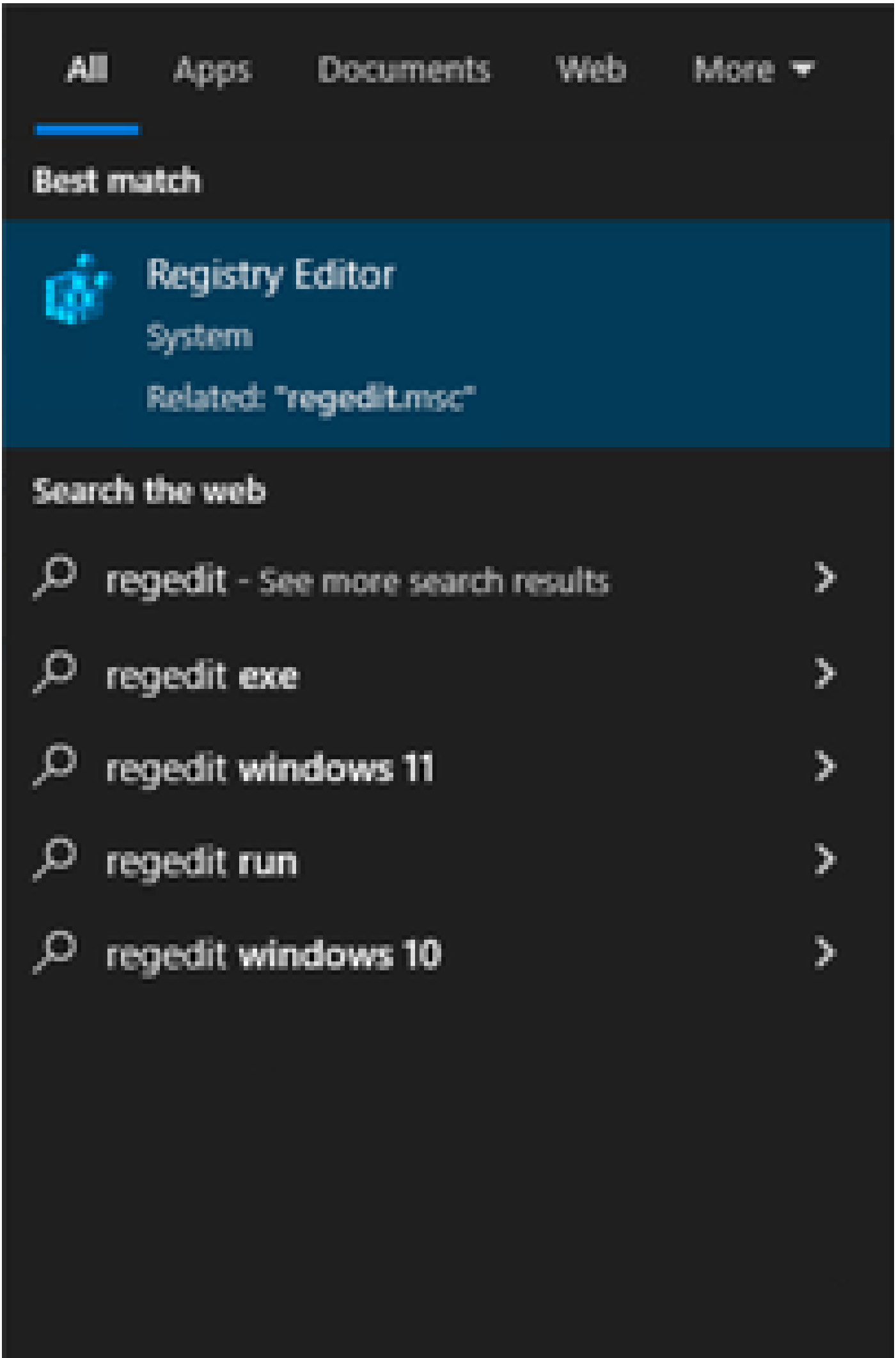
In Windows 10, Windows 11 en Windows Server 2012 voorkomt het besturingssysteem standaard dat Network Access Manager (NAM) het systeemwachtwoord kan ophalen dat vereist is voor de verificatie van het systeem. Als gevolg hiervan werkt machineverificatie met het machinewachtwoord niet, tenzij een registerfix is toegepast.

Als u de NAM toegang wilt geven tot de systeemreferenties, past u de Microsoft KB 2743127-fix toe op het clientbureaublad.



Let op: Het onjuist bewerken van het Windows-register kan ernstige problemen veroorzaken. Zorg ervoor dat u een back-up van het register maakt voordat u wijzigingen aanbrengt.

Stap 1. Voer in de zoekbalk van Windows regedit in en klik vervolgens op Register-editor.

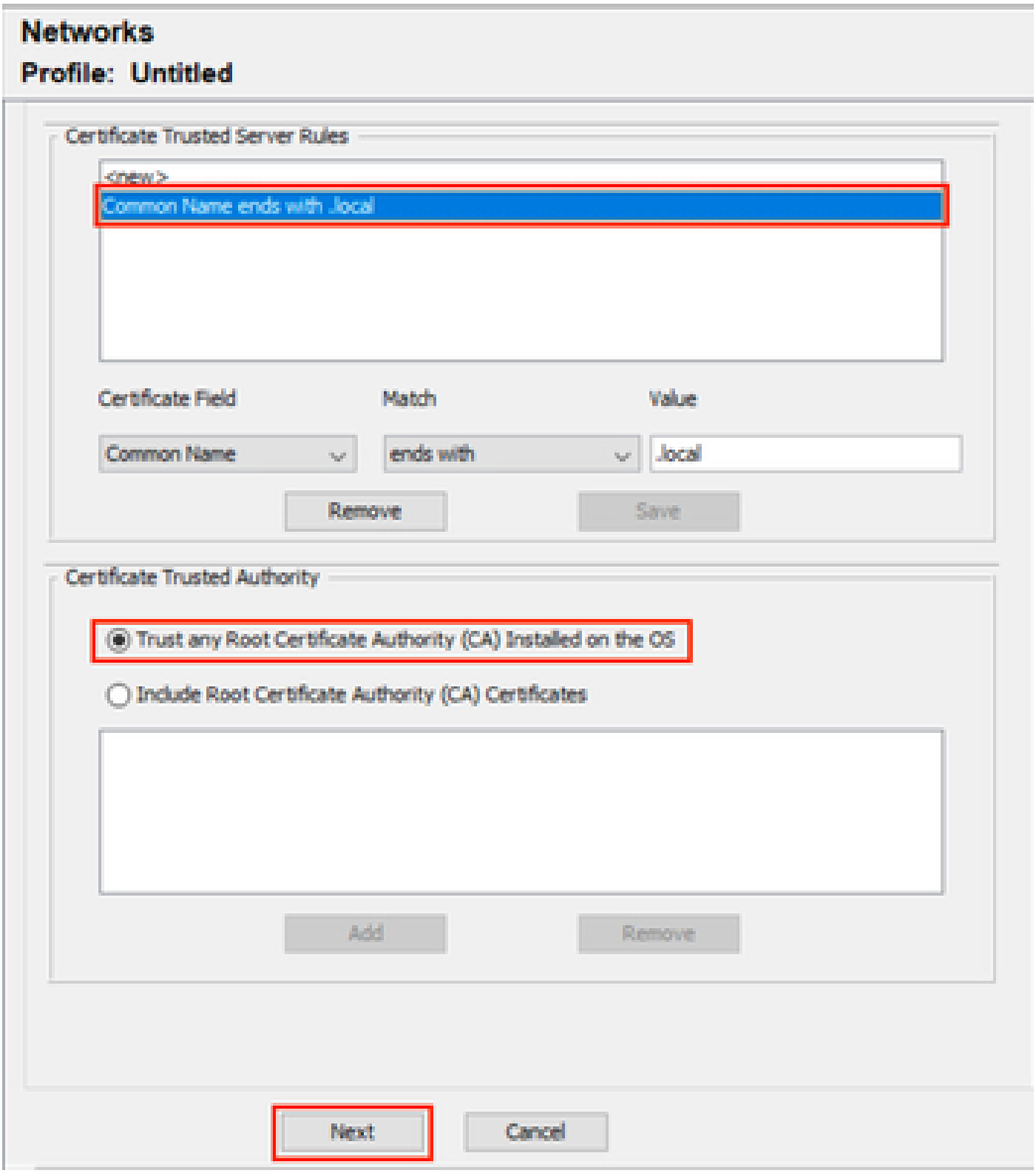

All
Apps
Documents
Web
More
Best match
Registry Editor
System
Related: "regedit.msc"
Search the web
regedit - See more search results
regedit exe
regedit windows 11
regedit run
regedit windows 10

In dit voorbeeld wordt het PSN-knooppuntcertificaat uitgegeven door varshaah.varshaah.local. Vandaar dat de regel Common Name eindigt met .local wordt gebruikt. Met deze regel wordt het certificaat gevalideerd dat de server tijdens de EAP-TTLS-stroom presenteert.

U kunt ook de algemene naam van het EAP-verificatiecertificaat voor de Policy Service Node (PSN) opgeven.

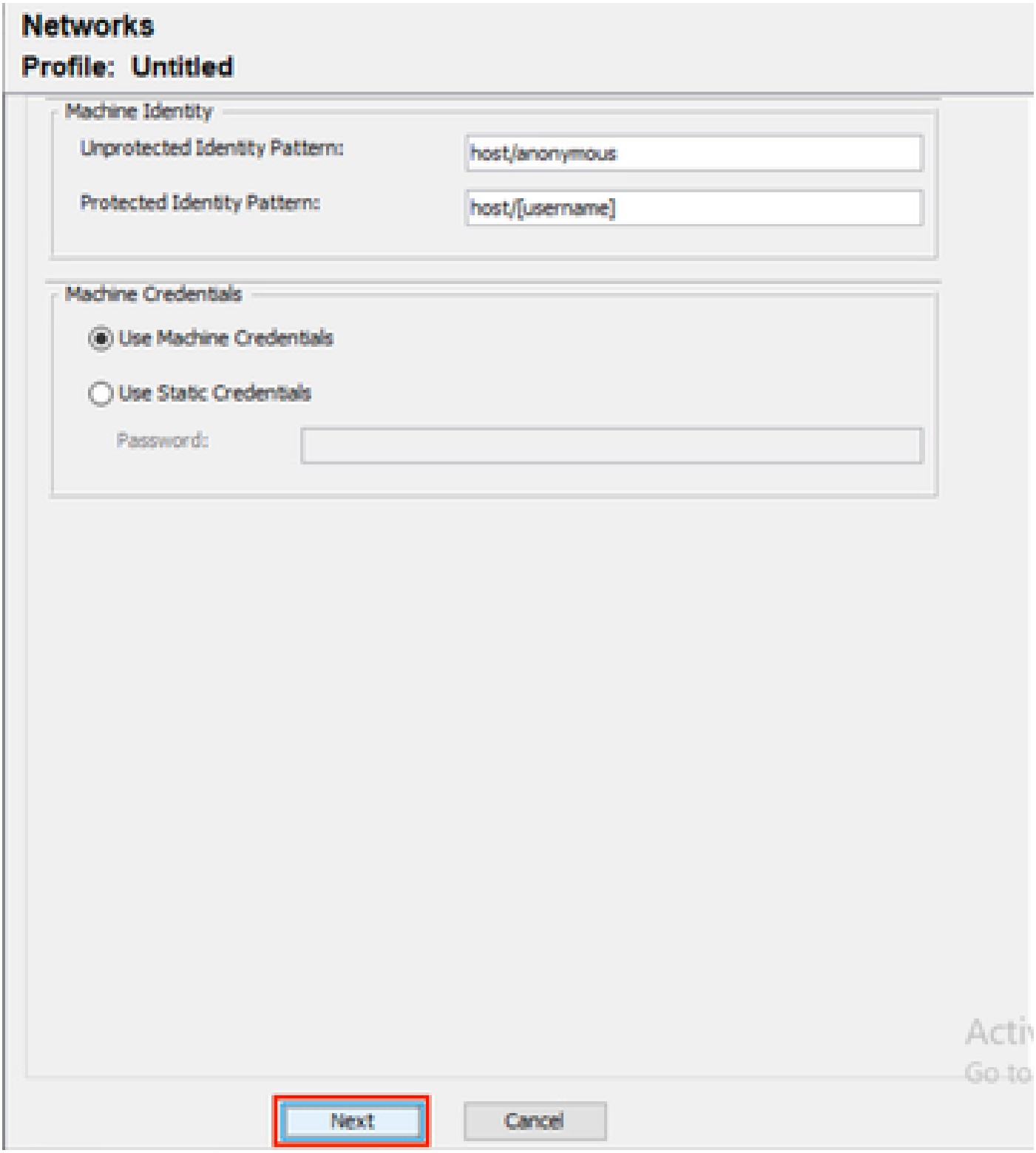
- Onder Certificaat Vertrouwde Autoriteit zijn twee opties beschikbaar.
  In dit scenario wordt de optie Trust any Root Certificate Authority (CA) geïnstalleerd op het besturingssysteem gebruikt in plaats van een specifiek CA-certificaat toe te voegen.

  Met deze optie vertrouwt het Windows-apparaat elk EAP-certificaat dat is ondertekend door een certificaat dat is opgenomen in Certificaten - Huidige gebruiker > Vertrouwde basiscertificeringsinstanties > Certificaten (beheerd door het besturingssysteem).
- Klik op Volgende om door te gaan.



Certificaten NAM Profile Editor

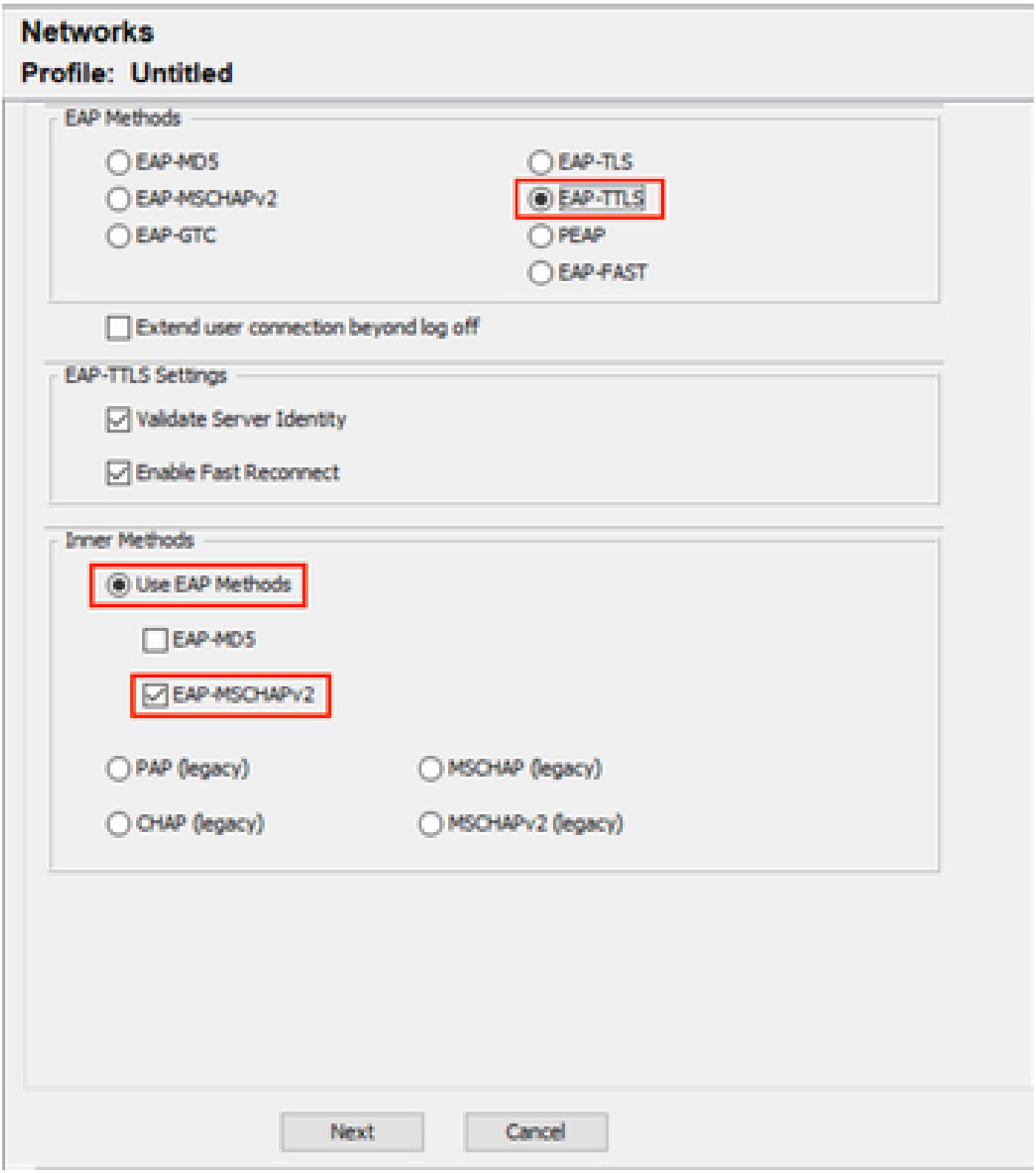
Stap 6. Selecteer in de sectie Inloggegevens machine de optie Inloggegevens machine gebruiken en klik vervolgens op Volgende.



Referenties NAM-profieleditor

Stap 7. Sectie Gebruikersverificatie configureren.

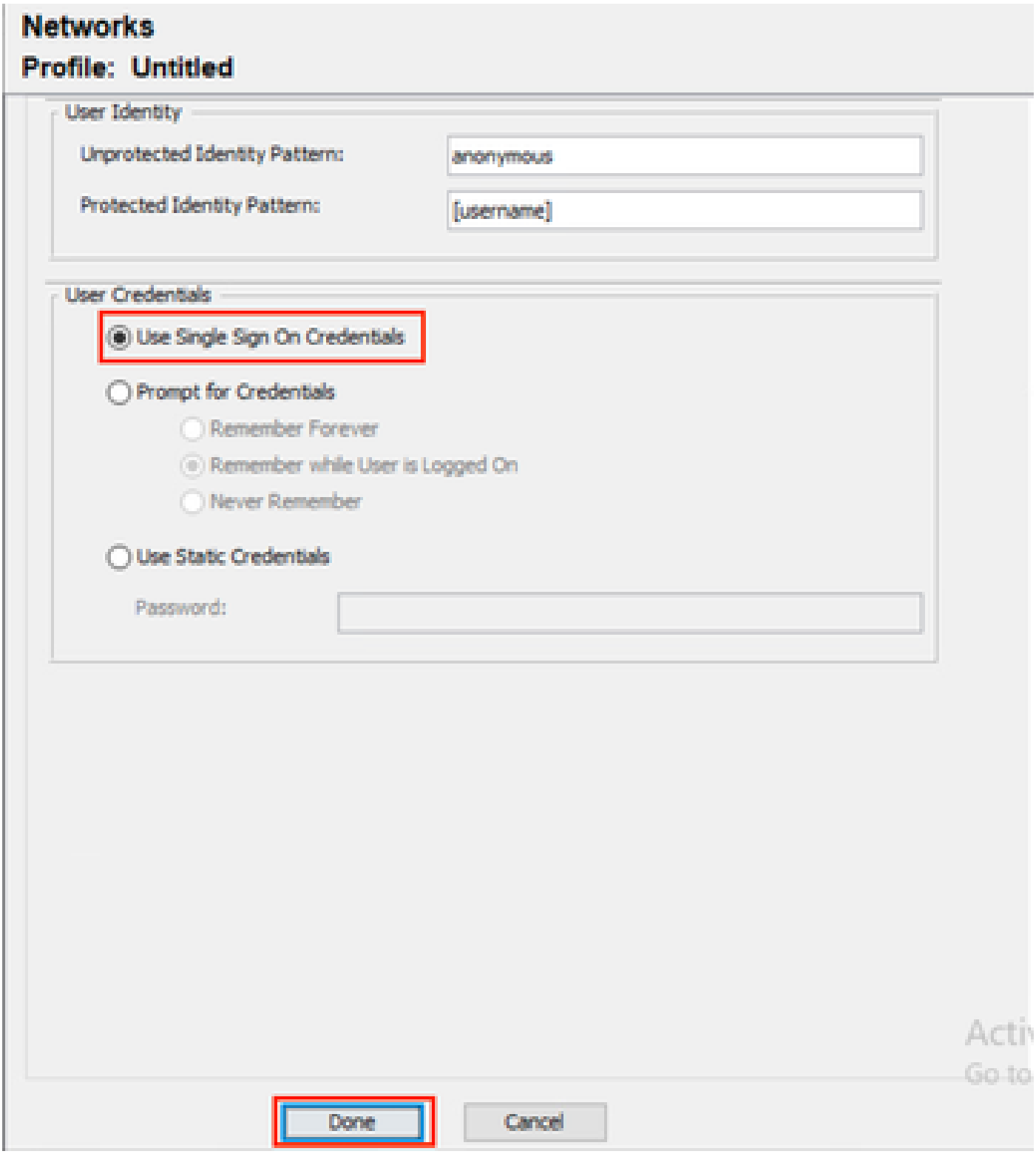
- Selecteer EAP-TTLS onder EAP-methoden.
- Selecteer onder Innerlijke methoden de optie EAP-methoden gebruiken en selecteer EAP-MSCHAPv2.
- Klik op Next (Volgende).



Gebruikersverificatie NAM-profieleditor

Stap 8. Configureer in Certificaten dezelfde regels voor certificaatvalidatie als beschreven in stap 5.

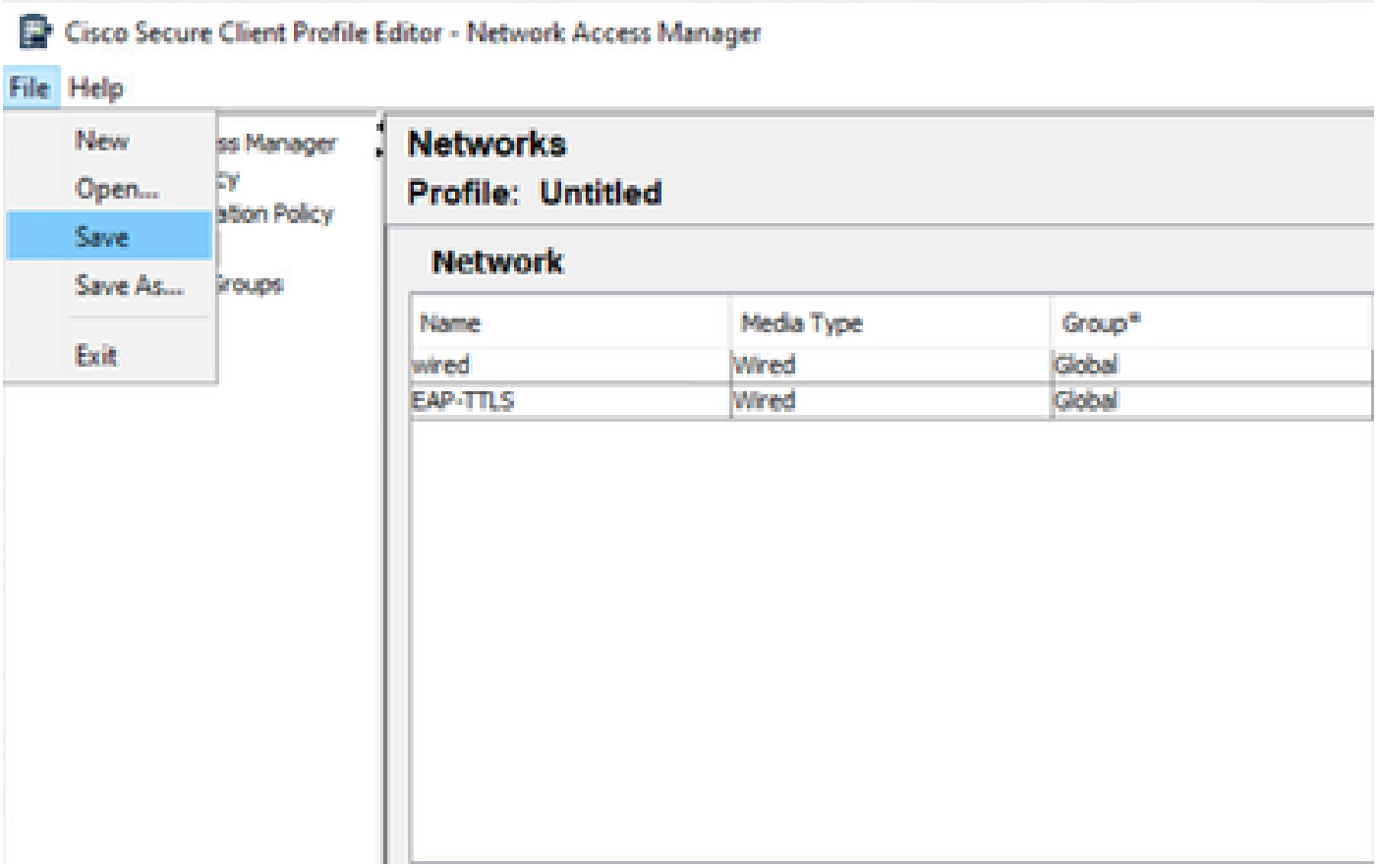
Stap 9. Selecteer in Gebruikersreferenties de optie Credentials voor eenmalige aanmelding gebruiken en klik op Gereed.



Gebruikersreferenties NAM Profile Editor

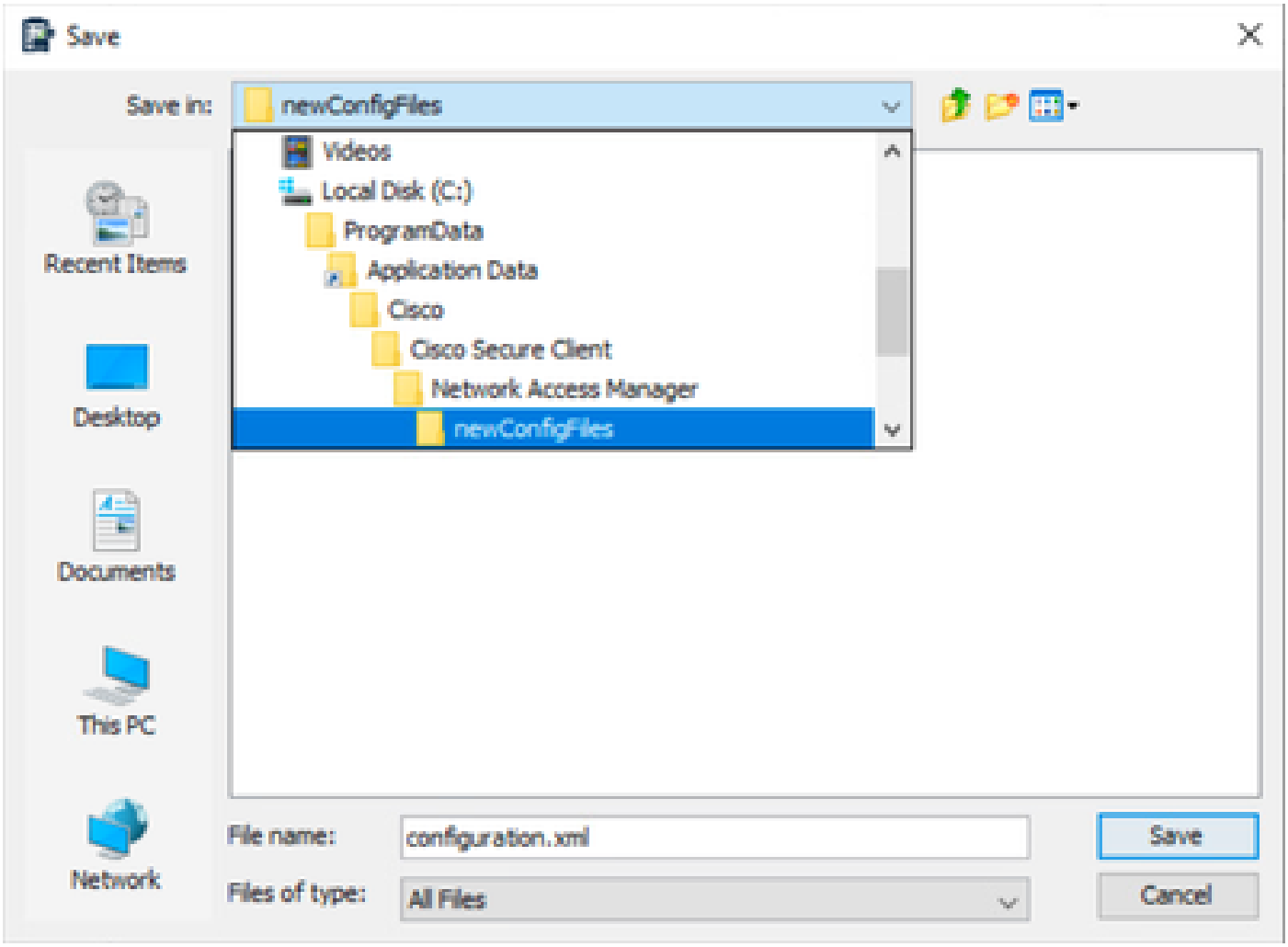
Deel 6: Het netwerkconfiguratiebestand opslaan

Stap 1. Klik op Bestand > Opslaan.



NAM Profile Editor Netwerkconfiguratie opslaan

Stap 2. Sla het bestand op als configuration.xml in de map newConfigFiles.

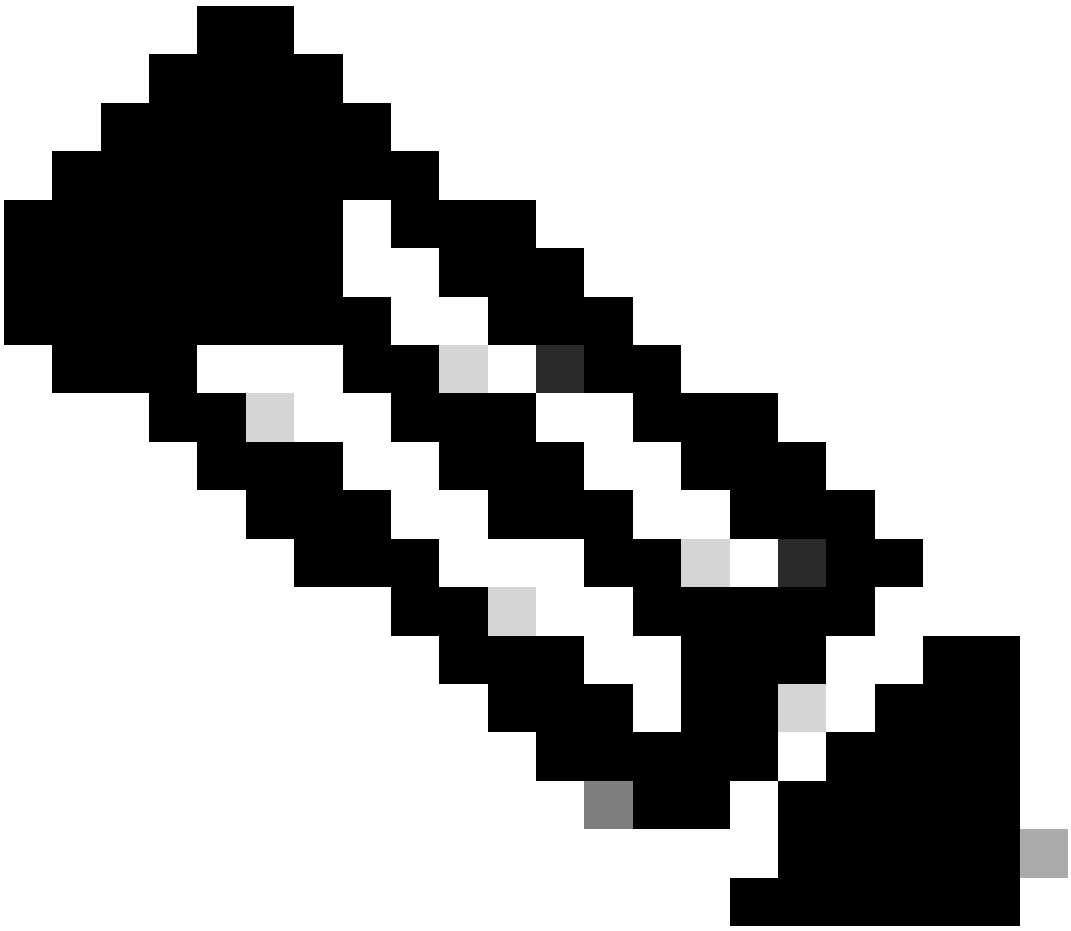


Netwerkconfiguratie opslaan

Deel 7: AAA op de Switch configureren

```
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
```



> Opmerking: De opdracht dot1x system-auth-control wordt niet weergegeven in de uitvoer voor actieve configuratie van de show, maar is vereist om 802.1X wereldwijd in te schakelen.

Configureer de Switch-interface voor 802.1X:

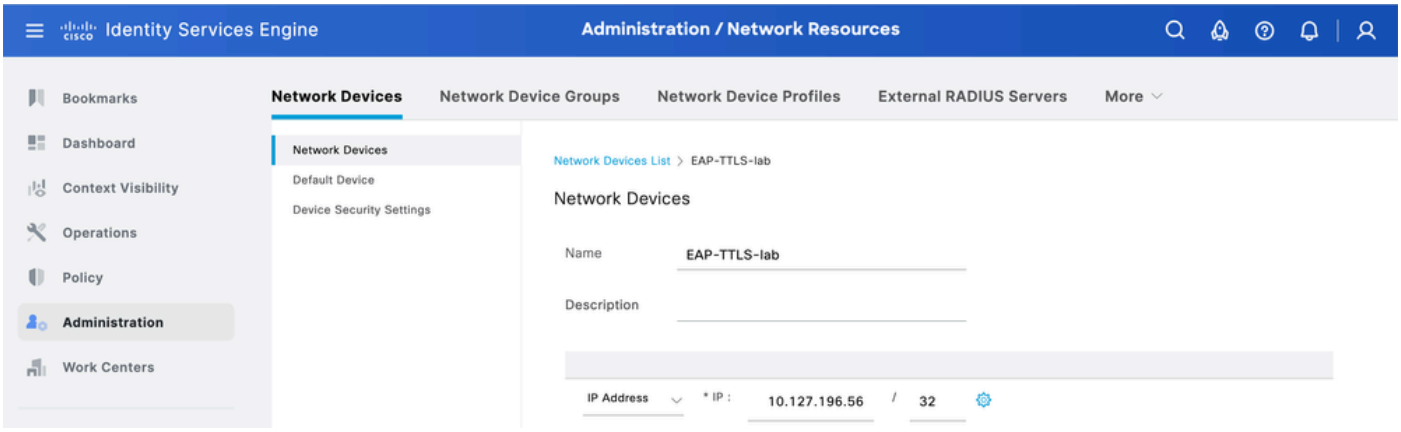
```
C9300-1(config)#do sh run int gig1/0/44
Building configuration...

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
```

Deel 8: ISE-configuraties

Stap 1. Switch configureren op ISE.

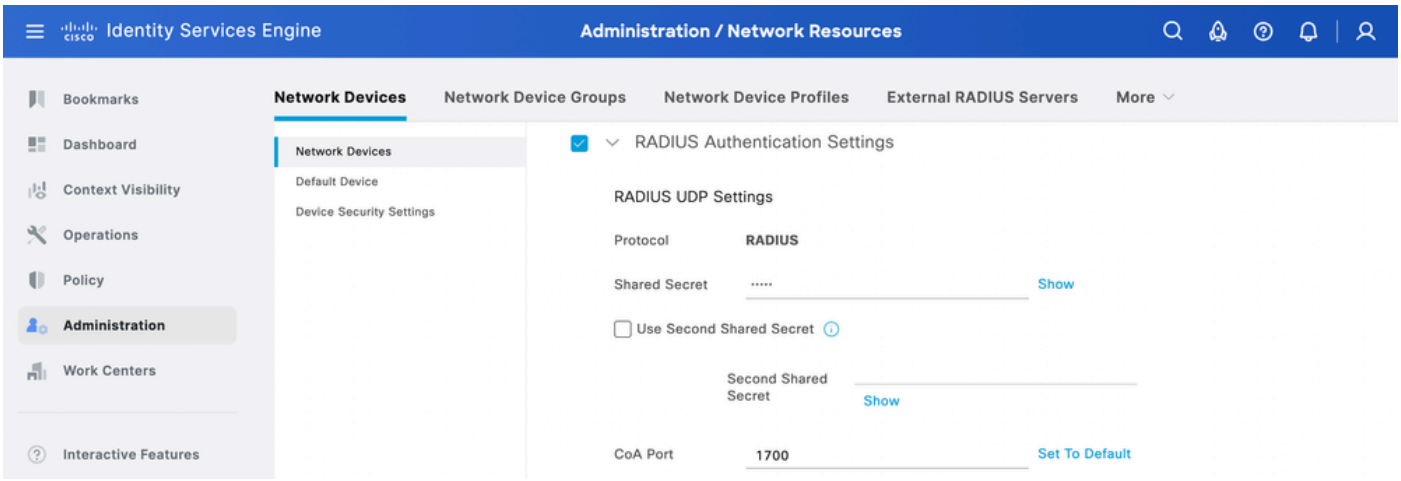
Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten en klik op Toevoegen.

Voer hier de naam en het IP-adres van de switch in.



Netwerkapparaat ISE toevoegen

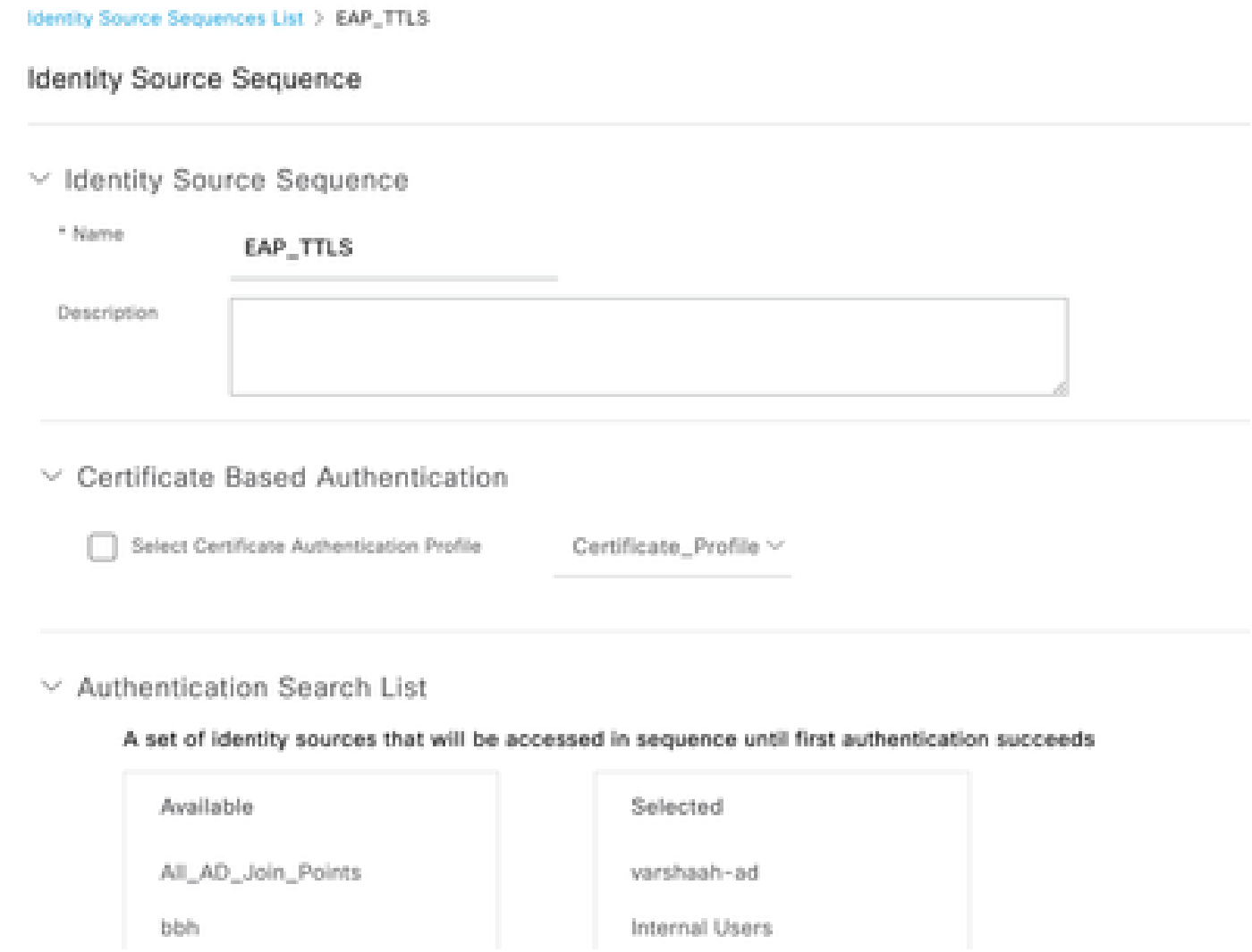
Voer het gedeelde RADIUS-geheim in, hetzelfde als het eerder op de switch geconfigureerde geheim.



RADIUS Shared Secret ISE

Stap 2. Identiteitsbronsequentie configureren.

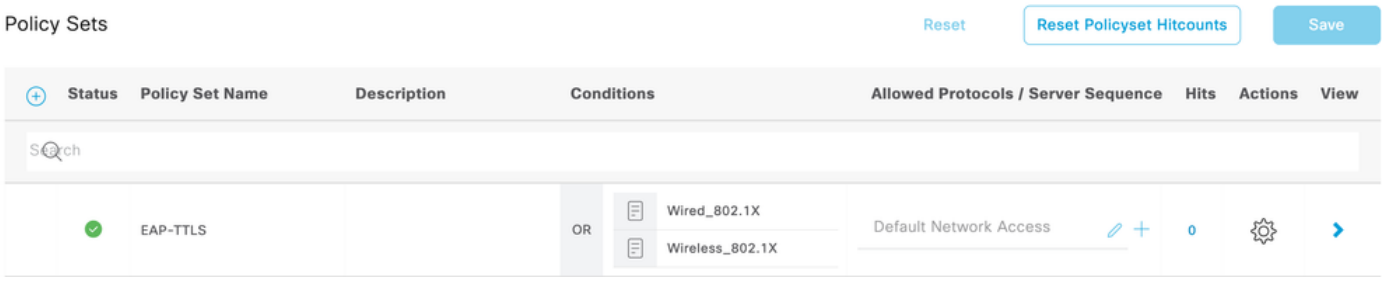
- Navigeer naar Beheer > Identiteitsbeheer > Identiteitsbronsequenties.
- Klik op Toevoegen om een nieuwe identiteitsbronreeks te maken.
- Configureer de identiteitsbronnen onder Zoeklijst voor verificatie.



ISE-identiteitsbronsequentie

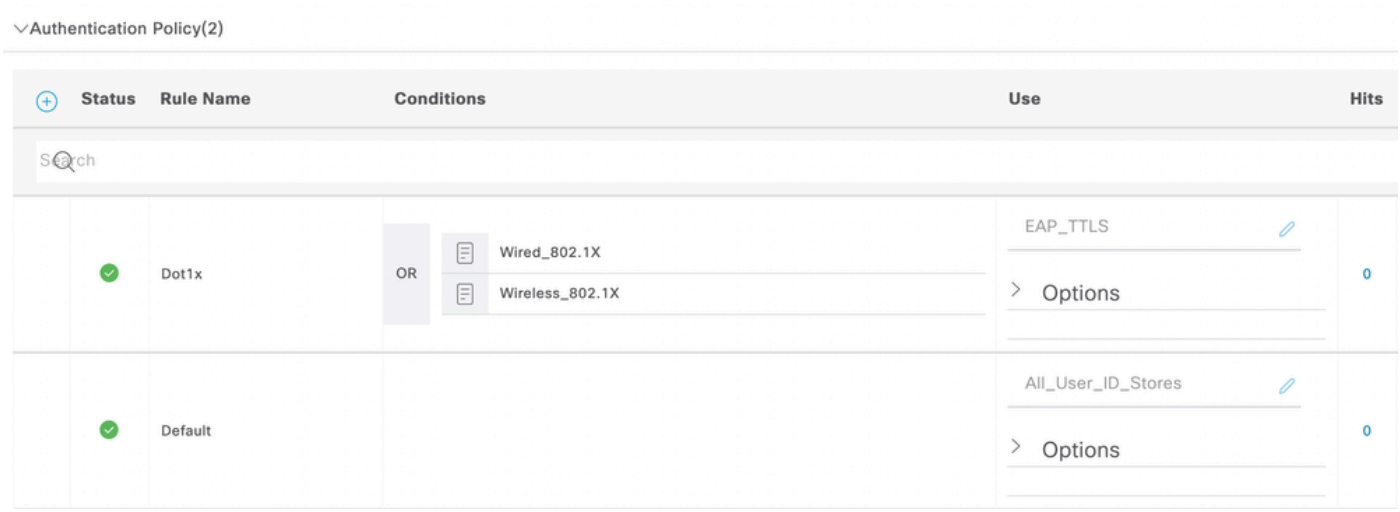
Stap 3. Beleidsset configureren.

Navigeer naar Beleid > Beleidsreeksen en maak een nieuwe beleidsset. Configureer de voorwaarden als Wired_802.1x OF Wireless_802.1x. Kies Standaardnetwerktoegang voor Toegestane Protocollen:



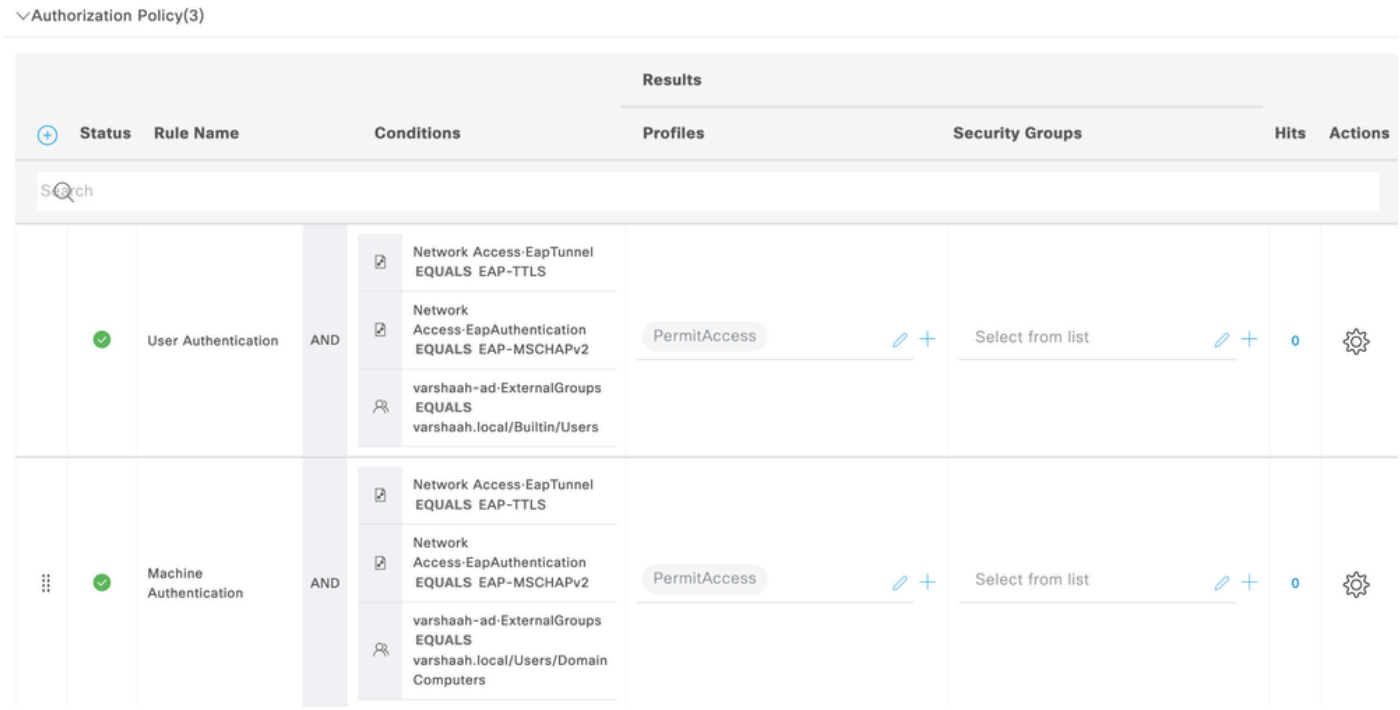
EAP-TTLS-beleidsset

Maak het verificatiebeleid voor punt1x en kies de identiteitsbronreeks die is gemaakt in stap 4.



EAP-TTLS-verificatiebeleid

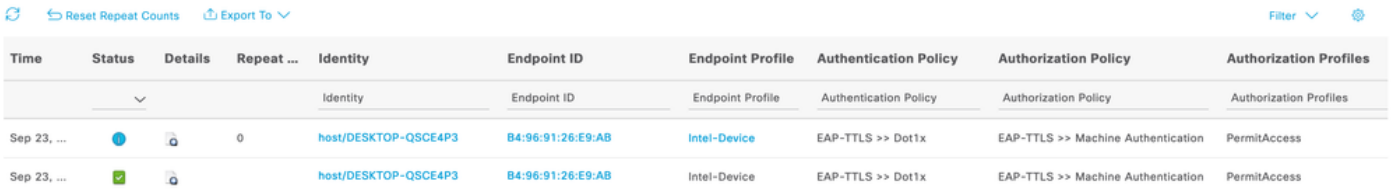
Maak voor het machtigingsbeleid de regel met drie voorwaarden. De eerste voorwaarde controleert of de EAP-TTLS-tunnel wordt gebruikt. De tweede voorwaarde controleert of EAP-MSCHAPv2 wordt gebruikt als de interne EAP-methode. De derde voorwaarde controleert voor de respectieve AD-groep.



Dot1x-autorisatiebeleid

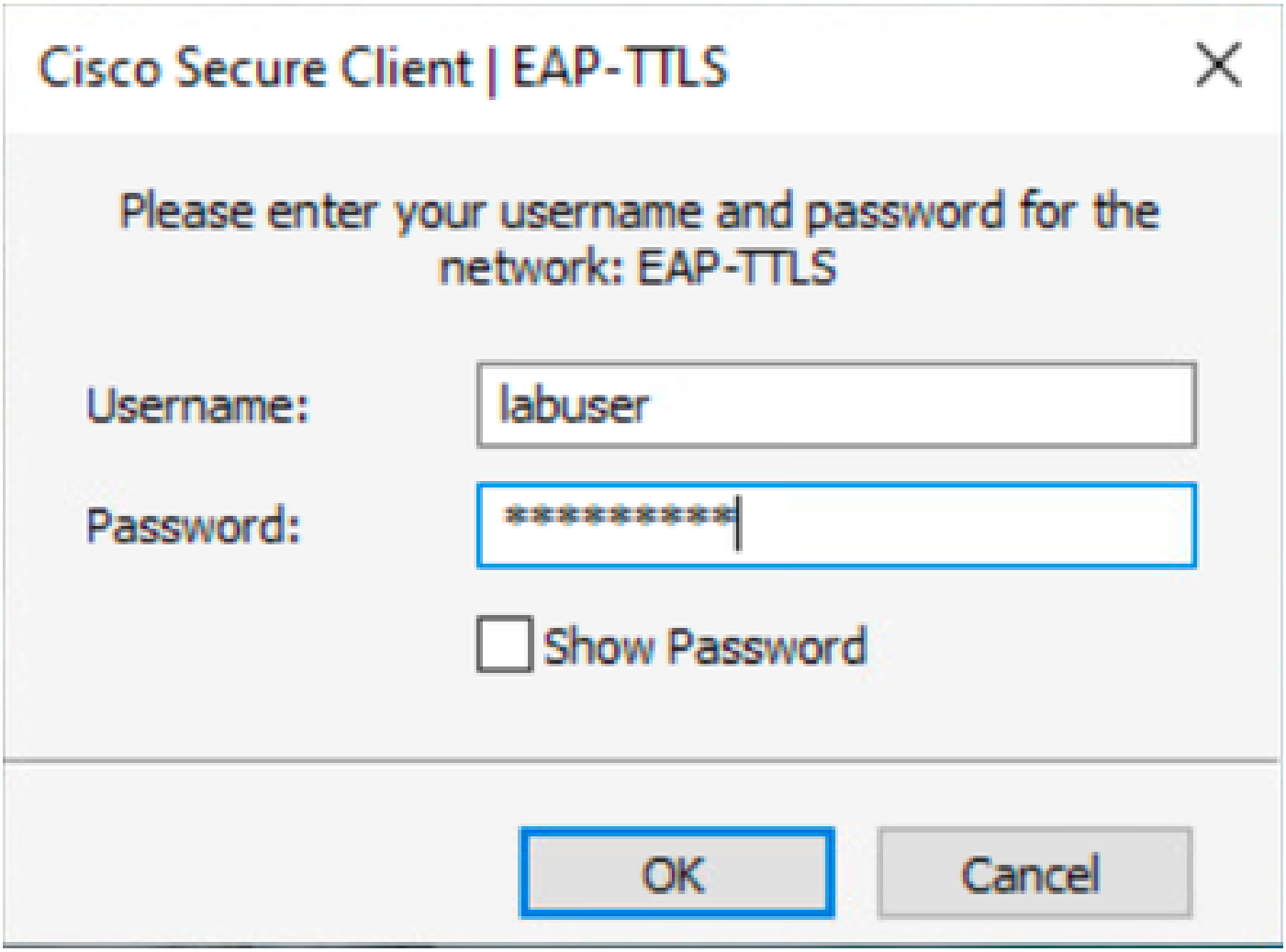
Verifiëren

U kunt het Windows 10-systeem opnieuw opstarten of u kunt zich afmelden en u vervolgens aanmelden. Wanneer het inlogscherm van Windows wordt weergegeven, wordt de systeemverificatie geactiveerd.

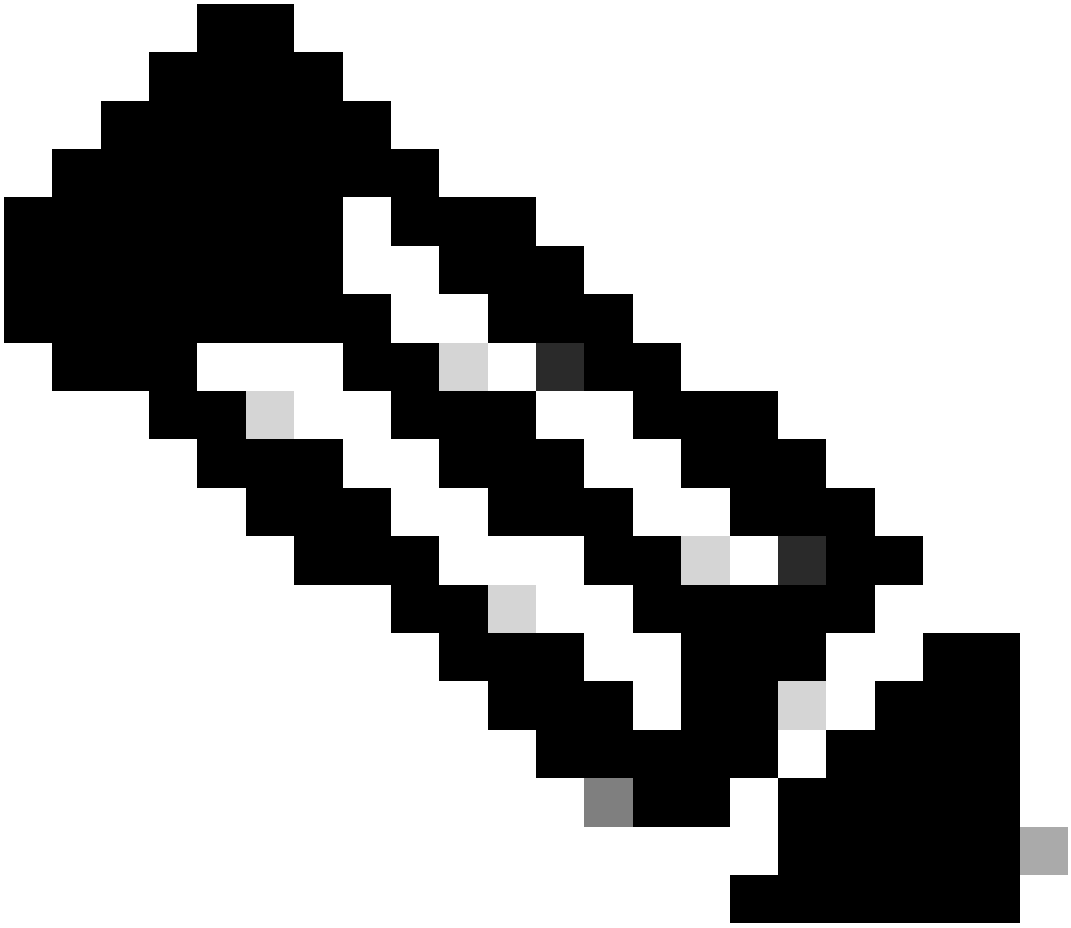


Verificatie van live logboeksysteem

Wanneer u zich aanmeldt bij de pc met referenties, wordt gebruikersverificatie geactiveerd.

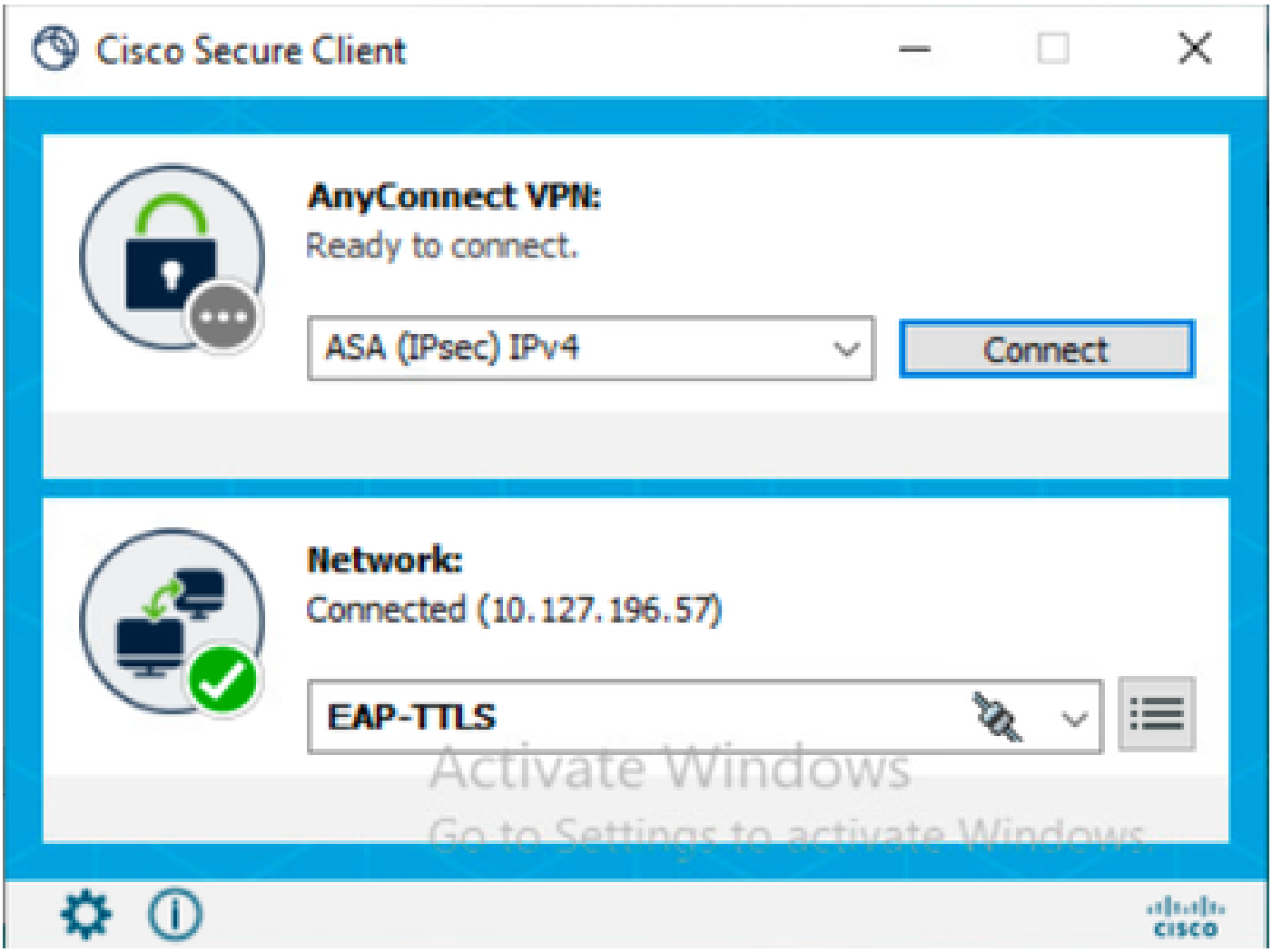


Gebruikersreferenties

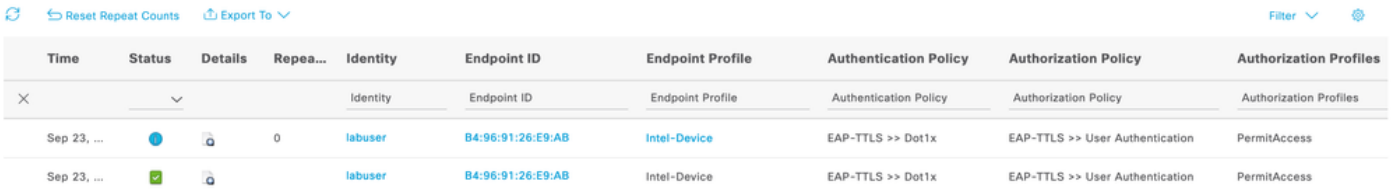


Opmerking: in dit voorbeeld worden Active Directory-gebruikersreferenties gebruikt voor verificatie. U kunt ook een interne gebruiker maken in Cisco ISE en deze referenties gebruiken om u aan te melden.

Nadat de referenties zijn ingevoerd en met succes zijn geverifieerd, wordt het eindpunt met gebruikersverificatie verbonden met het netwerk.



EAP-TTLS aangesloten



Gebruikersverificatie Live-log

ISE RADIUS Live Logs analyseren

Deze sectie illustreert de RADIUS live logboekvermeldingen voor een succesvolle machine- en gebruikersverificatie.

machineverificatie

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

gebruikersverificatie

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-logboeken analyseren

NAM-logs, vooral nadat u Extended Logging hebt ingeschakeld, bevatten een grote hoeveelheid gegevens, waarvan de meeste niet relevant zijn en kunnen worden genegeerd. In dit gedeelte worden de foutopsporingslijnen weergegeven om aan te tonen welke stappen de NAM neemt om een netwerkverbinding tot stand te brengen. Wanneer u een logboek doorneemt, kunnen deze sleutelzinnen nuttig zijn om een deel van het logboek te vinden dat relevant is voor het probleem.

machineverificatie

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

De client ontvangt een EAP-TTLS-pakket van de switch van het netwerk en start de EAP-TTLS-sessie. Dit is het startpunt voor de machine-authenticatietunnel.

```
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
```

De client ontvangt de Hello Server van ISE en begint het servercertificaat te valideren (CN=varshaah.varshaah.local). Het certificaat is te vinden in het vertrouwensarchief van de klant en toegevoegd voor validatie.

```
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
```

Het servercertificaat is met succes gevalideerd en de TLS-tunnelinstelling is voltooid.

```
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-
```

De client geeft aan dat de verificatie is geslaagd. De interface wordt gedeblokkeerd en de interne status van het systeem wordt gewijzigd in USER_T_NOT_DISCONNECTED, wat aangeeft dat het systeem nu verkeer kan doorgeven.

```
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-
```

De adapter rapporteert geverifieerd en de NAM AccessStateMachine gaat over naar ACCESS_AUTHENTICATED. Dit bevestigt dat de machine de verificatie met succes heeft voltooid en volledige netwerktoegang heeft.

gebruikersverificatie

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

De NAM-client start het EAP-TTLS-verbindingsproces.

```
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
```

De NAM verbindt de fysieke adapter met het EAP-TTLS-netwerk en gaat over naar de status ACCESS_ATTACHED, waarmee wordt bevestigd dat de adapter klaar is voor verificatie.

```
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
```

De client gaat over van AANGESLOTEN naar VERBINDEN, vanaf de 802.1X-uitwisseling.

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

De client verzendt een EAPOL-Start om het verificatieproces te starten.

```
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
```

De switch vraagt om een identiteitsbewijs en de klant bereidt zich voor om te reageren met een identiteit in de buitenwereld.

```
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
```

NAM stuurt de uiterlijke identiteit. Standaard is dit anoniem, wat aangeeft dat de uitwisseling voor gebruikersverificatie is (niet voor machine).

```
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
```

Zowel de client als de server stemmen ermee in om EAP-TTLS als methode voor de buitenwereld te gebruiken.

```
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
```

De client verzendt Client Hello en ontvangt de Hello Server, die het ISE-certificaat bevat.

```
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
```

Het servercertificaat wordt gepresenteerd. De klant zoekt de CN varshaah.varshaah.local op, vindt een match en valideert het certificaat. De handdruk wordt onderbroken terwijl het X.509-certificaat wordt gecontroleerd.

```
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
```

De tunnel is aangelegd. De NAM vraagt en bereidt nu de beschermde identiteit en referenties voor innerlijke authenticatie voor.

```
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
```

De TLS handshake is voltooid. Er is nu een beveiligde tunnel voor interne authenticatie.

```
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
```

De beschermde identiteit (gebruikersnaam) wordt verzonden en geaccepteerd door ISE.

```
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
```

ISE vraagt het wachtwoord aan. NAM stuurt het beveiligde wachtwoord binnen de TLS-tunnel.

```
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
```

ISE valideert het wachtwoord, verzendt EAP-Success en NAM-overgangen naar AUTHENTICATED. Op dit punt is de gebruikersverificatie voltooid en heeft de client toegang tot het netwerk.

Problemen oplossen

Bij het oplossen van problemen met Network Access Manager (NAM) met Cisco ISE en switch-integratie moeten logbestanden worden verzameld van alle drie de onderdelen: Secure Client (NAM), Cisco ISE en de switch .

Logboeken van Secure Client (NAM)

1. Schakel uitgebreide NAM-logboekregistratie in door deze stappen te volgen.
2. Het probleem reproduceren. Als het netwerkprofiel niet van toepassing is, voert u Network Repair uit in Secure Client.
3. Verzamel de DART-bundel met behulp van de Diagnostics and Reporting Tool (DART).

Cisco ISE Logs

Schakel deze debugs in ISE in om verificatie- en directory-interacties vast te leggen:

- runtime-AAA

- NSF
- NSF-sessie

Switch Logs

Basisfouten

```
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
```

Geavanceerde debugs (indien vereist)

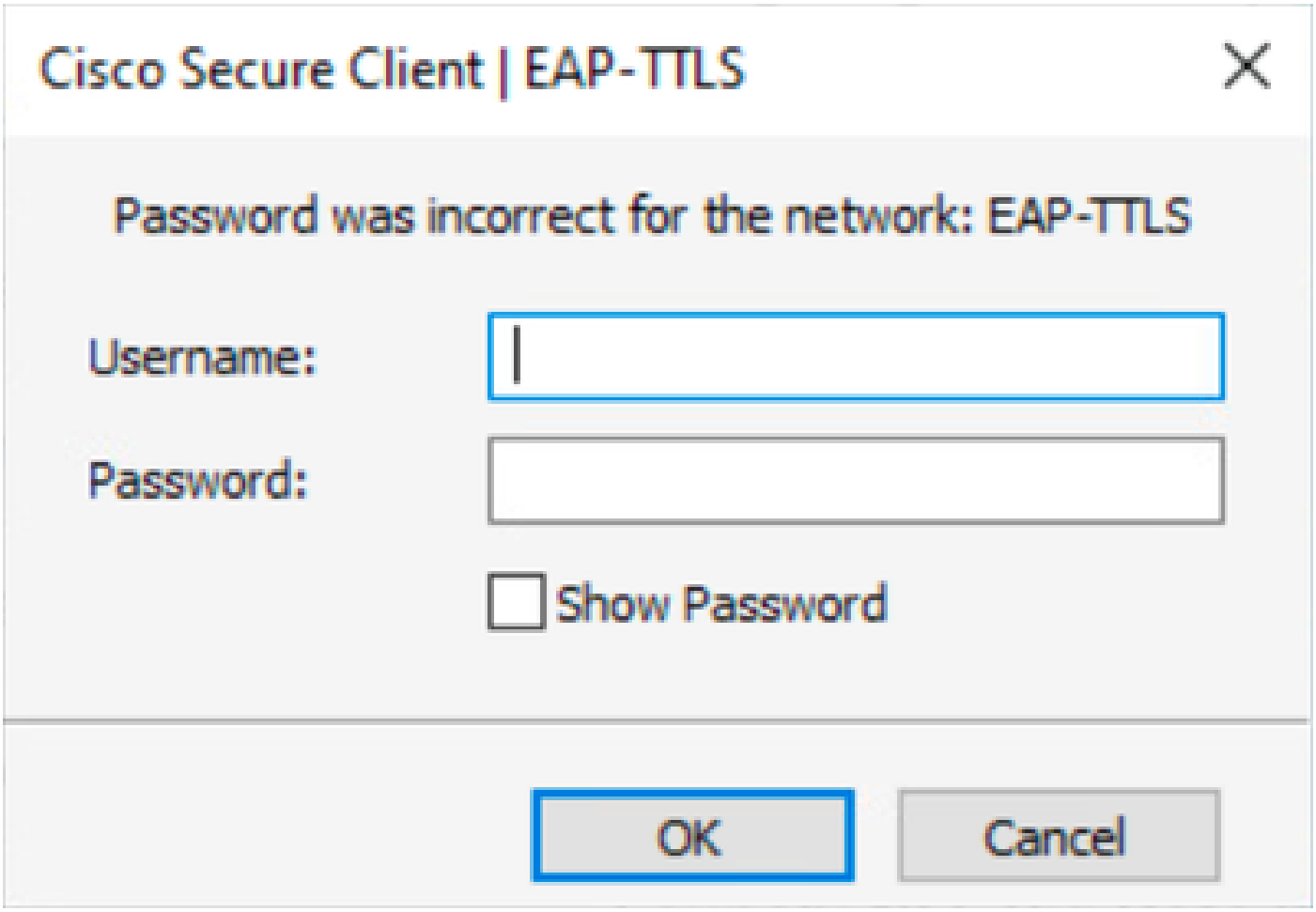
```
set platform software trace smd switch active R0 epm-all debug
set platform software trace smd switch active R0 pre-all debug
```

Opdrachten weergeven

```
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
```

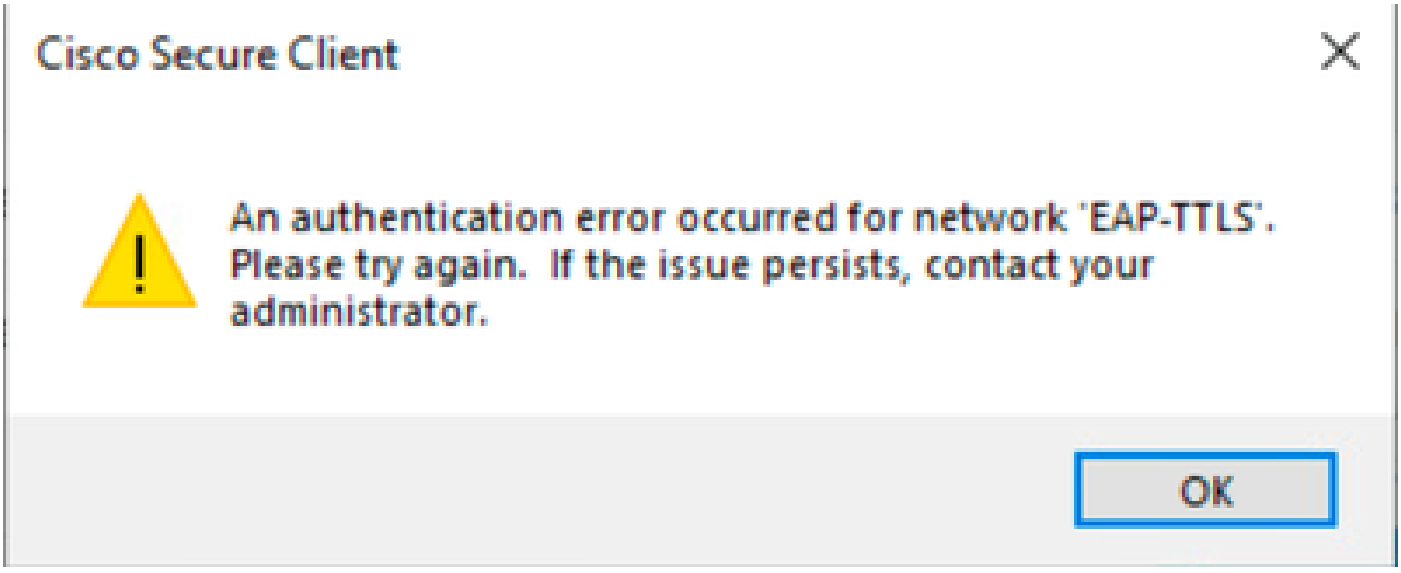
Fout bij gebruikersverificatie vanwege ongeldige referenties

Wanneer een gebruiker onjuiste referenties invoert, geeft Secure Client een algemeen wachtwoord weer dat onjuist was voor het netwerk: EAP-TTLS-bericht. De fout op het scherm geeft niet aan of het probleem te wijten is aan een ongeldige gebruikersnaam of wachtwoord.



Fout met onjuist wachtwoord

Als de verificatie twee keer achter elkaar mislukt, geeft Secure Client dit bericht weer: er is een verificatiefout opgetreden voor 'EAP-TTLS' van het netwerk. Please try again. Als het probleem zich blijft voordoen, neemt u contact op met de beheerder.



Probleem met gebruikersverificatie

Om de oorzaak te identificeren, bekijkt u de NAM-logs.

1. Onjuist wachtwoord:

Wanneer een gebruiker een onjuist wachtwoord invoert, worden in de NAM-logs vermeldingen weergegeven die vergelijkbaar zijn met deze uitvoer:

```
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
```

In Cisco ISE-livelogs wordt de bijbehorende gebeurtenis weergegeven als:

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

Onjuist wachtwoord

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. Onjuiste gebruikersnaam:

Wanneer een gebruiker een onjuiste gebruikersnaam invoert, tonen de NAM-logs vermeldingen die vergelijkbaar zijn met deze uitvoer:

```
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
```

In Cisco ISE-livelogs wordt de bijbehorende gebeurtenis weergegeven als:

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).

Onjuiste gebruikersnaam

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**

Bekende gebreken

Bug-ID	Beschrijving
Cisco bug ID 63395	ISE 3.0 kan REST ID-winkel niet vinden nadat services opnieuw zijn gestart

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.