Konfigurieren der Computer- und Benutzerauthentifizierung mit EAP-TTLS

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Computer- und Benutzerauthentifizierung mit EAP-TTLS (EAP-MSCHAPv2) auf Secure Client NAM und Cisco ISE konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesen Themen verfügen, bevor Sie mit der Bereitstellung fortfahren:

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

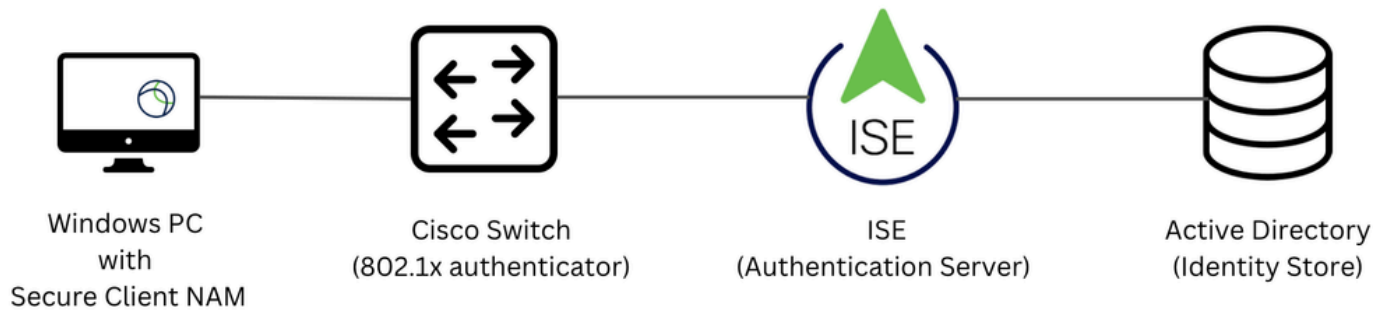
Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine (ISE) Version 3.4
- C9300-Switch mit Cisco IOS® XE Software, Version 16.12.01
- Windows 10 Pro Version 22H2, Build 19045.3930

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerktopologie



Netzwerktopologie

Konfigurieren

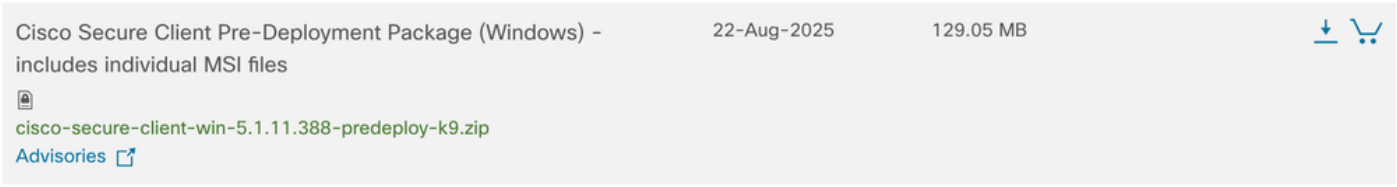
Konfigurationen

Teil 1: Herunterladen und Installieren von Secure Client NAM (Network Access Manager)

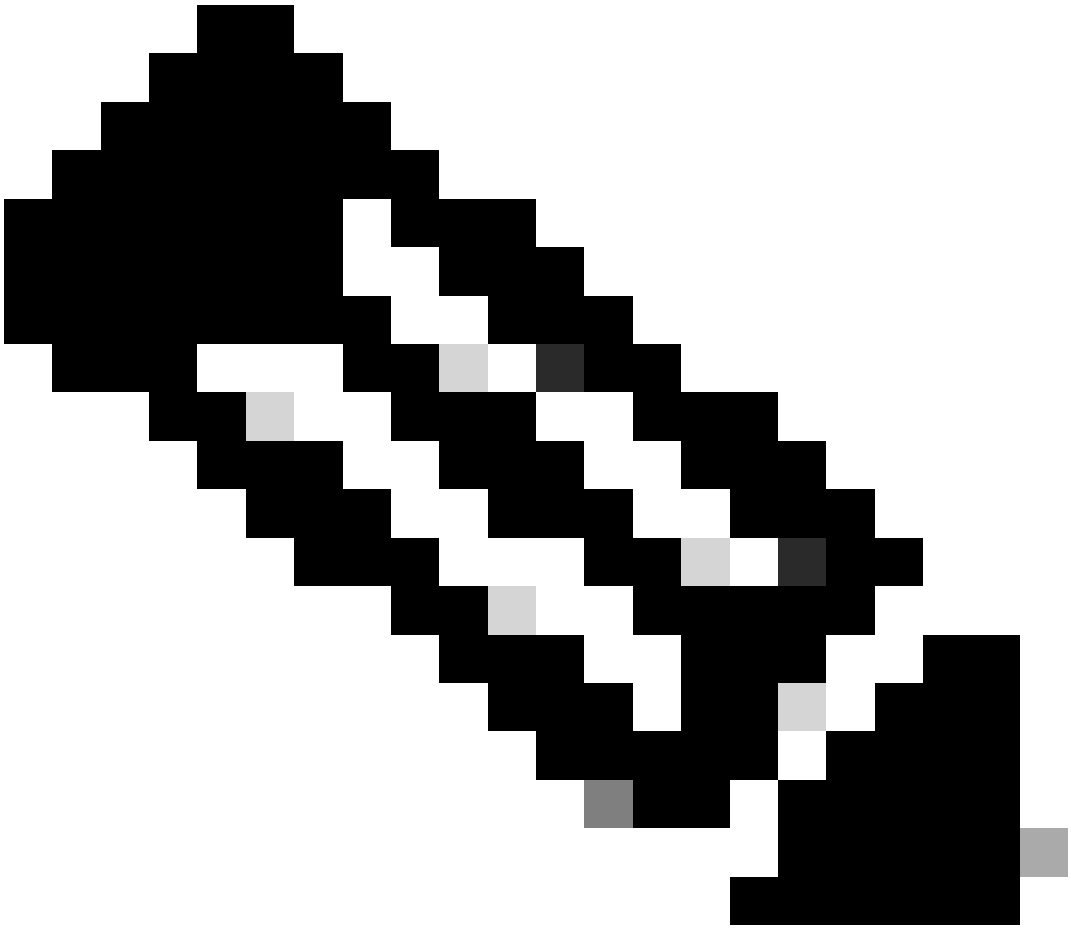
Schritt 1: Fahren Sie mit Cisco Software Download fort. Geben Sie in der Produktsuchleiste Secure Client 5 ein.

In diesem Konfigurationsbeispiel wird Version 5.1.11.388 verwendet. Die Installation wird mit der Pre-Deployment-Methode durchgeführt.

Suchen Sie auf der Download-Seite nach dem Cisco Secure Client Pre-Deployment Package (Windows), und laden Sie es herunter.

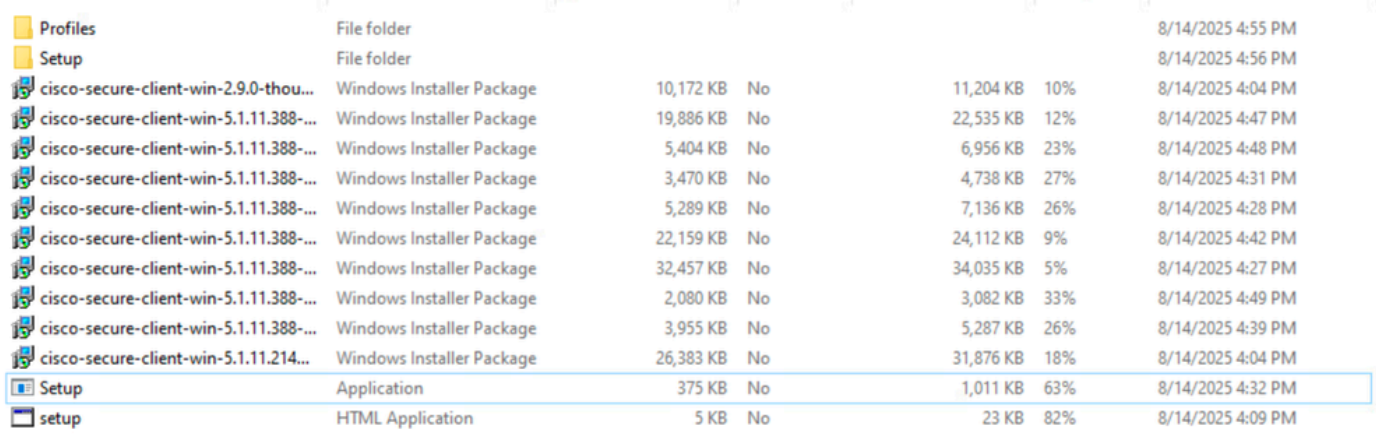


ZIP-Datei vor der Bereitstellung



Anmerkung: Cisco AnyConnect ist veraltet und nicht mehr auf der Cisco Software-Download-Site verfügbar.

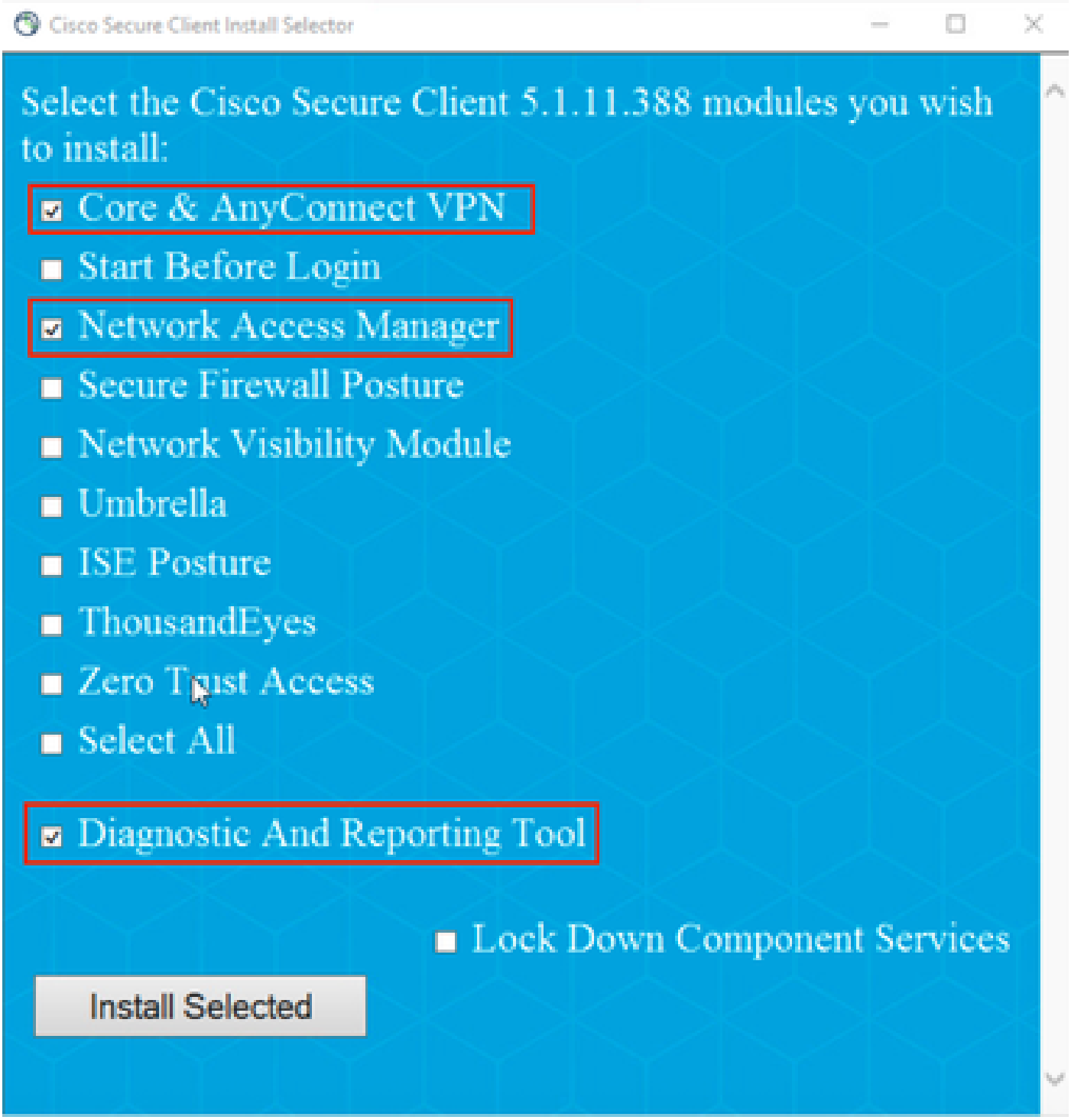
Schritt 2: Nach dem Herunterladen und Extrahieren klicken Sie auf Setup.



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

Vorbereitstellungs-Zip-Datei

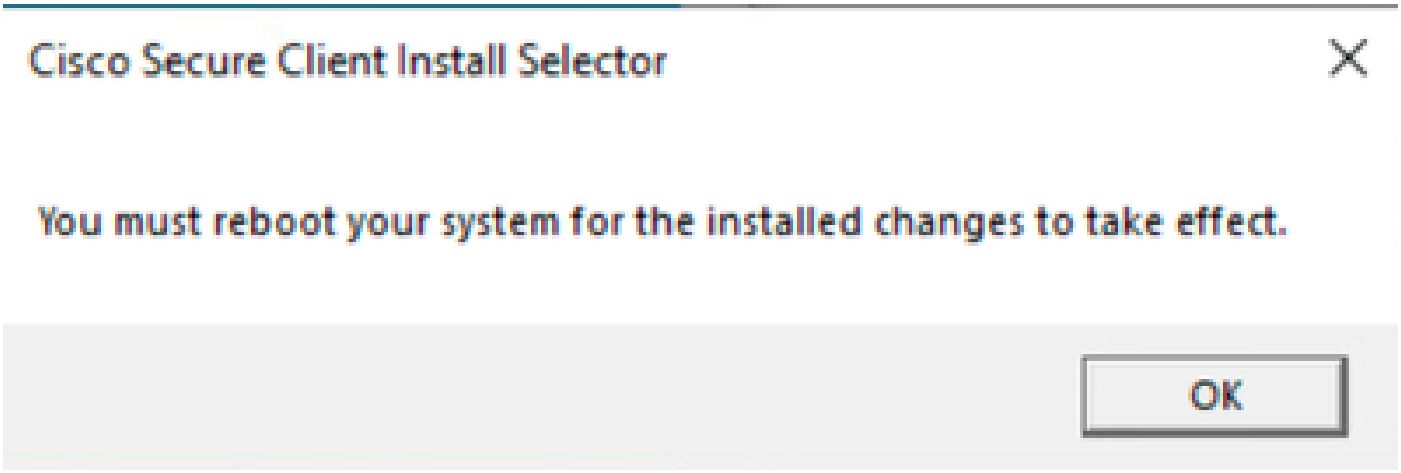
Schritt 3: Installieren Sie das Core & AnyConnect VPN, Network Access Manager und die Diagnostics and Reporting Toolmodule.



Secure Client-Installationsprogramm

Klicken Sie auf Install Selected (Ausgewählte installieren).

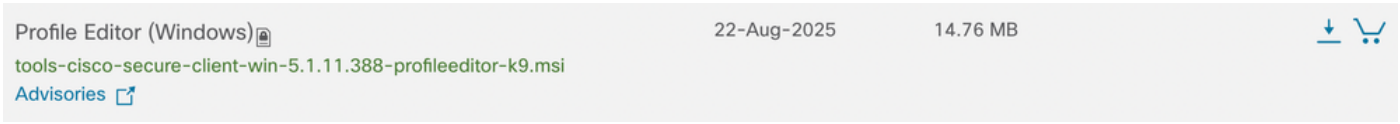
Schritt 4: Nach der Installation ist ein Neustart erforderlich. Klicken Sie auf OK, und starten Sie das Gerät neu.



Neustart erforderlich Pop-up

Teil 2: Herunterladen und Installieren des Secure Client NAM Profile Editor

Schritt 1. Der Profil-Editor befindet sich auf derselben Seite für Downloads wie der sichere Client. In diesem Konfigurationsbeispiel wird Version 5.1.11.388 verwendet.



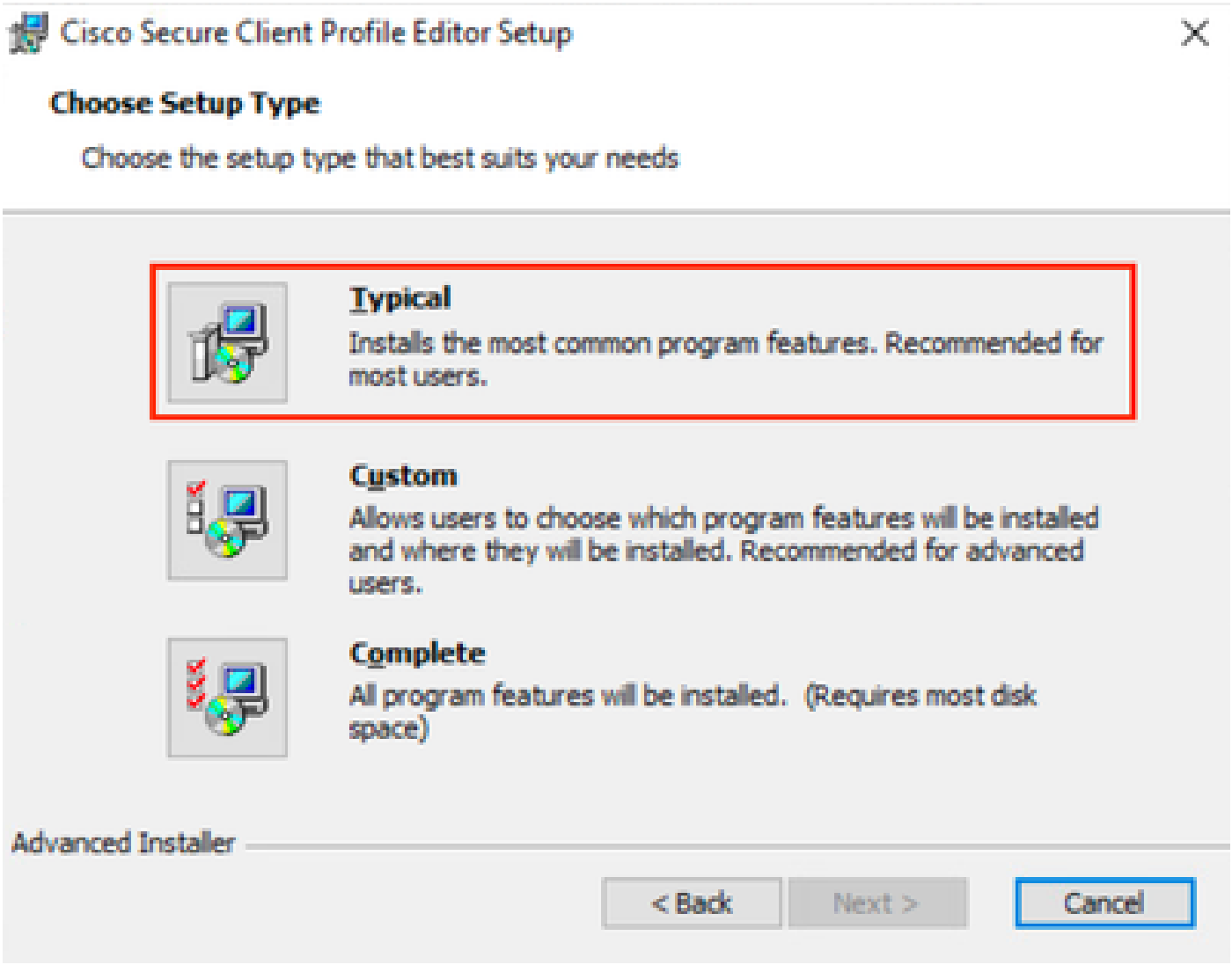
Profil-Editor

Laden Sie den Profil-Editor herunter, und installieren Sie ihn.

Schritt 2: Führen Sie die MSI-Datei aus.

Setup-Start des Profileditors

Schritt 3: Verwenden Sie die Option Typisches Setup, und installieren Sie den NAM Profile Editor.

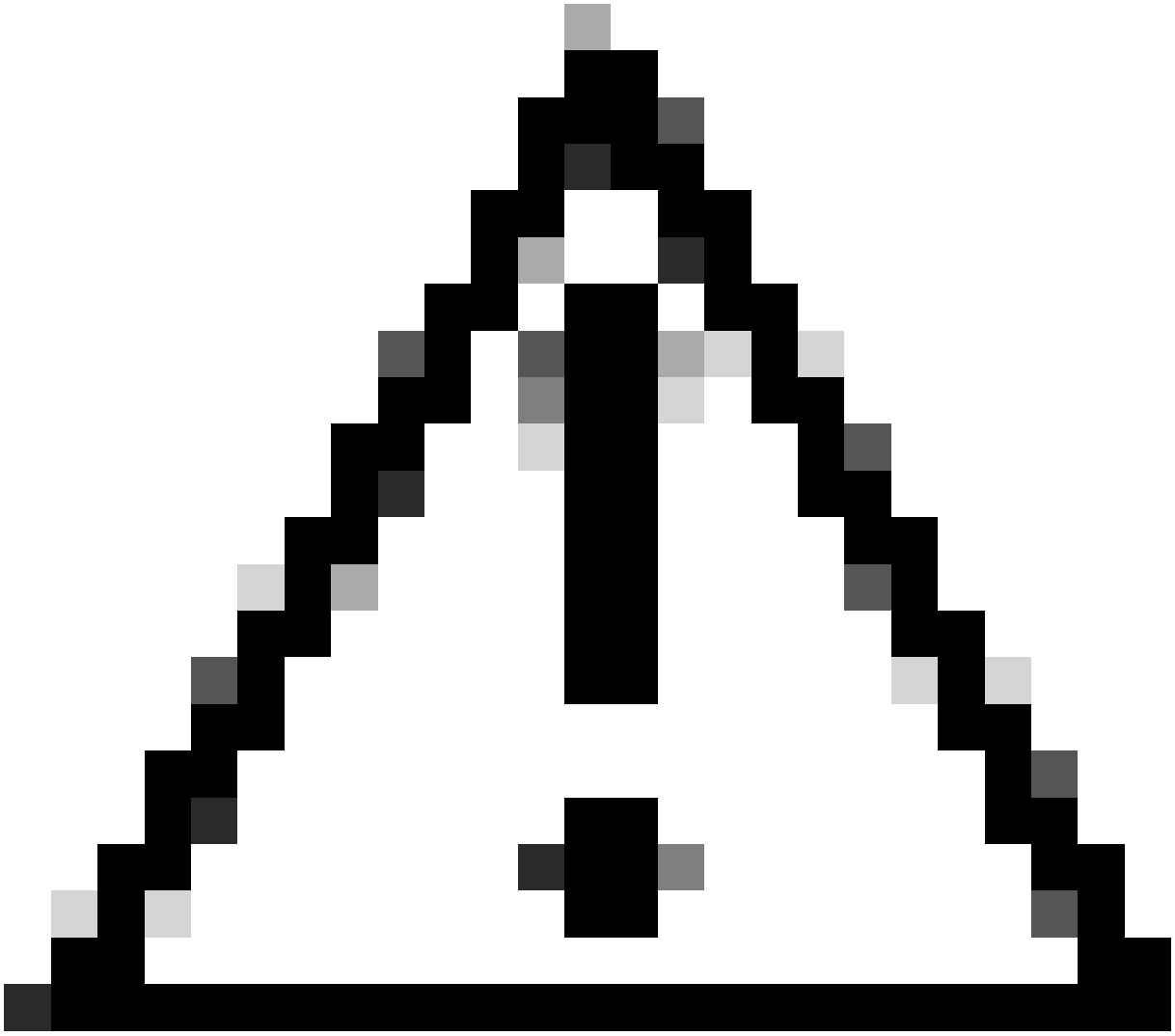


Profil-Editor einrichten

Teil 3: Zugriff auf Windows-Cacheanmeldeinformationen durch NAM zulassen

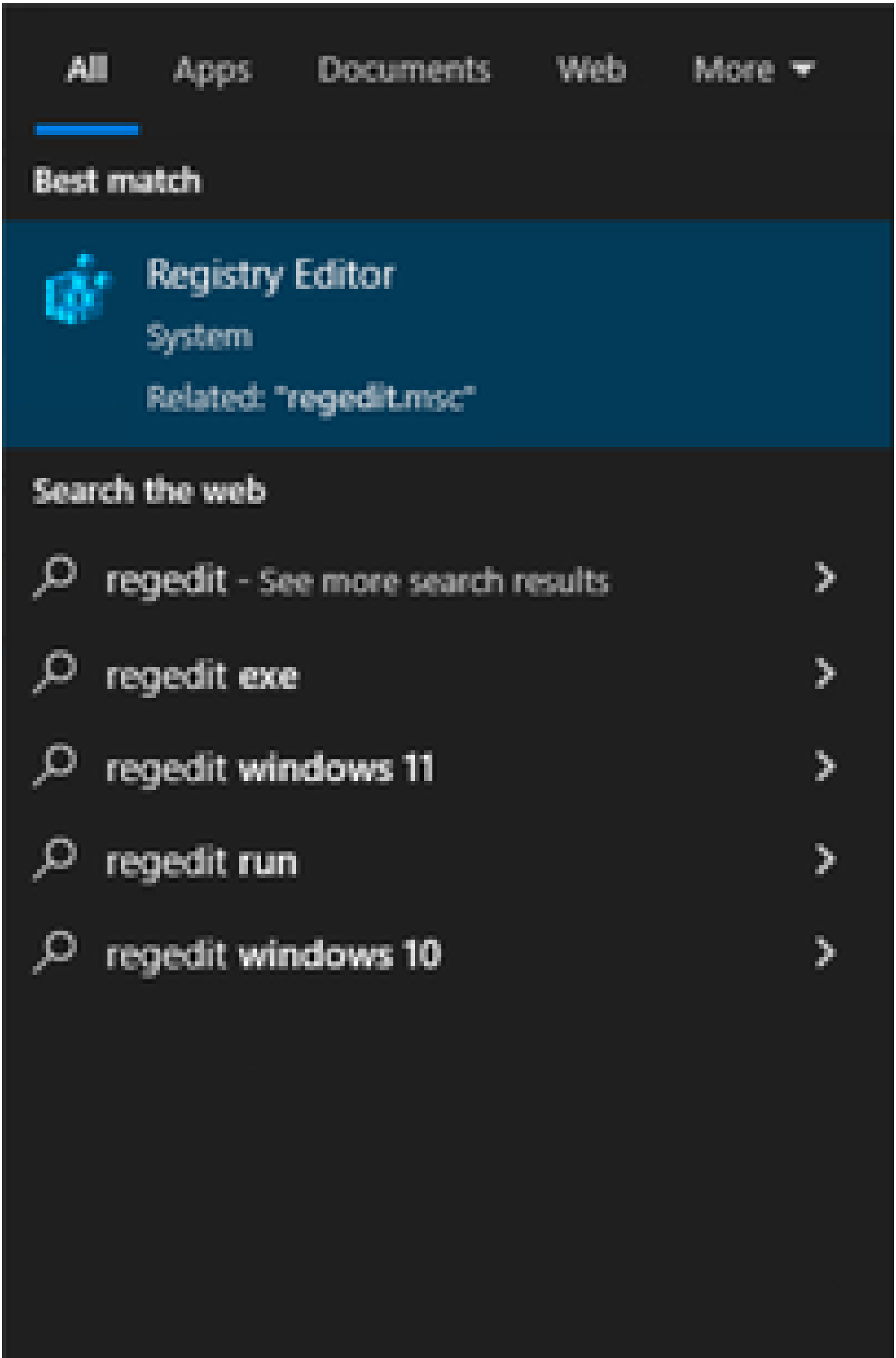
Standardmäßig verhindert das Betriebssystem in Windows 10, Windows 11 und Windows Server 2012, dass Network Access Manager (NAM) das für die Computerauthentifizierung erforderliche Computerkennwort abruft. Daher funktioniert die Computerauthentifizierung mit dem Computerkennwort nur dann, wenn ein Registrierungsfix angewendet wird.

Um NAM den Zugriff auf die Anmeldeinformationen des Computers zu ermöglichen, wenden Sie den Microsoft KB 2743127 Fix auf dem Client-Desktop an.



Vorsicht: Wenn Sie die Windows-Registrierung falsch bearbeiten, können schwerwiegende Probleme auftreten. Sichern Sie die Registrierung, bevor Sie Änderungen vornehmen.

Schritt 1: Geben Sie in der Windows-Suchleiste regedit ein, und klicken Sie dann auf Registrierungs-Editor.

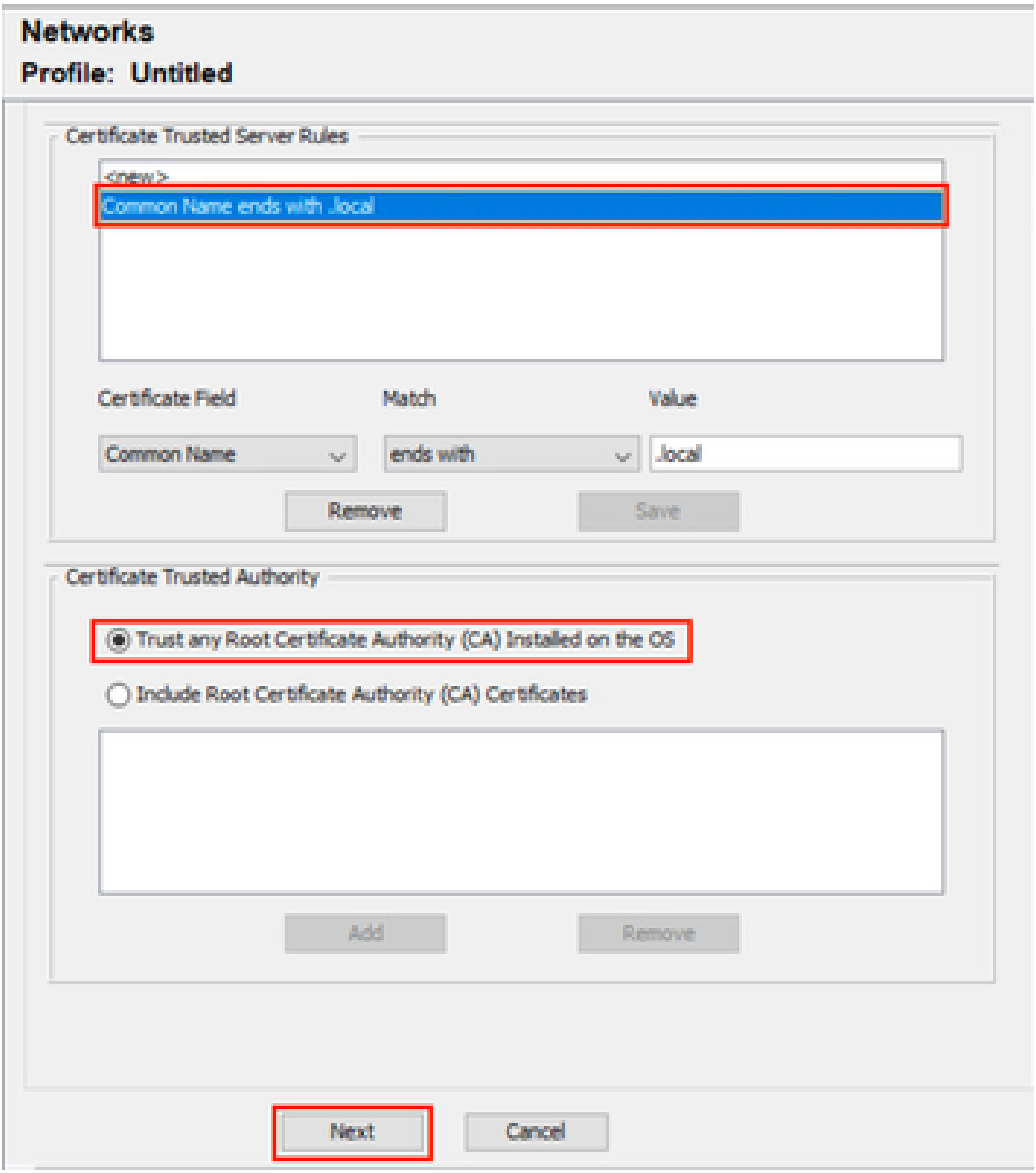

All
Apps
Documents
Web
More
Best match
Registry Editor
System
Related: "regedit.msc"
Search the web
regedit - See more search results
regedit exe
regedit windows 11
regedit run
regedit windows 10

In diesem Beispiel wird das PSN-Knotenzertifikat von varshaah.varshaah.local ausgestellt. Daher wird die Regel "Common Name" endet mit ".local" verwendet. Mit dieser Regel wird das Zertifikat validiert, das der Server während des EAP-TTLS-Flows präsentiert.

Sie können auch den allgemeinen Namen des PSN-EAP-Authentifizierungszertifikats (Policy Service Node) angeben.

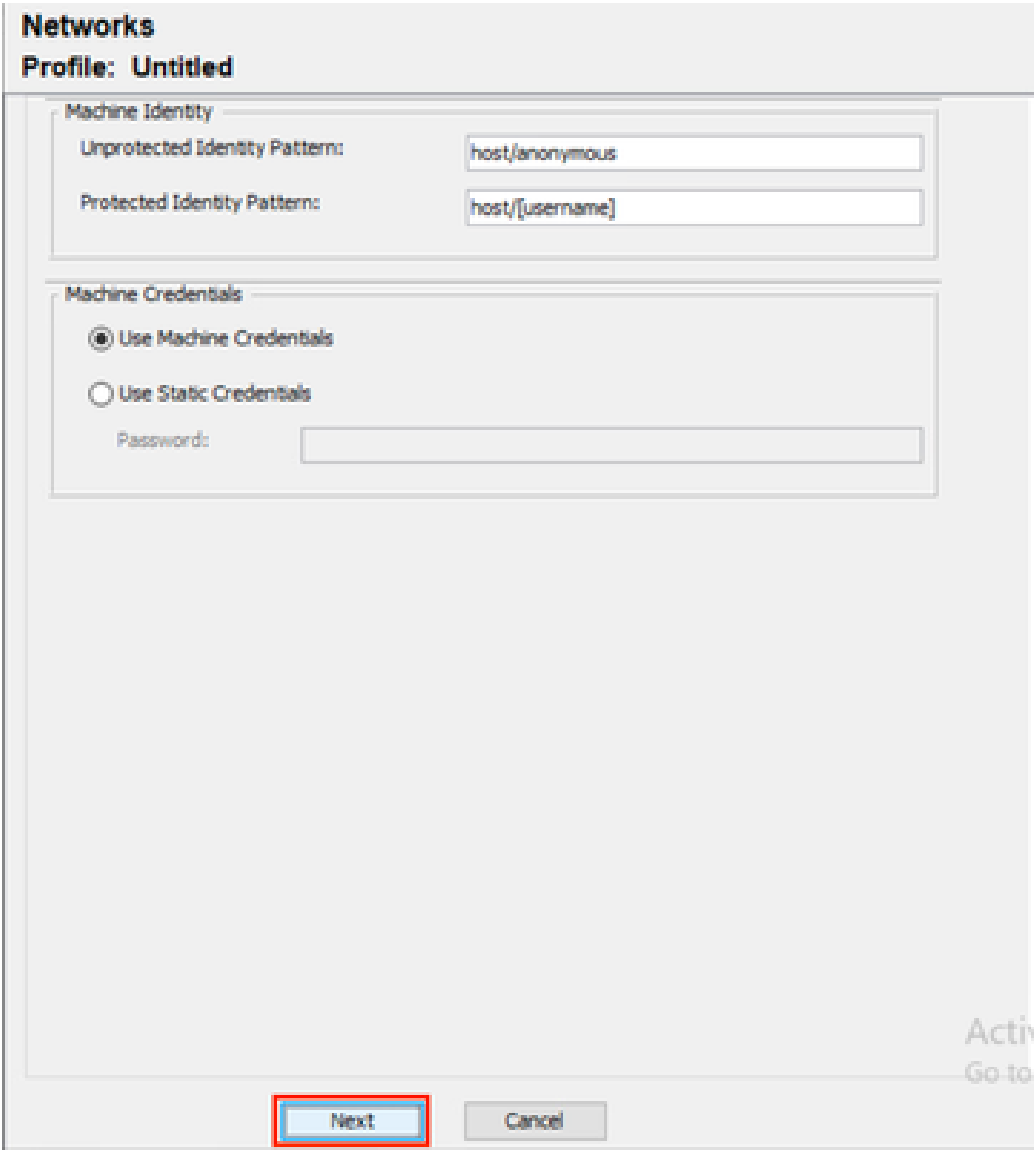
- Unter Certificate Trusted Authority (Vertrauenswürdige Zertifizierungsstelle für Zertifikate) stehen zwei Optionen zur Verfügung.
  In diesem Szenario wird die Option Auf eine beliebige auf dem Betriebssystem installierte Stammzertifizierungsstelle vertrauen verwendet, anstatt ein bestimmtes Zertifizierungsstellenzertifikat hinzuzufügen.

  Mit dieser Option vertraut das Windows-Gerät jedem EAP-Zertifikat, das von einem Zertifikat signiert wird, das in Certificates - Current User > Trusted Root Certification Authorities > Certificates (verwaltet vom Betriebssystem) enthalten ist.
- Klicken Sie auf Weiter, um fortzufahren.



NAM-Profil-Editor-Zertifikate

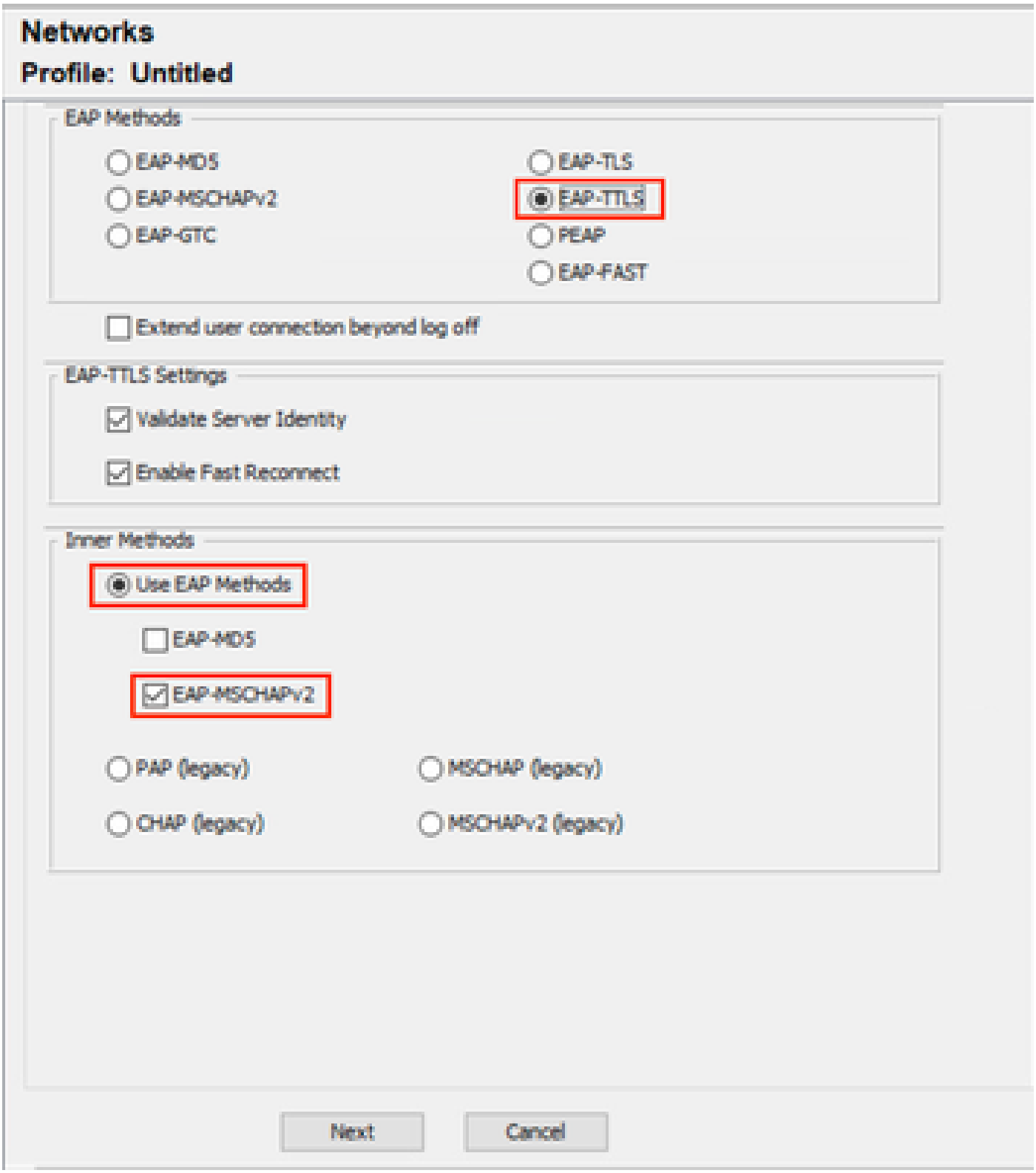
Schritt 6. Wählen Sie im Abschnitt Computeranmeldeinformationen die Option Computeranmeldeinformationen verwenden aus, und klicken Sie dann auf Weiter.



NAM-Profil-Editor-Anmeldeinformationen

Schritt 7: Konfigurieren Sie den Abschnitt "Benutzerauthentifizierung".

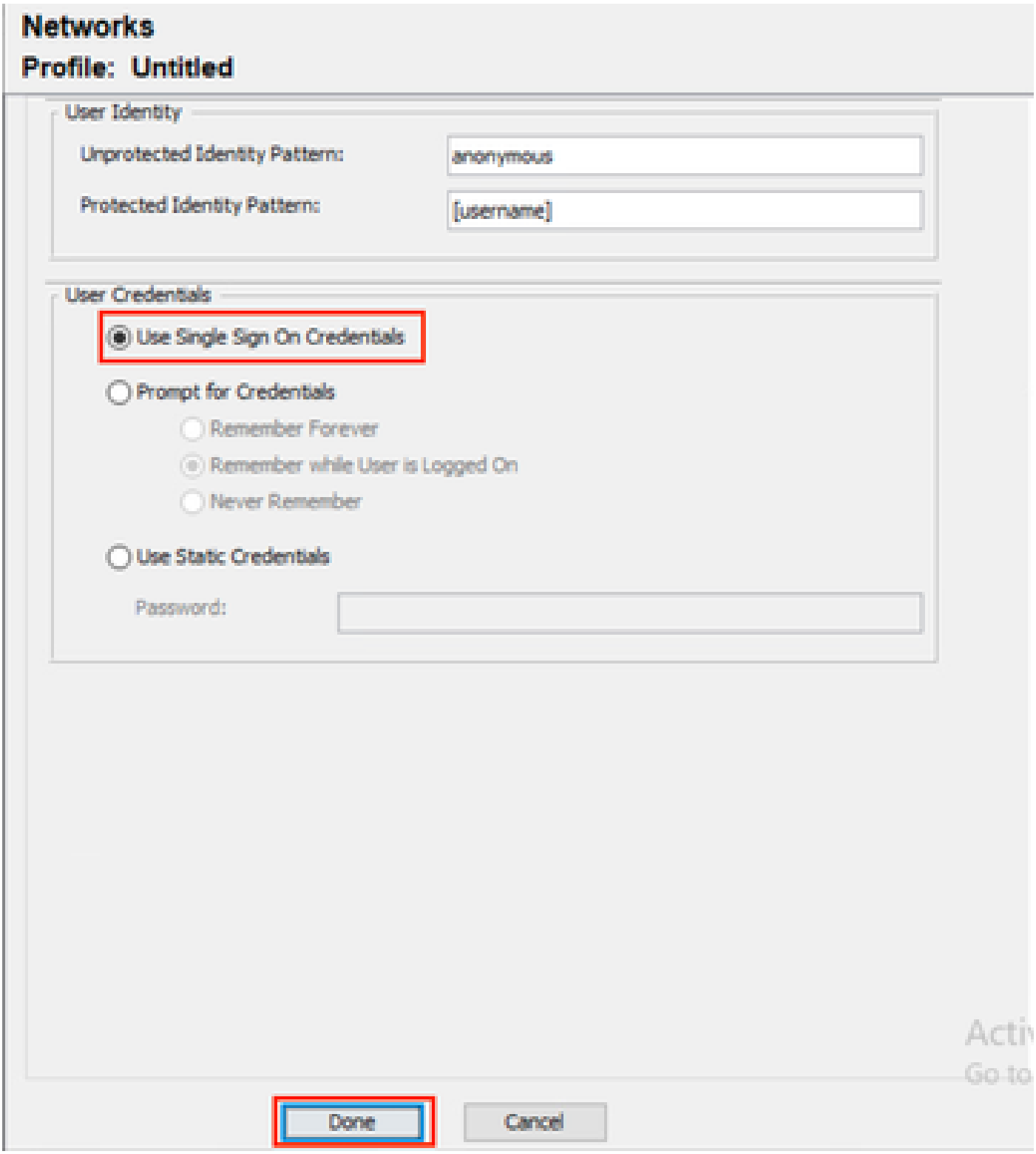
- Wählen Sie EAP-TTLS unter EAP-Methoden aus.
- Wählen Sie unter Interne Methoden die Option EAP-Methoden verwenden und dann EAP-MSCHAPv2 aus.
- Klicken Sie auf Next (Weiter).



Benutzerauthentifizierung im NAM-Profil-Editor

Schritt 8: Konfigurieren Sie in Certificates (Zertifikate) die gleichen Regeln für die Zertifikatsvalidierung wie in Schritt 5 beschrieben.

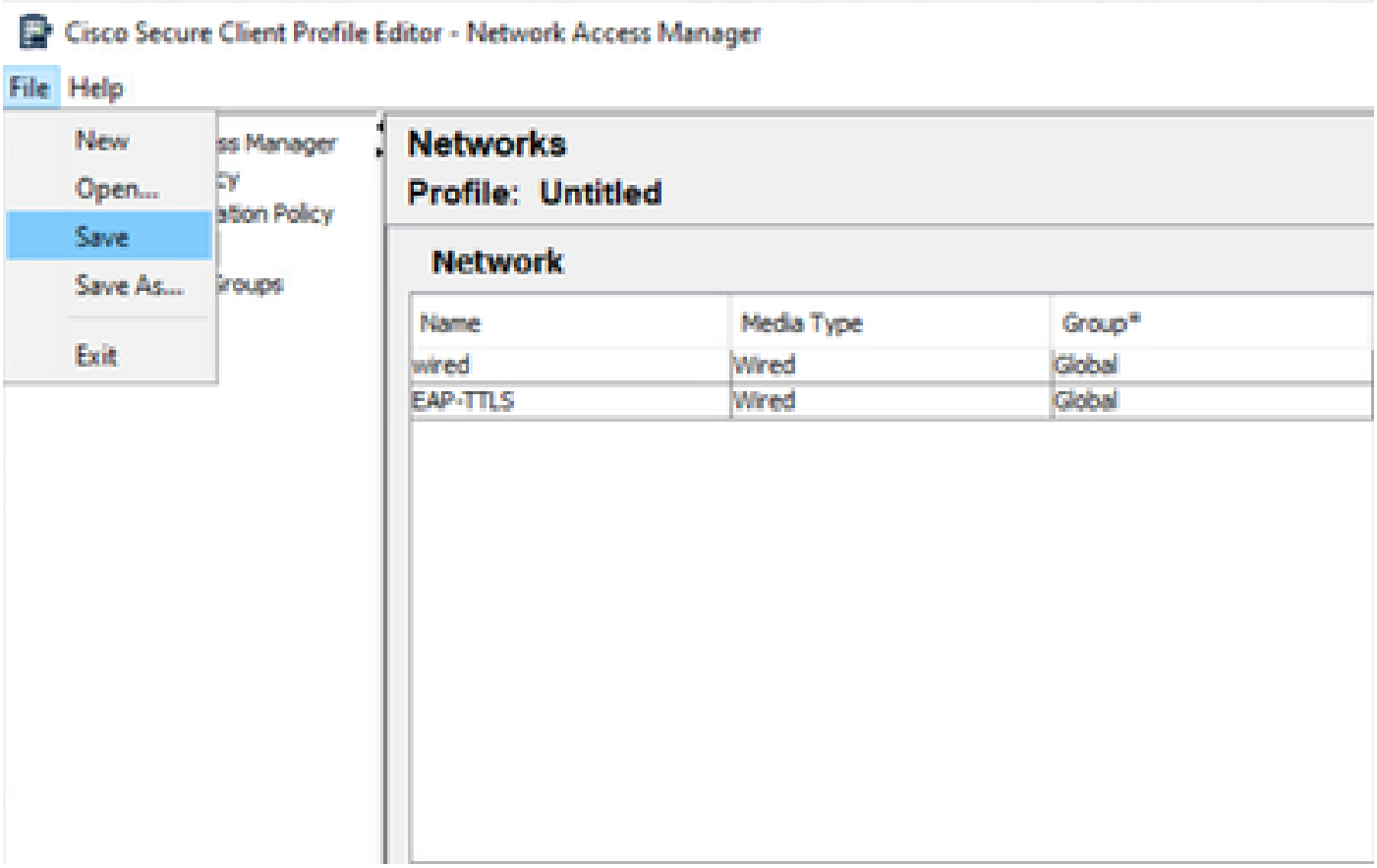
Schritt 9: Wählen Sie unter Benutzeranmeldeinformationen die Option Anmeldeinformationen für einmaliges Anmelden verwenden aus, und klicken Sie dann auf Fertig.



Benutzeranmeldeinformationen im NAM-Profil-Editor

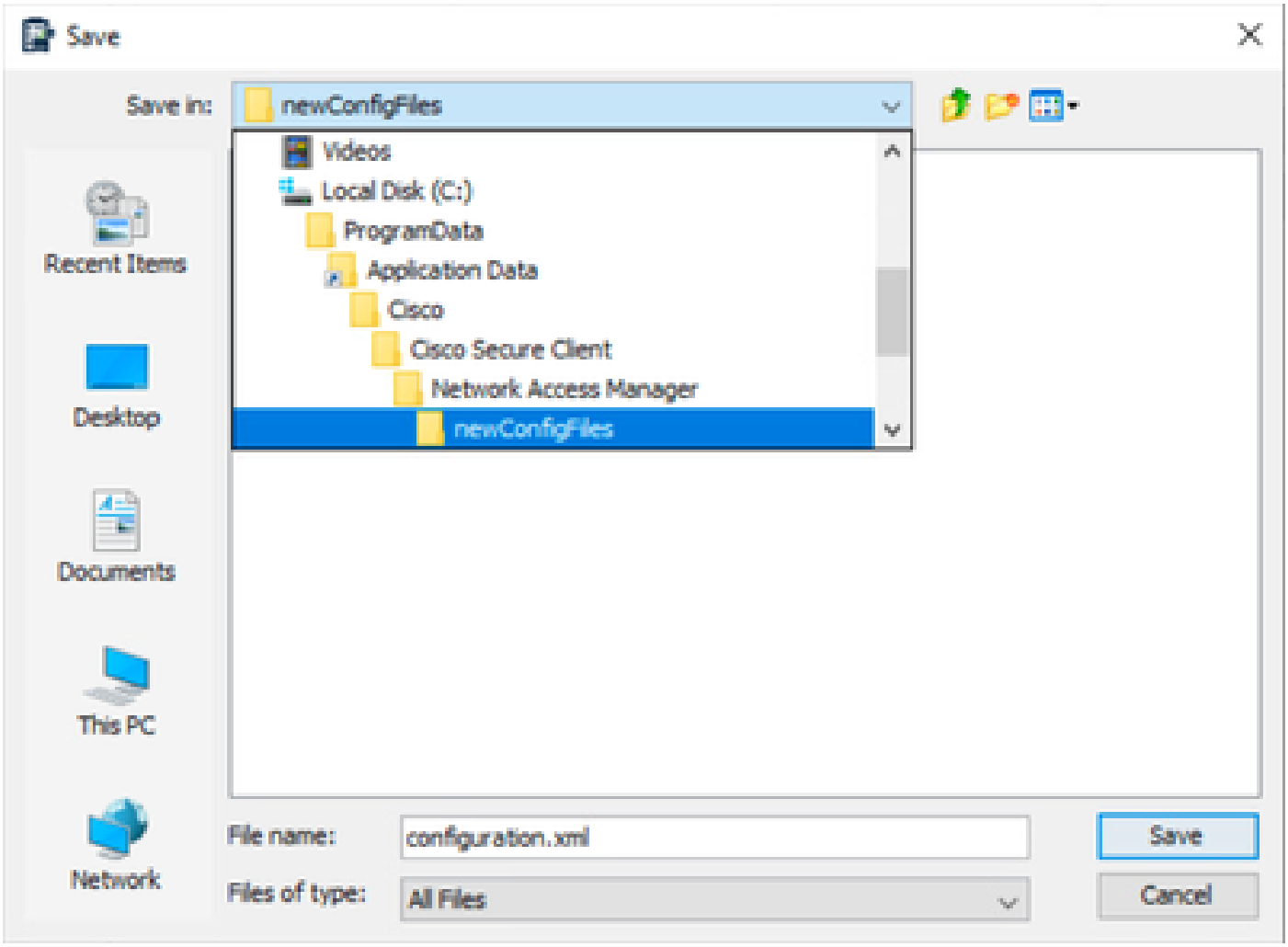
Teil 6: Speichern der Netzwerkkonfigurationsdatei

Schritt 1: Klicken Sie auf Datei > Speichern.



NAM Profile Editor Netzwerkkonfiguration speichern

Schritt 2: Speichern Sie die Datei als configuration.xml im Ordner newConfigFiles.

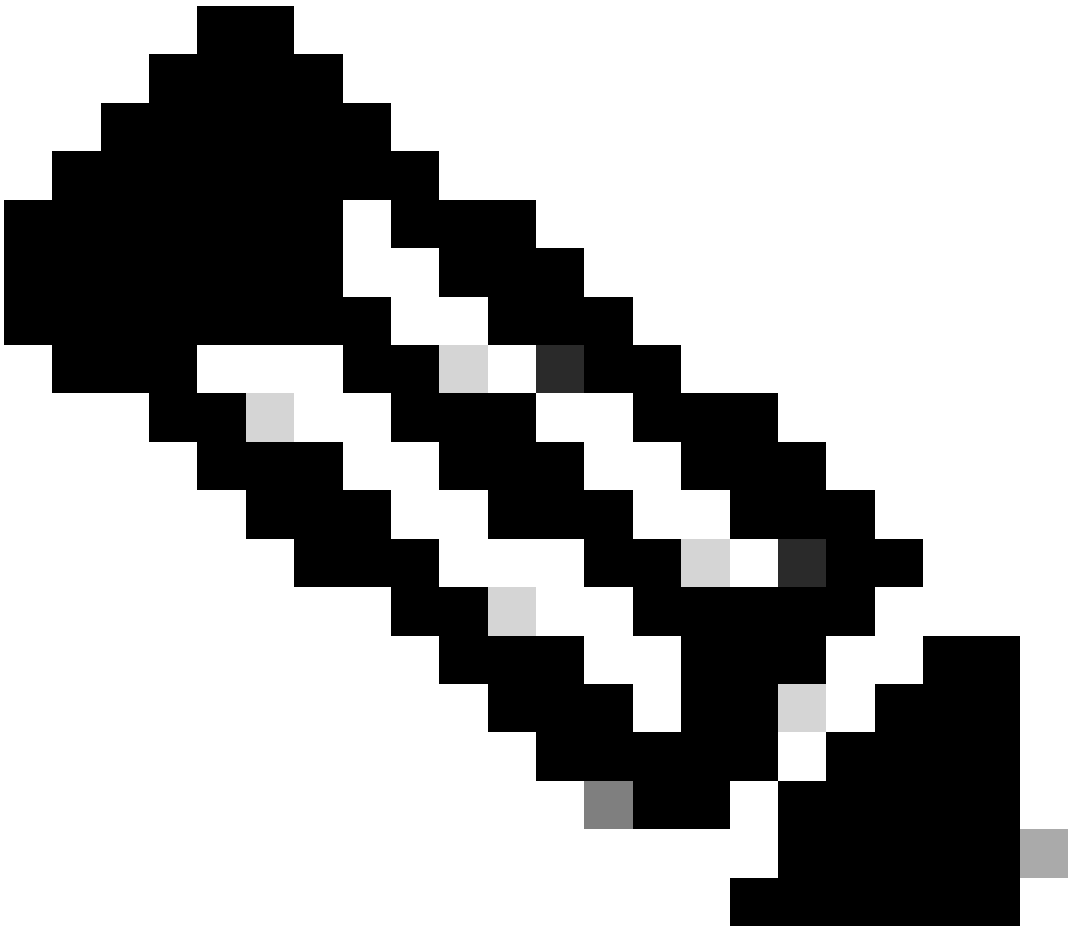


Netzwerkkonfiguration speichern

Teil 7: Konfigurieren von AAA auf dem Switch

```
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
```



> Anmerkung: Der Befehl dot1x system-auth-control wird in der Ausgabe von show running-config nicht angezeigt. Er ist jedoch erforderlich, um 802.1x global zu aktivieren.

Konfigurieren Sie die Switch-Schnittstelle für 802.1X:

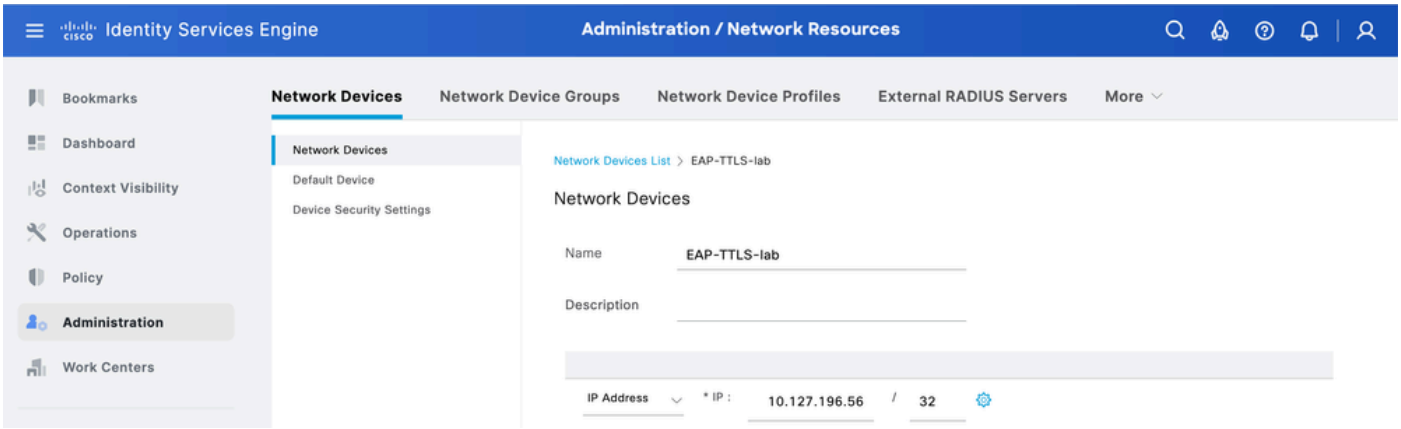
```
C9300-1(config)#do sh run int gig1/0/44
Building configuration...

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
```

Teil 8: ISE-Konfigurationen

Schritt 1: Konfigurieren des Switches auf der ISE

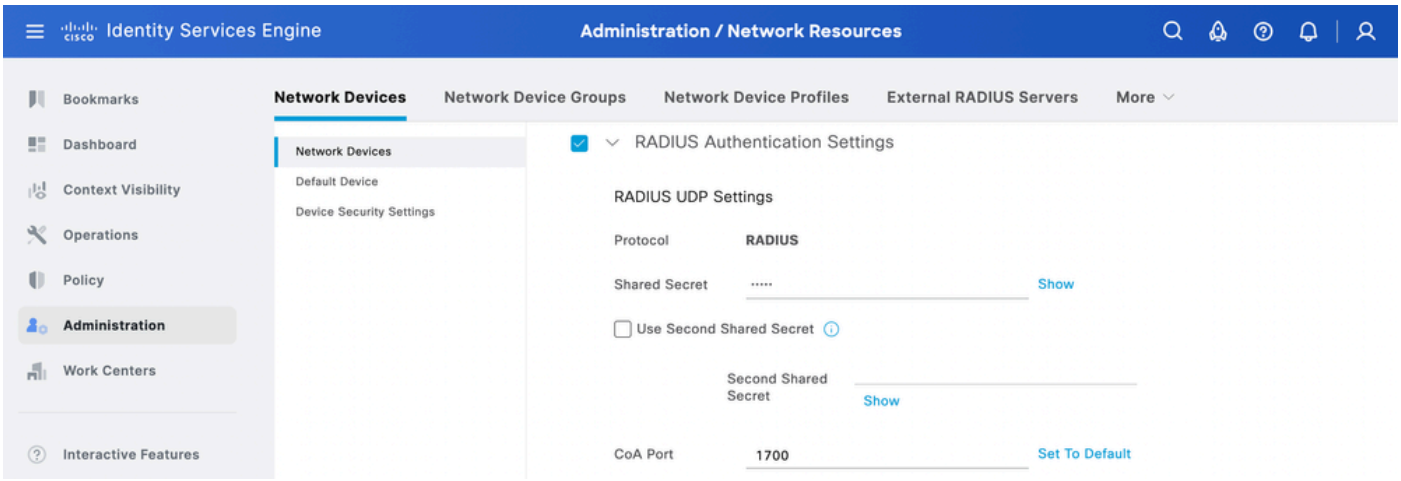
Navigieren Sie zu Administration > Network Resources > Network Devices, und klicken Sie auf Add.

Geben Sie hier den Namen und die IP-Adresse des Switches ein.



Hinzufügen der Netzwerkgerät-ISE

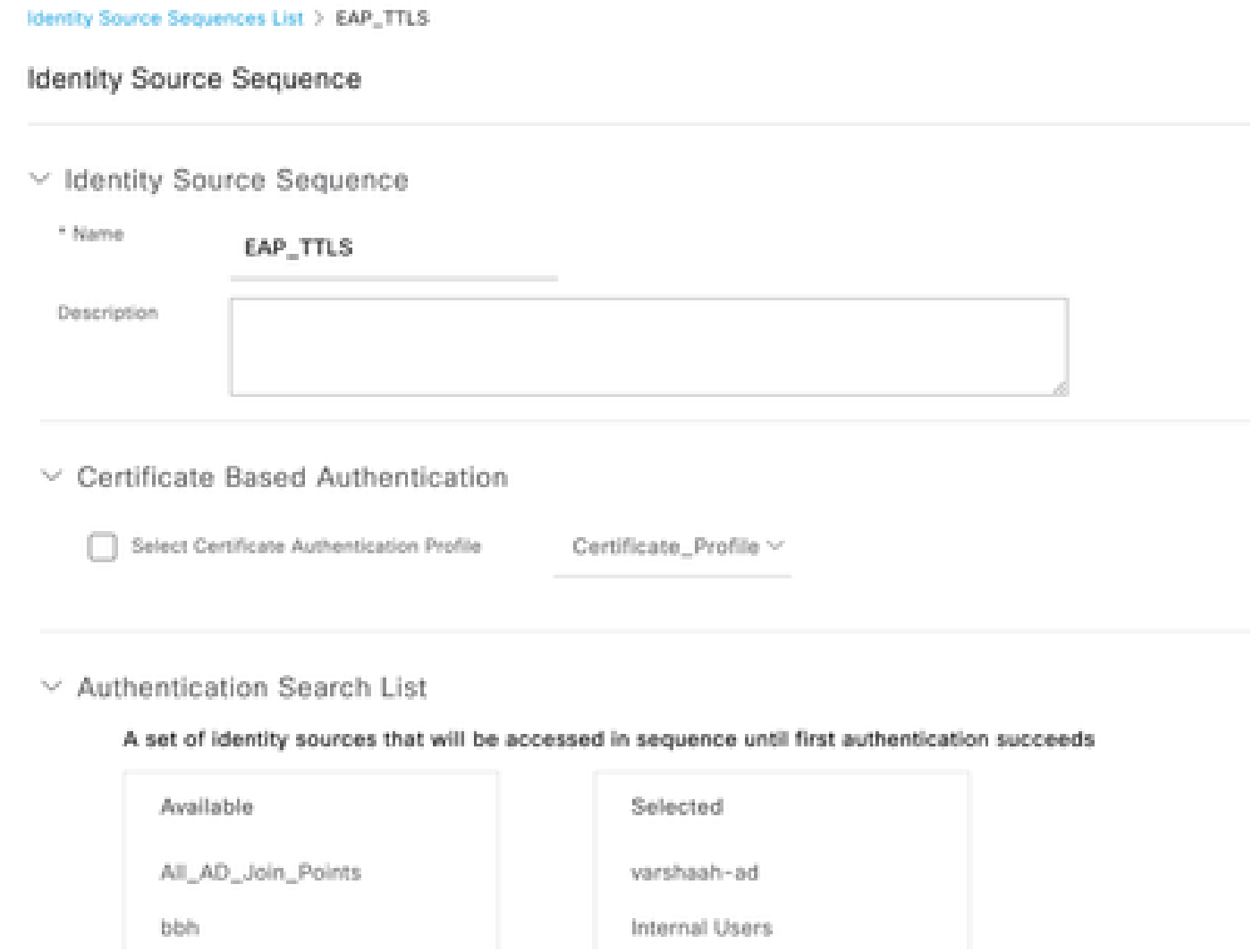
Geben Sie den gemeinsamen geheimen RADIUS-Schlüssel ein, der mit dem zuvor auf dem Switch konfigurierten Schlüssel identisch ist.



Gemeinsam genutzter geheimer RADIUS-ISE

Schritt 2: Konfigurieren der Identitätsquellsequenz

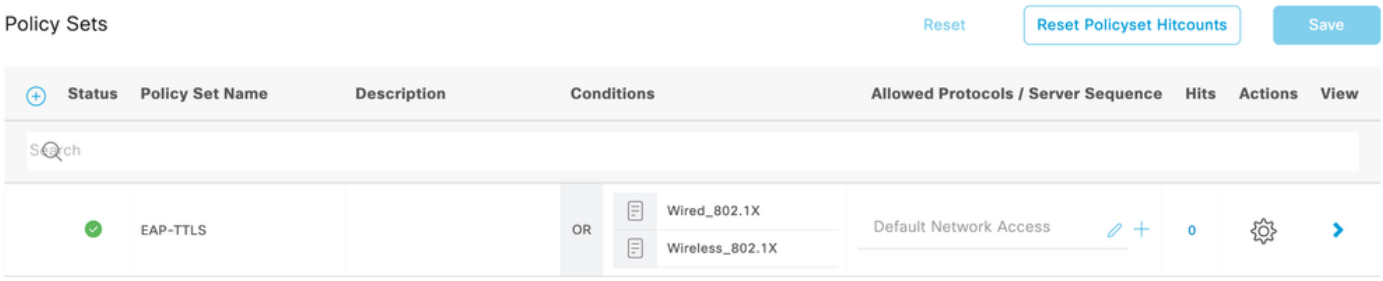
- Navigieren Sie zu Administration > Identity Management > Identity Source Sequences.
- Klicken Sie auf Hinzufügen, um eine neue Identitätsquellensequenz zu erstellen.
- Konfigurieren Sie die Identitätsquellen unter Authentifizierungssuchliste.



ISE-Identitätsquellensequenz

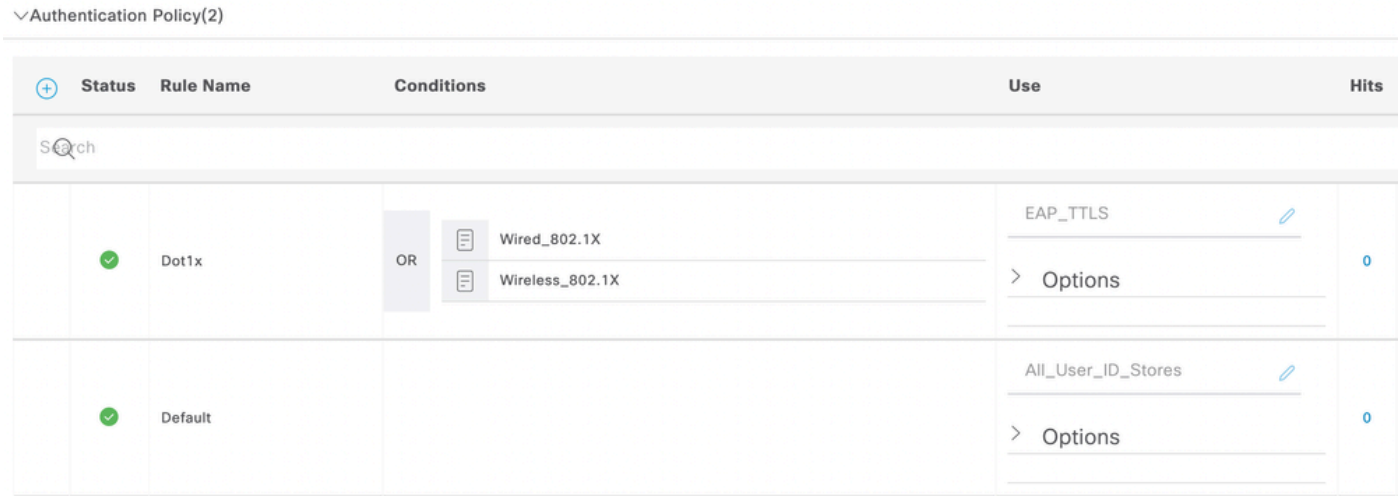
Schritt 3: Konfigurieren des Richtliniensatzes

Navigieren Sie zu Policy > Policy Sets, und erstellen Sie einen neuen Policy Set. Konfigurieren Sie die Bedingungen als Wired_802.1x ODER Wireless_802.1x. Wählen Sie für zulässige Protokolle Standard-Netzwerkzugriff aus:



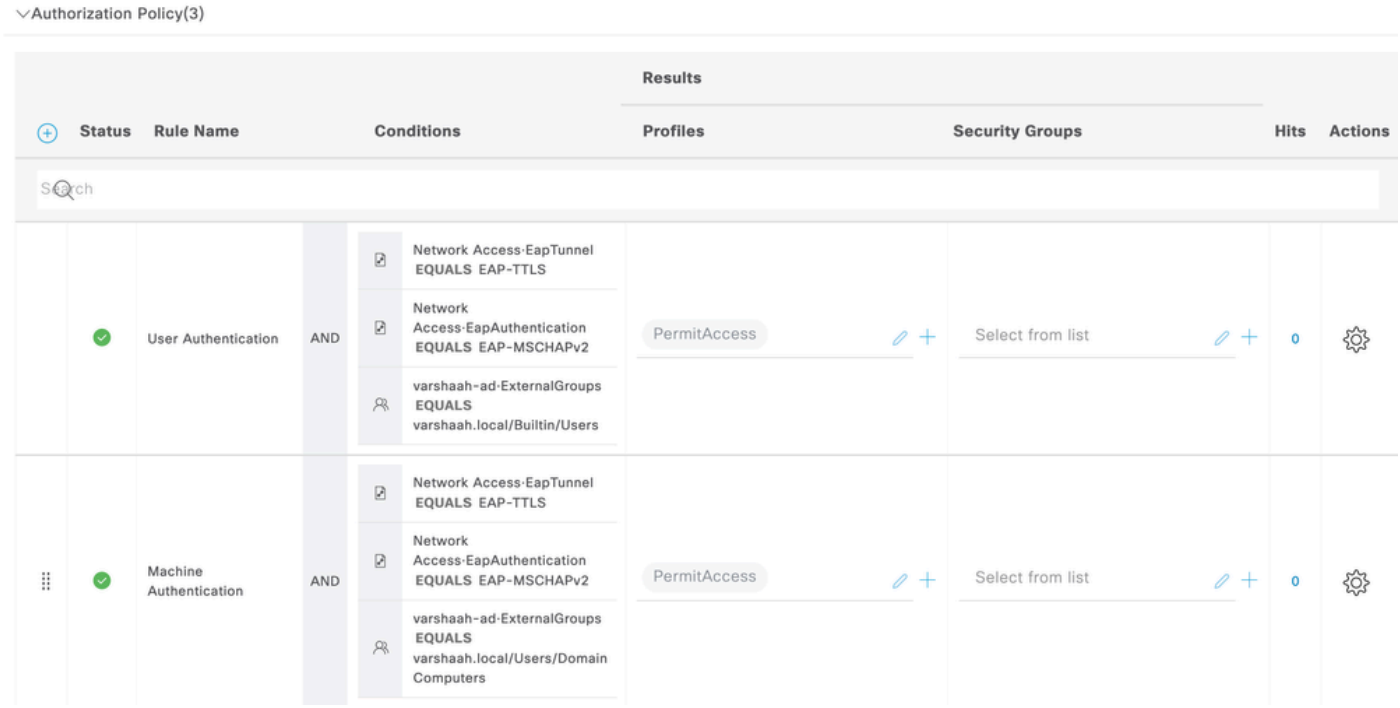
EAP-TTLS-Richtlinienset

Erstellen Sie die Authentifizierungsrichtlinie für dot1x, und wählen Sie die in Schritt 4 erstellte Identitätsquellensequenz aus.



EAP-TTLS-Authentifizierungsrichtlinie

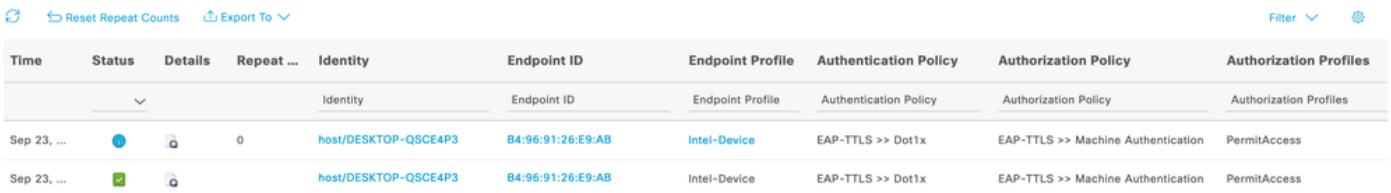
Erstellen Sie für die Autorisierungsrichtlinie die Regel mit drei Bedingungen. Die erste Bedingung prüft, ob der EAP-TTLS-Tunnel verwendet wird. Die zweite Bedingung prüft, ob EAP-MSCHAPv2 als innere EAP-Methode verwendet wird. Die dritte Bedingung prüft für die jeweilige AD-Gruppe.



dot1x-Autorisierungsrichtlinie

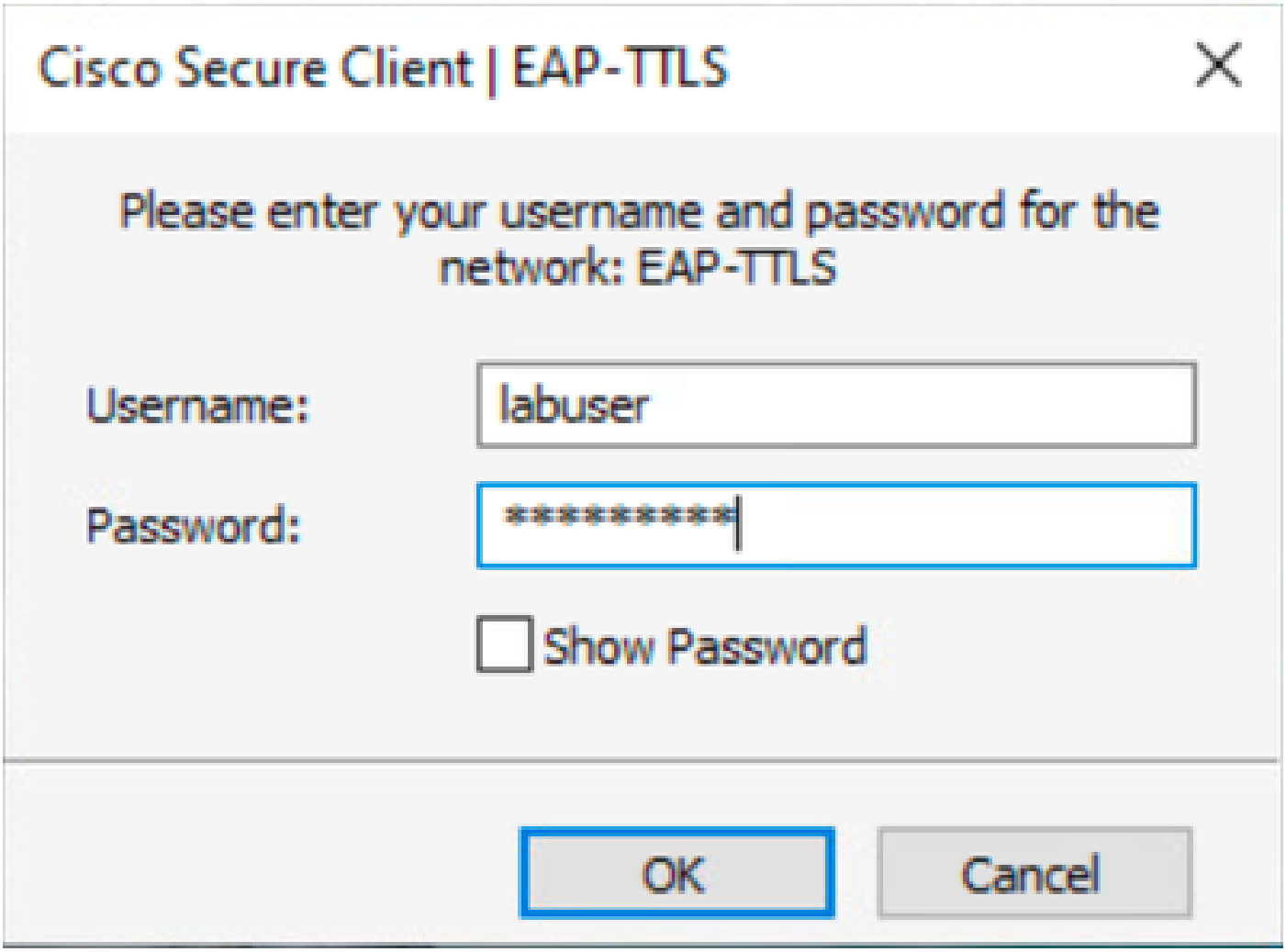
Überprüfung

Sie können den Windows 10-Computer neu starten oder sich abmelden und dann anmelden. Bei jeder Anzeige des Windows-Anmeldebildschirms wird die Systemauthentifizierung ausgelöst.

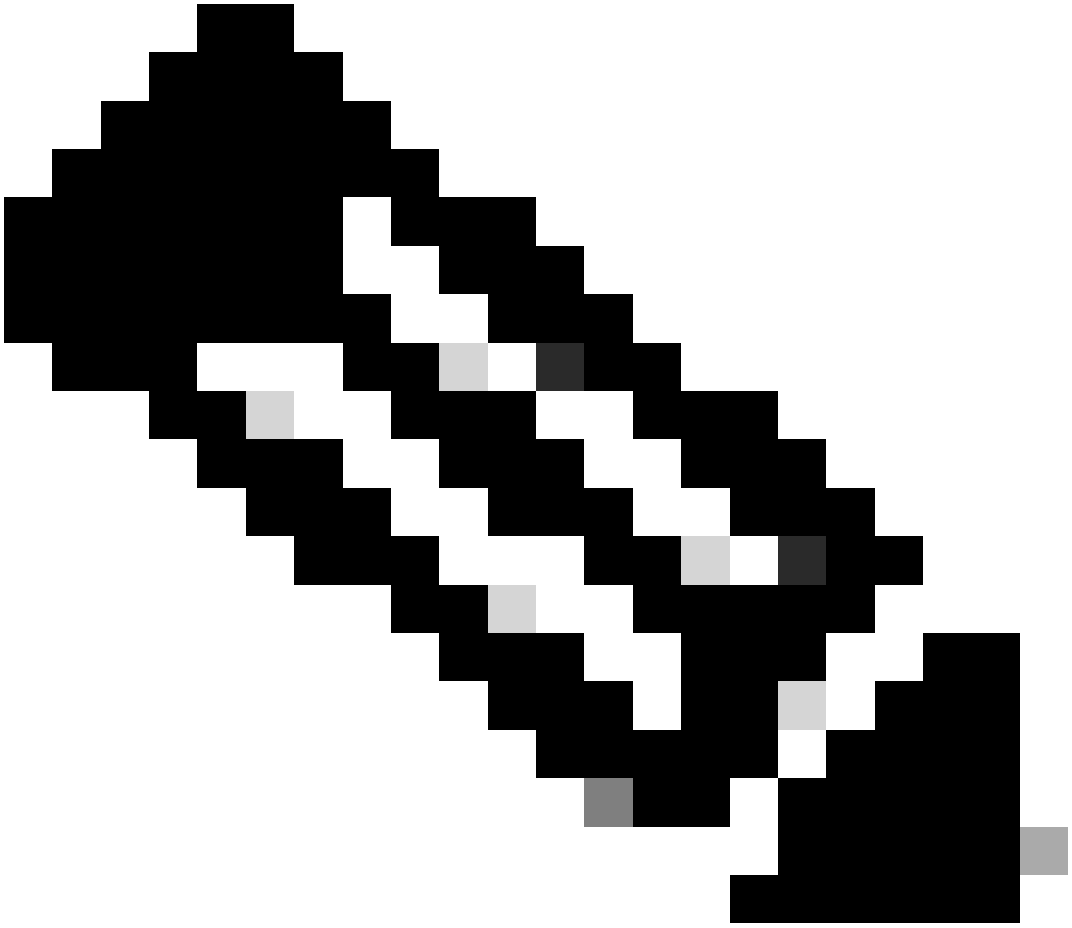


Live Log Machine-Authentifizierung

Wenn Sie sich mit Anmeldeinformationen beim PC anmelden, wird die Benutzerauthentifizierung ausgelöst.

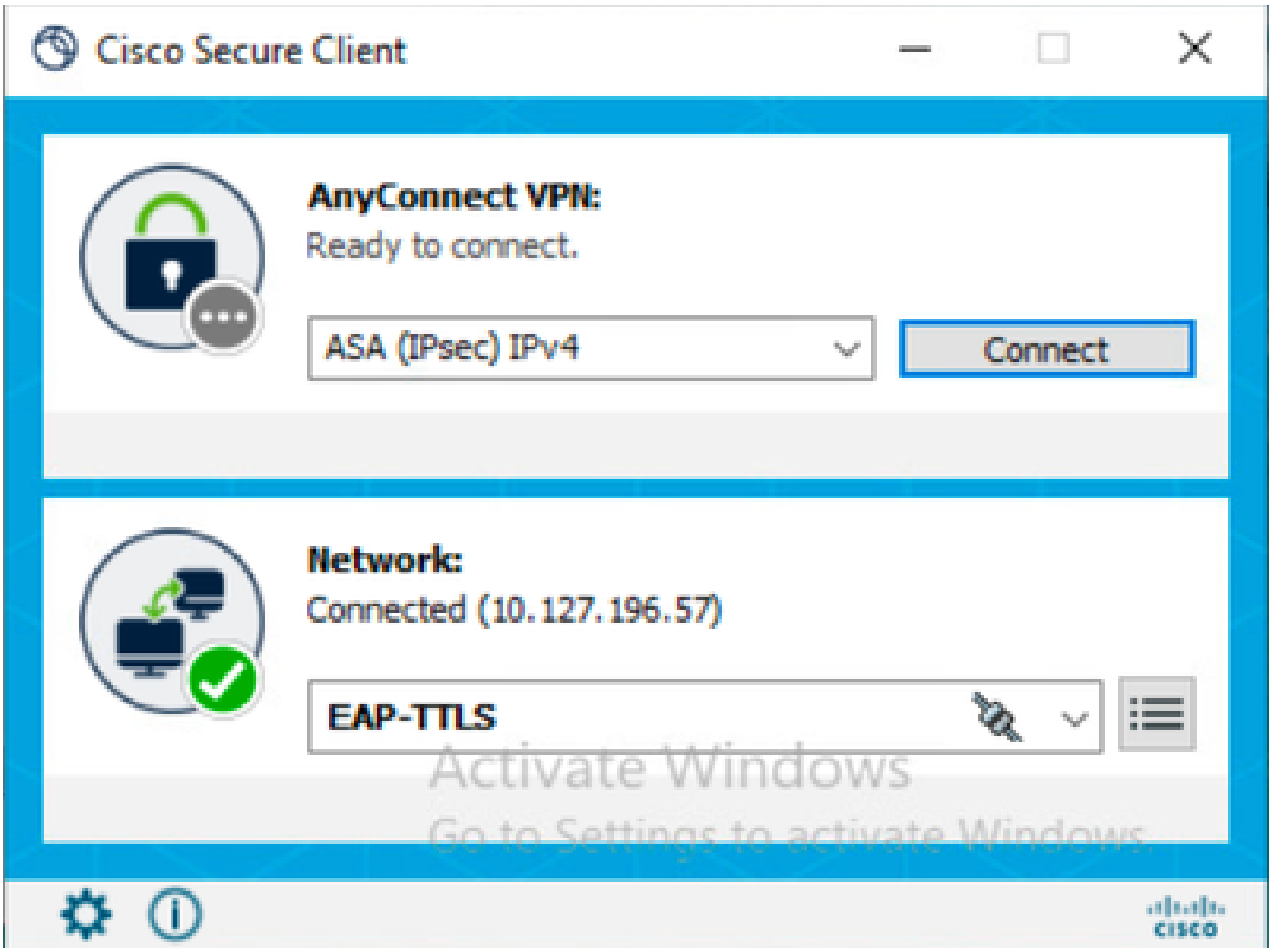


Anmeldeinformationen für die Benutzerauthentifizierung

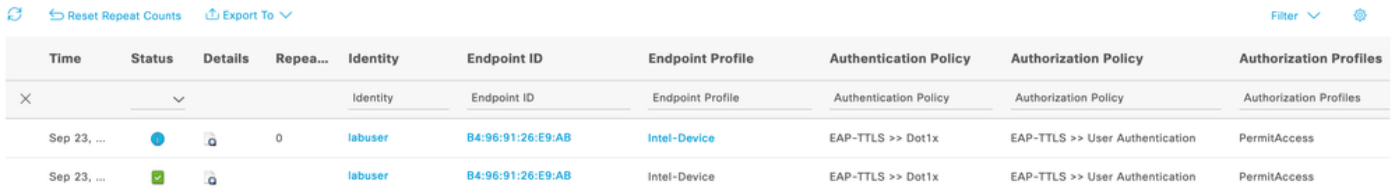


Anmerkung: In diesem Beispiel werden Active Directory-Benutzeranmeldeinformationen für die Authentifizierung verwendet. Alternativ können Sie einen internen Benutzer in der Cisco ISE erstellen und diese Anmeldeinformationen für die Anmeldung verwenden.

Nachdem die Anmeldeinformationen eingegeben und erfolgreich verifiziert wurden, wird der Endpunkt mit der Benutzerauthentifizierung mit dem Netzwerk verbunden.



EAP-TTLS verbunden



Benutzerauthentifizierung Live Log

Analyse von ISE RADIUS-Live-Protokollen

In diesem Abschnitt werden die RADIUS-Live-Protokolleinträge für die erfolgreiche Computer- und Benutzerauthentifizierung veranschaulicht.

Authentifizierung des Systems

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

Benutzerauthentifizierung

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-Protokolle analysieren

NAM-Protokolle enthalten, insbesondere nachdem Sie die erweiterte Protokollierung aktiviert haben, eine große Datenmenge, von der die meisten irrelevant sind und ignoriert werden können. In diesem Abschnitt werden die Debug-Zeilen aufgelistet, um die einzelnen Schritte von NAM zum Herstellen einer Netzwerkverbindung zu veranschaulichen. Wenn Sie ein Protokoll durcharbeiten, können diese Schlüsselbegriffe hilfreich sein, um einen Teil des Protokolls zu finden, der für das Problem relevant ist.

Authentifizierung des Systems

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

Der Client empfängt ein EAP-TTLS-Paket vom Netzwerk-Switch und initiiert so die EAP-TTLS-Sitzung. Dies ist der Ausgangspunkt für den Computer-Authentifizierungstunnel.

```
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
```

Der Client empfängt den Server Hello von der ISE und beginnt mit der Validierung des Serverzertifikats (CN=varshaah.varshaah.local). Das Zertifikat wurde im Vertrauensspeicher des Clients gefunden und zur Validierung hinzugefügt.

```
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
```

Das Serverzertifikat wurde erfolgreich validiert und schließt die Einrichtung des TLS-Tunnels ab.

```
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-
```

Der Client signalisiert, dass die Authentifizierung erfolgreich war. Die Schnittstelle ist entsperrt, und der interne Statuscomputer wechselt zu USER_T_NOT_DISCONNECTED, was darauf hinweist, dass der Computer jetzt Datenverkehr weiterleiten kann.

```
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-
```

Der Adapter meldet die Authentifizierung, und der NAM AccessStateMachine wechselt zu ACCESS_AUTHENTICATED. Dadurch wird bestätigt, dass der Computer die Authentifizierung erfolgreich abgeschlossen hat und über uneingeschränkten Netzwerkzugriff verfügt.

Benutzerauthentifizierung

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

Der NAM-Client startet den EAP-TTLS-Verbindungsvorgang.

```
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
```

NAM bindet den physischen Adapter an das EAP-TTLS-Netzwerk und wechselt in den Zustand ACCESS_ATTACHED, wodurch bestätigt wird, dass der Adapter für die Authentifizierung bereit ist.

```
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
```

Der Client wechselt von ANGESCHLOSSEN zu VERBINDEN und beginnt mit dem Austausch nach 802.1X.

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

Der Client sendet einen EAPOL-Start, um den Authentifizierungsprozess auszulösen.

```
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
```

Der Switch fordert eine Identität an, und der Client bereitet sich darauf vor, mit einer äußeren Identität zu antworten.

```
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 sendet die äußere Identität. Standardmäßig ist dies anonym, was darauf hinweist, dass der Austausch für die Benutzerauthentifizierung (nicht für den Computer) erfolgt.

```
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
```

Sowohl der Client als auch der Server stimmen zu, EAP-TTLS als äußere Methode zu verwenden.

```
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
```

Der Client sendet Client Hello und empfängt Server Hello, das das ISE-Zertifikat enthält.

```
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
```

Das Serverzertifikat wird angezeigt. Der Client sucht nach der CN varshaah.varshaah.local, findet eine Übereinstimmung und validiert das Zertifikat. Der Handshake wird angehalten, während das X.509-Zertifikat überprüft wird.

```
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
```

Der Tunnel ist eingerichtet. NAM fordert nun die geschützte Identität und die Anmeldeinformationen für die interne Authentifizierung an und bereitet diese vor.

```
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
```

Der TLS-Handshake ist beendet. Für die innere Authentifizierung wurde ein sicherer Tunnel eingerichtet.

```
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
```

Die geschützte Identität (Benutzername) wird von der ISE gesendet und akzeptiert.

```
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
```

Die ISE fordert das Kennwort an. NAM sendet das geschützte Kennwort in den 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
```

Die ISE validiert das Kennwort, sendet EAP-Success und NAM-Übergänge an AUTHENTIFIZIERT. An diesem Punkt ist die Benutzerauthentifizierung abgeschlossen, und dem Client wird der Netzwerkzugriff gewährt.

Fehlerbehebung

Bei der Behebung von Network Access Manager (NAM)-Problemen mit der Cisco ISE und Switch-Integration müssen Protokolle von allen drei Komponenten erfasst werden: Secure Client (NAM), Cisco ISE und der Switch.

Protokolle des sicheren Clients (NAM)

1. Aktivieren Sie die erweiterte NAM-Protokollierung, indem Sie folgende Schritte ausführen.
2. Reproduzieren des Problems Wenn das Netzwerkprofil nicht zutrifft, führen Sie Network Repair in Secure Client aus.
3. Sammeln Sie das DART-Paket mithilfe des Diagnose- und Reporting-Tools (DART).

Cisco ISE-Protokolle

Aktivieren Sie diese Fehlerbehebungen auf der ISE, um die Authentifizierung und Verzeichnisinteraktionen zu erfassen:

- Laufzeit-AAA
- NSF
- NSF-Sitzung

Switch-Protokolle

Grundlegende Debugs

```
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
```

Erweiterte Debugs (falls erforderlich)

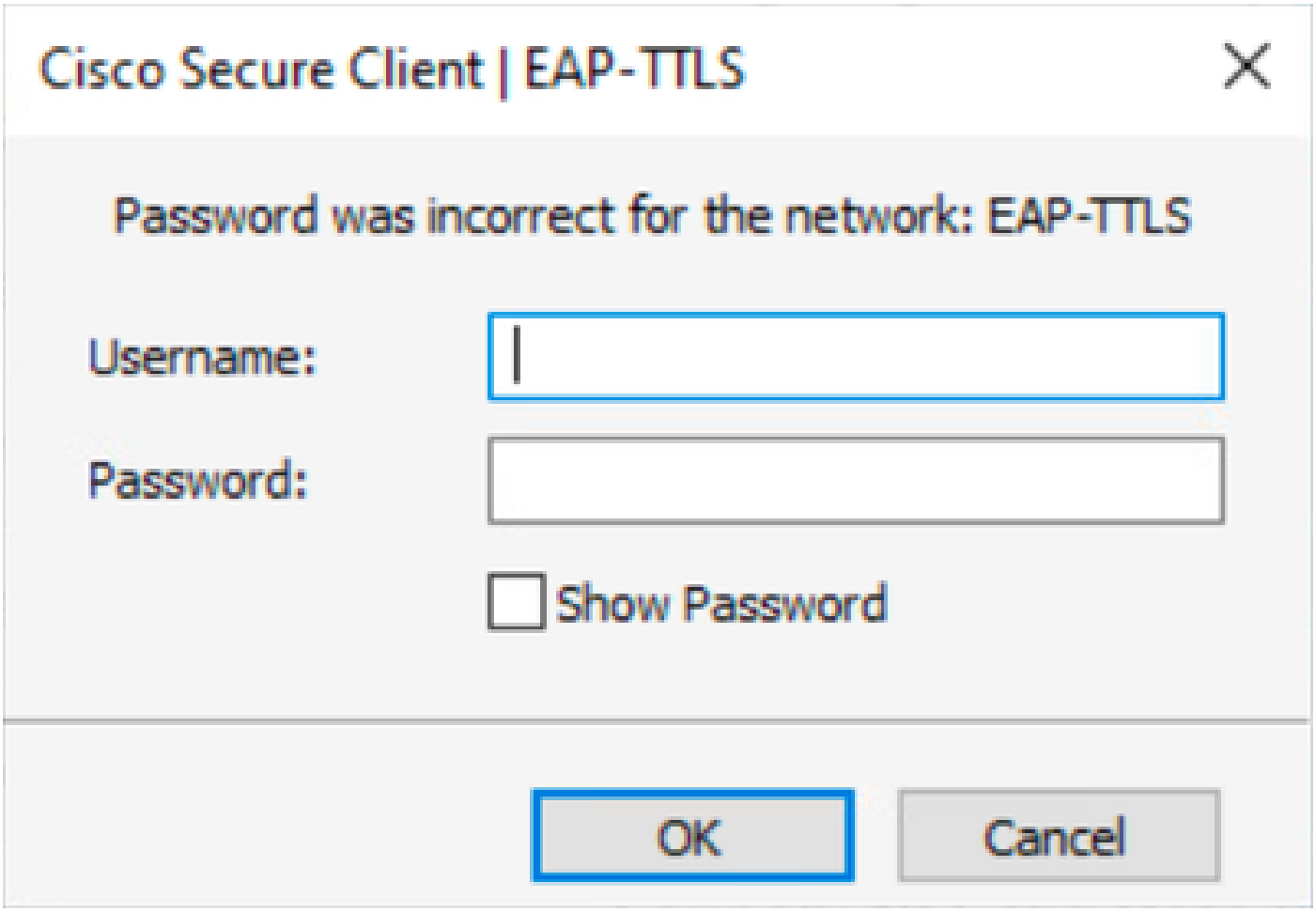
```
set platform software trace smd switch active R0 epm-all debug
set platform software trace smd switch active R0 pre-all debug
```

show-Befehle

```
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
```

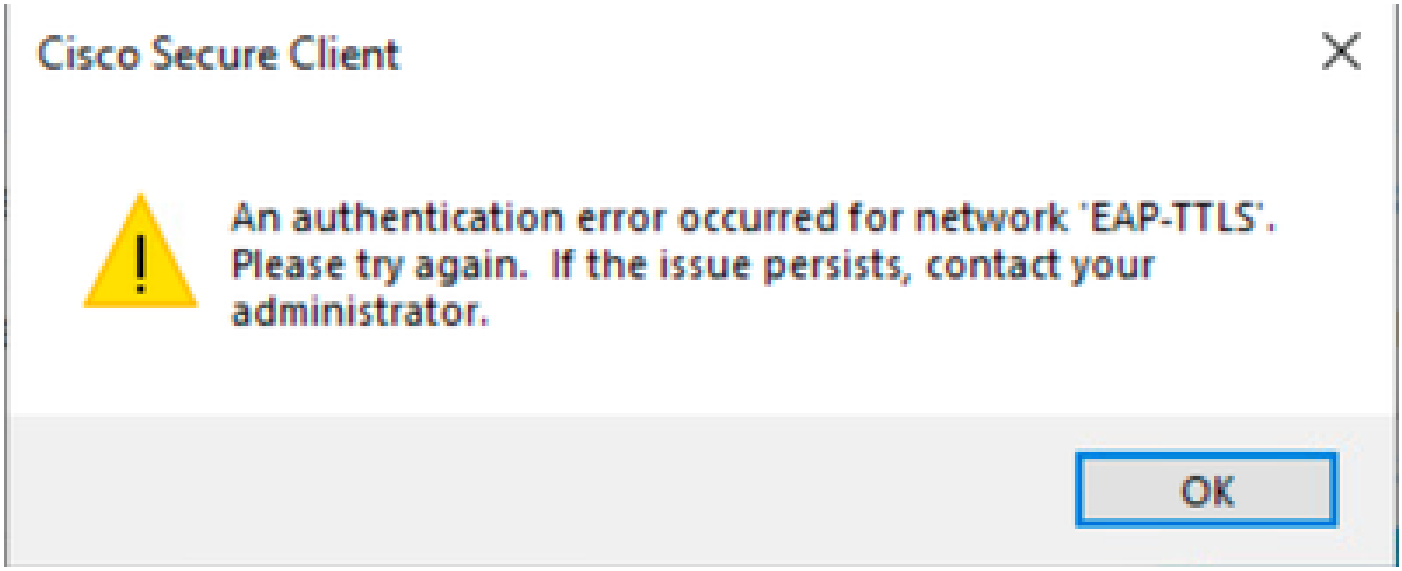
Fehler bei der Benutzerauthentifizierung aufgrund ungültiger Anmeldeinformationen

Wenn ein Benutzer falsche Anmeldeinformationen eingibt, zeigt Secure Client ein allgemeines Kennwort an, das für das Netzwerk falsch war: EAP-TTLS-Nachricht. Der Fehler auf dem Bildschirm gibt nicht an, ob das Problem auf einen ungültigen Benutzernamen oder ein ungültiges Kennwort zurückzuführen ist.



Falscher Kennwortfehler

Wenn die Authentifizierung zweimal hintereinander fehlschlägt, zeigt Secure Client die folgende Meldung an: Ein Authentifizierungsfehler ist für das Netzwerk 'EAP-TTLS' aufgetreten. Bitte versuchen Sie es erneut. Wenn das Problem weiterhin besteht, wenden Sie sich an Ihren Administrator.



Problem mit der Benutzerauthentifizierung

Um die Ursache zu ermitteln, überprüfen Sie die NAM-Protokolle.

1. Falsches Kennwort:

Wenn ein Benutzer ein falsches Kennwort eingibt, werden in den NAM-Protokollen ähnliche Einträge wie diese Ausgabe angezeigt:

```
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 den Live-Protokollen der Cisco ISE wird das entsprechende Ereignis wie folgt angezeigt:

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

Falsches Kennwort

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. Falscher Benutzername:

Wenn ein Benutzer einen falschen Benutzernamen eingibt, werden in den NAM-Protokollen ähnliche Einträge wie diese Ausgabe angezeigt:

```
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 den Live-Protokollen der Cisco ISE wird das entsprechende Ereignis wie folgt angezeigt:

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).

Falscher Benutzername

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**

Bekannte Fehler

Bug-ID	Beschreibung
Cisco Bug-ID: 63395	ISE 3.0 kann REST-ID-Speicher nach Neustart der Services nicht finden

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.