802.1x-WLAN + VLAN-Außerkraftsetzung mit Mobility Express (ME) 8.2 und ISE 2.1

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie ein WLAN (Wireless Local Area Network) mit Wi-Fi Protected Access 2 (WPA2) Enterprise-Sicherheit mit einem Mobility Express-Controller und einem externen RADIUS-Server (Remote Authentication Dial-In User Service) einrichten. Identity Service Engine (ISE) wird als Beispiel für externe RADIUS-Server verwendet.

Das in diesem Leitfaden verwendete Extensible Authentication Protocol (EAP) ist Protected Extensible Authentication Protocol (PEAP). Außerdem ist der Client einem bestimmten VLAN zugewiesen (außer dem VLAN, das standardmäßig zugewiesen ist).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- 802.1x
- PEAP
- Zertifizierungsstelle
- Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

ME v8.2

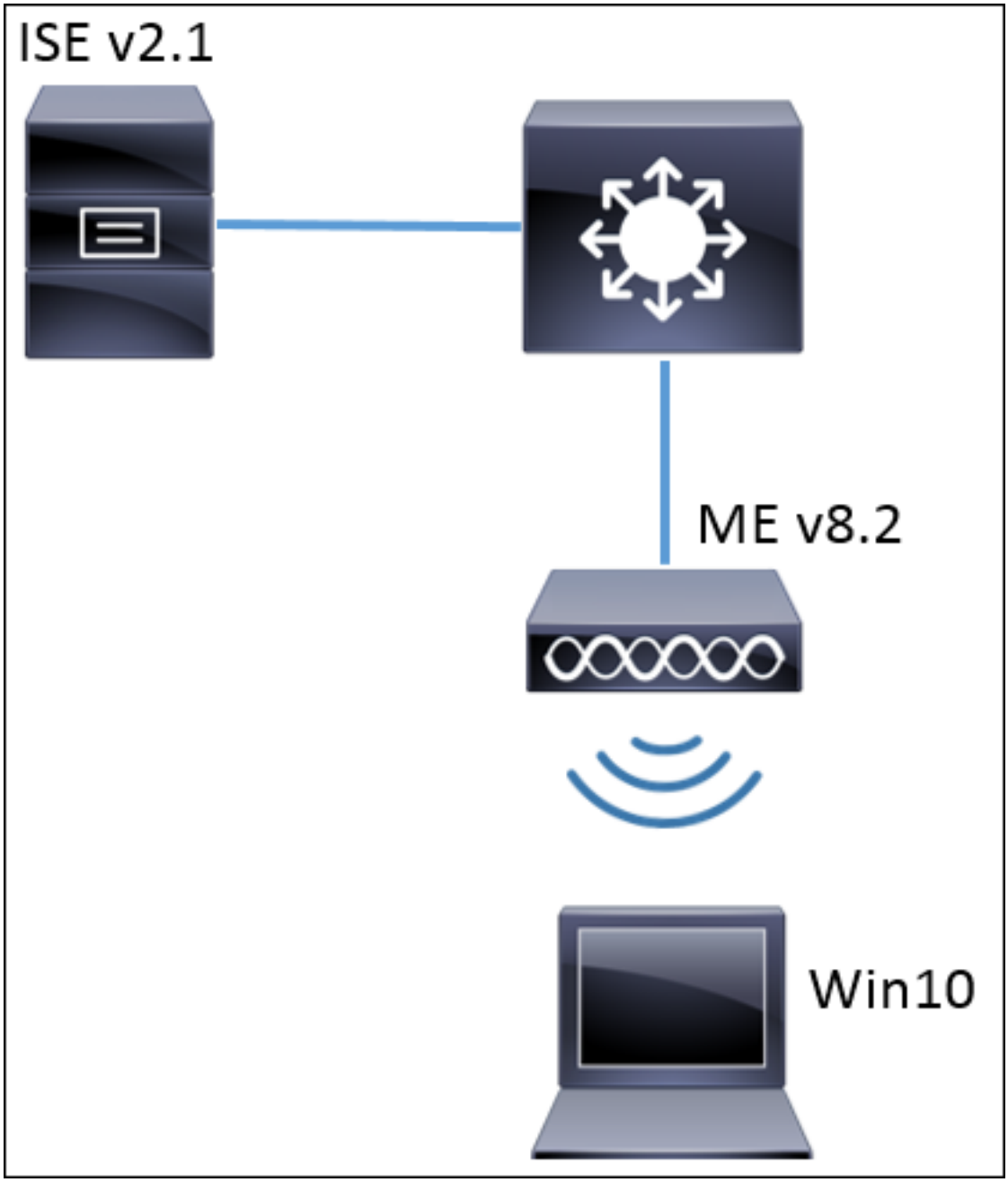
ISE v2.1

Windows 10-Laptop

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

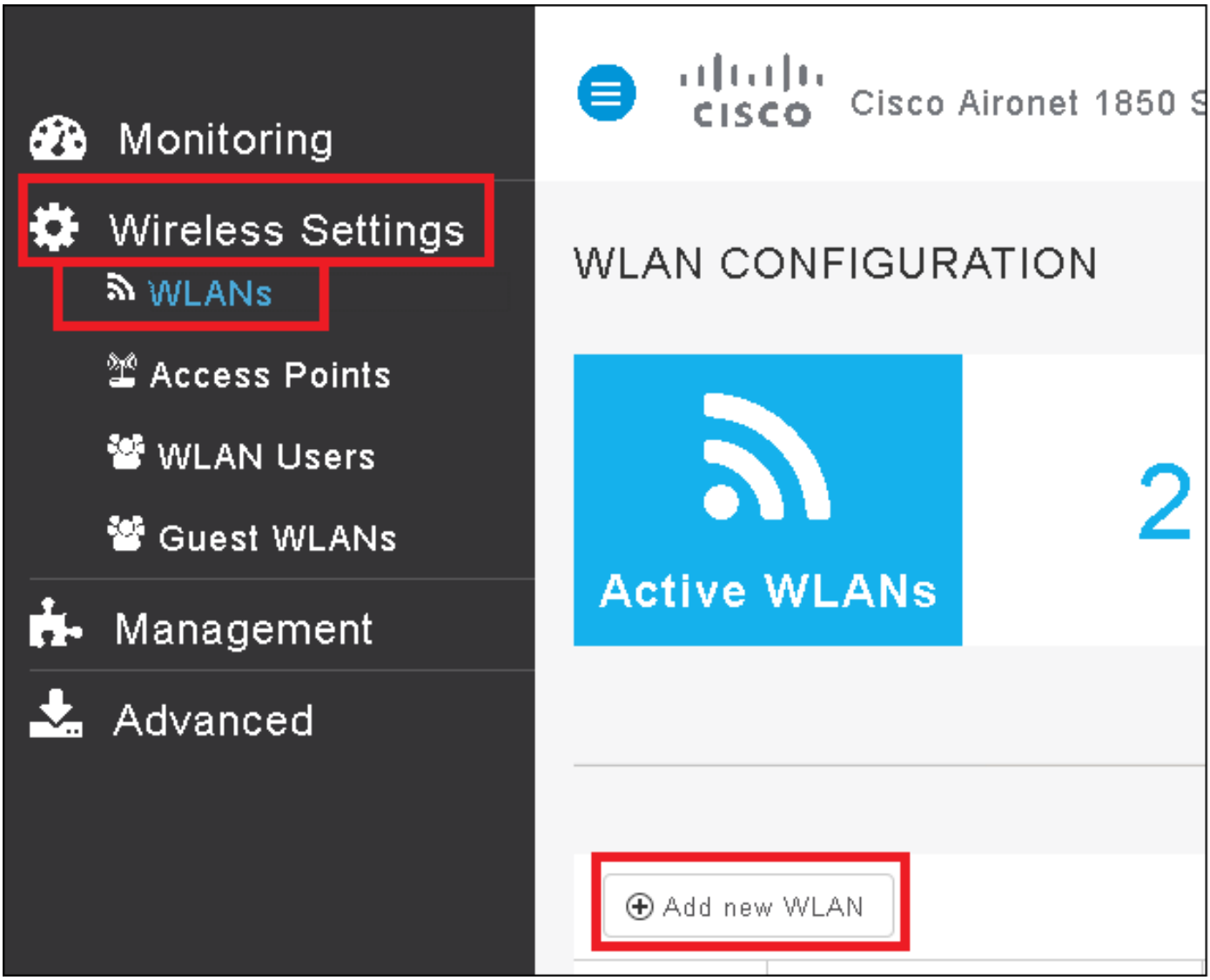
Die allgemeinen Schritte sind:

1. Erstellen Sie den Service Set Identifier (SSID) in ME, und deklarieren Sie den RADIUS-Server (in diesem Beispiel ISE) für ME.
2. Deklarieren von ME auf RADIUS-Server (ISE)
3. Erstellen Sie eine Authentifizierungsregel für die ISE.
4. Erstellen einer Autorisierungsregel für die ISE
5. Konfigurieren des Endpunkts

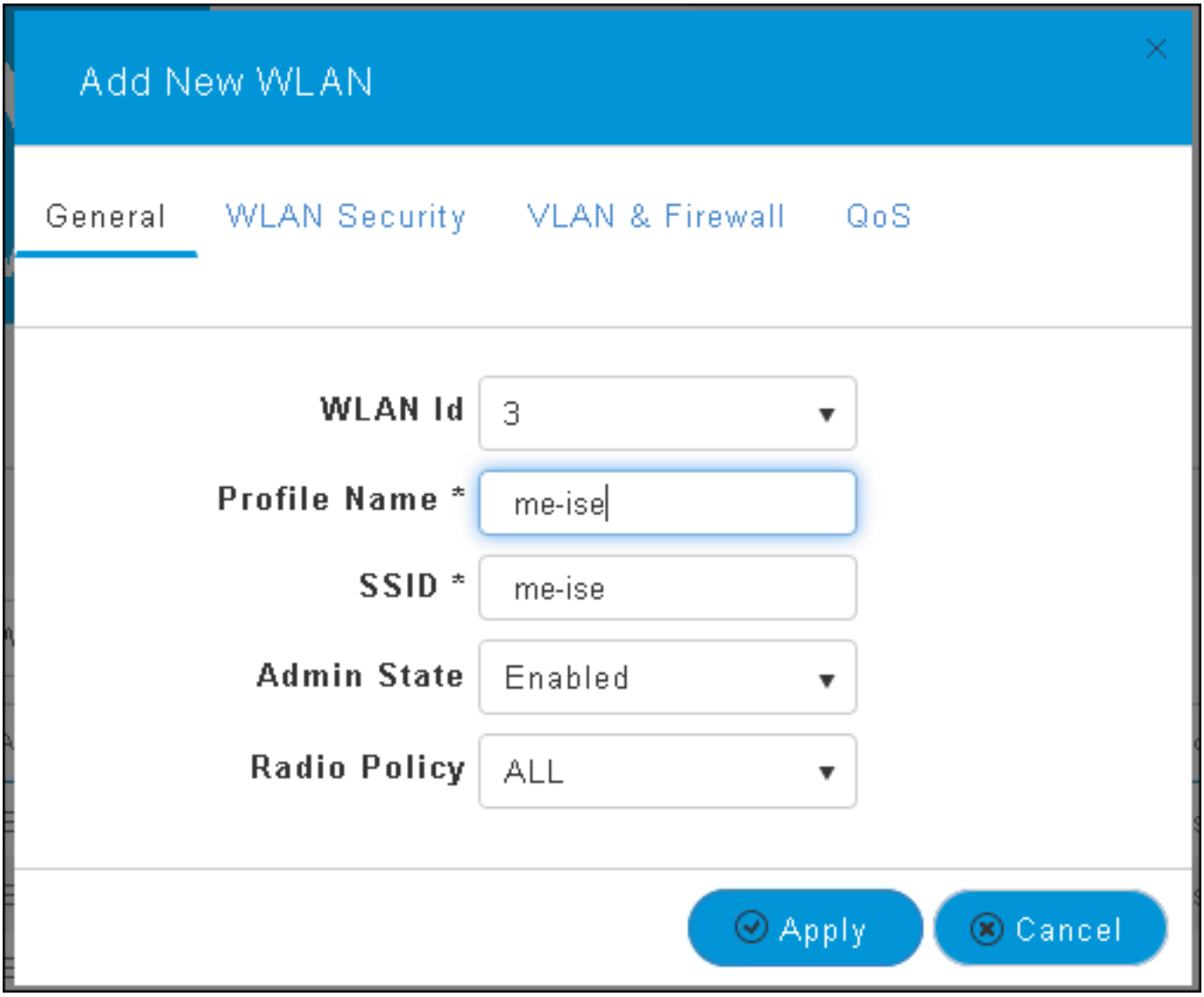
Konfiguration auf ME

Um die Kommunikation zwischen RADIUS-Server und ME zu ermöglichen, ist es erforderlich, RADIUS-Server auf ME und umgekehrt zu registrieren. In diesem Schritt wird veranschaulicht, wie der RADIUS-Server auf ME registriert wird.

Schritt 1: Öffnen Sie die Benutzeroberfläche von ME, und navigieren Sie zu **Wireless-Einstellungen > WLANs > Neues WLAN hinzufügen.**

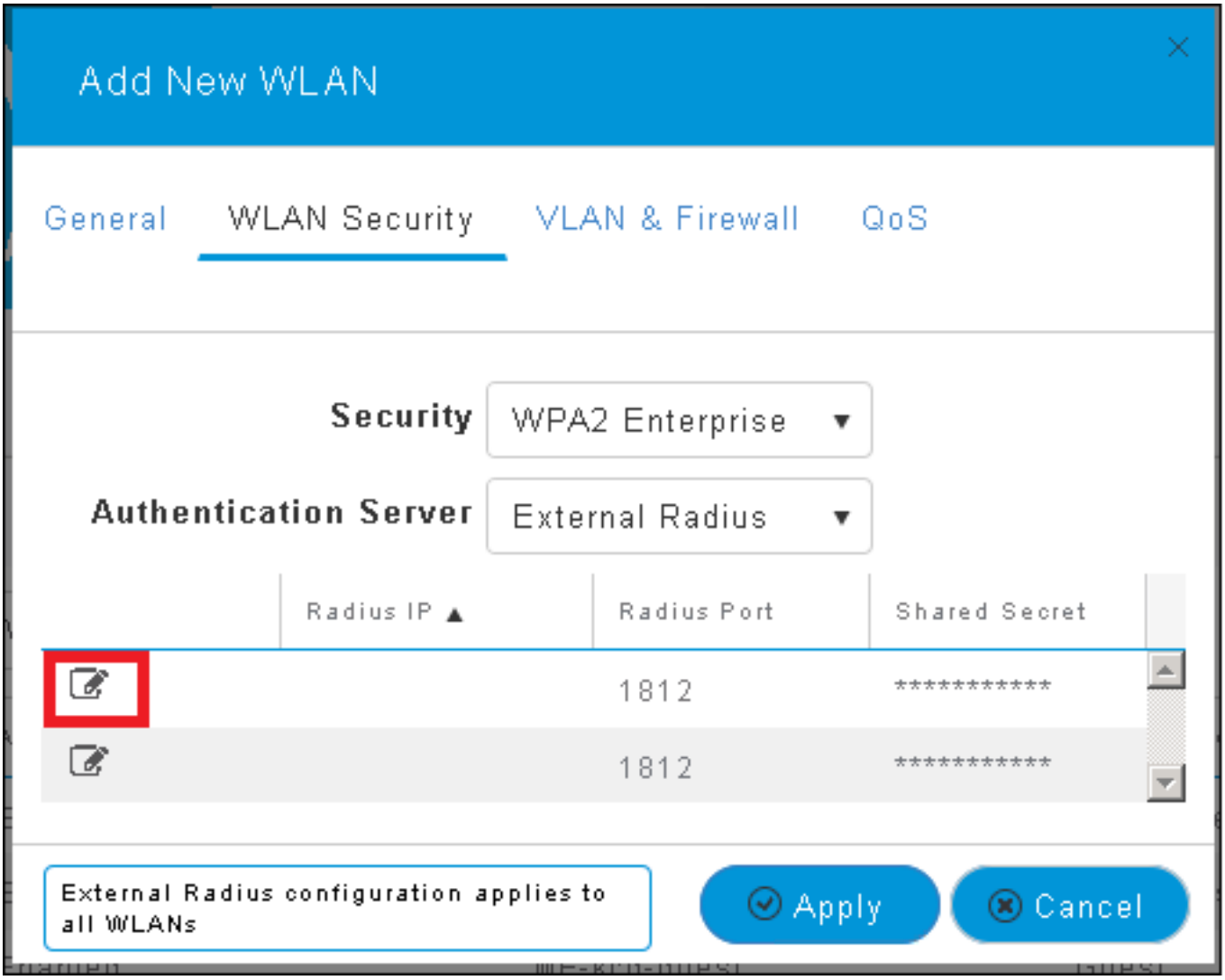


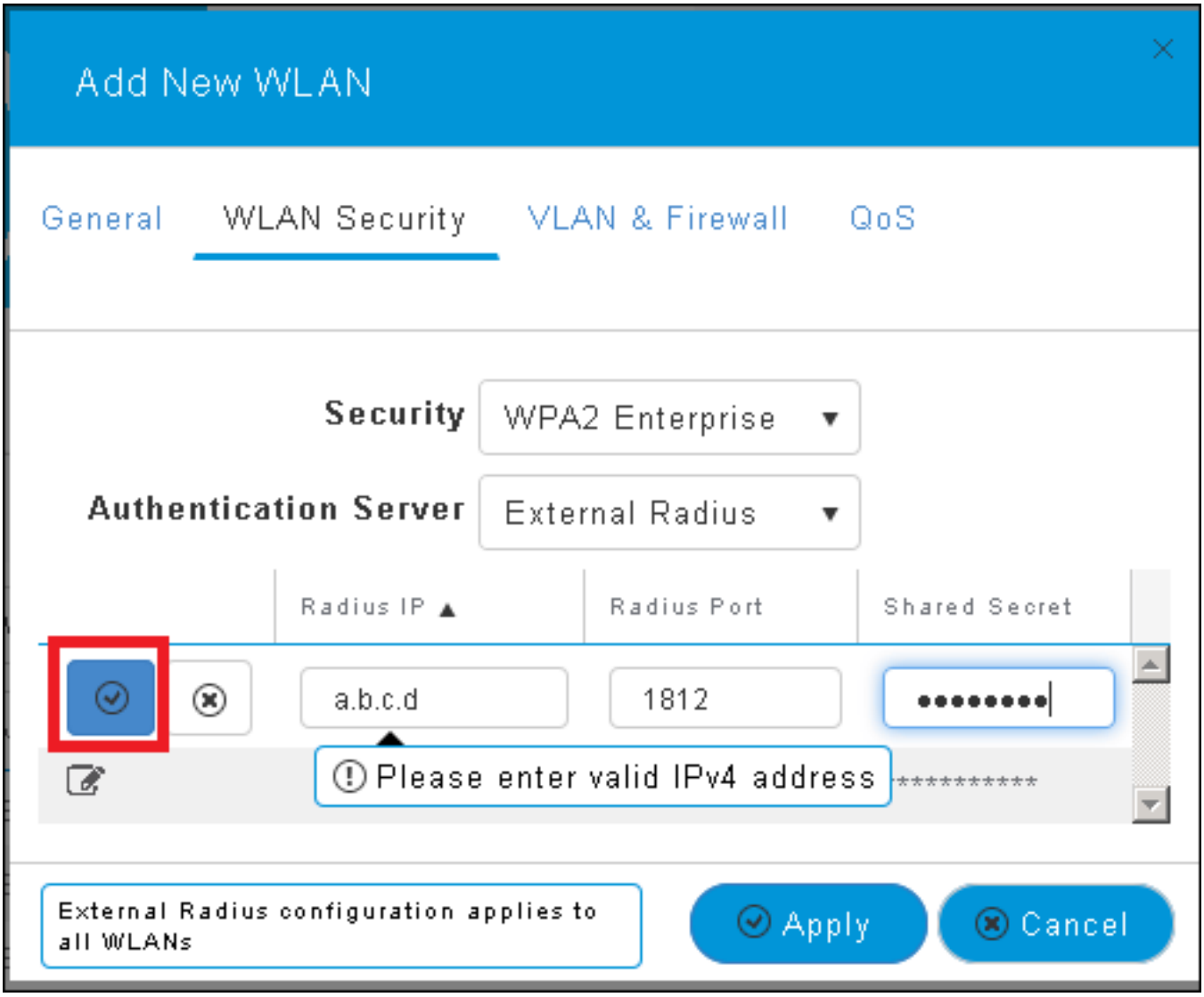
Schritt 2: Wählen Sie einen Namen für das WLAN aus.



Schritt 3: Geben Sie die Sicherheitskonfiguration auf der Registerkarte **WLAN-Sicherheit** an.

Wählen Sie **WPA2 Enterprise aus**, für den Authentifizierungsserver wählen Sie **External RADIUS aus**. Klicken Sie auf die Bearbeitungsoption, um die IP-Adresse des RADIUS hinzuzufügen, und wählen Sie einen Schlüssel **für den gemeinsamen geheimen** Schlüssel aus.


Add New WLAN
General
WLAN Security
VLAN & Firewall
QoS
Security
WPA2 Enterprise
Authentication Server
External Radius
Radius IP
Radius Port
Shared Secret
1812
****
1812
****
External Radius configuration applies to all WLANs
Apply
Cancel

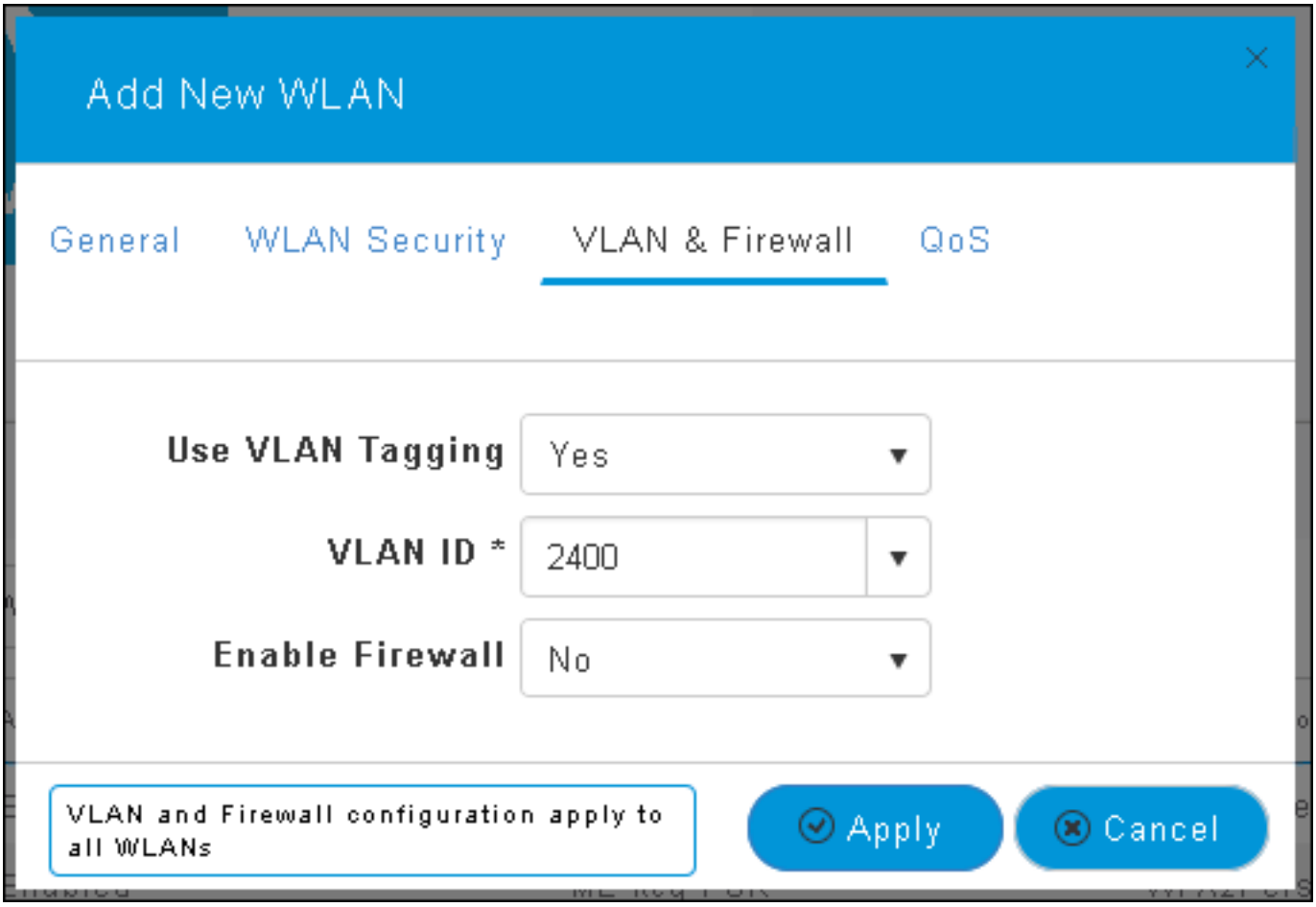


<a.b.c.d> entspricht dem RADIUS-Server.

Schritt 4: Weisen Sie der SSID ein VLAN zu.

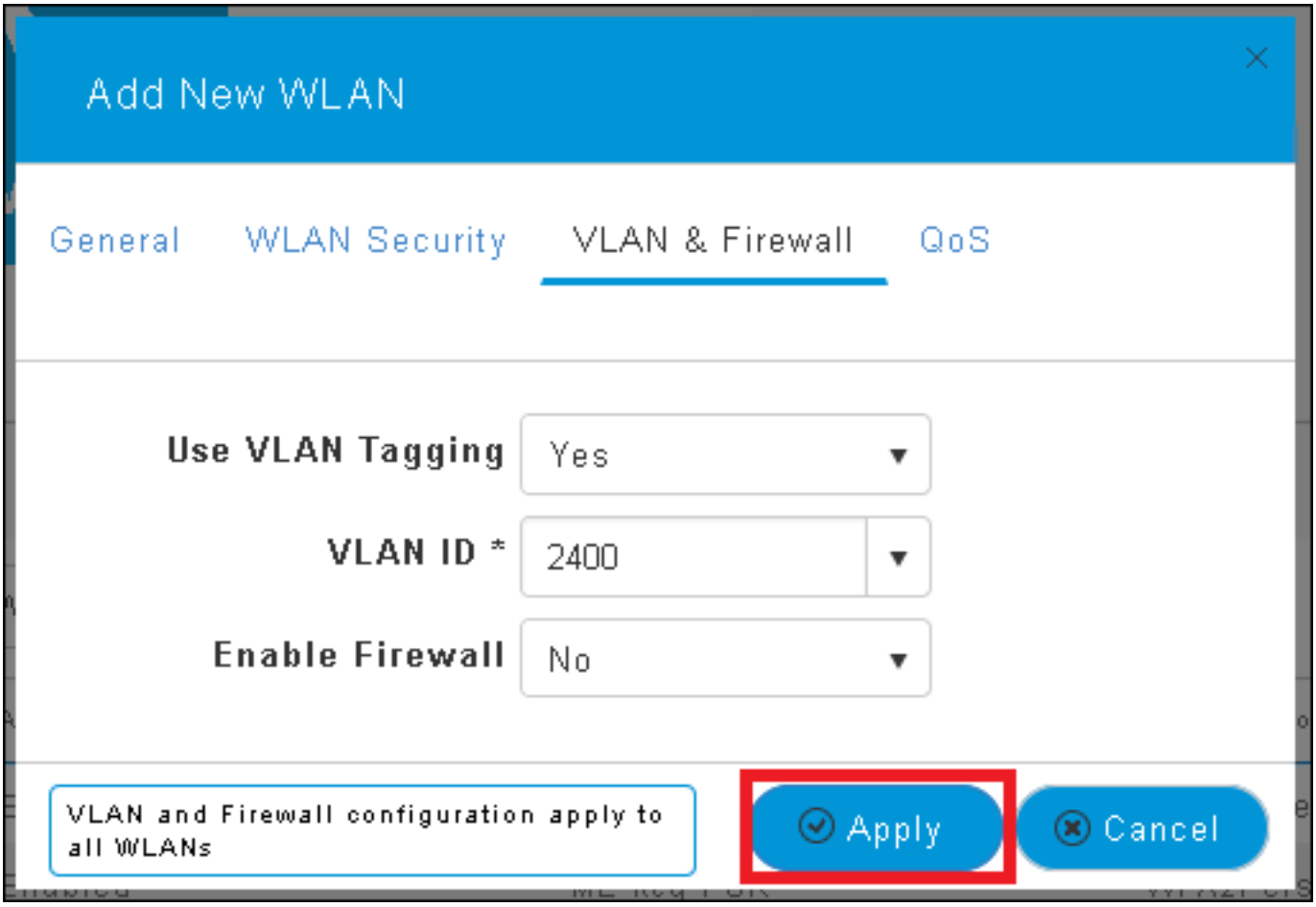
Wenn die SSID dem VLAN des AP zugewiesen werden muss, kann dieser Schritt übersprungen werden.

Um die Benutzer für diese SSID einem bestimmten VLAN (außer dem VLAN des AP) zuzuweisen, aktivieren Sie **VLAN Tagging verwenden** und weisen Sie die gewünschte **VLAN-ID zu**.



Hinweis: Wenn VLAN Tagging verwendet wird, stellen Sie sicher, dass der Switch-Port, mit dem der Access Point verbunden ist, als Trunk-Port konfiguriert und das AP-VLAN als nativ konfiguriert ist.

Schritt 5: Klicken Sie auf **Apply**, um die Konfiguration abzuschließen.



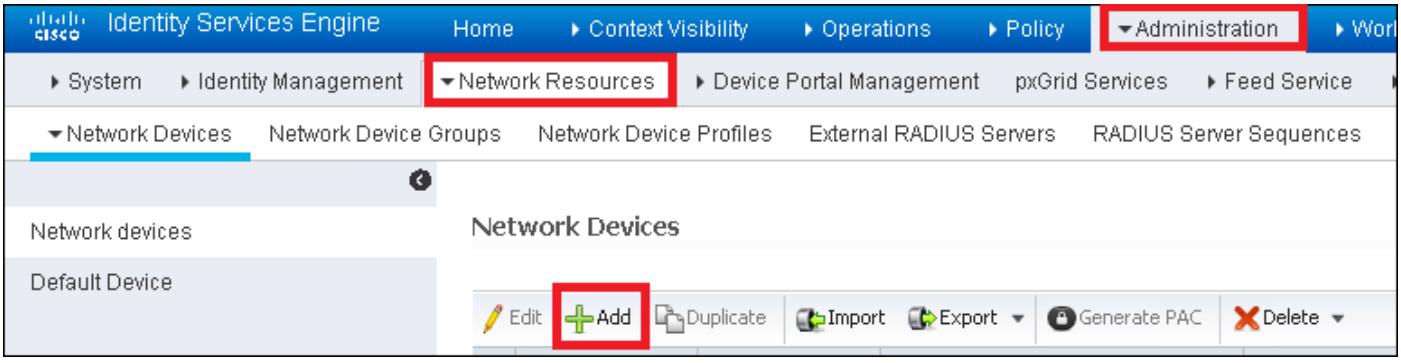
Schritt 6: Konfigurieren Sie optional das WLAN so, dass das VLAN-Override akzeptiert wird.

Aktivieren Sie AAA override im WLAN, und fügen Sie die erforderlichen VLANs hinzu. Dazu müssen Sie eine CLI-Sitzung mit der ME-Verwaltungsschnittstelle öffnen und die folgenden Befehle ausführen:

```
>config wlan disable <wlan-id>
>config wlan aaa-override enable <wlan-id>
>config wlan enable <wlan-id>
>config flexconnect group default-flexgroup vlan add <vlan-id>
```

Deklarieren Sie mich auf ISE.

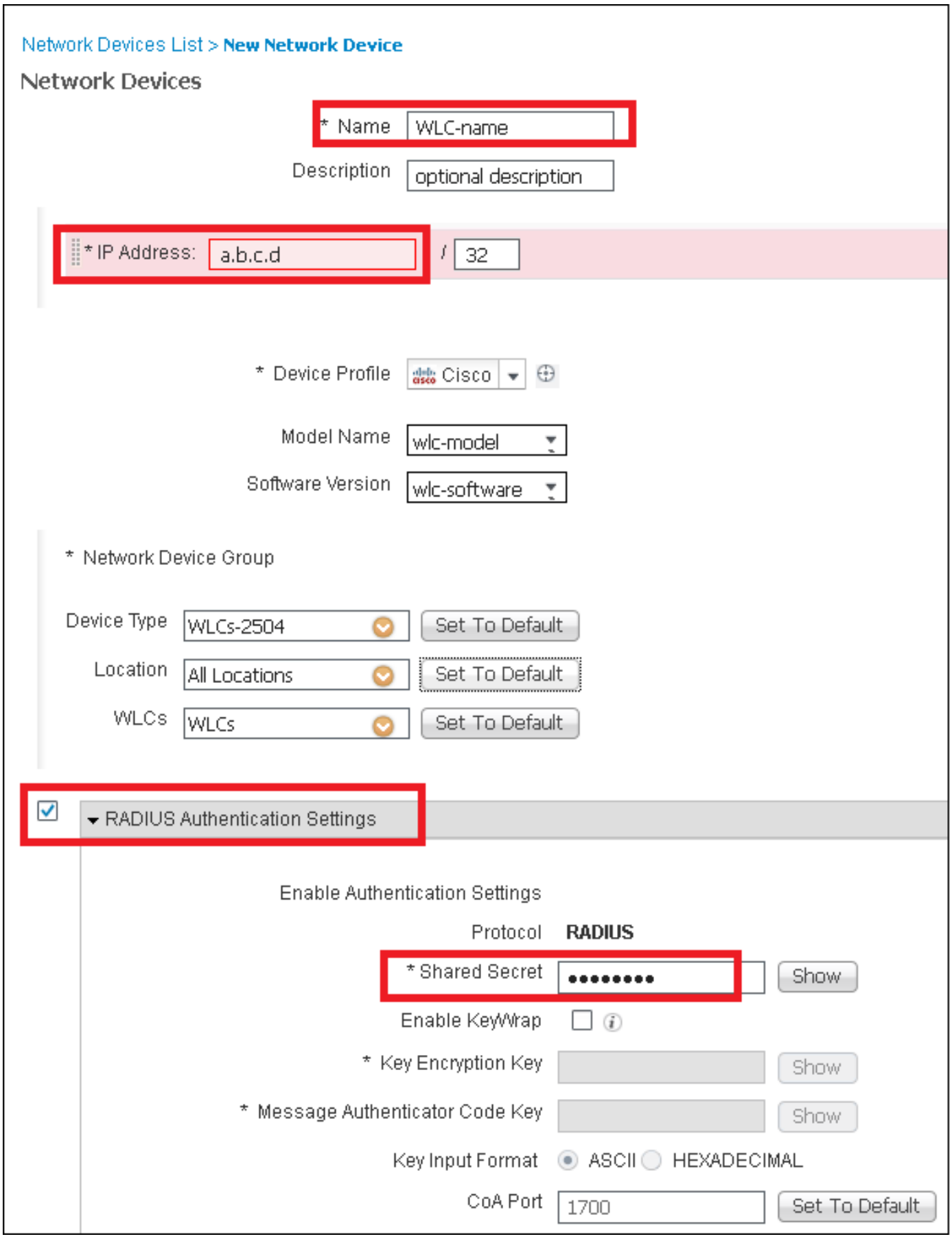
Schritt 1: Öffnen Sie die ISE-Konsole, und navigieren Sie zu **Administration > Network Resources > Network Devices > Add.**



Schritt 2: Geben Sie die Informationen ein.

Optional kann ein Modellname, eine Softwareversion, eine Beschreibung und die Zuweisung von Netzwerkgerätegruppen basierend auf Gerätetypen, Standorten oder WLCs angegeben werden.

a.b.c.d entspricht der IP-Adresse von ME.

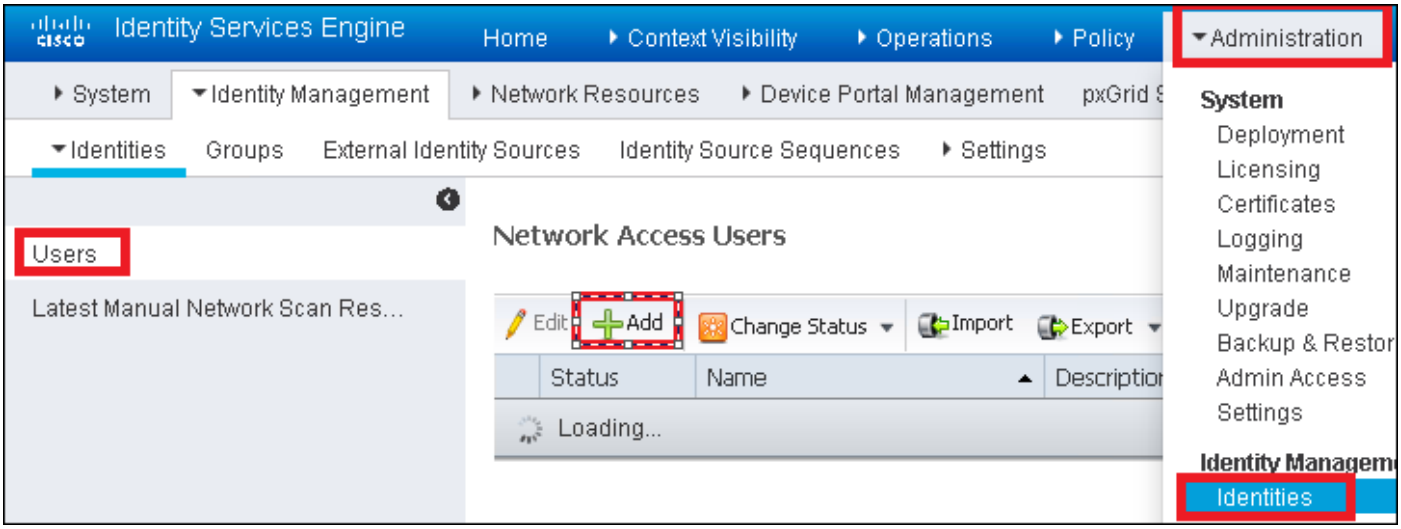


Weitere Informationen zu Netzwerkgerätegruppen finden Sie unter:

[ISE = Network Device Groups (Netzwerkgerätegruppen)]

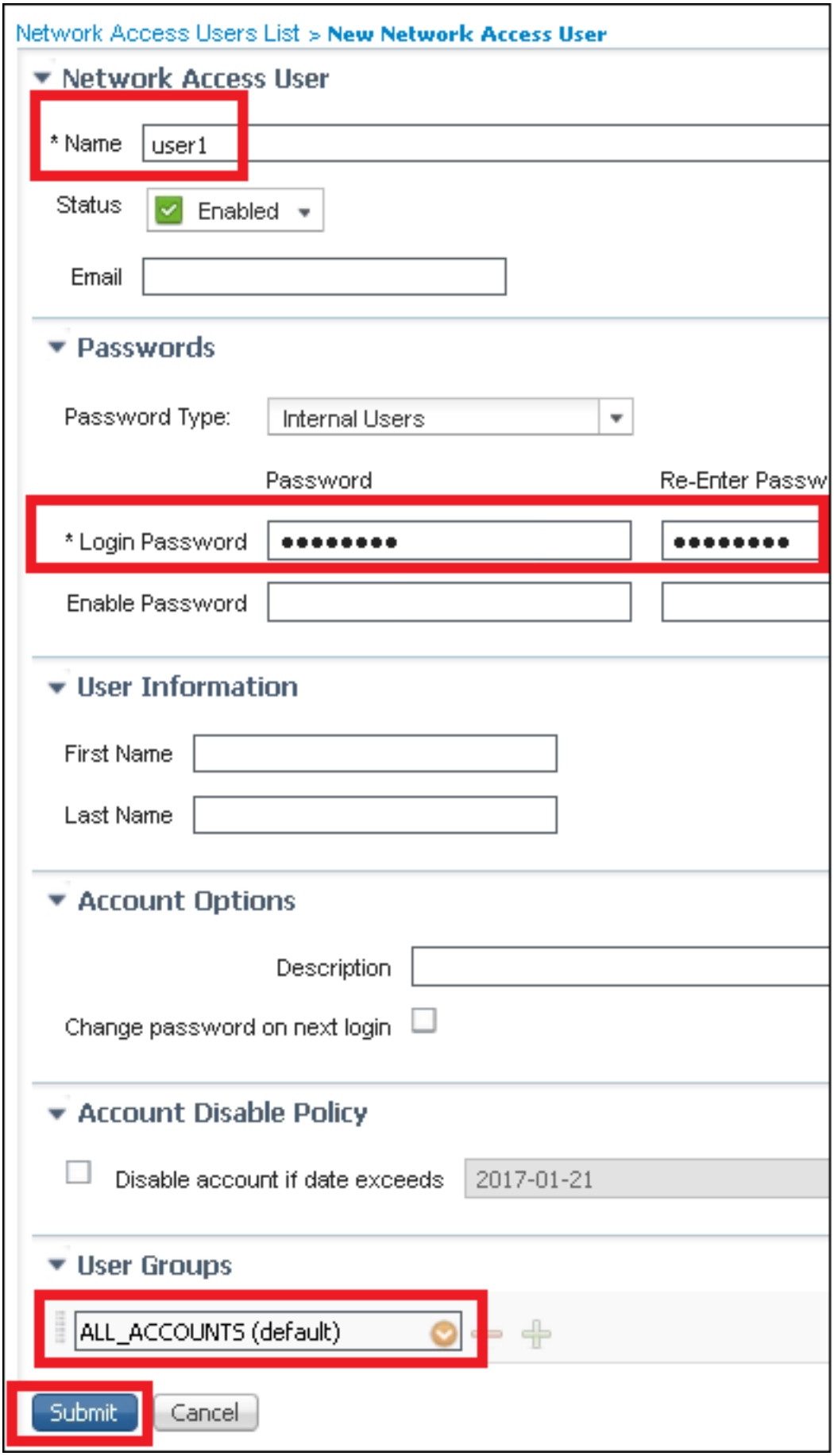
Neuen Benutzer auf der ISE erstellen

Schritt 1: Navigieren zu **Administration > Identity Management > Identities > Users > Add.**



Schritt 2: Geben Sie die Informationen ein.

In diesem Beispiel gehört dieser Benutzer zu einer Gruppe namens ALL_ACCOUNTS, kann jedoch nach Bedarf angepasst werden.

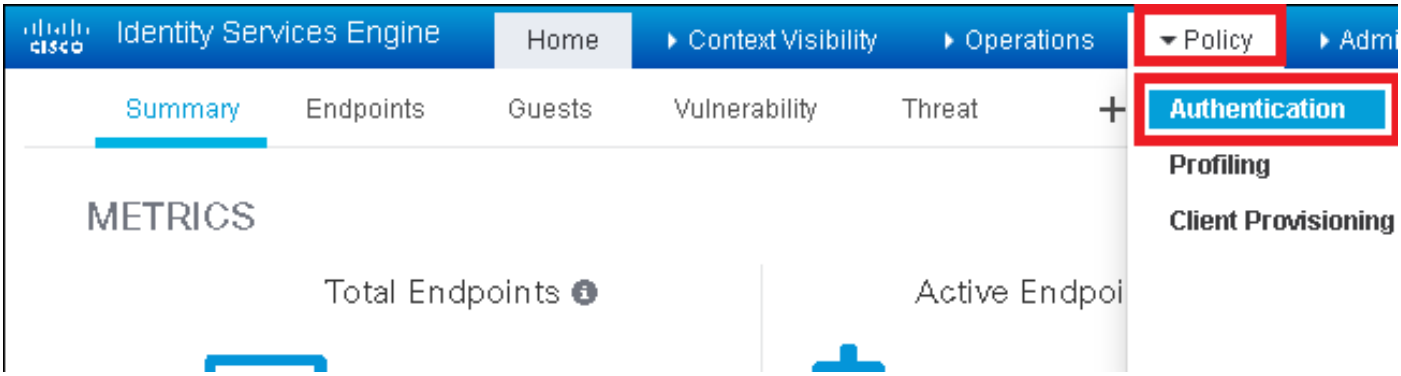


Erstellen der Authentifizierungsregel

Authentifizierungsregeln werden verwendet, um zu überprüfen, ob die Anmeldeinformationen der Benutzer richtig sind (Überprüfen Sie, ob der Benutzer wirklich der ist, den er vorgibt) und die

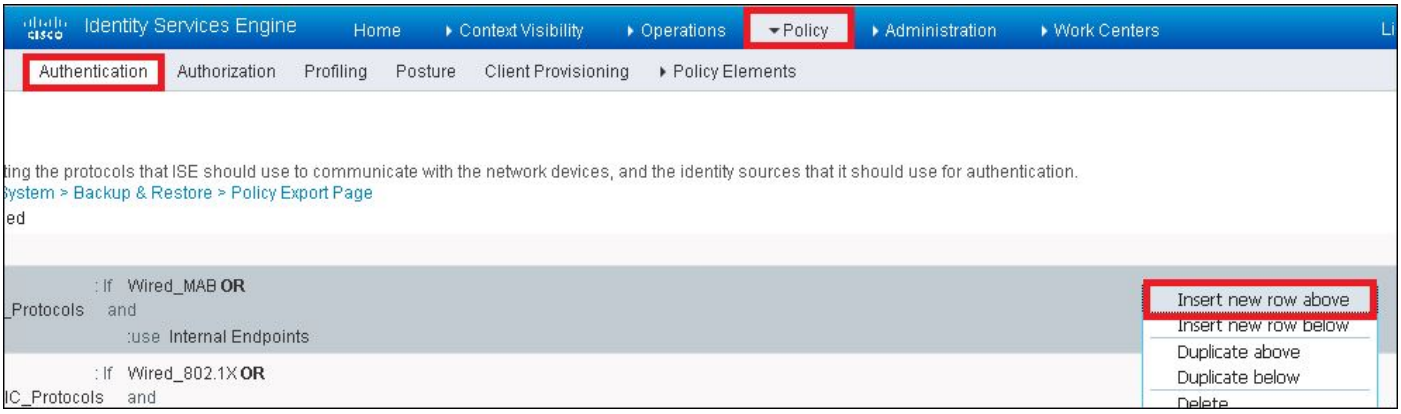
Authentifizierungsmethoden zu beschränken, die von ihm verwendet werden dürfen.

Schritt 1: Navigieren auf **Policy > Authentication (Richtlinien > Authentifizierung)**.



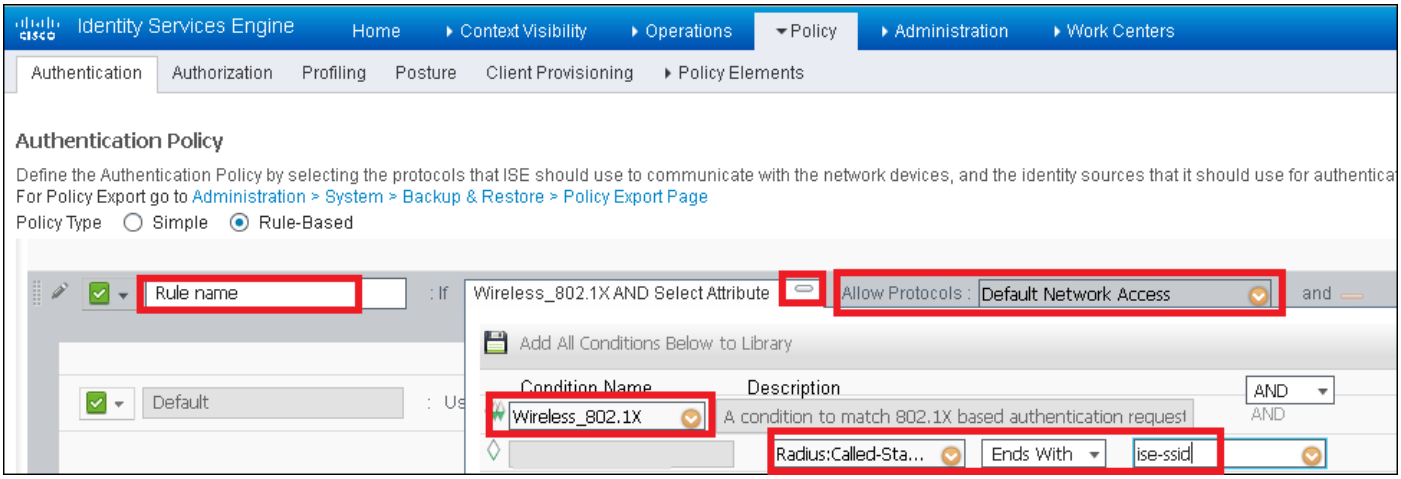
Schritt 2: Fügen Sie eine neue Authentifizierungsregel ein.

Navigieren Sie dazu zu **Richtlinien > Authentifizierung > Neue Zeile oben/unten einfügen.**

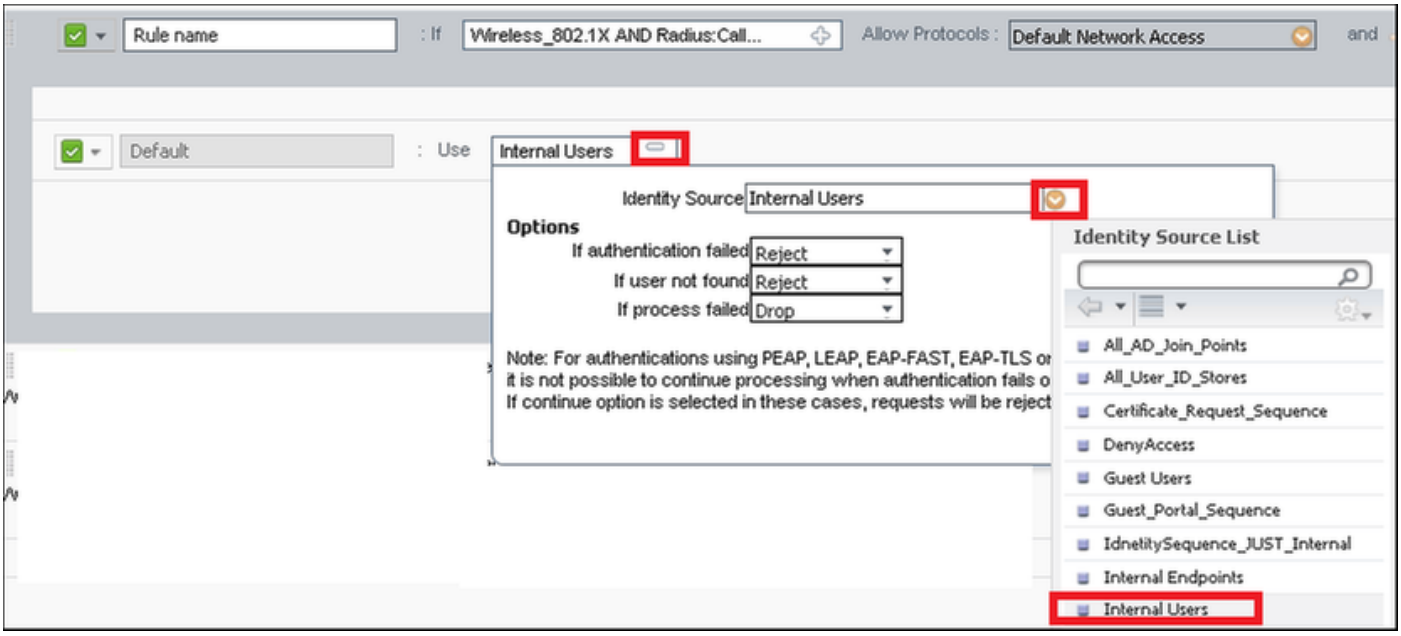


Schritt 3: Geben Sie die erforderlichen Informationen ein.

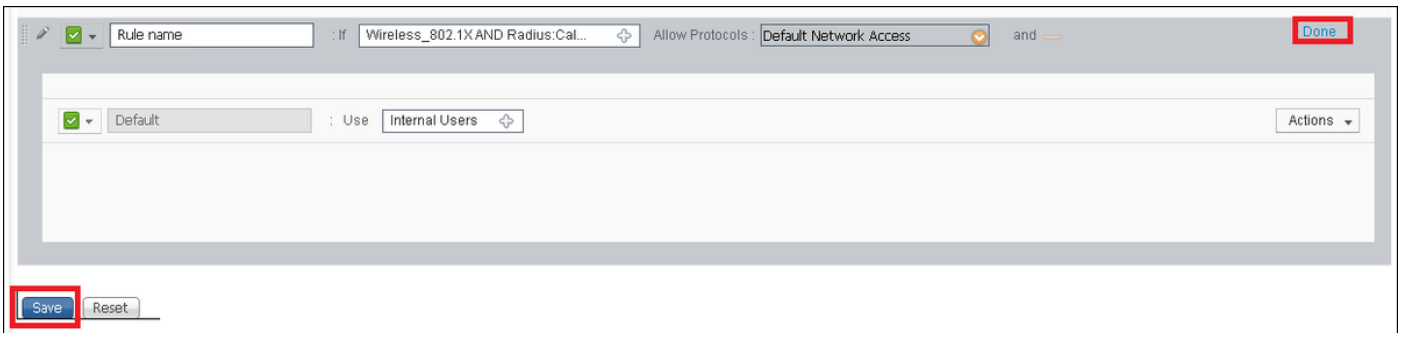
Dieses Beispiel für eine Authentifizierungsregel ermöglicht alle Protokolle, die in der Liste für den **Standard-Netzwerkzugriff** aufgeführt sind. Dies gilt für die Authentifizierungsanforderung für Wireless 802.1x-Clients und mit der Called Station-ID und endet mit *ise-ssid*.



Wählen Sie außerdem die Identitätsquelle für die Clients aus, die dieser Authentifizierungsregel entsprechen. In diesem Beispiel wird sie für *interne Benutzer* verwendet.



Wenn der Vorgang abgeschlossen ist, klicken Sie auf **Fertig** und **Speichern**



Weitere Informationen zu Regeln für das Zulassen von Protokollen finden Sie unter:

[Zugelassener Protokolldienst]

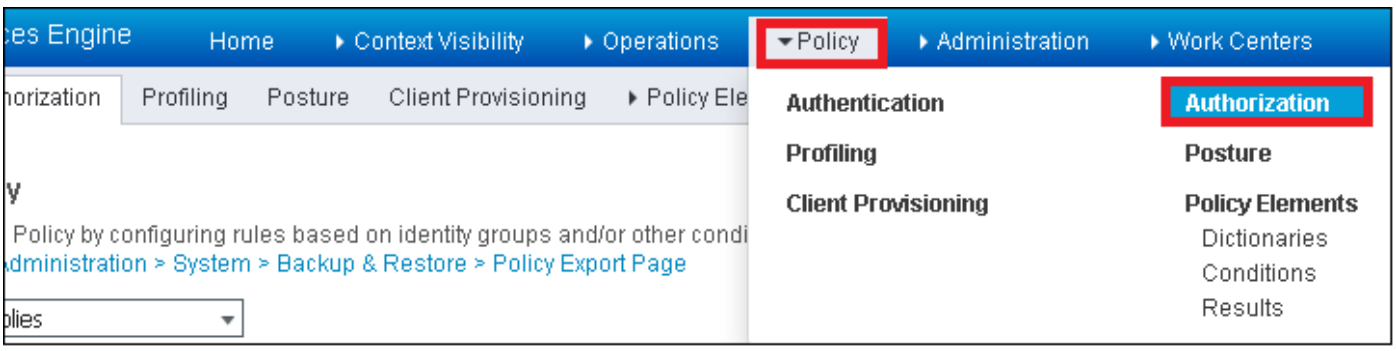
Weitere Informationen zu Identitätsquellen finden Sie unter:

[Erstellen einer Benutzeridentitätsgruppe]

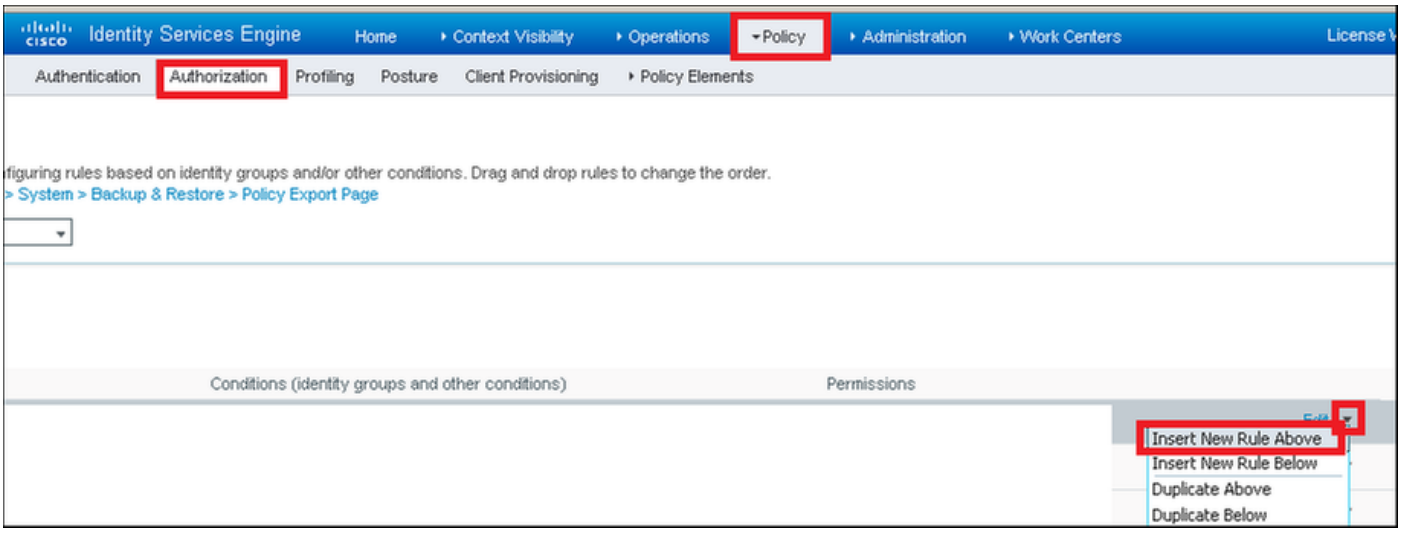
Erstellen der Autorisierungsregel

Die Autorisierungsregel ist die, die bestimmt, ob der Client dem Netzwerk beitreten darf oder nicht.

Schritt 1: Navigieren Sie zu **Richtlinien > Autorisierung.**

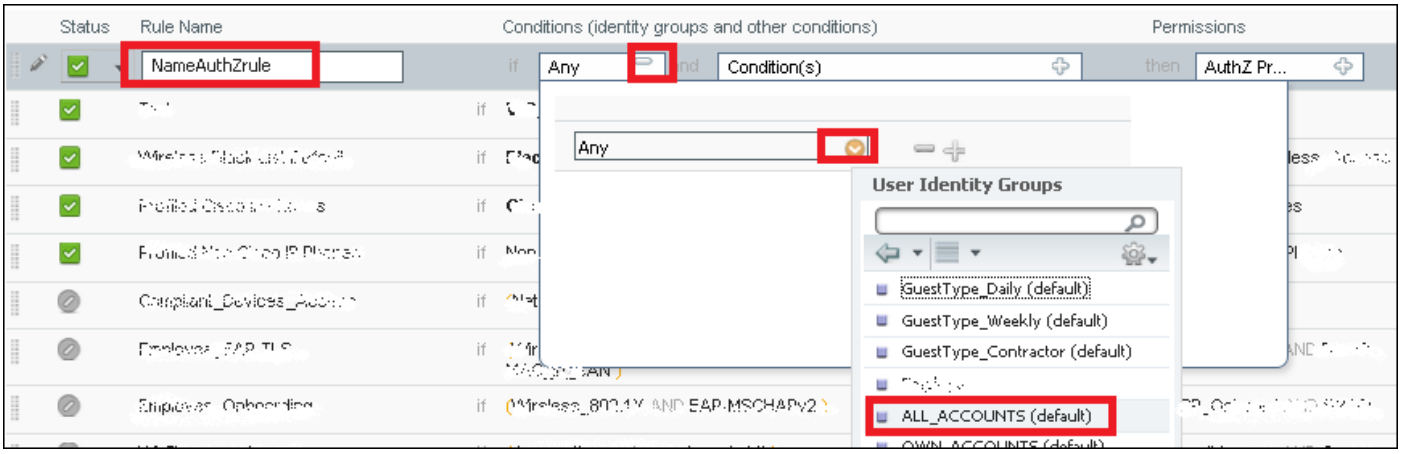


Schritt 2: Fügen Sie eine neue Regel ein. Navigieren Sie zu **Richtlinien > Autorisierung > Neue Regel oben/unten einfügen.**

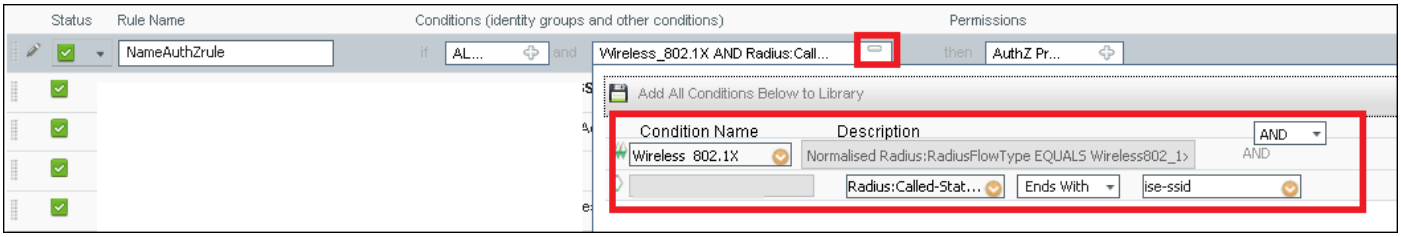


Schritt 3: Geben Sie die Informationen ein.

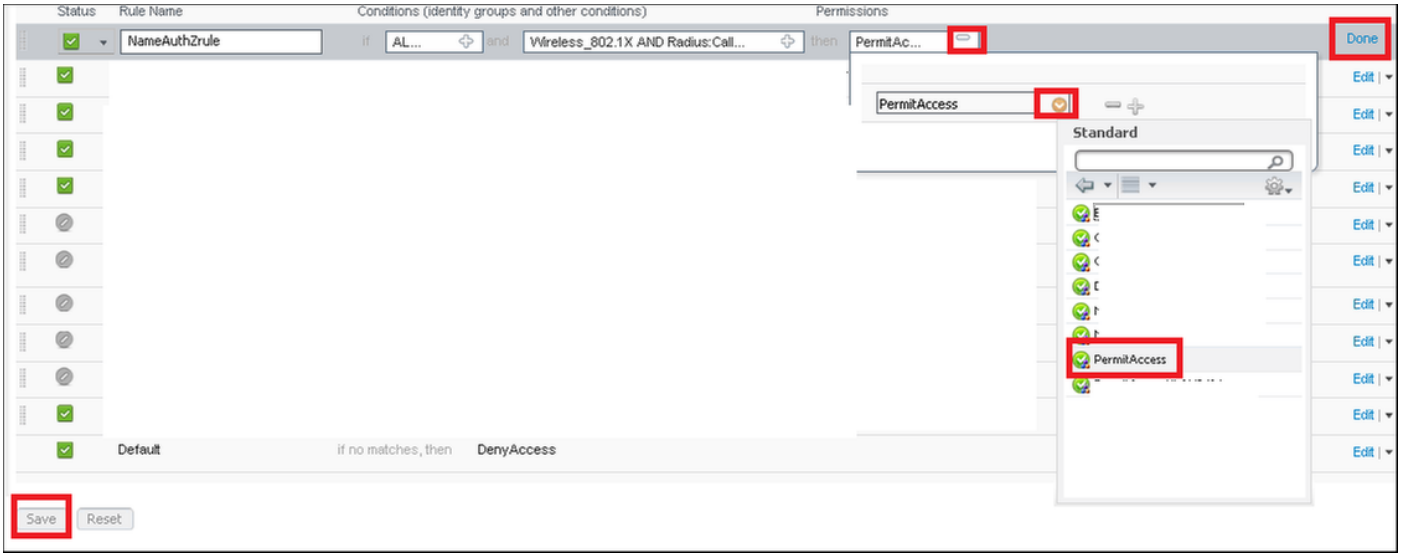
Wählen Sie zuerst einen Namen für die Regel und die Identitätsgruppen aus, in denen der Benutzer gespeichert ist. In diesem Beispiel wird der Benutzer in der Gruppe *ALL_ACCOUNTS* gespeichert.



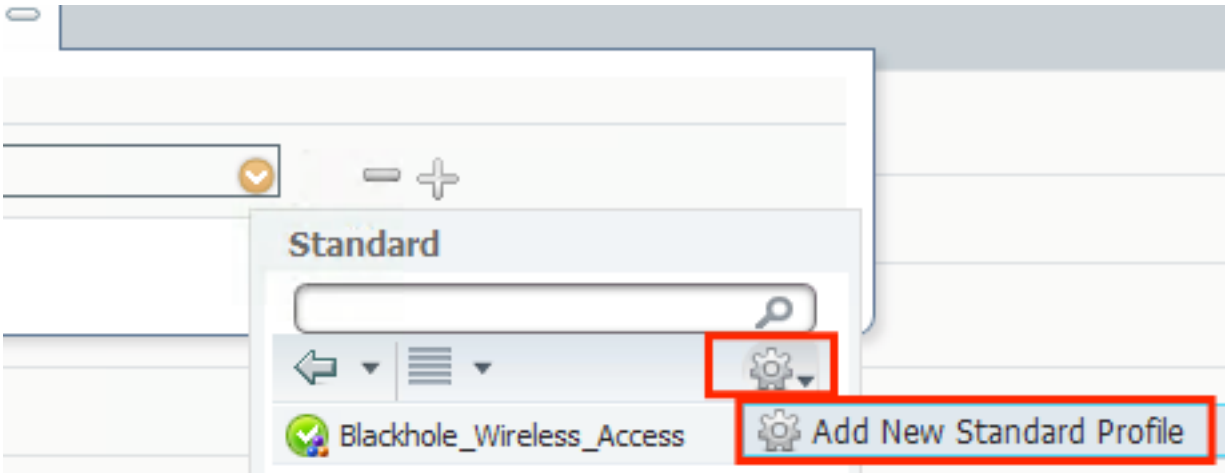
Wählen Sie anschließend andere Bedingungen, die den Autorisierungsprozess in diese Regel einbeziehen. In diesem Beispiel trifft der Autorisierungsprozess auf diese Regel, wenn 802.1x Wireless verwendet wird und die Station-ID mit *ise-ssid* endet.



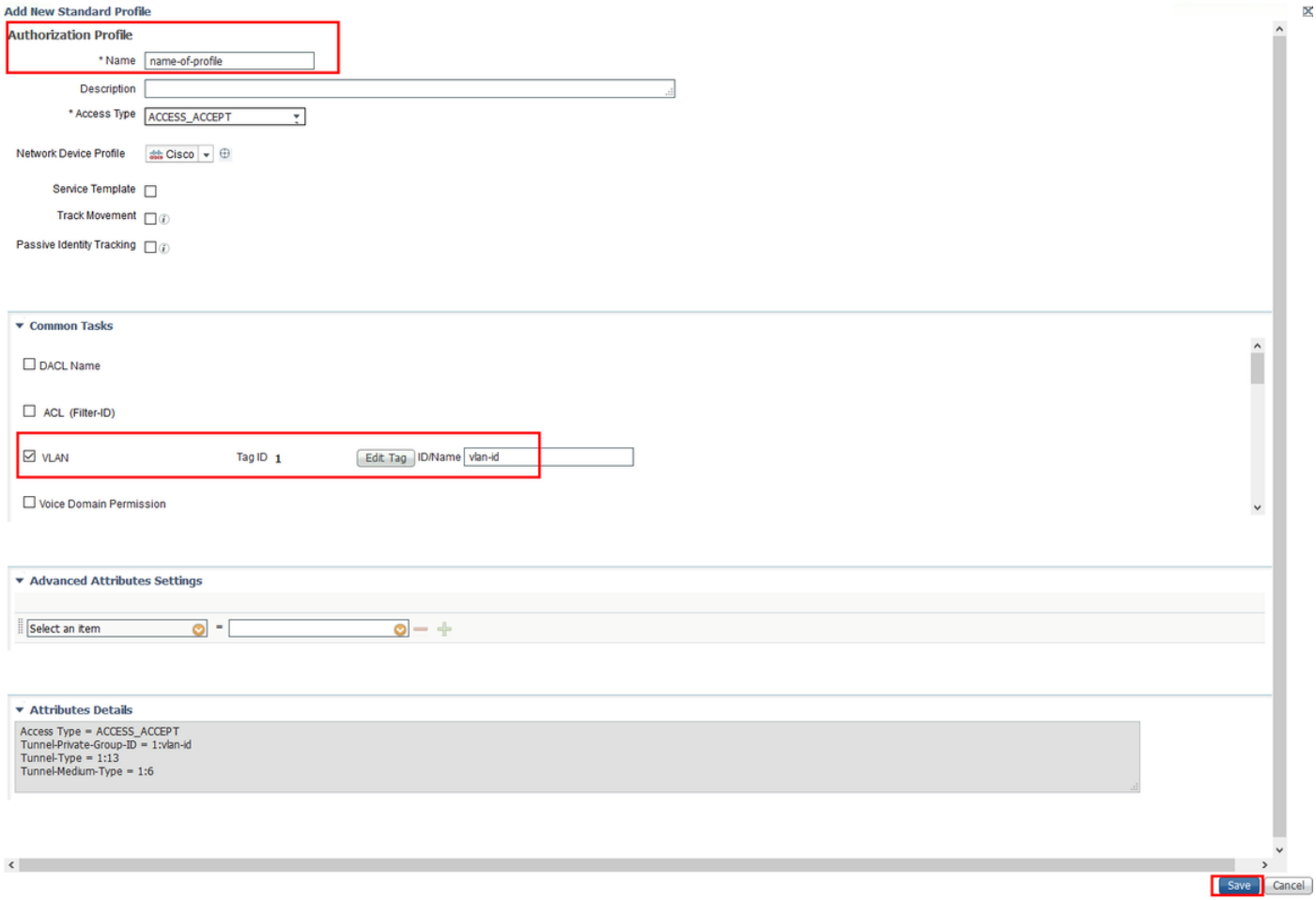
Wählen Sie schließlich das Autorisierungsprofil aus, mit dem die Clients dem Netzwerk beitreten können, klicken Sie auf **Fertig** und **Speichern.**



Sie können optional ein neues Autorisierungsprofil erstellen, das den Wireless-Client einem anderen VLAN zuweist:



Geben Sie die Informationen ein:



Konfiguration des Endgeräts

Konfigurieren eines Windows 10-Laptops für die Verbindung mit einer SSID mit 802.1x-Authentifizierung mithilfe von PEAP/MS-CHAPv2 (Microsoft-Version des Challenge-Handshake Authentication Protocol Version 2)

In diesem Konfigurationsbeispiel verwendet die ISE das selbstsignierte Zertifikat, um die Authentifizierung durchzuführen.

Zum Erstellen des WLAN-Profils auf dem Windows-Computer gibt es zwei Optionen:

1. Installieren Sie das selbstsignierte Zertifikat auf dem Computer, um den ISE-Server zu validieren und zu vertrauen, um die Authentifizierung abzuschließen.
2. Umgehen Sie die Validierung des RADIUS-Servers, und vertrauen Sie jedem RADIUS-Server, der für die Authentifizierung verwendet wird (wird nicht empfohlen, da dies zu einem Sicherheitsproblem werden kann).

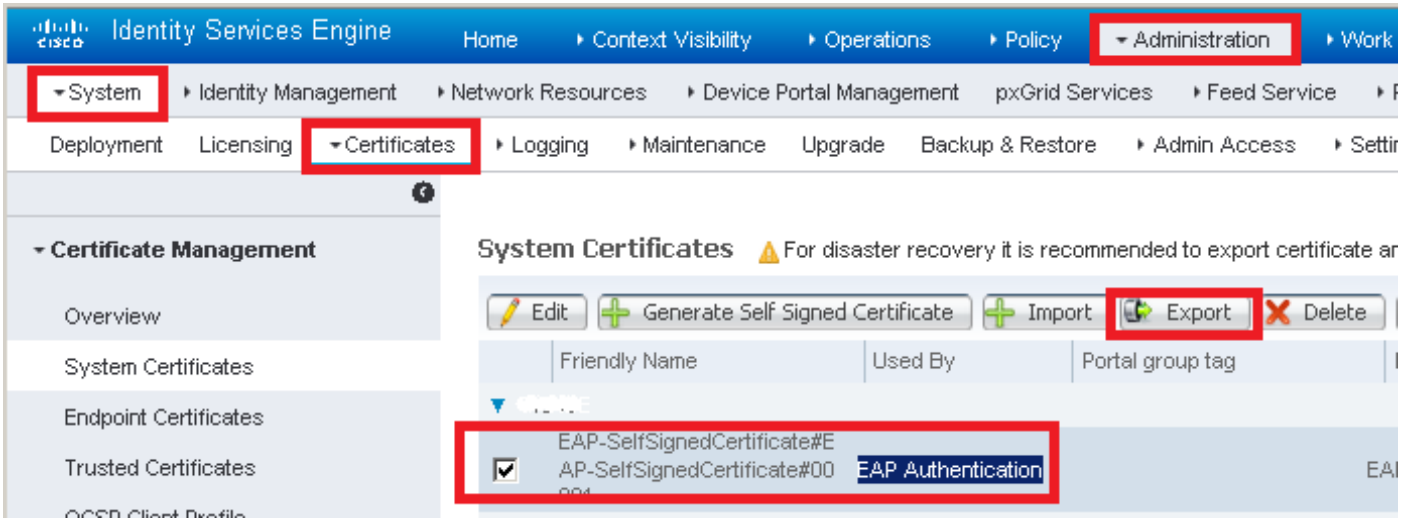
Die Konfiguration für diese Optionen wird unter Endgerätekonfiguration - WLAN-Profil erstellen - Schritt 7 erläutert.

Endgerätekonfiguration - Installation eines selbstsignierten ISE-Zertifikats

Schritt 1: Eigensigniertes Zertifikat von der ISE exportieren.

Melden Sie sich bei der ISE an, und navigieren Sie zu **Administration > System > Certificates > System Certificates**.

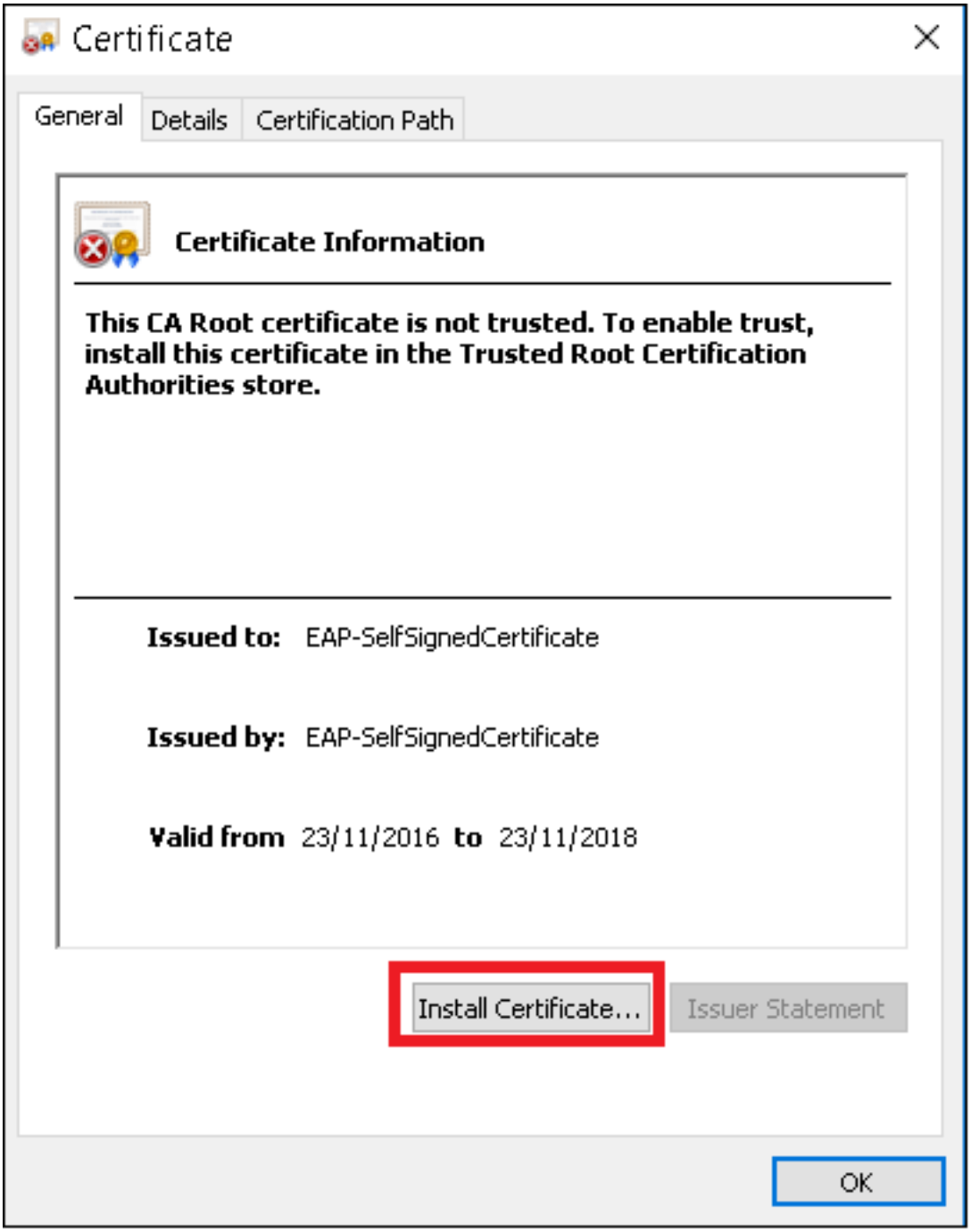
Wählen Sie dann das für die **EAP-Authentifizierung** verwendete Zertifikat aus und klicken Sie auf **Exportieren.**



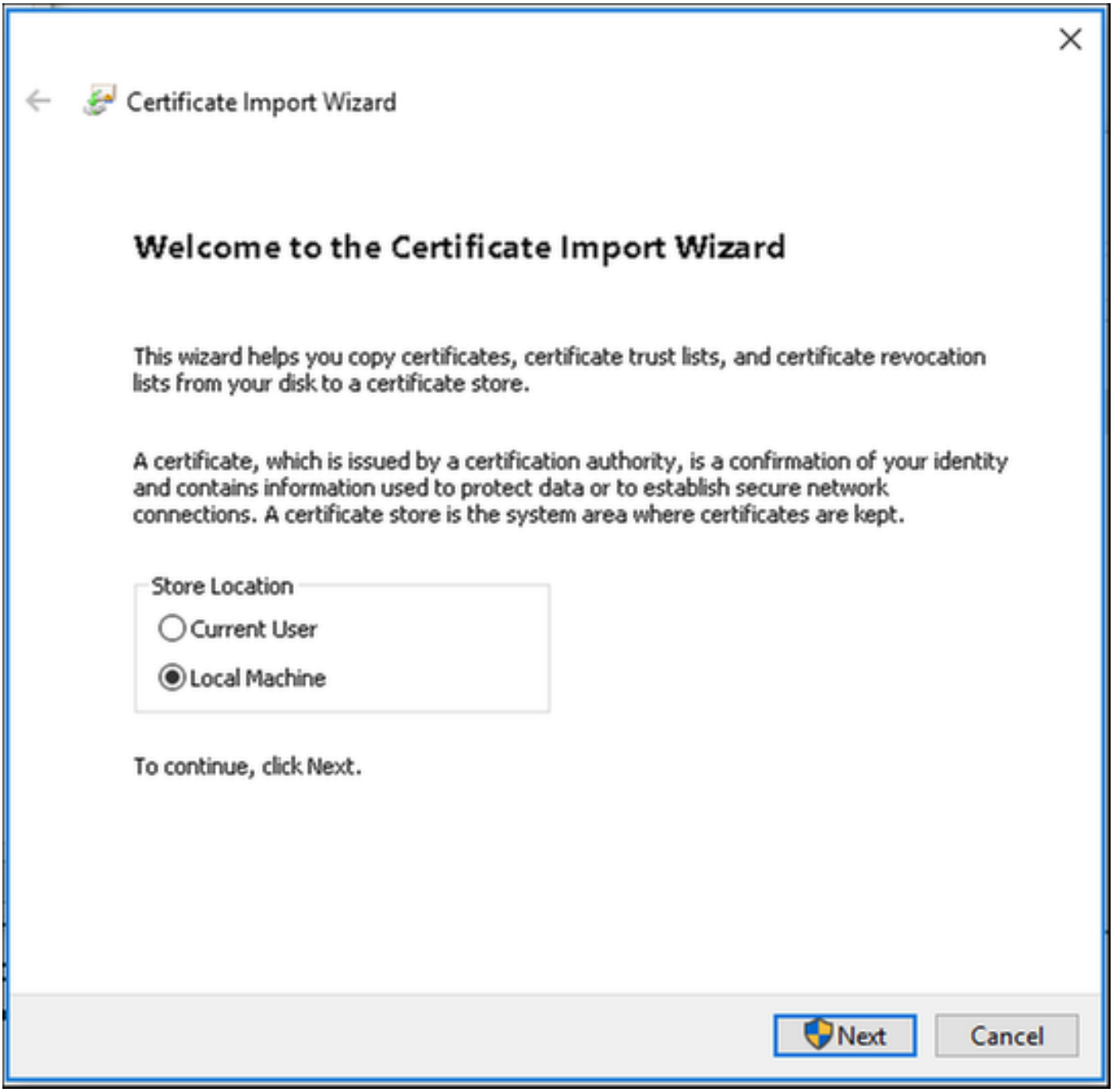
Speichern Sie das Zertifikat am gewünschten Ort. Dieses Zertifikat wird auf dem Windows-Computer installiert.

Schritt 2: Installieren Sie das Zertifikat auf dem Windows-Computer.

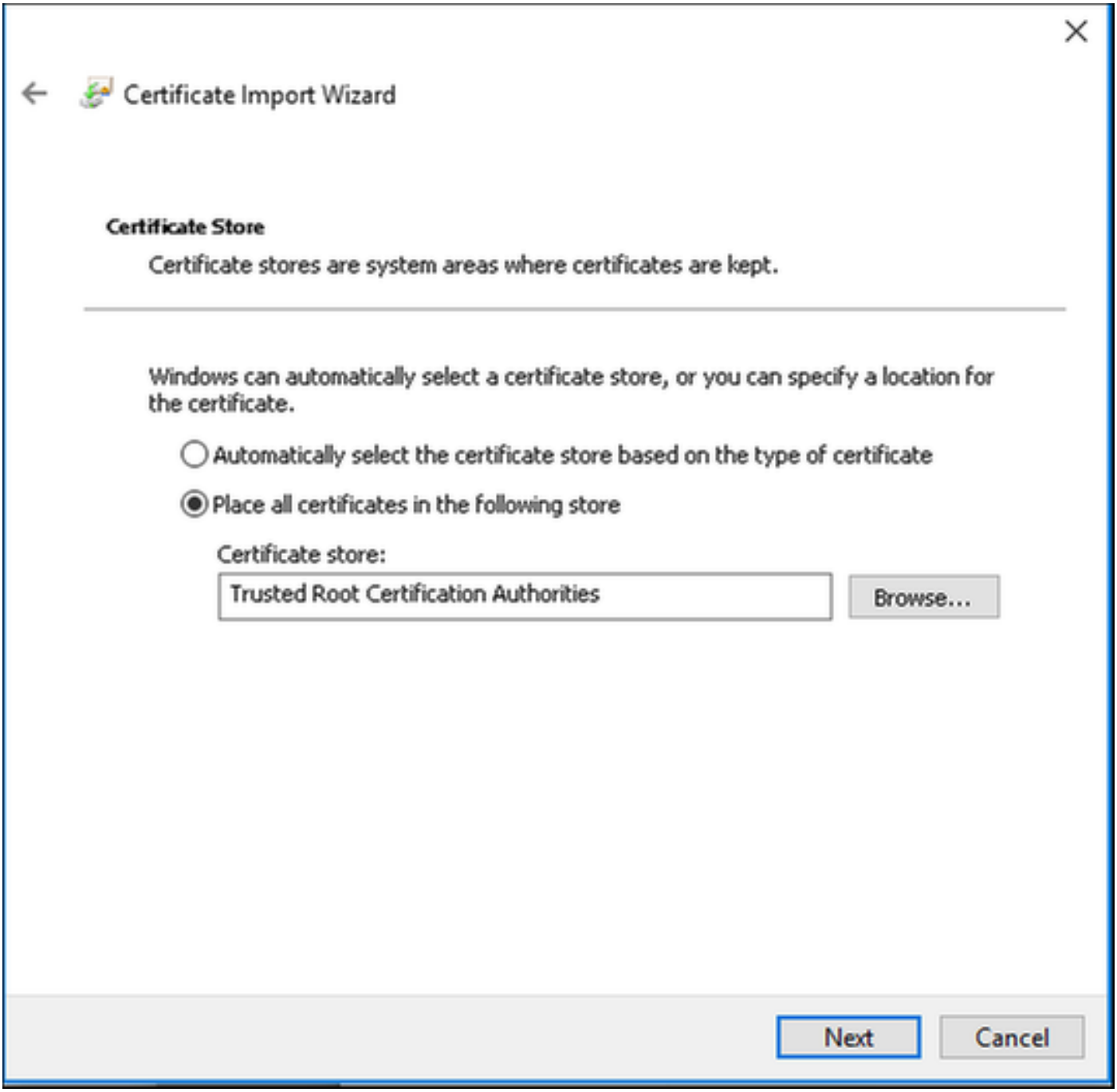
Kopieren Sie das zuvor exportierte Zertifikat auf den Windows-Computer, ändern Sie die Dateierweiterung von .pem auf .crt, nachdem Sie darauf doppelgeklickt haben, und wählen Sie **Zertifikat installieren aus...**.



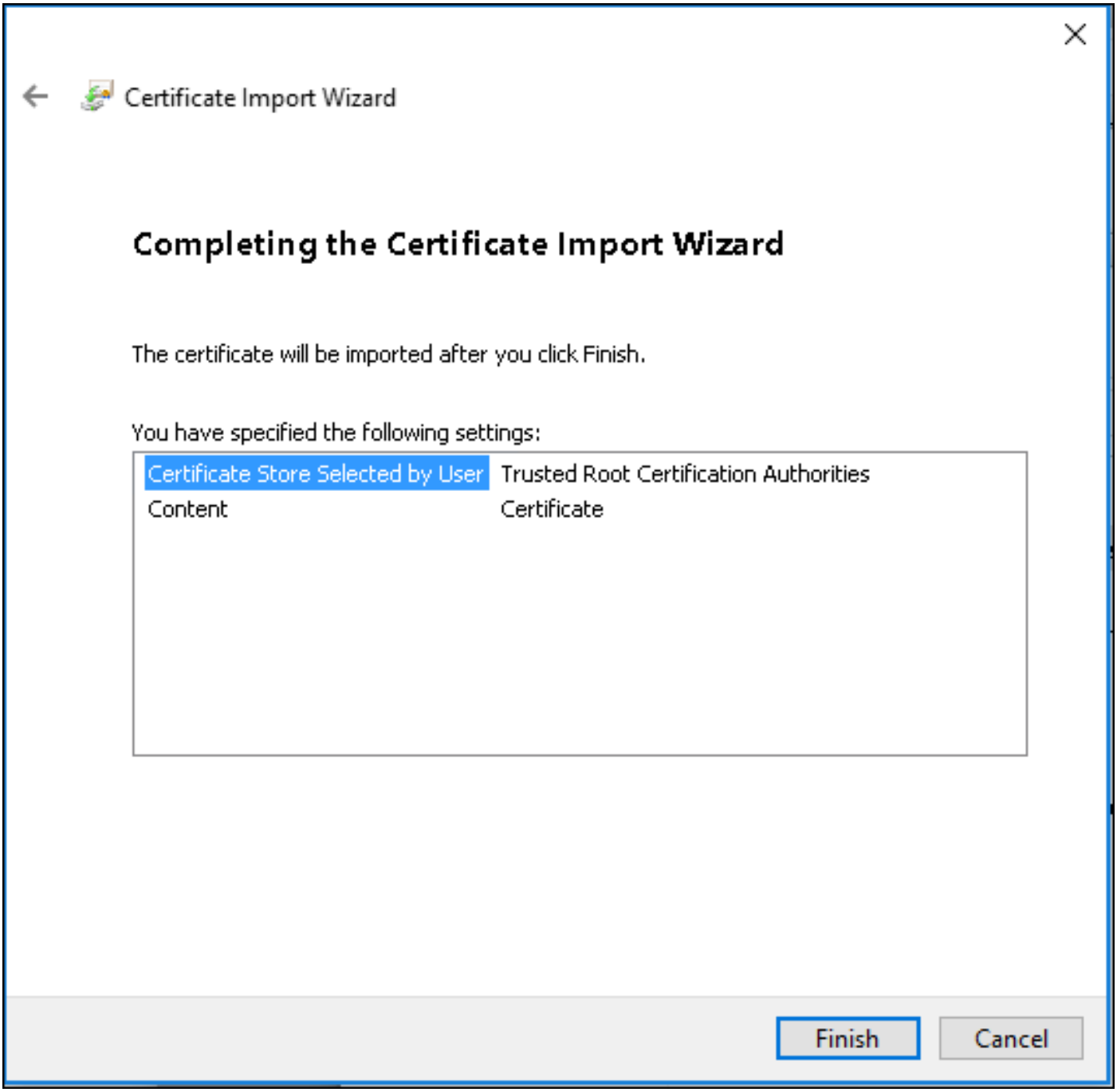
Wählen Sie die Installation auf dem **lokalen Computer aus,** und klicken Sie dann auf **Weiter.**



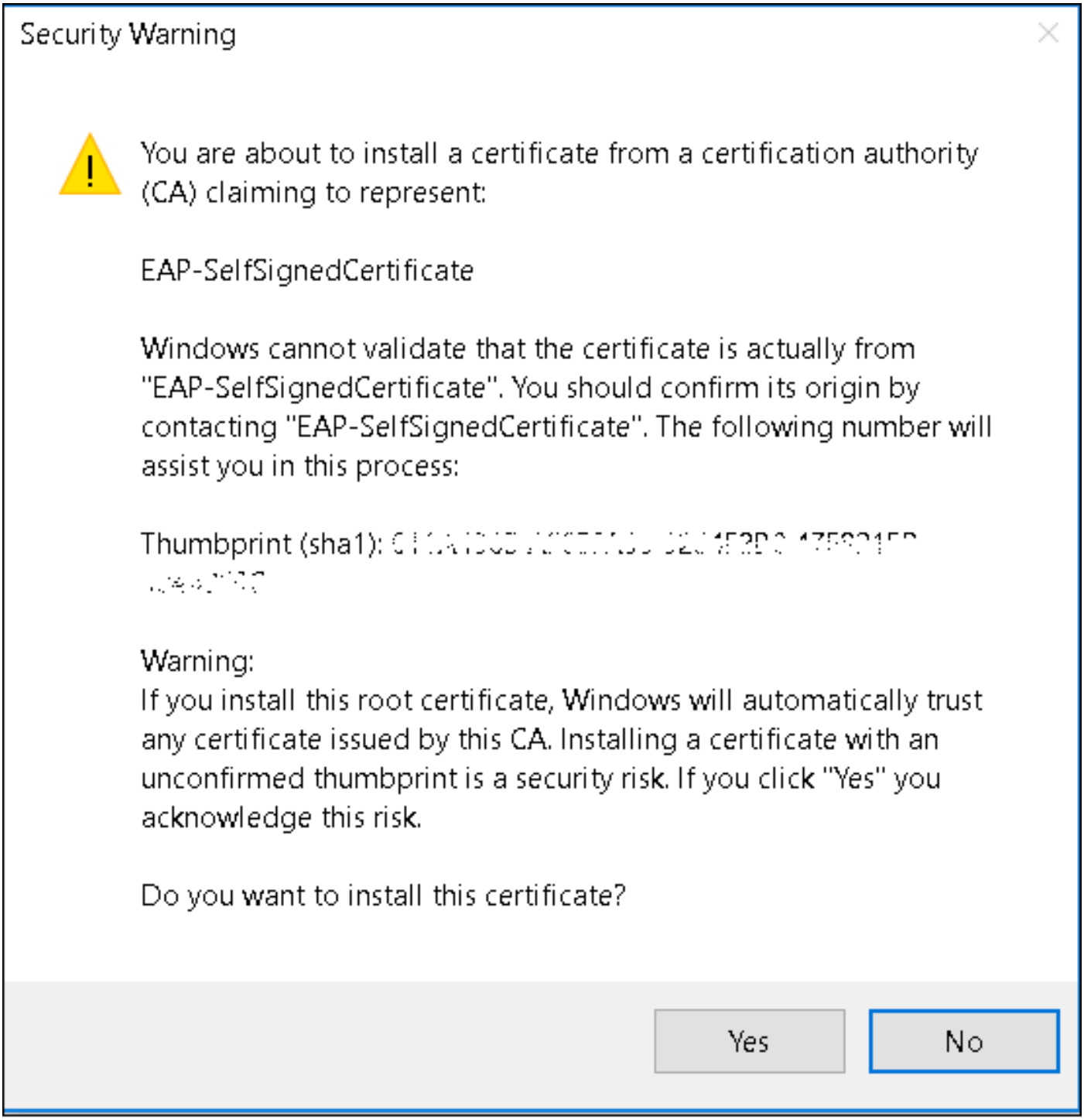
Wählen Sie **Alle Zertifikate im folgenden Speicher ablegen aus**, suchen Sie anschließend nach **vertrauenswürdigen Stammzertifizierungsstellen** und wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen aus**. Klicken Sie anschließend auf **Weiter**.



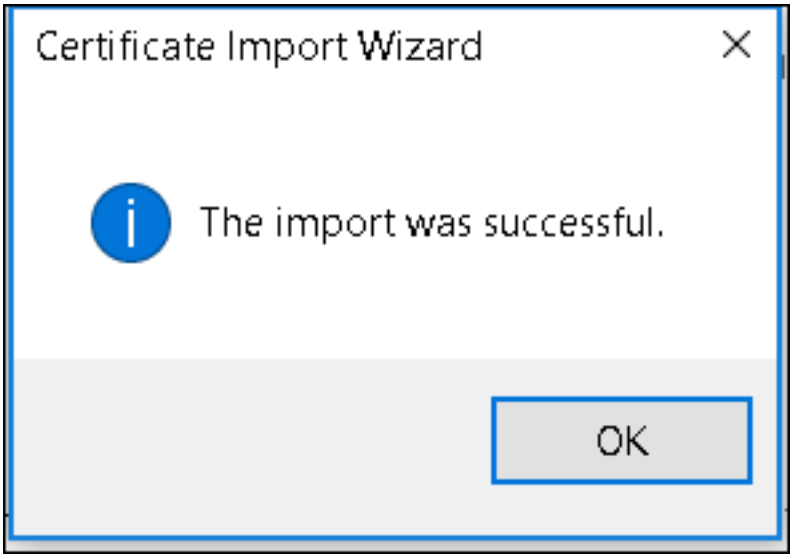
Klicken Sie anschließend auf **Fertig stellen.**



Klicken Sie am Ende auf **Ja**, um die Installation des Zertifikats zu bestätigen.

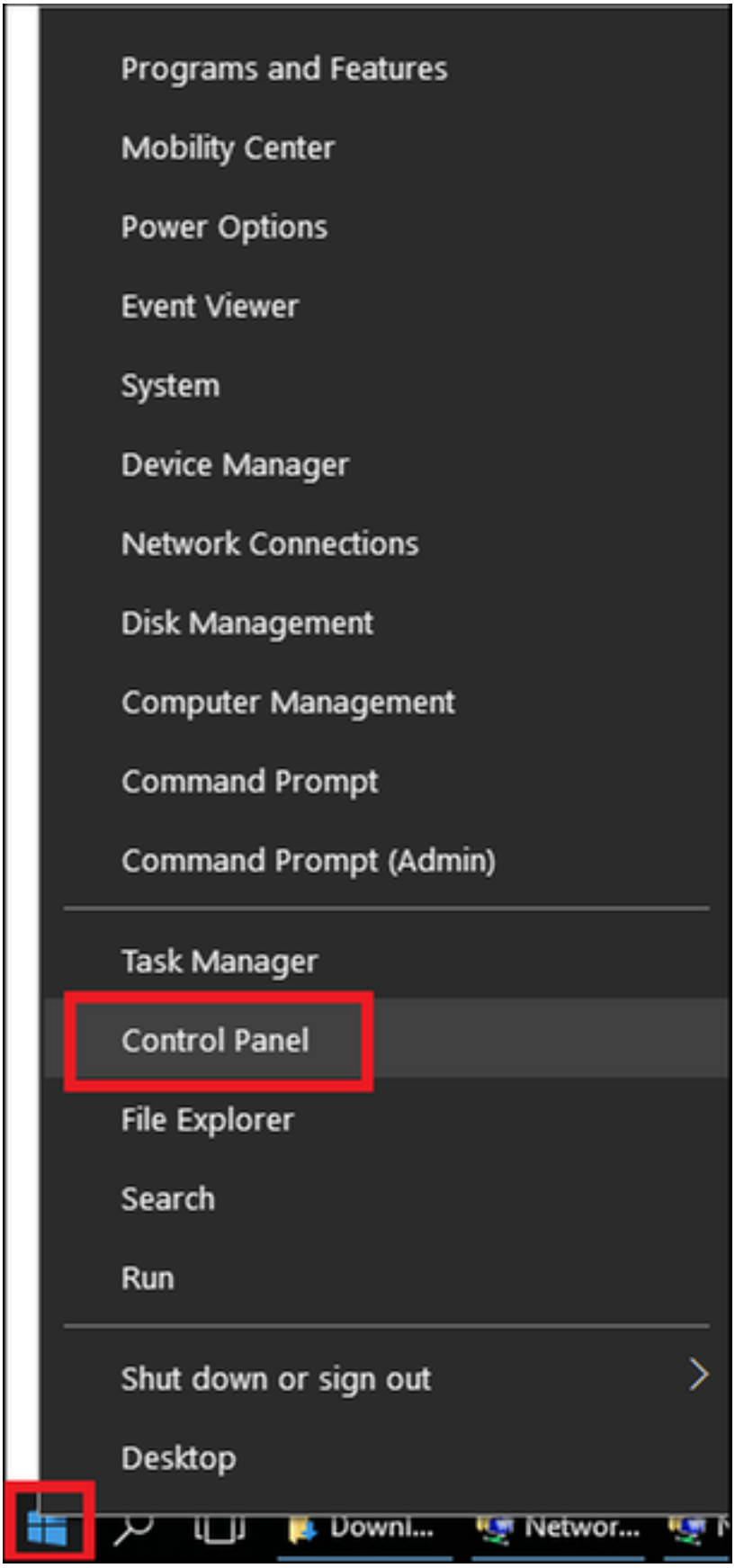


Klicken Sie abschließend auf **OK.**

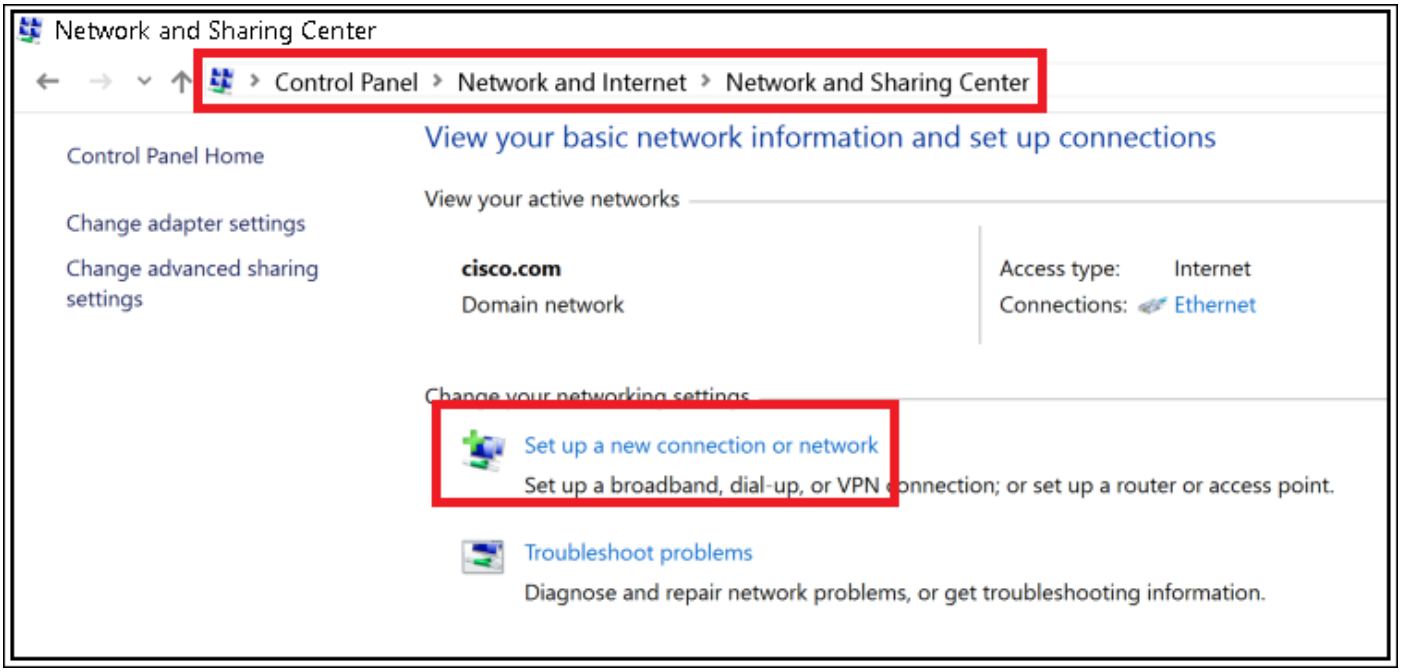


Endgerätekonfiguration - Erstellen eines WLAN-Profils

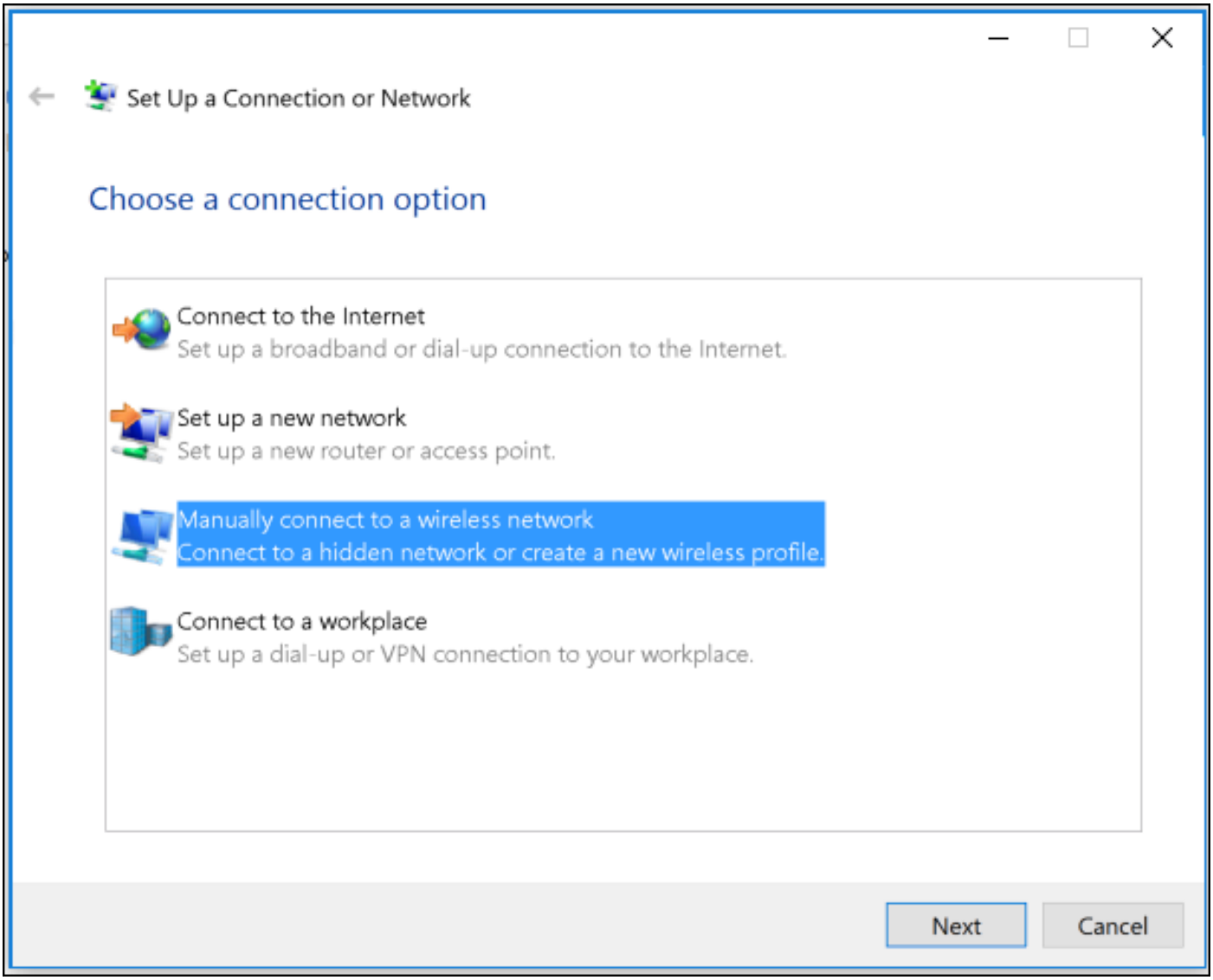
Schritt 1: Klicken Sie mit der rechten Maustaste auf das **Start-**Symbol, und wählen Sie **Systemsteuerung aus.**



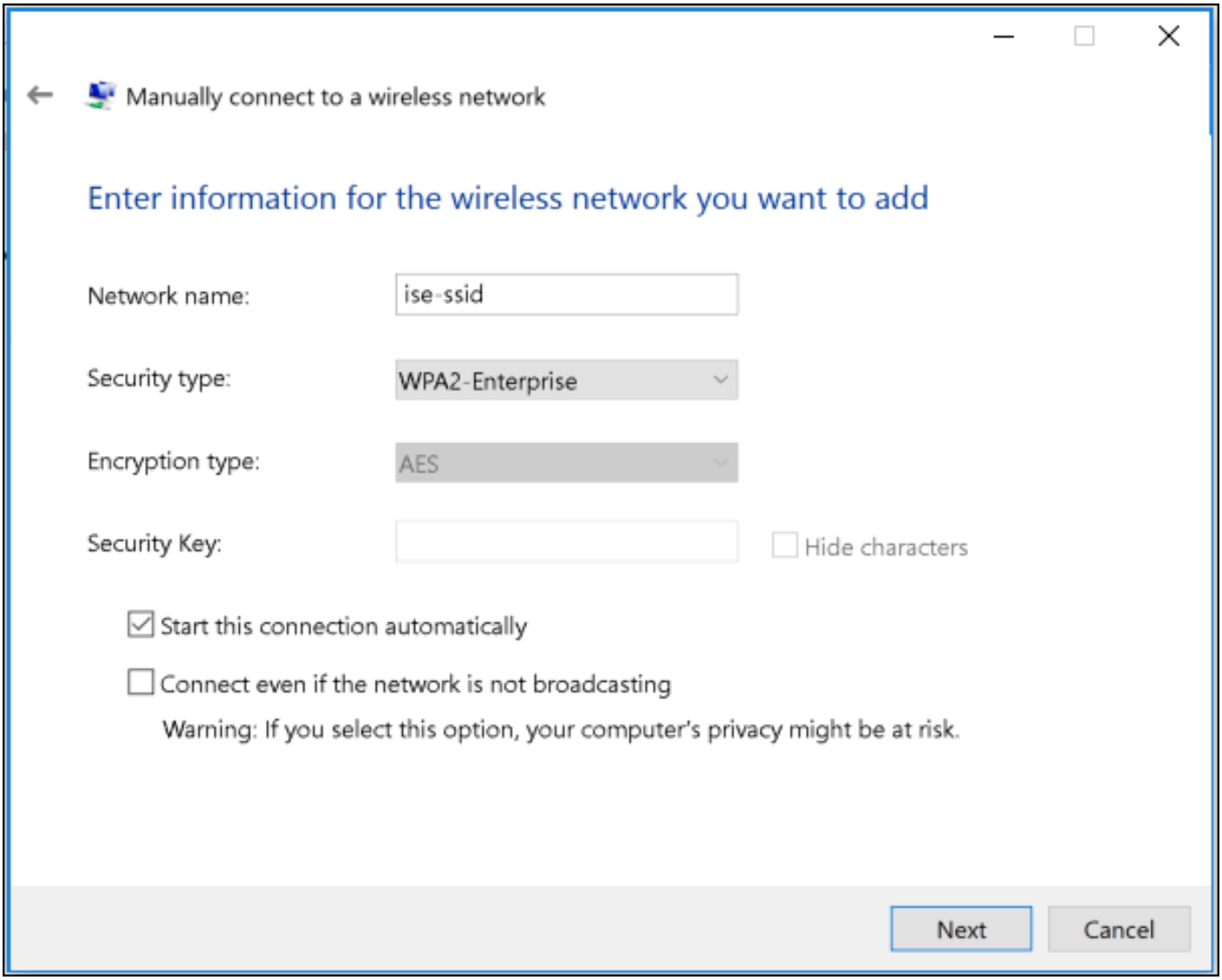
Schritt 2: Navigieren Sie zu **Netzwerk und Internet** und dann zum **Netzwerk- und Freigabecenter**, und klicken Sie auf **Neue Verbindung oder neues Netzwerk einrichten.**



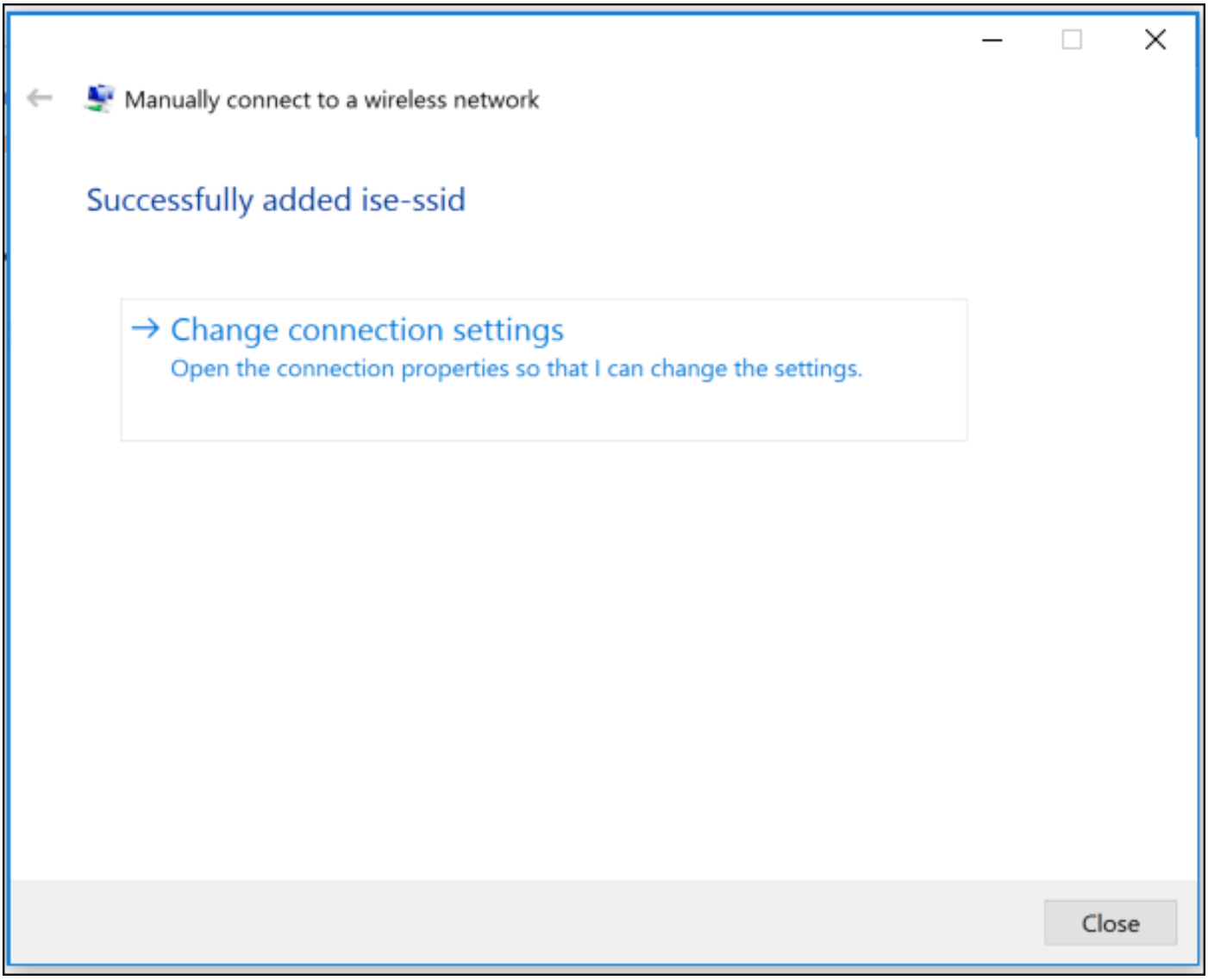
Schritt 3: Wählen Sie **Manuelle Verbindung mit einem Wireless-Netzwerk herstellen aus**, und klicken Sie auf **Weiter**.



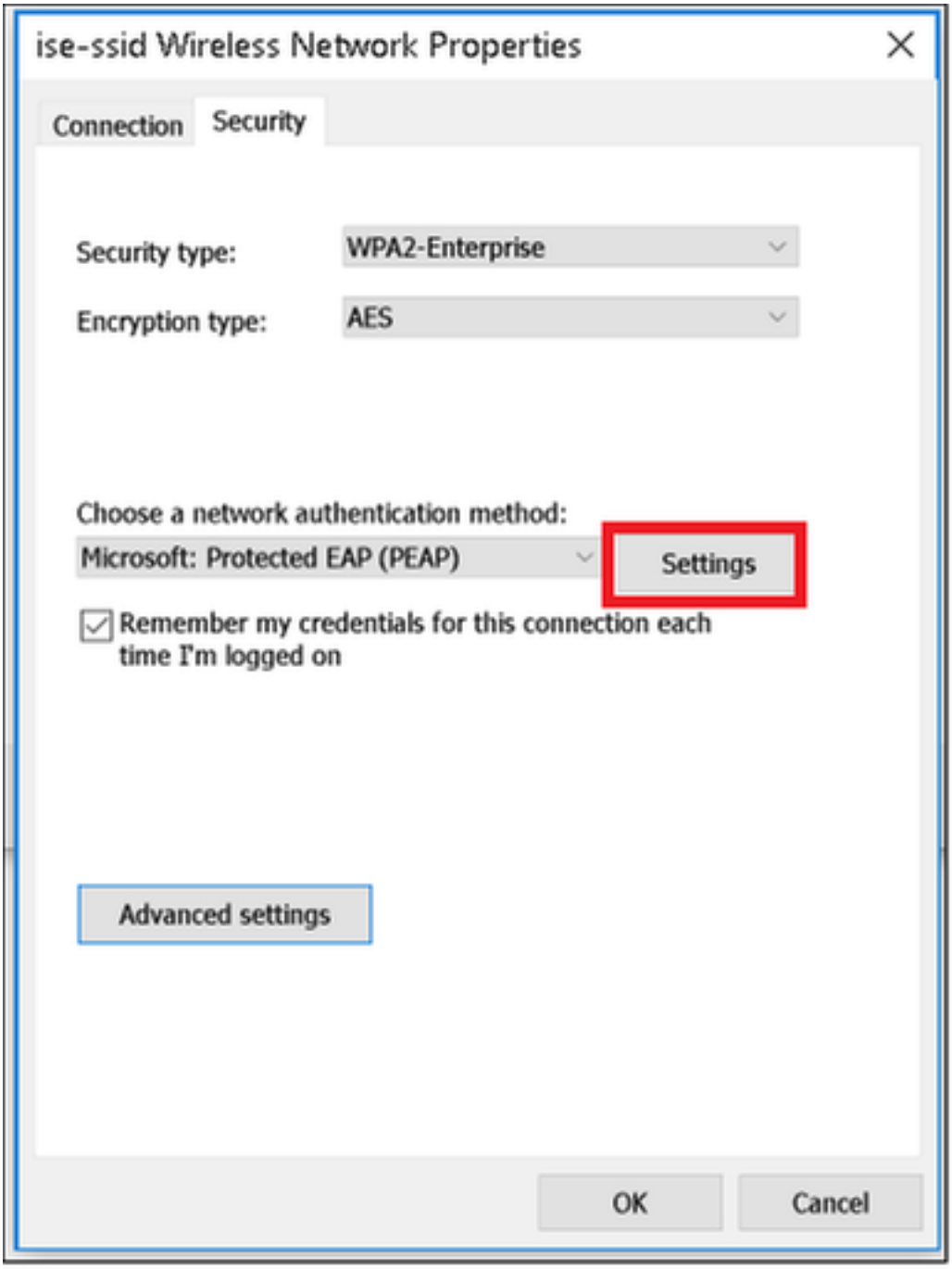
Schritt 4: Geben Sie die Informationen mit dem Namen der SSID und des Sicherheitstyps WPA2-Enterprise ein, und klicken Sie auf **Weiter**.



Schritt 5: Wählen Sie **Verbindungseinstellungen ändern**, um die Konfiguration des WLAN-Profils anzupassen.



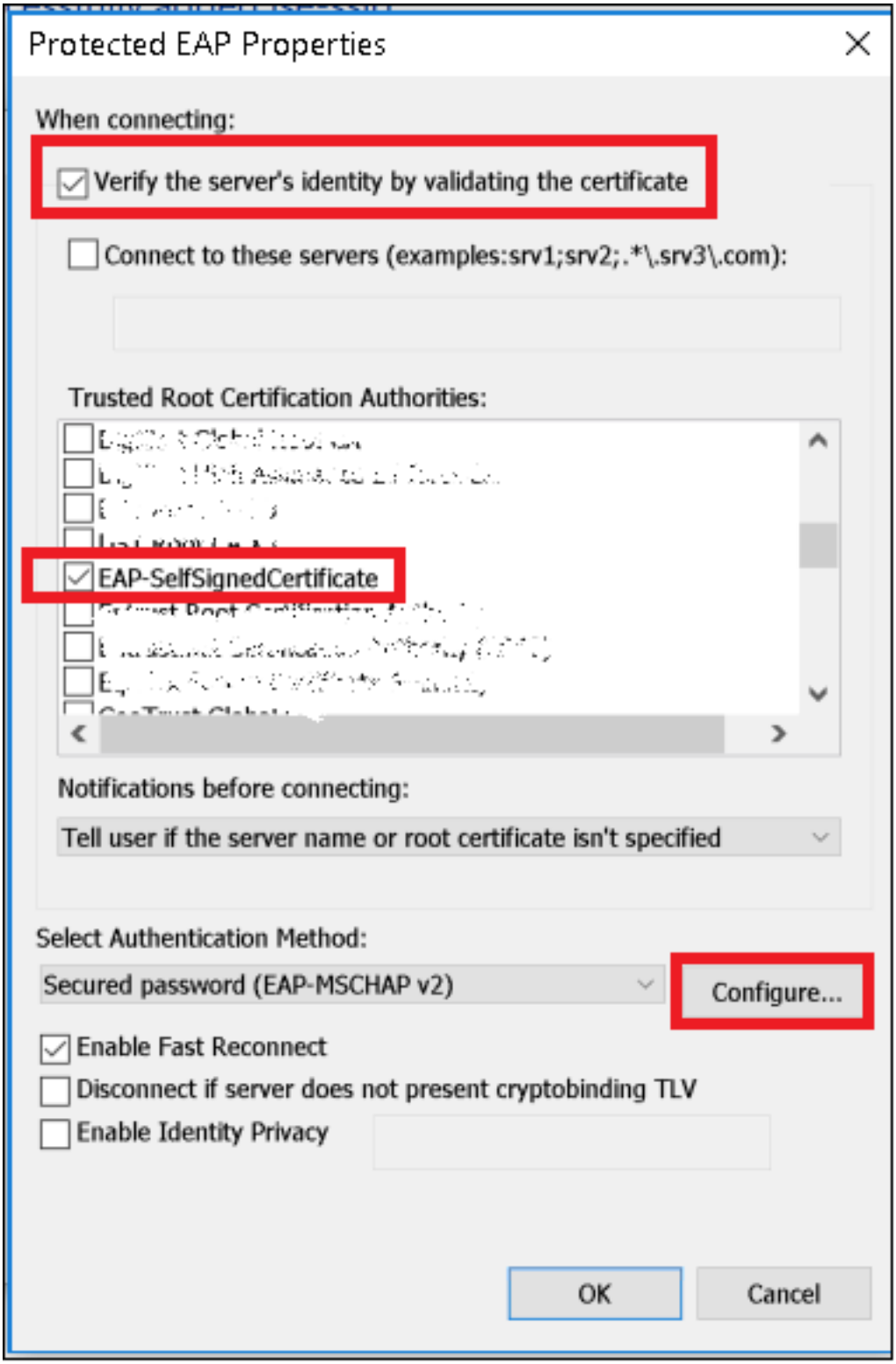
Schritt 6: Navigieren Sie zur Registerkarte **Sicherheit**, und klicken Sie auf **Einstellungen.**

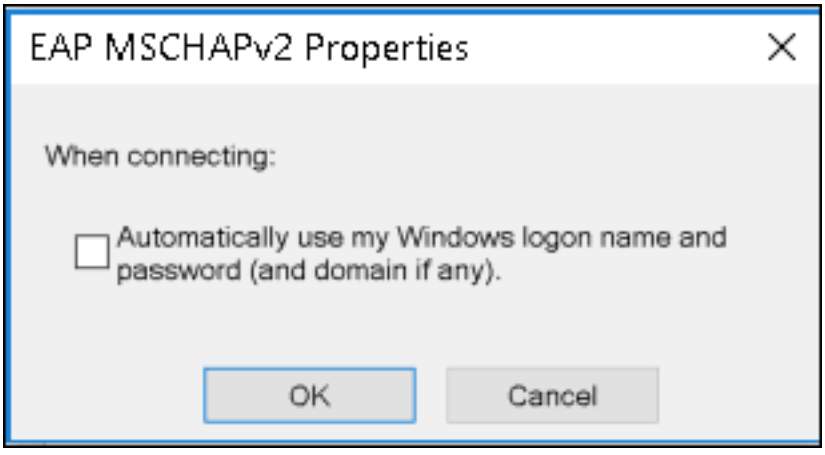


Schritt 7: Wählen Sie aus, ob der RADIUS-Server validiert wurde.

Falls ja, aktivieren Sie **Verifizieren der Serveridentität durch Validieren des Zertifikats** und von **Trusted Root Certification Authority:** Wählen Sie das selbstsignierte Zertifikat der ISE aus.

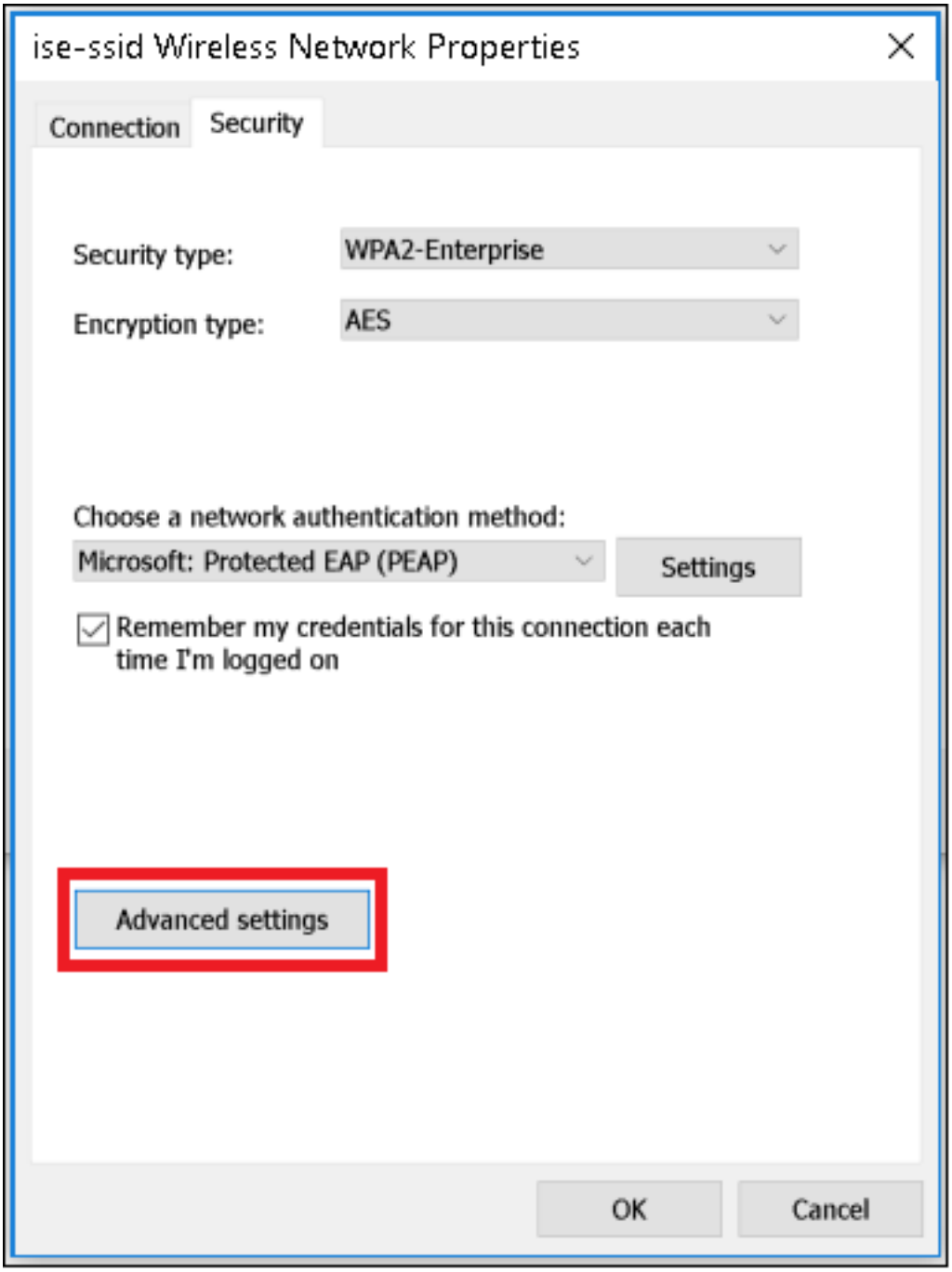
Wählen Sie anschließend **Configure** and disable **Automatisch my Windows logon name and password...**, und klicken Sie dann auf **OK.**

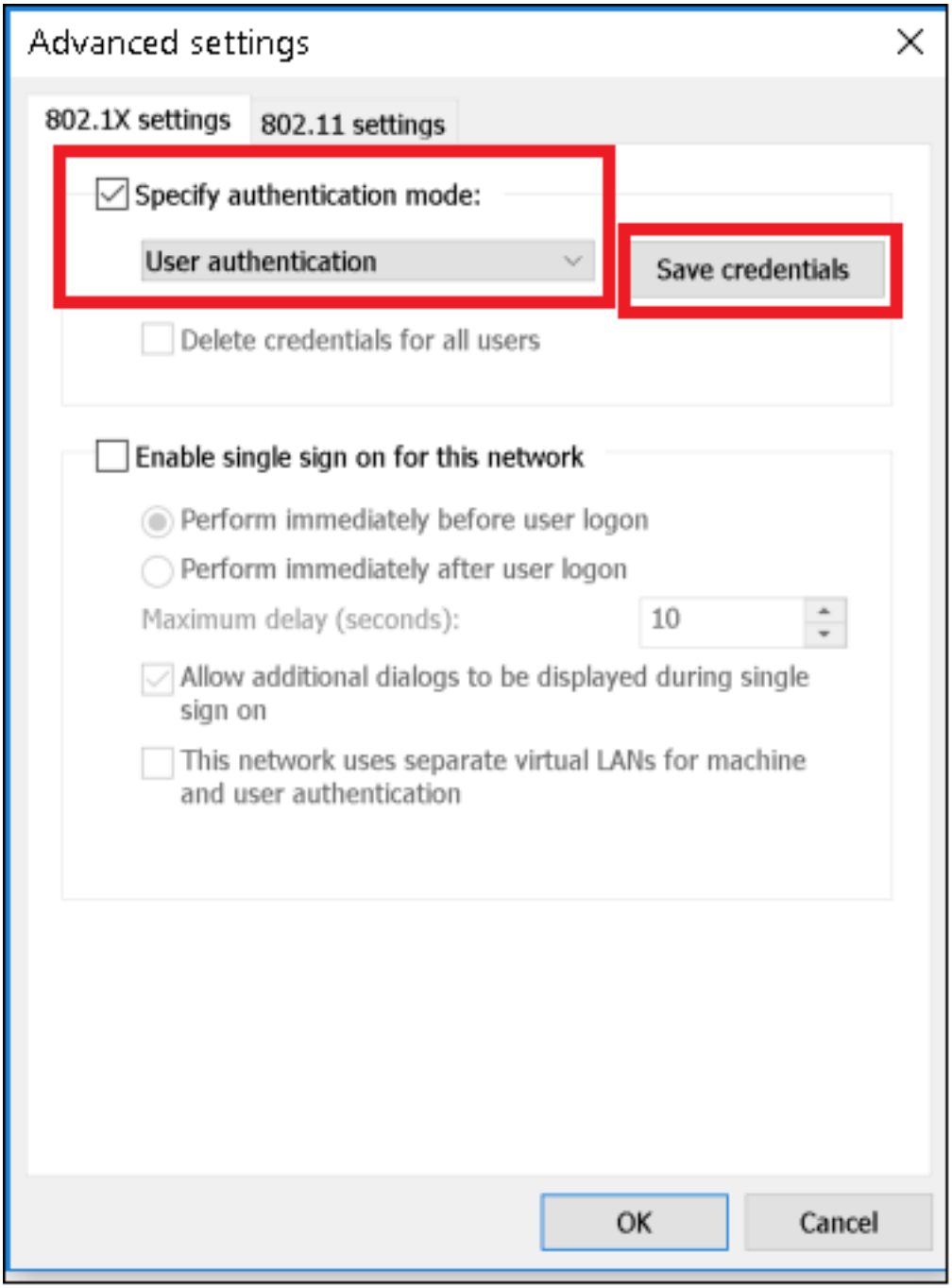

Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
EAP-SelfSignedCertificate
Notifications before connecting:
Tell user if the server name or root certificate isn't specified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

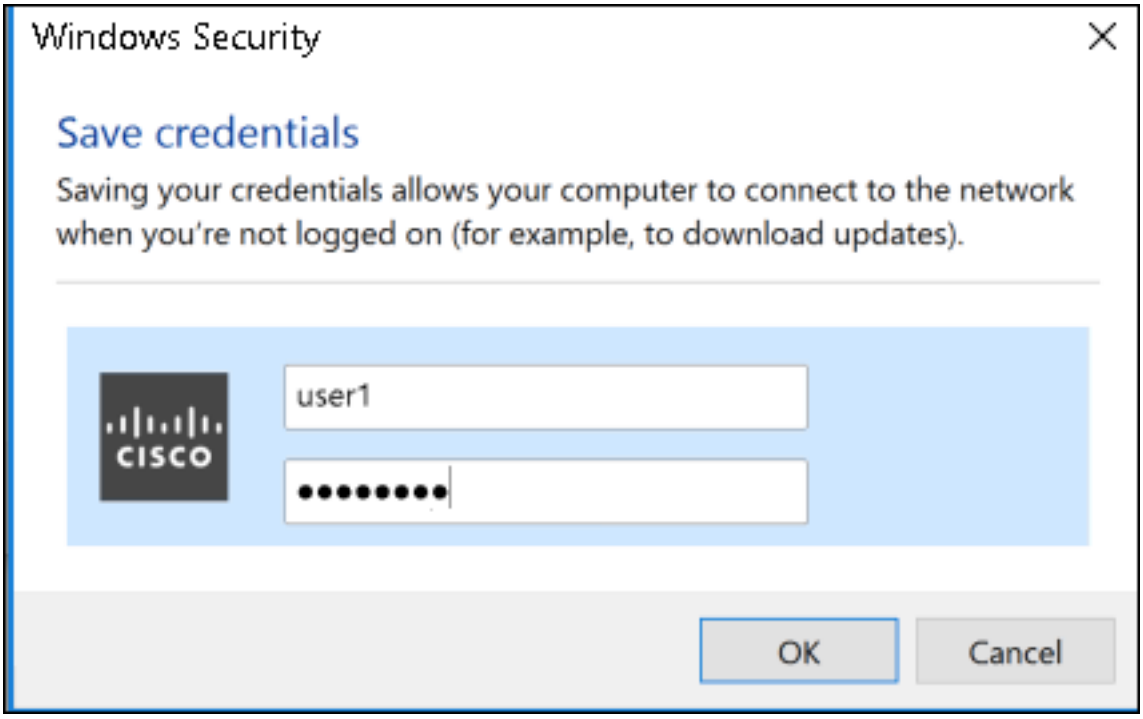

EAP MSCHAPv2 Properties
When connecting:
Automatically use my Windows logon name and password (and domain if any).
OK
Cancel

Schritt 8: Konfigurieren der Benutzeranmeldeinformationen

Wenn Sie wieder zur Registerkarte **Sicherheit** zurückkehren, wählen Sie **Erweiterte Einstellungen aus**, geben Sie den Authentifizierungsmodus als **Benutzerauthentifizierung** an, und speichern Sie die Anmeldeinformationen, die für die ISE konfiguriert wurden, um den Benutzer zu authentifizieren.




Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel



Überprüfen

Der Authentifizierungsablauf kann aus WLC- oder ISE-Perspektive überprüft werden.

Authentifizierungsprozess für ME

Führen Sie diesen Befehl aus, um den Authentifizierungsprozess für einen bestimmten Benutzer zu überwachen:

```
> debug client <mac-add-client>
```

Beispiel für eine erfolgreiche Authentifizierung (einige Ausgabe wurde weggelassen):

```
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Processing assoc-req
station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 thread:669ba80
*apfMsConnTask_0: Nov 25 16:36:24.333: 08:74:02:77:13:45 Association received from mobile on
BSSID 38:ed:18:c6:7b:4d AP 1852-4
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying site-specific Local Bridging
override for station 08:74:02:77:13:45 - vapId 3, site 'FlexGroup', interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Applying Local Bridging Interface
Policy for station 08:74:02:77:13:45 - vlan 0, interface id 0, interface 'management'
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Set Clinet Non AP specific
apfMsAccessVlan = 2400
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 This apfMsAccessVlan may be changed
later from AAA after L2 Auth
*apfMsConnTask_0: Nov 25 16:36:24.334: 08:74:02:77:13:45 Received 802.11i 802.1X key management
suite, enabling dot1x Authentication
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state START (0)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state AUTHCHECK (2)
```

*apfMsConnTask_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client**
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 apfPemAddUser2:session timeout forstation 08:74:02:77:13:45 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Stopping deletion of Mobile Station: (callerId: 48)
*apfMsConnTask_0: Nov 25 16:36:24.335: 08:74:02:77:13:45 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0
*apfMsConnTask_0: Nov 25 16:36:24.335: 0**8:74:02:77:13:45 Sending assoc-resp with status 0 station:08:74:02:77:13:45 AP:38:ed:18:c6:7b:40-01 on apVapId 3**
*apfMsConnTask_0: Nov 25 16:36:24.335: **08:74:02:77:13:45 Sending Assoc Response to station on BSSID 38:ed:18:c6:7b:4d (status 0) ApVapId 3 Slot 1**
*spamApTask0: Nov 25 16:36:24.341: 08:74:02:77:13:45 Sent dot1x auth initiate message for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 reauth_sm state transition 0 ---> 1 for mobile 08:74:02:77:13:45 at 1x_reauth_sm.c:47
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 EAP-PARAM Debug - eap-params for Wlan-Id :3 is disabled - applying Global eap timers and retries
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Connecting state
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.342: **08:74:02:77:13:45 Sending EAP-Request/Identity to mobile 08:74:02:77:13:45 (EAP Id 1)**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received EAPOL EAPPKT from mobile 08:74:02:77:13:45**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:24.401: **08:74:02:77:13:45 Received Identity Response (count=1) from mobile 08:74:02:77:13:45**
.
.
.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Processing Access-Accept for mobile 08:74:02:77:13:45**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: **08:74:02:77:13:45 Username entry (user1) created in mscb for mobile, length = 253**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Station 08:74:02:77:13:45 setting dot1x reauth timeout = 1800
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.978: 08:74:02:77:13:45 Creating a PKC PMKID Cache entry for station 08:74:02:77:13:45 (RSN 2)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding BSSID 38:ed:18:c6:7b:4d to PMKID cache at index 0 for station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Adding Audit session ID payload in Mobility handoff
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Disabling re-auth since PMK lifetime can take care of same.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Sending EAP-Success to mobile 08:74:02:77:13:45 (EAP Id 70)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Freeing AAACB from Dot1xCB as AAA auth is done for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: 08:74:02:77:13:45 Found an cache entry for BSSID 38:ed:18:c6:7b:4d in PMKID cache at index 0 of station 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: Including PMKID in M1 (16)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] 80 3a 20 8c 8f c2 4c 18 7d 4c 28 e7 7f 10 11 03
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0000] dd 14 00 0f ac 04 80 3a 20 8c 8f c2 4c 18 7d 4c
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: [0016] 28 e7 7f 10 11 03

*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.979: **08:74:02:77:13:45 Starting key exchange to mobile 08:74:02:77:13:45, data packets will be dropped**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: **08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45**
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Entering Backend Auth Success state (id=70) for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 Received Auth Success while in Authenticating state for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.980: 08:74:02:77:13:45 dot1x - moving mobile 08:74:02:77:13:45 into Authenticated state
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received EAPOL-Key from mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: **08:74:02:77:13:45 Received EAPOL-key in PTK_START state (message 2) from mobile 08:74:02:77:13:45**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.983: 08:74:02:77:13:45 Received valid MIC in EAPOL Key Message M2!!!!!
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 0..............
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: 00 0f ac 01 0c 00 ......
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000000: 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ....
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 00000010: ac 01 0c 00 ....
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 PMK: Sending cache add
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: **08:74:02:77:13:45 Sending EAPOL-Key Message to mobile 08:74:02:77:13:45**
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.984: 08:74:02:77:13:45 Reusing allocated memory for EAP Pkt for retransmission to mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: **08:74:02:77:13:45 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 08:74:02:77:13:45**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Stopping retransmission timer for mobile 08:74:02:77:13:45
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: **08:74:02:77:13:45 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vlan Ip: 172.16.0.136, Vlan mask : 255.255.255.224
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Virtual Ip: 192.0.2.1
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) DHCP required on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3for this client
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 38:ed:18:c6:7b:40 vapId 3 apVapId 3 flex-acl-name:
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: **08:74:02:77:13:45 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)**
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6623, Adding TMP rule
*Dot1x_NW_MsgTask_0: Nov 25 16:36:25.988: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule

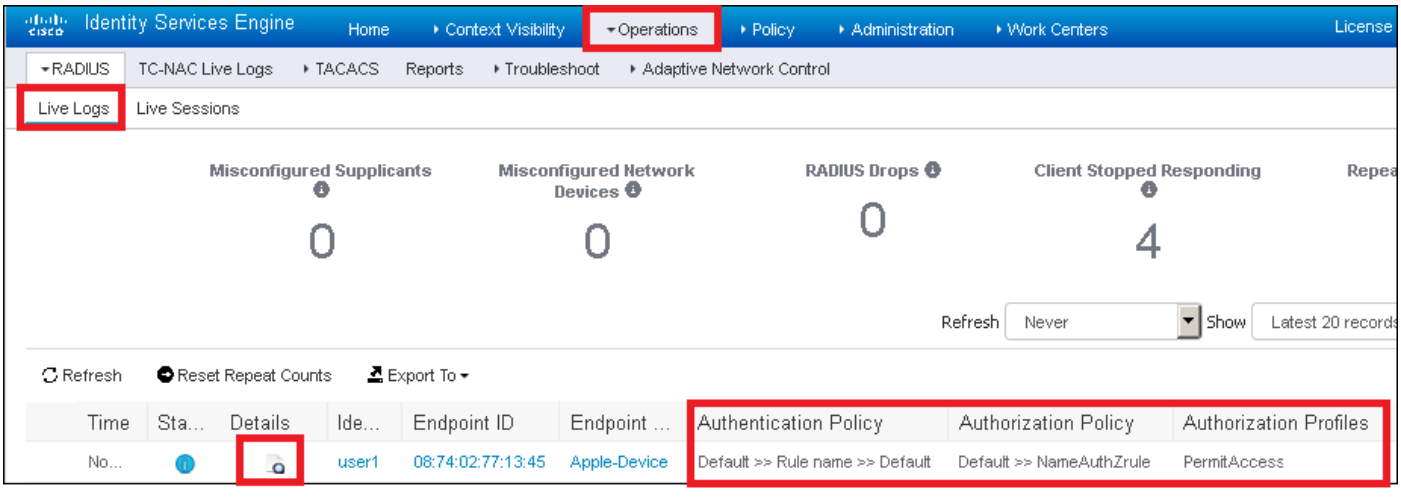
```
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) mobility role
update request from Unassociated to Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.136
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
6261, Adding TMP rule
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Replacing Fast
Path rule
type = Airespace AP - Learn IP address
on AP 38:ed:18:c6:7b:40, slot 1, interface = 1, QOS = 0
IPv4 ACL ID = 255,
*apfReceiveTask: Nov 25 16:36:25.989: 08:74:02:77:13:45 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*pemReceiveTask: Nov 25 16:36:25.990: 08:74:02:77:13:45 0.0.0.0 Added NPU entry of type 9,
dtlFlags 0x0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 In apfRegisterIpAddrOnMscb_debug:
regType=1 Invalid src IP address, 0.0.0.0 is part of reserved ip address range (caller
apf_ms.c:3593)
*apfReceiveTask: Nov 25 16:36:27.835: 08:74:02:77:13:45 IPv4 Addr: 0:0:0:0
*apfReceiveTask: Nov 25 16:36:27.840: 08:74:02:77:13:45 WcdbClientUpdate: IP Binding from WCDB
ip_learn_type 1, add_or_delete 1
*apfReceiveTask: Nov 25 16:36:27.841: 08:74:02:77:13:45 172.16.0.16 DHCP_REQD (7) Change state
to RUN (20) last state DHCP_REQD (7)
```

Verwenden Sie das *Wireless Debug Analyzer*-Tool, um die Debug-Client-Ausgaben leicht zu lesen:

[Wireless-Debug-Analyzer]

Authentifizierungsprozess für die ISE

Navigieren Sie zu **Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live-Protokolle)**, um herauszufinden, welche Authentifizierungsrichtlinie, Autorisierungsrichtlinie und welches Autorisierungsprofil dem Benutzer zugewiesen sind.



Für weitere Informationen klicken Sie auf **Details**, um einen detaillierteren

Authentifizierungsprozess anzuzeigen.