Konfigurieren der 802.1X-Authentifizierung mit PEAP, ISE 2.1 und WLC 8.3

Inhalt

Einleitung

In diesem Dokument wird die Einrichtung eines Wireless Local Area Network (WLAN) mit 802.1x-Sicherheit und Virtual Local Area Network (VLAN) Override beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- 802.1x
- Protected Extensible Authentication Protocol (PEAP)
- Zertifizierungsstelle (CA)
- Zertifikate

Verwendete Komponenten

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

- WLC Version 8.3.102.0

- Identity Service Engine (ISE) Version 2.1
- Windows 10-Laptop

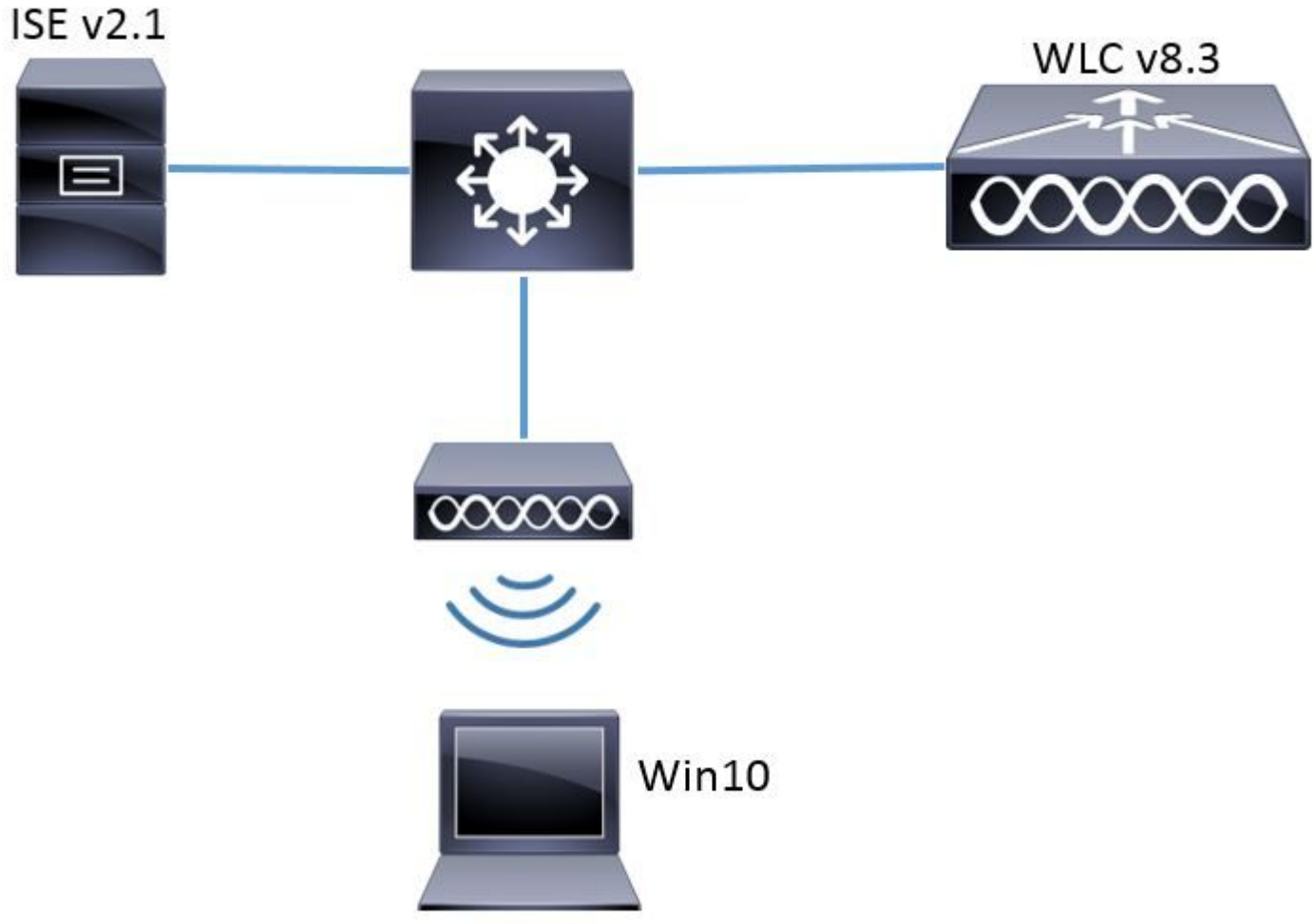
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Hintergrundinformationen

Wenn Sie ein WLAN mit 802.1x-Sicherheit und VLAN einrichten, können Sie das Protected Extensible Authentication Protocol als Extensible Authentication Protocol (EAP) außer Kraft setzen.

Konfigurieren

Netzwerkdiagramm



Konfiguration

Die allgemeinen Schritte sind wie folgt:

1. Deklarieren Sie den RADIUS-Server auf dem WLC und umgekehrt, um die Kommunikation untereinander zu ermöglichen.
2. Erstellen Sie den Service Set Identifier (SSID) im WLC.

3. Erstellen Sie die Authentifizierungsregel auf der ISE.
4. Erstellen Sie das Autorisierungsprofil auf der ISE.
5. Erstellen Sie die Autorisierungsregel für die ISE.
6. Konfigurieren Sie den Endpunkt.

RADIUS-Server auf WLC deklarieren

Um die Kommunikation zwischen dem RADIUS-Server und dem WLC zu ermöglichen, müssen Sie den RADIUS-Server auf dem WLC registrieren und umgekehrt.

GUI:

Schritt 1: Öffnen Sie die grafische Benutzeroberfläche des WLC, und navigieren Sie zu **SECURITY > RADIUS > Authentication > New,** wie im Bild dargestellt.

Schritt 2: Geben Sie die Informationen zum RADIUS-Server wie im Bild dargestellt ein.

CLI:

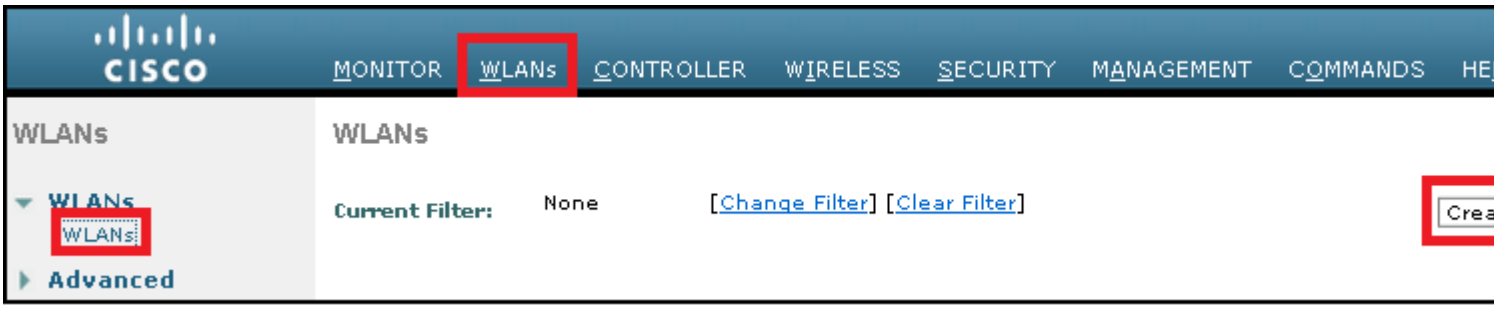
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

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

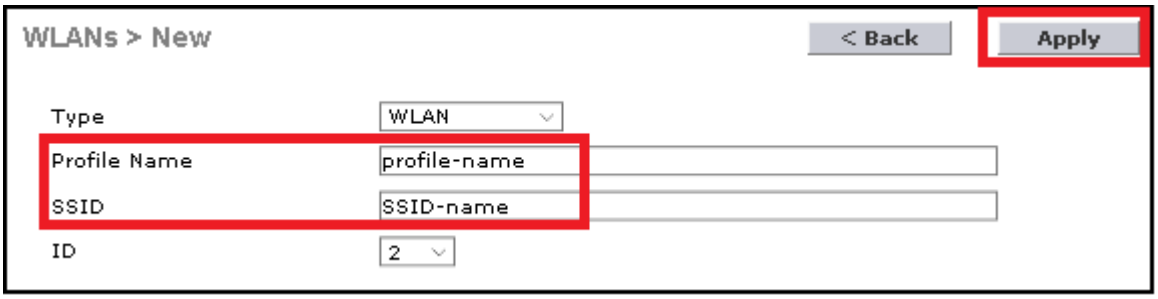
SSID erstellen

GUI:

Schritt 1: Öffnen Sie die grafische Benutzeroberfläche des WLC, und navigieren Sie zu **WLANs > Create New > Go** (WLANs > Neues erstellen > Gehe zu), wie im Bild dargestellt.



Schritt 2: Wählen Sie einen Namen für die SSID und das Profil aus, und klicken Sie dann wie im Bild dargestellt auf **Apply**.



CLI:

```
> config wlan create <id> <profile-name> <ssid-name>
```

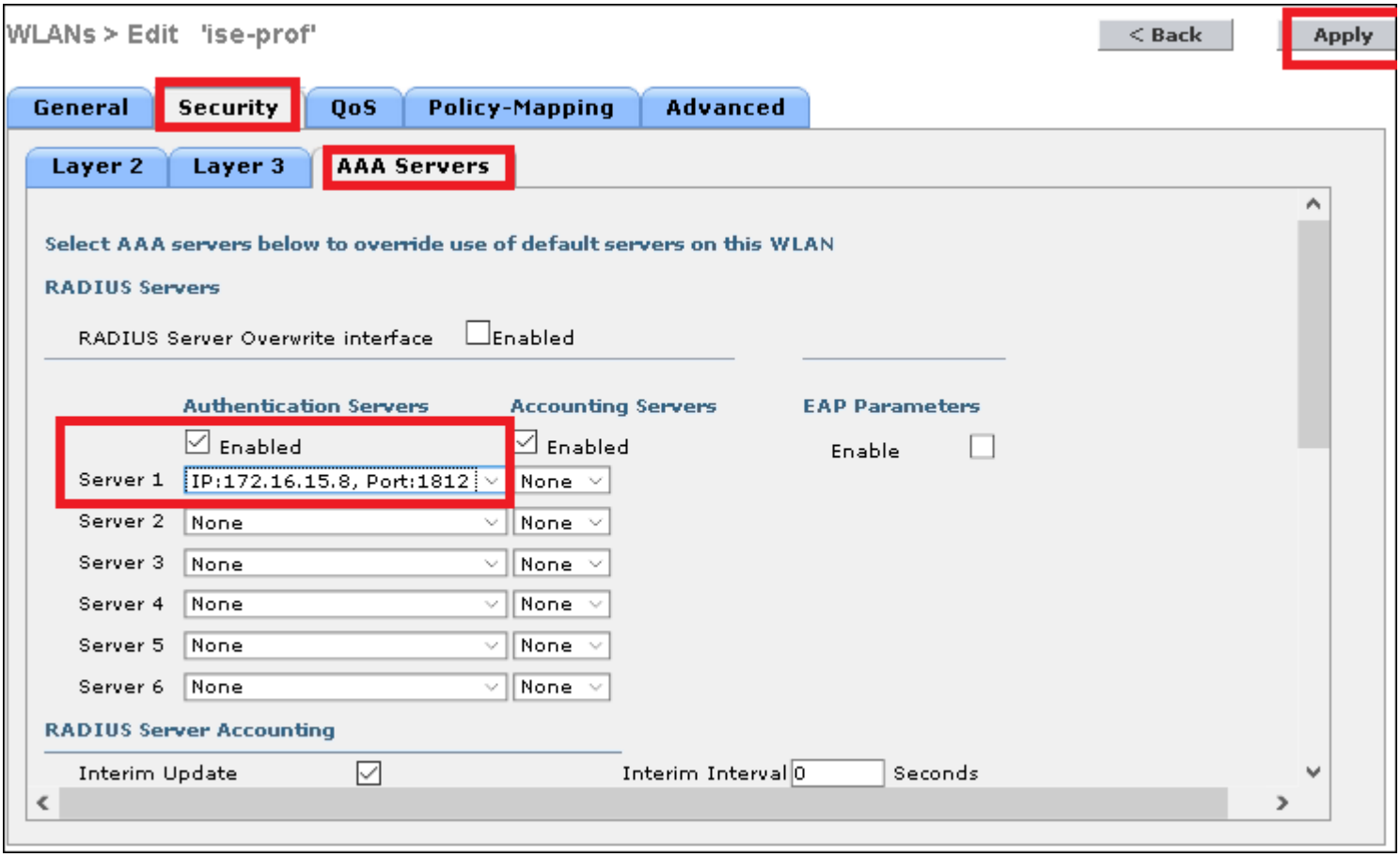
Schritt 3: Weisen Sie den RADIUS-Server dem WLAN zu.

CLI:

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

Navigieren Sie zu **Security > AAA Servers**, und wählen Sie den gewünschten RADIUS-Server aus. Drücken Sie dann auf **Apply** (Anwenden), wie im Bild dargestellt.



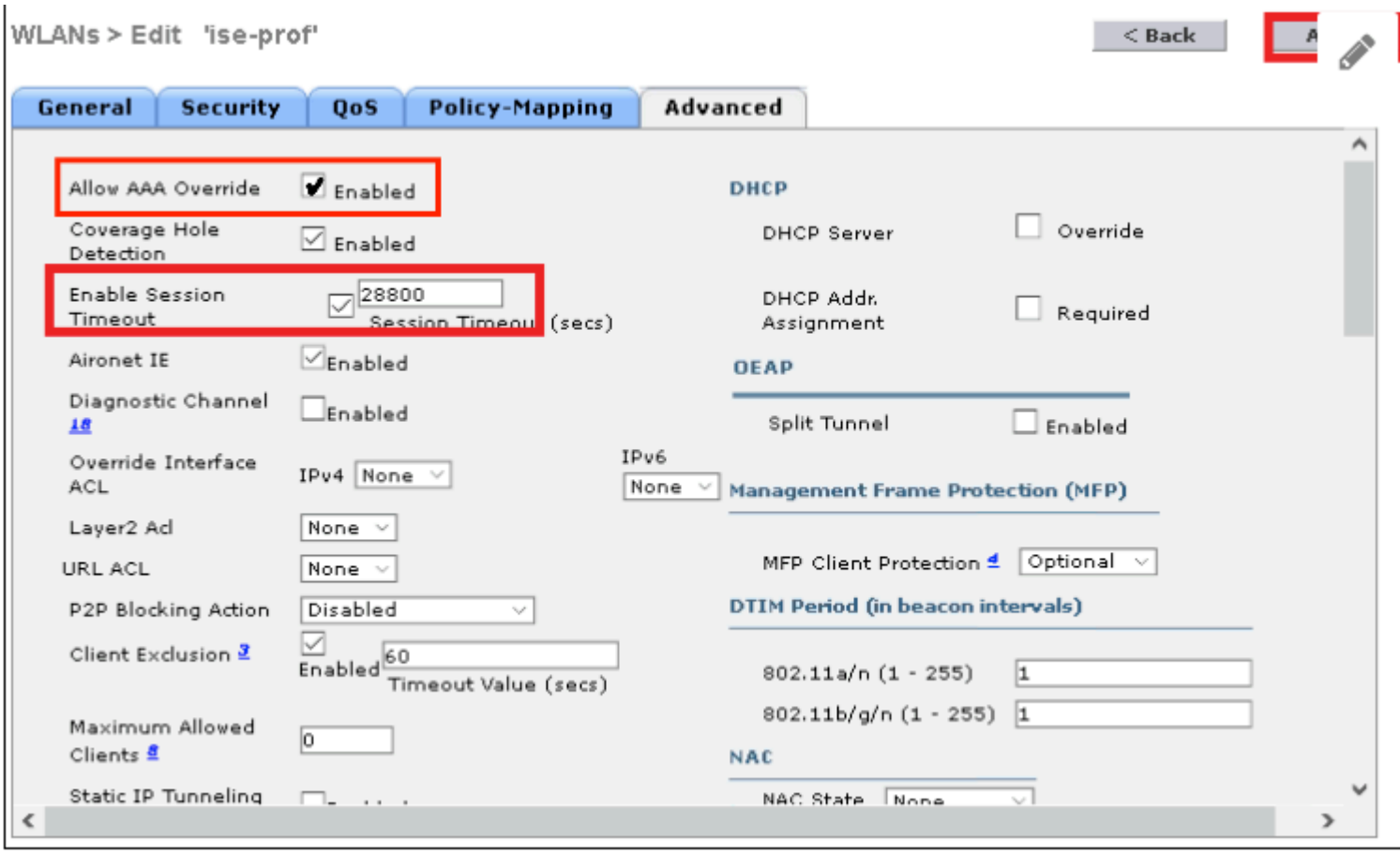
Schritt 4: Aktivieren Sie **AAA-Außerkraftsetzung zulassen,** und erhöhen Sie optional das Sitzungs-Timeout.

CLI:

```
> config wlan aaa-override enable <wlan-id>
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

Navigieren Sie zu **WLANs > WLAN ID > Advanced,** und aktivieren Sie **Allow AAA Override**. Geben Sie optional das Sitzungstimeout wie im Bild dargestellt an.



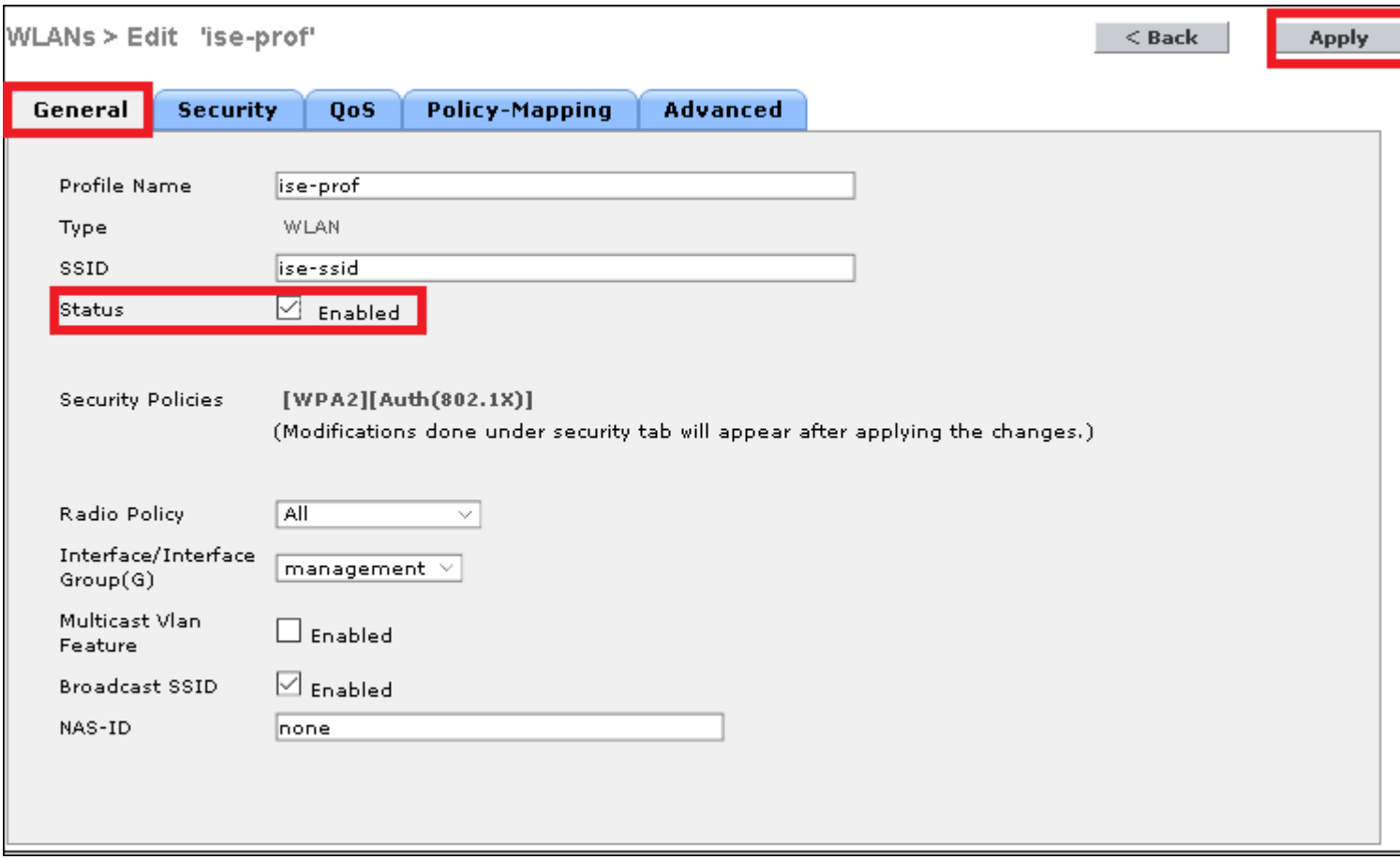
Schritt 5: Aktivieren des WLAN

CLI:

```
> config wlan enable <wlan-id>
```

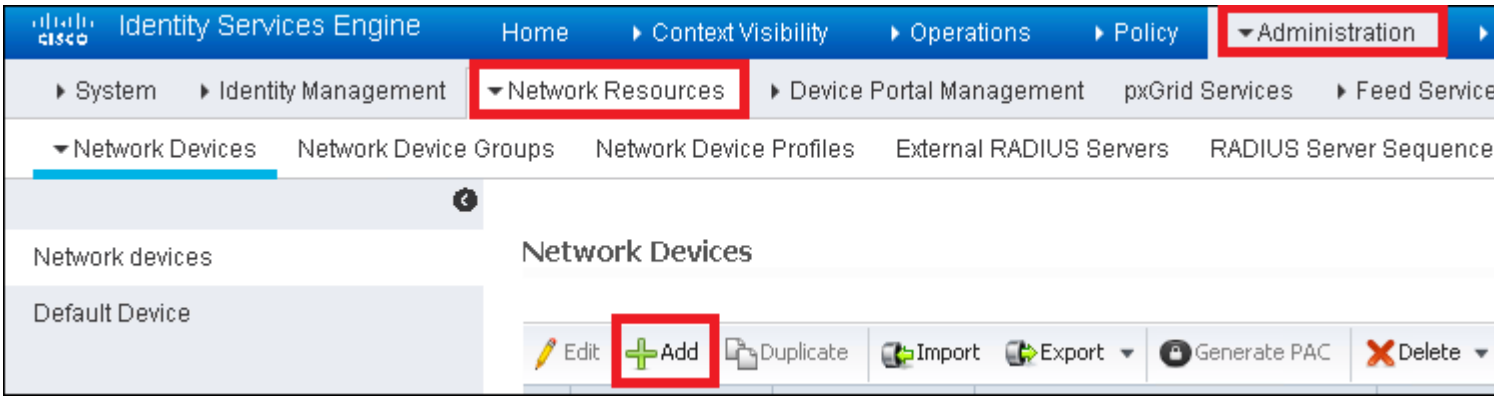
GUI:

Navigieren Sie zu **WLANs > WLAN ID > General (WLAN-ID > Allgemein)**, und aktivieren Sie die SSID, wie im Bild dargestellt.



WLC auf der ISE deklarieren

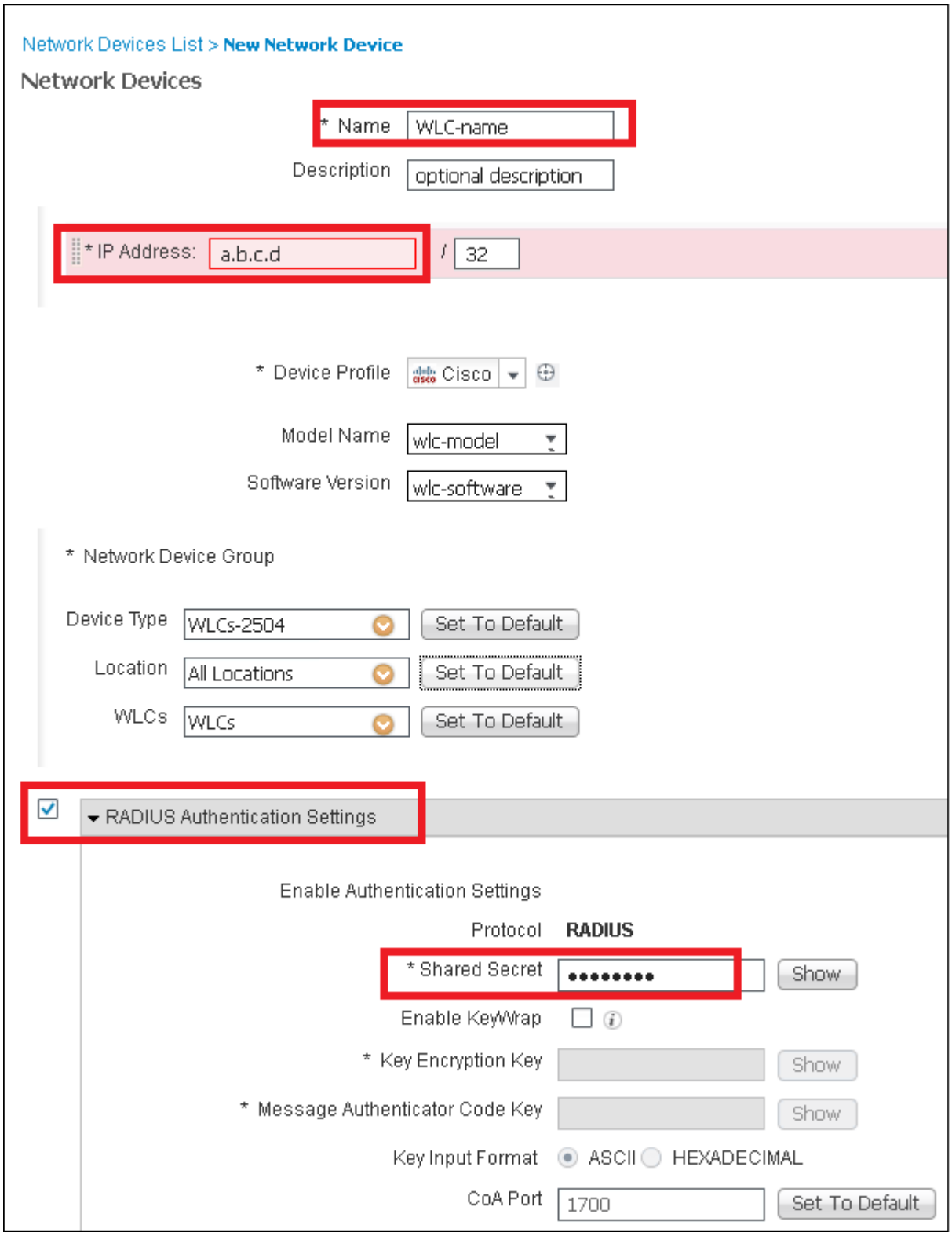
Schritt 1: Öffnen Sie die ISE-Konsole, und navigieren Sie zu **Administration** > **Network Resources** > **Network Devices** > **Add**, wie im Bild dargestellt.



Schritt 2: Geben Sie die Werte ein.

Optional können ein bestimmter Modellname, eine bestimmte Softwareversion, eine Beschreibung sowie die Zuweisung von Netzwerkgerätegruppen basierend auf Gerätetypen, Standort oder WLCs angegeben werden.

a.b.c.d entspricht der WLC-Schnittstelle, die die angeforderte Authentifizierung sendet. Standardmäßig ist dies die Management-Schnittstelle, wie im Bild dargestellt.

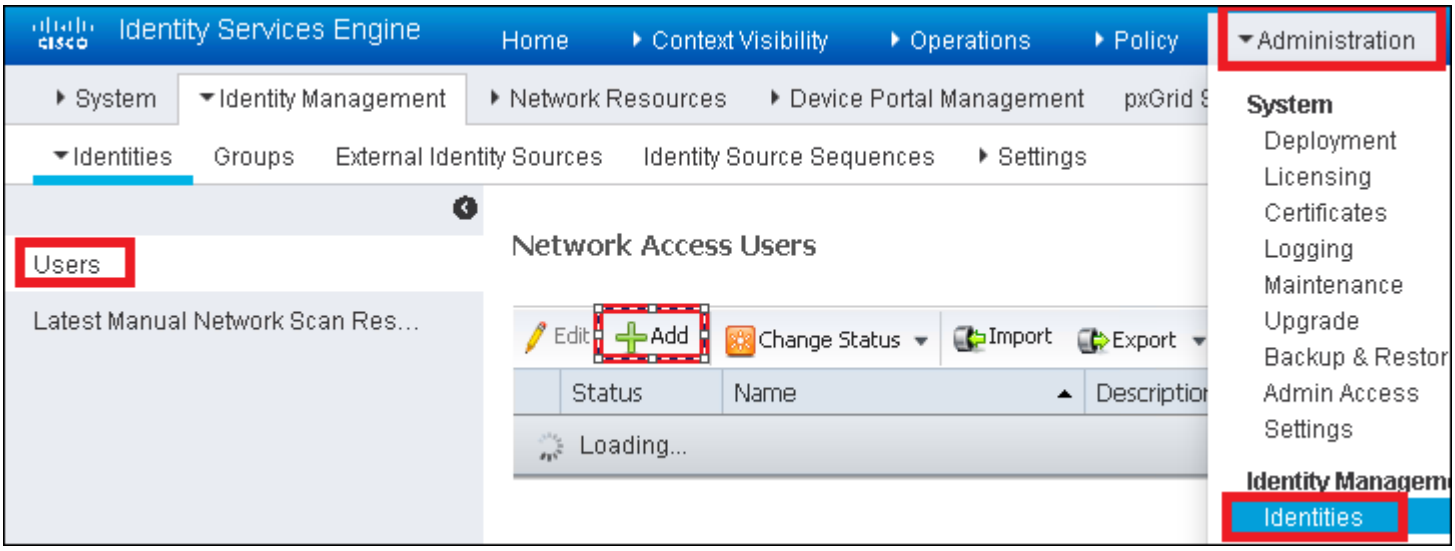


Weitere Informationen zu Netzwerk-Gerätegruppen:

ISE â€“ Netzwerkgerätegruppen

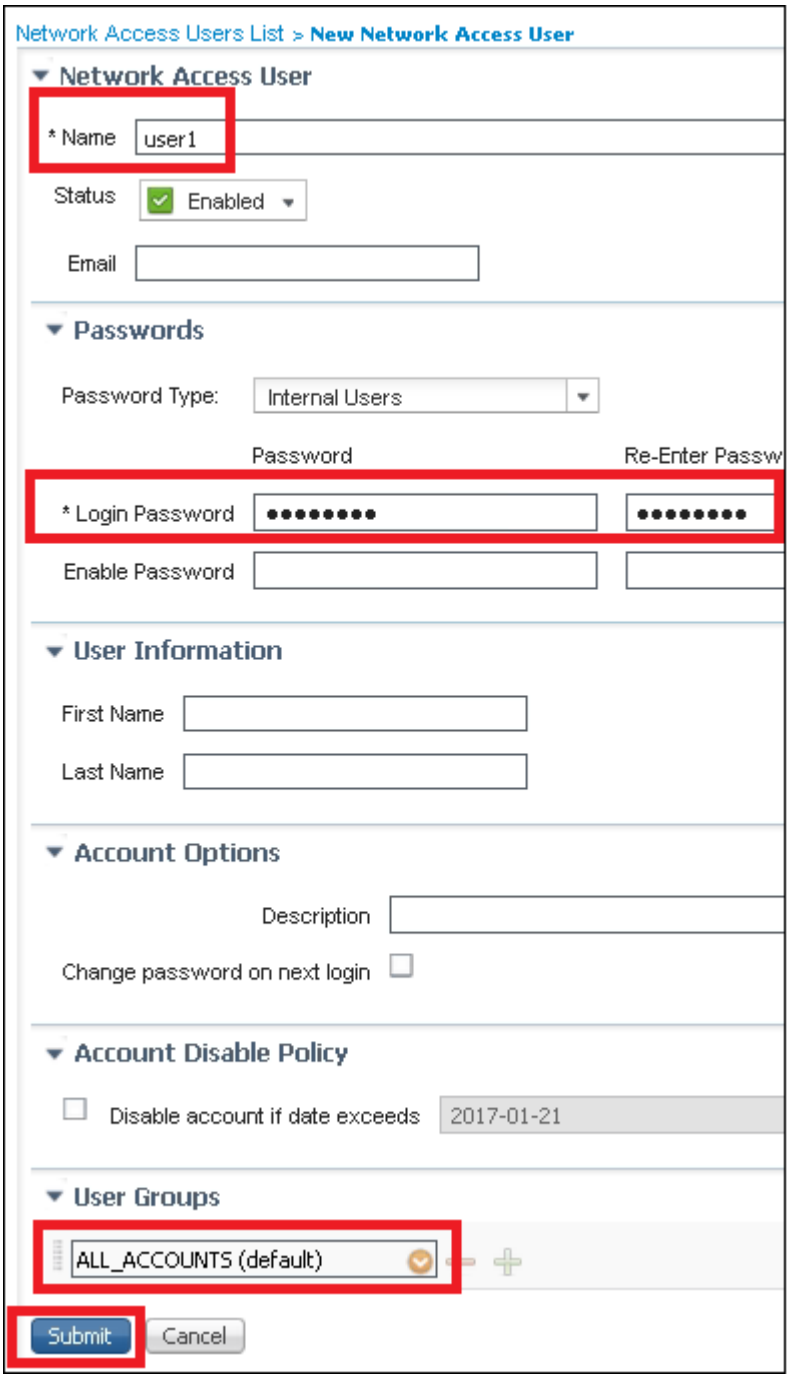
Neuen Benutzer auf ISE erstellen

Schritt 1: Navigieren Sie zu Administration > Identity Management > Identities > Users > Add (Administration > Identitätsmanagement > Identitäten > Benutzer > Hinzufügen), wie in der Abbildung dargestellt.



Schritt 2: Geben Sie die Informationen ein.

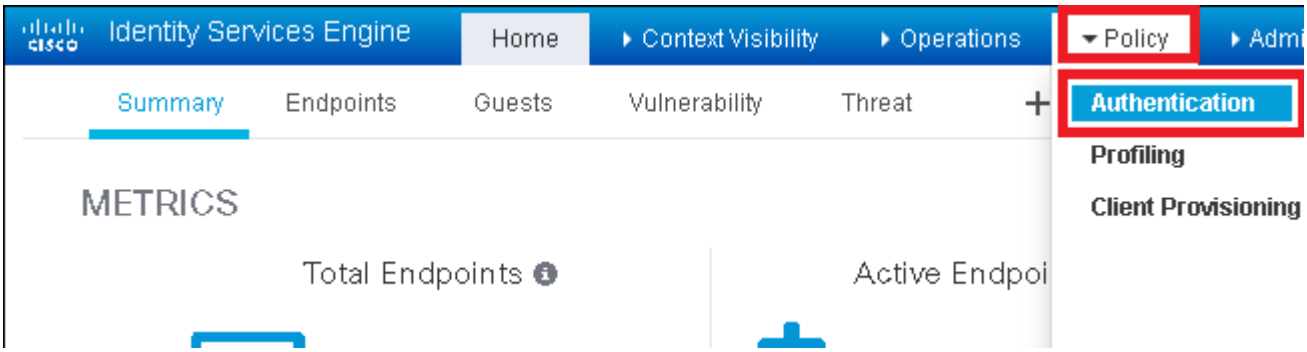
In diesem Beispiel gehört dieser Benutzer zu einer Gruppe mit dem Namen ALL_ACCOUNTS, kann jedoch nach Bedarf angepasst werden, wie im Bild gezeigt.



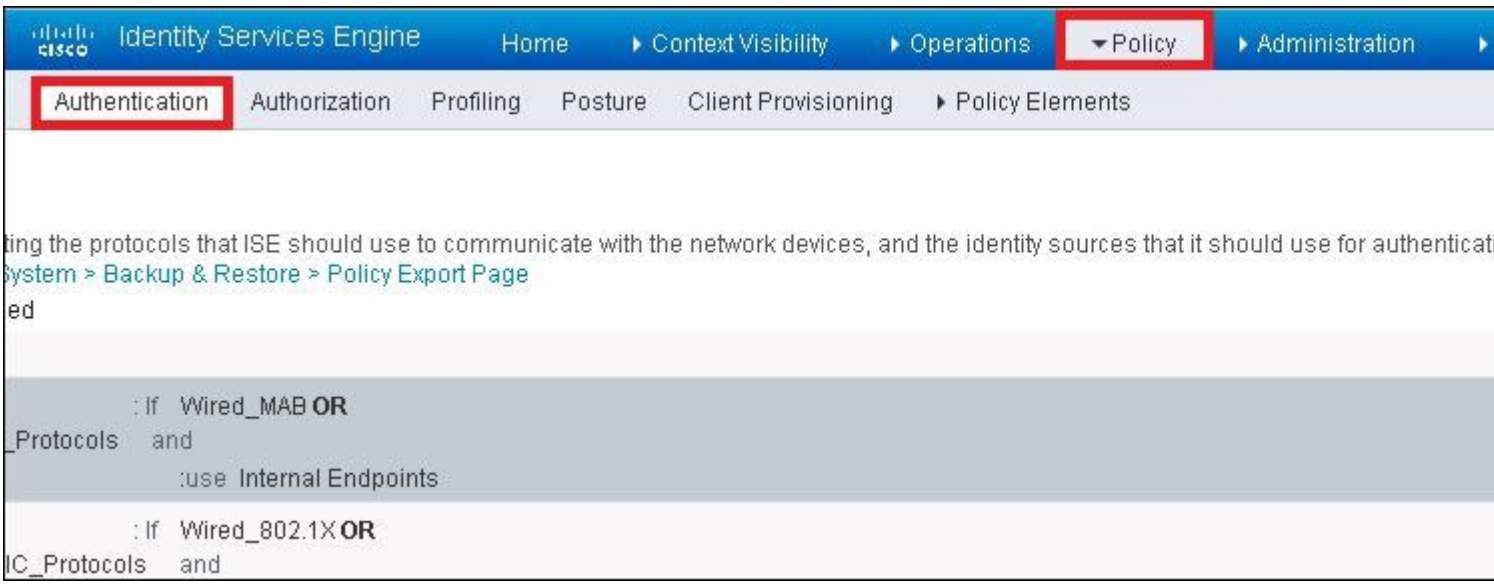
Authentifizierungsregel erstellen

Authentifizierungsregeln werden verwendet, um zu überprüfen, ob die Anmeldeinformationen der Benutzer korrekt sind (überprüfen Sie, ob der Benutzer wirklich der ist, für den er sich ausgibt), und um die Authentifizierungsmethoden einzuschränken, die von ihm verwendet werden dürfen.

Schritt 1: Navigieren Sie zu **Policy > Authentication (Richtlinie > Authentifizierung)**, wie im Bild dargestellt.

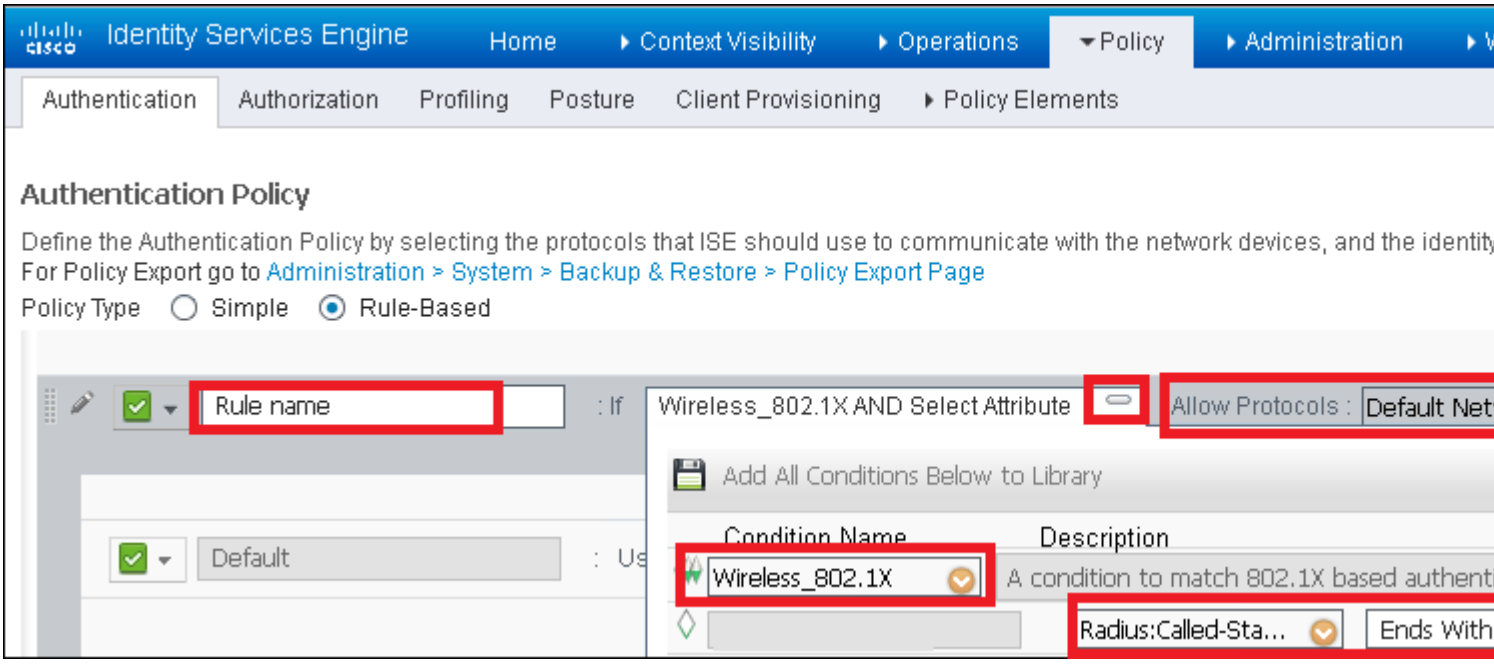


Schritt 2: Fügen Sie eine neue Authentifizierungsregel wie im Bild dargestellt ein.

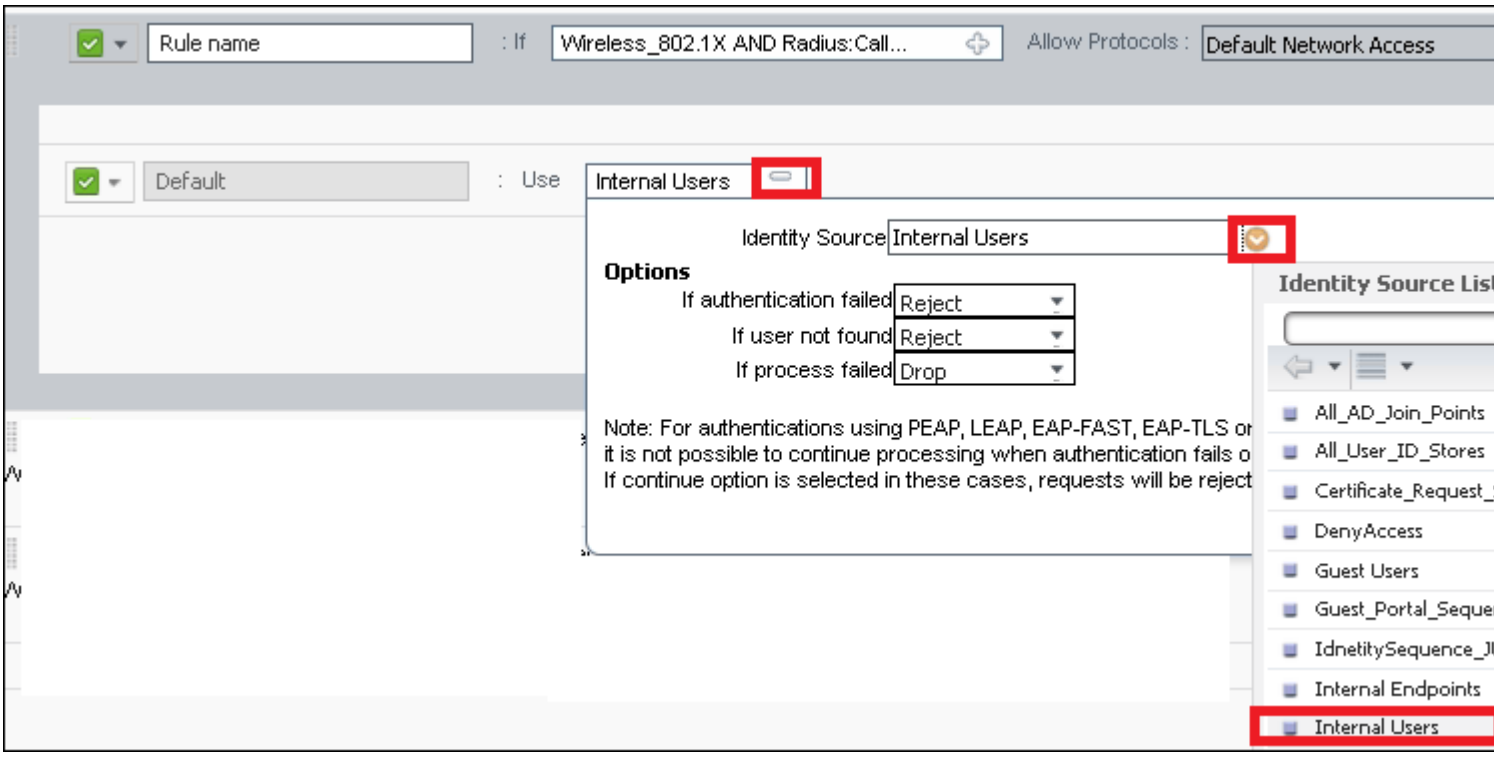


Schritt 3: Geben Sie die Werte ein.

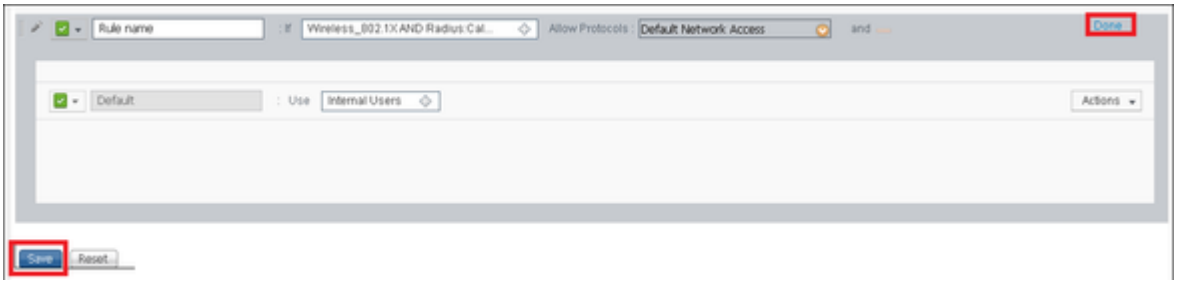
Diese Authentifizierungsregel lässt alle Protokolle zu, die in der Liste "Standard-Netzwerkzugriff" aufgeführt sind. Dies gilt für die Authentifizierungsanforderung für Wireless-802.1x-Clients mit Called-Station-ID und endet mit ise-ssid, wie im Bild gezeigt.



Wählen Sie außerdem die Identitätsquelle für die Clients aus, die dieser Authentifizierungsregel entsprechen. In diesem Beispiel wird die Identitätsquellenliste für interne Benutzer verwendet, wie im Bild dargestellt.



Klicken Sie abschließend auf **Fertig** und **Speichern,** wie im Bild dargestellt.



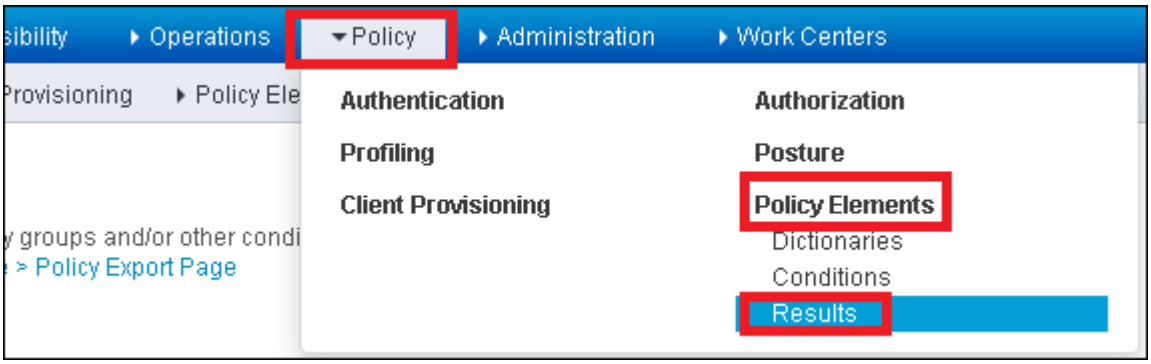
Weitere Informationen zu Identitätsquellen finden Sie unter diesem Link:

Benutzeridentitätsgruppe erstellen

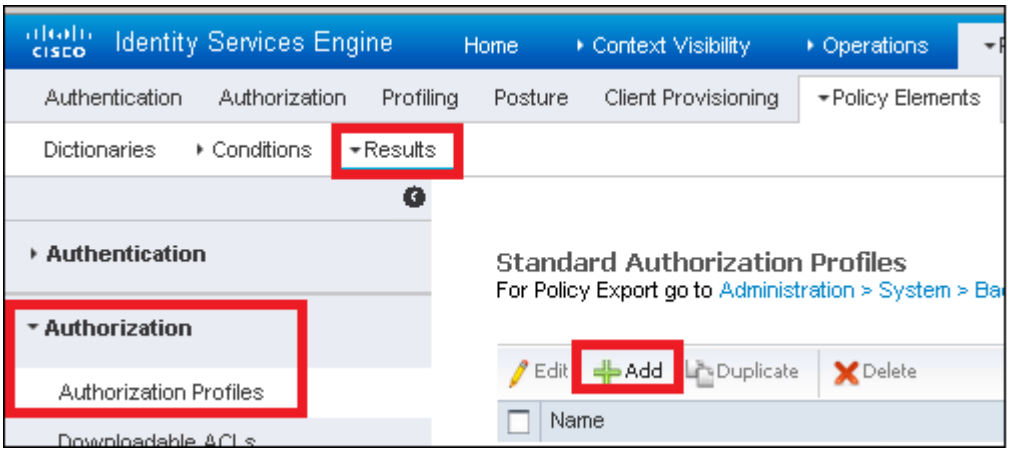
Erstellen des Autorisierungsprofils

Das Autorisierungsprofil bestimmt, ob Sie Zugriff auf das Netzwerk haben. Push-Zugriffskontrolllisten (ACLs), VLAN-Übersteuerung oder andere Parameter. Das in diesem Beispiel gezeigte Autorisierungsprofil sendet eine Bestätigung für den Zugang an Sie und weist VLAN 2404 zu.

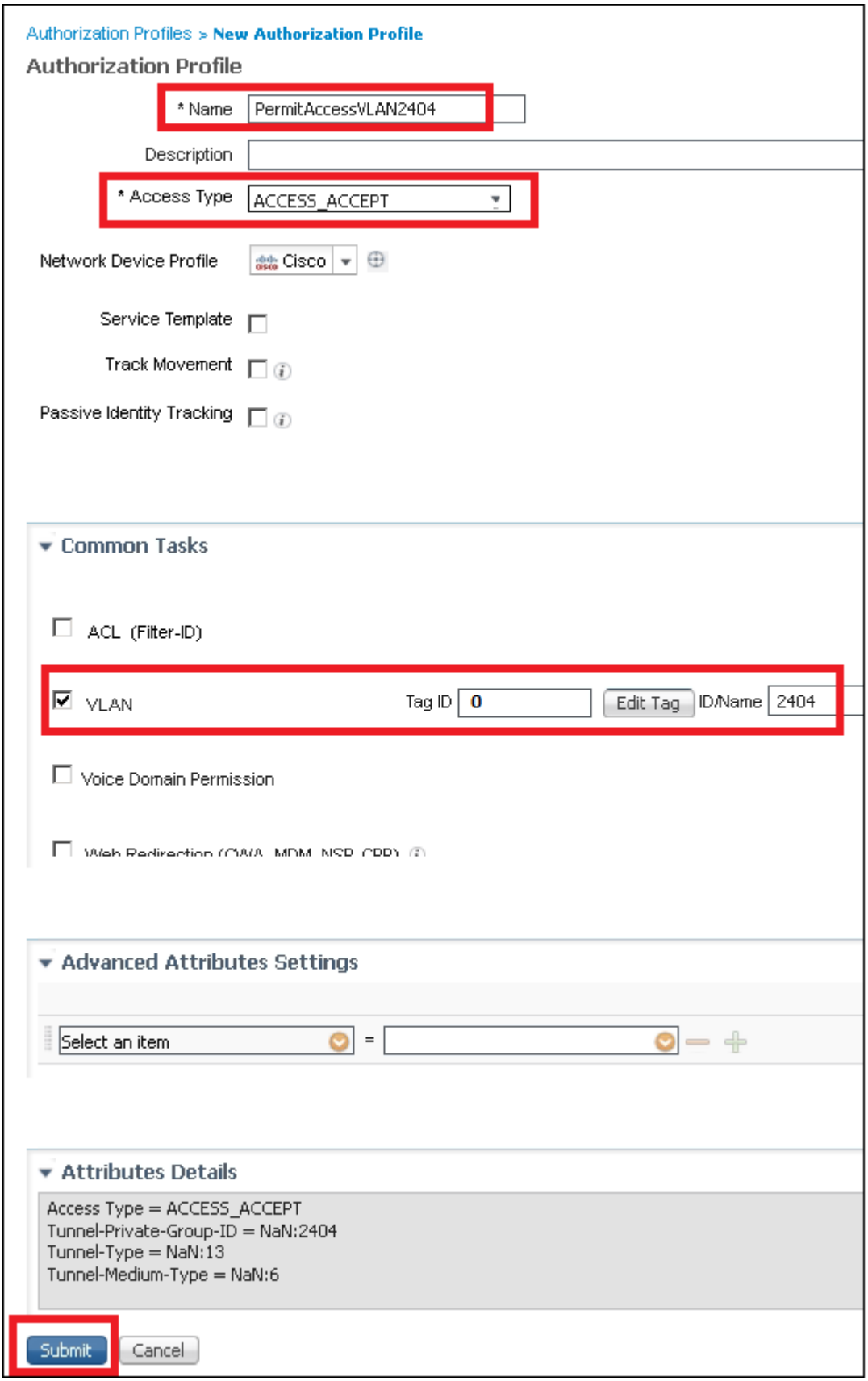
Schritt 1: Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse**, wie im Bild dargestellt.



Schritt 2: Hinzufügen eines neuen Autorisierungsprofils Navigieren Sie zu **Autorisierung > Autorisierungsprofile > Hinzufügen,** wie im Bild dargestellt.



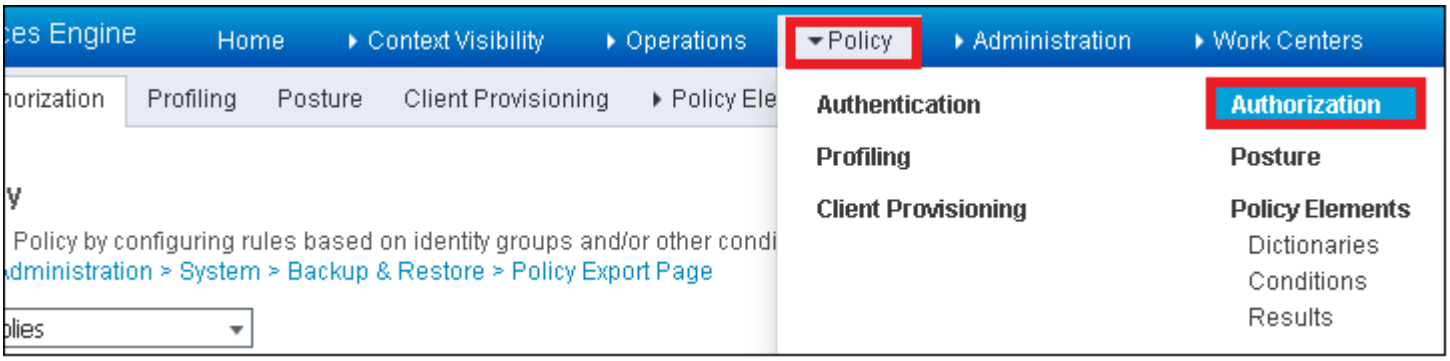
Schritt 3: Geben Sie die im Bild angezeigten Werte ein.



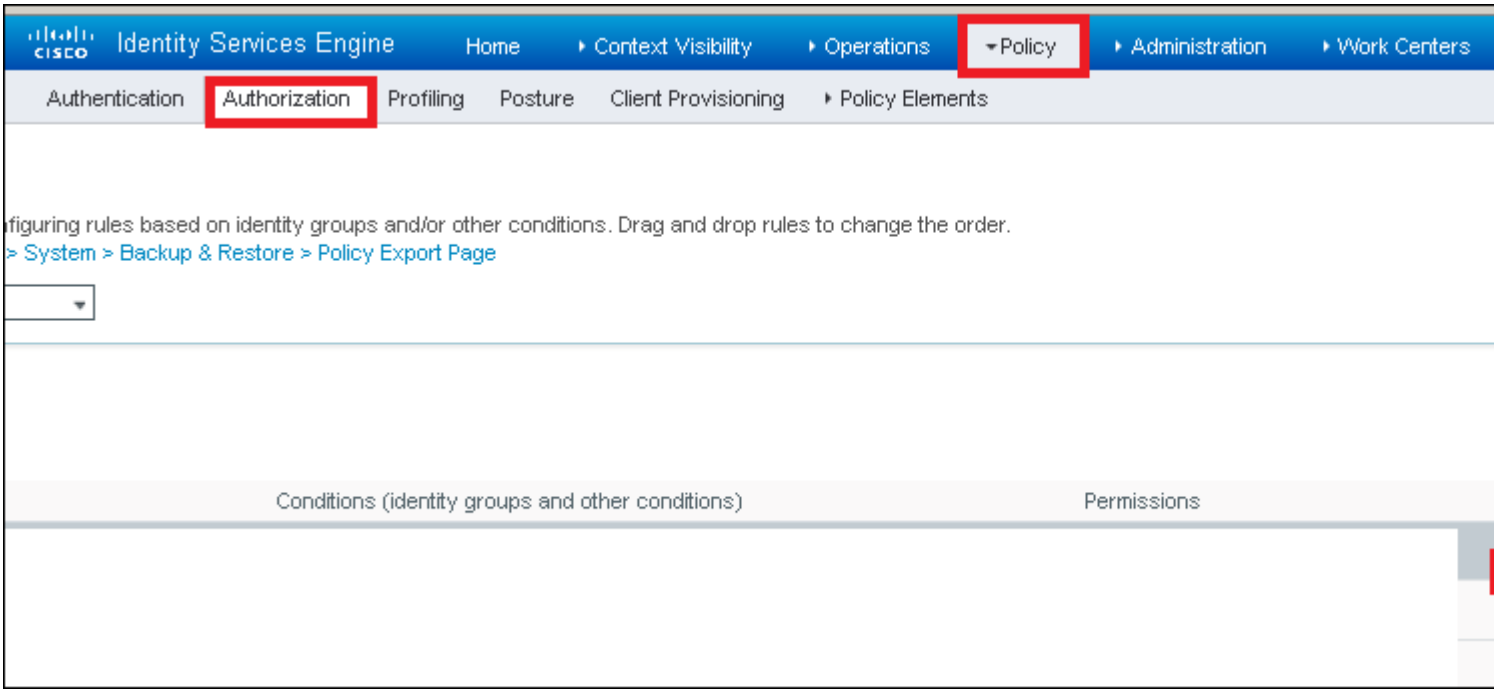
Autorisierungsregel erstellen

Die Autorisierungsregel bestimmt, welche Berechtigungen (welches Autorisierungsprofil) auf Sie angewendet werden.

Schritt 1: Navigieren Sie zu **Policy > Authorization (Richtlinie > Autorisierung)**, wie im Bild dargestellt.

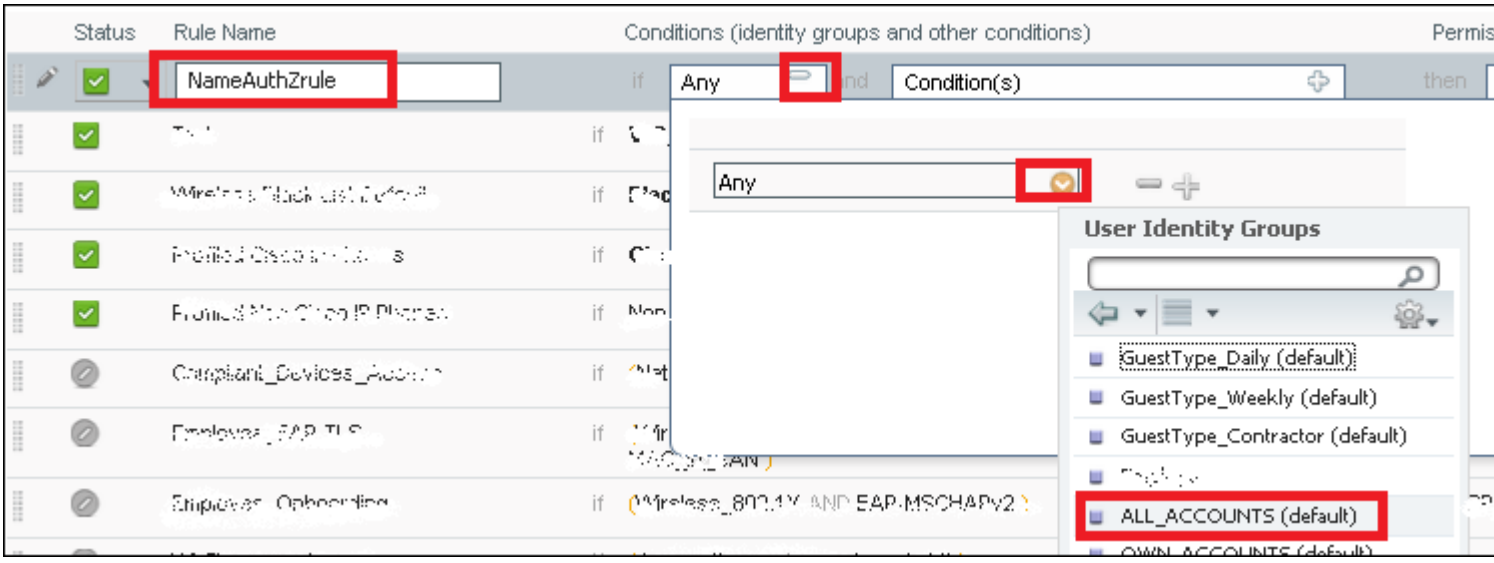


Schritt 2: Fügt eine neue Regel wie im Bild dargestellt ein.

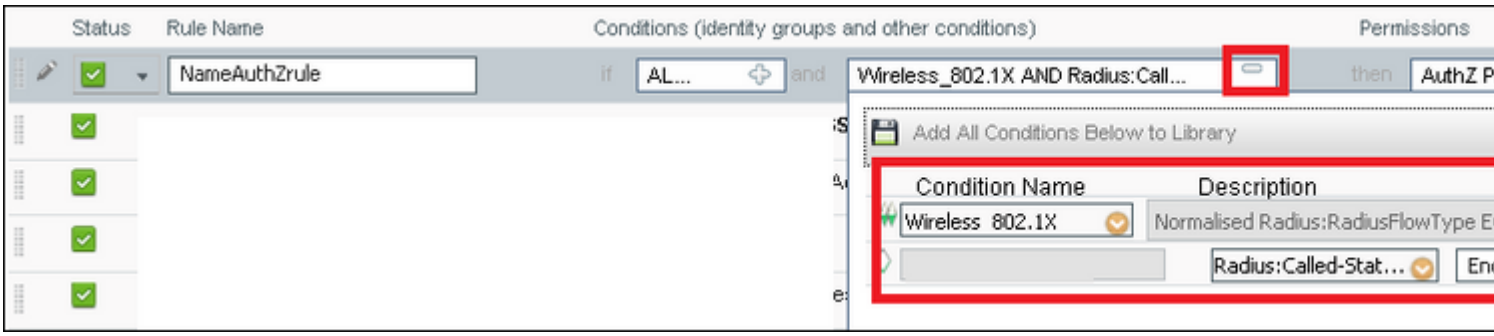


Schritt 3: Geben Sie die Werte ein.

Wählen Sie zunächst einen Namen für die Regel und die Identitätsgruppe aus, in der der Benutzer gespeichert ist (ALL_ACCOUNTS), wie im Bild gezeigt.



Wählen Sie anschließend andere Bedingungen aus, die dazu führen, dass der Autorisierungsprozess in diese Regel fällt. In diesem Beispiel trifft der Autorisierungsprozess diese Regel, wenn er 802.1x Wireless verwendet und die angerufene Stations-ID mit ise-ssid endet, wie im Bild gezeigt.



Wählen Sie abschließend das Autorisierungsprofil aus, das Ihnen zugewiesen ist und auf diese Regel trifft. Klicken Sie auf **Fertig** und **Speichern**, wie im Bild dargestellt.

Konfiguration des Endgeräts

Konfigurieren Sie einen Windows 10-Laptop-Computer für die Verbindung mit einer SSID mit 802.1x-Authentifizierung und PEAP/MS-CHAPv2 (Microsoft-Version des Challenge-Handshake-Authentifizierungsprotokolls) Version 2.

In diesem Konfigurationsbeispiel verwendet die ISE ein selbstsigniertes Zertifikat für die Authentifizierung.

Um das WLAN-Profil auf dem Windows-Computer zu erstellen, gibt es zwei Optionen:

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

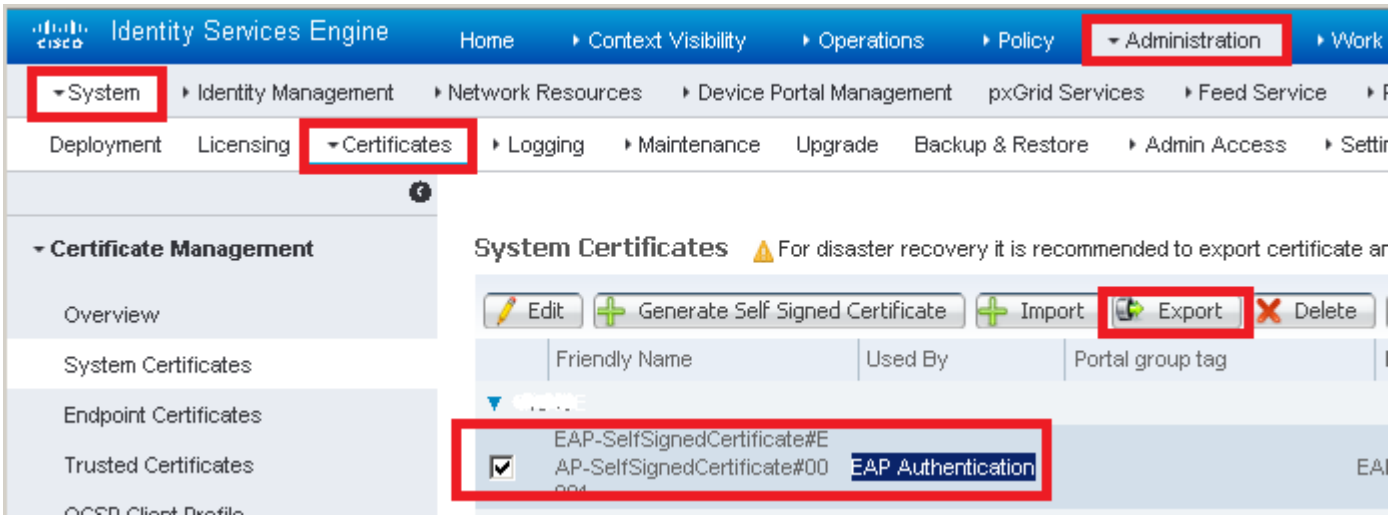
Die Konfiguration dieser Optionen wird unter Endgerätekonfiguration - Erstellen des WLAN-Profils - Schritt 7 erläutert.

Endgerätekonfiguration - ISE-selbstsigniertes Zertifikat installieren

Schritt 1: Selbstsigniertes Zertifikat exportieren

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

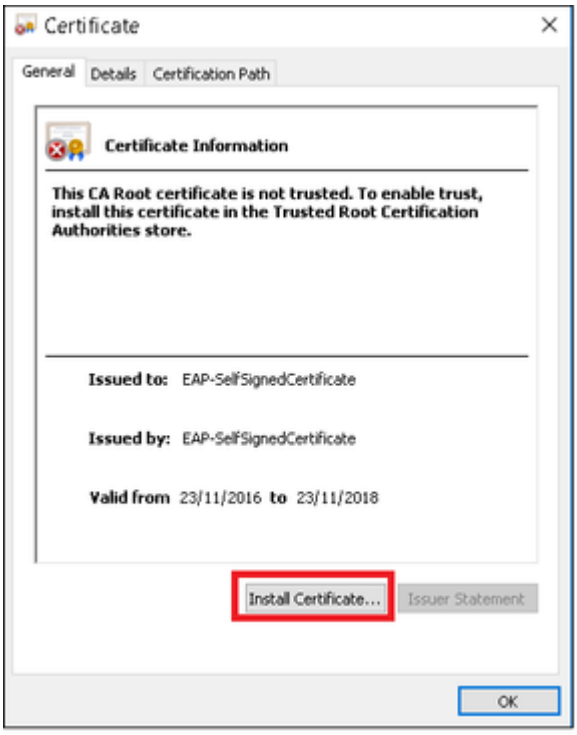
Wählen Sie dann das für die **EAP-Authentifizierung** verwendete Zertifikat aus, und klicken Sie wie im Bild dargestellt auf **Exportieren**.



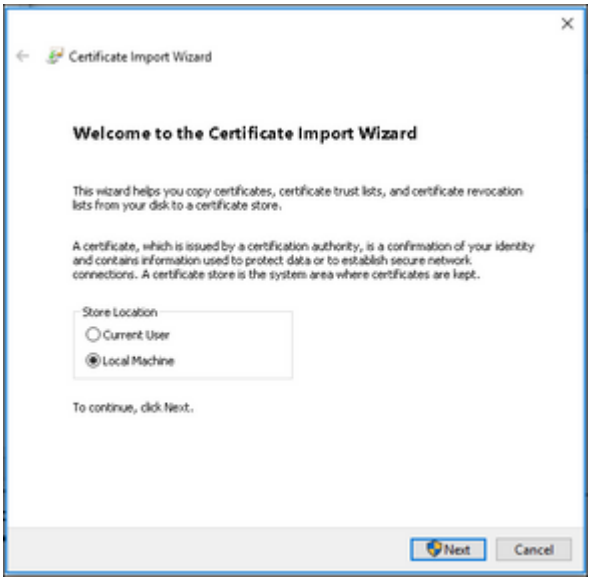
Speichern Sie das Zertifikat am erforderlichen Speicherort. Dieses Zertifikat muss auf dem Windows-Computer installiert werden, wie im Bild dargestellt.

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

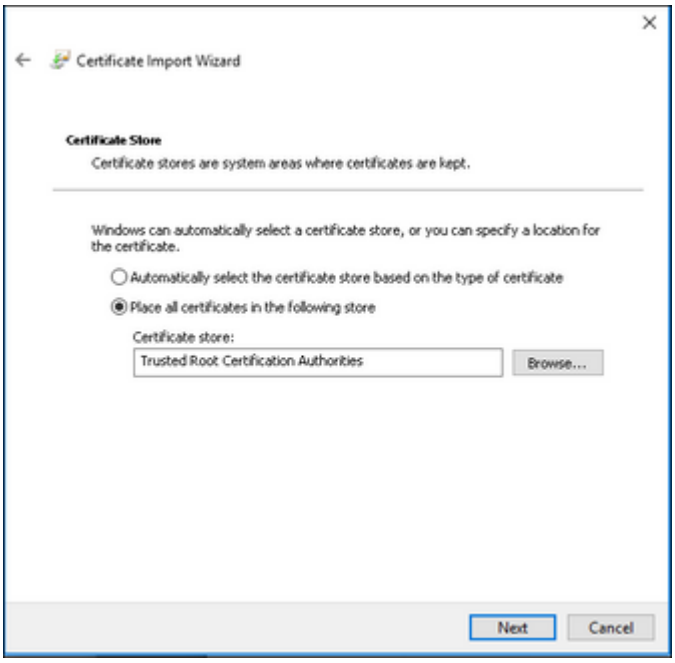
Kopieren Sie das von ISE exportierte Zertifikat in den Windows-Computer, ändern Sie die Dateierweiterung von .pem in .crt, und doppelklicken Sie danach, um sie wie im Bild gezeigt zu installieren.



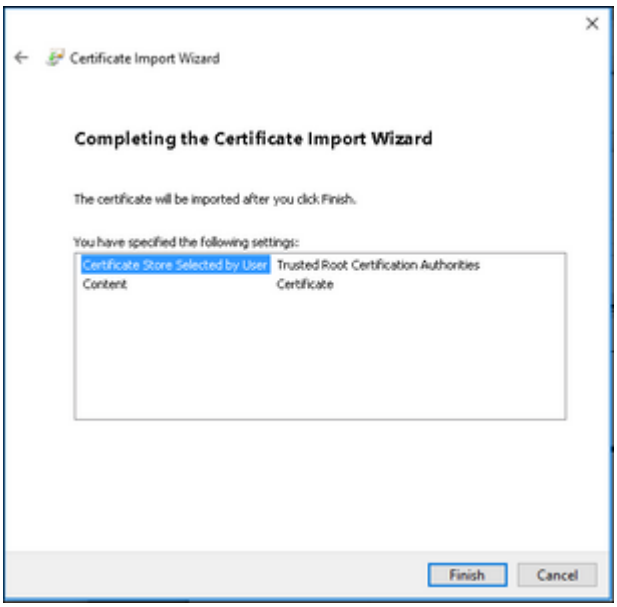
Schritt 3: Wählen Sie Install it in **Local Machine (Lokaler Computer**) aus, und klicken Sie auf **Next (Weiter**), wie im Bild dargestellt.



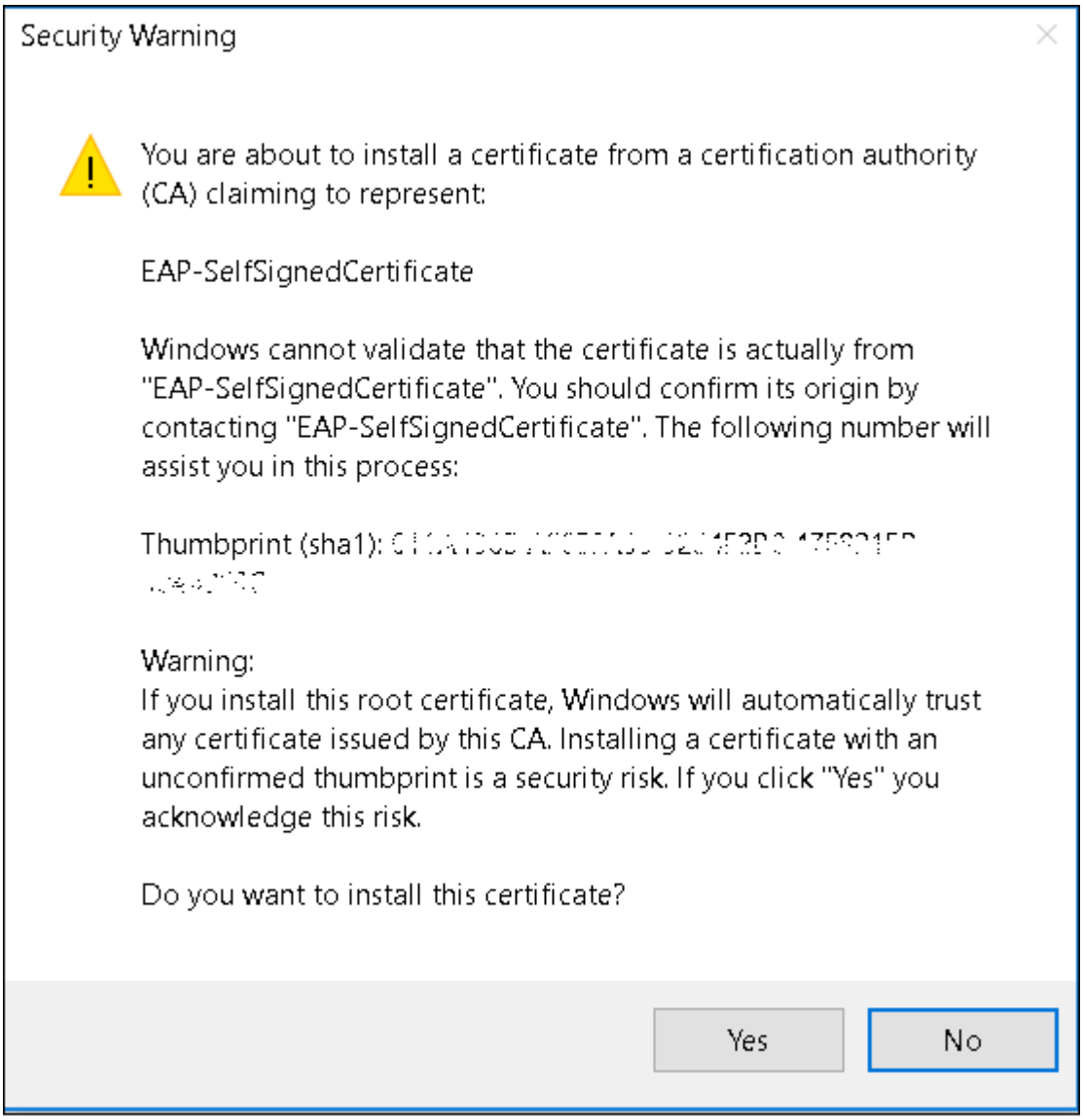
Schritt 4: Wählen Sie **Alle Zertifikate in diesem Speicher platzieren,** dann die Option **Vertrauenswürdige Stammzertifizierungsstellen** durchsuchen und auswählen**.** Klicken Sie anschließend auf **Weiter**, wie im Bild gezeigt.



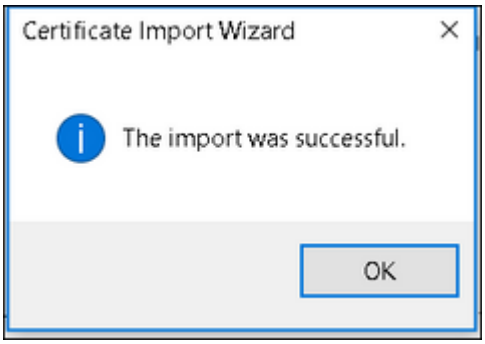
Schritt 5: Klicken Sie dann auf **Fertig stellen**, wie im Bild dargestellt.



Schritt 6: Bestätigen Sie die Installation des Zertifikats. Klicken Sie wie in der Abbildung dargestellt auf **Ja**.

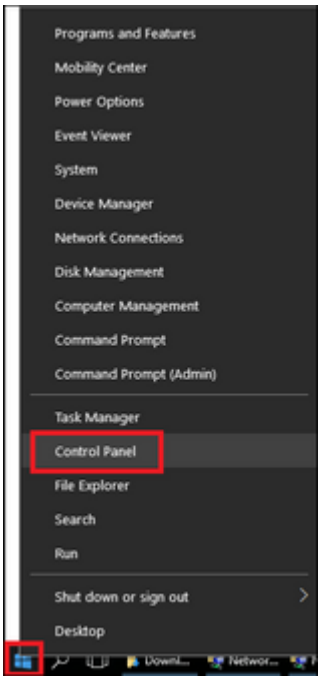


Schritt 7. Klicken Sie abschließend auf **OK**, wie im Bild gezeigt.

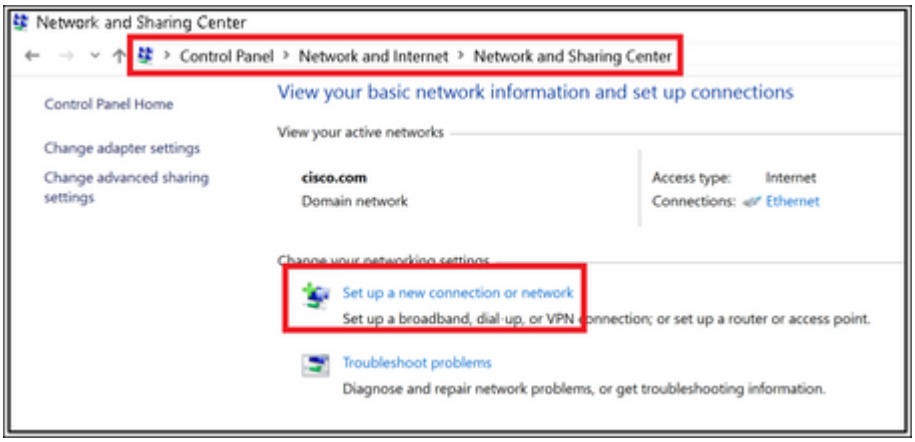


Endgerätekonfiguration - Erstellen Sie das WLAN-Profil.

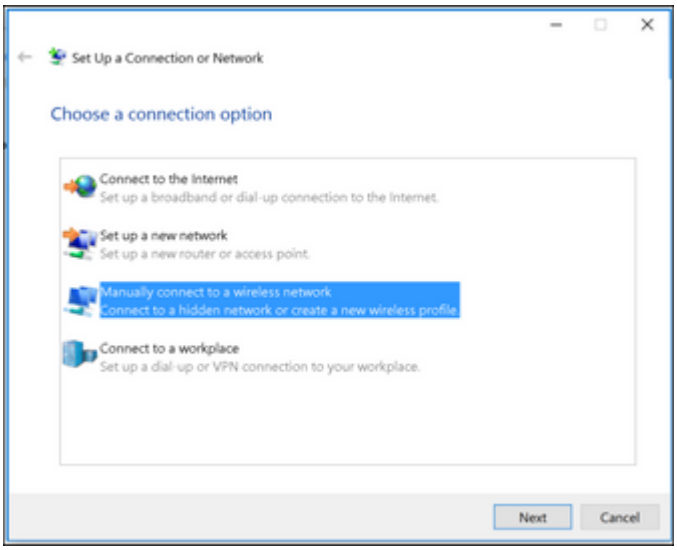
Schritt 1: Klicken Sie mit der rechten Maustaste auf das Symbol **Start**, und wählen Sie **Systemsteuerung** wie im Bild dargestellt aus.



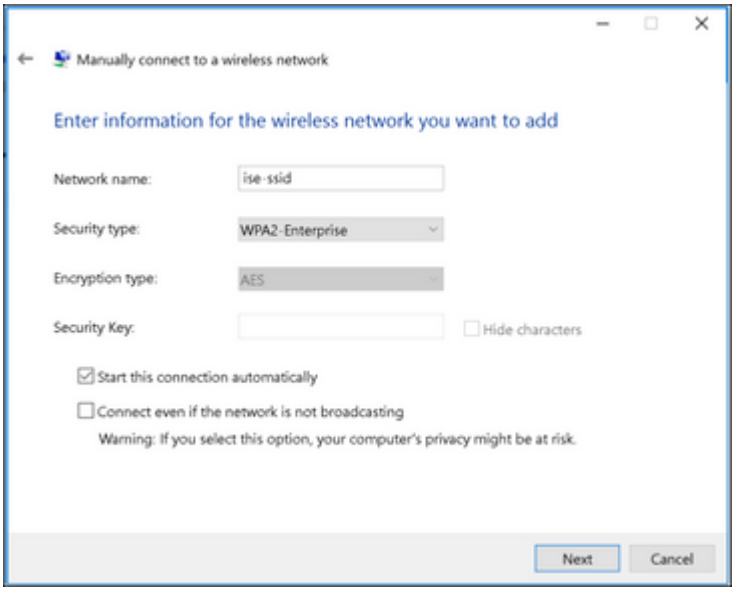
Schritt 2: Navigieren Sie zu **Netzwerk und Internet**, navigieren Sie anschließend zum **Netzwerk- und Freigabecenter,** und klicken Sie auf **Neue Verbindung oder neues Netzwerk einrichten,** wie im Bild dargestellt.



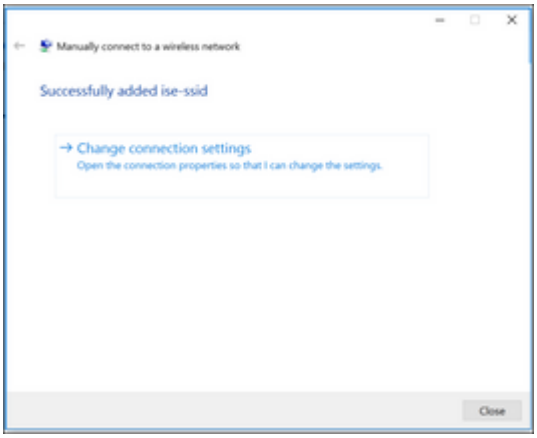
Schritt 3: Wählen Sie **Manuell mit einem Wireless-Netzwerk verbinden aus**, und klicken Sie auf **Weiter,** wie im Bild gezeigt.



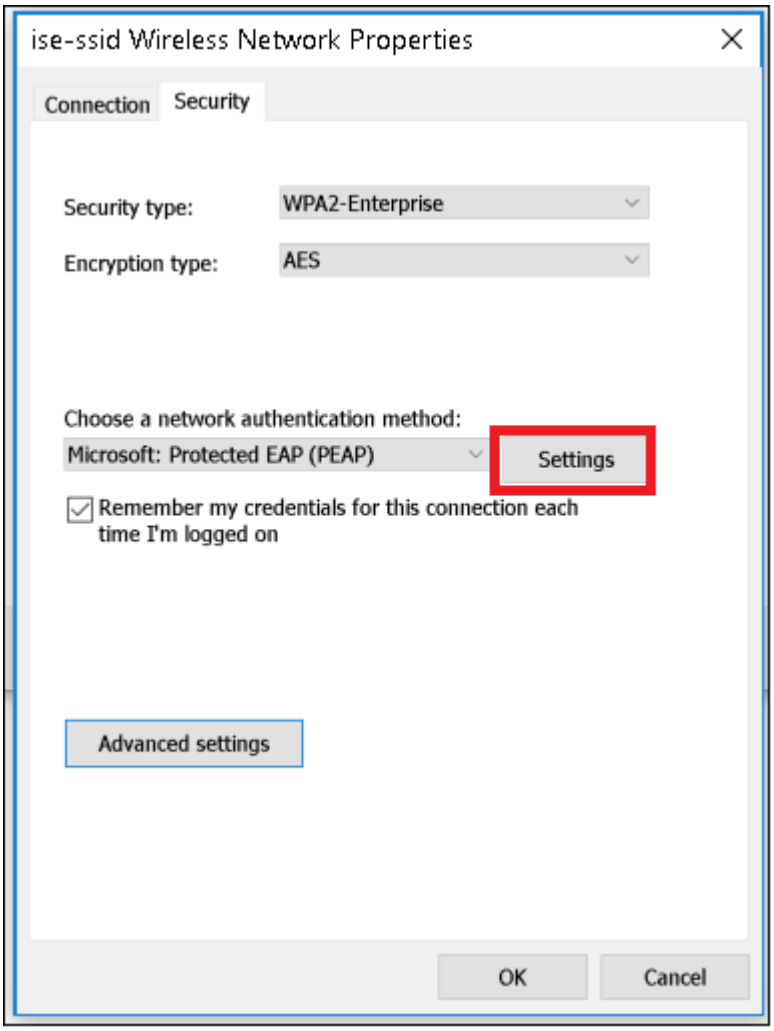
Schritt 4: Geben Sie die Informationen mit dem Namen der SSID und dem Sicherheitstyp WPA2-Enterprise ein, und klicken Sie auf **Weiter**, wie im Bild dargestellt.



Schritt 5: Wählen Sie **Verbindungseinstellungen ändern** aus, um die Konfiguration des WLAN-Profils wie im Bild dargestellt anzupassen.



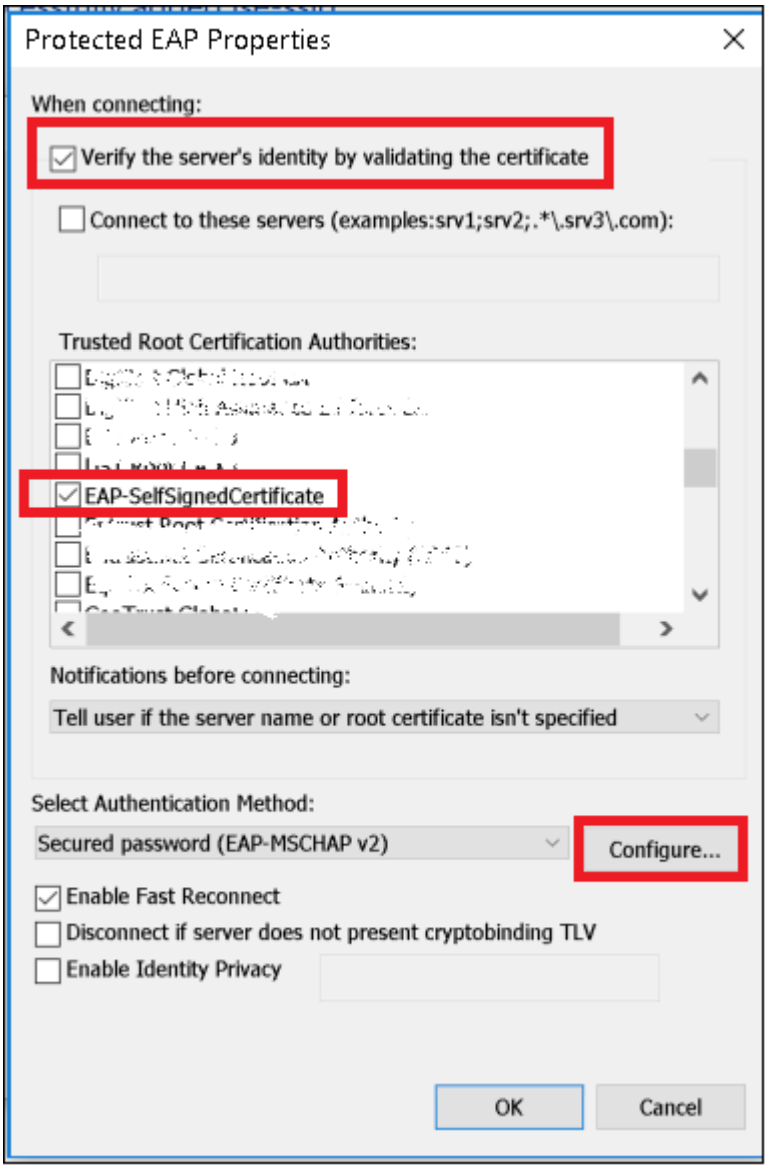
Schritt 6: Navigieren Sie zur Registerkarte **Sicherheit**, und klicken Sie auf **Einstellungen**, wie im Bild dargestellt.

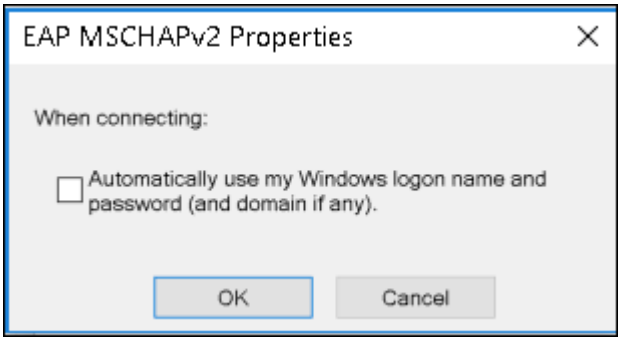


Schritt 7. Wählen Sie aus, ob der RADIUS-Server validiert ist oder nicht.

Wenn ja, aktivieren Sie **Überprüfen der Serveridentität durch Validieren des Zertifikats** und von **Trusted Root Certification Authorities:** list wählen Sie das selbstsignierte Zertifikat von ISE aus.

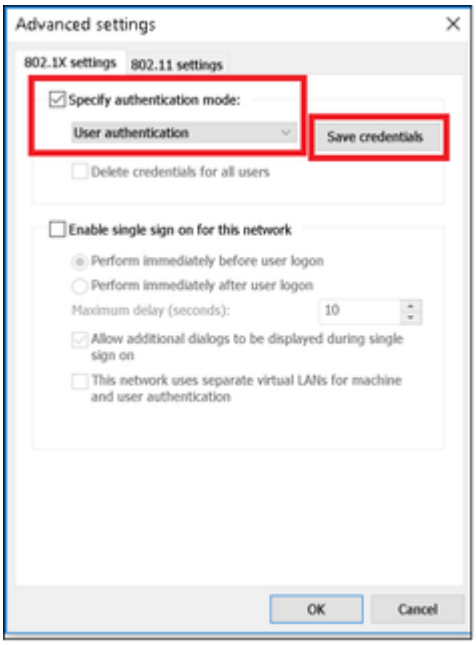
Wählen Sie anschließend **Konfigurieren** und Deaktivieren **Automatisch meinen Windows-Anmeldenamen und mein Kennwort verwenden...**, und klicken Sie dann auf **OK,** wie in den Bildern dargestellt.

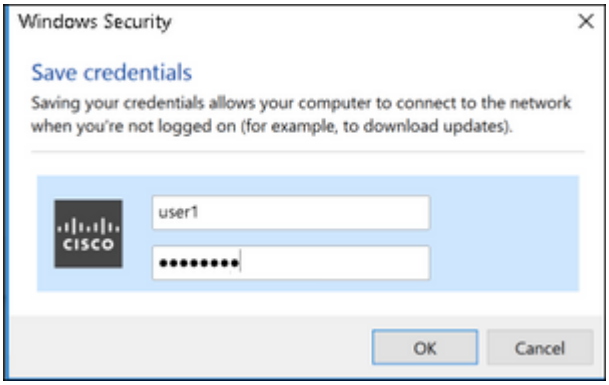




Schritt 8: Konfigurieren Sie die Anmeldeinformationen des Benutzers.

Wenn Sie wieder zur Registerkarte **Sicherheit** zurückkehren, wählen Sie **Erweiterte Einstellungen aus,** geben Sie den Authentifizierungsmodus als Benutzerauthentifizierung an, und **speichern Sie** die auf der ISE konfigurierten Anmeldeinformationen, um den Benutzer wie in den Abbildern dargestellt zu authentifizieren.





Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Der Authentifizierungsfluss kann aus WLC- oder ISE-Sicht verifiziert werden.

Authentifizierungsprozess auf WLC

Führen Sie die folgenden Befehle aus, um den Authentifizierungsprozess für einen bestimmten Benutzer zu überwachen:

```
> debug client <mac-add-client>
> debug dot1x event enable
> debug dot1x aaa enable
```

Beispiel für eine erfolgreiche Authentifizierung (einige Ausgaben wurden ausgelassen):

<#root>

```
*apfMsConnTask_1: Nov 24 04:30:44.317:

e4:b3:18:7c:30:58 Processing assoc-req station:e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00

 thread:1a5cc288
*apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00:
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobile
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for st
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities:  60
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as non-

e4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication

11w Capable
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b3
*apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID:  (16)
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mob
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache fo
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Nov 24 04:30:44.319:

e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rul
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf_policy.c:437) Changing stat
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b3
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId:
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session T
*apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:c
*spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 0
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Received ADD_MOBILE ack - Initiating 1x to STA e4:b
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58

Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth_sm state transition 0 ---> 1 for mobi
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326:
```

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authenti
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) for
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ===> 215 f
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:7
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) for
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
.
.
.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 acl from 255 to 255
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex acl from 65535 to 65
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:
```

e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name received: vlan2404

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intgr
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over P
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:
```

e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

```
        MAC: e4:b3:18:7c:30:58, source 4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overrid
*Dot1x_NW_MsgTask_0: Nov 24
```

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name receive

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobil
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got fr
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x reau
```

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for station
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for station
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:2c:d1 to PMKID cach
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for static
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can tak
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:30
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is do
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26:2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: Including PMKID in M1  (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0016] cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:
```

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:
```

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

```
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authenticatin
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 into
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL-
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTK_START state (message 2) from mobile

```
 e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key c
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for re
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL-
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

```
 from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Bufer for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

```
e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vlan Ip: 172.16.0.134, Vlan mask
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Virtual Ip: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LW
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:

e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677,
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255, IPv
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed m
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mob
*spamApTask2: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 0
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update reque
  Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobility
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Add
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
  IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobil
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 wh
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:

e4:b3:18:7c:30:58 172.16.0.151 DHCP_REQD (7) Change state to RUN (20)

 last state DHCP_REQD (7)
```

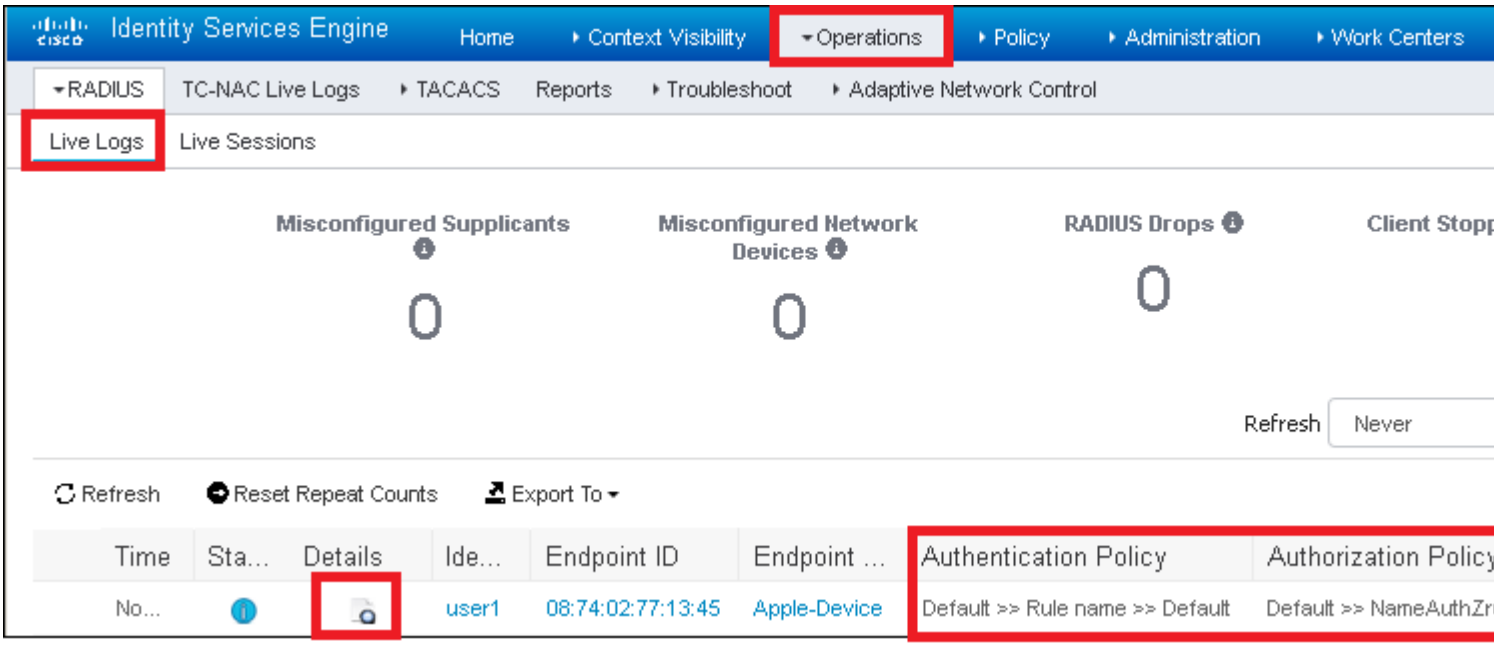
Eine einfache Möglichkeit zum Lesen von Debug-Client-Ausgaben bietet das Wireless Debug Analyzer-Tool:

Wireless-Debug-Analyzer

Authentifizierungsprozess auf der ISE

Navigieren Sie zu **Operations > RADIUS > Live Logs**, um festzustellen, welche Authentifizierungsrichtlinie, Autorisierungsrichtlinie und welches Autorisierungsprofil dem Benutzer zugewiesen wurde.

Für weitere Informationen klicken Sie auf **Details**, um einen detaillierteren Authentifizierungsprozess anzuzeigen, wie im Bild dargestellt.



Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

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.