Konfigurieren von EAP-TLS auf dem 9800 WLC mit interner ISE-Zertifizierungsstelle

Inhalt

Einleitung

In diesem Dokument wird die EAP-TLS-Authentifizierung mithilfe der Certificate Authority of

Identity Services Engine zur Benutzerauthentifizierung beschrieben.

Voraussetzungen

Verwendete Komponenten

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

- Wireless-Controller: C9800-40-K9 mit 17.09.04a
- Cisco ISE: Ausführung von Version 3 Patch 4
- AP-Modell: C9130AXI-D
- Switch: 9200-L-24P

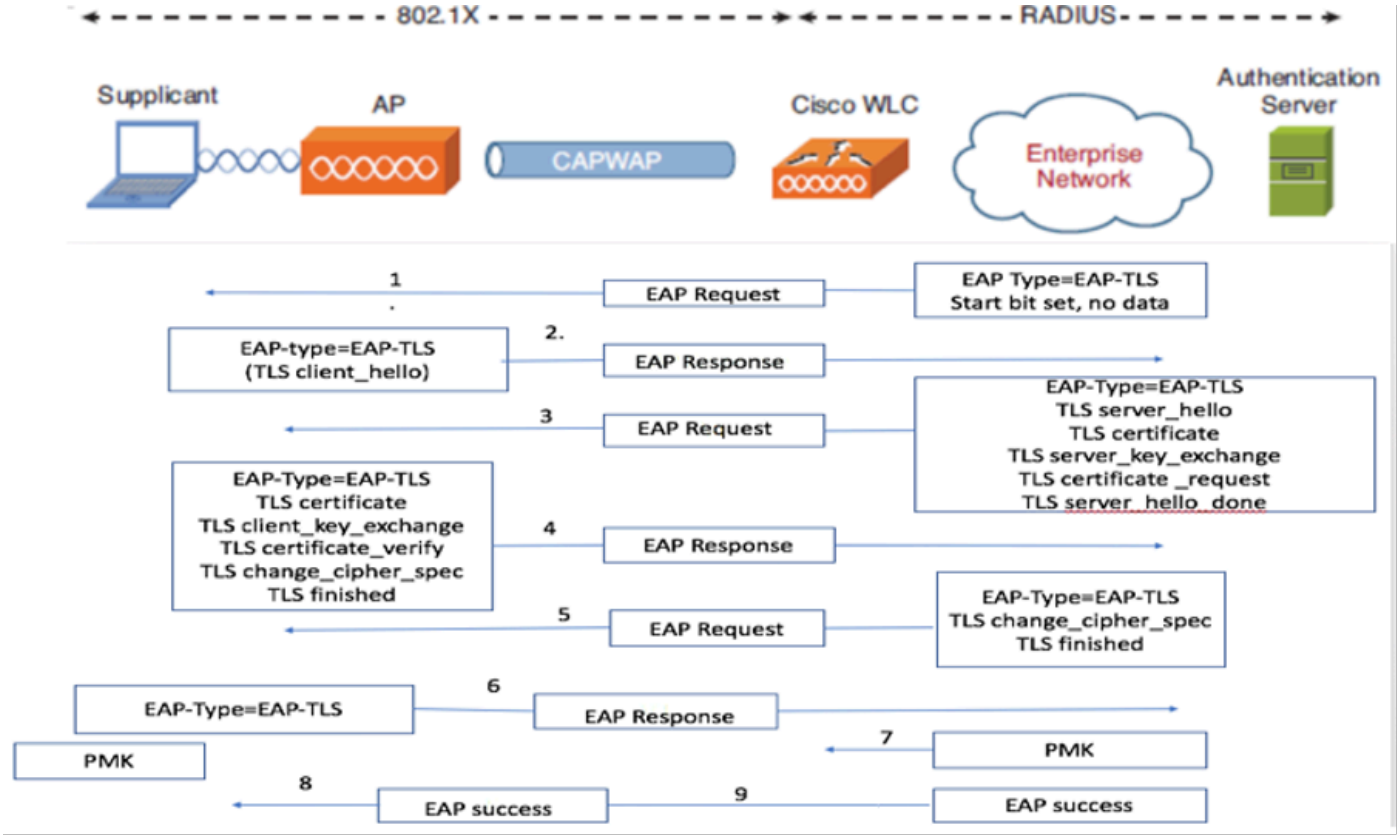
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Hintergrundinformationen

Die meisten Unternehmen verfügen über eine eigene Zertifizierungsstelle, die Endbenutzern Zertifikate für die EAP-TLS-Authentifizierung ausstellt. Die ISE umfasst eine integrierte Zertifizierungsstelle, mit der Zertifikate für Benutzer generiert werden können, die für die EAP-TLS-Authentifizierung verwendet werden sollen. In Szenarien, in denen die Verwendung einer vollwertigen Zertifizierungsstelle nicht möglich ist, ist die Verwendung der ISE-Zertifizierungsstelle für die Benutzerauthentifizierung von Vorteil.

In diesem Dokument werden die erforderlichen Konfigurationsschritte für die effektive Nutzung der ISE-CA zur Authentifizierung von Wireless-Benutzern beschrieben. EAP-TLS-Authentifizierungsablauf

EAP-TLS-Authentifizierungsablauf



EAP-TLS-Authentifizierungsablauf

Schritte im EAP-TLS-Fluss

1. Der Wireless-Client wird mit dem Access Point (AP) verknüpft.
2. Zu diesem Zeitpunkt lässt der WAP keine Datenübertragung zu und sendet eine Authentifizierungsanforderung.
3. Der Client antwortet als Supplicant mit einer EAP-Response-Identität.
4. Der Wireless LAN Controller (WLC) leitet die Benutzer-ID-Informationen an den Authentifizierungsserver weiter.
5. Der RADIUS-Server antwortet dem Client mit einem EAP-TLS-Startpaket.
6. Die EAP-TLS-Konversation beginnt an diesem Punkt.
7. Der Client sendet eine EAP-Antwort zurück an den Authentifizierungsserver, einschließlich einer client_hello-Handshake-Nachricht mit einem auf NULL gesetzten Schlüssel.
8. Der Authentifizierungsserver antwortet mit einem Access-Challenge-Paket, das Folgendes enthält:

```
TLS server_hello
Handshake message
Certificate
Server_key_exchange
Certificate request
Server_hello_done
```

9. Der Client antwortet mit einer EAP-Antwortnachricht, die Folgendes enthält:

```
Certificate (for server validation)
Client_key_exchange
Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished
```

10. Nach erfolgreicher Client-Authentifizierung sendet der RADIUS-Server eine Access-Challenge, die Folgendes enthält:

```
Change_cipher_spec
Handshake finished message
```

11. Der Client überprüft den Hash, um den RADIUS-Server zu authentifizieren.

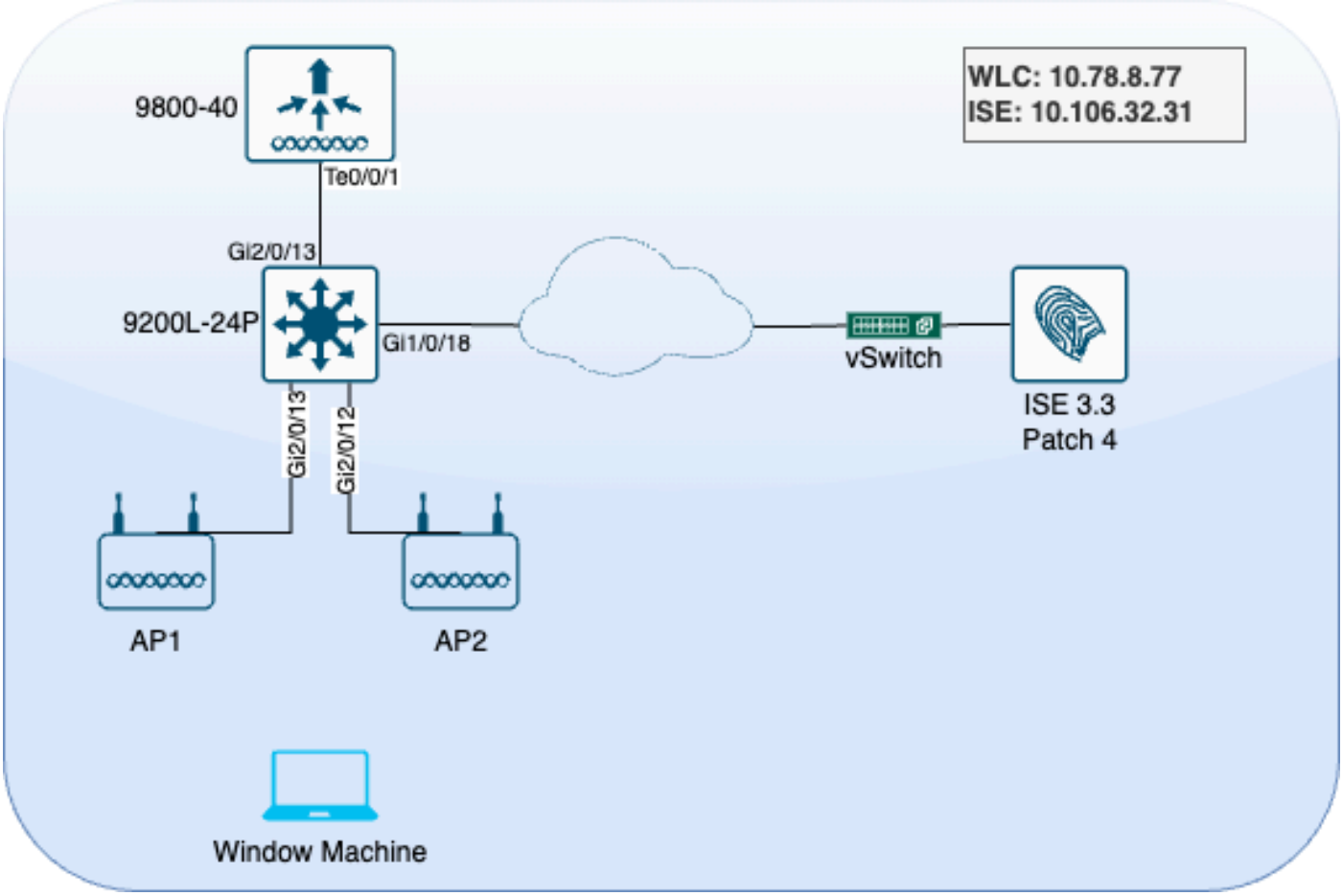
12. Während des TLS-Handshakes wird dynamisch ein neuer Verschlüsselungsschlüssel aus dem Schlüssel abgeleitet.

13. Eine EAP-Erfolgsmeldung wird vom Server an den Authentifikator und dann an den Supplicant gesendet.

14. Der EAP-TLS-fähige Wireless-Client kann jetzt auf das Wireless-Netzwerk zugreifen.

Konfigurieren

Netzwerkdiagramm



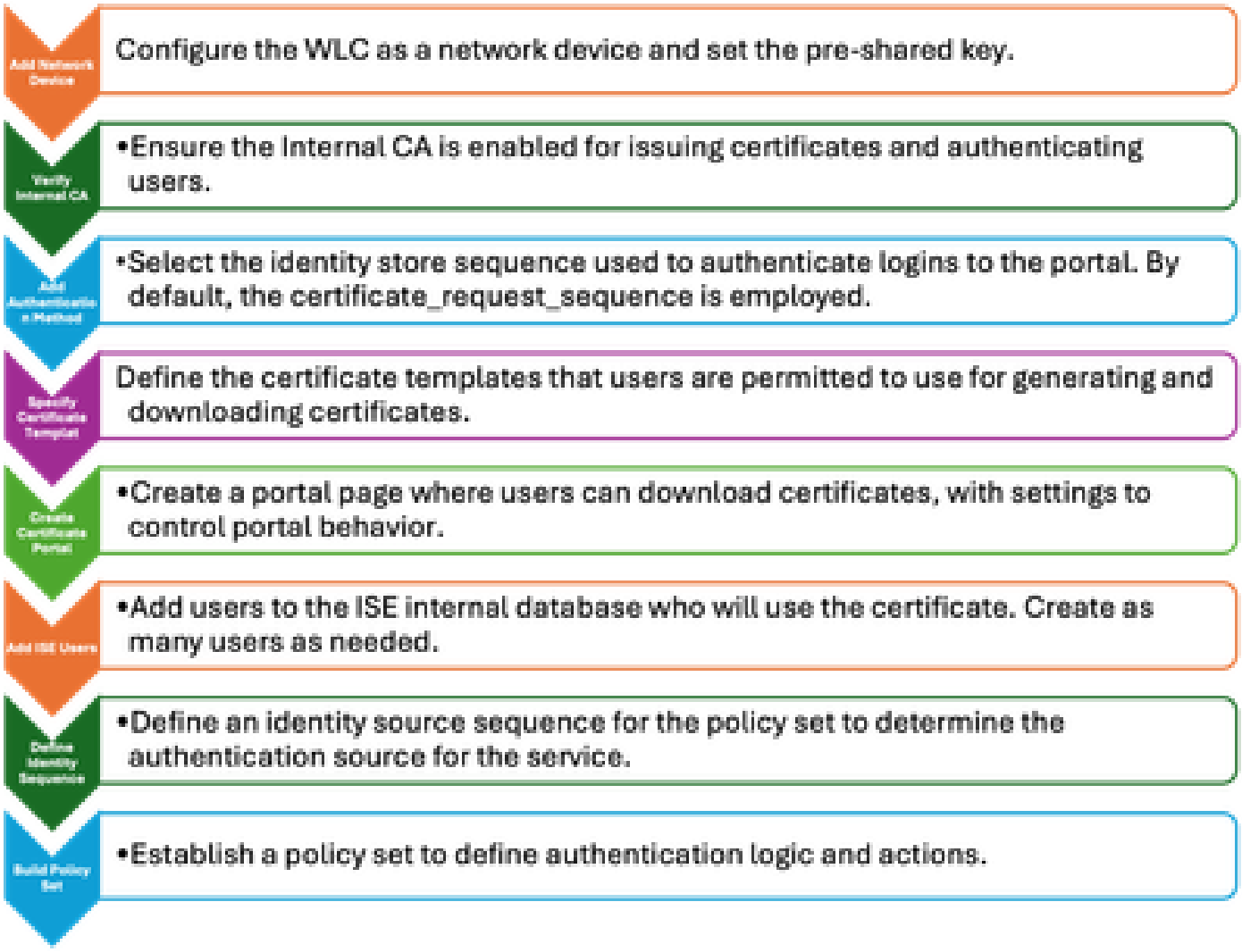
LAB-Topologie

Konfigurationen

In diesem Abschnitt werden zwei Komponenten konfiguriert: ISE und 9800 WLC

ISE-Konfiguration

Hier sind die Konfigurationsschritte für den ISE-Server. Jeder Schritt wird von Screenshots in diesem Abschnitt begleitet, um eine visuelle Orientierung zu bieten.

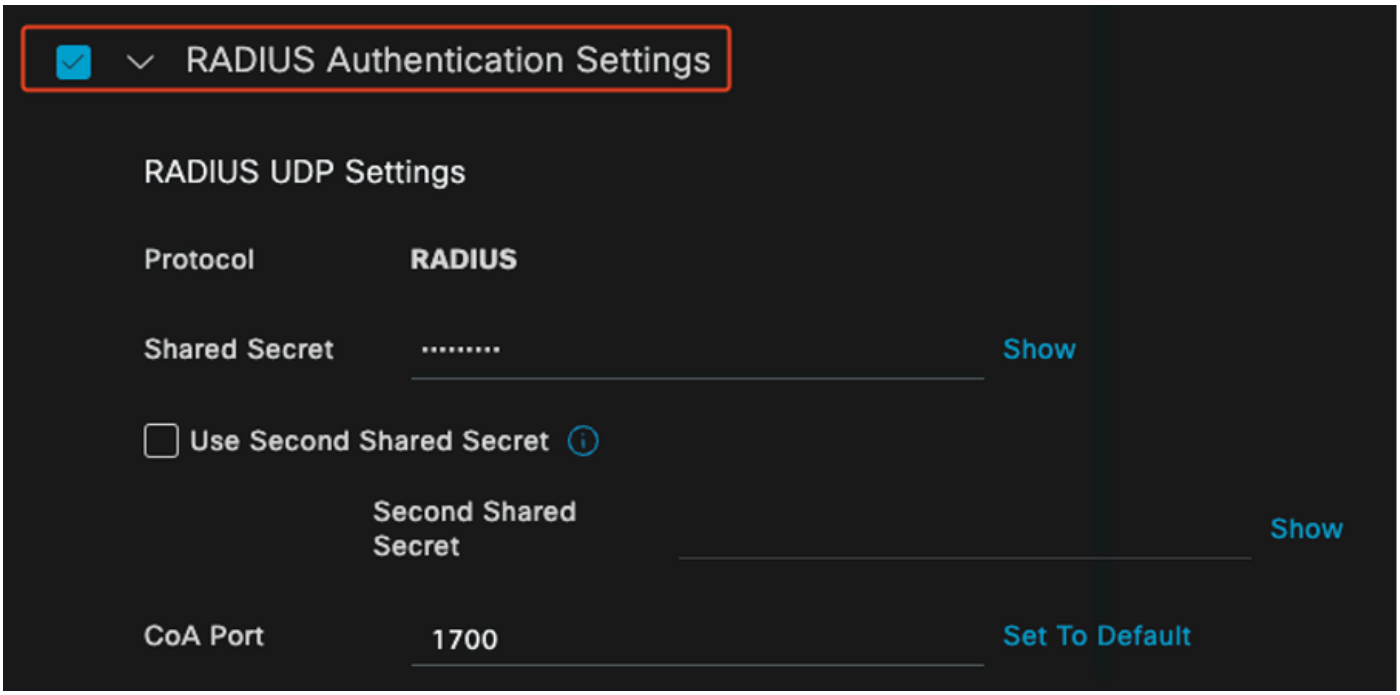


ISE-Serverkonfigurationsschritte

Hinzufügen eines Netzwerkgeräts

Gehen Sie wie folgt vor, um den Wireless LAN Controller (WLC) als Netzwerkgerät hinzuzufügen:

1. Navigieren Sie zu Administration > Network Resources > Network Devices.
2. Klicken Sie auf das Symbol +Hinzufügen, um das Hinzufügen des WLC zu initiieren.
3. Stellen Sie sicher, dass der Pre-Shared Key mit dem WLC- und dem ISE-Server übereinstimmt, um eine ordnungsgemäße Kommunikation zu ermöglichen.
4. Wenn Sie alle Details richtig eingegeben haben, klicken Sie unten links auf Senden, um die Konfiguration zu speichern.

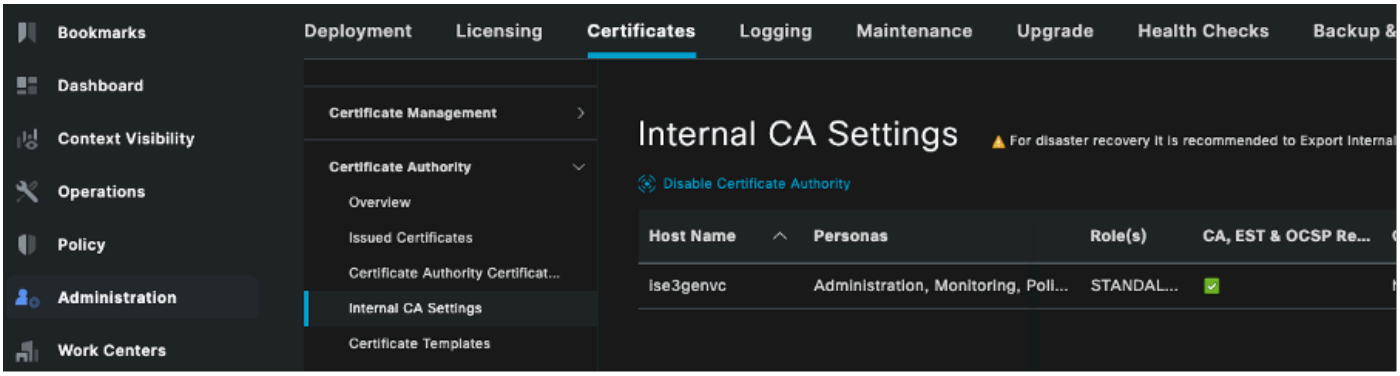


Hinzufügen eines Netzwerkgeräts

Interne Zertifizierungsstelle überprüfen

So überprüfen Sie die Einstellungen der internen Zertifizierungsstelle:

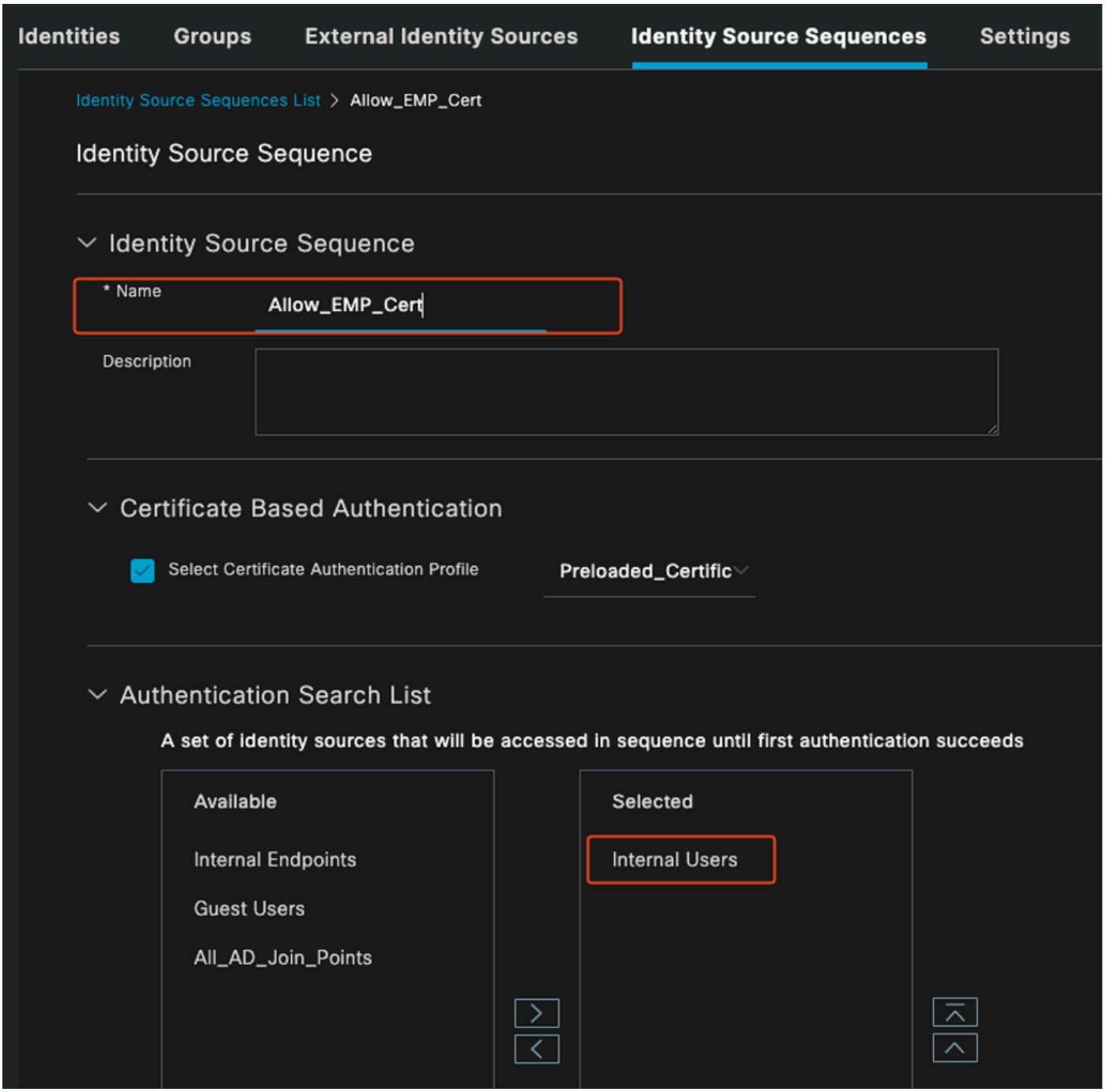
1. Gehen Sie zu Administration > System > Certificates > Certificate Authority > Internal CA Settings.
2. Stellen Sie sicher, dass die CA-Spalte aktiviert ist, um zu bestätigen, dass die interne CA aktiv ist.



Interne Zertifizierungsstelle überprüfen

Authentifizierungsmethode hinzufügen

Navigieren Sie zu Administration > Identity Management > Identity Source Sequences. Fügen Sie eine benutzerdefinierte Identitätssequenz hinzu, um die Portal-Anmeldequelle zu steuern.



Authentifizierungsmethode

Zertifikatvorlage angeben

Gehen Sie folgendermaßen vor, um eine Zertifikatvorlage anzugeben:

Schritt 1: Navigieren Sie zu Administration > System > Certificates > Certificate Authority > Certificate Templates.

Schritt 2. Klicken Sie auf das Symbol +Hinzufügen, um eine neue Zertifikatvorlage zu erstellen:

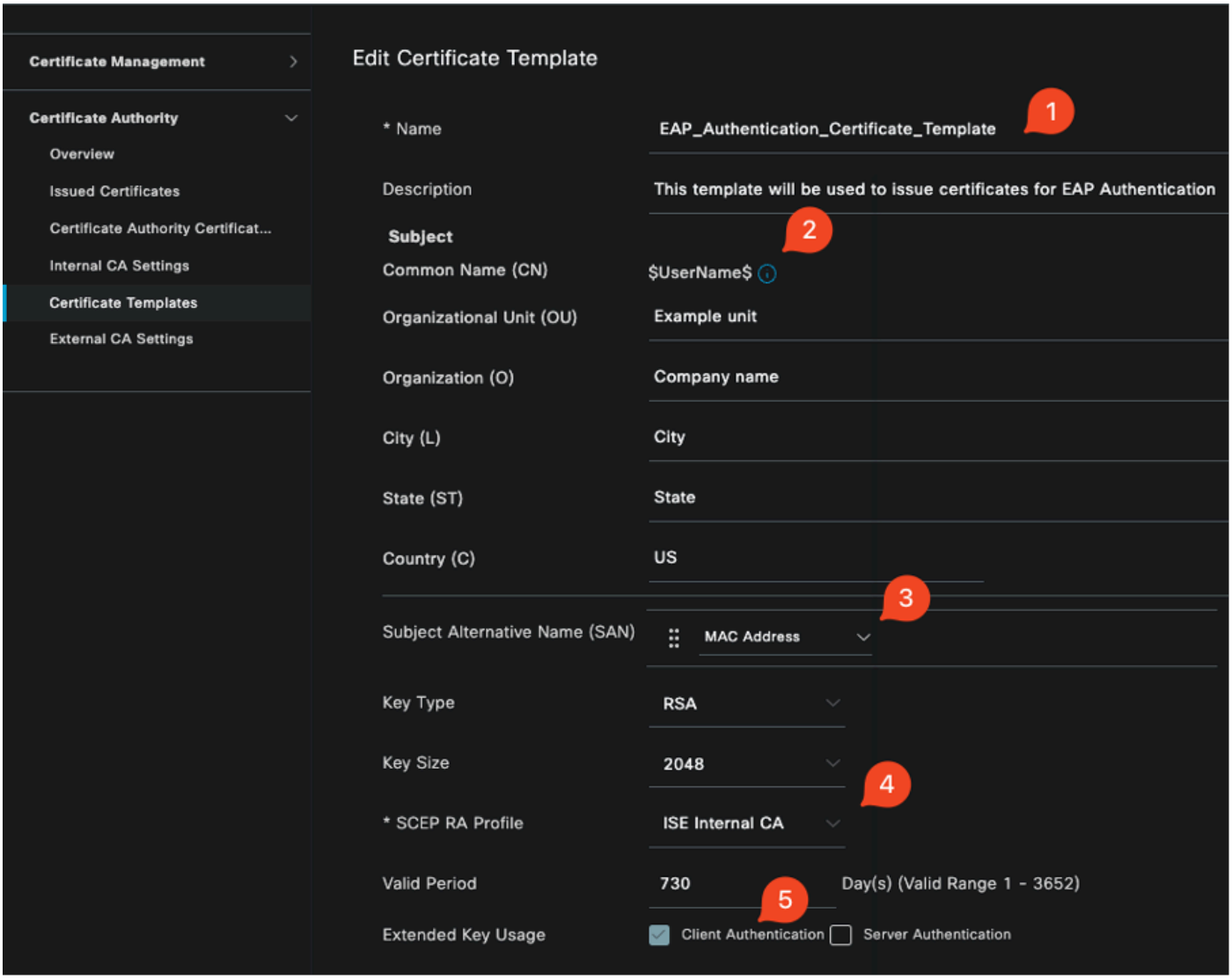
2.1 Geben Sie einen eindeutigen Namen an, der sich lokal auf dem ISE-Server für die Vorlage befindet.

2.2 Stellen Sie sicher, dass der Common Name (CN) auf $UserName$ gesetzt ist.

2.3 Überprüfen Sie, ob der Subject Alternative Name (SAN) der MAC-Adresse zugeordnet ist.

2.4 Setzen Sie das SCEP-RA-Profil auf die interne ISE-CA.

2.5 Aktivieren Sie im Abschnitt zur erweiterten Schlüsselverwendung die Clientauthentifizierung.



Zertifikatvorlage

Zertifikatportal erstellen

Gehen Sie folgendermaßen vor, um ein Zertifikatportal für die Clientzertifikatgenerierung zu erstellen:

Schritt 1: Navigieren Sie zu Administration > Device Portal Management > Certificate Provisioning.

Schritt 2: Klicken Sie auf Erstellen, um eine neue Portalseite einzurichten.

Schritt 3: Geben Sie einen eindeutigen Namen für das Portal an, um es leicht zu identifizieren.

3.1. Wählen Sie die Portnummer für das Portal aus. auf 8443 eingestellt.

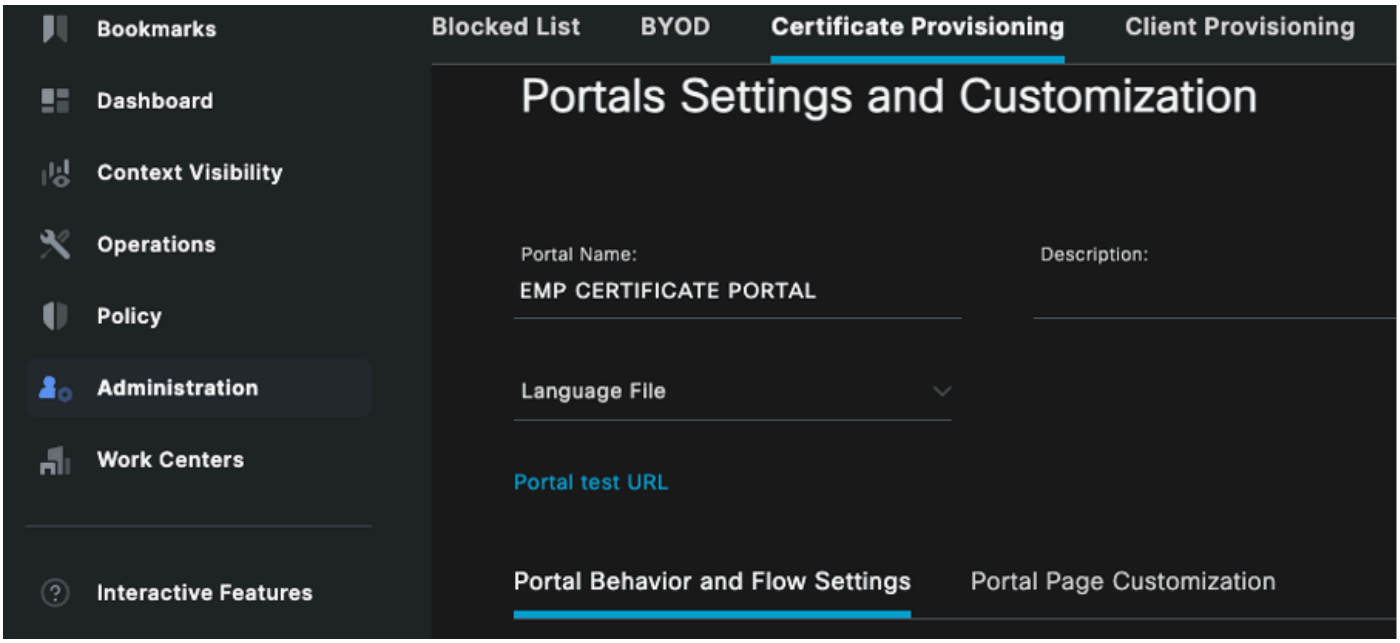
3.2. Geben Sie die Schnittstellen an, auf denen ISE dieses Portal überwacht.

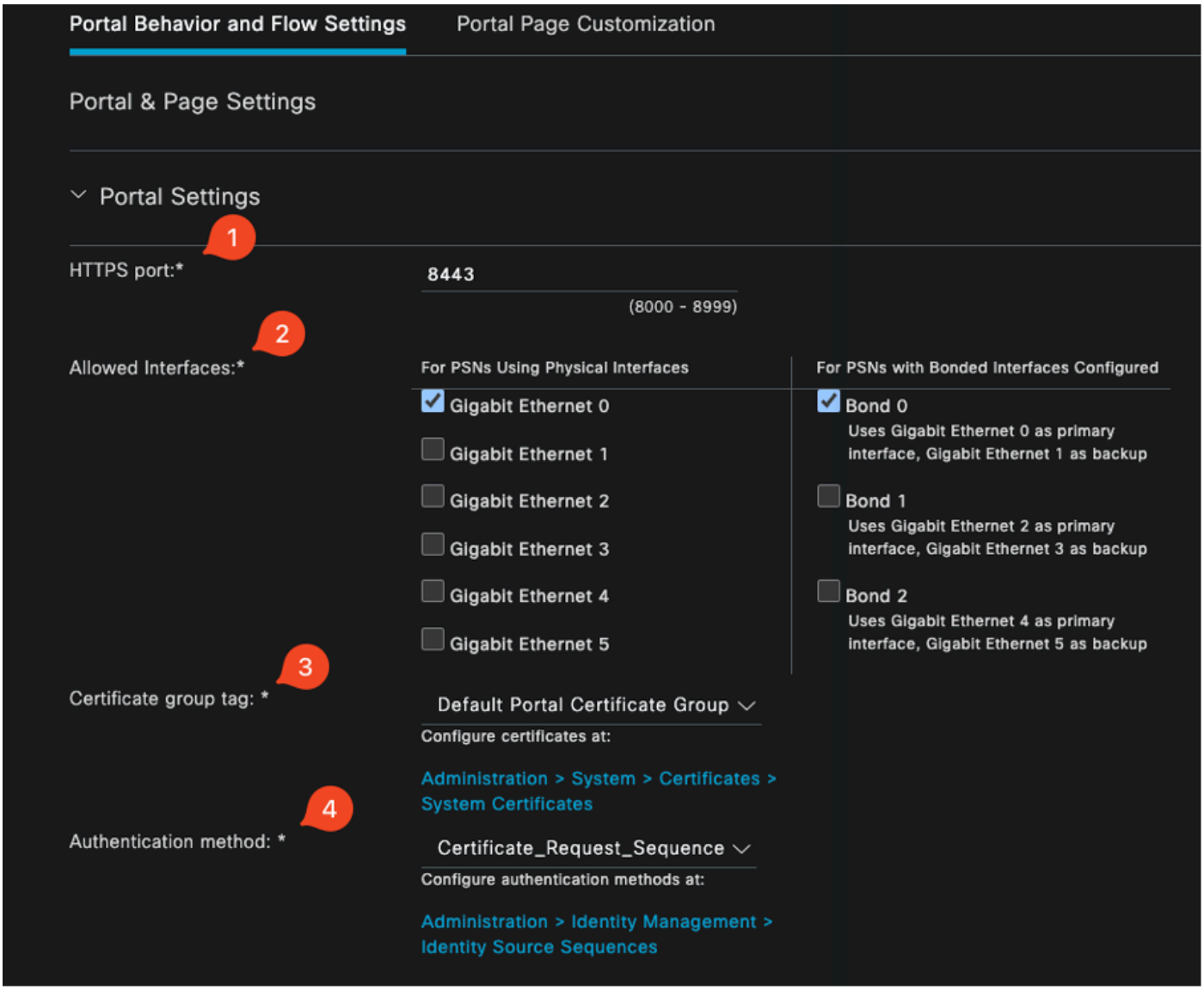
3.3. Wählen Sie das Zertifikatgruppen-Tag als Standardportalzertifikatgruppe aus.

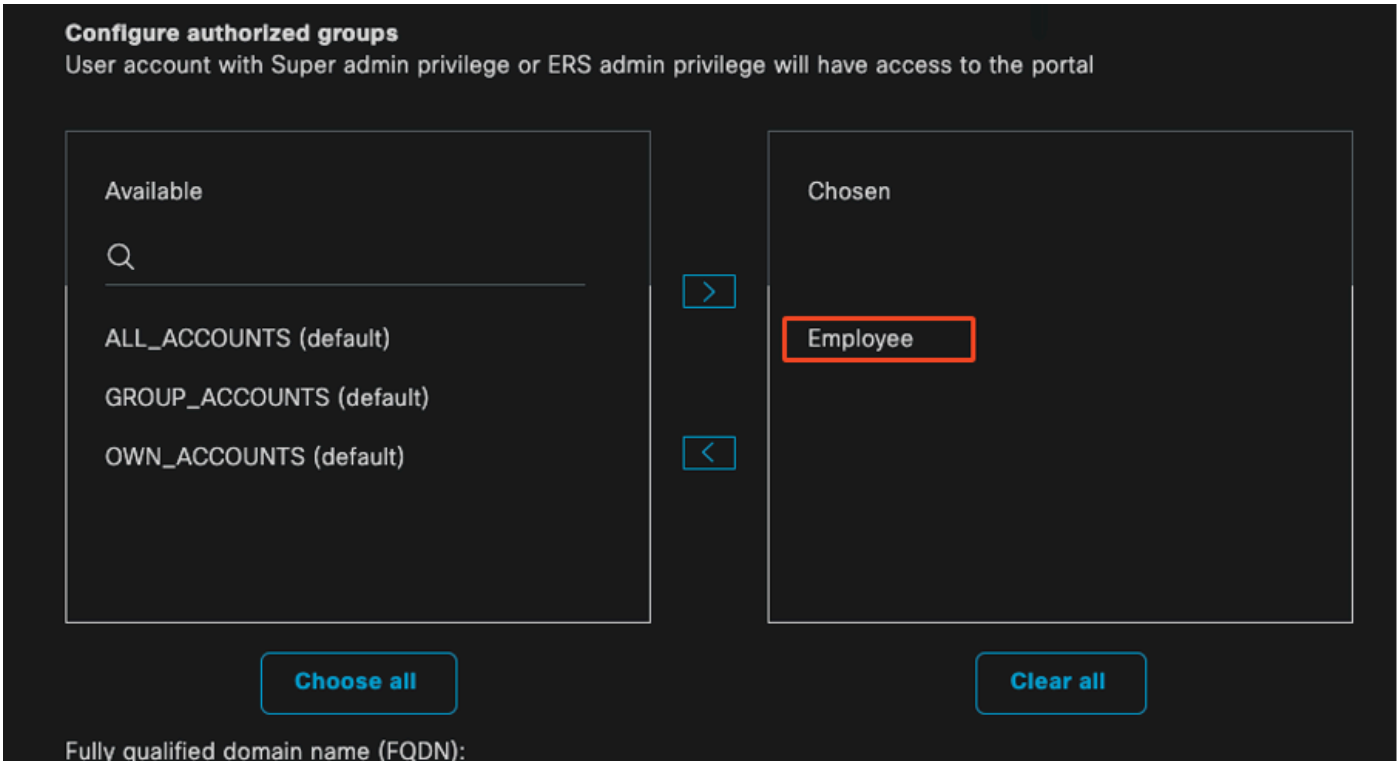
3.4. Wählen Sie die Authentifizierungsmethode aus, die die Identitätsspeichersequenz angibt, mit der die Anmeldung bei diesem Portal authentifiziert wird.

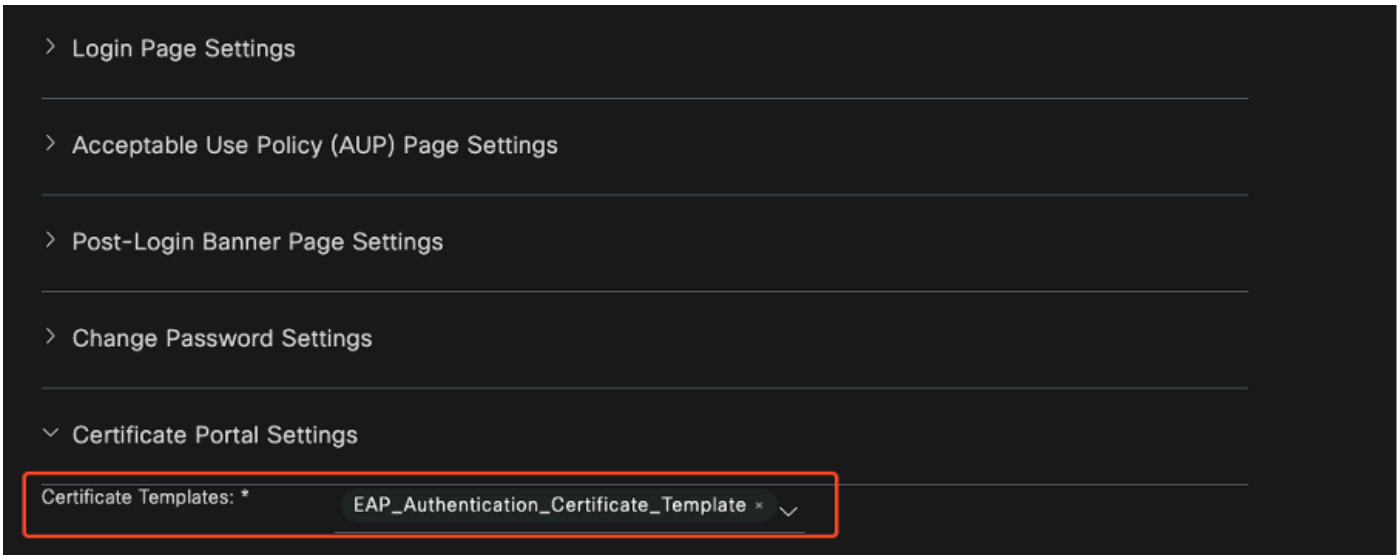
3.5. Schließen Sie die autorisierten Gruppen ein, deren Mitglieder auf das Portal zugreifen können. Wählen Sie beispielsweise die Benutzergruppe Employee aus, wenn Ihre Benutzer zu dieser Gruppe gehören.

3.6. Definieren Sie die Zertifikatvorlagen, die unter den Einstellungen für die Zertifikatbereitstellung zulässig sind.



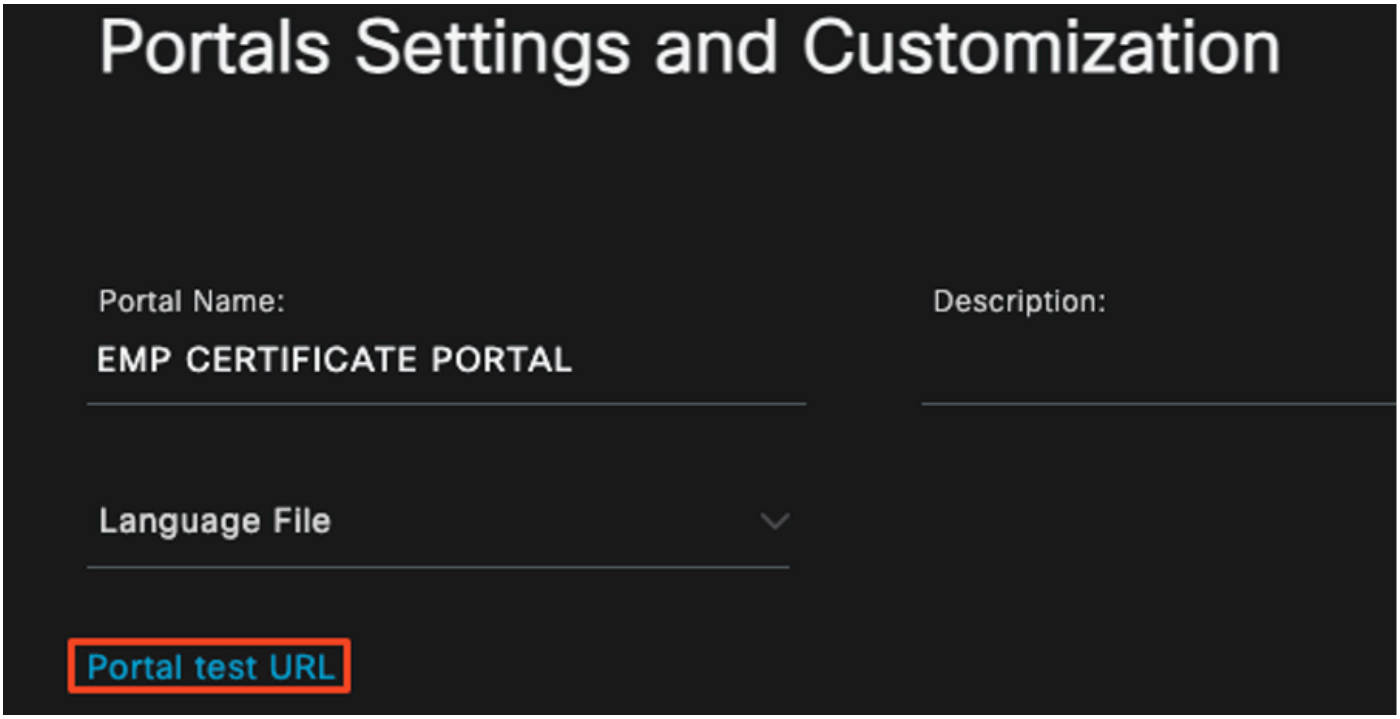

Portal Behavior and Flow Settings
Portal Page Customization
Portal & Page Settings
Portal Settings
1
HTTPS port:*
8443
(8000 - 8999)
2
Allowed Interfaces:*
For PSNs Using Physical Interfaces
Gigabit Ethernet 0
Gigabit Ethernet 1
Gigabit Ethernet 2
Gigabit Ethernet 3
Gigabit Ethernet 4
Gigabit Ethernet 5
For PSNs with Bonded Interfaces Configured
Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup
3
Certificate group tag: *
Default Portal Certificate Group
Configure certificates at:
Administration > System > Certificates > System Certificates
4
Authentication method: *
Certificate_Request_Sequence
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences


Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal
Available
ALL_ACCOUNTS (default)
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)
Chosen
Employee
Choose all
Clear all
Fully qualified domain name (FQDN):

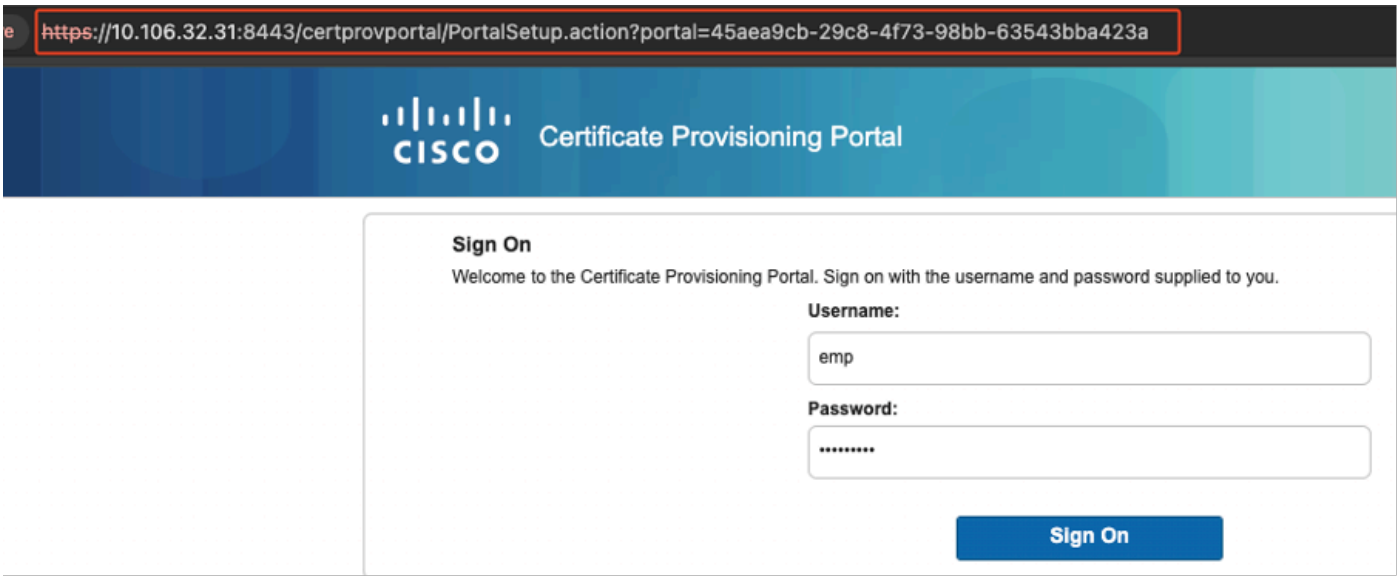


Zertifikatportalkonfiguration

Nach Abschluss dieser Einrichtung können Sie das Portal testen, indem Sie auf die URL für den Portaltest klicken. Mit dieser Aktion wird die Portalseite geöffnet.



URL der Testportalseite

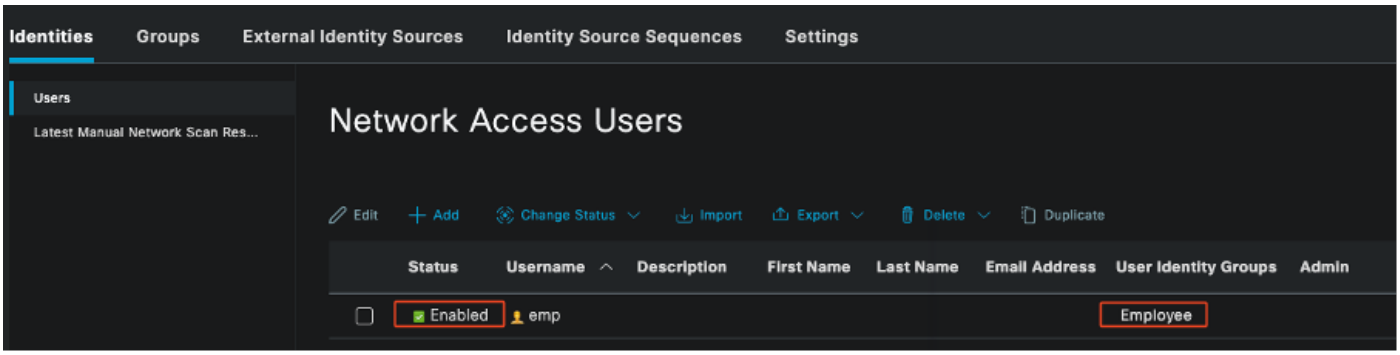


Portalseite

Internen Benutzer hinzufügen

Gehen Sie folgendermaßen vor, um einen Benutzer für die Authentifizierung über das Zertifikatportal zu erstellen:

1. Gehen Sie zu Administration > Identity Management > Identities > Users.
2. Klicken Sie auf die Option, um dem System einen Benutzer hinzuzufügen.
3. Wählen Sie die Benutzeridentitätsgruppen aus, zu denen der Benutzer gehört. Weisen Sie in diesem Beispiel den Benutzer der Gruppe Employee zu.



Hinzufügen eines internen Benutzers

ISE-Zertifikatbereitstellungsportal und RADIUS-Richtlinienkonfiguration

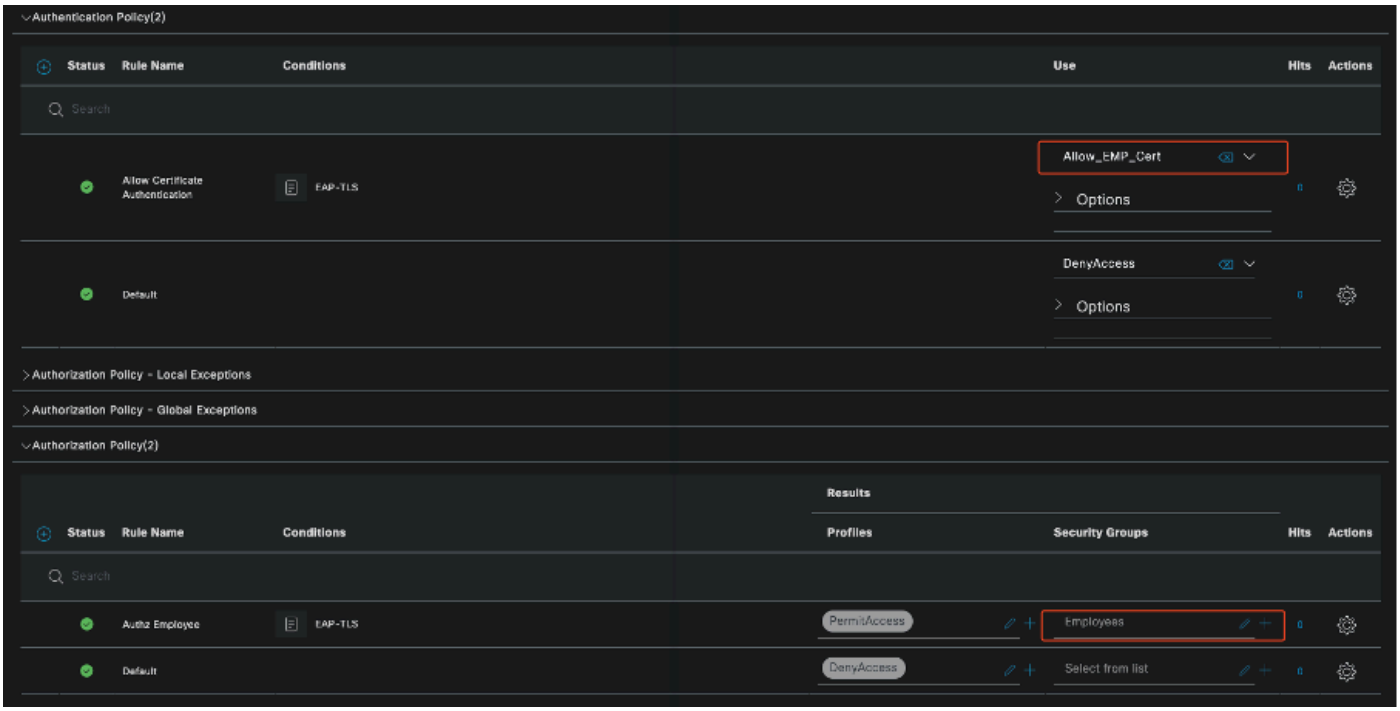
Im vorherigen Abschnitt wurde die Einrichtung des ISE-Zertifikatbereitstellungsportals behandelt. Nun konfigurieren wir die ISE-RADIUS-Richtliniensätze so, dass die Benutzerauthentifizierung möglich ist.

1. Konfigurieren von ISE-RADIUS-Richtliniensätzen
2. Navigieren Sie zu Policy > Policy Sets (Richtlinie > Richtliniensätze).
3. Klicken Sie auf das Pluszeichen (+), um einen neuen Richtliniensatz zu erstellen.

Richten Sie in diesem Beispiel einen einfachen Richtliniensatz ein, der Benutzer anhand ihrer

Zertifikate authentifiziert.

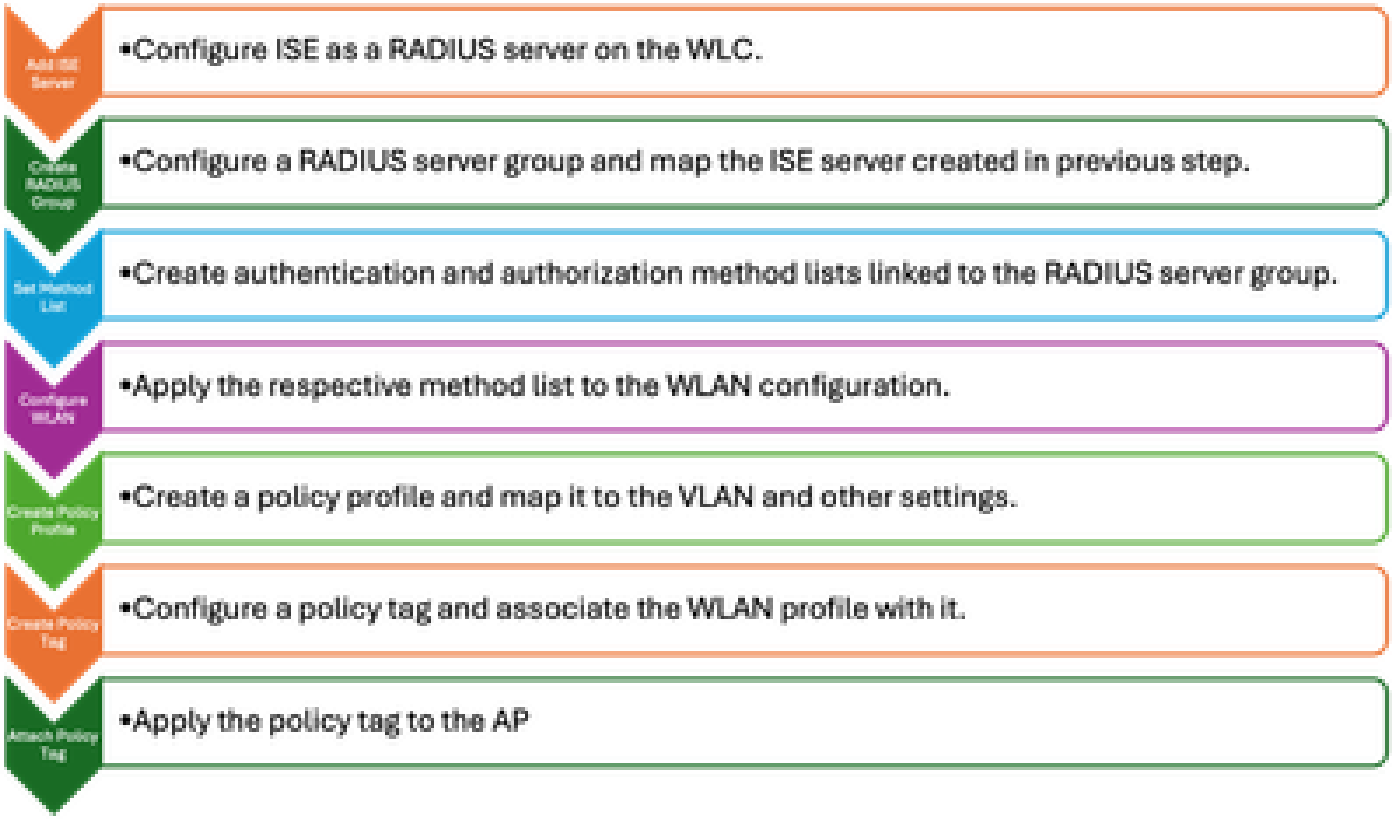
Richtliniensatz



Richtliniensatz mit Authentifizierungs- und Autorisierungsrichtlinien

9800 WLC-Konfiguration

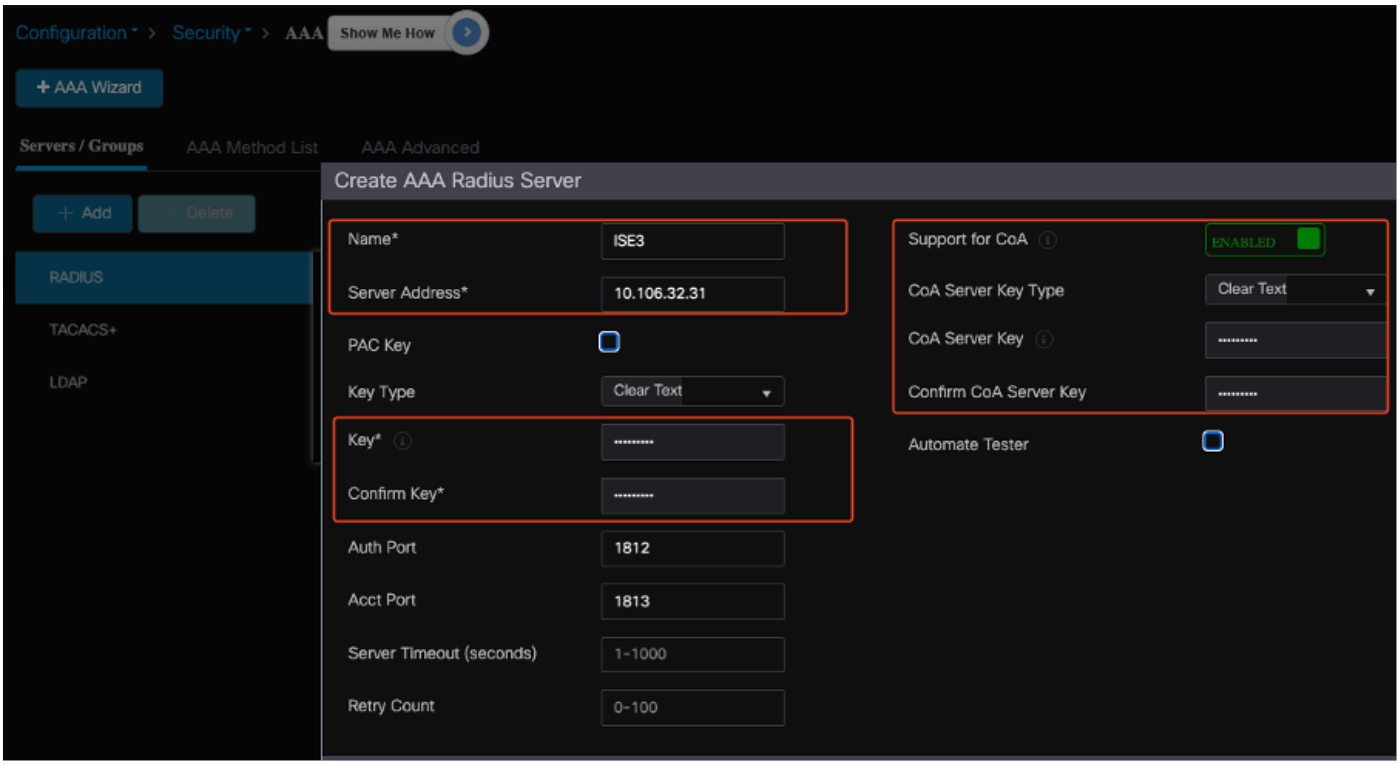
Hier sind die Konfigurationsschritte für den 9800 WLC. Jeder Schritt wird von Screenshots in diesem Abschnitt begleitet, um visuelle Anleitungen bereitzustellen.



WLC-Konfigurationsschritte

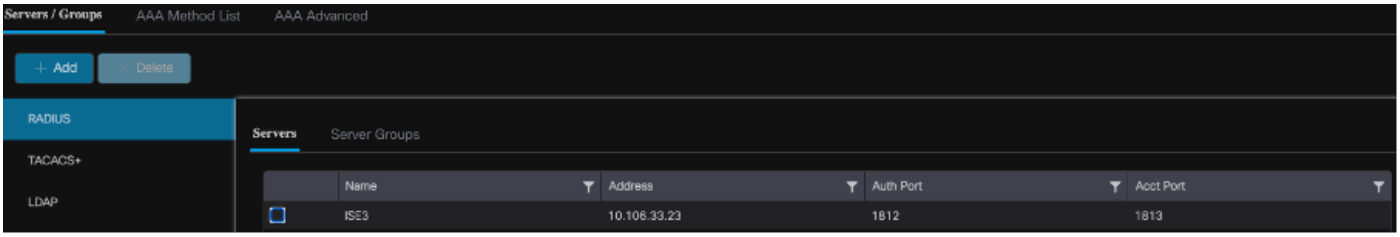
ISE-Server zu 9800 WLC hinzufügen

1. Gehen Sie wie folgt vor, um den ISE-Server in den Wireless LAN Controller (WLC) 9800 zu integrieren:
2. Gehen Sie zu Configuration > Security > AAA.
3. Klicken Sie auf die Schaltfläche Add (Hinzufügen), um den ISE-Server in die WLC-Konfiguration aufzunehmen.



Hinzufügen des ISE-Servers zum WLC

Sobald der Server hinzugefügt wurde, wird er in der Serverliste angezeigt.

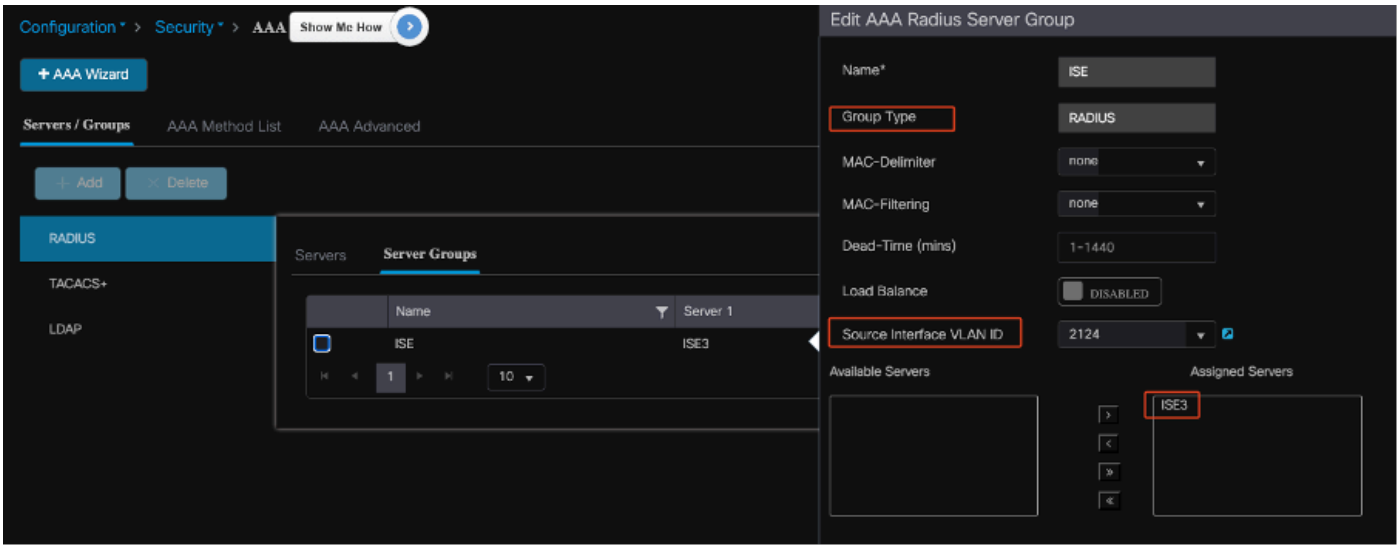


RADIUS-Server anzeigen

Servergruppe auf 9800 WLC hinzufügen

Gehen Sie wie folgt vor, um dem Wireless LAN Controller 9800 eine Servergruppe hinzuzufügen:

1. Navigieren Sie zu Konfiguration > Sicherheit > AAA.
2. Klicken Sie auf die Registerkarte Server Group (Servergruppe), und klicken Sie dann auf Add (Hinzufügen), um eine neue Servergruppe zu erstellen.

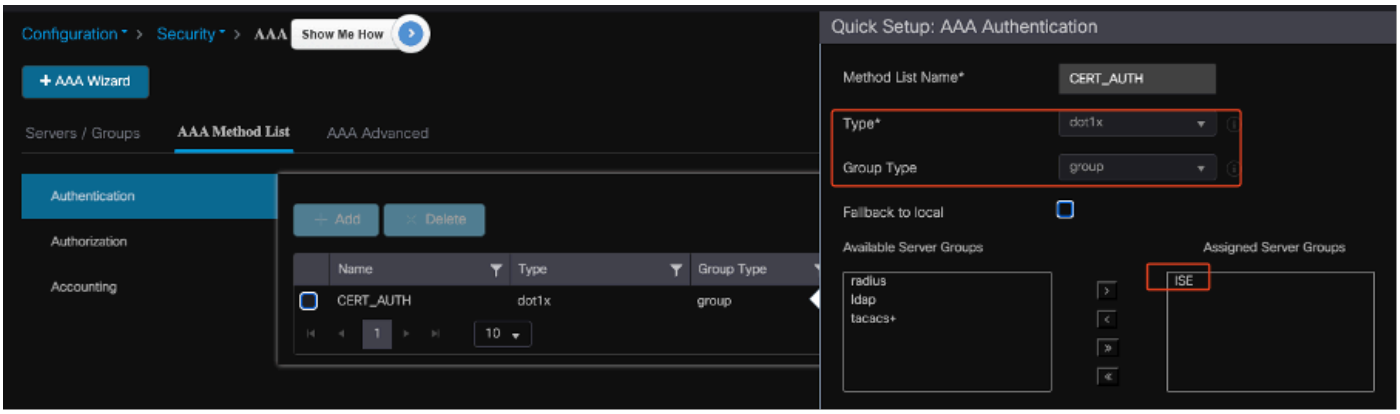


Zuordnung von ISE-Servern zu einer Radius-Servergruppe

Konfigurieren der AAA-Methodenliste für den 9800 WLC

Konfigurieren Sie nach dem Erstellen der Servergruppe die Liste der Authentifizierungsmethoden mit den folgenden Schritten:

1. Navigieren Sie zu Configuration > Security > AAA > AAA Method List (Konfiguration > Sicherheit > AAA-Methodenliste).
2. Fügen Sie auf der Registerkarte Authentifizierung eine neue Liste der Authentifizierungsmethoden hinzu.
3. Setzen Sie den Typ auf dot1x.
4. Wählen Sie Gruppe als Gruppentyp aus.
5. Schließen Sie die ISE-Servergruppen ein, die Sie zuvor als Servergruppen erstellt haben.



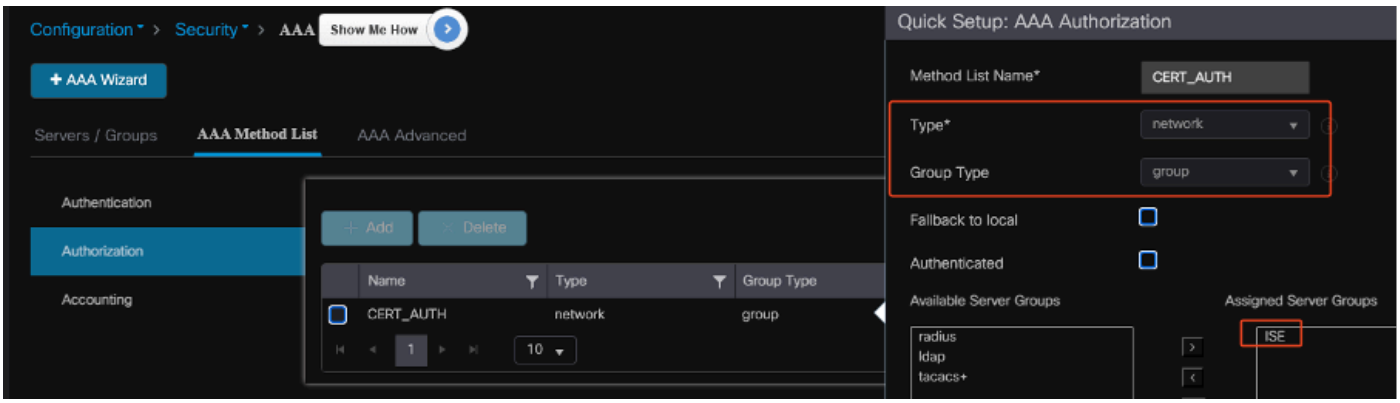
Erstellen von Authentifizierungsmethodenlisten

Konfiguration der Autorisierungsmethodenliste auf dem 9800 WLC

Führen Sie die folgenden Schritte aus, um die Liste der Autorisierungsmethoden einzurichten:

1. Navigieren Sie zur Registerkarte Authorization (Autorisierung) im Abschnitt AAA Method List (AAA-Methodenliste).
2. Klicken Sie auf Hinzufügen, um eine neue Autorisierungsmethodenliste zu erstellen.

3. Wählen Sie als Typ Netzwerk aus.
4. Wählen Sie Gruppe als Gruppentyp aus.
5. Integrieren Sie die ISE-Servergruppe als Servergruppe.

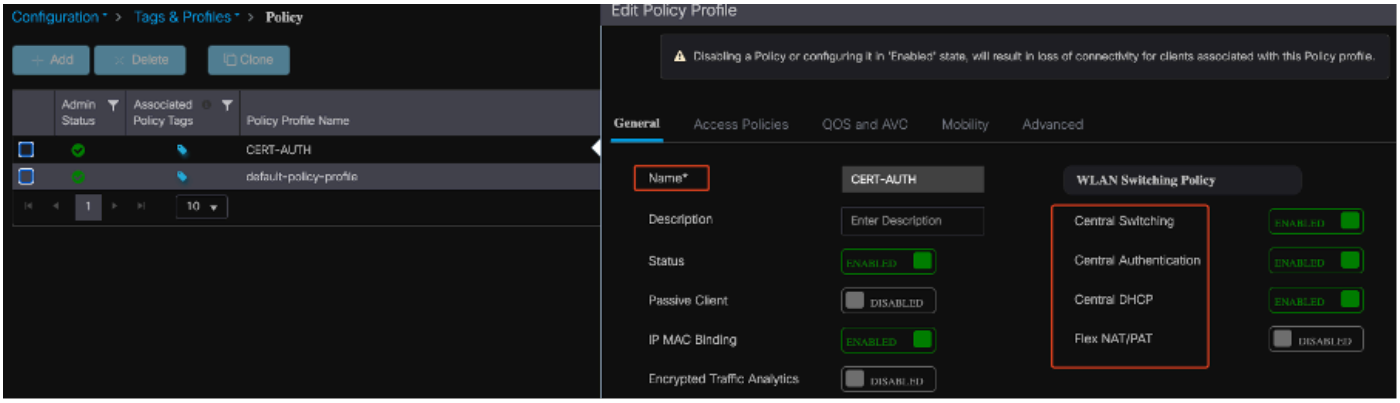


Hinzufügen einer Autorisierungsmethodenliste

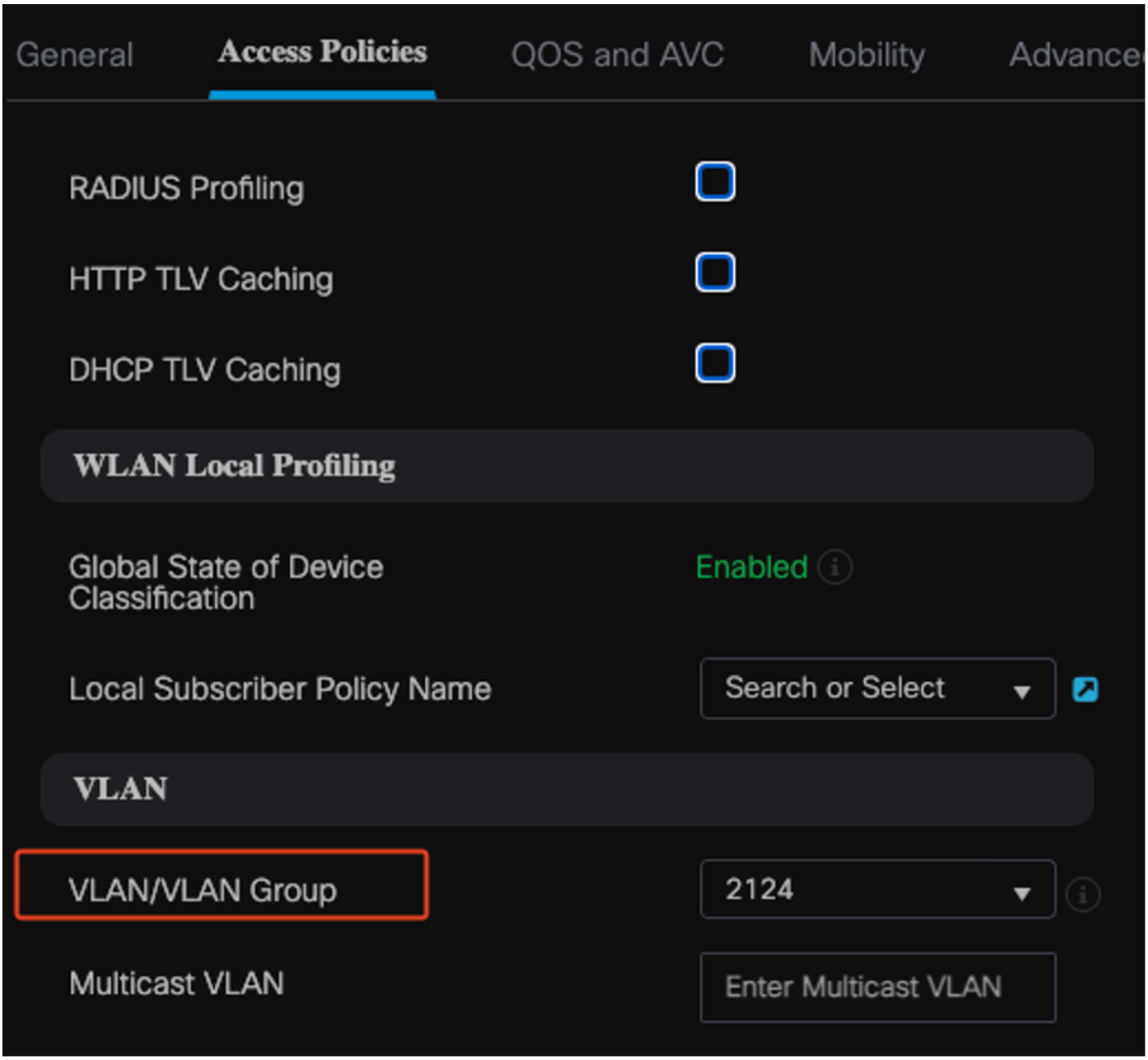
Erstellen eines Richtlinienprofils auf dem 9800 WLC

Fahren Sie nach Abschluss der RADIUS-Gruppenkonfiguration mit der Erstellung eines Richtlinienprofils fort:

1. Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie.
2. Klicken Sie auf Hinzufügen, um ein neues Richtlinienprofil zu erstellen.
3. Wählen Sie die entsprechenden Parameter für Ihr Richtlinienprofil aus. In diesem Beispiel ist alles zentral, und das LAB-VLAN wird als Client-VLAN verwendet.

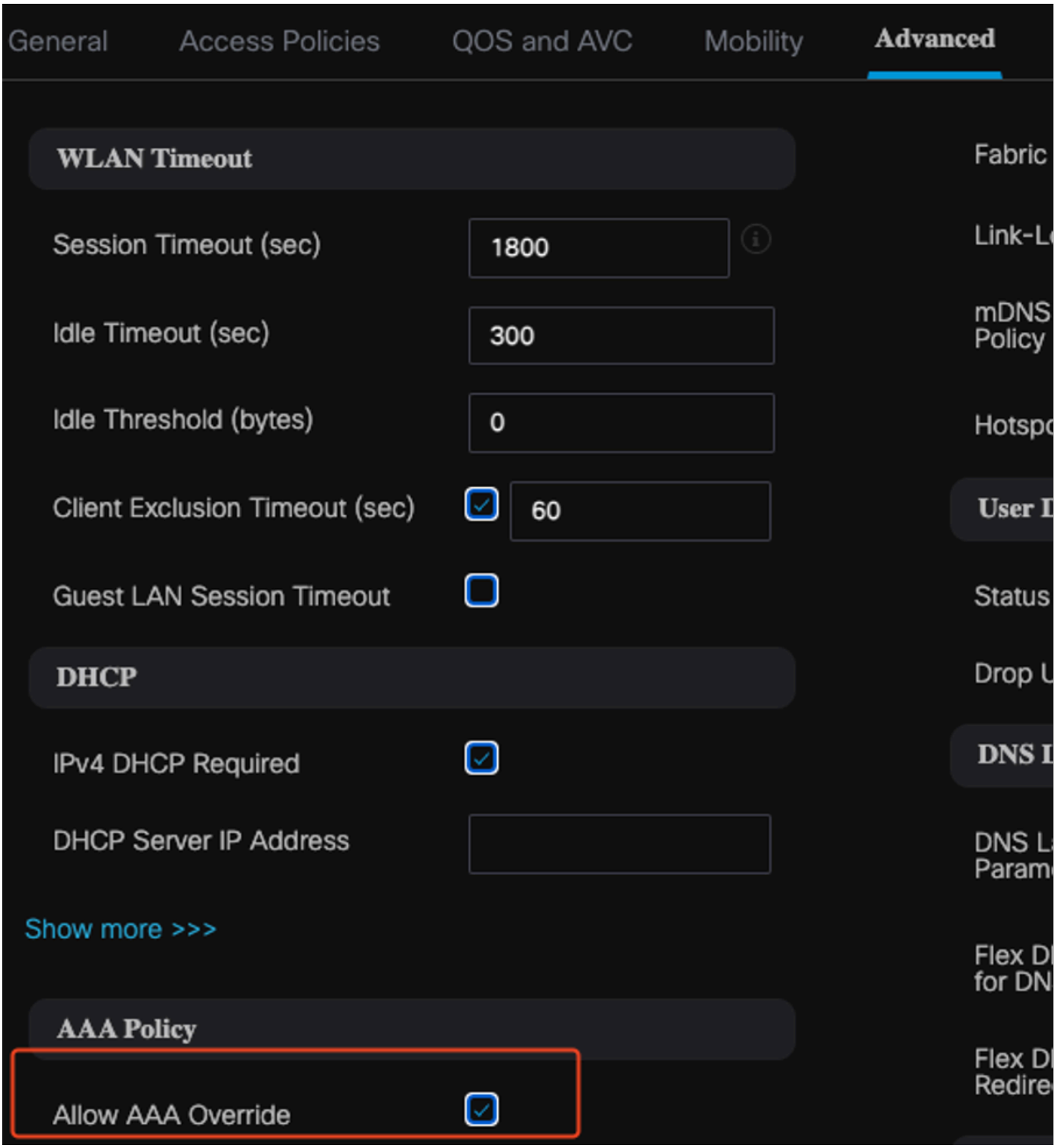


Konfigurieren des Richtlinienprofils



VLAN-Richtlinienzuordnung

Stellen Sie beim Konfigurieren der RADIUS-Autorisierung sicher, dass die Option AAA Override auf der Registerkarte Advanced (Erweitert) der Richtlinienprofileinstellungen aktiviert ist. Mit dieser Einstellung kann der Wireless LAN Controller RADIUS-basierte Autorisierungsrichtlinien auf Benutzer und Geräte anwenden.

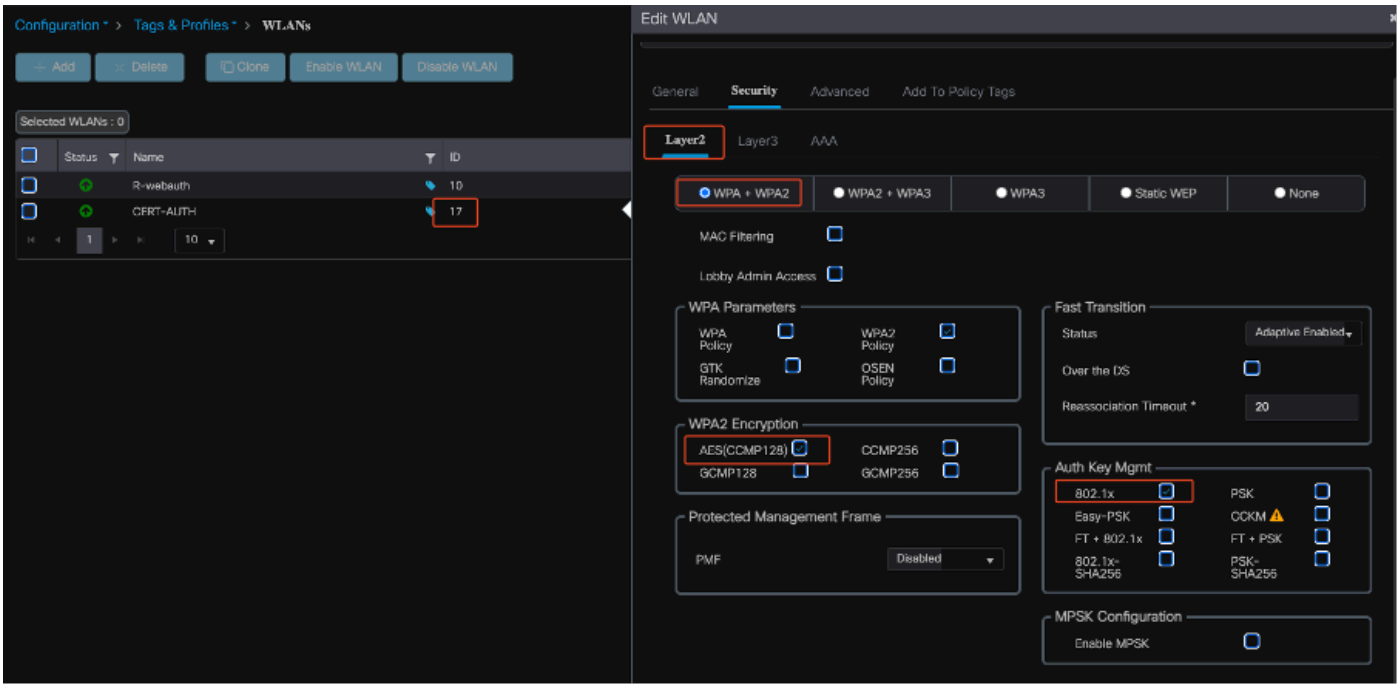


AAA überschreiben

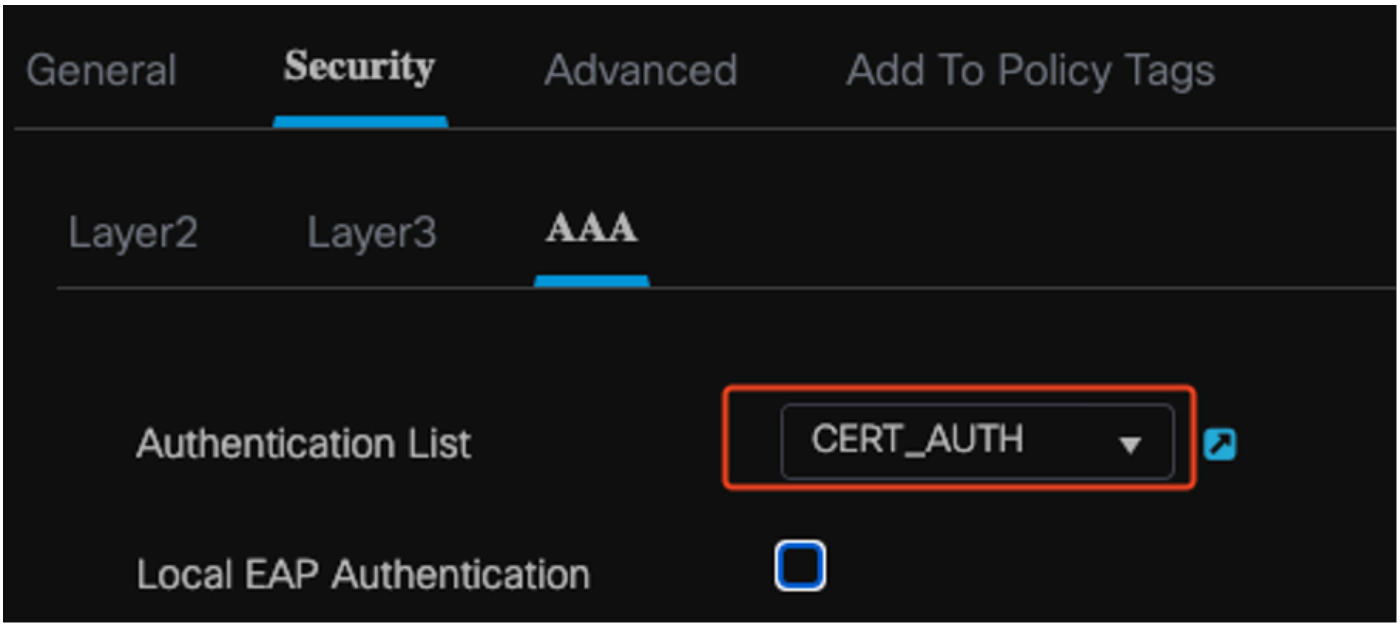
Erstellen eines WLAN auf dem 9800 WLC

Gehen Sie wie folgt vor, um ein neues WLAN mit 802.1x-Authentifizierung einzurichten:

1. Navigieren Sie zu Konfiguration > Tags & Profile > WLANs.
2. Klicken Sie auf Hinzufügen, um ein neues WLAN zu erstellen.
3. Wählen Sie die Authentifizierungseinstellungen für Layer 2 aus, und aktivieren Sie die 802.1x-Authentifizierung.



WLAN-Profilkonfiguration

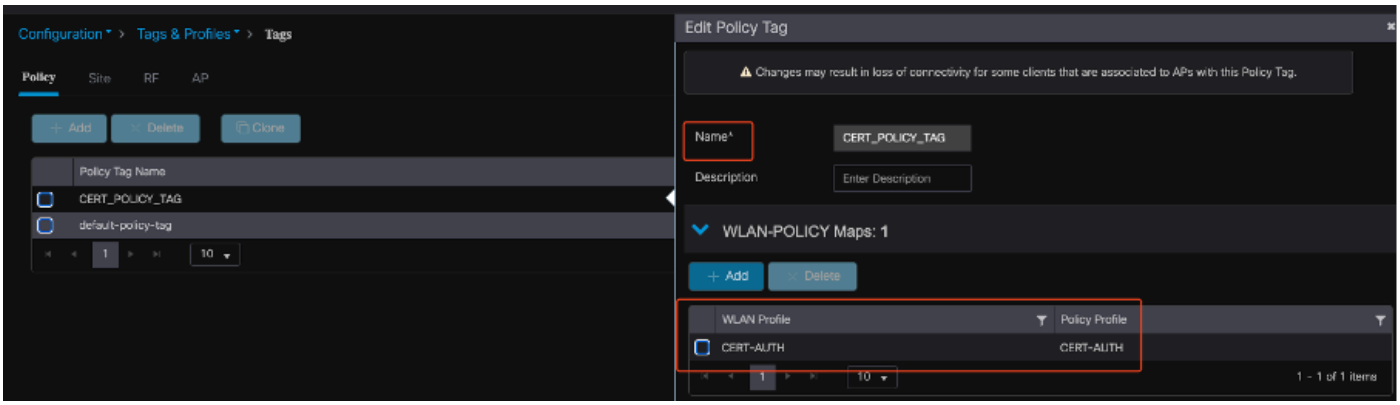


Zuordnung des WLAN-Profils zur Methodenliste

Zuordnung von WLAN mit Richtlinienprofil auf dem 9800 WLC

Um Ihr WLAN einem Richtlinienprofil zuzuordnen, gehen Sie wie folgt vor:

1. Navigieren Sie zu Konfiguration > Tags & Profile > Tags.
2. Klicken Sie auf Hinzufügen, um ein neues Tag hinzuzufügen.
3. Ordnen Sie das neu erstellte WLAN im Abschnitt "WLAN-POLICY" dem entsprechenden Richtlinienprofil zu.

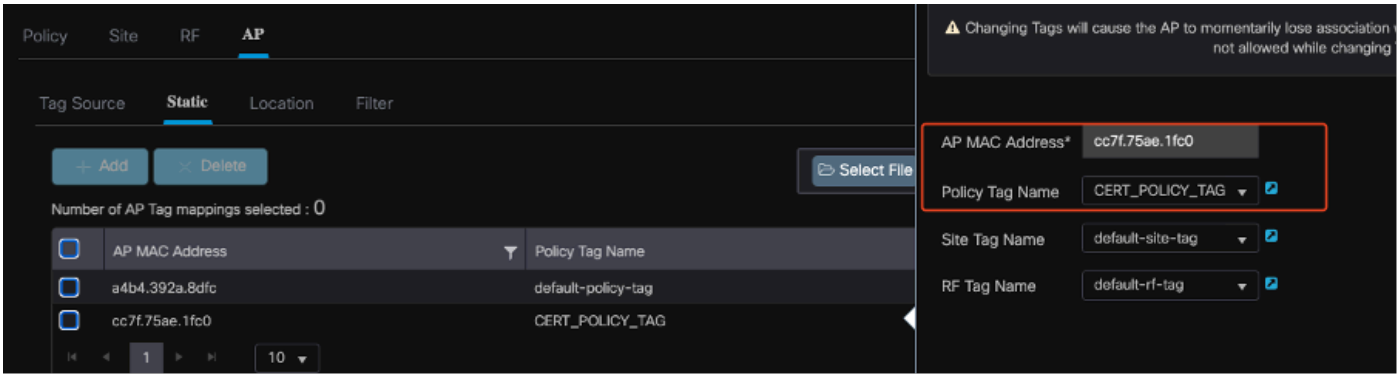


Richtlinien-Tag-Konfiguration

Richtlinienkennzeichnung auf Access Point auf 9800 WLC zuordnen

Gehen Sie wie folgt vor, um einem Access Point (AP) das Policy-Tag zuzuweisen:

1. Navigieren Sie zu Konfiguration > Tags & Profile > Tags > AP.
2. Gehen Sie zum Abschnitt Statisch innerhalb der AP-Konfiguration.
3. Klicken Sie auf den AP, den Sie konfigurieren möchten.
4. Weisen Sie dem ausgewählten Access Point das erstellte Policy-Tag zu.



AP-TAG-Zuweisung

Ausführen der Konfiguration des WLC nach Abschluss der Einrichtung

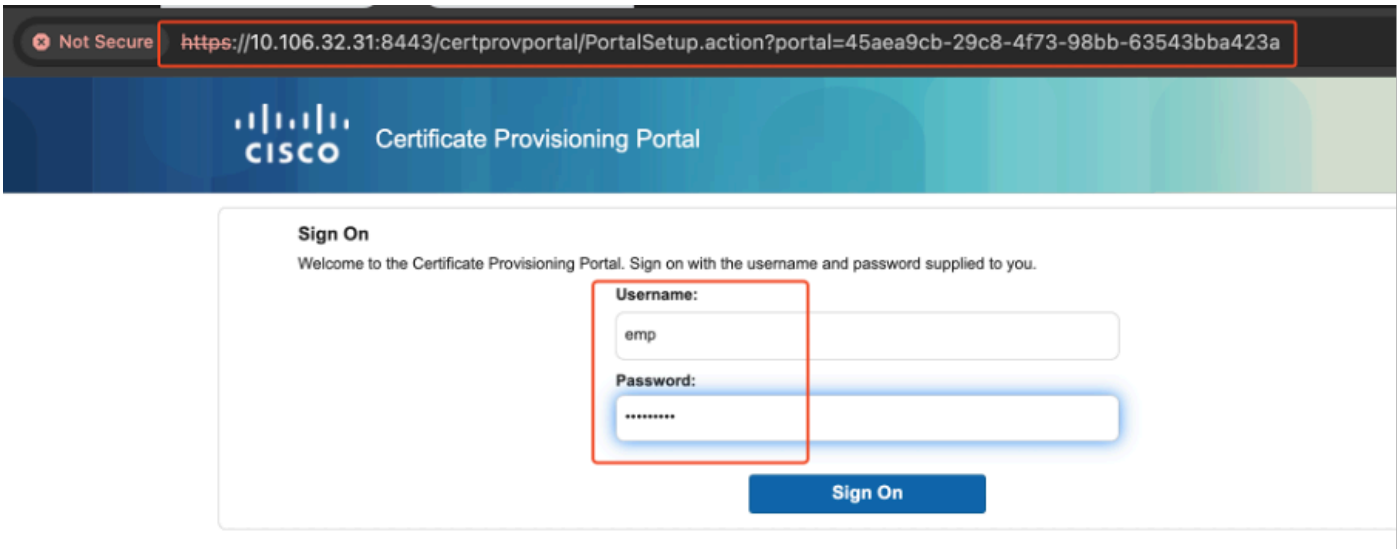
```
aaa group server radius ISE
 server name ISE3
 ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
 client 10.106.32.31 server-key Cisco!123
!

wireless profile policy CERT-AUTH
 aaa-override
 ipv4 dhcp required
 vlan 2124
 no shutdown
 wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
```

```
 security dot1x authentication-list CERT_AUTH
 no shutdown
!
wireless tag policy CERT_POLICY_TAG
 wlan CERT-AUTH policy CERT-AUTH
```

Zertifikat für den Benutzer erstellen und herunterladen

Gehen Sie folgendermaßen vor, um ein Zertifikat für einen Benutzer zu erstellen und herunterzuladen:

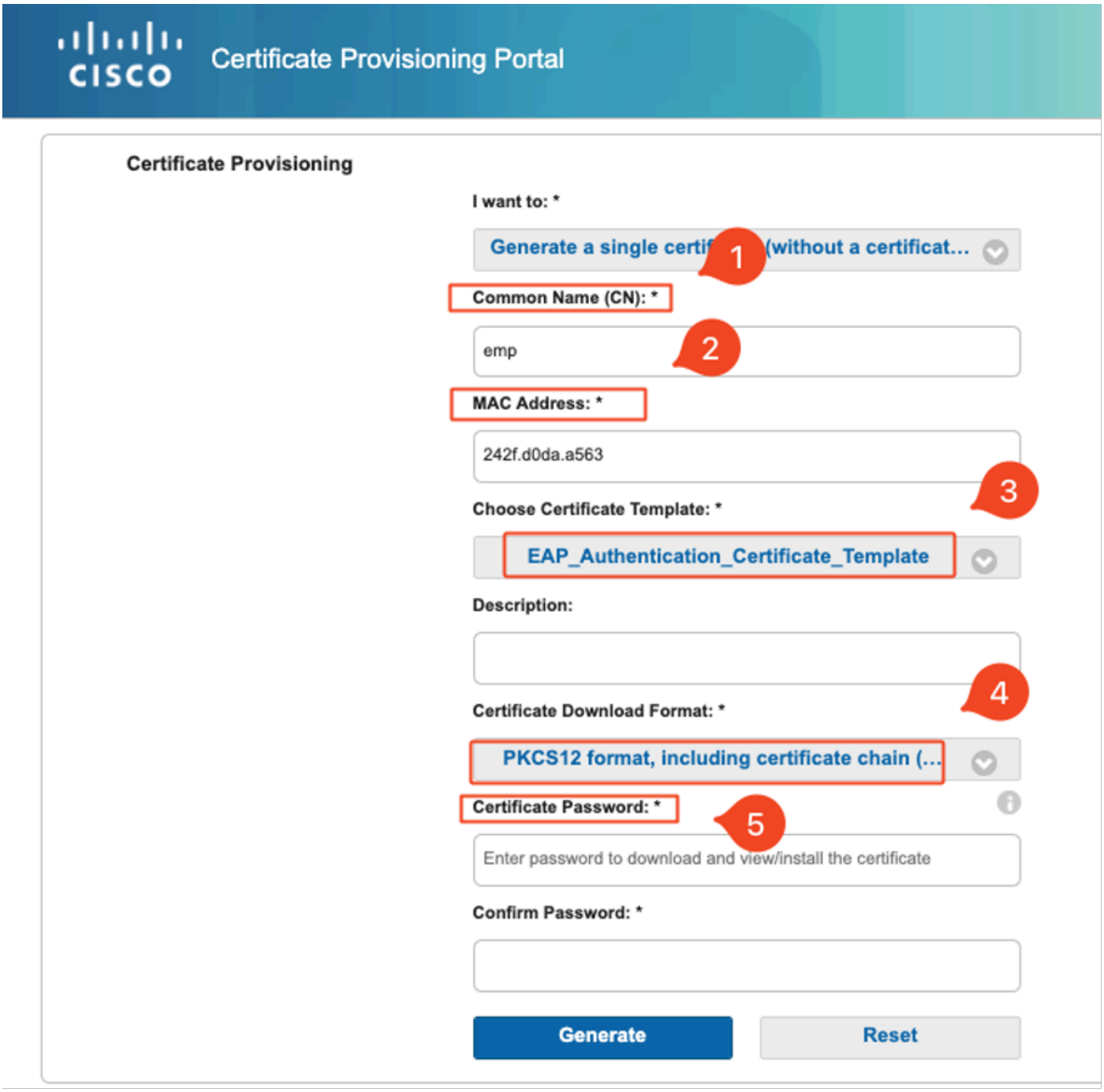
1. Der Benutzer muss sich beim Zertifikatportal anmelden, das zuvor eingerichtet wurde.



Zugriff auf das Zertifikatportal

2. Akzeptieren Sie die Richtlinien zur akzeptablen Nutzung. Die ISE stellt dann eine Seite für die Zertifikatgenerierung dar.

3. Wählen Sie Einzelnes Zertifikat generieren (ohne Signieranforderung für das Zertifikat).



Zertifikat wird generiert

Um ein Zertifikat über das Zertifikatbereitstellungsportal zu erstellen, stellen Sie sicher, dass die folgenden Pflichtfelder ausgefüllt sind:

- KN Der Authentifizierungsserver verwendet den Wert, der im Feld Allgemeiner Name im Clientzertifikat angegeben ist, um einen Benutzer zu authentifizieren. Geben Sie im Feld Common Name (Allgemeiner Name) den Benutzernamen ein (den Sie für die Anmeldung beim Zertifikatbereitstellungsportal verwendet haben).
- MAC-Adresse: Subject Alternative Names (SAN) ist eine X.509-Erweiterung, mit der verschiedene Werte einem Sicherheitszertifikat zugeordnet werden können. Cisco ISE Version 2.0 unterstützt nur MAC-Adressen. Daher im Feld SAN/MAC-Adresse.
    - Zertifikatvorlage: Die Zertifikatvorlage definiert eine Reihe von Feldern, die die Zertifizierungsstelle bei der Validierung einer Anforderung und der Ausstellung eines

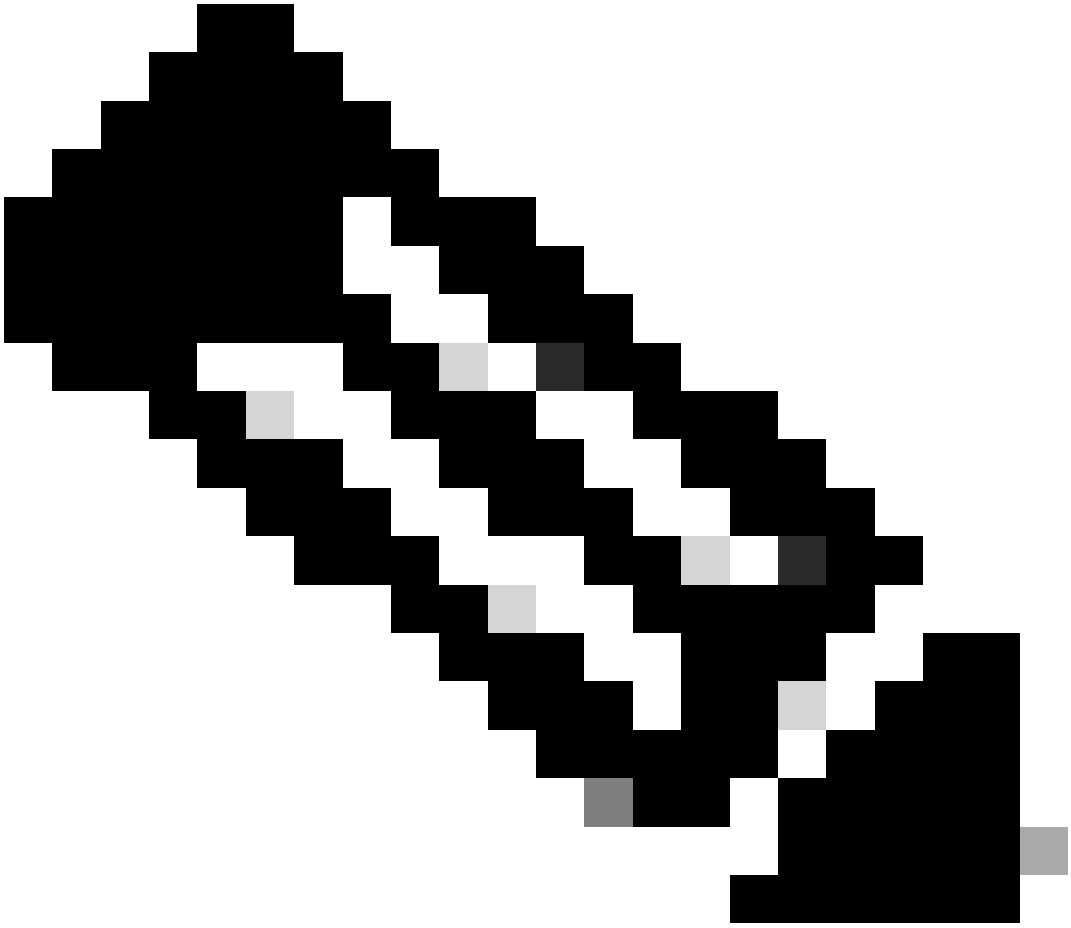
Zertifikats verwendet. Zur Validierung der Anforderung werden Felder wie der Common Name (CN) verwendet (CN muss mit dem Benutzernamen übereinstimmen). Andere Felder werden von der Zertifizierungsstelle während der Ausstellung des Zertifikats verwendet.

- Zertifikatkennwort: Sie benötigen ein Zertifikatkennwort, um Ihr Zertifikat zu sichern. Sie müssen das Zertifikatkennwort angeben, um den Inhalt des Zertifikats anzuzeigen und das Zertifikat auf ein Gerät zu importieren.
- Ihr Kennwort muss folgenden Regeln entsprechen:
- Das Kennwort muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer enthalten.
    - Das Kennwort muss zwischen 8 und 15 Zeichen lang sein.
    - Mögliche Zeichen sind A-Z, a-z, 0-9, _, #

Wenn Sie alle Felder ausgefüllt haben, wählen Sie Generate (Generieren) aus, um das Zertifikat zu erstellen und herunterzuladen.

Zertifikatinstallation auf einem Windows 10-Computer

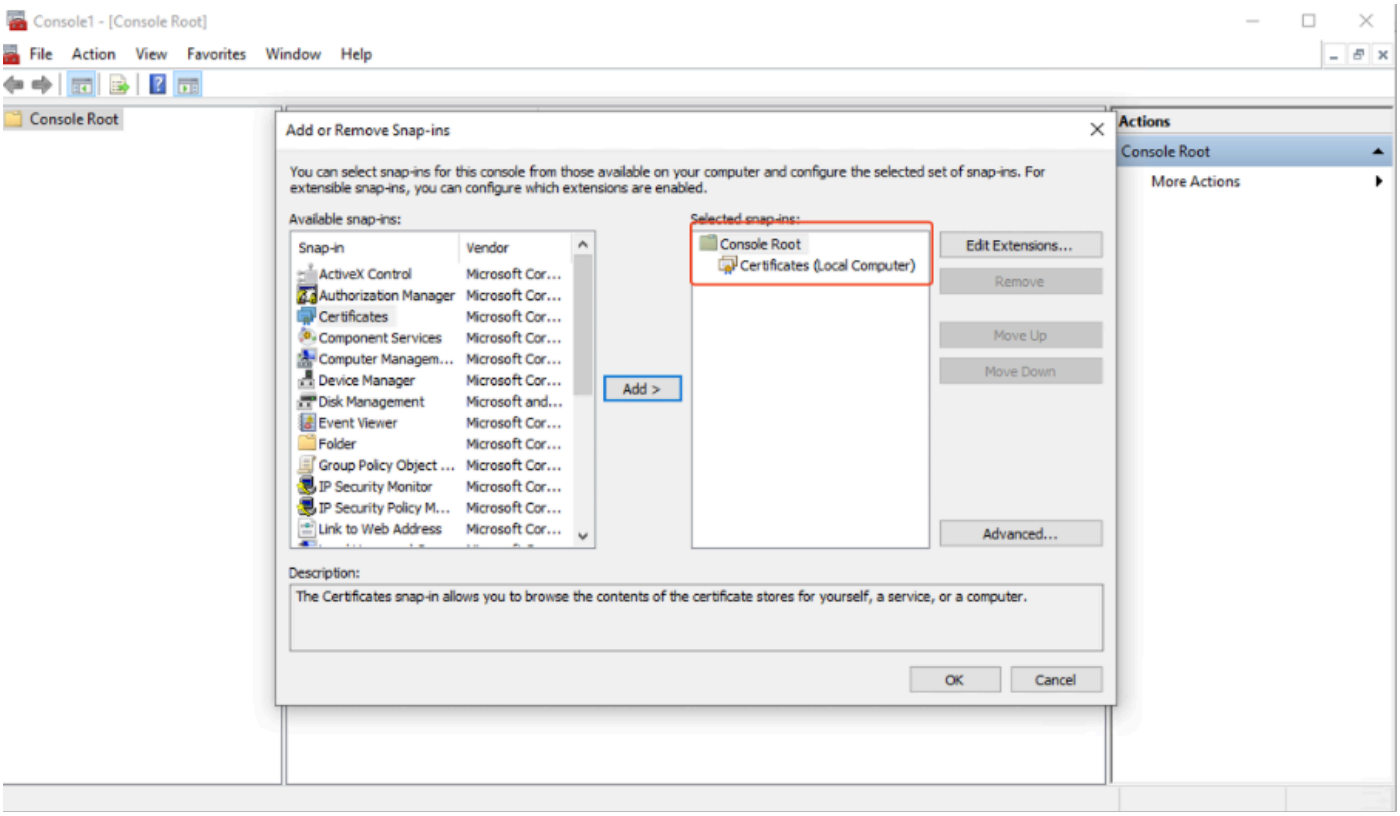
Um ein Zertifikat auf einem Windows 10-Computer zu installieren, öffnen Sie die Microsoft Management Console (MMC) wie folgt:



Anmerkung: Diese Anleitungen können je nach Windows-Setup variieren. Deshalb wird empfohlen, die Microsoft-Dokumentation für spezifische Details zu konsultieren.

1. Klicken Sie auf Start und dann auf Ausführen.
2. Geben Sie mmc in das Feld Ausführen ein, und drücken Sie die Eingabetaste. Die Microsoft Management Console wird geöffnet.
3. Snap-In Zertifikat hinzufügen:
4. Gehen Sie zu Datei > Snap-In hinzufügen/entfernen.
5. Wählen Sie Hinzufügen aus, wählen Sie dann Zertifikate aus, und klicken Sie auf Hinzufügen.
6. Wählen Sie Computerkonto, dann Lokaler Computer aus, und klicken Sie auf Fertig stellen.

Mit diesen Schritten können Sie Zertifikate auf dem lokalen Computer verwalten.



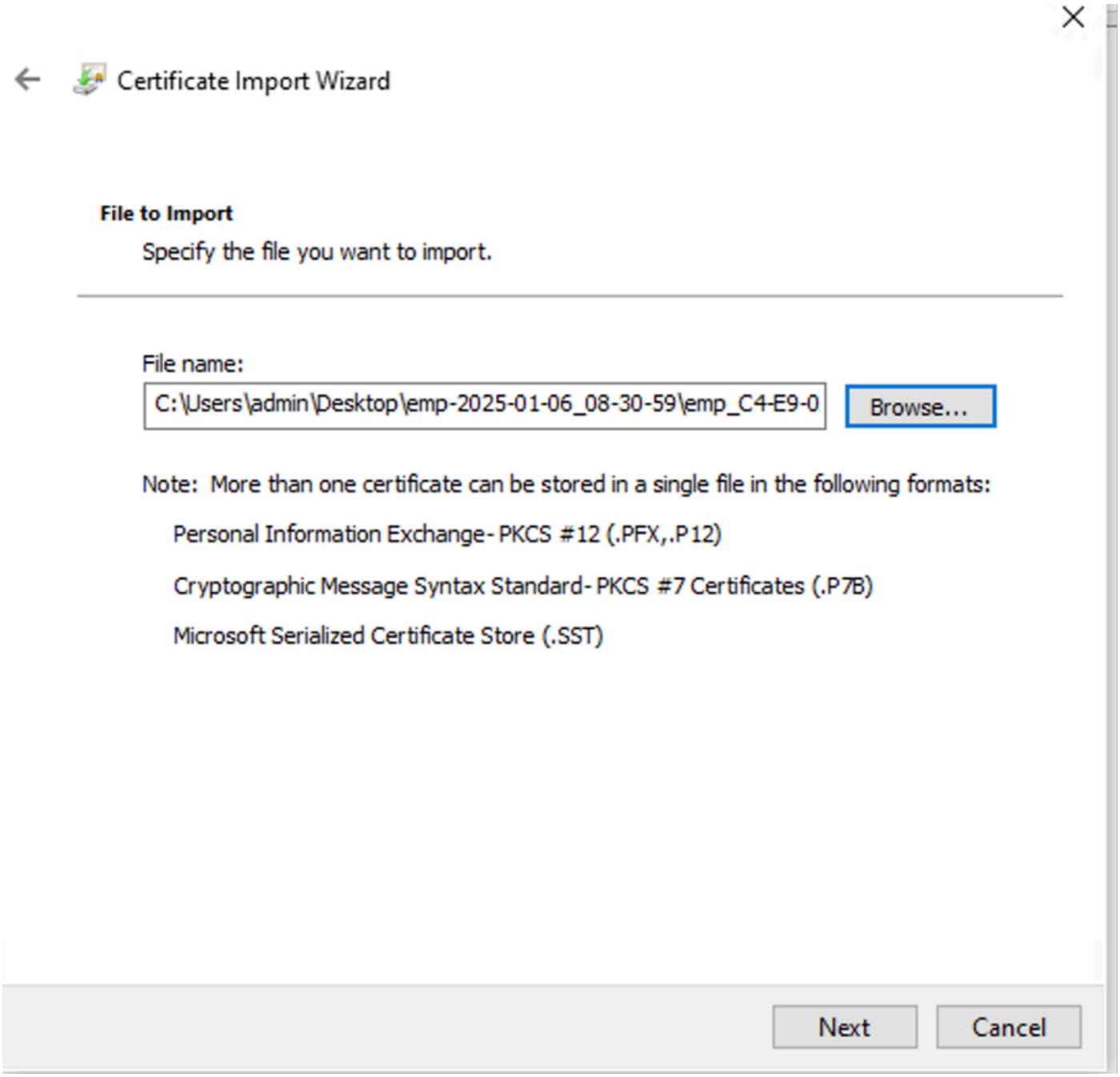
Windows MMC-Konsole

Schritt 1: Zertifikat importieren:

1.1. Klicken Sie auf Aktion im Menü.

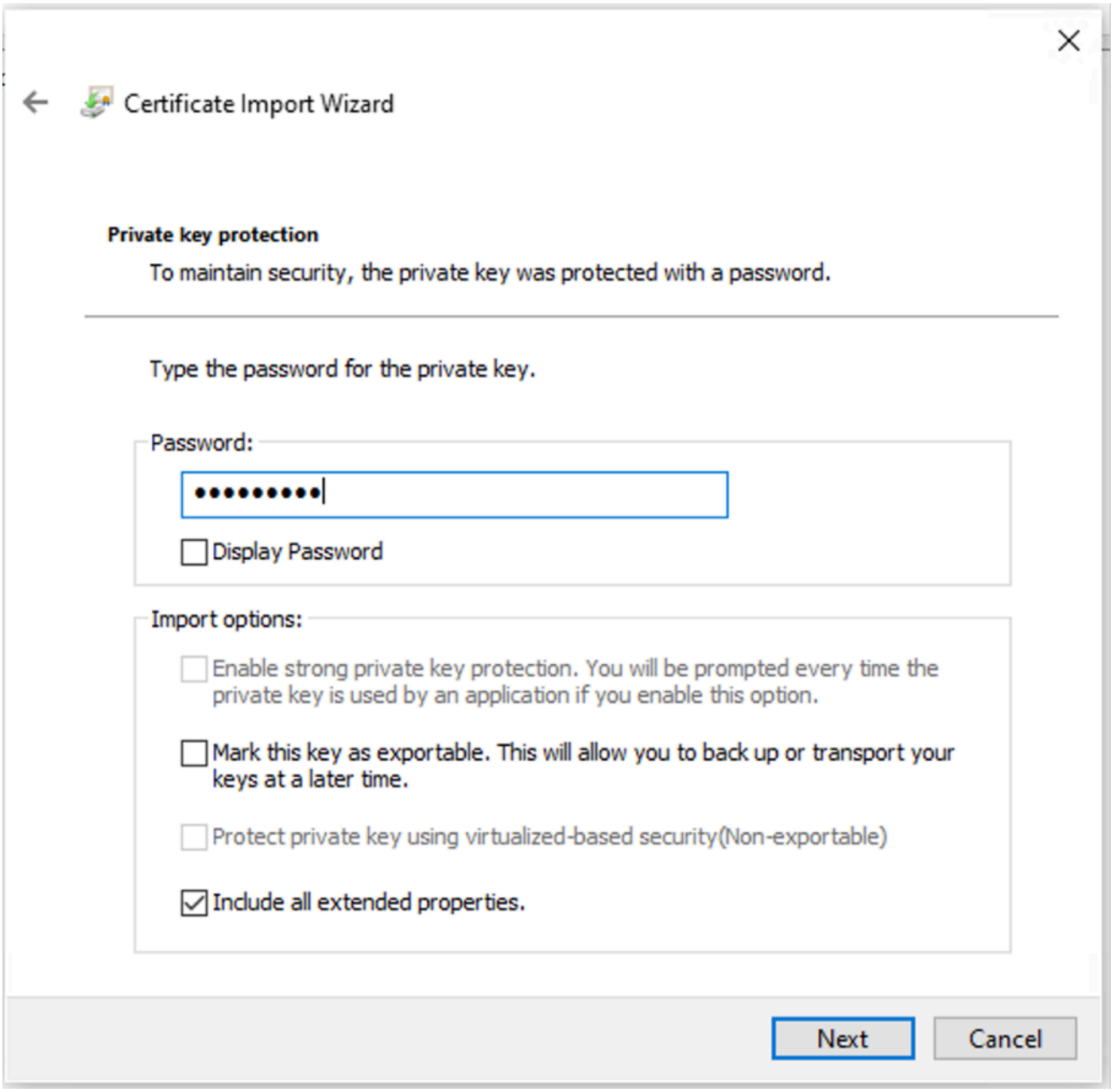
1.2. Gehen Sie zu Alle Tasks, und wählen Sie dann Importieren aus.

1.3. Fahren Sie mit den Aufforderungen fort, um die auf Ihrem Computer gespeicherte Zertifikatsdatei zu suchen und auszuwählen.



Zertifikat importieren

Während des Zertifikatsimports werden Sie aufgefordert, das Kennwort einzugeben, das Sie beim Generieren des Zertifikats im Portal erstellt haben. Stellen Sie sicher, dass Sie dieses Kennwort korrekt eingeben, um das Zertifikat erfolgreich auf Ihrem Computer zu importieren und zu installieren.



Zertifikatskennwort eingeben

Schritt 2: Verschieben von Zertifikaten in die entsprechenden Ordner:

2.1. Öffnen Sie die Microsoft Management Console (MMC) und navigieren Sie zu Certificates (Local Computer) > Personal folder.

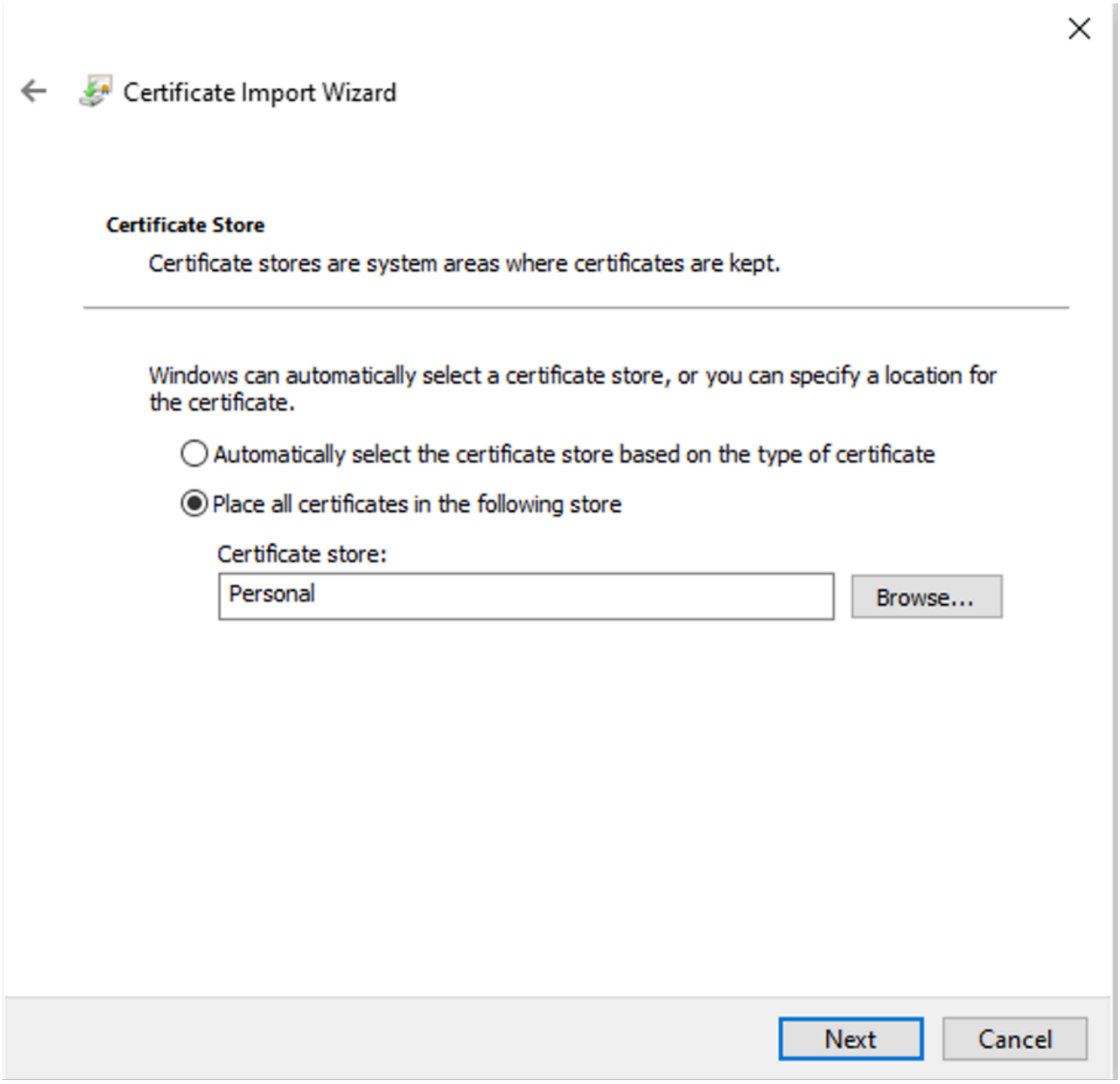
2.2. Überprüfen Sie die Zertifikate, und bestimmen Sie deren Typen (z. B. Stammzertifizierungsstelle, Zwischenzertifizierungsstelle oder Personal).

2.3. Verschieben Sie jedes Zertifikat in den entsprechenden Speicher:

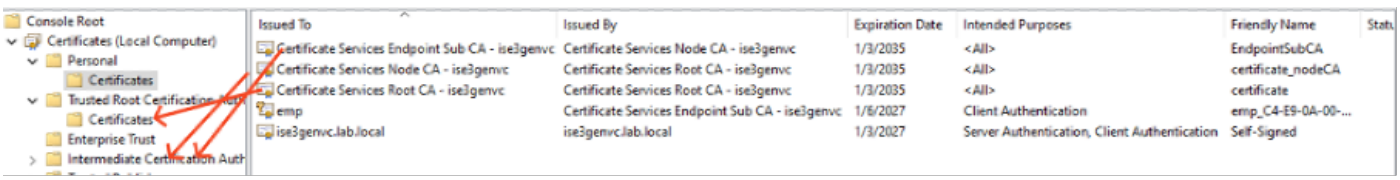
2.4. Zertifikate der Stammzertifizierungsstelle: Wechsel zu vertrauenswürdigen Stammzertifizierungsstellen

2.5. Zertifikate der Zwischen-Zertifizierungsstelle: Wechsel zu Zertifizierungsstellen für mittlere Unternehmen

2.6. Persönliche Zertifikate: Lassen Sie das Dokument im persönlichen Ordner.



Speichern von Zertifikaten im persönlichen Ordner

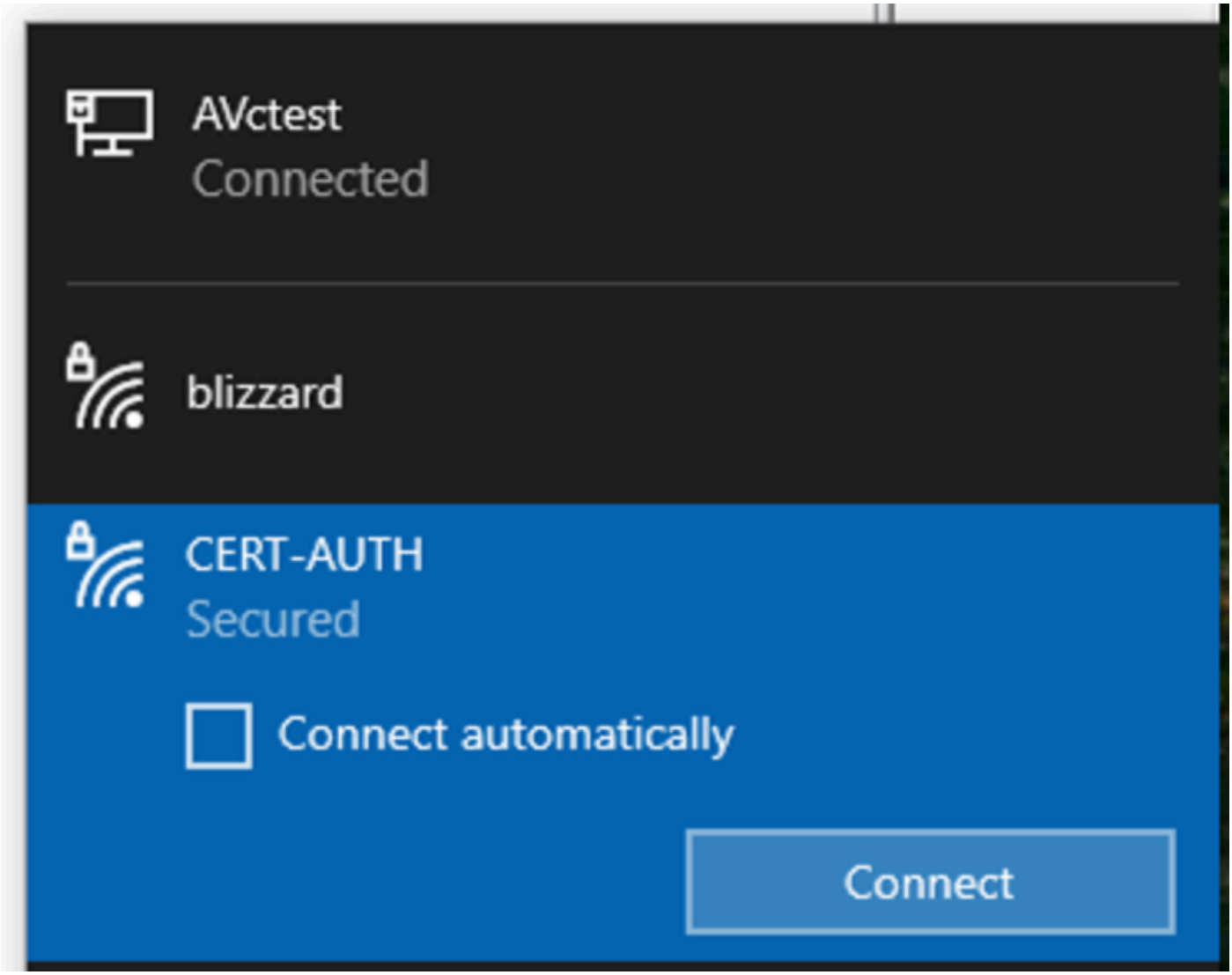


Verschieben von Zertifikaten in ihren Läden

Verbinden des Windows-Computers

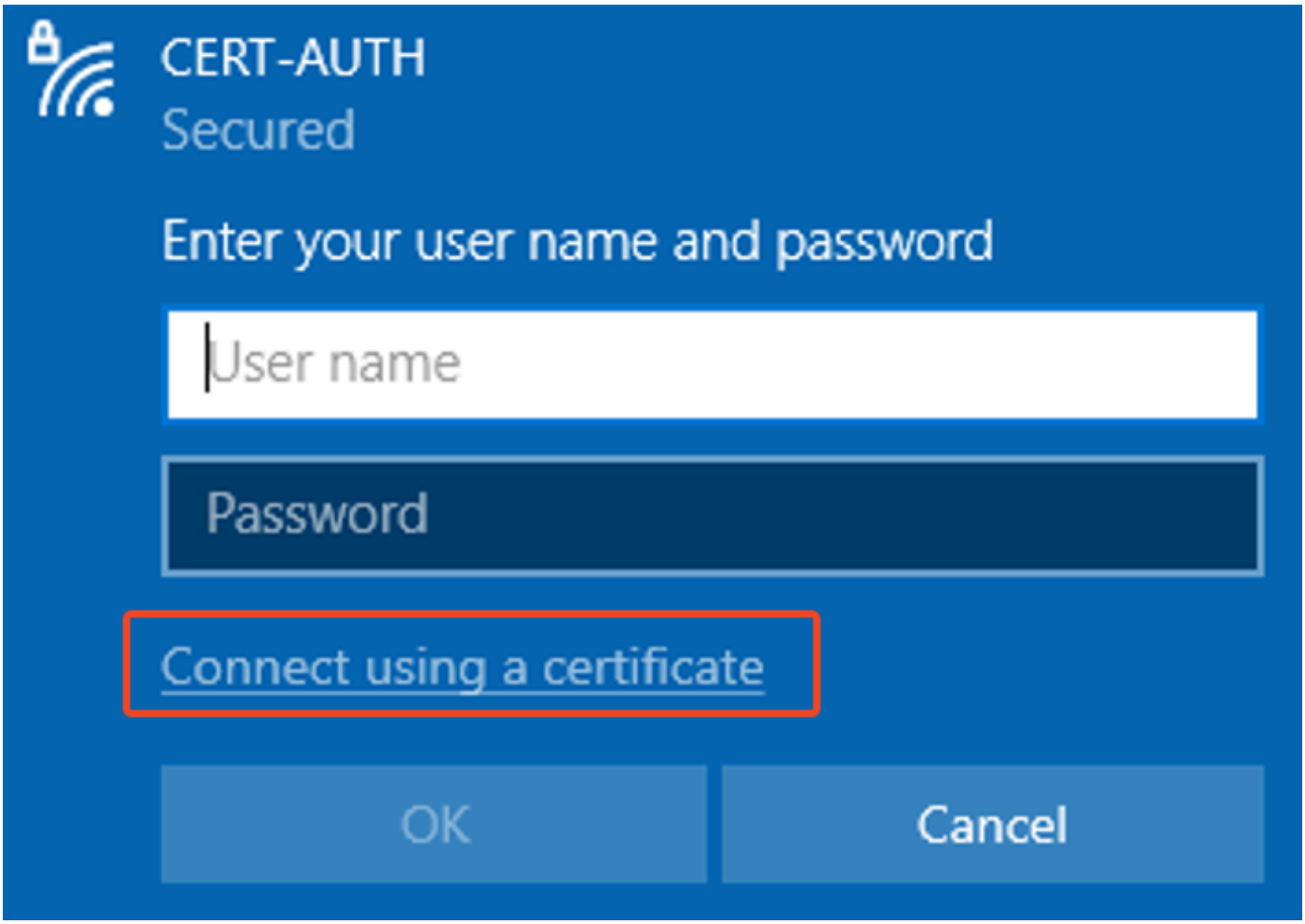
Nachdem die Zertifikate in die richtigen Läden verschoben wurden, führen Sie die folgenden Schritte aus, um eine Verbindung mit dem WLAN herzustellen:

1. Klicken Sie auf das Netzwerk-Symbol in der Taskleiste, um verfügbare Wireless-Netzwerke anzuzeigen.
2. Suchen Sie das WLAN, mit dem Sie eine Verbindung herstellen möchten, und klicken Sie darauf.
3. Klicken Sie auf Verbinden, und fahren Sie mit allen weiteren Aufforderungen fort, um den Verbindungsvorgang mit dem Zertifikat für die Authentifizierung abzuschließen.



Herstellen einer Verbindung mit dem Wireless-Netzwerk

Wenn Sie während des Verbindungsprozesses mit dem WLAN dazu aufgefordert werden, wählen Sie die Option Verbindung über ein Zertifikat herstellen aus.



Zertifikat als Anmeldeinformationen verwenden

Dadurch können Sie mithilfe des Zertifikats erfolgreich eine Verbindung zum Wireless-Netzwerk herstellen.

```
C:\>netsh wlan  show interface

There is 1 interface on the system:

    Name                   : Wi-Fi 3
    Description            : TP-Link Wireless USB Adapter
    GUID                   : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
    Physical address       : 24:2f:d0:da:a5:63
    State                  : connected
    SSID                   : CERT-AUTH
    BSSID                  : a4:88:73:9e:8d:af
    Network type           : Infrastructure
    Radio type             : 802.11ac
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 36
    Receive rate (Mbps)    : 360
    Transmit rate (Mbps)   : 360
    Signal                 : 100%
    Profile                : CERT-AUTH

    Hosted network status  : Not available


C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
    EAP type               : Microsoft: Smart Card or other certificate
```

Wireless-Profil überprüfen

Überprüfung

Vergewissern Sie sich, dass das WLAN vom WLC übertragen wird:

<#root>

```
POD6_9800#show wlan summ
Number of WLANs: 2
ID Profile Name SSID Status Security
-------------------------------------------------------------------------------------------------
```

17

CERT-AUTH

CERT-AUTH

UP [WPA2][802.1x][AES]

Stellen Sie sicher, dass der Access Point am WLC betriebsbereit ist:

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-------------------------------------------------------------------------------------------------
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

Stellen Sie sicher, dass der Access Point das WLAN überträgt:

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
------------------------
17 a488.739e.8da0

POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
------------------------
```

17

```
 a488.739e.8daf
```

Über EAP-TLS verbundener Client:

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----------------------------------------------------------------------------------------------------
242f.d0da.a563 AP1 WLAN
```

17

```
 IP Learn 11ac
```

Dot1x

```
 Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
```

Wireless LAN Network Name (SSID): CERT-AUTH

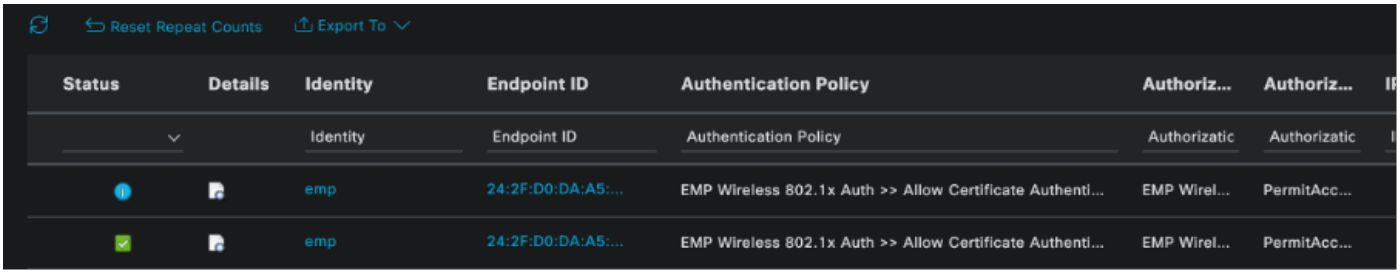
```
BSSID : a488.739e.8daf
```

EAP Type : EAP-TLS

```
VLAN : 2124
Multicast VLAN : 0
```

VLAN : 2124

Cisco Radius ISE Live-Protokolle:

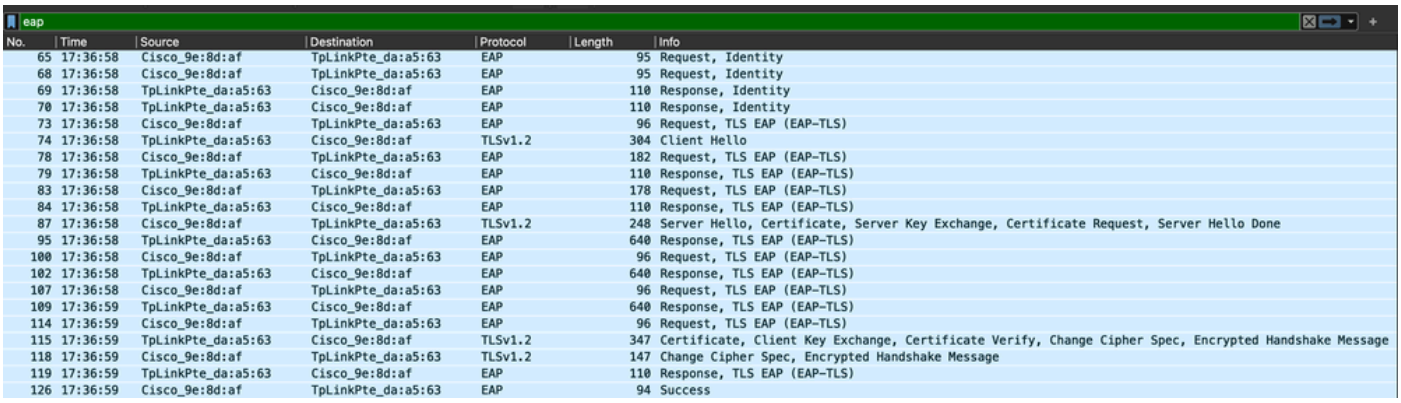


ISE Radius-Live-Protokolle

Detaillierter Authentifizierungstyp:

Detaillierte ISE-Protokolle

WLC EPC Capture mit EAP-TLS-Paketen:



eap

No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

WLC-Erfassung mit EAP-Transaktion

- Die Paketnummer 87 entspricht Schritt 8 des zu Beginn des Dokuments beschriebenen EAP-TLS-Flusses.
- Die Paketnummer 115 entspricht Schritt 9 im zu Beginn des Dokuments beschriebenen EAP-TLS-Flow.
- Die Paketnummer 118 entspricht Schritt 10 des zu Beginn des Dokuments beschriebenen EAP-TLS-Flusses.

Radio Active (RA) Trace mit Client-Verbindung: Diese RA-Verfolgung wird gefiltert, um einige der relevanten Zeilen der Authentifizierungstransaktion anzuzeigen.

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (debug) Verschlüsselte DTLS-Nachricht wird gesendet. Ziel IP 10.78.8.78[5256], Länge 499
2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Sendezugriffsanforderung an 10.106.33.23 1812 id 0/25, len 390
2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS empfangen von ID 1812/25 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Gesendetes EAPOL-Paket - Version 3, EAPOL-Typ EAP, Nutzlastlänge 6, EAP AP-Type = EAP-TLS
2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Empfangenes EAPOL-Paket - Version 1,EAPOL-Typ EAP, Nutzlastlänge 20 4, EAP-Type = EAP-TLS
2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Sendezugriffsanforderung an 10.106.33.23 1812 id 0/26, len 663
2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS empfangen von ID 1812/26 10.106.33.23 0, Access-Challenge, len 1135
2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Gesendetes EAPOL-Paket - Version 3,EAPOL-Typ EAP, Nutzlastlänge 10 12, EAP-Type = EAP-TLS
2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Empfangenes EAPOL-Paket - Version 1,EAPOL-Typ EAP, Nutzlastlänge 6, EAP AP-Type = EAP-TLS
2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Sendezugriffsanforderung an 10.106.33.23 1812 id 0/27, len 465
2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS empfangen von

ID 1812/27 10.106.33.23 0, Access-Challenge, len 1131
2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Gesendetes EAPOL-Paket - Version 3,EAPOL-Typ EAP, Nutzlastlänge 10 08, EAP-Type = EAP-TLS
2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Empfangenes EAPOL-Paket - Version 1,EAPOL-Typ EAP, Nutzlastlänge 6, EAP AP-Type = EAP-TLS
2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Sendezugriffsanforderung an 10.106.33.23 1812 id 0/28, len 465
2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS empfangen von id 1812/28 10.106.33.23 0, Access-Challenge, len 275
2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Gesendetes EAPOL-Paket - Version 3,EAPOL-Typ EAP, Nutzlastlänge 15 8, EAP-Type = EAP-TLS
2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Empfangenes EAPOL-Paket - Version 1,EAPOL-Typ EAP, Nutzlastlänge 14 92, EAP-Type = EAP-TLS
2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Sendezugriffsanforderung an 10.106.33.23 1812 id 0/29, len 1961
2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS empfangen von id 1812/29 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Gesendetes EAPOL-Paket - Version 3, EAPOL-Typ EAP, Nutzlastlänge 6, EAP AP-Type = EAP-TLS
2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Empfangenes EAPOL-Paket - Version 1,EAPOL-Typ EAP, Nutzlastlänge 14 92, EAP-Type = EAP-TLS
2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Sendezugriffsanforderung an 10.106.33.23 1812 id 0/30, len 1961
2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS empfangen von id 1812/30 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Gesendetes EAPOL-Paket - Version 3, EAPOL-Typ EAP, Nutzlastlänge 6, EAP AP-Type = EAP-TLS
2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Empfangenes EAPOL-Paket - Version 1,EAPOL-Typ EAP, Nutzlastlänge 14 92, EAP-Type = EAP-TLS
2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Sendezugriffsanforderung an 10.106.33.23 1812 id 0/31, len 1961
2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS empfangen von id 1812/31 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Gesendetes EAPOL-Paket - Version 3, EAPOL-Typ EAP, Nutzlastlänge 6, EAP AP-Type = EAP-TLS
2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Empfangenes EAPOL-Paket - Version 1,EAPOL-Typ EAP, Nutzlastlänge 24

7, EAP-Type = EAP-TLS
2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Sendezugriffsanforderung an 10.106.33.23 1812 id 0/32, len 706
2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS empfangen von id 1812/32 10.106.33.23 0, Access-Challenge, len 174
2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Gesendetes EAPOL-Paket - Version 3,EAPOL-Typ EAP, Nutzlastlänge 57 EAP-Type = EAP-TLS
2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Empfangenes EAPOL-Paket - Version 1,EAPOL-Typ EAP, Nutzlastlänge 6, EAP AP-Type = EAP-TLS
2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Sendezugriffsanforderung an 10.106.33.23 1812 id 0/33, len 465
2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS empfangen von id 1812/33 10.106.33.23 0, Access-Accept, len 324
2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Ausgelöstes Identitätsaktualisierungsereignis für die EAP-Methode EAP-TLS

Fehlerbehebung

Außer den üblichen Fehlerbehebungsverfahren für Wireless 802.1x gibt es für dieses Problem keine weiteren spezifischen Schritte:

1. Client RA Trace-Debugs durchführen, um den Authentifizierungsprozess zu überprüfen
2. Führen Sie eine WLC-EPC-Erfassung durch, um die Pakete zwischen dem Client, dem WLC und dem RADIUS-Server zu untersuchen.
3. Überprüfen Sie die ISE-Live-Protokolle, um sicherzustellen, dass die Anforderung mit der richtigen Richtlinie übereinstimmt.
4. Überprüfen Sie auf dem Windows-Endpunkt, ob das Zertifikat korrekt installiert ist und die gesamte Vertrauenskette vorhanden ist.

Referenzen

- Häufig gestellte Fragen zum Zertifikatbereitstellungsportal, Version 3.2
- Kenntnis der internen Services der ISE-Zertifizierungsstelle
- Verständnis und Konfiguration von EAP-TLS mit einem WLC und der ISE

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.