Verständnis und Konfiguration von EAP-TLS mit einem WLC und der ISE

Inhalt

Einleitung

In diesem Dokument wird die Einrichtung eines Wireless Local Area Network (WLAN) mit 802.1X und Extensible Authentication Protocol EAP-TLS beschrieben.

Voraussetzungen

Anforderungen

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

- 802.1X-Authentifizierungsprozess
- Zertifikate

Verwendete Komponenten

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

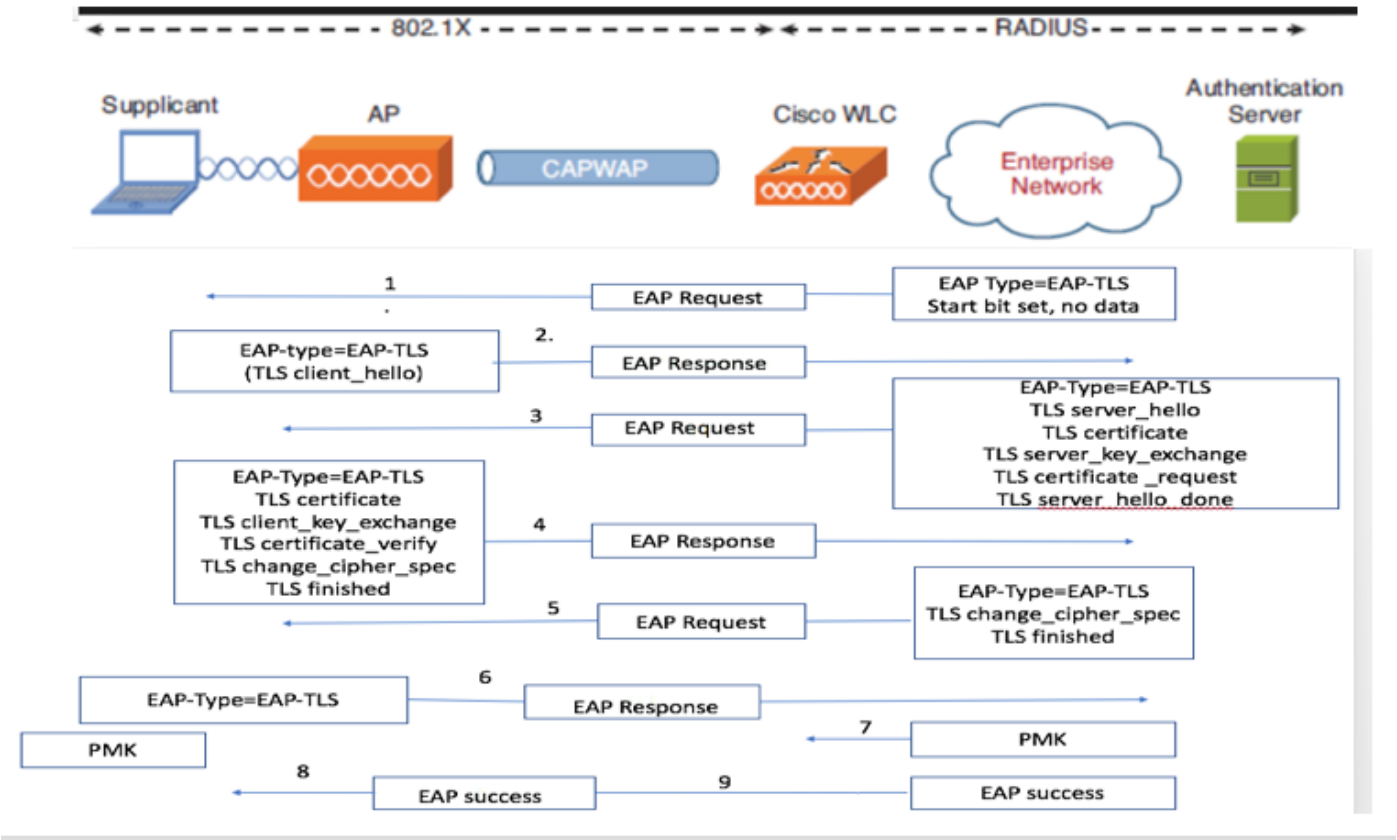
Versionen:

- WLC 3504 Version 8.10
- Identity Services Engine (ISE) Version 2.7

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 verstehen.

Hintergrundinformationen

EAP-TLS-Fluss



Schritte im EAP-TLS-Fluss

1. Der Wireless-Client wird mit dem Access Point (AP) verknüpft. AP erlaubt dem Client an dieser Stelle nicht, Daten zu senden und sendet eine Authentifizierungsanforderung.Der Supplicant antwortet dann mit einer EAP-Response-Identität. Der WLC übermittelt dann die Benutzer-ID-Informationen an den Authentifizierungsserver. Der RADIUS-Server antwortet mit einem EAP-TLS-Startpaket auf den Client. Die EAP-TLS-Konversation beginnt an diesem Punkt.
2. Der Peer sendet eine EAP-Antwort zurück an den Authentifizierungsserver, die eine "client_hello"-Handshake-Nachricht enthält, eine Chiffre, die auf NULL gesetzt ist
3. 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.
```

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

```
Certificate ¬ Server can validate to verify that it is trusted.

client_key_exchange

certificate_verify ¬ Verifies the server is trusted

change_cipher_spec

TLS finished
```

5.Nachdem der Client erfolgreich authentifiziert wurde, antwortet der RADIUS-Server mit einer Access-Challenge, die die Meldung "change_cipher_spec" und den Handshake-Abschluss enthält.

6. Wenn er dies erhält, überprüft der Client den Hash, um den Radius-Server zu authentifizieren.

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

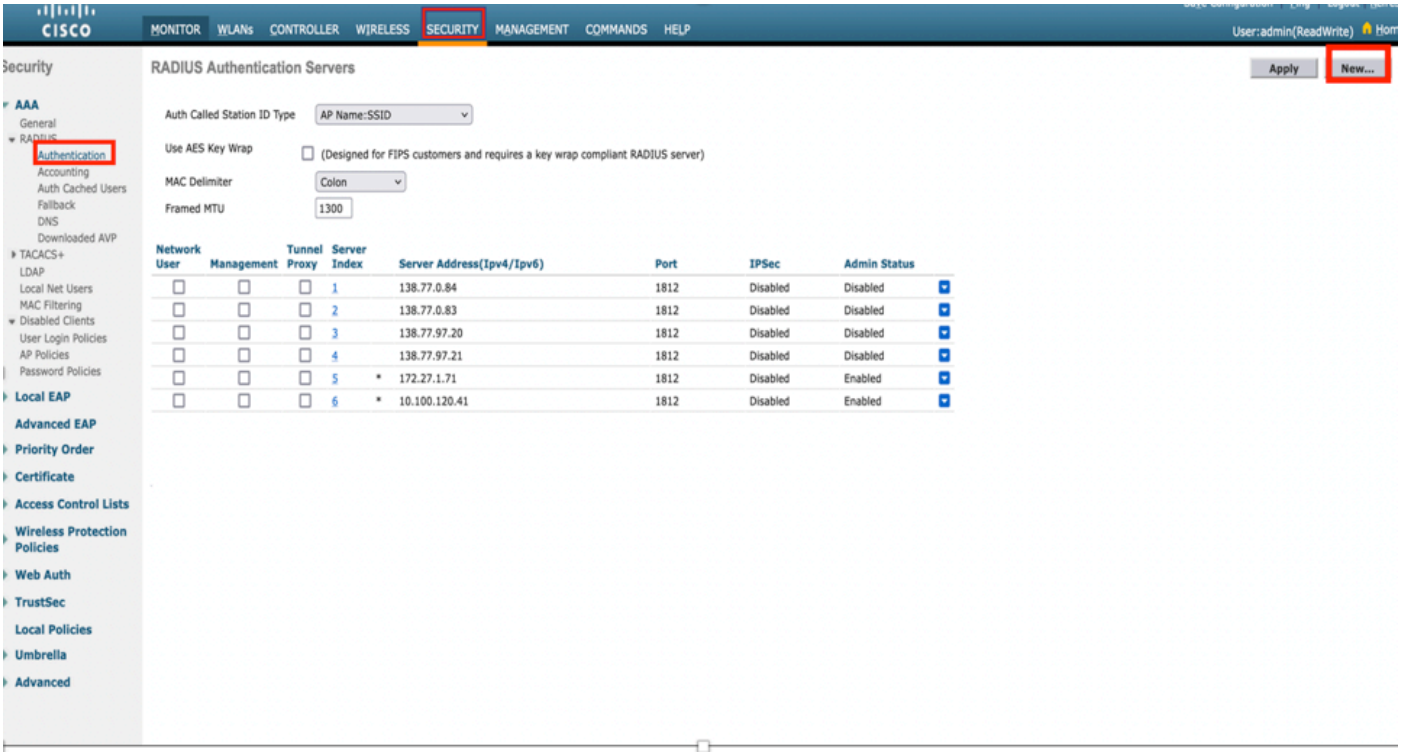
8/9.EAP-Success wird schließlich vom Server an den Authentifikator gesendet, der dann an den Supplicant weitergeleitet wird.

An diesem Punkt kann der EAP-TLS-fähige Wireless-Client auf das Wireless-Netzwerk zugreifen.

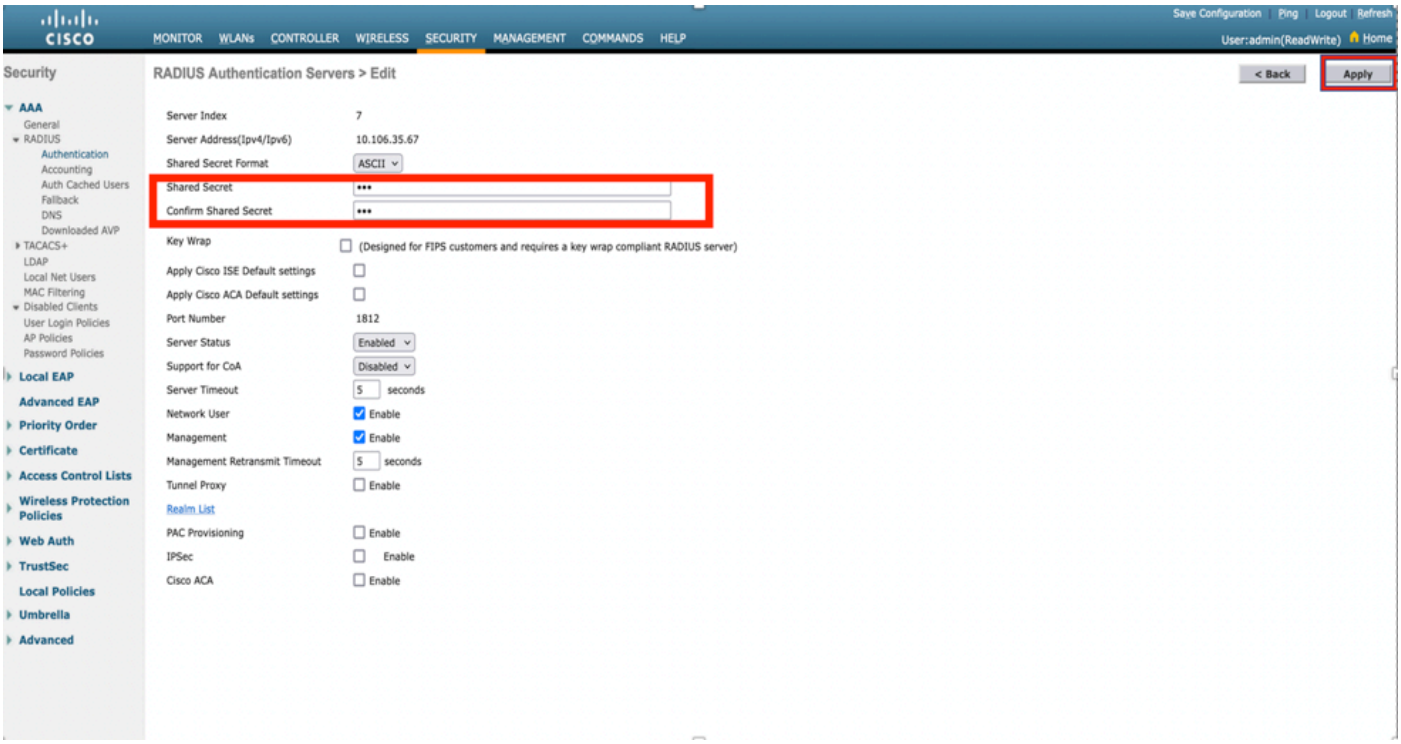
Konfigurieren

Cisco Wireless LAN-Controller

Schritt 1: Im ersten Schritt wird der RADIUS-Server auf dem Cisco WLC konfiguriert. Um einen RADIUS-Server hinzuzufügen, navigieren Sie zu **Security > RADIUS > Authentication**. Klicken Sie wie im Bild dargestellt auf **Neu**.



Schritt 2: Geben Sie hier die IP-Adresse und den gemeinsamen geheimen Schlüssel <Kennwort> ein, der zur Validierung des WLC auf der ISE verwendet wird. Klicken Sie auf **Apply**, um fortzufahren, wie im Bild dargestellt.

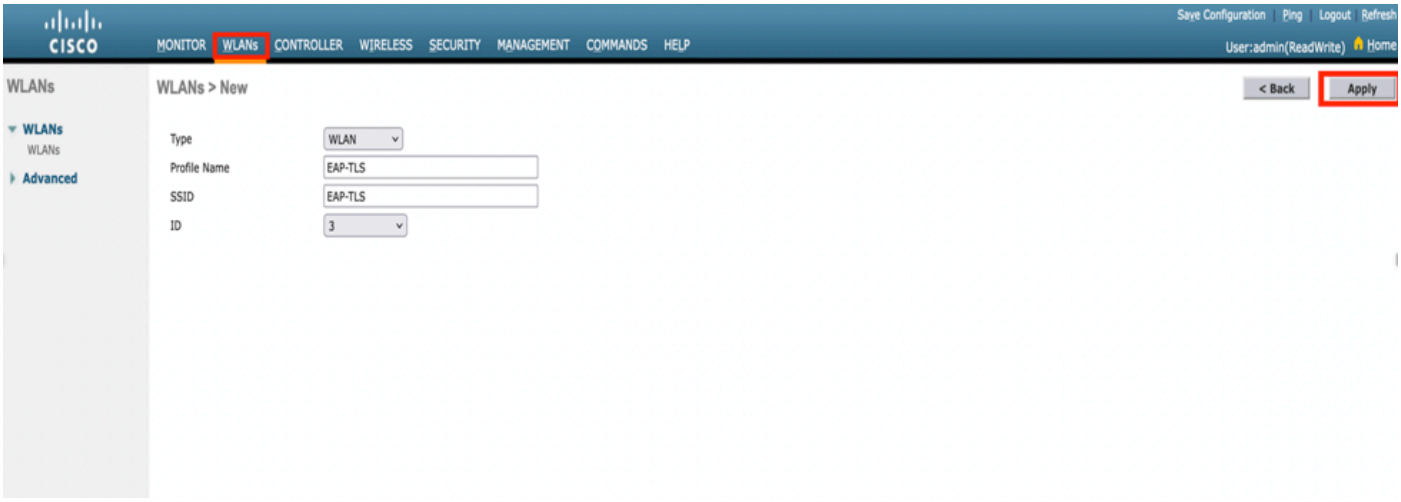


Schritt 3: Erstellen eines WLAN für die RADIUS-Authentifizierung

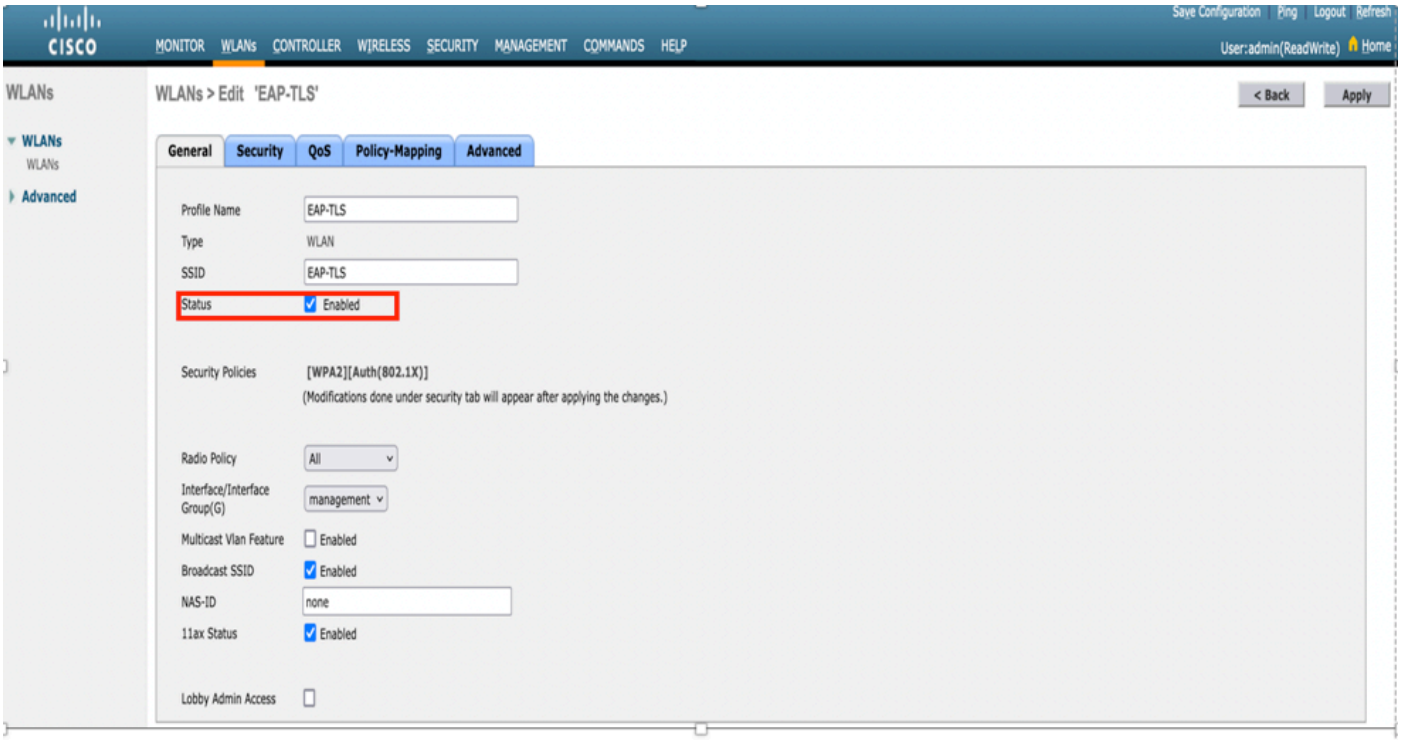
Jetzt können Sie ein neues WLAN erstellen und es so konfigurieren, dass es den WPA-Enterprise-Modus verwendet, sodass es RADIUS für die Authentifizierung verwenden kann.

Schritt 4. Wählen Sie **WLANs** aus dem Hauptmenü, wählen Sie **Create New** und klicken Sie auf **Go** wie in der Abbildung dargestellt.

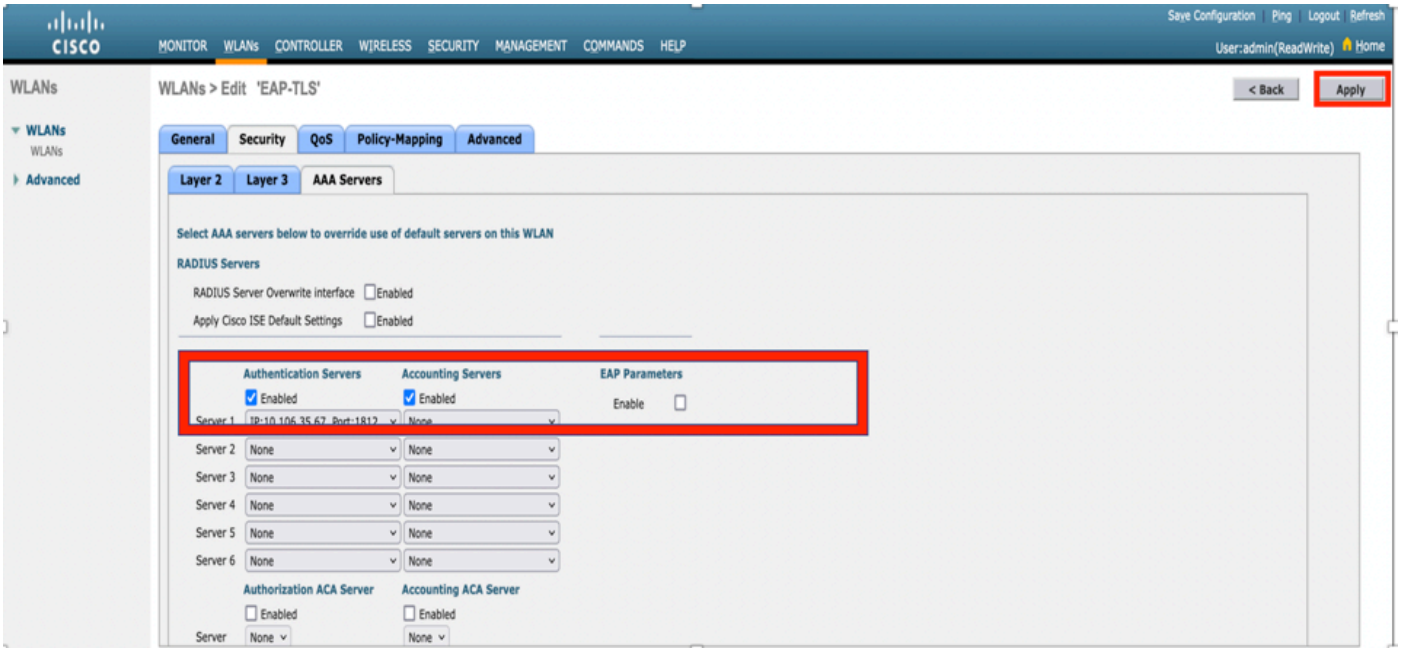
Schritt 5: Benennen Sie das neue WLAN **EAP-TLS**. Klicken Sie auf **Apply**, um fortzufahren, wie im Bild dargestellt.



Schritt 6: Klicken Sie auf **Allgemein**, und stellen Sie sicher, dass der Status **aktiviert** ist. Die Standard-Sicherheitsrichtlinien sind 802.1X-Authentifizierung und WPA2, wie im Bild gezeigt.



Schritt 7: Navigieren Sie nun zur Registerkarte **Security > AAA Servers** (**Sicherheit > AAA-Server**), und wählen Sie den RADIUS-Server aus, den Sie gerade konfiguriert haben und wie im Bild dargestellt.



Anmerkung: Bevor Sie fortfahren, sollten Sie überprüfen, ob Sie vom WLC aus auf den RADIUS-Server zugreifen können. RADIUS verwendet den UDP-Port 1812 (für die Authentifizierung), sodass Sie sicherstellen müssen, dass dieser Datenverkehr nicht irgendwo im Netzwerk blockiert wird.

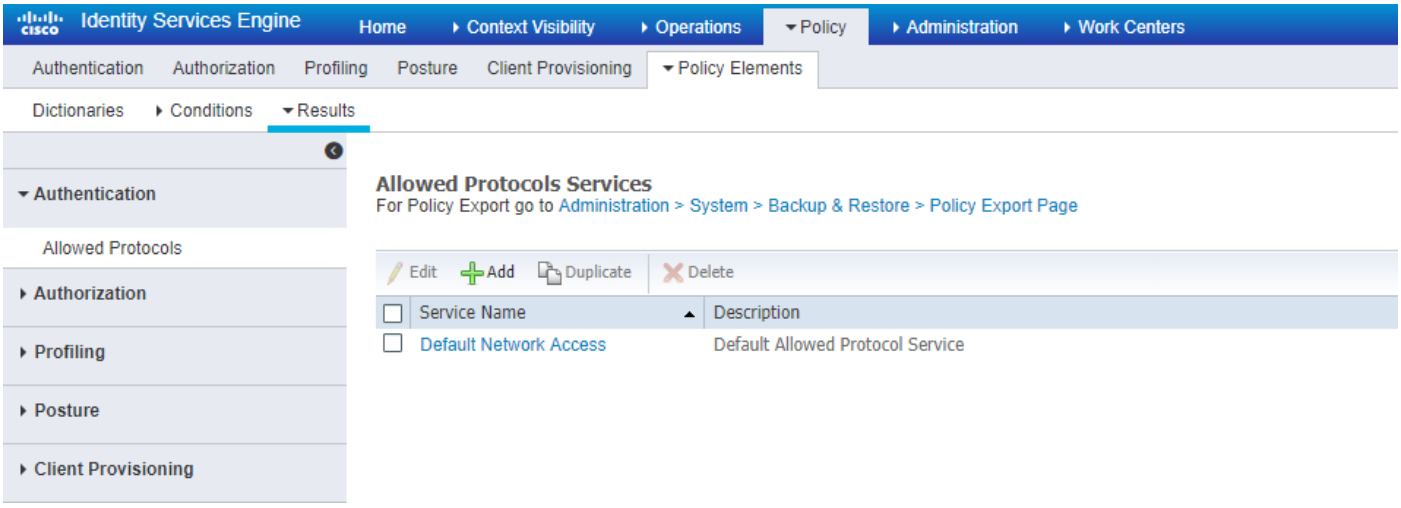
ISE mit Cisco WLC

EAP-TLS-Einstellungen

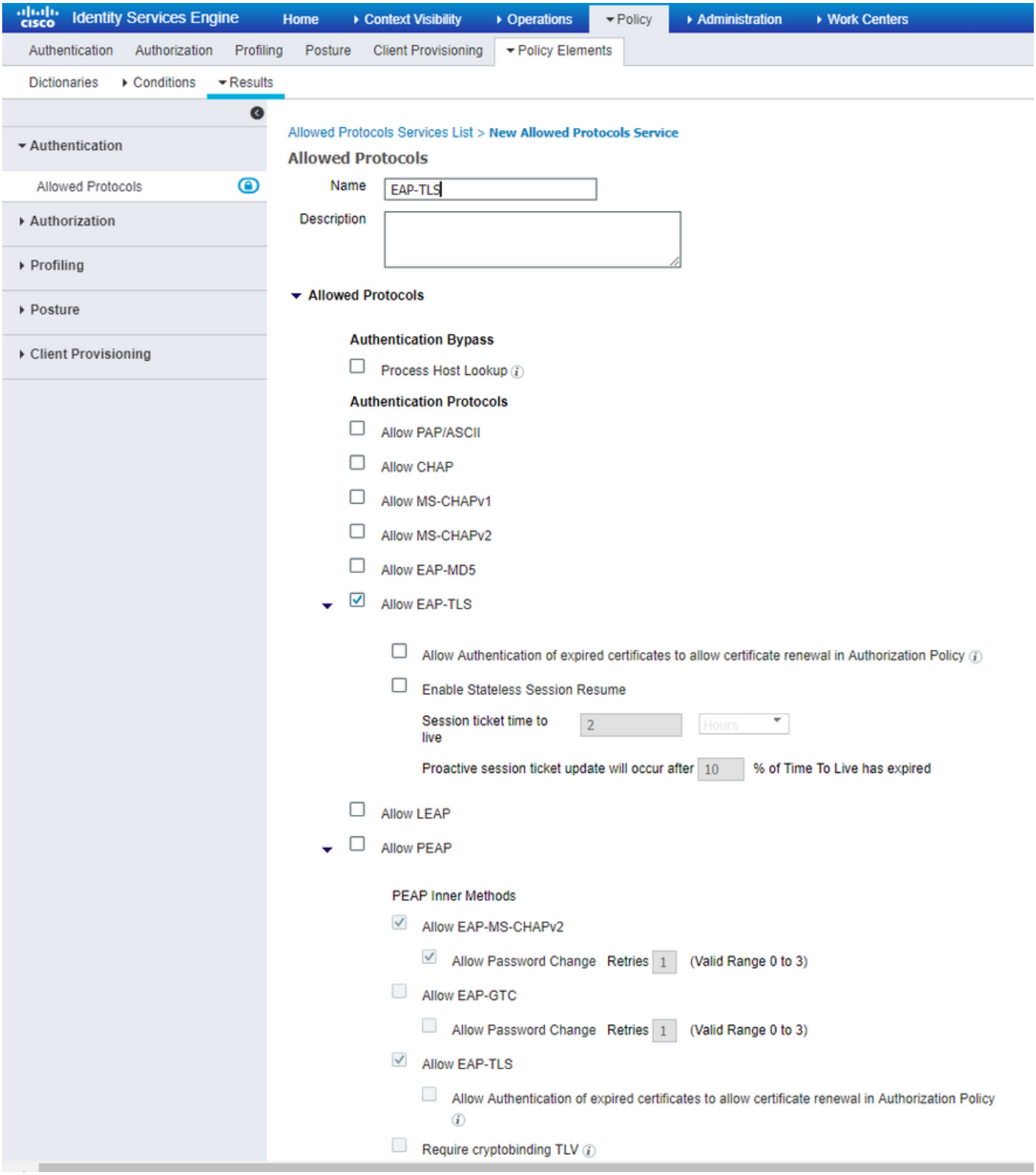
Um die Richtlinie zu erstellen, müssen Sie die Liste der zulässigen Protokolle erstellen, die in unserer Richtlinie verwendet werden dürfen. Da eine dot1x-Richtlinie geschrieben wurde, geben Sie den zulässigen EAP-Typ basierend auf der Konfiguration der Richtlinie an.

Wenn Sie die Standardeinstellung verwenden, lassen Sie die meisten EAP-Typen für die Authentifizierung zu, die nicht bevorzugt werden, wenn Sie den Zugriff auf einen bestimmten EAP-Typ sperren müssen.

Schritt 1: Navigieren Sie **zuRichtlinie > Richtlinienelemente > Ergebnisse > Authentifizierung > Zugelassene** Protokolle, und **klicken Sie auf Hinzufügen**, wie im Bild dargestellt.

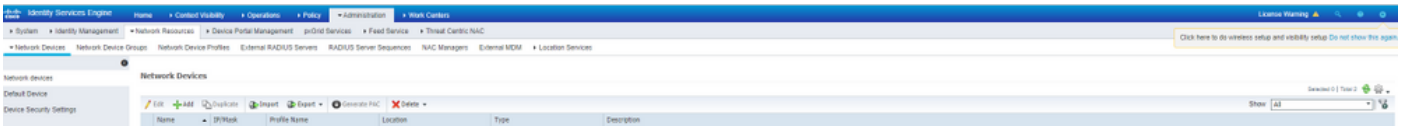


Schritt 2: In dieser Liste der zulässigen Protokolle können Sie den Namen der Liste eingeben. In diesem Fall ist das Kontrollkästchen **EAP-TLS zulassen** aktiviert, und andere Kontrollkästchen sind deaktiviert, wie im Bild gezeigt.

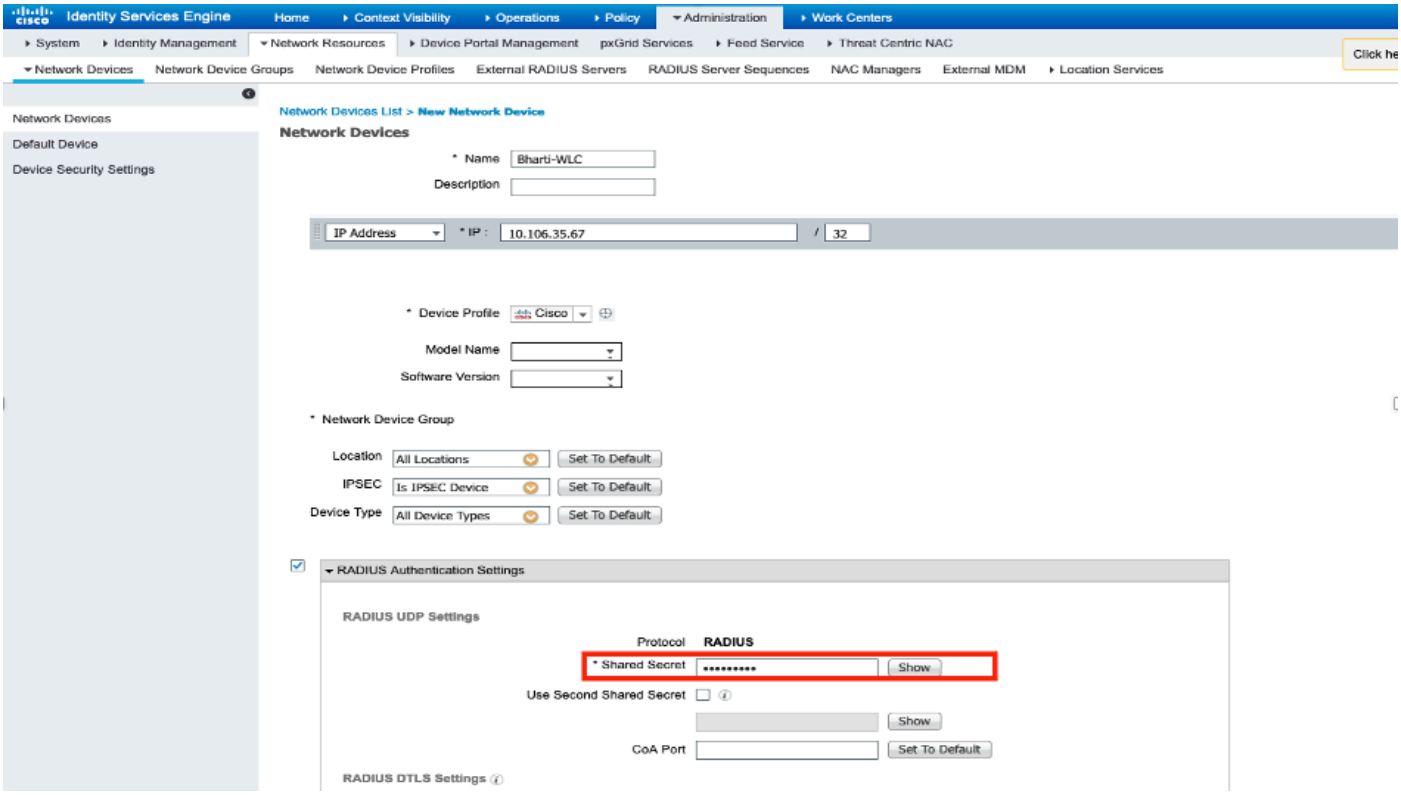


WLC-Einstellungen auf der ISE

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

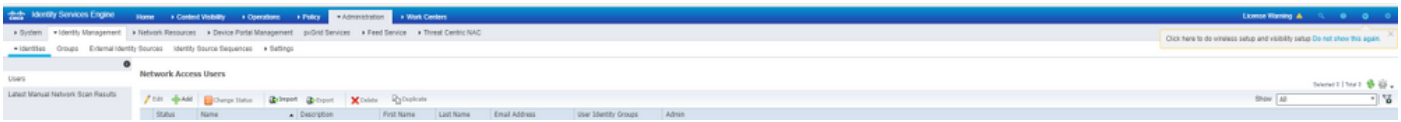


Schritt 2: Geben Sie die im Bild angezeigten Werte ein.

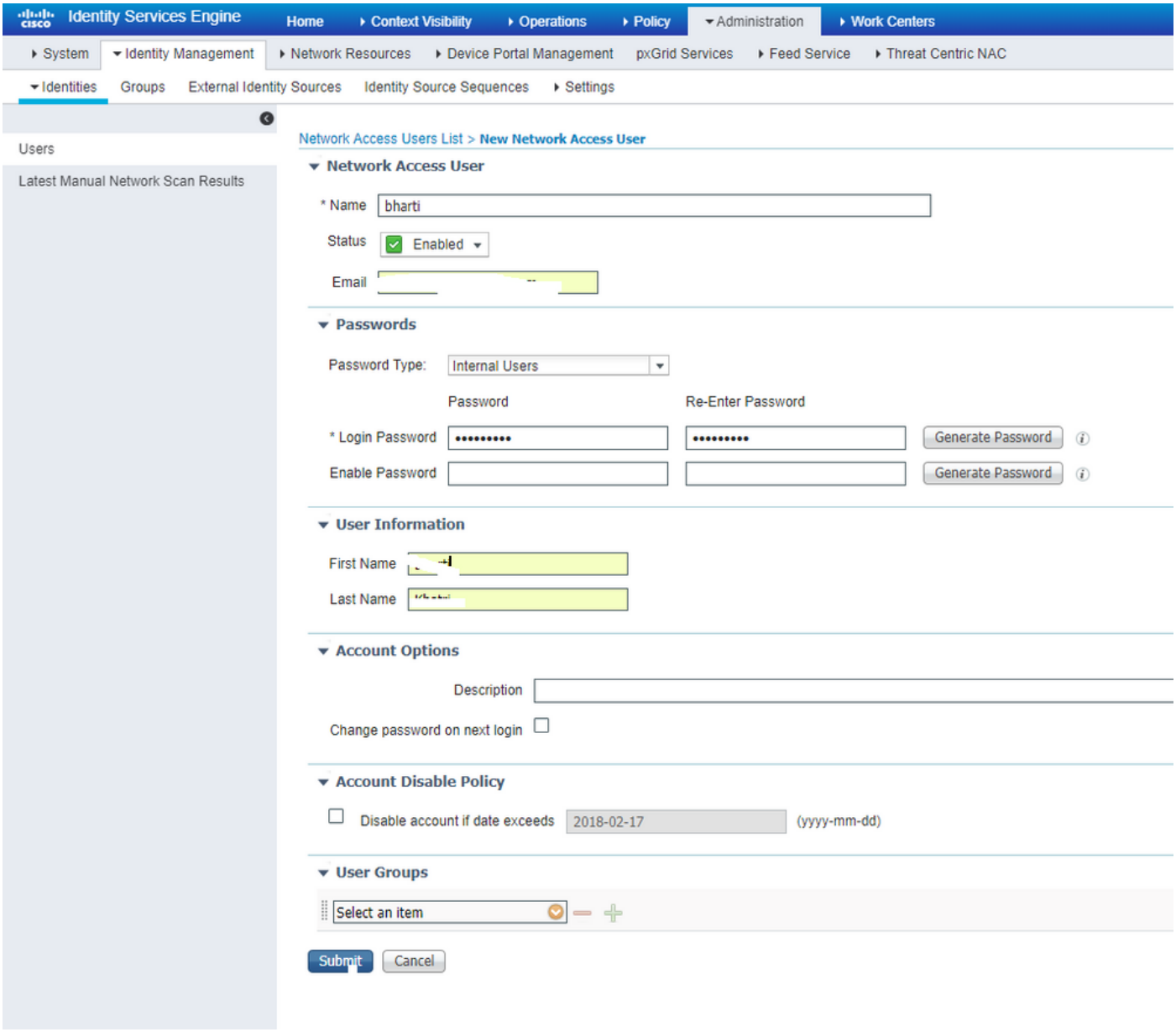


Neuen Benutzer auf ISE erstellen

Schritt 1: Navigieren Sie zu **Administration > Identity Management > Identities > Users > Add (Verwaltung > Identitätsverwaltung > Identitäten > Benutzer > Hinzufügen** wie im Bild dargestellt.



Schritt 2: Geben Sie die im Bild angezeigten Informationen ein.

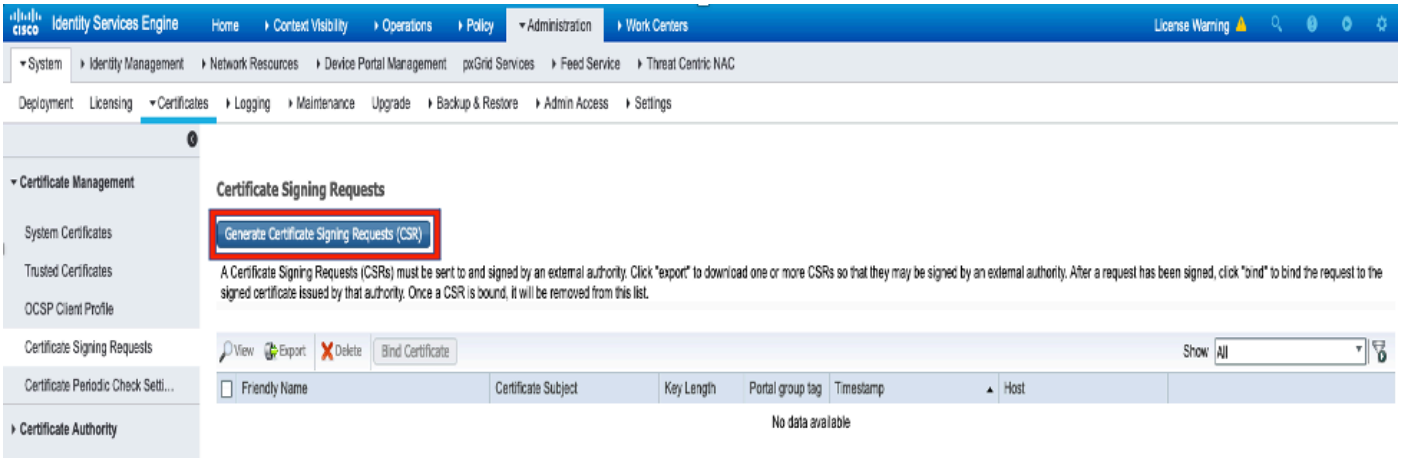


Zertifikat auf ISE vertrauen

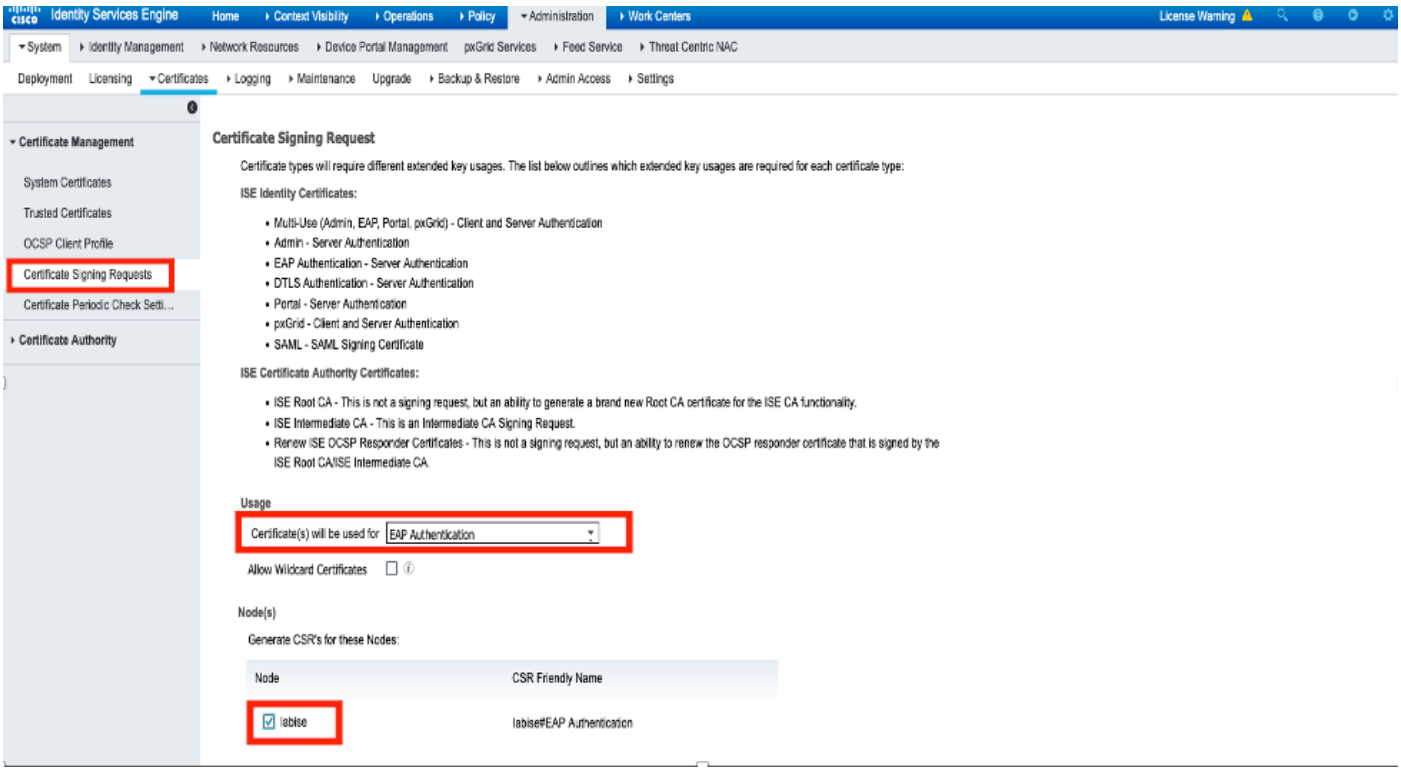
Schritt 1: Navigieren Sie zu **Administration > System > Certificates > Certificate Management > Trusted Certificates**.

Klicken Sie auf **Importieren**, um ein Zertifikat in die ISE zu importieren. Wenn Sie einen WLC hinzufügen und einen Benutzer auf der ISE erstellen, müssen Sie den wichtigsten Teil von EAP-TLS ausführen, d. h. dem Zertifikat auf der ISE vertrauen. Dafür müssen wir CSR erzeugen.

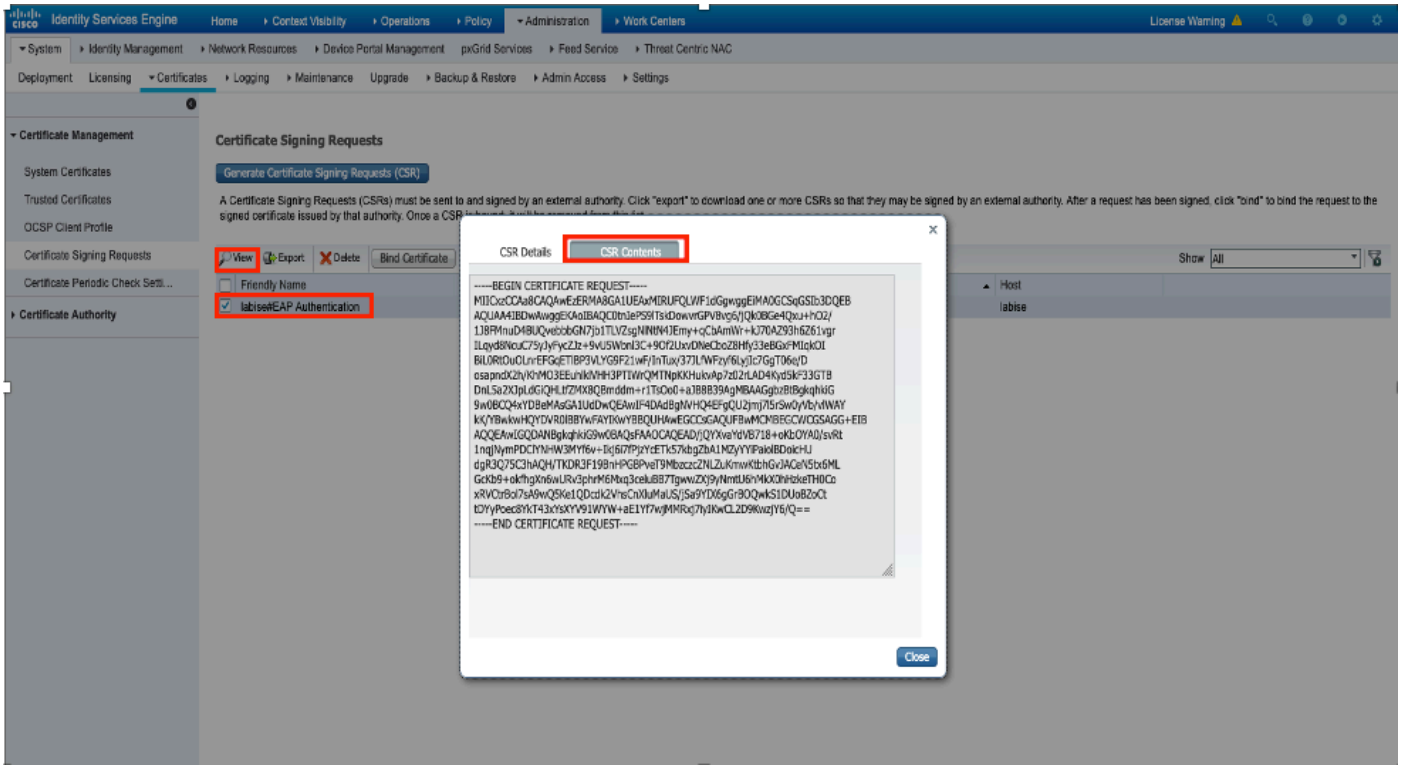
Schritt 2: Navigieren Sie zu **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR),** wie im Bild dargestellt.



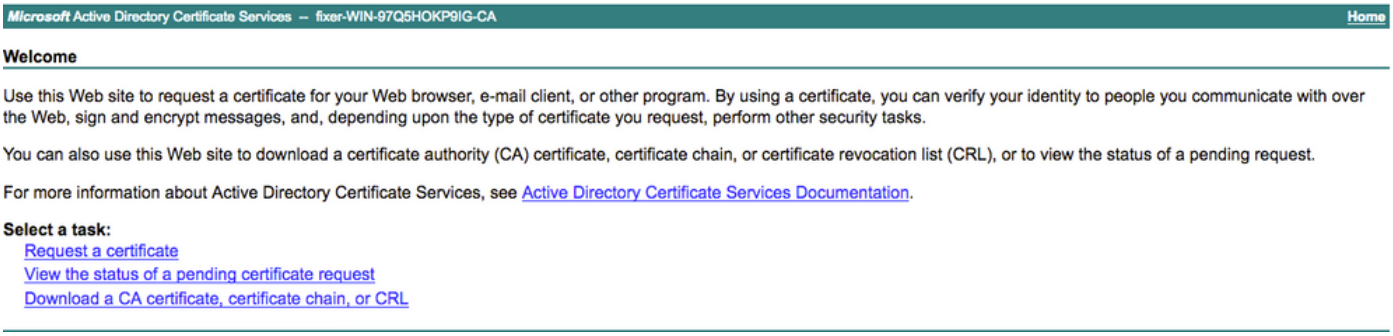
Schritt 3: Um die CSR-Anfrage zu erstellen, navigieren Sie zu **Usage (Verwendung)** und wählen Sie aus den **Zertifikaten, die für die** Dropdown-Optionen **verwendet werden, EAP Authentication (EAP-Authentifizierung)** aus, wie im Bild dargestellt.



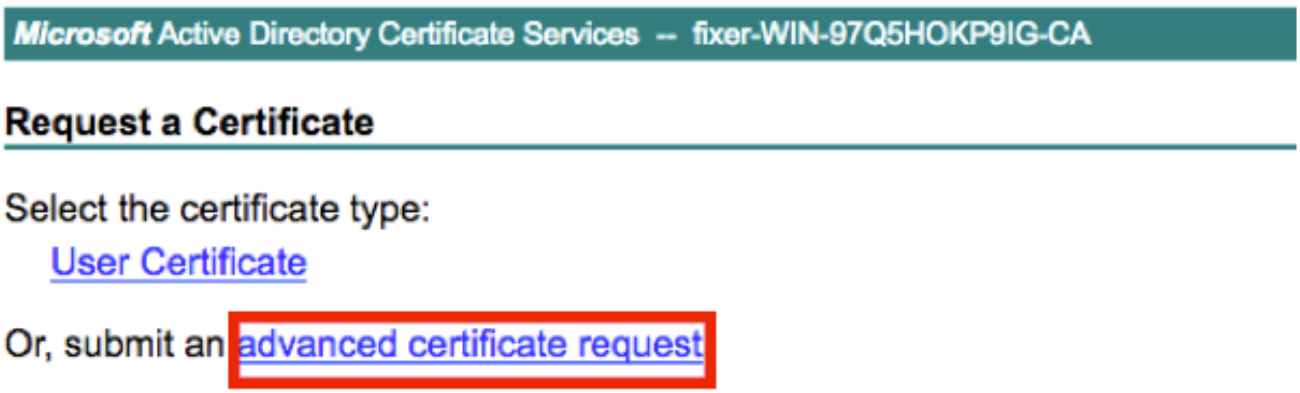
Schritt 4: Die von der ISE generierte CSR-Anfrage kann angezeigt werden. Klicken Sie auf **Ansicht**, wie im Bild dargestellt.



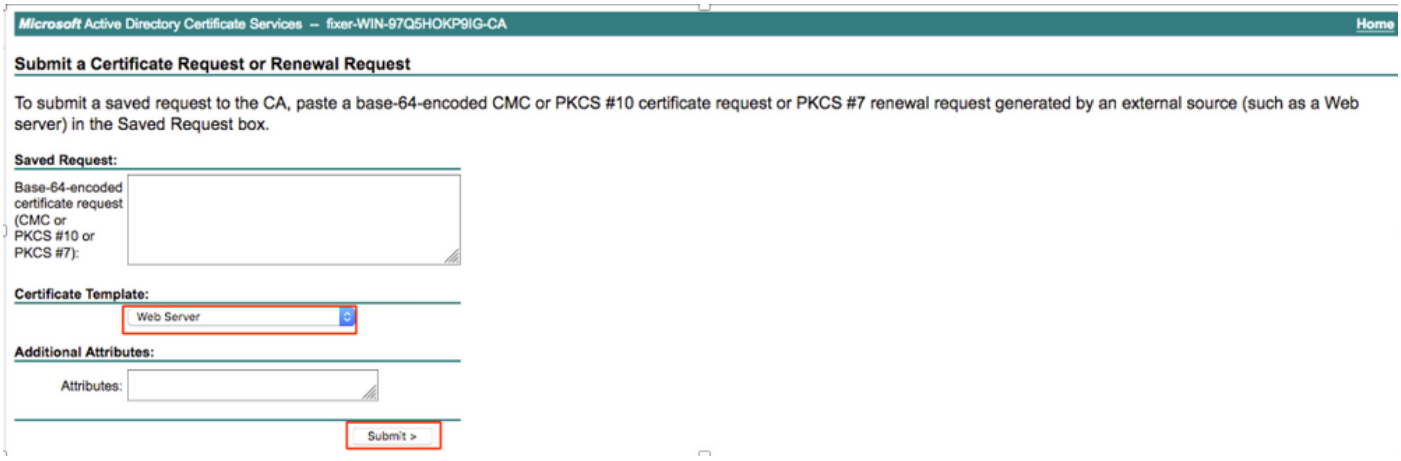
Schritt 5: Sobald der CSR generiert wurde, suchen Sie nach dem CA-Server und klicken Sie auf **Request a certificate** wie in der Abbildung dargestellt:



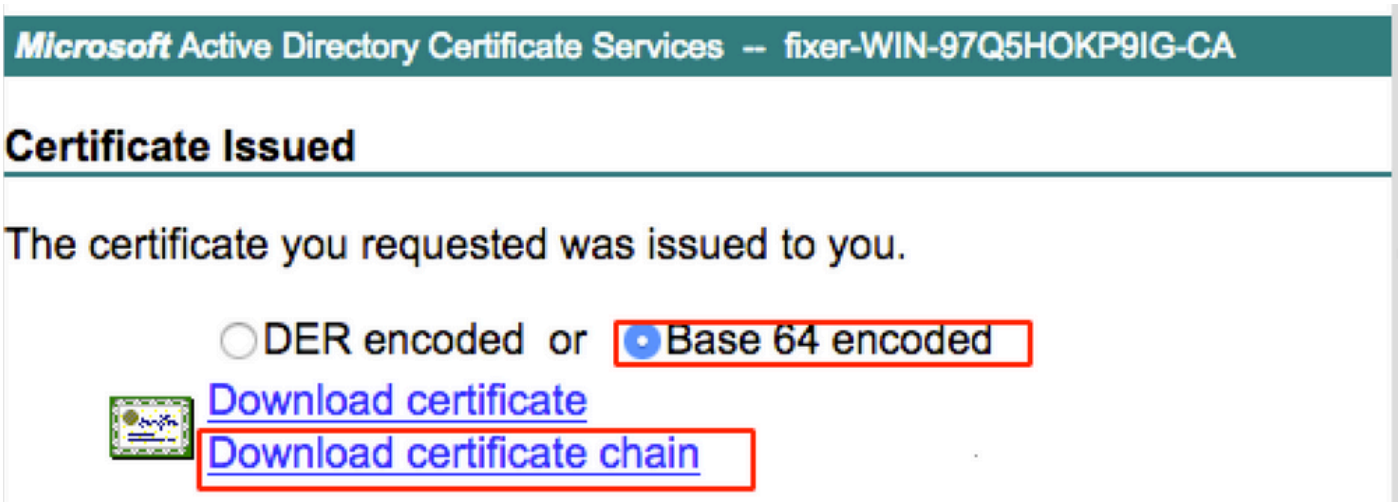
Schritt 6. Nachdem Sie ein Zertifikat angefordert haben, erhalten Sie Optionen für **Benutzerzertifikat** und **erweiterte Zertifikatanforderung.** Klicken Sie auf **Erweiterte Zertifikatanforderung,** wie im Bild dargestellt.



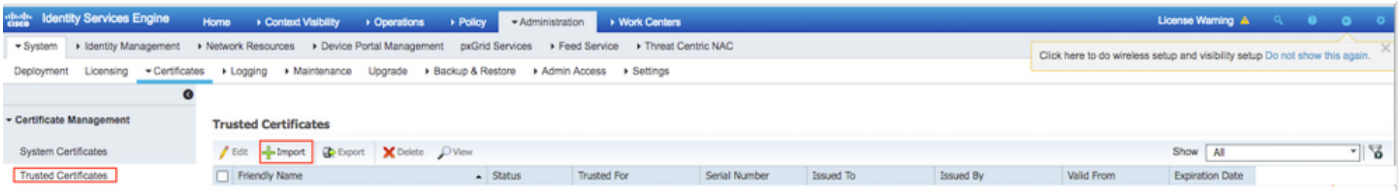
Schritt 7: Fügen Sie die in der **Base-64-kodierten Zertifikatsanforderung** erzeugte CSR ein. Aus der **Zertifikatvorlage:** Wählen Sie **Web Server** aus, und klicken Sie auf **Submit (Senden)**, wie im Bild dargestellt.

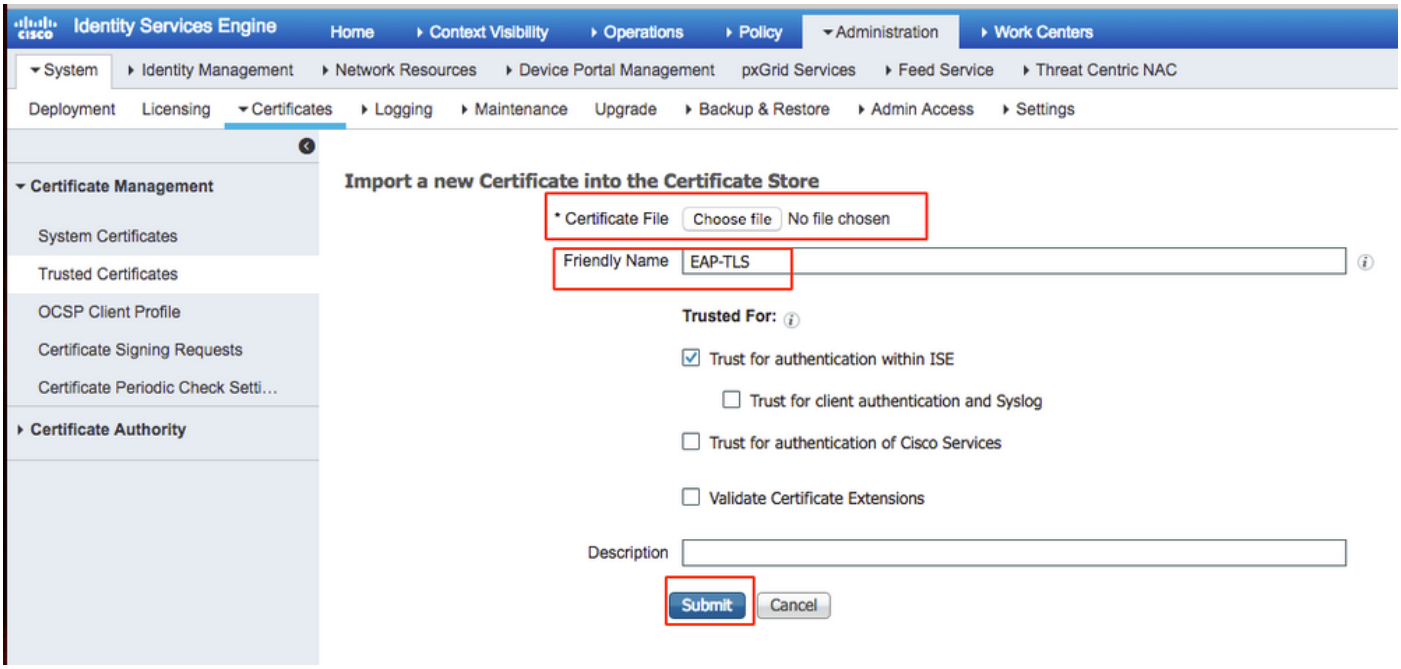


Schritt 8. Sobald Sie auf **Senden** klicken, erhalten Sie die Option, den Typ des Zertifikats auszuwählen, **Base-64 verschlüsselt** auszuwählen und auf **Download certificate chain** klicken, wie im Bild gezeigt.

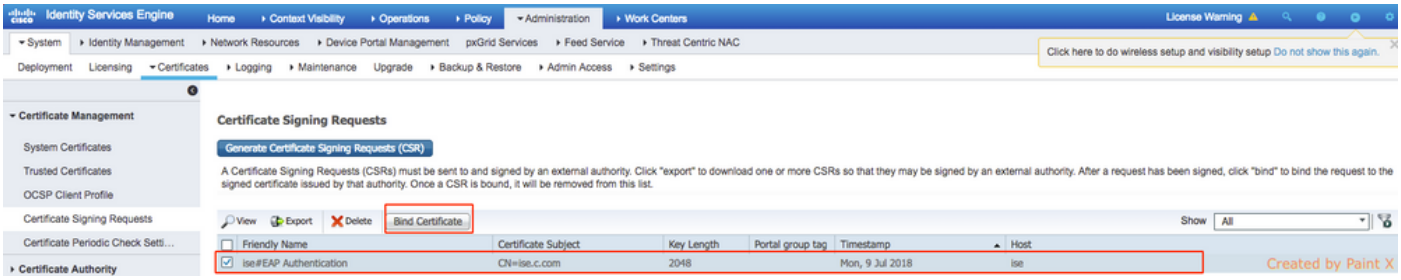


Schritt 9: Der Zertifikatsdownload für den ISE-Server ist abgeschlossen. Sie können das Zertifikat extrahieren, das Zertifikat enthält zwei Zertifikate, ein Stammzertifikat und ein anderes Zwischenprodukt. Das Stammzertifikat kann importiert werden unter **Administration > Certificates > Trusted Certificates > Import** wie in den Bildern dargestellt.

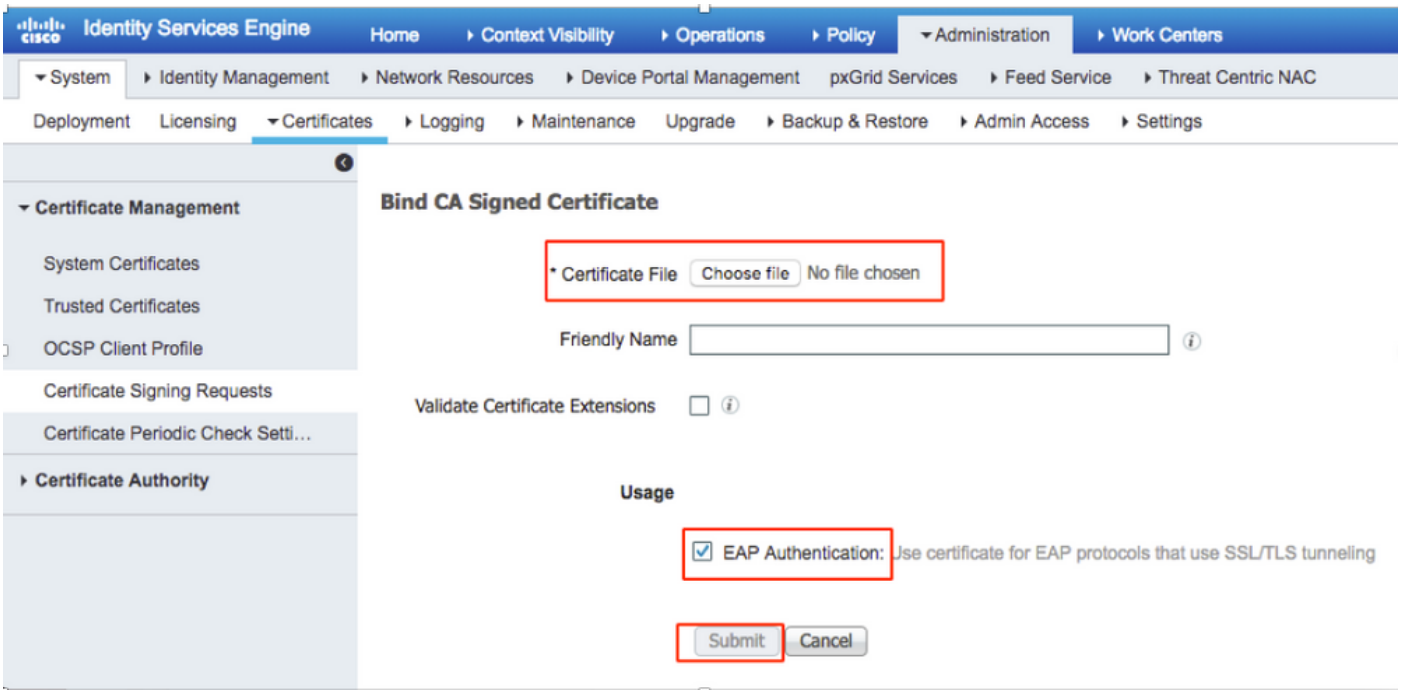




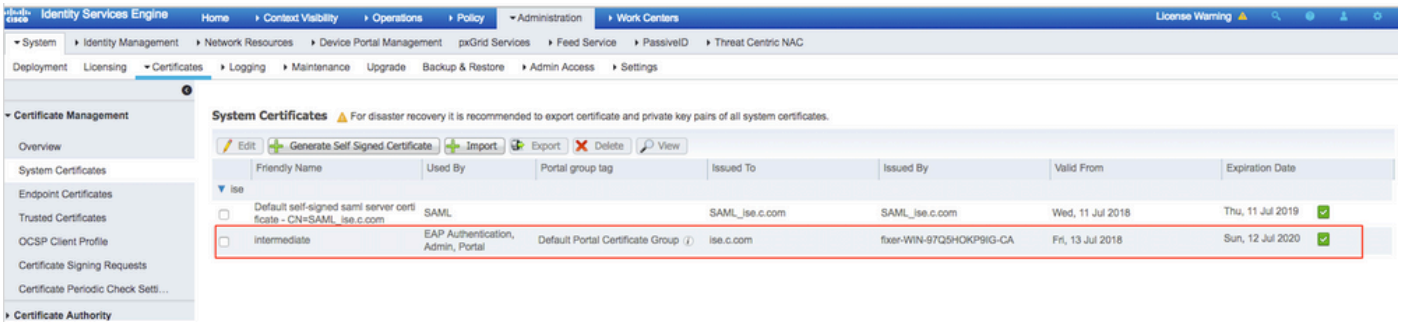
Schritt 10: Wenn Sie auf **Senden** klicken, wird das Zertifikat der Liste der vertrauenswürdigen Zertifikate hinzugefügt. Außerdem wird das Zwischenzertifikat benötigt, um eine Bindung mit CSR herzustellen, wie im Bild dargestellt.



Schritt 11. Sobald Sie auf **Zertifikat binden** klicken, gibt es eine Option, um die Zertifikatsdatei auf Ihrem Desktop gespeichert wählen. Navigieren Sie zum Zwischenzertifikat, und klicken Sie wie im Bild dargestellt auf **Senden**.



Schritt 12: Um das Zertifikat anzuzeigen, navigieren Sie zu **Administration > Certificates > System Certificates** wie im Bild dargestellt.



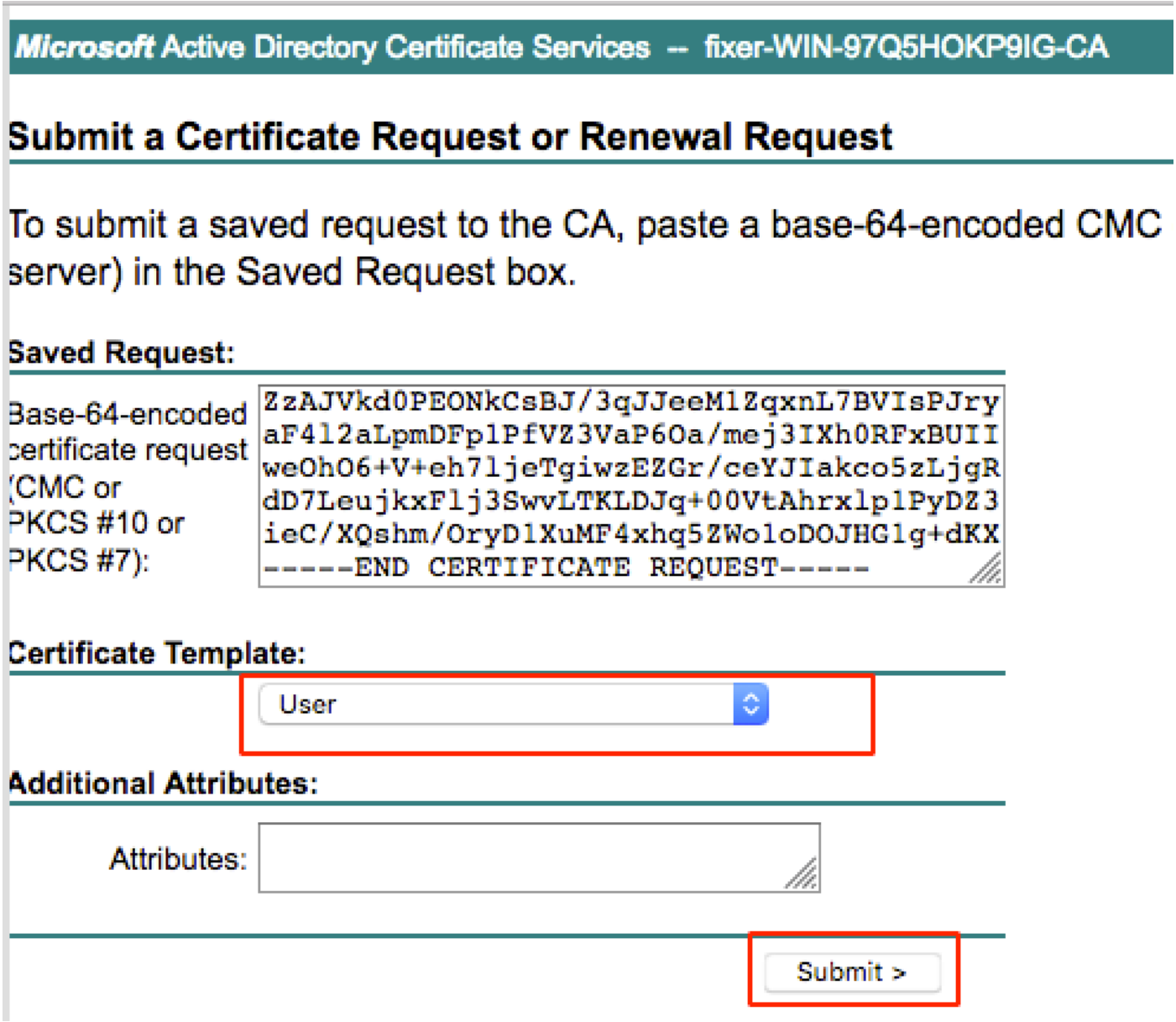
Client für EAP-TLS

Benutzerzertifikat auf Client-Computer herunterladen (Windows-Desktop)

Schritt 1: Um einen Wireless-Benutzer über EAP-TLS zu authentifizieren, müssen Sie ein Client-Zertifikat generieren. Verbinden Sie den Windows-Computer mit dem Netzwerk, sodass Sie auf den Server zugreifen können. Öffnen Sie einen Webbrowser, und geben Sie die folgende Adresse ein: https://sever ip addr/certsrv

Schritt 2: Beachten Sie, dass die Zertifizierungsstelle mit der identisch sein muss, mit der das Zertifikat für die ISE heruntergeladen wurde.

Dazu müssen Sie nach dem gleichen CA-Server suchen, den Sie zum Herunterladen des Zertifikats für den Server verwendet haben. Klicken Sie auf derselben CA auf **Zertifikat anfordern** wie zuvor, diesmal müssen Sie jedoch **Benutzer** als Zertifikatvorlage auswählen, wie im Bild gezeigt.



Schritt 3. Klicken Sie dann auf **Download Zertifikatskette**, wie zuvor für Server getan.

Wenn Sie die Zertifikate erhalten haben, gehen Sie wie folgt vor, um das Zertifikat auf Windows Laptop zu importieren:

Schritt 4: Um das Zertifikat zu importieren, müssen Sie von der Microsoft Management Console (MMC) darauf zugreifen.

1. Um die MMC zu öffnen, navigieren Sie zu **Start > Ausführen > MMC**.
2. Navigieren Sie zu **Datei > Snap-In hinzufügen/entfernen**
3. Doppelklicken Sie auf **Zertifikate**.
4. **Wählen Sie Computerkonto aus**.
5. **Lokalen Computer** auswählen **> Fertig stellen**
6. Klicken Sie auf **OK**, um das Snap-In-Fenster zu verlassen.
7. Klicken Sie auf **[+]** neben **Zertifikate > Persönlich > Zertifikate**.
8. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, und wählen Sie **Alle Aufgaben > Importieren aus**.
9. Klicken Sie auf **Next** (Weiter).
10. Klicken Sie auf **Durchsuchen**.

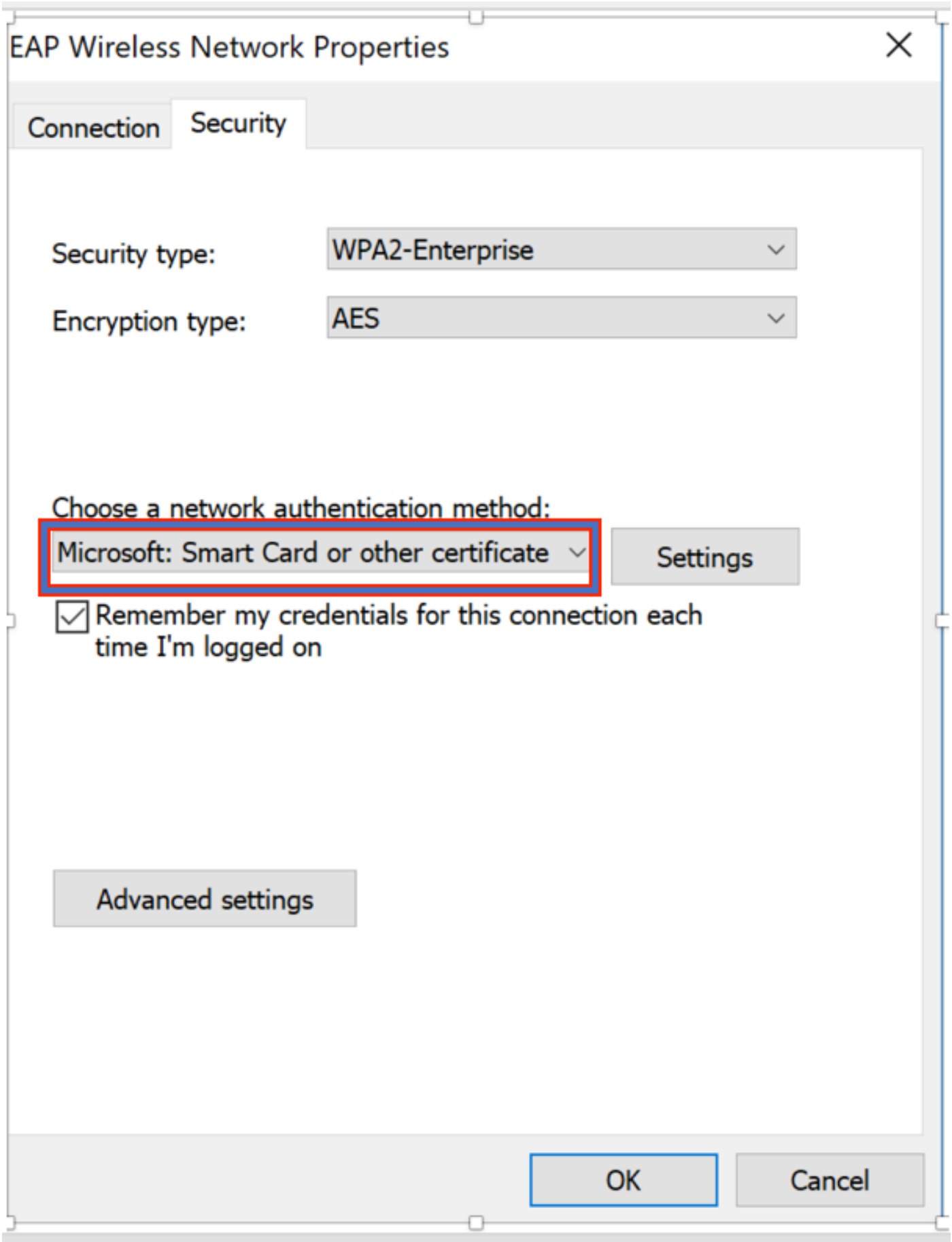
11. Wählen Sie die **.cer, .crt oder .pfx aus**, die Sie importieren möchten.
12. Klicken Sie auf **Öffnen**.
13. Klicken Sie auf **Next** (Weiter).
14. Wählen Sie **den Zertifikatspeicher basierend auf dem Zertifikatstyp automatisch aus**.
15. Klicken Sie auf **Fertig stellen und OK.**

Nach dem Import des Zertifikats müssen Sie Ihren Wireless-Client (in diesem Beispiel Windows Desktop) für EAP-TLS konfigurieren.

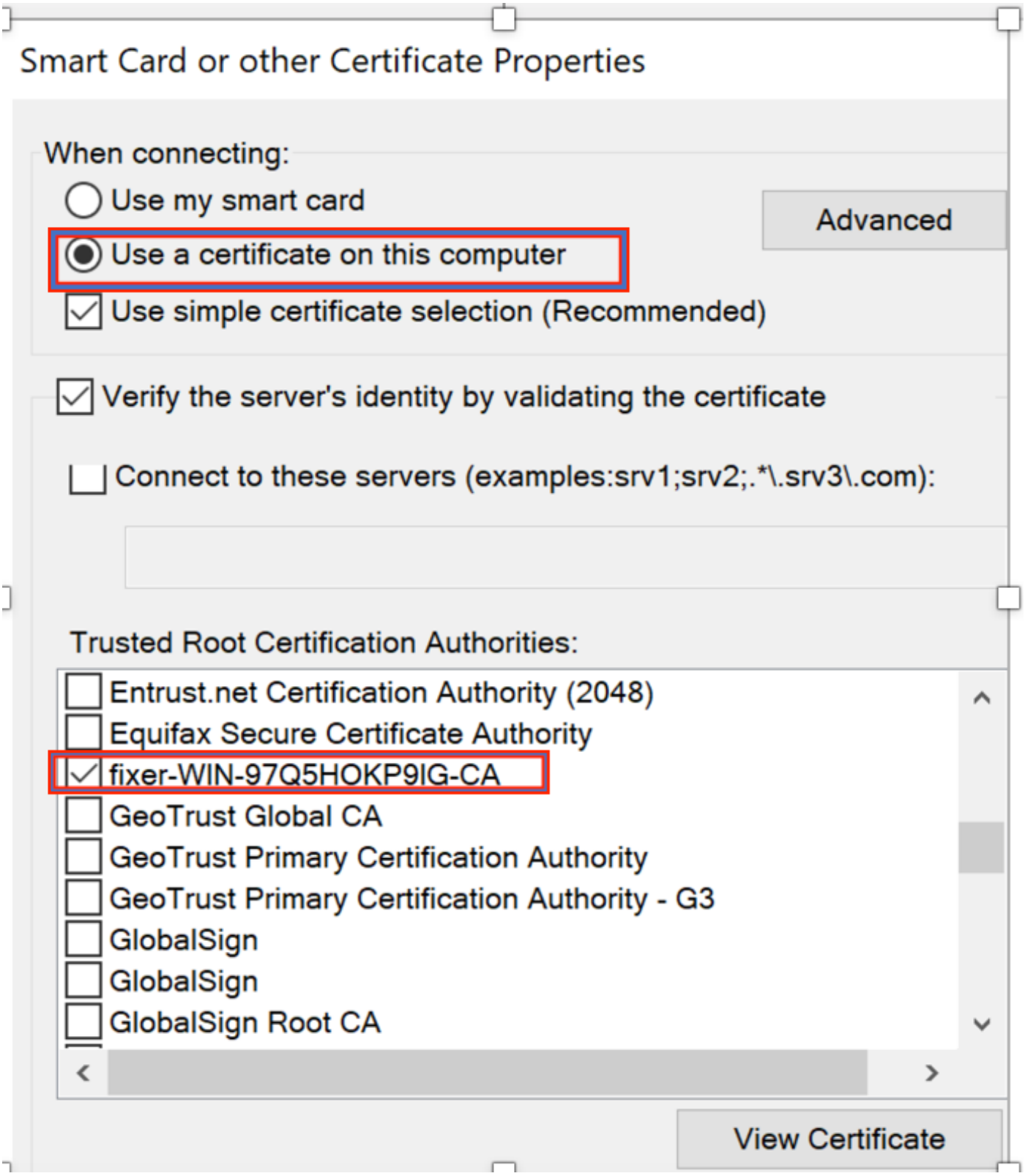
Wireless-Profil für EAP-TLS

Schritt 1: Ändern Sie das Wireless-Profil, das zuvor für Protected Extensible Authentication Protocol (PEAP) erstellt wurde, um stattdessen EAP-TLS zu verwenden. Klicken Sie auf **EAP Wireless Profile**.

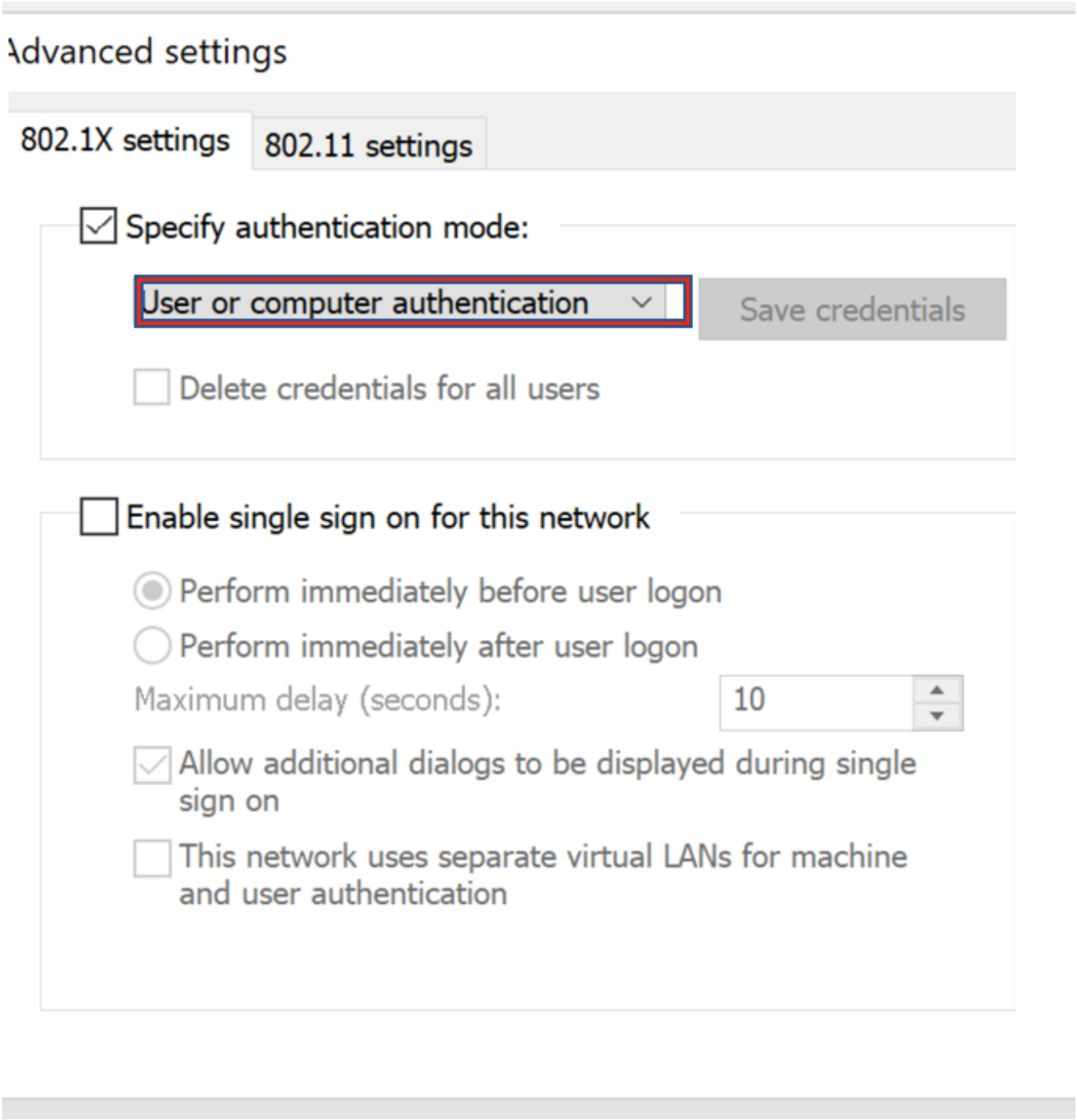
Schritt 2. Wählen Sie **Microsoft: Smartcard oder anderes Zertifikat** und klicken Sie auf **OK** im Bild angezeigt.



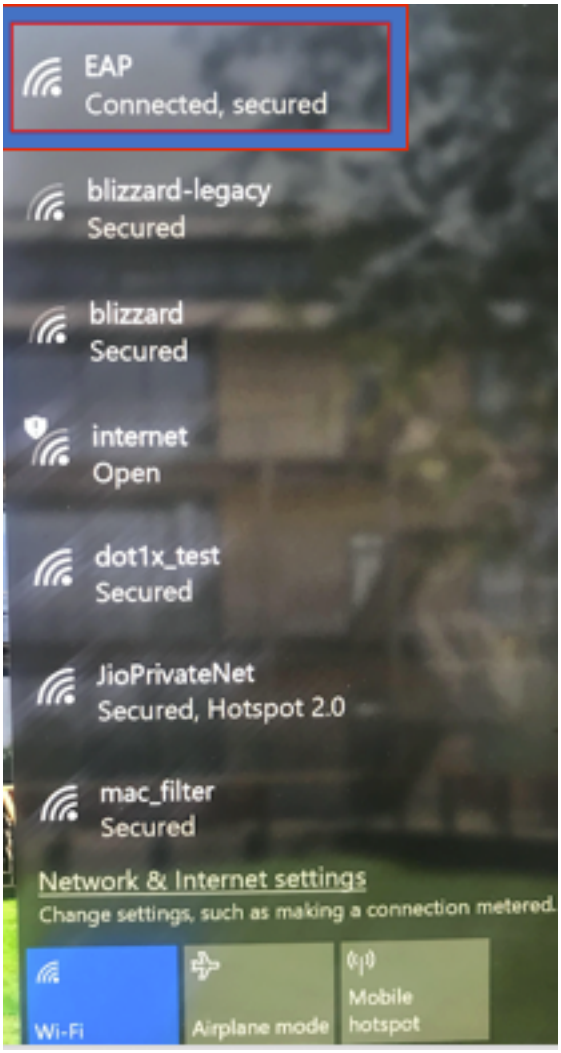
Schritt 3: Klicken Sie auf **Einstellungen** und wählen Sie das vom CA-Server ausgestellte Stammzertifikat aus, wie im Bild dargestellt.



Schritt 4: Klicken Sie auf **Erweiterte Einstellungen**, und wählen Sie **Benutzer- oder Computerauthentifizierung** aus der Registerkarte mit den 802.1x-Einstellungen aus, wie im Bild dargestellt.



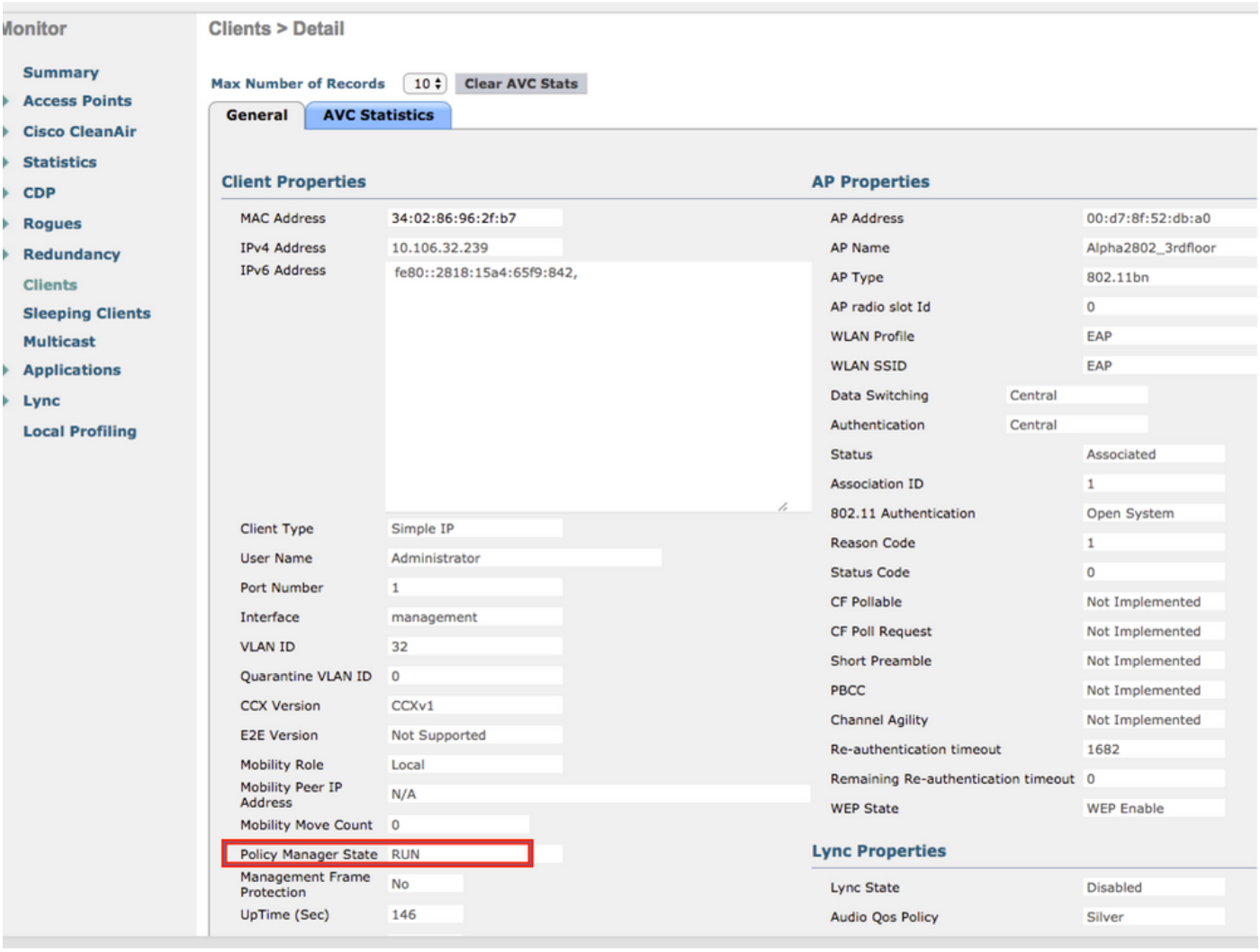
Schritt 5. Versuchen Sie nun, erneut eine Verbindung zum Wireless-Netzwerk herzustellen, wählen Sie das richtige Profil (in diesem Beispiel EAP) aus, und **verbinden Sie**. Sie sind wie im Bild dargestellt mit dem Wireless-Netzwerk verbunden.



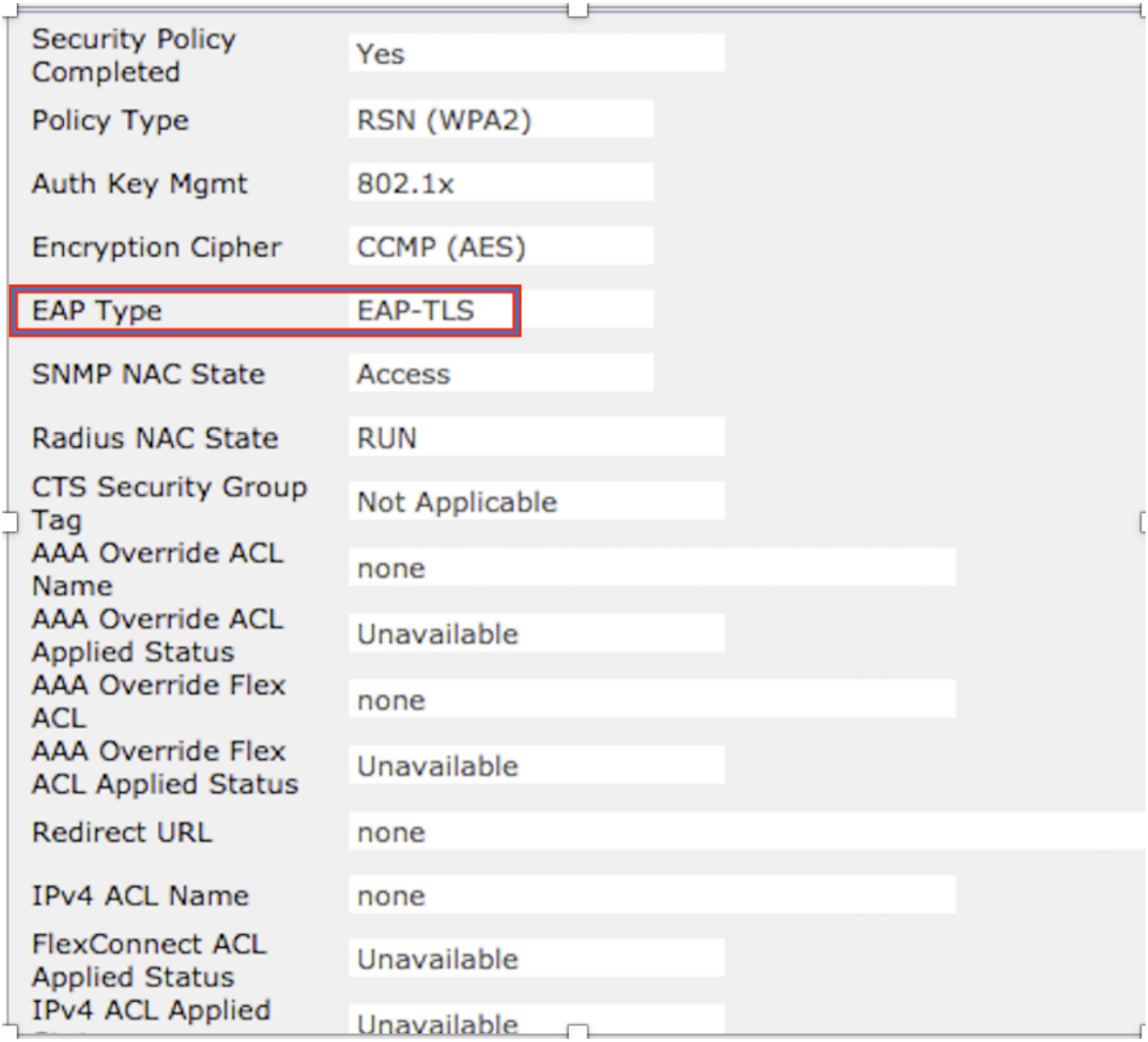
Überprüfung

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

Schritt 1: Der Status des Client-Richtlinienmanagers muss als **RUN** angezeigt werden. Das bedeutet, dass der Client die Authentifizierung abgeschlossen und die IP-Adresse abgerufen hat und bereit ist, den im Bild angezeigten Datenverkehr weiterzuleiten.



Schritt 2: Überprüfen Sie auch die richtige EAP-Methode auf dem WLC auf der Client-Detailseite, wie im Bild gezeigt.

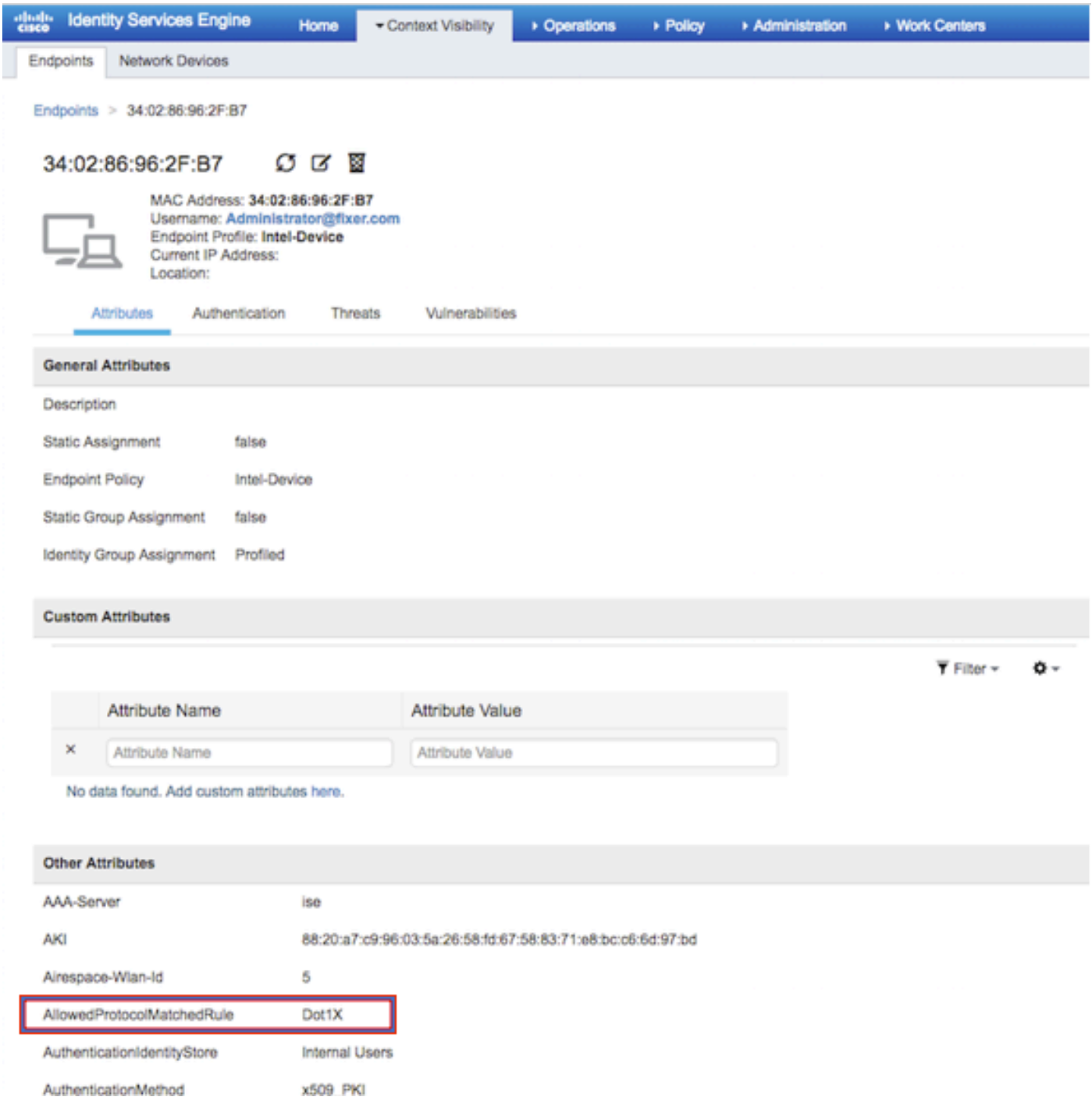


Schritt 3. Hier sind die Client-Details aus der CLI des Controllers (Ausgabe abgeschnitten):

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address.............................. 34:02:86:96:2f:b7
Client Username ................................ Administrator
AP MAC Address.................................. 00:d7:8f:52:db:a0
AP Name......................................... Alpha2802_3rdfloor
AP radio slot Id................................ 0
Client State.................................... Associated
Wireless LAN Id................................. 5
Wireless LAN Network Name (SSID)................ EAP
Wireless LAN Profile Name....................... EAP
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:d7:8f:52:db:a4
Connected For .................................. 48 secs
Channel......................................... 1
IP Address...................................... 10.106.32.239
Gateway Address................................. 10.106.32.1
Netmask......................................... 255.255.255.0
Policy Manager State............................ RUN
Policy Type..................................... WPA2
Authentication Key Management................... 802.1x
```

```
Encryption Cipher.............................. CCMP-128 (AES)
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type....................................... EAP-TLS
```

Schritt 4: Navigieren Sie auf der ISE zu **Kontexttransparenz > Endpunkte > Attribute,** wie in den Bildern gezeigt.



BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7
MatchedPolicy	Intel-Device
MessageCode	5200
NAS-IP-Address	10.106.32.223
NAS-Identifier	HA_Pri
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	HA_Pri
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLErrorStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	AccessRequest
SSID	00-d7-8f-52-db-a0:EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 00 11

Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Problembehebung 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.