Verständnis und Konfiguration von EAP-TLS mit Mobility Express und ISE

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie ein Wireless Local Area Network (WLAN) mit 802.1x-Sicherheit in einem Mobility Express-Controller einrichten. In diesem Dokument wird auch speziell die Verwendung von Extensible Authentication Protocol (EAP) - Transport Layer Security (TLS) erläutert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Ersteinrichtung von Mobility Express
- 802.1x-Authentifizierungsprozess
- Zertifikate

Verwendete Komponenten

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

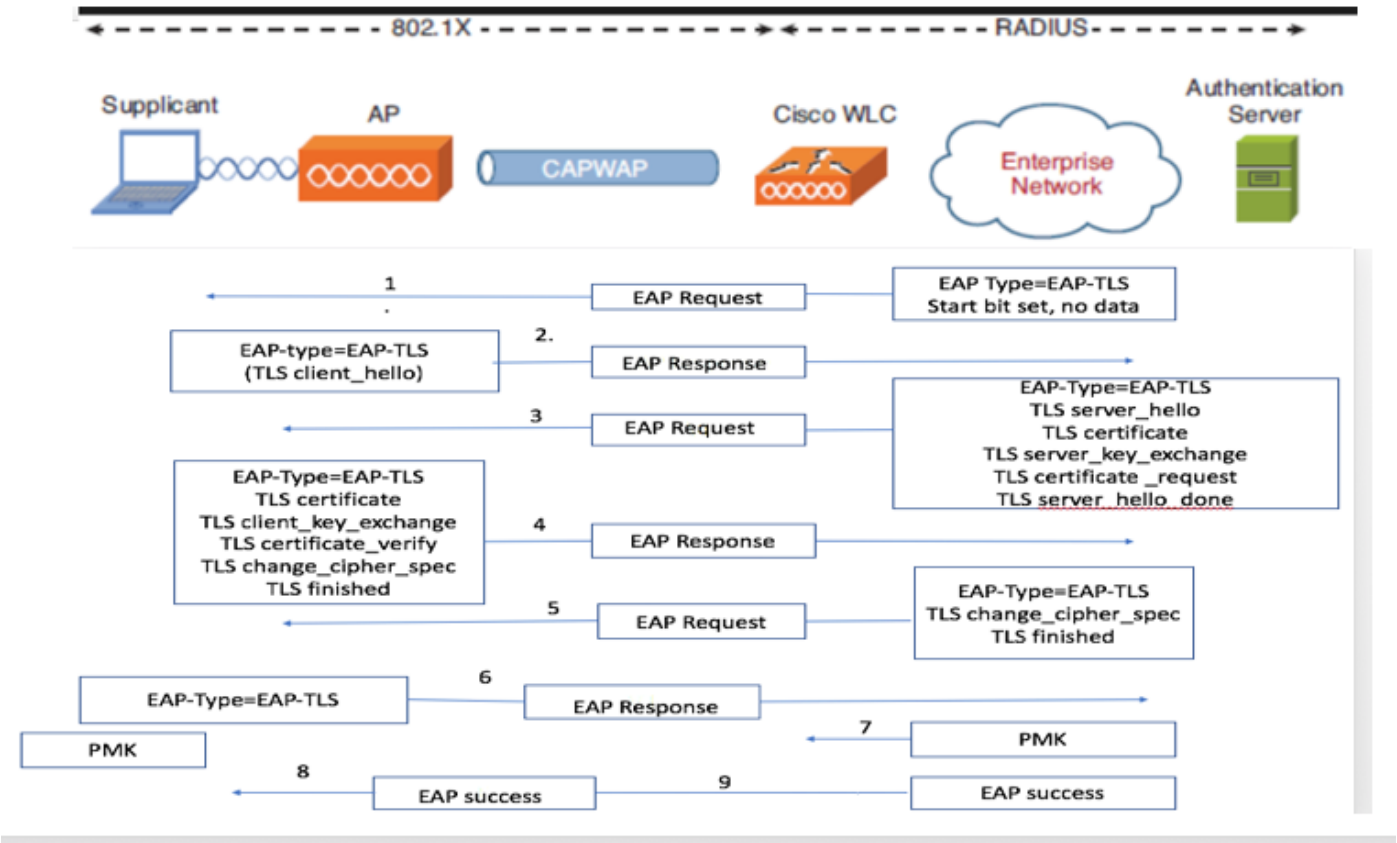
Hardwareversionen:

- WLC 5508 Version 8.5
- Identity Services Engine (ISE) Version 2.1

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

Hintergrundinformationen

EAP-TLS-Fluss



Schritte im EAP-TLS-Fluss

1. Der Wireless-Client wird dem Access Point (AP) zugeordnet.
2. AP erlaubt dem Client zu diesem Zeitpunkt keine Daten zu senden und sendet eine Authentifizierungsanfrage.
3. Der Supplicant antwortet dann mit einer EAP-Antwortidentität. Der WLC leitet die Benutzer-ID-Informationen dann an den Authentifizierungsserver weiter.
4. Der RADIUS-Server antwortet mit einem EAP-TLS-Startpaket auf den Client zurück. Die EAP-TLS-Konversation beginnt an diesem Punkt.
5. Der Peer sendet eine EAP-Antwort zurück an den Authentifizierungsserver, der eine Handshake-Meldung "client_hello" enthält, eine Chiffre, die für NULL festgelegt ist.

6. 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.
```

7. 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
```

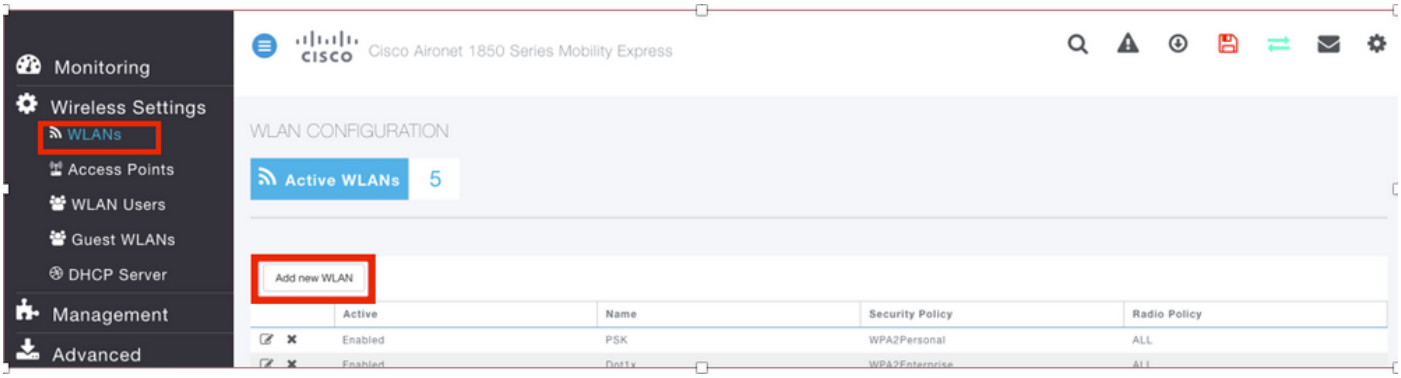
8. Nachdem der Client sich erfolgreich authentifiziert hat, antwortet der RADIUS-Server mit einer Access-Challenge, die die Meldung "change_cipher_spec" und die Handshake-Fertigstellung enthält. Beim Empfang dieser Nachricht überprüft der Client den Hash, um den RADIUS-Server zu authentifizieren. Beim TLS-Handshake wird dynamisch ein neuer Verschlüsselungsschlüssel aus dem geheimen Schlüssel abgeleitet.

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

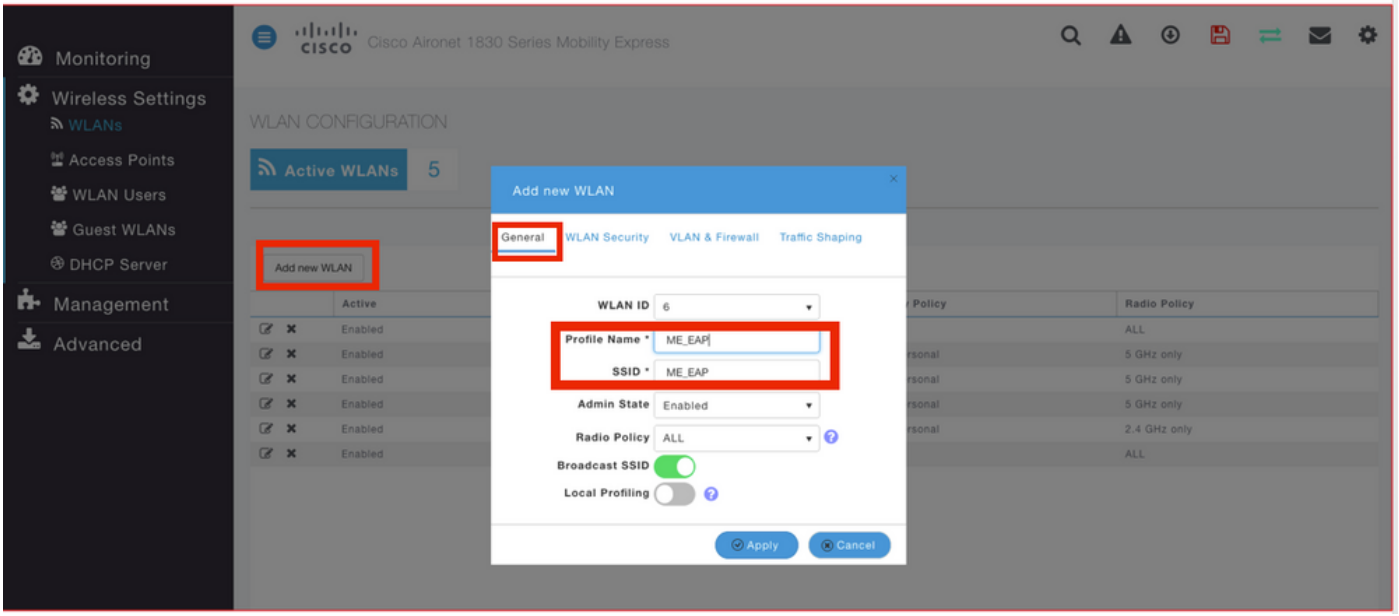
Konfigurieren

Cisco Mobility Express

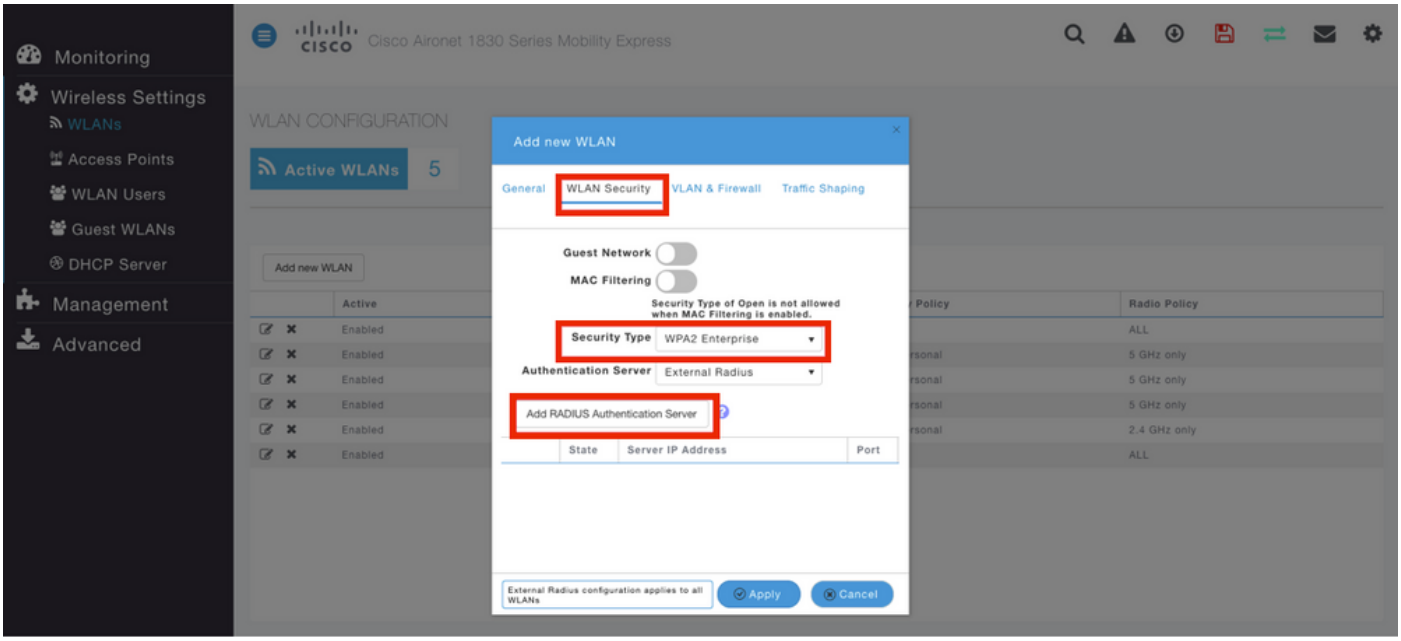
Schritt 1: Der erste Schritt besteht in der Erstellung eines WLAN auf Mobility Express. Um ein WLAN zu erstellen, navigieren Sie zu **WLAN > Add new WLAN** wie im Bild gezeigt.



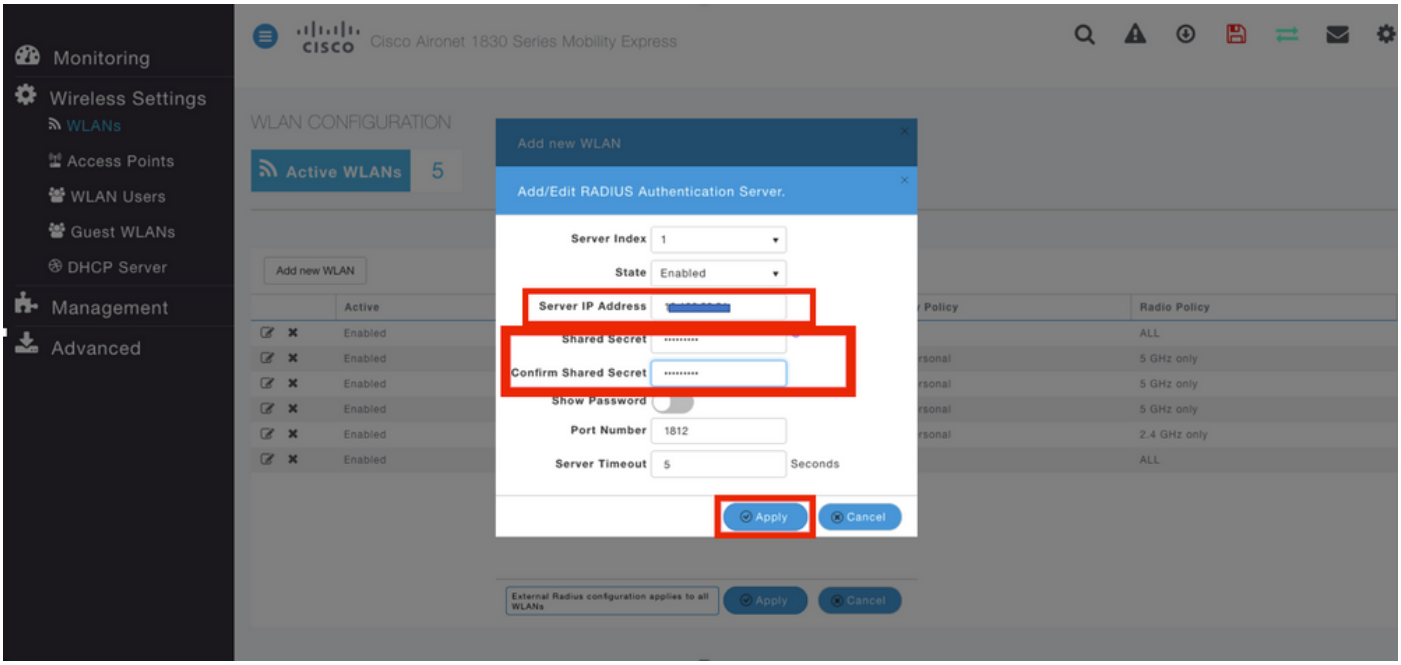
Schritt 2: Ein neues Popup-Fenster wird angezeigt, wenn Sie auf **Neues WLAN hinzufügen** klicken. Um einen Profilnamen zu erstellen, navigieren Sie zu **Neues WLAN hinzufügen > Allgemein**, wie im Bild gezeigt.



Schritt 3: Konfigurieren Sie den Authentifizierungstyp als WPA Enterprise für 802.1x, und konfigurieren Sie RADIUS-Server unter **Neues WLAN hinzufügen > WLAN-Sicherheit**, wie im Bild gezeigt.



Schritt 4: Klicken Sie auf **RADIUS Authentication Server hinzufügen**, und geben Sie die IP-Adresse des RADIUS-Servers und des Shared Secret an, die genau mit den auf der ISE konfigurierten Daten übereinstimmen muss, und klicken Sie dann wie im Bild gezeigt **auf Apply**.



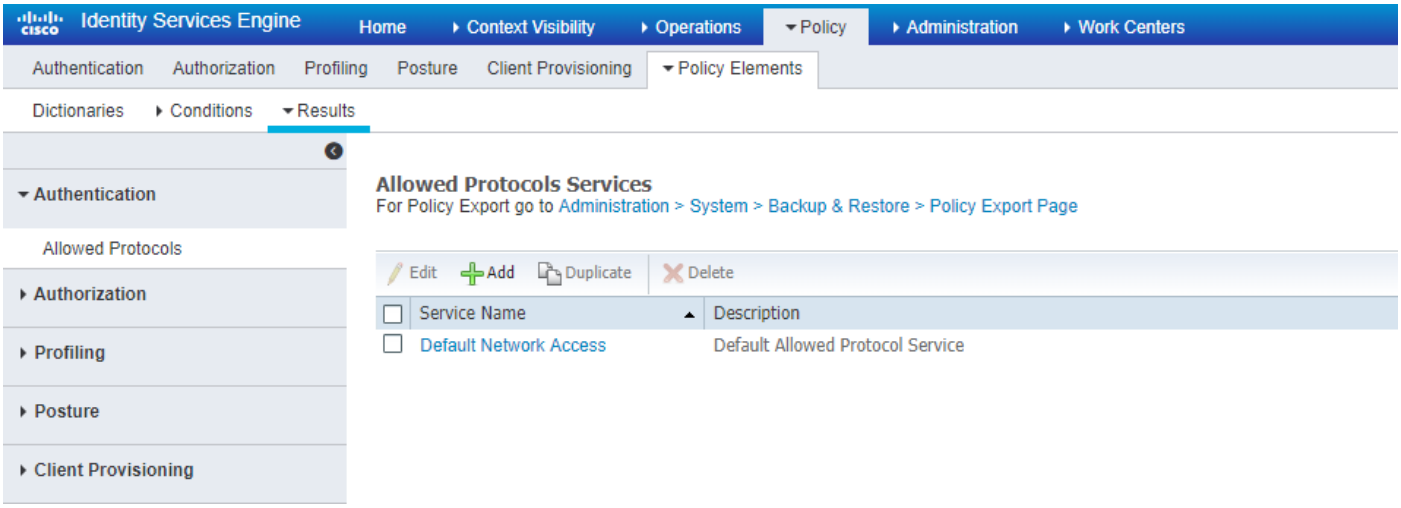
ISE mit Cisco Mobility Express

EAP-TLS-Einstellungen

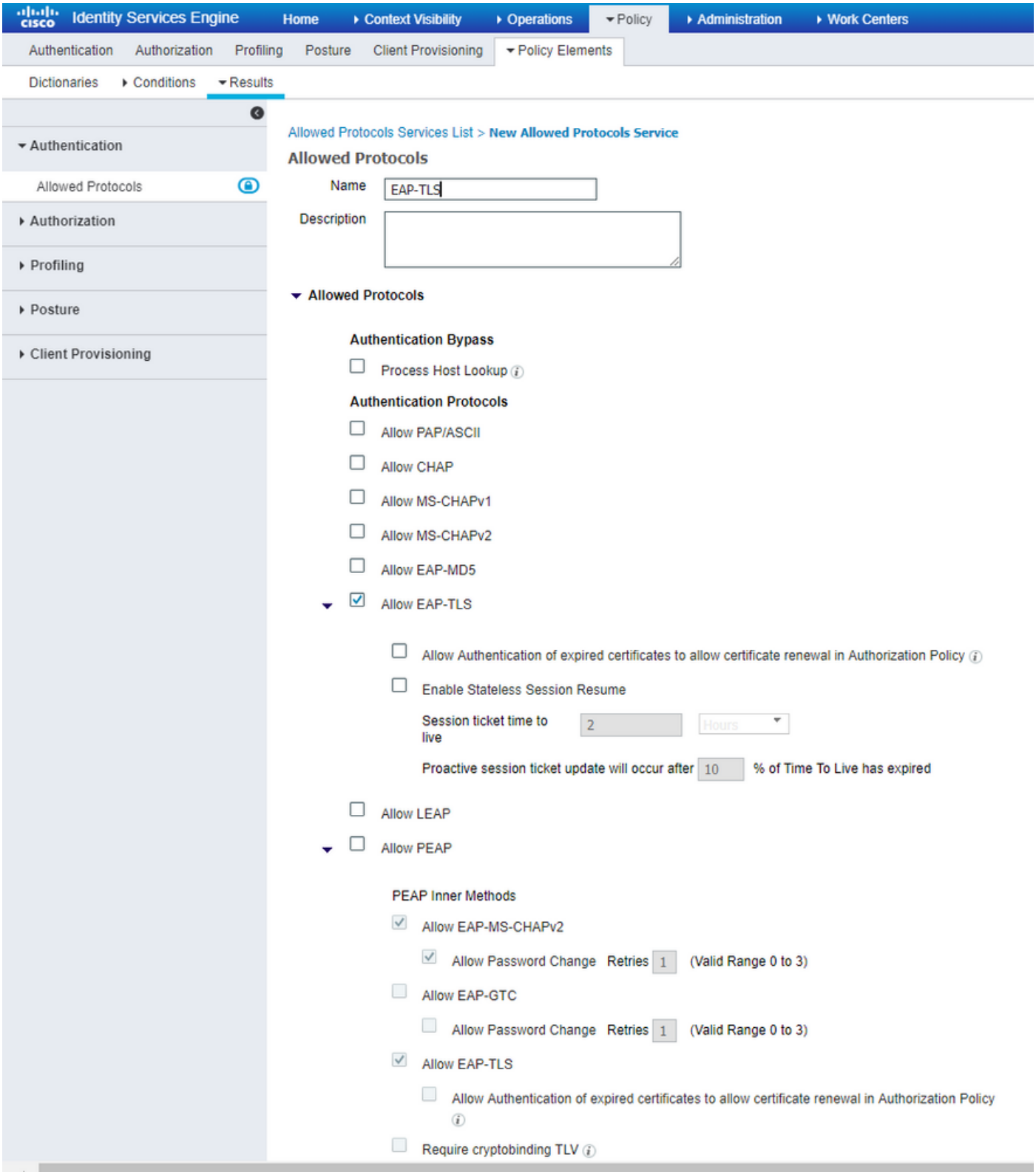
Um die Richtlinie zu erstellen, müssen Sie die zulässige Protokollliste erstellen, die in der Richtlinie verwendet werden soll. Da eine 802.1x-Richtlinie geschrieben wird, geben Sie den zulässigen EAP-Typ basierend auf der Konfiguration der Richtlinie an.

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

Schritt 1: Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Authentifizierung > Zulässige Protokolle**, und klicken Sie auf **Hinzufügen**, wie im Bild gezeigt.

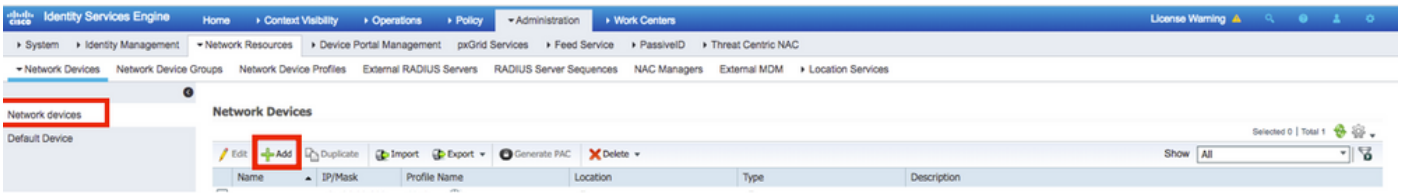


Schritt 2: In dieser Liste der zulässigen Protokolle können Sie den Namen für die Liste eingeben. In diesem Fall ist das Kontrollkästchen **Zulassen von EAP-TLS** aktiviert, und andere Felder sind wie im Bild gezeigt deaktiviert.

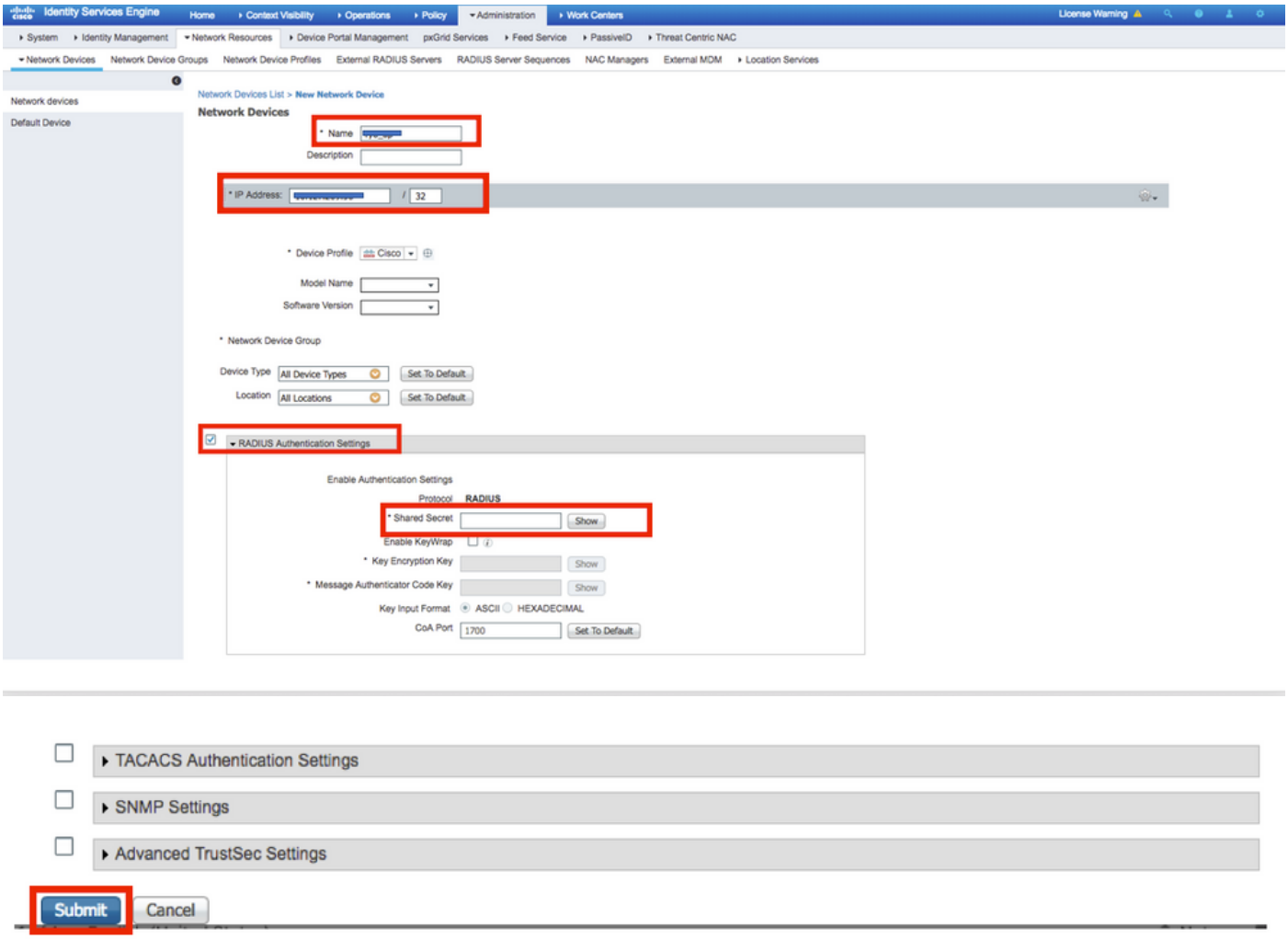


Mobility Express-Einstellungen für die ISE

Schritt 1: Öffnen Sie die ISE-Konsole, und navigieren Sie zu **Administration > Network Resources > Network Devices > Add** (**Verwaltung > Netzwerkressourcen > Netzwerkgeräte > Hinzufügen**, wie im Bild gezeigt.



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

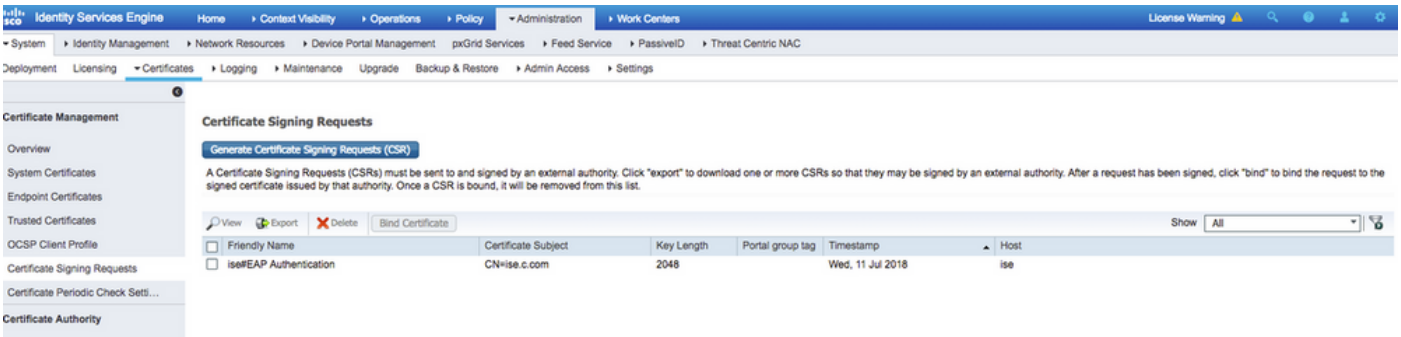


Vertrauenszertifikat auf ISE

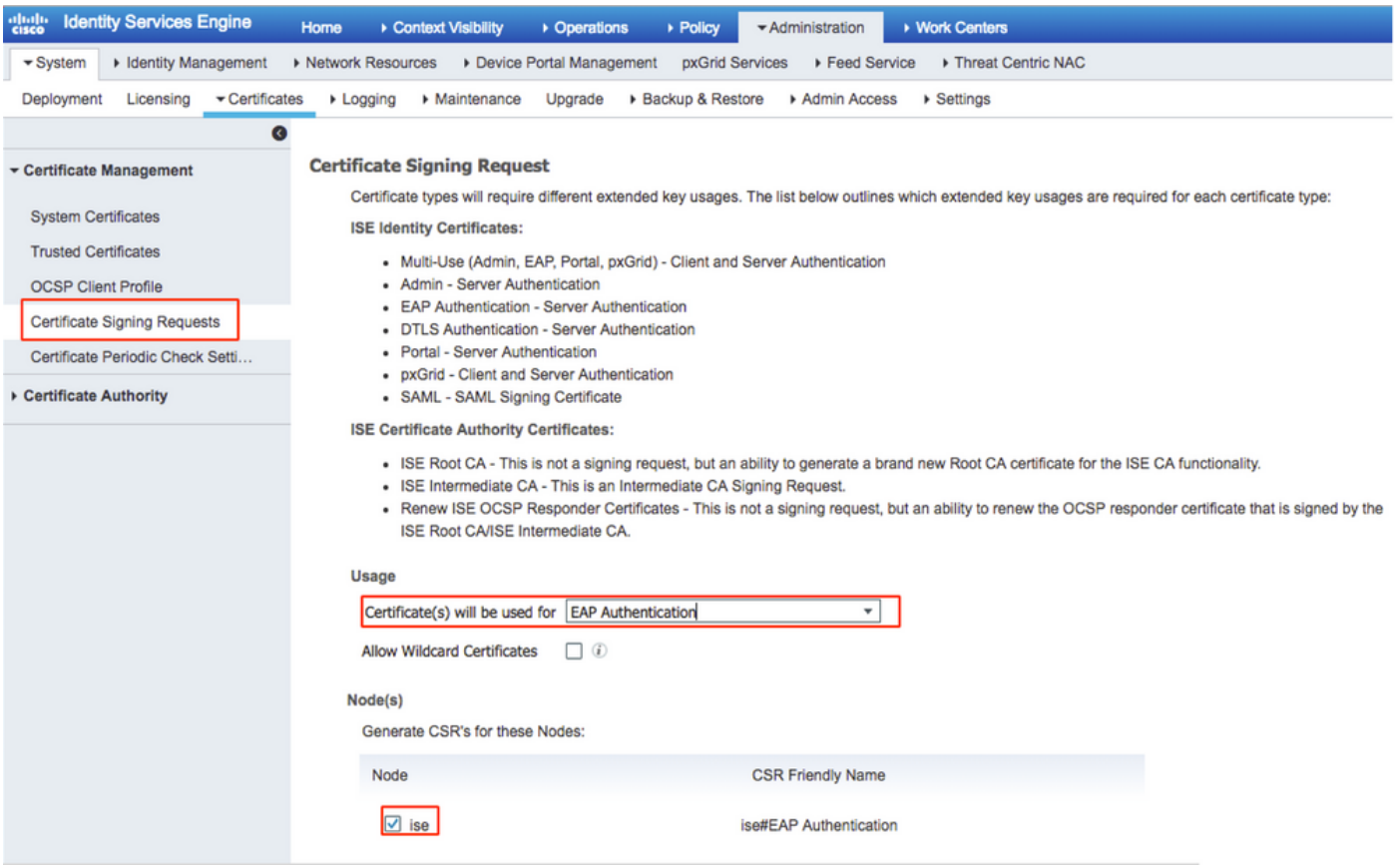
Schritt 1: Navigieren Sie zu **Administration > System > Certificates > Certificate Management > Trusted Certificates**.

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, der darin besteht, dem Zertifikat auf der ISE zu vertrauen. Dafür müssen Sie CSR generieren.

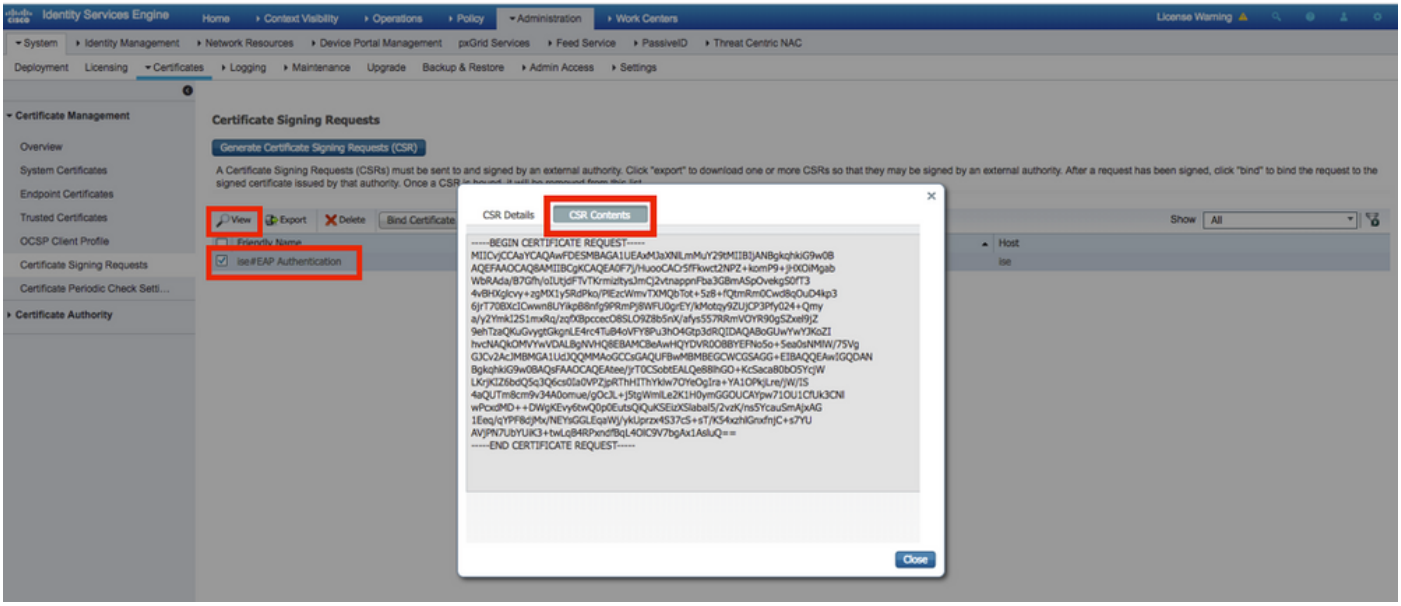
Schritt 2: Navigieren Sie zu **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR) (Verwaltung > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR)** wie im Bild gezeigt.



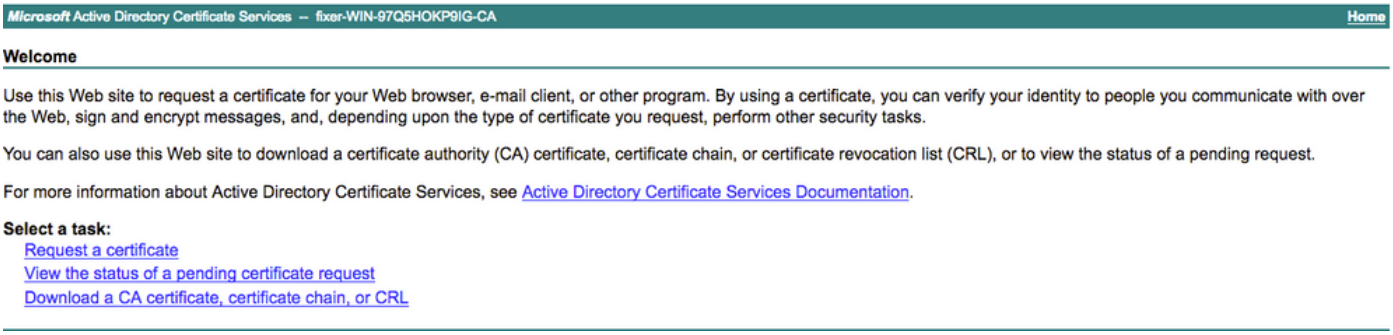
Schritt 3: Um eine CSR-Anfrage zu erstellen, navigieren Sie zu **Usage** (**Nutzung**), und **die Zertifikate werden für** Dropdown-Optionen **verwendet**, um die **EAP-Authentifizierung** wie im Bild gezeigt auszuwählen.



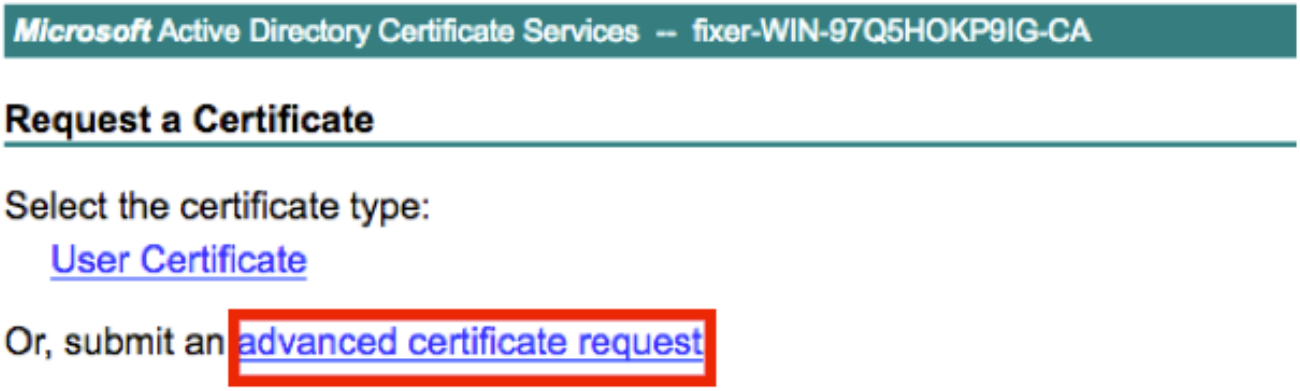
Schritt 4: Der auf der ISE generierte CSR kann angezeigt werden. Klicken Sie auf **Ansicht**, wie im Bild gezeigt.



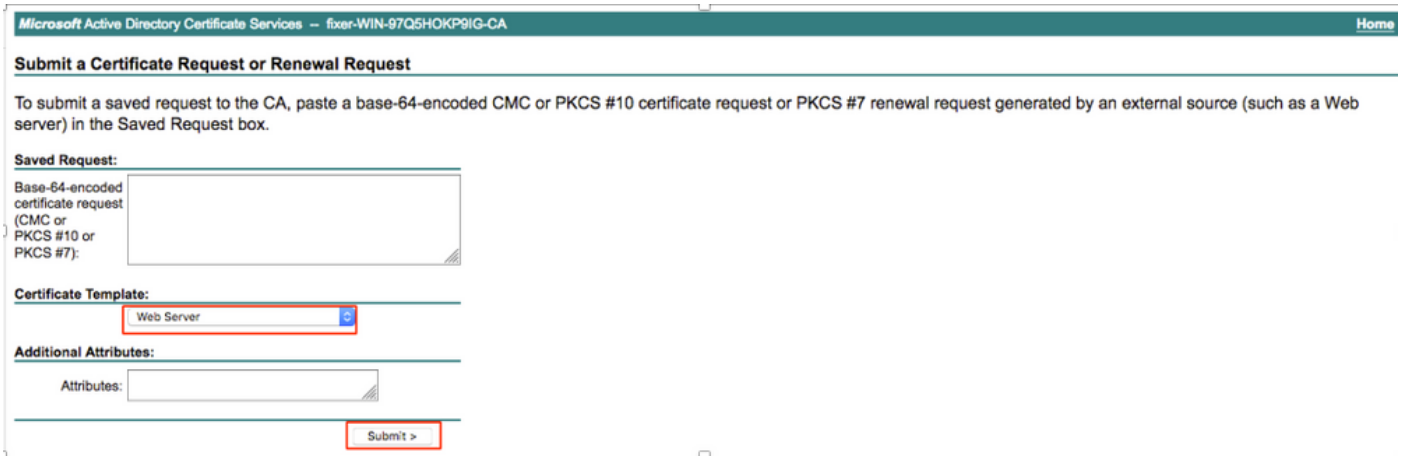
Schritt 5: Sobald der CSR erstellt wurde, suchen Sie nach dem CA-Server, und klicken Sie auf **Zertifikat anfordern**, wie im Bild gezeigt:



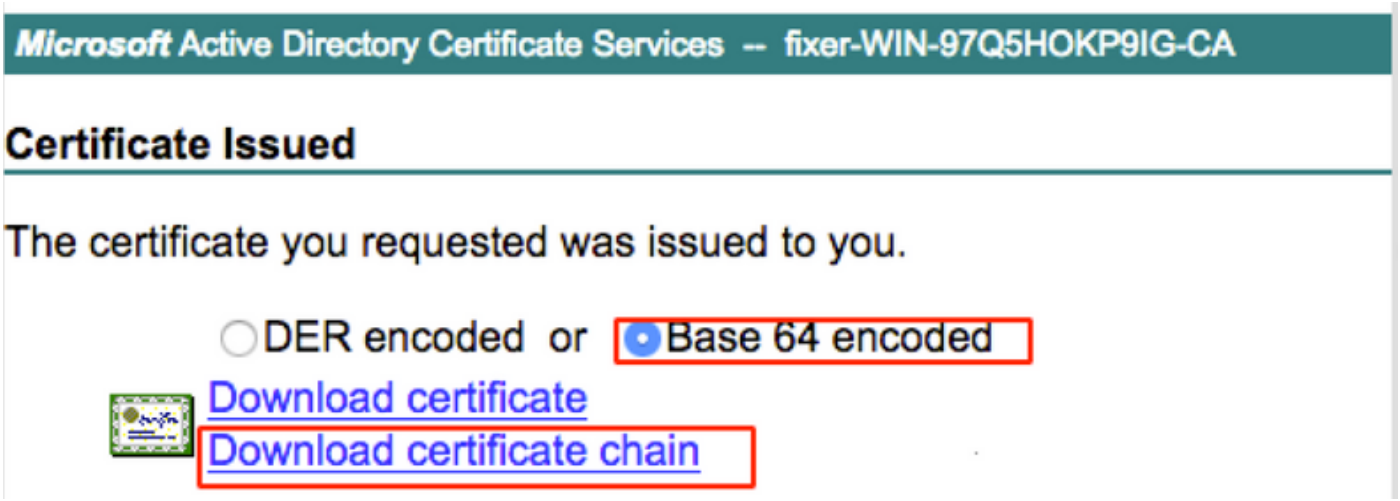
Schritt 6: Wenn Sie ein Zertifikat anfordern, erhalten Sie Optionen für **Benutzerzertifikat** und **erweiterte Zertifikatsanforderung**, und klicken Sie auf **Erweiterte Zertifikatsanforderung** wie im Bild gezeigt.



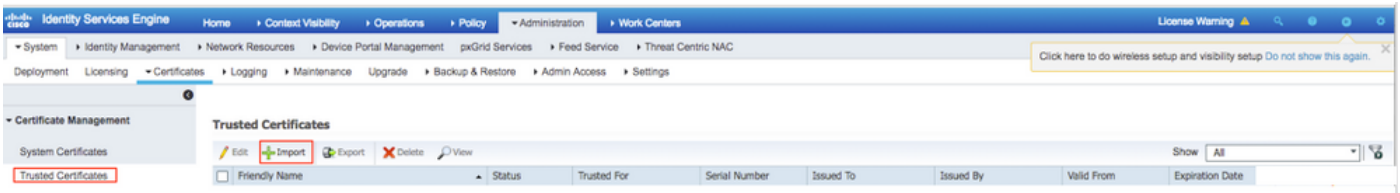
Schritt 7: Fügen Sie den in **Base-64 kodierten Zertifikatsanforderung** generierten CSR ein. Wählen Sie aus der Dropdown-Option **Zertifikatsvorlage: die Option Webserver aus**, und klicken Sie auf **Senden**, wie im Bild gezeigt.

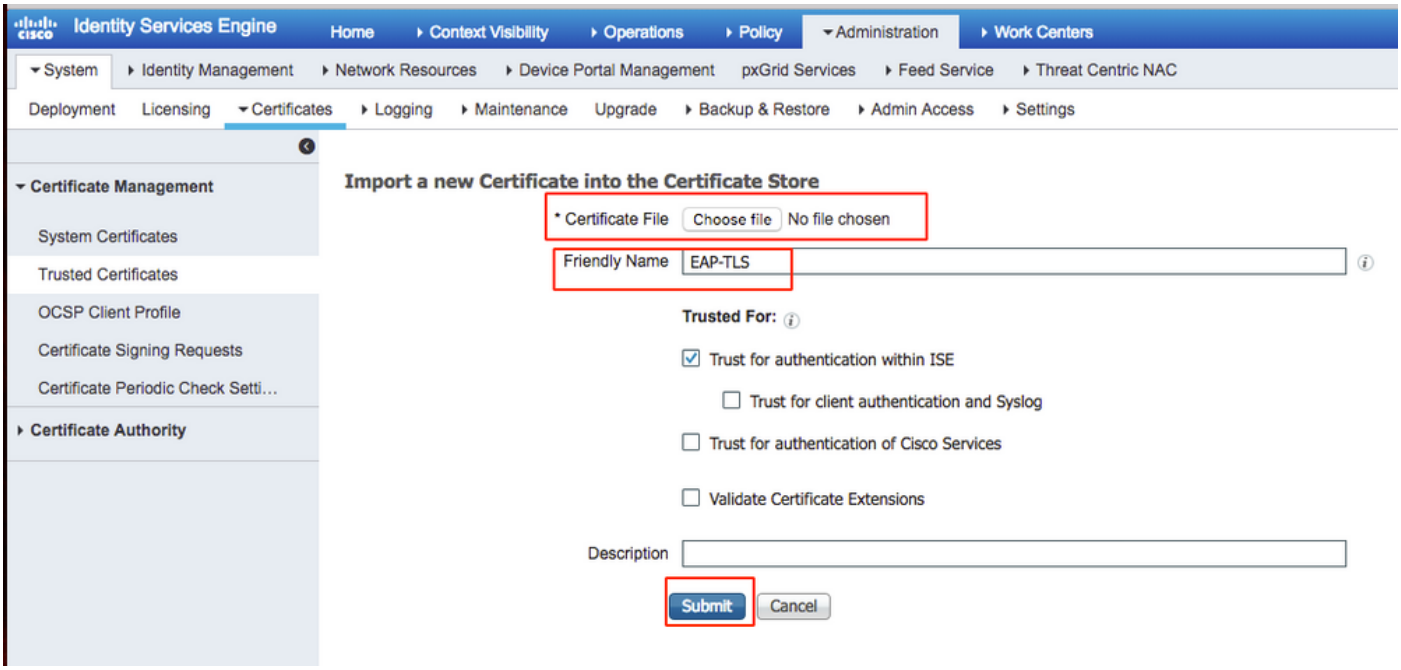


Schritt 8: Wenn Sie auf **Senden** klicken, können Sie den Zertifikatstyp auswählen, **Base-64-verschlüsselt** auswählen und auf **Zertifikatskette** herunterladen klicken, wie im Bild gezeigt.

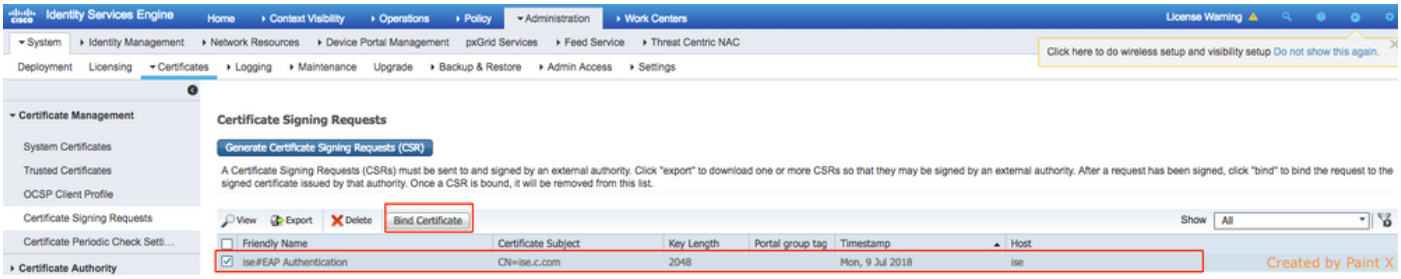


Schritt 9: Der Zertifikatsdownload ist für den ISE-Server abgeschlossen. Sie können das Zertifikat extrahieren. Das Zertifikat enthält zwei Zertifikate, ein Stammzertifikat und ein anderes Zwischenzertifikat. Das Stammzertifikat kann unter **Administration > Certificates > Trusted Certificates > Import**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

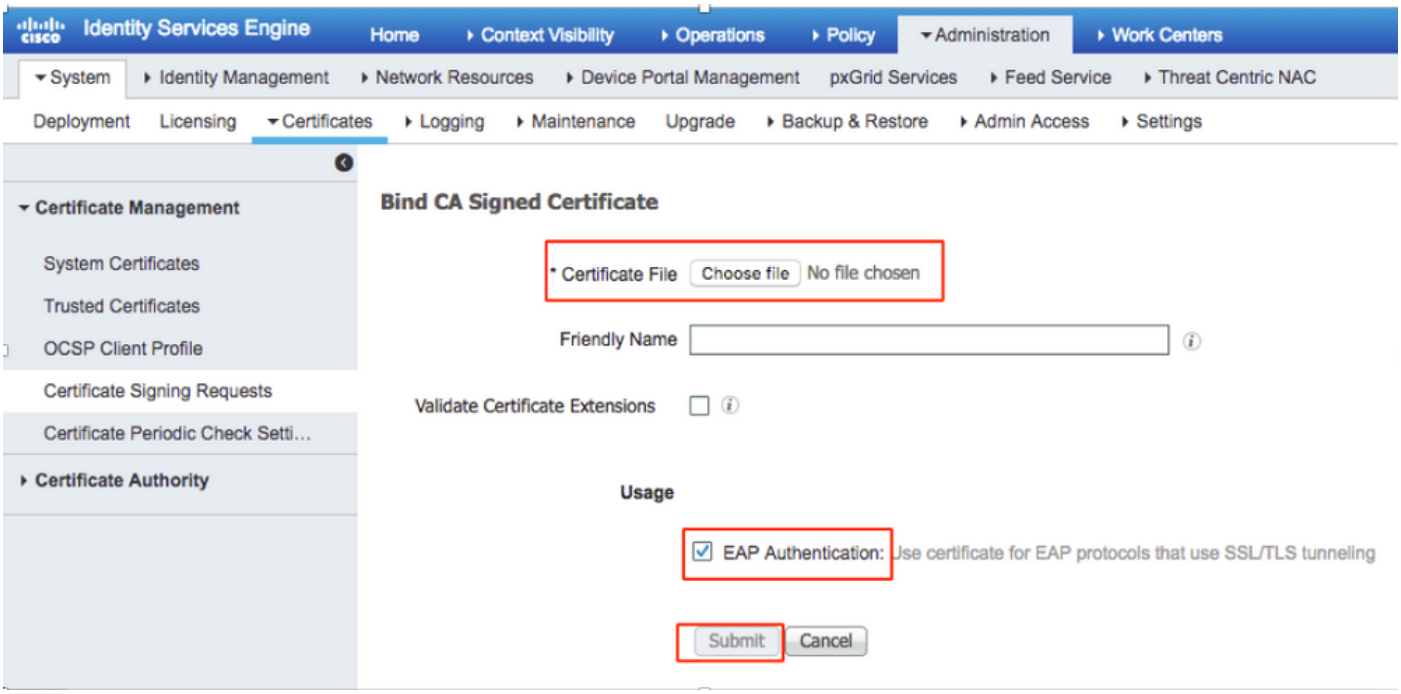




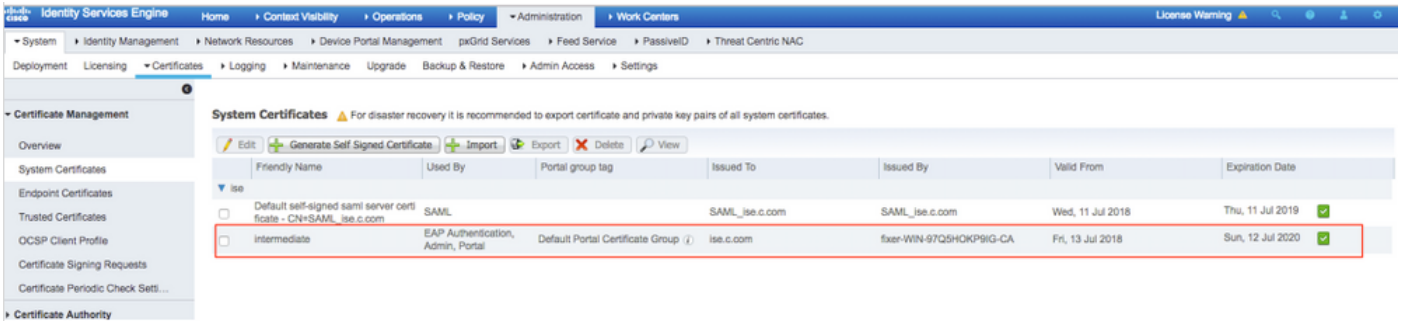
Schritt 10: Wenn Sie auf **Senden** klicken, wird das Zertifikat der Liste der vertrauenswürdigen Zertifikate hinzugefügt. Außerdem wird das Zwischenzertifikat benötigt, um wie im Bild gezeigt an CSR zu binden.



Schritt 11: Wenn Sie auf **Bind Certificate** klicken, können Sie die auf Ihrem Desktop gespeicherte Zertifikatsdatei auswählen. Navigieren Sie zum Zwischenzertifikat, und klicken Sie auf **Senden**, wie im Bild gezeigt.



Schritt 12: Um das Zertifikat anzuzeigen, navigieren Sie zu **Administration > Certificates > System Certificates (Verwaltung > Zertifikate > Systemzertifikate)**, wie im Bild gezeigt.



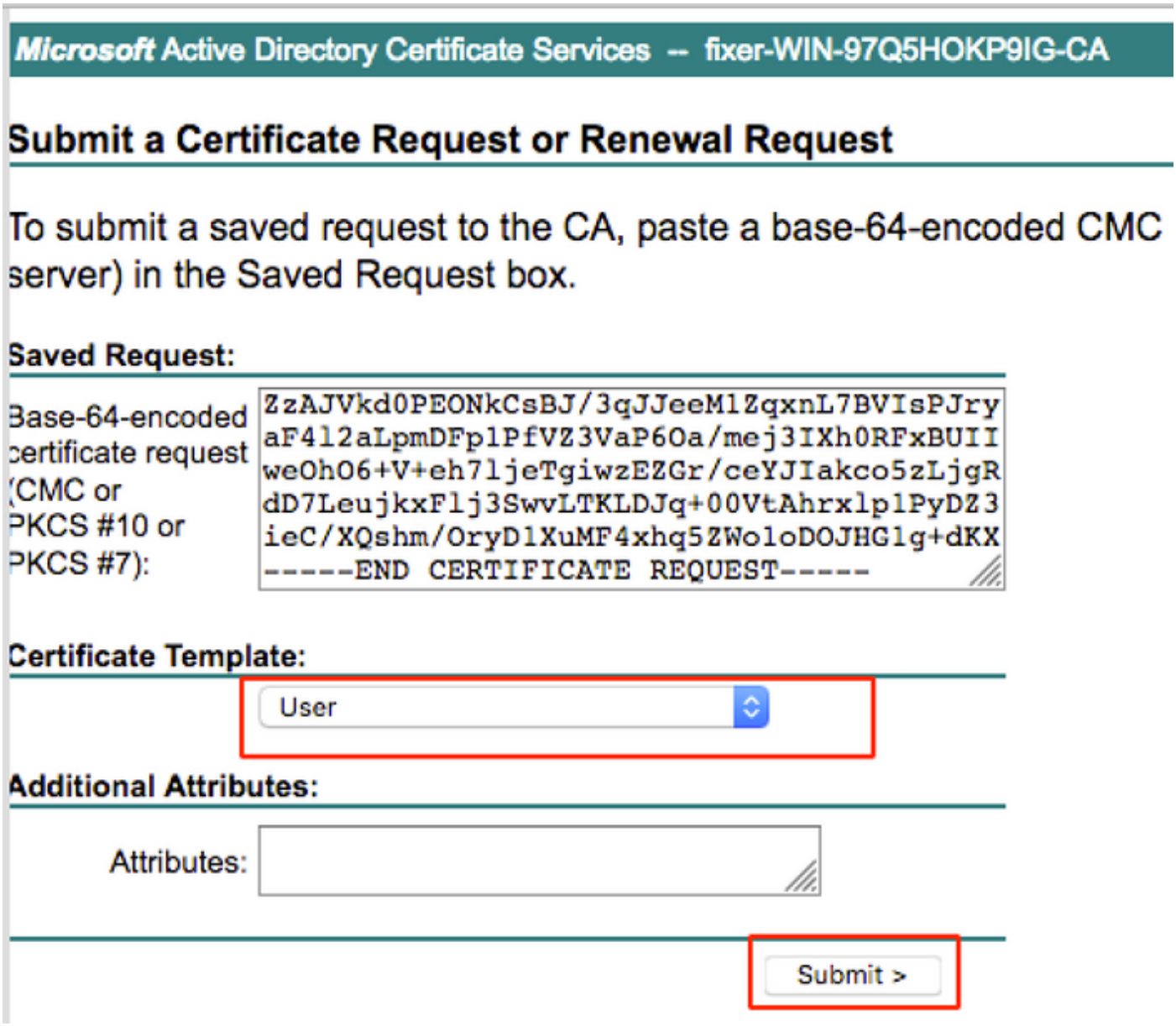
Client für EAP-TLS

Benutzerzertifikat auf dem Client-Computer herunterladen (Windows-Desktop)

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

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

Dazu müssen Sie nach demselben 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 Zertifikatsvorlage auswählen, wie im Bild gezeigt.



Schritt 3: Klicken Sie anschließend auf **Zertifikatskette herunterladen**, wie zuvor für den Server ausgeführt.

Wenn Sie die Zertifikate erhalten haben, führen Sie die folgenden Schritte aus, um das Zertifikat auf dem Windows-Laptop zu importieren.

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

1. Um die MMC zu öffnen, navigieren Sie zu **Start > Ausführen > MMC**.
2. Navigieren Sie zu **Datei > Einblenden hinzufügen/entfernen.**
3. Doppelklicken Sie auf **Zertifikate**.
4. Wählen Sie **Computerkonto aus**.

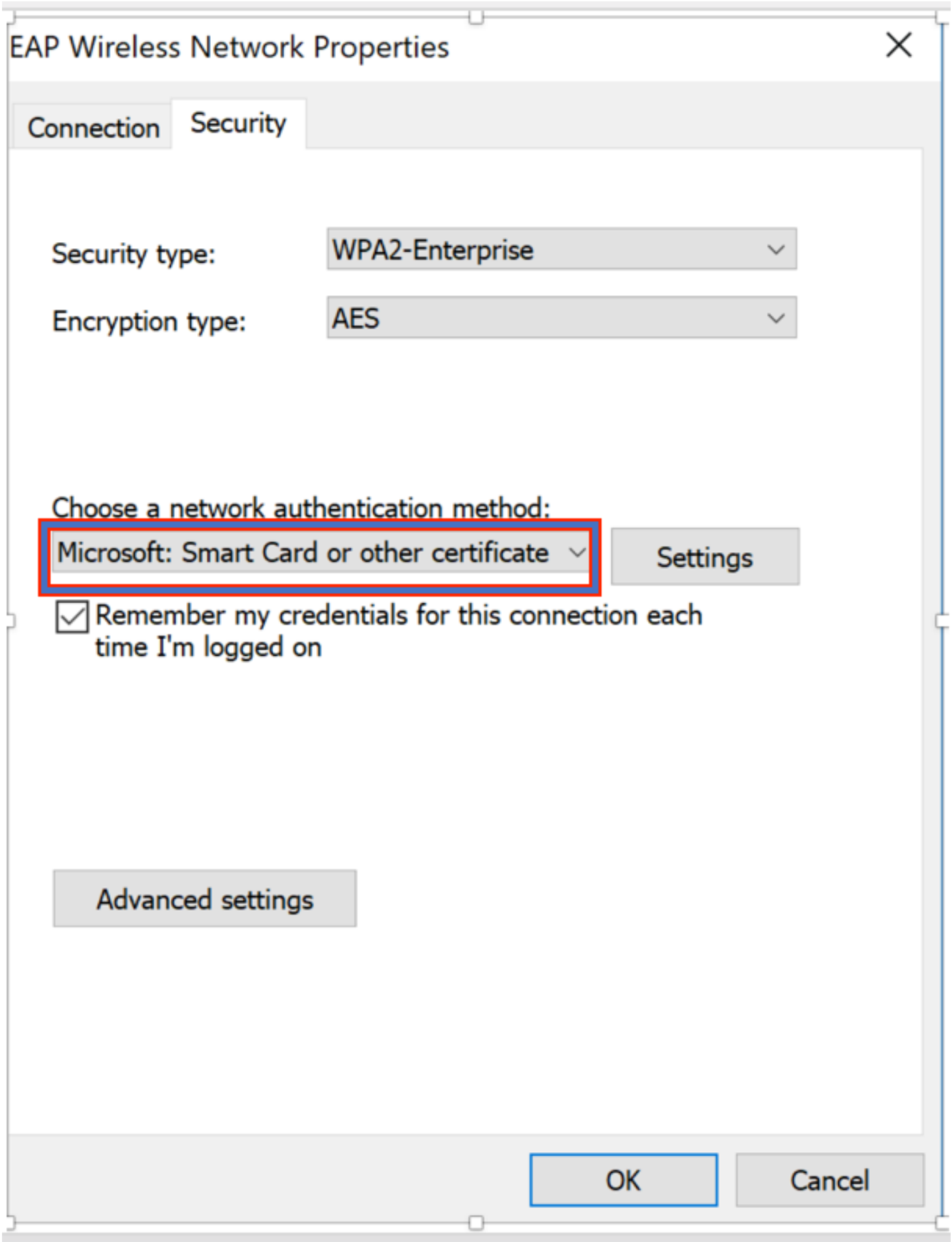
5. Wählen Sie **Lokaler Computer > Fertig stellen**
6. Klicken Sie auf **OK**, um das Snap-In-Fenster zu schließen.
7. Klicken Sie auf **[+]** neben **Zertifikate > Personal > Zertifikate**.
8. Klicken Sie mit der rechten Maustaste auf **Zertifikate** und wählen Sie **Alle Tasks > Importieren aus**.
9. Klicken Sie auf **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 **Weiter**.
14. Wählen Sie **Automatisch den Zertifikatsspeicher basierend auf dem Zertifikatstyp aus**.
15. Klicken Sie auf **Fertig stellen und OK.**

Nachdem der Import des Zertifikats abgeschlossen ist, müssen Sie den Wireless-Client (Windows-Desktop in diesem Beispiel) für EAP-TLS konfigurieren.

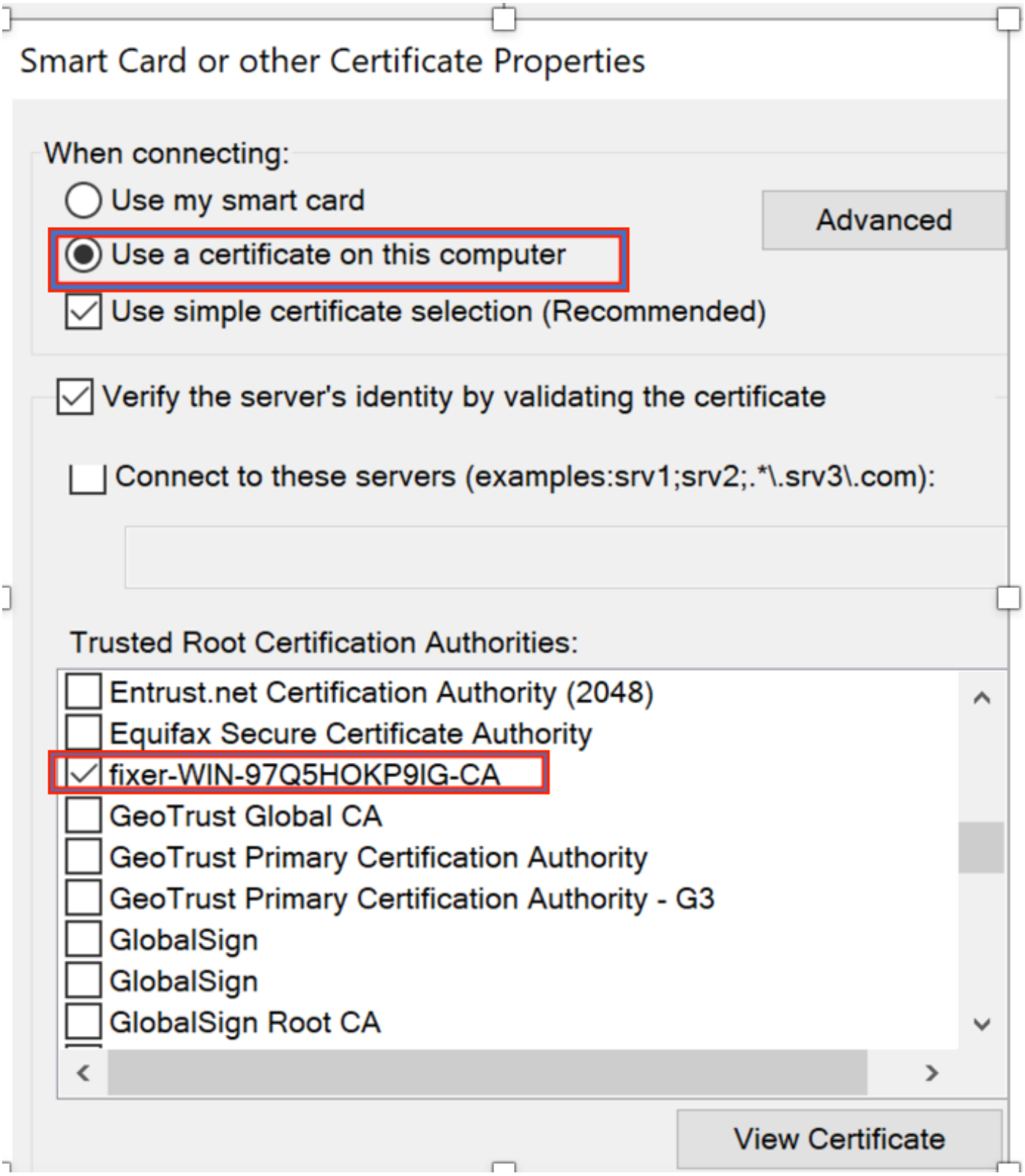
Wireless-Profil für EAP-TLS

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

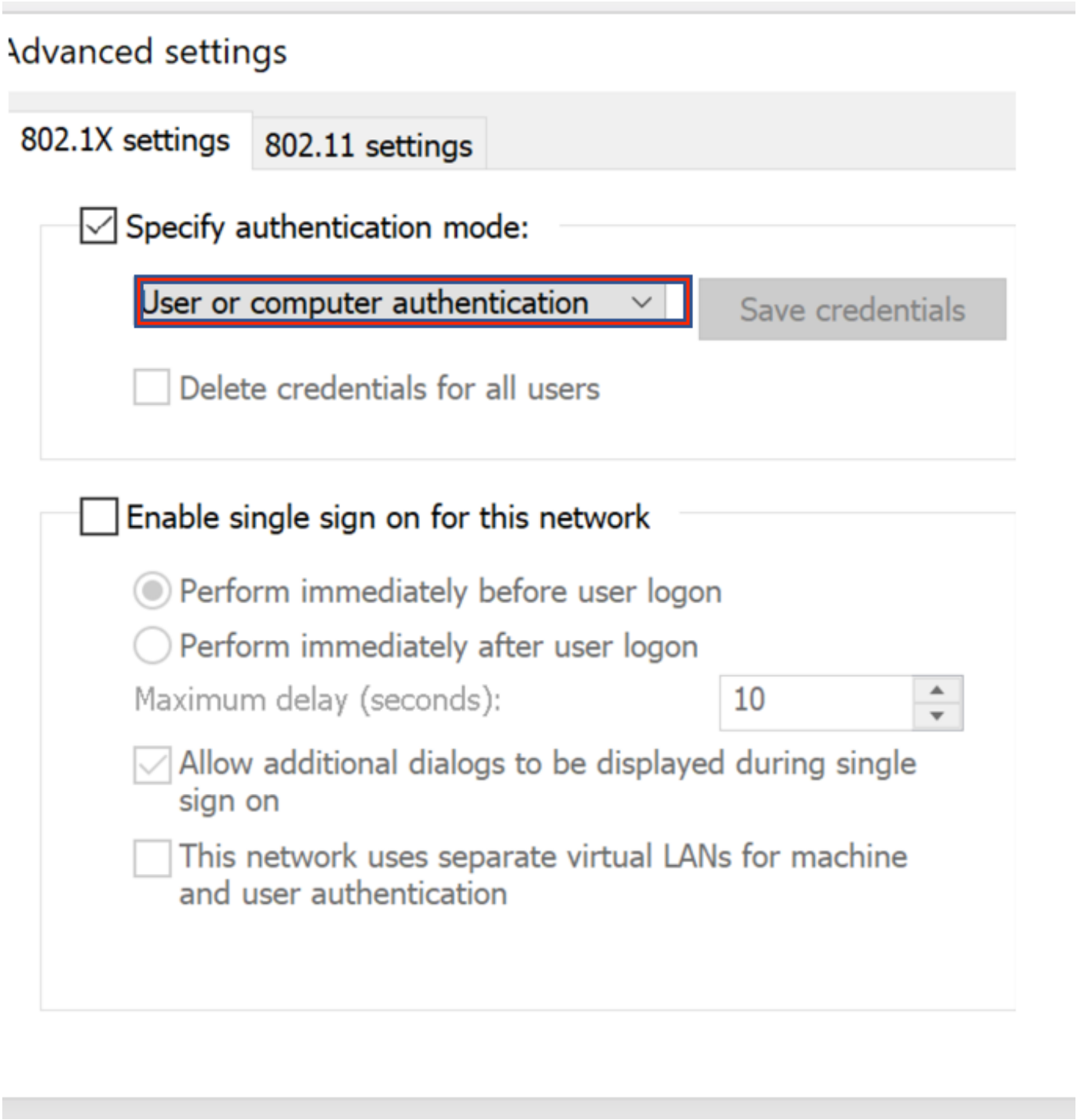
Schritt 2: Wählen Sie **Microsoft: Smartcard oder anderes Zertifikat** und klicken Sie auf **OK**, wie im Bild gezeigt.



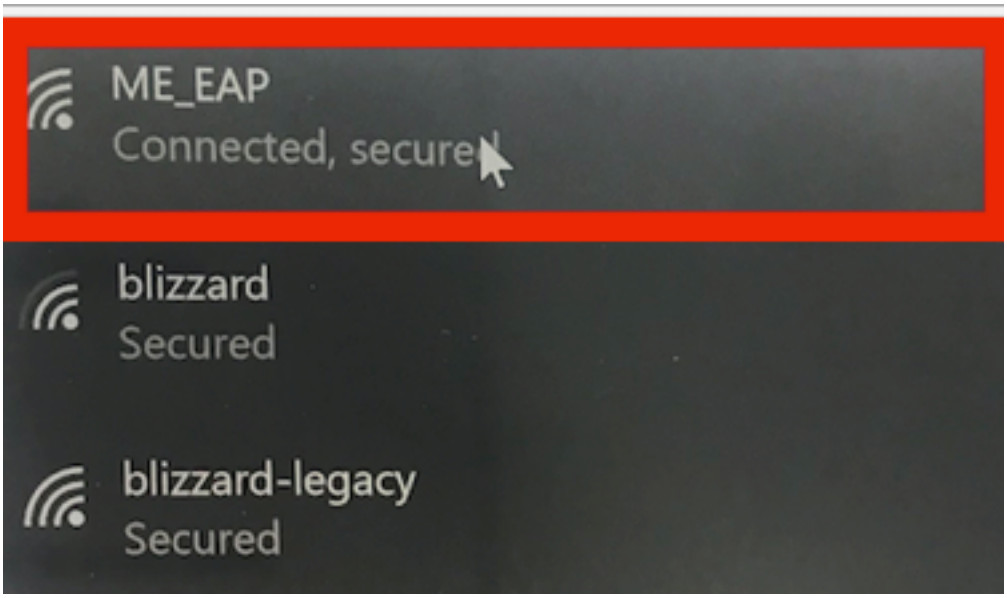
Schritt 3: Klicken Sie auf **Einstellungen**, und wählen Sie das Stammzertifikat aus, das vom CA-Server ausgegeben wurde, wie im Bild gezeigt.



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



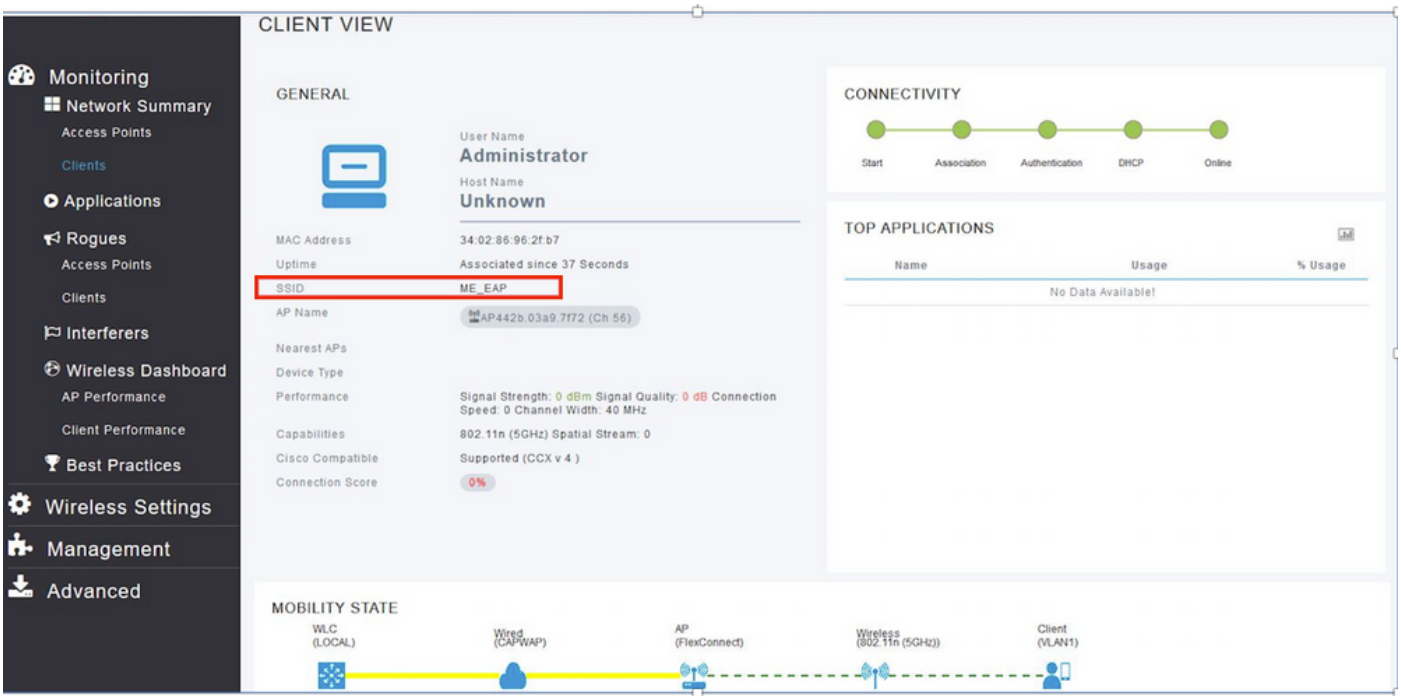
Schritt 5: Versuchen Sie jetzt erneut, eine Verbindung zum Wireless-Netzwerk herzustellen, wählen Sie das richtige Profil (in diesem Beispiel EAP) aus, und **stellen Sie eine Verbindung her**. Sie sind mit dem Wireless-Netzwerk verbunden, wie im Bild gezeigt.

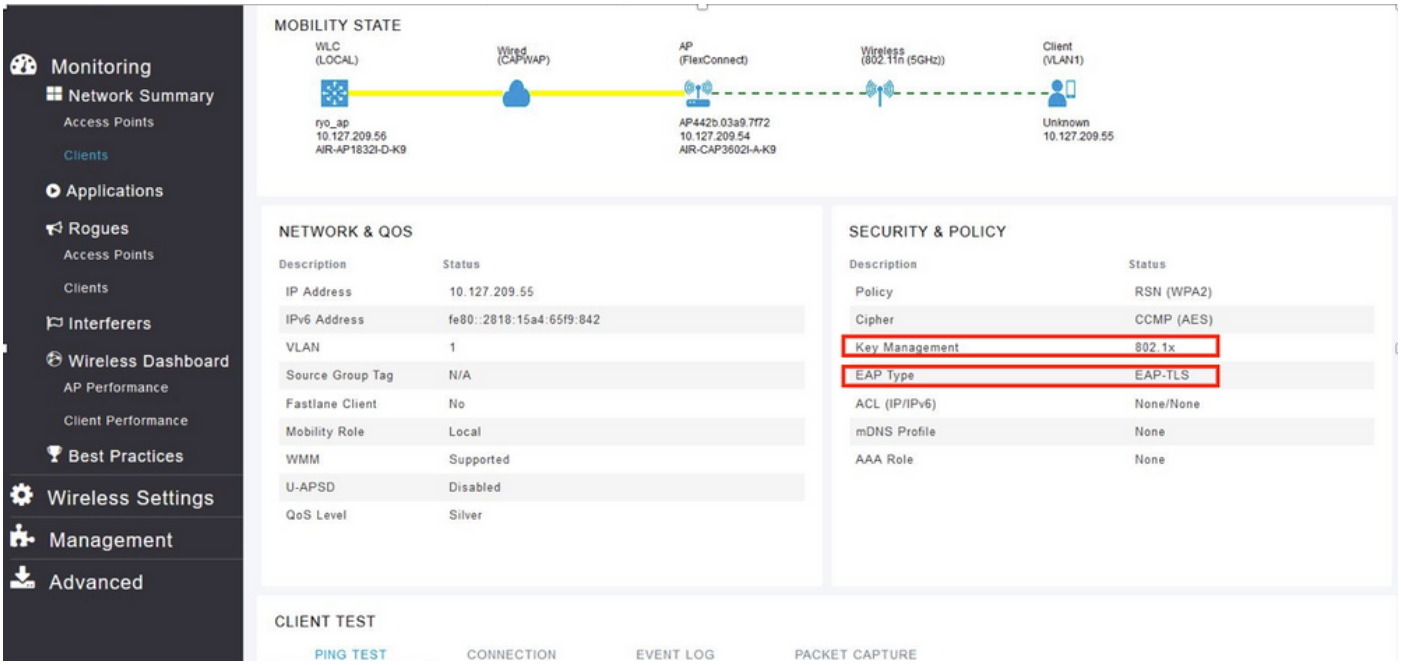


Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: Beim Client-EAP-Typ muss es sich um EAP-TLS handeln. Dies bedeutet, dass der Client die Authentifizierung mithilfe von EAP-TLS abgeschlossen hat, IP-Adresse erhalten hat und bereit ist, den Datenverkehr wie in den Bildern gezeigt zu übergeben.

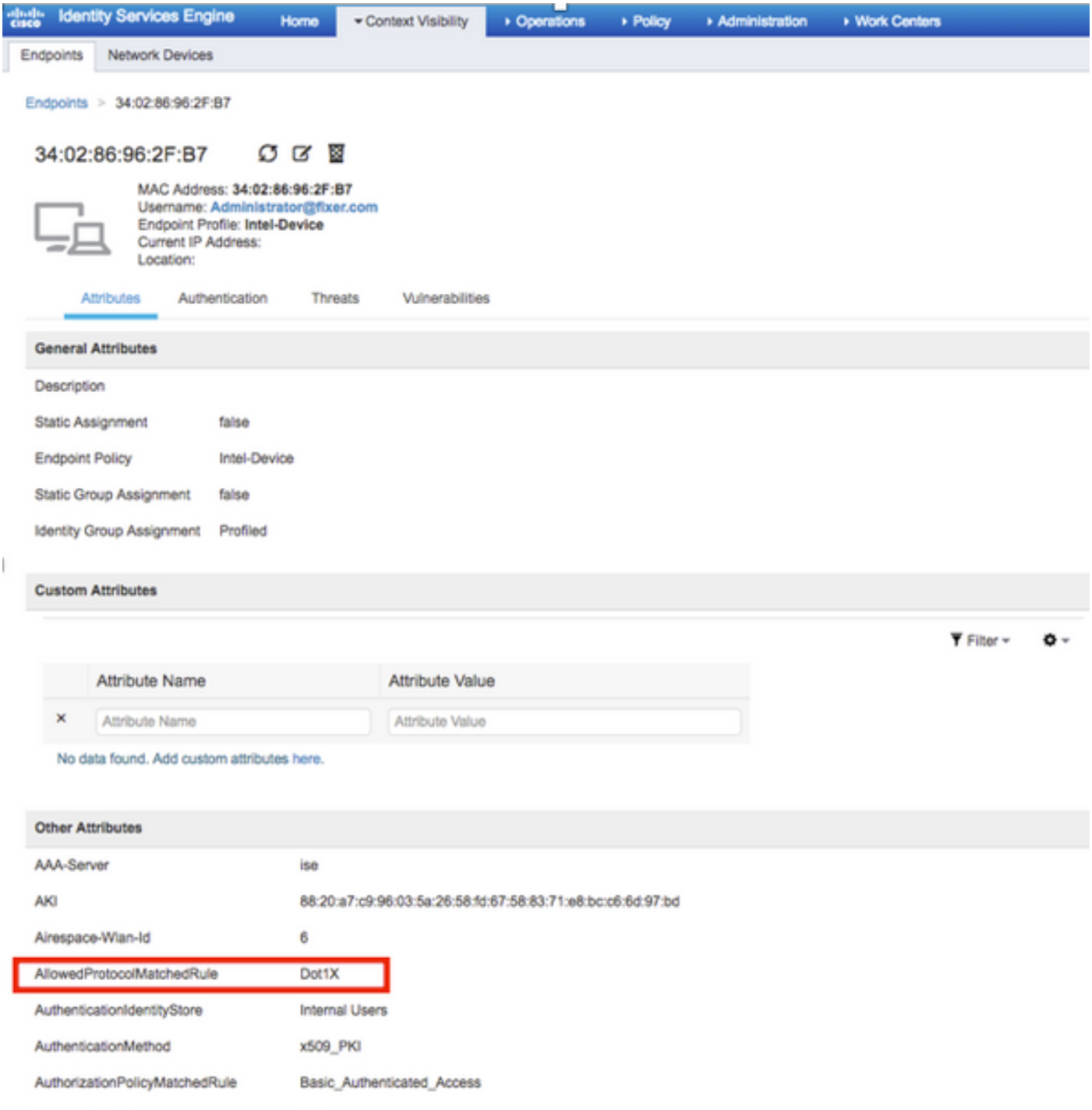




Schritt 2: Nachfolgend finden Sie die Client-Details aus der CLI des Controllers (Ausgabe geklickt):

```
(Cisco Controller) > show client detail 34:02:86:96:2f:b7
Client MAC Address.............................. 34:02:86:96:2f:b7
Client Username ................................ Administrator
AP MAC Address.................................. c8:f9:f9:83:47:b0
AP Name......................................... AP442b.03a9.7f72
AP radio slot Id................................ 1
Client State.................................... Associated
Client User Group............................... Administrator
Client NAC OOB State............................ Access
Wireless LAN Id................................. 6
Wireless LAN Network Name (SSID)................ ME_EAP
Wireless LAN Profile Name....................... ME_EAP
Hotspot (802.11u)............................... Not Supported
BSSID........................................... c8:f9:f9:83:47:ba
Connected For .................................. 18 secs
Channel......................................... 56
IP Address...................................... 10.127.209.55
Gateway Address................................. 10.127.209.49
Netmask......................................... 255.255.255.240
IPv6 Address.................................... fe80::2818:15a4:65f9:842
--More-- or (q)uit
Security Policy Completed....................... Yes
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 3: Navigieren Sie auf der ISE zu **Kontext-Transparenz > Endpunkte > Attribute**, wie in den Bildern gezeigt.


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Endpoints
Network Devices
Endpoints > 34:02:86:96:2F:B7
34:02:86:96:2F:B7
MAC Address: 34:02:86:96:2F:B7
Username: Administrator@fixer.com
Endpoint Profile: Intel-Device
Current IP Address:
Location:
Attributes
Authentication
Threats
Vulnerabilities
General Attributes
Description
Static Assignment false
Endpoint Policy Intel-Device
Static Group Assignment false
Identity Group Assignment Profiled
Custom Attributes
Filter
Attribute Name
Attribute Value
Attribute Name
Attribute Value
No data found. Add custom attributes here.
Other Attributes
AAA-Server ise
AKI 88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd
Airespace-Wlan-Id 6
AllowedProtocolMatchedRule Dot1X
AuthenticationIdentityStore Internal Users
AuthenticationMethod x509_PKI
AuthorizationPolicyMatchedRule Basic_Authenticated_Access

BYODRegistration	Unknown
Called-Station-ID	c8-f9-f9-83-47-b0:ME_EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	344
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.127.209.56
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	21
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	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA\,DC=fixer\,DC=co
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com
Key Usage	0, 2
Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7

MatchedPolicy	Intel-Device
MessageCode	5411
NAS-IP-Address	10.127.209.56
NAS-Identifier	ryo_ap
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	ryo_ap
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	Drop
SSID	c8-f9-f9-83-47-b0:ME_EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.