

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

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[EAP-TLS-Fluss](#)

[Schritte im EAP-TLS-Fluss](#)

[Konfigurieren](#)

[Cisco Mobility Express](#)

[ISE mit Cisco Mobility Express](#)

[EAP-TLS-Einstellungen](#)

[Mobility Express-Einstellungen für die ISE](#)

[Vertrauenszertifikat auf ISE](#)

[Client für EAP-TLS](#)

[Benutzerzertifikat auf dem Client-Computer herunterladen \(Windows-Desktop\)](#)

[Wireless-Profil für EAP-TLS](#)

[Überprüfen](#)

[Fehlerbehebung](#)

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

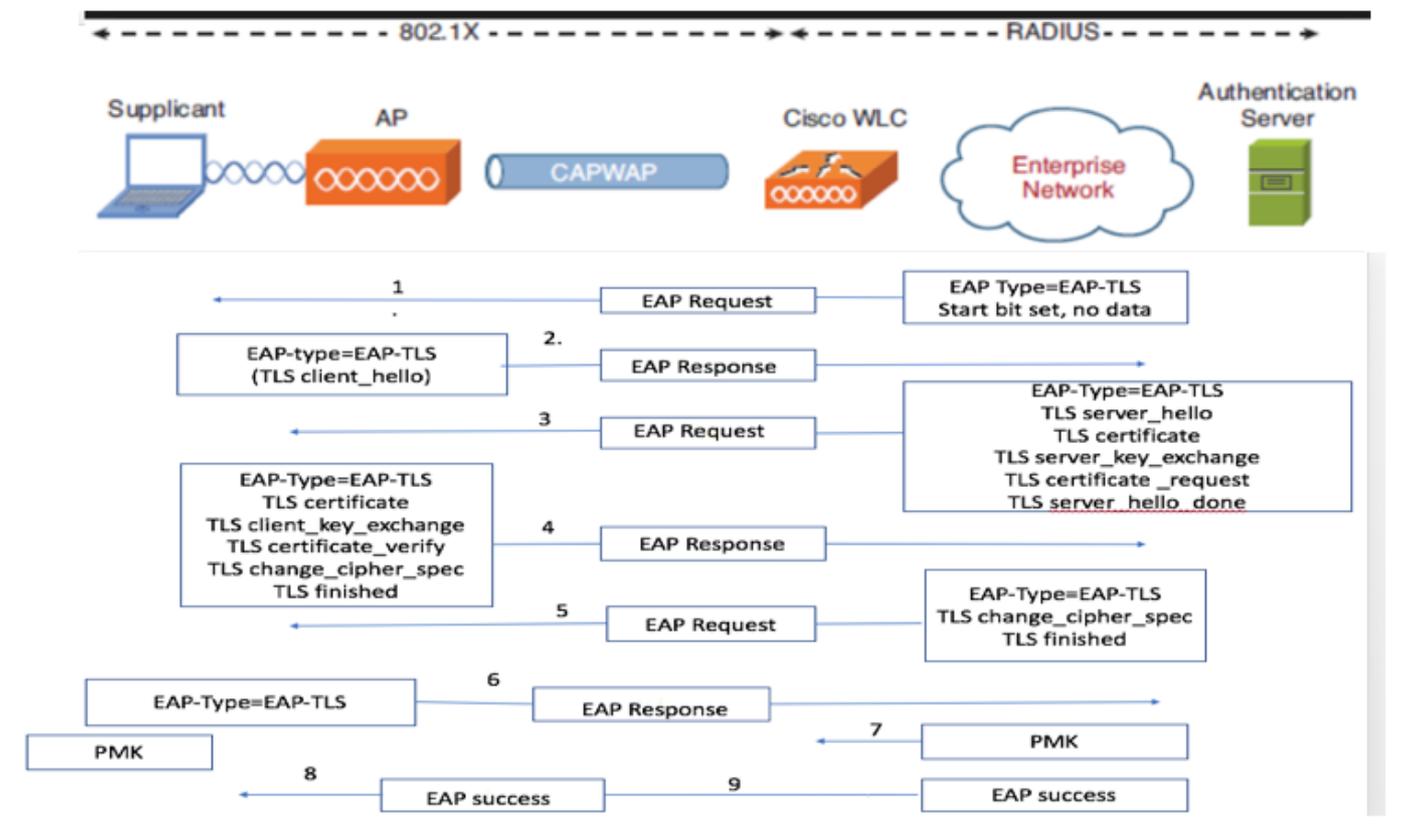
Hardwareversionen:

- 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
```

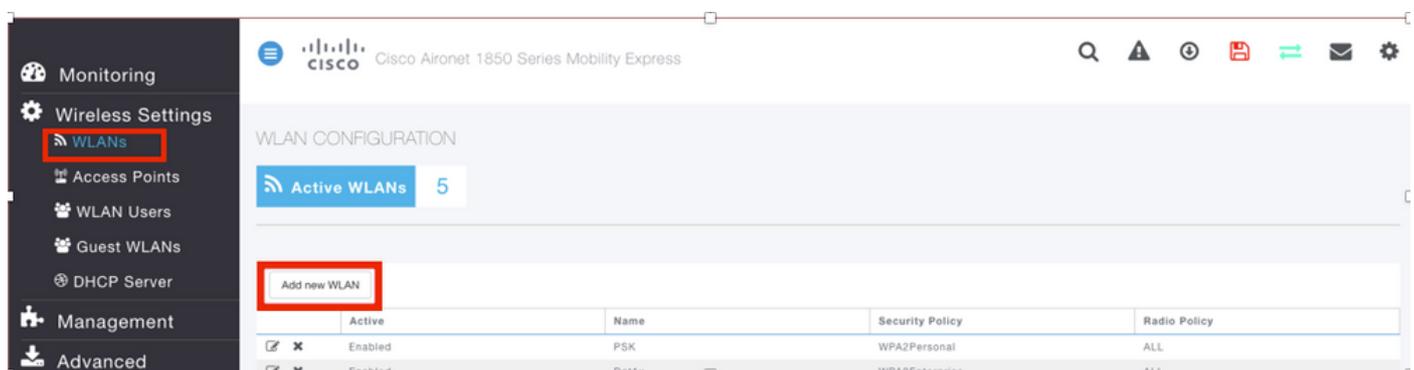
8. Nachdem der Client sich erfolgreich authentifiziert hat, antwortet der RADIUS-Server mit einer Access-Challenge, die die Meldung "change_cipher_spec" und die Handshake-Fertigstellung enthält. Beim Empfang dieser Nachricht überprüft der Client den Hash, um den RADIUS-Server zu authentifizieren. Beim 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.

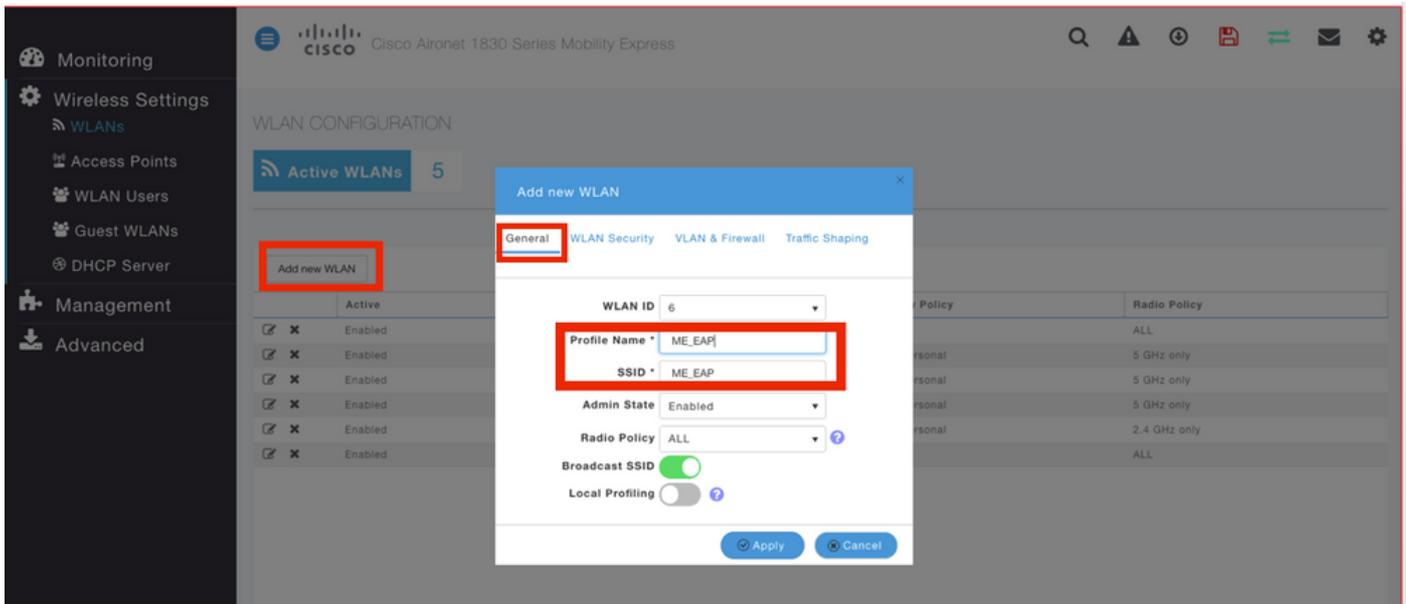
Konfigurieren

Cisco Mobility Express

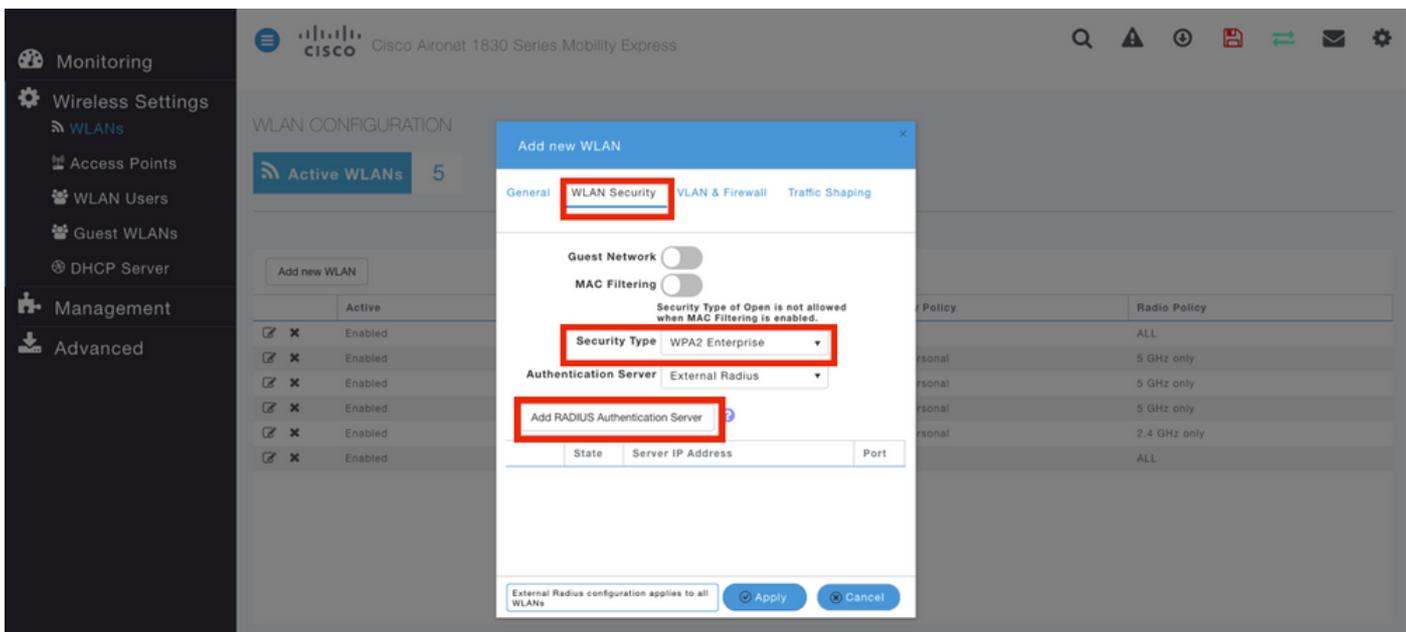
Schritt 1: Der erste Schritt besteht in der Erstellung eines WLAN auf Mobility Express. Um ein WLAN zu erstellen, navigieren Sie zu **WLAN > Add new WLAN** wie im Bild gezeigt.



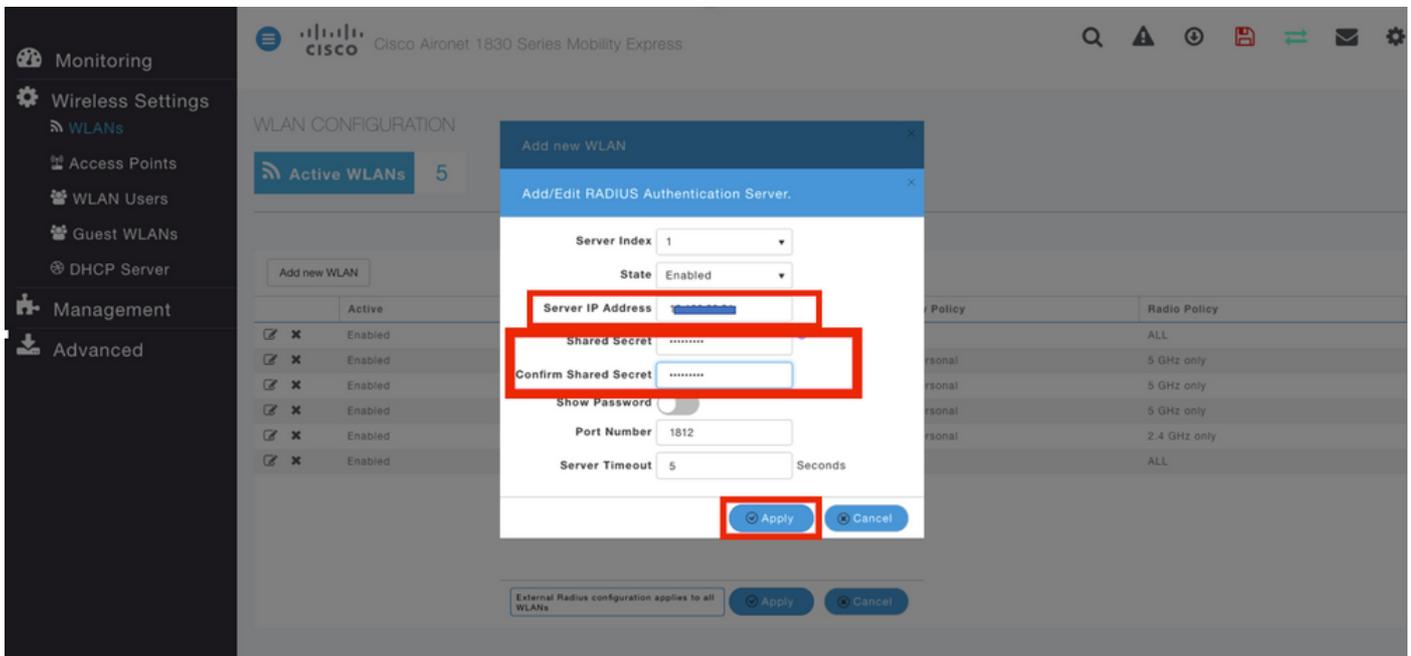
Schritt 2: Ein neues Popup-Fenster wird angezeigt, wenn Sie auf **Neues WLAN hinzufügen** klicken. Um einen Profilnamen zu erstellen, navigieren Sie zu **Neues WLAN hinzufügen > Allgemein**, wie im Bild gezeigt.



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**.



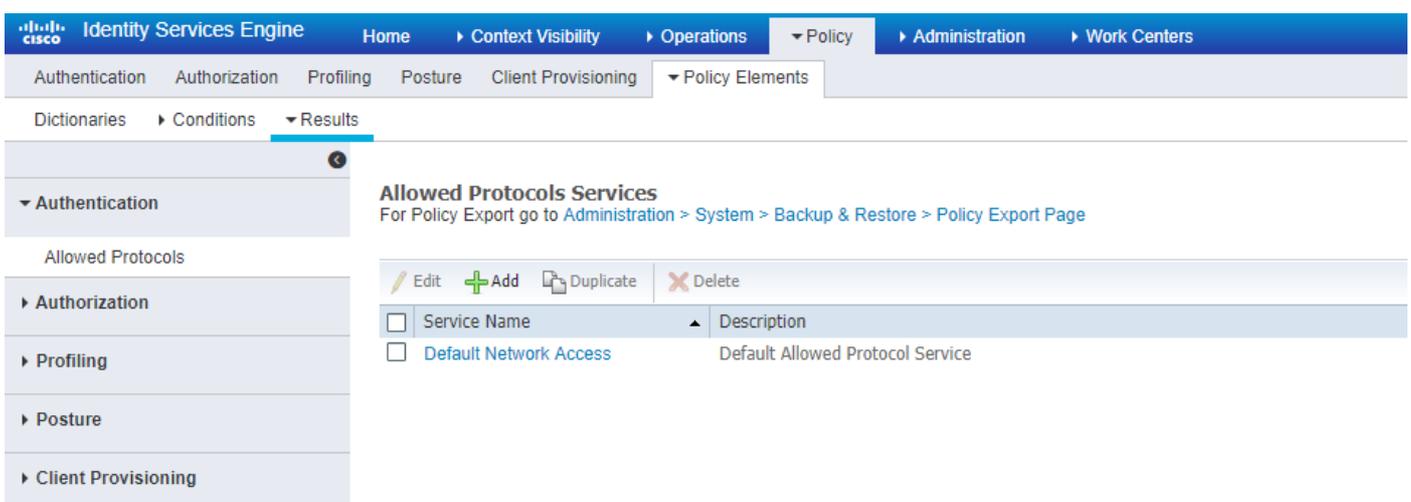
ISE mit Cisco Mobility Express

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.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionaries > Conditions > Results

Allowed Protocols Services List > **New Allowed Protocols Service**

Allowed Protocols

Name

Description

Allowed Protocols

- Authentication Bypass
 - Process Host Lookup *(?)*
- Authentication Protocols
 - Allow PAP/ASCII
 - Allow CHAP
 - Allow MS-CHAPv1
 - Allow MS-CHAPv2
 - Allow EAP-MD5
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy *(?)*
 - Enable Stateless Session Resume
 - Session ticket time to live
 - Proactive session ticket update will occur after % of Time To Live has expired
 - Allow LEAP
 - Allow PEAP
 - PEAP Inner Methods
 - Allow EAP-MS-CHAPv2
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-GTC
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy *(?)*
 - Require cryptobinding TLV *(?)*

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).

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Add Duplicate Import Export Generate PAC Delete

Show All

Name	IP/Mask	Profile Name	Location	Type	Description
------	---------	--------------	----------	------	-------------

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

Network Devices List > New Network Device

Network Devices

Name

Description

* IP Address: / 32

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

RADIUS Authentication Settings

Enable Authentication Settings

Protocol RADIUS

* Shared Secret

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

CoA Port

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

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.

Identity Services Engine

Administration > Certificates

Certificate Management

Overview

System Certificates

Endpoint Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Sets...

Certificate Authority

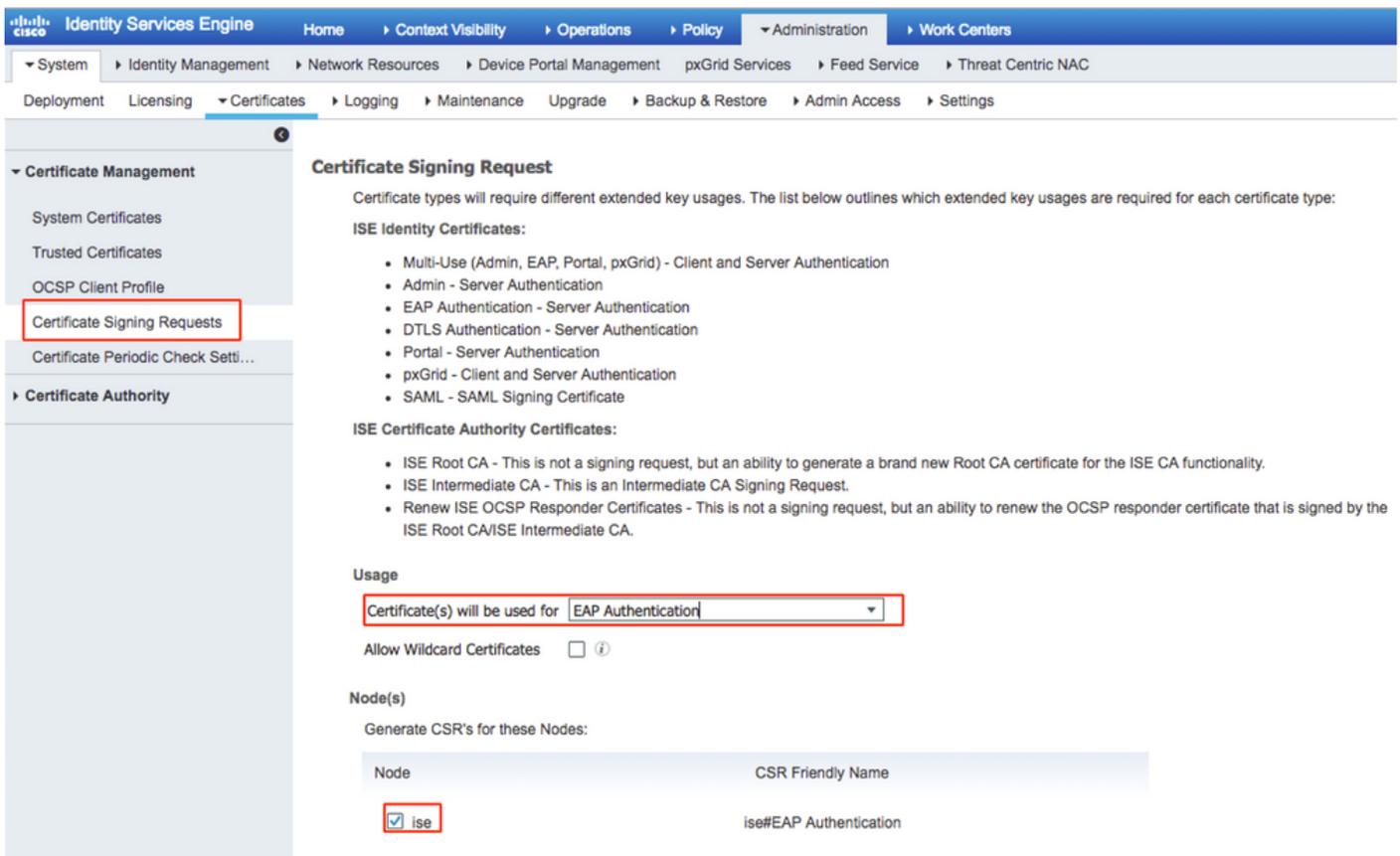
Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

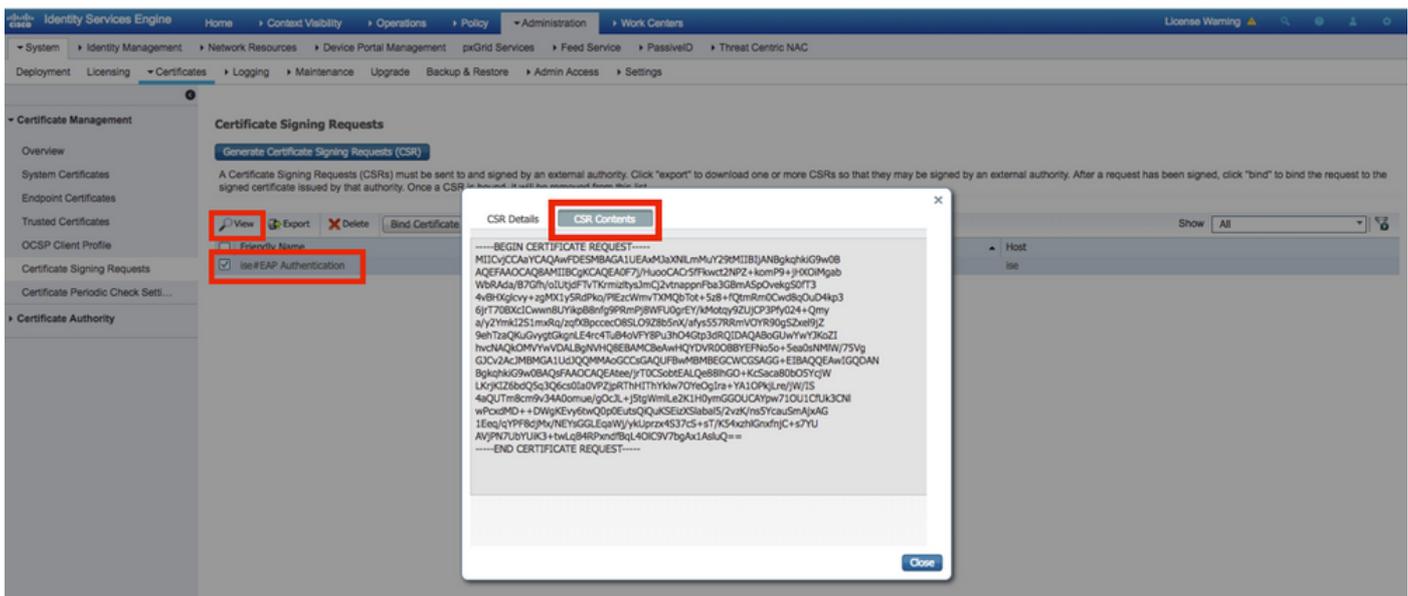
A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input type="checkbox"/> ise#EAP Authentication	CN=ise.c.com	2048		Wed, 11 Jul 2018	ise

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:

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

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.

Microsoft Active Directory Certificate Services – fixer-WIN-97Q5HOKP9IG-CA

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#)

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.

Microsoft Active Directory Certificate Services – fixer-WIN-97Q5HOKP9IG-CA Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

Additional Attributes:

Attributes:

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.

Certificate Issued

The certificate you requested was issued to you.

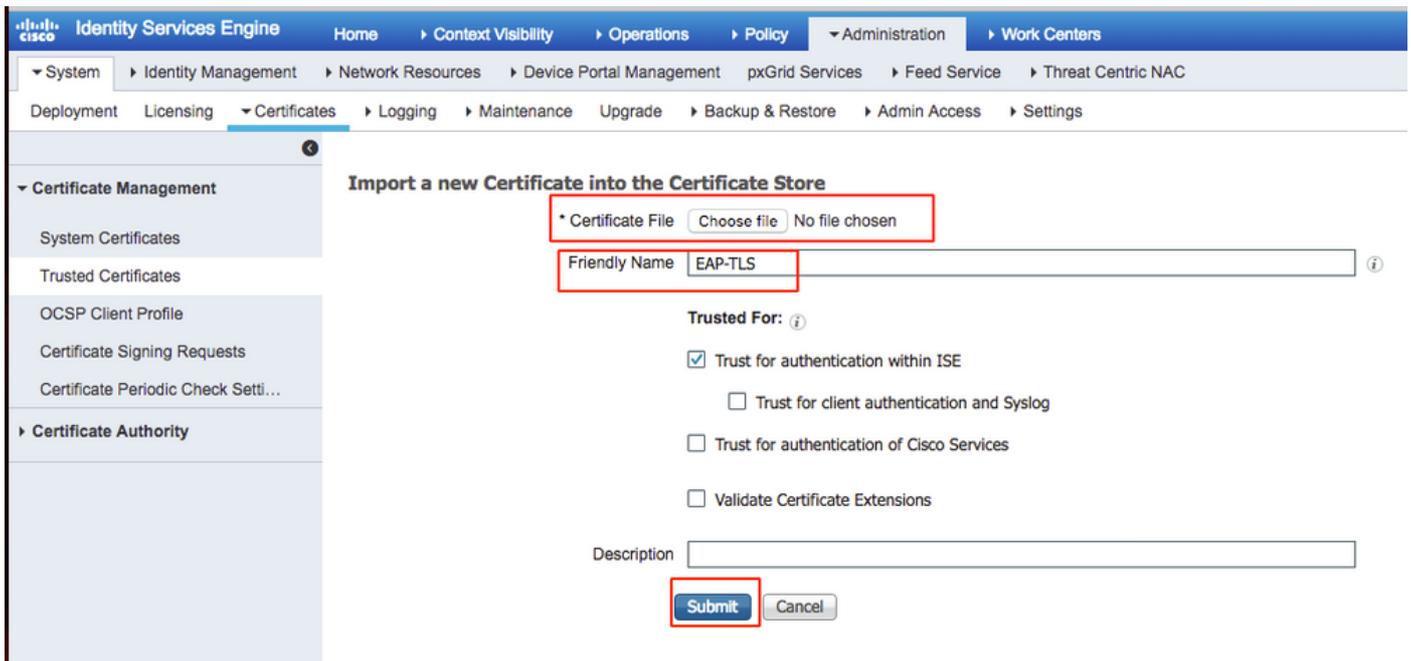
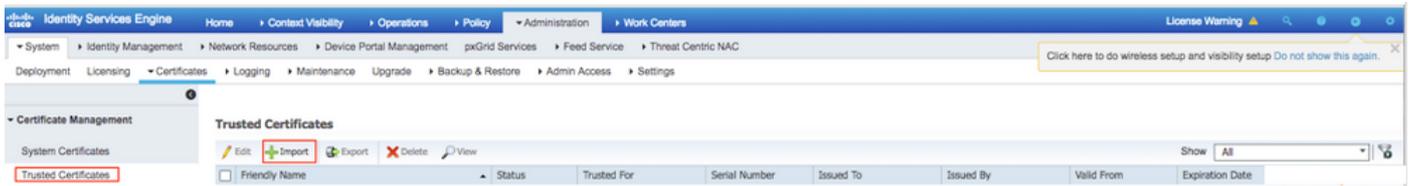
DER encoded or Base 64 encoded



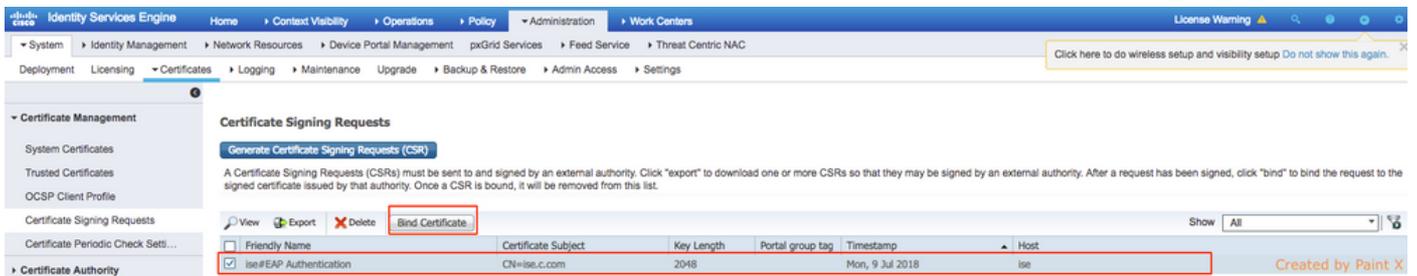
[Download certificate](#)

[Download certificate chain](#)

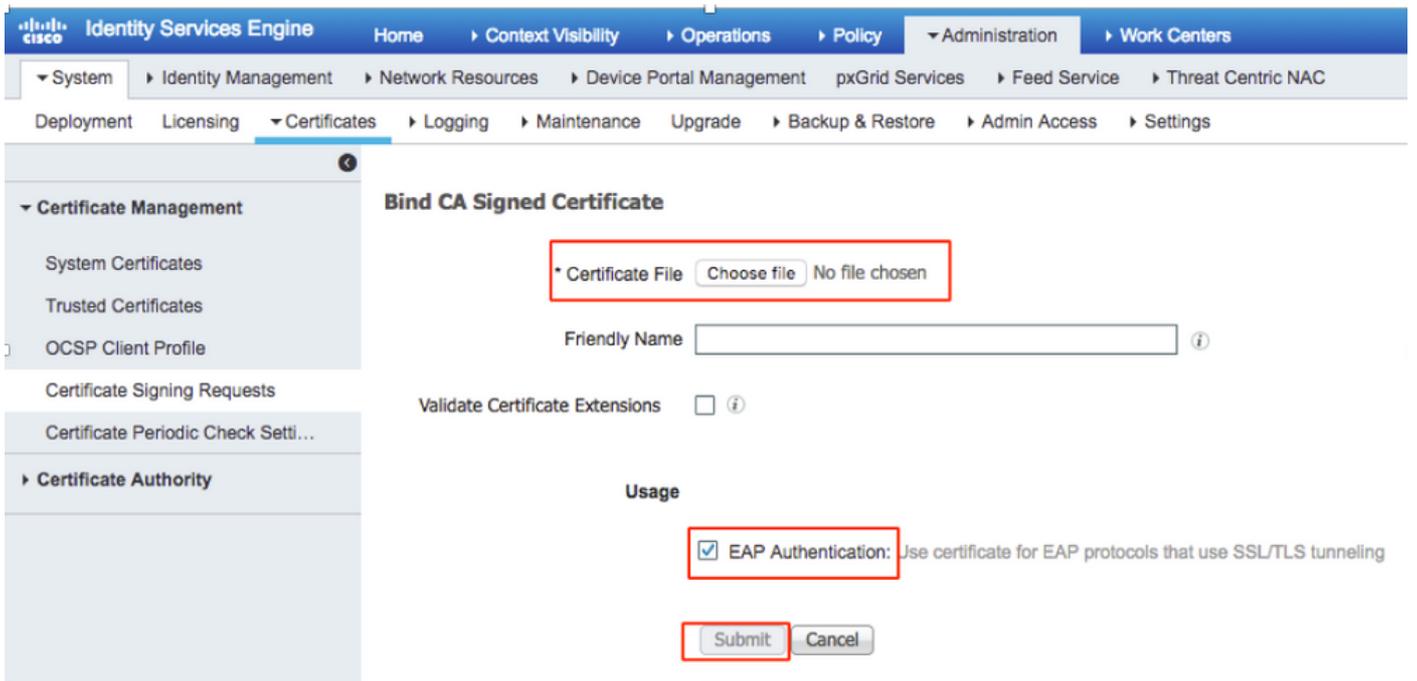
Schritt 9: Der Zertifikatsdownload ist für den ISE-Server abgeschlossen. Sie können das Zertifikat extrahieren. Das Zertifikat enthält zwei Zertifikate, ein Stammzertifikat und ein anderes Zwischenzertifikat. Das Stammzertifikat kann unter **Administration > Certificates > Trusted Certificates > Import**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



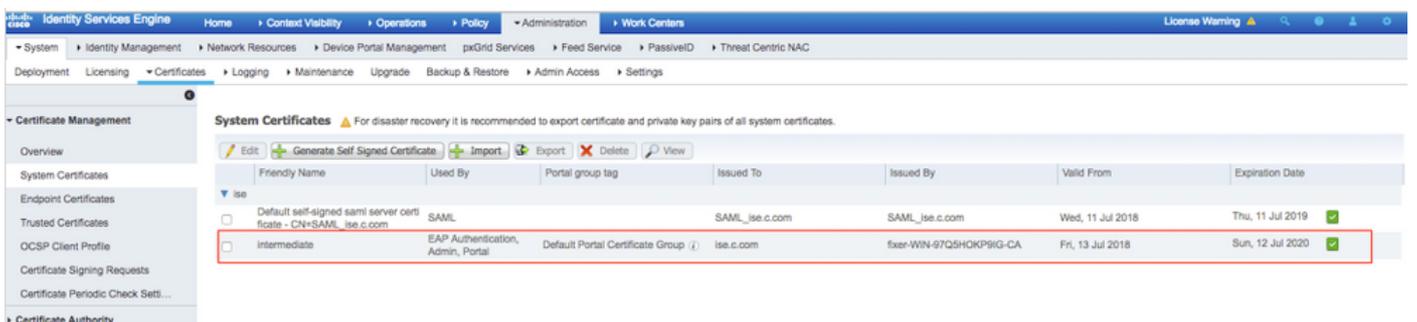
Schritt 10: Wenn Sie auf **Senden** klicken, wird das Zertifikat der Liste der vertrauenswürdigen Zertifikate hinzugefügt. Außerdem wird das Zwischenzertifikat benötigt, um wie im Bild gezeigt an CSR zu binden.



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.

Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
ZzAJVkd0PEONkCsBJ/3qJJeeMlZqxnL7BVIspJry  
aF412aLpmDFp1PfvZ3VaP6Oa/mej3IXh0RFxBUII  
we0h06+V+eh71jeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxF1j3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

Attributes:

Submit >

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.

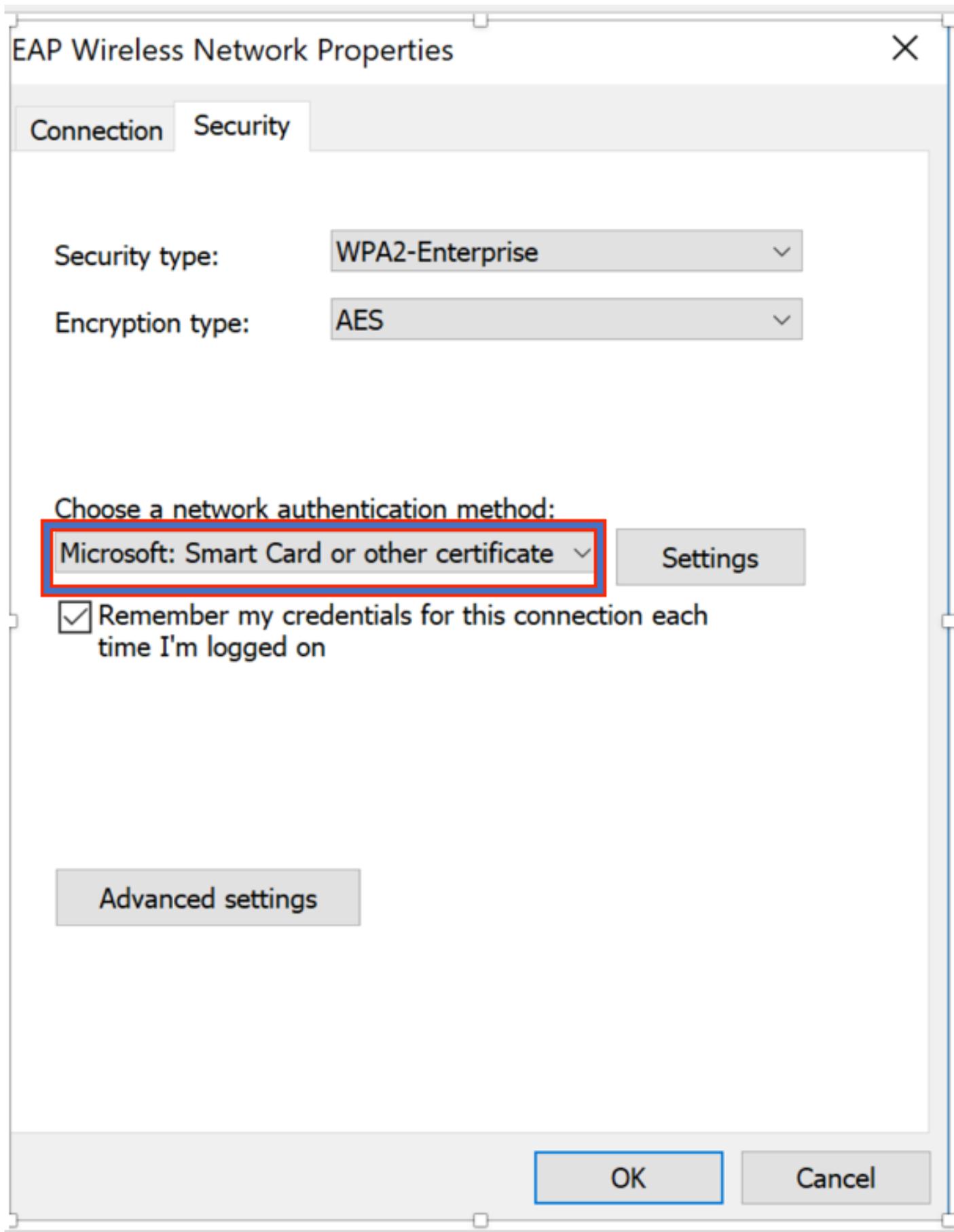
5. Wählen Sie **Lokaler Computer > Fertig stellen**
6. Klicken Sie auf **OK**, um das Snap-In-Fenster zu schließen.
7. Klicken Sie auf **[+]** neben **Zertifikate > Personal > Zertifikate**.
8. Klicken Sie mit der rechten Maustaste auf **Zertifikate** und wählen Sie **Alle Tasks > Importieren aus**.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

Smart Card or other Certificate Properties

When connecting:

Use my smart card

Use a certificate on this computer

Advanced

Use simple certificate selection (Recommended)

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1; srv2; *.srv3\com):

Trusted Root Certification Authorities:

Entrust.net Certification Authority (2048)

Equifax Secure Certificate Authority

fixer-WIN-97Q5HOKP9IG-CA

GeoTrust Global CA

GeoTrust Primary Certification Authority

GeoTrust Primary Certification Authority - G3

GlobalSign

GlobalSign

GlobalSign Root CA

View Certificate

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

Advanced settings

802.1X settings

802.11 settings

Specify authentication mode:

User or computer authentication

Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

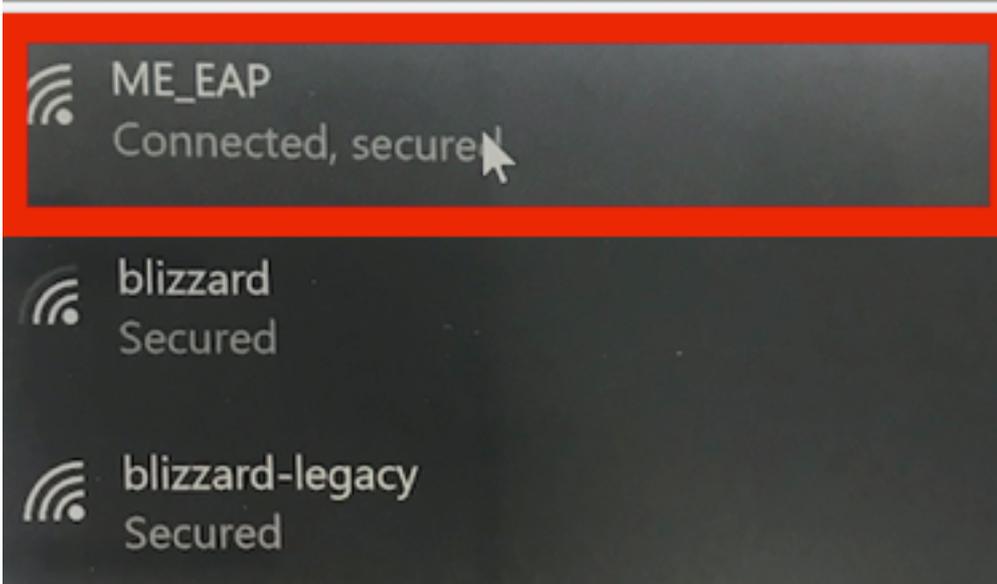
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

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.

The screenshot shows a network management console interface. On the left is a navigation menu with categories: Monitoring (Network Summary, Access Points, Clients), Applications, Rogues (Access Points, Clients), Interferers, Wireless Dashboard (AP Performance, Client Performance), Best Practices, Wireless Settings, Management, and Advanced. The main area is titled "CLIENT VIEW" and contains several sections:

- GENERAL**: Includes a laptop icon, User Name "Administrator", Host Name "Unknown", MAC Address "34:02:86:96:2f:b7", Uptime "Associated since 37 Seconds", SSID "ME_EAP" (highlighted with a red box), AP Name "AP442b.03a9.7f72 (Ch 56)", Nearest APs, Device Type, Performance (Signal Strength: 0 dBm, Signal Quality: 0 dB, Connection Speed: 0, Channel Width: 40 MHz), Capabilities "802.11n (5GHz) Spatial Stream: 0", Cisco Compatible "Supported (CCX v 4)", and Connection Score "0%".
- CONNECTIVITY**: A flow diagram showing the process: Start -> Association -> Authentication -> DHCP -> Online, with all steps marked as successful.
- TOP APPLICATIONS**: A table with columns "Name", "Usage", and "% Usage", showing "No Data Available!".
- MOBILITY STATE**: A diagram showing the network path: WLC (LOCAL) -> Wired (CAP-WAP) -> AP (FlexConnect) -> Wireless (802.11n (5GHz)) -> Client (VLAN1).

The screenshot displays the Cisco ISE GUI for a wireless client. The left sidebar contains navigation options like 'Monitoring', 'Wireless Settings', and 'Management'. The main area is divided into several sections:

- MOBILITY STATE:** A diagram showing the connection path from the WLC (LOCAL) through the Wired (CAPWAP) and AP (FlexConnect) to the Wireless (802.11n (5GHz)) and finally to the Client (VLAN1).
- NETWORK & QOS:** A table listing network parameters such as IP Address (10.127.209.55), IPv6 Address (fe80::2818:15a4:65f9:842), VLAN (1), and QoS Level (Silver).
- SECURITY & POLICY:** A table showing security settings. Two rows are highlighted with red boxes: 'Key Management' with status '802.1x' and 'EAP Type' with status 'EAP-TLS'.
- CLIENT TEST:** A section with tabs for 'PING TEST', 'CONNECTION', 'EVENT LOG', and 'PACKET CAPTURE'.

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.

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
<input type="text" value="Attribute Name"/>	<input type="text" value="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, 1.3.6.1.4.1.311.1f
FailureReason	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9\G-CA,DC=fixer,DC=cc
Issuer - Common Name	fixer-WIN-97Q5HOKP9\G-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"
OpenSSLStack	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.