

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

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[EAP-TLS-Fluss](#)

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

[Konfigurieren](#)

[Cisco Wireless LAN-Controller](#)

[ISE mit Cisco WLC](#)

[EAP-TLS-Einstellungen](#)

[WLC-Einstellungen auf der ISE](#)

[Neuen Benutzer auf ISE erstellen](#)

[Zertifikat auf ISE vertrauen](#)

[Client für EAP-TLS](#)

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

[Wireless-Profil für EAP-TLS](#)

[Überprüfung](#)

[Fehlerbehebung](#)

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-

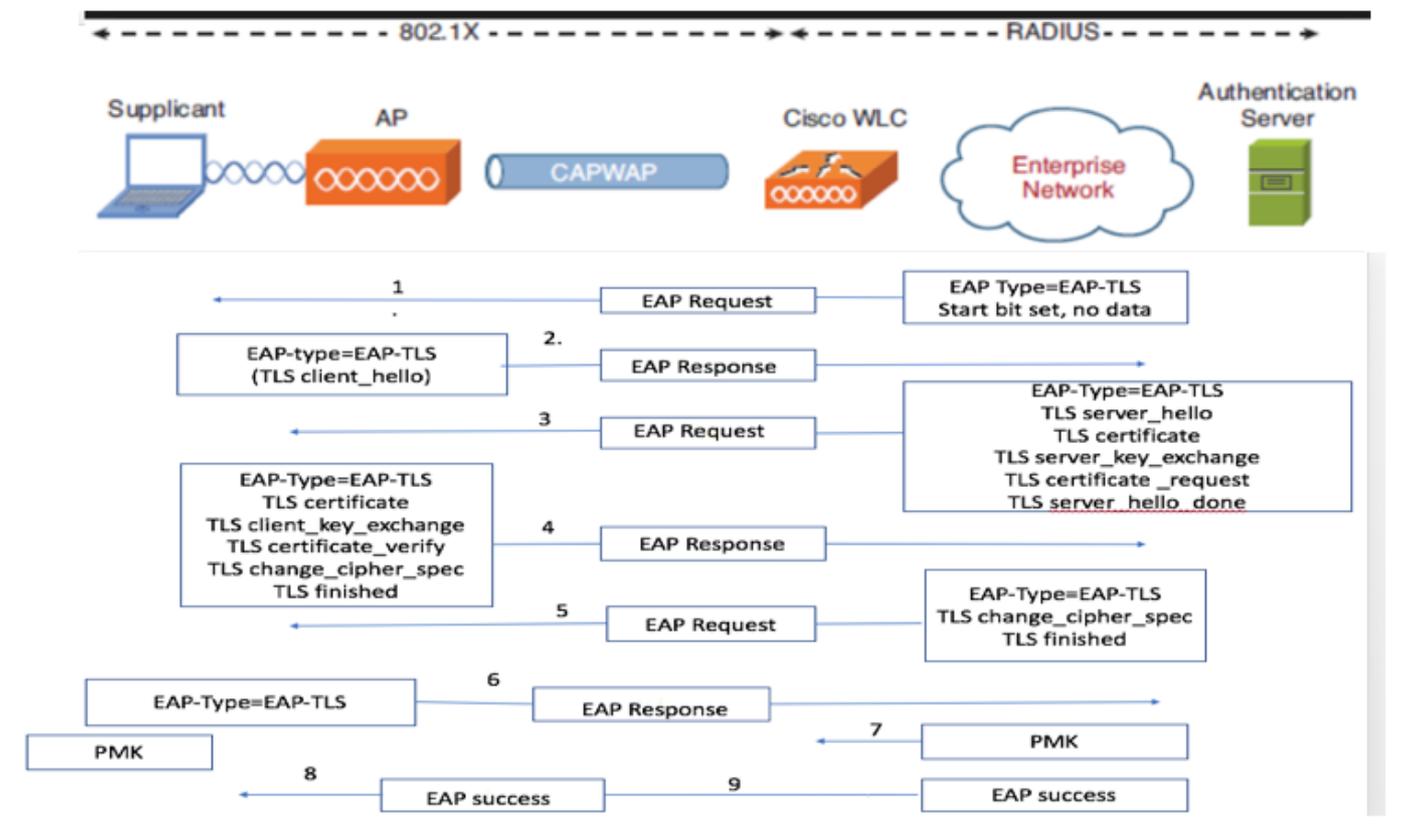
Versionen:

- 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.

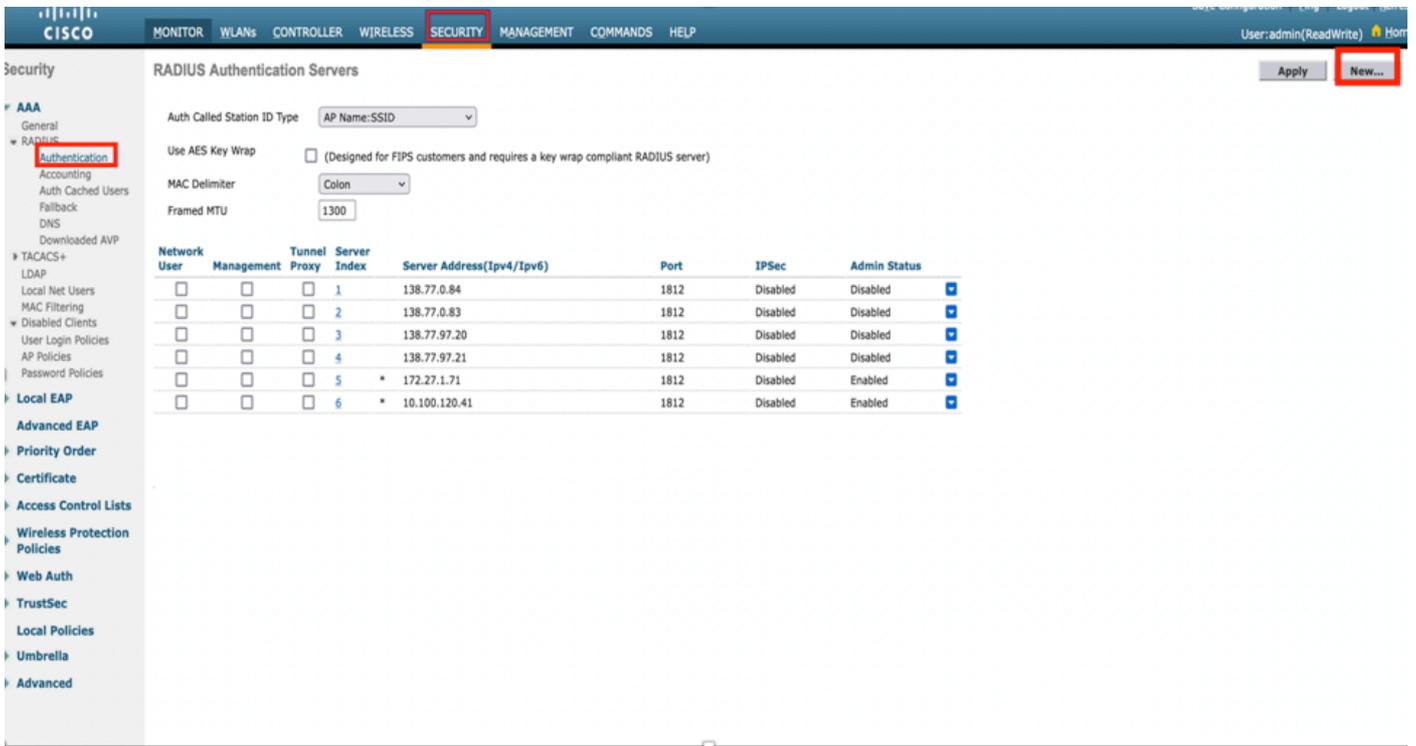
8/9. EAP-Success wird schließlich vom Server an den Authentifikator gesendet, der dann an den Supplicant weitergeleitet wird.

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

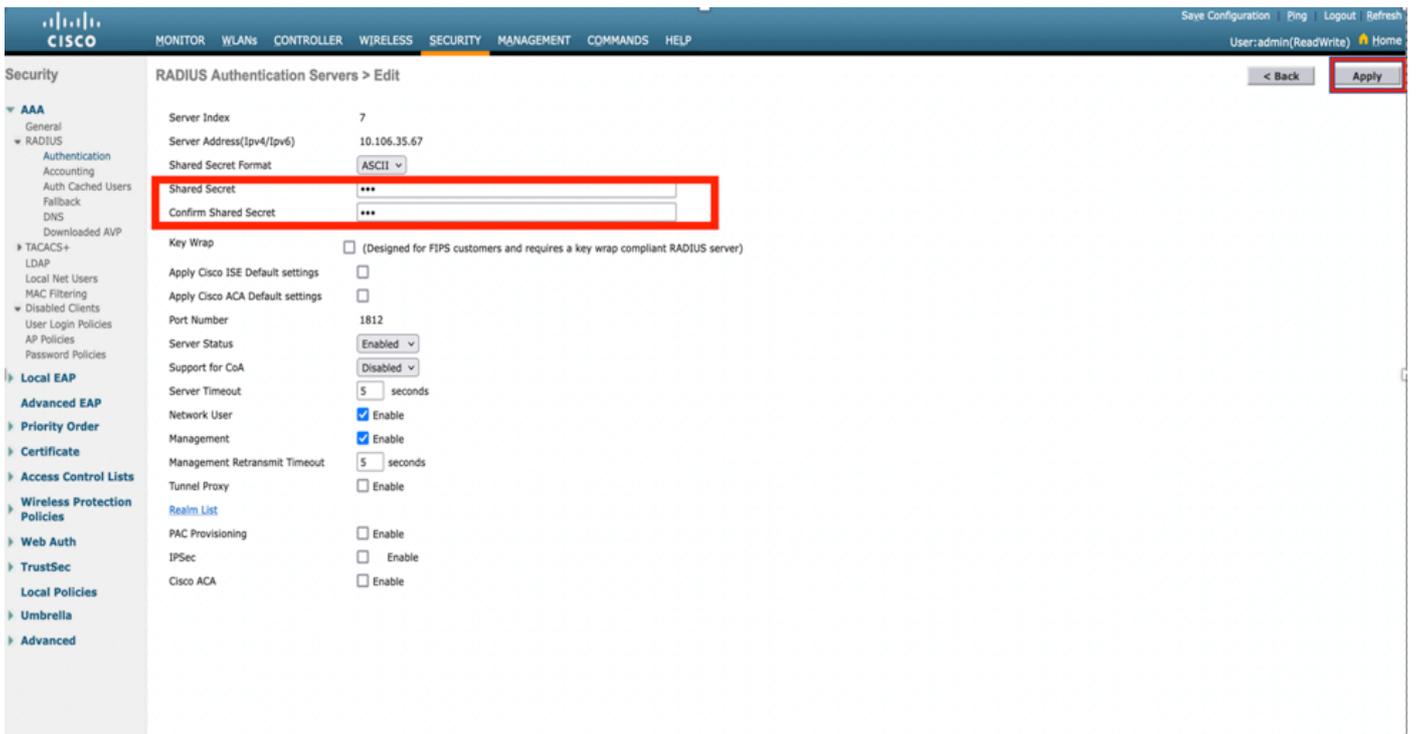
Konfigurieren

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.



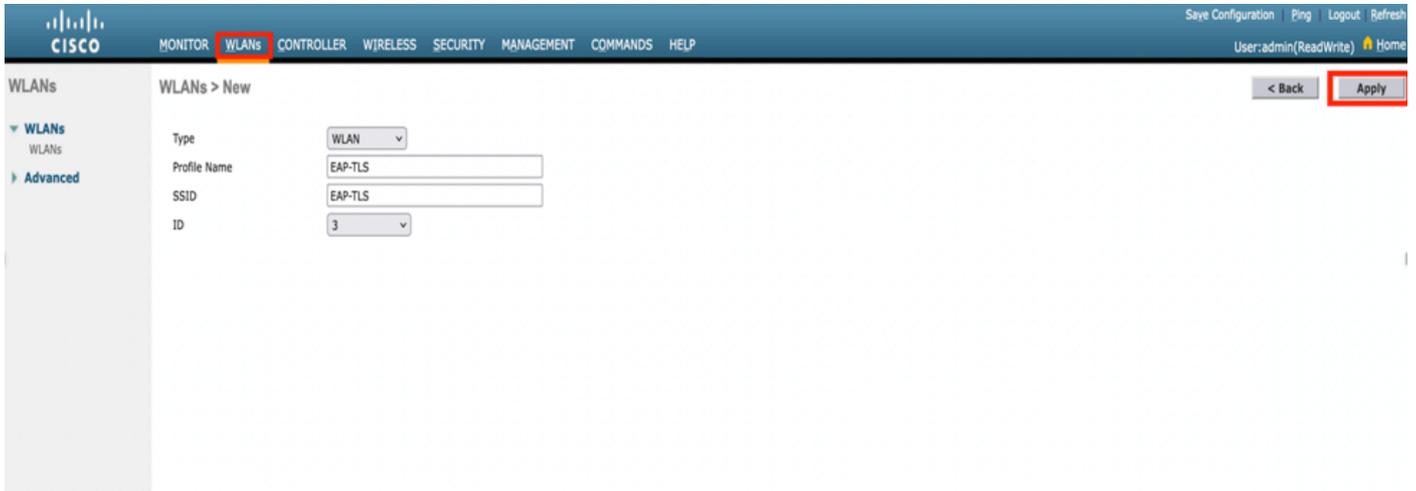
Schritt 3: Erstellen eines WLAN für die RADIUS-Authentifizierung

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.

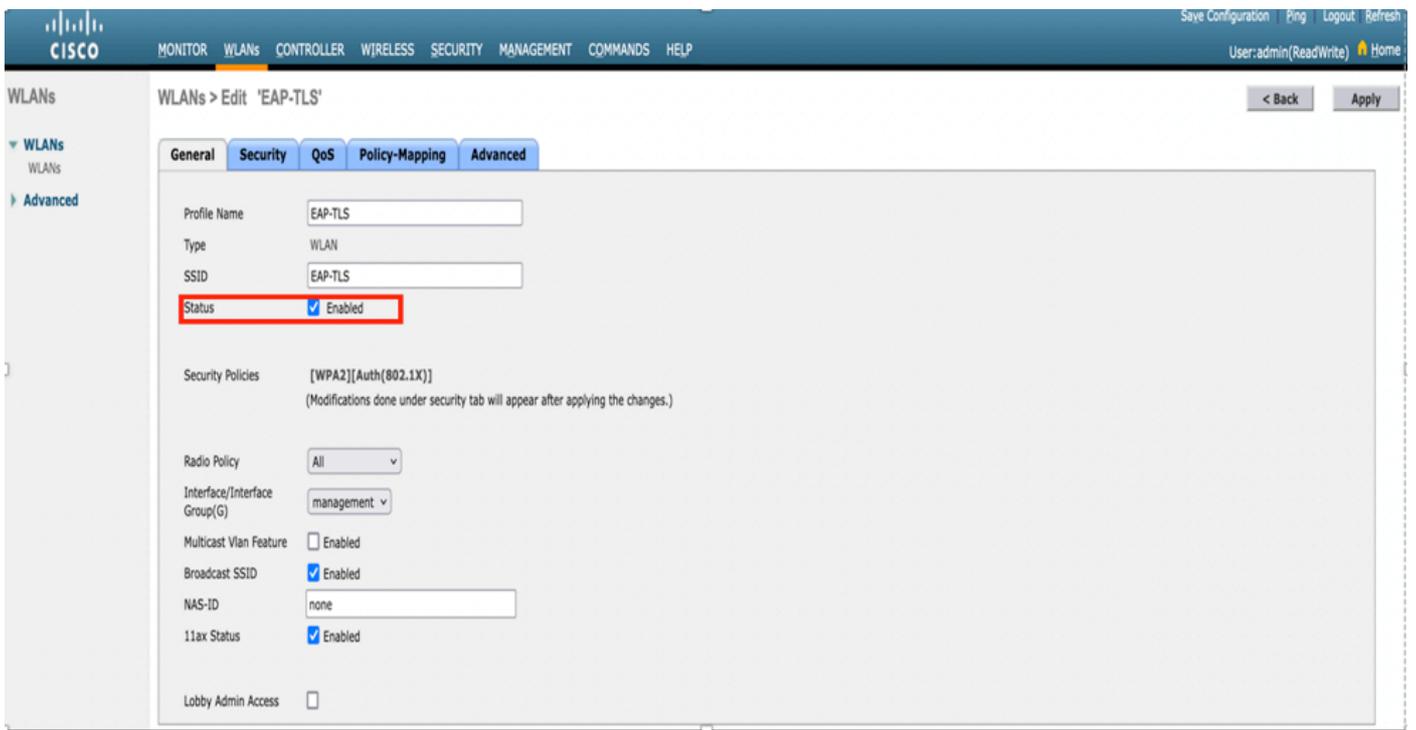
Schritt 4. Wählen Sie **WLANs** aus dem Hauptmenü, wählen Sie **Create New** und klicken Sie auf **Go** wie in der Abbildung dargestellt.



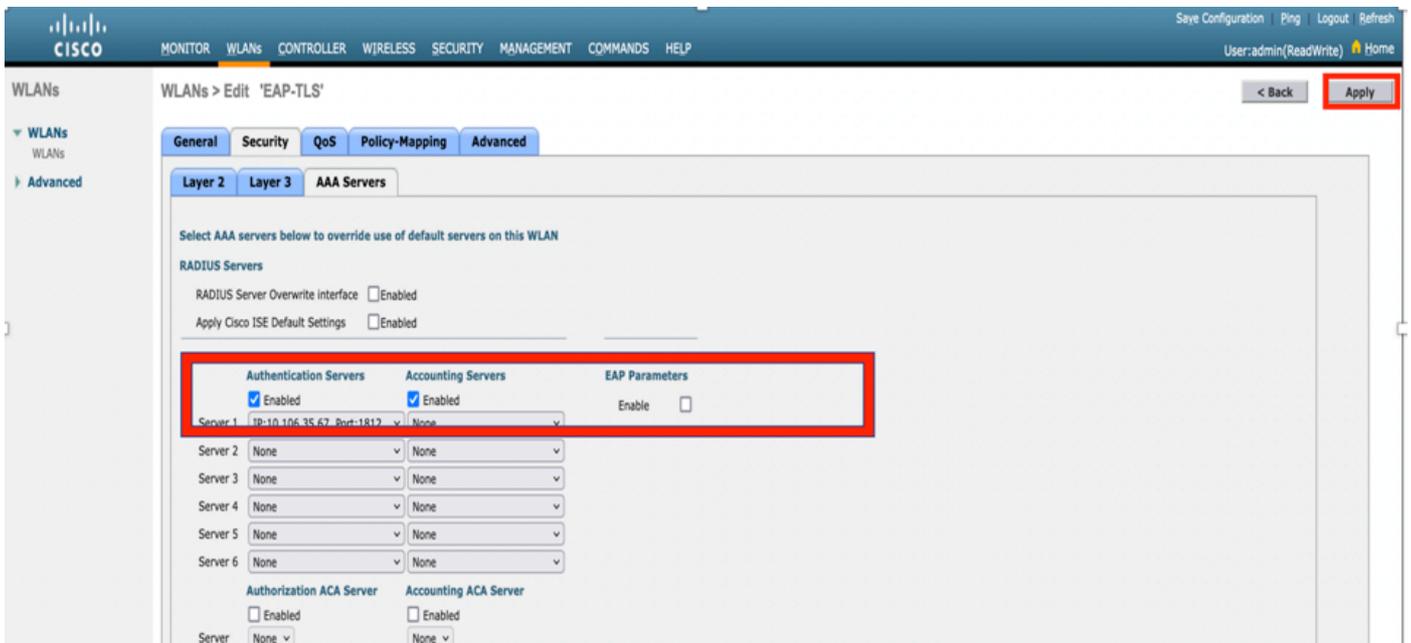
Schritt 5: Benennen Sie das neue WLAN **EAP-TLS**. Klicken Sie auf **Apply**, um fortzufahren, wie im Bild dargestellt.



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 zu **Richtlinie > Richtlinienelemente > Ergebnisse > Authentifizierung > Zugelassene Protokolle**, und klicken Sie auf **Hinzufügen**, wie im Bild dargestellt.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit Add Duplicate Delete

<input type="checkbox"/>	Service Name	Description
<input type="checkbox"/>	Default Network Access	Default Allowed Protocol Service

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.

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service 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 List > New Network Device

Network Devices

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings [?](#)

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.

Identity Services Engine Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Network Access Users

Latest Manual Network Scan Results

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
--------	------	-------------	------------	-----------	---------------	----------------------	-------

Show

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name

Status Enabled

Email

Passwords

Password Type:

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

User Information

First Name

Last Name

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

User Groups

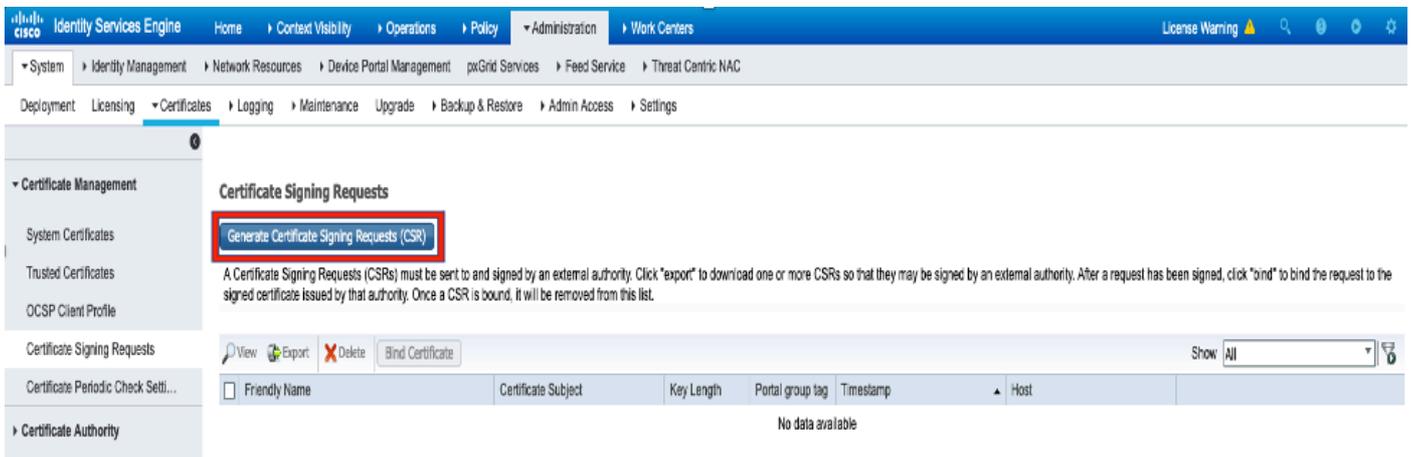
Select an item

Zertifikat auf ISE vertrauen

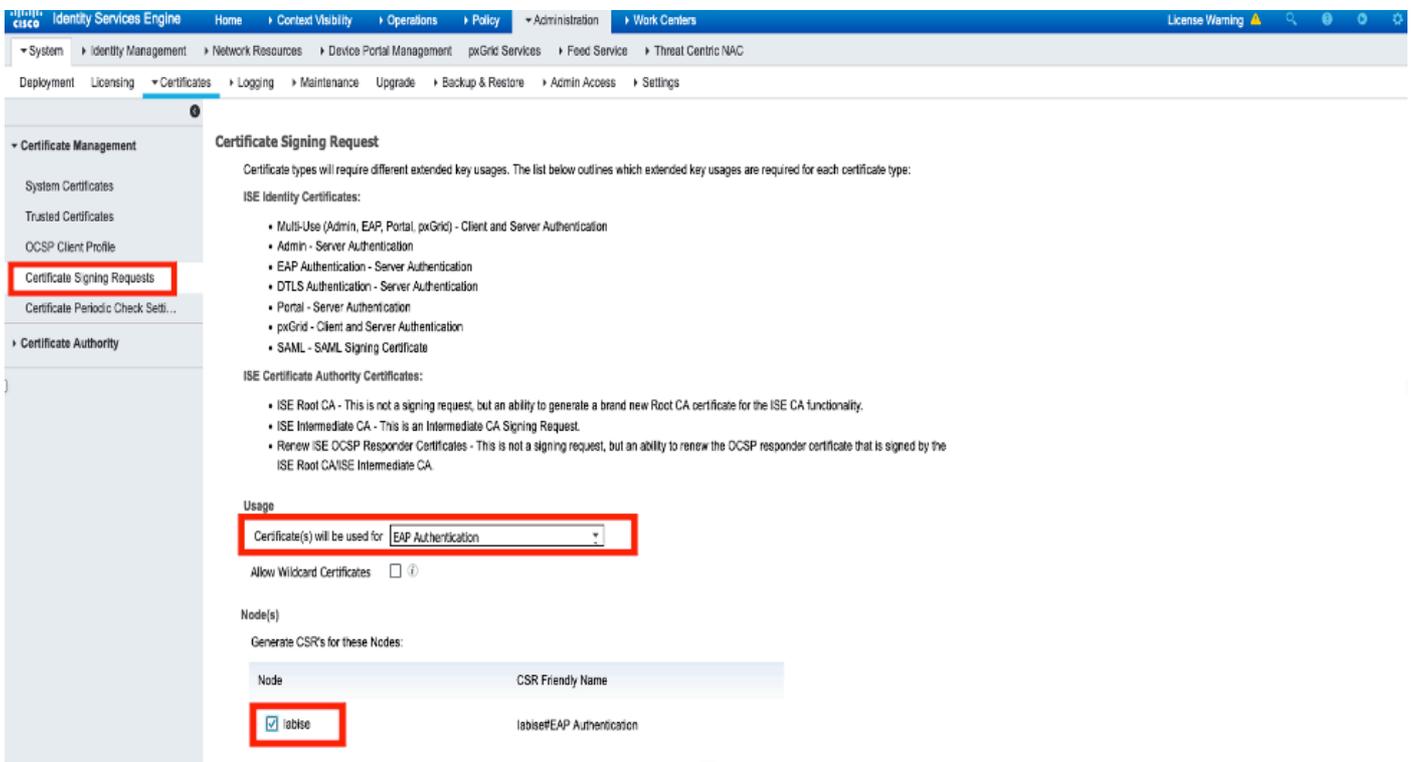
Schritt 1: Navigieren Sie zu **Administration > System > Certificates > Certificate Management > Trusted Certificates**.

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.

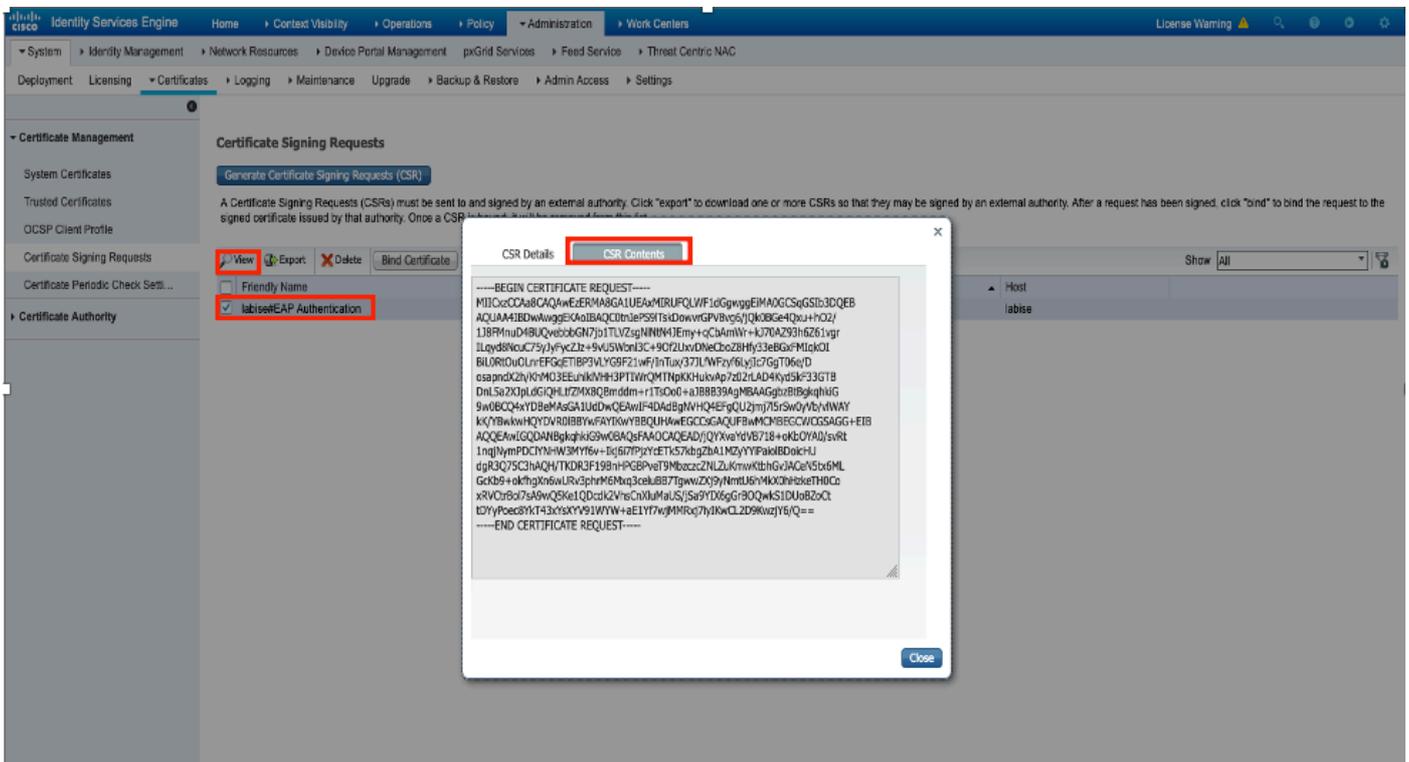
Schritt 2: Navigieren Sie zu **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR)**, wie im Bild dargestellt.



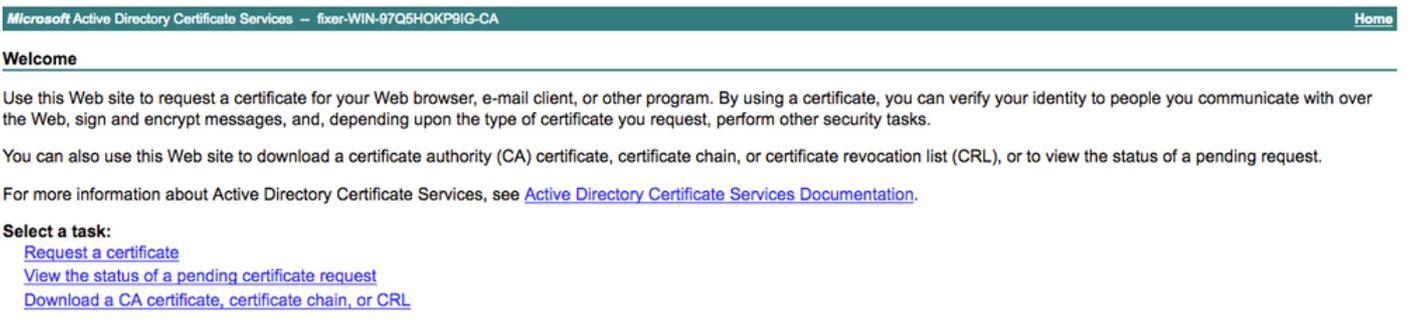
Schritt 3: Um die CSR-Anfrage zu erstellen, navigieren Sie zu **Usage (Verwendung)** und wählen Sie aus den **Zertifikaten**, die für die Dropdown-Optionen verwendet werden, **EAP Authentication (EAP-Authentifizierung)** aus, wie im Bild dargestellt.



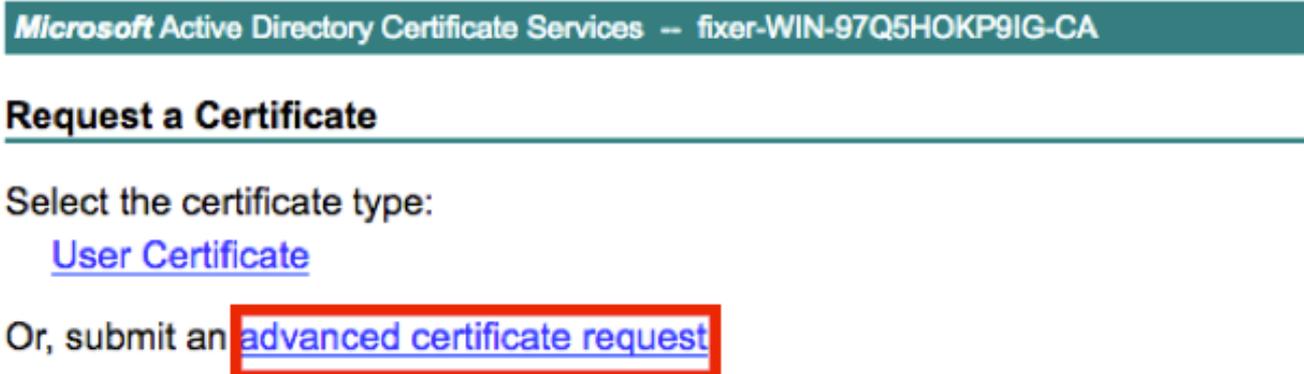
Schritt 4: Die von der ISE generierte CSR-Anfrage kann angezeigt werden. Klicken Sie auf **Ansicht**, wie im Bild dargestellt.



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 **Zertifikatsvorlage**: Wählen Sie **Web Server** aus, und klicken Sie auf **Submit (Senden)**, wie im Bild dargestellt.

Import a new Certificate into the Certificate Store

* Certificate File No file chosen

Friendly Name

Trusted For:

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

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.

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 checked="" type="checkbox"/> ise#EAP Authentication	CN=ise.c.com	2048	Mon, 9 Jul 2018	ise	Created by Paint X

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**.

Bind CA Signed Certificate

* Certificate File No file chosen

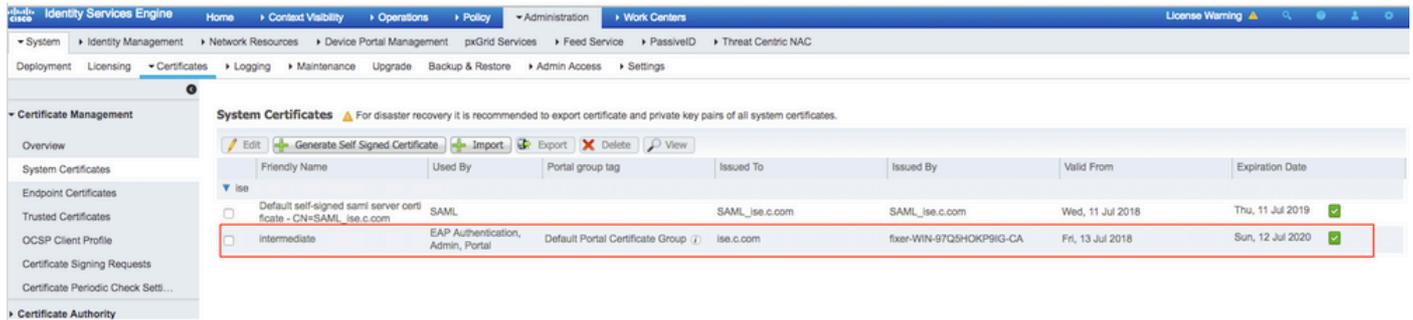
Friendly Name

Validate Certificate Extensions

Usage

EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

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.

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/3qJJeeM1ZqxnL7BVIspJry  
aF4l2aLpmDFp1PfVZ3VaP6Oa/mej3IXh0RFxBUII  
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxF1j3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

Attributes:

Submit >

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**.

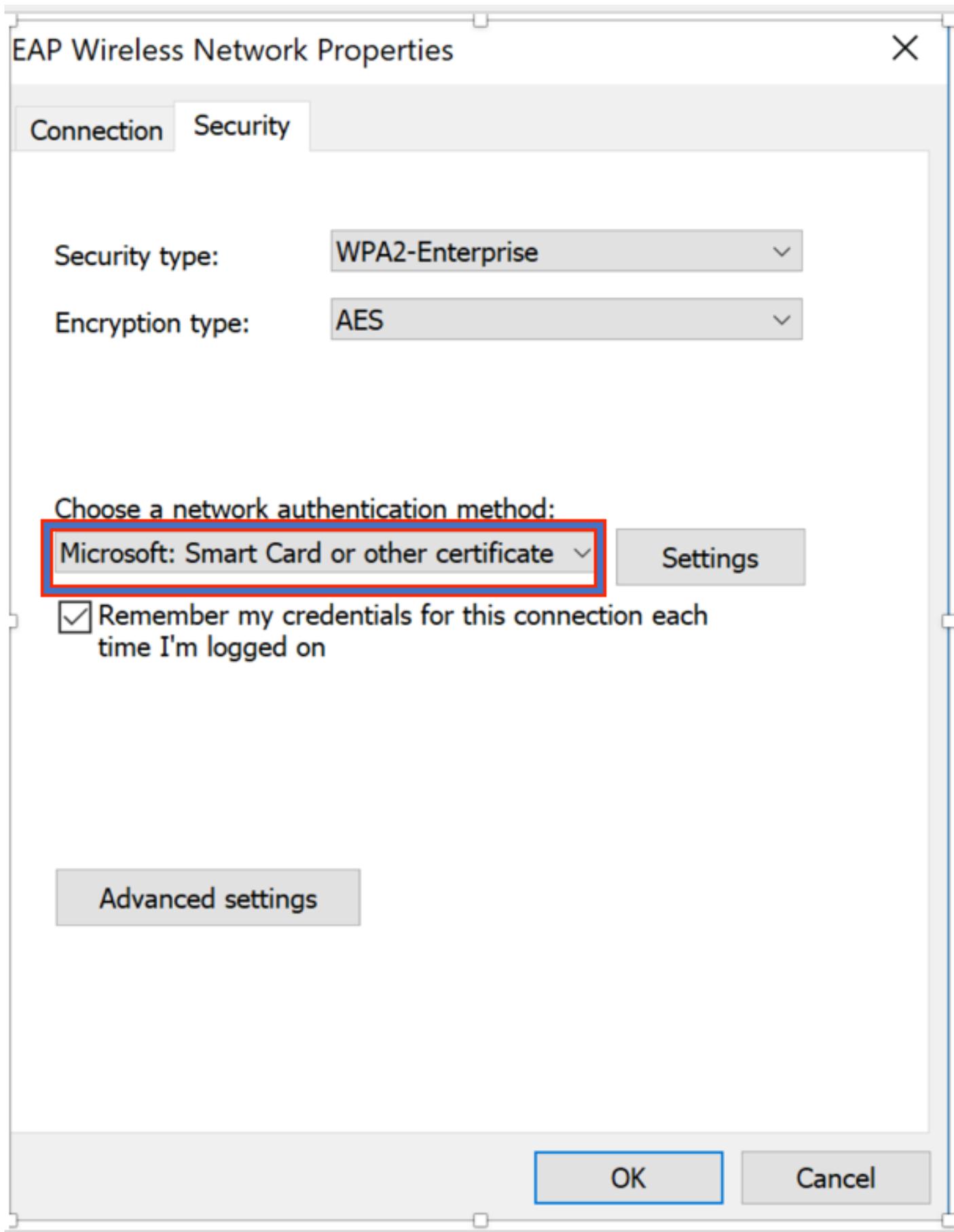
11. Wählen Sie die **.cer, .crt oder .pfx aus**, die Sie importieren möchten.
12. Klicken Sie auf **Öffnen**.
13. Klicken Sie auf **Next** (Weiter).
14. Wählen Sie **den Zertifikatspeicher basierend auf dem Zertifikatstyp automatisch aus**.
15. Klicken Sie auf **Fertig stellen und OK**.

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.

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 mit den 802.1x-Einstellungen aus, wie im Bild dargestellt.

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

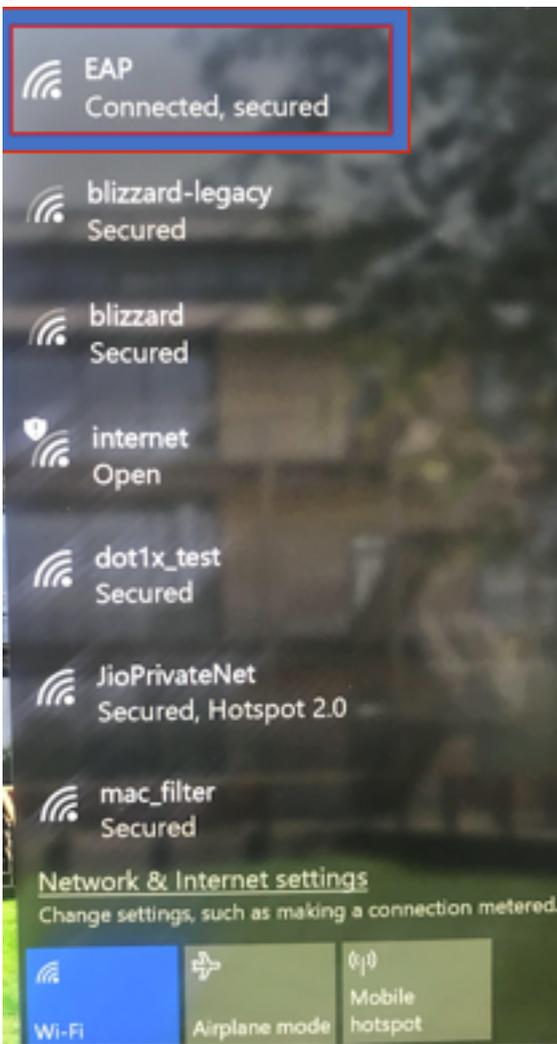
Maximum delay (seconds):

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 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.

Monitor

Clients > Detail

Max Number of Records Clear AVC Stats

General **AVC Statistics**

Client Properties		AP Properties	
MAC Address	34:02:86:96:2f:b7	AP Address	00:d7:8f:52:db:a0
IPv4 Address	10.106.32.239	AP Name	Alpha2802_3rdfloor
IPv6 Address	fe80::2818:15a4:65f9:842,	AP Type	802.11bn
		AP radio slot Id	0
		WLAN Profile	EAP
		WLAN SSID	EAP
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
Client Type	Simple IP	802.11 Authentication	Open System
User Name	Administrator	Reason Code	1
Port Number	1	Status Code	0
Interface	management	CF Pollable	Not Implemented
VLAN ID	32	CF Poll Request	Not Implemented
Quarantine VLAN ID	0	Short Preamble	Not Implemented
CCX Version	CCXv1	PBCC	Not Implemented
E2E Version	Not Supported	Channel Agility	Not Implemented
Mobility Role	Local	Re-authentication timeout	1682
Mobility Peer IP Address	N/A	Remaining Re-authentication timeout	0
Mobility Move Count	0	WEP State	WEP Enable
Policy Manager State	RUN	Lync Properties	
Management Frame Protection	No	Lync State	Disabled
UpTime (Sec)	146	Audio Qos Policy	Silver

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

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Auth Key Mgmt	802.1x
Encryption Cipher	CCMP (AES)
EAP Type	EAP-TLS
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	none
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied	Unavailable

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below this, there are tabs for 'Endpoints' and 'Network Devices'. The breadcrumb path is 'Endpoints > 34:02:86:96:2F:B7'. The main content area displays the MAC address '34:02:86:96:2F:B7' and a list of details: 'MAC Address: 34:02:86:96:2F:B7', 'Username: Administrator@flxer.com', 'Endpoint Profile: Intel-Device', 'Current IP Address:', and 'Location:'. Below these details are tabs for 'Attributes', 'Authentication', 'Threats', and 'Vulnerabilities'. The 'Attributes' tab is active, showing 'General Attributes' and 'Custom Attributes'. The 'General Attributes' section includes a 'Description' and a table with the following data:

Static Assignment	false
Endpoint Policy	Intel-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

The 'Custom Attributes' section is currently empty, with a message: 'No data found. Add custom attributes here.' Below this is a table for 'Other Attributes' with the following data:

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	5
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509_PKI

The 'AllowedProtocolMatchedRule' attribute is highlighted with a red box in the original image.

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 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.