

EAP-TLS begrijpen en configureren met Mobility Express en ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[EAP-TLS-stroom](#)

[Stappen in EAP-TLS-stroom](#)

[Configureren](#)

[Cisco Mobility Express](#)

[ISE met Cisco Mobility Express](#)

[EAP-TLS-instellingen](#)

[Mobility Express-instellingen voor ISE](#)

[Trustcertificaat op ISE](#)

[Cliënt voor EAP-TLS](#)

[Gebruikershandleiding downloaden op clientmachine \(Windows bureaublad\)](#)

[Draadloos profiel voor EAP-TLS](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Deze documenten beschrijft hoe u een Wireless Local Area Network (WLAN) kunt instellen met 802.1x-beveiliging in een Mobility Express controller. In dit document wordt ook het gebruik van Extensible Authentication Protocol (EAP) - Transport Layer Security (TLS) specifiek uitgelegd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Eerste instelling voor Mobility Express
- 802.1x-authenticatieproces
- Certificaten

Gebruikte componenten

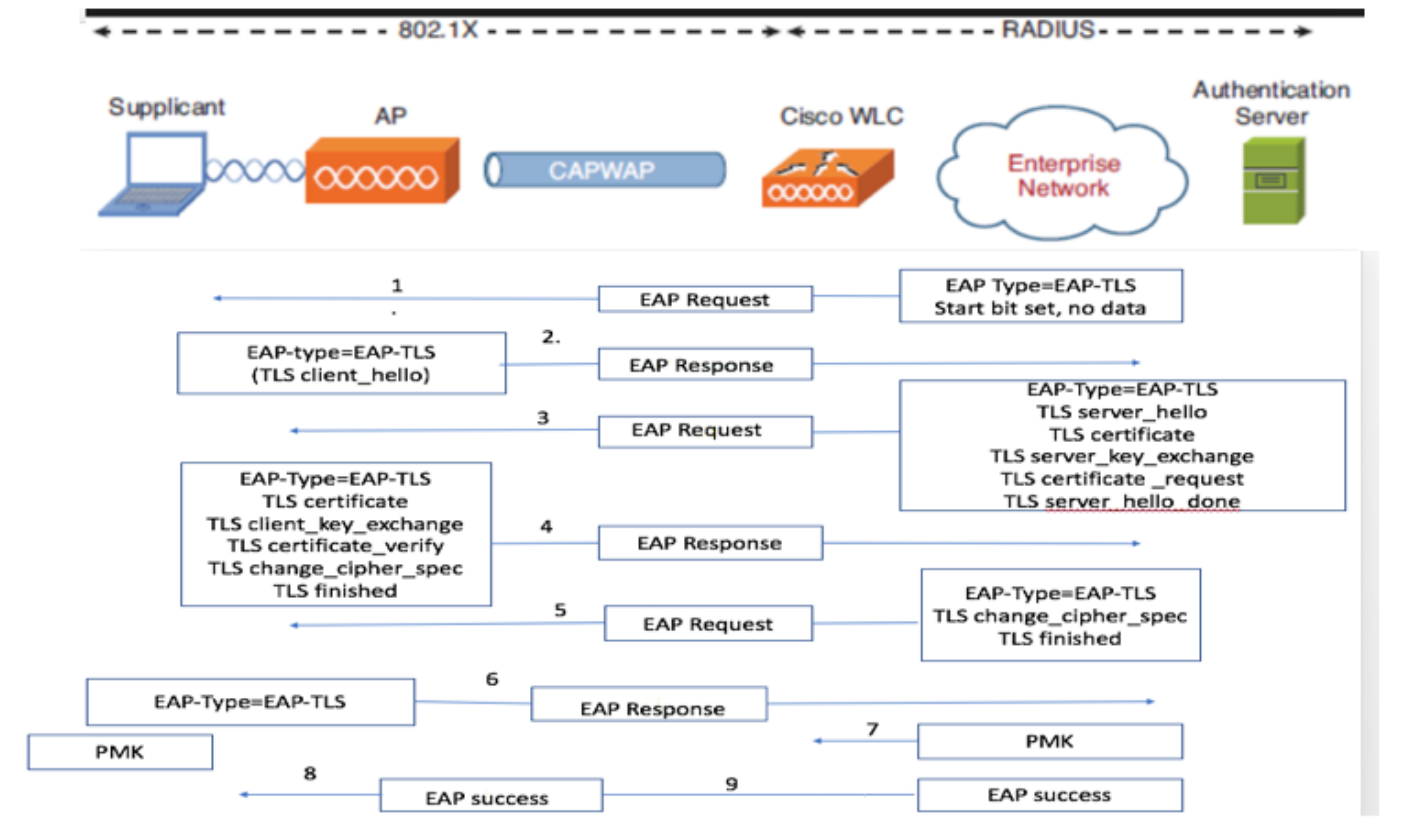
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

EAP-TLS-stroom



Stappen in EAP-TLS-stroom

1. Draadloze client wordt gekoppeld aan het access point (AP).
2. AP staat de cliënt niet toe om op dit punt gegevens te verzenden en een authenticatieverzoek te versturen.
3. De aanvrager reageert daarop met een MAP-antwoordidentiteit. De WLC geeft vervolgens de gebruiker-id informatie door aan de verificatieserver.
4. RADIUS-server reageert weer op de client met een EAP-TLS Start-pakket. De EAP-TLS-discussie begint nu.
5. De peer stuurt een EAP-Response terug naar de authenticatieserver die een "client_hallo" handdruk bericht bevat, een algoritme dat voor NULL is ingesteld.
6. De authenticatieserver reageert met een Access-challenge pakket dat bestaat uit:

TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.

7. De client reageert met een MAP-antwoordbericht dat bevat:

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

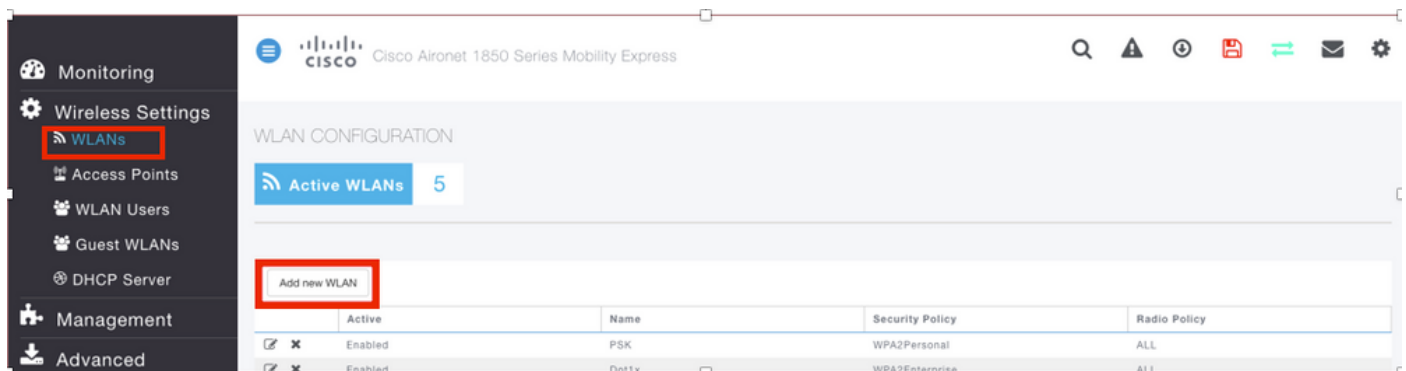
8. Nadat de client is geauthentiseerd, reageert de RADIUS-server met een Access-challenge, die het afgewerkte bericht "change_algoritme_spec" en de handdruk bevat. Na ontvangst verifieert de client de hash om de RADIUS-server voor echt te maken. Een nieuwe encryptiesleutel wordt dynamisch afgeleid van het geheim tijdens de TLS-handdruk.

9. Op dit punt kan de EAP-TLS-enabled draadloze client toegang krijgen tot het draadloze netwerk.

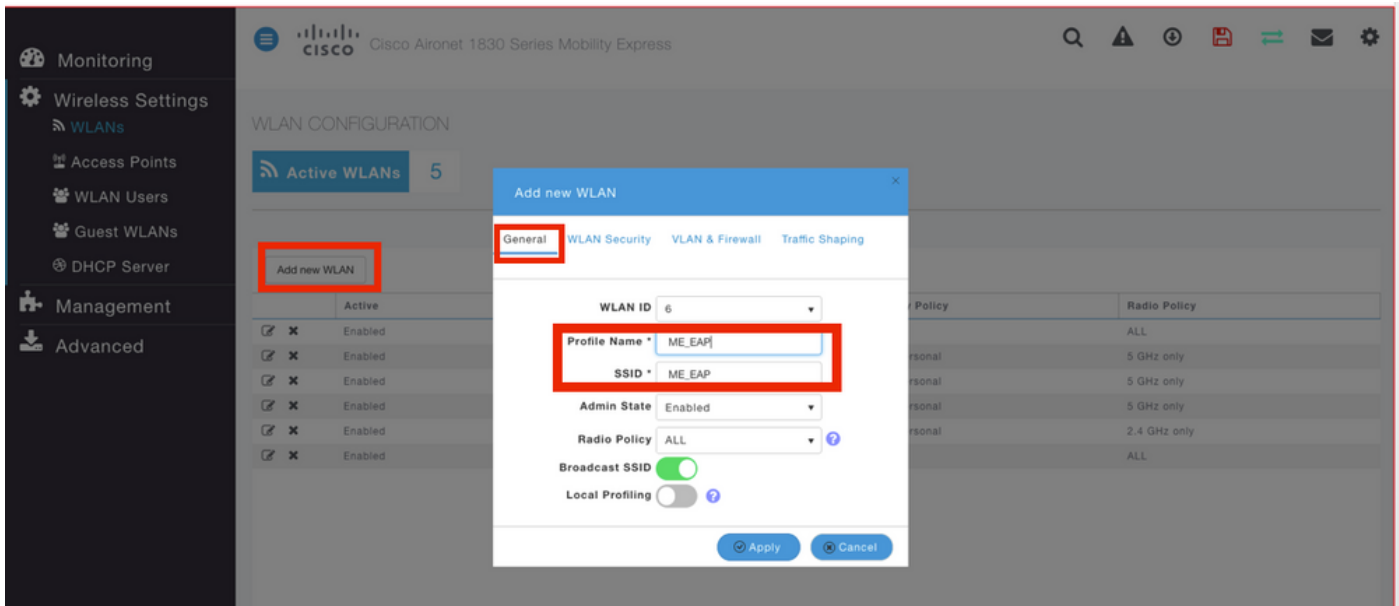
Configureren

Cisco Mobility Express

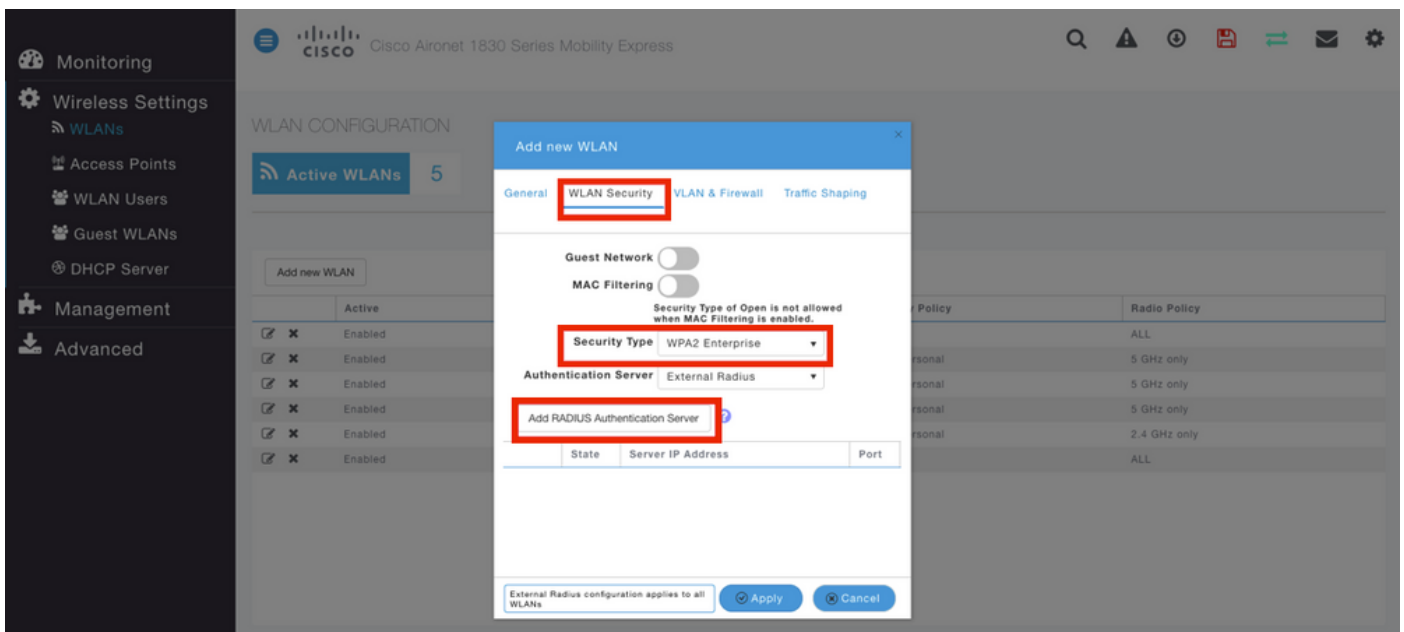
Stap 1. De eerste stap is het maken van een WLAN-functie bij Mobility Express. Om een WLAN te maken, navigeer dan naar **WLAN > Voeg nieuwe WLAN toe** zoals in de afbeelding.



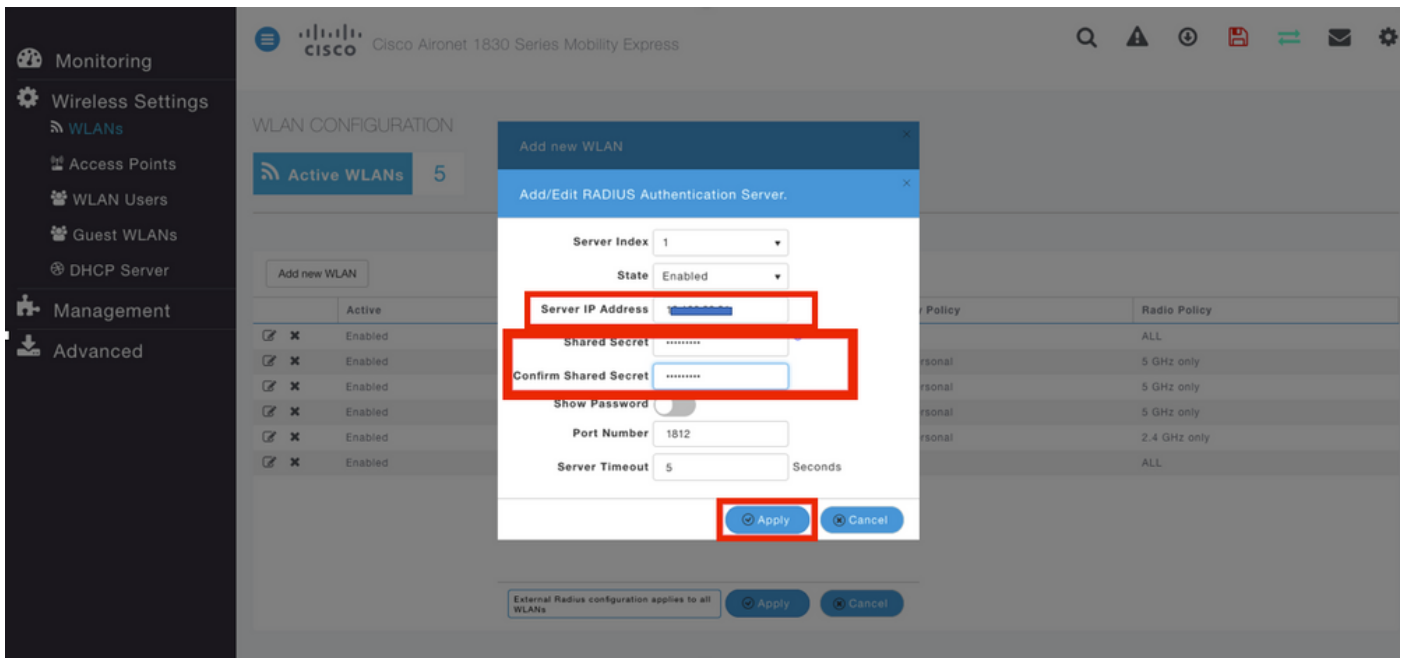
Stap 2. Er verschijnt een nieuw pop-upvenster nadat u op **Add new WLAN** klikt. Als u een Profile name wilt maken, navigeer u om **nieuwe WLAN > General** toe te voegen zoals in de afbeelding.



Stap 3. Configureer het verificatietype als WAP Enterprise voor 802.1x en stel RADIUS-server in onder **Add new WLAN > WLAN-beveiliging** zoals in de afbeelding.



Stap 4. Klik op **RADIUS-verificatieserver toevoegen** en geef het IP-adres op van de RADIUS-server en het gedeelde geheim dat precies overeenkomt met wat op ISE is ingesteld en klik vervolgens op **Toepassen** zoals in de afbeelding.



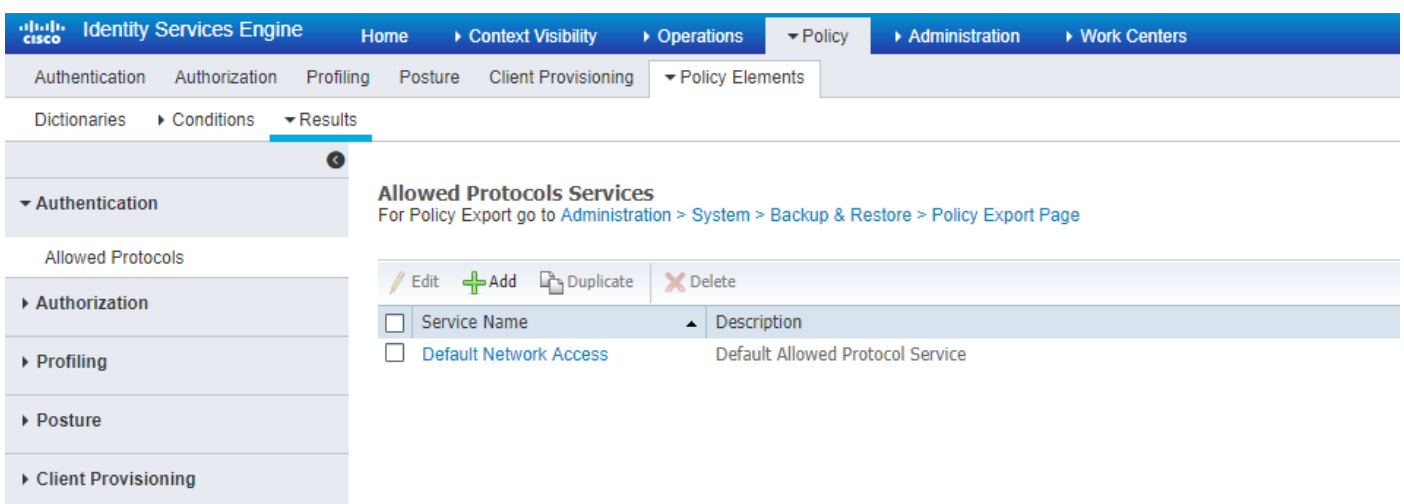
ISE met Cisco Mobility Express

EAP-TLS-instellingen

Om het beleid te kunnen bouwen, moet u de toegestane protocollijst maken die in uw beleid moet worden gebruikt. Aangezien er een dot1x-beleid is geschreven, moet u het toegestane MAP-type specificeren op basis van de manier waarop het beleid wordt ingesteld.

Als u de standaardinstelling gebruikt, staat u de meeste MAP-typen toe voor authenticatie die wellicht niet de voorkeur genieten als u de toegang tot een specifiek MAP-type moet afsluiten.

Stap 1. Navigeer in op **Policy > Policy Elementen > Resultaten > Verificatie > Toegestane protocollen** en klik op **Add** zoals in de afbeelding.



Stap 2. Op deze toegestane protocollijst kunt u de naam voor de lijst invoeren. In dit geval is het vakje **EAP-TLS toestaan** ingeschakeld en zijn andere vakjes niet ingeschakeld zoals in de afbeelding wordt weergegeven.

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 List > New Allowed Protocols Service

Allowed Protocols

Name

Description

Allowed Protocols

Authentication Bypass

Process Host Lookup (i)

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 (i)

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 (i)

Require cryptobinding TLV (i)

Mobility Express-instellingen voor ISE

Stap 1. Open ISE-console en navigeer naar **Beheer > Netwerkbronnen > Netwerkkapparaten > Toevoegen** zoals in de afbeelding.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

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

Network Devices

Selected 0 | Total 1

Name	IP/Mask	Profile Name	Location	Type	Description

Stap 2. Voer de informatie in zoals in de afbeelding.

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 HEXADECEIMAL

CoA Port

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Trustcertificaat op ISE

Stap 1. Navigeer naar **Administratie > Systeem > Certificaten > certificaatbeheer > Vertrouwde certificaten**.

Klik op **Importeren** om een certificaat te importeren naar ISE. Zodra u een WLC hebt toegevoegd en een gebruiker op ISE hebt gemaakt, moet u het belangrijkste onderdeel van EAP-TLS doen dat is om het certificaat op ISE te vertrouwen. Daarvoor moet je CSR genereren.

Stap 2. Navigeer naar **Advisering > Certificaten > Verzoeken voor certificatie > Generate certificaatsignalering (CSR)** zoals in de afbeelding getoond.

Certificate Management

Overview

System Certificates

Endpoint Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Sett...

Certificate Authority

Certificate Signing Requests

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.

Show

<input type="checkbox"/>	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

Stap 3. Om CSR te genereren, navigeer dan naar **Gebruik en van het(de) Certificaat(en) wordt (worden) gebruikt voor uitroopties**, selecteer **EAP-verificatie** zoals in de afbeelding.

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](#)

Stap 6. Nadat u een certificaat hebt aangevraagd, krijgt u opties voor **Gebruikerscertificaat en geavanceerde certificaataanvraag**, klikt u op **geavanceerde certificaataanvraag** zoals in de afbeelding.

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

Request a Certificate

Select the certificate type:

[User Certificate](#)

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

Stap 7. Plakt de CSR die in **Base-64 gecodeerd certificaatverzoek** is gegenereerd. Selecteer de optie **Webserver** selecteren in de vervolgkeuzelijst: klik op **Webserver** en klik op **Inzenden** zoals in de afbeelding.

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:

v

Additional Attributes:

Attributes:

Stap 8. Zodra u op **Inzenden** klikt, krijgt u de optie om het type certificaat te selecteren, selecteert u **Base-64 gecodeerd** en klikt u op **Download certificaat** zoals in de afbeelding.

Certificate Issued

The certificate you requested was issued to you.

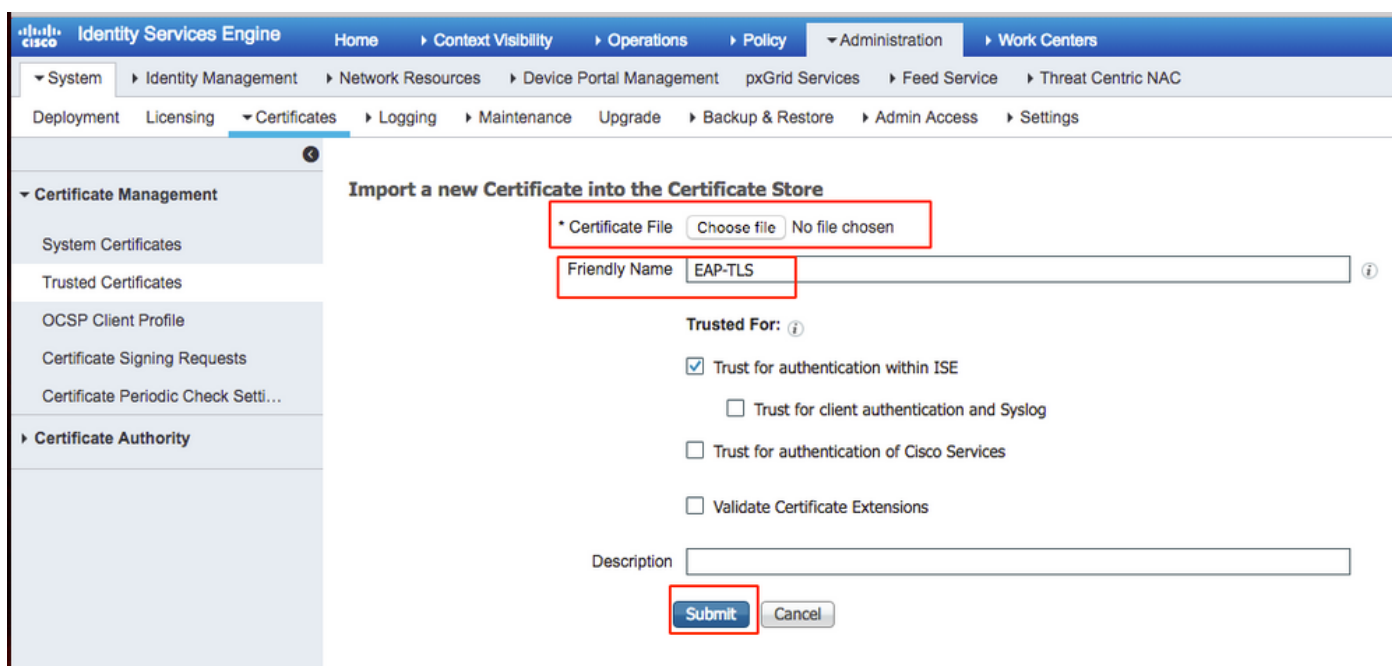
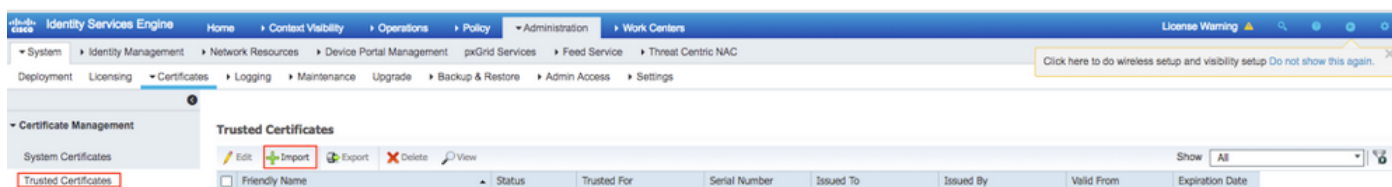
DER encoded or Base 64 encoded



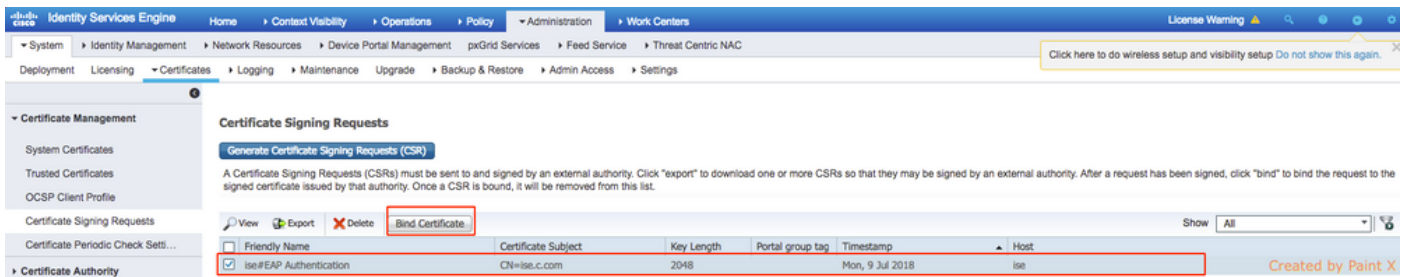
[Download certificate](#)

[Download certificate chain](#)

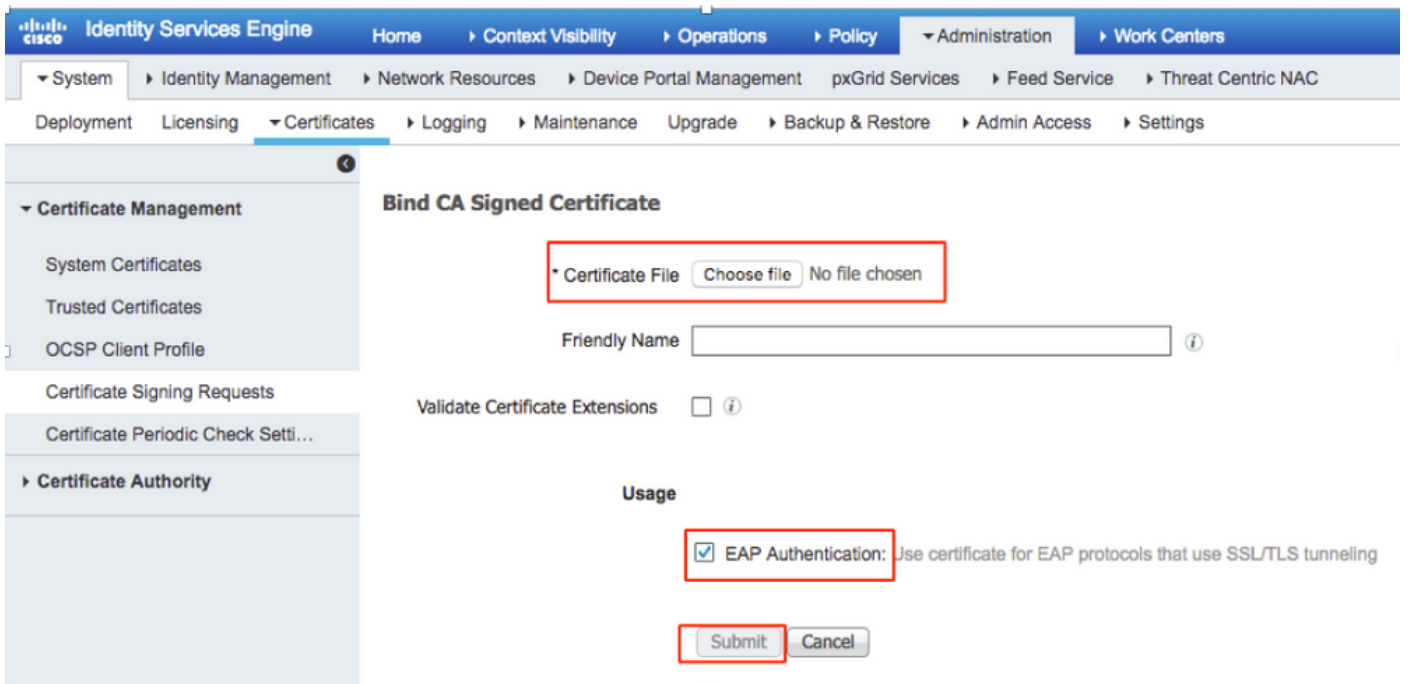
Stap 9. Het certificaat is gedownload voor de ISE-server. U kunt het certificaat opvragen, het certificaat bevat twee certificaten, één wortelcertificaat en een ander tussenproduct. Het basiscertificaat kan worden geïmporteerd onder **Beheer > Certificaten > Vertrouwde certificaten > Importeren** zoals in de afbeeldingen.



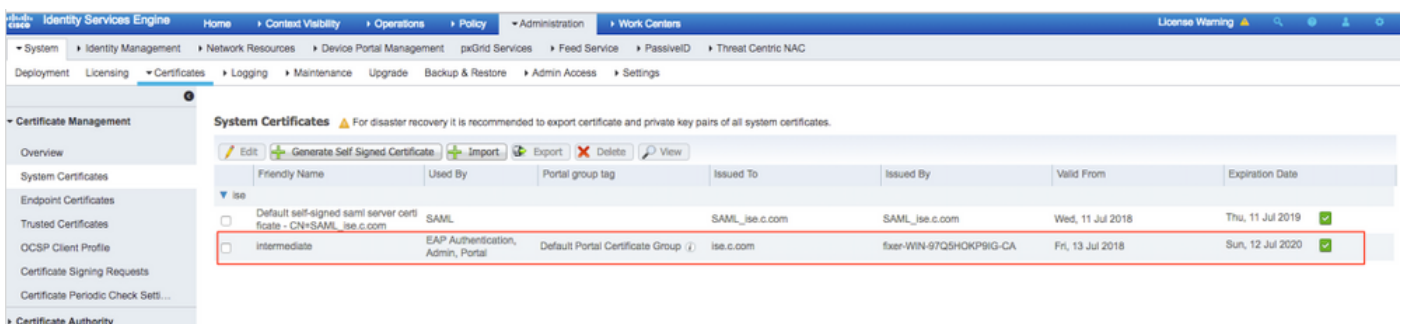
Stap 10. Zodra u op **Inzenden** klikt, wordt het certificaat toegevoegd aan de lijst met vertrouwde certificaten. Bovendien is het intermediaire certificaat nodig om aan CSR te binden zoals in de afbeelding.



Stap 1. Zodra u op **Bind certificaat** klikt, kunt u het certificaatbestand kiezen dat in uw bureaublad is opgeslagen. Bladeren naar het intermediaire certificaat en klik op **Inzenden** zoals in de afbeelding.



Stap 12. Om het certificaat te kunnen weergeven, navigeer dan naar **Administratie > Certificaten > Systemcertificaten** zoals in de afbeelding.



Client voor EAP-TLS

Gebruikershandleiding downloaden op clientmachine (Windows bureaublad)

Stap 1. Om een draadloze gebruiker via EAP-TLS te authenticeren, moet u een client certificaat genereren. Sluit uw Windows-computer aan op het netwerk zodat u toegang hebt tot de server. Open een webbrowser en voer dit adres in: <https://sever.ip.adr.certsrv>

Stap 2. Merk op dat de CA hetzelfde moet zijn als waarmee het certificaat voor ISE is

gedownload.

Hiervoor moet u voor dezelfde CA-server bladeren die u het certificaat voor server hebt gedownload. Klik op **Aanvragen van een certificaat** zoals eerder gedaan. U moet echter deze keer **Gebruiker** selecteren als de certificaatsjabloon zoals in de afbeelding weergegeven.

The screenshot shows the 'Microsoft Active Directory Certificate Services' web page for the CA 'fixer-WIN-97Q5HOKP9IG-CA'. The main heading is 'Submit a Certificate Request or Renewal Request'. Below this, there is a text instruction: 'To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.' The 'Saved Request:' section contains a text area with a base-64 encoded certificate request. The 'Certificate Template:' section has a dropdown menu currently set to 'User'. The 'Additional Attributes:' section has an empty text area. At the bottom right, there is a 'Submit >' button.

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/3qJJeeM1ZqxnL7BVIspJry  
aF4l2aLpmDFp1PfvZ3VaP6Oa/mej3IXh0RFxBUII  
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

Attributes:

Submit >

Stap 3. Klik vervolgens op de **downloadcertificaatketen** zoals eerder voor de server is gedaan.

Nadat u de certificaten heeft gekregen, volgt u deze stappen om het certificaat op Windows-laptop te importeren.

Stap 4. Om het certificaat te kunnen importeren, moet u het vanaf de Microsoft Management Console (MMC) benaderen.

1. Om de MMC te openen navigeer naar **Start > Run > MMC**.
2. Navigeren in op **bestand > Magnetisch toevoegen / verwijderen**
3. Dubbelklik op **certificaten**.
4. Selecteer **Computer-account**.
5. Selecteer **Local Computer > Finish**
6. Klik op **OK** om het Magnetisch-In venster te verlaten.

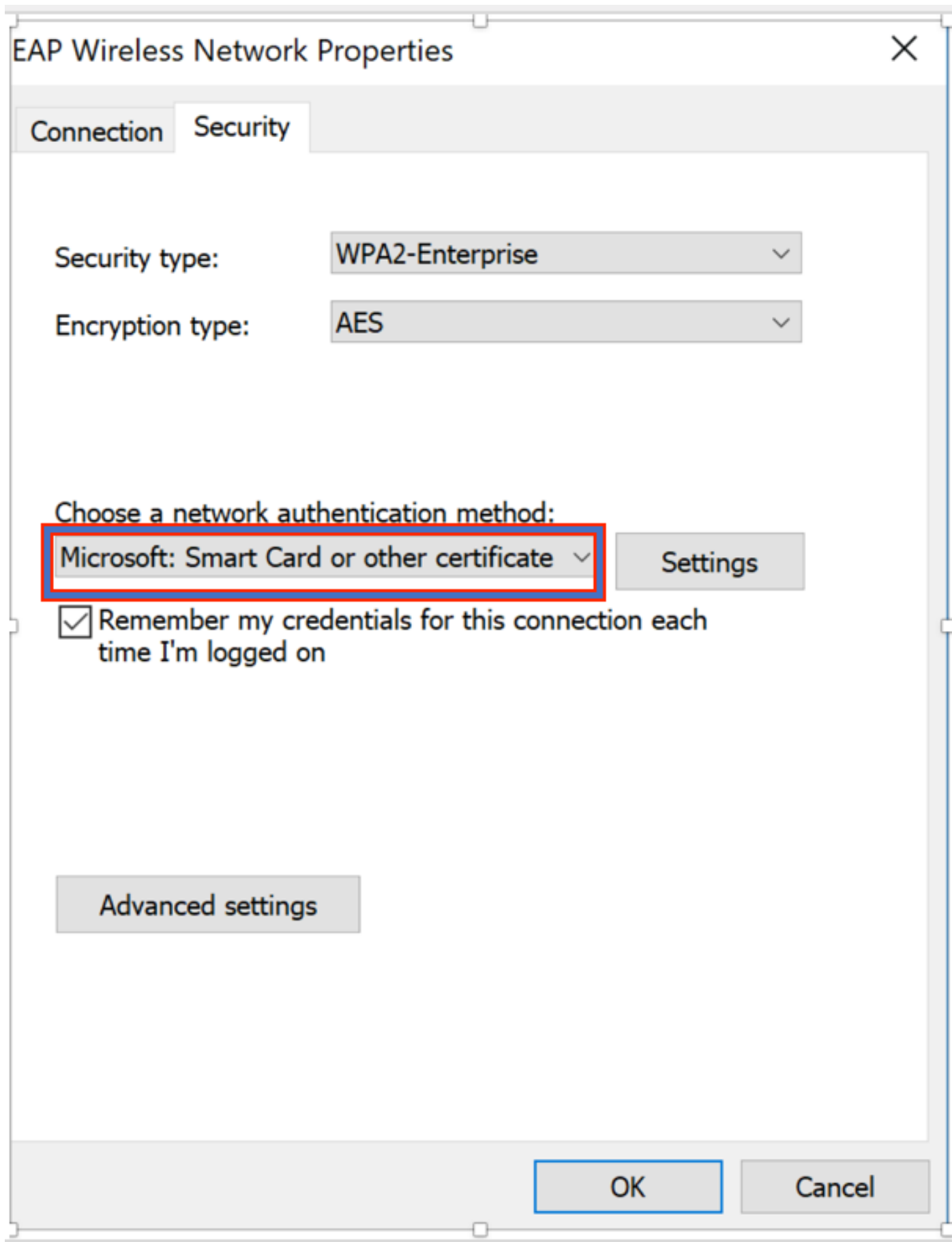
7. Klik op **[+]** naast **certificaten > Persoonlijk > Certificaten**.
8. Klik met de rechtermuisknop op **Certificaten** en selecteer **Alle taken > Importeren**.
9. Klik op **Volgende**.
10. Klik op **Bladeren**.
11. Selecteer de optie **.cer, .crt of .pfx** die u wilt importeren.
12. Klik op **Openen**.
13. Klik op **Volgende**.
14. Selecteer **Automatisch de certificaatwinkel selecteren op basis van het type certificaat**.
15. Klik op **Voltooien & OK**

Nadat het certificaat is ingevoerd, moet u uw draadloze client (Windows bureaublad in dit voorbeeld) voor EAP-TLS configureren.

Draadloos profiel voor EAP-TLS

Stap 1. Verander het draadloze profiel dat eerder was gemaakt voor Protected Extensible Authentication Protocol (PEAP) om in plaats daarvan EAP-TLS te gebruiken. Klik op **EAP draadloos profiel**.

Stap 2. Selecteer **Microsoft: Smart Card of ander certificaat** en klik op **OK** zoals in de afbeelding.



Stap 3. Klik op **Instellingen** en selecteer het basiscertificaat dat is verstrekt vanaf een CA-server zoals in de afbeelding.

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

Stap 4. Klik op **Geavanceerde instellingen** en selecteer **Gebruiker of computerverificatie** in het tabblad 802.1x Instellingen zoals in de afbeelding.

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

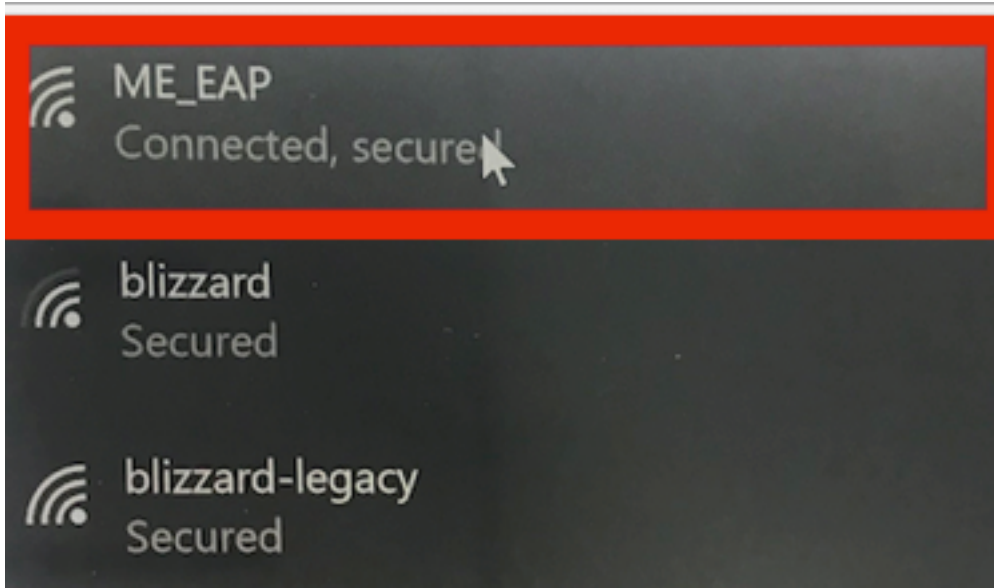
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

Stap 5. Probeer nu opnieuw verbinding te maken met het draadloze netwerk, selecteer het juiste profiel (EAP in dit voorbeeld) en **Connect**. U bent aangesloten op het draadloze netwerk zoals in de afbeelding wordt weergegeven.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Stap 1. Het MAP-type van de cliënt moet een MAP-TLS zijn. Dit betekent dat de cliënt, met behulp van EAP-TLS, een IP-adres heeft verkregen en bereid is het verkeer door te geven zoals in de afbeeldingen wordt getoond.

The screenshot shows a network management interface with a sidebar on the left and a main content area. The sidebar includes sections for Monitoring, Wireless Settings, Management, and Advanced. The main content area is titled 'CLIENT VIEW' and displays details for a client with SSID 'ME_EAP'. The 'GENERAL' section shows the user name 'Administrator', host name 'Unknown', MAC address '34:02:86:96:2f:b7', and uptime 'Associated since 37 Seconds'. The 'CONNECTIVITY' section shows a flowchart with steps: Start, Association, Authentication, DHCP, and Online. The 'TOP APPLICATIONS' section is empty. The 'MOBILITY STATE' section shows a diagram of the network path: WLC (LOCAL) -> Wired (CAP-WAP) -> AP (FlexConnect) -> Wireless (802.11n (5GHz)) -> Client (VLAN1).

Name	Usage	% Usage
No Data Available!		

The screenshot displays a network management dashboard with a sidebar on the left containing navigation options like Monitoring, Network Summary, Applications, Rogues, Interferers, Wireless Dashboard, Best Practices, Wireless Settings, Management, and Advanced. The main content area is divided into three sections:

- MOBILITY STATE:** A diagram showing the connection path from a WLC (LOCAL) through a Wired (CAPWAP) and AP (FlexConnect) to a Wireless (802.11n (5GHz)) and finally to a 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, with 'Key Management' (802.1x) and 'EAP Type' (EAP-TLS) highlighted in red boxes.



At the bottom, there is a 'CLIENT TEST' section with tabs for PING TEST, CONNECTION, EVENT LOG, and PACKET CAPTURE.

Stap 2. Dit is de clientdetails van CLI van de controller (vastgemaakt):

```
(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
```

Stap 3. Op ISE, navigeer naar **ACHTERGROND > Eindpunten > Eigenschappen** zoals in de afbeeldingen.

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
x <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, 1.3.6.1.4.1.311.11
FailureReason	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA,DC=fixer,DC=cc
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"
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 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.