

Comprendre et configurer EAP-TLS avec un WLC et ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Flux EAP-TLS](#)

[Étapes du flux EAP-TLS](#)

[Configuration](#)

[Contrôleur LAN sans fil Cisco](#)

[ISE avec Cisco WLC](#)

[Paramètres EAP-TLS](#)

[Paramètres WLC sur ISE](#)

[Créer un nouvel utilisateur sur ISE](#)

[Certificat de confiance sur ISE](#)

[Client pour EAP-TLS](#)

[Télécharger le certificat utilisateur sur l'ordinateur client \(Bureau Windows\)](#)

[Profil sans fil pour EAP-TLS](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer un réseau local sans fil (WLAN) avec 802.1X et le protocole d'authentification extensible EAP-TLS

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Processus d'authentification 802.1X
- Certificats

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de

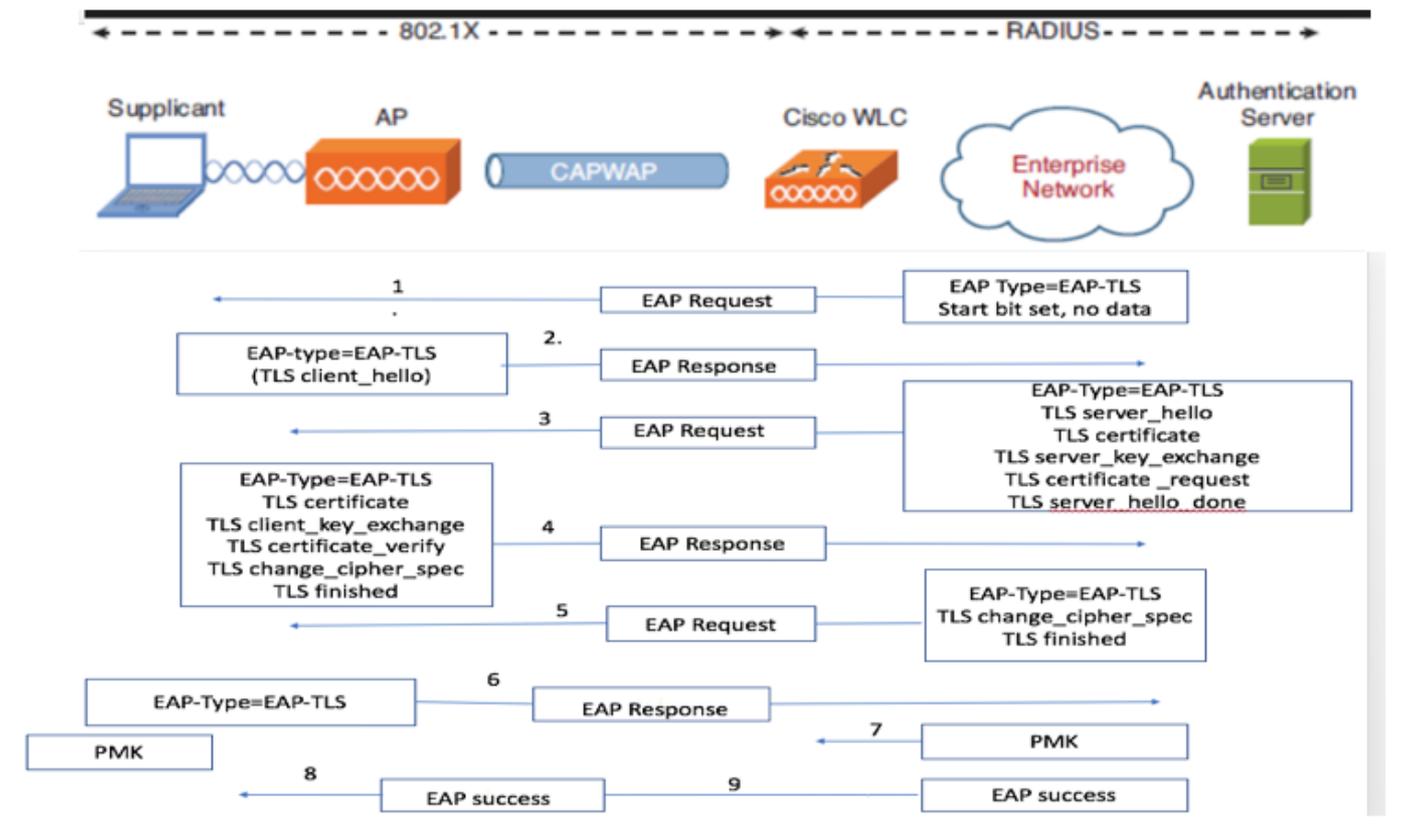
logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Flux EAP-TLS



Étapes du flux EAP-TLS

1. Le client sans fil est associé au point d'accès. Le point d'accès ne permet pas au client d'envoyer des données à ce stade et envoie une demande d'authentification. Le demandeur répond alors avec une identité de réponse EAP. Le WLC communique ensuite les informations d'ID d'utilisateur au serveur d'authentification. Le serveur RADIUS répond au client avec un paquet de démarrage EAP-TLS. La conversation EAP-TLS commence à ce stade.
2. L'homologue renvoie une réponse EAP au serveur d'authentification qui contient un message d'échange « client_hello », un chiffre défini sur NULL
3. Le serveur d'authentification répond par un paquet de demande d'accès contenant :

TLS server_hello
handshake message
certificate

server_key_exchange
certificate request
server_hello_done.

4. Le client répond par un message EAP-Response contenant :

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. Une fois que le client s'est authentifié avec succès, le serveur RADIUS répond par un Access-challenge, qui contient le message « change_cipher_spec » et handshake finished.

6. Quand il reçoit ceci, le client vérifie le hachage afin d'authentifier le serveur radius.

7. Une nouvelle clé de chiffrement est dérivée dynamiquement du secret pendant la connexion TLS

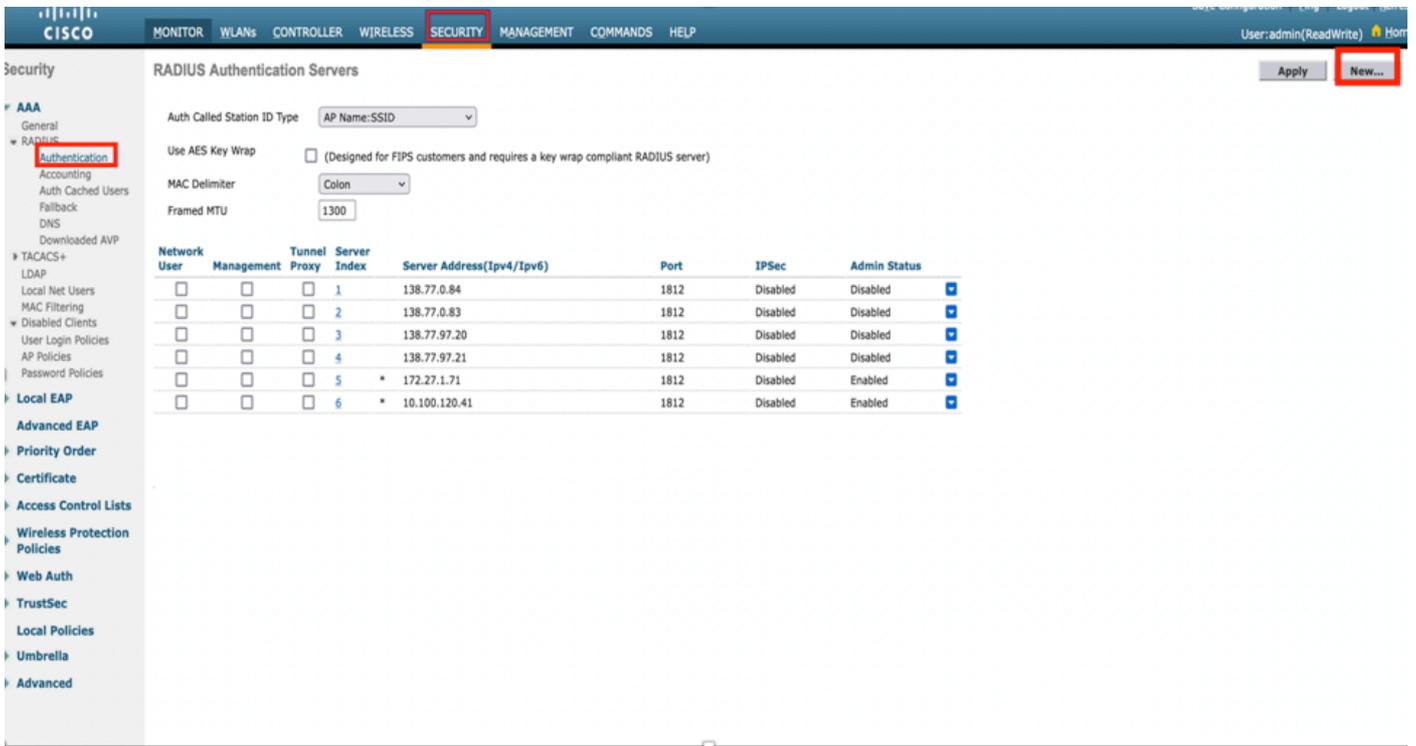
8/9. EAP-Success est finalement envoyé du serveur à l'authentificateur qui est ensuite transmis au demandeur.

À ce stade, le client sans fil compatible EAP-TLS peut accéder au réseau sans fil.

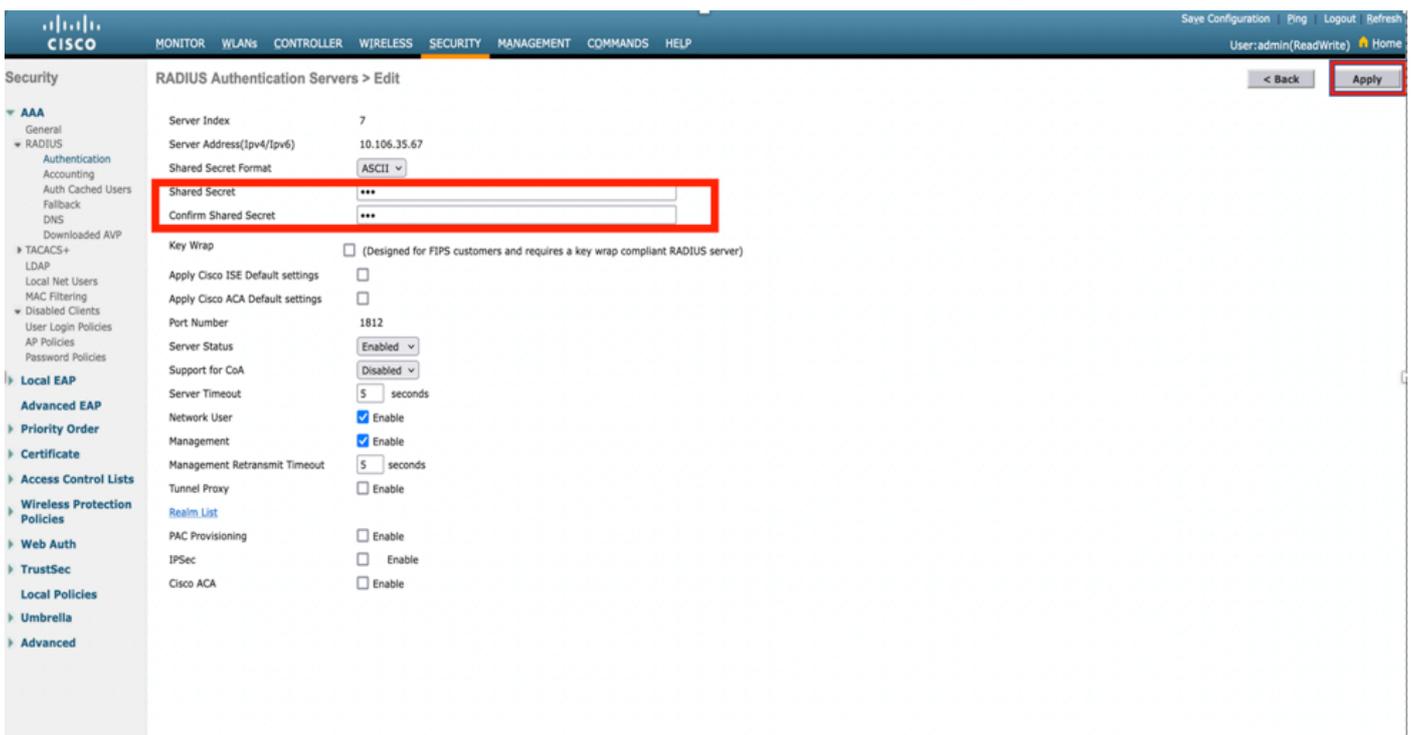
Configuration

Contrôleur LAN sans fil Cisco

Étape 1. La première étape consiste à configurer le serveur RADIUS sur le WLC Cisco. Afin d'ajouter un serveur RADIUS, naviguez vers **Security > RADIUS > Authentication**. Cliquez sur **New** comme indiqué dans l'image.



Étape 2. Ici, vous devez entrer l'adresse IP et le secret partagé <password> qui est utilisé afin de valider le WLC sur l'ISE. Cliquez sur **Apply** afin de continuer comme indiqué dans l'image.



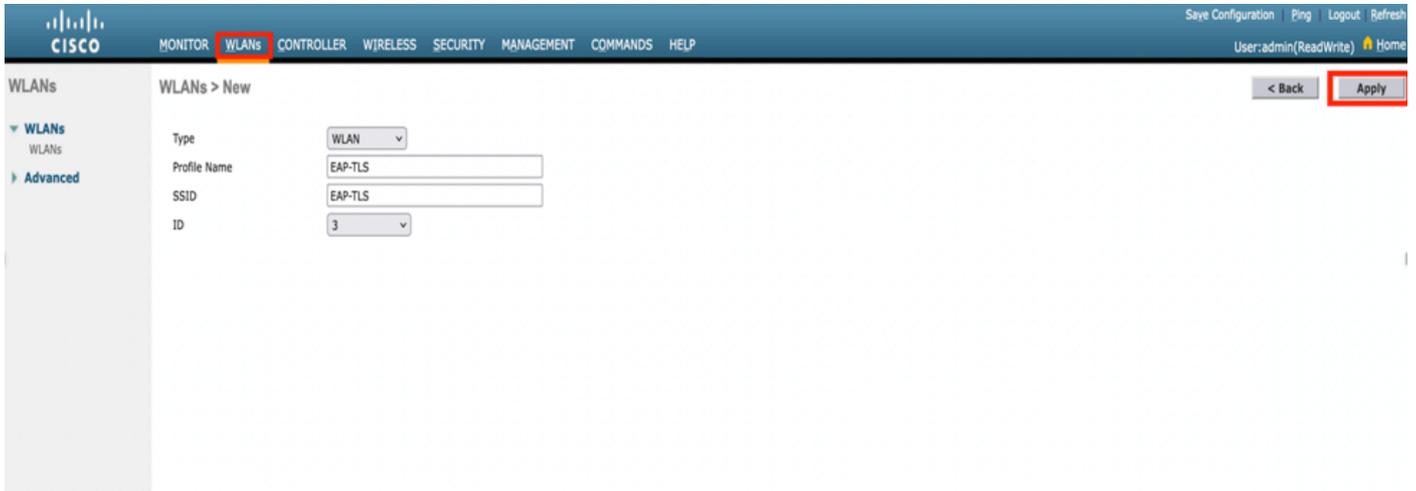
Étape 3 : création d'un WLAN pour l'authentification RADIUS

Vous pouvez maintenant créer un nouveau WLAN et le configurer pour qu'il utilise le mode WPA entreprise, afin qu'il puisse utiliser RADIUS pour l'authentification.

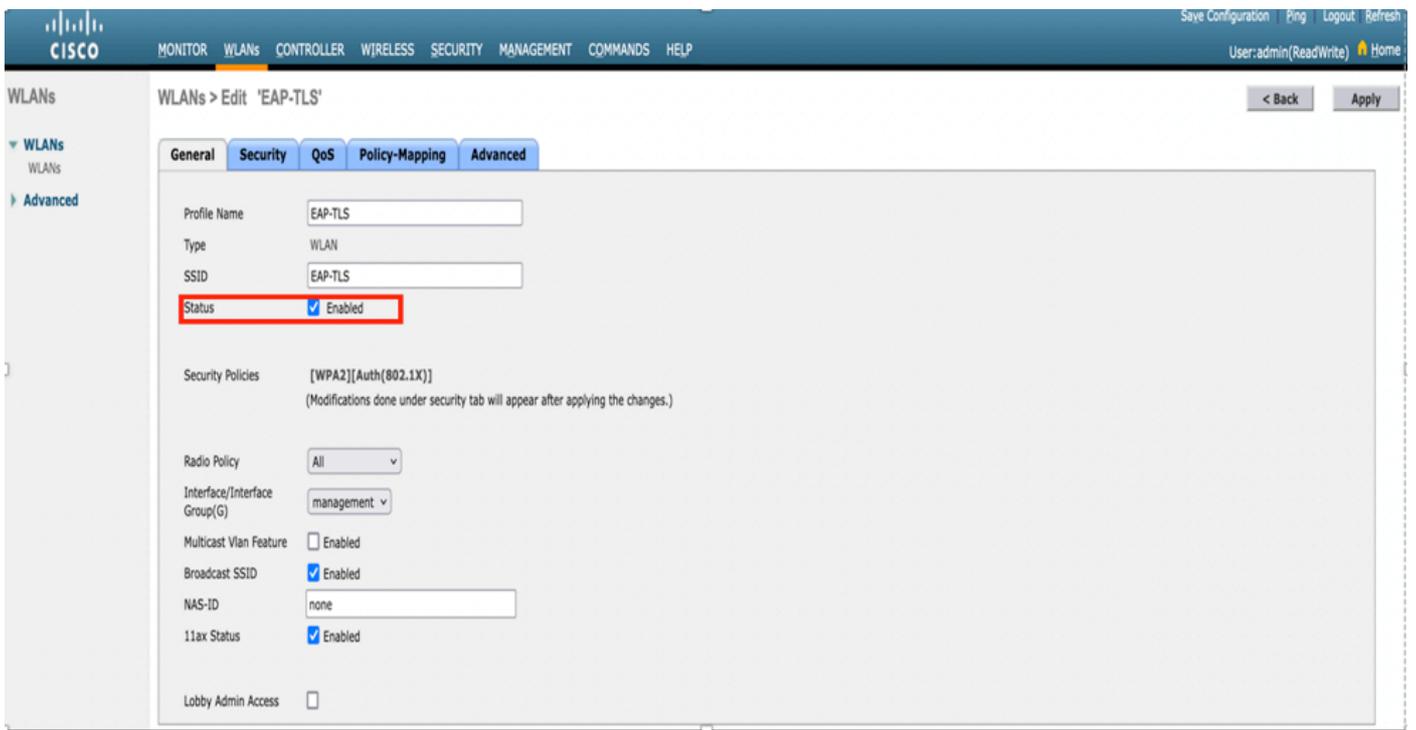
Étape 4. Sélectionnez **WLANs** dans le menu principal, choisissez **Create New** et cliquez sur **Go** comme indiqué dans l'image.



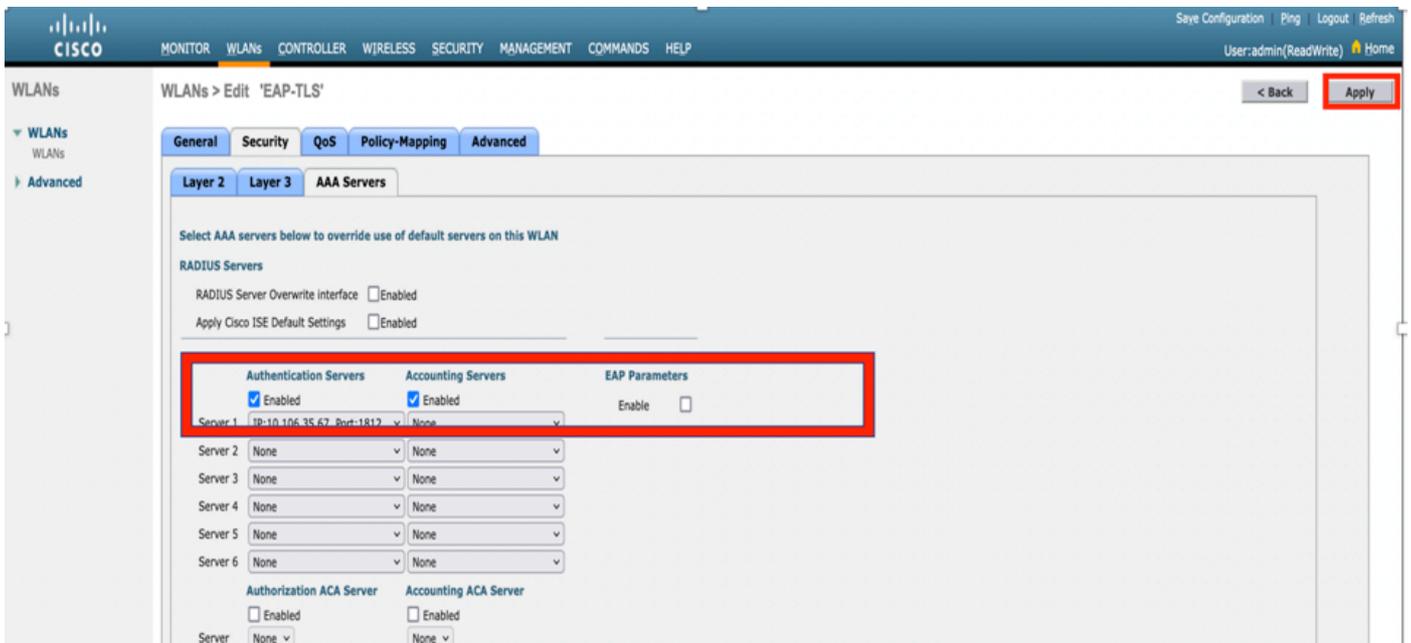
Étape 5. Attribuez un nom au nouveau WLAN EAP-TLS. Cliquez sur **Apply** afin de continuer comme indiqué dans l'image.



Étape 6. Cliquez sur **General** et vérifiez que le statut est **Enabled**. Les stratégies de sécurité par défaut sont l'authentification 802.1X et WPA2, comme illustré dans l'image.



Étape 7. À présent, accédez à **Security > AAA Servers** tab, sélectionnez le serveur RADIUS que vous venez de configurer et comme indiqué dans l'image.



Note: Il est conseillé de vérifier que vous pouvez atteindre le serveur RADIUS à partir du WLC avant de continuer. RADIUS utilise le port UDP 1812 (pour l'authentification). Vous devez donc vous assurer que ce trafic n'est bloqué nulle part sur le réseau.

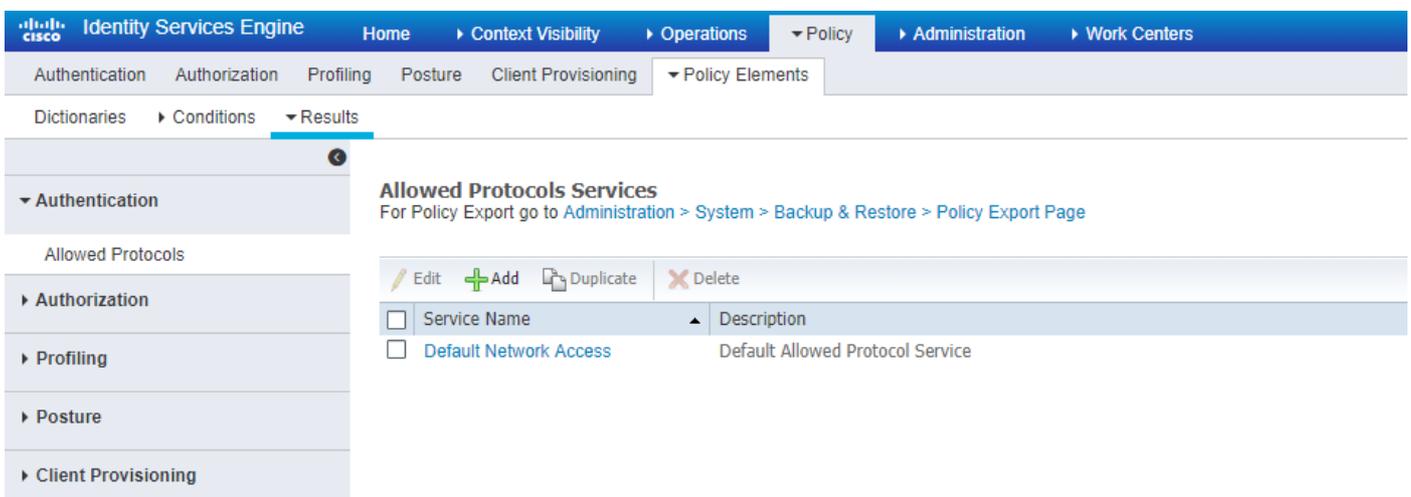
ISE avec Cisco WLC

Paramètres EAP-TLS

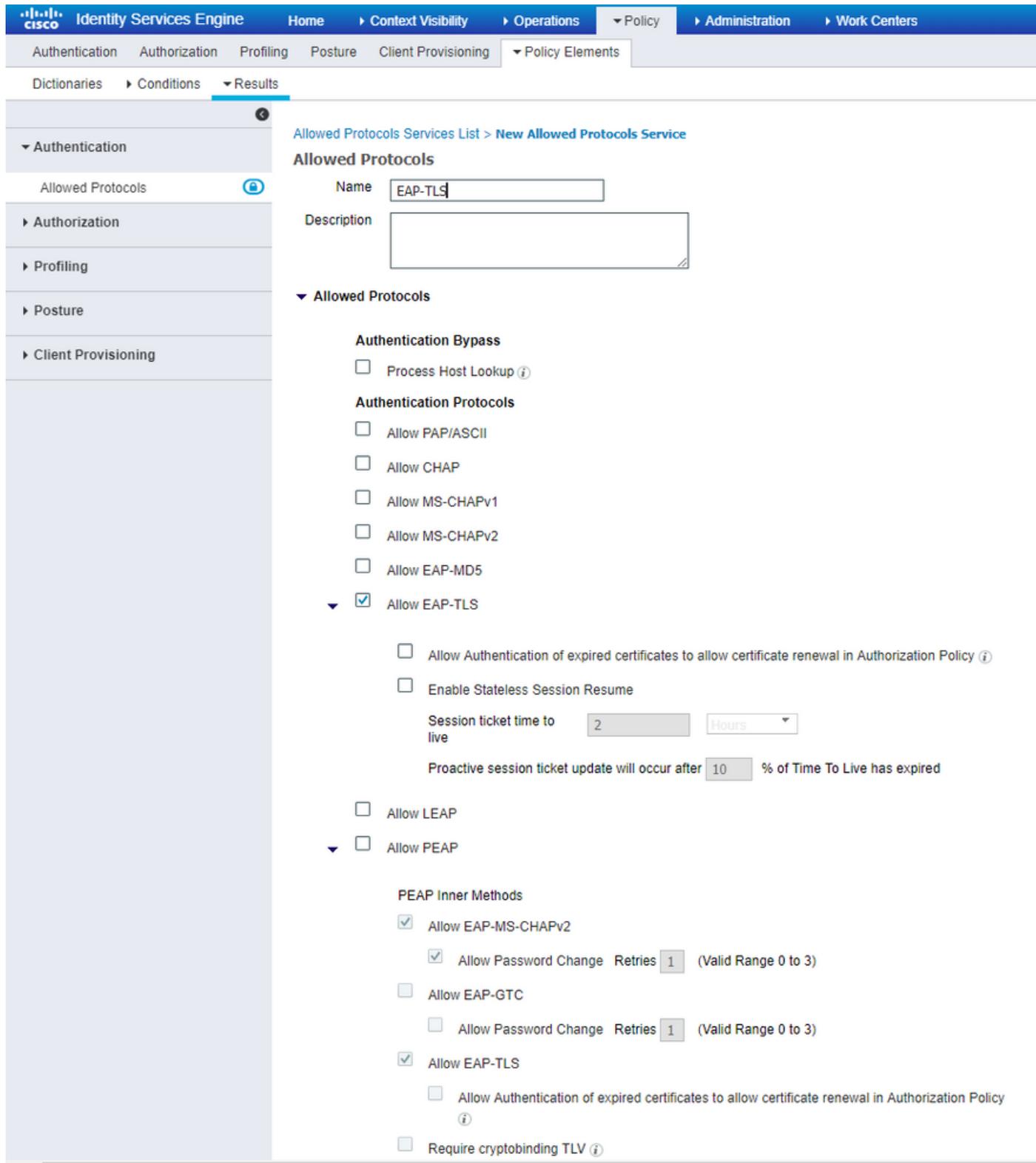
Pour créer la stratégie, vous devez créer la liste de protocoles autorisés à utiliser dans notre stratégie. Comme une stratégie dot1x est écrite, spécifiez le type EAP autorisé en fonction de la configuration de la stratégie.

Si vous utilisez la valeur par défaut, vous autorisez la plupart des types EAP pour l'authentification qui ne sont pas préférés si vous devez verrouiller l'accès à un type EAP spécifique.

Étape 1. Accédez à **Policy > Policy Elements > Results > Authentication > Allowed Protocols** et cliquez sur **Add** comme indiqué dans l'image.

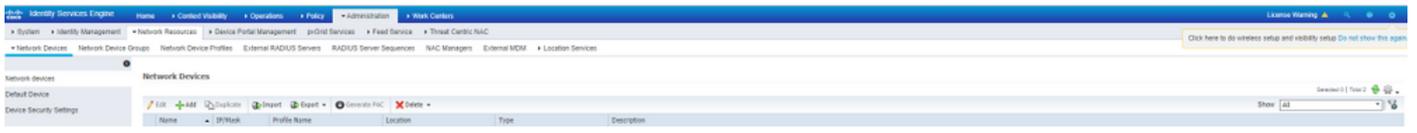


Étape 2. Dans cette liste de protocoles autorisés, vous pouvez entrer le nom de la liste. Dans ce cas, la case **Allow EAP-TLS** est cochée et les autres cases sont décochées comme illustré dans l'image.

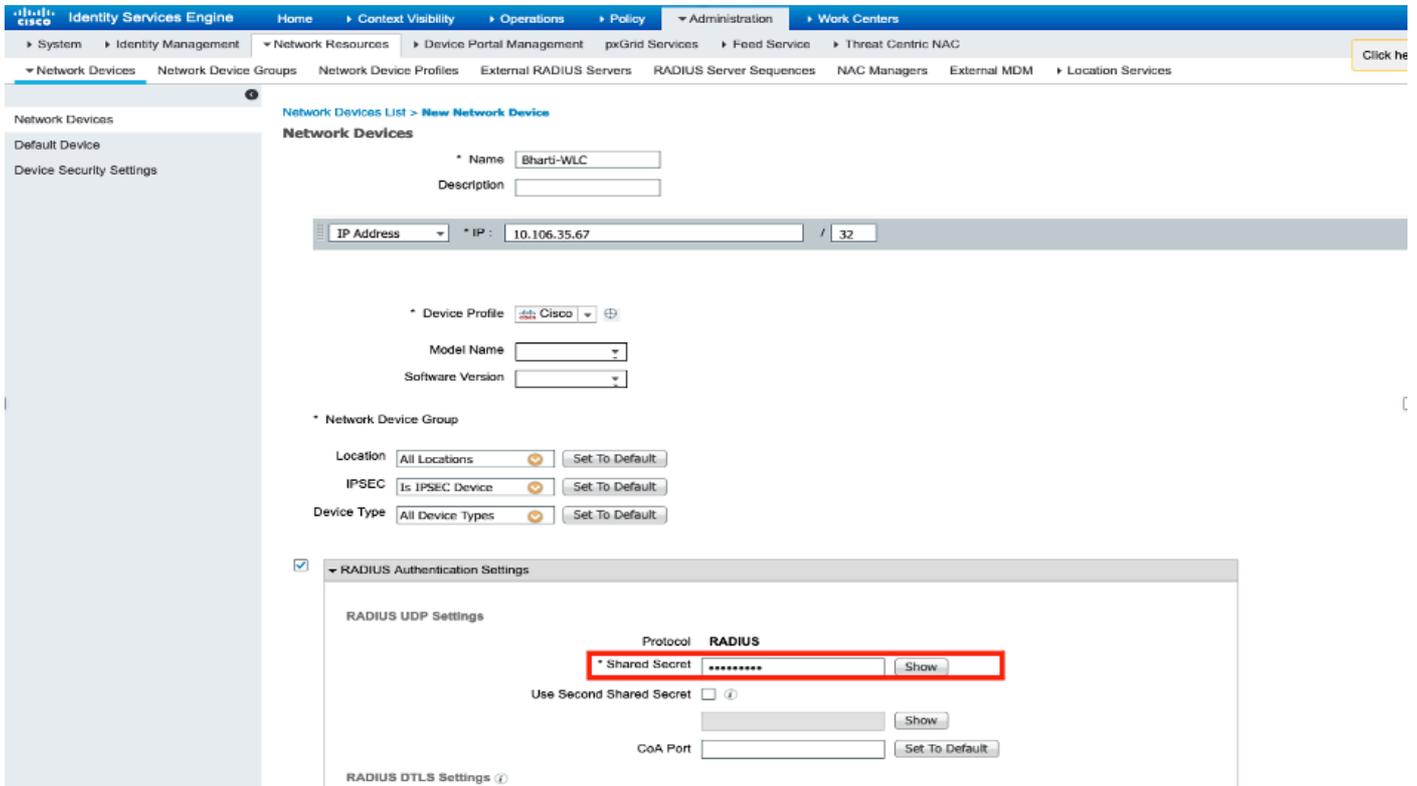


Paramètres WLC sur ISE

Étape 1. Ouvrez la console ISE et accédez à **Administration > Network Resources > Network Devices > Add** comme indiqué dans l'image.



Étape 2. Entrez les valeurs indiquées dans l'image.



Créer un nouvel utilisateur sur ISE

Étape 1. Accédez à **Administration > Identity Management > Identities > Users > Add** comme indiqué dans l'image.



Étape 2. Entrez les informations comme indiqué dans l'image.

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

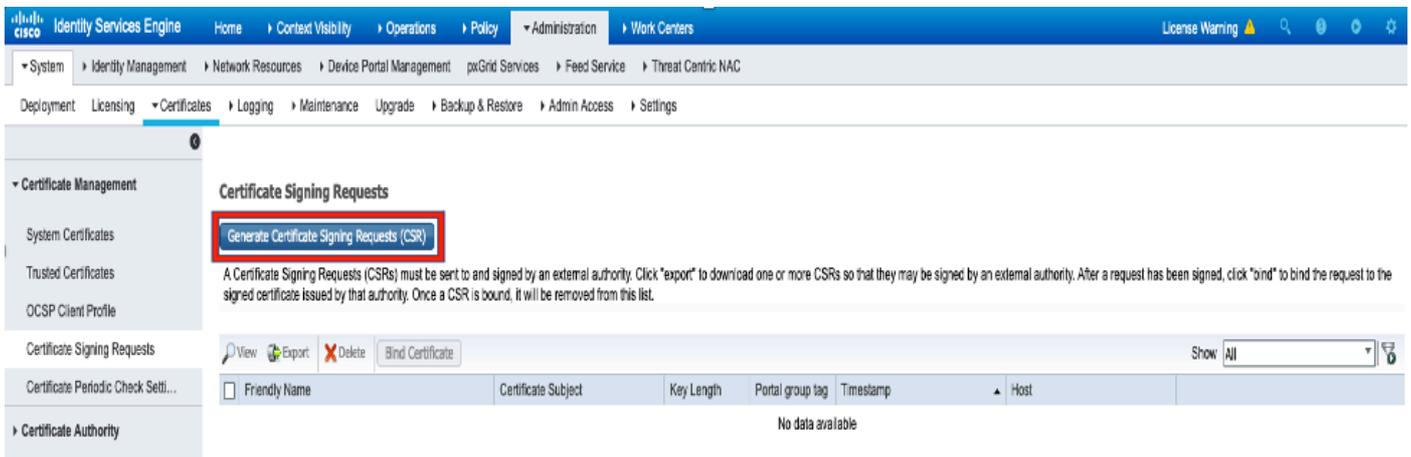
Select an item

Certificat de confiance sur ISE

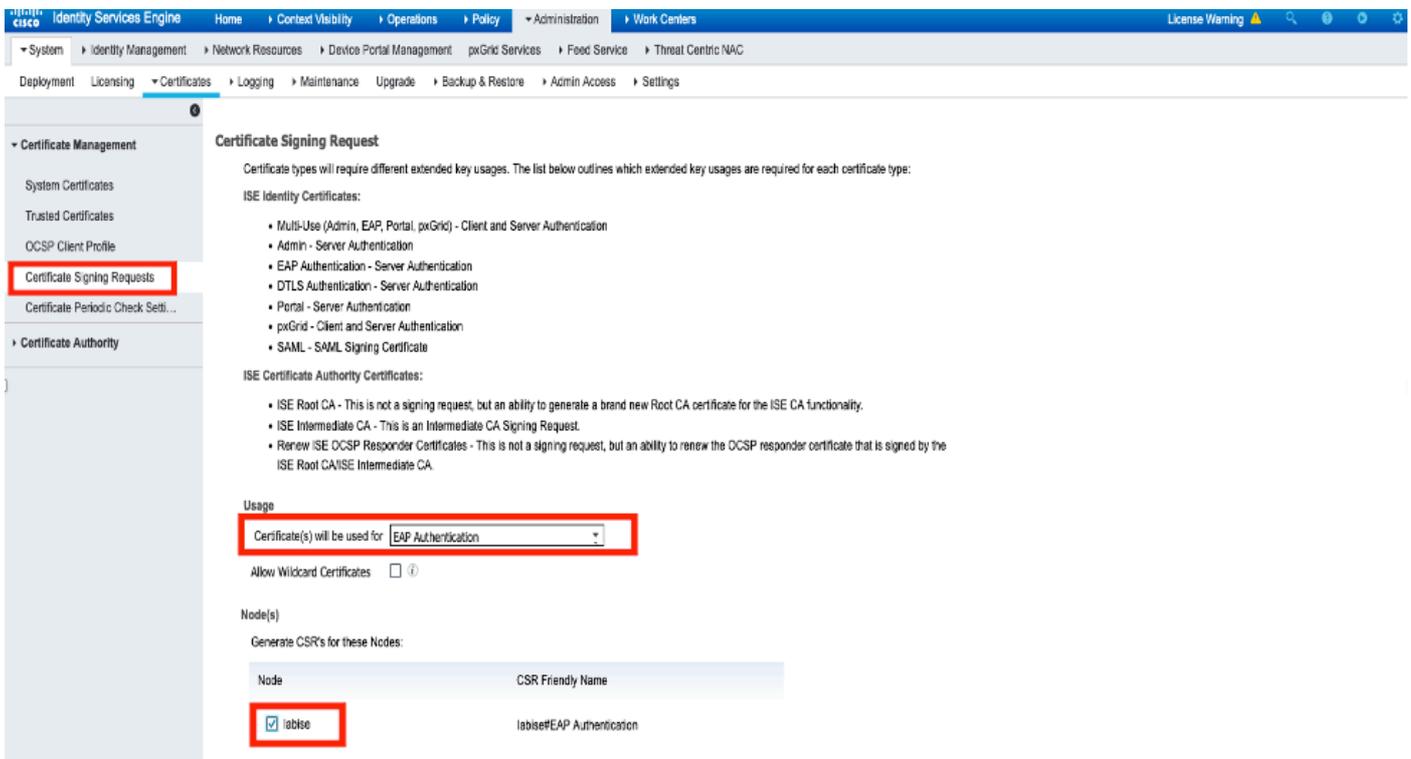
Étape 1. Accédez à **Administration > System > Certificates > Certificate Management > Trusted certificates**.

Cliquez sur **Import** afin d'importer un certificat vers ISE. Une fois que vous avez ajouté un WLC et créé un utilisateur sur ISE, vous devez faire la partie la plus importante de EAP-TLS qui est de faire confiance au certificat sur ISE. Pour cela, nous devons générer de la RSE.

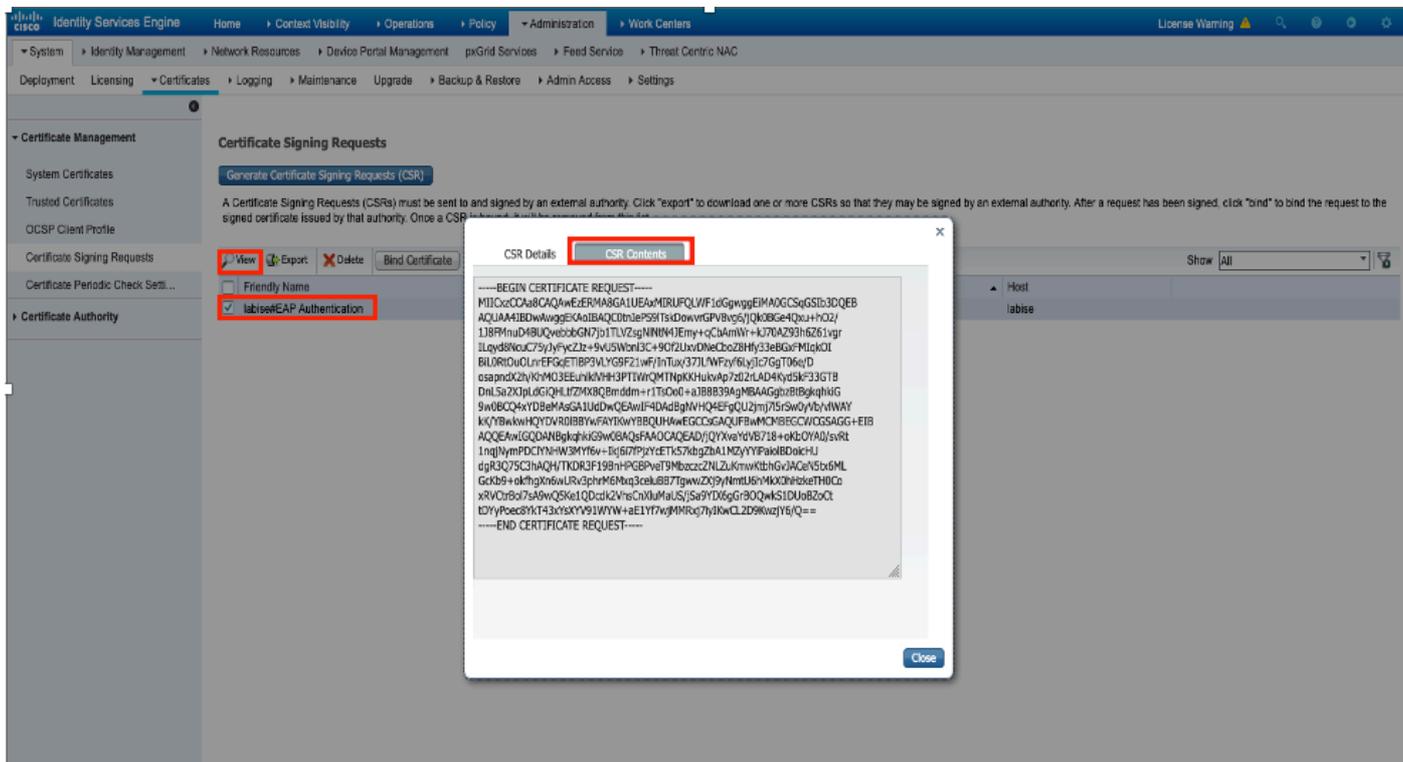
Étape 2. Accédez à **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR)** comme indiqué dans l'image.



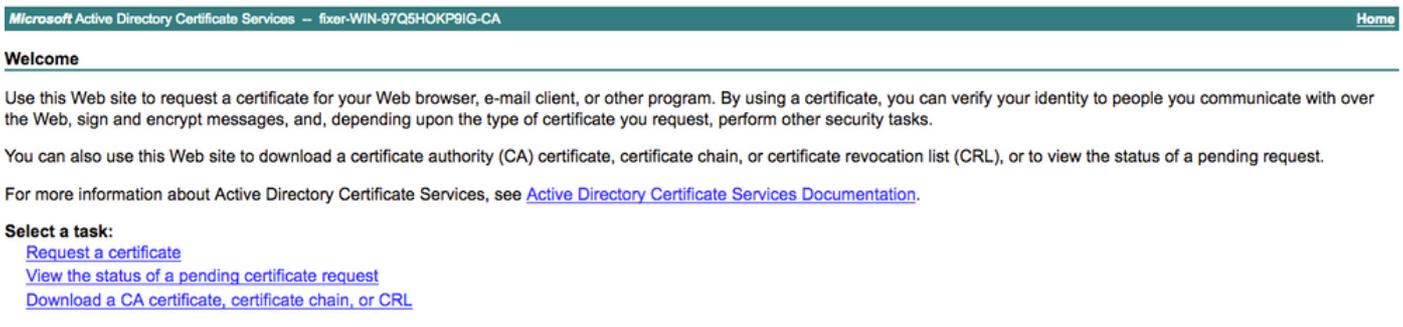
Étape 3. Afin de générer CSR, naviguez vers **Usage** et à partir du **ou des certificats sont utilisés** pour les options déroulantes sélectionnez **EAP Authentication** comme indiqué dans l'image.



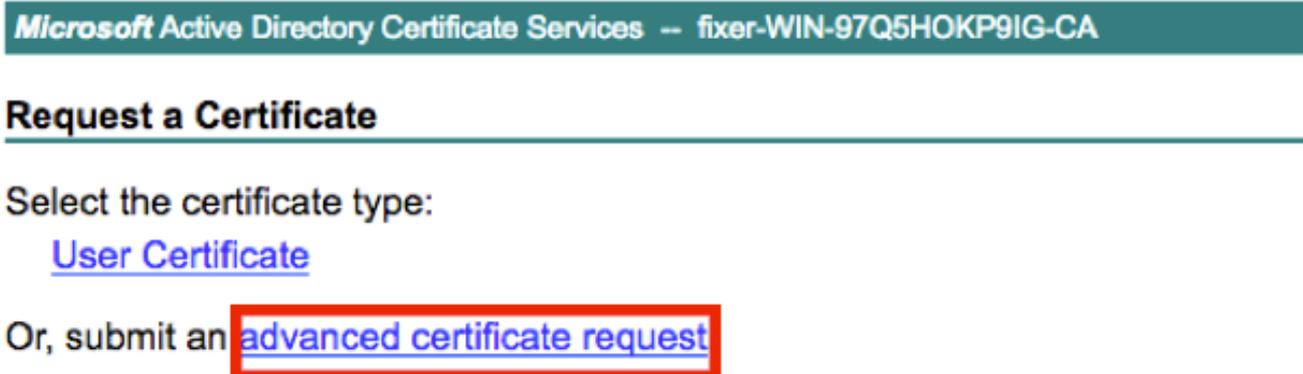
Étape 4. Le CSR généré sur ISE peut être affiché. Cliquez sur **View** comme indiqué dans l'image.



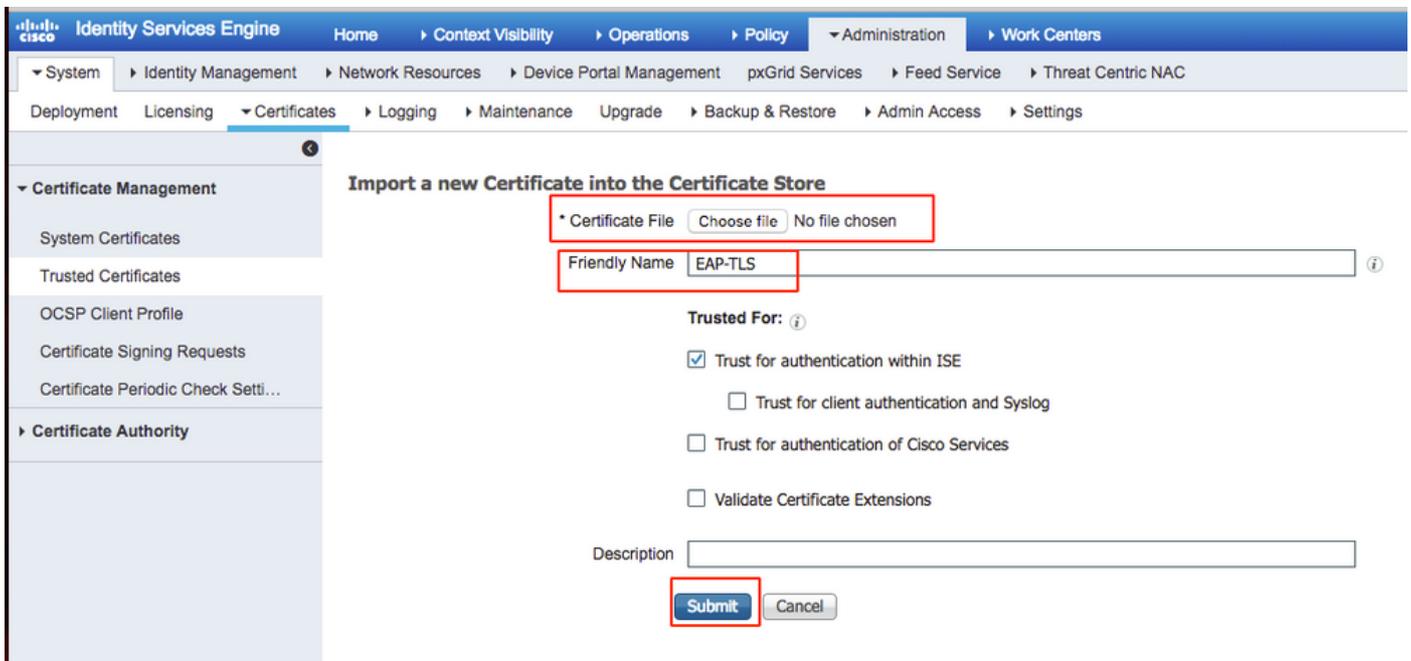
Étape 5. Une fois la CSR générée, recherchez le serveur AC et cliquez sur **Request a certificate (Demander un certificat)** comme indiqué dans l'image :



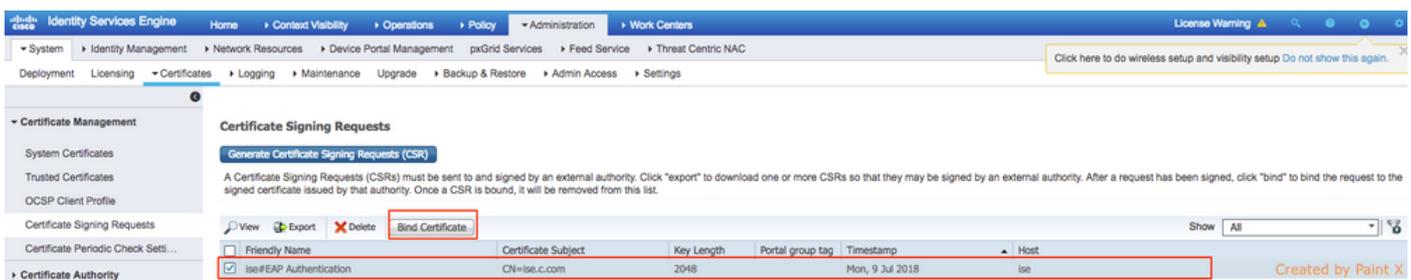
Étape 6. Une fois que vous avez demandé un certificat, vous obtenez les options **User Certificate** et **advanced certificate request**, cliquez sur **advanced certificate request** comme indiqué dans l'image.



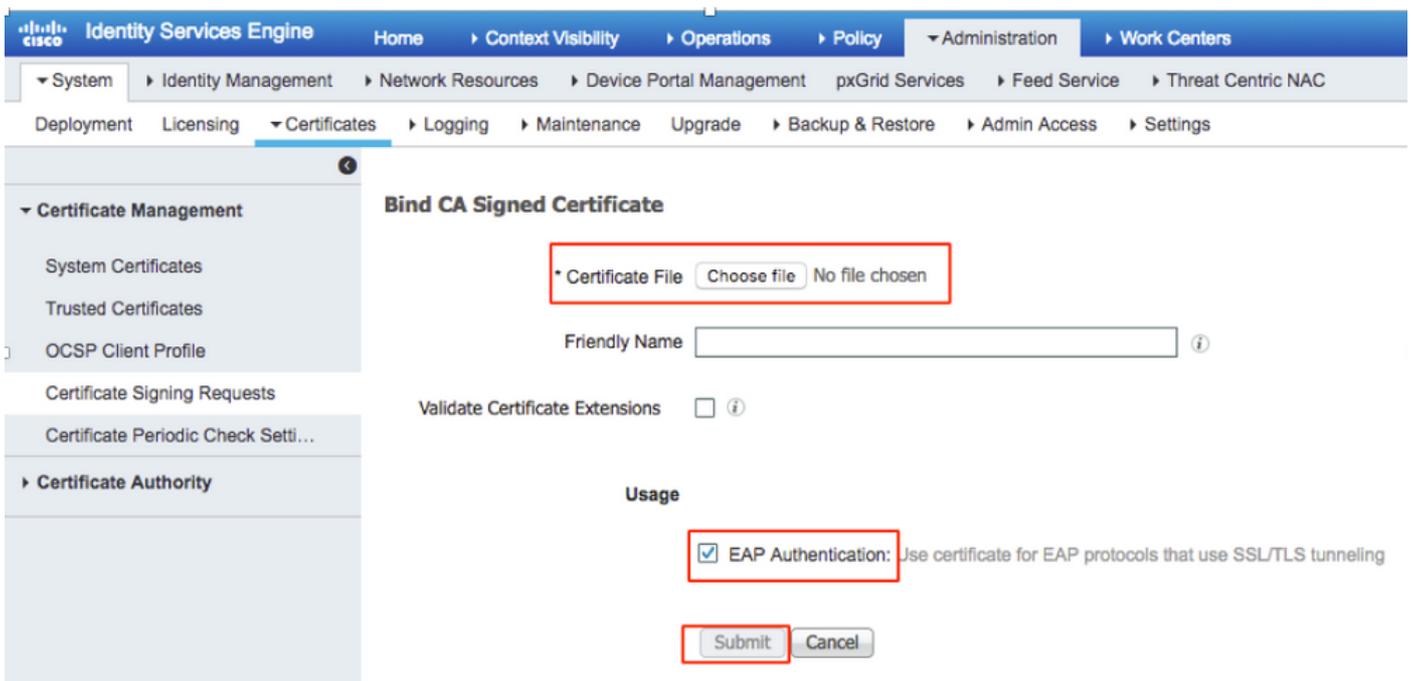
Étape 7. Collez le CSR généré dans la **demande de certificat codé en base 64**. À partir du **modèle de certificat** : , choisissez **Web Server** et cliquez sur **Submit**, comme illustré dans l'image.



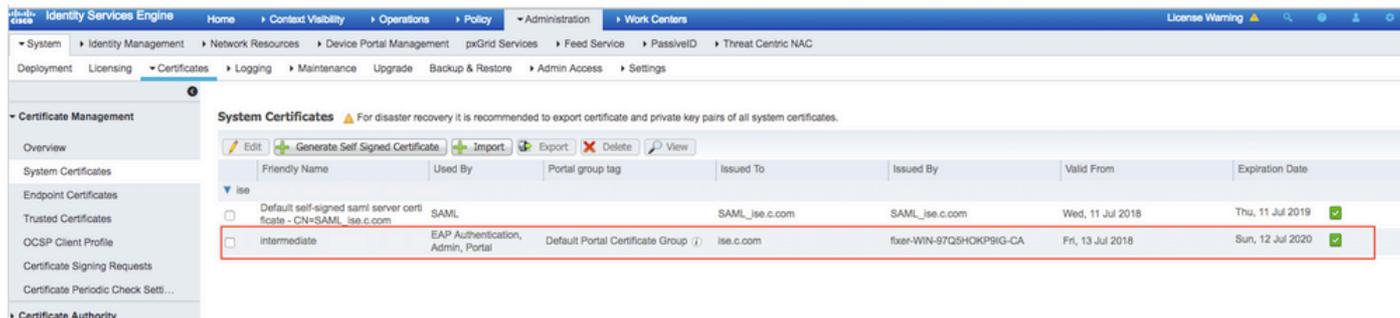
Étape 10. Une fois que vous avez cliqué sur **Submit**, le certificat est ajouté à la liste des certificats de confiance. En outre, le certificat intermédiaire est nécessaire pour établir une liaison avec CSR, comme illustré dans l'image.



Étape 11. Une fois que vous avez cliqué sur **Lier le certificat**, il y a une option pour choisir le fichier de certificat enregistré sur votre bureau. Accédez au certificat intermédiaire et cliquez sur **Submit** comme indiqué dans l'image.



Étape 12. Pour afficher le certificat, accédez à **Administration > Certificates > System Certificates** comme indiqué dans l'image.



Client pour EAP-TLS

Télécharger le certificat utilisateur sur l'ordinateur client (Bureau Windows)

Étape 1. Pour authentifier un utilisateur sans fil via EAP-TLS, vous devez générer un certificat client. Connectez votre ordinateur Windows au réseau afin de pouvoir accéder au serveur. Ouvrez un navigateur Web et entrez l'adresse suivante : <https://sever ip addr/certsrv> :

Étape 2. Notez que l'autorité de certification doit être identique à celle avec laquelle le certificat a été téléchargé pour ISE.

Pour cela, vous devez rechercher le même serveur AC que celui que vous avez utilisé pour télécharger le certificat pour le serveur. Sur la même autorité de certification, cliquez sur **Demander un certificat** comme précédemment fait, mais cette fois vous devez sélectionner **User** comme modèle de certificat comme indiqué dans l'image.

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 >

Étape 3. Cliquez ensuite sur **télécharger la chaîne de certificats** comme cela a été fait précédemment pour le serveur.

Une fois que vous obtenez les certificats, suivez ces étapes afin d'importer le certificat sur l'ordinateur portable Windows :

Étape 4. Pour importer le certificat, vous devez y accéder à partir de la console MMC (Microsoft Management Console).

1. Afin d'ouvrir la MMC naviguez à **Démarrer > Exécuter > MMC**.
2. Accédez à **Fichier > Ajouter/Supprimer un composant logiciel enfichable**
3. Double-cliquez sur **Certificats**.
4. **Sélectionnez Compte d'ordinateur**.
5. Sélectionnez **Ordinateur local > Terminer**
6. Cliquez sur **OK** afin de quitter la fenêtre du composant logiciel enfichable.
7. Cliquez sur **[+]** en regard de **Certificats > Personnel > Certificats**.
8. Cliquez avec le bouton droit sur **Certificats** et sélectionnez **All Tasks > Import**.
9. Cliquez sur **Next** (Suivant).
10. Cliquez sur **Browse**.

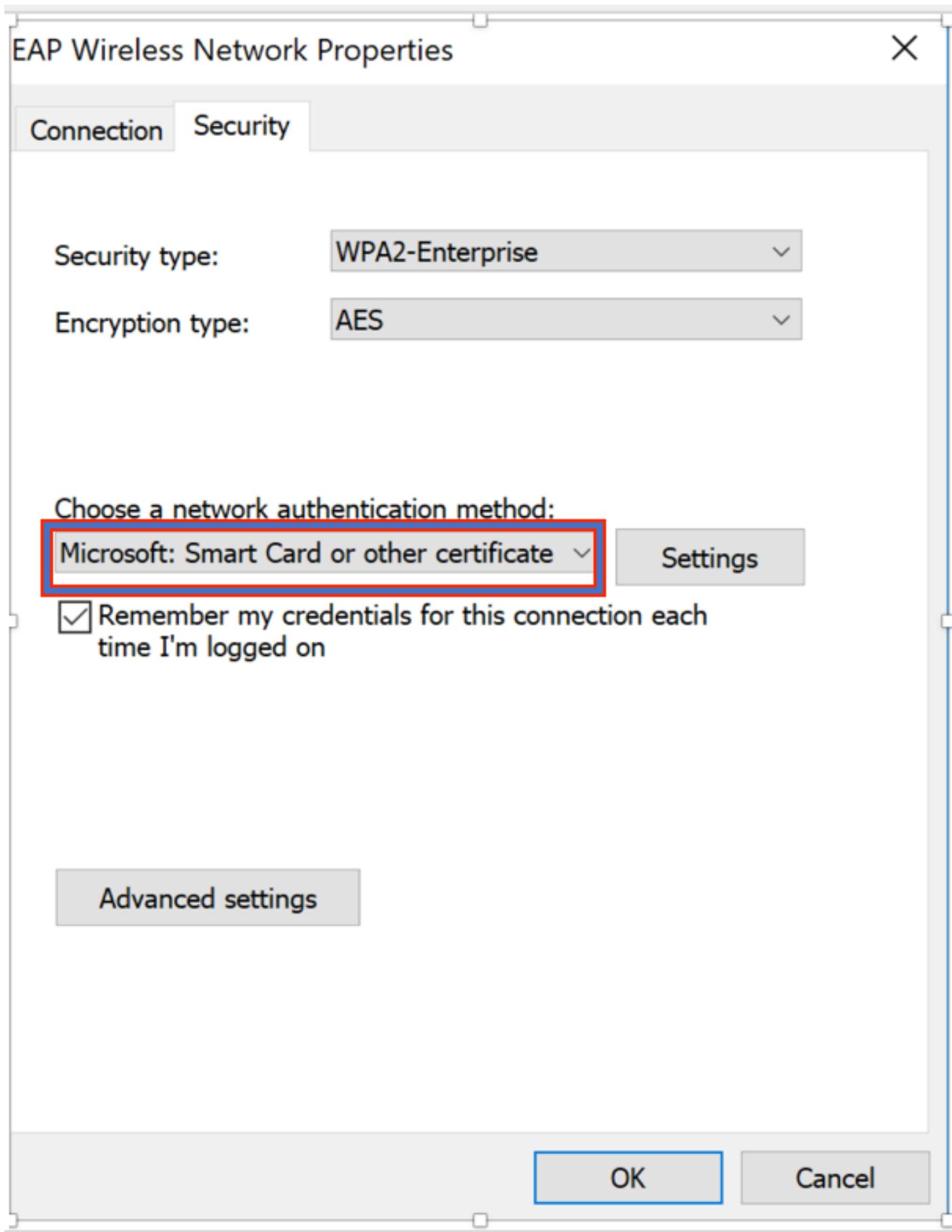
11. Sélectionnez le fichier **.cer**, **.crt** ou **.pfx** que vous souhaitez importer.
12. Cliquez sur **Open**.
13. Cliquez sur **Next** (Suivant).
14. Sélectionnez **Sélectionner automatiquement le magasin de certificats en fonction du type de certificat**.
15. Cliquez sur **Terminer** et sur **OK**

Une fois l'importation du certificat terminée, vous devez configurer votre client sans fil (bureau Windows dans cet exemple) pour EAP-TLS.

Profil sans fil pour EAP-TLS

Étape 1 : modification du profil sans fil créé précédemment pour le protocole PEAP (Protected Extensible Authentication Protocol) afin d'utiliser le protocole EAP-TLS à la place Cliquez sur **Profil sans fil EAP**.

Étape 2. Sélectionnez **Microsoft : Carte à puce ou autre certificat** et cliquez sur **OK** affiché dans l'image.



Étape 3. Cliquez sur **settings** et sélectionnez le certificat racine émis à partir du serveur AC, comme indiqué dans l'image.

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

Étape 4. Cliquez sur **Advanced Settings** et sélectionnez **User or computer authentication** dans l'onglet 802.1x settings comme indiqué dans l'image.

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

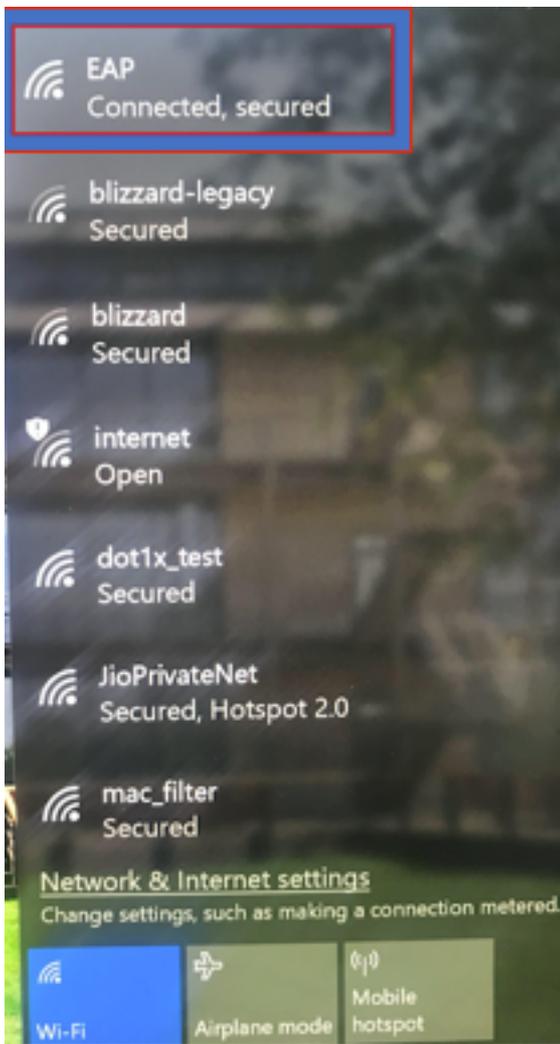
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

Étape 5. Maintenant, essayez de vous reconnecter au réseau sans fil, sélectionnez le profil correct (EAP dans cet exemple) et **Connect**. Vous êtes connecté au réseau sans fil comme illustré dans l'image.



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. L'état du gestionnaire de stratégies client doit être **RUN**. Cela signifie que le client a terminé l'authentification, obtenu l'adresse IP et est prêt à transmettre le trafic affiché dans l'image.

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

Étape 2. Vérifiez également la méthode EAP correcte sur le WLC dans la page de détails du client, comme illustré dans l'image.

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

Étape 3. Voici les détails du client de l'interface de ligne de commande du contrôleur (résultats écrêtés) :

```
(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

Étape 4. Sur ISE, accédez à **Context Visibility > End Points > Attributes** comme indiqué dans les images.

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 main content area displays the endpoint details for MAC address 34:02:86:96:2F:B7. The 'Attributes' tab is selected, showing 'General Attributes' and 'Other Attributes'. The 'AllowedProtocolMatchedRule' attribute is highlighted with a red box.

Endpoint Details:
 MAC Address: 34:02:86:96:2F:B7
 Username: Administrator@fixer.com
 Endpoint Profile: Intel-Device
 Current IP Address:
 Location:

General Attributes

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

Custom Attributes

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	5
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509 PKI

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"
OpenSSLerorStack	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...

Dépannage

Aucune information spécifique n'est actuellement disponible pour le dépannage de cette configuration.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.