

Comprendre et configurer EAP-TLS avec Mobility Express et ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Flux EAP-TLS](#)

[Étapes du flux EAP-TLS](#)

[Configuration](#)

[Cisco Mobility Express](#)

[ISE avec Cisco Mobility Express](#)

[Paramètres EAP-TLS](#)

[Paramètres Mobility Express 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 la sécurité 802.1x dans un contrôleur Mobility Express. Ce document explique également l'utilisation du protocole EAP (Extensible Authentication Protocol) - TLS (Transport Layer Security).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration initiale de Mobility Express
- Processus d'authentification 802.1x
- Certificats

Components Used

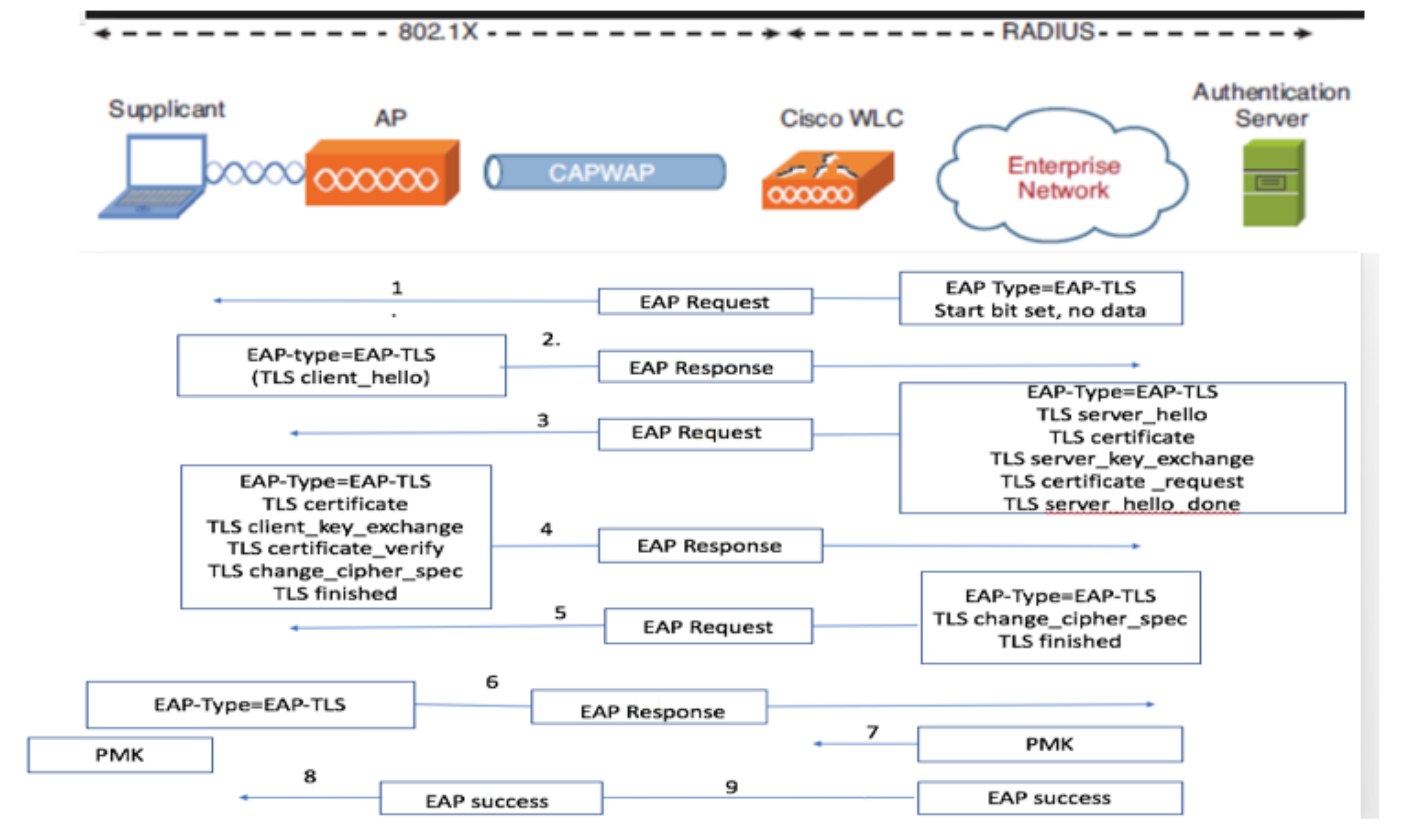
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

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 (AP).
2. Le point d'accès n'autorise pas le client à envoyer des données à ce stade et envoie une demande d'authentification.
3. Le demandeur répond ensuite avec une identité de réponse EAP. Le WLC communique ensuite les informations d'ID utilisateur au serveur d'authentification.
4. Le serveur RADIUS répond au client avec un paquet de démarrage EAP-TLS. La conversation EAP-TLS commence à ce stade.
5. L'homologue renvoie une réponse EAP au serveur d'authentification qui contient un message de connexion « client_hello », un chiffre défini sur NULL.
6. Le serveur d'authentification répond par un paquet Access-Challenge qui contient :

TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.

7. Le client répond avec un message de réponse EAP qui contient :

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

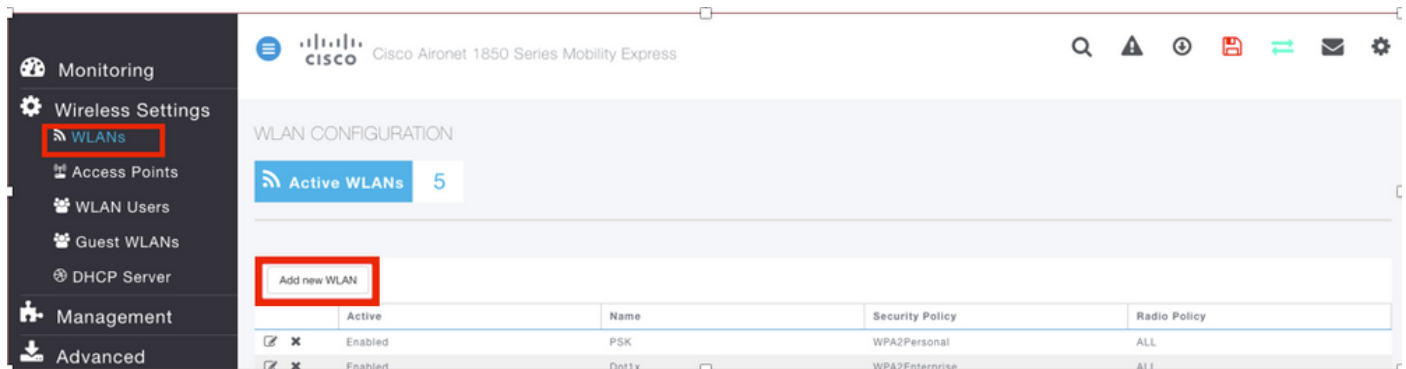
8. Une fois le client authentifié, le serveur RADIUS répond avec un défi d'accès, qui contient le message « change_cipher_spec » et le message de fin de la connexion. À la réception de ce message, le client vérifie le hachage afin d'authentifier le serveur RADIUS. Une nouvelle clé de chiffrement est dérivée dynamiquement du secret pendant la connexion TLS.

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

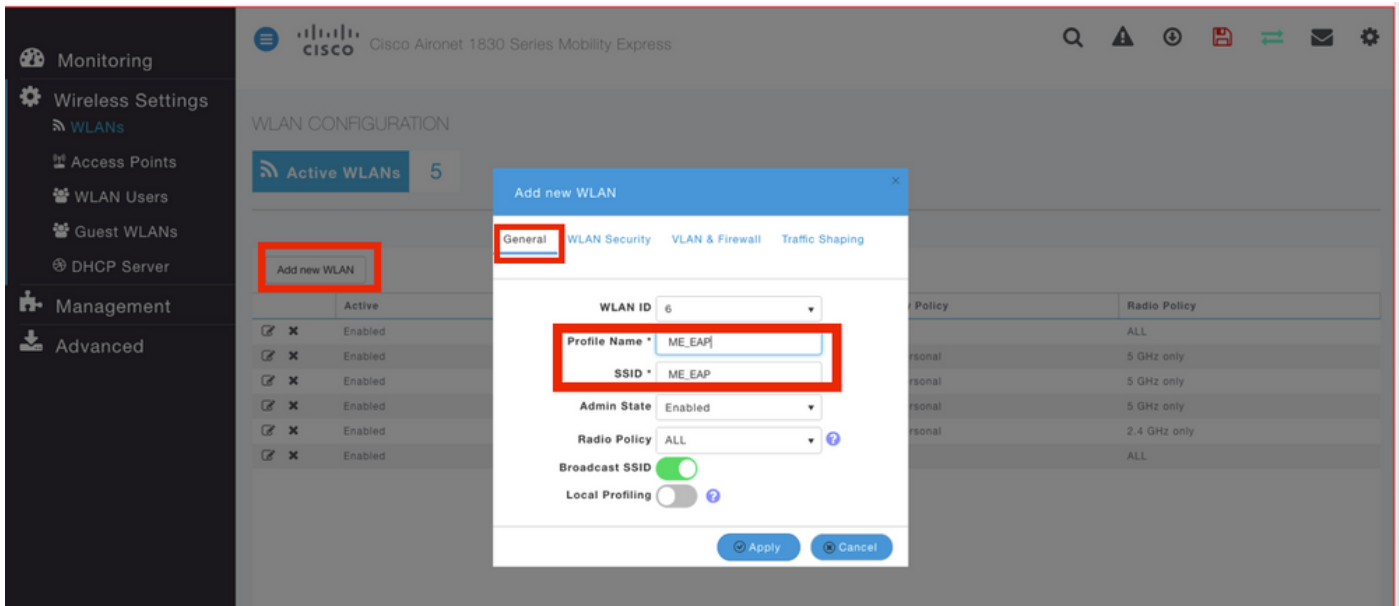
Configuration

Cisco Mobility Express

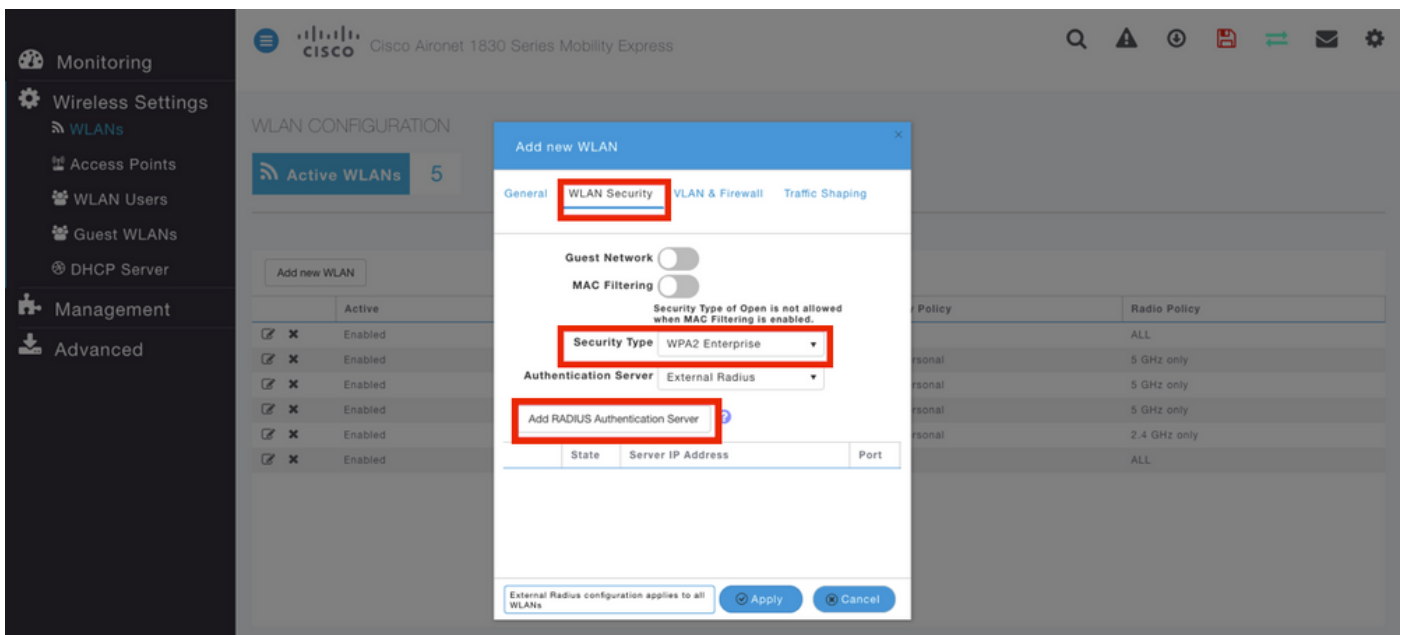
Étape 1. La première étape consiste à créer un WLAN sur Mobility Express. Afin de créer un WLAN, accédez à **WLAN > Add new WLAN** comme indiqué dans l'image.



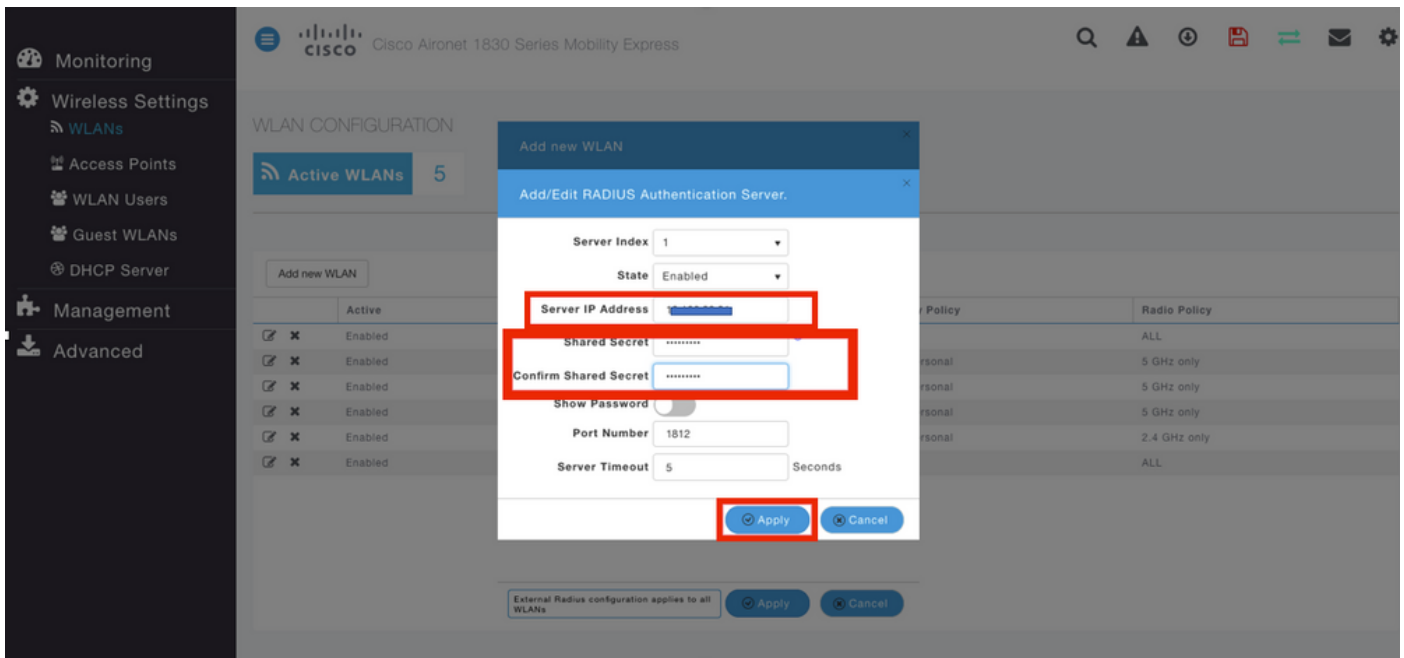
Étape 2. Une nouvelle fenêtre contextuelle apparaît lorsque vous cliquez sur **Ajouter un nouveau WLAN**. Afin de créer un nom de profil, accédez à **Ajouter un nouveau WLAN > Général** comme indiqué dans l'image.



Étape 3. Configurez le type d'authentification en tant que WPA Enterprise pour 802.1x et configurez RADIUS Server sous **Ajouter un nouveau WLAN > WLAN Security** comme indiqué dans l'image.



Étape 4. Cliquez sur **Add RADIUS Authentication Server** et indiquez l'adresse IP du serveur RADIUS et du secret partagé qui doit correspondre exactement à ce qui a été configuré sur ISE, puis cliquez sur **Apply** comme indiqué dans l'image.



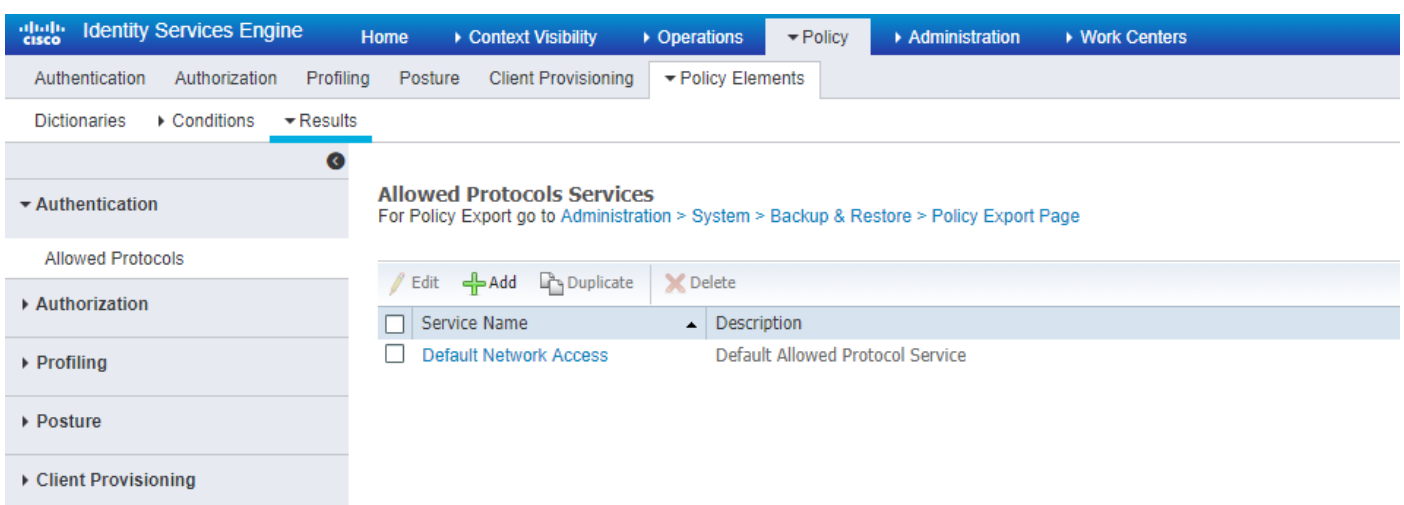
ISE avec Cisco Mobility Express

Paramètres EAP-TLS

Pour créer la stratégie, vous devez créer la liste de protocoles autorisée à utiliser dans votre stratégie. Étant donné qu'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, ce qui peut ne pas être préférable si vous devez verrouiller l'accès à un type EAP spécifique.

Étape 1. Accédez à **Stratégie > Eléments de stratégie > Résultats > Authentification > Protocoles autorisés** et cliquez sur **Ajouter** 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 **Autoriser EAP-TLS** est cochée et d'autres cases sont décochées comme indiqué dans l'image.

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 *(?)*

Paramètres Mobility Express sur ISE

Étape 1. Ouvrez la console ISE et accédez à **Administration > Network Resources > Network Devices > Add** 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 > 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

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

The screenshot shows the 'New Network Device' configuration page in Cisco ISE. The 'RADIUS Authentication Settings' section is expanded, and the 'Shared Secret' field is highlighted with a red box. Below the main form, there are three expandable sections: 'TACACS Authentication Settings', 'SNMP Settings', and 'Advanced TrustSec Settings'. At the bottom, the 'Submit' button is highlighted with a red box.

Certificat de confiance sur ISE

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

Cliquez sur **Import** afin d'importer un certificat dans 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 d'approuver le certificat sur ISE. Pour cela, vous devez générer CSR.

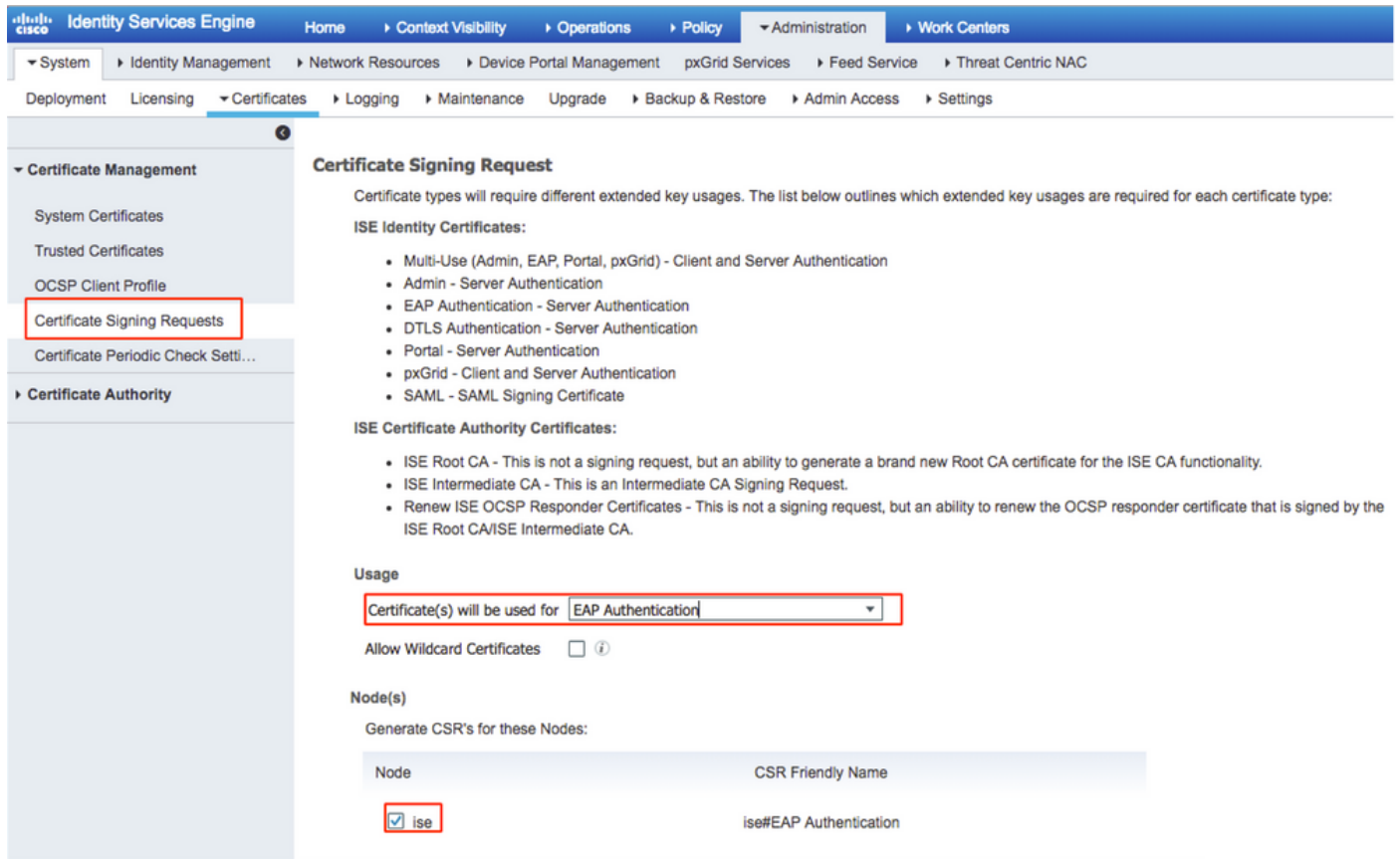
Étape 2. Accédez à **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Requests (CSR)**, comme indiqué dans l'image.

The screenshot shows the 'Generate Certificate Signing Requests (CSR)' page in Cisco ISE. The page displays a table with the following data:

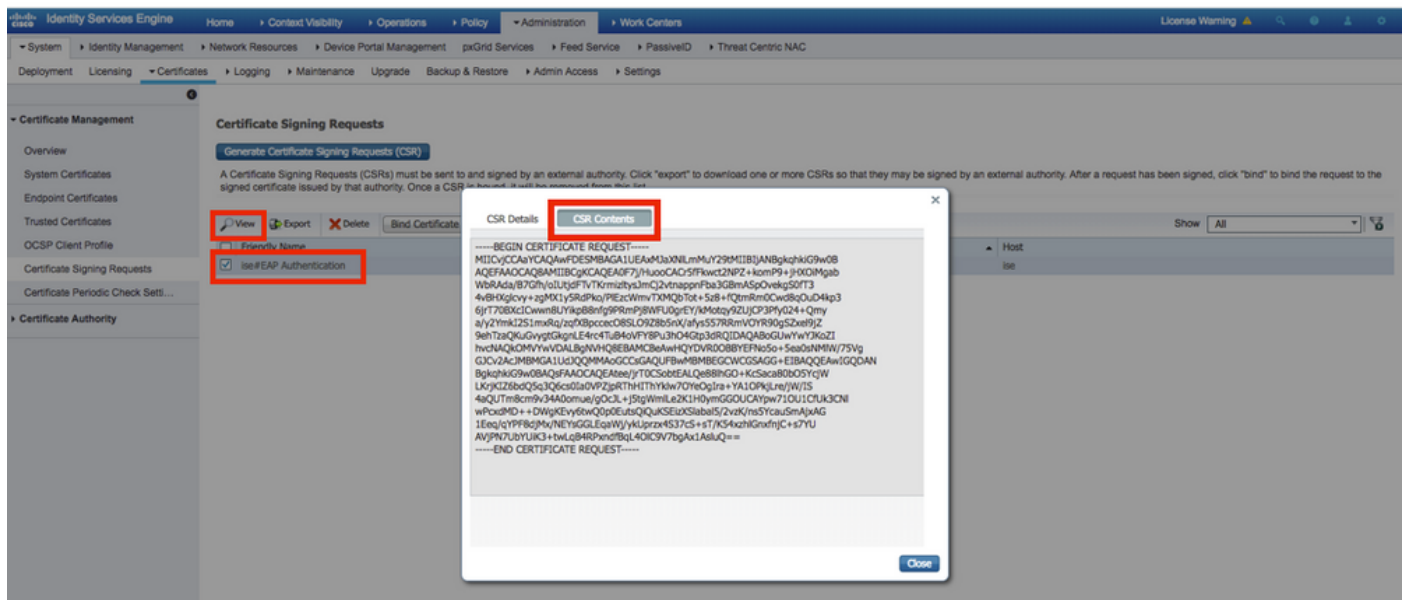
Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input type="checkbox"/> ise#EAP Authentication	CN=ise.c.com	2048	ise	Wed, 11 Jul 2018	ise

Étape 3. Afin de générer CSR, accédez à **Utilisation** et à partir du **ou des certificats seront utilisés** pour les options de liste déroulante sélectionnez **Authentification EAP** comme indiqué dans

l'image.



Étape 4. La CSR générée sur ISE peut être affichée. Cliquez sur **Affichage** comme indiqué dans l'image.



Étape 5. Une fois le CSR généré, recherchez le serveur AC et cliquez sur **Demander un certificat** comme indiqué dans l'image :

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](#)

Étape 6. Une fois que vous avez demandé un certificat, vous obtenez des options pour le **certificat utilisateur** et la **demande de certificat avancée**, cliquez sur **demande de certificat avancée** comme indiqué dans l'image.

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

Request a Certificate

Select the certificate type:

[User Certificate](#)

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

Étape 7. Collez la CSR générée dans la **demande de certificat codée Base-64**. Dans l'option **Modèle de certificat** : déroulante, sélectionnez **Serveur Web** et cliquez sur **Envoyer** comme indiqué dans l'image.

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:

Étape 8. Une fois que vous avez cliqué sur **Soumettre**, vous avez la possibilité de sélectionner le type de certificat, sélectionnez **Codé Base-64** et cliquez sur **Télécharger la chaîne de certificats** comme indiqué dans l'image.

Certificate Issued

The certificate you requested was issued to you.

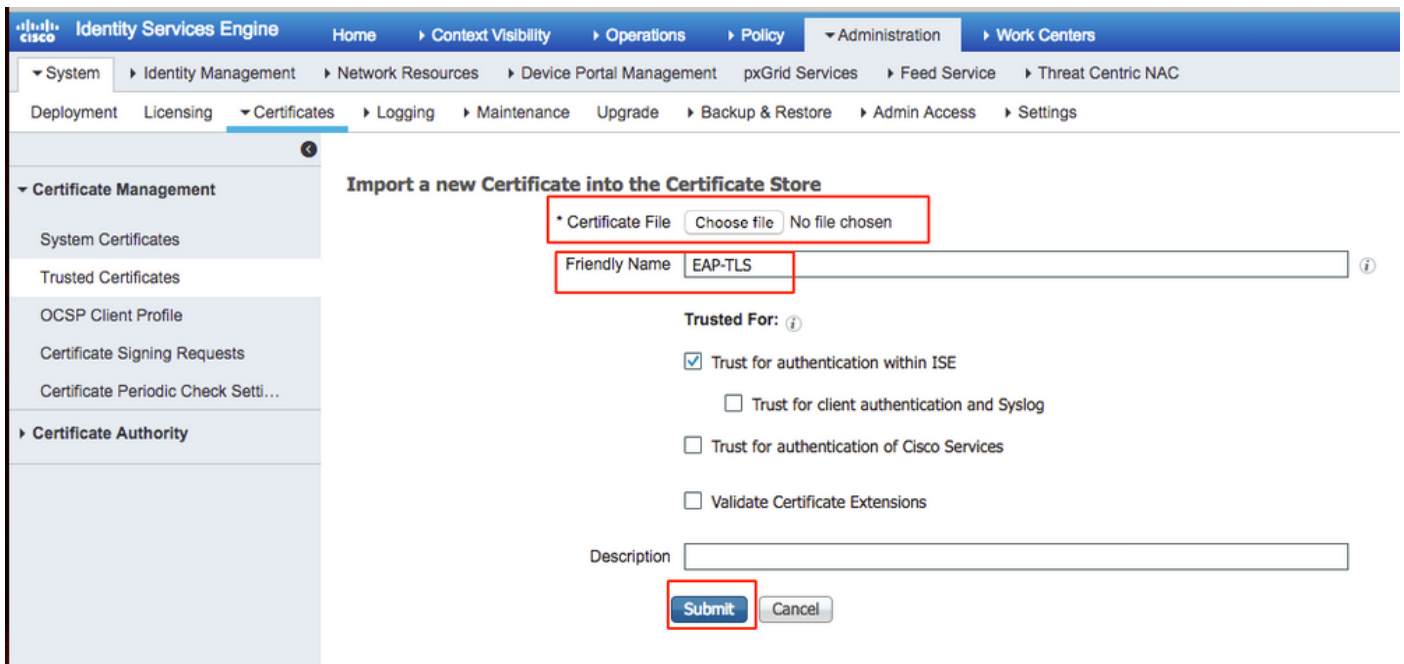
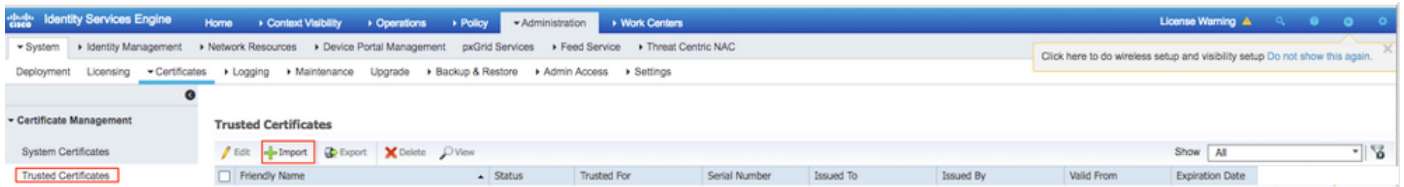
DER encoded or Base 64 encoded



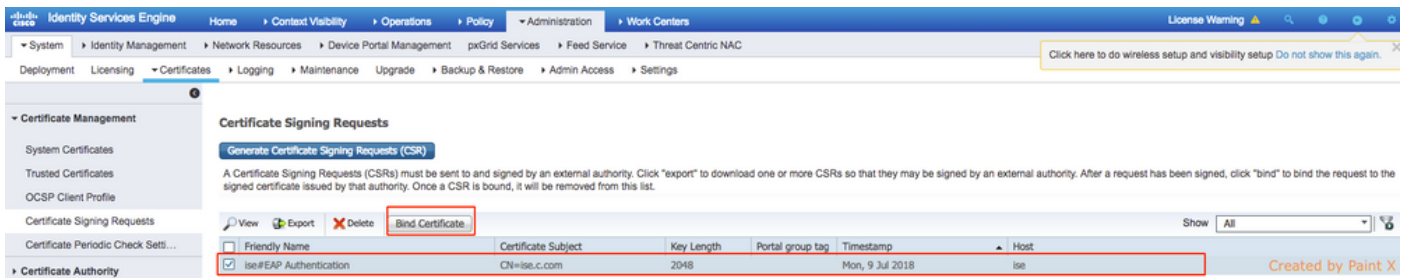
[Download certificate](#)

[Download certificate chain](#)

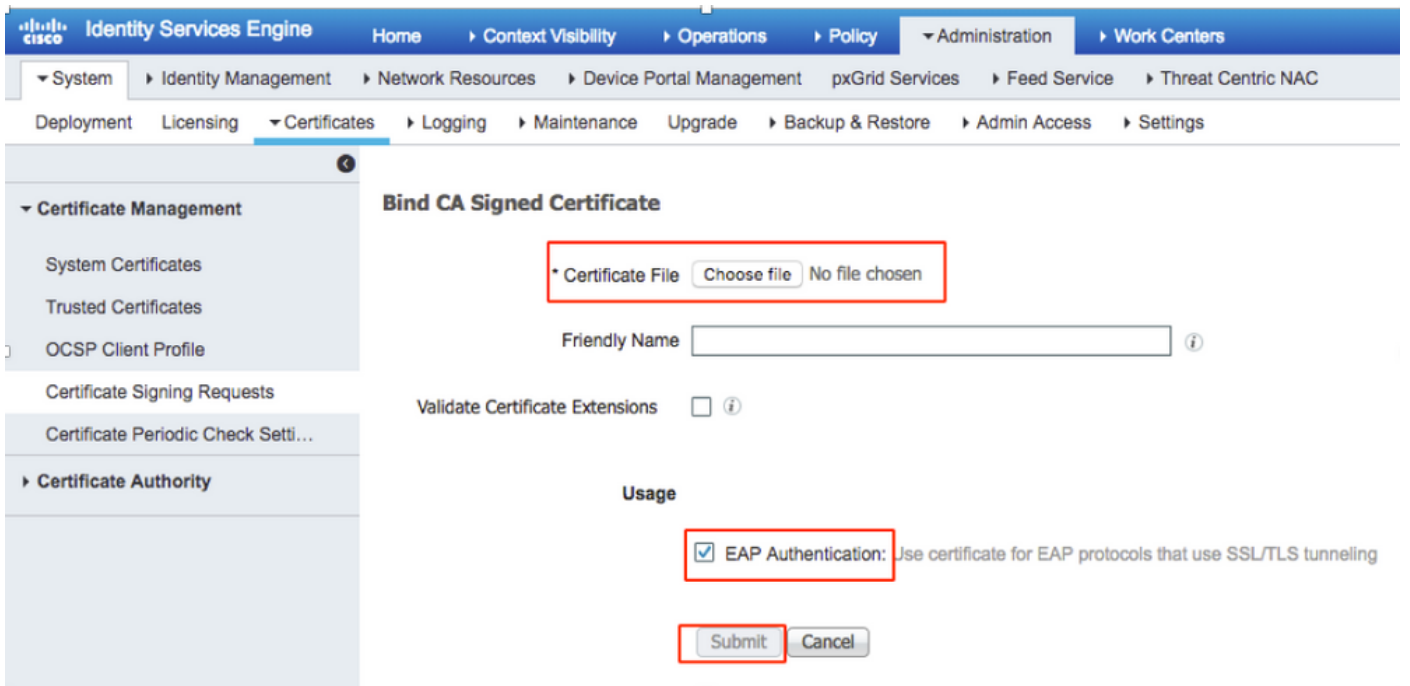
Étape 9. Le téléchargement du certificat est terminé pour le serveur ISE. Vous pouvez extraire le certificat, le certificat contient deux certificats, un certificat racine et un autre certificat intermédiaire. Le certificat racine peut être importé sous **Administration > Certificats > Certificats approuvés > Importer** comme indiqué dans les images.



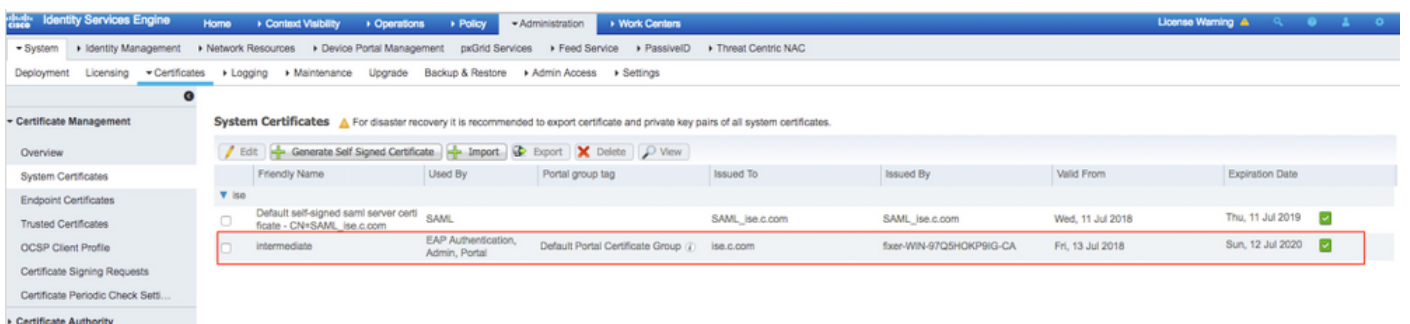
Étape 10. Lorsque vous cliquez sur **Soumettre**, le certificat est ajouté à la liste des certificats approuvés. En outre, le certificat intermédiaire est nécessaire pour se lier à CSR comme indiqué dans l'image.



Étape 11. Lorsque vous cliquez sur **Lier le certificat**, vous pouvez choisir le fichier de certificat enregistré sur votre bureau. Accédez au certificat intermédiaire et cliquez sur **Soumettre** 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 pour accéder au serveur. Ouvrez un navigateur Web et entrez cette adresse : <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 **Utilisateur** comme modèle de certificat comme indiqué dans l'image.

The screenshot shows the 'Submit a Certificate Request or Renewal Request' page. At the top, the title bar reads 'Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA'. Below the title, the main heading is 'Submit a Certificate Request or Renewal Request'. A paragraph of instructions states: '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 the following content: 'Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7): ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIspJry aF412aLpmDFp1PfvZ3VaP6Oa/mej3IXh0RFxBUII we0h06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR dD7LeujkxF1j3SwvLTKLDJq+00VtAhrxlp1PyDZ3 ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX -----END CERTIFICATE REQUEST-----'. Below this, the 'Certificate Template:' section features a dropdown menu with 'User' selected. The 'Additional Attributes:' section has an empty text area. At the bottom right, a 'Submit >' button is highlighted with a red box.

Étape 3. Ensuite, cliquez sur **télécharger la chaîne de certificats** comme précédemment pour le serveur.

Une fois les certificats obtenus, 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 Microsoft Management Console (MMC).

1. Pour ouvrir MMC, accédez à **Démarrer > Exécuter > MMC**.
2. Accédez à **Fichier > Ajouter/Supprimer un composant logiciel enfichable**
3. Double-cliquez sur **Certificats**.
4. Sélectionnez **Compte d'ordinateur**.

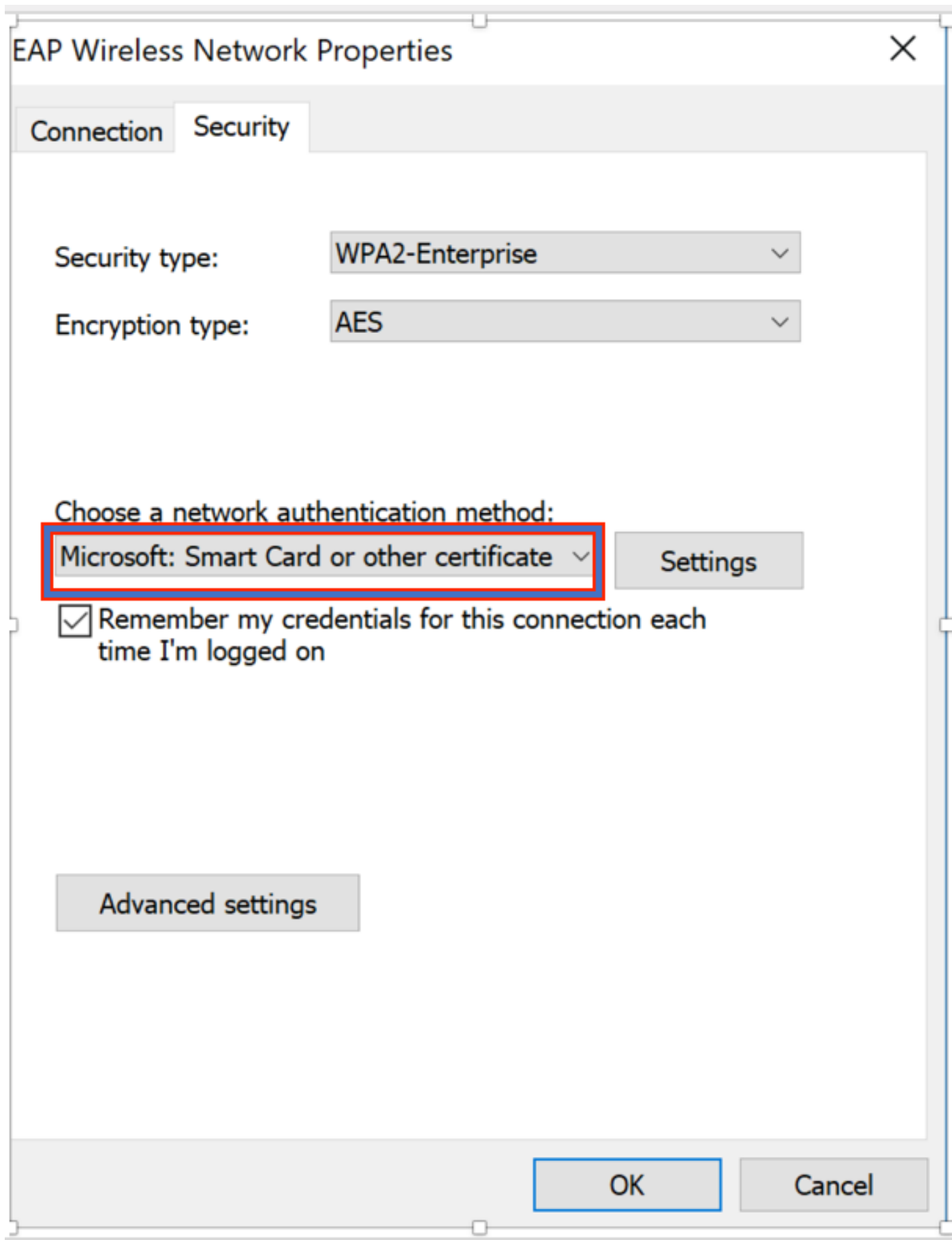
5. Sélectionnez **Ordinateur local > Terminer**
6. Cliquez sur **OK** afin de quitter la fenêtre du composant logiciel enfichable.
7. Cliquez sur **[+]** en regard de **Certificats > Personnel > Certificats**.
8. Cliquez avec le bouton droit sur **Certificats** et sélectionnez **Toutes les tâches > Importer**.
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 OK**

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

Profil sans fil pour EAP-TLS

Étape 1. Modifiez le profil sans fil créé précédemment pour le protocole PEAP (Protected Extensible Authentication Protocol) afin d'utiliser 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** comme indiqué dans l'image.



Étape 3. Cliquez sur **Paramètres** 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 (Paramètres avancés) 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

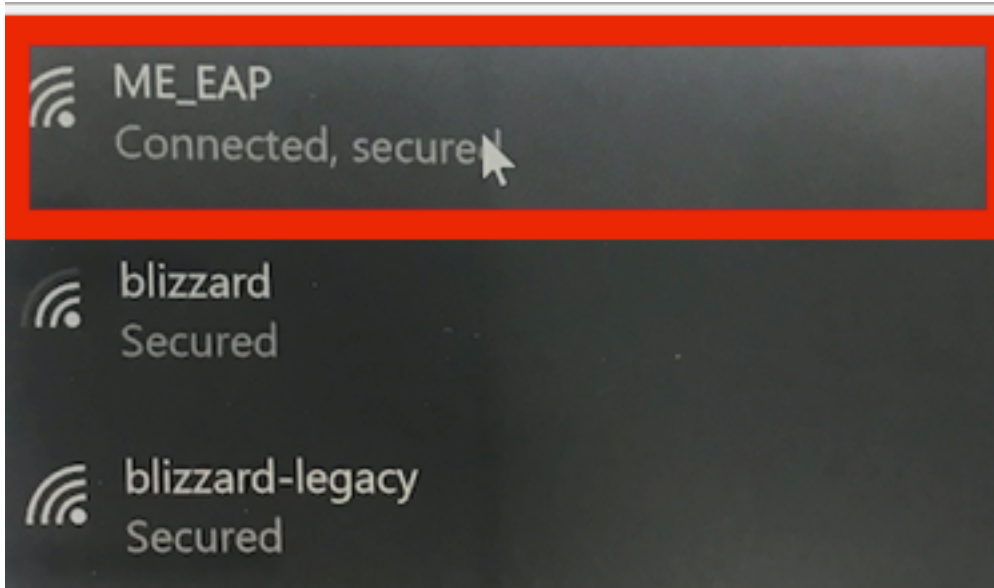
Maximum delay (seconds):

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 l'illustre l'image.



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Le type EAP du client doit être EAP-TLS. Cela signifie que le client a terminé l'authentification, avec l'utilisation d'EAP-TLS, obtenu l'adresse IP et est prêt à transmettre le trafic comme indiqué dans les images.




The screenshot displays a network management interface with a sidebar on the left and a main content area. The sidebar includes sections for Monitoring, Applications, Rogues, Interferers, Wireless Dashboard, Best Practices, Wireless Settings, Management, and Advanced. The main content area is titled 'CLIENT VIEW' and shows details for a client with SSID 'ME_EAP'. The 'GENERAL' section includes fields for User Name (Administrator), Host Name (Unknown), MAC Address (34:02:86:96:2f:b7), Uptime (Associated since 37 Seconds), 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%). The 'CONNECTIVITY' section shows a flowchart with five steps: Start, Association, Authentication, DHCP, and Online, all marked as successful. 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).

Étape 2. Voici les détails client de l'interface de ligne de commande du contrôleur (sortie cliquée) :

```
(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
```

Étape 3. Sur ISE, naviguez jusqu'à **Visibilité contextuelle > Terminaux > Attributs** comme indiqué dans les images.

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, 1.3.6.1.4.1.311.11
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

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.