

Configuration d'EAP-TLS sur le WLC 9800 avec CA interne ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Informations générales](#)

[Flux d'authentification EAP-TLS](#)

[Étapes du flux EAP-TLS](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration ISE](#)

[Ajout d'un périphérique réseau](#)

[Vérifier la CA interne](#)

[Ajouter une méthode d'authentification](#)

[Spécifier le modèle de certificat](#)

[Créer un portail de certificats](#)

[Ajouter un utilisateur interne](#)

[Configuration du portail d'approvisionnement de certificats ISE et de la stratégie RADIUS](#)

[Configuration WLC 9800](#)

[Ajouter un serveur ISE au WLC 9800](#)

[Ajouter un groupe de serveurs sur le WLC 9800](#)

[Configurer la liste de méthodes AAA sur le WLC 9800](#)

[Configurer la liste des méthodes d'autorisation sur le WLC 9800](#)

[Créer un profil de stratégie sur le WLC 9800](#)

[Créer un WLAN sur le WLC 9800](#)

[Mappage du WLAN avec le profil de stratégie sur le WLC 9800](#)

[Mapper la balise de stratégie au point d'accès sur le WLC 9800](#)

[Exécution de la configuration du WLC après la fin de l'installation](#)

[Créer et télécharger un certificat pour l'utilisateur](#)

[Installation de certificat sur un ordinateur Windows 10](#)

[Vérifier](#)

[Dépannage](#)

[Références](#)

Introduction

Ce document décrit l'authentification EAP-TLS à l'aide de l'autorité de certification du moteur

Identity Services Engine pour authentifier les utilisateurs.

Conditions préalables

Composants utilisés

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

- Contrôleur sans fil : C9800-40-K9 exécutant 17.09.04a
- Cisco ISE : Exécution du correctif 4 de la version 3
- Modèle AP : C9130AXI-D
- Commutateur : 9200-L-24P

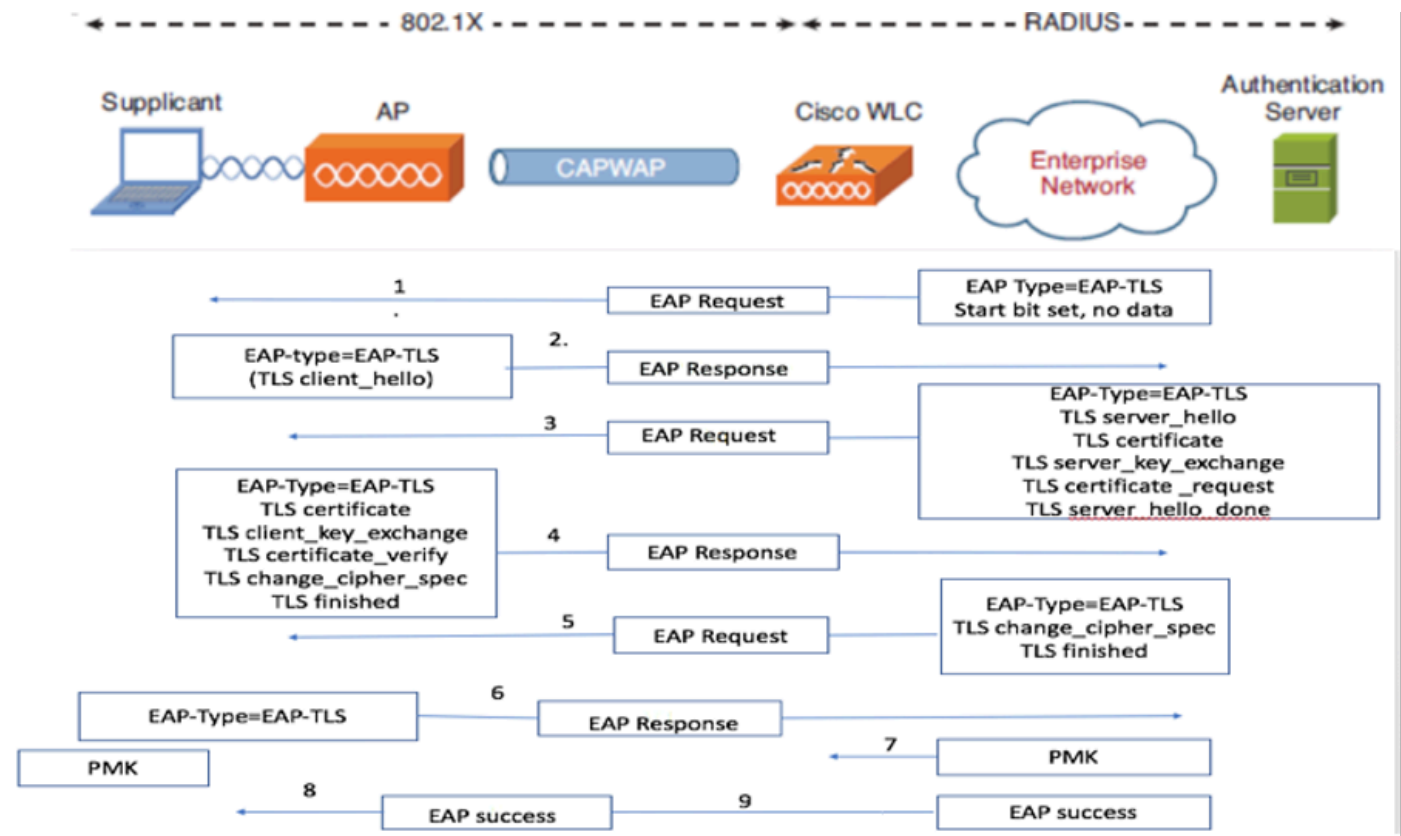
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La plupart des entreprises disposent de leur propre autorité de certification qui délivre des certificats aux utilisateurs finaux pour l'authentification EAP-TLS. ISE inclut une autorité de certification intégrée qui peut être utilisée pour générer des certificats pour les utilisateurs à utiliser dans l'authentification EAP-TLS. Dans les cas où il n'est pas possible d'utiliser une autorité de certification complète, l'utilisation de l'autorité de certification ISE pour l'authentification des utilisateurs devient avantageuse.

Ce document décrit les étapes de configuration requises pour utiliser efficacement l'autorité de certification ISE pour authentifier les utilisateurs sans fil. Flux d'authentification EAP-TLS

Flux d'authentification EAP-TLS



Flux d'authentification EAP-TLS

Étapes du flux EAP-TLS

1. Le client sans fil s'associe au point d'accès (AP).
2. À ce stade, le point d'accès n'autorise pas la transmission de données et envoie une demande d'authentification.
3. Le client, agissant en tant que demandeur, répond avec une identité de réponse EAP.
4. Le contrôleur de réseau local sans fil (WLC) transmet les informations d'ID utilisateur au serveur d'authentification.
5. Le serveur RADIUS répond au client avec un paquet de démarrage EAP-TLS.
6. La conversation EAP-TLS commence à ce stade.
7. Le client renvoie une réponse EAP au serveur d'authentification, y compris un message de connexion client_hello avec un chiffre défini sur NULL.
8. Le serveur d'authentification répond par un paquet Access-Challenge contenant :

TLS server_hello
 Handshake message
 Certificate
 Server_key_exchange
 Certificate request
 Server_hello_done

9. Le client répond par un message de réponse EAP qui inclut :

Certificate (for server validation)
Client_key_exchange
Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished

10. Une fois l'authentification du client réussie, le serveur RADIUS envoie une demande d'accès contenant :

Change_cipher_spec
Handshake finished message

11. Le client vérifie le hachage pour authentifier le serveur RADIUS.

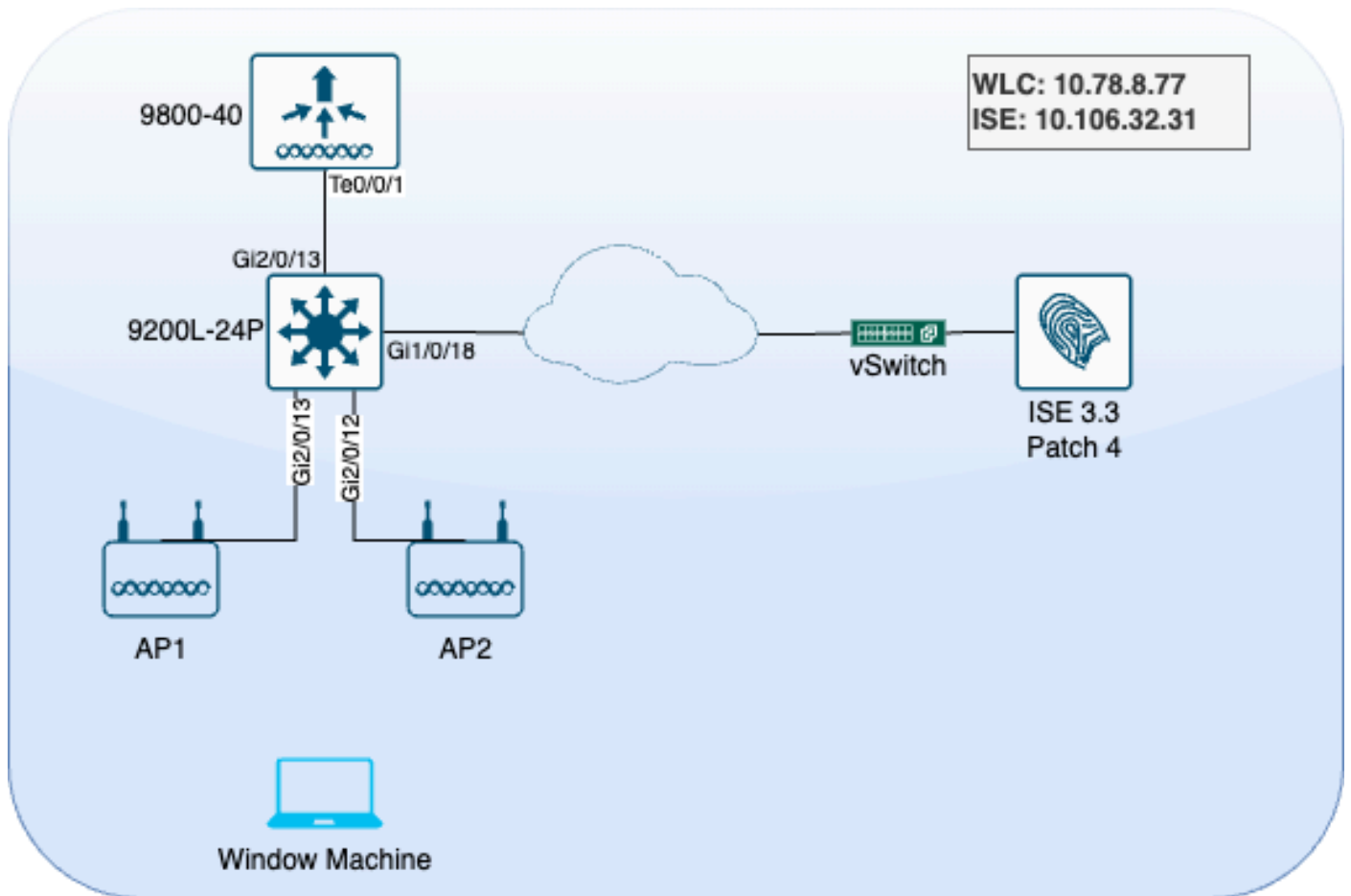
12. Une nouvelle clé de chiffrement est dérivée dynamiquement du secret lors de la connexion TLS.

13. Un message EAP-Success est envoyé du serveur à l'authentificateur, puis au demandeur.

14. Le client sans fil compatible EAP-TLS peut désormais accéder au réseau sans fil.

Configurer

Diagramme du réseau



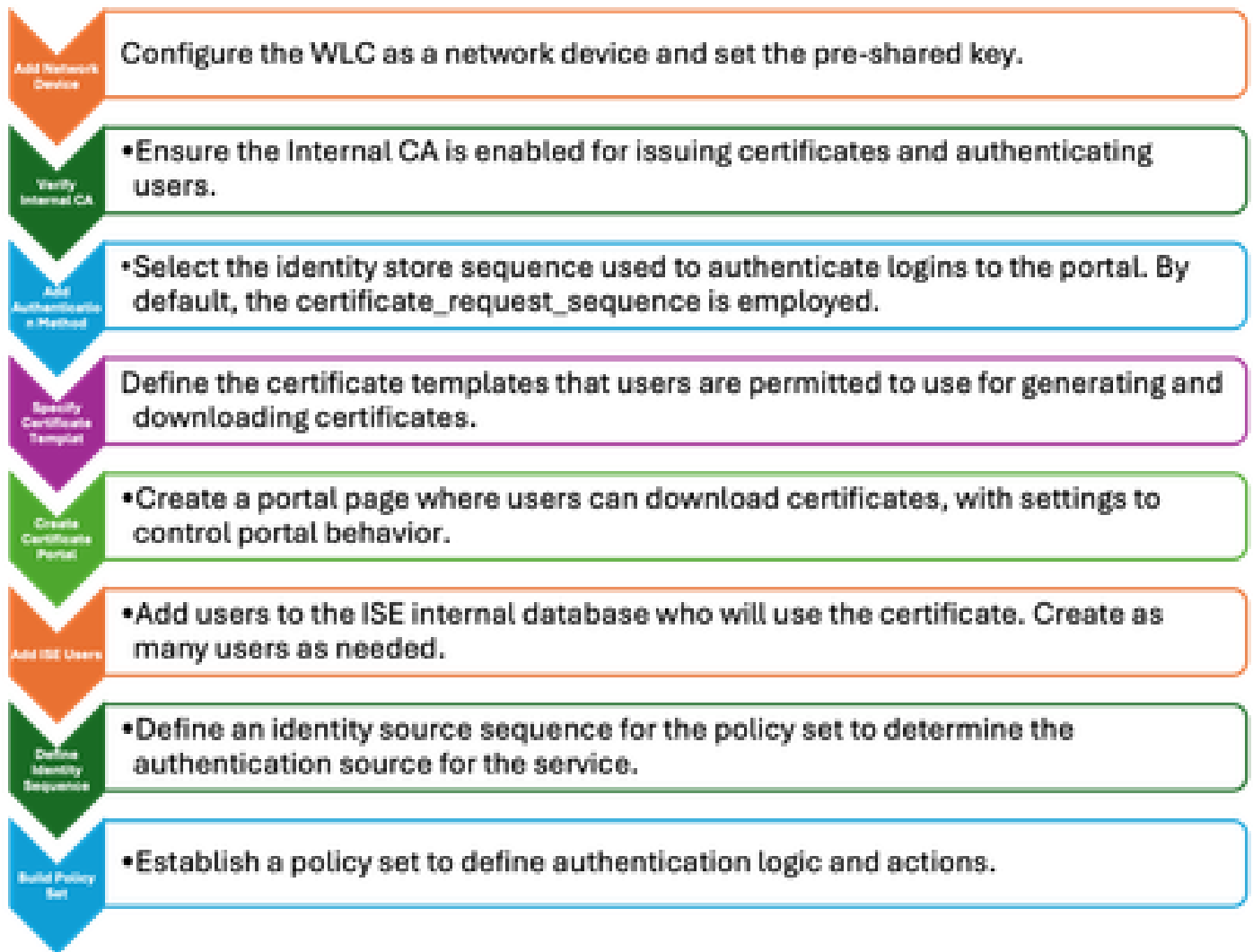
Topologie des travaux pratiques

Configurations

Dans cette section, nous configurons deux composants : ISE et WLC 9800.

Configuration ISE

Voici les étapes de configuration du serveur ISE. Chaque étape est accompagnée de captures d'écran dans cette section pour fournir une assistance visuelle.

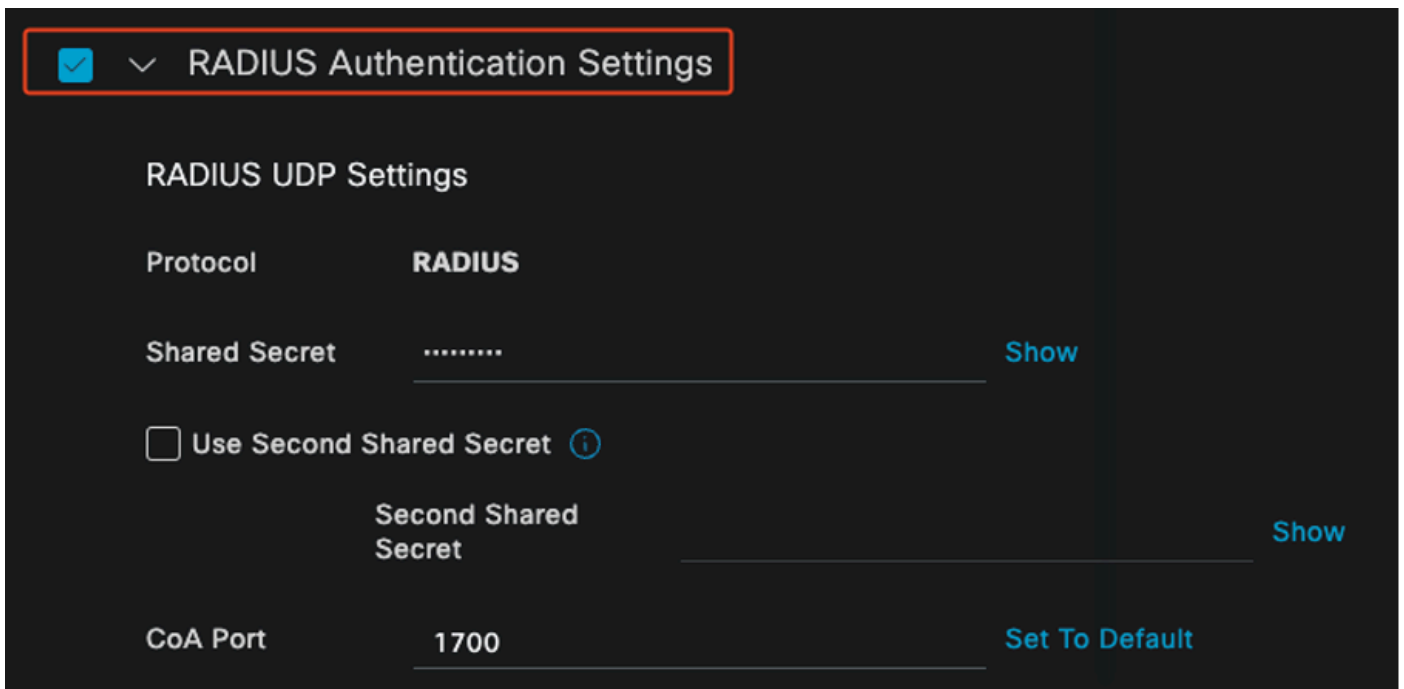


Étapes de configuration du serveur ISE

Ajout d'un périphérique réseau

Pour ajouter le contrôleur LAN sans fil (WLC) en tant que périphérique réseau, procédez comme suit :

1. Accédez à Administration > Network Resources > Network Devices.
2. Cliquez sur l'icône +Add pour lancer le processus d'ajout du WLC.
3. Assurez-vous que la clé pré-partagée correspond à la fois au WLC et au serveur ISE pour permettre une communication correcte.
4. Une fois que tous les détails sont correctement entrés, cliquez sur Submit dans le coin inférieur gauche pour enregistrer la configuration

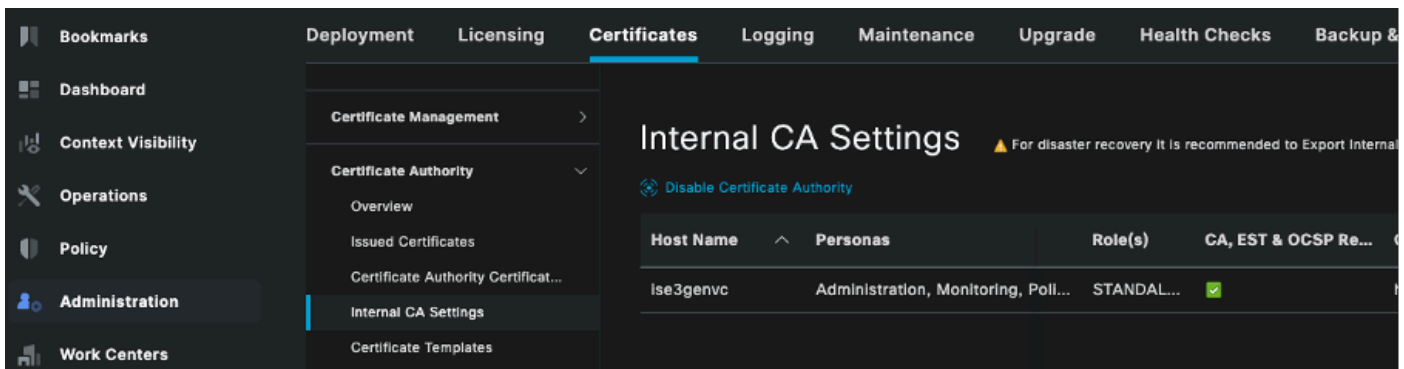


Ajout d'un périphérique réseau

Vérifier la CA interne

Pour vérifier les paramètres de l'autorité de certification interne, procédez comme suit :

1. Accédez à Administration > System > Certificates > Certificate Authority > Internal CA Settings.
2. Assurez-vous que la colonne CA est activée pour confirmer que la CA interne est active.



Vérifier la CA interne

Ajouter une méthode d'authentification

Accédez à Administration > Identity Management > Identity Source Sequences. Ajoutez une séquence d'identité personnalisée pour contrôler la source de connexion au portail.

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > Allow_EMP_Cert

Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile Preloaded_Certific

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	<input type="text" value="Internal Users"/>
Guest Users	
All_AD_Join_Points	

> < < >

Méthode d'authentification

Spécifier le modèle de certificat

Pour spécifier un modèle de certificat, procédez comme suit :

Étape 1. Accédez à Administration > System > Certificates > Certificate Authority > Certificate Templates.

Étape 2. Cliquez sur l'icône +Add pour créer un nouveau modèle de certificat :

2.1 Attribuez un nom unique local au serveur ISE pour le modèle.

2.2 Assurez-vous que le nom commun (CN) est défini sur \$UserName\$.

2.3 Vérifiez que le nom alternatif du sujet (SAN) est mappé à l'adresse MAC.

2.4 Définissez le profil d'autorité de certification SCEP sur CA interne ISE.

2.5 Dans la section d'utilisation de clé étendue, activez l'authentification client.

Field	Value
* Name	EAP_Authentication_Certificate_Template
Description	This template will be used to issue certificates for EAP Authentication
Subject	\$UserName\$
Common Name (CN)	\$UserName\$
Organizational Unit (OU)	Example unit
Organization (O)	Company name
City (L)	City
State (ST)	State
Country (C)	US
Subject Alternative Name (SAN)	MAC Address
Key Type	RSA
Key Size	2048
* SCEP RA Profile	ISE Internal CA
Valid Period	730 Day(s) (Valid Range 1 - 3652)
Extended Key Usage	<input checked="" type="checkbox"/> Client Authentication <input type="checkbox"/> Server Authentication

Modèle de certificat

Créer un portail de certificats

Pour créer un portail de certificats pour la génération de certificats client, procédez comme suit :

Étape 1. Accédez à Administration > Device Portal Management > Certificate Provisioning.

Étape 2. Cliquez sur Créer pour configurer une nouvelle page de portail.

Étape 3. Attribuez un nom unique au portail pour faciliter son identification.

3.1. Choisissez le numéro de port sur lequel le portail doit fonctionner ; définissez cette valeur sur 8443.

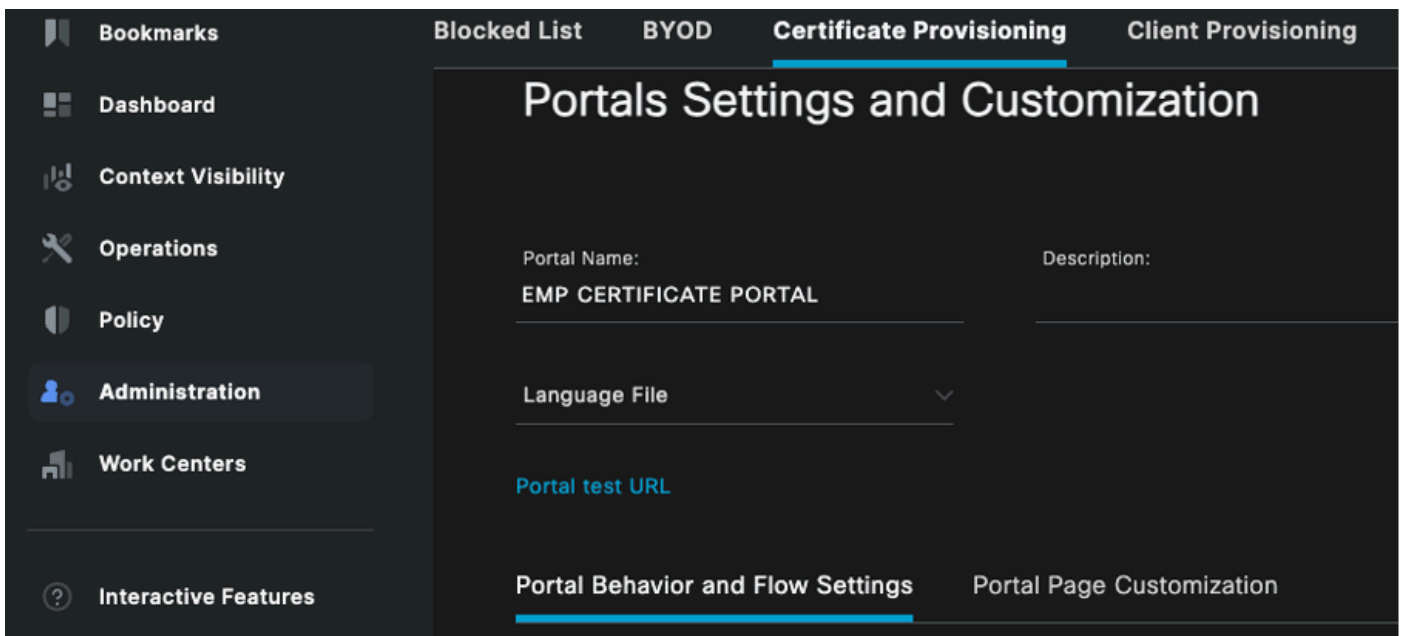
3.2. Spécifiez les interfaces sur lesquelles ISE écoute ce portail.

3.3. Sélectionnez la balise de groupe de certificats comme groupe de certificats du portail par défaut.

3.4. Sélectionnez la méthode d'authentification, qui indique la séquence de stockage d'identité utilisée pour authentifier la connexion à ce portail.

3.5. Inclure les groupes autorisés dont les membres peuvent accéder au portail. Par exemple, sélectionnez le groupe d'utilisateurs Employé si vos utilisateurs appartiennent à ce groupe.

3.6. Définissez les modèles de certificat qui sont autorisés dans les paramètres de mise en service de certificat.



Portal & Page Settings

Portal Settings

HTTPS port:*

1

8443

(8000 - 8999)

Allowed Interfaces:*

2

For PSNs Using Physical Interfaces

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3
- Gigabit Ethernet 4
- Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured

- Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
- Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
- Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: *

3

Default Portal Certificate Group

Configure certificates at:

[Administration > System > Certificates > System Certificates](#)

Authentication method: *

4

Certificate_Request_Sequence

Configure authentication methods at:

[Administration > Identity Management > Identity Source Sequences](#)

Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available

Q

- ALL_ACCOUNTS (default)
- GROUP_ACCOUNTS (default)
- OWN_ACCOUNTS (default)

Chosen

Employee

Choose all

Clear all

Fully qualified domain name (FQDN):

> Login Page Settings

> Acceptable Use Policy (AUP) Page Settings

> Post-Login Banner Page Settings

> Change Password Settings

∨ Certificate Portal Settings

Certificate Templates: *

EAP_Authentication_Certificate_Template × ∨

Configuration du portail de certificats

Une fois la configuration terminée, vous pouvez tester le portail en cliquant sur l'URL de test du portail. Cette action ouvre la page du portail.

Portals Settings and Customization

Portal Name:

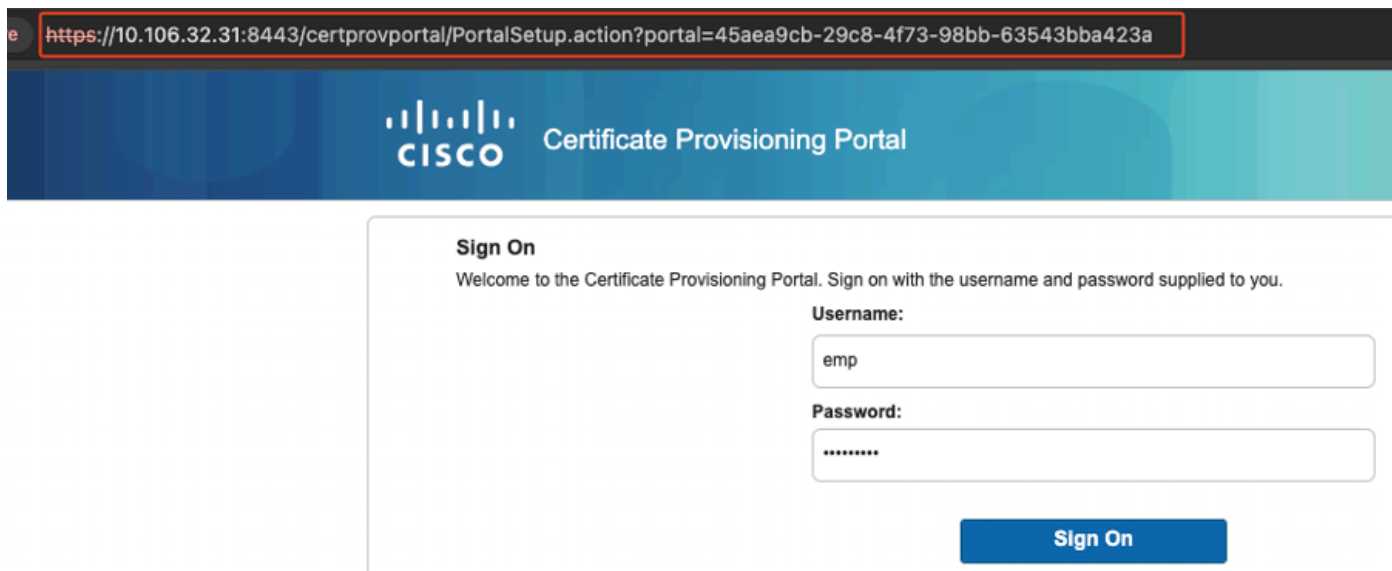
EMP CERTIFICATE PORTAL

Description:

Language File

Portal test URL

URL de la page Test Portal

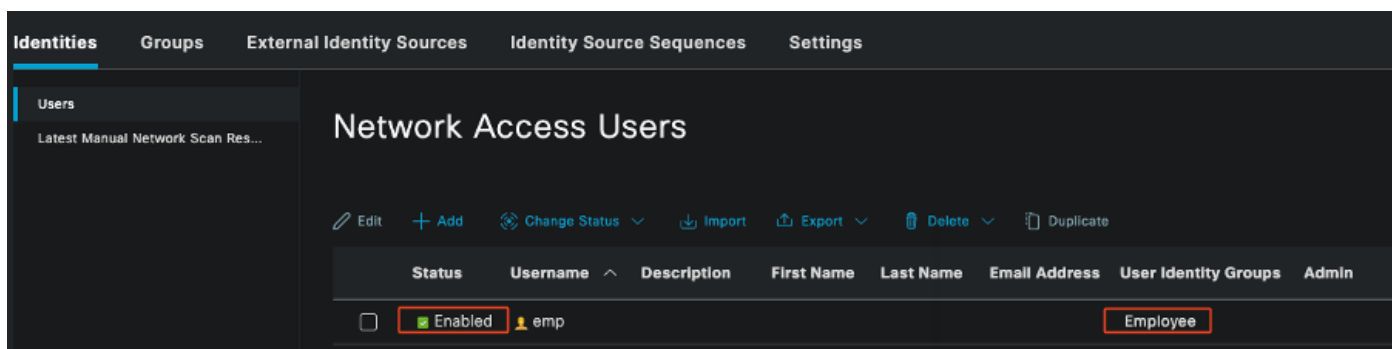


Page du portail

Ajouter un utilisateur interne

Pour créer un utilisateur pour l'authentification via le portail de certificats, procédez comme suit :

1. Accédez à Administration > Identity Management > Identities > Users.
2. Cliquez sur l'option pour ajouter un utilisateur au système.
3. Sélectionnez les groupes d'identités d'utilisateurs auxquels l'utilisateur appartient. Dans cet exemple, affectez l'utilisateur au groupe Employé.



Ajout d'un utilisateur interne

Configuration du portail d'approvisionnement de certificats ISE et de la stratégie RADIUS

La section précédente traitait de la configuration du portail de mise en service des certificats ISE. À présent, nous configurons les ensembles de stratégies ISE RADIUS pour autoriser l'authentification des utilisateurs.

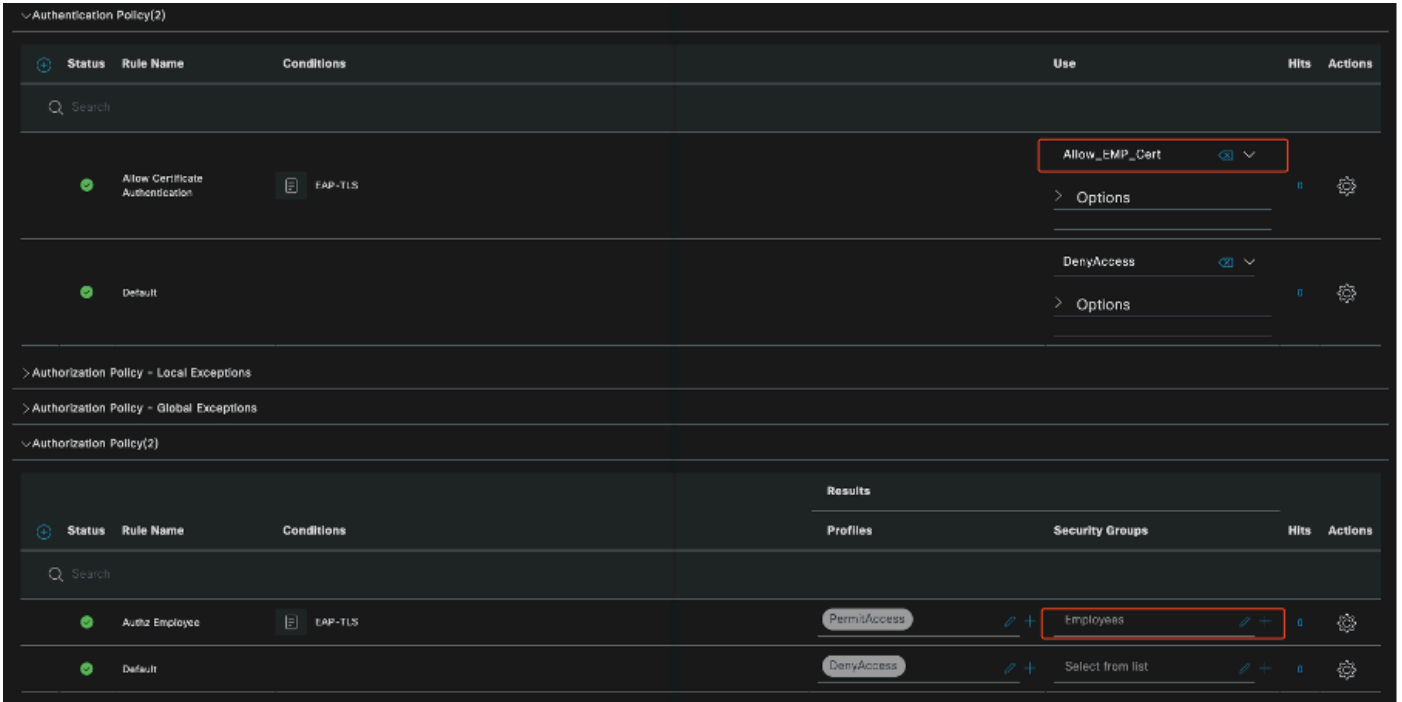
1. Configurer les ensembles de stratégies RADIUS ISE
2. Rendez-vous à Policy > Policy Sets (Politique > Ensembles de politiques).
3. Cliquez sur le signe plus (+) pour créer un nouveau jeu de stratégies.

Dans cet exemple, configurez un jeu de stratégies simple conçu pour authentifier les utilisateurs à

l'aide de leurs certificats.



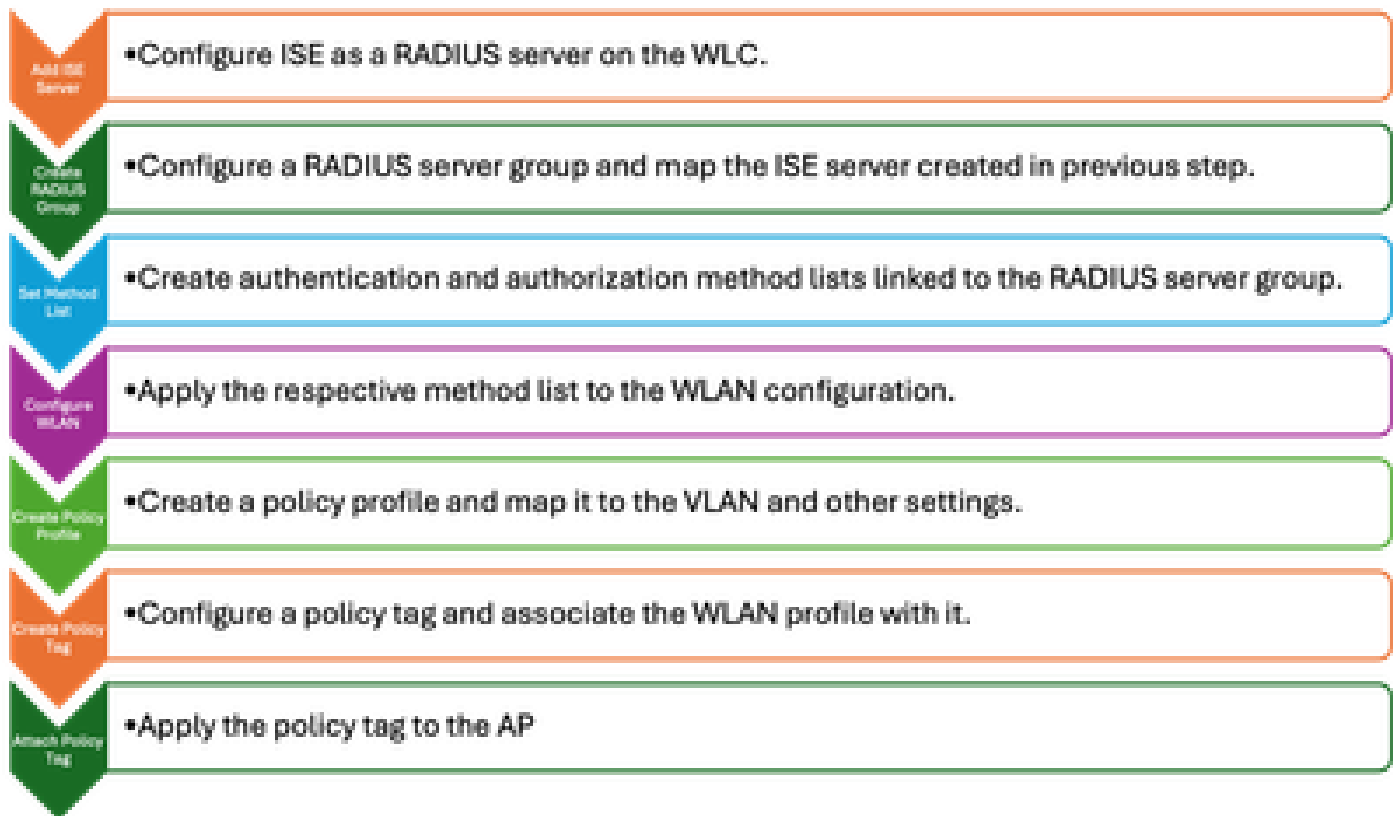
Ensemble de stratégies



Ensemble de stratégies affichant les stratégies d'authentification et d'autorisation

Configuration WLC 9800

Voici les étapes de configuration pour le WLC 9800. Chaque étape est accompagnée de captures d'écran dans cette section pour fournir une orientation visuelle.



Étapes de configuration WLC

Ajouter un serveur ISE au WLC 9800

1. Pour intégrer le serveur ISE au contrôleur LAN sans fil (WLC) 9800, procédez comme suit :
2. Accédez à Configuration > Security > AAA.
3. Cliquez sur le bouton Add pour inclure le serveur ISE dans la configuration WLC.

Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add Delete

RADIUS

TACACS+

LDAP

Create AAA Radius Server

Name* ISE3

Server Address* 10.106.32.31

PAC Key

Key Type Clear Text

Key*

Confirm Key*

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA ⓘ ENABLED

CoA Server Key Type Clear Text

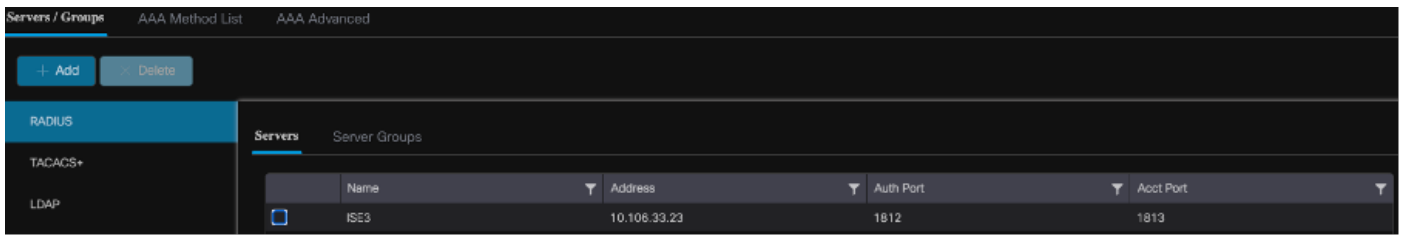
CoA Server Key ⓘ

Confirm CoA Server Key

Automate Tester

Ajout d'un serveur ISE dans le WLC

Une fois le serveur ajouté, il apparaît dans la liste des serveurs.

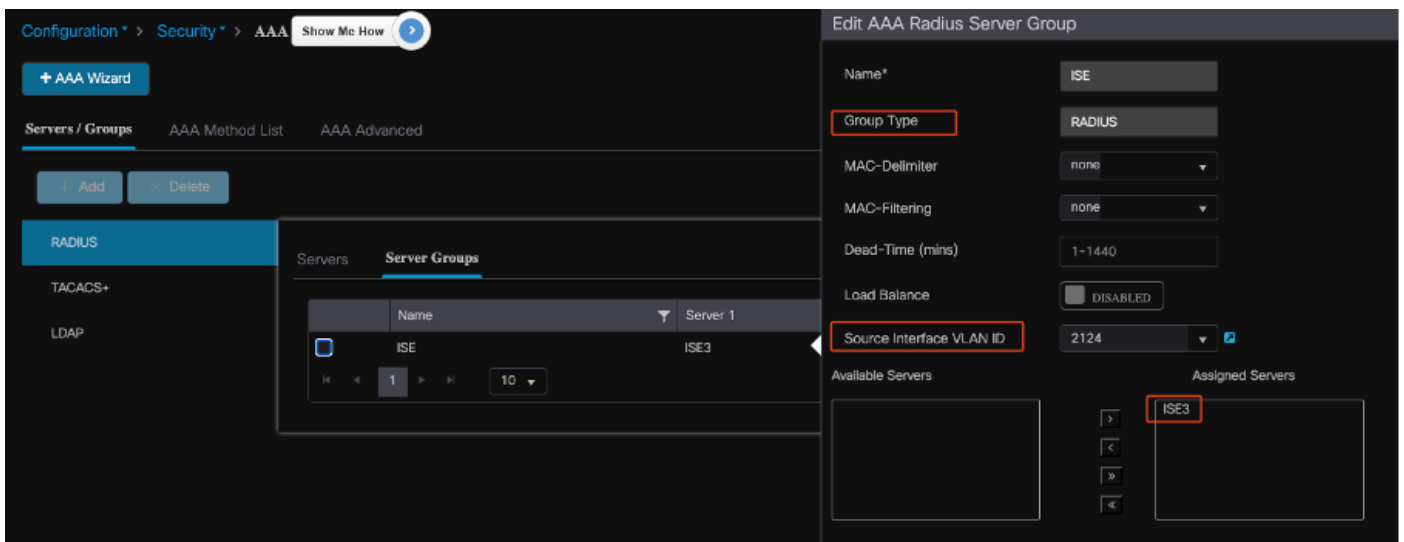


Affichage des serveurs Radius

Ajouter un groupe de serveurs sur le WLC 9800

Pour ajouter un groupe de serveurs sur le contrôleur LAN sans fil 9800, procédez comme suit :

1. Accédez à Configuration > Security > AAA.
2. Cliquez sur l'onglet Groupe de serveurs, puis sur Ajouter pour créer un nouveau groupe de serveurs.

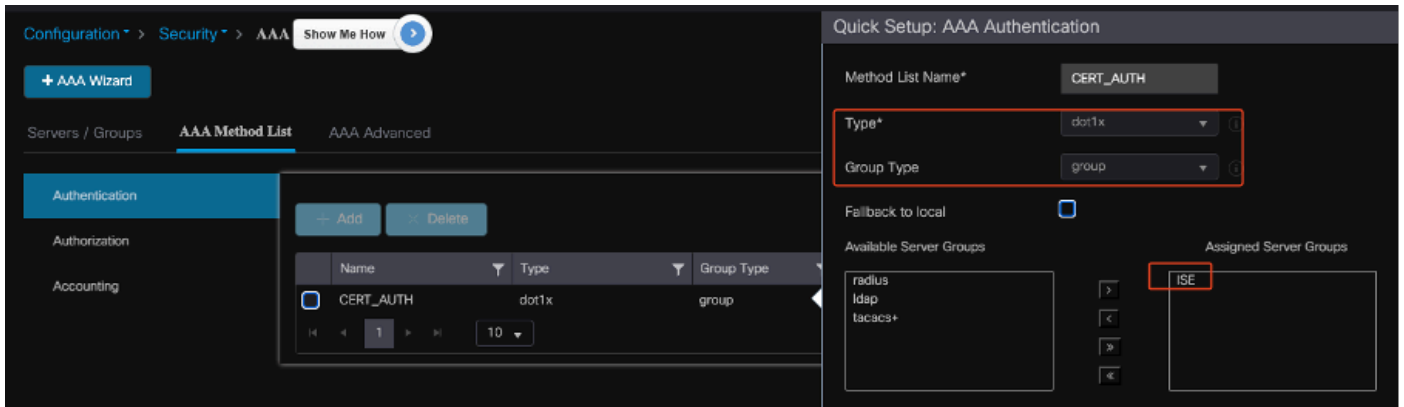


Mappage de serveurs ISE à un groupe de serveurs Radius

Configurer la liste de méthodes AAA sur le WLC 9800

Après avoir créé le groupe de serveurs, configurez la liste des méthodes d'authentification en procédant comme suit :

1. Accédez à Configuration > Security > AAA > AAA Method List.
2. Dans l'onglet Authentification, ajoutez une nouvelle liste de méthodes d'authentification.
3. Définissez le type sur dot1x.
4. Sélectionnez group comme type de groupe.
5. Incluez les groupes de serveurs ISE que vous avez créés précédemment en tant que groupes de serveurs.

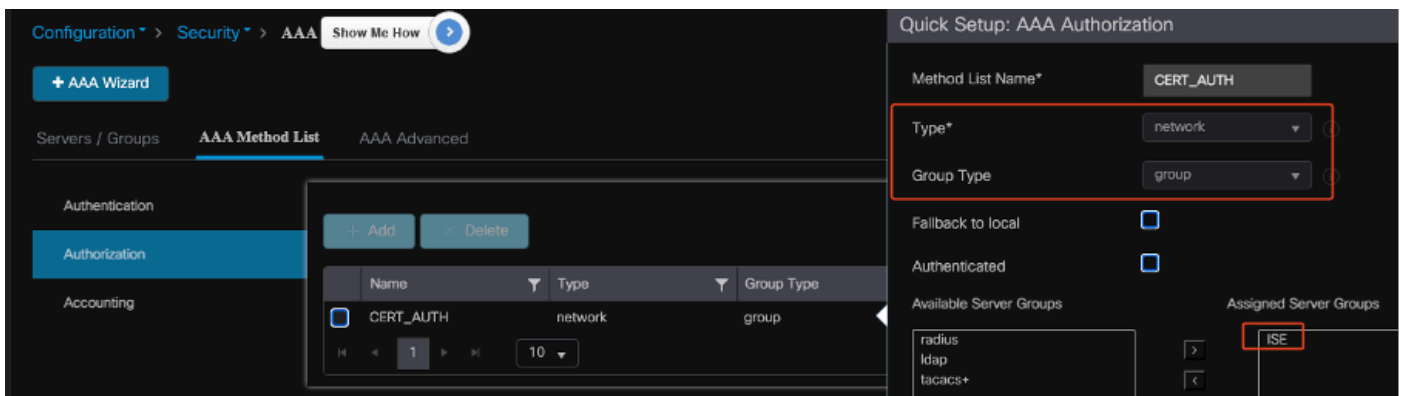


Création de listes de méthodes d'authentification

Configurer la liste des méthodes d'autorisation sur le WLC 9800

Pour configurer la liste des méthodes d'autorisation, procédez comme suit :

1. Accédez à l'onglet Autorisation dans la section Liste de méthodes AAA.
2. Cliquez sur Add pour créer une nouvelle liste de méthodes d'autorisation.
3. Sélectionnez network comme type.
4. Sélectionnez group comme type de groupe.
5. Incluez le groupe de serveurs ISE en tant que groupe de serveurs.

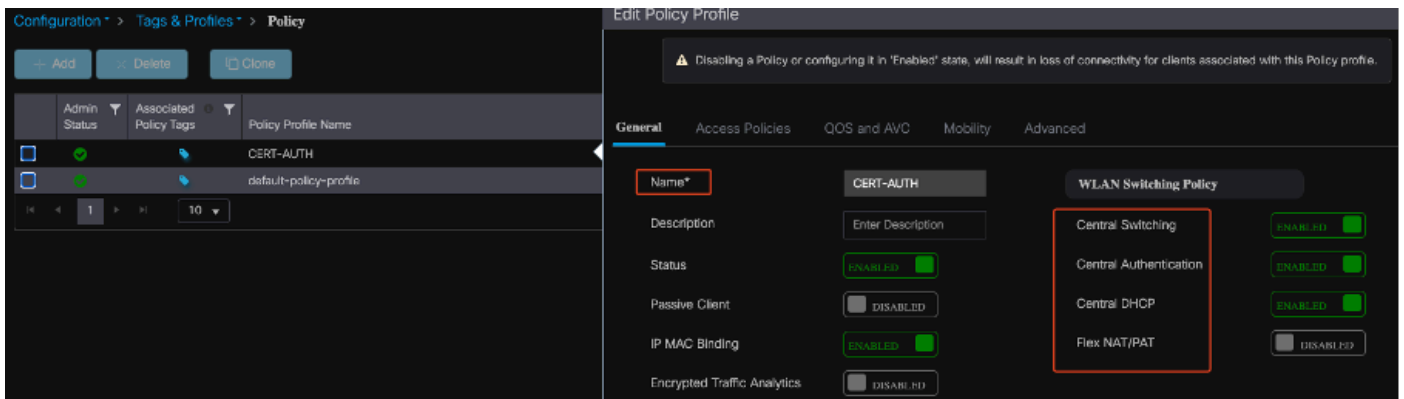


Ajout de la liste des méthodes d'autorisation

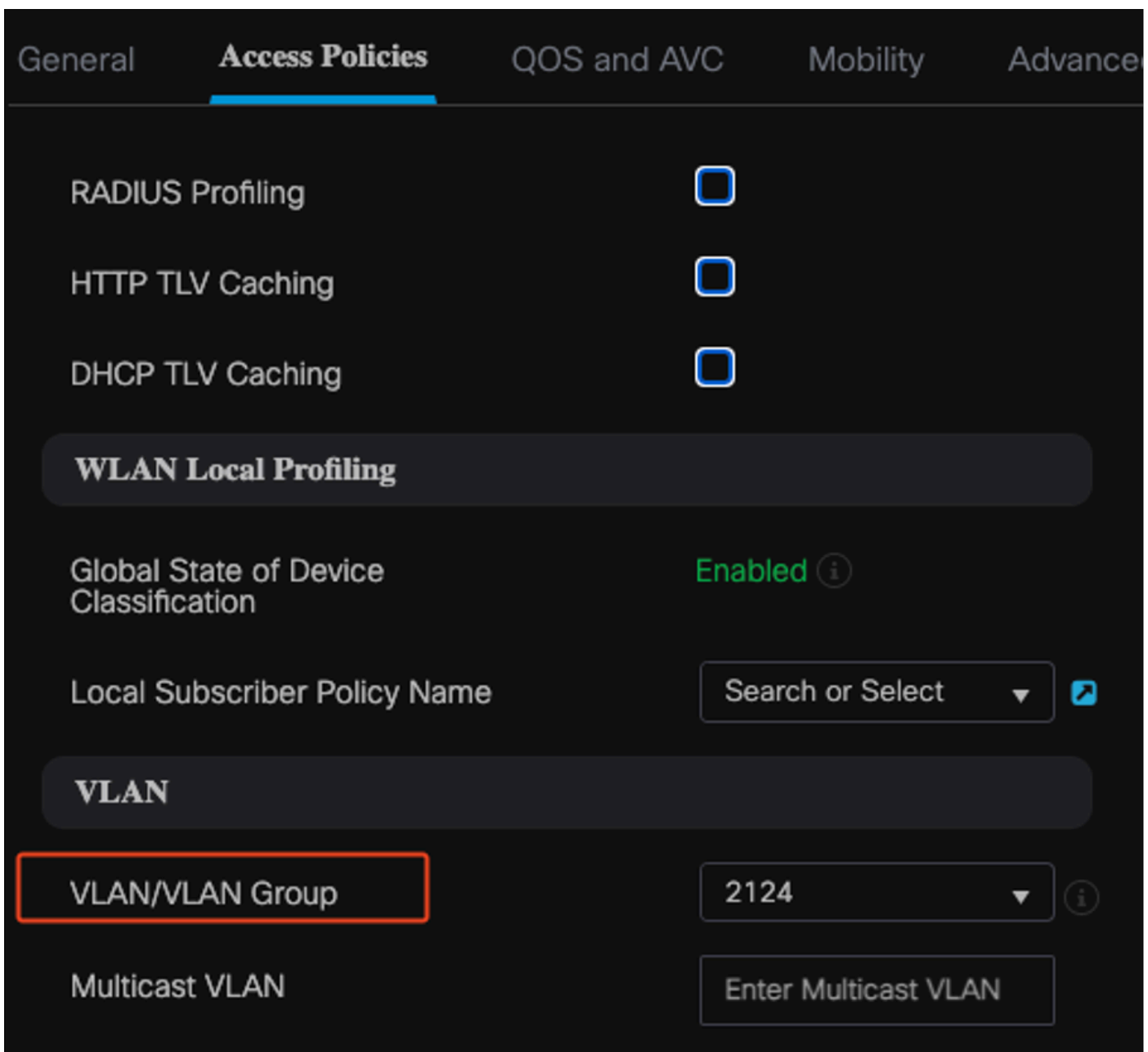
Créer un profil de stratégie sur le WLC 9800

Une fois la configuration du groupe RADIUS terminée, créez un profil de stratégie :

1. Accédez à Configuration > Tags & Profiles > Policy.
2. Cliquez sur Add pour créer un nouveau profil de stratégie.
3. Sélectionnez les paramètres appropriés pour votre profil de stratégie. Dans cet exemple, tout est central et le VLAN LAB est utilisé comme VLAN client.



Configuration du profil de stratégie



Mappage VLAN à stratégie

Lors de la configuration de l'autorisation RADIUS, assurez-vous que l'option AAA Override est activée dans l'onglet avancé des paramètres de profil de stratégie. Ce paramètre permet au

contrôleur de réseau local sans fil d'appliquer des stratégies d'autorisation basées sur RADIUS aux utilisateurs et aux périphériques.

The screenshot shows the 'Advanced' configuration tab for a WLAN. It is divided into three sections: 'WLAN Timeout', 'DHCP', and 'AAA Policy'. The 'WLAN Timeout' section includes fields for Session Timeout (1800), Idle Timeout (300), Idle Threshold (0), Client Exclusion Timeout (checked, 60), and Guest LAN Session Timeout (unchecked). The 'DHCP' section includes IPv4 DHCP Required (checked) and an empty DHCP Server IP Address field. The 'AAA Policy' section has 'Allow AAA Override' checked, which is highlighted with a red box. A 'Show more >>>' link is visible between the DHCP and AAA Policy sections.

Section	Parameter	Value
WLAN Timeout	Session Timeout (sec)	1800
	Idle Timeout (sec)	300
	Idle Threshold (bytes)	0
	Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> 60
	Guest LAN Session Timeout	<input type="checkbox"/>
DHCP	IPv4 DHCP Required	<input checked="" type="checkbox"/>
	DHCP Server IP Address	
AAA Policy	Allow AAA Override	<input checked="" type="checkbox"/>

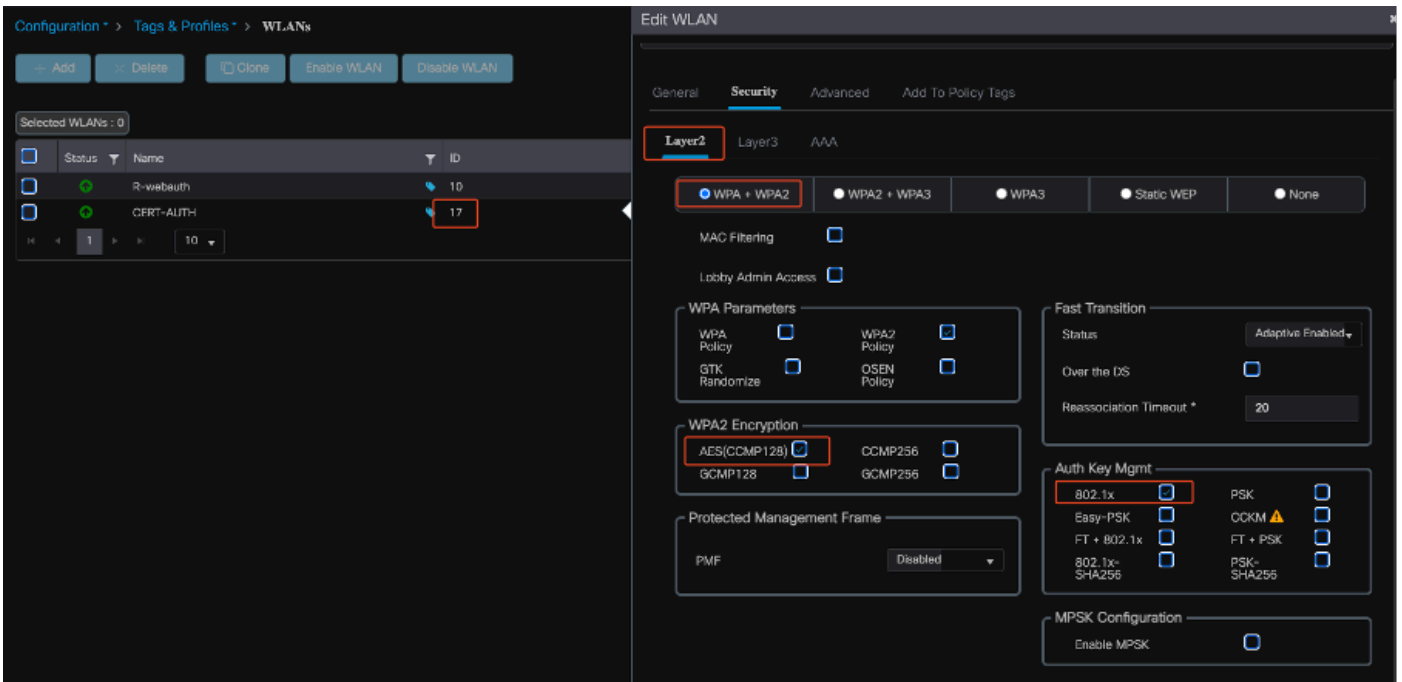
Remplacement AAA

Créer un WLAN sur le WLC 9800

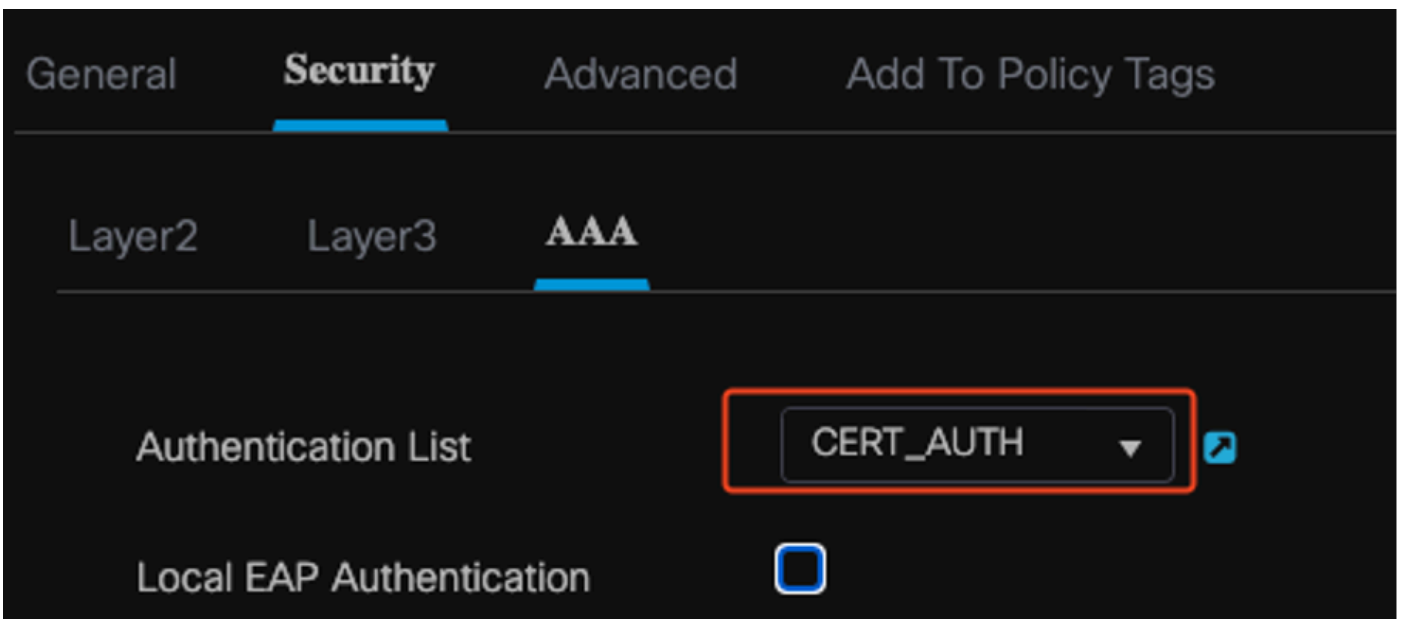
Pour configurer un nouveau WLAN avec l'authentification 802.1x, procédez comme suit :

1. Accédez à Configuration > Tags & Profiles > WLANs.
2. Cliquez sur Add pour créer un nouveau WLAN.

3. Sélectionnez les paramètres d'authentification de couche 2 et activez l'authentification 802.1x.



Configuration du profil WLAN

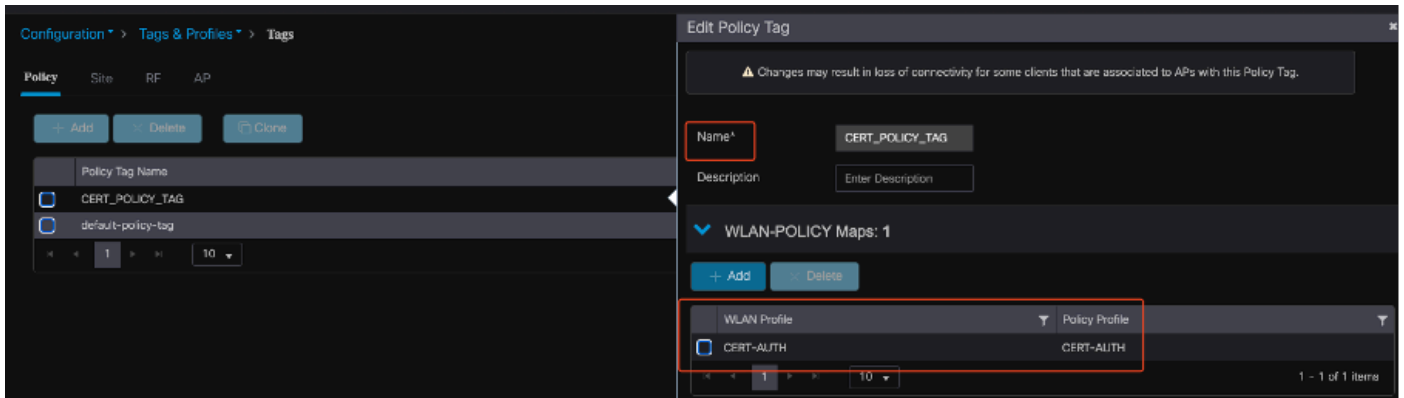


Profil WLAN vers carte de liste de méthodes

Mappage du WLAN avec le profil de stratégie sur le WLC 9800

Pour associer votre WLAN à un profil de stratégie, procédez comme suit :

1. Accédez à Configuration > Tags & Profiles > Tags.
2. Cliquez sur Add pour ajouter une nouvelle balise.
3. Dans la section WLAN-POLICY, mappez le WLAN nouvellement créé au profil de stratégie approprié.

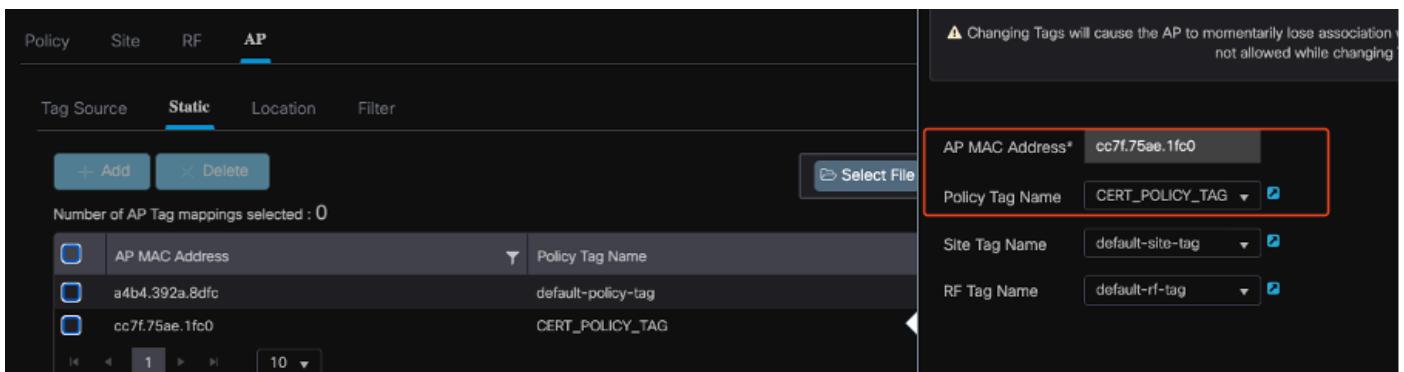


Configuration des balises des politiques

Mapper la balise de stratégie au point d'accès sur le WLC 9800

Pour attribuer la balise de stratégie à un point d'accès (AP), procédez comme suit :

1. Accédez à Configuration > Tags & Profiles > Tags > AP.
2. Accédez à la section Static dans la configuration AP.
3. Cliquez sur le point d'accès spécifique que vous souhaitez configurer.
4. Attribuez la balise de stratégie que vous avez créée au point d'accès sélectionné.



Attribution de balise AP

Exécution de la configuration du WLC après la fin de l'installation

```

aaa group server radius ISE
 server name ISE3
 ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
 client 10.106.32.31 server-key Cisco!123
!
```

```

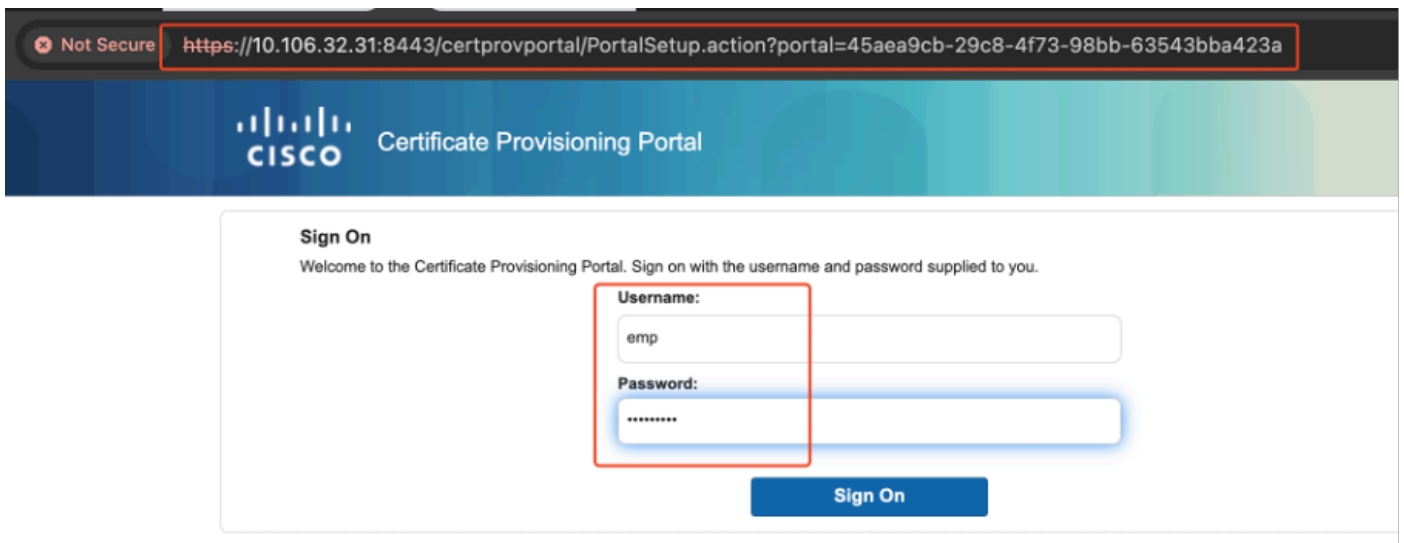
wireless profile policy CERT-AUTH
aaa-override
 ipv4 dhcp required
 vlan 2124
 no shutdown
 wlan CERT-AUTH policy CERT-AUTH
 wlan CERT-AUTH 17 CERT-AUTH
```

```
security dot1x authentication-list CERT_AUTH
no shutdown
!
wireless tag policy CERT_POLICY_TAG
wlan CERT-AUTH policy CERT-AUTH
```

Créer et télécharger un certificat pour l'utilisateur

Pour créer et télécharger un certificat pour un utilisateur, procédez comme suit :

1. Demandez à l'utilisateur de se connecter au portail de certificats qui a été configuré précédemment.



The screenshot shows a web browser window with the address bar displaying `https://10.106.32.31:8443/certprovportal/PortalSetup.action?portal=45aea9cb-29c8-4f73-98bb-63543bba423a`. The page header features the Cisco logo and the text "Certificate Provisioning Portal". The main content area is titled "Sign On" and includes the message: "Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you." Below this message are two input fields: "Username:" with the value "emp" and "Password:" with masked characters "*****". A blue "Sign On" button is positioned below the password field.

Accès au portail de certificats

2. Acceptez la politique d'utilisation acceptable (AUP). L'ISE présente ensuite une page pour la génération de certificats.

3. Sélectionnez Générer un certificat unique (sans demande de signature de certificat).

Certificate Provisioning

I want to: *

Generate a single certificate (without a certificat... ▼

Common Name (CN): *

emp

MAC Address: *

242f.d0da.a563

Choose Certificate Template: *

EAP_Authentication_Certificate_Template ▼

Description:

Certificate Download Format: *

PKCS12 format, including certificate chain (... ▼

Certificate Password: *

Enter password to download and view/install the certificate

Confirm Password: *

Generate

Reset

Génération du certificat

Pour générer un certificat via le portail d'approvisionnement de certificats, assurez-vous que les champs obligatoires suivants sont remplis :

- CN : Le serveur d'authentification utilise la valeur présentée dans le champ Nom commun du certificat client pour authentifier un utilisateur. Dans le champ Nom commun, saisissez le nom d'utilisateur (que vous avez utilisé pour vous connecter au portail d'approvisionnement de certificats).
- Adresse MAC : Subject Alternative Names (SAN) est une extension X.509 qui permet d'associer diverses valeurs à un certificat de sécurité. Cisco ISE, version 2.0 prend uniquement en charge les adresses MAC. Par conséquent, dans le champ d'adresse SAN/MAC.
 - Modèle de certificat : Le modèle de certificat définit un ensemble de champs que

l'autorité de certification utilise lors de la validation d'une demande et de l'émission d'un certificat. Des champs tels que le nom commun (CN) sont utilisés pour valider la demande (CN doit correspondre au nom d'utilisateur). D'autres champs sont utilisés par l'autorité de certification lors de l'émission du certificat.

- Mot de passe du certificat : Vous avez besoin d'un mot de passe de certificat pour sécuriser votre certificat. Vous devez fournir le mot de passe du certificat pour afficher le contenu du certificat et pour importer le certificat sur un périphérique.
- Votre mot de passe doit respecter les règles suivantes :
- Le mot de passe doit contenir au moins 1 lettre majuscule, 1 lettre minuscule et 1 chiffre
 - Le mot de passe doit comporter entre 8 et 15 caractères
 - Les caractères autorisés sont A-Z, a-z, 0-9, _, #

Une fois que tous les champs sont remplis, sélectionnez Generate pour créer et télécharger le certificat.

Installation de certificat sur un ordinateur Windows 10

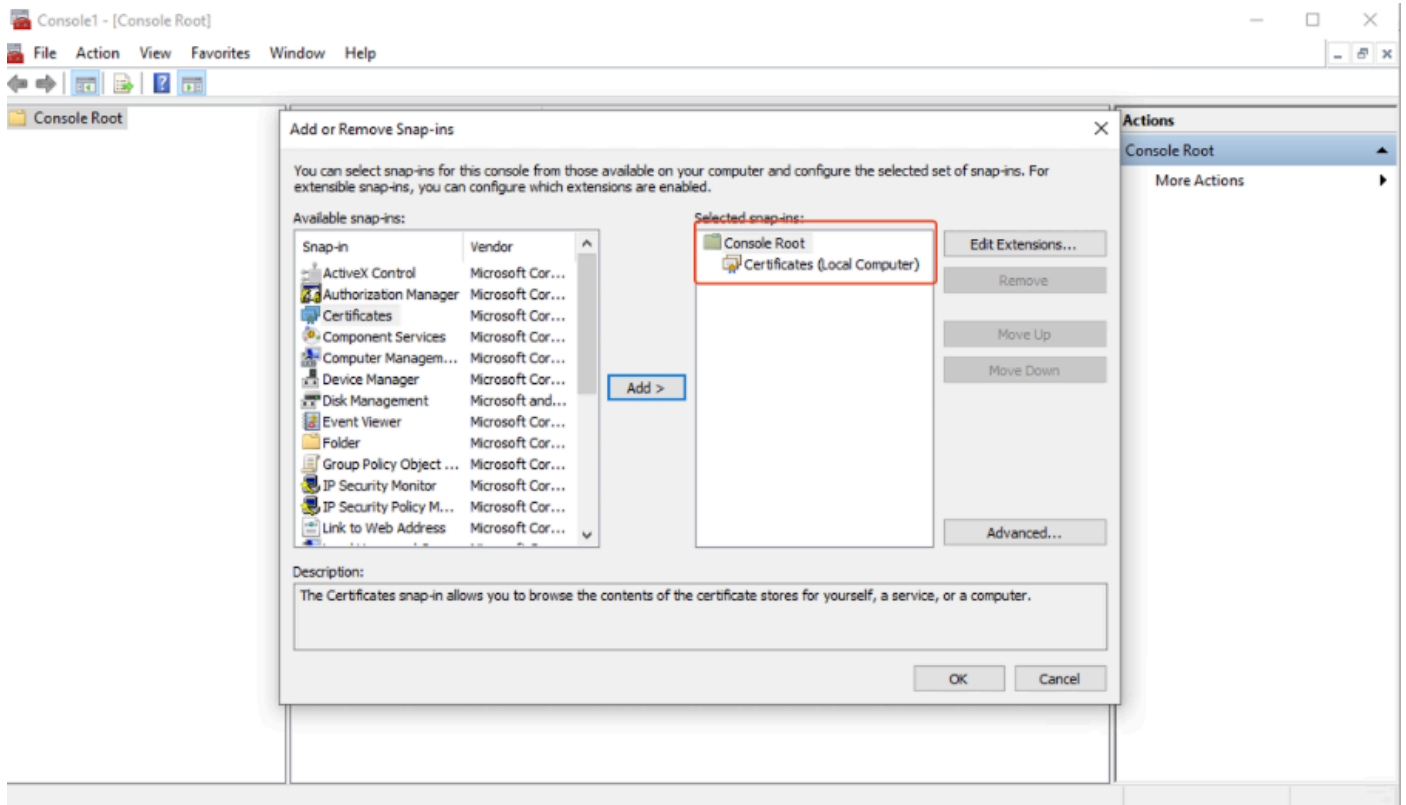
Pour installer un certificat sur un ordinateur Windows 10, ouvrez la console MMC (Microsoft Management Console) en procédant comme suit :



Remarque : Ces instructions peuvent varier en fonction de votre installation de Windows. Nous vous recommandons donc de consulter la documentation Microsoft pour obtenir des détails spécifiques.

-
1. Cliquez sur Démarrer, puis sur Exécuter.
 2. Tapez mmc dans la zone Run et appuyez sur Entrée. Microsoft Management Console s'ouvre.
 3. Ajouter un composant logiciel enfichable de certificat :
 4. Accédez à Fichier > Ajouter/Supprimer un composant logiciel enfichable.
 5. Sélectionnez Add, puis choisissez Certificates et cliquez sur Add.
 6. Sélectionnez Compte d'ordinateur, puis Ordinateur local, puis cliquez sur Terminer.

Ces étapes vous permettent de gérer les certificats sur votre ordinateur local.




Console MMC Windows

Étape 1. Importez le certificat :

- 1.1. Cliquez sur Action dans le menu.
- 1.2. Accédez à Toutes les tâches, puis sélectionnez Importer.
- 1.3. Passez en revue les invites pour localiser et sélectionner le fichier de certificat stocké sur votre ordinateur.



←  Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\admin\Desktop\emp-2025-01-06_08-30-59\emp_C4-E9-0

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX, .P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Next

Cancel

Importation du certificat

Au cours du processus d'importation de certificat, vous êtes invité à entrer le mot de passe que vous avez créé lors de la génération du certificat sur le portail. Assurez-vous que vous entrez ce mot de passe correctement pour importer et installer le certificat sur votre ordinateur.

← Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

●●●●●●●●●●

Display Password

Import options:

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

Protect private key using virtualized-based security(Non-exportable)

Include all extended properties.

Next Cancel

Saisie du mot de passe du certificat

Étape 2. Déplacer les certificats vers les dossiers appropriés :

2.1. Ouvrez Microsoft Management Console (MMC) et accédez au dossier Certificats (Ordinateur local) > Personal.

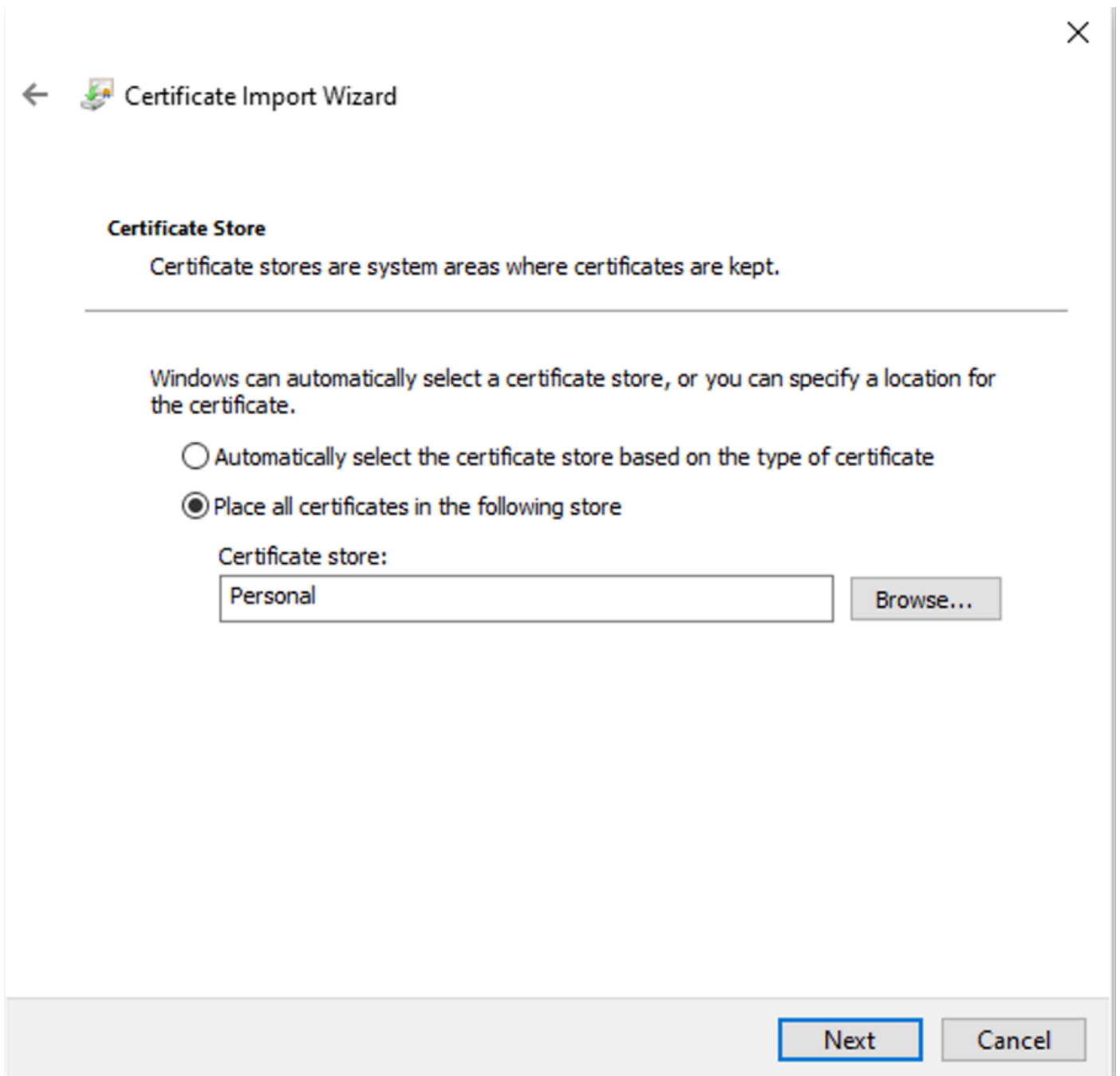
2.2. Examinez les certificats et déterminez leur type (par exemple, Autorité de certification racine, Autorité de certification intermédiaire ou Personnel).

2.3. Déplacer chaque certificat vers le magasin approprié :

2.4. Certificats d'autorité de certification racine : Passer aux autorités de certification racine de confiance.

2.5. Certificats d'autorité de certification intermédiaires : Passer aux autorités de certification intermédiaires.

2.6. Certificats personnels : Laissez dans le dossier Personnel.



Stockage des certificats dans le dossier personnel

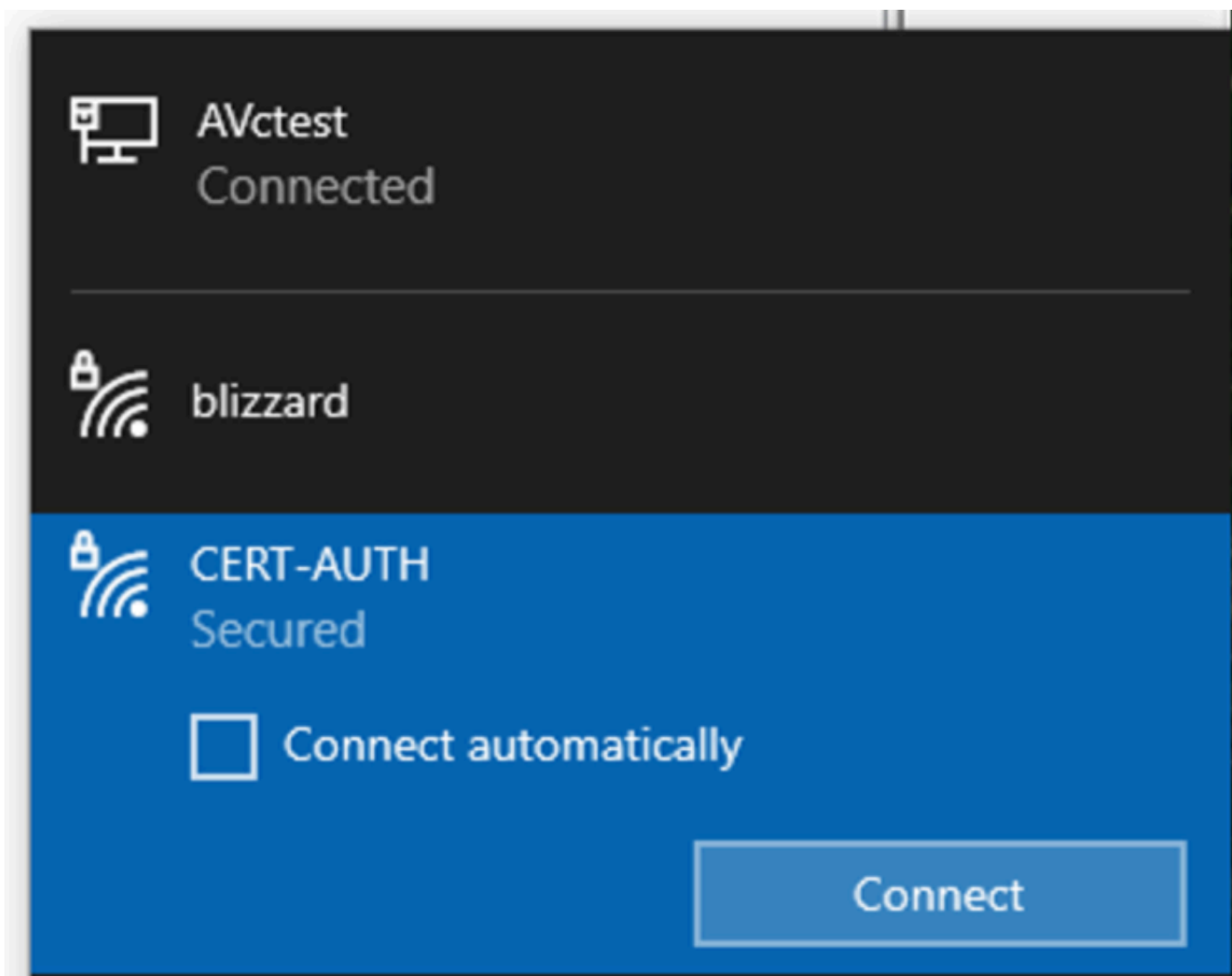
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Stat.
Certificate Services Endpoint Sub CA - ise3genvc	Certificate Services Node CA - ise3genvc	1/3/2035	<All>	EndpointSubCA	
Certificate Services Node CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate_nodeCA	
Certificate Services Root CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate	
emp	Certificate Services Endpoint Sub CA - ise3genvc	1/6/2027	Client Authentication	emp_CA-E9-0A-00-...	
ise3genvc.lab.local	ise3genvc.lab.local	1/3/2027	Server Authentication, Client Authentication	Self-Signed	

Déplacement de certificats dans leurs magasins

Connexion de l'ordinateur Windows

Une fois les certificats déplacés vers les magasins appropriés, procédez comme suit pour vous connecter au WLAN :

1. Cliquez sur l'icône network dans la barre d'état système pour afficher les réseaux sans fil disponibles.
2. Recherchez et cliquez sur le nom du WLAN auquel vous souhaitez vous connecter.
3. Cliquez sur Connect et poursuivez avec toutes les invites supplémentaires pour terminer le processus de connexion en utilisant votre certificat pour l'authentification.



Connexion au réseau sans fil

Lorsque vous y êtes invité pendant le processus de connexion au WLAN, sélectionnez l'option Connect using a certificate.



CERT-AUTH

Secured

Enter your user name and password

Connect using a certificate

OK

Cancel

Utilisation du certificat comme informations d'identification

Cela vous permet de vous connecter au réseau sans fil à l'aide du certificat.

```
C:\>netsh wlan show interface
```

```
There is 1 interface on the system:
```

```
Name : Wi-Fi 3
Description : TP-Link Wireless USB Adapter
GUID : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
Physical address : 24:2f:d0:da:a5:63
State : connected
SSID : CERT-AUTH
BSSID : a4:88:73:9e:8d:af
Network type : Infrastructure
Radio type : 802.11ac
Authentication : WPA2-Enterprise
Cipher : CCMP
Connection mode : Profile
Channel : 36
Receive rate (Mbps) : 360
Transmit rate (Mbps) : 360
Signal : 100%
Profile : CERT-AUTH
```

```
Hosted network status : Not available
```

```
C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
```

```
EAP type : Microsoft: Smart Card or other certificate
```

Vérification du profil sans fil

Vérifier

Vérifiez que le WLAN est diffusé par le WLC :

```
<#root>
```

```
POD6_9800#show wlan summ
```

```
Number of WLANs: 2
```

```
ID Profile Name SSID Status Security
```

```
-----
```

```
17
```

```
CERT-AUTH
```

```
CERT-AUTH
```

```
UP [WPA2][802.1x][AES]
```

Vérifiez que le point d'accès est actif sur le WLC :


```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-----
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

Assurez-vous que le point d'accès diffuse le WLAN :

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
-----
17 a488.739e.8da0
```

```
POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
-----
17
a488.739e.8daf
```

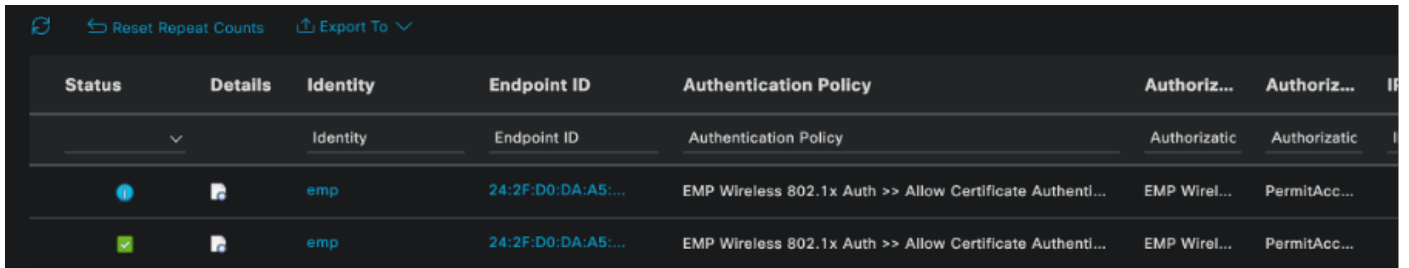
Client connecté via EAP-TLS :

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----
242f.d0da.a563 AP1 WLAN
17
IP Learn 11ac
Dot1x
Local
POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
Wireless LAN Network Name (SSID): CERT-AUTH
BSSID : a488.739e.8daf
EAP Type : EAP-TLS
VLAN : 2124
Multicast VLAN : 0
```

VLAN : 2124

Journaux en direct Cisco Radius ISE :



The screenshot shows a table of authentication logs from Cisco ISE. The table has columns for Status, Details, Identity, Endpoint ID, Authentication Policy, and Authoriz... (Authorization). Two entries are visible, both for the identity 'emp' and endpoint ID '24:2F:D0:DA:A5:...'. The first entry has a status of 'i' (info) and the second has a status of '✓' (success). Both entries show the authentication policy 'EMP Wireless 802.1x Auth >> Allow Certificate Authenti...' and authorization 'EMP Wire...' and 'PermitAcc...'.

Status	Details	Identity	Endpoint ID	Authentication Policy	Authoriz...	Authoriz...
i		emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wire...	PermitAcc...
✓		emp	24:2F:D0:DA:A5:...	EMP Wireless 802.1x Auth >> Allow Certificate Authenti...	EMP Wire...	PermitAcc...

Journaux en direct ISE Radius

Type d'authentification détaillé :

Authentication Details

Source Timestamp	2025-01-08 11:58:21.055
Received Timestamp	2025-01-08 11:58:21.055
Policy Server	ise3genvc
Event	5200 Authentication succeeded
Username	emp
Endpoint Id	24:2F:D0:DA:A5:63
Calling Station Id	24-2f-d0-da-a5-63
Endpoint Profile	TP-LINK-Device
Identity Group	User Identity Groups:Employee,Profiled
Audit Session Id	4D084E0A0000007E46F0C6F7
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	lab-9800
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.78.8.77
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccess
Security Group	Employees

Journaux détaillés ISE

Capture EPC WLC montrant les paquets EAP-TLS :

No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLsv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLsv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLsv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLsv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

Capture WLC montrant la transaction EAP

- Le paquet numéro 87 correspond à l'étape 8 du flux EAP-TLS décrit au début du document.
- Le paquet numéro 115 correspond à l'étape 9 du flux EAP-TLS décrit au début du document.
- Le paquet numéro 118 correspond à l'étape 10 du flux EAP-TLS décrit au début du document.

Suivi Radio Active (RA) montrant la connexion client : Cette trace RA est filtrée pour afficher quelques-unes des lignes pertinentes de la transaction d'authentification.

```

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (debug)
Envoi d'un message DTLS chiffré. Adresse IP dest 10.78.8.78[5256], longueur 499
2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Envoyer une
demande d'accès à 10.106.33.23 1812 id 0/25, len 390
2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Reçu de l'id
1812/25 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11.58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL envoyé - Version 3,EAPOL Type EAP, Payload Length 6,
EAP-Type = EAP-TLS
2025/01/08 11.58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL reçu - Version 1,EAPOL Type EAP, Payload Length 204,
EAP-Type = EAP-TLS
2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Envoyer une
demande d'accès à 10.106.33.23 1812 id 0/26, len 663
2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Reçu de l'id
1812/26 10.106.33.23 0, Access-Challenge, len 1135
2025/01/08 11.58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL envoyé - Version 3,EAPOL Type EAP, Payload Length 1012,
EAP-Type = EAP-TLS
2025/01/08 11.58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL reçu - Version 1,EAPOL Type EAP, Payload Length 6, EAP-
Type = EAP-TLS
2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Envoyer une
demande d'accès à 10.106.33.23 1812 id 0/27, len 465
2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Reçu de l'id
1812/27 10.106.33.23 0, Access-Challenge, len 1131
2025/01/08 11.58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563

```

capwap_90800005] Paquet EAPOL envoyé - Version 3,EAPOL Type EAP, Payload Length 1008, EAP-Type = EAP-TLS
2025/01/08 11.58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL reçu - Version 1,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Envoyer une demande d'accès à 10.106.33.23 1812 id 0/28, len 465
2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Reçu de l'id 1812/28 10.106.33.23 0, Access-Challenge, len 275
2025/01/08 11.58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL envoyé - Version 3,EAPOL Type EAP, Payload Length 158, EAP-Type = EAP-TLS
2025/01/08 11.58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL reçu - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-Type = EAP-TLS
2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Envoyer une demande d'accès à 10.106.33.23 1812 id 0/29, len 1961
2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Reçu de l'id 1812/29 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11.58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL envoyé - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11.58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL reçu - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-Type = EAP-TLS
2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Envoyer une demande d'accès à 10.106.33.23 1812 id 0/30, len 1961
2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Reçu de l'id 1812/30 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11.58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL envoyé - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11.58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL reçu - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-Type = EAP-TLS
2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Envoyer une demande d'accès à 10.106.33.23 1812 id 0/31, len 1961
2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Reçu de l'id 1812/31 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11.58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL envoyé - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11.58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563
capwap_90800005] Paquet EAPOL reçu - Version 1,EAPOL Type EAP, Payload Length 247, EAP-Type = EAP-TLS
2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Envoyer une

demande d'accès à 10.106.33.23 1812 id 0/32, len 706

2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Reçu de l'id 1812/32 10.106.33.23 0, Access-Challenge, len 174

2025/01/08 11.58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Paquet EAPOL envoyé - Version 3,EAPOL Type EAP, Payload Length 57, EAP-Type = EAP-TLS

2025/01/08 11.58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Paquet EAPOL reçu - Version 1,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS

2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Envoyer une demande d'accès à 10.106.33.23 1812 id 0/33, len 465

2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Reçu de l'id 1812/33 10.106.33.23 0, Access-Accept, len 324

2025/01/08 11.58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Événement de mise à jour d'identité déclenché pour la méthode EAP EAP-TLS

Dépannage

Il n'existe pas d'étapes de dépannage spécifiques pour ce problème en dehors des procédures de dépannage sans fil 802.1x standard :

1. Effectuez les débogages de trace RA du client pour vérifier le processus d'authentification.
2. Effectuez une capture EPC WLC pour examiner les paquets entre le client, le WLC et le serveur RADIUS.
3. Vérifiez les journaux en direct ISE pour vous assurer que la demande correspond à la stratégie appropriée.
4. Vérifiez sur le point de terminaison Windows que le certificat est correctement installé et que la chaîne d'approbation complète est présente.

Références

- [FAQ sur le portail d'approvisionnement des certificats, version 3.2](#)
- [Comprendre les services ISE internes des autorités de certification](#)
- [Comprendre et configurer EAP-TLS avec un WLC et ISE](#)

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.