Configuration du WLC Catalyst 9800 avec authentification LDAP pour 802.1X et Web-auth

Contenu

Introduction

Ce document décrit comment configurer un Catalyst 9800 afin d'authentifier les clients avec un serveur LDAP comme base de données pour les identifiants d'utilisateur.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Serveurs Microsoft Windows
- Active Directory ou toute autre base de données LDAP

Components Used

C9800 EWC sur point d'accès C9100 qui exécute Cisco IOS®-XE version 17.3.2a

Serveur Microsoft Active Directory (AD) avec stockage d'accès réseau (NAS) QNAP qui agit comme base de données LDAP

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.

Configurer LDAP avec un SSID Webauth

Diagramme du réseau

Cet article a été écrit sur la base d'une configuration très simple :

Un point d'accès EWC AP 9115 avec IP 192.168.1.15

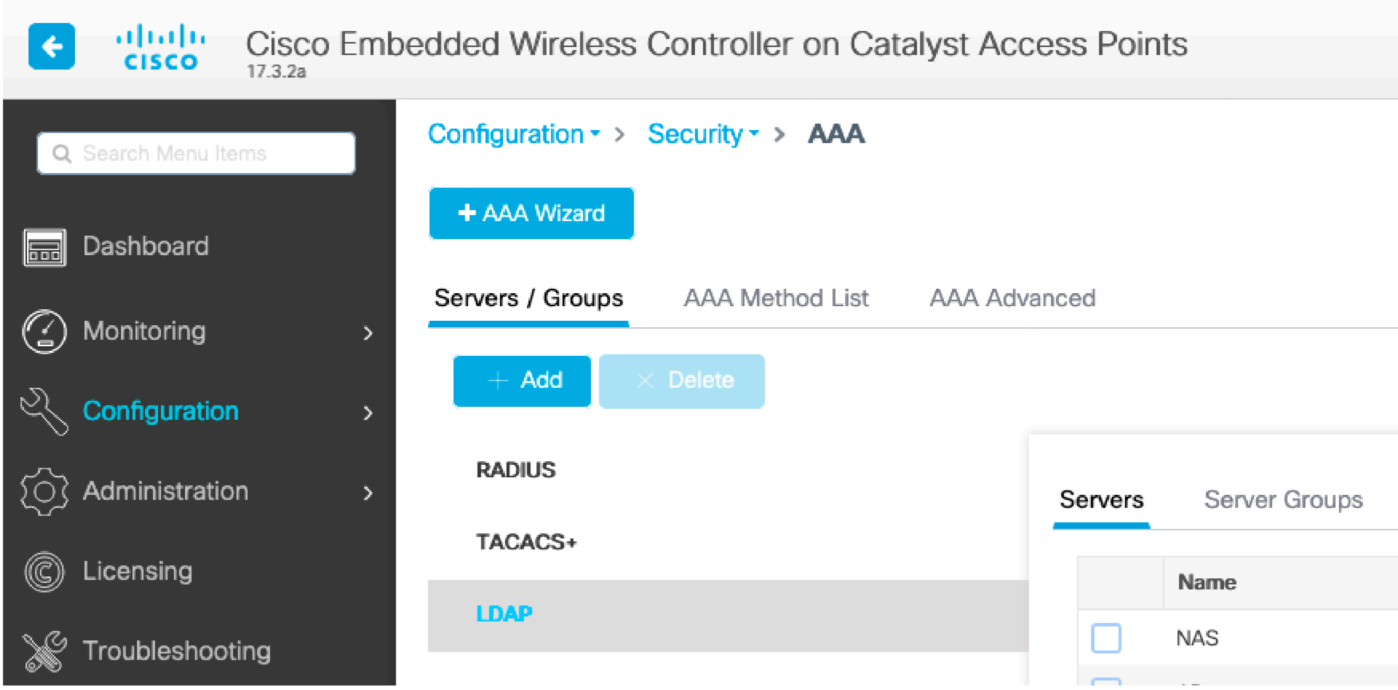
Un serveur Active Directory avec IP 192.168.1.192

Client qui se connecte au point d'accès interne du CEE

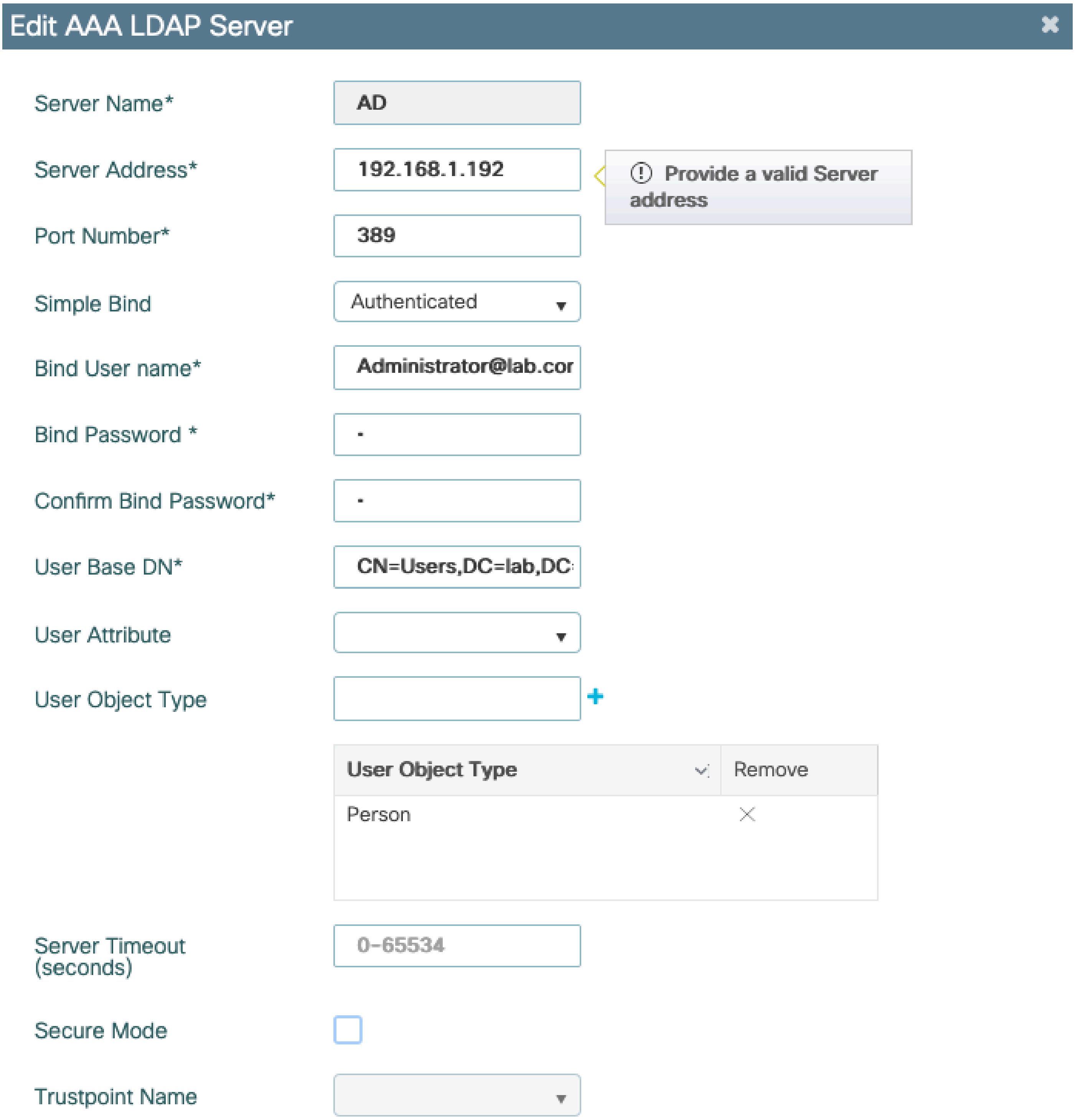
Configurer le contrôleur

Étape 1 : configuration du serveur LDAP

Accédez à **Configuration > Security > AAA> Servers/Groups > LDAP** et cliquez sur **+ Add**



Choisissez un nom pour votre serveur LDAP et renseignez les détails. Pour obtenir des explications sur chaque champ, reportez-vous à la section « Comprendre les détails du serveur LDAP » de ce document.



Edit AAA LDAP Server

Server Name*	AD
Server Address*	192.168.1.192
Port Number*	389
Simple Bind	Authenticated
Bind User name*	Administrator@lab.cor
Bind Password *	•
Confirm Bind Password*	•
User Base DN*	CN=Users,DC=lab,DC:
User Attribute	
User Object Type	
Server Timeout (seconds)	0-65534
Secure Mode	□
Trustpoint Name	

Provide a valid Server address

User Object Type	Remove
Person	×

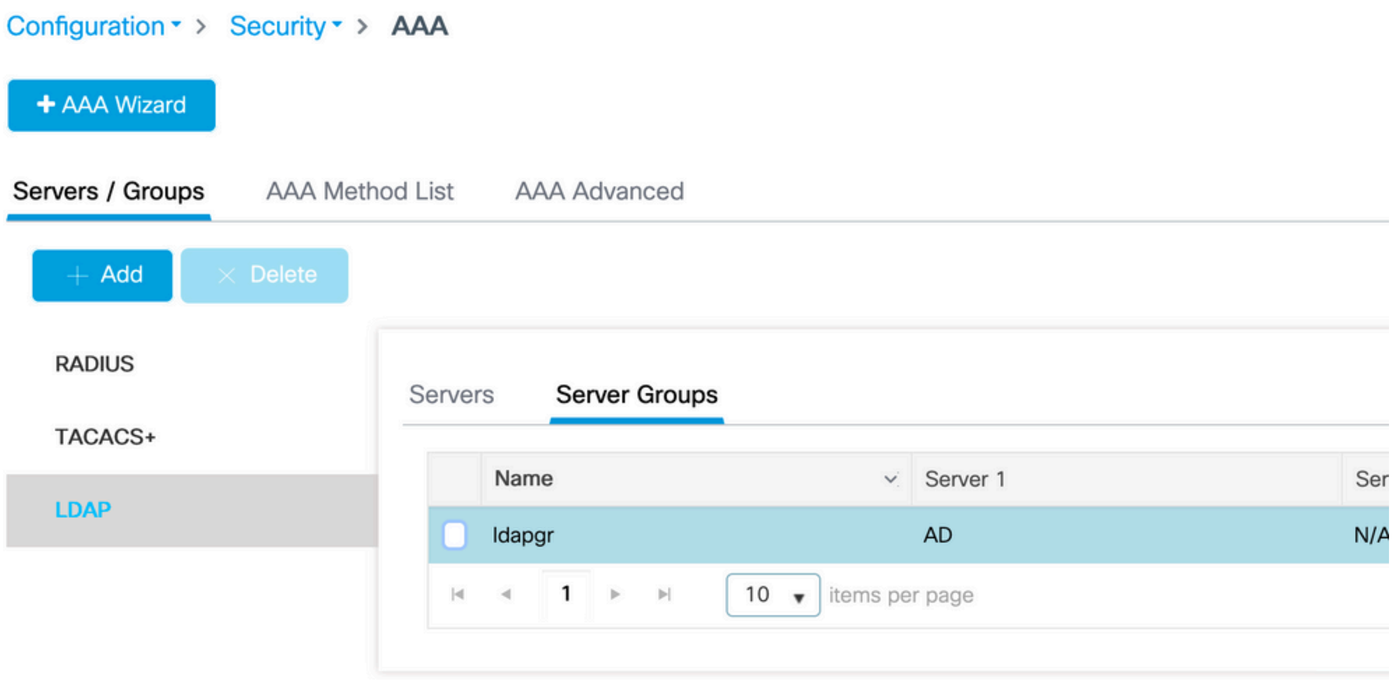
Enregistrer en cliquant sur **Mettre à jour et appliquer au périphérique**

Commandes CLI :

```
ldap server AD ipv4 192.168.1.192 bind authenticate root-dn Administrator@lab.com password 6
WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB base-dn CN=Users,DC=lab,DC=com search-filter user-object-type
Person
```

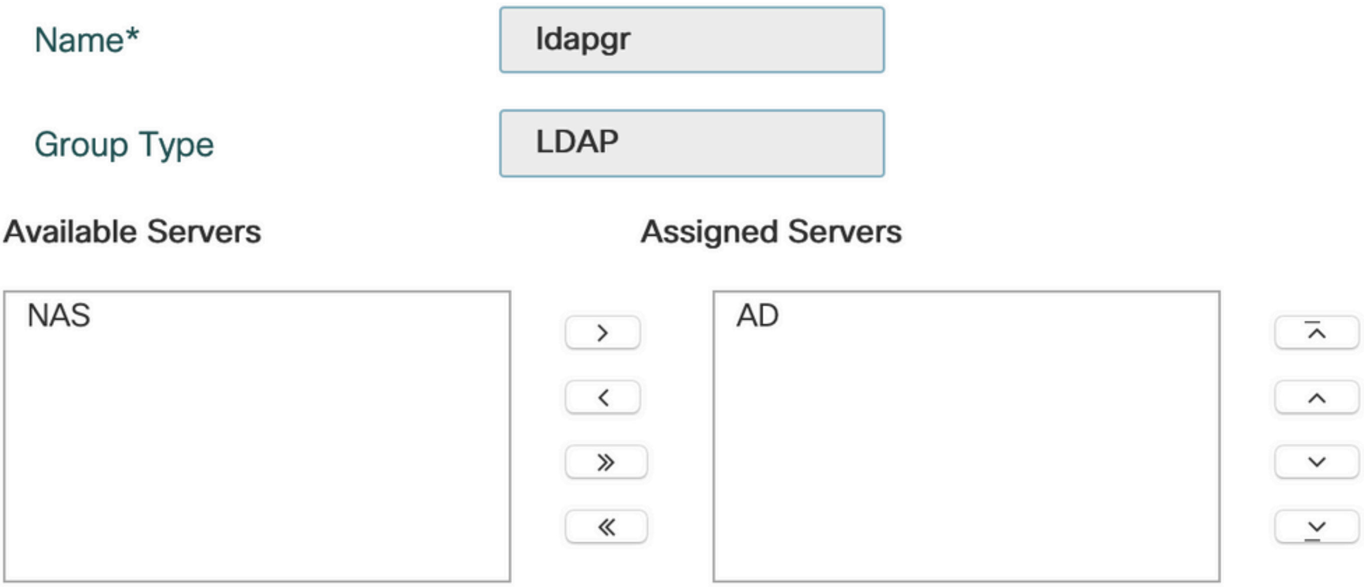
Étape 2 : configuration d’un groupe de serveurs LDAP

Accédez à **Configuration > Security > AAA > Servers/ Groups > LDAP > Server Groups** et cliquez sur **+ADD**



	Name	Server 1	Ser
□	ldapgr	AD	N/A

Entrez un nom et ajoutez le serveur LDAP que vous avez configuré à l'étape précédente.



Name*	ldapgr
Group Type	LDAP

Available Servers	Assigned Servers
NAS	AD

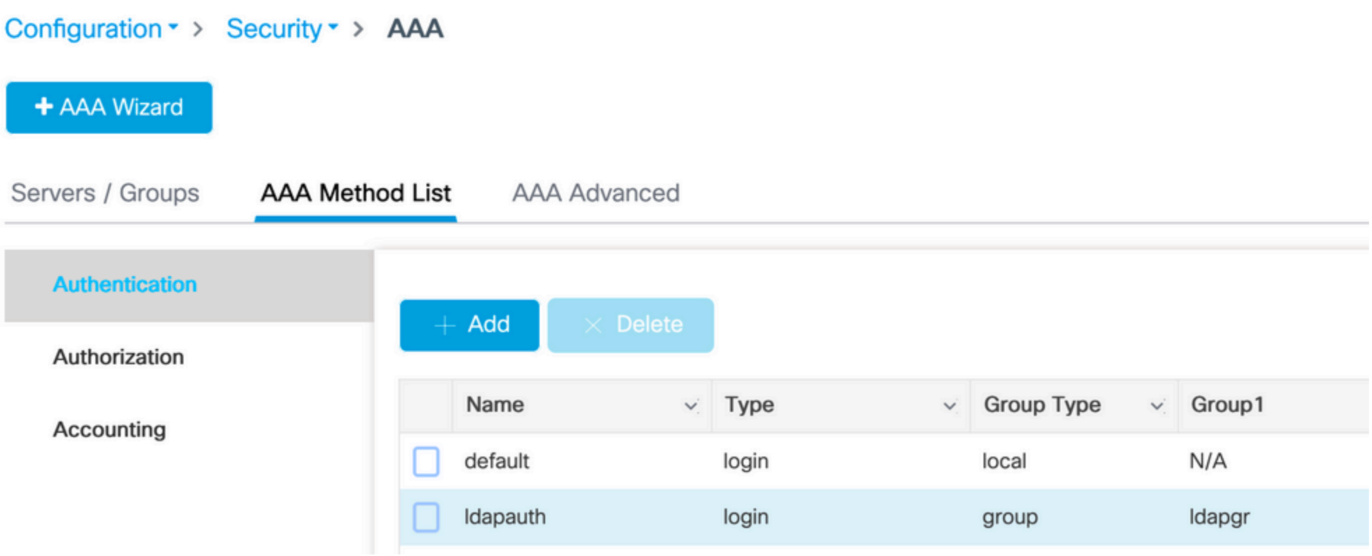
Cliquez sur **Mettre à jour et appliquer** pour enregistrer.

Commandes CLI :

```
aaa group server ldap ldapgr server AD
```

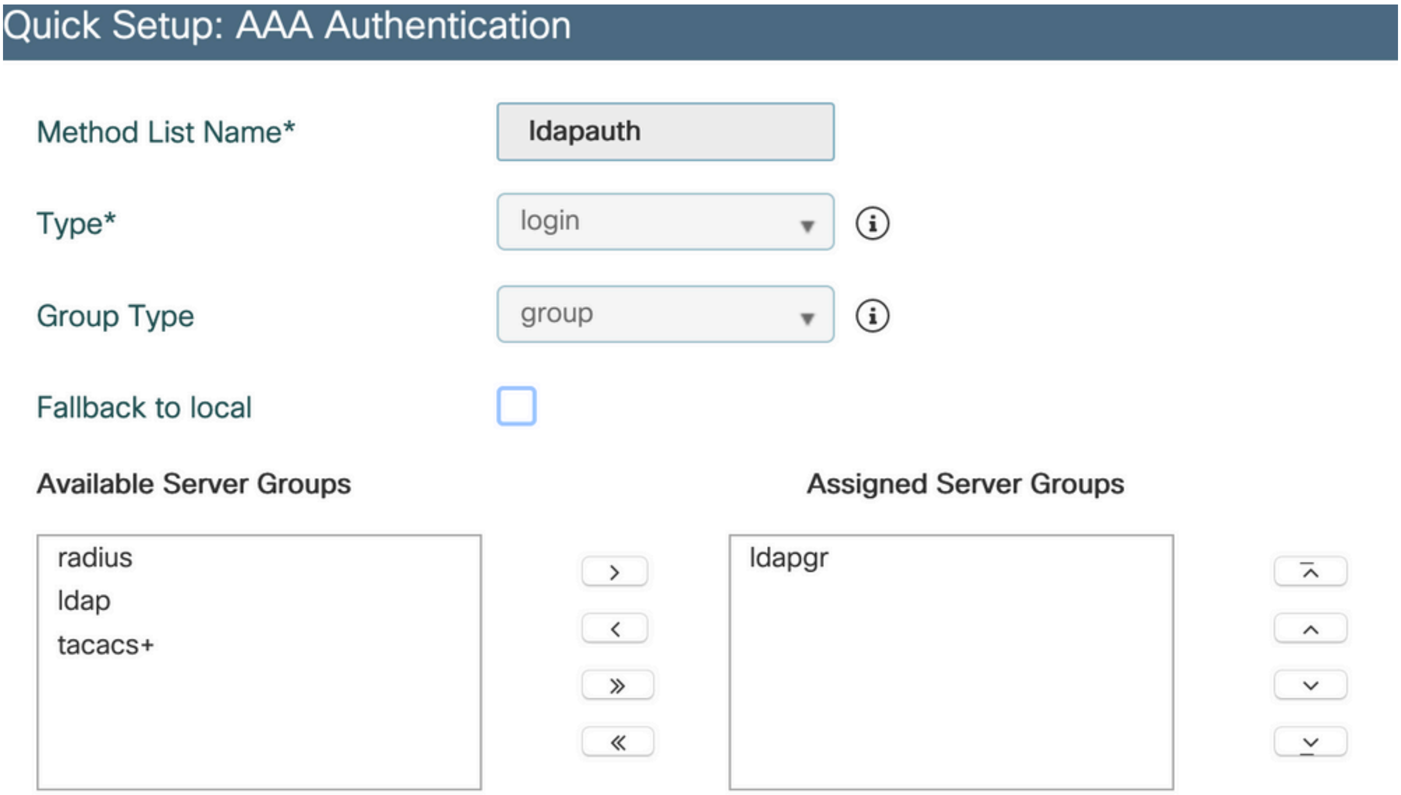
Étape 3 : configuration de la méthode d’authentification AAA

Accédez à **Configuration > Security > AAA > AAA method List > Authentication** et cliquez sur **+Add**



	Name	Type	Group Type	Group1
□	default	login	local	N/A
□	ldapauth	login	group	ldapgr

Entrez un nom, choisissez le type de **connexion** et pointez sur le groupe de serveurs LDAP configuré précédemment.



Method List Name* : ldapauth

Type* : login

Group Type : group

Fallback to local : □

Available Server Groups : radius, ldap, tacacs+

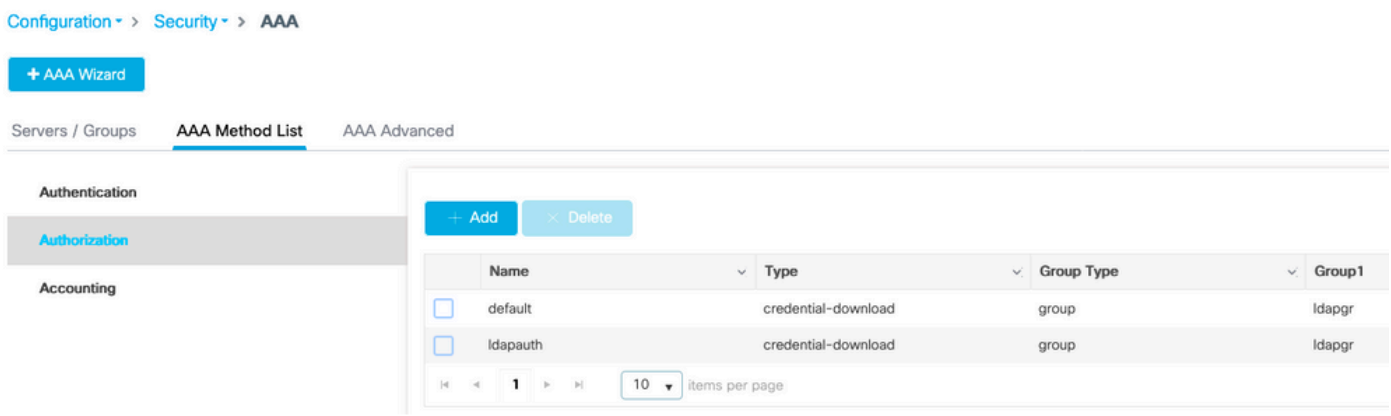
Assigned Server Groups : ldapgr

Commandes CLI :

```
aaa authentication login ldapauth group ldapgr
```

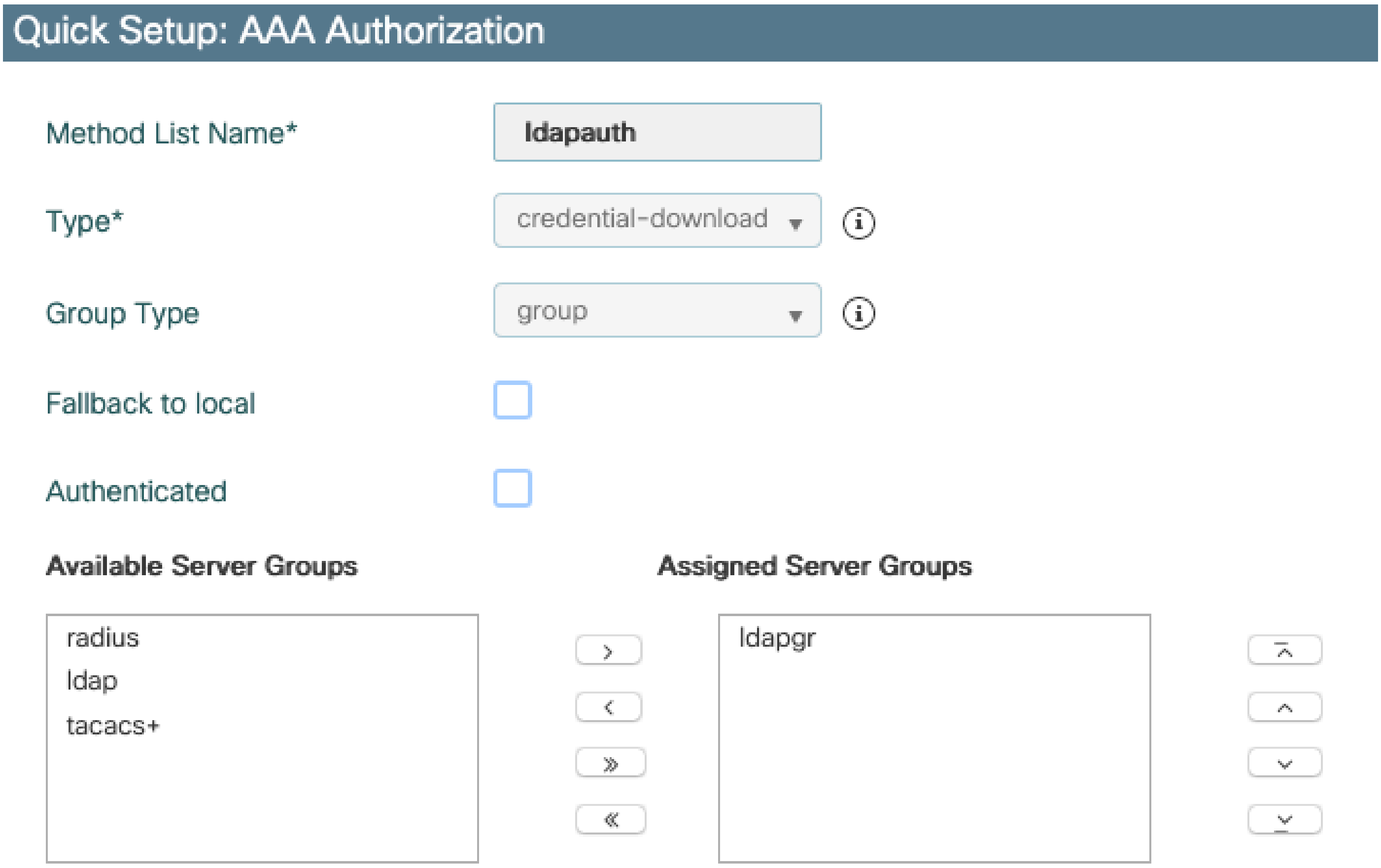
Étape 4 : configuration d’une méthode d’autorisation AAA

Accédez à **Configuration > Security > AAA** > AAA method list > Authorization et cliquez sur **+Add**



Name	Type	Group Type	Group1
default	credential-download	group	ldapgr
ldapauth	credential-download	group	ldapgr

Créez une règle de type Credential-Download du nom de votre choix et pointez-la vers le groupe de serveurs LDAP créé précédemment


Quick Setup: AAA Authorization

Method List Name*: ldapauth

Type*: credential-download

Group Type: group

Fallback to local: □

Authenticated: □

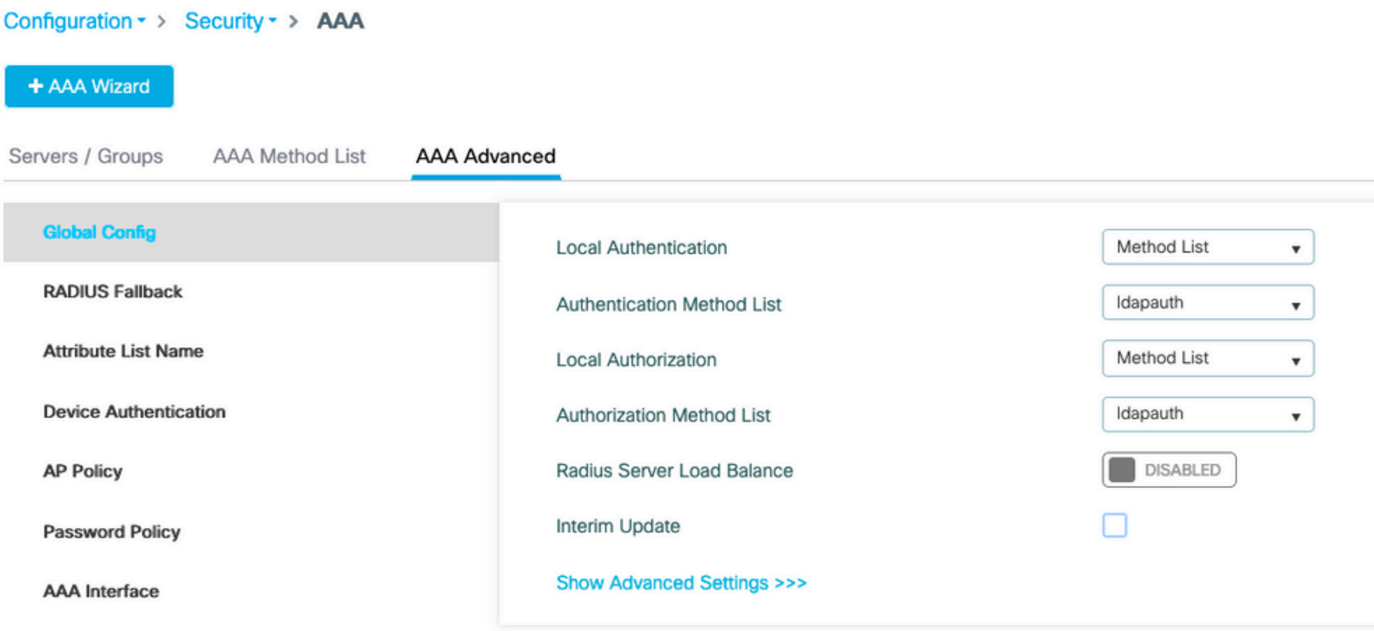
Commandes CLI :

```
aaa authorization credential-download ldapauth group ldapgr
```

Étape 5 : configuration de l’authentification locale

Accédez à **Configuration > Security > AAA > AAA Advanced > Global Config**

Définissez l'authentification locale et l'autorisation locale sur **Method List** et choisissez la méthode d'authentification et d'autorisation configurée précédemment.



Local Authentication: Method List

Authentication Method List: ldapauth

Local Authorization: Method List

Authorization Method List: ldapauth

Radius Server Load Balance: DISABLED

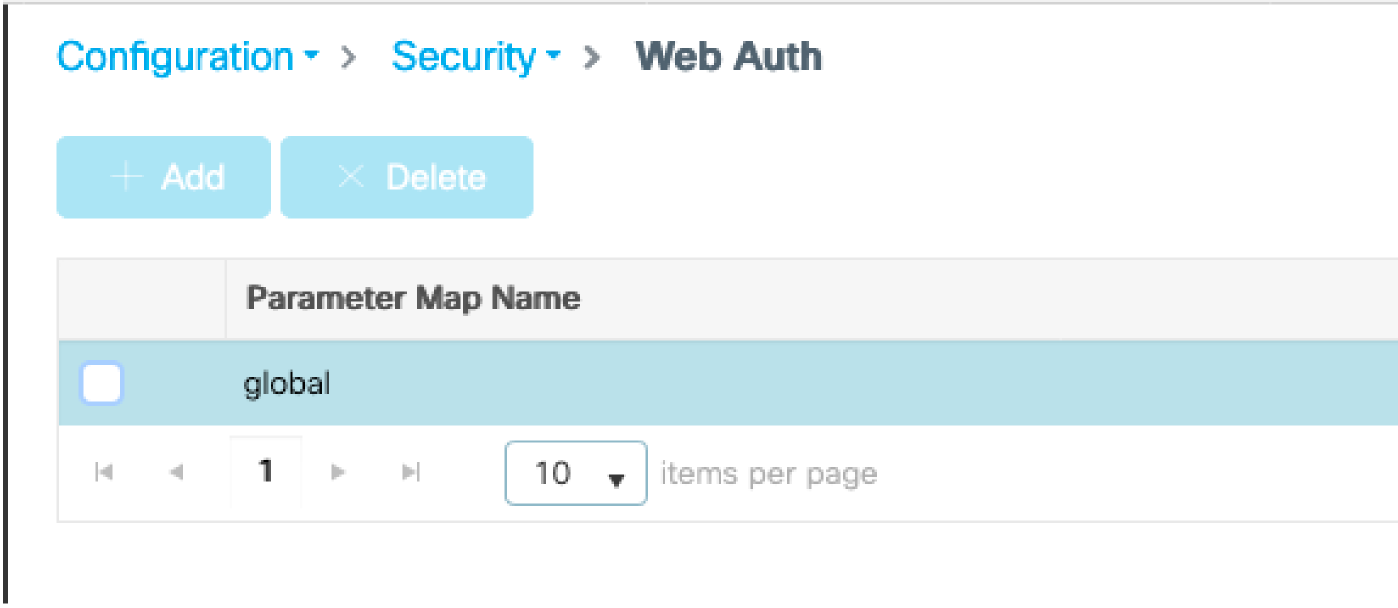
Interim Update: □

Commandes CLI :

```
aaa local authentication ldapauth authorization ldapauth
```

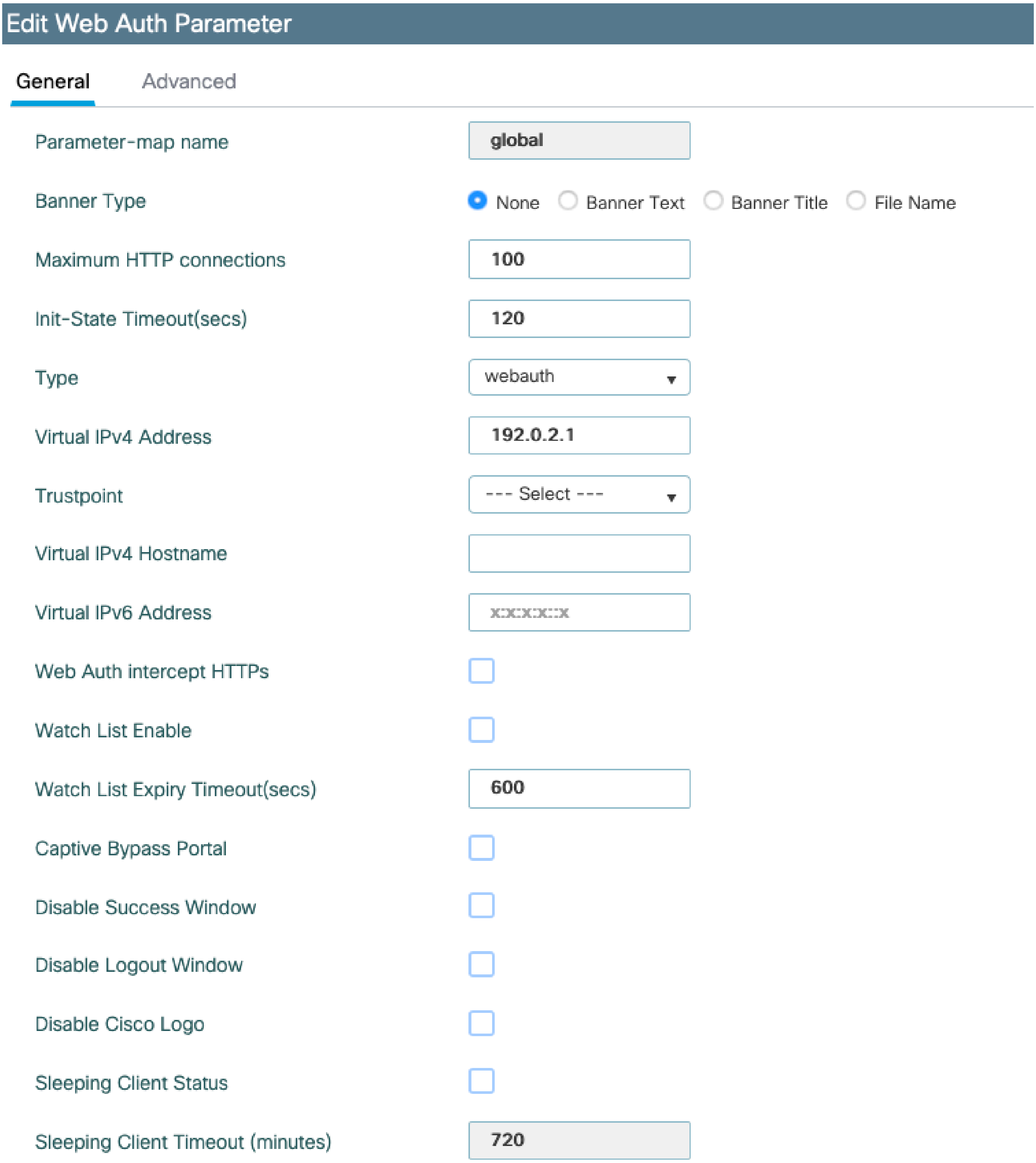
Étape 6 : configuration de la carte-paramètre webauth

Accédez à **Configuration > Security > Web Auth** et modifiez la carte **globale**



	Parameter Map Name
□	global

Assurez-vous de configurer une adresse IPv4 virtuelle telle que 192.0.2.1 (cette adresse IP/sous-réseau spécifique est réservée à l'adresse IP virtuelle non routable).



Edit Web Auth Parameter

General Advanced

Parameter-map name	global
Banner Type	● None ○ Banner Text ○ Banner Title ○ File Name
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	webauth ▾
Virtual IPv4 Address	192.0.2.1
Trustpoint	--- Select --- ▾
Virtual IPv4 Hostname	
Virtual IPv6 Address	X:X:X:X::X
Web Auth intercept HTTPs	□
Watch List Enable	□
Watch List Expiry Timeout(secs)	600
Captive Bypass Portal	□
Disable Success Window	□
Disable Logout Window	□
Disable Cisco Logo	□
Sleeping Client Status	□
Sleeping Client Timeout (minutes)	720

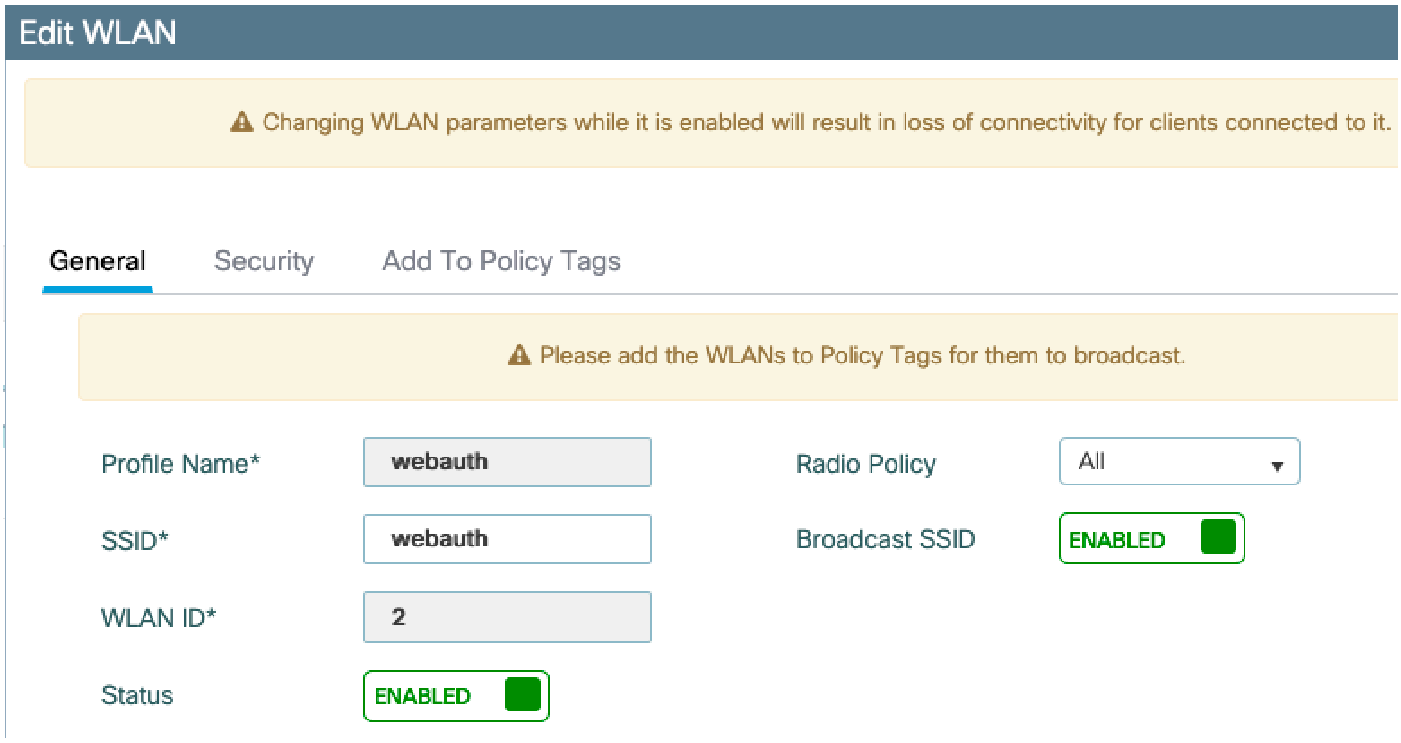
Cliquez sur **Apply** pour enregistrer.

Commandes CLI :

```
parameter-map type webauth global type webauth virtual-ip ipv4 192.0.2.1
```

Étape 7 : configuration d’un WLAN webauth

Accédez à **Configuration > WLANs** et cliquez sur **+Add**



Edit WLAN

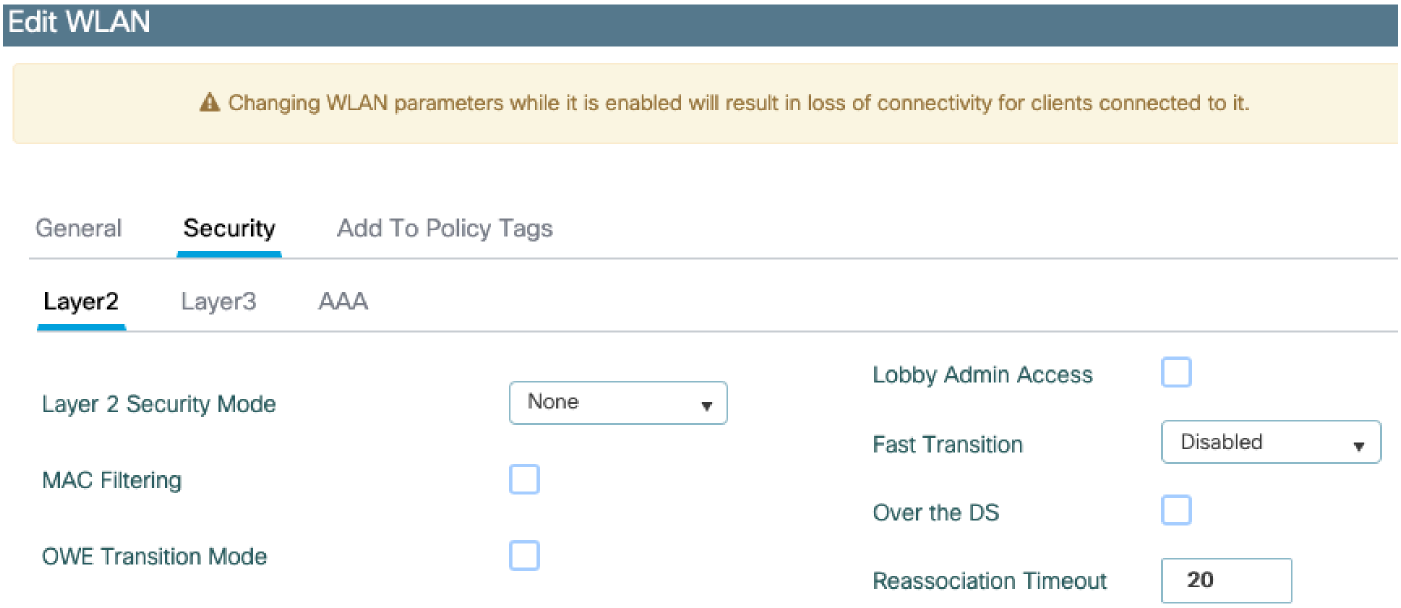
⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

⚠ Please add the WLANs to Policy Tags for them to broadcast.

Profile Name*	webauth	Radio Policy	All
SSID*	webauth	Broadcast SSID	ENABLED
WLAN ID*	2		
Status	ENABLED		

Configurez le nom, assurez-vous qu'il est à l'état activé, puis passez à l'onglet **Sécurité**.

Dans le sous-onglet **Layer 2**, assurez-vous qu'il n'y a aucune sécurité et que la transition rapide est désactivée.

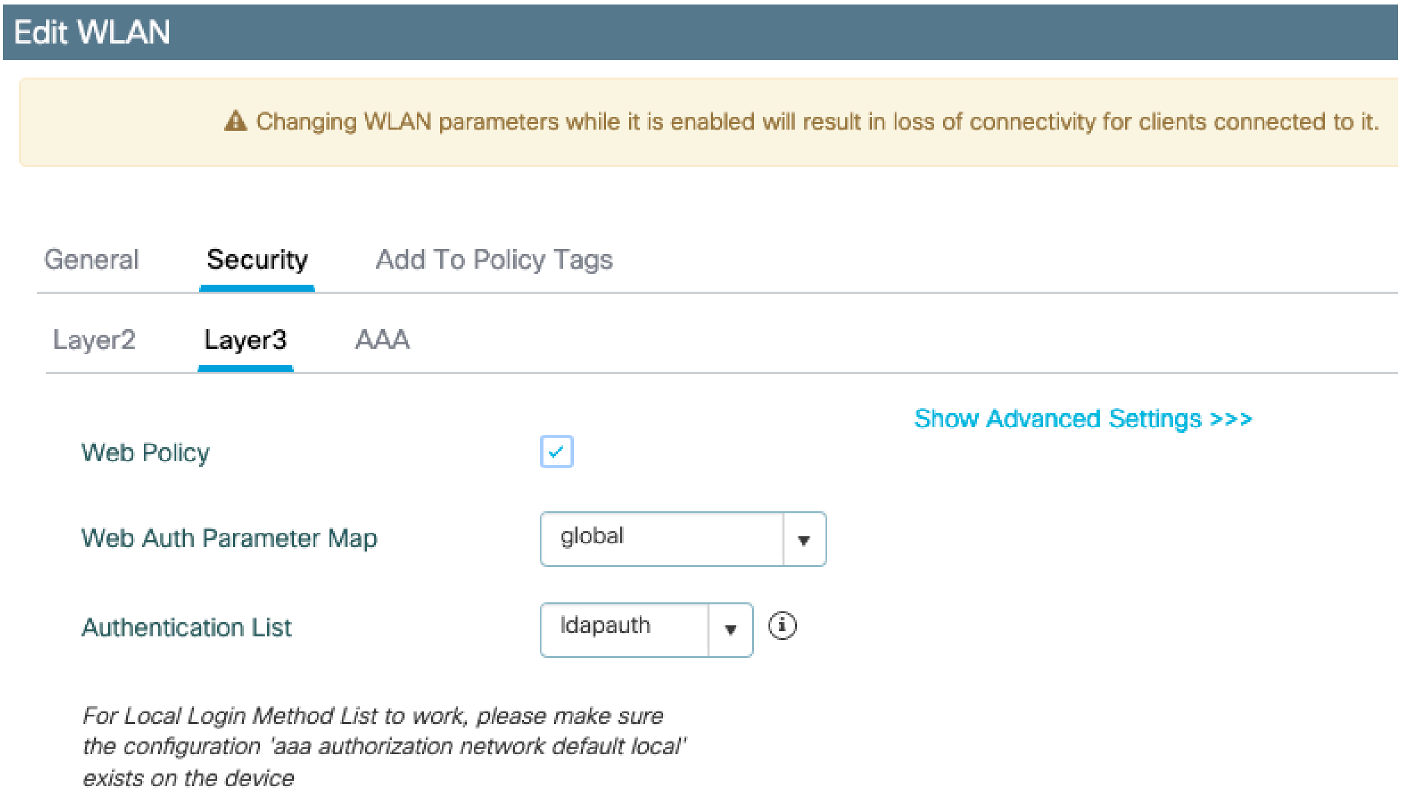


Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Layer 2 Security Mode	None	Lobby Admin Access	□
MAC Filtering	□	Fast Transition	Disabled
OWE Transition Mode	□	Over the DS	□
		Reassociation Timeout	20

Dans l'onglet **Layer3**, activez la **stratégie Web**, définissez la carte de paramètre sur **global** et définissez la liste d'authentification sur la méthode de connexion aaa configurée précédemment.



Edit WLAN
⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.
General
Security
Add To Policy Tags
Layer2
Layer3
AAA
Show Advanced Settings >>>

Web Policy ☑

Web Auth Parameter Map: global

Authentication List: ldapauth

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

Enregistrer en cliquant sur **Appliquer**

Commandes CLI :

```
wlan webauth 2 webauth no security ft adaptive no security wpa no security wpa wpa2 no security
wpa wpa2 ciphers aes no security wpa akm dot1x security web-auth security web-auth
authentication-list ldapauth security web-auth parameter-map global no shutdown
```

Étape 8. Assurez-vous que le SSID est diffusé

Accédez à **Configuration > Tags** et assurez-vous que le SSID est inclus dans le profil de stratégie actuellement géré par le SSID (le default-policy-tag pour une nouvelle configuration si vous n'avez pas encore configuré les tags). Par défaut, default-policy-tag ne diffuse pas les nouveaux SSID que vous créez tant que vous ne les incluez pas manuellement.

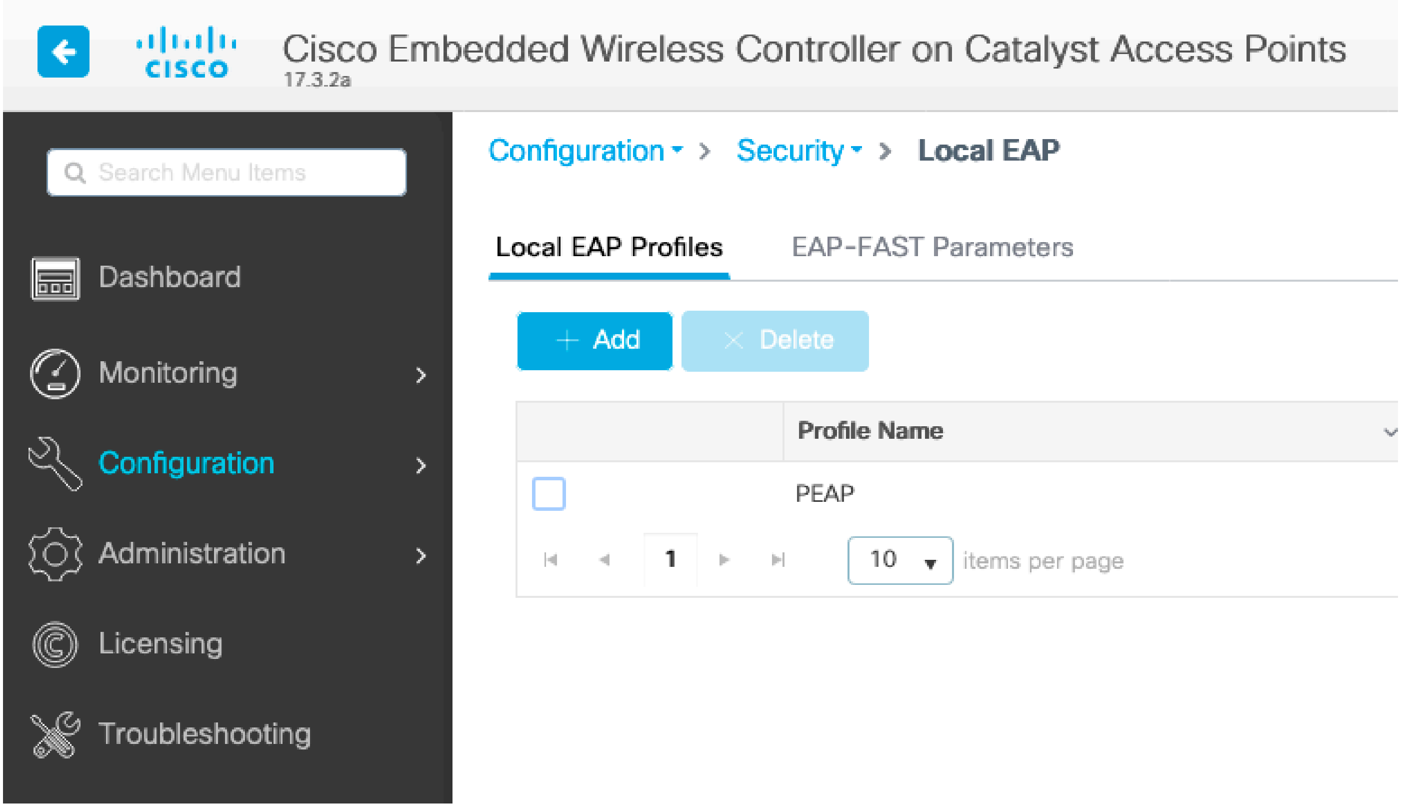
Cet article ne traite pas de la configuration des profils de stratégie et suppose que vous connaissez cette partie de la configuration.

Configurer LDAP avec un SSID dot1x (à l'aide de l'EAP local)

La configuration de LDAP pour un SSID 802.1X sur le 9800 nécessite généralement également la configuration de Local EAP. Si vous deviez utiliser RADIUS, votre serveur RADIUS serait chargé d'établir une connexion avec la base de données LDAP et cela sort du cadre de cet article.Avant d'essayer cette configuration, il est conseillé de configurer Local EAP avec un utilisateur local configuré sur le WLC en premier, un exemple de configuration est fourni dans la section références à la fin de cet article. Cela fait, vous pouvez essayer de déplacer la base de données utilisateur vers LDAP.

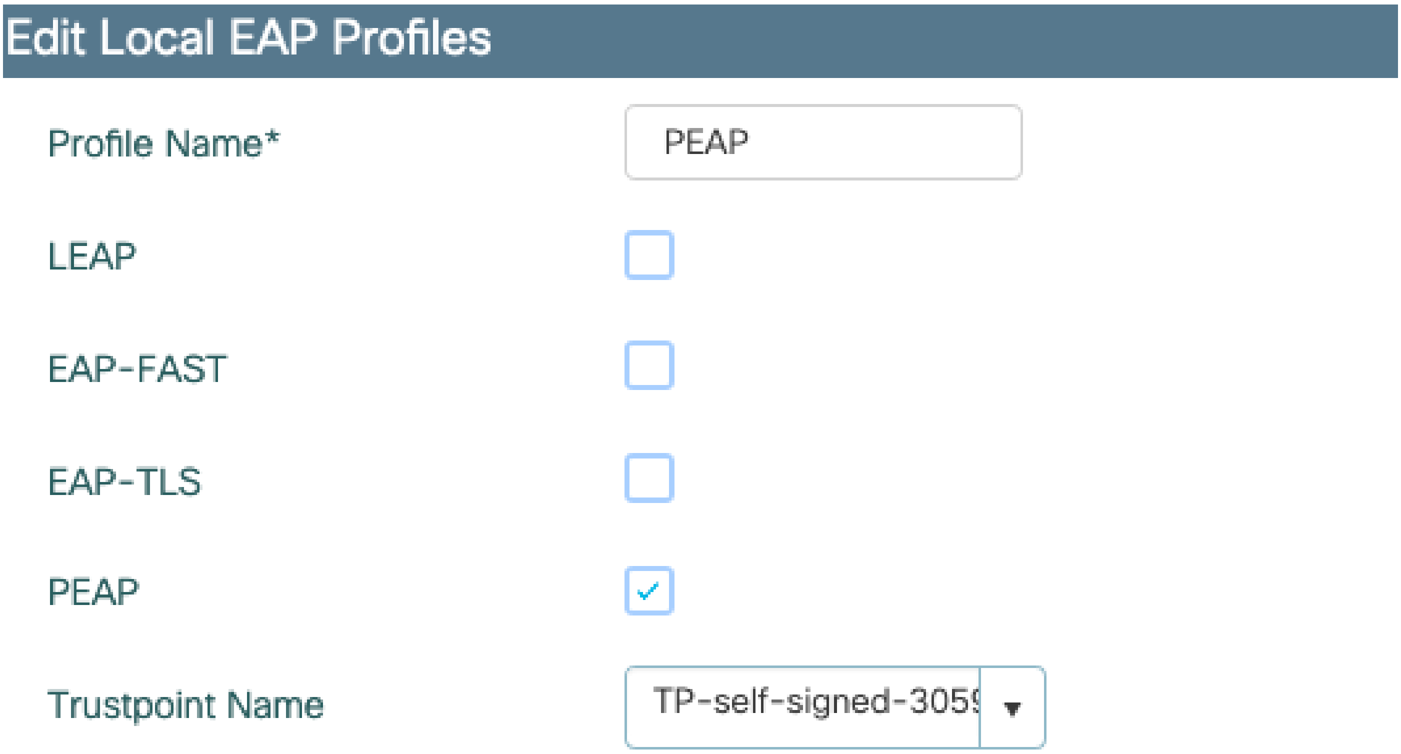
Étape 1 : configuration d’un profil EAP local

Accédez à **Configuration > Local EAP** et cliquez sur **+Add**



	Profile Name
□	PEAP

Choisissez un nom pour votre profil. Activez au moins PEAP et sélectionnez un nom de point de confiance. Par défaut, votre WLC n'a que des certificats auto-signés, donc peu importe lequel vous choisissez (typiquement TP-self-signed-xxxx est le meilleur à cet effet), mais comme les nouvelles versions du système d'exploitation des smartphones font confiance à de moins en moins de certificats auto-signés, pensez à installer un certificat publiquement signé approuvé.



Edit Local EAP Profiles

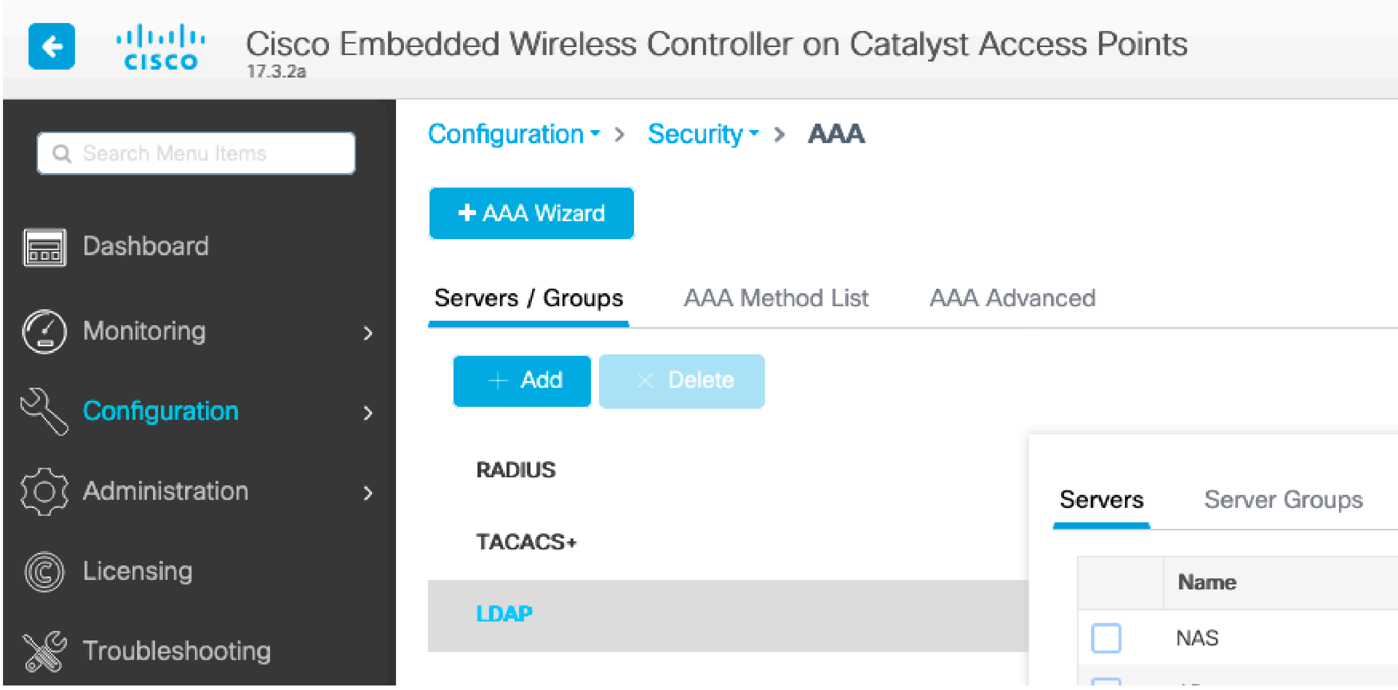
Profile Name*	PEAP
LEAP	□
EAP-FAST	□
EAP-TLS	□
PEAP	☑
Trustpoint Name	TP-self-signed-305

Commandes CLI :

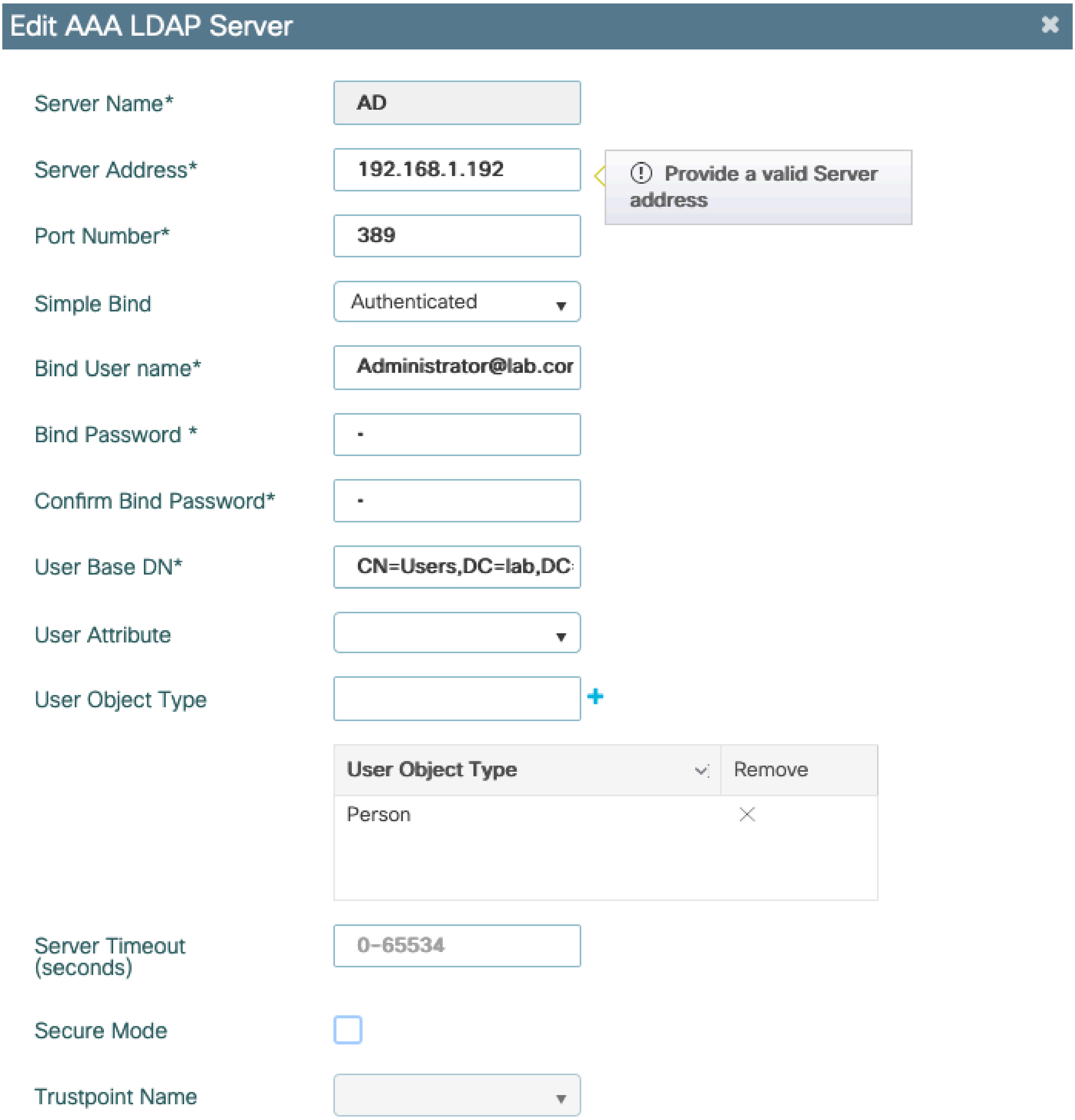
```
eap profile PEAP method peap pki-trustpoint TP-self-signed-3059261382
```

Étape 2 : configuration du serveur LDAP

Accédez à **Configuration > Security > AAA> Servers/Groups > LDAP** et cliquez sur **+ Add**



Choisissez un nom pour votre serveur LDAP et renseignez les détails. Pour obtenir des explications sur chaque champ, reportez-vous à la section « Comprendre les détails du serveur LDAP » de ce document.



Edit AAA LDAP Server

Server Name*	AD
Server Address*	192.168.1.192
Port Number*	389
Simple Bind	Authenticated
Bind User name*	Administrator@lab.cor
Bind Password *	•
Confirm Bind Password*	•
User Base DN*	CN=Users,DC=lab,DC
User Attribute	
User Object Type	
Server Timeout (seconds)	0-65534
Secure Mode	□
Trustpoint Name	

ⓘ Provide a valid Server address

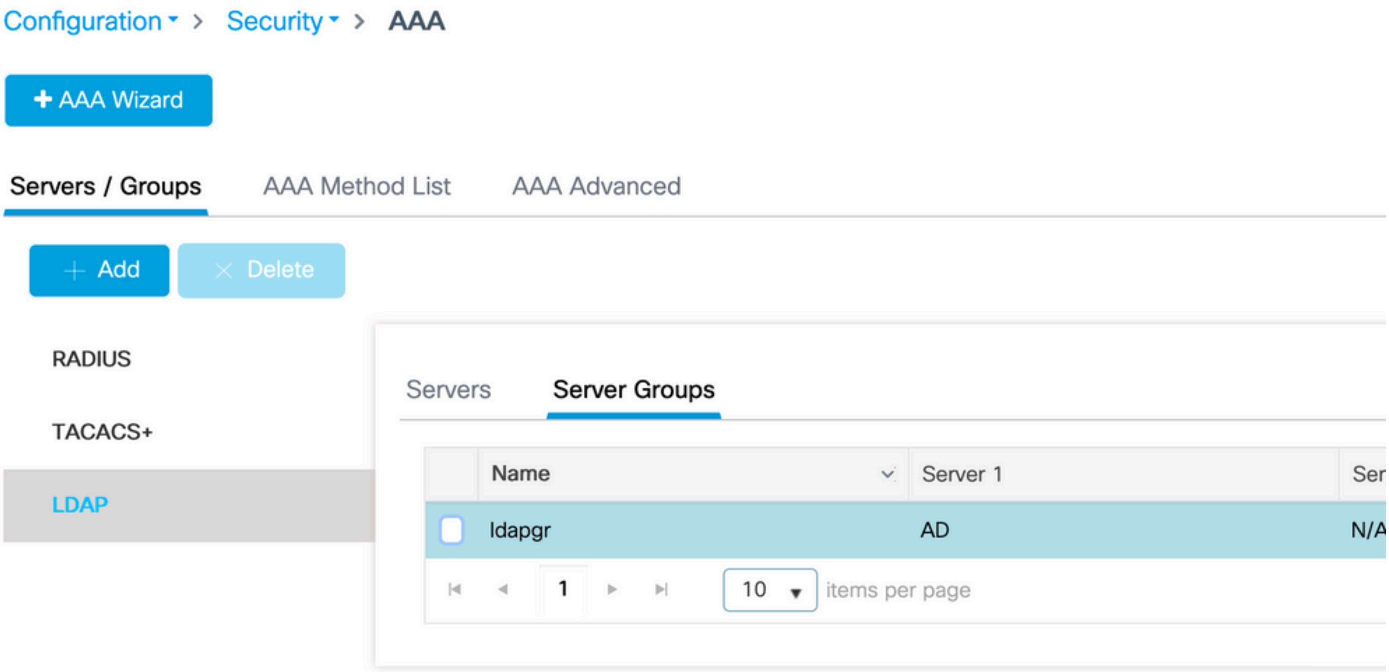
User Object Type	Remove
Person	×

Enregistrer en cliquant sur **Mettre à jour et appliquer au périphérique**

```
ldap server AD ipv4 192.168.1.192 bind authenticate root-dn Administrator@lab.com password 6
WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB base-dn CN=Users,DC=lab,DC=com search-filter user-object-type
Person
```

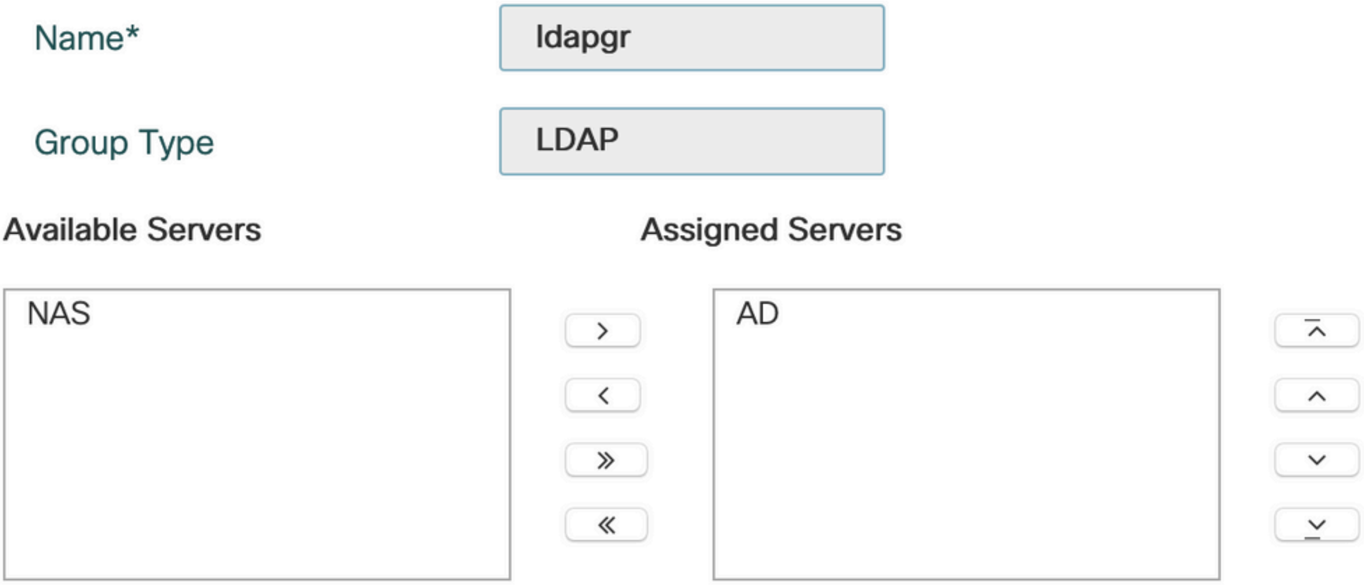
Étape 3 : configuration d’un groupe de serveurs LDAP

Accédez à **Configuration > Security > AAA > Servers/ Groups > LDAP > Server Groups** et cliquez sur **+ADD**



	Name	Server 1	Ser
□	ldapgr	AD	N/A

Entrez un nom et ajoutez le serveur LDAP que vous avez configuré à l'étape précédente.



Name* ldapgr

Group Type LDAP

Cliquez sur **Mettre à jour et appliquer** pour enregistrer.

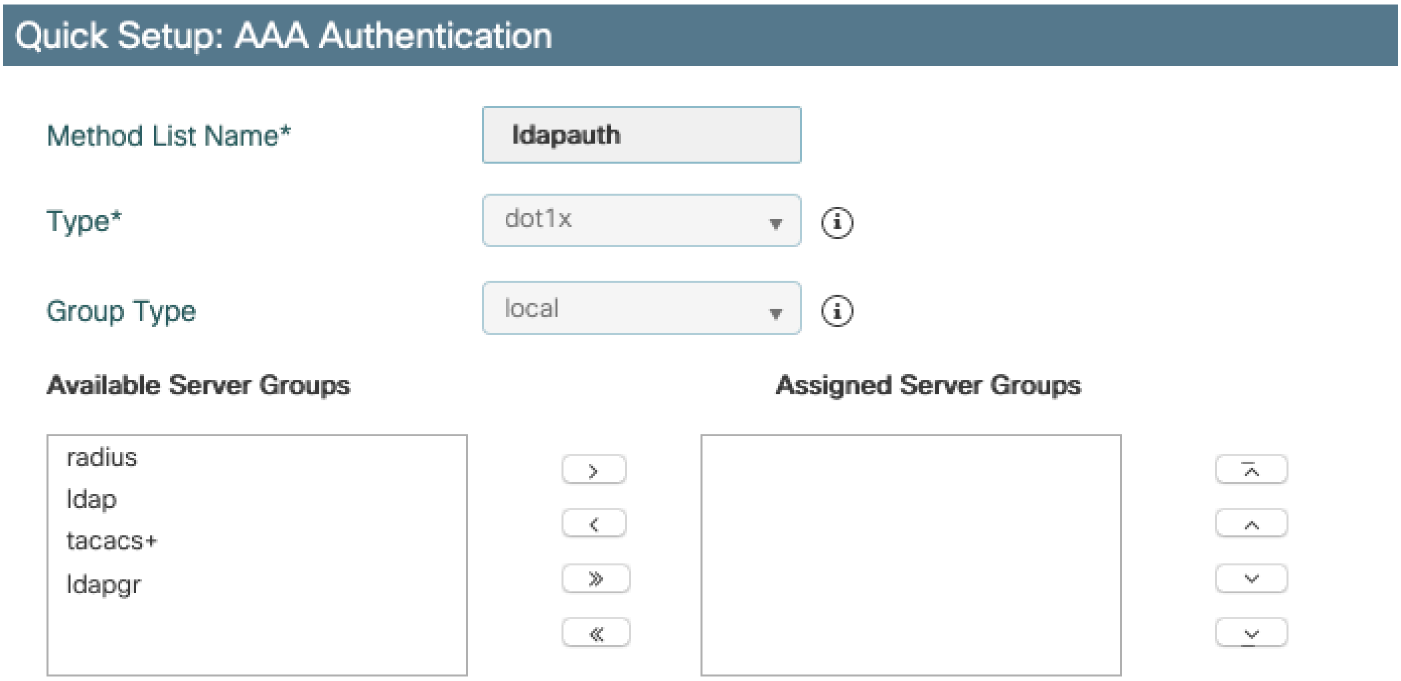
Commandes CLI :

```
aaa group server ldap ldapgr server AD
```

Étape 4 : configuration d’une méthode d’authentification AAA

Accédez à **Configuration > Security > AAA > AAA Method List > Authentication** et cliquez sur **+Add**

Configurez une méthode d'authentification de type **dot1x** et pointez-la vers local uniquement. Il serait tentant de pointer vers le groupe de serveurs LDAP, mais c'est le WLC lui-même qui agit ici en tant qu'authentificateur 802.1X (bien que la base de données utilisateur soit sur LDAP, mais c'est le travail de méthode d'autorisation).


Quick Setup: AAA Authentication

Method List Name* ldapauth

Type* dot1x

Group Type local

Available Server Groups
radius
ldap
tacacs+
ldapgr

Assigned Server Groups

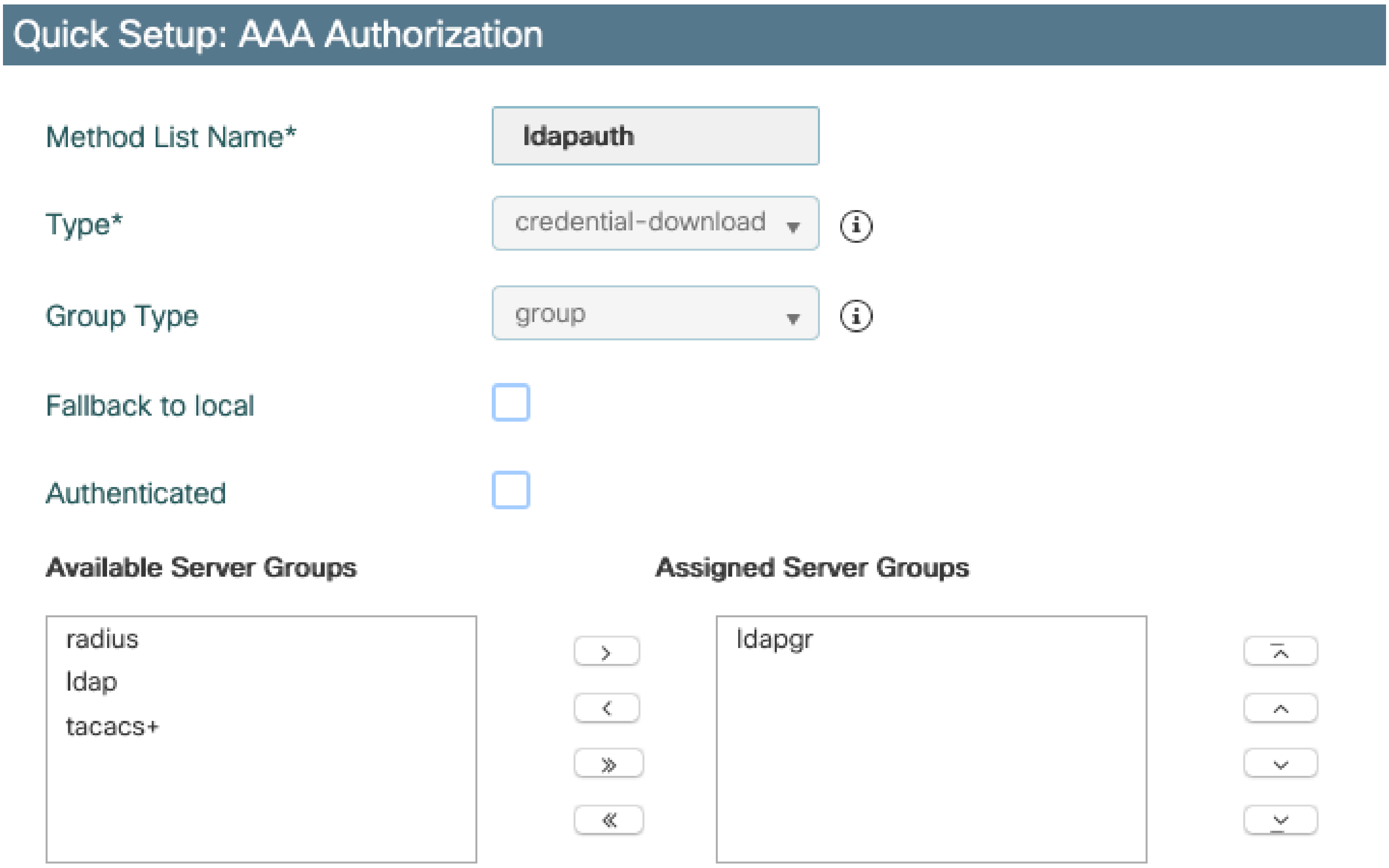
Commande CLI :

```
aaa authentication dot1x ldapauth local
```

Étape 5 : configuration d’une méthode d’autorisation AAA

Accédez à **Configuration > Security > AAA > AAA Method List > Authorization** et cliquez sur **+Add**

Créez une méthode d'autorisation de type **credential-download** et faites-la pointer vers le groupe LDAP.



Quick Setup: AAA Authorization

Method List Name* ldapauth

Type* credential-download

Group Type group

Fallback to local □

Authenticated □

Available Server Groups	Assigned Server Groups
radius ldap tacacs+	ldapgr

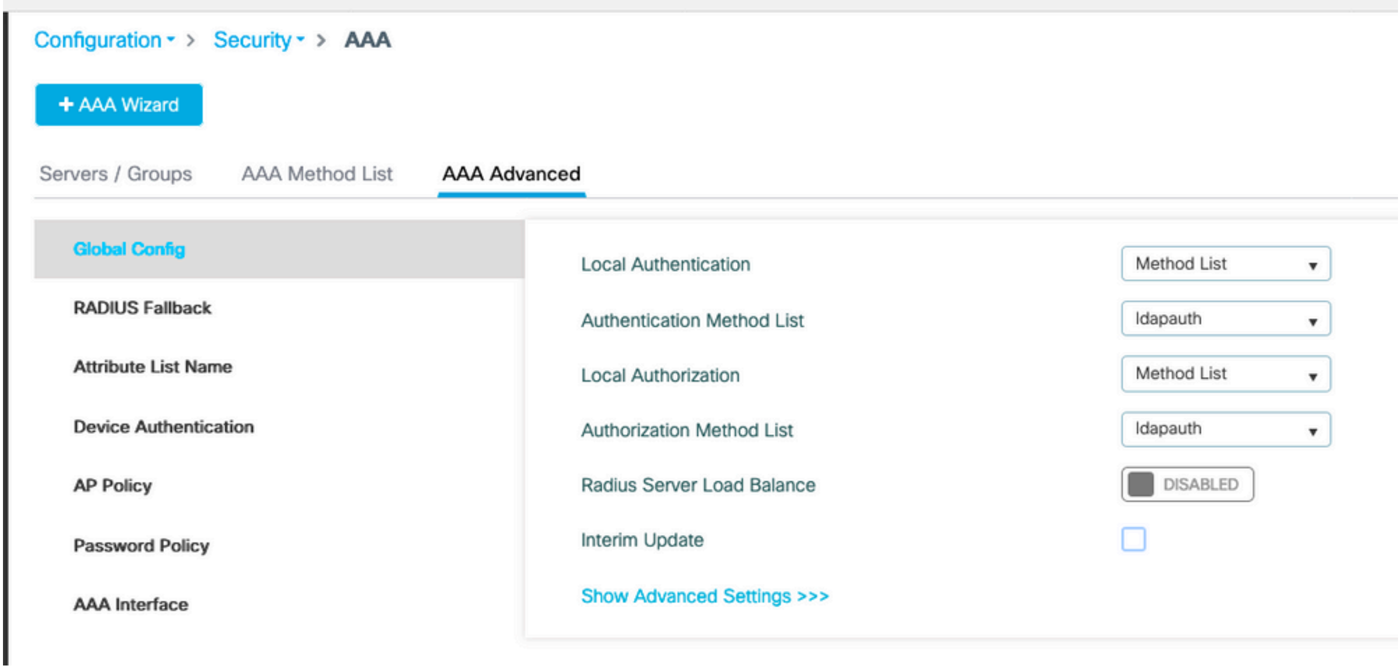
Commande CLI :

```
aaa authorization credential-download ldapauth group ldapgr
```

Étape 6. Configuration des détails de l’authentification locale

Accédez à **Configuration > Security > AAA > AAA Method List > AAA advanced**

Choisissez **Method List** pour l'authentification et l'autorisation et choisissez la méthode d'authentification dot1x pointant localement et la méthode d'autorisation de téléchargement d'identifiants pointant vers LDAP



Configuration > Security > AAA

Global Config

Local Authentication	Method List
Authentication Method List	ldapauth
Local Authorization	Method List
Authorization Method List	ldapauth
Radius Server Load Balance	DISABLED
Interim Update	□

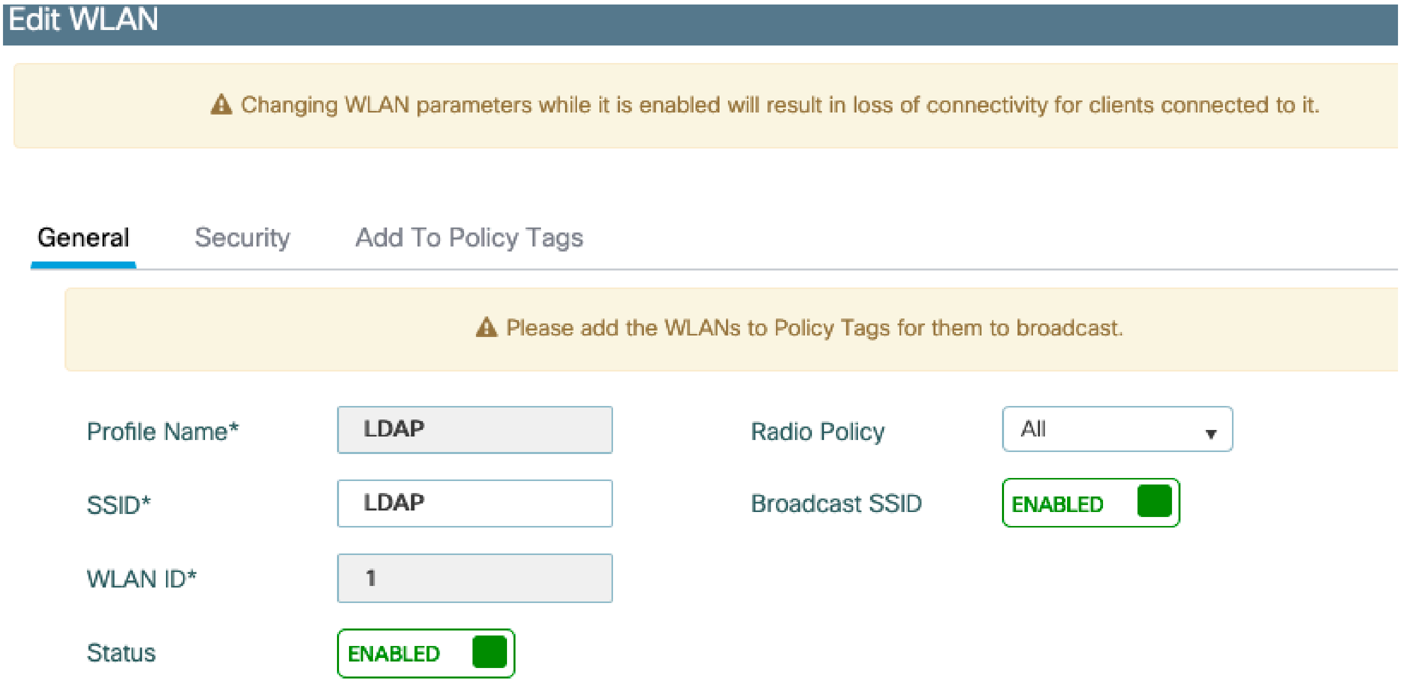
Commande CLI :

```
aaa local authentication ldapauth authorization ldapauth
```

Étape 7 : configuration d'un réseau local sans fil dot1x

Accédez à **Configuration > WLAN** et cliquez sur **+Add**

Choisissez un profil et un nom SSID et assurez-vous qu'il est activé.



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

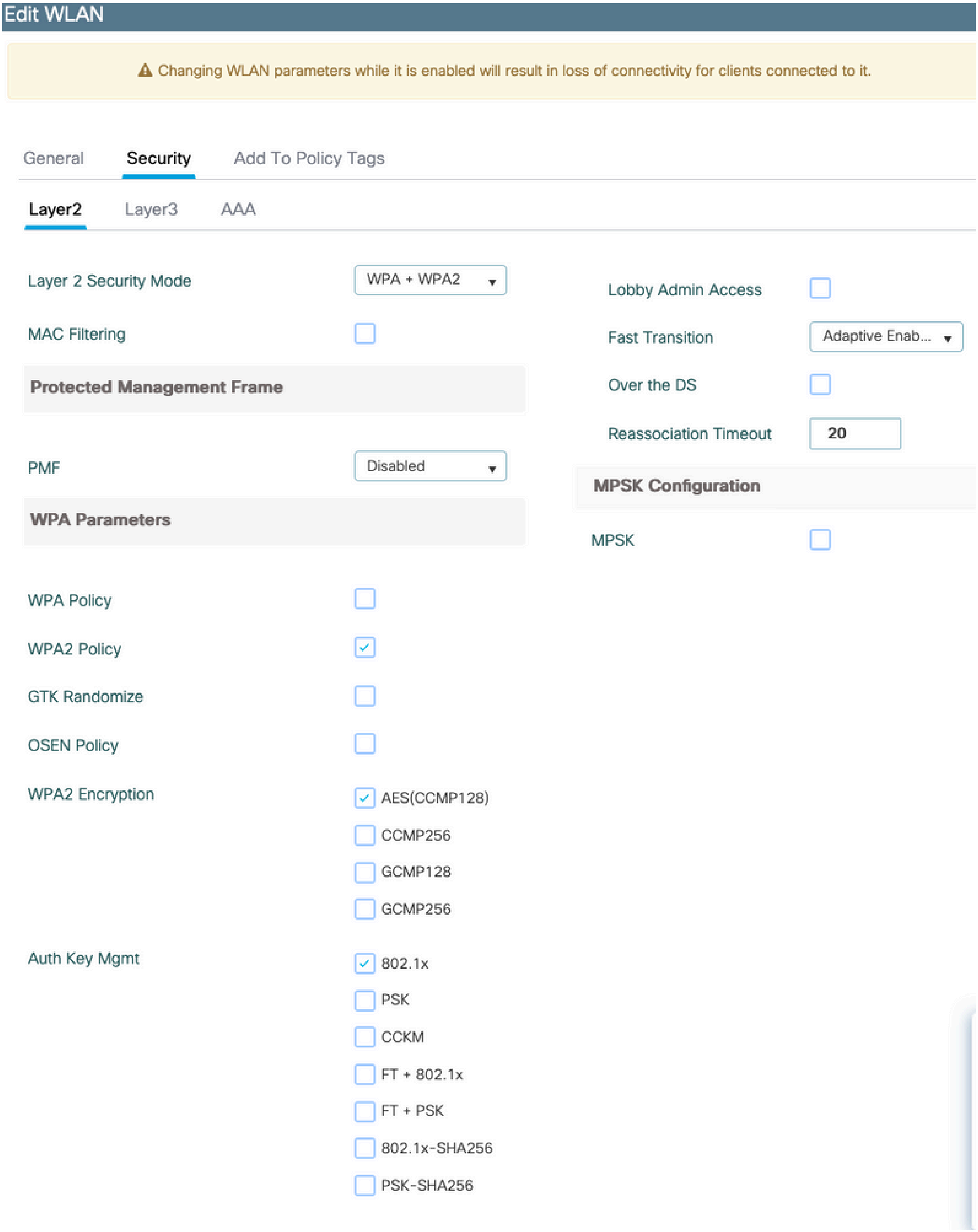
⚠ Please add the WLANs to Policy Tags for them to broadcast.

Profile Name*	LDAP	Radio Policy	All
SSID*	LDAP	Broadcast SSID	ENABLED
WLAN ID*	1		
Status	ENABLED		

Accédez à l'onglet Layer 2 **security**.

Choisissez WPA+WPA2 comme **mode de sécurité de couche 2**

Vérifiez que WPA2 et AES sont activés dans les **paramètres WPA** et activez **802.1X**



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Layer 2 Security Mode: WPA + WPA2

MAC Filtering □

Protected Management Frame

PMF: Disabled

WPA Parameters

WPA Policy □

WPA2 Policy ☑

GTK Randomize □

OSEN Policy □

WPA2 Encryption: ☑ AES(CCMP128) □ CCMP256 □ GCMP128 □ GCMP256

Auth Key Mgmt: ☑ 802.1x □ PSK □ CCKM □ FT + 802.1x □ FT + PSK □ 802.1x-SHA256 □ PSK-SHA256

Lobby Admin Access □

Fast Transition: Adaptive Enab...

Over the DS □

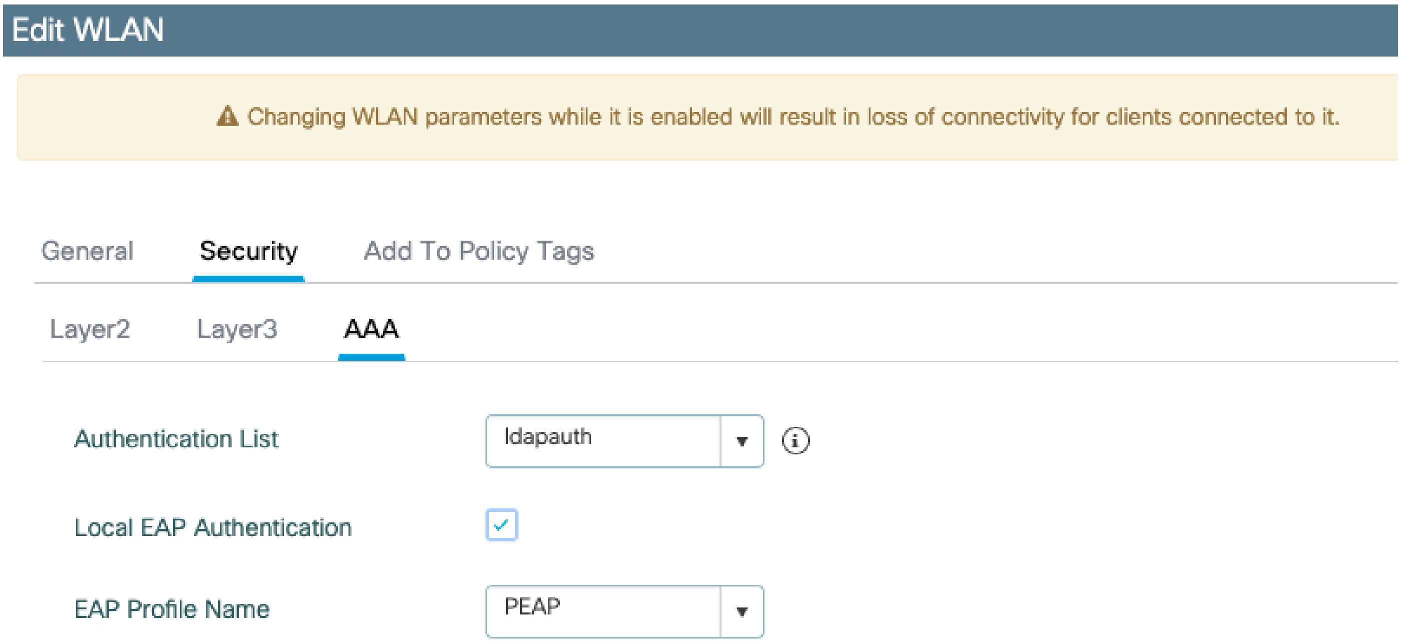
Reassociation Timeout: 20

MPSK Configuration

MPSK □

Accédez au sous-onglet **AAA**.

Choisissez la méthode d'authentification dot1x créée précédemment, activez l'authentification EAP locale et choisissez le profil EAP configuré à la première étape.



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Authentication List: ldapauth

Local EAP Authentication: ☑

EAP Profile Name: PEAP

Enregistrer en cliquant sur Appliquer

Commandes CLI :

```
wlan LDAP 1 LDAP local-auth PEAP security dot1x authentication-list ldapauth no shutdown
```

Étape 8. Vérification de la diffusion du WLAN

Accédez à **Configuration > Tags** et assurez-vous que le SSID est inclus dans le profil de stratégie actuellement géré par le SSID (le default-policy-tag pour une nouvelle configuration si vous n'avez pas encore configuré les tags). Par défaut, default-policy-tag ne diffuse pas les nouveaux SSID que vous créez tant que vous ne les incluez pas manuellement.

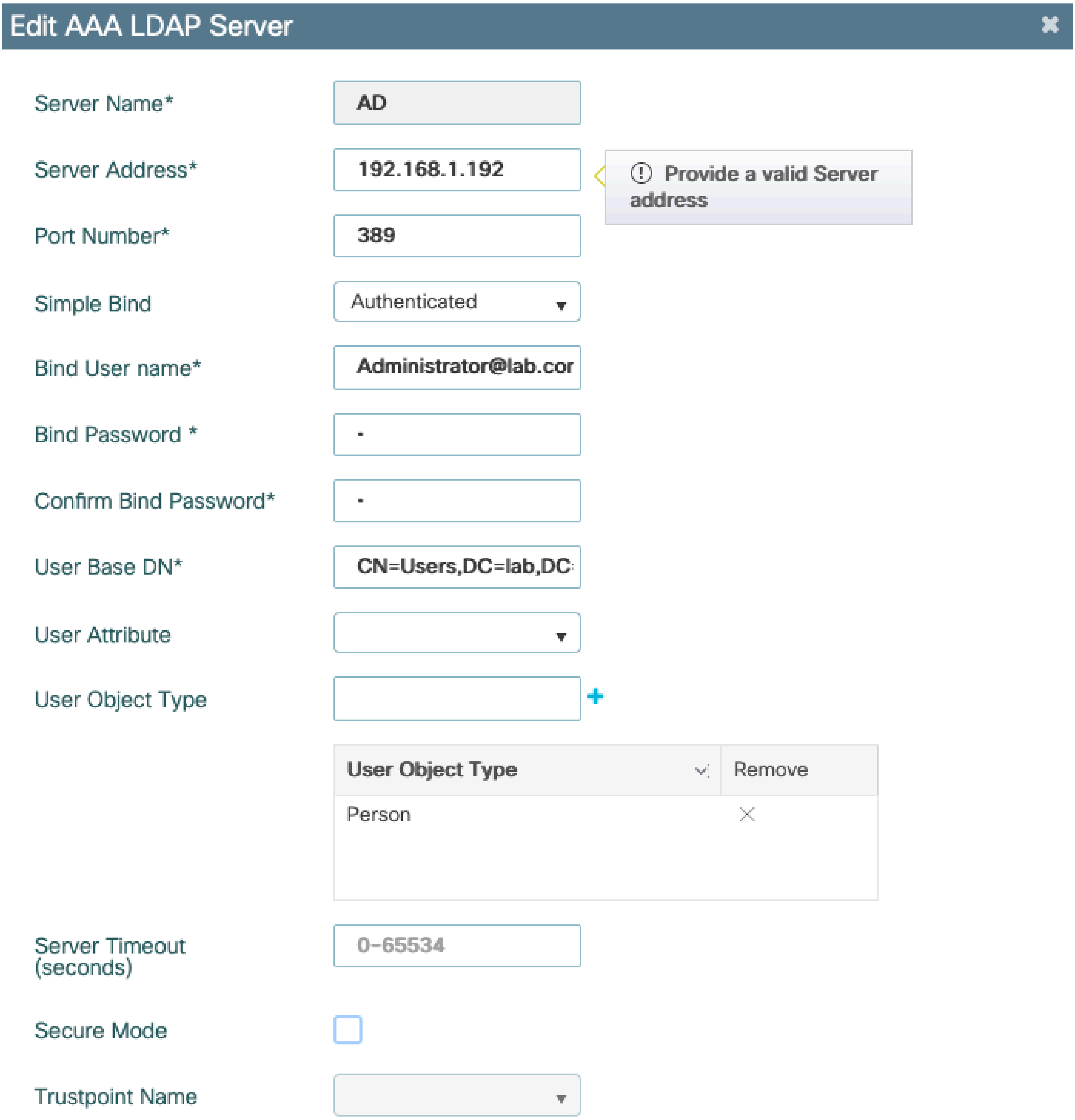
Cet article ne traite pas de la configuration des profils de stratégie et suppose que vous connaissez cette partie de la configuration.

Si vous utilisez Active Directory, vous devez configurer le serveur AD pour envoyer l'attribut « userPassword ». Cet attribut doit être envoyé au WLC. C'est parce que le WLC effectue la vérification, pas le serveur AD. Vous pouvez également rencontrer des problèmes d'authentification avec la méthode PEAP-mschapv2 car le mot de passe n'est jamais envoyé en texte clair et ne peut donc pas être vérifié avec la base de données LDAP, seule la méthode PEAP-GTC fonctionnerait avec certaines bases de données LDAP.

Comprendre les détails du serveur LDAP

Comprendre les champs de l'interface utilisateur Web du 9800

Voici un exemple d'Active Directory de base qui agit comme serveur LDAP configuré sur le 9800



Edit AAA LDAP Server

Server Name*	AD
Server Address*	192.168.1.192
Port Number*	389
Simple Bind	Authenticated
Bind User name*	Administrator@lab.cor
Bind Password *	•
Confirm Bind Password*	•
User Base DN*	CN=Users,DC=lab,DC:
User Attribute	
User Object Type	
Server Timeout (seconds)	0-65534
Secure Mode	□
Trustpoint Name	

Provide a valid Server address

User Object Type	Remove
Person	×

Le nom et l'adresse IP sont probablement explicites.

Port : 389 est le port par défaut pour LDAP, mais votre serveur peut en utiliser un autre.

Liaison simple : de nos jours, il est très rare d'avoir une base de données LDAP qui prend en charge la liaison non authentifiée (ce qui signifie que n'importe qui peut faire une recherche LDAP dessus sans aucun formulaire d'authentification). La liaison simple authentifiée est le type d'authentification le plus courant et ce qu'Active Directory autorise par défaut. Vous pouvez entrer un nom de compte administrateur et un mot de passe pour pouvoir effectuer une recherche dans la base de données utilisateur à partir de cet emplacement.

Nom d'utilisateur : Vous devez pointer vers un nom d'utilisateur avec des privilèges d'administrateur dans Active Directory. AD tolère le format « user@domain » alors que de nombreuses autres bases de données LDAP attendent un format « CN=xxx, DC=xxx » pour le nom d'utilisateur. Un exemple avec une autre base de données LDAP qu'AD est fourni plus loin dans cet article.

Mot de passe Bind : Entrez le mot de passe que vous avez entré précédemment.

DN de base utilisateur : Entrez ici la "racine de recherche", c'est-à-dire l'emplacement dans votre arborescence LDAP où les recherches commencent. Dans cet exemple, tous nos utilisateurs se trouvent sous le groupe « Users », dont le nom de domaine est « CN=Users, DC=lab, DC=com » (puisque le domaine LDAP donné en exemple est lab.com). Un exemple de la façon de découvrir ce DN de base utilisateur est fourni plus loin dans cette section.

Attribut utilisateur : Vous pouvez laisser ce champ vide ou pointer vers un mappage d'attributs LDAP qui indique quel champ LDAP compte comme nom d'utilisateur pour votre base de données LDAP. Cependant, en raison de l'ID de bogue Cisco CSCv11813 , le WLC tente une authentification avec le champ CN quoi qu'il arrive.

Type d'objet utilisateur : Détermine le type d'objets considérés comme des utilisateurs. Il s'agit généralement de « Personne ». Il peut s'agir d'« ordinateurs » si vous disposez d'une base de données Active Directory et que vous authentifiez des comptes d'ordinateur, mais là encore, le protocole LDAP permet de nombreuses personnalisations.

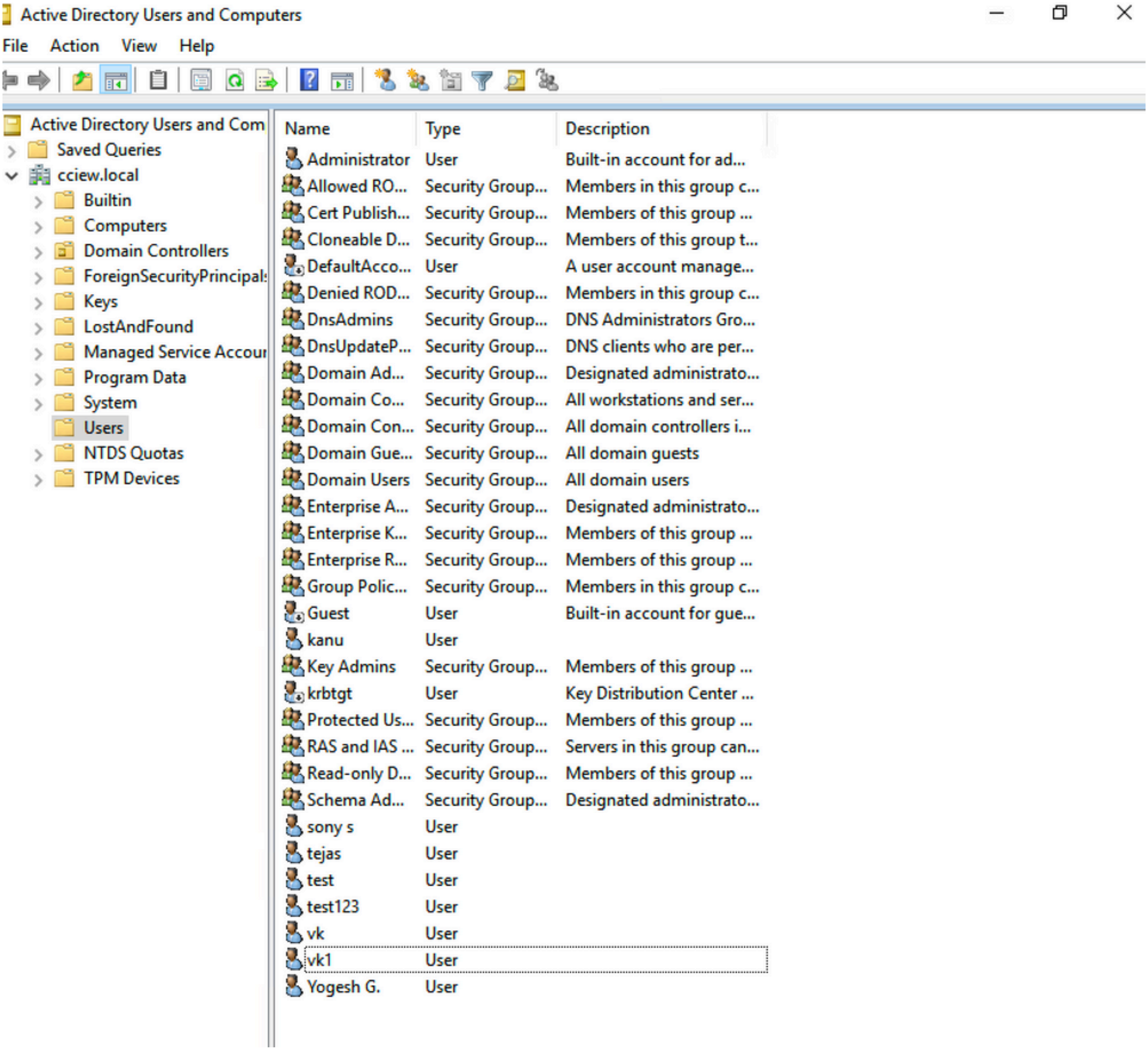
Le mode sécurisé active le protocole LDAP sécurisé sur TLS et vous oblige à sélectionner un point de confiance sur le 9800 pour utiliser un certificat pour le cryptage TLS.

Authentification LDAP 802.1x avec attribut sAMAaccountName.

Cette amélioration est introduite dans la version 17.6.1.

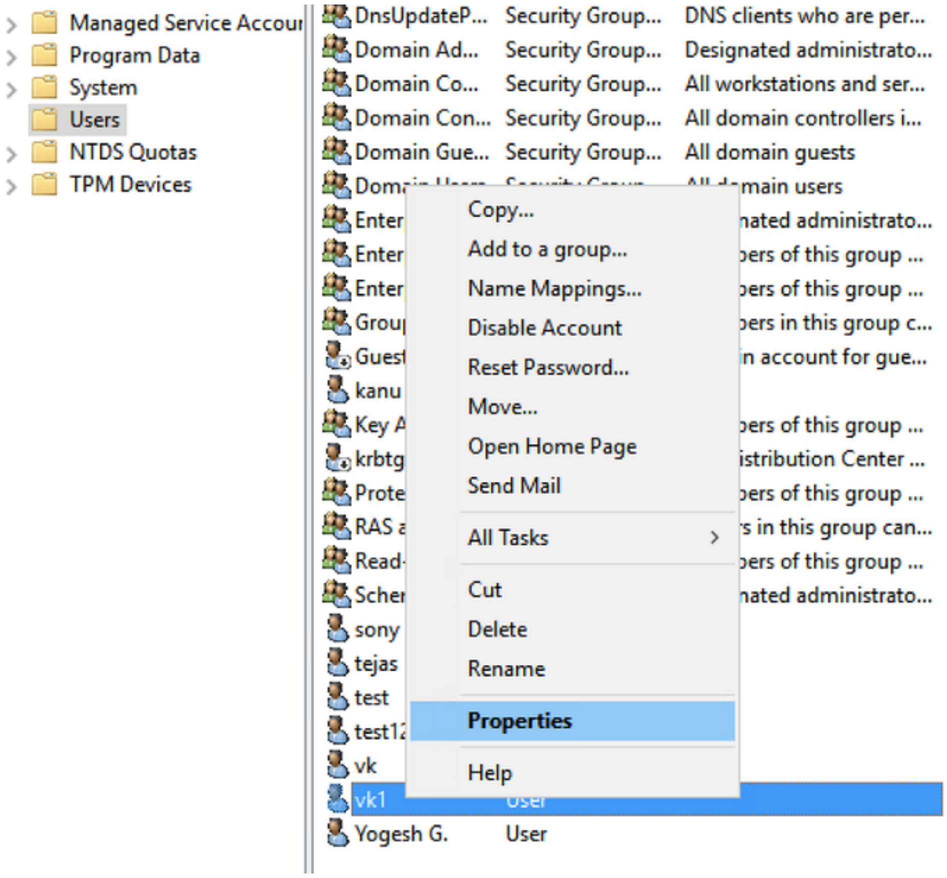
Configurez l'attribut « userPassword » pour l'utilisateur.

Étape 1. Sur le serveur Windows, accédez à Utilisateurs et ordinateurs Active Directory

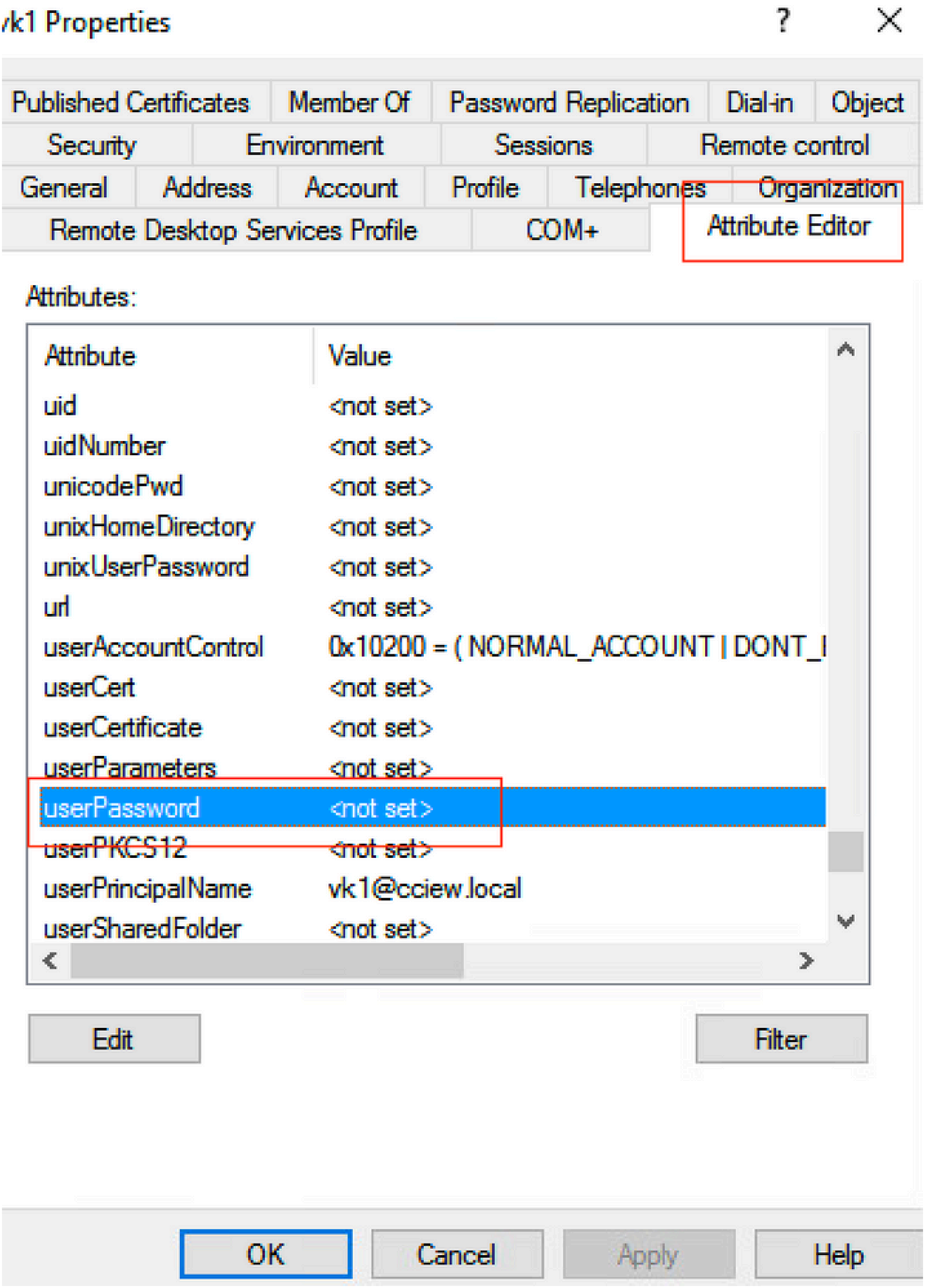


Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
kanu	User	
Key Admins	Security Group...	Members of this group ...
krbtgt	User	Key Distribution Center ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
sony s	User	
tejas	User	
test	User	
test123	User	
vk	User	
vk1	User	
Yogesh G.	User	

Étape 2. Cliquez avec le bouton droit sur le nom d’utilisateur correspondant et sélectionnez les propriétés


Managed Service Accour
Program Data
System
Users
NTDS Quotas
TPM Devices
DnsUpdateP... Security Group... DNS clients who are per...
Domain Ad... Security Group... Designated administrato...
Domain Co... Security Group... All workstations and ser...
Domain Con... Security Group... All domain controllers i...
Domain Gue... Security Group... All domain guests
All domain users
Copy...
Add to a group...
Name Mappings...
Disable Account
Reset Password...
Move...
Open Home Page
Send Mail
All Tasks
Cut
Delete
Rename
Properties
Help
kanu
sony
tejas
test
vk
vk1
Yogesh G. User

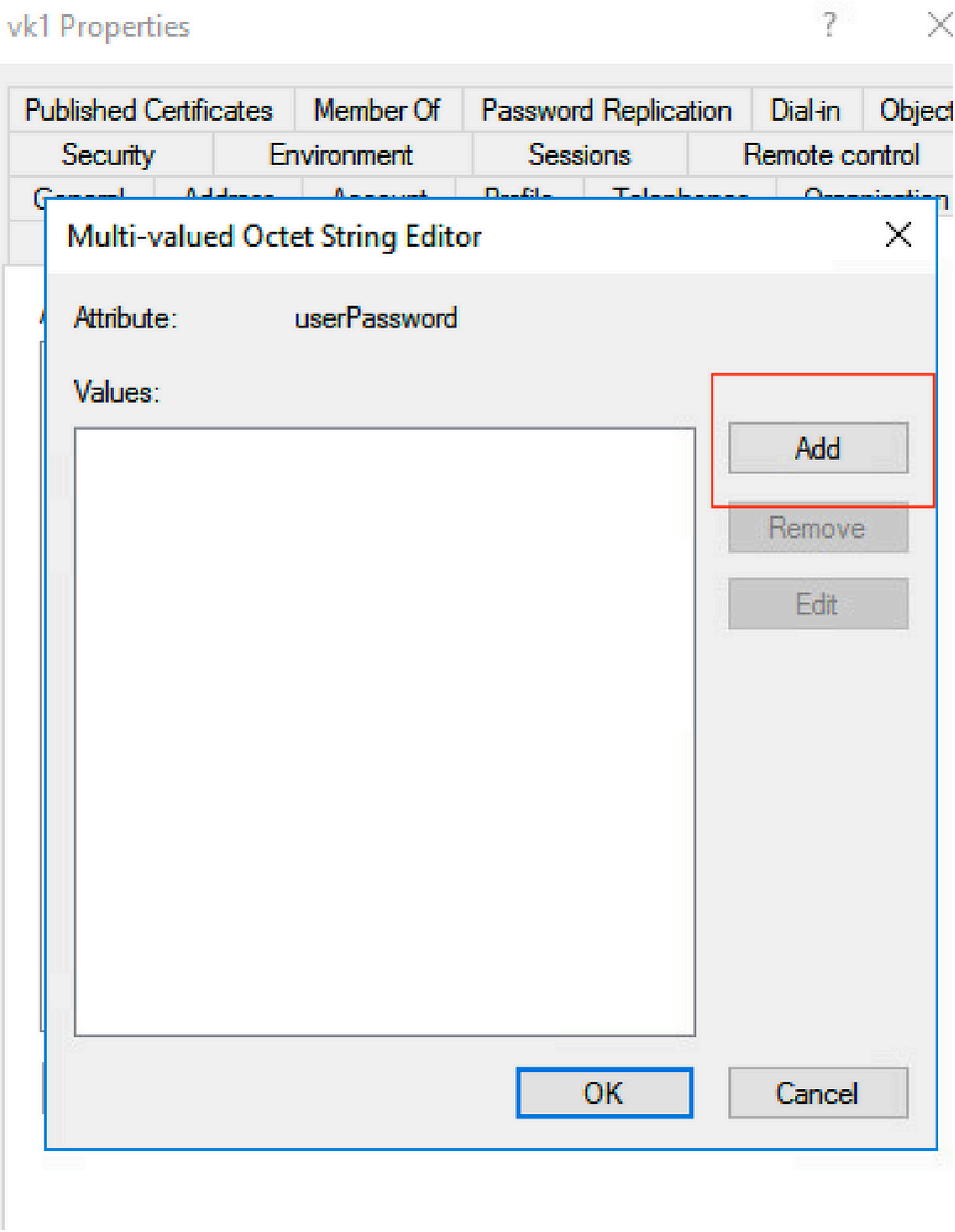
Étape 3. Sélectionnez l'éditeur d'attributs dans la fenêtre des propriétés



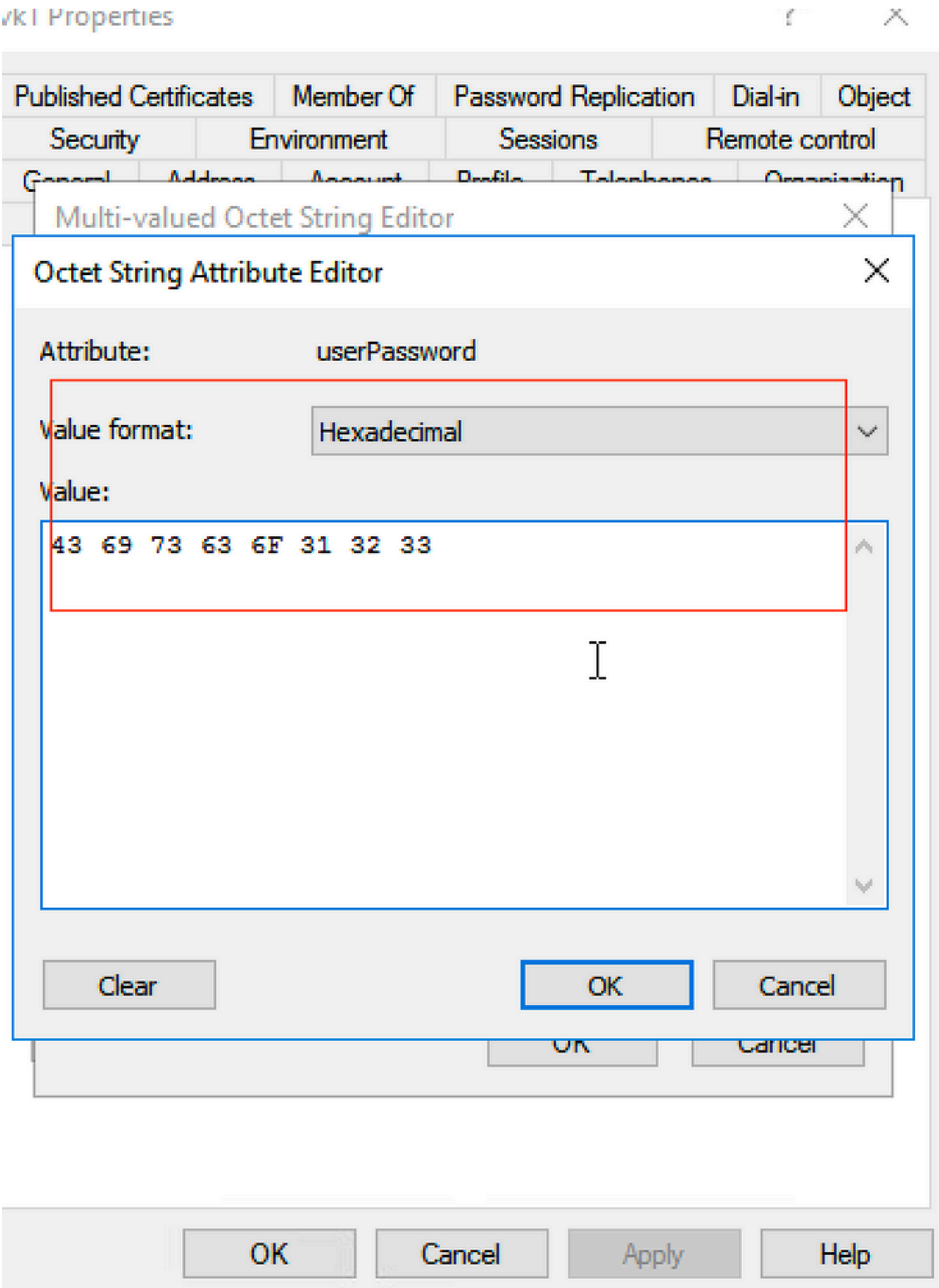
Attributes:

Attribute	Value
uid	<not set>
uidNumber	<not set>
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_I
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>
userPKCS12	<not set>
userPrincipalName	vk1@cciew.local
userSharedFolder	<not set>

Étape 4 : configuration de l'attribut « userPassword » Il s'agit du mot de passe de l'utilisateur, qui doit être configuré en valeur hexadécimale.



Attribute: userPassword



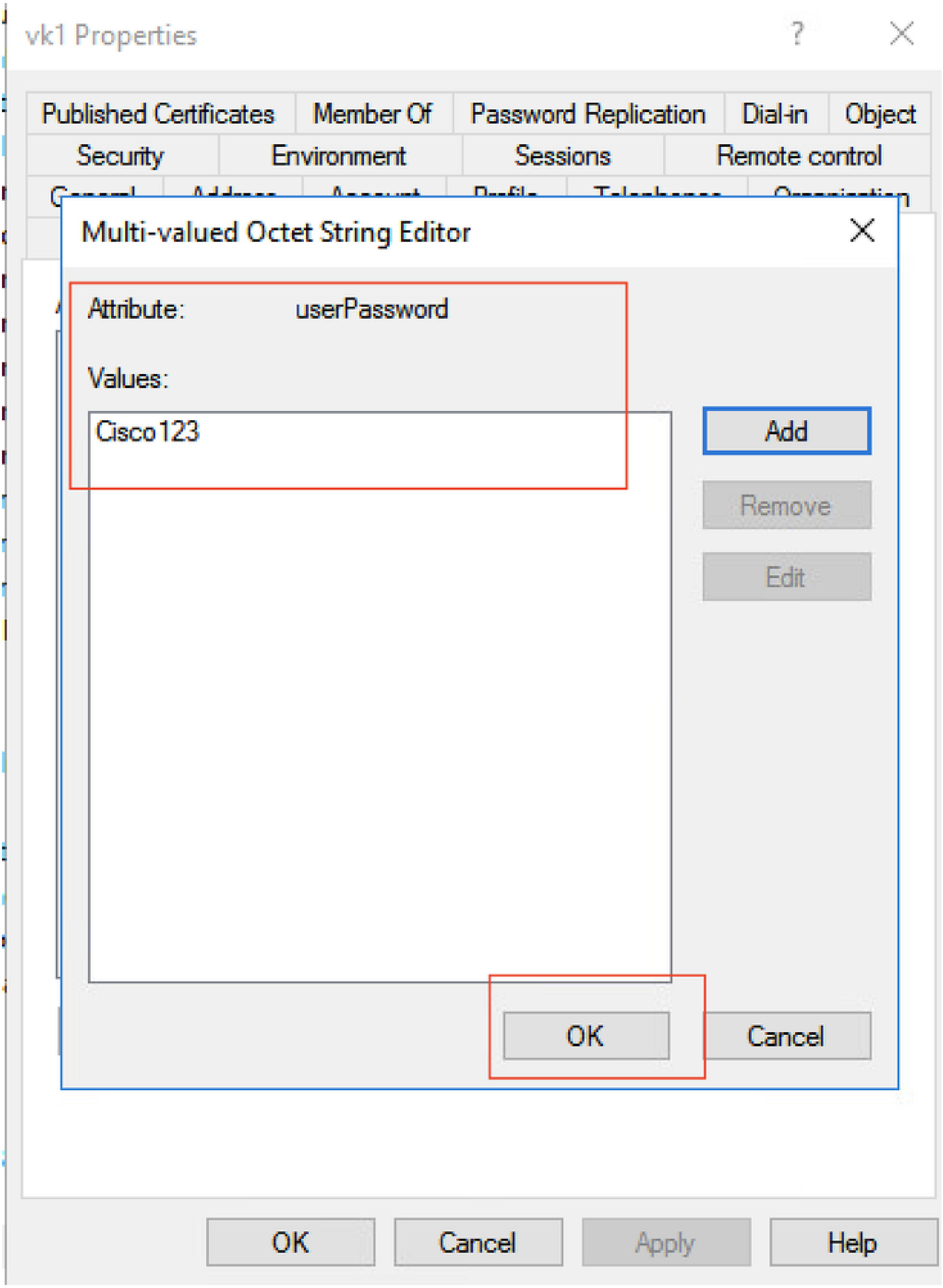
Attribute: userPassword

Value format: Hexadecimal

Value:

```
43 69 73 63 6F 31 32 33
```

Cliquez sur ok, vérifiez qu'il affiche le mot de passe correct

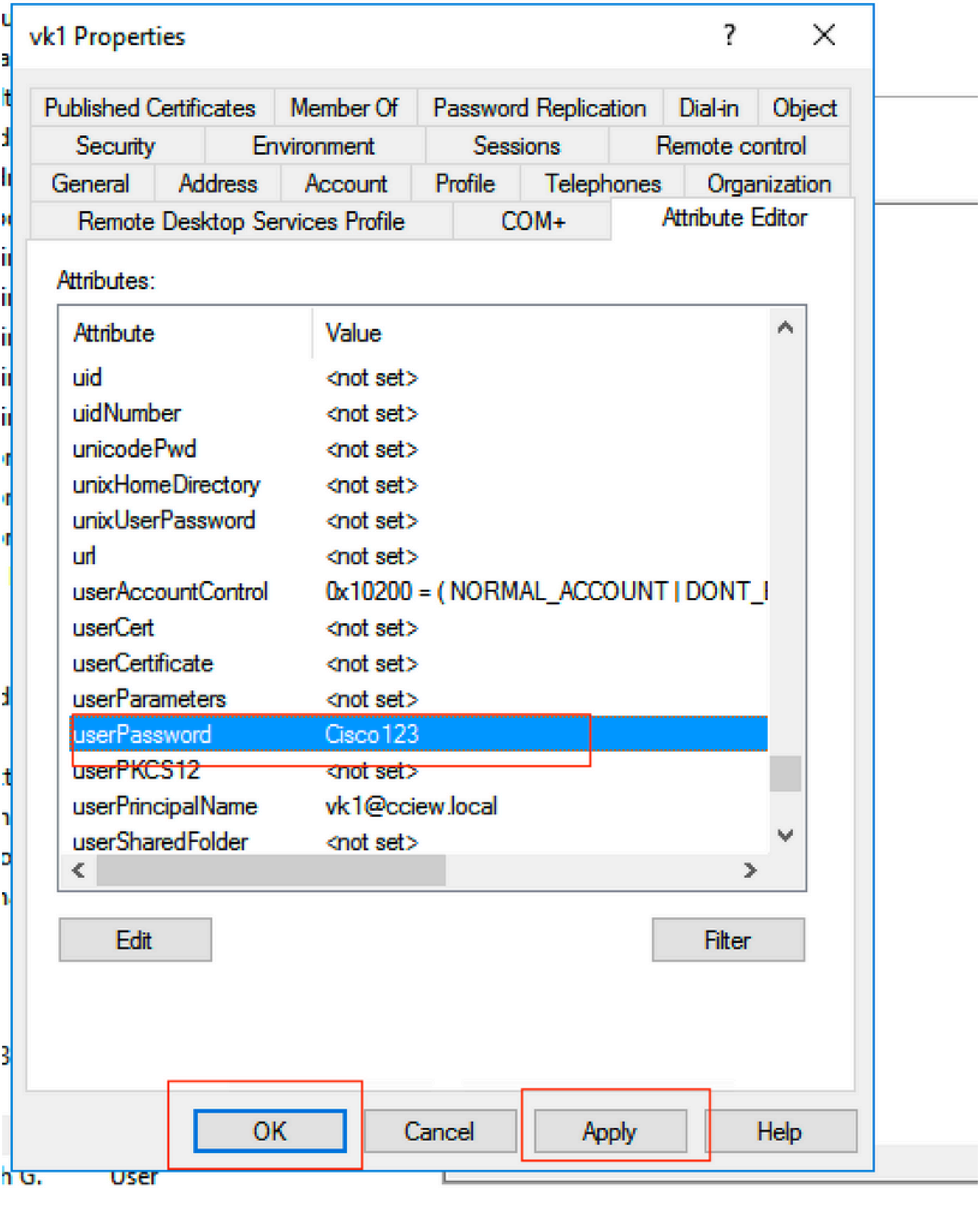


Attribute: userPassword

Values:

Cisco123

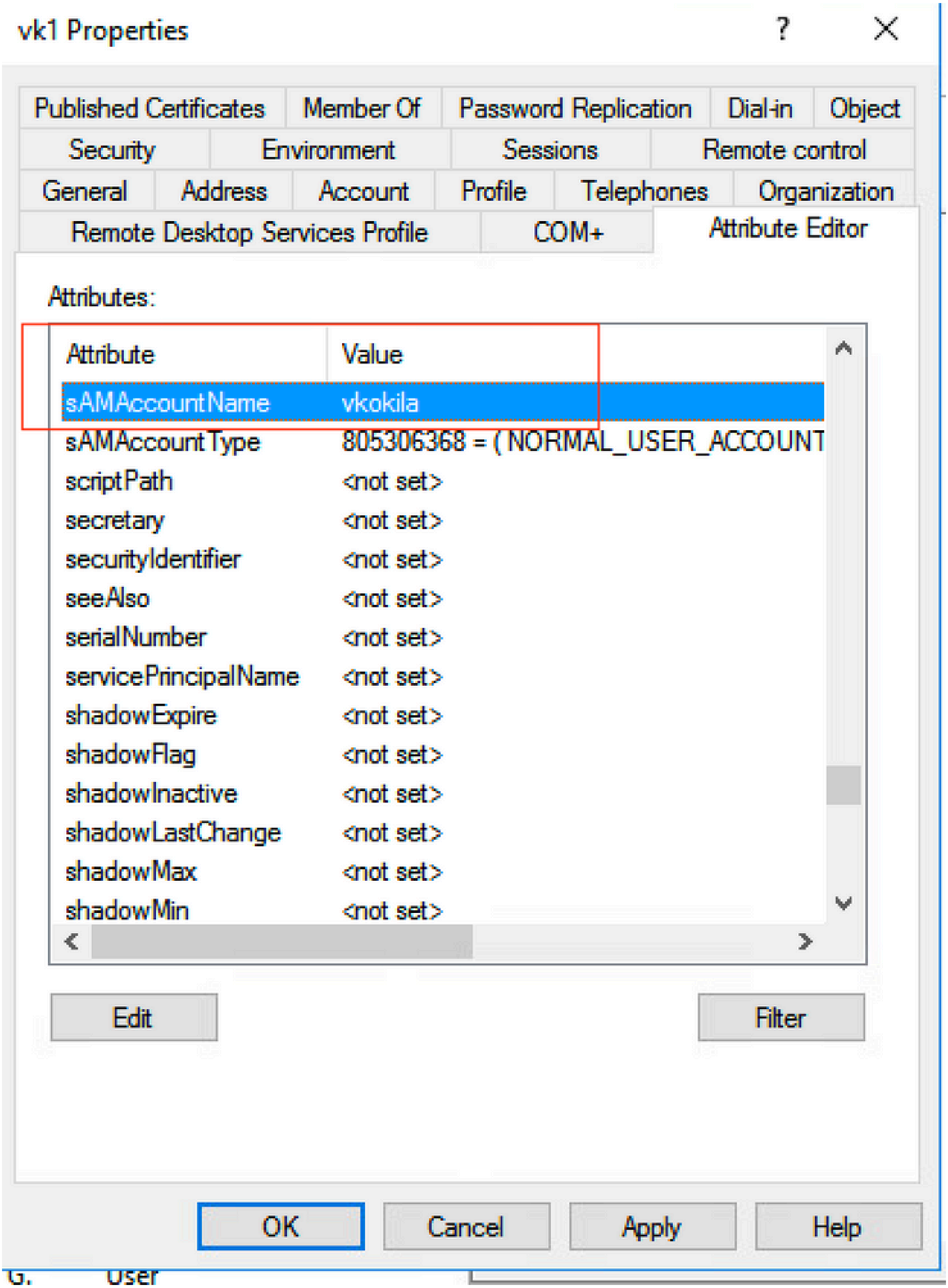
Étape 5. Cliquez sur Apply, puis sur OK



Attributes:

Attribute	Value
uid	<not set>
uidNumber	<not set>
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	Cisco123
userPKCS12	<not set>
userPrincipalName	vk1@cciew.local
userSharedFolder	<not set>

Étape 6 : vérification de la valeur de l'attribut « sAMAccountName » pour l'utilisateur et vérification du nom d'utilisateur pour l'authentification



Attributes:

Attribute	Value
sAMAccountName	vkokila
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	<not set>
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>
shadowMax	<not set>
shadowMin	<not set>

Configuration WLC :

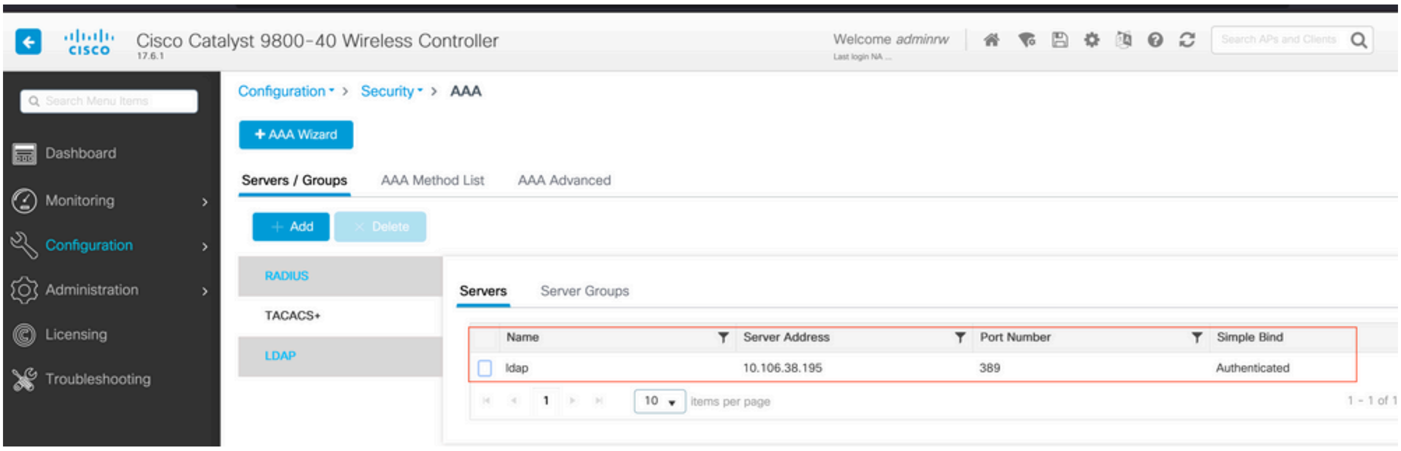
Étape 1 : création d’un MAP d’attribut LDAP

Étape 2. Configurer l'attribut « sAMAccountName » et entrer « username »

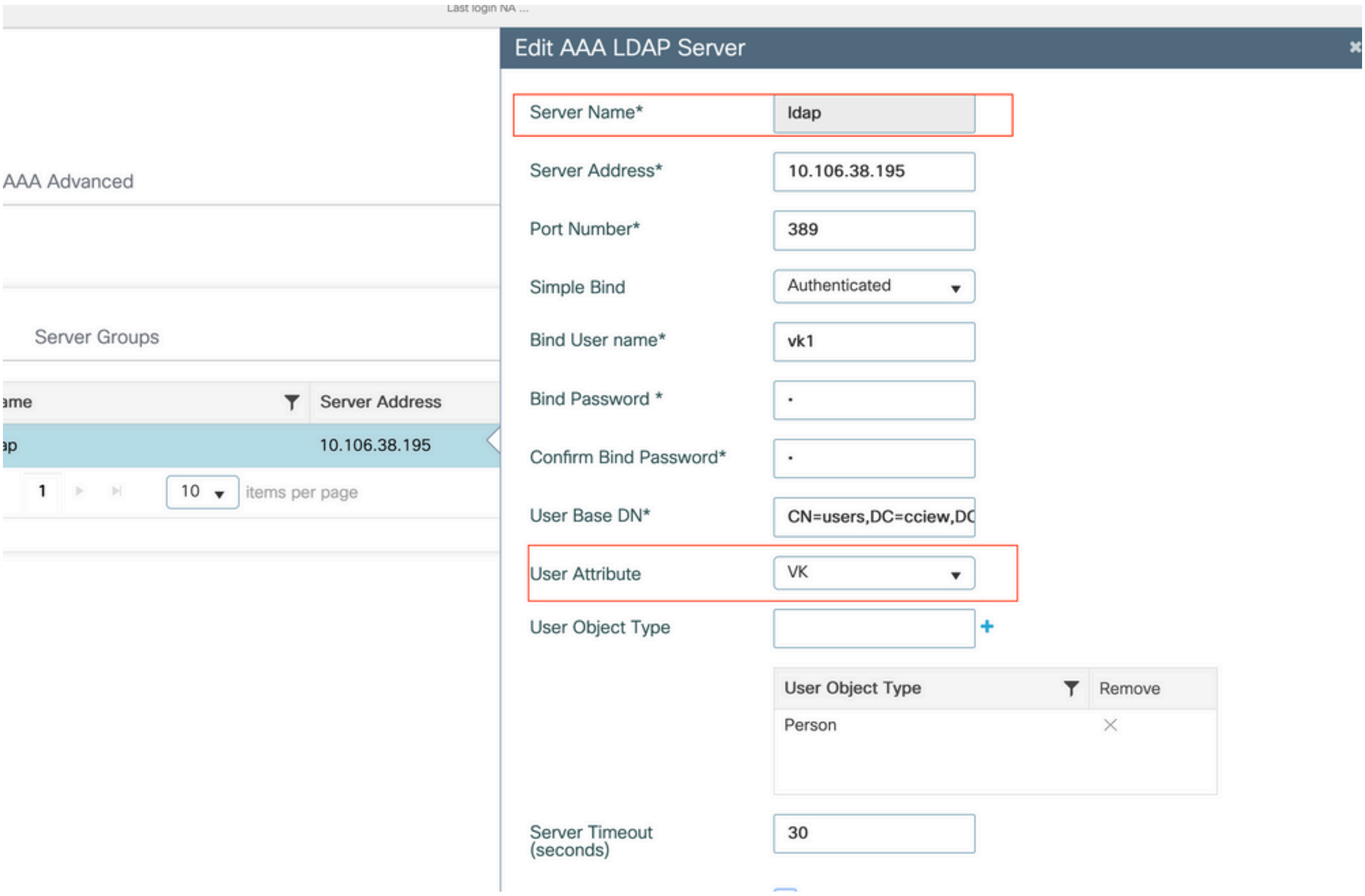
Étape 3. Choisissez l'attribut créé MAP sous la configuration du serveur LDAP.

```
ldap attribute-map VK

 map type sAMAccountName username




ldap server ldap

 ipv4 10.106.38.195

 attribute map VK

 bind authenticate root-dn vk1 password 7 00271A1507545A545C

 base-dn CN=users,DC=cciew,DC=local

 search-filter user-object-type Person
```

Vérifiez à partir de l'interface Web :



	Name	Server Address	Port Number	Simple Bind
□	ldap	10.106.38.195	389	Authenticated



Last login NA ...

Edit AAA LDAP Server

AAA Advanced

Server Groups

ame	Server Address
ap	10.106.38.195

1 ▸ ▸| 10 ▾ items per page

Server Name*	ldap
Server Address*	10.106.38.195
Port Number*	389
Simple Bind	Authenticated ▾
Bind User name*	vk1
Bind Password *	·
Confirm Bind Password*	·
User Base DN*	CN=users,DC=cciew,DC
User Attribute	VK ▾
User Object Type	+

User Object Type	Remove
Person	×

Server Timeout (seconds)	30

Vérification

Pour vérifier votre configuration, vérifiez à nouveau les commandes CLI avec celles de cet article.

Les bases de données LDAP ne fournissent généralement pas de journaux d'authentification. Il peut donc être difficile de savoir ce qui se passe. Consultez la section Dépannage de cet article pour savoir comment effectuer des suivis et une capture de renifleur afin de voir si une connexion est établie avec la base de données LDAP ou non.

Dépannage

Pour résoudre ce problème, il est préférable de le diviser en deux parties. La première partie consiste à valider la partie EAP local. La seconde consiste à vérifier que le 9800 communique correctement avec le serveur LDAP.

Comment vérifier le processus d'authentification sur le contrôleur

Vous pouvez collecter une trace Radioactive afin d'obtenir les "debugs" de la connexion client.

Accédez simplement à **Troubleshooting > Radioactive Trace**. Ajoutez l'adresse MAC du client (attention, votre client peut utiliser un MAC aléatoire et non son propre MAC, vous pouvez le vérifier dans le profil SSID sur le périphérique client lui-même) et appuyez sur Démarrer.

Une fois que vous avez reproduit la tentative de connexion, vous pouvez cliquer sur "Générer" et obtenir les journaux pour les X dernières minutes. Assurez-vous de cliquer sur **internal** car certaines lignes de journal LDAP n'apparaissent pas si vous ne l'activez pas.

Voici un exemple de trace radiocative d'un client s'authentifiant avec succès sur un SSID d'authentification Web. Certaines pièces redondantes ont été supprimées pour plus de clarté :

```
2021/01/19 21:57:55.890953 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (note): MAC:
2e1f.3a65.9c09 Association received. BSSID f80f.6f15.66ae, WLAN webauth, Slot 1 AP
f80f.6f15.66a0, AP7069-5A74-933C 2021/01/19 21:57:55.891049 {wncd_x_R0-0}{1}: [client-orch-sm]
[9347]: (debug): MAC: 2e1f.3a65.9c09 Received Dot11 association request. Processing
started,SSID: webauth, Policy profile: LDAP, AP Name: AP7069-5A74-933C, Ap Mac Address:
f80f.6f15.66a0 BSSID MAC0000.0000.0000 wlan ID: 2RSSI: -45, SNR: 0 2021/01/19 21:57:55.891282
{wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 Client state
transition: S_CO_INIT -> S_CO_ASSOCIATING 2021/01/19 21:57:55.891674 {wncd_x_R0-0}{1}: [dot11-
validate] [9347]: (info): MAC: 2e1f.3a65.9c09 WiFi direct: Dot11 validate P2P IE. P2P IE not
present. 2021/01/19 21:57:55.892114 {wncd_x_R0-0}{1}: [dot11] [9347]: (debug): MAC:
2e1f.3a65.9c09 dot11 send association response. Sending association response with
resp_status_code: 0 2021/01/19 21:57:55.892182 {wncd_x_R0-0}{1}: [dot11-frame] [9347]: (info):
MAC: 2e1f.3a65.9c09 WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
2021/01/19 21:57:55.892248 {wncd_x_R0-0}{1}: [dot11] [9347]: (info): MAC: 2e1f.3a65.9c09 dot11
send association response. Sending assoc response of length: 179 with resp_status_code: 0,
DOT11_STATUS: DOT11_STATUS_SUCCESS 2021/01/19 21:57:55.892467 {wncd_x_R0-0}{1}: [dot11] [9347]:
(note): MAC: 2e1f.3a65.9c09 Association success. AID 2, Roaming = False, WGB = False, 11r =
False, 11w = False 2021/01/19 21:57:55.892497 {wncd_x_R0-0}{1}: [dot11] [9347]: (info): MAC:
2e1f.3a65.9c09 DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED 2021/01/19
21:57:55.892616 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09 Station
Dot11 association is successful. 2021/01/19 21:57:55.892730 {wncd_x_R0-0}{1}: [client-orch-sm]
[9347]: (debug): MAC: 2e1f.3a65.9c09 Starting L2 authentication. Bssid in state
machine:f80f.6f15.66ae Bssid in request is:f80f.6f15.66ae 2021/01/19 21:57:55.892783 {wncd_x_R0-
0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 Client state transition:
S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS 2021/01/19 21:57:55.892896 {wncd_x_R0-0}{1}:
[client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 L2 Authentication initiated. method WEBAUTH,
Policy VLAN 1,AAA override = 0 2021/01/19 21:57:55.893115 {wncd_x_R0-0}{1}: [auth-mgr] [9347]:
(info): [2e1f.3a65.9c09:capwap_90000004] Session Start event called from SANET-SHIM with
conn_hdl 14, vlan: 0 2021/01/19 21:57:55.893154 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Wireless session sequence, create context with method WebAuth
2021/01/19 21:57:55.893205 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] - authc_list: ldapauth 2021/01/19 21:57:55.893211 {wncd_x_R0-
0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] - authz_list:
Not present under wlan configuration 2021/01/19 21:57:55.893254 {wncd_x_R0-0}{1}: [client-auth]
[9347]: (info): MAC: 2e1f.3a65.9c09 Client auth-interface state transition: S_AUTHIF_INIT ->
S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP 2021/01/19 21:57:55.893461 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:unknown] auth mgr attr change notification is received for attr
(952) 2021/01/19 21:57:55.893532 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1263)
2021/01/19 21:57:55.893603 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (220)
2021/01/19 21:57:55.893649 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (952)
2021/01/19 21:57:55.893679 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Retrieved Client IIF ID 0xd3001364 2021/01/19 21:57:55.893731
{wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Allocated audit
session id 000000000000009C1CA610D7 2021/01/19 21:57:55.894285 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Device type found in cache Samsung Galaxy S10e
2021/01/19 21:57:55.894299 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Device type for the session is detected as Samsung Galaxy S10e
and old device-type not classified earlier &Device name for the session is detected as Unknown
Device and old device-name not classified earlier & Old protocol map 0 and new is 1057
2021/01/19 21:57:55.894551 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1337)
2021/01/19 21:57:55.894587 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:57:55.894593
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:57:55.894827 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received
```

```
for attr (1337) 2021/01/19 21:57:55.894858 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]:
(info): [2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:57:55.894862
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:57:55.895918 {wncd_x_R0-0}{1}: [auth-mgr-
feat_wireless] [9347]: (info): [0000.0000.0000:unknown] retrieving vlanid from name failed
2021/01/19 21:57:55.896094 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] SM Reauth Plugin: Received valid timeout = 86400 2021/01/19
21:57:55.896807 {wncd_x_R0-0}{1}: [webauth-sm] [9347]: (info): [ 0.0.0.0]Starting Webauth, mac
[2e:1f:3a:65:9c:09],IIF 0 , audit-ID 000000000000009C1CA610D7 2021/01/19 21:57:55.897106
{wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
0.0.0.0]Applying IPv4 intercept ACL via SVM, name: IP-Adm-V4-Int-ACL-global, priority: 50, IIF-
ID: 0 2021/01/19 21:57:55.897790 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info):
[0000.0000.0000:unknown] URL-Redirect-ACL = IP-Adm-V4-Int-ACL-global 2021/01/19 21:57:55.898813
{wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
0.0.0.0]Applying IPv6 intercept ACL via SVM, name: IP-Adm-V6-Int-ACL-global, priority: 52, IIF-
ID: 0 2021/01/19 21:57:55.899406 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info):
[0000.0000.0000:unknown] URL-Redirect-ACL = IP-Adm-V6-Int-ACL-global 2021/01/19 21:57:55.903552
{wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client auth-interface state
transition: S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP -> S_AUTHIF_L2_WEBAUTH_PENDING 2021/01/19
21:57:55.903575 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [9347]: (note): Authentication Success.
Resolved Policy bitmap:11 for client 2e1f.3a65.9c09 2021/01/19 21:57:55.903592 {wncd_x_R0-0}{1}:
[client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client auth-interface state transition:
S_AUTHIF_L2_WEBAUTH_PENDING -> S_AUTHIF_L2_WEBAUTH_PENDING 2021/01/19 21:57:55.903709
{wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client auth-interface state
transition: S_AUTHIF_L2_WEBAUTH_PENDING -> S_AUTHIF_L2_WEBAUTH_DONE 2021/01/19 21:57:55.903774
{wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Device type for
the session is detected as Samsung Galaxy S10e and old Samsung Galaxy S10e &Device name for the
session is detected as Unknown Device and old Unknown Device & Old protocol map 1057 and new is
1025 2021/01/19 21:57:55.903858 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Device type for the session is detected as Samsung Galaxy S10e
and old Samsung Galaxy S10e &Device name for the session is detected as Unknown Device and old
Unknown Device & Old protocol map 1057 and new is 1025 2021/01/19 21:57:55.903924 {wncd_x_R0-
0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Device type for the session
is detected as Samsung Galaxy S10e and old Samsung Galaxy S10e &Device name for the session is
detected as Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1025
2021/01/19 21:57:55.904005 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC:
2e1f.3a65.9c09 L2 Authentication of station is successful., L3 Authentication : 1 2021/01/19
21:57:55.904173 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (note): MAC: 2e1f.3a65.9c09 Mobility
discovery triggered. Client mode: Flex - Local Switching 2021/01/19 21:57:55.904181 {wncd_x_R0-
0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 Client state transition:
S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS 2021/01/19 21:57:55.904245
{wncd_x_R0-0}{1}: [mm-transition] [9347]: (info): MAC: 2e1f.3a65.9c09 MMIF FSM transition:
S_MA_INIT -> S_MA_MOBILITY_DISCOVERY_PROCESSED_TR on E_MA_MOBILITY_DISCOVERY 2021/01/19
21:57:55.904410 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Invalid
transmitter ip in build client context 2021/01/19 21:57:55.904777 {wncd_x_R0-0}{1}: [mm-client]
[9347]: (debug): MAC: 2e1f.3a65.9c09 Received mobile_announce, sub type: 0 of XID (0) from
(WNCD[0]) 2021/01/19 21:57:55.904955 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC:
2e1f.3a65.9c09 Add MCC by tdl mac: client_ifid 0x90000006 is assigned to client 2021/01/19
21:57:55.905072 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 0000.0000.0000 Sending
mobile_announce_nak of XID (0) to (WNCD[0]) 2021/01/19 21:57:55.905157 {wncd_x_R0-0}{1}: [mm-
client] [9347]: (debug): MAC: 2e1f.3a65.9c09 Received mobile_announce_nak, sub type: 1 of XID
(0) from (WNCD[0]) 2021/01/19 21:57:55.905267 {wncd_x_R0-0}{1}: [mm-transition] [9347]: (info):
MAC: 2e1f.3a65.9c09 MMIF FSM transition: S_MA_INIT_WAIT_ANNOUNCE_RSP -> S_MA_NAK_PROCESSED_TR on
E_MA_NAK_RCVD 2021/01/19 21:57:55.905283 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC:
2e1f.3a65.9c09 Roam type changed - None -> None 2021/01/19 21:57:55.905317 {wncd_x_R0-0}{1}:
[mm-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Mobility role changed - Unassoc -> Local
2021/01/19 21:57:55.905515 {wncd_x_R0-0}{1}: [mm-client] [9347]: (note): MAC: 2e1f.3a65.9c09
Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Client IFID:
0x90000006, Client Role: Local PoA: 0x90000004 PoP: 0x0 2021/01/19 21:57:55.905570 {wncd_x_R0-
0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09 Processing mobility response from
MMIF. Client ifid: 0x90000006, roam type: None, client role: Local 2021/01/19 21:57:55.906210
{wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Client QoS add mobile cb
2021/01/19 21:57:55.906369 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC:
2e1f.3a65.9c09 No QoS PM Name or QoS Level received from SANet for pm_dir:0. Check client is
```

```
fastlane, otherwise set pm name to none 2021/01/19 21:57:55.906399 {wncd_x_R0-0}{1}: [ewlc-qos-
client] [9347]: (info): MAC: 2e1f.3a65.9c09 No QoS PM Name or QoS Level received from SANet for
pm_dir:1. Check client is fastlane, otherwise set pm name to none 2021/01/19 21:57:55.906486
{wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 ADD MOBILE sent. Client
state flags: 0x12 BSSID: MAC: f80f.6f15.66ae capwap IFID: 0x90000004 2021/01/19 21:57:55.906613
{wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 Client state
transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS 2021/01/19
21:57:55.907326 {wncd_x_R0-0}{1}: [dot11] [9347]: (note): MAC: 2e1f.3a65.9c09 Client datapath
entry params - ssid:webauth,slot_id:1 bssid ifid: 0x0, radio_ifid: 0x90000002, wlan_ifid:
0xf0400002 2021/01/19 21:57:55.907544 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC:
2e1f.3a65.9c09 Client QoS dpath create params 2021/01/19 21:57:55.907594 {wncd_x_R0-0}{1}: [avc-
afc] [9347]: (debug): AVC enabled for client 2e1f.3a65.9c09 2021/01/19 21:57:55.907701
{wncd_x_R0-0}{1}: [dpath_svc] [9347]: (note): MAC: 2e1f.3a65.9c09 Client datapath entry created
for ifid 0x90000006 2021/01/19 21:57:55.908229 {wncd_x_R0-0}{1}: [client-orch-state] [9347]:
(note): MAC: 2e1f.3a65.9c09 Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS ->
S_CO_IP_LEARN_IN_PROGRESS 2021/01/19 21:57:55.908704 {wncd_x_R0-0}{1}: [client-iplearn] [9347]:
(info): MAC: 2e1f.3a65.9c09 IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
2021/01/19 21:57:55.918694 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
2021/01/19 21:57:55.922254 {wncd_x_R0-0}{1}: [dot11k] [9347]: (info): MAC: 2e1f.3a65.9c09
Neighbor AP fc5b.3984.8220 lookup has failed, ap contextnot available on this instance
2021/01/19 21:57:55.922260 {wncd_x_R0-0}{1}: [dot11k] [9347]: (info): MAC: 2e1f.3a65.9c09
Neighbor AP 88f0.3169.d390 lookup has failed, ap contextnot available on this instance
2021/01/19 21:57:55.962883 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (note): MAC:
2e1f.3a65.9c09 Client IP learn successful. Method: IP Snooping IP: 192.168.1.17 2021/01/19
21:57:55.963827 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 Client IP
learn successful. Method: IPv6 Snooping IP: fe80::2c1f:3aff:fe65:9c09 2021/01/19 21:57:55.964481
{wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] auth mgr attr
change notification is received for attr (8) 2021/01/19 21:57:55.965176 {wncd_x_R0-0}{1}:
[client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 IP-learn state transition:
S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE 2021/01/19 21:57:55.965550 {wncd_x_R0-0}{1}: [auth-
mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is
received for attr (10) 2021/01/19 21:57:55.966127 {wncd_x_R0-0}{1}: [client-iplearn] [9347]:
(info): MAC: 2e1f.3a65.9c09 IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
2021/01/19 21:57:55.966328 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC:
2e1f.3a65.9c09 Received ip learn response. method: IPLEARN_METHOD_IP_SNOOPING 2021/01/19
21:57:55.966413 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09
Triggered L3 authentication. status = 0x0, Success 2021/01/19 21:57:55.966424 {wncd_x_R0-0}{1}:
[client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 Client state transition:
S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS 2021/01/19 21:57:55.967404 {wncd_x_R0-
0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 L3 Authentication initiated. LWA
2021/01/19 21:57:55.967433 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING
2021/01/19 21:57:55.968312 {wncd_x_R0-0}{1}: [sisf-packet] [9347]: (debug): RX: ARP from
interface capwap_90000004 on vlan 1 Source MAC: 2e1f.3a65.9c09 Dest MAC: ffff.ffff.ffff ARP
REQUEST, ARP sender MAC: 2e1f.3a65.9c09 ARP target MAC: ffff.ffff.ffff ARP sender IP:
192.168.1.17, ARP target IP: 192.168.1.17, 2021/01/19 21:57:55.968519 {wncd_x_R0-0}{1}: [client-
iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 iplearn receive client learn method update. Prev
method (IP Snooping) Cur method (ARP) 2021/01/19 21:57:55.968522 {wncd_x_R0-0}{1}: [client-
iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 Client IP learn method update successful. Method:
ARP IP: 192.168.1.17 2021/01/19 21:57:55.968966 {wncd_x_R0-0}{1}: [client-iplearn] [9347]:
(info): MAC: 2e1f.3a65.9c09 IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE
2021/01/19 21:57:57.762648 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC:
2e1f.3a65.9c09 iplearn receive client learn method update. Prev method (ARP) Cur method (IP
Snooping) 2021/01/19 21:57:57.762650 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC:
2e1f.3a65.9c09 Client IP learn method update successful. Method: IP Snooping IP: 192.168.1.17
2021/01/19 21:57:57.763032 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC:
2e1f.3a65.9c09 IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE 2021/01/19
21:58:00.992597 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]GET rcvd when in INIT state 2021/01/19
21:58:00.992617 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]HTTP GET request 2021/01/19 21:58:00.992669
{wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]Parse GET, src [192.168.1.17] dst [192.168.1.15] url
```

```
[http://connectivitycheck.gstatic.com/generate_204] 2021/01/19 21:58:00.992694 {wncd_x_R0-0}{1}:
[webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Retrieved user-
agent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/60.0.3112.32 Safari/537.36 2021/01/19 21:58:00.993558 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received
for attr (1248) 2021/01/19 21:58:00.993637 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]:
(info): [2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:00.993645
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:58:00.996320 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Device type for the session is detected as
Linux-Workstation and old Samsung Galaxy S10e &Device name for the session is detected as
Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19
21:58:00.996508 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] DC
Profile-name has been changed to Linux-Workstation 2021/01/19 21:58:00.996524 {wncd_x_R0-0}{1}:
[auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] update event: Policy is not applied
for this Handle 0xB7000080 2021/01/19 21:58:05.808144 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]:
(info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]HTTP GET request 2021/01/19
21:58:05.808226 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Parse GET, src [192.168.1.17] dst [192.168.1.15]
url [http://connectivitycheck.gstatic.com/generate_204] 2021/01/19 21:58:05.808251 {wncd_x_R0-
0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Retrieved
user-agent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/60.0.3112.32 Safari/537.36 2021/01/19 21:58:05.860465 {wncd_x_R0-0}{1}: [webauth-httpd]
[9347]: (info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]GET rcvd when in GET_REDIRECT
state 2021/01/19 21:58:05.860483 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]HTTP GET request 2021/01/19 21:58:05.860534
{wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]Parse GET, src [192.168.1.17] dst [192.168.1.15] url
[http://connectivitycheck.gstatic.com/generate_204] 2021/01/19 21:58:05.860559 {wncd_x_R0-0}{1}:
[webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Retrieved user-
agent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/60.0.3112.32 Safari/537.36 2021/01/19 21:58:06.628209 {wncd_x_R0-0}{1}: [webauth-httpd]
[9347]: (info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]GET rcvd when in GET_REDIRECT
state 2021/01/19 21:58:06.628228 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]HTTP GET request 2021/01/19 21:58:06.628287
{wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]Parse GET, src [192.168.1.17] dst [192.0.2.1] url
[https://192.0.2.1:443/login.html?redirect=http://connectivitycheck.gstatic.com/generate_204]
2021/01/19 21:58:06.628316 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Retrieved user-agent = Mozilla/5.0 (Linux; Android
11; SM-G970F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Mobile Safari/537.36
2021/01/19 21:58:06.628832 {wncd_x_R0-0}{1}: [webauth-page] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Sending Webauth login form, len 8077 2021/01/19
21:58:06.629613 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004]
auth mgr attr change notification is received for attr (1248) 2021/01/19 21:58:06.629699
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004]
Check aaa acct configured 2021/01/19 21:58:06.629709 {wncd_x_R0-0}{1}: [auth-mgr-feat_template]
[9347]: (info): [0000.0000.0000:capwap_90000004] access_session_acct_filter_spec is NULL
2021/01/19 21:58:06.633058 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Device type for the session is detected as Samsung Galaxy S10e
and old Linux-Workstation &Device name for the session is detected as Unknown Device and old
Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19 21:58:06.633219 {wncd_x_R0-
0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] DC Profile-name has been
changed to Samsung Galaxy S10e 2021/01/19 21:58:06.633231 {wncd_x_R0-0}{1}: [auth-mgr] [9347]:
(info): [2e1f.3a65.9c09:capwap_90000004] update event: Policy is not applied for this Handle
0xB7000080 2021/01/19 21:58:06.719502 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]GET rcvd when in LOGIN state 2021/01/19
21:58:06.719521 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]HTTP GET request 2021/01/19 21:58:06.719591
{wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]Parse GET, src [192.168.1.17] dst [192.0.2.1] url
[https://192.0.2.1:443/favicon.ico] 2021/01/19 21:58:06.719646 {wncd_x_R0-0}{1}: [webauth-httpd]
[9347]: (info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Retrieved user-agent = Mozilla/5.0
(Linux; Android 11; SM-G970F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Mobile
```

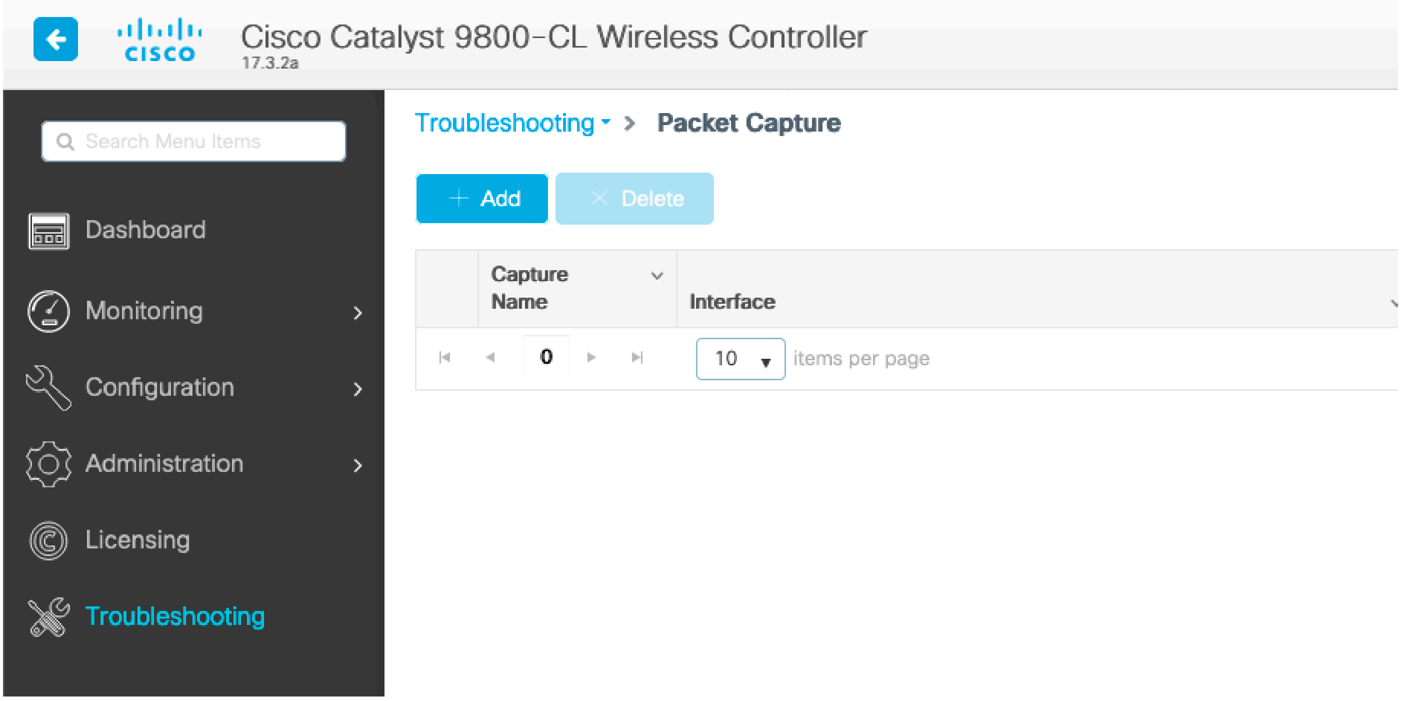
```
Safari/537.36 2021/01/19 21:58:06.720038 {wncd_x_R0-0}{1}: [webauth-error] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Parse logo GET, File "/favicon.ico" not found
2021/01/19 21:58:06.720623 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1248)
2021/01/19 21:58:06.720707 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:06.720716
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:58:06.724036 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Device type for the session is detected as
Samsung Galaxy S10e and old Samsung Galaxy S10e &Device name for the session is detected as
Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19
21:58:06.746127 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]GET rcvd when in LOGIN state 2021/01/19
21:58:06.746145 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]HTTP GET request 2021/01/19 21:58:06.746197
{wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]Parse GET, src [192.168.1.17] dst [192.0.2.1] url
[https://192.0.2.1:443/favicon.ico] 2021/01/19 21:58:06.746225 {wncd_x_R0-0}{1}: [webauth-httpd]
[9347]: (info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Retrieved user-agent = Mozilla/5.0
(Linux; Android 11; SM-G970F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Mobile
Safari/537.36 2021/01/19 21:58:06.746612 {wncd_x_R0-0}{1}: [webauth-error] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Parse logo GET, File "/favicon.ico" not found
2021/01/19 21:58:06.747105 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received for attr (1248)
2021/01/19 21:58:06.747187 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:06.747197
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:58:06.750598 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Device type for the session is detected as
Samsung Galaxy S10e and old Samsung Galaxy S10e &Device name for the session is detected as
Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19
21:58:15.902342 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]GET rcvd when in LOGIN state 2021/01/19
21:58:15.902360 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]HTTP GET request 2021/01/19 21:58:15.902410
{wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]Parse GET, src [192.168.1.17] dst [192.168.1.15] url
[http://connectivitycheck.gstatic.com/generate_204] 2021/01/19 21:58:15.902435 {wncd_x_R0-0}{1}:
[webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Retrieved user-
agent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/60.0.3112.32 Safari/537.36 2021/01/19 21:58:15.903173 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received
for attr (1248) 2021/01/19 21:58:15.903252 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]:
(info): [2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:15.903261
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:58:15.905950 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] Device type for the session is detected as
Linux-Workstation and old Samsung Galaxy S10e &Device name for the session is detected as
Unknown Device and old Unknown Device & Old protocol map 1057 and new is 1057 2021/01/19
21:58:15.906112 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] DC
Profile-name has been changed to Linux-Workstation 2021/01/19 21:58:15.906125 {wncd_x_R0-0}{1}:
[auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004] update event: Policy is not applied
for this Handle 0xB7000080 2021/01/19 21:58:16.357093 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]:
(info): capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]POST rcvd when in LOGIN state 2021/01/19
21:58:16.357443 {wncd_x_R0-0}{1}: [sadb-attr] [9347]: (info): Removing ipv6 addresses from the
attr list -1560276753,sm_ctx = 0x50840930, num_ipv6 = 1 2021/01/19 21:58:16.357674 {wncd_x_R0-
0}{1}: [caaa-authen] [9347]: (info): [CAAA:AUTHEN:b7000080] DEBUG: mlist=ldapauth for type=0
2021/01/19 21:58:16.374292 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Authc success from WebAuth, Auth event success 2021/01/19
21:58:16.374412 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [9347]: (note): Authentication Success.
Resolved Policy bitmap:0 for client 2e1f.3a65.9c09 2021/01/19 21:58:16.374442 {wncd_x_R0-0}{1}:
[client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client auth-interface state transition:
S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_PENDING 2021/01/19 21:58:16.374568 {wncd_x_R0-
0}{1}: [aaa-attr-inf] [9347]: (info): << username 0 "Nico">> 2021/01/19 21:58:16.374574
```

```
{wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): << sam-account-name 0 "Nico">> 2021/01/19
21:58:16.374584 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): << method 0 1 [webauth]>>
2021/01/19 21:58:16.374592 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): << clid-mac-addr 0
2e 1f 3a 65 9c 09 >> 2021/01/19 21:58:16.374597 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info):
<< intf-id 0 2415919108 (0x90000004)>> 2021/01/19 21:58:16.374690 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] auth mgr attr change notification is received
for attr (450) 2021/01/19 21:58:16.374797 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] Received User-Name Nico for client 2e1f.3a65.9c09 2021/01/19
21:58:16.375294 {wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]Applying IPv4 logout ACL via SVM, name: IP-Adm-V4-LOGOUT-ACL, priority: 51, IIF-ID:
0 2021/01/19 21:58:16.376120 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info):
[0000.0000.0000:unknown] URL-Redirect-ACL = IP-Adm-V4-LOGOUT-ACL 2021/01/19 21:58:16.377322
{wncd_x_R0-0}{1}: [webauth-page] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][
192.168.1.17]HTTP/1.0 200 OK 2021/01/19 21:58:16.378405 {wncd_x_R0-0}{1}: [client-auth] [9347]:
(note): MAC: 2e1f.3a65.9c09 L3 Authentication Successful. ACL:[] 2021/01/19 21:58:16.378426
{wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client auth-interface state
transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE 2021/01/19 21:58:16.379181
{wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Client QoS add mobile cb
2021/01/19 21:58:16.379323 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC:
2e1f.3a65.9c09 No QoS PM Name or QoS Level received from SANet for pm_dir:0. Check client is
fastlane, otherwise set pm name to none 2021/01/19 21:58:16.379358 {wncd_x_R0-0}{1}: [ewlc-qos-
client] [9347]: (info): MAC: 2e1f.3a65.9c09 No QoS PM Name or QoS Level received from SANet for
pm_dir:1. Check client is fastlane, otherwise set pm name to none 2021/01/19 21:58:16.379442
{wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 ADD MOBILE sent. Client
state flags: 0x8 BSSID: MAC: f80f.6f15.66ae capwap IFID: 0x90000004 2021/01/19 21:58:16.380547
{wncd_x_R0-0}{1}: [errmsg] [9347]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE:
Username entry (Nico) joined with ssid (webauth) for device with MAC: 2e1f.3a65.9c09 2021/01/19
21:58:16.380729 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute :bsn-vlan-
interface-name 0 "1" ] 2021/01/19 21:58:16.380736 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]:
(info): [ Applied attribute : timeout 0 86400 (0x15180) ] 2021/01/19 21:58:16.380812 {wncd_x_R0-
0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute : url-redirect-acl 0 "IP-Adm-V4-
LOGOUT-ACL" ] 2021/01/19 21:58:16.380969 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info):
MAC: 2e1f.3a65.9c09 Client QoS run state handler 2021/01/19 21:58:16.381033 {wncd_x_R0-0}{1}:
[rog-proxy-capwap] [9347]: (debug): Managed client RUN state notification: 2e1f.3a65.9c09
2021/01/19 21:58:16.381152 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC:
2e1f.3a65.9c09 Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN 2021/01/19
21:58:16.385252 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
QoS dpath run params 2021/01/19 21:58:16.385321 {wncd_x_R0-0}{1}: [avc-afc] [9347]: (debug): AVC
enabled for client 2e1f.3a65.9c09
```

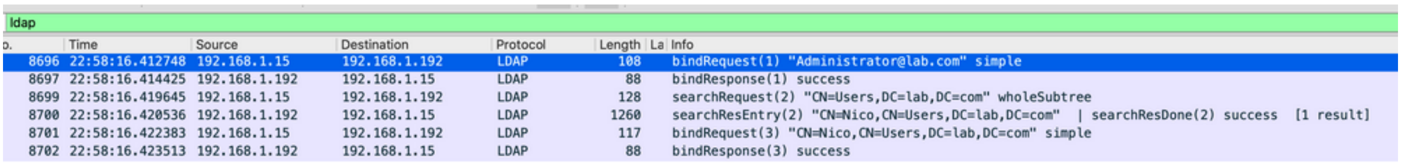
Vérification de la connectivité 9800 à LDAP

Vous pouvez prendre une capture intégrée dans le 9800 afin de voir quel trafic va vers LDAP.

Pour effectuer une capture à partir du WLC, accédez à **Troubleshooting > Packet Capture** et cliquez sur **+Add**. Sélectionnez le port de liaison ascendante et commencez la capture.



Voici un exemple d'authentification réussie pour l'utilisateur **Nico**



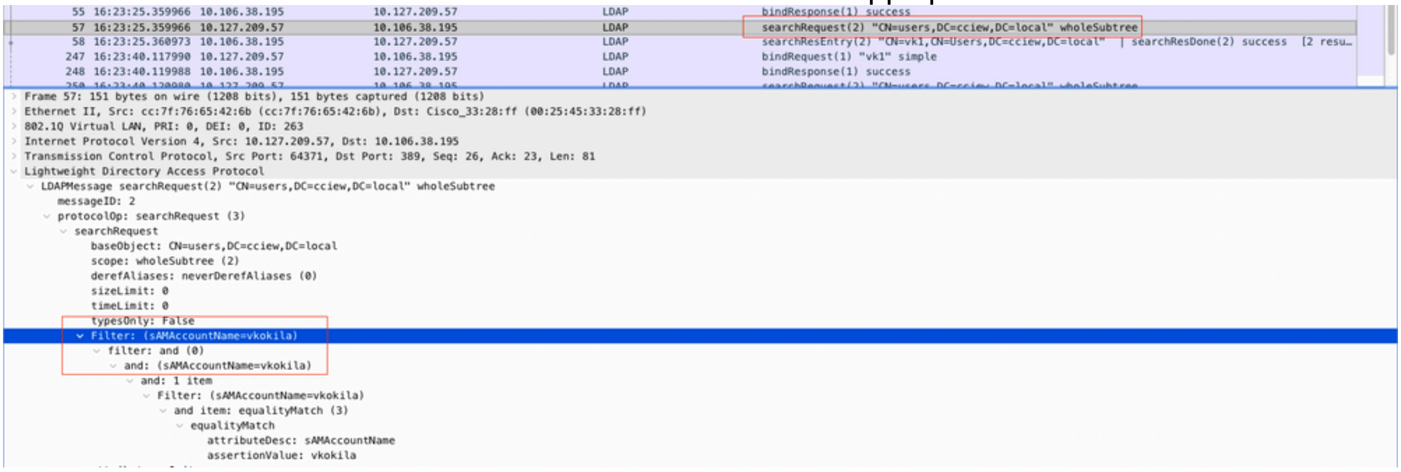
```
ldap
o.    Time             Source        Destination   Protocol  Length La Info
 8696 22:58:16.412748 192.168.1.15  192.168.1.192 LDAP       108     bindRequest(1) "Administrator@lab.com" simple
 8697 22:58:16.414425 192.168.1.192 192.168.1.15  LDAP        88     bindResponse(1) success
 8699 22:58:16.419645 192.168.1.15  192.168.1.192 LDAP       128     searchRequest(2) "CN=Users,DC=lab,DC=com" wholeSubtree
 8700 22:58:16.420536 192.168.1.192 192.168.1.15  LDAP      1260     searchResEntry(2) "CN=Nico,CN=Users,DC=lab,DC=com"  | searchResDone(2) success  [1 result]
 8701 22:58:16.422383 192.168.1.15  192.168.1.192 LDAP       117     bindRequest(3) "CN=Nico,CN=Users,DC=lab,DC=com" simple
 8702 22:58:16.423513 192.168.1.192 192.168.1.15  LDAP        88     bindResponse(3) success
```

Les 2 premiers paquets représentent la liaison WLC à la base de données LDAP, c'est-à-dire le WLC s'authentifiant auprès de la base de données avec l'utilisateur admin (afin de pouvoir effectuer une recherche).

Ces 2 paquets LDAP représentent le WLC effectuant une recherche dans le DN de base (ici CN=Users, DC=lab, DC=com). L'intérieur du paquet contient un filtre pour le nom d'utilisateur (ici "Nico"). La base de données LDAP renvoie les attributs utilisateur comme une réussite

Les 2 derniers paquets représentent le WLC essayant de s'authentifier avec ce mot de passe utilisateur pour tester si le mot de passe est le bon.

1. Collectez EPC et vérifiez si « sAMAccountName » est appliqué comme filtre :

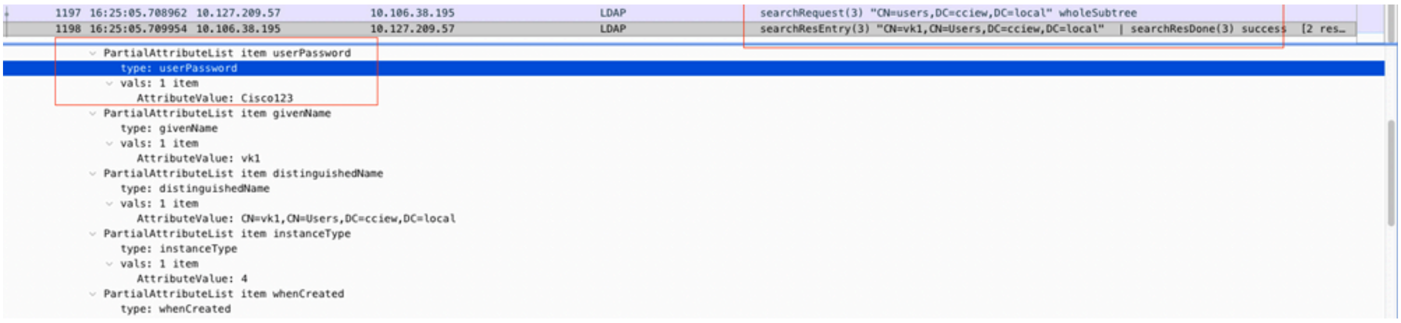


```
   55 16:23:25.359966 10.106.38.195   10.127.209.57   LDAP   bindResponse(1) success
   57 16:23:25.359966 10.127.209.57   10.106.38.195   LDAP   searchRequest(2) "CN=users,DC=cciew,DC=local" wholeSubtree
   58 16:23:25.360973 10.106.38.195   10.127.209.57   LDAP   searchResEntry(2) "CN=vk1,CN=Users,DC=cciew,DC=local"  | searchResDone(2) success  [2 resu…
  247 16:23:40.117990 10.127.209.57   10.106.38.195   LDAP   bindRequest(1) "vk1" simple
  248 16:23:40.119988 10.106.38.195   10.127.209.57   LDAP   bindResponse(1) success
  250 16:23:40.120080 10.127.209.57   10.106.38.195   LDAP   searchRequest(2) "CN=users,DC=cciew,DC=local" wholeSubtree
> Frame 57: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
> Ethernet II, Src: cc:7f:76:65:42:6b (cc:7f:76:65:42:6b), Dst: Cisco_33:28:ff (00:25:45:33:28:ff)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 263
> Internet Protocol Version 4, Src: 10.127.209.57, Dst: 10.106.38.195
> Transmission Control Protocol, Src Port: 64371, Dst Port: 389, Seq: 26, Ack: 23, Len: 81
v Lightweight Directory Access Protocol
  v LDAPMessage searchRequest(2) "CN=users,DC=cciew,DC=local" wholeSubtree
      messageID: 2
    v protocolOp: searchRequest (3)
      v searchRequest
          baseObject: CN=users,DC=cciew,DC=local
          scope: wholeSubtree (2)
          derefAliases: neverDerefAliases (0)
          sizeLimit: 0
          timeLimit: 0
          typesOnly: False
        v Filter: (sAMAccountName=vkokila)
          v filter: and (0)
            v and: (sAMAccountName=vkokila)
              v and: 1 item
                v Filter: (sAMAccountName=vkokila)
                  v and item: equalityMatch (3)
                    v equalityMatch
                        attributeDesc: sAMAccountName
                        assertionValue: vkokila
```

Si le filtre affiche « cn » et si « sAMAccountName » est utilisé comme nom d'utilisateur, l'authentification échoue.

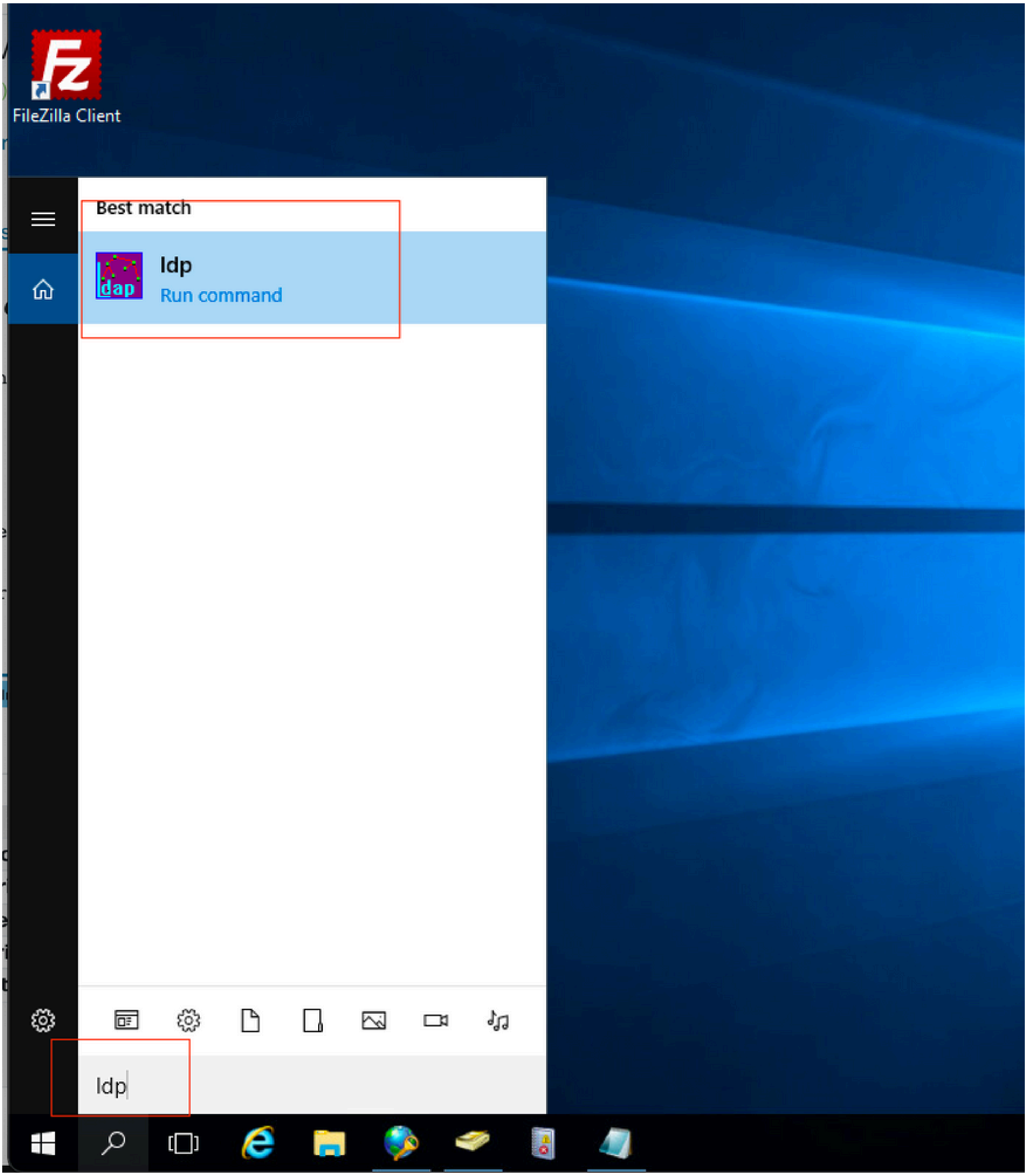
Reconfigurez l'attribut de mappage ldap à partir de l'interface de ligne de commande WLC.

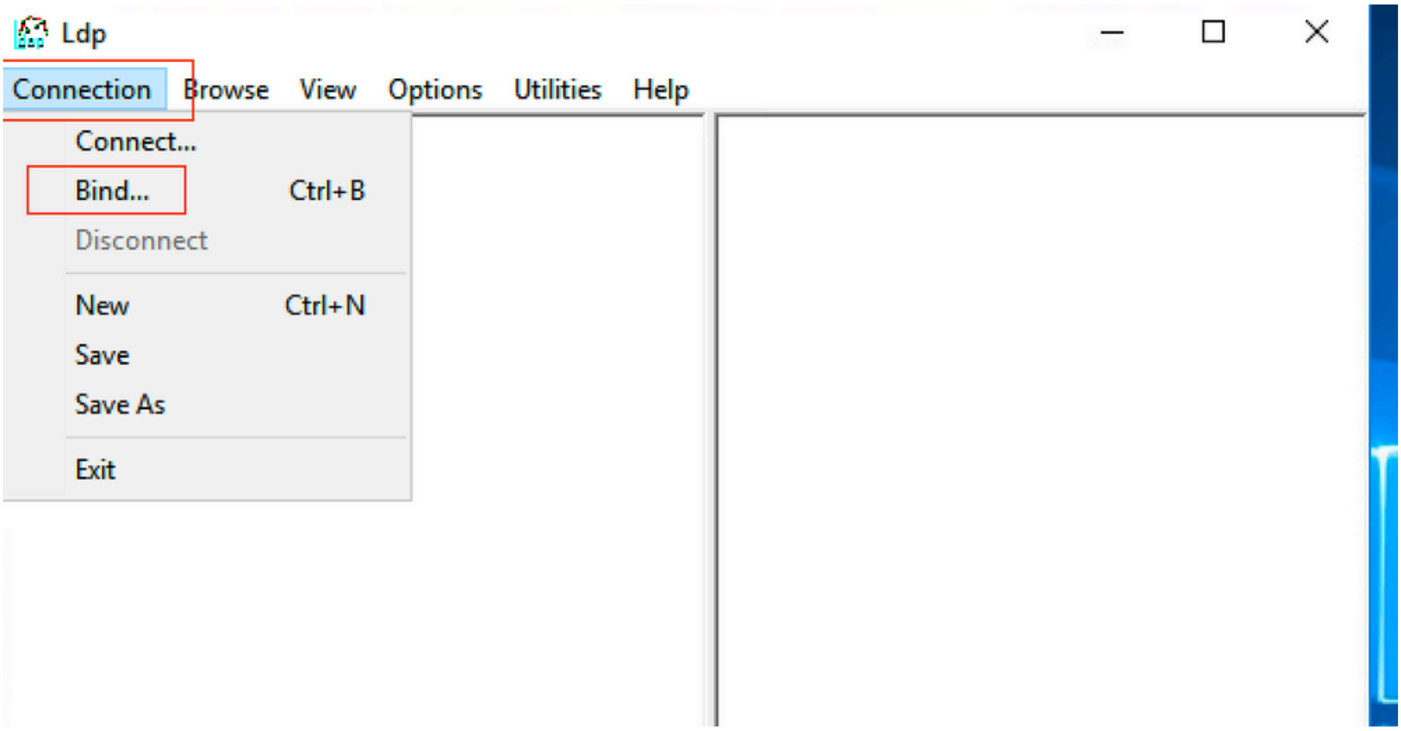
2. Assurez-vous que le serveur renvoie « userPassword » en texte clair, sinon l'authentification échoue.

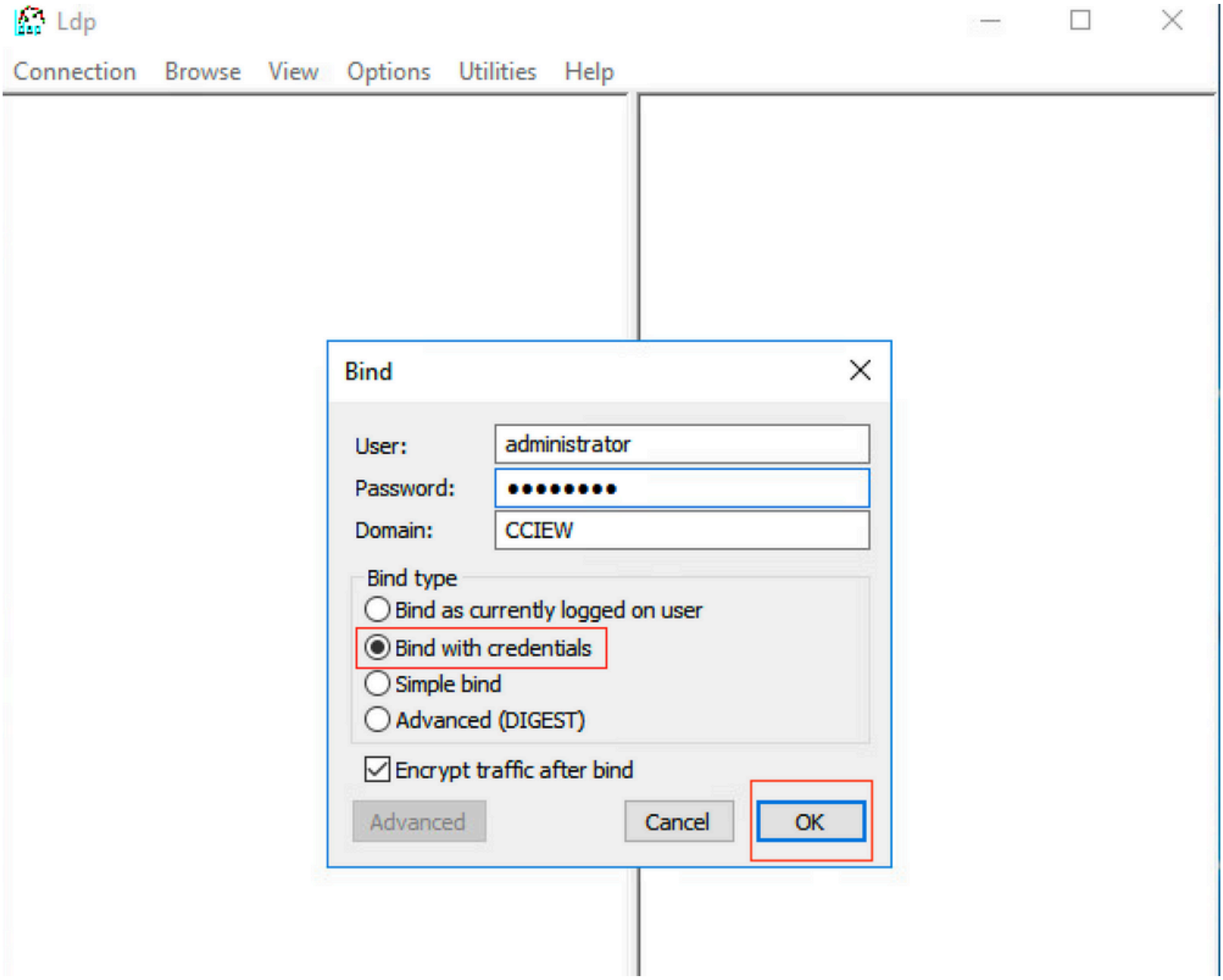


```
1197 16:25:05.708962 10.127.209.57    10.106.38.195    LDAP    searchRequest(3) "CN=users,DC=cciew,DC=local" wholeSubtree
1198 16:25:05.709954 10.106.38.195    10.127.209.57    LDAP    searchResEntry(3) "CN=vk1,CN=Users,DC=cciew,DC=local"  | searchResDone(3) success  [2 res…

    PartialAttributeList item userPassword
      type: userPassword
      vals: 1 item
        AttributeValue: Cisco123
    PartialAttributeList item givenName
      type: givenName
      vals: 1 item
        AttributeValue: vk1
    PartialAttributeList item distinguishedName
      type: distinguishedName
      vals: 1 item
        AttributeValue: CN=vk1,CN=Users,DC=cciew,DC=local
    PartialAttributeList item instanceType
      type: instanceType
      vals: 1 item
        AttributeValue: 4
    PartialAttributeList item whenCreated
      type: whenCreated
```

3. Utilisez l'outil ldp.exe sur le serveur pour valider les informations de nom unique de base.


FileZilla Client
Best match
ldp
Run command
ldp





User: administrator

Password: •••••••••

Domain: CCIEW

Bind type

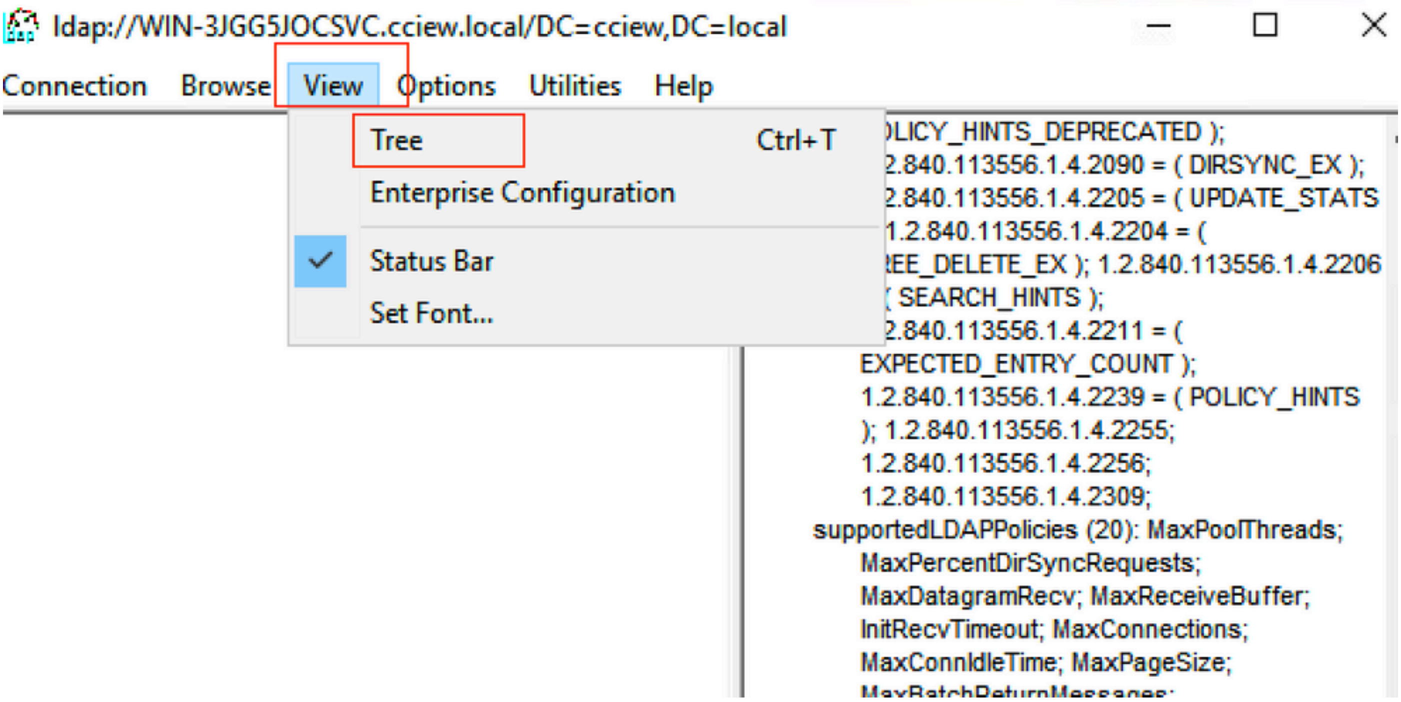
○ Bind as currently logged on user

● Bind with credentials

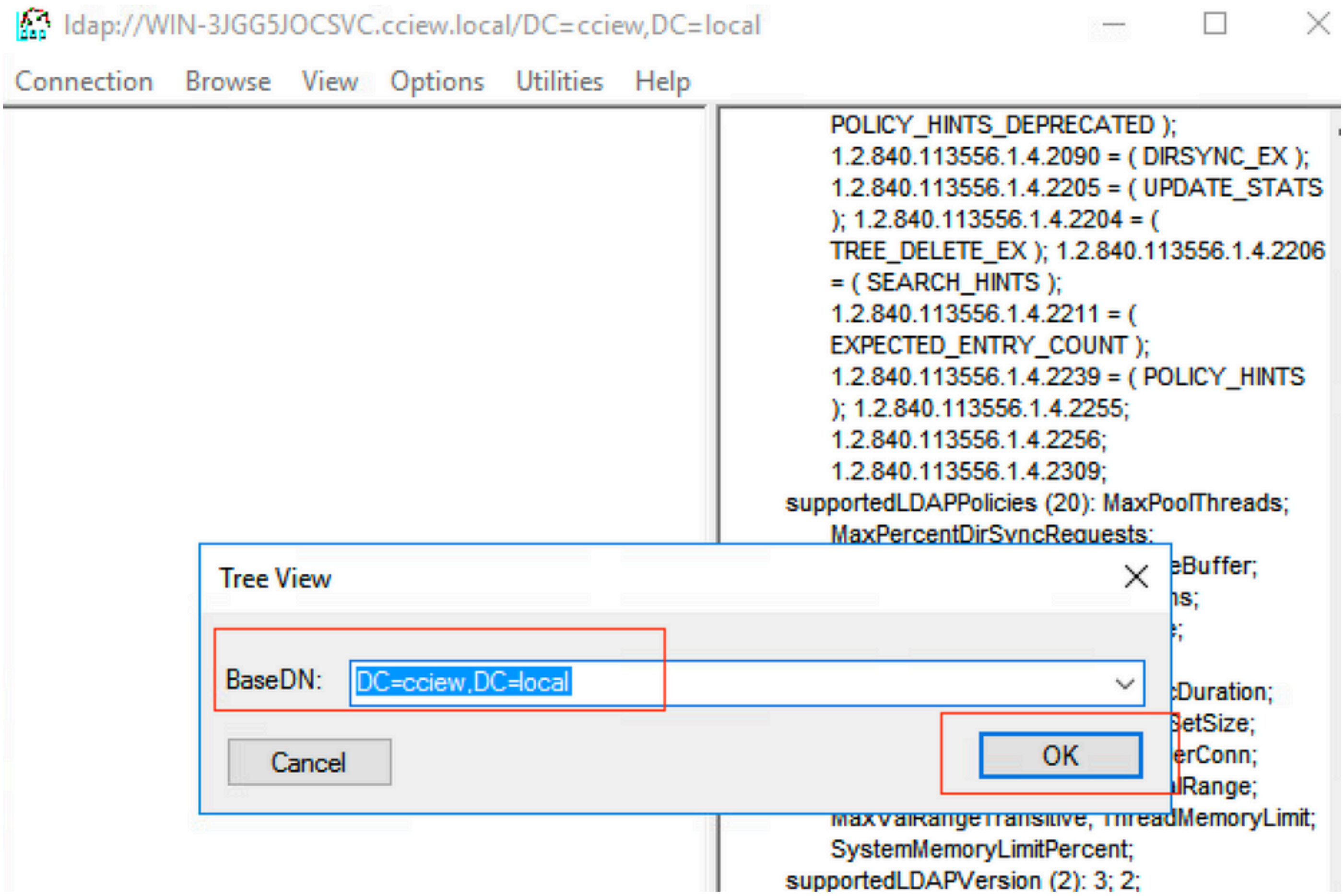
○ Simple bind

○ Advanced (DIGEST)

☑ Encrypt traffic after bind

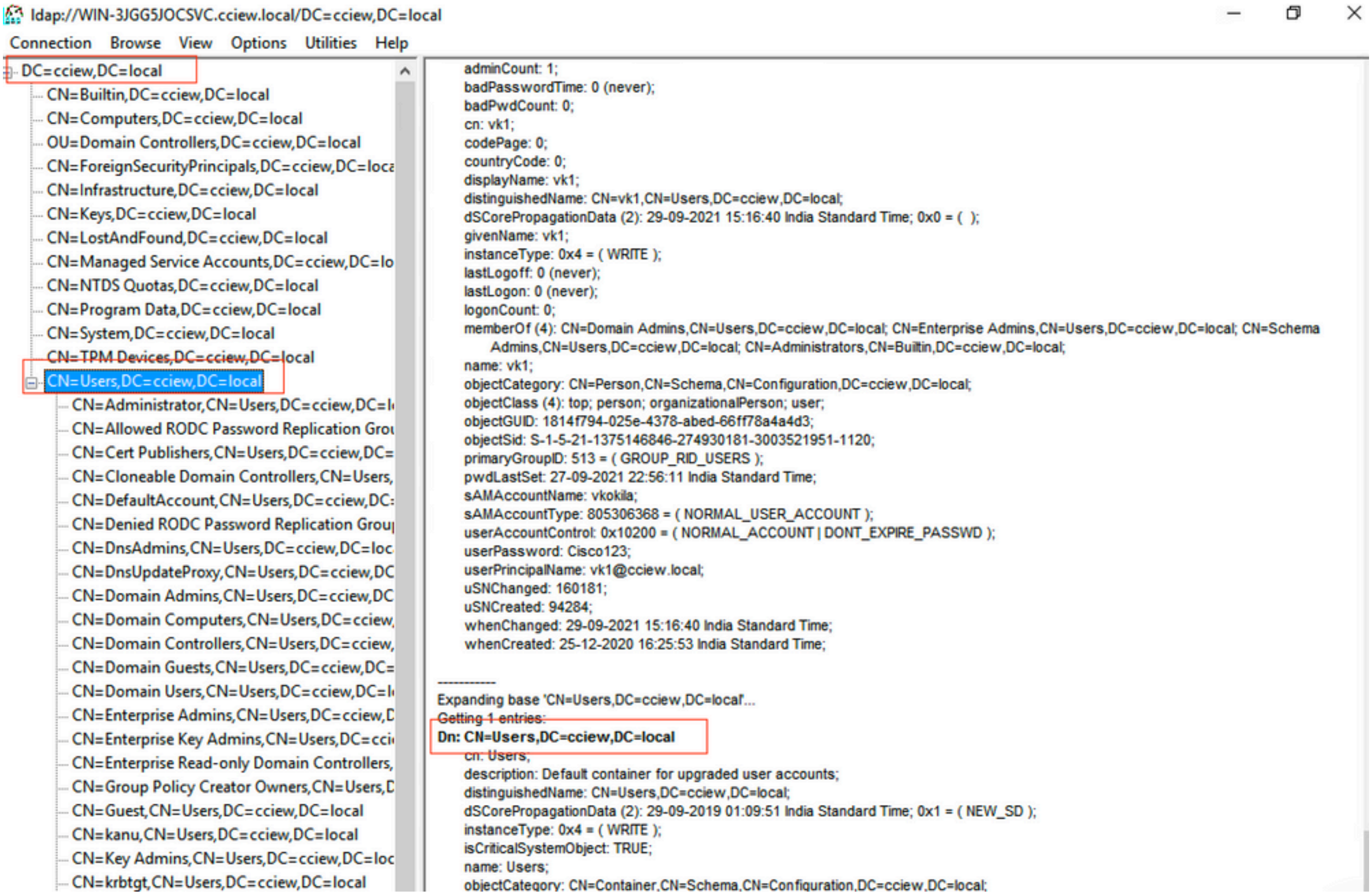


```
        )LICY_HINTS_DEPRECATED );
        2.840.113556.1.4.2090 = ( DIRSYNC_EX );
        2.840.113556.1.4.2205 = ( UPDATE_STATS
        1.2.840.113556.1.4.2204 = (
        REE_DELETE_EX ); 1.2.840.113556.1.4.2206
        ( SEARCH_HINTS );
        2.840.113556.1.4.2211 = (
        EXPECTED_ENTRY_COUNT );
        1.2.840.113556.1.4.2239 = ( POLICY_HINTS
        ); 1.2.840.113556.1.4.2255;
        1.2.840.113556.1.4.2256;
        1.2.840.113556.1.4.2309;
    supportedLDAPPolicies (20): MaxPoolThreads;
        MaxPercentDirSyncRequests;
        MaxDatagramRecv; MaxReceiveBuffer;
        InitRecvTimeout; MaxConnections;
        MaxConnIdleTime; MaxPageSize;
        MaxBatchReturnMessages;
```



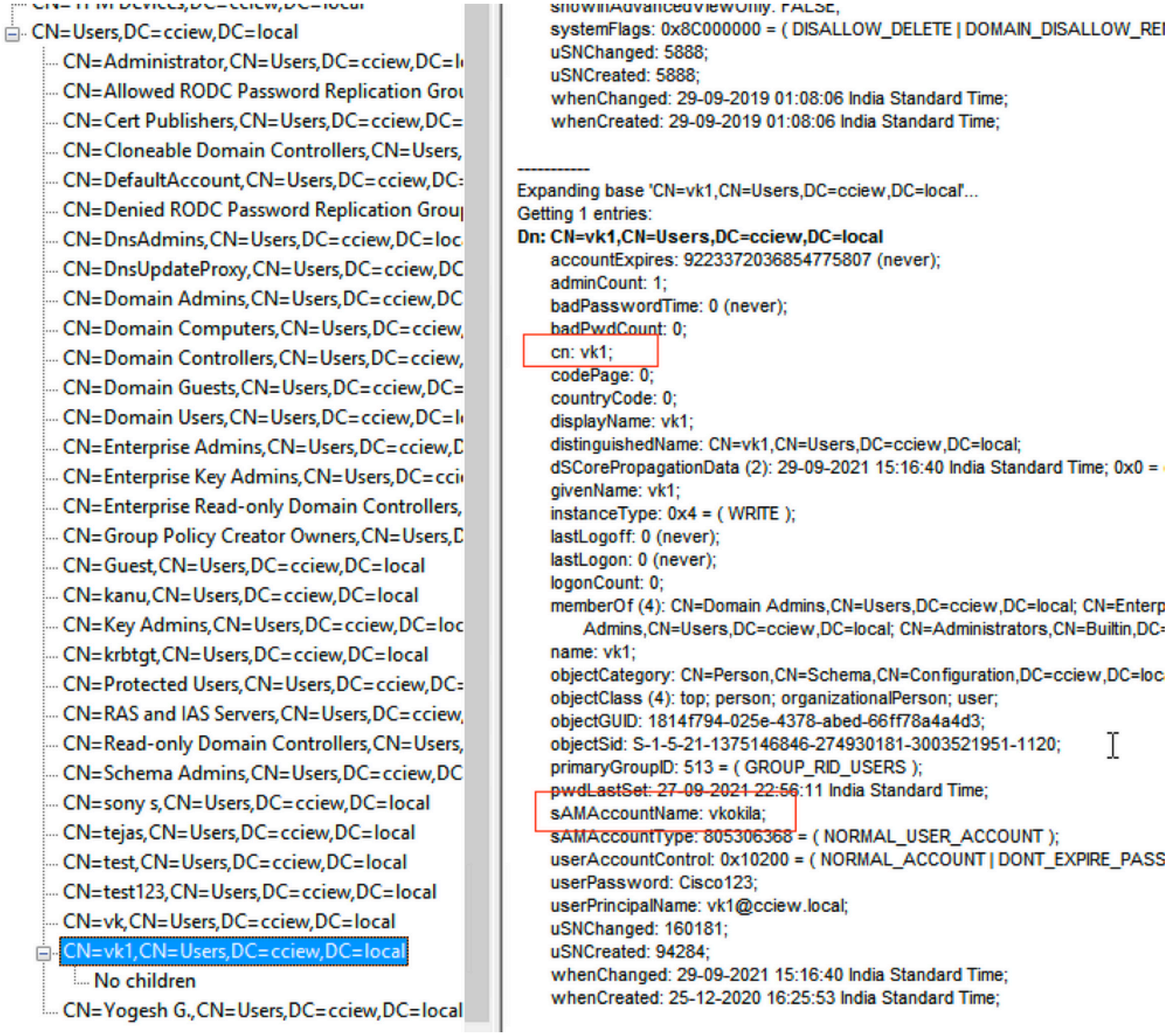
```
        POLICY_HINTS_DEPRECATED );
        1.2.840.113556.1.4.2090 = ( DIRSYNC_EX );
        1.2.840.113556.1.4.2205 = ( UPDATE_STATS
        ); 1.2.840.113556.1.4.2204 = (
        TREE_DELETE_EX ); 1.2.840.113556.1.4.2206
        = ( SEARCH_HINTS );
        1.2.840.113556.1.4.2211 = (
        EXPECTED_ENTRY_COUNT );
        1.2.840.113556.1.4.2239 = ( POLICY_HINTS
        ); 1.2.840.113556.1.4.2255;
        1.2.840.113556.1.4.2256;
        1.2.840.113556.1.4.2309;
    supportedLDAPPolicies (20): MaxPoolThreads;
        MaxPercentDirSyncRequests;
                                   eBuffer;
                                   ns;
                                   e;

                                   :Duration;
                                   SetSize;
                                   erConn;
                                   lRange;
        MaxValRangeTransitive; ThreadMemoryLimit;
        SystemMemoryLimitPercent;
    supportedLDAPVersion (2): 3; 2;
```

BaseDN: DC=cciew,DC=local



```
DC=cciew,DC=local
    CN=Builtin,DC=cciew,DC=local
    CN=Computers,DC=cciew,DC=local
    OU=Domain Controllers,DC=cciew,DC=local
    CN=ForeignSecurityPrincipals,DC=cciew,DC=loca
    CN=Infrastructure,DC=cciew,DC=local
    CN=Keys,DC=cciew,DC=local
    CN=LostAndFound,DC=cciew,DC=local
    CN=Managed Service Accounts,DC=cciew,DC=lo
    CN=NTDS Quotas,DC=cciew,DC=local
    CN=Program Data,DC=cciew,DC=local
    CN=System,DC=cciew,DC=local
    CN=TPM Devices,DC=cciew,DC=local
    CN=Users,DC=cciew,DC=local
        CN=Administrator,CN=Users,DC=cciew,DC=l
        CN=Allowed RODC Password Replication Grou
        CN=Cert Publishers,CN=Users,DC=cciew,DC=
        CN=Cloneable Domain Controllers,CN=Users,
        CN=DefaultAccount,CN=Users,DC=cciew,DC=
        CN=Denied RODC Password Replication Grou
        CN=DnsAdmins,CN=Users,DC=cciew,DC=loc
        CN=DnsUpdateProxy,CN=Users,DC=cciew,DC
        CN=Domain Admins,CN=Users,DC=cciew,DC
        CN=Domain Computers,CN=Users,DC=cciew,
        CN=Domain Controllers,CN=Users,DC=cciew,
        CN=Domain Guests,CN=Users,DC=cciew,DC=
        CN=Domain Users,CN=Users,DC=cciew,DC=l
        CN=Enterprise Admins,CN=Users,DC=cciew,D
        CN=Enterprise Key Admins,CN=Users,DC=cci
        CN=Enterprise Read-only Domain Controllers,
        CN=Group Policy Creator Owners,CN=Users,D
        CN=Guest,CN=Users,DC=cciew,DC=local
        CN=kanu,CN=Users,DC=cciew,DC=local
        CN=Key Admins,CN=Users,DC=cciew,DC=loc
        CN=krbtgt,CN=Users,DC=cciew,DC=local
```

```
    adminCount: 1;
    badPasswordTime: 0 (never);
    badPwdCount: 0;
    cn: vk1;
    codePage: 0;
    countryCode: 0;
    displayName: vk1;
    distinguishedName: CN=vk1,CN=Users,DC=cciew,DC=local;
    dSCorePropagationData (2): 29-09-2021 15:16:40 India Standard Time; 0x0 = (  );
    givenName: vk1;
    instanceType: 0x4 = ( WRITE );
    lastLogoff: 0 (never);
    lastLogon: 0 (never);
    logonCount: 0;
    memberOf (4): CN=Domain Admins,CN=Users,DC=cciew,DC=local; CN=Enterprise Admins,CN=Users,DC=cciew,DC=local; CN=Schema
        Admins,CN=Users,DC=cciew,DC=local; CN=Administrators,CN=Builtin,DC=cciew,DC=local;
    name: vk1;
    objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cciew,DC=local;
    objectClass (4): top; person; organizationalPerson; user;
    objectGUID: 1814f794-025e-4378-abed-66ff78a4a4d3;
    objectSid: S-1-5-21-1375146846-274930181-3003521951-1120;
    primaryGroupID: 513 = ( GROUP_RID_USERS );
    pwdLastSet: 27-09-2021 22:56:11 India Standard Time;
    sAMAccountName: vkokila;
    sAMAccountType: 805306368 = ( NORMAL_USER_ACCOUNT );
    userAccountControl: 0x10200 = ( NORMAL_ACCOUNT | DONT_EXPIRE_PASSWD );
    userPassword: Cisco123;
    userPrincipalName: vk1@cciew.local;
    uSNChanged: 160181;
    uSNCreated: 94284;
    whenChanged: 29-09-2021 15:16:40 India Standard Time;
    whenCreated: 25-12-2020 16:25:53 India Standard Time;

-----------
Expanding base 'CN=Users,DC=cciew,DC=local'...
Getting 1 entries:
Dn: CN=Users,DC=cciew,DC=local
    cn: Users;
    description: Default container for upgraded user accounts;
    distinguishedName: CN=Users,DC=cciew,DC=local;
    dSCorePropagationData (2): 29-09-2019 01:09:51 India Standard Time; 0x1 = ( NEW_SD );
    instanceType: 0x4 = ( WRITE );
    isCriticalSystemObject: TRUE;
    name: Users;
    objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=cciew,DC=local;
```



```
CN=TPM Devices,DC=cciew,DC=local
CN=Users,DC=cciew,DC=local
    CN=Administrator,CN=Users,DC=cciew,DC=l
    CN=Allowed RODC Password Replication Grou
    CN=Cert Publishers,CN=Users,DC=cciew,DC=
    CN=Cloneable Domain Controllers,CN=Users,
    CN=DefaultAccount,CN=Users,DC=cciew,DC=
    CN=Denied RODC Password Replication Grou
    CN=DnsAdmins,CN=Users,DC=cciew,DC=loc
    CN=DnsUpdateProxy,CN=Users,DC=cciew,DC
    CN=Domain Admins,CN=Users,DC=cciew,DC
    CN=Domain Computers,CN=Users,DC=cciew,
    CN=Domain Controllers,CN=Users,DC=cciew,
    CN=Domain Guests,CN=Users,DC=cciew,DC=
    CN=Domain Users,CN=Users,DC=cciew,DC=l
    CN=Enterprise Admins,CN=Users,DC=cciew,D
    CN=Enterprise Key Admins,CN=Users,DC=cci
    CN=Enterprise Read-only Domain Controllers,
    CN=Group Policy Creator Owners,CN=Users,D
    CN=Guest,CN=Users,DC=cciew,DC=local
    CN=kanu,CN=Users,DC=cciew,DC=local
    CN=Key Admins,CN=Users,DC=cciew,DC=loc
    CN=krbtgt,CN=Users,DC=cciew,DC=local
    CN=Protected Users,CN=Users,DC=cciew,DC=
    CN=RAS and IAS Servers,CN=Users,DC=cciew,
    CN=Read-only Domain Controllers,CN=Users,
    CN=Schema Admins,CN=Users,DC=cciew,DC
    CN=sony s,CN=Users,DC=cciew,DC=local
    CN=tejas,CN=Users,DC=cciew,DC=local
    CN=test,CN=Users,DC=cciew,DC=local
    CN=test123,CN=Users,DC=cciew,DC=local
    CN=vk,CN=Users,DC=cciew,DC=local
    CN=vk1,CN=Users,DC=cciew,DC=local
        No children
    CN=Yogesh G.,CN=Users,DC=cciew,DC=local
```

```
    showInAdvancedViewOnly: FALSE;
    systemFlags: 0x8C000000 = ( DISALLOW_DELETE | DOMAIN_DISALLOW_REI
    uSNChanged: 5888;
    uSNCreated: 5888;
    whenChanged: 29-09-2019 01:08:06 India Standard Time;
    whenCreated: 29-09-2019 01:08:06 India Standard Time;

-----------
Expanding base 'CN=vk1,CN=Users,DC=cciew,DC=local'...
Getting 1 entries:
Dn: CN=vk1,CN=Users,DC=cciew,DC=local
    accountExpires: 9223372036854775807 (never);
    adminCount: 1;
    badPasswordTime: 0 (never);
    badPwdCount: 0;
    cn: vk1;
    codePage: 0;
    countryCode: 0;
    displayName: vk1;
    distinguishedName: CN=vk1,CN=Users,DC=cciew,DC=local;
    dSCorePropagationData (2): 29-09-2021 15:16:40 India Standard Time; 0x0 =
    givenName: vk1;
    instanceType: 0x4 = ( WRITE );
    lastLogoff: 0 (never);
    lastLogon: 0 (never);
    logonCount: 0;
    memberOf (4): CN=Domain Admins,CN=Users,DC=cciew,DC=local; CN=Enterp
        Admins,CN=Users,DC=cciew,DC=local; CN=Administrators,CN=Builtin,DC=
    name: vk1;
    objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cciew,DC=loc
    objectClass (4): top; person; organizationalPerson; user;
    objectGUID: 1814f794-025e-4378-abed-66ff78a4a4d3;
    objectSid: S-1-5-21-1375146846-274930181-3003521951-1120;
    primaryGroupID: 513 = ( GROUP_RID_USERS );
    pwdLastSet: 27-09-2021 22:56:11 India Standard Time;
    sAMAccountName: vkokila;
    sAMAccountType: 805306368 = ( NORMAL_USER_ACCOUNT );
    userAccountControl: 0x10200 = ( NORMAL_ACCOUNT | DONT_EXPIRE_PASS
    userPassword: Cisco123;
    userPrincipalName: vk1@cciew.local;
    uSNChanged: 160181;
    uSNCreated: 94284;
    whenChanged: 29-09-2021 15:16:40 India Standard Time;
    whenCreated: 25-12-2020 16:25:53 India Standard Time;
```

4. Vérifier les statistiques du serveur et l'attribut MAP

```
C9800-40-K9#show ldap server all

Server Information for ldap

================================

Server name              :ldap

Server Address           :10.106.38.195

Server listening Port    :389

Bind Root-dn             :vk1

Server mode              :Non-Secure

Cipher Suite             :0x00

Authentication Seq       :Search first. Then Bind/Compare password next

Authentication Procedure:Bind with user password
```

```
Base-Dn                 :CN=users,DC=cciew,DC=local

Object Class            :Person

Attribute map           :VK

Request timeout         :30

Deadtime in Mins        :0

State                   :ALIVE

---------------------------------

* LDAP STATISTICS *

Total messages  [Sent:2, Received:3]

Response delay(ms) [Average:2, Maximum:2]

Total search    [Request:1, ResultEntry:1, ResultDone:1]

Total bind      [Request:1, Response:1]

Total extended  [Request:0, Response:0]

Total compare   [Request:0, Response:0]

Search [Success:1, Failures:0]

Bind   [Success:1, Failures:0]

Missing attrs in Entry [0]

Connection   [Closes:0, Aborts:0, Fails:0, Timeouts:0]

----------------------------------

No. of active connections   :0

---------------------------------
```

Références

Exemple de configuration EAP local sur le 9800

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.