802.1XおよびWeb認証のためのLDAP認証を使用したCatalyst 9800 WLCの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[Webauth SSIDを使用したLDAPの設定](#)
[ネットワーク図](#)
[コントローラの設定](#)
[dot1x SSIDを使用したLDAPの設定（ローカルEAPを使用）](#)
[LDAPサーバの詳細について](#)
[9800 Web UIのフィールドについて](#)
[sAMAaccountName属性を使用したLDAP 802.1x認証。](#)
[WLC の設定:](#)
[Webインターフェイスから確認します。](#)
[確認](#)
[トラブルシュート](#)
[コントローラの認証プロセスを確認する方法](#)
[9800からLDAPへの接続を確認する方法](#)
[参考資料](#)

概要

このドキュメントでは、ユーザクレデンシャルのデータベースとしてLDAPサーバを使用してクライアントを認証するためにCatalyst 9800を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Microsoft Windows Server
- Active Directoryまたはその他のLDAPデータベース

使用するコンポーネント

Cisco IOS®-XEバージョン17.3.2aが稼働するC9100アクセスポイント(AP)上のC9800 EWC

LDAPデータベースとして機能するQNAPネットワークアクセスストレージ(NAS)を備えたMicrosoft Active Directory(AD)サーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

Webauth SSIDを使用したLDAPの設定

ネットワーク図

この記事は非常にシンプルな設定に基づいて書かれています。

IPアドレス192.168.1.15のEWC AP 9115

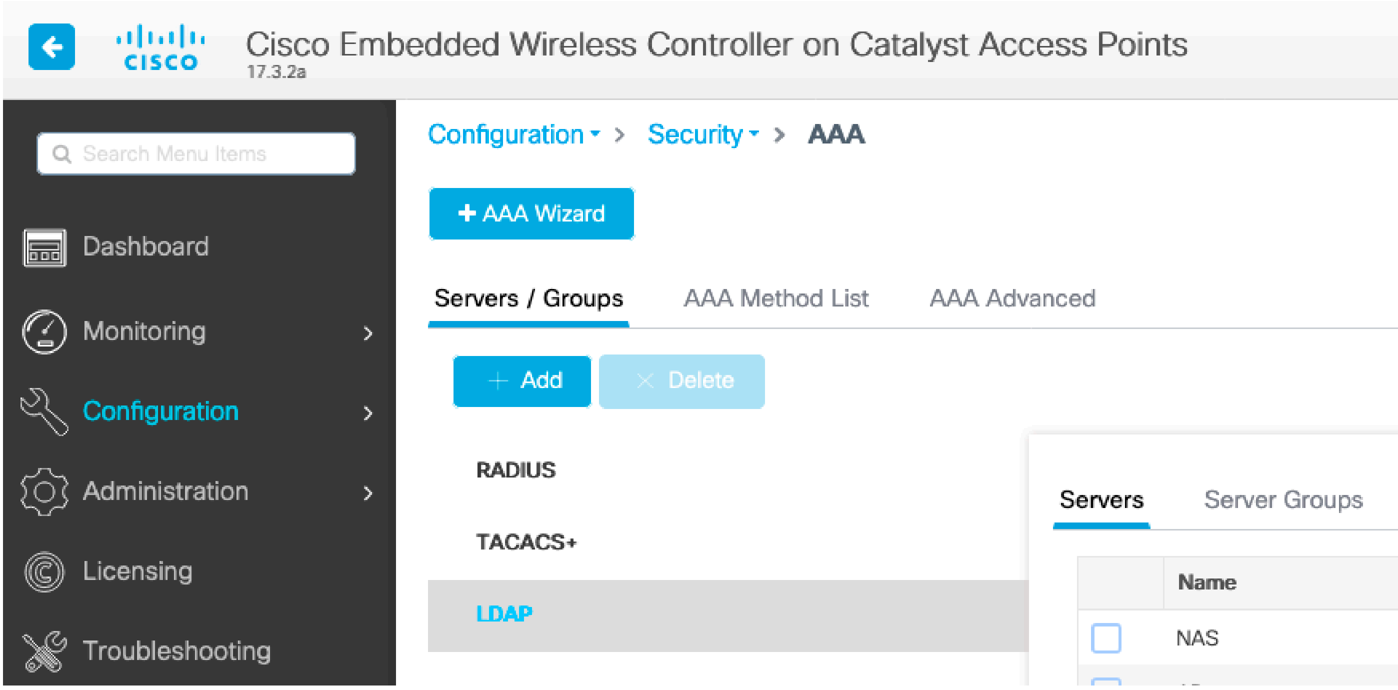
IPアドレスが192.168.1.192のActive Directoryサーバ

EWCの内部APに接続するクライアント

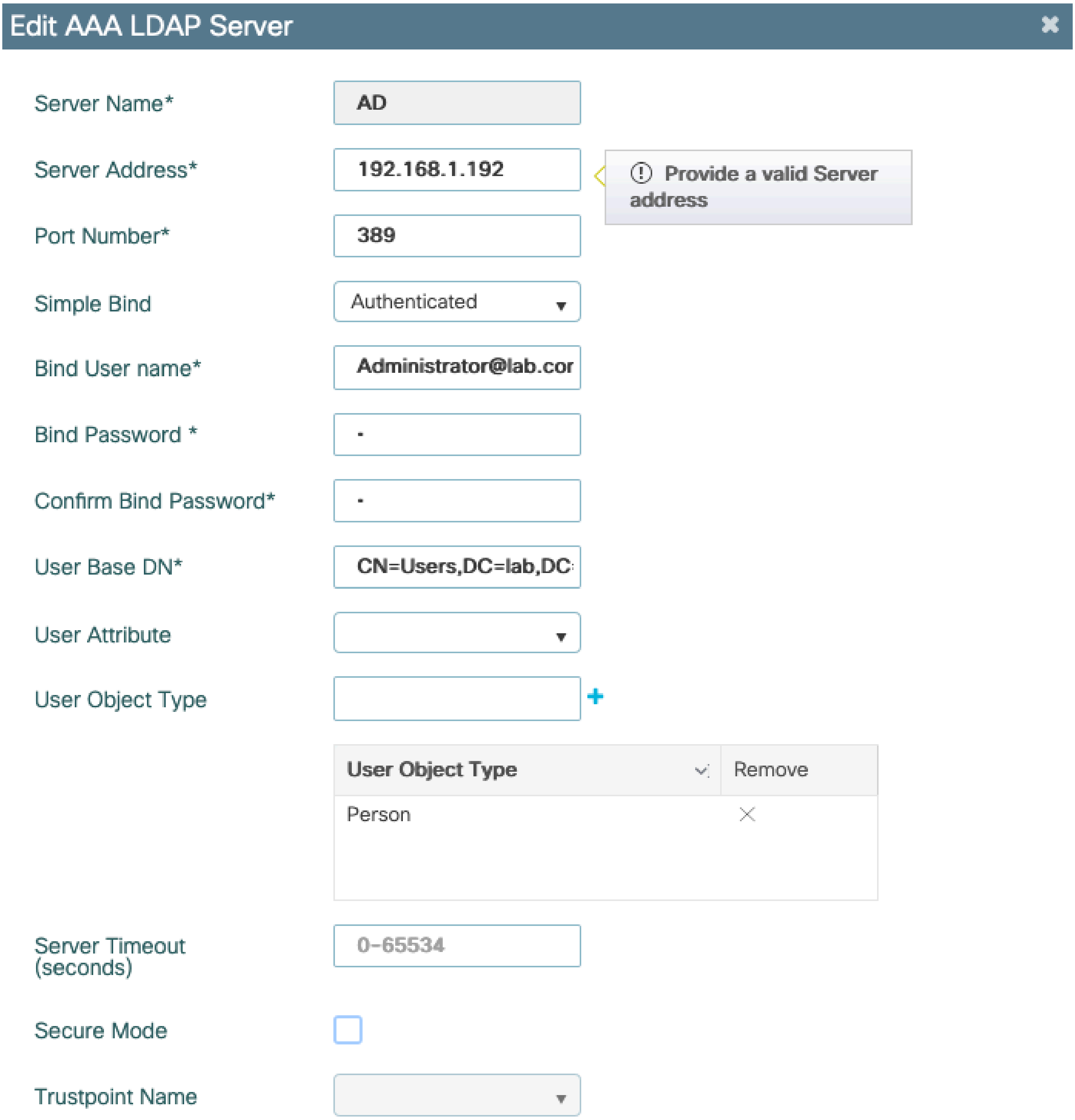
コントローラの設定

ステップ1:LDAPサーバを設定する

[Configuration] > [Security] > [AAA] > [Servers/Groups] > [LDAP] に移動し、[Add] をクリックします。



LDAPサーバの名前を選択し、詳細を入力します。各フィールドの説明については、このドキュメントの「LDAPサーバの詳細について」の項を参照してください。



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	×

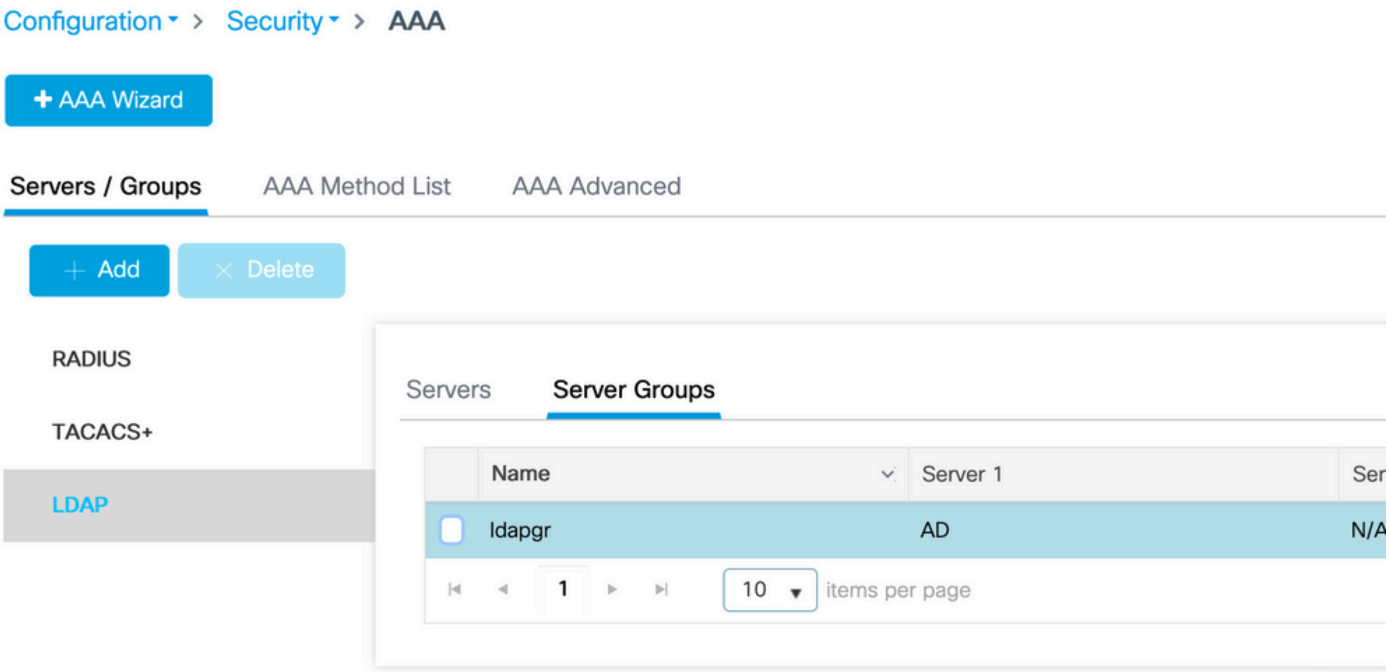
[Update and apply to device]をクリックして保存します。

CLI コマンド:

```
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
```

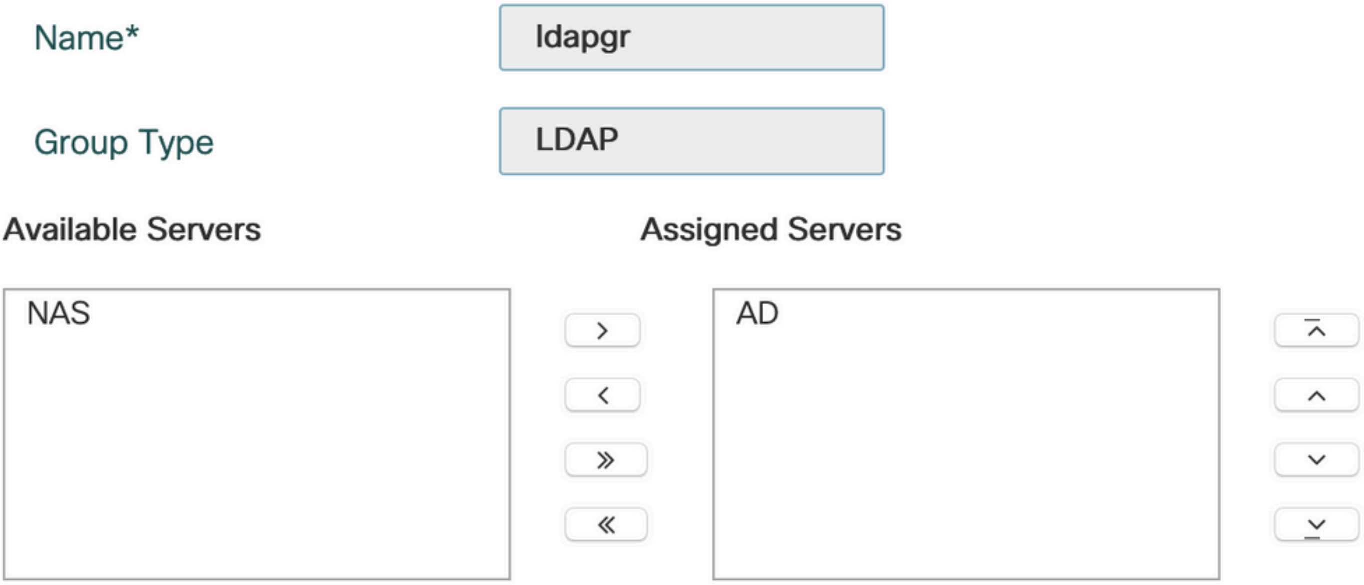
ステップ2:LDAPサーバグループを設定します。

[Configuration] > [Security] > [AAA] > [Servers/ Groups] > [LDAP] > [Server Groups] に移動し、[ADD] をクリックします



	Name	Server 1	Ser
□	ldapgr	AD	N/A

名前を入力し、前の手順で設定したLDAPサーバを追加します。



Name*	ldapgr
Group Type	LDAP

Available Servers	Assigned Servers
NAS	AD

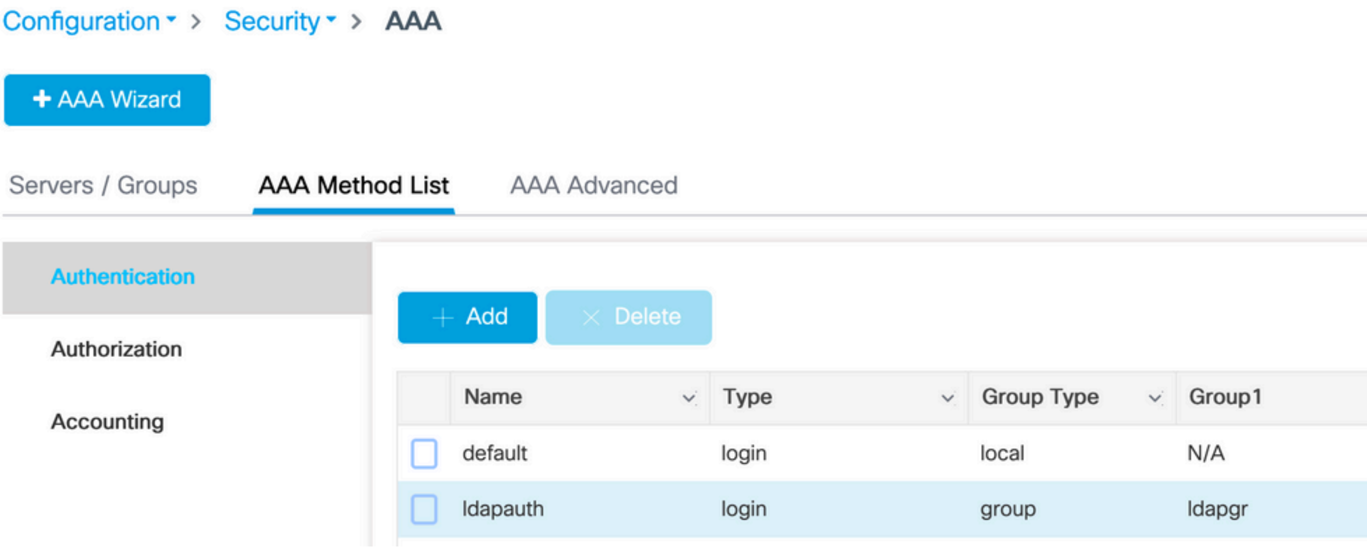
[Update and apply] をクリックして保存します。

CLI コマンド:

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

ステップ3:AAA認証方式の設定

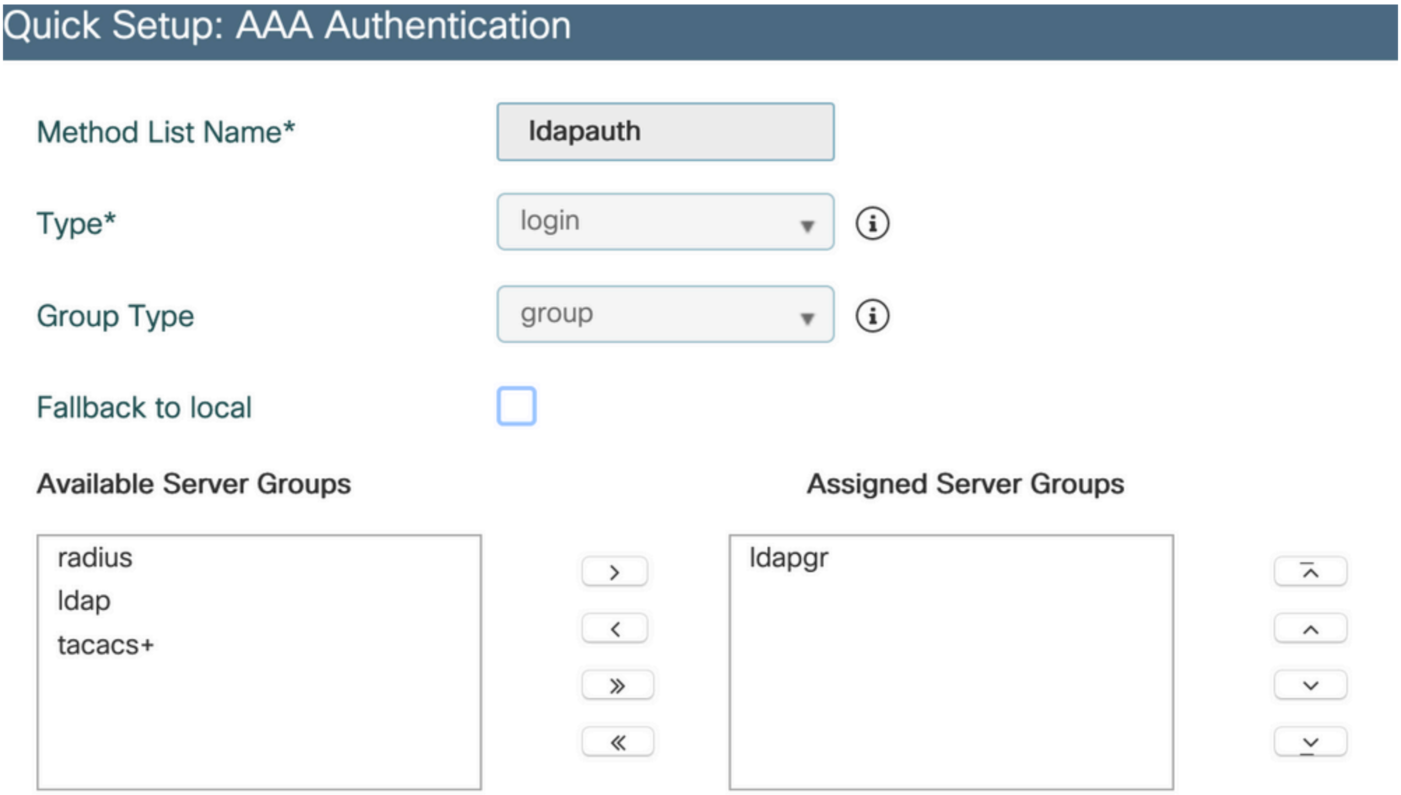
[Configuration] > [Security] > [AAA] > [AAA method List] > [Authentication] に移動し、[Add] をクリックします



Configuration > Security > AAA

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

名前を入力し、[Login] タイプを選択して、以前に設定したLDAPサーバグループをポイントします。



Quick Setup: AAA Authentication

Method List Name*	ldapauth
Type*	login
Group Type	group
Fallback to local	□

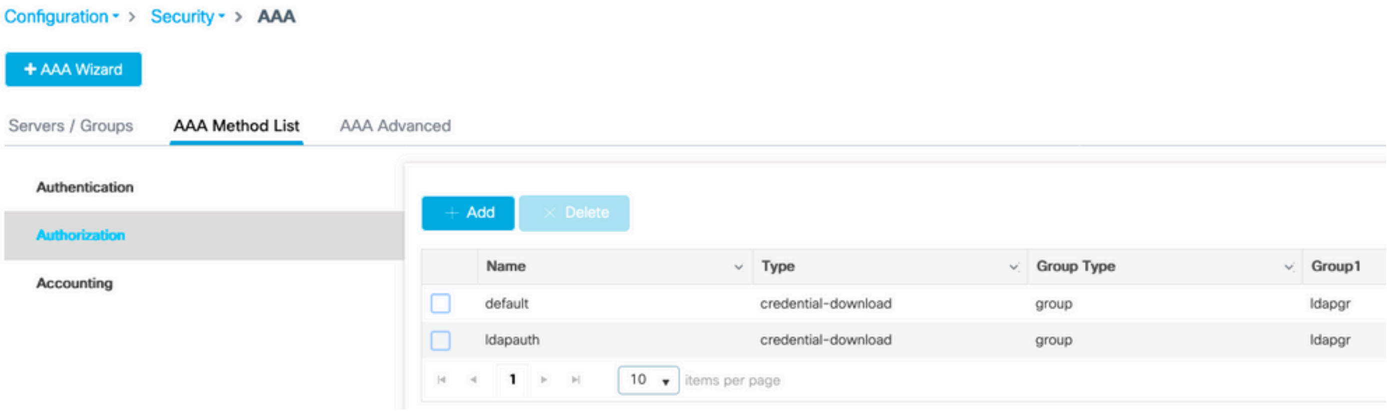
Available Server Groups	Assigned Server Groups
radius ldap tacacs+	ldapgr

CLI コマンド:

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

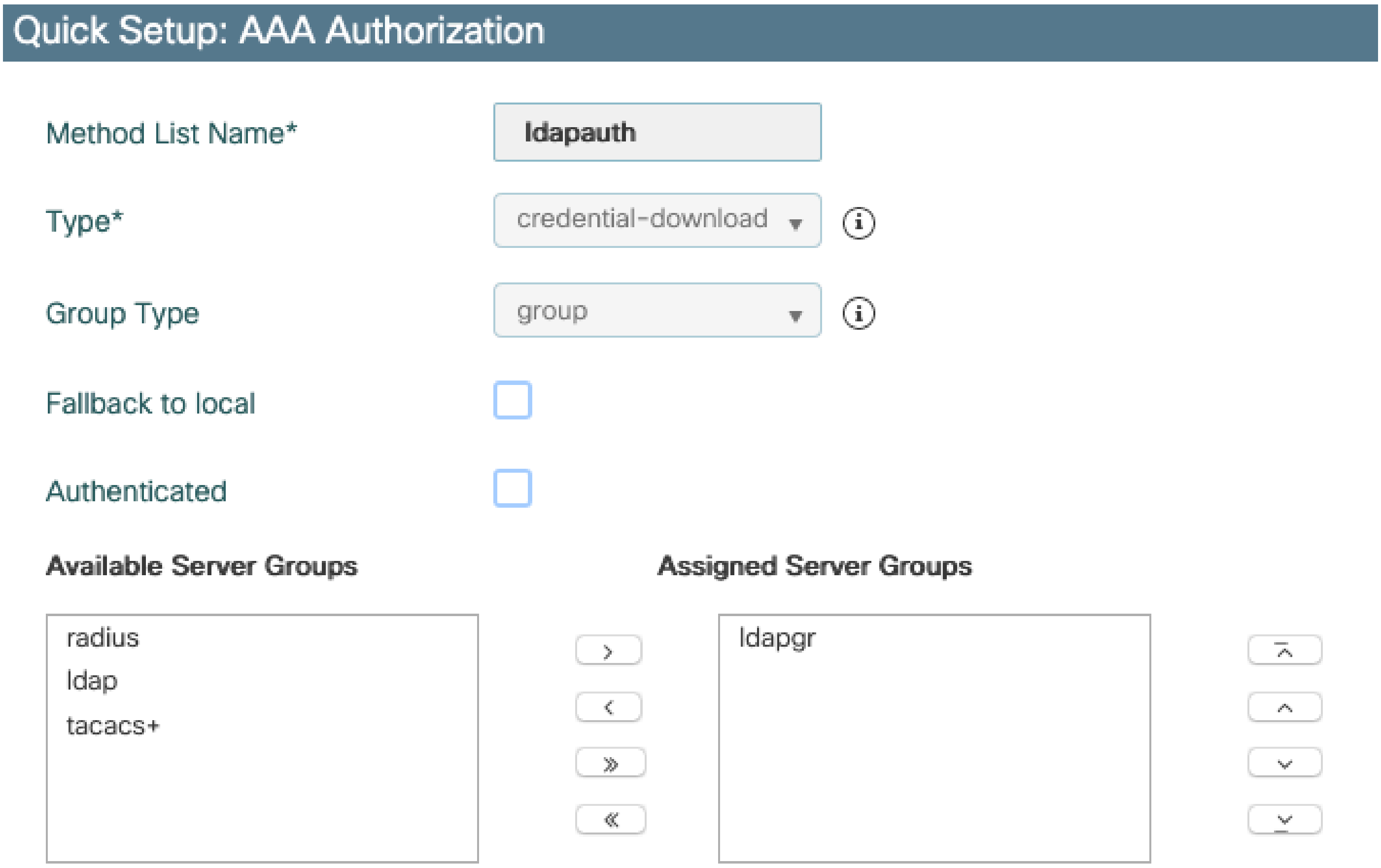
ステップ4:AAA認可方式の設定

[Configuration] > [Security] > [AAA] > [AAA method list] > [Authorization] に移動し、[Add] をクリックします


Configuration > Security > AAA

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

選択した名前のクレデンシャルダウンロードタイプのルールを作成し、前に作成したLDAPサーバグループを指定します


Quick Setup: AAA Authorization

Method List Name*: ldapauth

Type*: credential-download

Group Type: group

Fallback to local: □

Authenticated: □

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: ldapgr

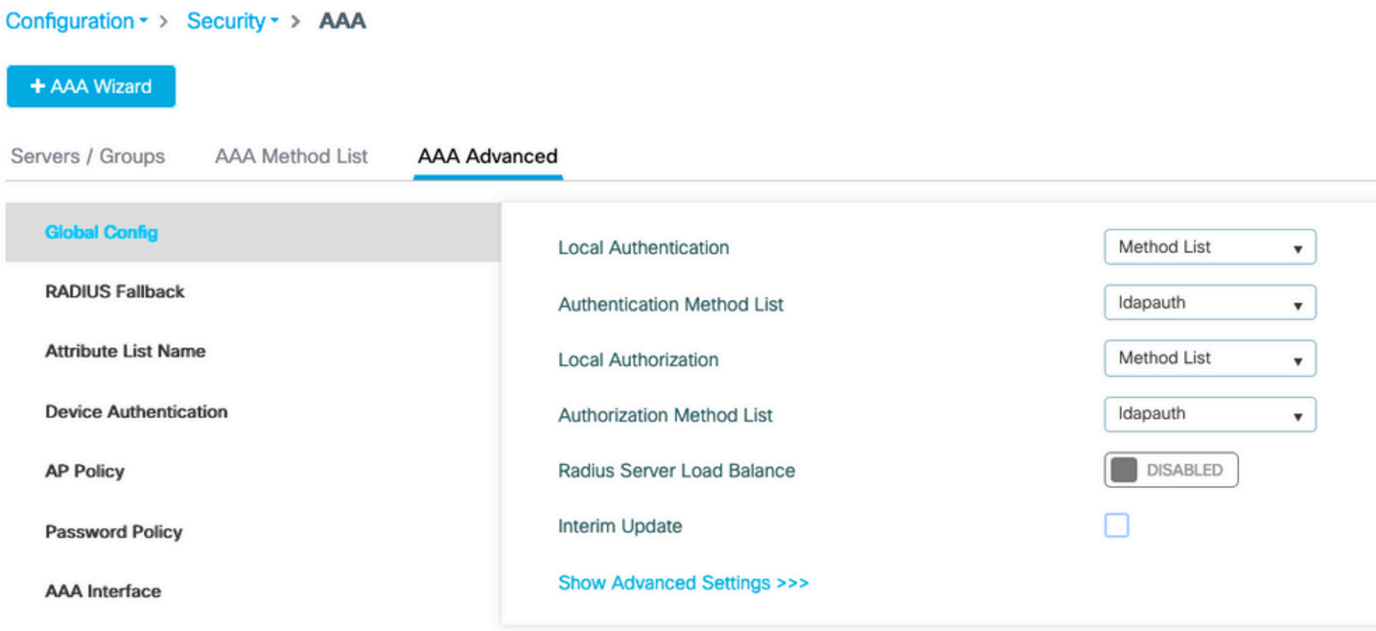
CLI コマンド:

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

ステップ5:ローカル認証の設定

[Configuration] > [Security] > [AAA] > [AAA Advanced] > [Global Config] に移動します。

ローカル認証とローカル認可を[Method List] に設定し、以前に設定した認証と認可の方式を選択します。



Local Authentication: Method List

Authentication Method List: ldapauth

Local Authorization: Method List

Authorization Method List: ldapauth

Radius Server Load Balance: DISABLED

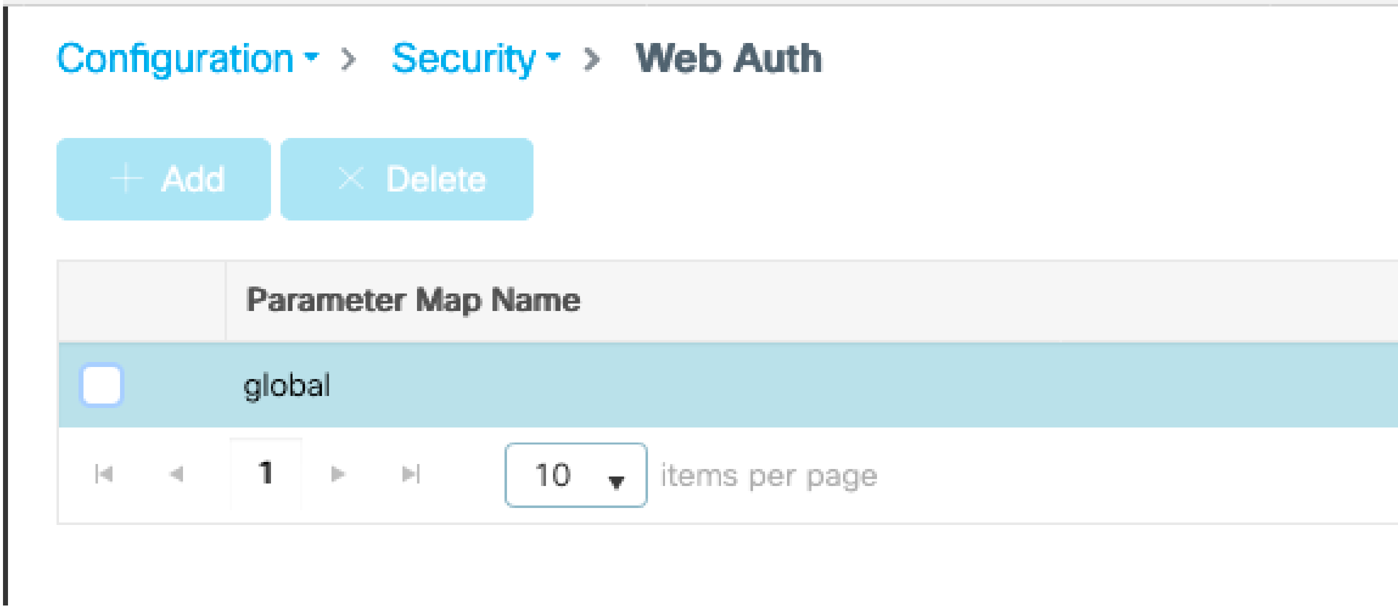
Interim Update: □

CLI コマンド:

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

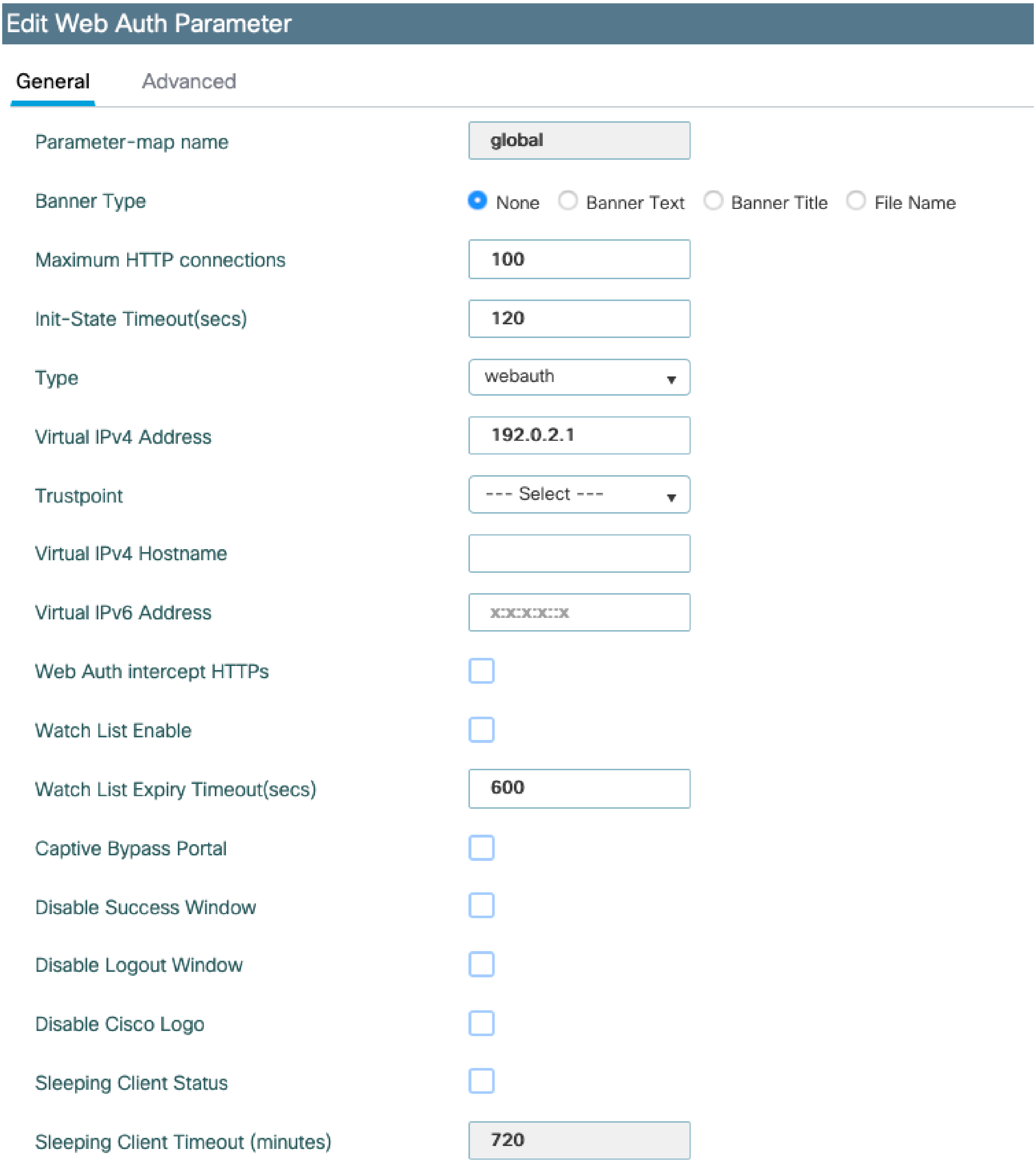
ステップ6:webauthパラメータマップの設定

[Configuration] > [Security] > [Web Auth] に移動し、**global**マップを編集します



	Parameter Map Name
□	global

192.0.2.1などの仮想IPv4アドレスを必ず設定してください（その特定のIP/サブネットはルーティング不可能な仮想IP用に予約されています）。



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

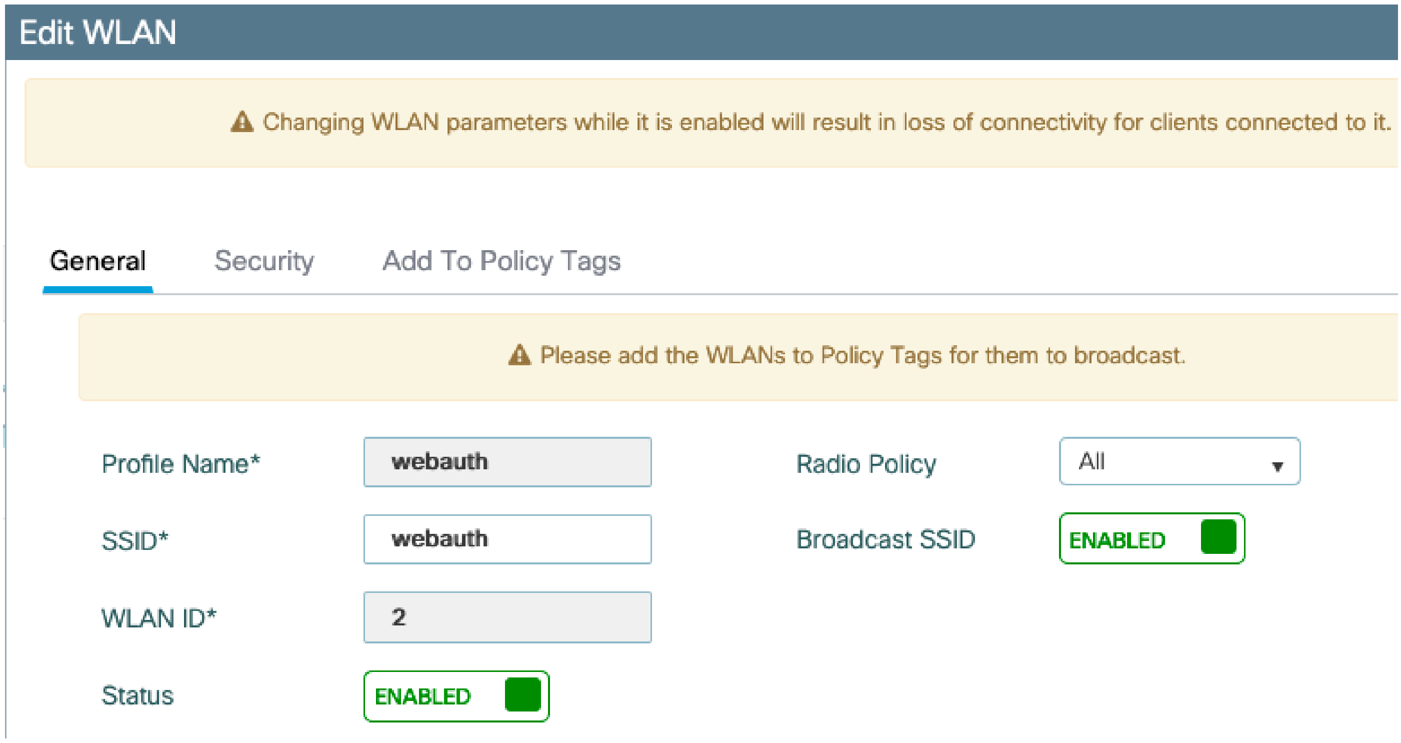
Applyをクリックして保存します。

CLI コマンド:

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

ステップ7:webauth WLANの設定

[Configuration] > [WLANs] に移動し、[Add] をクリックします



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

SSID* webauth

WLAN ID* 2

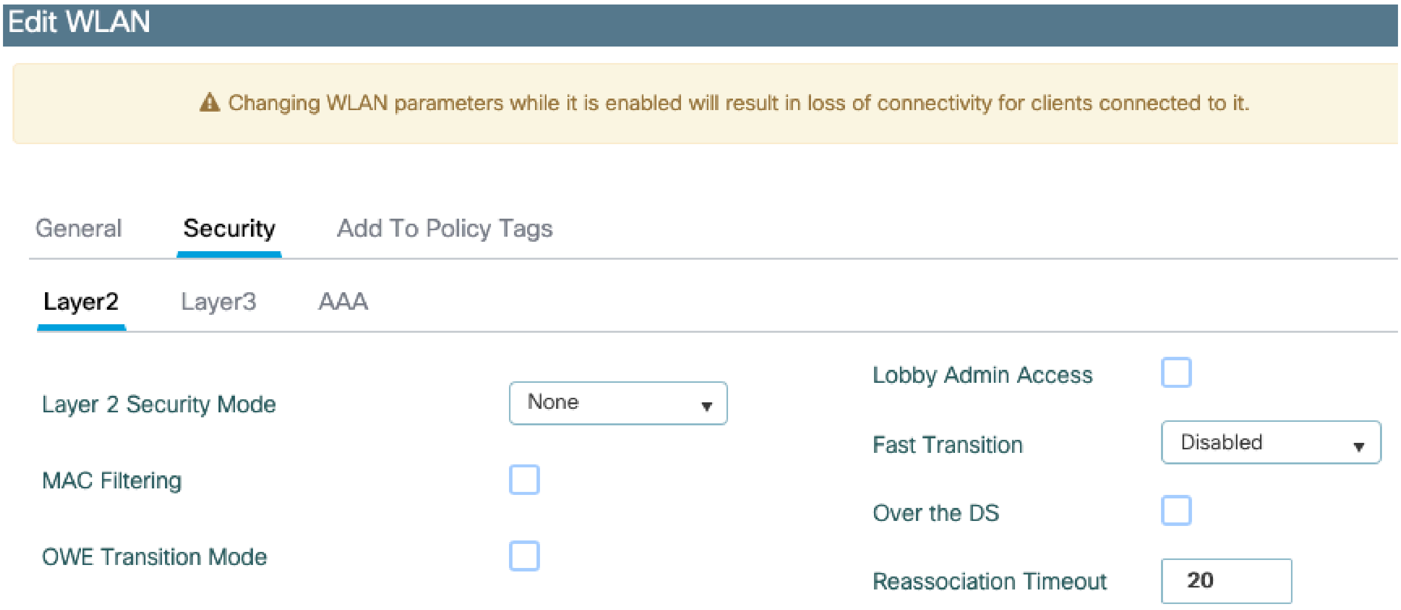
Status ENABLED

Radio Policy All

Broadcast SSID ENABLED

名前を設定し、有効な状態であることを確認してから、[Security] タブに移動します。

[Layer 2] サブタブで、セキュリティが設定されておらず、[Fast Transition]が無効になっていることを確認します。



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

MAC Filtering □

OWE Transition Mode □

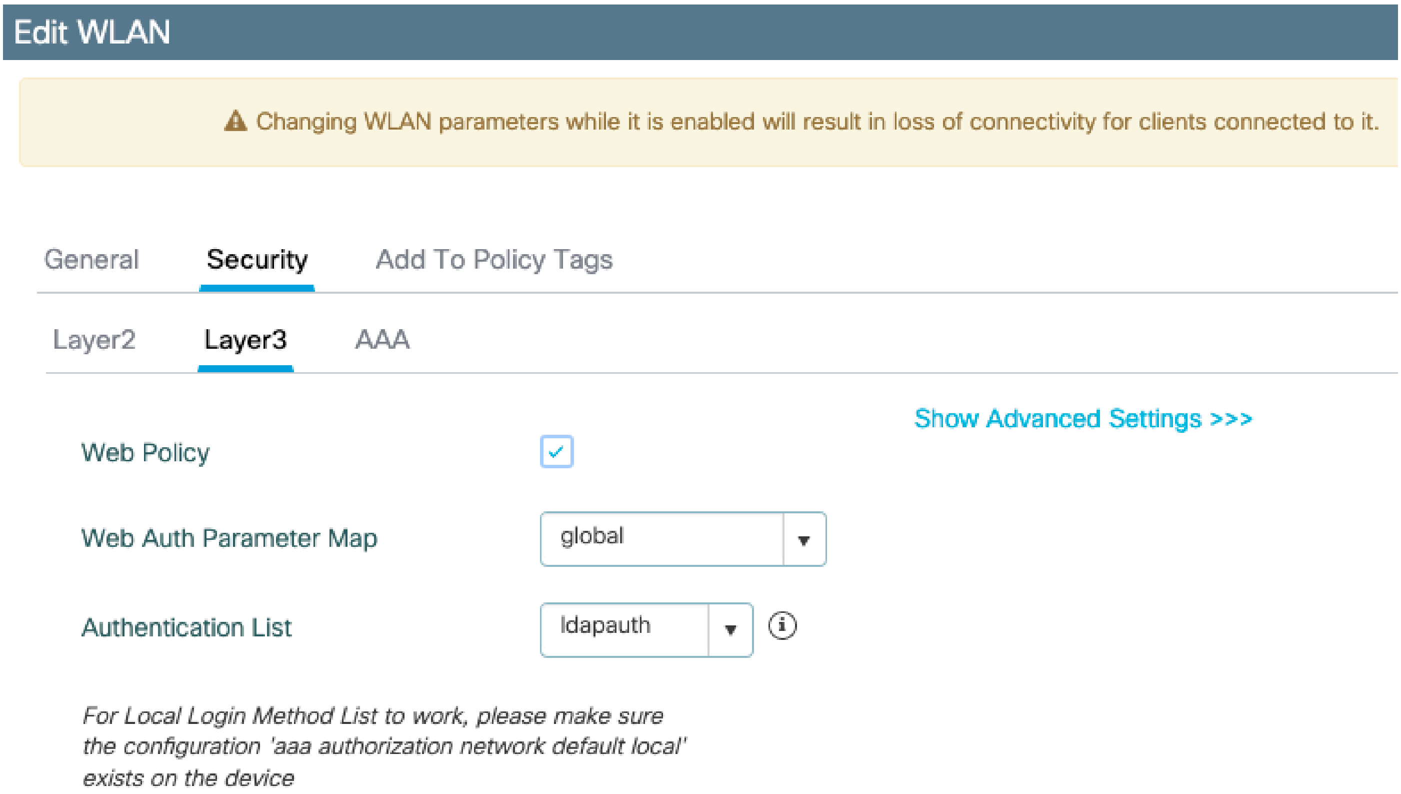
Lobby Admin Access □

Fast Transition Disabled

Over the DS □

Reassociation Timeout 20

[Layer3] タブで、**web policy**を有効にし、パラメータマップを**global**に設定し、認証リストを以前に設定したaaaログイン方式に設定します。



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

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

[Apply] をクリックして保存します。

CLI コマンド:

```
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
```

ステップ8:SSIDがブロードキャストされることを確認します

[Configuration] > [Tags] に移動し、そのSSIDがSSIDによって現在サービスされているポリシープロファイルに含まれていることを確認します（まだタグを設定していない場合の新しい設定用のdefault-policy-tag）。 デフォルトでは、default-policy-tagは、手動で組み込むまで、作成した新しいSSIDをブロードキャストしません。

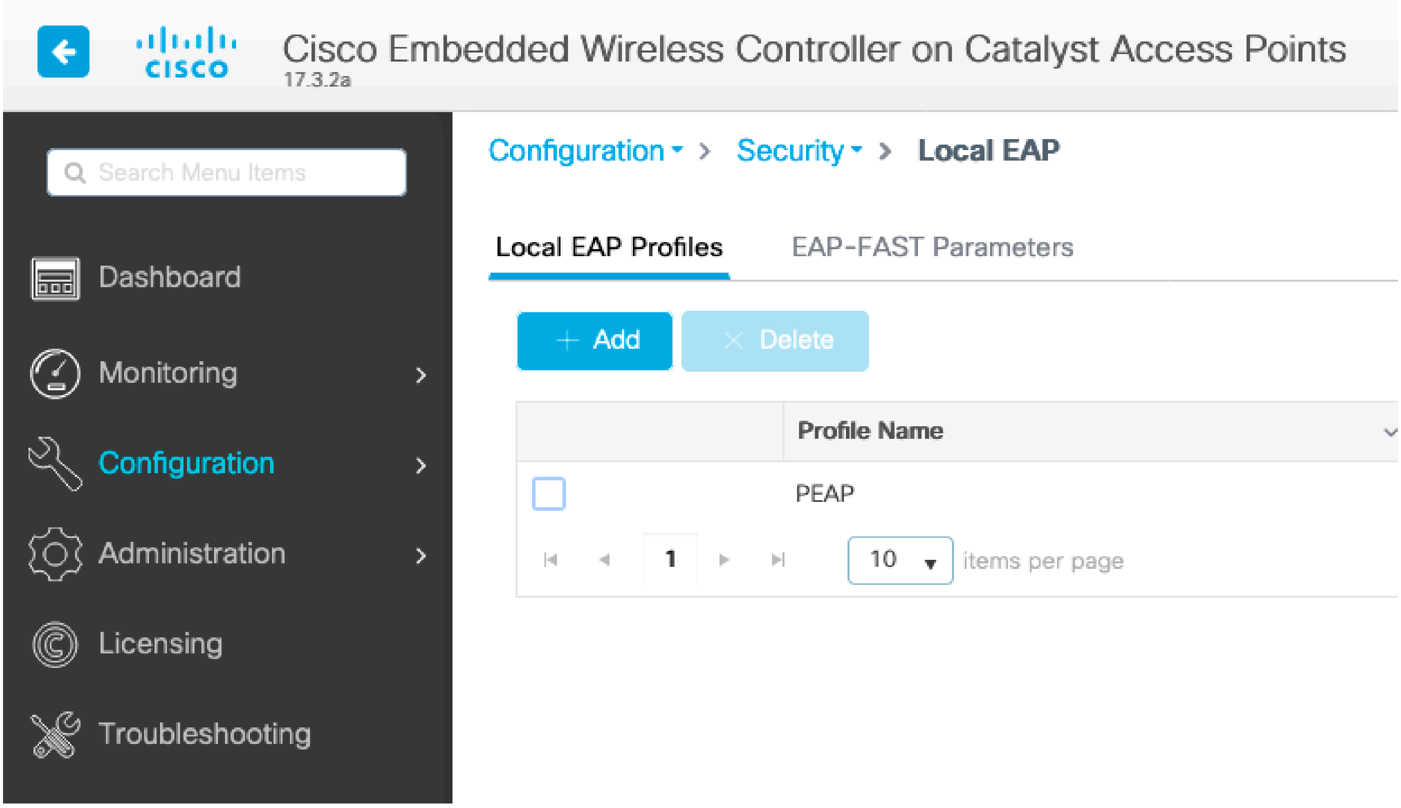
この記事では、ポリシープロファイルの設定については説明せず、設定のその部分に精通していることを前提としています。

dot1x SSIDを使用したLDAPの設定（ローカルEAPを使用）

通常、9800で802.1X SSIDのLDAPを設定するには、ローカルEAPも設定する必要があります。RADIUSを使用する場合、LDAPデータベースとの接続を確立するのはRADIUSサーバであり、この記事では説明しません。この設定を行う前に、まずWLCで設定したローカルユーザを使用してローカルEAPを設定することをお勧めします。設定例については、この記事の最後にある「参考資料」の項を参照してください。完了したら、ユーザデータベースをLDAPに移動できます。

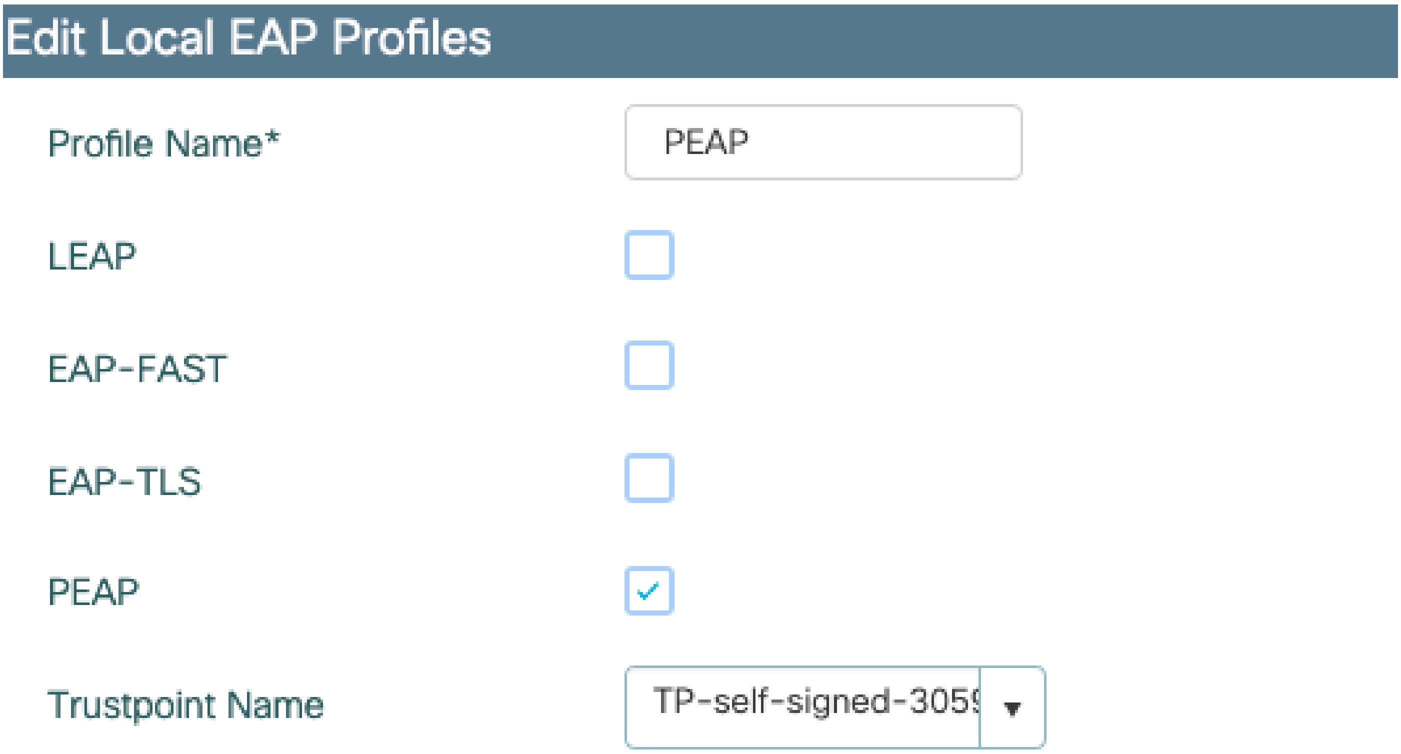
ステップ1：ローカルEAPプロファイルの設定

[Configuration] > [Local EAP] に移動し、[Add] をクリックします



	Profile Name
□	PEAP

プロファイルの名前を選択します。少なくともPEAPを有効にして、トラストポイント名を選択します。デフォルトでは、WLCには自己署名証明書しか存在しないため、どの証明書を選択しても実際には関係ありません（通常、TP-self-signed-xxxxが最適です）。ただし、新しいスマートフォンのOSバージョンでは、信頼される自己署名証明書の数が少なくなるため、信頼できる公開署名証明書のインストールを検討してください。



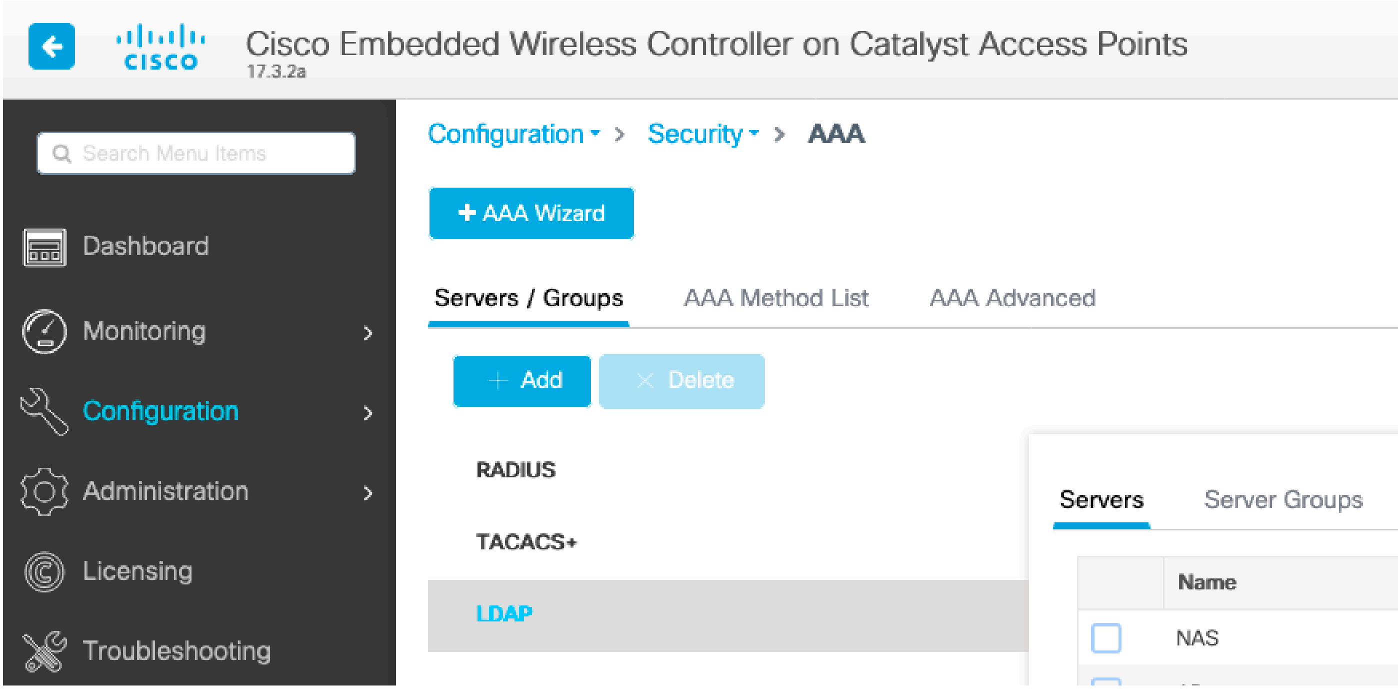
Profile Name*	PEAP
LEAP	□
EAP-FAST	□
EAP-TLS	□
PEAP	☑
Trustpoint Name	TP-self-signed-305

CLI コマンド:

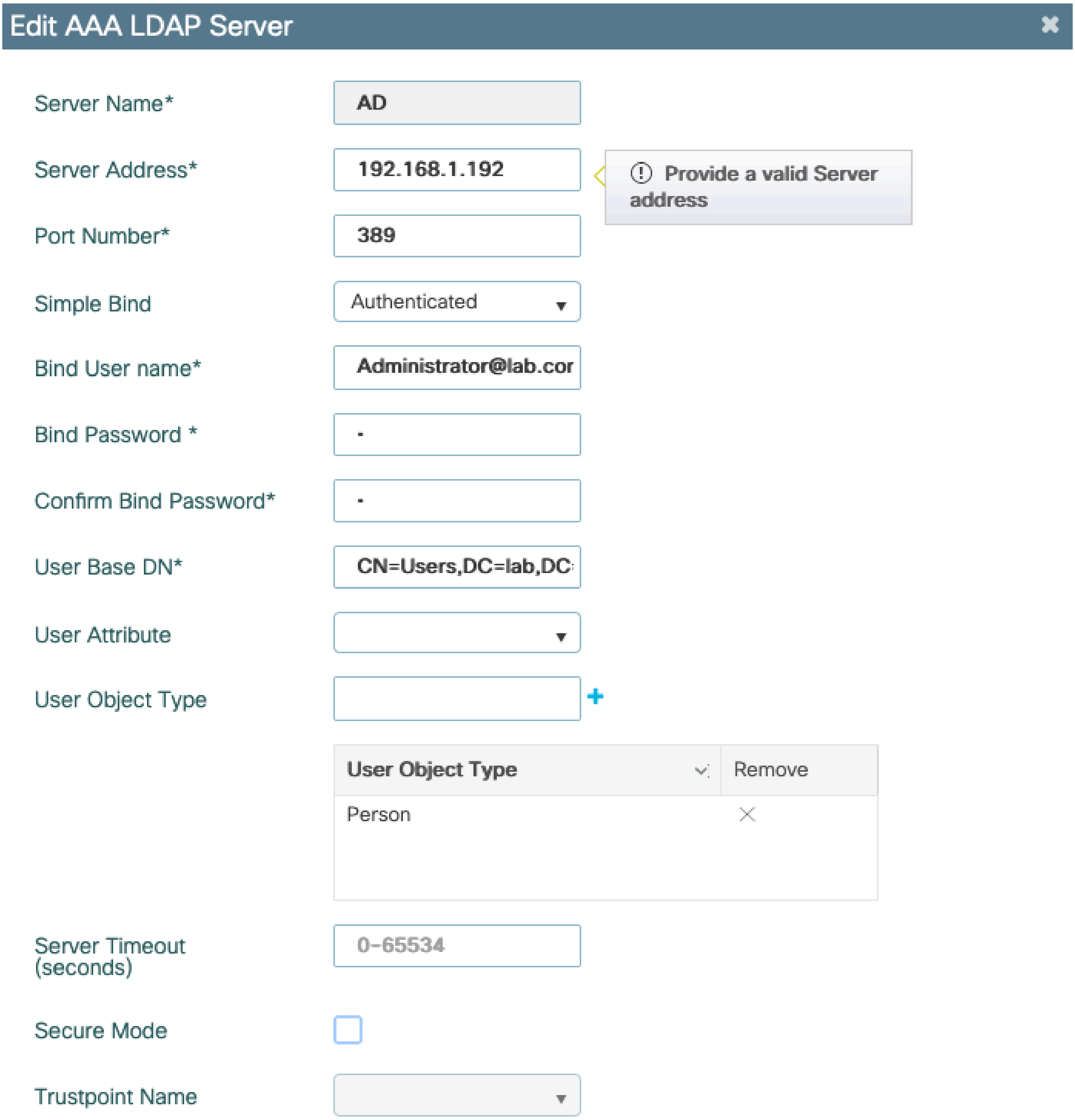
```
eap profile PEAP method peap pki-trustpoint TP-self-signed-3059261382
```

ステップ2:LDAPサーバを設定する

[Configuration] > [Security] > [AAA] > [Servers/Groups] > [LDAP] に移動し、[Add] をクリックします。



LDAPサーバの名前を選択し、詳細を入力します。各フィールドの説明については、このドキュメントの「LDAPサーバの詳細について」の項を参照してください。



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

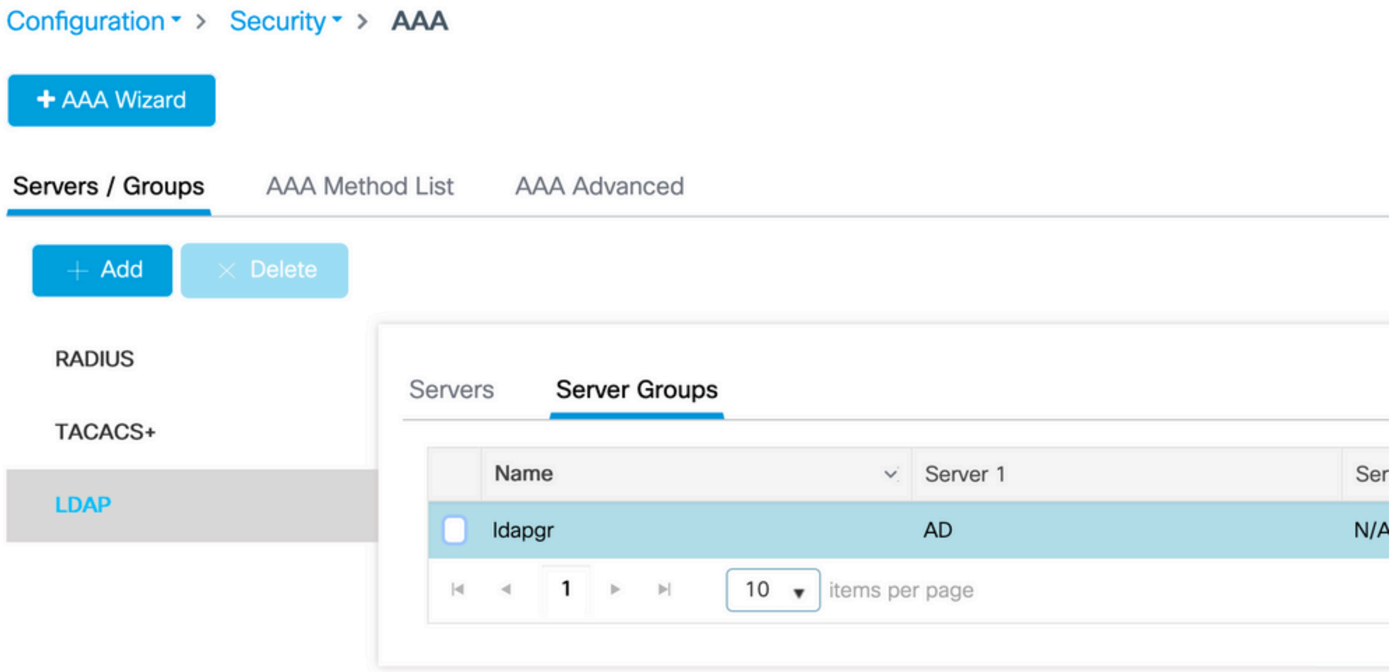
User Object Type	Remove
Person	×

[Update and apply to device]をクリックして保存します。

```
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
```

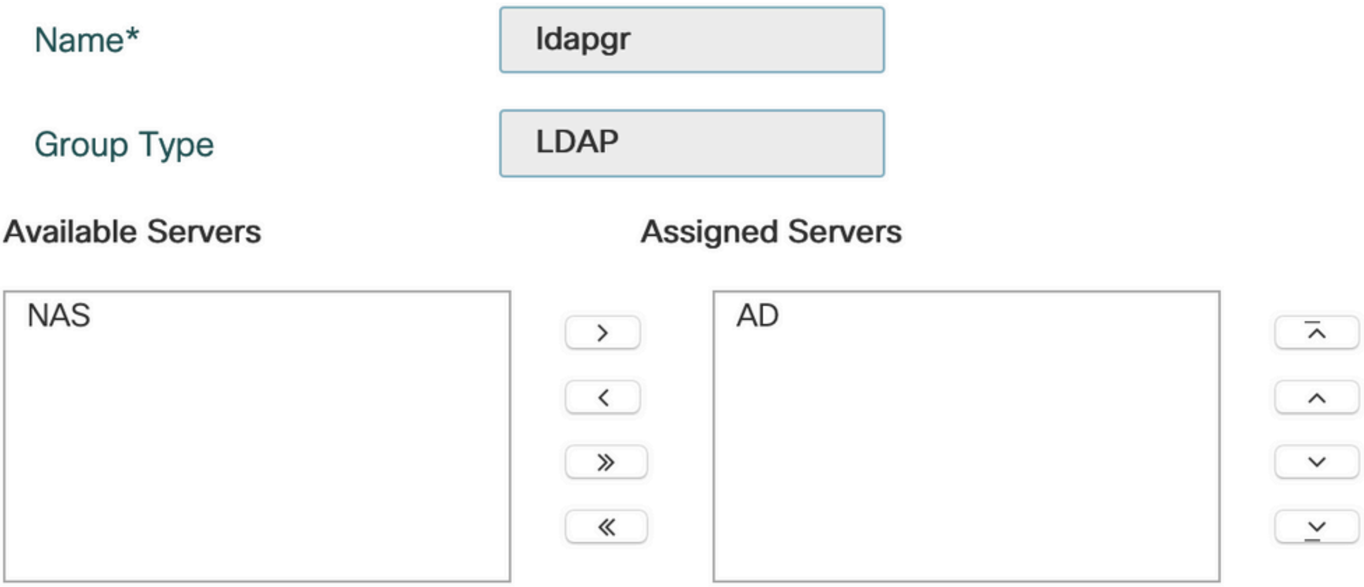
ステップ3:LDAPサーバグループを設定します。

[Configuration] > [Security] > [AAA] > [Servers/ Groups] > [LDAP] > [Server Groups] に移動し、[ADD] をクリックします



Name	Server 1	Ser
ldapgr	AD	N/A

名前を入力し、前の手順で設定したLDAPサーバを追加します。


Name*: ldapgr

Group Type: LDAP

Available Servers: NAS

Assigned Servers: AD

[Update and apply] をクリックして保存します。

CLI コマンド:

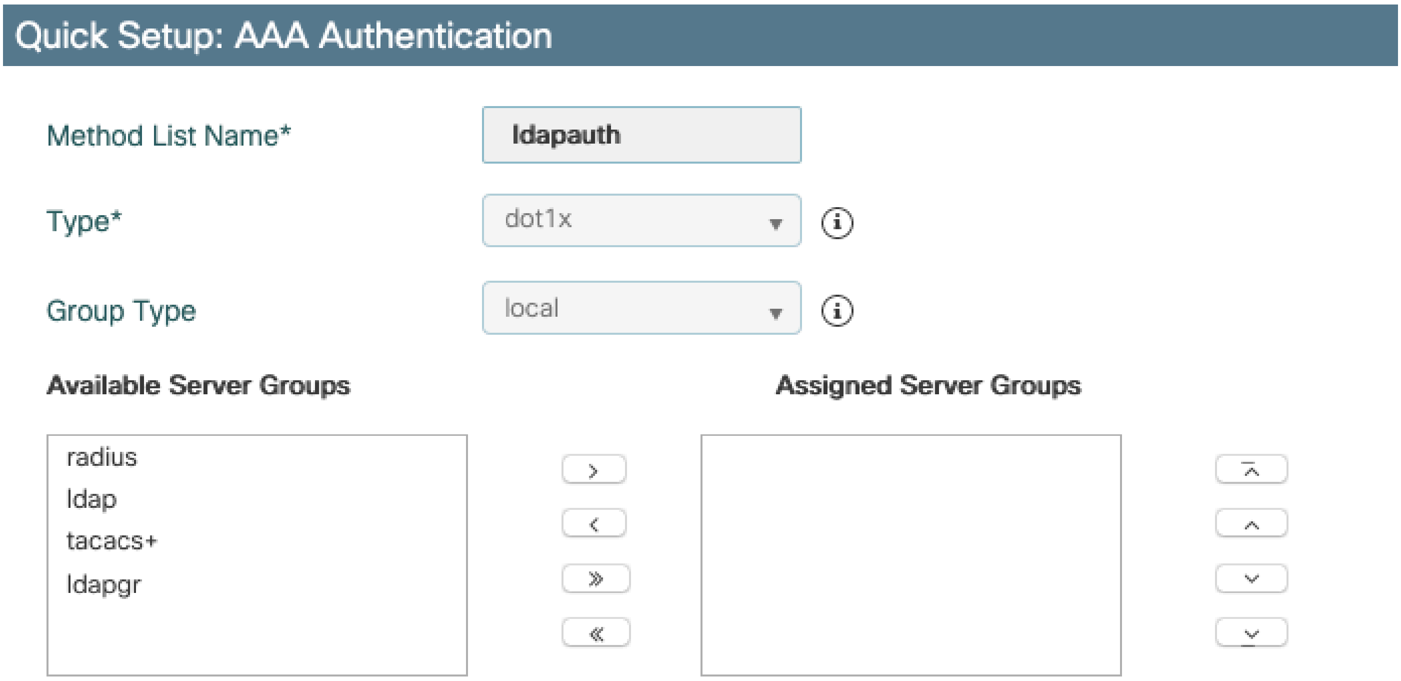
```
aaa group server ldap ldapgr server AD
```

ステップ4:AAA認証方式の設定

[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authentication] に移動し、[Add] をクリックします

dot1xタイプの認証方式を設定し、ローカルだけをポイントします。LDAPサーバグループを指すようになりがちですが、ここで802.1Xオーセンティケータとして機能するのはWLC自体です（ユ

ーザデータベースはLDAP上にありますが、これは認可方式のジョブです）。


Quick Setup: AAA Authentication

Method List Name*: ldapauth

Type*: dot1x

Group Type: local

Available Server Groups: radius, ldap, tacacs+, ldapgr

Assigned Server Groups:

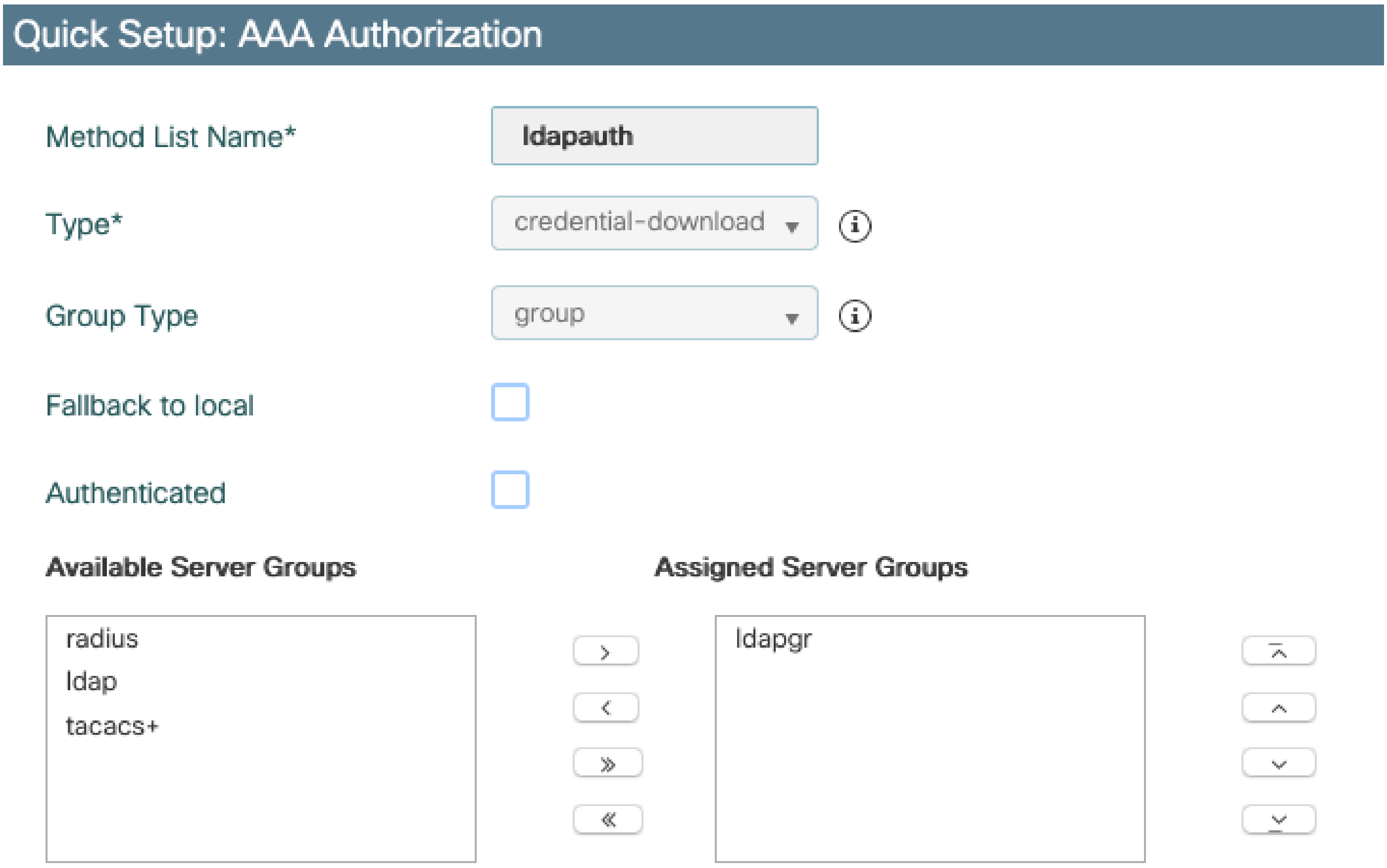
CLI コマンド:

```
aaa authentication dot1x ldapauth local
```

ステップ5:AAA認可方式の設定

[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authorization] に移動し、[Add] をクリックします

認可方式の**credential-download**タイプを作成し、LDAPグループをポイントするようにします。



Quick Setup: AAA Authorization

Method List Name* ldapauth

Type* credential-download

Group Type group

Fallback to local □

Authenticated □

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: ldapgr

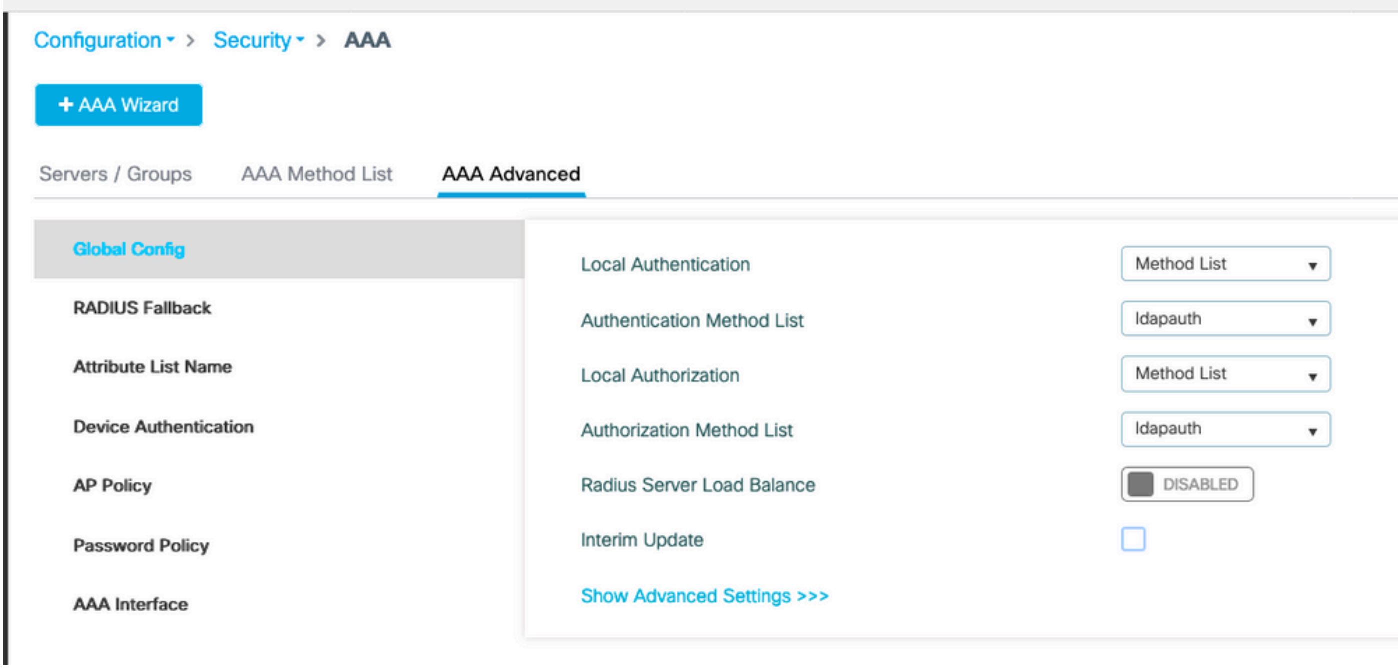
CLI コマンド:

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

ステップ6:ローカル認証の詳細を設定する

[Configuration] > [Security] > [AAA] > [AAA Method List] > [AAA advanced] に移動します。

認証と認可の両方に[Method List] を選択し、ローカルを指すdot1x認証方式と、LDAPを指すクレデンシャルダウンロード認証方式を選択します



Configuration > Security > AAA

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

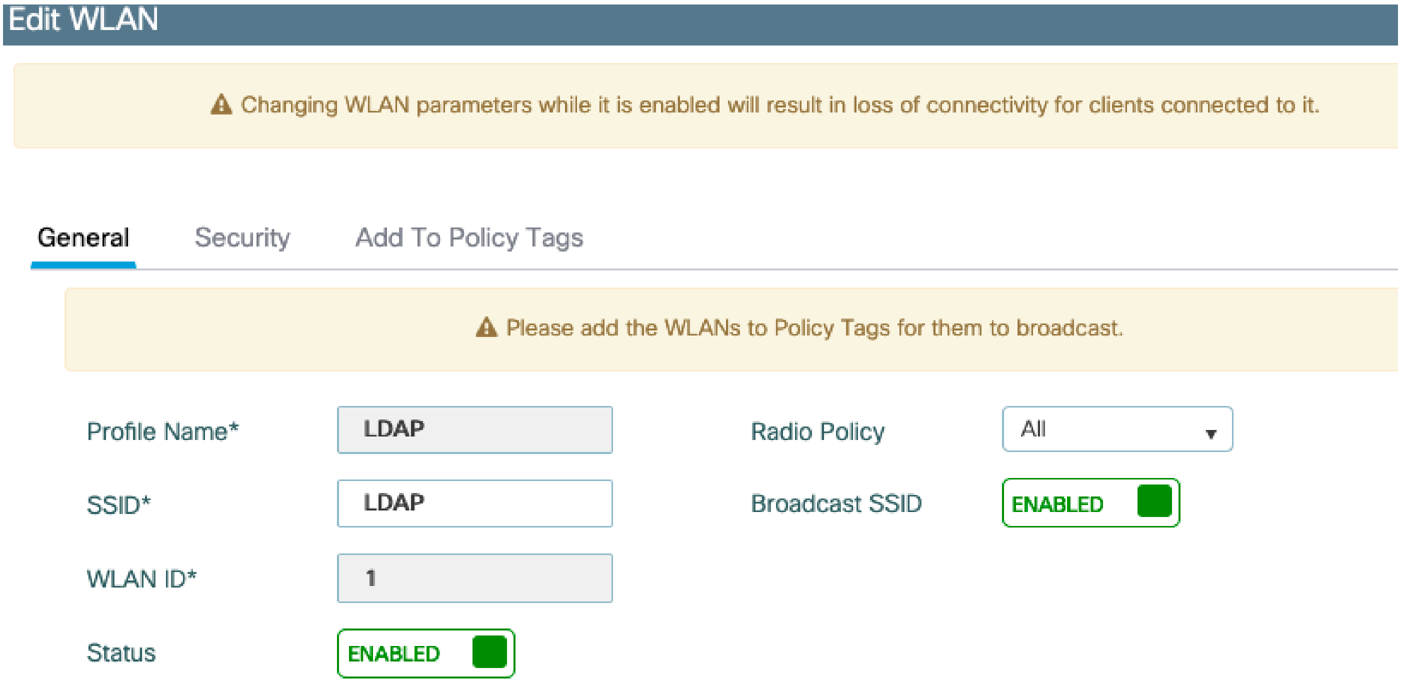
CLI コマンド:

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

手順7:dot1x WLANの設定

[Configuration] > [WLAN] に移動し、[Add] をクリックします

プロファイルとSSID名を選択し、有効になっていることを確認します。



Edit WLAN

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

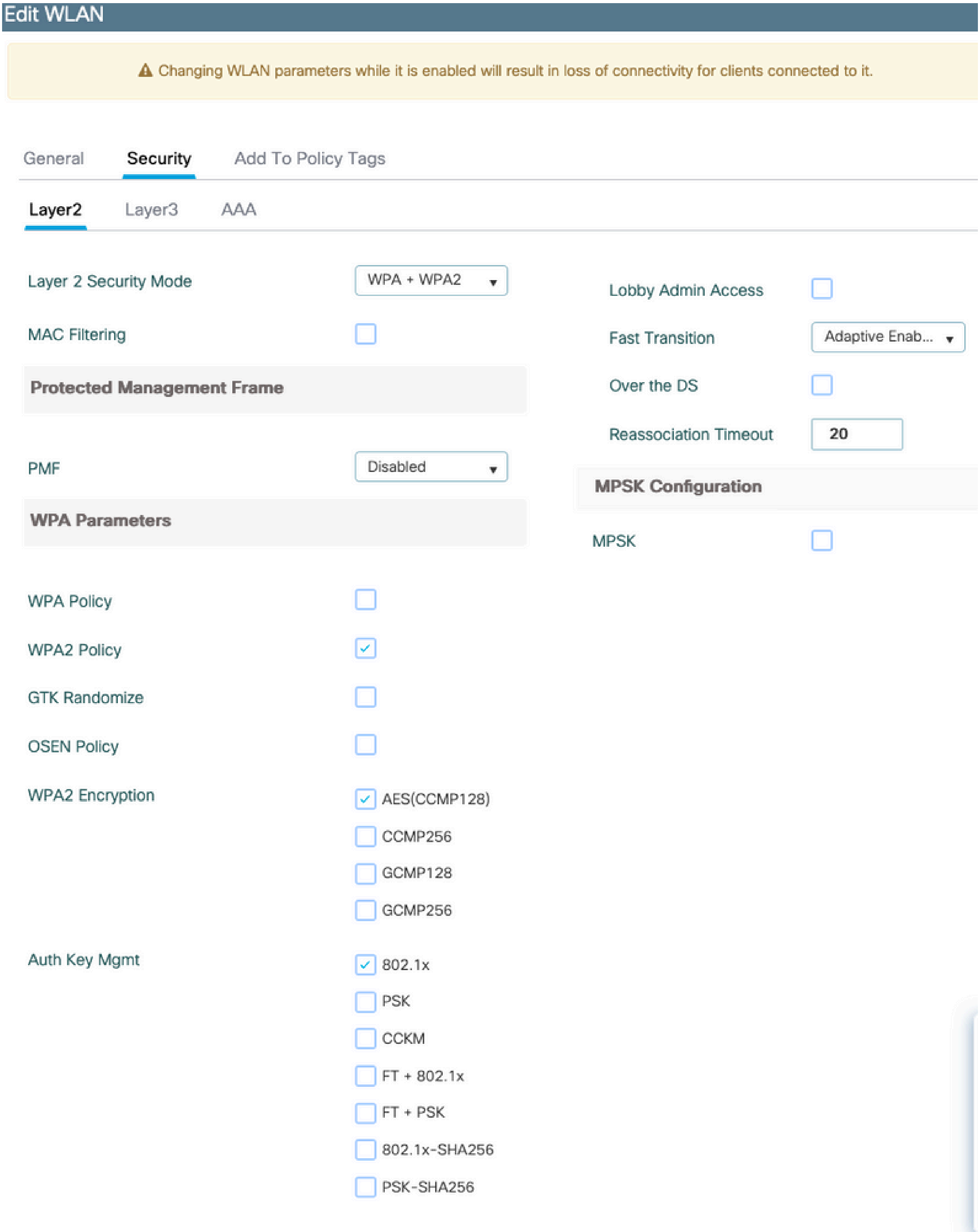
⚠ Please add the WLANs to Policy Tags for them to broadcast.

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

[Layer 2 security] タブに移動します。

レイヤ2セキュリティモードとして[WPA+WPA2]**を選択します。**

[WPA Parameters] でWPA2とAESが有効になっており、**802.1X**が有効になっていることを確認します



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: □

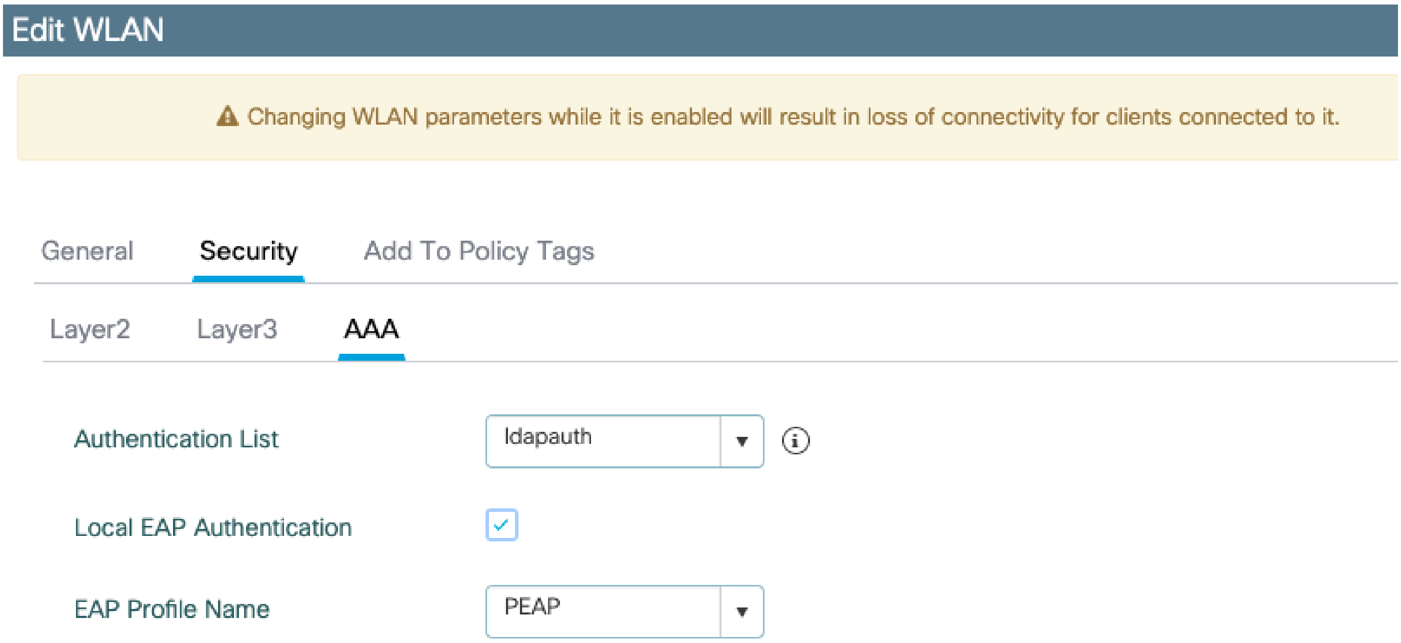
Reassociation Timeout: 20

MPSK Configuration

MPSK: □

AAAサブタブに移動します。

先ほど作成したdot1x認証方式を選択し、ローカルEAP認証を有効にして、最初の手順で設定したEAPプロファイルを選択します。


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

[Apply]をクリックして保存します。

CLI コマンド:

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

ステップ8:WLANがブロードキャストされていることを確認する

[Configuration] > [Tags] に移動し、そのSSIDがSSIDによって現在サービスされているポリシープロファイルに含まれていることを確認します（まだタグを設定していない場合の新しい設定用のdefault-policy-tag）。 デフォルトでは、default-policy-tagは、手動で組み込むまで、作成した新しいSSIDをブロードキャストしません。

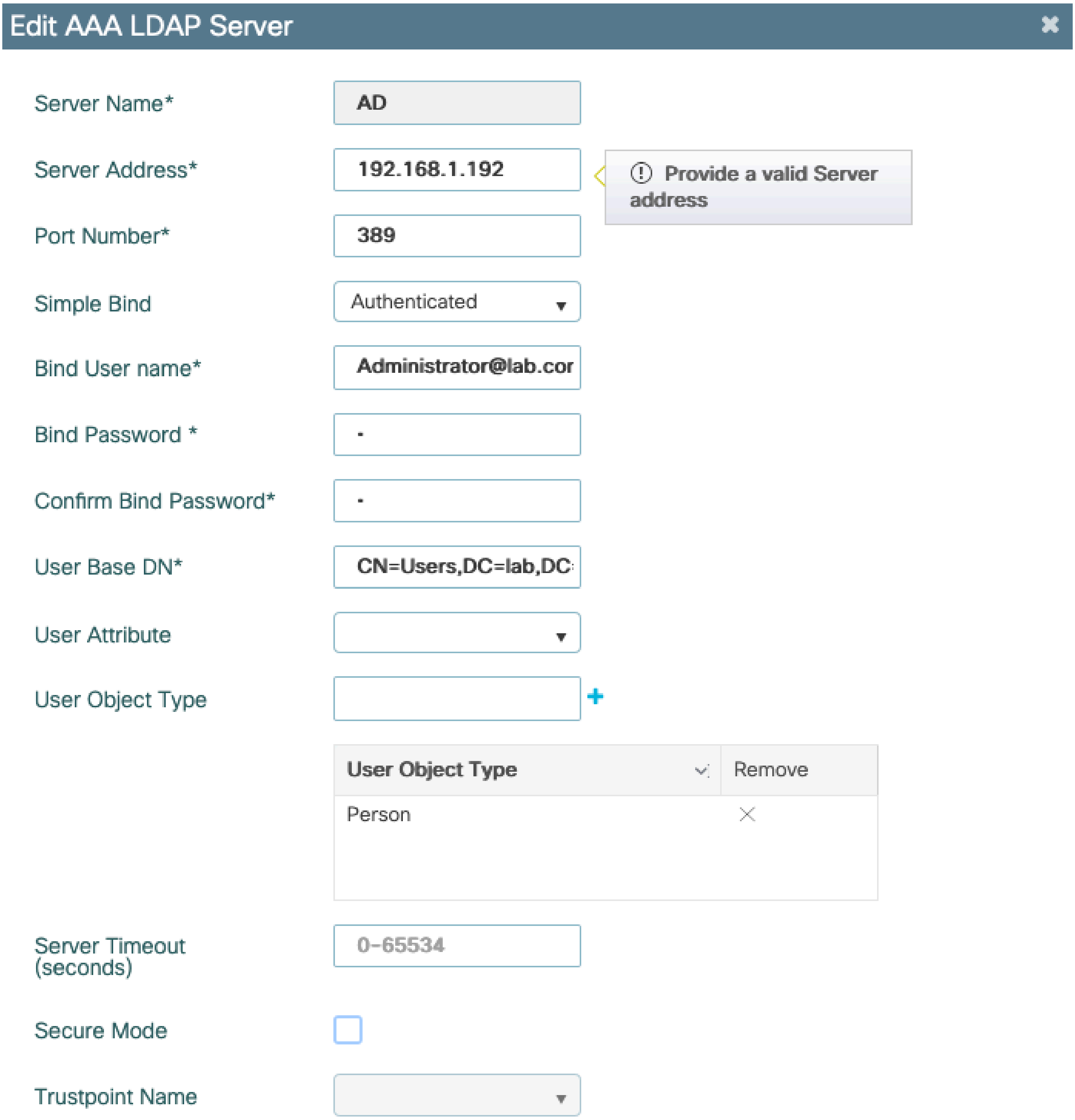
この記事では、ポリシープロファイルの設定については説明せず、設定のその部分に精通していることを前提としています。

Active Directoryを使用している場合は、属性「userPassword」を送信するようにADサーバを設定する必要があります。 この属性をWLCに送信する必要があります。これは、WLCがADサーバではなく検証を実行するためです。また、パスワードがクリアテキストで送信されないため、LDAPデータベースで確認できないため、PEAP-mschapv2方式での認証に問題が発生する場合があります。PEAP-GTC方式のみが特定のLDAPデータベースで機能します。

LDAPサーバの詳細について

9800 Web UIのフィールドについて

9800で設定されたLDAPサーバとして機能する非常に基本的なActive Directoryの例を次に示します



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	×

名前とIPは分かりやすく説明されています。

Port：389はLDAPのデフォルトポートですが、サーバは別のポートを使用できます。

簡易バインド：最近では、認証されていないバインドをサポートするLDAPデータベースを持つことは非常にまれです（つまり、認証形式を持たない誰でもLDAP検索を実行できます）。 認証された簡易バインドは、最も一般的な種類の認証であり、Active Directoryがデフォルトで許可する認証です。管理者アカウント名とパスワードを入力すると、そこからユーザデータベース内で検索を実行できます。

Bind Username:Active Directoryで管理者権限を持つユーザ名を指定する必要があります。ADでは「user@domain」形式を使用できますが、他の多くのLDAPデータベースではユーザ名に「

CN=xxx,DC=xxx」形式を使用できます。AD以外のLDAPデータベースの例については、この記事の後半で説明します。

バインドパスワード：前に入力したadminユーザ名のパスワードを入力します。

ユーザベースDN:「検索ルート」を入力します。これは、検索が開始されるLDAPツリー内の場所です。この例では、すべてのユーザが「Users」グループに属しています。このグループのDNは「CN=Users,DC=lab,DC=com」です(例のLDAPドメインはlab.comであるため)。 このユーザベースDNを確認する方法の例は、このセクションで後述します。

User Attribute:これは空のままにすることも、LDAPデータベースのユーザ名としてカウントされるLDAPフィールドを示すLDAP属性マップをポイントすることもできます。ただし、Cisco Bug ID CSCv11813 WLCは、CNフィールドを使用して認証を試みます。

ユーザオブジェクトタイプ：これにより、ユーザと見なされるオブジェクトのタイプが決まります。通常は「個人」です。 ADデータベースがあり、コンピュータアカウントを認証する場合は「コンピュータ」ですが、LDAPでは多くのカスタマイズが提供されます。

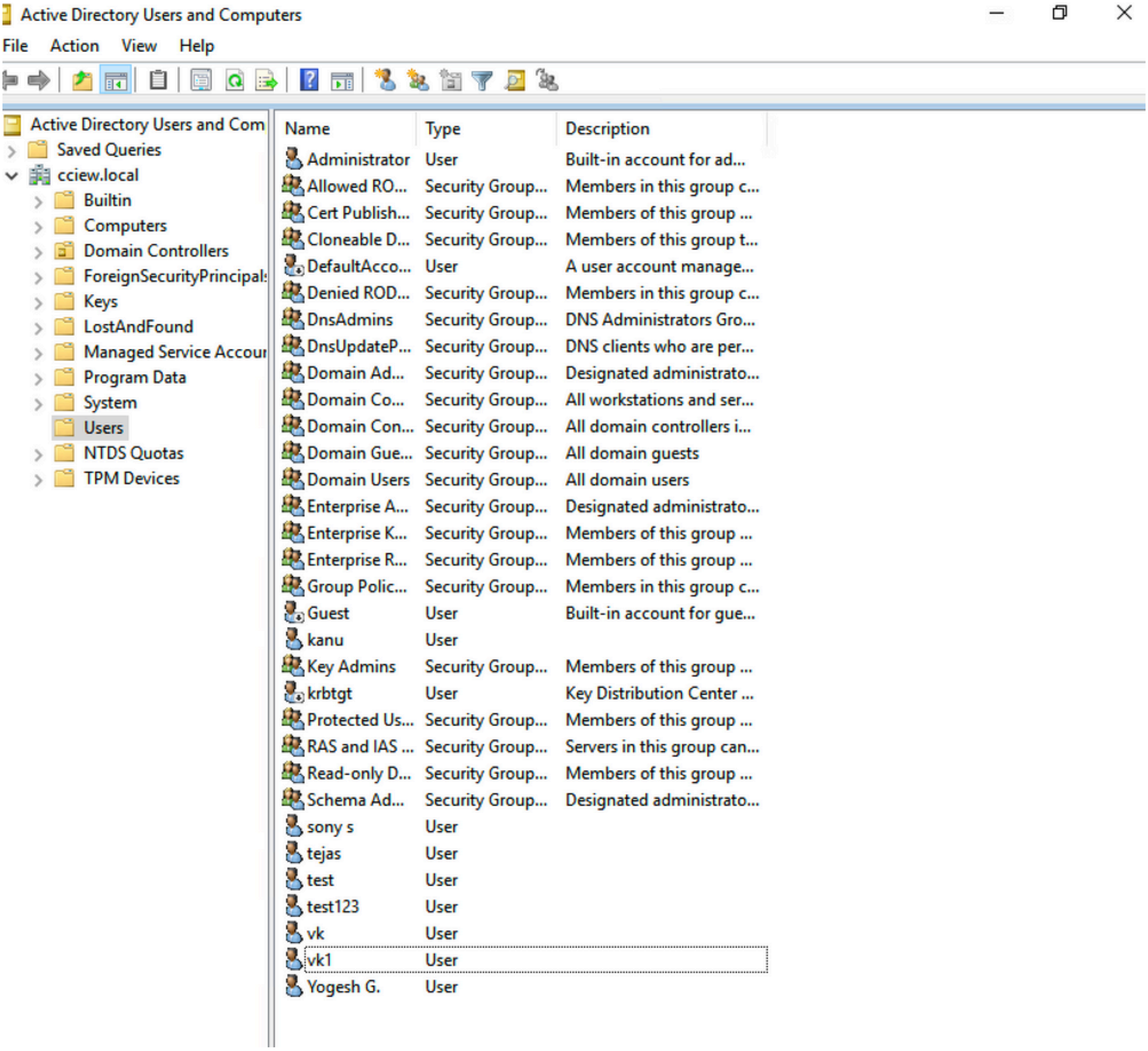
セキュアモードでは、Secure LDAP over TLSが有効になり、TLS暗号化に証明書を使用するには、9800でトラストポイントを選択する必要があります。

sAMAaccountName属性を使用したLDAP 802.1x認証。

この拡張は、17.6.1バージョンで導入されました。

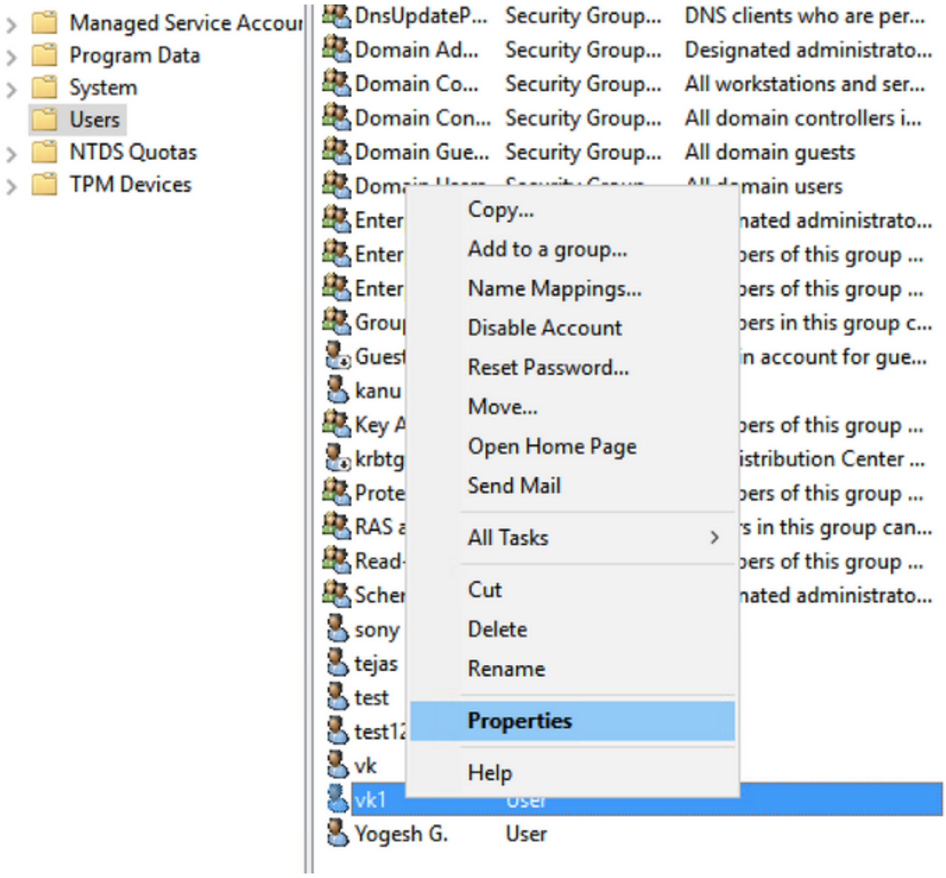
ユーザの「userPassword」属性を設定します。

ステップ1:Windowsサーバで、[ActiveDirectory Users and Computers]に移動します

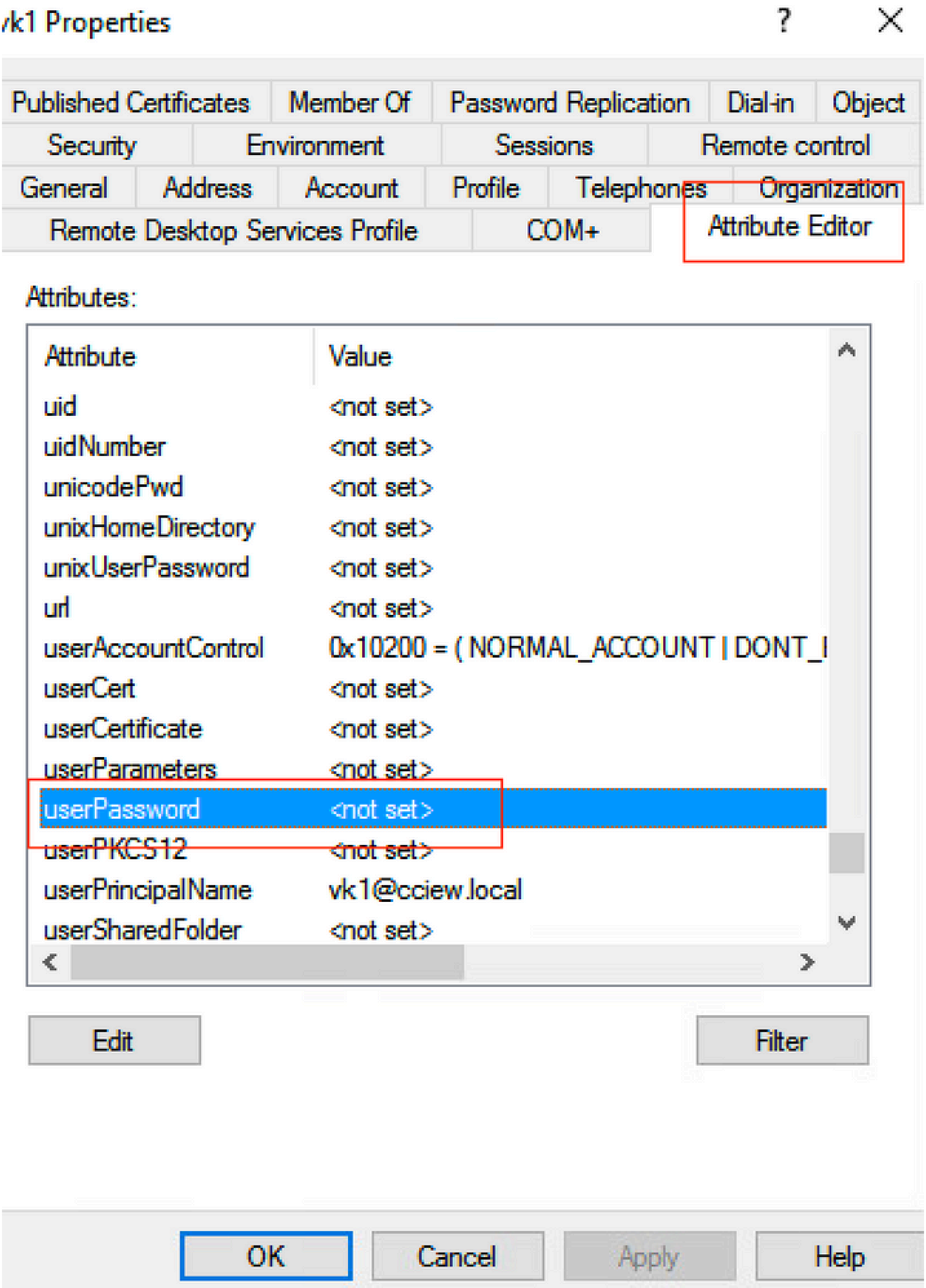


Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	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	

ステップ2：該当するユーザ名を右クリックし、[properties]を選択します


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
Dom... All domain users
Enter ...nated administrato...
Enter ...bers of this group ...
Enter ...bers of this group ...
Grou ...bers in this group c...
Guest ...n account for gue...
kanu
Key A ...bers of this group ...
krbtg ...istribution Center ...
Prote ...bers of this group ...
RAS a ...s in this group can...
Read ...bers of this group ...
Scher ...nated administrato...
sony
tejas
test
test12
vk
vk1 User
Yogesh G. User
Copy...
Add to a group...
Name Mappings...
Disable Account
Reset Password...
Move...
Open Home Page
Send Mail
All Tasks
Cut
Delete
Rename
Properties
Help

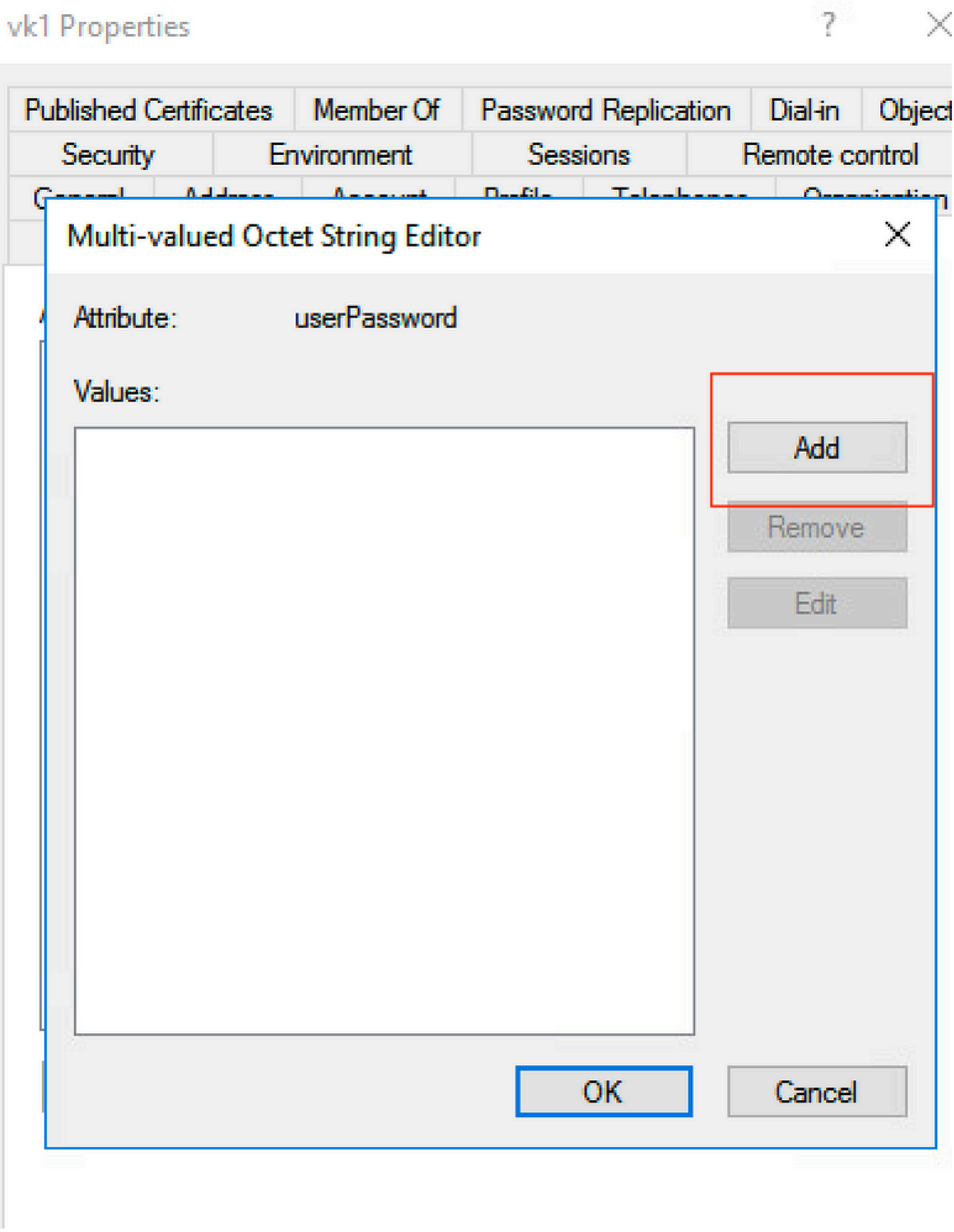
ステップ3:[Properties]ウィンドウで[Attribute Editor]を選択します



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>

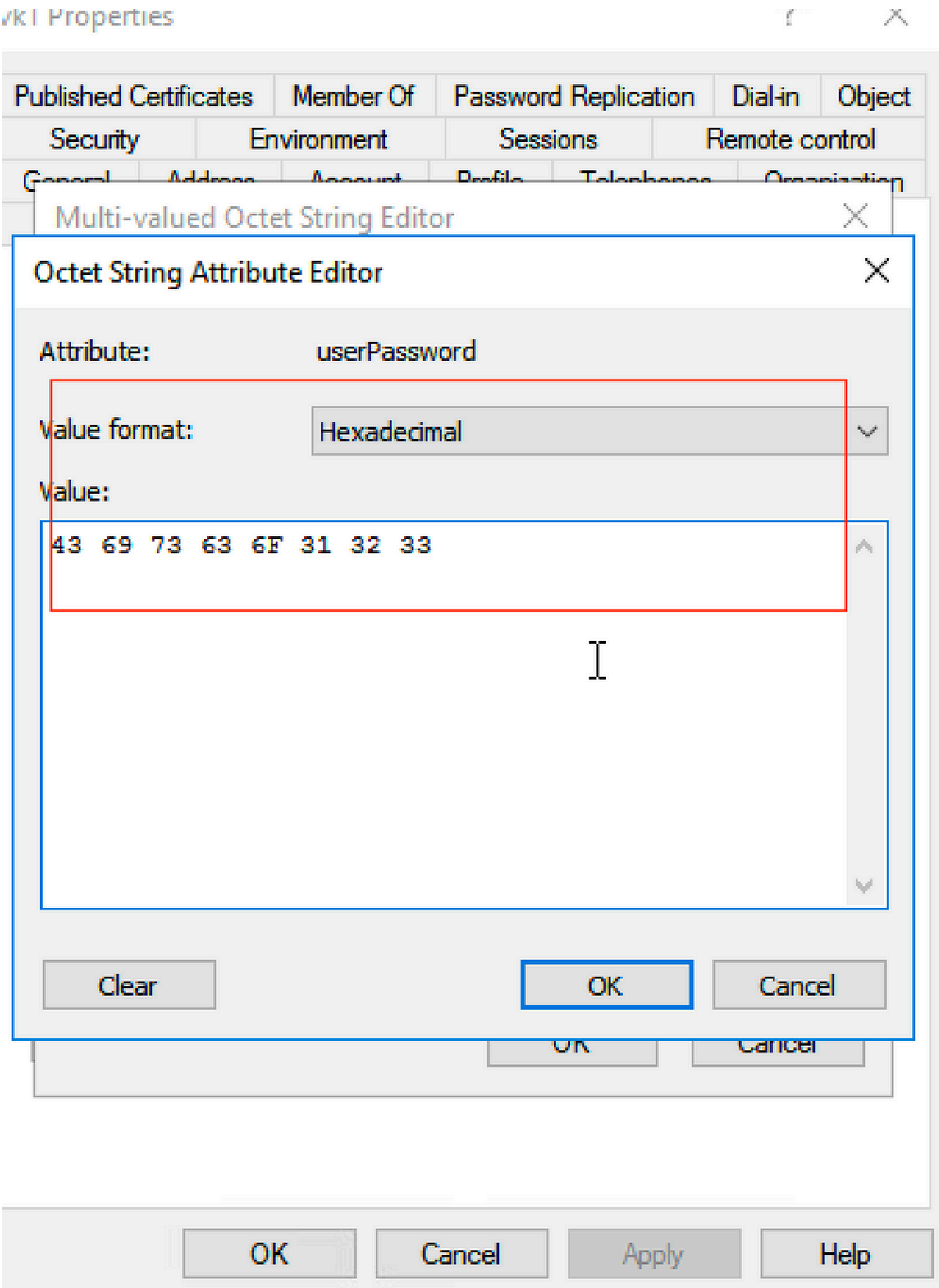
ステップ4:「userPassword」属性を設定します。これはユーザのパスワードで、16進数値で設定

する必要があります。



Attribute: userPassword

Values:



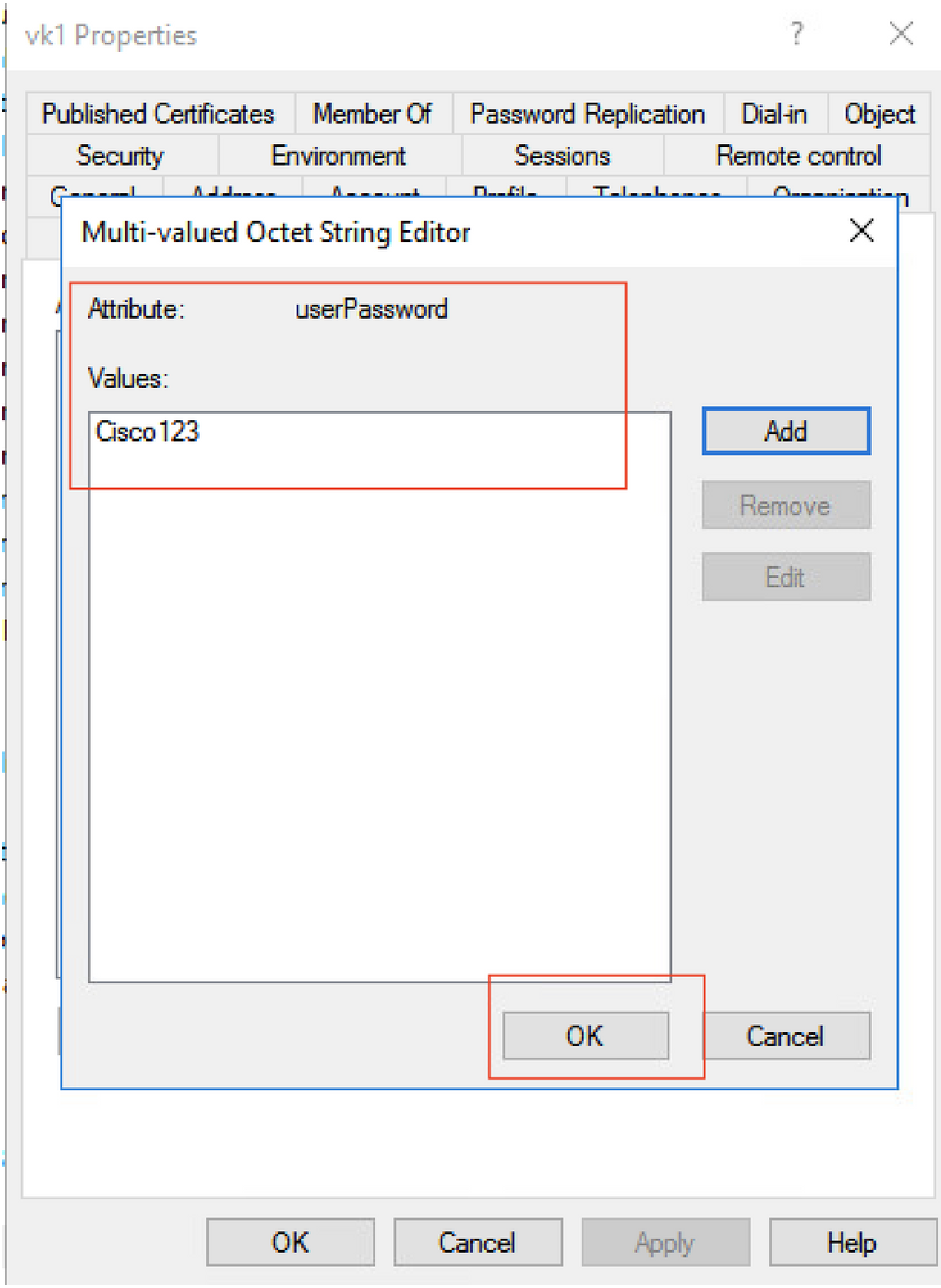
Attribute: userPassword

Value format: Hexadecimal

Value:

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

[ok]をクリックし、正しいパスワードが表示されることを確認します

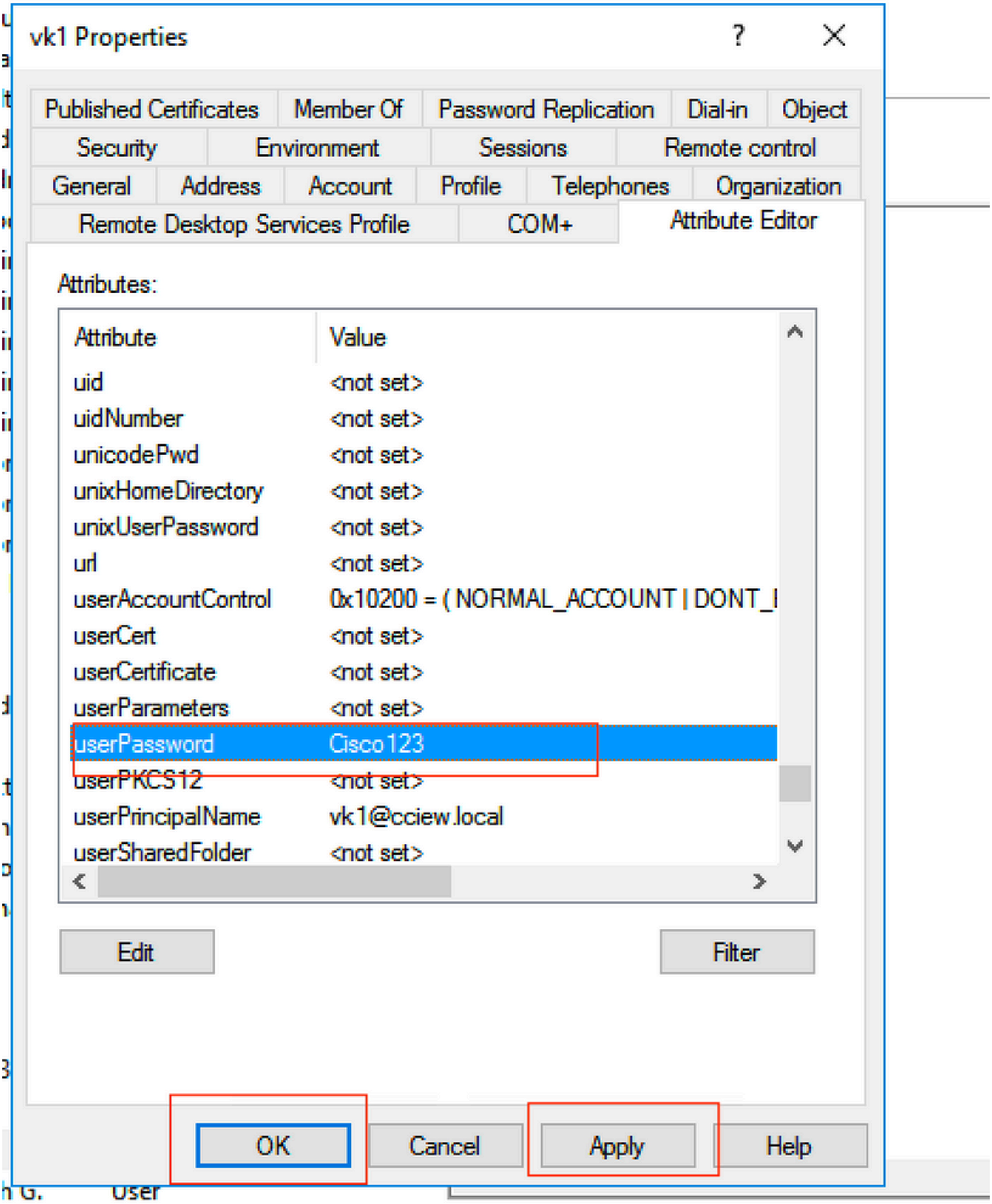


Attribute: userPassword

Values:

Cisco123

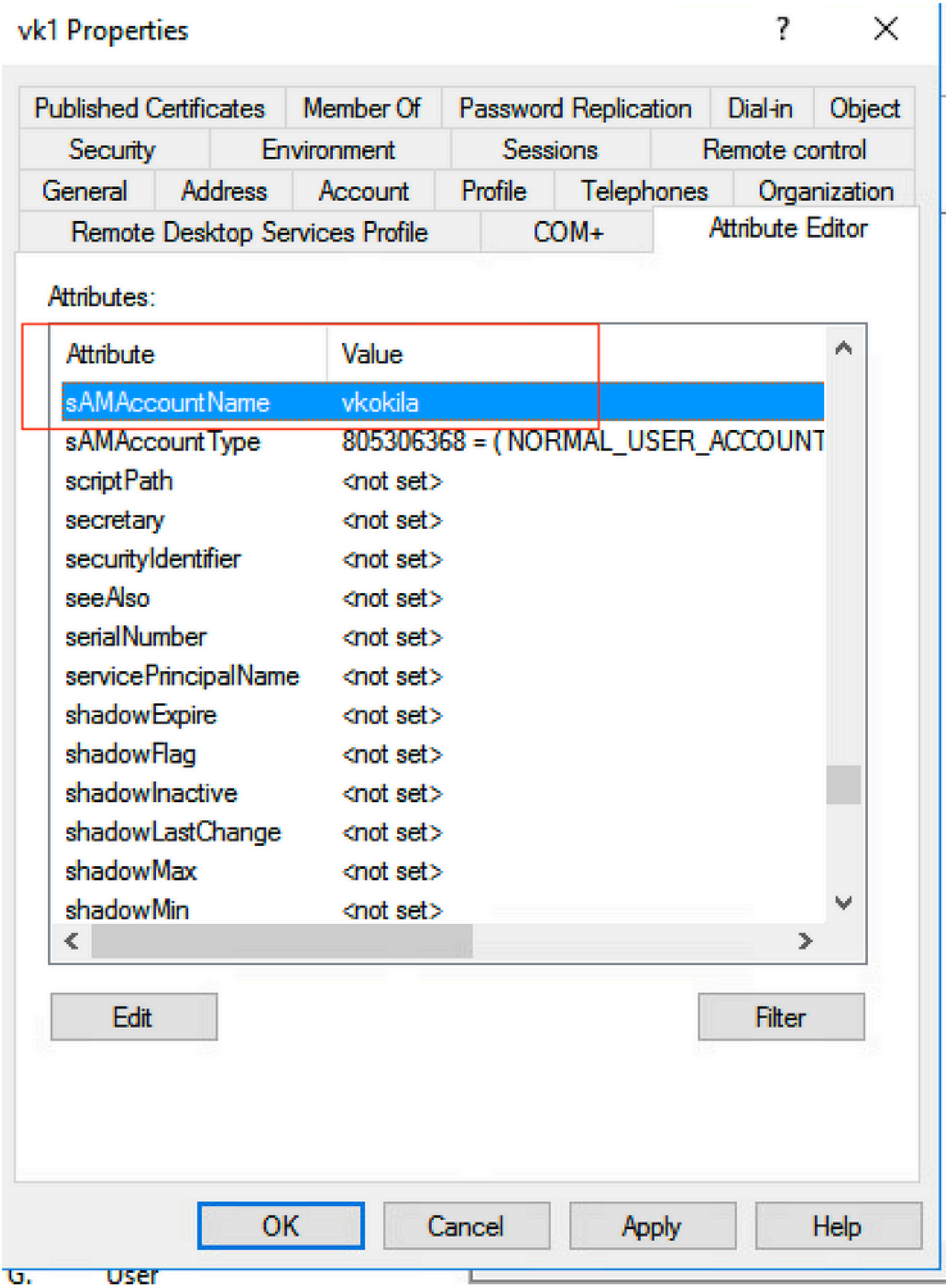
ステップ5:[Apply]をクリックし、[OK]をクリックします。



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	Cisco123
userPKCS12	<not set>
userPrincipalName	vk1@cciew.local
userSharedFolder	<not set>

ステップ6：ユーザの「sAMAccountName」属性値と、認証用のユーザ名を確認します。



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>

WLC の設定:

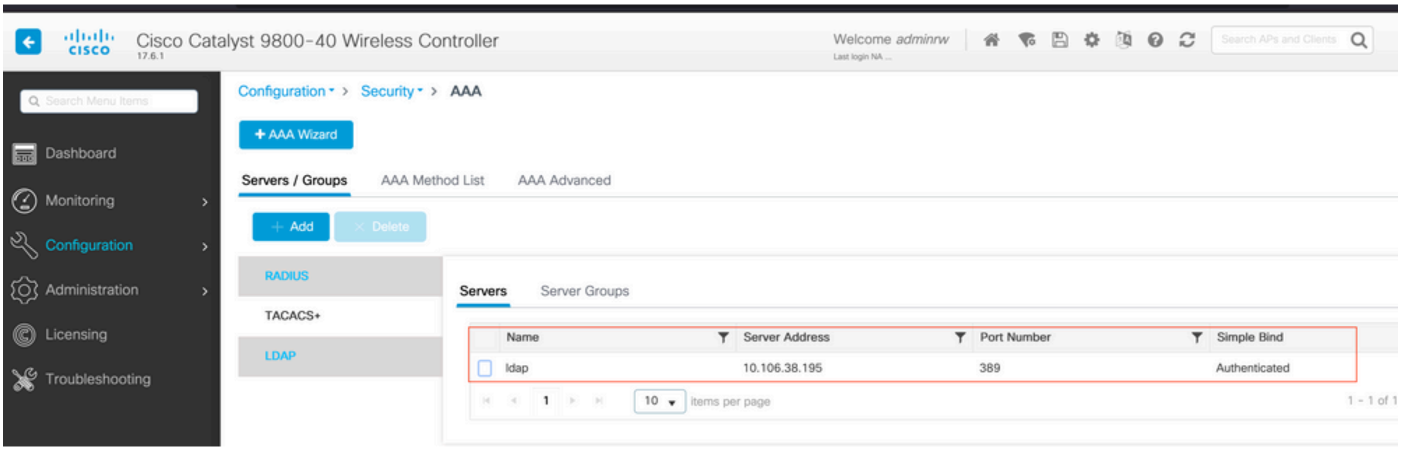
ステップ1:LDAP属性マップの作成

ステップ2:「sAMAccountName」属性を設定し、「username」と入力します。

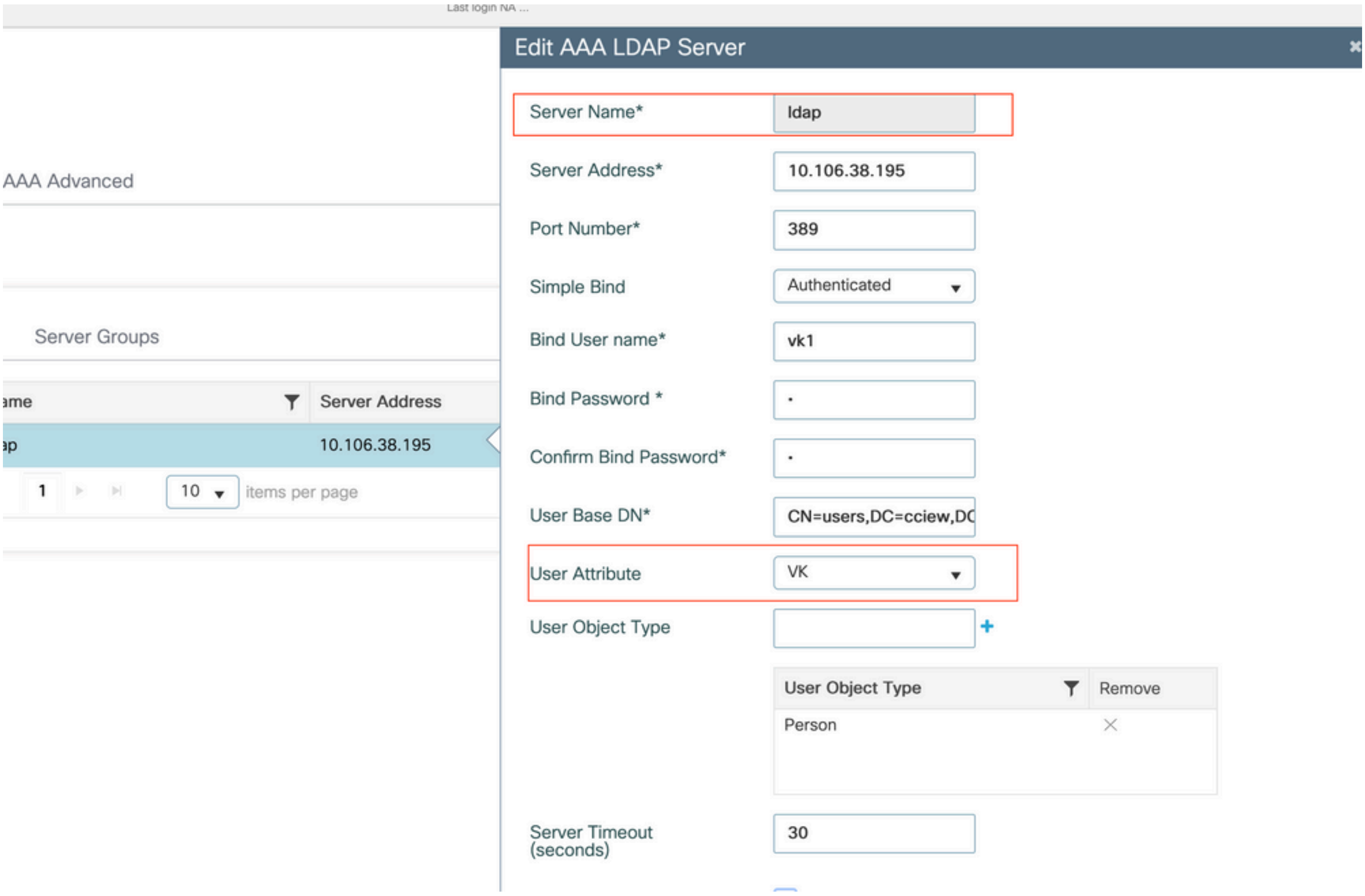
ステップ3:LDAPサーバ設定で、作成した属性MAPを選択します。

```
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
```

Webインターフェイスから確認します。



Name	Server Address	Port Number	Simple Bind
ldap	10.106.38.195	389	Authenticated



Edit AAA LDAP Server

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

確認

設定を確認するには、CLIコマンドをこの記事のコマンドで再確認します。

通常、LDAPデータベースには認証ログがないため、何が起こっているかを把握するのは困難です。LDAPデータベースへの接続が確立されているかどうかを確認するためにトレースとスニファキャプチャを実行する方法については、この記事の「トラブルシューティング」セクションを参照してください。

トラブルシュート

これをトラブルシューティングするには、これを2つの部分に分割するのが最適です。最初の部分は、ローカルEAP部分の検証です。2つ目は、9800がLDAPサーバと正しく通信していることを検証することです。

コントローラの認証プロセスを確認する方法

クライアント接続の「デバッグ」を取得するために、放射性トレースを収集できます。

[Troubleshooting] > [Radioactive Trace] に移動します。クライアントのMACアドレスを追加し（クライアントが独自のMACではなくランダムなMACを使用している可能性があることに注意してください。クライアントデバイス自体のSSIDプロファイルでこれを確認できます）、startを押します。

接続の試行を再現したら、[Generate]をクリックして過去X分間のログを取得できます。一部のLDAPログ行は表示されないため、internalをクリックしてください。

次に、Web認証SSIDで正常に認証されるクライアントの放射性トレースの例を示します。一部の冗長パーツは、分かりやすくするために取り外されました（図16を参照）。

```
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
```

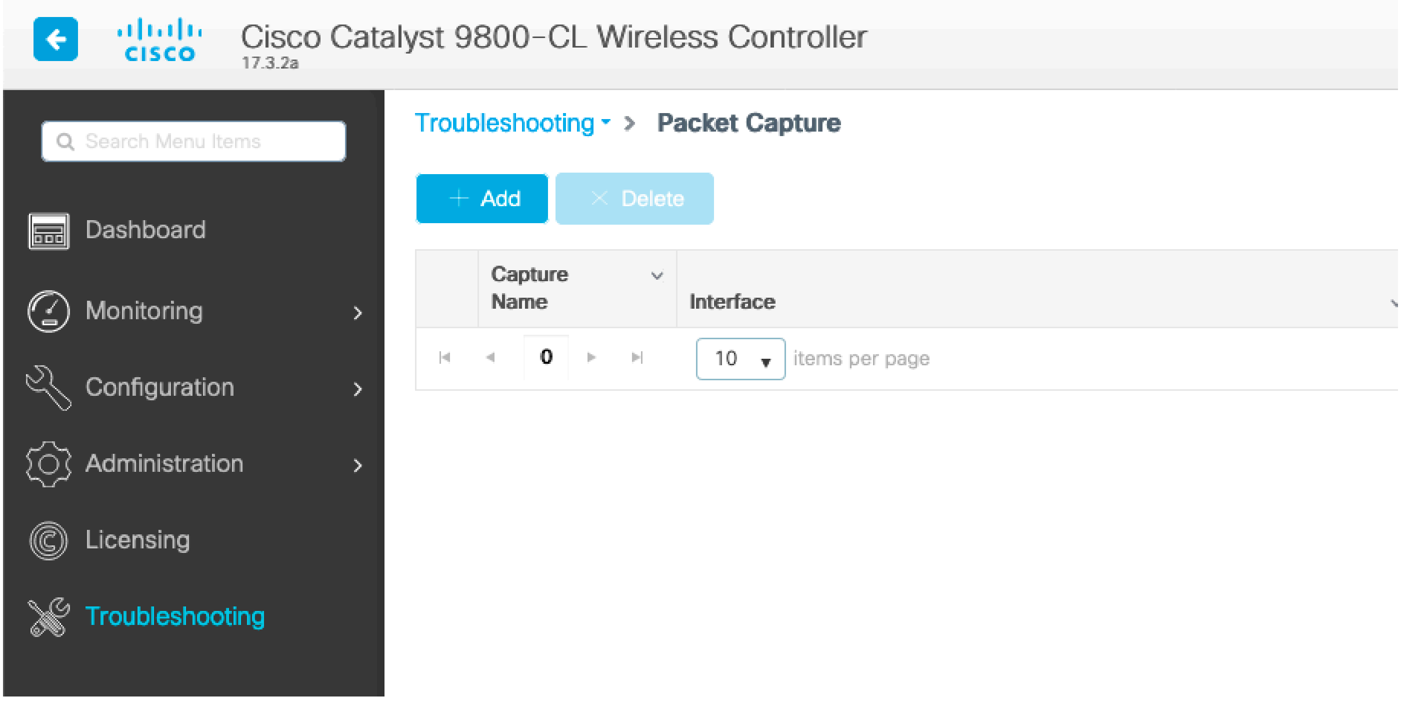
```
Safari/537.36 2021/01/19 21:58:06.720038 {wncd_x_R0-0}{1}: [webauth-error] [9347]: (info):
capwap_90000004[2e1f.3a65.9c09][ 192.168.1.17]Parse logo GET, File "/favicon.ico" not found
2021/01/19 21:58:06.720623 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2e1f.3a65.9c09:capwap_90000004] auth mgr 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
```

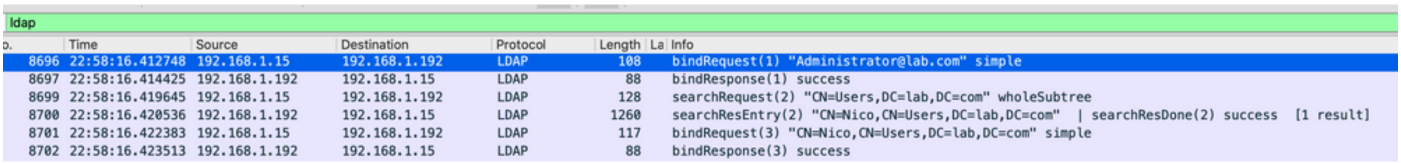
9800からLDAPへの接続を確認する方法

9800に埋め込まれたキャプチャを取得して、LDAPに向かうトラフィックを確認できます。

WLCからキャプチャを取得するには、[Troubleshooting] > [Packet Capture] に移動し、[Add] をクリックします。アップリンクポートを選択し、キャプチャを開始します。



次に、ユーザNicoの成功認証の例を示します



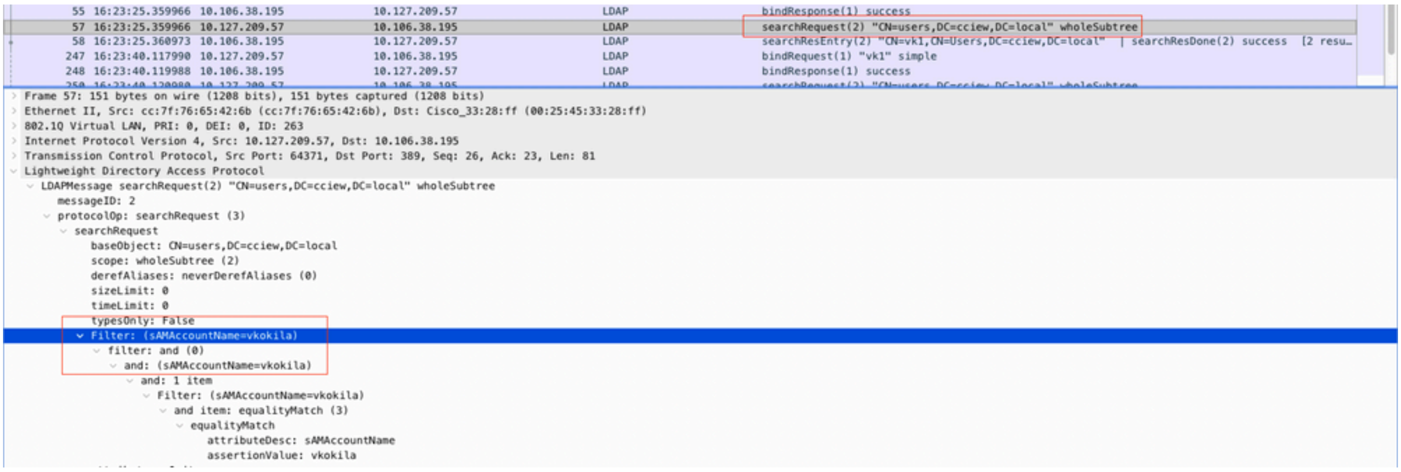
```
ldap
o.    Time             Source         Destination    Protocol  Length La Info
 8696 22:58:16.412748 192.168.1.15   192.168.1.192  LDAP        108    bindRequest(1) "Administrator@lab.com" simple
 8697 22:58:16.414425 192.168.1.192  192.168.1.15   LDAP         88    bindResponse(1) success
 8699 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
```

最初の2つのパケットは、LDAPデータベースにバインドしているWLCを表します。これは、管理ユーザがデータベースに対して認証しているWLCです（検索を実行できるようにするため）。

これら2つのLDAPパケットは、ベースDN（ここではCN=Users,DC=lab,DC=com）での検索を実行するWLCを表します。 パケットの内部には、ユーザ名（ここでは「Nico」）のフィルタが含まれています。 LDAPデータベースは、ユーザ属性を正常に返します

最後の2つのパケットは、パスワードが正しいかどうかをテストするために、そのユーザパスワードで認証を試みるWLCを表します。

1. EPCを収集し、「sAMAccountName」がフィルタとして適用されているかどうかを確認します。



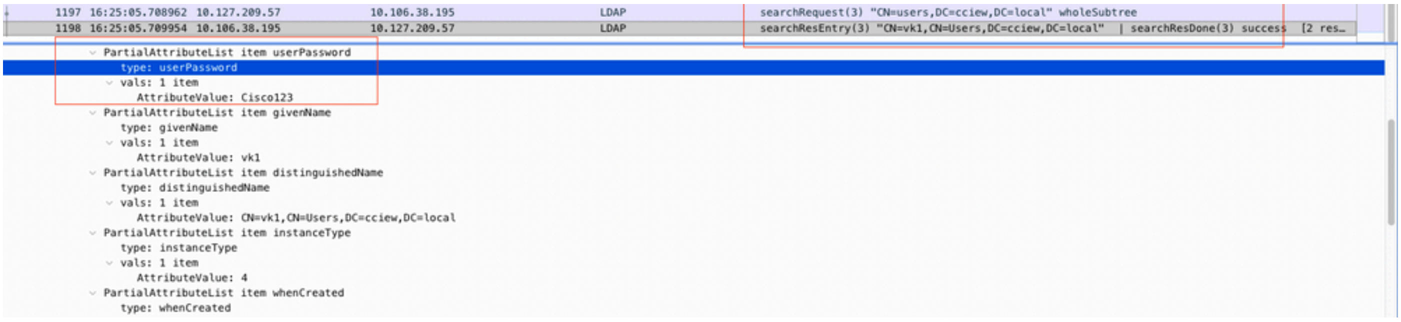
```
   55 16:23:25.359966 10.106.38.195    10.127.209.57    LDAP    bindResponse(1) success
   57 16:23:25.359966 10.127.209.57    10.106.38.195    LDAP    searchRequest(2) "CN=users,DC=cciew,DC=local" wholeSubtree
   58 16:23:25.360973 10.106.38.195    10.127.209.57    LDAP    searchResEntry(2) "CN=vk1,CN=Users,DC=cciew,DC=local"  | 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 16:23:40.120980 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
```

フィルタに「cn」と表示され、ユーザ名として「sAMAccountName」が使用されている場合、認

証は失敗します。

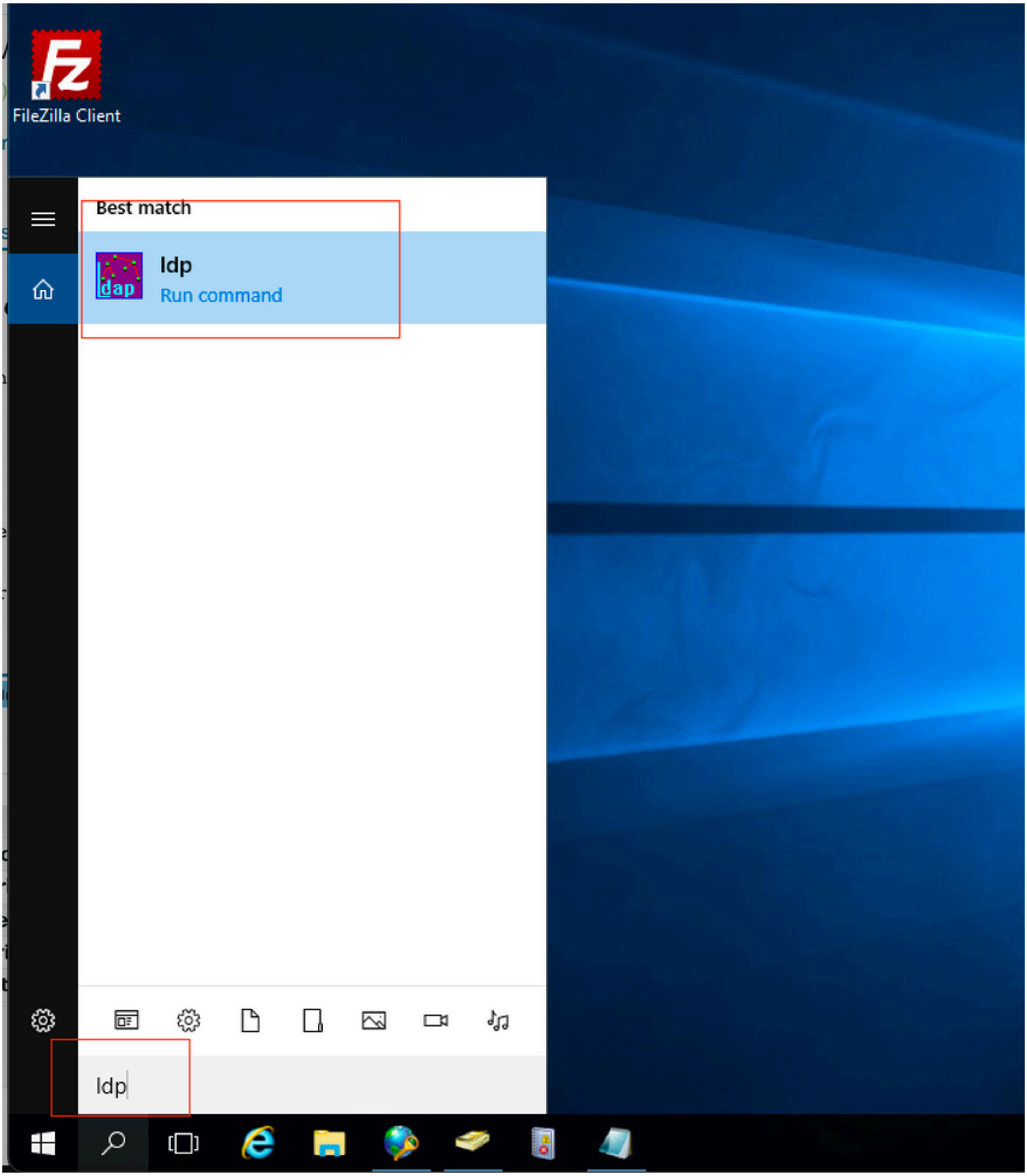
WLC CLIからLDAPマップ属性を再設定します。

2. サーバがクリアテキストで「userPassword」を返すことを確認します。そうでない場合、認証は失敗します。

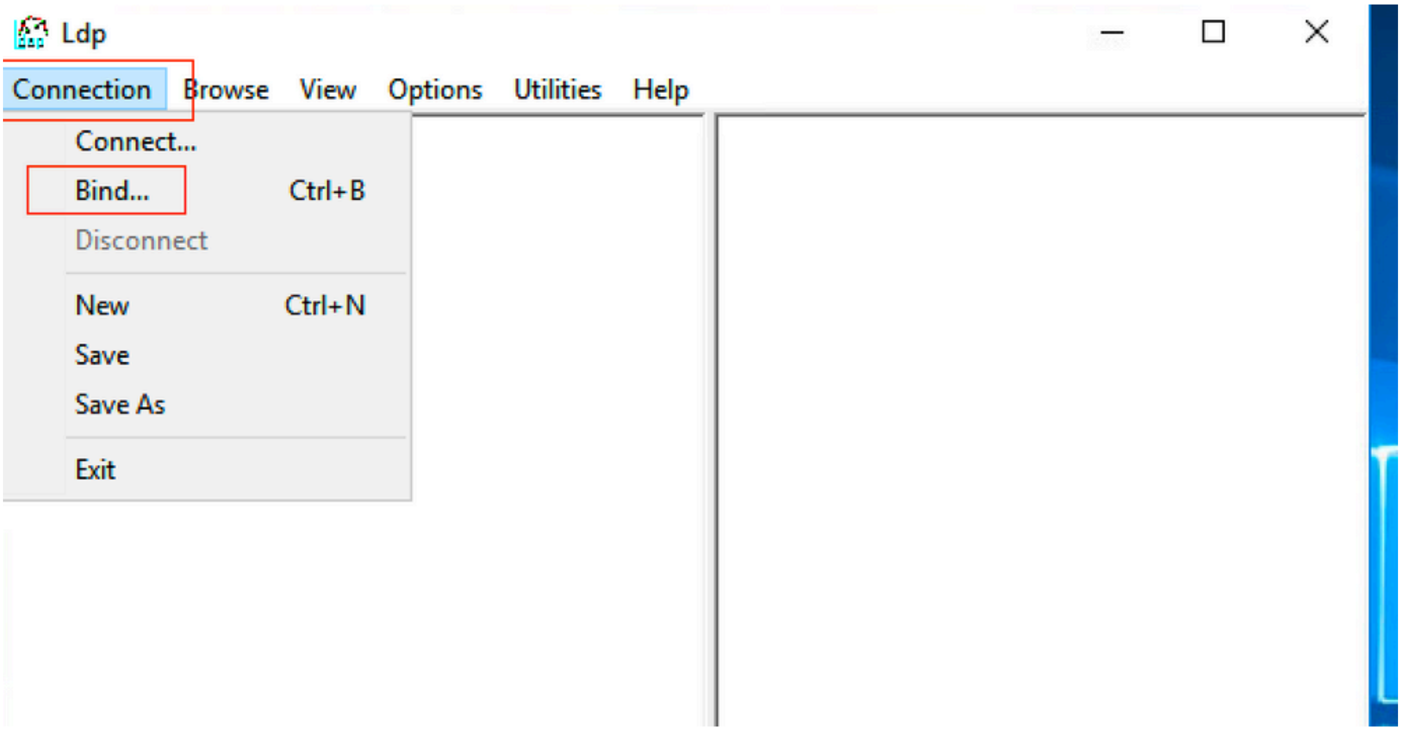


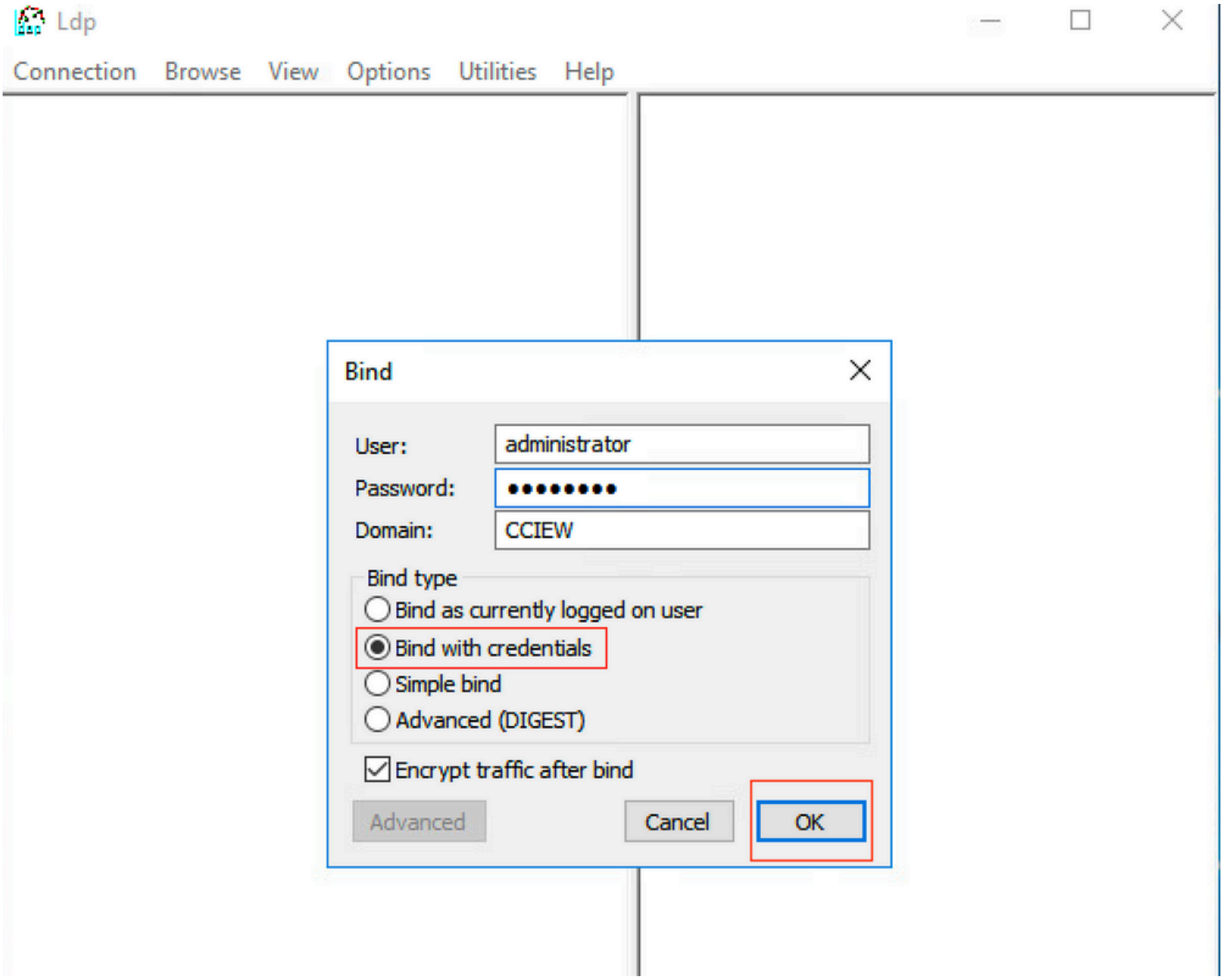
```
1197 16:25:05.708962 10.127.209.57     10.106.38.195     LDAP     searchRequest(3) "CN=users,DC=cciew,DC=local" wholeSubtree
1198 16:25:05.709954 10.106.38.195     10.127.209.57     LDAP     searchResEntry(3) "CN=vk1,CN=Users,DC=cciew,DC=local"  | searchResDone(3) success  [2 res…
    ⌄ PartialAttributeList 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. サーバでldp.exeツールを使用して、ベースDN情報を検証します。



FileZilla Client
Best match
ldp
Run command
ldp





User: administrator

Password: •••••••••

Domain: CCIEW

Bind type

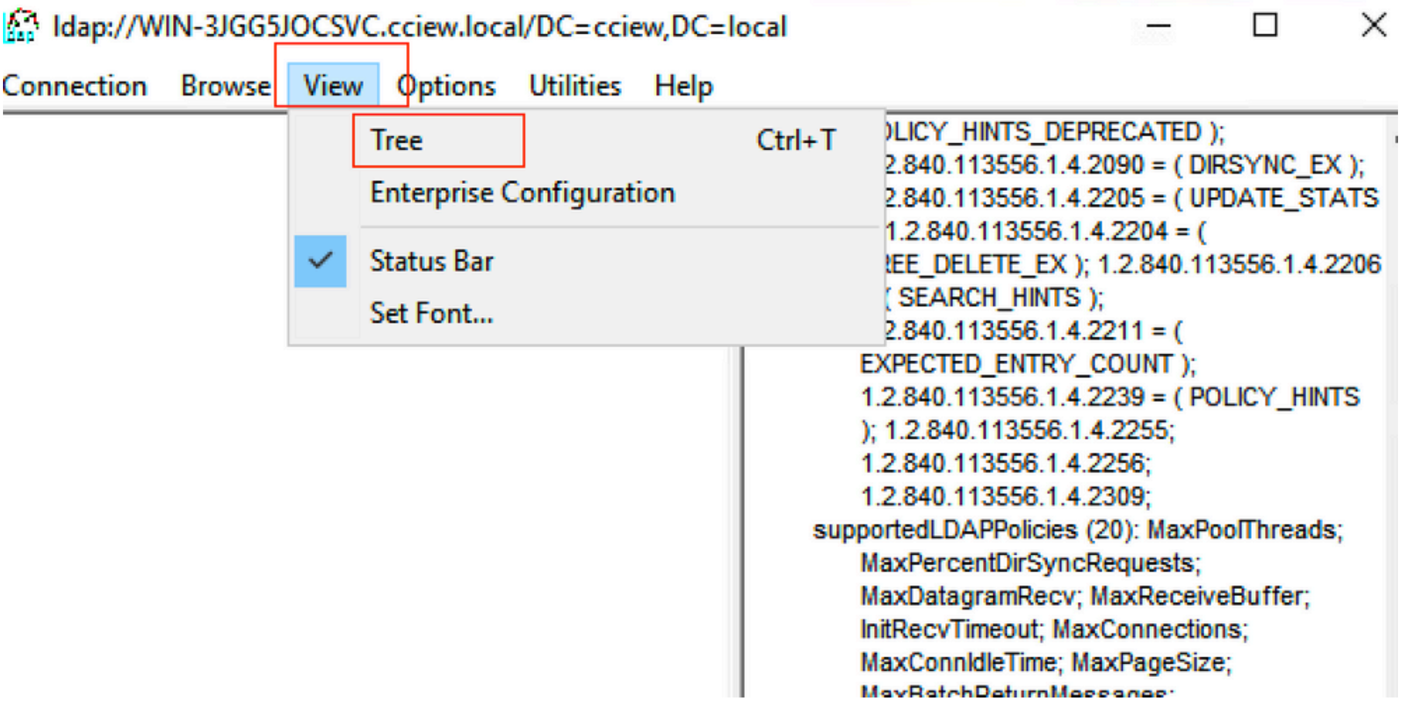
○ Bind as currently logged on user

● Bind with credentials

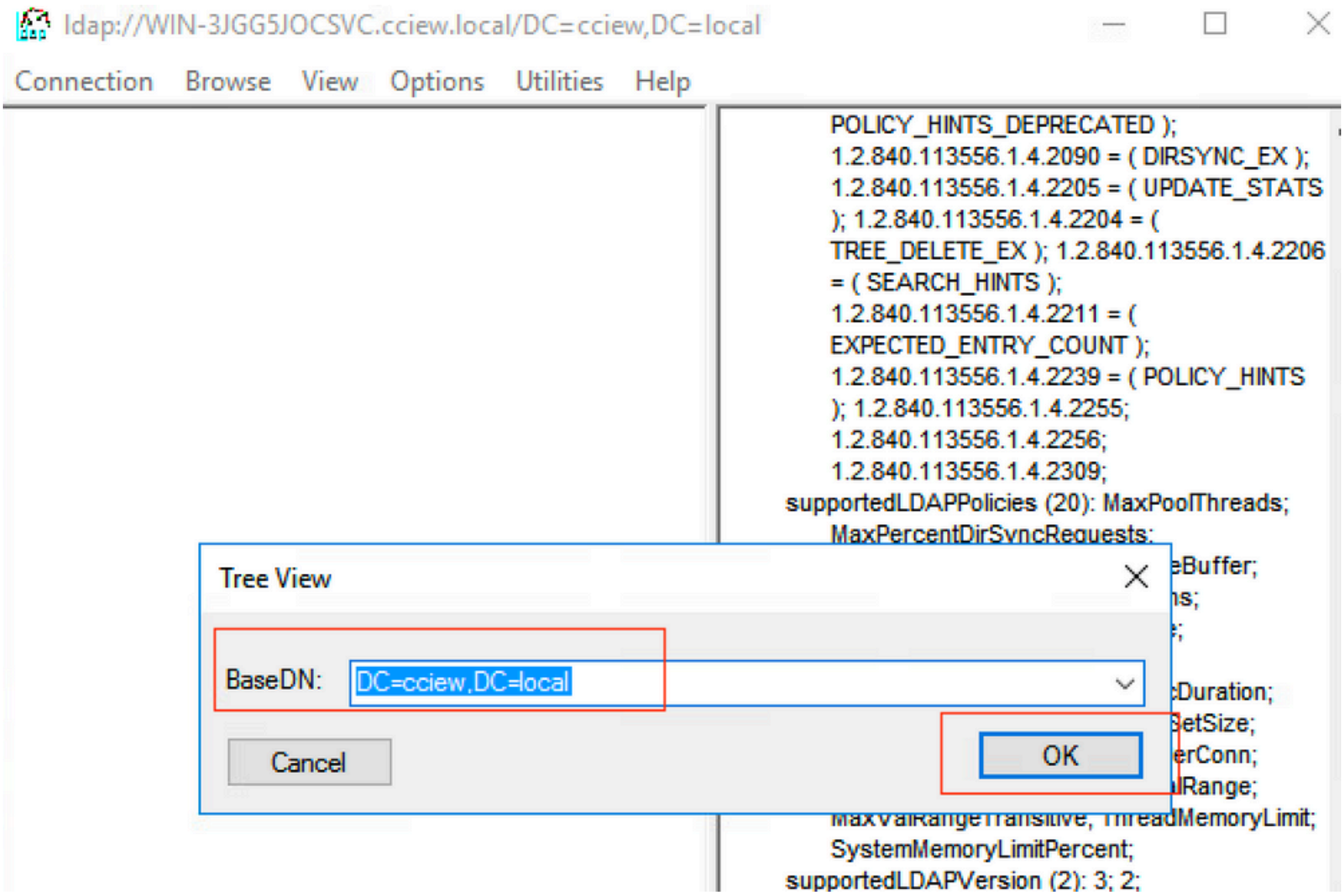
○ Simple bind

○ Advanced (DIGEST)

☑ Encrypt traffic after bind

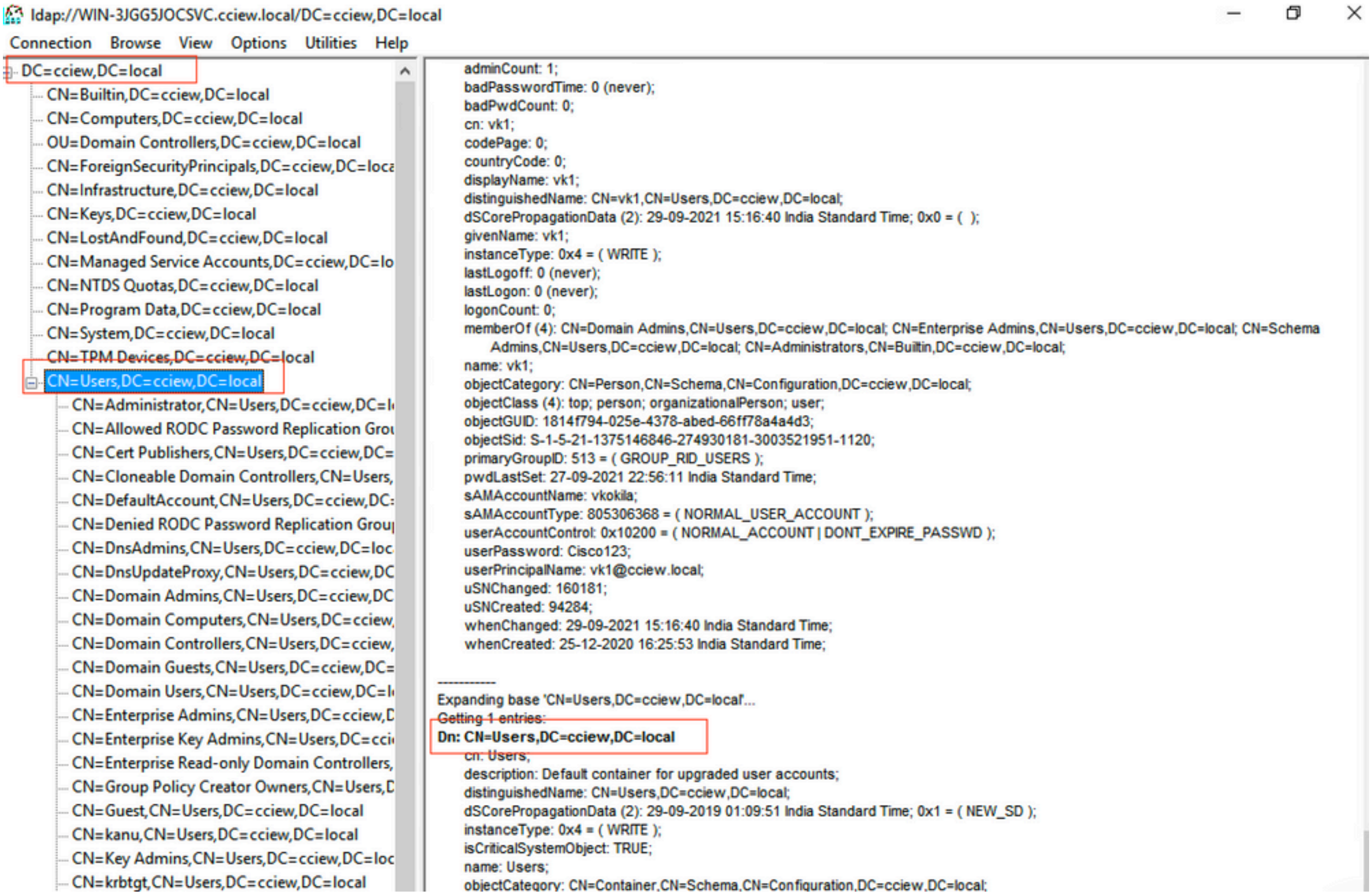


```
)LICY_HINTS_DEPRECATED );
2.840.113556.1.4.2090 = ( DIRSYNC_EX );
2.840.113556.1.4.2205 = ( UPDATE_STATS
1.2.840.113556.1.4.2204 = (
(EE_DELETE_EX ); 1.2.840.113556.1.4.2206
( SEARCH_HINTS );
2.840.113556.1.4.2211 = (
EXPECTED_ENTRY_COUNT );
1.2.840.113556.1.4.2239 = ( POLICY_HINTS
); 1.2.840.113556.1.4.2255;
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;
```



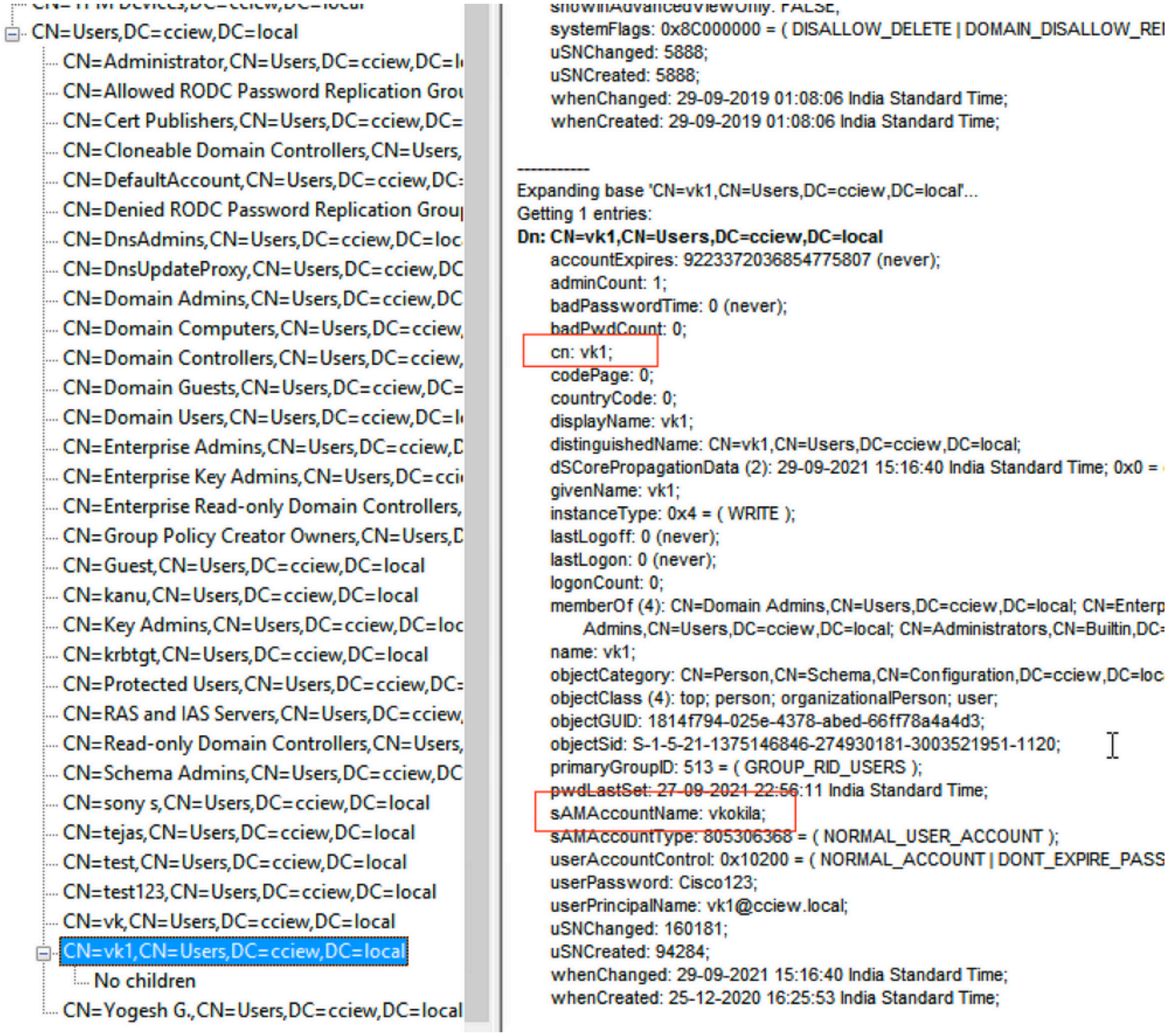
```
POLICY_HINTS_DEPRECATED );
1.2.840.113556.1.4.2090 = ( DIRSYNC_EX );
1.2.840.113556.1.4.2205 = ( UPDATE_STATS
); 1.2.840.113556.1.4.2204 = (
TREE_DELETE_EX ); 1.2.840.113556.1.4.2206
= ( SEARCH_HINTS );
1.2.840.113556.1.4.2211 = (
EXPECTED_ENTRY_COUNT );
1.2.840.113556.1.4.2239 = ( POLICY_HINTS
); 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. サーバの統計情報と属性MAPを確認します。

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

参考資料

9800でのローカルEAPの設定例

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。