Configure Catalyst 9800 WLC with LDAP Authentication

Contents

Introduction

This document describes how to configure a Catalyst 9800 in order to authenticate clients with a LDAP Server as the database for user credentials.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Microsoft Windows Servers
- Active Directory or any other LDAP database

Components Used

The information in this document is based on these software and hardware versions:

- C9800 EWC on C9100 Access Point (AP) that runs Cisco IOS® XE version 17.3.2a

- Microsoft Active Directory (AD) Server with QNAP Network Access Storage (NAS) that acts as LDAP database

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. If your network is live, ensure that you understand the potential impact of any command.

Configure LDAP with a Webauth SSID for 802.1X and Web-auth

Network Diagram

This article was written based on a very simple setup:

An EWC AP 9115 with IP 192.168.1.15

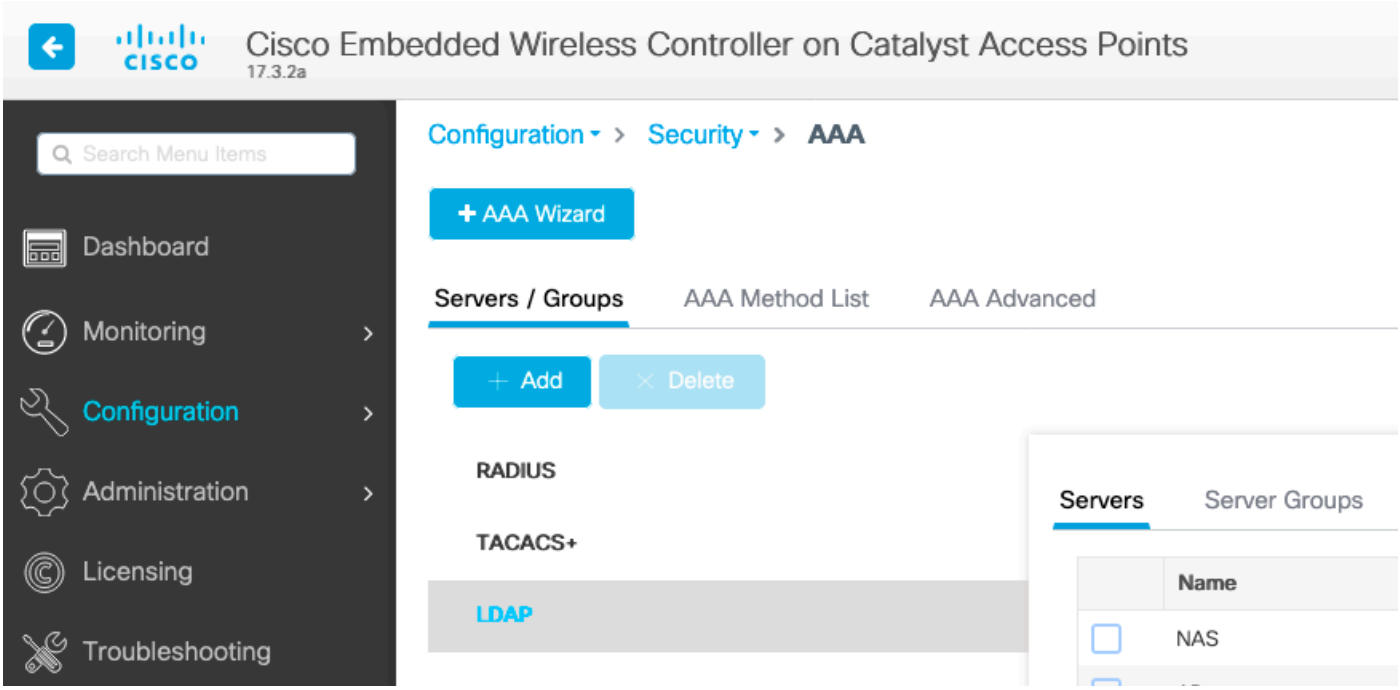
An Active Directory server with IP 192.168.1.192

A client that connects to the internal AP of the EWC

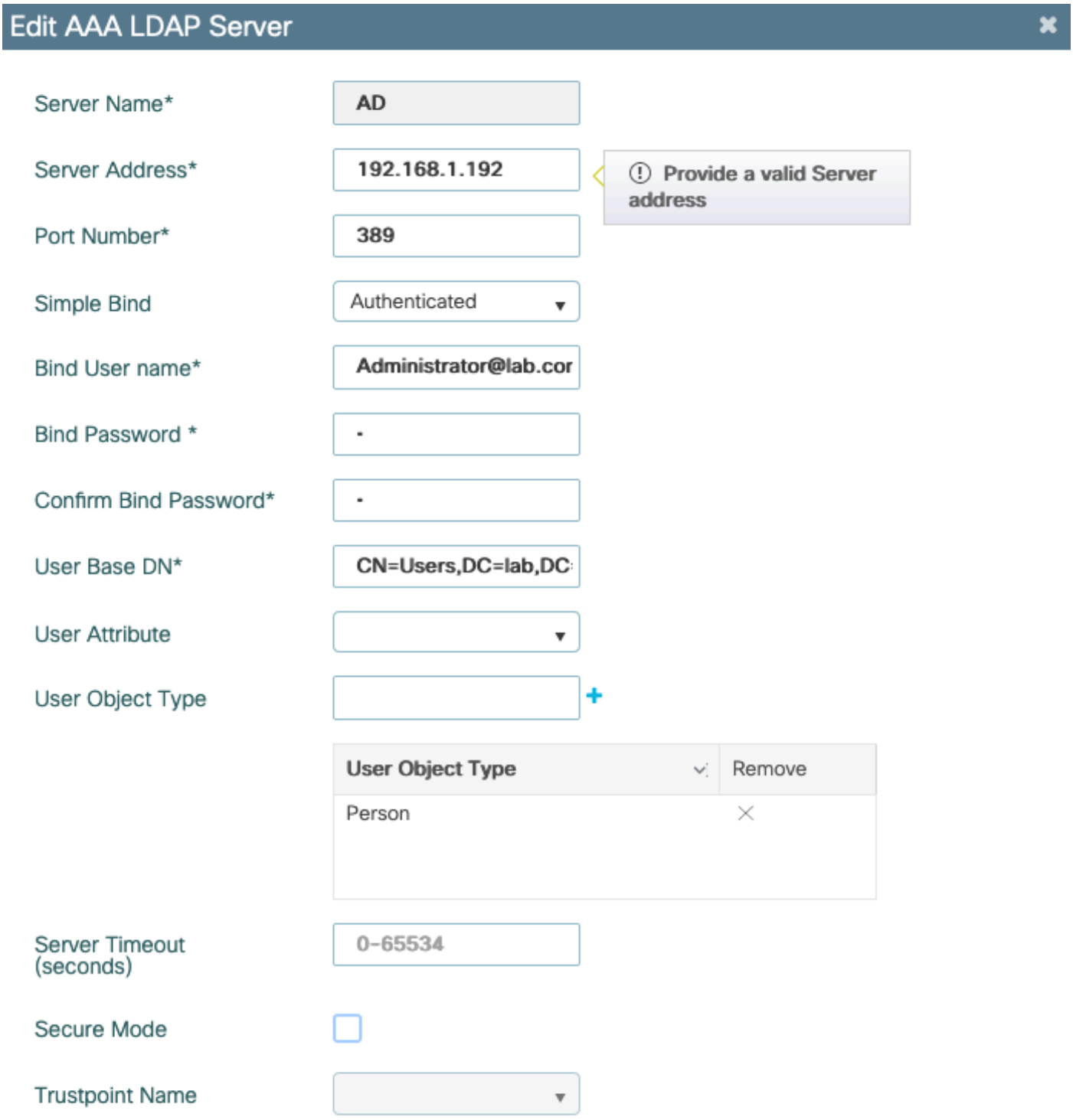
Configure the Controller

Step 1**.** Configure the LDAP server.

Navigate to **Configuration > Security > AAA> Servers/Groups > LDAP** and click **+ Add**.



Chose a name for your LDAP server and fill in the details. For explanation on each field, refer to the section Understand LDAP Server Details of this document.



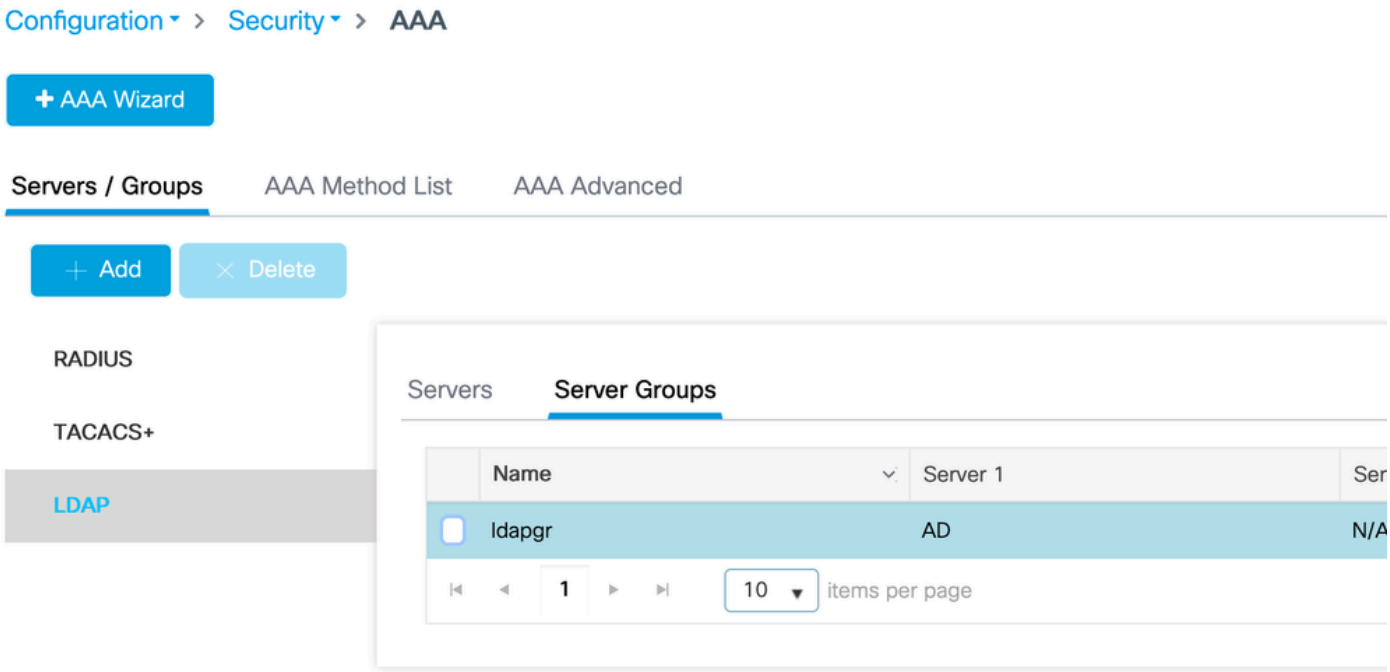
Save by clicking **Update and apply to device**.

CLI commands:

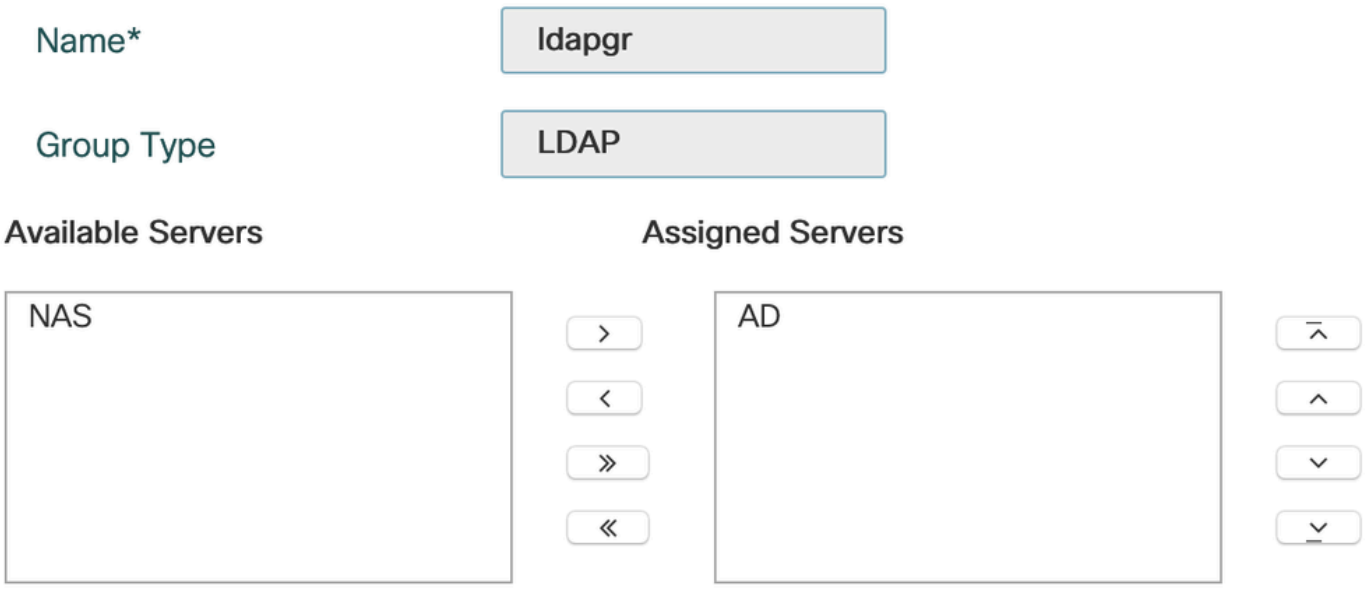
```
ldap server AD
 ipv4 192.168.1.192
 bind authenticate root-dn Administrator@lab.com password 6 WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB
 base-dn CN=Users,DC=lab,DC=com
 search-filter user-object-type Person
```

Step 2. Configure an LDAP server group.

Navigate to **Configuration > Security > AAA > Servers/ Groups > LDAP > Server Groups** and click **+ADD**.



Enter a name and add the LDAP server you configured in the previous step.



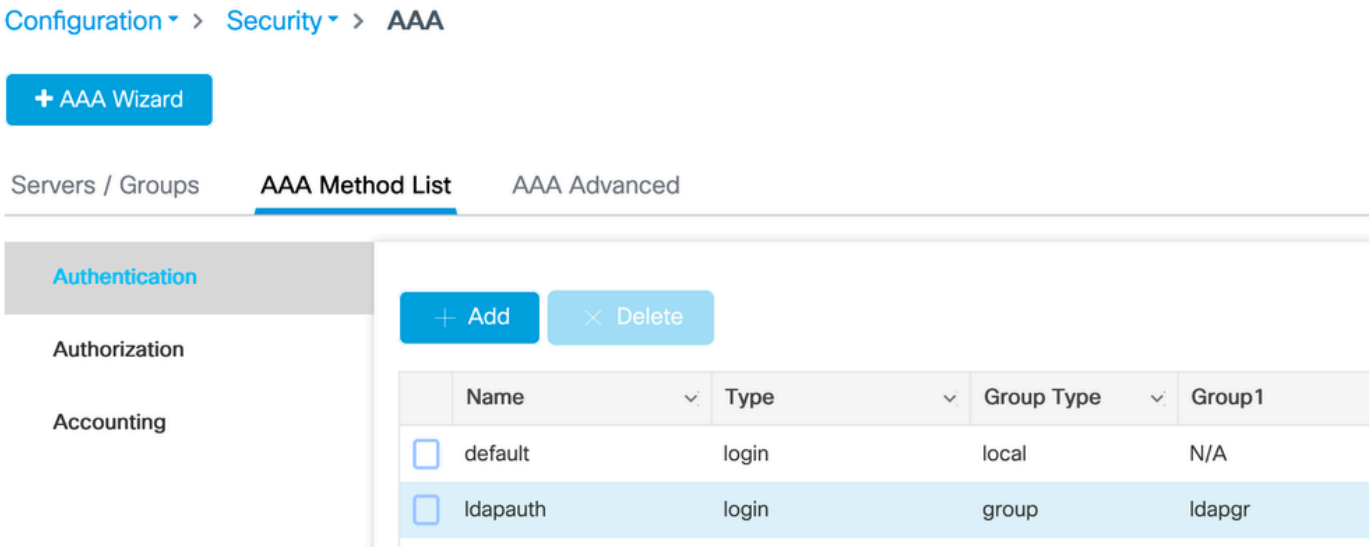
Click on **Update and apply** to save.

CLI commands:

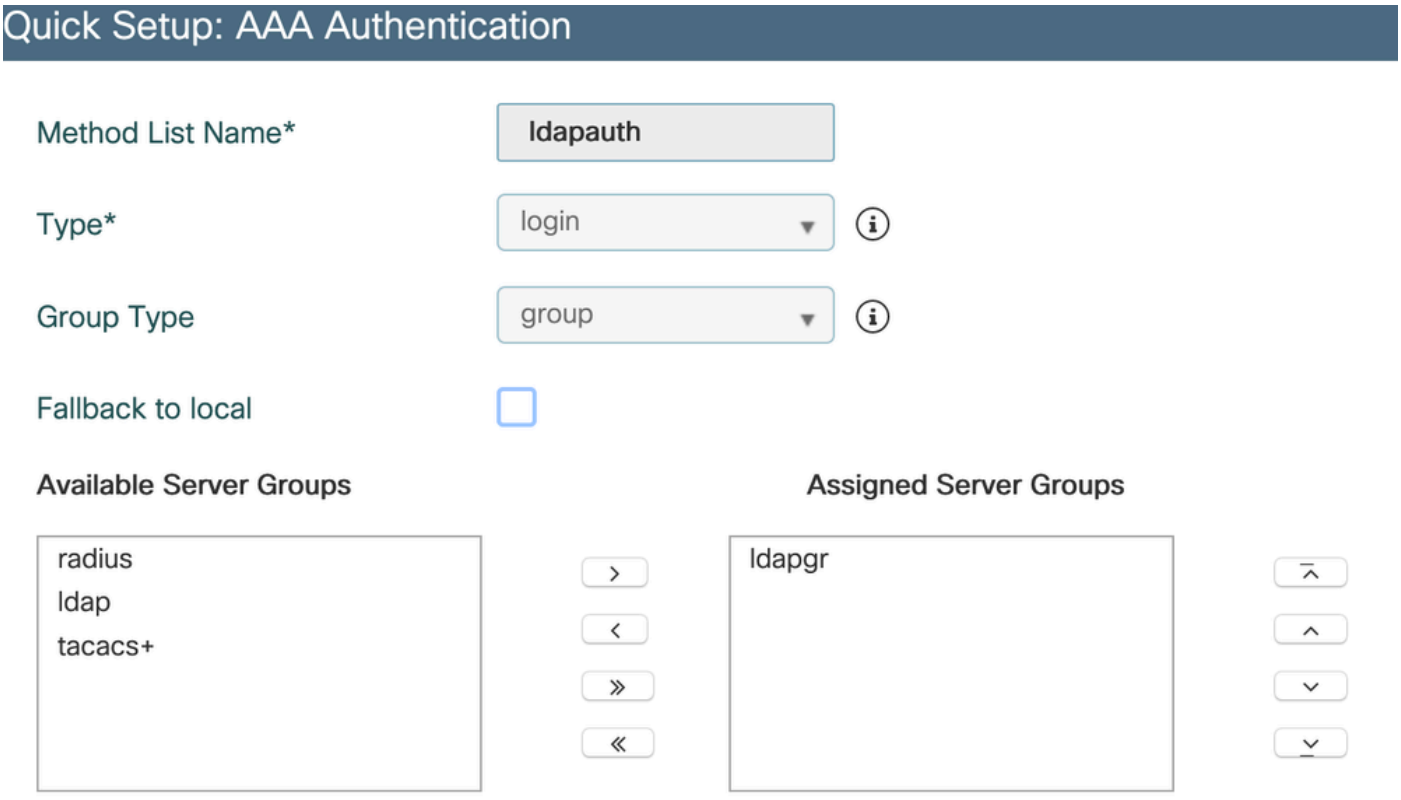
```
aaa group server ldap ldapgr
 server AD
```

Step 3. Configure AAA authentication method.

Navigate to **Configuration > Security > AAA > AAA method List > Authentication** and click **+Add**.



Enter a name, chose the **Login** type and point to the LDAP server group configured previously.

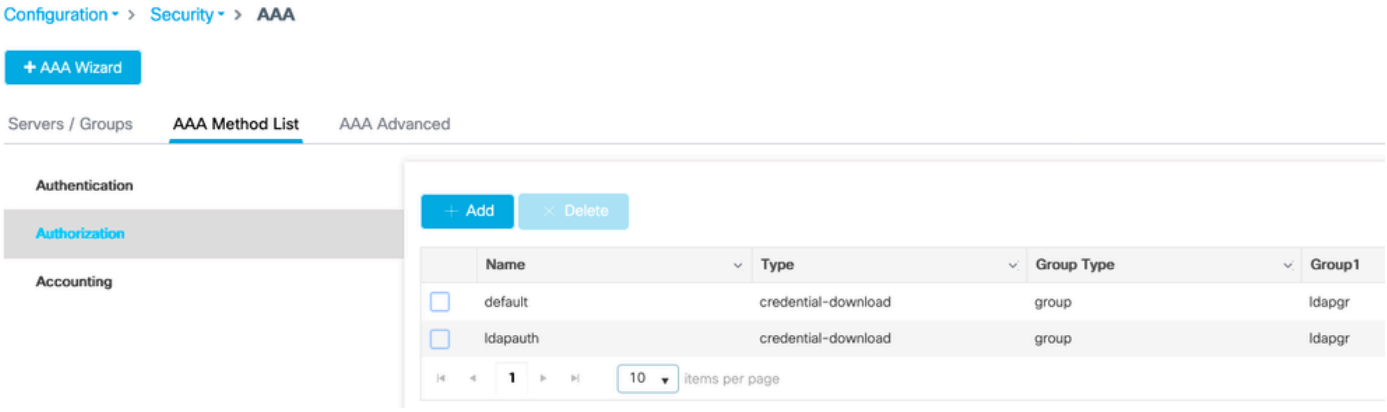


CLI commands:

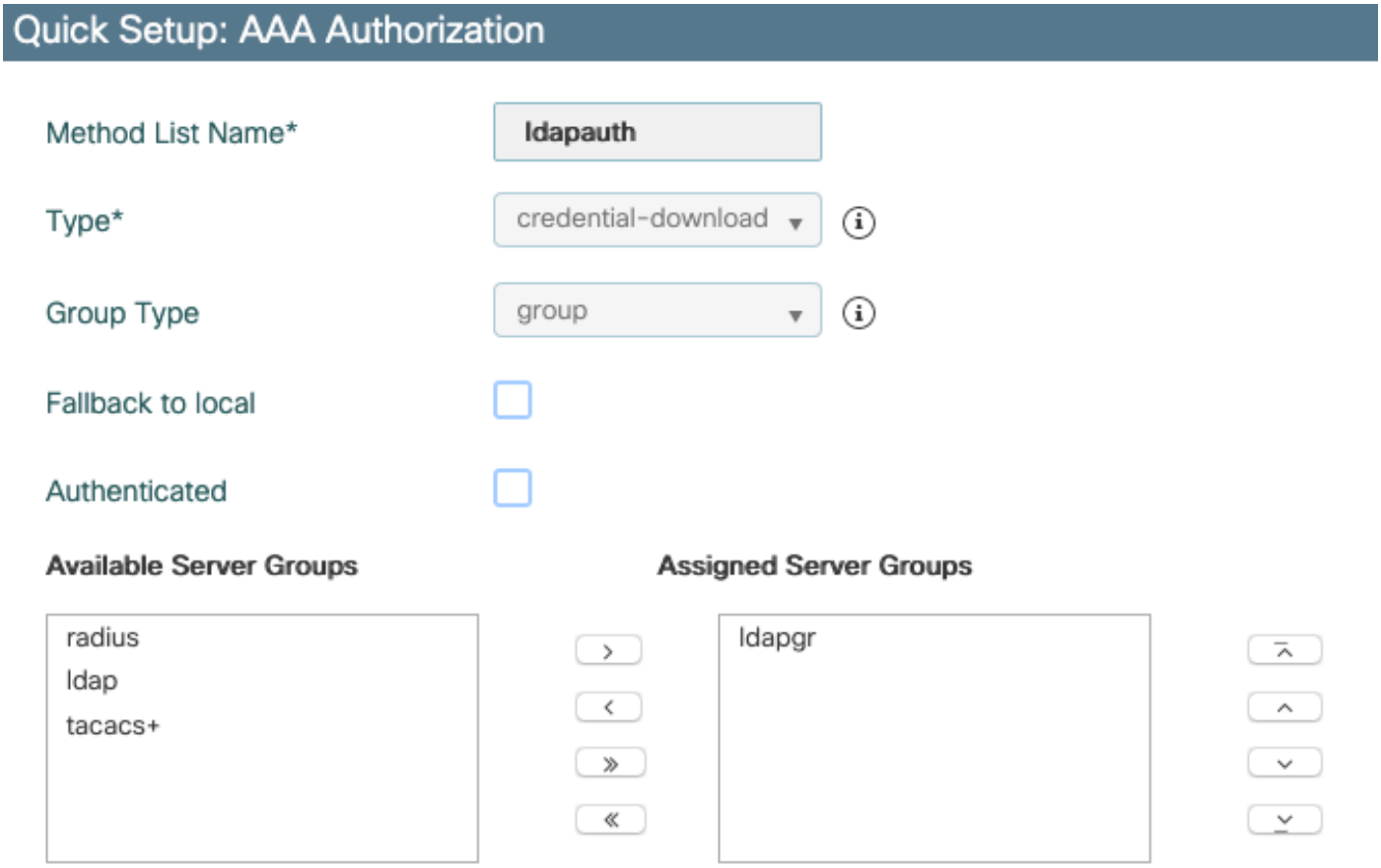
```
aaa authentication login ldapauth group ldapgr
```

Step 4. Configure a AAA authorization method.

Navigate to **Configuration > Security > AAA > AAA method list > Authorization** and click **+Add**.



Create a credential-download type rule of the name of your choice and point it to the LDAP server group created previously.



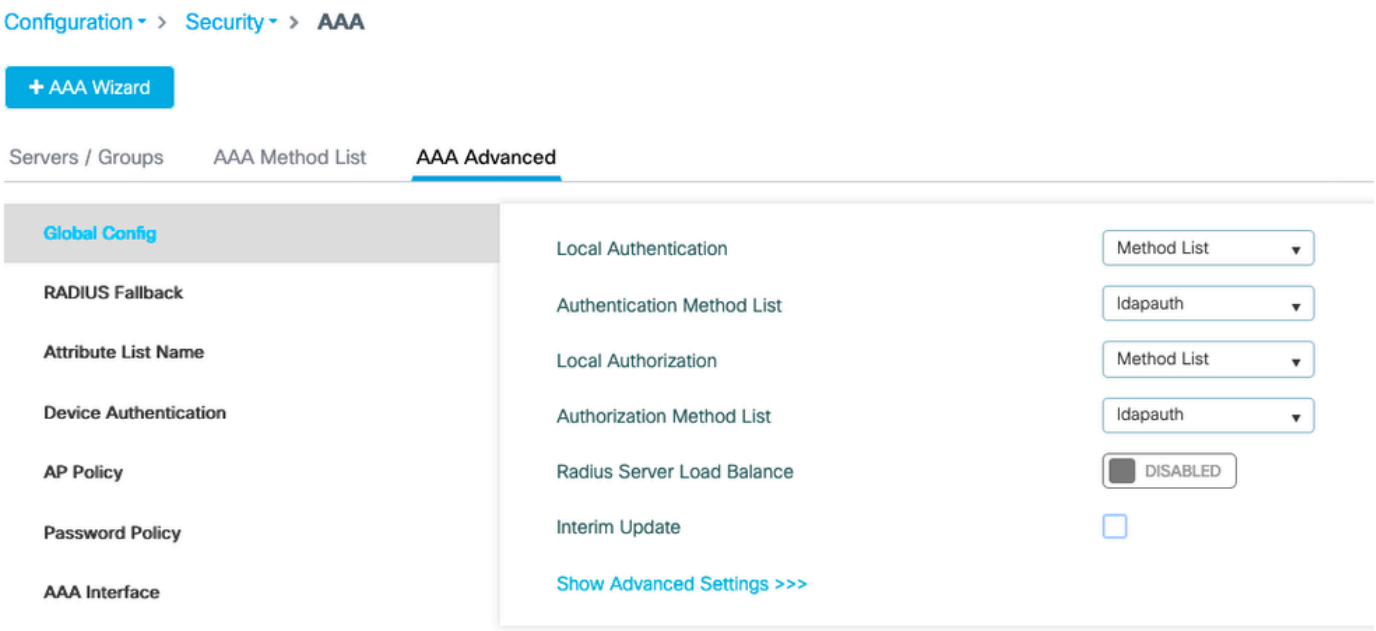
CLI commands:

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

Step 5. Configure local authentication.

Navigate to **Configuration > Security > AAA > AAA Advanced > Global Config**.

Set local authentication and local authorization to **Method List** and pick the authentication and authorization method configured previously.

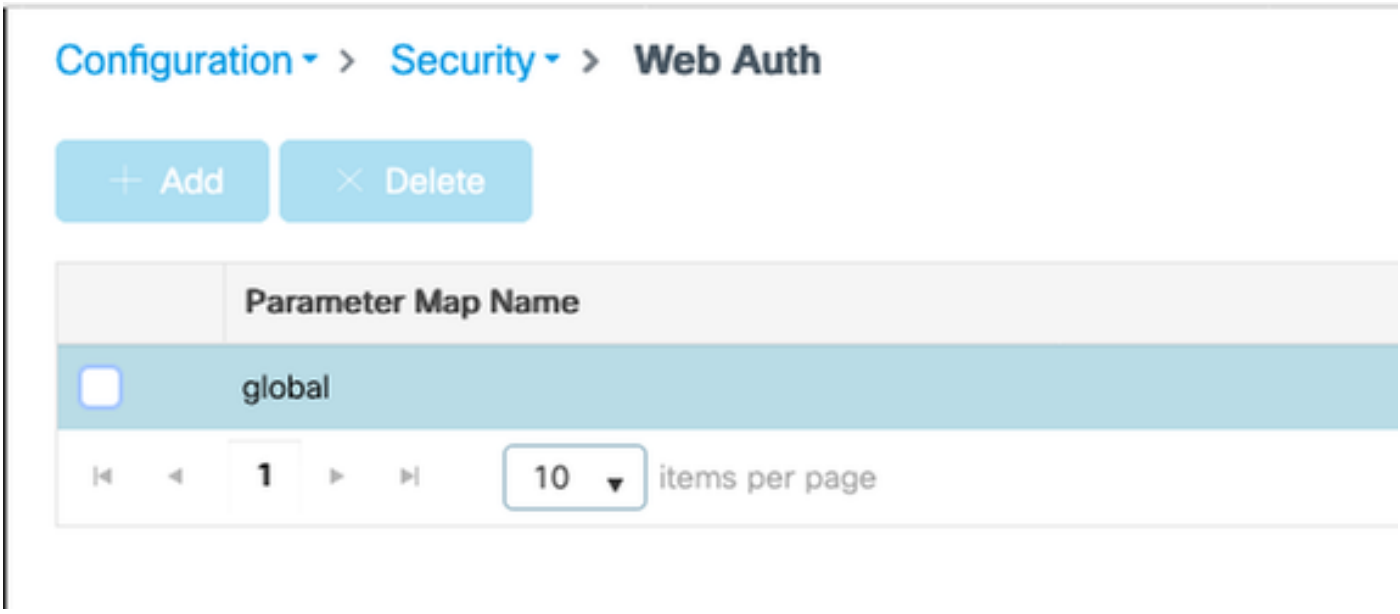


CLI commands:

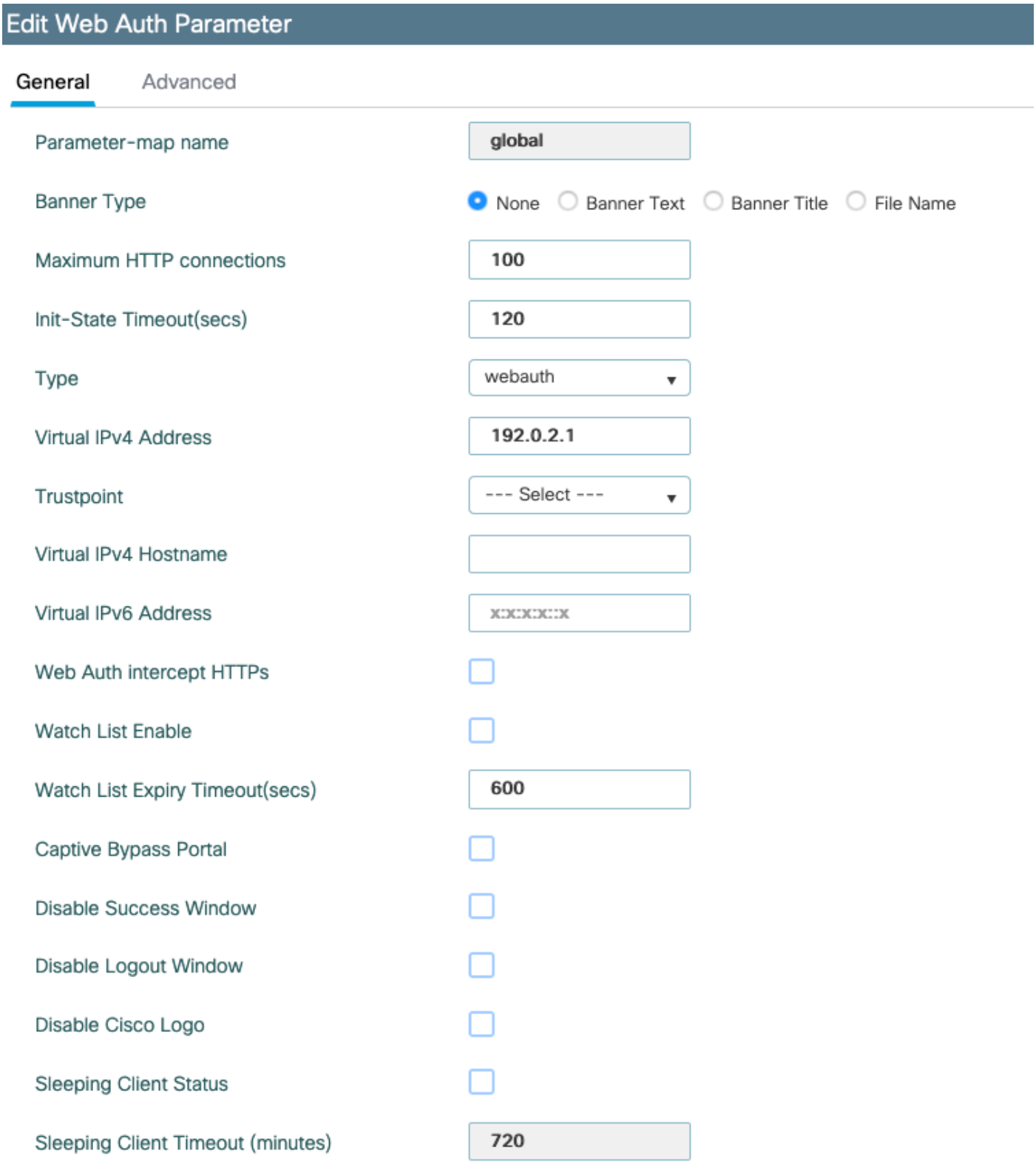
```
aaa local authentication ldapauth authorization ldapauth
```

Step 6. Configure the webauth parameter-map.

Navigate to **Configuration > Security > Web Auth** and edit the **global** map.



Make sure to configure a virtual IPv4 address such as 192.0.2.1 (that specific IP/subnet is reserved for non-routable Virtual IP).



Click **Apply** to save.

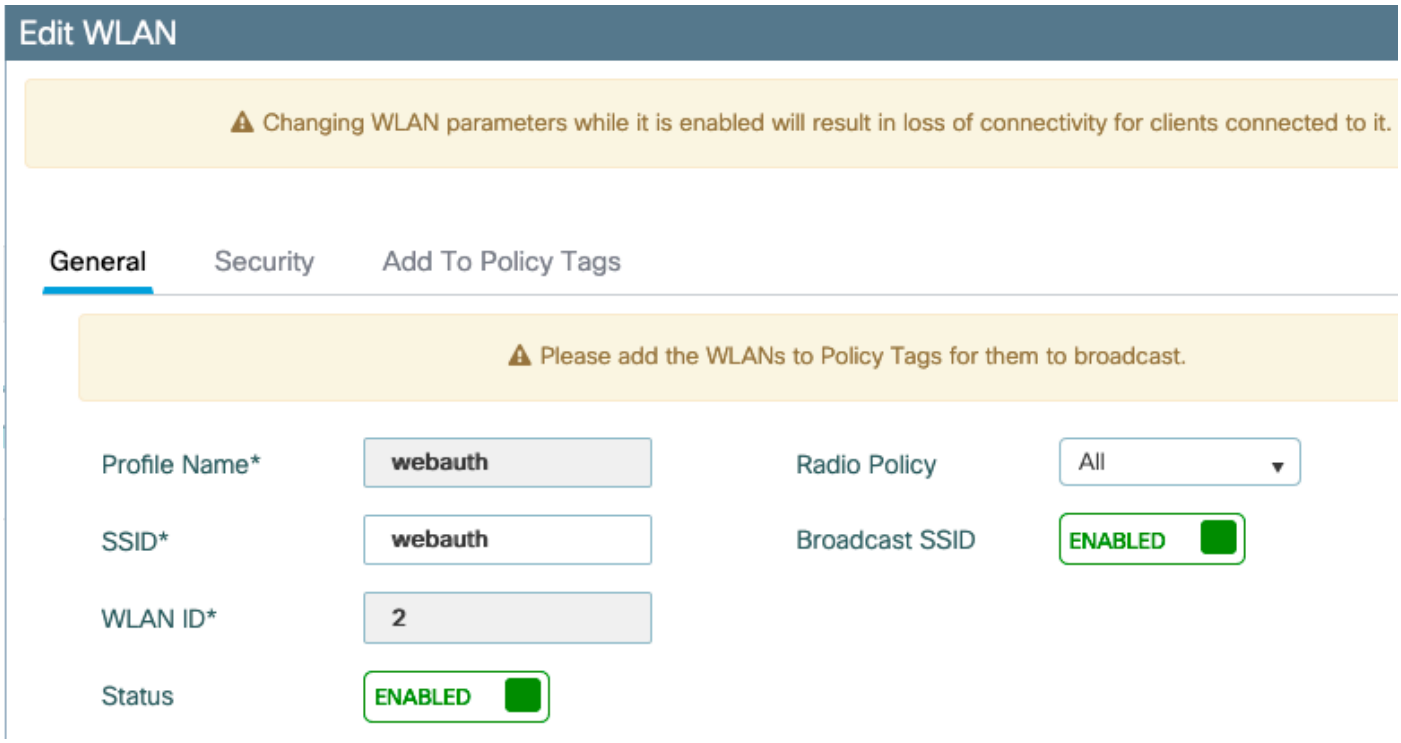
CLI commands:

```
parameter-map type webauth global
 type webauth
```

```
virtual-ip ipv4 192.0.2.1
```

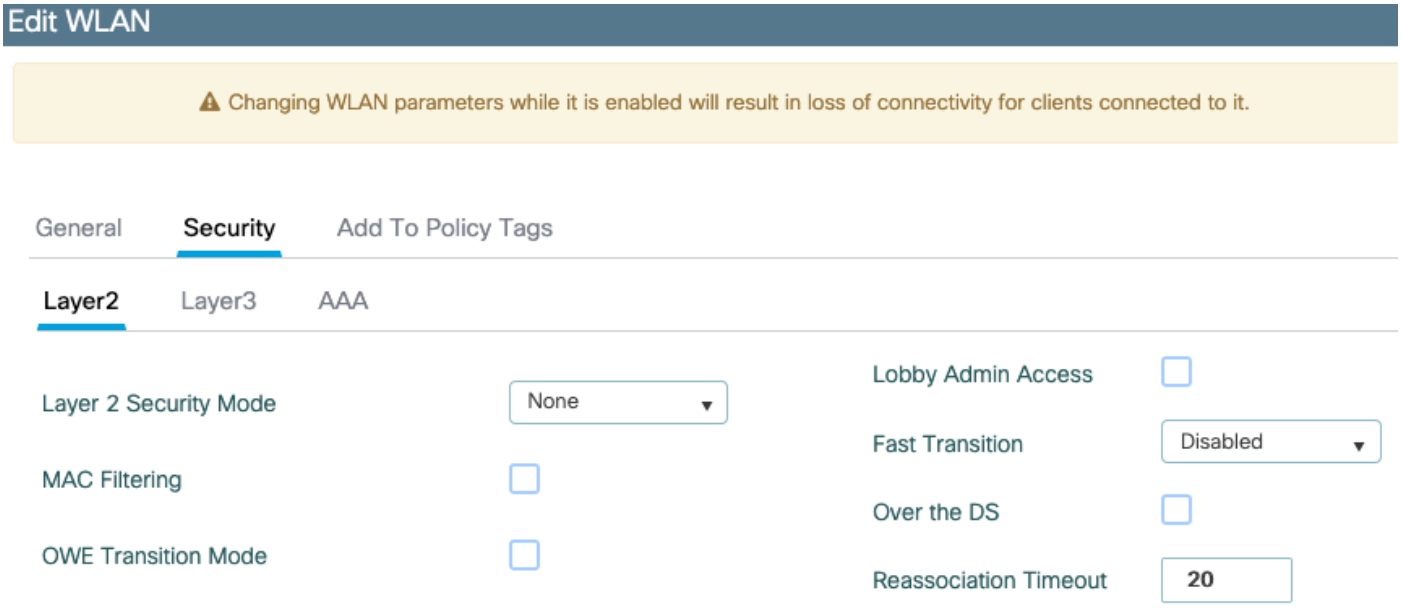
Step 7. Configure a webauth WLAN.

Navigate to **Configuration > WLANs** and click **+Add**.

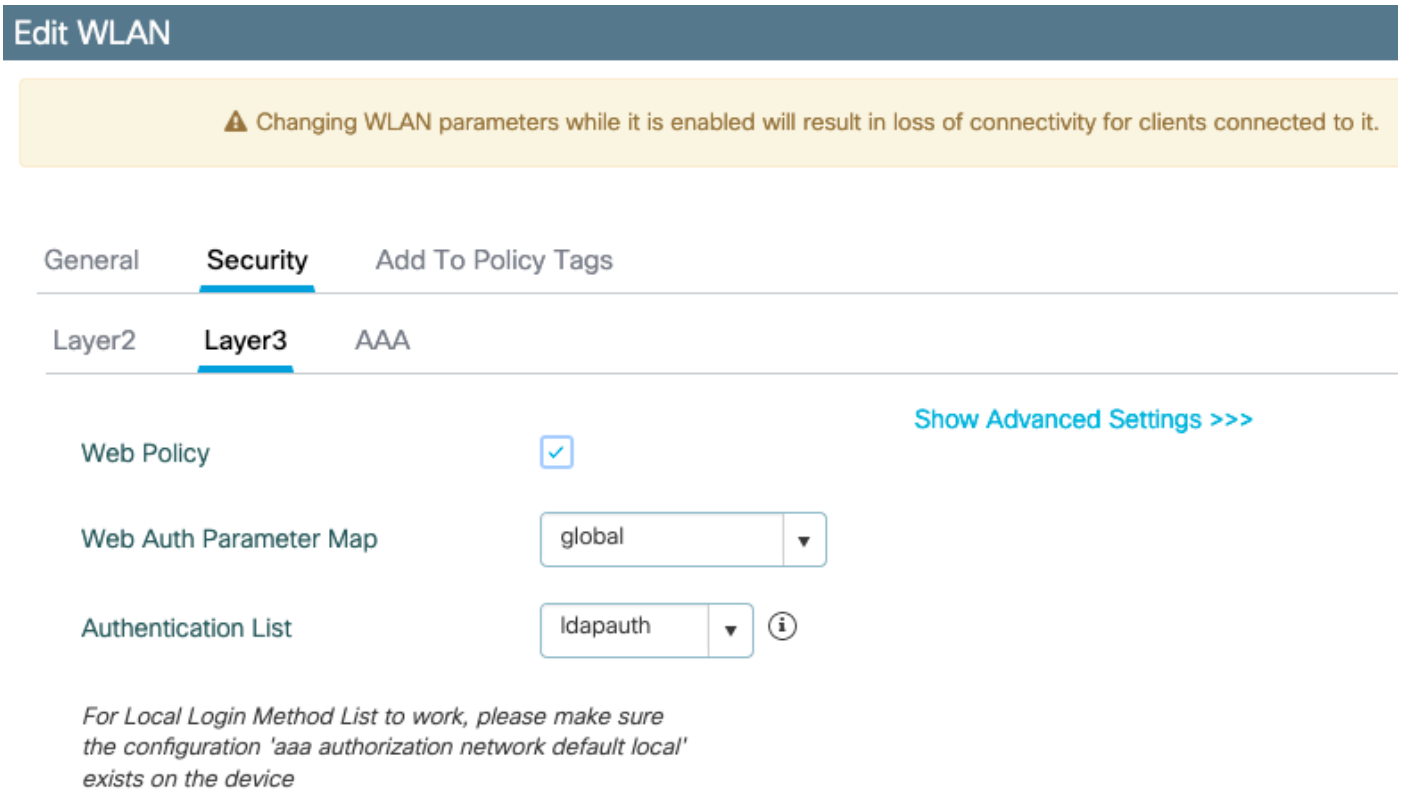


Configure the name, make sure it is in the enabled state, then move to the **Security** tab.

In the **Layer 2** sub-tab, make sure there no security and that Fast Transition is disabled.



In the **Layer3** tab, enable **web policy**, set the parameter map to **global** and set the authentication list to the AAA log in method configured previously.



Save by clicking **Apply**.

CLI commands:

```
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
```

Step 8. Make sure the SSID is broadcast.

Navigate to **Configuration > Tags** and make sure the SSID is included in the policy profile currently service by the SSID (the default-policy-tag for a fresh new configuration if you have not configured tags yet). By default the default-policy-tag does not broadcast new SSIDs you create until you include them manually.

This article does not cover the configuration of policy profiles and assumes you are familiar with that part of the configuration.

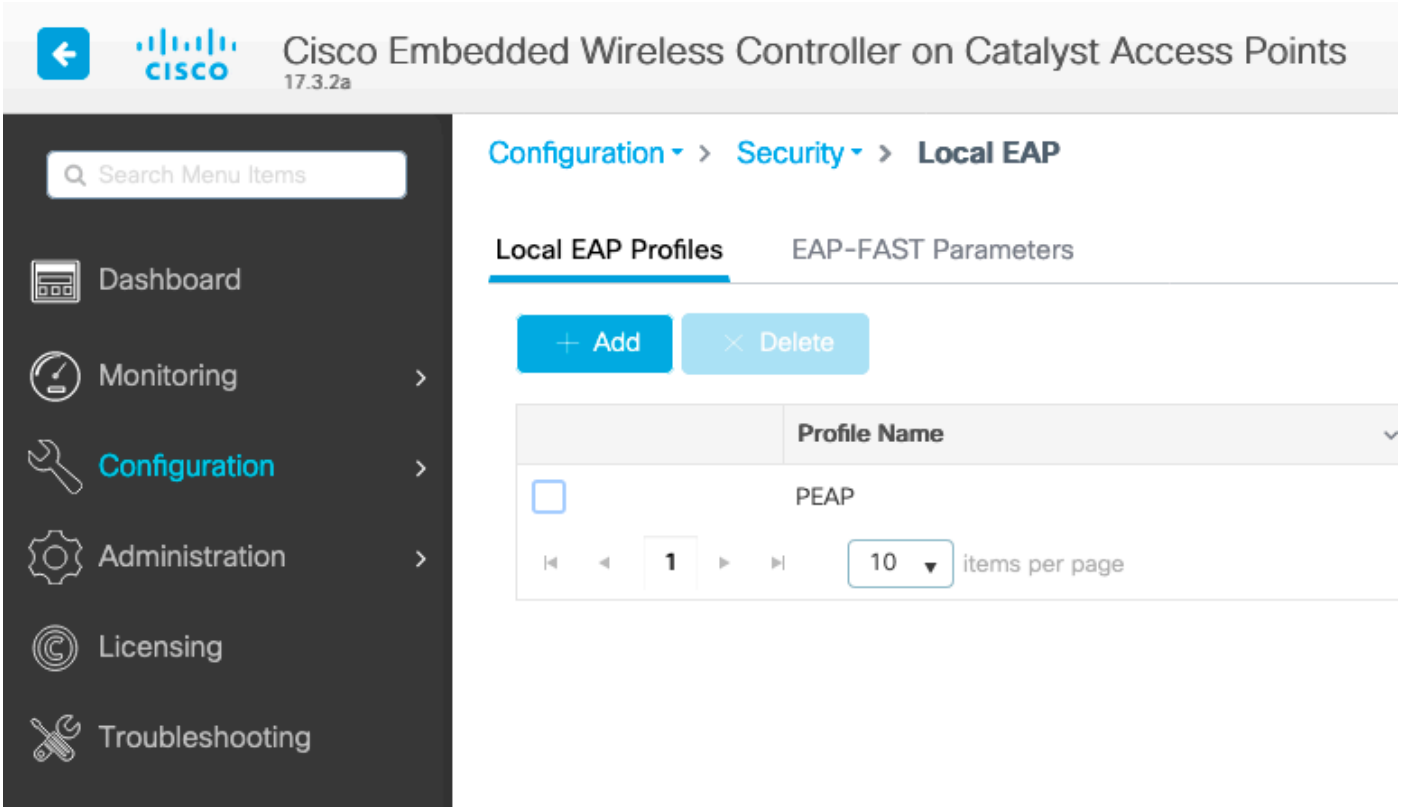
Configure LDAP with a dot1x SSID (using Local EAP)

Configuring LDAP for a 802.1X SSID on the 9800 typically requires also configuring Local EAP. If you were to use RADIUS, then it would be your RADIUS server to establish a connection with the LDAP

database and that is outside of the scope of this article.Before attempting this configuration it is advised to configure Local EAP with a local user configured on the WLC first, a configuration example is provided in the references section at the end of this article. Once done, you can try to move the user database towards LDAP.

Step 1. Configure a Local EAP profile

Navigate to **Configuration > Local EAP** and click **+Add**



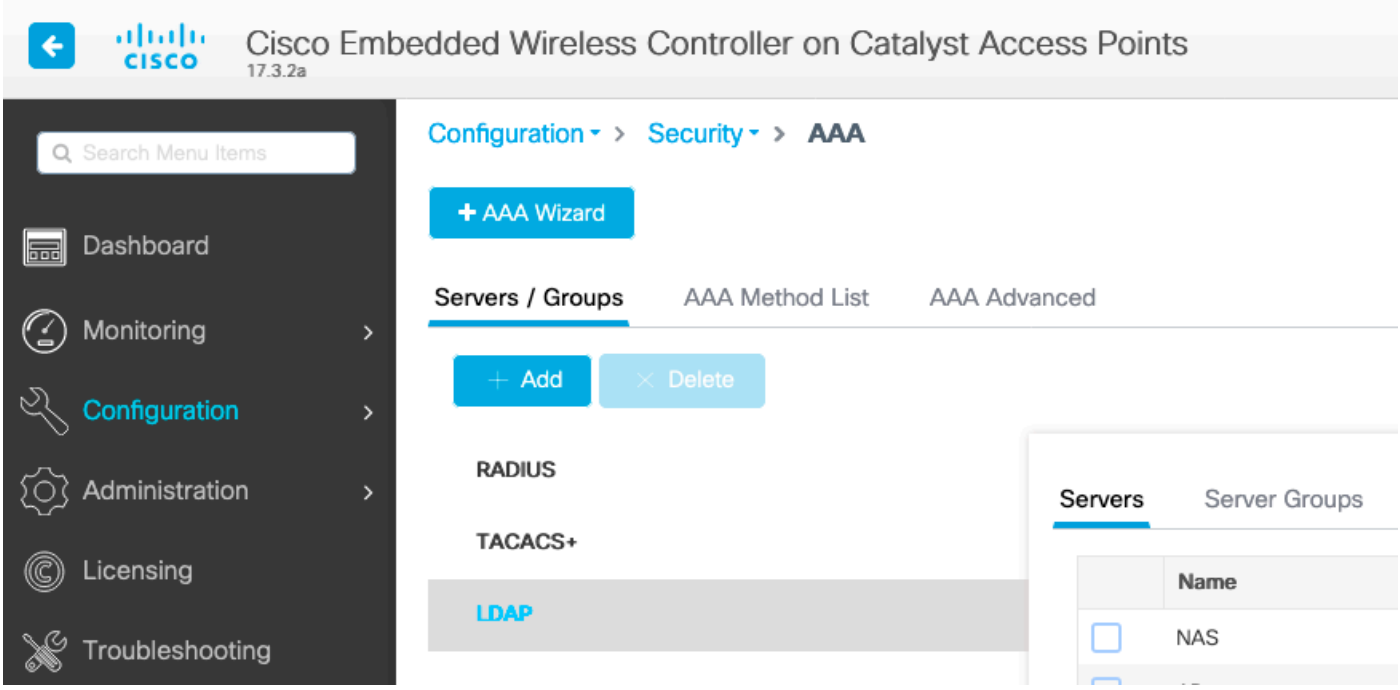
Pick any name for your profile. Enable at least PEAP and pick a Trustpoint Name. By default, your WLC has only self-signed certificates, so it does not really matter which one you pick (typically TP-self-signed-xxxx is the best one for this purpose) but as new smartphones OS versions trust less and less self-signed certificates, consider installing a trusted publicly signed certificate.

CLI commands:

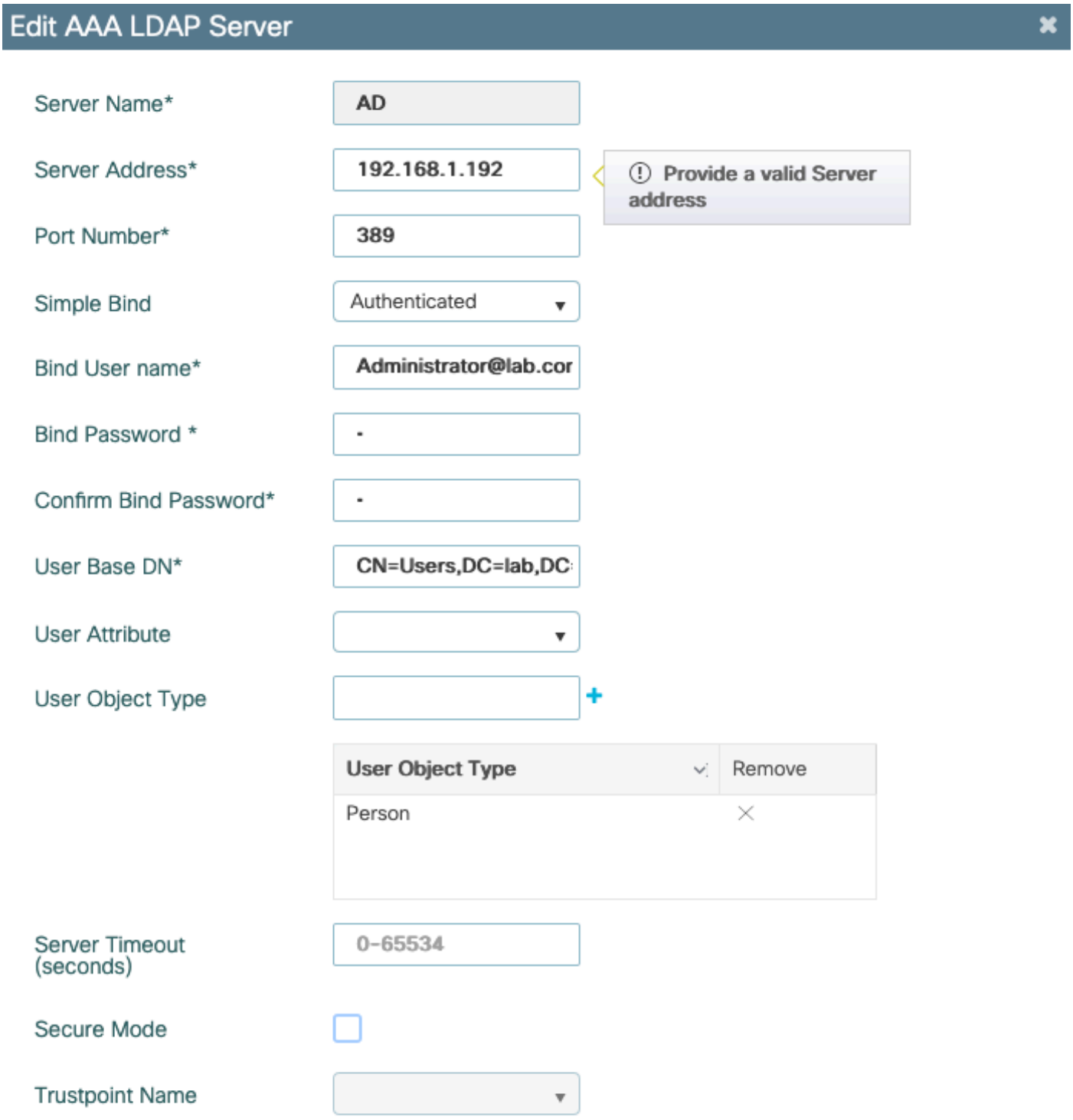
```
eap profile PEAP
 method peap
 pki-trustpoint TP-self-signed-3059261382
```

Step 2. Configure the LDAP server.

Navigate to **Configuration > Security > AAA> Servers/Groups > LDAP** and click **+ Add**.



Chose a name for your LDAP server and fill in the details. For explanation on each field, refer to the section Understand LDAP Server Details of this document.

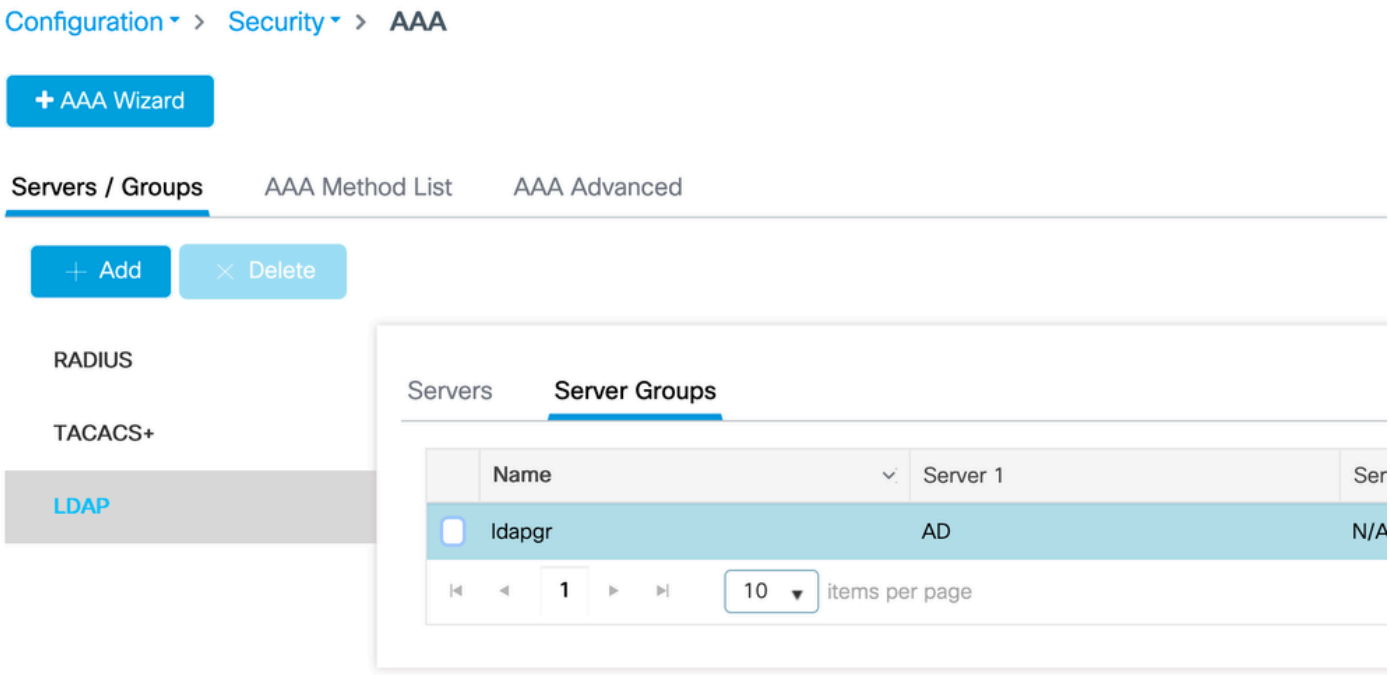


Save by clicking **Update and apply to device**.

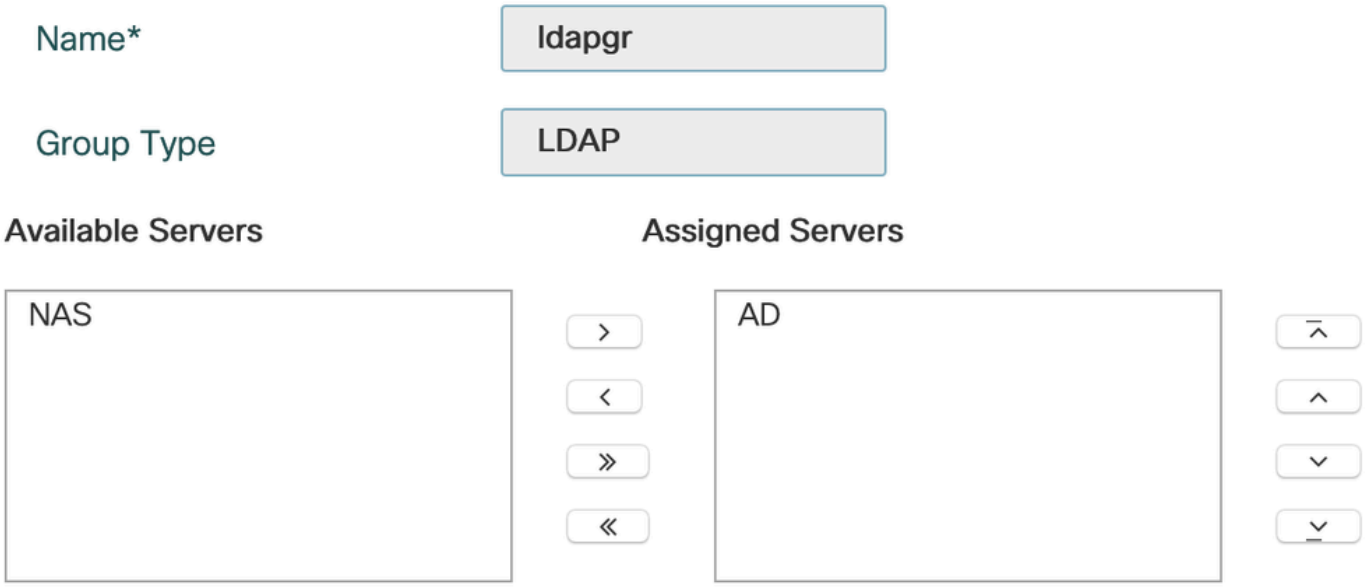
```
ldap server AD
 ipv4 192.168.1.192
 bind authenticate root-dn Administrator@lab.com password 6 WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB
 base-dn CN=Users,DC=lab,DC=com
 search-filter user-object-type Person
```

Step 3. Configure an LDAP server group.

Navigate to **Configuration > Security > AAA > Servers/ Groups > LDAP > Server Groups** and click **+ADD**.



Enter a name and add the LDAP server you configured in the previous step.



Click on **Update and apply** to save.

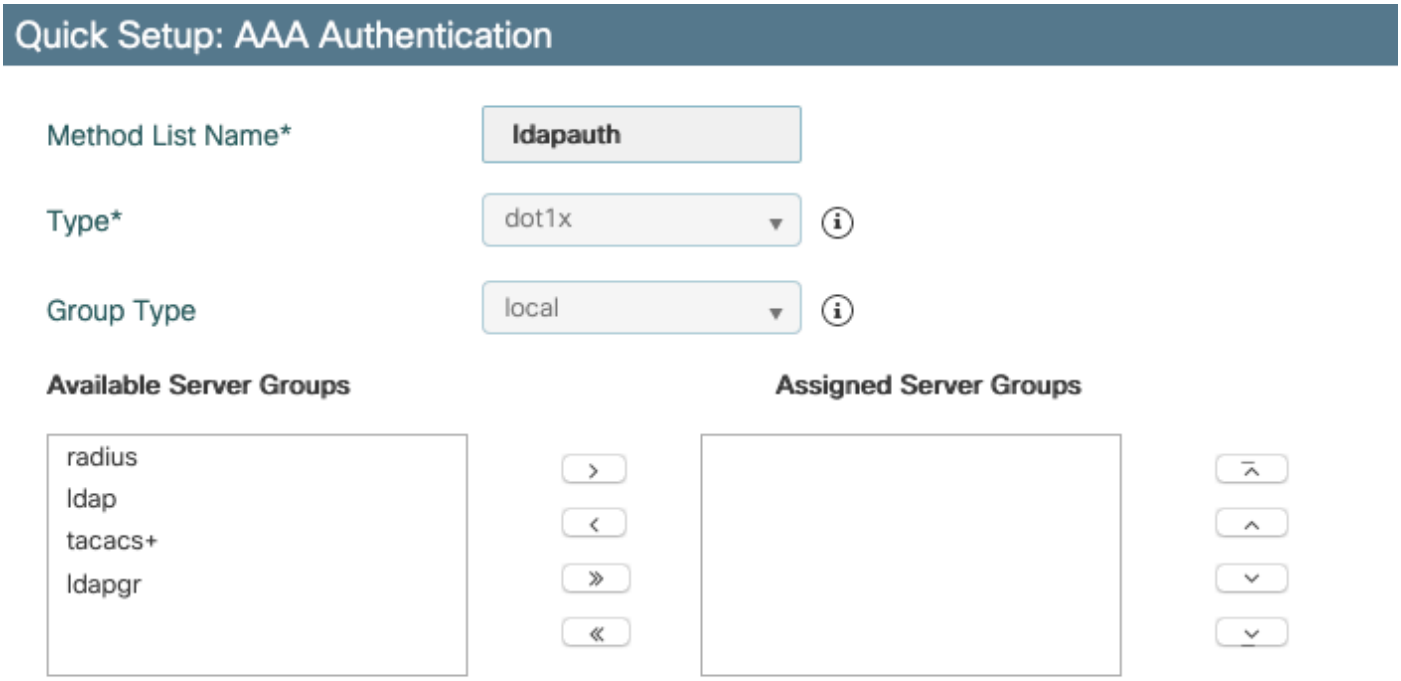
CLI commands:

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

Step 4. Configure a AAA Authentication method.

Navigate to **Configuration > Security > AAA > AAA Method List > Authentication** and click **+Add**,

Configure a **dot1x** type authentication method and point it to local only. It would be tempting to point to the LDAP server group but it is the WLC itself that acts as the 802.1X authenticator here (although the user database is on LDAP, but that is the authorization method job).



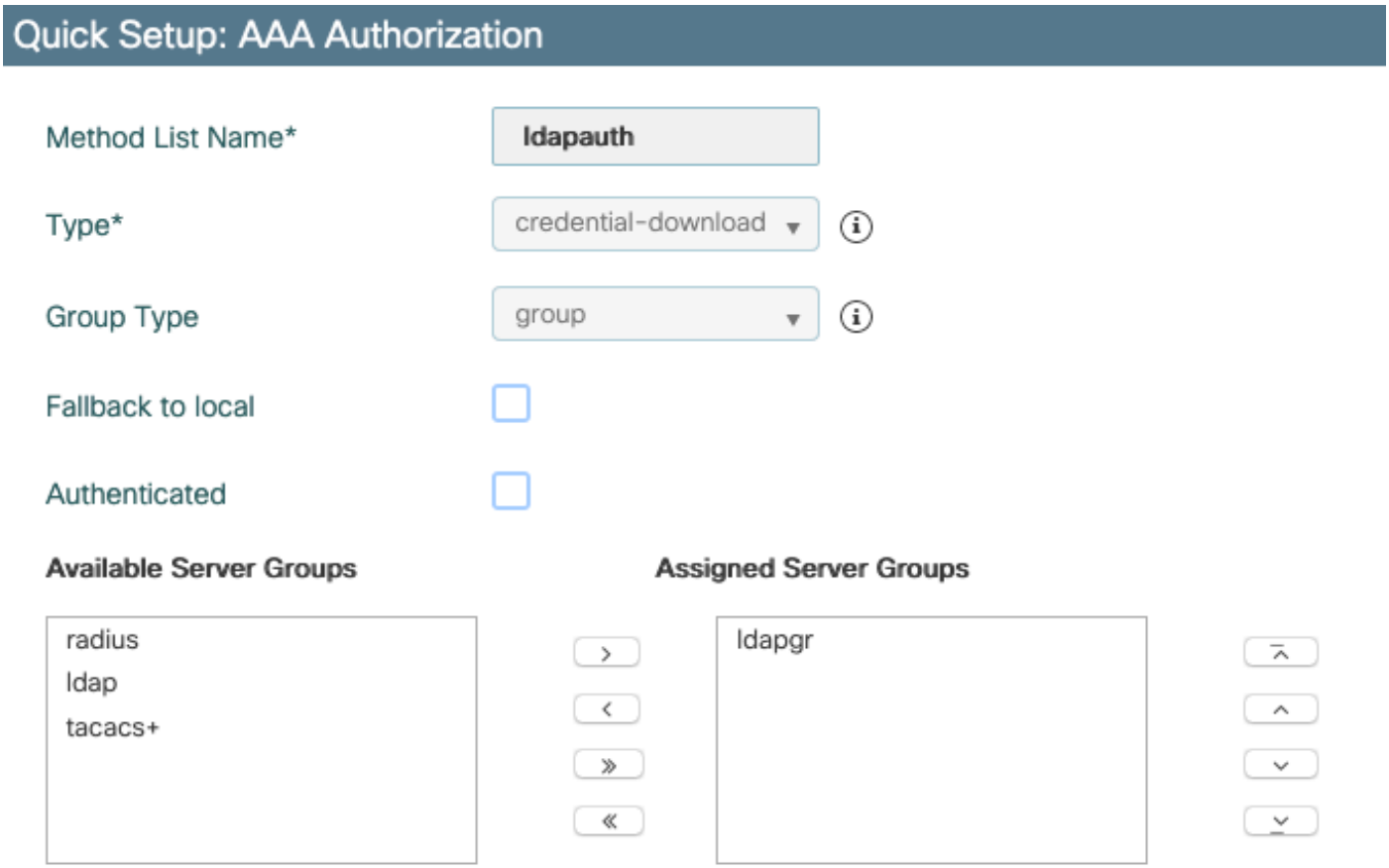
CLI command:

```
aaa authentication dot1x ldapauth local
```

Step 5. Configure a AAA authorization method.

Navigate to **Configuration > Security > AAA > AAA Method List > Authorization** and click **+Add**.

Create a **credential-download** type of authorization method and make it point to the LDAP group.



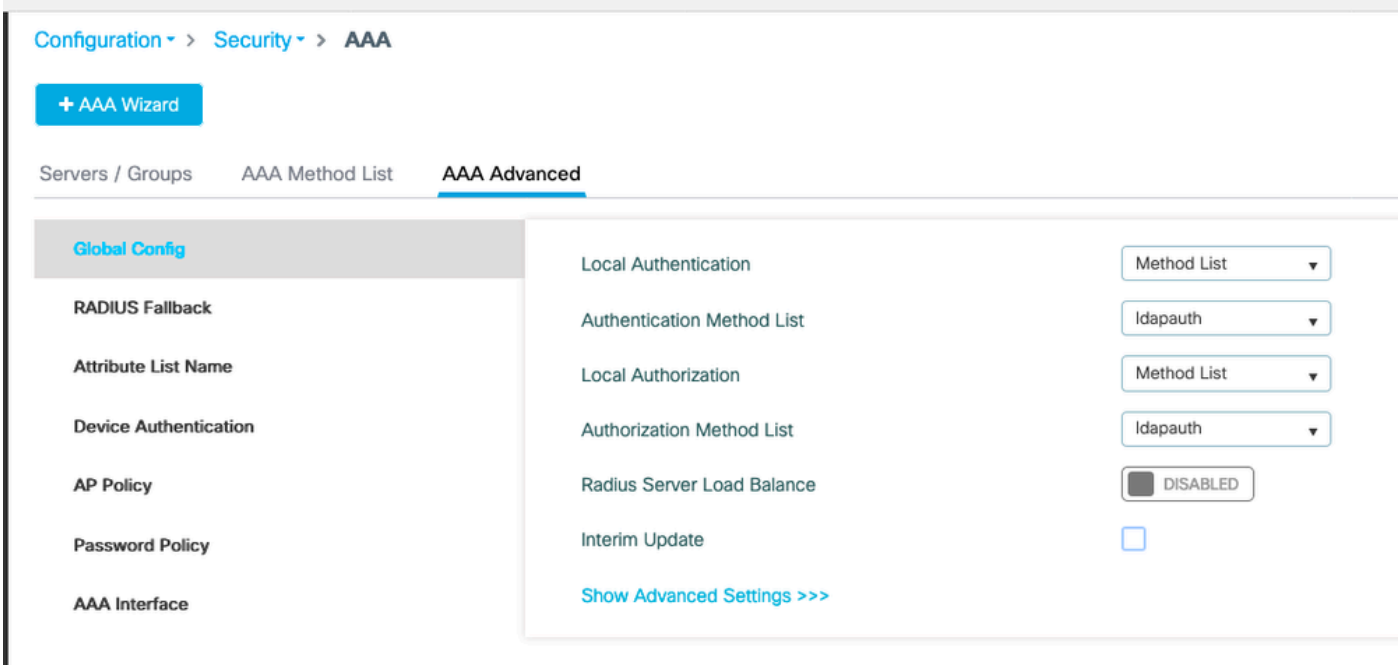
CLI command:

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

Step 6. Configure local authentication details.

Navigate to **Configuration > Security > AAA > AAA Method List > AAA advanced**.

Chose **Method List** for both authentication and authorization and pick the dot1x authentication method pointing locally and the credential-download authorization method pointing towards LDAP.



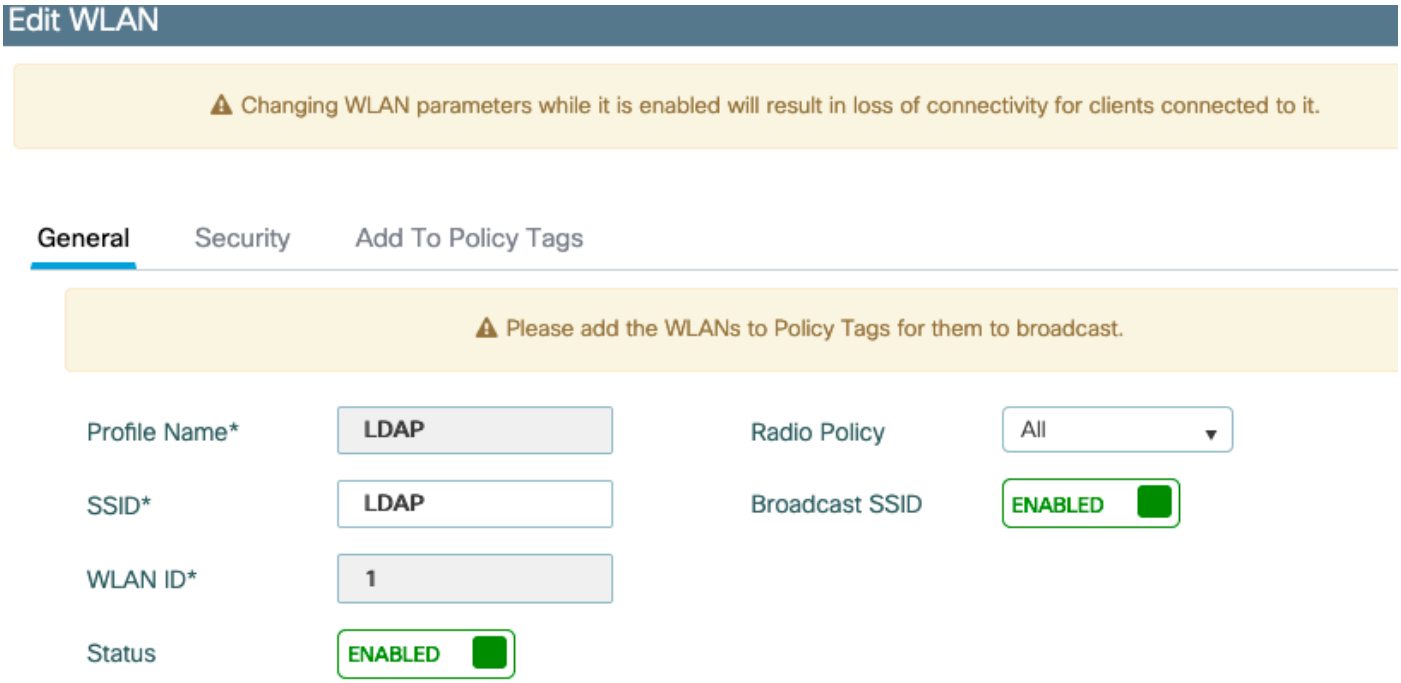
CLI command :

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

Step 7. Configure a dot1x WLAN.

Navigate to **Configuration** > **WLAN** and click **+Add**.

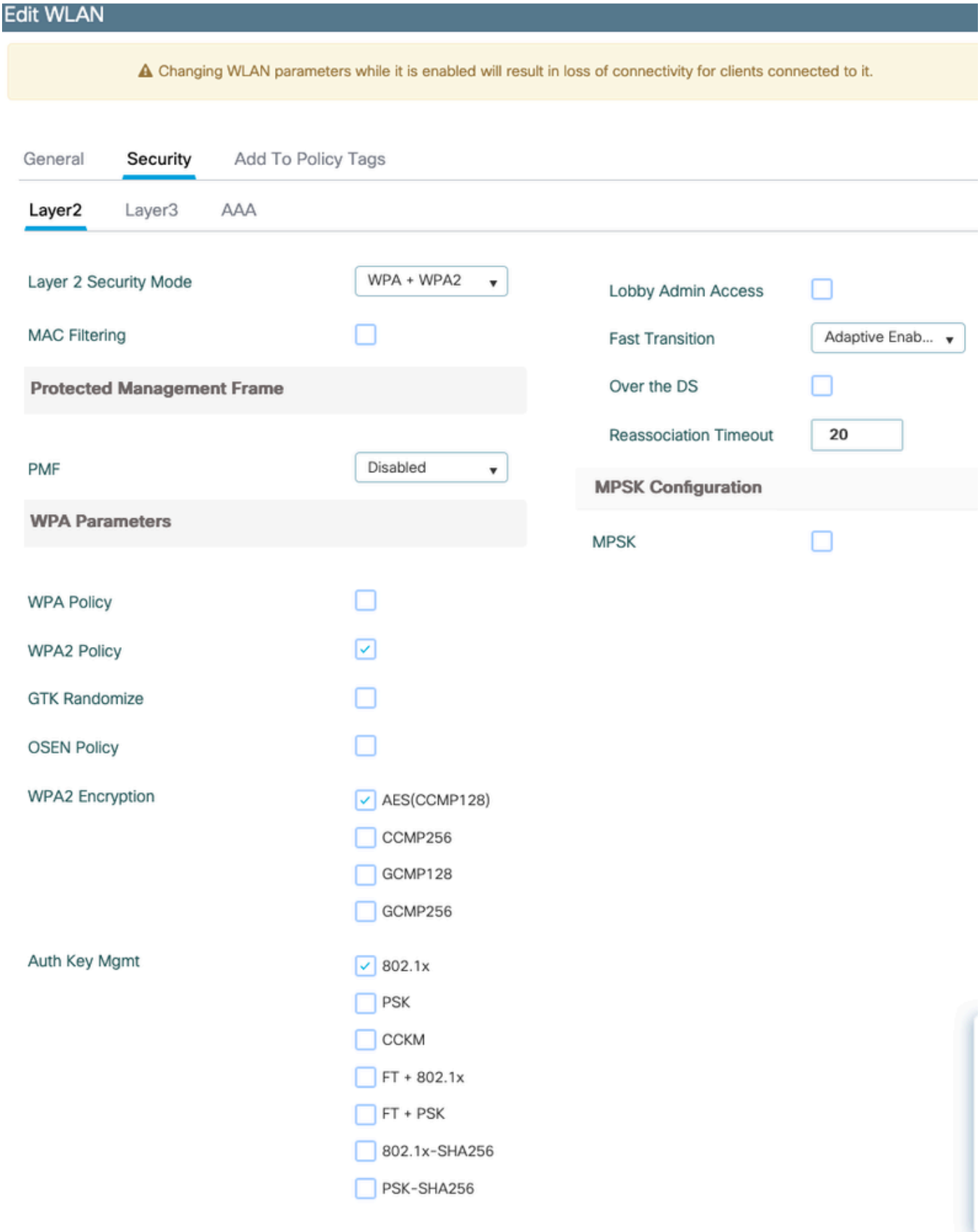
Chose a profile and SSID name and make sure it is enabled.



Move to the Layer 2 **Security** tab.

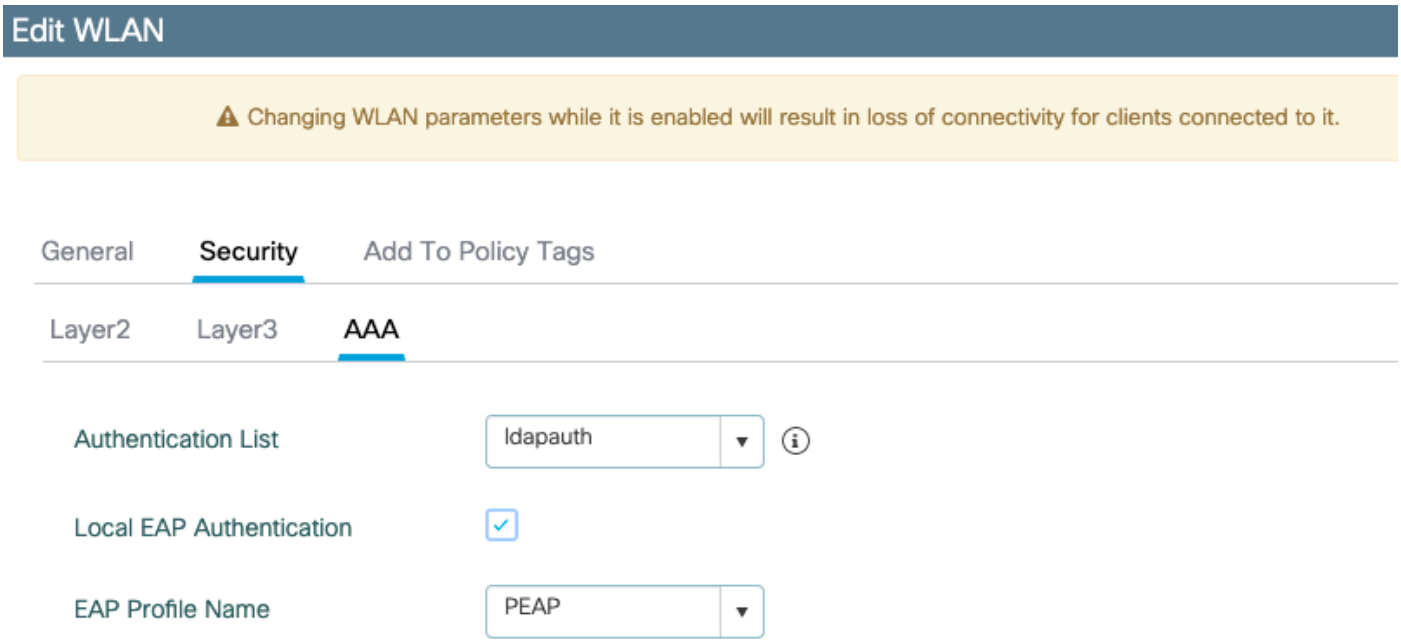
Chose WPA+WPA2 as **Layer 2 security mode**.

Make sure WPA2 and AES are enabled in the **WPA Parameters** and enable **802.1X**.



Move to the **AAA** sub tab.

Pick the dot1x authentication method created earlier, enable Local EAP authentication and pick the EAP profile configured in the first step.



Save by clicking **Apply**.

CLI commands:

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

Step 8. Verify that the WLAN is broadcast.

Navigate to **Configuration > Tags** and make sure the SSID is included in the policy profile currently service by the SSID (the default-policy-tag for a fresh new configuration if you have not configured tags yet). By default the default-policy-tag does not broadcast new SSIDs you create until you include them manually.

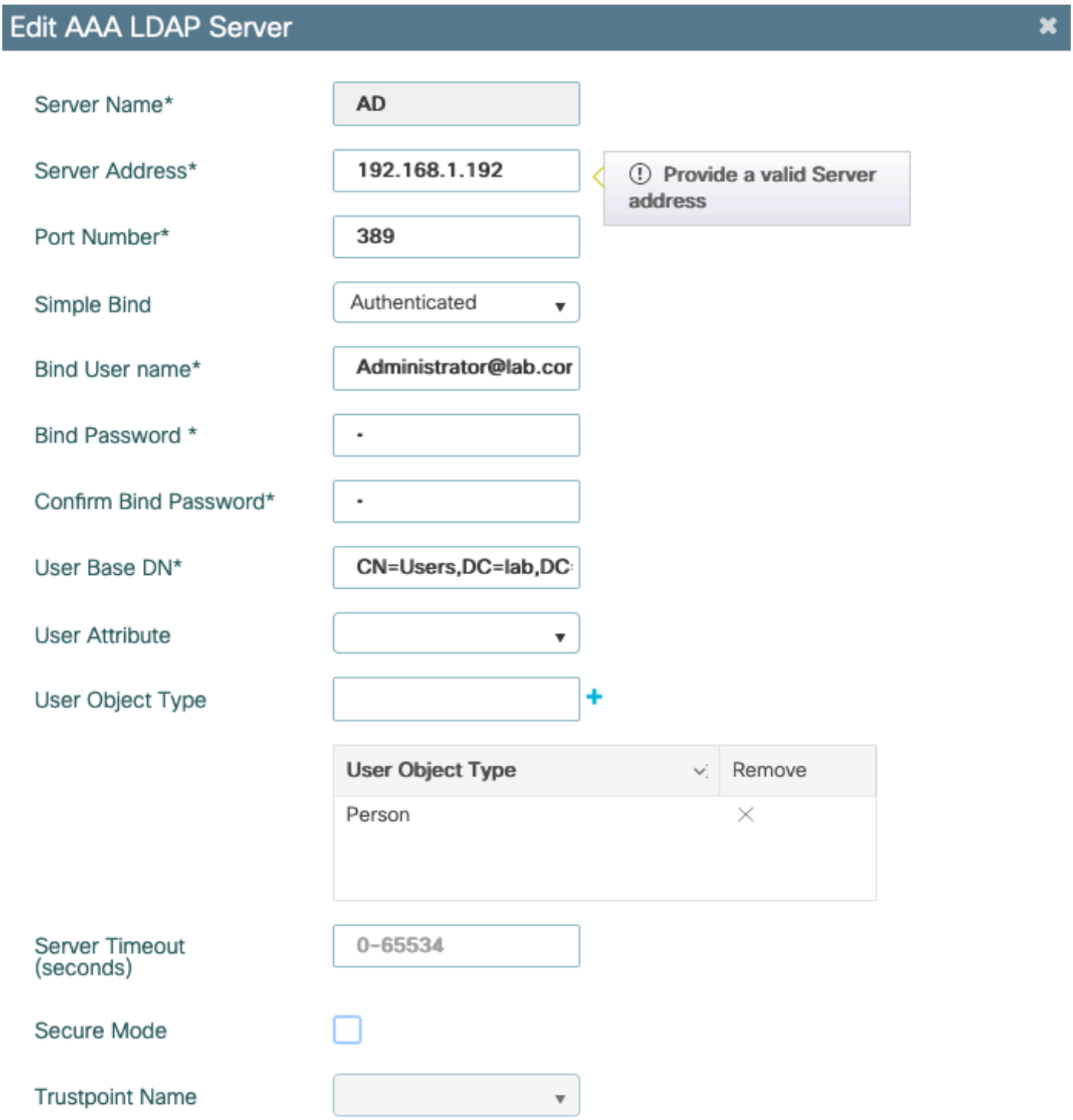
This article does not cover the configuration of policy profiles and assumes you are familiar with that part of the configuration.

If using Active Directory, you have to configure the AD server to send the attribute **userPassword**. This attribute needs to be sent to the WLC. This is because the WLC does the verification, not the AD server. You can also have issues authenticating with PEAP-mschapv2 method as the password is never sent in clear text and therefore cannot be checked with the LDAP database, only PEAP-GTC method would work with certain LDAP databases.

Understand LDAP Server Details

Understand Fields on the 9800 Web UI

Here is an example of a very basic Active Directory that acts as LDAP server configured on the 9800.



Name and IP are hopefuilly self-explanatory.

Port: 389 is the default port for LDAP but your server can use another one.

Simple bind: It is very rare to have an LDAP database nowadays that supports unauthenticated bind (that means anyone can do an LDAP search on it without any authentication form). Authenticated simple bind is the most common type of authentication and what Active Directory allows by default. You can enter an administrator account name and password to be able to do search in the user database from there.

Bind Username: You need to point to a username with administrator privileges in Active Directory. AD

tolerates the "user@domain" format for it while many other LDAP databases expect a "CN=xxx,DC=xxx" format for the username. An example with another LDAP database than AD is provided later in this article.

Bind password: Enter the password the admin username entered previously.

User Base DN: Enter here the search root, that is the location in your LDAP tree where searches start. In this example, all our uses are under the Users group, whose DN is CN=Users,DC=lab,DC=com (since the example LDAP domain is lab.com). An example of how to find out this User base DN is provided later in this section.

User attribute: This can be left empty, or point to an LDAP attribute-map that indicates which LDAP field counts as username for your LDAP database. However, due to Cisco bug ID CSCvv11813, the WLC attempts a authentication with the CN field no matter what.

User object type: This determines the type of objects that are considered as users. Typically this is Person. It could be Computers if you have an AD database and authenticates computer accounts, but there again LDAP provides for a lot of customization.

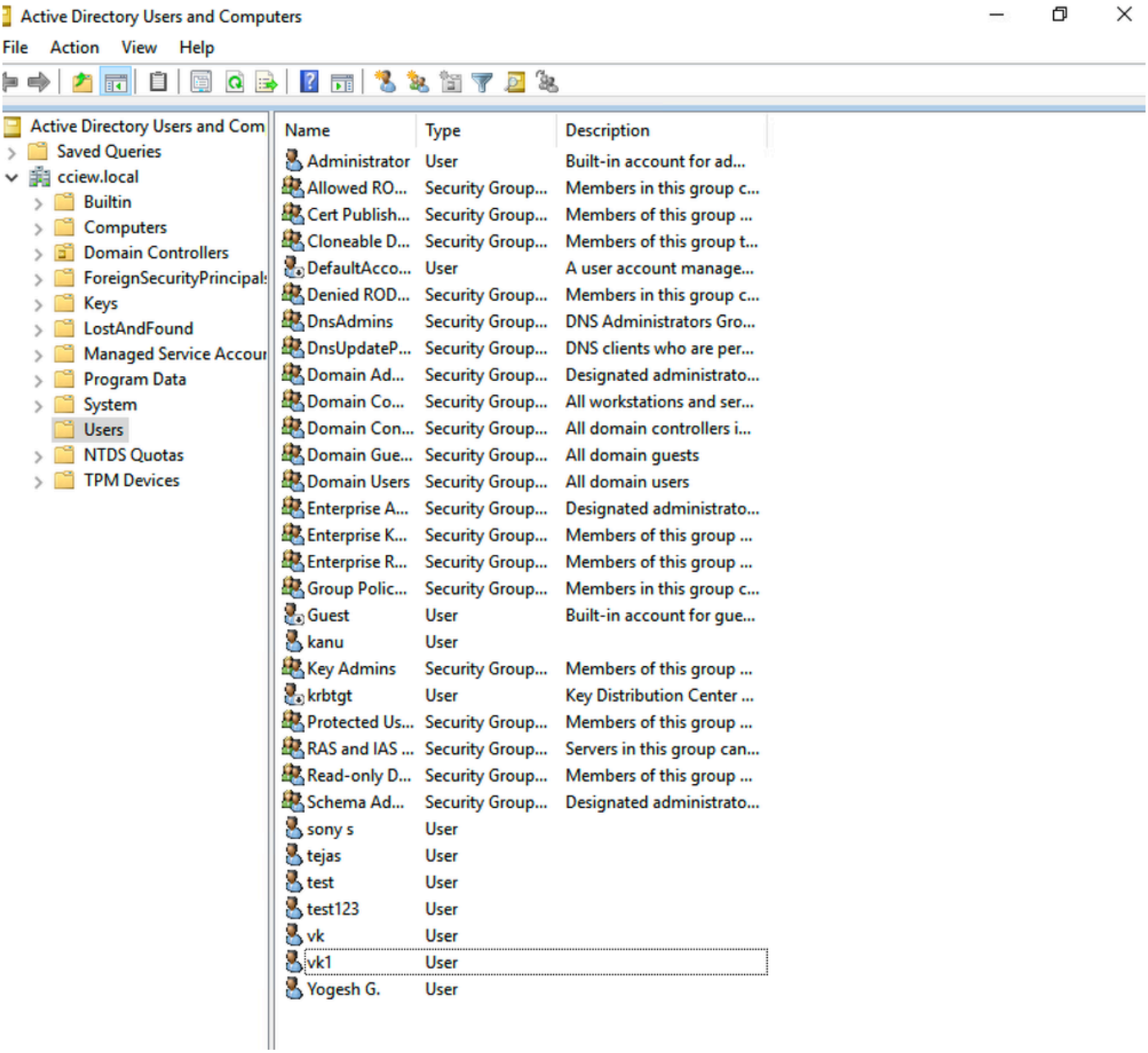
Secure mode enables Secure LDAP over TLS and requires you to select a Trustpoint on the 9800 to use a certificate for the TLS encryption.

LDAP 802.1x Authentication with sAMAaccountName Attribute

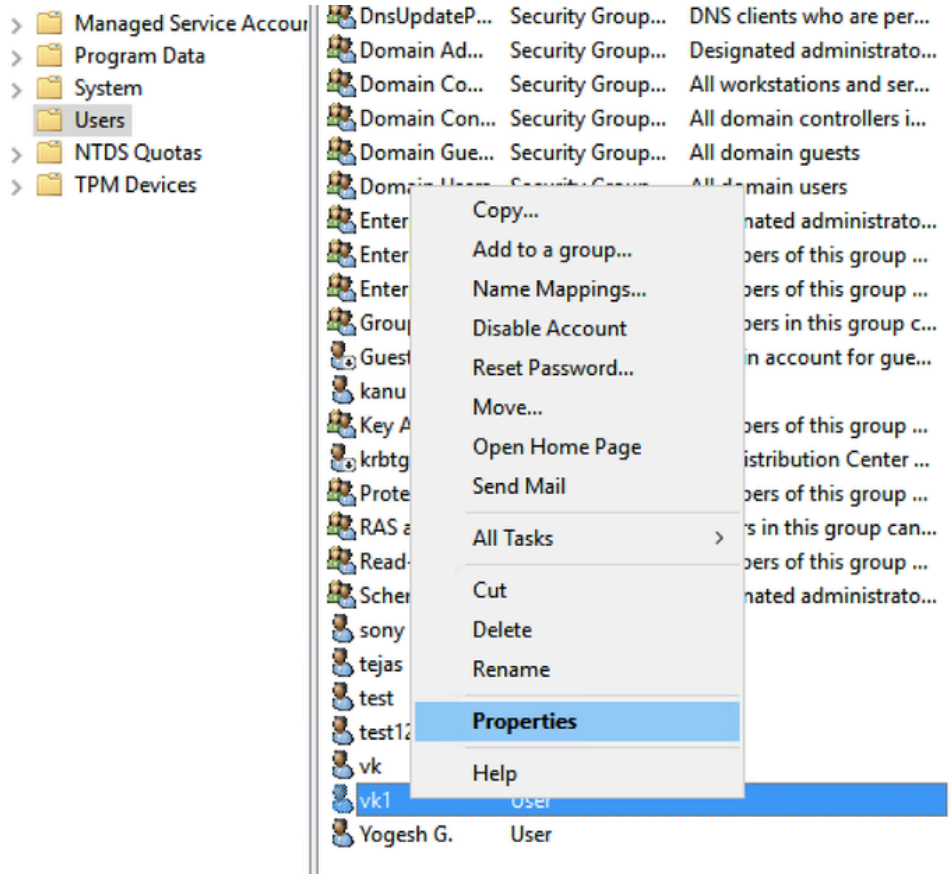
This enhancement is introduced in 17.6.1 version.

Configure userPassword Attribute for the User

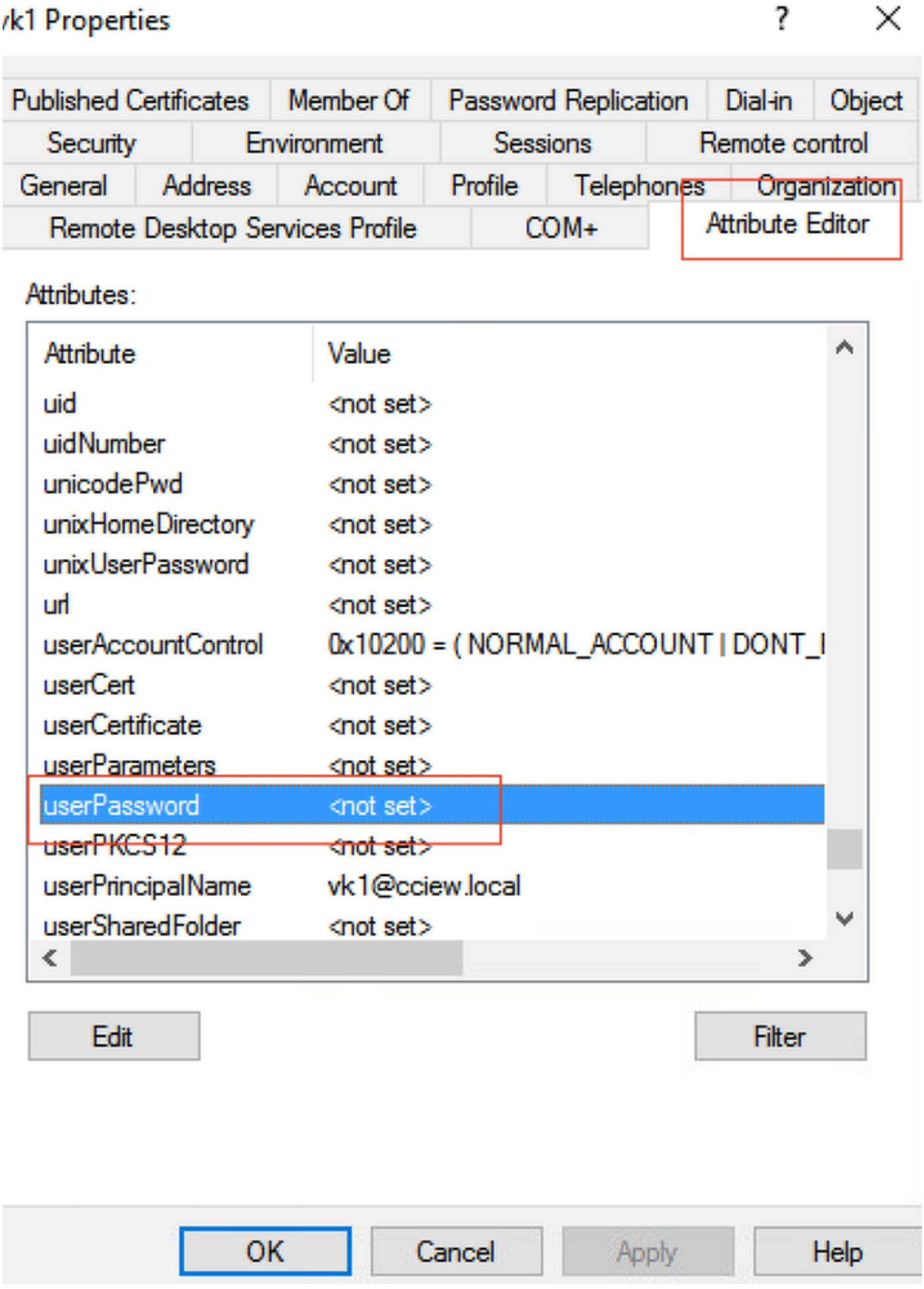
Step 1. On the Windows server navigate to ActiveDirectory Users and Computers.



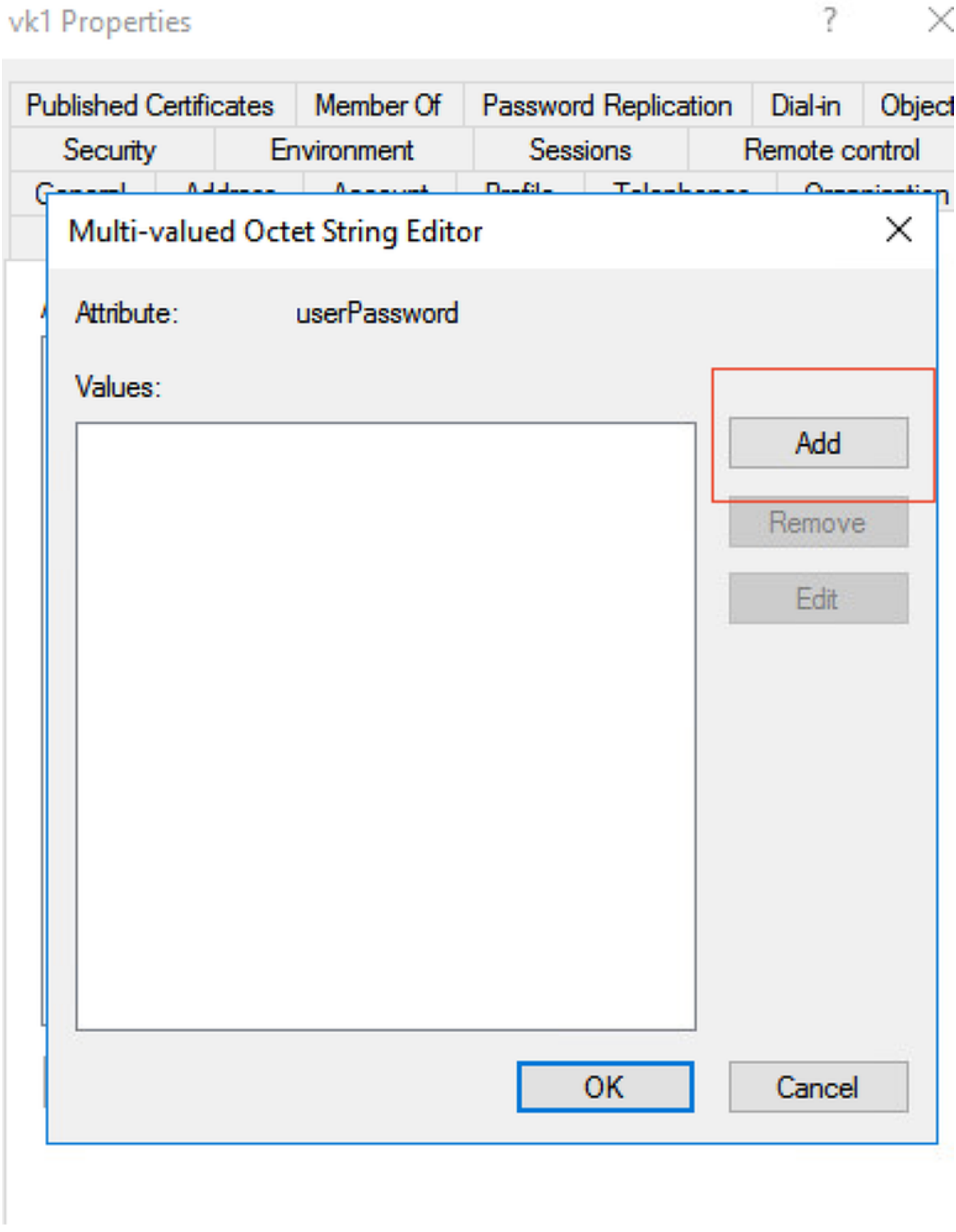
Step 2. Right click on the respective username and select properties.

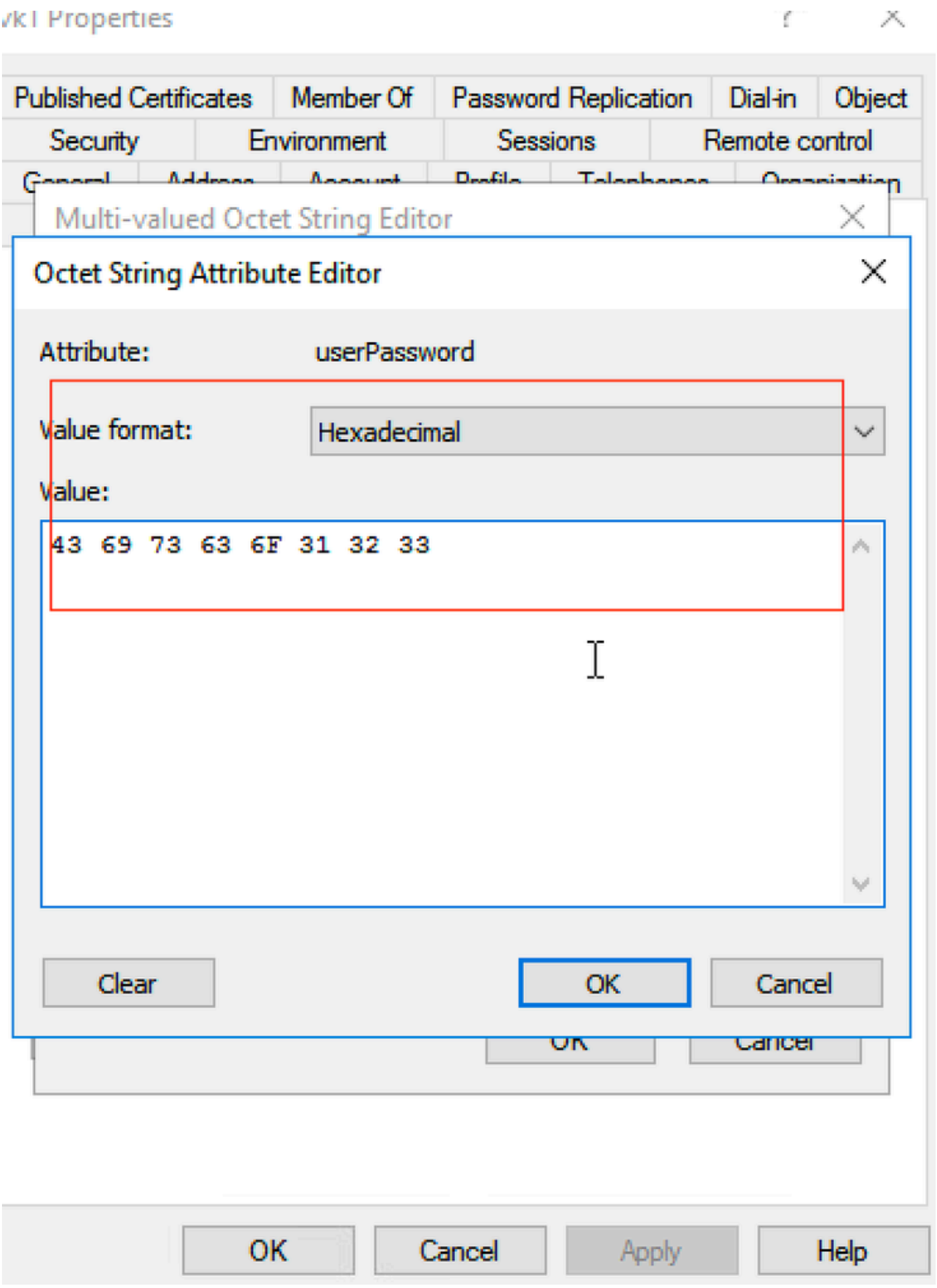


Step 3. Select attribute editor in the properties window.

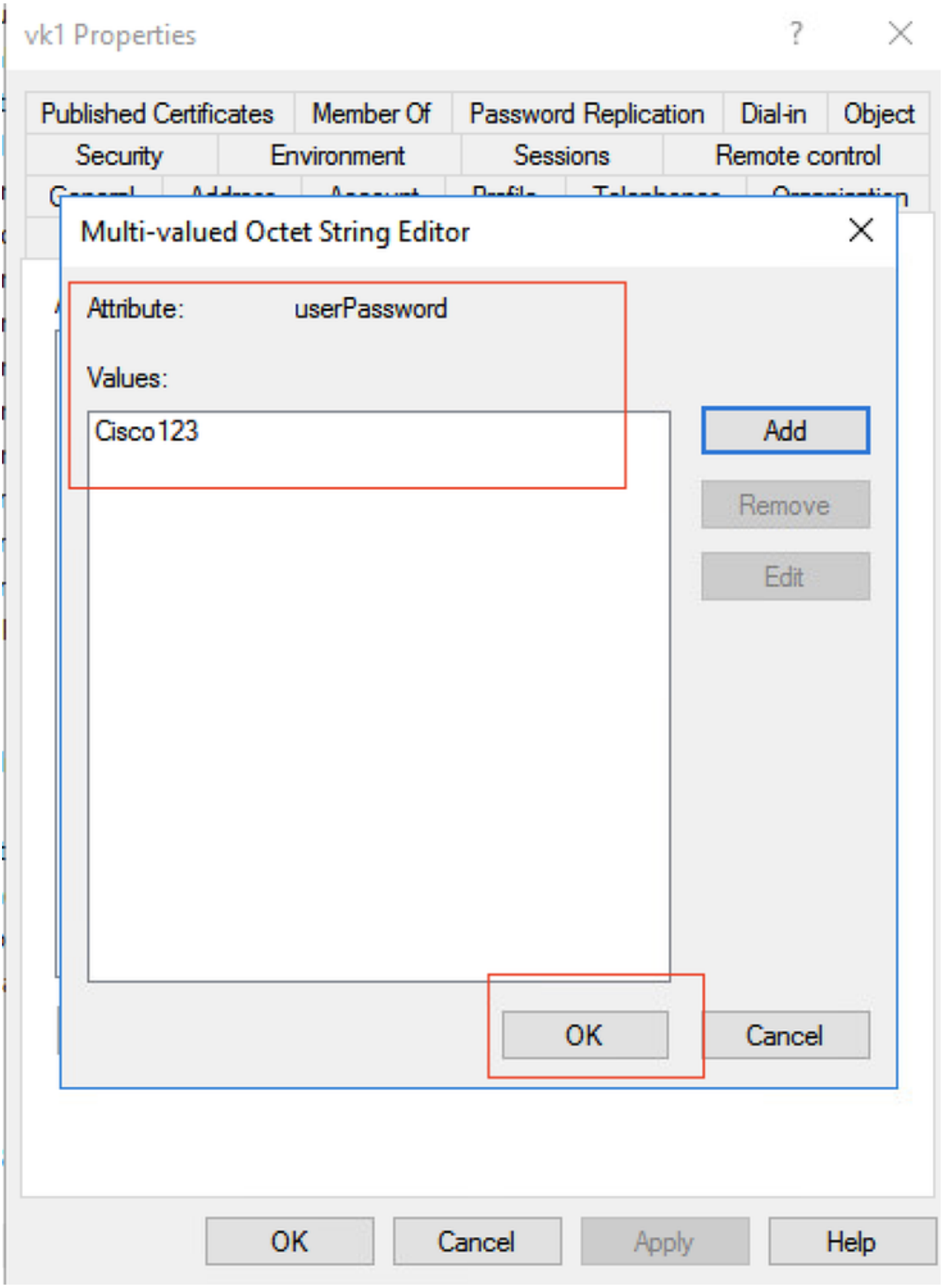

vk1 Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Security
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Remote Desktop Services Profile
COM+
Attribute Editor
Attributes:
Attribute
Value
uid
<not set>
uidNumber
<not set>
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>
Edit
Filter
OK
Cancel
Apply
Help

Step 4. Configure userPassword attribute. This is the password for the user, which needs to be configured in Hex value.

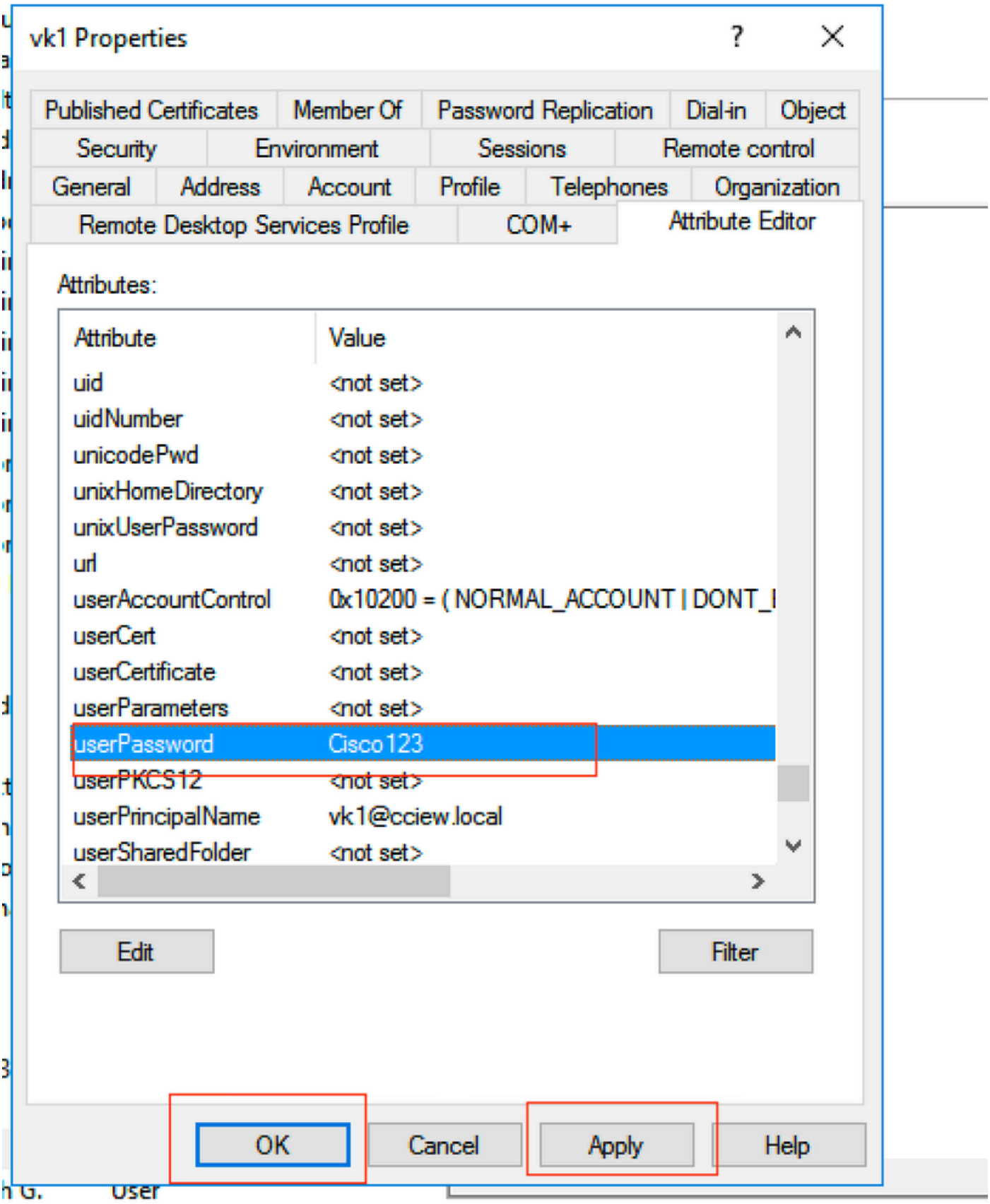




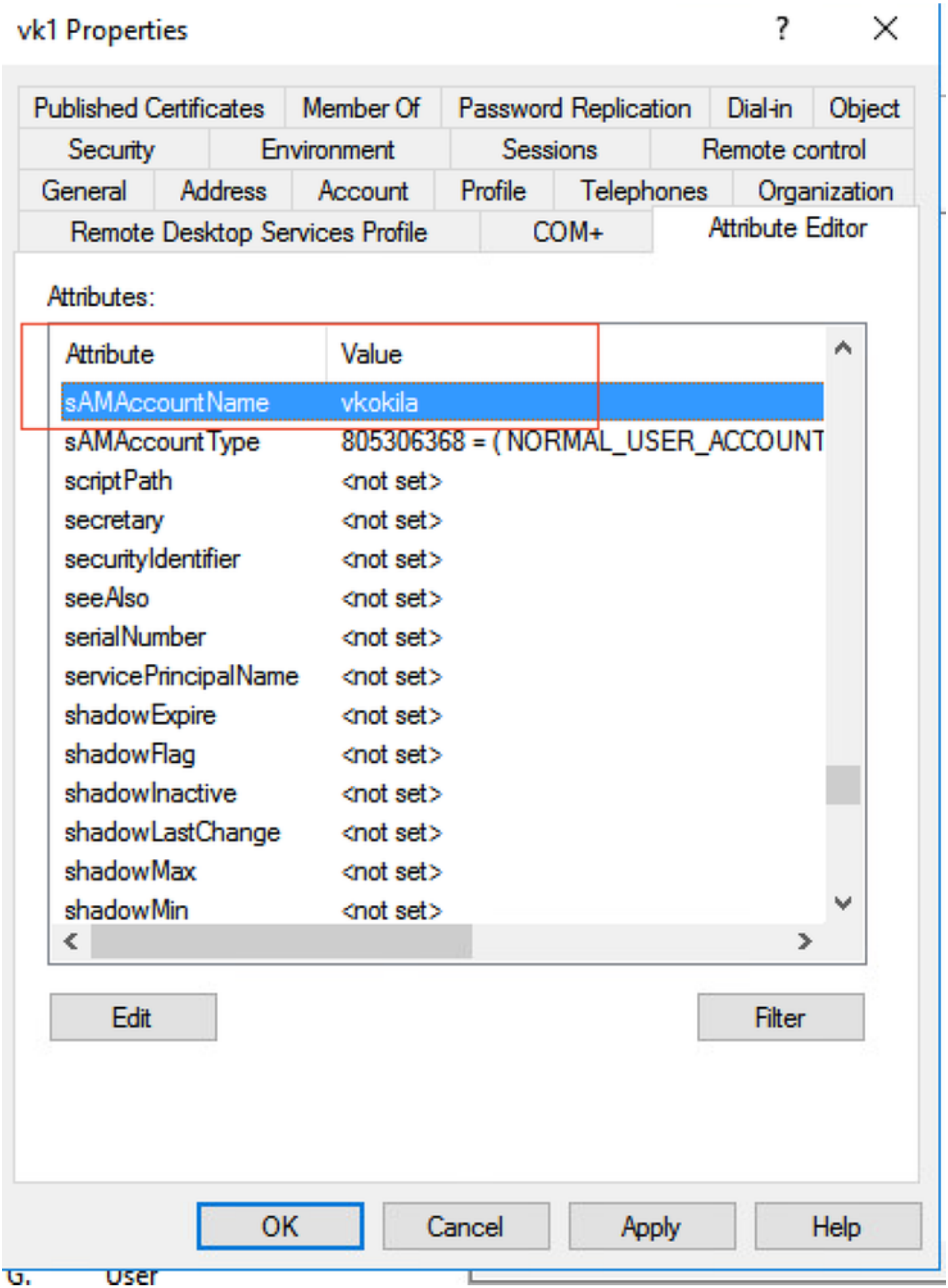
Click **ok,** the verify if it shows the correct password.



Step 5. Click **Apply** and then **OK**.



Step 6. Verify the sAMAccountName attribute value for the user and it would the username for authentication.



WLC Configuration

Step 1. Create LDAP attribute MAP.

Step 2. Configure sAMAccountName attribute and type as username.

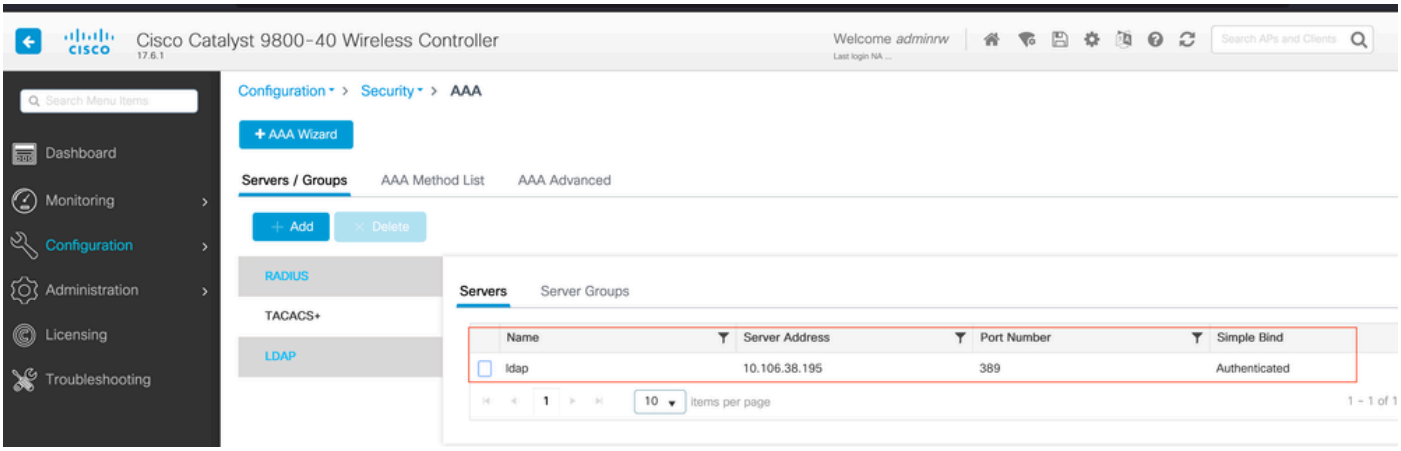
Step 3. Choose the created attribute MAP under the LDAP server configuration.

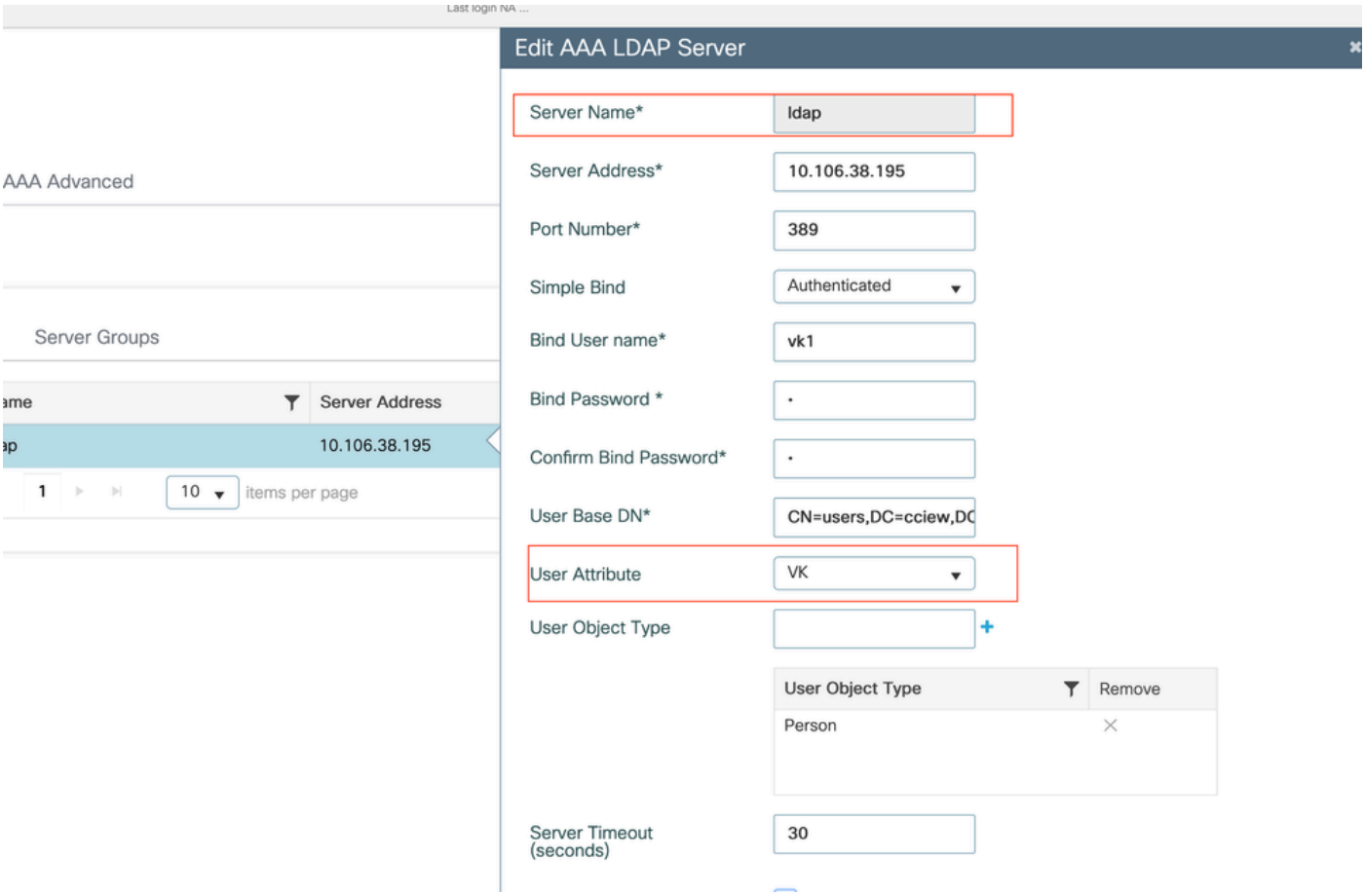
```
ldap attribute-map VK
 map type sAMAccountName username



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
```

Verify from Web Interface





Verify

To verify your configuration, double check the CLI commands with the ones from this article.

LDAP databases typically do not provide authentication logs so it can be hard to know what is going on. Visit the Troubleshoot section of this article to see how to take traces and sniffer capture in order to see if a connection is established to the LDAP database or not.

Troubleshoot

To troubleshoot this, it is best to split this into two parts. The first part is validating the Local EAP portion. The second is validating that the 9800 is communicating with the LDAP server properly.

How to Verify the Authentication Process on the Controller

You can collect a Radioactive trace in order to get the debugs of the client connection.

Simply go to **Troubleshooting > Radioactive Trace**. Add the client MAC address (pay attention that your client can be using a random MAC and not its own MAC, you can verify this in the SSID profile on the client device itself) and hit start.

Once you reproduced the connection attempt, you can click on Generate and obtain the logs for the last X minutes. Make sure to click **internal** as some LDAP log lines do not appear if you do not enable it.

Here is an example of radioactive trace of a client successfully authenticating on a web authentication SSID. Some redundant parts were removed for clarity :

```
2021/01/19 21:57:55.890953 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (note): MAC: 2e1f.3a65.9c09  Asso
2021/01/19 21:57:55.891049 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09  Rec
2021/01/19 21:57:55.891282 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09  C
2021/01/19 21:57:55.891674 {wncd_x_R0-0}{1}: [dot11-validate] [9347]: (info): MAC: 2e1f.3a65.9c09  WiFi
2021/01/19 21:57:55.892114 {wncd_x_R0-0}{1}: [dot11] [9347]: (debug): MAC: 2e1f.3a65.9c09  dot11 send a
2021/01/19 21:57:55.892182 {wncd_x_R0-0}{1}: [dot11-frame] [9347]: (info): MAC: 2e1f.3a65.9c09  WiFi di
2021/01/19 21:57:55.892248 {wncd_x_R0-0}{1}: [dot11] [9347]: (info): MAC: 2e1f.3a65.9c09  dot11 send as
2021/01/19 21:57:55.892467 {wncd_x_R0-0}{1}: [dot11] [9347]: (note): MAC: 2e1f.3a65.9c09  Association s
2021/01/19 21:57:55.892497 {wncd_x_R0-0}{1}: [dot11] [9347]: (info): MAC: 2e1f.3a65.9c09  DOT11 state t
2021/01/19 21:57:55.892616 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09  Sta
2021/01/19 21:57:55.892730 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09  Sta
2021/01/19 21:57:55.892783 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09  C
2021/01/19 21:57:55.892896 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09  L2 Auth
2021/01/19 21:57:55.893115 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893154 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893205 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:57:55.893211 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:57:55.893254 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09  Client
2021/01/19 21:57:55.893461 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:unknown] auth m
2021/01/19 21:57:55.893532 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893603 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893649 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893679 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893731 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894285 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894299 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894551 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894587 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:57:55.894593 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:57:55.894827 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894858 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:57:55.894862 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:57:55.895918 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [0000.0000.0000:u
2021/01/19 21:57:55.896094 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.896807 {wncd_x_R0-0}{1}: [webauth-sm] [9347]: (info): [       0.0.0.0]Starting Web
2021/01/19 21:57:55.897106 {wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2e1f.3a65.9c
2021/01/19 21:57:55.897790 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info): [0000.0000.0000:unknown] UR
2021/01/19 21:57:55.898813 {wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2e1f.3a65.9c
2021/01/19 21:57:55.899406 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info): [0000.0000.0000:unknown] UR
2021/01/19 21:57:55.903552 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09  Client
2021/01/19 21:57:55.903575 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [9347]: (note): Authentication Success. R
2021/01/19 21:57:55.903592 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09  Client
2021/01/19 21:57:55.903709 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09  Client
2021/01/19 21:57:55.903774 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.903858 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.903924 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.904005 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09  L2
2021/01/19 21:57:55.904173 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (note): MAC: 2e1f.3a65.9c09  Mobi
2021/01/19 21:57:55.904181 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09  C
2021/01/19 21:57:55.904245 {wncd_x_R0-0}{1}: [mm-transition] [9347]: (info): MAC: 2e1f.3a65.9c09  MMIF
2021/01/19 21:57:55.904410 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2e1f.3a65.9c09  Invalid t
2021/01/19 21:57:55.904777 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2e1f.3a65.9c09  Received
2021/01/19 21:57:55.904955 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2e1f.3a65.9c09  Add MCC
2021/01/19 21:57:55.905072 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 0000.0000.0000  Sending
2021/01/19 21:57:55.905157 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2e1f.3a65.9c09  Received
2021/01/19 21:57:55.905267 {wncd_x_R0-0}{1}: [mm-transition] [9347]: (info): MAC: 2e1f.3a65.9c09  MMIF
2021/01/19 21:57:55.905283 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2e1f.3a65.9c09  Roam type
2021/01/19 21:57:55.905317 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2e1f.3a65.9c09  Mobility
2021/01/19 21:57:55.905515 {wncd_x_R0-0}{1}: [mm-client] [9347]: (note): MAC: 2e1f.3a65.9c09  Mobility
2021/01/19 21:57:55.905570 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09  Pro
2021/01/19 21:57:55.906210 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09  Cli
2021/01/19 21:57:55.906369 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09  No
```

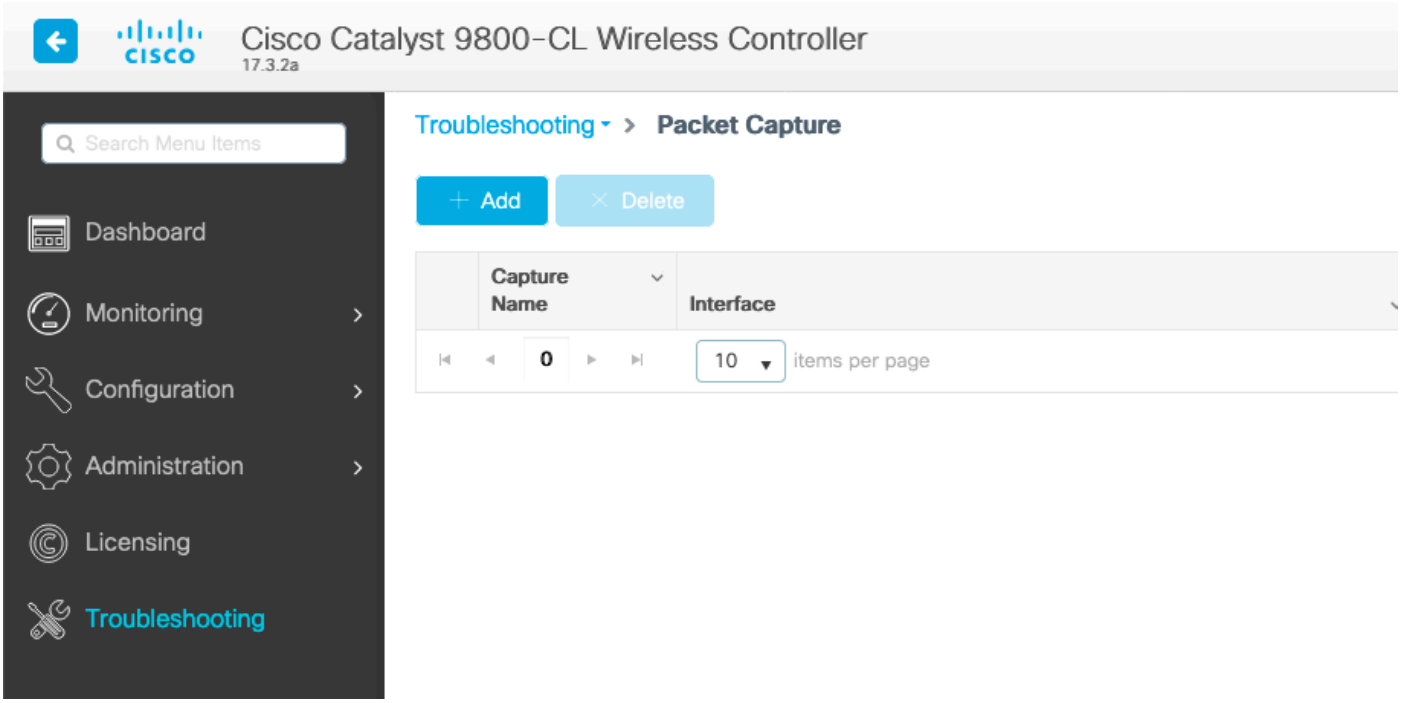
```
2021/01/19 21:57:55.906399 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09  No
2021/01/19 21:57:55.906486 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09  ADD MOB
2021/01/19 21:57:55.906613 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09  C
2021/01/19 21:57:55.907326 {wncd_x_R0-0}{1}: [dot11] [9347]: (note): MAC: 2e1f.3a65.9c09  Client datapa
2021/01/19 21:57:55.907544 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09  Cli
2021/01/19 21:57:55.907594 {wncd_x_R0-0}{1}: [avc-afc] [9347]: (debug): AVC enabled for client 2e1f.3a6
2021/01/19 21:57:55.907701 {wncd_x_R0-0}{1}: [dpath_svc] [9347]: (note): MAC: 2e1f.3a65.9c09  Client da
2021/01/19 21:57:55.908229 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09  C
2021/01/19 21:57:55.908704 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  IP-l
2021/01/19 21:57:55.918694 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09  Client
2021/01/19 21:57:55.922254 {wncd_x_R0-0}{1}: [dot11k] [9347]: (info): MAC: 2e1f.3a65.9c09  Neighbor AP
2021/01/19 21:57:55.922260 {wncd_x_R0-0}{1}: [dot11k] [9347]: (info): MAC: 2e1f.3a65.9c09  Neighbor AP
2021/01/19 21:57:55.962883 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (note): MAC: 2e1f.3a65.9c09  Clie
2021/01/19 21:57:55.963827 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  Clie
2021/01/19 21:57:55.964481 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.965176 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  IP-l
2021/01/19 21:57:55.965550 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.966127 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  IP-l
2021/01/19 21:57:55.966328 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09  Rec
2021/01/19 21:57:55.966413 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09  Tri
2021/01/19 21:57:55.966424 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09  C
2021/01/19 21:57:55.967404 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09  L3 Auth
2021/01/19 21:57:55.967433 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09  Client
2021/01/19 21:57:55.968312 {wncd_x_R0-0}{1}: [sisf-packet] [9347]: (debug): RX: ARP from interface capw
2021/01/19 21:57:55.968519 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  iple
2021/01/19 21:57:55.968522 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  Clie
2021/01/19 21:57:55.968966 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  IP-l
2021/01/19 21:57:57.762648 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  iple
2021/01/19 21:57:57.762650 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  Clie
2021/01/19 21:57:57.763032 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09  IP-l
2021/01/19 21:58:00.992597 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:00.992617 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:00.992669 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:00.992694 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:00.993558 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:00.993637 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:00.993645 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:00.996320 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:00.996508 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:00.996524 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:05.808144 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.808226 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.808251 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.860465 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.860483 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.860534 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.860559 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.628209 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.628228 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.628287 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.628316 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.628832 {wncd_x_R0-0}{1}: [webauth-page] [9347]: (info): capwap_90000004[2e1f.3a65.9
2021/01/19 21:58:06.629613 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.629699 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:06.629709 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:06.633058 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.633219 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.633231 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.719502 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.719521 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.719591 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.719646 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
```

```
2021/01/19 21:58:06.720038 {wncd_x_R0-0}{1}: [webauth-error] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.720623 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:06.720707 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:06.720716 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:06.724036 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:06.746127 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.746145 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.746197 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.746225 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.746612 {wncd_x_R0-0}{1}: [webauth-error] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.747105 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:06.747187 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:06.747197 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:06.750598 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:15.902342 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:15.902360 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:15.902410 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:15.902435 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:15.903173 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:15.903252 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:15.903261 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:15.905950 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:15.906112 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:15.906125 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:16.357093 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:16.357443 {wncd_x_R0-0}{1}: [sadb-attr] [9347]: (info): Removing ipv6 addresses from t
2021/01/19 21:58:16.357674 {wncd_x_R0-0}{1}: [caaa-authen] [9347]: (info): [CAAA:AUTHEN:b7000080] DEBUG
2021/01/19 21:58:16.374292 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:16.374412 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [9347]: (note): Authentication Success. R
2021/01/19 21:58:16.374442 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09  Client
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_9000000
2021/01/19 21:58:16.374797 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_9000000
2021/01/19 21:58:16.375294 {wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2e1f.3a65.9c
2021/01/19 21:58:16.376120 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info): [0000.0000.0000:unknown] UR
2021/01/19 21:58:16.377322 {wncd_x_R0-0}{1}: [webauth-page] [9347]: (info): capwap_90000004[2e1f.3a65.9
2021/01/19 21:58:16.378405 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09  L3 Auth
2021/01/19 21:58:16.378426 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09  Client
2021/01/19 21:58:16.379181 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09  Cli
2021/01/19 21:58:16.379323 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09  No
2021/01/19 21:58:16.379358 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09  No
2021/01/19 21:58:16.379442 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09  ADD MOB
2021/01/19 21:58:16.380547 {wncd_x_R0-0}{1}: [errmsg] [9347]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_T
2021/01/19 21:58:16.380729 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute :bsn-vl
2021/01/19 21:58:16.380736 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute :
2021/01/19 21:58:16.380812 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute :    ur
2021/01/19 21:58:16.380969 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09  Cli
2021/01/19 21:58:16.381033 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [9347]: (debug): Managed client RUN sta
2021/01/19 21:58:16.381152 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09  C
2021/01/19 21:58:16.385252 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09  Cli
2021/01/19 21:58:16.385321 {wncd_x_R0-0}{1}: [avc-afc] [9347]: (debug): AVC enabled for client 2e1f.3a6
```

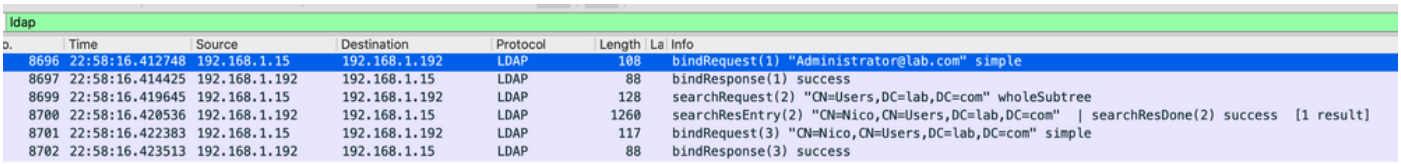
How to Verify 9800 to LDAP Connectivity

You can take an embedded capture in the 9800 in order to see what traffic is going towards LDAP.

To take a capture from the WLC, navigate to **Troubleshooting > Packet Capture** and click **+Add**. Chose the uplink port and start capturing.



Here is a sample success authentication for user **Nico**.

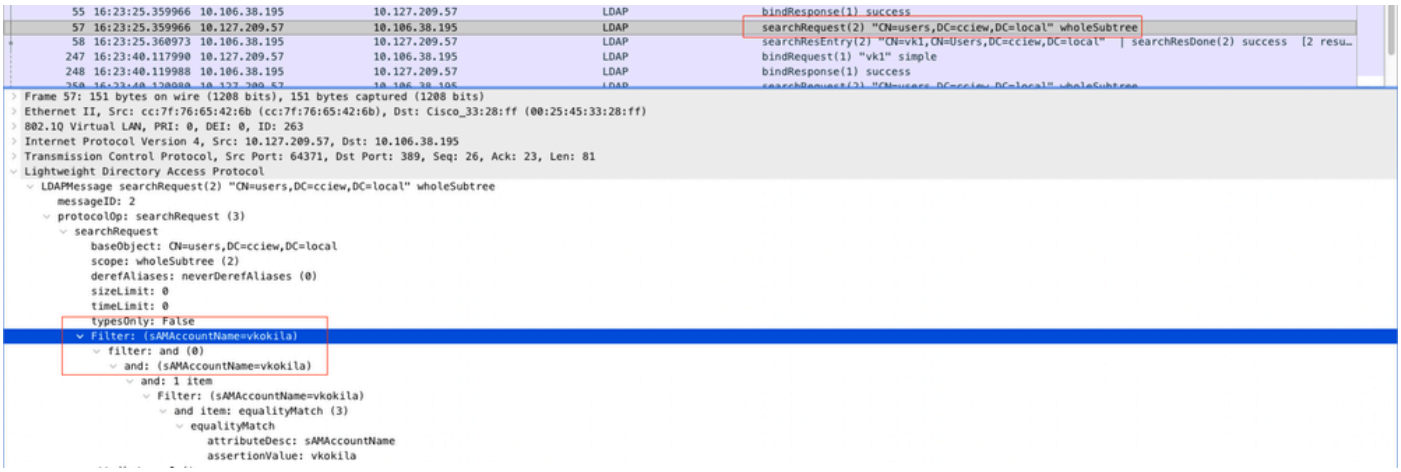


The first 2 packets represent the WLC binding to the LDAP db, that is the WLC authenticating to the database with the admin user (in order to be able to perform a search).

These 2 LDAP packets represent the WLC doing a search in the base DN (here CN=Users,DC=lab,DC=com). The inside of the packet contains a filter for the username (here Nico). The LDAP database return the user attributes as a success.

The last 2 packets represent the WLC trying to authenticate with that user password to test if the password is the right one.

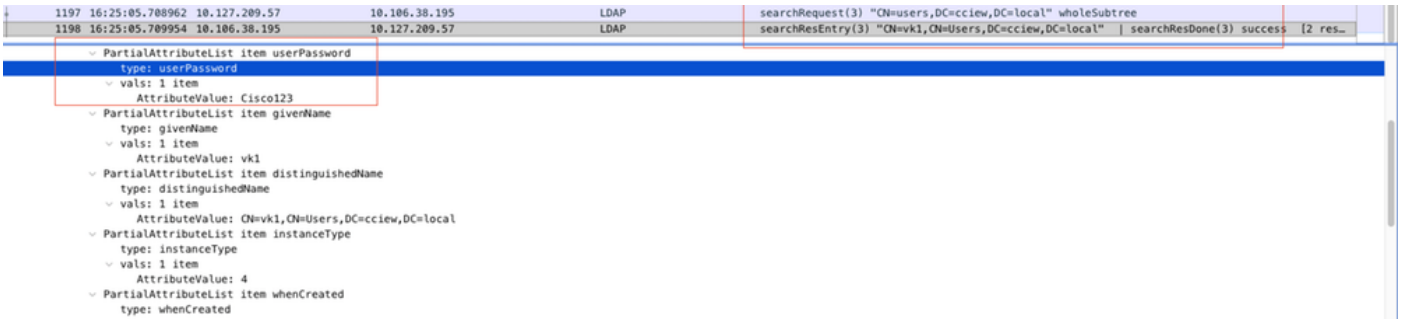
1. Collect EPC and check if sAMAccountName is applied as filter:



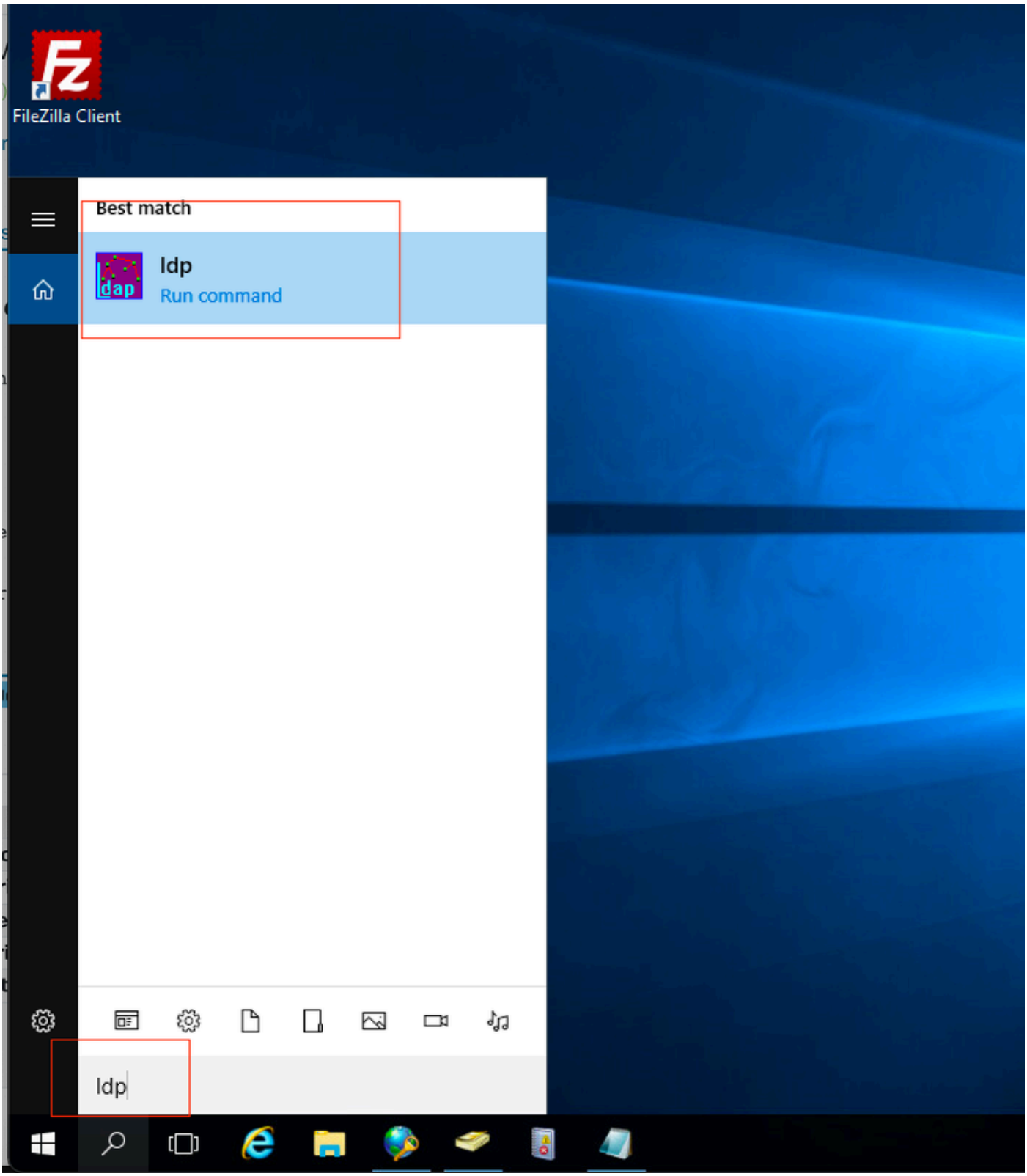
If the filter shows **cn** and if sAMAccountName is being used as the username, then authentication fails.

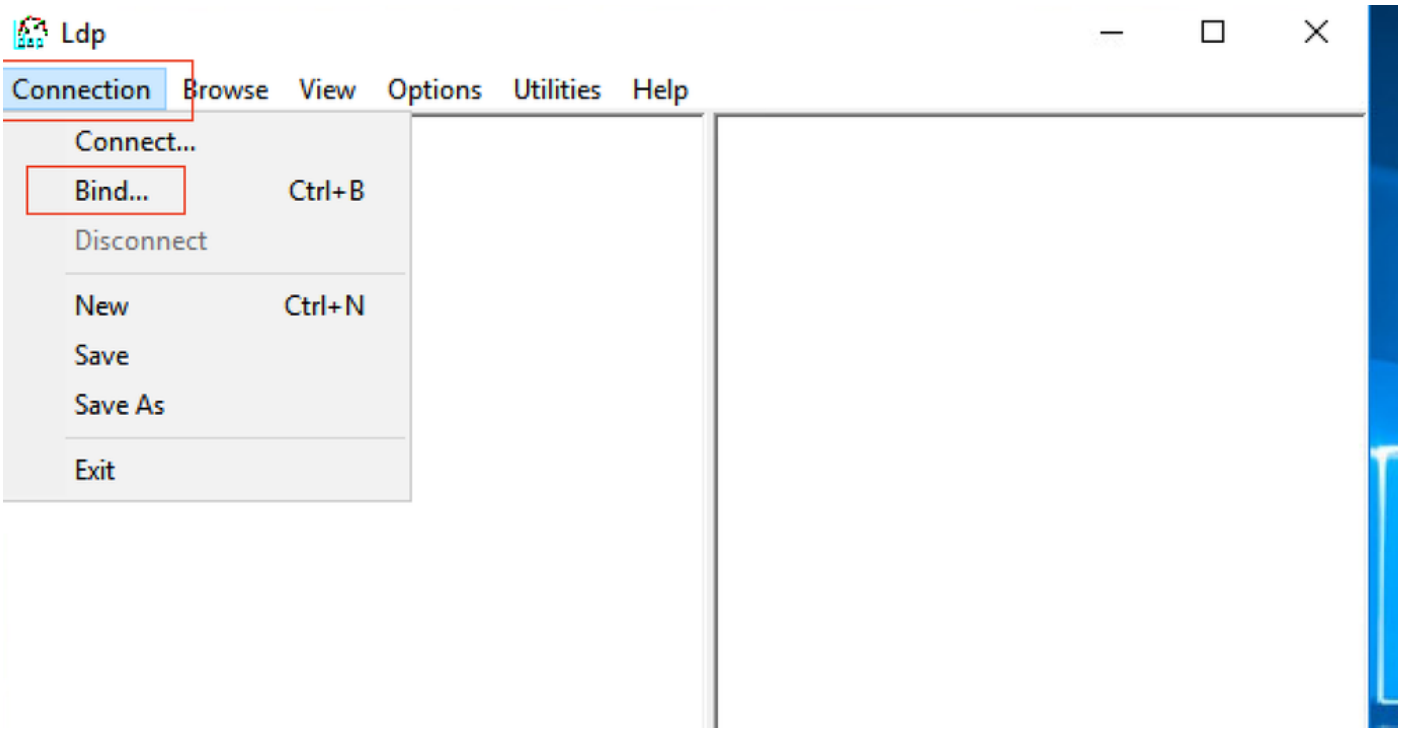
Reconfigure the ldap map attribute from WLC cli.

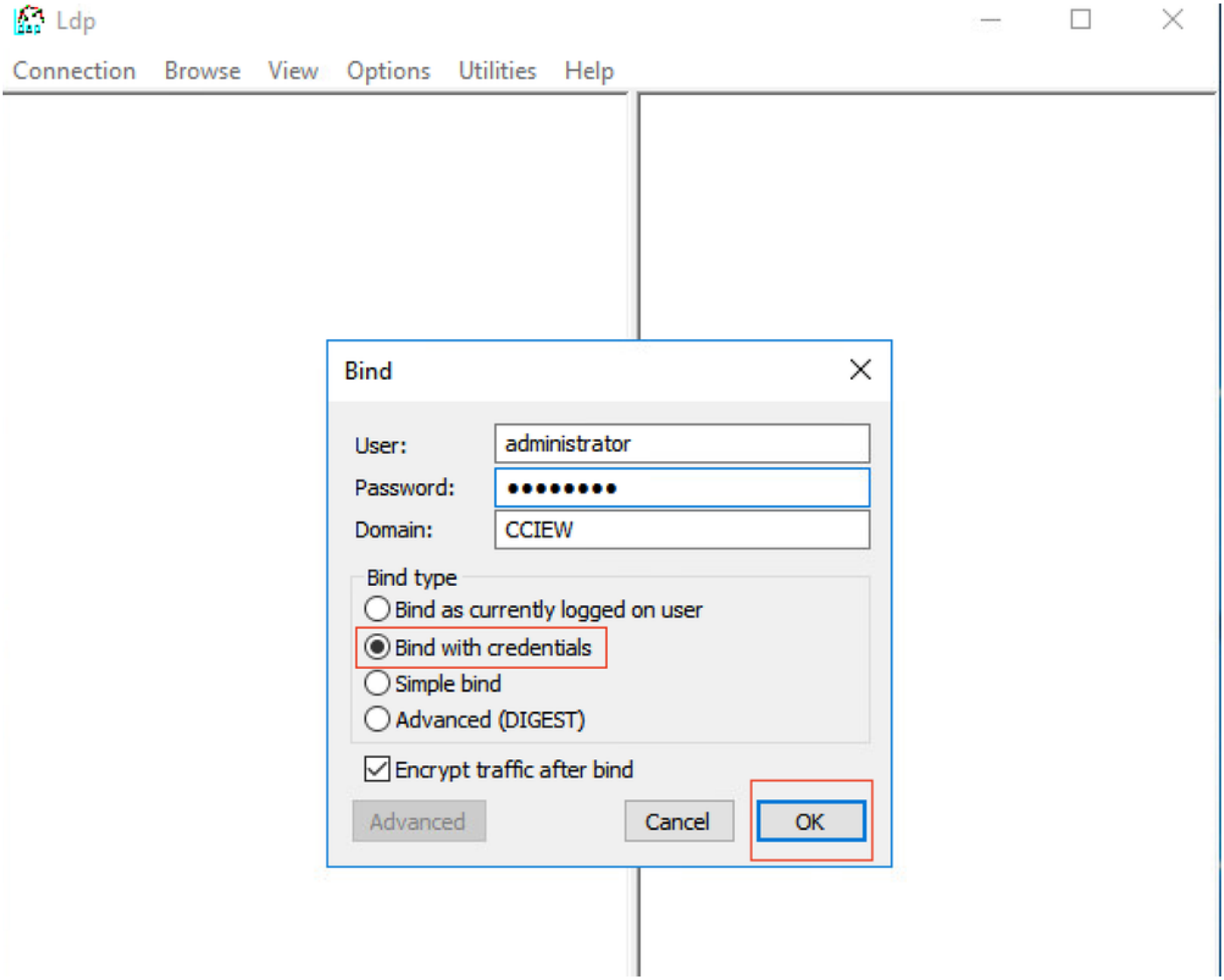
2. Ensure server returns userPassword in cleartext, else authentication fails.

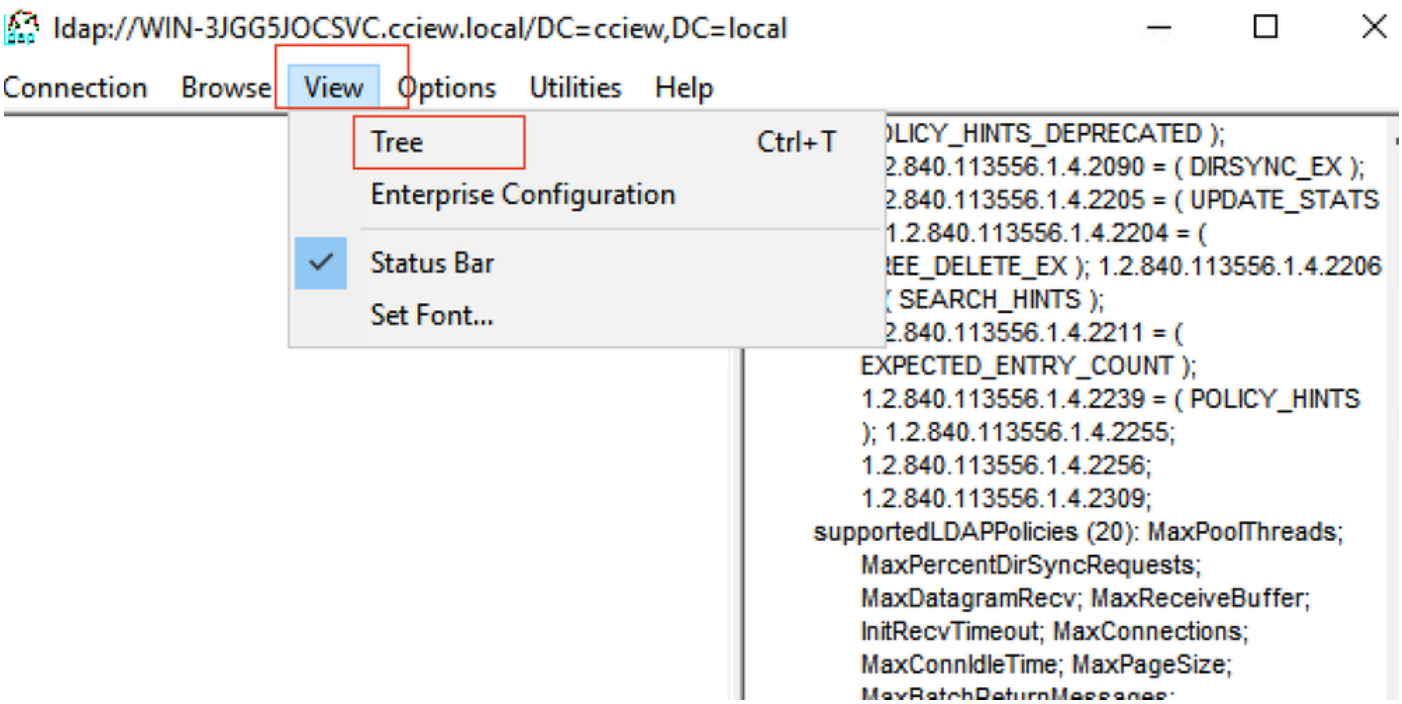


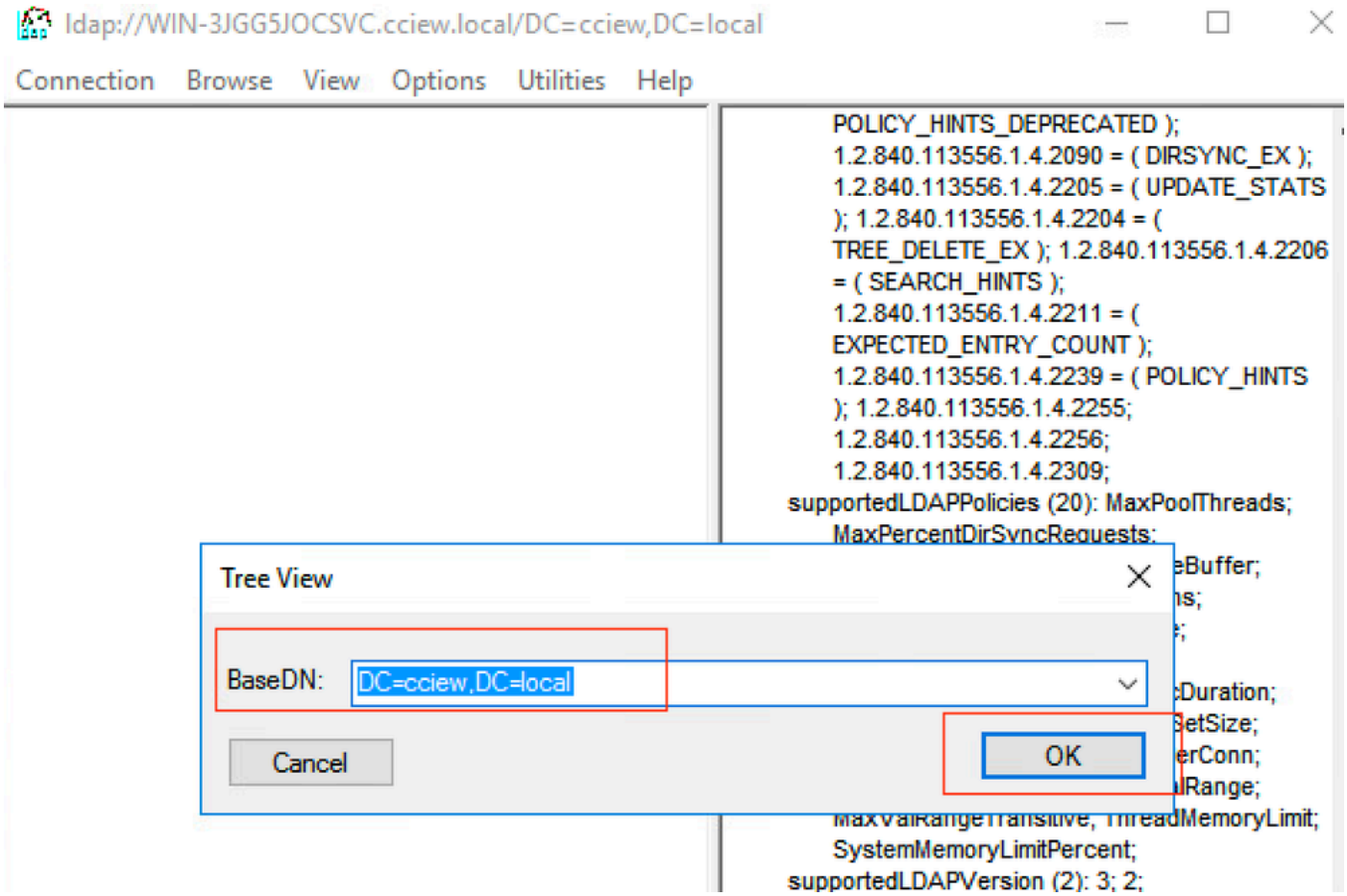
3. Use the ldp.exe tool on the server to validate Base DN information.

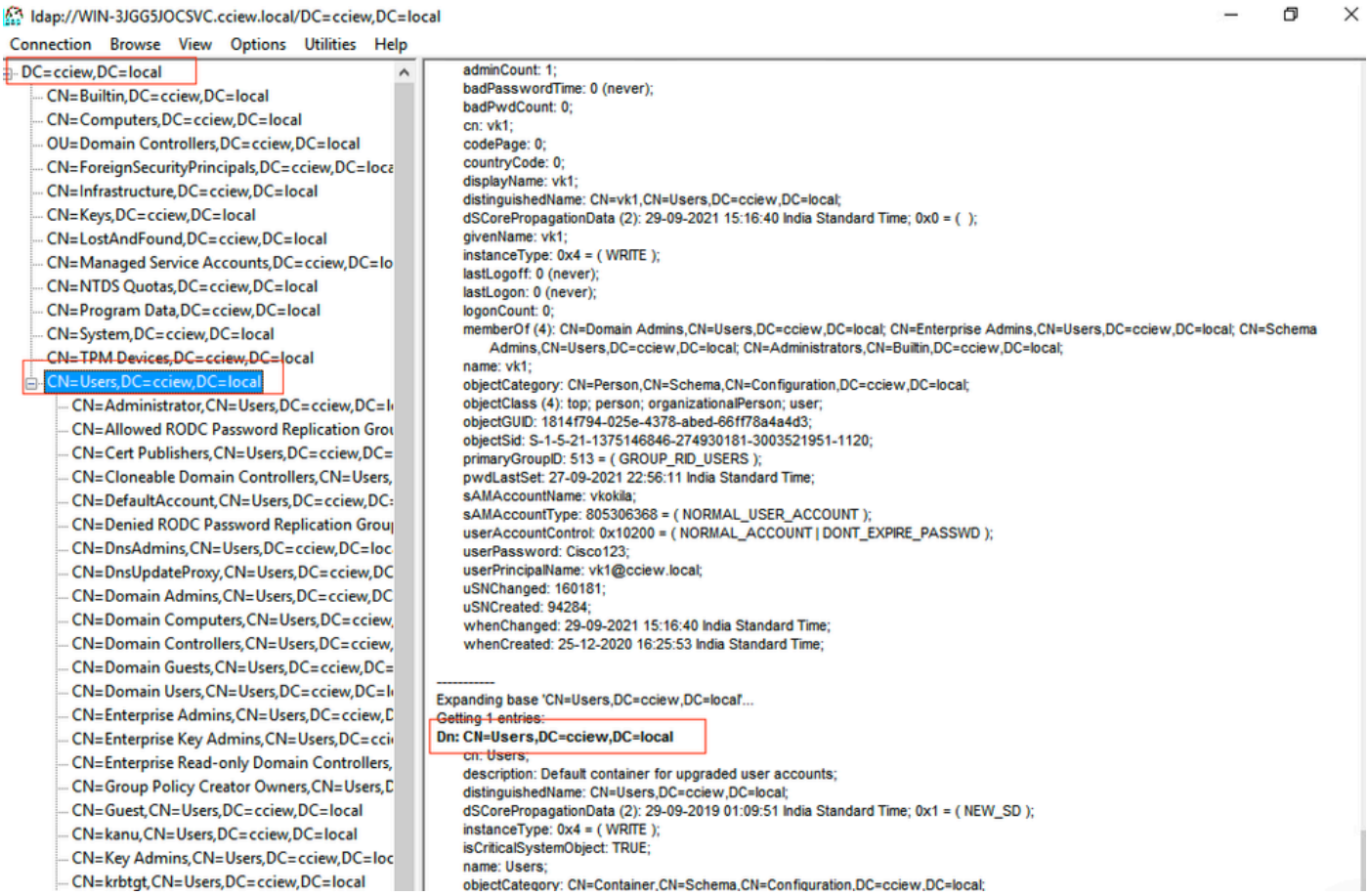

FileZilla Client
Best match
ldp
Run command
ldp

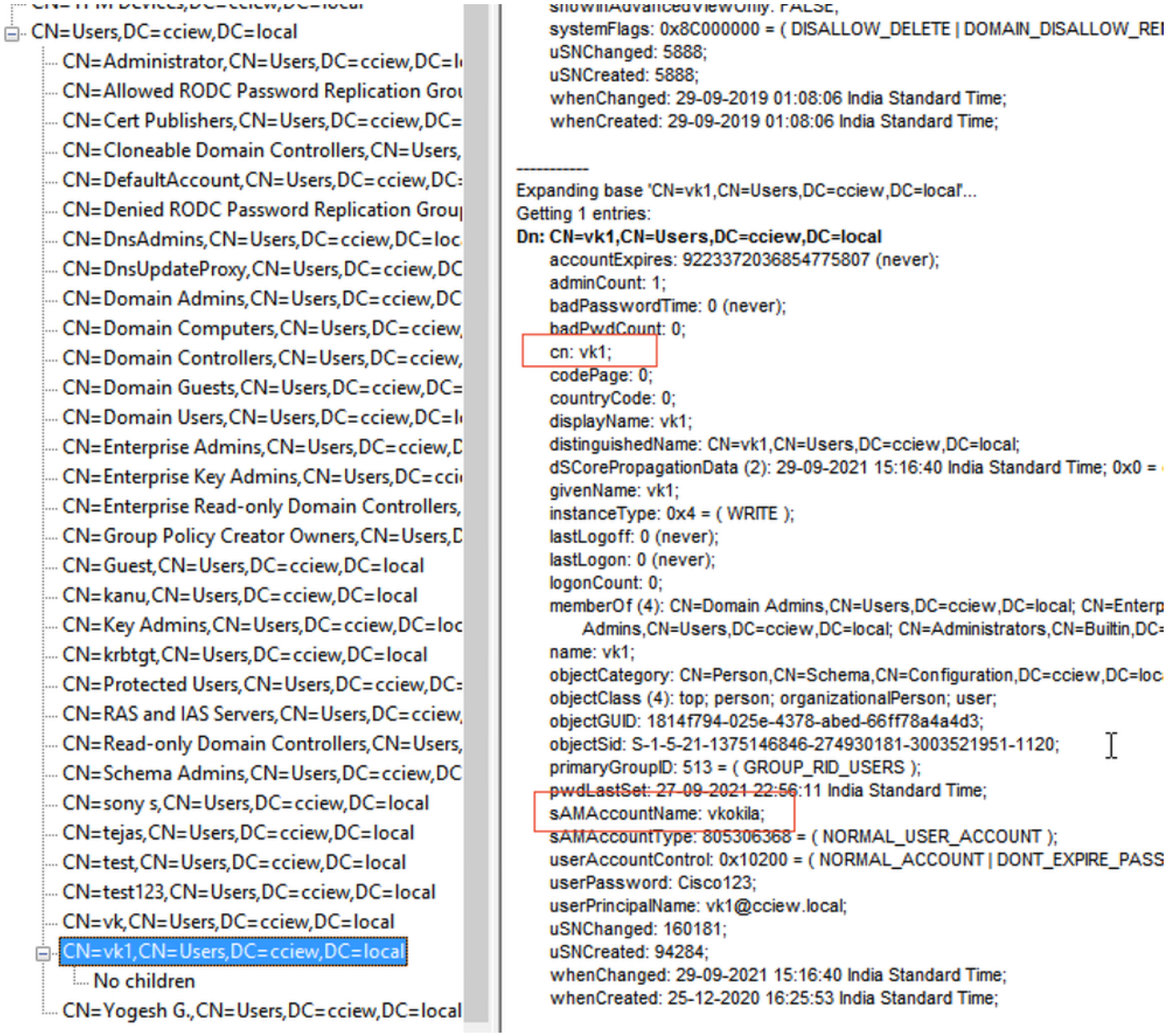

Ldp
Connection
Browse
View
Options
Utilities
Help
Connect...
Bind... Ctrl+B
Disconnect
New Ctrl+N
Save
Save As
Exit


Ldp
Connection
Browse
View
Options
Utilities
Help
Bind
User:
administrator
Password:
Domain:
CCIEW
Bind type
Bind as currently logged on user
Bind with credentials
Simple bind
Advanced (DIGEST)
Encrypt traffic after bind
Advanced
Cancel
OK


ldap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local
Connection
Browse
View
Options
Utilities
Help
Tree
Ctrl+T
Enterprise Configuration
Status Bar
Set Font...
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;


ldap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local
Connection
Browse
View
Options
Utilities
Help
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;
SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
Tree View
BaseDN:
DC=cciew,DC=local
Cancel
OK


ldap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local
Connection Browse View Options Utilities Help
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;



4. Check server statistics and attribute MAP.

<#root>

```
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

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

Related Information

- Local EAP on 9800 configuration example
- Cisco Technical Support & Downloads