为Catalyst 9800 WLC配置802.1X的LDAP身份验证和网络身份验证

目录

简介

本文档介绍如何配置Catalyst 9800以使用LDAP服务器作为用户凭证数据库对客户端进行身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- Microsoft Windows服务器
- Active Directory或任何其他LDAP数据库

使用的组件

运行Cisco IOS®-XE版本17.3.2a的C9100接入点(AP)上的C9800 EWC

具有QNAP网络访问存储(NAS)（用作LDAP数据库）的Microsoft Active Directory(AD)服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

使用Webauth SSID配置LDAP

网络图

本文基于一个非常简单的设置：

具有IP 192.168.1.15的EWC AP 9115

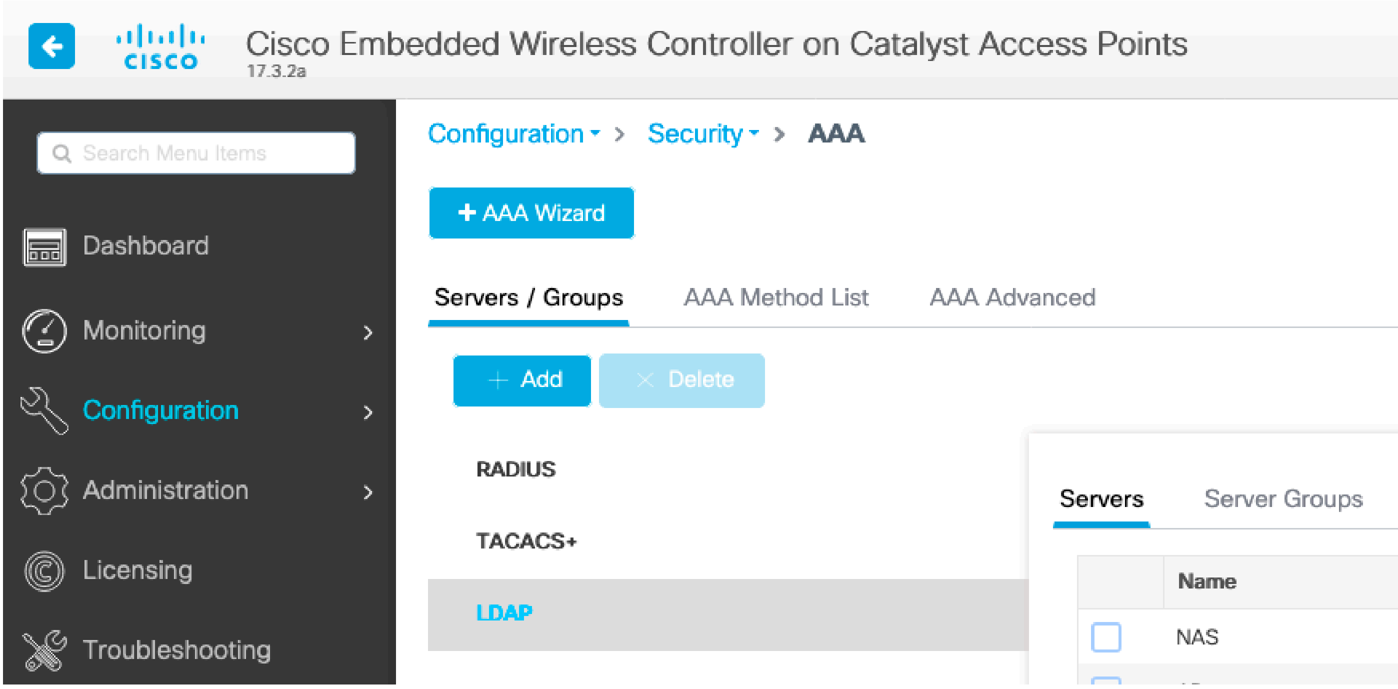
IP为192.168.1.192的Active Directory服务器

连接到EWC内部AP的客户端

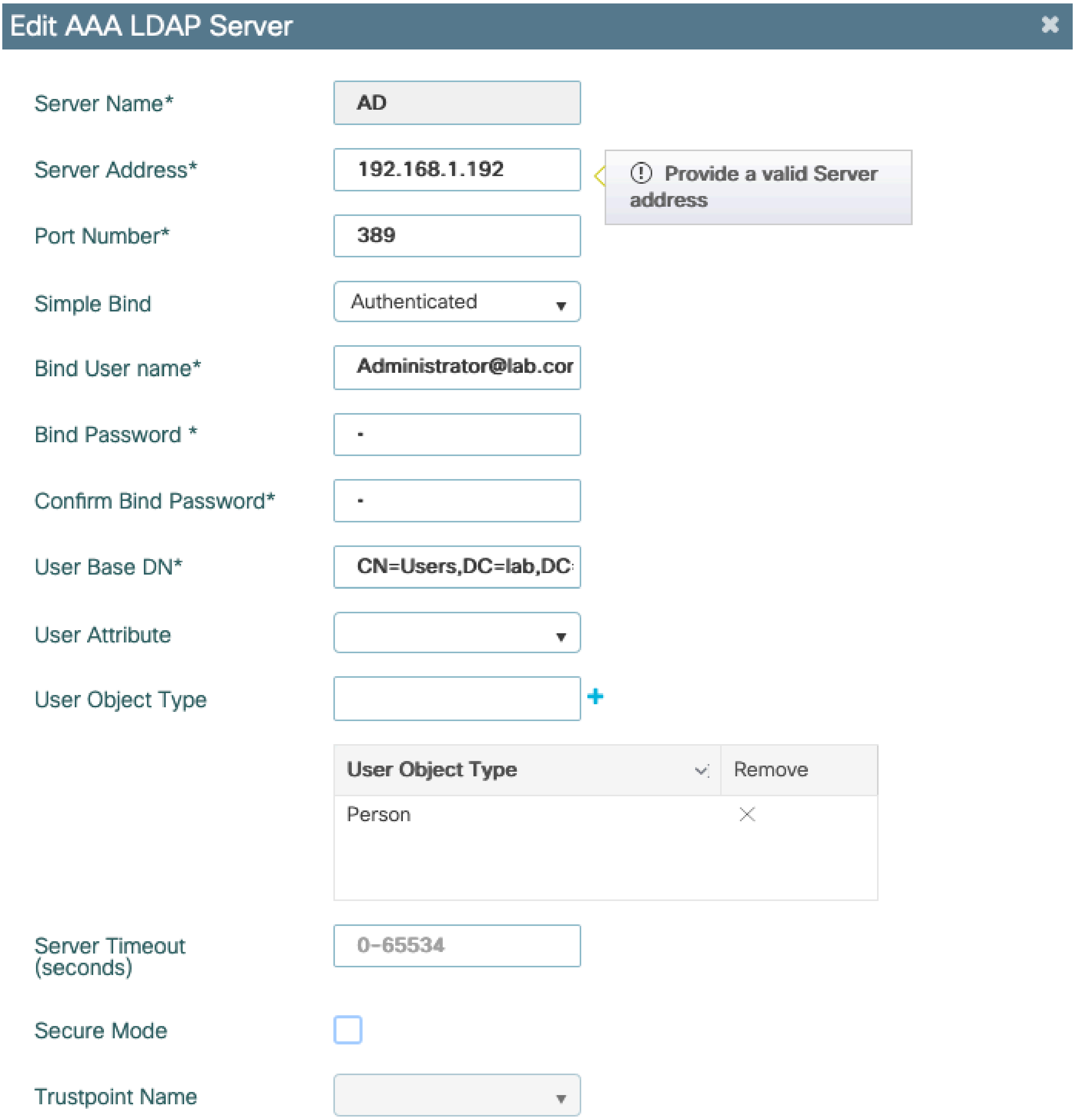
配置控制器

步骤1.配置LDAP服务器

导航到**Configuration > Security > AAA> Servers/Groups > LDAP**，然后点击**+ Add**



为LDAP服务器选择名称并填写详细信息。有关每个字段的说明，请参阅本文档的“了解LDAP服务器详细信息”部分。



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	×

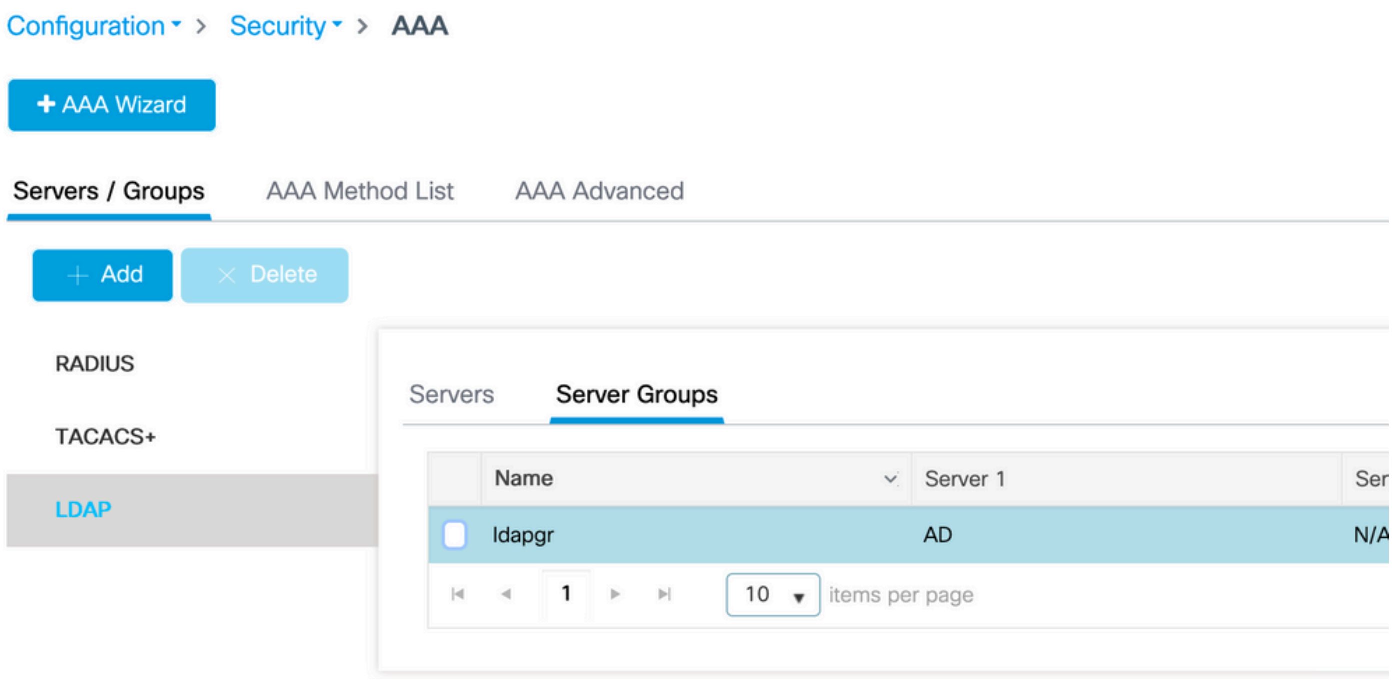
通过点击**Update**(更**新)保存并应用到设备**

CLI命令：

```
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
```

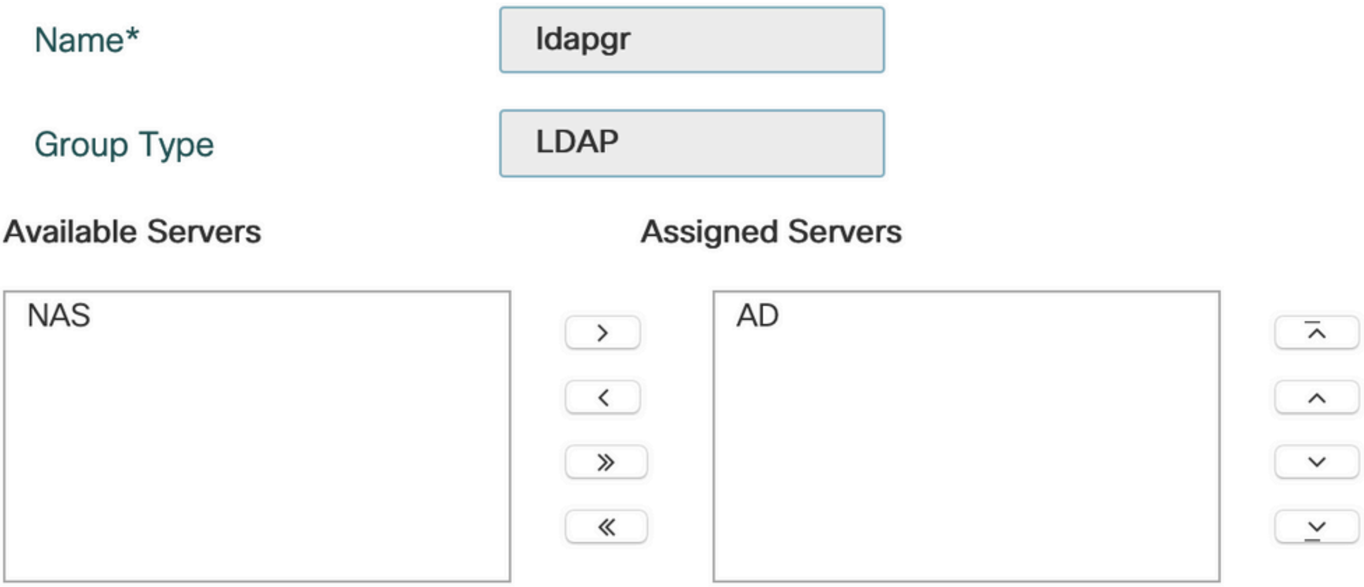
步骤2.配置LDAP服务器组。

导航到**配置>安全> AAA >服务器/组> LDAP >服务器组**，然后单击**+ADD**



	Name	Server 1	Ser
□	ldapgr	AD	N/A

输入名称并添加在上一步中配置的LDAP服务器。



Name*	ldapgr
Group Type	LDAP

Available Servers	Assigned Servers
NAS	AD

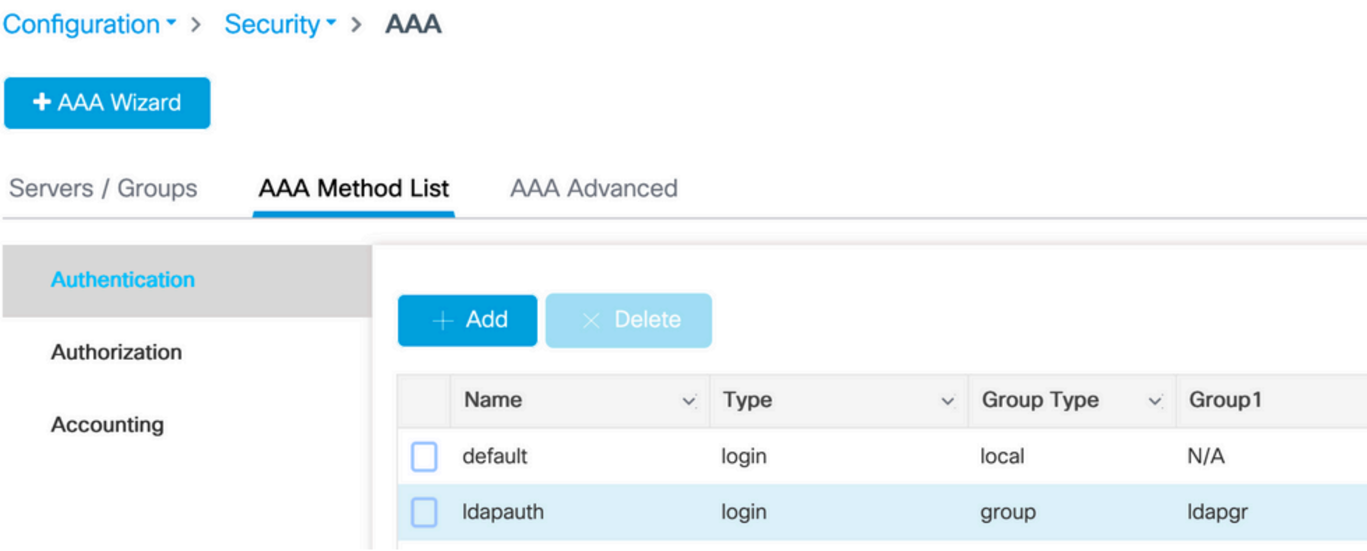
单击**Update and apply**进行保存。

CLI命令：

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

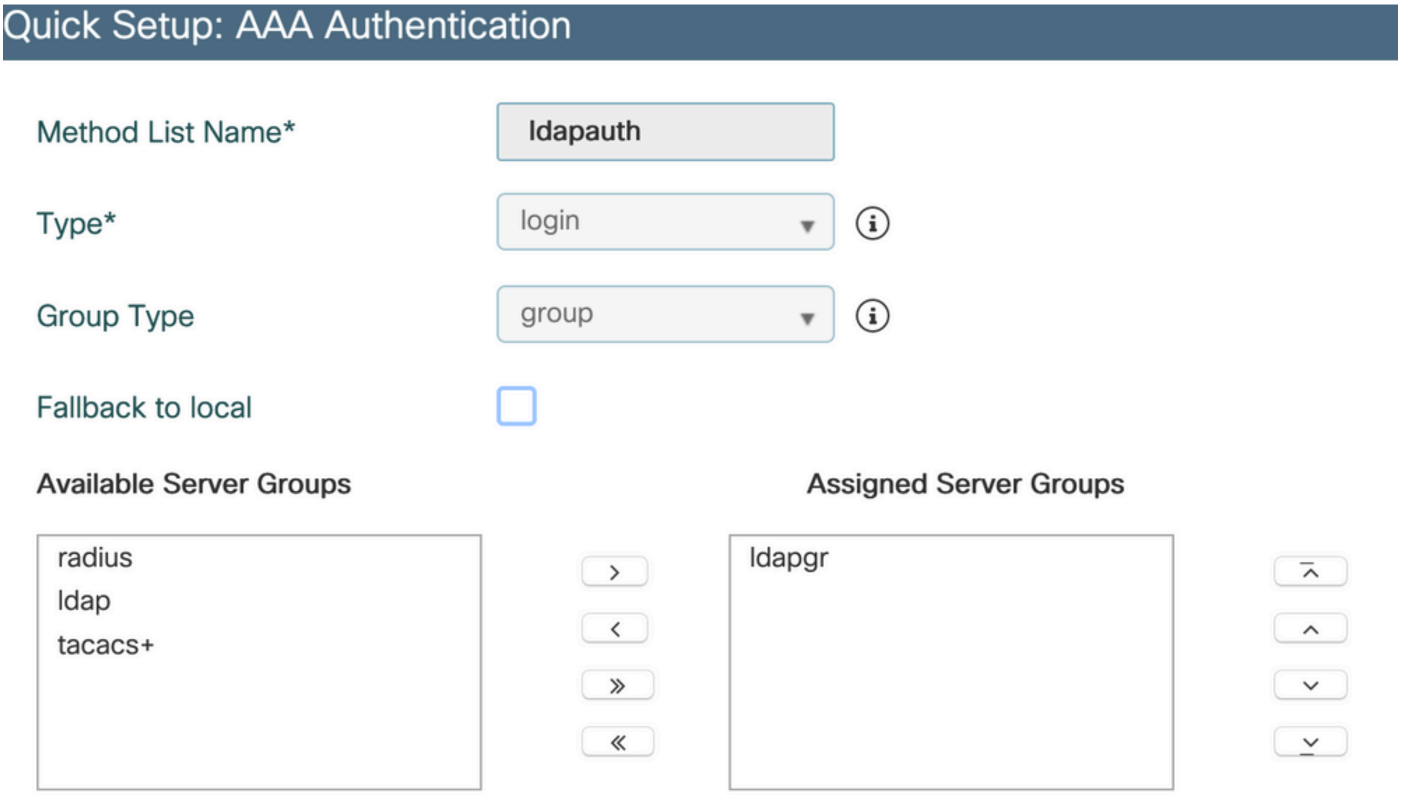
步骤3.配置AAA身份验证方法

导航到**Configuration > Security > AAA > AAA method List > Authentication**，然后单击**+Add**



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

输入名称，选择**Login**类型并指向之前配置的LDAP服务器组。



Quick Setup: AAA Authentication

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

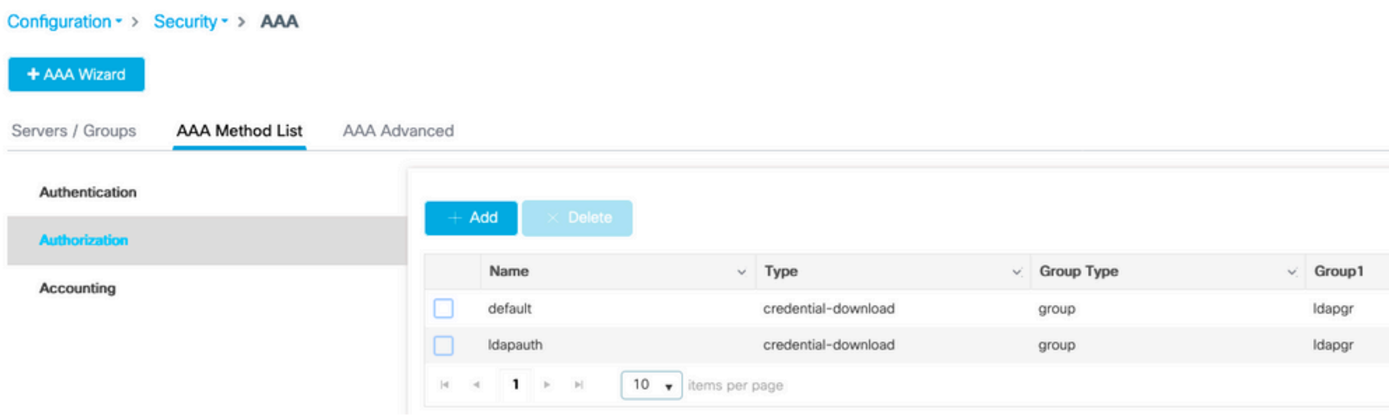
Available Server Groups	Assigned Server Groups
radius ldap tacacs+	ldapgr

CLI命令：

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

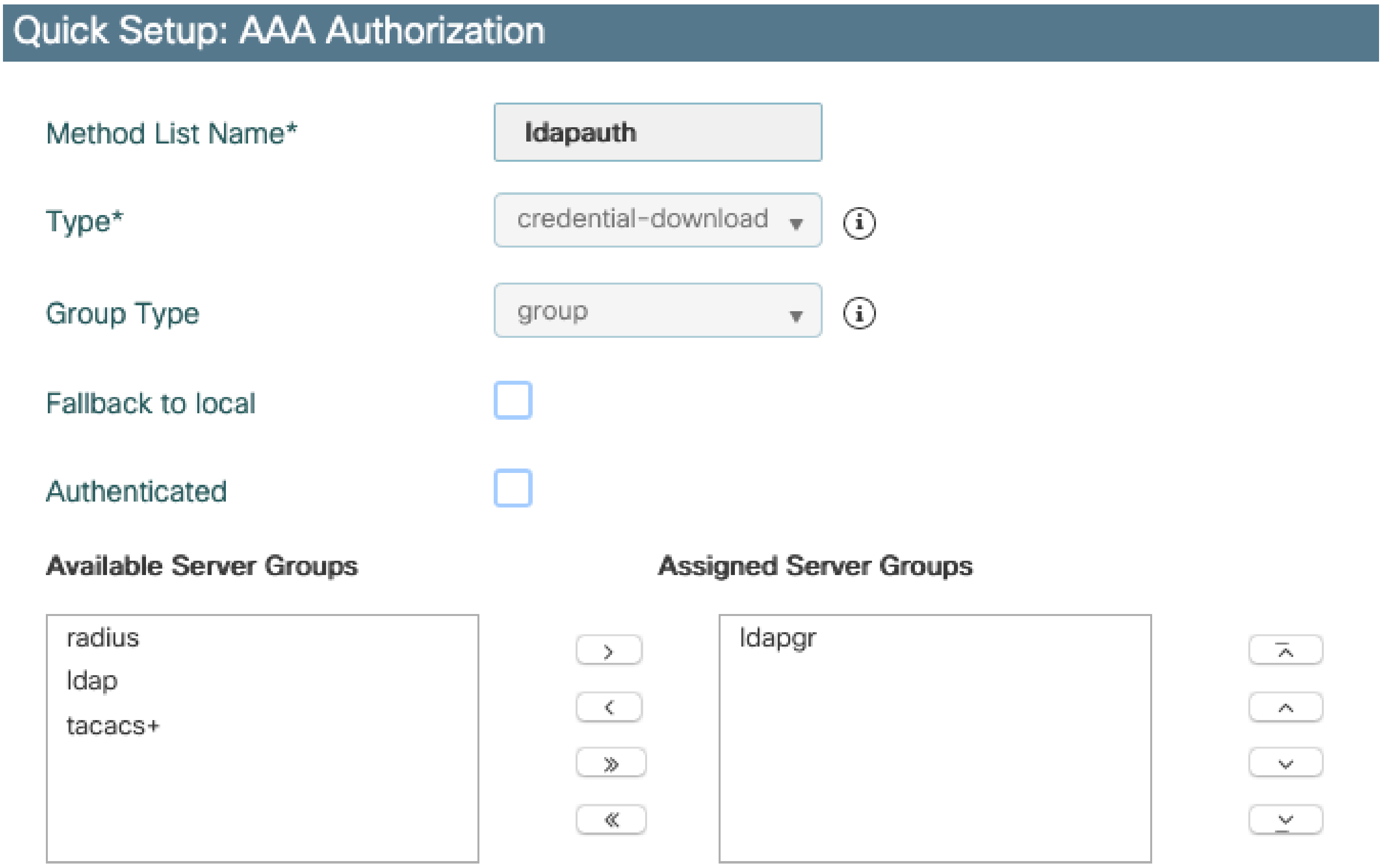
步骤4.配置AAA授权方法

导航到**Configuration > Security > AAA > AAA method list > Authorization，然**后点击**+Add**



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

创建所选名称的凭证下载类型规则，并将其指向之前创建的LDAP服务器组



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

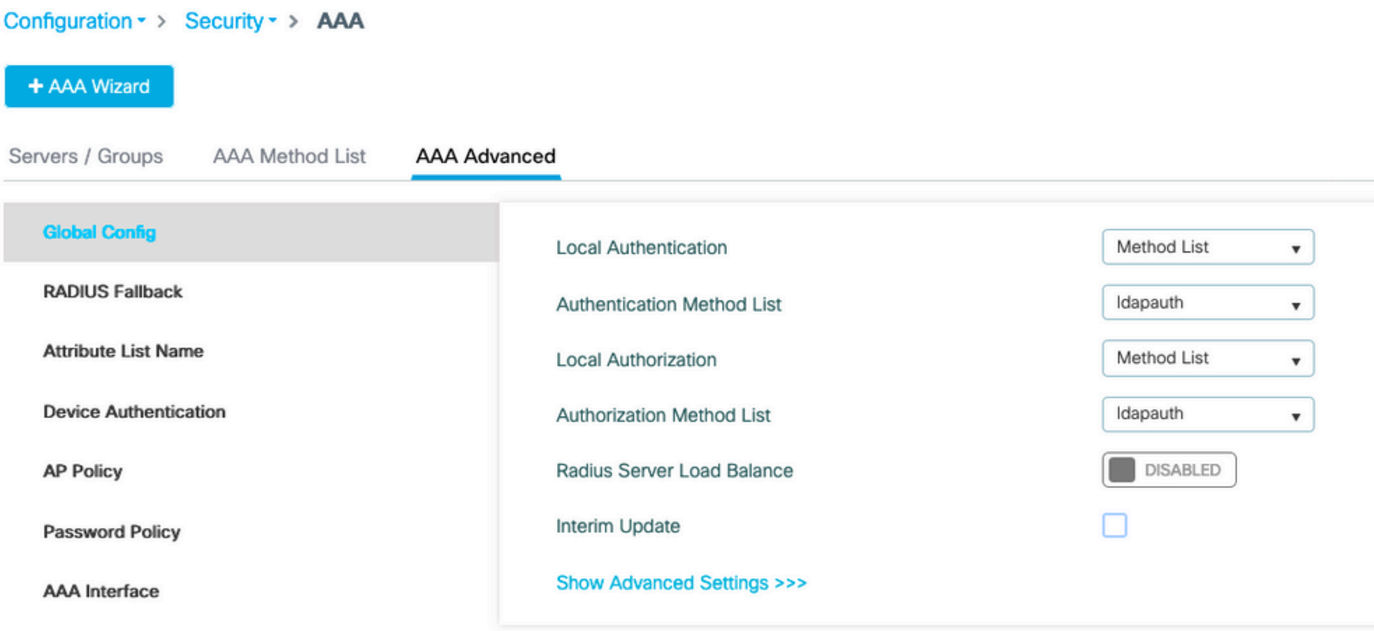
CLI命令：

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

步骤5.配置本地身份验证

导航到**Configuration > Security > AAA > AAA Advanced > Global Config**

将本地身份验证和本地授权设置为**Method List**，并选择之前配置的身份验证和授权方法。



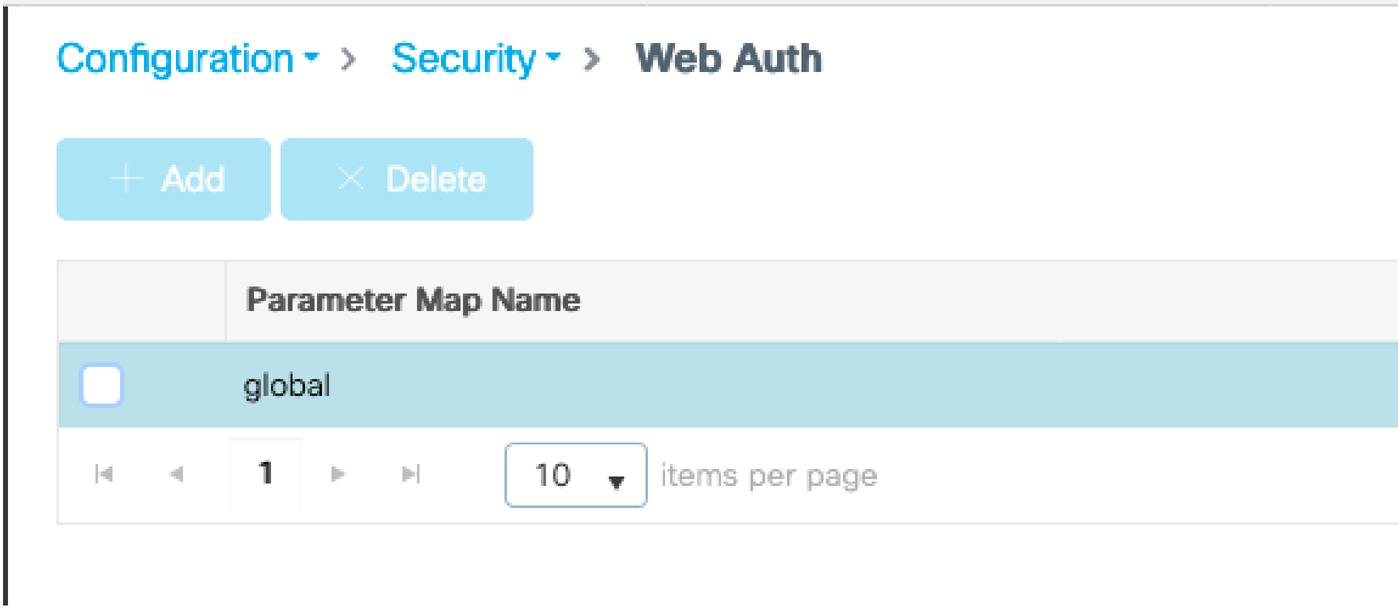
Local Authentication: Method List
Authentication Method List: ldapauth
Local Authorization: Method List
Authorization Method List: ldapauth
Radius Server Load Balance: DISABLED
Interim Update: □

CLI命令：

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

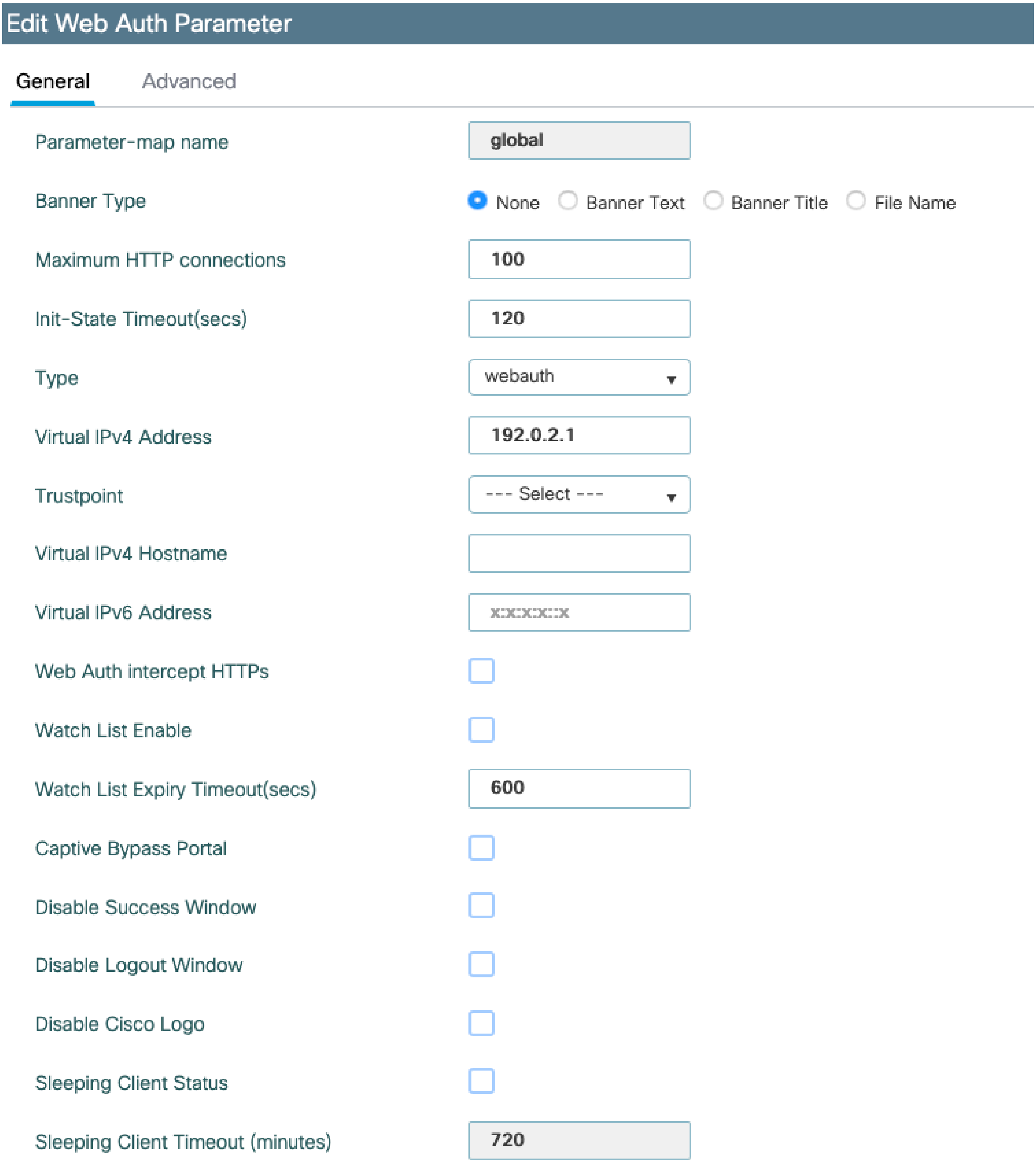
步骤6.配置webauth参数映射

导航到**Configuration > Security > Web Auth**，然后编辑**全局**映射



	Parameter Map Name
□	global

确保配置虚拟IPv4地址，例如192.0.2.1（该特定IP/子网保留用于不可路由的虚拟IP）。



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

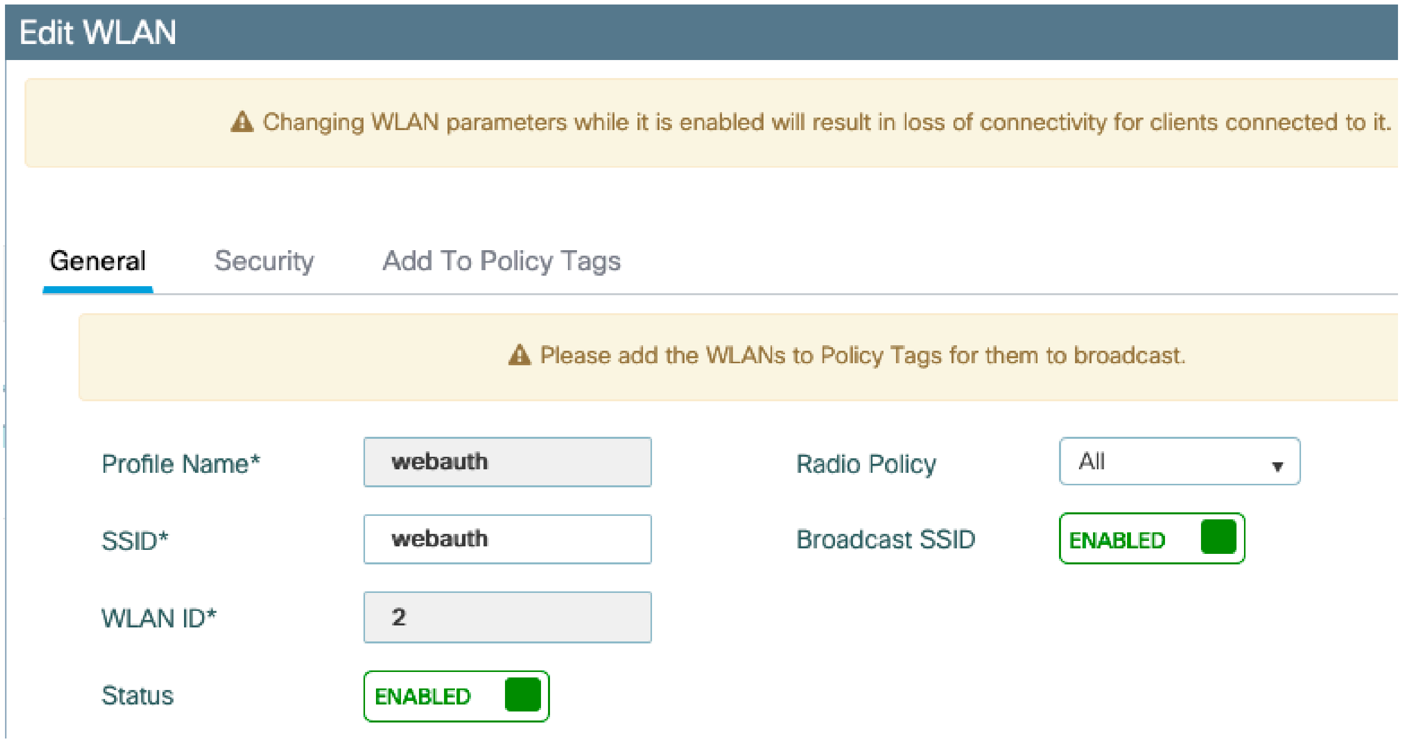
单击**Apply**保存。

CLI命令：

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

步骤7.配置webauth WLAN

导航到**配置> WLANs**，然后单击**+Add**



Edit WLAN

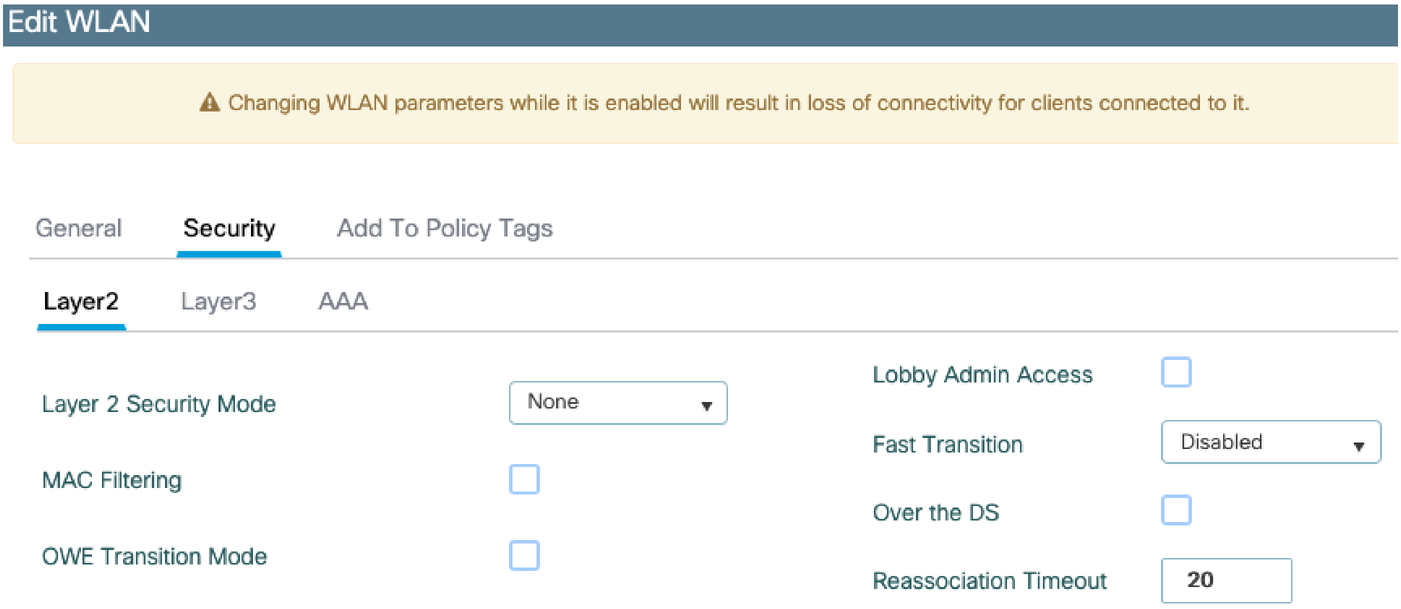
⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

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

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

配置名称，确保其处于启用状态，然后转到**安全**选项卡。

在**Layer 2**子选项卡中，确保没有安全性并且禁用了快速转换。

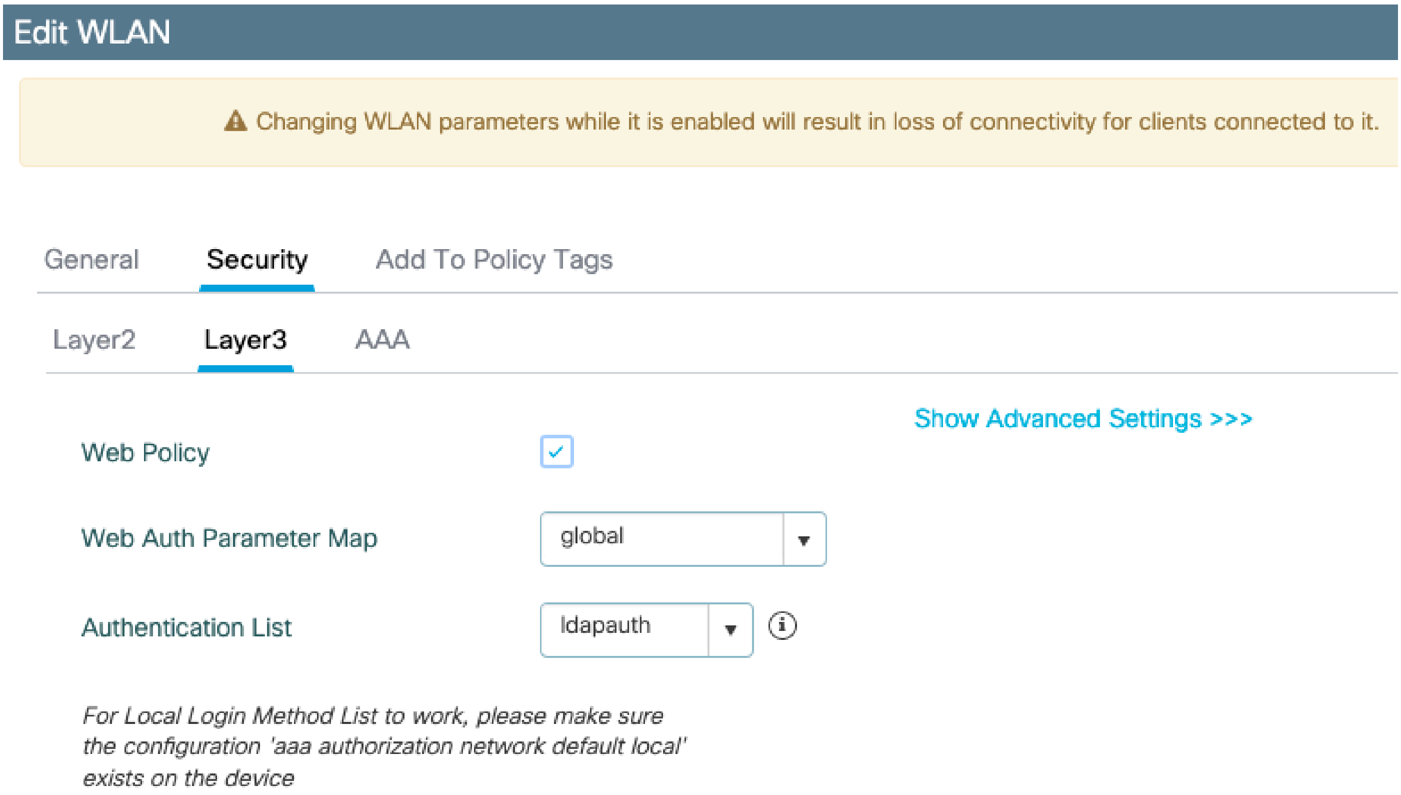


Edit WLAN

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

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

在**Layer3**选项卡中，启用**web policy**，将参数映射设置为**global**，并将身份验证列表设置为之前配置的aaa登录方法。


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

Web Policy ☑

Web Auth Parameter Map: global

Authentication List: ldapauth

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

通过点击应用保**存**

CLI命令：

```
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
```

步骤8.确保广播了SSID

导航到**Configuration > Tags**，确保SSID包含在当前由SSID提供服务的策略配置文件中（如果尚未配置标记，则为全新配置提供default-policy-tag）。 默认情况下，default-policy-tag不会广播您创建的新SSID，直到您手动包含这些SSID。

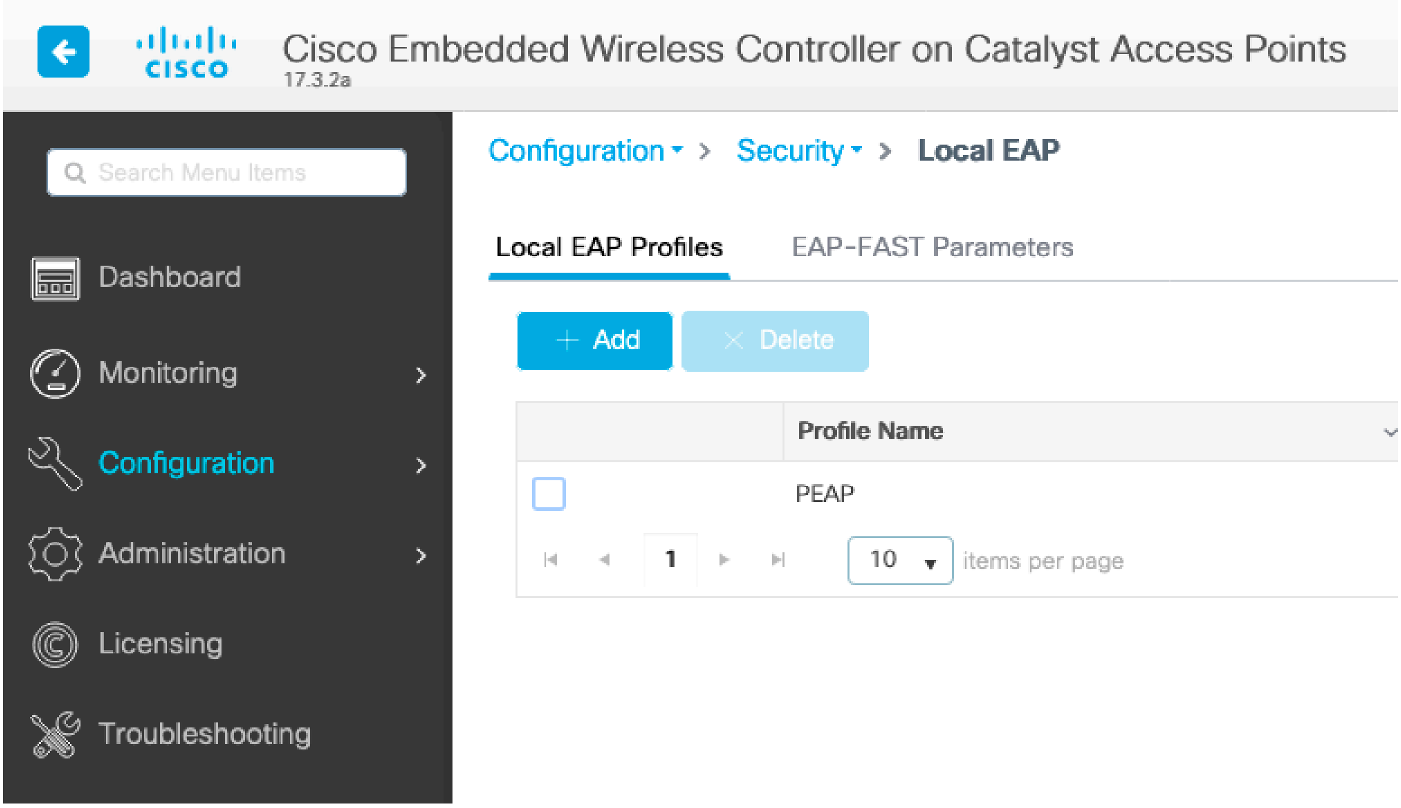
本文不涉及策略配置文件的配置，并假设您熟悉该部分配置。

使用dot1x SSID配置LDAP（使用本地EAP）

在9800上为802.1X SSID配置LDAP通常还需要配置本地EAP。如果您要使用RADIUS，则您的RADIUS服务器将与LDAP数据库建立连接，这不在本文的讨论范围之内。在尝试此配置之前，建议首先在WLC上配置本地用户来配置本地EAP，本文结尾的参考一节中提供了一个配置示例。完成后，您可以尝试将用户数据库移至LDAP。

步骤1.配置本地EAP配置文件

导航到**Configuration > Local EAP**，然后单击**+Add**



Cisco Embedded Wireless Controller on Catalyst Access Points
17.3.2a

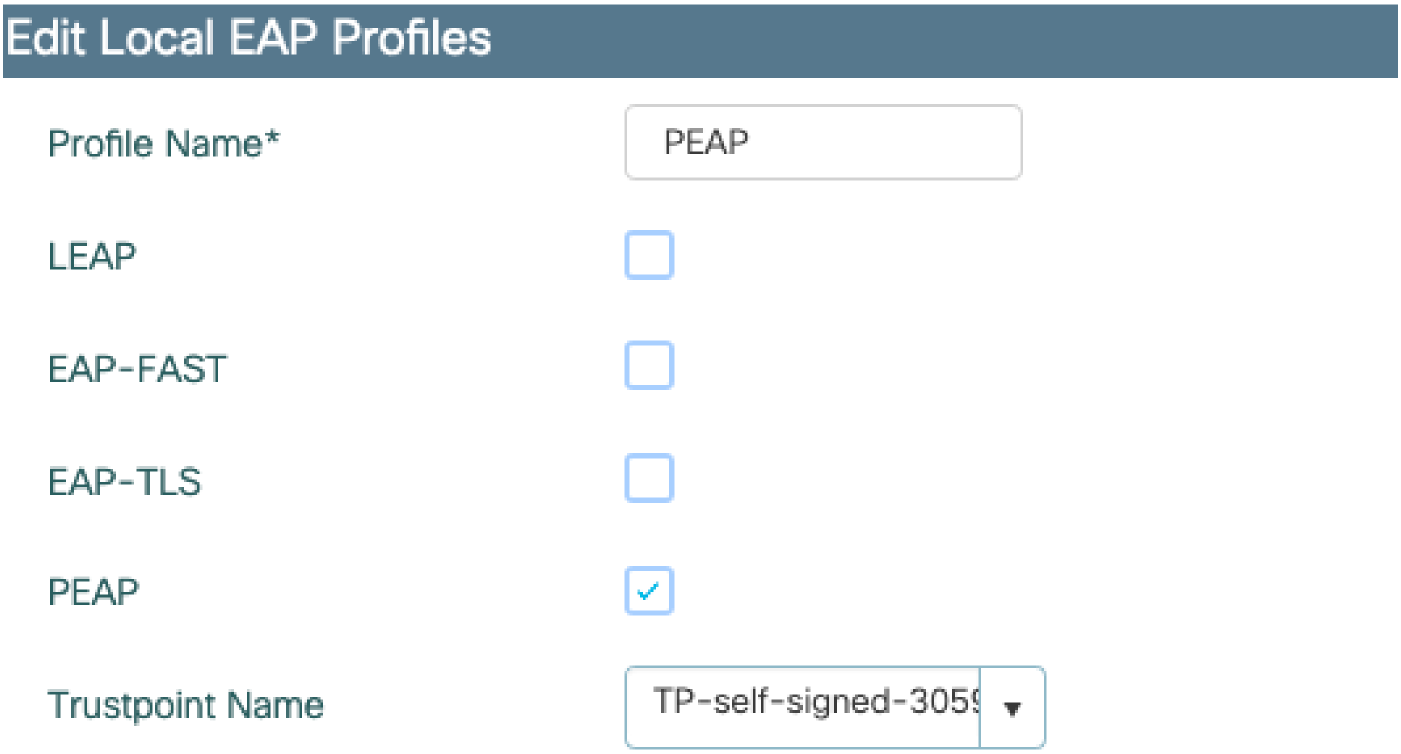
Configuration > Security > Local EAP

Local EAP Profiles | EAP-FAST Parameters

	Profile Name
□	PEAP

1 | 10 items per page

为您的配置文件选择任意名称。至少启用PEAP并选择信任点名称。默认情况下，您的WLC仅具有自签名证书，因此您选择哪一个证书并不重要（通常TP-self-signed-xxxx是此用途的最佳证书），但是由于新的智能手机OS版本信任越来越少的自签名证书，请考虑安装受信任的公共签名证书。



Edit Local EAP Profiles

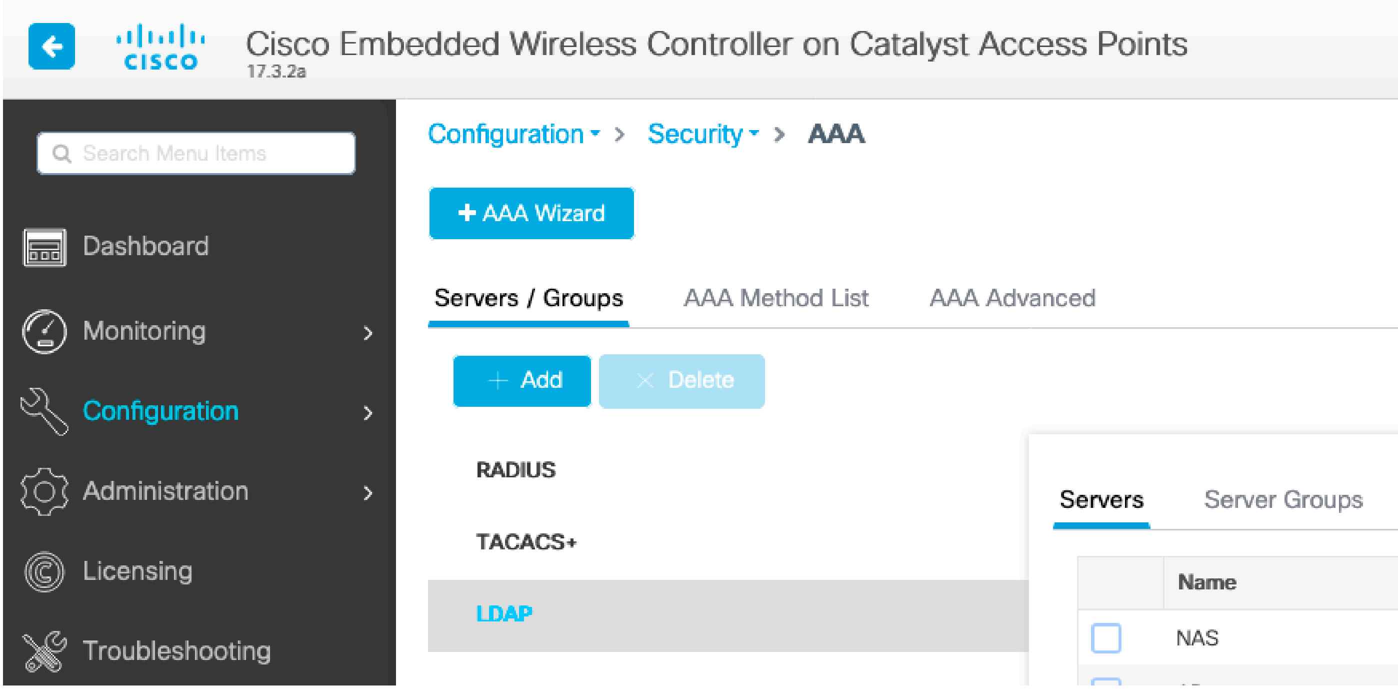
Profile Name*	PEAP
LEAP	□
EAP-FAST	□
EAP-TLS	□
PEAP	☑
Trustpoint Name	TP-self-signed-305 ▾

CLI命令：

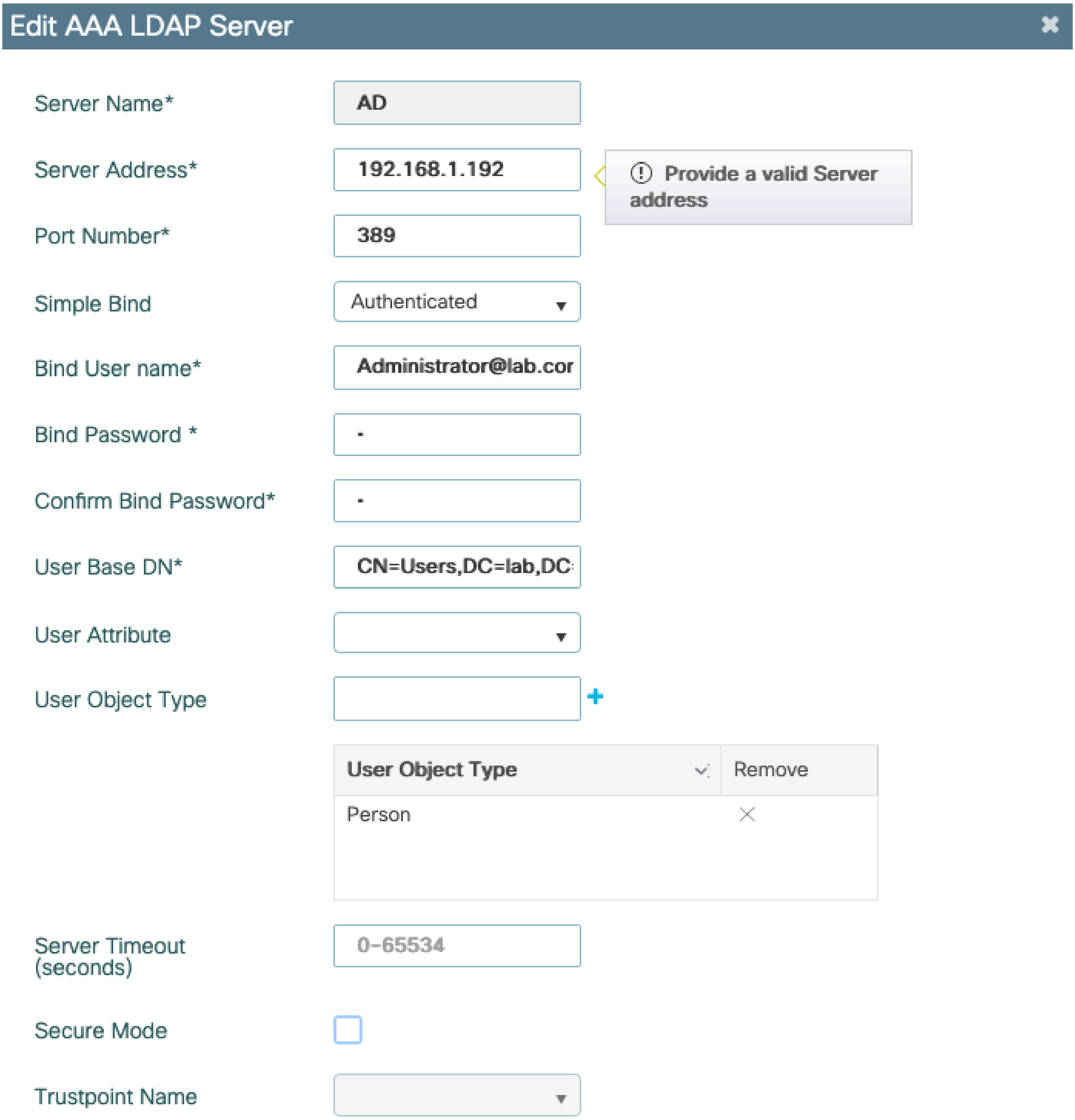
```
eap profile PEAP method peap pki-trustpoint TP-self-signed-3059261382
```

步骤2.配置LDAP服务器

导航到**Configuration > Security > AAA> Servers/Groups > LDAP**，然后点击**+ Add**



为LDAP服务器选择名称并填写详细信息。有关每个字段的说明，请参阅本文档的“了解LDAP服务器详细信息”部分。



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

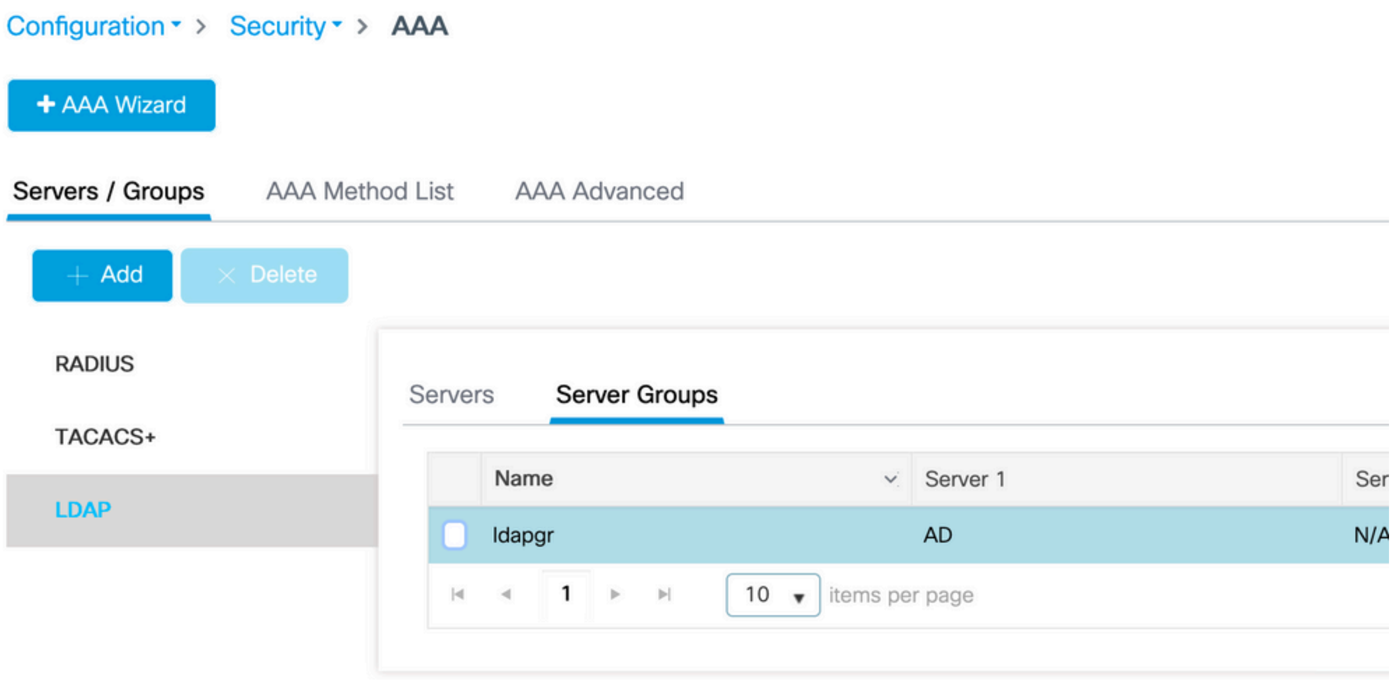
User Object Type	Remove
Person	×

通过点击**Update(**更**新)保存并应用到设备**

```
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
```

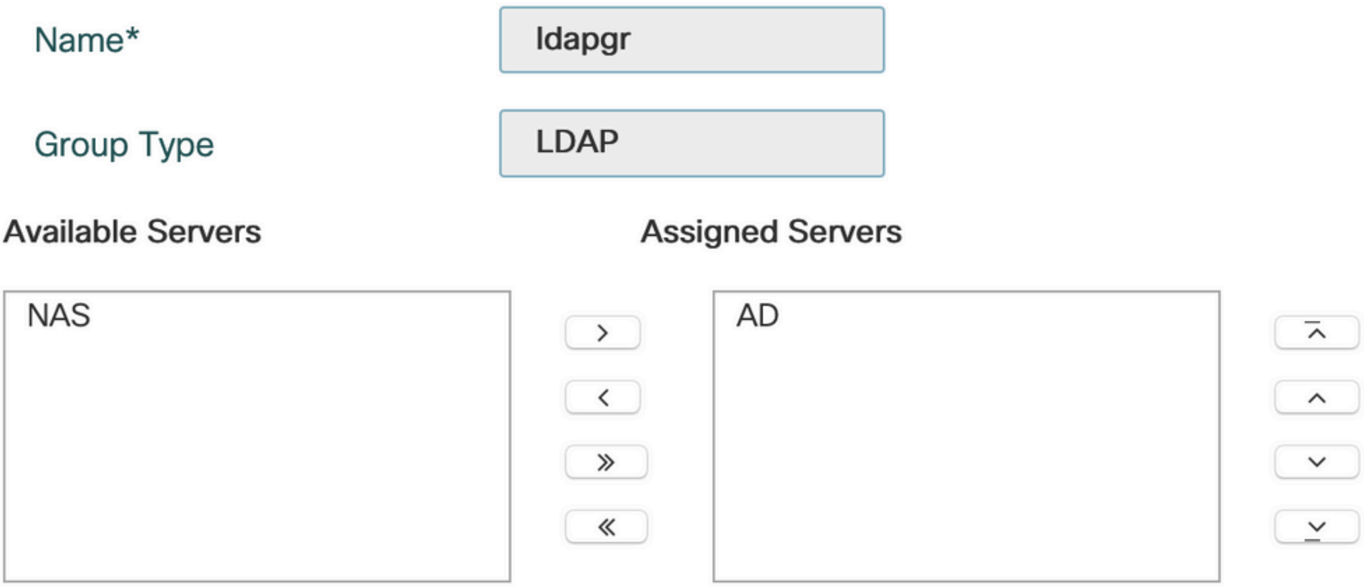
步骤3.配置LDAP服务器组。

导航到**配置>安全> AAA >服务器/组> LDAP >服务器组**，然后单击**+ADD**



	Name	Server 1	Ser
□	ldapgr	AD	N/A

输入名称并添加在上一步中配置的LDAP服务器。



Name*: ldapgr

Group Type: LDAP

Available Servers: NAS

Assigned Servers: AD

单击**Update and apply**进行保存。

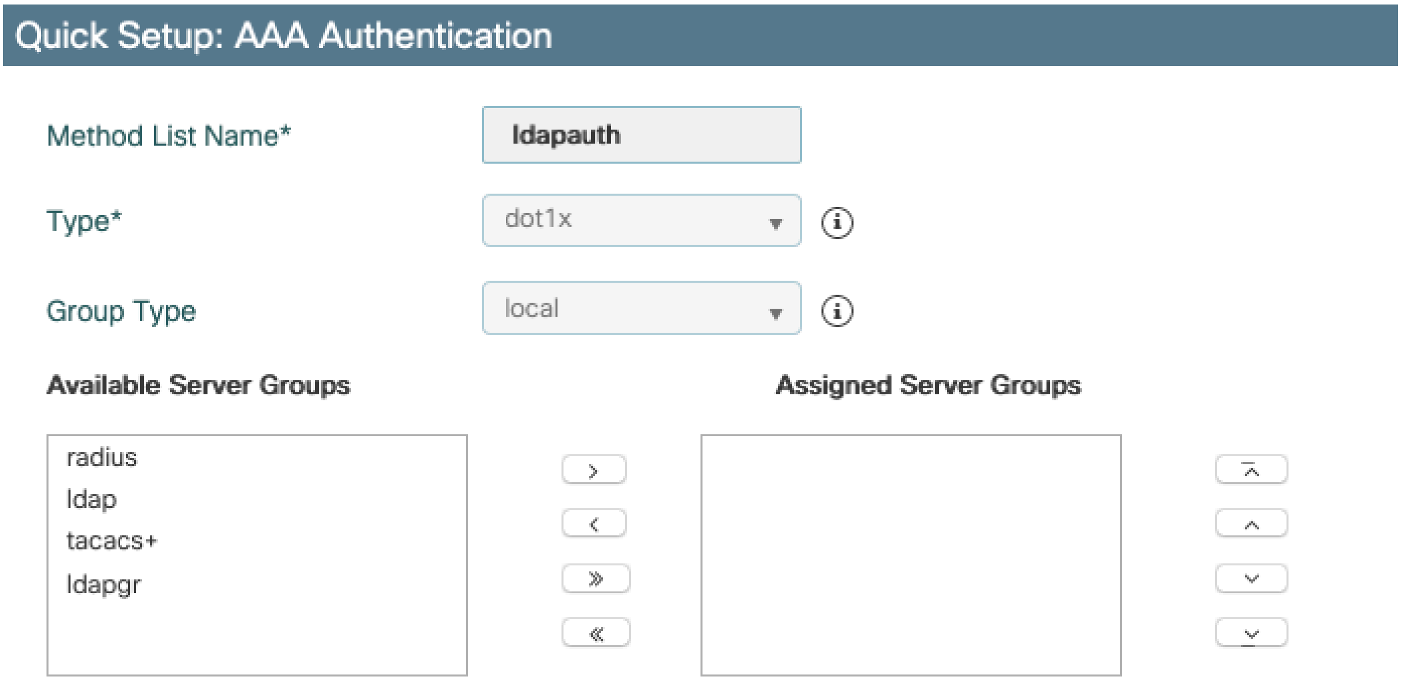
CLI命令：

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

步骤4.配置AAA身份验证方法

导航到**Configuration > Security > AAA > AAA Method List > Authentication**，然后单击**+Add**

配置**dot1x**类型身份验证方法，并将其指向仅本地。指向LDAP服务器组很有吸引力，但此处充当802.1X身份验证器的是WLC本身（虽然用户数据库位于LDAP上，但这是授权方法作业）。



Quick Setup: AAA Authentication

Method List Name* ldapauth

Type* dot1x

Group Type local

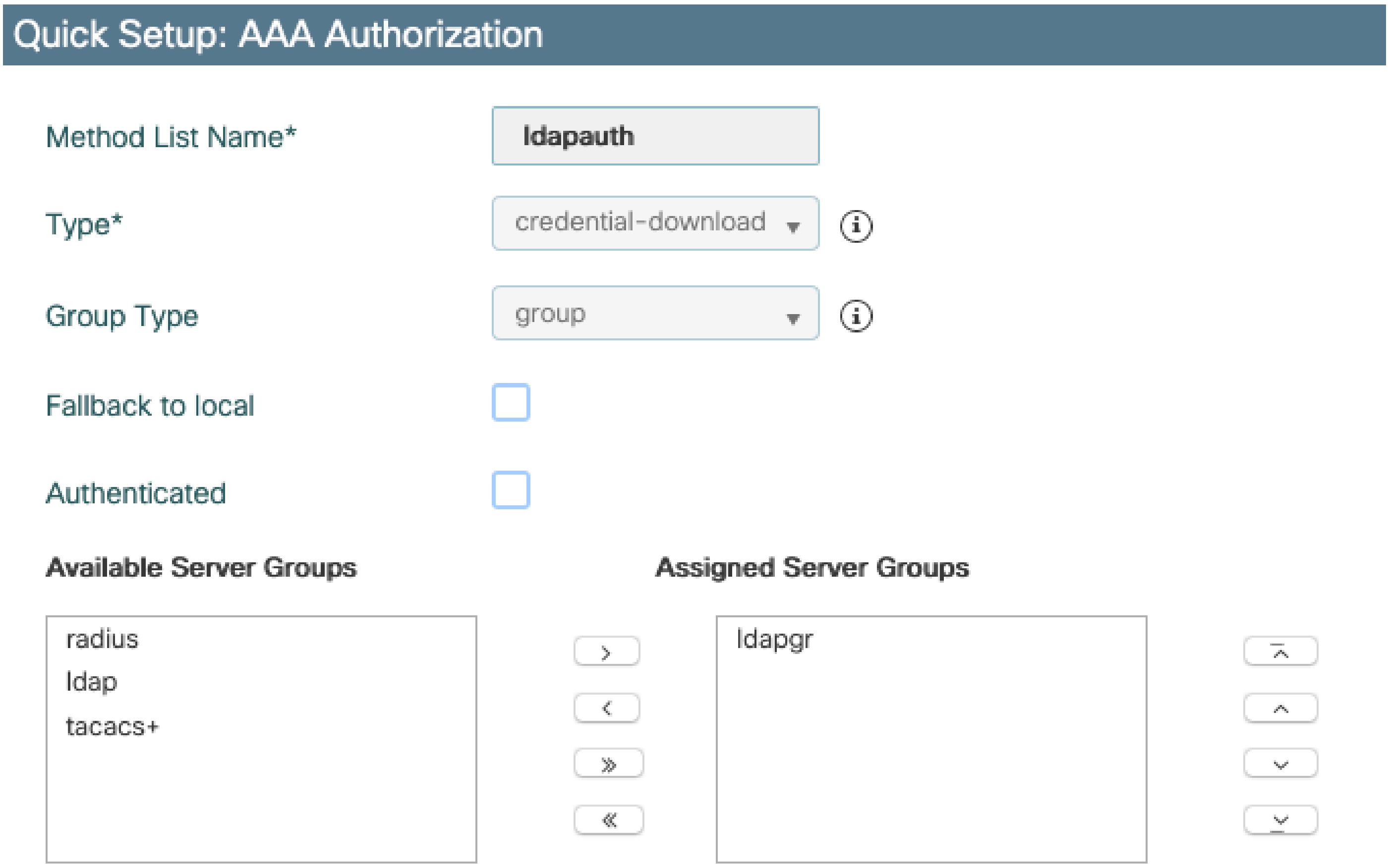
CLI命令：

```
aaa authentication dot1x ldapauth local
```

步骤5.配置AAA授权方法

导航到**Configuration > Security > AAA > AAA Method List > Authorization**，然后单击**+Add**

创建**credential-download**类型的授权方法，并使其指向LDAP组。



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

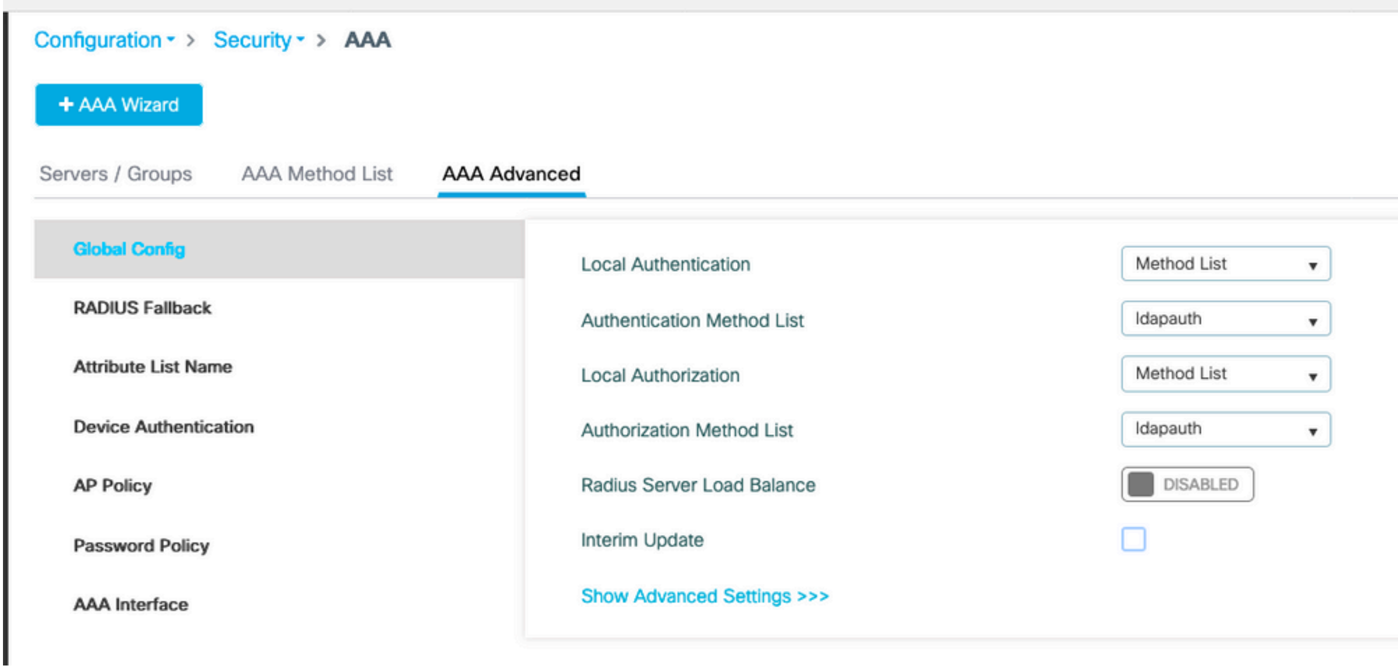
CLI命令：

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

步骤6.配置本地身份验证详细信息

导航到**Configuration > Security > AAA > AAA Method List > AAA Advanced**

选择**Method List**进行身份验证和授权，并选择本地指向的dot1x身份验证方法和指向LDAP的凭证下载授权方法


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: □

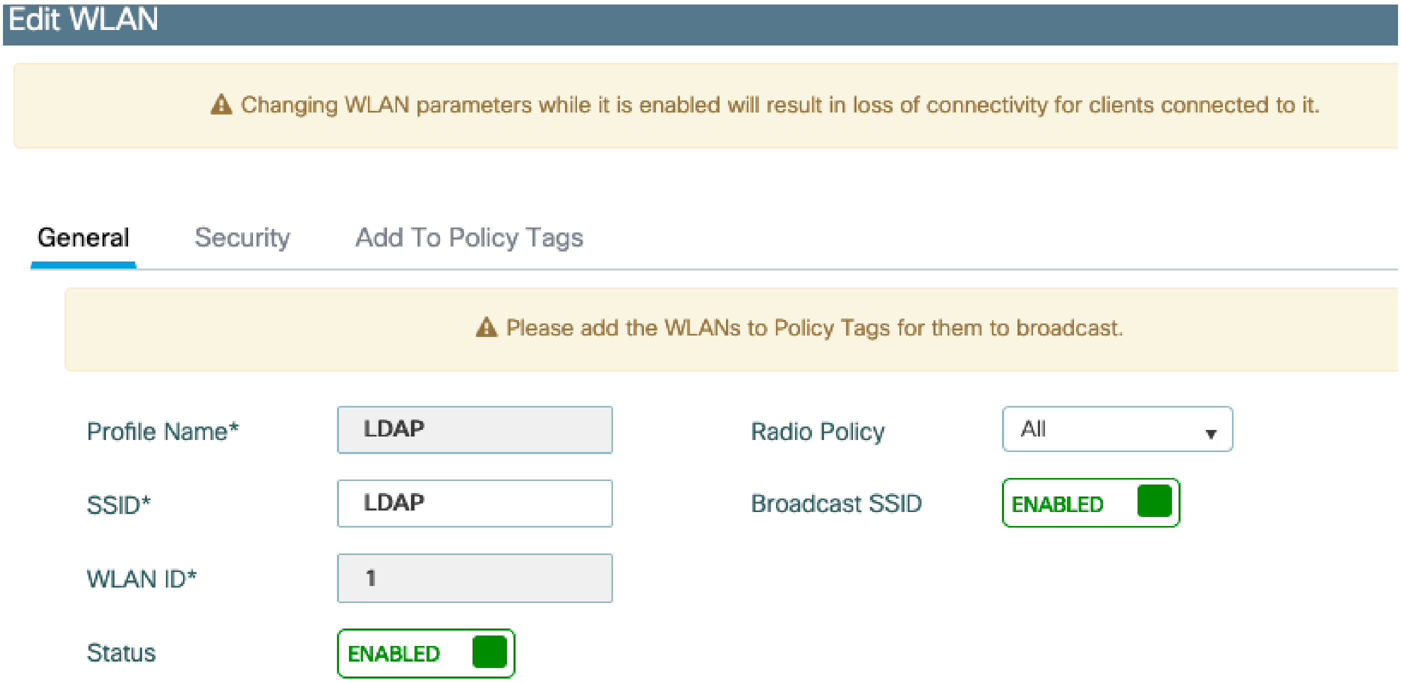
CLI命令：

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

步骤7.配置dot1x WLAN

导航到**配置> WLAN**，然后单击**+添加**

选择配置文件和SSID名称，并确保已启用。


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

SSID*: LDAP

WLAN ID*: 1

Status: ENABLED

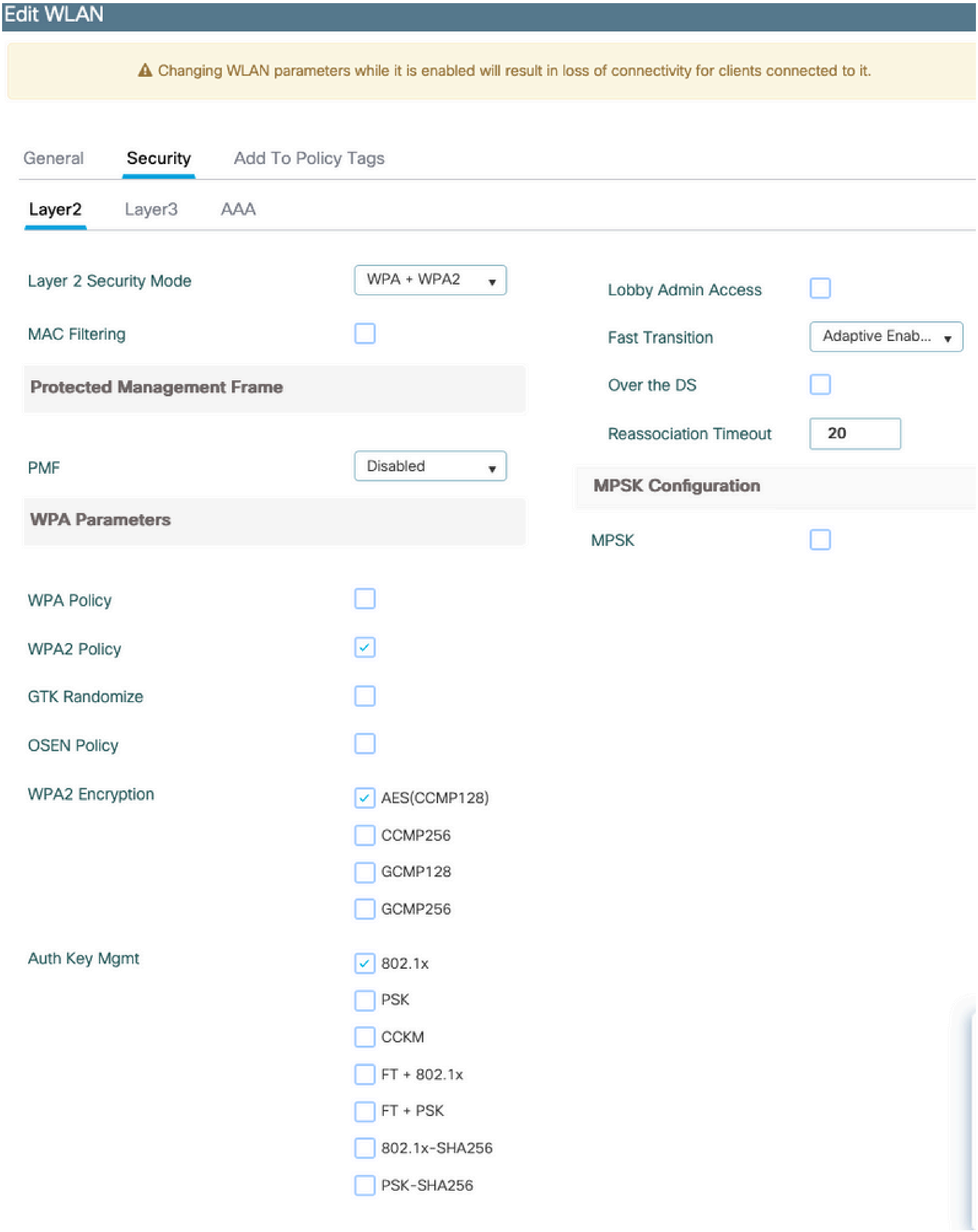
Radio Policy: All

Broadcast SSID: ENABLED

转到Layer 2 **security**选项卡。

选择WPA+WPA2作为**第2层安全模式**

确保WPA2和AES在WPA参数**中启**用，并**启用802.1X**



Edit WLAN

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

Layer 2 Security Mode: WPA + WPA2 ▾

MAC Filtering □

Protected Management Frame

PMF: Disabled ▾

WPA Parameters

WPA Policy □

WPA2 Policy ☑

GTK Randomize □

OSEN Policy □

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

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

Lobby Admin Access □

Fast Transition: Adaptive Enab... ▾

Over the DS □

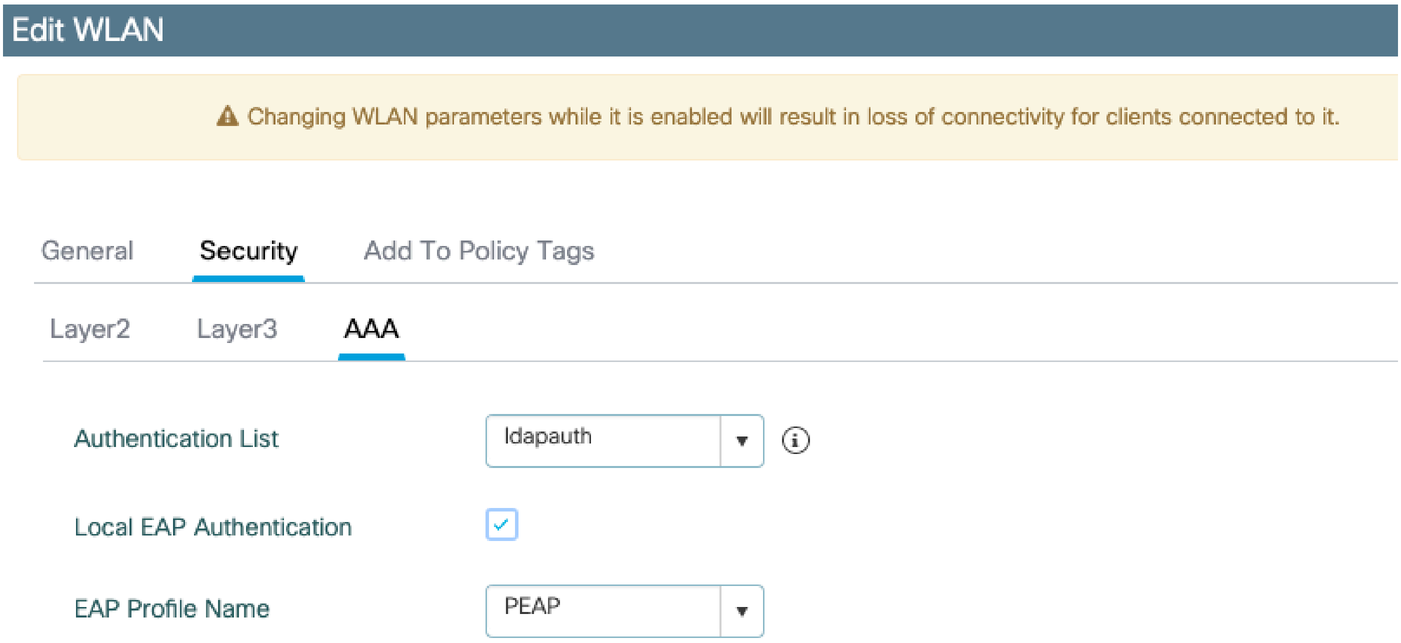
Reassociation Timeout: 20

MPSK Configuration

MPSK □

转到**AAA**子选项卡。

选择之前创建的dot1x身份验证方法，启用本地EAP身份验证并选择第一步中配置的EAP配置文件。


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

通过点击应用保存

CLI命令：

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

步骤8.检验是否已广播WLAN

导航到**Configuration > Tags**，确保SSID包含在当前由SSID提供服务的策略配置文件中（如果尚未配置标记，则为全新配置提供default-policy-tag）。 默认情况下，default-policy-tag不会广播您创建的新SSID，直到您手动包含这些SSID。

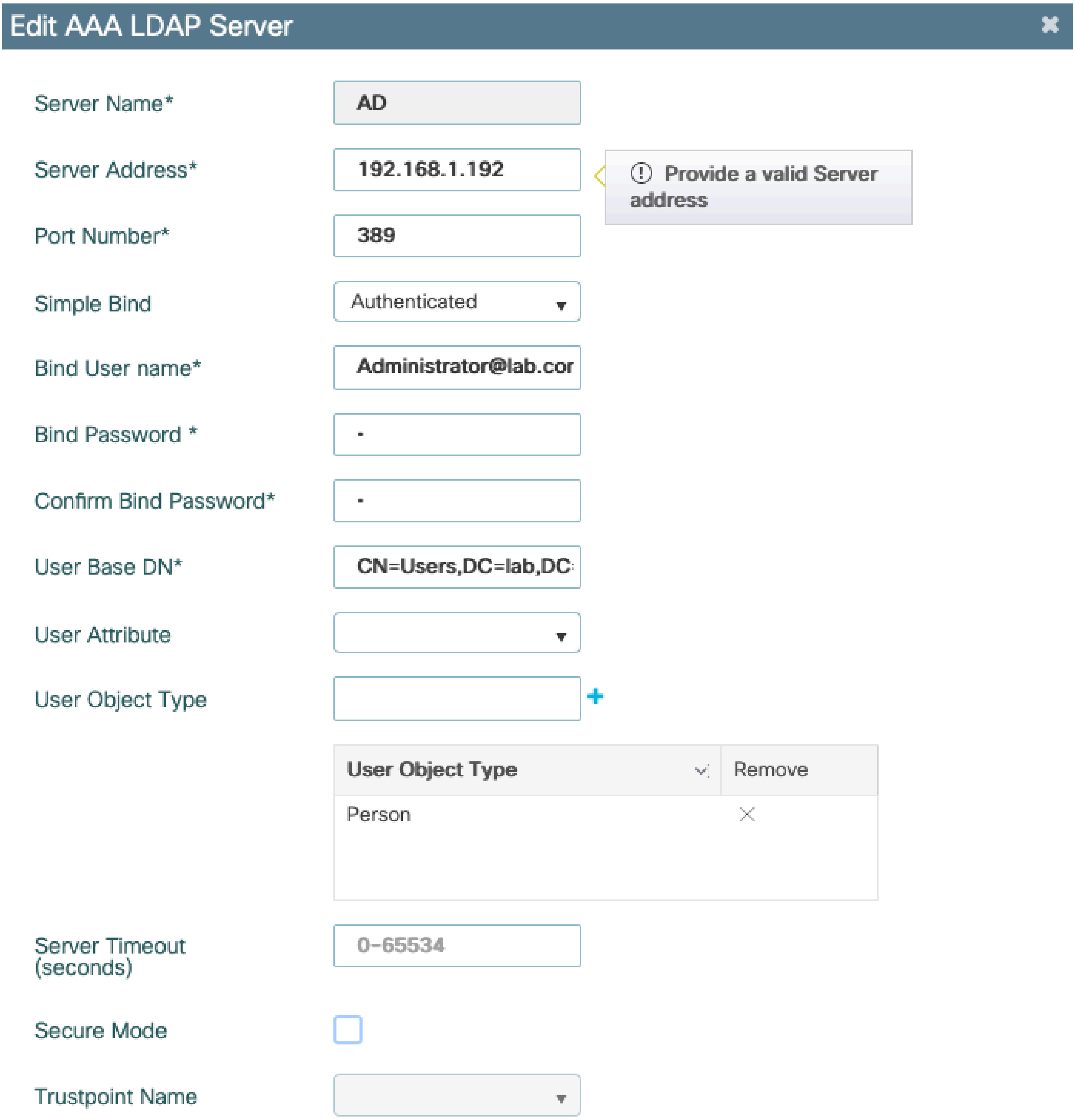
本文不涉及策略配置文件的配置，并假设您熟悉该部分配置。

如果使用Active Directory，则必须配置AD服务器以发送属性“userPassword”。 此属性需要发送到WLC。这是因为WLC执行验证，而不是AD服务器。您还可能遇到使用PEAP-mschapv2方法进行身份验证的问题，因为密码永远不会以明文形式发送，因此无法使用LDAP数据库进行检查，只有PEAP-GTC方法适用于某些LDAP数据库。

了解LDAP服务器详细信息

了解9800 Web UI上的字段

以下是一个非常基本的Active Directory的示例，它用作9800上配置的LDAP服务器



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	×

名称和IP可能是不言自明的。

端口：389是LDAP的默认端口，但您的服务器可以使用其他端口。

简单绑定：如今，很少有支持未经身份验证绑定的LDAP数据库（这意味着任何人都可以在它上进行LDAP搜索，而无需任何身份验证形式）。 经过身份验证的简单绑定是最常见的身份验证类型以及Active Directory默认允许的内容。您可以输入管理员帐户名和密码，以便能够在用户数据库中执行搜索。

绑定用户名：您需要在Active Directory中指向具有管理员权限的用户名。AD允许使用“user@domain”格式，而许多其他LDAP数据库期望用户名使用“CN=xxx，DC=xxx”格式。本文后面提供了另一个LDAP数据库而不是AD的示例。

绑定密码：输入管理员用户名之前输入的密码。

用户群DN:在此处输入“搜索根”，即LDAP树中开始搜索的位置。在本示例中，我们所有使用都在“Users”组下，其DN为“CN=Users，DC=lab，DC=com”(因为示例LDAP域为lab.com)。 本节后面提供了如何查找此用户基础DN的示例。

用户属性：可以将此字段留空，或指向指示哪个LDAP字段计为LDAP数据库用户名的LDAP属性映射。但是，由于思科漏洞ID CSCvv11813 ,WLC尝试使用CN字段进行身份验证，无论什么内容。

用户对象类型：这决定了被视为用户的对象的类型。通常为“人”。 如果您有AD数据库并验证计算机帐户，则可能是“计算机”，但LDAP同样提供了大量自定义功能。

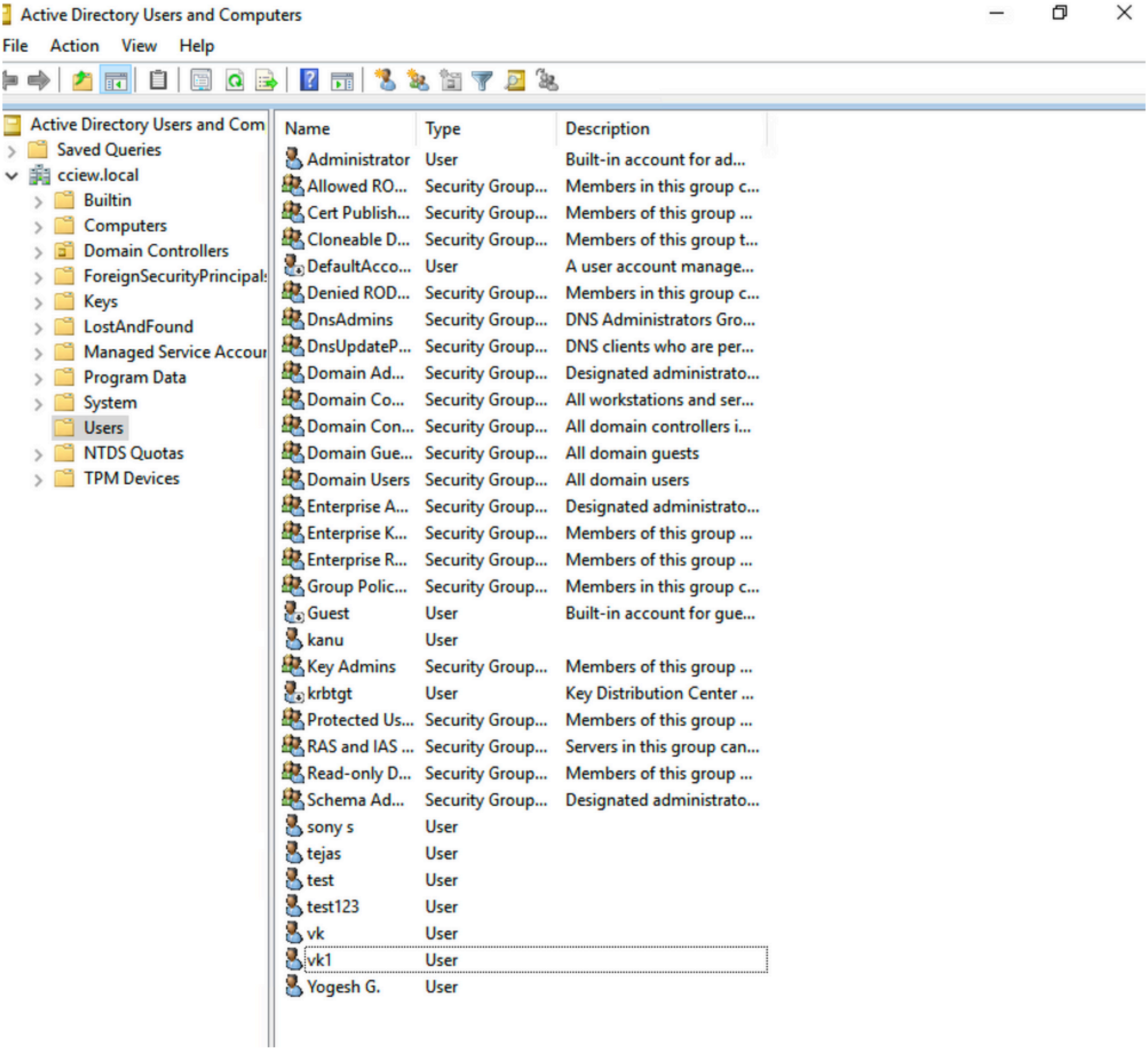
安全模式启用基于TLS的安全LDAP，并要求您在9800上选择信任点以使用证书进行TLS加密。

具有sAMAaccountName属性的LDAP 802.1x身份验证。

17.6.1版本中引入了此增强功能。

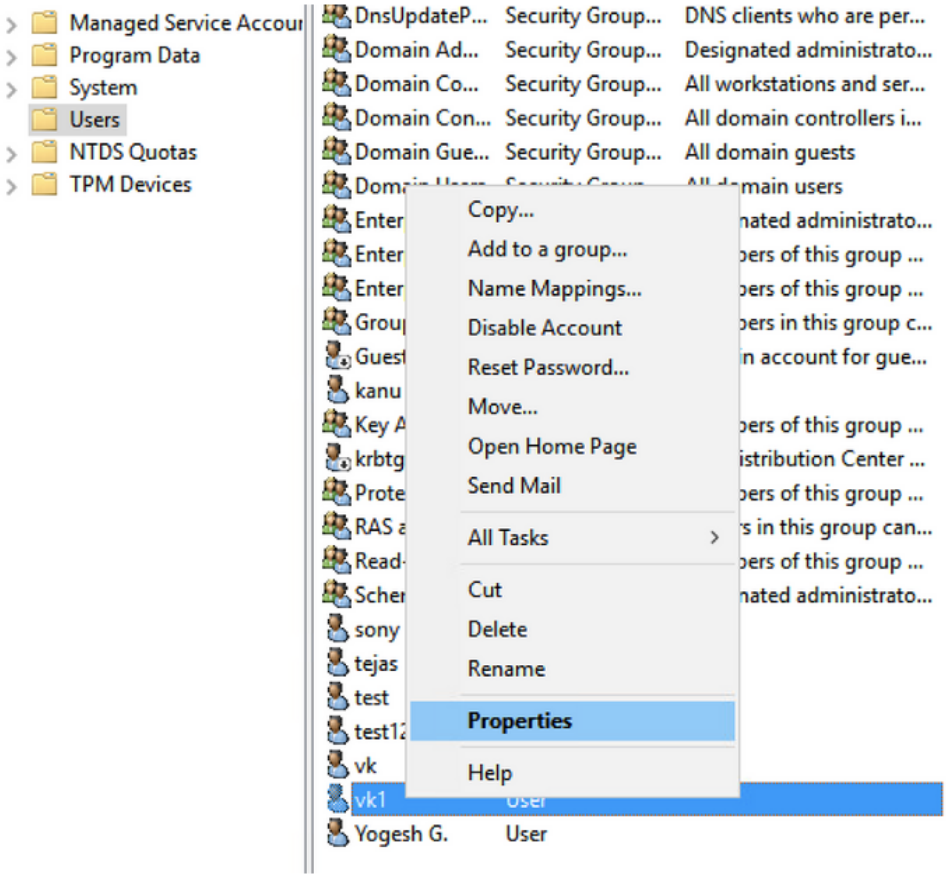
配置用户的“userPassword”属性。

步骤1.在Windows服务器上，导航到ActiveDirectory用户和计算机

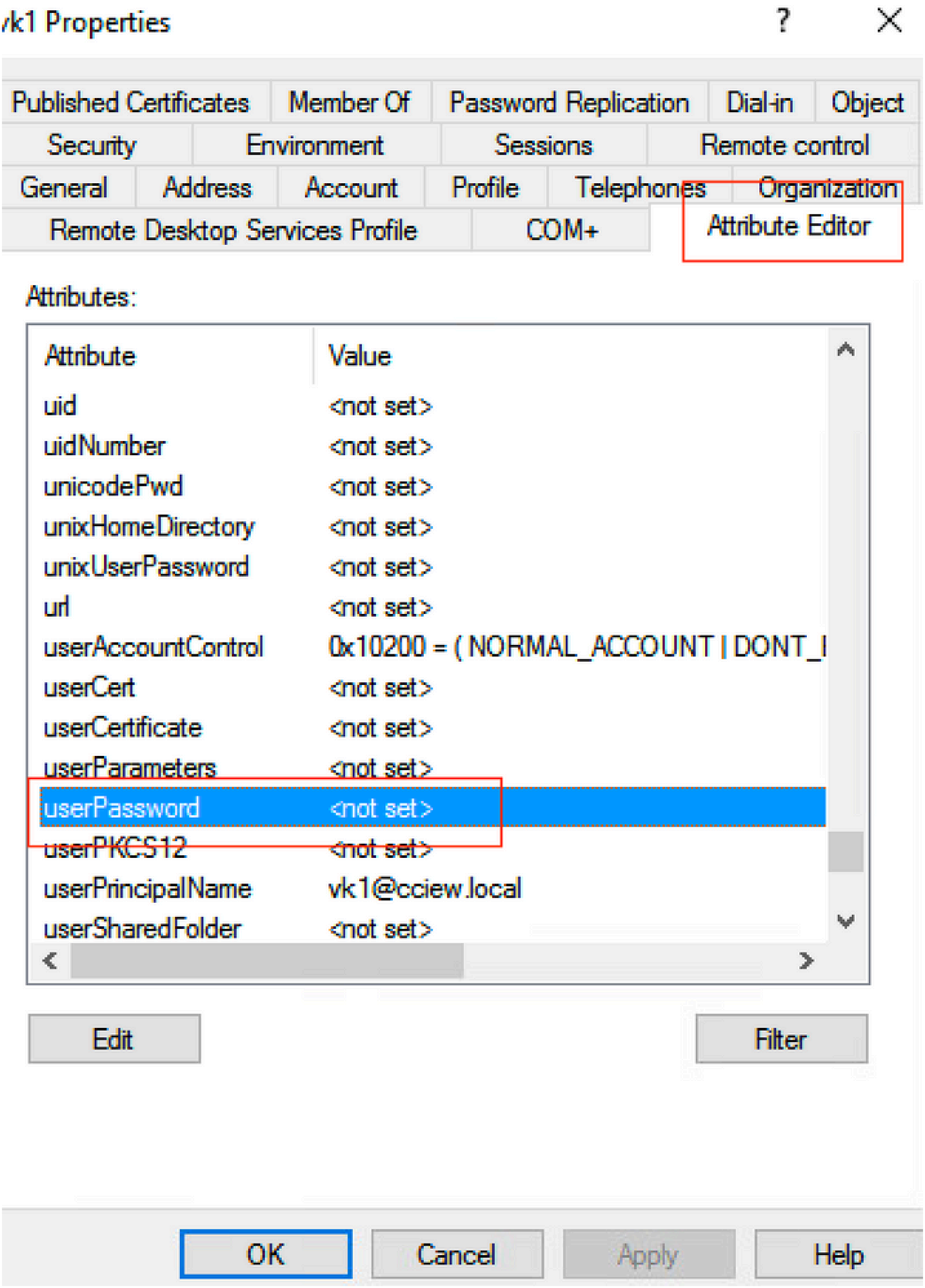


Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...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

步骤2.右键单击各自的用户名并选择属性

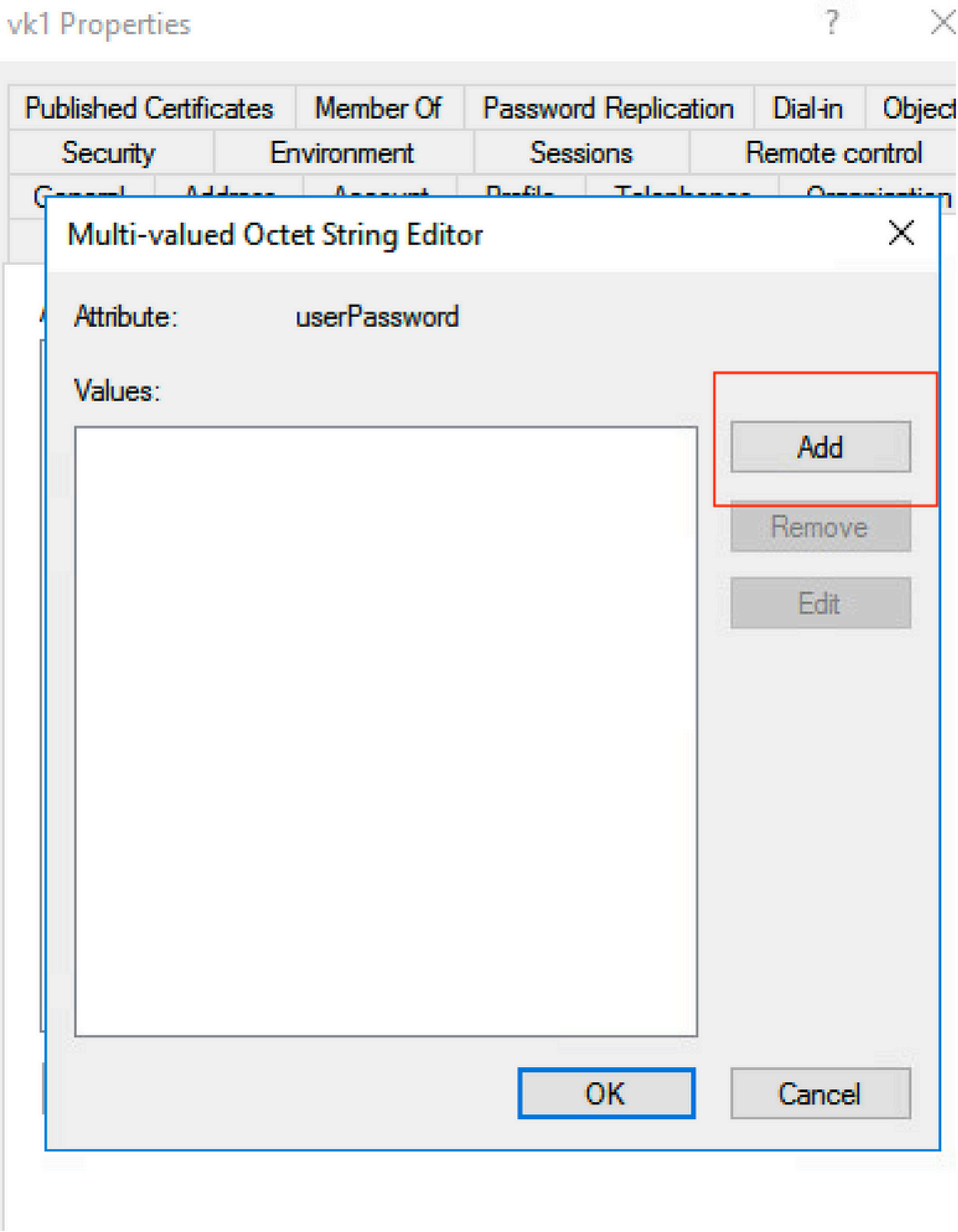

Managed Service Accour
Program Data
System
Users
NTDS Quotas
TPM Devices
DnsUpdateP... Security Group... DNS clients who are per...
Domain Ad... Security Group... Designated administrato...
Domain Co... Security Group... All workstations and ser...
Domain Con... Security Group... All domain controllers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

步骤3.在属性窗口中选择属性编辑器



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>

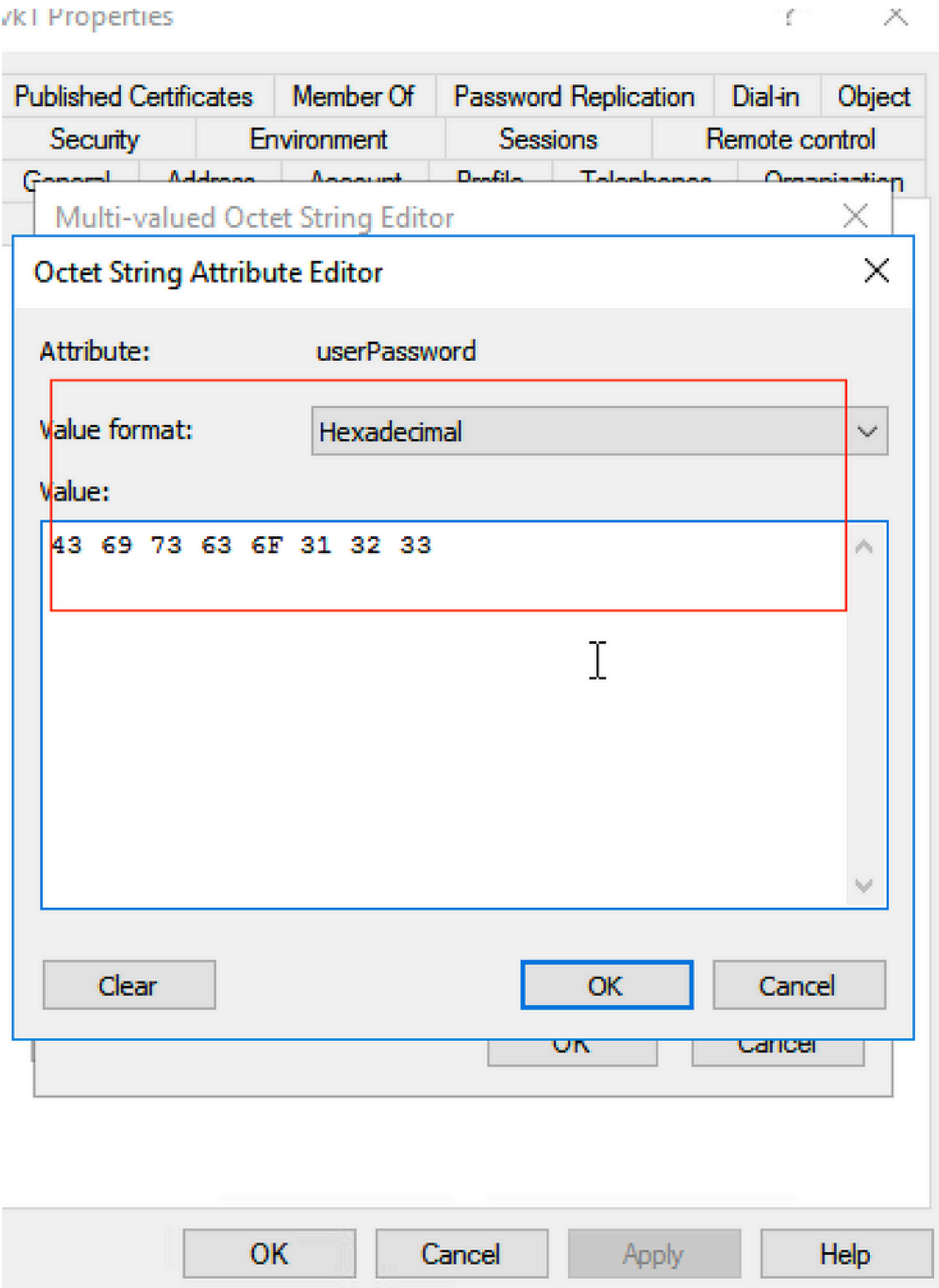
步骤4.配置“userPassword”属性。这是用户的密码，需要以十六进制值配置。


vk1 Properties

Multi-valued Octet String Editor

Attribute: userPassword

Values:



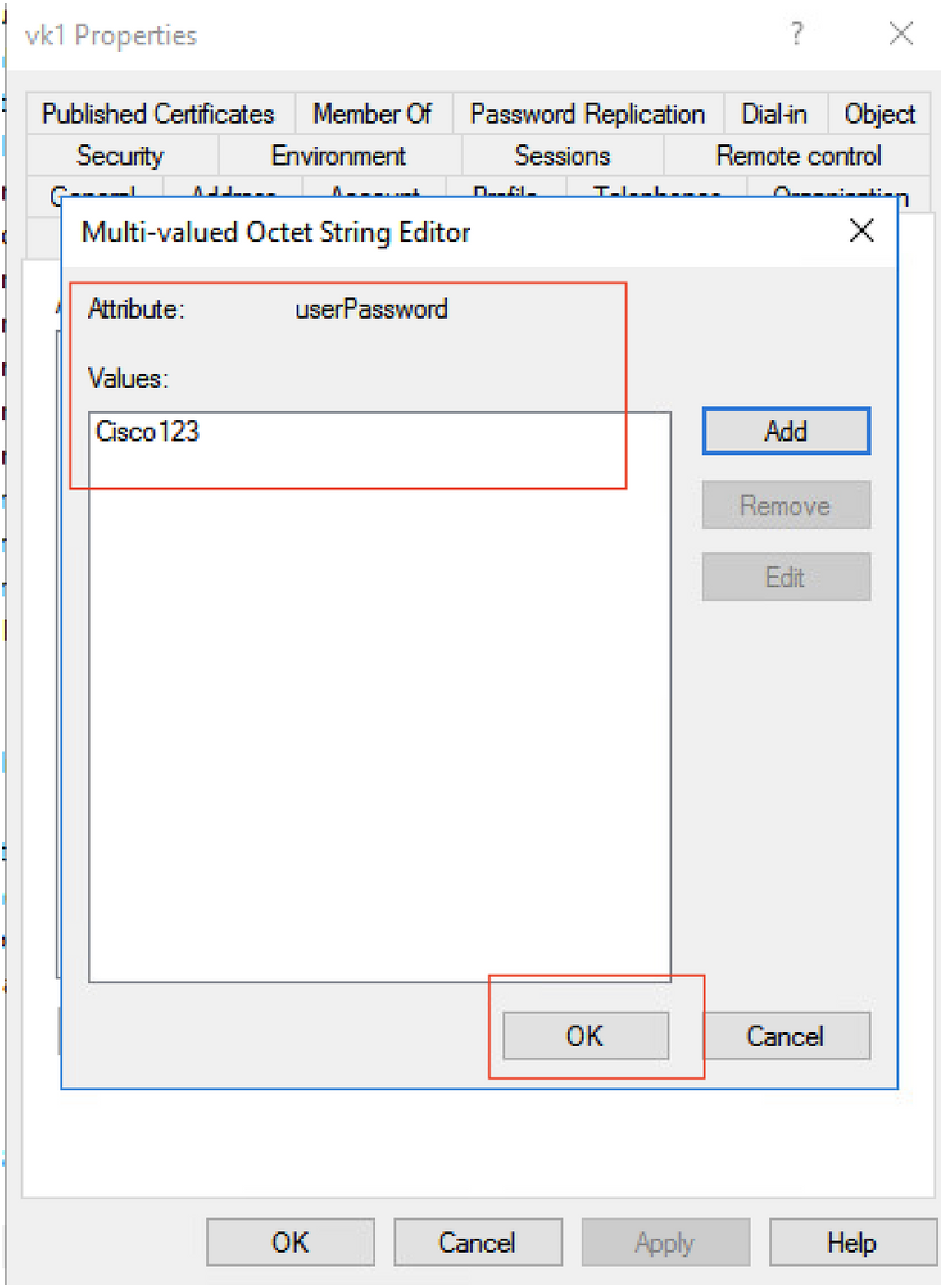
Attribute: userPassword

Value format: Hexadecimal

Value:

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

点击ok，验证它是否显示正确的密码

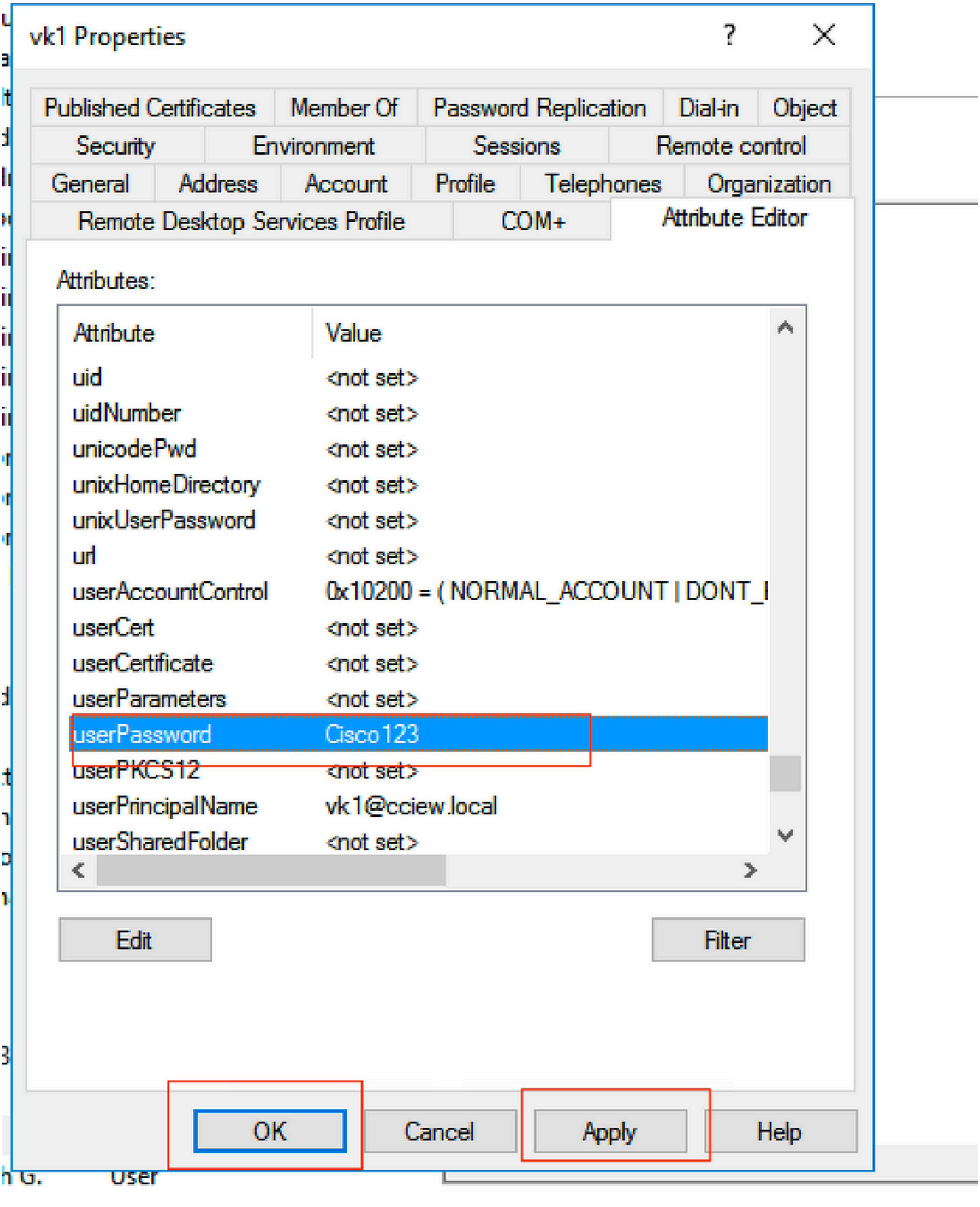


Attribute: userPassword

Values:

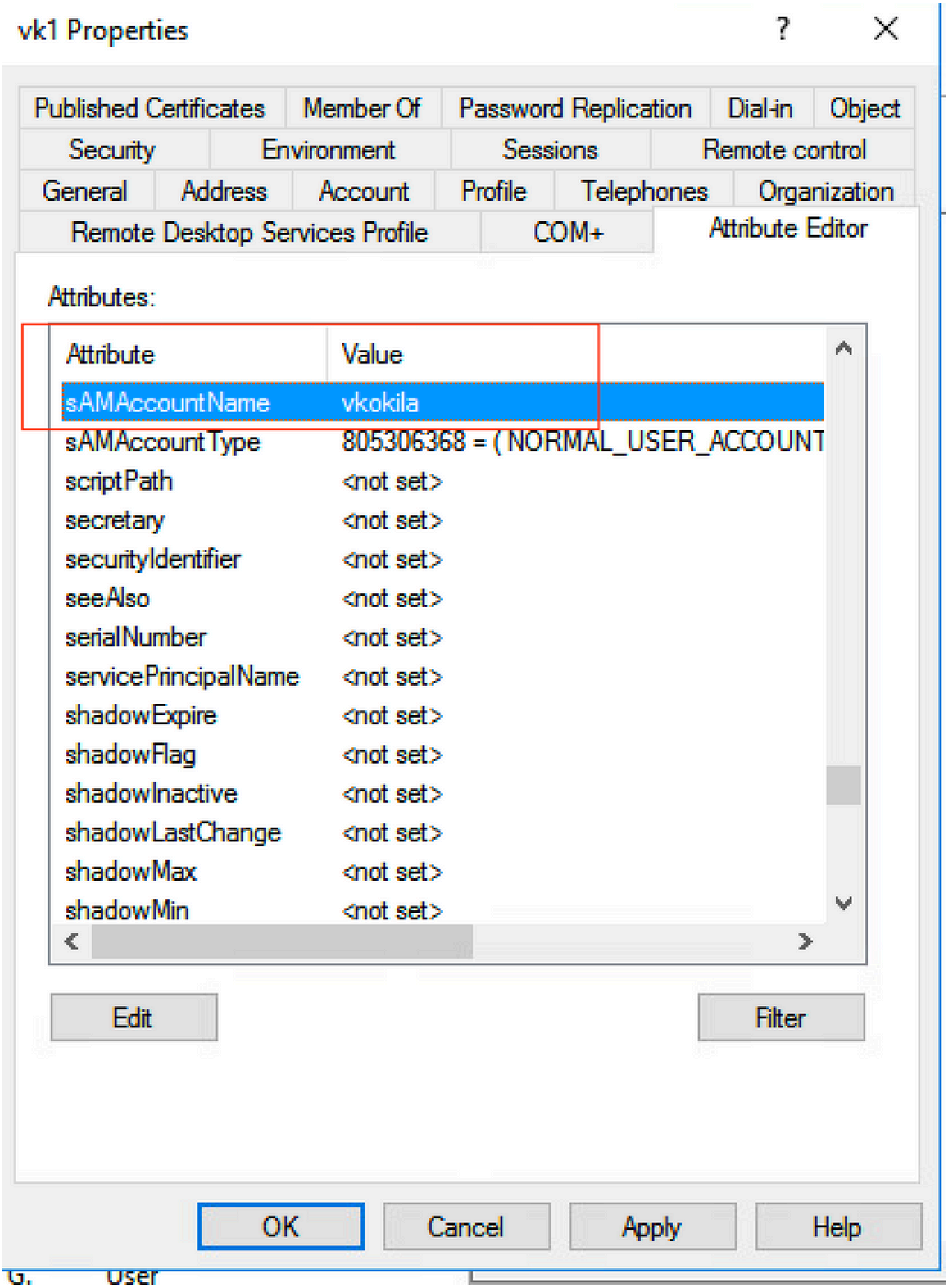
Cisco123

步骤5.单击应用，然后单击确定



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>

步骤6.验证用户的“sAMAccountName”属性值以及身份验证的用户名。



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 配置:

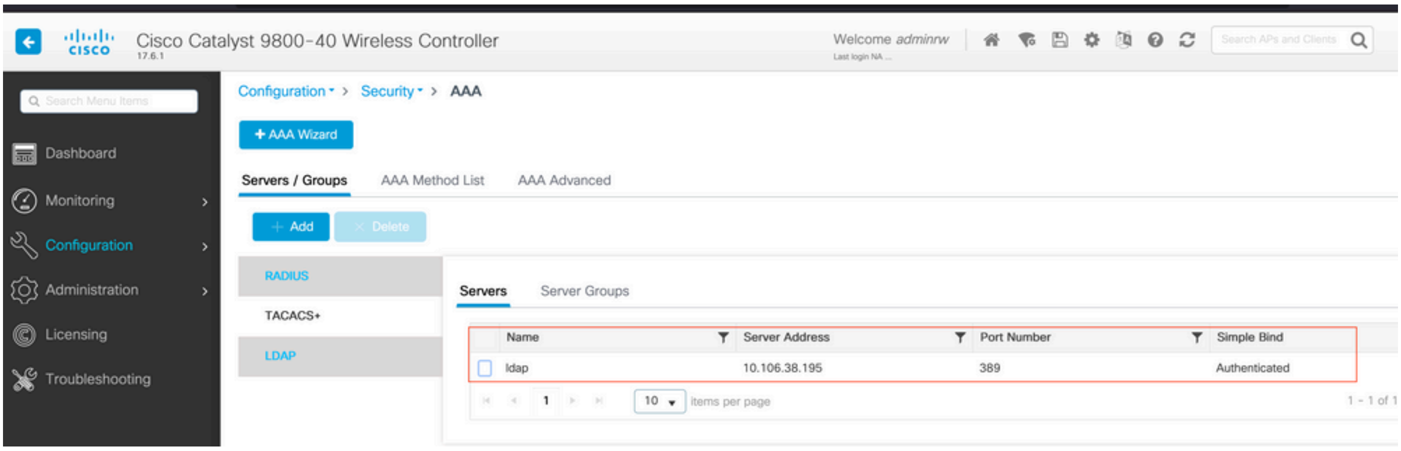
步骤1.创建LDAP属性映射

步骤2.配置“sAMAccountName”属性并键入“username”

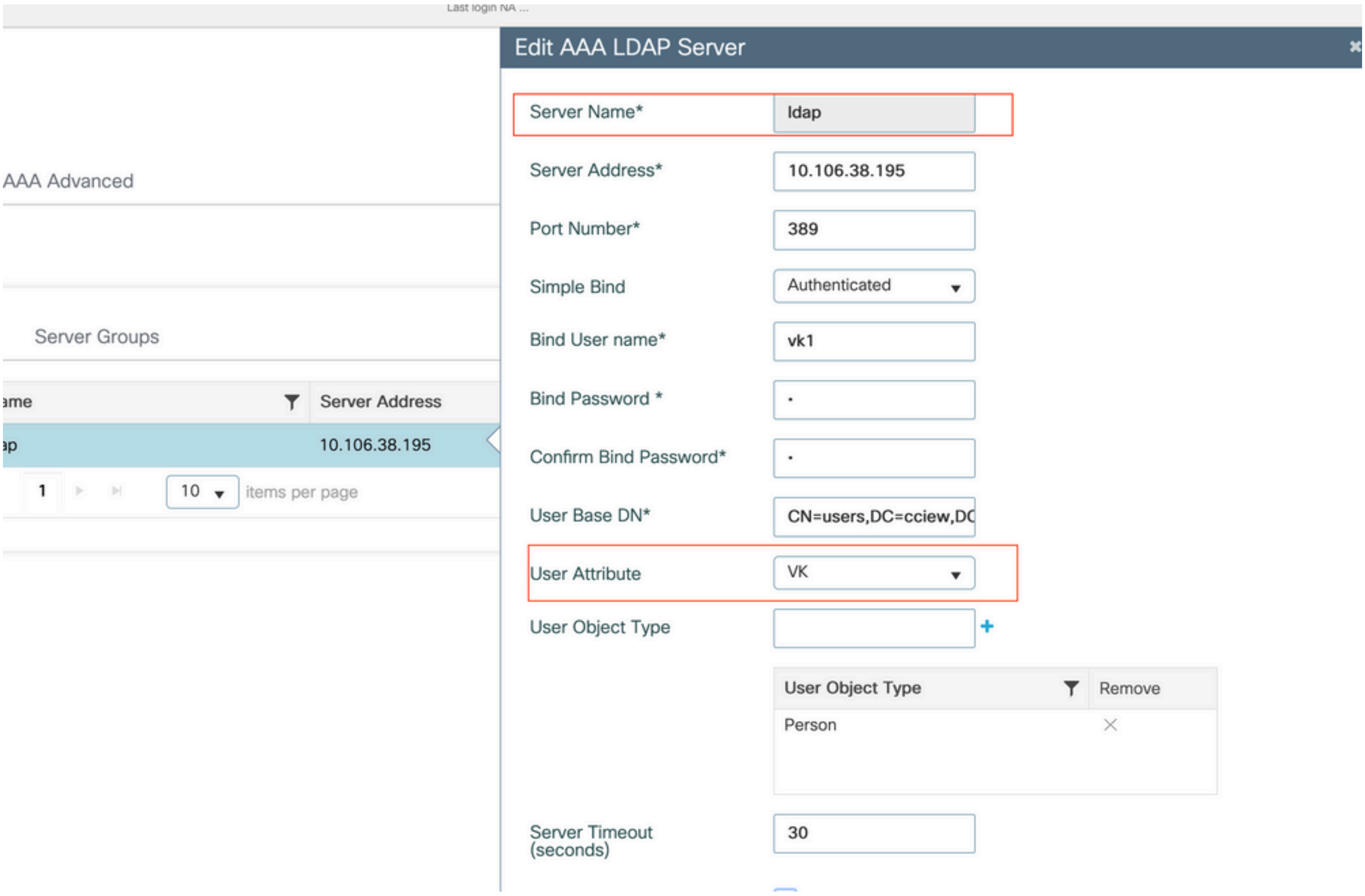
步骤3.在LDAP服务器配置下选择创建的属性MAP。

```
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
```

从Web界面验证：



	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	
Server Timeout (seconds)	30

User Object Type	Remove
Person	×

10.106.38.195

验证

要验证您的配置，请使用本文中的CLI命令仔细检查。

LDAP数据库通常不提供身份验证日志，因此可能很难知道发生了什么情况。请访问本文的故障排除部分，了解如何进行跟踪和嗅探器捕获，以查看是否已与LDAP数据库建立连接。

故障排除

要解决此问题，最好将其分为两个部分。第一部分是验证本地EAP部分。第二个是验证9800是否与LDAP服务器正常通信。

如何验证控制器上的身份验证过程

您可以收集放射性跟踪以获得客户端连接的“调试”。

只需转到**故障排除>放射性跟踪**。添加客户端MAC地址（注意您的客户端可以使用随机MAC而不是自己的MAC，您可以在客户端设备本身的SSID配置文件中验证这一点）并点击start。

重现连接尝试后，您可以点击“Generate”并获取最后X分钟的日志。请确保点击**internal**，因为如果您不启用某些LDAP日志行，则不会显示该日志行。

以下是客户端在Web身份验证SSID上成功进行身份验证的辐射跟踪示例。为清楚起见，删除了一些冗余部件：

```
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):
```

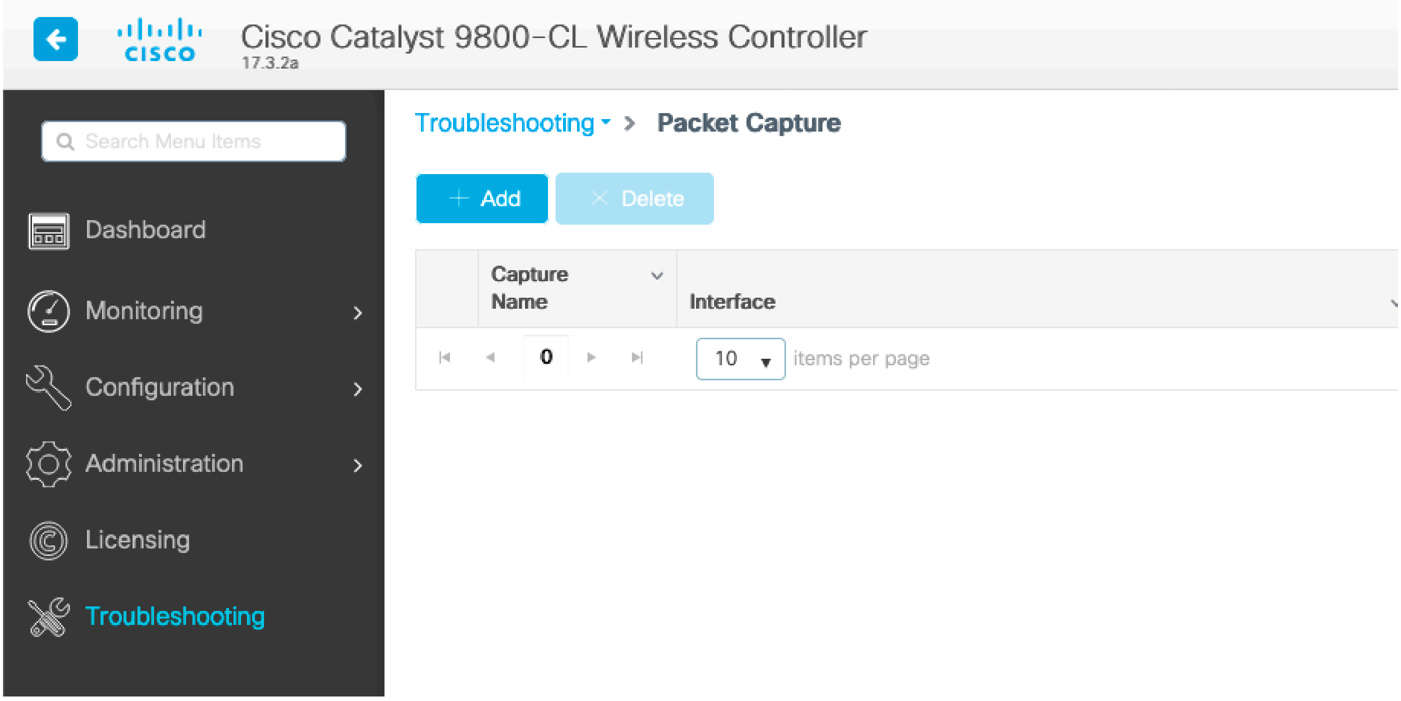
```
[2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:06.720716
{wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:58:06.724036 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2e1f.3a65.9c09:capwap_90000004] 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
```

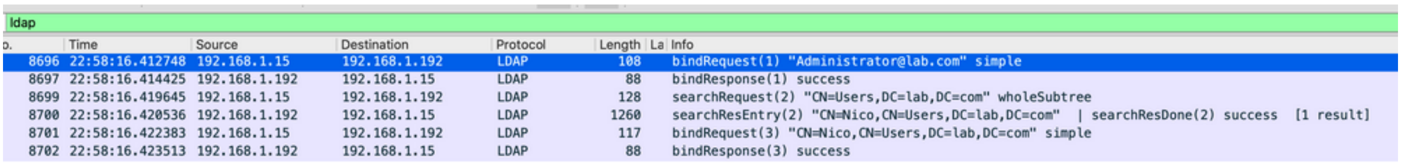
如何验证9800到LDAP的连接

您可以在9800中执行嵌入式捕获，以查看哪些流量流向LDAP。

要从WLC获取捕获，请导航到**故障排除>数据包捕获**，然后单击**+Add**。选择上行链路端口并开始捕获。



以下是用户Nico的成功身份验证示**例**



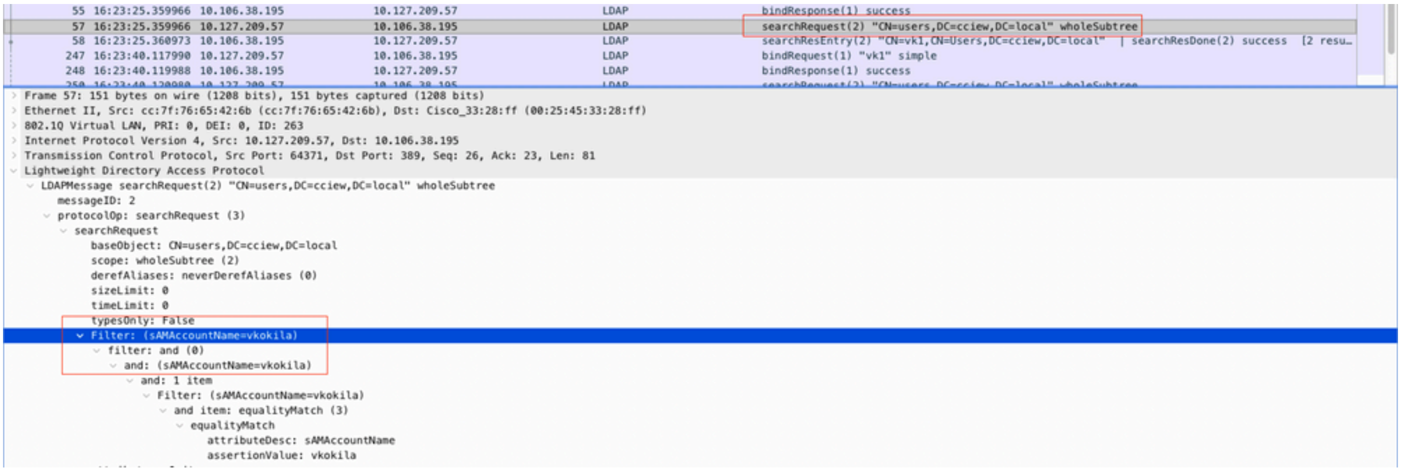
```
ldap
o.    Time             Source         Destination    Protocol  Length La Info
 8696 22:58:16.412748  192.168.1.15   192.168.1.192  LDAP         108    bindRequest(1) "Administrator@lab.com" simple
 8697 22:58:16.414425  192.168.1.192  192.168.1.15   LDAP          88    bindResponse(1) success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

前2个数据包代表与LDAP数据库的WLC绑定，即WLC使用管理员用户向数据库进行身份验证（以便能够执行搜索）。

这2个LDAP数据包表示在基本DN中执行搜索的WLC（此处CN=Users，DC=lab，DC=com）。 数据包的内部包含用户名过滤器（此处“Nico”）。 LDAP数据库成功返回用户属性

最后2个数据包代表尝试使用该用户密码进行身份验证以测试密码是否正确的WLC。

1. 收集EPC并检查“sAMAccountName”是否应用为过滤器：

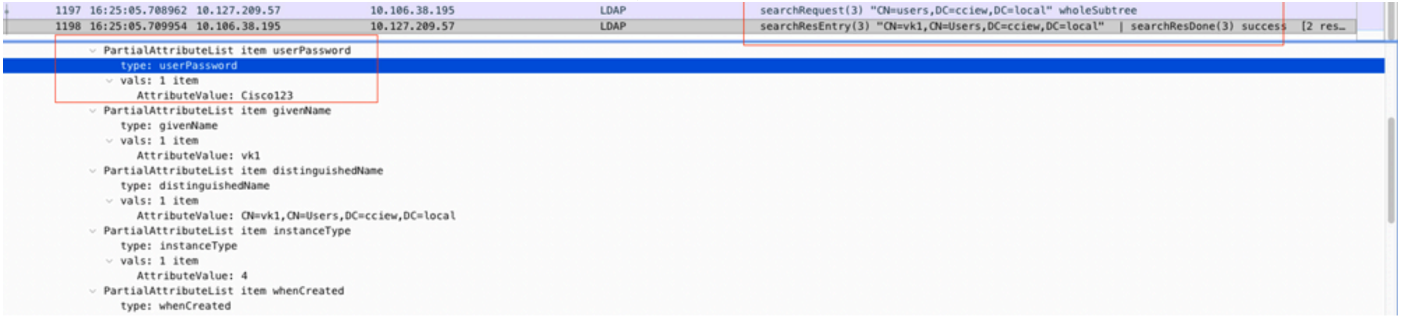


```
   55 16:23:25.359966 10.106.38.195    10.127.209.57    LDAP    bindResponse(1) success
   57 16:23:25.359966 10.127.209.57    10.106.38.195    LDAP    searchRequest(2) "CN=users,DC=cciew,DC=local" wholeSubtree
   58 16:23:25.360973 10.106.38.195    10.127.209.57    LDAP    searchResEntry(2) "CN=vk1,CN=Users,DC=cciew,DC=local"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

如果过滤器显示“cn”，并且正在使用“sAMAccountName”作为用户名，则身份验证失败。

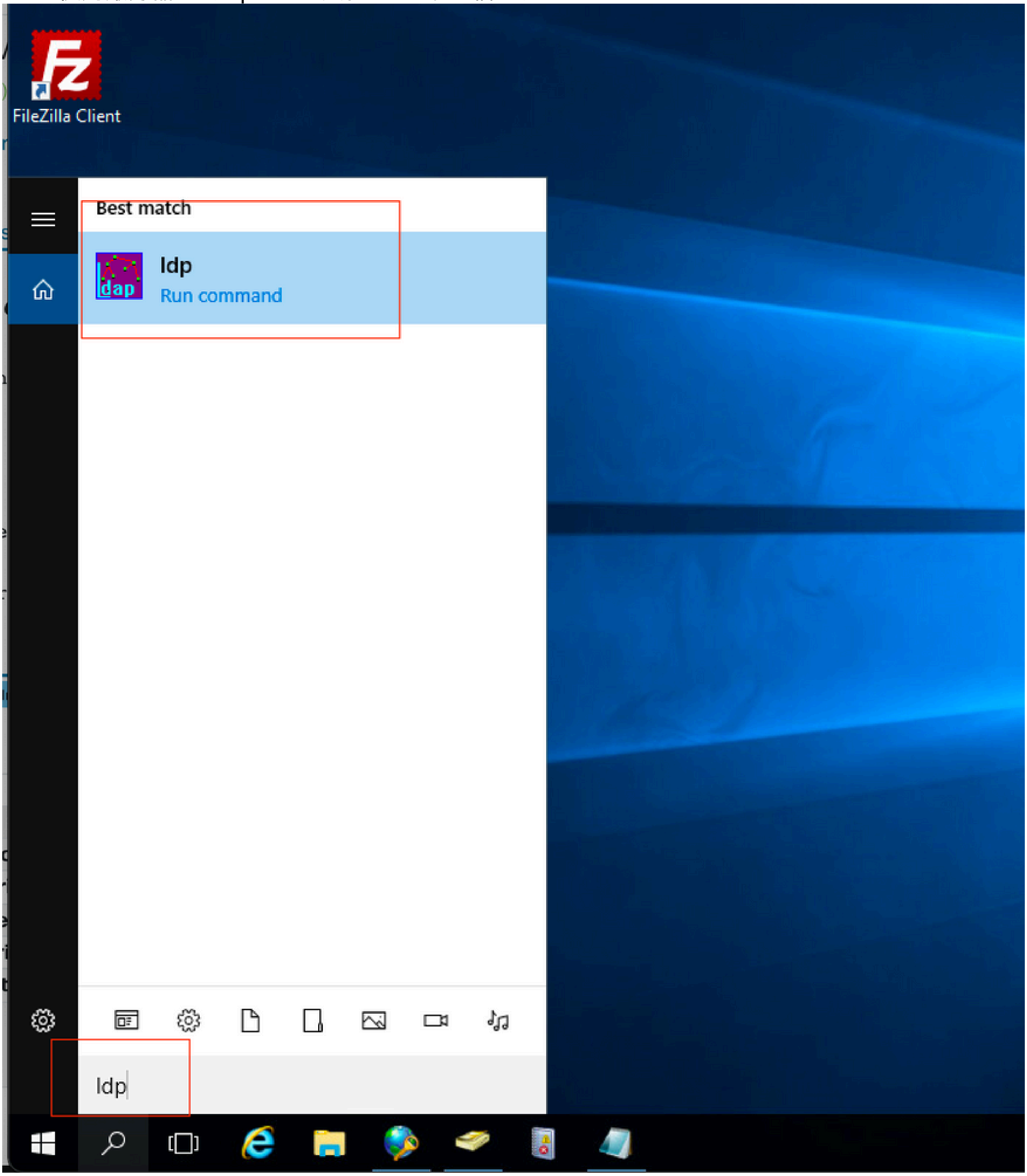
从WLC cli重新配置ldap映射属性。

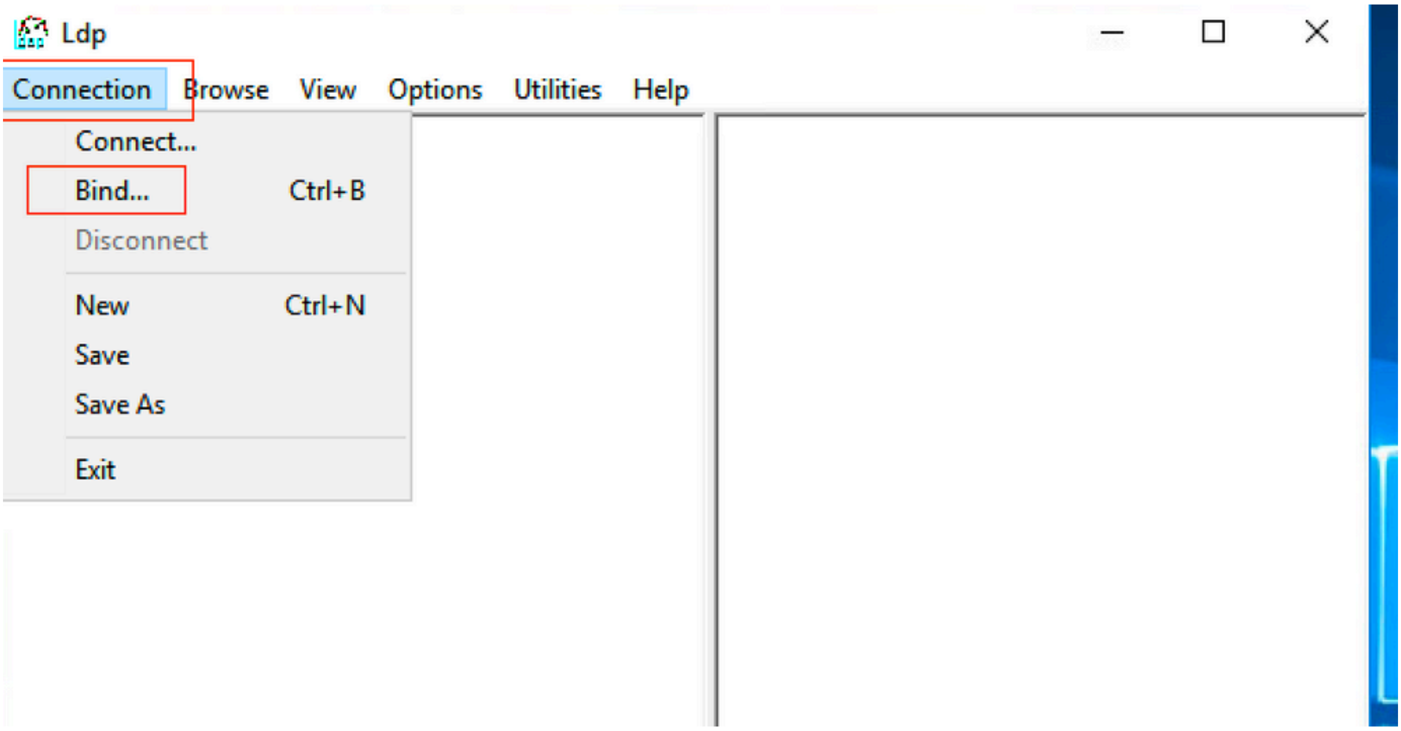
2. 确保服务器以明文返回“userPassword”，否则身份验证失败。

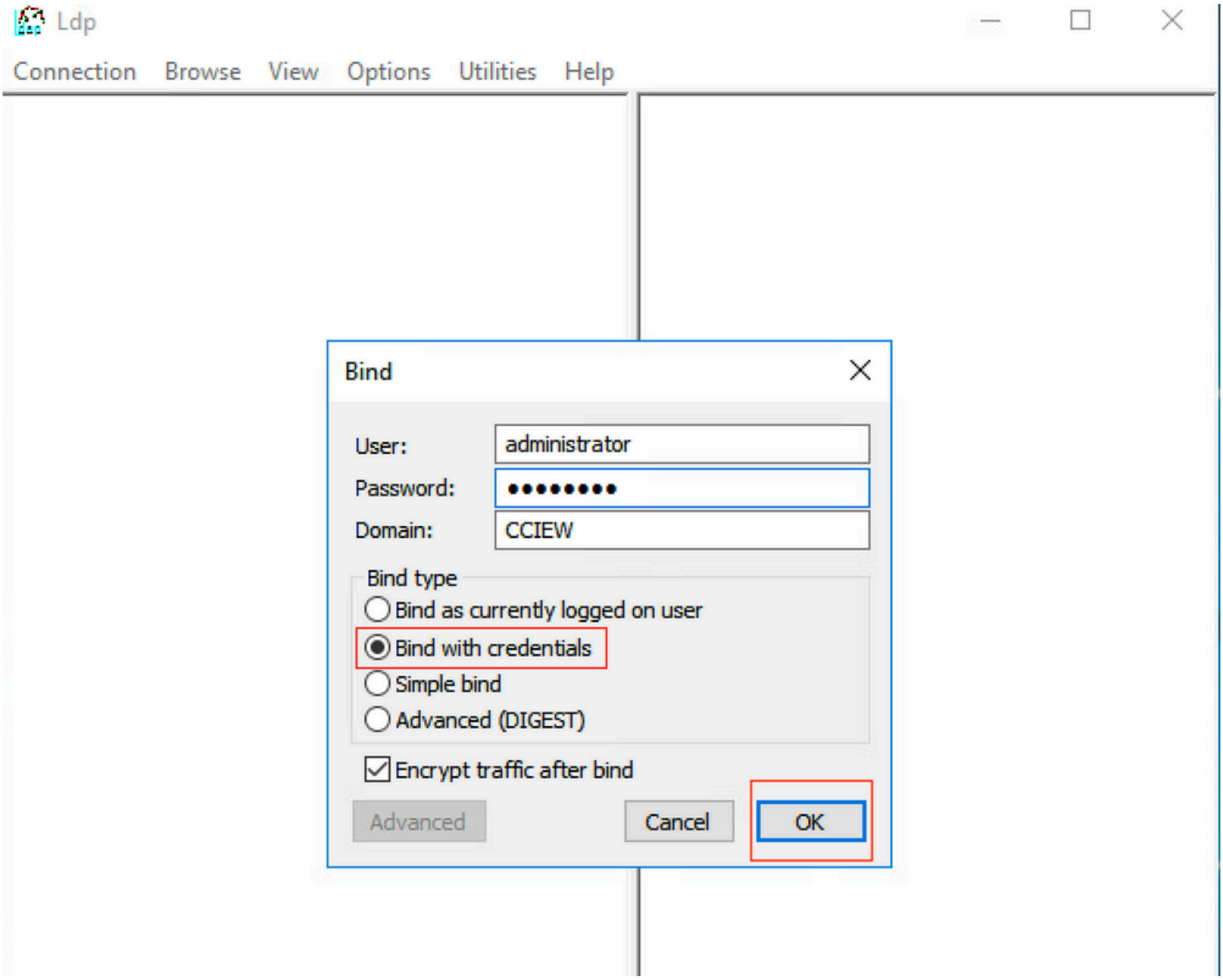


```
1197 16:25:05.708962 10.127.209.57    10.106.38.195    LDAP    searchRequest(3) "CN=users,DC=cciew,DC=local" wholeSubtree
1198 16:25:05.709954 10.106.38.195    10.127.209.57    LDAP    searchResEntry(3) "CN=vk1,CN=Users,DC=cciew,DC=local"  | searchResDone(3) success  [2 res…
      PartialAttributeList 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. 使用服务器上的ldp.exe工具验证基础DN信息。







User: administrator

Password: •••••••••

Domain: CCIEW

Bind type

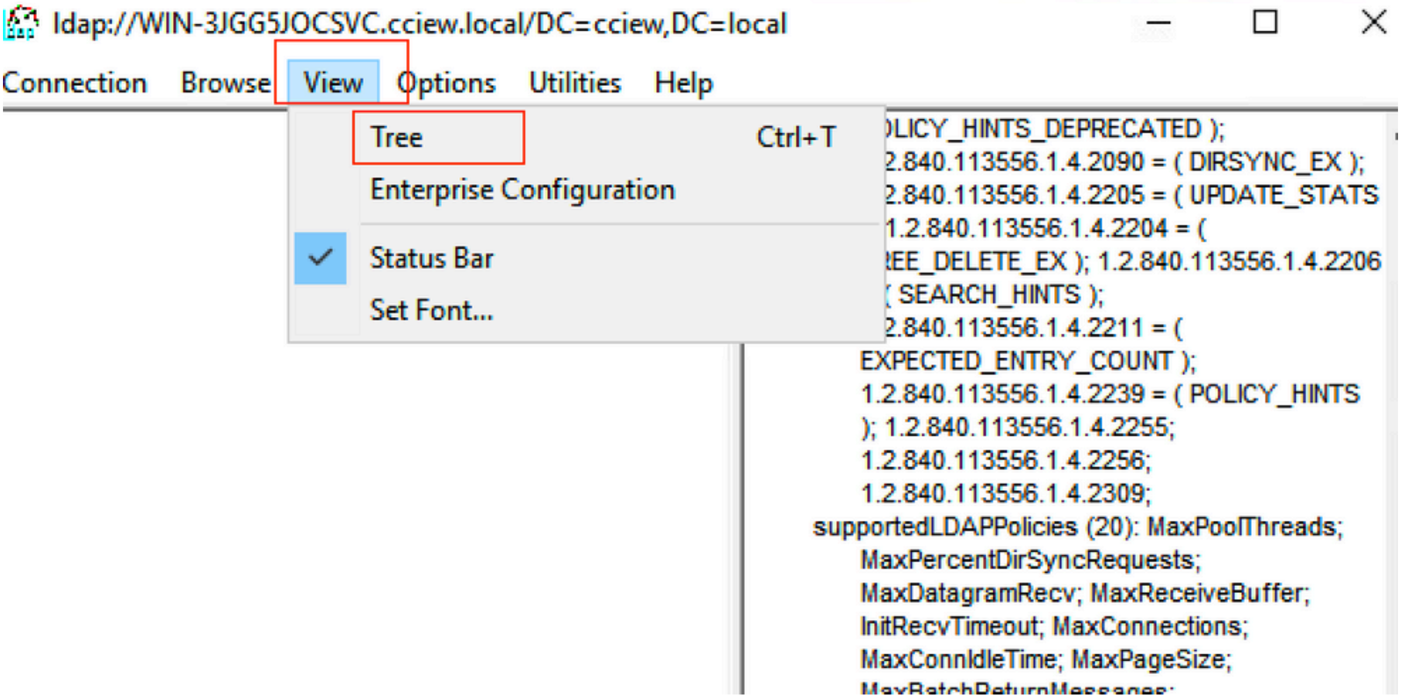
○ Bind as currently logged on user

● Bind with credentials

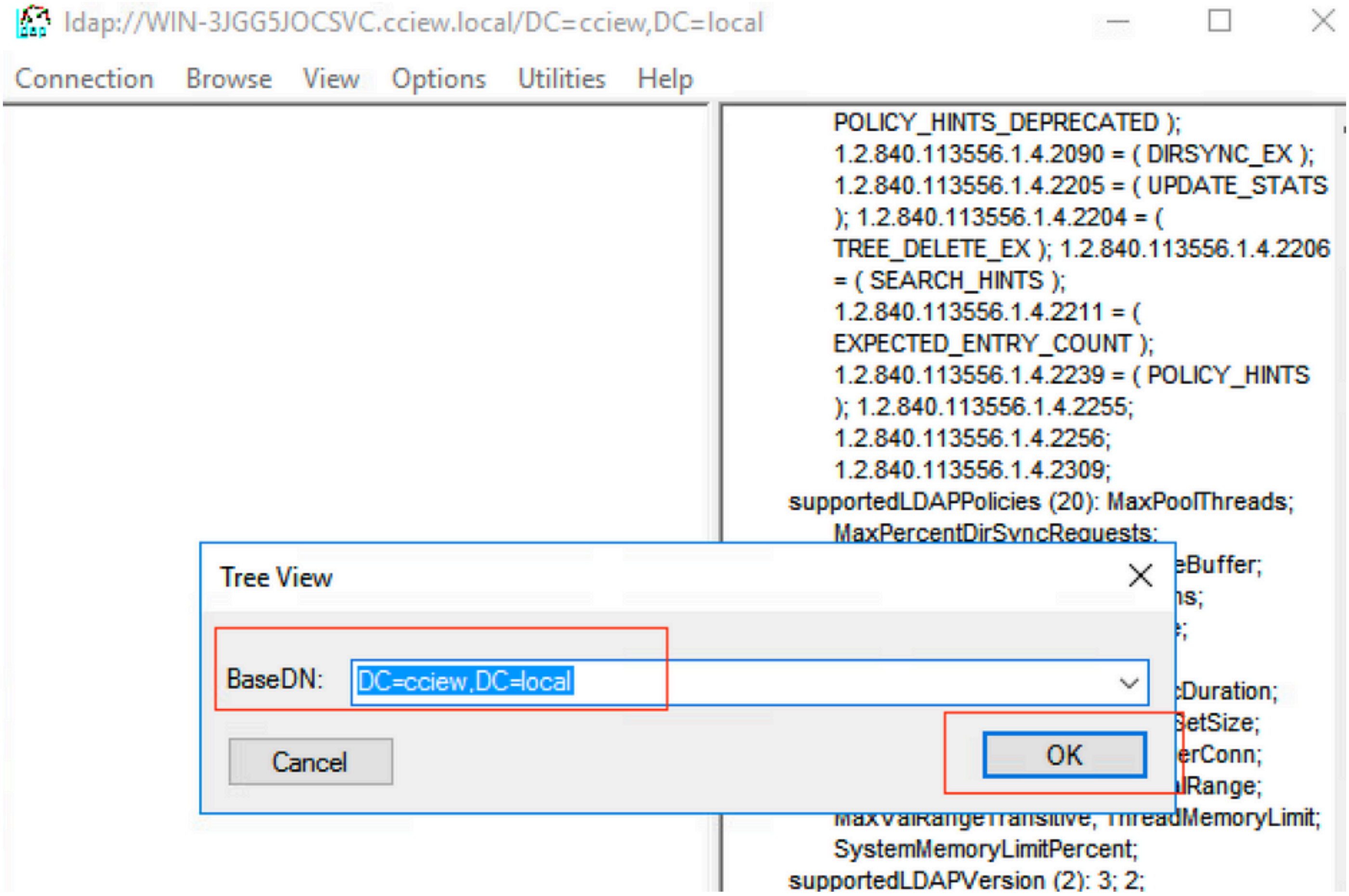
○ Simple bind

○ Advanced (DIGEST)

☑ Encrypt traffic after bind

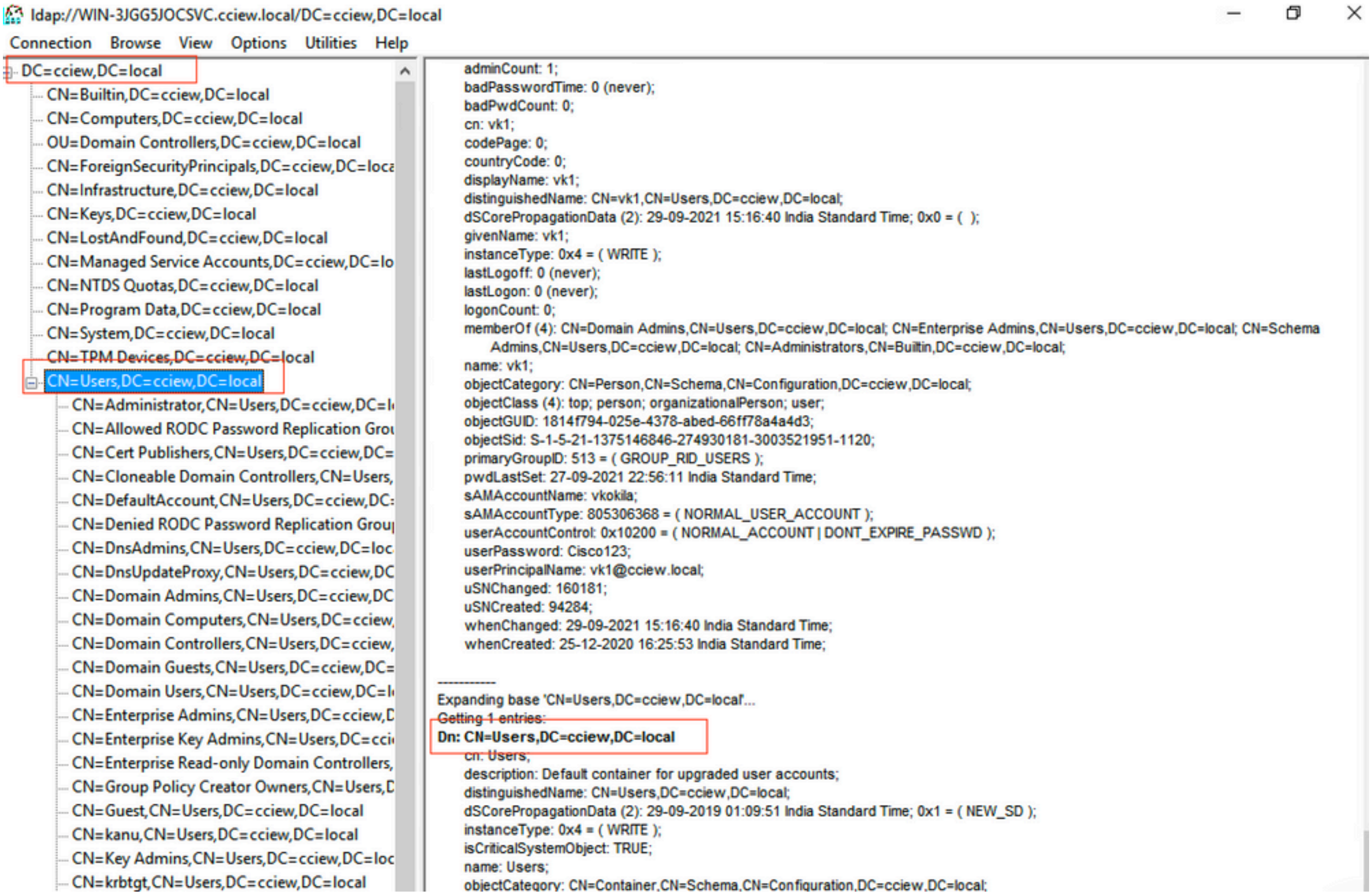


```
                )LICY_HINTS_DEPRECATED );
                2.840.113556.1.4.2090 = ( DIRSYNC_EX );
                2.840.113556.1.4.2205 = ( UPDATE_STATS
                1.2.840.113556.1.4.2204 = (
                ŒE_DELETE_EX ); 1.2.840.113556.1.4.2206
                ( SEARCH_HINTS );
                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;
```



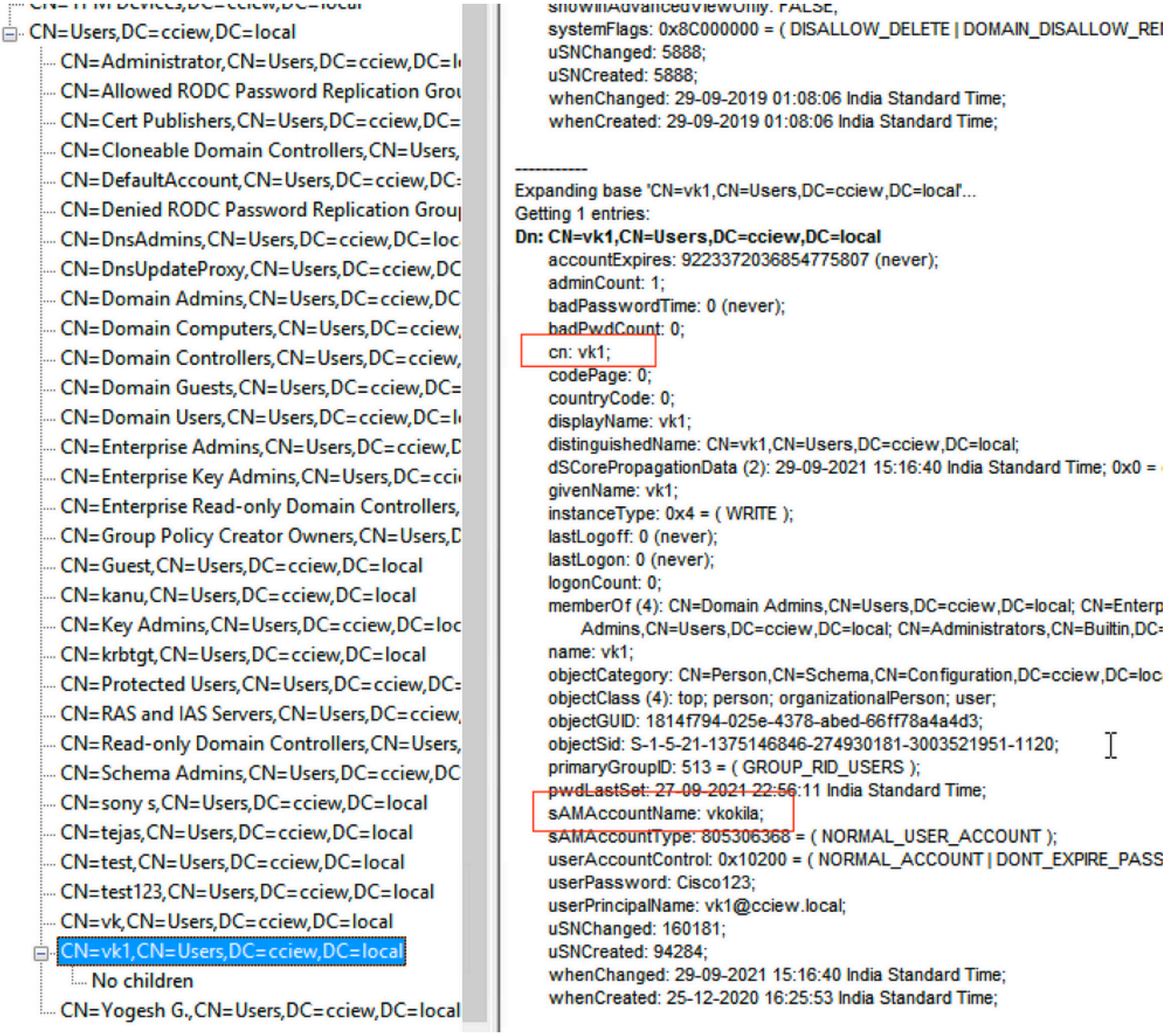
BaseDN: DC=cciew,DC=local

```
        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;
```



```
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. 检查服务器统计信息和属性MAP

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

Server Information for ldap

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

Server name              :ldap

Server Address           :10.106.38.195

Server listening Port    :389

Bind Root-dn             :vk1

Server mode              :Non-Secure

Cipher Suite             :0x00

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

Authentication Procedure:Bind with user password
```

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

Object Class            :Person

Attribute map           :VK

Request timeout         :30

Deadtime in Mins        :0

State                   :ALIVE

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

* LDAP STATISTICS *

Total messages  [Sent:2, Received:3]

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

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

Total bind      [Request:1, Response:1]

Total extended  [Request:0, Response:0]

Total compare   [Request:0, Response:0]

Search [Success:1, Failures:0]

Bind   [Success:1, Failures:0]

Missing attrs in Entry [0]

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

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

No. of active connections   :0

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

参考

9800上的本地EAP配置示例

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。