為Catalyst 9800 WLC設定802.1X的LDAP驗證和Web-auth

目錄

簡介

本文檔介紹如何配置Catalyst 9800以便使用LDAP伺服器作為使用者憑據的資料庫來驗證客戶端。

必要條件

需求

思科建議您瞭解以下主題：

- Microsoft Windows伺服器
- Active Directory或任何其他LDAP資料庫

採用元件

執行Cisco IOS®-XE版本17.3.2a的C9100存取點(AP)上的C9800 EWC

具有QNAP網路訪問儲存(NAS)的Microsoft Active Directory(AD)伺服器（充當LDAP資料庫）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

使用Webauth SSID配置LDAP

網路圖表

本文基於一個非常簡單的設定：

採用IP 192.168.1.15的EWC AP 9115

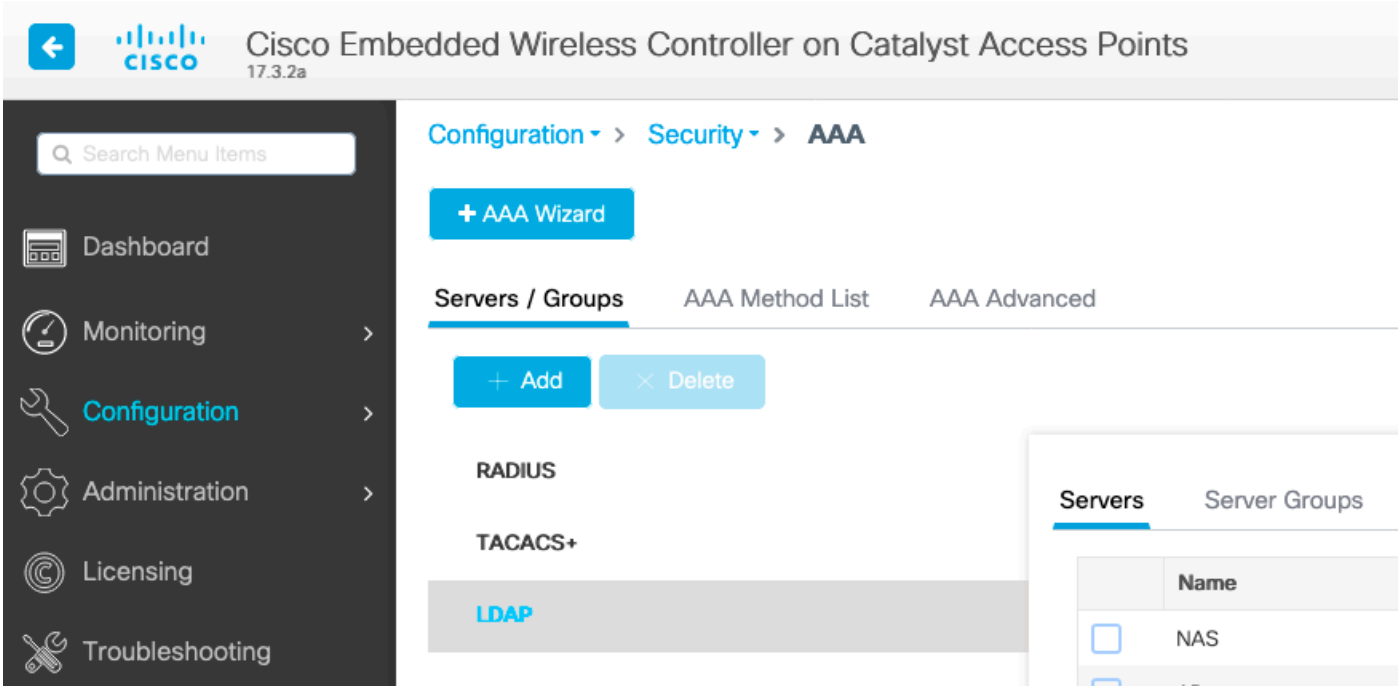
IP為192.168.1.192的Active Directory伺服器

連線到EWC內部AP的客戶端

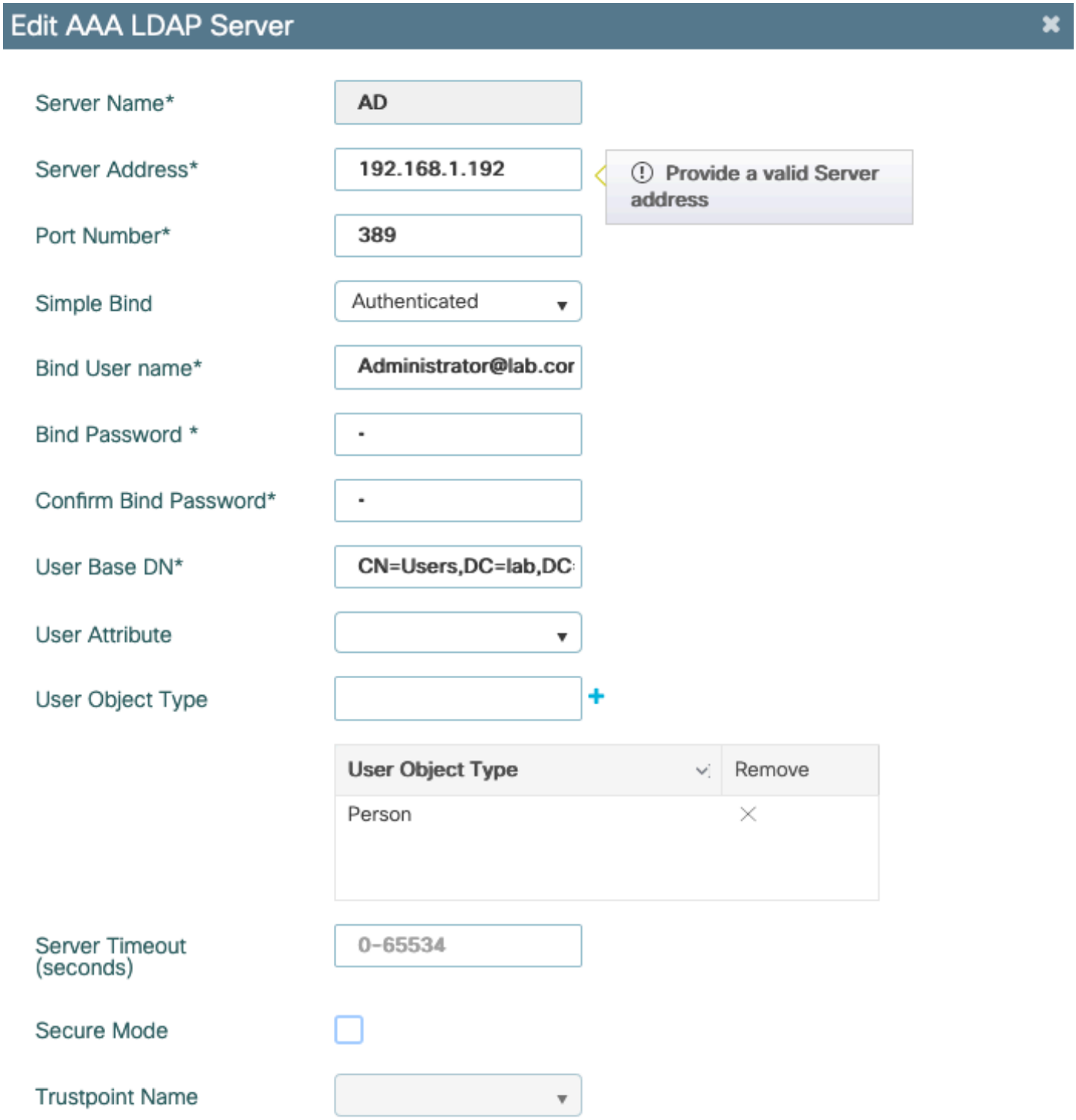
設定控制器

步驟1.配置LDAP伺服器

導航到**Configuration > Security > AAA> Servers/Groups > LDAP**，然後點選**+ Add**



為LDAP伺服器選擇名稱並填寫詳細資訊。有關每個欄位的說明，請參閱本文檔的「瞭解LDAP伺服器詳細資訊」部分。



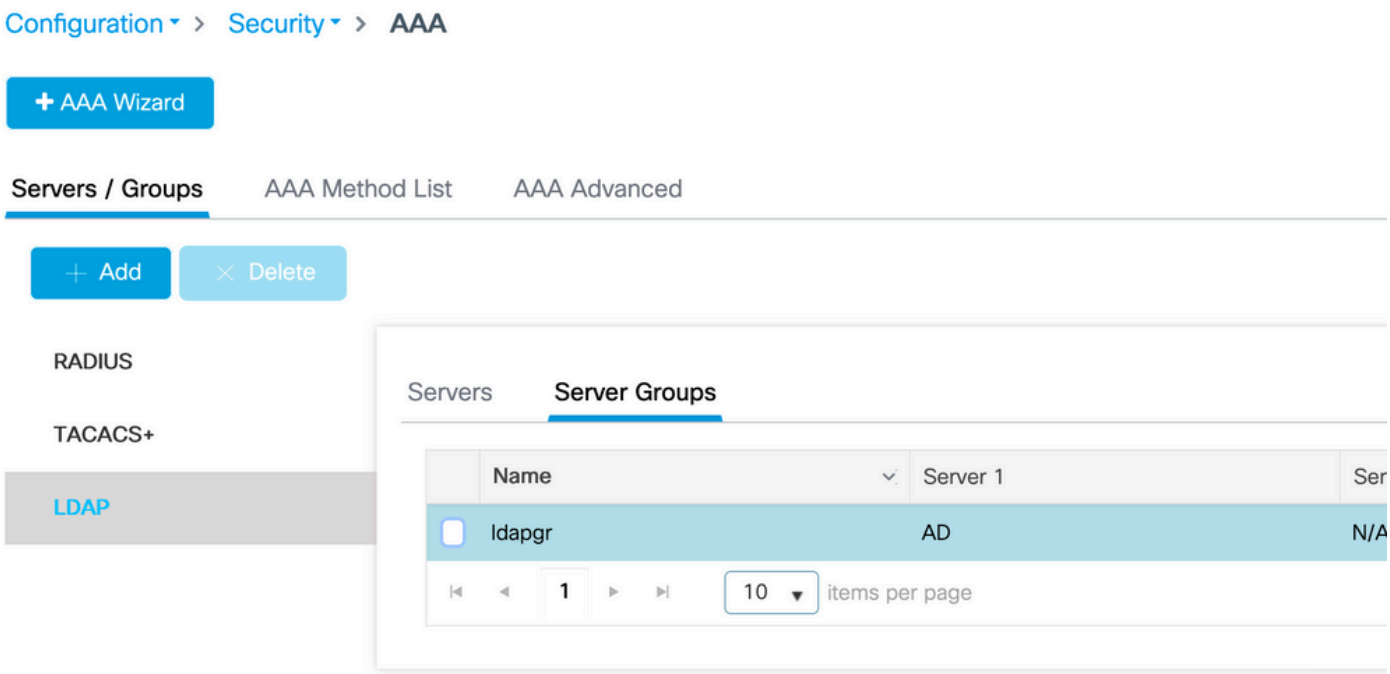
按一下**Update and apply to device**儲存

CLI命令：

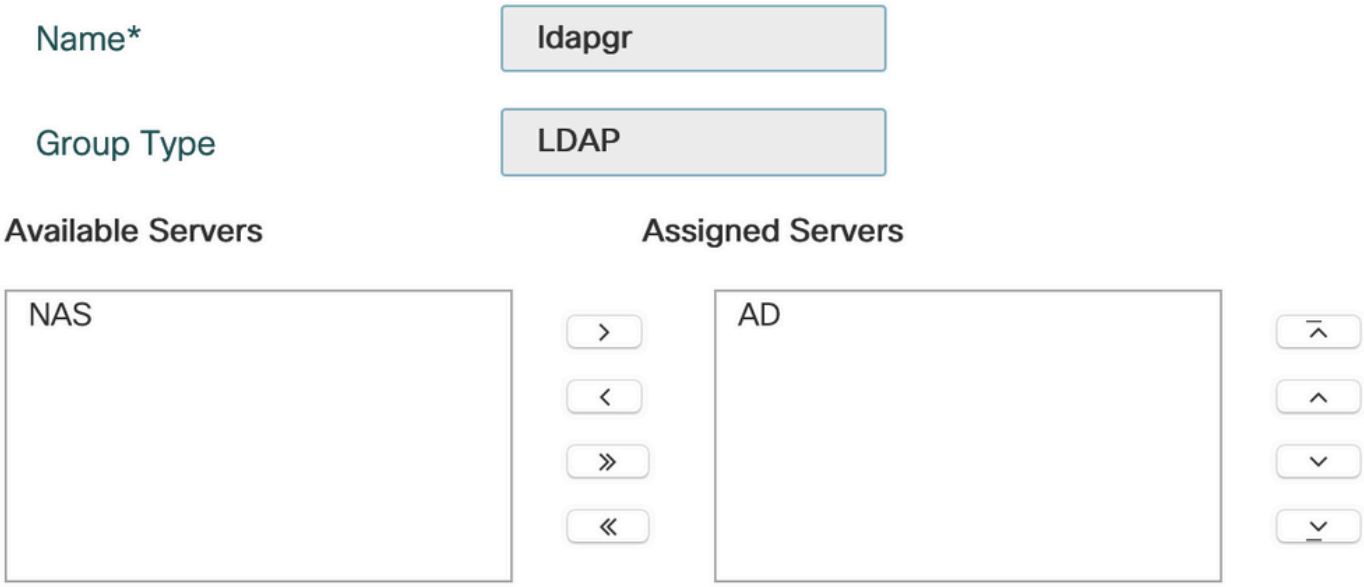
```
ldap server AD ipv4 192.168.1.192 bind authenticate root-dn Administrator@lab.com password 6
WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB base-dn CN=Users,DC=lab,DC=com search-filter user-object-type
Person
```

步驟2.配置LDAP伺服器組。

導航到**Configuration > Security > AAA > Servers/Groups > LDAP > Server Groups**，然後按一下**+ADD**



輸入名稱並新增在上一步中配置的LDAP伺服器。



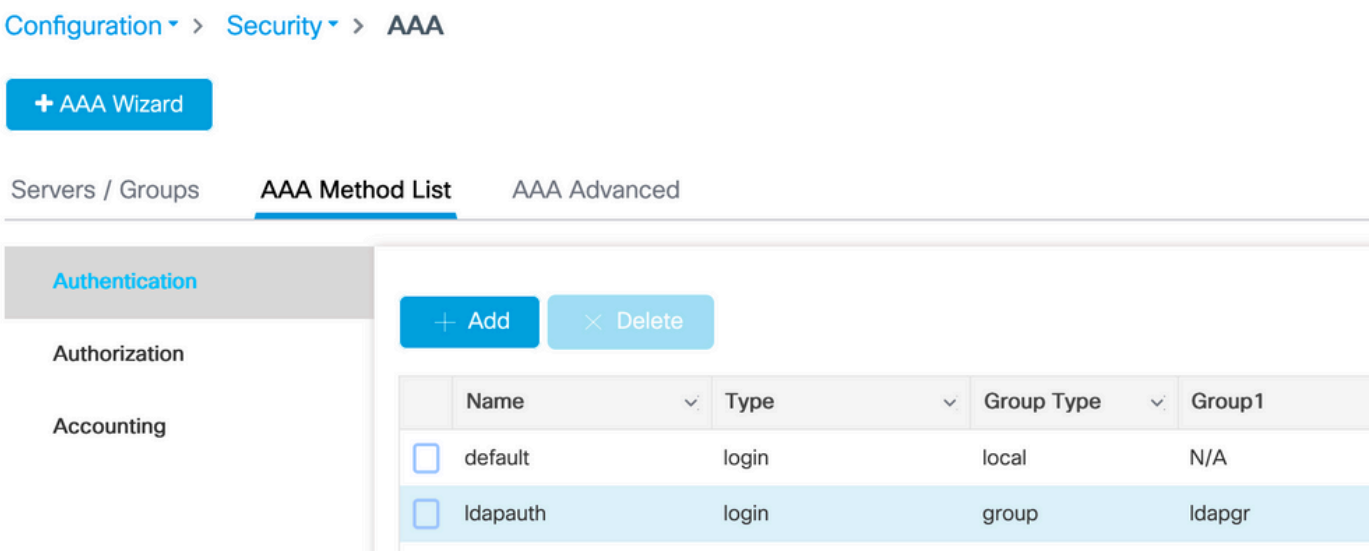
按一下**Update and apply**儲存。

CLI命令：

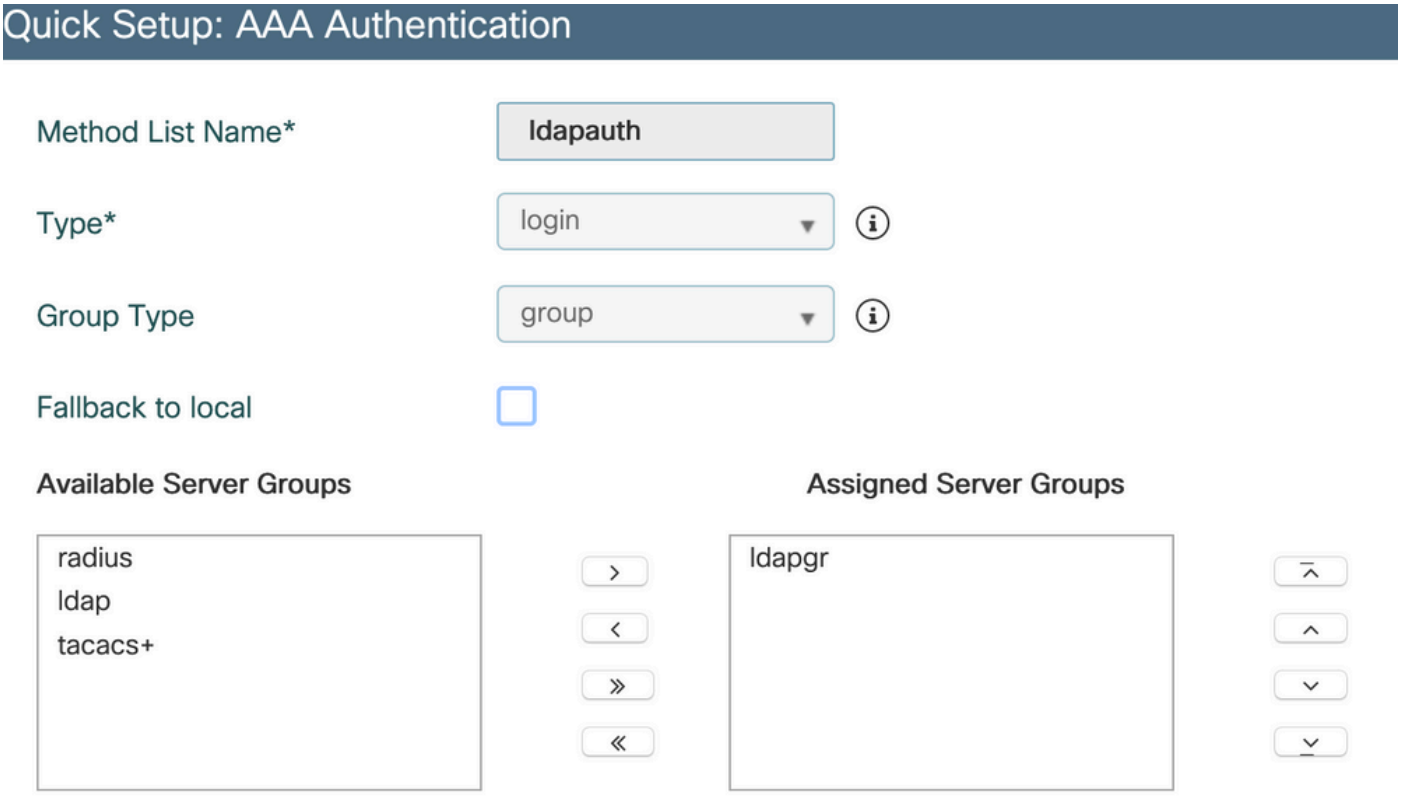
```
aaa group server ldap ldapgr server AD
```

步驟3.配置AAA身份驗證方法

導覽至**Configuration > Security > AAA > AAA method List > Authentication**，然後按一下**+Add**



輸入名稱，選擇**Login**型別並指向之前配置的LDAP伺服器組。

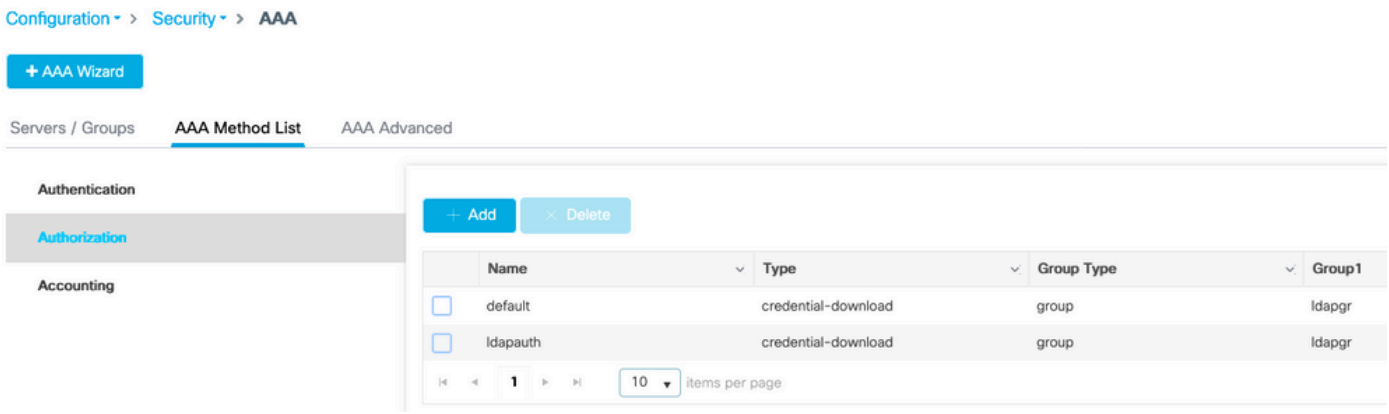


CLI命令：

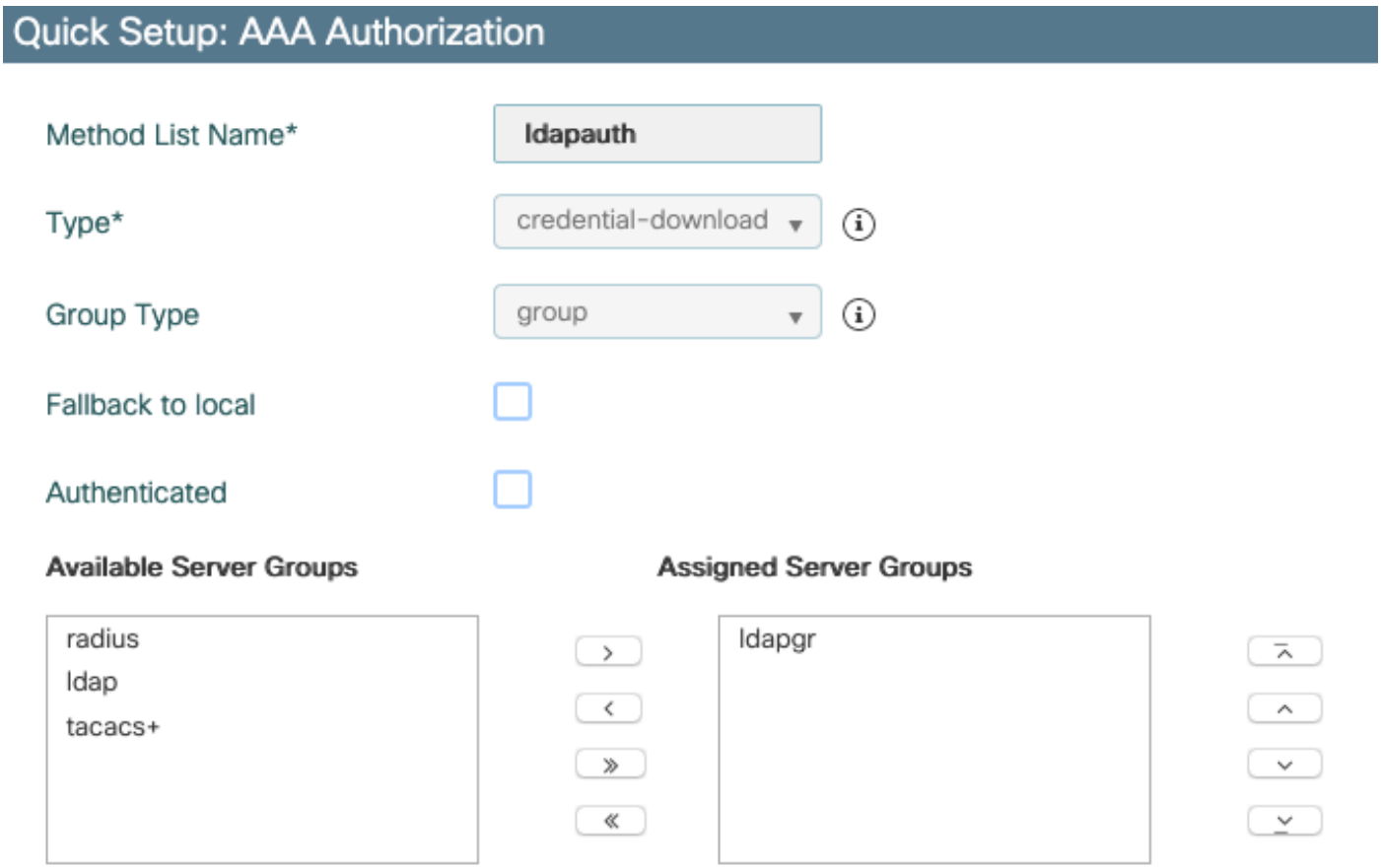
```
aaa authentication login ldapauth group ldapgr
```

步驟4.配置AAA授權方法

導航到**Configuration > Security > AAA > AAA method list > Authorization**，然後點選**+Add**



建立所選名稱的憑據下載型別規則，並將其指向之前建立的LDAP伺服器組



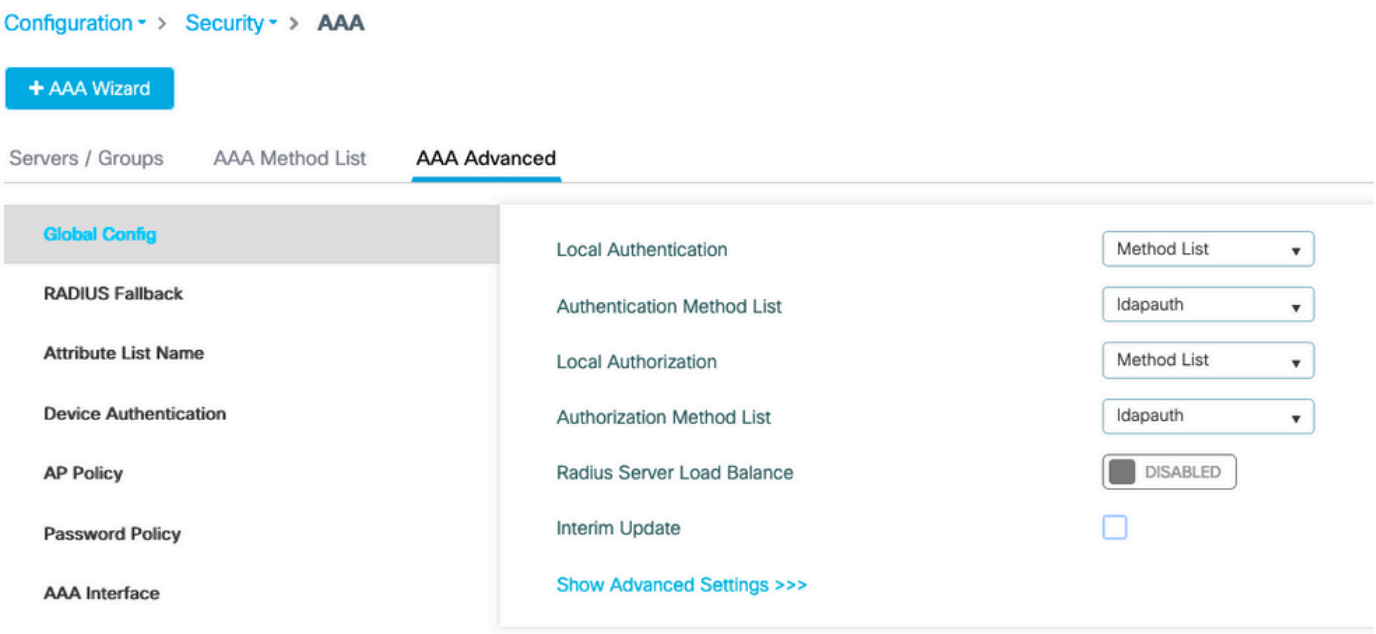
CLI命令：

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

步驟5.配置本地身份驗證

導覽至Configuration > Security > AAA > AAA Advanced > Global Config

將本地身份驗證和本地授權設定為Method List，並選擇之前配置的身份驗證和授權方法。

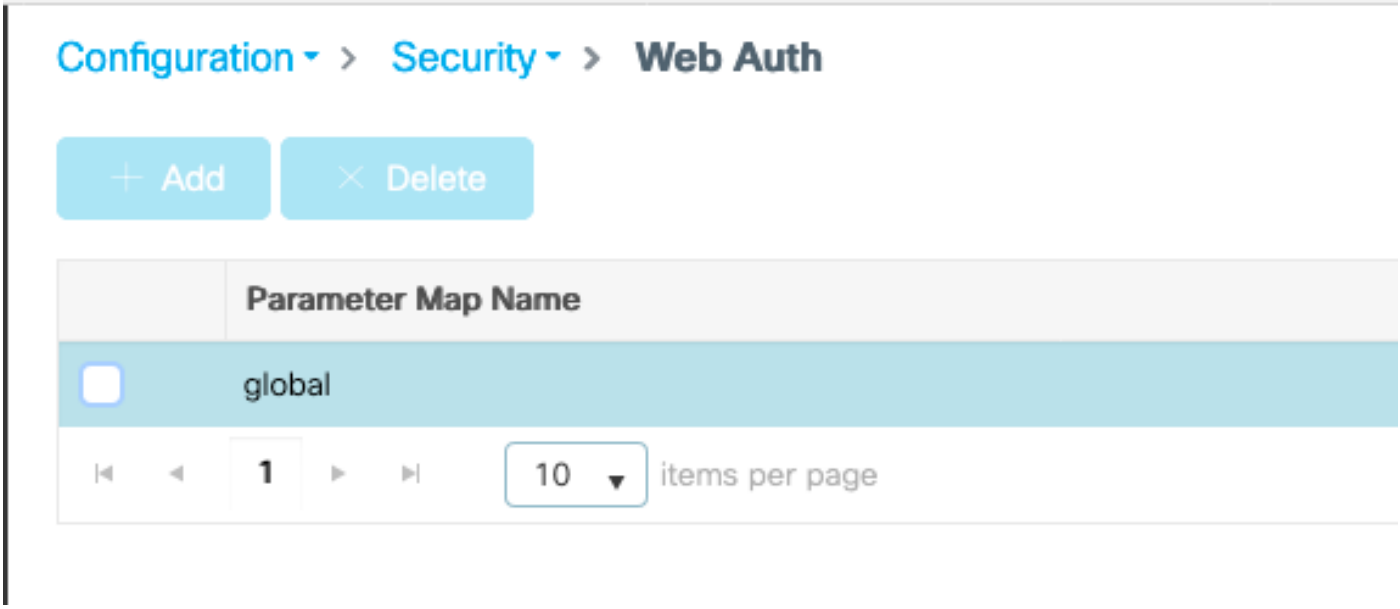


CLI命令：

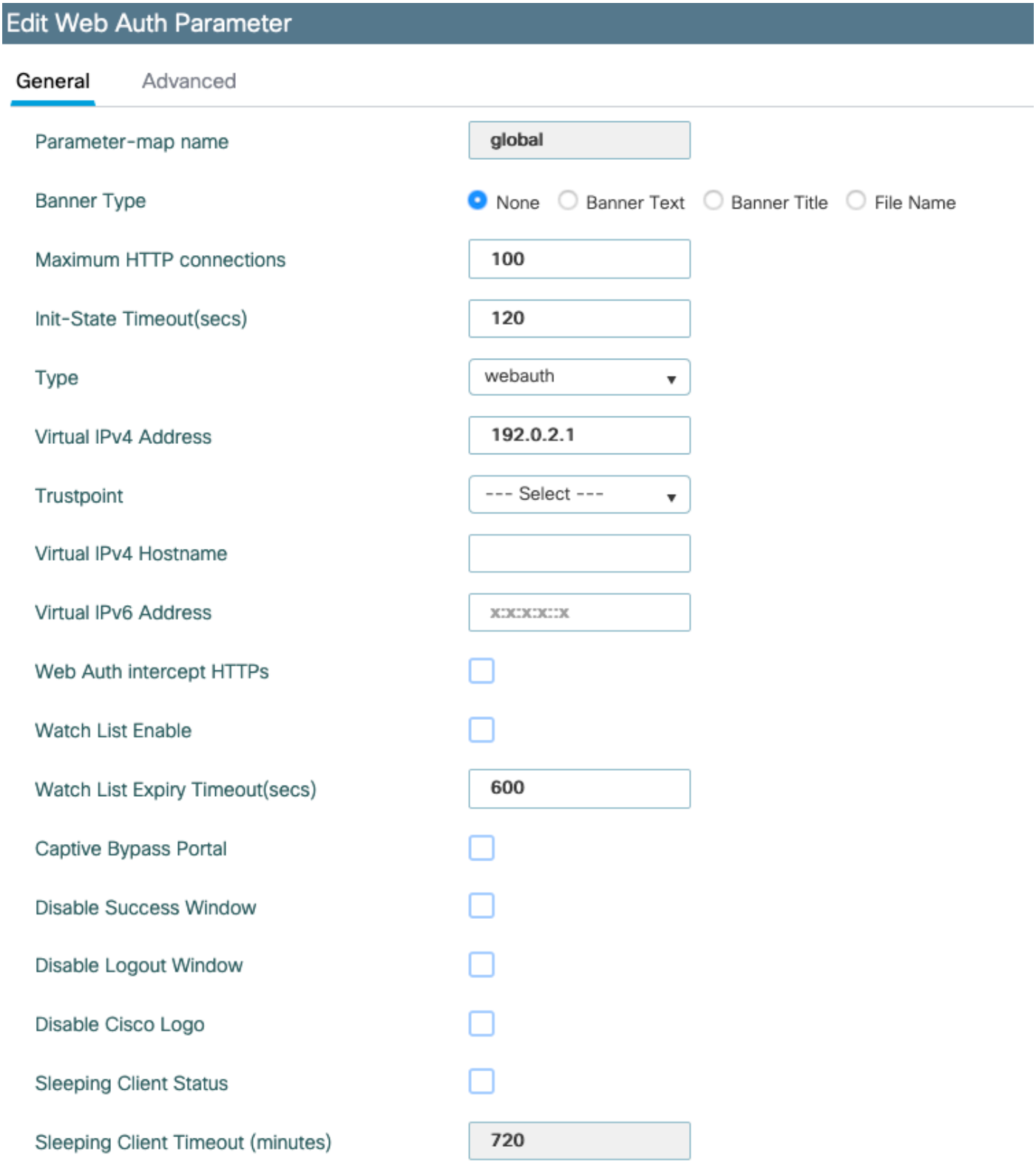
```
aaa local authentication ldapauth authorization ldapauth
```

步驟6.設定webauth引數映像

導覽至**Configuration > Security > Web Auth**，然後編輯**全域映**射



確保配置虛擬IPv4地址，例如192.0.2.1（該特定IP/子網保留用於不可路由的虛擬IP）。



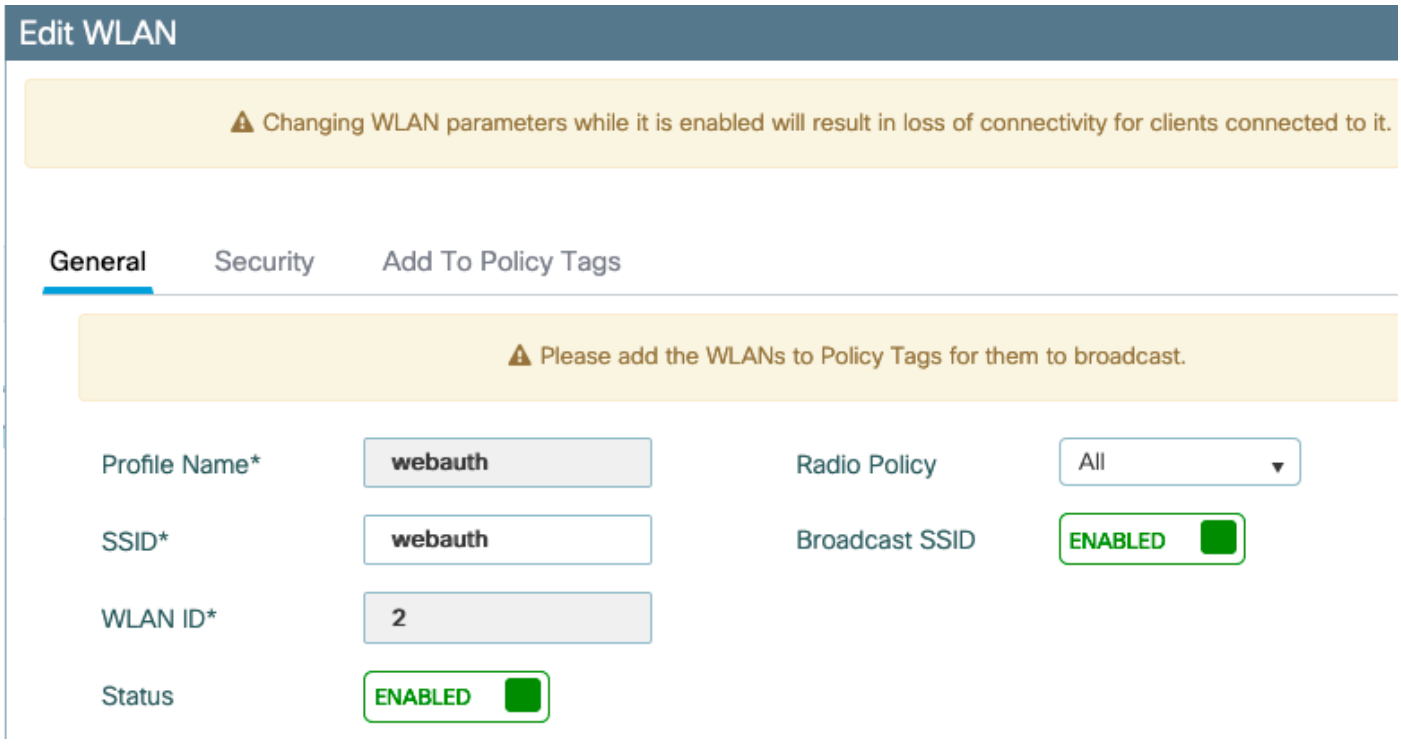
按一下「**Apply**」以儲存。

CLI命令：

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

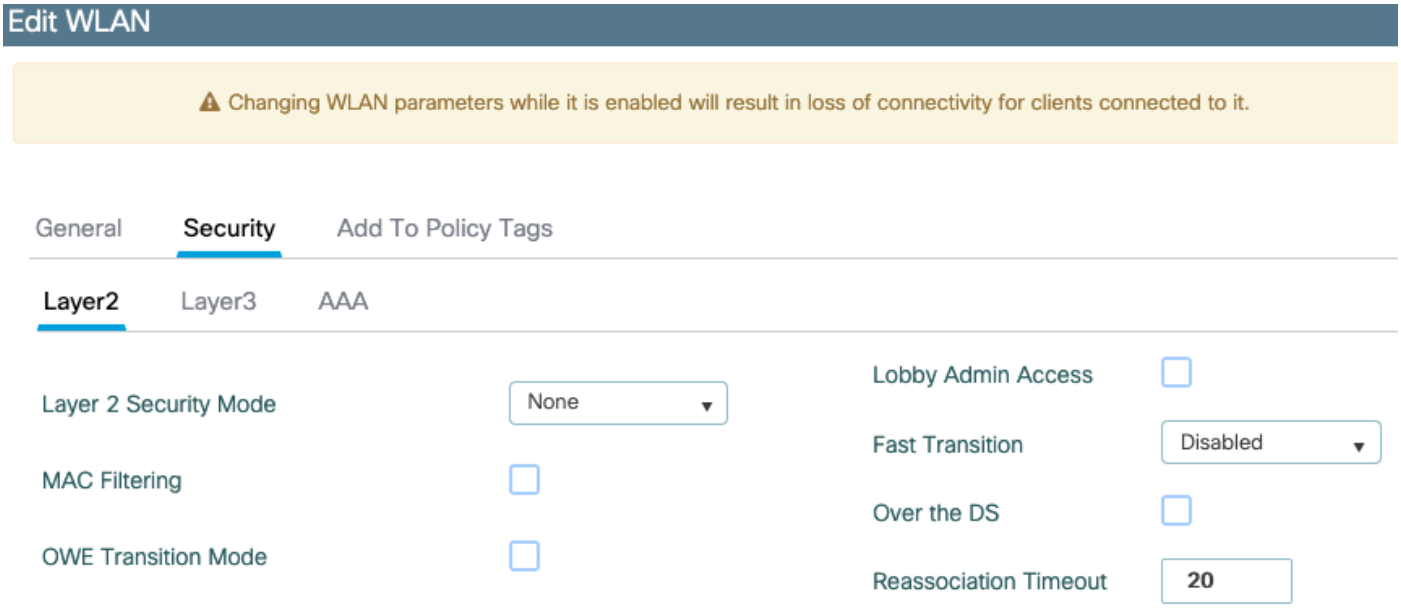
步驟7.設定webauth WLAN

導覽至Configuration > WLANs，然後按一下+Add

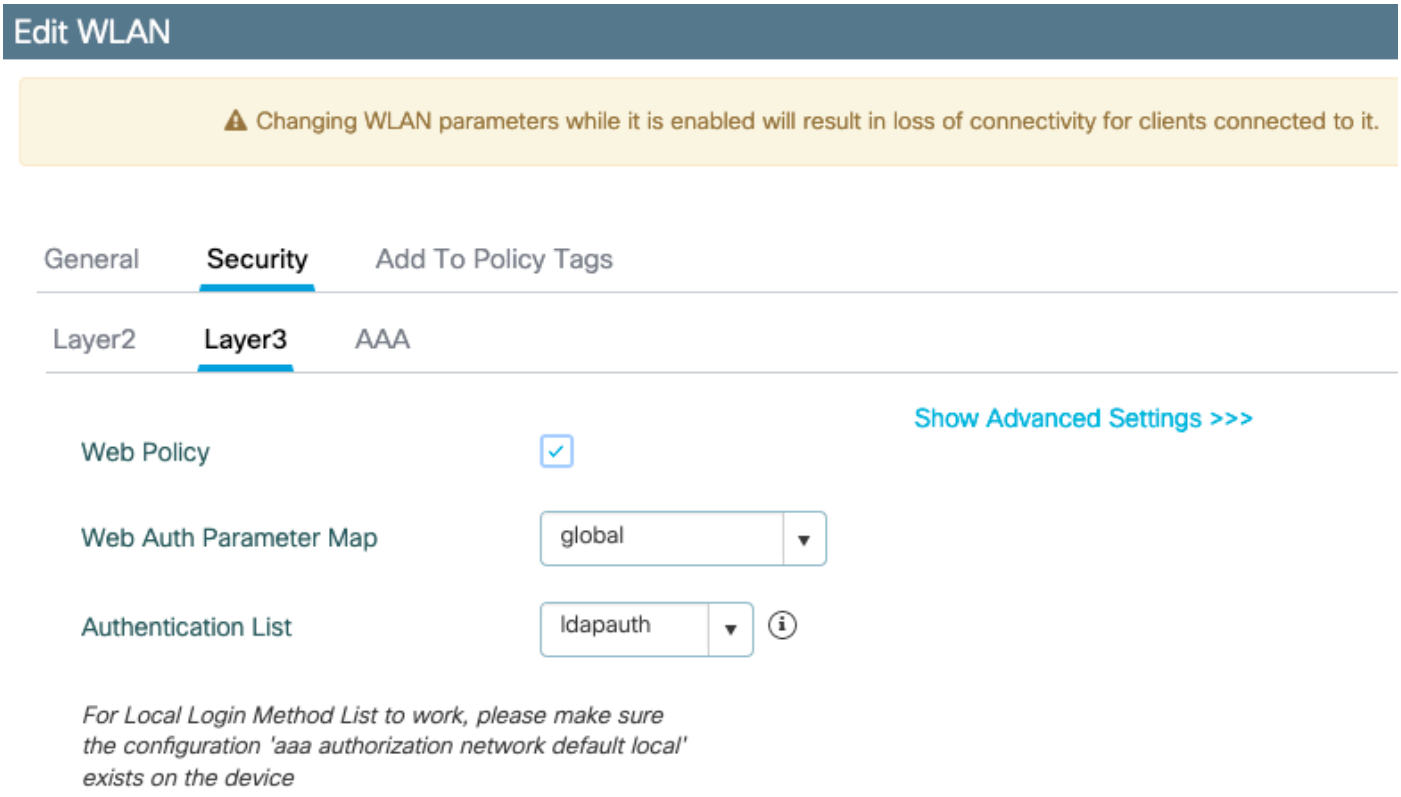


配置名稱，確保其處於啟用狀態，然後轉到**安全**頁籤。

在Layer 2子頁籤中，確保沒有安全性並禁用「快速轉換」。



在Layer3頁籤中，啟用Web**策略**，將引數對映設定為global，並將身份驗證清單設定為之前配置的aaa登入方法。



按一下「應用」**儲存**

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
```

步驟8.確保廣播了SSID

導航到**Configuration > Tags**，確保SSID包含在當前由SSID提供的策略配置檔案中（如果尚未配置標籤，則為全新配置預設策略標籤）。 預設情況下，default-policy-tag不會廣播您建立的新SSID，除非您手動包括這些SSID。

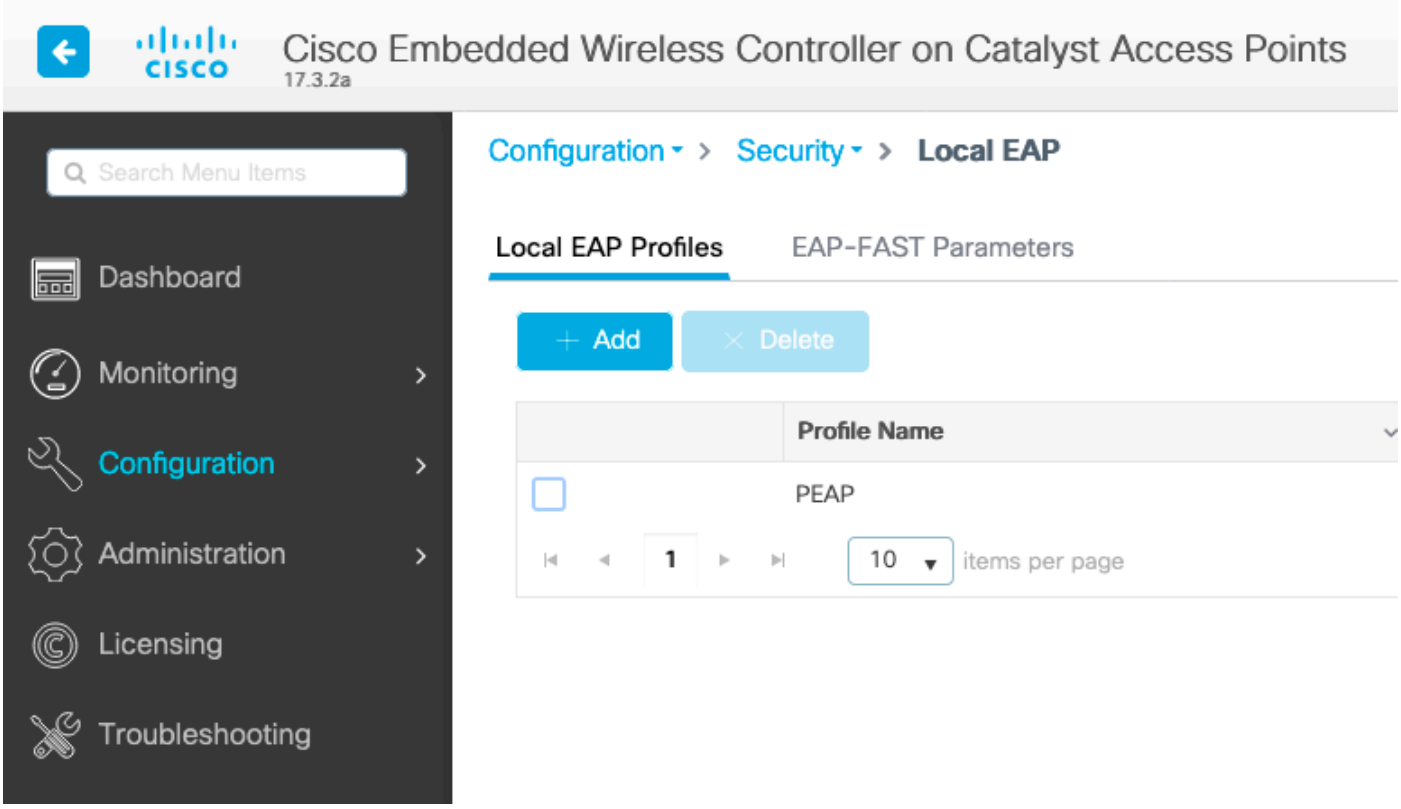
本文不涉及策略配置檔案的配置，假定您熟悉該部分配置。

使用dot1x SSID配置LDAP（使用本地EAP）

在9800上配置802.1X SSID的LDAP通常還需要配置本地EAP。如果您要使用RADIUS，則您的RADIUS伺服器將建立與LDAP資料庫的連線，這超出了本文的範圍。在嘗試此配置之前，建議首先在WLC上配置本地使用者來配置本地EAP，本文結尾的參考一節中提供了配置示例。完成後，您可以嘗試將使用者資料庫移至LDAP。

步驟1.配置本地EAP配置檔案

導航到**Configuration > Local EAP**，然後點選**+Add**



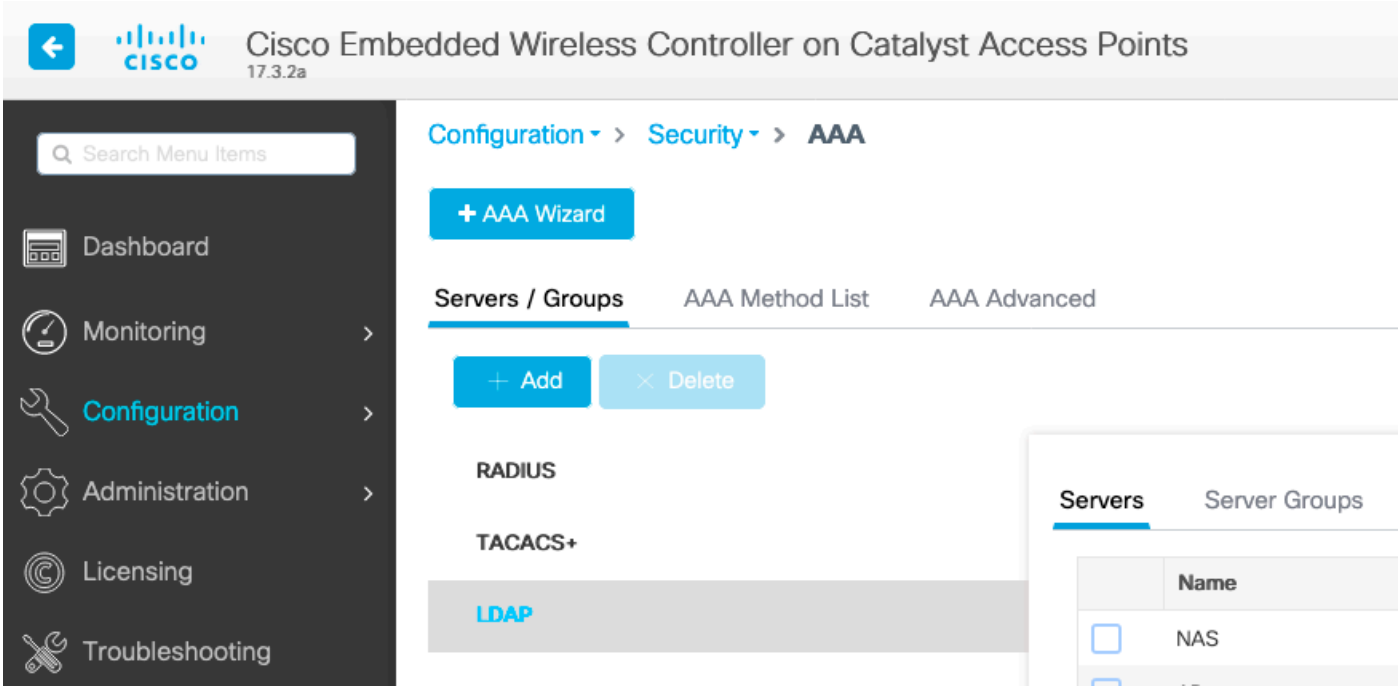
選擇配置檔案的任何名稱。至少啟用PEAP並選擇信任點名稱。預設情況下，您的WLC僅具有自簽名證書，因此您選擇哪個自簽名證書並不重要（通常TP-self-signed-xxxx是此用途的最佳自簽名證書），但是由於新的智慧手機OS版本信任自簽名證書越來越少，請考慮安裝受信任的公共簽名證書。

CLI命令：

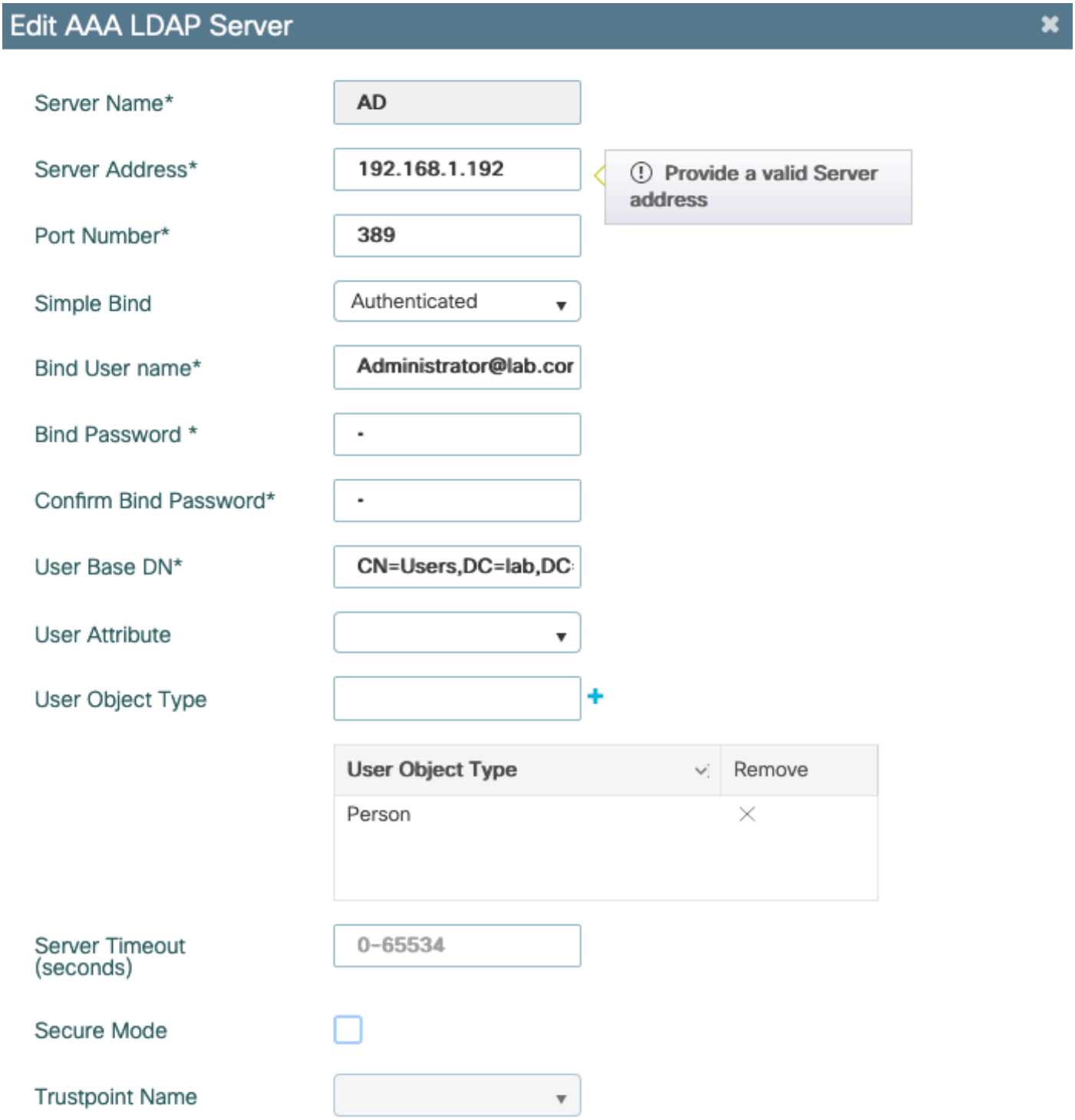
```
eap profile PEAP method peap pki-trustpoint TP-self-signed-3059261382
```

步驟2.配置LDAP伺服器

導航到**Configuration > Security > AAA> Servers/Groups > LDAP**，然後點選**+ Add**



為LDAP伺服器選擇名稱並填寫詳細資訊。有關每個欄位的說明，請參閱本文檔的「瞭解LDAP伺服器詳細資訊」部分。

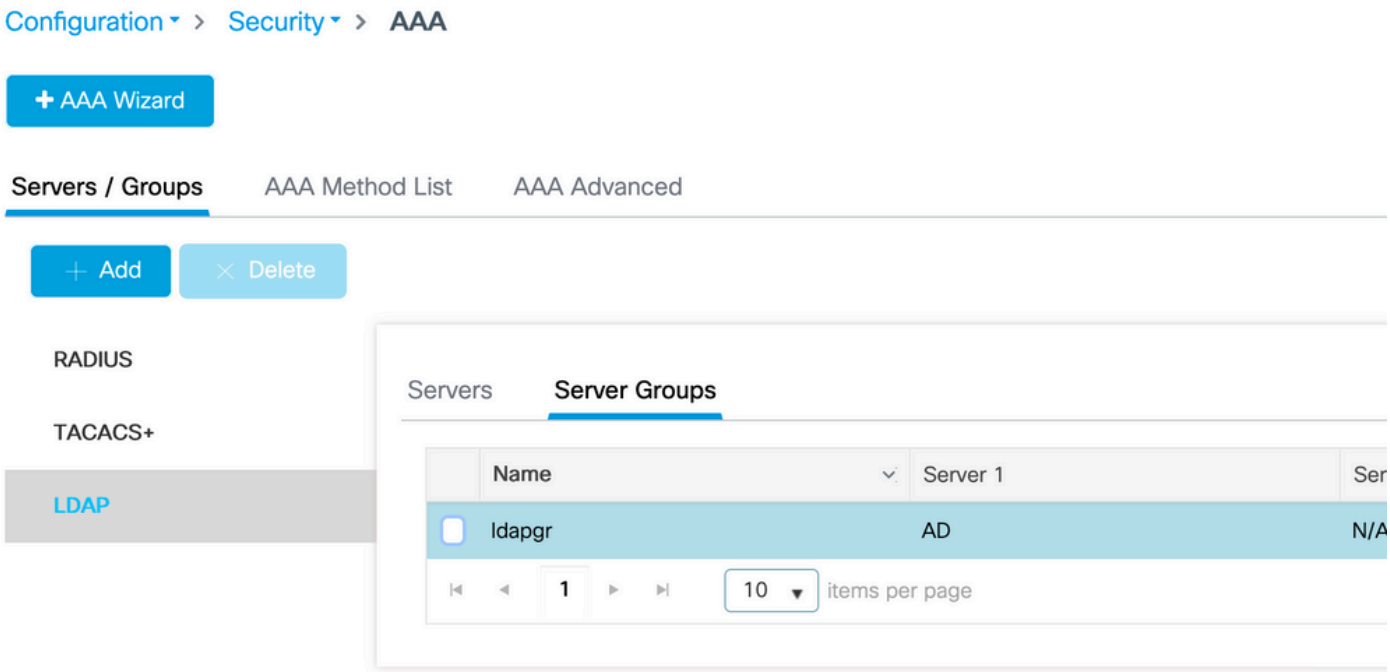


按一下Update and apply to device儲存

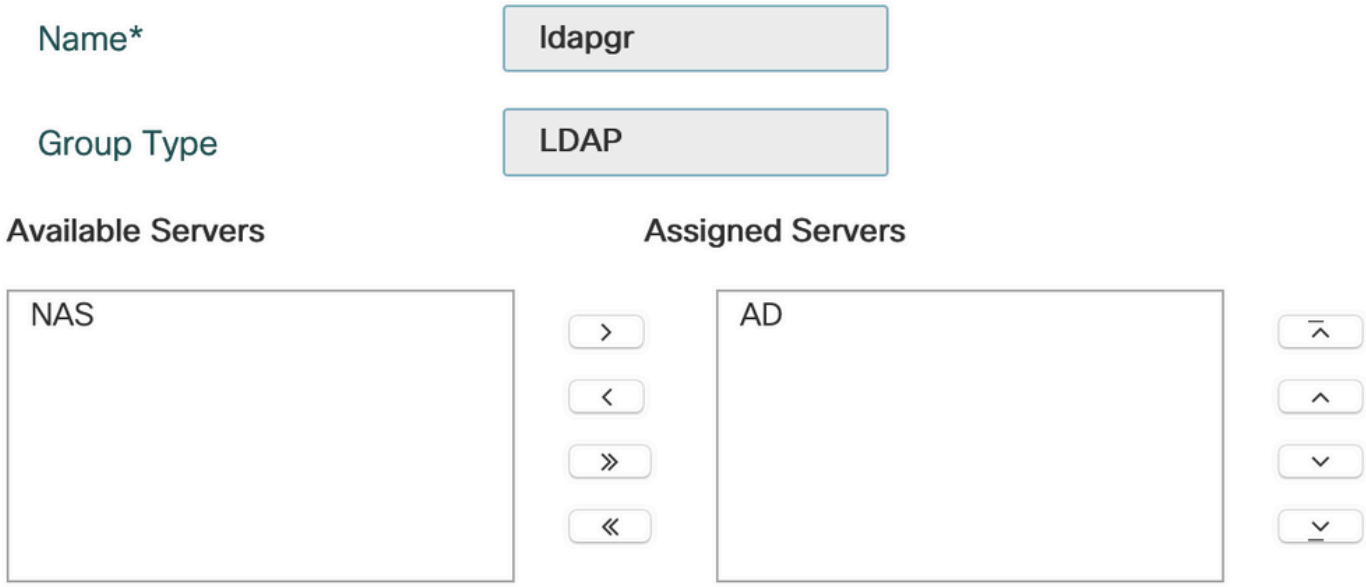
```
ldap server AD ipv4 192.168.1.192 bind authenticate root-dn Administrator@lab.com password 6
WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB base-dn CN=Users,DC=lab,DC=com search-filter user-object-type
Person
```

步驟3.配置LDAP伺服器組。

導航到Configuration > Security > AAA > Servers/Groups > LDAP > Server Groups，然後按一下+ADD



輸入名稱並新增在上一步中配置的LDAP伺服器。



按一下**Update and apply**儲存。

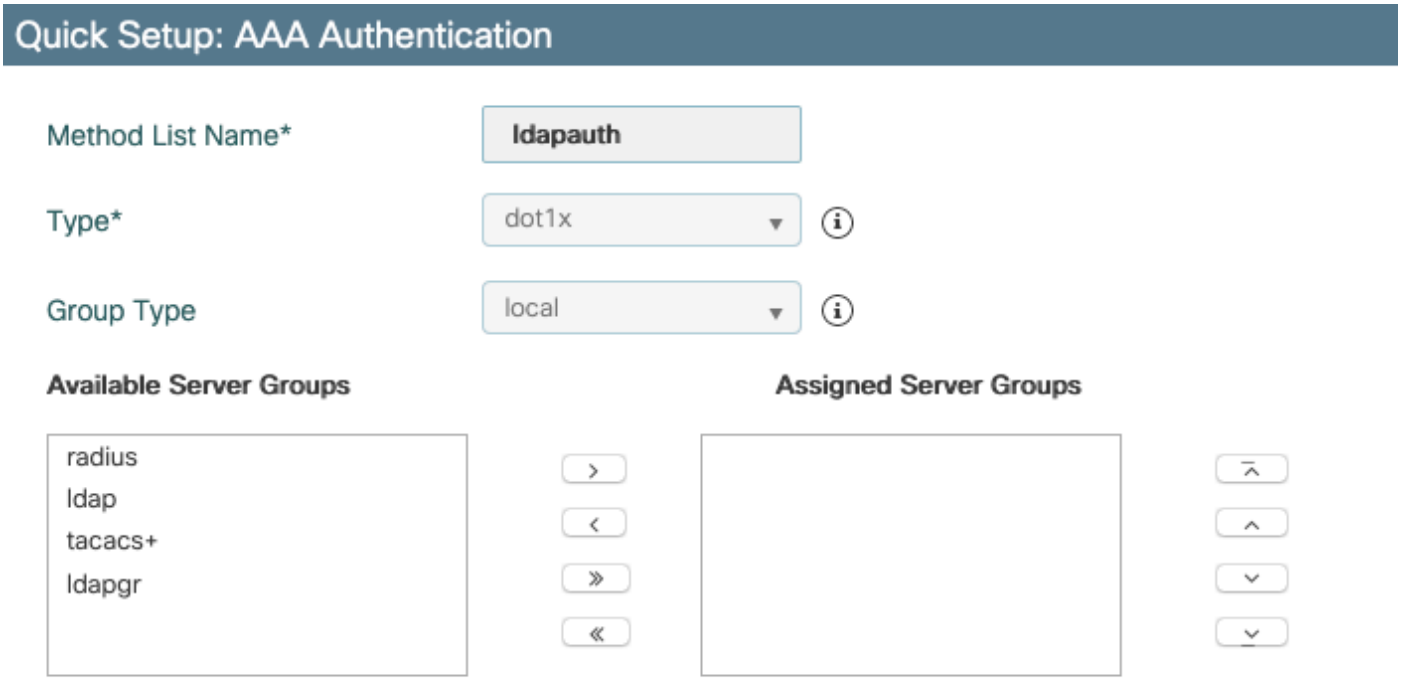
CLI命令：

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

步驟4.配置AAA身份驗證方法

導覽至**Configuration > Security > AAA > AAA Method List > Authentication**，然後按一下**+Add**

配置**dot1x**型別身份驗證方法，並將其僅指向本地。指向LDAP伺服器組是很有吸引力的，但這裡充當802.1X身份驗證器的是WLC本身（雖然使用者資料庫在LDAP上，但這是授權方法作業）。



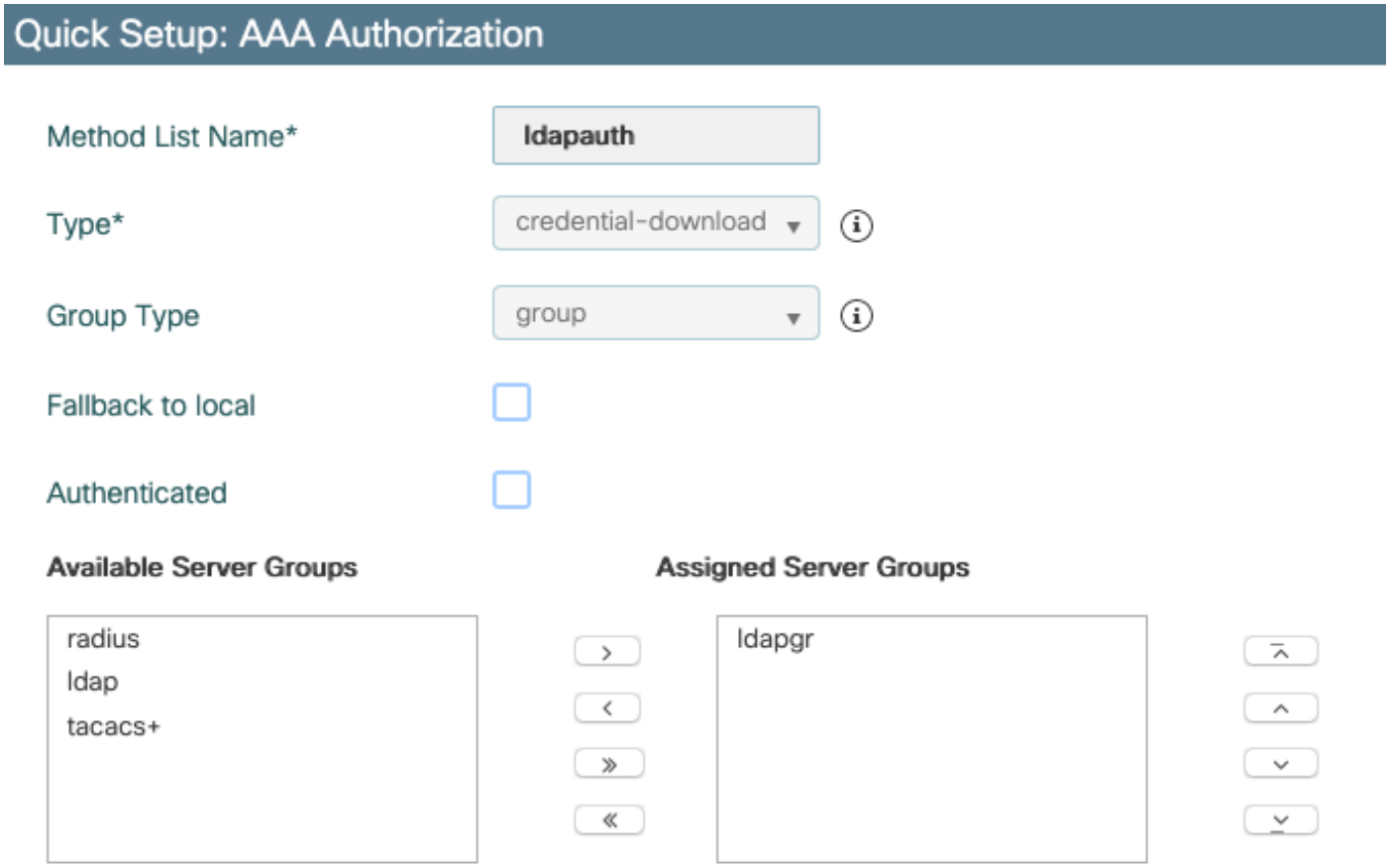
CLI命令：

```
aaa authentication dot1x ldapauth local
```

步驟5.配置AAA授權方法

導覽至**Configuration > Security > AAA > AAA Method List > Authorization**，然後按一下**+Add**

建立**憑據下載**型別的授權方法，並使其指向LDAP組。



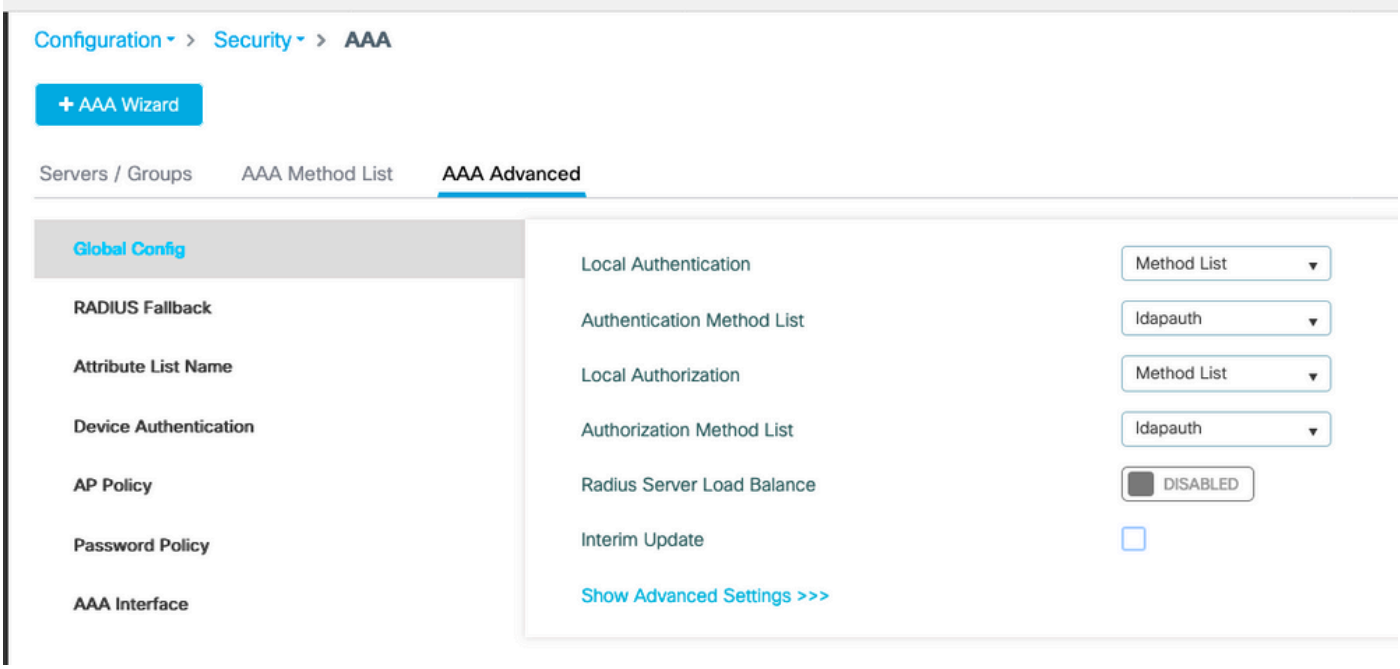
CLI命令：

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

步驟6.配置本地身份驗證詳細資訊

導覽至**Configuration > Security > AAA > AAA Method List > AAA Advanced**

選擇**Method List**進行身份驗證和授權，並選擇本地指向的dot1x身份驗證方法和指向LDAP的憑據下載授權方法



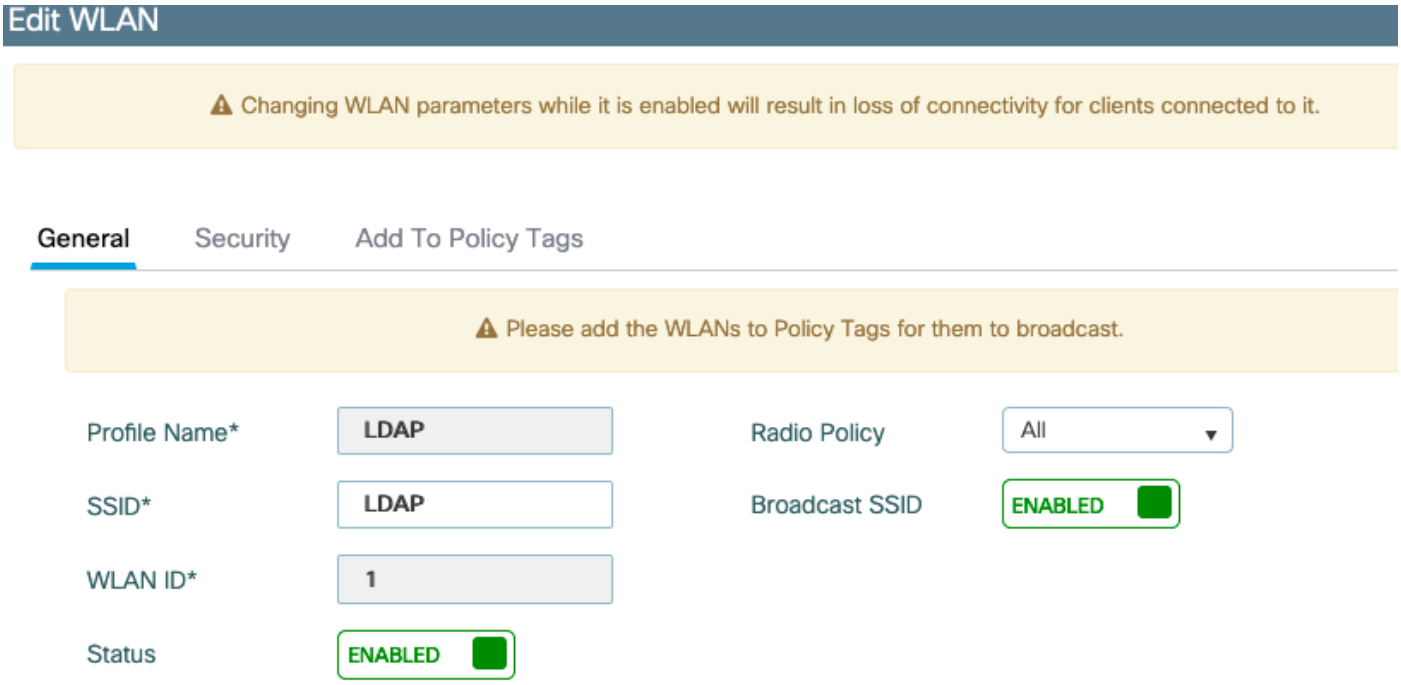
CLI命令：

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

步驟7.配置dot1x WLAN

導覽至**Configuration > WLAN**，然後按一下**+Add**

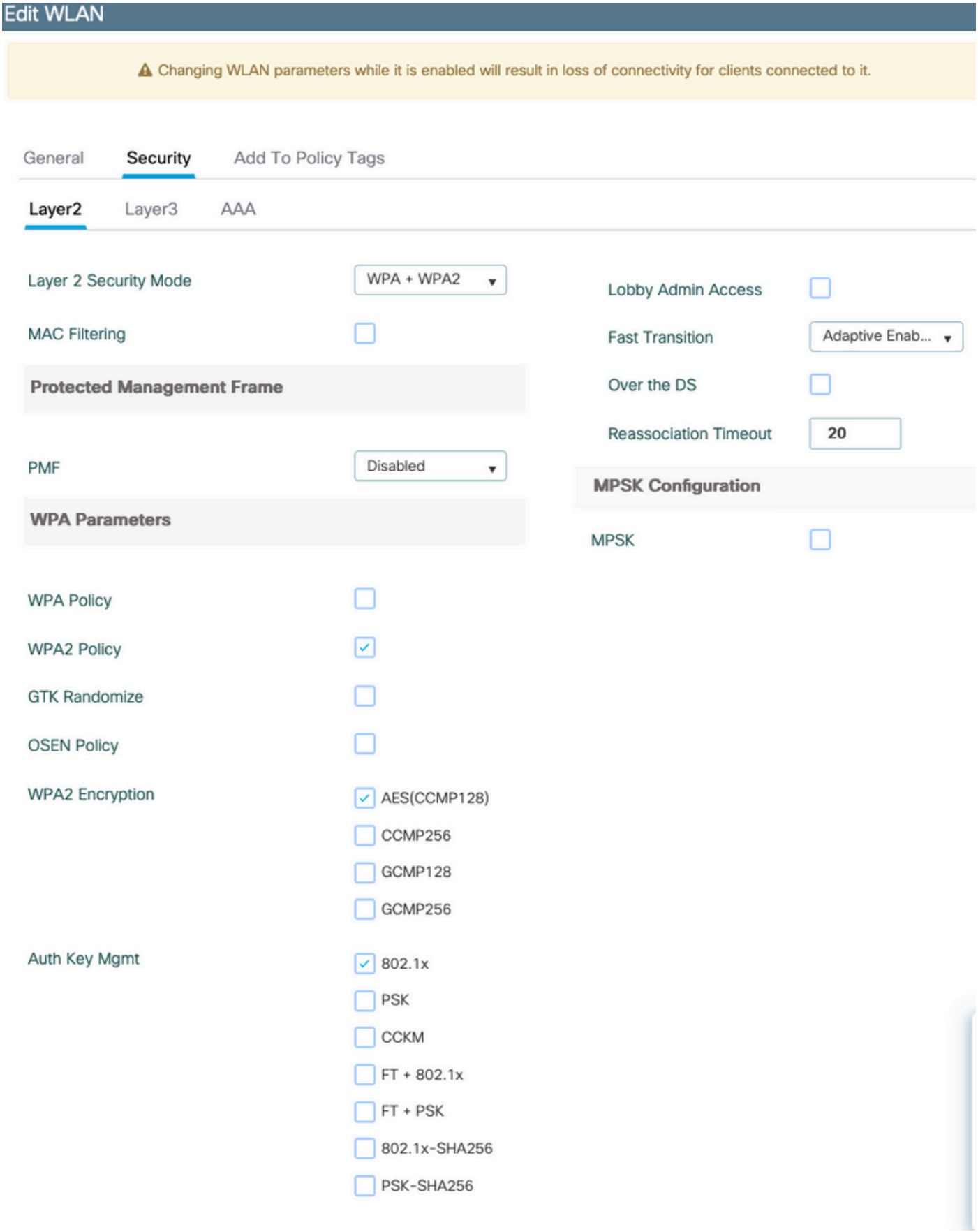
選擇配置檔案和SSID名稱並確保已啟用。



移至第2層安全**選項**卡。

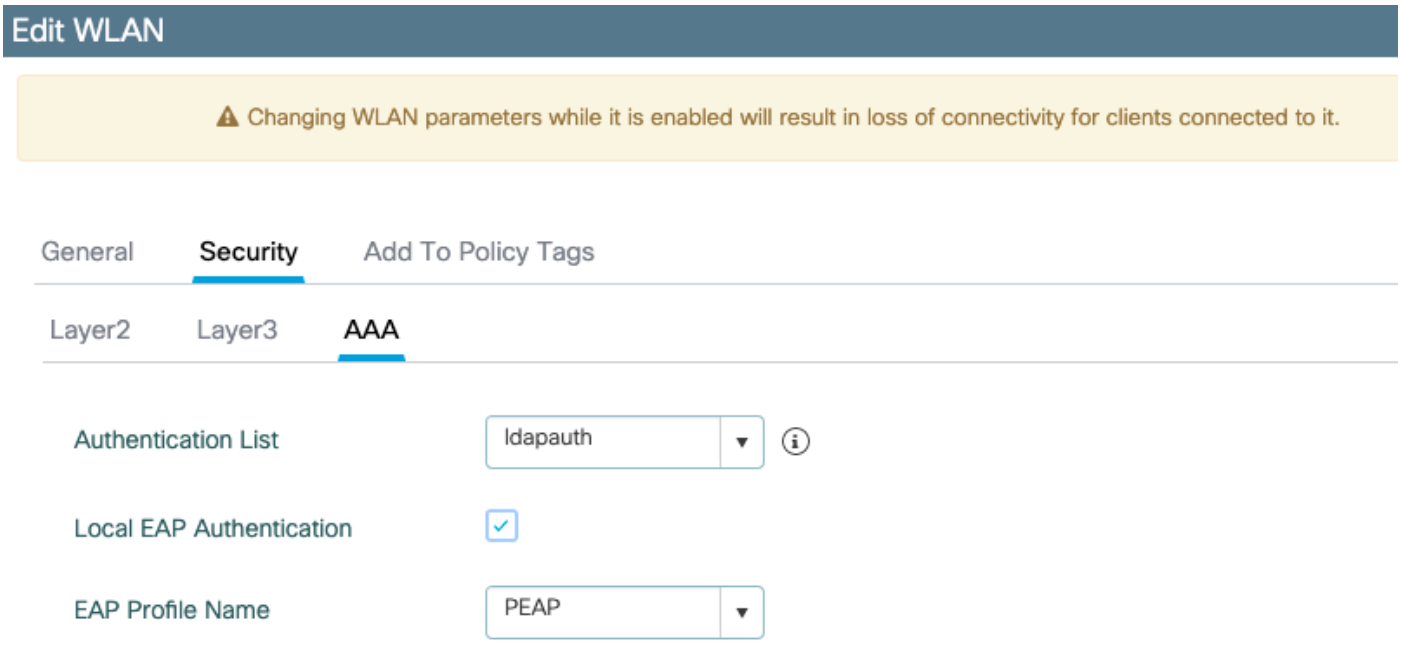
選擇WPA+WPA2作為**第2層安全模式**

確保在WPA引數中啟用了WPA2和AES，並啟用**802.1X**



轉到**AAA**子頁籤。

選擇先前建立的dot1x身份驗證方法，啟用本地EAP身份驗證，並選擇第一步中配置的EAP配置檔案。



按一下應用儲存

CLI命令：

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

步驟8.驗證是否已廣播WLAN

導航到**Configuration > Tags**，確保SSID包含在當前由SSID提供的策略配置檔案中（如果尚未配置標籤，則為全新配置預設策略標籤）。 預設情況下，default-policy-tag不會廣播您建立的新SSID，除非您手動包括這些SSID。

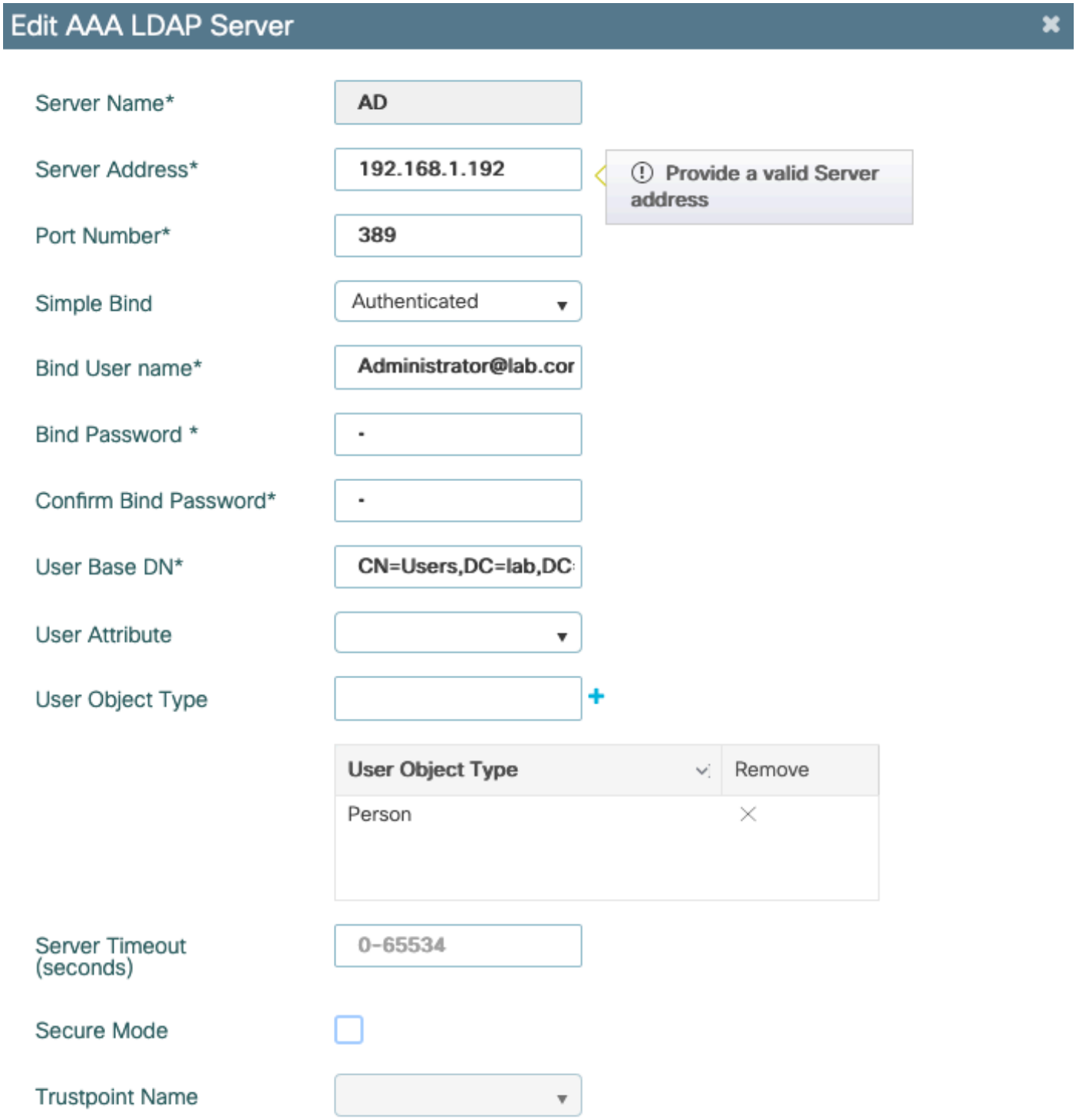
本文不涉及策略配置檔案的配置，假定您熟悉該部分配置。

如果使用Active Directory，則必須配置AD伺服器以傳送屬性「userPassword」。 此屬性需要傳送到WLC。這是因為WLC執行驗證，而不是AD伺服器。您也可能遇到使用PEAP-mschapv2方法進行身份驗證的問題，因為密碼從未以明文形式傳送，因此無法通過LDAP資料庫進行檢查，只有PEAP-GTC方法適用於某些LDAP資料庫。

瞭解LDAP伺服器詳細資訊

瞭解9800 Web UI上的欄位

以下是一個非常基本的Active Directory的示例，它用作9800上配置的LDAP伺服器



名稱和IP可能是不言自明的。

連接埠:389是LDAP的預設埠，但您的伺服器可以使用其他埠。

簡單繫結：現在很少有支援未經驗證繫結的LDAP資料庫（這意味著任何人都可以在它上進行LDAP搜尋，而無需任何驗證形式）。 經過身份驗證的簡單繫結是最常見的身份驗證型別，預設情況下是Active Directory允許的。可以輸入管理員帳戶名和密碼，以便能夠在使用者資料庫中搜尋。

繫結使用者名稱：您需要在Active Directory中指向具有管理員許可權的使用者名稱。AD允許使用「user@domain」格式，而許多其他LDAP資料庫期望使用者名稱使用「CN=xxx，DC=xxx」格式。本文稍後將提供另一個LDAP資料庫而不是AD的示例。

繫結密碼：輸入管理員使用者名稱之前輸入的密碼。

使用者基礎DN:在此處輸入「搜尋根」，即LDAP樹中搜尋開始的位置。在本示例中，我們所有的使用都位於「Users」組中，其DN是「CN=Users，DC=lab，DC=com」(因為示例LDAP域是lab.com)。 本節稍後部分提供了如何找到此使用者基礎DN的示例。

使用者屬性：該欄位可以留空，或者指向指示將哪個LDAP欄位計為LDAP資料庫的使用者名稱的LDAP屬性對映。但是，由於思科錯誤ID CSCvv11813 中，WLC會嘗試使用CN欄位進行驗證，無論結果如何。

使用者對象型別：這將確定被視為使用者的對象的型別。通常這是「人」。 如果您擁有AD資料庫並驗證電腦帳戶，則它可能是「電腦」，但同樣，LDAP提供了大量自定義功能。

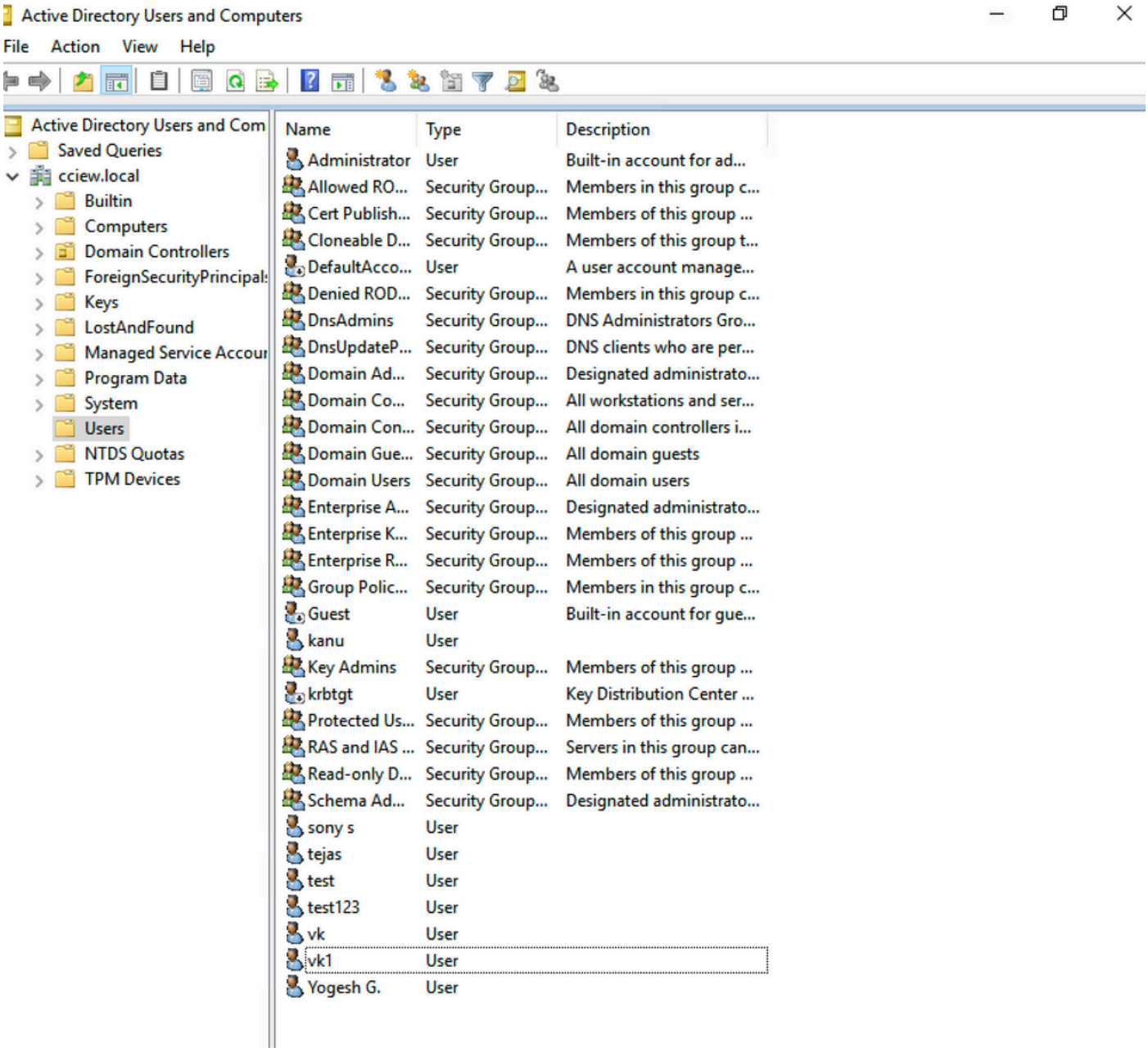
安全模式啟用通過TLS的安全LDAP，並要求您在9800上選擇一個信任點以使用證書進行TLS加密。

具有sAMAaccountName屬性的LDAP 802.1x身份驗證。

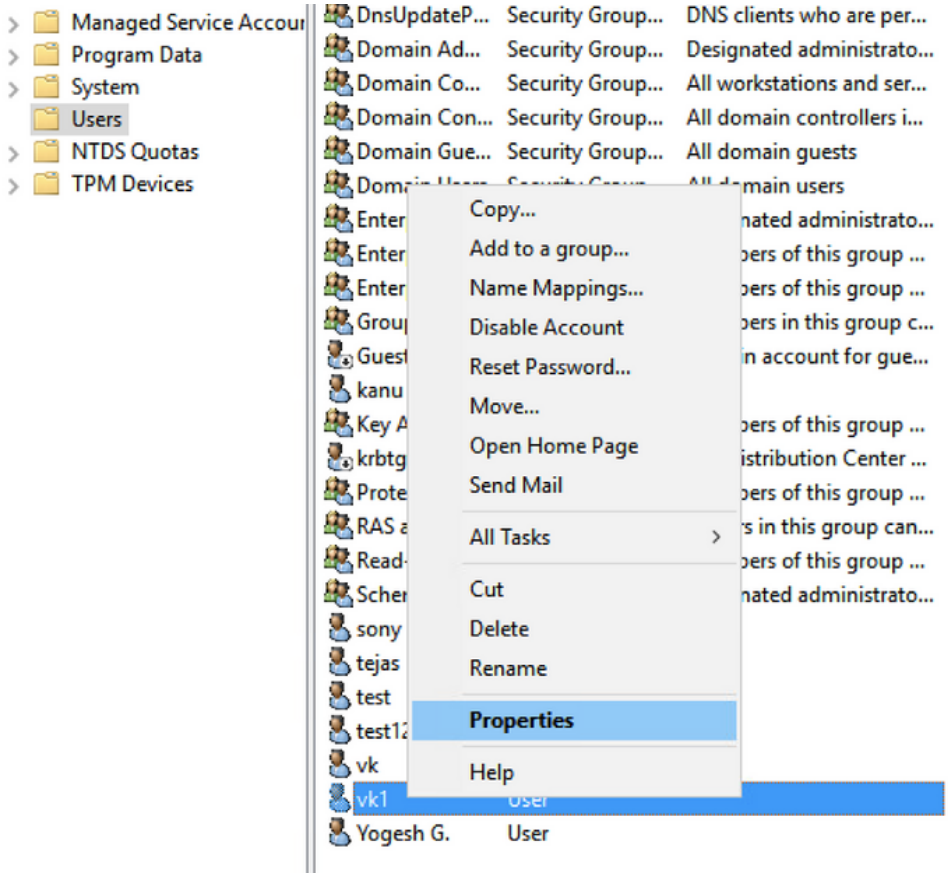
此增強功能是在17.6.1版中匯入。

配置使用者的「userPassword」屬性。

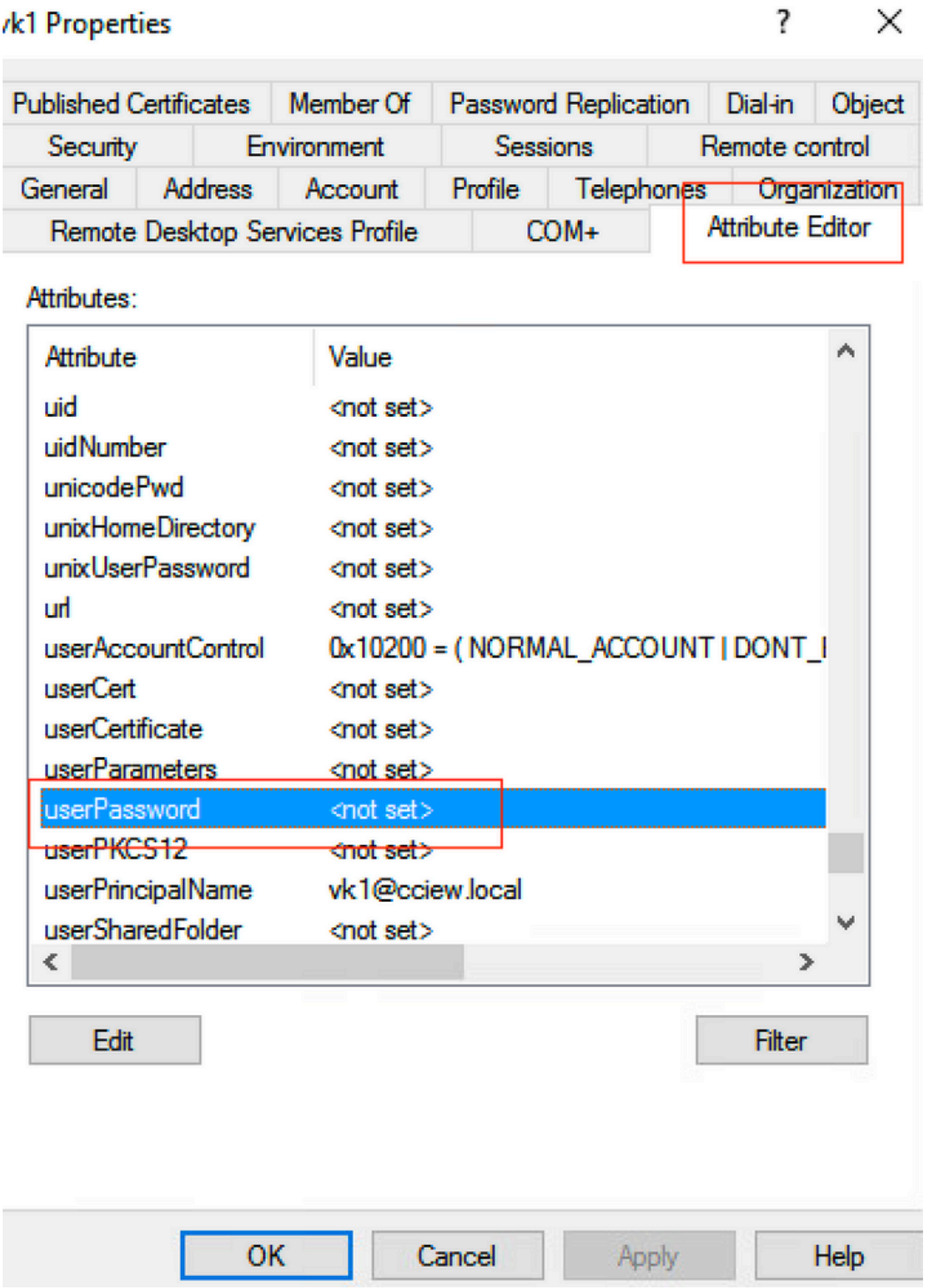
步驟1.在Windows伺服器上，導航至ActiveDirectory使用者和電腦



步驟2.按一下右鍵各自的使用者名稱並選擇屬性



步驟3.在屬性視窗中選擇屬性編輯器



步驟4.配置「userPassword」屬性。這是使用者的密碼，需要以十六進位制值配置。

vk1 Properties

Published Certificates | Member Of | Password Replication | Dial-in | Object

Security | Environment | Sessions | Remote control

General | Address | Account | Profile | Telephones | Organization

Multi-valued Octet String Editor

Attribute: userPassword

Values:

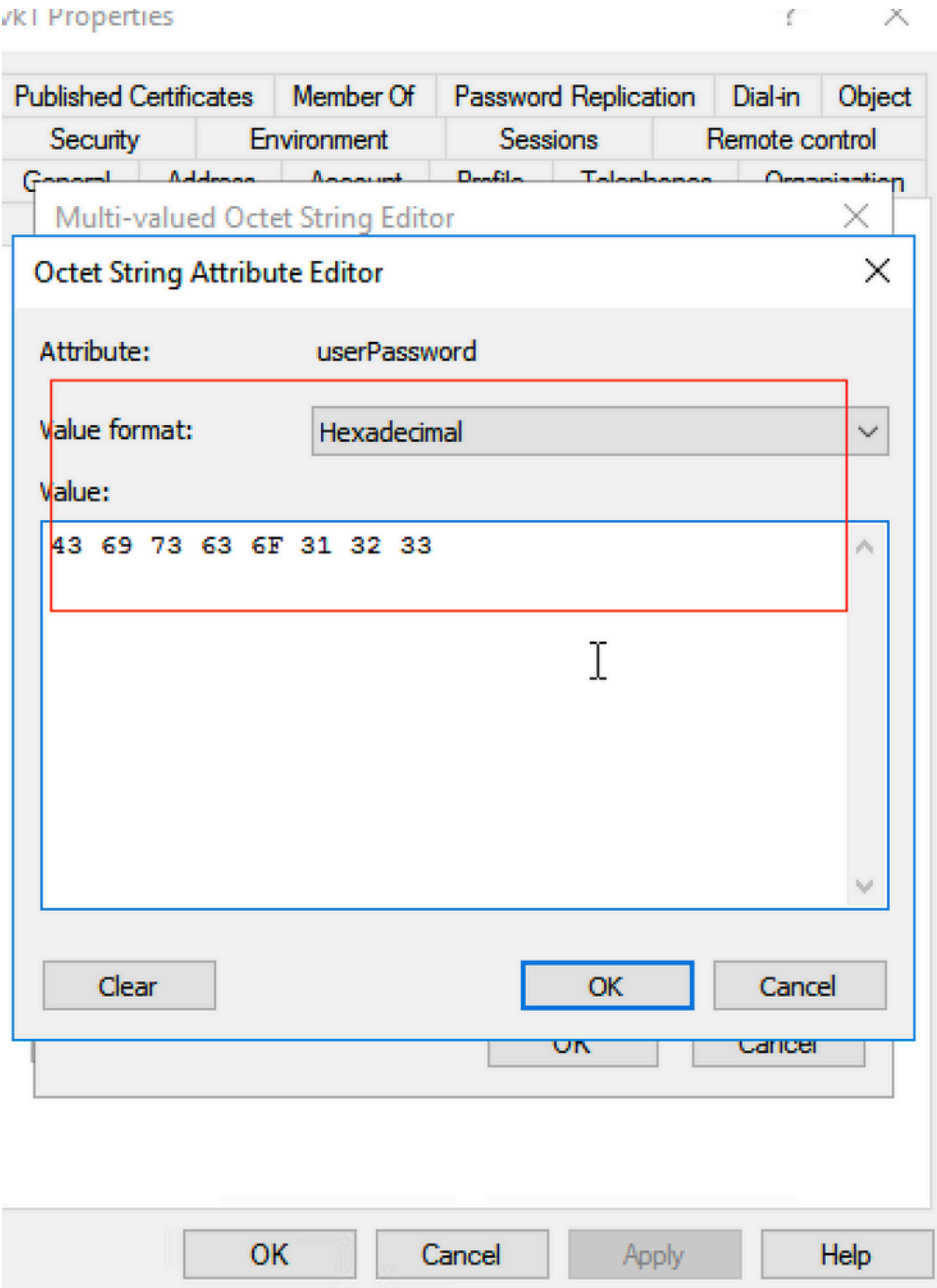
Add

Remove

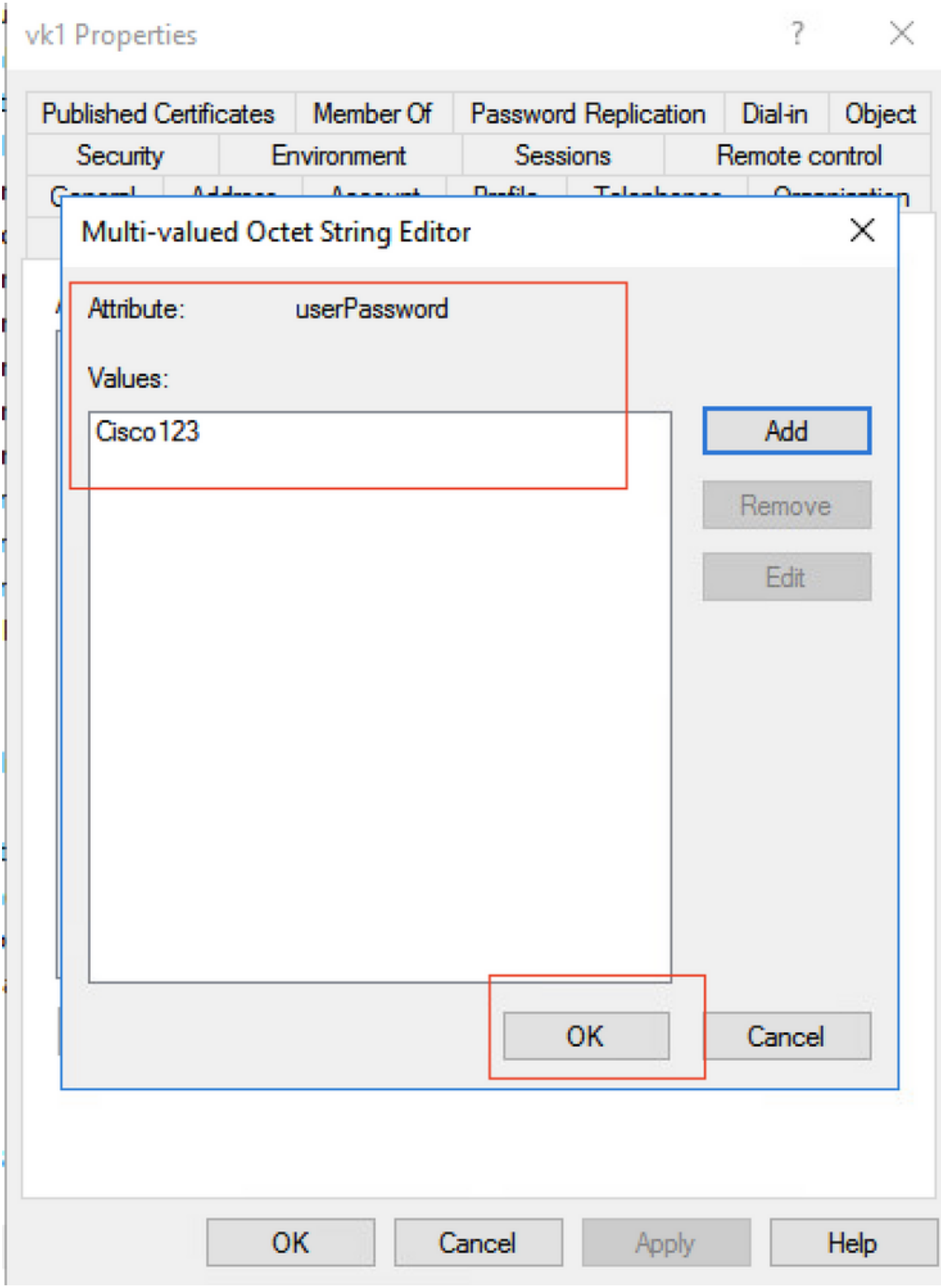
Edit

OK

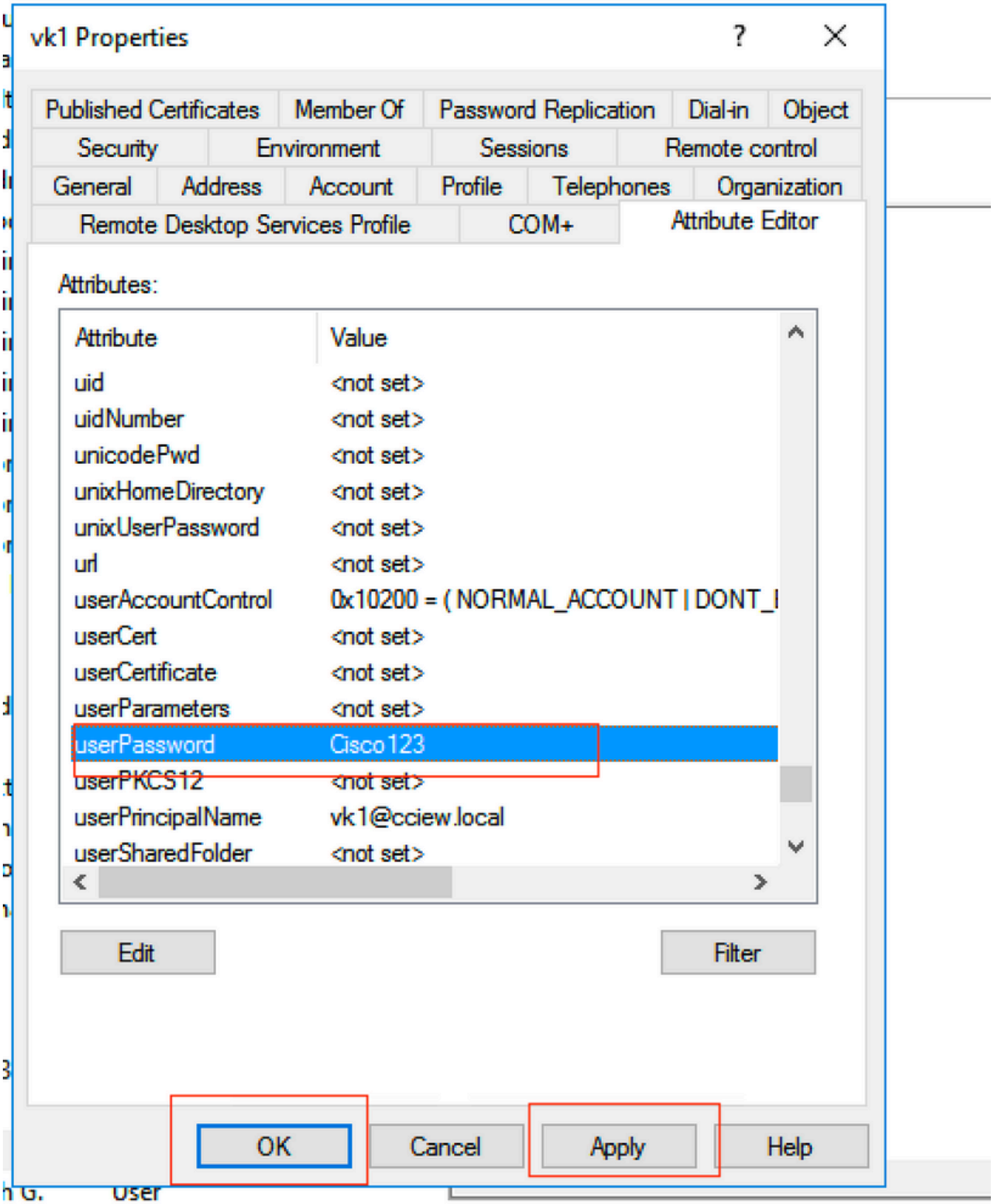
Cancel



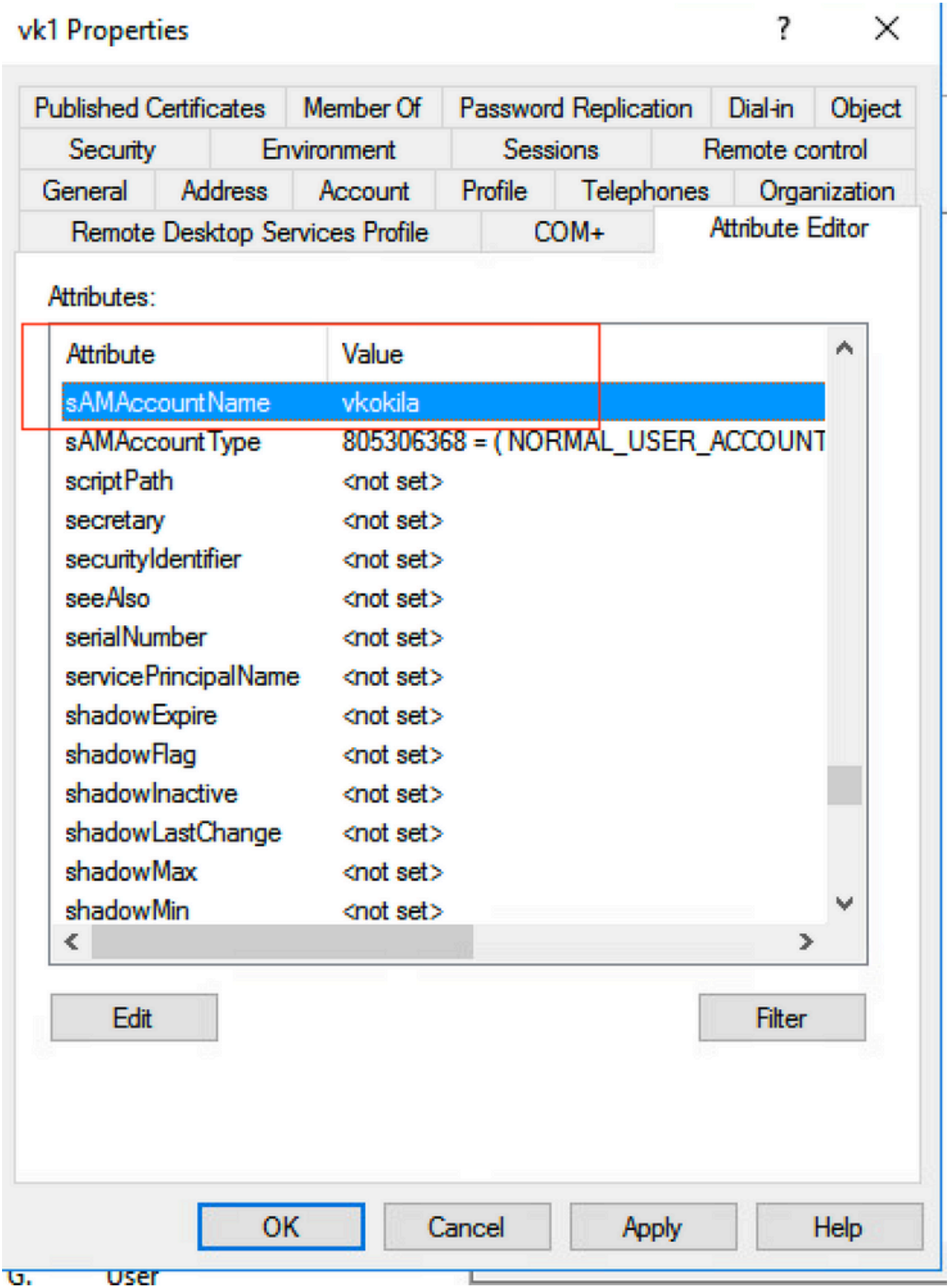
按一下確定，驗證它是否顯示正確的密碼



步驟5.按一下Apply，然後按一下OK



步驟6.驗證使用者的「sAMAccountName」屬性值以及驗證的使用者名稱。


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
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>
Edit
Filter
OK
Cancel
Apply
Help

WLC組態：

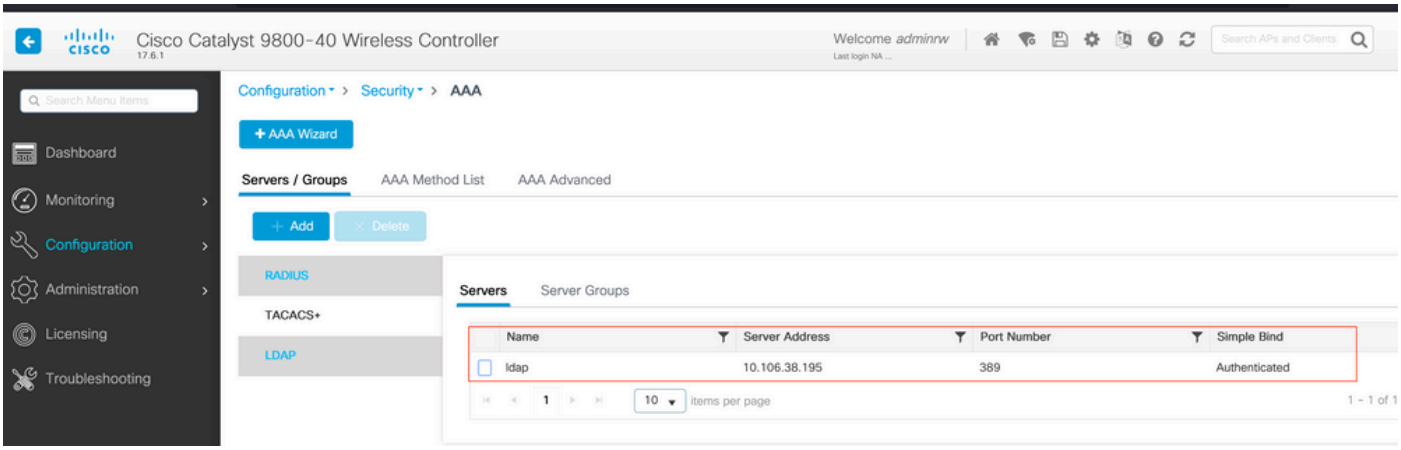
步驟1.建立LDAP屬性對映

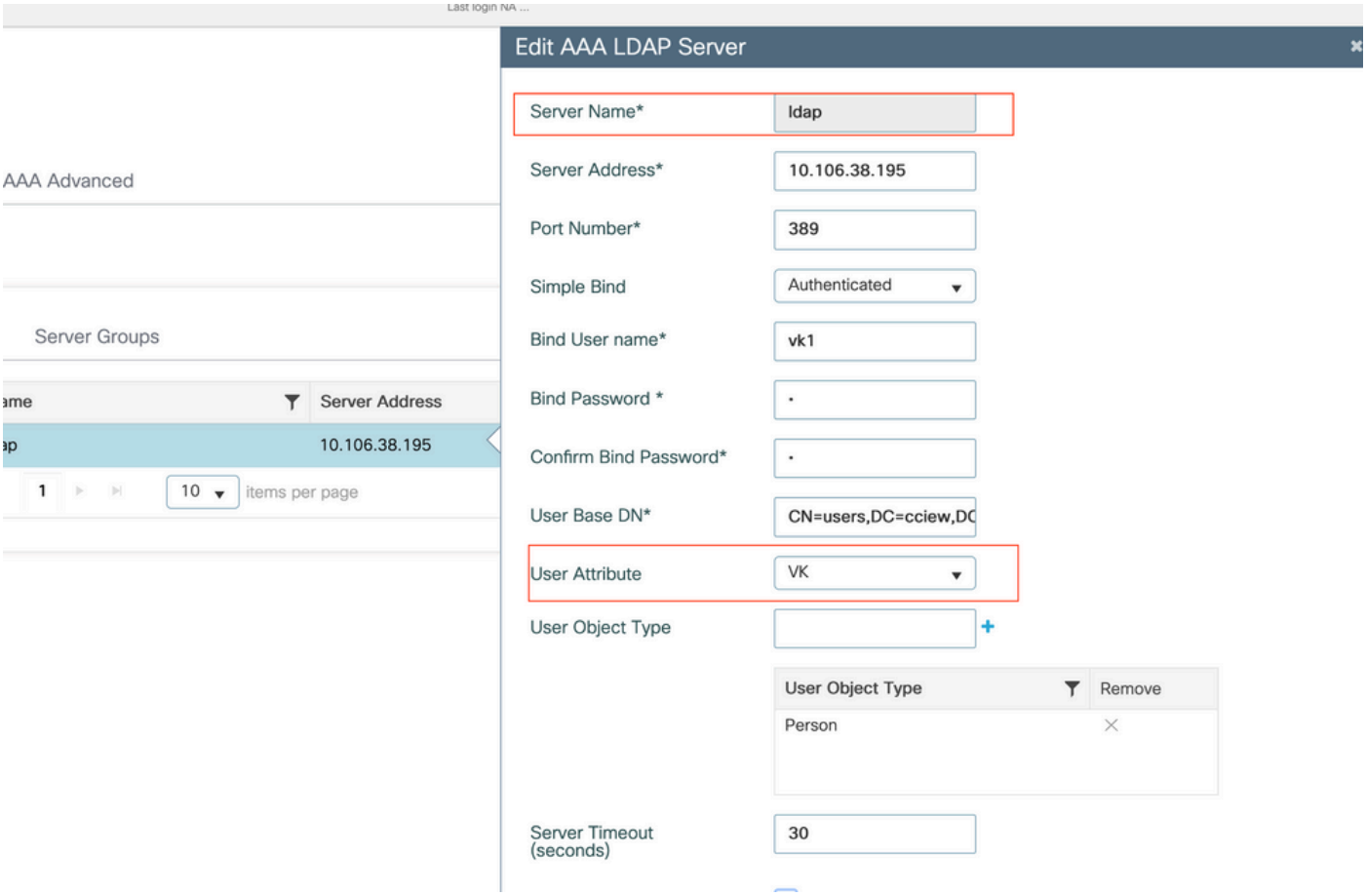
步驟2.配置「sAMAccountName」屬性並鍵入「username」

步驟3.在LDAP伺服器配置下選擇建立的屬性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
```

從Web介面驗證：





驗證

要驗證您的配置，請使用本文中的CLI命令仔細檢查。

LDAP資料庫通常不提供身份驗證日誌，因此可能很難知道發生了什麼情況。請訪問本文的故障排除部分，以瞭解如何執行跟蹤和監聽器捕獲，以便檢視是否已建立與LDAP資料庫的連線。

疑難排解

要解決此問題，最好將其分為兩個部分。第一部分是驗證本地EAP部分。第二個是驗證9800是否與LDAP伺服器正確通訊。

如何在控制器上驗證身份驗證過程

可以收集放射性跟蹤以便獲取客戶端連線的「調試」。

只需轉到**故障排除>放射性跟蹤**。新增客戶端MAC地址（注意您的客戶端可以使用隨機MAC而不是自己的MAC，您可以在客戶端裝置本身的SSID配置檔案中驗證這一點）並點選start。

重現連線嘗試後，可以按一下「生成」獲取最近X分鐘的日誌。確保按一下**internal**，因為如果您不啟用某些LDAP日誌行，則不會顯示。

以下是客戶端在Web身份驗證SSID上成功進行身份驗證的輻射跟蹤示例。為了清楚起見，刪除了一些冗餘部件：

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):

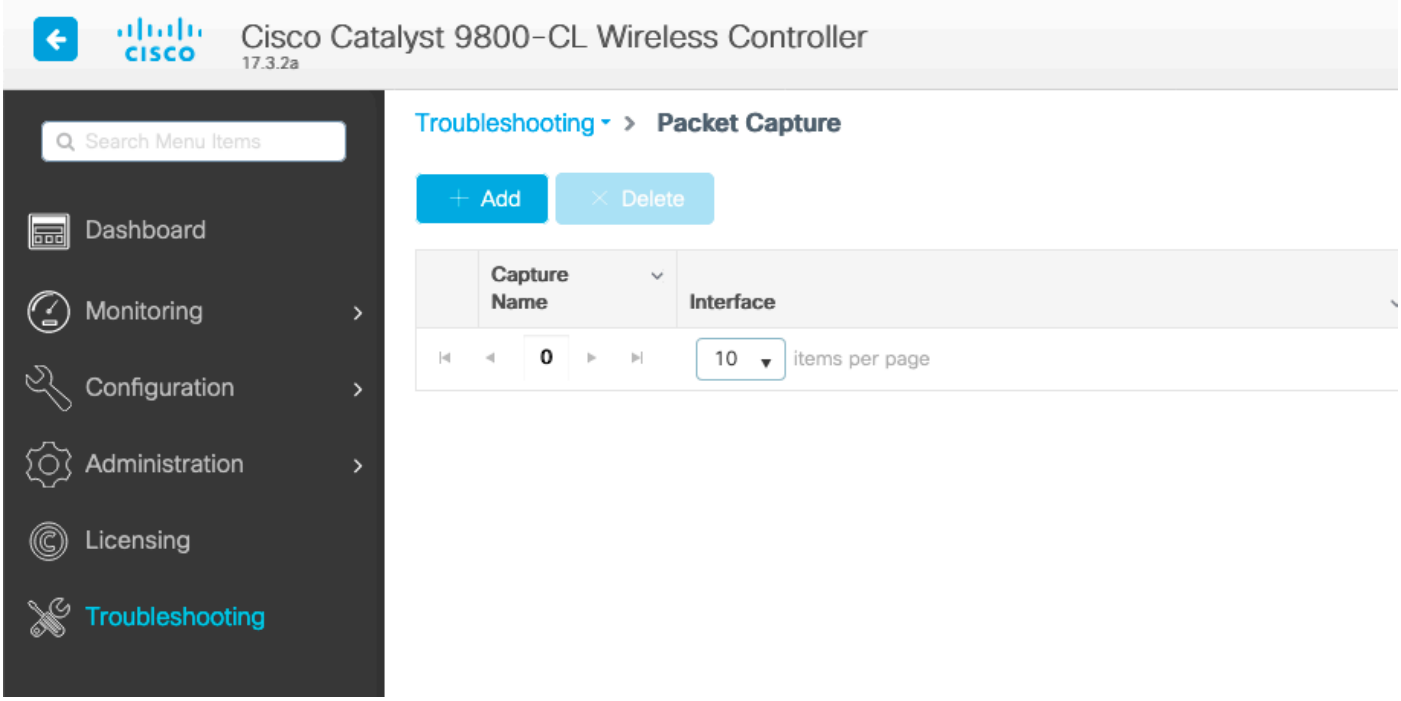
[2e1f.3a65.9c09:capwap_90000004] Check aaa acct configured 2021/01/19 21:58:06.720716 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:capwap_90000004] access_session_acct_filter_spec is NULL 2021/01/19 21:58:06.724036 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004]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

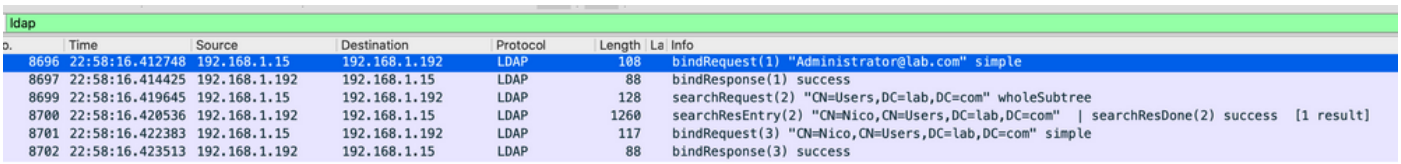
如何驗證9800到LDAP的連線

您可以在9800中執行嵌入式捕獲，以便檢視哪些流量流向LDAP。

若要從WLC進行擷取，請導覽至**疑難排解>封包擷取**，然後按一下**+Add**。選擇上行鏈路埠並開始捕獲。



以下是使用者Nico的成功驗證示**例**



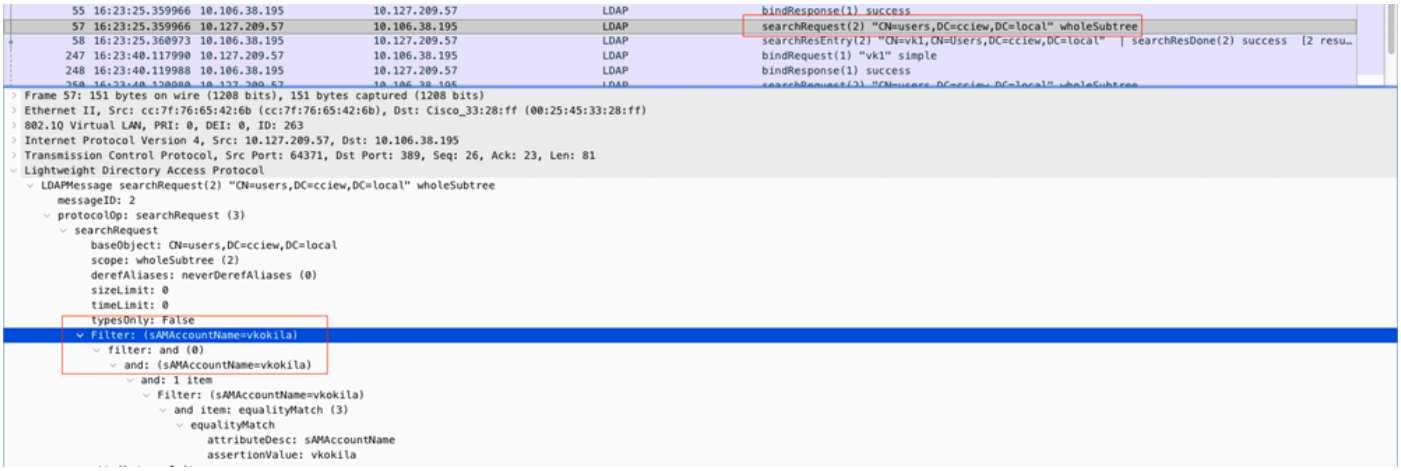
No.	Time	Source	Destination	Protocol	Length	La	Info
8696	22:58:16.412748	192.168.1.15	192.168.1.192	LDAP	108		bindRequest(1) "Administrator@lab.com" simple
8697	22:58:16.414425	192.168.1.192	192.168.1.15	LDAP	88		bindResponse(1) success
8699	22:58:16.419645	192.168.1.15	192.168.1.192	LDAP	128		searchRequest(2) "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個資料包代表與LDAP資料庫的WLC繫結，即WLC使用管理員使用者向資料庫進行身份驗證（以便執行搜尋）。

這2個LDAP封包代表WLC在基礎DN中執行搜尋（這裡CN=Users，DC=lab，DC=com）。 封包的內部包含使用者名稱的篩選條件（這裡為「Nico」）。 LDAP資料庫成功返回使用者屬性

最後2個封包代表嘗試使用該使用者密碼進行驗證以測試密碼是否正確的WLC。

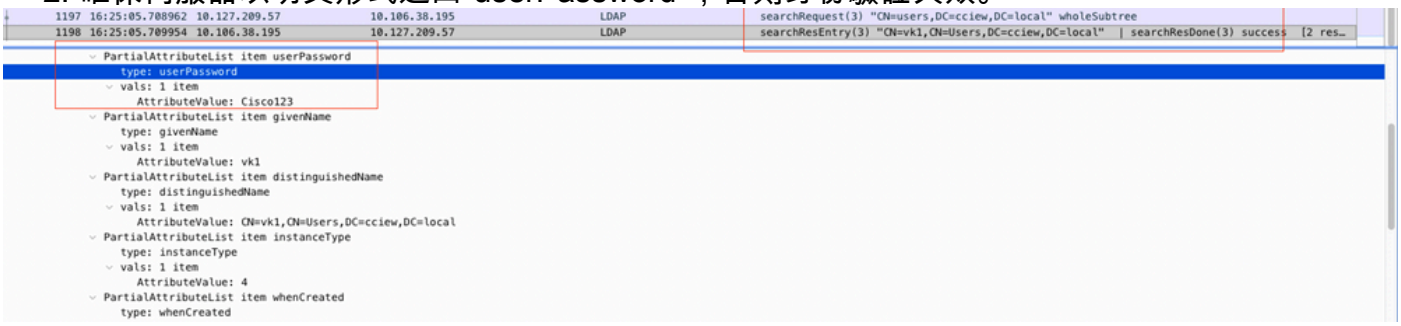
1. 收集EPC並檢查是否將「sAMAccountName」應用為篩選器：



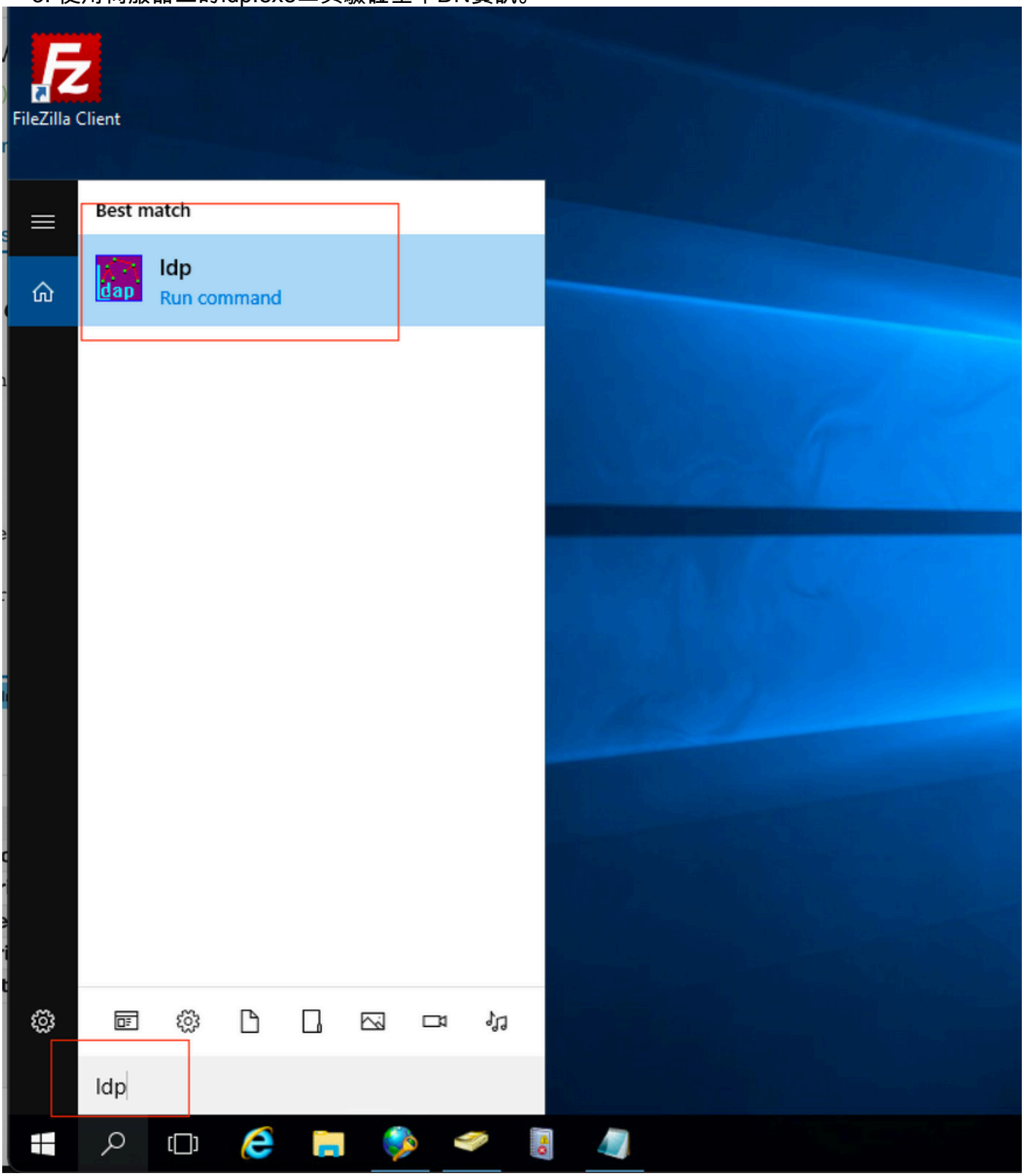
如果過濾器顯示「cn」且正在使用「sAMAccountName」作為使用者名稱，則驗證失敗。

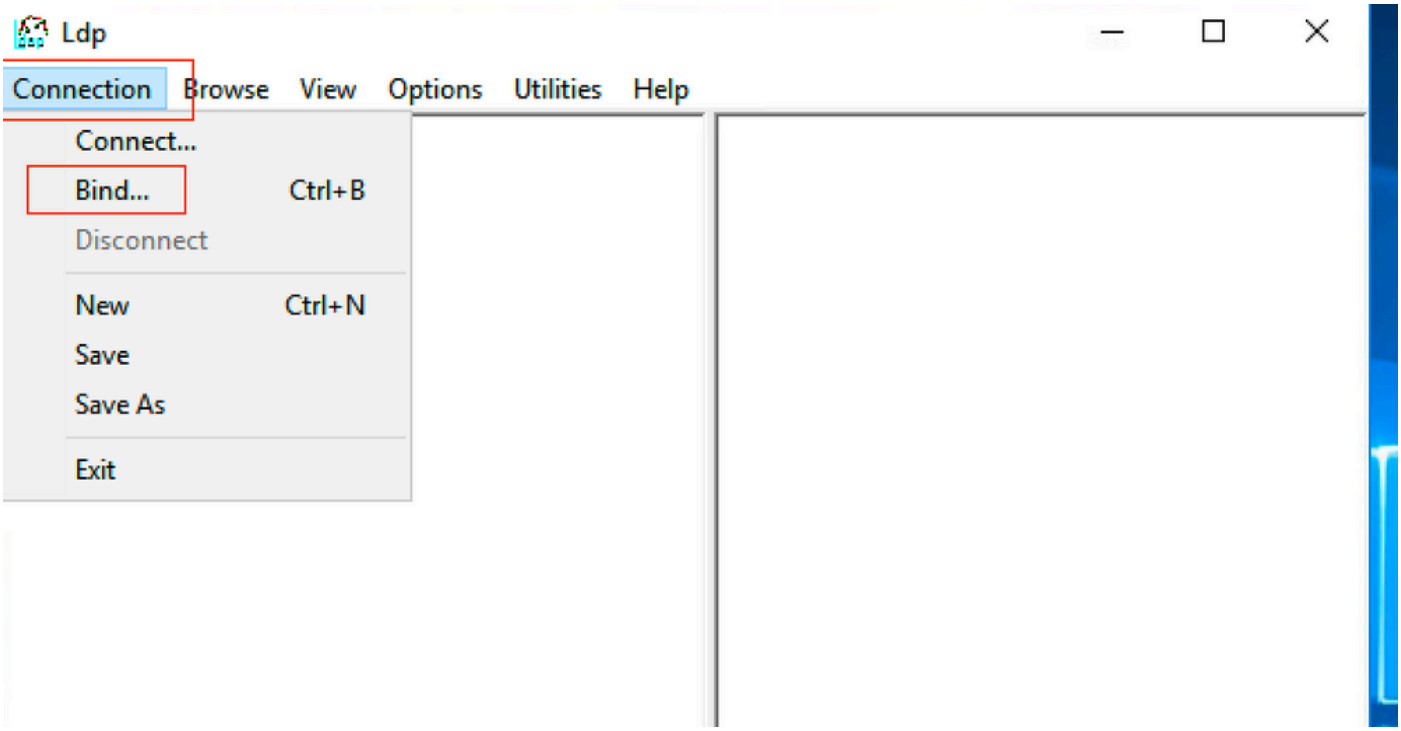
從WLC cli重新配置ldap對映屬性。

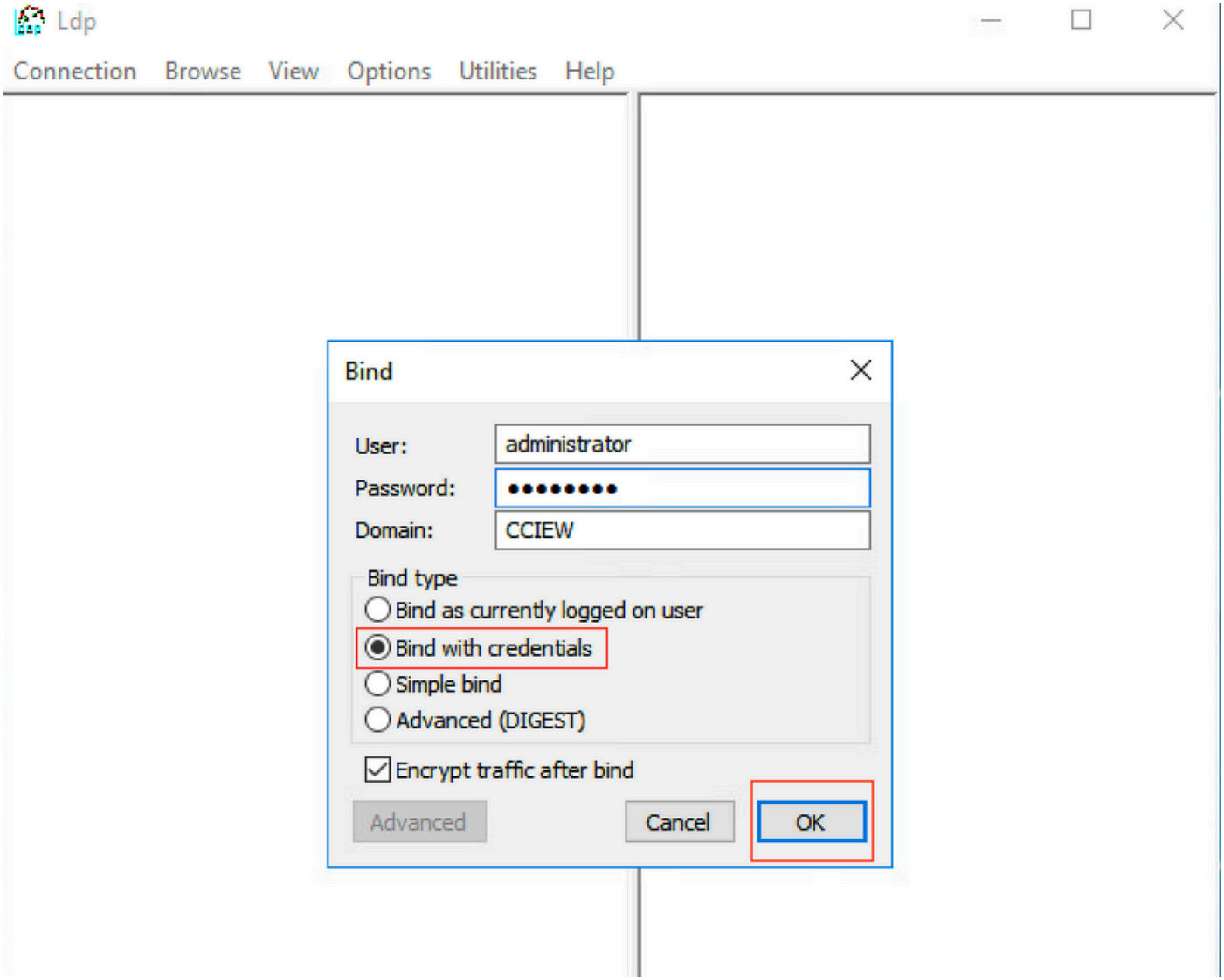
2. 確保伺服器以明文形式返回"userPassword"，否則身份驗證失敗。

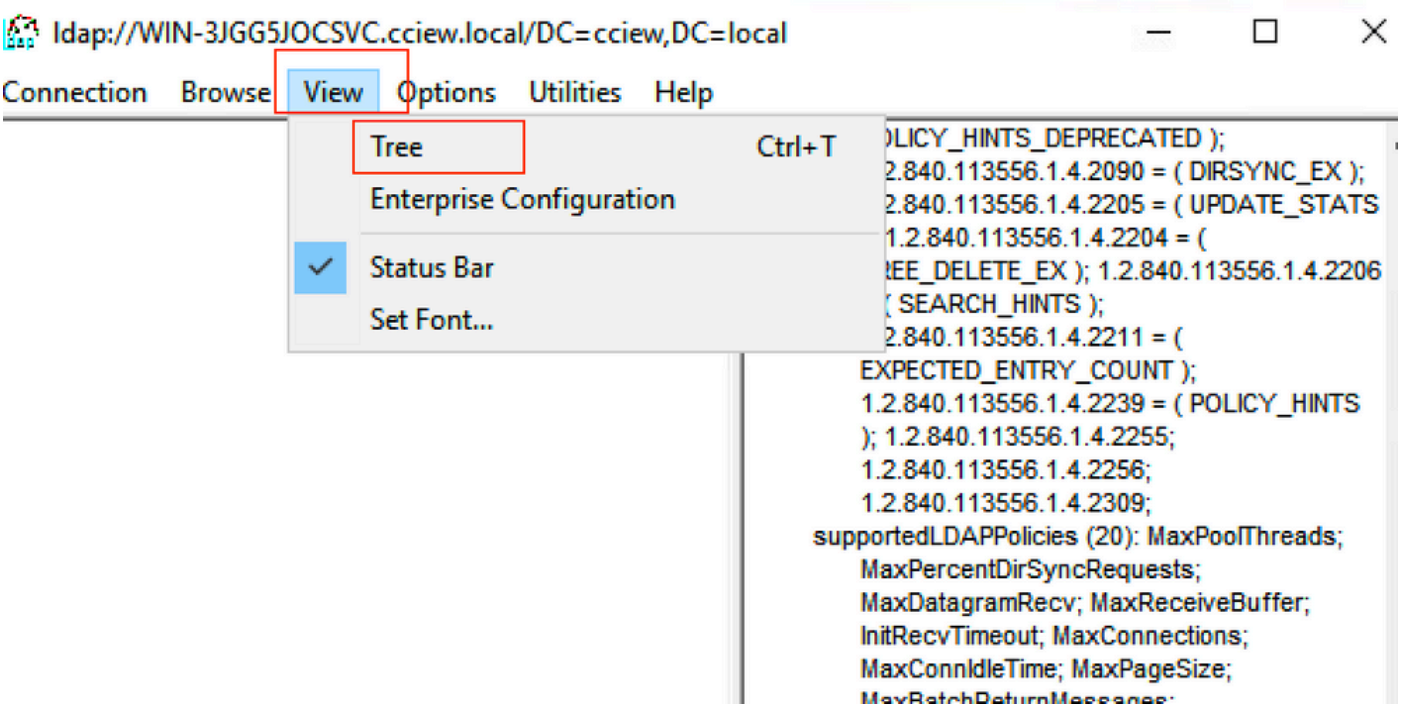


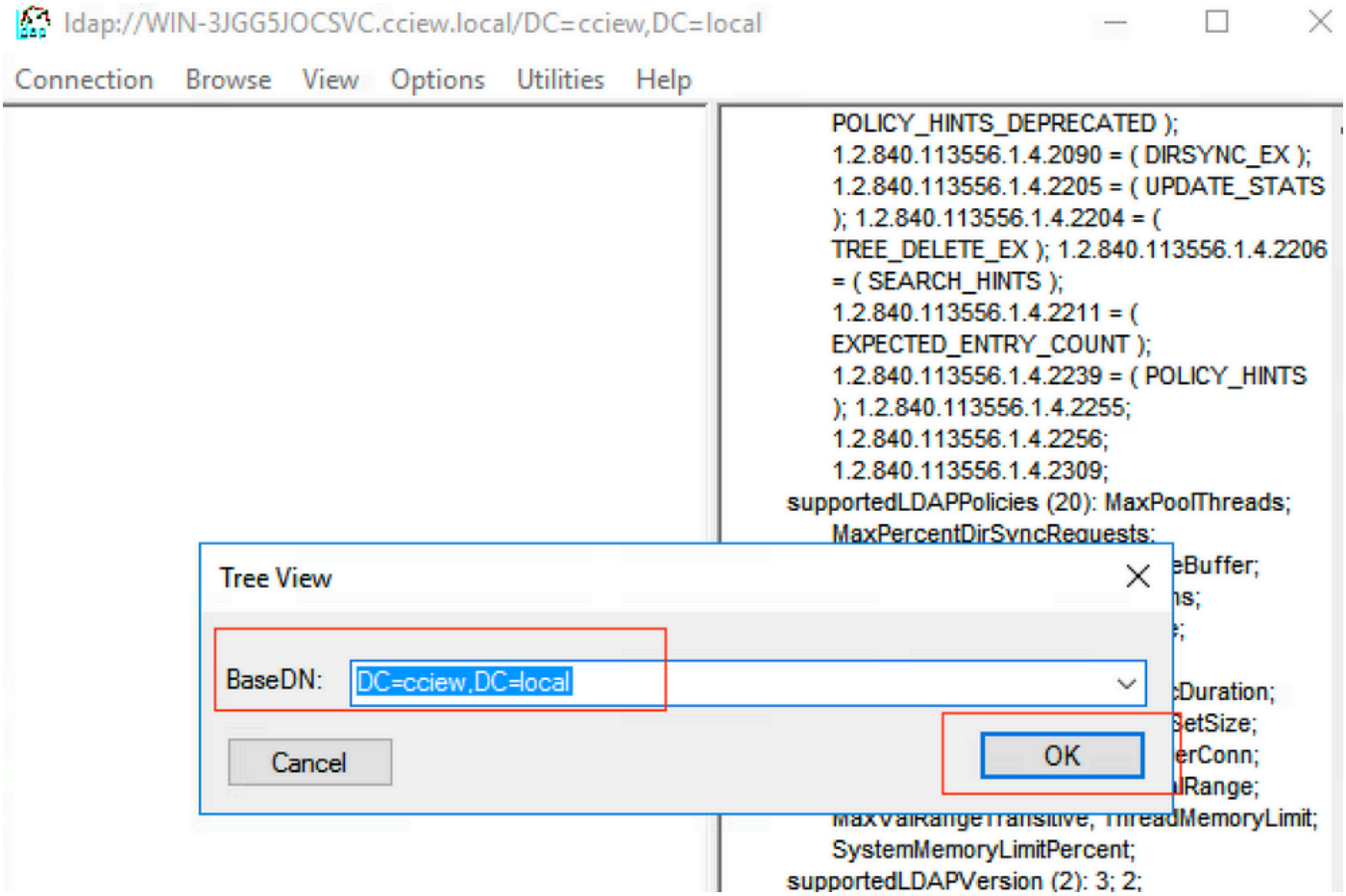
3. 使用伺服器上的ldp.exe工具驗證基本DN資訊。




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;

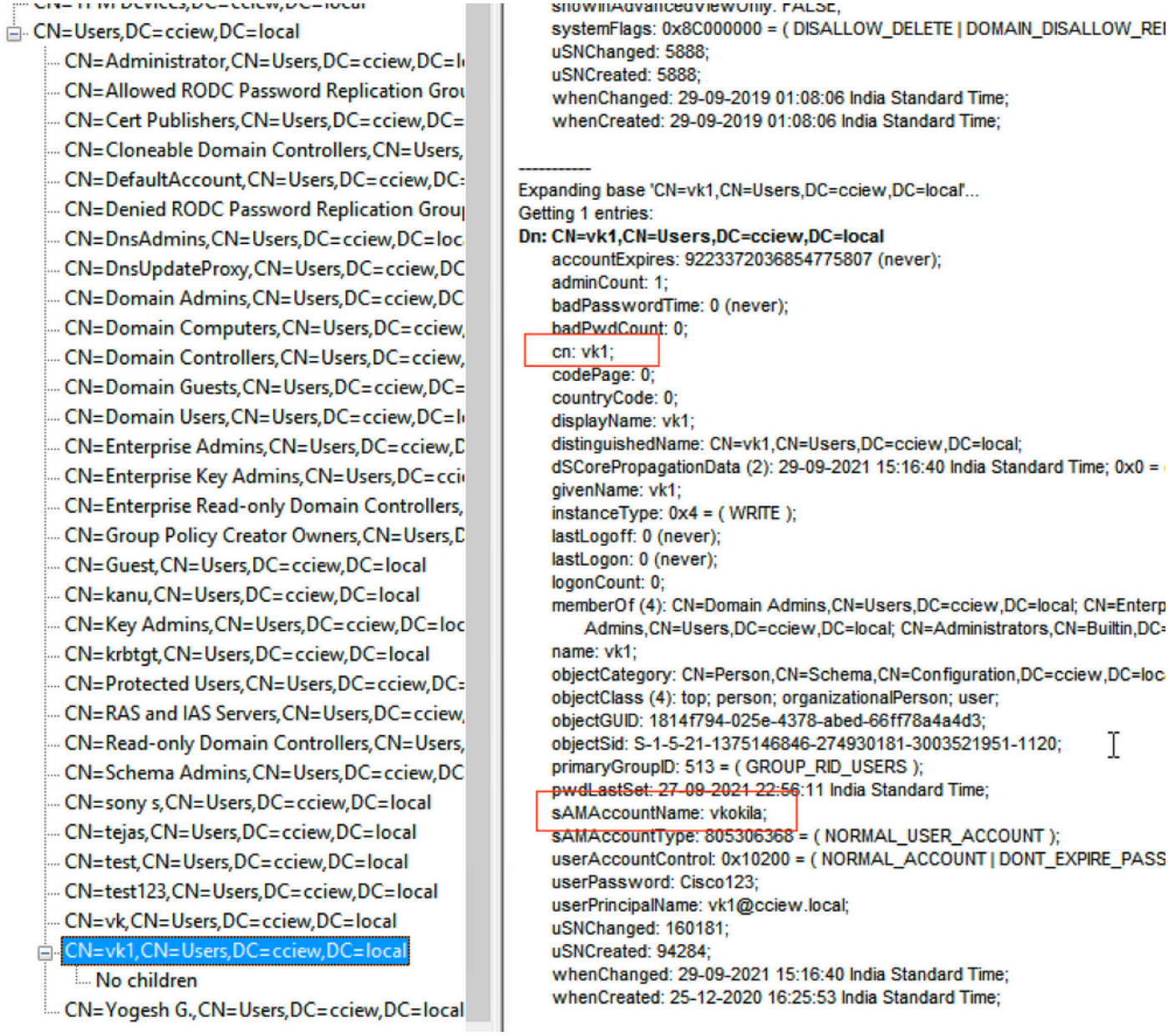

ldap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local
Connection
Browse
View
Options
Utilities
Help
POLICY_HINTS_DEPRECATED);
1.2.840.113556.1.4.2090 = (DIRSYNC_EX);
1.2.840.113556.1.4.2205 = (UPDATE_STATS
); 1.2.840.113556.1.4.2204 = (
TREE_DELETE_EX); 1.2.840.113556.1.4.2206
= (SEARCH_HINTS);
1.2.840.113556.1.4.2211 = (
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. 檢查伺服器統計資訊和屬性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

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

參考資料

[9800上的本地EAP配置示例]