تكوين Catalyst 9800 WLC مع مصادقة LDAP لـ Web-auth و 802.1X

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
تكوين LDAP باستخدام SSID لـ WebAuth
الرسم التخطيطي للشبكة
تكوين وحدة التحكم
تكوين LDAP باستخدام DOT1x SSID (باستخدام EAP المحلي)
فهم تفاصيل خادم LDAP
فهم الحقول على واجهة مستخدم ويب 9800
مصادقة LDAP 802.1x مع سمة sAMAaccountName.
تكوين WLC:
التحقق من واجهة الويب:
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
كيفية التحقق من عملية المصادقة على وحدة التحكم
كيفية التحقق من اتصال 9800 بـ LDAP
المراجع

المقدمة

يصف هذا وثيقة كيف أن يشكل مادة حفازة 9800 in order to صادقت زبون مع LDAP نادل بما أن القاعدة معطيات للمستخدم مسوغات.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- خوادم Microsoft Windows
- Active Directory أو أي قاعدة بيانات LDAP أخرى

المكونات المستخدمة

C9800 EWC على نقطة الوصول (AP) C9100 التي تعمل بنظام Cisco IOS®-XE الإصدار 17.3.2a

خادم Microsoft Active Directory (AD) المزود بوحدة تخزين الوصول إلى الشبكة (NAS) من QNAP

التي تعمل كقاعدة بيانات LDAP

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تكوين LDAP باستخدام SSID ل WebAuth

الرسم التخطيطي للشبكة

كتبت هذه المقالة استنادا إلى إعداد بسيط جدا:

نقطة الوصول EWC AP 9115 مع IP 192.168.1.15

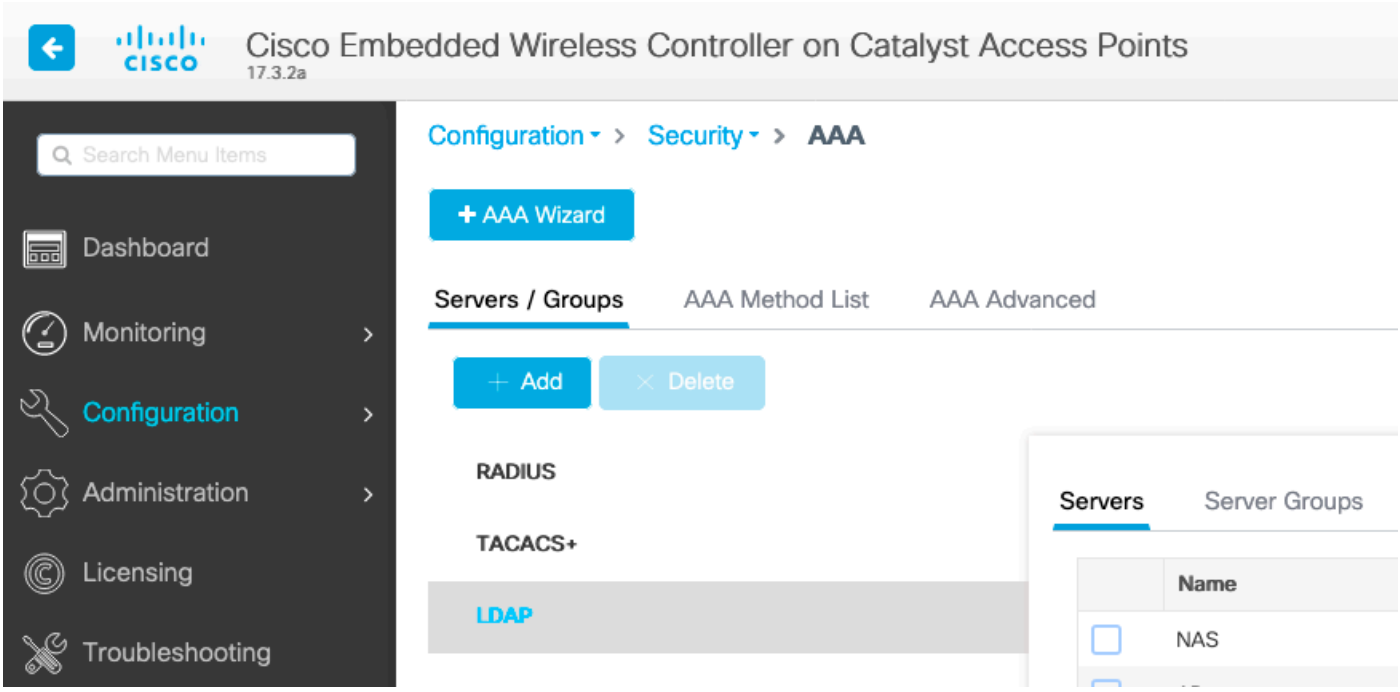
خادم Active Directory مع IP 192.168.1.192

عميل يتصل بنقطة الوصول الداخلية من EWC

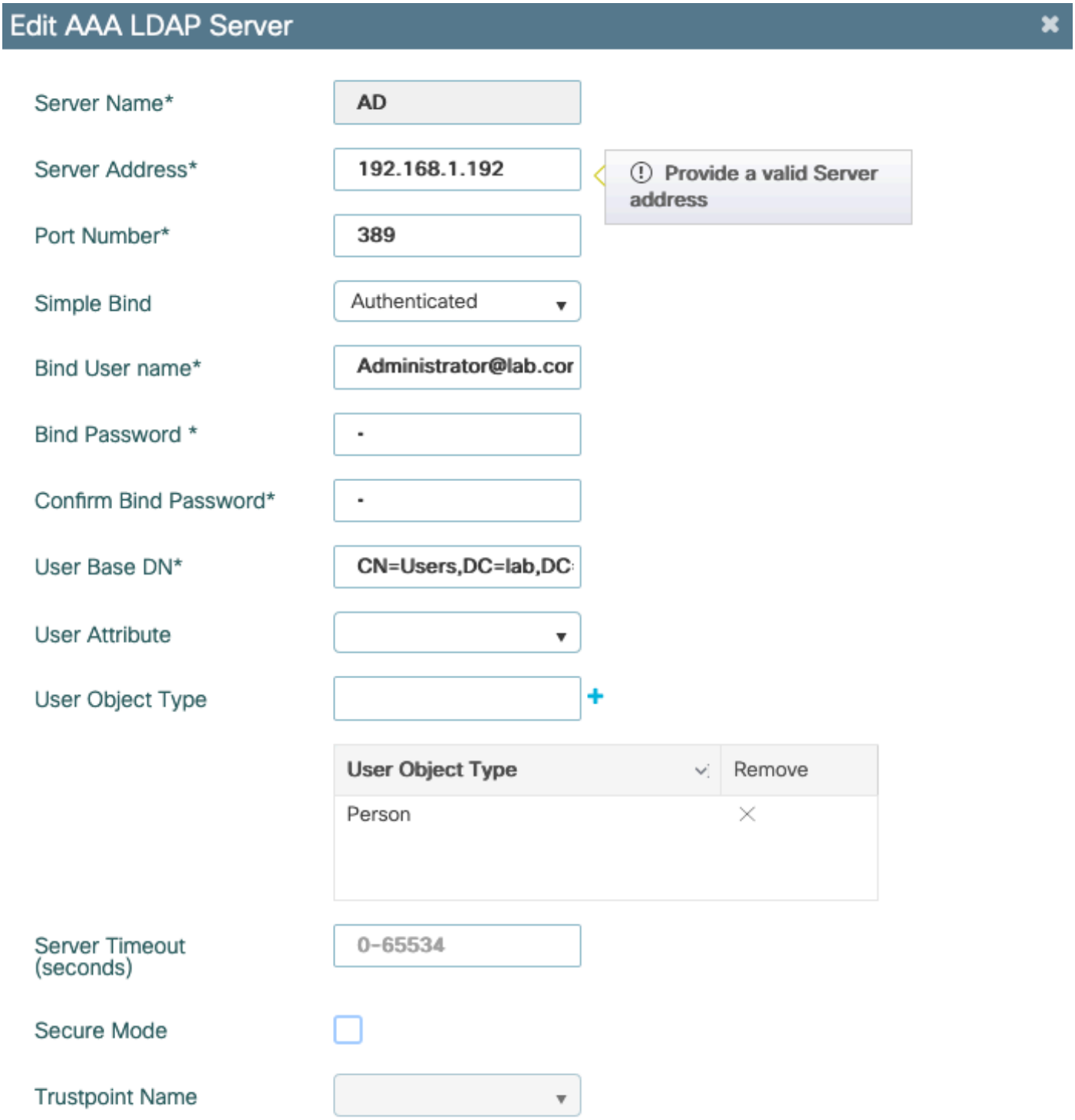
تكوين وحدة التحكم

الخطوة 1. تكوين خادم LDAP

انتقل إلى **التكوين > الأمان > AAA> الخوادم/المجموعات > LDAP** وانقر فوق **+ إضافة**



أختر اسما لخادم LDAP الخاص بك وقم بتعبئة التفاصيل. لشرح كل حقل، راجع قسم "فهم تفاصيل خادم LDAP" بهذا المستند.



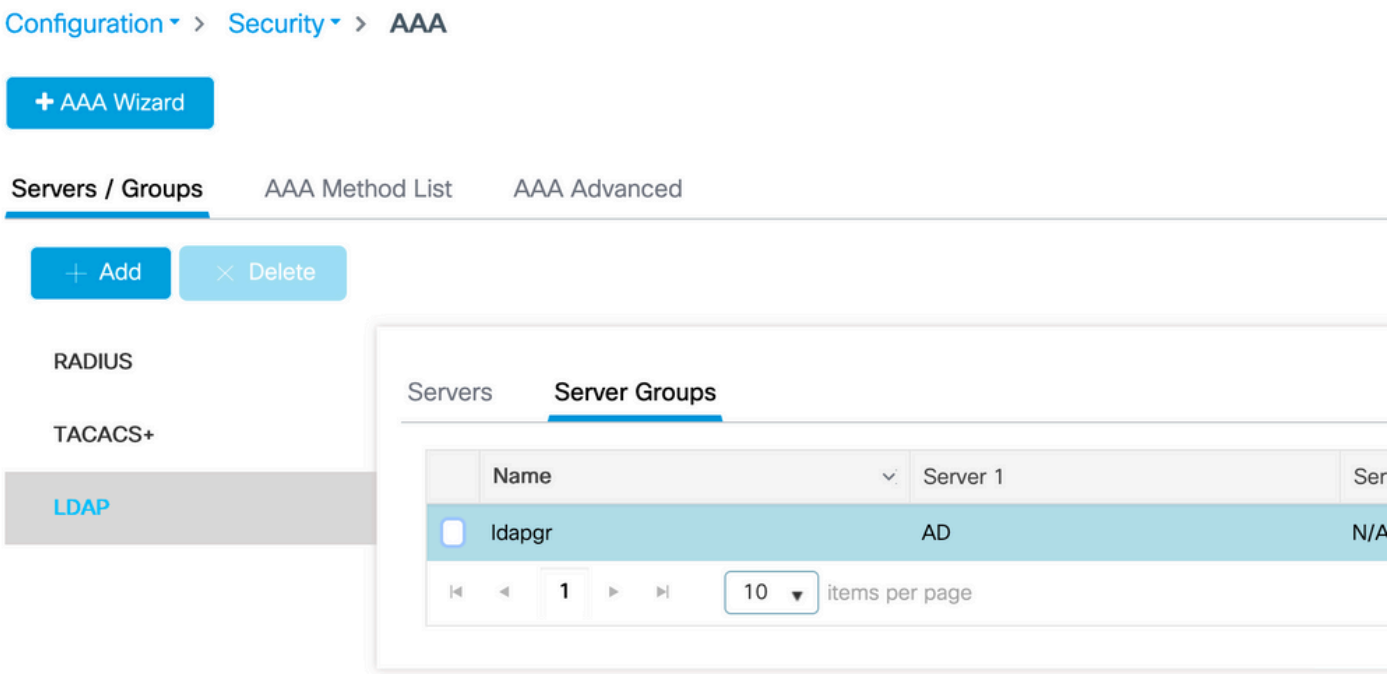
حفظ بالنقر فوق **تحديث وتطبيق على الجهاز**

أوامر CLI:

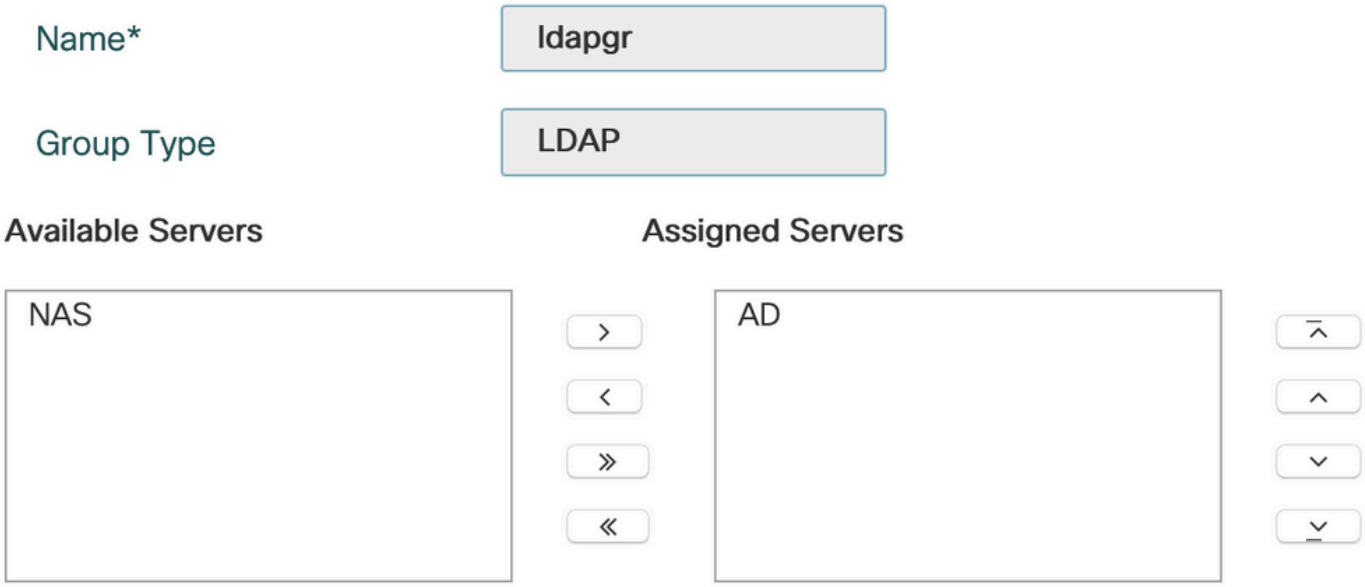
```
ldap server AD ipv4 192.168.1.192 bind authenticate root-dn Administrator@lab.com password 6
WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB base-dn CN=Users,DC=lab,DC=com search-filter user-object-type
Person
```

الخطوة 2. تكوين مجموعة خوادم LDAP.

انتقل إلى **التكوين > التأمين > AAA > الخوادم/ المجموعات > LDAP > مجموعات الخوادم** وانقر فوق **+إضافة**



أدخل اسم أو أضف خادم LDAP الذي قمت بتكوينه في الخطوة السابقة.



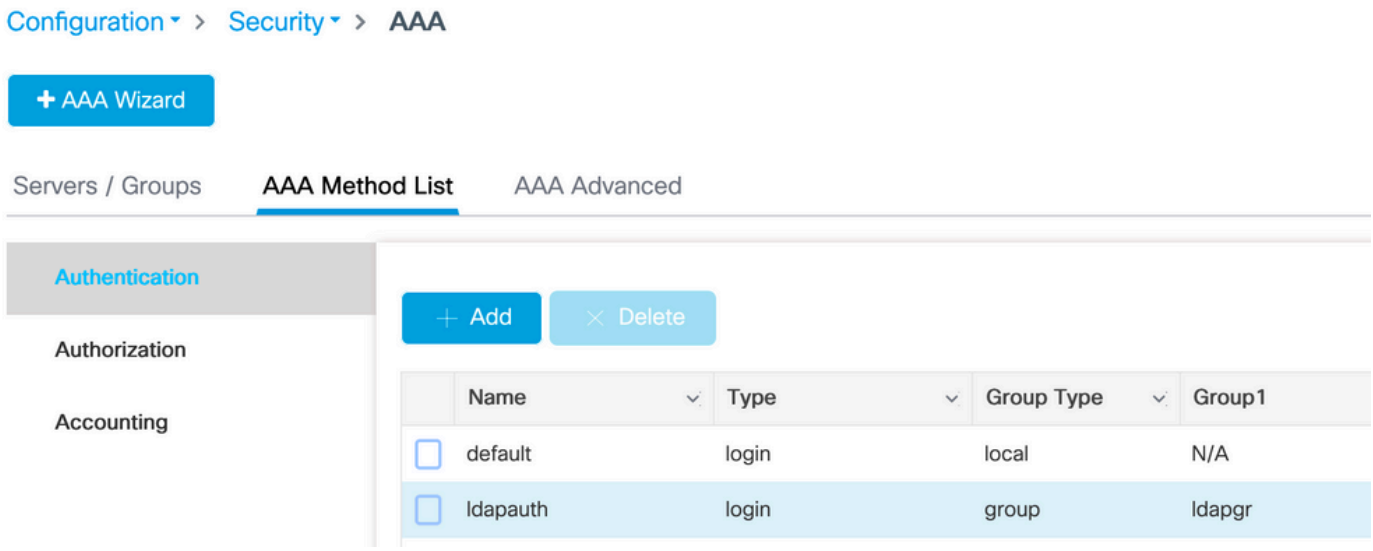
انقر فوق **تحديث وقم بتطبيق** للحفظ.

أوامر CLI :

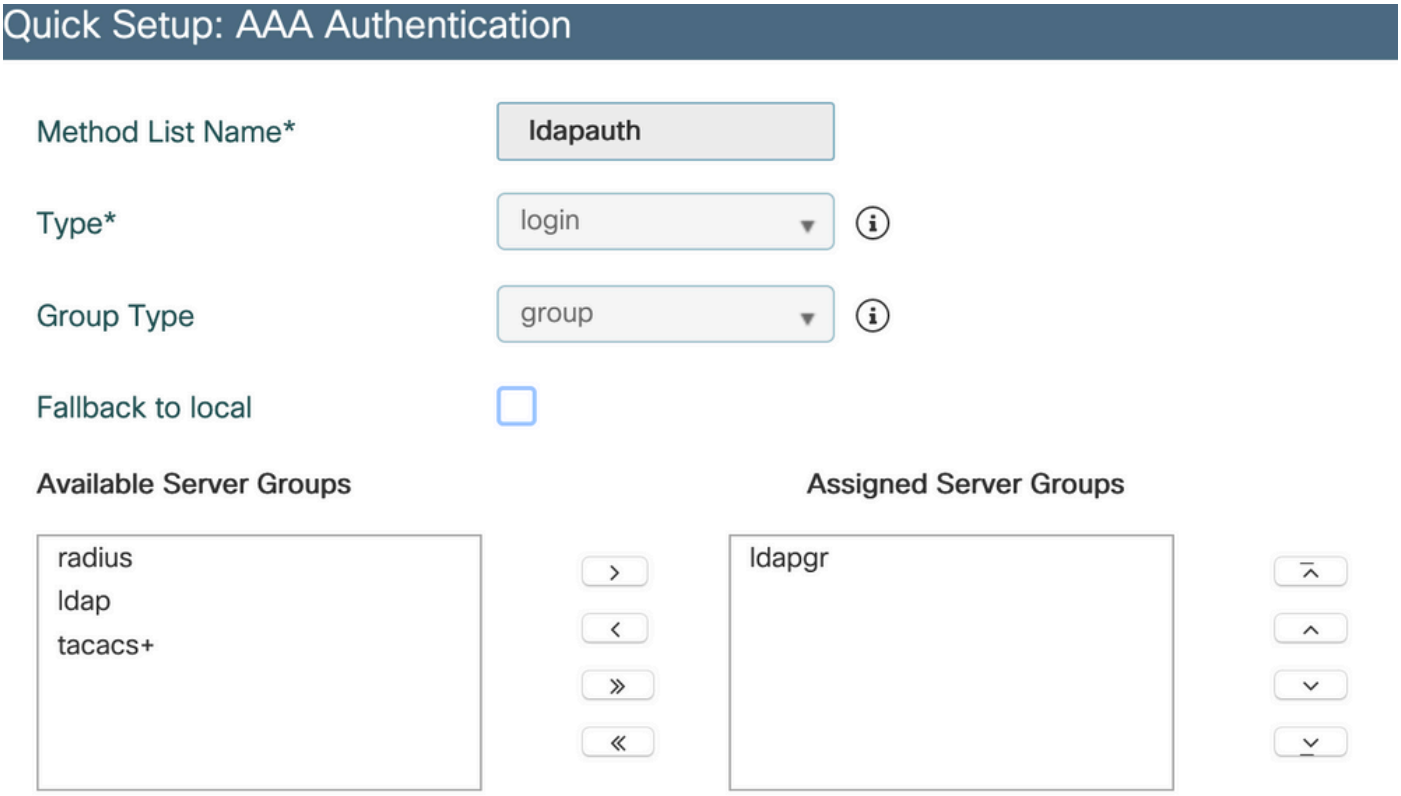
```
aaa group server ldap ldapgr server AD
```

الخطوة 3. تكوين أسلوب مصادقة AAA

انتقل إلى **التكوين > التأمين > AAA > قائمة طرق AAA > المصادقة** وانقر **+إضافة**



أدخل اسما، واختر نوع **تسجيل الدخول** وأشر إلى مجموعة خوادم LDAP التي تم تكوينها مسبقا.

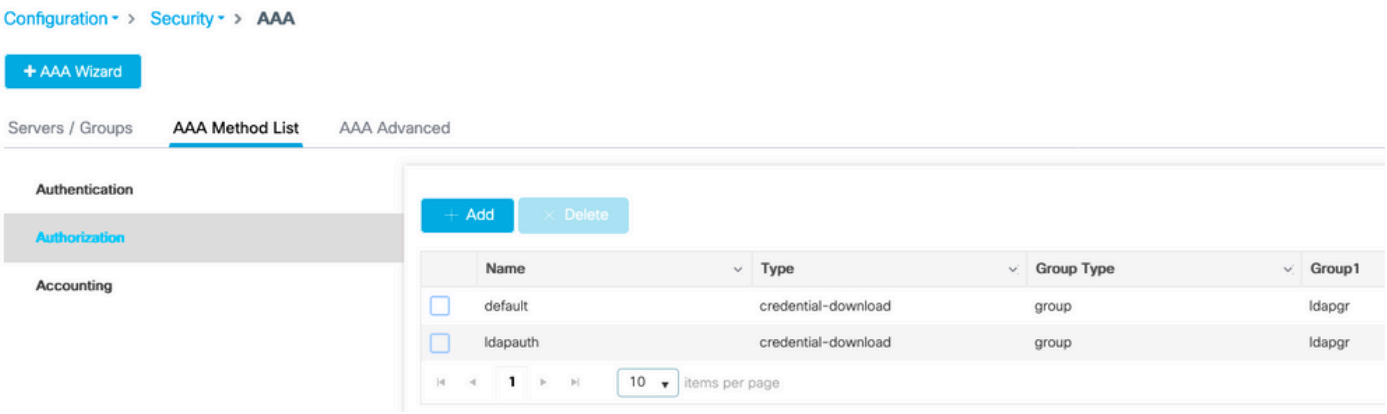


أوامر CLI :

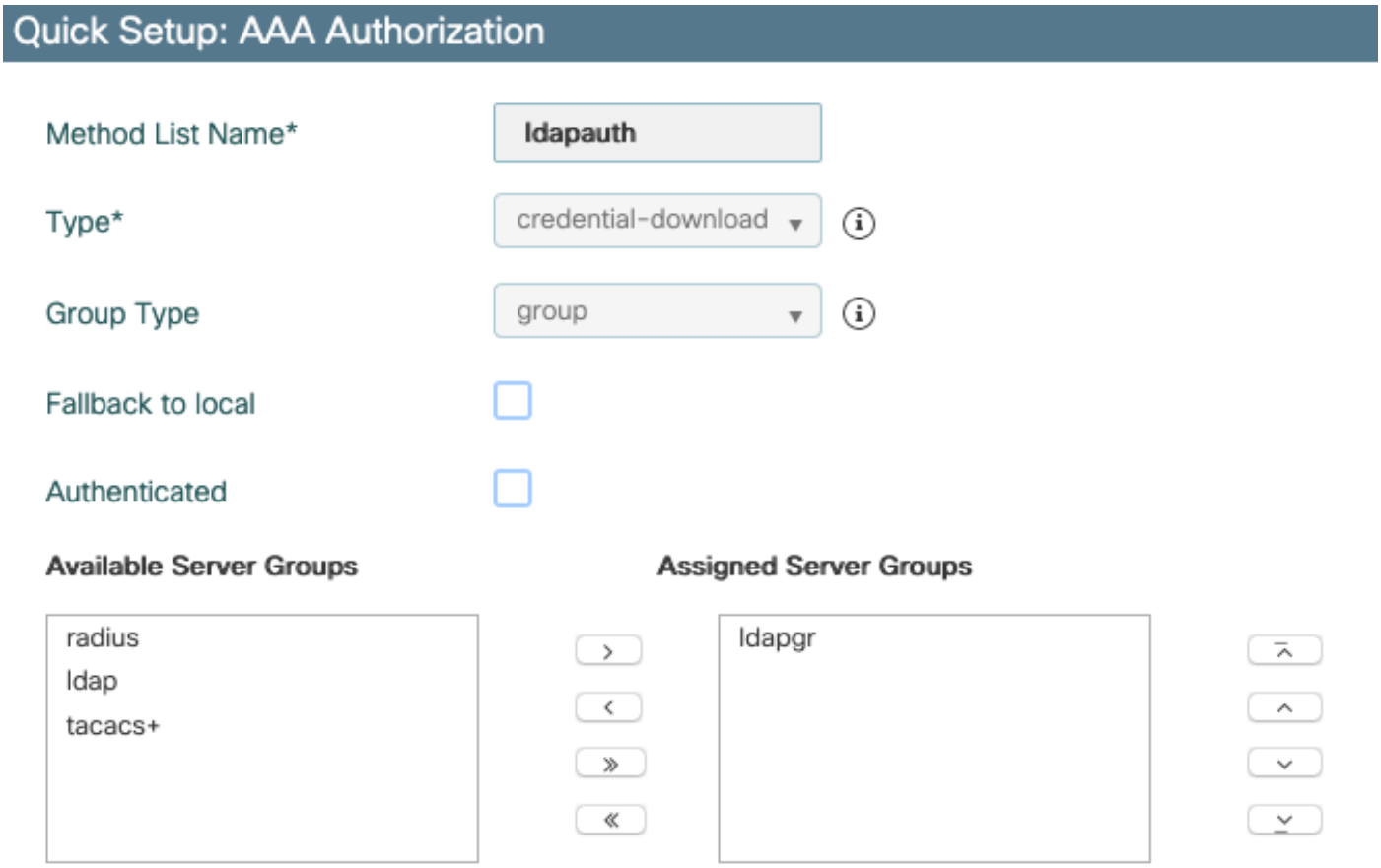
```
aaa authentication login ldapauth group ldapgr
```

الخطوة 4. تكوين أسلوب تفويض AAA

انتقل إلى **التكوين > الأمان > AAA> قائمة طرق AAA > التفويض** وانقر فوق **+إضافة**



قم بإنشاء قاعدة نوع تنزيل بيانات الاعتماد لاسم إختيارك وأشر بها إلى مجموعة خوادم LDAP التي تم إنشاؤها مسبقا



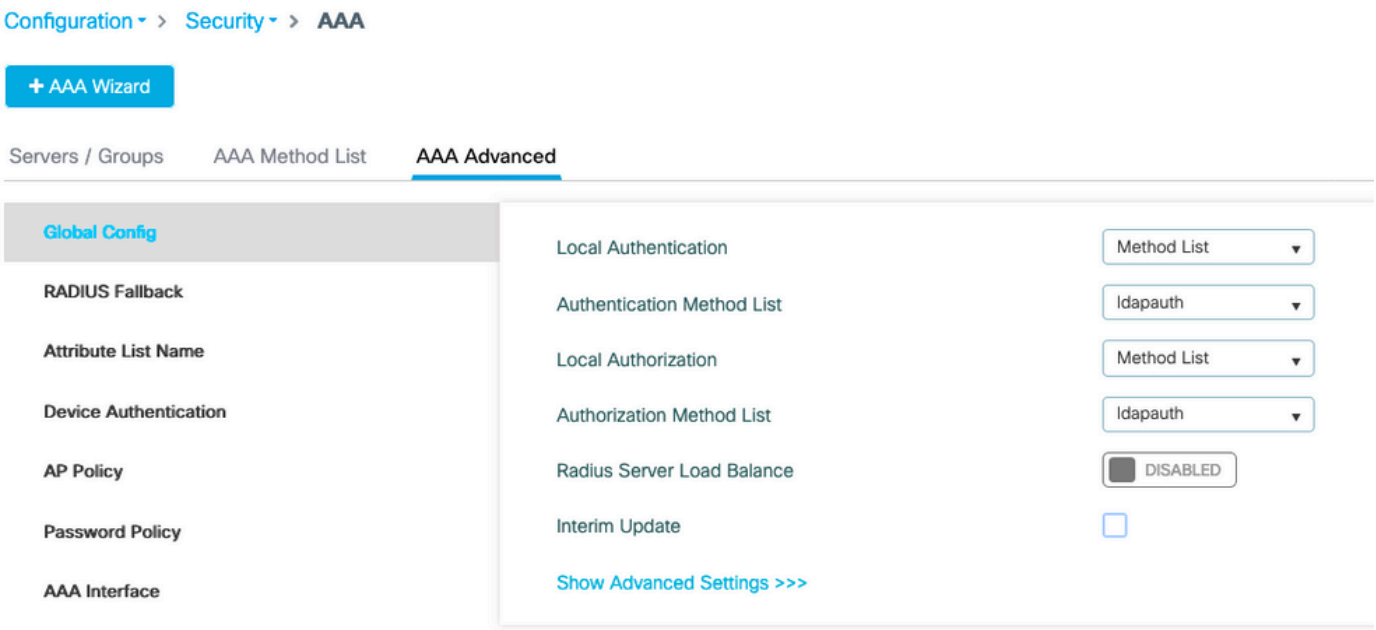
أوامر CLI :

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

الخطوة 5. تكوين المصادقة المحلية

انتقل إلى **التكوين > الأمان > AAA > AAA Advanced > التكوين العام**

قم بتعيين المصادقة المحلية والتفويض المحلي إلى **قائمة الطرق** واختر طريقة المصادقة والتفويض التي تم تكوينها مسبقا.

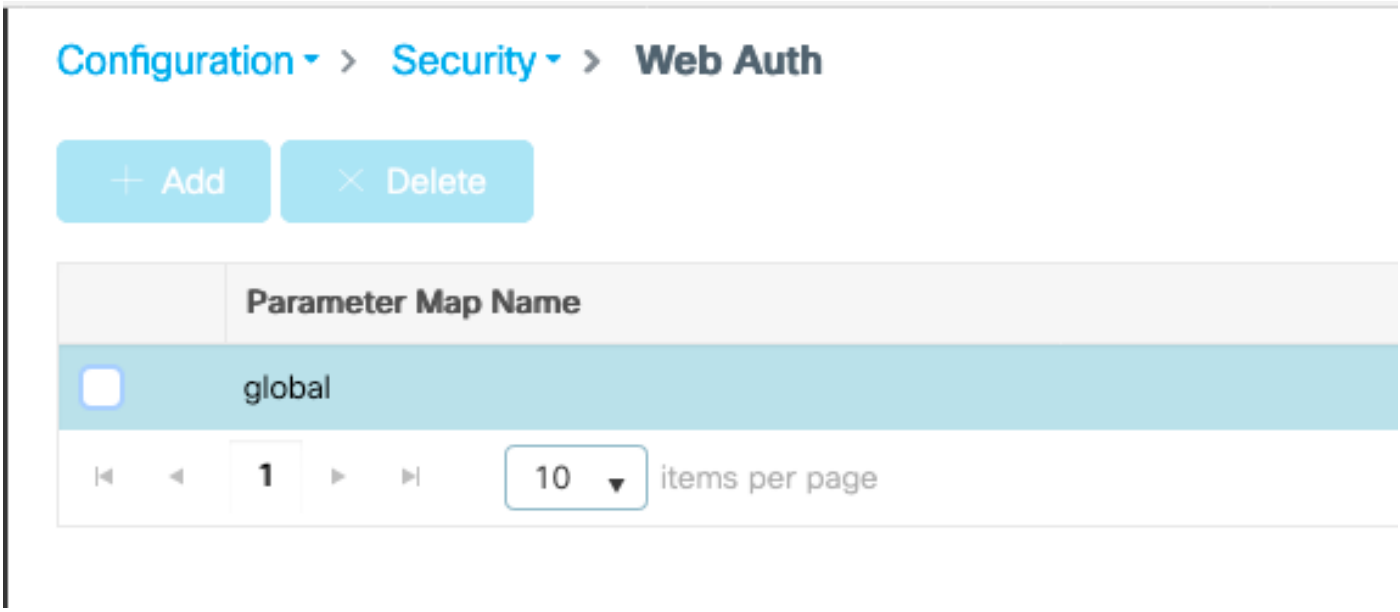


أوامر CLI :

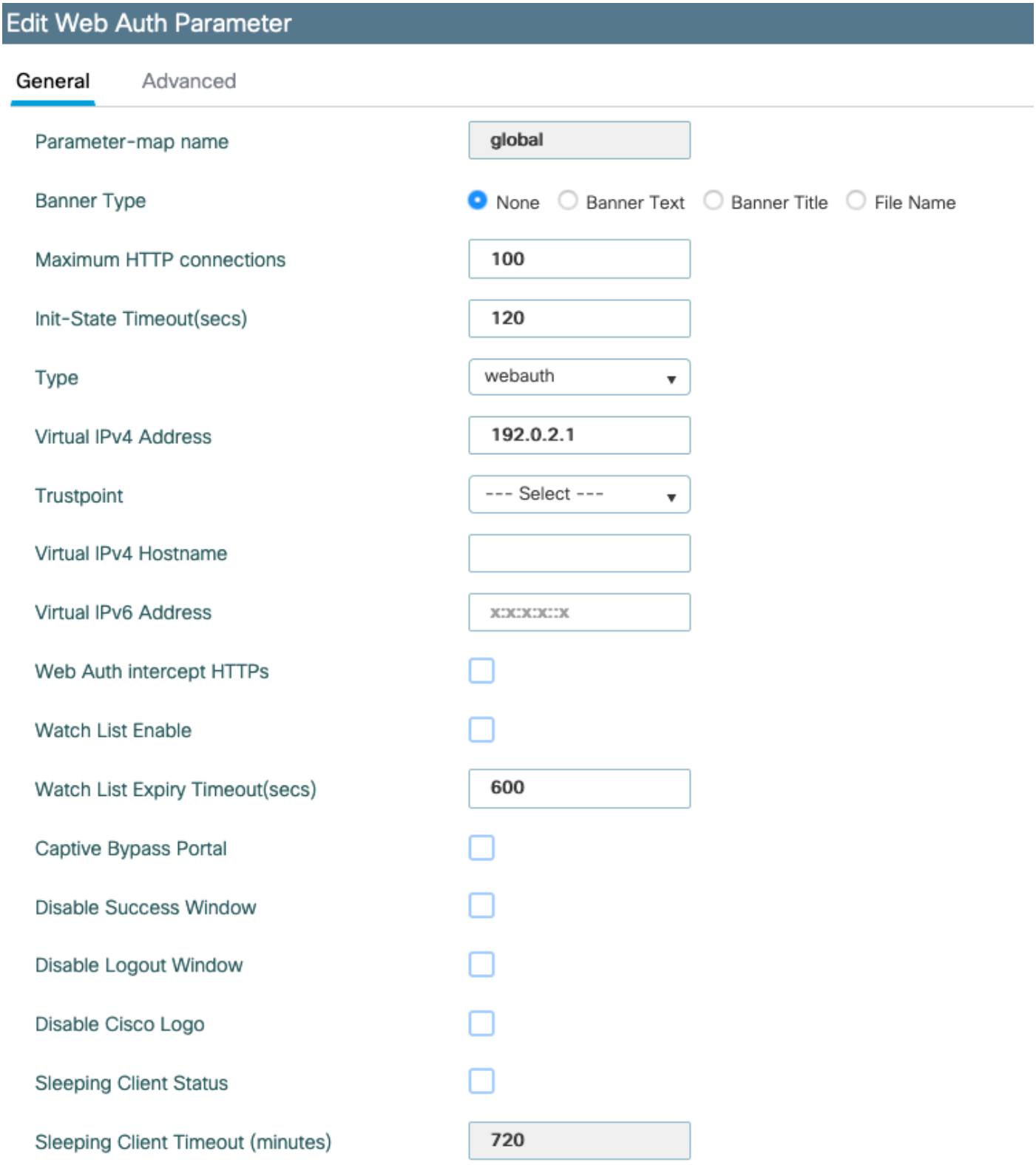
```
aaa local authentication ldapauth authorization ldapauth
```

الخطوة 6. تكوين معلمة-map webAuth

انتقل إلى **التكوين > الأمان > مصادقة الويب** وتحرير الخريطة **العامة**



تأكد من تكوين عنوان IPv4 ظاهري مثل 192.0.2.1 (يتم حجز شبكة IP/الشبكة الفرعية المحددة لبروتوكول IP الظاهري غير القابل للتوجيه).



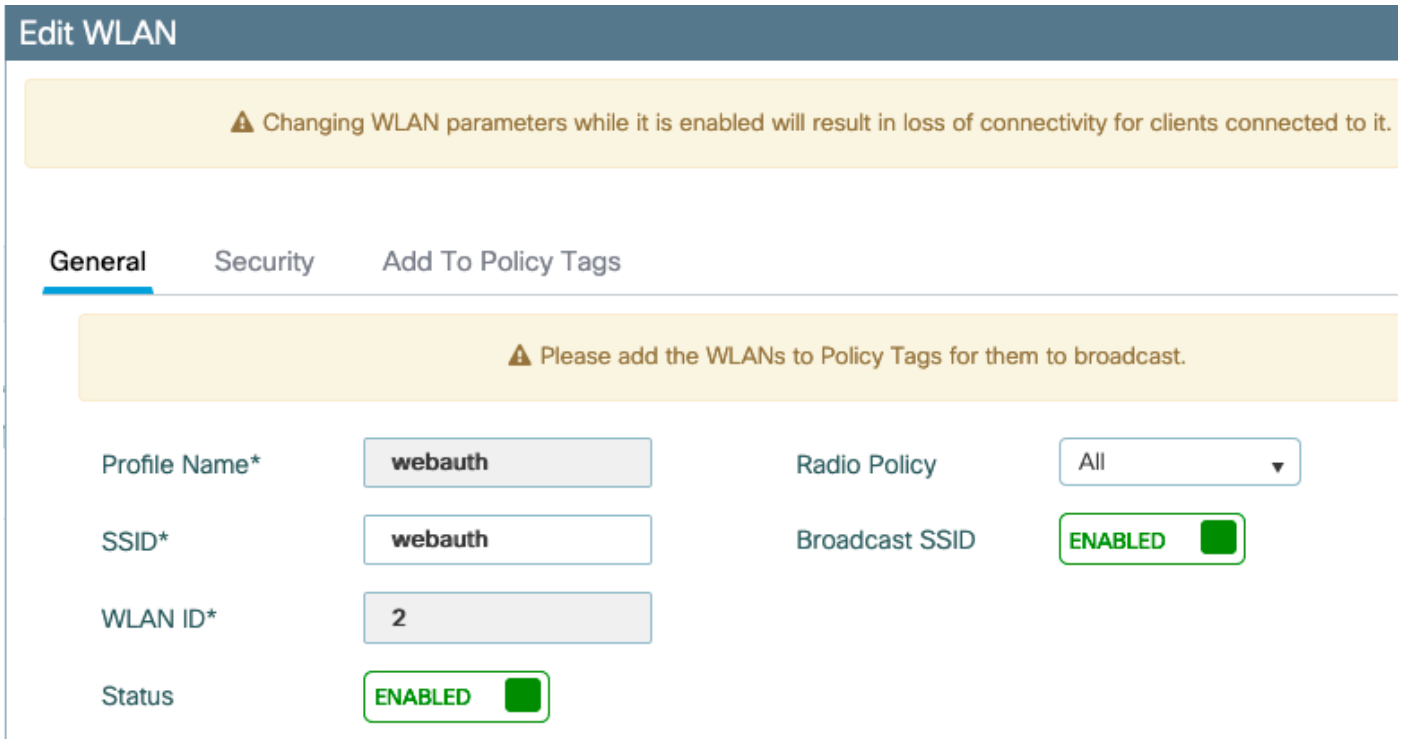
انقر فوق **تطبيق** للحفظ.

أوامر CLI :

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

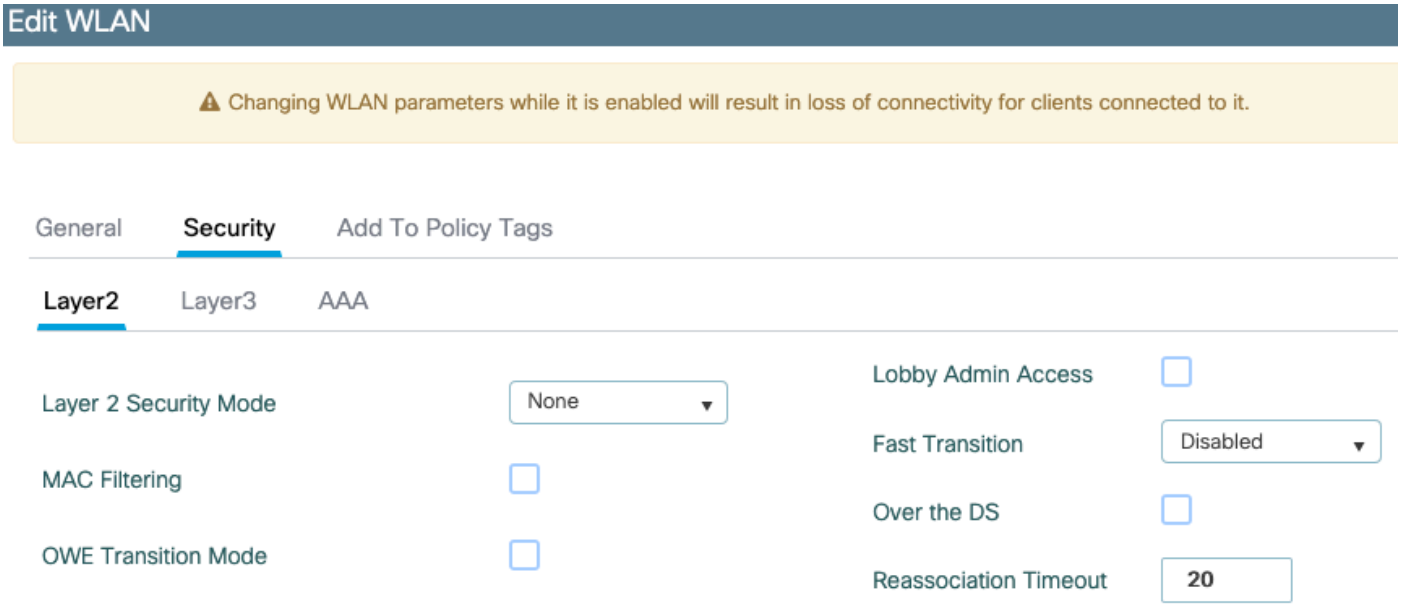
الخطوة 7. تكوين شبكة WLAN لـ WebAuth

انتقل إلى **التكوين > شبكات WLAN** وانقر **+إضافة**

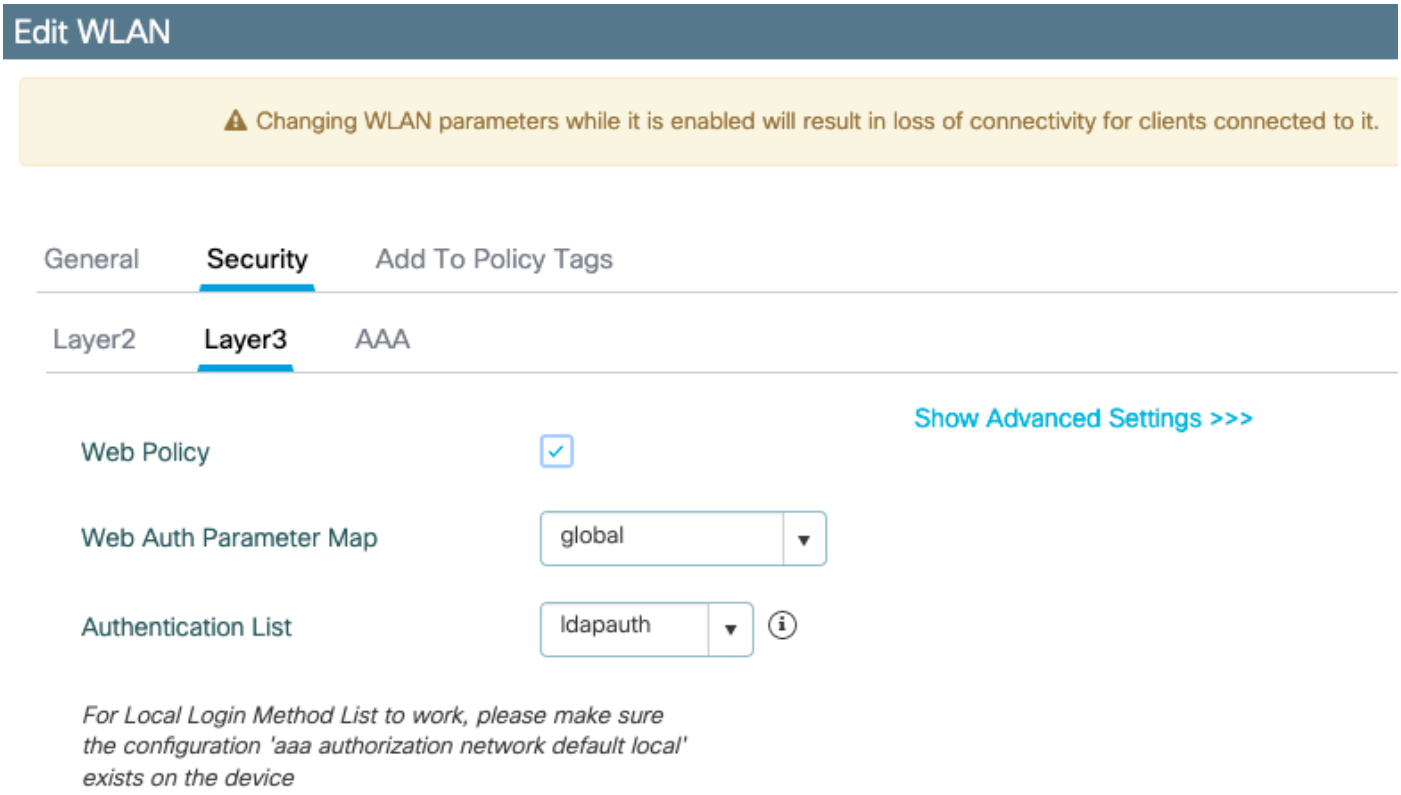


قم بتكوين الاسم، وتأكد من أنه في حالة التمكين، ثم انتقل إلى علامة التبويب **أمان**.

في علامة التبويب الفرعية **الطبقة 2**، تأكد من عدم وجود أمان ومن تعطيل الانتقال السريع.



في علامة التبويب **طبقة 3**، قم بتمكين **سياسة الويب**، وتعيين خريطة المعلمات على **عمومي**، وتعيين قائمة المصادقة على طريقة تسجيل الدخول AAA التي تم تكوينها مسبقا.



حفظ بالنقر فوق **تطبيق**

أوامر CLI :

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

الخطوة 8. تأكد من بث SSID

انتقل إلى **التكوين > عالمات التمييز** وتأكد من تضمين SSID في ملف تعريف السياسة الذي تتم خدمته حاليا بواسطة SSID (عالمة النهج الافتراضية لتكوين جديد جديد جديد إذا لم تقم بتكوين عالمات بعد). بشكل افتراضي، ال تبث عالمة السياسة الافتراضية SSIDs جديدة تقوم بإنشائها حتى تقوم بتضمينها يدويا.

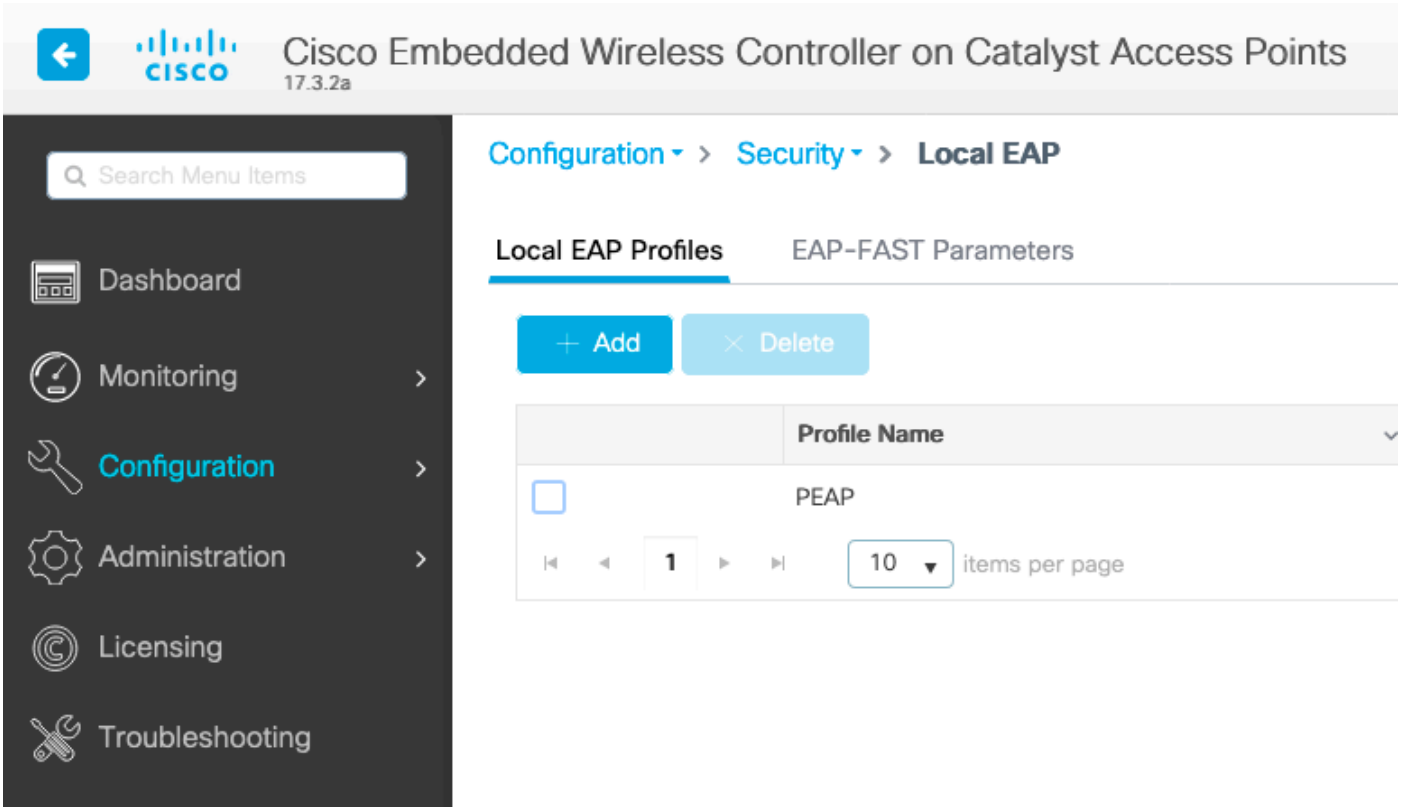
ال تغطي هذه المقالة تكوين ملفات تعريف السياسة وتفترض أنك على دراية بذلك الجزء من التكوين.

تكوين LDAP باستخدام DOT1x SSID (باستخدام EAP المحلي)

عادة ما يتطلب تكوين LDAP لمعرف SSID 802.1X على 9800 أيضا تكوين EAP محلي. إذا كنت تريد إستخدام RADIUS، فسيكون خادم RADIUS لديك إنشاء اتصال بقاعدة بيانات LDAP وذلك خارج نطاق هذه المقالة.قبل محاولة اذا التكوين، ينصح بتكوين EAP محلي باستخدام مستخدم محلي تم تكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) أوال، وتم توفير مثال تكوين في قسم المراجع في نهاية هذه المقالة. بمجرد الانتهاء، يمكنك محاولة نقل قاعدة بيانات المستخدم إلى LDAP.

الخطوة 1. تكوين ملف تعريف EAP محلي

انتقل إلى **التكوين > EAP المحلي** وانقر **+إضافة**



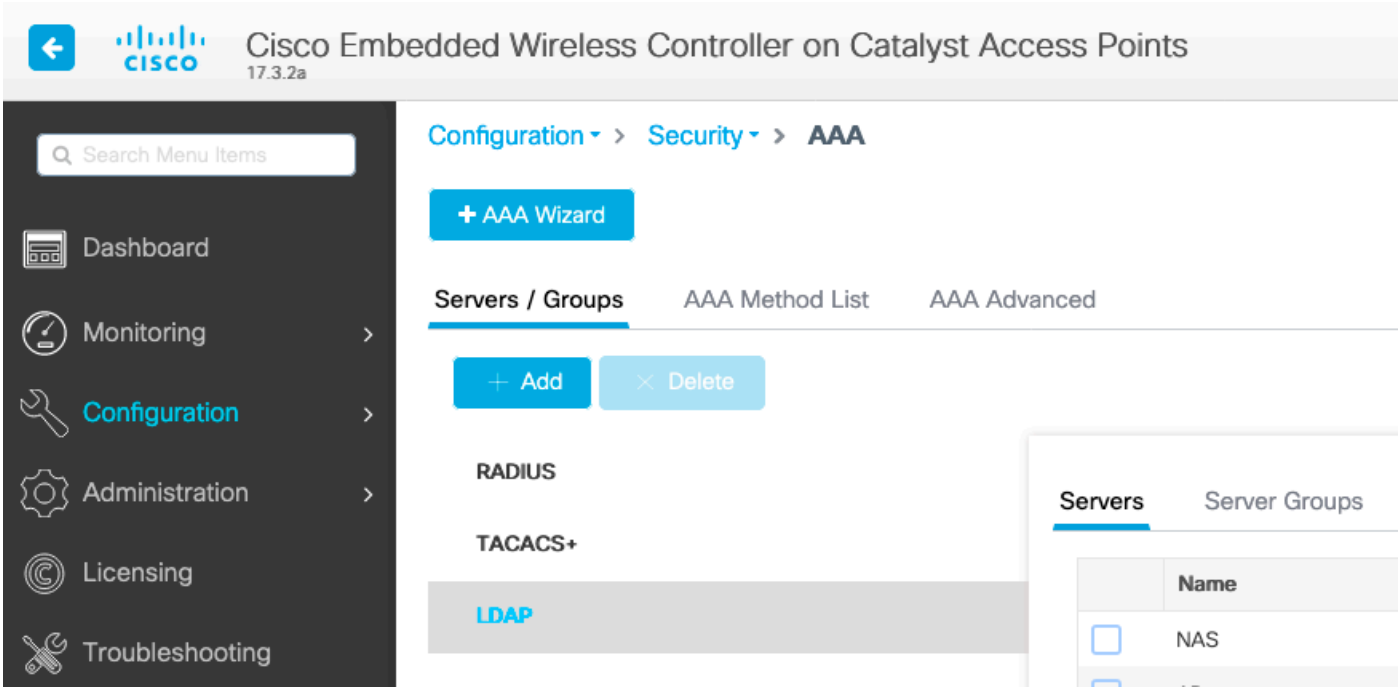
أختر أي اسم لملف التعريف الخاص بك. تمكين PEAP على الأقل واختيار اسم TrustPoint. بشكل افتراضي، تحتوي عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لديك قطع على شهادات موقعة ذاتيا، لذلك ال يهم حقا أي واحد تختار (عادة TP-XXXXX وهو الأفضل لهذا الغرض) ولكن لأن إصدارات أنظمة تشغيل الهواتف الذكية الجديدة تثق في شهادات موقعة ذاتيا أقل وأقل، ضع في الاعتبار تثبيت شهادة موقعة من قبل العامة.

أوامر CLI :

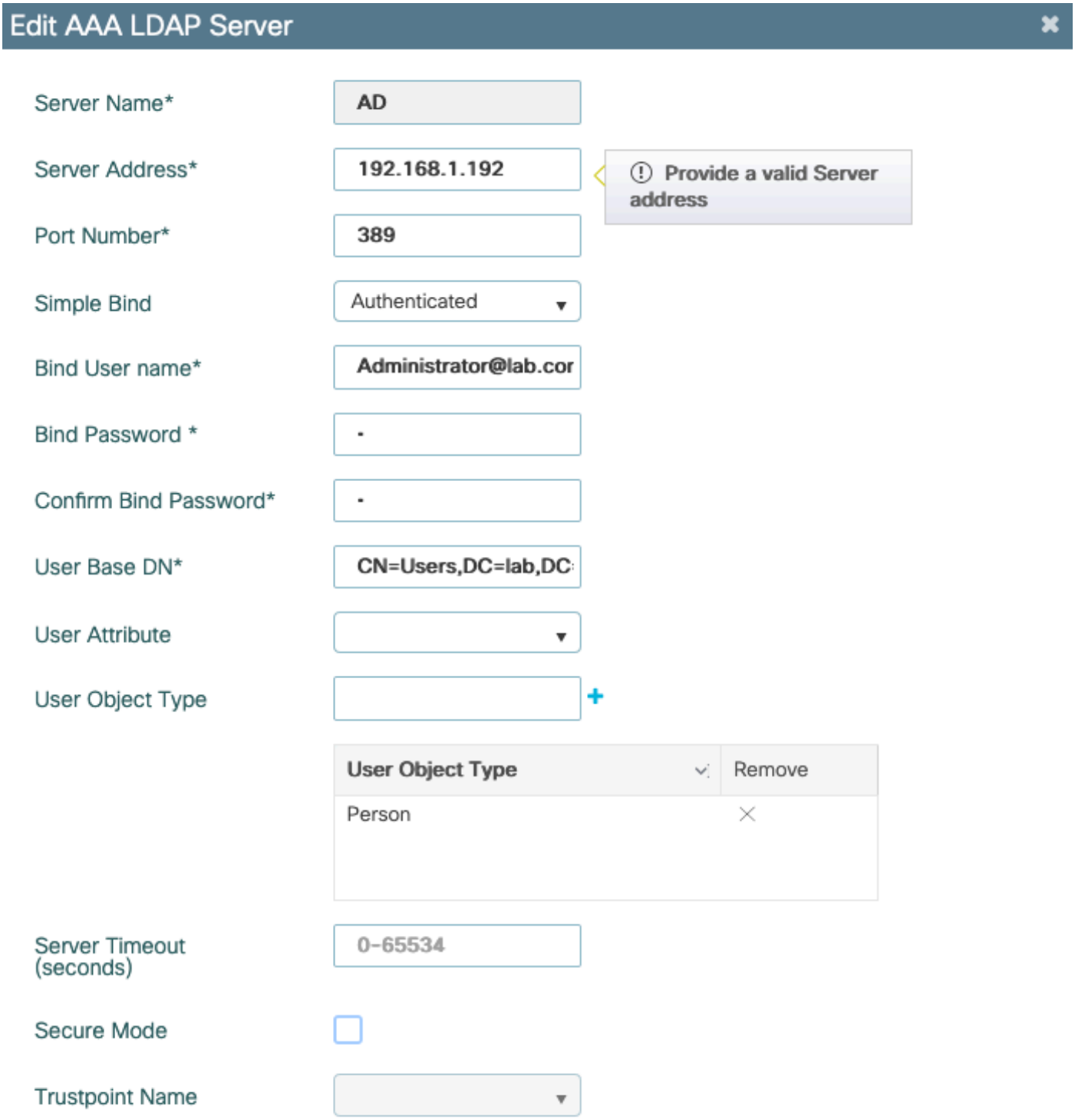
```
eap profile PEAP method peap pki-trustpoint TP-self-signed-3059261382
```

الخطوة 2. تكوين خادم LDAP

انتقل إلى **التكوين > الأمان > AAA> الخوادم/المجموعات > LDAP** وانقر فوق **+ إضافة**



أختر اسما لخادم LDAP الخاص بك وقم بتعبئة التفاصيل. لشرح كل حقل، راجع قسم "فهم تفاصيل خادم LDAP" بهذا المستند.

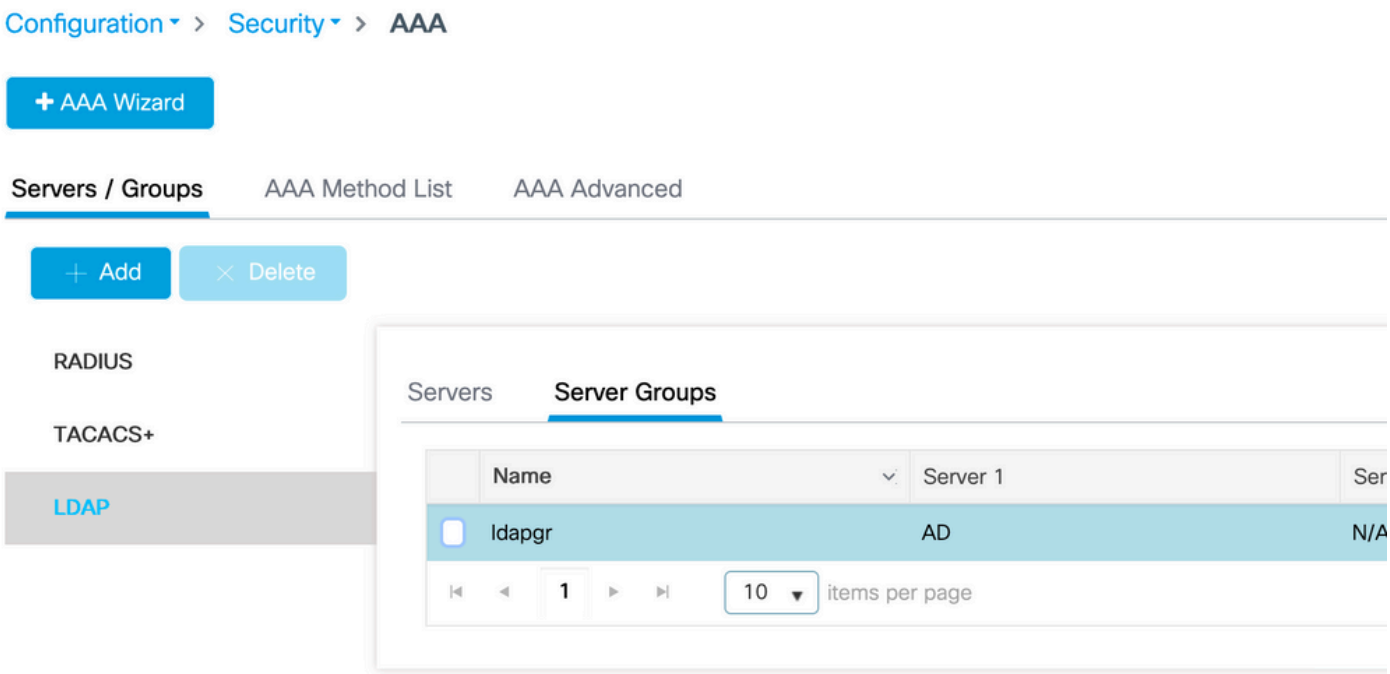


حفظ بالنقر فوق **تحديث وتطبيق على الجهاز**

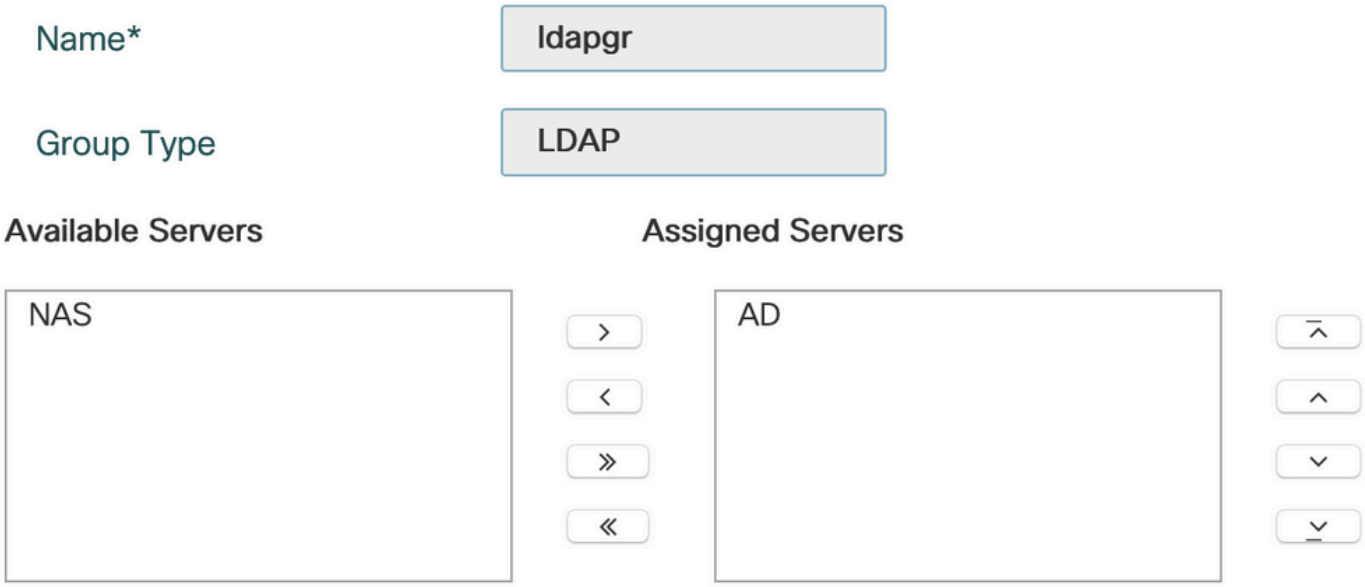
```
ldap server AD ipv4 192.168.1.192 bind authenticate root-dn Administrator@lab.com password 6
WCGYHKTDQPV]DeaHLSPF_GZ[E_MNi_AAB base-dn CN=Users,DC=lab,DC=com search-filter user-object-type
Person
```

الخطوة 3. تكوين مجموعة خوادم LDAP.

انتقل إلى **التكوين > التأمين > AAA > الخوادم/ المجموعات > LDAP > مجموعات الخوادم** وانقر فوق **+إضافة**



أدخل اسم أو أضف خادم LDAP الذي قمت بتكوينه في الخطوة السابقة.



انقر فوق **تحديث وقم بتطبيق** للحفظ.

أوامر CLI :

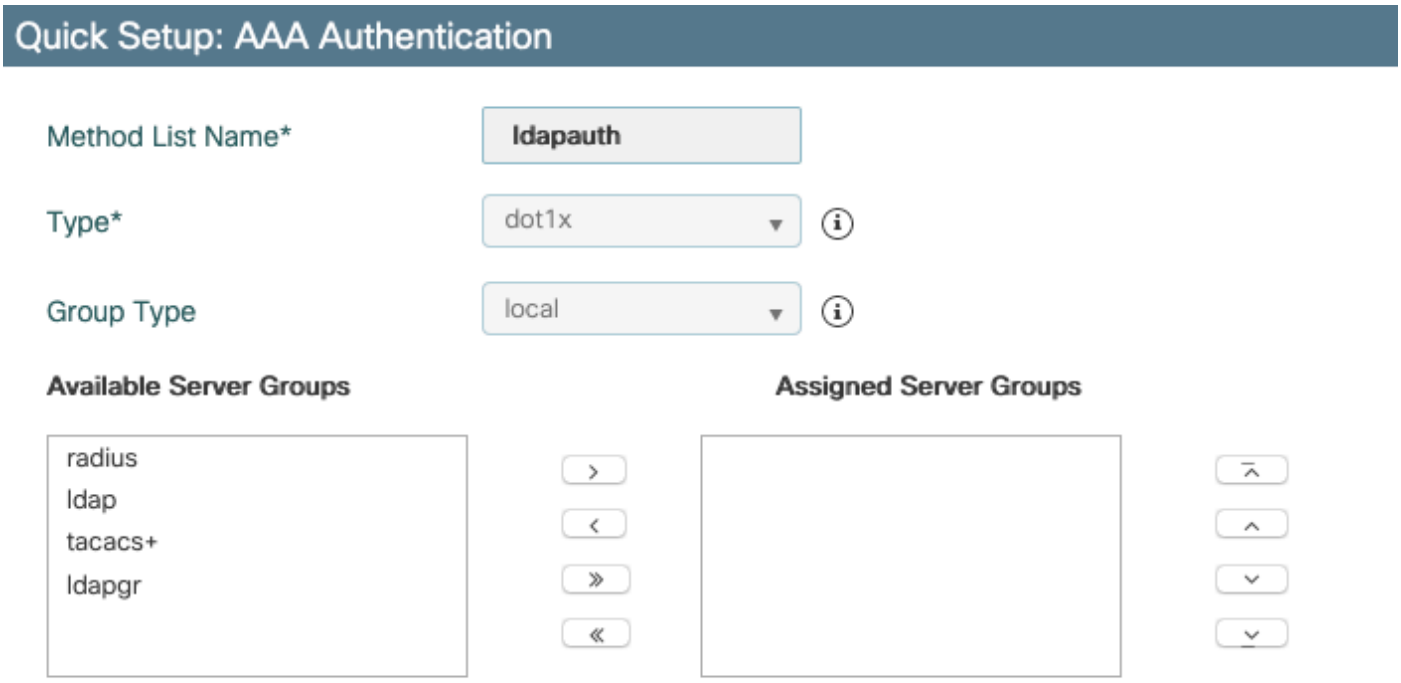
```
aaa group server ldap ldapgr server AD
```

الخطوة 4. تكوين أسلوب مصادقة AAA

انتقل إلى **التكوين > التأمين > AAA > قائمة طرق AAA > المصادقة** وانقر **+إضافة**

قم بتكوين أسلوب مصادقة **dot1x** النوع وقم بإشارته إلى المحلي فقط. قد يكون من المغري الإشارة إلى مجموعة خوادم LDAP ولكن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) نفسه هو الذي يعمل كمصدق 802.1X انه (على الرغم من أن قاعدة بيانات

المستخدم موجودة على LDAP، ولكن هذه هي وظيفة طريقة التخويل).



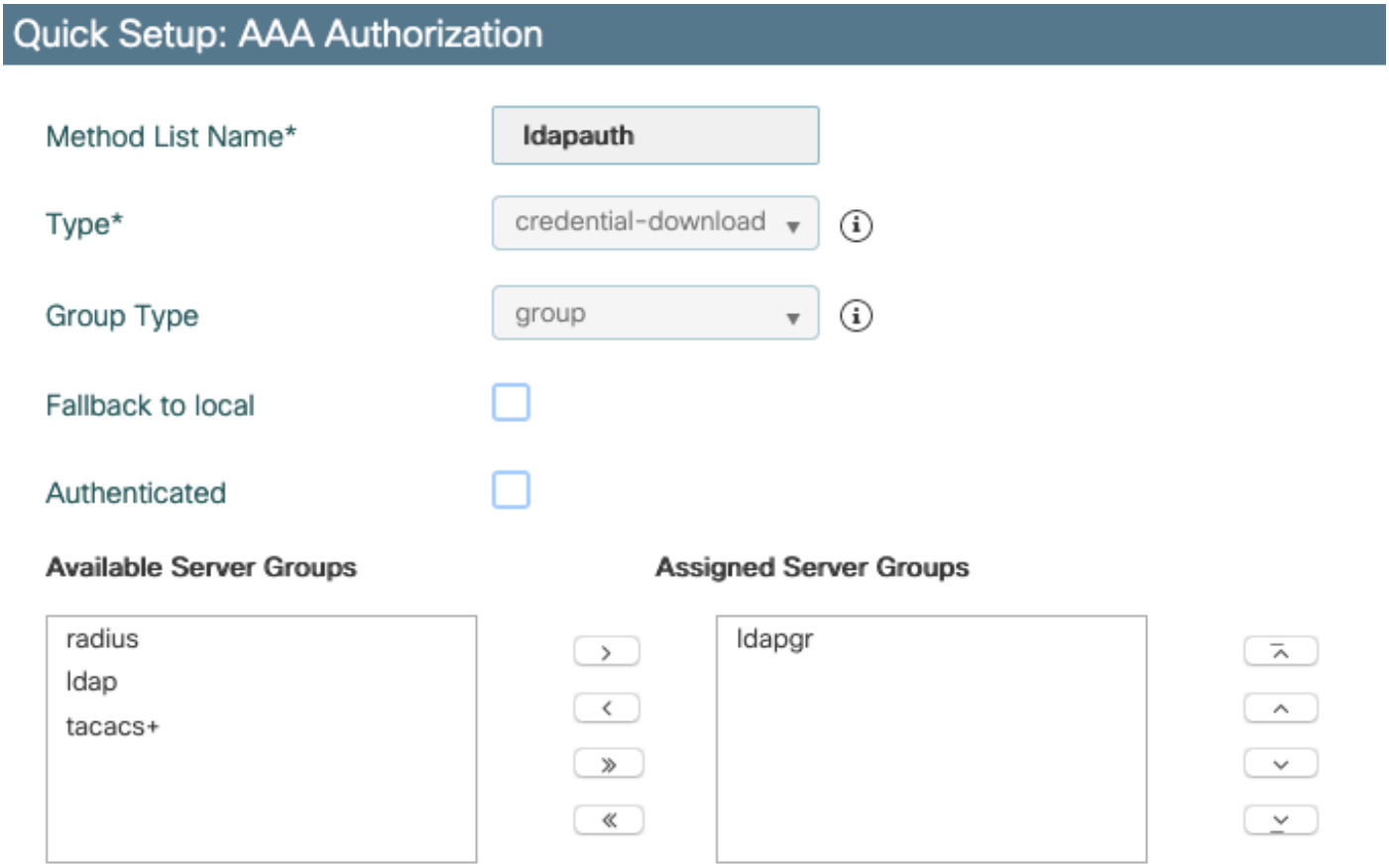
أمر CLI:

```
aaa authentication dot1x ldapauth local
```

الخطوة 5. تكوين أسلوب تفويض AAA

انتقل إلى **التكوين > التأمين > AAA > قائمة طرق AAA > التفويض** وانقر **+إضافة**

قم بإنشاء نوع **تنزيل بيانات الاعتماد** لأسلوب التخويل وجعله يشير إلى مجموعة LDAP.



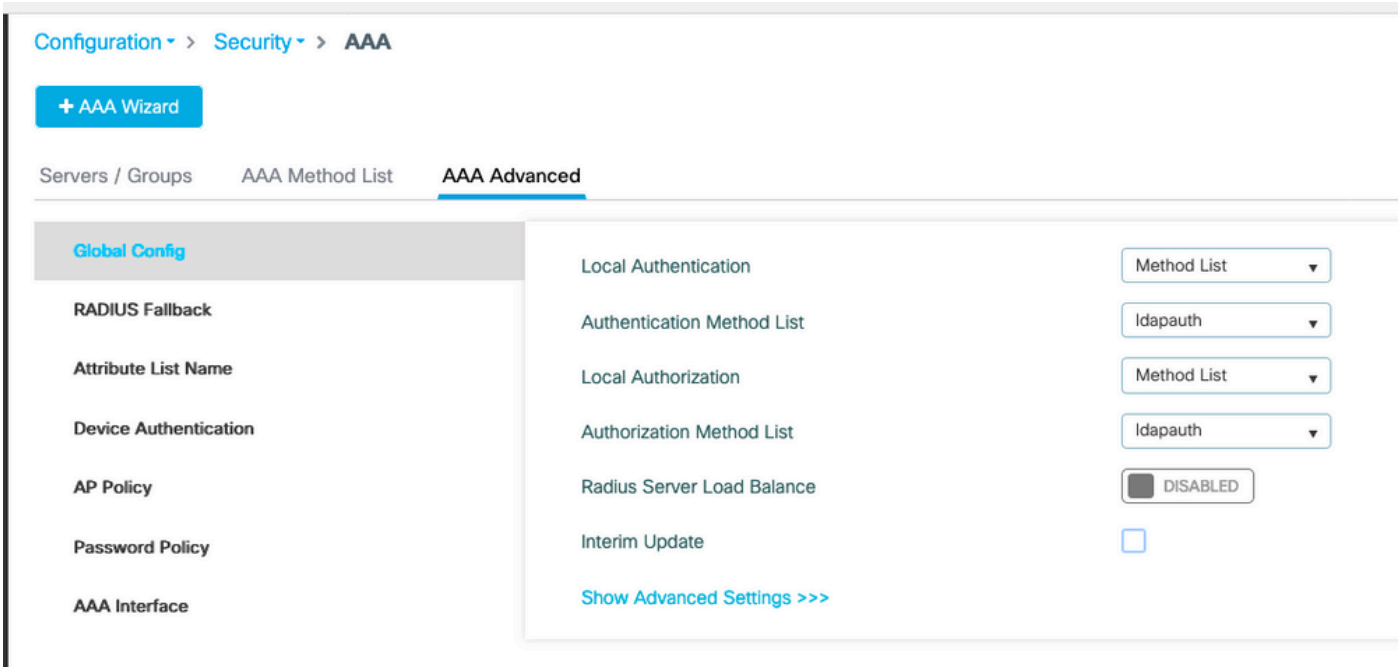
أمر واجهة سطر الأوامر :

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

الخطوة 6. تكوين تفاصيل المصادقة المحلية

انتقل إلى **التكوين > الأمان > AAA > قائمة طرق AAA > خيارات AAA المتقدمة**

أخترت **أسلوب قائمة** لكل من المصادقة والتفويض واخترت ال dot1x صحة هوية طريقة يشير محليا وأسلوب تخويل تنزيل بيانات الاعتماد يشير إلى LDAP



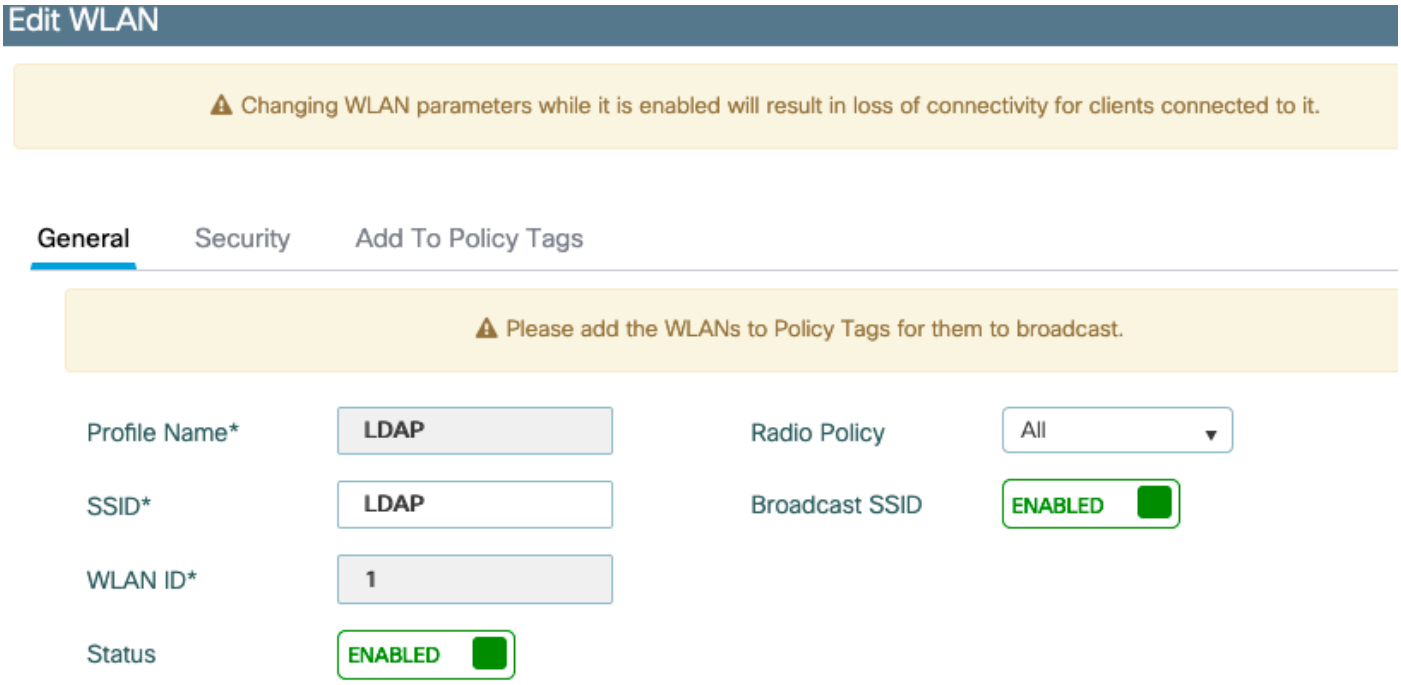
أمر واجهة سطر الأوامر :

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

الخطوة 7. تكوين a dot1x WLAN

انتقل إلى **التكوين > WLAN** وانقر **+إضافة**

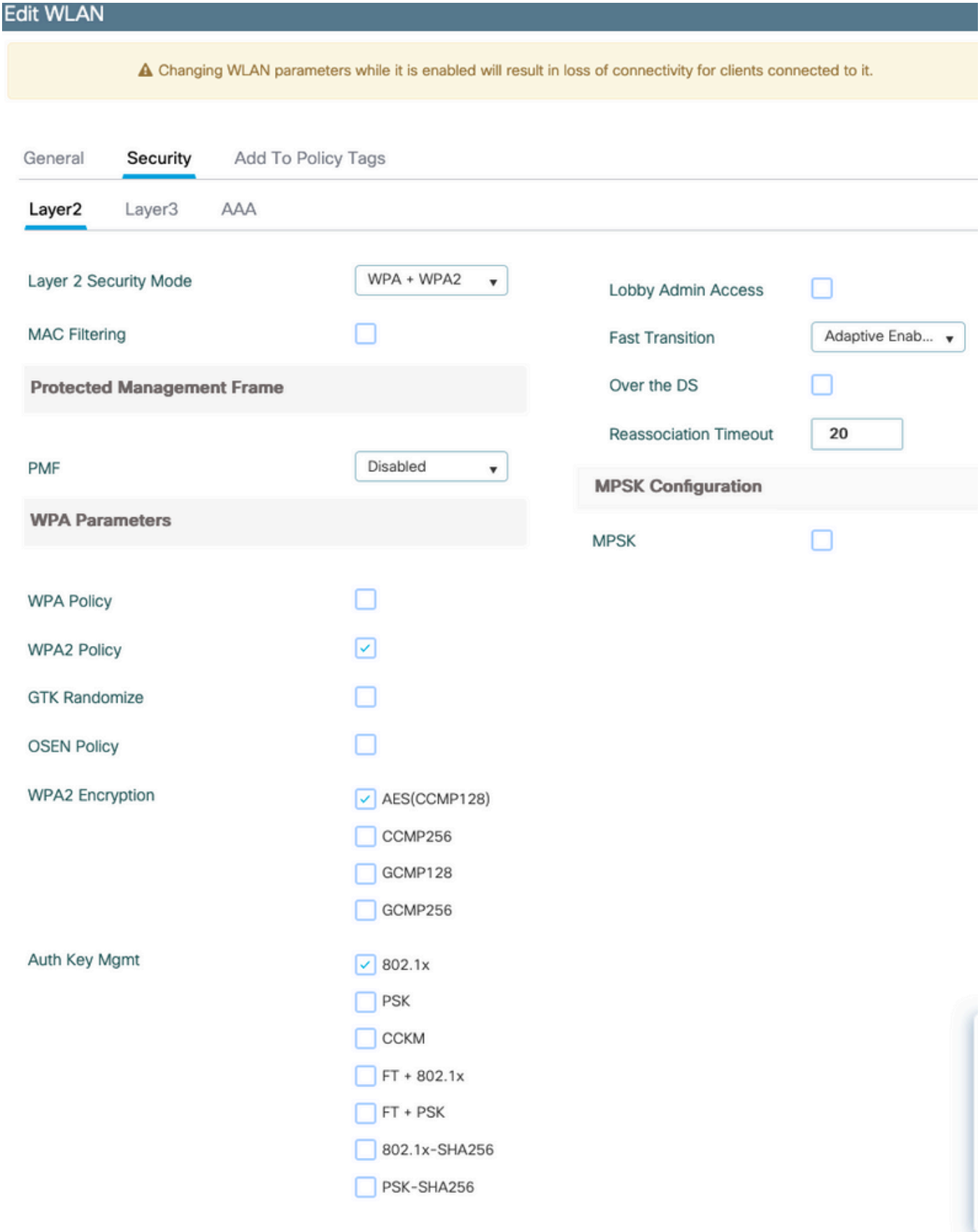
أختر توصيف واسم SSID وتأكد من تمكينه.



الانتقال إلى صفحة **تأمين** الطبقة 2.

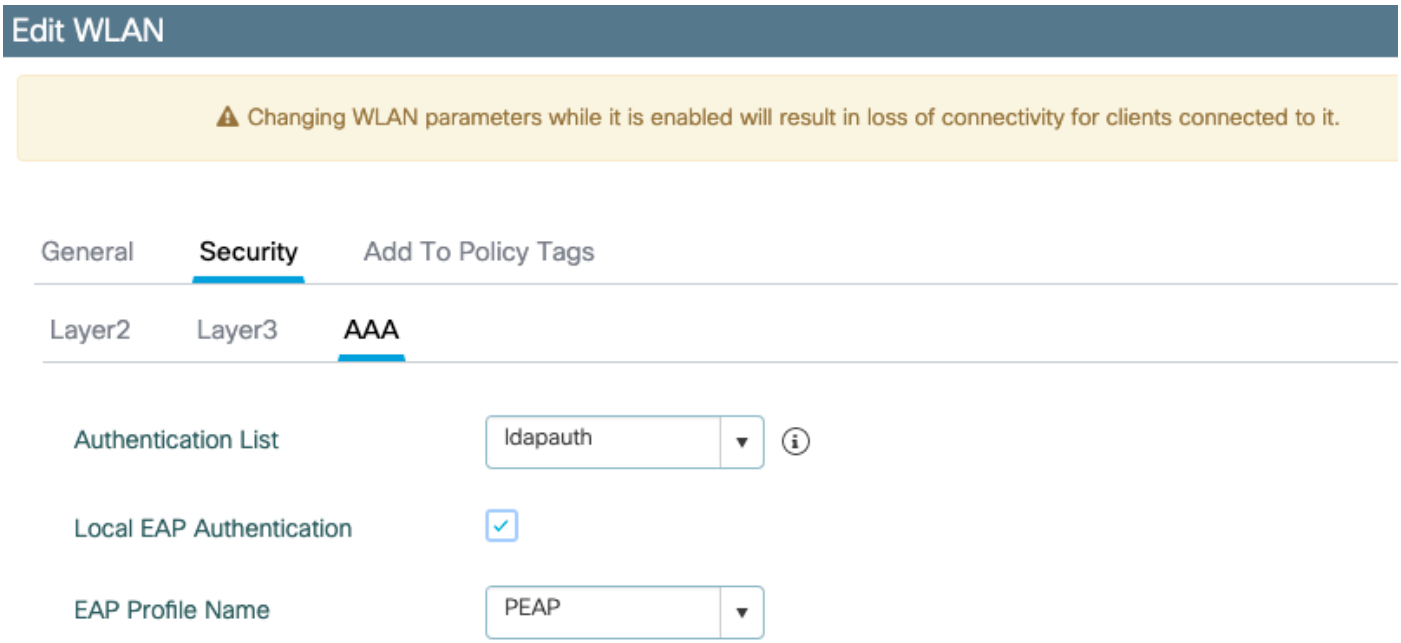
أختر WPA+WPA2 كوضع **تأمين الطبقة 2**

تأكد من تمكين WPA2 و AES في **معلمات WPA** وتمكين **802.1X**



انتقل إلى علامة التبويب الفرعية **AAA**.

انتقاء أسلوب مصادقة dot1x الذي تم إنشاؤه سابقا وتمكين مصادقة EAP المحلية وانتقاء ملف تعريف EAP الذي تم تكوينه في الخطوة الأولى.



حفظ بالنقر فوق تطبيق

أوامر CLI:

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

الخطوة 8. التحقق من بث WLAN

انتقل إلى **التكوين > علامات التمييز** وتأكد من تضمين SSID في ملف تعريف السياسة الذي تتم خدمته حاليا بواسطة SSID (علامة النهج الافتراضية لتكوين جديد جديد جديد جديد إذا لم تقم بتكوين علامات بعد). بشكل افتراضي، ال ثبت علامة السياسة الافتراضية SSIDs جديدة تقوم بإنشائها حتى تقوم بتضمينها يدويا.

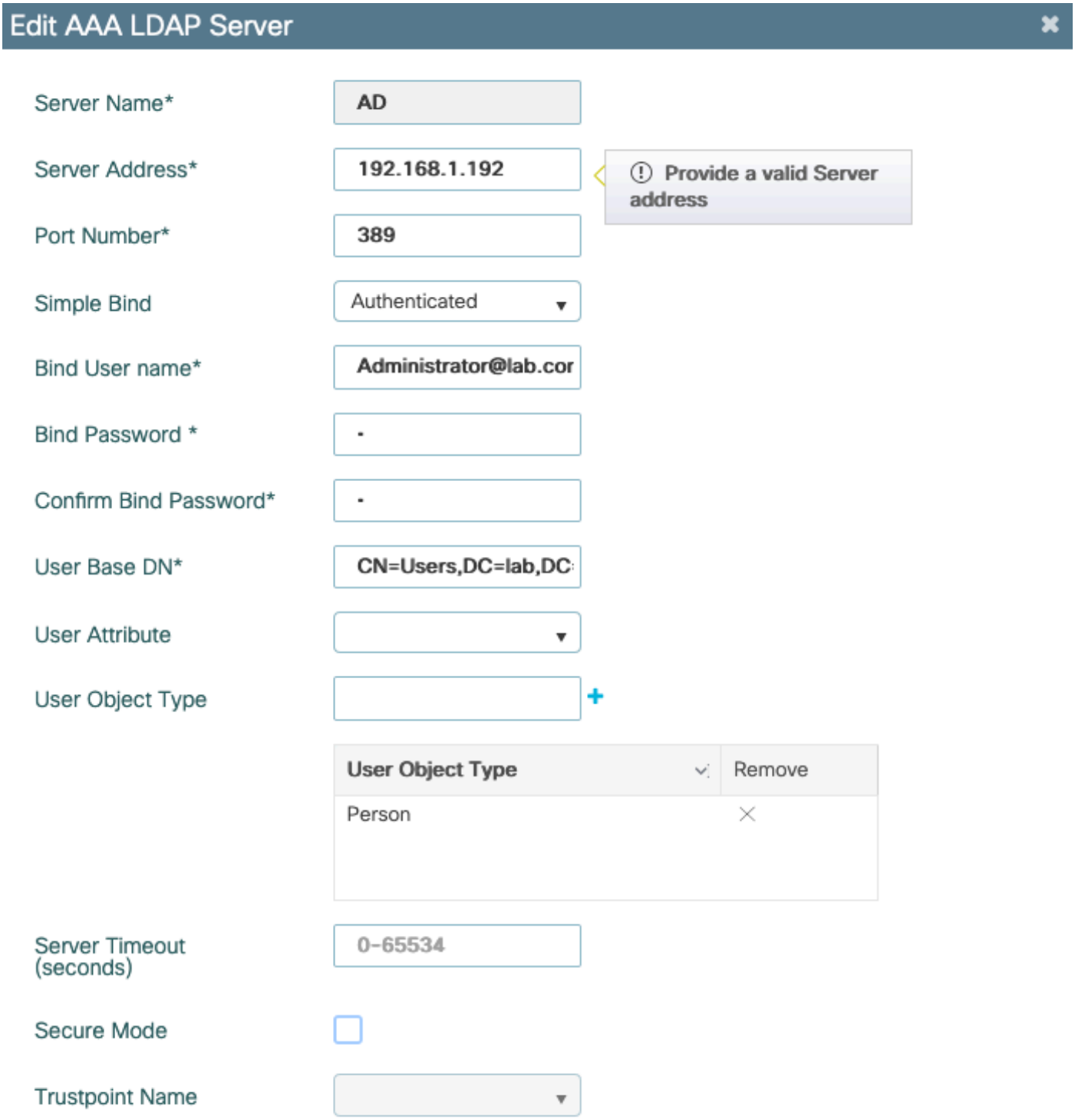
ال تغطي هذه المقالة تكوين ملفات تعريف السياسة وتفترض أنك على دراية بذلك الجزء من التكوين.

في حالة إستخدام Active Directory، يجب تكوين خادم AD لإرسال السمة "userPassword". يجب إرسال هذه السمة إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). وذلك لأن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يقوم بالتحقق، وليس خادم AD. يمكنك أيضا أن تواجه مشاكل في المصادقة مع أسلوب PEAP-MSCHAPV2 حيث أن كلمة المرور ال يتم إرسالها أبدا في نص واضح وبالتالي ال يمكن فحصها مع قاعدة بيانات LDAP، فالطريقة PEAP-GTC فقط هي التي تعمل مع قواعد بيانات LDAP معينة.

فهم تفاصيل خادم LDAP

فهم الحقول على واجهة مستخدم ويب 9800

فيما يلي مثال على Active Directory أساسي جدا يعمل كخادم LDAP تم تكوينه على 9800



الإسم و IP ذاتي التفسير بشكل مخيف.

المنفذ: 389 وه المنفذ الافتراضي ل LDAP ولكن يمكن للخادم الخاص بك إستخدام منفذ آخر.

ربط بسيط: من النادر جدا أن يكون لديك قاعدة بيانات LDAP في الوقت الحالي تدعم الربط غير المصدق عليه (هذا يعني أنه أي شخص يمكنه إجراء بحث LDAP عليه بدون أي نموذج مصادقة). الربط البسيط المصدق هو النوع الأكثر شيوعا للمصادقة وما يسمح به Active Directory بشكل افتراضي. يمكنك إدخال اسم حساب مستخدم وكلمة مرور لتتمكن من إجراء البحث في قاعدة بيانات المستخدم من هناك.

ربط اسم المستخدم: تحتاج إلى الإشارة إلى اسم مستخدم له امتيازات المسؤول في Active

Directory. تتحمل AD تنسيق "user@domain" له بيئمإ تتوقع العديد من قواعد بيانات LDAP الأخرى تنسيق "CN=xxx،DC=xxx" لاسم المستخدم. يوجد مثال على قاعدة بيانات LDAP أخرى غير AD يرد فيما بعد في هذه المقالة.

ربط كلمة السر : دخلت الكلمة الإدارة username دخلت سابقا.

DN الخاص بقاعدة المستخدم: أدخل هنا "جذر البحث"، وهو الموقع الموجود في شجرة LDAP حيث تبدأ عمليات البحث. في هذا المثال، تكون جميع استخدامات نمضن مجموعة "المستخدمين"، والتي يكون DN الخاص بها "cn=Users،dc=lab،dc=com" (انظر المثال LDAP لمجال lab.com). يتم توفير مثال على كيفية اكتشاف DN قاعدة المستخدم هذه لاحقا في هذا القسم.

سمة المستخدم: يمكن ترك هذا الحقل فارغا أو الإشارة إلى خطط سمة LDAP الذي يشير إلى حقل LDAP الذي يعد اسم المستخدم لقاعدة بيانات LDAP الخاصة بك. مهم، واجب cisco قبل id CSCvv11813 ، تحاول عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إجراء اتصال مع حقل CN بغض النظر عن أي شيء.

نوع كائن المستخدم: يحدد هذا نوع الكائنات التي تعتبر مستخدمين. عادة ما يكون هذا الشخص وهو الشخص. يمكن أن تكون "أجهزة كمبيوتر" إذا كان لديك قاعدة بيانات AD وتخول حسابات الكمبيوتر، ولكن هناك مرة أخرى وفر LDAP الكثير من التخصيص.

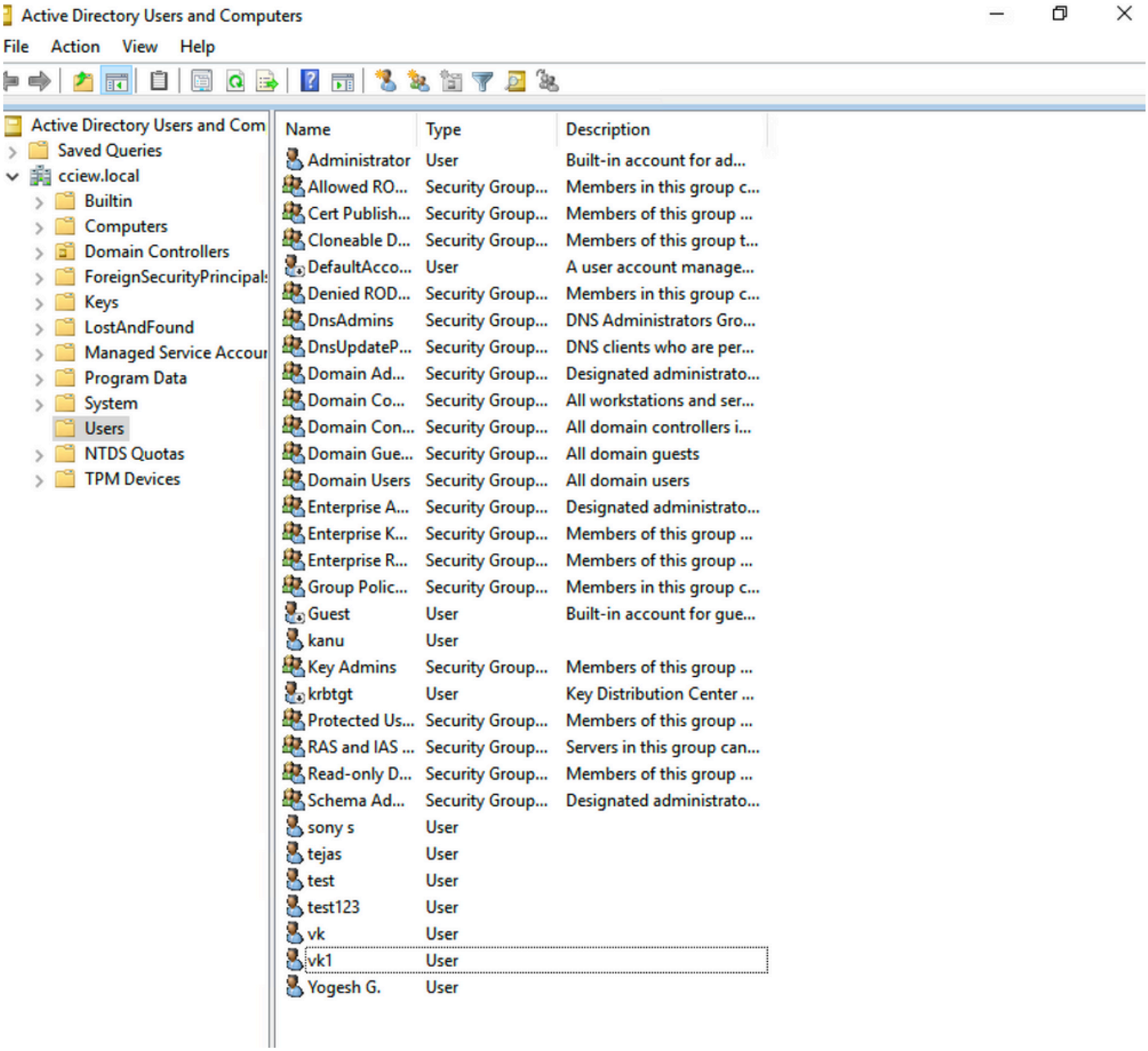
يتيح الوضع الآمن LDAP الآمن عبر TLS ويتطلب منك تحديد TrustPoint على 9800 لاستخدام شهادة لتشفير TLS.

مصادقة LDAP 802.1x مع سمة sAMAaccountName.

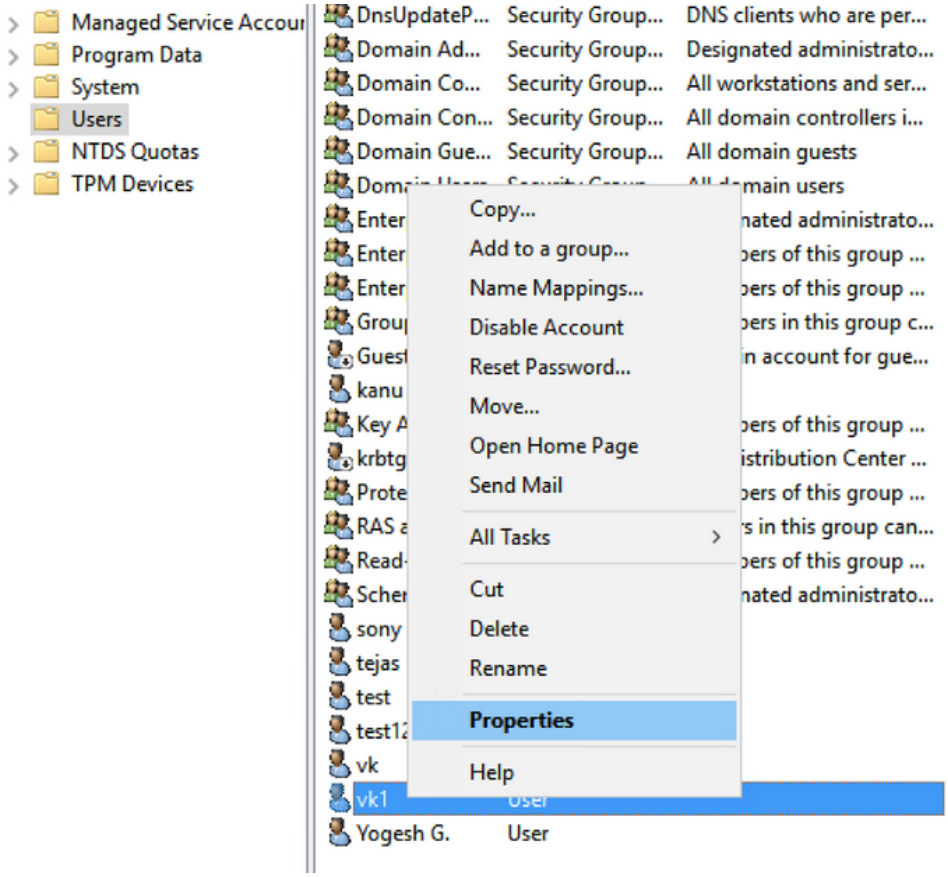
وقد تم إدخال هذا التعزيز في الإصدار 17.6.1.

قم بتكوين سمة "userPassword" للمستخدم.

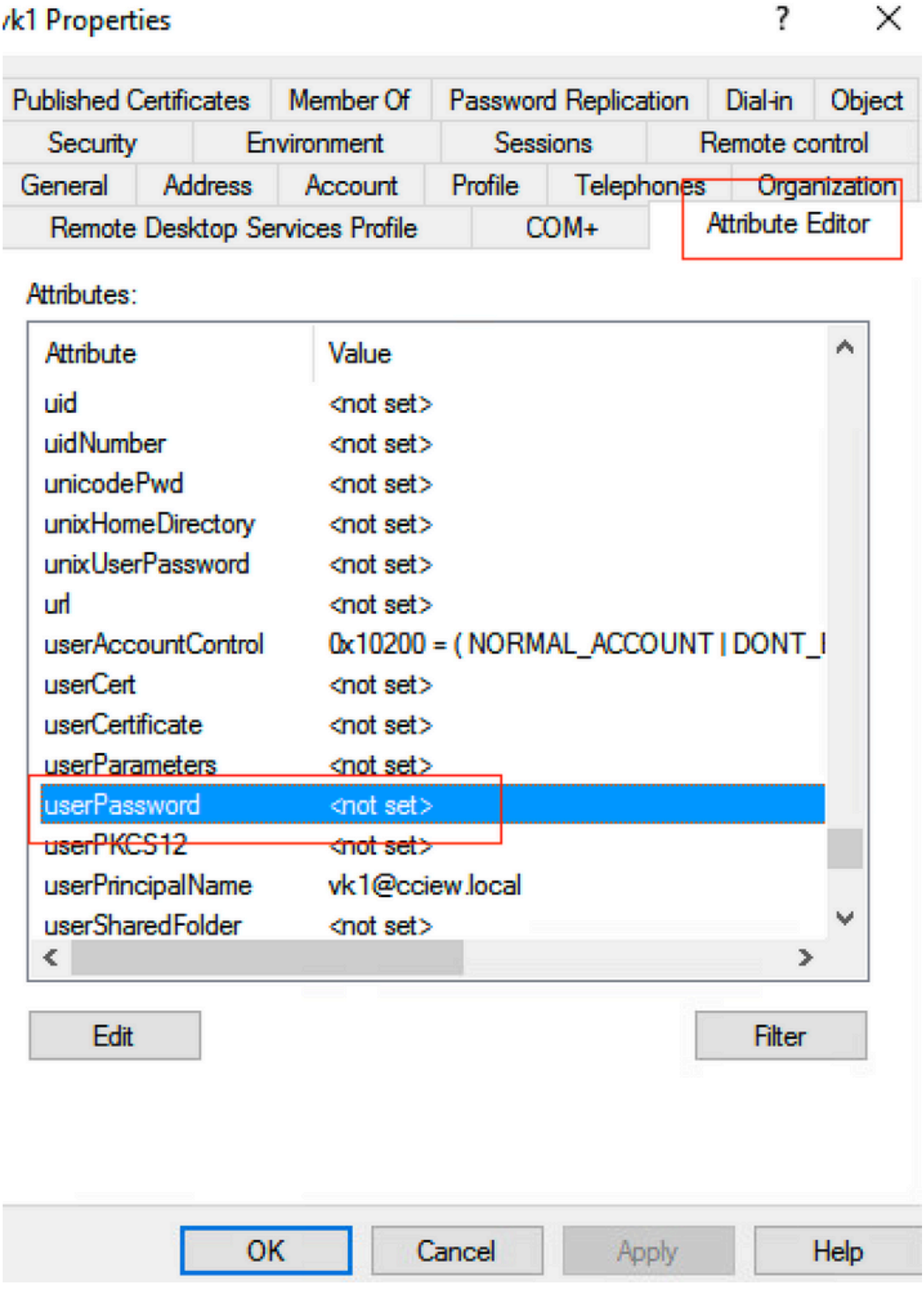
الخطوة 1. على خادم Windows انتقل إلى ActiveDirectory Users and Computers



الخطوة 2. انقر بزر الماوس الأيمن فوق اسم المستخدم الخاص وحدد الخصائص

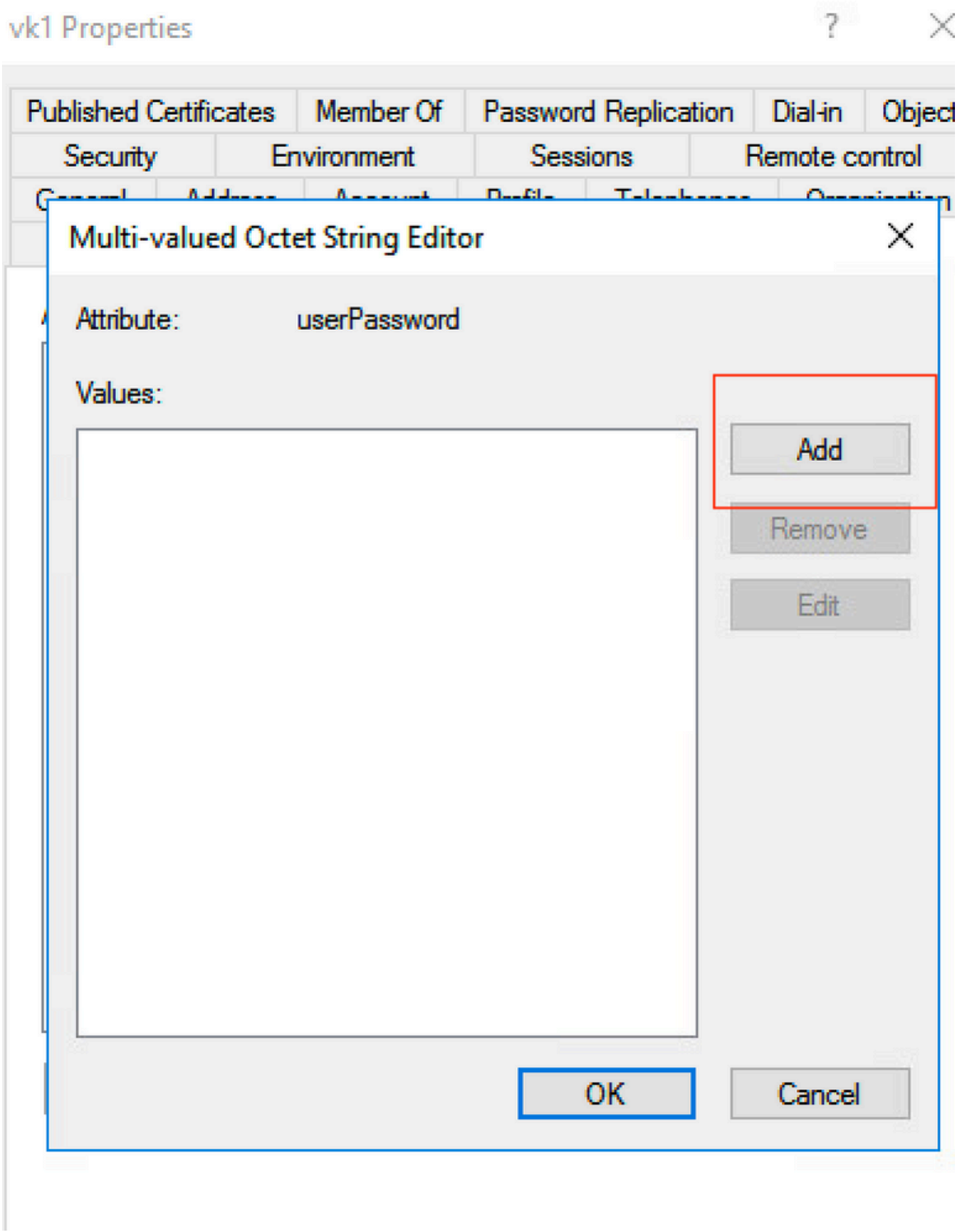


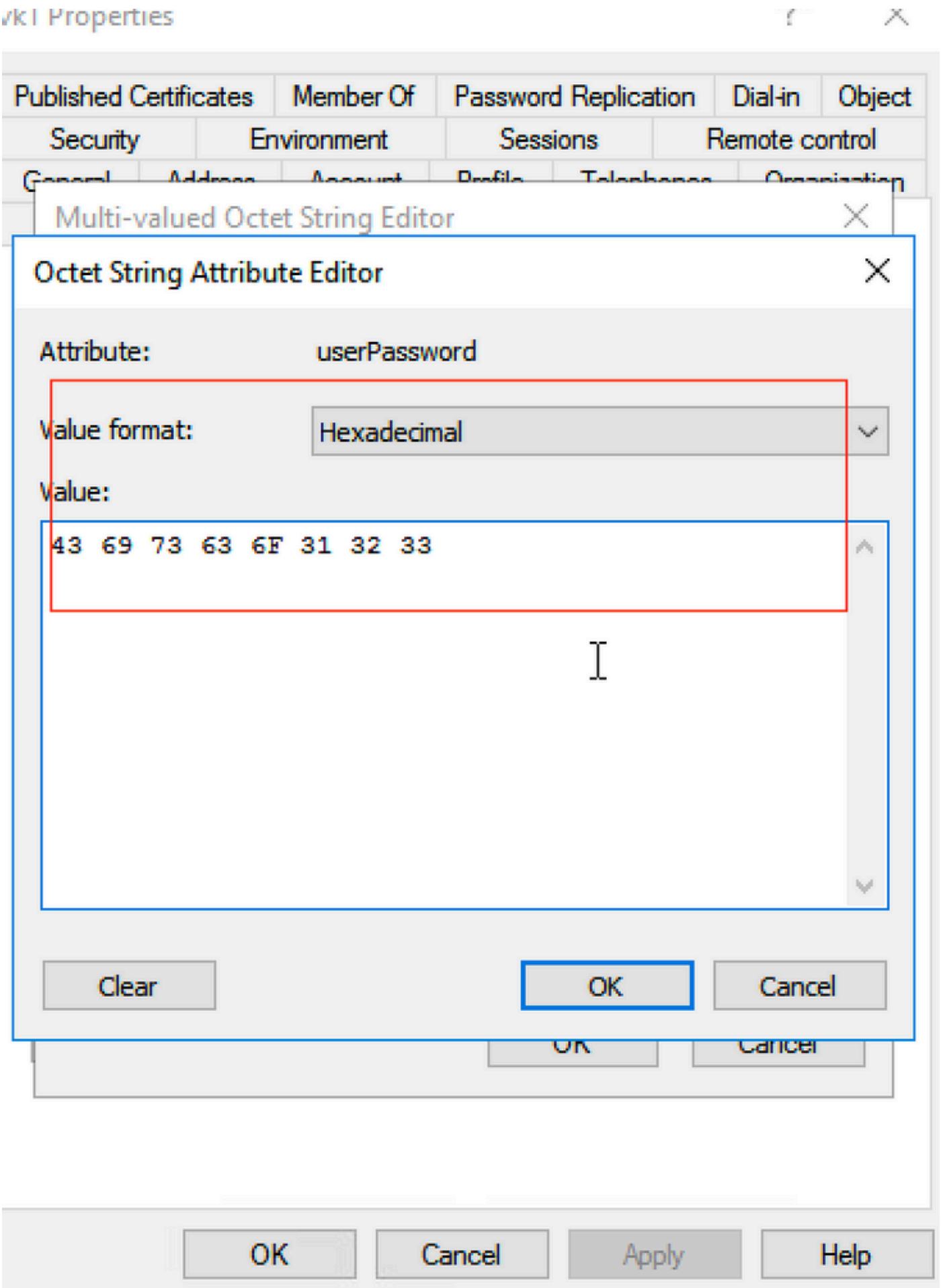
الخطوة 3. تحديد محرر السمات في نافذة الخصائص



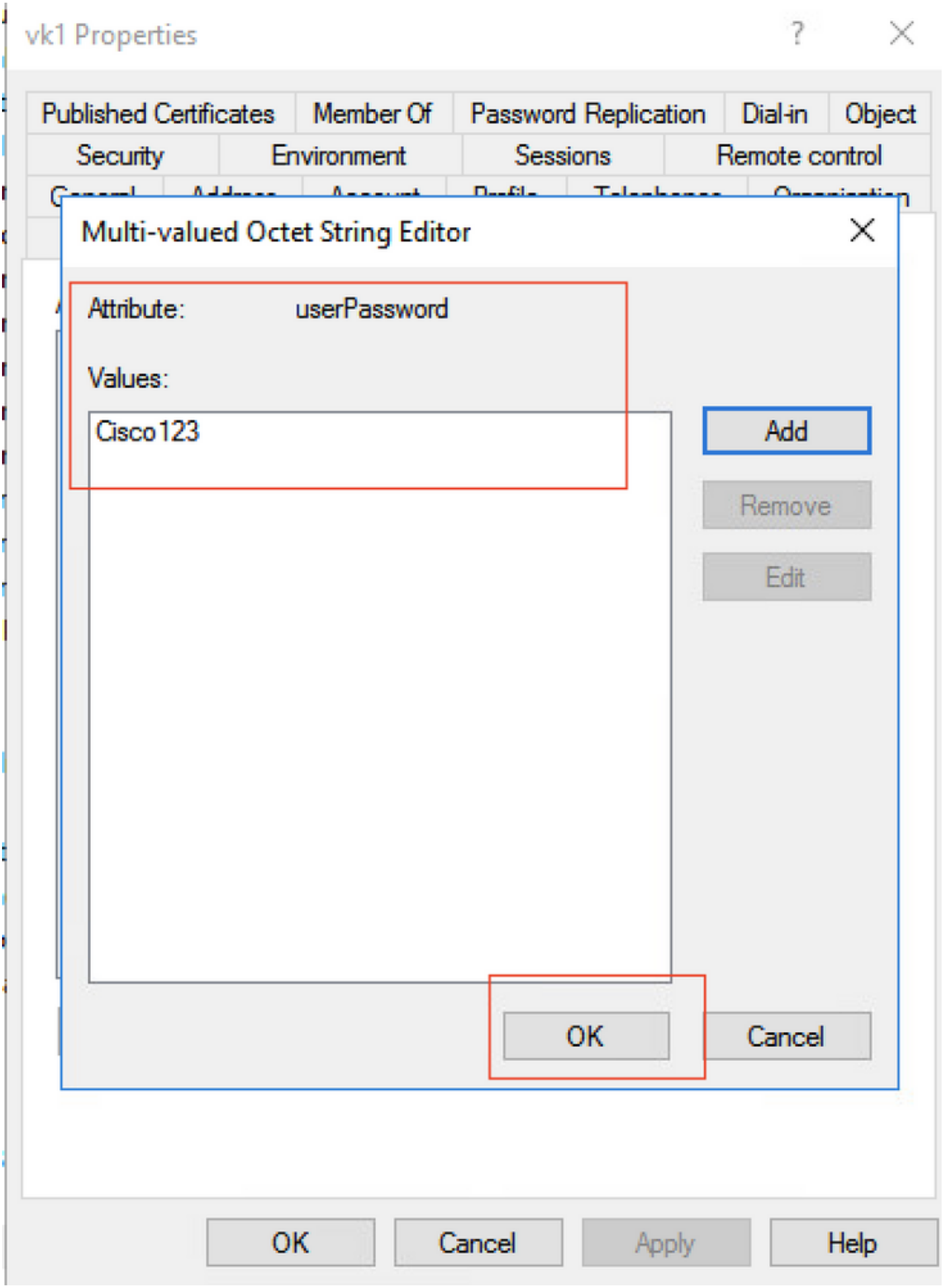
الخطوة 4. تكوين سمة "userPassword". هذه هي كلمة المرور للمستخدم، والتي يجب تكوينها

في قيمة سداسية عشرية.

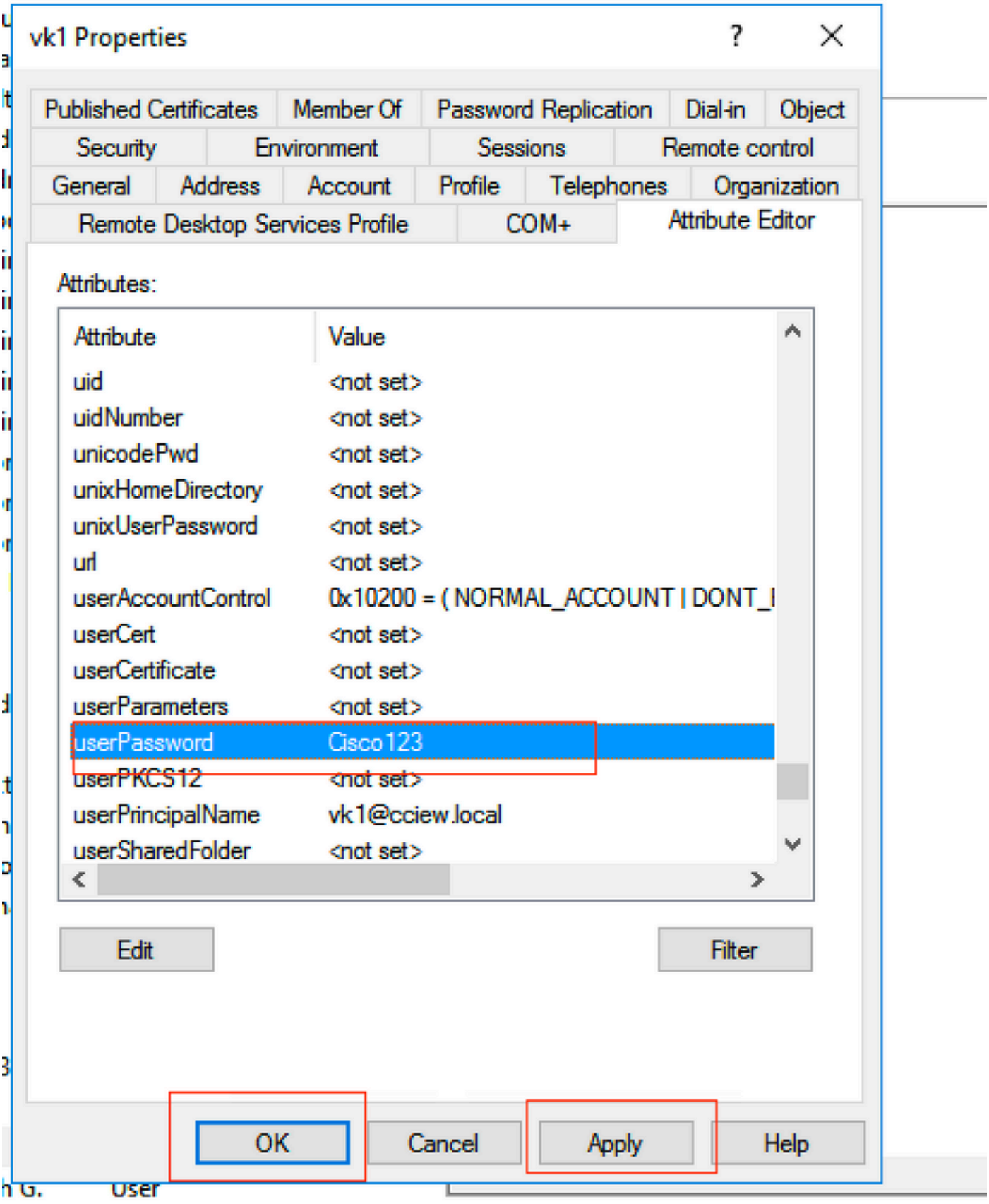




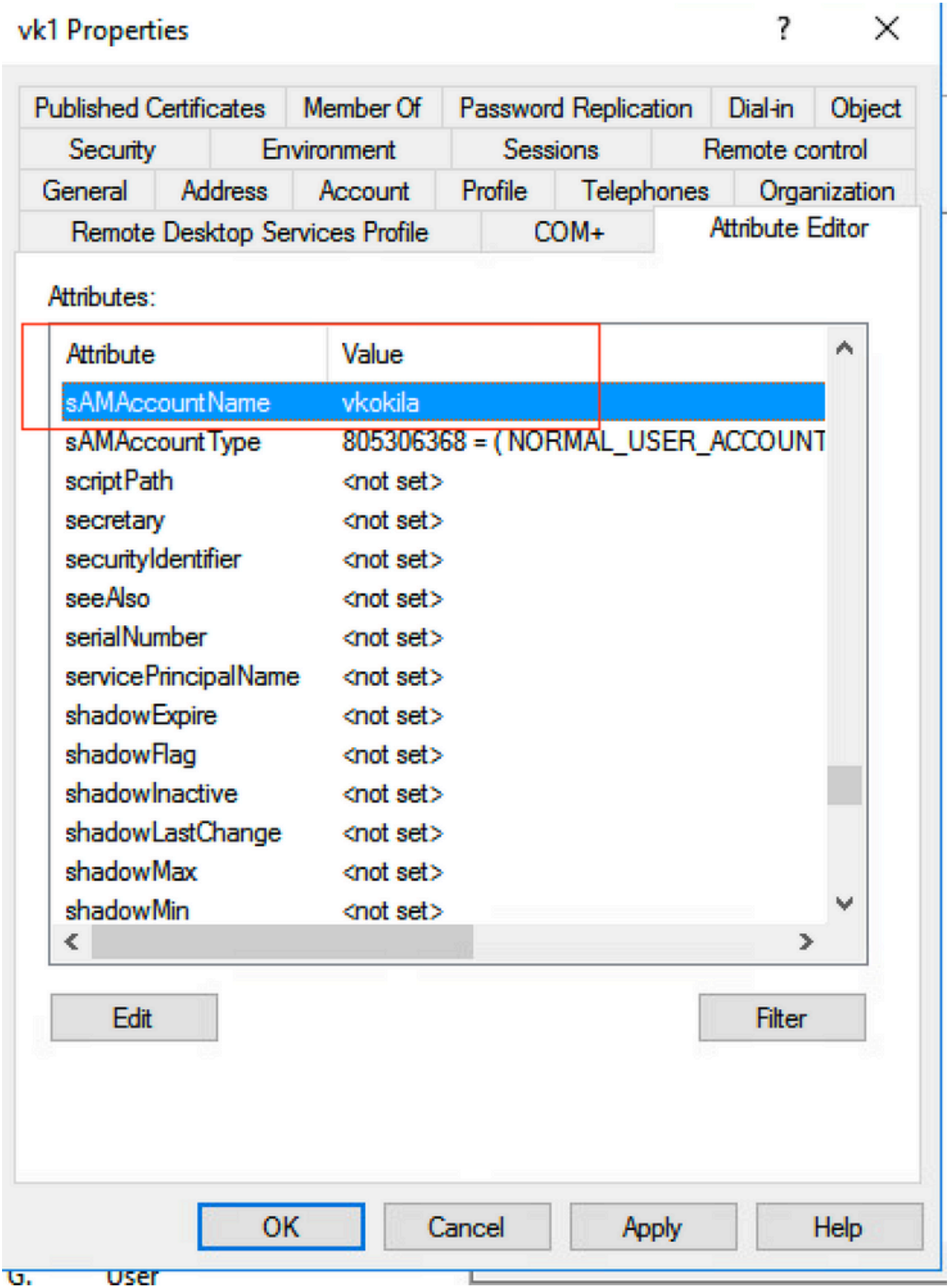
انقر فوق موافق، تحقق مما إذا كانت تظهر كلمة المرور الصحيحة



الخطوة 5. طقطقة يطبق وبعد ذلك ok



الخطوة 6. تحقق من قيمة السمة "sAMAccountName " للمستخدم وسوف يكون هو اسم المستخدم للمصادقة.


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
secretary
securityIdentifier
seeAlso
serialNumber
servicePrincipalName
shadowExpire
shadowFlag
shadowInactive
shadowLastChange
shadowMax
shadowMin
<not set>
Edit
Filter
OK
Cancel
Apply
Help

تكوين WLC:

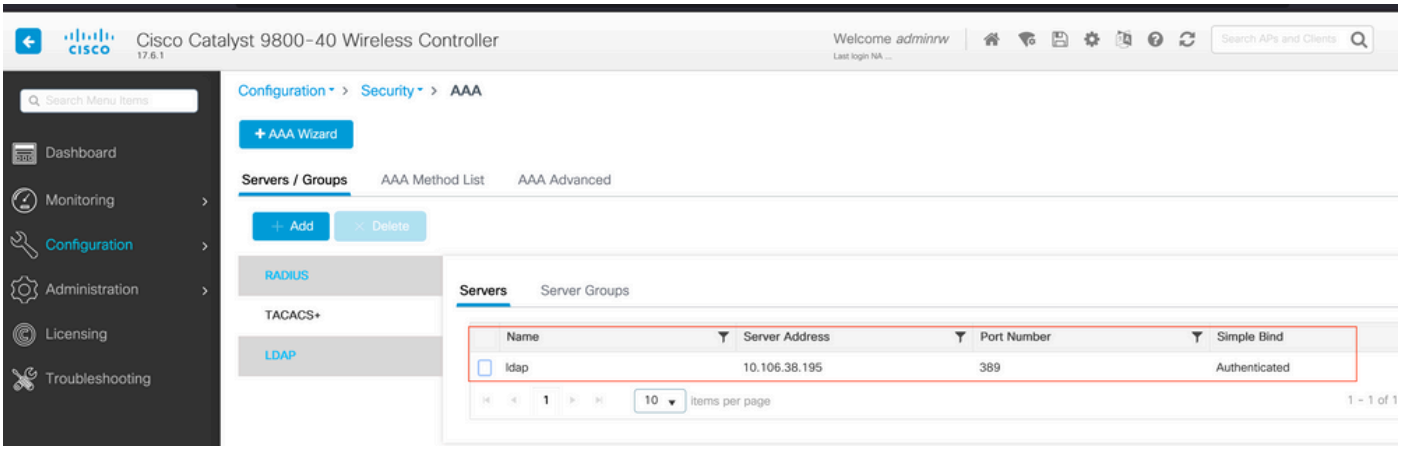
الخطوة 1. إنشاء تعيين سمة LDAP

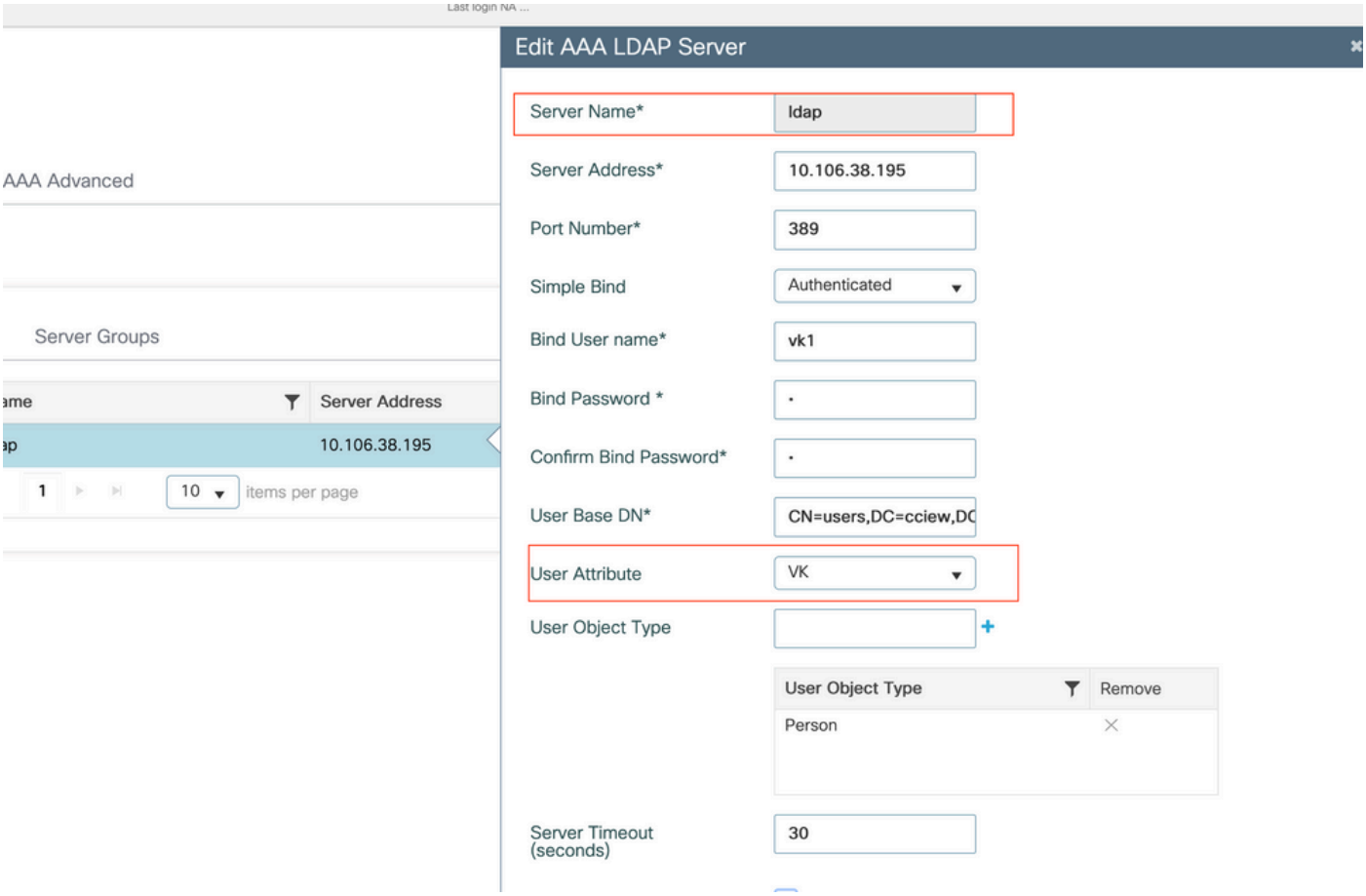
الخطوة 2. تكوين السمة "sAMAccountName" والنوع ك "username"

الخطوة 3. أختر تعيين السمات التي تم إنشاؤها ضمن تكوين خادم LDAP.

```
ldap attribute-map VK

 map type sAMAccountName username



ldap server ldap

 ipv4 10.106.38.195

 attribute map VK

 bind authenticate root-dn vk1 password 7 00271A1507545A545C

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

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

التحقق من واجهة الويب:





التحقق من الصحة

للتحقق من التكوين الخاص بك، تحقق مرة أخرى من أوامر CLI باستخدام الأوامر الواردة من هذه المقالة.

لا توفر قواعد بيانات LDAP عادة سجلات مصادقة حتى يمكن أن يكون من الصعب معرفة ما يحدث. قم بزيارة قسم أستكشاف الأخطاء وإصلاحها في هذه المقالة لمعرفة كيفية أخذ المسارات والتقاط sniffer لمعرفة ما إذا تم إنشاء اتصال بقاعدة بيانات LDAP أم لا.

استكشاف الأخطاء وإصلاحها

لاستكشاف هذه المشكلة وإصلاحها، من الأفضل تقسيمها إلى جزئين. يقوم الجزء الأول بالتحقق من صحة جزء EAP المحلي. والثاني هو التحقق من صحة اتصال 9800 بخادم LDAP بشكل صحيح.

كيفية التحقق من عملية المصادقة على وحدة التحكم

يمكنك تجميع تتبع مشع للحصول على "تصحيح أخطاء" اتصال العميل.

ما عليك سوى الانتقال إلى ميزة **أستكشاف المشكلات وحلها > التتبع الإشعاعي**. أضف عنوان MAC للعميل (انتبه إلى أن العميل يمكن أن يستخدم MAC عشوائي وليس MAC الخاص به، ويمكنك التحقق من ذلك في ملف تعريف SSID على جهاز العميل نفسه) واضغط على البدء.

بمجرد إعادة إنشاء محاولة الاتصال، يمكنك النقر فوق "إنشاء" والحصول على السجلات خلال الدقائق X الأخيرة. تأكد من النقر **داخلي** لأن بعض سطور سجل LDAP لا تظهر إذا لم تكن

قارداا علىذلك.

فيما يلي مثال على التتبع الإشعاعي لعميل تمت مصادقته بنجاح على SSID لمصادقة ويب. تمت إزالة بعض الأجزاء المتكررة لضمان الوضوح :

```
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

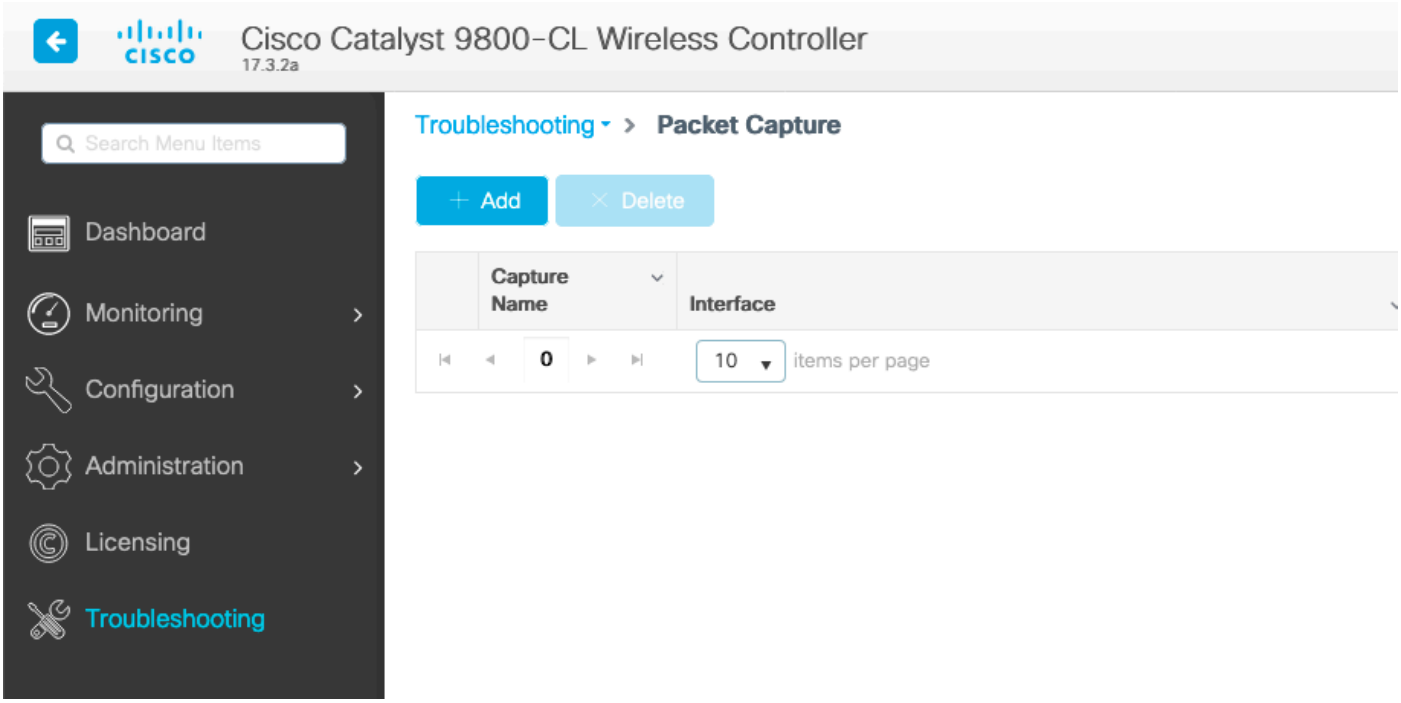
[https://192.0.2.1:443/favicon.ico] 2021/01/19 21:58:06.719646 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.9c09][192.168.1.17]Retrieved user-agent = Mozilla/5.0 (Linux; Android 11; SM-G970F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Mobile Safari/537.36 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
```

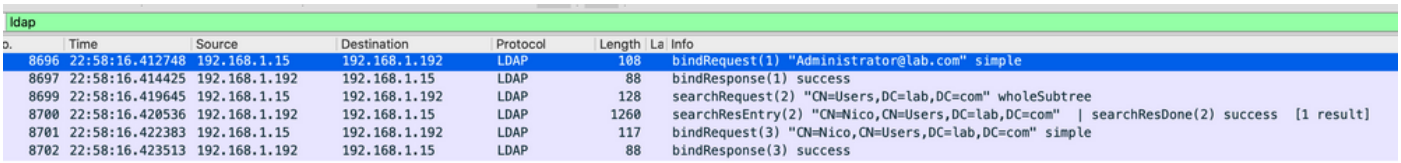
كيفية التحقق من اتصال 9800 ب LDAP

يمكنك أخذ التقاط مدمج في ال 9800 in order to رأيت أي حركة مرور باتجاه LDAP.

التقاط من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى **أدوات استكشاف الأخطاء وإصلاحها > التقاط الحزمة** وقوق رقنوا **إضافة+**. أختر منفذ الوصلة التقاط.



فيما يلي نموذج للمصادقة الناجحة للمستخدم Nico



تمثل الحزم الأولى 2 ربط WLC ب LDAP، وهو مصادقة WLC إلى قاعدة البيانات مع مستخدم المسؤول (من أجل أن يكون قادرا على إجراء بحث).

تمثل حزم LDAP التالية عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) التي تقوم بالبحث في شبكة DN الأساسية (هنا CN=Users،DC=lab،DC=com). يحتوي الجزء الداخلي للحزمة على عامل تصفية السمة المستخدم (هنا "Nico"). ترجع قاعدة بيانات LDAP سمات المستخدم كنجاح

تمثل الحزم 2 الأخيرة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الذي يحاول المصادقة مع كلمة مرور المستخدم هذه لاختبار ما إذا كانت كلمة المرور هي الكلمة الصحيحة.

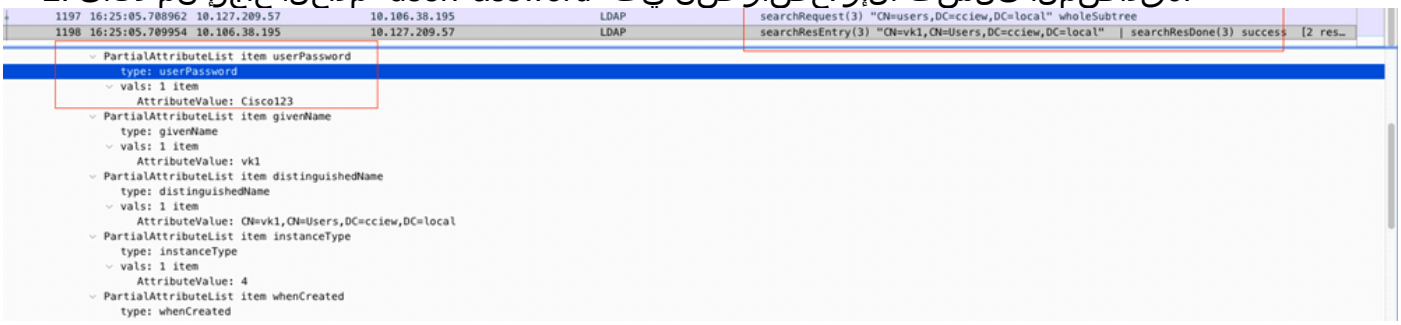
1. تجميع EPC والتحقق من تطبيق "sAMAccountName" كعامل تصفية:

إذا عرض عامل التصفية "cn" وكان "sAMAccountName" قيد الاستخدام كاسم مستخدم، فإن

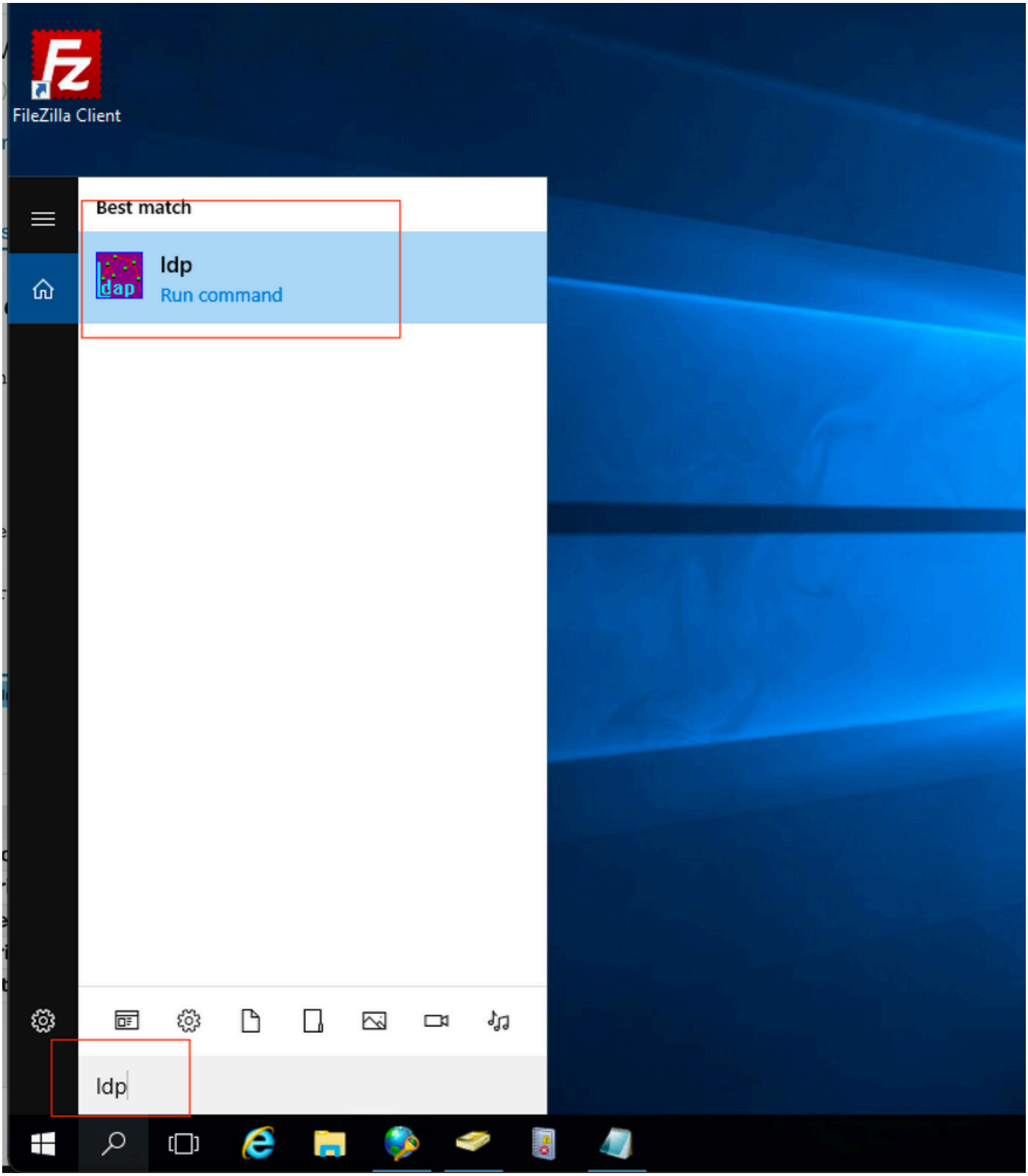
المصادقة تفشل.

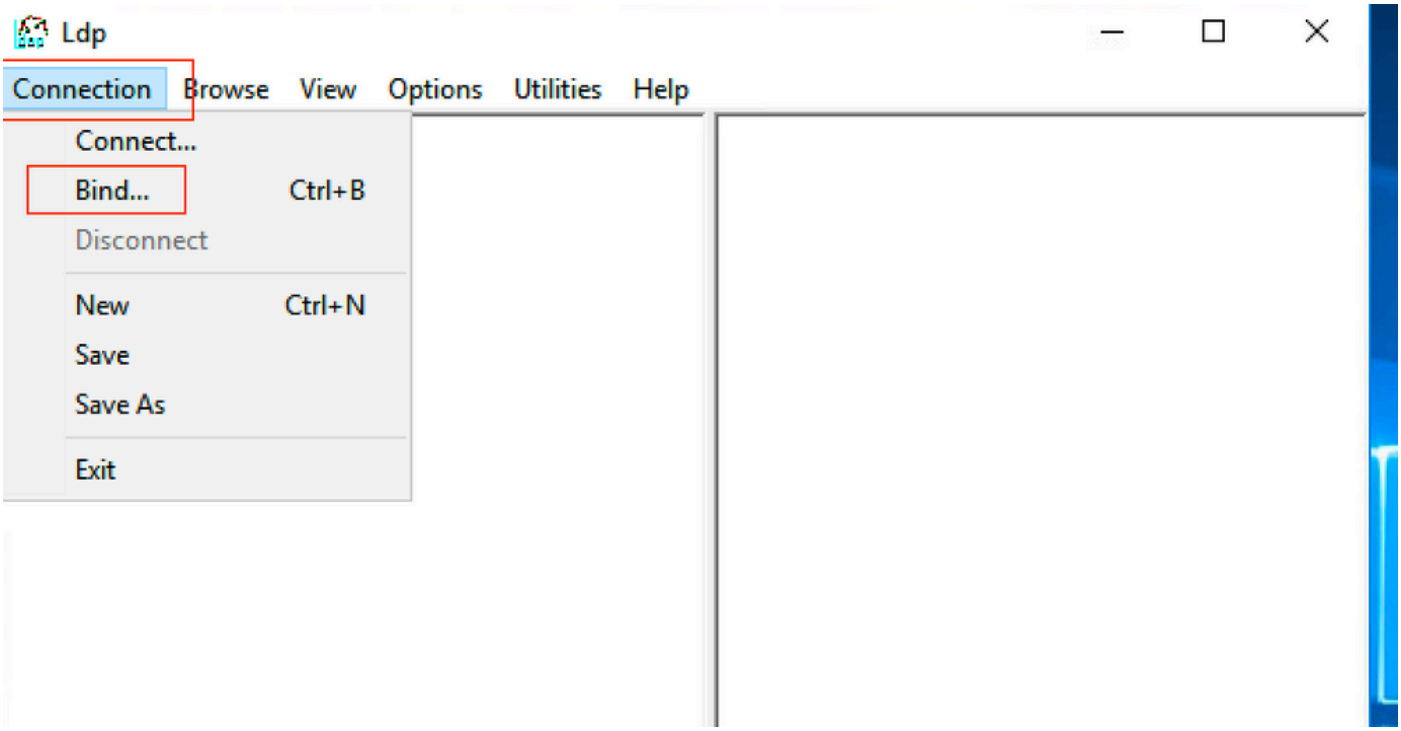
أعد تكوين سمة خريطة ldap من واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC).

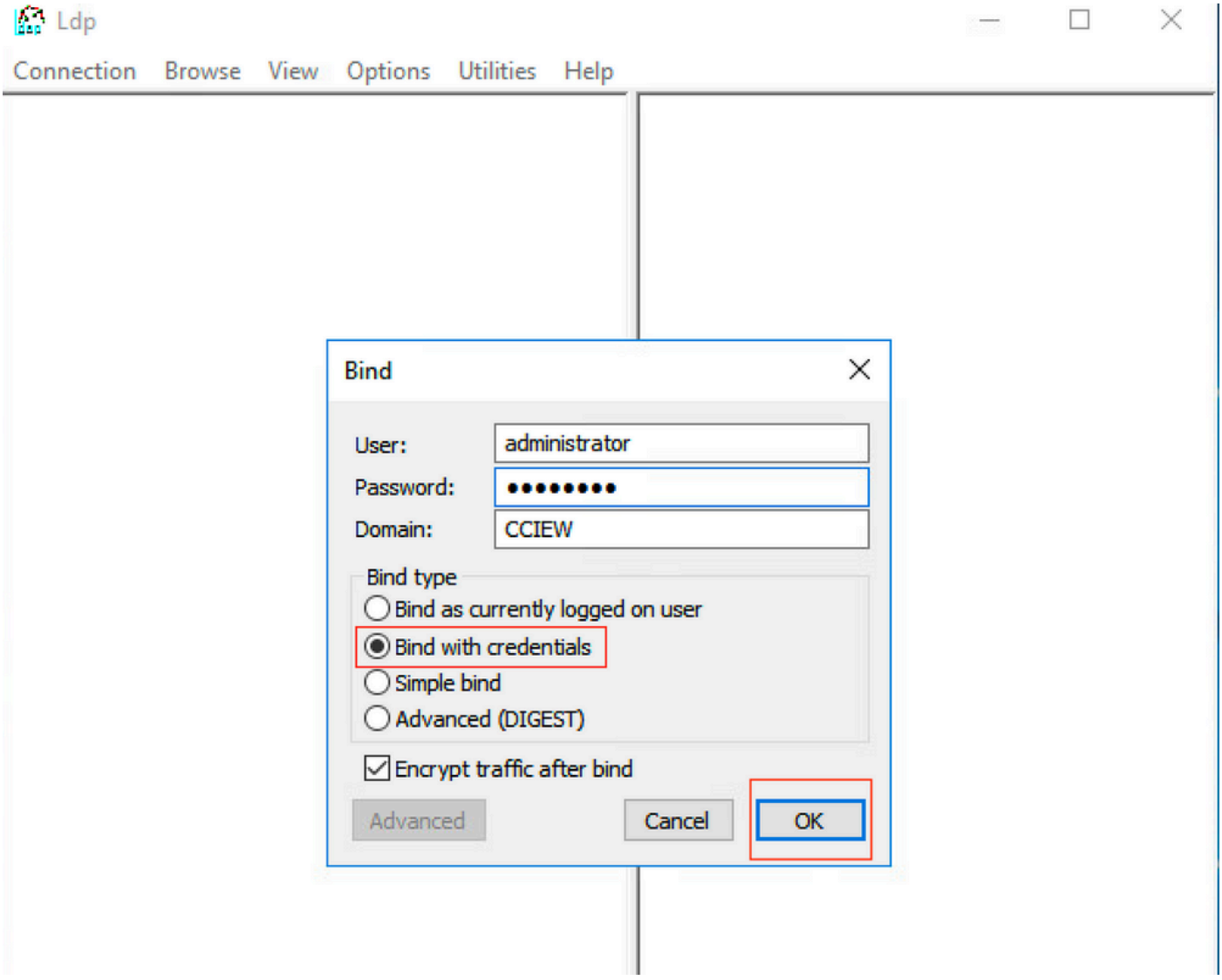
2. تأكد من إرجاع الخادم "userPassword" في نص واضح، وإلا فشلت المصادقة.

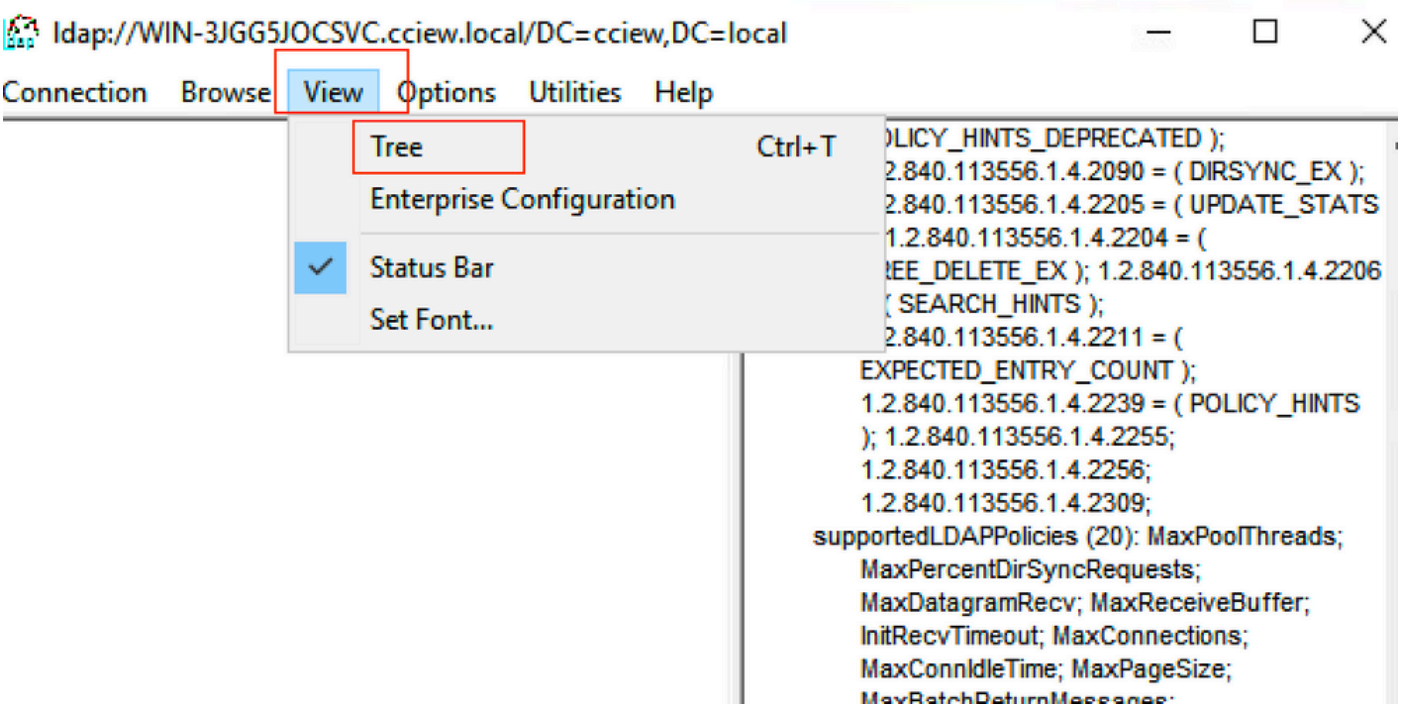


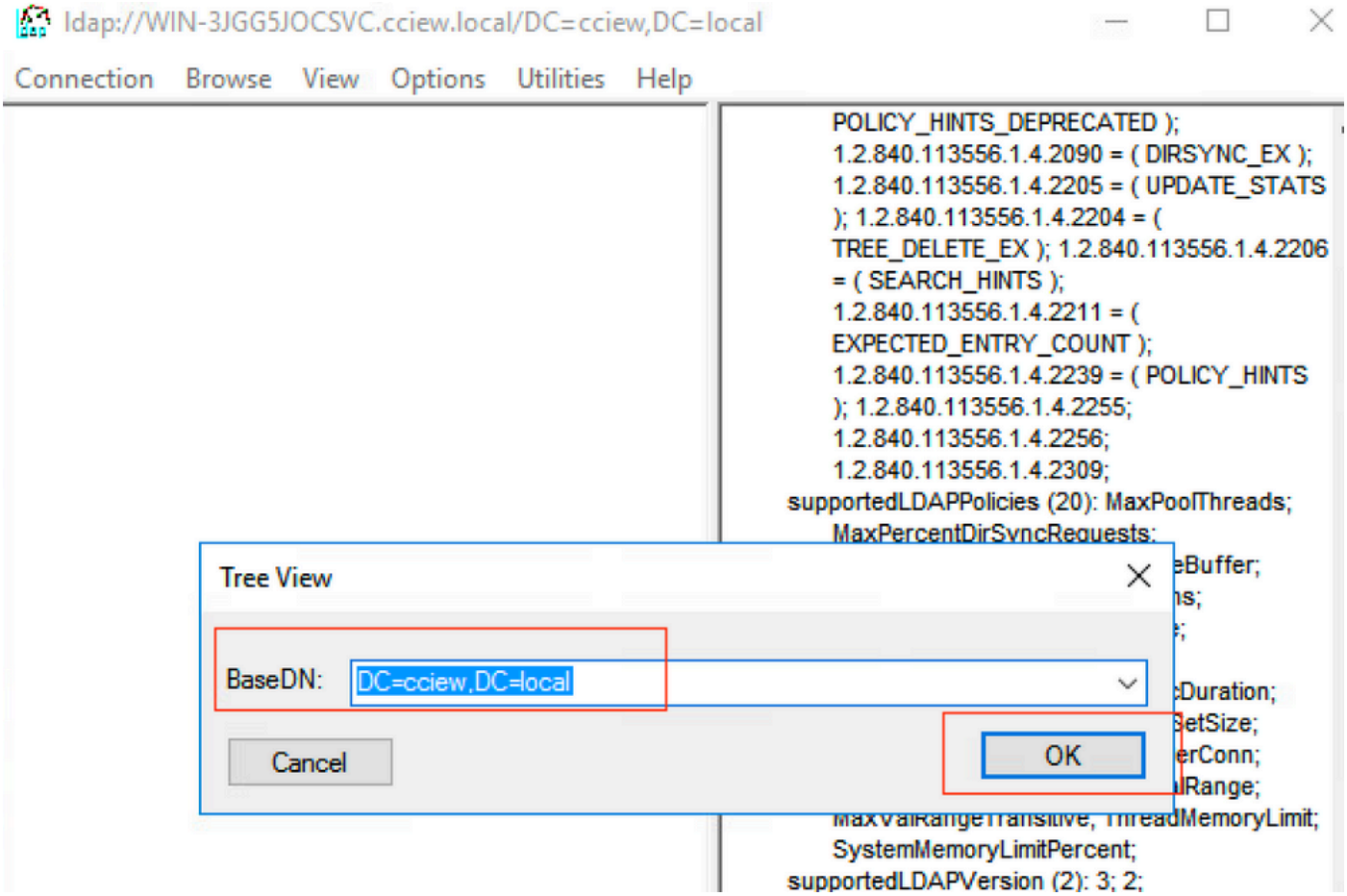
3. أستخدم أداة LDP.exe على الخادم للتحقق من معلومات DN الأساسية.

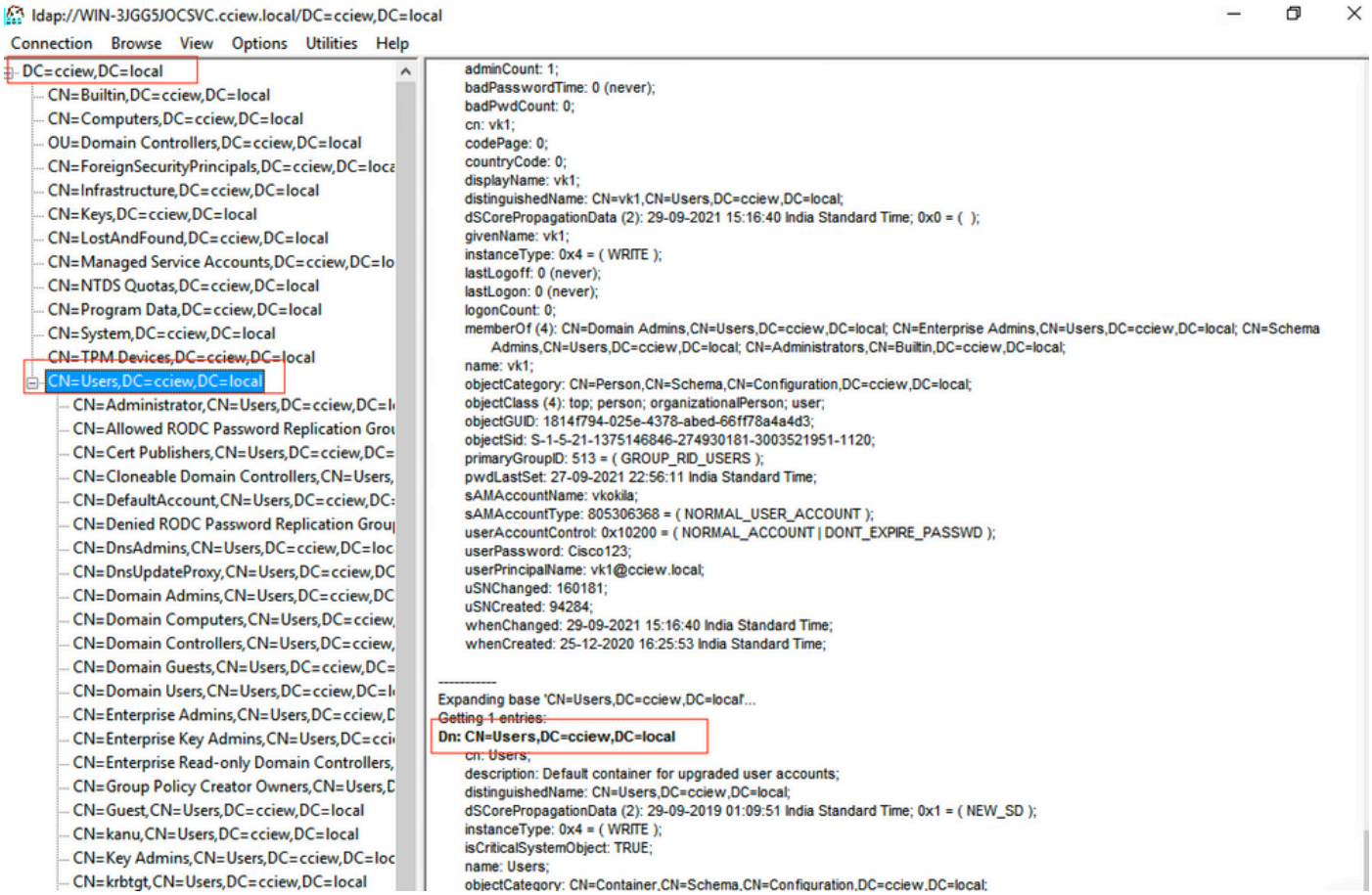

FileZilla Client
Best match
ldp
Run command
ldp

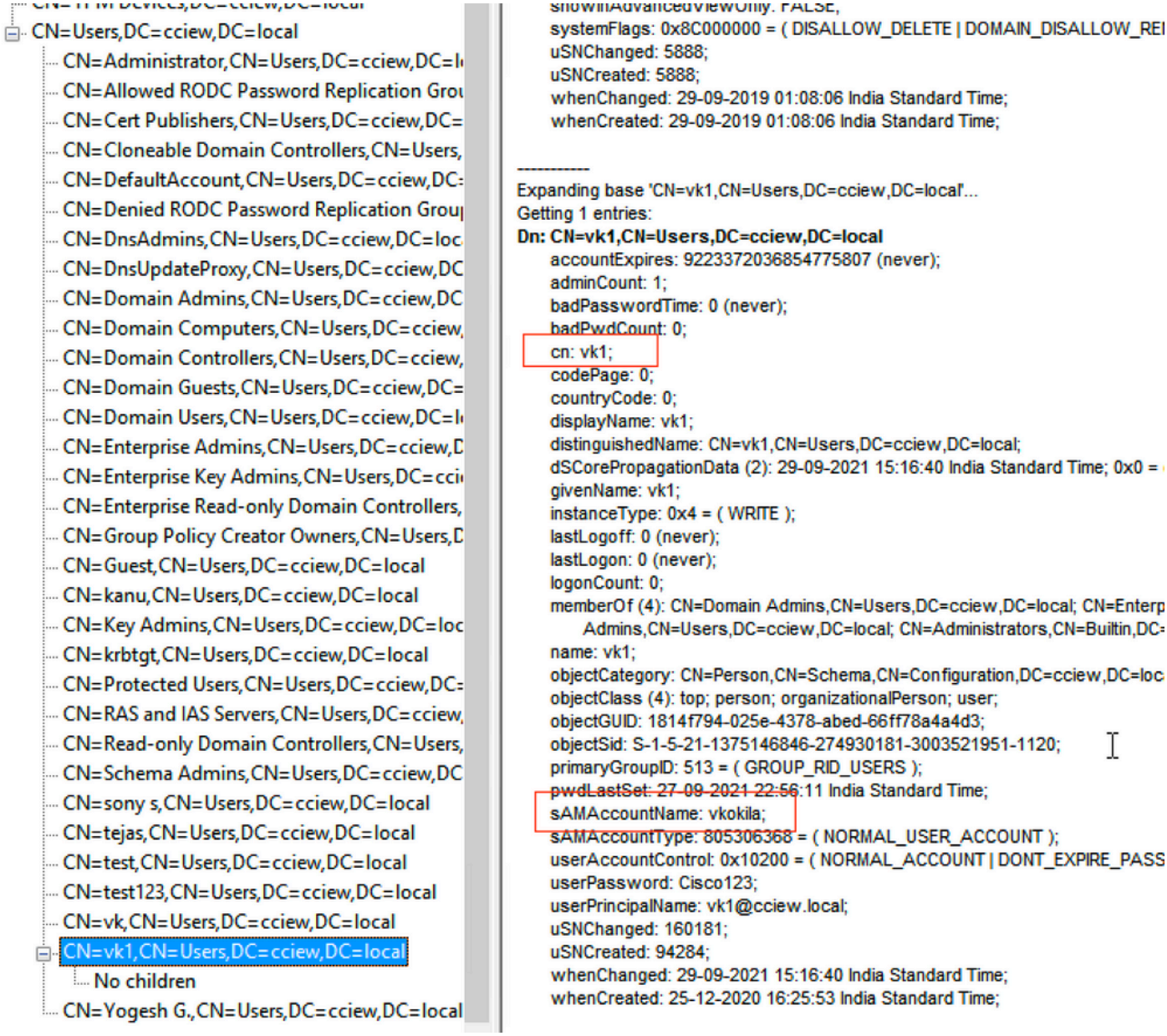

Ldp
Connection
Browse
View
Options
Utilities
Help
Connect...
Bind... Ctrl+B
Disconnect
New Ctrl+N
Save
Save As
Exit


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


ldap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local
Connection
Browse
View
Options
Utilities
Help
Tree
Ctrl+T
Enterprise Configuration
Status Bar
Set Font...
LICY_HINTS_DEPRECATED);
2.840.113556.1.4.2090 = (DIRSYNC_EX);
2.840.113556.1.4.2205 = (UPDATE_STATS
1.2.840.113556.1.4.2204 = (
EE_DELETE_EX); 1.2.840.113556.1.4.2206
(SEARCH_HINTS);
2.840.113556.1.4.2211 = (
EXPECTED_ENTRY_COUNT);
1.2.840.113556.1.4.2239 = (POLICY_HINTS
); 1.2.840.113556.1.4.2255;
1.2.840.113556.1.4.2256;
1.2.840.113556.1.4.2309;
supportedLDAPPolicies (20): MaxPoolThreads;
MaxPercentDirSyncRequests;
MaxDatagramRecv; MaxReceiveBuffer;
InitRecvTimeout; MaxConnections;
MaxConnIdleTime; MaxPageSize;


ldap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local
Connection
Browse
View
Options
Utilities
Help
POLICY_HINTS_DEPRECATED);
1.2.840.113556.1.4.2090 = (DIRSYNC_EX);
1.2.840.113556.1.4.2205 = (UPDATE_STATS
); 1.2.840.113556.1.4.2204 = (
TREE_DELETE_EX); 1.2.840.113556.1.4.2206
= (SEARCH_HINTS);
1.2.840.113556.1.4.2211 = (
EXPECTED_ENTRY_COUNT);
1.2.840.113556.1.4.2239 = (POLICY_HINTS
); 1.2.840.113556.1.4.2255;
1.2.840.113556.1.4.2256;
1.2.840.113556.1.4.2309;
supportedLDAPPolicies (20): MaxPoolThreads;
MaxPercentDirSyncRequests;
SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
Tree View
BaseDN:
DC=cciew,DC=local
Cancel
OK


ldap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local
Connection Browse View Options Utilities Help
DC=cciew,DC=local
CN=Builtin,DC=cciew,DC=local
CN=Computers,DC=cciew,DC=local
OU=Domain Controllers,DC=cciew,DC=local
CN=ForeignSecurityPrincipals,DC=cciew,DC=loca
CN=Infrastructure,DC=cciew,DC=local
CN=Keys,DC=cciew,DC=local
CN=LostAndFound,DC=cciew,DC=local
CN=Managed Service Accounts,DC=cciew,DC=lo
CN=NTDS Quotas,DC=cciew,DC=local
CN=Program Data,DC=cciew,DC=local
CN=System,DC=cciew,DC=local
CN=TPM Devices,DC=cciew,DC=local
CN=Users,DC=cciew,DC=local
CN=Administrator,CN=Users,DC=cciew,DC=l
CN=Allowed RODC Password Replication Grou
CN=Cert Publishers,CN=Users,DC=cciew,DC=
CN=Cloneable Domain Controllers,CN=Users,
CN=DefaultAccount,CN=Users,DC=cciew,DC=
CN=Denied RODC Password Replication Grou
CN=DnsAdmins,CN=Users,DC=cciew,DC=loc
CN=DnsUpdateProxy,CN=Users,DC=cciew,DC
CN=Domain Admins,CN=Users,DC=cciew,DC
CN=Domain Computers,CN=Users,DC=cciew,
CN=Domain Controllers,CN=Users,DC=cciew,
CN=Domain Guests,CN=Users,DC=cciew,DC=
CN=Domain Users,CN=Users,DC=cciew,DC=l
CN=Enterprise Admins,CN=Users,DC=cciew,D
CN=Enterprise Key Admins,CN=Users,DC=cci
CN=Enterprise Read-only Domain Controllers,
CN=Group Policy Creator Owners,CN=Users,D
CN=Guest,CN=Users,DC=cciew,DC=local
CN=kanu,CN=Users,DC=cciew,DC=local
CN=Key Admins,CN=Users,DC=cciew,DC=loc
CN=krbtgt,CN=Users,DC=cciew,DC=local
adminCount: 1;
badPasswordTime: 0 (never);
badPwdCount: 0;
cn: vk1;
codePage: 0;
countryCode: 0;
displayName: vk1;
distinguishedName: CN=vk1,CN=Users,DC=cciew,DC=local;
dSCorePropagationData (2): 29-09-2021 15:16:40 India Standard Time; 0x0 = ( );
givenName: vk1;
instanceType: 0x4 = (WRITE);
lastLogoff: 0 (never);
lastLogon: 0 (never);
logonCount: 0;
memberOf (4): CN=Domain Admins,CN=Users,DC=cciew,DC=local; CN=Enterprise Admins,CN=Users,DC=cciew,DC=local; CN=Schema Admins,CN=Users,DC=cciew,DC=local; CN=Administrators,CN=Builtin,DC=cciew,DC=local;
name: vk1;
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cciew,DC=local;
objectClass (4): top; person; organizationalPerson; user;
objectGUID: 1814f794-025e-4378-abed-66ff78a4a4d3;
objectSid: S-1-5-21-1375146846-274930181-3003521951-1120;
primaryGroupID: 513 = (GROUP_RID_USERS);
pwdLastSet: 27-09-2021 22:56:11 India Standard Time;
sAMAccountName: vkokila;
sAMAccountType: 805306368 = (NORMAL_USER_ACCOUNT);
userAccountControl: 0x10200 = (NORMAL_ACCOUNT | DONT_EXPIRE_PASSWD);
userPassword: Cisco123;
userPrincipalName: vk1@cciew.local;
uSNChanged: 160181;
uSNCreated: 94284;
whenChanged: 29-09-2021 15:16:40 India Standard Time;
whenCreated: 25-12-2020 16:25:53 India Standard Time;
Expanding base 'CN=Users,DC=cciew,DC=local'...
Getting 1 entries:
Dn: CN=Users,DC=cciew,DC=local
cn: Users;
description: Default container for upgraded user accounts;
distinguishedName: CN=Users,DC=cciew,DC=local;
dSCorePropagationData (2): 29-09-2019 01:09:51 India Standard Time; 0x1 = (NEW_SD);
instanceType: 0x4 = (WRITE);
isCriticalSystemObject: TRUE;
name: Users;
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=cciew,DC=local;



4. التحقق من إحصائيات الخادم ومخطط السمات

```
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

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

المراجع

[EAP المحلي على مثال التكوين 9800]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).