

# Catalyst 9800 WLC met LDAP-verificatie voor 802.1X en Web-auth configureren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[LDAP configureren met een Webauth-SSID](#)

[Netwerkdigram](#)

[De controller configureren](#)

[LDAP configureren met een dot1x SSID \(met behulp van Local EAP\)](#)

[LDAP-servergegevens begrijpen](#)

[De velden op de 9800 web UI begrijpen](#)

[LDAP 802.1x-verificatie met het kenmerk AMAccountName.](#)

[WLC-configuratie:](#)

[Controleer via de webinterface:](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Hoe het verificatieproces op de controller te verifiëren](#)

[Hoe de 9800-LDAP-connectiviteit te verifiëren](#)

[Referenties](#)

## Inleiding

Dit document beschrijft hoe u een Catalyst 9800 kunt configureren om clients met een LDAP-server te verifiëren als de database voor gebruikersreferenties.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Microsoft Windows-servers
- Active Directory of een andere LDAP-database

### Gebruikte componenten

C9800 EAC op C9100 access point (AP) dat Cisco IOS®-XE versie 17.3.2a draait

Microsoft Active Directory (AD)-server met QNAP Network Access Storage (NAS) die fungeert als LDAP-database

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## LDAP configureren met een Webauth-SSID

### Netwerkdigram

Dit artikel is gebaseerd op een zeer eenvoudige opzet:

Een EWC AP 9115 met IP 192.168.1.15

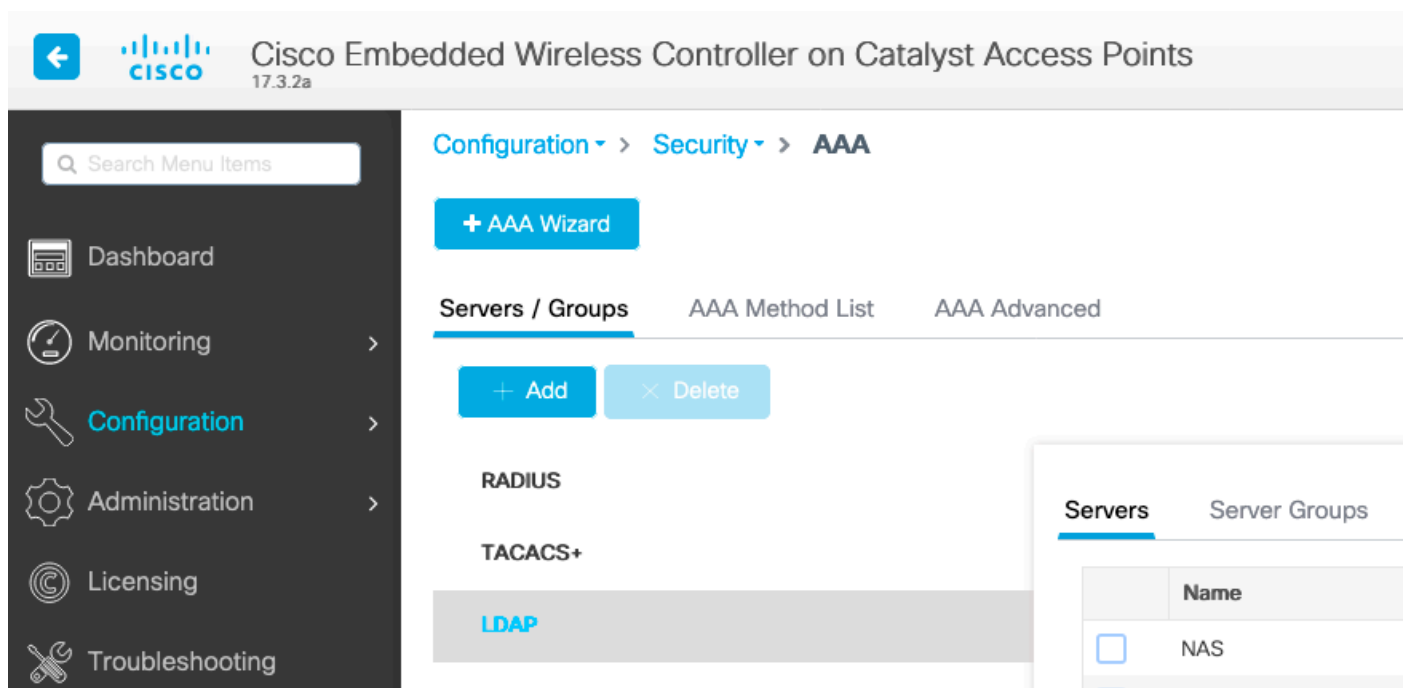
Een Active Directory-server met IP 192.168.1.192

Een client die verbinding maakt met het interne toegangspunt van de EWC

### De controller configureren

#### Stap 1. De LDAP-server configureren

Navigeer naar **Configuration > Security > AAA > servers/groepen > LDAP** en klik op **+ Add**



The screenshot shows the Cisco Embedded Wireless Controller configuration interface. The breadcrumb navigation is **Configuration > Security > AAA**. Under the **AAA** section, there are three tabs: **Servers / Groups**, **AAA Method List**, and **AAA Advanced**. The **Servers / Groups** tab is active, showing a list of servers and groups. The **LDAP** option is highlighted. A modal window is open, showing a table with columns **Servers** and **Server Groups**. The **Servers** column has a checkbox and the **Server Groups** column has the text **NAS**.

Kies een naam voor uw LDAP-server en vul de gegevens in. Voor uitleg over elk veld raadpleegt u de sectie "LDAP-servergegevens begrijpen" van dit document.

Server Name*	<input type="text" value="AD"/>					
Server Address*	<input type="text" value="192.168.1.192"/>	⚠ Provide a valid Server address				
Port Number*	<input type="text" value="389"/>					
Simple Bind	<input type="text" value="Authenticated"/>					
Bind User name*	<input type="text" value="Administrator@lab.cor"/>					
Bind Password *	<input type="text" value="."/>					
Confirm Bind Password*	<input type="text" value="."/>					
User Base DN*	<input type="text" value="CN=Users,DC=lab,DC:"/>					
User Attribute	<input type="text"/>					
User Object Type	<input type="text"/>	+				
	<table border="1"> <thead> <tr> <th>User Object Type</th> <th>Remove</th> </tr> </thead> <tbody> <tr> <td>Person</td> <td>✕</td> </tr> </tbody> </table>	User Object Type	Remove	Person	✕	
User Object Type	Remove					
Person	✕					
Server Timeout (seconds)	<input type="text" value="0-65534"/>					
Secure Mode	<input type="checkbox"/>					
Trustpoint Name	<input type="text"/>					

Opslaan door op **Bijwerken** te klikken en op **apparaat toe te passen**

CLI-opdrachten:

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

**Stap 2.** Een LDAP-servergroep configureren.

Ga naar **Configuratie > Beveiliging > AAA > Servers/groepen > LDAP > Servergroepen** en klik op **+ADD**

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Groups

Name	Server 1	Ser
<input type="checkbox"/> Idapgr	AD	N/A

1 10 items per page

Voer een naam in en voeg de LDAP-server toe die u in de vorige stap hebt geconfigureerd.

Name\*

Idapgr

Group Type

LDAP

Available Servers

Assigned Servers

NAS

>

AD

<

>>

<<

⏪

⏩

⏴

⏵

Klik op **Bijwerken** en klik op **Opslaan**.

CLI-opdrachten:

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

**Stap 3.** AAA-verificatiemethode configureren

Navigeer naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Verificatie** en klik op **+Add**

+ AAA Wizard

Authentication

Authorization

Accounting

+ Add    × Delete

	Name	Type	Group Type	Group1
<input type="checkbox"/>	default	login	local	N/A
<input type="checkbox"/>	ldapauth	login	group	ldapgr

Voer een naam in, kies het **inlogtype** en wijs de eerder ingestelde LDAP-servergroep aan.

### Quick Setup: AAA Authentication

Method List Name\*    ldapauth

Type\*    login ⓘ

Group Type    group ⓘ

Fallback to local   

Available Server Groups    Assigned Server Groups

radius    >    ldapgr    <-

ldap    <       ^

tacacs+    >>       v

   <<       v

CLI-opdrachten:

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

#### Stap 4. Een AAA-autorisatiemethode configureren

Navigeren naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Autorisatie** en klik op **+Add**

+ AAA Wizard

Servers / Groups    **AAA Method List**    AAA Advanced

Authentication

Authorization

Accounting

+ Add
× Delete

	Name	Type	Group Type	Group1
<input type="checkbox"/>	default	credential-download	group	ldapgr
<input type="checkbox"/>	ldapauth	credential-download	group	ldapgr

1 items per page

Maak een credential-download type regel van de naam van uw keus en wijs het aan de eerder gemaakte LDAP servergroep

## Quick Setup: AAA Authorization

Method List Name\*

Type\*  ⓘ

Group Type  ⓘ

Fallback to local

Authenticated

**Available Server Groups**

radius

ldap

tacacs+

>

<

>>

<<

**Assigned Server Groups**

ldapgr

⏪

⏩

⏴

⏵

CLI-opdrachten:

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

### Step 5. Lokale verificatie configureren

Naar **configuratie** navigeren > **Beveiliging** > **AAA** > **Geavanceerd AAA** > **Globale configuratie**

Stel lokale verificatie en lokale autorisatie in op **methodelijst** en kies de verificatie- en autorisatiemethode die eerder is geconfigureerd.

+ AAA Wizard

<b>Global Config</b>	Local Authentication	Method List
RADIUS Fallback	Authentication Method List	ldapauth
Attribute List Name	Local Authorization	Method List
Device Authentication	Authorization Method List	ldapauth
AP Policy	Radius Server Load Balance	<input checked="" type="checkbox"/> DISABLED
Password Policy	Interim Update	<input type="checkbox"/>
AAA Interface	<a href="#">Show Advanced Settings &gt;&gt;&gt;</a>	

CLI-opdrachten:

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

**Stap 6.** Configureer de webauth parameter-map

Navigeer naar **Configuration > Security > Web Auth** en bewerk de **globale** kaart

Configuration > Security > **Web Auth**

+ Add   × Delete

	Parameter Map Name
<input type="checkbox"/>	global

◀ ◁ 1 ▷ ▶ 10 items per page

Zorg ervoor dat u een virtueel IPv4-adres configureert zoals 192.0.2.1 (dat specifieke IP/subnettoegang is gereserveerd voor niet-routeerbare virtuele IP).

## Edit Web Auth Parameter

General

Advanced

Parameter-map name	<input type="text" value="global"/>
Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Banner Title <input type="radio"/> File Name
Maximum HTTP connections	<input type="text" value="100"/>
Init-State Timeout(secs)	<input type="text" value="120"/>
Type	<input type="text" value="webauth"/>
Virtual IPv4 Address	<input type="text" value="192.0.2.1"/>
Trustpoint	<input type="text" value="--- Select ---"/>
Virtual IPv4 Hostname	<input type="text"/>
Virtual IPv6 Address	<input type="text" value=":::"/>
Web Auth intercept HTTPs	<input type="checkbox"/>
Watch List Enable	<input type="checkbox"/>
Watch List Expiry Timeout(secs)	<input type="text" value="600"/>
Captive Bypass Portal	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>
Sleeping Client Status	<input type="checkbox"/>
Sleeping Client Timeout (minutes)	<input type="text" value="720"/>

Klik op **Toepassen** om op te slaan.

CLI-opdrachten:

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

**Stap 7.** Een webauth configureren WLAN



Navigeer naar **Configuration > WLAN's** en klik op **+Add**

### Edit WLAN

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

**General** Security Add To Policy Tags

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

Profile Name*	<input type="text" value="webauth"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="webauth"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="2"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Configureer de naam, zorg ervoor dat deze in de ingeschakelde staat staat staat staat en ga vervolgens naar het tabblad **Beveiliging**.

Zorg er in **Layer 2**-subtabblad voor dat er geen beveiliging is en dat Fast Transition is uitgeschakeld.

### Edit WLAN

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

General **Security** Add To Policy Tags

**Layer2** Layer3 AAA

Layer 2 Security Mode	<input type="text" value="None"/>	Lobby Admin Access	<input type="checkbox"/>
MAC Filtering	<input type="checkbox"/>	Fast Transition	<input type="text" value="Disabled"/>
OWE Transition Mode	<input type="checkbox"/>	Over the DS	<input type="checkbox"/>
		Reassociation Timeout	<input type="text" value="20"/>

In het tabblad **Layer 3**, **webbeleid** inschakelen, de parameterkaart instellen op **globaal** en de verificatielijst instellen op de eerder ingestelde aaa-inlogmethode.

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

General **Security** Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy



[Show Advanced Settings >>>](#)

Web Auth Parameter Map

global



Authentication List

ldapauth



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

Opslaan door op **Toepassen** te klikken

CLI-opdrachten:

```
wlan webauth 2 webauth no security ft adaptive no security wpa no security wpa wpa2 no security
wpa wpa2 ciphers aes no security wpa akmdot1x security web-auth security web-auth
authentication-list ldapauth security web-auth parameter-map global no shutdown
```

**Stap 8.** Controleer of de SSID wordt uitgezonden

Navigeer naar **Configuration > Tags** en zorg ervoor dat de SSID is opgenomen in het beleidsprofiel dat momenteel wordt gebruikt door de SSID (de standaard-beleidstag voor een nieuwe configuratie als u nog geen tags hebt geconfigureerd). Standaard worden nieuwe SSID's die u maakt niet uitgezonden door de standaard-policy-tag totdat u ze handmatig opneemt.

Dit artikel behandelt niet de configuratie van beleidsprofielen en veronderstelt u met dat deel van de configuratie vertrouwd bent.

## LDAP configureren met een dot1x SSID (met behulp van Local EAP)

Voor het configureren van LDAP voor een 802.1X SSID op de 9800 is doorgaans ook het configureren van Local EAP vereist. Als u RADIUS zou gebruiken, dan zou het uw RADIUS-server zijn om een verbinding te maken met de LDAP-database en dat is buiten het bereik van dit artikel. Alvorens deze configuratie te proberen, is het raadzaam om Local EAP te configureren met een lokale gebruiker die eerst op de WLC is geconfigureerd, een configuratievoorbeeld wordt gegeven in de sectie referenties aan het eind van dit artikel. Als u klaar bent, kunt u proberen de gebruikersdatabase naar LDAP te verplaatsen.

**Stap 1.** Een lokaal EAP-profiel configureren

Navigeer naar **Configuratie > Lokale EAP** en klik op **+Add**

The screenshot shows the Cisco Embedded Wireless Controller interface. The top navigation bar includes the Cisco logo and the text "Cisco Embedded Wireless Controller on Catalyst Access Points 17.3.2a". The main navigation menu on the left lists: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area is titled "Configuration > Security > Local EAP". Below this, there are two tabs: "Local EAP Profiles" (active) and "EAP-FAST Parameters". There are two buttons: "+ Add" and "× Delete". A table with one row is visible, with a checkbox in the first column and "PEAP" in the second column. Below the table is a pagination control showing "1" of "10 items per page".

Kies een naam voor uw profiel. Schakel ten minste PEAP in en kies een Trustpoint Name. Standaard heeft uw WLC alleen zelf-ondertekende certificaten, dus het maakt niet echt uit welke u kiest (meestal TP-self-signed-xxxx is de beste voor dit doel), maar als nieuwe smartphones OS versies vertrouwen minder en minder zelf-ondertekende certificaten, overwegen het installeren van een betrouwbaar publiek ondertekend certificaat.

## Edit Local EAP Profiles

Profile Name*	PEAP
LEAP	<input type="checkbox"/>
EAP-FAST	<input type="checkbox"/>
EAP-TLS	<input type="checkbox"/>
PEAP	<input checked="" type="checkbox"/>
Trustpoint Name	TP-self-signed-3059 ▼

CLI-opdrachten:

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

## Stap 2. De LDAP-server configureren

Navigeer naar **Configuration > Security > AAA > servers/groepen > LDAP** en klik op **+ Add**

The screenshot shows the Cisco Embedded Wireless Controller configuration interface. The breadcrumb navigation is **Configuration > Security > AAA**. The main content area is titled **Servers / Groups** and includes a **+ AAA Wizard** button. Below this, there are three tabs: **Servers / Groups** (selected), **AAA Method List**, and **AAA Advanced**. There are **+ Add** and **× Delete** buttons. The **Servers** tab is active, showing a list of servers with columns for **Name** and a checkbox. The **LDAP** server is highlighted in the list, and a modal window is open for its configuration, showing a table with the following data:

Servers	
	Name
<input type="checkbox"/>	NAS
<input type="checkbox"/>	

Kies een naam voor uw LDAP-server en vul de gegevens in. Voor uitleg over elk veld raadpleegt u de sectie "LDAP-servergegevens begrijpen" van dit document.

Server Name*	<input type="text" value="AD"/>					
Server Address*	<input type="text" value="192.168.1.192"/>	⚠ Provide a valid Server address				
Port Number*	<input type="text" value="389"/>					
Simple Bind	<input type="text" value="Authenticated"/>	▼				
Bind User name*	<input type="text" value="Administrator@lab.cor"/>					
Bind Password *	<input type="text" value="."/>					
Confirm Bind Password*	<input type="text" value="."/>					
User Base DN*	<input type="text" value="CN=Users,DC=lab,DC:"/>					
User Attribute	<input type="text"/>	▼				
User Object Type	<input type="text"/>	+				
	<table border="1"> <thead> <tr> <th>User Object Type</th> <th>Remove</th> </tr> </thead> <tbody> <tr> <td>Person</td> <td>✕</td> </tr> </tbody> </table>		User Object Type	Remove	Person	✕
User Object Type	Remove					
Person	✕					
Server Timeout (seconds)	<input type="text" value="0-65534"/>					
Secure Mode	<input type="checkbox"/>					
Trustpoint Name	<input type="text"/>	▼				

Opslaan door op **Bijwerken** te klikken en op apparaat toe te passen

```
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
```

**Stap 3.** Een LDAP-servergroep configureren.

Ga naar **Configuratie > Beveiliging > AAA > Servers/groepen > LDAP > Servergroepen** en klik op **+ADD**

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers **Server Groups**

Name	Server 1	Ser
<input type="checkbox"/> Idapgr	AD	N/A

1 10 items per page

Voer een naam in en voeg de LDAP-server toe die u in de vorige stap hebt geconfigureerd.

Name\*

Idapgr

Group Type

LDAP

Available Servers

Assigned Servers

NAS

AD

>

<

>>

<<

⌵

⌶

⌷

⌸

Klik op **Bijwerken** en klik op **Opslaan**.

CLI-opdrachten:

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

#### Stap 4. Een AAA-verificatiemethode configureren

Navigeer naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Verificatie** en klik op **+Add**

Configureer een **dot1x**-verificatiemethode en wijs deze alleen op lokaal. Het zou verleidelijk zijn om naar de LDAP servergroep te wijzen, maar het is de WLC zelf die fungeert als de 802.1X authenticator hier (hoewel de gebruikersdatabase zich op LDAP bevindt, maar dat is de

autorisatiemethode taak).

## Quick Setup: AAA Authentication

Method List Name\*

ldapauth

Type\*

dot1x



Group Type

local



Available Server Groups

radius  
ldap  
tacacs+  
ldapgr



Assigned Server Groups



CLI-opdracht:

```
aaa authentication dot1x ldapauth local
```

**Stap 5.** Een AAA-autorisatiemethode configureren

Navigeer naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Autorisatie** en klik op **+Add**

Maak een **credential-download** type autorisatiemethode en maak het punt naar de LDAP groep.

## Quick Setup: AAA Authorization

Method List Name\*

ldapauth

Type\*

credential-download ▾



Group Type

group ▾



Fallback to local

Authenticated

Available Server Groups

radius  
ldap  
tacacs+

Assigned Server Groups

ldapgr



CLI-opdracht :

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

### Stap 6. Lokale verificatiedetails configureren

Navigeren naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > AAA geavanceerde**

Kies een **methodelijst** voor zowel de verificatie als de autorisatie en kies de verificatiemethode dot1x die lokaal wijst en de aanmeldingsmethode credential-download die naar LDAP wijst



Configuration > Security > AAA

+ AAA Wizard

Servers / Groups    AAA Method List    **AAA Advanced**

**Global Config**

- RADIUS Fallback
- Attribute List Name
- Device Authentication
- AP Policy
- Password Policy
- AAA Interface

Local Authentication: Method List

Authentication Method List: Idapauth

Local Authorization: Method List

Authorization Method List: Idapauth

Radius Server Load Balance:  DISABLED

Interim Update:

[Show Advanced Settings >>>](#)

CLI-opdracht :

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

### Stap 7. Een dot1x WLAN configureren

Navigeer naar **Configuration > WLAN** en klik op **+Add**

Kies een profiel en een SSID-naam en controleer of dit is ingeschakeld.

**Edit WLAN**

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

**General**    Security    Add To Policy Tags

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

Profile Name\*    LDAP    Radio Policy    All

SSID\*    LDAP    Broadcast SSID    **ENABLED**

WLAN ID\*    1

Status    **ENABLED**

Naar het tabblad **Beveiliging Layer 2** gaan.

Kies WPA+WPA2 als **Layer 2-beveiligingsmodus**

Zorg ervoor dat WPA2 en AES zijn ingeschakeld in de **WPA-parameters** en schakel **802.1X** in

## Edit WLAN

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

General **Security** Add To Policy Tags

**Layer2** Layer3 AAA

Layer 2 Security Mode

MAC Filtering

### Protected Management Frame

PMF

### WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption  AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt  802.1x

PSK

CCKM

FT + 802.1x

FT + PSK

802.1x-SHA256

PSK-SHA256

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

### MPSK Configuration

MPSK

Naar het tabblad **AAA** gaan.

Selecteer de eerder gemaakte dot1x-verificatiemethode, schakel lokale EAP-verificatie in en kies het EAP-profiel dat in de eerste stap is geconfigureerd.

## Edit WLAN

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

General **Security** Add To Policy Tags

Layer2 Layer3 **AAA**

Authentication List

ldapauth ▼ ⓘ

Local EAP Authentication



EAP Profile Name

PEAP ▼

Opslaan door op Toepassen te klikken

CLI-opdrachten:

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

### Stap 8. Controleer dat het WLAN wordt uitgezonden

Navigeer naar **Configuration > Tags** en zorg ervoor dat de SSID is opgenomen in het beleidsprofiel dat momenteel wordt gebruikt door de SSID (de standaard-beleidstag voor een nieuwe configuratie als u nog geen tags hebt geconfigureerd). Standaard worden nieuwe SSID's die u maakt niet uitgezonden door de standaard-policy-tag totdat u ze handmatig opneemt.

Dit artikel behandelt niet de configuratie van beleidsprofielen en veronderstelt u met dat deel van de configuratie vertrouwd bent.

Als u Active Directory gebruikt, moet u de AD-server configureren om het kenmerk "userPassword" te verzenden. Deze eigenschap moet naar de WLC worden gezonden. Dit komt doordat de WLC de verificatie doet, niet de AD-server. Je kunt ook problemen hebben met het authenticeren met de PEAP-mschapv2 methode, omdat het wachtwoord nooit wordt verzonden in duidelijke tekst en daarom niet kan worden gecontroleerd met de LDAP database, alleen de PEAP-GTC methode zou werken met bepaalde LDAP databases.

## LDAP-servergegevens begrijpen

### De velden op de 9800 web UI begrijpen

Hier is een voorbeeld van een zeer fundamentele Active Directory die fungeert als LDAP server

## Edit AAA LDAP Server



Server Name*	<input type="text" value="AD"/>					
Server Address*	<input type="text" value="192.168.1.192"/>	Provide a valid Server address				
Port Number*	<input type="text" value="389"/>					
Simple Bind	<input type="text" value="Authenticated"/>					
Bind User name*	<input type="text" value="Administrator@lab.cor"/>					
Bind Password *	<input type="password" value="."/>					
Confirm Bind Password*	<input type="password" value="."/>					
User Base DN*	<input type="text" value="CN=Users,DC=lab,DC:"/>					
User Attribute	<input type="text"/>					
User Object Type	<input type="text"/>					
	<table border="1"> <thead> <tr> <th>User Object Type</th> <th>Remove</th> </tr> </thead> <tbody> <tr> <td>Person</td> <td></td> </tr> </tbody> </table>	User Object Type	Remove	Person		
User Object Type	Remove					
Person						
Server Timeout (seconds)	<input type="text" value="0-65534"/>					
Secure Mode	<input type="checkbox"/>					
Trustpoint Name	<input type="text"/>					

Naam en IP zijn hopelijk vanzelfsprekend.

Port: 389 is de standaardpoort voor LDAP, maar uw server kan een andere poort gebruiken.

Eenvoudige binding: het is zeer zeldzaam om een LDAP-databank vandaag de dag te hebben die niet-geverifieerde bind ondersteunt (dit betekent dat iedereen een LDAP-zoekopdracht kan uitvoeren op deze databank zonder enige authenticatieformulier). Geverifieerde eenvoudige bind is het meest gebruikelijke type van verificatie en wat Active Directory standaard toestaat. U kunt een naam en wachtwoord voor een beheerdersaccount invoeren om vanaf daar te kunnen zoeken in de gebruikersdatabank.

Bind Gebruikersnaam : U moet verwijzen naar een gebruikersnaam met beheerdersrechten in Active Directory. AD accepteert het "user@domain" formaat voor het terwijl veel andere LDAP databases een "CN=xxx, DC=xxx" formaat verwachten voor de gebruikersnaam. Een voorbeeld met een andere LDAP-database dan AD wordt later in dit artikel gegeven.

Bind wachtwoord: Voer het wachtwoord in dat de eerder ingevoerde beheerdersnaam bevat.

Gebruikersbasis-DN: Voer hier de "zoekwortel" in, dat is de locatie in uw LDAP-boom waar zoekopdrachten beginnen. In dit voorbeeld vallen al onze toepassingen onder de groep "Gebruikers", waarvan het DN "CN=Gebruikers, DC=lab, DC=com" is (aangezien het voorbeeld LDAP-domein lab.com is). Een voorbeeld van hoe u dit gebruikersbestand DN kunt vinden, vindt u later in deze sectie.

Gebruikerskenmerk : Dit kan leeg worden gelaten, of wijzen naar een LDAP attribuut-map die aangeeft welke LDAP-veld telt als gebruikersnaam voor uw LDAP-database. Vanwege Cisco-bug-id [CSCv11813](#) De WLC probeert echter een authenticatie met het veld CN.

Objecttype gebruiker : Dit bepaalt het type objecten dat als gebruikers wordt beschouwd. Meestal is dit "Persoon". Het zou "Computers" kunnen zijn als je een AD-database hebt en computeraccounts autoriseert, maar ook daar zorgt LDAP voor veel aanpassingen.

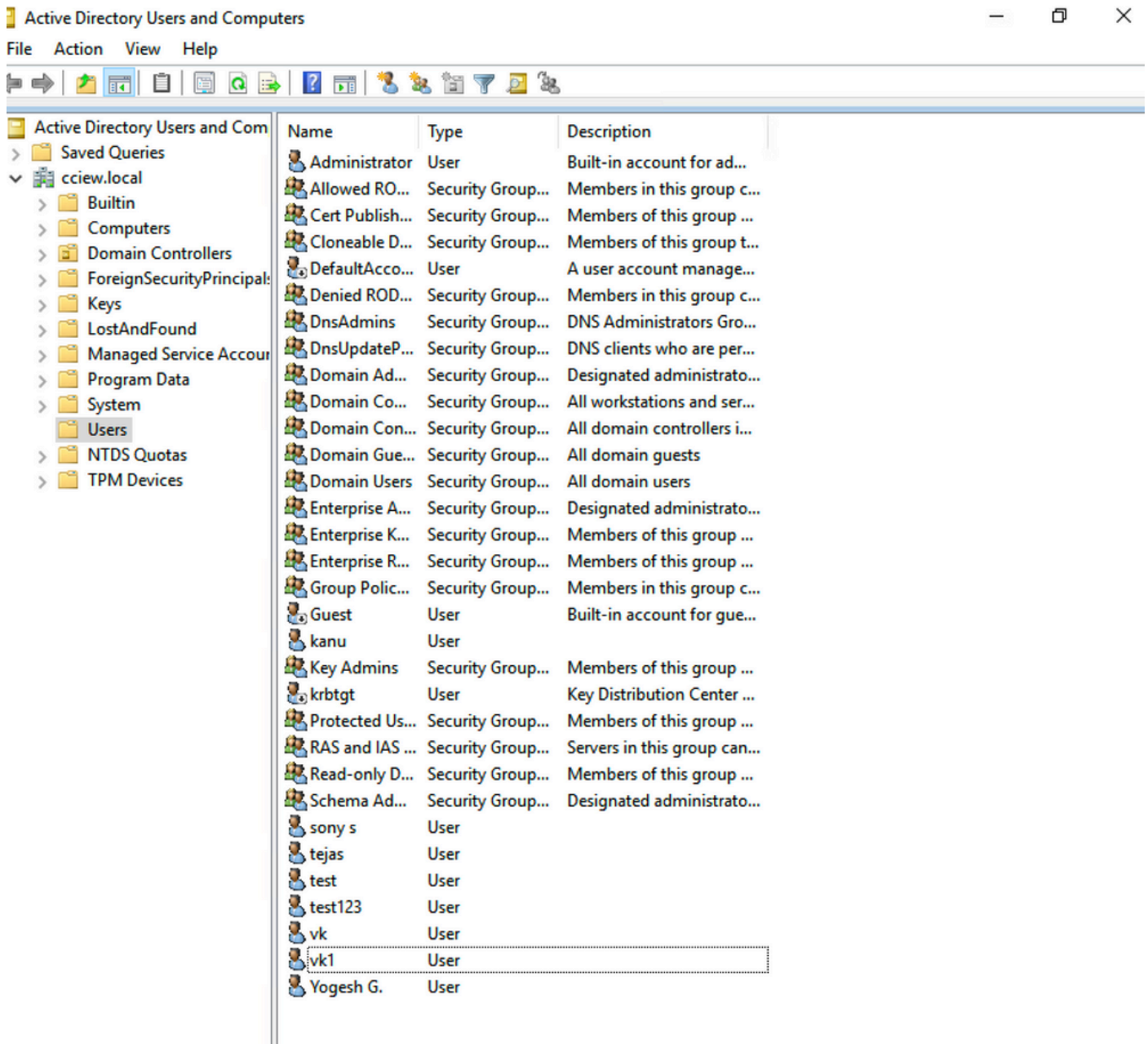
Secure Mode maakt Secure LDAP via TLS mogelijk en vereist dat u op de 9800 een Trustpoint selecteert om een certificaat te gebruiken voor de TLS-codering.

## **LDAP 802.1x-verificatie met het kenmerk AMAaccountName.**

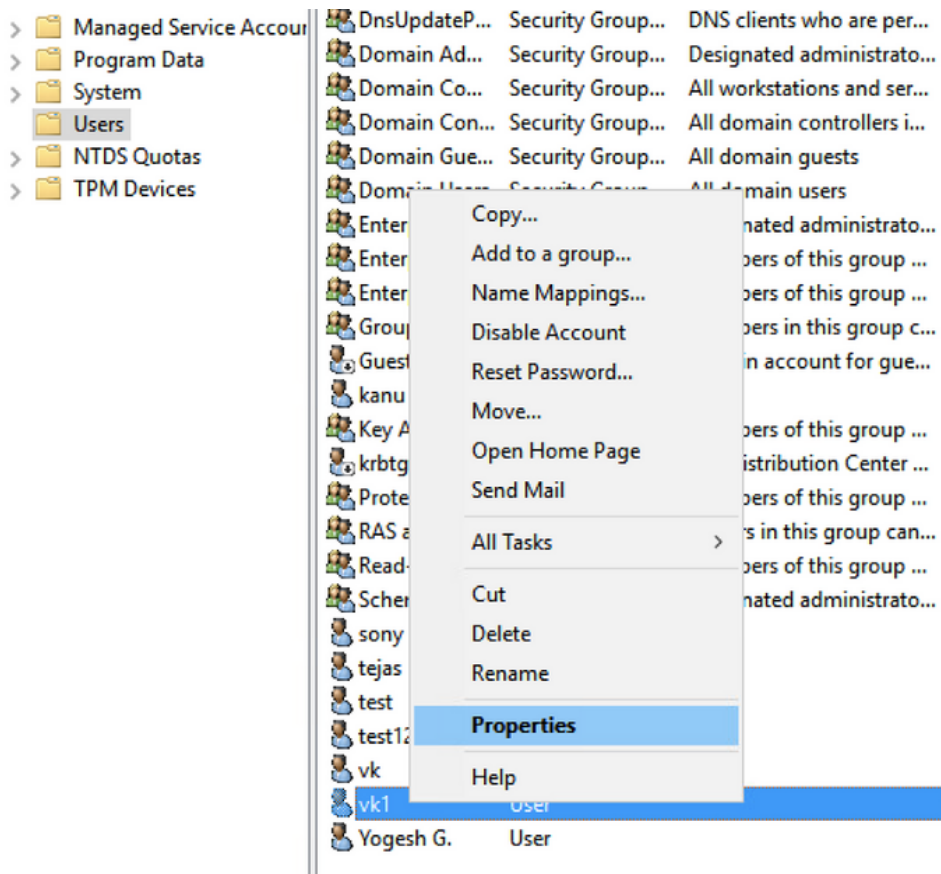
Deze verbetering is geïntroduceerd in versie 17.6.1.

**Configureer het "userPassword"-kenmerk voor de gebruiker.**

Stap 1. Ga op de Windows-server naar Active Directory-gebruikers en -computers



Stap 2. Klik met de rechtermuisknop op de respectievelijke gebruikersnaam en selecteer eigenschappen



Stap 3. Selecteer de eigenschappeneditor in het eigenschappenvenster

Published Certificates	Member Of	Password Replication	Dial-in	Object	
Security	Environment	Sessions	Remote control		
General	Address	Account	Profile	Telephones	Organization
Remote Desktop Services Profile			COM+	Attribute Editor	

## Attributes:

Attribute	Value
uid	<not set>
uidNumber	<not set>
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x10200 = ( NORMAL_ACCOUNT   DONT_I
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>
userPKCS12	<not set>
userPrincipalName	vk1@cciew.local
userSharedFolder	<not set>

Edit

Filter

OK

Cancel

Apply

Help

Stap 4. Configureer het kenmerk "userPassword". Dit is het wachtwoord voor de gebruiker, die in



Hex-waarde moet worden geconfigureerd.

vk1 Properties



Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
General	Address	Account	Profile	Telephones

Multi-valued Octet String Editor

Attribute: userPassword

Values:

[Empty list box for values]

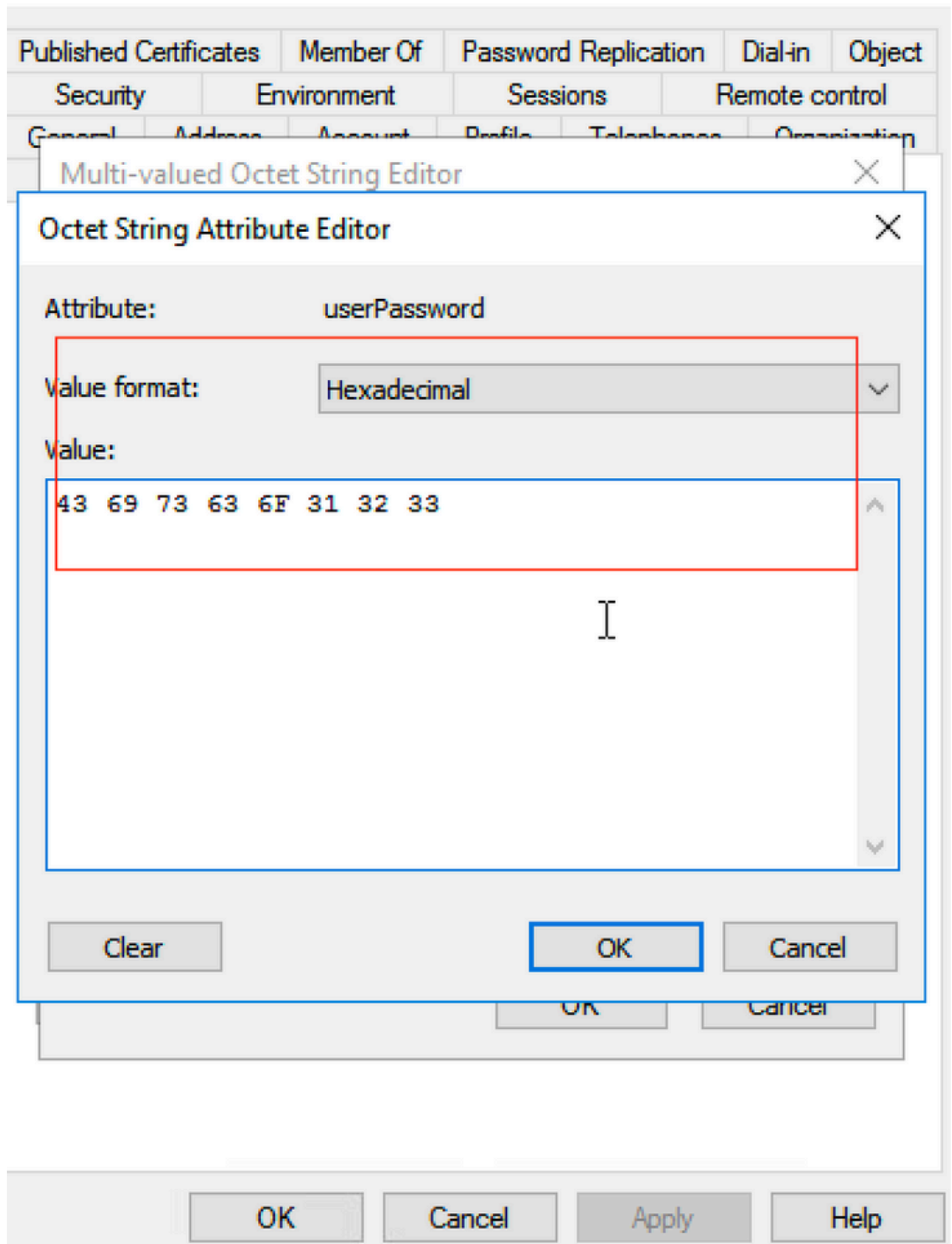
Add

Remove

Edit

OK

Cancel



Klik op OK, controleer of het juiste wachtwoord wordt weergegeven

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 X

Attribute: userPassword

Values:

Cisco123

Add

Remove

Edit

OK

Cancel

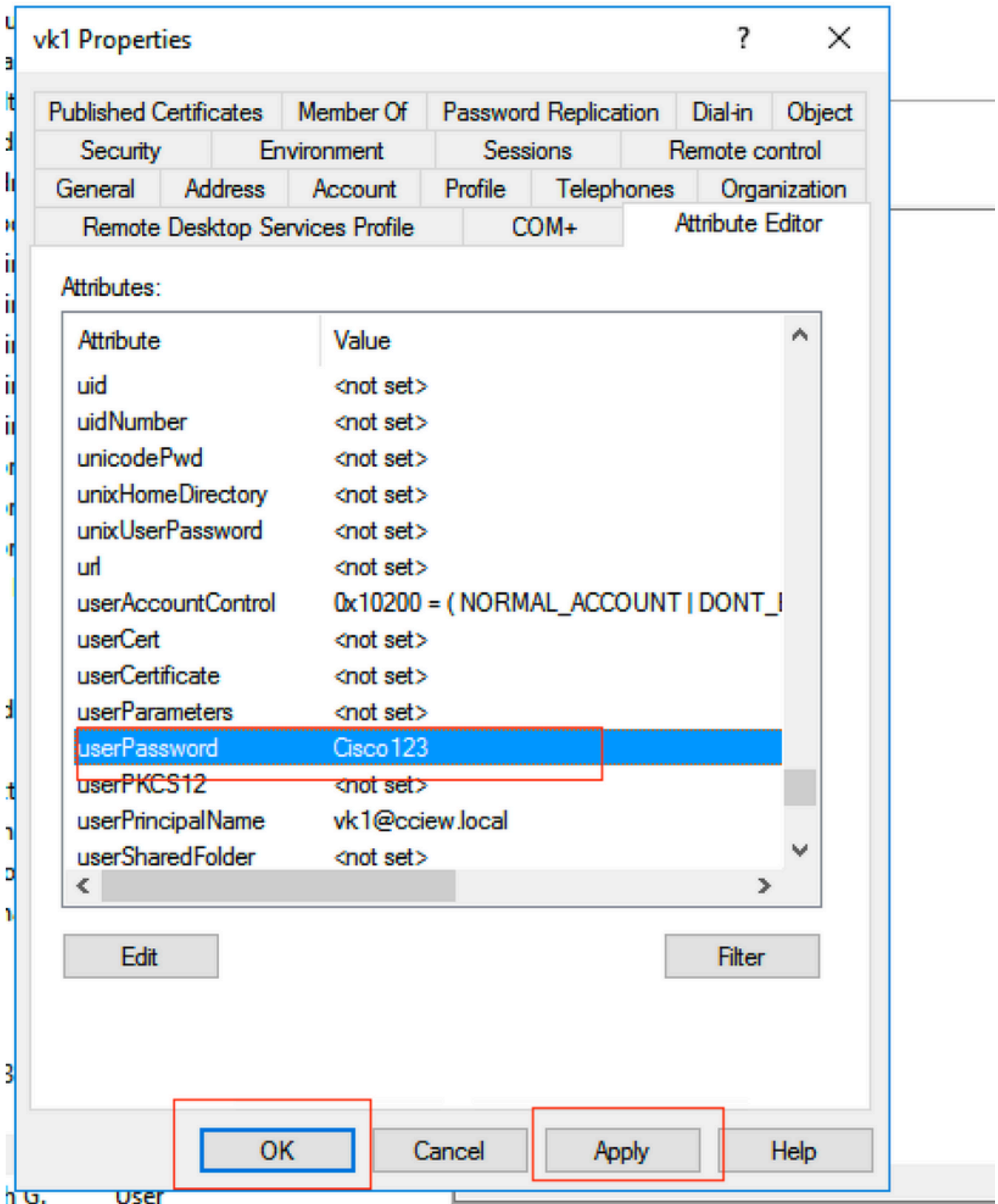
OK

Cancel

Apply

Help

Stap 5. Klik op Toepassen en vervolgens op OK



Stap 6. Controleer de "sMAAccountName" attribuut waarde voor de gebruiker en het zou de gebruikersnaam voor verificatie.

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

G. User

WLC-configuratie:

Stap 1. Maak LDAP attribuut MAP

Stap 2. Het kenmerk "AccountName" configureren en als "gebruikersnaam" typen

Stap 3. Kies de gemaakte attribuut MAP onder de LDAP-serverconfiguratie.

```
ldap attribute-map VK
```

```
map type sAMAccountName username
```

```
ldap server ldap
```

```
ipv4 10.106.38.195
```

```
attribute map VK
```

```
bind authenticate root-dn vkl password 7 00271A1507545A545C
```

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

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

## Controleer via de webinterface:

The screenshot shows the Cisco Catalyst 9800-40 Wireless Controller web interface. The breadcrumb navigation is Configuration > Security > AAA. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Servers / Groups' and includes a '+ AAA Wizard' button. Below this, there are tabs for 'Servers / Groups', 'AAA Method List', and 'AAA Advanced'. A '+ Add' button and a 'Delete' button are visible. A sidebar on the left lists 'RADIUS', 'TACACS+', and 'LDAP'. The 'LDAP' section is expanded, showing a table of servers. The table has columns for Name, Server Address, Port Number, and Simple Bind. One server is listed with Name 'ldap', Server Address '10.106.38.195', Port Number '389', and Simple Bind 'Authenticated'. The table is paginated to show 10 items per page, and the current page is 1 of 1.

Name	Server Address	Port Number	Simple Bind
ldap	10.106.38.195	389	Authenticated

Last login NA ...

Edit AAA LDAP Server ✕

Server Name\*

Server Address\*

Port Number\*

Simple Bind

Bind User name\*

Bind Password \*

Confirm Bind Password\*

User Base DN\*

User Attribute

User Object Type

User Object Type	Remove
Person	✕

Server Timeout (seconds)

## Verifiëren

Om uw configuratie te verifiëren, controleer de CLI-opdrachten met de opdrachten uit dit artikel.

LDAP-databases bieden doorgaans geen verificatielogboeken, zodat het moeilijk is om te weten wat er gebeurt. Ga naar de sectie Probleemoplossing van dit artikel om te zien hoe u sporen kunt nemen en hoe u kunt snuiven vastleggen om te zien of er een verbinding is met de LDAP-database of niet.

## Problemen oplossen

Om dit op te lossen, is het best om dit in twee delen te splitsen. Het eerste deel is het valideren van het lokale EAP-gedeelte. De tweede is controleren dat de 9800 goed communiceert met de LDAP-server.

### Hoe het verificatieproces op de controller te verifiëren

U kunt een radioactief spoor verzamelen om de "debugs" van de clientverbinding te krijgen.

Ga simpelweg naar **Problemen oplossen > Radioactive Trace**. Voeg het client-MAC-adres toe (let op dat uw client een willekeurige MAC kan gebruiken en niet zijn eigen MAC, u kunt dit verifiëren in het SSID-profiel op het client-apparaat zelf) en start.

Nadat u de verbindingsooging hebt gereproduceerd, kunt u op "Generate" klikken en de logbestanden van de laatste X minuten verkrijgen. Zorg ervoor dat u op **intern** klikt omdat bepaalde LDAP-logregels niet verschijnen als u dit niet kunt doen.

Hier is een voorbeeld van radiocatief spoor van een cliënt die met succes op een Web authenticatie SSID voor authentiek verklaart. Sommige redundante onderdelen zijn voor de duidelijkheid verwijderd:

```
2021/01/19 21:57:55.890953 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (note): MAC:
2elf.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: 2elf.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: 2elf.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: 2elf.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:
2elf.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: 2elf.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: 2elf.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: 2elf.3a65.9c09 Association success. AID 2, Roaming = False, WGB = False, llr =
False, llw = False 2021/01/19 21:57:55.892497 {wncd_x_R0-0}{1}: [dot11] [9347]: (info): MAC:
2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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): [2elf.3a65.9c09:capwap_900000004] 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):
[2elf.3a65.9c09:capwap_900000004] 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):
[2elf.3a65.9c09:capwap_900000004] - authc_list: ldapauth 2021/01/19 21:57:55.893211 {wncd_x_R0-
0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [2elf.3a65.9c09:capwap_900000004] - authz_list:
Not present under wlan configuration 2021/01/19 21:57:55.893254 {wncd_x_R0-0}{1}: [client-auth]
[9347]: (info): MAC: 2elf.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): [2elf.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):
[2elf.3a65.9c09:capwap_900000004] 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):
[2elf.3a65.9c09:capwap_900000004] 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):
[2elf.3a65.9c09:capwap_900000004] 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):
[2elf.3a65.9c09:capwap_900000004] Retrieved Client IIF ID 0xd3001364 2021/01/19 21:57:55.893731
{wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2elf.3a65.9c09:capwap_900000004] Allocated audit
session id 000000000000009C1CA610D7 2021/01/19 21:57:55.894285 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2elf.3a65.9c09:capwap_900000004] Device type found in cache Samsung Galaxy S10e
2021/01/19 21:57:55.894299 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info):
[2elf.3a65.9c09:capwap_900000004] 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):
[2elf.3a65.9c09:capwap_900000004] 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):
[2elf.3a65.9c09:capwap_900000004] 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_900000004]
access_session_acct_filter_spec is NULL 2021/01/19 21:57:55.894827 {wncd_x_R0-0}{1}: [auth-mgr]
```



[9347]: (info): [2elf.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): [2elf.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): [2elf.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[2elf.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[2elf.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: 2elf.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 2elf.3a65.9c09 2021/01/19 21:57:55.903592 {wncd\_x\_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2elf.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: 2elf.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): [2elf.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): [2elf.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): [2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.3a65.9c09 Received mobile\_announce, sub type: 0 of XID (0) from (WNCID[0]) 2021/01/19 21:57:55.904955 {wncd\_x\_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2elf.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 (WNCID[0]) 2021/01/19 21:57:55.905157 {wncd\_x\_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2elf.3a65.9c09 Received mobile\_announce\_nak, sub type: 1 of XID (0) from (WNCID[0]) 2021/01/19 21:57:55.905267 {wncd\_x\_R0-0}{1}: [mm-transition] [9347]: (info): MAC: 2elf.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: 2elf.3a65.9c09 Roam type changed - None -> None 2021/01/19 21:57:55.905317 {wncd\_x\_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2elf.3a65.9c09 Mobility role changed - Unassoc -> Local 2021/01/19 21:57:55.905515 {wncd\_x\_R0-0}{1}: [mm-client] [9347]: (note): MAC: 2elf.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: 2elf.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: 2elf.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:

2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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 2elf.3a65.9c09 2021/01/19 21:57:55.907701 {wncd\_x\_R0-0}{1}: [dpath\_svc] [9347]: (note): MAC: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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): [2elf.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: 2elf.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): [2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.3a65.9c09 L3 Authentication initiated. LWA 2021/01/19 21:57:55.967433 {wncd\_x\_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2elf.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: 2elf.3a65.9c09 Dest MAC: ffff.ffff.ffff ARP REQUEST, ARP sender MAC: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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[2elf.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[2elf.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[2elf.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[2elf.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): [2elf.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): [2elf.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): [2elf.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): [2elf.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): [2elf.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[2elf.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[2elf.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[2elf.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[2elf.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[2elf.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[2elf.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[2elf.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[2elf.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[2elf.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[2elf.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[2elf.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[2elf.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): [2elf.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): [2elf.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):  
[2elf.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): [2elf.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): [2elf.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[2elf.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[2elf.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[2elf.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[2elf.3a65.9c09][ 192.168.1.17]Retrieved user-agent = Mozilla/5.0

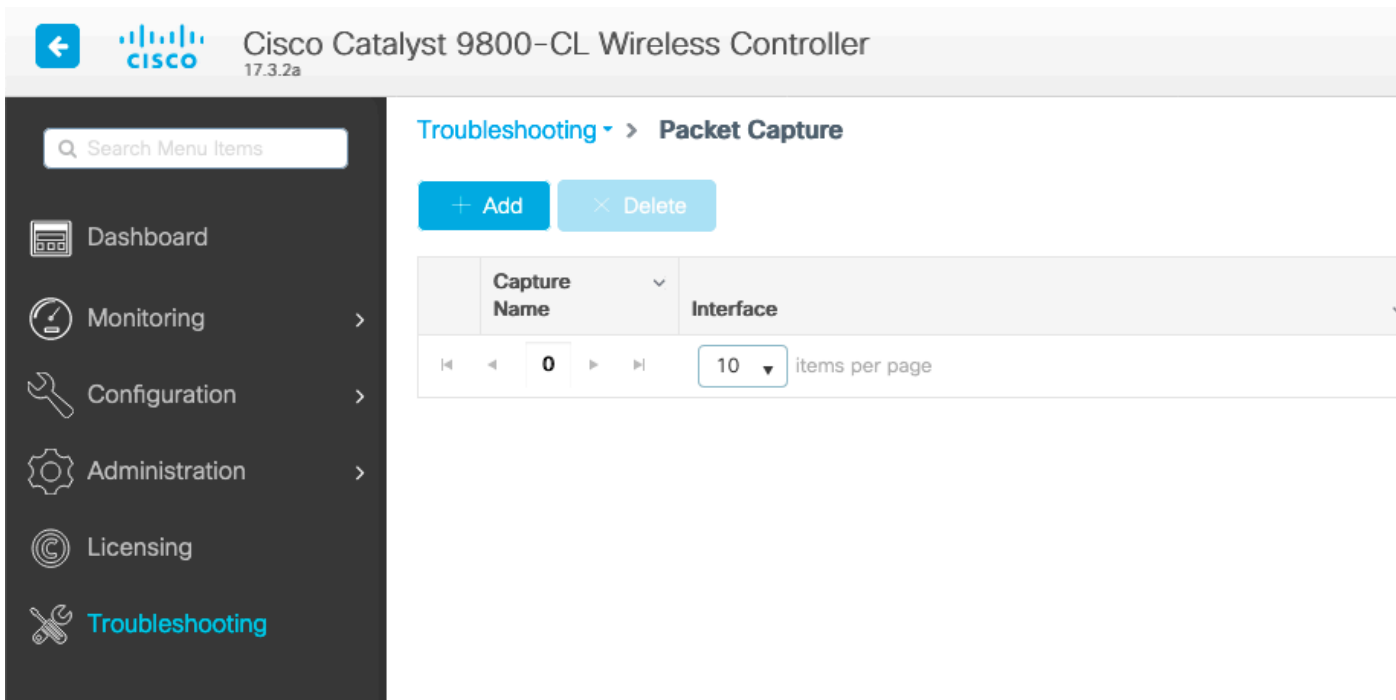
(Linux; Android 11; SM-G970F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Mobile Safari/537.36 2021/01/19 21:58:06.720038 {wncd\_x\_R0-0}{1}: [webauth-error] [9347]: (info): capwap\_90000004[2elf.3a65.9c09][ 192.168.1.17]Parse logo GET, File "/favicon.ico" not found 2021/01/19 21:58:06.720623 {wncd\_x\_R0-0}{1}: [auth-mgr] [9347]: (info): [2elf.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): [2elf.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): [2elf.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[2elf.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[2elf.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[2elf.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[2elf.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[2elf.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): [2elf.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): [2elf.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): [2elf.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[2elf.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[2elf.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[2elf.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[2elf.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): [2elf.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): [2elf.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): [2elf.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): [2elf.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): [2elf.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[2elf.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): [2elf.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 2elf.3a65.9c09 2021/01/19 21:58:16.374442 {wncd\_x\_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2elf.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): [2elf.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):
[2elf.3a65.9c09:capwap_90000004] Received User-Name Nico for client 2elf.3a65.9c09 2021/01/19
21:58:16.375294 {wncd_x_R0-0}{1}: [webauth-acl] [9347]: (info): capwap_90000004[2elf.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[2elf.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: 2elf.3a65.9c09 L3 Authentication Successful. ACL:[ ] 2021/01/19 21:58:16.378426
{wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2elf.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: 2elf.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:
2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.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: 2elf.3a65.9c09
2021/01/19 21:58:16.381152 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC:
2elf.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: 2elf.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 2elf.3a65.9c09
```

## Hoe de 9800-LDAP-connectiviteit te verifiëren

Je kunt een ingebedde opname nemen in de 9800 om te zien welk verkeer naar LDAP gaat.

Om een opname van WLC te maken, navigeer naar **Problemen oplossen > Packet Capture** en klik op **+Add**. Kies de uplinkpoort en start het opnemen.



Hier is een voorbeeld van succesverificatie voor gebruiker Nico

Time	Source	Destination	Protocol	Length	La Info
8696	22:58:16.412748	192.168.1.15	192.168.1.192	108	bindRequest(1) "Administrator@lab.com" simple
8697	22:58:16.414425	192.168.1.192	192.168.1.15	88	bindResponse(1) success
8699	22:58:16.419645	192.168.1.15	192.168.1.192	128	searchRequest(2) "CN=Users,DC=lab,DC=com" wholeSubtree
8700	22:58:16.420536	192.168.1.192	192.168.1.15	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	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	88	bindResponse(3) success

De eerste 2 pakketten vertegenwoordigen de WLC-binding aan de LDAP-dB, dat wil zeggen de WLC-authenticatie aan de database met de admin-gebruiker (om een zoekopdracht uit te kunnen voeren).

Deze 2 LDAP pakketten vertegenwoordigen WLC die een onderzoek in de basis DN doen (hier CN=users, DC=lab, DC=com). De binnenkant van het pakket bevat een filter voor de gebruikersnaam (hier "Nico"). De LDAP-database retourneert de gebruikerskenmerken als een succes

De laatste 2 pakketten vertegenwoordigen de WLC die probeert te verifiëren met dat gebruikerswachtwoord om te testen of het wachtwoord het juiste wachtwoord is.

### 1. Verzamel EPC en controleer of "sAMAccountName" is toegepast als filter:

Als het filter "cn" toont en als "sAMAaccountName" wordt gebruikt als gebruikersnaam, mislukt de verificatie.

Herstel het kenmerk ldap map van de WLC-client.

## 2. Zorg ervoor dat server "userPassword" teruggeeft in cleartext, anders authenticatie mislukt.

1197	16:25:05.708962	10.127.209.57	10.106.38.195	LDAP	searchRequest(3) "CN=users,DC=cciew,DC=local" wholeSubtree	
1198	16:25:05.709954	10.106.38.195	10.127.209.57	LDAP	searchResEntry(3) "CN=vk1,OU=Users,DC=cciew,DC=local"   searchResDone(3) success	[2 res...

- PartialAttributeList item userPassword
  - type: userPassword
  - vals: 1 item
    - AttributeValue: Cisco123
- PartialAttributeList item givenName
  - type: givenName
  - vals: 1 item
    - AttributeValue: vk1
- PartialAttributeList item distinguishedName
  - type: distinguishedName
  - vals: 1 item
    - AttributeValue: CN=vk1,OU=Users,DC=cciew,DC=local
- PartialAttributeList item instanceType
  - type: instanceType
  - vals: 1 item
    - AttributeValue: 4
- PartialAttributeList item whenCreated
  - type: whenCreated

## 3. Gebruik het gereedschap ldp.exe op de server om Base-DN-informatie te valideren.



FileZilla Client



Best match



Idp

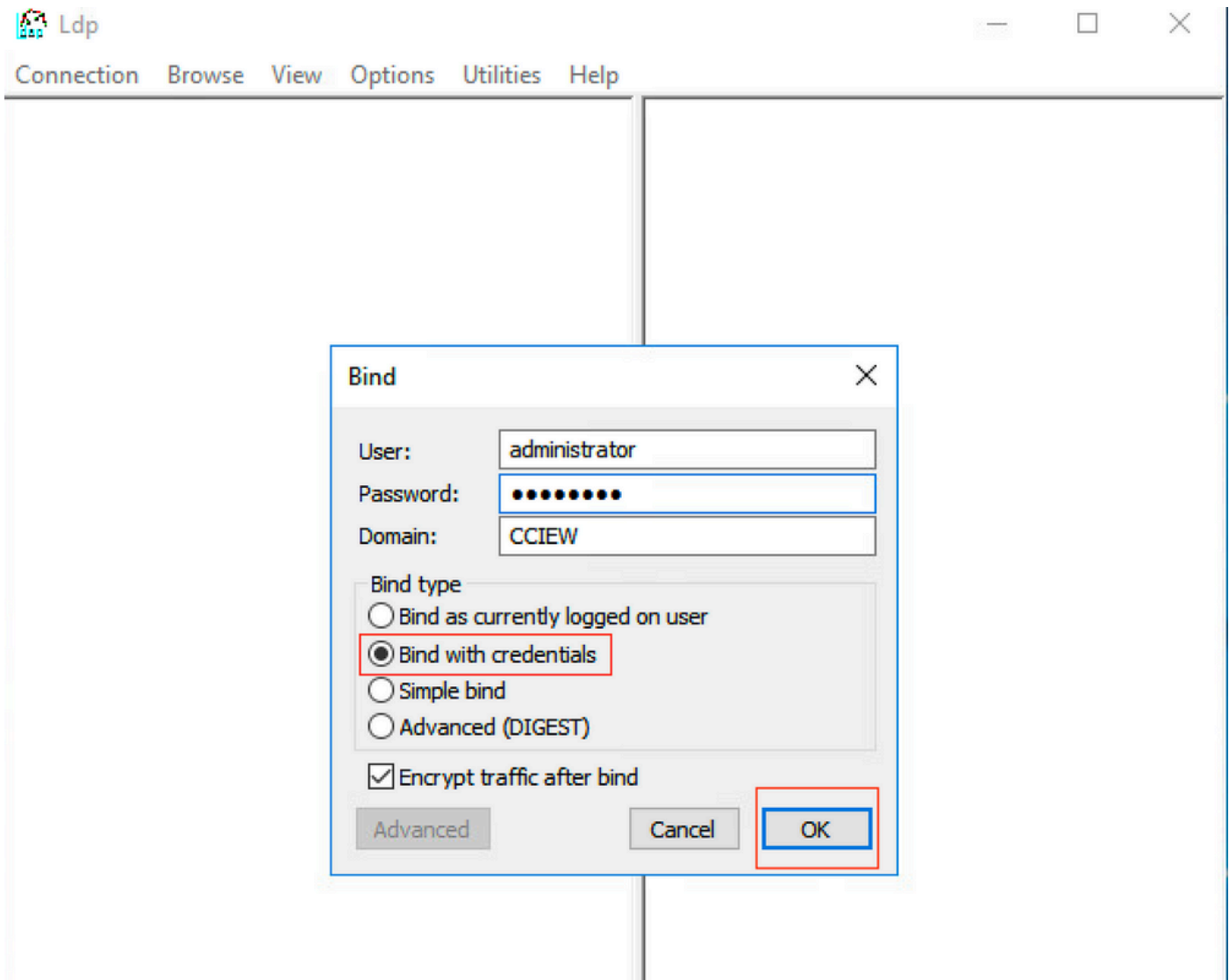
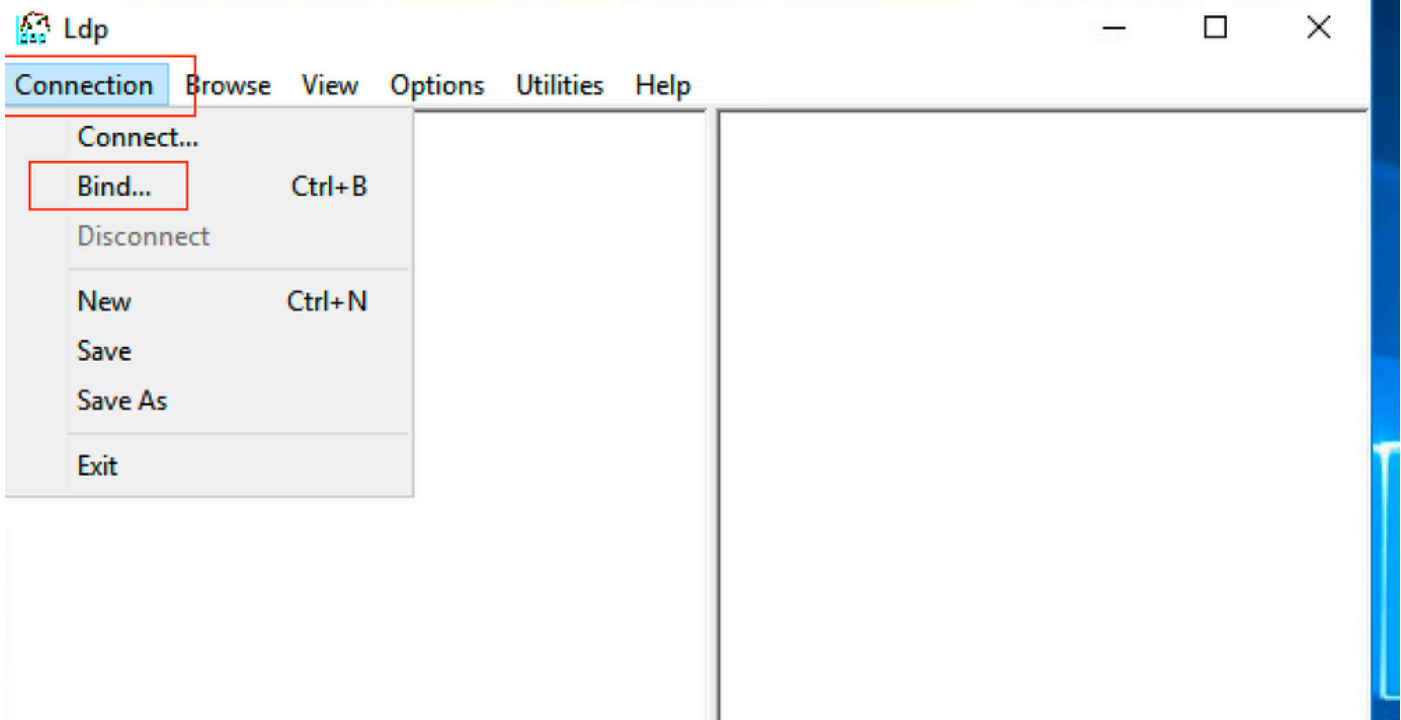
Run command



Idp







Idap://WIN-3JGG5JOCSVC.cciew.local/DC=cciew,DC=local

Connection Browse **View** Options Utilities Help

- Tree Ctrl+T
- Enterprise Configuration
- Status Bar
- Set Font...

```
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;
MaxDatagramRecv; MaxReceiveBuffer;
InitRecvTimeout; MaxConnections;
MaxConnIdleTime; MaxPageSize;
MaxBatchReturnMessage;
```

Idap://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;
```

**Tree View**

BaseDN:

```
MaxReceiveBuffer;
ns;
;
Duration;
SetSize;
erConn;
Range;
maxvarrange transitive, threadMemoryLimit;
SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
```

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=local
- ... 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=local
- ... 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=local
- ... CN=Allowed RODC Password Replication Group,CN=Users,DC=cciew,DC=local
- ... CN=Cert Publishers,CN=Users,DC=cciew,DC=local
- ... CN=Cloneable Domain Controllers,CN=Users,DC=cciew,DC=local
- ... CN=DefaultAccount,CN=Users,DC=cciew,DC=local
- ... CN=Denied RODC Password Replication Group,CN=Users,DC=cciew,DC=local
- ... CN=DnsAdmins,CN=Users,DC=cciew,DC=local
- ... CN=DnsUpdateProxy,CN=Users,DC=cciew,DC=local
- ... CN=Domain Admins,CN=Users,DC=cciew,DC=local
- ... CN=Domain Computers,CN=Users,DC=cciew,DC=local
- ... CN=Domain Controllers,CN=Users,DC=cciew,DC=local
- ... CN=Domain Guests,CN=Users,DC=cciew,DC=local
- ... CN=Domain Users,CN=Users,DC=cciew,DC=local
- ... CN=Enterprise Admins,CN=Users,DC=cciew,DC=local
- ... CN=Enterprise Key Admins,CN=Users,DC=cciew,DC=local
- ... CN=Enterprise Read-only Domain Controllers,CN=Users,DC=cciew,DC=local
- ... CN=Group Policy Creator Owners,CN=Users,DC=cciew,DC=local
- ... CN=Guest,CN=Users,DC=cciew,DC=local
- ... CN=kanu,CN=Users,DC=cciew,DC=local
- ... CN=Key Admins,CN=Users,DC=cciew,DC=local
- ... 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-abad-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_PASSWORD );
userPassword: Cisco123;
userPrincipalName: vk1@cciew.local;
uSNChanged: 160181;
uSNCreated: 94284;
whenChanged: 29-09-2021 15:16:40 India Standard Time;
whenCreated: 25-12-2020 16:25:53 India Standard Time;
-----
Expanding base 'CN=Users,DC=cciew,DC=local'...
Getting 1 entries:
Dn: CN=Users,DC=cciew,DC=local
cn: Users;
description: Default container for upgraded user accounts;
distinguishedName: CN=Users,DC=cciew,DC=local;
dSCorePropagationData (2): 29-09-2019 01:09:51 India Standard Time; 0x1 = ( NEW_SD );
instanceType: 0x4 = ( WRITE );
isCriticalSystemObject: TRUE;
name: Users;
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=cciew,DC=local;

```

```

... CN=Users,DC=cciew,DC=local
... CN=Administrator,CN=Users,DC=cciew,DC=local
... CN=Allowed RODC Password Replication Group,CN=Users,DC=cciew,DC=local
... CN=Cert Publishers,CN=Users,DC=cciew,DC=local
... CN=Cloneable Domain Controllers,CN=Users,DC=cciew,DC=local
... CN=DefaultAccount,CN=Users,DC=cciew,DC=local
... CN=Denied RODC Password Replication Group,CN=Users,DC=cciew,DC=local
... CN=DnsAdmins,CN=Users,DC=cciew,DC=local
... CN=DnsUpdateProxy,CN=Users,DC=cciew,DC=local
... CN=Domain Admins,CN=Users,DC=cciew,DC=local
... CN=Domain Computers,CN=Users,DC=cciew,DC=local
... CN=Domain Controllers,CN=Users,DC=cciew,DC=local
... CN=Domain Guests,CN=Users,DC=cciew,DC=local
... CN=Domain Users,CN=Users,DC=cciew,DC=local
... CN=Enterprise Admins,CN=Users,DC=cciew,DC=local
... CN=Enterprise Key Admins,CN=Users,DC=cciew,DC=local
... CN=Enterprise Read-only Domain Controllers,CN=Users,DC=cciew,DC=local
... CN=Group Policy Creator Owners,CN=Users,DC=cciew,DC=local
... CN=Guest,CN=Users,DC=cciew,DC=local
... CN=kanu,CN=Users,DC=cciew,DC=local
... CN=Key Admins,CN=Users,DC=cciew,DC=local
... CN=krbtgt,CN=Users,DC=cciew,DC=local
... CN=Protected Users,CN=Users,DC=cciew,DC=local
... CN=RAS and IAS Servers,CN=Users,DC=cciew,DC=local
... CN=Read-only Domain Controllers,CN=Users,DC=cciew,DC=local
... CN=Schema Admins,CN=Users,DC=cciew,DC=local
... CN=sony s,CN=Users,DC=cciew,DC=local
... CN=tejas,CN=Users,DC=cciew,DC=local
... CN=test,CN=Users,DC=cciew,DC=local
... CN=test123,CN=Users,DC=cciew,DC=local
... CN=vk,CN=Users,DC=cciew,DC=local
... CN=vk1,CN=Users,DC=cciew,DC=local
... No children
... CN=Yogesh G.,CN=Users,DC=cciew,DC=local

```

```

showInAdvancedViewOnly: FALSE,
systemFlags: 0x8C000000 = ( DISALLOW_DELETE | DOMAIN_DISALLOW_REI
uSNChanged: 5888;
uSNCreated: 5888;
whenChanged: 29-09-2019 01:08:06 India Standard Time;
whenCreated: 29-09-2019 01:08:06 India Standard Time;

```

```

Expanding base 'CN=vk1,CN=Users,DC=cciew,DC=local'...
Getting 1 entries:

```

```

Dn: CN=vk1,CN=Users,DC=cciew,DC=local
accountExpires: 9223372036854775807 (never);
adminCount: 1;
badPasswordTime: 0 (never);
badPwdCount: 0;
cn: vk1;
codePage: 0;
countryCode: 0;
displayName: vk1;
distinguishedName: CN=vk1,CN=Users,DC=cciew,DC=local;
dSCorePropagationData (2): 29-09-2021 15:16:40 India Standard Time; 0x0 =
givenName: vk1;
instanceType: 0x4 = ( WRITE );
lastLogoff: 0 (never);
lastLogon: 0 (never);
logonCount: 0;
memberOf (4): CN=Domain Admins,CN=Users,DC=cciew,DC=local; CN=Enterp
Admins,CN=Users,DC=cciew,DC=local; CN=Administrators,CN=Builtin,DC=
name: vk1;
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cciew,DC=loc
objectClass (4): top; person; organizationalPerson; user;
objectGUID: 1814f794-025e-4378-abad-66ff78a4a4d3;
objectSid: S-1-5-21-1375146846-274930181-3003521951-1120;
primaryGroupID: 513 = ( GROUP_RID_USERS );
pwdLastSet: 27-09-2021 22:56:11 India Standard Time;
sAMAccountName: vkokila;
sAMAccountType: 805306368 = ( NORMAL_USER_ACCOUNT );
userAccountControl: 0x10200 = ( NORMAL_ACCOUNT | DONT_EXPIRE_PASS
userPassword: Cisco123;
userPrincipalName: vk1@cciew.local;
uSNChanged: 160181;
uSNCreated: 94284;
whenChanged: 29-09-2021 15:16:40 India Standard Time;
whenCreated: 25-12-2020 16:25:53 India Standard Time;

```

#### 4. Controleer serverstatistieken en attribuut 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

-----

## Referenties

[Lokale EAP-configuratie op 9800-voorbeeld](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.