

# Konfigurieren von Catalyst 9800 WLC mit LDAP-Authentifizierung für 802.1X und Web-Authentifizierung

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[LDAP mit einer Webauth-SSID konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurieren des Controllers](#)

[Konfigurieren Sie LDAP mit einer dot1x SSID \(unter Verwendung von lokalem EAP\)](#)

[LDAP-Serverdetails verstehen](#)

[Grundlegende Informationen zu den Feldern auf der 9800-Webbenutzeroberfläche](#)

[LDAP 802.1x-Authentifizierung mit dem Attribut "sAMAccountName".](#)

[WLC-Konfiguration:](#)

[Überprüfung über Webschnittstelle:](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Überprüfen des Authentifizierungsprozesses auf dem Controller](#)

[So überprüfen Sie die Verbindung von 9800 mit LDAP](#)

[Referenzen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Catalyst 9800 konfigurieren, um Clients mit einem LDAP-Server als Datenbank für Benutzeranmeldeinformationen zu authentifizieren.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Microsoft Windows Server
- Active Directory oder eine andere LDAP-Datenbank

### Verwendete Komponenten

C9800 EWC auf einem C9100 Access Point (AP) mit Cisco IOS®-XE Version 17.3.2a

Microsoft Active Directory (AD) Server mit QNAP Network Access Storage (NAS), der als LDAP-Datenbank fungiert

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## LDAP mit einer Webauth-SSID konfigurieren

### Netzwerkdiagramm

Dieser Artikel basiert auf einer sehr einfachen Konfiguration:

Ein EWC AP 9115 mit IP 192.168.1.15

Ein Active Directory-Server mit der IP-Adresse 192.168.1.192

Ein Client, der sich mit dem internen AP des EWC verbindet.

### Konfigurieren des Controllers

#### Schritt 1: Konfigurieren des LDAP-Servers

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Gruppen > LDAP**, und klicken Sie auf **+ Hinzufügen**

The screenshot shows the Cisco Embedded Wireless Controller configuration interface. The breadcrumb navigation is **Configuration > Security > AAA**. Under the **Servers / Groups** tab, there are buttons for **+ Add** and **× Delete**. Below these buttons, there are sections for **RADIUS**, **TACACS+**, and **LDAP**. The **LDAP** section is highlighted. On the right side, there is a table with the following structure:

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

Wählen Sie einen Namen für Ihren LDAP-Server und geben Sie die Details ein. Eine Erläuterung der einzelnen Felder finden Sie im Abschnitt "LDAP-Serverdetails verstehen" dieses Dokuments.

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><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"/>	▼				

Speichern Sie, indem Sie auf **Aktualisieren** klicken und auf **das Gerät anwenden**.

CLI-Befehle:

```
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
```

**Schritt 2:** Konfigurieren einer LDAP-Servergruppe

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Gruppen > LDAP > Servergruppen**, und klicken Sie auf **+HINZUFÜGEN**

+ 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

Geben Sie einen Namen ein, und fügen Sie den LDAP-Server hinzu, den Sie im vorherigen Schritt konfiguriert haben.

Name\*

Idapgr

Group Type

LDAP

Available Servers

Assigned Servers

NAS



AD



Klicken Sie auf **Aktualisieren** und speichern.

CLI-Befehle:

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

**Schritt 3:** Konfigurieren der AAA-Authentifizierungsmethode

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methode Liste > Authentifizierung**, und klicken Sie auf **+Hinzufügen**

+ 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

Geben Sie einen Namen ein, wählen Sie den **Anmeldetyp aus**, und zeigen Sie auf die zuvor konfigurierte LDAP-Servergruppe.

### Quick Setup: AAA Authentication

Method List Name\*   

Type\*     ⓘ

Group Type     ⓘ

Fallback to local   

Available Server Groups    Assigned Server Groups

radius

ldap

tacacs+

>

<

>>

<<

ldapgr

⏪

⏩

⏴

⏵

CLI-Befehle:

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

#### Schritt 4: Konfigurieren einer AAA-Autorisierungsmethode

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Autorisierung**, und klicken Sie auf **+Hinzufügen**

+ 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

Erstellen Sie eine Regel für den Download von Anmeldeinformationen des gewünschten Namens, und verweisen Sie sie auf die zuvor erstellte LDAP-Servergruppe.

### 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-Befehle:

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

#### Schritt 5: Konfigurieren der lokalen Authentifizierung

Navigieren Sie zu **Configuration > Security > AAA > AAA Advanced > Global Config**

Legen Sie die lokale Authentifizierung und die lokale Autorisierung auf **Methodenliste fest**, und wählen Sie die zuvor konfigurierte Authentifizierungs- und Autorisierungsmethode aus.

+ 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-Befehle:

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

### Schritt 6: Konfigurieren der Webauth-Parameterzuordnung

Navigieren Sie zu **Configuration > Security > Web Auth**, und bearbeiten Sie die globale Zuordnung.

Configuration > Security > **Web Auth**

+ Add   × Delete

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

1   10 items per page

Konfigurieren Sie eine virtuelle IPv4-Adresse wie 192.0.2.1 (diese spezifische IP/Subnetz ist für nicht routbare virtuelle IPs reserviert).

## 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"/>

Klicken Sie zum Speichern auf **Anwenden**.

CLI-Befehle:

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

**Schritt 7:** Konfigurieren eines Webauthentifizierungs-WLAN



Navigieren Sie zu **Konfiguration > WLANs**, und klicken Sie auf **+Hinzufügen**

### 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		

Konfigurieren Sie den Namen, stellen Sie sicher, dass er aktiviert ist, und wechseln Sie dann zur Registerkarte **Sicherheit**.

Vergewissern Sie sich auf der Unterregisterkarte "**Layer 2**", dass keine Sicherheitsmaßnahmen vorhanden sind und dass "Fast Transition" deaktiviert ist.

### 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"/>

Aktivieren Sie auf der Registerkarte **Layer3** die **Webrichtlinie**, legen Sie die Parameterzuordnung auf **global fest** und setzen Sie die Authentifizierungsliste auf die zuvor konfigurierte AAA-Anmeldemethode.

⚠ 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*

Speichern durch Klicken auf **Übernehmen**

CLI-Befehle:

```
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
```

**Schritt 8:** Stellen Sie sicher, dass die SSID übertragen wird.

Navigieren Sie zu **Configuration > Tags (Konfiguration > Tags)**, und stellen Sie sicher, dass die SSID vom SSID (dem Standard-Policy-Tag für eine neue Konfiguration, wenn Sie noch keine Tags konfiguriert haben) in das aktuelle Richtlinienprofil integriert wird. Standardmäßig sendet das default-policy-tag keine neuen SSIDs, die Sie erstellen, bevor Sie sie manuell hinzufügen.

Dieser Artikel behandelt nicht die Konfiguration von Richtlinienprofilen und geht davon aus, dass Sie mit diesem Teil der Konfiguration vertraut sind.

## Konfigurieren Sie LDAP mit einer dot1x SSID (unter Verwendung von lokalem EAP)

Zum Konfigurieren von LDAP für eine 802.1X-SSID auf dem 9800 muss in der Regel auch der lokale EAP konfiguriert werden. Wenn Sie RADIUS verwenden, muss der RADIUS-Server eine Verbindung mit der LDAP-Datenbank herstellen. Dies ist nicht Gegenstand dieses Artikels. Vor dem Versuch dieser Konfiguration wird empfohlen, Local EAP mit einem auf dem WLC konfigurierten lokalen Benutzer zu konfigurieren. Am Ende dieses Artikels finden Sie ein Konfigurationsbeispiel im Abschnitt "Referenzen". Anschließend können Sie versuchen, die Benutzerdatenbank in Richtung LDAP zu verschieben.

**Schritt 1:** Konfigurieren eines lokalen EAP-Profiles

Navigieren Sie zu **Konfiguration > Lokales EAP**, und klicken Sie auf **+Hinzufügen**

The screenshot shows the Cisco Embedded Wireless Controller configuration 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 in blue), Administration, Licensing, and Troubleshooting. The breadcrumb path is "Configuration > Security > Local EAP". Below the breadcrumb, there are two tabs: "Local EAP Profiles" (active) and "EAP-FAST Parameters". There are two buttons: "+ Add" and "X 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" items per page and a dropdown menu set to "10 items per page".

Wählen Sie einen beliebigen Namen für Ihr Profil aus. Aktivieren Sie mindestens PEAP, und wählen Sie einen Vertrauenspunktnamen aus. Standardmäßig verfügt Ihr WLC nur über selbstsignierte Zertifikate, sodass es keine Rolle spielt, welches Zertifikat Sie auswählen (normalerweise ist TP-self-signed-xxxx das beste für diesen Zweck), aber da neue Versionen des Smartphone-Betriebssystems immer weniger selbstsignierten Zertifikaten vertrauen, sollten Sie ein vertrauenswürdigen öffentlich signiertes Zertifikat installieren.

## Edit Local EAP Profiles

Profile Name\*

PEAP

LEAP

EAP-FAST

EAP-TLS

PEAP

Trustpoint Name

TP-self-signed-3059



CLI-Befehle:

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

### Schritt 2: Konfigurieren des LDAP-Servers

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Gruppen > LDAP**, und klicken Sie auf **+ Hinzufügen**

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 tabs for **Servers / Groups**, **AAA Method List**, and **AAA Advanced**. The **Servers / Groups** tab is active, showing a table with columns for **RADIUS** and **TACACS+**. A **LDAP** entry is highlighted in the table. To the right, a modal window is open for adding a new server, with a **Servers** tab selected and a table containing a **NAS** entry.

Wählen Sie einen Namen für Ihren LDAP-Server und geben Sie die Details ein. Eine Erläuterung

der einzelnen Felder finden Sie im Abschnitt "LDAP-Serverdetails verstehen" dieses Dokuments.

**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"/>	▼				

Speichern Sie, indem Sie auf **Aktualisieren** klicken und auf **das Gerät anwenden**.

```
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
```

**Schritt 3:** Konfigurieren Sie eine LDAP-Servergruppe.

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Server/Gruppen > LDAP > Servergruppen**, und klicken Sie auf **+HINZUFÜGEN**

+ 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

Geben Sie einen Namen ein, und fügen Sie den LDAP-Server hinzu, den Sie im vorherigen Schritt konfiguriert haben.

Name\*

Idapgr

Group Type

LDAP

Available Servers

Assigned Servers

NAS

>

AD

<

>>

<<

⏪

⏩

⏴

⏵

Klicken Sie auf **Aktualisieren** und speichern.

CLI-Befehle:

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

#### Schritt 4: Konfigurieren einer AAA-Authentifizierungsmethode

Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authentication**, und klicken Sie auf **+Add**

Konfigurieren Sie eine Authentifizierungsmethode vom Typ **dot1x**, und verweisen Sie sie nur auf

lokal. Es wäre verführerisch, auf die LDAP-Servergruppe zu verweisen, aber es ist der WLC selbst, der hier als 802.1X-Authentifizierer fungiert (obwohl die Benutzerdatenbank auf LDAP basiert, dies jedoch der Autorisierungsmethodenauftrag ist).

## Quick Setup: AAA Authentication

Method List Name*	<input type="text" value="ldapauth"/>
Type*	<input type="text" value="dot1x"/> ⓘ
Group Type	<input type="text" value="local"/> ⓘ

### Available Server Groups

radius
ldap
tacacs+
ldapgr

### Assigned Server Groups

>	⏪
<	⏩
»	⏴
«	⏵

CLI-Befehl:

```
aaa authentication dot1x ldapauth local
```

### Schritt 5: Konfigurieren einer AAA-Autorisierungsmethode

Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authorization**, und klicken Sie auf **+Add**

Erstellen Sie eine Autorisierungsmethode **für den Download** von Anmeldeinformationen, und verweisen Sie auf die LDAP-Gruppe.

## 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-Befehl:

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

### Schritt 6: Lokale Authentifizierungsdetails konfigurieren

Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > AAA Advanced**.

Wählen Sie **Methodenliste** für Authentifizierung und Autorisierung aus, und wählen Sie die lokal zeigende 802.1x-Authentifizierungsmethode und die Autorisierungsmethode zum Herunterladen von Anmeldeinformationen für LDAP aus.



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    ldapauth

Local Authorization    Method List

Authorization Method List    ldapauth

Radius Server Load Balance     DISABLED

Interim Update   

[Show Advanced Settings >>>](#)

CLI-Befehl:

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

### Schritt 7: Konfigurieren eines dot1x-WLAN

Navigieren Sie zu **Konfiguration > WLAN**, und klicken Sie auf **+Hinzufügen**

Wählen Sie ein Profil und einen SSID-Namen aus, und stellen Sie sicher, dass diese Option aktiviert ist.

### 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	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	1		
Status	<input checked="" type="checkbox"/> ENABLED		

Wechseln Sie zur Registerkarte Layer 2-Sicherheit.

WPA+WPA2 als **Layer-2-Sicherheitsmodus** auswählen

Stellen Sie sicher, dass WPA2 und AES in den **WPA-Parametern** aktiviert sind, und aktivieren Sie **802.1X**.

**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

Wechseln Sie zur Unterregisterkarte **AAA**.

Wählen Sie die zuvor erstellte 802.1x-Authentifizierungsmethode aus, aktivieren Sie die lokale EAP-Authentifizierung, und wählen Sie das im ersten Schritt konfigurierte EAP-Profil aus.

## 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	<input type="text" value="ldapauth"/> ⓘ
Local EAP Authentication	<input checked="" type="checkbox"/>
EAP Profile Name	<input type="text" value="PEAP"/>

Speichern durch Klicken auf Anwenden

CLI-Befehle:

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

### Schritt 8: Überprüfen des WLAN-Broadcasts

Navigieren Sie zu **Configuration > Tags (Konfiguration > Tags)**, und stellen Sie sicher, dass die SSID vom SSID (dem Standard-Policy-Tag für eine neue Konfiguration, wenn Sie noch keine Tags konfiguriert haben) in das aktuelle Richtlinienprofil integriert wird. Standardmäßig sendet das default-policy-tag keine neuen SSIDs, die Sie erstellen, bevor Sie sie manuell hinzufügen.

Dieser Artikel behandelt nicht die Konfiguration von Richtlinienprofilen und geht davon aus, dass Sie mit diesem Teil der Konfiguration vertraut sind.

Wenn Sie Active Directory verwenden, müssen Sie den AD-Server so konfigurieren, dass das Attribut "userPassword" gesendet wird. Dieses Attribut muss an den WLC gesendet werden. Der Grund hierfür ist, dass der WLC die Überprüfung übernimmt, nicht der AD-Server. Sie können auch Probleme bei der Authentifizierung mit der PEAP-mschapv2-Methode haben, da das Kennwort nie im Klartext gesendet wird und daher nicht mit der LDAP-Datenbank überprüft werden kann. Nur die PEAP-GTC-Methode würde mit bestimmten LDAP-Datenbanken funktionieren.

## LDAP-Serverdetails verstehen

Grundlegende Informationen zu den Feldern auf der 9800-Webbenutzeroberfläche

Hier ist ein Beispiel für ein sehr einfaches Active Directory, das als LDAP-Server auf dem 9800 konfiguriert wird.

### Edit AAA LDAP Server ✕

Server Name*	<input type="text" value="AD"/>					
Server Address*	<input type="text" value="192.168.1.192"/>	<span>⚠ Provide a valid Server address</span>				
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"/>	<span>+</span>				
<table><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"/>					

Name und IP sind hoffentlich selbsterklärend.

Anschluss: 389 ist der Standardport für LDAP, Ihr Server kann jedoch einen anderen verwenden.

Einfache Bindung: Es ist heutzutage sehr selten, dass eine LDAP-Datenbank nicht authentifizierte Bindungen unterstützt (das heißt, jeder kann ohne Authentifizierungsformular eine LDAP-Suche durchführen). Authentifizierte einfache Bindung ist der häufigste Authentifizierungstyp und ermöglicht Active Directory standardmäßig. Sie können einen Namen und ein Kennwort für ein Administratorkonto eingeben, um von dort aus in der Benutzerdatenbank suchen zu können.

**Bind-Benutzername:** Sie müssen auf einen Benutzernamen mit Administratorrechten in Active Directory zeigen. AD toleriert das Format "user@domain", während viele andere LDAP-Datenbanken ein "CN=xxx,DC=xxx"-Format für den Benutzernamen erwarten. Ein Beispiel mit einer anderen LDAP-Datenbank als AD finden Sie weiter unten in diesem Artikel.

**Bind-Passwort:** Geben Sie das Kennwort ein, das Sie zuvor mit dem Benutzernamen admin eingegeben haben.

**Benutzerbasis-DN:** Geben Sie hier den "Suchbegriff" ein, d.h. den Ort in Ihrem LDAP-Baum, an dem die Suche beginnt. In diesem Beispiel befinden sich alle unsere Verwendungen unter der Gruppe "Benutzer", deren DN "CN=Users,DC=lab,DC=com" ist (da die Beispiel-LDAP-Domäne lab.com ist). Ein Beispiel, wie Sie diese Benutzerbasis-DN herausfinden, finden Sie weiter unten in diesem Abschnitt.

**Benutzerattribut:** Dies kann leer gelassen werden, oder Sie zeigen auf eine LDAP-Attributzuordnung, die angibt, welches LDAP-Feld als Benutzername für Ihre LDAP-Datenbank gezählt wird. Aufgrund der Bug-ID von Cisco [CSCv11813](#), versucht der WLC eine Authentifizierung mit dem CN-Feld, egal was passiert.

**Benutzerobjekttyp:** Bestimmt den Typ von Objekten, die als Benutzer betrachtet werden. Normalerweise ist dies "Person". Es könnte "Computer" sein, wenn Sie eine AD-Datenbank haben und Computerkonten authentifizieren, aber auch hier bietet LDAP eine Menge Anpassung.

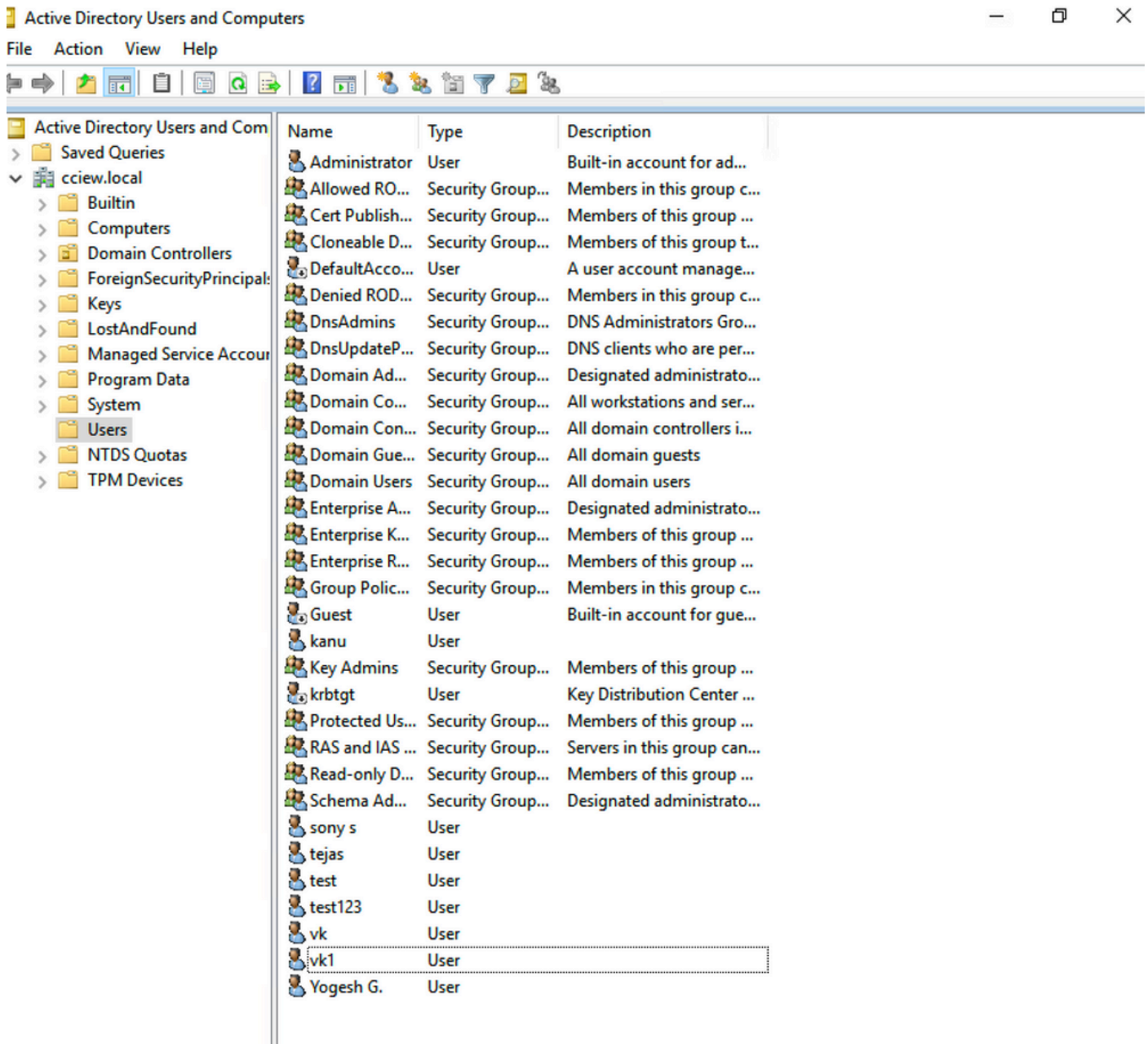
Der sichere Modus aktiviert Secure LDAP over TLS und erfordert die Auswahl eines Vertrauenspunkts auf dem 9800, um ein Zertifikat für die TLS-Verschlüsselung zu verwenden.

## **LDAP 802.1x-Authentifizierung mit dem Attribut "sAMAaccountName".**

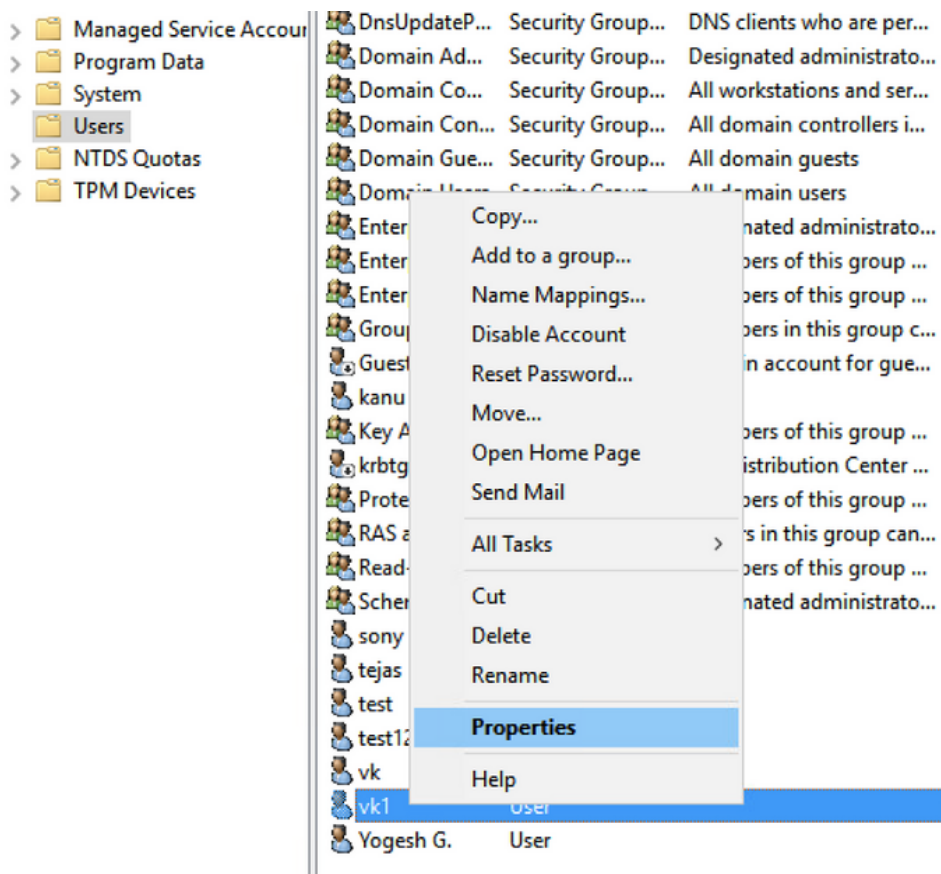
Diese Erweiterung wird in Version 17.6.1 eingeführt.

**Konfigurieren Sie das Attribut "userPassword" für den Benutzer.**

Schritt 1. Navigieren Sie auf dem Windows-Server zu Active Directory-Benutzer und -Computer.



Schritt 2. Klicken Sie mit der rechten Maustaste auf den entsprechenden Benutzernamen und wählen Sie Eigenschaften



Schritt 3: Wählen Sie im Eigenschaftenfenster den Attribut-Editor

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

Schritt 4: Konfigurieren des Attributs "userPassword" Dies ist das Kennwort für den Benutzer, der



als Hexadezimalwert konfiguriert werden muss.

vk1 Properties



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

Multi-valued Octet String Editor

Attribute: userPassword

Values:

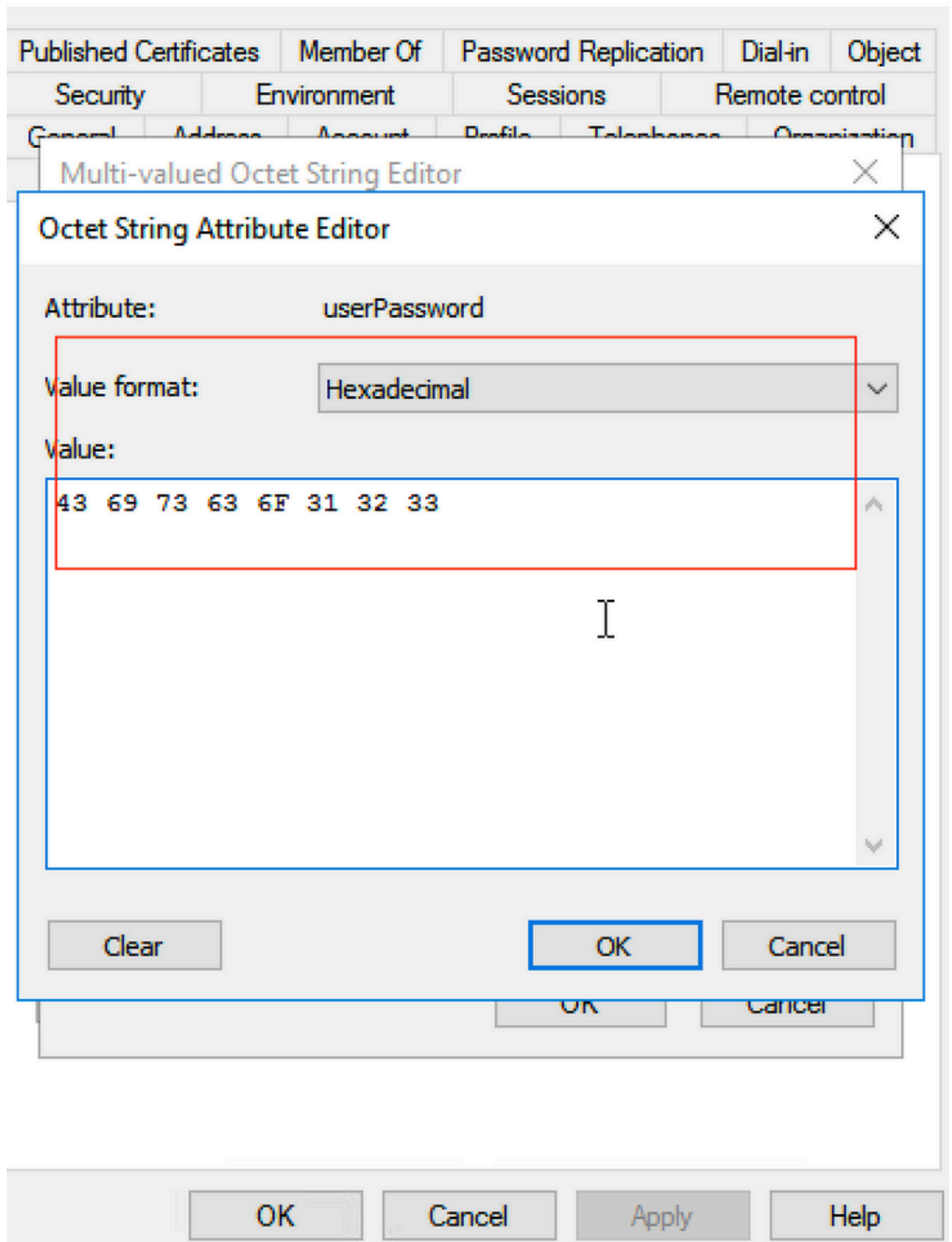
Add

Remove

Edit

OK

Cancel



Klicken Sie auf OK, und prüfen Sie, ob das Kennwort richtig angezeigt wird.

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

## Multi-valued Octet String Editor ✕

Attribute: userPassword

Values:

Cisco123

Add

Remove

Edit

OK

Cancel

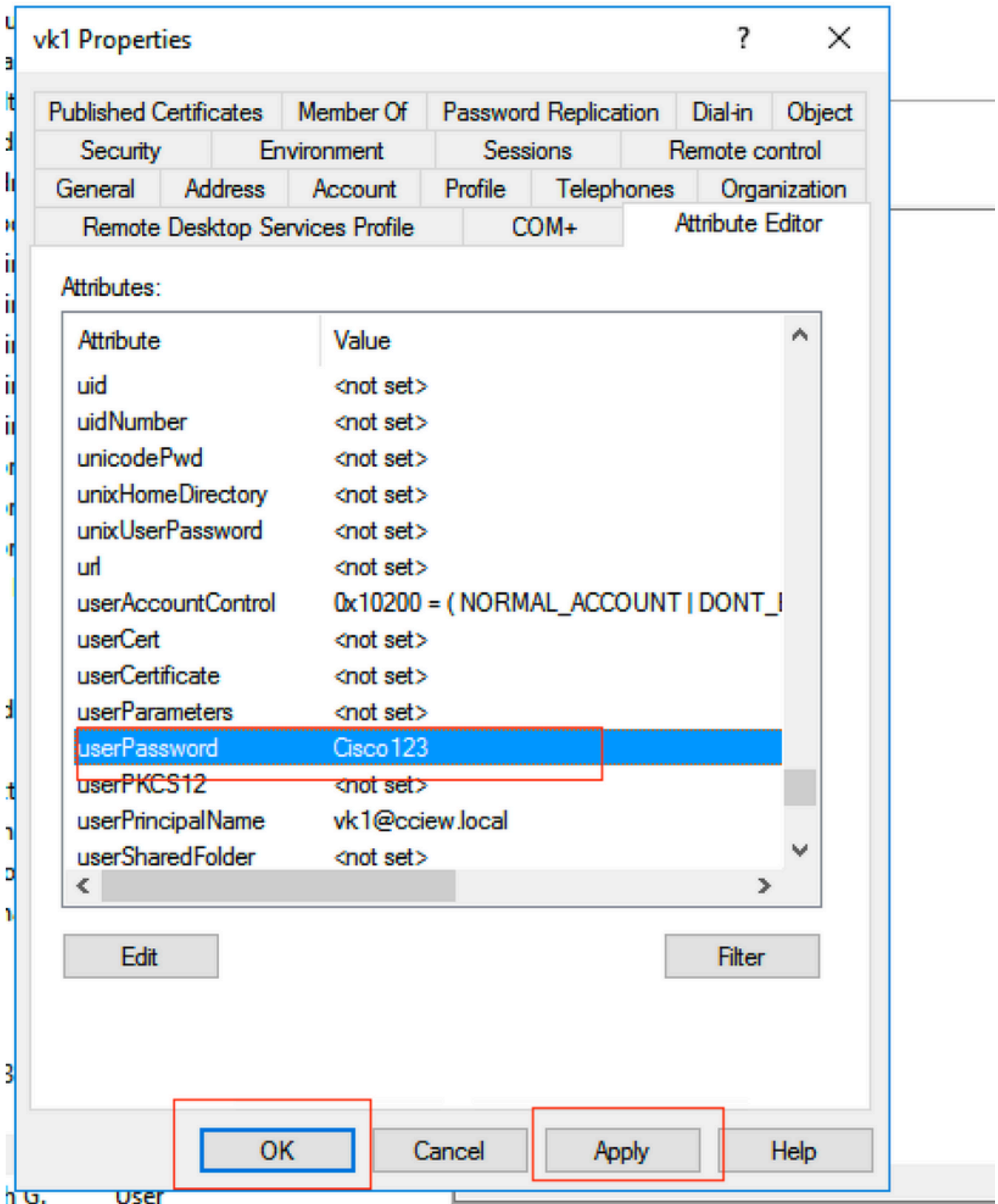
OK

Cancel

Apply

Help

Schritt 5: Klicken Sie auf Apply und dann auf OK



Schritt 6: Überprüfen Sie den Attributwert "sAMAccountName" für den Benutzer und den Benutzernamen für die Authentifizierung.

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>

Buttons: Edit, Filter, OK, Cancel, Apply, Help

G. User

WLC-Konfiguration:

Schritt 1: LDAP-Attribut erstellen MAP

Schritt 2: Konfigurieren Sie das Attribut "sAMAccountName", und geben Sie "username" ein.

Schritt 3: Wählen Sie das erstellte Attribut MAP unter der LDAP-Serverkonfiguration.

```
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
```

## Überprüfung über Webschnittstelle:

The screenshot shows the Cisco Catalyst 9800-40 Wireless Controller configuration page. 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 an 'Add' button and a 'Delete' button. Below this, there are tabs for 'Servers' and 'Server Groups'. The 'Servers' tab is active, displaying a table with the following data:

Name	Server Address	Port Number	Simple Bind
ldap	10.106.38.195	389	Authenticated

The table has a search icon in the first column and a '10 items per page' dropdown at the bottom. The page number '1 - 1 of 1' is visible in the bottom right corner.

Last login NA ...

Edit AAA LDAP Server

---

AAA Advanced

---

Server Groups

Name	Server Address
ldap	10.106.38.195

1 ▶ ◀ 10 ▼ items per page

**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)**

## Überprüfung

Überprüfen Sie die CLI-Befehle mit den in diesem Artikel beschriebenen Befehlen, um Ihre Konfiguration zu überprüfen.

LDAP-Datenbanken bieten in der Regel keine Authentifizierungsprotokolle, sodass es schwierig sein kann, zu wissen, was geschieht. Im Abschnitt "Fehlerbehebung" dieses Artikels erfahren Sie, wie Sie Ablaufverfolgungen und Sniffer-Erfassung durchführen, um festzustellen, ob eine Verbindung zur LDAP-Datenbank besteht.

## Fehlerbehebung

Um dieses Problem zu beheben, ist es am besten, es in zwei Teile aufzuteilen. Im ersten Teil wird der lokale EAP-Teil validiert. Zum anderen muss überprüft werden, ob der 9800 ordnungsgemäß mit dem LDAP-Server kommuniziert.

### Überprüfen des Authentifizierungsprozesses auf dem Controller

Sie können eine radioaktive Spur sammeln, um die "debugs" der Clientverbindung zu erhalten.

Gehen Sie einfach zu **Troubleshooting > Radioactive Trace**. Fügen Sie die Client-MAC-Adresse hinzu (achten Sie darauf, dass Ihr Client eine zufällige MAC und nicht seine eigene MAC verwenden kann, Sie können dies im SSID-Profil auf dem Client-Gerät selbst überprüfen) und drücken Sie Start.

Sobald Sie den Verbindungsversuch reproduziert haben, können Sie auf "Generieren" klicken und

die Protokolle für die letzten X Minuten abrufen. Vergewissern Sie sich, dass Sie auf **Intern** klicken, da einige LDAP-Protokollzeilen nicht angezeigt werden, wenn Sie dies nicht zulassen.

Im Folgenden finden Sie ein Beispiel für die radioaktive Verfolgung eines Clients, der sich erfolgreich auf einer Webauthentifizierungs-SSID authentifiziert. Aus Gründen der Klarheit wurden einige redundante Teile entfernt:

```
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_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):
[2elf.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):
[2elf.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): [2elf.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: 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_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):
[2elf.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):
[2elf.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):
[2elf.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): [2elf.3a65.9c09:capwap_90000004] Allocated audit
session id 00000000000009C1CA610D7 2021/01/19 21:57:55.894285 {wncd_x_R0-0}{1}: [auth-mgr]
[9347]: (info): [2elf.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):
[2elf.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):
[2elf.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): [2elf.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): [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

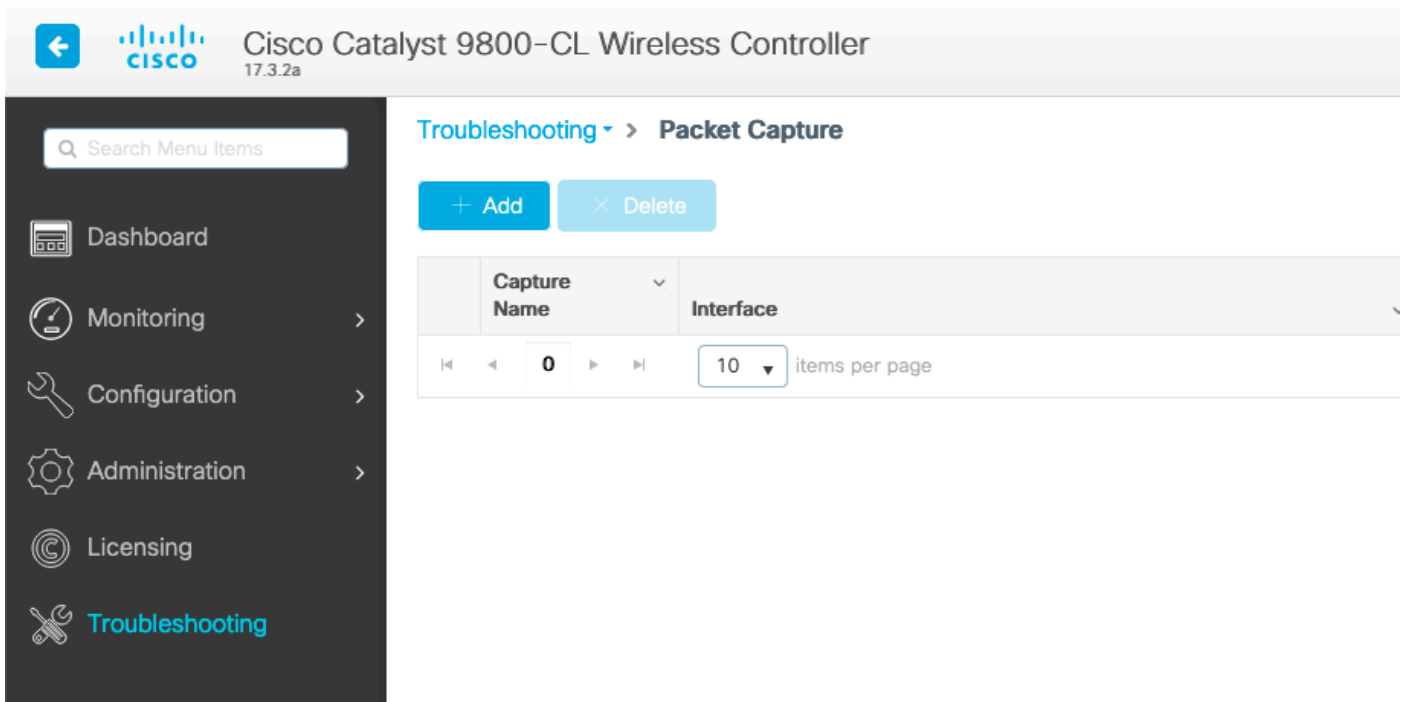
{wncd\_x\_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap\_90000004[2elf.3a65.9c09][192.168.1.17]Parse GET, src [192.168.1.17] dst [192.0.2.1] url [https://192.0.2.1:443/favicon.ico] 2021/01/19 21:58:06.719646 {wncd\_x\_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap\_90000004[2elf.3a65.9c09][ 192.168.1.17]Retrieved 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
```

## So überprüfen Sie die Verbindung von 9800 mit LDAP

Sie können eine integrierte Erfassung im 9800 durchführen, um zu sehen, welcher Datenverkehr zum LDAP geht.

Um eine Aufzeichnung vom WLC zu übernehmen, navigieren Sie zu **Troubleshooting > Packet Capture**, und klicken Sie auf **+Add**. Wählen Sie den Uplink-Port aus, und fangen Sie mit der Erfassung an.



Hier ist ein Beispiel für die erfolgreiche Authentifizierung des Benutzers Nico

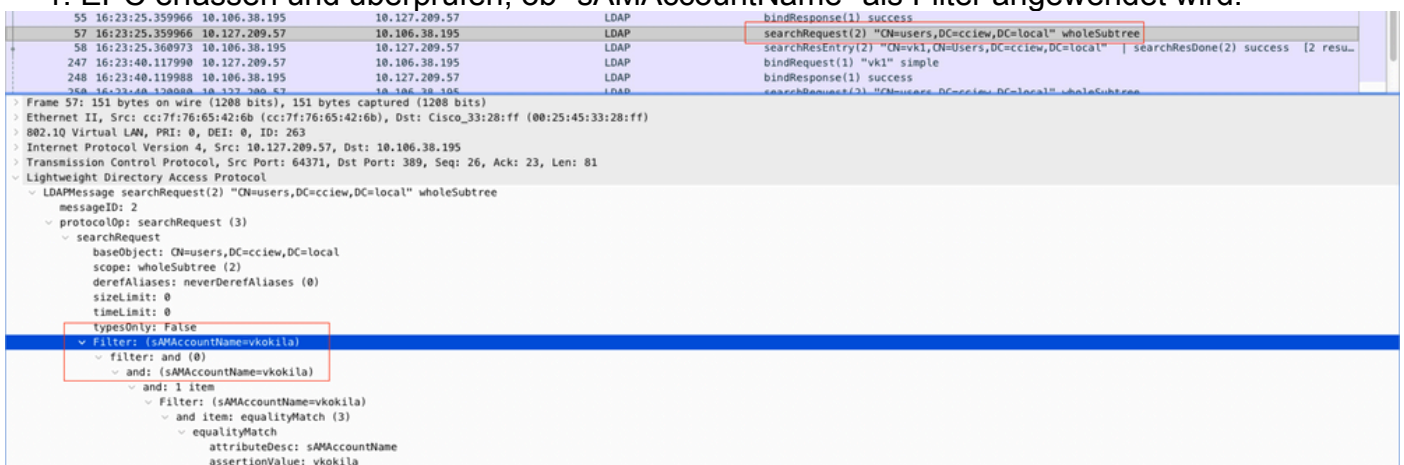
Time	Source	Destination	Protocol	Length	La	Info
8696	22:58:16.412748	192.168.1.15	192.168.1.192	LDAP	108	bindRequest(1) "Administrator@lab.com" simple
8697	22:58:16.414425	192.168.1.192	192.168.1.15	LDAP	88	bindResponse(1) success
8699	22:58:16.419645	192.168.1.15	192.168.1.192	LDAP	128	searchRequest(2) "CN=Users,DC=lab,DC=com" wholeSubtree
8700	22:58:16.420536	192.168.1.192	192.168.1.15	LDAP	1260	searchResEntry(2) "CN=Nico,CN=Users,DC=lab,DC=com"   searchResDone(2) success [1 result]
8701	22:58:16.422383	192.168.1.15	192.168.1.192	LDAP	117	bindRequest(3) "CN=Nico,CN=Users,DC=lab,DC=com" simple
8702	22:58:16.423513	192.168.1.192	192.168.1.15	LDAP	88	bindResponse(3) success

Die ersten 2 Pakete stellen die WLC-Bindung an die LDAP-Datenbank dar, d. h. der WLC authentifiziert sich bei der Datenbank mit dem Admin-Benutzer (um eine Suche durchführen zu können).

Diese 2 LDAP-Pakete stellen den WLC dar, der in der Basis-DN sucht (hier CN=Users,DC=lab,DC=com). Das Paketinnere enthält einen Filter für den Benutzernamen (hier "Nico"). Die LDAP-Datenbank gibt die Benutzerattribute als erfolgreich zurück.

Die letzten zwei Pakete stellen den WLC dar, der versucht, sich mit diesem Benutzerkennwort zu authentifizieren, um zu testen, ob das Kennwort richtig ist.

### 1. EPC erfassen und überprüfen, ob "sAMAccountName" als Filter angewendet wird:



Wenn der Filter "cn" anzeigt und "sAMAccountName" als Benutzername verwendet wird, schlägt

die Authentifizierung fehl.

Konfigurieren Sie das LDAP-Zuordnungsattribut aus der WLC-CLI neu.

2. Stellen Sie sicher, dass der Server "userPassword" im Klartext zurückgibt, andernfalls schlägt die Authentifizierung fehl.

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

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

3. Verwenden Sie das Tool ldp.exe auf dem Server, um die Basis-DN-Informationen zu überprüfen.



FileZilla Client



Best match



Idp

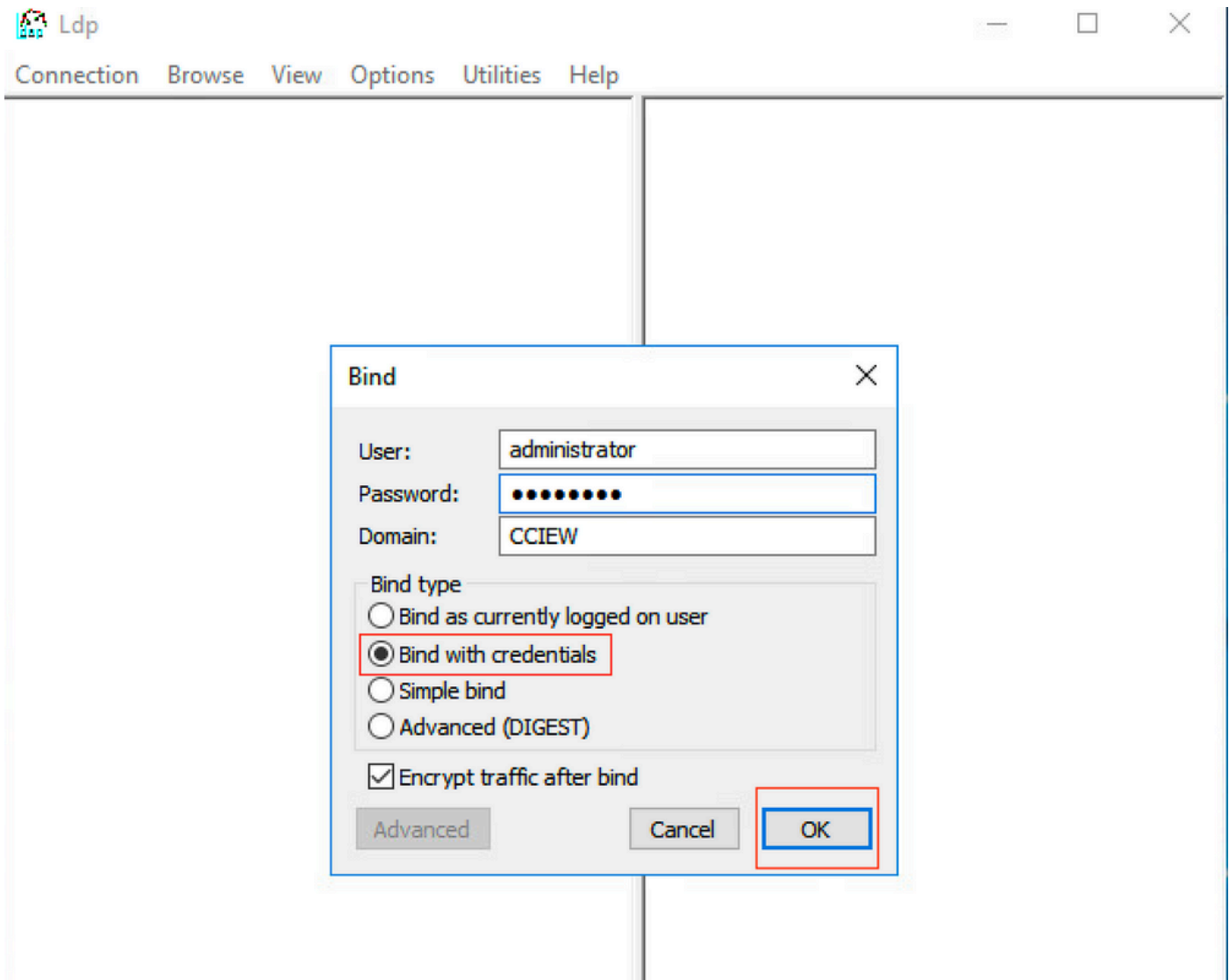
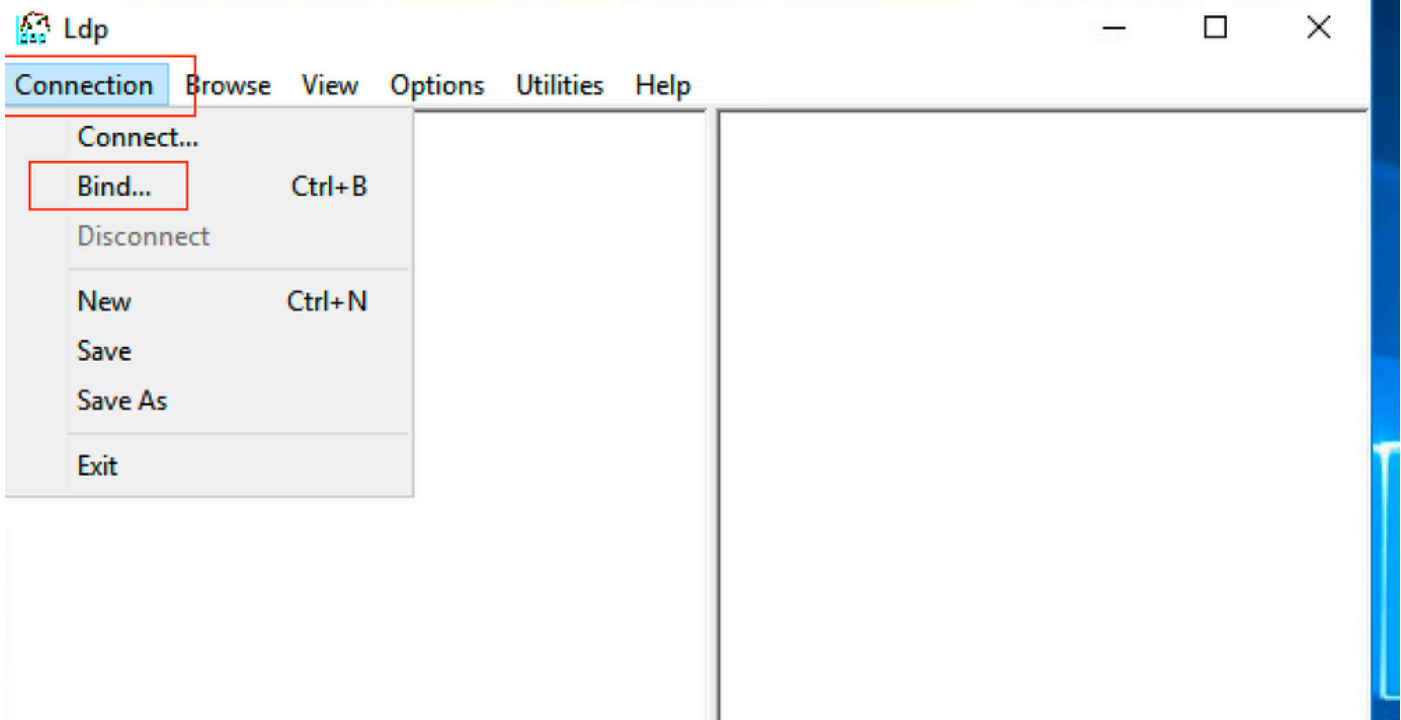
Run command



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;
lRange;
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. Serverstatistiken und Attribut-MAP überprüfen

```
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

-----

## Referenzen

[Lokales EAP am 9800-Konfigurationsbeispiel](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.