

Configurazione di Catalyst 9800 WLC con autenticazione LDAP per 802.1X e Web-auth

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurare LDAP con un SSID Webauth](#)

[Esempio di rete](#)

[Configurare il controller](#)

[Configurare LDAP con un SSID dot1x \(mediante EAP locale\)](#)

[Informazioni sui dettagli del server LDAP](#)

[Informazioni sui campi nell'interfaccia utente Web 9800](#)

[Autenticazione LDAP 802.1x con attributo sAMAaccountName.](#)

[Configurazione WLC](#)

[Verifica dall'interfaccia Web](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Come verificare il processo di autenticazione sul controller](#)

[Come verificare la connettività da 9800 a LDAP](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare un Catalyst 9800 in modo che autentichi i client con un server LDAP come database per le credenziali utente.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Server Microsoft Windows
- Active Directory o qualsiasi altro database LDAP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C9800 EWC su access point C9100 (AP) con Cisco IOS® XE versione 17.3.2a
- Server Microsoft Active Directory (AD) con archiviazione QNAP Network Access (NAS) che funge da database LDAP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurare LDAP con un SSID Webauth

Esempio di rete

Questo articolo si basa su una configurazione molto semplice:

EWC AP 9115 con IP 192.168.1.15

Un server Active Directory con IP 192.168.1.192

Un client che si connette al punto di accesso interno del CAE

Configurare il controller

Passaggio 1. Configurare il server LDAP.

Selezionare Configurazione > Protezione > AAA > Server/Gruppi > LDAP e fare clic su + Aggiungi.

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 list of servers with columns for 'Name' and a checkbox. A table is visible with the following content:

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

Scegliere un nome per il server LDAP e specificare i dettagli. Per ulteriori informazioni su ciascun campo, consultare la sezione Informazioni sui dettagli del server LDAP di questo documento.

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="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"/>					

Salvare facendo clic su Aggiorna e applica al dispositivo.

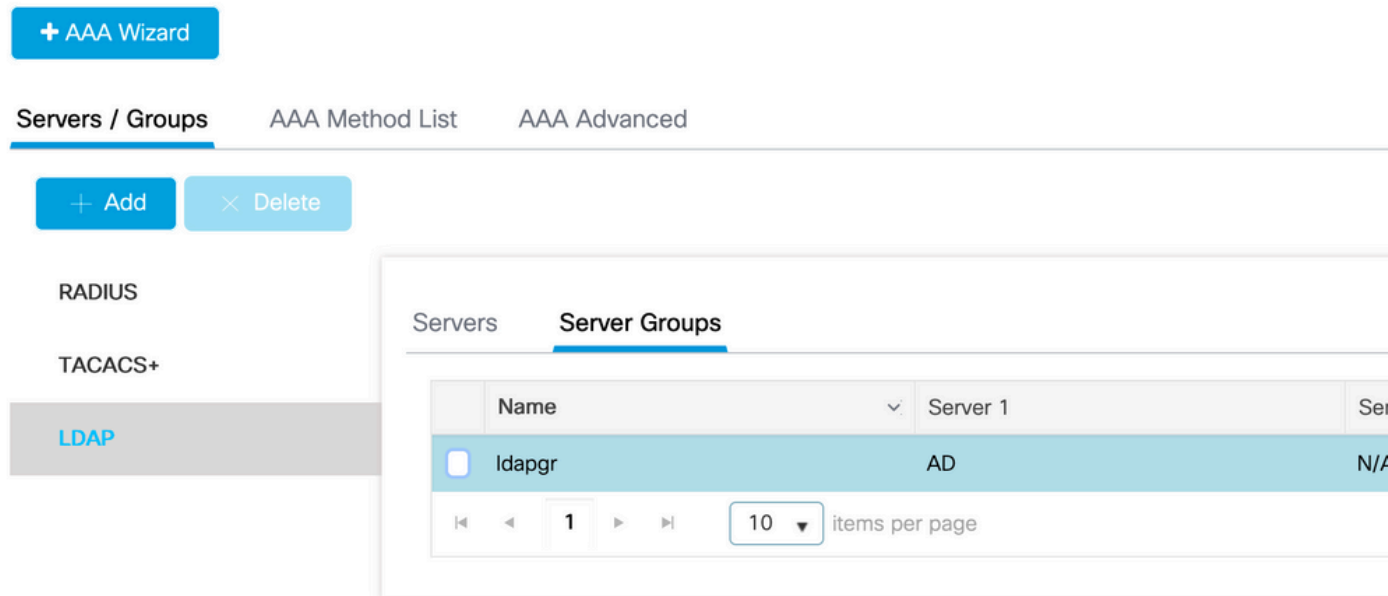
Comandi CLI:

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

Passaggio 2. Configurare un gruppo di server LDAP.

Selezionare Configurazione > Protezione > AAA > Server/ Gruppi > LDAP > Gruppi di server e fare clic su +ADD.

Configuration > Security > AAA



Immettere un nome e aggiungere il server LDAP configurato nel passaggio precedente.

Name*

Group Type

Available Servers

Assigned Servers

Navigation buttons: >, <, >>, <<, ^, v, v

Fare clic su Aggiorna e applicare per salvare.

Comandi CLI:

```
aaa group server ldap ldapgr
```

server AD

Passaggio 3. Configurare il metodo di autenticazione AAA.

Selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione e fare clic su +Aggiungi.

Configuration > Security > AAA

+ AAA Wizard

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

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

Immettere un nome, scegliere il tipo di login e scegliere il gruppo di server LDAP configurato in precedenza.

Quick Setup: AAA Authentication

Method List Name* ldapauth

Type* login ⓘ

Group Type group ⓘ

Fallback to local

Available Server Groups Assigned Server Groups

radius
ldap
tacacs+ > < >> << ldapgr ⏪ ⏩ ⏴ ⏵

Comandi CLI:

aaa authentication login ldapauth group ldapgr

Passaggio 4. Configurare un metodo di autorizzazione AAA.

Selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione e fare clic su +Aggiungi.

Configuration > Security > AAA

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

Creare una regola per il download delle credenziali con il nome desiderato e puntarla al gruppo di server LDAP creato in precedenza.

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

Comandi CLI:

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

Passaggio 5. Configura autenticazione locale.

Selezionare Configurazione > Sicurezza > AAA > AAA Avanzate > Configurazione globale.

Impostare l'autenticazione e l'autorizzazione locali su Elenco metodi e scegliere il metodo di autenticazione e autorizzazione configurato in precedenza.

[Configuration](#) > [Security](#) > [AAA](#)

The screenshot shows the 'AAA Advanced' configuration page. On the left, there is a sidebar with a '+ AAA Wizard' button and a list of configuration sections: 'Global Config' (highlighted), 'RADIUS Fallback', 'Attribute List Name', 'Device Authentication', 'AP Policy', 'Password Policy', and 'AAA Interface'. The main content area is titled 'AAA Advanced' and contains several settings:

- Local Authentication: Method List (dropdown)
- Authentication Method List: ldapauth (dropdown)
- Local Authorization: Method List (dropdown)
- Authorization Method List: ldapauth (dropdown)
- Radius Server Load Balance: DISABLED (checkbox)
- Interim Update:

At the bottom of the main content area, there is a link: [Show Advanced Settings >>>](#)

Comandi CLI:

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

Passaggio 6. Configurare la mappa dei parametri webauth.

Passare a Configurazione > Sicurezza > Autenticazione Web e modificare la mappa globale.

Configuration > Security > Web Auth

+ Add

× Delete

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

◀ ◁ 1 ▷ ▶ 10 items per page

Assicurarsi di configurare un indirizzo IPv4 virtuale, ad esempio 192.0.2.1 (la subnet/IP specifico è riservato all'IP virtuale non instradabile).

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"/>

Fare clic su Apply (Applica) per salvare.

Comandi CLI:

```
parameter-map type webauth global  
type webauth
```

virtual-ip ipv4 192.0.2.1

Passaggio 7. Configurare una WLAN webauth.

Selezionare Configurazione > WLAN e fare clic su +Aggiungi.

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		

Configurare il nome, verificare che sia nello stato abilitato, quindi passare alla scheda Protezione.

Nella scheda secondaria Layer 2, verificare che non vi siano protezioni e che la funzione Transizione rapida sia disabilitata.

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"/>

Nella scheda Layer3, abilitare il criterio Web, impostare la mappa dei parametri su global e impostare l'elenco di autenticazione sul metodo di accesso aaa configurato in precedenza.

Edit WLAN

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

General **Security** Add To Policy Tags

Layer2 **Layer3** AAA

[Show Advanced Settings >>>](#)

Web Policy



Web Auth Parameter Map

global



Authentication List

ldapauth



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

Salvare facendo clic su Applica.

Comandi CLI:

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

Passaggio 8. Verificare che il SSID sia trasmesso.

Passare a Configurazione > Tag e verificare che il SSID sia incluso nel profilo dei criteri attualmente utilizzato dal SSID (il tag predefinito per una nuova configurazione se non sono ancora stati configurati i tag). Per impostazione predefinita, il tag default-policy-tag non trasmette i nuovi SSID creati fino a quando non vengono inclusi manualmente.

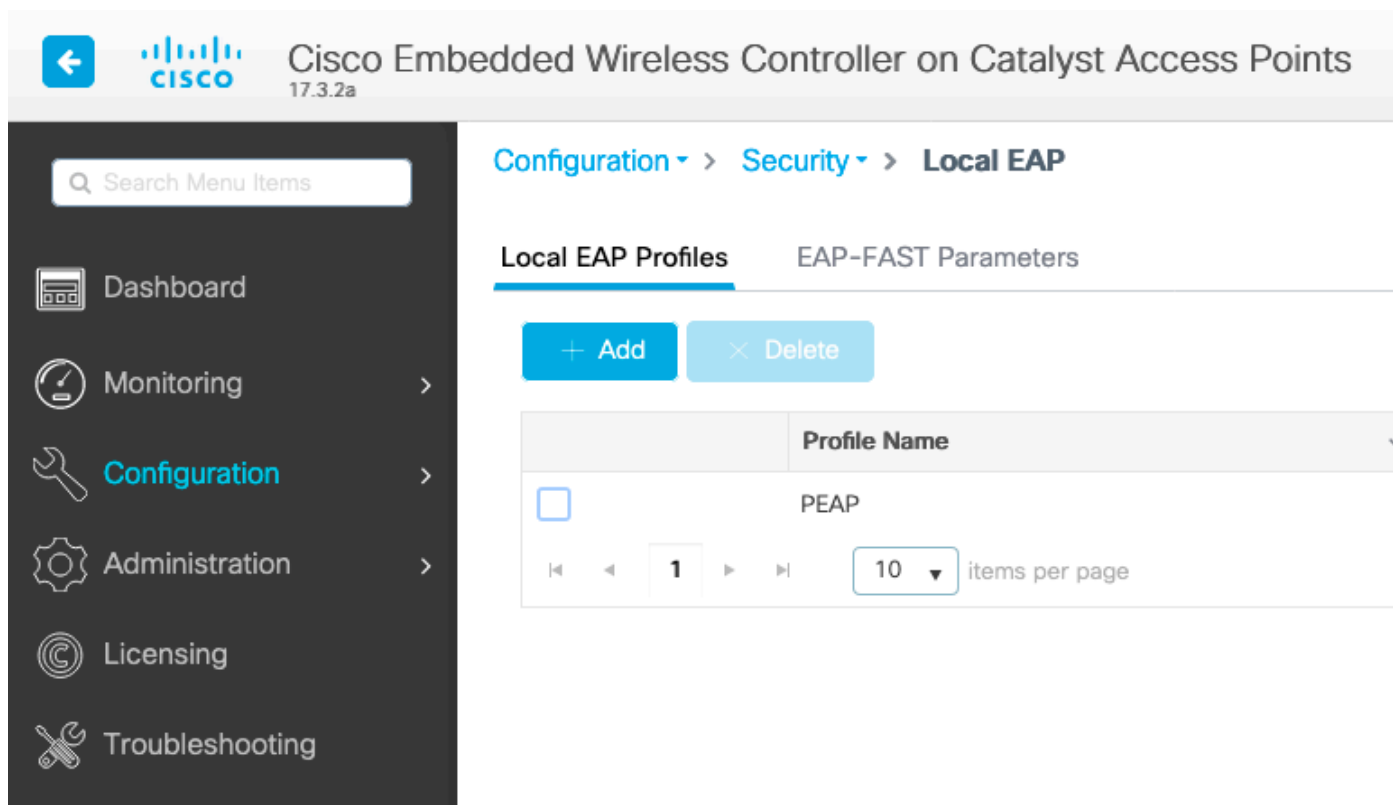
In questo articolo non viene illustrata la configurazione dei profili dei criteri e si presume che l'utente abbia familiarità con tale parte della configurazione.

Configurare LDAP con un SSID dot1x (mediante EAP locale)

La configurazione di LDAP per un SSID 802.1X su 9800 in genere richiede anche la configurazione di EAP locale. Se si dovesse utilizzare RADIUS, sarebbe il server RADIUS a stabilire una connessione con il database LDAP e ciò esula dall'ambito di questo articolo. Prima di provare questa configurazione, è consigliabile configurare Local EAP con un utente locale configurato sul WLC. Un esempio di configurazione è fornito nella sezione Riferimenti alla fine di questo articolo. Al termine, è possibile provare a spostare il database utenti verso LDAP.

Passaggio 1. Configurare un profilo EAP locale

Selezionare Configurazione > EAP locale e fare clic su +Aggiungi



The screenshot shows the Cisco Embedded Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Security > Local EAP. The 'Local EAP Profiles' tab is active, showing a table with one profile named 'PEAP'. The interface includes a search bar, a sidebar menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting, and buttons for '+ Add' and 'Delete'. The table has a checkbox and a 'Profile Name' column. The page shows 1 of 10 items per page.

	Profile Name
<input type="checkbox"/>	PEAP

Scegli un nome per il tuo profilo. Abilitare almeno PEAP e scegliere un nome di trust. Per impostazione predefinita, il WLC dispone solo di certificati autofirmati, quindi non importa quale sia quello scelto (in genere TP-self-signed-xxxx è quello più adatto a questo scopo). Tuttavia, poiché le nuove versioni del sistema operativo per gli smartphone considerano sempre meno attendibili i certificati autofirmati, è consigliabile installare un certificato protetto con firma pubblica.

Edit Local EAP Profiles

Profile Name*

PEAP

LEAP

EAP-FAST

EAP-TLS

PEAP

Trustpoint Name

TP-self-signed-3059



Comandi CLI:

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

Passaggio 2. Configurare il server LDAP.

Selezionare Configurazione > Protezione > AAA > Server/Gruppi > LDAP e fare clic su + Aggiungi.



Search Menu Items



Dashboard



Monitoring >



Configuration >



Administration >



Licensing



Troubleshooting

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Groups

Name



NAS

Scegliere un nome per il server LDAP e specificare i dettagli. Per ulteriori informazioni su ciascun campo, consultare la sezione Informazioni sui dettagli del server LDAP di questo documento.

Server Name*	<input type="text" value="AD"/>	
Server Address*	<input type="text" value="192.168.1.192"/>	<div style="border: 1px solid gray; padding: 5px; display: inline-block;">⚠ Provide a valid Server address</div>
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"/>	+

User Object Type	Remove
Person	×

Server Timeout (seconds)	<input type="text" value="0-65534"/>
Secure Mode	<input type="checkbox"/>
Trustpoint Name	<input type="text"/>

Salvare facendo clic su **Aggiorna e applica** al dispositivo.

```

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
    
```

Passaggio 3. Configurare un gruppo di server LDAP.

Selezionare Configurazione > Protezione > AAA > Server/ Gruppi > LDAP > Gruppi di server e fare clic su +ADD.

Configuration > Security > AAA

+ 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

Immettere un nome e aggiungere il server LDAP configurato nel passaggio precedente.

Name*

Idapgr

Group Type

LDAP

Available Servers

Assigned Servers

NAS

>

AD

<

>>

<<

⏪

⏩

⏴

⏵

Fare clic su Aggiorna e applicare per salvare.

Comandi CLI:

```
aaa group server ldap ldapgr
```


server AD

Passaggio 4. Configurare un metodo di autenticazione AAA.

Selezionare Configuration > Security > AAA > AAA Method List > Authentication (Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione), quindi fare clic su +Add (Aggiungi),

Configurare un metodo di autenticazione di tipo dot1x e puntarlo solo su local. Sarebbe interessante puntare al gruppo di server LDAP, ma è il WLC stesso a fungere da autenticatore 802.1X qui (anche se il database utenti è su LDAP, ma questo è il processo del metodo di autorizzazione).

Quick Setup: AAA Authentication

Method List Name*

ldapauth

Type*

dot1x



Group Type

local



Available Server Groups

radius
ldap
tacacs+
ldapgr



Assigned Server Groups



CLI:

```
aaa authentication dot1x ldapauth local
```

Passaggio 5. Configurare un metodo di autorizzazione AAA.

Selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione e fare clic su +Aggiungi.

Creare un tipo di metodo di autorizzazione per il download delle credenziali e fare in modo che punti al gruppo LDAP.

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



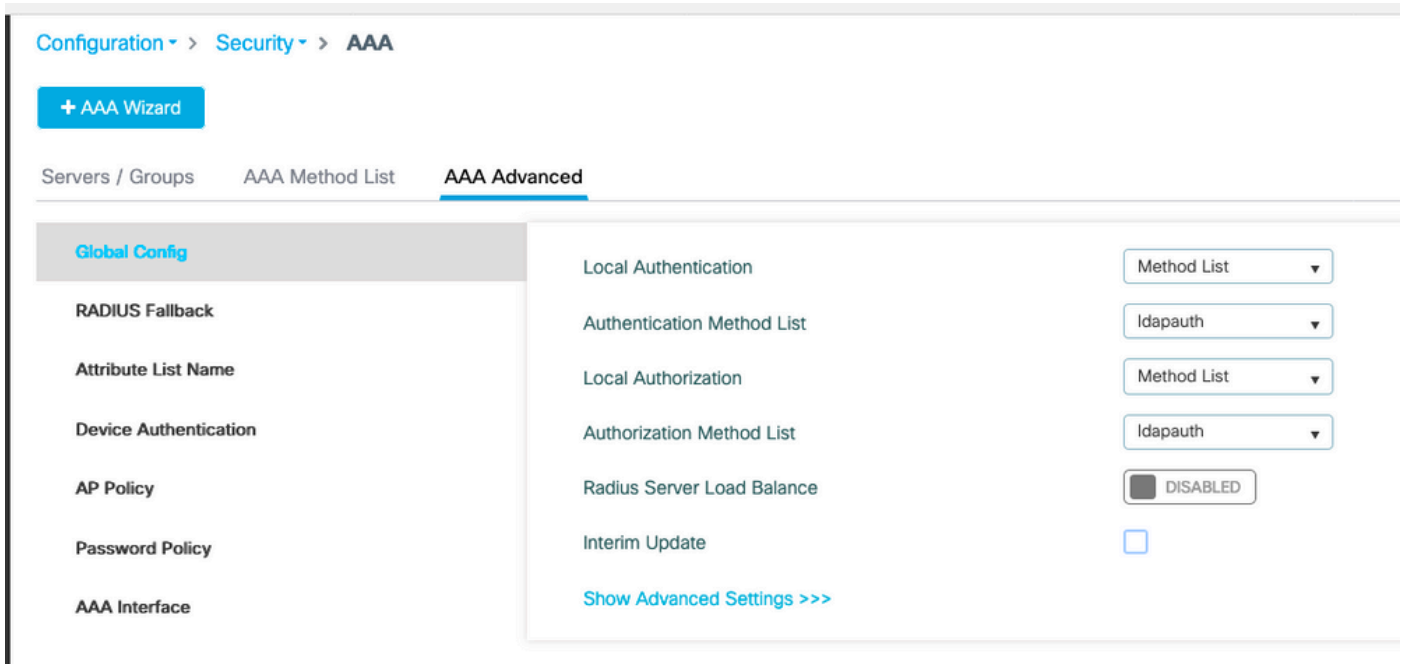
CLI:

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

Passaggio 6. Configurare i dettagli dell'autenticazione locale.

Passare a Configurazione > Sicurezza > AAA > Elenco metodi AAA > AAA avanzato.

Selezionare Elenco metodi sia per l'autenticazione che per l'autorizzazione e scegliere il metodo di autenticazione dot1x che punta localmente e il metodo di autorizzazione download credenziali che punta verso LDAP.



Comando CLI:

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

Passaggio 7. Configurare una WLAN dot1x.

Selezionare Configurazione > WLAN e fare clic su +Aggiungi.

Scegliere un profilo e un nome SSID e assicurarsi che sia abilitato.

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

Passare alla scheda Protezione Layer 2.

Scegliere WPA+WPA2 come modalità di protezione di livello 2.

Assicurarsi che WPA2 e AES siano abilitati nei parametri WPA e abilitare 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

Spostarsi sulla scheda secondaria AAA.

Selezionare il metodo di autenticazione dot1x creato in precedenza, abilitare l'autenticazione EAP locale e scegliere il profilo EAP configurato nel primo passaggio.

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	Idapauth	▼	ⓘ
Local EAP Authentication	<input checked="" type="checkbox"/>		
EAP Profile Name	PEAP	▼	

Salvare facendo clic su Applica.

Comandi CLI:

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

Passaggio 8. Verificare che la WLAN sia trasmessa.

Passare a Configurazione > Tag e verificare che il SSID sia incluso nel profilo dei criteri attualmente utilizzato dal SSID (il tag predefinito per una nuova configurazione se non sono ancora stati configurati i tag). Per impostazione predefinita, il tag default-policy-tag non trasmette i nuovi SSID creati fino a quando non vengono inclusi manualmente.

In questo articolo non viene illustrata la configurazione dei profili dei criteri e si presume che l'utente abbia familiarità con tale parte della configurazione.

Se si utilizza Active Directory, è necessario configurare il server AD per l'invio dell'attributo userPassword. Questo attributo deve essere inviato al WLC. Ciò è dovuto al fatto che la verifica viene eseguita dal WLC, non dal server AD. È inoltre possibile che si verifichino problemi di autenticazione con il metodo PEAP-mschapv2, in quanto la password non viene mai inviata in testo non crittografato e pertanto non può essere verificata con il database LDAP. Solo il metodo PEAP-GTC funzionerebbe con alcuni database LDAP.

Informazioni sui dettagli del server LDAP

Informazioni sui campi nell'interfaccia utente Web 9800

Di seguito è riportato un esempio di Active Directory di base che funge da server LDAP configurato sullo switch 9800.

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><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"/>					

Il nome e l'indirizzo IP possono essere facilmente comprensibili.

Porta: 389 è la porta predefinita per LDAP, ma il server può utilizzarne un'altra.

Binding semplice: è molto raro disporre di un database LDAP che supporti il binding non autenticato (ciò significa che chiunque può eseguire una ricerca LDAP senza alcun modulo di autenticazione). L'autenticazione semplice autenticata è il tipo di autenticazione più comune e ciò che Active Directory consente per impostazione predefinita. È possibile immettere il nome e la password di un account amministratore per eseguire ricerche nel database utenti da tale posizione.

Associa nome utente: è necessario puntare a un nome utente con privilegi di amministratore in Active Directory. AD accetta il formato "user@domain", mentre molti altri database LDAP prevedono per il nome utente un formato "CN=xxx,DC=xxx". Un esempio con un database LDAP diverso da AD viene fornito più avanti in questo articolo.

Password di binding: immettere la password immessa in precedenza dal nome utente amministratore.

DN base utente: immettere qui la radice di ricerca, ovvero la posizione nella struttura LDAP in cui vengono avviate le ricerche. In questo esempio, tutti gli utenti sono inclusi nel gruppo "Utenti", il cui DN è "CN=Users,DC=lab,DC=com" (poiché il dominio LDAP di esempio è lab.com). Un esempio di come trovare questo DN della base utente è fornito più avanti in questa sezione.

Attributo utente: può essere lasciato vuoto o fare riferimento a una mappa di attributi LDAP che indica quale campo LDAP viene conteggiato come nome utente per il database LDAP. Tuttavia, a causa dell'ID bug Cisco [CSCv11813](#), il WLC tenta un'autenticazione con il campo CN in ogni caso.

Tipo di oggetto utente: determina il tipo di oggetti considerati utenti. In genere si tratta di Persona. Potrebbe trattarsi di Computer se si dispone di un database di Active Directory e si autenticano gli account computer, ma anche in questo caso il protocollo LDAP consente numerose personalizzazioni.

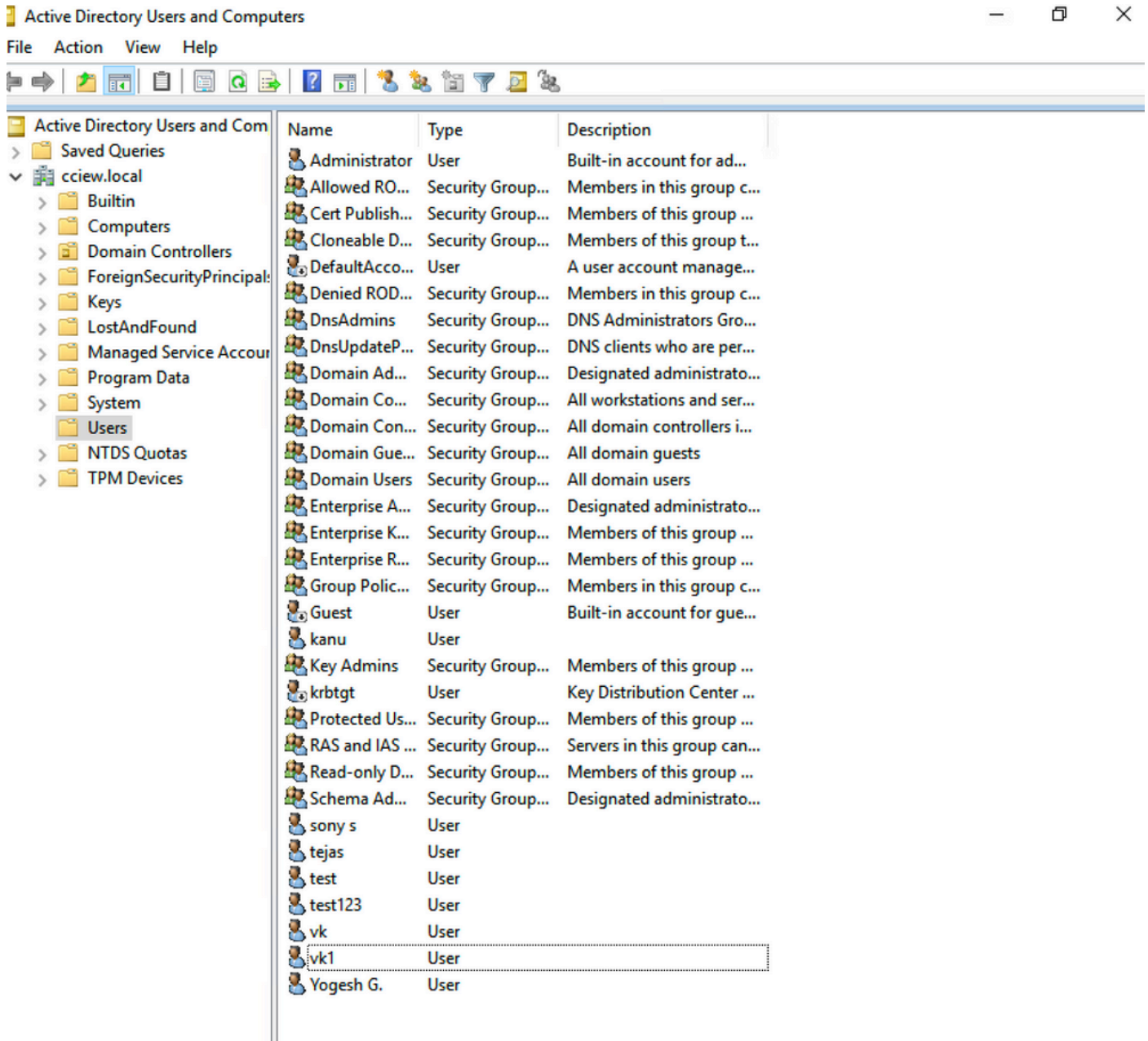
La modalità protetta consente di abilitare il protocollo LDAP sicuro su TLS e richiede la selezione di un Trustpoint su 9800 per l'utilizzo di un certificato per la crittografia TLS.

Autenticazione LDAP 802.1x con attributo sAMAaccountName.

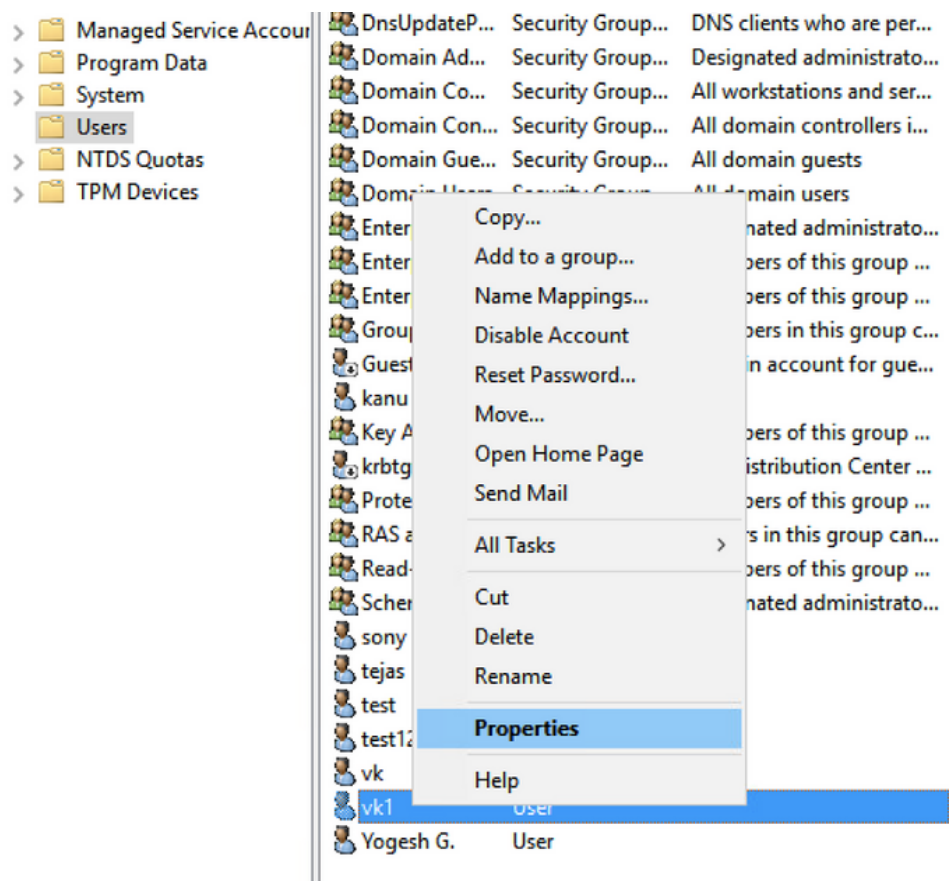
Questo miglioramento è stato introdotto nella versione 17.6.1.

Configurare l'attributo userPassword per l'utente.

Passaggio 1. Nel server Windows passare a Utenti e computer di Active Directory.



Passaggio 2. Fare clic con il pulsante destro del mouse sul nome utente corrispondente e selezionare Proprietà.



Passaggio 3. Selezionare editor attributi nella finestra delle proprietà.

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

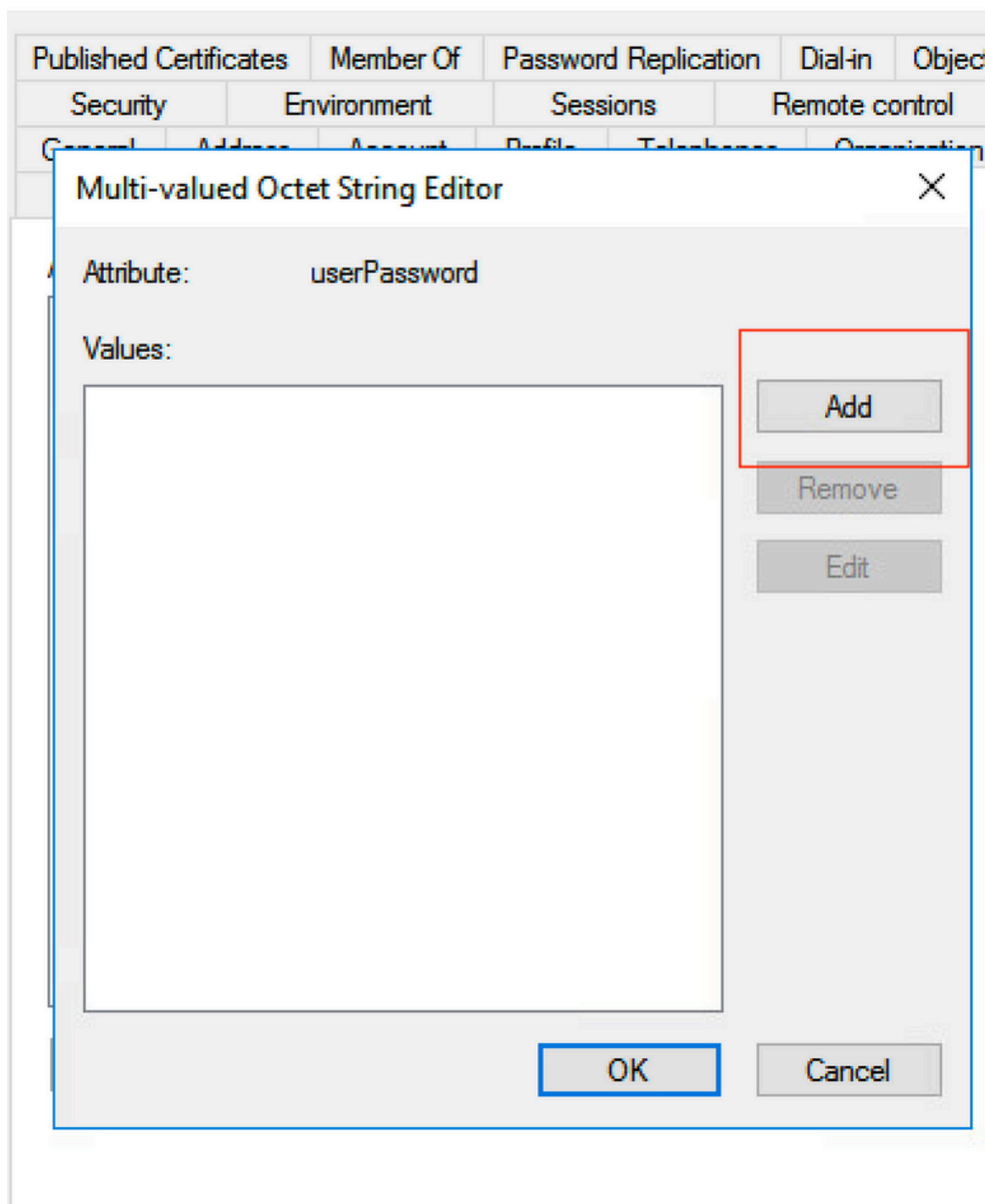
Cancel

Apply

Help

Passaggio 4. Configurare l'attributo userPassword. Questa è la password dell'utente, che deve essere configurata in valore esadecimale.

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 ✖

Octet String Attribute Editor ✖

Attribute: userPassword

Value format: Hexadecimal ▾

Value:
43 69 73 63 6F 31 32 33

Clear OK Cancel

OK Cancel Apply Help

Fare clic su OK, verificare che la password visualizzata sia corretta

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:

Cisco123

Add

Remove

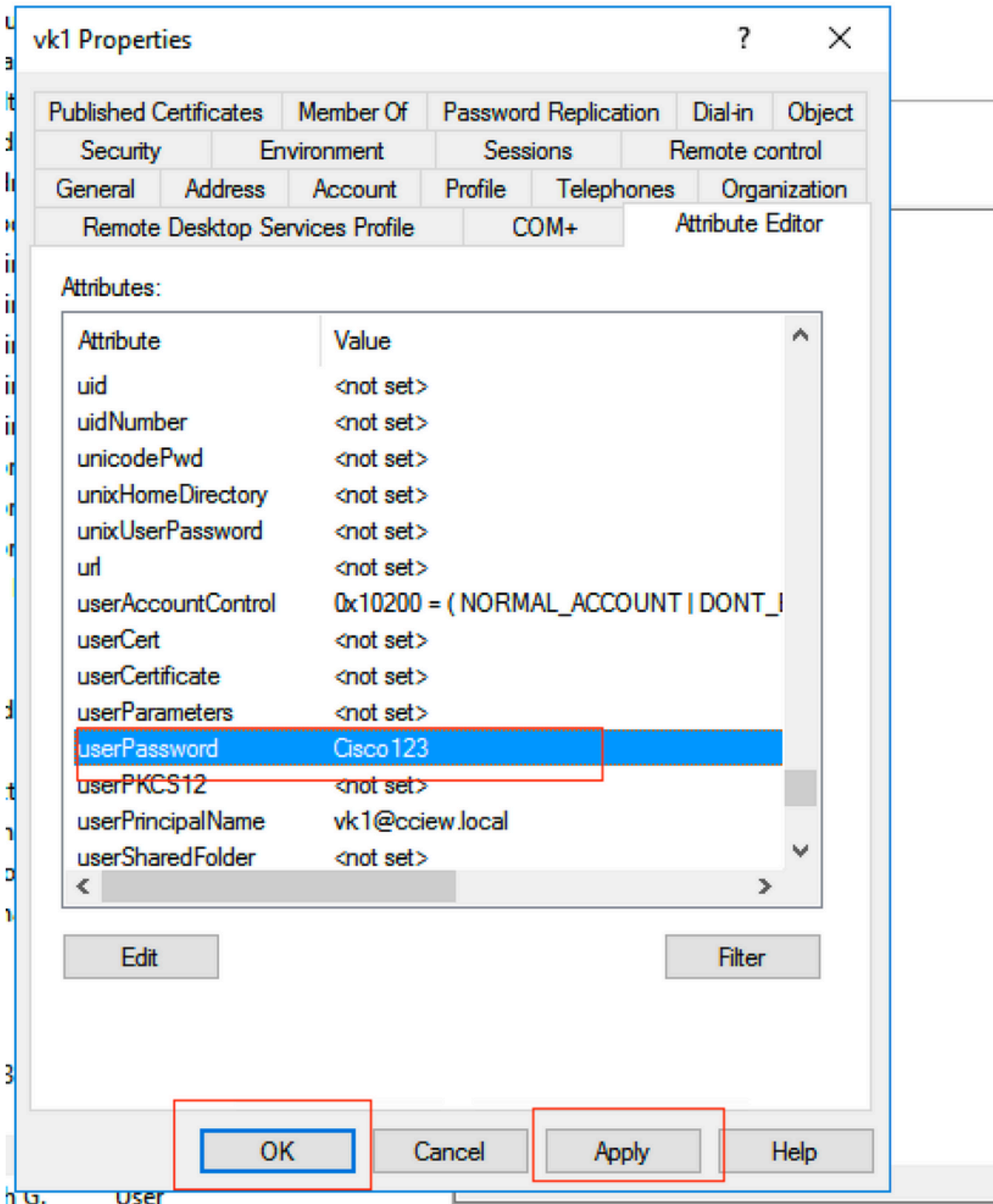
Edit

OK

Cancel

OK Cancel Apply Help

Passaggio 5. Fare clic su Applica, quindi su OK.



Passaggio 6. Verificare il valore dell'attributo sAMAccountName per l'utente e il nome utente per l'autenticazione.

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

Configurazione WLC

Passaggio 1. Creare la MAPPA degli attributi LDAP.

Passaggio 2. Configurare l'attributo sAMAccountName e digitare come nome utente.

Passaggio 3. Scegliere l'attributo MAP creato nella configurazione del server LDAP.

ldap attribute-map VK

```
map type sAMAccountName username
```

ldap server ldap

```
ipv4 10.106.38.195
```

```
attribute map VK
```

```
bind authenticate root-dn vk1 password 7 00271A1507545A545C
```

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

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

Verifica dall'interfaccia Web

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 shows the AAA configuration page with tabs for Servers / Groups, AAA Method List, and AAA Advanced. The Servers / Groups tab is active, and the Servers sub-tab is selected. A table lists the configured servers:

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 dropdown menu for 'Items per page' set to 10. The page number '1 - 1 of 1' is visible in the bottom right corner.

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)

Verifica

Per verificare la configurazione, controllare i comandi CLI con quelli descritti in questo articolo.

I database LDAP in genere non forniscono registri di autenticazione, pertanto può essere difficile sapere cosa sta succedendo. Visitare la sezione Risoluzione dei problemi di questo articolo per vedere come eseguire l'acquisizione di tracce e sniffer per verificare se è stata stabilita una connessione al database LDAP o meno.

Risoluzione dei problemi

Per risolvere il problema, è consigliabile suddividere l'operazione in due parti. La prima parte è la convalida della parte EAP locale. Il secondo consiste nel verificare che il 9800 comunichi correttamente con il server LDAP.

Come verificare il processo di autenticazione sul controller

È possibile raccogliere una traccia radioattiva per ottenere i debug della connessione client.

È sufficiente selezionare Risoluzione dei problemi > Traccia radioattiva. Aggiungere l'indirizzo MAC del client (fare attenzione che il client possa utilizzare un MAC casuale e non il proprio MAC, è possibile verificarlo nel profilo SSID sul dispositivo client stesso) e premere start.

Una volta riprodotto il tentativo di connessione, è possibile fare clic su Generate e ottenere i log

per gli ultimi X minuti. Accertarsi di fare clic su interno in quanto alcune linee di registro LDAP non vengono visualizzate se non viene attivata.

Di seguito è riportato un esempio di traccia radioattiva di un client che ha completato l'autenticazione su un SSID di autenticazione Web. Alcune parti ridondanti sono state rimosse per maggiore chiarezza:

```
2021/01/19 21:57:55.890953 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (note): MAC: 2e1f.3a65.9c09 Assoc
2021/01/19 21:57:55.891049 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09 Recv
2021/01/19 21:57:55.891282 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 C
2021/01/19 21:57:55.891674 {wncd_x_R0-0}{1}: [dot11-validate] [9347]: (info): MAC: 2e1f.3a65.9c09 Wi-Fi
2021/01/19 21:57:55.892114 {wncd_x_R0-0}{1}: [dot11] [9347]: (debug): MAC: 2e1f.3a65.9c09 dot11 send a
2021/01/19 21:57:55.892182 {wncd_x_R0-0}{1}: [dot11-frame] [9347]: (info): MAC: 2e1f.3a65.9c09 Wi-Fi di
2021/01/19 21:57:55.892248 {wncd_x_R0-0}{1}: [dot11] [9347]: (info): MAC: 2e1f.3a65.9c09 dot11 send as
2021/01/19 21:57:55.892467 {wncd_x_R0-0}{1}: [dot11] [9347]: (note): MAC: 2e1f.3a65.9c09 Association s
2021/01/19 21:57:55.892497 {wncd_x_R0-0}{1}: [dot11] [9347]: (info): MAC: 2e1f.3a65.9c09 DOT11 state t
2021/01/19 21:57:55.892616 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09 Sta
2021/01/19 21:57:55.892730 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09 Sta
2021/01/19 21:57:55.892783 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 C
2021/01/19 21:57:55.892896 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 L2 Auth
2021/01/19 21:57:55.893115 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893154 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893205 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:57:55.893211 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:57:55.893254 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
2021/01/19 21:57:55.893461 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:unknown] auth m
2021/01/19 21:57:55.893532 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893603 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893649 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893679 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.893731 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894285 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894299 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894551 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894587 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:57:55.894593 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:57:55.894827 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.894858 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:57:55.894862 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:57:55.895918 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [9347]: (info): [0000.0000.0000:u
2021/01/19 21:57:55.896094 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.896807 {wncd_x_R0-0}{1}: [webauth-sm] [9347]: (info): [ 0.0.0.0]Starting Web
2021/01/19 21:57:55.897106 {wncd_x_R0-0}{1}: [webauth-ac1] [9347]: (info): capwap_90000004[2e1f.3a65.9c
2021/01/19 21:57:55.897790 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info): [0000.0000.0000:unknown] UR
2021/01/19 21:57:55.898813 {wncd_x_R0-0}{1}: [webauth-ac1] [9347]: (info): capwap_90000004[2e1f.3a65.9c
2021/01/19 21:57:55.899406 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info): [0000.0000.0000:unknown] UR
2021/01/19 21:57:55.903552 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
2021/01/19 21:57:55.903575 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [9347]: (note): Authentication Success. R
2021/01/19 21:57:55.903592 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
2021/01/19 21:57:55.903709 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
2021/01/19 21:57:55.903774 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.903858 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.903924 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.904005 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09 L2
2021/01/19 21:57:55.904173 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (note): MAC: 2e1f.3a65.9c09 Mobi
2021/01/19 21:57:55.904181 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 C
2021/01/19 21:57:55.904245 {wncd_x_R0-0}{1}: [mm-transition] [9347]: (info): MAC: 2e1f.3a65.9c09 MMIF
2021/01/19 21:57:55.904410 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Invalid t
```

2021/01/19 21:57:55.904777 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2e1f.3a65.9c09 Received
2021/01/19 21:57:55.904955 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2e1f.3a65.9c09 Add MCC
2021/01/19 21:57:55.905072 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 0000.0000.0000 Sending
2021/01/19 21:57:55.905157 {wncd_x_R0-0}{1}: [mm-client] [9347]: (debug): MAC: 2e1f.3a65.9c09 Received
2021/01/19 21:57:55.905267 {wncd_x_R0-0}{1}: [mm-transition] [9347]: (info): MAC: 2e1f.3a65.9c09 MMIF
2021/01/19 21:57:55.905283 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Roam type
2021/01/19 21:57:55.905317 {wncd_x_R0-0}{1}: [mm-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Mobility
2021/01/19 21:57:55.905515 {wncd_x_R0-0}{1}: [mm-client] [9347]: (note): MAC: 2e1f.3a65.9c09 Mobility
2021/01/19 21:57:55.905570 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09 Pro
2021/01/19 21:57:55.906210 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Cli
2021/01/19 21:57:55.906369 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 No
2021/01/19 21:57:55.906399 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 No
2021/01/19 21:57:55.906486 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 ADD MOB
2021/01/19 21:57:55.906613 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 C
2021/01/19 21:57:55.907326 {wncd_x_R0-0}{1}: [dot11] [9347]: (note): MAC: 2e1f.3a65.9c09 Client datapa
2021/01/19 21:57:55.907544 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Cli
2021/01/19 21:57:55.907594 {wncd_x_R0-0}{1}: [avc-afc] [9347]: (debug): AVC enabled for client 2e1f.3a6
2021/01/19 21:57:55.907701 {wncd_x_R0-0}{1}: [dpath_svc] [9347]: (note): MAC: 2e1f.3a65.9c09 Client da
2021/01/19 21:57:55.908229 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 C
2021/01/19 21:57:55.908704 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 IP-1
2021/01/19 21:57:55.918694 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
2021/01/19 21:57:55.922254 {wncd_x_R0-0}{1}: [dot11k] [9347]: (info): MAC: 2e1f.3a65.9c09 Neighbor AP
2021/01/19 21:57:55.922260 {wncd_x_R0-0}{1}: [dot11k] [9347]: (info): MAC: 2e1f.3a65.9c09 Neighbor AP
2021/01/19 21:57:55.962883 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (note): MAC: 2e1f.3a65.9c09 Clie
2021/01/19 21:57:55.963827 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 Clie
2021/01/19 21:57:55.964481 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.965176 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 IP-1
2021/01/19 21:57:55.965550 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:57:55.966127 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 IP-1
2021/01/19 21:57:55.966328 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09 Rec
2021/01/19 21:57:55.966413 {wncd_x_R0-0}{1}: [client-orch-sm] [9347]: (debug): MAC: 2e1f.3a65.9c09 Tri
2021/01/19 21:57:55.966424 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 C
2021/01/19 21:57:55.967404 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 L3 Auth
2021/01/19 21:57:55.967433 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
2021/01/19 21:57:55.968312 {wncd_x_R0-0}{1}: [sisf-packet] [9347]: (debug): RX: ARP from interface capw
2021/01/19 21:57:55.968519 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 iple
2021/01/19 21:57:55.968522 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 Clie
2021/01/19 21:57:55.968966 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 IP-1
2021/01/19 21:57:57.762648 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 iple
2021/01/19 21:57:57.762650 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 Clie
2021/01/19 21:57:57.763032 {wncd_x_R0-0}{1}: [client-iplearn] [9347]: (info): MAC: 2e1f.3a65.9c09 IP-1
2021/01/19 21:58:00.992597 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:00.992617 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:00.992669 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:00.992694 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:00.993558 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:00.993637 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:00.993645 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:00.996320 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:00.996508 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:00.996524 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:05.808144 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.808226 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.808251 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.860465 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.860483 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.860534 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:05.860559 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.628209 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.628228 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.628287 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.628316 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.

2021/01/19 21:58:06.628832 {wncd_x_R0-0}{1}: [webauth-page] [9347]: (info): capwap_90000004[2e1f.3a65.9
2021/01/19 21:58:06.629613 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.629699 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:06.629709 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:06.633058 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.633219 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.633231 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.719502 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.719521 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.719591 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.719646 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.720038 {wncd_x_R0-0}{1}: [webauth-error] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.720623 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.720707 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:06.720716 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:06.724036 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.746127 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.746145 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.746197 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.746225 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.746612 {wncd_x_R0-0}{1}: [webauth-error] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:06.747105 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:06.747187 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:06.747197 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:06.750598 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:15.902342 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:15.902360 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:15.902410 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:15.902435 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:15.903173 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:15.903252 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [2e1f.3a65.9c09:c
2021/01/19 21:58:15.903261 {wncd_x_R0-0}{1}: [auth-mgr-feat_template] [9347]: (info): [0000.0000.0000:c
2021/01/19 21:58:15.905950 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:15.906112 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:15.906125 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:16.357093 {wncd_x_R0-0}{1}: [webauth-httpd] [9347]: (info): capwap_90000004[2e1f.3a65.
2021/01/19 21:58:16.357443 {wncd_x_R0-0}{1}: [sadb-attr] [9347]: (info): Removing ipv6 addresses from t
2021/01/19 21:58:16.357674 {wncd_x_R0-0}{1}: [caaa-authen] [9347]: (info): [CAAA:AUTHEN:b7000080] DEBUG
2021/01/19 21:58:16.374292 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:16.374412 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [9347]: (note): Authentication Success. R
2021/01/19 21:58:16.374442 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
2021/01/19 21:58:16.374568 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info):
<< username 0 "Nico">>
2021/01/19 21:58:16.374574 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info):
<< sam-account-name 0 "Nico">>
2021/01/19 21:58:16.374584 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info):
<< method 0 1 [webauth]>>
2021/01/19 21:58:16.374592 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info):
<< clid-mac-addr 0 2e 1f 3a 65 9c 09 >>
2021/01/19 21:58:16.374597 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info):
<< intf-id 0 2415919108 (0x90000004)>>
2021/01/19 21:58:16.374690 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:16.374797 {wncd_x_R0-0}{1}: [auth-mgr] [9347]: (info): [2e1f.3a65.9c09:capwap_90000004
2021/01/19 21:58:16.375294 {wncd_x_R0-0}{1}: [webauth-ac] [9347]: (info): capwap_90000004[2e1f.3a65.9c
2021/01/19 21:58:16.376120 {wncd_x_R0-0}{1}: [epm-redirect] [9347]: (info): [0000.0000.0000:unknown] UR
2021/01/19 21:58:16.377322 {wncd_x_R0-0}{1}: [webauth-page] [9347]: (info): capwap_90000004[2e1f.3a65.9
2021/01/19 21:58:16.378405 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 L3 Auth
2021/01/19 21:58:16.378426 {wncd_x_R0-0}{1}: [client-auth] [9347]: (info): MAC: 2e1f.3a65.9c09 Client
2021/01/19 21:58:16.379181 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Cli
2021/01/19 21:58:16.379323 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 No
2021/01/19 21:58:16.379358 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 No
2021/01/19 21:58:16.379442 {wncd_x_R0-0}{1}: [client-auth] [9347]: (note): MAC: 2e1f.3a65.9c09 ADD MOB

```

2021/01/19 21:58:16.380547 {wncd_x_R0-0}{1}: [errmsg] [9347]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_T
2021/01/19 21:58:16.380729 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute :bsn-vl
2021/01/19 21:58:16.380736 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute :
2021/01/19 21:58:16.380812 {wncd_x_R0-0}{1}: [aaa-attr-inf] [9347]: (info): [ Applied attribute : ur
2021/01/19 21:58:16.380969 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Cli
2021/01/19 21:58:16.381033 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [9347]: (debug): Managed client RUN sta
2021/01/19 21:58:16.381152 {wncd_x_R0-0}{1}: [client-orch-state] [9347]: (note): MAC: 2e1f.3a65.9c09 C
2021/01/19 21:58:16.385252 {wncd_x_R0-0}{1}: [ewlc-qos-client] [9347]: (info): MAC: 2e1f.3a65.9c09 Cli
2021/01/19 21:58:16.385321 {wncd_x_R0-0}{1}: [avc-afc] [9347]: (debug): AVC enabled for client 2e1f.3a6

```

Come verificare la connettività da 9800 a LDAP

È possibile eseguire un'acquisizione incorporata nel router 9800 per verificare il traffico diretto al server LDAP.

Per acquisire un pacchetto dal WLC, selezionare Risoluzione dei problemi > Packet Capture e fare clic su +Add. Scegliere la porta uplink e avviare la cattura.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main content area is titled 'Troubleshooting > Packet Capture'. There are two buttons: '+ Add' and 'Delete'. Below these is a table with two columns: 'Capture Name' and 'Interface'. The table is currently empty. There are also navigation icons and a '0' in a box, and a dropdown menu set to '10 items per page'.

Di seguito è riportato un esempio di autenticazione riuscita per l'utente Nico.

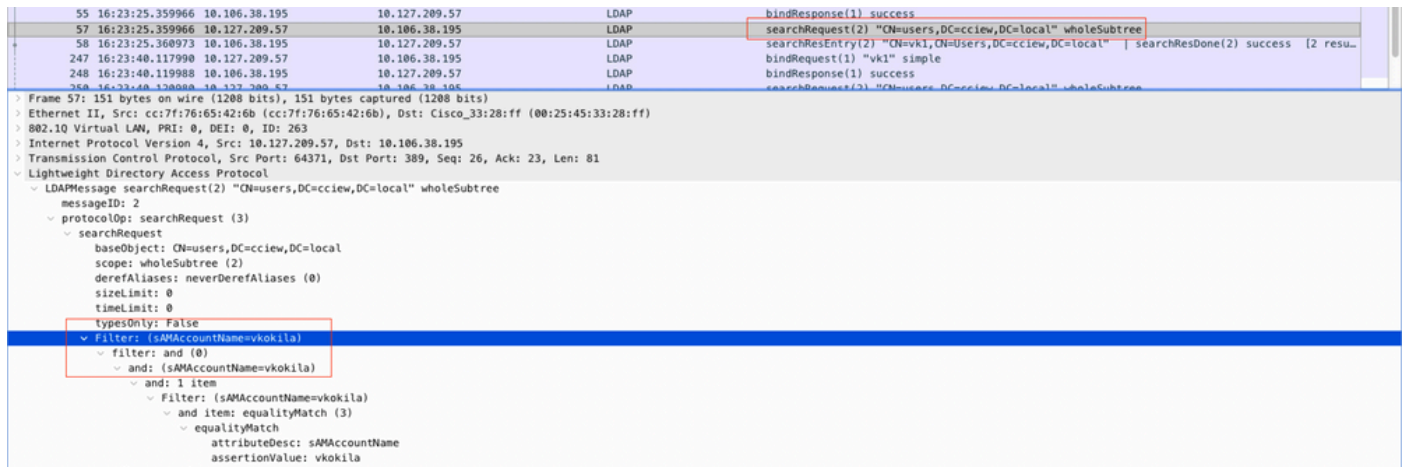
o.	Time	Source	Destination	Protocol	Length	La Info
8696	22:58:16.412748	192.168.1.15	192.168.1.192	LDAP	108	bindRequest(1) "Administrator@lab.com" simple
8697	22:58:16.414425	192.168.1.192	192.168.1.15	LDAP	88	bindResponse(1) success
8699	22:58:16.419645	192.168.1.15	192.168.1.192	LDAP	128	searchRequest(2)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

I primi 2 pacchetti rappresentano il binding WLC al database LDAP, ossia il WLC che esegue l'autenticazione al database con l'utente admin (per poter eseguire una ricerca).

Questi 2 pacchetti LDAP rappresentano il WLC che esegue una ricerca nel DN di base (qui CN=Users,DC=lab,DC=com). L'interno del pacchetto contiene un filtro per il nome utente (qui Nico). Il database LDAP restituisce correttamente gli attributi utente.

Gli ultimi 2 pacchetti rappresentano il WLC che tenta di autenticarsi con quella password utente per verificare se la password è quella giusta.

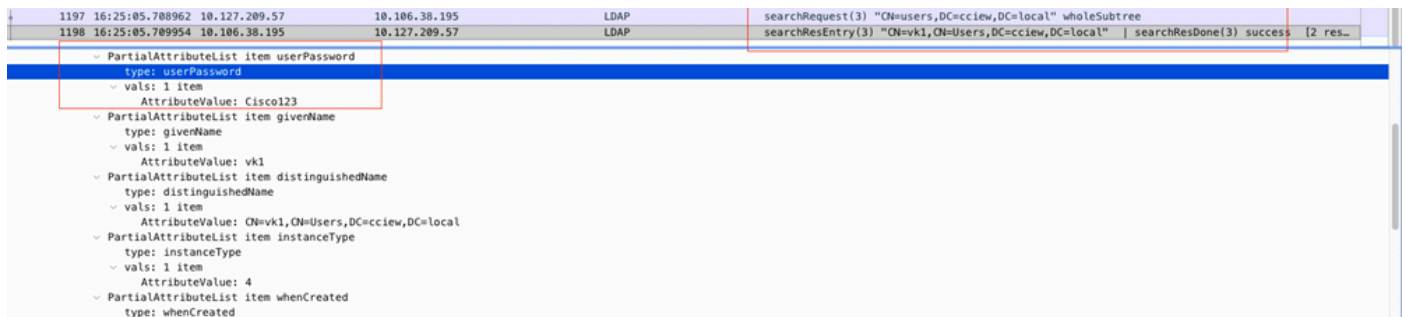
1. Raccogli EPC e verifica se sAMAccountName viene applicato come filtro:



Se il filtro mostra cn e sAMAccountName è utilizzato come nome utente, l'autenticazione non riesce.

Riconfigurare l'attributo della mappa ldap dalla cli del WLC.

2. Assicurarsi che il server restituisca userPassword in testo non crittografato, altrimenti l'autenticazione non riesce.



3. Utilizzare lo strumento ldap.exe nel server per convalidare le informazioni sul DN di base.



FileZilla Client



Best match



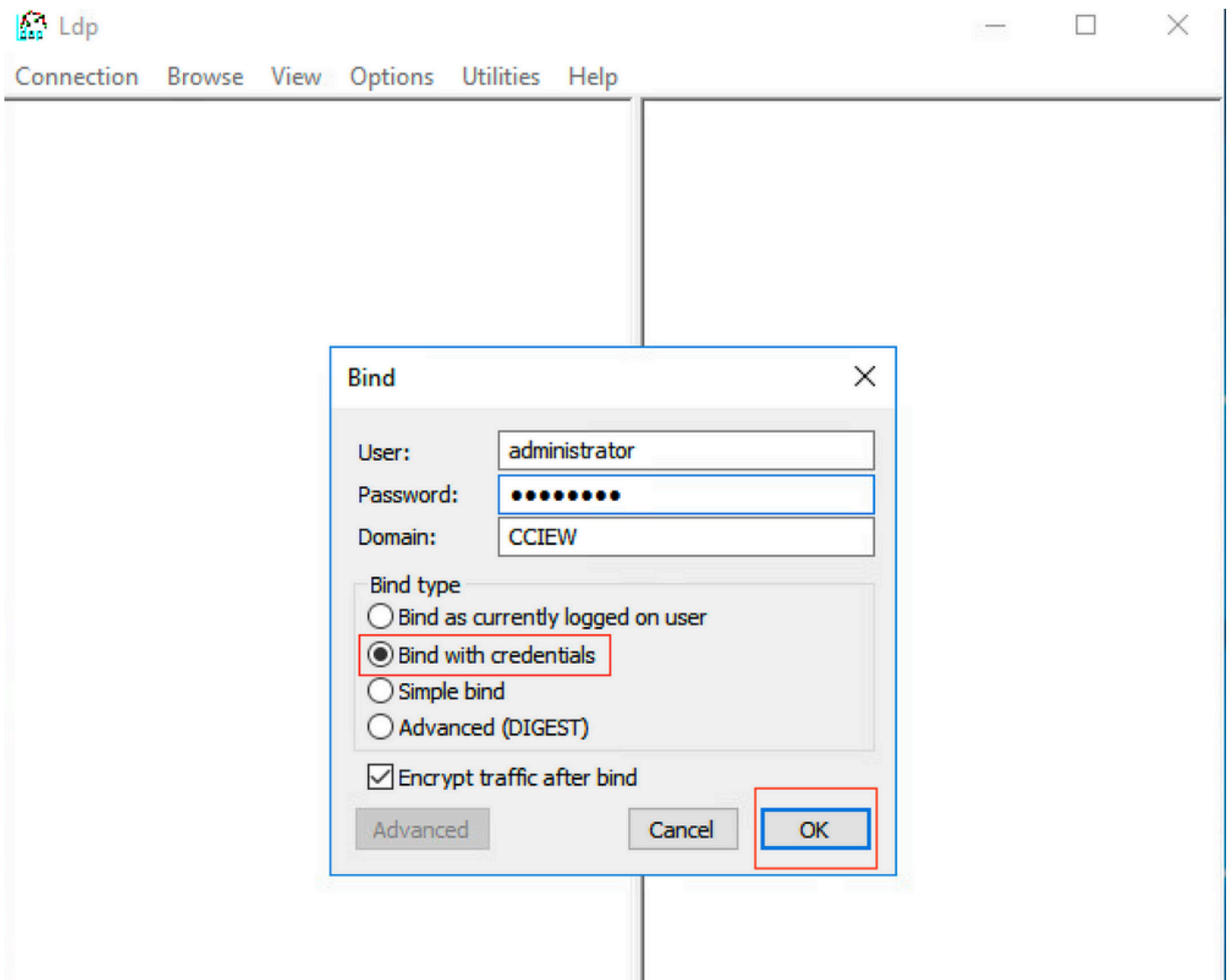
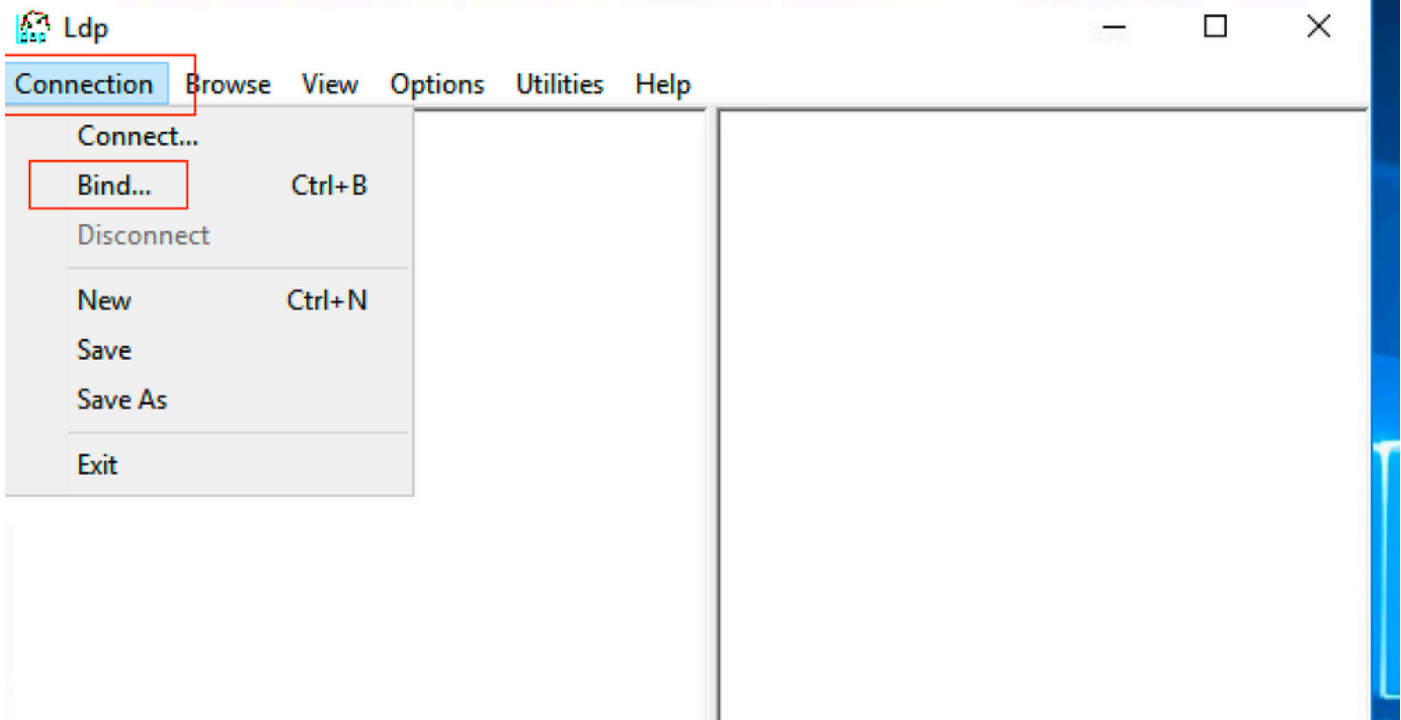
Idp

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;
MaxReceiveBuffer;
MaxDatagramRecv;
MaxReceiveBuffer;
MaxPercentDirSyncRequests;
MaxDatagramRecv;
MaxReceiveBuffer;
InitRecvTimeout; MaxConnections;
MaxConnIdleTime; MaxRange;
maxValueRangeTransitive; ThreadMemoryLimit;
SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;

Tree View

BaseDN:

Cancel

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. Controllare le statistiche del server e l'attributo MAP.

```
<#root>
```

```
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

Informazioni correlate

- [Esempio di configurazione di EAP locale su 9800](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).