# Configurazione del WLC con autenticazione LDAP per le WLAN 802.1x e Web-Auth

## Sommario



## Introduzione

In questo documento viene descritta la procedura per configurare un WLC di AireOS in modo da autenticare i client con un server LDAP come database utenti.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Server Microsoft Windows
- Active Directory

### Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Cisco WLC 8.2.10.0

- Microsoft Windows Server 2012 R2

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.

# Premesse

## Contesto tecnico

- LDAP è un protocollo utilizzato per accedere ai server delle directory.
- I server di directory sono database gerarchici orientati agli oggetti.
- Gli oggetti sono organizzati in contenitori, ad esempio Unità organizzative (OU, Organizational Units), Gruppi o Contenitori Microsoft predefiniti, come CN=Users.
- La parte più difficile di questa configurazione è configurare correttamente i parametri del server LDAP sul WLC.

Per informazioni più dettagliate su questi concetti, fare riferimento alla sezione Introduzione di Come configurare Wireless LAN Controller (WLC) per l'autenticazione LDAP (Lightweight Directory Access Protocol).

## Domande frequenti

- Quale nome utente deve essere utilizzato per il binding al server LDAP?

Esistono due modi per eseguire l'associazione a un server LDAP: Anonimo o Autenticato (fare riferimento a per comprendere la differenza tra entrambi i metodi).

Il nome utente associato deve disporre dei privilegi di amministratore per poter eseguire query per altri nomi utente/password.

- Se autenticato: il nome utente di binding si trova nello stesso contenitore di tutti gli utenti?

**No:** utilizza l'intero percorso. Ad esempio:

**CN=Administrator,CN=Domain Admins,CN=Users,DC=labm,DC=cisco,DC=com**

**Sì:** utilizzare solo il nome utente. Ad esempio:

**Amministratore**

- Cosa succede se gli utenti si trovano in contenitori diversi? Tutti gli utenti LDAP wireless interessati devono trovarsi nello stesso contenitore?

No, è possibile specificare un DN di base che includa tutti i contenitori necessari.

- Quali attributi deve cercare il WLC?

Il WLC corrisponde all'attributo utente e al tipo di oggetto specificati.

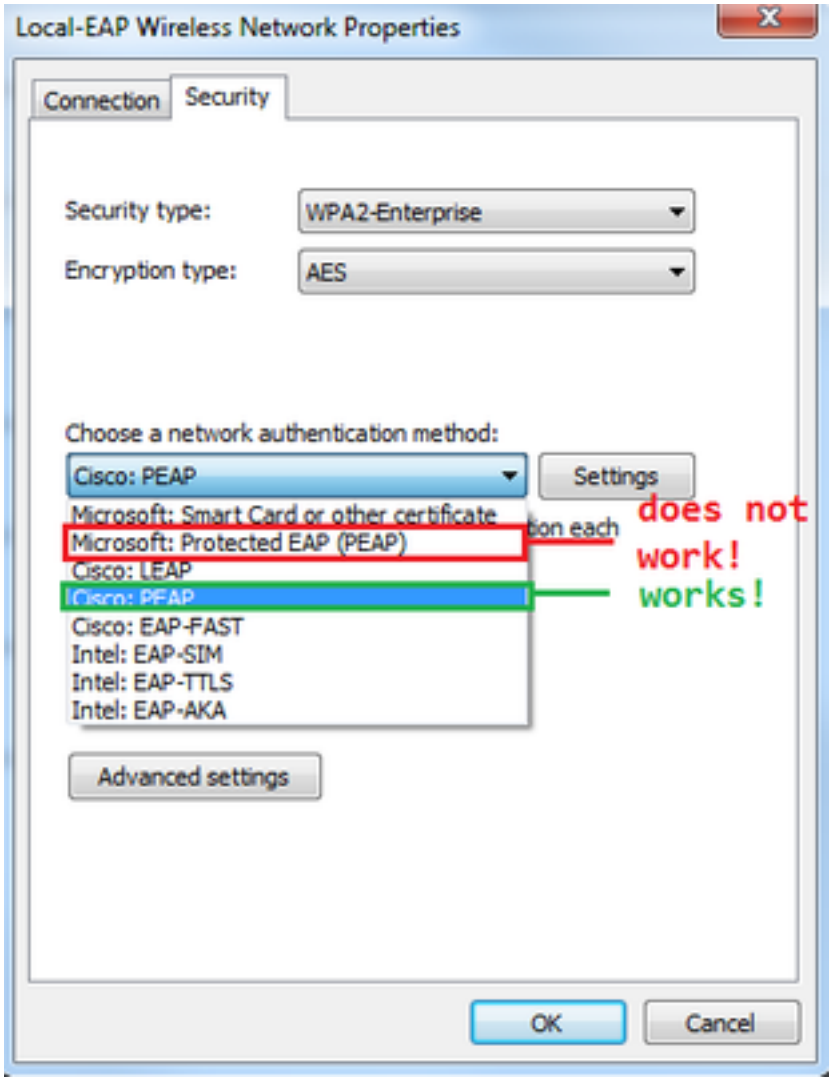
**Nota**: **sAMAccountName** fa distinzione tra maiuscole e minuscole, ma person non lo fa.

Pertanto, **sAMAccountName=RICARDO** e **sAMAccountName=ricardo** sono gli stessi e funzionano, a differenza di **samaccountname=RICARDO** e **samaccountname=ricardo**.

- Quali metodi EAP (Extensible Authentication Protocol) è possibile utilizzare?

Solo EAP-FAST, PEAP-GTC e EAP-TLS. I supplicant predefiniti Android, iOS e MacOS funzionano con PEAP (Protected Extensible Authentication Protocol).

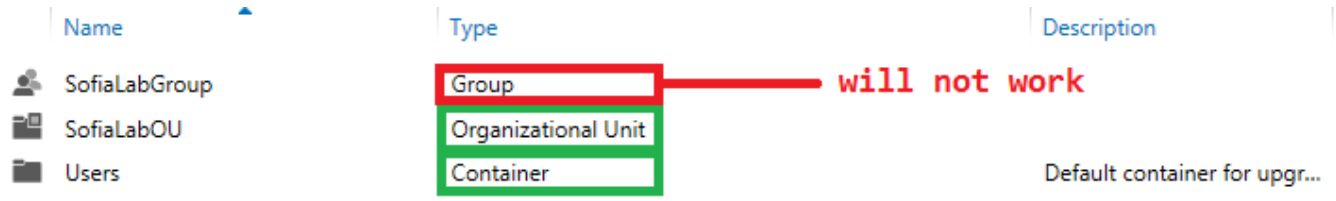
Per Windows, è necessario usare Anyconnect Network Access Manager (NAM) o il supplicant predefinito di Windows con Cisco:PEAP sulle schede wireless supportate, come mostrato nell'immagine.




**Nota**: i plug-in EAP di Cisco per Windows includono una versione di Open Secure Socket Layer (OpenSSL 0.9.8k) su cui ha effetto l'ID bug Cisco CSCva09670, Cisco non prevede di rilasciare altre versioni dei plug-in EAP per Windows e consiglia ai clienti di utilizzare AnyConnect Secure Mobility Client.

- Perché il WLC non trova gli utenti?

Impossibile autenticare gli utenti all'interno di un gruppo. Devono trovarsi all'interno di un contenitore predefinito (CN, Default Container) o di un'unità organizzativa (OU, Organizational Unit), come mostrato nell'immagine.




# Configurazione

Esistono diversi scenari in cui è possibile utilizzare un server LDAP, sia con l'autenticazione 802.1x sia con l'autenticazione Web.

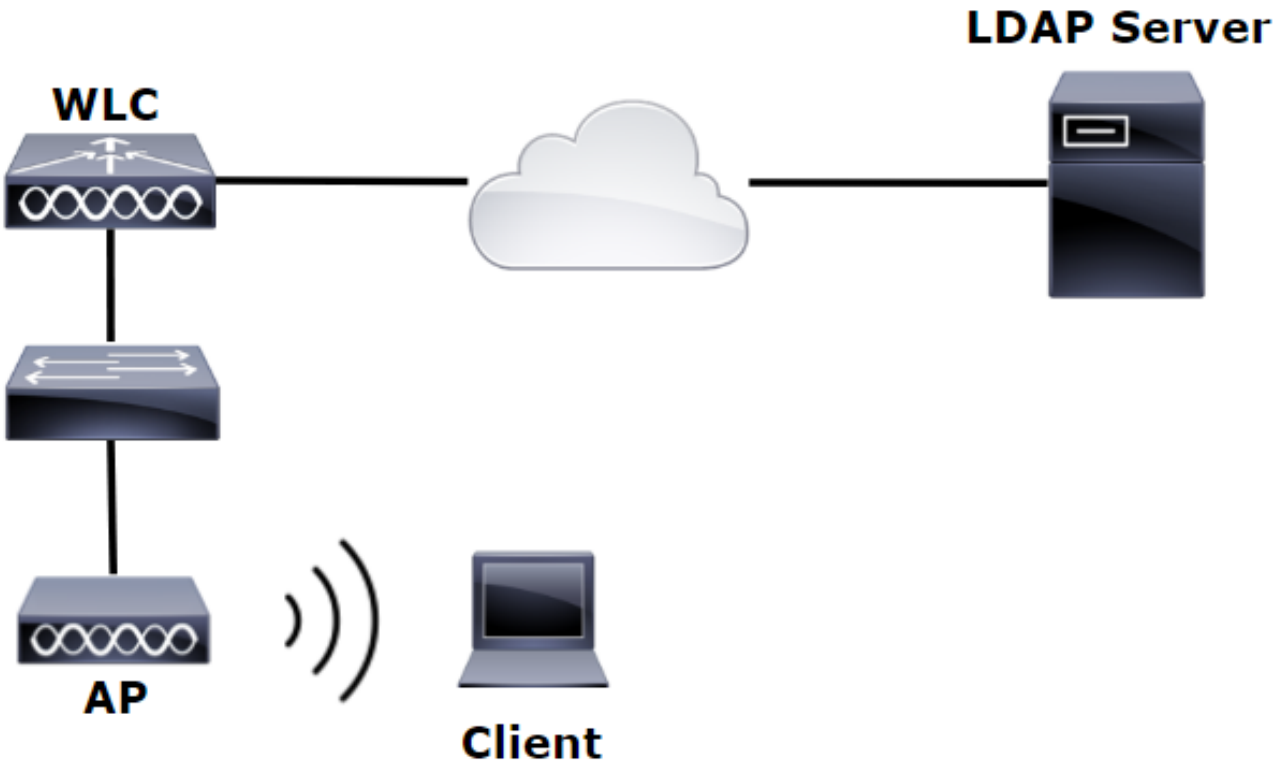
Per questa procedura, è necessario autenticare solo gli utenti all'interno di OU=SofiaLabOU.

Per informazioni su come utilizzare lo strumento Label Distribution Protocol (LDP), configurare e risolvere i problemi relativi a LDAP, consultare la guida alla configurazione di LDAP nel WLC.

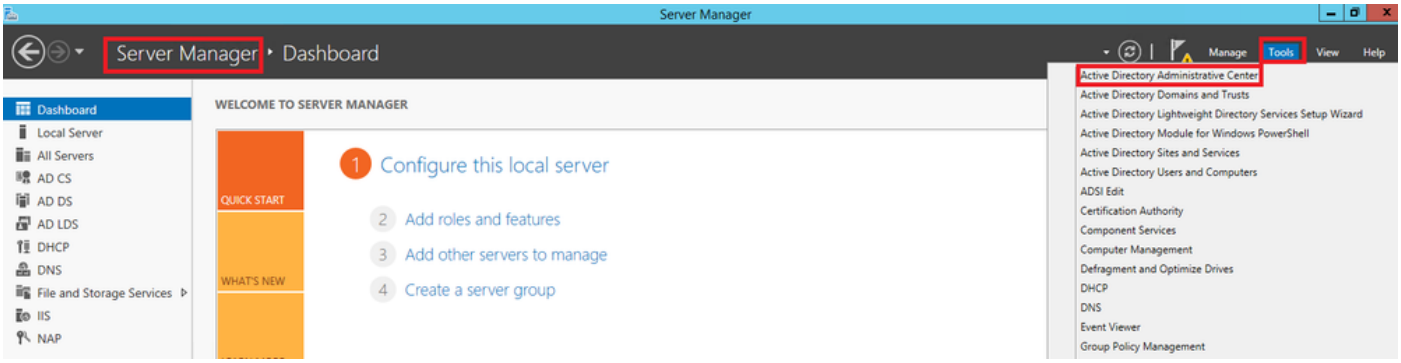
## Creazione di una WLAN basata sul server LDAP per autenticare gli utenti tramite 802.1x

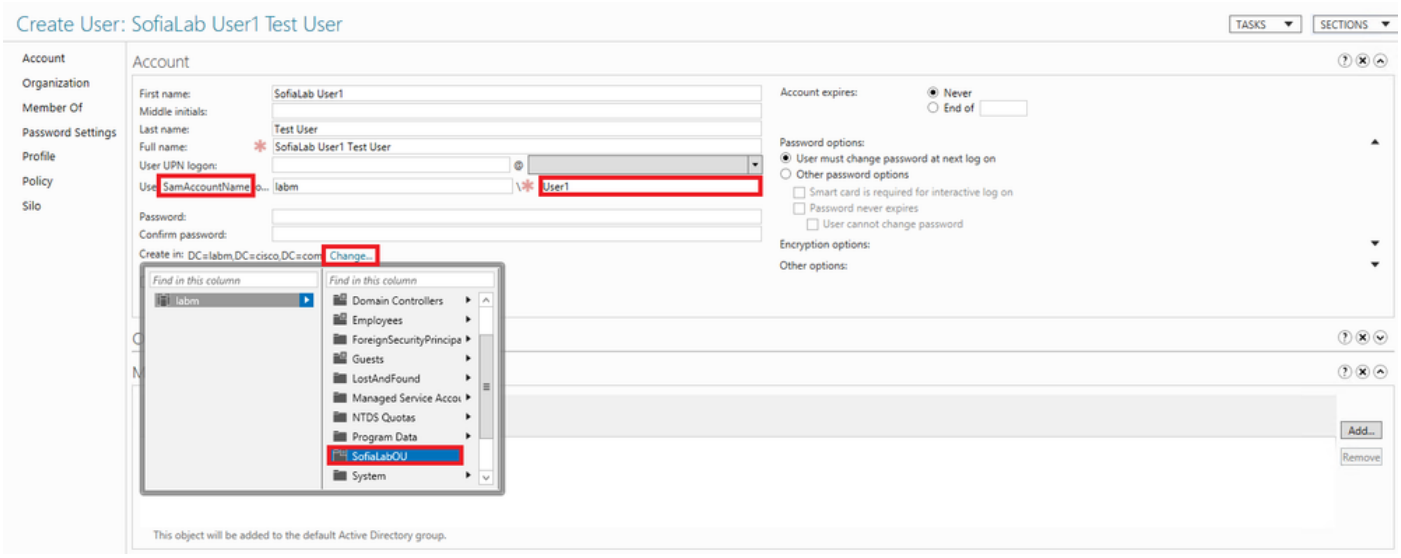
### Esempio di rete

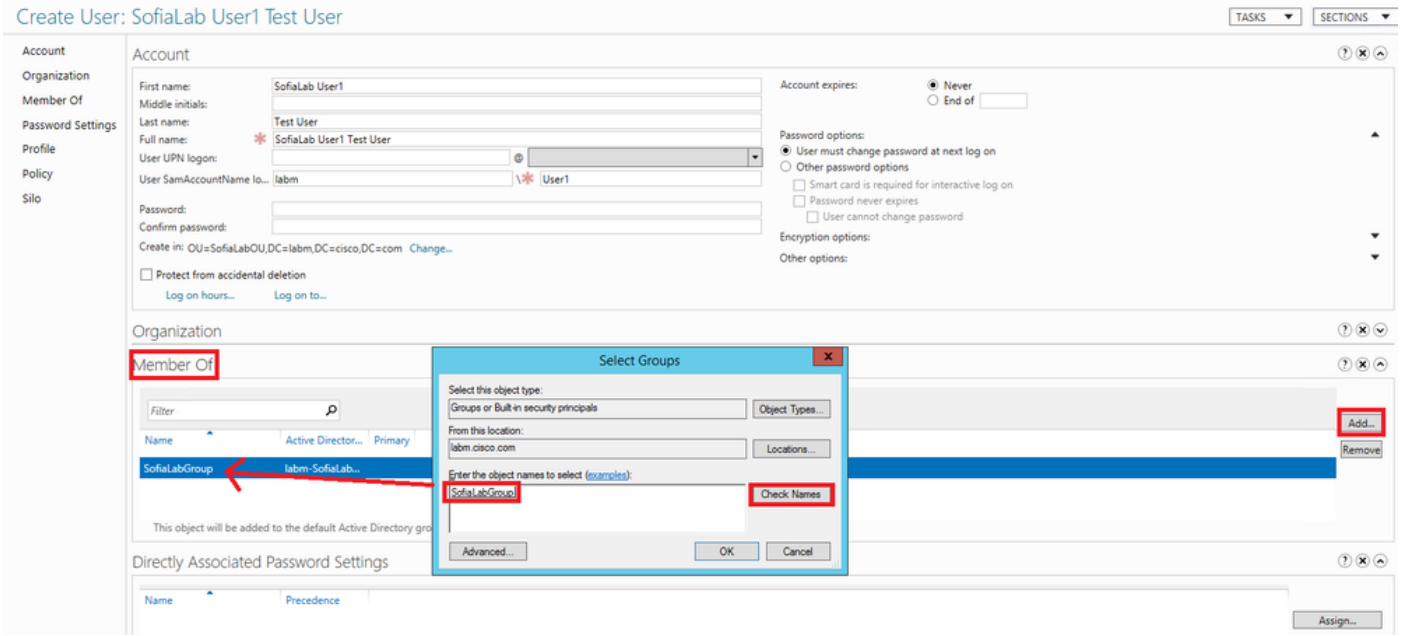
In questo scenario, il protocollo LDAP-dot1x della WLAN utilizza un server LDAP per autenticare gli utenti con l'uso di 802.1x.



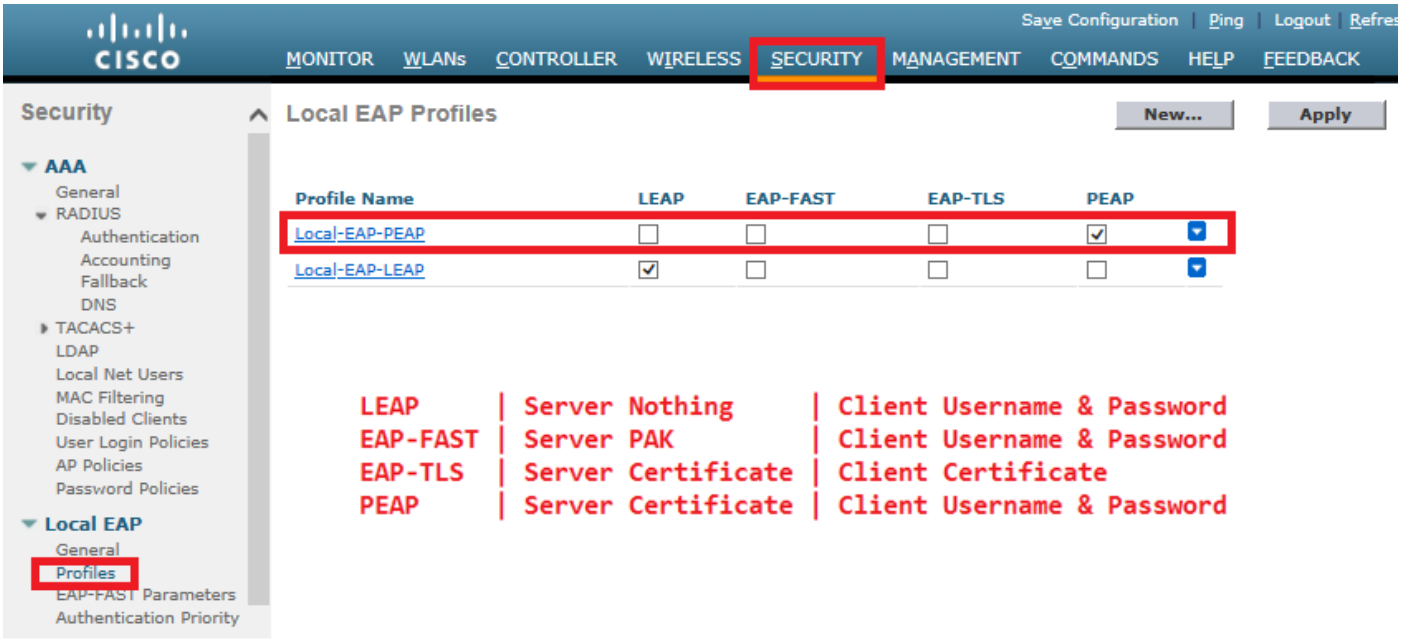

Passaggio 1. Creare un utente **User1** nel membro Server LDAP di SofiaLabOU e SofiaLabGroup.



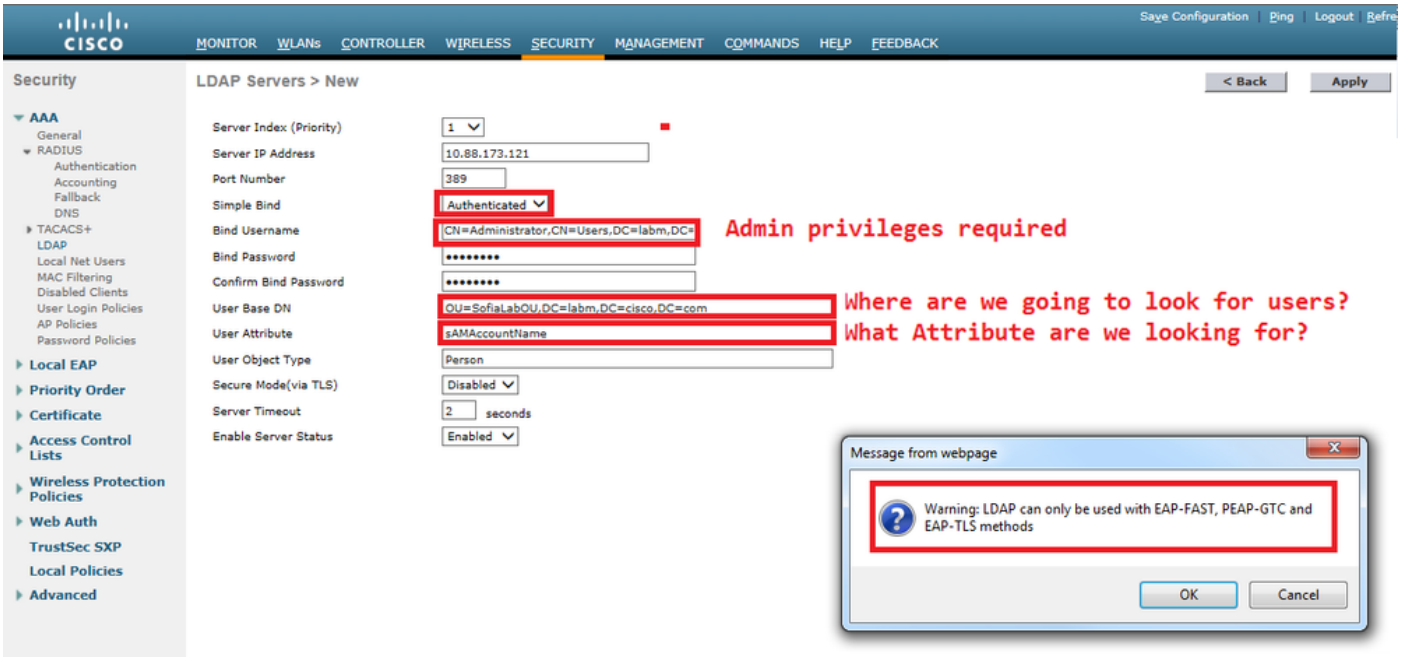




Passaggio 2. Creare un profilo EAP sul WLC con il metodo EAP desiderato (utilizzare PEAP).



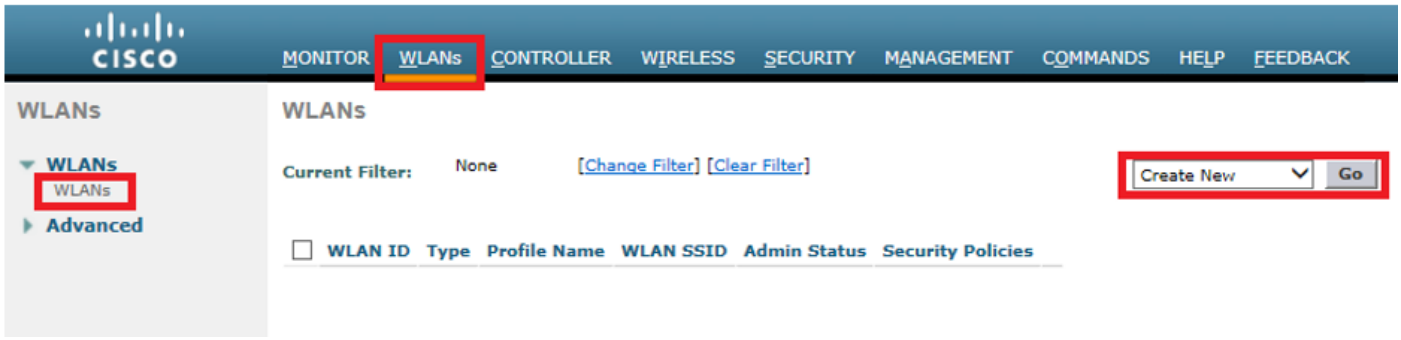

Passaggio 3. Associare il WLC al server LDAP.

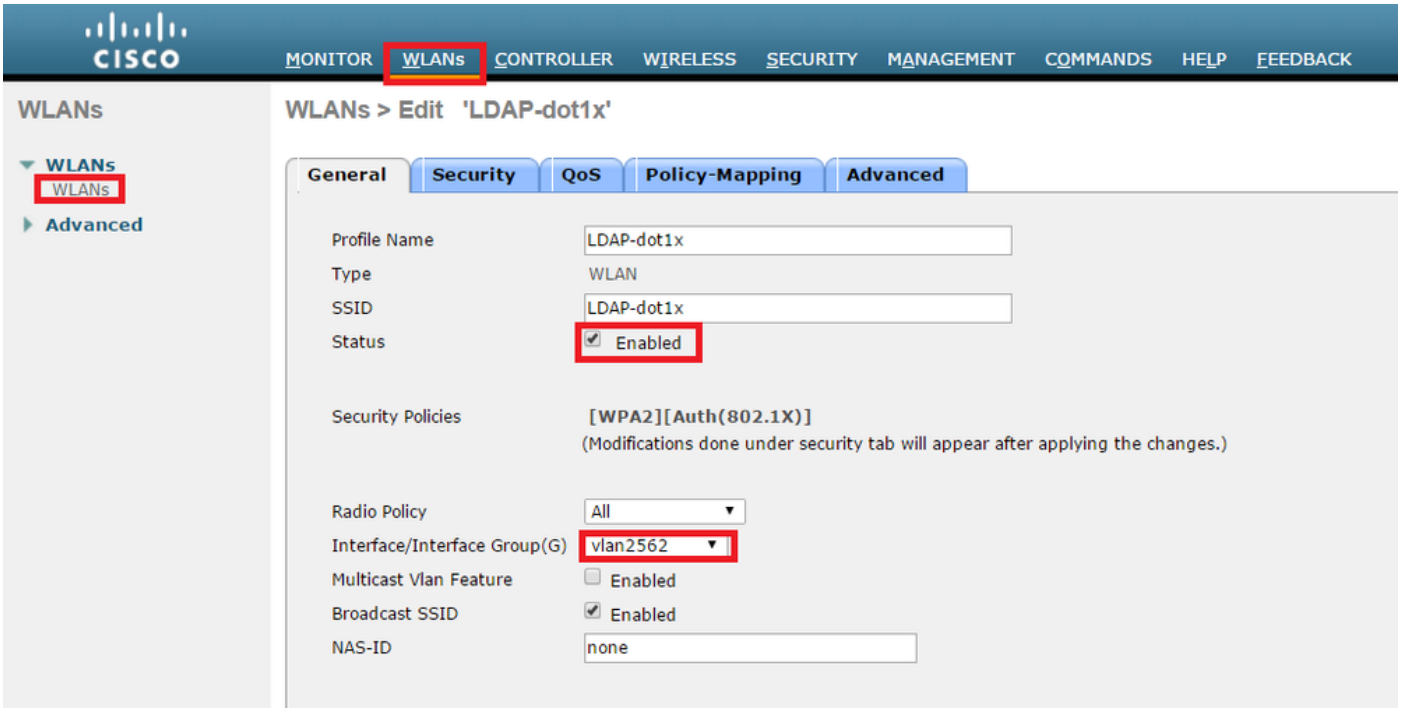
> **Suggerimento**: se il nome utente di associazione non si trova nel DN della base utente, è necessario scrivere l'intero percorso all'utente **Admin** come mostrato nell'immagine. In caso contrario, è sufficiente immettere **Administrator**.



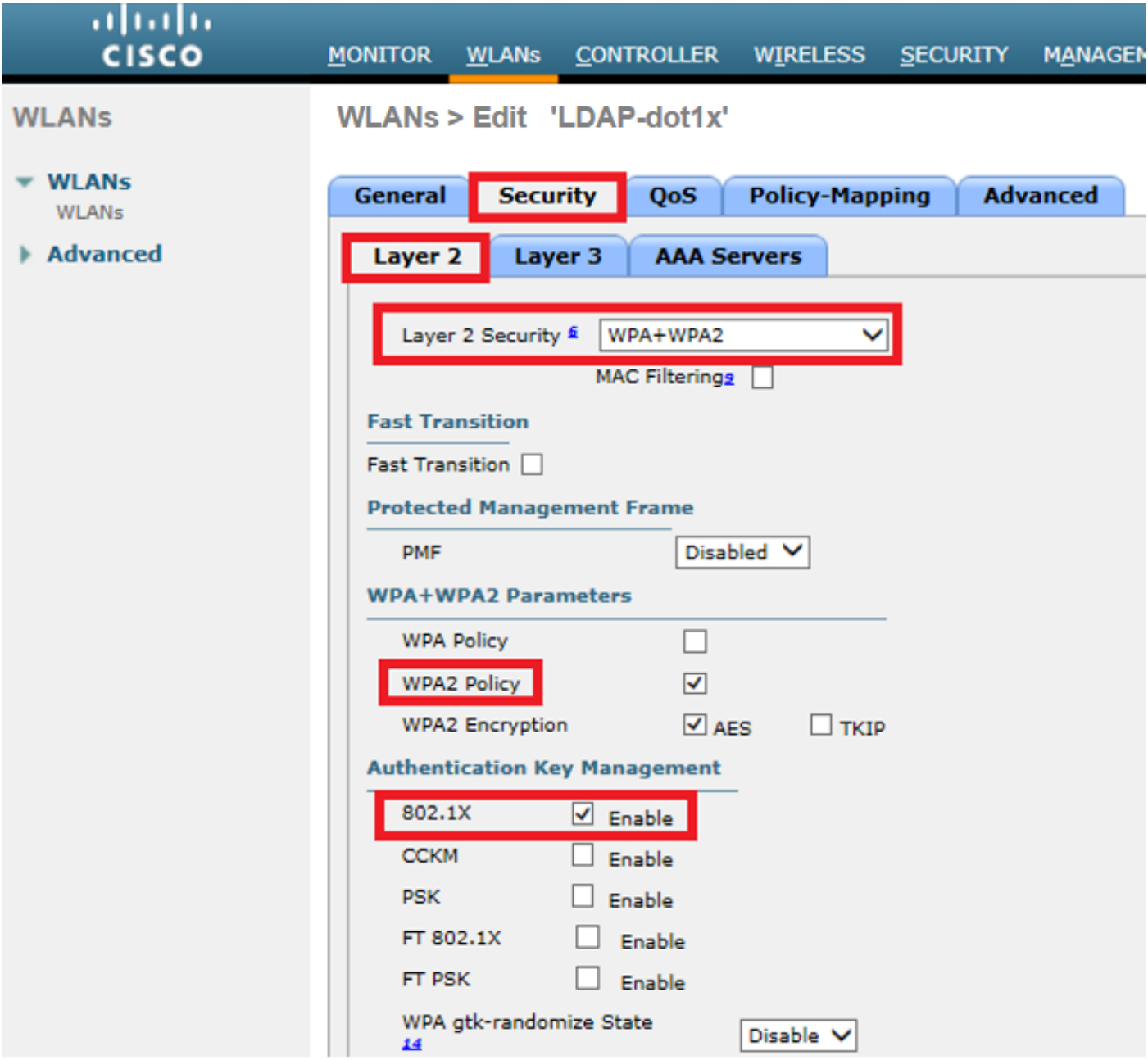

Passaggio 4. Impostare l'ordine di autenticazione su Solo utenti interni + LDAP o LDAP.


Passaggio 5. Creare la WLAN LDAP-dot1x.

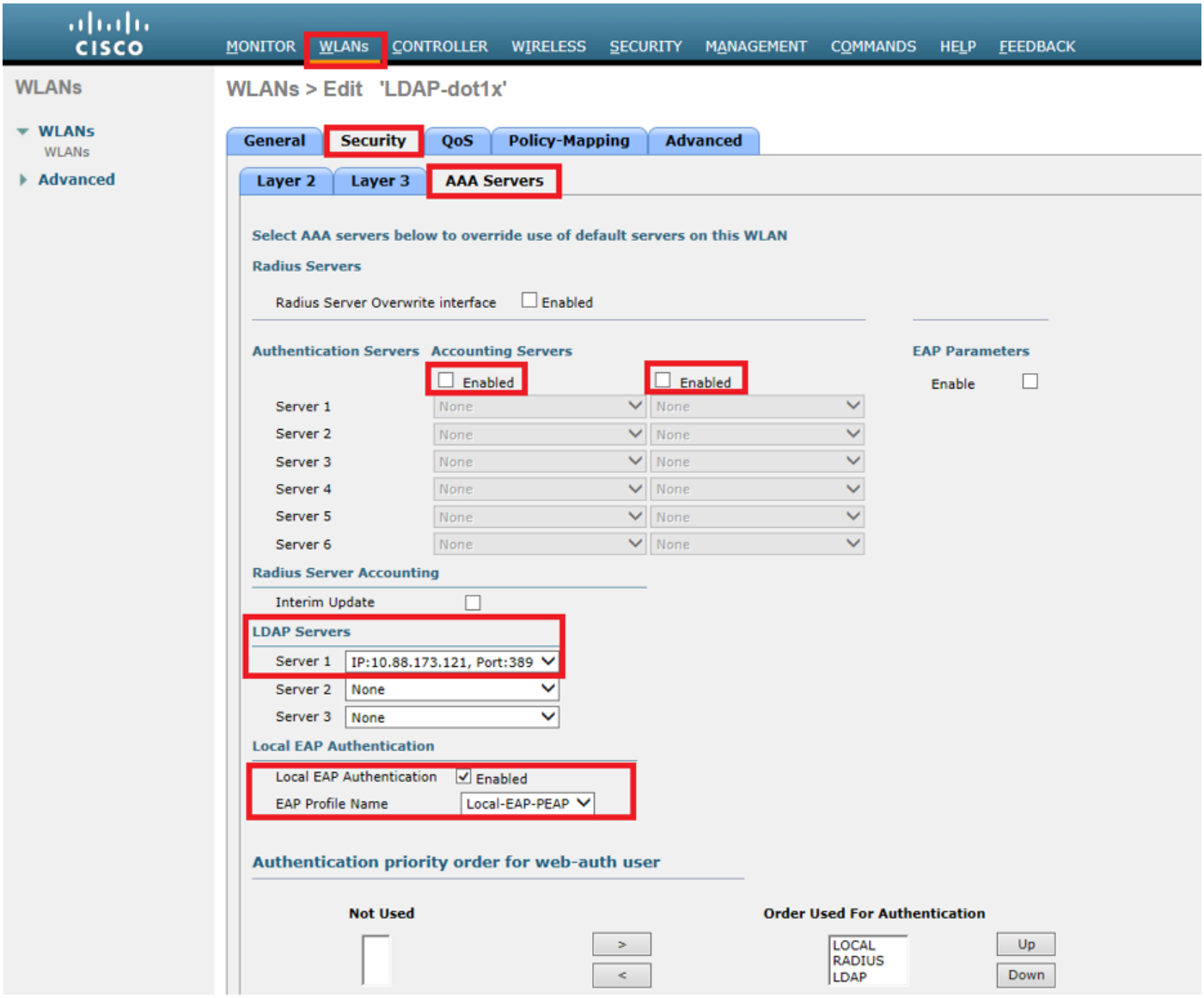





Passaggio 6. Impostare il metodo di protezione L2 su WPA2 + 802.1x e la protezione L3 su none (nessuno).




Passaggio 7. Abilitare l'autenticazione EAP locale e assicurarsi che le opzioni Server di autenticazione e Server di accounting siano disabilitate e che LDAP sia abilitato.



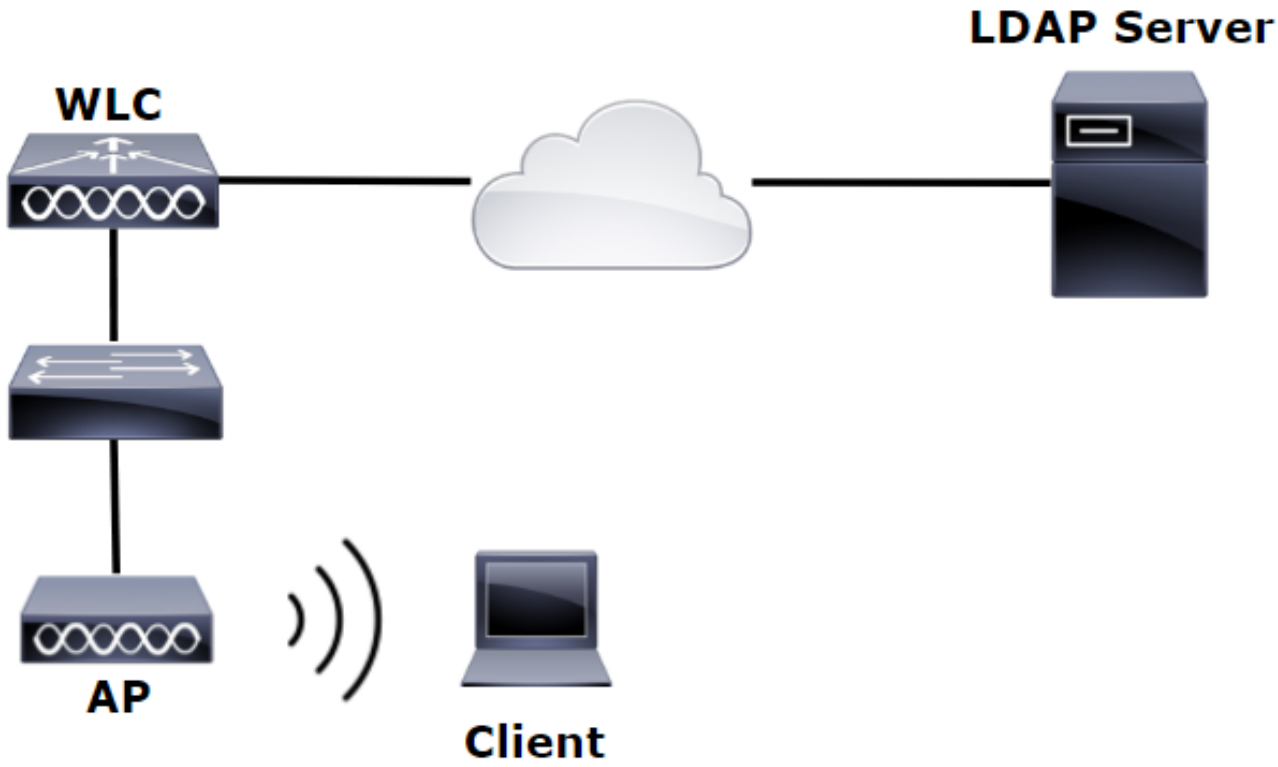

Tutte le altre impostazioni possono essere lasciate in posizione predefinita.

> **Note:**
> Utilizzate lo strumento LDP per confermare i parametri di configurazione.
> La base di ricerca non può essere un gruppo, ad esempio SofiaLabGroup.
> Se si tratta di un computer Windows, è necessario utilizzare PEAP-GTC o Cisco:PEAP anziché Microsoft:PEAP nel supplicant. Microsoft:PEAP funziona per impostazione predefinita con MacOS/iOS/Android.

## Creazione di una WLAN basata sul server LDAP per autenticare gli utenti tramite il portale Web WLC interno

### Esempio di rete

In questo scenario, il protocollo LDAP-Web della WLAN utilizza un server LDAP per autenticare gli utenti con il portale Web WLC interno.




Assicurarsi che i passaggi da 1 a 4 siano stati eseguiti dall'esempio precedente. Da qui, la configurazione WLAN è impostata in modo diverso.

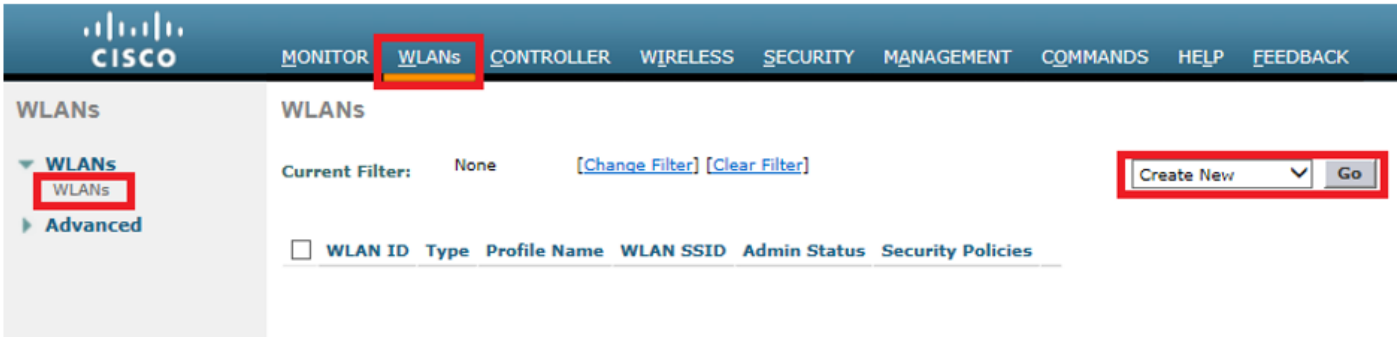
Passaggio 1. Creare un utente **User1** nel membro Server LDAP dell'OU SofiaLabOU e del Gruppo SofiaLabGroup.

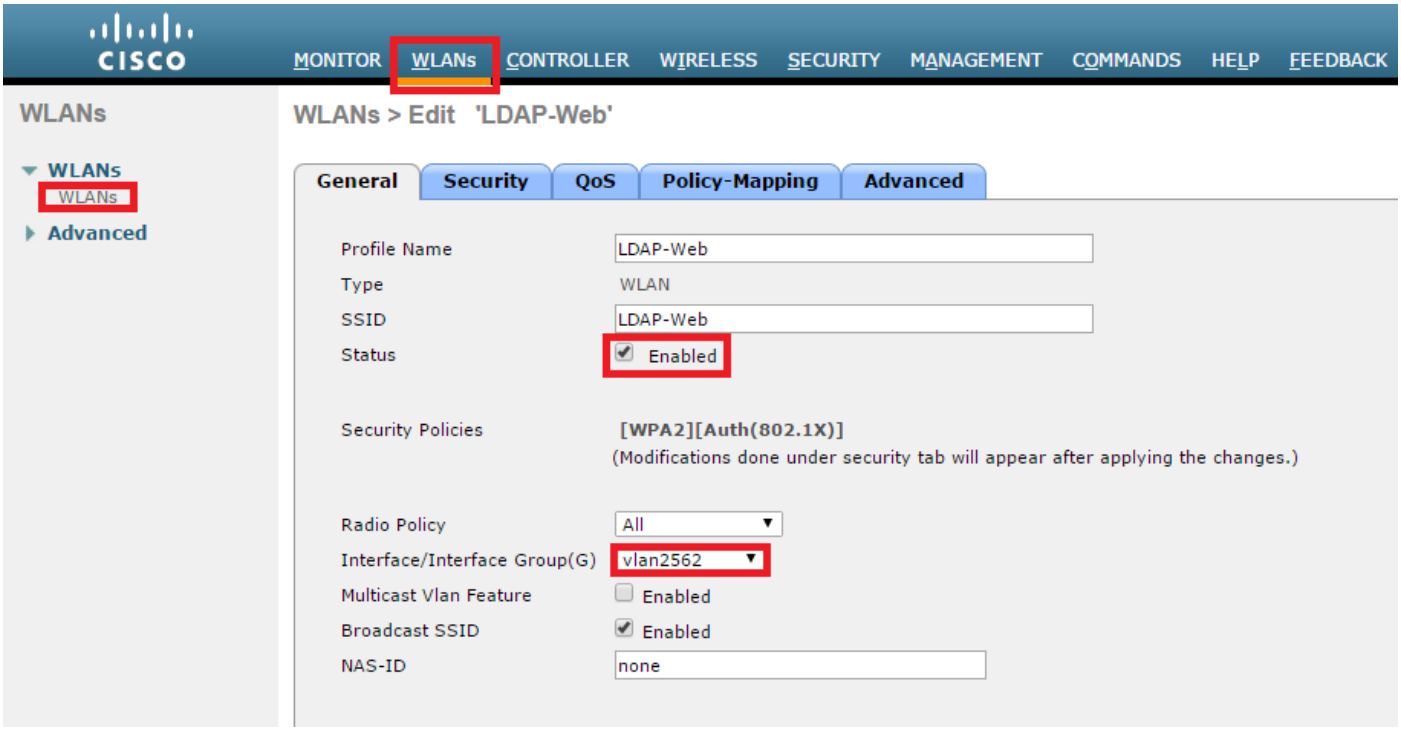
Passaggio 2. Creare un profilo EAP sul WLC con il metodo EAP desiderato (utilizzare PEAP).

Passaggio 3. Associare il WLC al server LDAP.

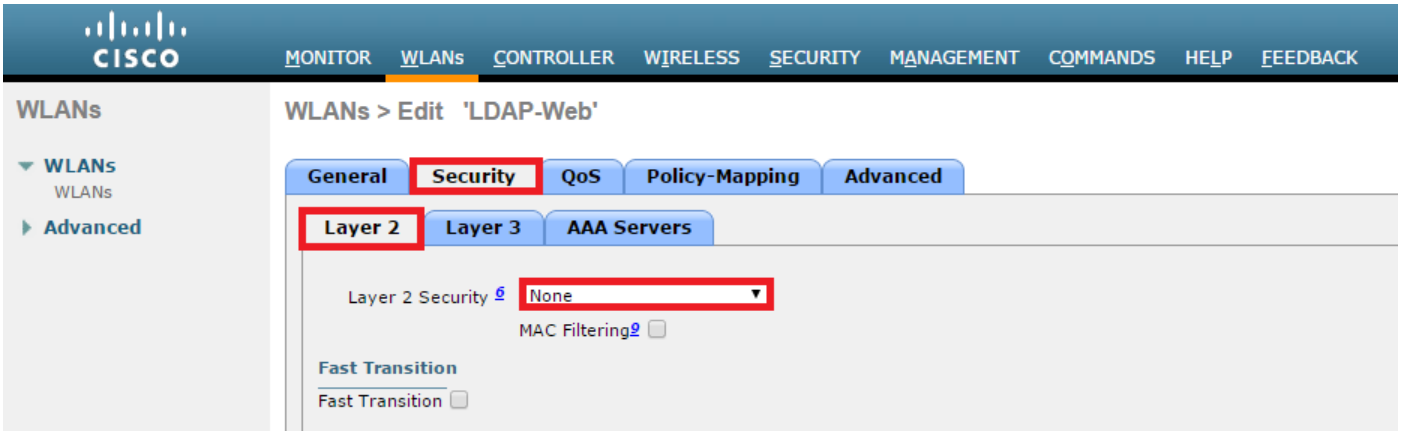
Passaggio 4. Impostare l'ordine di autenticazione su Internal Users + LDAP.

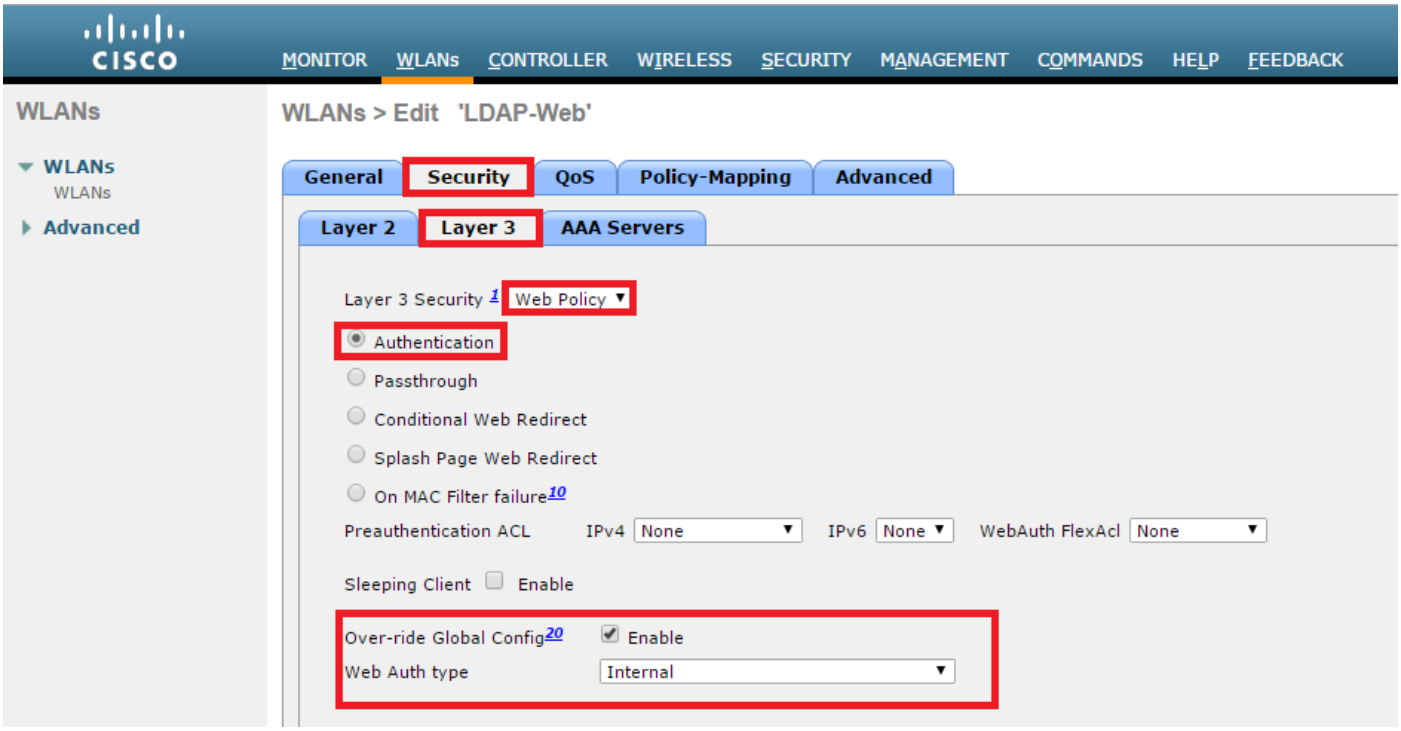
Passaggio 5. Creare la WLAN LDAP-Web come mostrato nelle immagini.



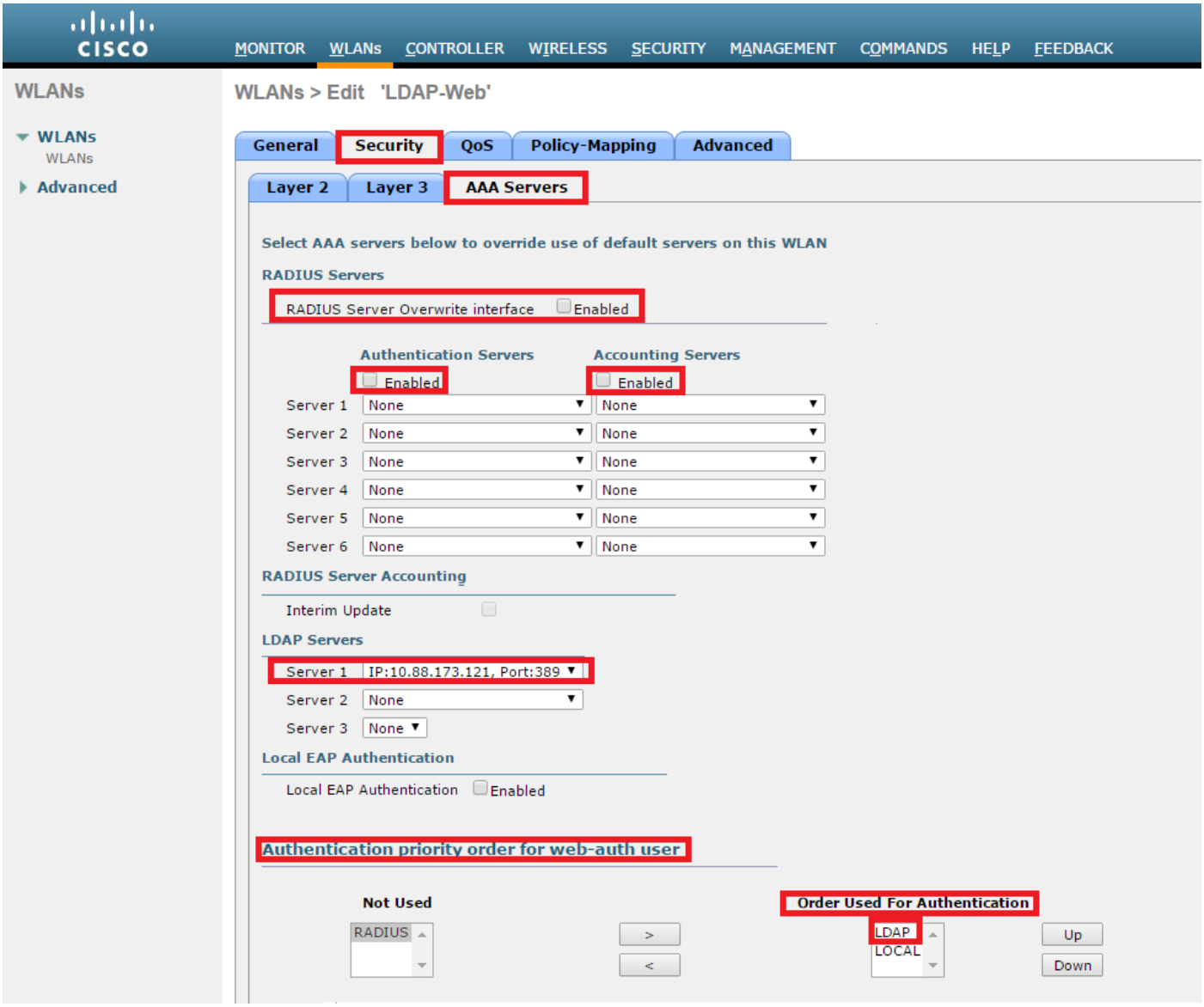



Passaggio 6. Imposta sicurezza L2 su nessuna e sicurezza L3 su criteri Web - Autenticazionecome mostrato nelle immagini.






Passaggio 7. Impostare l'ordine di priorità dell'autenticazione per l'autenticazione Web per utilizzare LDAP e assicurarsi che le opzioni Server di autenticazione e Server di accounting siano disattivate.

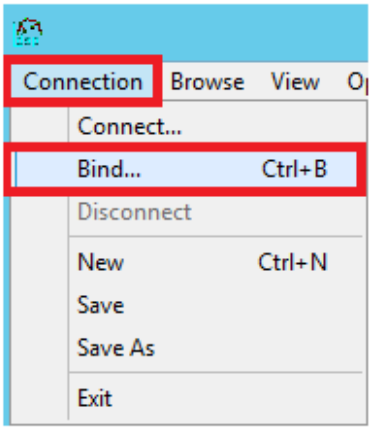


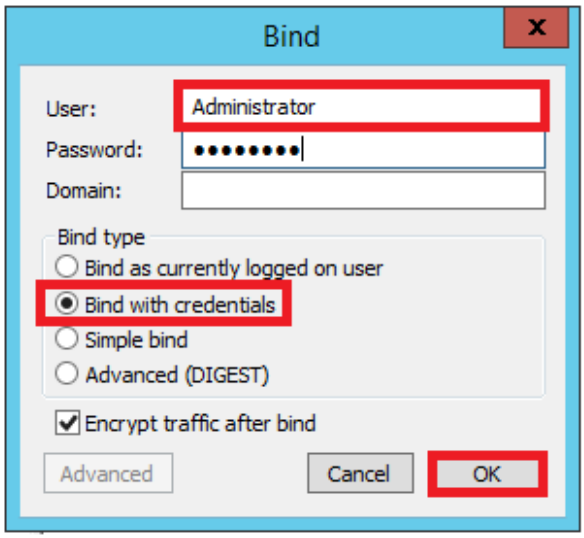

Tutte le altre impostazioni possono essere lasciate in posizione predefinita.

## Utilizzare Lo Strumento LDP Per Configurare E Risolvere I Problemi Relativi A LDAP

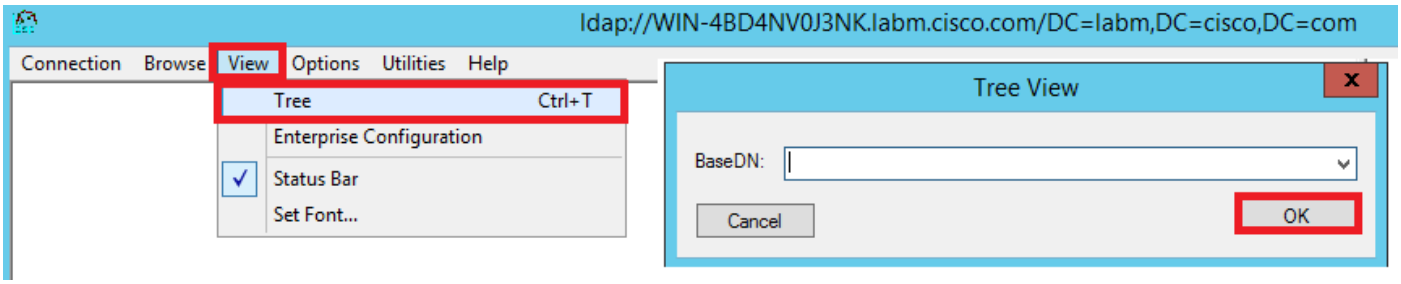
Passaggio 1. Aprire lo strumento LDP sul server LDAP o su un host con connettività (la porta TCP 389 deve essere consentita al server).

Passaggio 2. Passare a **Connessione > Binding,** accedere con un utente Admin e selezionare il pulsante di opzione **Binding con credenziali**.

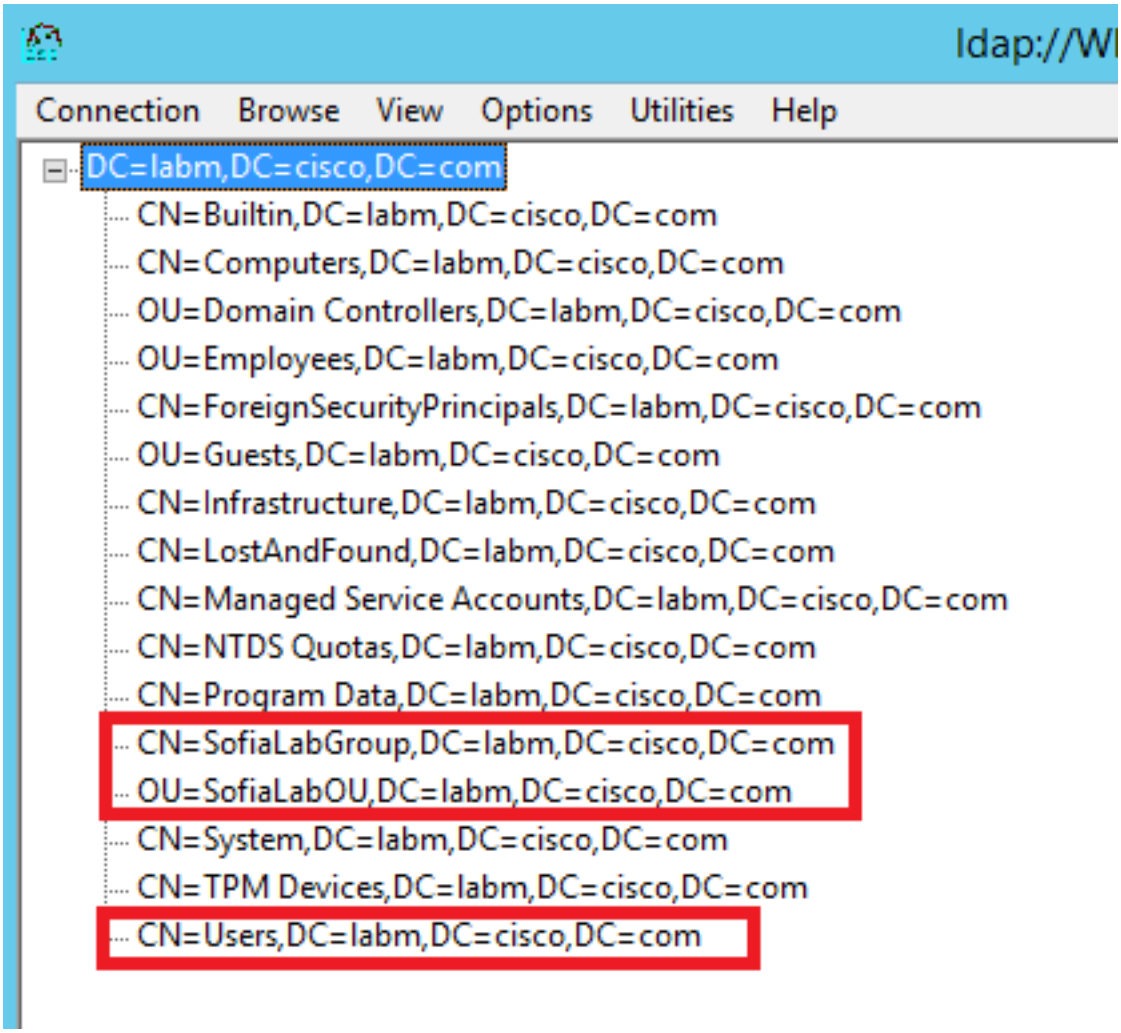


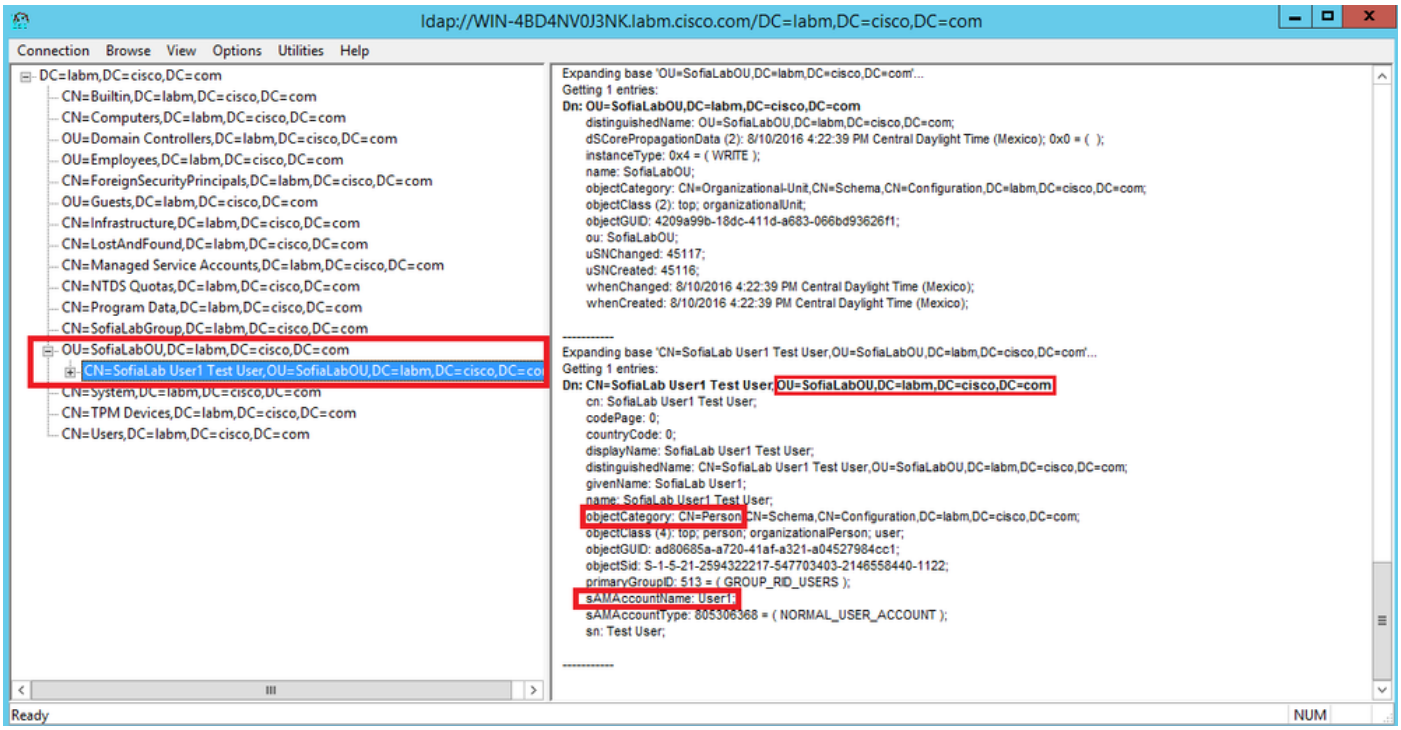

Passaggio 3. Passare a **Visualizza > Albero** e selezionare **OK** nel DN di base.



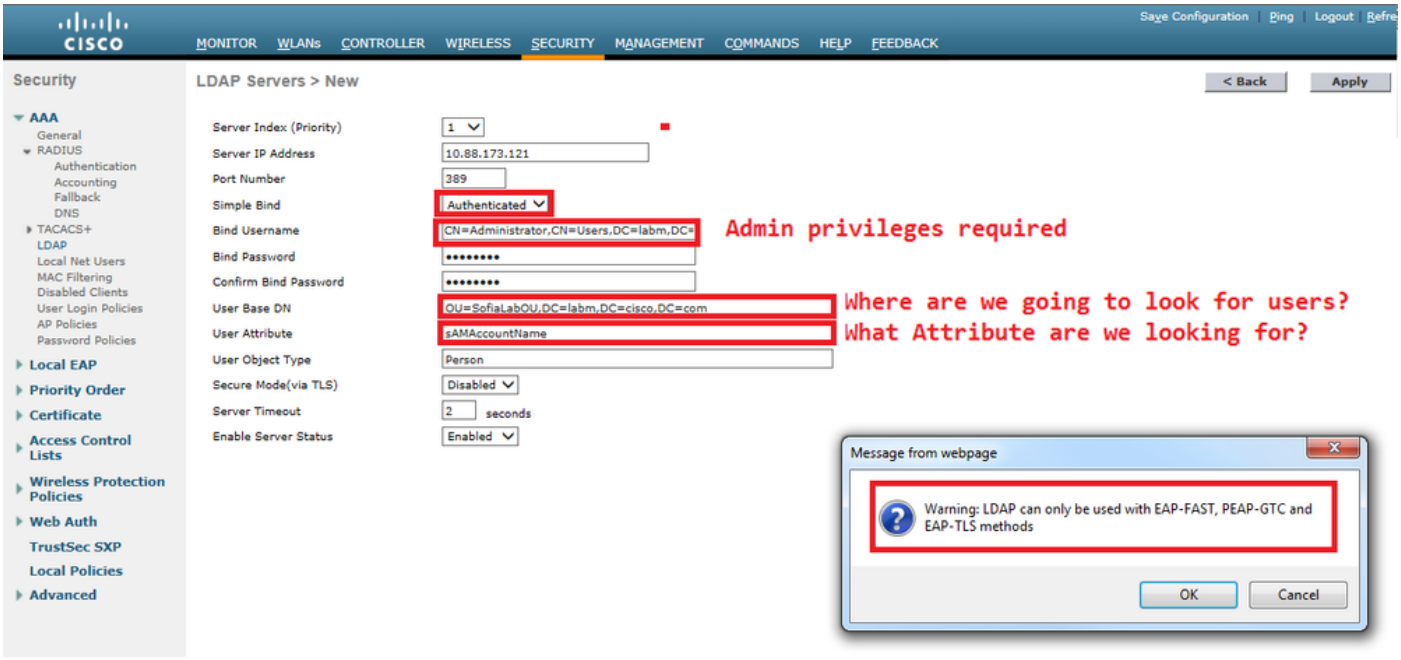

Passaggio 4. Espandere la struttura per visualizzare la struttura e cercare il DN della base di ricerca. È possibile utilizzare qualsiasi tipo di contenitore, ad eccezione dei gruppi. Può trattarsi dell'intero dominio, di un'unità organizzativa specifica o di un CN come CN=Users.



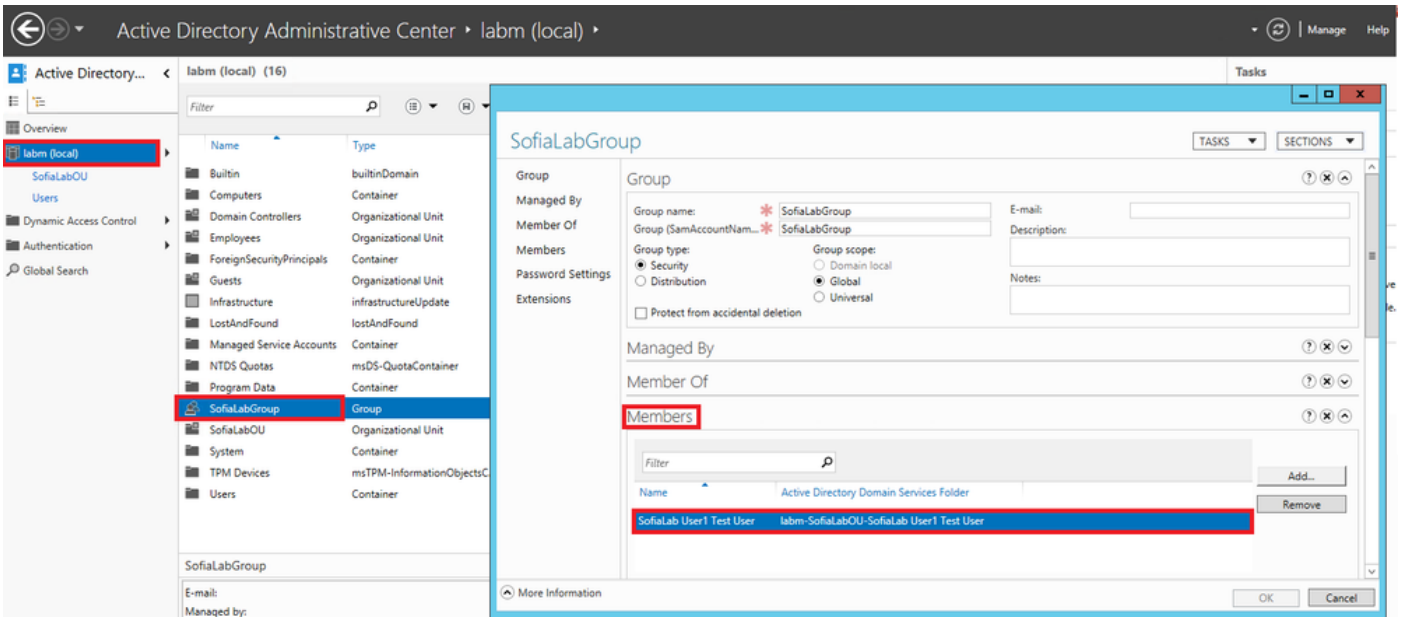

Passaggio 5. Espandere SofiaLabOU per vedere quali utenti si trovano al suo interno. È presente l'utente 1 creato in precedenza.




Passaggio 6. Tutto il necessario per configurare LDAP.




Passaggio 7. Gruppi come SofiaLabGroup non possono essere utilizzati come DN di ricerca. Espandere il gruppo e cercare gli utenti al suo interno, dove l'utente 1 creato in precedenza deve esserecome illustrato.




L'utente 1 era presente ma LDP non è stato in grado di trovarlo. Significa che il WLC non è in grado di eseguire questa operazione e per questo motivo i gruppi non sono supportati come DN della base di ricerca.

# Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

```
(cisco-controller) >show ldap summary

Idx Server Address Port Enabled Secure
```

```
--- ------------------------ ------ ------- ------
1 10.88.173.121 389 Yes No



(cisco-controller) >show ldap 1

Server Index..................................... 1
Address.......................................... 10.88.173.121
Port............................................. 389
Server State..................................... Enabled
User DN.......................................... OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
User Attribute................................... sAMAccountName
User Type........................................ Person
Retransmit Timeout............................... 2 seconds
Secure (via TLS)................................. Disabled
Bind Method ..................................... Authenticated
Bind Username.................................... CN=Administrator,CN=Domain
Admins,CN=Users,DC=labm,DC=cisco,DC=com
```

# Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

```
(cisco-controller) >debug client <MAC Address>

(cisco-controller) >debug aaa ldap enable

(cisco-controller) >show ldap statistics

Server Index..................................... 1
Server statistics:
Initialized OK................................... 0
Initialization failed............................ 0
Initialization retries........................... 0
Closed OK........................................ 0
Request statistics:
Received......................................... 0
Sent............................................. 0
OK............................................... 0
Success.......................................... 0
Authentication failed............................ 0
Server not found................................. 0
No received attributes........................... 0
No passed username............................... 0
Not connected to server.......................... 0
Internal error................................... 0
Retries.......................................... 0
```

# Informazioni correlate

- LDAP - Guida alla configurazione di WLC 8.2
- Configurazione di Wireless Lan Controller (WLC) per l'autenticazione LDAP (Lightweight Directory Access Protocol) - di Vinay Sharma
- Esempio di configurazione dell'autenticazione Web tramite LDAP sui Wireless LAN Controller

(WLC) - di Yahya Jaber e Ayman Alfares
- Documentazione e supporto tecnico – Cisco Systems

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).