Configureer WLC met LDAP-verificatie voor 802.1x en Web-Autation WLAN's

Inhoud

Inleiding

In dit document wordt de procedure beschreven voor het configureren van een AireOS WLC om clients met een LDAP Server als gebruikersdatabase te authenticeren.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Microsoft Windows-servers
- Active Directory

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco WLC-software 8.2.10.0

- Microsoft Windows Server 2012 R2

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

Achtergrondinformatie

Technische achtergrond

- LDAP is een protocol dat wordt gebruikt voor de toegang tot directory servers.
- Directory servers zijn hiërarchische, object georiënteerde databases.
- Objecten worden georganiseerd in containers zoals Organisatorische Eenheden (OU), Groepen, of standaard Microsoft Containers als CN=Gebruikers.
- Het moeilijkste deel van deze opstelling is de LDAP serverparameters correct op WLC te vormen.

Voor gedetailleerdere informatie over deze concepten, raadpleegt u de sectie Inleiding van Hoe u Wireless LAN Controller (WLC) kunt configureren voor LDAP-verificatie (Lichtgewicht Directory Access Protocol).

Veelgestelde vragen

- Welke gebruikersnaam moet worden gebruikt om te binden met de LDAP-server?

Er zijn twee manieren om te binden tegen een LDAP-server, Anoniem of Geverifieerd (raadpleeg de sectie om het verschil tussen beide methoden te begrijpen).

Deze bind gebruikersnaam moet beheerdersrechten hebben om te kunnen vragen naar andere gebruikersnamen/wachtwoorden.

- Indien geverifieerd: is de bind gebruikersnaam binnen dezelfde container dan alle gebruikers?

Nee: gebruik het hele pad. Voorbeeld:

CN=Administrator, CN=Domain Admins, CN=Gebruikers, DC=labm, DC=cisco, DC=com

Ja: gebruik alleen de gebruikersnaam. Voorbeeld:

Beheerder

- Wat als er gebruikers zijn in verschillende containers? Moeten alle betrokken draadloze LDAP-gebruikers in dezelfde container zitten?

Nee, een basis DN die alle benodigde containers bevat kan worden gespecificeerd.

- Welke eigenschappen moet de WLC zoeken?

WLC past het gespecificeerde Gebruikerskenmerk en het gespecificeerde objecttype aan.

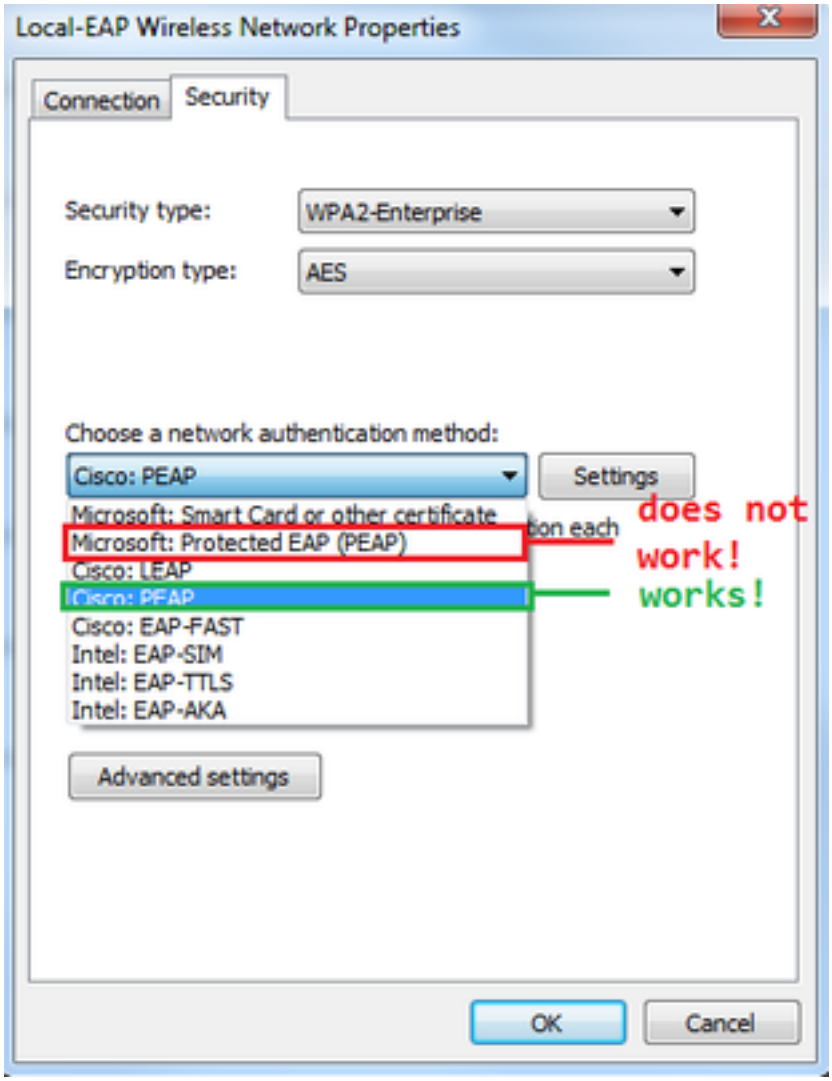
Opmerking: **sAMAccountName** is hoofdlettergevoelig, maar persoon niet. Daarom zijn

sAMAccountName=RICARDO en **sAMAccountName=ricardo** hetzelfde en werkt dit, terwijl **samaccountname=RICARDO** en **samaccountname=ricardo** dit niet doen.

- Welke EAP-methoden kunnen worden gebruikt?

Alleen EAP-FAST, PEAP-GTC en EAP-TLS. Android, iOS en MacOS standaardapplicaties werken met Protected Extensible Verification Protocol (PEAP).

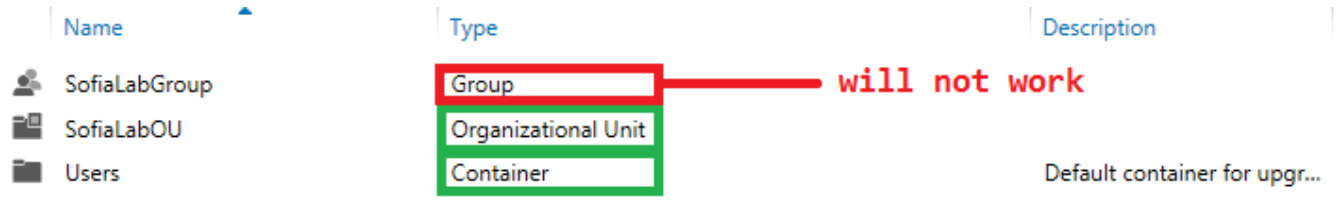
In Windows moet AnyConnect Network Access Manager (NAM) of de standaard Windows-aanvrager met Cisco:PEAP worden gebruikt voor ondersteunde draadloze adapters zoals in de afbeelding.



Opmerking: De Cisco EAP plug-ins voor Windows bevatten een versie van Open Secure Socket Layer (OpenSSL 0.9.8k) die wordt beïnvloed door Cisco bug-id CSC09670, Cisco is niet van plan om meer releases van de EAP plug-ins voor Windows uit te geven en raadt klanten aan in plaats daarvan de AnyConnect Secure Mobility Client te gebruiken.

- Waarom kan de WLC geen gebruikers vinden?

Gebruikers binnen een groep kunnen niet worden geverifieerd. Ze moeten zich in een Default Container (CN) of een Organisatorische Eenheid (OU) bevinden zoals getoond in de afbeelding.



Configureren

Er zijn verschillende scenario's waarin een LDAP-server kan worden gebruikt, met 802.1x-verificatie of webverificatie.

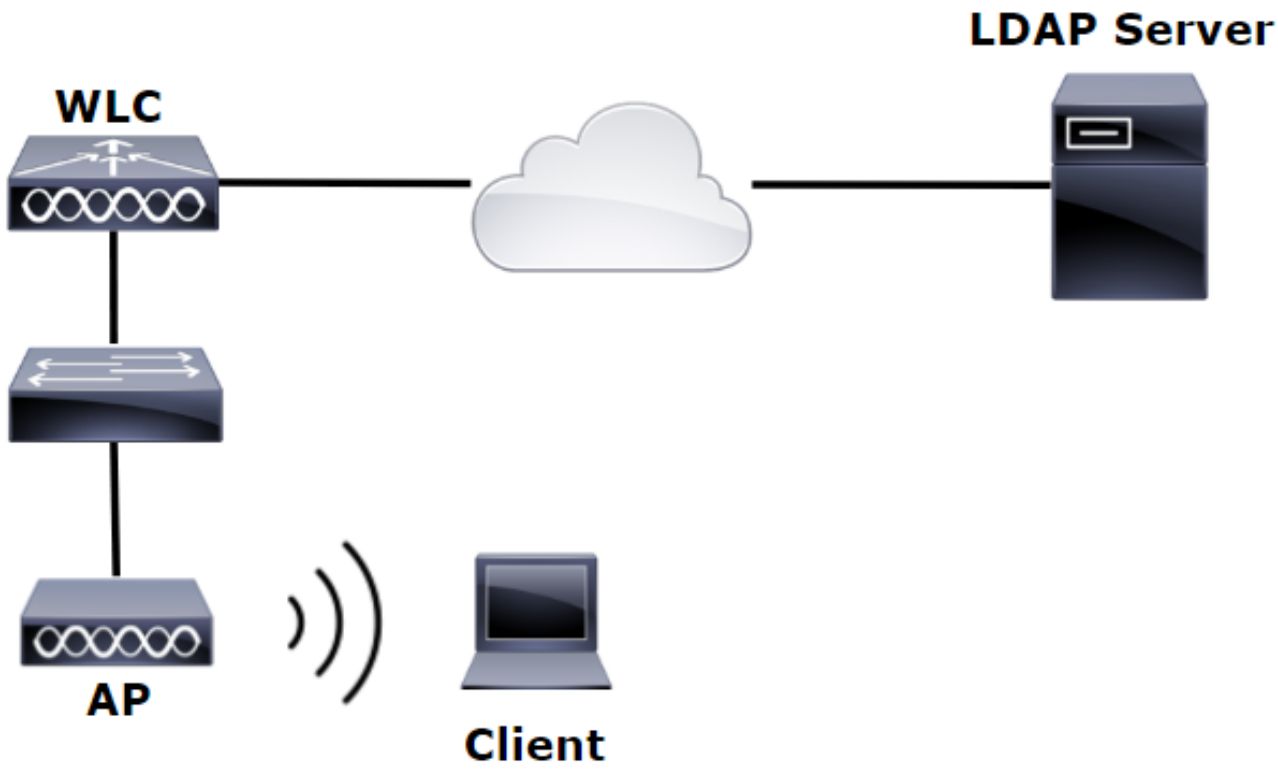
Voor deze procedure, slechts moeten de gebruikers binnen OU=SofiaLabOU worden voor authentiek verklaard.

Raadpleeg de WLC LDAP Configuration Guide voor informatie over het gebruik van LDAP (Label Distribution Protocol), het configureren en oplossen van problemen.

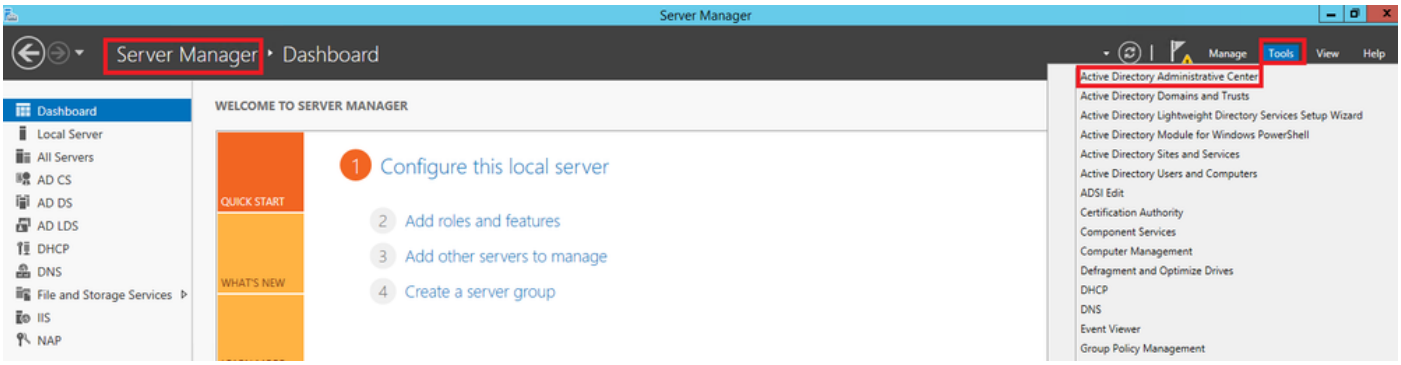
WLAN's maken die afhankelijk zijn van LDAP-server om gebruikers te verifiëren via 802.1x

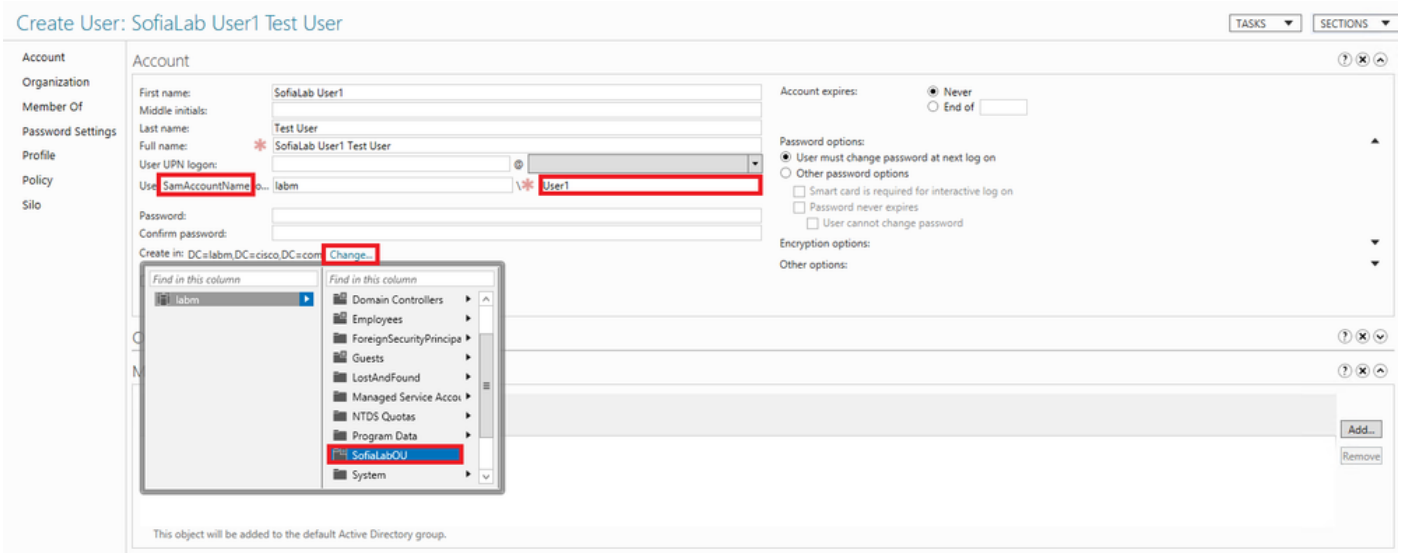
Netwerkdiagram

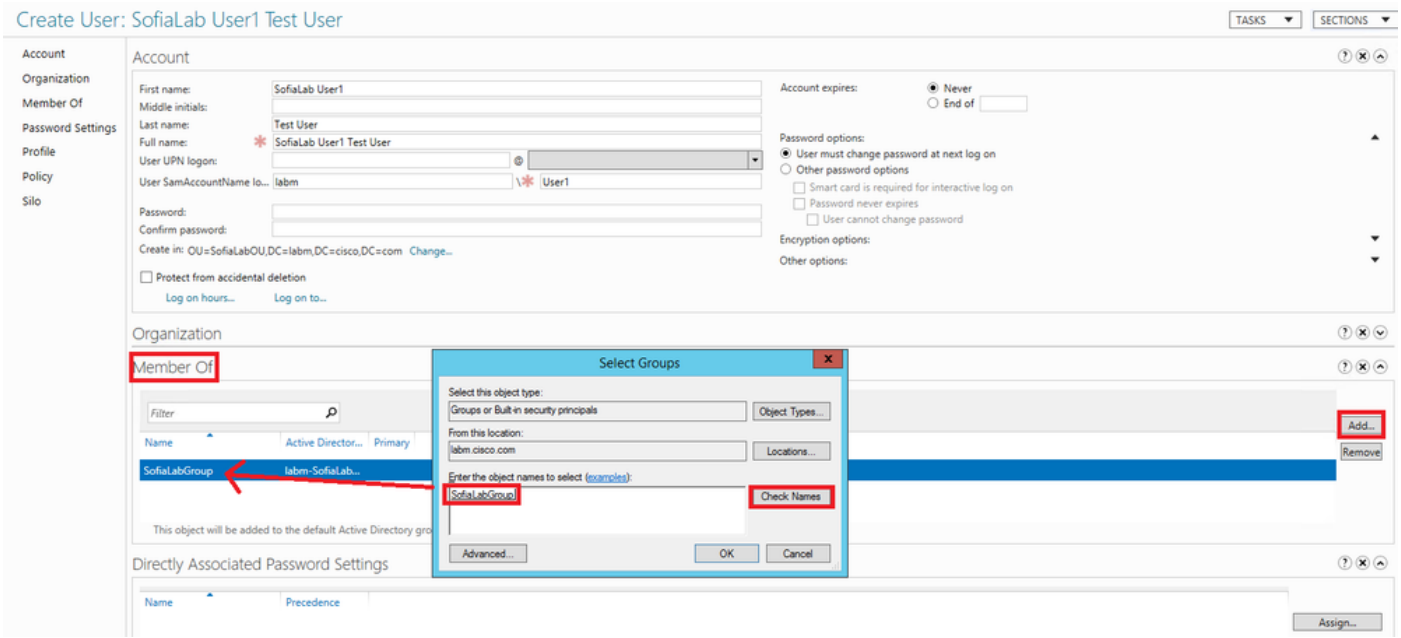
In dit scenario maakt WLAN LDAP-dot1x gebruik van een LDAP-server om de gebruikers te verifiëren met het gebruik van 802.1x.



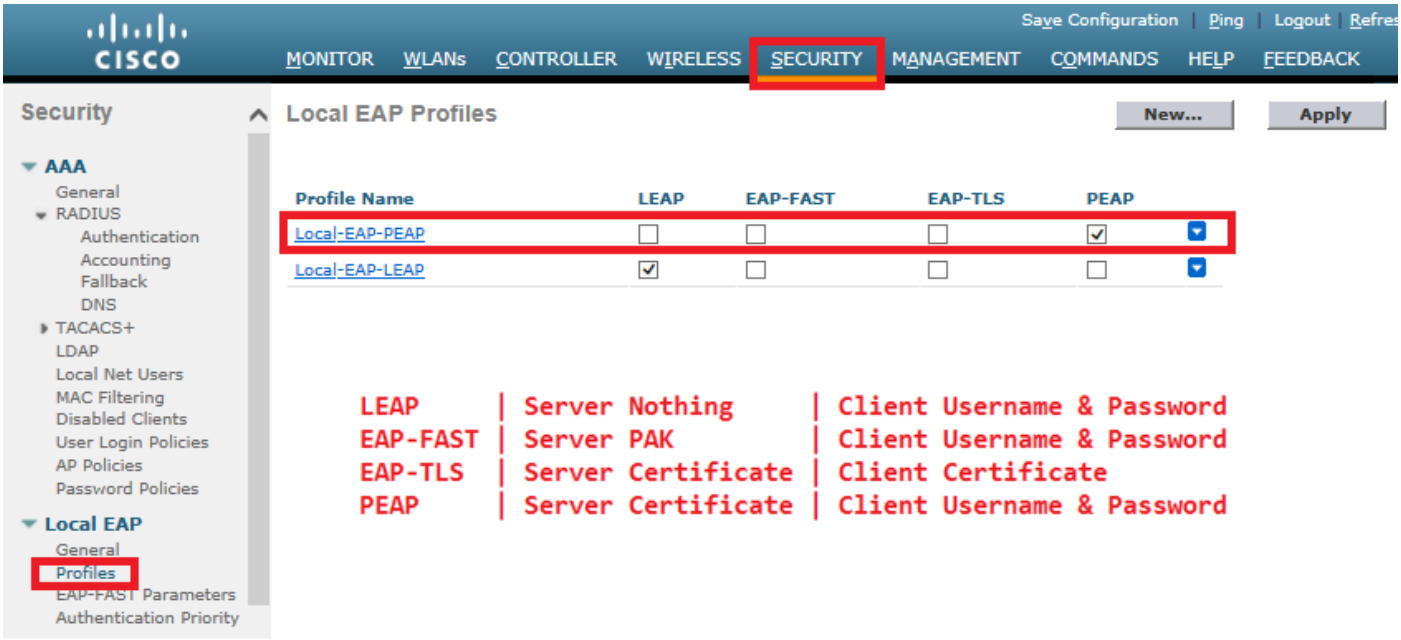
Stap 1. Maak een gebruiker **Gebruiker1** in het LDAP Server lid van SofiaLabOU en SofiaLabGroup.





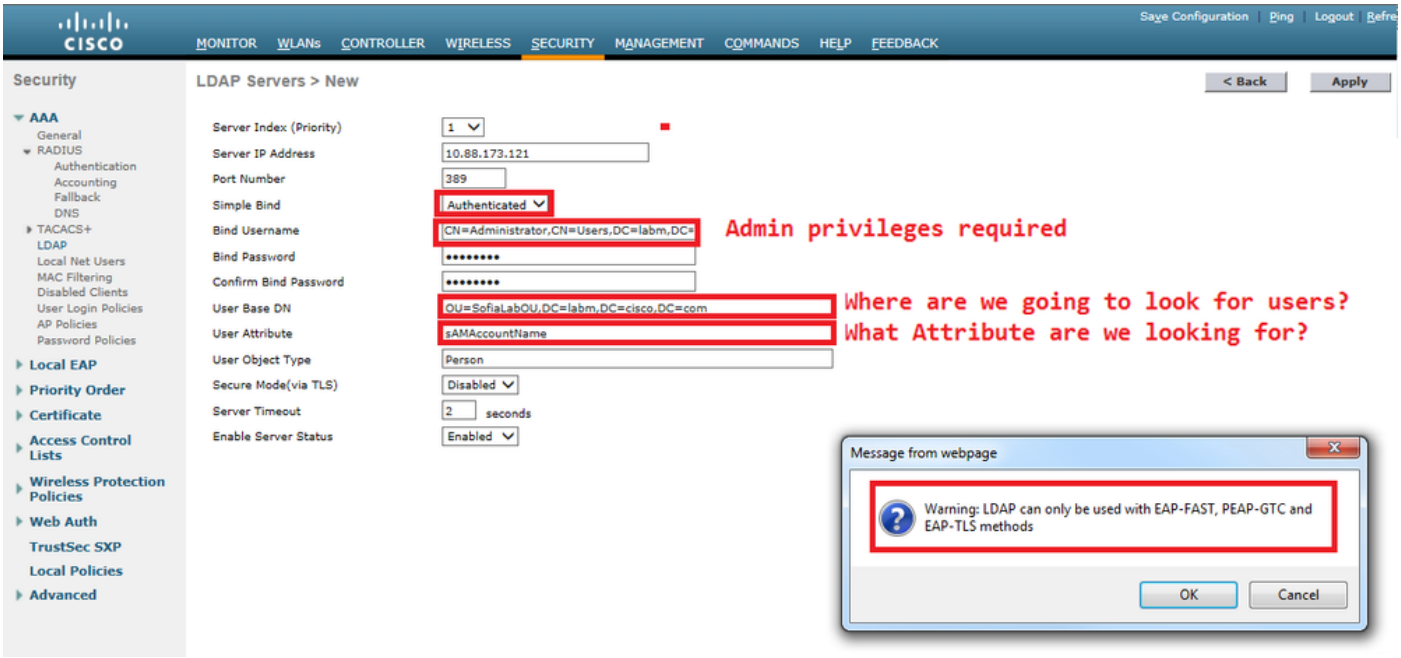


Stap 2. Maak een EAP-profiel bij de WLC met de gewenste EAP-methode (gebruik PEAP).



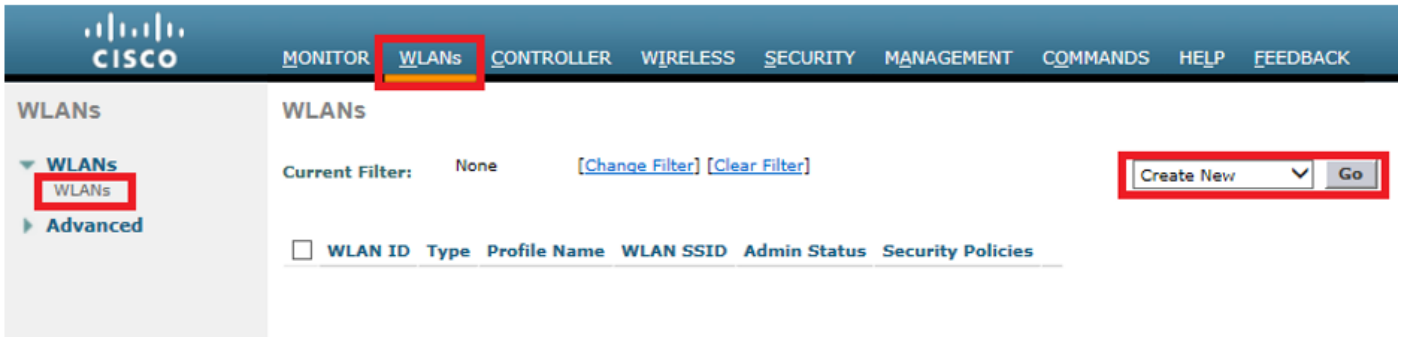
Stap 3. Bind de WLC met de LDAP Server.

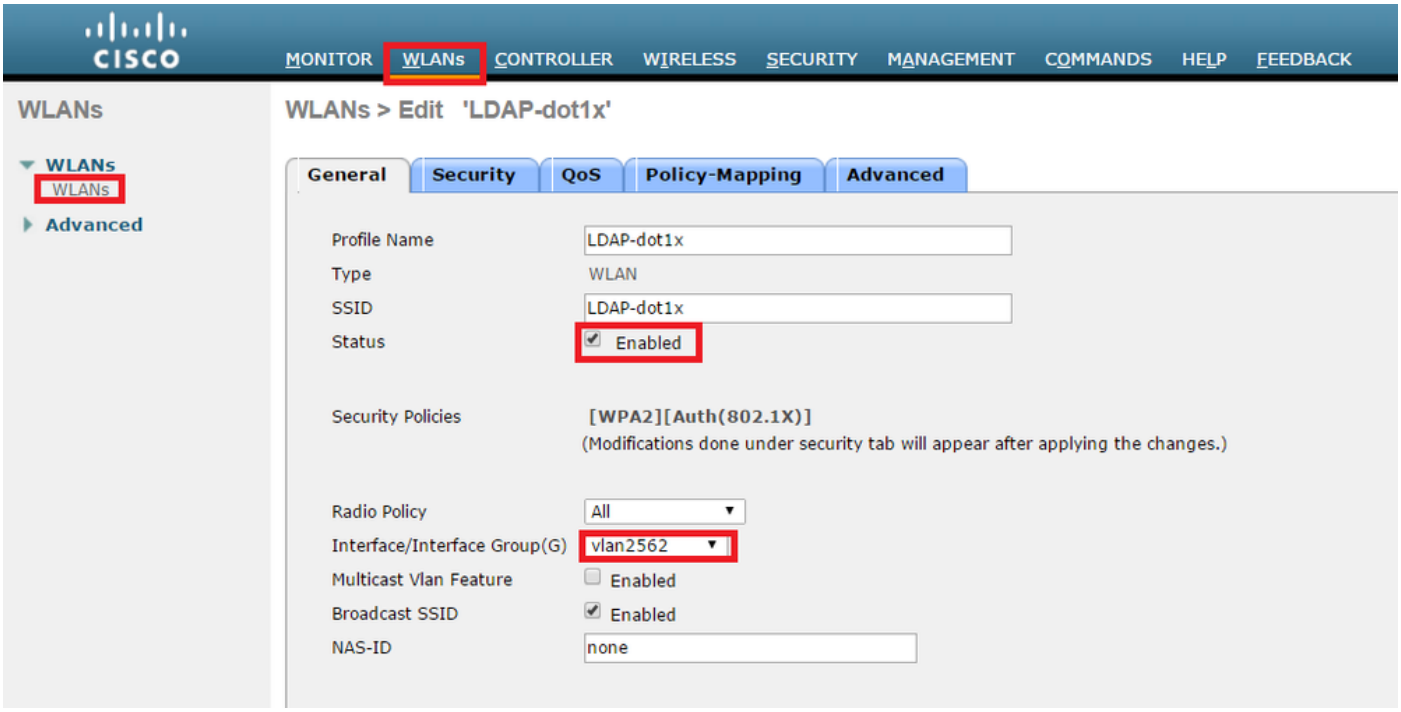
> **Tip**: Als de bind Gebruikersnaam niet in de User Base-ISDN staat, moet u het gehele pad naar de **Admin-**gebruiker schrijven zoals in de afbeelding. Anders kunt u eenvoudig **Administrator** invoeren.



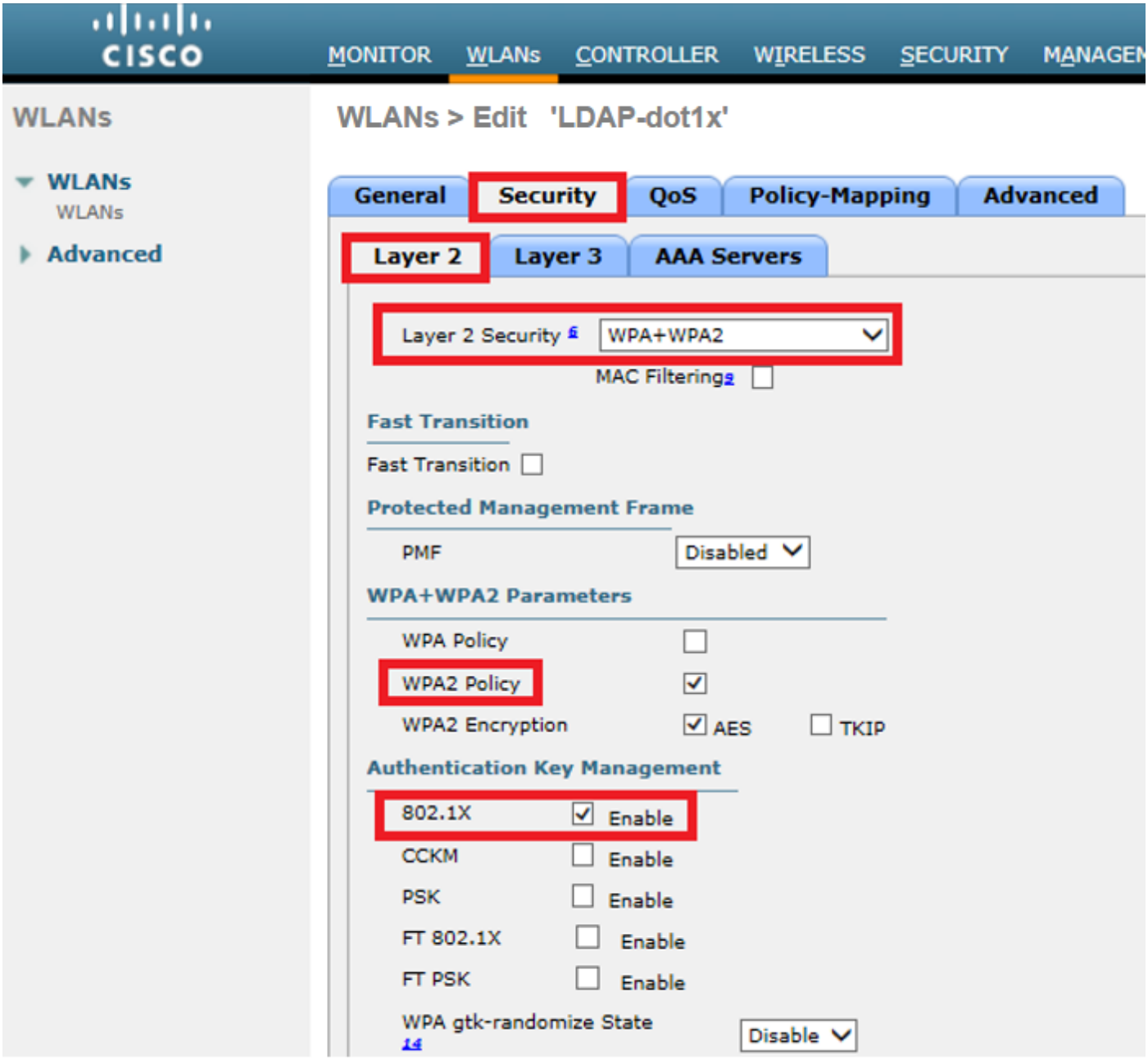
Stap 4. Stel de verificatievolgorde in op alleen Interne Gebruikers + LDAP of LDAP.

Stap 5. Maak de LDAP-dot1x WLAN aan.

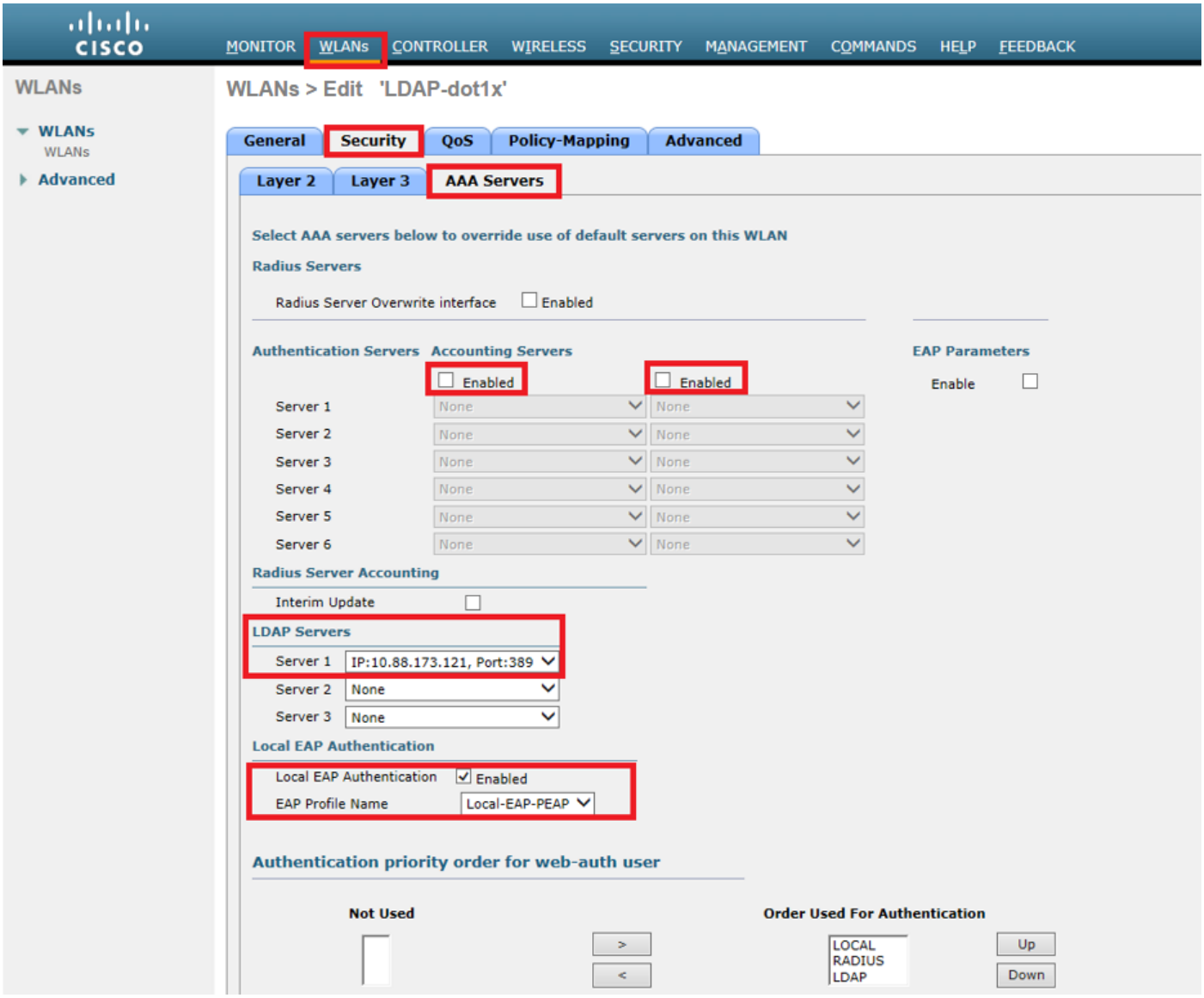




Stap 6. Stel de L2 beveiligingsmethode in op WPA2 + 802.1x en stel L3 beveiliging in op nul.



Stap 7. Schakel lokale EAP-verificatie in en zorg ervoor dat de opties voor verificatieservers en accountingservers worden uitgeschakeld en dat LDAP is ingeschakeld.



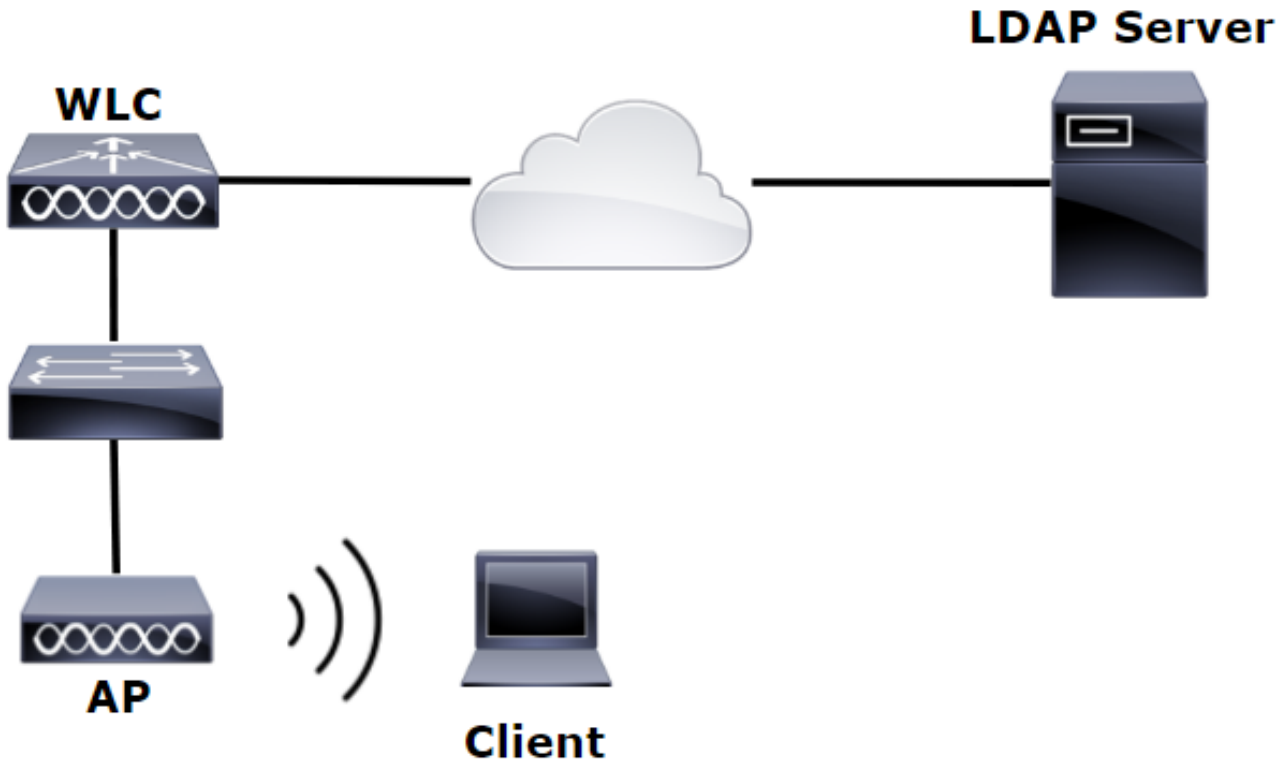
Alle andere instellingen kunnen standaard ingeschakeld worden.

Opmerkingen:
Gebruik het LDP-gereedschap om de configuratieparameters te bevestigen.
De Zoekbasis kan geen Groep zijn (zoals SofiaLabGroup).
PEAP-GTC of Cisco:PEAP moeten worden gebruikt in plaats van Microsoft:PEAP bij de aanvrager als het een Windows-machine is. Microsoft:PEAP werkt standaard met MacOS/iOS/Android.

WLAN's maken die op LDAP-server vertrouwen om gebruikers te verifiëren via het interne WLC-webportal

Netwerkdiagram

In dit scenario maakt WLAN LDAP-Web gebruik van een LDAP-server om de gebruikers te verifiëren met de interne WLC Web Portal.



Verzeker Stappen 1. door Stappen 4. zijn genomen van het vorige voorbeeld. Van daaruit wordt de WLAN-configuratie anders ingesteld.

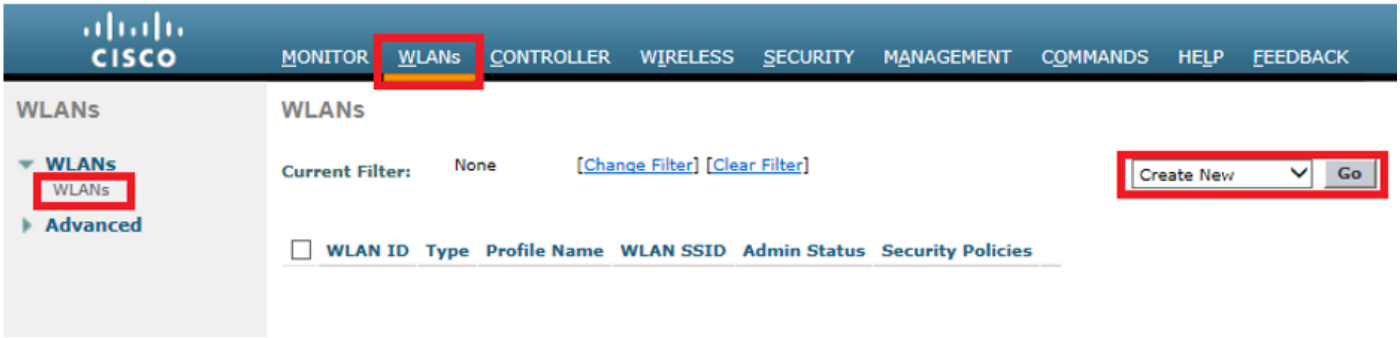
Stap 1. Maak een gebruiker **Gebruiker1** in het LDAP Server lid van de OU SofiaLabOU en de Groep SofiaLabGroup.

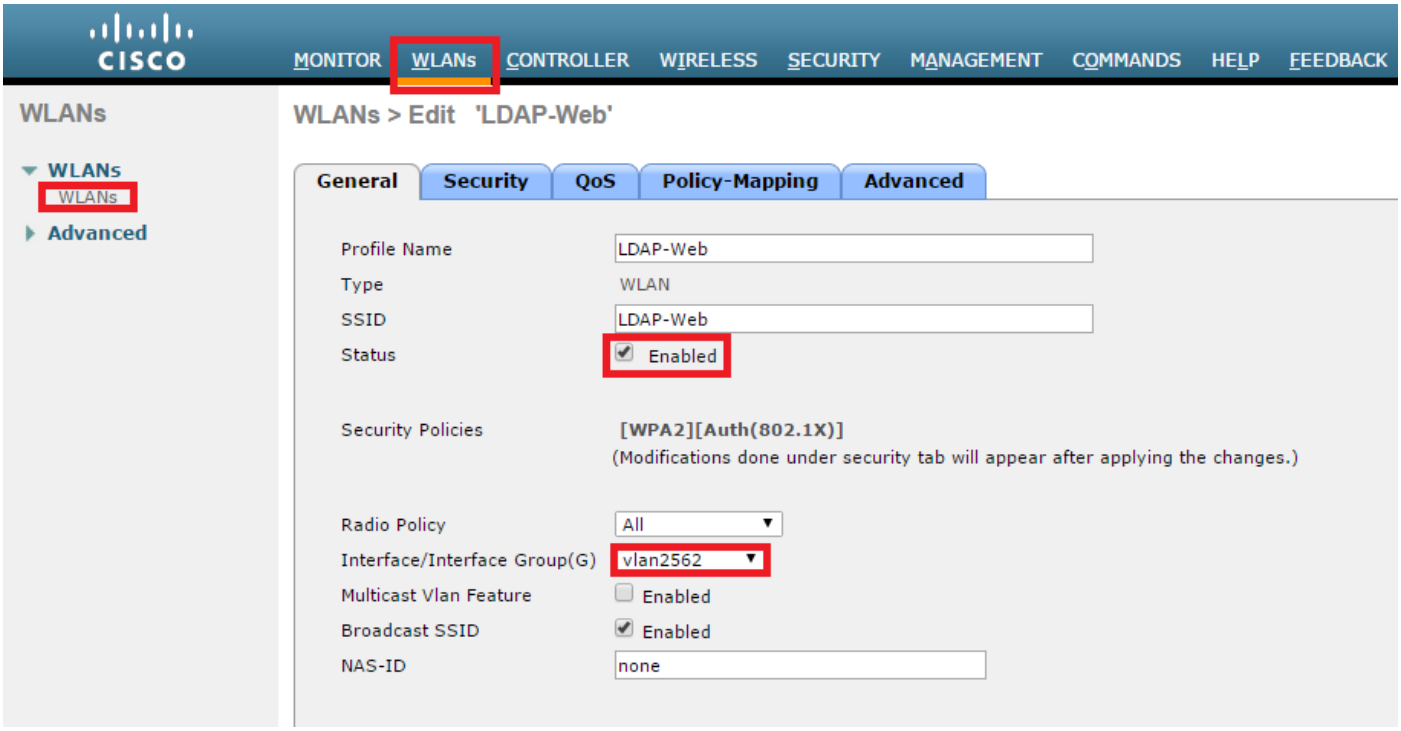
Stap 2. Maak een EAP-profiel bij de WLC met de gewenste EAP-methode (gebruik PEAP).

Stap 3. Bind de WLC met de LDAP Server.

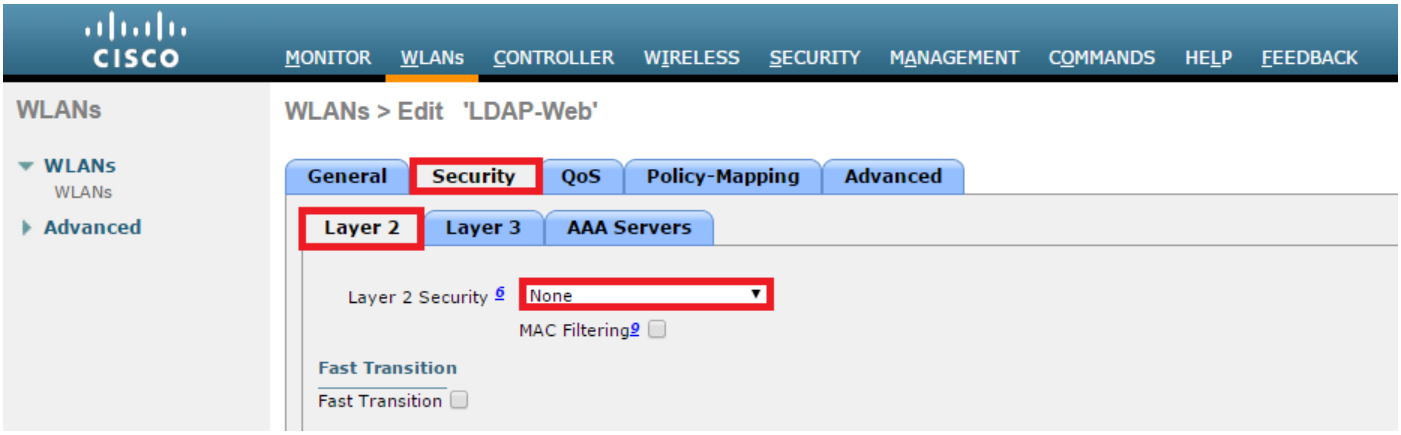
Stap 4. Stel de verificatievolgorde in op Interne gebruikers + LDAP.

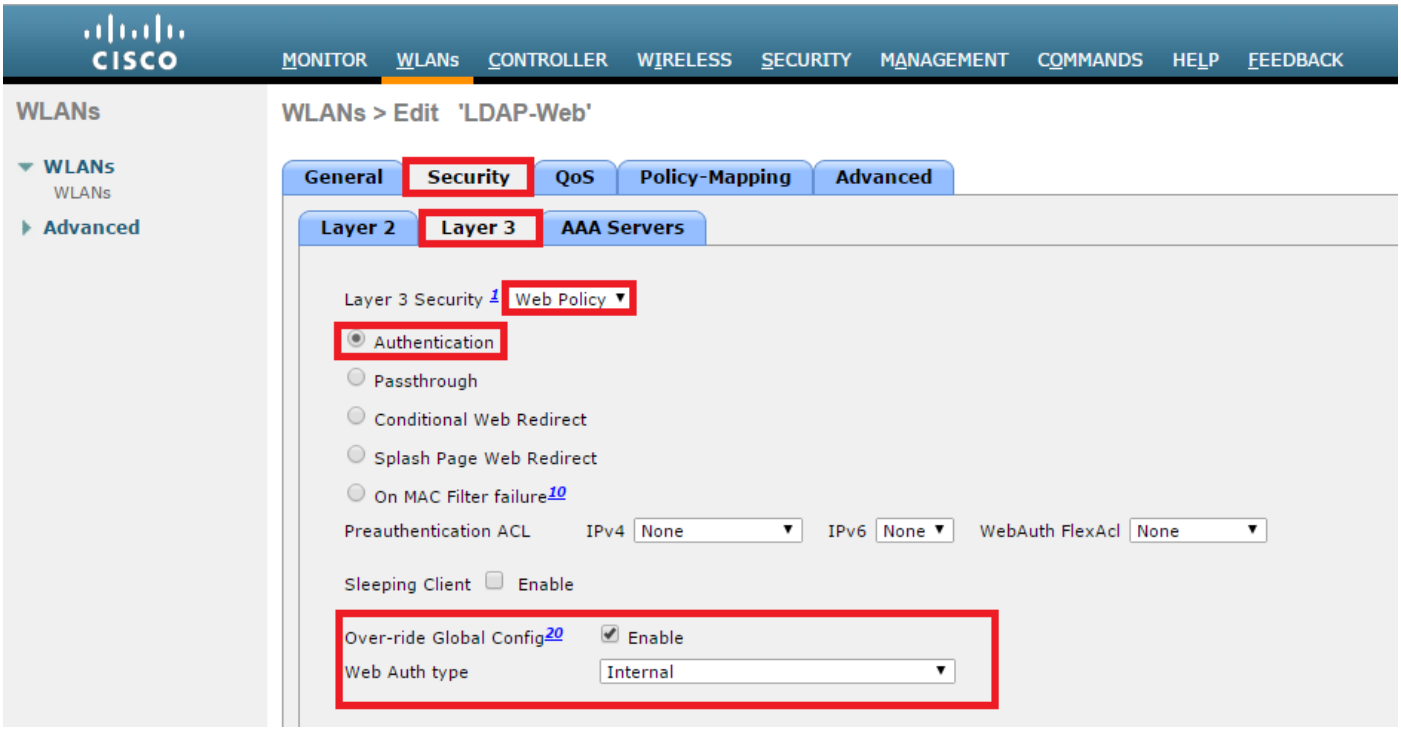
Stap 5. Maak het LDAP-Web WLAN zoals in de afbeeldingen wordt getoond.



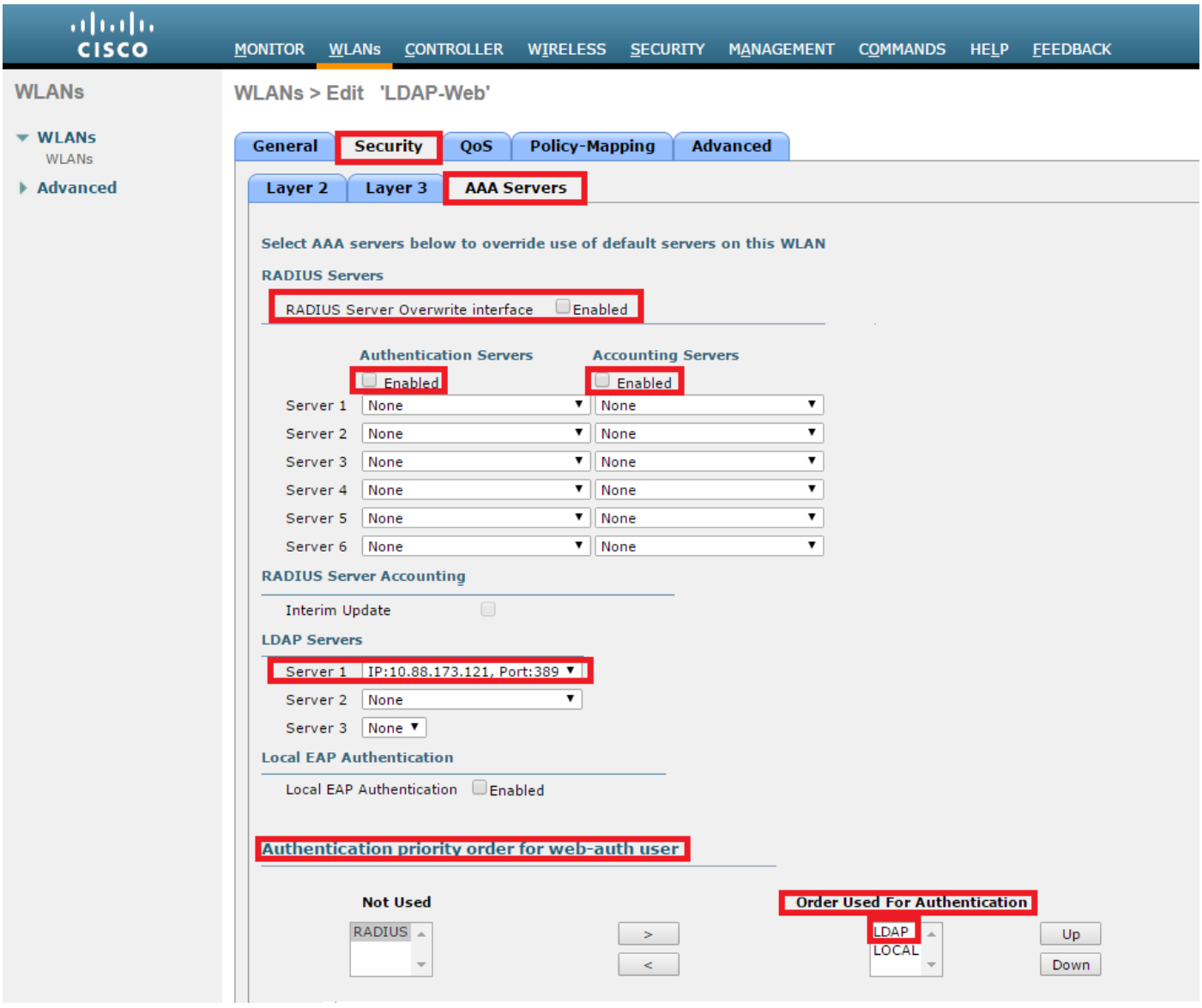


Stap 6. L2-beveiliging op nul en L3-beveiliging op webbeleid instellen - verificatiezoals in de afbeeldingen wordt getoond.





Stap 7. Stel de prioriteitsvolgorde voor de verificatie voor web-auth in om LDAP te gebruiken en zorg ervoor dat de opties voor de verificatieservers en de accountingservers zijn uitgeschakeld.

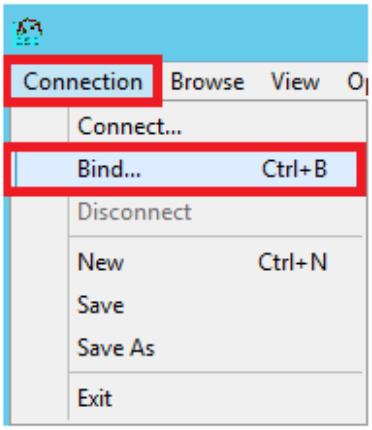


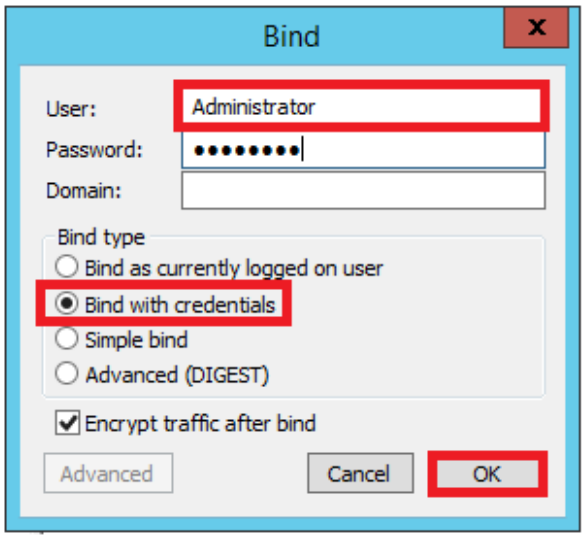
Alle andere instellingen kunnen standaard ingeschakeld worden.

Gebruik LDP-tool om LDAP te configureren en problemen op te lossen

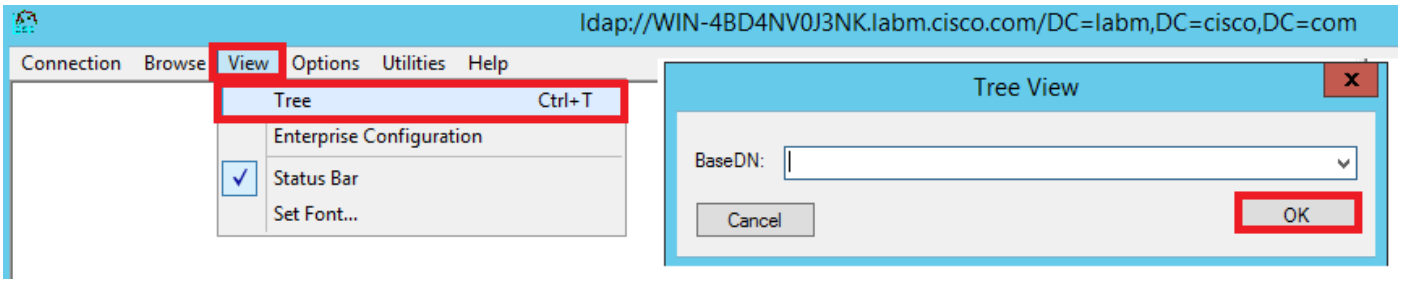
Stap 1. Open het LDP-gereedschap op de LDAP-server of op een host met connectiviteit (poort TCP 389 moet aan de server zijn toegestaan).

Stap 2. Navigeer naar **Verbinding > Bind,** log in met een beheerder gebruiker en selecteer **Bind met referenties** keuzerondje.

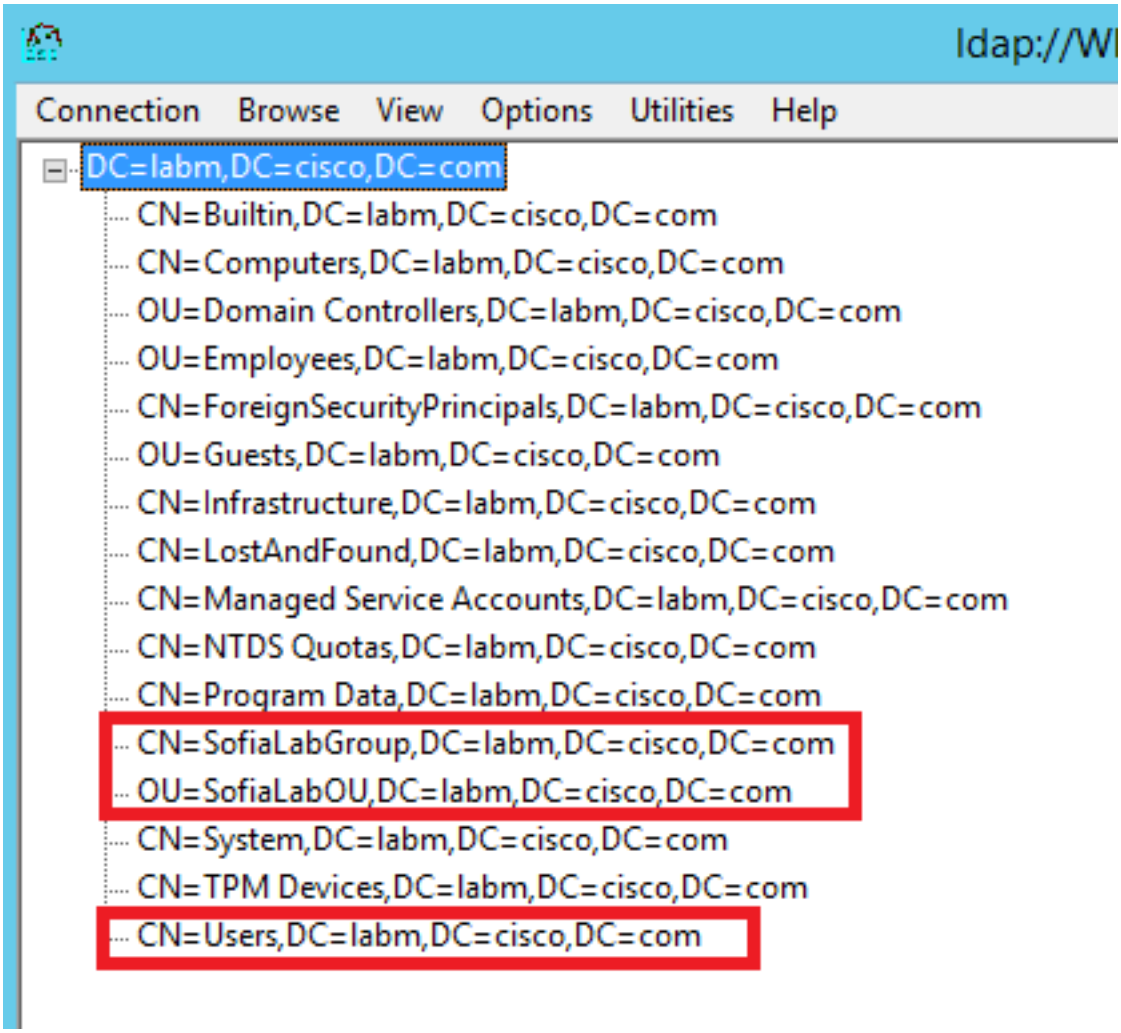




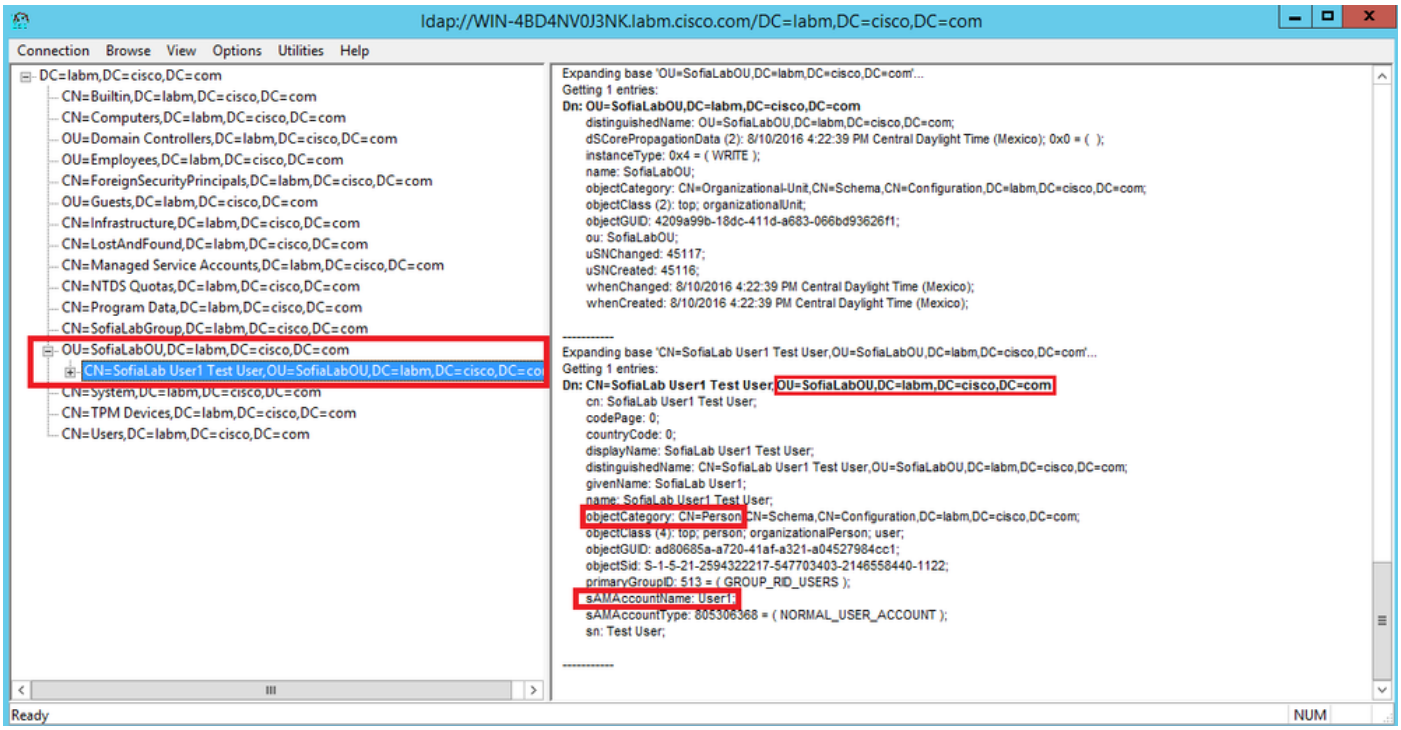
Stap 3. Navigeer naar **Beeld > Boom** en selecteer **OK** in de basis-DN.



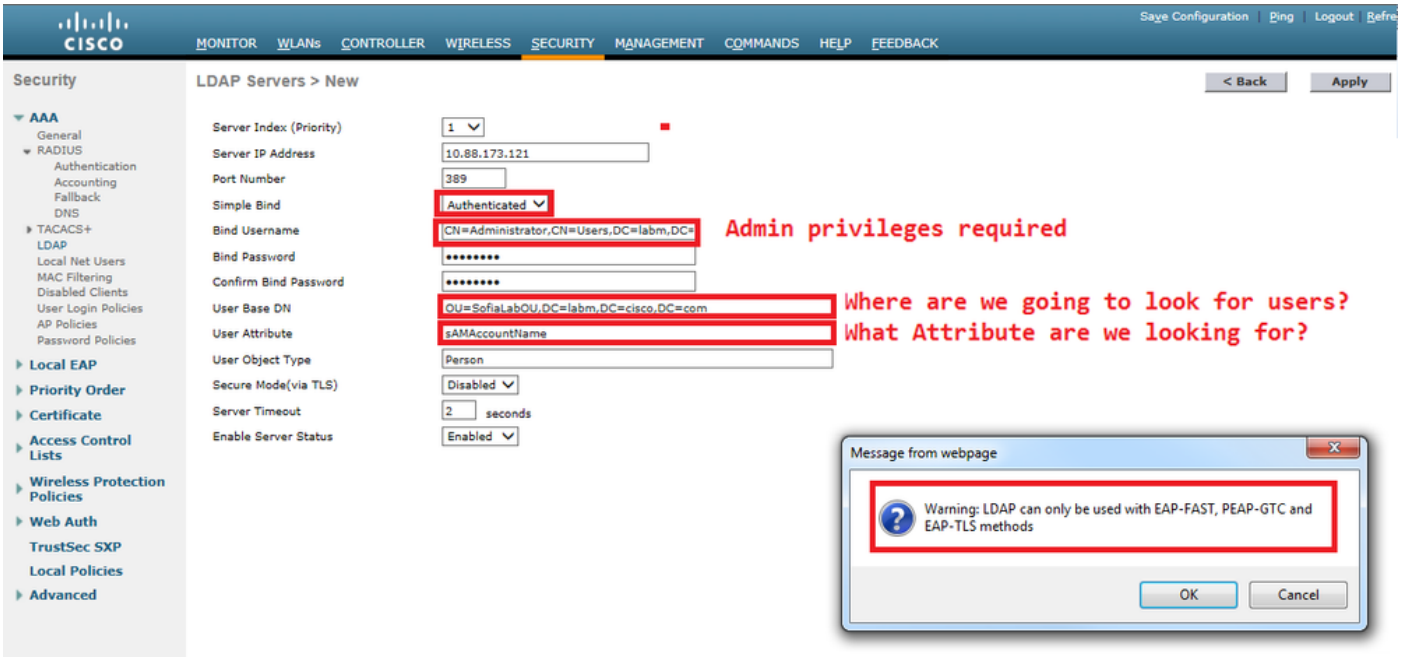
Stap 4. Breid de structuur uit om de structuur te bekijken en te zoeken naar de zoekbasis DN. Bedenk dat het elk containertype kan zijn, behalve Groepen. Het kan het hele domein zijn, een specifieke OU of een CN zoals CN=User.



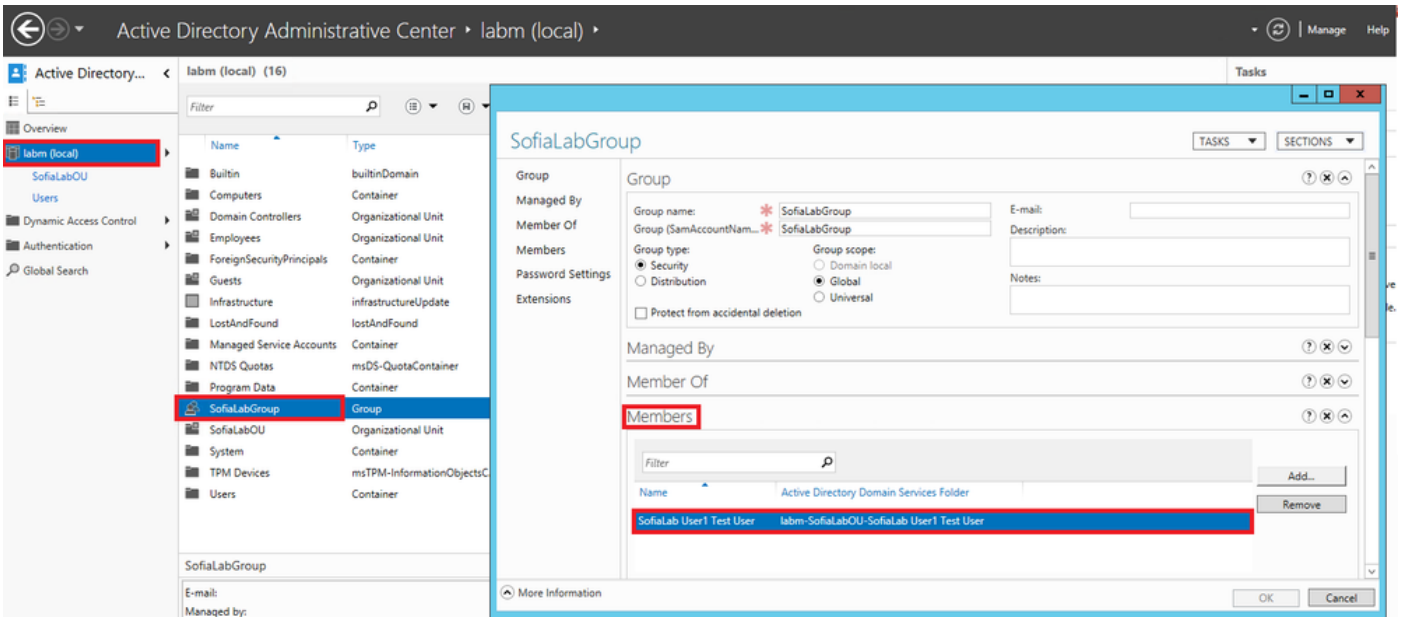
Stap 5. Breid de SofiaLabOU uit om te zien welke gebruikers er in zitten. Er is de Gebruiker1 die eerder is gemaakt.



Stap 6. Alles wat nodig is om LDAP te configureren.



Stap 7. Groepen zoals SofiaLabGroup kunnen niet worden gebruikt als een zoekopdracht-DN. Breid de groep uit en zoek naar de gebruikers erin, waar de eerder gemaakte Gebruiker1 moet zijnzoals getoond.



Gebruiker1 was er maar LDP kon het niet vinden. Het betekent dat de WLC niet in staat is om het ook te doen en dat is de reden waarom Groepen niet worden ondersteund als een Search Base DN.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

```
(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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

```
(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
```

Gerelateerde informatie

- LDAP - WLC 8.2 configuratiehandleiding
- Hoe te om Draadloze LAN Controller (WLC) voor Lichtgewicht Directory Access Protocol (LDAP) verificatie te configureren - door Vinay Sharma
- Webverificatie met LDAP op configuratievoorbeeld van draadloze LAN-controllers (WLCs) - door Yahya Jaber en Ayman Alfare

- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

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