Konfigurieren des WLC mit LDAP-Authentifizierung für 802.1x- und Web-Auth-WLANs

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Konfiguration eines AireOS-WLC beschrieben, um Clients mit einem LDAP-Server als Benutzerdatenbank zu authentifizieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Microsoft Windows Server
- Active Directory

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco WLC Software 8.2.110.0
- Microsoft Windows Server 2012 R2

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

Hintergrundinformationen

Technischer Hintergrund

- LDAP ist ein Protokoll für den Zugriff auf Verzeichnisserver.
- Verzeichnisserver sind hierarchische, objektorientierte Datenbanken.
- Objekte werden in Containern wie Organisationseinheiten (OU), Gruppen oder Microsoft-Standardcontainern als CN=Users organisiert.
- Der schwierigste Teil dieser Konfiguration ist die korrekte Konfiguration der LDAP-Serverparameter auf dem WLC.

Weitere Informationen zu diesen Konzepten finden Sie im Abschnitt Einführung in So konfigurieren Sie den Wireless LAN Controller (WLC) für die LDAP-Authentifizierung (Lightweight Directory Access Protocol).

Häufig gestellte Fragen

- Welcher Benutzername muss für die Verbindung mit dem LDAP-Server verwendet werden?

Es gibt zwei Möglichkeiten, eine Bindung mit einem LDAP-Server herzustellen: Anonym oder Authentifiziert (siehe , um den Unterschied zwischen beiden Methoden zu verstehen).

Dieser bindende Benutzername muss über Administratorrechte verfügen, um nach anderen Benutzernamen/Kennwörtern abfragen zu können.

- Wenn authentifiziert: Befindet sich der bind-Benutzername im selben Container wie alle Benutzer?

Nein: den gesamten Pfad verwenden. Beispiele:

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

Ja: Verwenden Sie nur den Benutzernamen. Beispiele:

Administrator

- Was geschieht, wenn sich Benutzer in verschiedenen Containern befinden? Müssen sich alle beteiligten Wireless-LDAP-Benutzer im gleichen Container befinden?

Nein, es kann ein Basis-DN angegeben werden, der alle erforderlichen Container enthält.

- Nach welchen Attributen muss der WLC suchen?

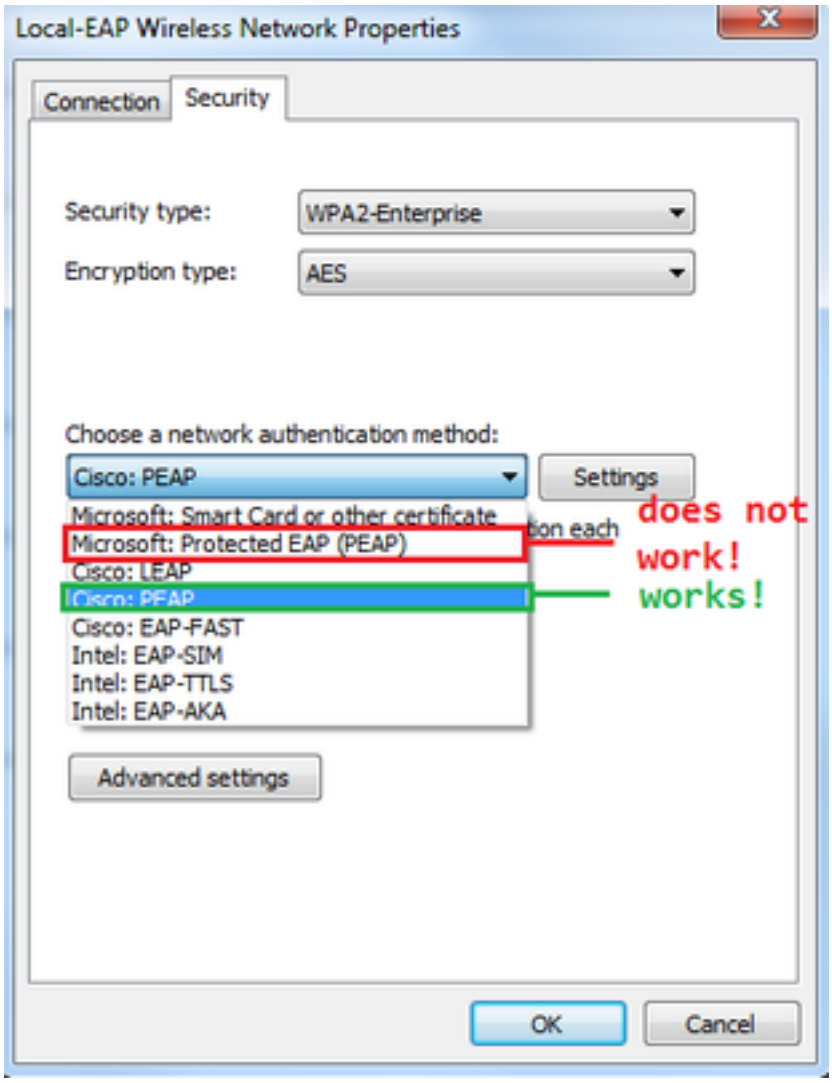
Der WLC entspricht dem angegebenen Benutzerattribut und Objekttyp.

> **Hinweis**: **sAMAccountName** unterscheidet zwischen Groß- und Kleinschreibung, aber Person nicht. Daher sind **sAMAccountName=RICARDO** und **sAMAccountName=ricardo** identisch und funktionieren, während **samaccountname=RICARDO** und **samaccountname=ricardo** dies nicht tun.

- Welche Extensible Authentication Protocol (EAP)-Methoden können verwendet werden?

Nur EAP-FAST, PEAP-GTC und EAP-TLS. Standardkomponenten für Android, iOS und MacOS können mit dem Protected Extensible Authentication Protocol (PEAP) verwendet werden.

Unter Windows muss AnyConnect Network Access Manager (NAM) oder die Standard-Windows-Komponente mit Cisco:PEAP auf unterstützten Wireless-Adaptern verwendet werden, wie im Bild gezeigt.

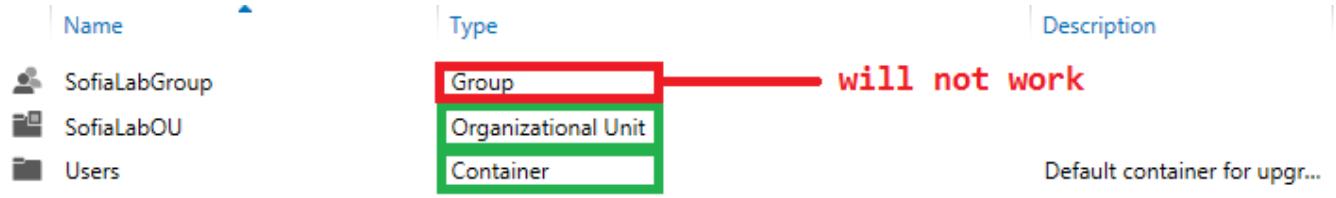


> **Hinweis:** Die Cisco EAP-Plug-ins für Windows enthalten eine Version von Open Secure Socket Layer (OpenSSL 0.9.8k), die von der Cisco Bug-ID CSCva09670 betroffen ist. Cisco plant nicht, weitere Versionen der EAP-Plug-ins für Windows herauszugeben, und empfiehlt, stattdessen den AnyConnect Secure Mobility Client zu verwenden. 1.

- Warum kann der WLC keine Benutzer finden?

Benutzer innerhalb einer Gruppe können nicht authentifiziert werden. Sie müssen sich in einem

Standardcontainer (CN) oder einer Organisationseinheit (OU) befinden, wie im Bild gezeigt.



Konfigurieren

Es gibt verschiedene Szenarien, in denen ein LDAP-Server verwendet werden kann, entweder mit 802.1x-Authentifizierung oder Web-Authentifizierung.

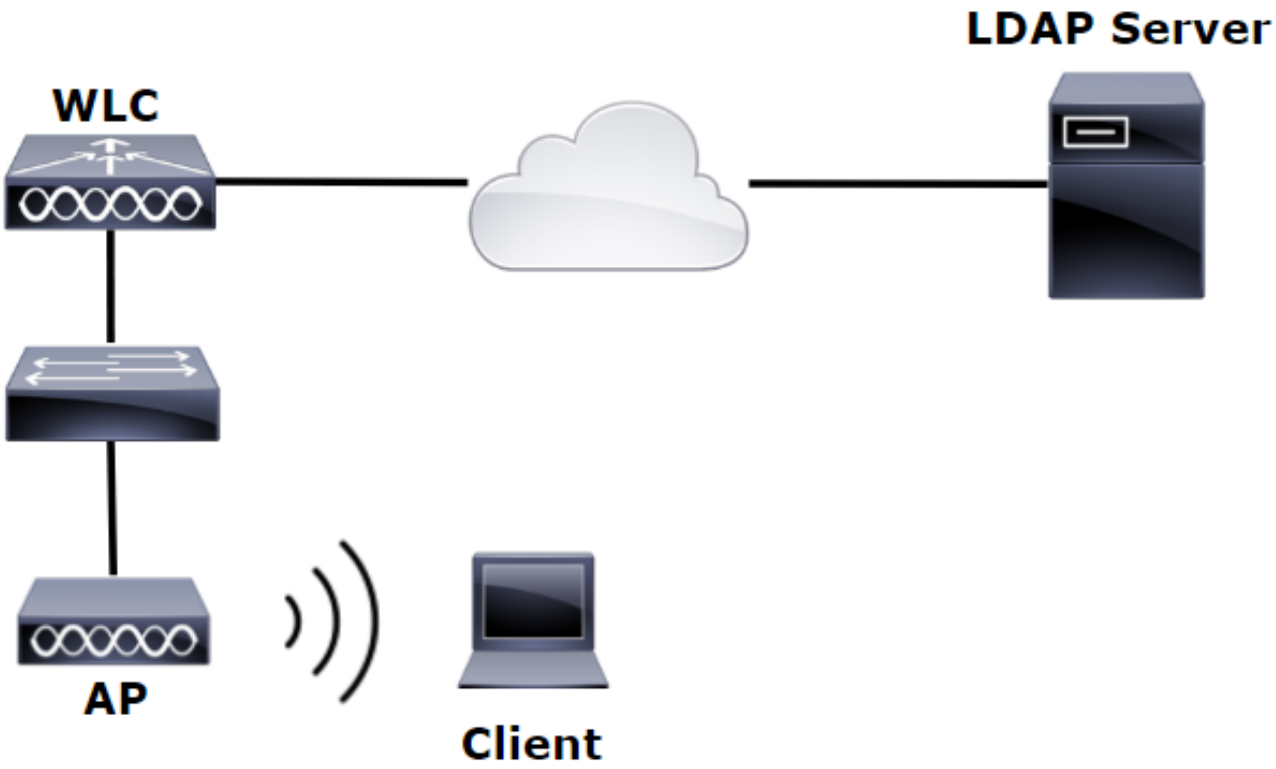
Für dieses Verfahren müssen nur Benutzer innerhalb der OU=SofiaLabOU authentifiziert werden.

Informationen zur Verwendung des LDP-Tools (Label Distribution Protocol) zum Konfigurieren und Beheben von LDAP-Problemen finden Sie im WLC LDAP-Konfigurationshandbuch.

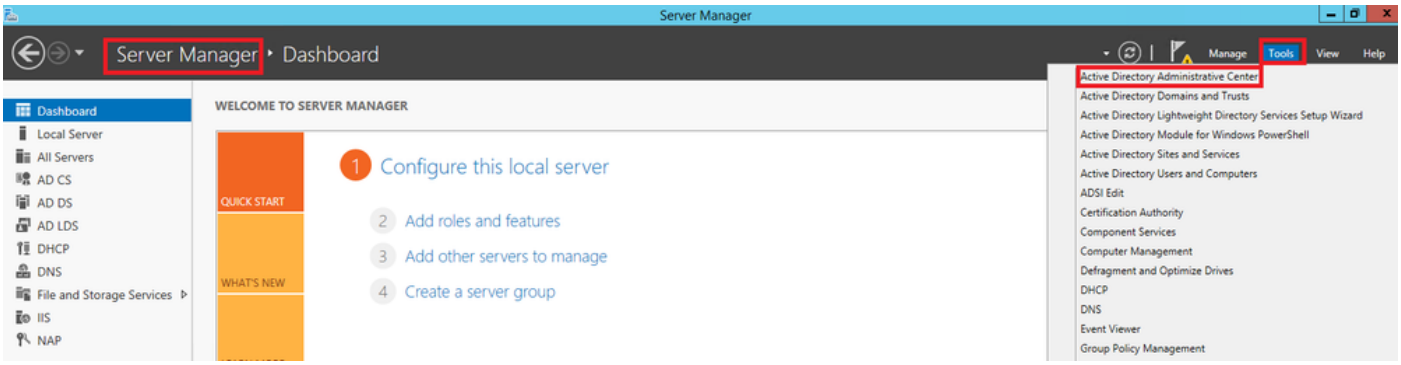
Erstellen eines WLAN, das sich auf den LDAP-Server stützt, um Benutzer über 802.1x zu authentifizieren

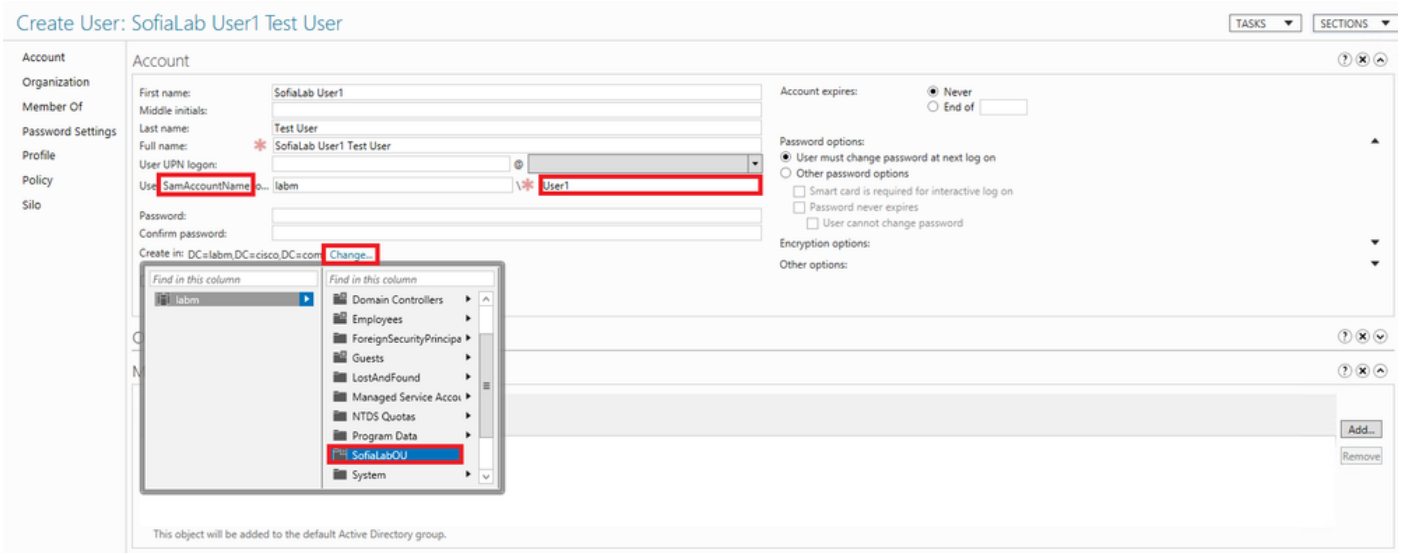
Netzwerkdiagramm

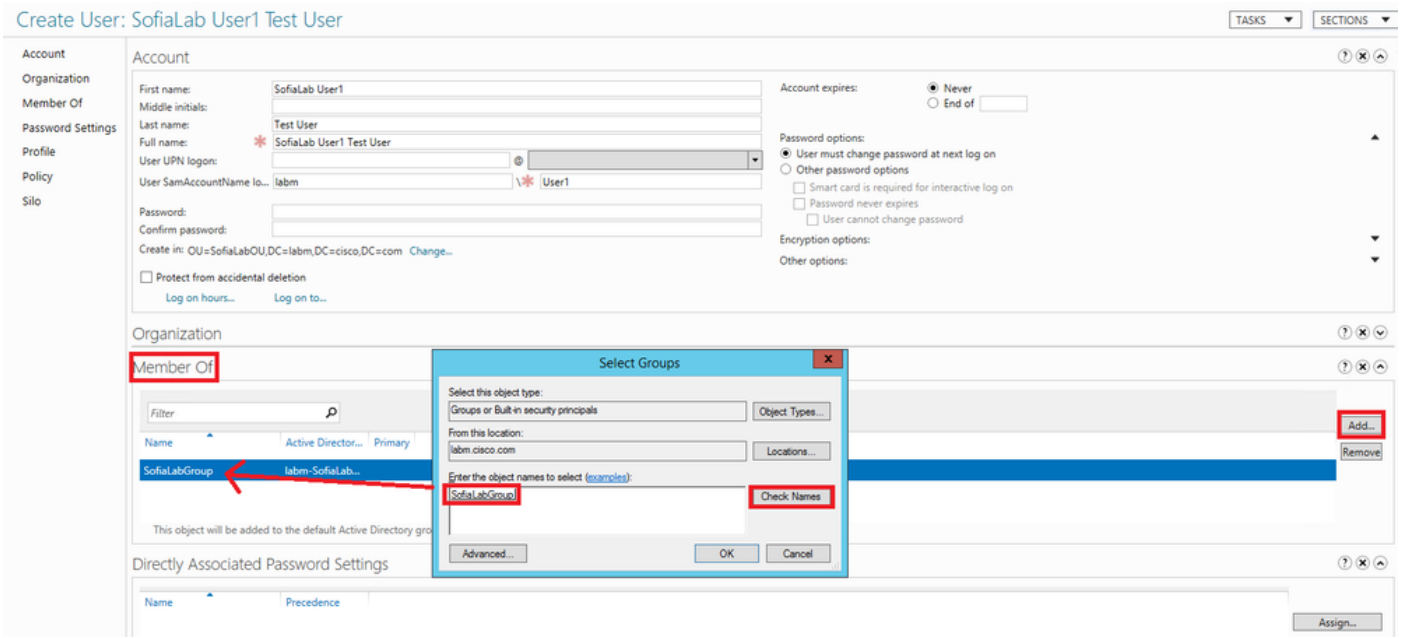
In diesem Szenario verwendet LDAP-dot1x im WLAN einen LDAP-Server, um die Benutzer mithilfe von 802.1x zu authentifizieren.



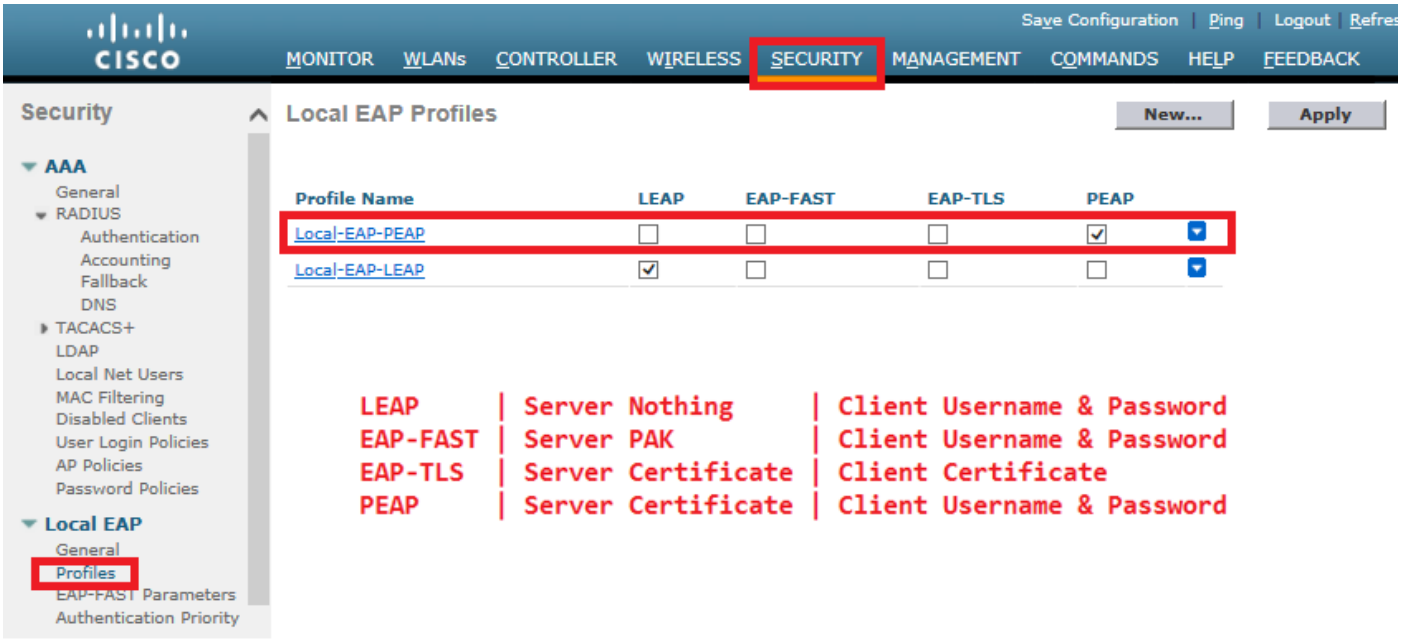
Schritt 1: Erstellen Sie einen Benutzer **User1** im LDAP-Servermitglied der SofiaLabOU und der SofiaLabGroup.





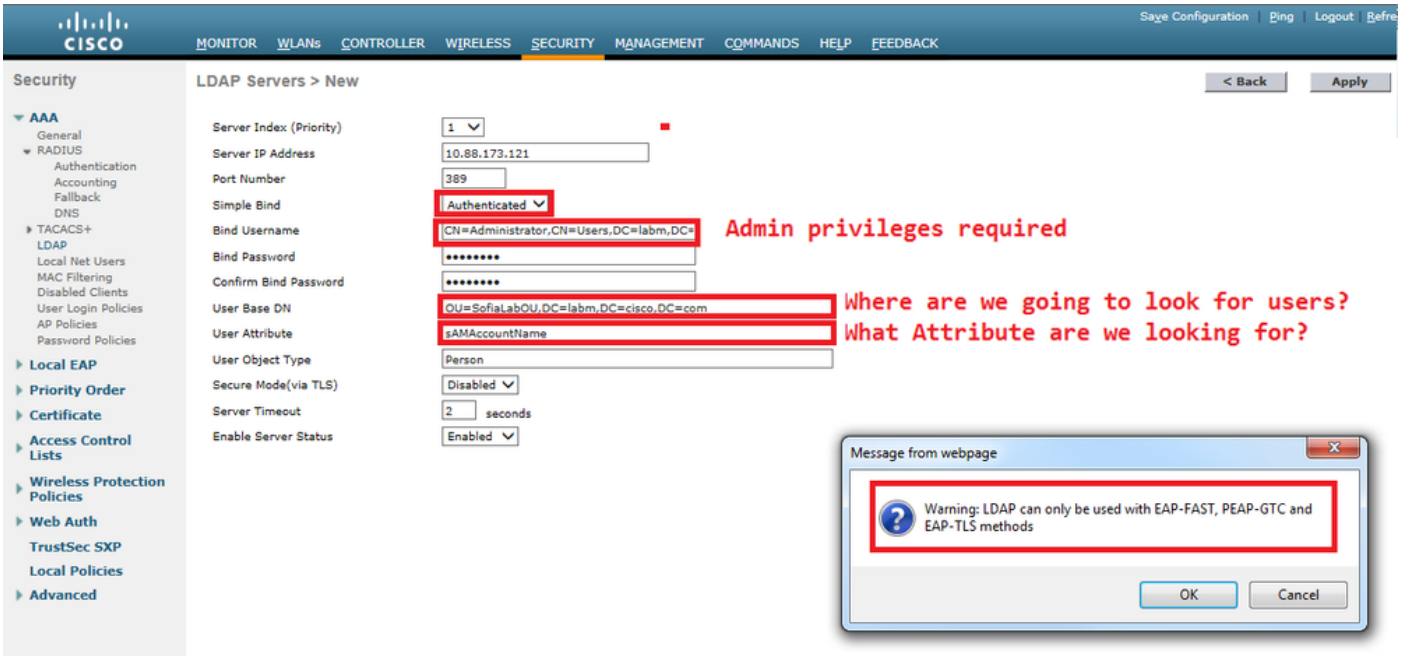


Schritt 2: Erstellen Sie ein EAP-Profil am WLC mit der gewünschten EAP-Methode (verwenden Sie PEAP).



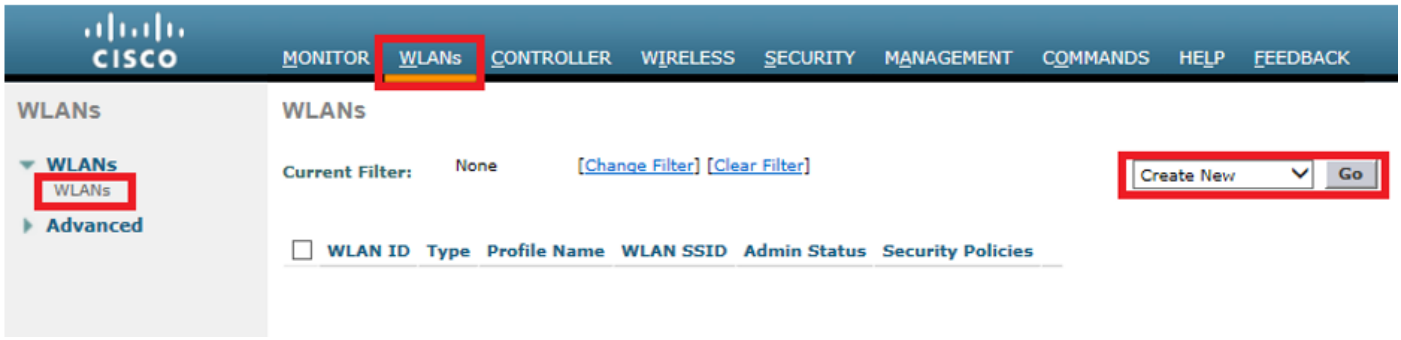
Schritt 3: Anbinden des WLC an den LDAP-Server.

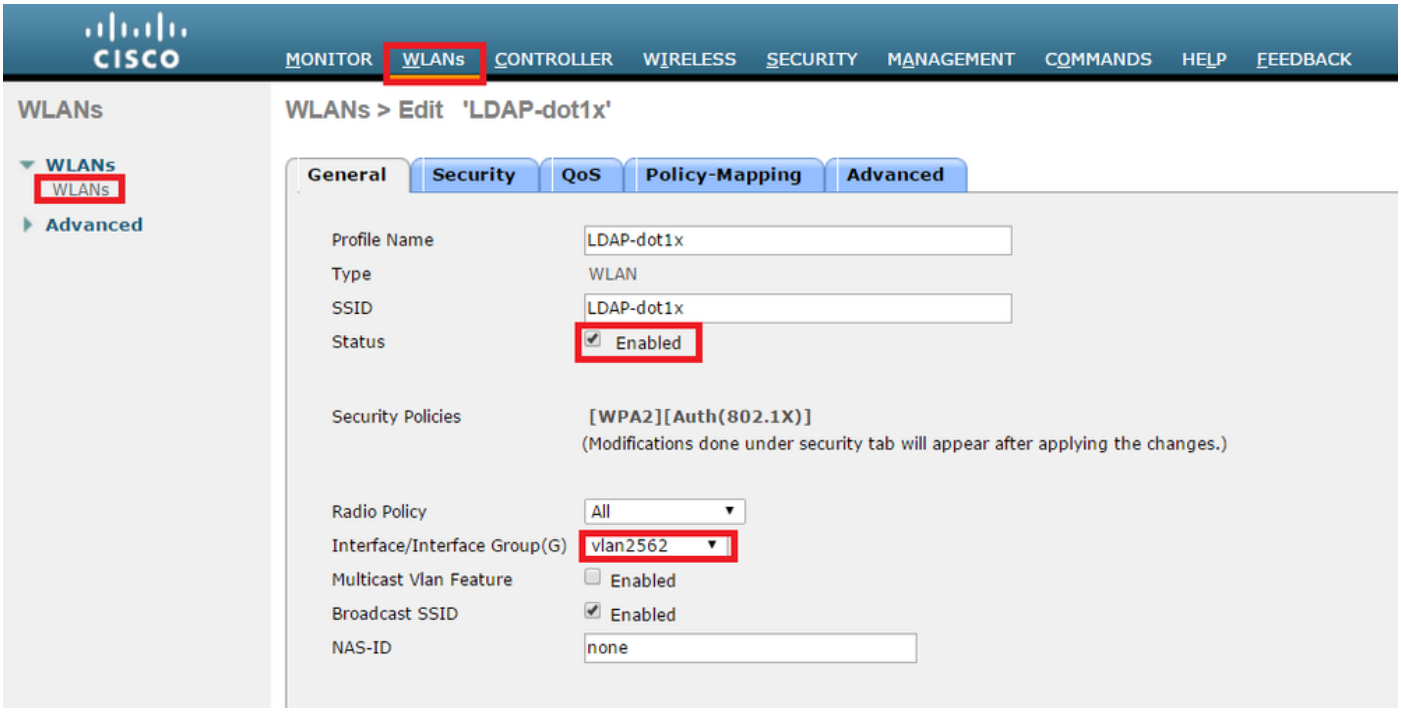
Tipp: Wenn der bind-Benutzername nicht in der DN der Benutzerbasis enthalten ist, müssen Sie den gesamten Pfad zum **Admin-**Benutzer wie im Bild dargestellt eingeben. Andernfalls können Sie einfach **Administrator** eingeben.



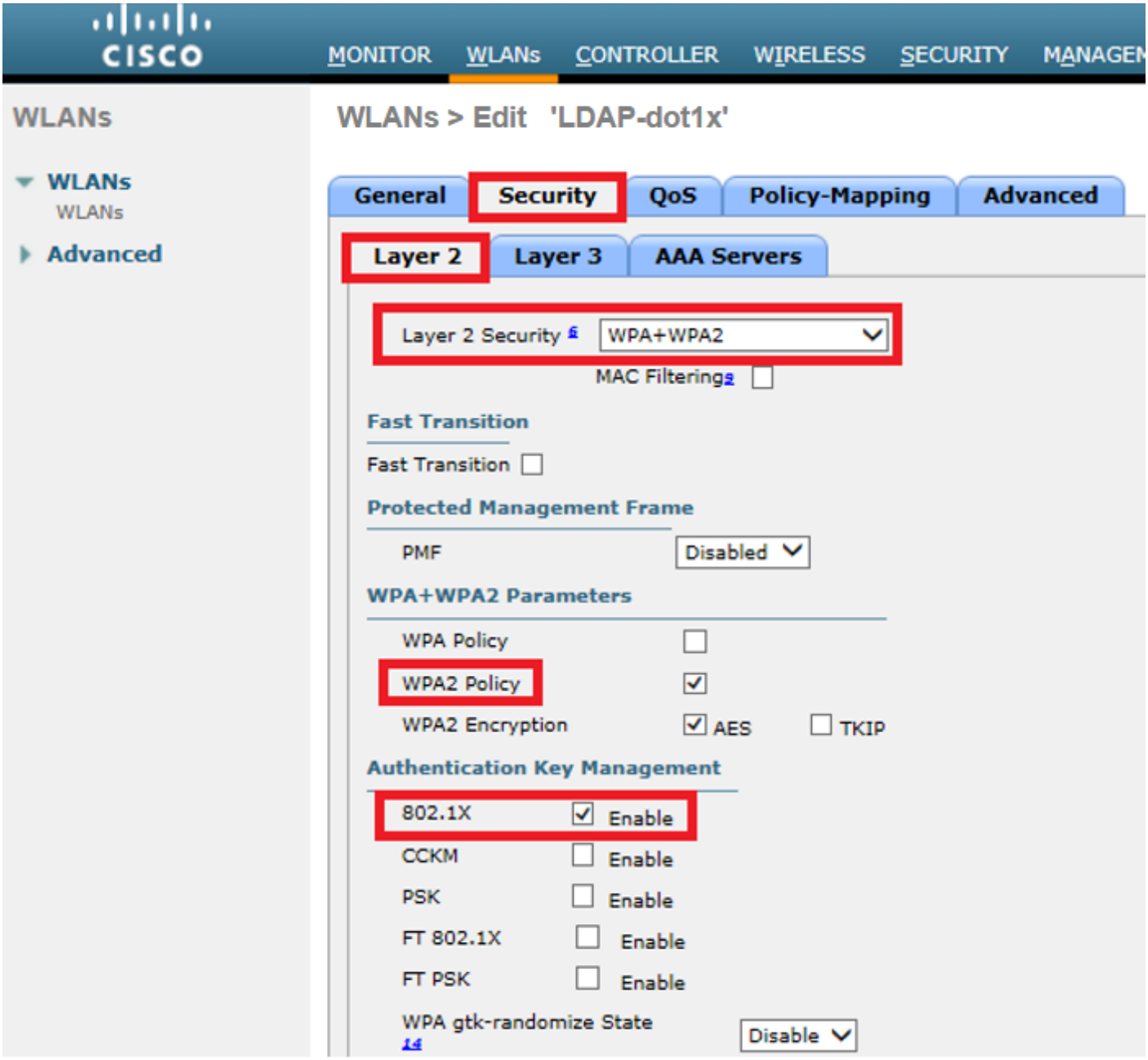
Schritt 4: Legen Sie die Authentifizierungsreihenfolge auf "Interne Benutzer + LDAP" oder "Nur LDAP" fest.

Schritt 5: Erstellen Sie das LDAP-dot1x-WLAN.

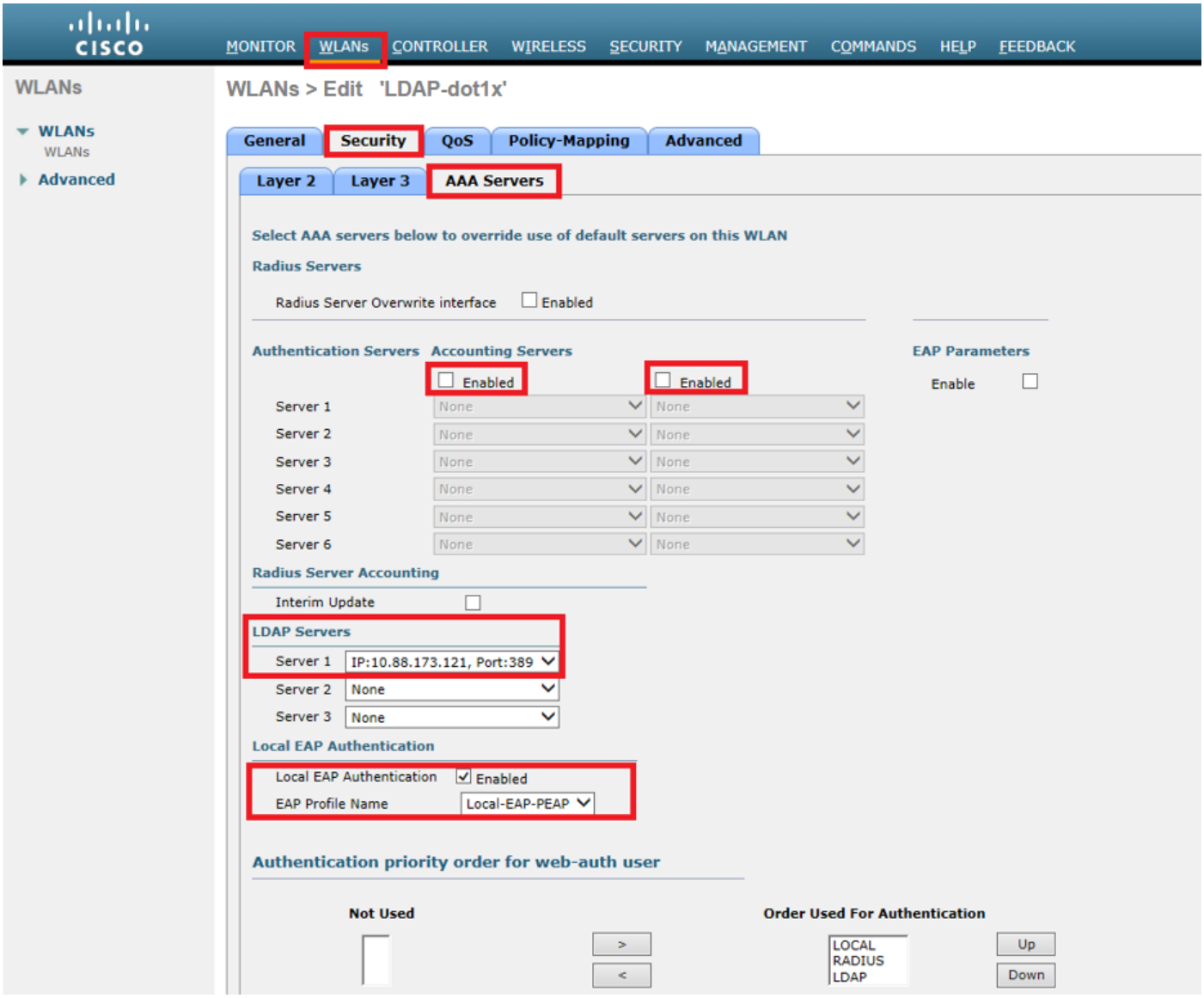




Schritt 6: Legen Sie für die L2-Sicherheitsmethode WPA2 + 802.1x und für die L3-Sicherheit None fest.



Schritt 7. Aktivieren Sie die lokale EAP-Authentifizierung, und stellen Sie sicher, dass die Optionen für Authentifizierungsserver und Buchungsserver deaktiviert und LDAP aktiviert sind.



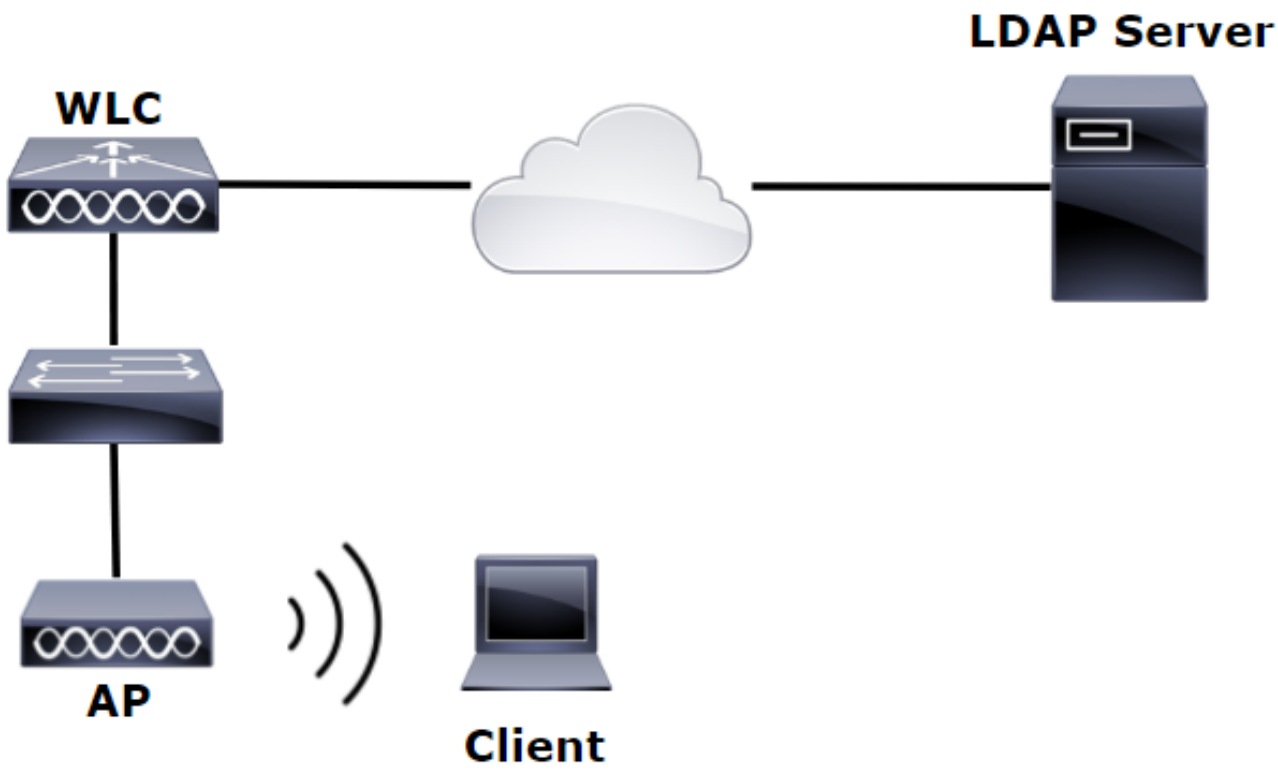
Alle anderen Einstellungen können auf den Standardeinstellungen belassen werden.

Hinweise:
Verwenden Sie das LDP-Tool, um die Konfigurationsparameter zu bestätigen.
Bei der Suchbasis kann es sich nicht um eine Gruppe (z. B. SofiaLabGroup) handeln.
PEAP-GTC oder Cisco:PEAP müssen anstelle von Microsoft:PEAP am Supplicant verwendet werden, wenn es sich um einen Windows-Rechner handelt. Microsoft:PEAP funktioniert standardmäßig mit MacOS/iOS/Android.

Erstellen eines WLAN, das auf dem LDAP-Server für die Benutzerauthentifizierung über das interne WLC-Webportal basiert

Netzwerkdiagramm

In diesem Szenario verwendet WLAN LDAP-Web einen LDAP-Server, um die Benutzer des internen WLC-Webportals zu authentifizieren.



Stellen Sie sicher, dass die Schritte 1 bis 4 aus dem vorherigen Beispiel übernommen wurden. Anschließend wird die WLAN-Konfiguration anders festgelegt.

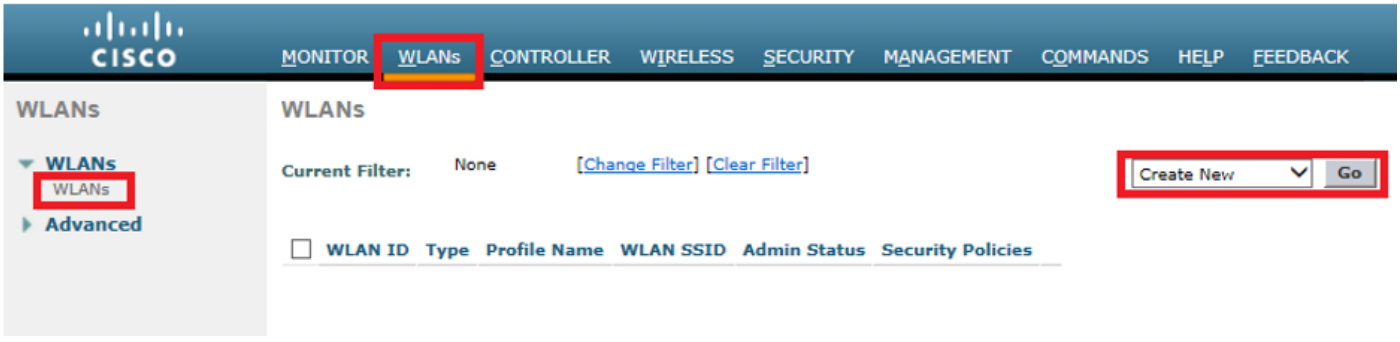
Schritt 1: Erstellen Sie einen Benutzer **User1** im LDAP-Servermitglied der OU SofiaLabOU und der Gruppe SofiaLabGroup.

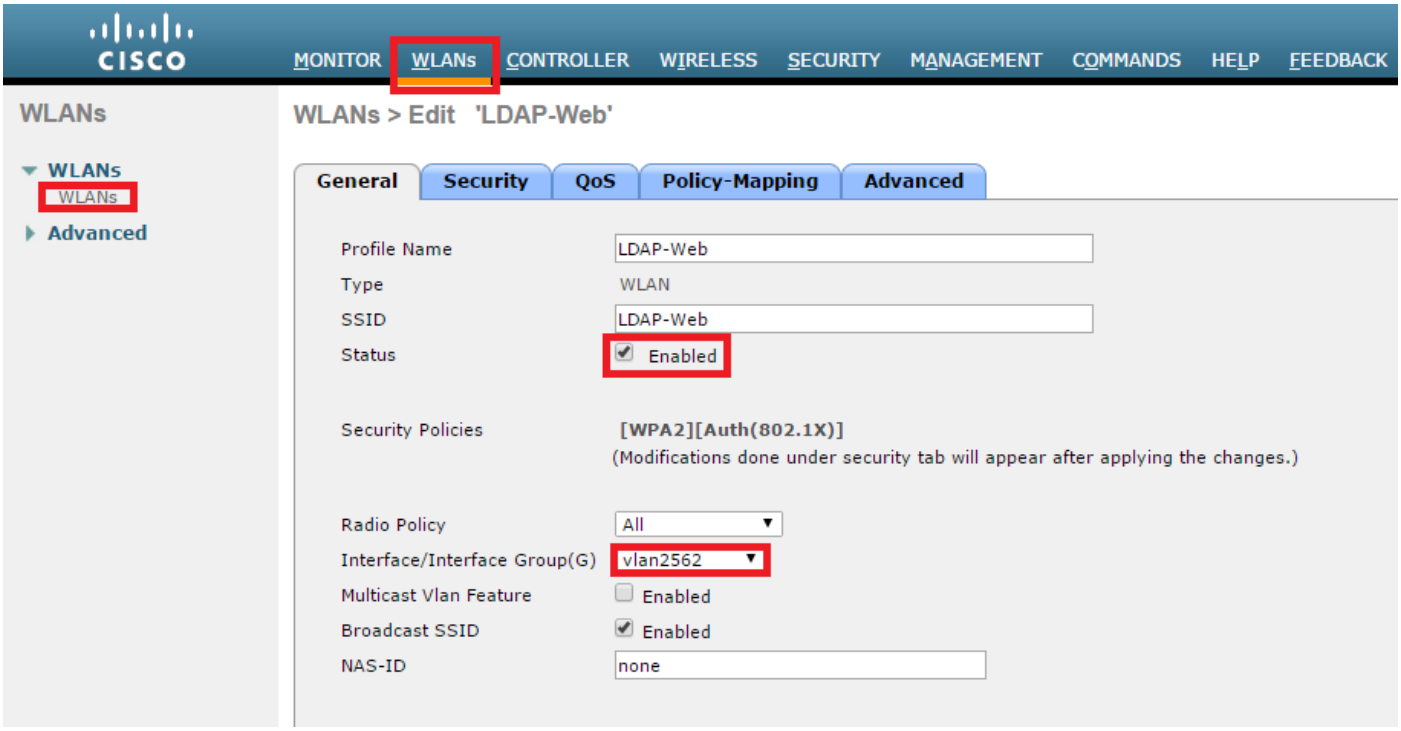
Schritt 2: Erstellen Sie ein EAP-Profil am WLC mit der gewünschten EAP-Methode (verwenden Sie PEAP).

Schritt 3: Anbinden des WLC an den LDAP-Server

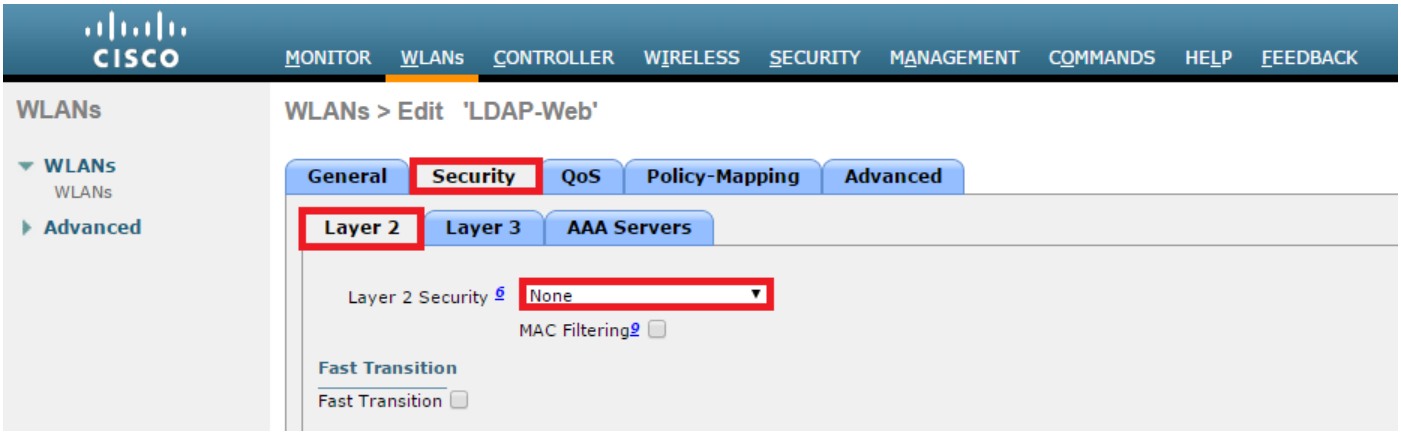
Schritt 4: Legen Sie die Authentifizierungsreihenfolge auf "Interne Benutzer + LDAP" fest.

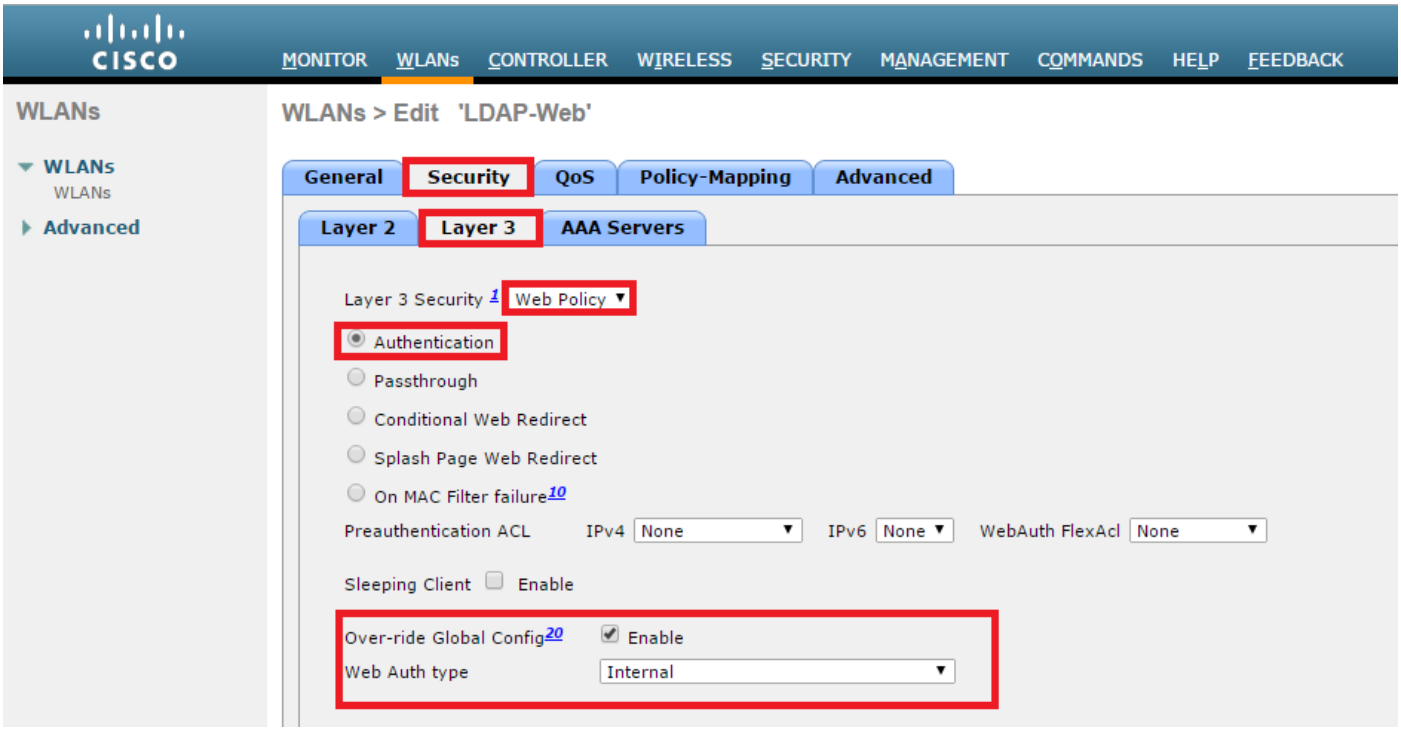
Schritt 5: Erstellen Sie das LDAP-Web-WLAN, wie in den Bildern dargestellt.



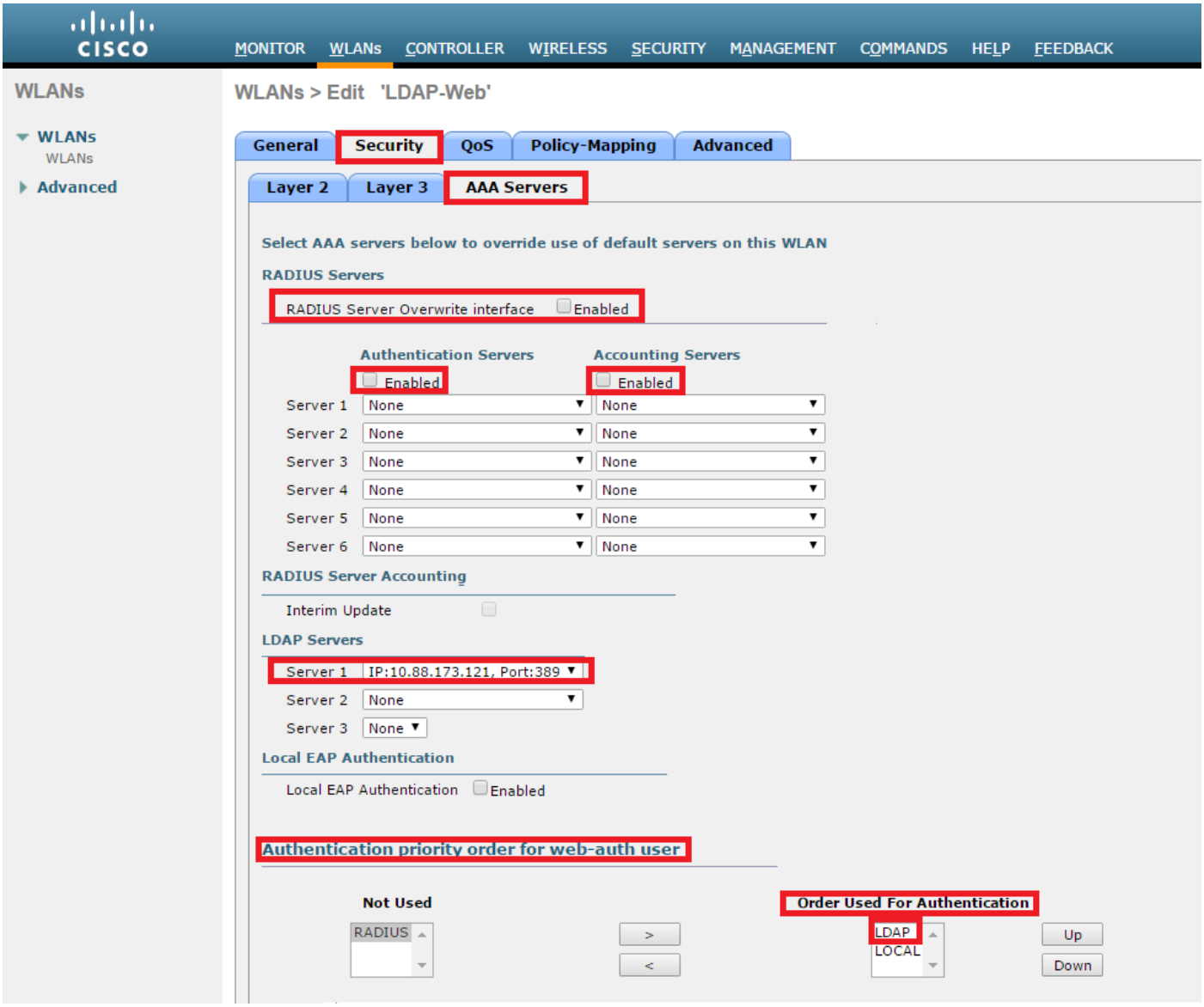


Schritt 6: L2-Sicherheit auf "none" und L3-Sicherheit auf "Web Policy" setzen - Authentifizierungwie in den Bildern dargestellt.





Schritt 7. Legen Sie die Prioritätsreihenfolge der Authentifizierung für die Webauthentifizierung fest, sodass LDAP verwendet wird, und stellen Sie sicher, dass die Optionen für Authentifizierungsserver und Abrechnungsserver deaktiviert sind.



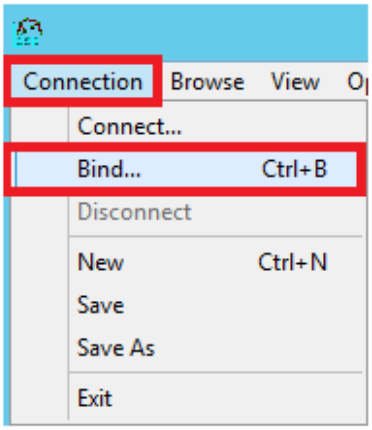
Alle anderen Einstellungen können auf den Standardeinstellungen belassen werden.

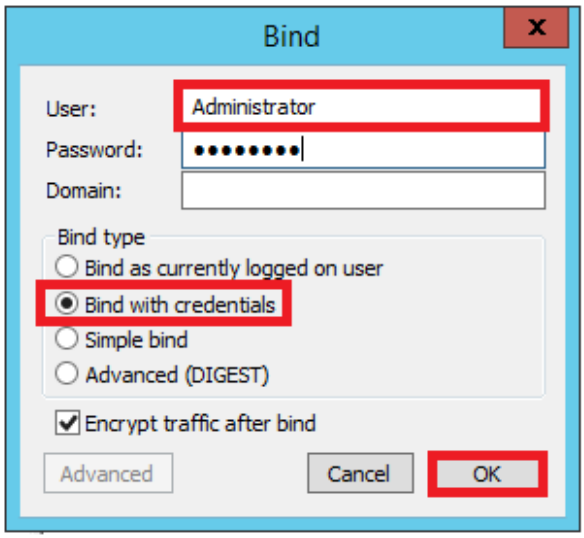
Verwenden des LDP-Tools zum Konfigurieren und Beheben von LDAP-Problemen

Schritt 1: Öffnen Sie das LDP-Tool entweder auf dem LDAP-Server oder auf einem Host mit Konnektivität (Port TCP 389 muss zum Server zugelassen sein).

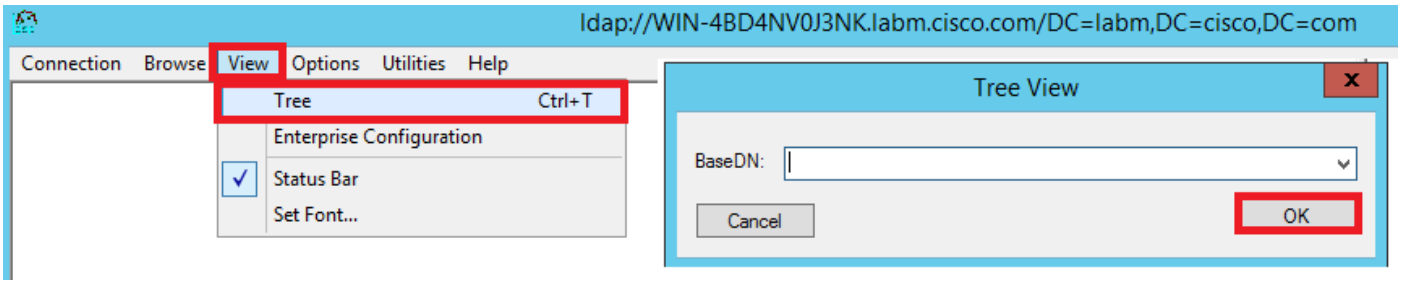
Schritt 2: Navigieren Sie zu **Verbindung > Binden,** melden Sie sich bei einem Administrator-

Benutzer an, und wählen Sie das Optionsfeld **Mit Anmeldeinformationen binden aus**.

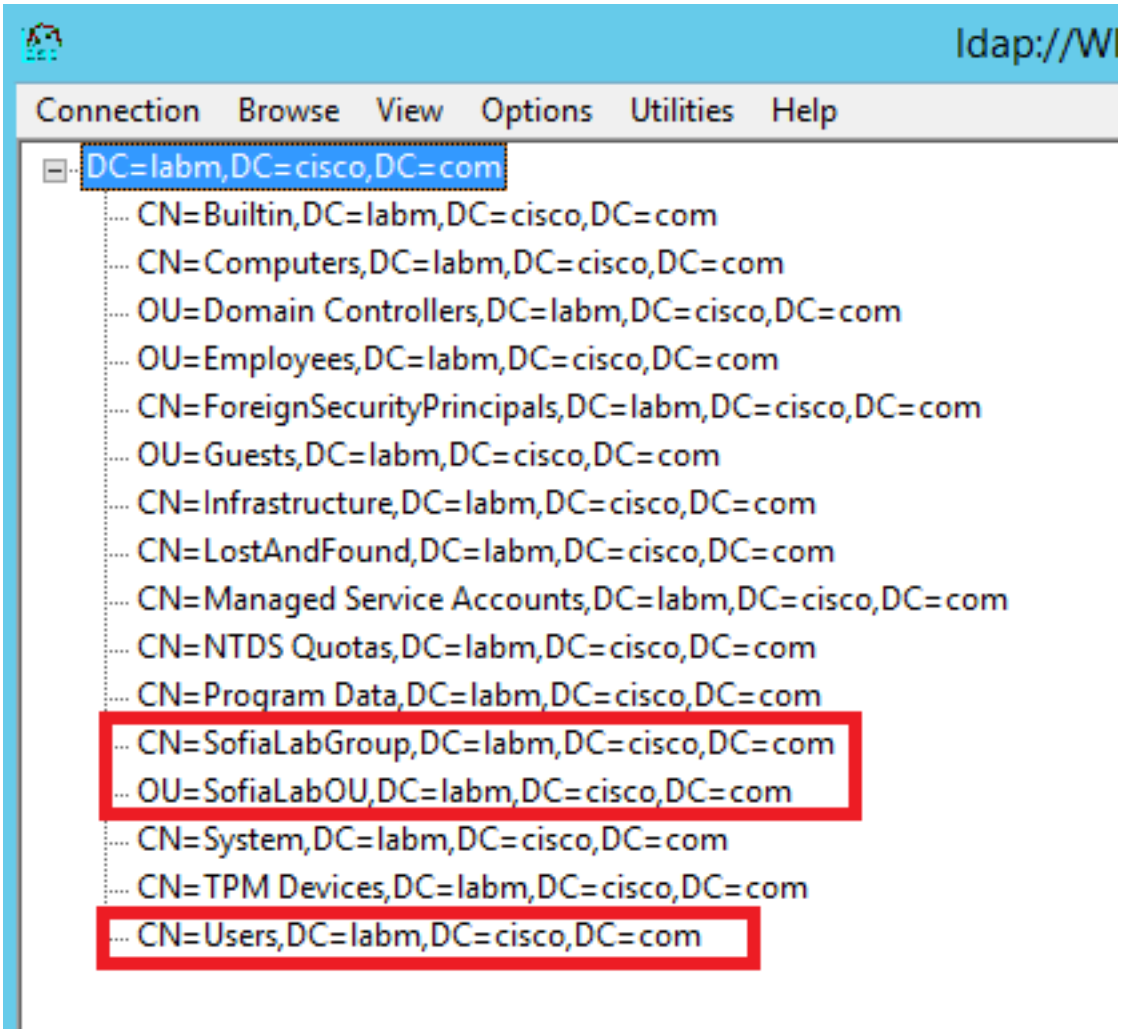




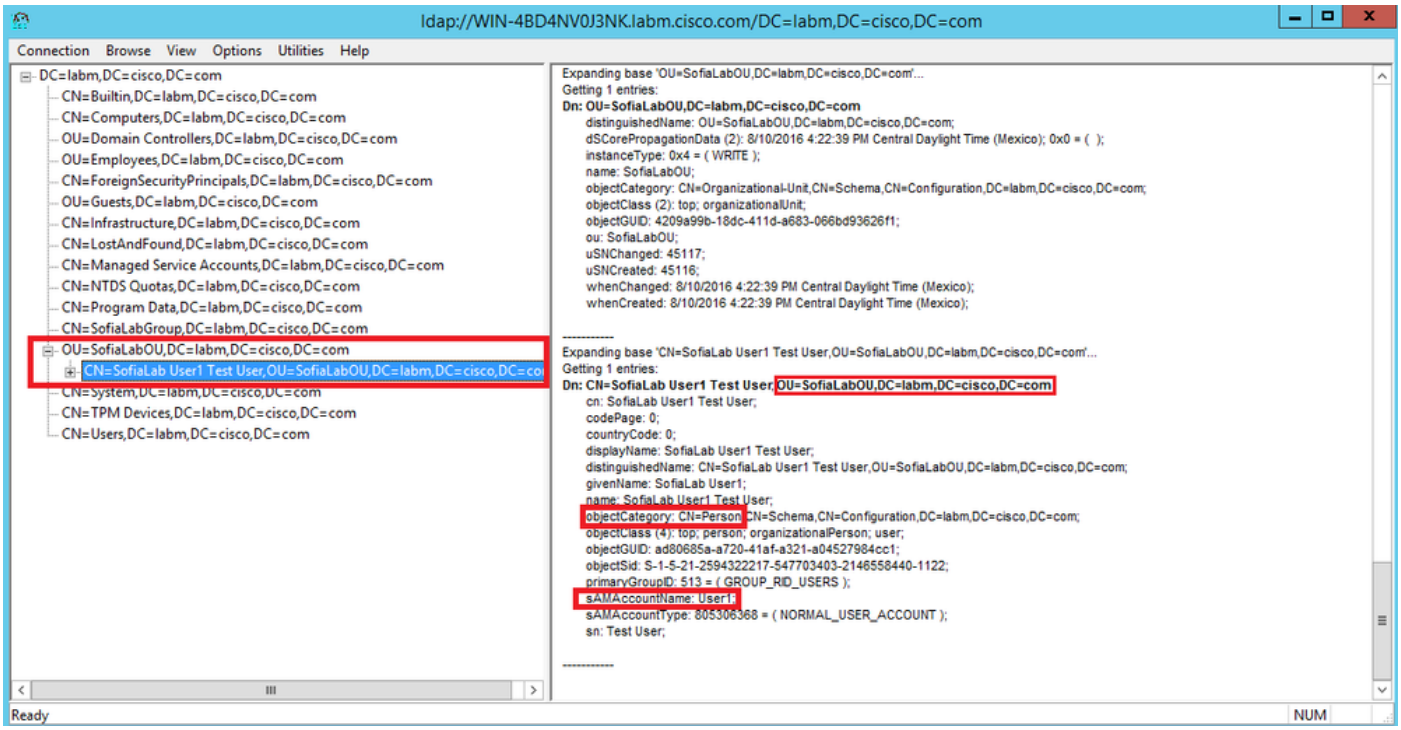
Schritt 3: Navigieren Sie zu **Ansicht > Baum,** und wählen Sie **OK** in der Basis-DN.



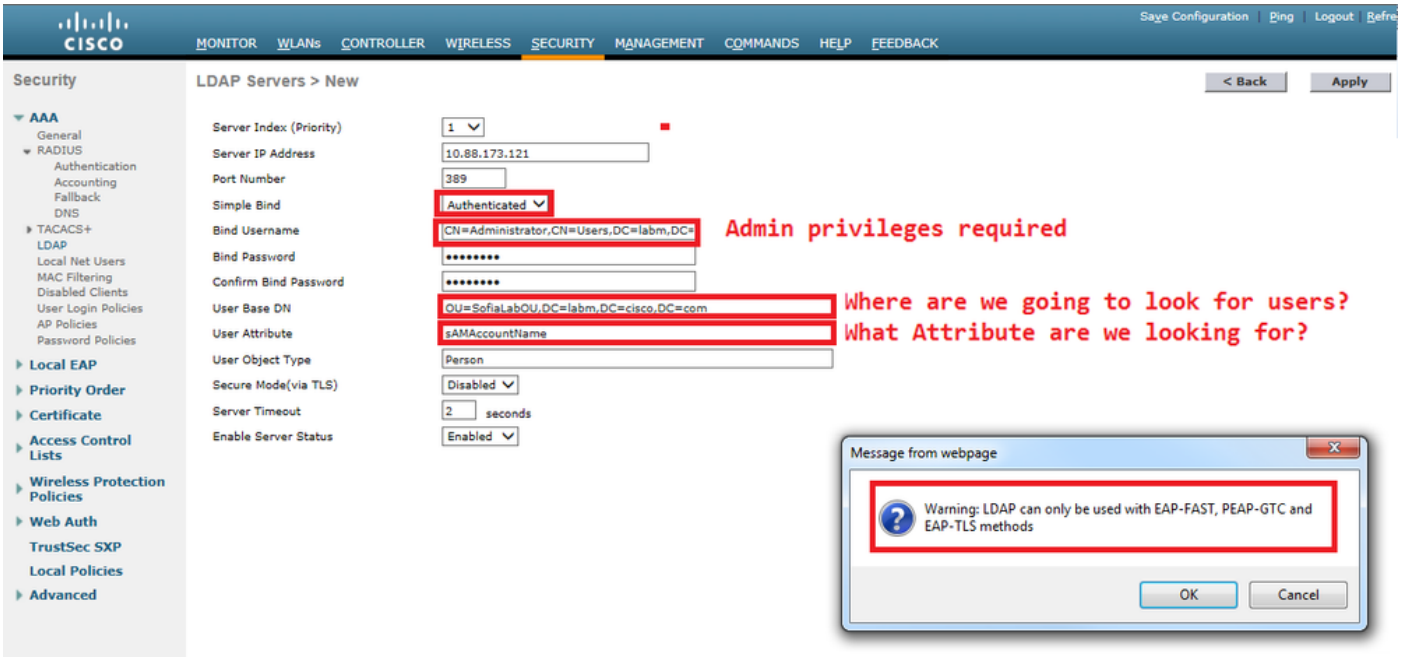
Schritt 4: Erweitern Sie die Struktur, um die Struktur anzuzeigen, und suchen Sie nach der DN für die Suchbasis. Beachten Sie, dass es sich um jeden Containertyp außer Gruppen handeln kann. Dabei kann es sich um die gesamte Domäne, eine bestimmte OU oder eine CN wie CN=Users handeln.



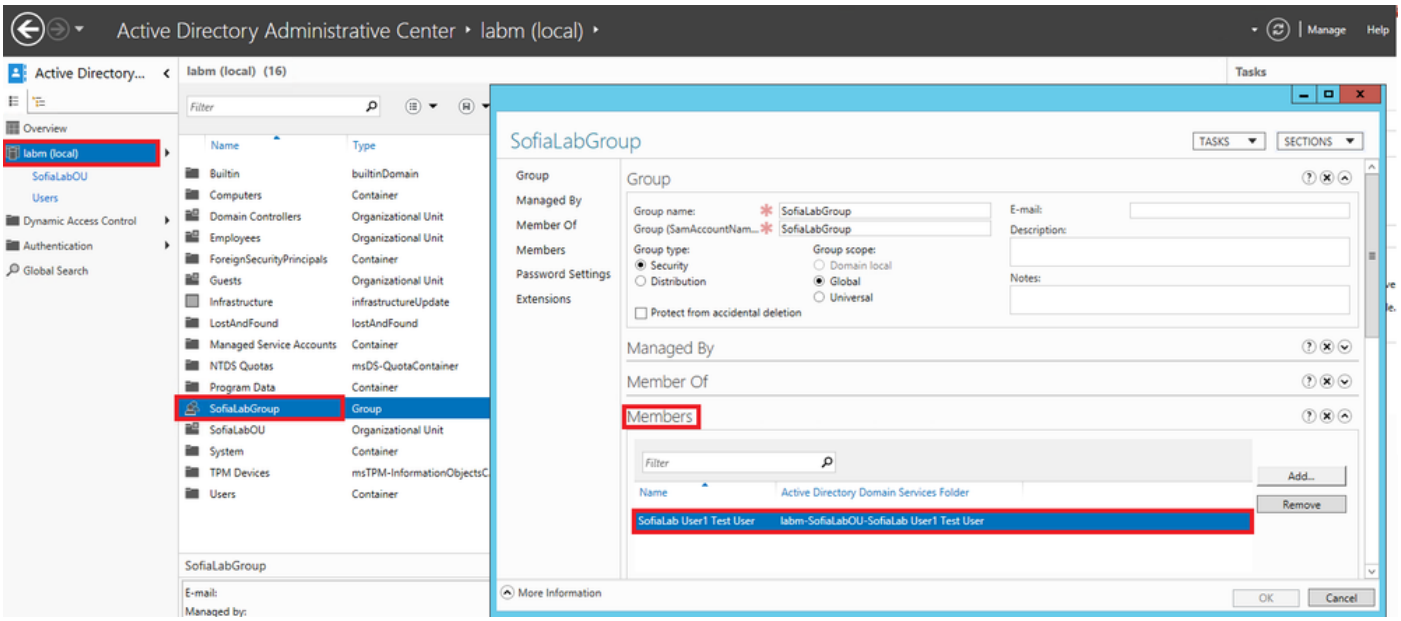
Schritt 5: Erweitern Sie das SofiaLabOU, um zu sehen, welche Benutzer sich darin befinden. Es gibt den User1, der zuvor erstellt wurde.



Schritt 6: Alles, was Sie für die LDAP-Konfiguration benötigen.



Schritt 7. Gruppen wie SofiaLabGroup können nicht als Such-DN verwendet werden. Erweitern Sie die Gruppe, und suchen Sie nach den darin enthaltenen Benutzern, wobei Benutzer1 zuvor erstellt werden musswie dargestellt.



User1 war da, aber LDP konnte ihn nicht finden. Dies bedeutet, dass der WLC nicht in der Lage ist, dies ebenfalls zu tun, und dass Gruppen nicht als Basis-DN für die Suche unterstützt werden.

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

```
(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
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

```
(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
```

Zugehörige Informationen

- LDAP - WLC 8.2 - Konfigurationsleitfaden
- So konfigurieren Sie den Wireless LAN Controller (WLC) für die LDAP-Authentifizierung (Lightweight Directory Access Protocol) - von Vinay Sharma
- Web-Authentifizierung mit LDAP auf Wireless LAN Controllern (WLCs) Konfigurationsbeispiel - von Yahya Jaber und Ayman Alfares

- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

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