Configurer WLC avec l’authentification LDAP pour les réseaux WLAN 802.1x et Web-Auth

Table des matières

Introduction

Ce document décrit la procédure pour configurer un WLC AireOS afin d'authentifier les clients avec un serveur LDAP comme base de données des utilisateurs.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Serveurs Microsoft Windows
- Active Directory

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel Cisco WLC 8.2.10.0

- Microsoft Windows Server 2012 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Contexte technique

- LDAP est un protocole utilisé pour accéder aux serveurs d'annuaire.
- Les serveurs d'annuaire sont des bases de données hiérarchiques orientées objet.
- Les objets sont organisés en conteneurs, tels que les unités d'organisation (OU), les groupes ou les conteneurs Microsoft par défaut, sous la forme CN=Users.
- La partie la plus difficile de cette configuration est de configurer correctement les paramètres du serveur LDAP sur le WLC.

Pour plus d'informations sur ces concepts, référez-vous à la section Introduction de Comment configurer le contrôleur de réseau local sans fil (WLC) pour l'authentification LDAP (Lightweight Directory Access Protocol).

Forum aux questions

- Quel nom d'utilisateur doit être utilisé pour établir une liaison avec le serveur LDAP ?

Il existe deux façons de se lier à un serveur LDAP, Anonymous ou Authenticated (reportez-vous à la section pour comprendre la différence entre les deux méthodes).

Ce nom d'utilisateur de liaison doit disposer de privilèges d'administrateur pour pouvoir rechercher d'autres noms d'utilisateur/mots de passe.

- Si authentifié : le nom d'utilisateur bind est-il dans le même conteneur que tous les utilisateurs ?

Non : utilisez le chemin complet. Exemple :

CN=Administrateur, CN=Administrateurs de domaine, CN=Utilisateurs, DC=labm, DC=cisco, DC=com

Oui : utilisez uniquement le nom d'utilisateur. Exemple :

administrateur

- Que se passe-t-il si des utilisateurs se trouvent dans des conteneurs différents ? Tous les utilisateurs LDAP sans fil concernés doivent-ils se trouver dans le même conteneur ?

Non, vous pouvez spécifier un DN de base qui inclut tous les conteneurs nécessaires.

- Quels attributs le WLC doit-il rechercher ?

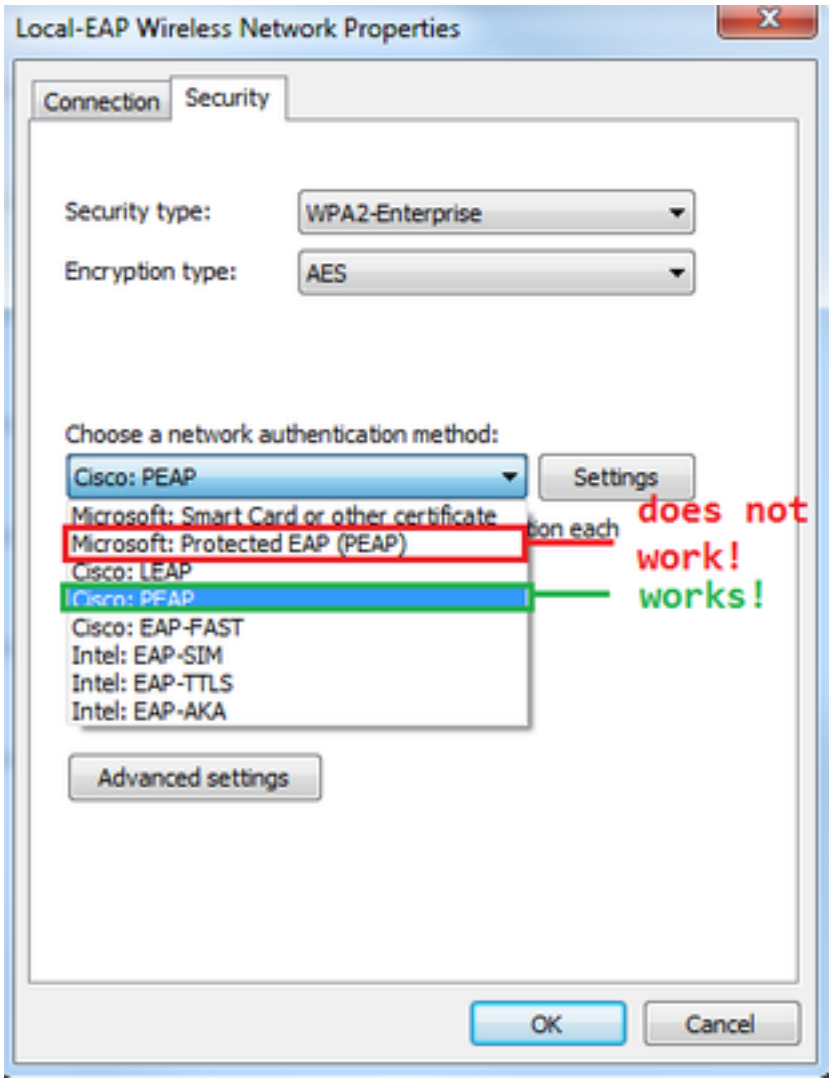
Le WLC correspond à l'attribut d'utilisateur et au type d'objet spécifiés.

Remarque : **sAMAccountName** est sensible à la casse, mais pas la personne. Par conséquent, **sAMAccountName=RICARDO** et **sAMAccountName=ricardo** sont identiques et fonctionnent alors que **samaccountname=RICARDO** et **samaccountname=ricardo** ne fonctionnent pas.

- Quelles méthodes EAP (Extensible Authentication Protocol) peuvent être utilisées ?

EAP-FAST, PEAP-GTC et EAP-TLS uniquement. Les demandeurs par défaut d'Android, iOS et MacOS fonctionnent avec le protocole PEAP (Protected Extensible Authentication Protocol).

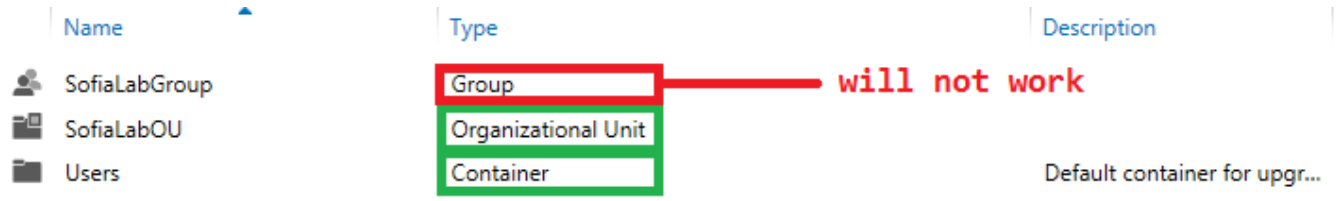
Pour Windows, Anyconnect Network Access Manager (NAM) ou le demandeur Windows par défaut avec Cisco : PEAP doivent être utilisés sur les cartes sans fil prises en charge, comme illustré dans l'image.



Remarque : les plug-ins Cisco EAP pour Windows incluent une version d'Open Secure Socket Layer (OpenSSL 0.9.8k) qui est affectée par l'ID de bogue Cisco CSCva09670, Cisco ne prévoit pas d'émettre d'autres versions des plug-ins EAP pour Windows et recommande aux clients d'utiliser le client AnyConnect Secure Mobility.

- Pourquoi le WLC ne trouve-t-il pas d'utilisateurs ?

Les utilisateurs d'un groupe ne peuvent pas être authentifiés. Ils doivent se trouver à l'intérieur d'un conteneur par défaut (CN) ou d'une unité d'organisation (OU), comme le montre l'image.



Configurer

Il existe différents scénarios dans lesquels un serveur LDAP peut être utilisé, soit avec l'authentification 802.1x, soit avec l'authentification Web.

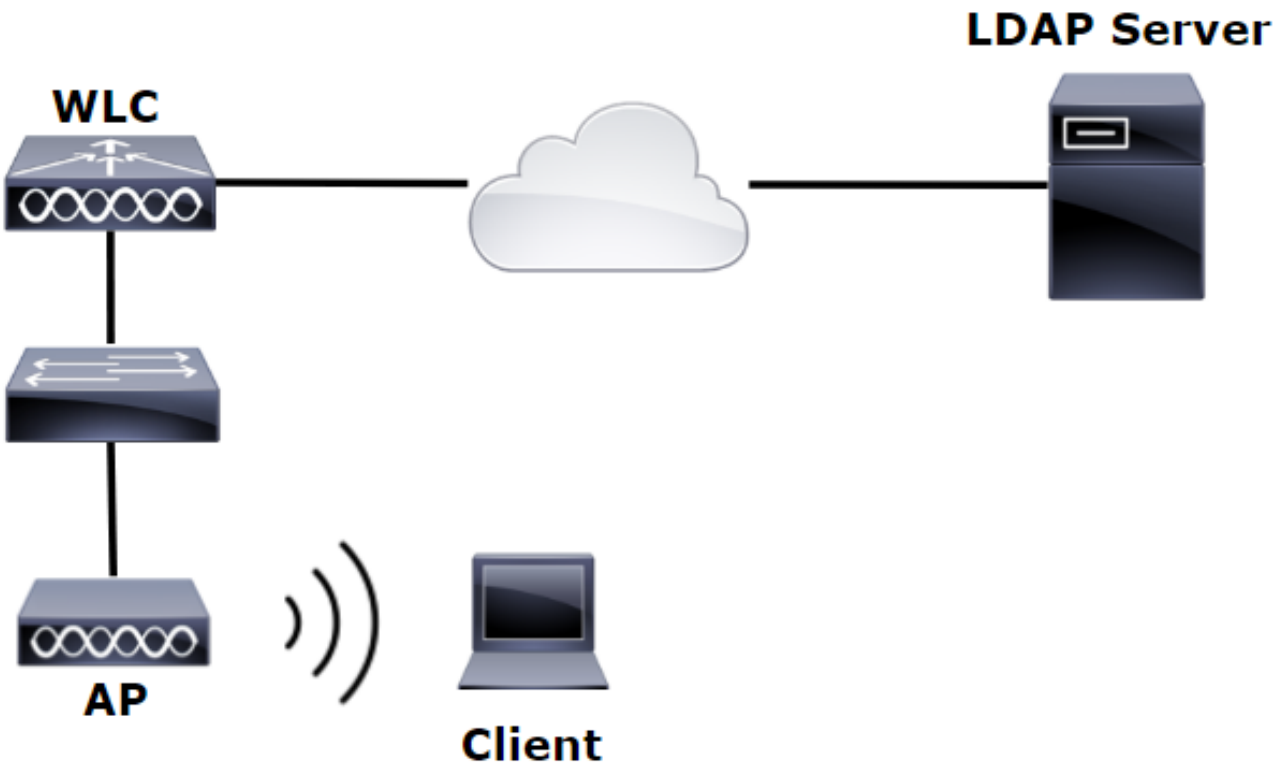
Pour cette procédure, seuls les utilisateurs à l'intérieur de l'OU=SofiaLabOU doivent être authentifiés.

Afin d'apprendre comment utiliser l'outil Label Distribution Protocol (LDP), configurer et dépanner LDAP, référez-vous au Guide de configuration LDAP du WLC.

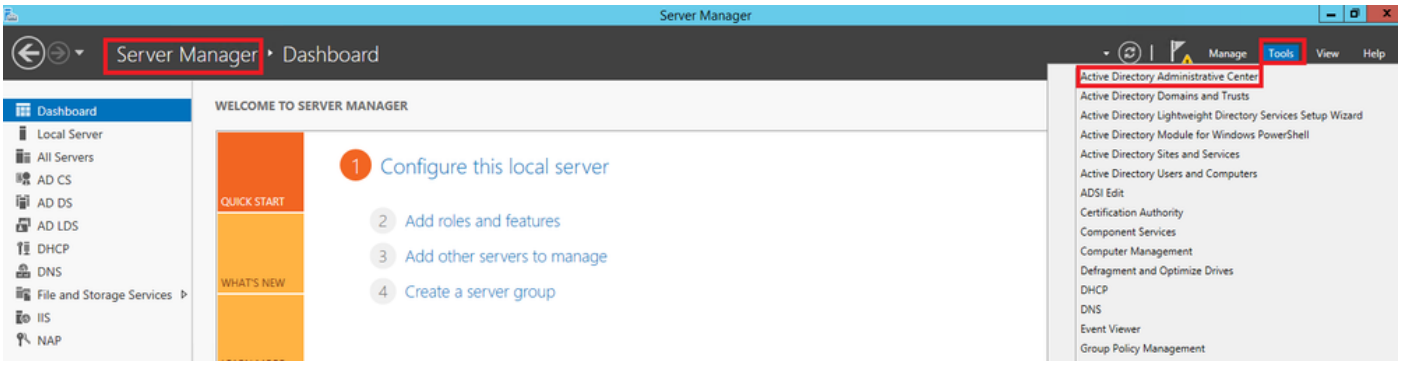
Créer un WLAN qui s'appuie sur le serveur LDAP pour authentifier les utilisateurs via 802.1x

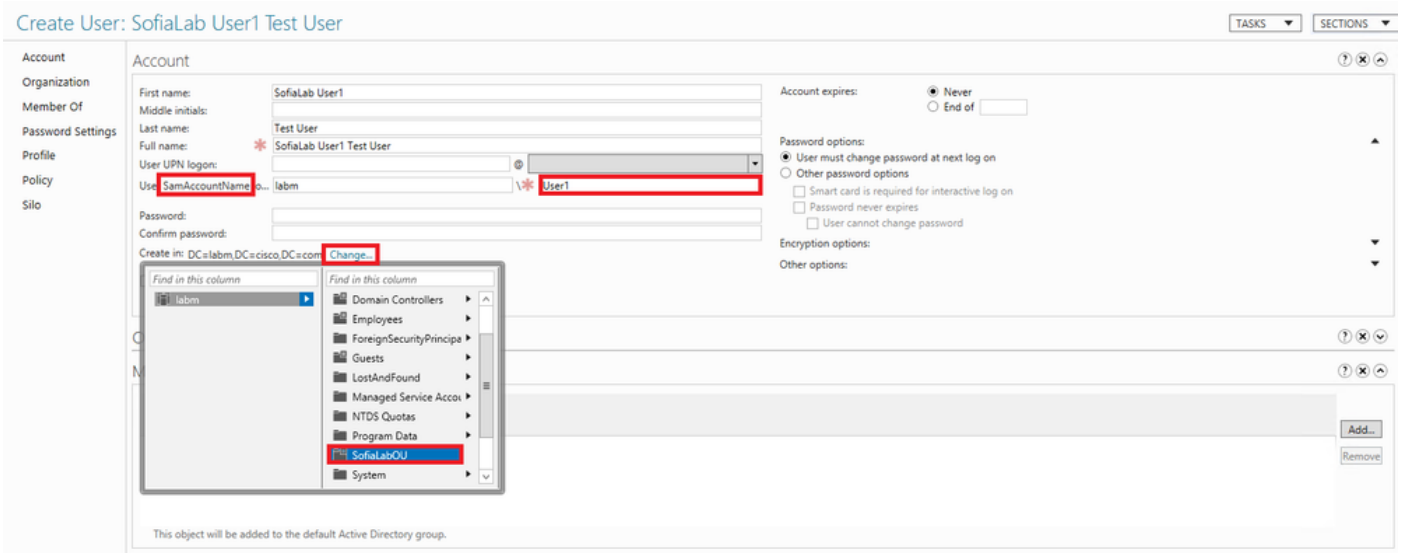
Diagramme du réseau

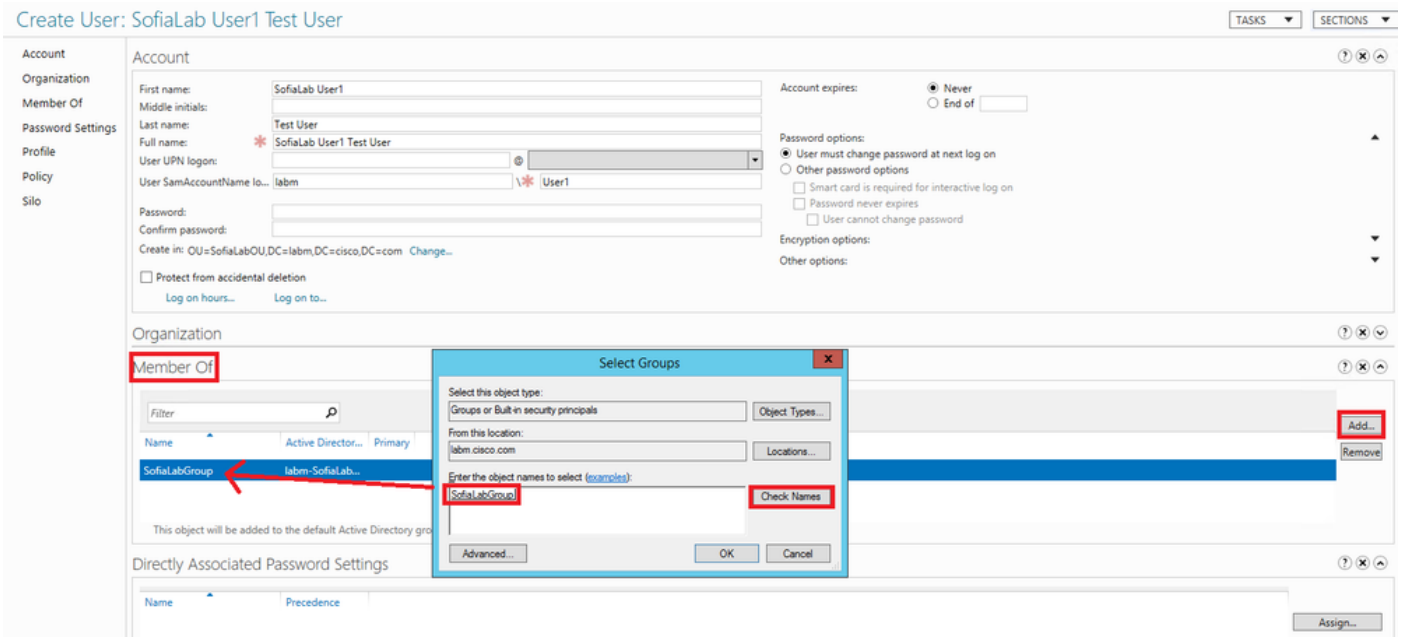
Dans ce scénario, WLAN LDAP-dot1x utilise un serveur LDAP pour authentifier les utilisateurs à l'aide de 802.1x.



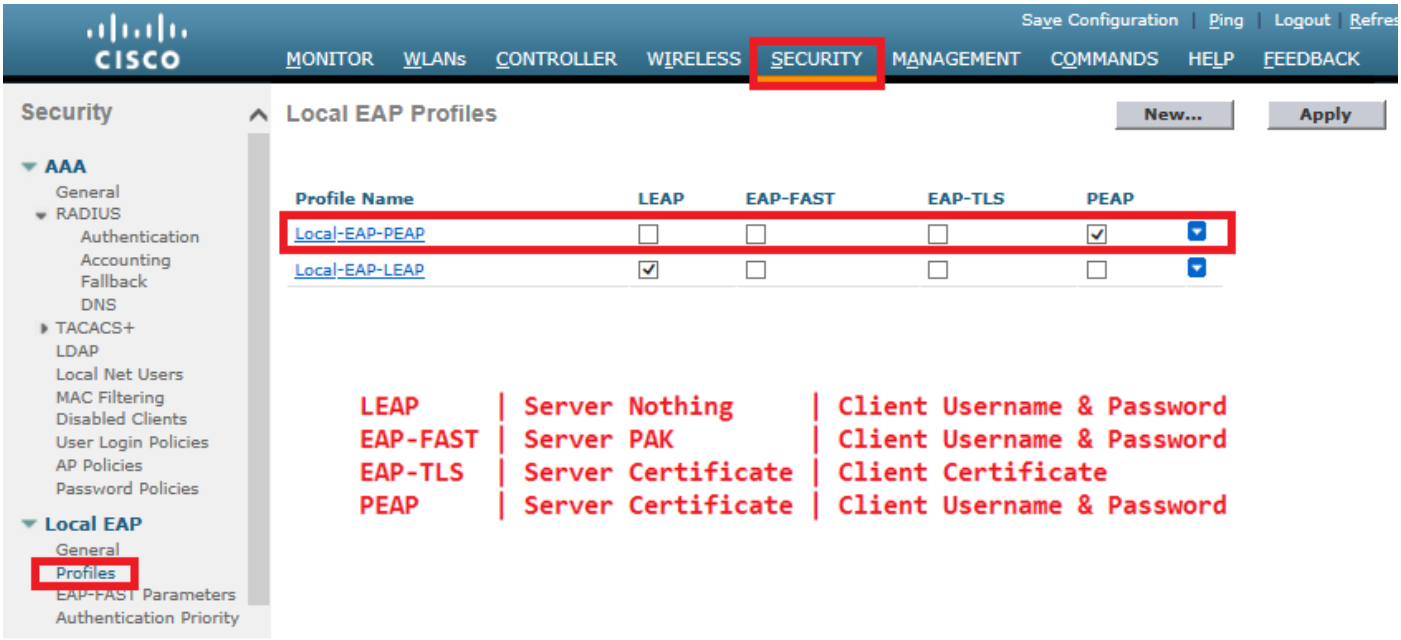
Étape 1. Créez un utilisateur **User1** dans le serveur LDAP membre des groupes SofiaLabOU et SofiaLabGroup.





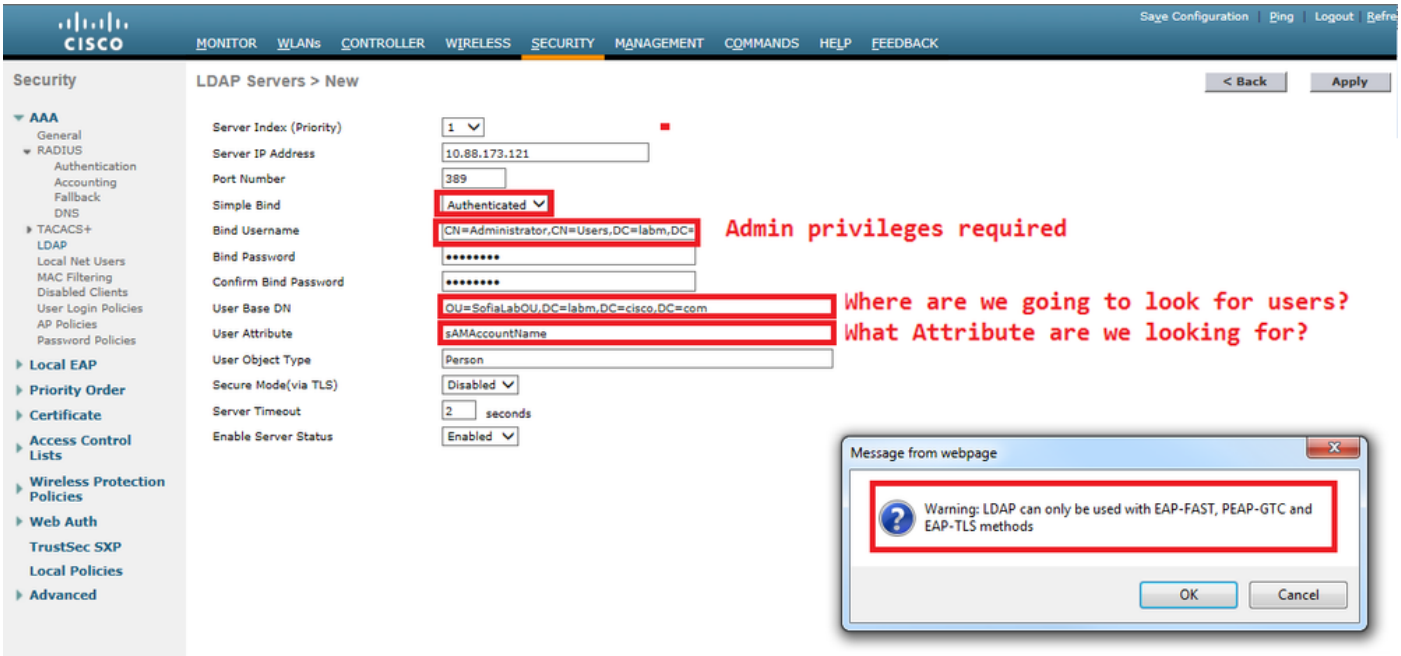


Étape 2. Créez un profil EAP au niveau du WLC avec la méthode EAP souhaitée (utilisez PEAP).



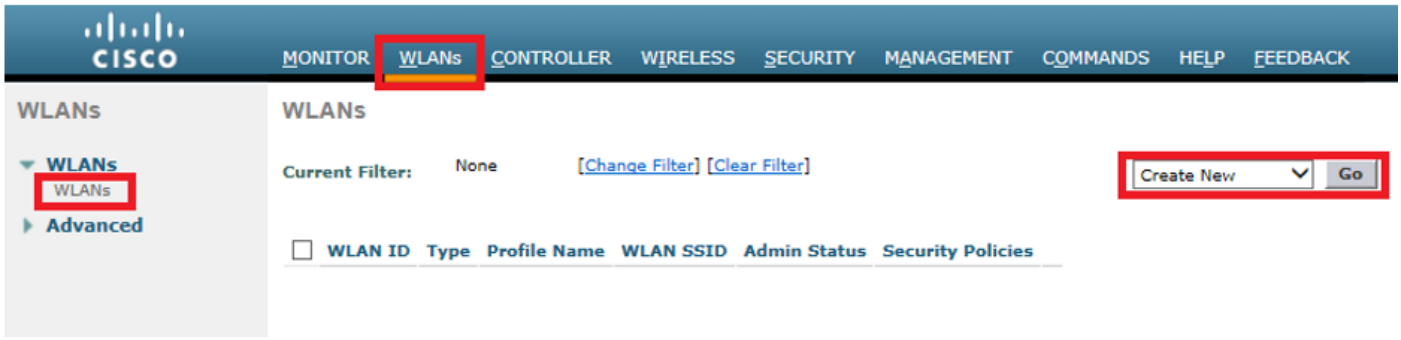
Étape 3. Liez le WLC au serveur LDAP.

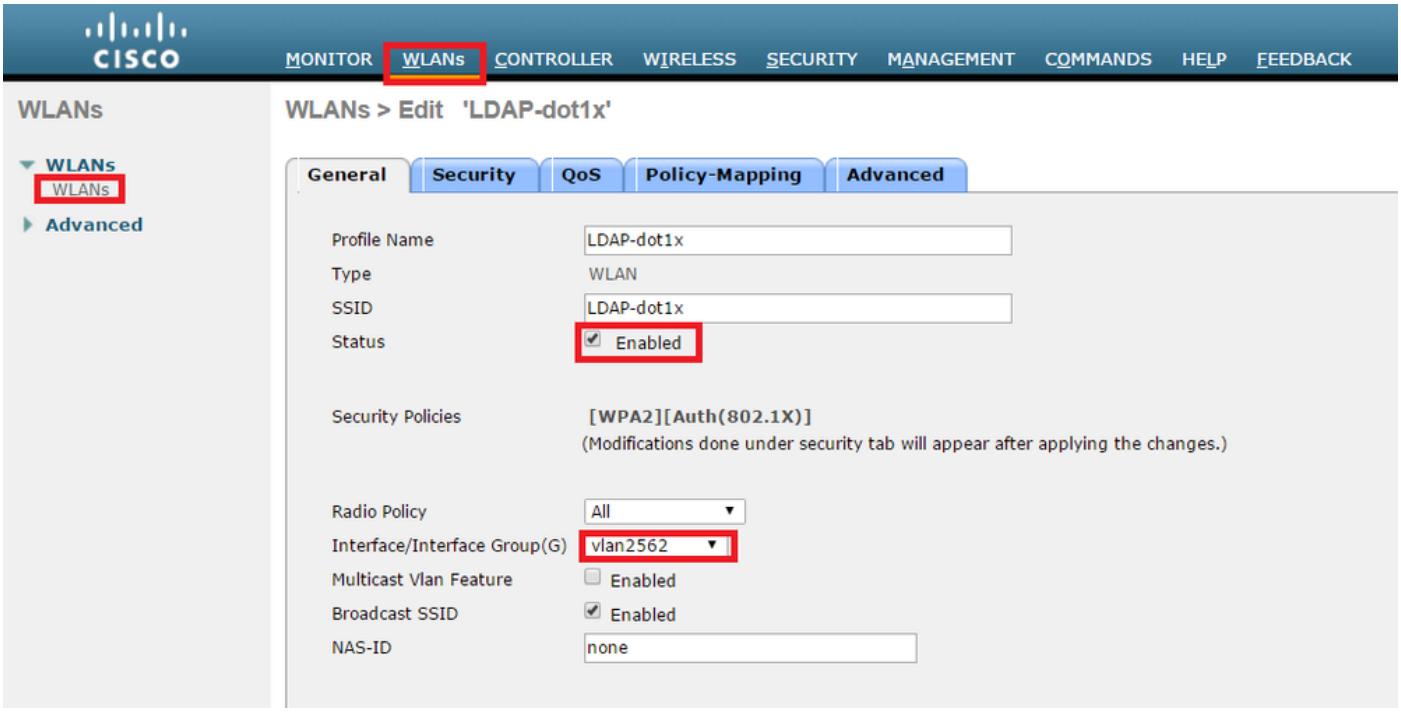
> **Conseil** : si le nom d'utilisateur de liaison ne figure pas dans le DN de base de l'utilisateur, vous devez écrire le chemin complet vers l'utilisateur **Admin** comme indiqué dans l'image. Sinon, vous pouvez simplement entrer **Administrator**.



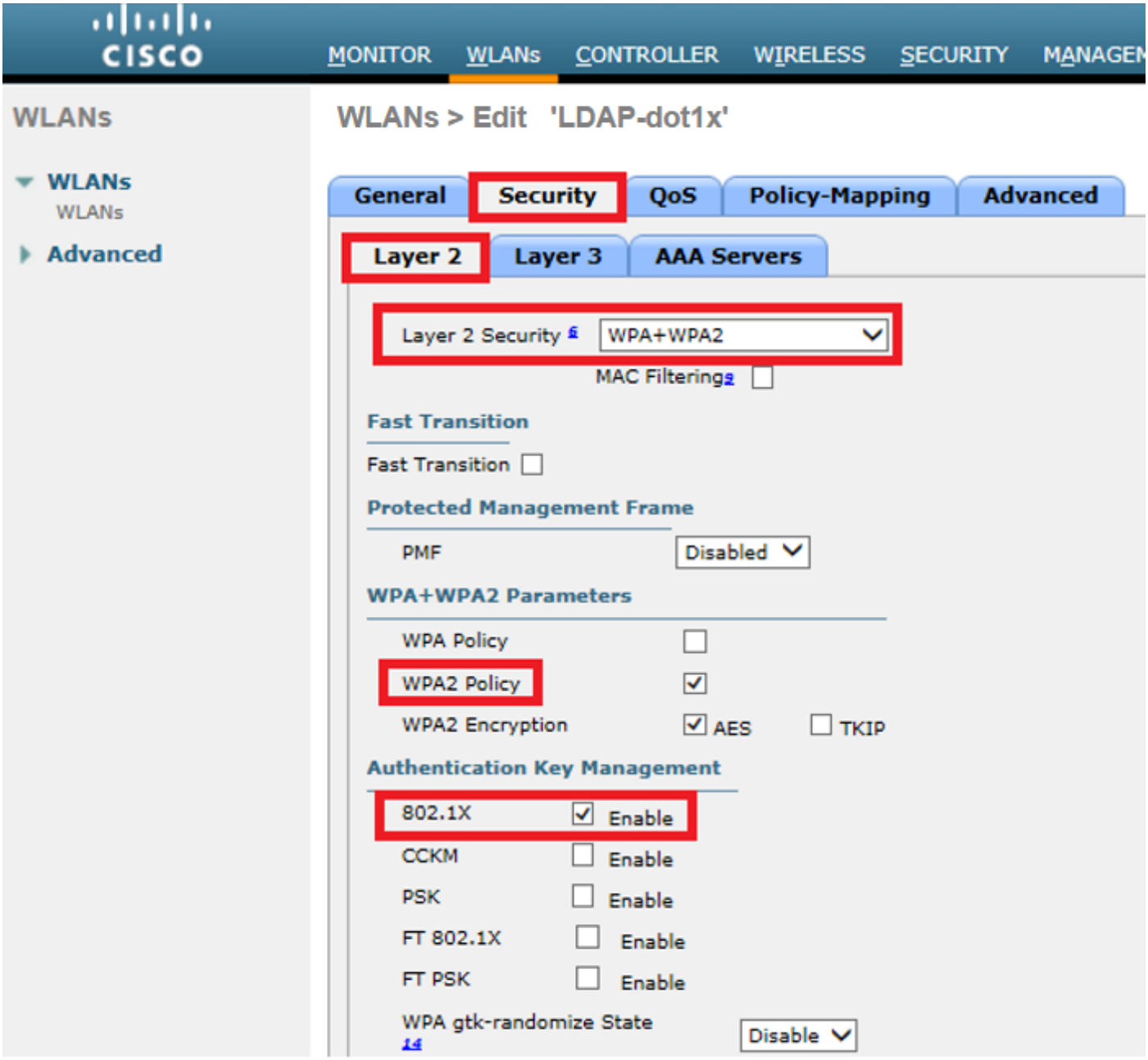
Étape 4. Définissez l'ordre d'authentification sur Utilisateurs internes + LDAP ou LDAP uniquement.

Étape 5. Créez le WLAN LDAP-dot1x.

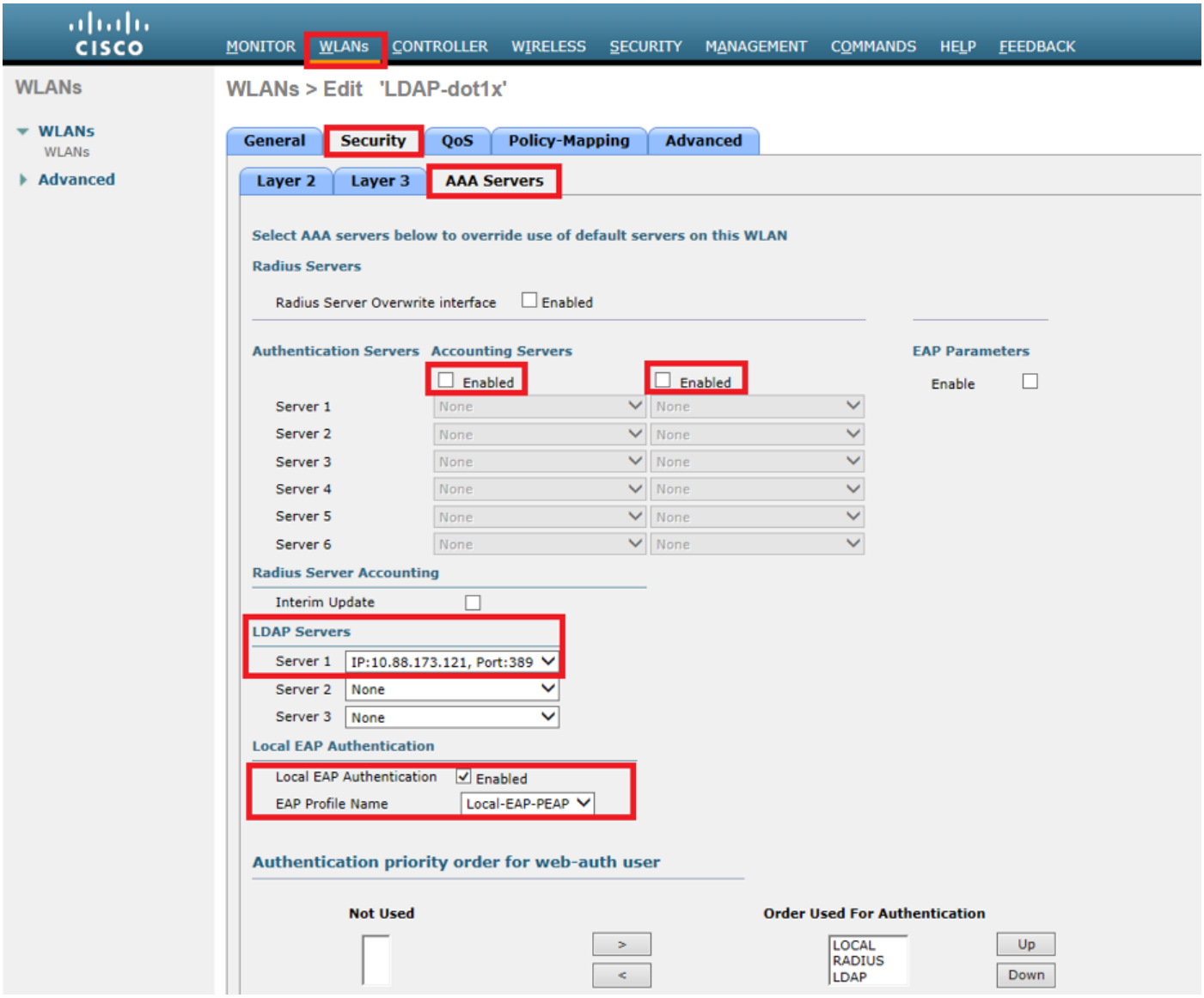




Étape 6. Définissez la méthode de sécurité L2 sur WPA2 + 802.1x et la sécurité L3 sur none.



Étape 7. Activez l'authentification EAP locale et assurez-vous que les options Serveurs d'authentification et Serveurs de comptabilité sont désactivées et que LDAP est activé.



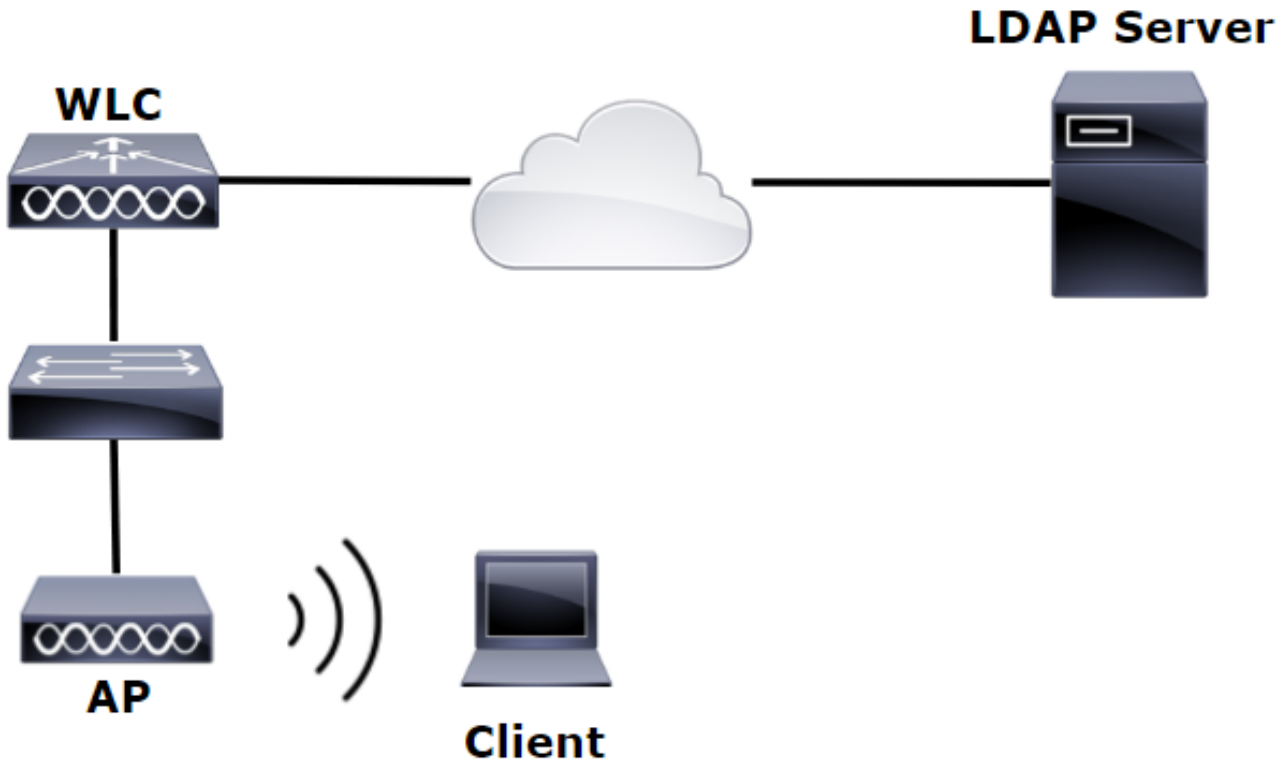
Tous les autres paramètres peuvent être conservés par défaut.

> **Remarques :**
> Utilisez l'outil LDP pour confirmer les paramètres de configuration.
> La base de recherche ne peut pas être un groupe (tel que SofiaLabGroup).
> PEAP-GTC ou Cisco : PEAP doivent être utilisés à la place de Microsoft : PEAP chez le demandeur s'il s'agit d'une machine Windows. Microsoft : PEAP fonctionne par défaut avec MacOS/iOS/Android.

Créer un WLAN qui s'appuie sur le serveur LDAP pour authentifier les utilisateurs via le portail Web interne du WLC

Diagramme du réseau

Dans ce scénario, WLAN LDAP-Web utilise un serveur LDAP pour authentifier les utilisateurs avec le portail Web interne WLC.



Assurez-vous que les étapes 1 à 4 ont été effectuées à partir de l'exemple précédent. De là, la configuration WLAN est définie différemment.

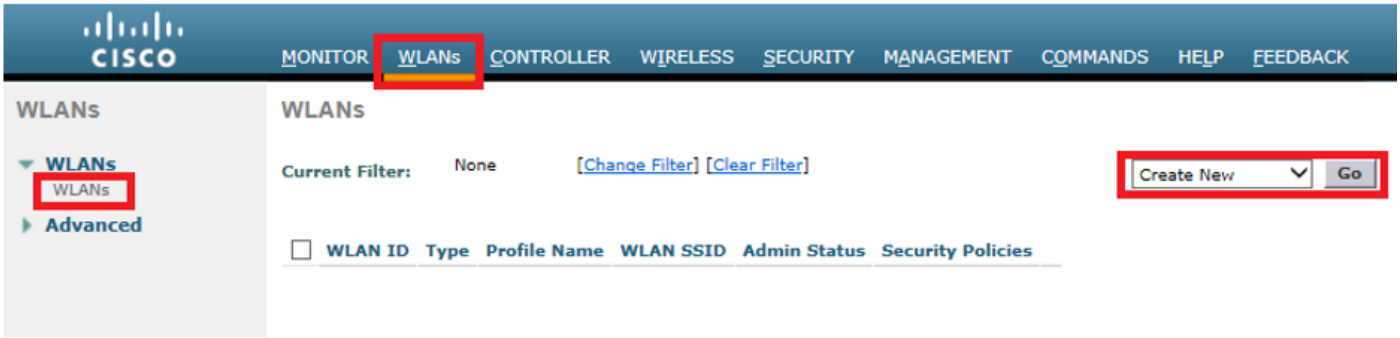
Étape 1. Créez un utilisateur **User1** dans le serveur LDAP membre de l'unité d'organisation SofiaLabOU et du groupe SofiaLabGroup.

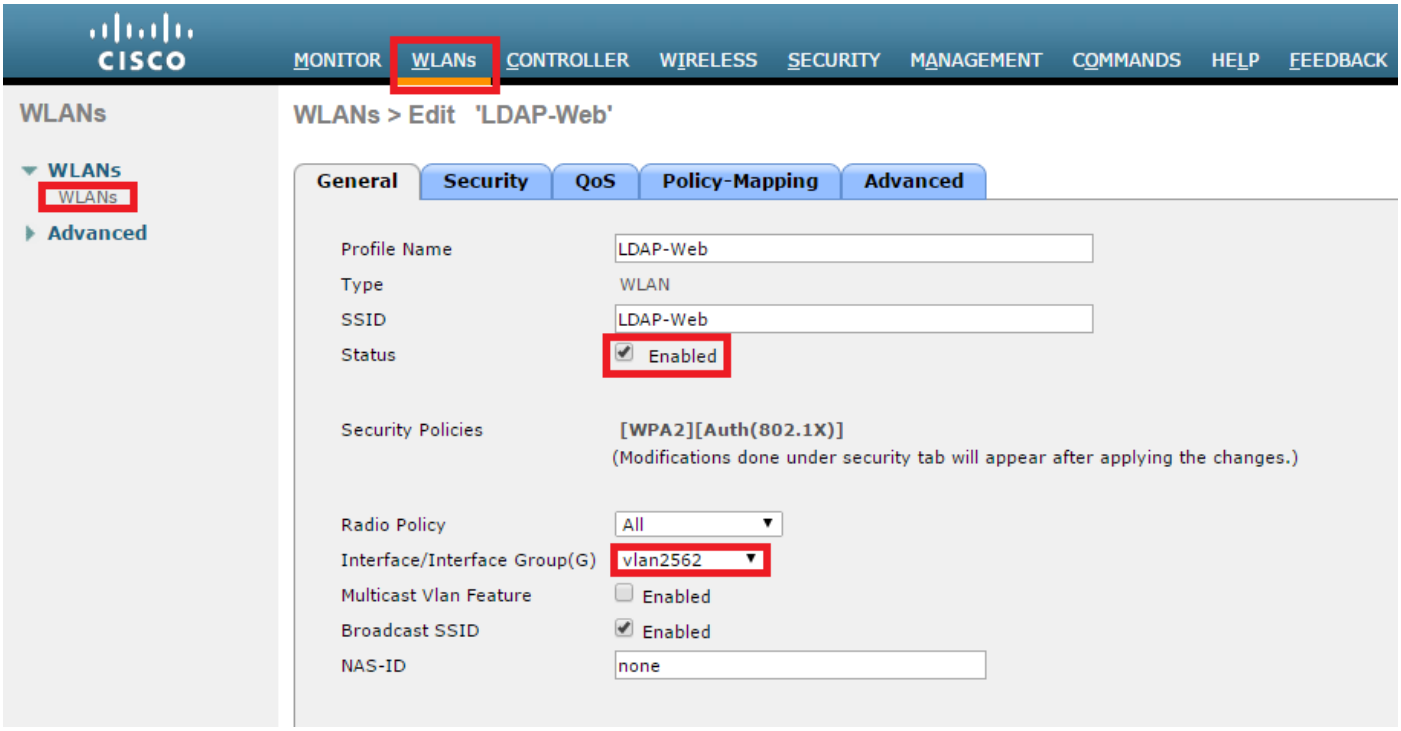
Étape 2. Créez un profil EAP au niveau du WLC avec la méthode EAP souhaitée (utilisez PEAP).

Étape 3. Liez le WLC au serveur LDAP.

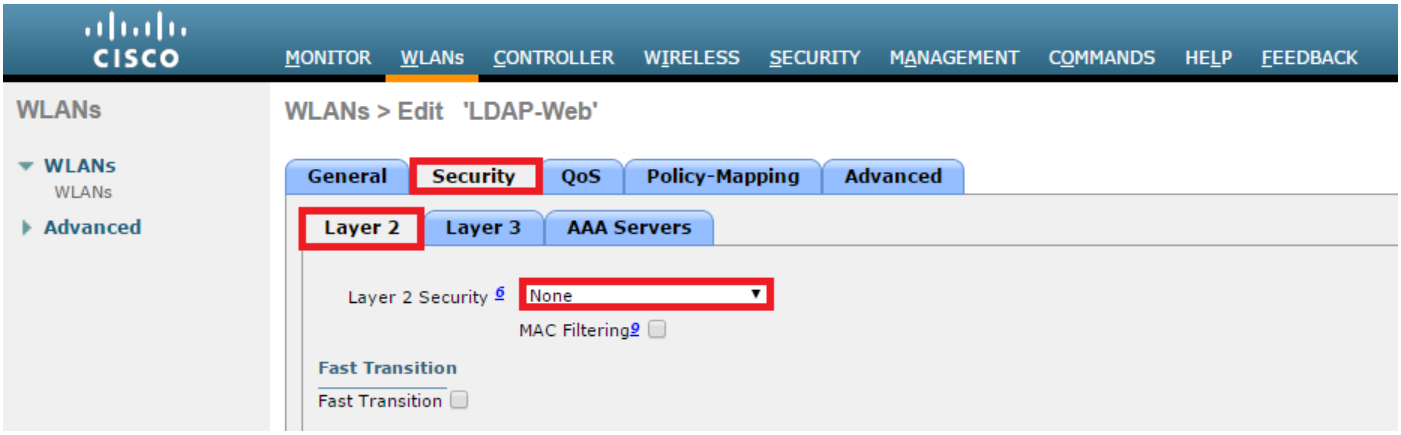
Étape 4. Définissez l'ordre d'authentification sur Utilisateurs internes + LDAP.

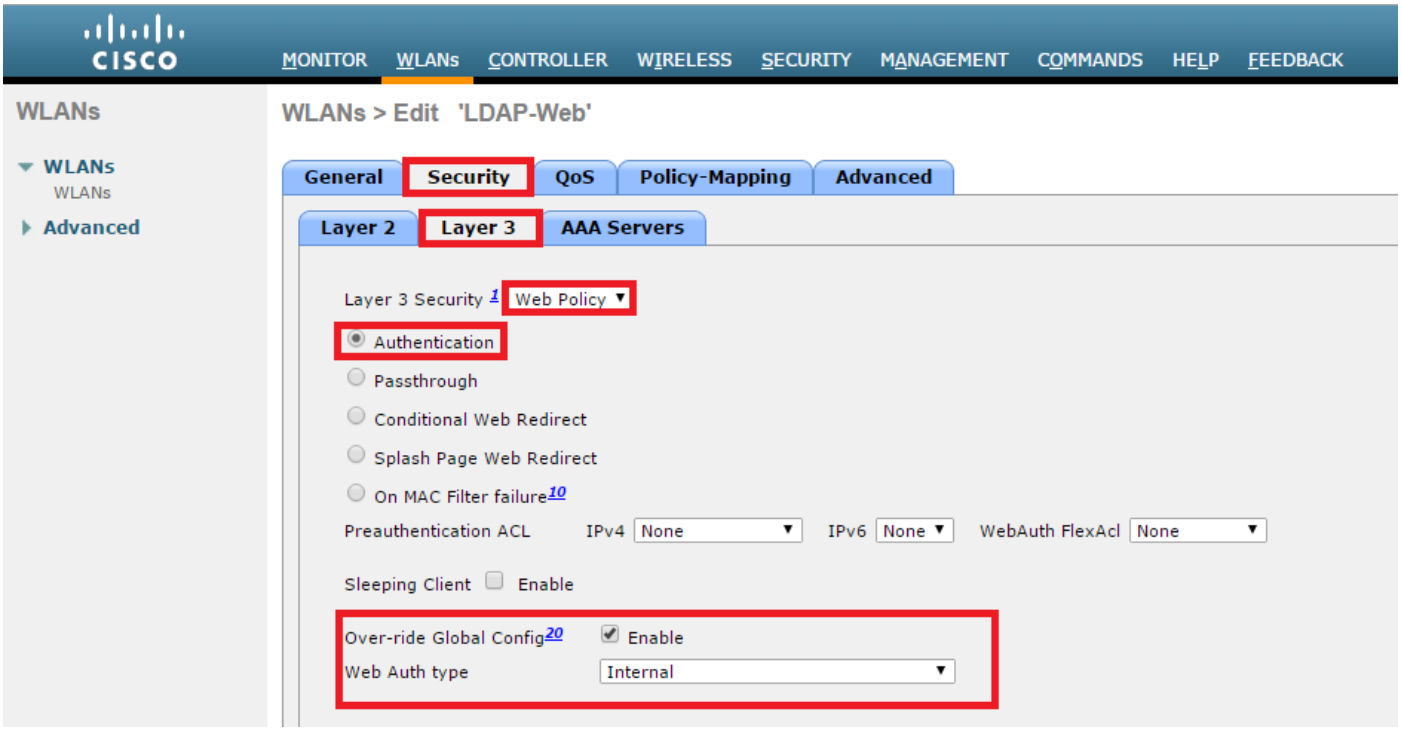
Étape 5. Créez le WLAN LDAP-Web comme indiqué dans les images.



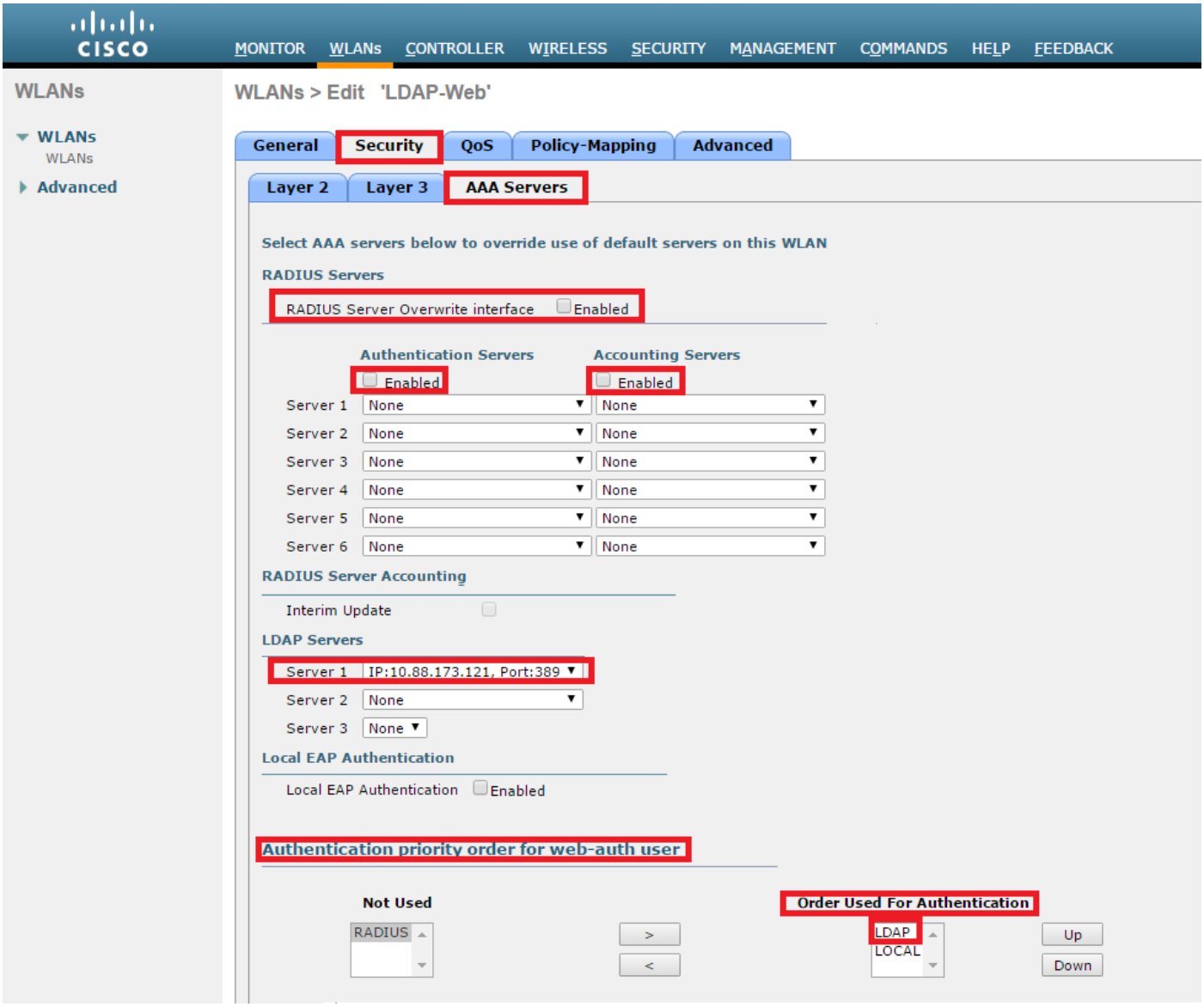


Étape 6. Définir la sécurité L2 sur aucun et la sécurité L3 sur Stratégie Web - Authentificationcomme le montrent les images.





Étape 7. Définissez l'ordre de priorité d'authentification pour l'authentification Web afin d'utiliser LDAP et assurez-vous que les options Serveurs d'authentification et Serveurs de gestion des comptes sont désactivées.



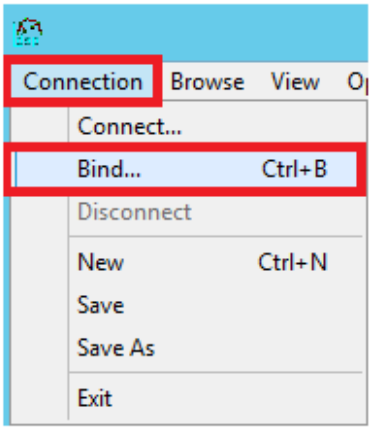
Tous les autres paramètres peuvent être conservés par défaut.

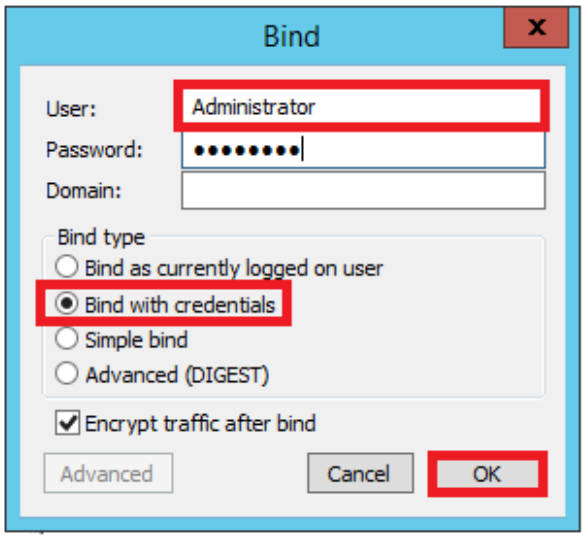
Utiliser L'Outil LDP Pour Configurer Et Dépanner LDAP

Étape 1. Ouvrez l'outil LDP sur le serveur LDAP ou sur un hôte connecté (le port TCP 389 doit être autorisé sur le serveur).

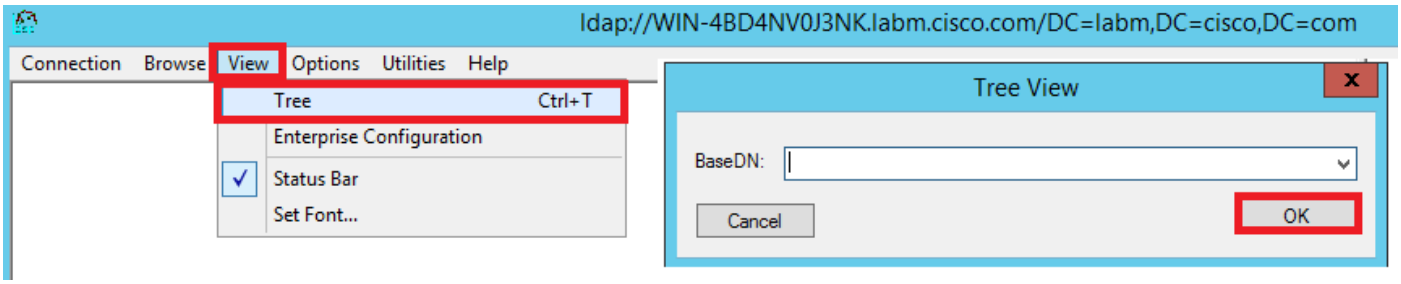
Étape 2. Accédez à **Connection > Bind,** connectez-vous avec un utilisateur Admin et sélectionnez

la case d'option **Bind with credentials**.

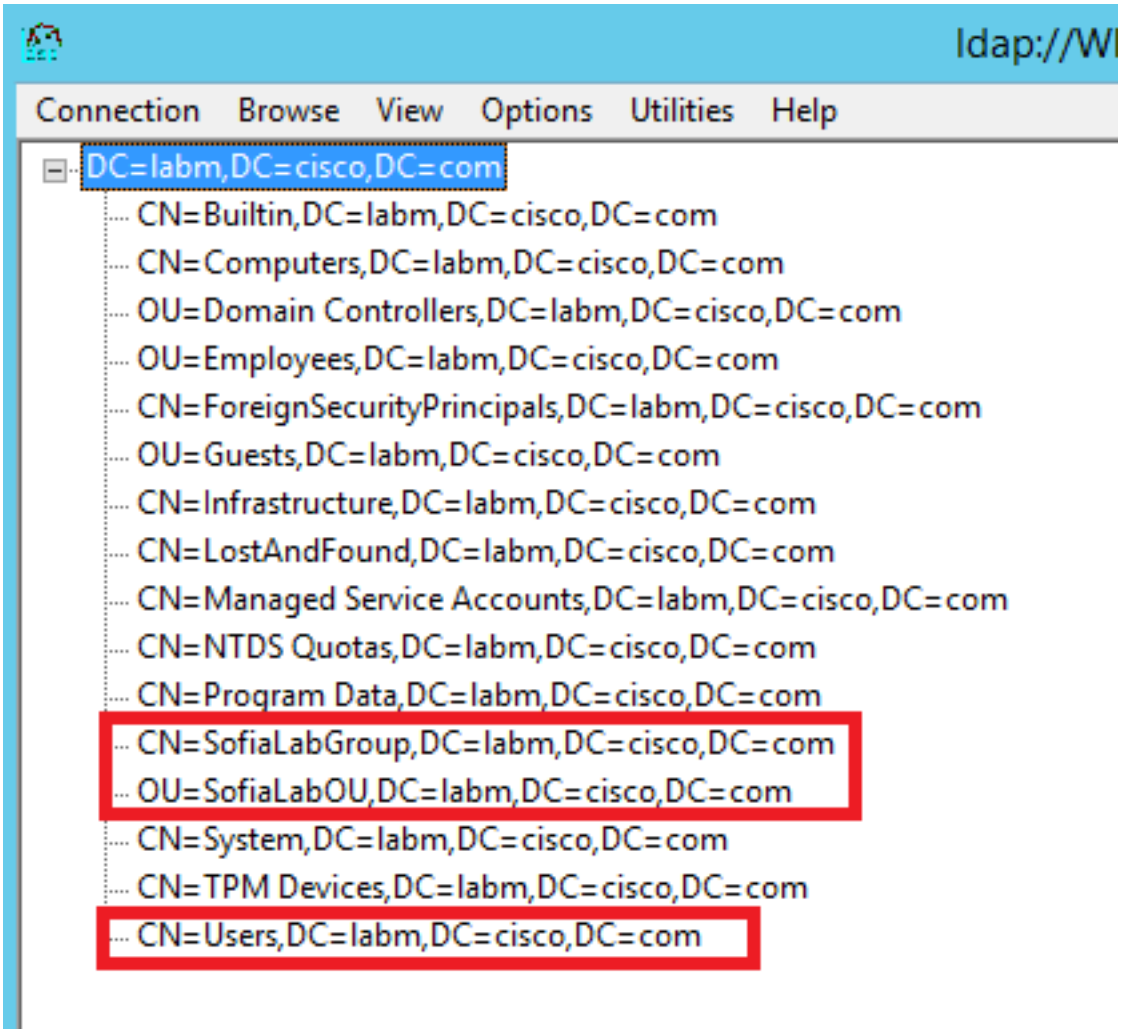




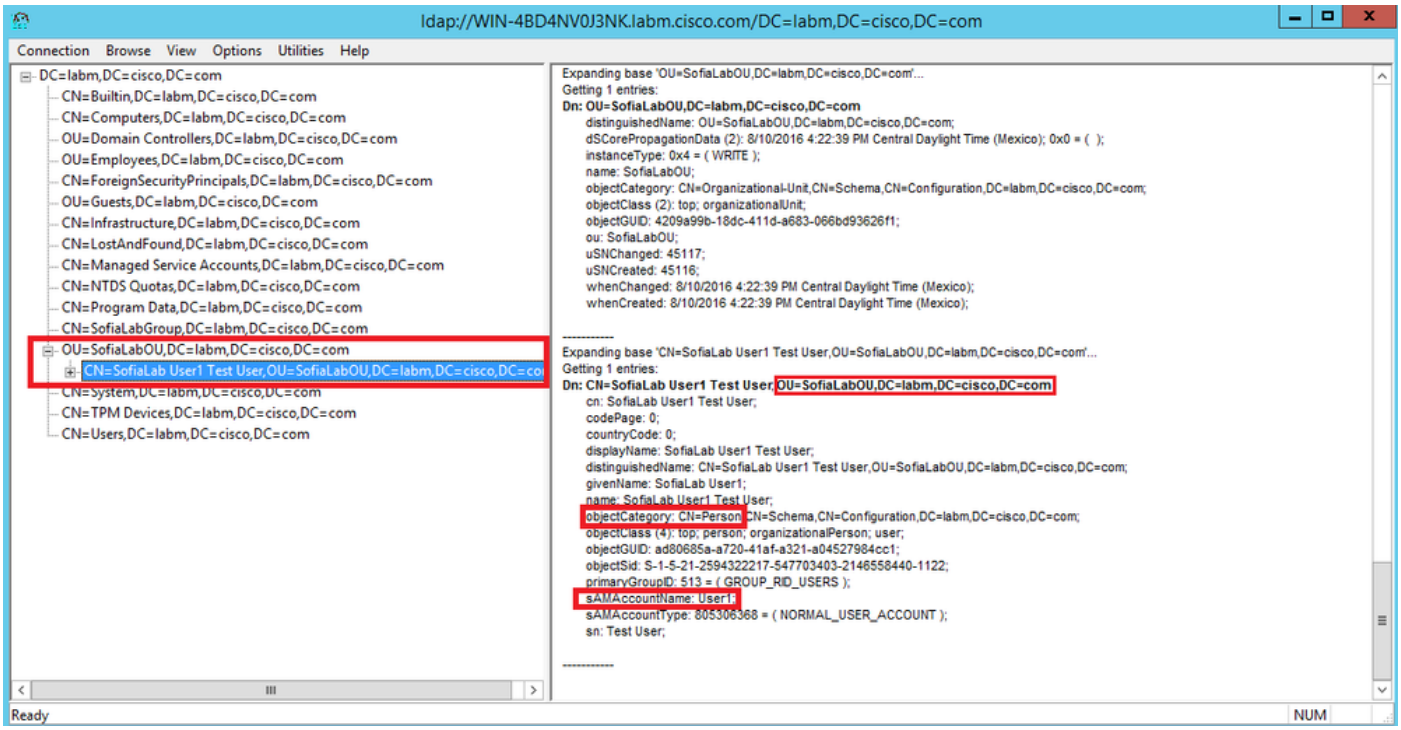
Étape 3. Naviguez jusqu'à **View > Tree** et sélectionnez **OK** dans le DN de base.



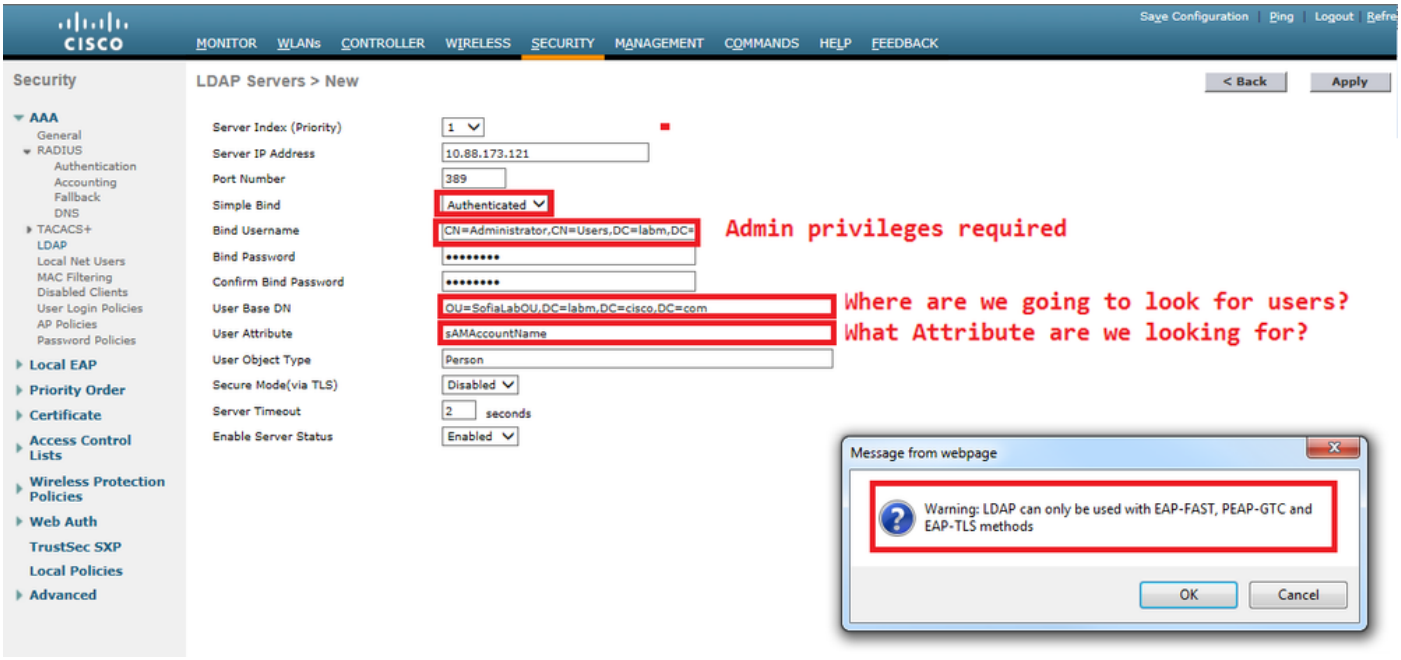
Étape 4. Développez l'arborescence pour afficher la structure et rechercher le DN de base de recherche. N'oubliez pas qu'il peut s'agir de tout type de conteneur excepté Groupes. Il peut s'agir de l'ensemble du domaine, d'une unité d'organisation spécifique ou d'un CN comme CN=Users.



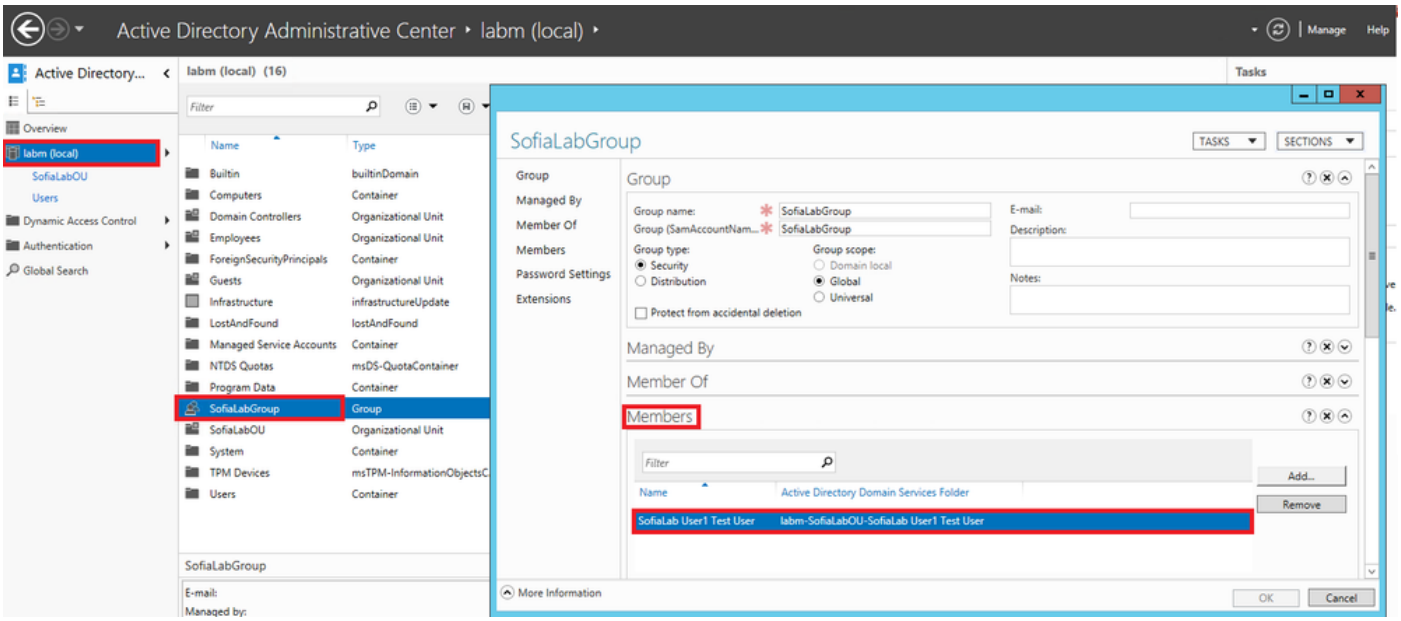
Étape 5. Développez le SofiaLabOU afin de voir quels utilisateurs sont à l'intérieur. Il s'agit de l'utilisateur User1 qui a été créé précédemment.



Étape 6. Tout ce dont vous avez besoin pour configurer LDAP.



Étape 7. Les groupes tels que SofiaLabGroup ne peuvent pas être utilisés comme DN de recherche. Développez le groupe et recherchez les utilisateurs qu'il contient, où l'utilisateur User1 précédemment créé doit êtrecomme illustré.



L'utilisateur 1 était présent, mais le protocole LDP ne l'a pas trouvé. Cela signifie que le WLC n'est pas capable de le faire aussi bien et c'est pourquoi les groupes ne sont pas pris en charge en tant que DN de base de recherche.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

```
(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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

```
(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
```

Informations connexes

- LDAP - Guide de configuration WLC 8.2
- Comment configurer le contrôleur LAN sans fil (WLC) pour l'authentification LDAP (Lightweight Directory Access Protocol) - par Vinay Sharma
- Exemple de configuration de l'authentification Web à l'aide de LDAP sur les contrôleurs de réseau local sans fil (WLC) - par Yahya Jaber et Ayman Alfares

- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.