Configuración del WLC con autenticación LDAP para las WLAN 802.1x y de autenticación web

Contenido

Introducción

Este documento describe el procedimiento para configurar un WLC de AireOS para autenticar clientes con un servidor LDAP como la base de datos de usuarios.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Servidores de Microsoft Windows
- Directorio activo

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software Cisco WLC 8.2.110.0

- Microsoft Windows Server 2012 R2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Antecedentes técnicos

- LDAP es un protocolo utilizado para acceder a los servidores de directorio.
- Los servidores de directorio son bases de datos jerárquicas orientadas a objetos.
- Los objetos se organizan en contenedores como unidades organizativas (OU), grupos o contenedores predeterminados de Microsoft como CN=Usuarios.
- La parte más difícil de esta configuración es configurar los parámetros del servidor LDAP correctamente en el WLC.

Para obtener información más detallada sobre estos conceptos, consulte la sección Introducción de Cómo configurar el Controlador de LAN Inalámbrica (WLC) para la autenticación del Protocolo ligero de acceso a directorios (LDAP).

Preguntas Frecuentes

- ¿Qué nombre de usuario se debe utilizar para enlazar con el servidor LDAP?

Hay dos maneras de enlazar contra un servidor LDAP, Anonymous o Authenticated (consulte para comprender la diferencia entre ambos métodos).

Este nombre de usuario de enlace debe tener privilegios de administrador para poder consultar otros nombres de usuario/contraseñas.

- Si se autentica: ¿el nombre de usuario de enlace está dentro del mismo contenedor que todos los usuarios?

No: utilice todo el trazado. Por ejemplo:

CN=Administrador,CN=Administradores de dominio,CN=Usuarios,DC=laboratorio,DC=cisco,DC=com

Sí: utilice sólo el nombre de usuario. Por ejemplo:

Administrador

- ¿Qué sucede si hay usuarios en diferentes contenedores? ¿Todos los usuarios de LDAP inalámbrico involucrados deben estar en el mismo contenedor?

No, se puede especificar un DN base que incluya todos los contenedores necesarios.

- ¿Qué atributos debe buscar el WLC?

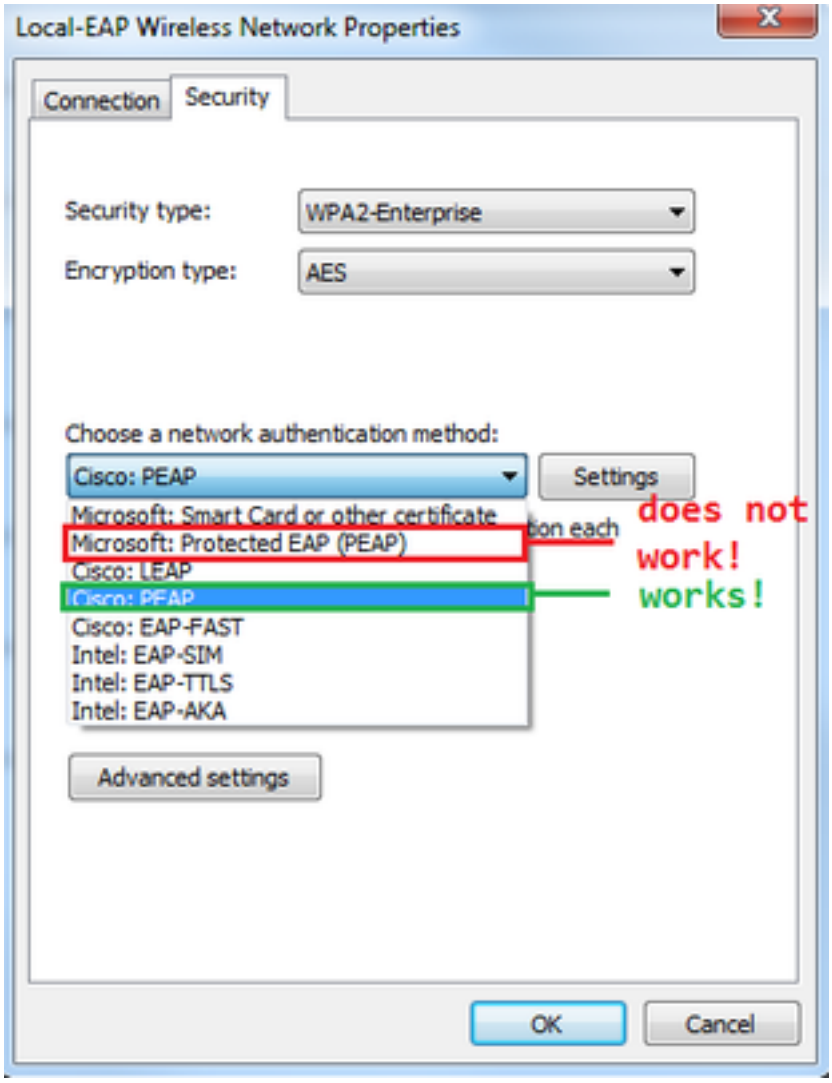
El WLC coincide con el atributo de usuario y el tipo de objeto especificados.

Nota: **sAMAccountName** distingue entre mayúsculas y minúsculas, pero person no lo hace. Por lo tanto, **sAMAccountName=RICARDO** y **sAMAccountName=ricardo** son iguales y funcionan, mientras que **samaccountname=RICARDO** y **samaccountname=ricardo** no.

- ¿Qué métodos de protocolo de autenticación extensible (EAP) se pueden utilizar?

Sólo EAP-FAST, PEAP-GTC y EAP-TLS. Los suplicantes predeterminados de Android, iOS y MacOS funcionan con el protocolo de autenticación ampliable protegido (PEAP).

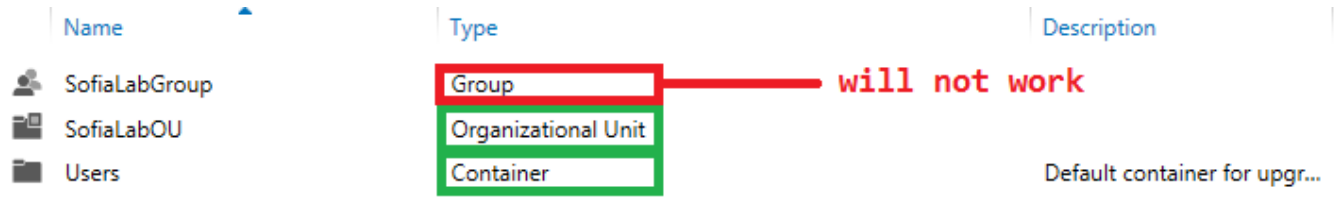
Para Windows, el administrador de acceso de red (NAM) de Anyconnect o el suplicante predeterminado de Windows con Cisco:PEAP se debe utilizar en adaptadores inalámbricos compatibles, como se muestra en la imagen.



Nota: los complementos EAP de Cisco para Windows incluyen una versión de Open Secure Socket Layer (OpenSSL 0.9.8k) que se ve afectada por el Id. de error de Cisco CSCva09670, Cisco no tiene previsto publicar más versiones de los complementos EAP para Windows y recomienda a los clientes que utilicen AnyConnect Secure Mobility Client.

- ¿Por qué el WLC no puede encontrar a los usuarios?

Los usuarios dentro de un grupo no se pueden autenticar. Deben estar dentro de un contenedor predeterminado (CN) o una unidad organizativa (OU), como se muestra en la imagen.



Configurar

Existen diferentes escenarios en los que se puede emplear un servidor LDAP, ya sea con autenticación 802.1x o autenticación Web.

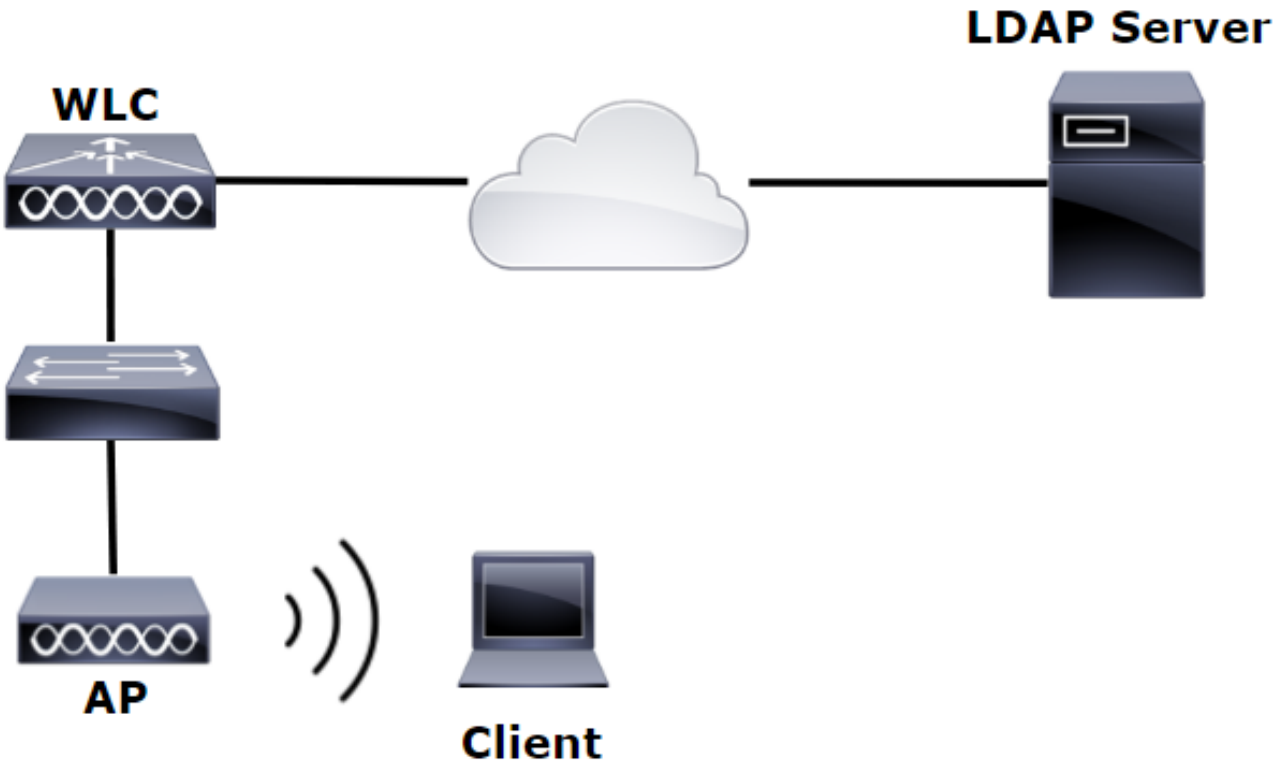
Para este procedimiento, sólo se deben autenticar los usuarios dentro de OU=SofiaLabOU.

Para aprender cómo utilizar la herramienta de Label Distribution Protocol (LDP), configure y resuelva problemas de LDAP, consulte la Guía de Configuración LDAP de WLC.

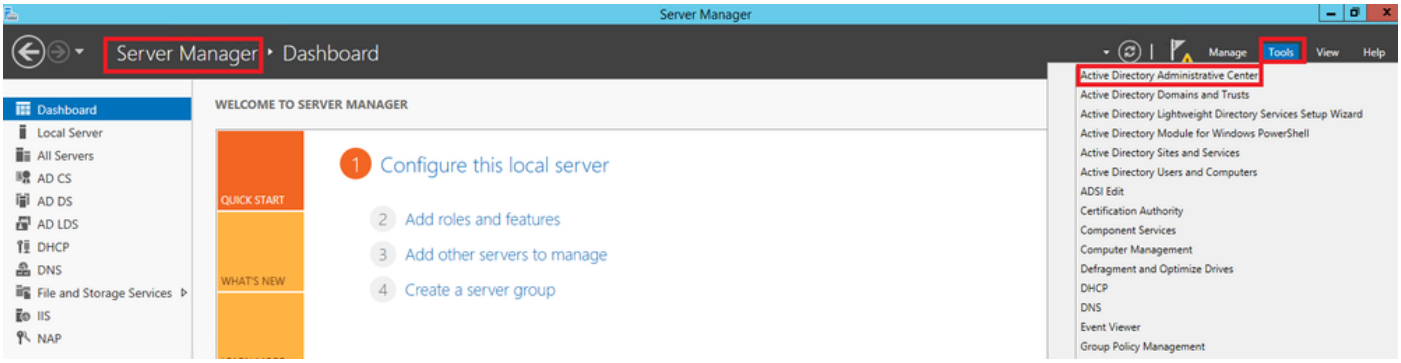
Crear una WLAN que se base en un servidor LDAP para autenticar usuarios a través de 802.1x

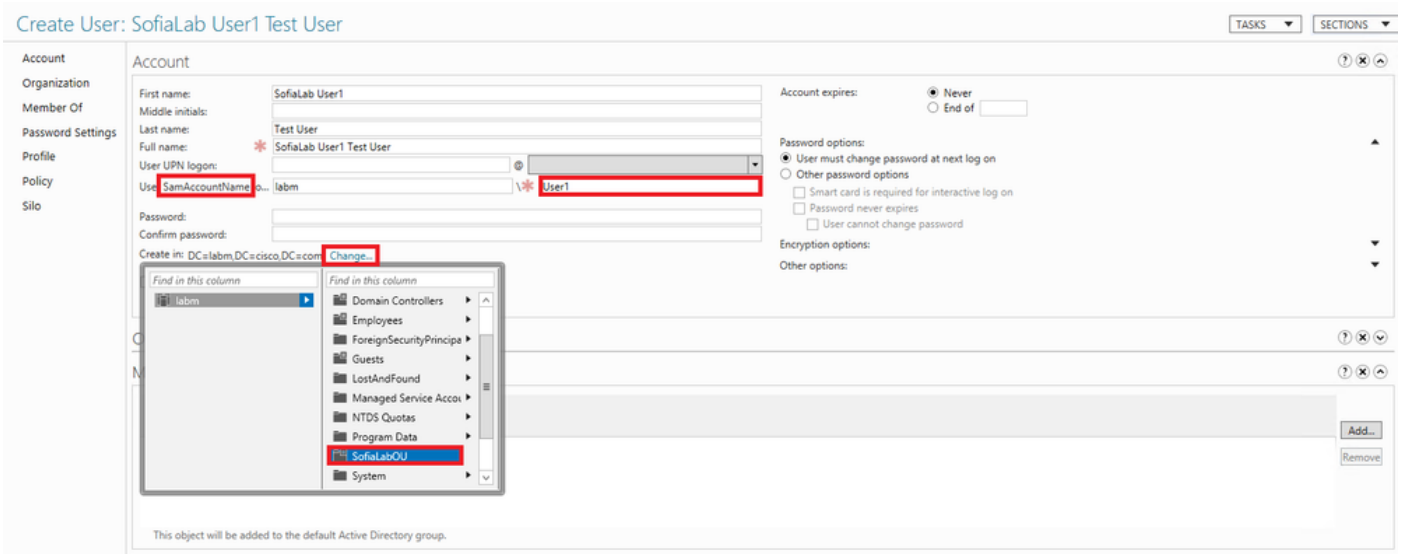
Diagrama de la red

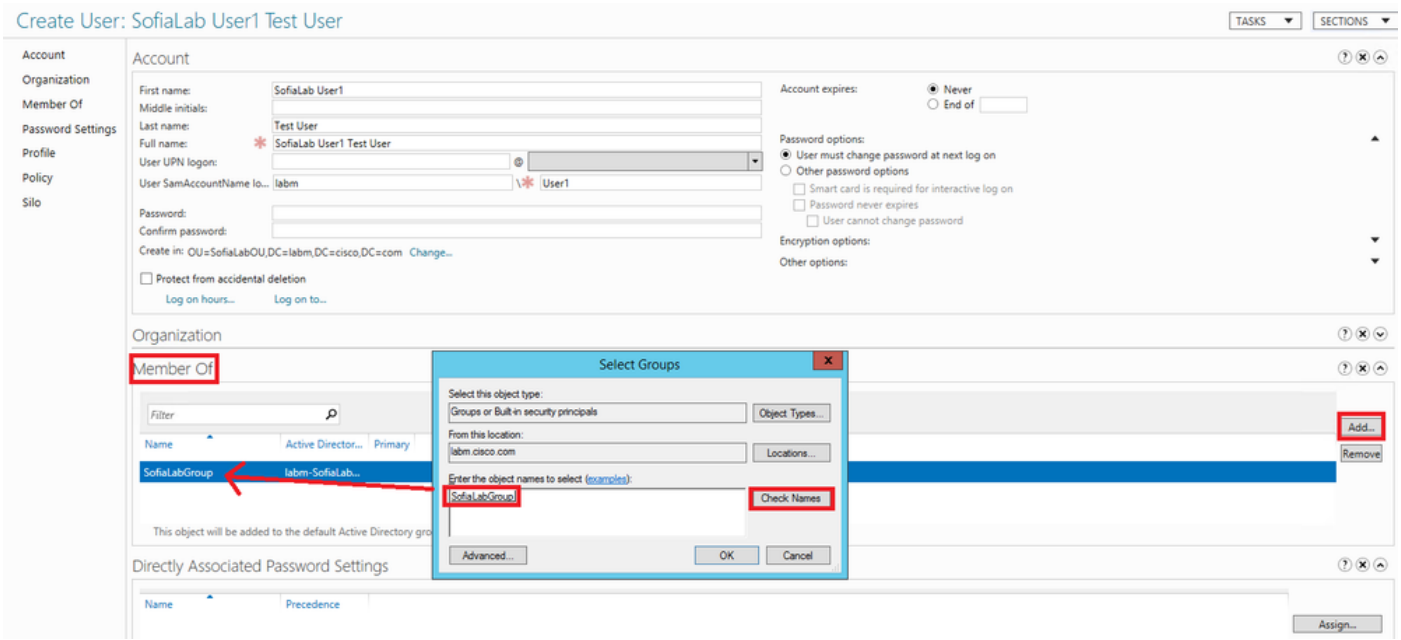
En este escenario, el LDAP-dot1x de WLAN utiliza un servidor LDAP para autenticar a los usuarios con el uso de 802.1x.



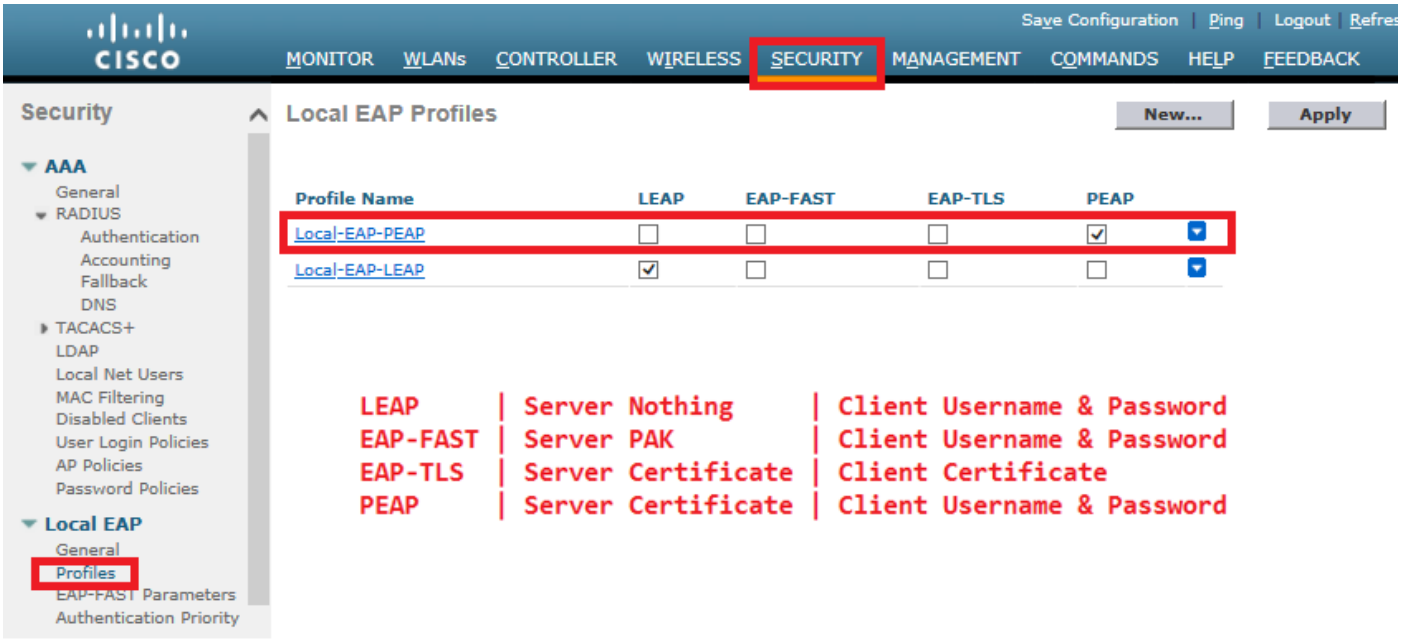
Paso 1. Cree un usuario **User1** en el servidor LDAP miembro de SofiaLabOU y SofiaLabGroup.





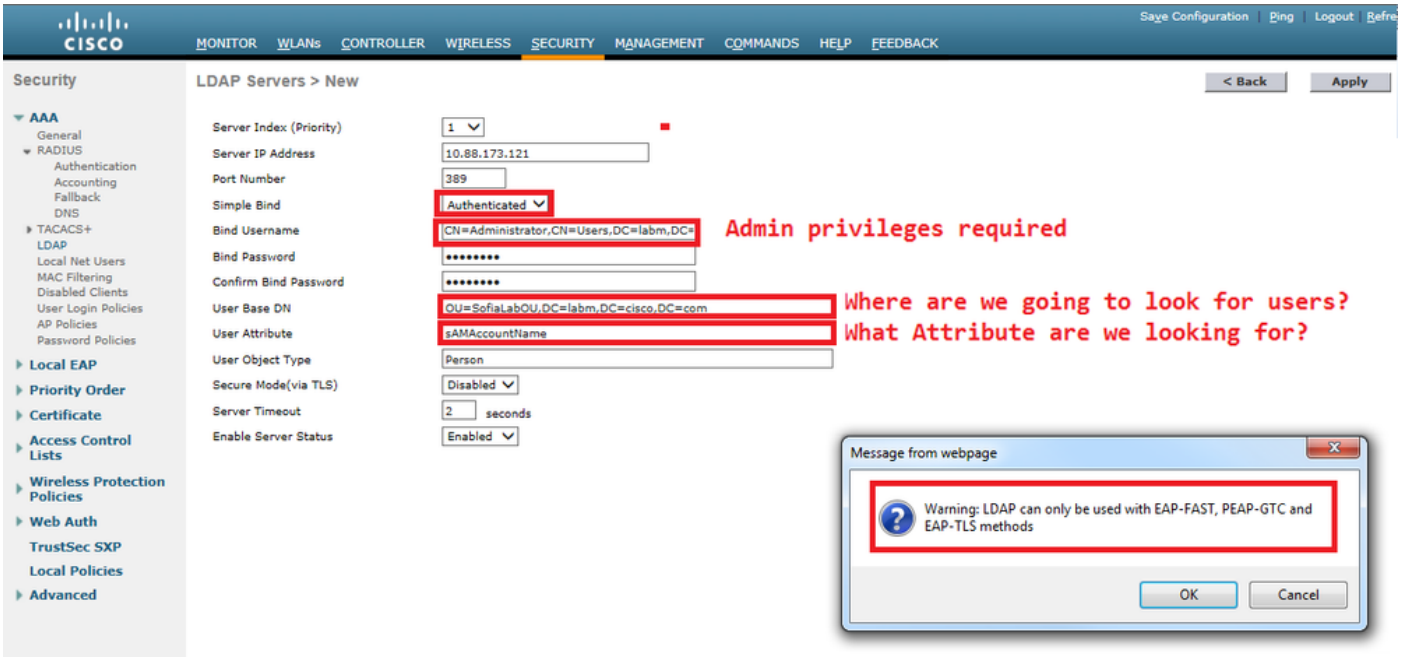


Paso 2. Cree un perfil EAP en el WLC con el método EAP deseado (utilice PEAP).



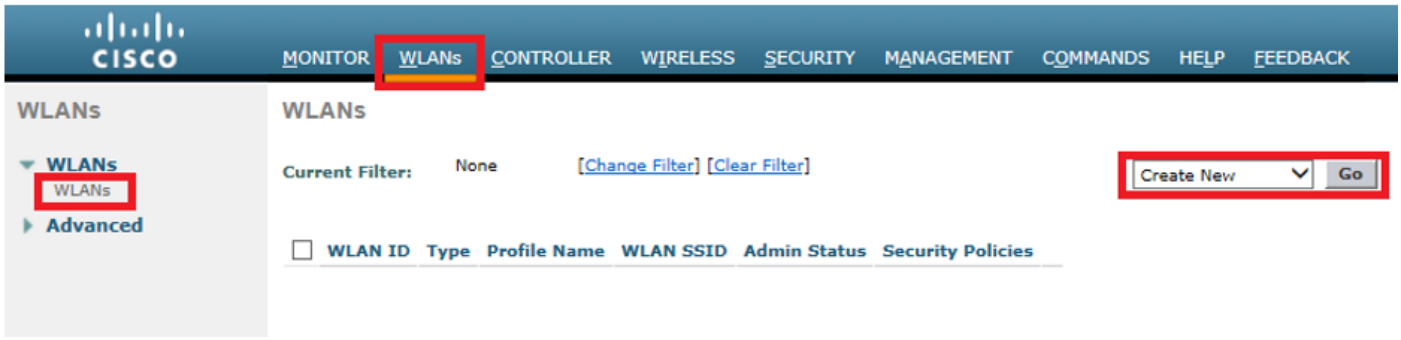
Paso 3. Enlace el WLC con el servidor LDAP.

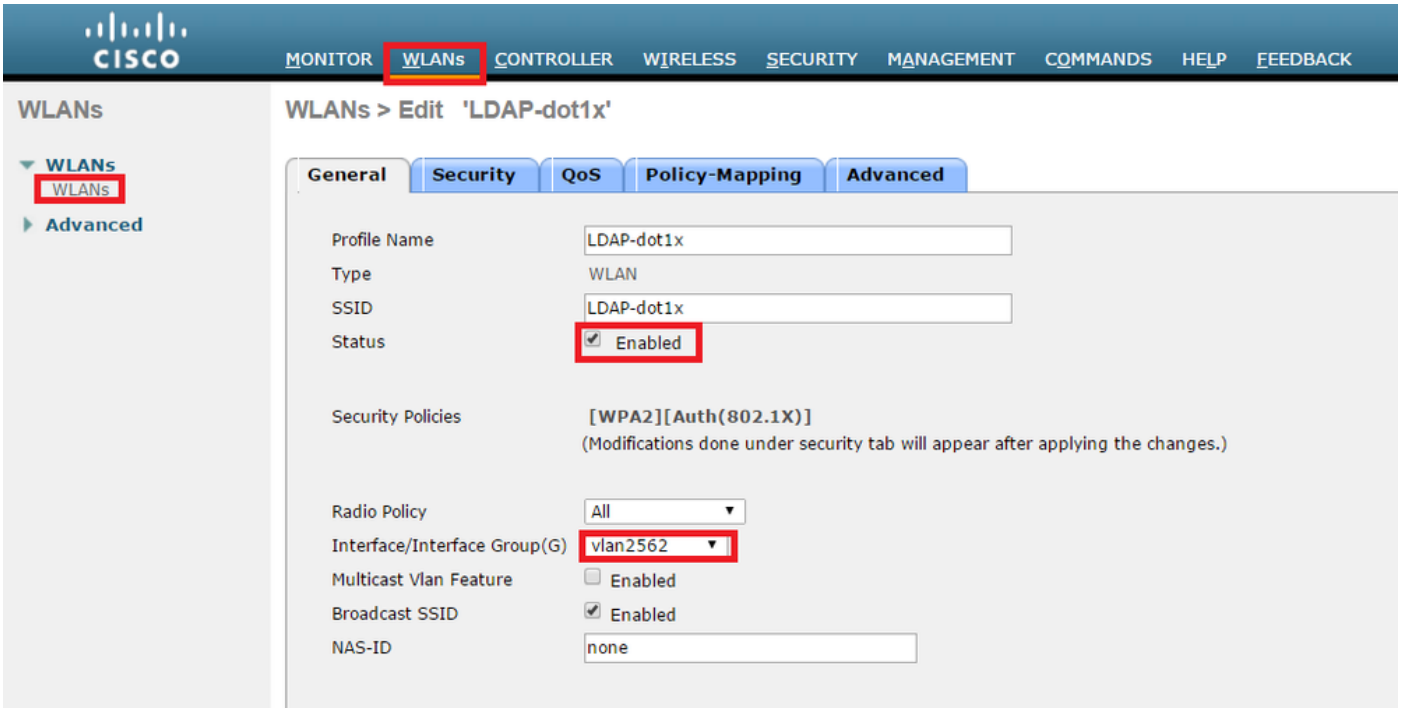
Sugerencia: Si el nombre de usuario de enlace no está en el DN base de usuario, debe escribir la ruta completa al usuario **Admin** tal y como se muestra en la imagen. De lo contrario, simplemente puede introducir **Administrator**.



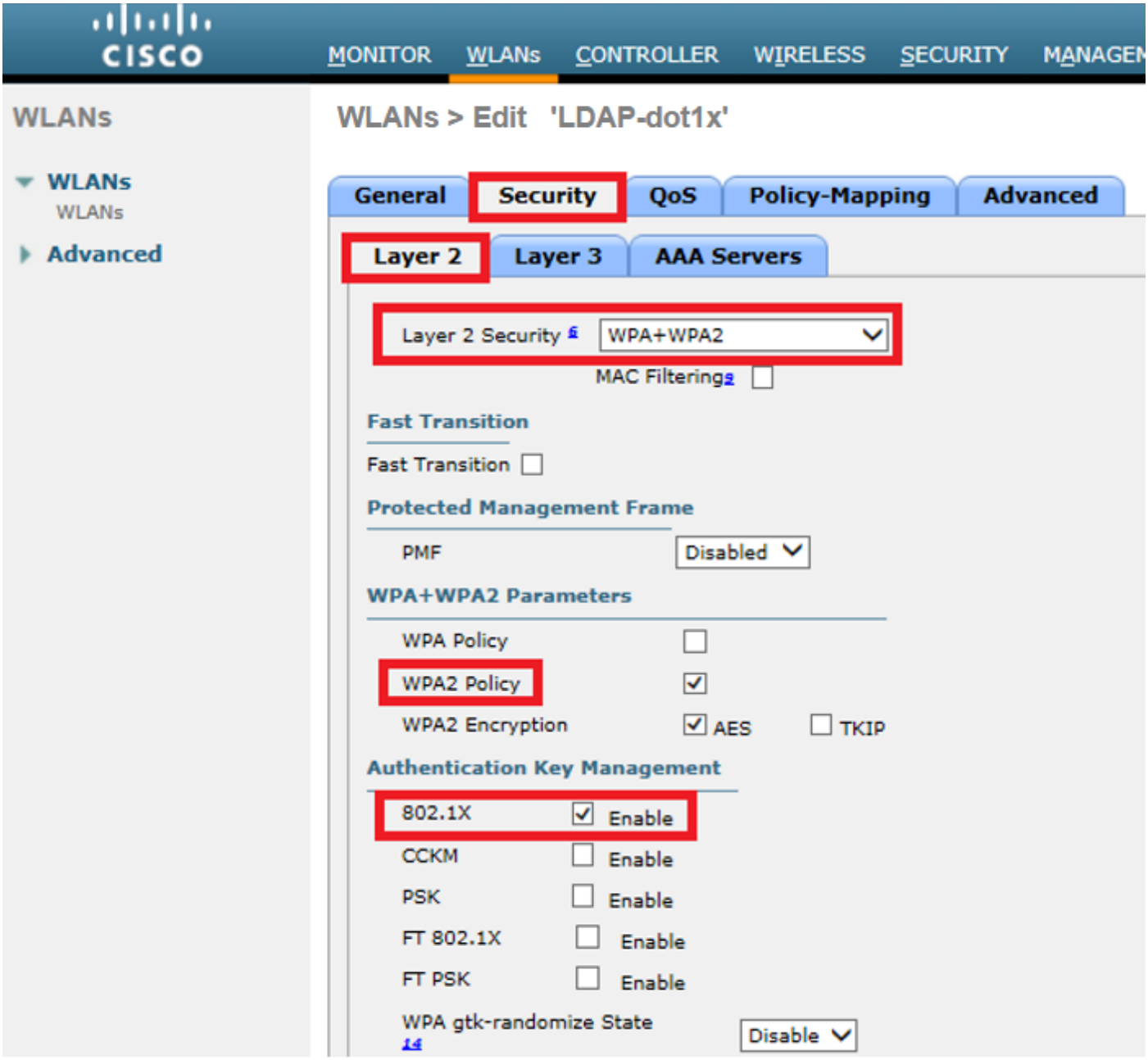
Paso 4. Establezca el Orden de autenticación para establecer en Usuarios internos + LDAP o LDAP solamente.

Paso 5. Cree la WLAN LDAP-dot1x.

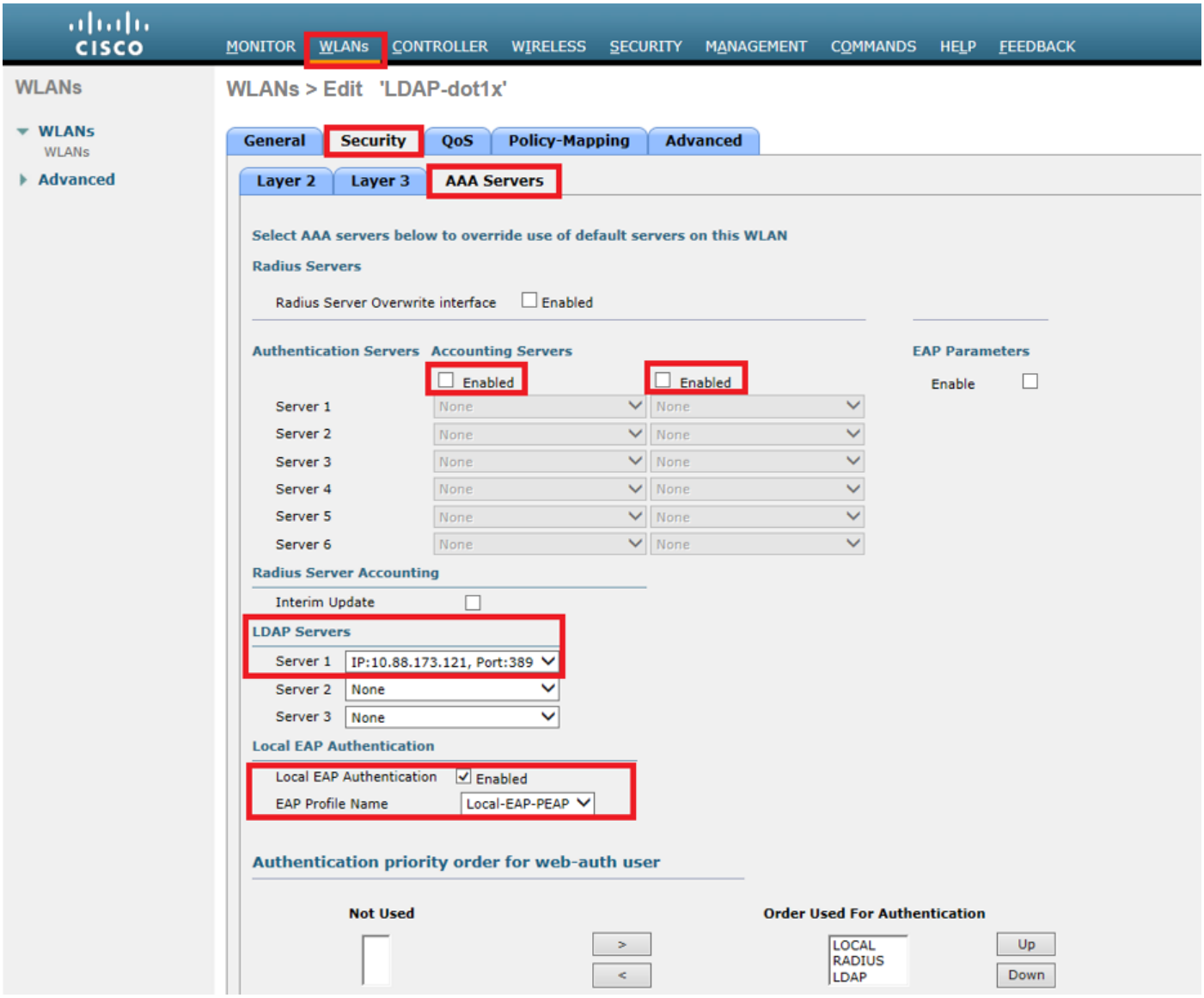




Paso 6. Establezca el método de seguridad L2 en WPA2 + 802.1x y establezca la seguridad L3 en none (ninguno).



Paso 7. Habilite la autenticación EAP local y asegúrese de que las opciones Servidores de autenticación y Servidores de cuentas estén inhabilitadas y que LDAP esté habilitado.



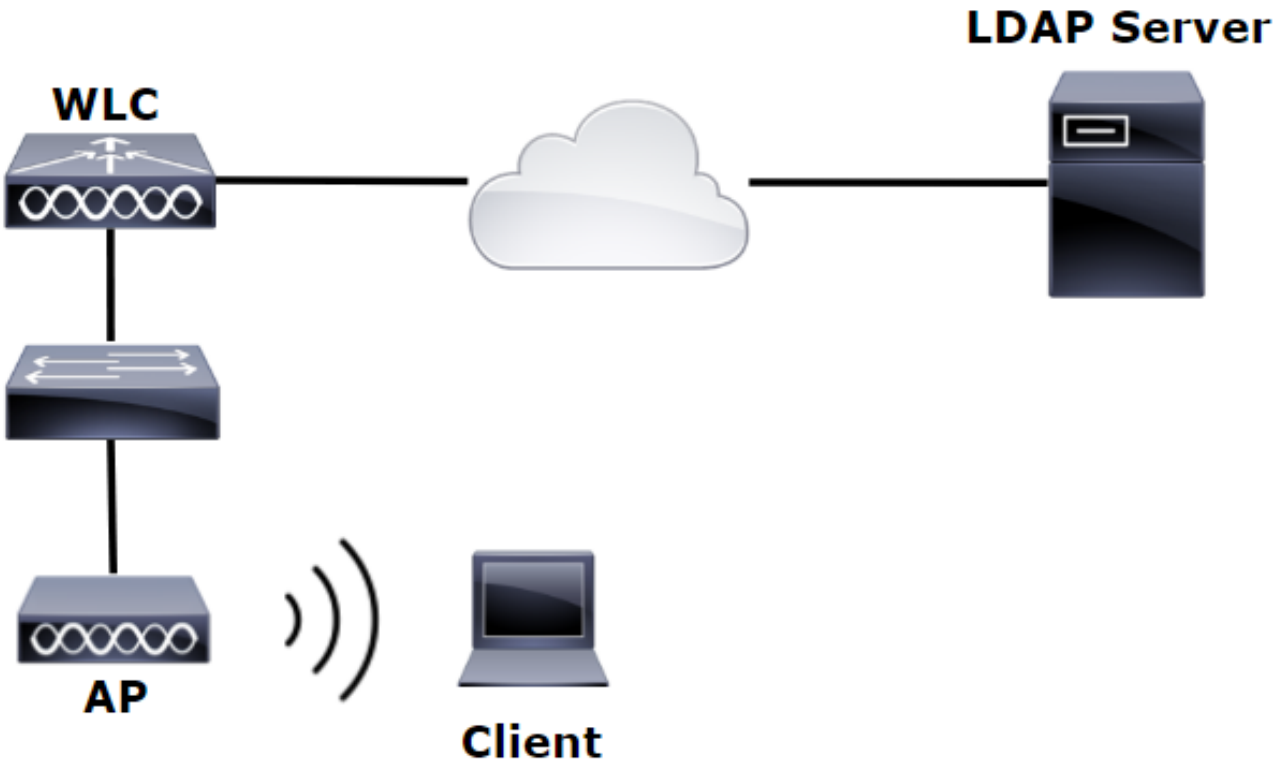
El resto de los parámetros se pueden dejar en los valores predeterminados.

Notas:
Utilice la herramienta LDP para confirmar los parámetros de configuración.
La base de búsqueda no puede ser un grupo (como SofiaLabGroup).
PEAP-GTC o Cisco:PEAP deben utilizarse en lugar de Microsoft:PEAP en el solicitante si se trata de un equipo con Windows. Microsoft:PEAP funciona de forma predeterminada con MacOS/iOS/Android.

Crear WLAN que confía en el servidor LDAP para autenticar a los usuarios a través del portal web interno del WLC

Diagrama de la red

En este escenario, el LDAP-Web de WLAN utiliza un servidor LDAP para autenticar a los usuarios con el portal Web interno del WLC.



Asegúrese de que los pasos 1. a 4. se han tomado del ejemplo anterior. A partir de ahí, la configuración de WLAN se establece de manera diferente.

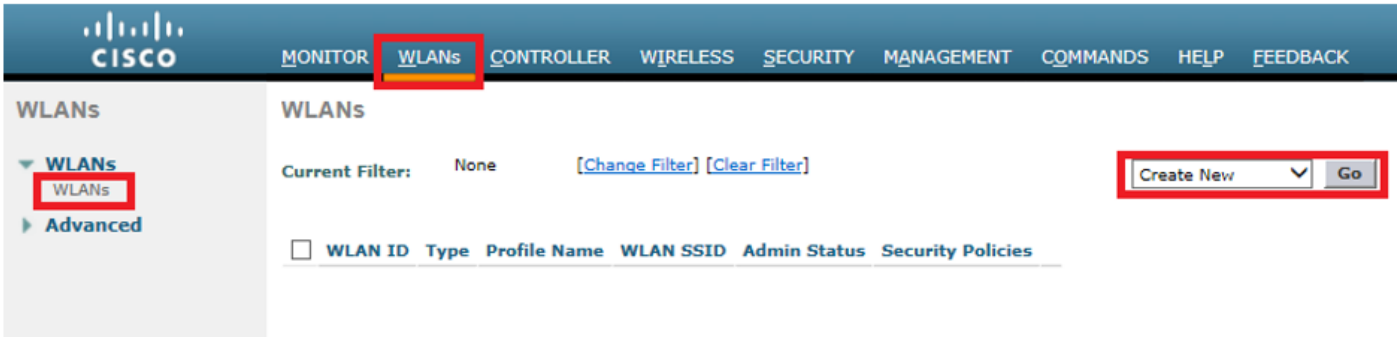
Paso 1. Cree un usuario **User1** en el miembro del servidor LDAP de OU SofiaLabOU y el grupo SofiaLabGroup.

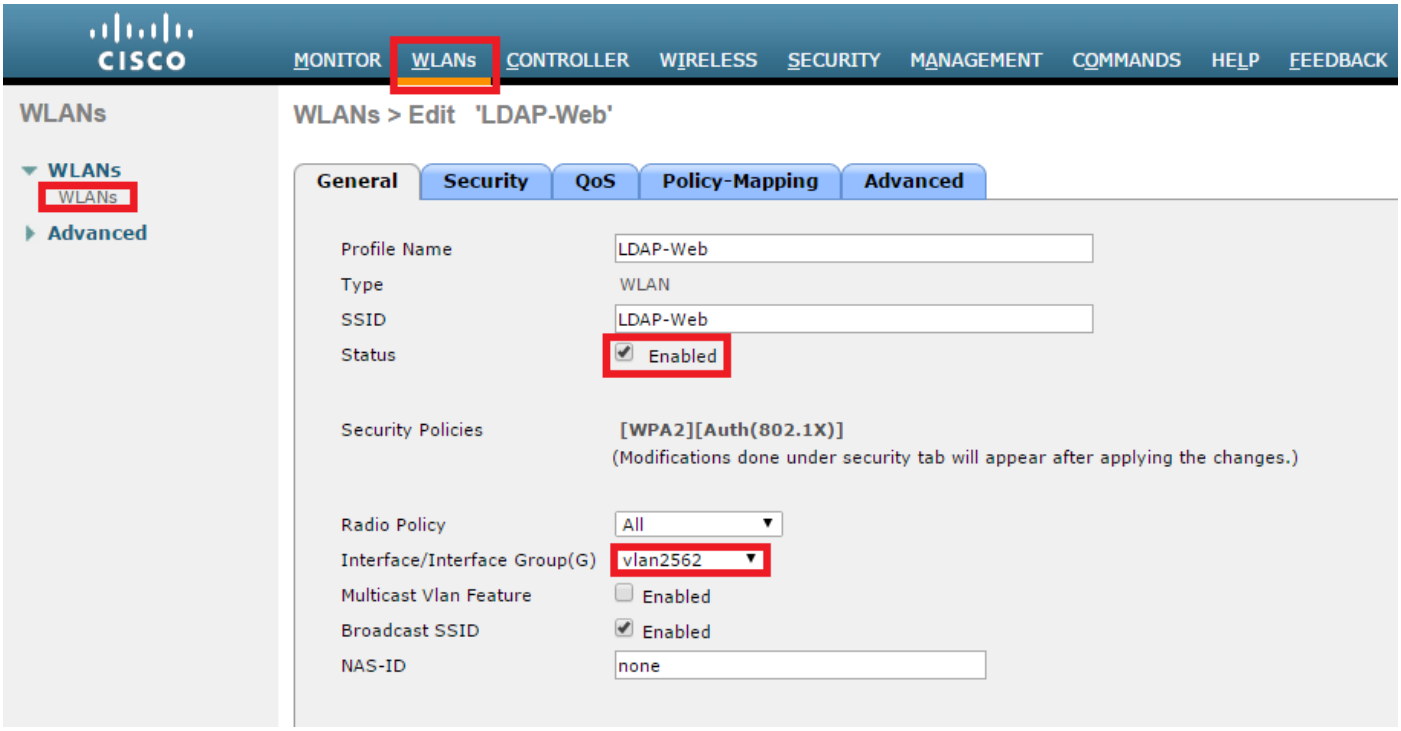
Paso 2. Cree un perfil EAP en el WLC con el método EAP deseado (utilice PEAP).

Paso 3. Enlace el WLC con el servidor LDAP.

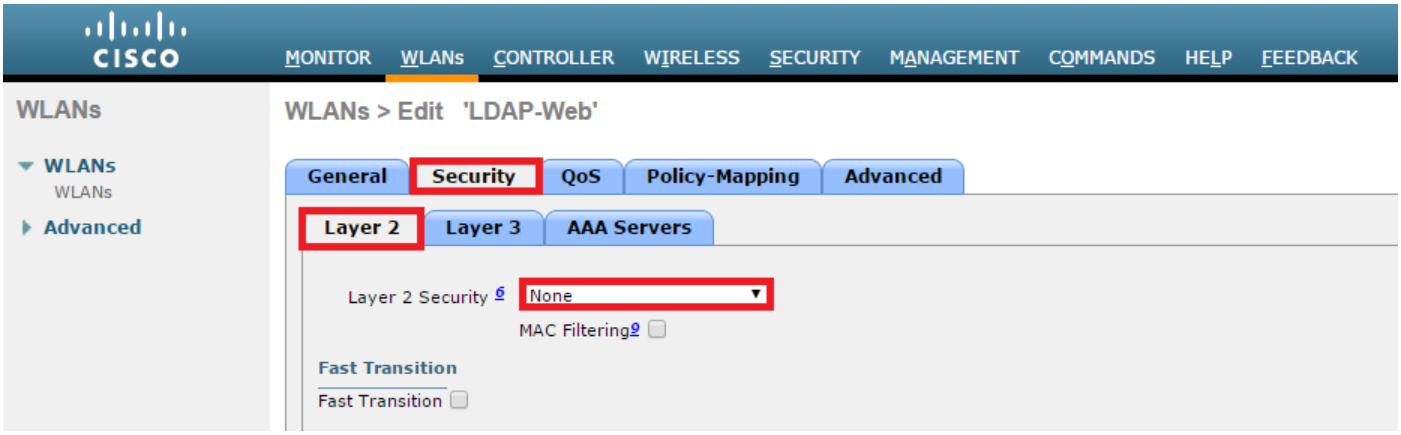
Paso 4. Establezca el Orden de autenticación en Usuarios internos + LDAP.

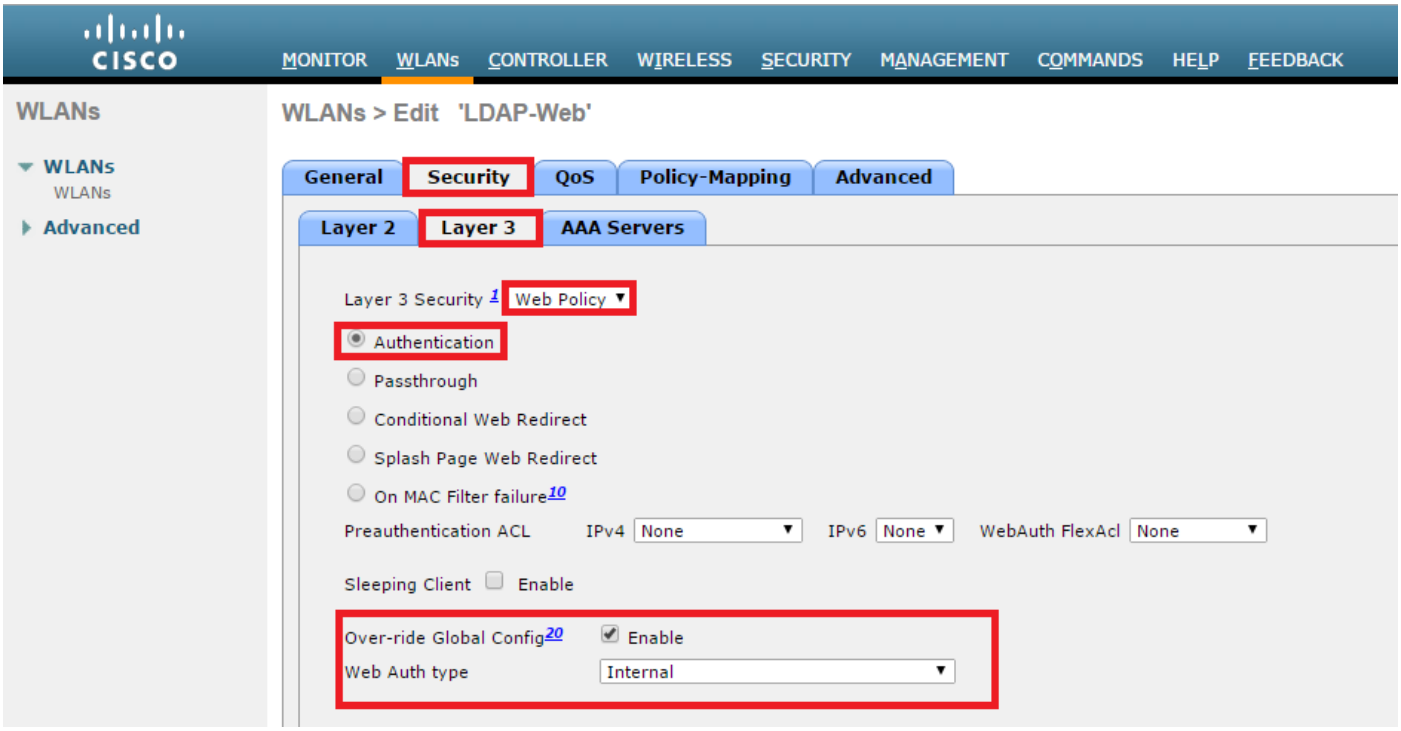
Paso 5. Cree la WLAN LDAP-Web como se muestra en las imágenes.



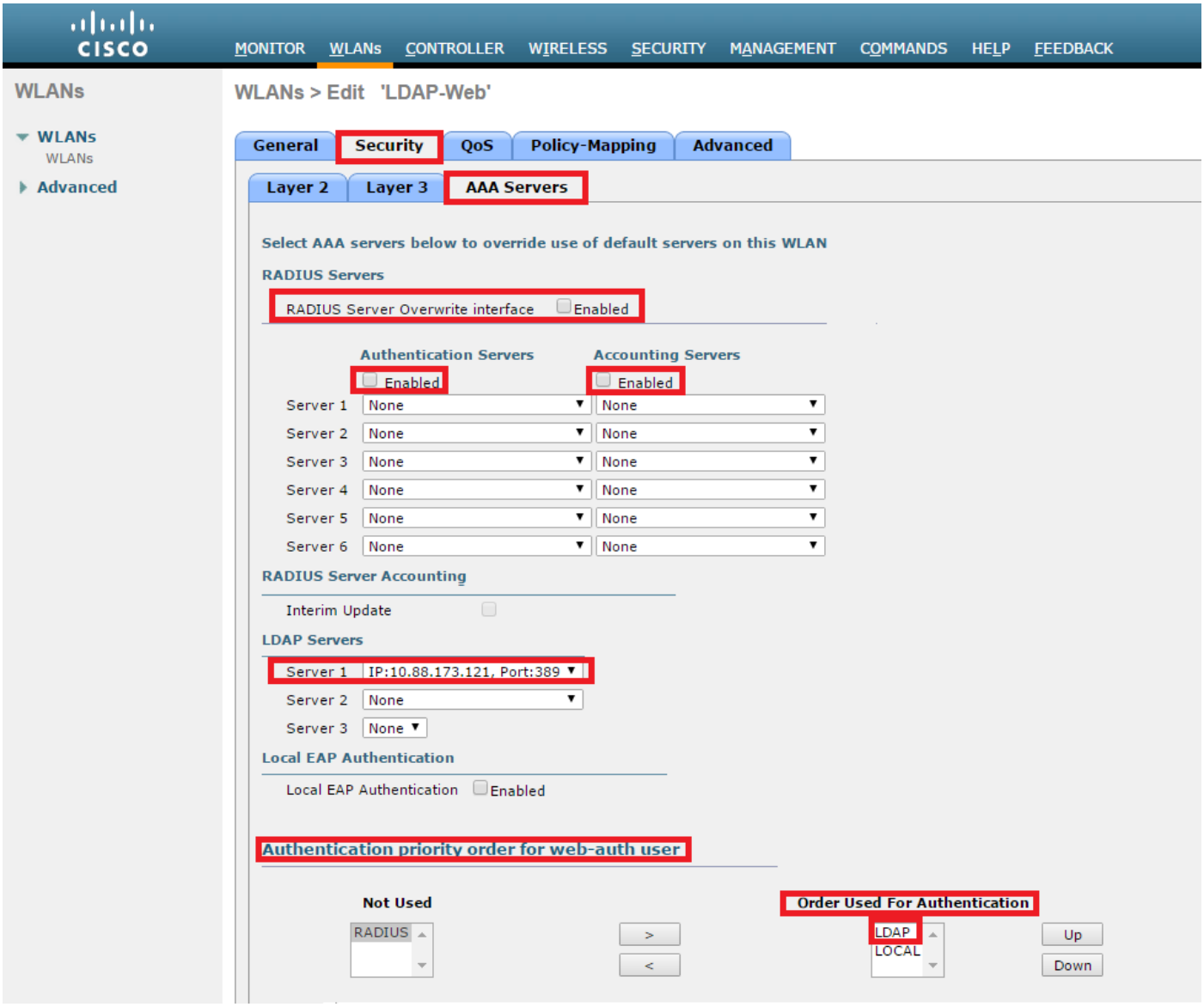


Paso 6. Establezca la seguridad L2 en none y la seguridad L3 en Web Policy - Authenticationcomo se muestra en las imágenes.





Paso 7. Establezca el orden de prioridad de autenticación para que web-auth utilice LDAP y asegúrese de que las opciones Servidores de autenticación y Servidores de cuentas estén inhabilitadas.



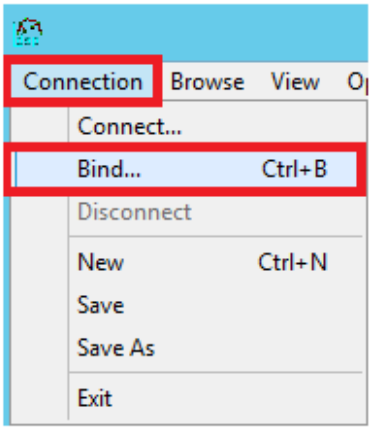
El resto de los parámetros se pueden dejar en los valores predeterminados.

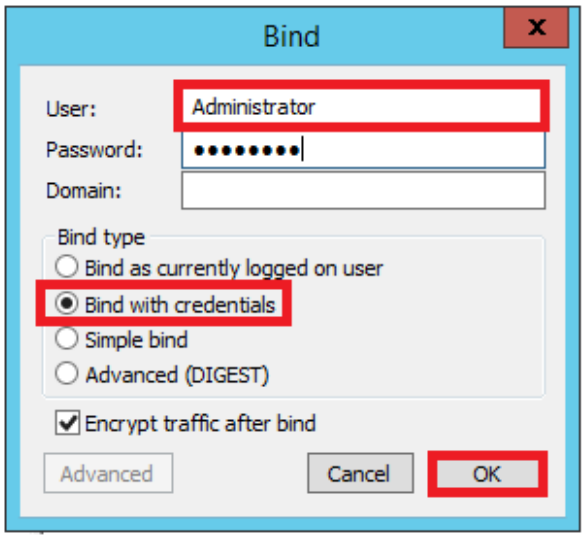
Utilice la herramienta LDP para configurar y solucionar problemas de LDAP

Paso 1. Abra la herramienta LDP en el servidor LDAP o en un host con conectividad (el puerto TCP 389 debe estar permitido al servidor).

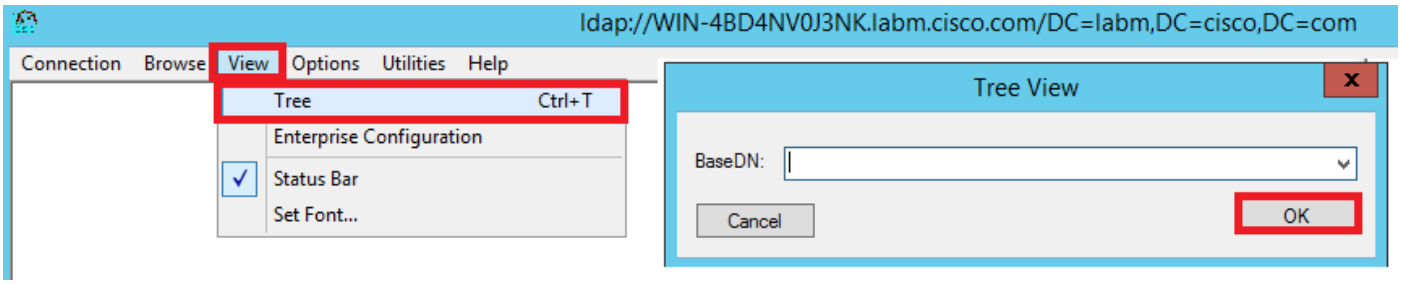
Paso 2. Navegue hasta **Conexión > Enlazar,** inicie sesión con un usuario administrador y

seleccione el botón de opción **Enlazar con credenciales**.

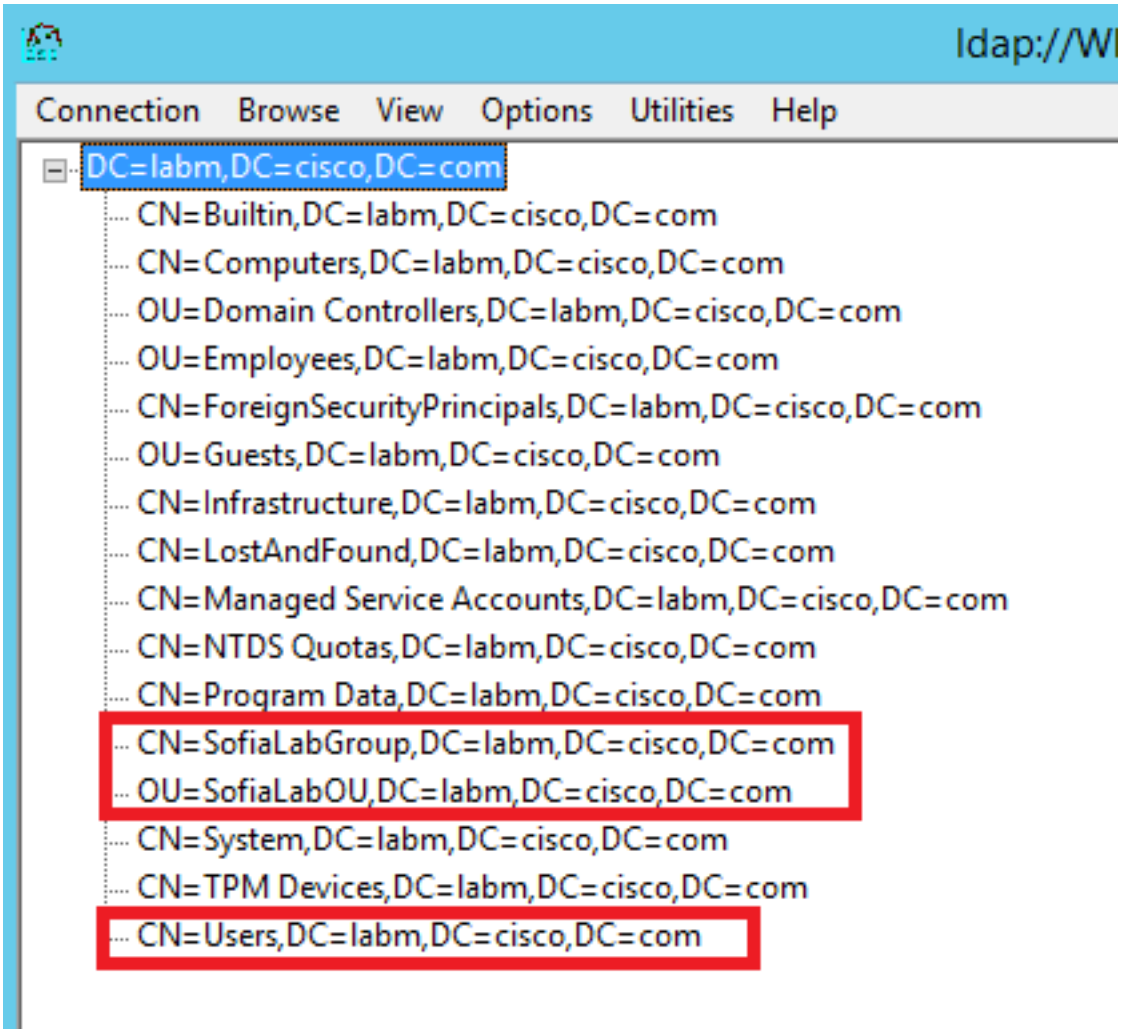




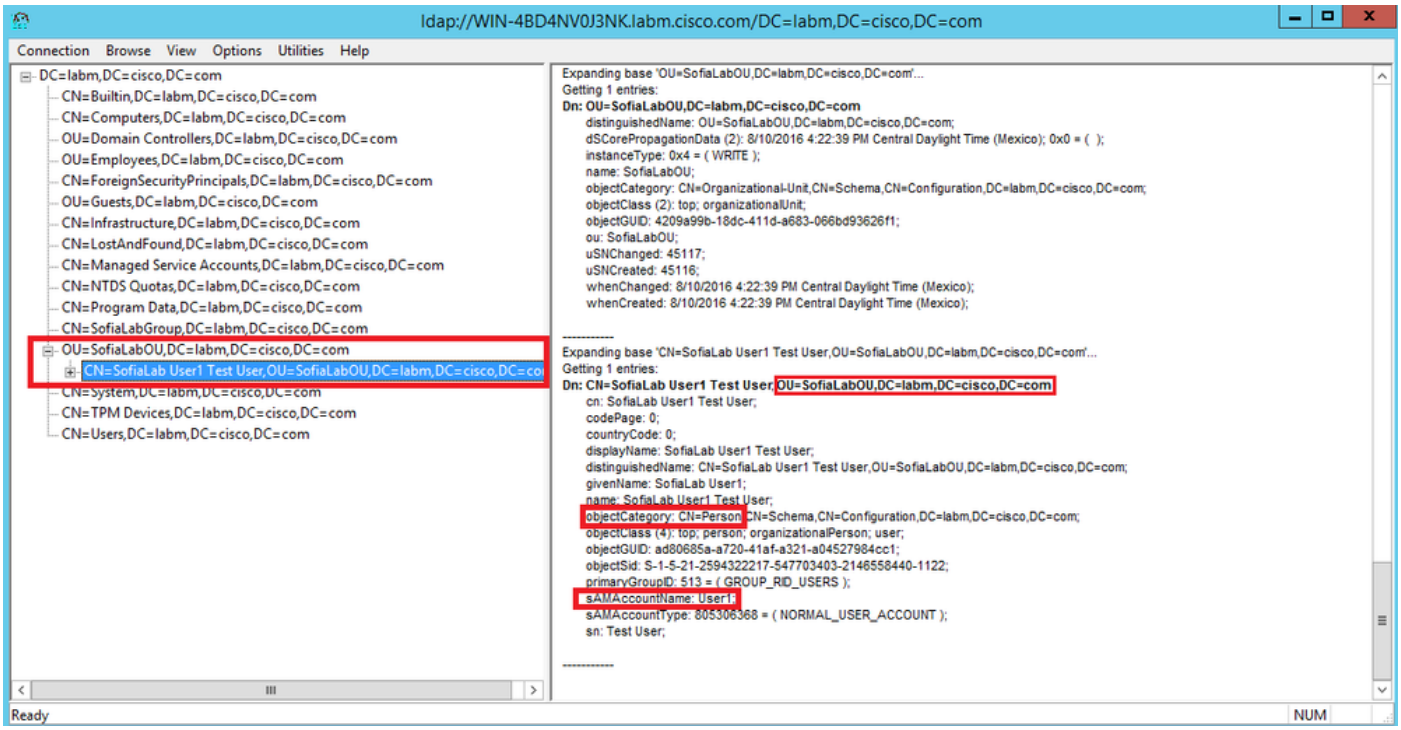
Paso 3. Navegue hasta **Ver > Árbol** y seleccione **Aceptar** en el DN base.



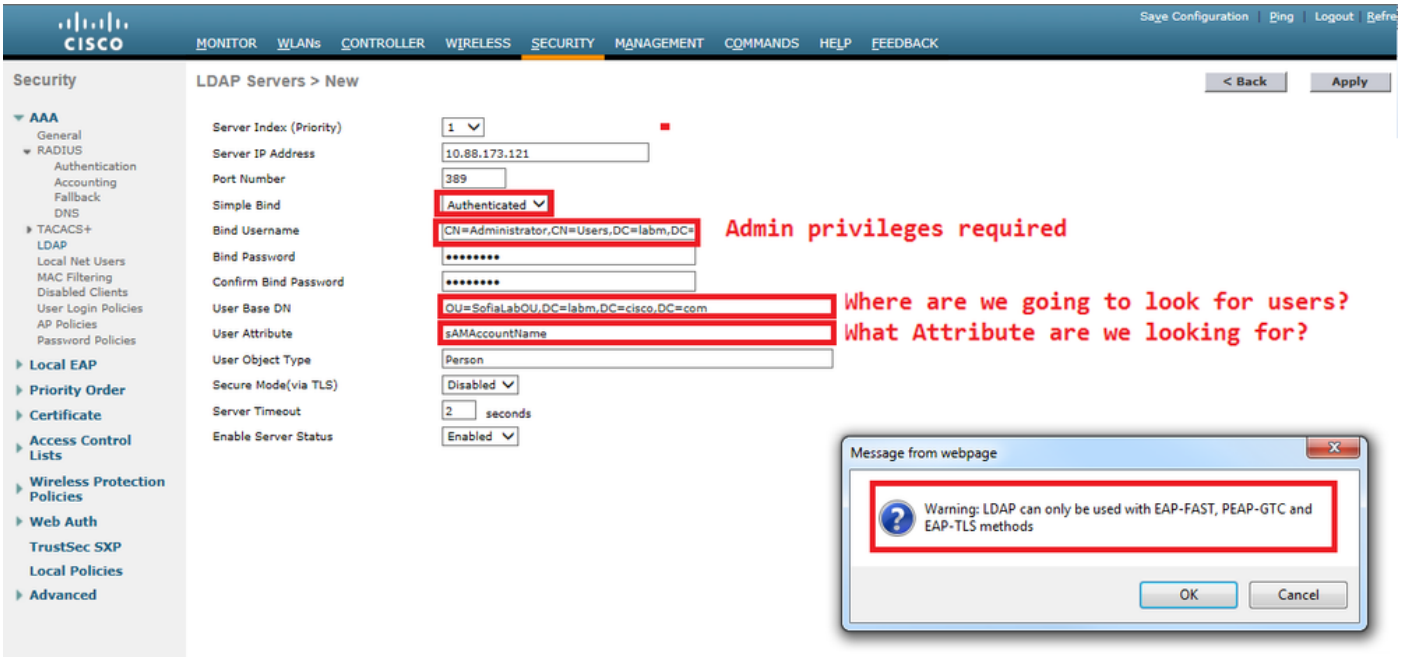
Paso 4. Expanda el árbol para ver la estructura y buscar el DN de base de búsqueda. Tenga en cuenta que puede ser cualquier tipo de contenedor excepto Grupos. Puede ser el dominio completo, una OU específica o un CN como CN=Users.



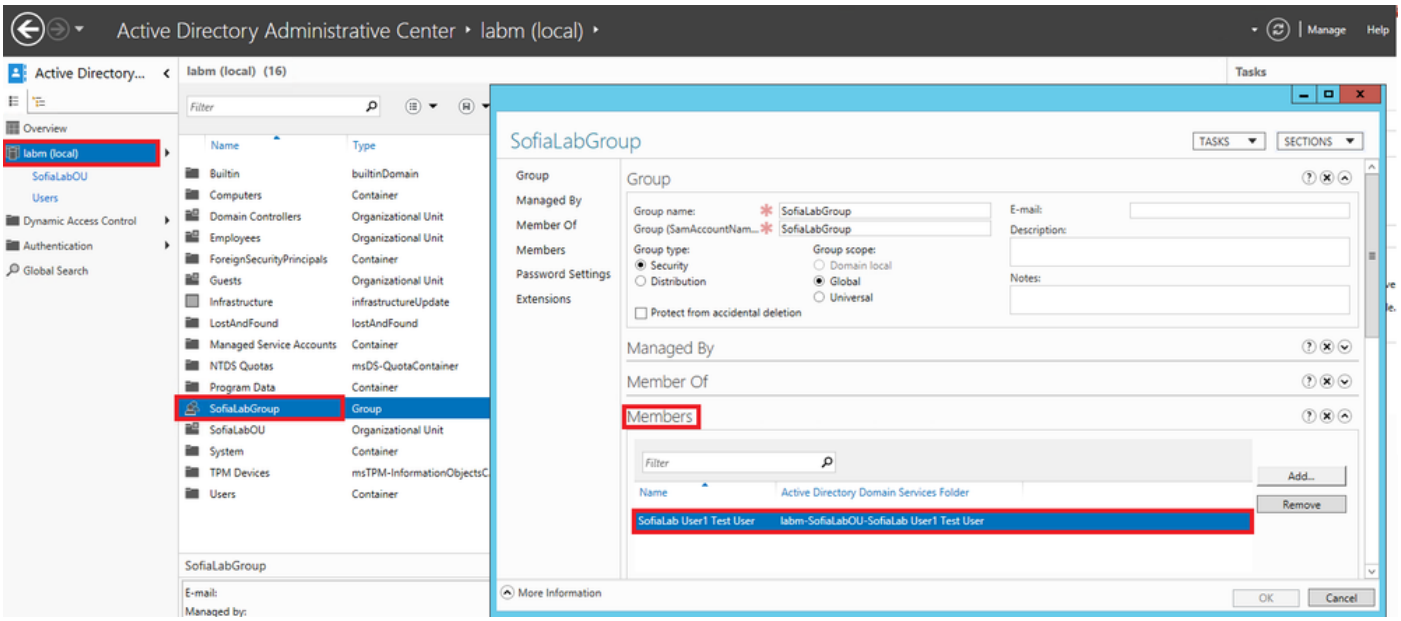
Paso 5. Expanda SofiaLabOU para ver qué usuarios están dentro de ella. Existe el usuario User1 que se creó anteriormente.



Paso 6. Todo lo necesario para configurar LDAP.



Paso 7. Los grupos como SofiaLabGroup no se pueden utilizar como DN de búsqueda. Expanda el grupo y busque los usuarios que se encuentran en su interior, donde debe estar el User1 creado anteriormentecomo se muestra.



El usuario 1 estaba allí, pero LDP no pudo encontrarlo. Significa que el WLC no puede hacerlo también y que es porqué los grupos no se soportan como un DN de la base de búsqueda.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

```
(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
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

```
(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
```

Información Relacionada

- Guía de Configuración de LDAP - WLC 8.2
- Cómo configurar el controlador de LAN inalámbrica (WLC) para la autenticación del protocolo ligero de acceso a directorios (LDAP) - por Vinay Sharma
- Ejemplo de Configuración de Autenticación Web Usando LDAP en Controladores LAN Inalámbricos (WLCs) - por Yahya Jaber y Ayman Alfares
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).