为 802.1x 和 Web-Auth WLAN 配置具备 LDAP 身份验证的 WLC

目录

简介

本文档介绍配置AireOS WLC以使用LDAP服务器作为用户数据库对客户端进行身份验证的过程。

先决条件

要求

建议掌握下列主题的相关知识：

- Microsoft Windows服务器
- Active Directory

使用的组件

本文档中的信息基于以下软件版本：

- 思科WLC软件8.2.110.0
- Microsoft Windows Server 2012 R2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

技术背景

- LDAP是用于访问目录服务器的协议。
- 目录服务器是分层的、面向对象的数据库。
- 对象以CN=Users形式组织到容器中，例如组织单位(OU)、组或默认Microsoft容器。
- 此设置最难的部分是在WLC上正确配置LDAP服务器参数。

有关这些概念的更多详细信息，请参阅如何为轻量级目录访问协议(LDAP)身份验证配置无线局域网控制器(WLC)的简介部分。

常见问题

- 必须使用什么用户名与LDAP服务器绑定？

有两种方法可以与LDAP服务器绑定，即Anonymous或Authenticated（为了了解两种方法之间的区别，请参阅）。

此绑定用户名需要具有管理员权限，才能查询其他用户名/密码。

- 如果经过身份验证：绑定用户名是否与所有用户位于同一容器中？

不：使用整个路径。例如：

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

是：仅使用用户名。例如：

管理员

- 如果用户位于不同的容器中怎么办？所有涉及的无线LDAP用户是否需要位于同一容器中？

否，可以指定包含所需所有容器的基本DN。

- WLC必须查找哪些属性？

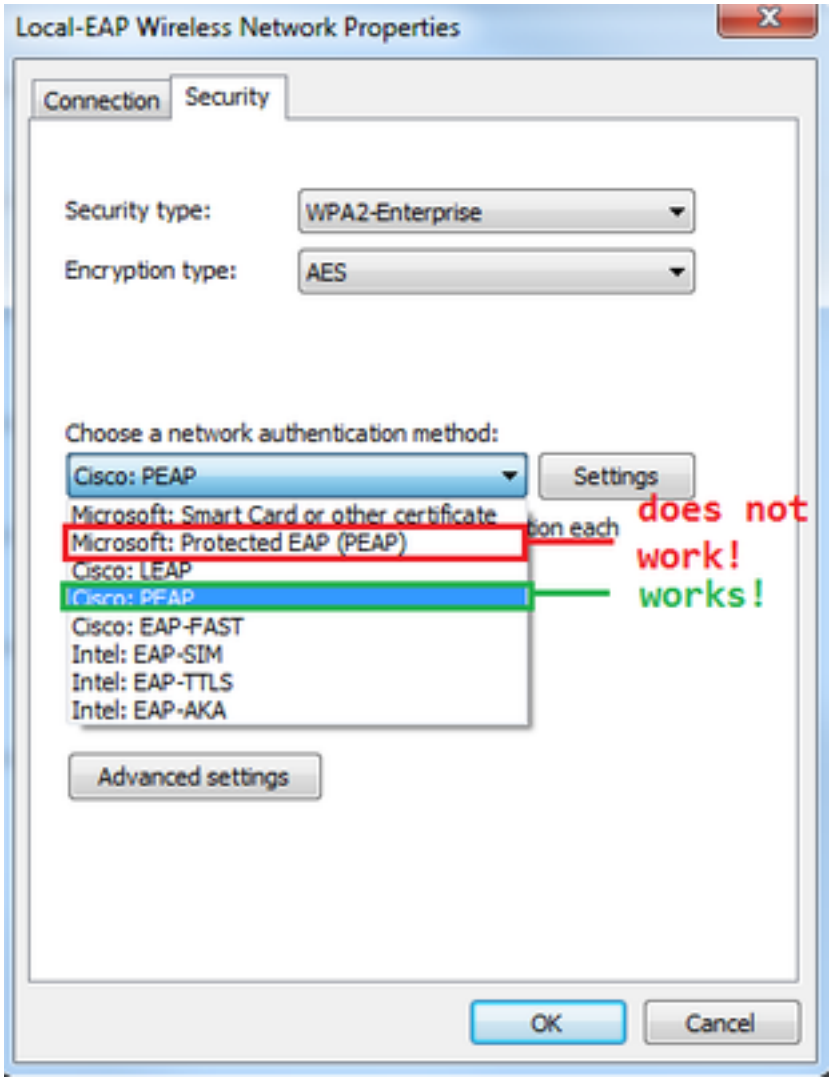
WLC与指定的用户属性和对象类型匹配。

> **注意**:**sAMAccountName**区分大小写，但person不区分大小写。因此，**sAMAccountName=RICARDO**和**sAMAccountName=ricardo**相同，并且工作正常，而**samaccountname=RICARDO**和**samaccountname=ricardo**则不同。

- 可以使用哪种可扩展身份验证协议(EAP)方法？

仅EAP-FAST、PEAP-GTC和EAP-TLS。Android、iOS和MacOS默认请求方使用受保护的可扩展身份验证协议(PEAP)。

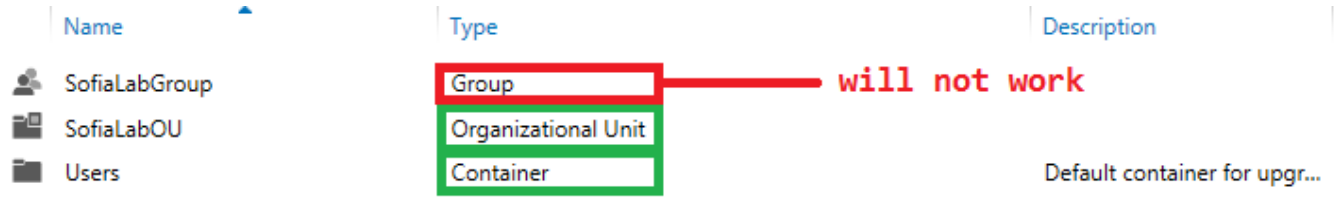
对于Windows，必须在支持的无线适配器上使用Anyconnect网络访问管理器(NAM)或带有Cisco:PEAP的默认Windows请求方，如图所示。



注意：Cisco EAP Plug-ins for Windows包括受Cisco bug ID CSCva09670影响的开放安全套接字层(OpenSSL 0.9.8k)版本，思科不计划发布任何其他版本的Windows EAP插件，并建议客户改用AnyConnect安全移动客户端。

- 为什么WLC找不到用户？

无法对组内的用户进行身份验证。它们需要位于默认容器(CN)或组织单位(OU)内，如图所示。



配置

有多种不同的方案可以采用LDAP服务器，包括802.1x身份验证或Web身份验证。

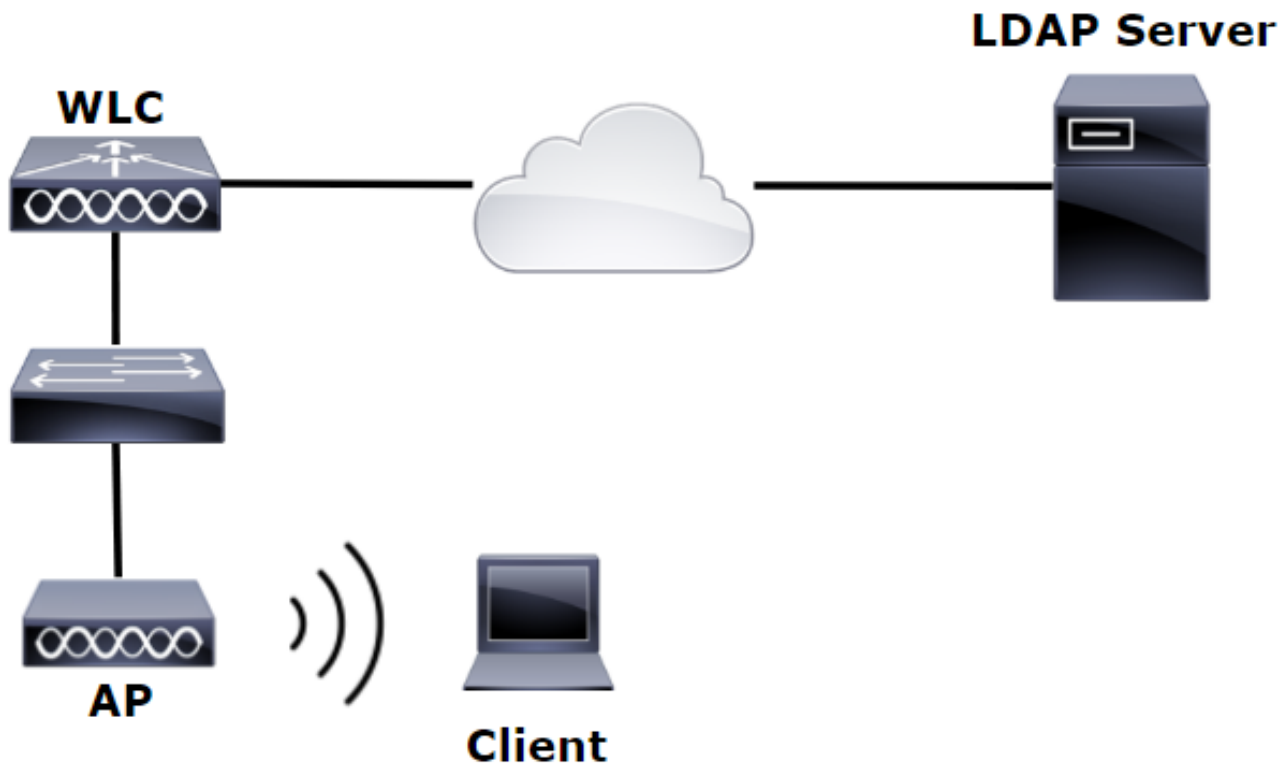
对于此过程，仅必须对OU=SofiaLabOU内的用户进行身份验证。

要了解如何使用Label Distribution Protocol(LDP)工具、配置并对LDAP进行故障排除，请参阅WLC LDAP配置指南。

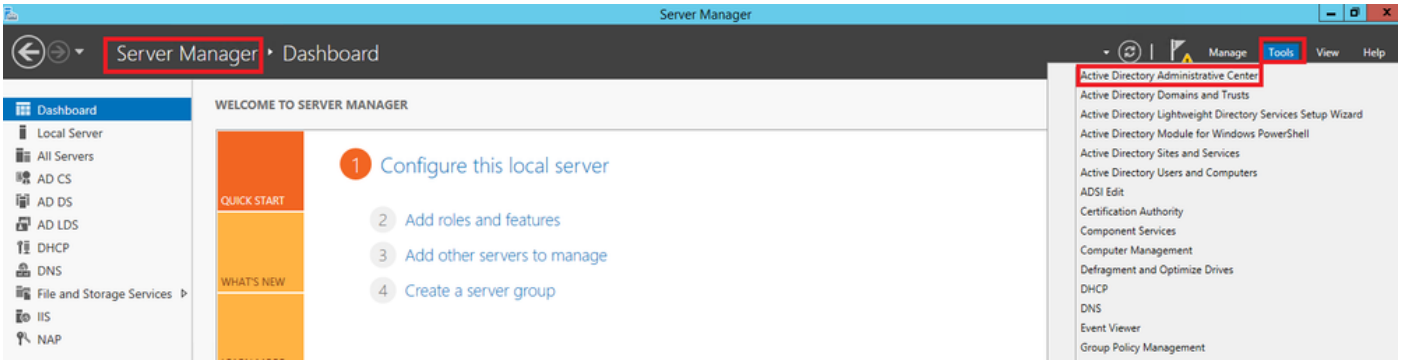
创建依赖LDAP服务器通过802.1x对用户进行身份验证的WLAN

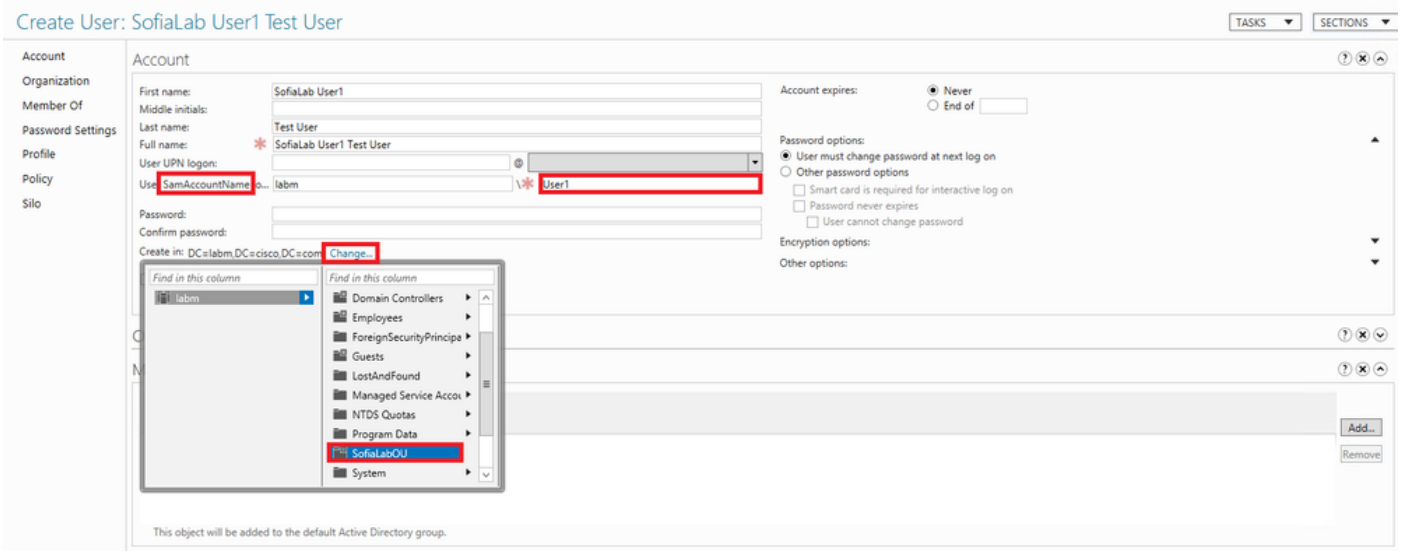
网络图

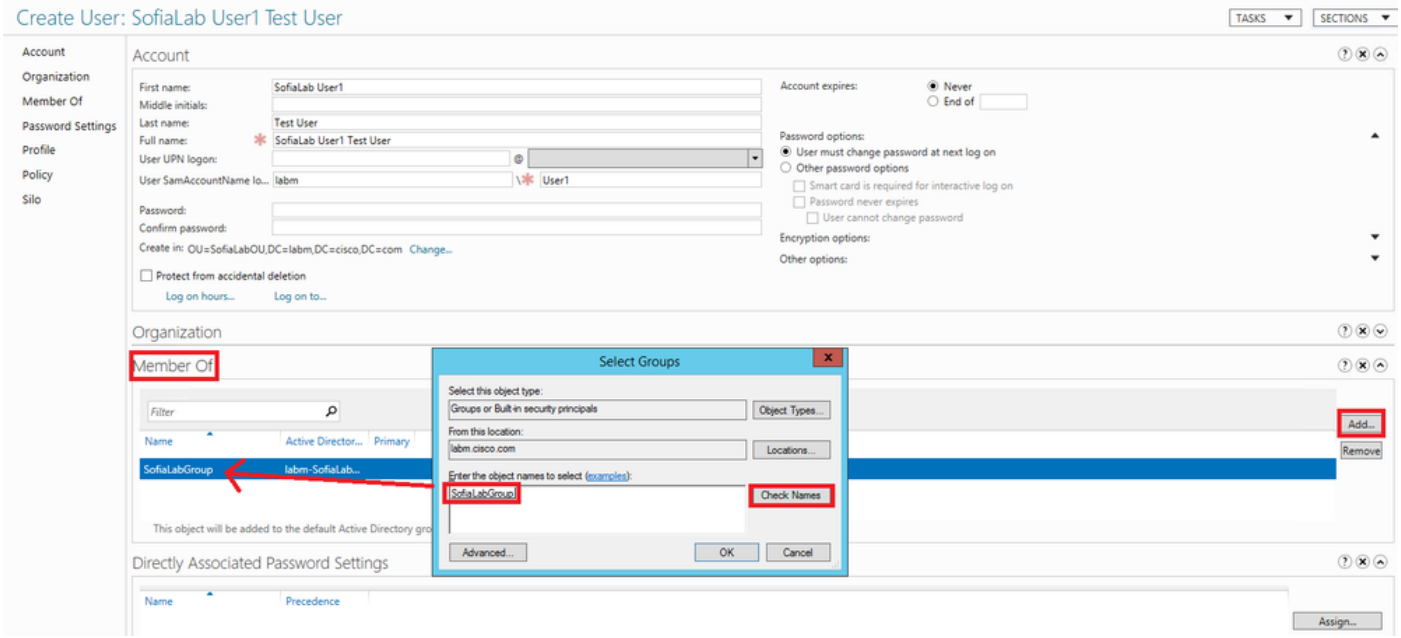
在此方案中，WLAN LDAP-dot1x使用LDAP服务器使用802.1x对用户进行身份验证。



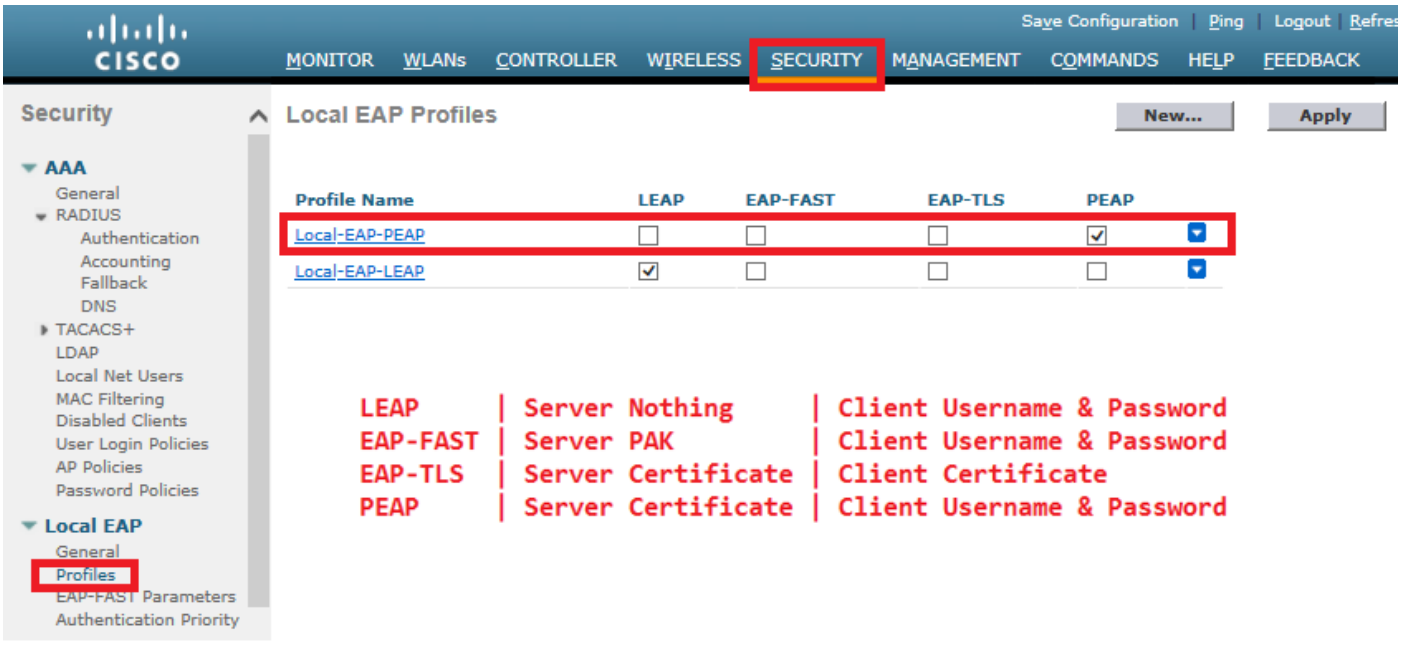
步骤1:在SofiaLabOU和SofiaLabGroup的LDAP服务器成员中创建用户**User1**。





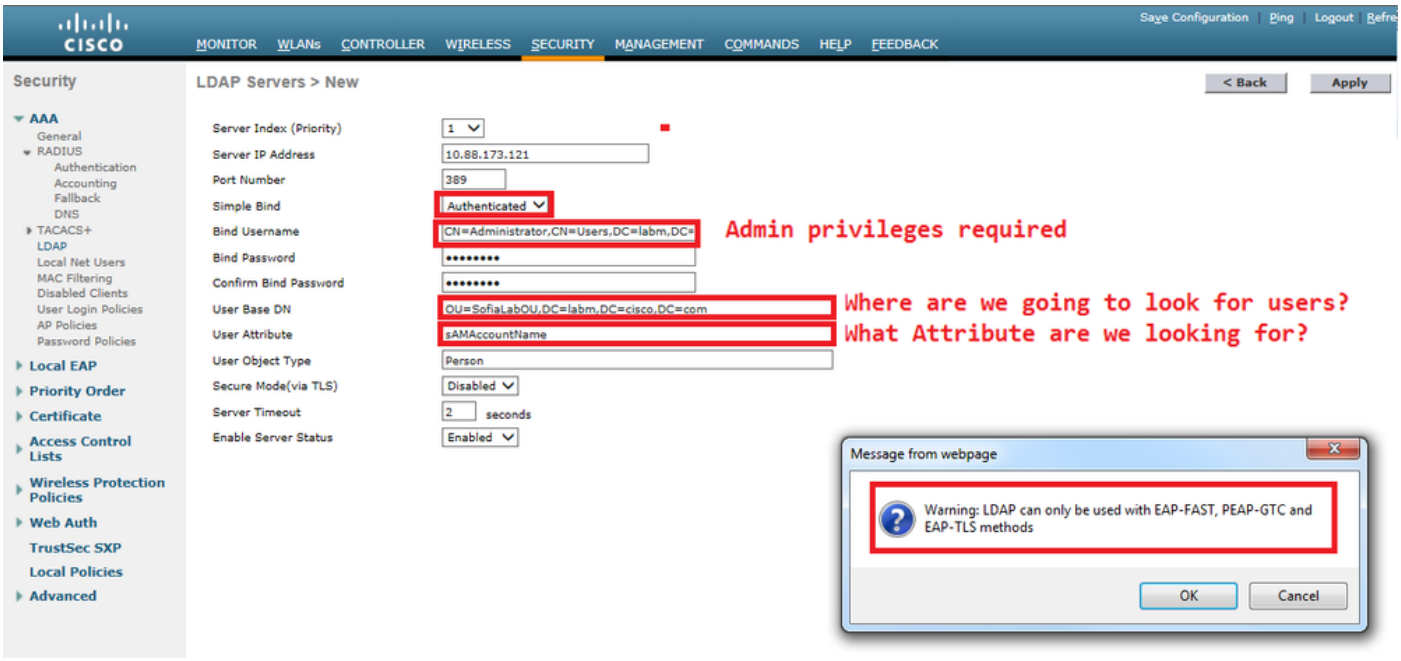


第二步：使用所需的EAP方法在WLC上创建EAP配置文件（使用PEAP）。



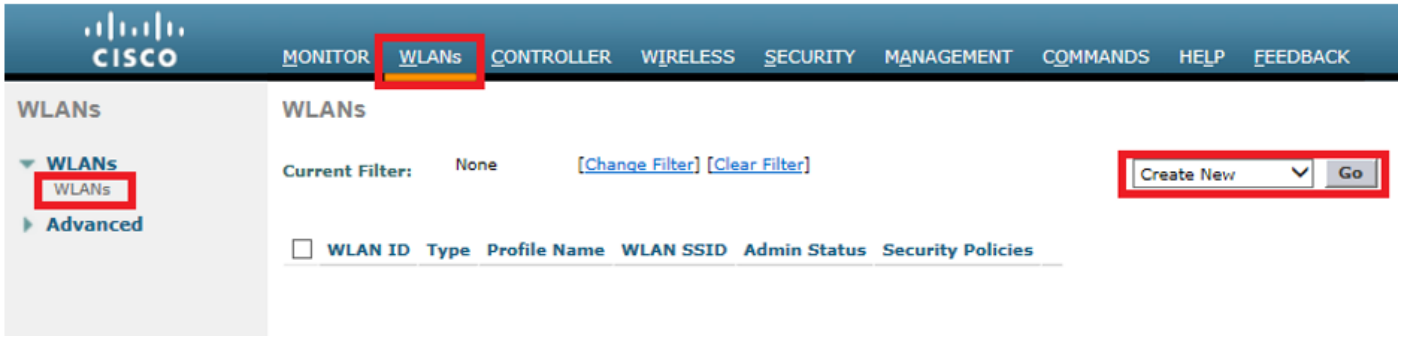
第三步：将WLC与LDAP服务器绑定。

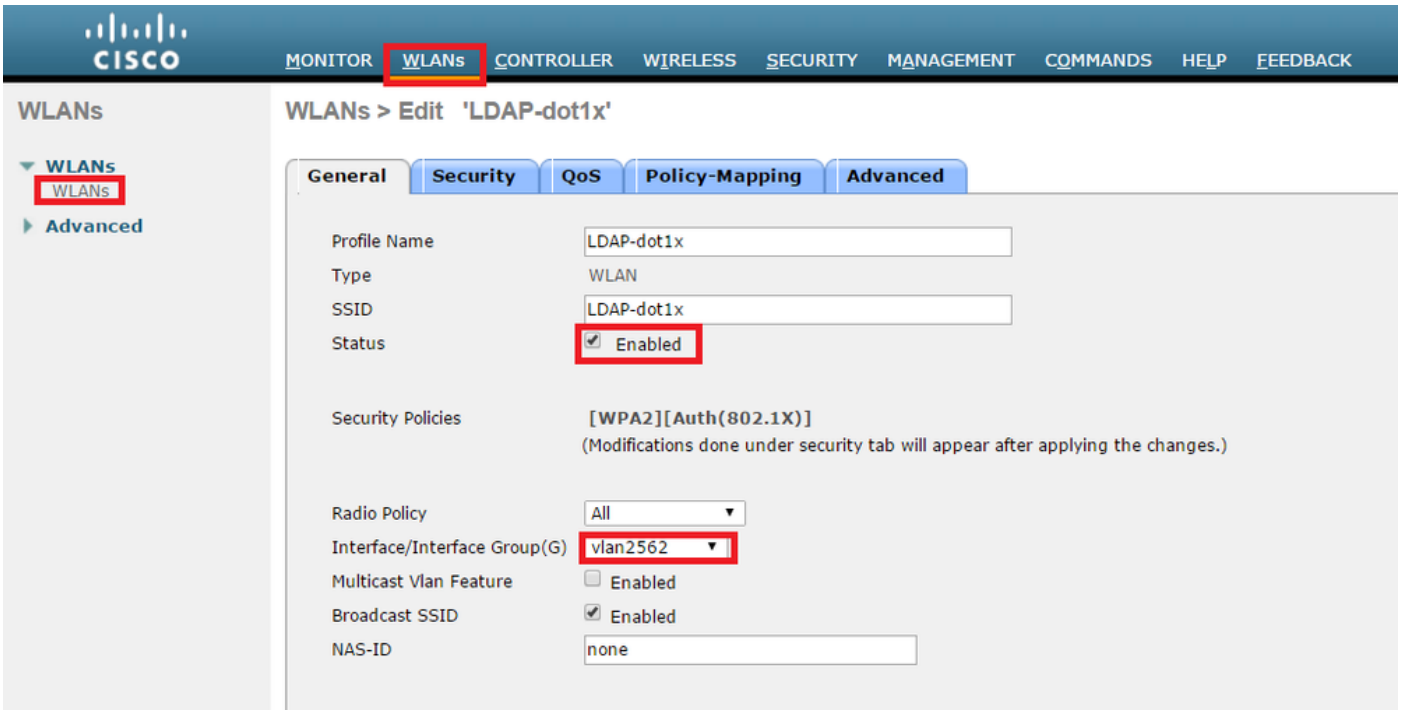
提示：如果绑定用户名不在用户基础DN中，则必须将整个路径写入管理员用户，如图所示。否则，您只需输入**Administrator**。



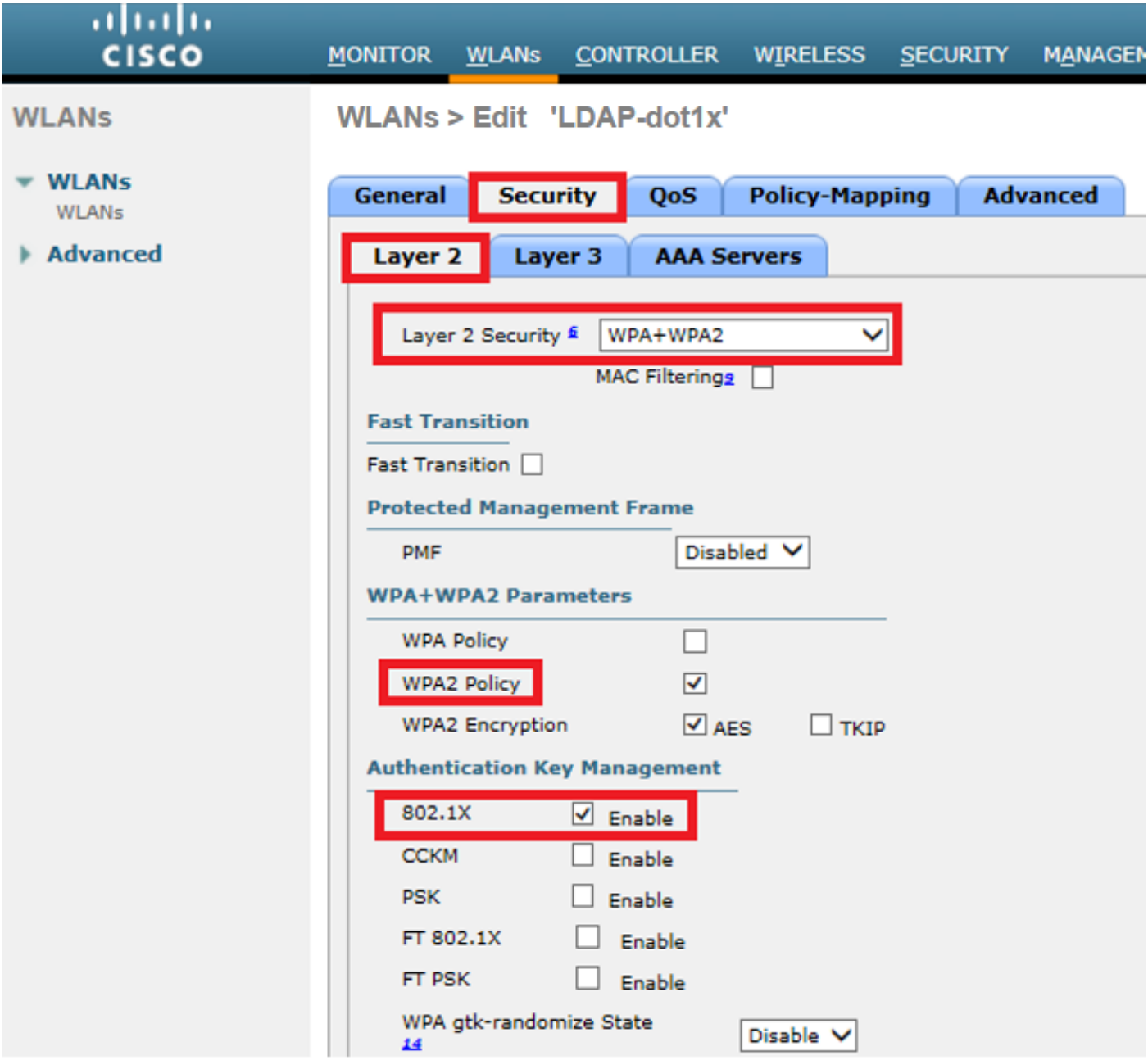
第四步：将Authentication Order设置为Internal Users + LDAP或仅LDAP。

第五步：创建LDAP-dot1x WLAN。

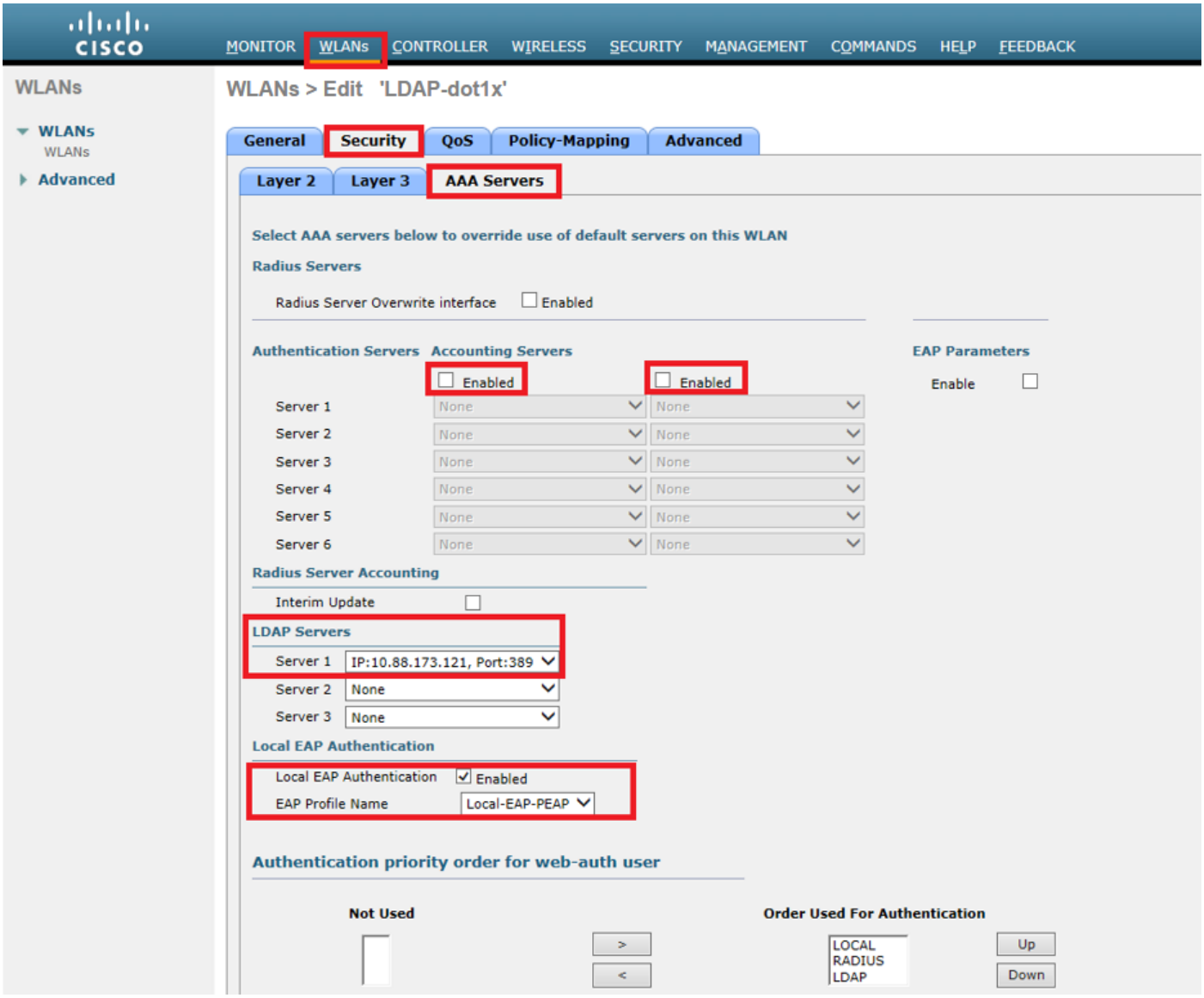




第六步：将L2安全方法设置为WPA2 + 802.1x，并将L3安全设置为none。



步骤 7.启用本地EAP身份验证，并确保已禁用Authentication Servers和Accounting Servers选项并启用LDAP。



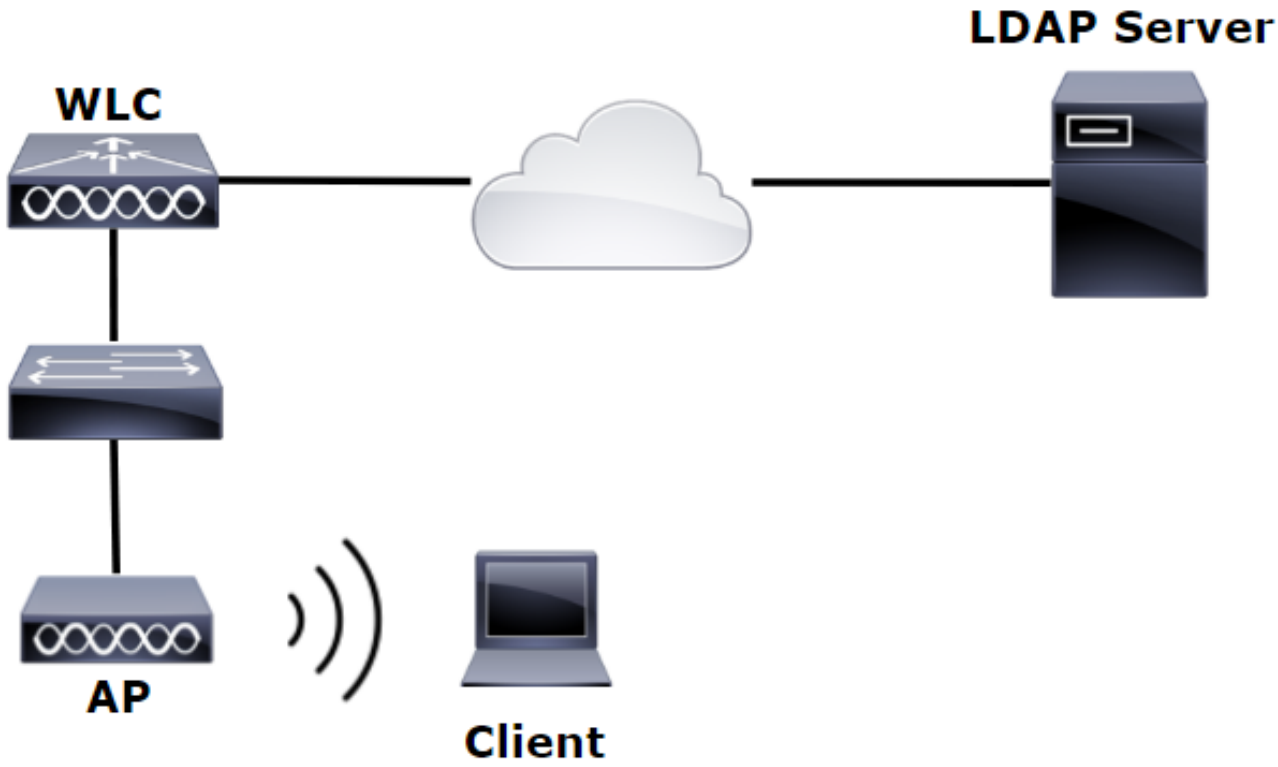
所有其他设置都可以保留为默认值。

注意：
使用LDP工具确认配置参数。
搜索基础不能是组（如SofiaLabGroup）。
如果是Windows计算机，则必须在请求方使用PEAP-GTC或Cisco:PEAP，而不是Microsoft:PEAP。Microsoft:PEAP默认情况下适用于MacOS/iOS/Android。

创建依赖LDAP服务器通过内部WLC Web门户对用户进行身份验证的WLAN

网络图

在此方案中，WLAN LDAP-Web使用LDAP服务器通过内部WLC Web门户对用户进行身份验证。



确保已在上一个示例中执行了步骤1.到步骤4.。WLAN配置从此处设置的方式不同。

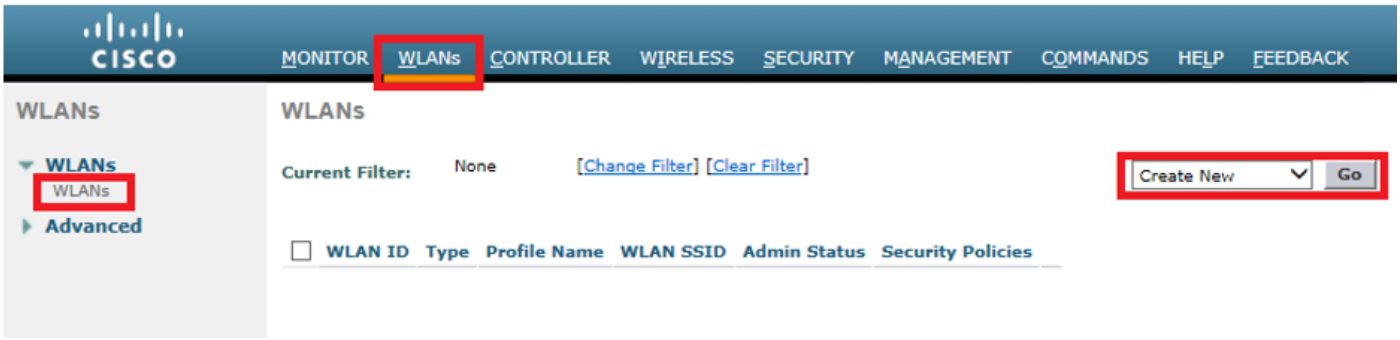
步骤1:在OU SofiaLabOU和组SofiaLabGroup的LDAP服务器成员中创建用户**User1**。

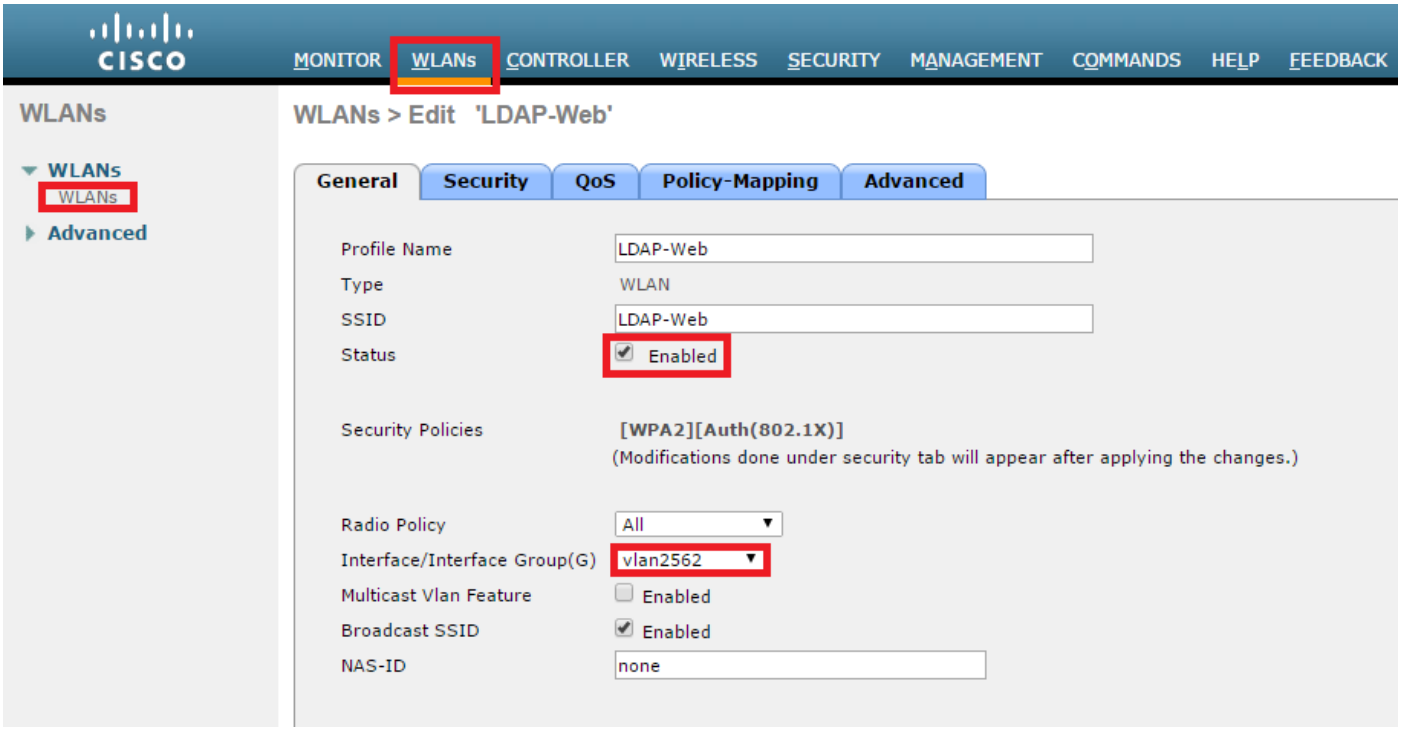
第二步：使用所需的EAP方法在WLC上创建EAP配置文件（使用PEAP）。

第三步：将WLC与LDAP服务器绑定。

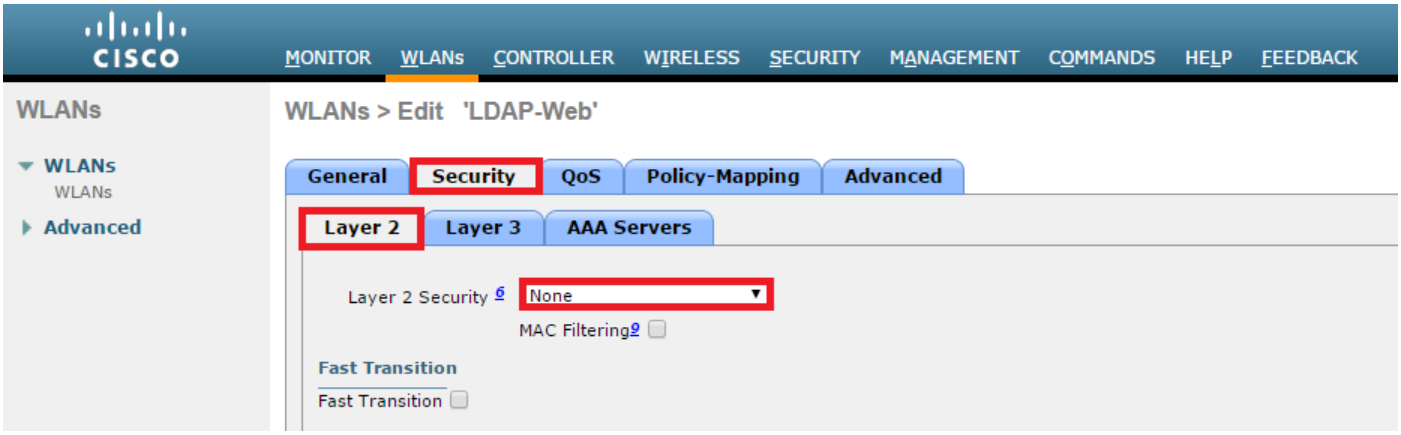
第四步：将Authentication Order设置为Internal Users + LDAP。

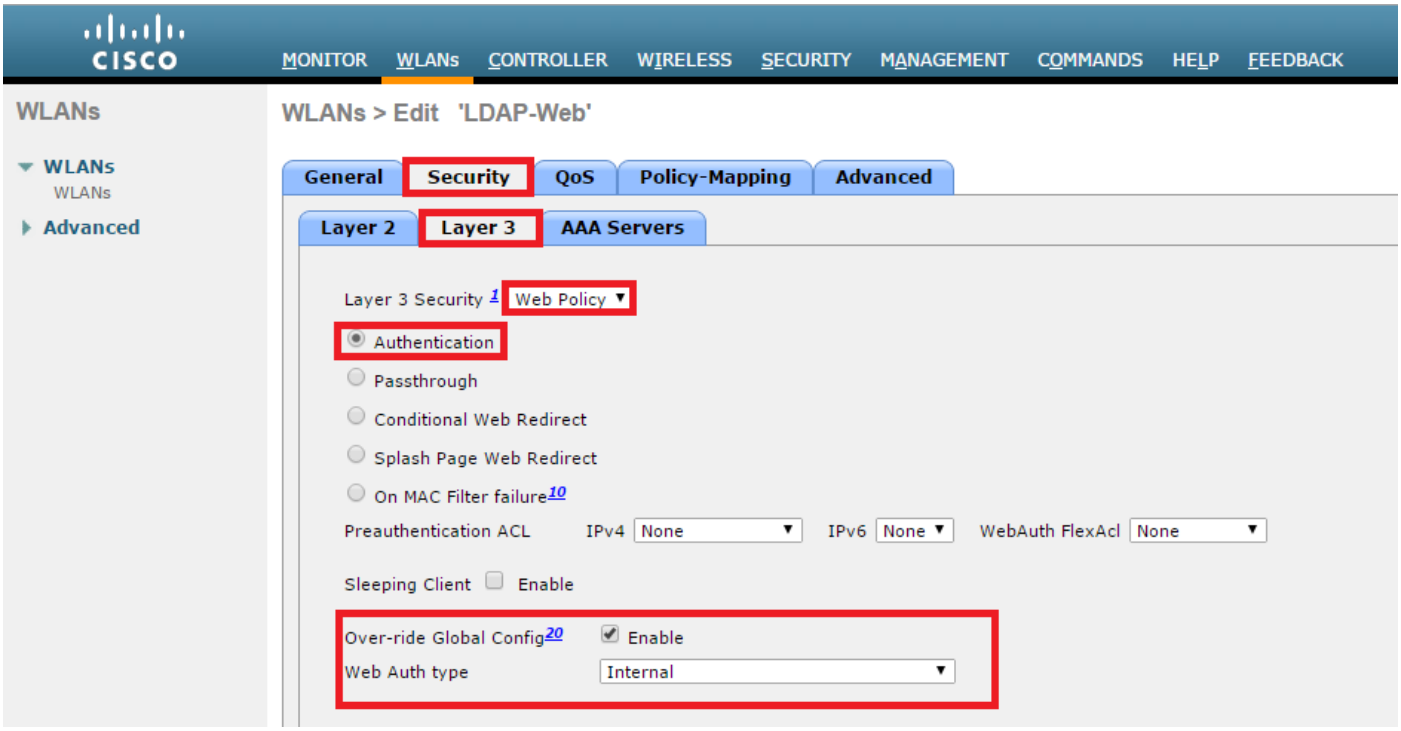
第五步：创建LDAP-Web WLAN，如图所示。



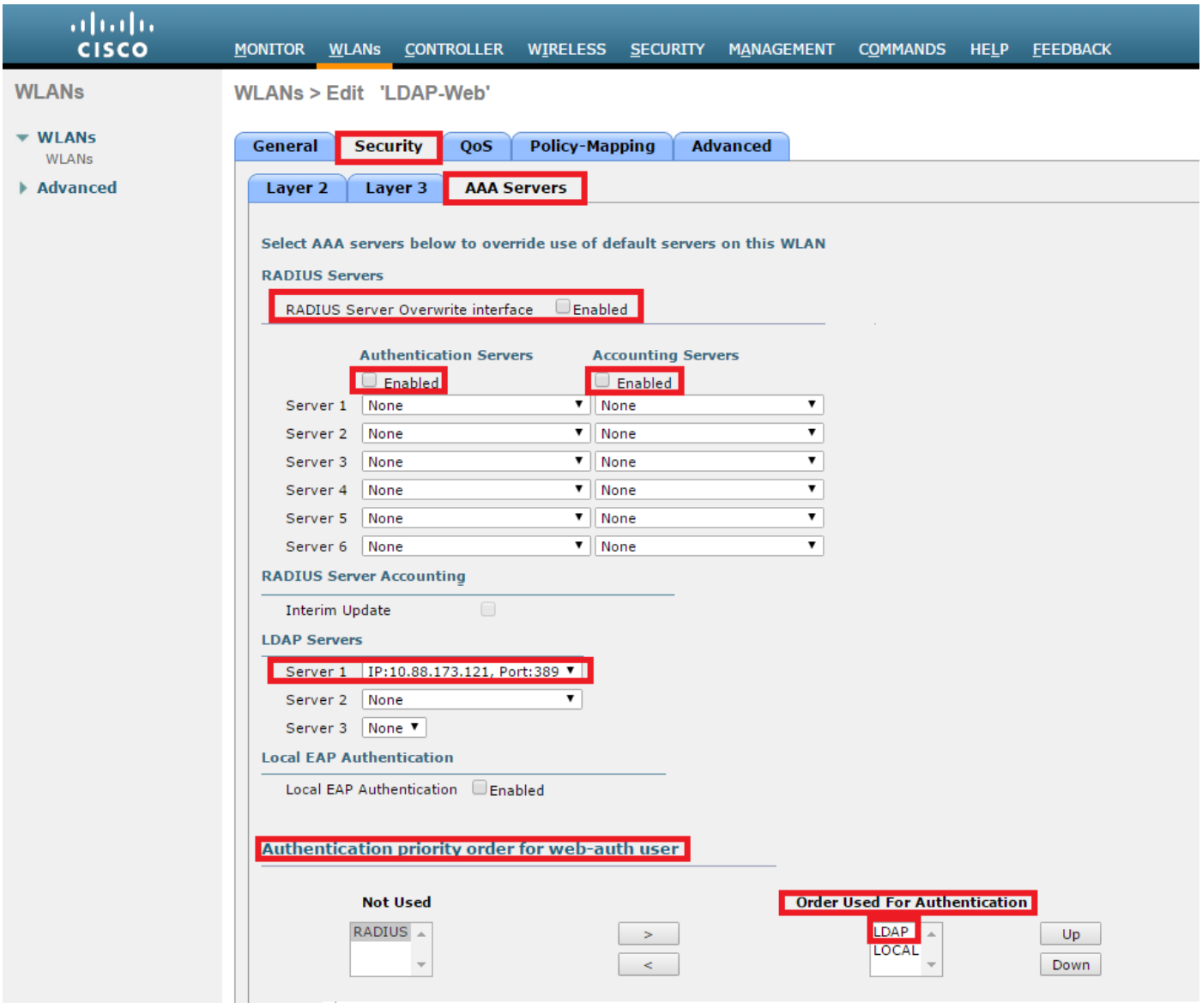


第六步：将L2 Security设置为none，将L3 Security设置为Web Policy - Authentication如图所示。





步骤 7. 将Web-auth的身份验证优先级顺序设置为使用LDAP，并确保已禁用Authentication Servers和Accounting Servers选项。

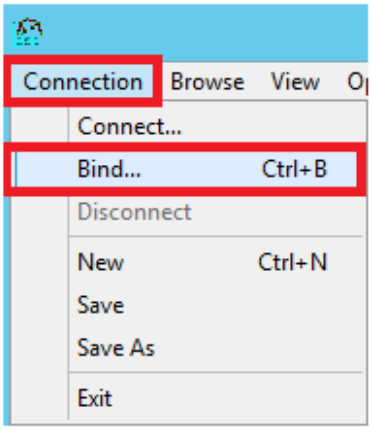


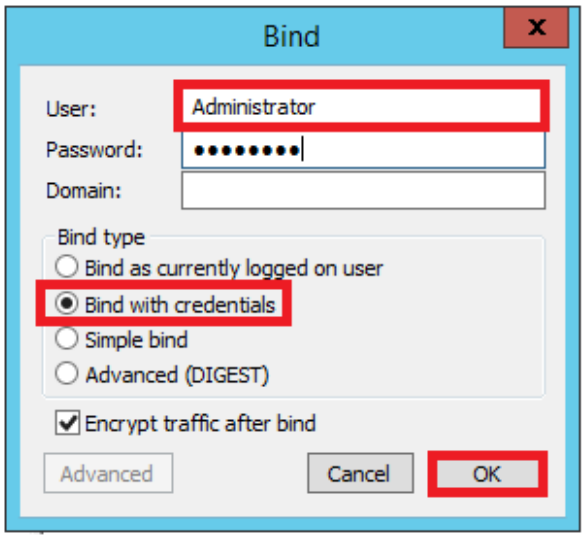
所有其他设置都可以保留为默认值。

使用LDP工具对LDAP进行配置和故障排除

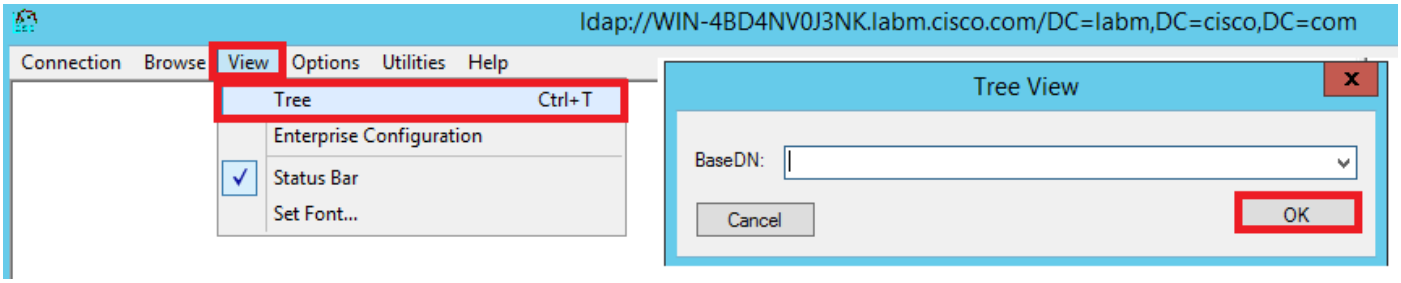
步骤1:在LDAP服务器或具有连接性的主机上打开LDP工具（必须允许到服务器的端口TCP 389）。

第二步： 导航到**Connection > Bind**，使用Admin用户登录，然后选择**Bind with credentials**单选按钮。

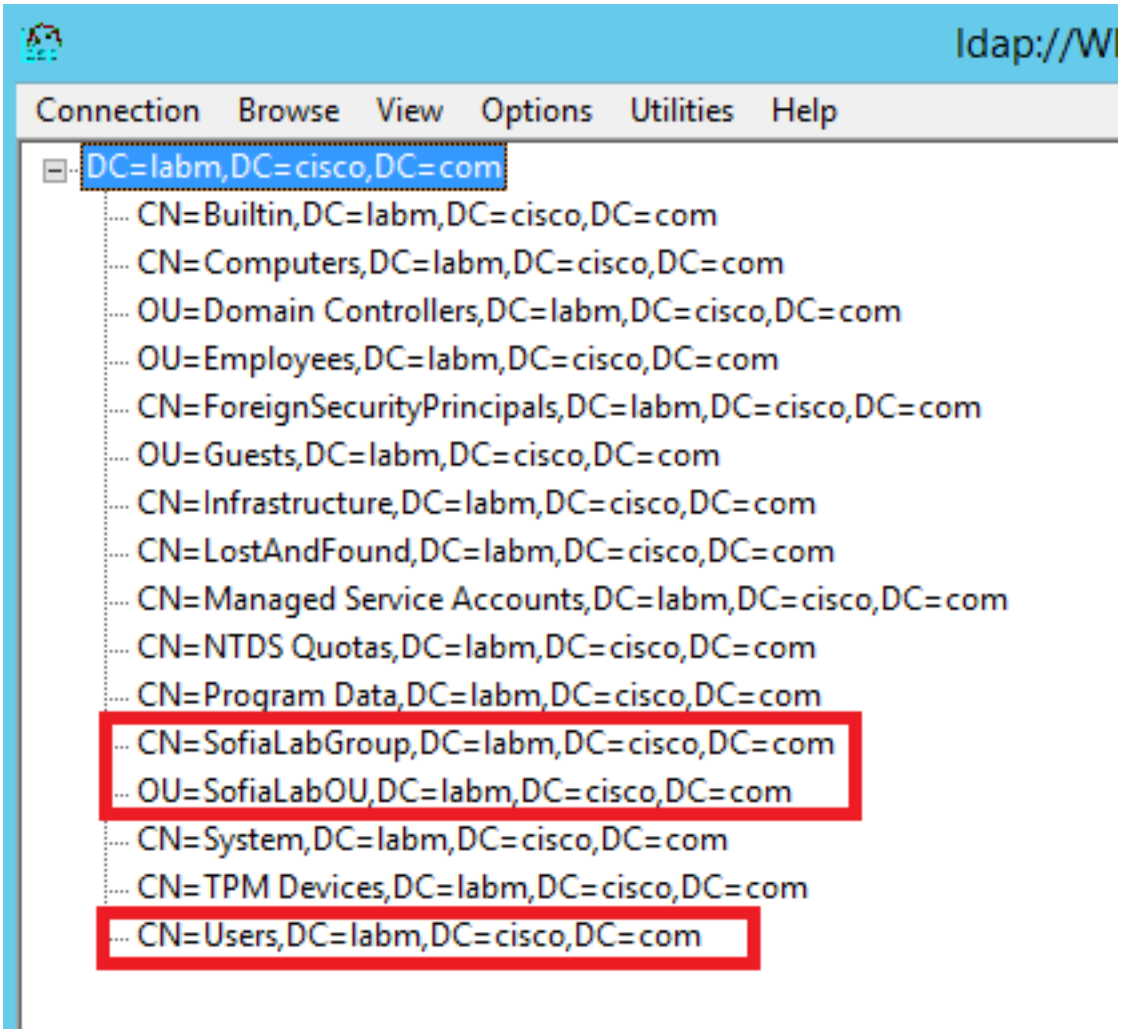




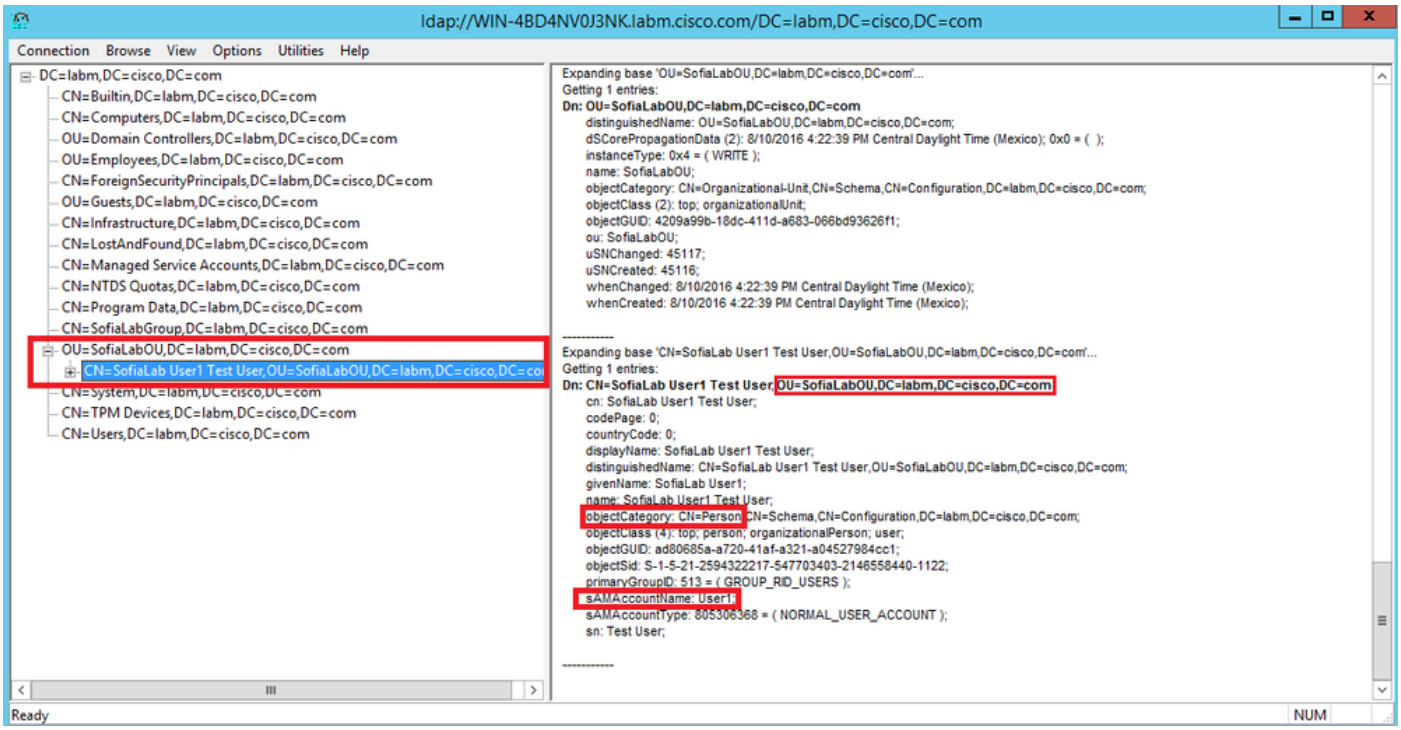
第三步：导航到**View > Tree**，然后在基本DN中选择**OK**。



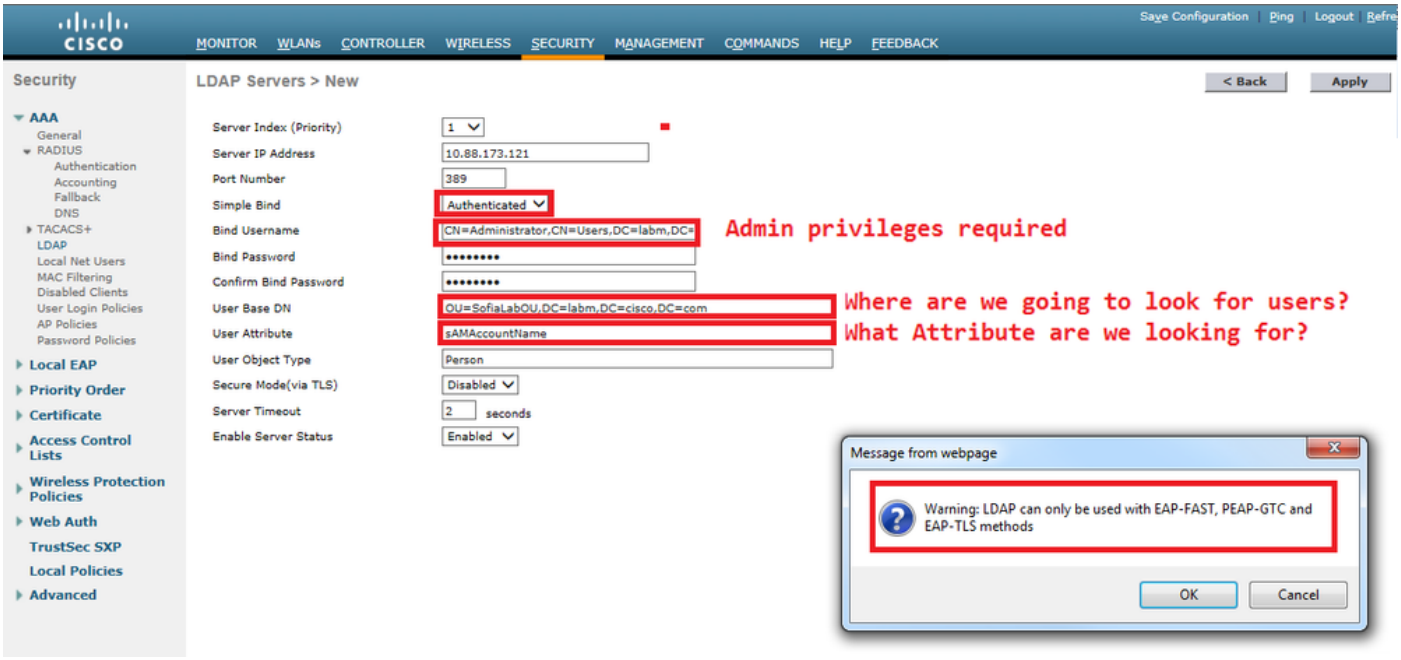
第四步：展开树以查看结构并查找Search Base DN。请考虑它可以是除“组”之外的任何容器类型。它可以是整个域、特定OU或类似CN=Users的CN。



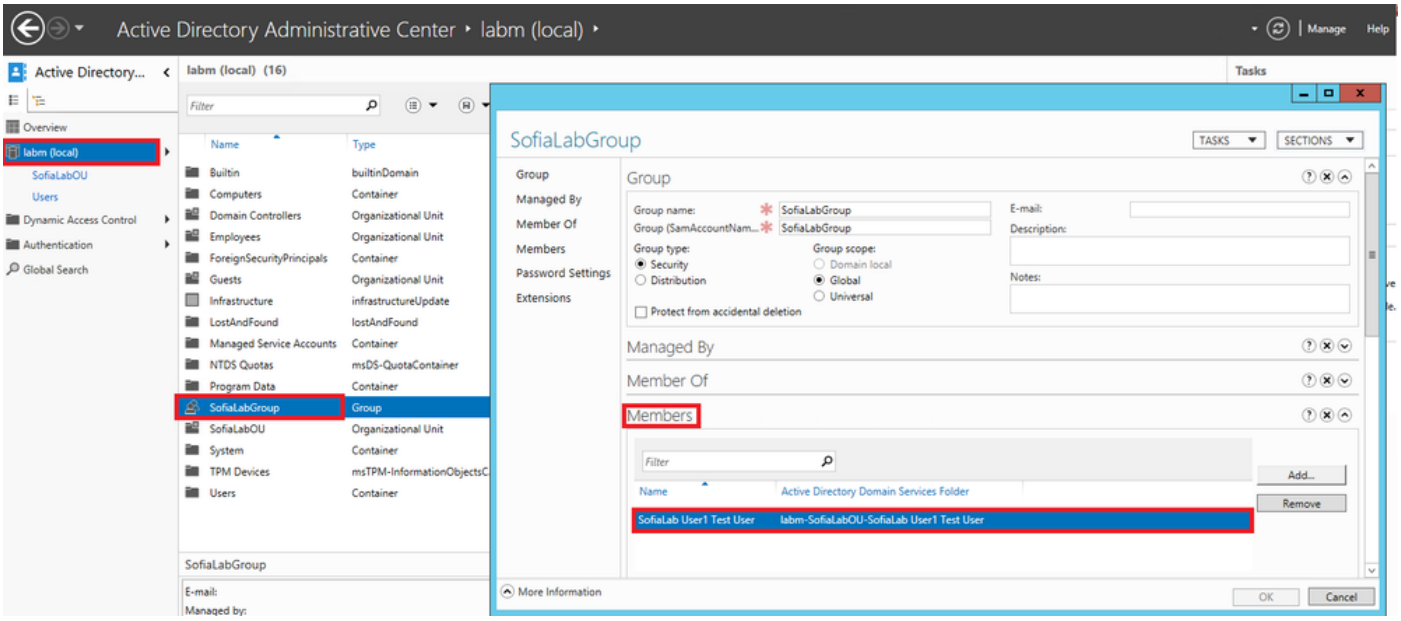
第五步：展开SofiaLabOU以查看其中的用户。这是之前创建的User1。



第六步：配置LDAP所需的一切。



步骤 7.SofiaLabGroup等组不能用作搜索DN。展开组并查找组内的用户，其中之前创建的User1必须是如所示.



User1曾在那里，但LDP找不到它。这意味着WLC无法同样执行此操作，因此不支持将组用作搜索库DN。

验证

使用本部分可确认配置能否正常运行。

```
(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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

```
(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
```

相关信息

- LDAP - WLC 8.2配置指南
- 如何为轻量级目录访问协议(LDAP)身份验证配置无线局域网控制器(WLC)- Vinay Sharma
- 在无线局域网控制器(WLC)上使用LDAP的Web身份验证配置示例 — Yahya Jaber和Ayman Alfares
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。