802.1x 및 웹 인증 WLAN에 대한 LDAP 인증을 사용하여 WLC 구성

목차

소개

이 문서에서는 LDAP 서버를 사용자 데이터베이스로 사용하여 클라이언트를 인증하기 위해 AireOS WLC를 구성하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Microsoft Windows 서버
- 액티브 디렉토리

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco WLC 소프트웨어 8.2.110.0
- Microsoft Windows Server 2012 R2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

기술 배경

- LDAP는 디렉토리 서버에 액세스하는 데 사용되는 프로토콜입니다.
- 디렉토리 서버는 계층 구조의 객체 지향 데이터베이스입니다.
- 개체는 OU(조직 구성 단위), 그룹 또는 CN=Users와 같은 기본 Microsoft 컨테이너와 같은 컨테이너에서 구성됩니다.
- 이 설정에서 가장 어려운 부분은 WLC에서 LDAP 서버 매개변수를 올바르게 구성하는 것입니다.

이러한 개념에 대한 자세한 내용은 LDAP(Lightweight Directory Access Protocol) 인증을 위해 WLC(Wireless Lan Controller)를 구성하는 방법의 소개 섹션을 참조하십시오.

자주 묻는 질문(FAQ)

- LDAP 서버와 바인딩하려면 어떤 사용자 이름을 사용해야 합니까?

LDAP 서버에 바인딩하는 방법에는 Anonymous(익명) 또는 Authenticated(인증됨)의 두 가지가 있습니다(두 방법 간의 차이점을 파악하려면 참조).

이 바인드 사용자 이름에는 다른 사용자 이름/비밀번호를 쿼리할 수 있는 관리자 권한이 있어야 합니다.

- 인증된 경우: 바인드 사용자 이름이 모든 사용자와 동일한 컨테이너 내에 있습니까?

아니요: 전체 경로를 사용합니다. 예를 들면 다음과 같습니다.

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

예: 사용자 이름만 사용하십시오. 예를 들면 다음과 같습니다.

관리자

- 다른 컨테이너에 있는 사용자는 어떻게 됩니까? 관련된 모든 무선 LDAP 사용자가 동일한 컨테이너에 있어야 합니까?

아니요. 필요한 모든 컨테이너를 포함하는 기본 DN을 지정할 수 있습니다.

- WLC에서 찾아야 하는 특성은 무엇입니까?

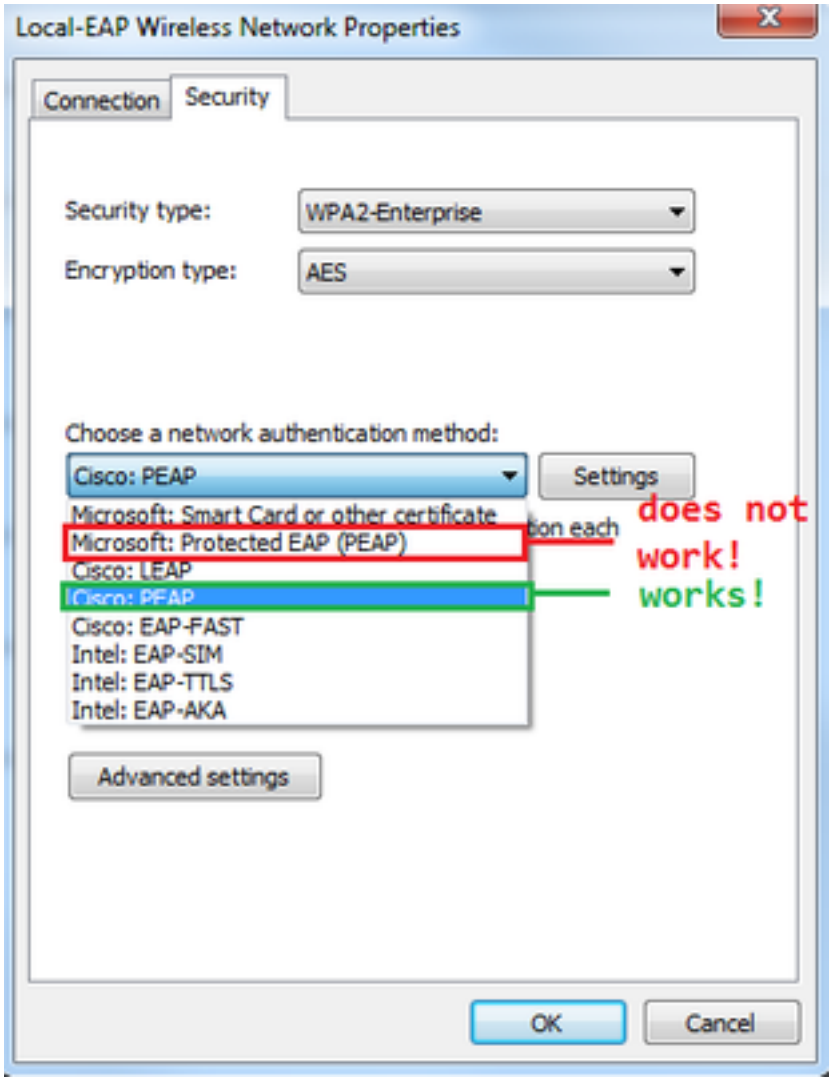
WLC는 지정된 사용자 특성 및 객체 유형과 일치합니다.

> **참고**: **sAMAccountName**은 대/소문자를 구분하지만 사람은 대/소문자를 구분하지 않습니다. 따라서 **sAMAccountName=RICARDO**와 **sAMAccountName=ricardo**는 동일하며 작동하는 반면 **samaccountname=RICARDO** 및 **samaccountname=ricardo**는 그렇지 않습니다.

- 어떤 EAP(Extensible Authentication Protocol) 방법을 사용할 수 있습니까?

EAP-FAST, PEAP-GTC 및 EAP-TLS 전용. Android, iOS 및 MacOS 기본 신청자는 PEAP(Protected Extensible Authentication Protocol)에서 작동합니다.

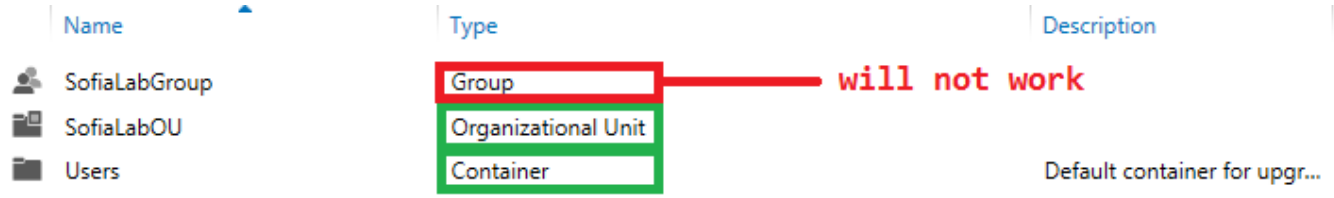
Windows의 경우 이미지에 표시된 대로 지원되는 무선 어댑터에서 Anyconnect NAM(Network Access Manager) 또는 기본 Windows 신청자(Cisco:PEAP 포함)를 사용해야 합니다.



참고: Windows용 Cisco EAP 플러그인에는 Cisco 버그 ID CSCva09670의 영향을 받는 OpenSSL 0.9.8k(Open Secure Socket Layer) 버전이 포함되어 있습니다. Cisco는 Windows용 EAP 플러그인의 릴리스를 더 이상 발급하지 않을 계획이며, 고객이 대신 AnyConnect Secure Mobility Client를 사용할 것을 권장합니다.

- WLC에서 사용자를 찾을 수 없는 이유는 무엇입니까?

그룹 내의 사용자는 인증할 수 없습니다. 이미지에 표시된 대로 기본 컨테이너(CN) 또는 OU(Organizational Unit) 내에 있어야 합니다.



구성

802.1x 인증 또는 웹 인증을 사용하여 LDAP 서버를 사용할 수 있는 다양한 시나리오가 있습니다.

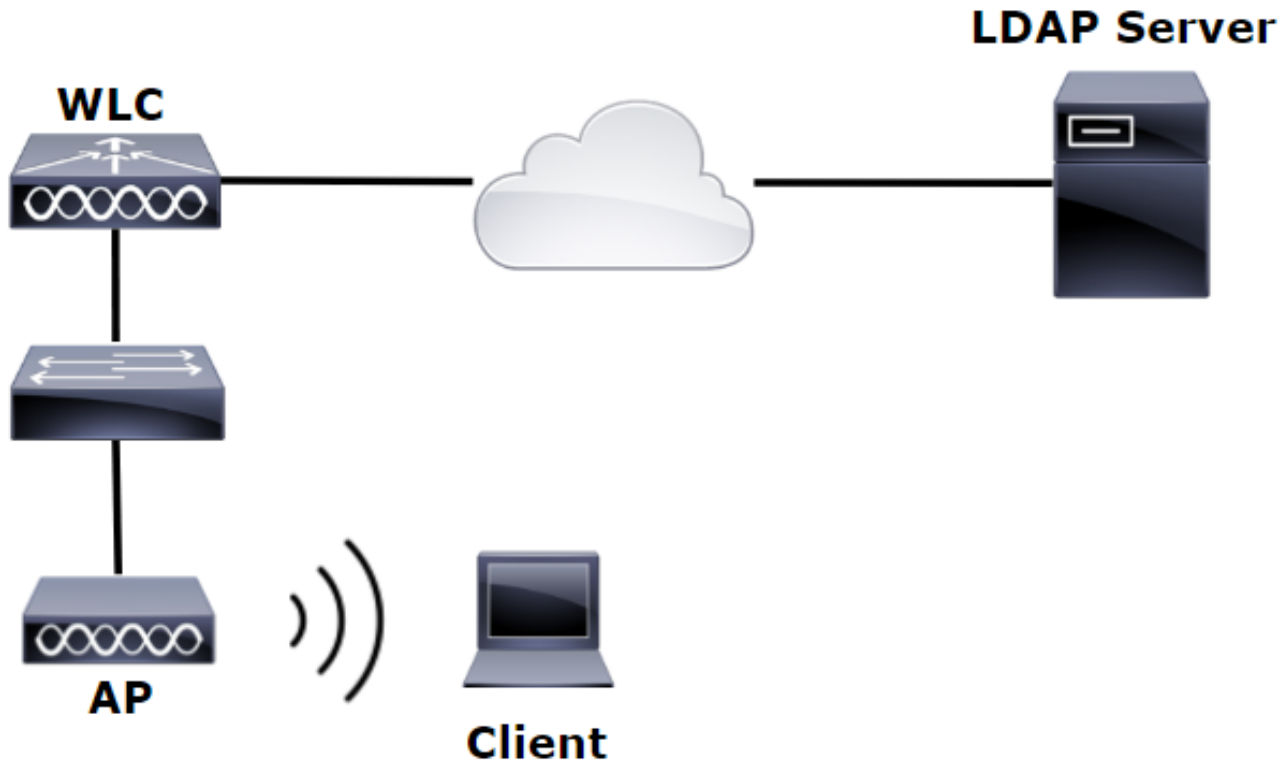
이 절차에서는 OU=SofiaLabOU 내부의 사용자만 인증해야 합니다.

LDP(Label Distribution Protocol) 툴, LDAP 구성 및 문제 해결 방법을 알아보려면 WLC LDAP 컨피그레이션 가이드를 참조하십시오.

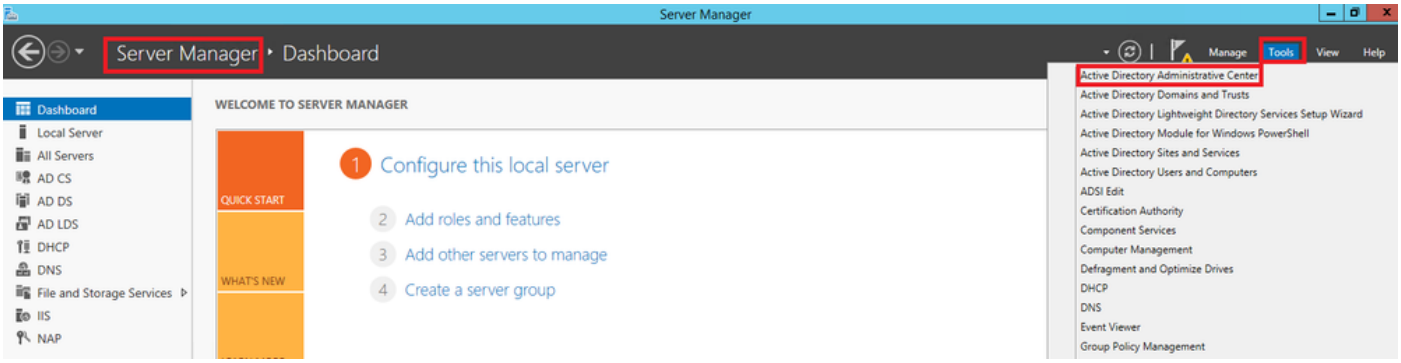
802.1x를 통해 사용자를 인증하기 위해 LDAP 서버를 사용하는 WLAN 생성

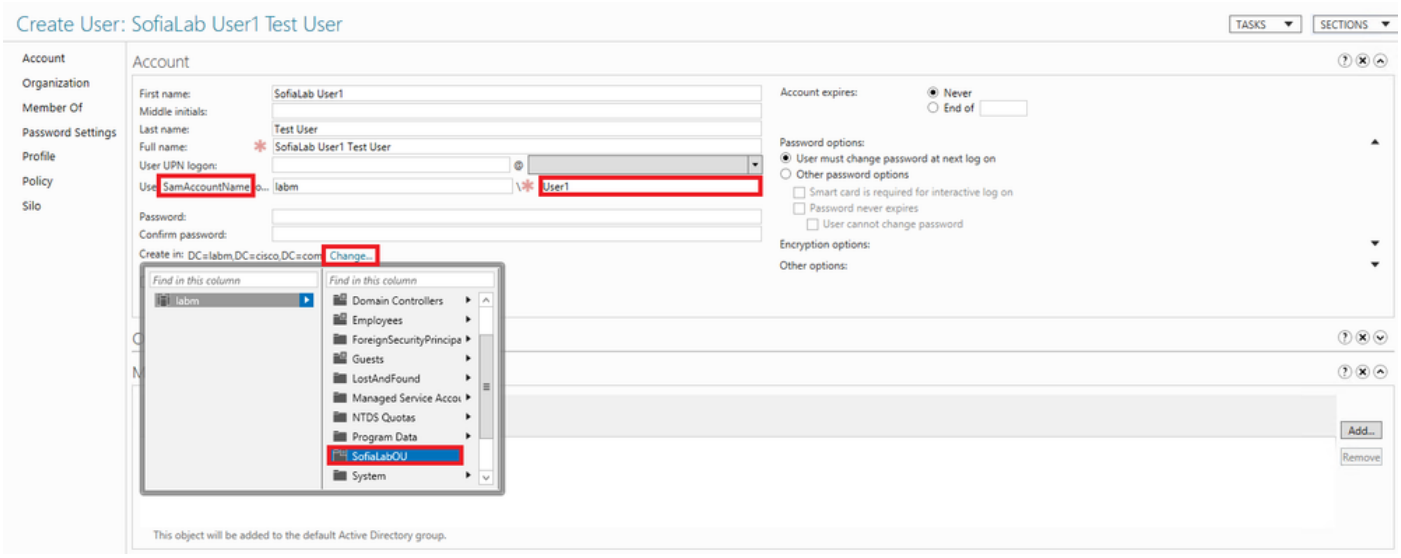
네트워크 다이어그램

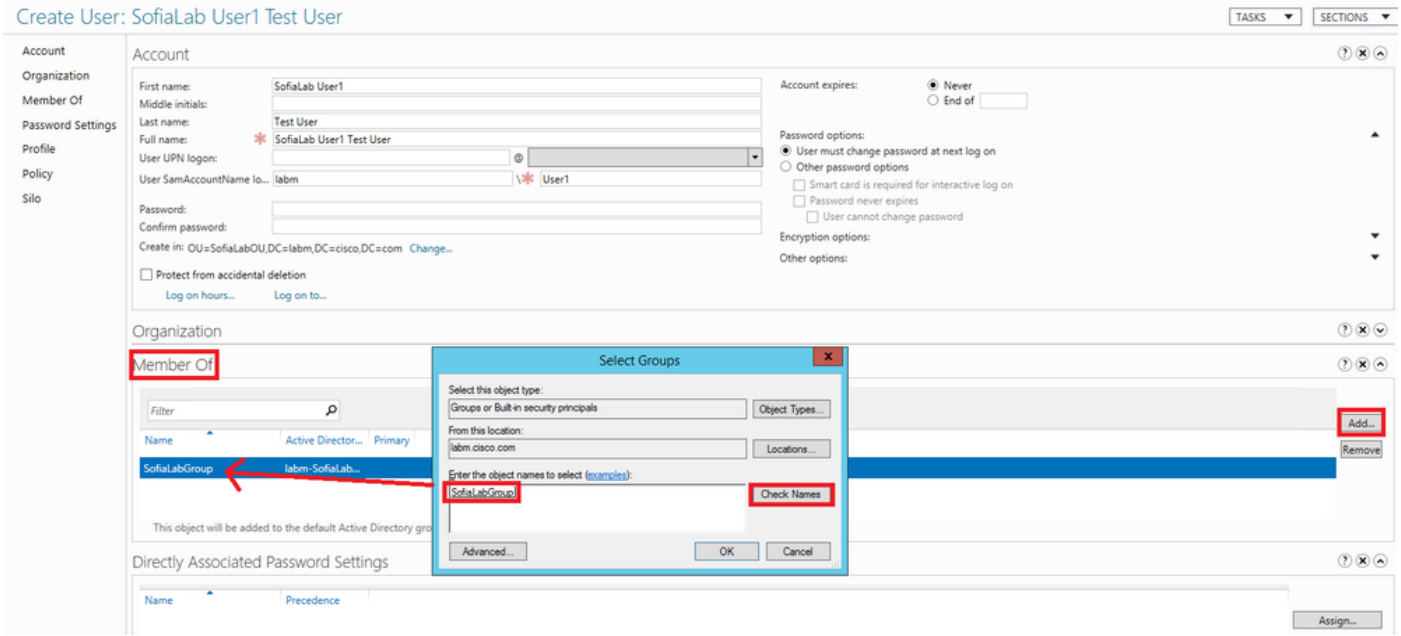
이 시나리오에서 WLAN LDAP-dot1x는 LDAP 서버를 사용하여 802.1x를 사용하여 사용자를 인증합니다.



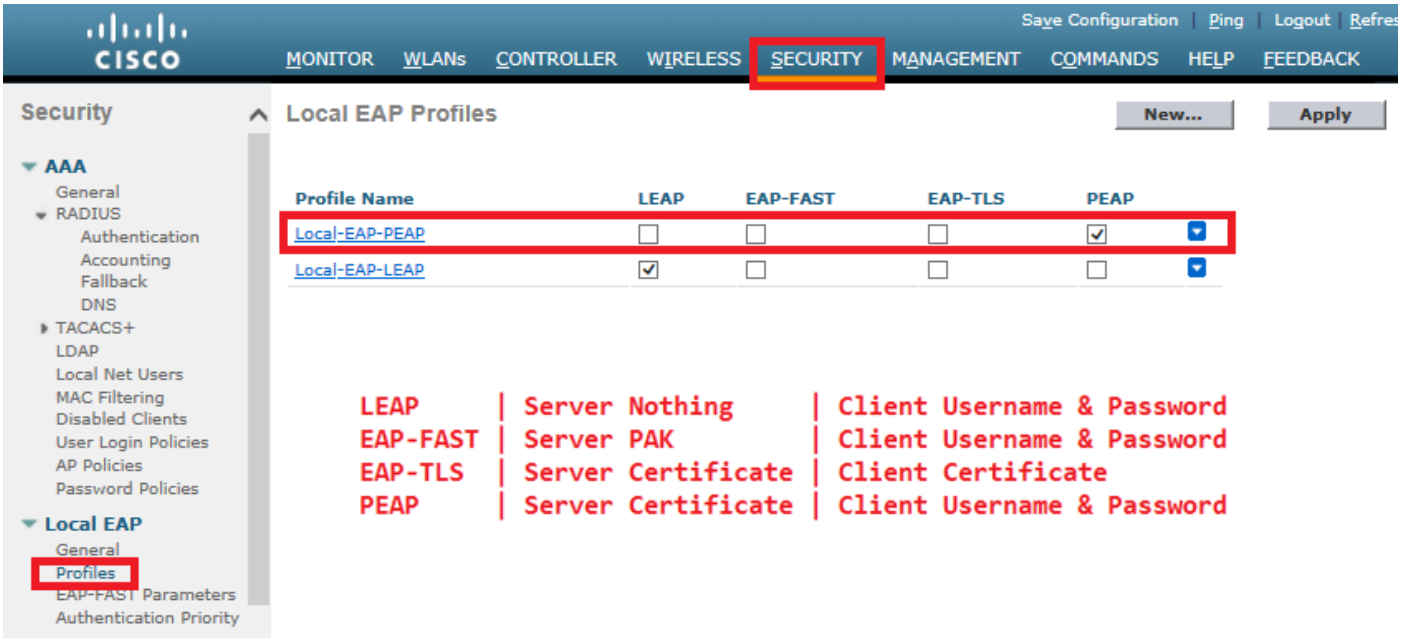
1단계. SofiaLabOU 및 **SofiaLabGroup**의 LDAP 서버 멤버에서 사용자 User1을 생성합니다.





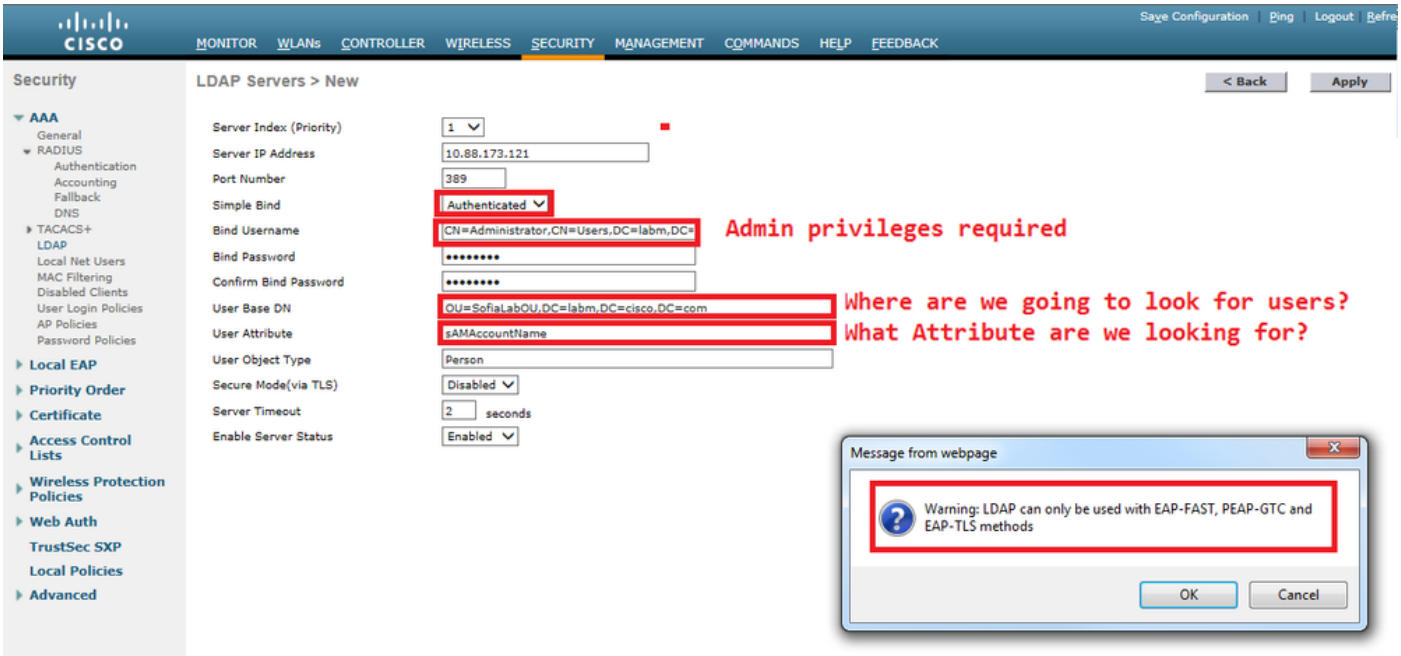


2단계. 원하는 EAP 방법(PEAP 사용)으로 WLC에서 EAP 프로파일을 생성합니다.



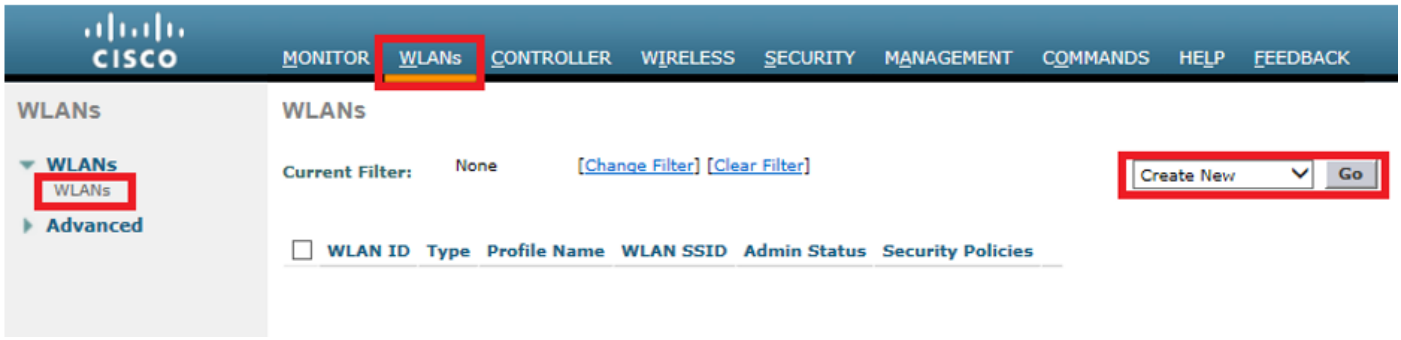
3단계. WLC를 LDAP 서버와 바인딩합니다.

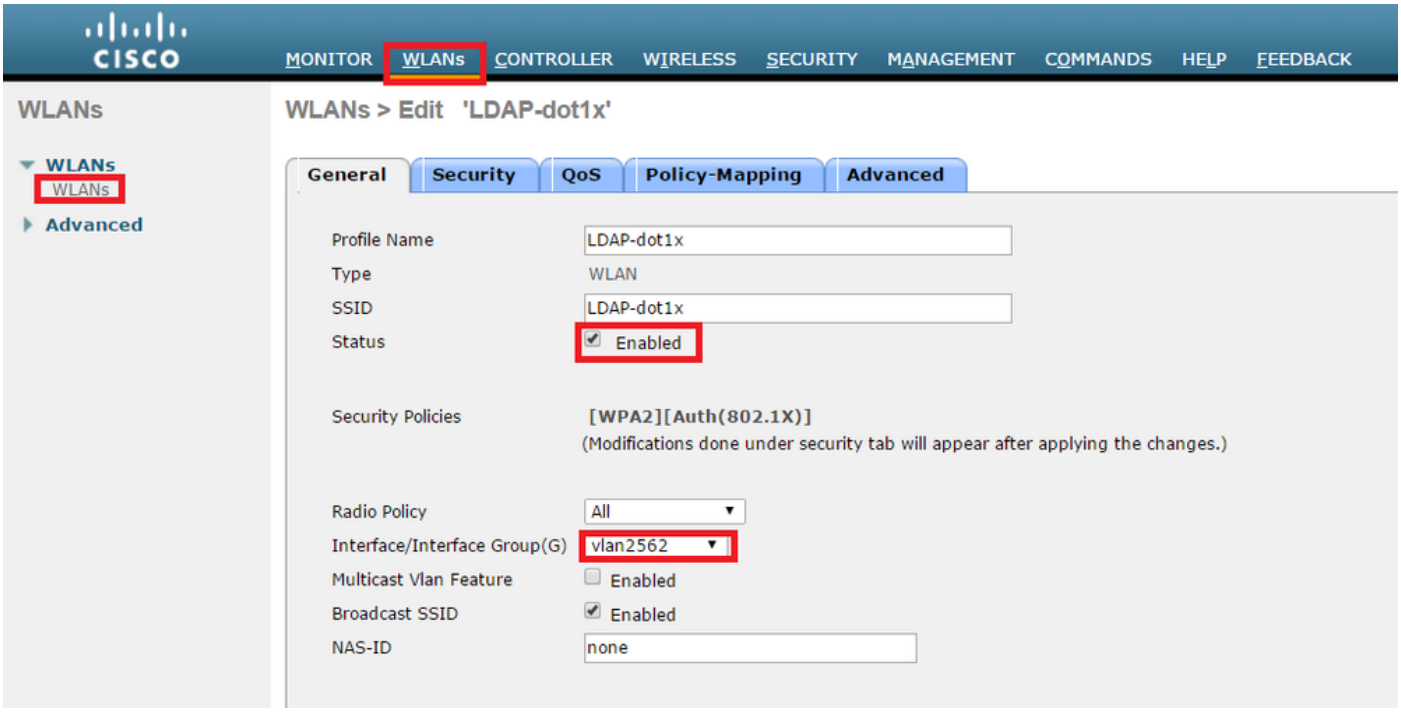
> **팁**: bind Username(바인드 사용자 이름)이 User Base DN에 없는 경우 이미지에 표시된 것처럼 **Admin 사용자**에게 전체 경로를 작성해야 합니다. 그렇지 않으면 Administrator를 입력하면 **됩니다**.



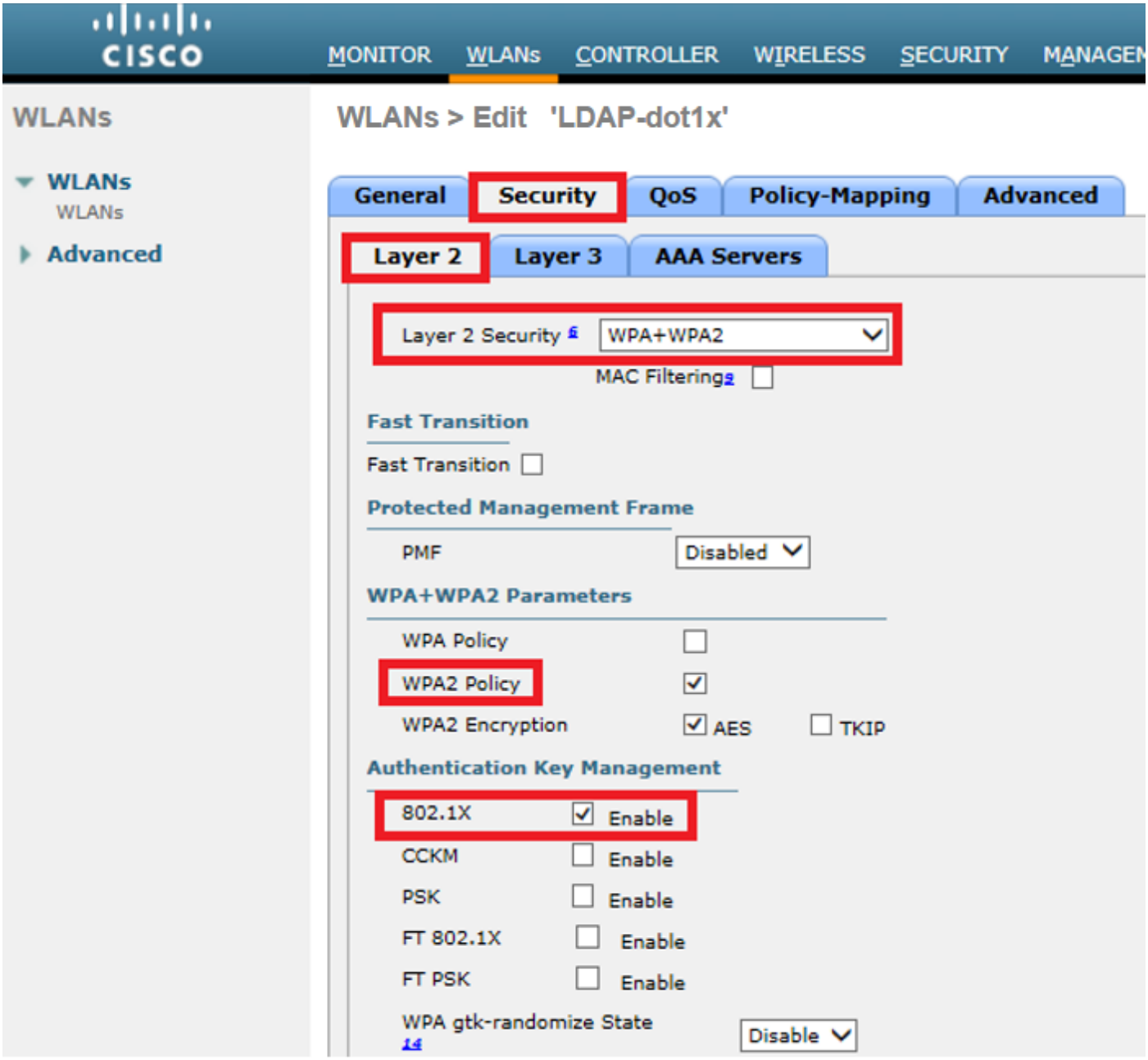
4단계. Authentication Order(인증 순서)를 Internal Users(내부 사용자) + LDAP 또는 LDAP only(LDAP 전용)로 설정합니다.

5단계. LDAP-dot1x WLAN을 생성합니다.

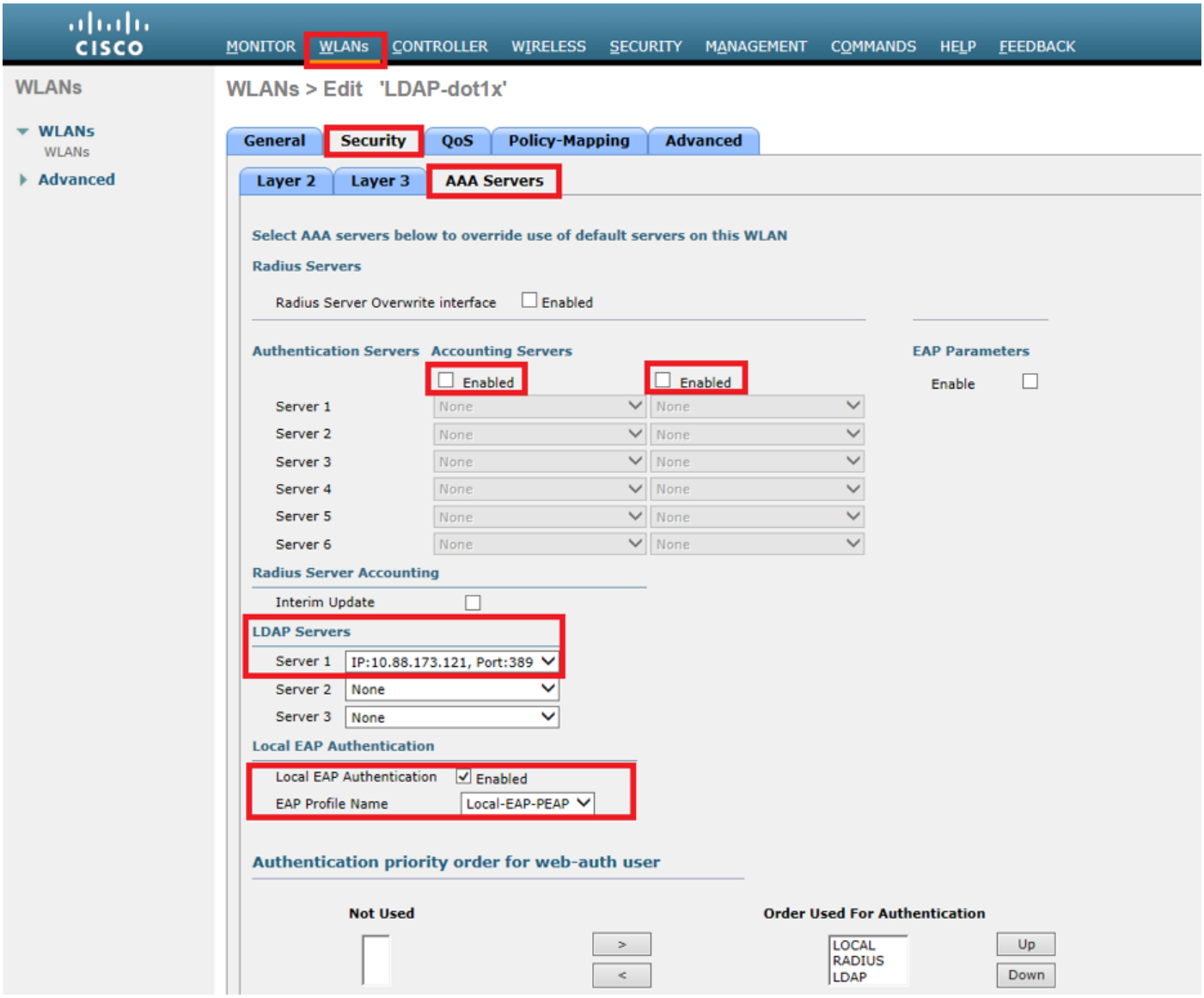




6단계. L2 보안 방법을 WPA2 + 802.1x로 설정하고 L3 보안을 none으로 설정합니다.



7단계. 로컬 EAP 인증을 활성화하고 Authentication Servers(인증 서버) 및 Accounting Servers(어카운팅 서버) 옵션이 비활성화되고 LDAP가 활성화되었는지 확인합니다.



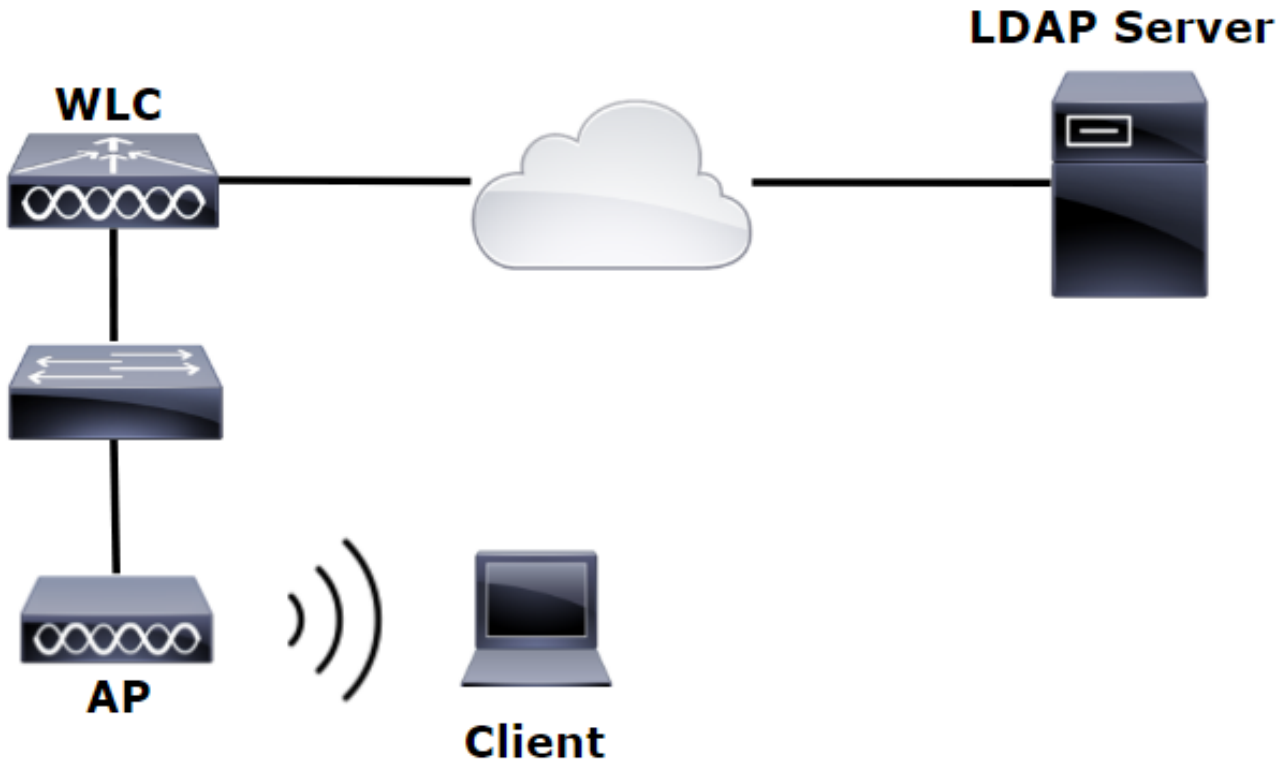
다른 모든 설정은 기본값으로 둘 수 있습니다.

참고:
LDP 툴을 사용하여 컨피그레이션 매개변수를 확인합니다.
검색 기준은 그룹(예: SofiaLabGroup)이 될 수 없습니다.
PEAP-GTC 또는 Cisco:PEAP는 서 플리 컨 트에서 Microsoft:PEAP 대신 사용 해야 합니다.
Microsoft:PEAP는 기본적으로 MacOS/iOS/Android에서 작동합니다.

내부 WLC 웹 포털을 통해 사용자를 인증하기 위해 LDAP 서버를 사용하는 WLAN 생성

네트워크 다이어그램

이 시나리오에서 WLAN LDAP-Web은 LDAP 서버를 사용하여 내부 WLC 웹 포털에서 사용자를 인증합니다.



이전 예에서 1~4단계를 수행했는지 확인합니다. 여기서 WLAN 컨피그레이션은 다르게 설정됩니다.

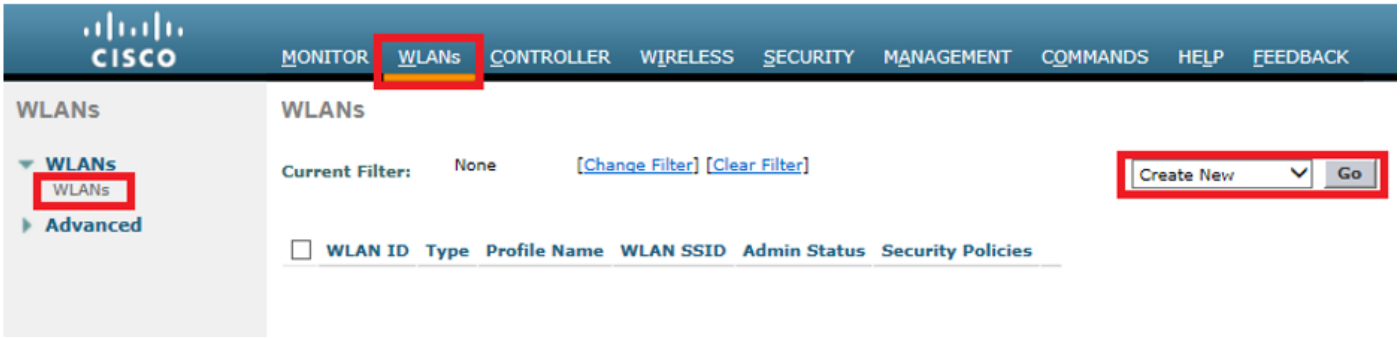
1단계. OU SofiaLabOU 및 그룹 SofiaLabGroup의 LDAP 서버 멤버에서 사용자 **User1**을 생성합니다.

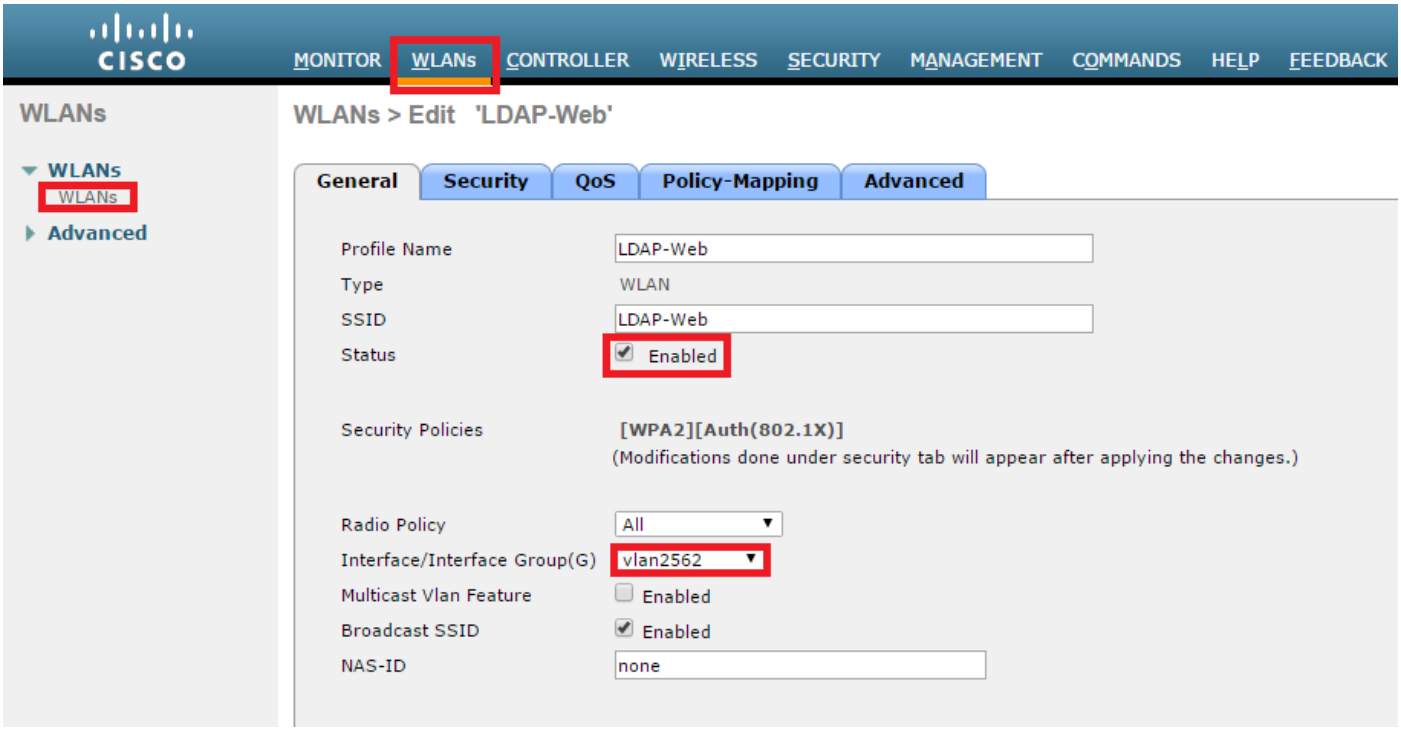
2단계. 원하는 EAP 방법(PEAP 사용)으로 WLC에서 EAP 프로파일을 생성합니다.

3단계. WLC를 LDAP 서버에 바인딩합니다.

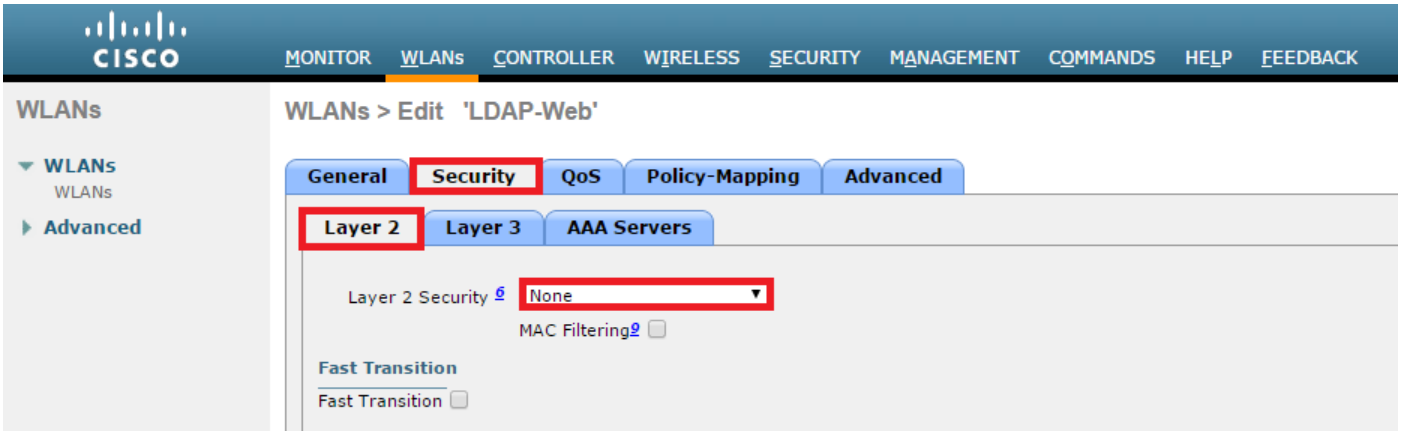
4단계. Authentication Order(인증 순서)를 Internal Users + LDAP로 설정합니다.

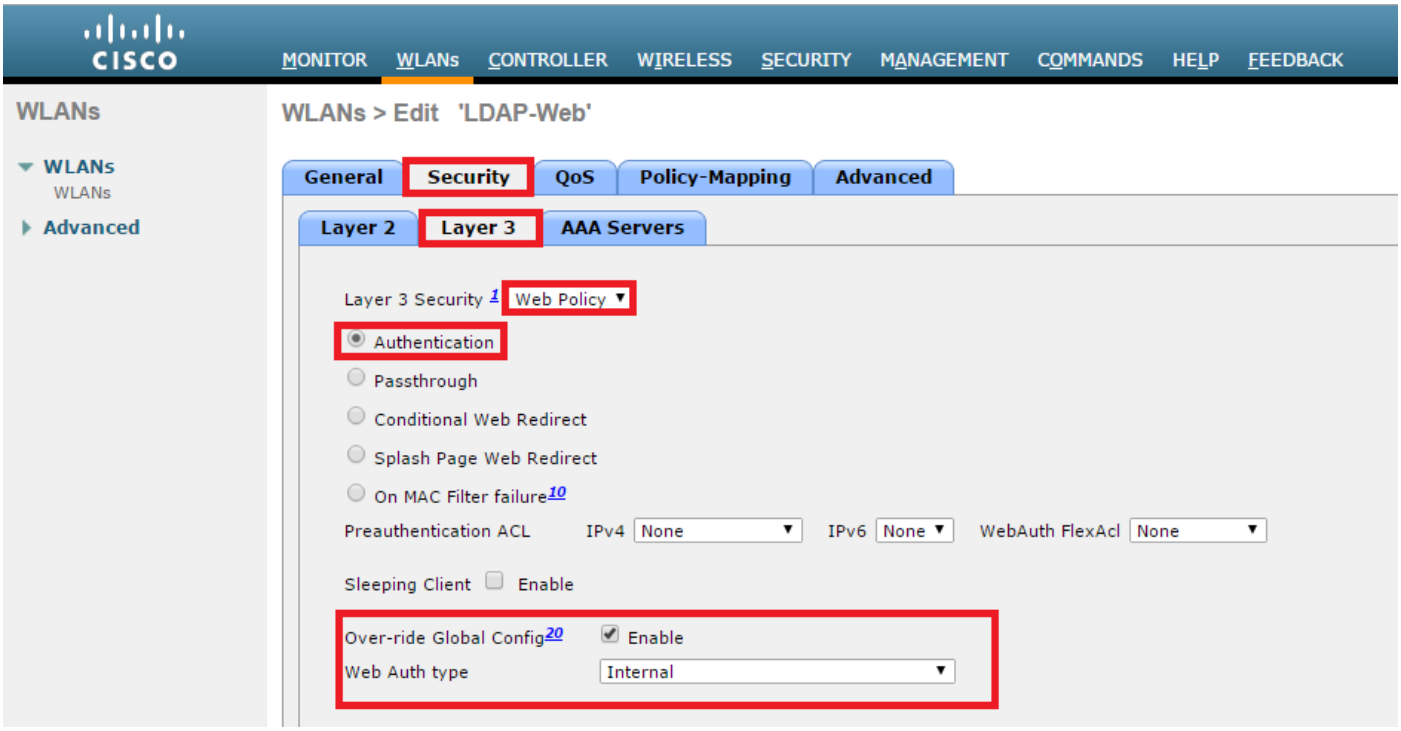
5단계. 이미지에 표시된 대로 LDAP-Web WLAN을 생성합니다.



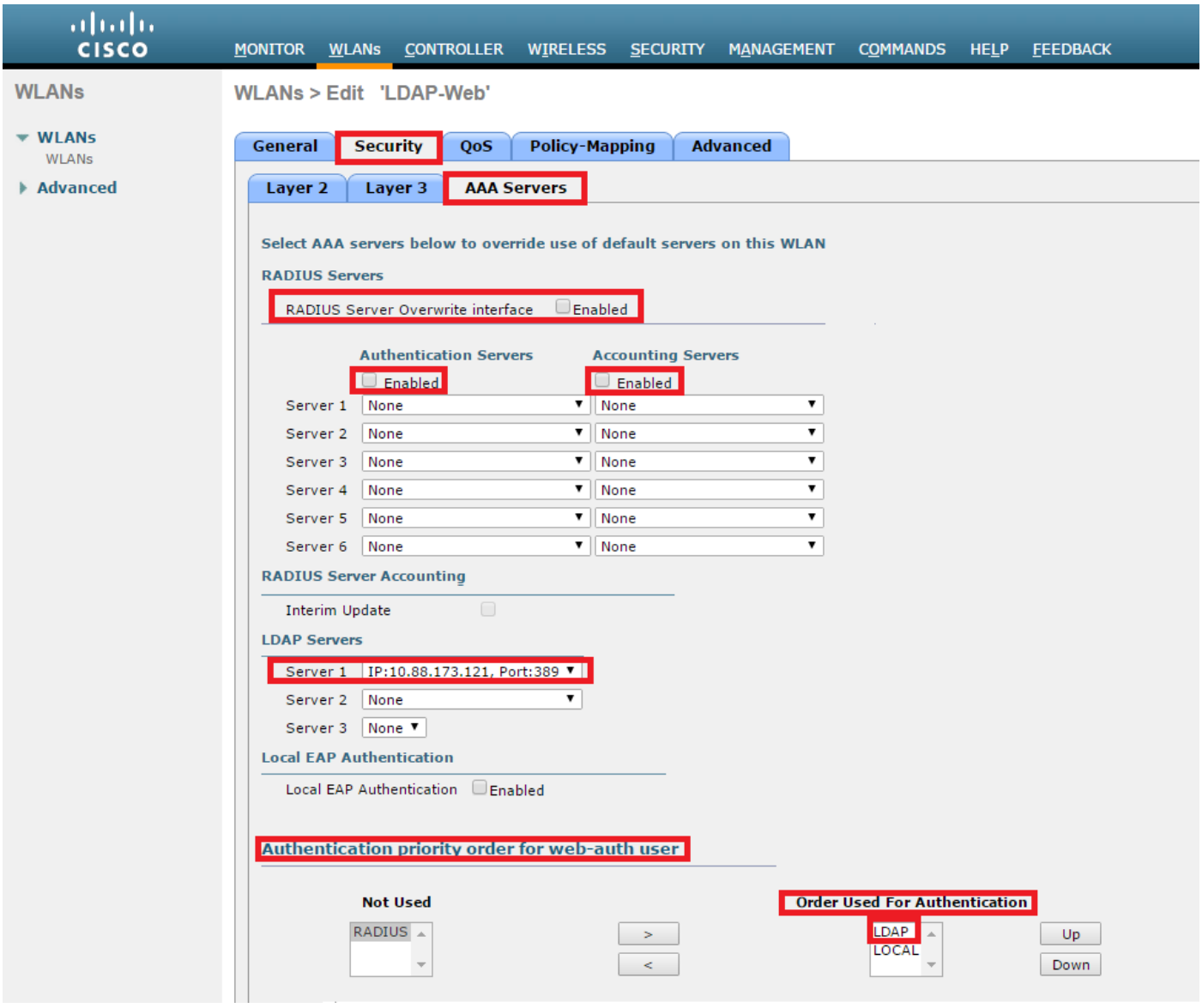


6단계. L2 Security를 none으로 설정하고 L3 Security를 Web Policy - Authentication으로 설정그림에 나와 있는 것처럼.





7단계. 웹 인증에서 LDAP를 사용하도록 인증 우선 순위를 설정하고 인증 서버 및 계정 관리 서버 옵션이 비활성화되었는지 확인합니다.

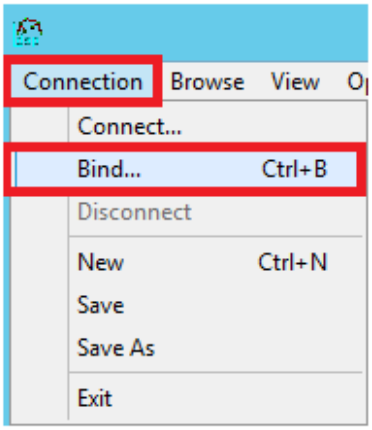


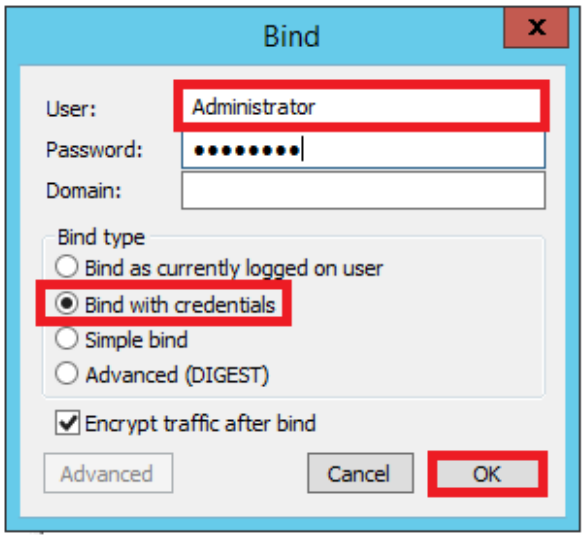
다른 모든 설정은 기본값으로 둘 수 있습니다.

LDP 툴을 사용하여 LDAP 구성 및 문제 해결

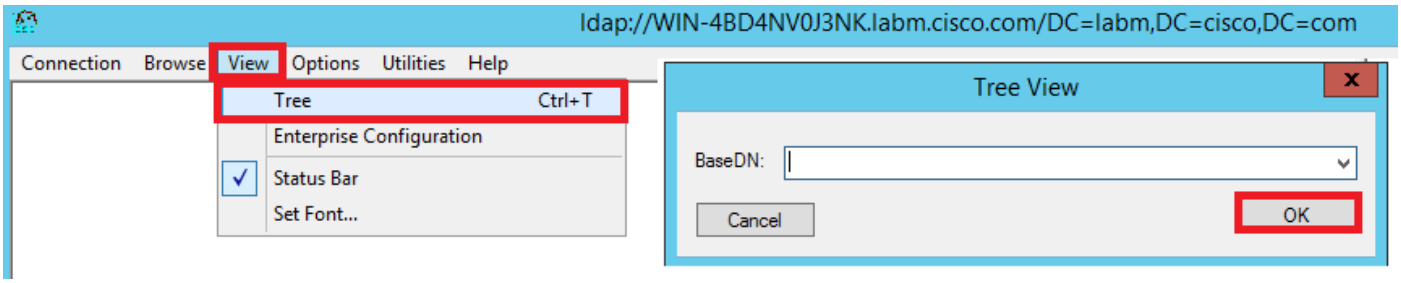
1단계. LDAP 서버 또는 연결된 호스트에서 LDP 툴을 엽니다(서버에 포트 TCP 389를 허용해야 함).

2단계. **Connection(연결) > Bind(바인드)로** 이동하여 Admin 사용자로 로그인하고 Bind with credentials(자격 증명**으로 바인딩)** 라디오 **버튼**을 선택합니다.

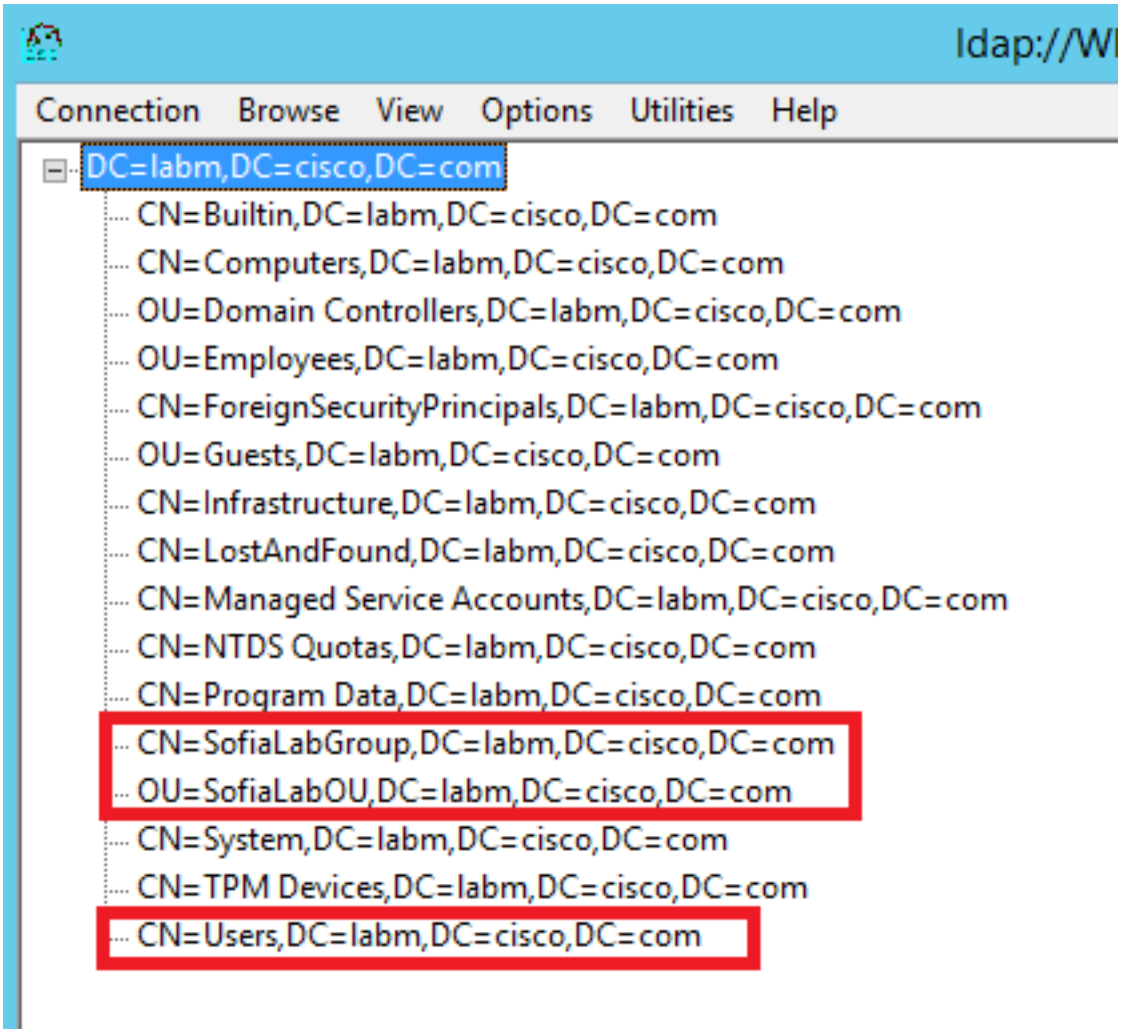




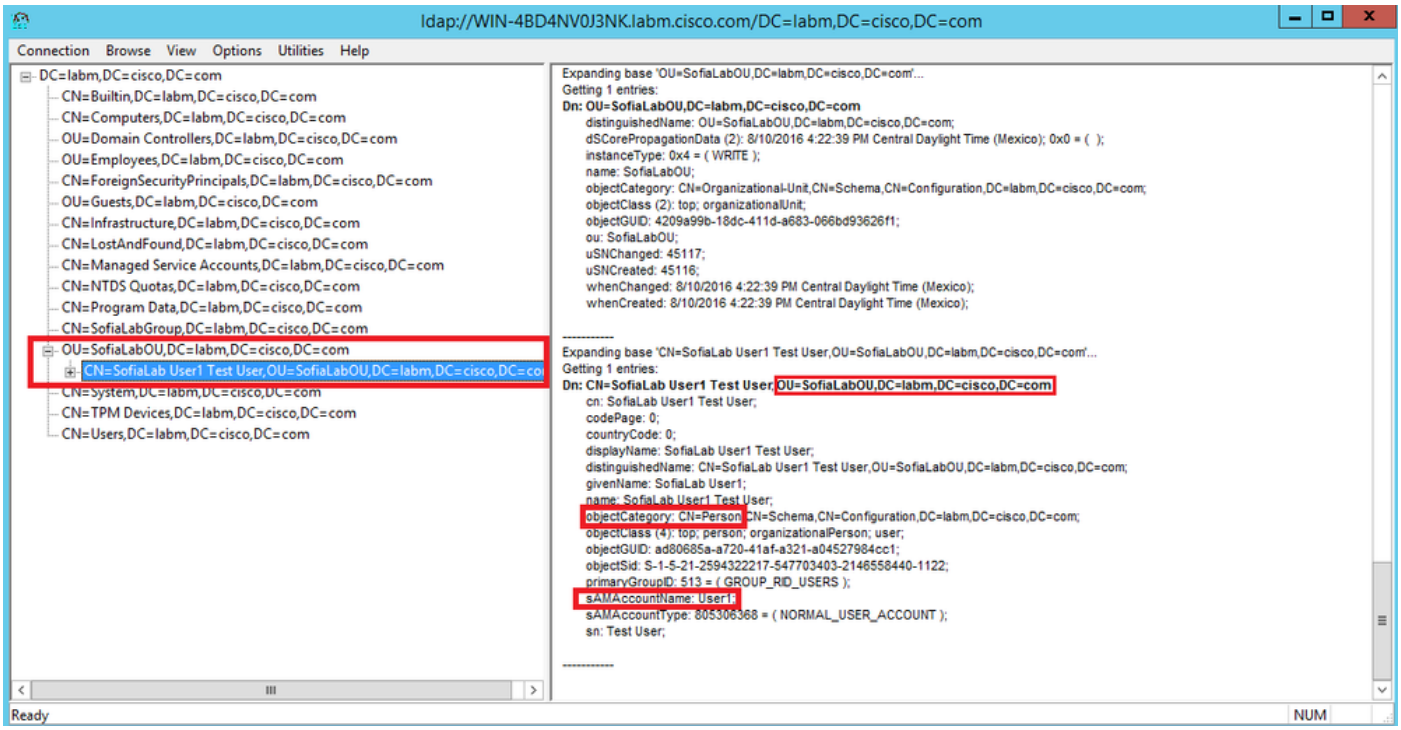
3단계. View(**보기) > Tree(트리)**로 이동하고 기본 DN에서 **OK(확인)**를 선택합니다.



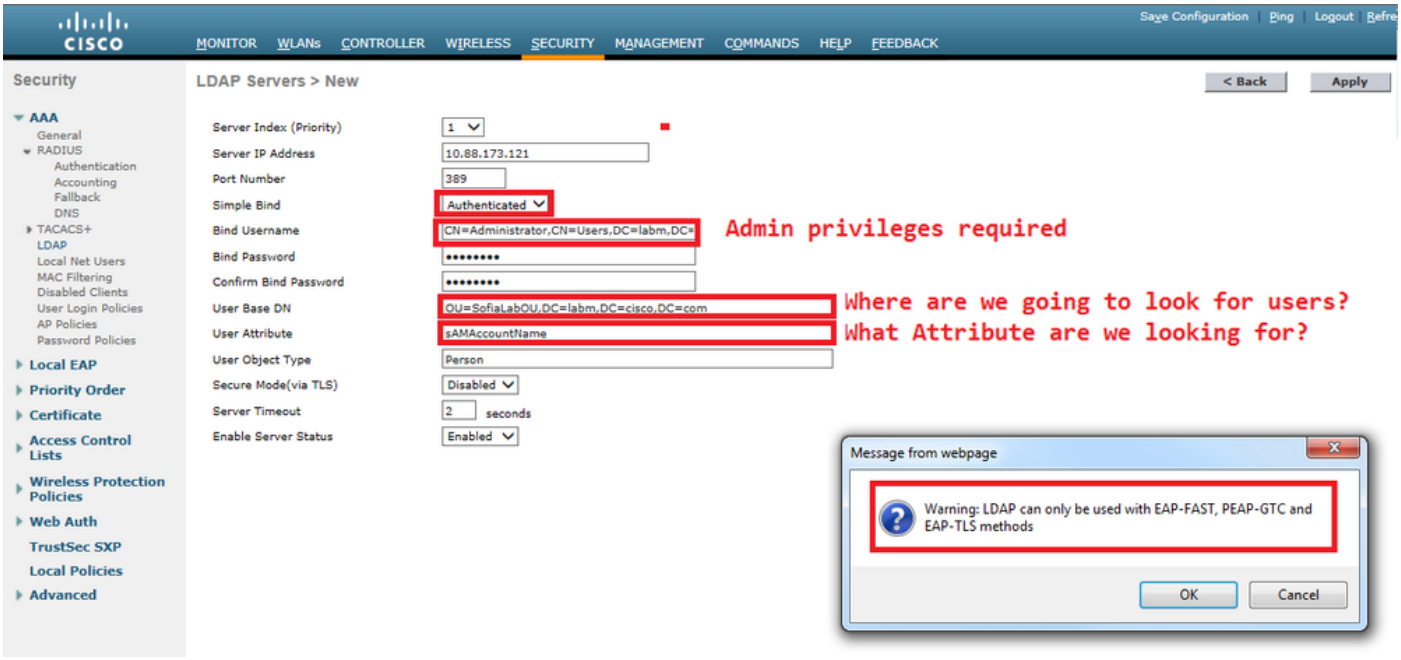
4단계. 트리를 확장하여 구조를 보고 Search Base DN을 찾습니다. 그룹을 제외한 모든 컨테이너 유형이 될 수 있습니다. 전체 도메인, 특정 OU 또는 CN=Users와 같은 CN일 수 있습니다.



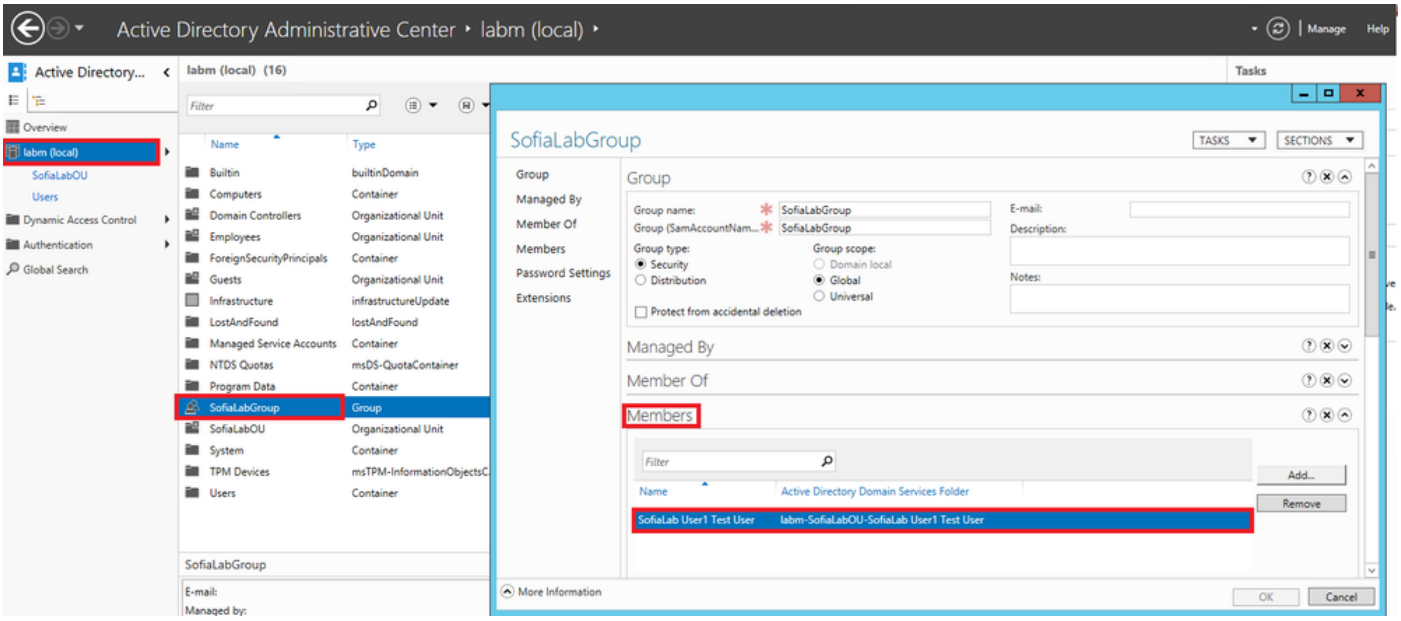
5단계. SofiaLabOU를 확장하여 어떤 사용자가 내부에 있는지 확인합니다. 이전에 생성한 User1이 있습니다.



6단계. LDAP 구성에 필요한 모든 것.



7단계. SofiaLabGroup과 같은 그룹은 검색 DN으로 사용할 수 없습니다. 그룹을 확장하고 그 안에 있는 사용자를 찾습니다. 여기서 이전에 생성한 User1은확인할 수 있습니다.



User1이(가) 있었지만 LDP에서 찾을 수 없습니다. 이는 WLC에서도 이 작업을 수행할 수 없으며, 따라서 그룹이 Search Base DN으로 지원되지 않는다는 것을 의미합니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

```
(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
```

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

```
(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
```

관련 정보

- LDAP - WLC 8.2 컨피그레이션 가이드
- LDAP(Lightweight Directory Access Protocol) 인증을 위해 WLC(Wireless Lan Controller)를 구성하는 방법 - Vinay Sharma
- WLC(Wireless LAN Controller)에서 LDAP를 사용한 웹 인증 컨피그레이션 예 - Yahya Jaber 및 Ayman Alfares
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.