為802.1x和Web-Auth WLAN配置WLC的LDAP身份驗證

目錄

簡介

本文檔介紹配置AireOS WLC的過程，以便使用LDAP伺服器作為使用者資料庫對客戶端進行身份驗證。

必要條件

需求

思科建議瞭解以下主題：

- Microsoft Windows伺服器
- Active Directory

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco WLC軟體8.2.110.0
- Microsoft Windows Server 2012 R2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

技術背景

- LDAP是用於訪問目錄伺服器的協定。
- 目錄伺服器是分層的、物件導向的資料庫。
- 對象以容器(如組織單位(OU)、組或預設的Microsoft Containers作為CN=Users)組織。
- 此設定最難的部分是在WLC上正確配置LDAP伺服器引數。

有關這些概念的更多詳細資訊，請參閱如何為輕量級目錄訪問協定(LDAP)身份驗證配置無線Lan控制器(WLC)的簡介部分。

常見問題

- 必須使用什麼使用者名稱與LDAP伺服器繫結？

針對LDAP伺服器進行繫結有兩種方法：Anonymous或Authenticated（為了瞭解兩種方法之間的區別，請參閱）。

此繫結使用者名稱需要具有管理員許可權，才能查詢其他使用者名稱/密碼。

- 如果通過身份驗證：繫結使用者名稱是否與所有使用者位於同一個容器中？

  不：使用整個路徑。例如：

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

是：僅使用使用者名稱。例如：

  管理員

- 如果使用者位於不同的容器中該怎麼辦？所有相關的無線LDAP使用者是否需要位於同一個容器中？

不能，可以指定一個包含所需所有容器的基本DN。

- WLC必須尋找哪些屬性？

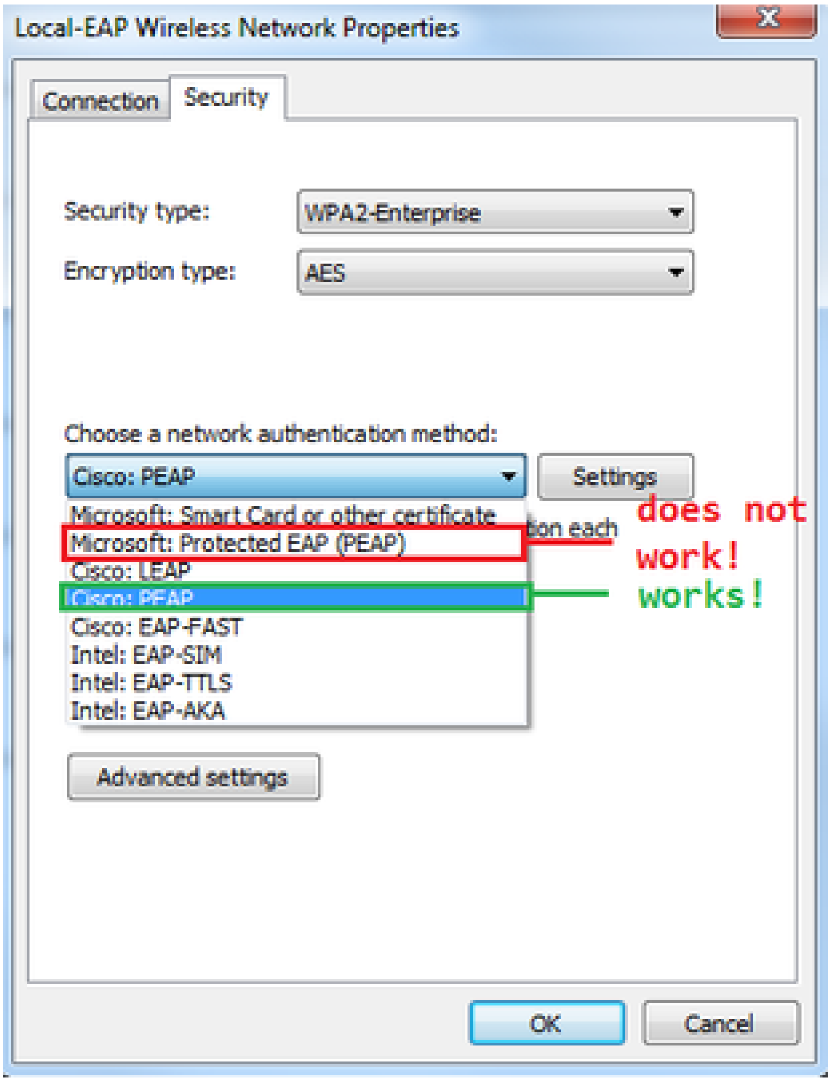
WLC與指定的使用者屬性和對象型別相匹配。

> **注意**:**sAMAccountName**區分大小寫，但person不區分大小寫。因此，**sAMAccountName=RICARDO**和**sAMAccountName=ricardo**是相同的，並且工作，而**samaccountname=RICARDO**和**samaccountname=ricardo**則不工作。

- 可以使用哪些可擴展身份驗證協定(EAP)方法？

僅限EAP-FAST、PEAP-GTC和EAP-TLS。Android、iOS和MacOS預設請求方與受保護的可擴展身份驗證協定(PEAP)配合使用。

對於Windows，必須在受支援的無線介面卡上使用Anyconnect Network Access Manager(NAM)或帶有Cisco:PEAP的預設Windows請求方，如下圖所示。



Local-EAP Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

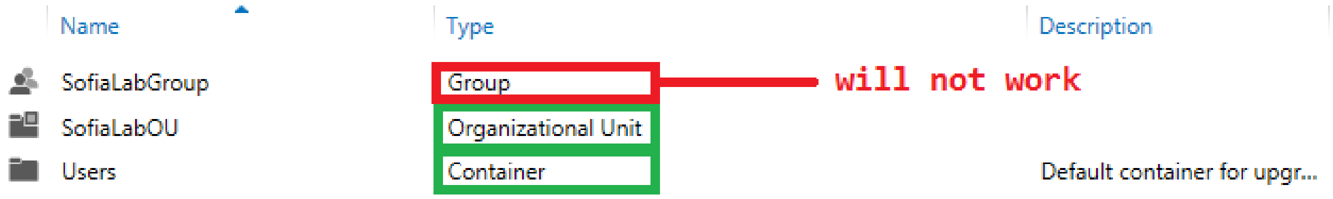
Cisco: PEAP

- Microsoft: Smart Card or other certificate
- Microsoft: Protected EAP (PEAP)
- Cisco: LEAP
- Cisco: PEAP
- Cisco: EAP-FAST
- Intel: EAP-SIM
- Intel: EAP-TTLS
- Intel: EAP-AKA

註:Cisco EAP Plug-ins for Windows包括受Cisco錯誤ID CSCva09670影響的開放安全套接字層(OpenSSL 0.9.8k)版本，思科不計畫發佈任何其他版本的Windows EAP外掛，並建議客戶改用AnyConnect安全移動客戶端。

- 為什麼WLC找不到使用者？

組內的使用者無法通過身份驗證。它們需要位於預設容器(CN)或組織單位(OU)中，如下圖所示。



Name	Type	Description
SofiaLabGroup	Group	
SofiaLabOU	Organizational Unit	
Users	Container	Default container for upgr...

設定

有多種不同的方案可以採用LDAP伺服器，包括802.1x身份驗證或Web身份驗證。

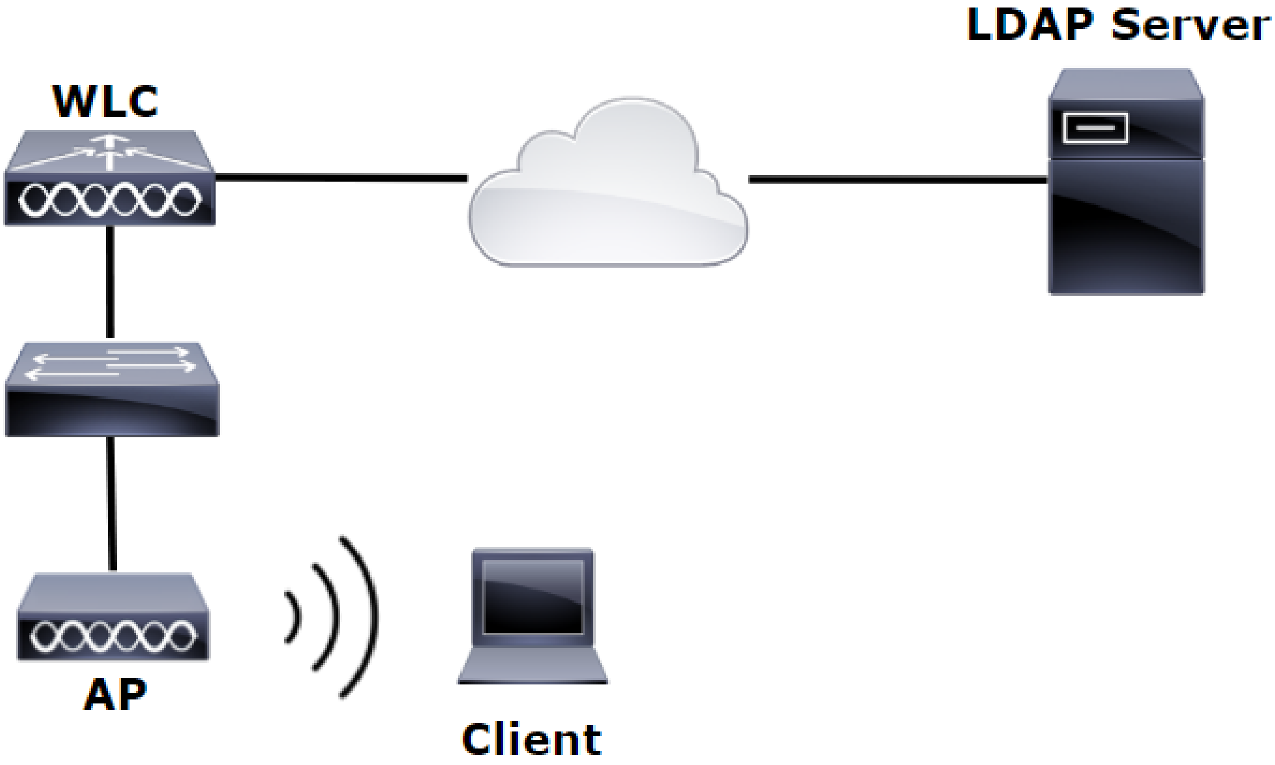
對於此過程，只有OU=SofiaLabOU內的使用者必須經過身份驗證。

若要瞭解如何使用Label Distribution Protocol(LDP)工具，請配置LDAP並對其進行故障排除，請參閱WLC LDAP配置指南。

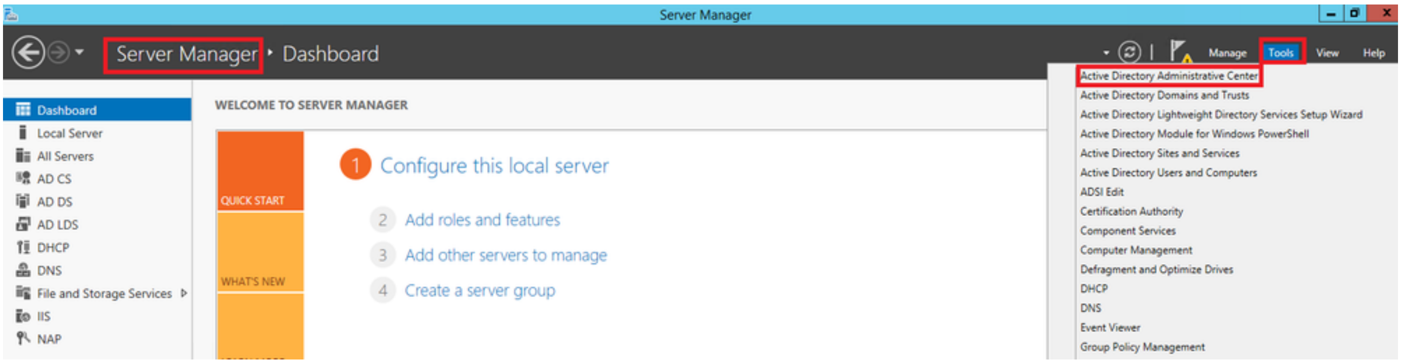
建立依賴LDAP伺服器通過802.1x驗證使用者身份的WLAN

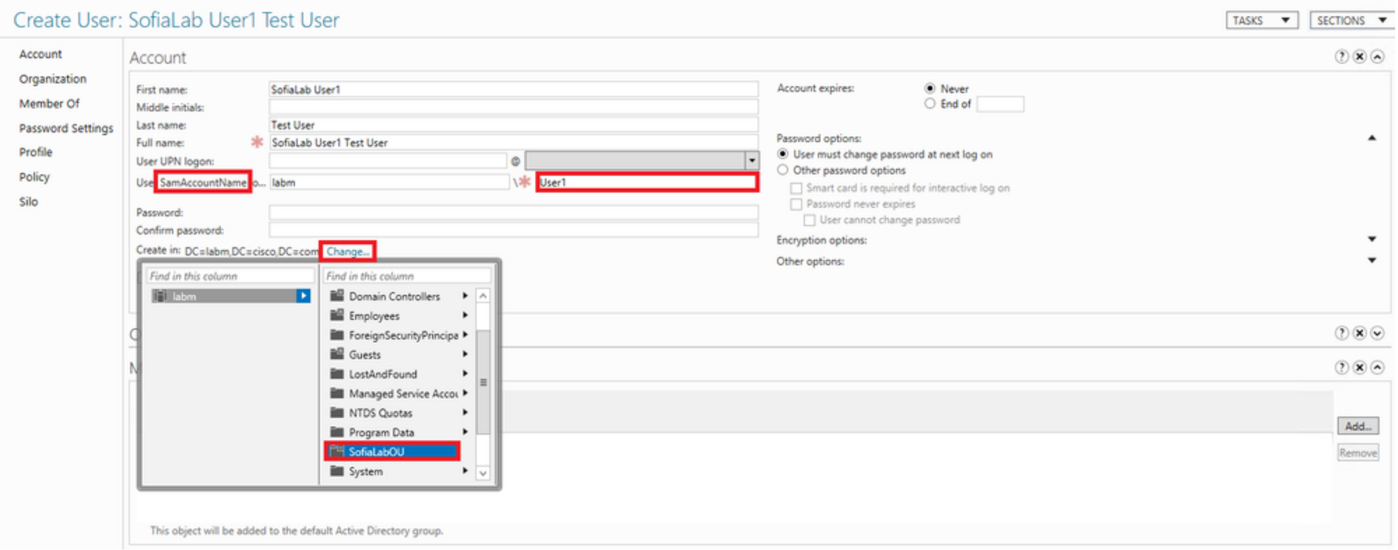
網路圖表

在此方案中，WLAN LDAP-dot1x使用LDAP伺服器使用802.1x對使用者進行身份驗證。



步驟1.在SofiaLabOU和SofiaLabGroup的LDAP伺服器成員中建立使用者**User1**。


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD CS
AD DS
AD LDS
DHCP
DNS
File and Storage Services
IIS
NAP
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Lightweight Directory Services Setup Wizard
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
DNS
Event Viewer
Group Policy Management



Create User: SofiaLab User1 Test User

Account

First name: SofiaLab User1
Middle initials:
Last name: Test User
Full name: SofiaLab User1 Test User
User UPN logon: @
User SamAccountName logon: labm \ User1
Password:
Confirm password:
Create in: DC=labm,DC=cisco,DC=com Change...

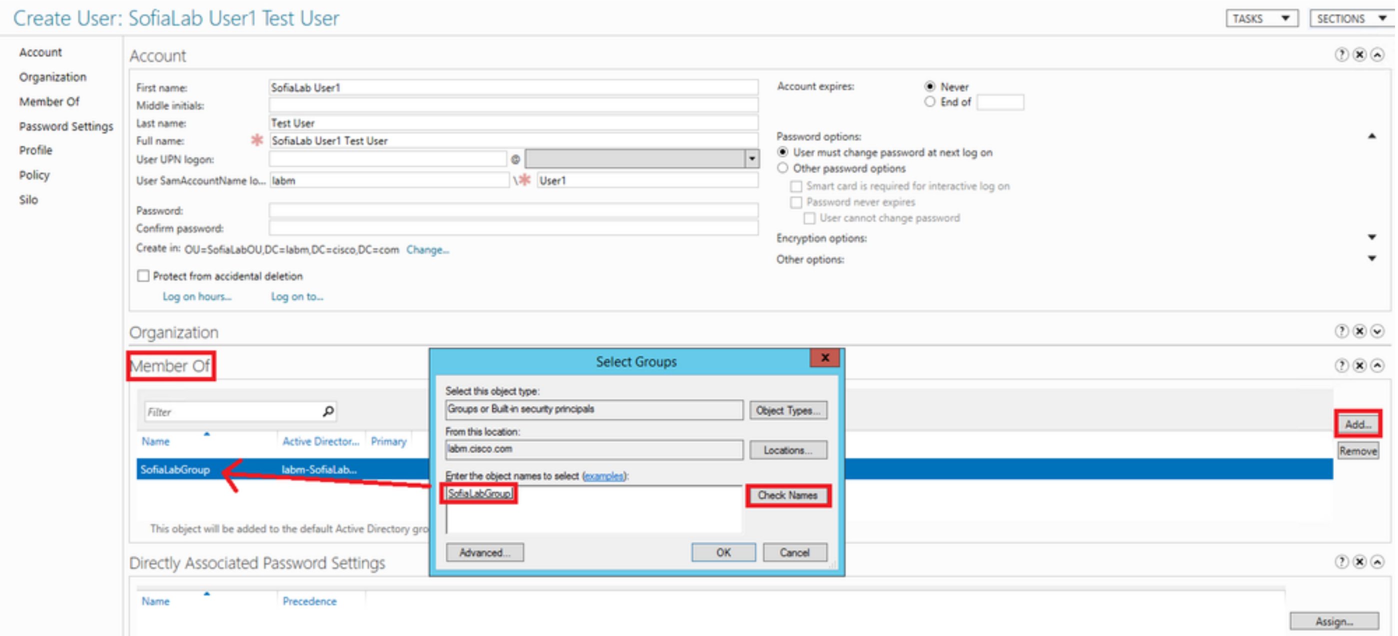
labm → SofiaLabOU

Account expires: ● Never ○ End of

Password options:
● User must change password at next log on
○ Other password options
□ Smart card is required for interactive log on
□ Password never expires
□ User cannot change password

Encryption options:
Other options:

This object will be added to the default Active Directory group.



Create User: SofiaLab User1 Test User

Account

First name: SofiaLab User1
Middle initials:
Last name: Test User
Full name: SofiaLab User1 Test User
User UPN logon: @
User SamAccountName lo... labm \ User1
Password:
Confirm password:
Create in: OU=SofiaLabOU,DC=labm,DC=cisco,DC=com Change...
□ Protect from accidental deletion
Log on hours... Log on to...

Account expires: ● Never ○ End of

Password options:
● User must change password at next log on
○ Other password options
□ Smart card is required for interactive log on
□ Password never expires
□ User cannot change password

Encryption options:
Other options:

Organization

Member Of

Filter

Name	Active Director...	Primary
SofiaLabGroup	labm-SofiaLab...	

This object will be added to the default Active Directory gro

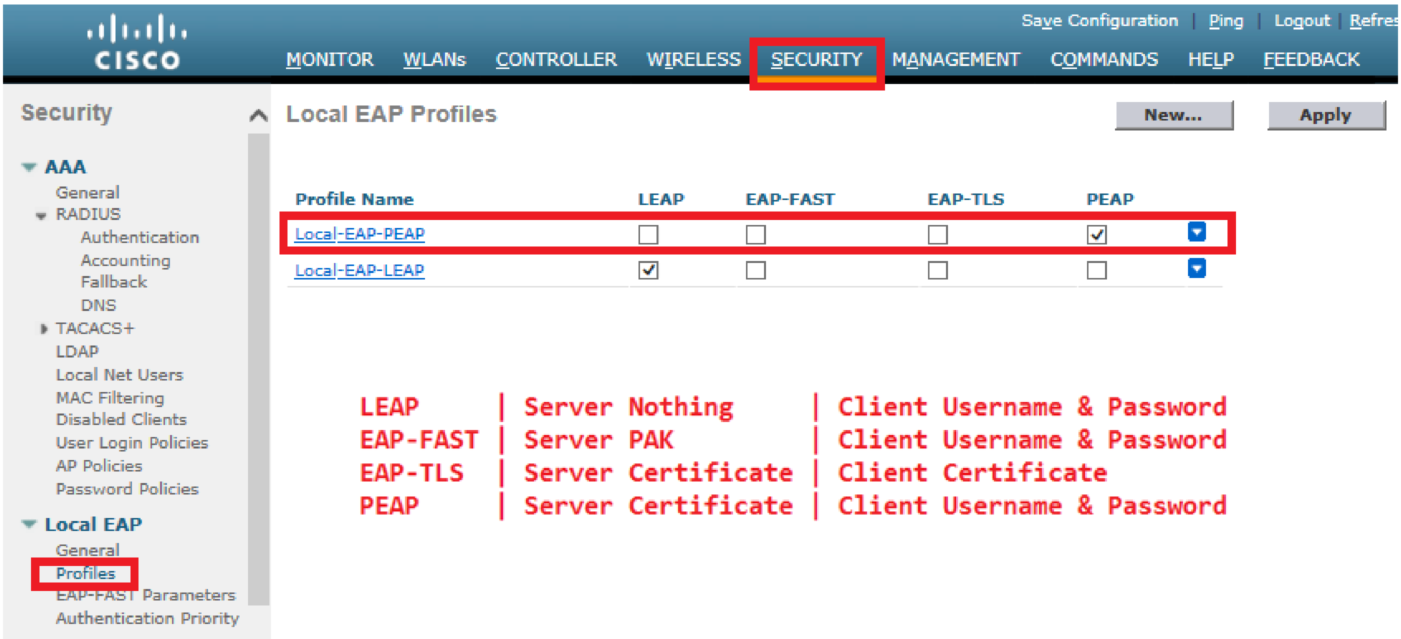
Select Groups

Select this object type: Groups or Built-in security principals
From this location: labm.cisco.com
Enter the object names to select (examples): SofiaLabGroup

Directly Associated Password Settings

Name	Precedence

步驟2.使用所需的EAP方法在WLC上建立EAP配置檔案（使用PEAP）。



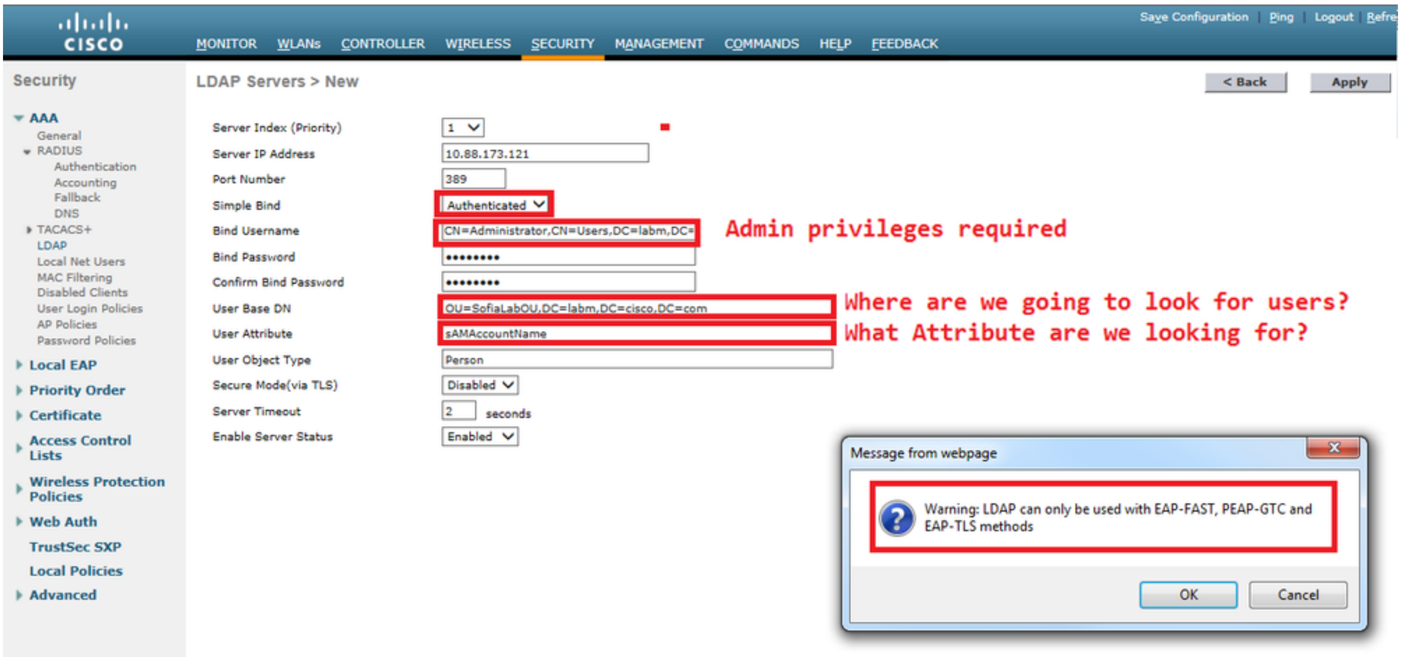
Local EAP Profiles

Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP
Local-EAP-PEAP	□	□	□	☑
Local-EAP-LEAP	☑	□	□	□

```
LEAP     | Server Nothing     | Client Username & Password
EAP-FAST | Server PAK         | Client Username & Password
EAP-TLS  | Server Certificate | Client Certificate
PEAP     | Server Certificate | Client Username & Password
```

步驟3.將WLC與LDAP伺服器繫結。

> **提示**：如果繫結使用者名稱不在使用者基本DN中，則必須將整個路徑寫入管理員用戶，如下圖所示。否則，您只需輸入**Administrator**。



LDAP Servers > New

Server Index (Priority): 1

Server IP Address: 10.88.173.121

Port Number: 389

Simple Bind: Authenticated

Bind Username: CN=Administrator,CN=Users,DC=labm,DC=

Bind Password: ••••••••

Confirm Bind Password: ••••••••

User Base DN: OU=SofiaLabOU,DC=labm,DC=cisco,DC=com

User Attribute: sAMAccountName

User Object Type: Person

Secure Mode(via TLS): Disabled

Server Timeout: 2 seconds

Enable Server Status: Enabled

Admin privileges required

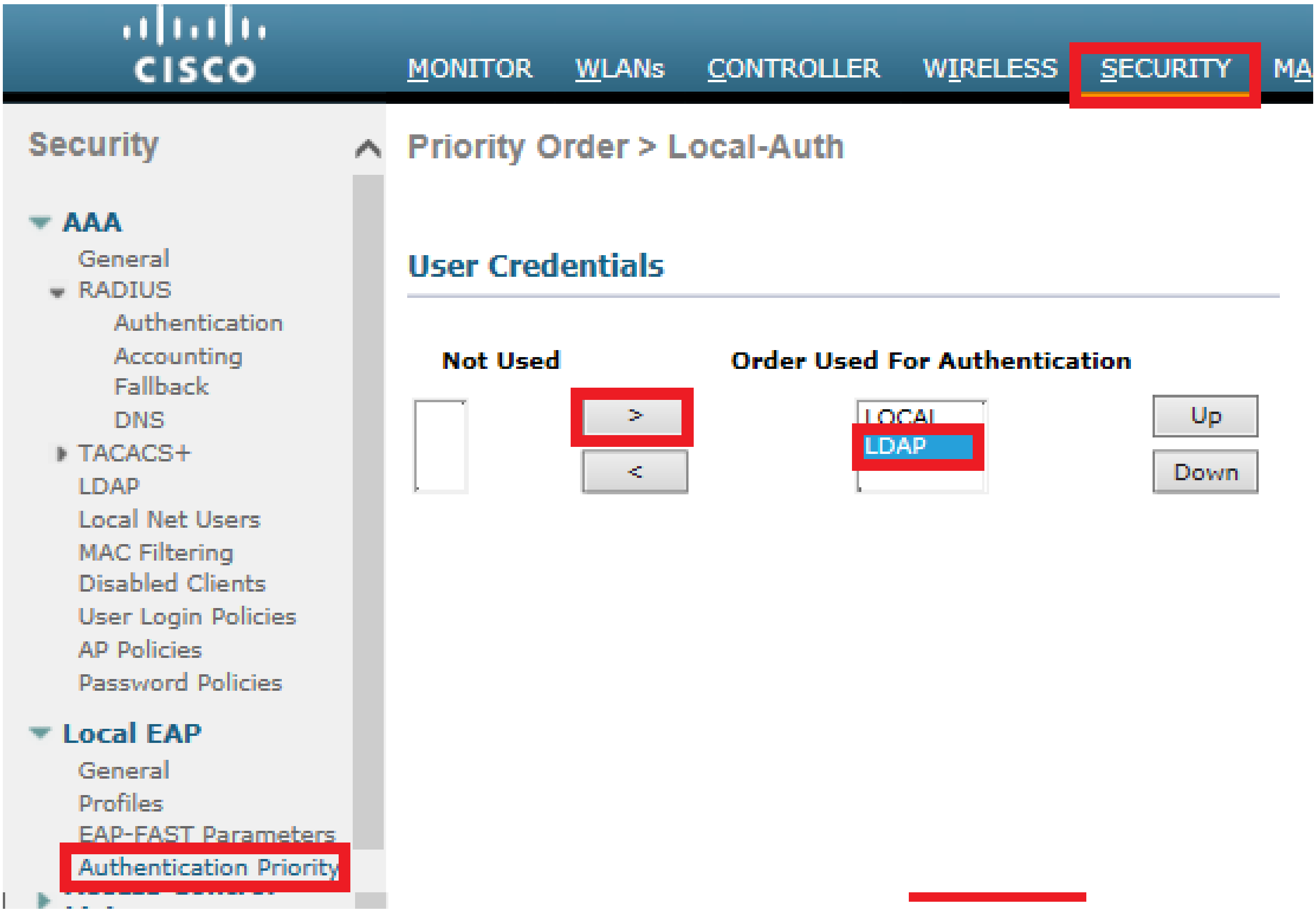
Where are we going to look for users?

What Attribute are we looking for?

Message from webpage

Warning: LDAP can only be used with EAP-FAST, PEAP-GTC and EAP-TLS methods

步驟4.將Authentication Order設定為Internal Users + LDAP或僅限LDAP。



Priority Order > Local-Auth

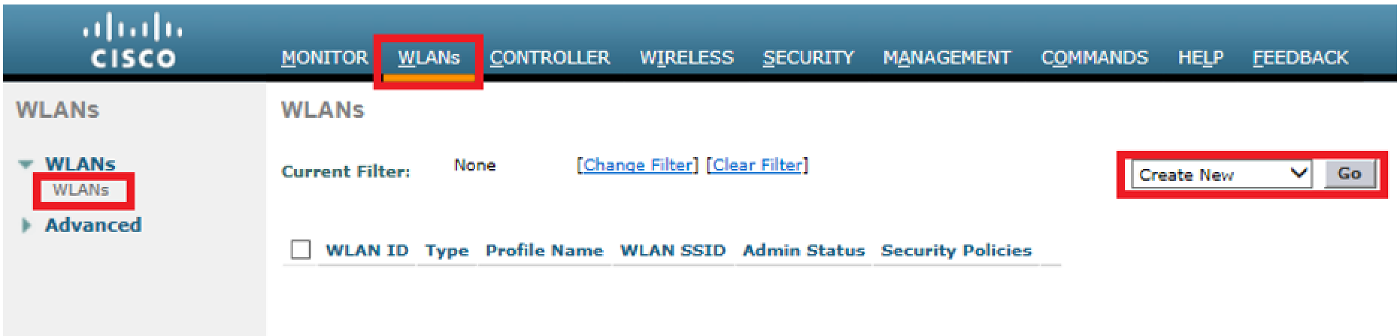
User Credentials

Not Used

Order Used For Authentication

LOCAL
LDAP

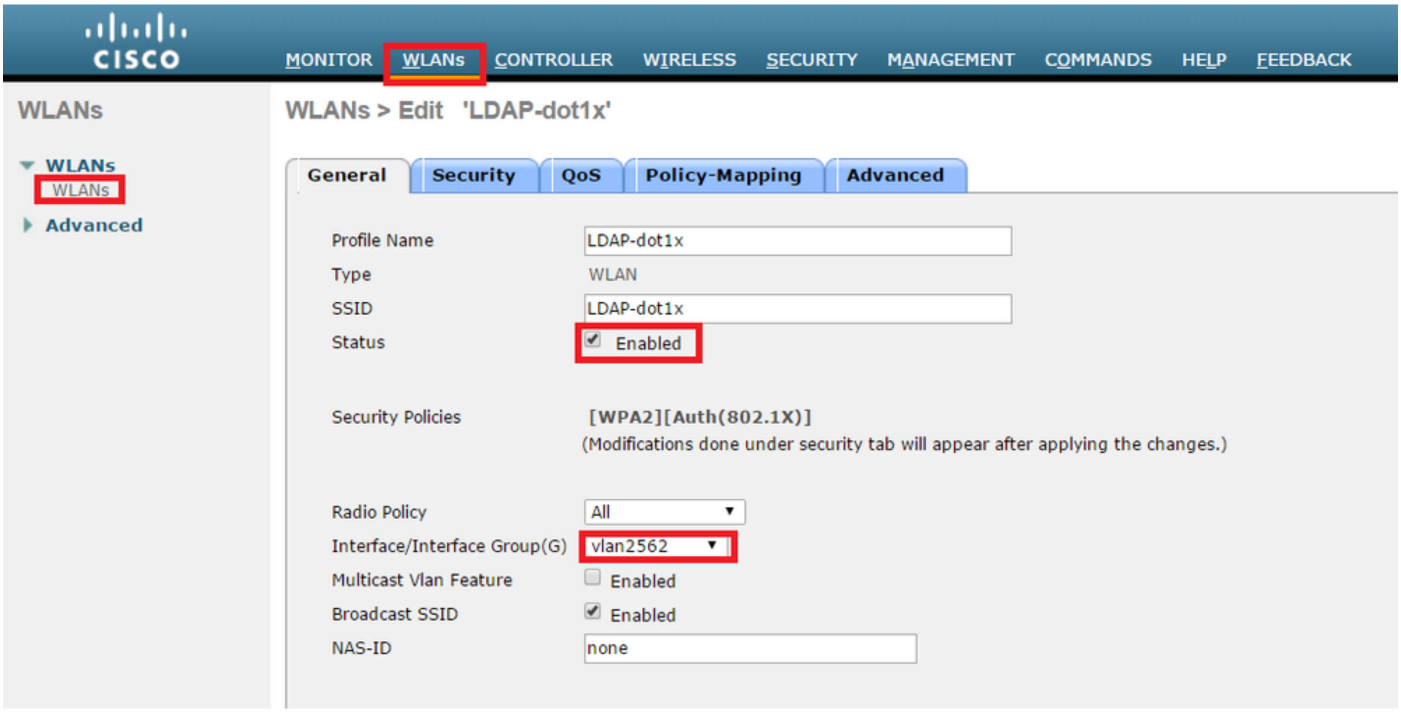
步驟5.建立LDAP-dot1x WLAN。



WLANs

Current Filter: None [Change Filter] [Clear Filter]

□	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies



WLANs > Edit 'LDAP-dot1x'

Profile Name: LDAP-dot1x

Type: WLAN

SSID: LDAP-dot1x

Status: ☑ Enabled

Security Policies: [WPA2][Auth(802.1X)]

(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

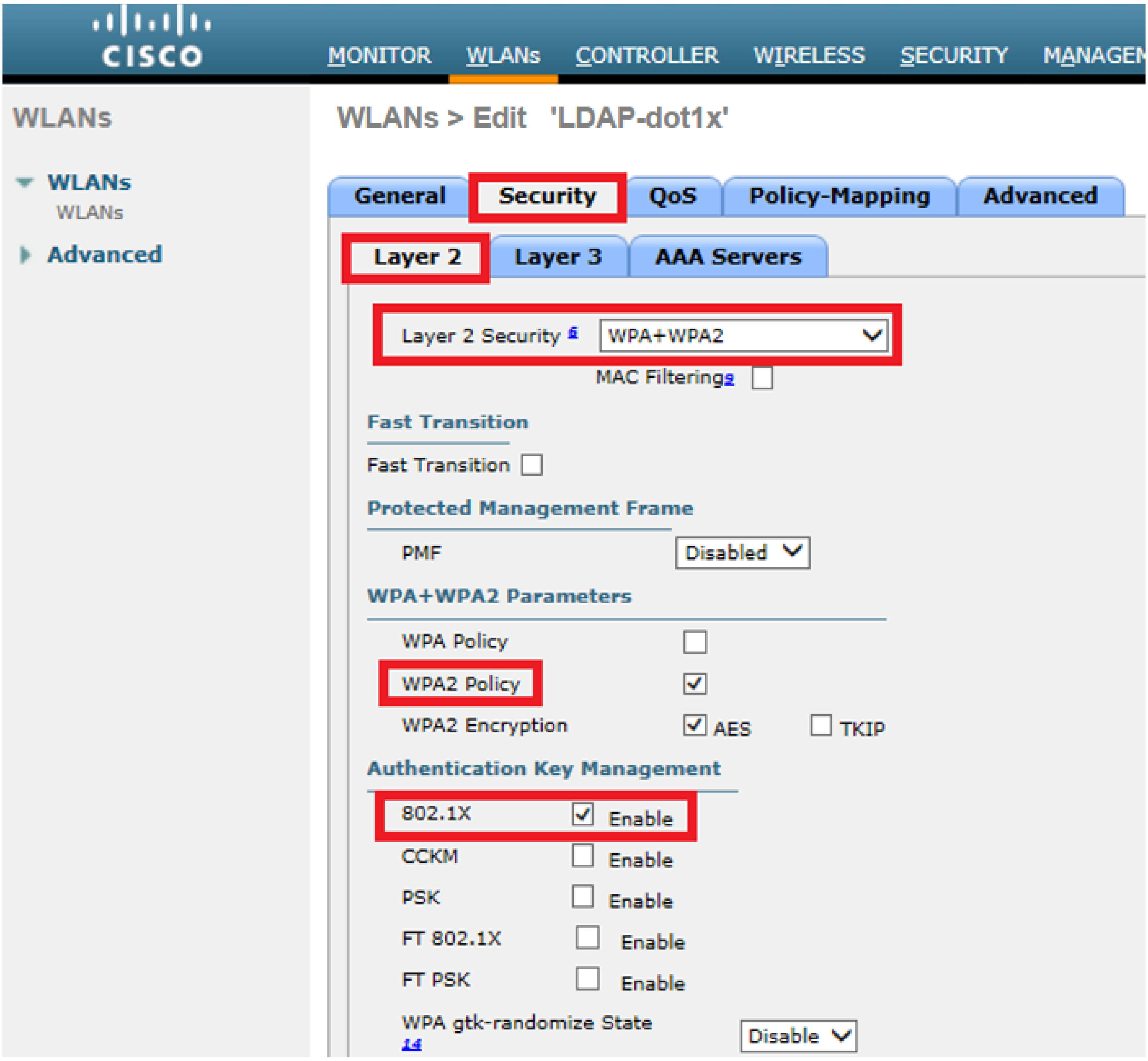
Interface/Interface Group(G): vlan2562

Multicast Vlan Feature: □ Enabled

Broadcast SSID: ☑ Enabled

NAS-ID: none

步驟6.將L2安全方法設定為WPA2 + 802.1x，並將L3安全設定為none。



WLANs > Edit 'LDAP-dot1x'

Layer 2 Security 6: WPA+WPA2

MAC Filtering2 □

Fast Transition

Fast Transition □

Protected Management Frame

PMF: Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

Authentication Key Management

802.1X ☑ Enable

CCKM □ Enable

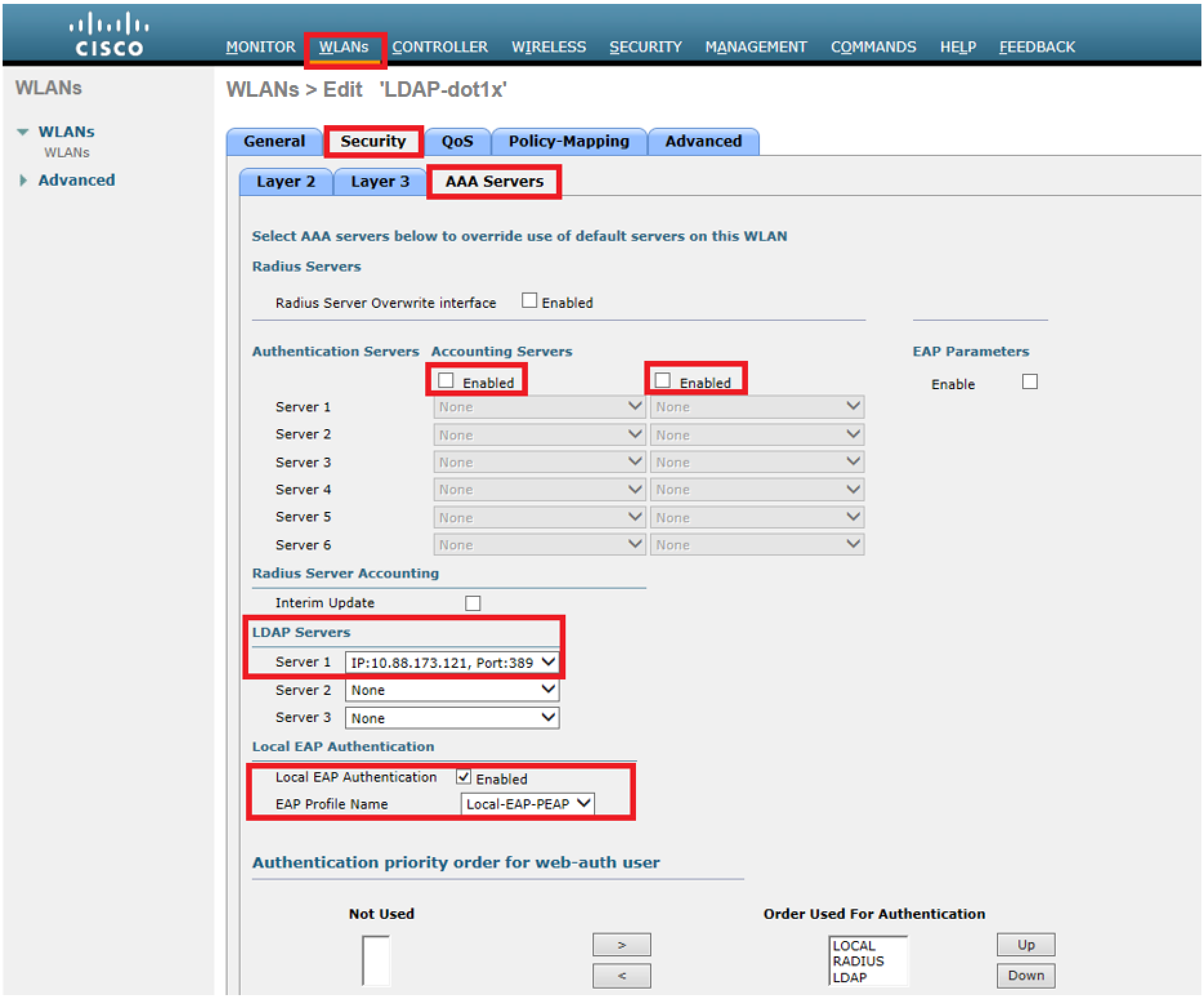
PSK □ Enable

FT 802.1X □ Enable

FT PSK □ Enable

WPA gtk-randomize State 14: Disable

步驟7.啟用本地EAP身份驗證，並確保禁用身份驗證伺服器和記帳伺服器選項並啟用LDAP。



WLANs > Edit 'LDAP-dot1x'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface □ Enabled

Authentication Servers	Accounting Servers		EAP Parameters	
	□ Enabled	□ Enabled	Enable	□
Server 1	None	None		
Server 2	None	None		
Server 3	None	None		
Server 4	None	None		
Server 5	None	None		
Server 6	None	None		

Radius Server Accounting

Interim Update □

LDAP Servers

Server 1	IP:10.88.173.121, Port:389
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication ☑ Enabled

EAP Profile Name Local-EAP-PEAP

Authentication priority order for web-auth user

Not Used

Order Used For Authentication

LOCAL
RADIUS
LDAP

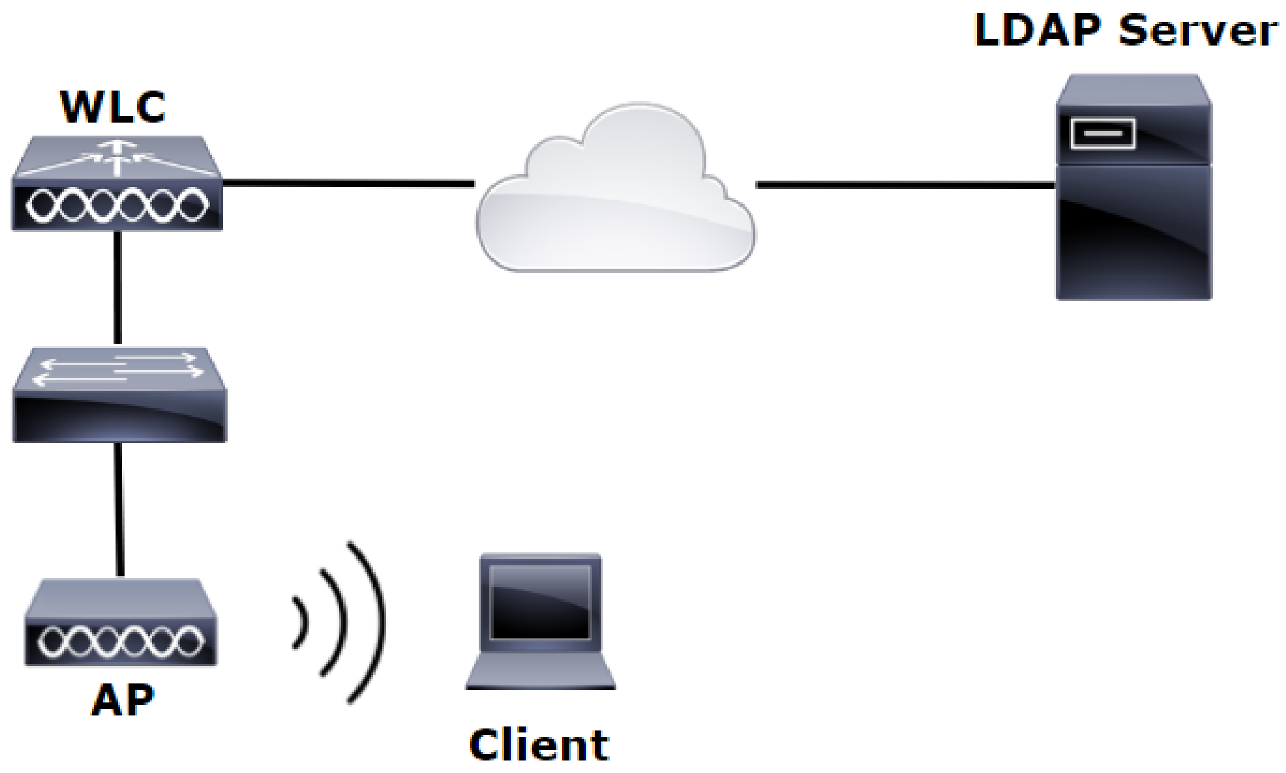
所有其他設定都可以保留為預設值。

> **附註**：
> 使用LDP工具確認配置引數。
> 搜尋基礎不能是組（如SofiaLabGroup）。
> 如果是Windows電腦，則必須使用PEAP-GTC或Cisco:PEAP，而不是請求方的Microsoft:PEAP。Microsoft:PEAP預設情況下可與MacOS/iOS/Android配合使用。

建立依賴LDAP伺服器通過內部WLC Web門戶對使用者進行身份驗證的WLAN

網路圖表

在此案例中，WLAN LDAP-Web使用LDAP伺服器通過內部WLC Web門戶對使用者進行身份驗證。



確保步驟1到步驟4.已取自上一示例。從這裡開始，WLAN配置的設定將有所不同。

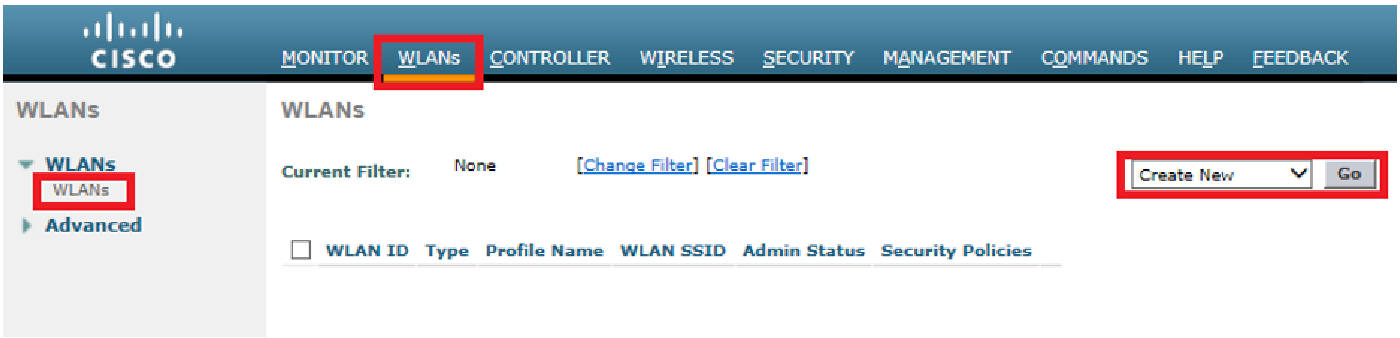
步驟1.在OU SofiaLabOU和組SofiaLabGroup的LDAP伺服器成員中建立使用者**User1**。

步驟2.使用所需的EAP方法在WLC上建立EAP配置檔案（使用PEAP）。

步驟3.將WLC與LDAP伺服器繫結。

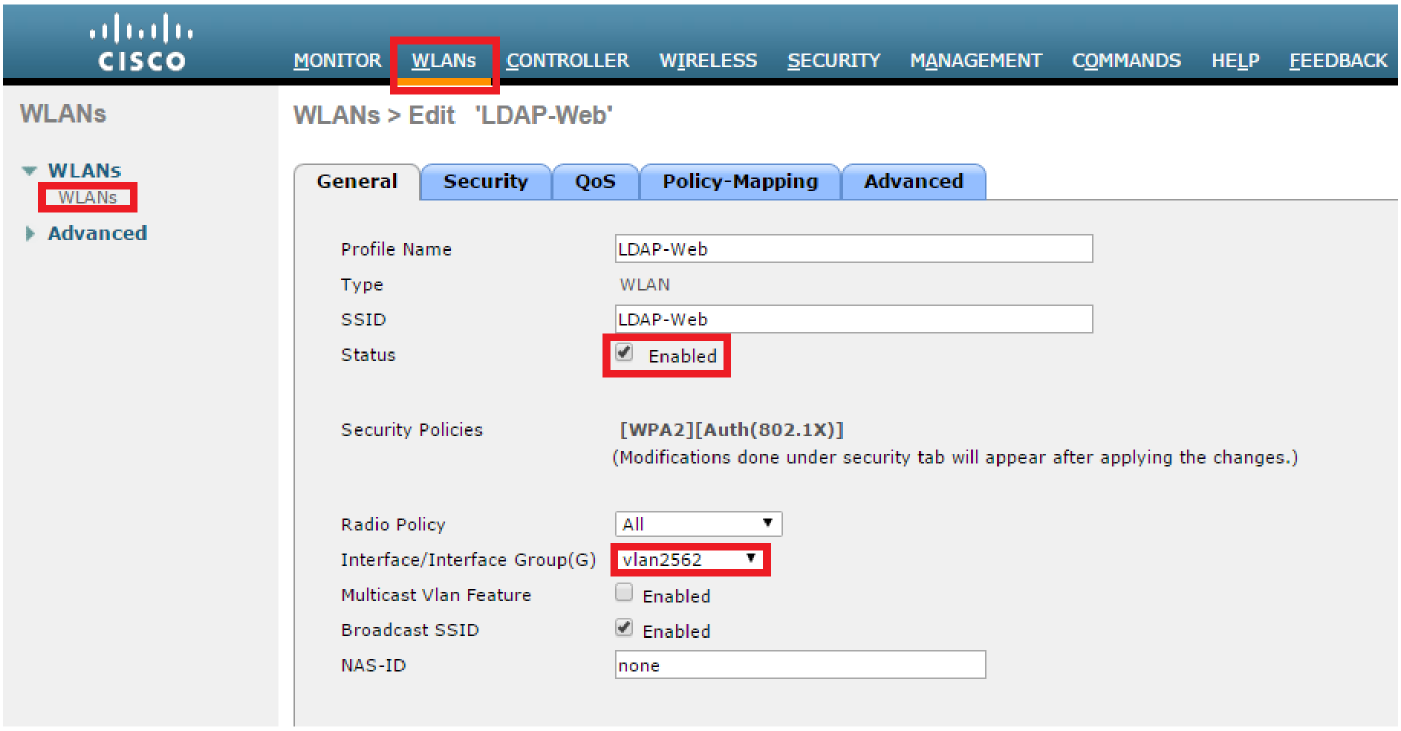
步驟4.將Authentication Order設定為Internal Users + LDAP。

步驟5.建立LDAP-Web WLAN，如圖所示。



Current Filter: None [Change Filter] [Clear Filter]

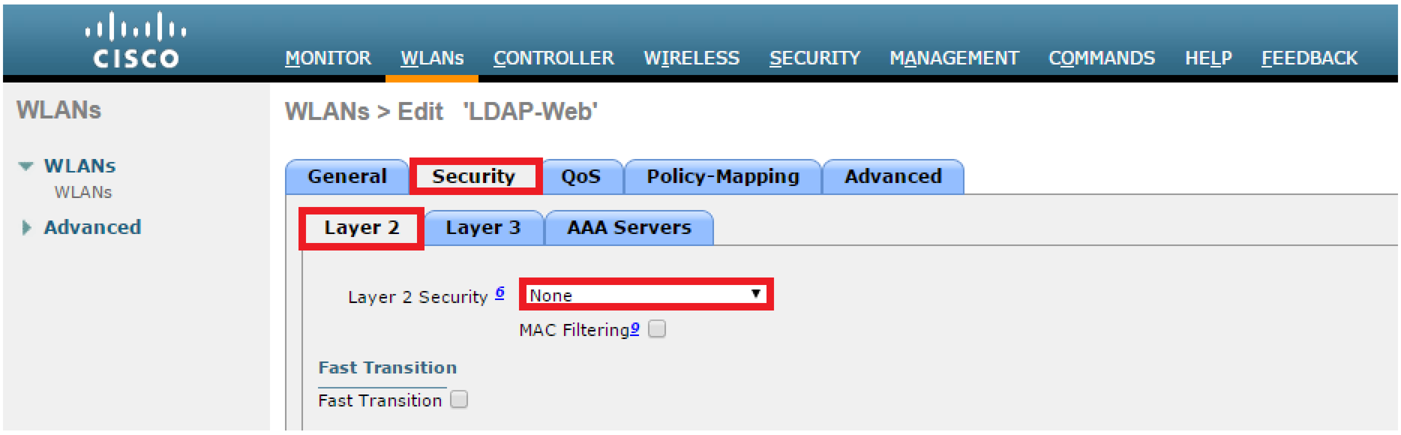
□	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies



WLANs > Edit 'LDAP-Web'

Profile Name	LDAP-Web
Type	WLAN
SSID	LDAP-Web
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	vlan2562
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

步驟6.將L2 Security設定為none，將L3 Security設定為Web Policy - Authentication如圖所示。



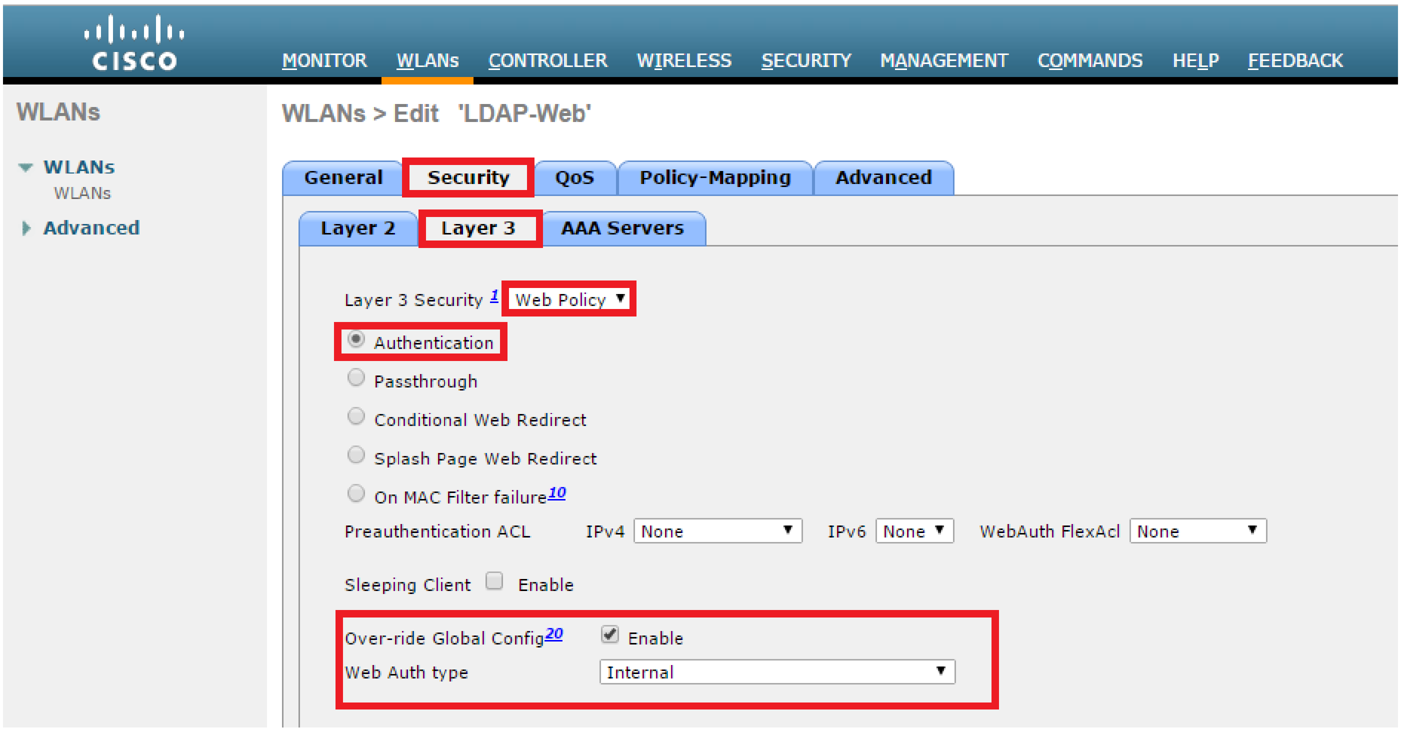
WLANs > Edit 'LDAP-Web'

Layer 2 Security 6 None

MAC Filtering9 □

Fast Transition

Fast Transition □



WLANs > Edit 'LDAP-Web'

Layer 3 Security [1] Web Policy

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

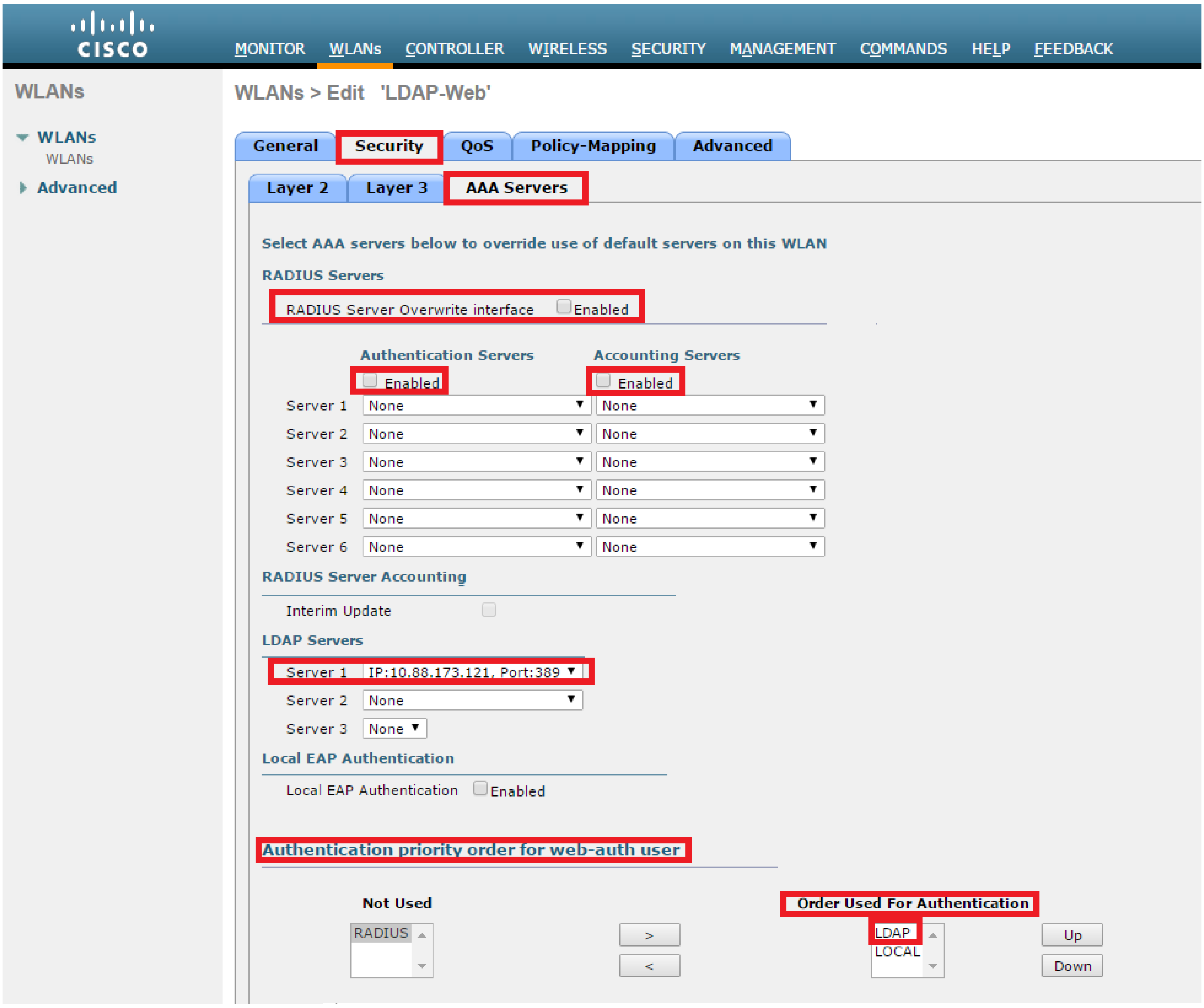
Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

Sleeping Client □ Enable

Over-ride Global Config[20] ☑ Enable

Web Auth type Internal

步驟7. 將Web-auth的身份驗證優先順序順序設定為使用LDAP，並確保已禁用身份驗證伺服器和記帳伺服器選項。



WLANs > Edit 'LDAP-Web'

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	□ Enabled	□ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

RADIUS Server Accounting

Interim Update □

LDAP Servers

Server 1 IP:10.88.173.121, Port:389

Server 2 None

Server 3 None

Local EAP Authentication

Local EAP Authentication □ Enabled

Authentication priority order for web-auth user

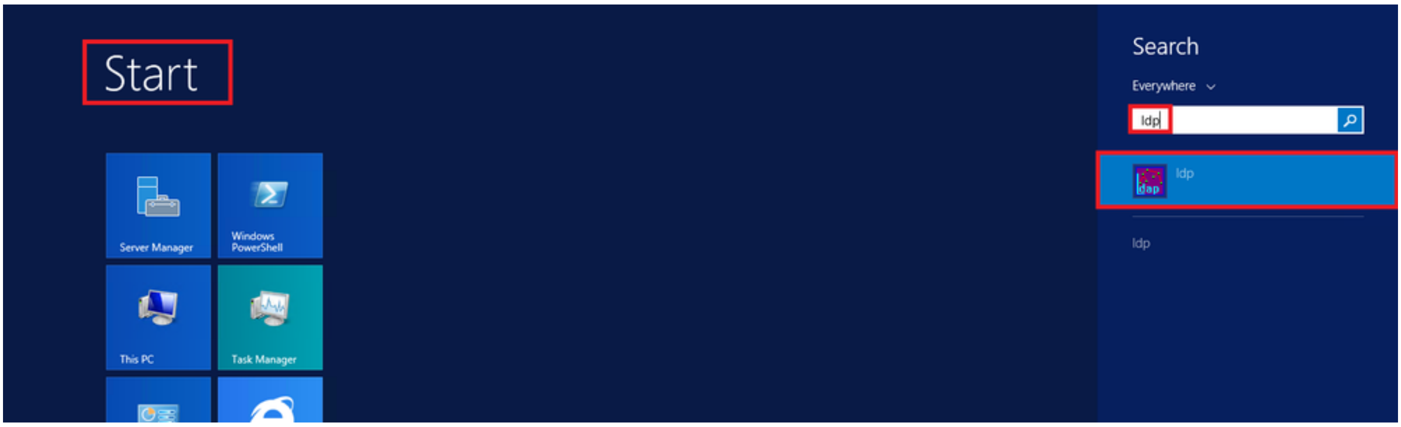
Not Used: RADIUS

Order Used For Authentication: LDAP, LOCAL

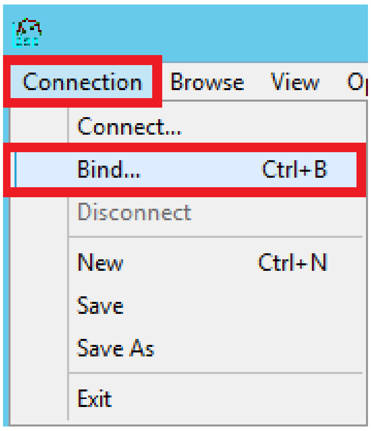
所有其他設定都可以保留為預設值。

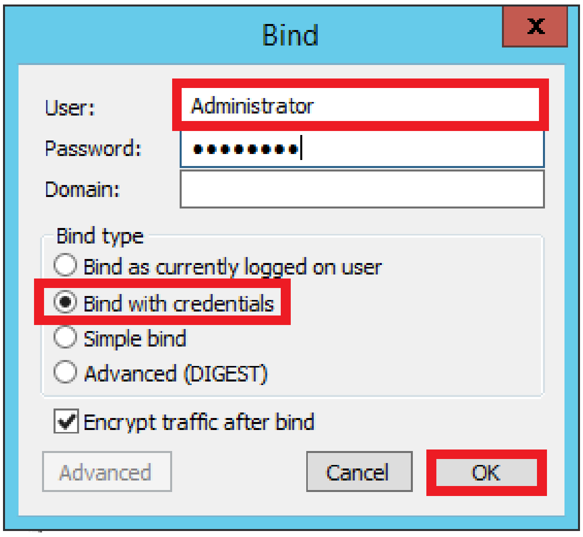
使用LDP工具對LDAP進行配置和故障排除

步驟1.在LDAP伺服器或具有連線的主機開啟LDP工具（必須允許到伺服器的埠TCP 389）。



步驟2. 導航到**Connection > Bind**，使用Admin使用者登入，然後選擇**Bind with credentials**單選按鈕。



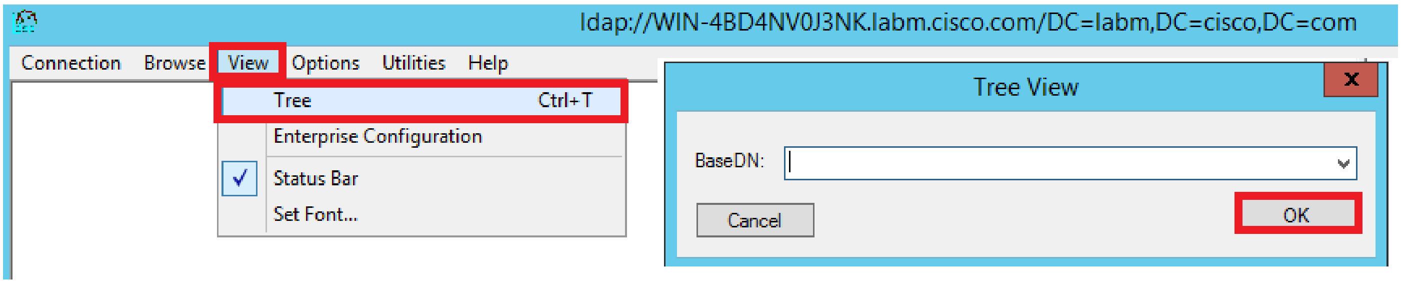


User: Administrator
Password: ••••••••
Domain:

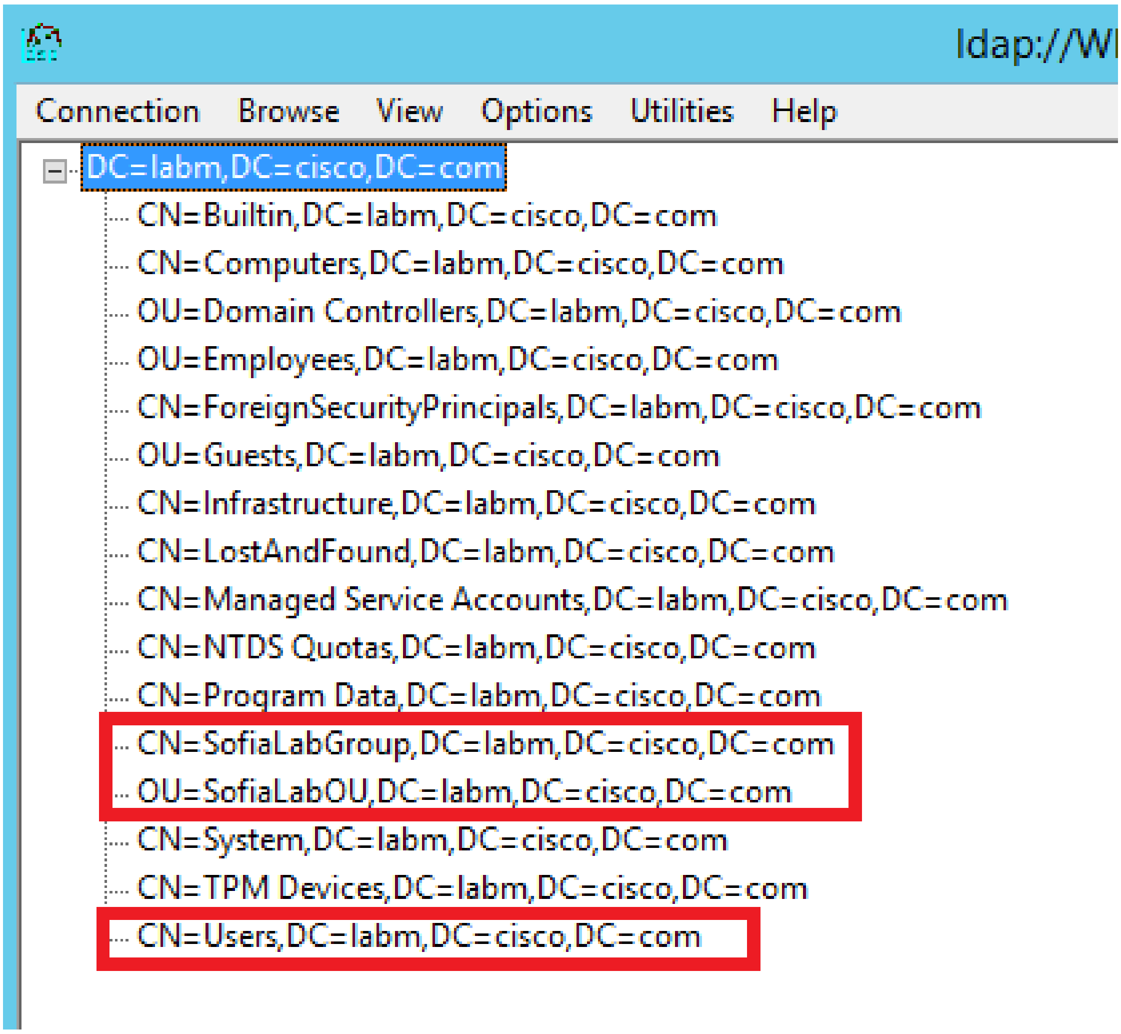
Bind type
○ Bind as currently logged on user
● Bind with credentials
○ Simple bind
○ Advanced (DIGEST)

☑ Encrypt traffic after bind

步驟3.導覽至**View > Tree**，然後在基本DN中選擇**OK**。

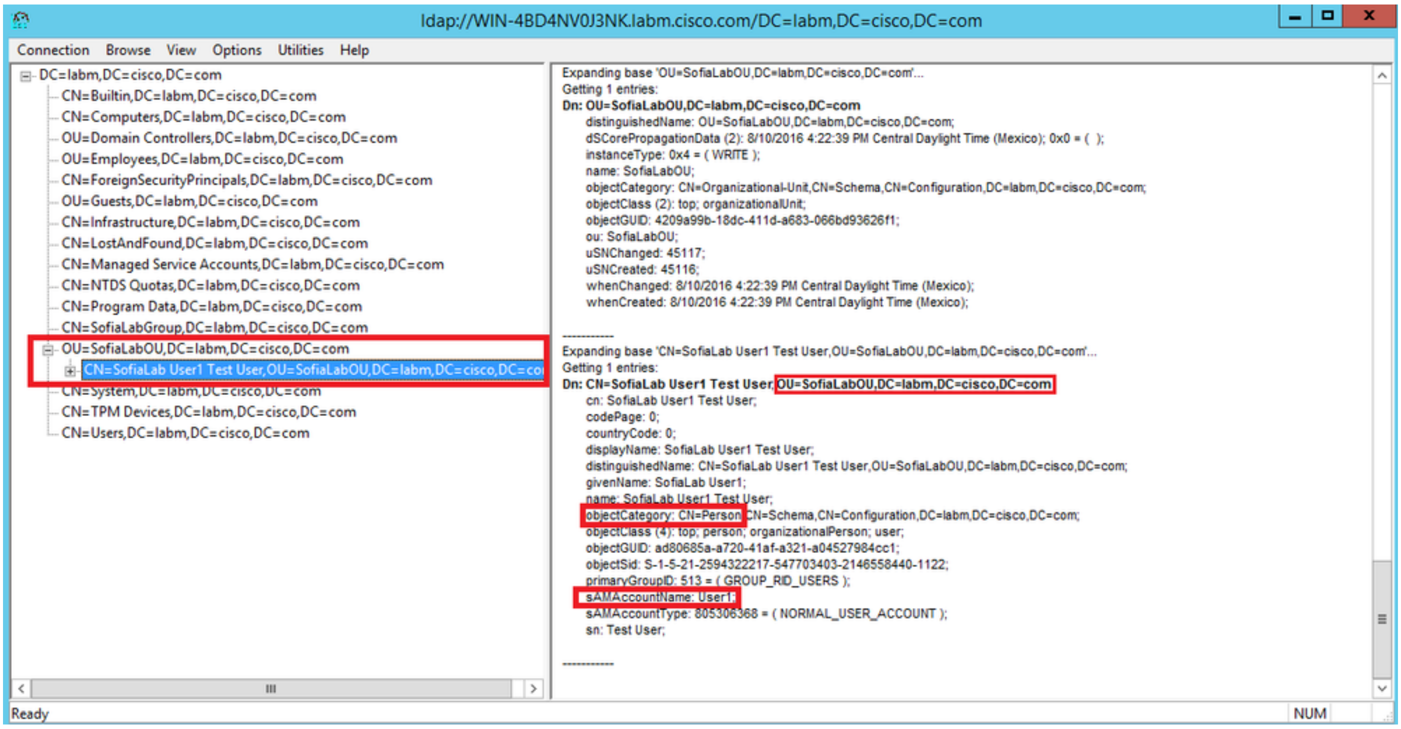

ldap://WIN-4BD4NV0J3NK.labm.cisco.com/DC=labm,DC=cisco,DC=com

步驟4.展開樹以檢視結構並查詢Search Base DN。請考慮它可以是除「組」之外的任何容器型別。可以是整個域、特定OU或類似CN=Users的CN。



```
DC=labm,DC=cisco,DC=com
    CN=Builtin,DC=labm,DC=cisco,DC=com
    CN=Computers,DC=labm,DC=cisco,DC=com
    OU=Domain Controllers,DC=labm,DC=cisco,DC=com
    OU=Employees,DC=labm,DC=cisco,DC=com
    CN=ForeignSecurityPrincipals,DC=labm,DC=cisco,DC=com
    OU=Guests,DC=labm,DC=cisco,DC=com
    CN=Infrastructure,DC=labm,DC=cisco,DC=com
    CN=LostAndFound,DC=labm,DC=cisco,DC=com
    CN=Managed Service Accounts,DC=labm,DC=cisco,DC=com
    CN=NTDS Quotas,DC=labm,DC=cisco,DC=com
    CN=Program Data,DC=labm,DC=cisco,DC=com
    CN=SofiaLabGroup,DC=labm,DC=cisco,DC=com
    OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
    CN=System,DC=labm,DC=cisco,DC=com
    CN=TPM Devices,DC=labm,DC=cisco,DC=com
    CN=Users,DC=labm,DC=cisco,DC=com
```

步驟5.展開SofiaLabOU以檢視其內部使用者。這是之前建立的User1。



ldap://WIN-4BD4NV0J3NK.labm.cisco.com/DC=labm,DC=cisco,DC=com
Connection Browse View Options Utilities Help
Ready
NUM

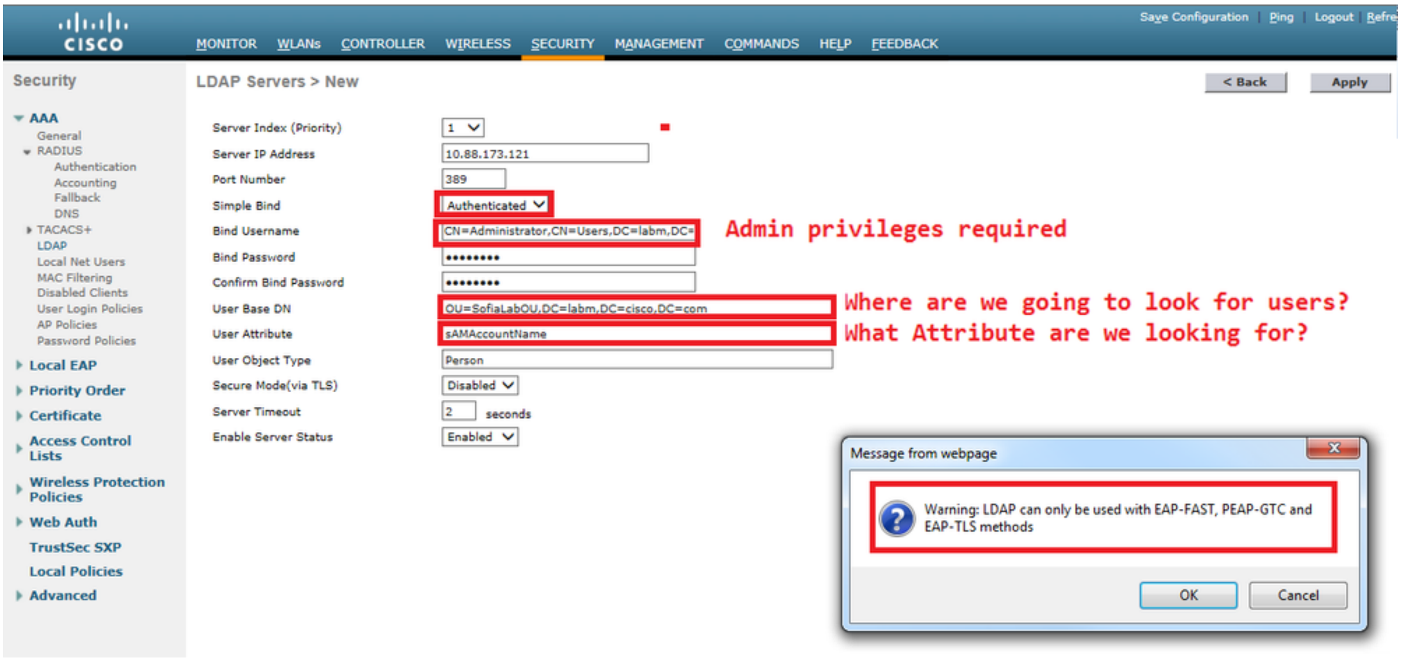
```
DC=labm,DC=cisco,DC=com
    CN=Builtin,DC=labm,DC=cisco,DC=com
    CN=Computers,DC=labm,DC=cisco,DC=com
    OU=Domain Controllers,DC=labm,DC=cisco,DC=com
    OU=Employees,DC=labm,DC=cisco,DC=com
    CN=ForeignSecurityPrincipals,DC=labm,DC=cisco,DC=com
    OU=Guests,DC=labm,DC=cisco,DC=com
    CN=Infrastructure,DC=labm,DC=cisco,DC=com
    CN=LostAndFound,DC=labm,DC=cisco,DC=com
    CN=Managed Service Accounts,DC=labm,DC=cisco,DC=com
    CN=NTDS Quotas,DC=labm,DC=cisco,DC=com
    CN=Program Data,DC=labm,DC=cisco,DC=com
    CN=SofiaLabGroup,DC=labm,DC=cisco,DC=com
    OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
        CN=SofiaLab User1 Test User,OU=SofiaLabOU,DC=labm,DC=cisco,DC=co
    CN=System,DC=labm,DC=cisco,DC=com
    CN=TPM Devices,DC=labm,DC=cisco,DC=com
    CN=Users,DC=labm,DC=cisco,DC=com
```

```
Expanding base 'OU=SofiaLabOU,DC=labm,DC=cisco,DC=com'...
Getting 1 entries:
Dn: OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
    distinguishedName: OU=SofiaLabOU,DC=labm,DC=cisco,DC=com;
    dSCorePropagationData (2): 8/10/2016 4:22:39 PM Central Daylight Time (Mexico); 0x0 = (  );
    instanceType: 0x4 = ( WRITE );
    name: SofiaLabOU;
    objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=labm,DC=cisco,DC=com;
    objectClass (2): top; organizationalUnit;
    objectGUID: 4209a99b-18dc-411d-a683-066bd93626f1;
    ou: SofiaLabOU;
    uSNChanged: 45117;
    uSNCreated: 45116;
    whenChanged: 8/10/2016 4:22:39 PM Central Daylight Time (Mexico);
    whenCreated: 8/10/2016 4:22:39 PM Central Daylight Time (Mexico);

-----------
Expanding base 'CN=SofiaLab User1 Test User,OU=SofiaLabOU,DC=labm,DC=cisco,DC=com'...
Getting 1 entries:
Dn: CN=SofiaLab User1 Test User,OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
    cn: SofiaLab User1 Test User;
    codePage: 0;
    countryCode: 0;
    displayName: SofiaLab User1 Test User;
    distinguishedName: CN=SofiaLab User1 Test User,OU=SofiaLabOU,DC=labm,DC=cisco,DC=com;
    givenName: SofiaLab User1;
    name: SofiaLab User1 Test User;
    objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=labm,DC=cisco,DC=com;
    objectClass (4): top; person; organizationalPerson; user;
    objectGUID: ad80685a-a720-41af-a321-a04527984cc1;
    objectSid: S-1-5-21-2594322217-547703403-2146558440-1122;
    primaryGroupID: 513 = ( GROUP_RID_USERS );
    sAMAccountName: User1;
    sAMAccountType: 805306368 = ( NORMAL_USER_ACCOUNT );
    sn: Test User;

-----------
```

步驟6.配置LDAP所需的全部資訊。



LDAP Servers > New

Server Index (Priority)	1
Server IP Address	10.88.173.121
Port Number	389
Simple Bind	Authenticated
Bind Username	CN=Administrator,CN=Users,DC=labm,DC=
Bind Password	••••••••
Confirm Bind Password	••••••••
User Base DN	OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
User Attribute	sAMAccountName
User Object Type	Person
Secure Mode(via TLS)	Disabled
Server Timeout	2 seconds
Enable Server Status	Enabled

Admin privileges required

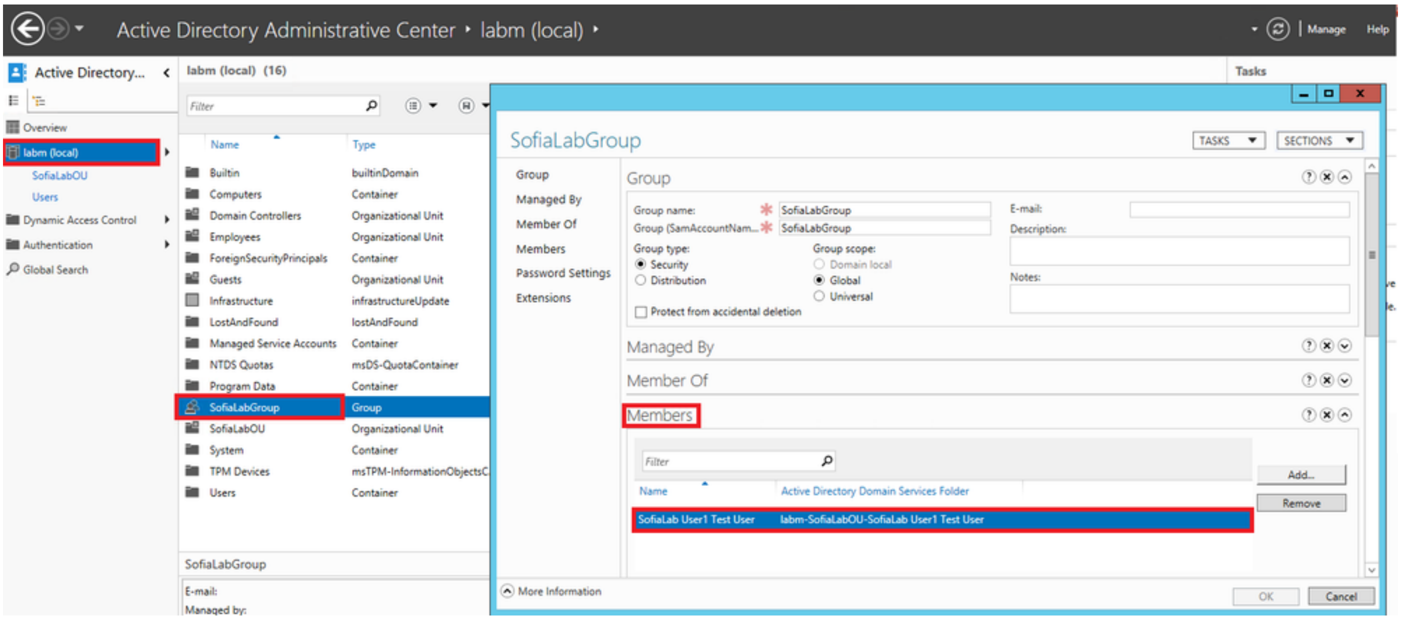
Where are we going to look for users?

What Attribute are we looking for?

Message from webpage

Warning: LDAP can only be used with EAP-FAST, PEAP-GTC and EAP-TLS methods

步驟7.SofiaLabGroup等組不能用作搜尋DN。展開組並查詢組內的使用者，其中之前建立的User1必須是如圖所示。



Name	Type
Builtin	builtinDomain
Computers	Container
Domain Controllers	Organizational Unit
Employees	Organizational Unit
ForeignSecurityPrincipals	Container
Guests	Organizational Unit
Infrastructure	infrastructureUpdate
LostAndFound	lostAndFound
Managed Service Accounts	Container
NTDS Quotas	msDS-QuotaContainer
Program Data	Container
SofiaLabGroup	Group
SofiaLabOU	Organizational Unit
System	Container
TPM Devices	msTPM-InformationObjectsC
Users	Container

SofiaLabGroup

E-mail:

Managed by:

SofiaLabGroup

Group

Group name: SofiaLabGroup

Group (SamAccountNam...: SofiaLabGroup

E-mail:

Description:

Notes:

Group type: ● Security ○ Distribution

Group scope: ○ Domain local ● Global ○ Universal

□ Protect from accidental deletion

Managed By

Member Of

Members

Name	Active Directory Domain Services Folder
SofiaLab User1 Test User	labm-SofiaLabOU-SofiaLab User1 Test User

User1曾在那裡，但LDP找不到它。這表示WLC無法順利執行，因此不支援群組作為搜尋基礎DN。

驗證

使用本節內容，確認您的組態是否正常運作。

```
 (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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

```
(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
```

相關資訊

- LDAP - WLC 8.2配置指南
- 如何為輕量型目錄存取通訊協定(LDAP)驗證設定無線Lan控制器(WLC)- Vinay Sharma
- 在無線LAN控制器(WLC)上使用LDAP的Web驗證組態範例 — Yahya Jaber和Ayman Alfares
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。