Configure WLC with LDAP Authentication for 802.1X & Web-Auth WLANs

Contents

Introduction

This document describes the procedure to configure an AireOS WLC in order to authenticate clients with a LDAP Server as the users database.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Microsoft Windows Servers
- Active Directory

Components Used

The information in this document is based on these software versions:

- Cisco WLC Software 8.2.110.0
- 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Technical Background

- LDAP is a protocol used to access directory servers.
- Directory servers are hierarchical, object oriented databases.
- Objects are organized in containers such as Organizational Units (OU), Groups, or default Microsoft Containers as CN=Users.
- The most difficult part of this setup is to configure the LDAP server parameters correctly on the WLC.

For more detailed information about these concepts, refer to the Introduction section of How to configure Wireless LAN Controller (WLC) for Lightweight Directory Access Protocol (LDAP) authentication.

Frequently Asked Questions

- What username must be used to bind with the LDAP Server?

There are two ways to bind against an LDAP Server, Anonymous or Authenticated (refer to in order to understand the difference between both methods).

This bind username needs to have Administrator privileges to be able to query for other usernames/passwords.

- If authenticated: is the bind username inside the same container than all users?

  No: use the whole path. For example:

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

  Yes: use the username only. For example:

  Administrator

- What if there are users are in different containers? Do all involved wireless LDAP users need to be in the same container?

No, a base DN that includes all the containers needed can be specified.

- What attributes must the WLC look for?

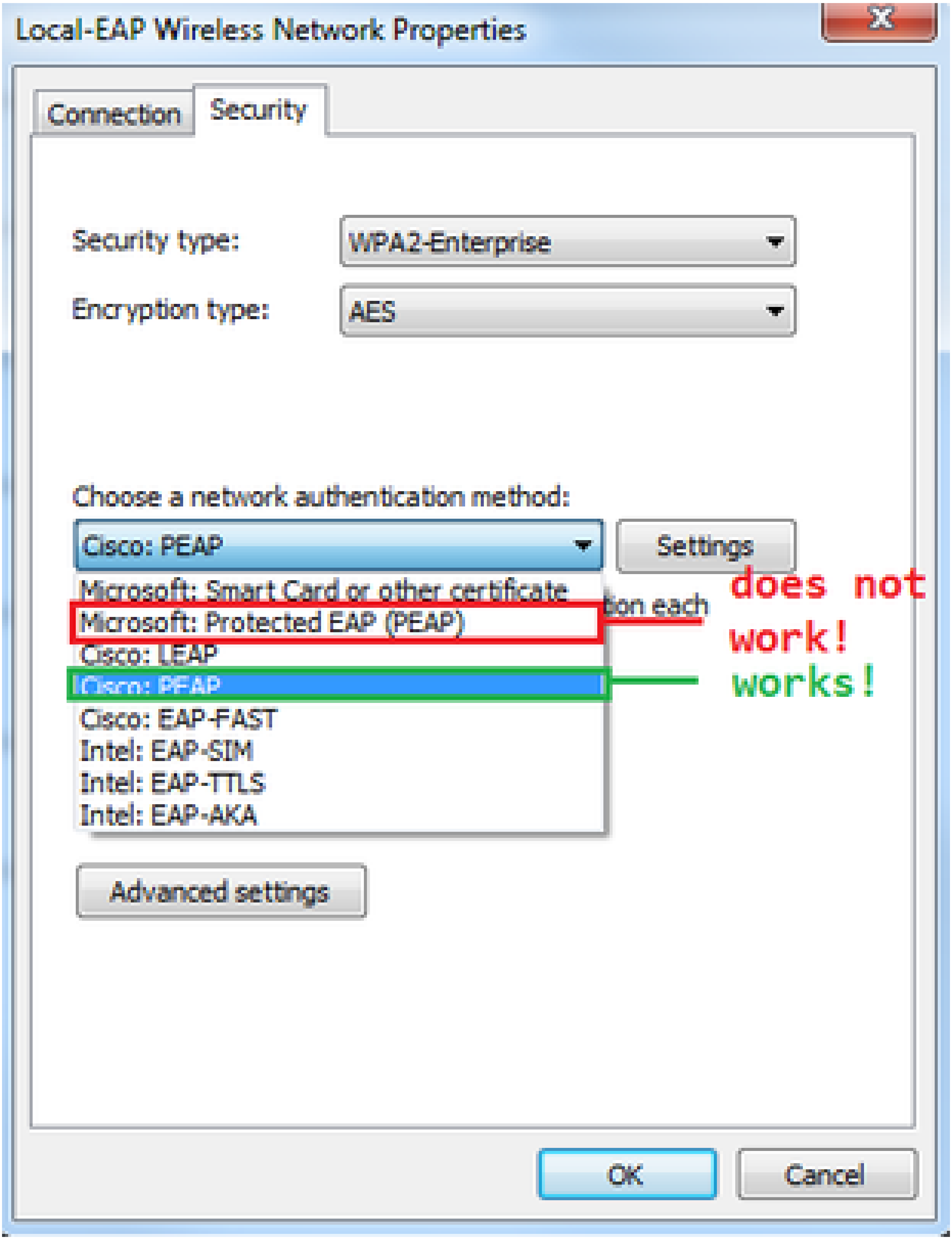
The WLC matches the User Attribute and Object Type specified.

Note: **sAMAccountName** is case sensitive but person is not. Therefore, **sAMAccountName=RICARDO** and **sAMAccountName=ricardo** are the same and works whereas **samaccountname=RICARDO** and **samaccountname=ricardo** does not.

- Which Extensible Authentication Protocol (EAP) methods can be used?

EAP-FAST, PEAP-GTC and EAP-TLS only. Android, iOS and MacOS default supplicants work with Protected Extensible Authentication Protocol (PEAP).

For Windows, Anyconnect Network Access Manager (NAM) or the default Windows supplicant with Cisco:PEAP must be used on supported wireless adapters as shown in the image.



Local-EAP Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: Cisco: PEAP

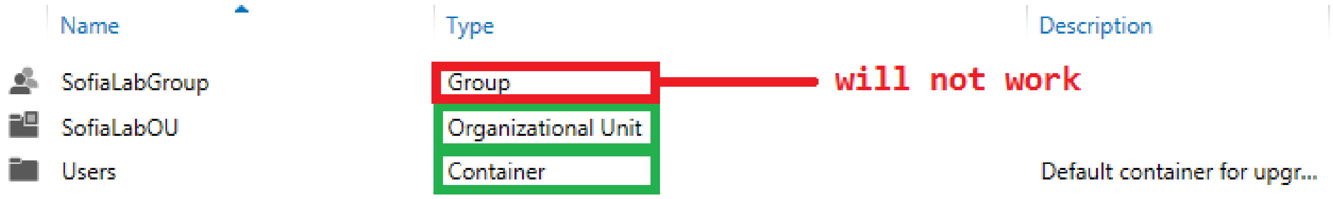
does not work!

works!

Note: The Cisco EAP Plug-ins for Windows include a version of Open Secure Socket Layer (OpenSSL 0.9.8k) that is affected by Cisco bug ID CSCva09670, Cisco does not plan to issue any more releases of the EAP Plug-ins for Windows, and recommends that customers instead use the AnyConnect Secure Mobility Client.

- Why can the WLC not find users?

Users inside a Group cannot be authenticated. They need to be inside a Default Container (CN) or an Organizational Unit (OU) as shown in the image.



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

will not work

Configure

There are different scenarios in which an LDAP server can be employed, either with 802.1x authentication or Web authentication.

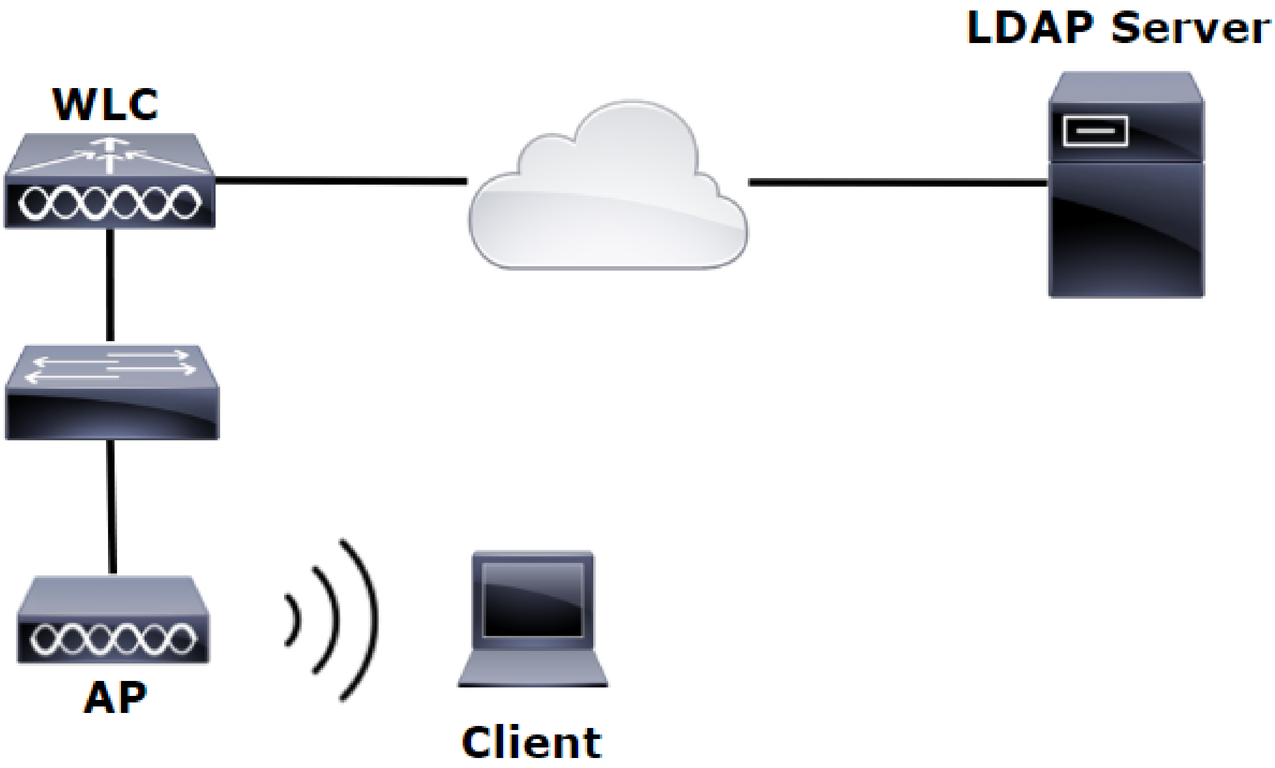
For this procedure, only users inside the OU=SofiaLabOU must be authenticated.

In order to learn how to use the Label Distribution Protocol (LDP) tool, configure and troubleshoot LDAP, refer to the WLC LDAP Configuration Guide.

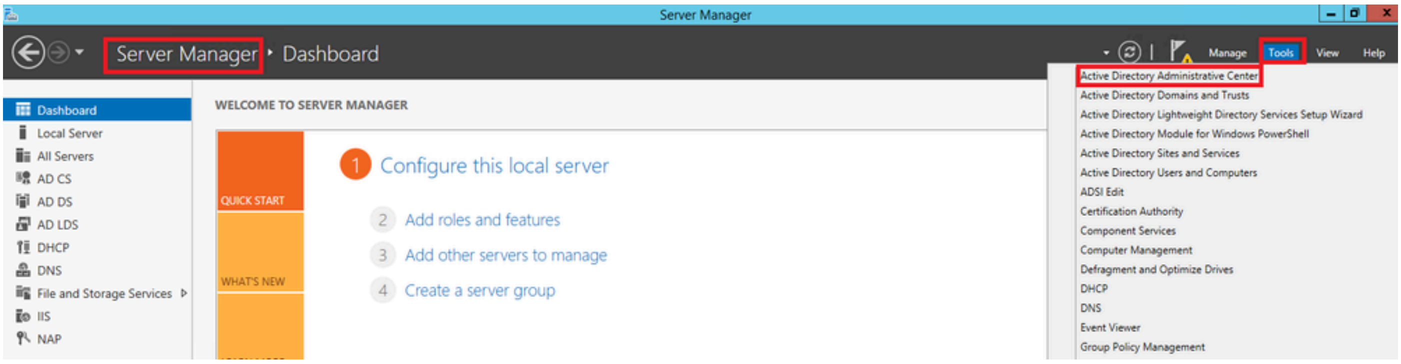
Create WLAN That Relies On LDAP Server To Authenticate Users Through 802.1x

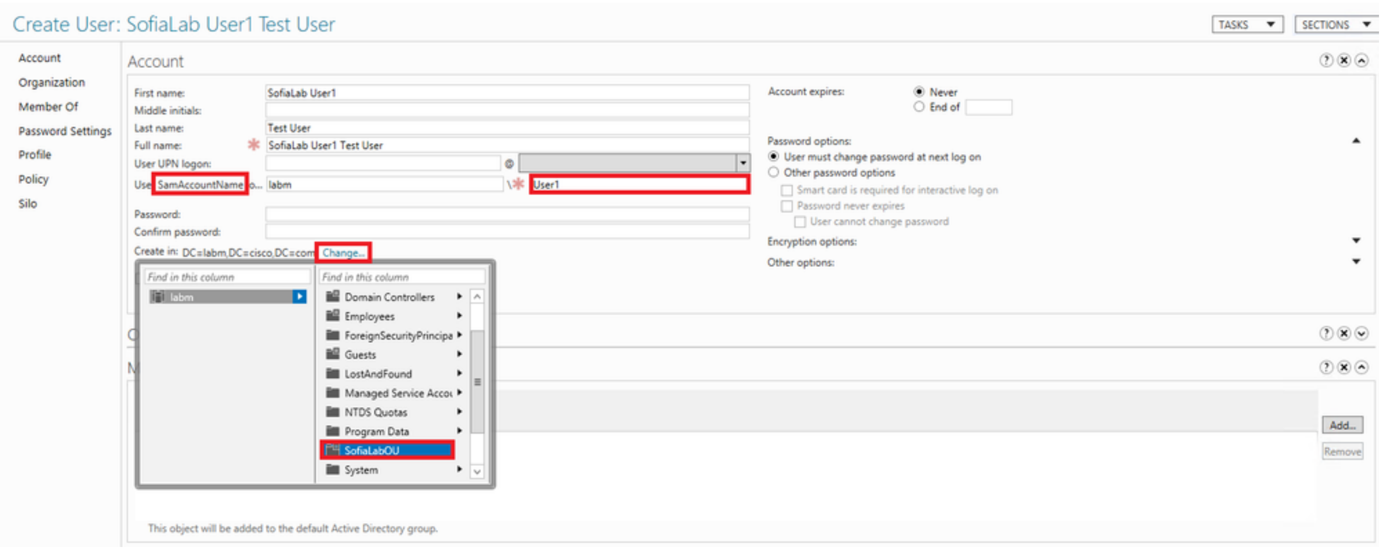
Network Diagram

In this scenario, WLAN LDAP-dot1x uses an LDAP Server to authenticate the users with the use of 802.1x.



Step 1. Create a user **User1** in the LDAP Server member of the SofiaLabOU and SofiaLabGroup.


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

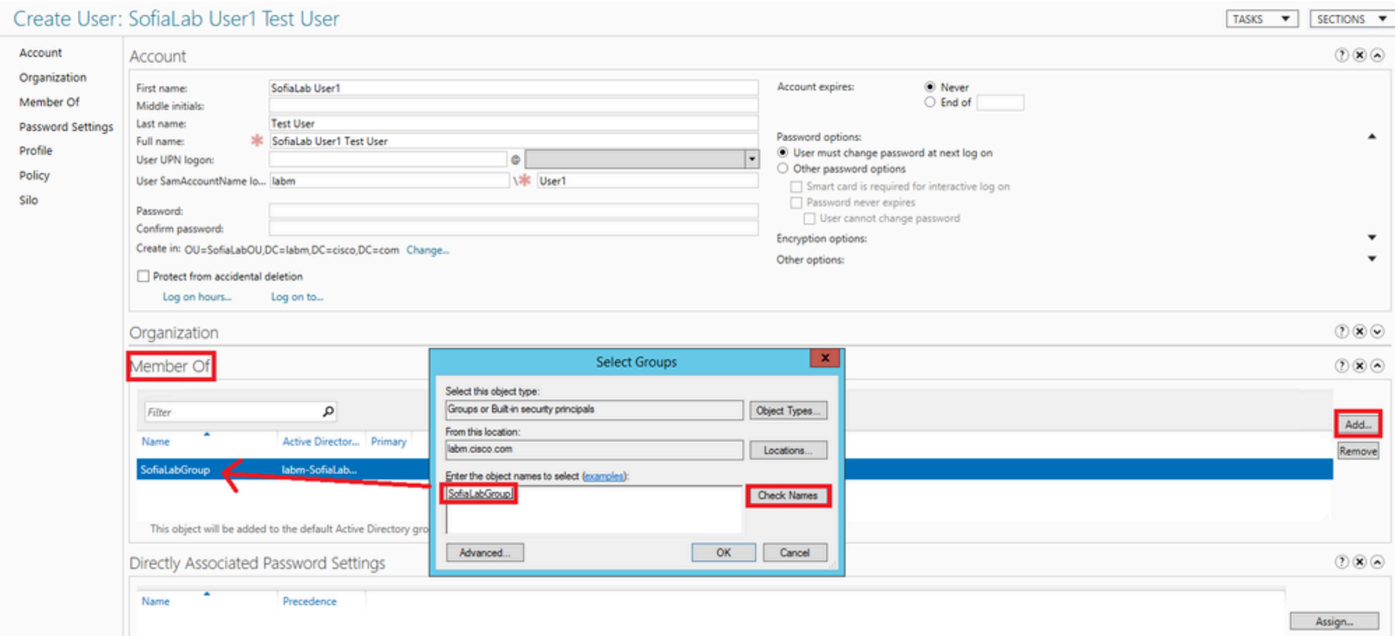
First name: SofiaLab User1
Middle initials:
Last name: Test User
Full name: * SofiaLab User1 Test User
User UPN logon: @
User SamAccountName lo... labm \ * User1
Password:
Confirm password:
Create in: DC=labm,DC=cisco,DC=com Change...

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

□ Protect from accidental deletion

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

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

This object will be added to the default Active Directory gro

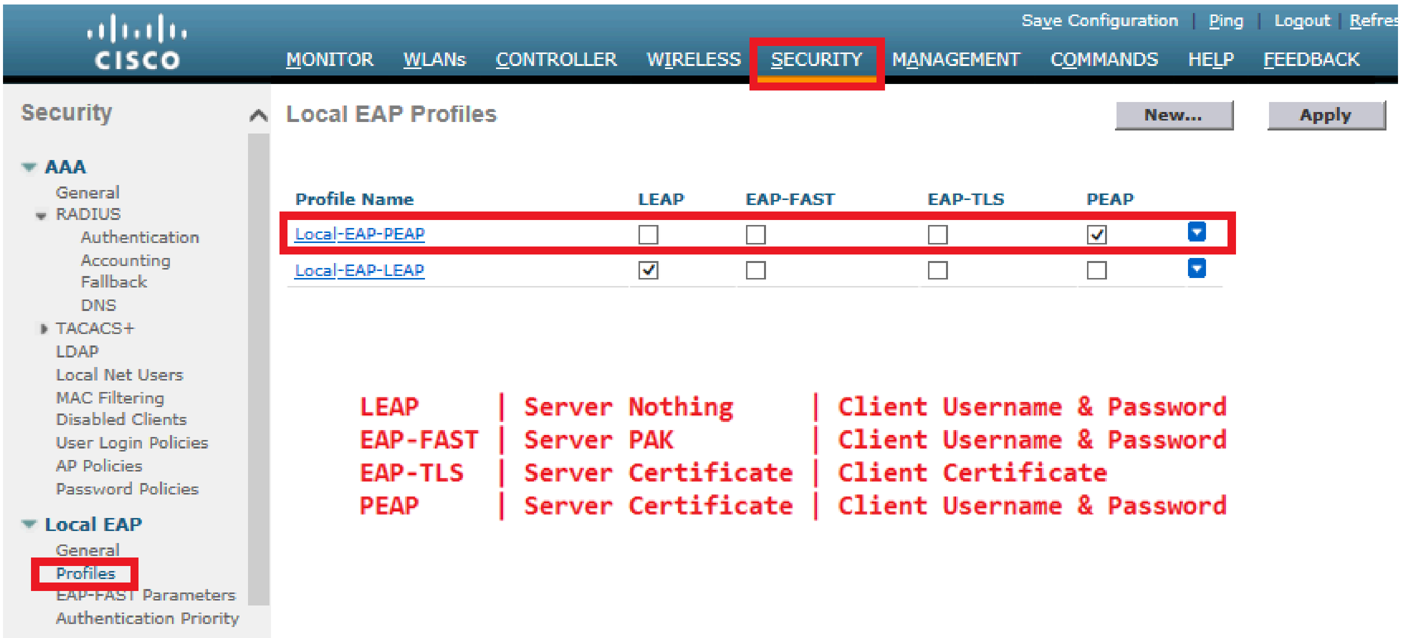
Select Groups

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

Step 2. Create an EAP Profile at the WLC with the desired EAP method (use PEAP).



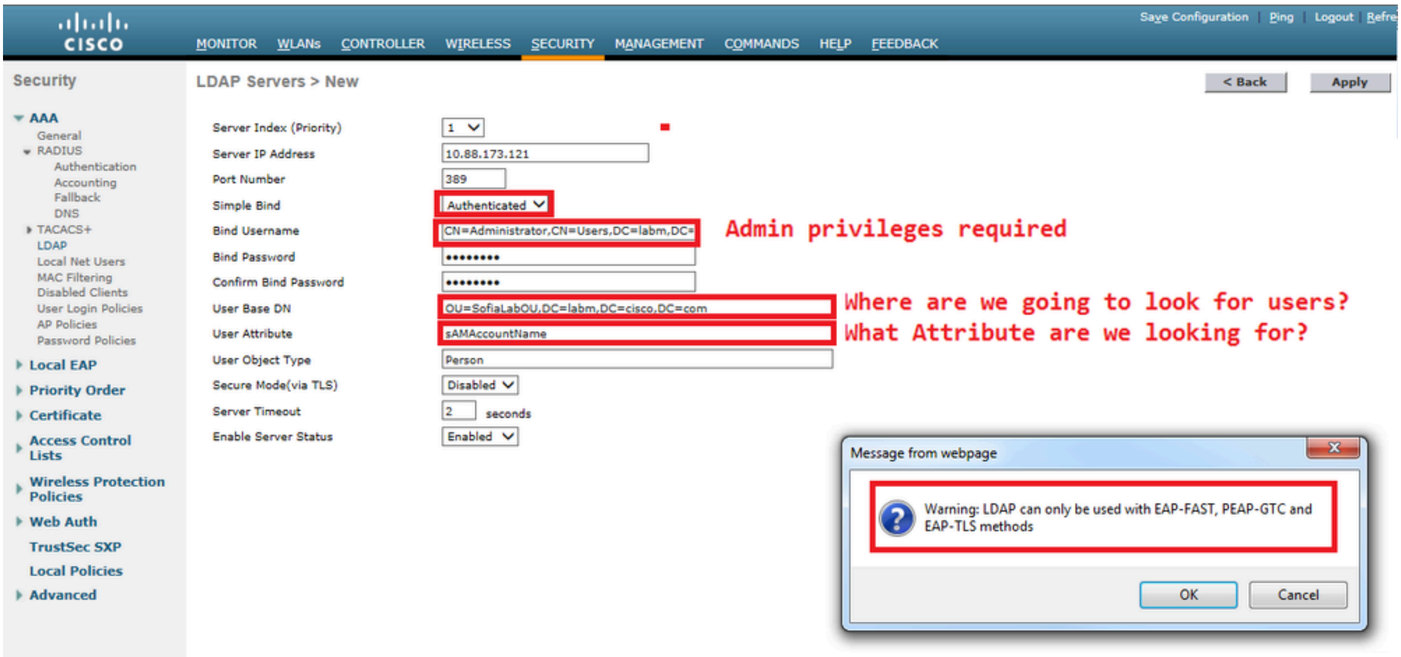
Local EAP Profiles

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

Step 3. Bind the WLC with the LDAP Server.

Tip: If the bind Username is not in the User Base DN, you have to write the entire path to the **Admin** user as shown in the image. Otherwise, you can simply enter **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

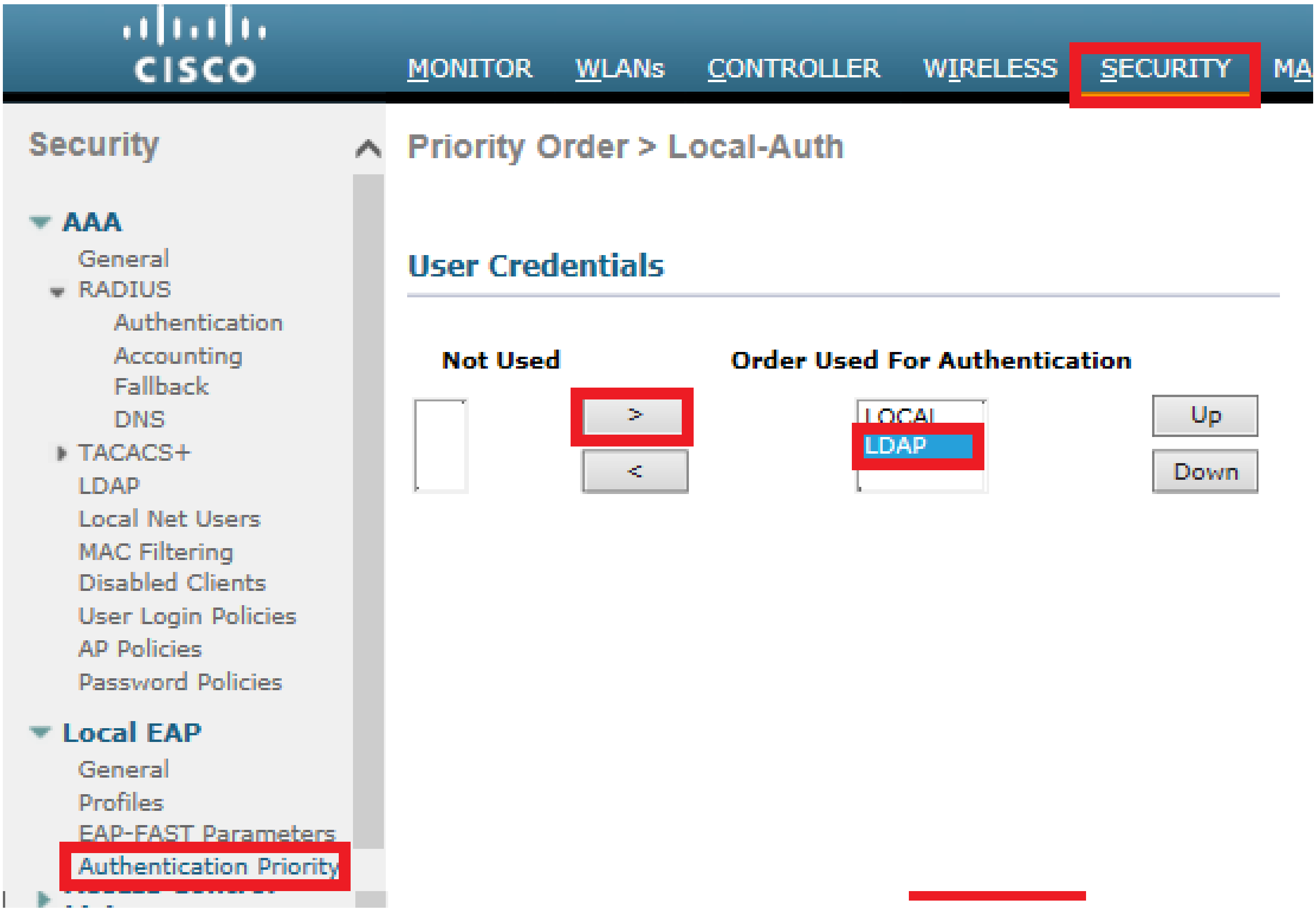
Where are we going to look for users?

What Attribute are we looking for?

Message from webpage

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

Step 4. Set the Authentication Order to be set to Internal Users + LDAP or LDAP only.



Priority Order > Local-Auth

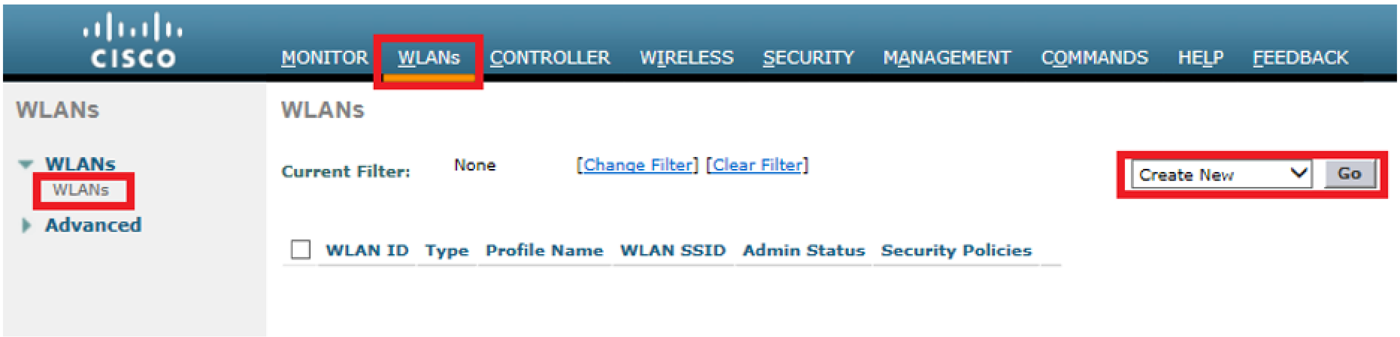
User Credentials

Not Used

Order Used For Authentication

LOCAL
LDAP

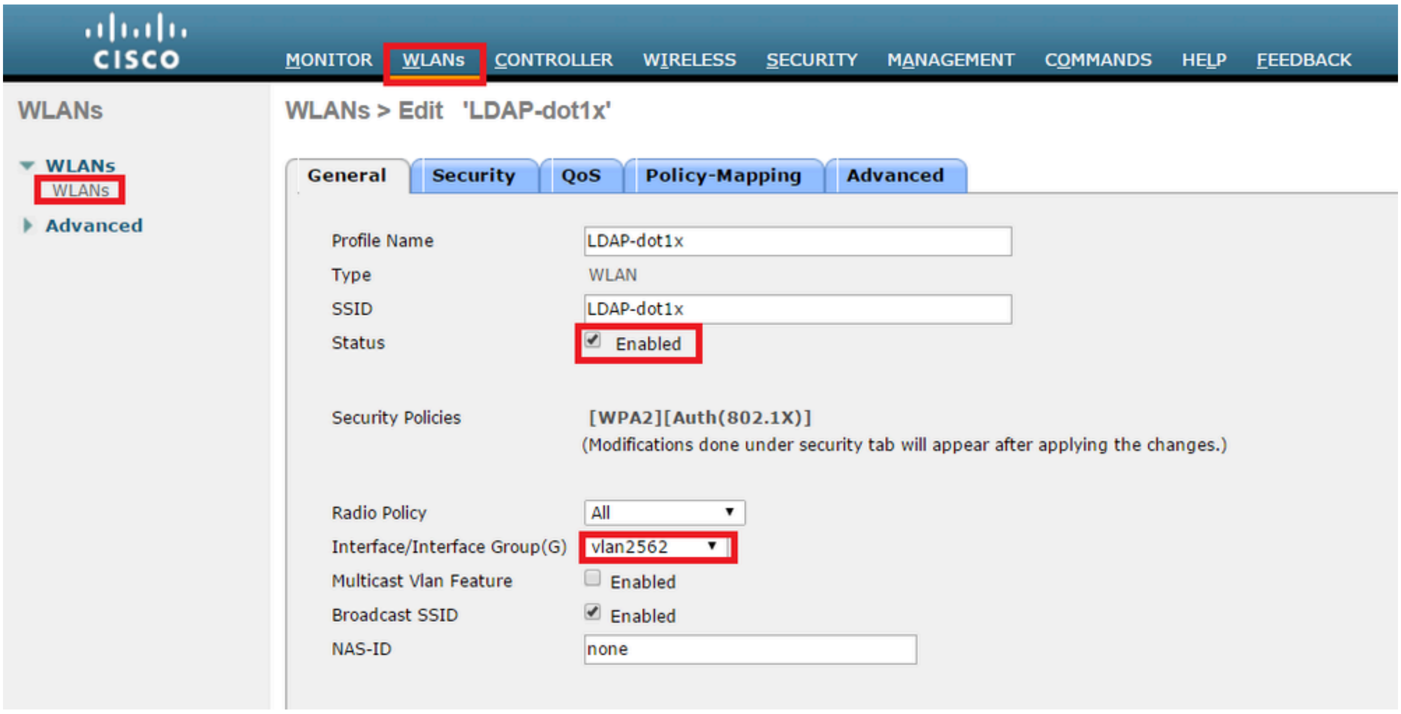
Step 5. Create the LDAP-dot1x WLAN.



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

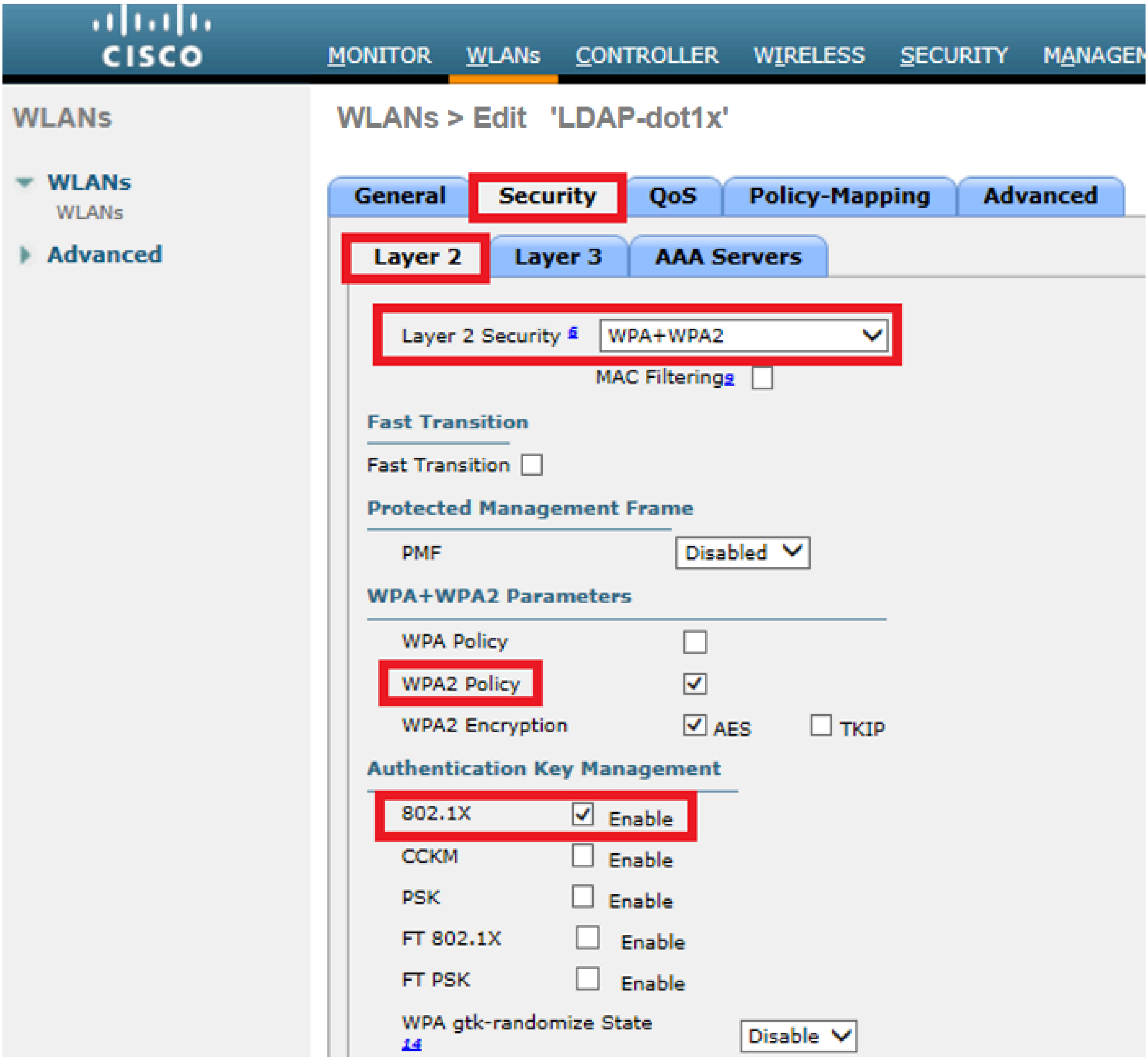
Interface/Interface Group(G): vlan2562

Multicast Vlan Feature: □ Enabled

Broadcast SSID: ☑ Enabled

NAS-ID: none

Step 6. Set the L2 security method to WPA2 + 802.1x and set L3 security to none.


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEM
WLANs
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers

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

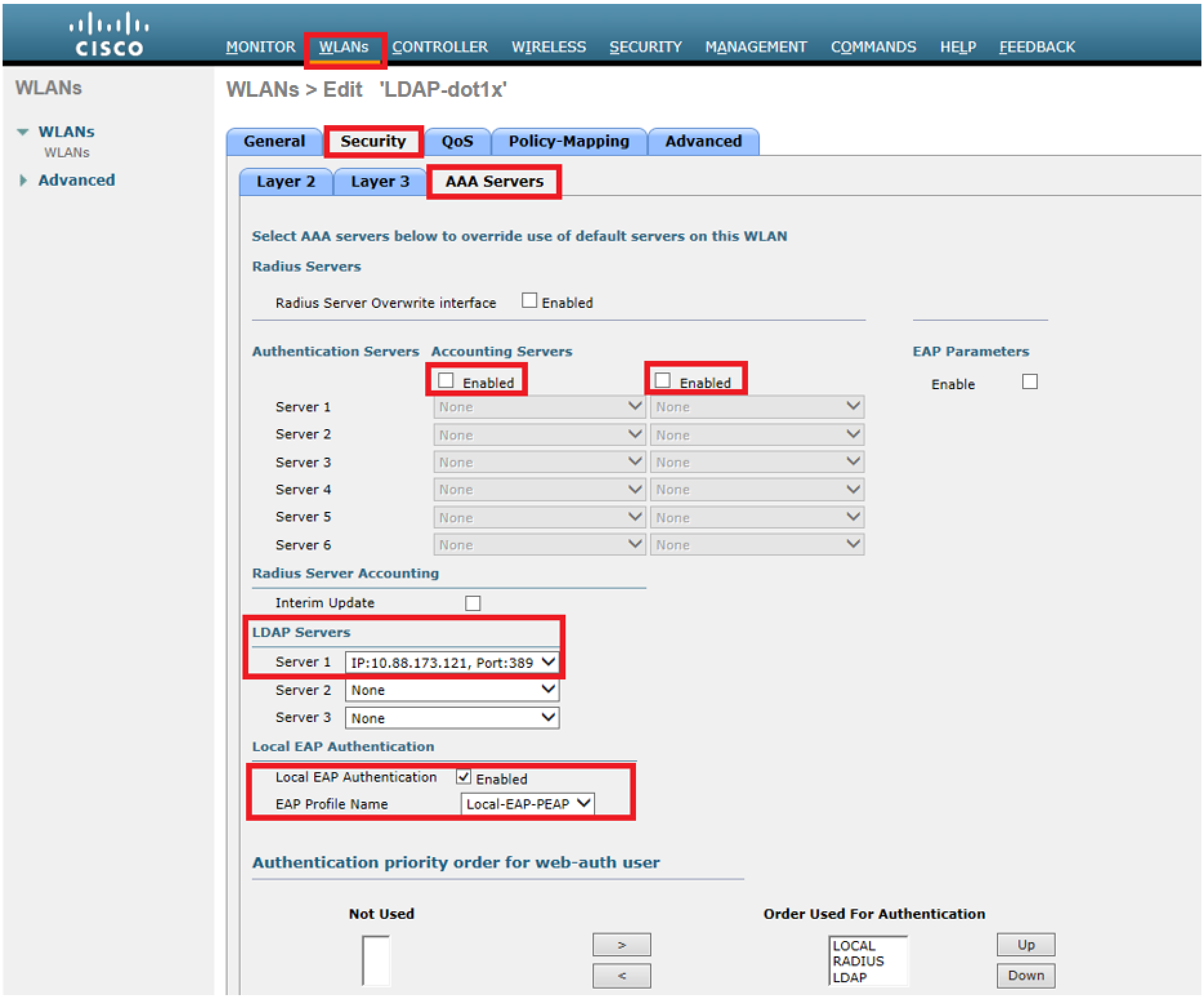
PSK □ Enable

FT 802.1X □ Enable

FT PSK □ Enable

WPA gtk-randomize State 14 Disable

Step 7. Enable local EAP Authentication and ensure Authentication Servers and Accounting Servers options are disabled and LDAP is enabled.



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
	□ 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

EAP Parameters

Enable □

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

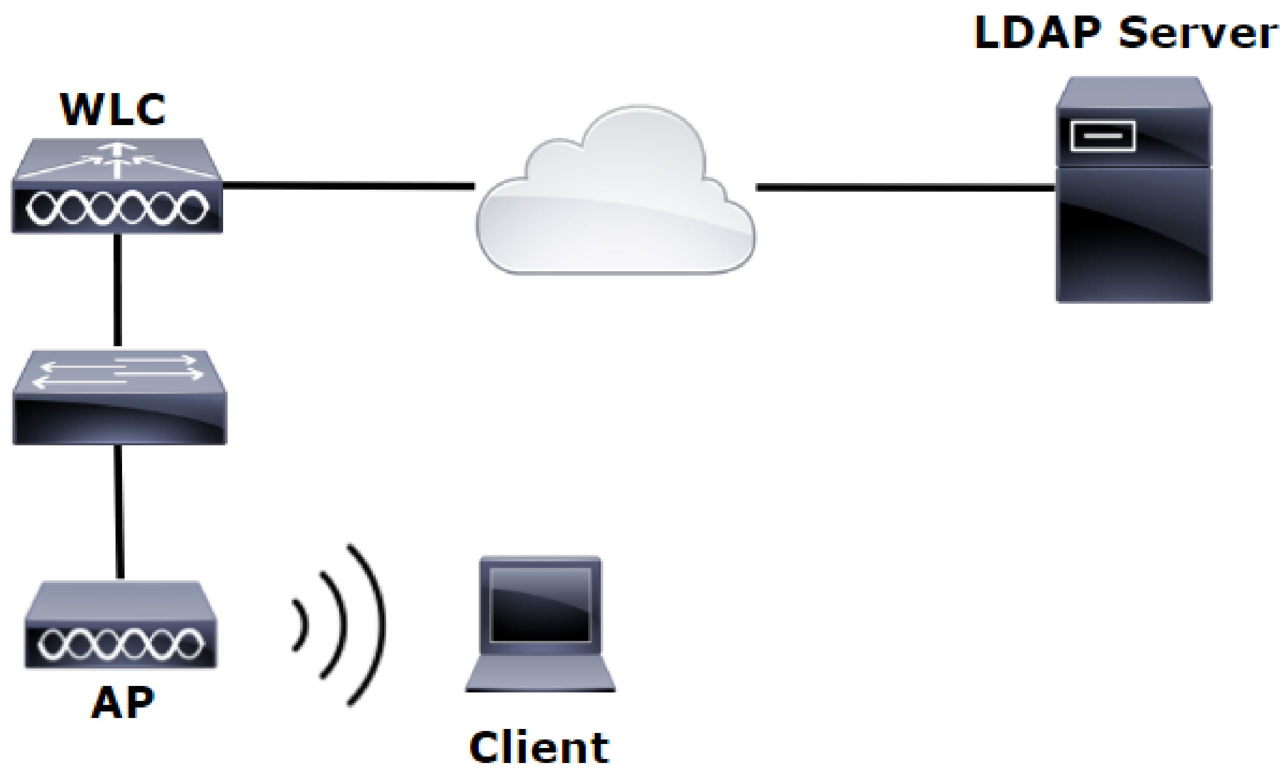
All other settings can be left at defaults.

Notes:
Use the LDP tool to confirm the configuration parameters.
The Search Base cannot be a Group (such as SofiaLabGroup).
PEAP-GTC or Cisco:PEAP have to be used instead of Microsoft:PEAP at the supplicant if it is a Windows Machine. Microsoft:PEAP works by default with MacOS/iOS/Android.

Create WLAN that Relies on LDAP Server to Authenticate Users through Internal WLC Web Portal

Network Diagram

In this scenario, WLAN LDAP-Web uses an LDAP server to authenticate the users with the internal WLC Web Portal.



Ensure Steps 1. through Steps 4. have been taken from the previous example. From there, the WLAN configuration is set differently.

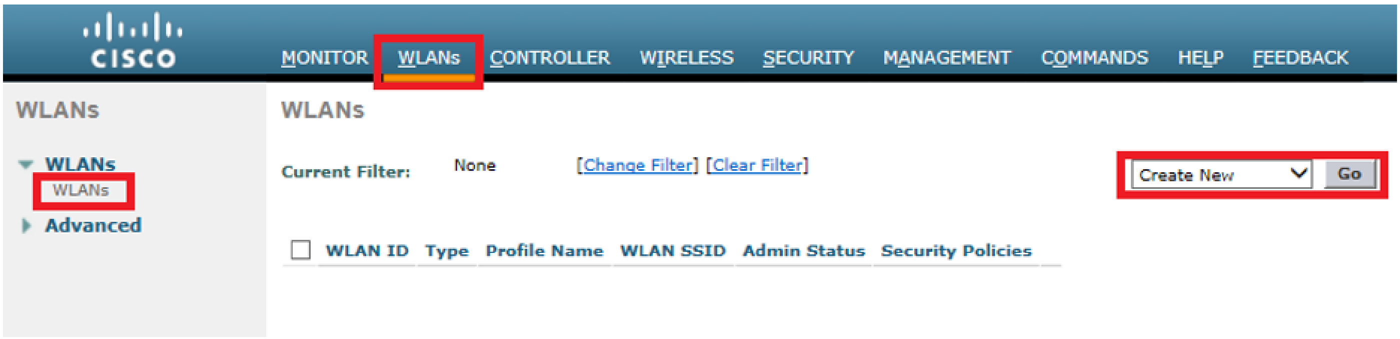
Step 1. Create a user **User1** in the LDAP Server member of the OU SofiaLabOU and the Group SofiaLabGroup.

Step 2. Create an EAP Profile at the WLC with the desired EAP method (use PEAP).

Step 3. Bind the WLC with the LDAP Server.

Step 4. Set the Authentication Order to be set to Internal Users + LDAP.

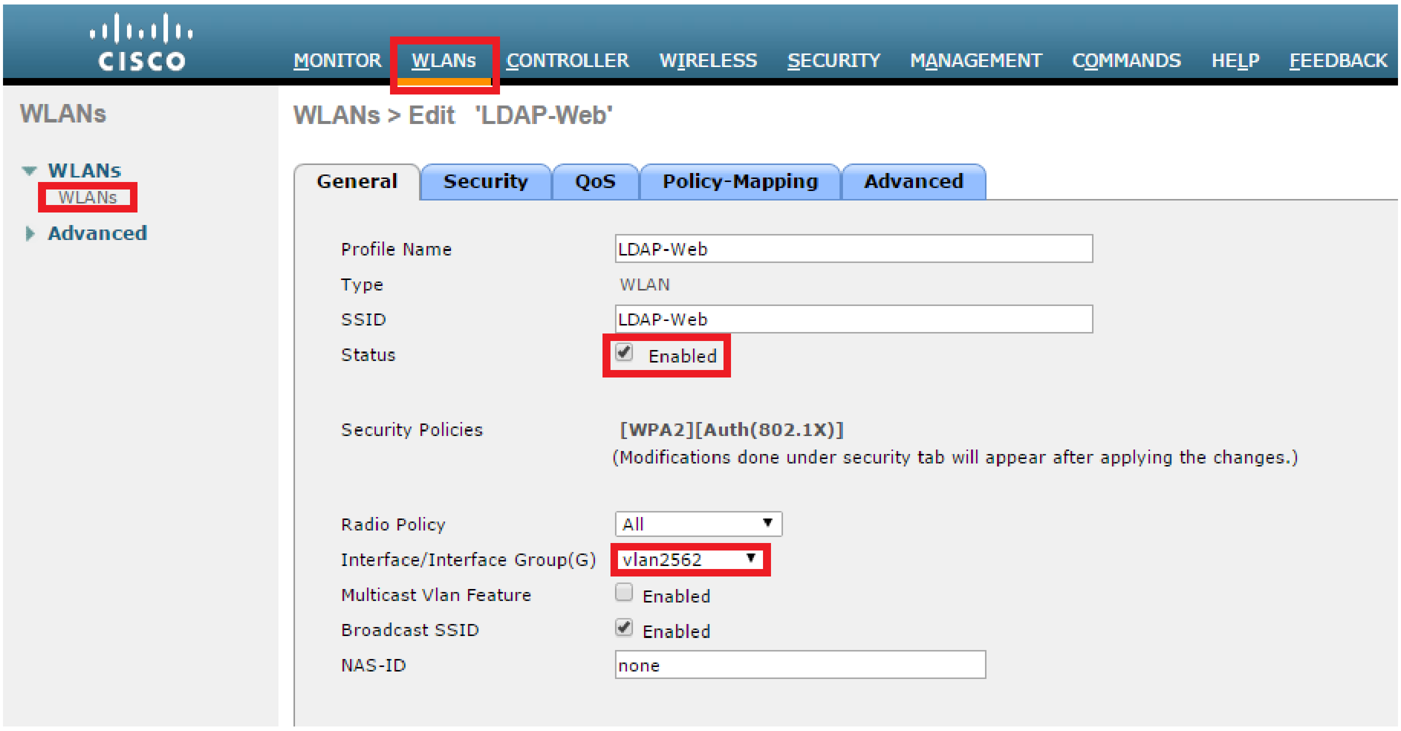
Step 5. Create the LDAP-Web WLAN as shown in the images.



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

Create New Go

□	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

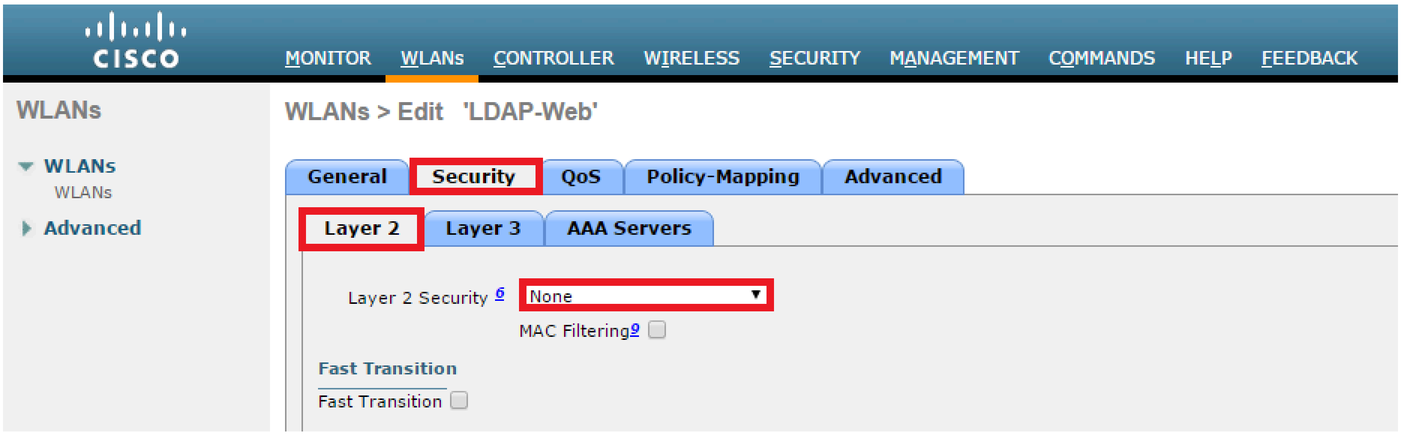
Interface/Interface Group(G): vlan2562

Multicast Vlan Feature: □ Enabled

Broadcast SSID: ☑ Enabled

NAS-ID: none

Step 6. Set L2 Security to none and L3 Security to Web Policy – Authenticationas shown in the images.



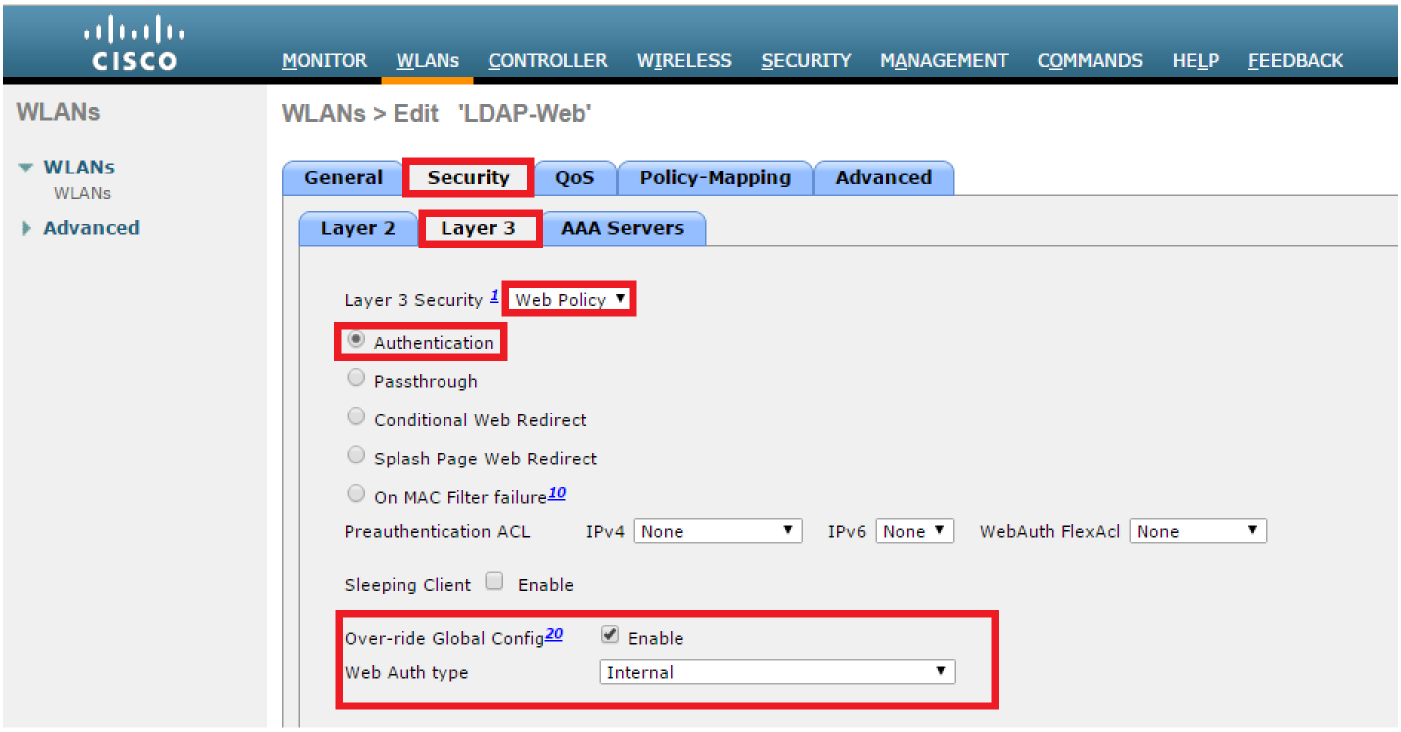
WLANs > Edit 'LDAP-Web'

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]

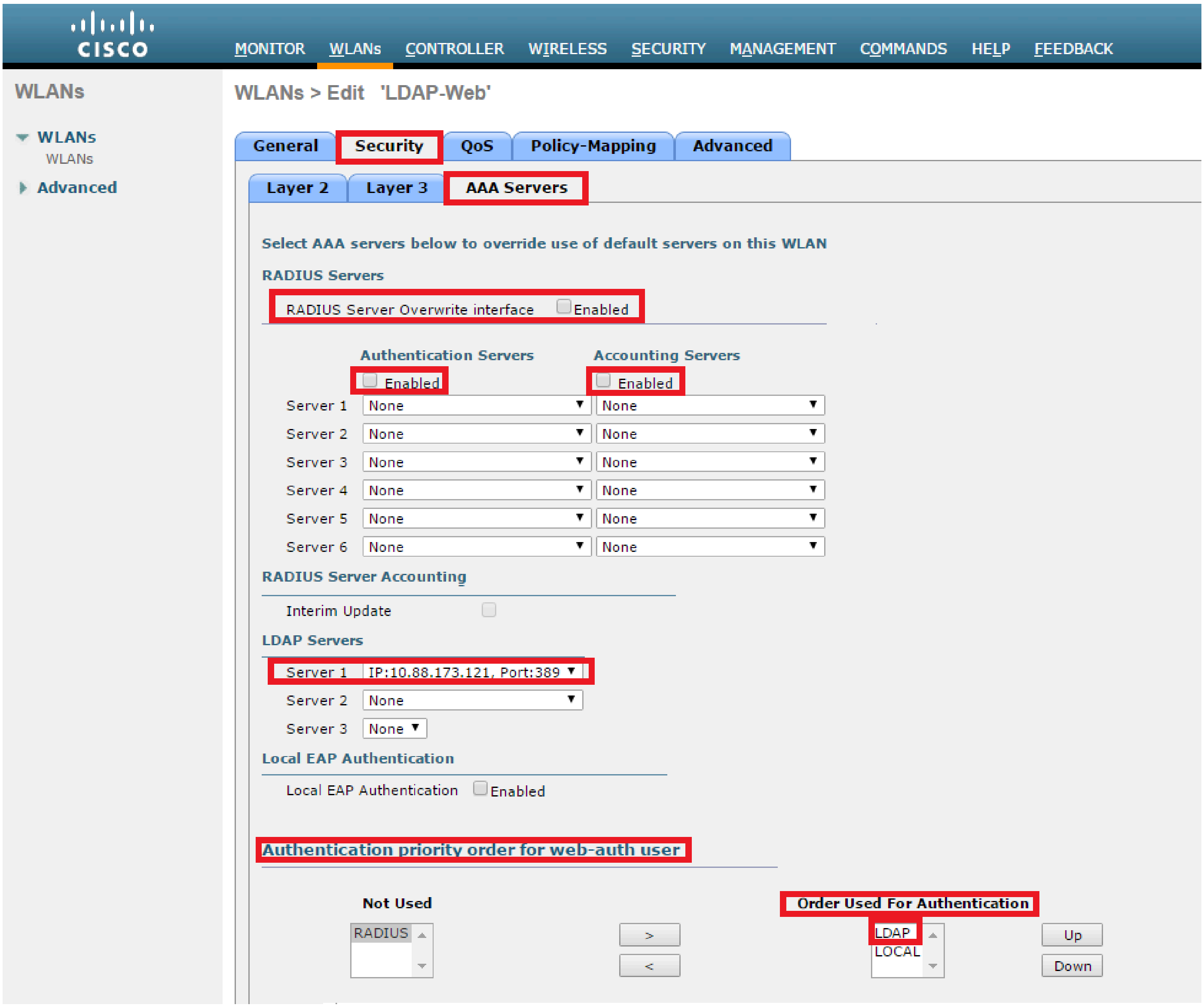
Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

Sleeping Client □ Enable

Over-ride Global Config[20] ☑ Enable

Web Auth type Internal

Step 7. Set the Authentication priority order for web-auth to use LDAP and ensure Authentication Servers and Accounting Servers options are disabled.



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

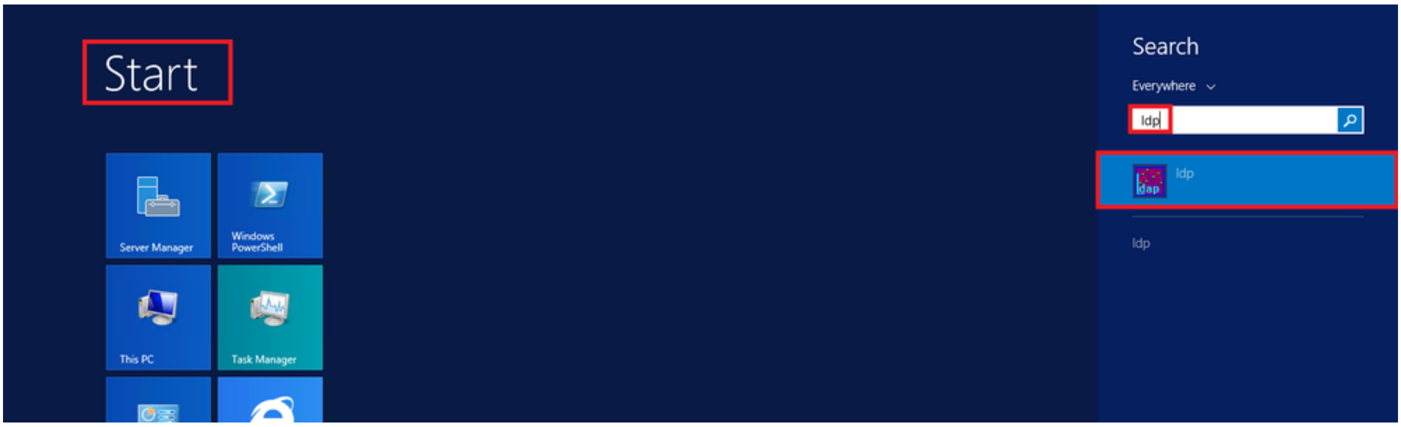
Authentication priority order for web-auth user

Not Used	Order Used For Authentication
RADIUS	LDAP LOCAL

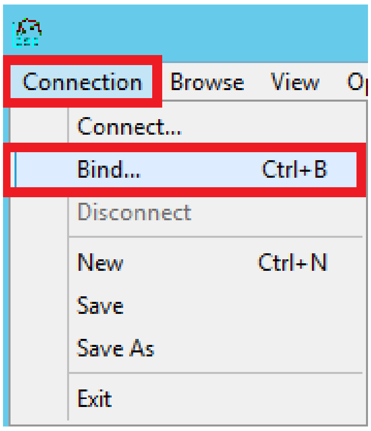
All other settings can be left at defaults.

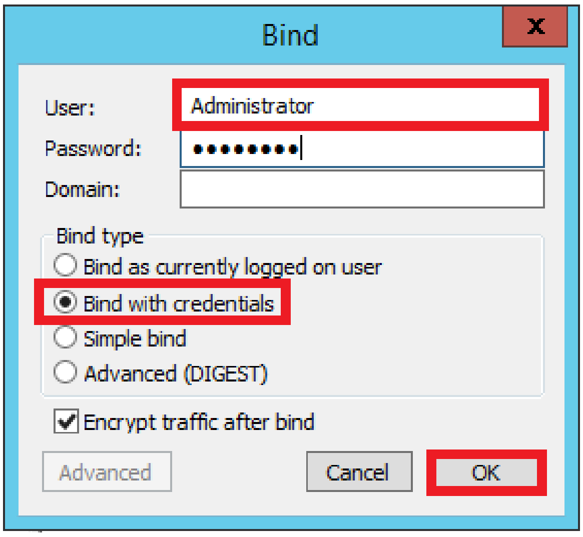
Use LDP Tool to Configure and Troubleshoot LDAP

Step 1. Open the LDP tool either at the LDAP server or at a host with connectivity (Port TCP 389 must be allowed to the server).



Step 2. Navigate to **Connection** > **Bind,** log in with an Admin user and select **Bind with credentials** radio button.




Bind

User: Administrator

Password: ••••••••

Domain:

Bind type

○ Bind as currently logged on user

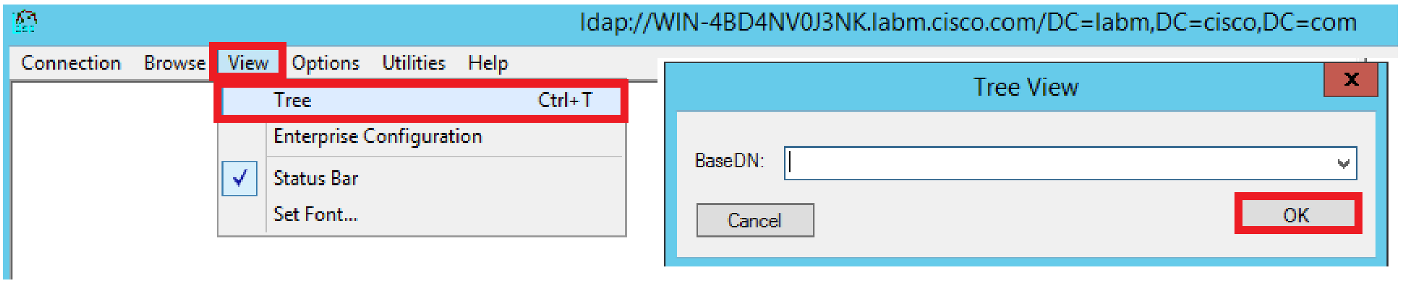
● Bind with credentials

○ Simple bind

○ Advanced (DIGEST)

☑ Encrypt traffic after bind

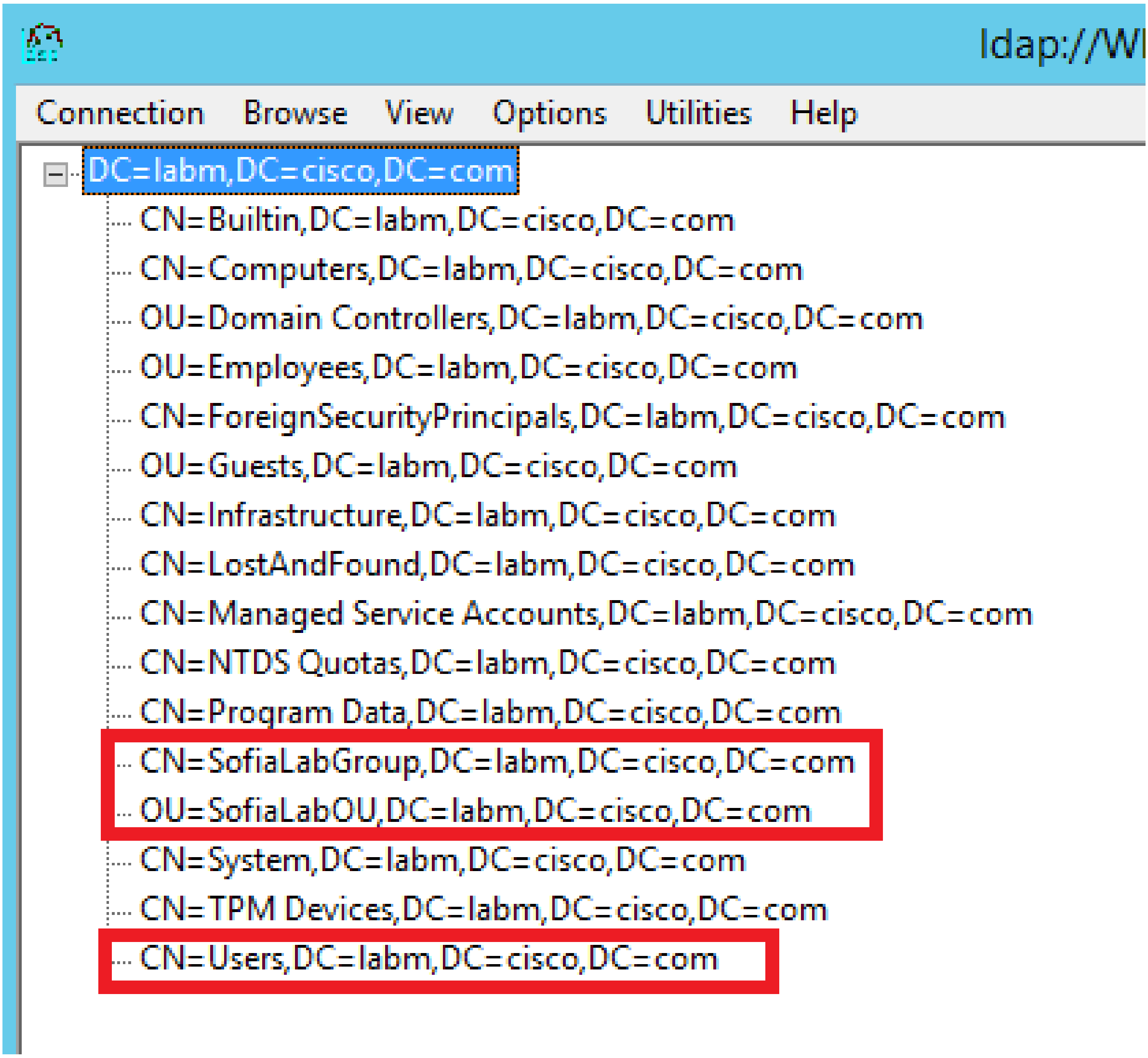
Step 3. Navigate to **View** > **Tree** and select **OK** in the base DN.


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

Tree View

BaseDN:

Step 4. Expand the tree to view the structure and look for the Search Base DN. Consider that it can be any container type except Groups. It can be the whole domain, a specific OU or a CN like CN=Users.



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

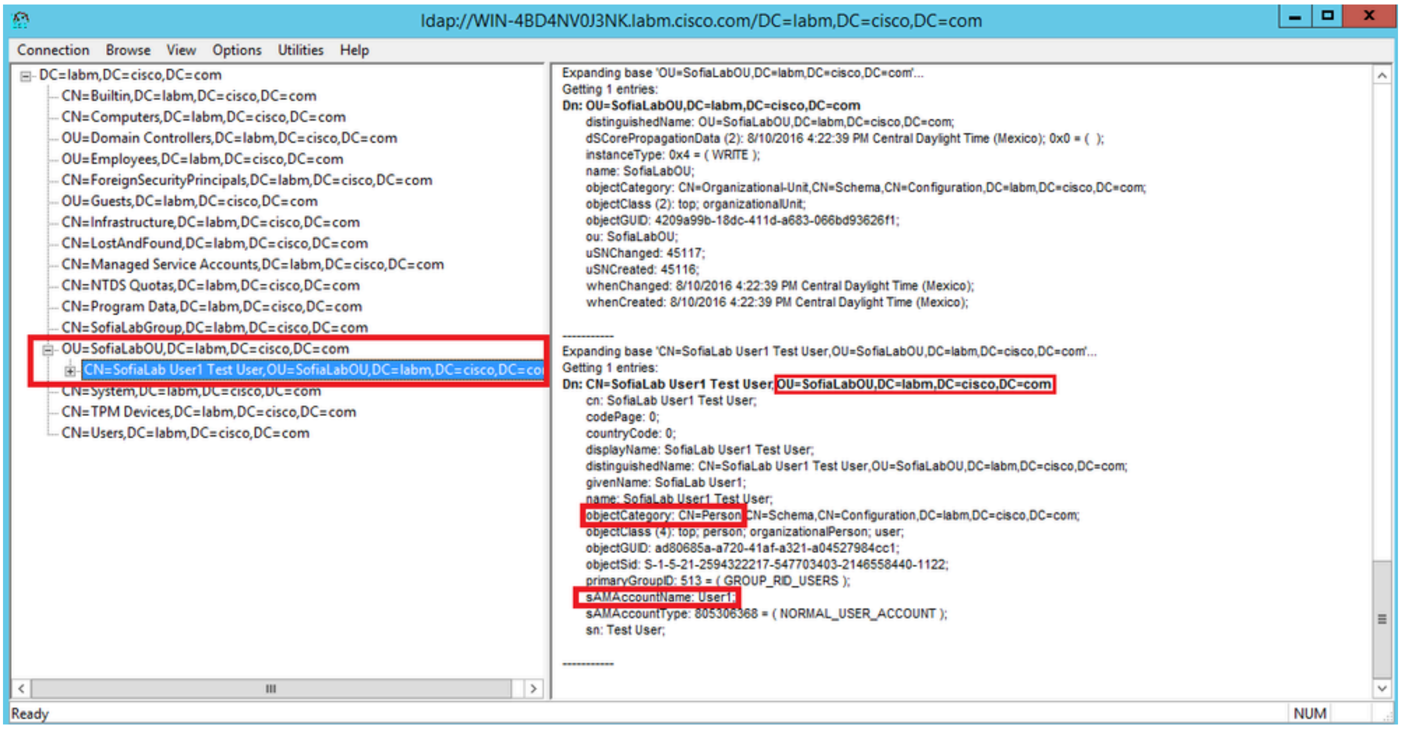
OU=SofiaLabOU,DC=labm,DC=cisco,DC=com

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

Step 5. Expand the SofiaLabOU in order to see which users are inside of it. There is the User1 that was created before.


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

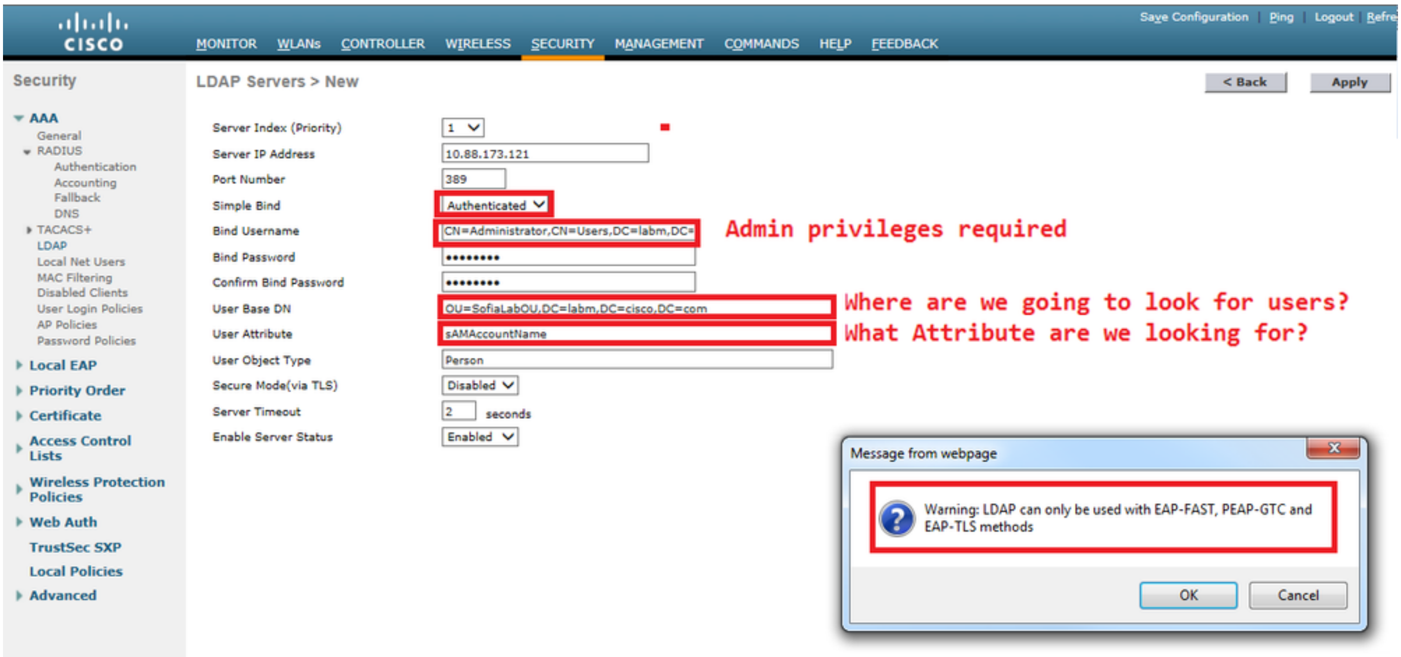
```
DC=labm,DC=cisco,DC=com
    CN=Builtin,DC=labm,DC=cisco,DC=com
    CN=Computers,DC=labm,DC=cisco,DC=com
    OU=Domain Controllers,DC=labm,DC=cisco,DC=com
    OU=Employees,DC=labm,DC=cisco,DC=com
    CN=ForeignSecurityPrincipals,DC=labm,DC=cisco,DC=com
    OU=Guests,DC=labm,DC=cisco,DC=com
    CN=Infrastructure,DC=labm,DC=cisco,DC=com
    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;

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

Step 6. Everything needed to configure LDAP.



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

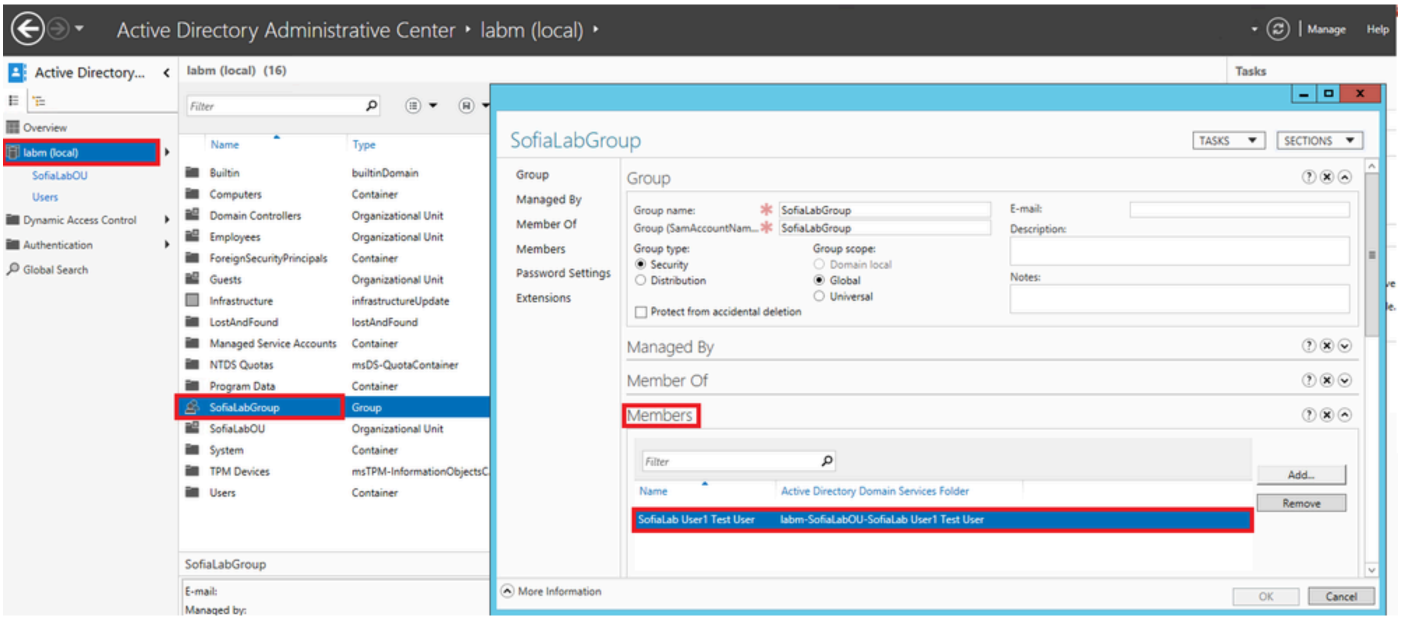
Where are we going to look for users?

What Attribute are we looking for?

Message from webpage

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

Step 7. Groups like SofiaLabGroup cannot be used as a search DN. Expand the group and look for the users inside it, where the User1 previously created must beas shown.



labm (local) (16)

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 was there but LDP was not able to find it. It means the WLC is not able to do it as well and which is why Groups are not supported as a Search Base DN.

Verify

Use this section to confirm that your configuration works properly.

```
 (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
```

Troubleshoot

This section provides information you can use to troubleshoot your 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
```

Related Information

- LDAP - WLC 8.2 Configuration Guide
- How to configure Wireless Lan Controller (WLC) for Lightweight Directory Access Protocol (LDAP) authentication - by Vinay Sharma
- Web Authentication Using LDAP on Wireless LAN Controllers (WLCs) Configuration Example - by Yahya Jaber and Ayman Alfares
- Cisco Technical Support & Downloads