Document on authenticating guest user via Active Directory server using LDAP protocol where portal mode is internal AP

Introduction

This document describes how to configure cnPilot Hotspot or E series device for web authentication using Active Directory (AD) server via LDAP.

Note: This feature is available from 3.0-b24 beta release build.

Devices used to explain the feature

Client device	: Mobile phone
Access Point	: Cambium Networks E600 Access point
Active Directory	: Windows 2008 server

Configure LDAP Server

The first step is to configure the LDAP server, which serves as a backend database to store user credentials of the wireless clients. In this example, the Microsoft Windows 2008R2 server is used as the LDAP server.

Create Users on the Domain Controller

Step1 : Create an Organizational Unit (OU) which can contain multiple groups that carry multiple users

Step2 : Create a group inside the organizational unit

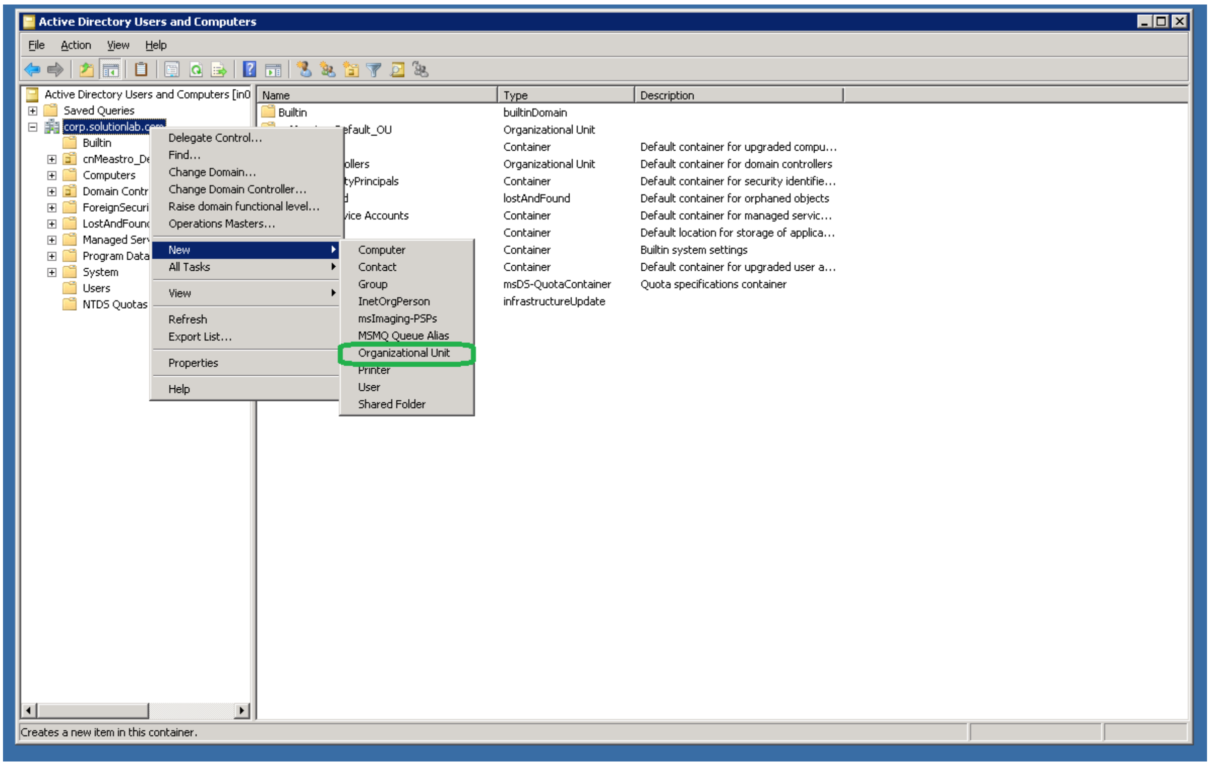
Step3 : Create a user and add the user to the group

In this example, a new OU “Test_Ldap” is created, and group “Test_Group_LdapTest” is created inside this OU. A user named “anand” is created, and added to the “Test_Group_Ldap”.

Note: The domain used in this example is corp.solutionlab.com

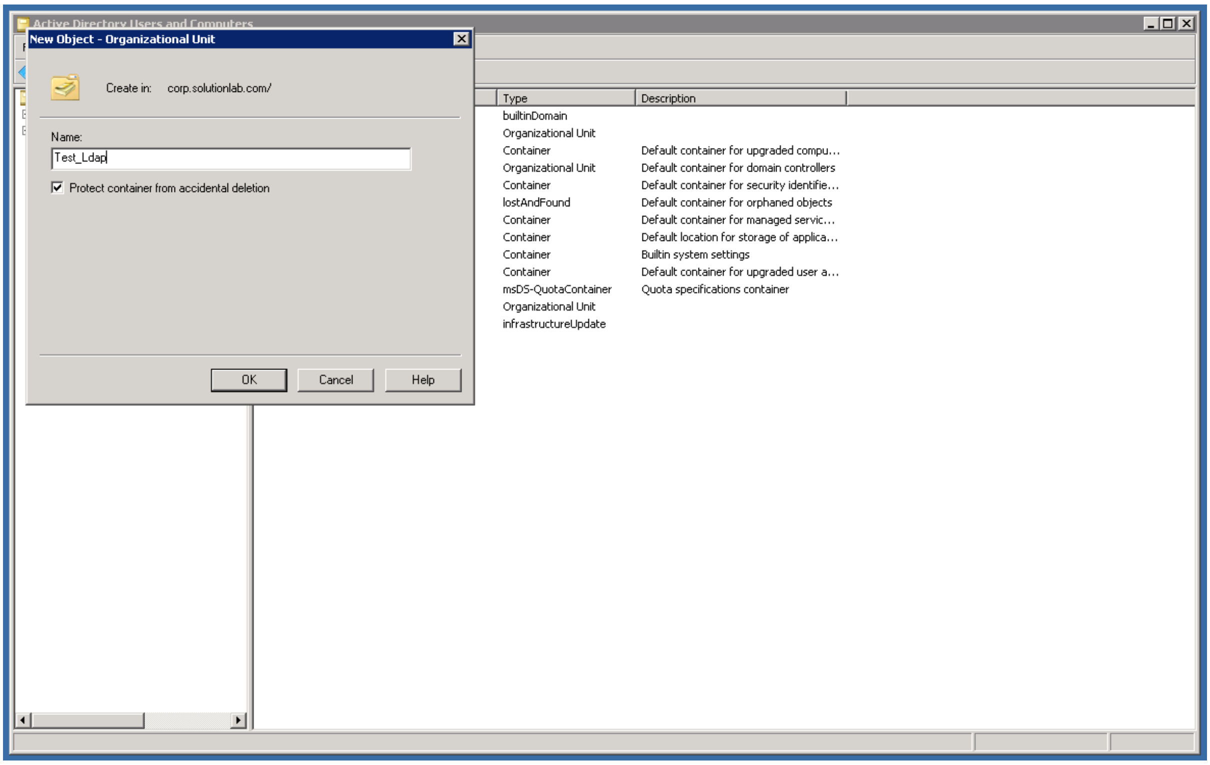
Attaching the screenshot for the steps described

Screenshot details are explained at the bottom of the screenshot



Name	Type	Description
Builtin	builtinDomain	
efault_OU	Organizational Unit	
	Container	Default container for upgraded compu…
ollers	Organizational Unit	Default container for domain controllers
tyPrincipals	Container	Default container for security identifie…
d	lostAndFound	Default container for orphaned objects
ice Accounts	Container	Default container for managed servic…
	Container	Default location for storage of applica…
	Container	Builtin system settings
	Container	Default container for upgraded user a…
	msDS-QuotaContainer	Quota specifications container
	infrastructureUpdate	

Right click on corp.solutions.com domain name to create an OU


Active Directory Users and Computers
New Object - Organizational Unit
OK
Cancel
Help

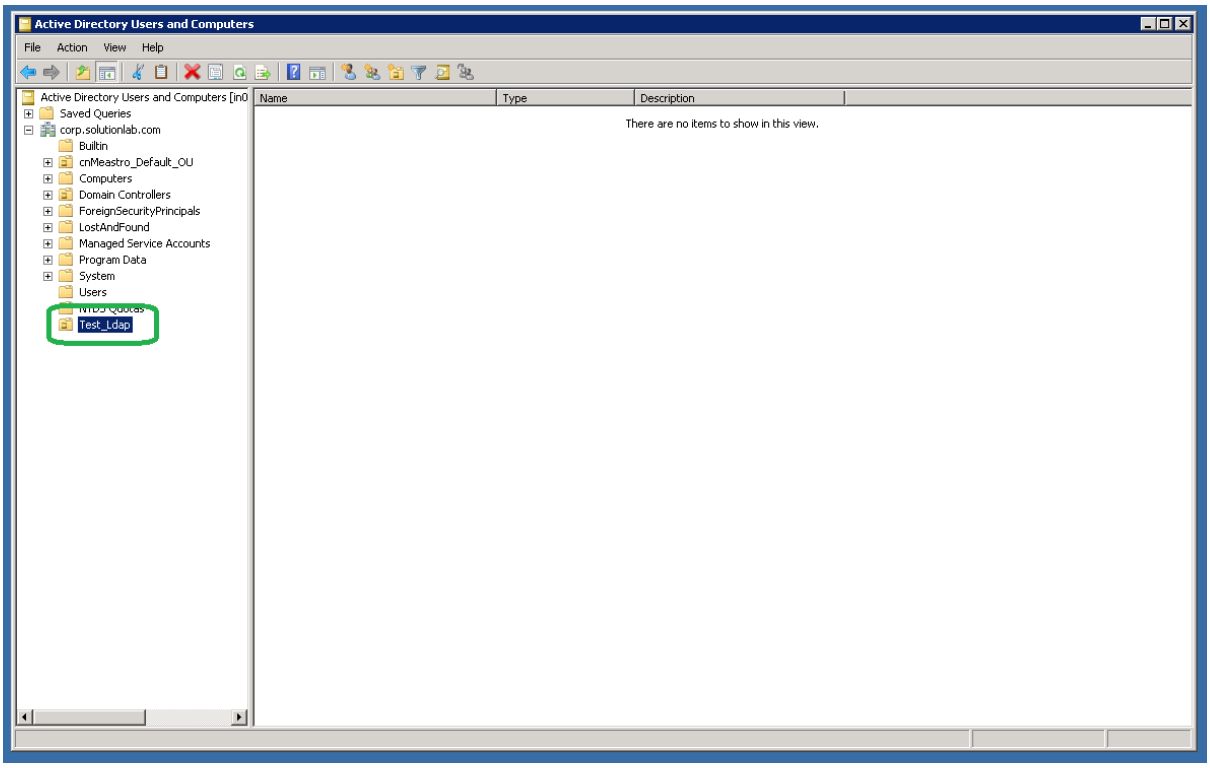
Create in: corp.solutionlab.com/

Name:
Test_Ldap

☑ Protect container from accidental deletion

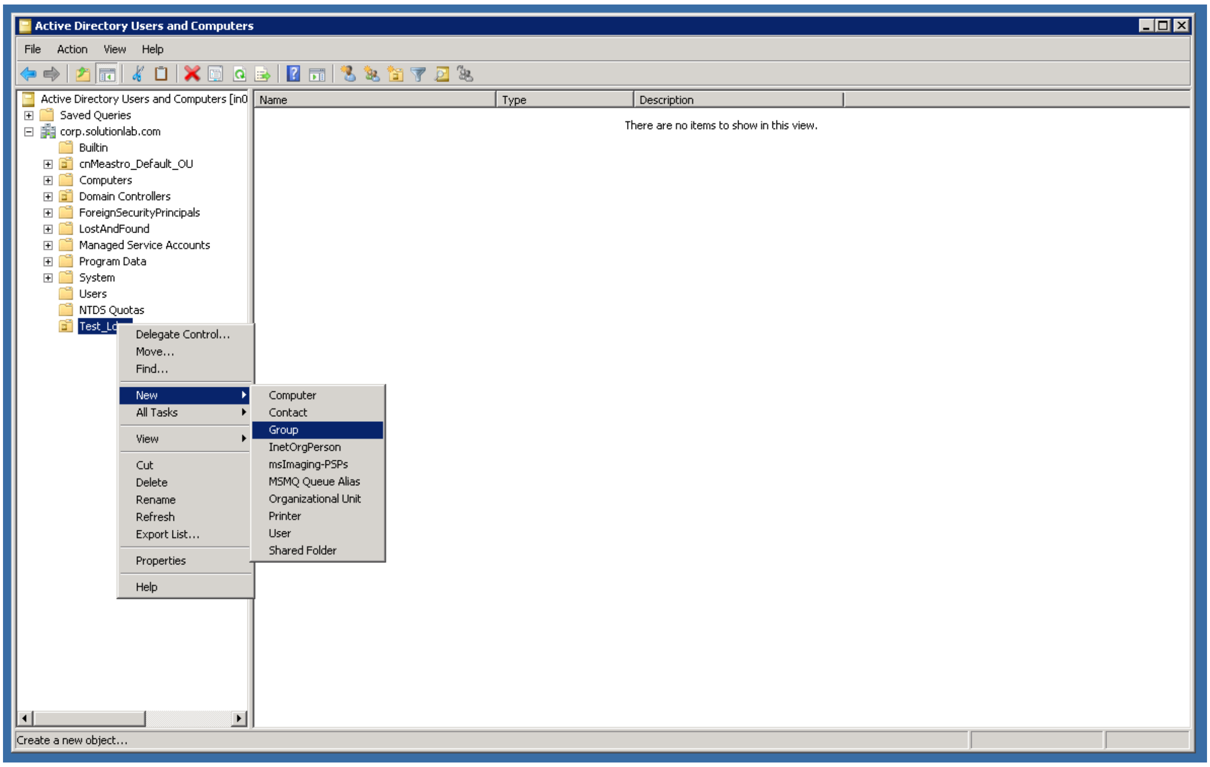
Type	Description
builtinDomain	
Organizational Unit	
Container	Default container for upgraded compu…
Organizational Unit	Default container for domain controllers
Container	Default container for security identifie…
lostAndFound	Default container for orphaned objects
Container	Default container for managed servic…
Container	Default location for storage of applica…
Container	Builtin system settings
Container	Default container for upgraded user a…
msDS-QuotaContainer	Quota specifications container
Organizational Unit	
infrastructureUpdate	

Enter the organizational name and click on OK



There are no items to show in this view.

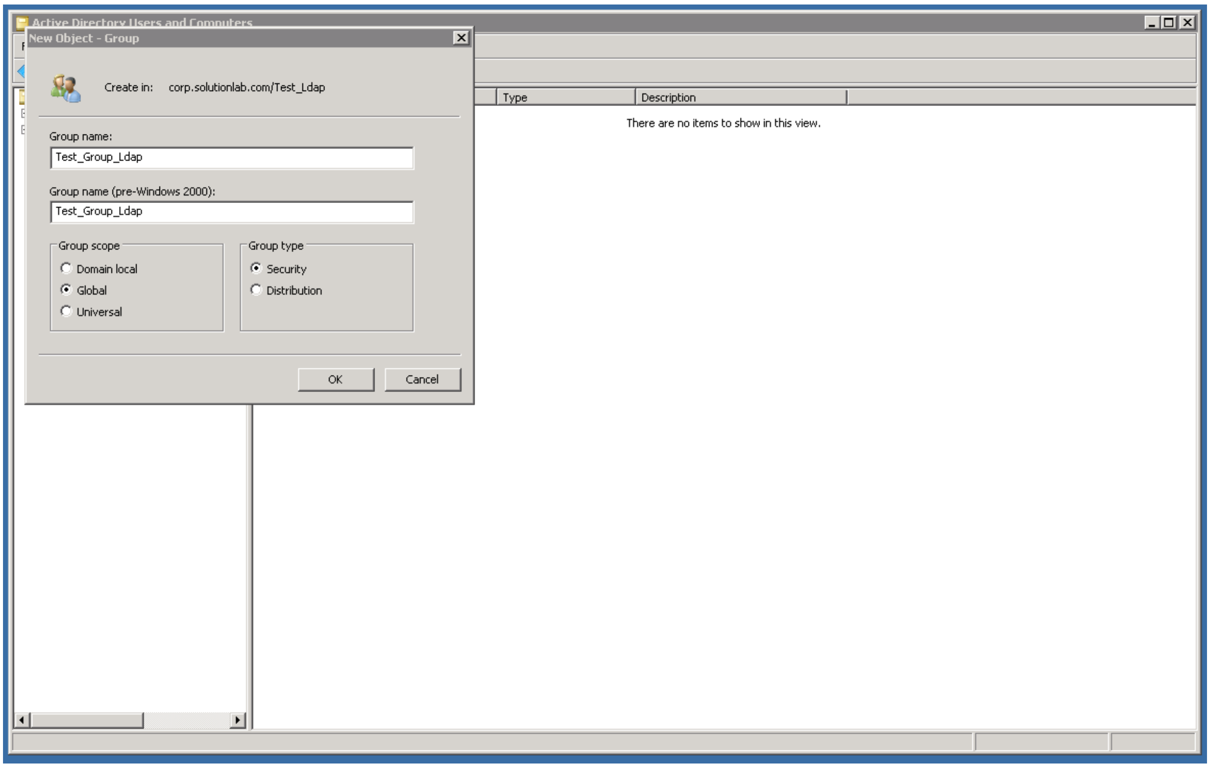
Test_Ldap OU is now created



There are no items to show in this view.

Create a new object…

Right click on Test_Ldap OU to create a new group


Active Directory Users and Computers
New Object - Group
Type
Description
There are no items to show in this view.
OK
Cancel

Create in: corp.solutionlab.com/Test_Ldap

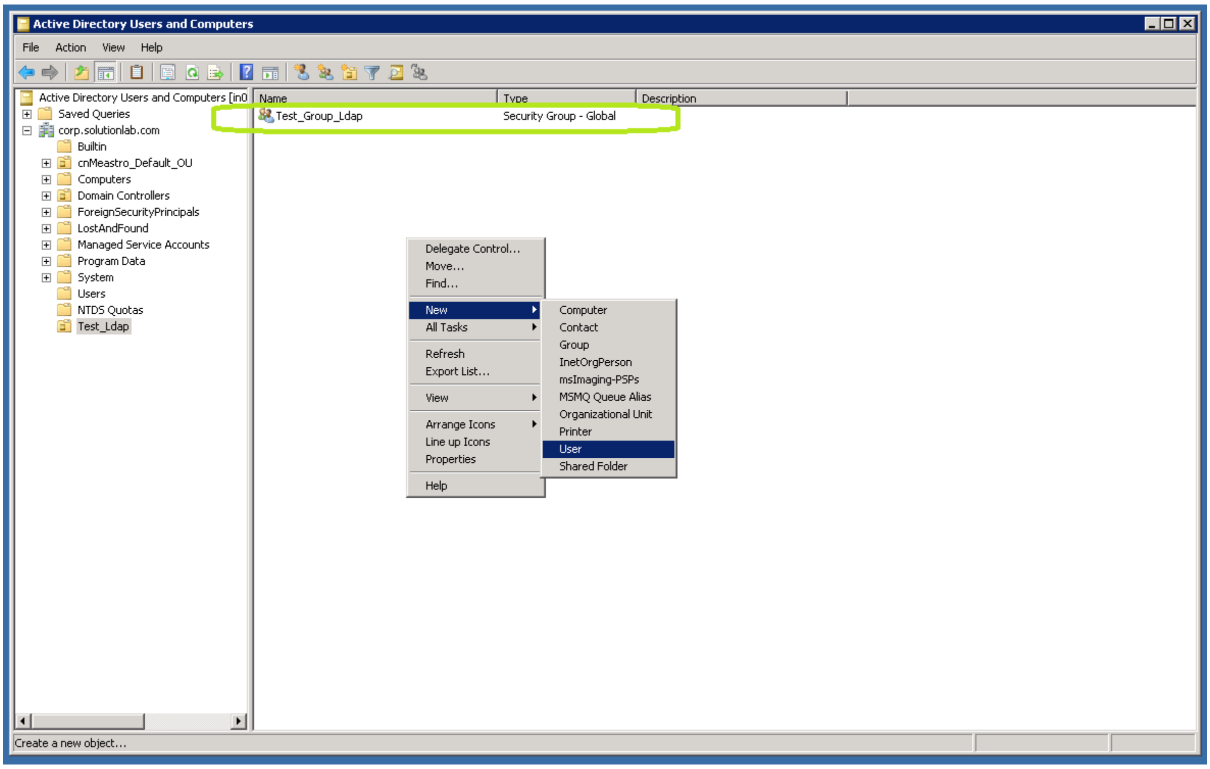
Group name:
Test_Group_Ldap

Group name (pre-Windows 2000):
Test_Group_Ldap

Group scope
○ Domain local
● Global
○ Universal

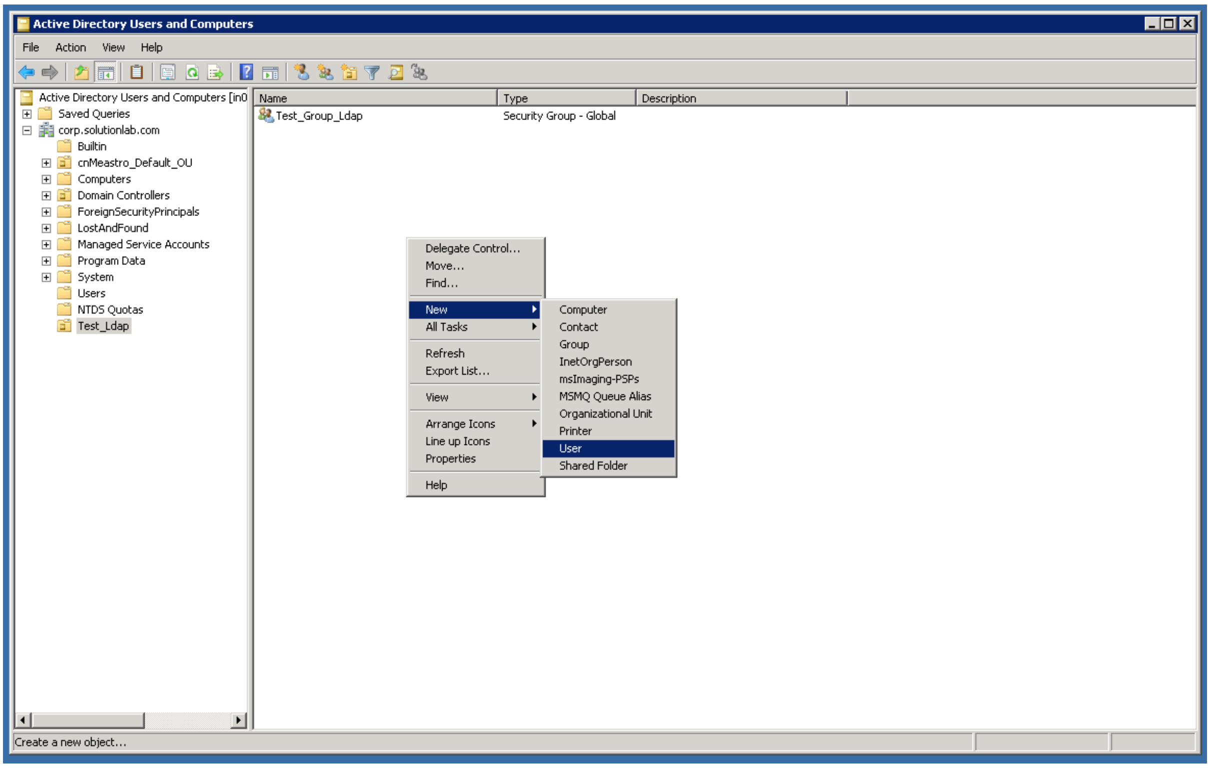
Group type
● Security
○ Distribution

Enter group name “Test_Group_Ldap” and click OK

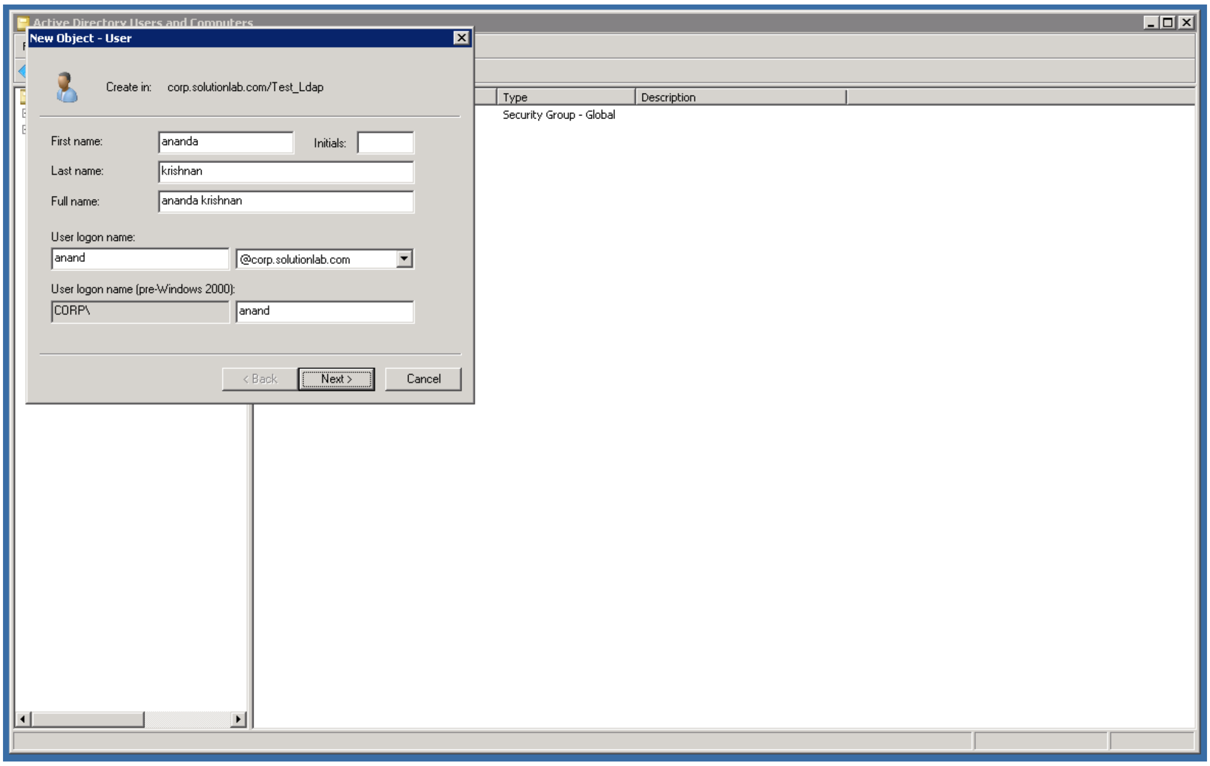


Name	Type	Description
Test_Group_Ldap	Security Group - Global	

“Test_Group_Ldap” group is now created



Right click on “Test_Ldap” OU to create a user



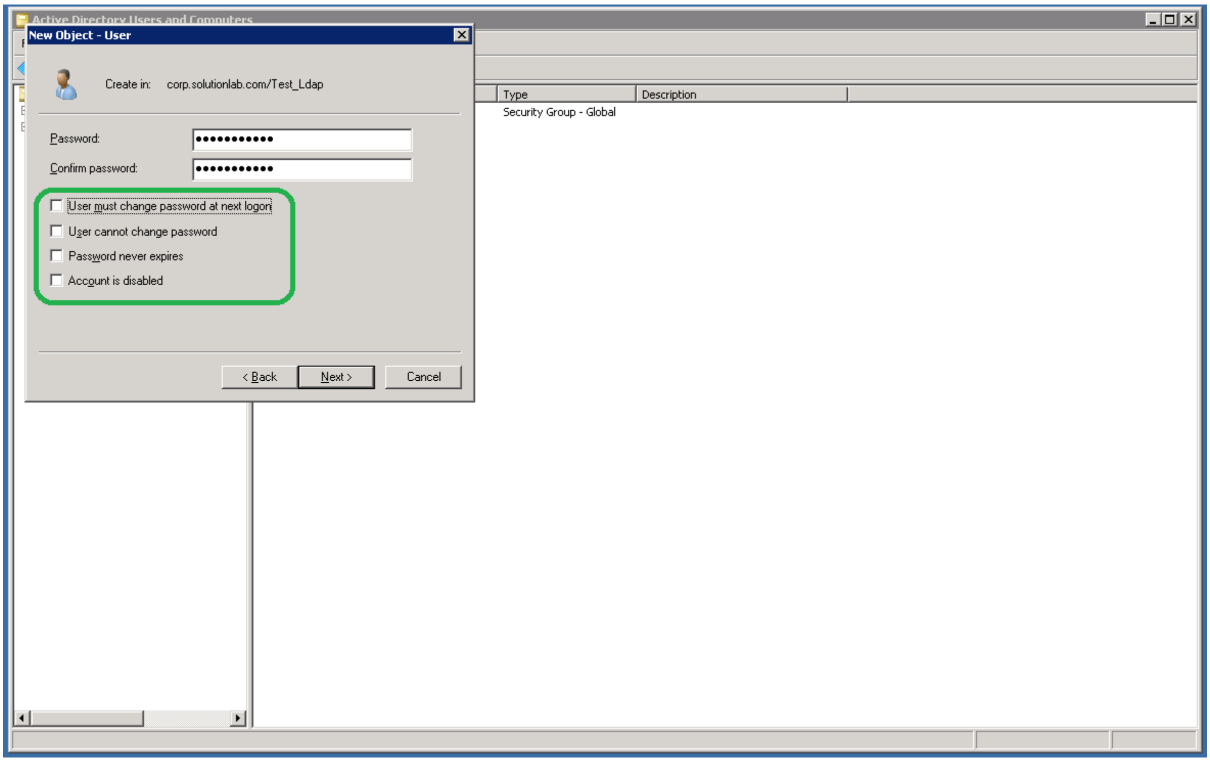
Create in: corp.solutionlab.com/Test_Ldap

First name: ananda
Initials:
Last name: krishnan
Full name: ananda krishnan

User logon name:
anand @corp.solutionlab.com

User logon name (pre-Windows 2000):
CORP\ anand

Add the user name and click NEXT



Create in: corp.solutionlab.com/Test_Ldap

Password: •••••••••••

Confirm password: •••••••••••

☐ User must change password at next logon

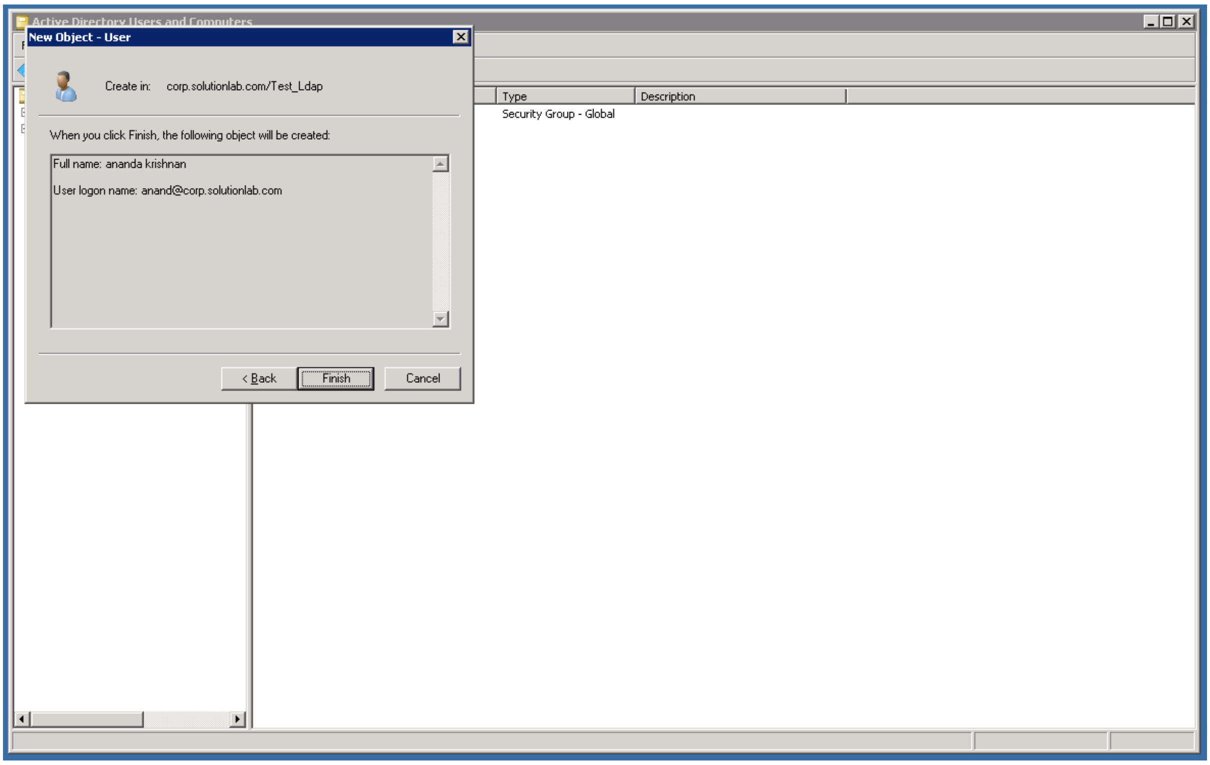
☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Security Group - Global

Add the password and click NEXT, check/uncheck the options in green which is applicable



Create in: corp.solutionlab.com/Test_Ldap

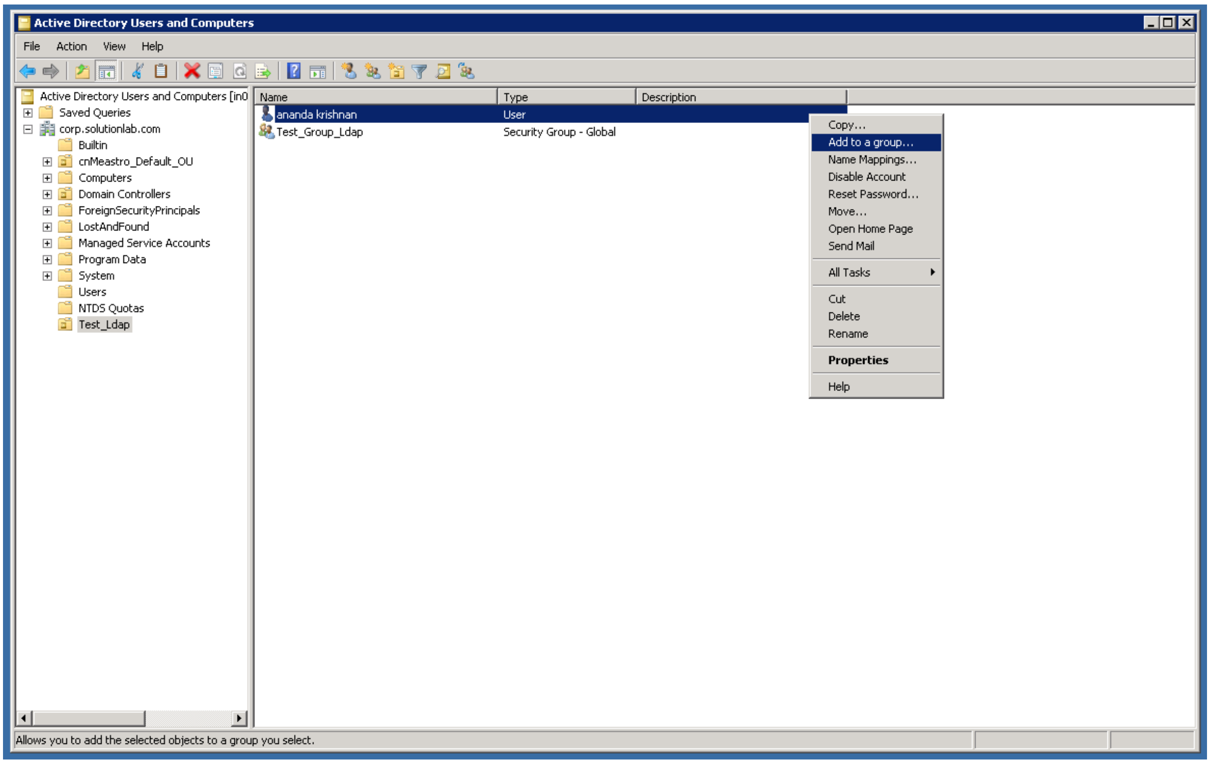
When you click Finish, the following object will be created:

Full name: ananda krishnan

User logon name: anand@corp.solutionlab.com

Security Group - Global

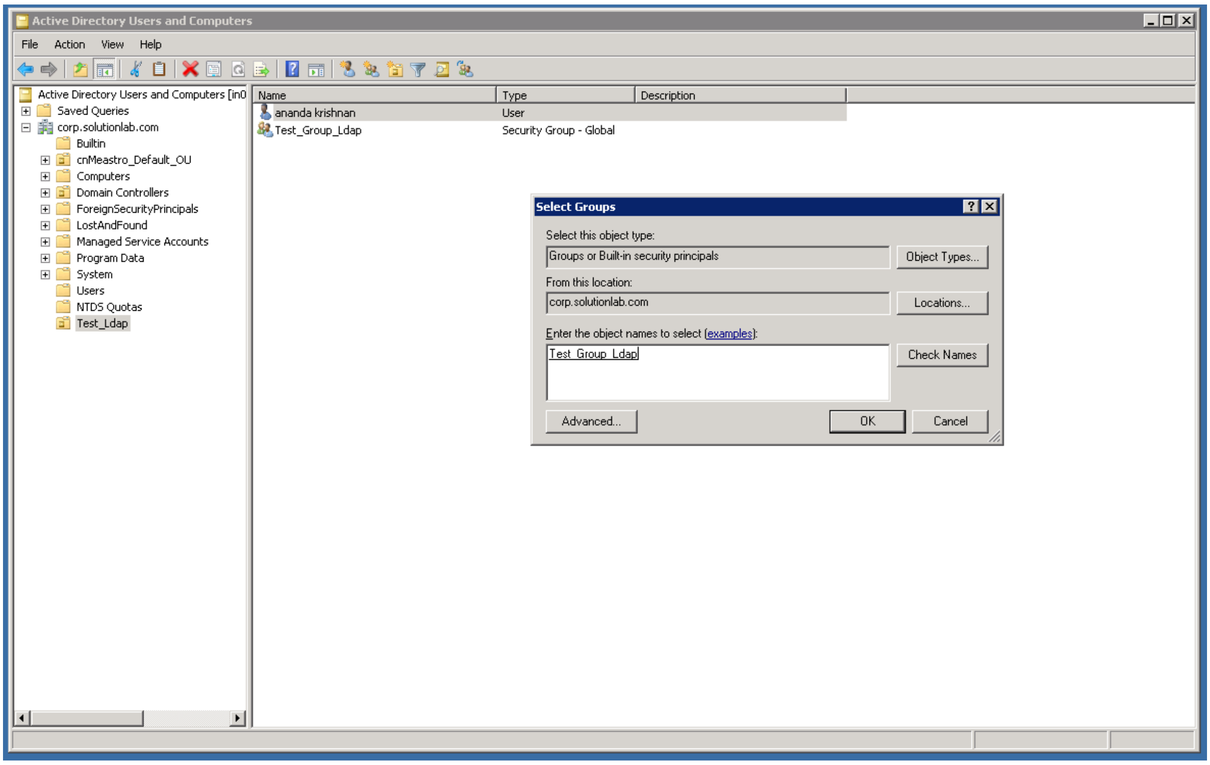
Click FINISH to create the user



Name	Type	Description
ananda krishnan	User	
Test_Group_Ldap	Security Group - Global	

Allows you to add the selected objects to a group you select.

Add the user to a group



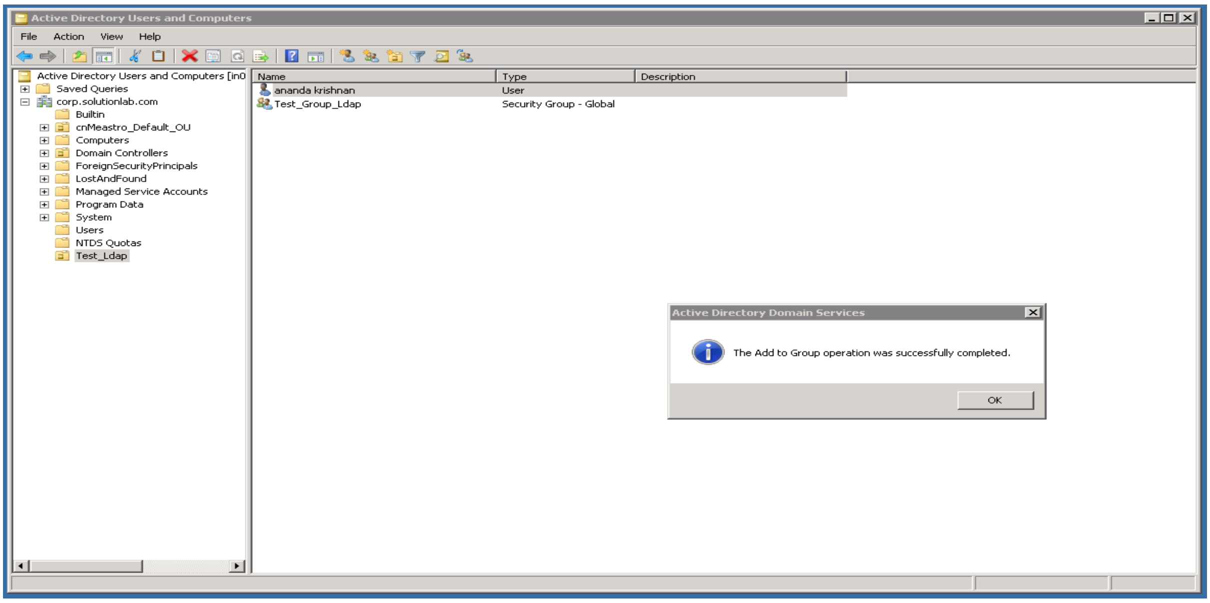
Name	Type	Description
ananda krishnan	User	
Test_Group_Ldap	Security Group - Global	

Select this object type:
Groups or Built-in security principals

From this location:
corp.solutionlab.com

Enter the object names to select (examples):
Test_Group_Ldap

Search the group to which the user needs to be added and click on OK



Name	Type	Description
ananda krishnan	User	
Test_Group_Ldap	Security Group - Global	

Active Directory Domain Services

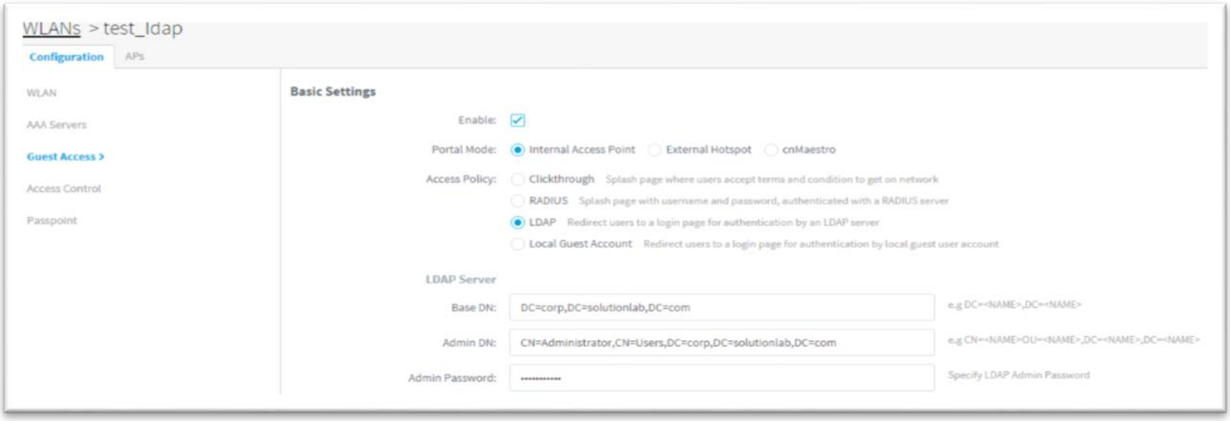
The Add to Group operation was successfully completed.

User successfully added to the group

Configure LDAP server credential on the cnMaestro/AP

In cnMaestro, Ldap guest is available at shared settings > wlan > wlan name > guest access

Below configuration is for default Administrator user which is part of Users



Basic Settings

Enable: ☑

Portal Mode: ● Internal Access Point ○ External Hotspot ○ cnMaestro

Access Policy: ○ Clickthrough Splash page where users accept terms and condition to get on network
○ RADIUS Splash page with username and password, authenticated with a RADIUS server
● LDAP Redirect users to a login page for authentication by an LDAP server
○ Local Guest Account Redirect users to a login page for authentication by local guest user account

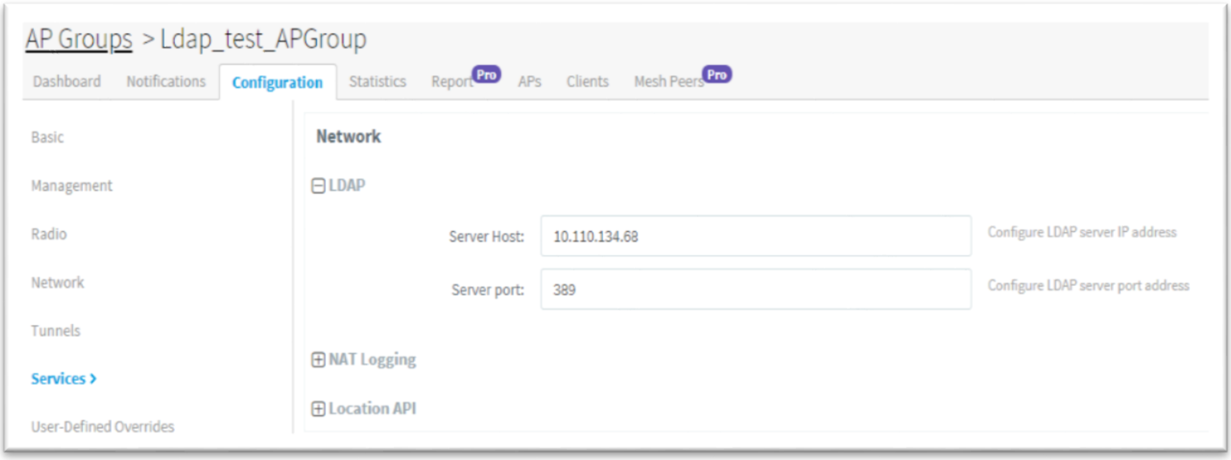
LDAP Server

Base DN: DC=corp,DC=solutionlab,DC=com e.g DC=<NAME>,DC=<NAME>

Admin DN: CN=Administrator,CN=Users,DC=corp,DC=solutionlab,DC=com e.g CN=<NAME>OU=<NAME>,DC=<NAME>,DC=<NAME>

Admin Password: ············ Specify LDAP Admin Password

In cnMaestro, LDAP IP address is configured at > AP_Group > Group name > Services >LDAP



Network

⊟ LDAP

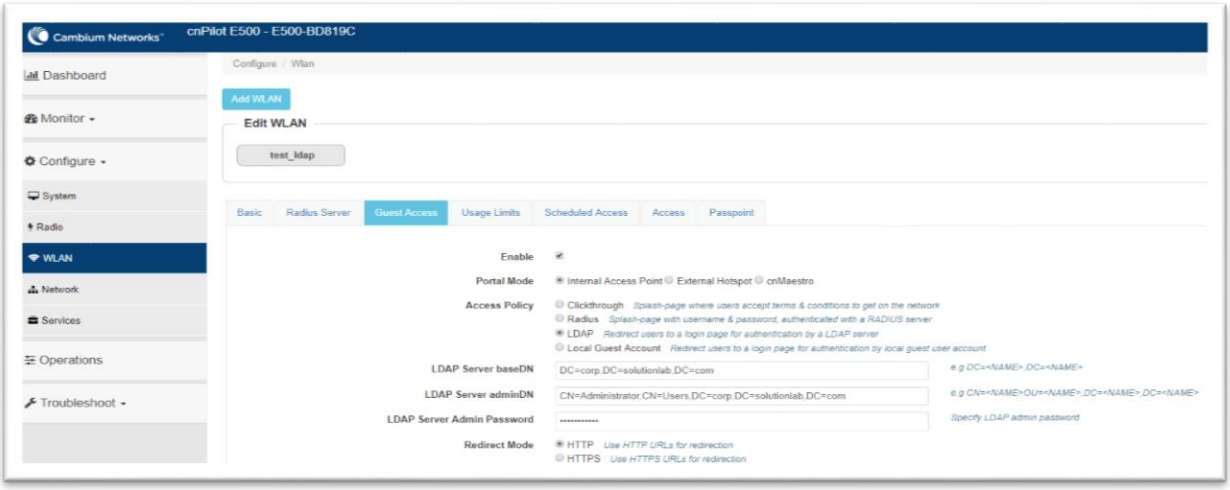
Server Host: 10.110.134.68 Configure LDAP server IP address

Server port: 389 Configure LDAP server port address

⊞ NAT Logging

⊞ Location API

In Access Point, LDAP guest configuration is available Configure> Wlan > Guest Access



Enable ☑

Portal Mode ● Internal Access Point ○ External Hotspot ○ cnMaestro

Access Policy
○ Clickthrough Splash-page where users accept terms & conditions to get on the network
○ Radius Splash-page with username & password, authenticated with a RADIUS server
● LDAP Redirect users to a login page for authentication by a LDAP server
○ Local Guest Account Redirect users to a login page for authentication by local guest user account

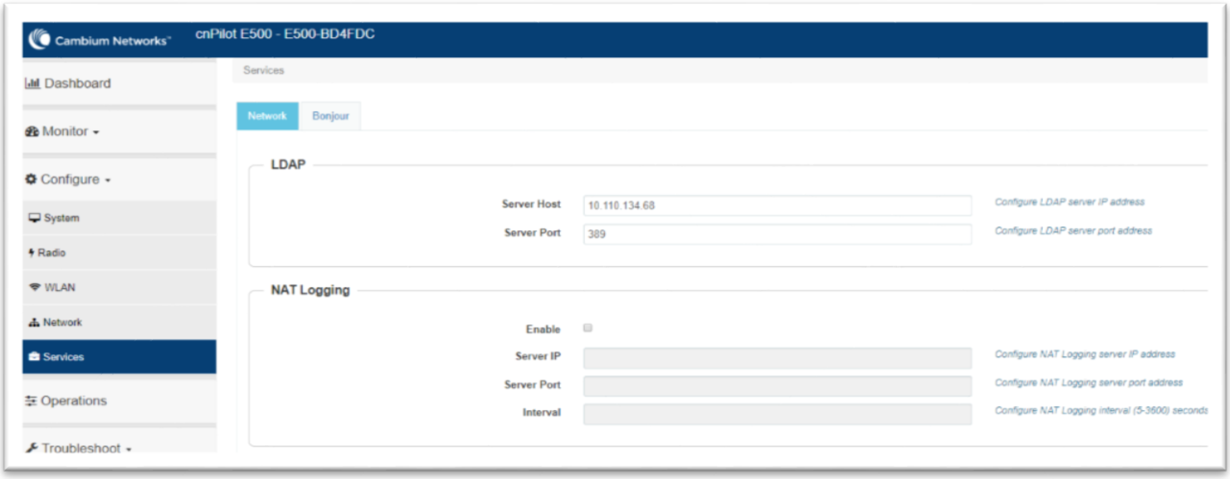
LDAP Server baseDN DC=corp,DC=solutionlab,DC=com e.g DC=<NAME>,DC=<NAME>

LDAP Server adminDN CN=Administrator,CN=Users,DC=corp,DC=solutionlab,DC=com e.g CN=<NAME>OU=<NAME>,DC=<NAME>,DC=<NAME>

LDAP Server Admin Password ············ Specify LDAP admin password

Redirect Mode
● HTTP Use HTTP URLs for redirection
○ HTTPS Use HTTPS URLs for redirection

In Access Point, LDAP IP address is configured at > Configure> Services > Network > LDAP



LDAP

Server Host 10.110.134.68 Configure LDAP server IP address

Server Port 389 Configure LDAP server port address

NAT Logging

Enable □

Server IP Configure NAT Logging server IP address

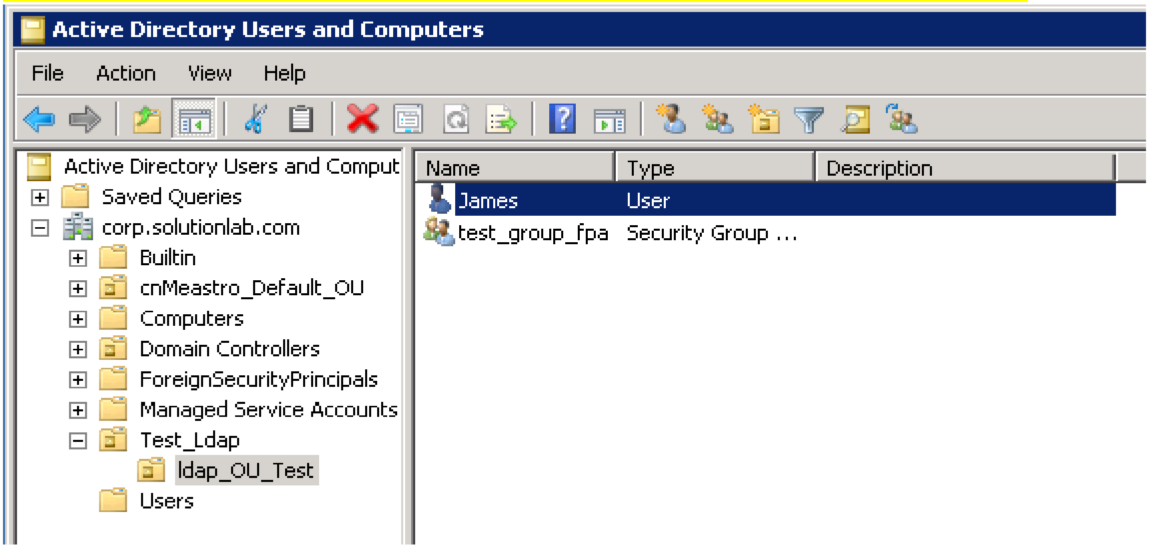
Server Port Configure NAT Logging server port address

Interval Configure NAT Logging interval (5-3600) seconds

Order of DC, OU and CN

Make sure that the order of configuring the DC and OU and CN are correct so that we do not have any issues in binding the AD. Here in this example, order is like this,

CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com



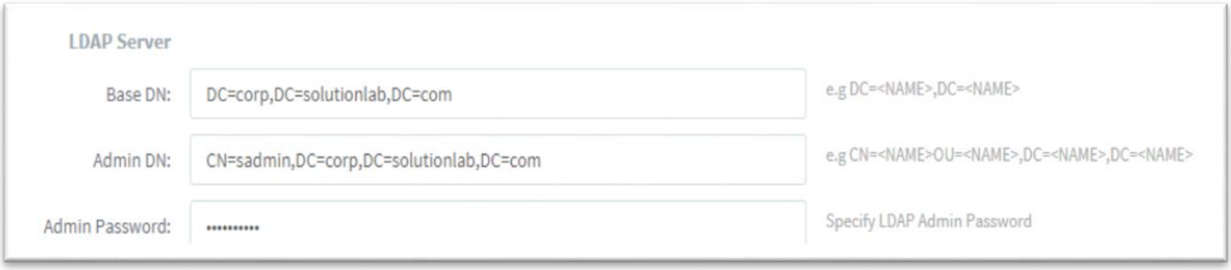
Name	Type	Description
James	User	
test_group_fpa	Security Group ...	

Let’s take different users created in different hierarchy of LDAP and bind with AP and authenticate

LDAP typically has following format. **cn=common name , ou=organizational unit , dc=domain**

“sadmin” –is an administrative user created at the root level.
“admin” is the user used to authenticate the client available at default users group.

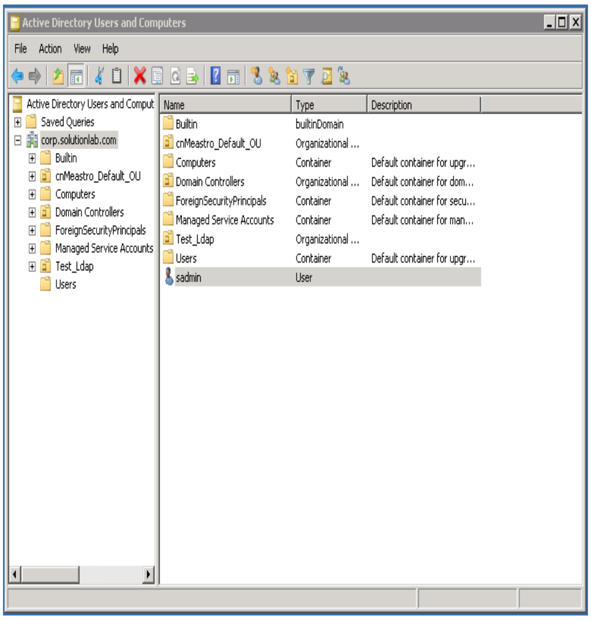
For the below example, cnMaestro/ AP configuration is,



LDAP Server

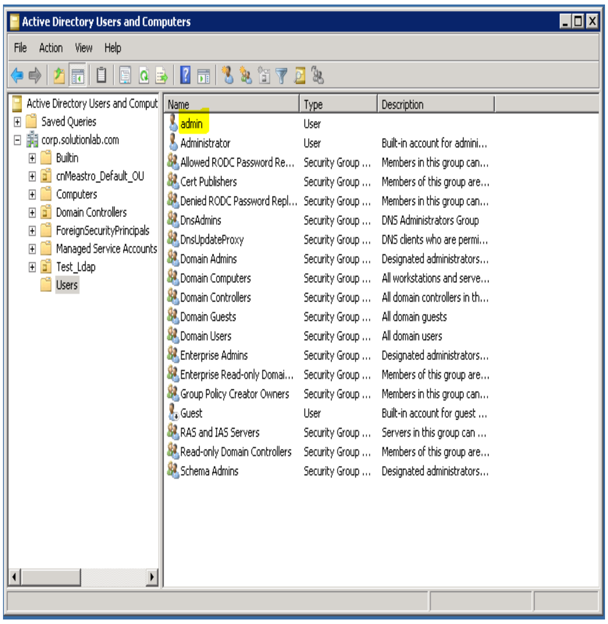
Base DN:	DC=corp,DC=solutionlab,DC=com	e.g DC=<NAME>,DC=<NAME>
Admin DN:	CN=sadmin,DC=corp,DC=solutionlab,DC=com	e.g CN=<NAME>OU=<NAME>,DC=<NAME>,DC=<NAME>
Admin Password:	••••••••••	Specify LDAP Admin Password

Note: We do not need to add OU here since “sadmin” user is not added to any group
Windows AD configuration, Bind user on the left pic and authentication user on the right pic



Active Directory Users and Comput
- Saved Queries
- corp.solutionlab.com
  - Builtin
  - cnMeastro_Default_OU
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Test_Ldap
  - Users

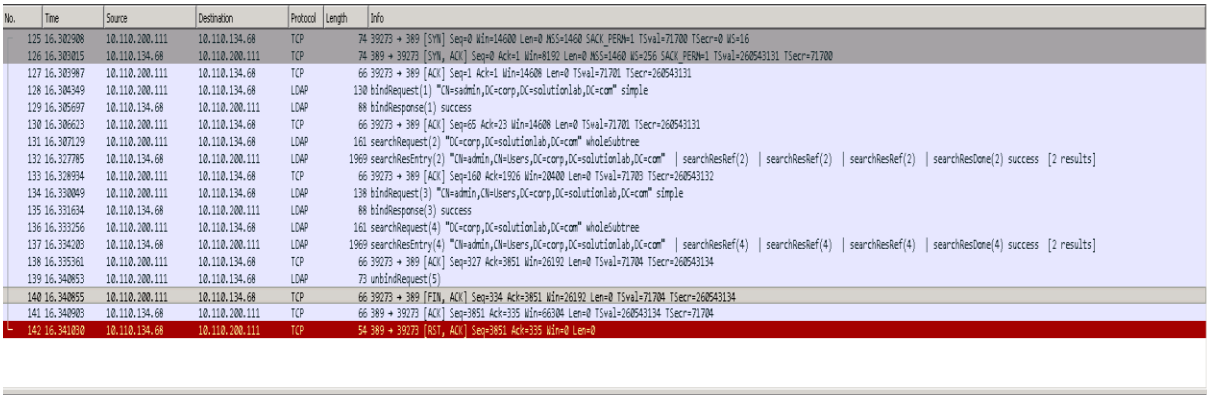
Name	Type	Description
Builtin	builtinDomain	
cnMeastro_Default_OU	Organizational ...	
Computers	Container	Default container for upgr...
Domain Controllers	Organizational ...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secu...
Managed Service Accounts	Container	Default container for man...
Test_Ldap	Organizational ...	
Users	Container	Default container for upgr...
sadmin	User	



Active Directory Users and Comput
- Saved Queries
- corp.solutionlab.com
  - Builtin
  - cnMeastro_Default_OU
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Test_Ldap
  - Users

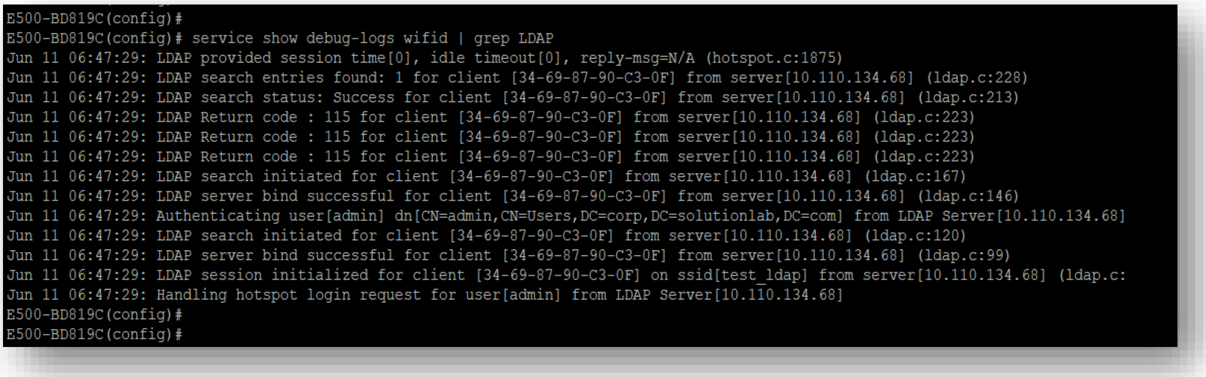
Name	Type	Description
admin	User	
Administrator	User	Built-in account for admini...
Allowed RODC Password Re...	Security Group ...	Members in this group can...
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password Repl...	Security Group ...	Members in this group can...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Enterprise Read-only Domai...	Security Group ...	Members of this group are...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...

Packet capture taken from the LDAP server when bind is success for user admin



```
No.  Time      Source          Destination     Protocol Length Info
 125 16.302908 10.110.200.111  10.110.134.68   TCP        74 39273 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=71700 TSecr=0 WS=16
 126 16.303015 10.110.134.68   10.110.200.111  TCP        74 389 → 39273 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=260543131 TSecr=71700
 127 16.303987 10.110.200.111  10.110.134.68   TCP        66 39273 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=71701 TSecr=260543131
 128 16.304349 10.110.200.111  10.110.134.68   LDAP      130 bindRequest(1) "CN=sadmin,DC=corp,DC=solutionlab,DC=com" simple
 129 16.305697 10.110.134.68   10.110.200.111  LDAP       88 bindResponse(1) success
 130 16.306623 10.110.200.111  10.110.134.68   TCP        66 39273 → 389 [ACK] Seq=65 Ack=23 Win=14608 Len=0 TSval=71701 TSecr=260543131
 131 16.307129 10.110.200.111  10.110.134.68   LDAP      161 searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
 132 16.327785 10.110.134.68   10.110.200.111  LDAP     1969 searchResEntry(2) "CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com"  | searchResRef(2)  | searchResRef(2)  | searchResRef(2)  | searchResDone(2) success  [2 results]
 133 16.328934 10.110.200.111  10.110.134.68   TCP        66 39273 → 389 [ACK] Seq=160 Ack=1926 Win=20400 Len=0 TSval=71703 TSecr=260543132
 134 16.330049 10.110.200.111  10.110.134.68   LDAP      138 bindRequest(3) "CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com" simple
 135 16.331634 10.110.134.68   10.110.200.111  LDAP       88 bindResponse(3) success
 136 16.333256 10.110.200.111  10.110.134.68   LDAP      161 searchRequest(4) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
 137 16.334203 10.110.134.68   10.110.200.111  LDAP     1969 searchResEntry(4) "CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com"  | searchResRef(4)  | searchResRef(4)  | searchResRef(4)  | searchResDone(4) success  [2 results]
 138 16.335361 10.110.200.111  10.110.134.68   TCP        66 39273 → 389 [ACK] Seq=327 Ack=3851 Win=26192 Len=0 TSval=71704 TSecr=260543134
 139 16.340853 10.110.200.111  10.110.134.68   LDAP       73 unbindRequest(5)
 140 16.340855 10.110.200.111  10.110.134.68   TCP        66 39273 → 389 [FIN, ACK] Seq=334 Ack=3851 Win=26192 Len=0 TSval=71704 TSecr=260543134
 141 16.340903 10.110.134.68   10.110.200.111  TCP        66 389 → 39273 [ACK] Seq=3851 Ack=335 Win=66304 Len=0 TSval=260543134 TSecr=71704
 142 16.341030 10.110.134.68   10.110.200.111  TCP        54 389 → 39273 [RST, ACK] Seq=3851 Ack=335 Win=0 Len=0
```

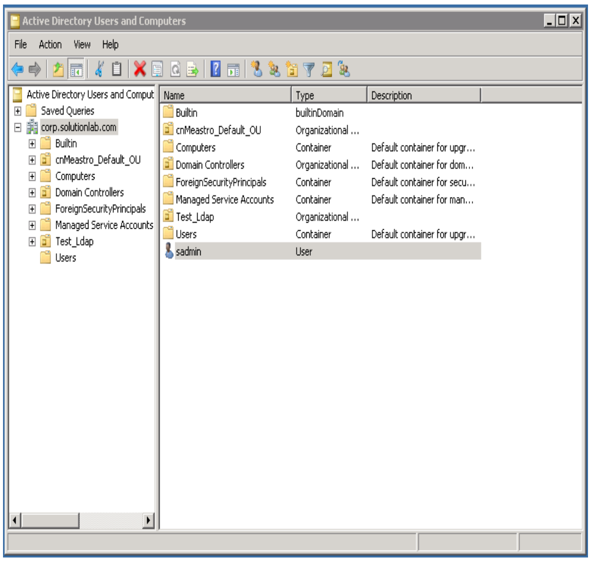
Logs from the AP for successful user authentication



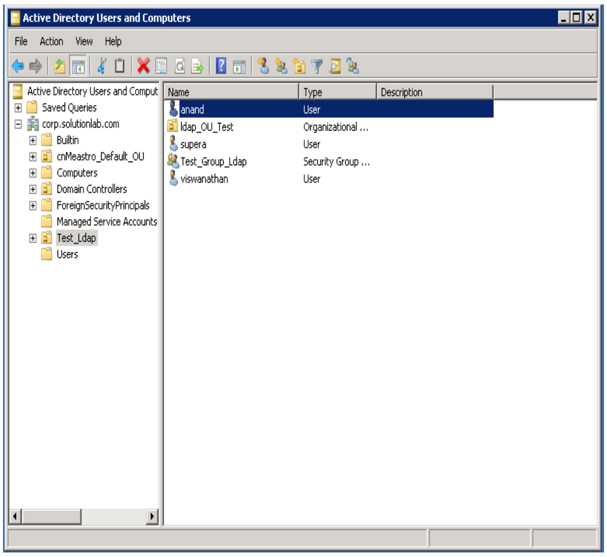
```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 06:47:29: LDAP provided session time[0], idle timeout[0], reply-msg=N/A (hotspot.c:1875)
Jun 11 06:47:29: LDAP search entries found: 1 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:228)
Jun 11 06:47:29: LDAP search status: Success for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:213)
Jun 11 06:47:29: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 06:47:29: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 06:47:29: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 06:47:29: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:167)
Jun 11 06:47:29: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:146)
Jun 11 06:47:29: Authenticating user[admin] dn[CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com] from LDAP Server[10.110.134.68]
Jun 11 06:47:29: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
Jun 11 06:47:29: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
Jun 11 06:47:29: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 06:47:29: Handling hotspot login request for user[admin] from LDAP Server[10.110.134.68]
E500-BD819C(config)#
E500-BD819C(config)#
```

"anand" is the user used to authenticate the client available at Test_Ldap OU.

Windows AD configuration, Bind the LDAP server with user (sadmin) credentials on the left pic and authenticate guest user (anand) on the right pic

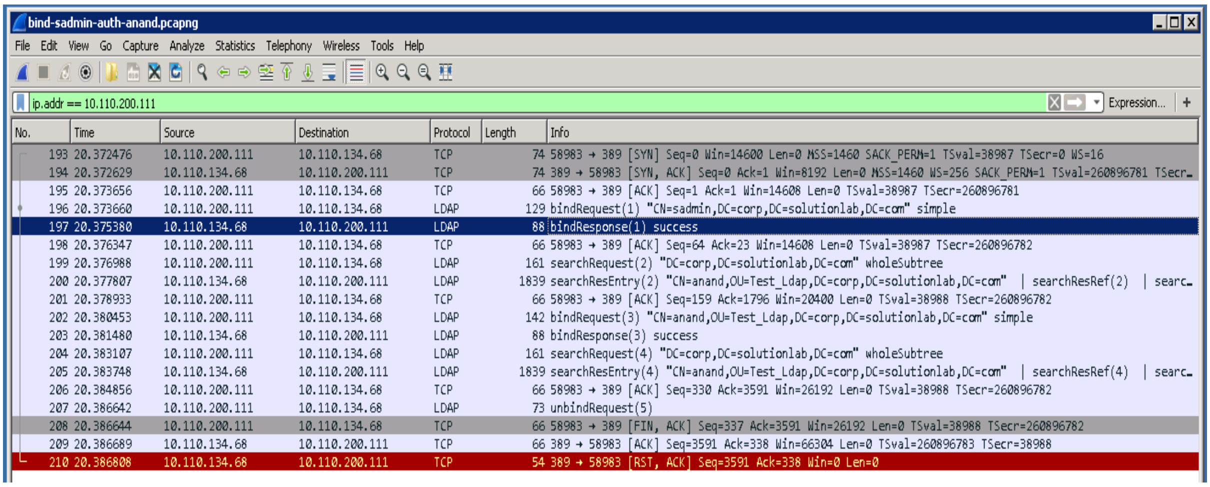


Name	Type	Description
Builtin	builtinDomain	
cnMeastro_Default_OU	Organizational ...	
Computers	Container	Default container for upgr...
Domain Controllers	Organizational ...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secu...
Managed Service Accounts	Container	Default container for man...
Test_Ldap	Organizational ...	
Users	Container	Default container for upgr...
sadmin	User	



Name	Type	Description
anand	User	
ldap_OU_Test	Organizational ...	
supera	User	
Test_Group_Ldap	Security Group ...	
viswanathan	User	

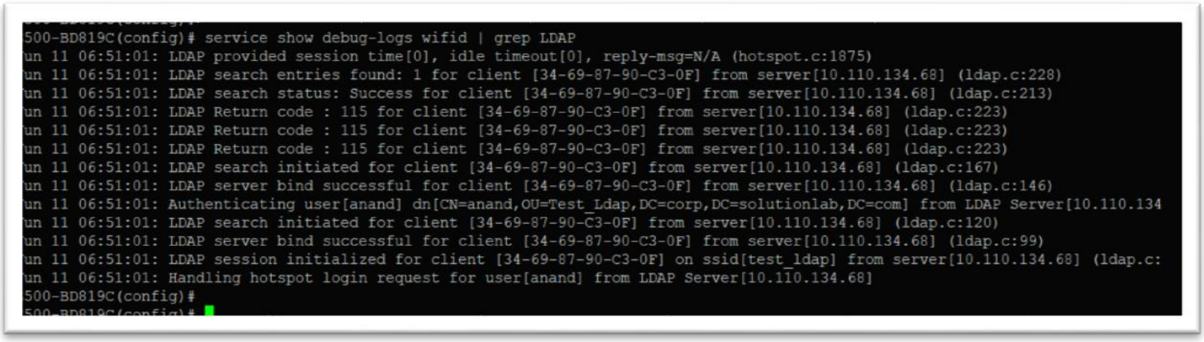
Packet capture taken from the LDAP server when bind is success for user anand



ip.addr == 10.110.200.111

No.	Time	Source	Destination	Protocol	Length	Info
193	20.372476	10.110.200.111	10.110.134.68	TCP	74	58983 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=38987 TSecr=0 WS=16
194	20.372629	10.110.134.68	10.110.200.111	TCP	74	389 → 58983 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=260896781 TSecr…
195	20.373656	10.110.200.111	10.110.134.68	TCP	66	58983 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=38987 TSecr=260896781
196	20.373660	10.110.200.111	10.110.134.68	LDAP	129	bindRequest(1) "CN=sadmin,DC=corp,DC=solutionlab,DC=com" simple
197	20.375380	10.110.134.68	10.110.200.111	LDAP	88	bindResponse(1) success
198	20.376347	10.110.200.111	10.110.134.68	TCP	66	58983 → 389 [ACK] Seq=64 Ack=23 Win=14608 Len=0 TSval=38987 TSecr=260896782
199	20.376988	10.110.200.111	10.110.134.68	LDAP	161	searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
200	20.377807	10.110.134.68	10.110.200.111	LDAP	1839	searchResEntry(2) "CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" | searchResRef(2) | searc…
201	20.378933	10.110.200.111	10.110.134.68	TCP	66	58983 → 389 [ACK] Seq=159 Ack=1796 Win=20400 Len=0 TSval=38988 TSecr=260896782
202	20.380453	10.110.200.111	10.110.134.68	LDAP	142	bindRequest(3) "CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" simple
203	20.381480	10.110.134.68	10.110.200.111	LDAP	88	bindResponse(3) success
204	20.383107	10.110.200.111	10.110.134.68	LDAP	161	searchRequest(4) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
205	20.383748	10.110.134.68	10.110.200.111	LDAP	1839	searchResEntry(4) "CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" | searchResRef(4) | searc…
206	20.384856	10.110.200.111	10.110.134.68	TCP	66	58983 → 389 [ACK] Seq=330 Ack=3591 Win=26192 Len=0 TSval=38988 TSecr=260896782
207	20.386642	10.110.200.111	10.110.134.68	LDAP	73	unbindRequest(5)
208	20.386644	10.110.200.111	10.110.134.68	TCP	66	58983 → 389 [FIN, ACK] Seq=337 Ack=3591 Win=26192 Len=0 TSval=38988 TSecr=260896782
209	20.386689	10.110.134.68	10.110.200.111	TCP	66	389 → 58983 [ACK] Seq=3591 Ack=338 Win=66304 Len=0 TSval=260896783 TSecr=38988
210	20.386808	10.110.134.68	10.110.200.111	TCP	54	389 → 58983 [RST, ACK] Seq=3591 Ack=338 Win=0 Len=0

Logs from the AP when user authentication is success



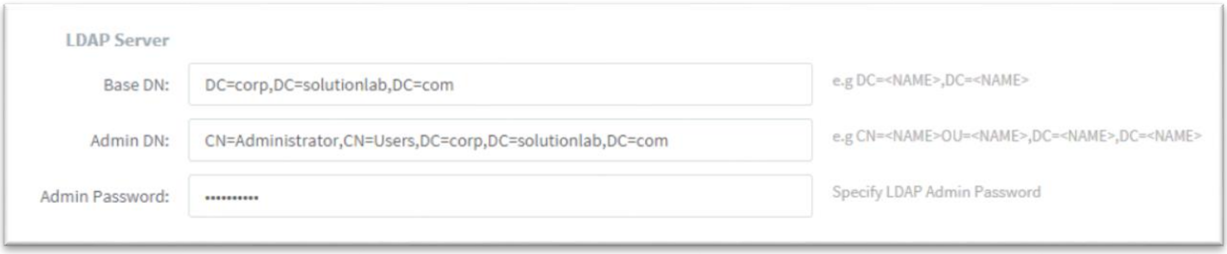
```
500-BD819C(config)# service show debug-logs wifid | grep LDAP
un 11 06:51:01: LDAP provided session time[0], idle timeout[0], reply-msg=N/A (hotspot.c:1875)
un 11 06:51:01: LDAP search entries found: 1 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:228)
un 11 06:51:01: LDAP search status: Success for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:213)
un 11 06:51:01: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
un 11 06:51:01: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
un 11 06:51:01: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
un 11 06:51:01: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:167)
un 11 06:51:01: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:146)
un 11 06:51:01: Authenticating user[anand] dn[CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com] from LDAP Server[10.110.134
un 11 06:51:01: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
un 11 06:51:01: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
un 11 06:51:01: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
un 11 06:51:01: Handling hotspot login request for user[anand] from LDAP Server[10.110.134.68]
500-BD819C(config)#
```

Let’s use another Administrative user to bind the AP with the Active directory.

“Administrator” –is an administrative user already available in the users group

“admin” is the user used to authenticate the client available at default users group.

cnMaestro/ AP configuration is, Note that here Users is mapped to CN not OU



LDAP Server

Base DN: DC=corp,DC=solutionlab,DC=com

e.g DC=<NAME>,DC=<NAME>

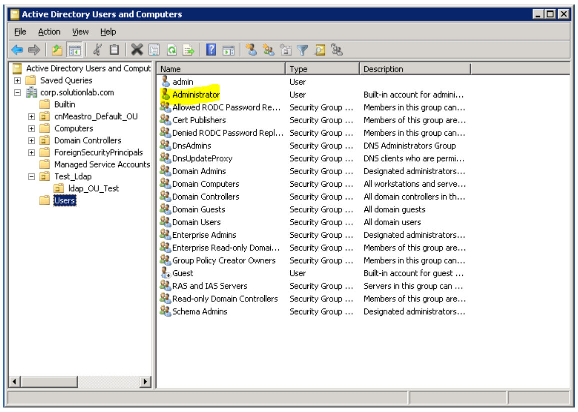
Admin DN: CN=Administrator,CN=Users,DC=corp,DC=solutionlab,DC=com

e.g CN=<NAME>OU=<NAME>,DC=<NAME>,DC=<NAME>

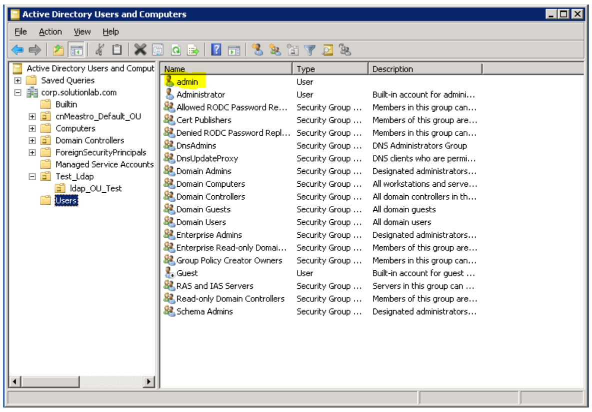
Admin Password: ••••••••••

Specify LDAP Admin Password

Windows AD configuration, Bind the LDAP server with user (Administrator) credentials on the left pic and authenticate guest user (admin) on the right pic

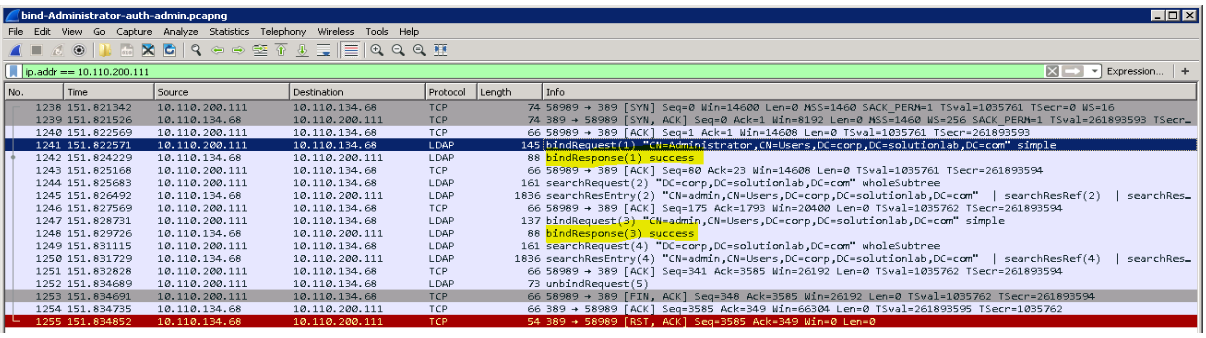


Name	Type	Description
admin	User	
Administrator	User	Built-in account for admini...
Allowed RODC Password Re...	Security Group ...	Members in this group can...
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password Repl...	Security Group ...	Members in this group can...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Enterprise Read-only Domai...	Security Group ...	Members of this group are...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...



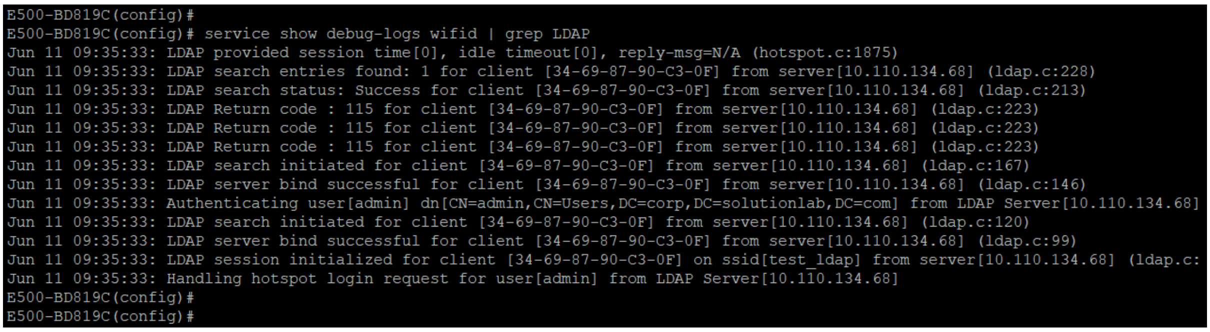
Name	Type	Description
admin	User	
Administrator	User	Built-in account for admini...
Allowed RODC Password Re...	Security Group ...	Members in this group can...
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password Repl...	Security Group ...	Members in this group can...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Enterprise Read-only Domai...	Security Group ...	Members of this group are...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...

Packet capture taken from LDAP server when bind is success and authentication is also success


bind-Administrator-auth-admin.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
ip.addr == 10.110.200.111

No.  Time       Source          Destination     Protocol Length Info
1238 151.821342 10.110.200.111  10.110.134.68   TCP        74 58989 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1035761 TSecr=0 WS=16
1239 151.821526 10.110.134.68   10.110.200.111  TCP        74 389 → 58989 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=261893593 TSecr…
1240 151.822569 10.110.200.111  10.110.134.68   TCP        66 58989 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=1035761 TSecr=261893593
1241 151.822571 10.110.200.111  10.110.134.68   LDAP      145 bindRequest(1) "CN=Administrator,CN=Users,DC=corp,DC=solutionlab,DC=com" simple
1242 151.824229 10.110.134.68   10.110.200.111  LDAP       88 bindResponse(1) success
1243 151.825168 10.110.200.111  10.110.134.68   TCP        66 58989 → 389 [ACK] Seq=80 Ack=23 Win=14608 Len=0 TSval=1035761 TSecr=261893594
1244 151.825683 10.110.200.111  10.110.134.68   LDAP      161 searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
1245 151.826492 10.110.134.68   10.110.200.111  LDAP     1836 searchResEntry(2) "CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com"  | searchResRef(2)  | searchRes…
1246 151.827569 10.110.200.111  10.110.134.68   TCP        66 58989 → 389 [ACK] Seq=175 Ack=1793 Win=20400 Len=0 TSval=1035762 TSecr=261893594
1247 151.828731 10.110.200.111  10.110.134.68   LDAP      137 bindRequest(3) "CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com" simple
1248 151.829726 10.110.134.68   10.110.200.111  LDAP       88 bindResponse(3) success
1249 151.831115 10.110.200.111  10.110.134.68   LDAP      161 searchRequest(4) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
1250 151.831729 10.110.134.68   10.110.200.111  LDAP     1836 searchResEntry(4) "CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com"  | searchResRef(4)  | searchRes…
1251 151.832828 10.110.200.111  10.110.134.68   TCP        66 58989 → 389 [ACK] Seq=341 Ack=3585 Win=26192 Len=0 TSval=1035762 TSecr=261893594
1252 151.834689 10.110.200.111  10.110.134.68   LDAP       73 unbindRequest(5)
1253 151.834691 10.110.200.111  10.110.134.68   TCP        66 58989 → 389 [FIN, ACK] Seq=348 Ack=3585 Win=26192 Len=0 TSval=1035762 TSecr=261893594
1254 151.834735 10.110.134.68   10.110.200.111  TCP        66 389 → 58989 [ACK] Seq=3585 Ack=349 Win=66304 Len=0 TSval=261893595 TSecr=1035762
1255 151.834852 10.110.134.68   10.110.200.111  TCP        54 389 → 58989 [RST, ACK] Seq=3585 Ack=349 Win=0 Len=0
```

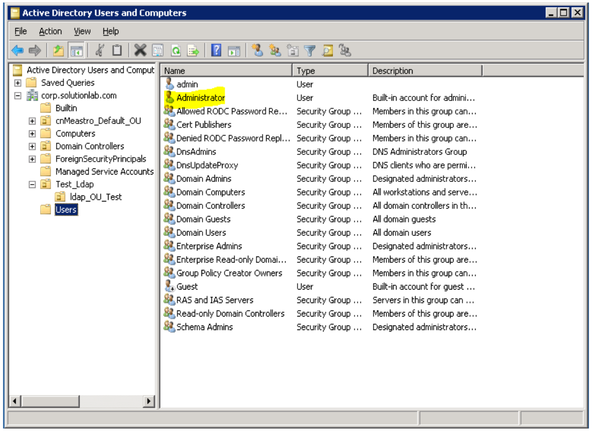
Logs from the AP when user authentication is success



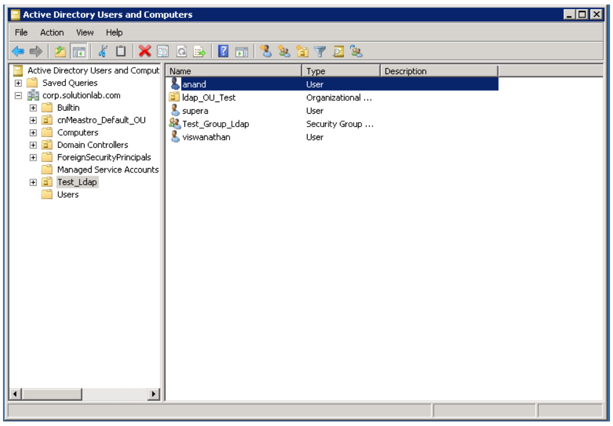
```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 09:35:33: LDAP provided session time[0], idle timeout[0], reply-msg=N/A (hotspot.c:1875)
Jun 11 09:35:33: LDAP search entries found: 1 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:228)
Jun 11 09:35:33: LDAP search status: Success for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:213)
Jun 11 09:35:33: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 09:35:33: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 09:35:33: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 09:35:33: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:167)
Jun 11 09:35:33: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:146)
Jun 11 09:35:33: Authenticating user[admin] dn[CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com] from LDAP Server[10.110.134.68]
Jun 11 09:35:33: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
Jun 11 09:35:33: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
Jun 11 09:35:33: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 09:35:33: Handling hotspot login request for user[admin] from LDAP Server[10.110.134.68]
E500-BD819C(config)#
E500-BD819C(config)#
```

"anand" is the user used to authenticate the client available at Test_Ldap OU.

Windows AD configuration, Bind user on the left pic and authentication user on the right pic

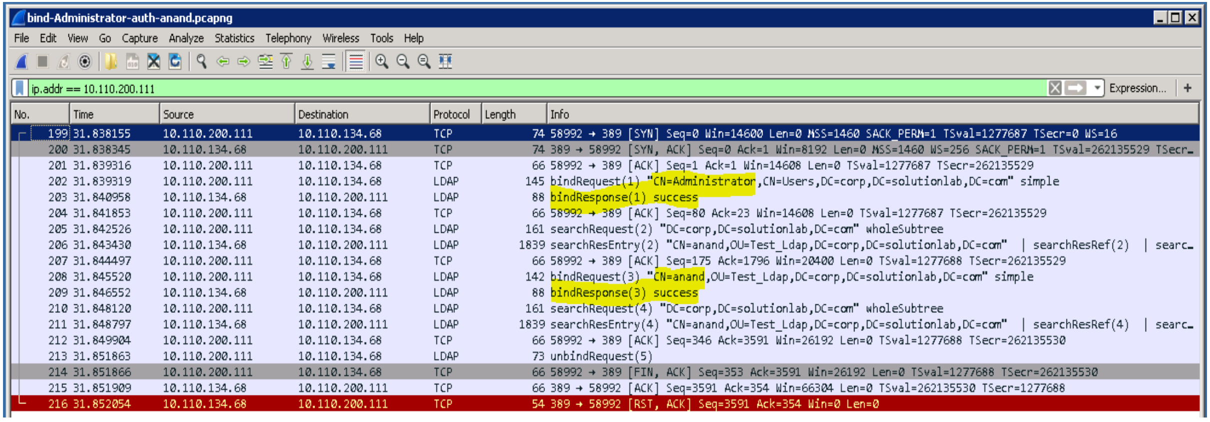


Name	Type	Description
admin	User	
Administrator	User	Built-in account for admini...
Allowed RODC Password Re...	Security Group ...	Members in this group can...
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password Repl...	Security Group ...	Members in this group can...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Enterprise Read-only Domai...	Security Group ...	Members of this group are...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...



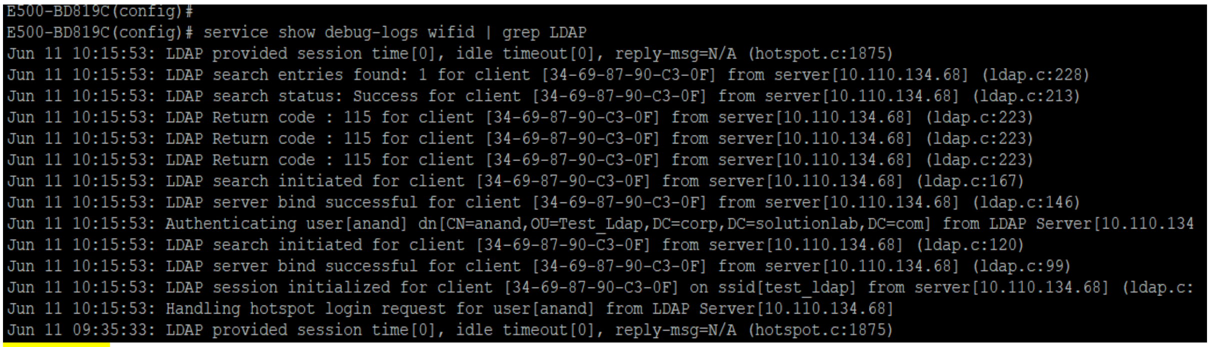
Name	Type	Description
anand	User	
ldap_OU_Test	Organizational ...	
supera	User	
Test_Group_Ldap	Security Group ...	
viswanathan	User	

Packet capture taken from LDAP when bind is success and authentication is also success


bind-Administrator-auth-anand.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

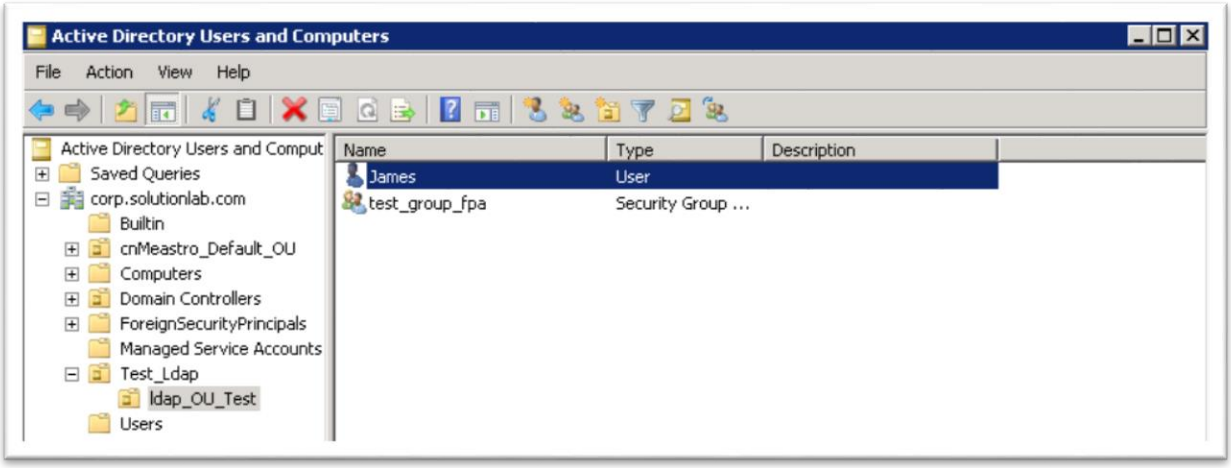
```
ip.addr == 10.110.200.111

No. Time      Source          Destination     Protocol Length Info
199 31.838155 10.110.200.111  10.110.134.68   TCP        74 58992 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1277687 TSecr=0 WS=16
200 31.838345 10.110.134.68   10.110.200.111  TCP        74 389 → 58992 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=262135529 TSecr…
201 31.839316 10.110.200.111  10.110.134.68   TCP        66 58992 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=1277687 TSecr=262135529
202 31.839319 10.110.200.111  10.110.134.68   LDAP      145 bindRequest(1) "CN=Administrator,CN=Users,DC=corp,DC=solutionlab,DC=com" simple
203 31.840958 10.110.134.68   10.110.200.111  LDAP       88 bindResponse(1) success
204 31.841853 10.110.200.111  10.110.134.68   TCP        66 58992 → 389 [ACK] Seq=80 Ack=23 Win=14608 Len=0 TSval=1277687 TSecr=262135529
205 31.842526 10.110.200.111  10.110.134.68   LDAP      161 searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
206 31.843430 10.110.134.68   10.110.200.111  LDAP     1839 searchResEntry(2) "CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com"  | searchResRef(2)  | searc…
207 31.844497 10.110.200.111  10.110.134.68   TCP        66 58992 → 389 [ACK] Seq=175 Ack=1796 Win=20400 Len=0 TSval=1277688 TSecr=262135529
208 31.845520 10.110.200.111  10.110.134.68   LDAP      142 bindRequest(3) "CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" simple
209 31.846552 10.110.134.68   10.110.200.111  LDAP       88 bindResponse(3) success
210 31.848120 10.110.200.111  10.110.134.68   LDAP      161 searchRequest(4) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
211 31.848797 10.110.134.68   10.110.200.111  LDAP     1839 searchResEntry(4) "CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com"  | searchResRef(4)  | searc…
212 31.849904 10.110.200.111  10.110.134.68   TCP        66 58992 → 389 [ACK] Seq=346 Ack=3591 Win=26192 Len=0 TSval=1277688 TSecr=262135530
213 31.851863 10.110.200.111  10.110.134.68   LDAP       73 unbindRequest(5)
214 31.851866 10.110.200.111  10.110.134.68   TCP        66 58992 → 389 [FIN, ACK] Seq=353 Ack=3591 Win=26192 Len=0 TSval=1277688 TSecr=262135530
215 31.851909 10.110.134.68   10.110.200.111  TCP        66 389 → 58992 [ACK] Seq=3591 Ack=354 Win=66304 Len=0 TSval=262135530 TSecr=1277688
216 31.852054 10.110.134.68   10.110.200.111  TCP        54 389 → 58992 [RST, ACK] Seq=3591 Ack=354 Win=0 Len=0
```

Logs from the AP when user authentication is success



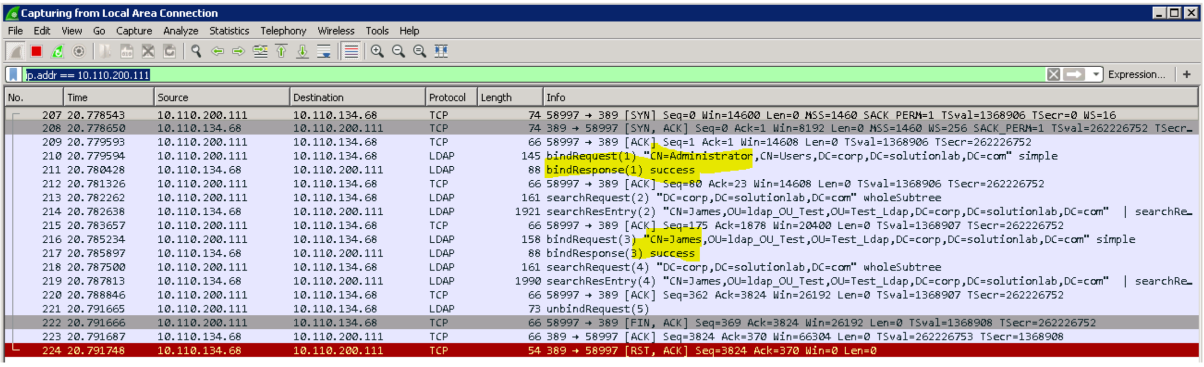
```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 10:15:53: LDAP provided session time[0], idle timeout[0], reply-msg=N/A (hotspot.c:1875)
Jun 11 10:15:53: LDAP search entries found: 1 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:228)
Jun 11 10:15:53: LDAP search status: Success for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:213)
Jun 11 10:15:53: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 10:15:53: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 10:15:53: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 10:15:53: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:167)
Jun 11 10:15:53: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:146)
Jun 11 10:15:53: Authenticating user[anand] dn[CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com] from LDAP Server[10.110.134
Jun 11 10:15:53: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
Jun 11 10:15:53: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
Jun 11 10:15:53: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 10:15:53: Handling hotspot login request for user[anand] from LDAP Server[10.110.134.68]
Jun 11 09:35:33: LDAP provided session time[0], idle timeout[0], reply-msg=N/A (hotspot.c:1875)
```

"James" is the user used to authenticate the client available at ldap_OU_Test OU which is inside the Test_Ldap OU



Name	Type	Description
James	User	
test_group_fpa	Security Group ...	

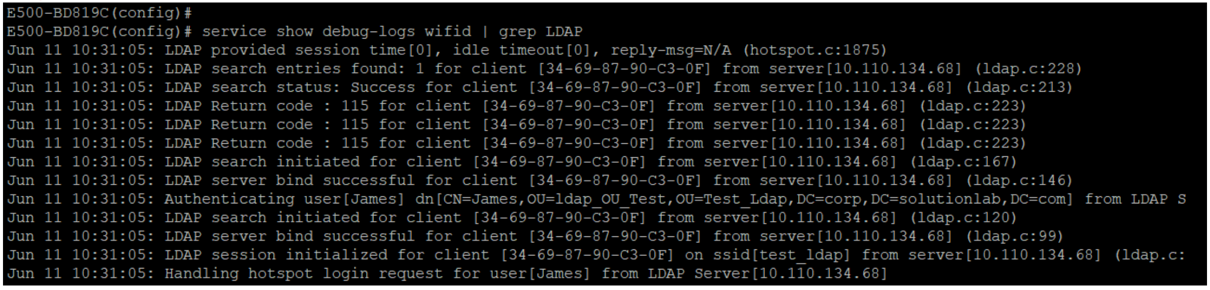
Packet capture taken from LDAP when bind is success and authentication is also success



ip.addr == 10.110.200.111

No.	Time	Source	Destination	Protocol	Length	Info
207	20.778543	10.110.200.111	10.110.134.68	TCP	74	58997 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1368906 TSecr=0 WS=16
208	20.778650	10.110.134.68	10.110.200.111	TCP	74	389 → 58997 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=262226752 TSecr…
209	20.779593	10.110.200.111	10.110.134.68	TCP	66	58997 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=1368906 TSecr=262226752
210	20.779594	10.110.200.111	10.110.134.68	LDAP	145	bindRequest(1) "CN=Administrator,CN=Users,DC=corp,DC=solutionlab,DC=com" simple
211	20.780428	10.110.134.68	10.110.200.111	LDAP	88	bindResponse(1) success
212	20.781326	10.110.200.111	10.110.134.68	TCP	66	58997 → 389 [ACK] Seq=80 Ack=23 Win=14608 Len=0 TSval=1368906 TSecr=262226752
213	20.782262	10.110.200.111	10.110.134.68	LDAP	161	searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
214	20.782638	10.110.134.68	10.110.200.111	LDAP	1921	searchResEntry(2) "CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" | searchRe…
215	20.783657	10.110.200.111	10.110.134.68	TCP	66	58997 → 389 [ACK] Seq=175 Ack=1878 Win=20400 Len=0 TSval=1368907 TSecr=262226752
216	20.785234	10.110.200.111	10.110.134.68	LDAP	158	bindRequest(3) "CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" simple
217	20.785897	10.110.134.68	10.110.200.111	LDAP	88	bindResponse(3) success
218	20.787500	10.110.200.111	10.110.134.68	LDAP	161	searchRequest(4) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
219	20.787813	10.110.134.68	10.110.200.111	LDAP	1990	searchResEntry(4) "CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" | searchRe…
220	20.788846	10.110.200.111	10.110.134.68	TCP	66	58997 → 389 [ACK] Seq=362 Ack=3824 Win=26192 Len=0 TSval=1368907 TSecr=262226752
221	20.791665	10.110.200.111	10.110.134.68	LDAP	73	unbindRequest(5)
222	20.791666	10.110.200.111	10.110.134.68	TCP	66	58997 → 389 [FIN, ACK] Seq=369 Ack=3824 Win=26192 Len=0 TSval=1368908 TSecr=262226752
223	20.791687	10.110.134.68	10.110.200.111	TCP	66	389 → 58997 [ACK] Seq=3824 Ack=370 Win=66304 Len=0 TSval=262226753 TSecr=1368908
224	20.791748	10.110.134.68	10.110.200.111	TCP	54	389 → 58997 [RST, ACK] Seq=3824 Ack=370 Win=0 Len=0

Logs from the AP when user authentication is success

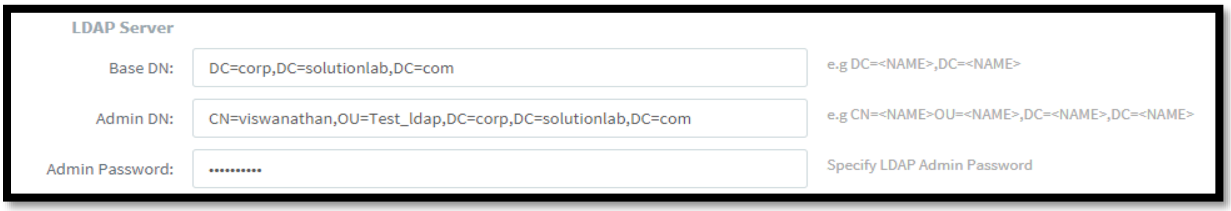


```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 10:31:05: LDAP provided session time[0], idle timeout[0], reply-msg=N/A (hotspot.c:1875)
Jun 11 10:31:05: LDAP search entries found: 1 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:228)
Jun 11 10:31:05: LDAP search status: Success for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:213)
Jun 11 10:31:05: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 10:31:05: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 10:31:05: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 10:31:05: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:167)
Jun 11 10:31:05: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:146)
Jun 11 10:31:05: Authenticating user[James] dn[CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com] from LDAP S
Jun 11 10:31:05: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
Jun 11 10:31:05: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
Jun 11 10:31:05: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 10:31:05: Handling hotspot login request for user[James] from LDAP Server[10.110.134.68]
```

Let's use another Administrative user to bind the AP with the Active directory.

"viswanathan" –is an administrative user already available in the Test_LDAP OU "admin" is the user used to authenticate the client available at default users group.

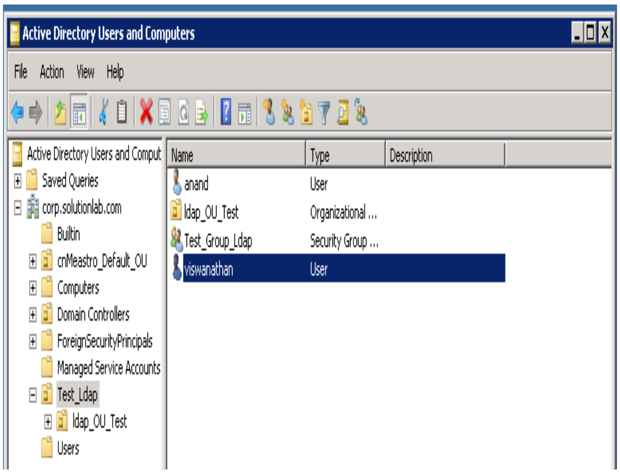
cnMaestro/ AP configuration is,



LDAP Server

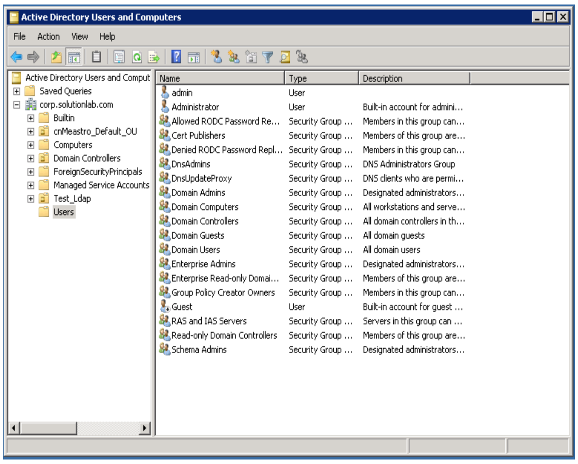
Base DN:	DC=corp,DC=solutionlab,DC=com	e.g DC=<NAME>,DC=<NAME>
Admin DN:	CN=viswanathan,OU=Test_ldap,DC=corp,DC=solutionlab,DC=com	e.g CN=<NAME>OU=<NAME>,DC=<NAME>,DC=<NAME>
Admin Password:	••••••••••	Specify LDAP Admin Password

Windows AD configuration, Bind user on the left pic and authentication user on the right pic



- Active Directory Users and Comput
  - Saved Queries
  - corp.solutionlab.com
    - Builtin
    - cnMeastro_Default_OU
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Test_Ldap
      - ldap_OU_Test
    - Users

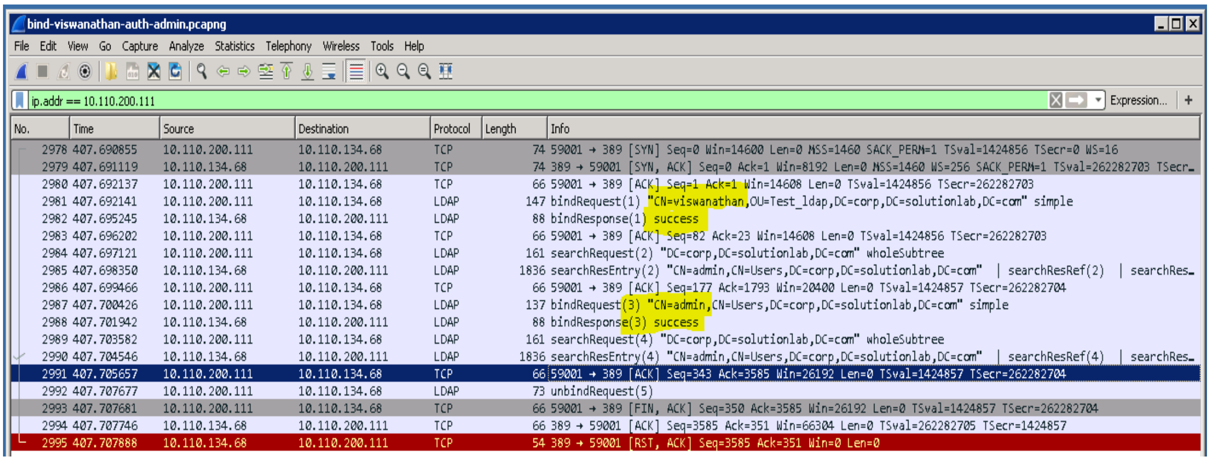
Name	Type	Description
anand	User	
ldap_OU_Test	Organizational ...	
Test_Group_Ldap	Security Group ...	
viswanathan	User	



- Active Directory Users and Comput
  - Saved Queries
  - corp.solutionlab.com
    - Builtin
    - cnMeastro_Default_OU
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Test_Ldap
    - Users

Name	Type	Description
admin	User	
Administrator	User	Built-in account for admini...
Allowed RODC Password Re...	Security Group ...	Members in this group can...
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password Repl...	Security Group ...	Members in this group can...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Enterprise Read-only Domai...	Security Group ...	Members of this group are...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...

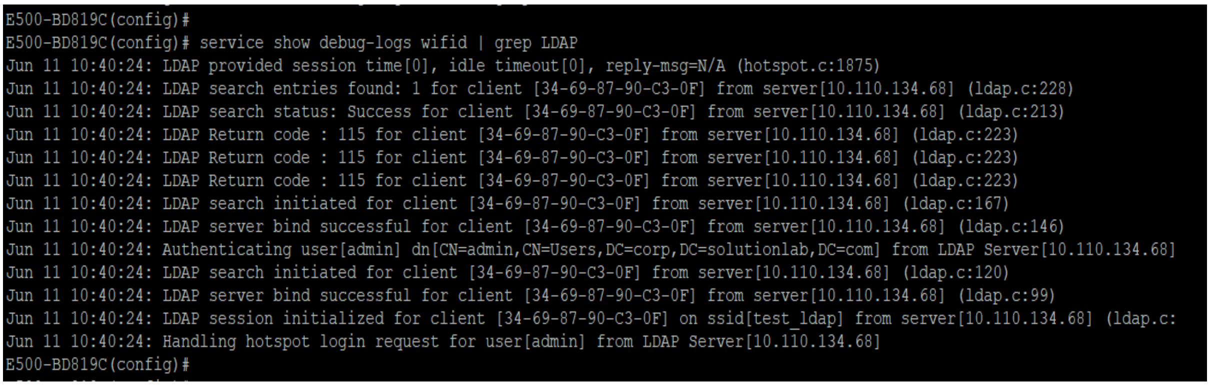
Packet capture taken from LDAP when bind is success and authentication is also success



ip.addr == 10.110.200.111

```
No.   Time        Source          Destination     Protocol Length Info
2978 407.690855 10.110.200.111  10.110.134.68   TCP        74 59001 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1424856 TSecr=0 WS=16
2979 407.691119 10.110.134.68   10.110.200.111  TCP        74 389 → 59001 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=262282703 TSecr…
2980 407.692137 10.110.200.111  10.110.134.68   TCP        66 59001 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=1424856 TSecr=262282703
2981 407.692141 10.110.200.111  10.110.134.68   LDAP      147 bindRequest(1) "CN=viswanathan,OU=Test_ldap,DC=corp,DC=solutionlab,DC=com" simple
2982 407.695245 10.110.134.68   10.110.200.111  LDAP       88 bindResponse(1) success
2983 407.696202 10.110.200.111  10.110.134.68   TCP        66 59001 → 389 [ACK] Seq=82 Ack=23 Win=14608 Len=0 TSval=1424856 TSecr=262282703
2984 407.697121 10.110.200.111  10.110.134.68   LDAP      161 searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
2985 407.698350 10.110.134.68   10.110.200.111  LDAP     1836 searchResEntry(2) "CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com"  | searchResRef(2)  | searchRes…
2986 407.699466 10.110.200.111  10.110.134.68   TCP        66 59001 → 389 [ACK] Seq=177 Ack=1793 Win=20400 Len=0 TSval=1424857 TSecr=262282704
2987 407.700426 10.110.200.111  10.110.134.68   LDAP      137 bindRequest(3) "CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com" simple
2988 407.701942 10.110.134.68   10.110.200.111  LDAP       88 bindResponse(3) success
2989 407.703582 10.110.200.111  10.110.134.68   LDAP      161 searchRequest(4) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
2990 407.704546 10.110.134.68   10.110.200.111  LDAP     1836 searchResEntry(4) "CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com"  | searchResRef(4)  | searchRes…
2991 407.705657 10.110.200.111  10.110.134.68   TCP        66 59001 → 389 [ACK] Seq=343 Ack=3585 Win=26192 Len=0 TSval=1424857 TSecr=262282704
2992 407.707677 10.110.200.111  10.110.134.68   LDAP       73 unbindRequest(5)
2993 407.707681 10.110.200.111  10.110.134.68   TCP        66 59001 → 389 [FIN, ACK] Seq=350 Ack=3585 Win=26192 Len=0 TSval=1424857 TSecr=262282704
2994 407.707746 10.110.134.68   10.110.200.111  TCP        66 389 → 59001 [ACK] Seq=3585 Ack=351 Win=66304 Len=0 TSval=262282705 TSecr=1424857
2995 407.707888 10.110.134.68   10.110.200.111  TCP        54 389 → 59001 [RST, ACK] Seq=3585 Ack=351 Win=0 Len=0
```

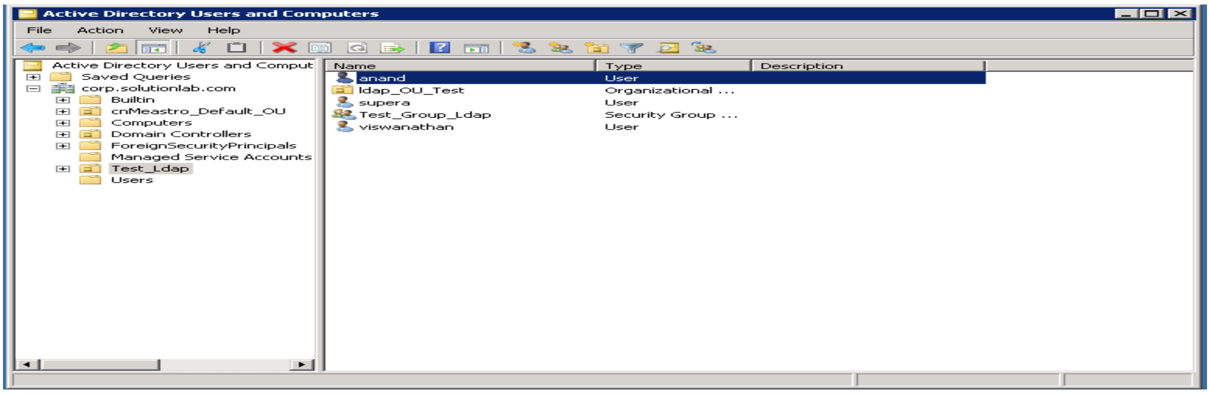
Logs from the AP when user authentication is success



```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 10:40:24: LDAP provided session time[0], idle timeout[0], reply-msg=N/A (hotspot.c:1875)
Jun 11 10:40:24: LDAP search entries found: 1 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:228)
Jun 11 10:40:24: LDAP search status: Success for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:213)
Jun 11 10:40:24: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 10:40:24: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 10:40:24: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 10:40:24: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:167)
Jun 11 10:40:24: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:146)
Jun 11 10:40:24: Authenticating user[admin] dn[CN=admin,CN=Users,DC=corp,DC=solutionlab,DC=com] from LDAP Server[10.110.134.68]
Jun 11 10:40:24: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
Jun 11 10:40:24: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
Jun 11 10:40:24: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 10:40:24: Handling hotspot login request for user[admin] from LDAP Server[10.110.134.68]
E500-BD819C(config)#
```

"anand" is the user used to authenticate the client available at Test_Ldap OU.

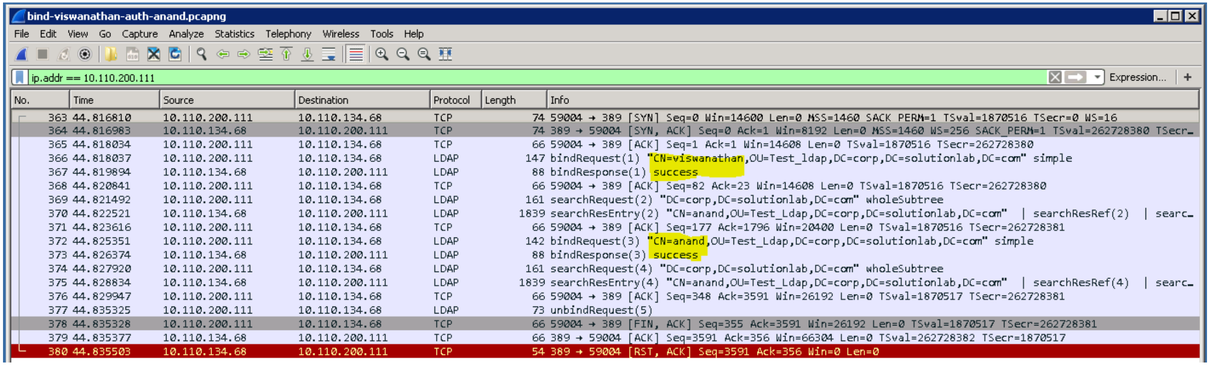
Windows AD configuration, authentication user screen shot from the Active Directory



```
Active Directory Users and Comput
  Saved Queries
  corp.solutionlab.com
    Builtin
    cnMeastro_Default_OU
    Computers
    Domain Controllers
    ForeignSecurityPrincipals
    Managed Service Accounts
    Test_Ldap
    Users
```

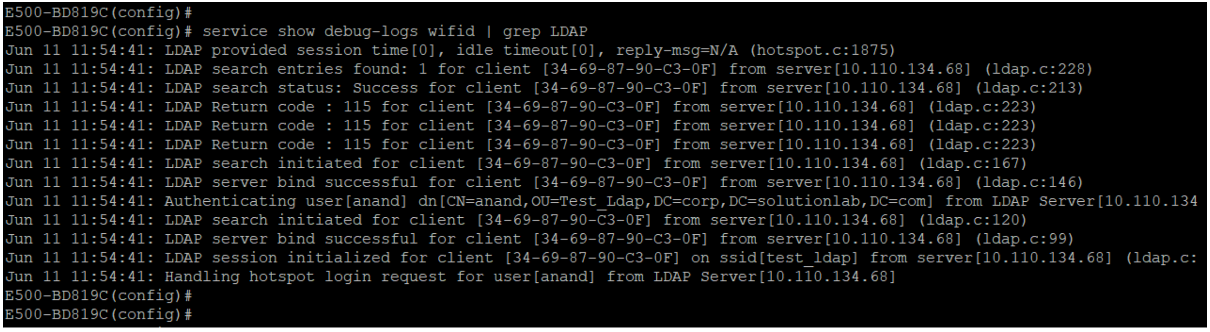
Name	Type	Description
anand	User	
ldap_OU_Test	Organizational ...	
supera	User	
Test_Group_Ldap	Security Group ...	
viswanathan	User	

Packet capture taken from LDAP when bind is success and authentication is also success



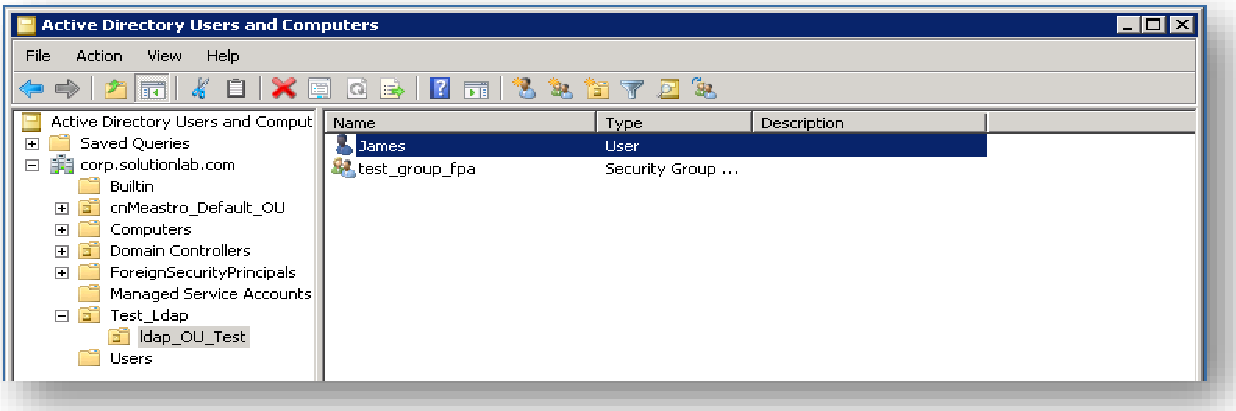
```
ip.addr == 10.110.200.111

No.   Time       Source          Destination     Protocol  Length Info
  363 44.816810  10.110.200.111  10.110.134.68   TCP        74 59004 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1870516 TSecr=0 WS=16
  364 44.816983  10.110.134.68   10.110.200.111  TCP        74 389 → 59004 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=262728380 TSecr…
  365 44.818034  10.110.200.111  10.110.134.68   TCP        66 59004 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=1870516 TSecr=262728380
  366 44.818037  10.110.200.111  10.110.134.68   LDAP      147 bindRequest(1) "CN=viswanathan,OU=Test_ldap,DC=corp,DC=solutionlab,DC=com" simple
  367 44.819894  10.110.134.68   10.110.200.111  LDAP       88 bindResponse(1) success
  368 44.820841  10.110.200.111  10.110.134.68   TCP        66 59004 → 389 [ACK] Seq=82 Ack=23 Win=14608 Len=0 TSval=1870516 TSecr=262728380
  369 44.821492  10.110.200.111  10.110.134.68   LDAP      161 searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
  370 44.822521  10.110.134.68   10.110.200.111  LDAP     1839 searchResEntry(2) "CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com"  | searchResRef(2)  | searc…
  371 44.823616  10.110.200.111  10.110.134.68   TCP        66 59004 → 389 [ACK] Seq=177 Ack=1796 Win=20400 Len=0 TSval=1870516 TSecr=262728381
  372 44.825351  10.110.200.111  10.110.134.68   LDAP      142 bindRequest(3) "CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" simple
  373 44.826374  10.110.134.68   10.110.200.111  LDAP       88 bindResponse(3) success
  374 44.827920  10.110.200.111  10.110.134.68   LDAP      161 searchRequest(4) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
  375 44.828834  10.110.134.68   10.110.200.111  LDAP     1839 searchResEntry(4) "CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com"  | searchResRef(4)  | searc…
  376 44.829947  10.110.200.111  10.110.134.68   TCP        66 59004 → 389 [ACK] Seq=348 Ack=3591 Win=26192 Len=0 TSval=1870517 TSecr=262728381
  377 44.835325  10.110.200.111  10.110.134.68   LDAP       73 unbindRequest(5)
  378 44.835328  10.110.200.111  10.110.134.68   TCP        66 59004 → 389 [FIN, ACK] Seq=355 Ack=3591 Win=26192 Len=0 TSval=1870517 TSecr=262728381
  379 44.835377  10.110.134.68   10.110.200.111  TCP        66 389 → 59004 [ACK] Seq=3591 Ack=356 Win=66304 Len=0 TSval=262728382 TSecr=1870517
  380 44.835503  10.110.134.68   10.110.200.111  TCP        54 389 → 59004 [RST, ACK] Seq=3591 Ack=356 Win=0 Len=0
```

Logs from the AP when user authentication is success



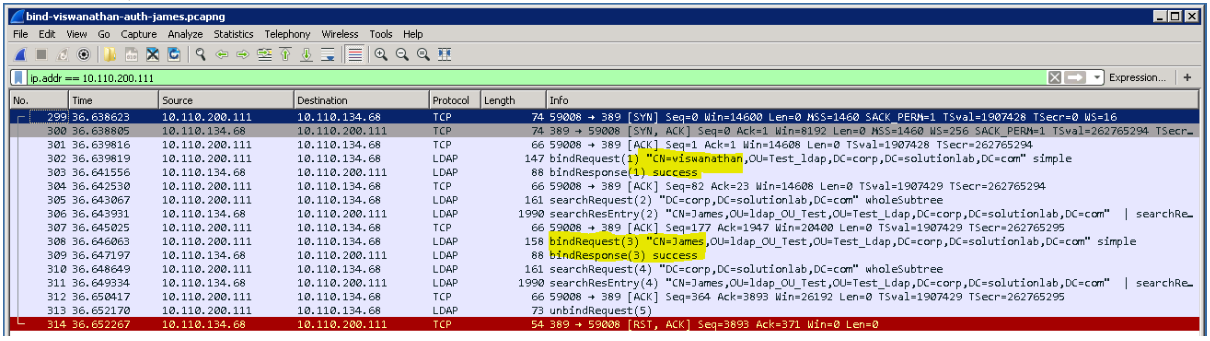
```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 11:54:41: LDAP provided session time[0], idle timeout[0], reply-msg=N/A (hotspot.c:1875)
Jun 11 11:54:41: LDAP search entries found: 1 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:228)
Jun 11 11:54:41: LDAP search status: Success for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:213)
Jun 11 11:54:41: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 11:54:41: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 11:54:41: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 11:54:41: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:167)
Jun 11 11:54:41: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:146)
Jun 11 11:54:41: Authenticating user[anand] dn[CN=anand,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com] from LDAP Server[10.110.134
Jun 11 11:54:41: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
Jun 11 11:54:41: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
Jun 11 11:54:41: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 11:54:41: Handling hotspot login request for user[anand] from LDAP Server[10.110.134.68]
E500-BD819C(config)#
E500-BD819C(config)#
```

James” is the user used to authenticate the client available at ldap_OU_Test OU which is inside the Test_Ldap OU



Name	Type	Description
James	User	
test_group_fpa	Security Group ...	

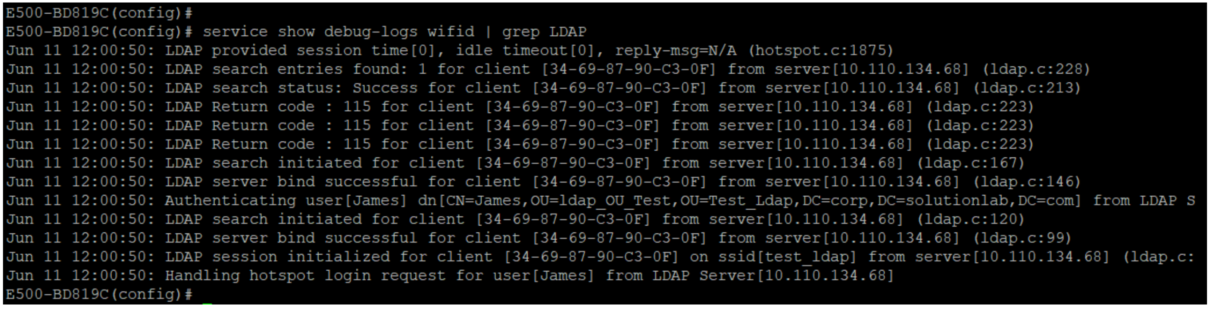
Packet capture taken from LDAP when bind is success and authentication is also success



ip.addr == 10.110.200.111

No.	Time	Source	Destination	Protocol	Length	Info
299	36.638623	10.110.200.111	10.110.134.68	TCP	74	59008 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1907428 TSecr=0 WS=16
300	36.638805	10.110.134.68	10.110.200.111	TCP	74	389 → 59008 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=262765294 TSecr…
301	36.639816	10.110.200.111	10.110.134.68	TCP	66	59008 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=1907428 TSecr=262765294
302	36.639819	10.110.200.111	10.110.134.68	LDAP	147	bindRequest(1) "CN=viswanathan,OU=Test_ldap,DC=corp,DC=solutionlab,DC=com" simple
303	36.641556	10.110.134.68	10.110.200.111	LDAP	88	bindResponse(1) success
304	36.642530	10.110.200.111	10.110.134.68	TCP	66	59008 → 389 [ACK] Seq=82 Ack=23 Win=14608 Len=0 TSval=1907429 TSecr=262765294
305	36.643067	10.110.200.111	10.110.134.68	LDAP	161	searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
306	36.643931	10.110.134.68	10.110.200.111	LDAP	1990	searchResEntry(2) "CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" | searchRe…
307	36.645025	10.110.200.111	10.110.134.68	TCP	66	59008 → 389 [ACK] Seq=177 Ack=1947 Win=20400 Len=0 TSval=1907429 TSecr=262765295
308	36.646063	10.110.200.111	10.110.134.68	LDAP	158	bindRequest(3) "CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" simple
309	36.647197	10.110.134.68	10.110.200.111	LDAP	88	bindResponse(3) success
310	36.648649	10.110.200.111	10.110.134.68	LDAP	161	searchRequest(4) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
311	36.649334	10.110.134.68	10.110.200.111	LDAP	1990	searchResEntry(4) "CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" | searchRe…
312	36.650417	10.110.200.111	10.110.134.68	TCP	66	59008 → 389 [ACK] Seq=364 Ack=3893 Win=26192 Len=0 TSval=1907429 TSecr=262765295
313	36.652170	10.110.200.111	10.110.134.68	LDAP	73	unbindRequest(5)
314	36.652267	10.110.134.68	10.110.200.111	TCP	54	389 → 59008 [RST, ACK] Seq=3893 Ack=371 Win=0 Len=0

Logs from the AP when user authentication is success

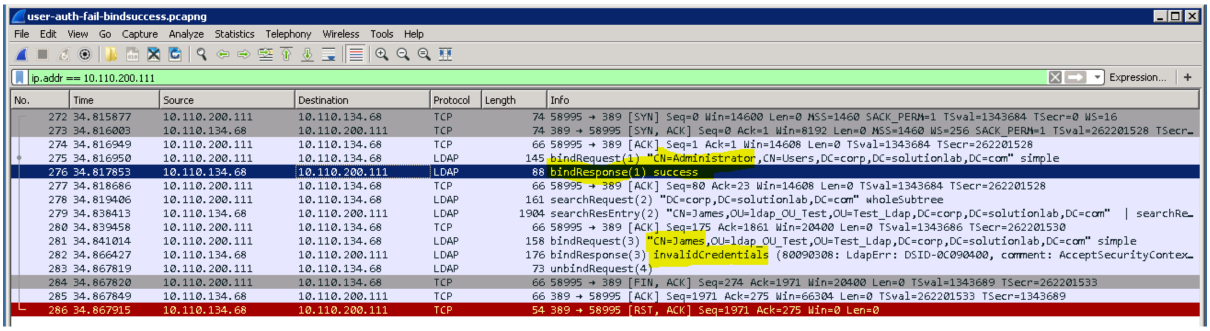


```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 12:00:50: LDAP provided session time[0], idle timeout[0], reply-msg=N/A (hotspot.c:1875)
Jun 11 12:00:50: LDAP search entries found: 1 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:228)
Jun 11 12:00:50: LDAP search status: Success for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:213)
Jun 11 12:00:50: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 12:00:50: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 12:00:50: LDAP Return code : 115 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:223)
Jun 11 12:00:50: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:167)
Jun 11 12:00:50: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:146)
Jun 11 12:00:50: Authenticating user[James] dn[CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com] from LDAP S
Jun 11 12:00:50: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
Jun 11 12:00:50: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
Jun 11 12:00:50: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 12:00:50: Handling hotspot login request for user[James] from LDAP Server[10.110.134.68]
E500-BD819C(config)#
```

How to analyse User authentication is fail

Scenario -1 - Bind is success, search is success and guest user authentication is failing (invalid credentials)

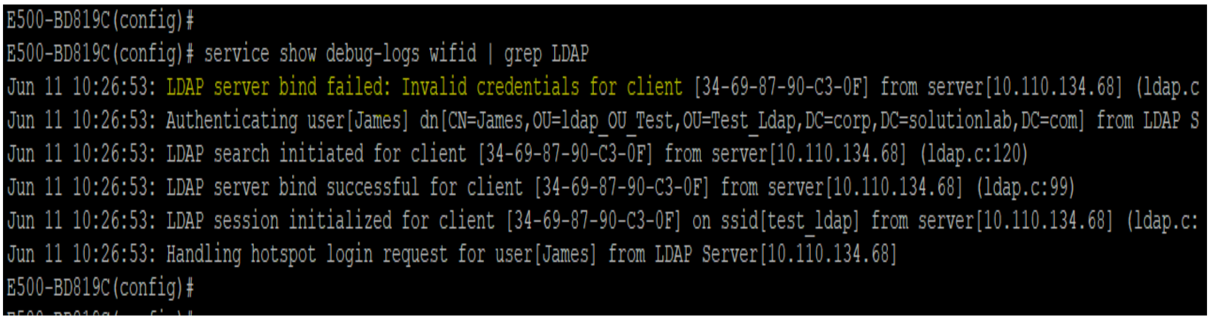
Packet capture taken from LDAP when bind is success and authentication is failure



```
user-auth-fail-bindsuccess.pcapng
ip.addr == 10.110.200.111

No.  Time       Source          Destination     Protocol Length Info
 272 34.815877  10.110.200.111  10.110.134.68   TCP        74 58995 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1343684 TSecr=0 WS=16
 273 34.816003  10.110.134.68   10.110.200.111  TCP        74 389 → 58995 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=262201528 TSecr…
 274 34.816949  10.110.200.111  10.110.134.68   TCP        66 58995 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=1343684 TSecr=262201528
 275 34.816950  10.110.200.111  10.110.134.68   LDAP      145 bindRequest(1) "CN=Administrator,CN=Users,DC=corp,DC=solutionlab,DC=com" simple
 276 34.817853  10.110.134.68   10.110.200.111  LDAP       88 bindResponse(1) success
 277 34.818686  10.110.200.111  10.110.134.68   TCP        66 58995 → 389 [ACK] Seq=80 Ack=23 Win=14608 Len=0 TSval=1343684 TSecr=262201528
 278 34.819406  10.110.200.111  10.110.134.68   LDAP      161 searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
 279 34.838413  10.110.134.68   10.110.200.111  LDAP     1904 searchResEntry(2) "CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com"  | searchRe…
 280 34.839458  10.110.200.111  10.110.134.68   TCP        66 58995 → 389 [ACK] Seq=175 Ack=1861 Win=20400 Len=0 TSval=1343686 TSecr=262201530
 281 34.841014  10.110.200.111  10.110.134.68   LDAP      158 bindRequest(3) "CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com" simple
 282 34.866427  10.110.134.68   10.110.200.111  LDAP      176 bindResponse(3) invalidCredentials (80090308: LdapErr: DSID-0C090400, comment: AcceptSecurityContex…
 283 34.867819  10.110.200.111  10.110.134.68   LDAP       73 unbindRequest(4)
 284 34.867820  10.110.200.111  10.110.134.68   TCP        66 58995 → 389 [FIN, ACK] Seq=274 Ack=1971 Win=20400 Len=0 TSval=1343689 TSecr=262201533
 285 34.867849  10.110.134.68   10.110.200.111  TCP        66 389 → 58995 [ACK] Seq=1971 Ack=275 Win=66304 Len=0 TSval=262201533 TSecr=1343689
 286 34.867915  10.110.134.68   10.110.200.111  TCP        54 389 → 58995 [RST, ACK] Seq=1971 Ack=275 Win=0 Len=0
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

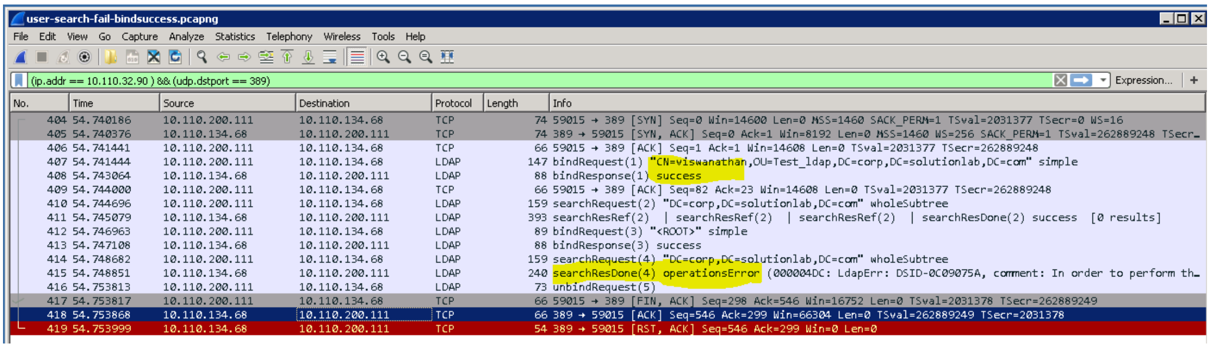
Logs from the AP when user authentication is failure and bind and search is success



```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 10:26:53: LDAP server bind failed: Invalid credentials for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c
Jun 11 10:26:53: Authenticating user[James] dn[CN=James,OU=ldap_OU_Test,OU=Test_Ldap,DC=corp,DC=solutionlab,DC=com] from LDAP S
Jun 11 10:26:53: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
Jun 11 10:26:53: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
Jun 11 10:26:53: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 10:26:53: Handling hotspot login request for user[James] from LDAP Server[10.110.134.68]
E500-BD819C(config)#
```

Scenario -2 – Bind is success, search fails and user authentication is failing

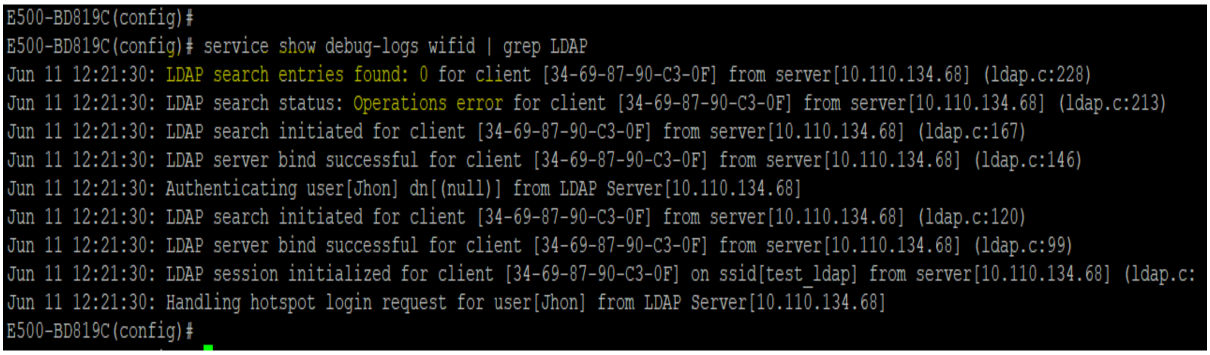
Packet capture taken from LDAP when bind is success and authentication is failure (search fails with reason OperationsError- reason user not available)



```
user-search-fail-bindsuccess.pcapng
(ip.addr == 10.110.32.90 ) && (udp.dstport == 389)

No.  Time       Source          Destination     Protocol Length Info
 404 54.740186  10.110.200.111  10.110.134.68   TCP        74 59015 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2031377 TSecr=0 WS=16
 405 54.740376  10.110.134.68   10.110.200.111  TCP        74 389 → 59015 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=262889248 TSecr…
 406 54.741441  10.110.200.111  10.110.134.68   TCP        66 59015 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=2031377 TSecr=262889248
 407 54.741444  10.110.200.111  10.110.134.68   LDAP      147 bindRequest(1) "CN=viswanathan,OU=Test_ldap,DC=corp,DC=solutionlab,DC=com" simple
 408 54.743064  10.110.134.68   10.110.200.111  LDAP       88 bindResponse(1) success
 409 54.744000  10.110.200.111  10.110.134.68   TCP        66 59015 → 389 [ACK] Seq=82 Ack=23 Win=14608 Len=0 TSval=2031377 TSecr=262889248
 410 54.744696  10.110.200.111  10.110.134.68   LDAP      159 searchRequest(2) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
 411 54.745079  10.110.134.68   10.110.200.111  LDAP      393 searchResRef(2)  | searchResRef(2)  | searchResRef(2)  | searchResDone(2) success  [0 results]
 412 54.746963  10.110.200.111  10.110.134.68   LDAP       89 bindRequest(3) "<ROOT>" simple
 413 54.747108  10.110.134.68   10.110.200.111  LDAP       88 bindResponse(3) success
 414 54.748682  10.110.200.111  10.110.134.68   LDAP      159 searchRequest(4) "DC=corp,DC=solutionlab,DC=com" wholeSubtree
 415 54.748851  10.110.134.68   10.110.200.111  LDAP      240 searchResDone(4) operationsError (000004DC: LdapErr: DSID-0C09075A, comment: In order to perform th…
 416 54.753813  10.110.200.111  10.110.134.68   LDAP       73 unbindRequest(5)
 417 54.753817  10.110.200.111  10.110.134.68   TCP        66 59015 → 389 [FIN, ACK] Seq=298 Ack=546 Win=16752 Len=0 TSval=2031378 TSecr=262889249
 418 54.753868  10.110.134.68   10.110.200.111  TCP        66 389 → 59015 [ACK] Seq=546 Ack=299 Win=66304 Len=0 TSval=262889249 TSecr=2031378
 419 54.753999  10.110.134.68   10.110.200.111  TCP        54 389 → 59015 [RST, ACK] Seq=546 Ack=299 Win=0 Len=0
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

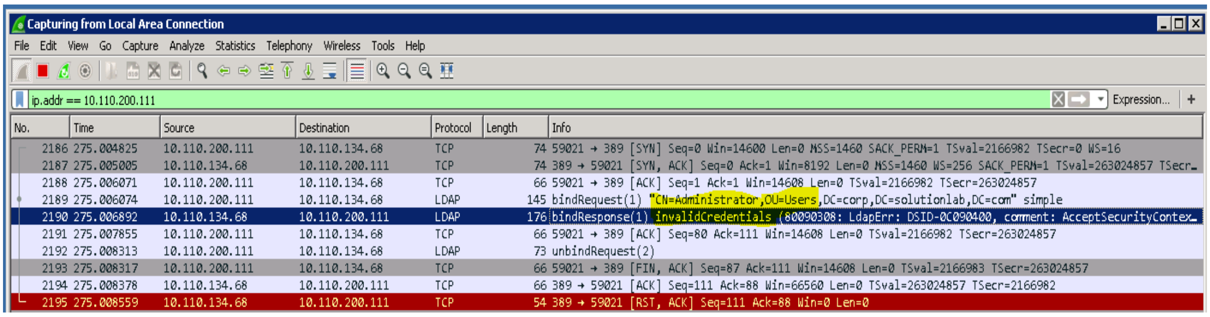
Logs from the AP when bind is success and search is failure resulting in user fail



```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 12:21:30: LDAP search entries found: 0 for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:228)
Jun 11 12:21:30: LDAP search status: Operations error for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:213)
Jun 11 12:21:30: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:167)
Jun 11 12:21:30: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:146)
Jun 11 12:21:30: Authenticating user[Jhon] dn[(null)] from LDAP Server[10.110.134.68]
Jun 11 12:21:30: LDAP search initiated for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:120)
Jun 11 12:21:30: LDAP server bind successful for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c:99)
Jun 11 12:21:30: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 12:21:30: Handling hotspot login request for user[Jhon] from LDAP Server[10.110.134.68]
E500-BD819C(config)#
```

Scenario -3 – Bind is failing, LDAP is reachable

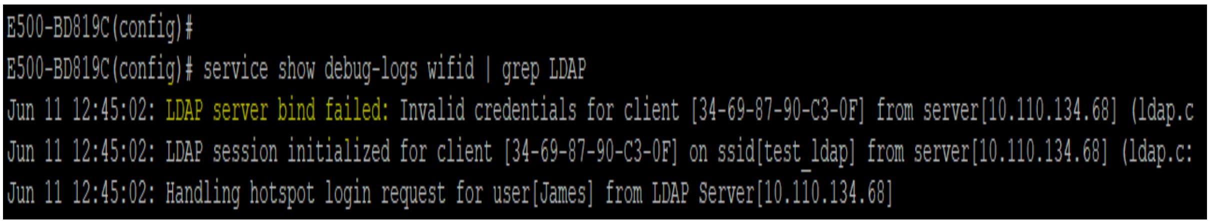
In the below capture, we can see that the OU=Users is not correct and that is the reason for the failure. Correct usage is "CN=Administrator,CN=users,…"



Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.110.200.111
Expression…

No.	Time	Source	Destination	Protocol	Length	Info
2186	275.004825	10.110.200.111	10.110.134.68	TCP	74	59021 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2166982 TSecr=0 WS=16
2187	275.005005	10.110.134.68	10.110.200.111	TCP	74	389 → 59021 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=263024857 TSecr…
2188	275.006071	10.110.200.111	10.110.134.68	TCP	66	59021 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=2166982 TSecr=263024857
2189	275.006074	10.110.200.111	10.110.134.68	LDAP	145	bindRequest(1) "CN=Administrator,OU=Users,DC=corp,DC=solutionlab,DC=com" simple
2190	275.006892	10.110.134.68	10.110.200.111	LDAP	176	bindResponse(1) invalidCredentials (80090308: LdapErr: DSID-0C090400, comment: AcceptSecurityContex…
2191	275.007855	10.110.200.111	10.110.134.68	TCP	66	59021 → 389 [ACK] Seq=80 Ack=111 Win=14608 Len=0 TSval=2166982 TSecr=263024857
2192	275.008313	10.110.200.111	10.110.134.68	LDAP	73	unbindRequest(2)
2193	275.008317	10.110.200.111	10.110.134.68	TCP	66	59021 → 389 [FIN, ACK] Seq=87 Ack=111 Win=14608 Len=0 TSval=2166983 TSecr=263024857
2194	275.008378	10.110.134.68	10.110.200.111	TCP	66	389 → 59021 [ACK] Seq=111 Ack=88 Win=66560 Len=0 TSval=263024857 TSecr=2166982
2195	275.008559	10.110.134.68	10.110.200.111	TCP	54	389 → 59021 [RST, ACK] Seq=111 Ack=88 Win=0 Len=0

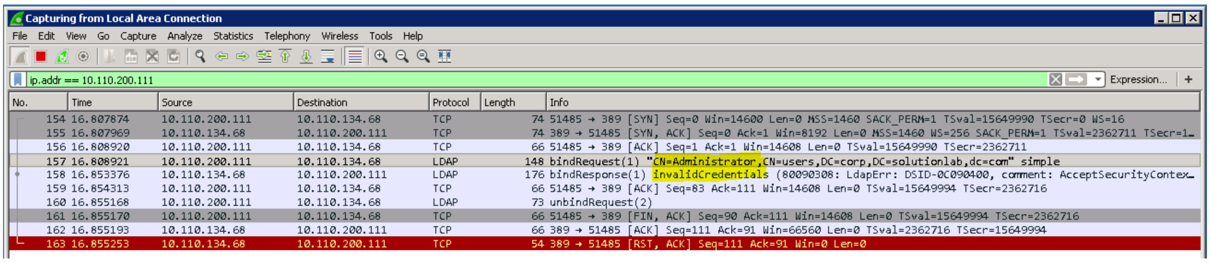
Logs from the AP when bind is failing



```
E500-BD819C(config)#
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 11 12:45:02: LDAP server bind failed: Invalid credentials for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c
Jun 11 12:45:02: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 11 12:45:02: Handling hotspot login request for user[James] from LDAP Server[10.110.134.68]
```

Scenario -4 – Bind is failing, LDAP is reachable, Administrator Password is wrong

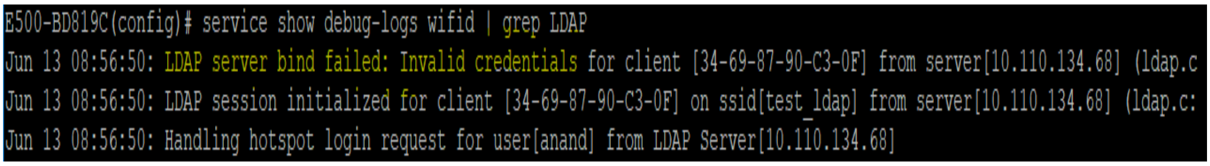
In the below capture, we can see that the response for bind request is invalid credentials.



Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.110.200.111
Expression…

No.	Time	Source	Destination	Protocol	Length	Info
154	16.807874	10.110.200.111	10.110.134.68	TCP	74	51485 → 389 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=15649990 TSecr=0 WS=16
155	16.807969	10.110.134.68	10.110.200.111	TCP	74	389 → 51485 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=2362711 TSecr=1…
156	16.808920	10.110.200.111	10.110.134.68	TCP	66	51485 → 389 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=15649990 TSecr=2362711
157	16.808921	10.110.200.111	10.110.134.68	LDAP	148	bindRequest(1) "CN=Administrator,CN=users,DC=corp,DC=solutionlab,dc=com" simple
158	16.853376	10.110.134.68	10.110.200.111	LDAP	176	bindResponse(1) invalidCredentials (80090308: LdapErr: DSID-0C090400, comment: AcceptSecurityContex…
159	16.854313	10.110.200.111	10.110.134.68	TCP	66	51485 → 389 [ACK] Seq=83 Ack=111 Win=14608 Len=0 TSval=15649994 TSecr=2362716
160	16.855168	10.110.200.111	10.110.134.68	LDAP	73	unbindRequest(2)
161	16.855170	10.110.200.111	10.110.134.68	TCP	66	51485 → 389 [FIN, ACK] Seq=90 Ack=111 Win=14608 Len=0 TSval=15649994 TSecr=2362716
162	16.855193	10.110.134.68	10.110.200.111	TCP	66	389 → 51485 [ACK] Seq=111 Ack=91 Win=66560 Len=0 TSval=2362716 TSecr=15649994
163	16.855253	10.110.134.68	10.110.200.111	TCP	54	389 → 51485 [RST, ACK] Seq=111 Ack=91 Win=0 Len=0

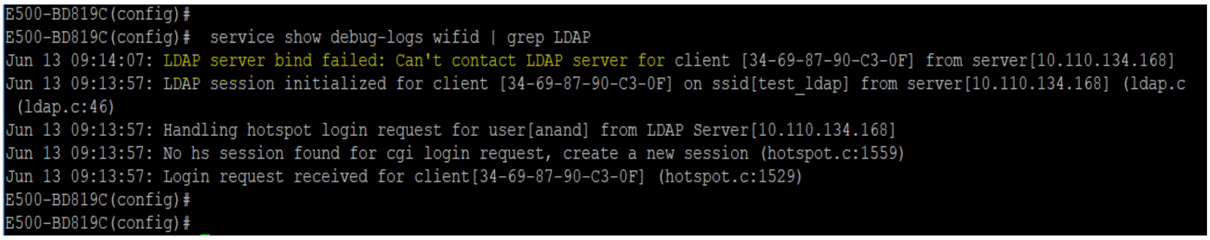
Logs from the AP when bind is failing



```
E500-BD819C(config)# service show debug-logs wifid | grep LDAP
Jun 13 08:56:50: LDAP server bind failed: Invalid credentials for client [34-69-87-90-C3-0F] from server[10.110.134.68] (ldap.c
Jun 13 08:56:50: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.68] (ldap.c:
Jun 13 08:56:50: Handling hotspot login request for user[anand] from LDAP Server[10.110.134.68]
```

Scenario -5 – Bind is failing, LDAP is not reachable,

Logs from the AP when bind is failing



```
E500-BD819C(config)#
E500-BD819C(config)#  service show debug-logs wifid | grep LDAP
Jun 13 09:14:07: LDAP server bind failed: Can't contact LDAP server for client [34-69-87-90-C3-0F] from server[10.110.134.168]
Jun 13 09:13:57: LDAP session initialized for client [34-69-87-90-C3-0F] on ssid[test_ldap] from server[10.110.134.168] (ldap.c
 (ldap.c:46)
Jun 13 09:13:57: Handling hotspot login request for user[anand] from LDAP Server[10.110.134.168]
Jun 13 09:13:57: No hs session found for cgi login request, create a new session (hotspot.c:1559)
Jun 13 09:13:57: Login request received for client[34-69-87-90-C3-0F] (hotspot.c:1529)
E500-BD819C(config)#
E500-BD819C(config)#
```