



# LDAP Configuration Examples

Avi Technical Reference (v18.2)

Copyright © 2020

# LDAP Configuration Examples

[view online](#)

## LDAP authentication profile examples

- Active Directory common settings: with Administrator bind, group membership tends to include full user DN.

Name *	LDAP AD Example I	Type	LDAP TACACS+
LDAP Servers	<input type="text" value="10.10.1.151"/> <input type="text" value="10.10.1.152"/> <input type="text" value="10.10.1.153"/> + Add LDAP Server	LDAP Port	<input type="text" value="636"/>
Base DN	<input type="text" value="dc=example,dc=com"/>	<input checked="" type="checkbox"/> Secure LDAP using TLS	
	<input checked="" type="radio"/> Administrator Bind <input type="radio"/> Anonymous Bind	Admin Bind Password	<input type="text" value="Password"/>
Admin Bind DN	<input type="text" value="cn=Administrator,cn=Users,dc=example,dc=com"/>	Group Search DN	<input type="text" value="cn=Groups, dc=example,dc=com"/>
User Search DN	<input type="text" value="cn=Users,dc=example,dc=com"/>	Group Search Scope	Scope Subtree
User Search Scope	Scope One	Group Filter	<input type="text" value="(objectCategory=group)"/>
User ID Attribute *	<input type="text" value="samAccountName"/>	Group Member Attribute	<input type="text" value="member"/>
		<input checked="" type="checkbox"/> Group member attribute is full DN	
		<input type="checkbox"/> Ignore Referrals	

- Active Directory common settings: with Anonymous bind. If LDAP/AD user can bind with the DN `jdoe@example.com` and password, it validates the user login

Name *	LDAP AD Example II	Type	LDAP TACACS+
LDAP Servers	<input type="text" value="10.10.1.151"/> <input type="text" value="10.10.1.152"/> <input type="text" value="10.10.1.153"/> + Add LDAP Server	LDAP Port	<input type="text" value="636"/>
Base DN	<input type="text" value="dc=example,dc=com"/>	<input checked="" type="checkbox"/> Secure LDAP using TLS	
	<input type="radio"/> Administrator Bind <input checked="" type="radio"/> Anonymous Bind	User ID Attribute	<input type="text" value="samAccountName"/>
User DN Pattern *	<input type="text" value="&lt;user&gt;@example.com"/>	User Token	<input type="text" value="&lt;user&gt;"/>

- OpenLDAP settings: with Administrator bind.

The screenshot shows the configuration for an OpenLDAP server named "OpenLDAP Example II". The Type is set to "LDAP". LDAP Servers are listed as 10.10.23.121, 10.10.23.122, and 10.10.23.123. The Base DN is "dc=example,dc=com". The Administrator Bind option is selected. The Admin Bind DN is "cn=admin,dc=example,dc=com" and the Admin Bind Password is masked. The User Search DN is "ou=people,dc=example,dc=com" with a search scope of "Scope One" and user ID attribute of "uid". The Group Search DN is "ou=Groups,dc=example,dc=com" with a search scope of "Scope Subtree" and group filter of "(objectClass=\*)". The Group Member Attribute is "memberUid".

- OpenLDAP settings: with Anonymous bind, If LDAP user can bind with the DN "cn=jdoe, ou=People, dc=example, dc=com" and password, it validates the user login

The screenshot shows the configuration for an OpenLDAP server named "OpenLDAP Example II". The Type is set to "LDAP". LDAP Servers are listed as 10.10.23.121, 10.10.23.122, and 10.10.23.123. The Base DN is "dc=example,dc=com". The Anonymous Bind option is selected. The User DN Pattern is "cn=<user>,ou=People,dc=example,dc=com" and the User ID Attribute is "cn". The User Token is "<user>".

- Secure vs Non-Secure LDAP settings: typically LDAP uses port 389 for clear text, port 636 for LDAPS. Where possible LDAPS is preferable. Just port alone does not determine LDAP security mode, hence administrator should explicitly check the box to indicate whether secure LDAP is in use or not.

LDAP Port ?

389

Secure LDAP using TLS ?

LDAP Port ?

636

Secure LDAP using TLS ?

- Group Filter, (objectClass=\*): safest option to set and will ensure every object is assumed as an LDAP group and searched for members. least optimal.

Group Search Scope ?

Scope Subtree

Group Filter ?

(objectClass=\*)

Group Member Attribute ?

member

- Group Filter, (objectCategory=group): typically group objects in LDAP have a category value set to "group".
  - Documentation from Active Directory: If you have a choice between using objectCategory and objectClass, it is recommended that you use objectCategory. That is because objectCategory is both single valued and

indexed, while objectClass is multi-valued and not indexed (except on Windows Server 2008 and above). A query using a filter with objectCategory will be more efficient than a similar filter with objectClass. Windows Server 2008 domain controllers (and above) have a special behavior that indexes the objectClass attribute.

The screenshot shows a configuration panel with three sections: 'Group Search Scope' with a dropdown menu set to 'Scope Subtree', 'Group Filter' with a text input field containing '(objectCategory=group)', and 'Group Member Attribute' with a text input field containing 'member'. Each section has a question mark icon for help.

- Group Filter, (objectClass=posixGroup): openLDAP groups can in some environments be of type "posixGroup" instead of just "group".

The screenshot shows a configuration panel with three sections: 'Group Search Scope' with a dropdown menu set to 'Scope Subtree', 'Group Filter' with a text input field containing '(objectClass=posixGroup)', and 'Group Member Attribute' with a text input field containing 'member'. Each section has a question mark icon for help.

- Group Filter, more complex options: (&(objectCategory=group)(cn=Avi-\*)) -- if all known groups of interest start with the name "Avi-"; the search can avoid fetching other groups. Some organizations have thousands of groups in some hierarchy and its preferable to filter them based on known scenarios.

Group Search Scope ?

Scope Subtree

Group Filter ?

(&(objectCategory=group)(cn=Avi-\*))

Group Member Attribute ?

member

- Group member is full DN or not? Auth Profile test page can print the full DN tree from base DN level. For group entries the member attribute value shows whether it is full DN or not.

### Verify Auth Profile: LDAP AD Example I

Name

LDAP AD Example I

Test user entry
  Test user group membership
  Test base DN

Results

```

dn: CN=Enterprise Admins,CN=Users,DC=avi,DC=local
objectClass: top
objectClass: group
cn: Enterprise Admins
description: Designated administrators of the enterprise
member: CN=jenkins test4,CN=Users,DC=avi,DC=local
member: CN=jenkins test3,CN=Users,DC=avi,DC=local
member: CN=Administrator,CN=Users,DC=avi,DC=local
distinguishedName: CN=Enterprise Admins,CN=Users,DC=avi,DC=local
instanceType: 4
whenCreated: 20130405220838.0Z
whenChanged: 20150806101658.0Z
uSNCreated: 7697
memberOf: CN=Denied RODC Password Replication Group,CN=Users,DC=avi,DC=local
memberOf: CN=Administrators,CN=Builtin,DC=avi,DC=local
uSNChanged: 83519
name: Enterprise Admins
objectGUID:: 91BXi/s9R0Si5rMpZHsuw==
    
```

- **Ignore referrals:** this is a useful option if LDAP group search is delayed due to unnecessary referral searches. When enabled, the group search will skip referrals links that connect to another LDAP server.

<b>Group Search Scope</b> ?
Scope Subtree
<b>Group Filter</b> ?
(objectClass=*)
<b>Group Member Attribute</b> ?
member
<input checked="" type="checkbox"/> Group member attribute is full DN ?
<input checked="" type="checkbox"/> Ignore Referrals ?