

LDAP Authentication

LDAP Authentication

To setup an LDAP server for authentication, you must perform the following three procedures:

- LDAP Authentication
 - Configure the LDAP Server:
 - LDAP Schema - Example
 - Creating a LDAP User:
 - Test the LDAP Server
 - Configure ProVision for LDAP Authentication

Configure the LDAP Server:

Configuring the LDAP server involves ((adding the schema)) and adding LDAP users / groups to the server:

LDAP Schema - Example

```
attributetype (1.3.6.1.4.1.5023215.2.3.21 NAME 'sixConnGroup' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
objectclass ( 1.3.6.1.4.1.5023215.2.4.2 NAME 'sixConnectPermissionsV2' DESC '6Connect Permissions Object v2'
SUP top AUXILIARY MUST ( sixConnGroup ) )
```

Creating a LDAP User:

SSH into your openLDAP server and create a new 'ldif' file. Example:

```
dn: cn=JoeSmith,ou=people,dc=6connect,dc=com
cn: JoeSmith
sn: JoeSmith
objectclass: top
objectclass: person
objectclass: sixConnectPermissionsV2
sixConnGroup: "Global Admins"
sixConnGroup: "IT Engineering"
sixConnGroup: "Sales"
sixConnGroup: "Customer Admin"
userPassword: testpass
```

To create a new user, make a new ldif file and change all instances of "JoeSmith" to whatever username you wish to create and update the password. Keep all of the object class definitions as listed above. Add a sixConnGroup declaration for each ProVision user group a user is in.

After the file is created, run the following command to add the new user to LDAP server:

```
ldapadd -h [SERVER] -x -f [LDIF FILE] -D [ROOTDN] -w [ROOT PW] -v
```

Example:

```
ldapadd -h localhost -x -f 6connect.ldif -D "cn=Manager,dc=6connect,dc=com" -w secret -v
```

The user will now be active in openLDAP and can be used to login to ProVision.

Test the LDAP Server

To query the LDAP server, run the following command on any server which has openLDAP enabled:

```
ldapsearch -b [BASE] -h [IPADDRESS] -D [DOMAIN] -w [PASSWORD] [USER]
```

Note: We have not been able to use a v6 address at with this tool, even though multiple sources say it should work.

At the end of the command where [USER] is specified, user or groups can be used (in LDAP format) to query.

Example:

```
ldapsearch -b "dc=6connect,dc=com" -h 50.240.195.129 -D "cn=Mayor,ou=people,dc=6connect,dc=com" -w testpass "cn=MajorMiner"
```

Configure ProVision for LDAP Authentication

To configure the use of LDAP authentication with ProVision, follow the steps below.

- Log into 6connect ProVision
- Go to Admin -> General Settings -> Authentication
- Click the LDAP Enable checkbox.
- Fill in the hostname or ip address, authentication port, LDAP Security, Auth DN, and Fetch DN.

The screenshot shows the 'Authentication Options' configuration page in ProVision. On the left, a sidebar lists 'Radius', 'LDAP' (selected), 'SAML Service', and 'DUO Mobile'. The main content area has a green banner stating 'LDAP functions are available.' Below this, the 'LDAP Enable' toggle is turned 'ON'. Fields for 'LDAP Server Address', 'LDAP Port', and 'LDAP Security' (set to 'None') are present, along with a 'Test Server' button. The 'LDAP Auth DN List' section contains five empty text boxes. The 'LDAP Fetch DN' and 'LDAP Group Attribute' fields are also empty. At the bottom, there is explanatory text about DN strings and a 'Save Changes' button.

Authentication Options

Radius

LDAP

SAML Service

DUO Mobile

LDAP functions are available.

LDAP Enable: ☒ ON

LDAP Server Address:

LDAP Port:

LDAP Security:

Test Server

LDAP Auth DN List:

LDAP Fetch DN:

LDAP Group Attribute:

The DN strings used to first authenticate the 6connect user and then to retrieve their permissions.

The string '%LOGIN%' should be inserted in place of the user's common name in both strings.

ex: cn=%LOGIN%,ou=people,dc=6connect,dc=com

Each Auth DN string will be tried in order until a user successfully authenticates.

LDAP servers must either be configured with the 6connect schema, located [here](#), or have an internal list of user groups defined by the LDAP Group Attribute above. If a Group Attribute is set it will be used. If no Group Attribute is present the 6connect schema will be used. If both fail then users will not be able to log in to ProVision.

Save Changes

Example values in this case would be:

LDAP Enable: (Checked)

LDAP Server Address: 52.240.195.12

LDAP Port: 389 (or SSL/TLS port is 636)

LDAP Security: None

LDAP Auth DN: cn=%LOGIN%,ou=people,dc=6connect,dc=com

LDAP Fetch DN: cn=%LOGIN%



Setting default login authentication options

In the login screen, you would select the authentication method from the dropdown. If you like, you can set the default login option in the following way:

Go to the /data/globals.php and open in vi (or other editor). Add in the following text as the last line of the file (before the closing ?>)

```
define('DEFAULT_LOGIN_TYPE', 'radius');
```

Acceptable values are "local", "radius" and "ldap". If this line is not present in globals.php, the default option is "local".



Using SSL encryption

To use SSL encryption with LDAP, the ldap.conf file must be correctly configured on the ProVision server.

Typically, the LDAP configuration file is kept at "/etc/ldap/ldap.conf". Make sure the following line is present:

```
TLS_REQCERT allow
```

and restart the webserver.