OpenLDAP Installation (eduroam & federated services)

These steps document the installation and setup of OpenLDAP to support eduroam and to act as an identity source for use with other trust and identity services.

I will be using Ubuntu 18.04 LTS with hardware specifications of 4GB RAM and 32GB of HDD. The. server is configured with a public IP and domain **iam**. ubuntunet.net

dc=ubuntunet, dc=net

#++++++++++++++++++

shows that enclosed contents are part of a configuration file.

#++++++++++++++++++

#++++++++++++++++++ The next line(s) is/are output of a command

Step-by-step guide

Base Installation

Step 1: Update the server repos and install prerequisite applications (This will prompt you to enter an Administrator Password on the 'Configuring slapd' screen. Please enter a password of choice such as **ldapx2021)**:

```
sudo apt update
sudo apt install slapd ldap-utils gnutls-bin ssl-cert vim
```

Step 2: Reconfigure slapd - this to ensure extra options are further configured. A prompt with different options will be presented, please enter them appropriately.

```
sudo dpkg-reconfigure slapd
#++++++++++++++++++
```

- Omit OpenLDAP server configuration? No
- DNS domain name: ubuntunet.net (use the server's domain name as this will form the tree: dc=ubuntunet, dc=net)
- Organization name: Your Institute (This will simply be added to the base entry as the name of your institute)
- Administrator password: ldapx2021
- Confirm password: must match the above
- Database backend to use: HDB (out of the choices, this has the most functionality)
- Do you want the database to be removed when slapd is purged? (your choice. Choose Yes to allow a completely clean removal, choose No to save your data even when the software is removed)
- Move old database? Yes

Certificates

Step 3: Create the certificate templates to be used for generating certificate-key pairs (one for the certificate authority and the other for the LDAP service)

3.1: Make a directory to store the templates, create the certificate authority template and open it in a text editor. Add the following contents

```
sudo mkdir /etc/ssl/templates
```

```
sudo vim /etc/ssl/templates/ca_server.conf
```

```
#+++++++++++++++
cn = LDAP Server CA
ca
cert_signing_key
#+++++++++++++++
```

3.2 Create the LDAP server certificate configuration and open it in a a text editor. Add the following contents (Please replace the organisation and cn accordingly. cn = server FQDN):

```
sudo vim /etc/ssl/templates/ldap_server.conf

#++++++++++++++++
organization = "UbuntuNet Alliance"
cn = iam.ubuntunet.net
tls_www_server
encryption_key
signing_key
expiration_days = 3652
#++++++++++++++++
```

3.3 Create the CA key and certificate using the certtool utility (the key will be stored in /etc/ssl/private and the certificate in /etc/ssl/certs)

```
sudo certtool -p --outfile /etc/ssl/private/ca_server.key

sudo certtool -s --load-privkey /etc/ssl/private/ca_server.key --template /etc/ssl/templates/ca_server.conf --
outfile /etc/ssl/certs/ca_server.pem
```

3.4 Create the LDAP service key and certificate using the certtool utility

```
sudo certtool -p --sec-param high --outfile /etc/ssl/private/ldap_server.key

sudo certtool -c --load-privkey /etc/ssl/private/ldap_server.key --load-ca-certificate /etc/ssl/certs/ca_server.
pem --load-ca-privkey /etc/ssl/private/ca_server.key --template /etc/ssl/templates/ldap_server.conf --outfile /etc
/ssl/certs/ldap_server.pem
```

3.5 Give OpenLDAP access to the LDAP server key

3.5.1 Set the appropriate permissions

```
sudo usermod -aG ssl-cert openldap

sudo chown :ssl-cert /etc/ssl/private/ldap_server.key

sudo chmod 640 /etc/ssl/private/ldap_server.key
```

3.5.2 Configure OpenLDAP to use the certificate and keys (our configuration changes shall be put in addcerts.ldif)

```
cd ~
vim addcerts.ldif

#++++++++++++++++
dn:cn=config
changetype:modify
replace:olcTLSCACertificateFile
olcTLSCACertificateFile:/etc/ssl/certs/ca_server.pem
-
replace:olcTLSCertificateFile
olcTLSCertificateFile:/etc/ssl/certs/ldap_server.pem
-
replace:olcTLSCertificateKeyFile
olcTLSCertificateKeyFile:/etc/ssl/private/ldap_server.key
#++++++++++++++++
```

3.5.3 Apply changes to the OpenLDAP system

```
# On one console, stop the slapd service and start in debug mode
sudo service slapd stop
sudo slapd -h ldapi:/// -u openldap -g openldap -d 65 -F /etc/ldap/slapd.d/ -d 65

# On another console, use ldapmodify to add the changes
sudo ldapmodify -H ldapi:// -Y EXTERNAL -f addcerts.ldif

# Stop the debug mode and restart the service
sudo service slapd start
```

3.6 Configure the OpenLDAP server with system-wide configurations for use with LDAP utilities

```
sudo cp /etc/ssl/certs/ca_server.pem /etc/ldap/ca_certs.pem


# Please uncomment the TLS_CACERT line in this file, and the the contents that follow below:
sudo vim /etc/ldap/ldap.conf
```

```
#+++++++++++++++
TLS_CACERT /etc/ldap/ca_certs.pem
TLS_REQCERT allow
#+++++++++++++++
```

3.7 Test STARTTLS and you should get the output below:

```
sudo ldapwhoami -H ldap:// -x -ZZ
```

```
anonymous
```

eduPerson & SHAC Schema

Step 4.1: Get the eduPerson and SHAC schemas downloaded as below:

```
wget https://wiki.ubuntunet.net/download/attachments/59015170/eduperson-201602.ldif
wget https://wiki.ubuntunet.net/download/attachments/59015170/SCHAC.ldif
```

Step 4.2 Load the schemas:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f eduperson-201602.ldif

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f SCHAC.ldif
```

OpenLDAP Test Users/Groups

Step 5.1: Create an LDIF file (ubuntunet.ldif - use your institution name)with institution details:

```
#++++++++++++++++++++

dn: ou=people,dc=ubuntunet,dc=net
objectClass: organizationalUnit
objectClass: top
ou: People

dn: ou=group,dc=ubuntunet,dc=net
objectClass: organizationalUnit
objectClass: top
ou: Group
description: All groups

dn: ou=servers,dc=ubuntunet,dc=net
description: servers
objectClass: top
objectClass: organizationalUnit
ou: servers

dn: cn=iam,ou=servers,dc=ubuntunet,dc=net
cn: idp
description: Identity Server
ipHostNumber: 3ffe: ffff: ffff: : 9
objectClass: top
objectClass: device
objectClass: ipHost
objectClass: simpleSecurityObject
userPassword: {crypt}iampass21

#+++++++++++++++++++++
```

Step 5.2: Add the above information to the LDAP directory (You will be prompted for the admin password set earlier in Step 1)

```
sudo ldapadd -H ldap:// -x -D "cn=admin,dc=ubuntunet,dc=net" -W -Z -f ubuntunet.ldif
```

Step 5.3 Create a Posix Group with a gidNumber and link a user to it as adm.ldif

```
#++++++++++++++++++
dn: cn=adm,ou=group,dc=ubuntunet,dc=net
cn: adm
description: System Admin Staff
gidNumber: 1000
objectClass: posixGroup
objectClass: top

dn: uid=alex.mwotil,ou=people,dc=ubuntunet,dc=net
cn: Mwotil alex
uid: alex.mwotil
uidNumber: 1001
gidNumber: 1000
givenName: Mwotil Alex
homeDirectory: /dev/null
homePhone: none
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: eduPerson
objectClass: posixAccount
objectClass: schacEntryMetadata
objectClass: schacLinkageIdentifiers
objectClass: extensibleObject
objectClass: top
objectClass: shadowAccount
sn: Mwotil
mobile: +256772123456
userPassword: Alex.pass77
mail: alex.mwotil@ubuntunet.net
email: mwotila@gmail.com
eduPersonAffiliation: staff

#+++++++++++++++++
```

Step 5.4 Add the above information to the LDAP directory (You will be prompted for the admin password set earlier in Step 1)

```
sudo ldapadd -H ldap:// -x -D "cn=admin,dc=ubuntunet,dc=net" -W -Z -f adm.ldif
```

Samba Integration

Step 6.1: Install SambaLDAP packages

```
sudo apt-get install samba smbldap-tools
```

Step 6.2: Copy and uncompress the samba schema file

```
sudo cp /usr/share/doc/samba/examples/LDAP/samba.schema.gz /etc/ldap/schema
sudo gzip -d /etc/ldap/schema/samba.schema.gz
```

Step 6.3: Create schema_convert.conf with the following:

```
#++++++++++++++++++
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/ldapns.schema
include /etc/ldap/schema/pmi.schema
include /etc/ldap/schema/samba.schema
#++++++++++++++++++
```

Step 6.4: Create a temporary file to hold the output

```
mkdir /tmp/ldif_output
```

Step 6.5: Determine the index of the schema (This returns 14 on the instance here)

```
slapcat -f schema_convert.conf -F ldif_output -n 0 | grep samba,cn=schema
```

Step 6.2: Convert the schema to LDIF format

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -H ldap:///cn={14}samba,cn=schema,cn=config -l cn=samba.
ldif
```

Step 6.2: Edit the generated cn=samba.ldif file to remove the index information on line 1 and line 3. This should now look as below:

```
dn: cn=samba,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: samba
```

Step 6.3: Also remove the bottom lines (Some of your attributes will vary):

```
structuralObjectClass: olcSchemaConfig
entryUUID: 6fe23ace-2652-103b-8ede-c19ae983d8e2
creatorsName: cn=config
createTimestamp: 20210331095140Z
entryCSN: 20210331095140.717718Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20210331095140Z
```

Step 6.2: Load the new samba schema to LDAP

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=samba.ldif
```

Step 6.2: View the new schema

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config 'cn=*samba*'
```

Step 6.2: Create the indices (samba_indices.ldif) to Samba attributes for improved search:

```
#+++++++++++++++++++
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: loginShell eq
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
#+++++++++++++++++++
```

Step 6.2: Load and search the new indices

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f samba_indices.ldif
```

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config olcDatabase={1}hdb olcDbIndex
```

Step 6.3: Retrieve the Samba domain SID

```
sudo net getlocalsid # Your output will be different from below:
#+++++++++++++++++++
SID for domain IAM is: S-1-5-21-2419233158-1789257387-3832146290
```

Step 6.3: Open the **smbldap.conf** and **smbldap_bind.conf** files and edit them with the correct LDAP settings

```
sudo cp /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz /etc/smbldap-tools/
sudo cp /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf /etc/smbldap-tools/
sudo gzip -d /etc/smbldap-tools/smbldap.conf.gz
```

Step 6.4: Modify **/etc/smbldap-tools/smbldap.conf** with the settings as per your LDAP installation:

```
sudo vi /etc/smbldap-tools/smbldap.conf

#++++++++++++++++++

[...]
SID="S-1-5-21-2419233158-1789257387-3832146290" ## Replace with your Domain SID ##
sambaDomain="IAM"  ## Enter your Domain name ##
#slaveLDAP="ldap://ldap.example.com/"  ## Make it comment, we don't have slave LDAP ##
masterLDAP="ldap://iam.ubuntunet.net/"  ## Enter your LDAP Domain name ##
ldapTLS="1" ## We use TLS, so set it to "1" ##
verify="required"  ## Set it to "required"
cafile="/etc/ldap/ca_certs.pem" #This is what we had set before
clientcert="/etc/smbldap-tools/smbldap-tools.ubuntunet.pem"
clientkey="/etc/smbldap-tools/smbldap-tools.ubuntunet.key"
suffix="dc=ubuntunet,dc=net"
usersdn="ou=people,${suffix}"
computersdn="ou=servers,${suffix}"
groupsdn="ou=group,${suffix}"
userSmbHome="\\IAM\%U"   ## Set your host name here ##
userProfile="\\IAM\profiles\%U"  ## Set your host name here ##
userHomeDrive="H:"  ## Set your Home drive ##
mailDomain="ubuntunet.net"
[...]


#++++++++++++++++++
```

Step 6.5: Generate the Samba SSL certificate and key pair (for this demo, I am using: **smbldap-tools.ubuntunet.pem** and **smbldap-tools.ubuntunet.key**). Where there are question prompts, please answer them appropriately.

```
sudo openssl req -new -newkey rsa:4096 -nodes -keyout smbldap-tools.ubuntunet.key -out smbldap-tools.ubuntunet.csr

sudo openssl x509 -req -sha256 -days 3650 -in smbldap-tools.ubuntunet.csr -signkey smbldap-tools.ubuntunet.key -
out smbldap-tools.ubuntunet.pem
```

Step 6.6: Modify **/etc/smbldap-tools/smbldap_bind.conf** with the settings as per your LDAP installation:

```
#++++++++++++++++++
[...]
#slaveDN="cn=Manager,dc=example,dc=com"  ## make it comment. we don't have a slave LDAP ##
#slavePw="secret"  ## Make it comment ##
masterDN="cn=admin,dc=ubuntunet,dc=net"  ## Enter LDAP admin username and LDAP suffixes ##
masterPw="password from step 1"  ## Enter LDAP root administrative account password ##
#++++++++++++++++++
```

Step 6.7: Populate the LDAP database

```
sudo smbldap-populate

#++++++++++++++++++

Populating LDAP directory for domain ULDAP (S-1-5-21-2419233158-1789257387-3832146290)
(using builtin directory structure)
entry dc=ubuntunet,dc=net already exist.
entry ou=people,dc=ubuntunet,dc=net already exist.
entry ou=group,dc=ubuntunet,dc=net already exist.
entry ou=servers,dc=ubuntunet,dc=net already exist.
adding new entry: ou=Idmap,dc=ubuntunet,dc=net
adding new entry: sambaDomainName=ULDAP,dc=ubuntunet,dc=net
adding new entry: uid=root,ou=people,dc=ubuntunet,dc=net
adding new entry: uid=nobody,ou=people,dc=ubuntunet,dc=net
adding new entry: cn=Domain Admins,ou=group,dc=ubuntunet,dc=net
adding new entry: cn=Domain Users,ou=group,dc=ubuntunet,dc=net
adding new entry: cn=Domain Guests,ou=group,dc=ubuntunet,dc=net
adding new entry: cn=Domain Computers,ou=group,dc=ubuntunet,dc=net
adding new entry: cn=Administrators,ou=group,dc=ubuntunet,dc=net
adding new entry: cn=Account Operators,ou=group,dc=ubuntunet,dc=net
adding new entry: cn=Print Operators,ou=group,dc=ubuntunet,dc=net
adding new entry: cn=Backup Operators,ou=group,dc=ubuntunet,dc=net
adding new entry: cn=Replicators,ou=group,dc=ubuntunet,dc=net

Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password: ## Enter Password ##
Retype new password:## Re-enter password ##
```

Step 6.8: Check the LDAP database for schema groups

```
sudo getent group
```

Step 6.9: Configure samba in **/etc/samba/smb.conf** and make the following changes:

```
sudo cp /usr/share/doc/smbldap-tools/examples/smb.conf.example /etc/samba/smb.conf
sudo vi /etc/samba/smb.conf
```

```
#+++++++++++++++++++
workgroup = UBUNTUNET  ## Your domain Name ##
netbios name = IAM  ## Samba server Host name ##

logon drive = H:  ## Logon drive ##

passdb backend = ldapsam:"ldap://iam.ubuntunet.net/"  ## Samba server FQDN ##
ldap ssl = start tls  ## Set to enable SSL
ldap admin dn = cn=admin,dc=ubuntunet,dc=net  ## LDAP admin account and LDAP suffixes ##

ldap suffix = dc=ubuntunet,dc=net  ## LDAP suffix ##
ldap user suffix = ou=people
ldap group suffix = ou=group
ldap machine suffix = ou=servers
#+++++++++++++++++++
```

Step 6.10: Restart the Samba services

```
sudo smbpasswd -w password # password is what was set in step 1
sudo /etc/init.d/smbd restart
sudo /etc/init.d/nmbd restart
```

LAM (LDAP Account Manager)

LAM (https://www.ldap-account-manager.org/lamcms/) is a GUI tool used to manage the LDAP seerver

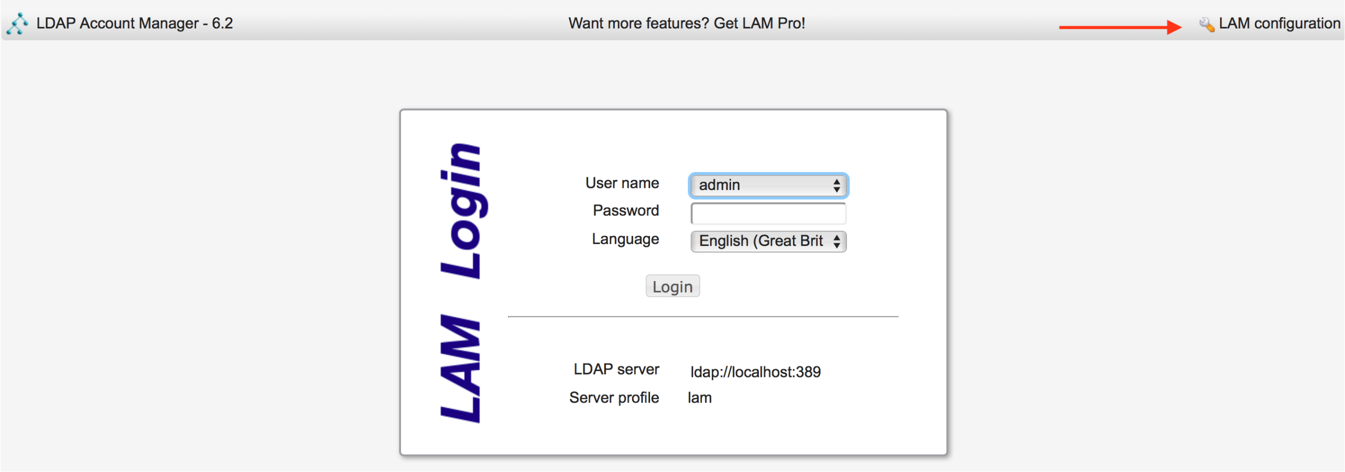
Step 7.1: Install the LAM server

```
sudo apt-get install ldap-account-manager
```

Step 7.2: Access the LAM server from a web browser by visiting http://ip-address/lam. For my demo, I will visit http://iam.ubuntunet.net/lam

The default password for lam administrative account is **“lam”** but you should change this (later on it)

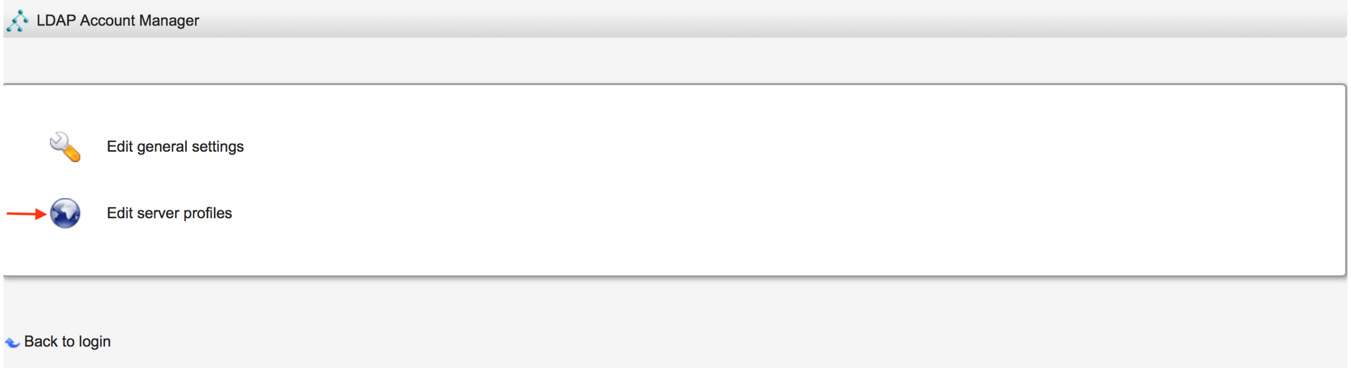
Step 7.3: Before we can fully access LAM, enter the LDAP admin user name and LDAP suffix in lam configuration file. This is done by clicking on **LAM configuration** on the right cornet of **lam** main console.



User name: admin
Password:
Language: English (Great Brit

LDAP server: ldap://localhost:389
Server profile: lam

Step 7.4: The above step leads us to the screen below, now click on **'Edit Server Profiles'** You will be prompted for the password (Use the default - lam if you haven't changed it yet)



LDAP Account Manager

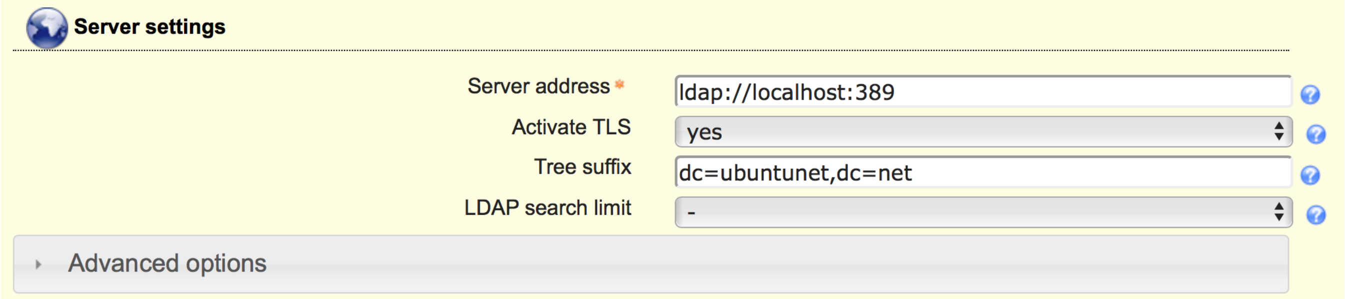
Edit general settings

Edit server profiles

Back to login

Step 7.5: On the General Settings tab, enter the following details:

Step 7.5.1: Server Settings

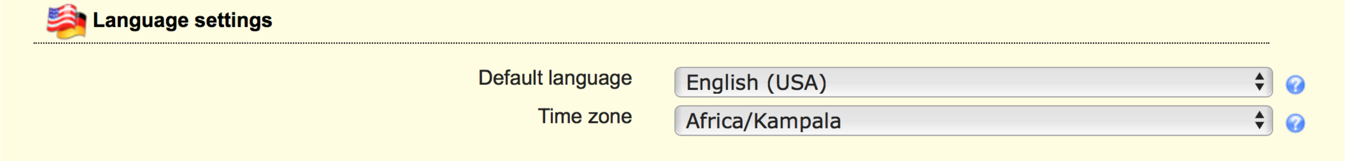


Server settings

Server address *	ldap://localhost:389
Activate TLS	yes
Tree suffix	dc=ubuntunet,dc=net
LDAP search limit	-

Advanced options

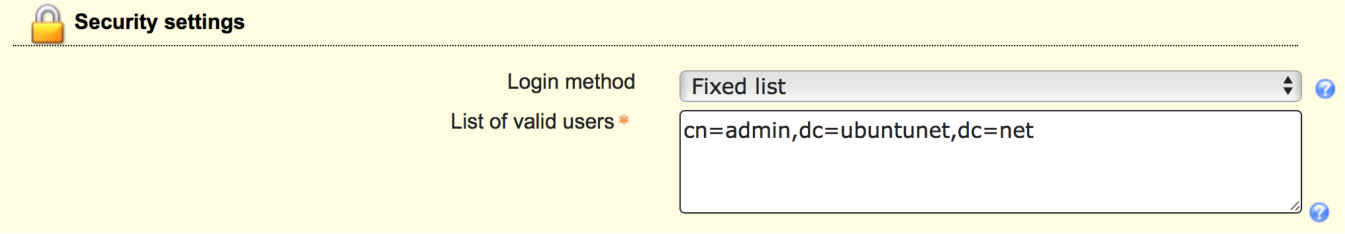
Step 7.5.1: Language Settings



Language settings

Default language	English (USA)
Time zone	Africa/Kampala

Step 7.5.1: Security Settings

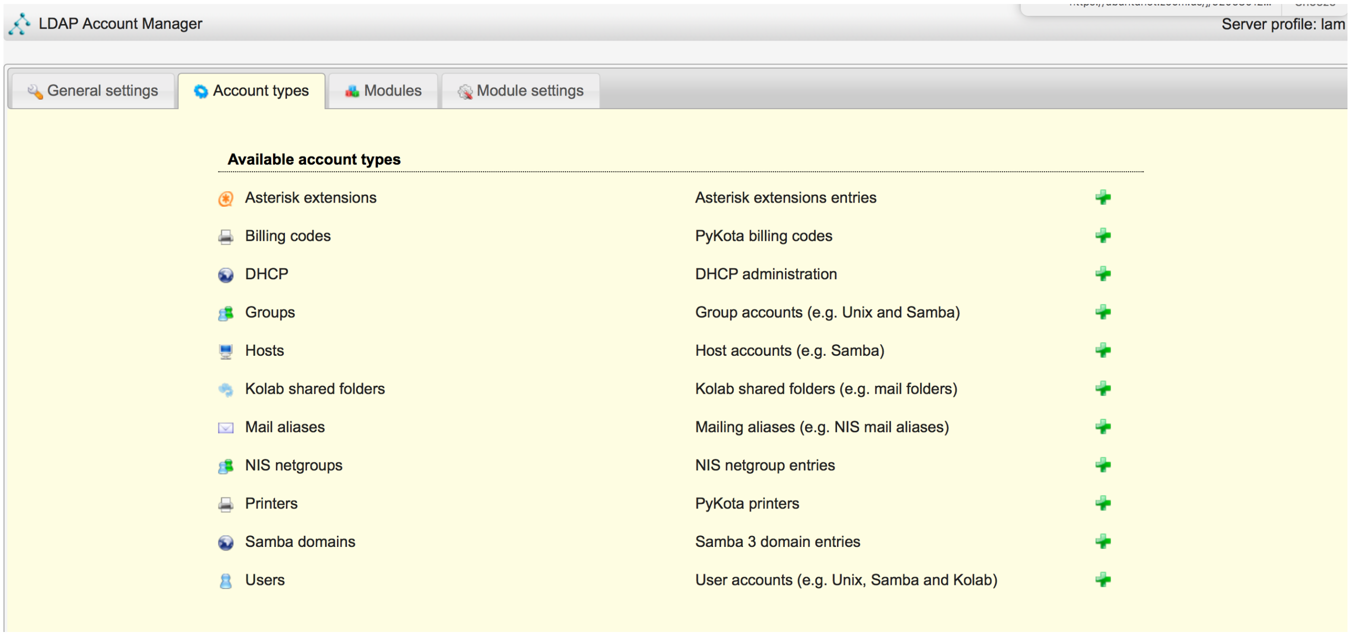


Security settings

Login method	Fixed list
List of valid users *	cn=admin,dc=ubuntunet,dc=net

Step 7.6: Under the Account Types tab, add the following settings:

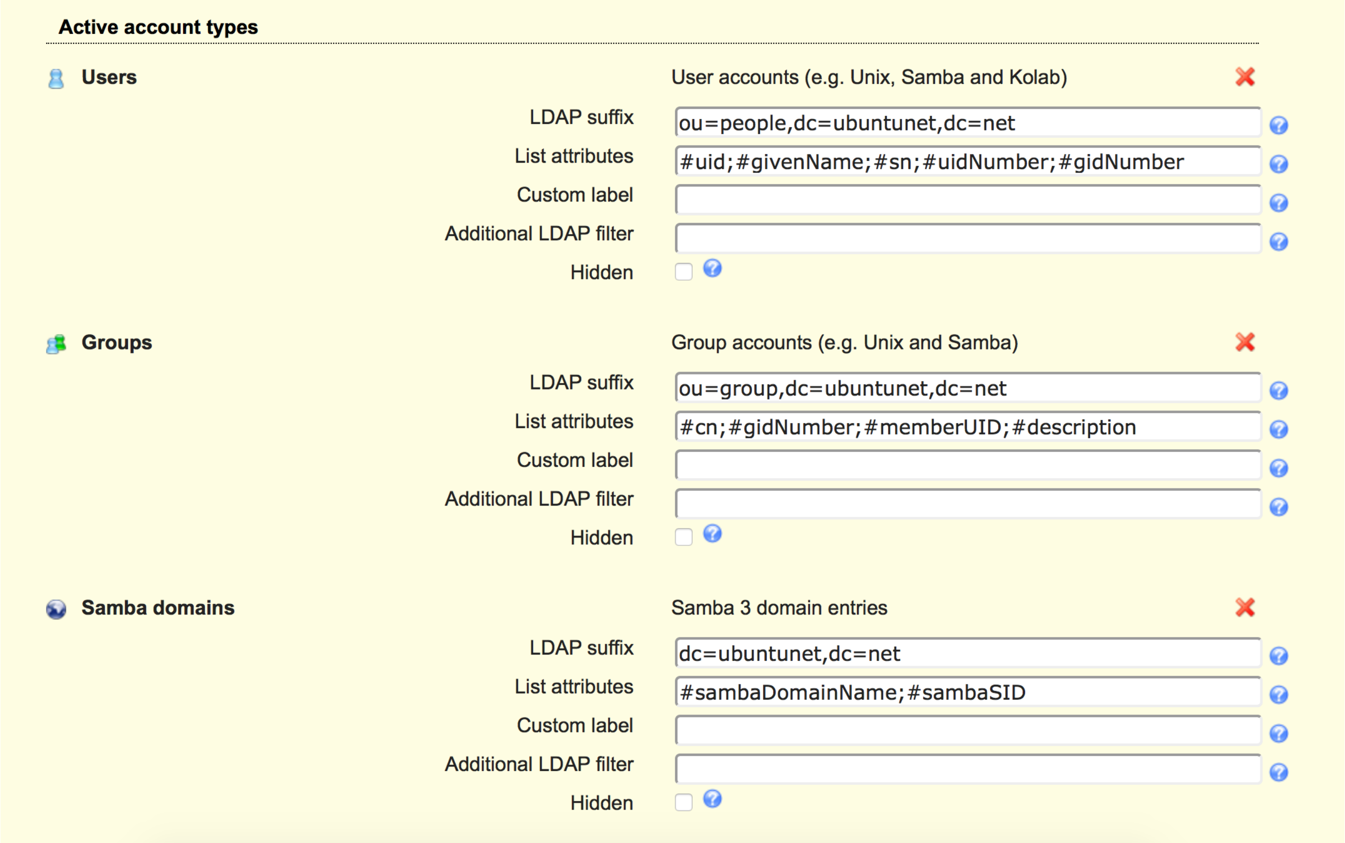
Step 7.6.1: Under Available account types add **Samba domains**.



Available account types

Asterisk extensions	Asterisk extensions entries	➕
Billing codes	PyKota billing codes	➕
DHCP	DHCP administration	➕
Groups	Group accounts (e.g. Unix and Samba)	➕
Hosts	Host accounts (e.g. Samba)	➕
Kolab shared folders	Kolab shared folders (e.g. mail folders)	➕
Mail aliases	Mailing aliases (e.g. NIS mail aliases)	➕
NIS netgroups	NIS netgroup entries	➕
Printers	PyKota printers	➕
Samba domains	Samba 3 domain entries	➕
Users	User accounts (e.g. Unix, Samba and Kolab)	➕

Step 7.6.2: Under Active account types, add the correct settings:



Active account types

Users — User accounts (e.g. Unix, Samba and Kolab) ✖

LDAP suffix	ou=people,dc=ubuntunet,dc=net
List attributes	#uid;#givenName;#sn;#uidNumber;#gidNumber
Custom label	
Additional LDAP filter	
Hidden	□

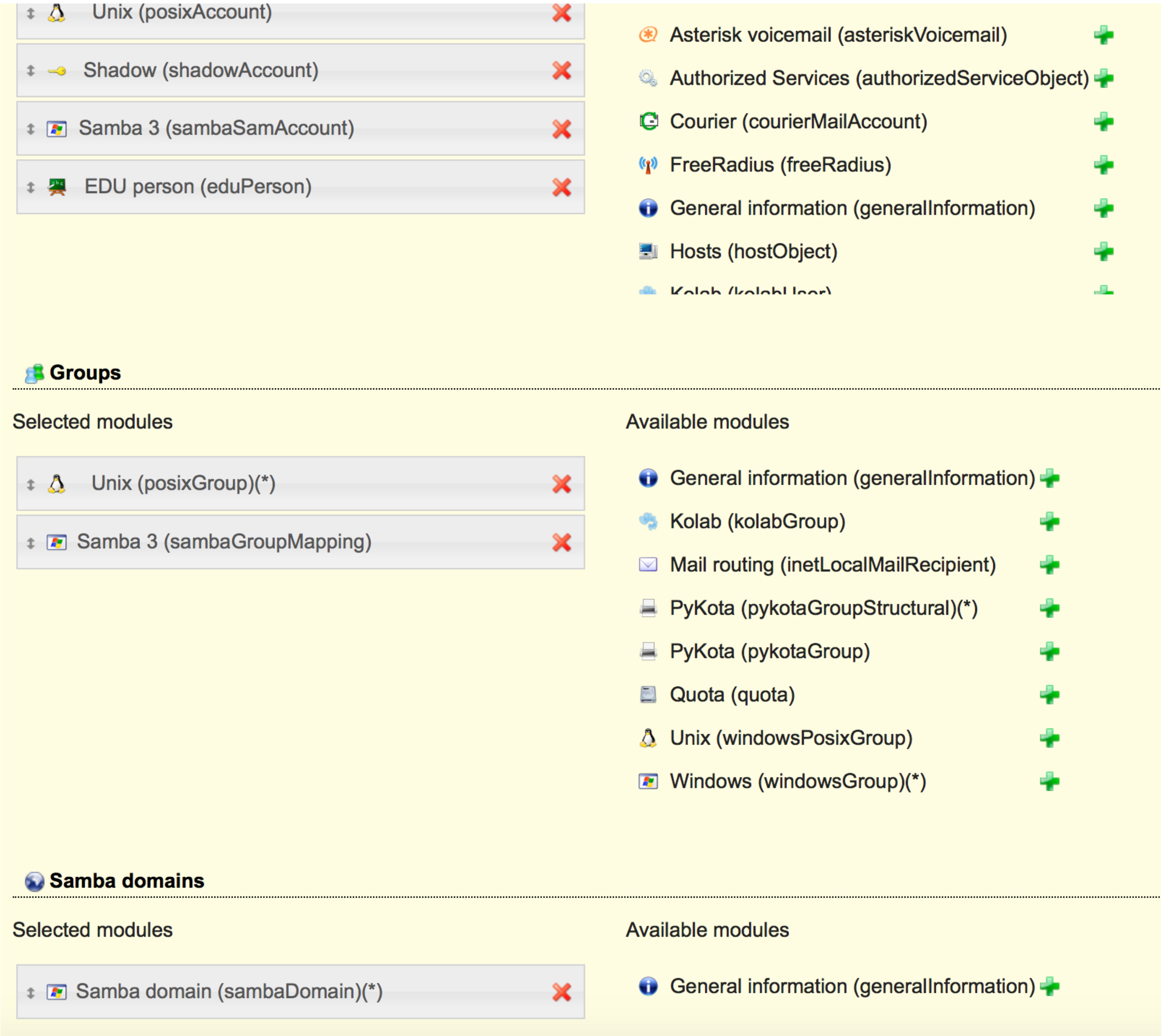
Groups — Group accounts (e.g. Unix and Samba) ✖

LDAP suffix	ou=group,dc=ubuntunet,dc=net
List attributes	#cn;#gidNumber;#memberUID;#description
Custom label	
Additional LDAP filter	
Hidden	□

Samba domains — Samba 3 domain entries ✖

LDAP suffix	dc=ubuntunet,dc=net
List attributes	#sambaDomainName;#sambaSID
Custom label	
Additional LDAP filter	
Hidden	□

Step 7.6: Under the Account Types tab, add the following settings (Take note of **Samba 3** and **ED person**):



Unix (posixAccount)

Shadow (shadowAccount)

Samba 3 (sambaSamAccount)

EDU person (eduPerson)

Asterisk voicemail (asteriskVoicemail)

Authorized Services (authorizedServiceObject)

Courier (courierMailAccount)

FreeRadius (freeRadius)

General information (generalInformation)

Hosts (hostObject)

Kolab (kolabUser)

Groups

Selected modules

Unix (posixGroup)(*)

Samba 3 (sambaGroupMapping)

Available modules

General information (generalInformation)

Kolab (kolabGroup)

Mail routing (inetLocalMailRecipient)

PyKota (pykotaGroupStructural)(*)

PyKota (pykotaGroup)

Quota (quota)

Unix (windowsPosixGroup)

Windows (windowsGroup)(*)

Samba domains

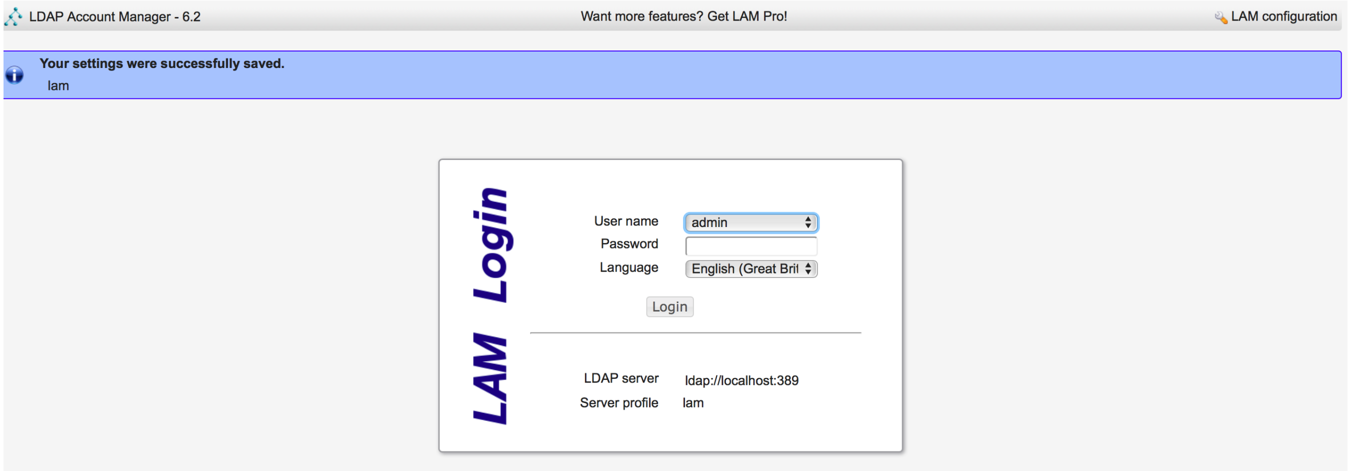
Selected modules

Samba domain (sambaDomain)(*)

Available modules

General information (generalInformation)

Step 7.7: You can now save and you will be redirected to the login screen where you can now login with LDAP credentials that were created earlier.



Your settings were successfully saved.
lam

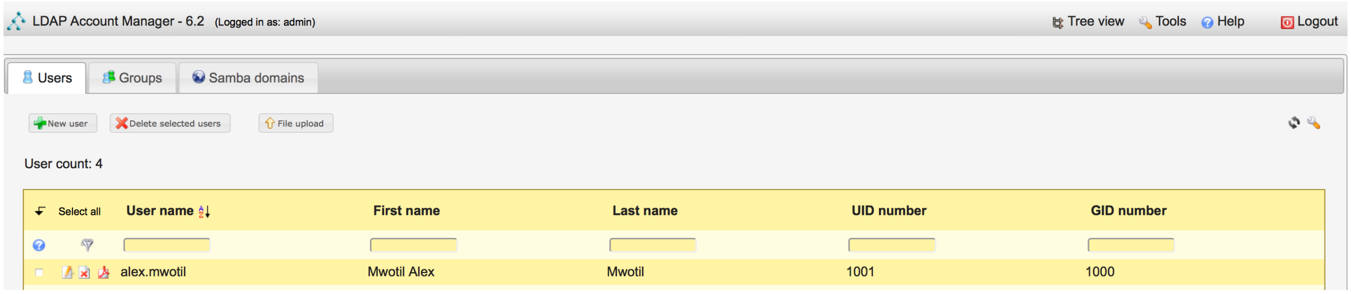
LAM Login

User name: admin
Password:
Language: English (Great Bri

LDAP server: ldap://localhost:389
Server profile: lam

Step 7.8: You can now be able to add Users, Groups and Samba Domains. When adding a user, please ensure that **Samba 3 Extension** and **EDU person extension** attributes are added.

Also when setting a user password **Unix** and **Samba 3** should be selected.



LDAP Account Manager - 6.2 (Logged in as: admin)

User count: 4

Select all	User name	First name	Last name	UID number	GID number
	alex.mwotil	Mwotil Alex	Mwotil	1001	1000

Step 7.9: You may now enable HTTPS access through LetsEncrypt

```
sudo apt install python-certbot-apache

sudo certbot --apache -d iam.ubuntunet.net #Answer the prompts correctly (The last prompt should ask about
redirection to https, enter that option - 2 at the time of this writing)
```

SCHAC.ldif

eduperson-201602.ldif

Related articles

- OpenLDAP Installation (eduroam & federated services)