LDAP Integration

LUCY has an LDAP API, which allows the administrator to:

- import recipients and users directly from your directory service
- authorize users in the Admin console, Enduser portal and Awareness website

Sync tool for Windows

Besides LDAP API, there is a tool that can be run on Windows machines to sync your Active Directory groups with Lucy, see more here.

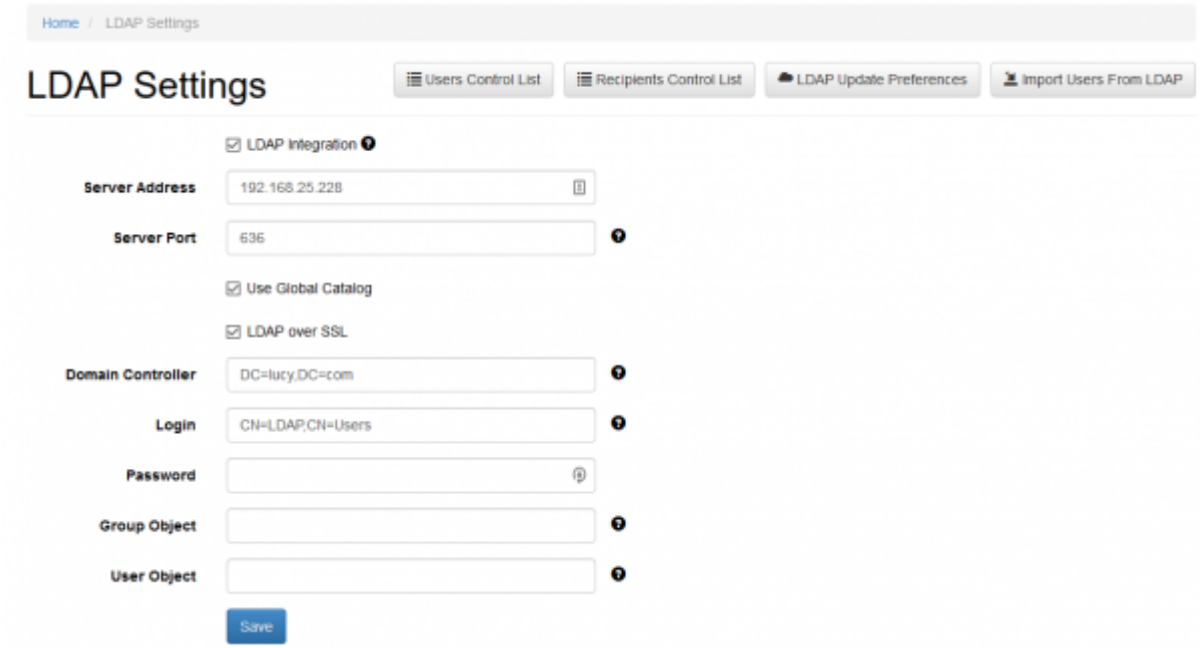
Setup

To configure the LDAP connection please go in LDAP settings (Settings → LDAP Settings) and save your server and authentication details. Within the field "Server Address" you need to enter your LDAP server IP address, within the field "Server Port" you should enter TCP/UDP port for LDAP (default port 389 or port 636 for LDAPS) and if "Use Global Catalog" and "LDAP over SSL" are enabled you should use the ports 3268 and 3269. Within the field "Domain Controller" you need to enter your LDAP Server Root RDN (example: "dc=domain,dc=com") and within the field "Login" you need to enter user RDN (example: "cn=Administrator,cn=Users").

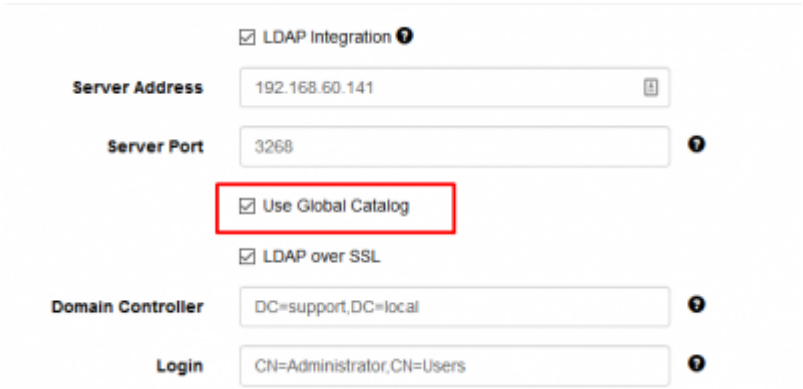
 LUCY summarizes the values for "Domain Controller" and "Login" on the backend. So if the LDAP login is "cn=ldap,cn=user,dc=domain,dc=com", put "dc=domain,dc=com" to the "Domain Controller" and "cn=ldap,cn=user" to "Login".

Fields "Group Object" and "User Object" are used to filter search from the LDAP objects. Objects within "Group Object" and "User Object" fields need to be separated with a comma and one space.

You may use regular Active Directory search filters, for example:
(|(objectClass=inetOrgPerson)(objectClass=user))



Also in the "LDAP settings" you can use Global Catalog:



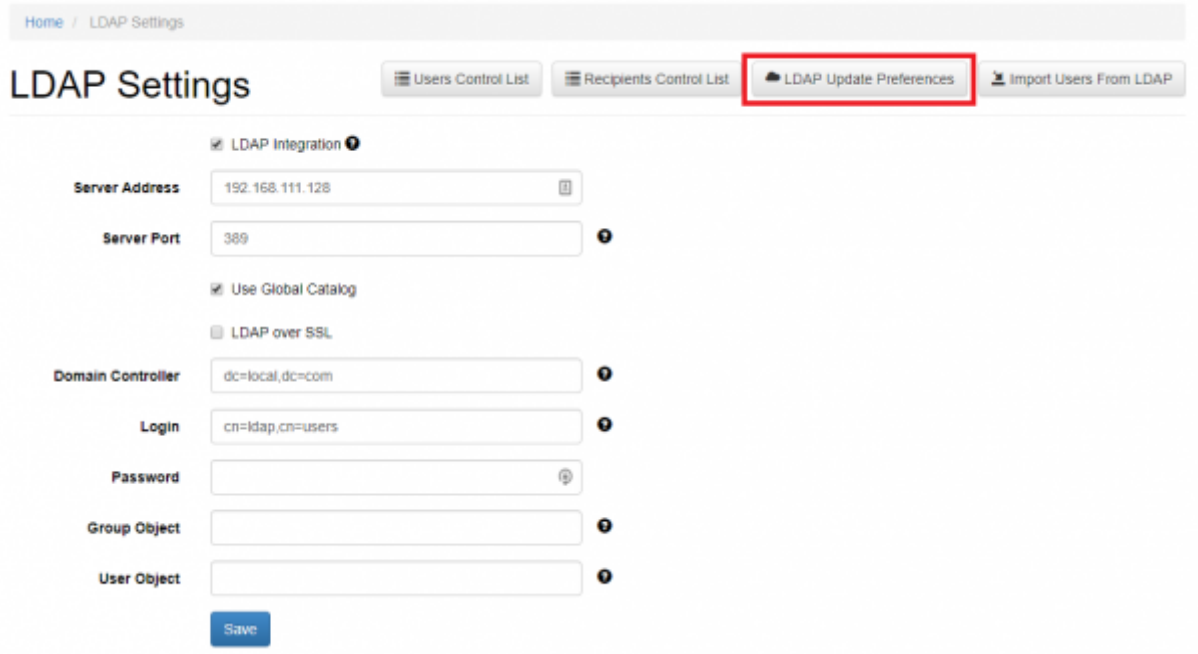
Note: The Global Catalogue allows the connection only via two special ports: 3268 or 3269. To use this functionality, please configure one of these ports for connection to AD.

The global catalog (GC) allows users and applications to find objects in an Active Directory domain tree, given one or more attributes of the target object. The global catalog contains a partial replica of every naming context in the directory. It contains the schema and configuration naming contexts as well. This means the GC holds a replica of every object in the directory but with only a small number of their attributes. The attributes in the GC are those most frequently used in search operations (such as a user's first and last names or login names) and those required to locate a full replica of the object.

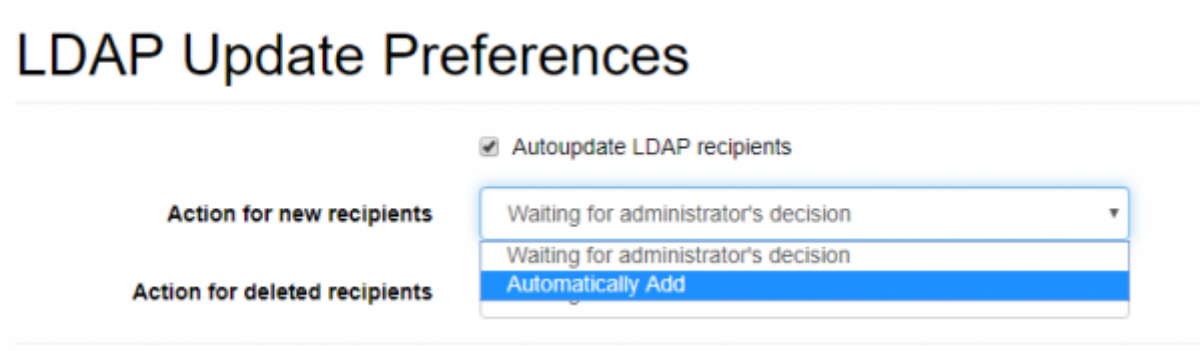
LDAP Update Preferences

This menu allows configuring automatic synchronization of LDAP recipients and users that were imported into LUCY. Automatic synchronization happens every 10 minutes.

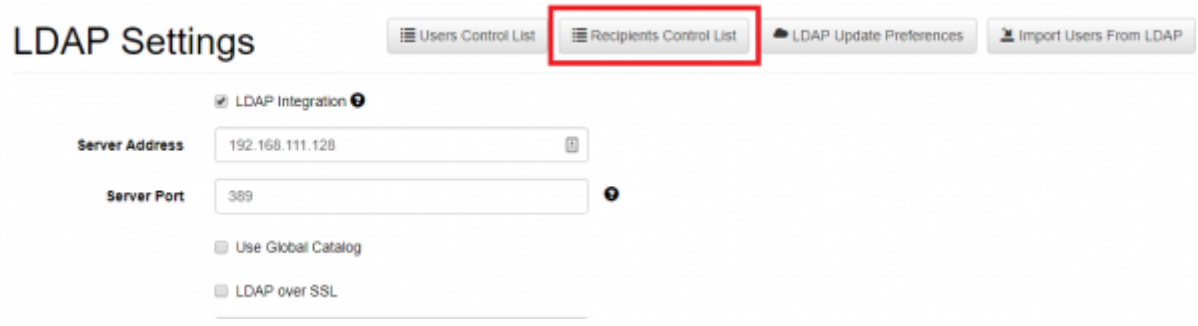
Note, these settings are global and all of the Autoupdate LDAP preferences per a group of recipients will be ignored with the settings enabled (see Autoupdate LDAP Recipients).



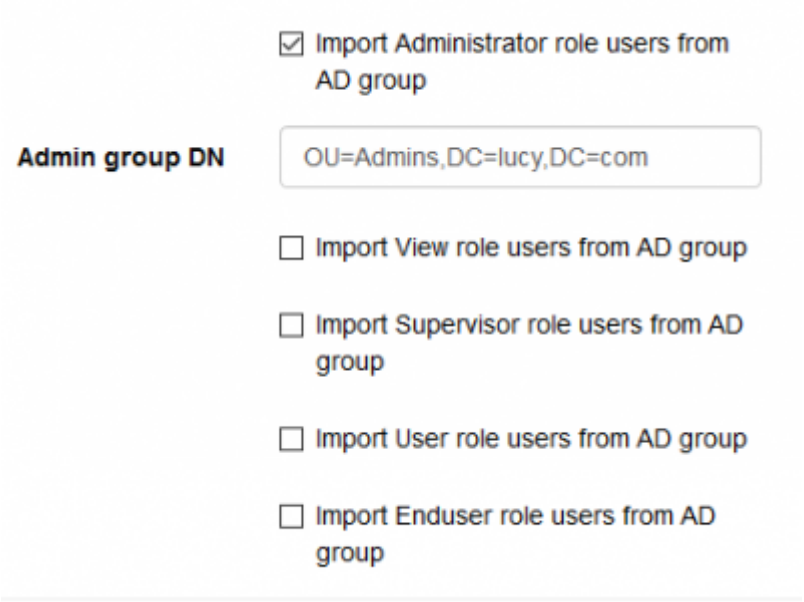
LDAP update preferences contain 2 options for automatic action. It is possible to configure LUCY to add users and recipients automatically or to wait for the Administrator's decision.



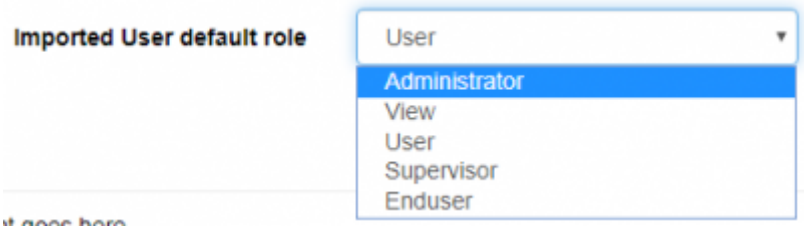
In case if you select "Waiting for administrator's decision", an Administrator will have to go to a control list and decide whether it is necessary to delete\add a recipient\user or not.



It is also possible to customize the pattern of automatic import of users from an Organization Unit. Lucy will scan a Distinguished Name (RDN) of the OrganizationUnit (eg. OU=Admins, DC=domain, DC=tld) and automatically bind a role to an imported user according to the settings that can be seen on the screenshot below.

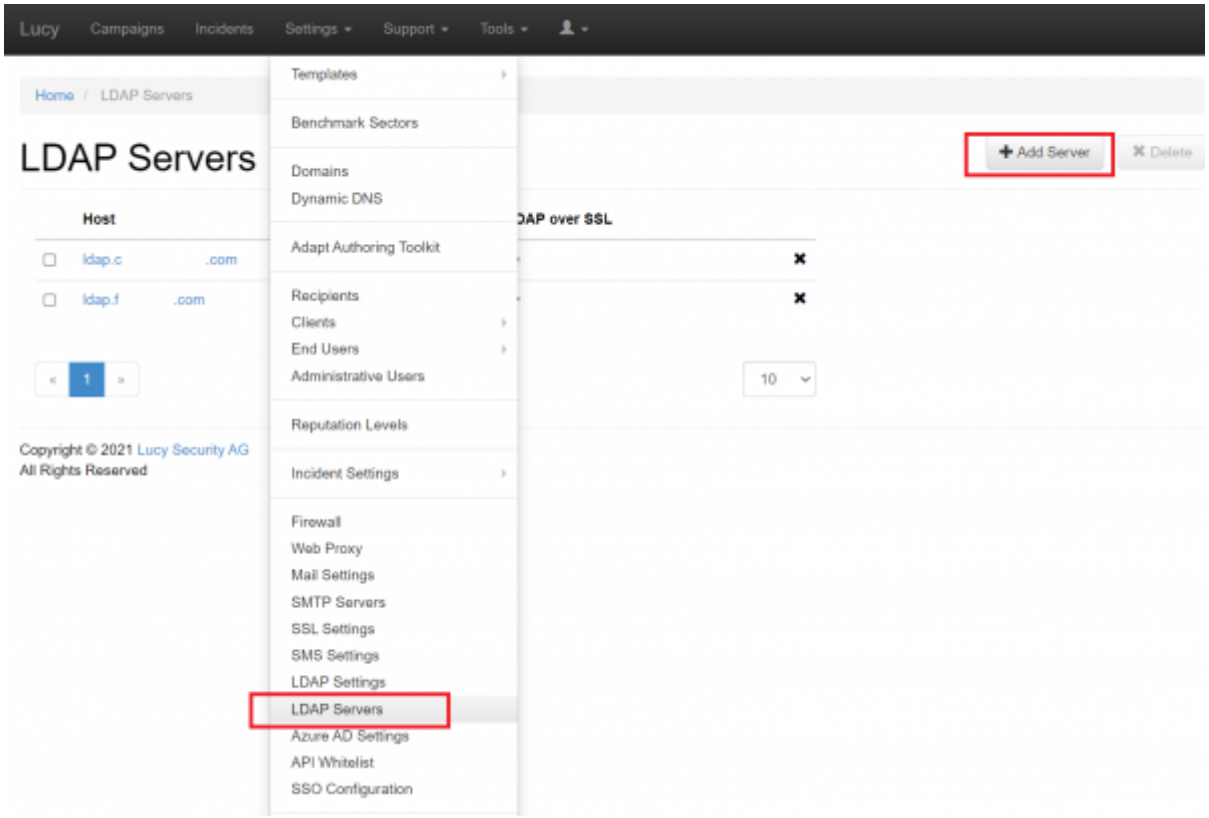


The user default role defines a role that will be assigned to users with manual import users from LDAP.

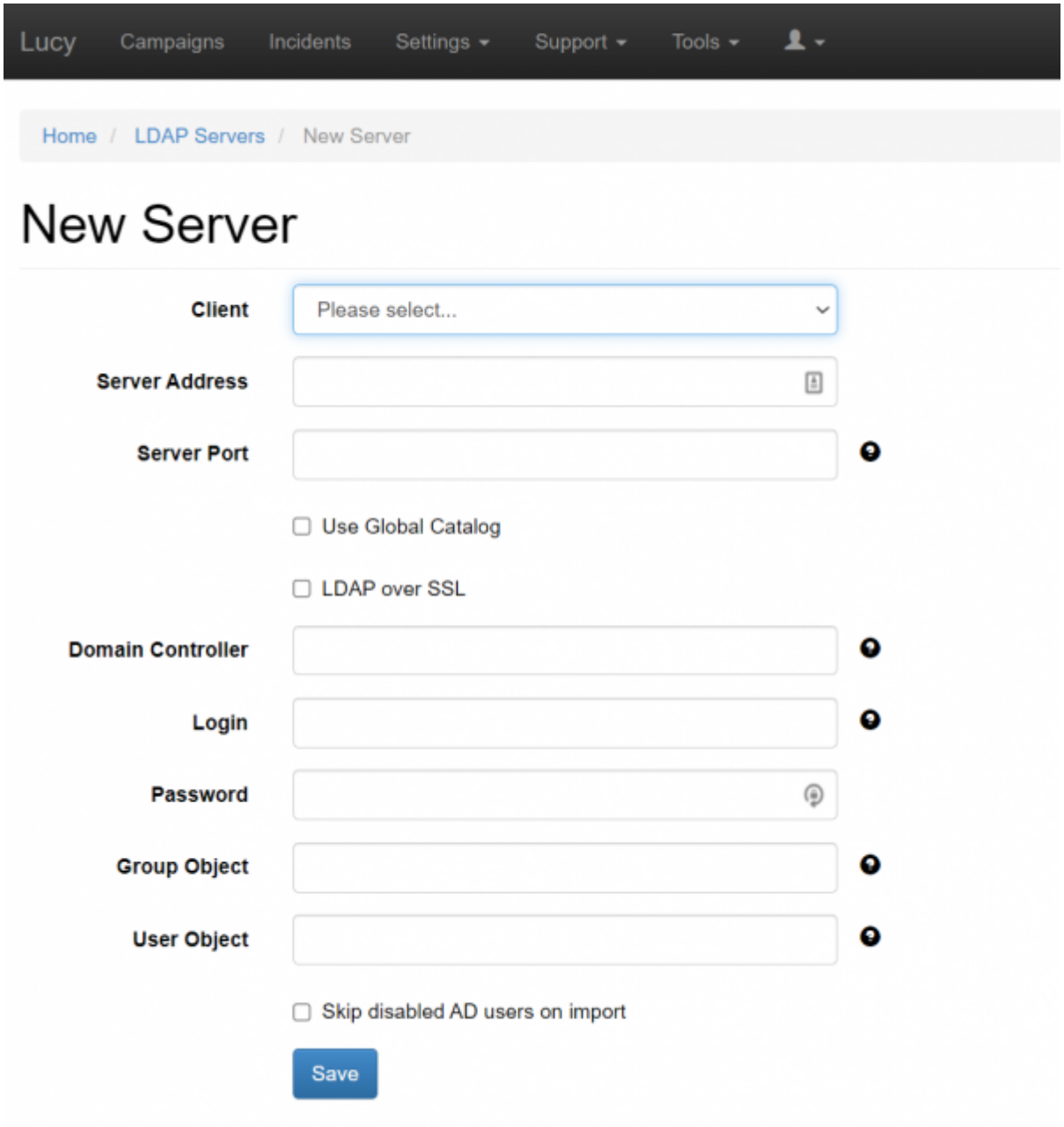


Multiple LDAP integrations

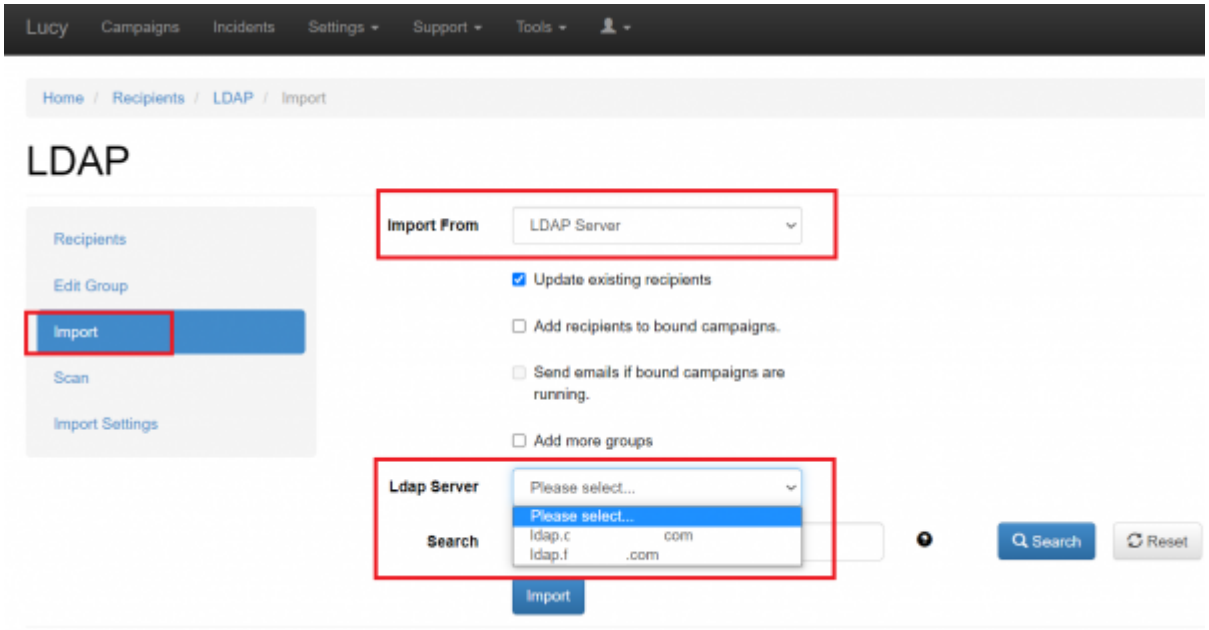
LUCY allows to configure and use multiple LDAP servers.
The dedicated section in the LUCY web interface can be found in the Settings:



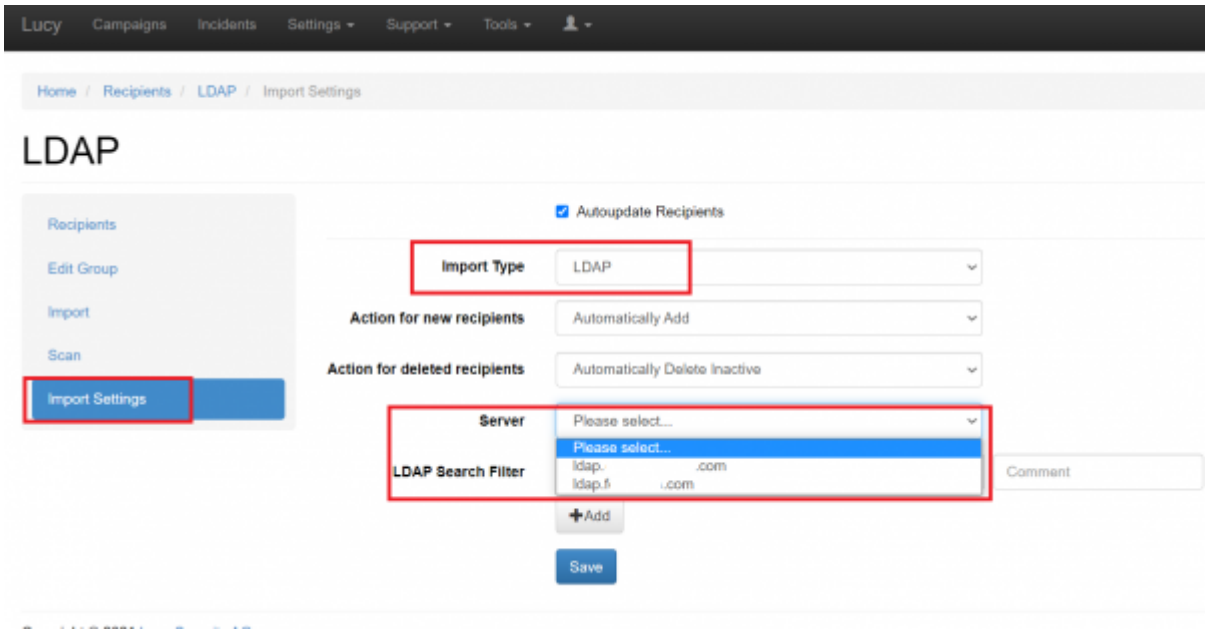
Pressing "Add Server" would result the usual LDAP server configuration page to appear. Configure the additional LDAP Server and press Save. It will appear in the list of available LDAP Servers ready for sync and import.



After setting-up multiple LDAP Servers, there would be a dropdown menu in the import settings of the recipient group to chose the specific server for the import.

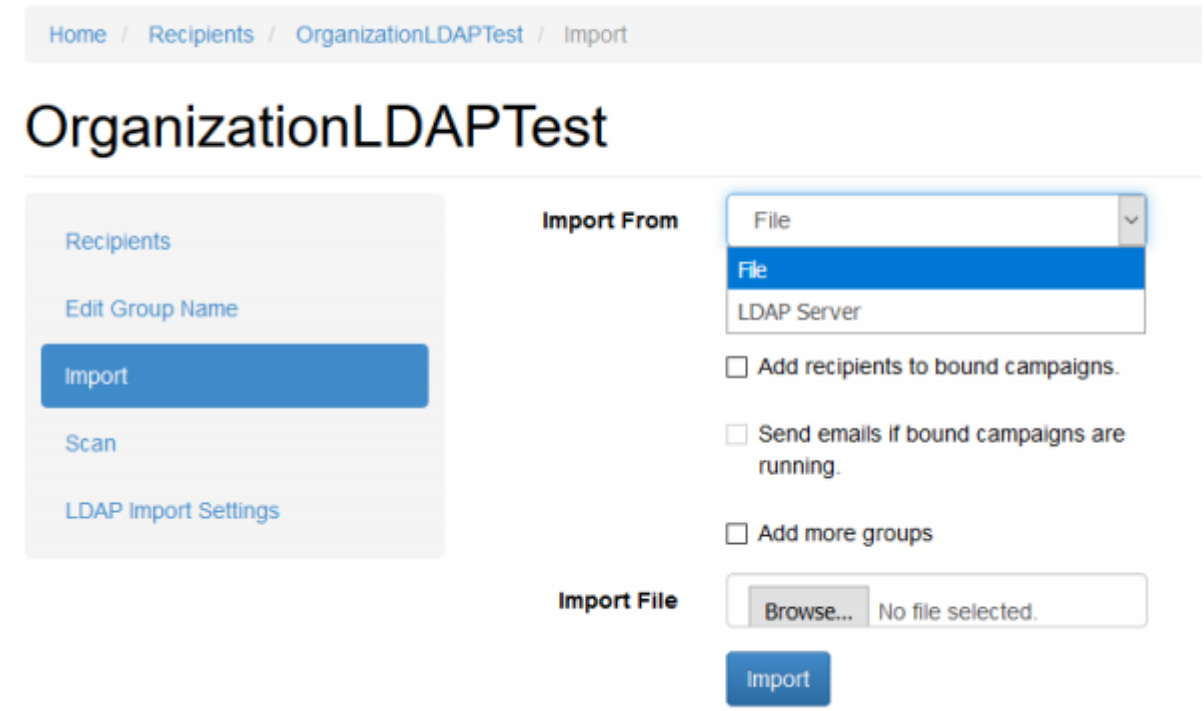


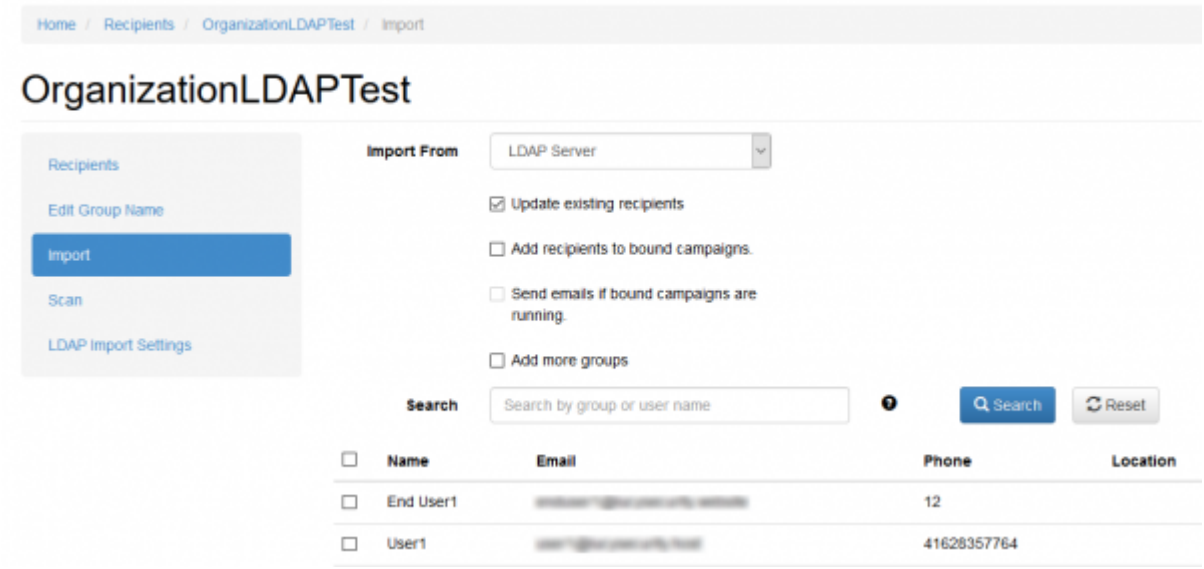
The same choice is available for the Autoupdate feature.



Importing recipients in a group for a campaign

When you create a new recipient group you will be able to use the previously configured LDAP connection to query and import all the users/groups:





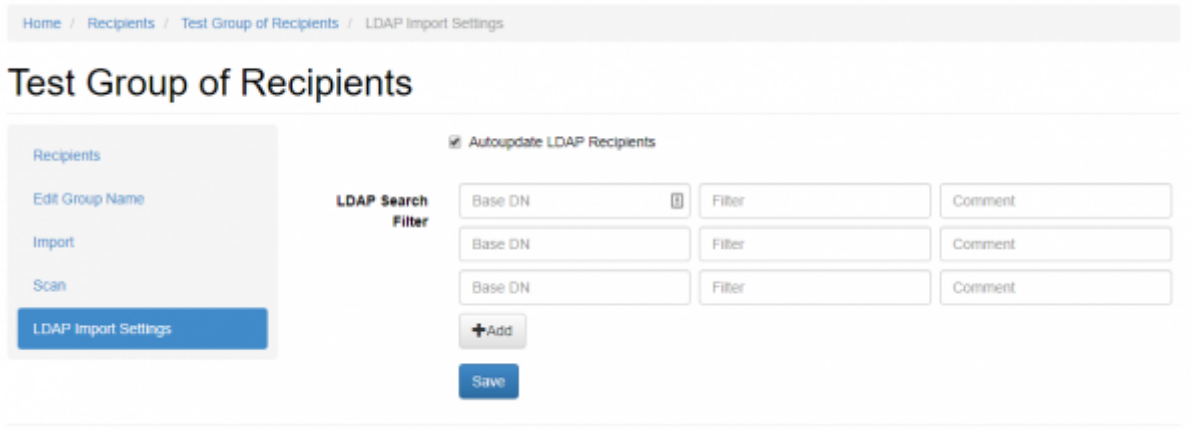
LUCY will automatically match the user's attributes in the LDAP directory with the available recipient attributes in LUCY.

If "Update existing recipients" option is enabled, recipient attributes will update during LDAP import if these recipients have been imported before.

Autoupdate LDAP Recipients

It is possible to configure LUCY autoupdate recipient list of from an LDAP Server.

Note, this configuration will not be active if there are global settings for recipients import disabled.



You may use regular Active Directory search filters, for example:

```
(|(objectClass=inetOrgPerson)(objectClass=user)).
```

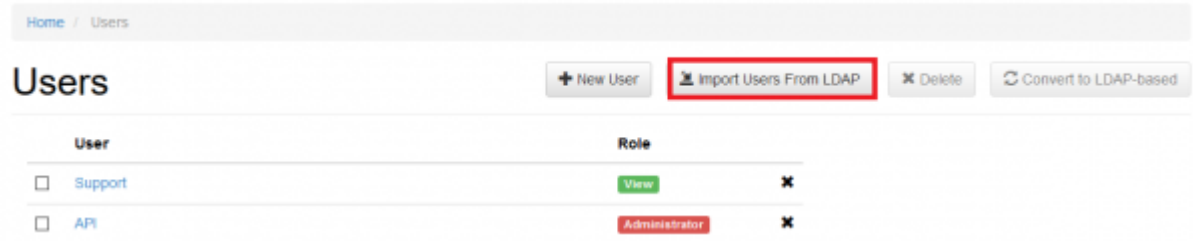
See Microsoft Documentation for more info.

The Base DN of the query must be specified in the following format:

```
dc=MyDomain,dc=com.
```

Importing users via LDAP

If you want to import users who can access LUCY using their AD account, you can go into the user settings menu (Settings > Users) and click the according button:



By default, the User role will be assigned for all imported users.

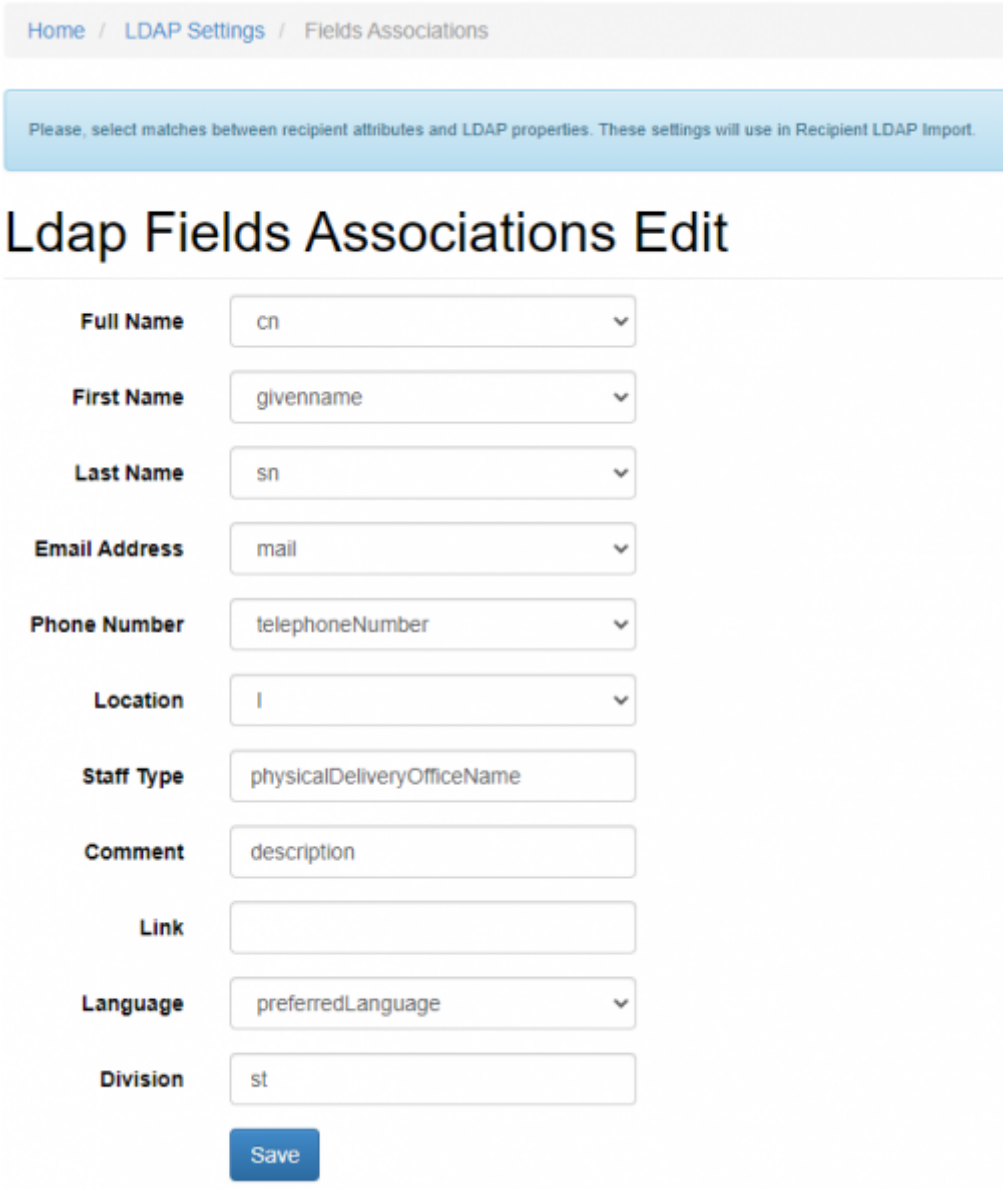
Which LDAP fields can be used?

LUCY will automatically match the user's attributes in the LDAP directory with the available recipient attributes in LUCY. Those are:

- 1.Email - Recipient's e-mail address
- 2.Name - Recipient's name
- 3.Location - Recipient's location
- 4.Phone - recipient phone number

To configure other recipient fields to match Active Directory attributes go to the LDAP Fields

Associations page (Settings > LDAP Settings > LDAP Fields Associations):



Recipient's custom fields are also supported.

Login Lucy through Active Directory (LDAP)

Lucy allows users to login with their Active Directory account.

Admin console & Enduser portal

In order users to login Admin console or Enduser portal you should first import accounts to Lucy from your Active Directory. See this section for more details.

Please note that to login Lucy you should use an appropriate user role that can be configured

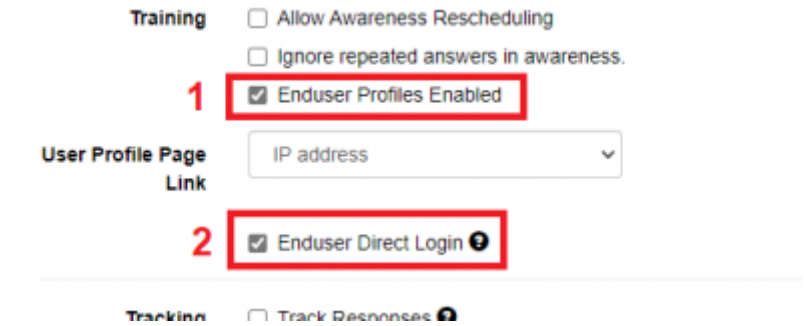
within the LDAP Update Preferences page (Settings > LDAP Settings > LDAP Update Preferences).

User roles used to access Admin console: **Administrator, View, User, Supervisor**.
User role used to access Enduser portal: **Enduser**.

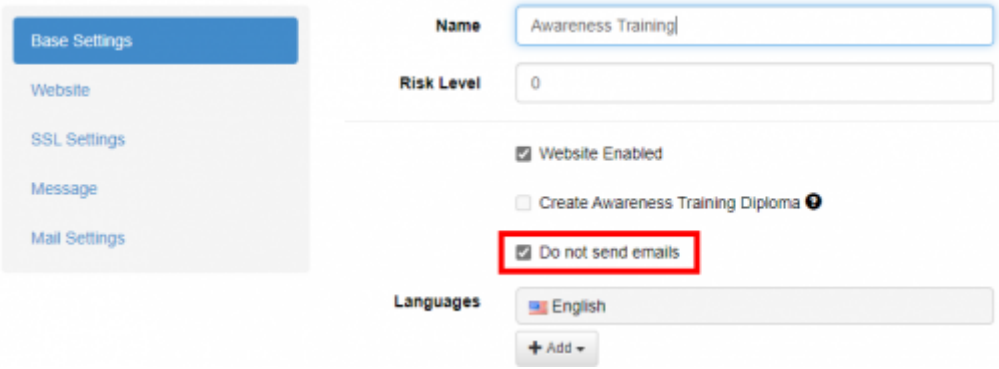
Awareness website

Lucy has an option to send a non-unique link for awareness website, but it requires users to login with their AD account to access the website. It also requires endusers to be imported into Lucy (see previous section).

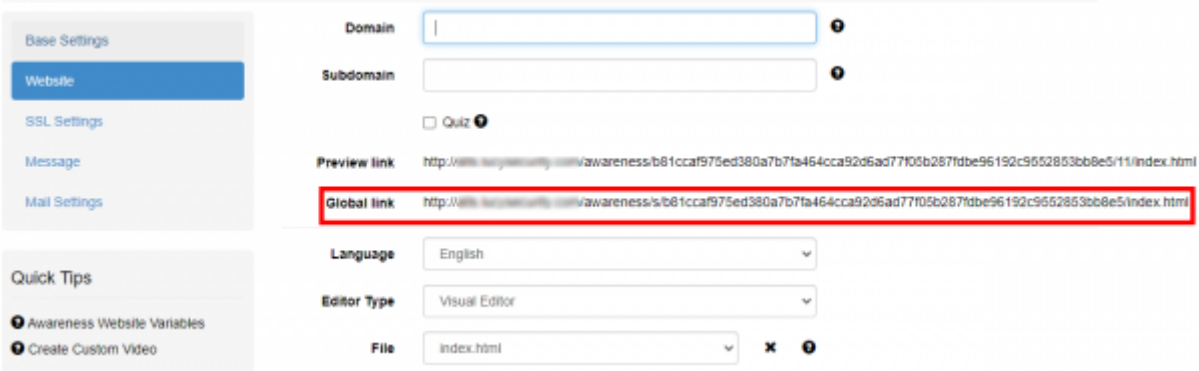
To enable LDAP login for Awareness website, tick the option "**Enduser Direct login**" within the Base Settings in your campaign:



and the option "**Do not send emails**" within the Website section of the Awareness settings:



This enables the Global Link that can be used to access Awareness website after successful login via LDAP:



The option "Do not send emails" disables sending awareness emails from campaign, that allows to share the Global Link through your own channel.

Troubleshoot problems

- An error occurs during the connection to Azure AD LDAPS:

```
Error connecting to LDAP Server: 80090308: LdapErr: DSID-0C090446,
comment: AcceptSecurityContext error, data 52e, v2580
```

Solution: Invalid Login or Password.
Login must be in the format CN=<username>OU=<ou>, for example:
CN=UserTest,OU=AADDC Users

- An error occurs when logging in at /admin or /user using Azure AD account: **Invalid LDAP user login or password.**

Solution: Please make sure you have enabled your NTLM password hash synchronization. Users cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of cloud-only and synced user accounts in your Azure AD directory.

Instructions for cloud-only user accounts
Instructions for synced user accounts