LDAP Integration

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

- import recipients
- import users (LUCY administrators)

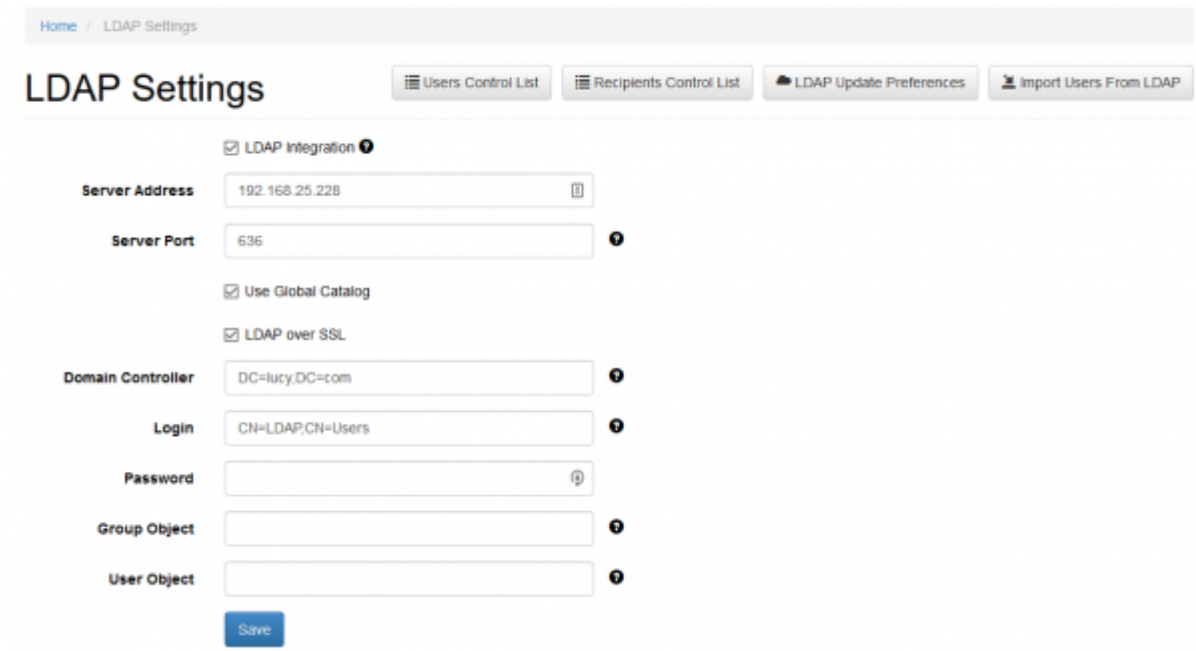
directly from your directory service.

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").

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:



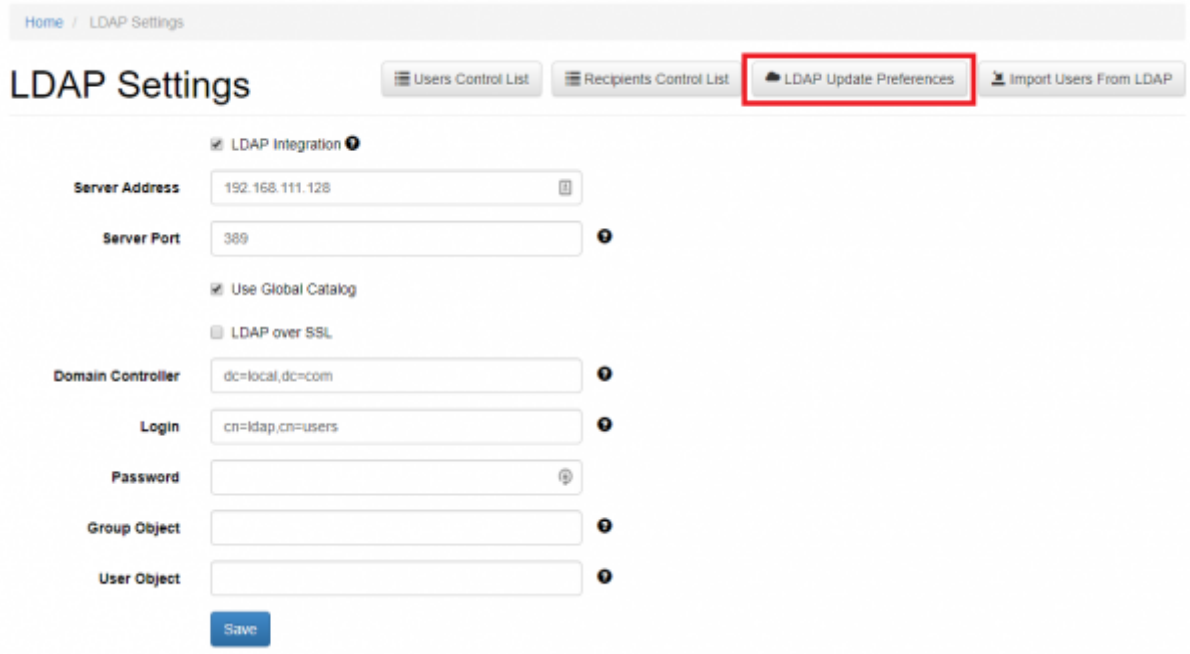
*Note:*The Global Catalogue allows the connection only via two special ports: 3268 or 3269. To use this functionality, please configure one of these ports for connection to AD.

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

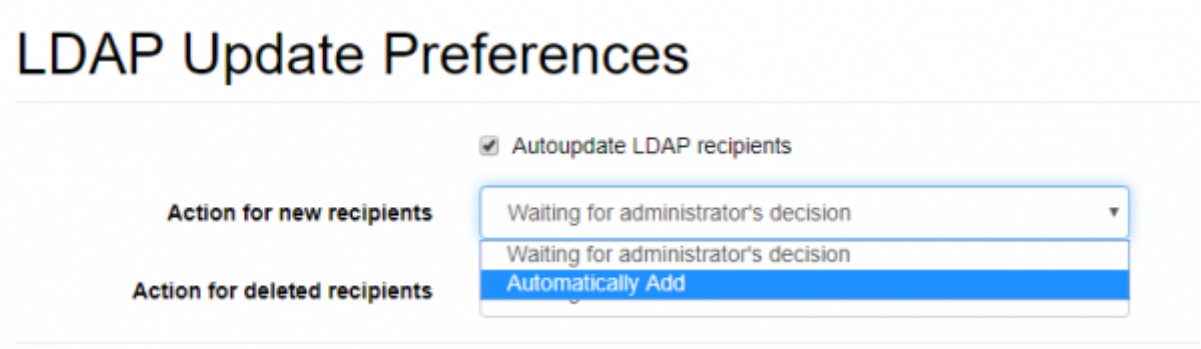
This menu allows configuring automatic synchronization of LDAP recipients and users that were imported into LUCY. Automatic synchronization happens every 10 minutes.

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).

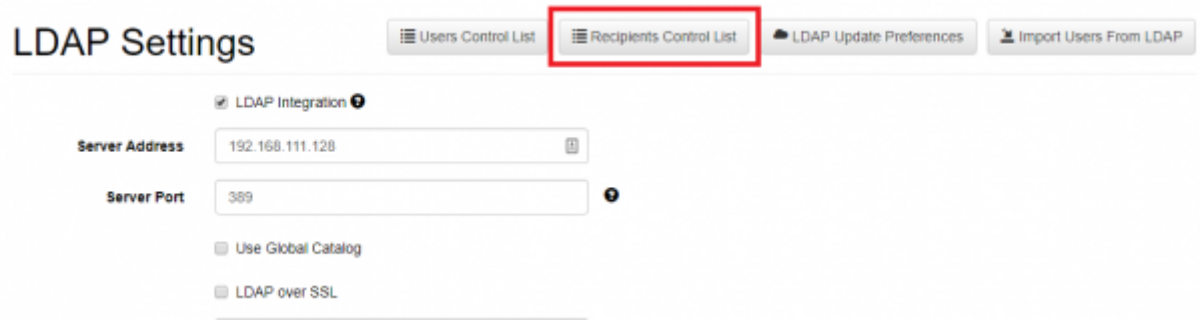


LDAP update preferences contain 2 options for automatic action. It is possible to configure LUCY to

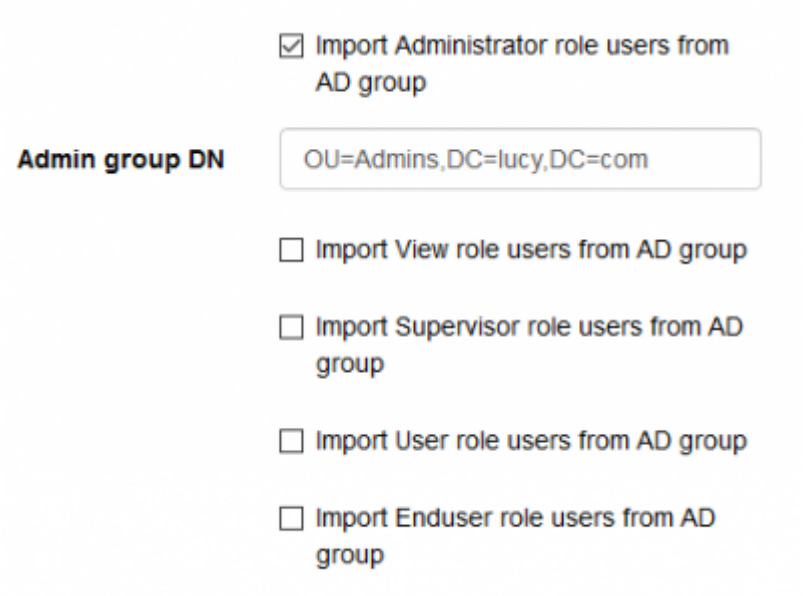
add users and recipients automatically or to wait for the Administrator's decision.



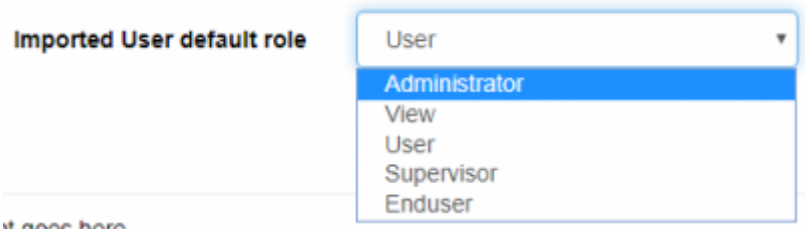
In case if you select "Waiting for administrator's decision", an Administrator will have to go to a control list and decide whether it is necessary to delete\add a recipient\user or not.



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.

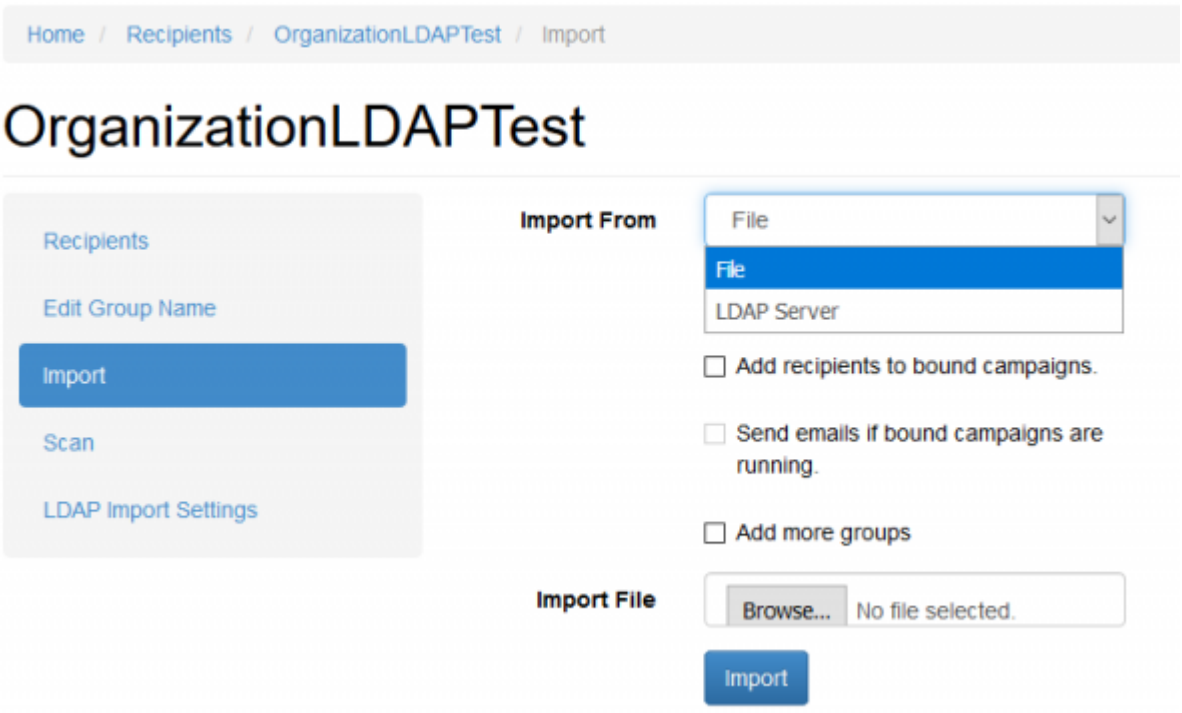


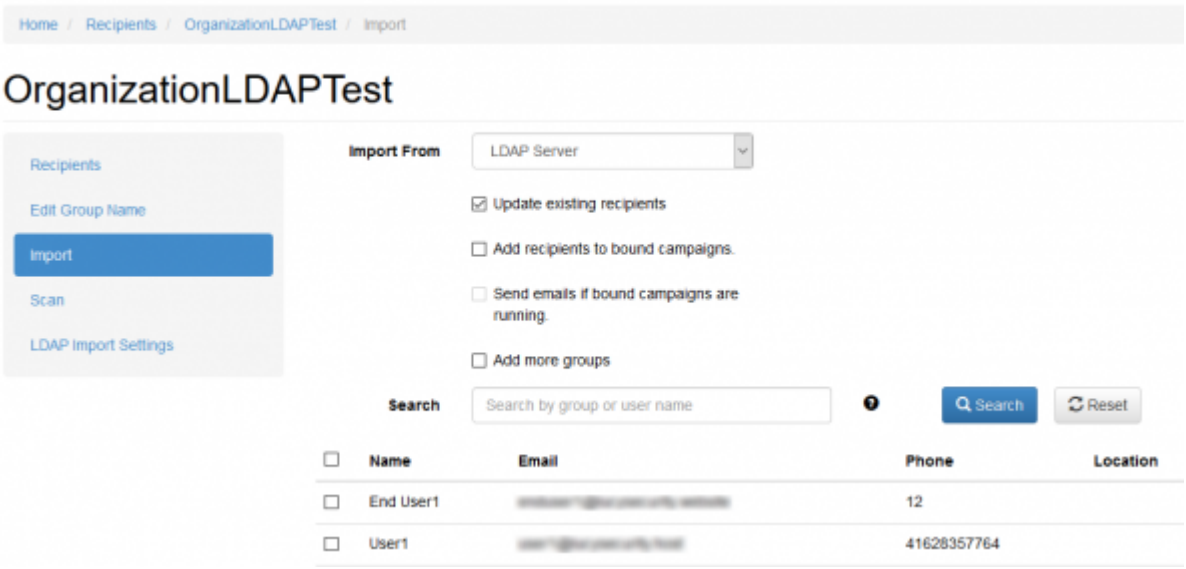
The user default role defines a role that will be assigned to users with manual import users from LDAP.



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:



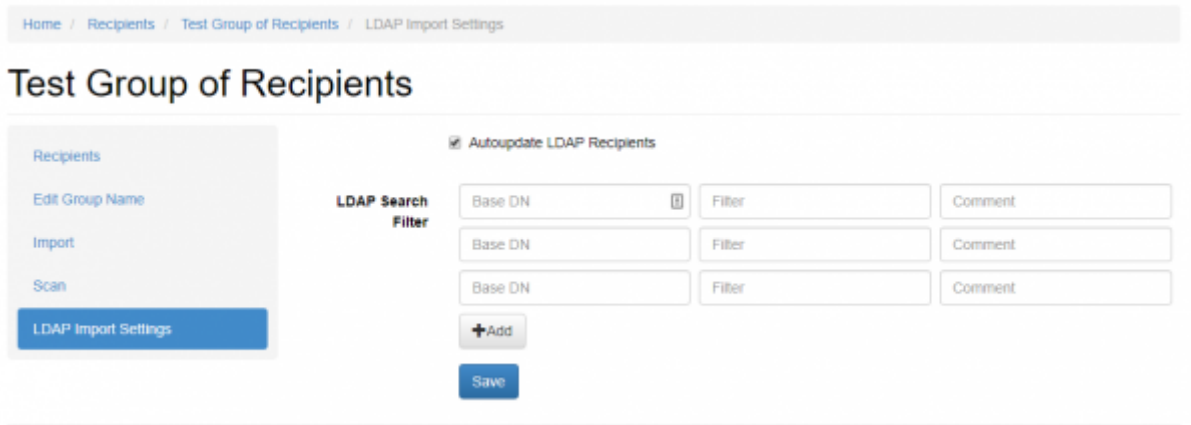


LUCY will automatically match the user's attributes in the LDAP directory with the available recipient attributes in LUCY.

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 enabled.



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

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

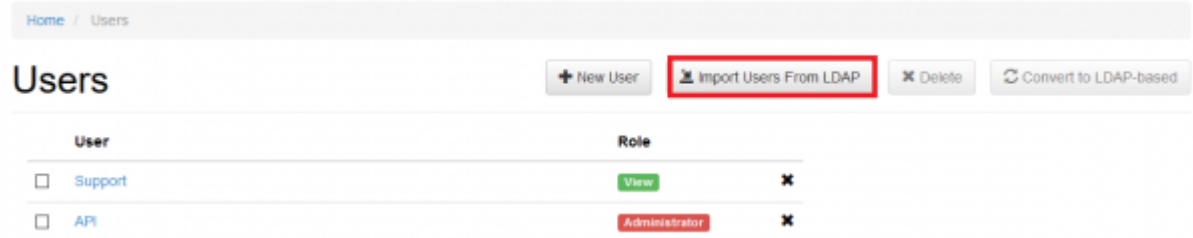
See Microsoft Documentation for more info.

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

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=ldap_integration&rev=1559639171

Last update: **2019/07/25 12:51**