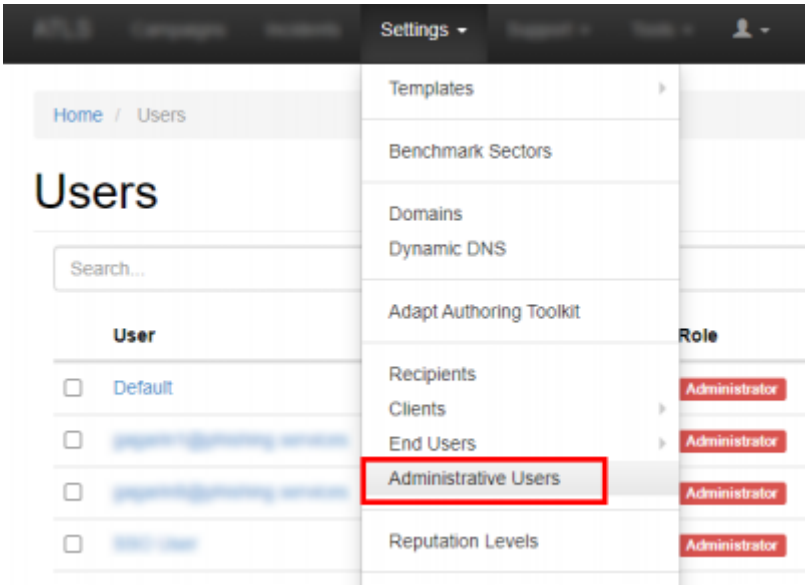
# Introduction

LUCY offers a role-based access control (RBAC), restricting system access to authorized users. The permissions to perform certain operations are assigned to specific roles within the user settings. Members or staff (or other system users) are assigned particular roles, and through that role, assignments acquire the computer permissions to perform particular LUCY functions.

## Where can you configure the user settings?

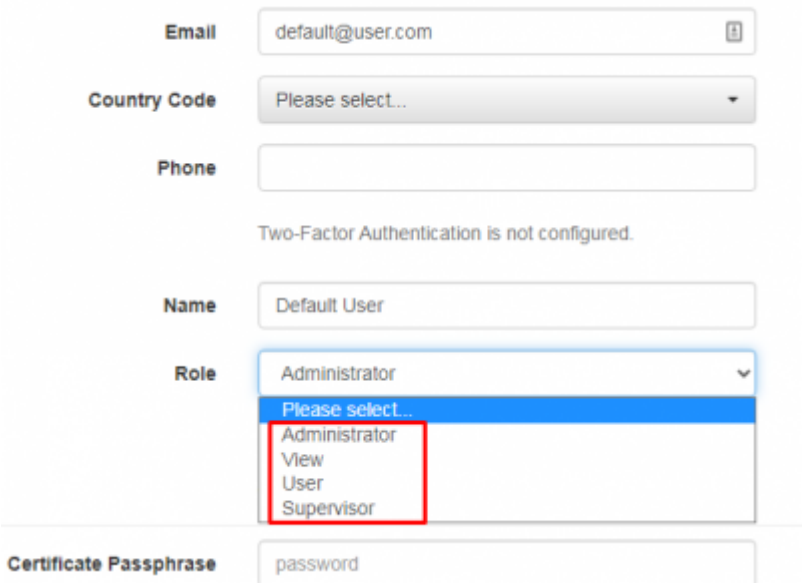
In LUCY you will find the user settings under **Settings** > **Administrative Users**. Press **+New User** button in order to set up new account.




## User Roles in Lucy

There are four types of admin accounts in Lucy:

1. Administrator
2. User
3. View
4. Supervisor




**Please note** that there are also End Users accounts in Lucy that come as a part of End User Portal functionality and have no admin rights. This type of accounts is automatically created for the recipients that were assigned to awareness training. More info here

# Is there a limitation on how many users can access LUCY?

No. You have the ability to create as many LUCY users that can access the web console as you want.

# What are the different user roles?

## Administrator

An administrative account with full access and the highest priveleges. An administrator is capable of creating and deleting campaigns, managing all the custom data: recipients, clients, templates and etc. Administrator is also able to manage other administrative users' account data. You cannot segregate administrators in a way, that an admin A doesn't see the clients from an admin B. This can only be done in the LUCY SaaS edition. However, content and recipient data can be managed separately with Users type of administrative account.

## User

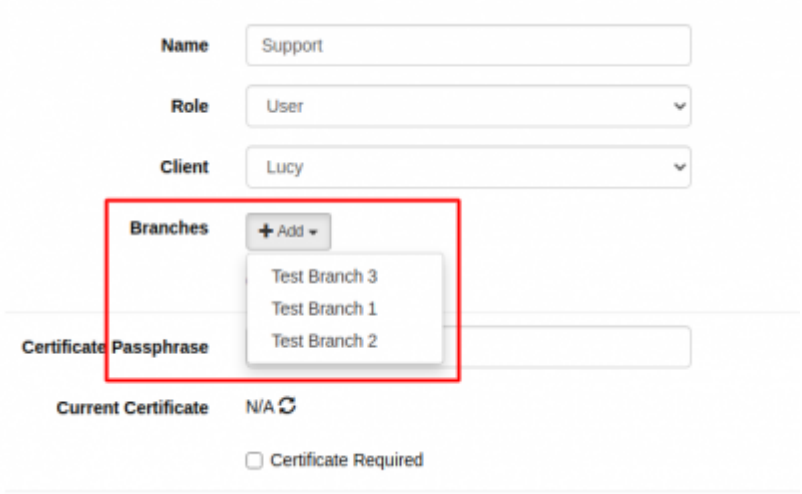
This user role can be used in order to separate control of Lucy content based on its affiliation with Clients. Users attributed to specific clients and branches (see below) will have access only to content (campaigns, custom templates, recipient groups) attributed to the same clients and branches. Please make sure to disable the user's permission "Access all Campaigns" to avoid the users from different clients / branches to access the data of one another. Details on this permission are mentioned in the table below in this article.

### Branches

Starting from the 4.8 version Branches functionality is introduced in Lucy.

In order to manage client-related Administrative Users, Lucy allows to create Branches for a client and may represent practically anything - from a tier of management to physical locations, to languages, to organization divisions, to openly defined security levels.

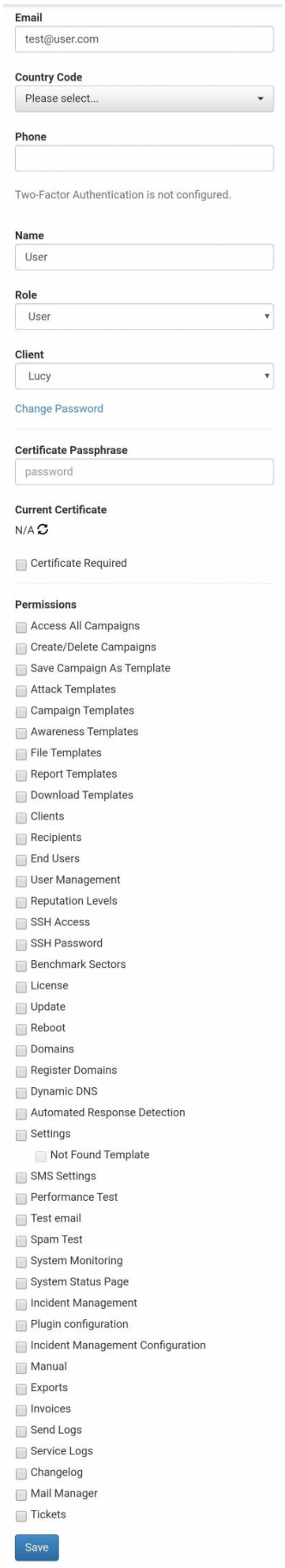
In case a client has already predefined branches (under the Settings > Clients > Branches - more here) it is possible to assign them to a user.




### User permissions

This user role can be given individual rights for each LUCY feature. After filling out personal data for User account, one may choose various user permissions - that will define which data User will have access to and which Lucy functionality will be available for that account.

**Please Note** - **Clients** and **Branches** attributes access policy. In order to separate control of the data related to particular **Clients** and **Branches** users are granted access to the content (templates, recipient groups, campaigns, reports) associated with their **Client** and **Branch** attributes. Also, data that is not associated with any client or branch is available for all users despite the **Clients** and **Branches** attributes access policy. Some of the **User permissions** are affected by this policy. Please refer to the table below in order to check whether **Clients** and **Branches** attributes access policy affects certain permission.


Email
test@user.com
Country Code
Please select...
Phone
Two-Factor Authentication is not configured.
Name
User
Role
User
Client
Lucy
Change Password
Certificate Passphrase
password
Current Certificate
N/A
Certificate Required
Permissions
Access All Campaigns
Create/Delete Campaigns
Save Campaign As Template
Attack Templates
Campaign Templates
Awareness Templates
File Templates
Report Templates
Download Templates
Clients
Recipients
End Users
User Management
Reputation Levels
SSH Access
SSH Password
Benchmark Sectors
License
Update
Reboot
Domains
Register Domains
Dynamic DNS
Automated Response Detection
Settings
Not Found Template
SMS Settings
Performance Test
Test email
Spam Test
System Monitoring
System Status Page
Incident Management
Plugin configuration
Incident Management Configuration
Manual
Exports
Invoices
Send Logs
Service Logs
Changelog
Mail Manager
Tickets
Save

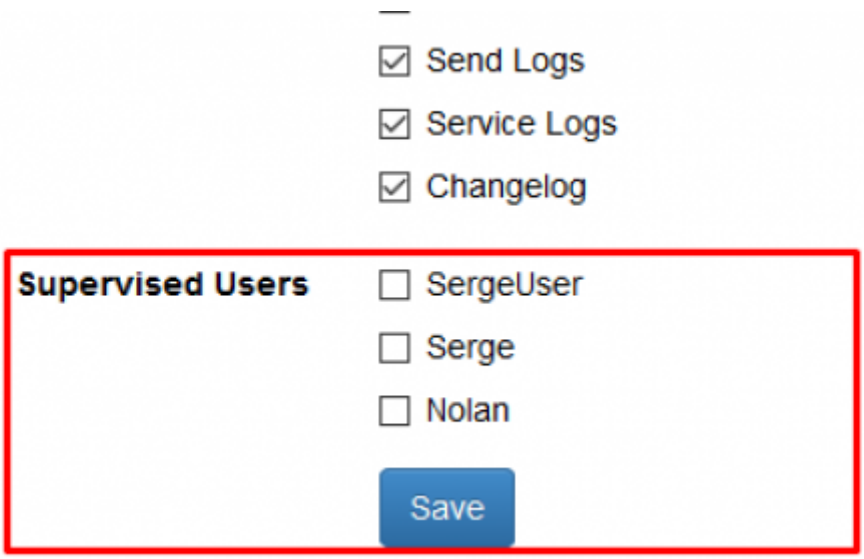
### List of permissions and its description

| | |
|---|---|
| Access All Campaigns | Right to access campaigns. If you activate this checkbox, the user can access all campaigns, regardless of who created them. This permission overrides **Clients** and **Branches** attributes access policy. |
| Create/Delete Campaigns | Right to Create or Delete campaigns. The user can create and delete campaigns and later access only the campaigns he created himself. Campaigns of other users are not displayed. |
| Save Campaign As Template | Right to save a campaign as a template. A campaign template can be used in the setup process when generating new campaigns. |
| Attack Templates | Access to the list of Attack Templates. Attack templates are predefined emails or websites which can be used for phishing simulations. Affected by **Clients** and **Branches** attributes access policy. |
| Campaign Templates | Access to the list of Campaign templates. Affected by **Clients** and **Branches** attributes access policy. |
| Awareness Templates | Access to the list of Awareness Templates. Awareness templates are used in training campaigns. Affected by **Clients** and **Branches** attributes access policy. |
| File Templates | Access to the list of File Templates. Affected by **Clients** and **Branches** attributes access policy. File Templates are used for file based attacks. |
| Report Templates. Affected by **Clients** and **Branches** attributes access policy. | Access to the Report Templates |
| Download Templates | Access to the menu of Templates Downloading |
| Clients | Access to the Clients menu |
| Recipients | Access to the list of Recipients. Recipients are the users that get attacked or trained. Affected by **Clients** and **Branches** attributes access policy. |
| End Users | Access to the list of End Users |
| User Management | Access to the User Management |
| Reputation Levels | Access to the Reputation Levels |
| SSH Access | Access to the SSH Access menu |
| SSH Password | Right to reset SSH Password |
| Benchmark Sectors | Access to the Benchmark Sectors |
| License | Right to access License menu |
| Update | Right to Update LUCY |
| Reboot | Right to Reboot LUCY |
| Domains | Right to access Domains menu |
| Register Domains | Right to register a domain |
| Dynamic DNS | Access to Dynamic DNS feature. |
| Automated Response Detection | Access to the Automated Responce Detection menu |
| Settings | Access to the Advanced Settings including the abillity to customize the 404 (not found page) |
| SMS Settings | An ability to set up Short Message Service (SMS) systems to send out text messages. LUCY has a build-in API that will connect to a centralized LUCY gateway when initializing SMS delivery. Please find more information here |
| Performance Test | Access to the Performance Tests |
| Test email | Right to send a test email |

| | |
|---|---|
| Spam Test | Access to the Spam Test |
| System Monitoring | Access to the System Monitoring |
| System Status Page | Access to the System Status Page. The status page gives a user access to certain logs |
| Incident Management | Access to the Incident Management |
| Plugin configuration | Right to configure Outlook plugin |
| Incident Management Configuration | Right to configure Incident Management |
| Manual | Access to LUCY manual. This is the WIKI page hosted on th LUCY server |
| Exports | Access to the exports |
| Invoices | Access to the Invoices. Invoices can be created inside LUCY as a receipt for purchases like domains, sms credits etc. |
| Send Logs | Access to "Send Logs" menu. |
| Service Logs | Access to the Service logs |
| Changelog | Access to the Changelog |
| Mail Manager | Access to the Mail Manager |
| Tickets | Access to the Ticket system |

## Supervisor

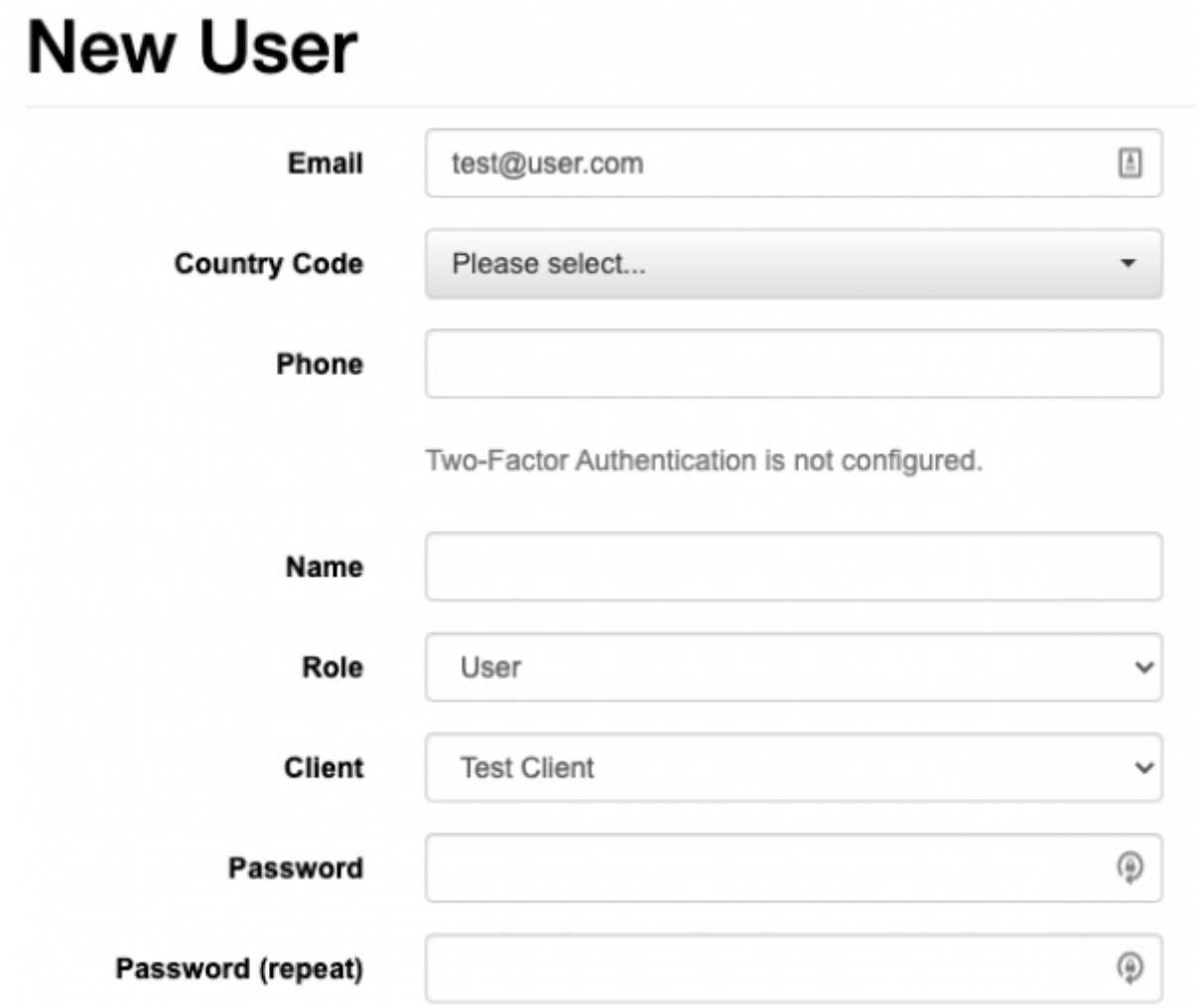
Maintain the overview with access to the campaign specifications. Communicate directly with the campaign creator (user) to suggest changes and give approval to greenlight the campaign. The supervisor is in the hierarchy above the user. Therefore it is not possible to supervise a system admin. The Supervisor is technically the same as the user account, but you may assign users to the supervisor account and approve/reject their campaigns. Within the settings you can select which users you want to supervise:



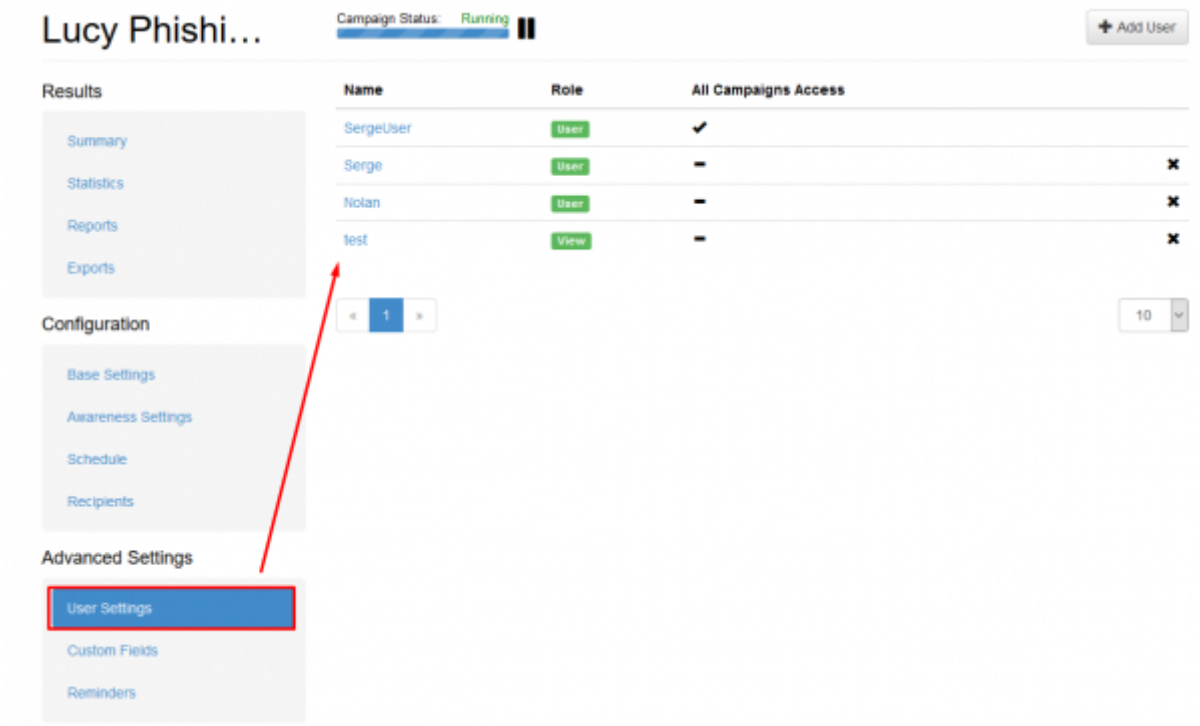

You have the ability to define a supervisor who is able to START/STOP the campaign which was created by a user. To do so add a user to a campaign with all permissions selected, add his supervisor to the same campaign with "Campaign start/stop" permission selected. As a result, the supervisor will only be able to go into the campaign and approve or reject the start.

## View Only Users

The View Only User can only see certain statistics of the campaign. This user cannot start/stop a campaign. The user also has no rights in viewing or changing any of the campaign settings. First, you need to create a client name. The client name is always associated with a campaign. Then you can associate that user with the **Client** and **Branch**. As a result, the View Only User will only see all the campaigns which belong to that specific client.

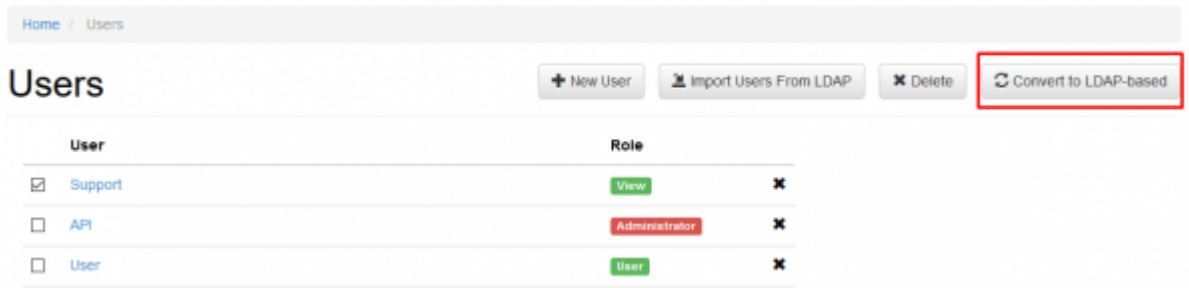



Please make sure you also add the view only user to the specific campaign:




## How to convert users to LDAP-based?

Lucy has the ability to convert the account to LDAP-based, so existing user can be logged in through LDAP. You can convert multiple accounts at once by selecting the necessary users and clicking the button "Convert to LDAP-based":




*Note:* Lucy admin should configure the connection to Active Directory service to be able to use this feature. Please find more information about LDAP Integration here.

## Can I enforce a password policy or strong authentication?

Yes. It is possible to adjust the password policy in the advanced settings. Please find more here.

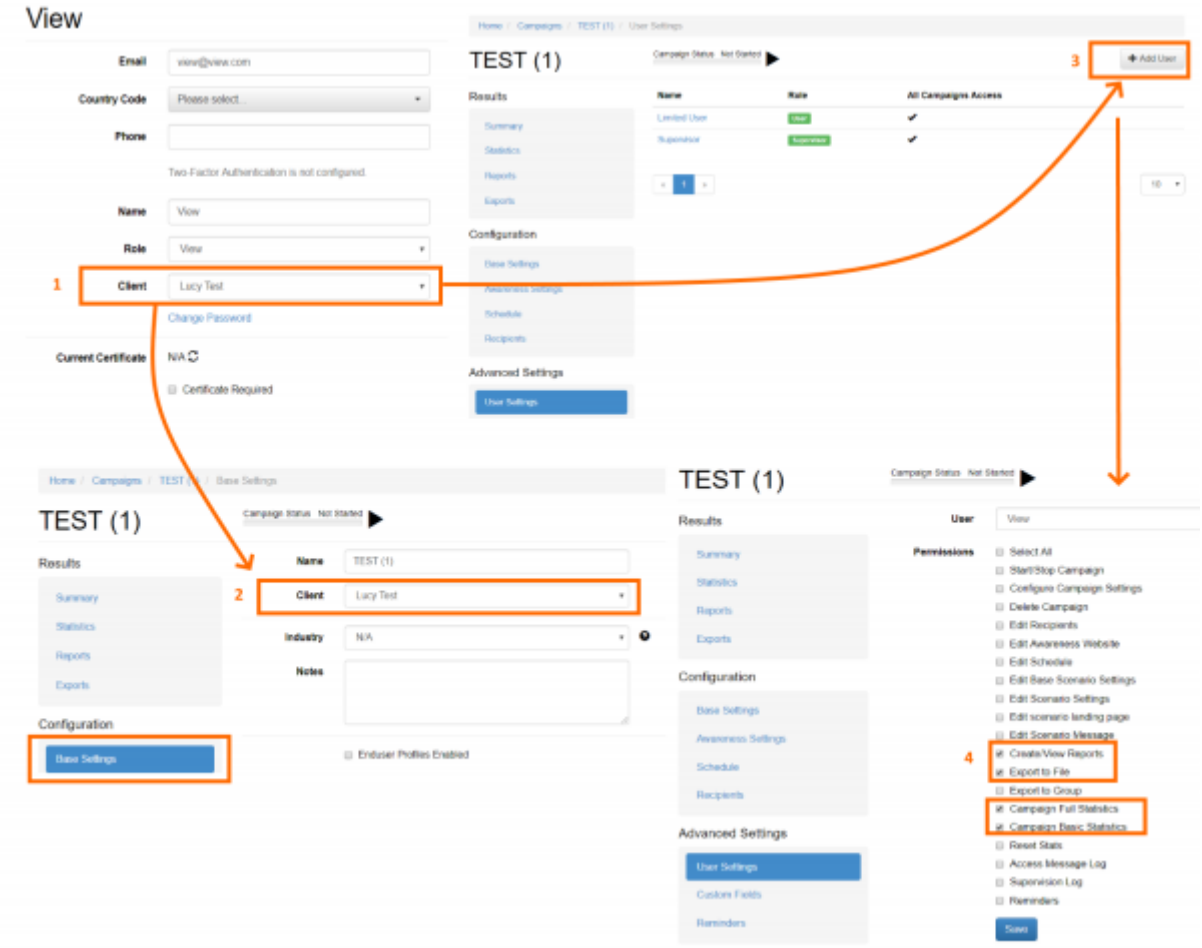
## Can I authenticate administrative users via SSO?

Yes. It is possible to use the AD Federation service and authenticate the users automatically. See chapter SSO.

# How to set up a multitenant capable administration

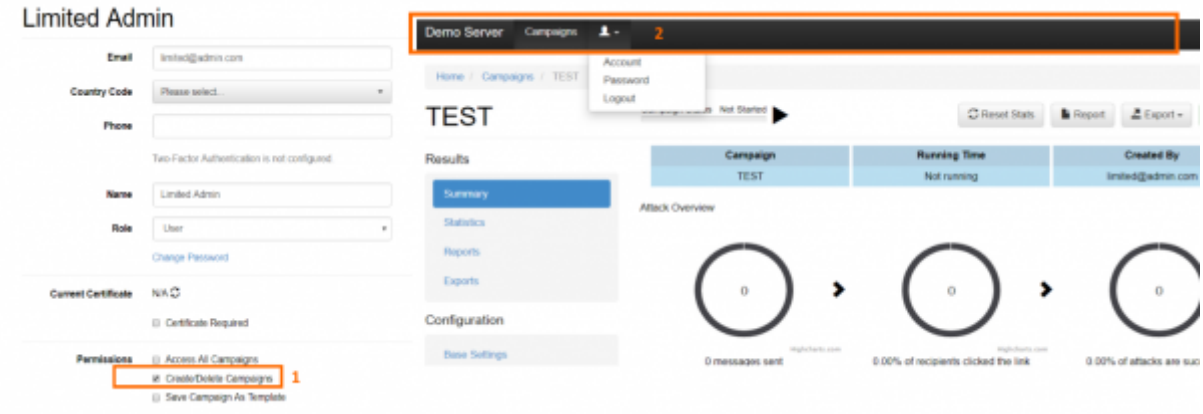
To set up a multitenant capable administration, you first need an administrator account. From there you can set up the appropriate users and rights. Here are two use cases and the corresponding configuration:

**Use case 1**: You create a campaign for your customer but want to give your customer access to the statistics within the campaign. It must be ensured that the customer only sees his own data and cannot intervene in the campaign configuration.




**Solution use case 1:** You create a view-only account (1) in "settings/users" and assign this account to your customer. As soon as you create a campaign, you will be asked to enter the customer of the campaign (2). The customer can be yourself, an organizational unit or a third party. Next, you should add the user to the campaign (3). You can then assign the rights to view the statistics to the user (4).

**Use case 2:** You have a customer who wants to create their own campaigns. However, the customer should only have access to his statistics and not see other customers.




**Solution use case 2:** You create an account with the status "user" in "settings/users". Give the user only the right "Create/delete campaign" (1). As soon as the customer logs in, he can then create his campaign and see only the data of the campaigns he created himself (regardless of the assignment of the customer). He won't have access to any other menu item (2). However, there are areas where this limited administrator has access to possibly sensitive data of other customers. Examples are custom-created templates that may contain customer-related information. But also all recipient groups created on the system can be seen by this customer when assigning recipients.