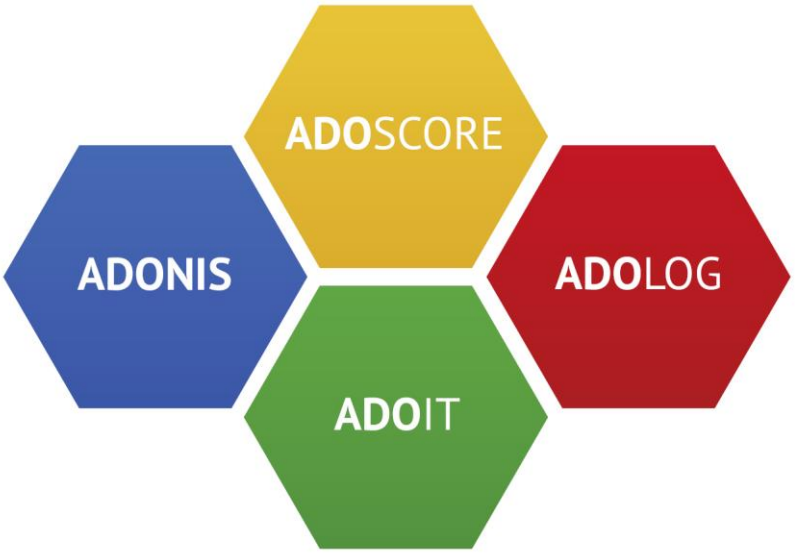
# Ask ADONIS NP / ADOIT

## Setup manual

Version 3.0




www.boc-group.com

# Content

# 1 Set up authenticated access to ADONIS NP / ADOIT

## 1.1 Requirements

The supported product and versions for the authenticated access are listed in the table below.

| Product | Version |
|---|---|
| ADONIS NP | 10.0.3 or higher |
| ADOIT | 11.0.3 or higher |

The supported mobile devices are:

- Phones and tablets using **Android 7.1** or higher.
- Apple iPhones and iPads using **iOS 12.0** or higher.

For mobile data connection we recommend 3G or higher.

## 1.2 Install ADONIS NP / ADOIT

Install the BOC Management Office product according to the Installation Manual.

## 1.3 Create Technical User in the Administration Toolkit

**Please note**

- Further information on setting up REST can be found in the full REST API Documentation, contained in the installation directory of your BOC Product (<installation directory>\books\rest\REST API Documentation.html).

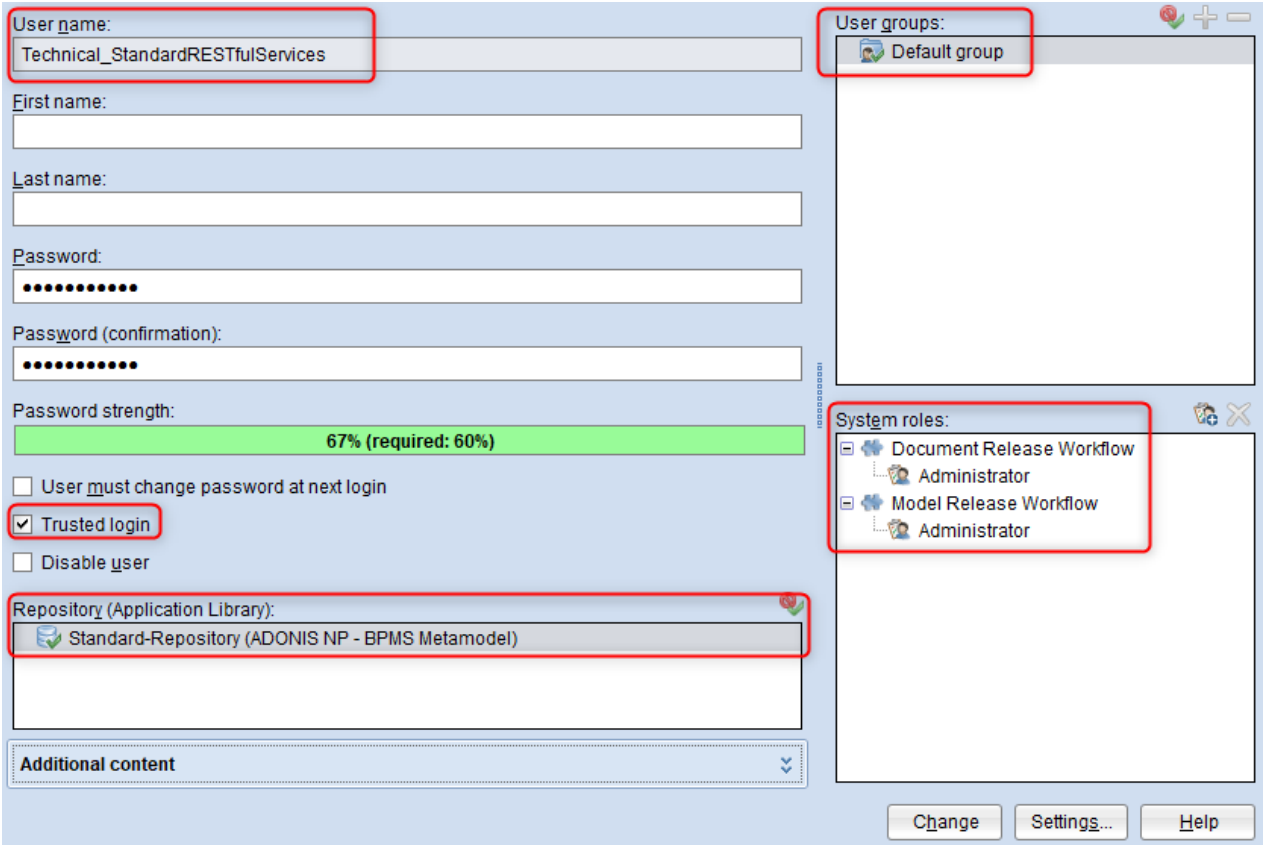
Create the following technical user in the Administration Toolkit:

- **User name**: “Technical_StandardRESTfulServices” (and a password of your choice)
- **Repository**: Only (!) assign the repository to the user which holds the data to be queried.
- **User groups**: This user belongs to the default group.
- **System roles**: If release workflows are licensed, and you want to use repository write APIs, map the technical user to the “Administrator” roles:

  - **ADONIS NP**: Document Release Workflow and Model Release Workflow
  - **ADOIT**: EA Workflow
- **Trusted Login**: Yes

**Important notes**

- You cannot activate “Trusted Login” during user creation. Only rights of already created users can be modified. Use the button “Create” in the “Create New User” tab to create the user before you activate “Trusted Login”.
- Creating a technical user is necessary regardless of the authentication method, as it is required for loading the initial configuration.



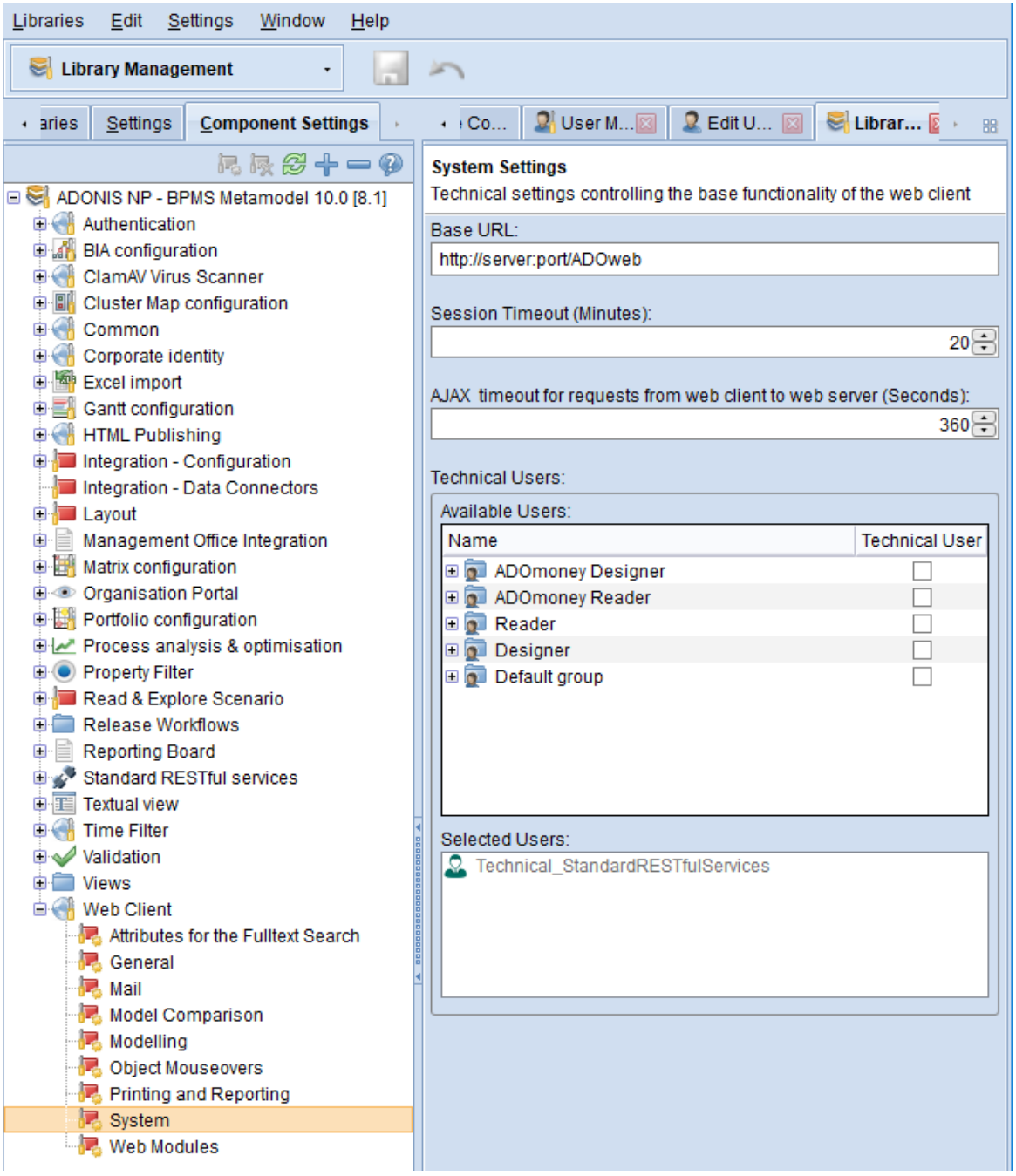

*1 Create technical user in the Administration Toolkit*

## 1.4 Edit System Settings

Now you must define a few technical settings controlling the base functionality of the web client. To edit the System settings:

1. Open the Library Management and switch to the tab Component Settings.

2. Double-click the desired library to open the list of components available for configuration.
3. Double-click Web Client, and then double-click System.
4. In the Base URL field, enter the URL where the web client can be reached from other machines.
5. In the Technical Users field, select the technical user you created from the Available users list, i.e. “Technical_StandardRESTfulServices”.
6. Click OK.




*2 System settings*

### Base URL Example

- You are configuring ADONIS NP 10.0. You are running the ADONIS NP web client on a machine with the IP 10.2.100.68. The URL should look like this: "*http://10.2.100.68:8000/ADONISNP10_0*"

### 1.4.1 Edit Settings for Standard RESTful Services

Now the Standard RESTful Services settings have to be adapted. In order to do so:

1. Open the Library Management and switch to the tab Component Settings.
2. Double-click the desired library to open the list of components available for configuration.
3. Double-click Standard RESTful Services, and then double-click General.
4. Select the Enable MFB REST globally check box to enable the Standard RESTful Services. All other options in this area are inactive unless you select this check box.
5. Setup a key, secret and pick a select a Technical User for the RESTful Services.

**Note on Technical User selection**

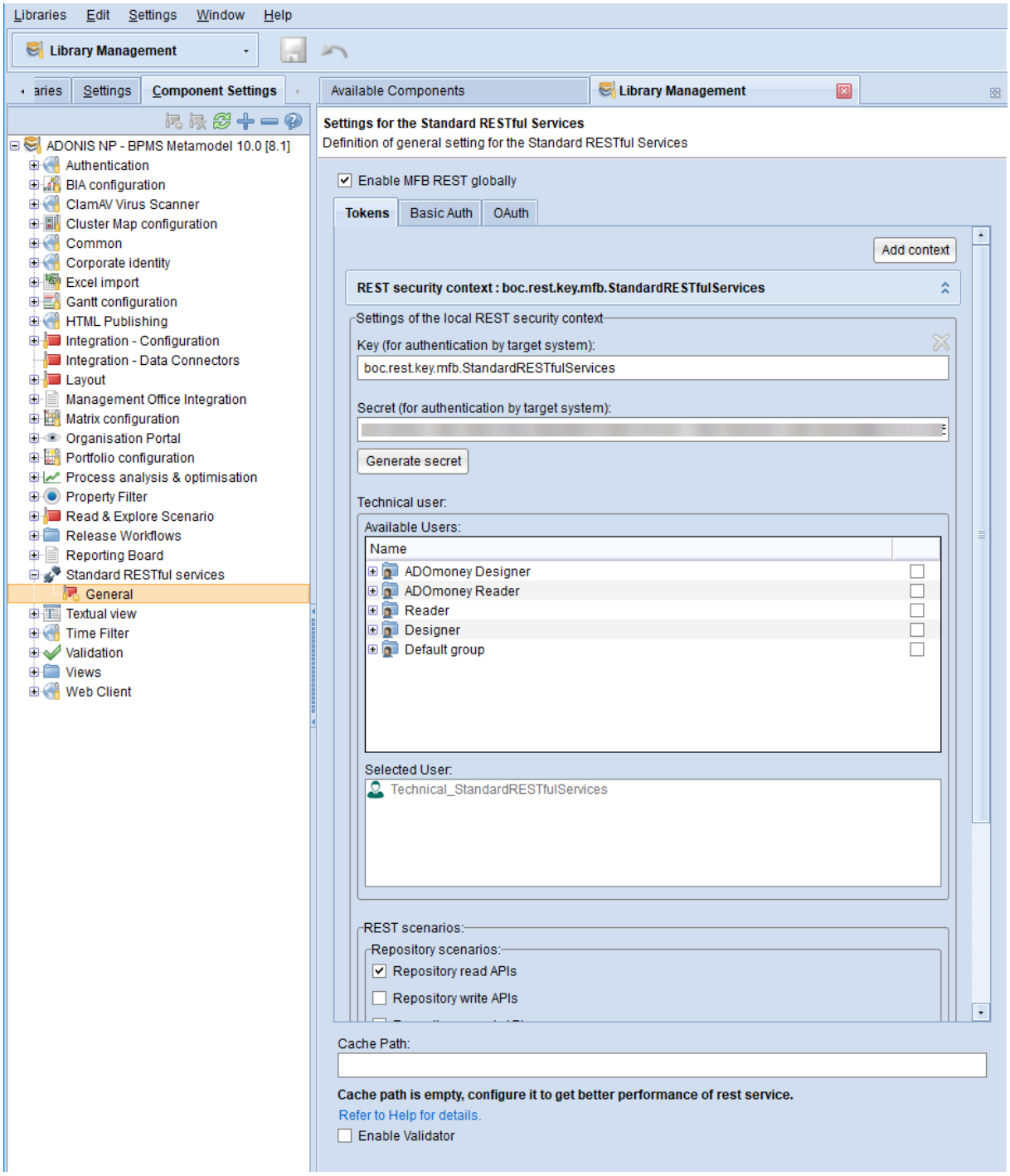
- This step is necessary for each type of RESTful Service authentication mechanism.
- The users that will be logged in via OAuth2 *will not have* the same permission rights as the Technical user defined in this setting.

6. [Recommended] Optionally, enable Cache path

   This parameter is optional. Enter the absolute path to the directory in which cache files must be stored. The user under which the Apache Tomcat web server service is running must have write access to this directory.

   Advantages of using this parameter:

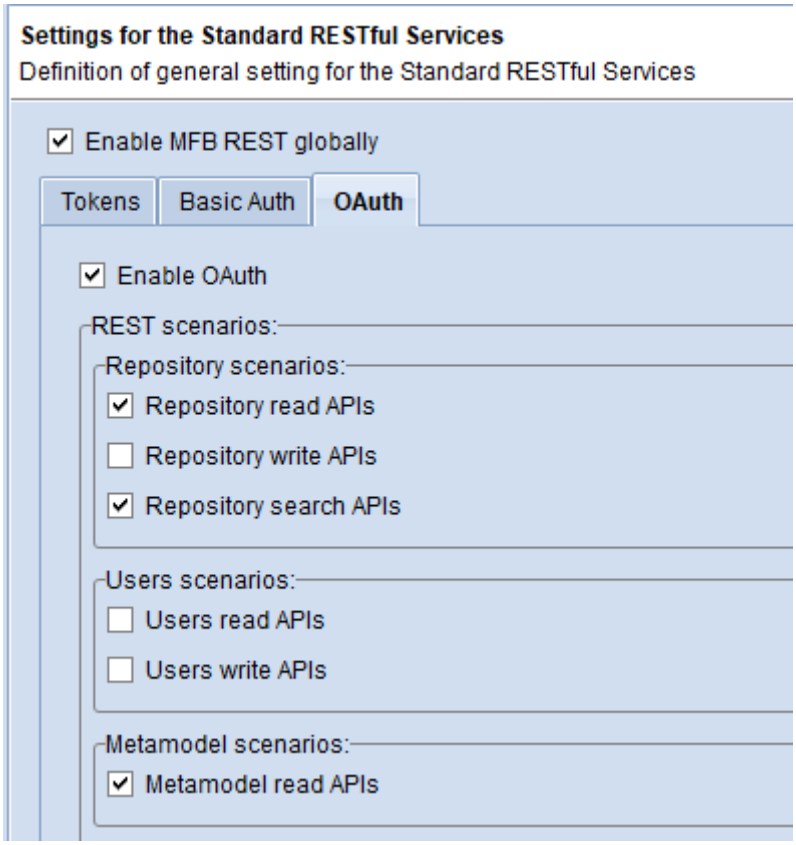
   - Model images and model image maps are generated only once and then cached. Every time the model image or image map is requested, a check is performed if the model has changed. If there are no changes, the information is loaded from the file system. Otherwise, the cache is updated first. As a result, responses to these types of requests are faster and use fewer server resources.
   - For search jobs the advantage is that created queries are saved in cache files and can be reused after a server restart. Without the cache path, queries are saved only in memory and are lost during restart.




*3 Settings for the Standard RESTful Services*

7. Edit the settings in the OAuth tab.

   a. Make sure the OAuth tab looks like this:




*4 Settings for the Standard RESTful Services (OAuth)*

   b. Click OK when you have completed the settings.

**Note**: In addition to enabling OAuth in the component settings, it must be enabled on the Admin Page as well. To do so:

   c. Open a web browser and navigate to http://<SERVER_NAME>:<TOMCAT_PORT>/<PRODUCT><VERSION>/admin.view.

   d. Enter your credentials (if needed) and log in.

   e. Go to Authentication → OAuth 2.0.

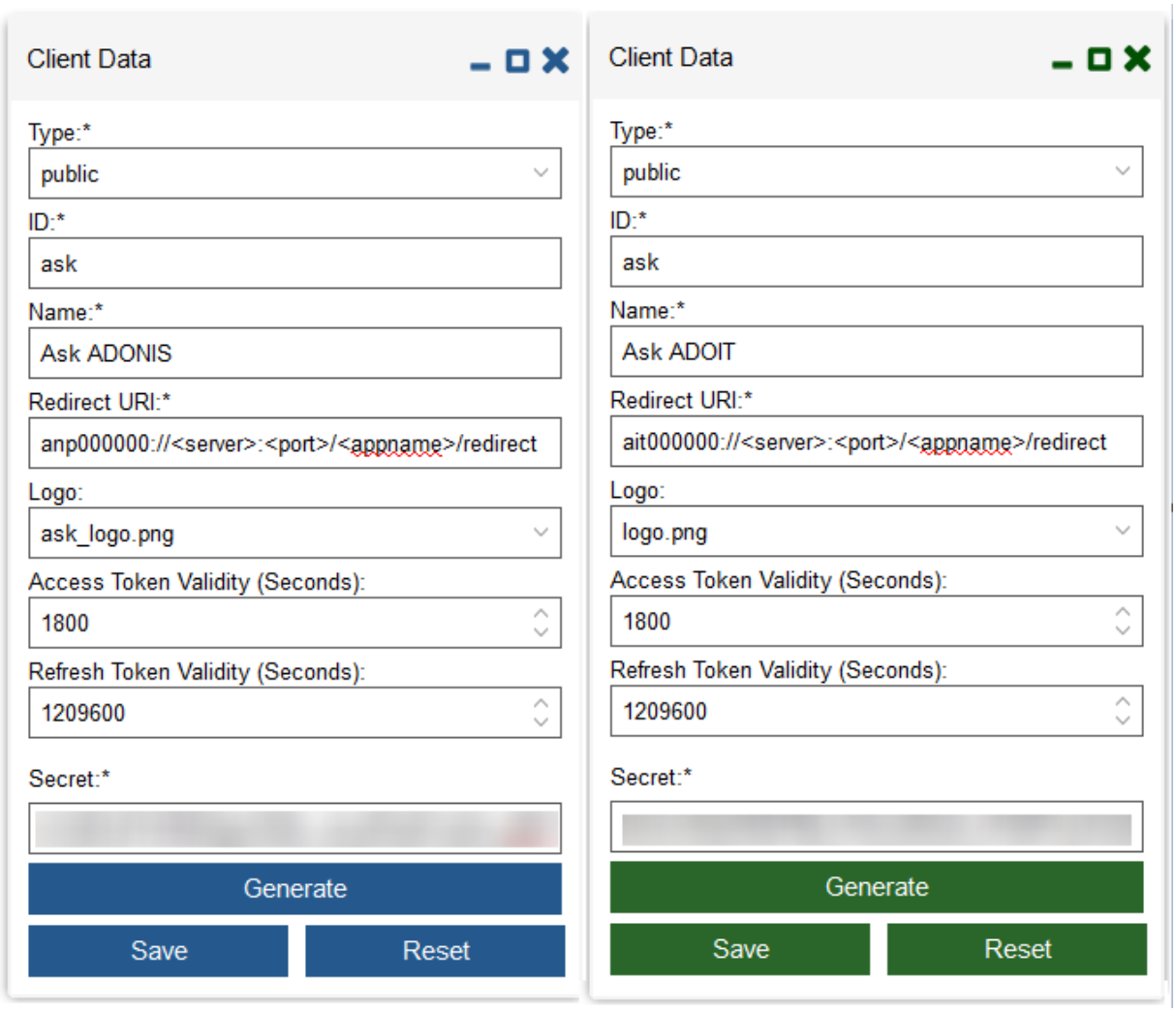
   f. Select the OAuth 2.0 enabled check box to enable OAuth.

   g. Click the Upload Logos button to upload a logo to represent the client application.

   h. Click the Add button to add a new client. The Client Data dialogue box opens.

   i. Complete the Client Data form. Save the changes afterwards.

      i. Make sure that the Client Data from looks like this:




*5 Client Data settings (ADONIS NP and ADOIT)*

ii. Especially:

- **Type** is “Public”.
- **ID** is “ask”.
- **Redirect URI**
  a. **ADONIS NP:** must start with “anp000000://” and end with “/redirect”.
  b. **ADOIT:** must start with “ait000000://” and end with “/redirect”.

j. Back on the OAuth 2.0 page, click Save changes to save the changes made on this page. Once the changes are saved on the Admin Page, they take effect immediately. A restart is not required.

8. *Done! Restart the Apache Tomcat web server and the application server. You can use the Ask Mobile apps for ADONIS NP / ADOIT.*

**Please note**

- Further information on setting up REST can be found in the full REST API Documentation, contained in the installation directory of your BOC Product (<installation directory>\books\rest\REST API Documentation.html).eeeeee

## 1.5 Additional setup for SSO scenarios

In case SSO is being used for user authentication, the following URL patterns must be whitelisted and passed through the ADONIS NP/ADOIT web application, without requiring user authentication:

if the base URL for ADONIS NP/ADOIT is:

- *https://ado.your-company.com/*

then the URL patterns to whitelist are:

- *https://ado.your-company.com/rest*
- *https://ado.your-company.com/oauth2*

including all the sub paths (e.g. to include *https://ado.your-company.com/rest/connection*).

While using the ASK Mobile Apps, the user will still be authenticated thro1ugh SSO during the first login.

## 1.6 Troubleshooting

### 1.6.1 Configuration of OAuth2 is deleted after the server is restarted

In case the OAuth2 configuration is deleted every time the ADONIS NP/ADOIT server is restarted, then it might be that a configuration is invalid after a recent migration or upgrade of the product.

To fix this issue, open the web properties file from:

- *<tomcat>\webapps\<ADONIS NP/ADOIT>\adoxx_web.properties*

and make sure that the following key is set to false:

- *auth.config.forceMigration=false*

Restart the ADONIS NP/ADOIT server and configure again OAuth2 (see chapter 1.4.1). Now the OAuth2 settings should not get deleted anymore.