BExIS 2.6.1

Security System

User Guide

Authors

Sven Thiel, Roman Gerlach, Nafiseh Navabpour

Contact

Website: <http://fusion.cs.uni-jena.de/bexis>

Email: bexis-support@uni-jena.de

Phone: +49-(0)3641-948968

Acknowledgement

The development of the BExIS 2 software would not be possible without the German Science Foundation (DFG) funding the BExIS++ project. BExIS++ is a collaboration of the Friedrich-Schiller-University Jena, Germany (Dept. of Computer Science, Dept. for Geography, Dept. of Ecology) and the Max-Planck-Institute for Biogeochemistry Jena, Germany.

Content

[1. Overview 3](#_Toc412188897)

[2. Account 3](#_Toc412188898)

[2.1. Registration 3](#_Toc412188899)

[2.2. LogOn 4](#_Toc412188900)

[3. Users 4](#_Toc412188901)

[3.1. Create a user 4](#_Toc412188902)

[3.2. Edit a user 5](#_Toc412188903)

[4. Groups 5](#_Toc412188904)

[4.1. Create a group 5](#_Toc412188905)

[4.2. Edit a group 6](#_Toc412188906)

[5. Permissions 6](#_Toc412188907)

[5.1. Features 6](#_Toc412188908)

[5.2. Datasets 8](#_Toc412188909)

# 1. Overview

**Caution! Do not delete the preset user and group!**

*Users*. After installation there is just a single user inside the database. The user name is “Administrator” and the password is “gWg2xG”. By default, this user has full access to the whole application (because of the relationship to group “Admin”, see next paragraph).

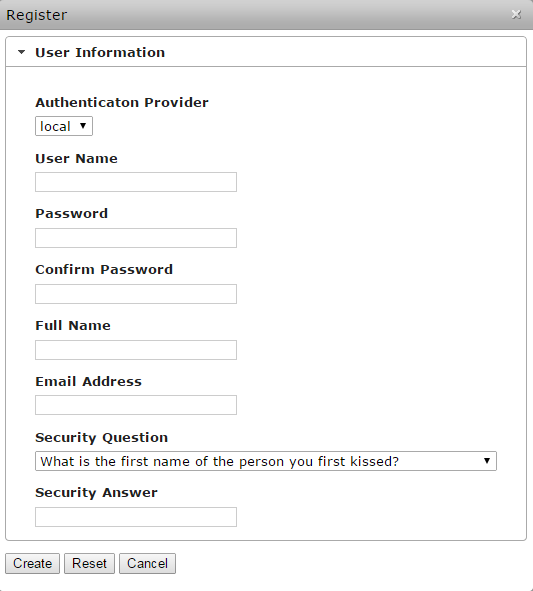
*Groups*. Similar to *Users*, there is just one group inside the database – and the group name is “Admin”. In addition to that, the user “Administrator” belongs to that group. By default, this group grants full access to the application.

*Features.* The set of features is fixed and corresponds to the different hierarchical items of the menu bar.

*Permissions*. Within the system, it is possible to add, remove or modify existing permissions on features and datasets.

# 2. Account

By default, only a few components of BExIS are accessible for anonymous users. Any further access to the application is available for authorized users, only. Therefore you need to register and create an account. After a successful registration you are able to logon to BExIS using your account credentials for authentication.



## 2.1. Registration

First press **[ Register ]** in the upper right corner. You have to complete the form before you press Register, otherwise the registration will fail. Furthermore, the system supports you with different validation messages if any information is not valid.

## 2.2. LogOn

First press **[ LogOn ]** in the upper right corner. The system redirects you to the logon form and you have to enter your account credentials (user name and password). If the logon is successful, you will see a short welcome message instead of **[ LogOn ]**. Otherwise, the system will notify you about the status and reason why the logon was not successful.

# 3. Users

**Caution! This part of the system is secured. You may not have access to it.**

BExIS provides different features for managing users. These are typically available to system administrators only. Each of them is described in more detail in one of the following subsections.

## New Picture (19).bmp

## 3.1. Create a user

In addition to the self-registration procedure, user accounts may also be created by an administrator. This feature is available from **Administration > Authorization > Users**. Please press the **Create** button. A modal window will pop up that contains the user creation form. Similar to the self-registration, the system supports you with validation on all information entered.

## New Picture (20).bmp3.2. Edit a user

Within BExIS you are able to display and modify user information. For security and usability reasons, the system allows modification only for certain parts of the user information. Please go to **Administration > Authorization > Users** and press the Edit button of the respective user. You are now able to alter the user information. Changes are committed to the system when you press the **Save** button.

For any given user memberships to certain groups need to be specified via the tab **Membership**.

You can change the status easily by (un)select the corresponding checkbox.

You can also delete a user directly by clicking on the Delete button. The deletion will be confirmed by clicking the **Delete** button.

# 4. Groups

**Caution! This part of the system is secured. You may not have access to it.**

BExIS provides different features for the managing groups. They are typically available to system administrators only. Each of them is described in more detail in the following subsections.

## New Picture (21).bmp

## 4.1. Create a group

This feature is available from **Administration > Authorization > Groups**. Please press the **Create** button. A modal window will pop up that contains the group creation form. The system supports you with validation on all information entered.

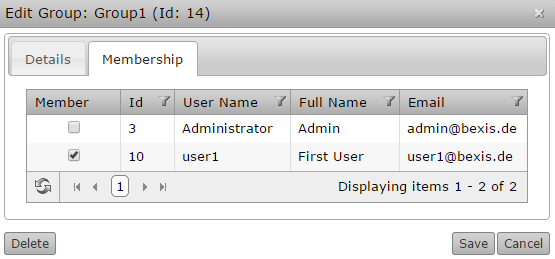
## 4.2. Edit a group

Within BEXIS you are able to display and modify group information. Please go to **Administration > Authorization > Groups** and press the Edit button of the respective group. You are now able to alter the group information. Changes are committed to the system once you pressed the **Save** button.

For any given user memberships to certain group need to be specified via the tab **Membership**.

You can change the status easily by (un)select the corresponding checkbox.

You can also delete a group directly by clicking on the Delete button. The deletion will be confirmed by clicking the **Delete** button.



# 5. Permissions

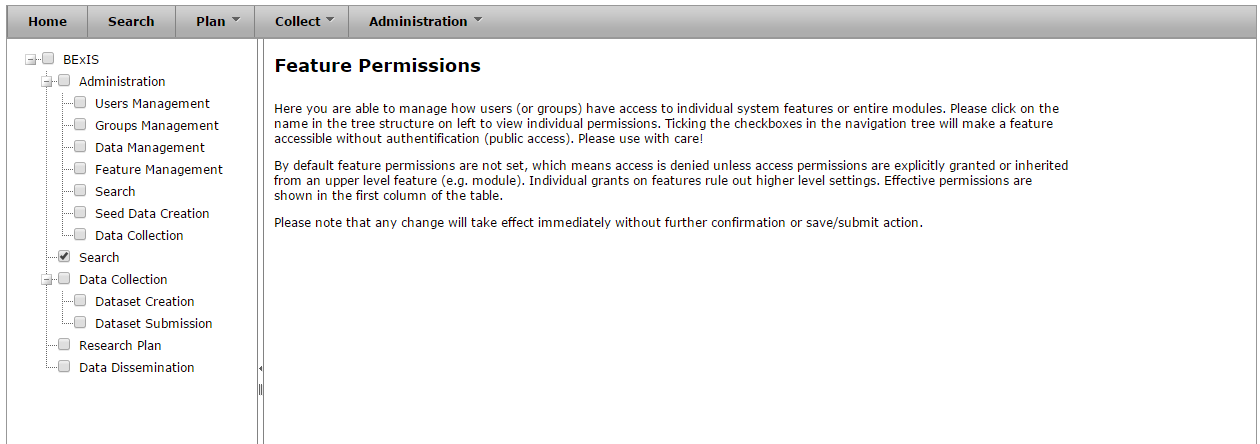
**Caution! This part of the system is secured. You may not have access to it.**

Permission is a rule that contains certain security regulations. In general, it is possible to set a rule on both, users and groups.

The security system of BExIS distinguishes between two types of permissions. On the one hand, there are feature permissions, which allow or prohibit the access to well-defined and delimited areas of the application. This type of permissions is working on functional objects (e.g. actions that should be performed) – so called *Features*. On the other hand, data permissions provide the ability to protect real data (e.g. datasets, research plans and so on).

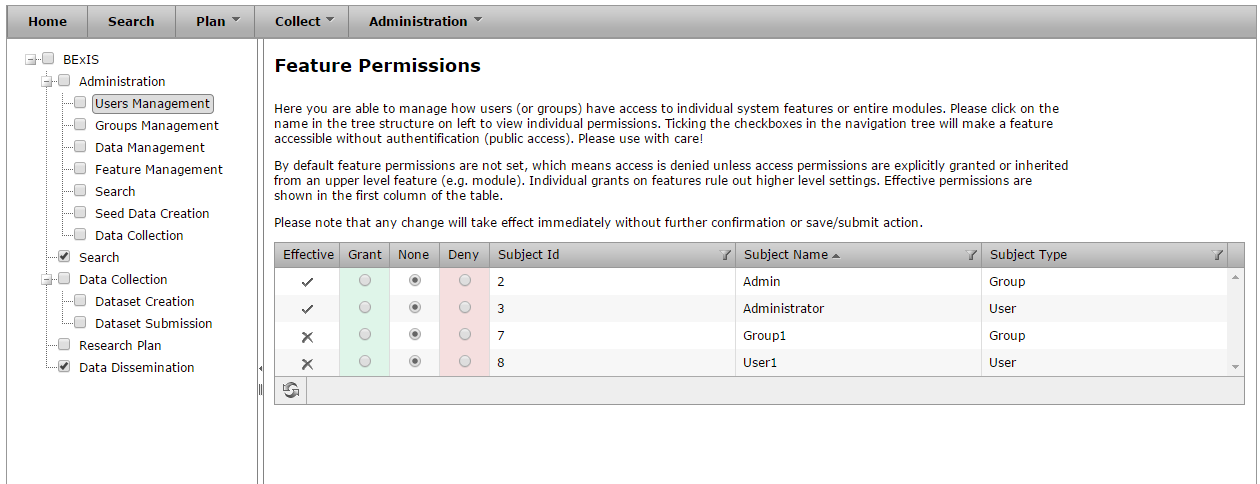
## 5.1. Features

Currently, features are fixed. It is not possible to add, edit or remove features. Furthermore you are not able to change well-defined and delimited area of a feature, but later on, the administrator will be able to modify features also. Please go to **Administration > Authorization > Features Manager**. This will bring up a page with a tree on the left side.



Selecting a checkbox in the navigation tree (e.g. Search) will make that feature accessible without authentication (public access). Please use with care!

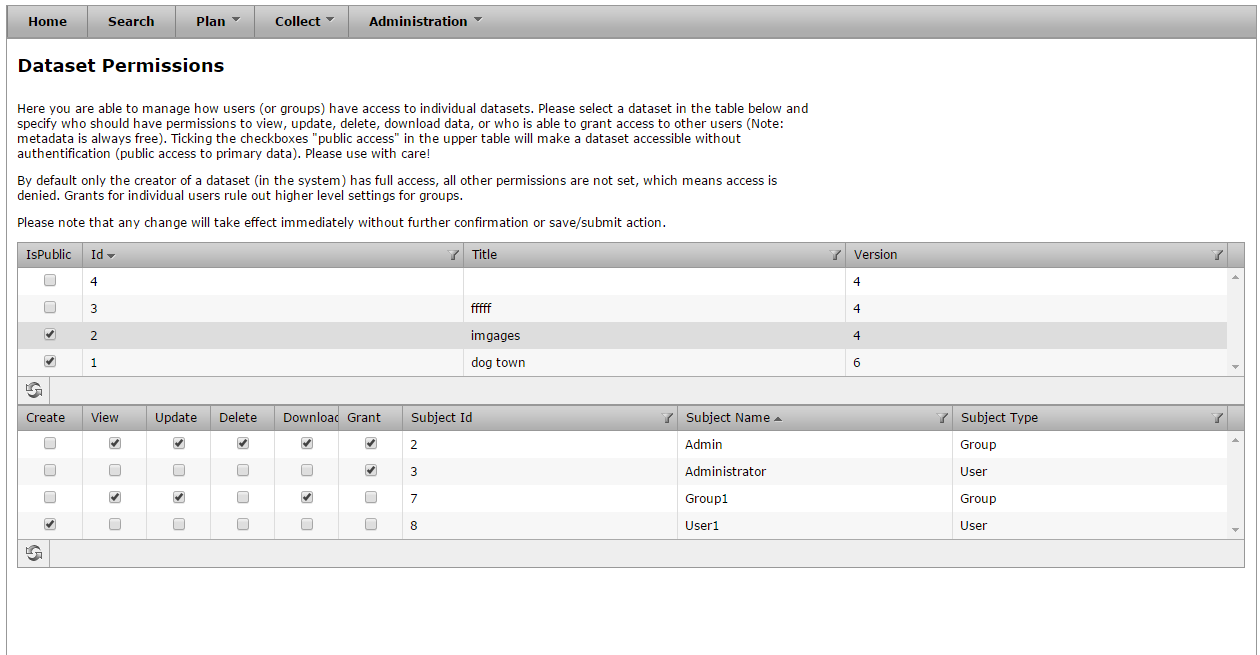
By clicking a feature name (a node in the tree), the system will show a table on the right side (see below). This table contains all subjects (users and groups) and their feature permission status. You may grant or deny permissions for individual users or groups using the radio buttons. If a permission is not explicitly set (i.e None) permissions are inherited from up level features. Inherited permissions are shown in the first column as effective permissions.



## 5.2. Datasets

The security system of BExIS is working on both, functional (features) and non-functional (dataset) items. Please go to **Administration > Authorization > Datasets** if you like to manage access to datasets.

By selecting a dataset (i.e. a row in the table), the system will show a second table underneath the first one, which contains all subjects (users and groups) and their different data permission statuses regarding the selected dataset. On this page, you are also able to alter the different kinds of data permissions for a selected dataset.



In general, the system works on six different data permission types:

* **Create:** allow/deny creating a dataset
* **View**: allow/deny view access to primary data
* **Update**: allow/deny manipulation (upload and update) of primary data
* **Delete**: allow/deny deletion of the whole dataset
* **Download**: allow/deny downloading primary data
* **Grant**: allow/deny to give permission to other users or groups

Selecting the checkbox in the first column (i.e. IsPublic) will allow public access to that dataset without any authentication.