




ix PERMISSIONS



UNITED PLANET INTREXX XTREME
RELEASE 4.5







Contents

- 1. Introduction 4**
- 2. Administration Login 6**
- 3. Portal Access Permissions 7**
- 4. User Manager 8**
 - 4.1. Global Permissions 8
 - 4.2. Individual Permissions 9
- 5. Application Permissions..... 10**
 - 5.1. Application Permissions 10
 - 5.2. Page Permissions 12
 - 5.3. Data Group Access Permissions 12
- 6. Menu Designer..... 13**
- 7. FileWalker 13**
 - 7.1. FileWalker Connection..... 13
 - 7.2. FileWalker View Element 14





Writing Conventions

In this handbook, text passages will be displayed in *italics* when they refer to settings in the displayed dialogs. Menu items that are available in context menus can, in addition, always be selected from the main menu. Main menu items will not be described if they are not available in the context menu. A description of the general main menu items can be found in the  *Center* handbook. Programming code in the text will be displayed in the Courier font. Context menus can be opened by clicking with the right mouse button on the described element.

In the following, *<xtreme>* refers to your Intrex installation path; under Windows, for example, this is usually  *C:\xtreme*. On Linux, the normal install path is  */opt/xtreme/*. The following symbols will be used for designation of special kinds of information:

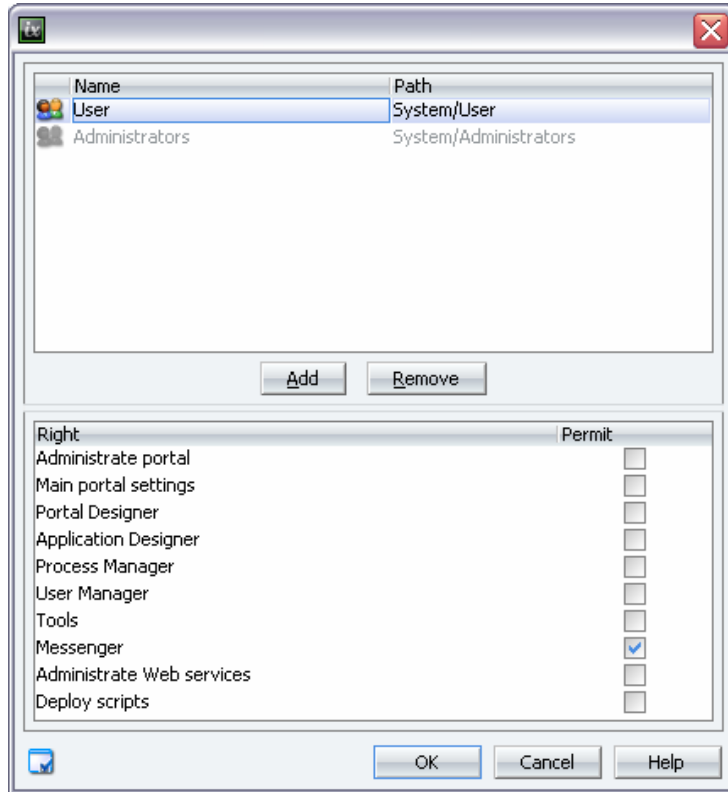
-  Important information
-  Tips and background information
-  References to additional information in an Intrex Xtreme handbook
-  Directories
-  URLs
-  Buttons in dialogs or assistants

Previous Knowledge


In order to understand this document, no special previous knowledge is required. You can find helpful information in the Intrex Xtreme handbooks  *Center*,  *Process Manager*,  *User Manager* and  *Application Designer*.

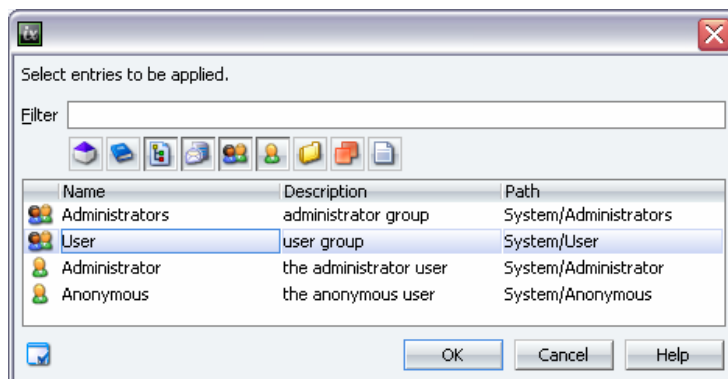
1. Introduction

In Intrex Xtreme, superior access permissions will be controlled from the *Extras* menu and special permissions will be controlled by individual modules. In the settings dialog, holders of permissions will be defined and individual permissions will be assigned. The settings dialog for permissions can be found on a tab in the properties dialog of an application, in the properties of menu items in the Menu Designer, in the User Manager, and under portal permissions.



Current permissions holders will be shown in the upper area of the dialog. In the *Name* column, the full name of the permissions holder will be given. In the *Path* column, position of the permissions holder in the object hierarchy of the User Manager will be shown.










Clicking  *Add* will open a dialog that allows a permissions holder to be selected.




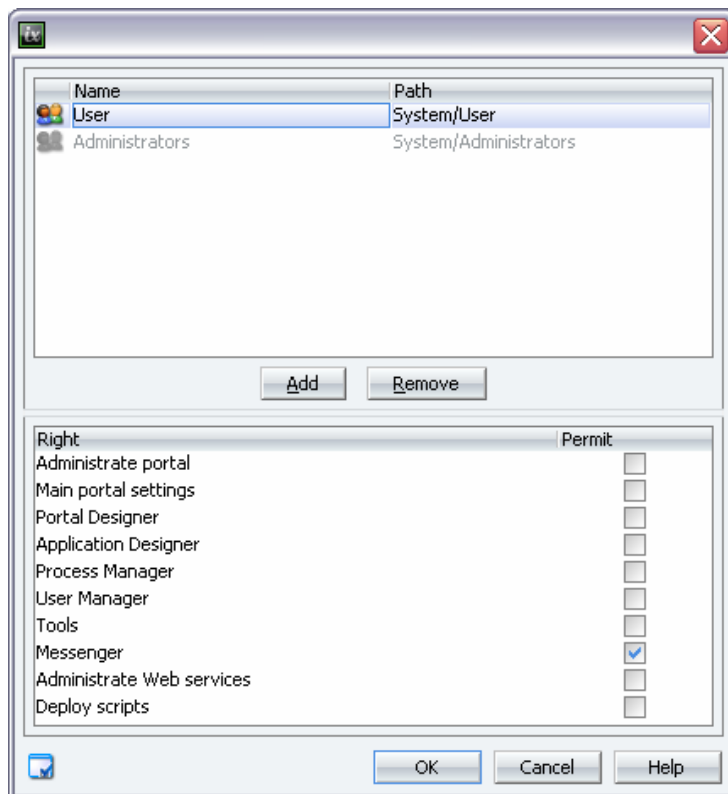
If you want to select multiple permissions holders, click on the individual permissions holders while holding down the *Ctrl-key*. With an entry in the *Filter* field, the list of permissions holders can be restricted.


The selection functions lexicographically, meaning that upon entering the letter *A*, only the permissions holders will be listed whose names begin with *A*. Additional character entries will further restrict the list.

With buttons, the list can be restricted to the various object classes of the User Manager:

-  Organizations
-  Organizational units
-  Roles
-  Distribution lists
-  User groups
-  Users
-  Containers
-  Sets
-  All other allowed types

Select the desired new possessor of permissions in the list and then click  *OK*.



With  *Remove*, the selected permissions holder can be removed from the list. This does not mean that all permissions will automatically be taken away from this permissions holder. The user may still possess access permissions in this area via membership in an organizational unit or user group.


If you select a permissions holder, the holder's individual access permissions will be shown in the lower area of the dialog. A permission can be issued by clicking its corresponding checkbox.

Click  *OK* to apply the new settings.

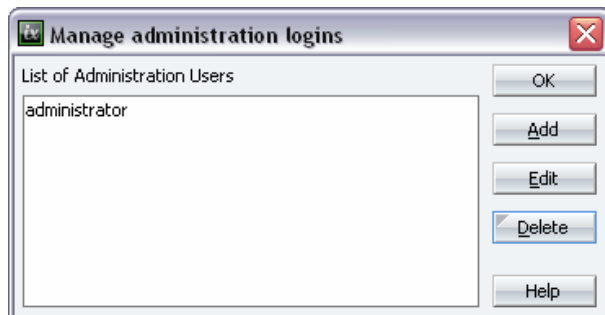
2. Administration Login




With an administration login, central, super-ordinate access permissions will be granted. These permissions apply to all portals. A user with this permission may:

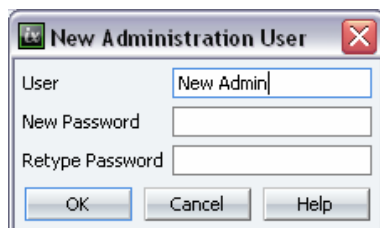
- Create portals
- Delete portals
- Import portals
- Change licensing details
- Manage administrator logins
- Use the tool *Systemcare*

 In the default install of Intrex Xtreme, in order to facilitate a quick setup of basic settings, the *administrator* user will be created without a password. As long as no password has been entered here, no login information will be requested when creating and deleting portals, when accessing the License Manager, and when managing administrator logins. Enter a password for the *administrator* user in order to eliminate access without a password.


Administration logins will be set up in the menu *Extras / Administration Logins*.

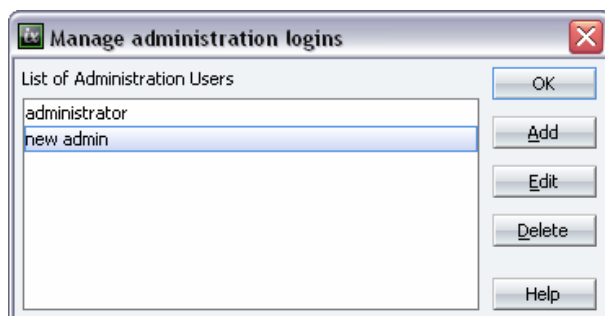



By clicking  *Add*, an unlimited number of additional administrators can be added with corresponding password information. Click  *Edit* to change an existing account.  *Delete* will delete a highlighted administration login from the list.

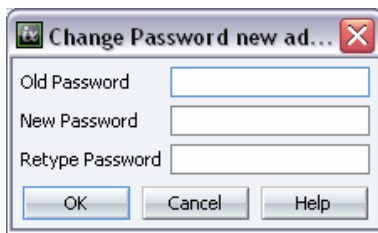


Enter a user name of your choice here. The user name for an administration login is unrelated to the user names of other administrators (such as in the User Manager). The names can be entered however you wish.

Enter a password and then repeat it in the following field. By clicking  *OK*, the new permissions holder will be created.

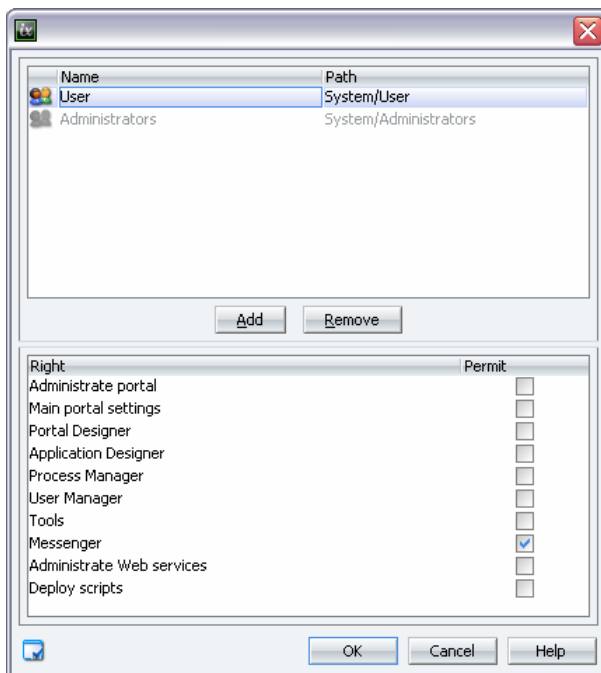


Select a permissions holder from the list and click  *Edit*.




In the following dialog, the password can be changed if needed.

3. Portal Access Permissions




Portal permissions will be controlled from the *Extras / Portal Access Permissions* menu. This menu item is only available after logging into a portal. All permissions set here are valid for the current portal.

Administrate Portal

This permission allows the portal properties to be configured. Additional information on this topic can be found in the handbook  *Center*.

Main Portal Settings

Permissions holders are allowed to administrate the main portal page. Information on this topic can be found in the handbook  *Portal and Portlets*.

Portal Designer

Application Designer


Process Manager

User Manager

Tools

Permissions holders have access to the corresponding module in the Portal Manager.

Messenger

Permissions holders are allowed to compose and send messages with the Messenger to users who have logged on to the portal (see handbook  *Portal and Portlets*).

Web Services

With this permission, WSDL registrations can be accomplished in the Integration Center.

Publish Scripts

With this permission, Groovy script can be published on the server.

4. User Manager

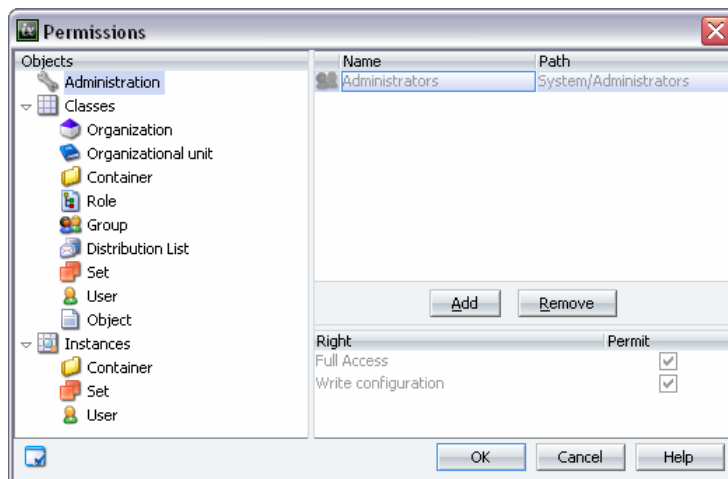
In the *User Manager* module, permissions are managed on two different levels: the global rights to administrate the object classes and object instances and the individual right to administrate the properties of the several object instances.

With global rights you can e.g. grant permissions to access the scheme manager, to add, edit and delete classes or attributes or to change the tree structure of the organization.

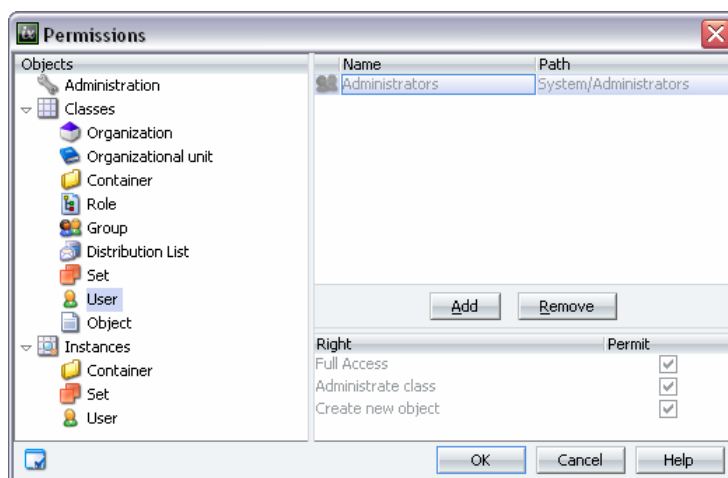
With the individual right to edit the properties of single object instances you'll permit to edit values, that are also stored physically on the database, e.g. the name of the instance, or address and contact data of an user object instance.

4.1. Global Permissions

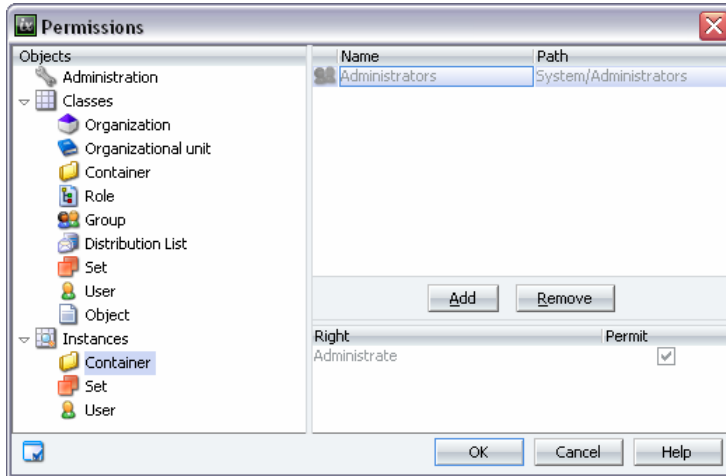
You will find the global settings for permissions to classes and objects in the menu item *User / Permissions*.



If an object in the User Manager has the *Full Access* permission to the *Administration*, it is able to create new object classes and administer them. The permission to *Write Configuration* allows only existing object classes to be edited. If one of these permissions is missing the scheme manager will not be available.



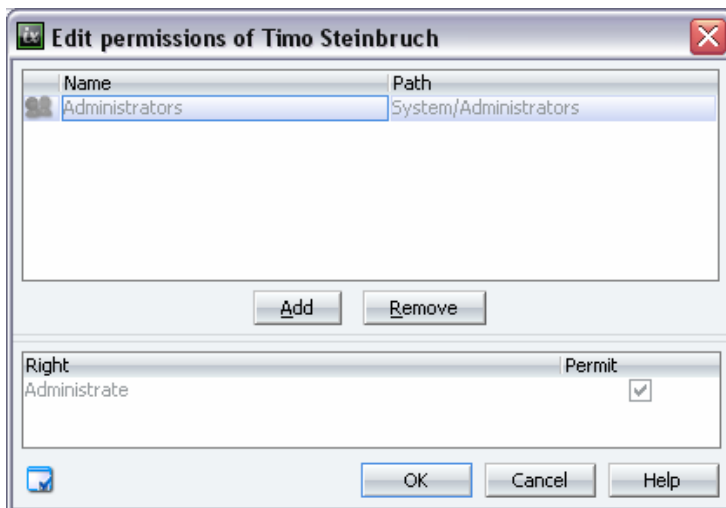
For the individual object classes, the permissions status will differ depending on whether it is allowed to administer classes or create new objects based on this class. *Full Access* activates both permissions.



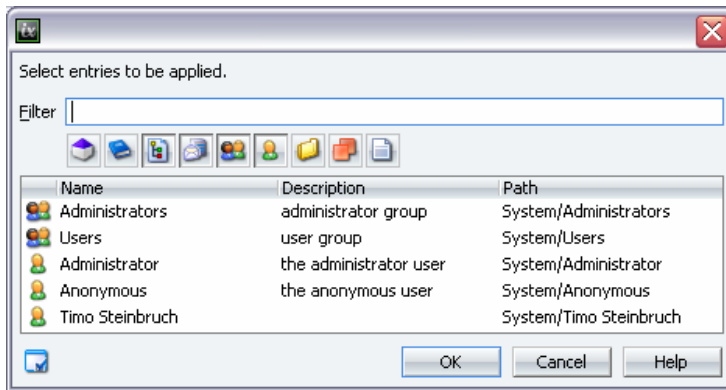
For *Object Instances*, only the *Administrate* permission can be set up for the three basic classes *Container*, *Set*, and *User*. With the permission *Administrate* all classes derived of the basic class and the instances of sub classes can be edited.

- ⓘ Please note that individual permissions in the object tree will be overwritten by global permissions.

4.2. Individual Permissions



This context menu item opens a dialog in which editing permissions to individual objects can be controlled. The administration permission only exists if the checkbox in the *Allow* column is activated. ➡ *Add* allows an object to be inserted into the list of objects with a specific permission.

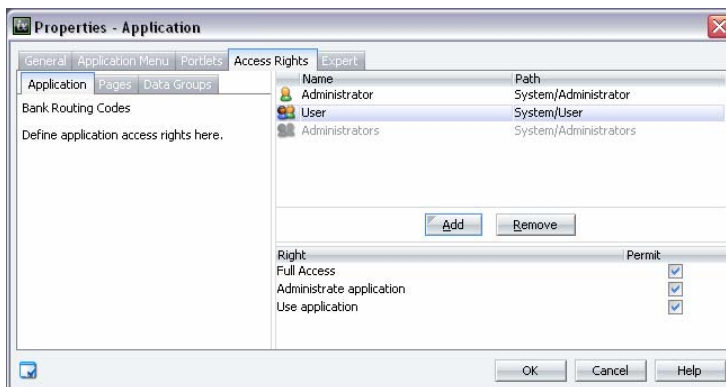


Select the object that should receive administration permissions here.

5. Application Permissions

In the Application Designer, access permissions to applications in the browser will be defined. In addition the administrative permission, which allows the application to be edited in the Application Designer, can be assigned here. In order to configure these permissions, the application must be opened in the Application Designer.

In the menu *Application / Access Permissions*, or in the properties dialog of the application, these permissions can be defined. In the properties dialog, switch to the *Access Permissions* tab.



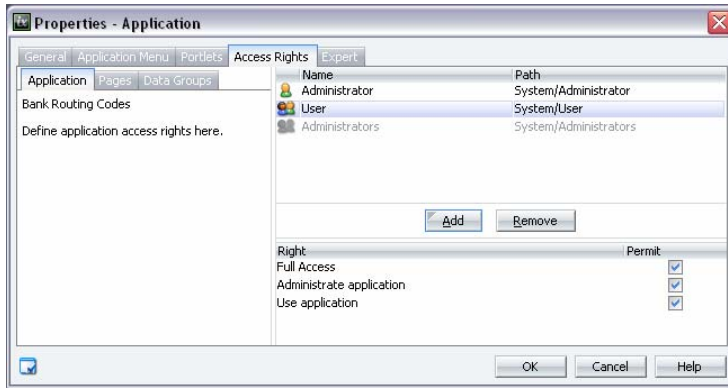
In the left area of the dialog you will see three tabs, which represent three levels at which permissions to access an application can be controlled:

- **Application** Access to the start page in the browser, administration permissions
- **Pages** Access to additional individual pages
- **Data Groups** Read and write access to application data

5.1. Application Permissions

The *Administrators* user group has full access to all pages and data groups of the application, as well as the application itself. This setting cannot be changed within the application permissions.

Remove a permissions possessor from the *Administrators* user group if you do not wish them to have the permission to administrate applications. The creator of an application has always the permission to administrate the application. This permission will be automatically given to the creator of an application.



Full Access

The *Full Access* setting automatically marks all additional permissions.

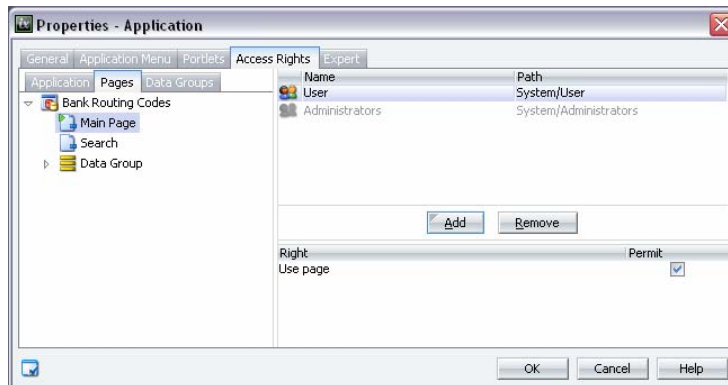
Administrate Application

Permissions holders are allowed to administrate the application in the Application Designer.

Use Application

Permissions holders have access to the application link and the starting page of the application.

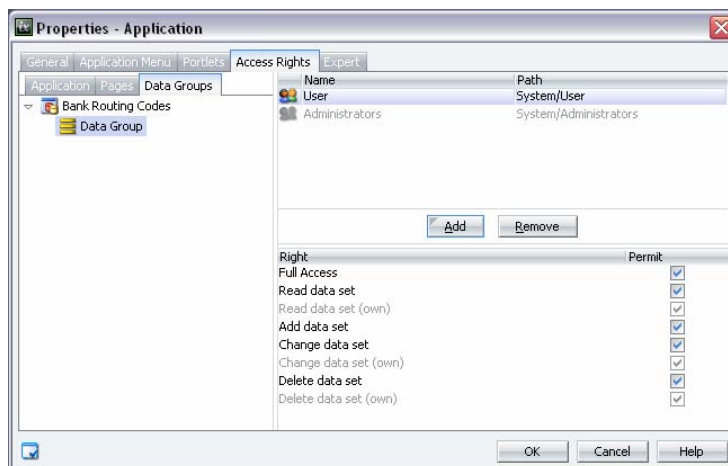
5.2. Page Permissions



With the *Use page* permission, you can control access to individual pages of the application. All pages that are not allowed will be automatically hidden from the application menu. Buttons that lead to a page that cannot be shown in this way will not be shown in the browser.

5.3. Data Group Access Permissions

Here you will define in which data group data can be read, added to, modified or deleted.



Full Access

The *Full access* setting automatically marks all additional permissions.

Read Data Set

Permissions holders may read the data of an application.

Read Data Set (own)

Permissions holders may read existing data records they have created.

Add Data Set

Permissions holders may add new data.

Change Data Set

Permissions holders may modify existing data records.

Change Data Set (own)

Permissions holders may modify existing data records they have created.

Delete Data Set

Permissions holders may delete existing data records.

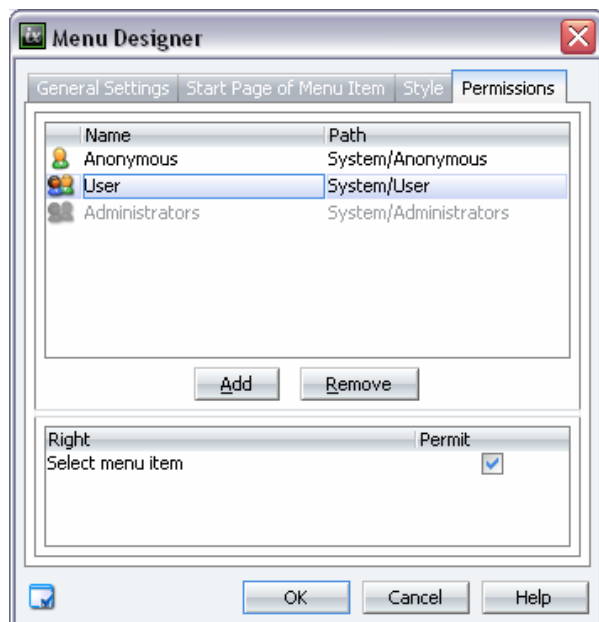
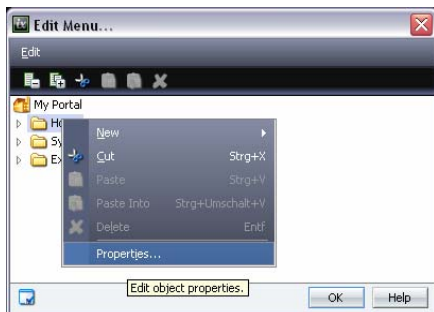
Delete Data Set (own)


Permissions holders may delete existing data records they have created.

Upon saving the application on the server, the new settings will be applied.

6. Menu Designer

The Menu Designer can be reached via the menu *Extras / Edit menu*. In the Menu Designer, the menu structure of the portal will be administrated (see handbook *Portal Designer*). Permissions can be assigned for each individual menu item. Menu items that a user may not select will be hidden in the browser. Select a menu item for which you wish to change access permissions in the Menu Designer. You can reach the settings dialog in the *Properties* context menu item or in the menu item *Edit / Properties*.



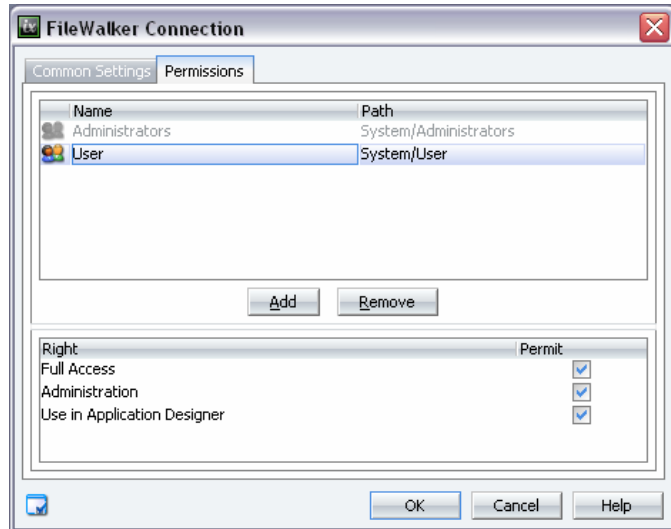
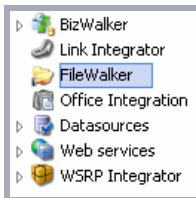
You can find additional information on the Menu Designer in the handbook  *Portal Designer*.

7. FileWalker

For access to files in the network, permissions will be controlled in two places: in the properties of the *Connection* and in the properties of the *FileWalker* view element.

7.1. FileWalker Connection

The permissions to the FileWalker connection will be assigned in the *Integration Center* module in the properties of a connection.



Full Access


The *Full access* setting automatically marks all additional permissions.

Administration

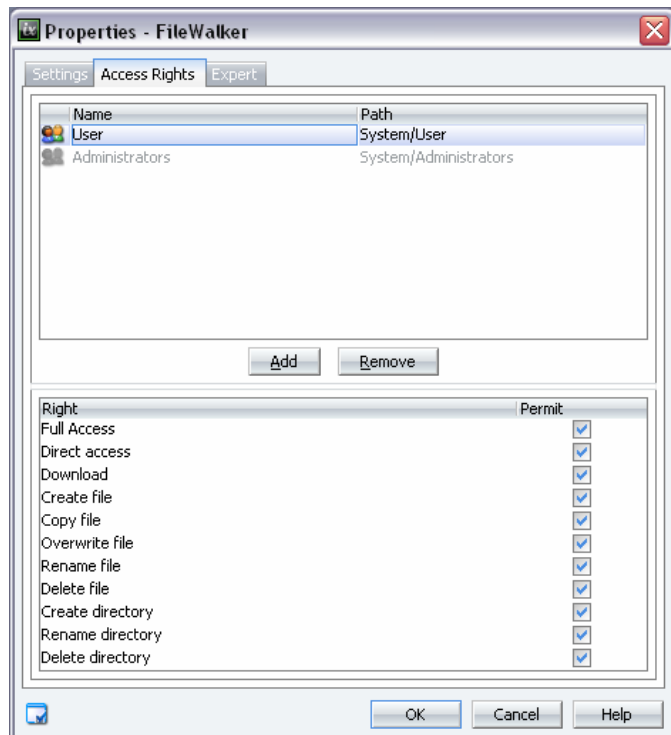
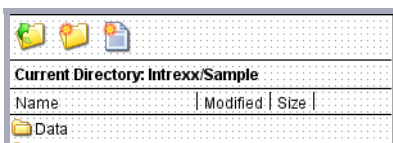
With this permission, the settings of the FileWalker connection can be administrated.

Use in Application Designer

Permissions holders are allowed to select the connection in the Application Designer and assign a FileWalker element to it.

 Please note that FileWalker connections cannot take into account directory permissions of the individual users.

7.2. FileWalker View Element



In the *Access Permissions* tab in the properties dialog, the following permissions will be assigned:

Full Access

The *Full access* setting automatically marks all additional permissions.

Direct Access

The permissions holder has direct access to all files. Changes will be applied to the original files.

Download

Permissions holders can download files.

Create File

The permissions holder is allowed to create new files in the network directory.

Copy File

The permissions holder can create copies of a file on the network.

Overwrite File

The permissions holder is allowed to overwrite files on the network.

Rename File

File names can be changed.

Delete File

Files can be deleted.

Create Directory

Additional network directories can be created.


Rename Directory

Directory names can be changed.

Delete Directory

Directories can be deleted.

Users of FileWalker require additional permissions to the application and to the page on which the FileWalker element is integrated.

You can find additional information in the *Integration Center* handbook and the  *Application Designer* handbook.