

Editing Security Groups

Once a security group has been created, you can edit further settings. To change settings for a security group at a later time, use the function **User Data - Security Groups** and click on **Edit** in the table row of the security group you wish to edit.

Master Data

On this tab you can change the name and the order number of the security group.

The freely definable order numbers enable security groups to be sorted for use by other accounts in the system. The following rights when creating (C), Reading (R), Editing (U - Update) or deleting (D) a security group come into play:

URL	Rights
portal.UserData.Create.SameRole.HigherOrdinal	Users are allowed to create (C), read (R), update (U) or delete (D) user accounts when these are associated with a security group whose ordinal number is higher than the ordinal number of the users own security group.
portal.UserData.Create.SameRole.LowerOrdinal	Users are allowed to create (C), read (R), update (U) or delete (D) user accounts when these are associated with a security group whose ordinal number is lower than the ordinal number of the users own security group.
portal.UserData.Create.SameRole.SameOrdinal	Users are allowed to create (C), read (R), update (U) or delete (D) user accounts when these are associated with a security group whose ordinal number is equal to the ordinal number of the users own security group.
portal.UserData.Create.SameSecurityGroup	Users are allowed to create (C), read (R), update (U) or delete (D) user accounts when these are associated with the same security group as the user.

Example: A security group with an ordinal number 50 has all rights for the URIs *UserData.Create.SameRole.LowerOrdinal* and *portal.UserData.Create.SameRole.SameOrdinal*. A user of this security group cannot create users in security groups who have a higher ordinal number (over 50). These ordinal settings can be used to prevent users from creating other users who have more rights in the system than they themselves have.

The values and system you use to assign the ordinal values is up to you. You can decide whether higher or lower ordinal numbers should have more or less rights.

Role Name

The text shown in the tab depends on the role which is associated with the security group (User, Client).

You will see a table of resources (described using their URN - uniform resource name), representing functions which can be assigned to the security group. The table shows which rights are assigned for the corresponding resource ("yes" in the corresponding cell).

- Create (C)
- Read (R)
- Update (U)
- Delete (D)
- Execute (X)

Usually, X means that an action or option is executable or visible. Other meanings are documented in the description field of the resource. The column **Menu Item** shows whether the resource relates to a menu item. If "yes" is displayed for Execute (X), the user can see and use the corresponding menu item in the main menu.

The column **Action** contains links to switch on or off the corresponding rights. Greyed out options, mean that the right for this URI cannot be changed. Use **0** to switch off all rights to use the resource, **1** to switch them all on.

Not all actions (CRUDX) are available for all functions.

Example:

URI ^a	Rechte hier zugewiesen	Beschreibung	Menüpunkt	Erstellen (C)	Lesen (R)	Aktualisieren (U)	Löschen (D)	Ausführen (X)	Aktion
portal.Acd		ACD	ja					ja	C R U D X O I
portal.Acd.AcdAgent.DiallerContacts.Address		AcAgent Dialler - Spalte "Adresse" ist sichtbar (X)						ja	C R U D X O I
portal.Acd.AcdAgent.DiallerContacts.City	ja	AcAgent Dialler - Spalte "Stadt" ist sichtbar (X)						ja	C R U D X O I H X

The question you need to answer when configuring access to resources is: Is it sensible or desirable for a member of this security group to have access to create, read, update or delete a particular resource.

These settings then control what functions are available in the web application after the user logs in.

In most cases, you can leave the predefined rights as is.

Workflow Application Types

Here you can (assuming your security group allows) assign workflow applications to the security group. Users of the security group can then create applications of this type.

Workflow Objects

Here you can (assuming your security group allows) assign workflow objects from workflow applications to the security group. Users of the security group can then create applications of this type.

Cockpit Types

Here you can see (assuming your security group allows) what cockpit types are associated with the security group.

Reports

Here you can see (assuming your security group allows) what reports are associated with the security group. Use **New** in the toolbar to add further reports. This allows all members of the security group to have access to certain statistics. You can still assign further reports to individual users.

You can also remove reports from the security group by clicking **Delete**.