ORTEC Workforce Scheduling 7

Implementation Manual

Access Control

March 2025

PUBLIC

ORTEC

Published: March 21, 2025

Version: 2025.1637531

Table of Contents

1 Access Control

The secured **Access Control** web application is used for user authentication, permissions and accountability in **ORTEC Workforce Scheduling (ORTEC WS)**.

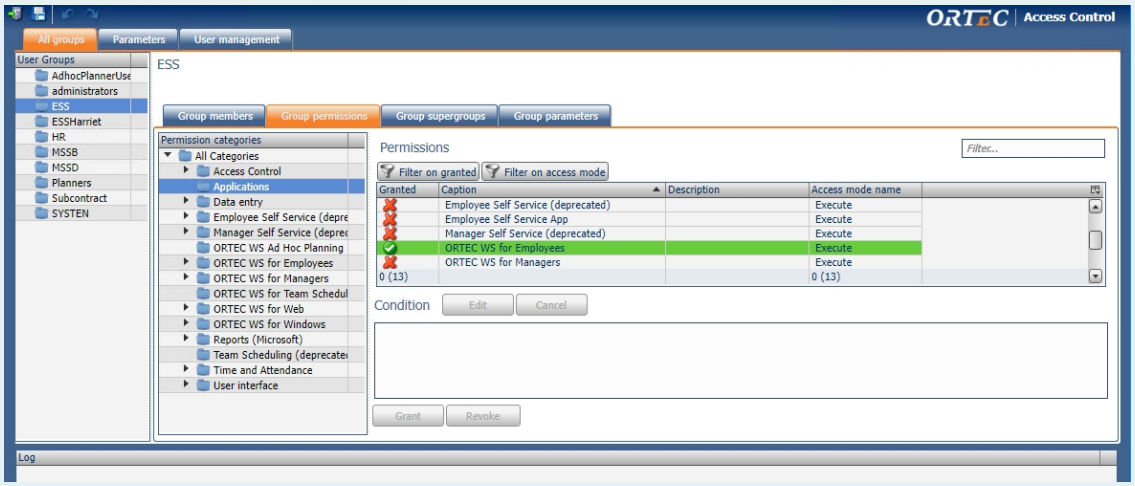
- **Authentication**: to confirm the identity of a user.
- **Permissions**: to specify whether a user (group) has access to specific parts of the system.

> - Not all permissions might be applicable to your system. This depends on the system configuration for your organization and the permissions granted to you.
> - It's also possible to grant permissions for the **Access Control** application itself.

- **Accountability**: to keep track of what parts of the system has been accessed by which user. This information can be used for auditing purposes.

Example

Access Control application.



2 Getting started

The **ORTEC WS Access Control** web application is available through your organization's intranet. You need the web address, a user name and a password before you can start using the application.

Alternatively, open **Access Control** within the **OWS Client**. For more information, see "SSO Access Control" on page 2.

2.1 Log in

1. Browse to the **Access Control** web address.
2. Select a **Language**.
3. Enter your **User name**.
4. Enter your **Password**.
5. Press Enter or click **Log in**.

2.2 Change password

> The Application manager can require users to change their password on their first login by selecting that option when issuing a password. In that situation the **Change password** page will be displayed after logging in for the first time

You can also change your password at any time as follows:

1. Select the checkbox **Change password** when logging in to the application.
2. Enter your **Current password**.
3. Enter a **New password**.
4. Enter the new password again in the **Confirm new password** box.
5. Click **Apply** to change your password and to finish logging in.

2.3 SSO Access Control

An ORTEC consultant or an Application manager can enable opening **Access Control** with single sign-on (SSO) within the **OWS Client**:

1. In the **OWS Client**, click with your right-mouse button on an empty space in the menu bar.
2. Select **Customize**.
3. In the **Commands** tab, select the **Maintenance** category.
4. Drag-and-drop the **Access Control** command to a menu. For example, the **Maintenance** menu.

3 User management

To simplify permission sharing and maintenance, it's advised to add individual users to user groups. If necessary, an individual user account can be disabled to restrict access.

Per user, specify the authentication method used to confirm each user's password validity.

3.1 Add user

1. Click the **User management** tab.
2. In the **Data management** section, click **Add user**.
3. On the **General** tab, enter values for the (required) fields.

   Required fields that are not filled are color marked , the tabs for which not all required fields are filled are flagged .

4. On the **User group** tab, add the user to one or more user groups.
   - Click the **New** button.
   - Find the correct user group(s).
   - Select user group(s). To select multiple user groups at once, hold down the Ctrl or Shift key.
   - Click **OK**.
5. Click **OK**.

3.2 Find user

1. Click the **User management** tab.
2. In the **Data management** section, click **Find user**.

   Or click **List users**. In the top-right corner, filter the user list.

3. In the **Find user** section, type the text (e.g. part of a user name) you want to search for.
4. Click **Search**.
   This performs a full text search in all columns shown in the results list, e.g. User name, Full name, Description.

   - To manage the columns shown, click - in the top-right column header - **Configure grid columns**.
   - To sort the results, click on a **column header**.
   - To group the results, press the **Shift key** + a **column header** to group the results in the grid based on the selected column.

3.3 Disable user account

A disabled user account has no access the system.

1. Click the **User management** tab.
2. Find the user account you want to disable.
3. Right-click the user account and click **Edit user**.
4. On the **General** tab, deselect the checkbox **Account enabled**.
5. Click **OK**.

3.4 Download credential file for user

Credential files can be used by an **ORTEC WS** application to identify itself to another **ORTEC WS** application.

1. Click the **User management** tab.
2. Find the user you want to download the credential file for.
3. Right-click the user account and click **Download credentials file**.
4. In the **Download credentials file** window, enter the **password** of the user, then click **OK**.
5. In the **File download** window, click **Save** and enter a **location** where the file should be saved.
6. Click **Save**, then click **Close**.

3.5 Set password restrictions for Comtec authentication method

1. On the **application server**, start **System Configuration**.
2. Enter your **Username**.
3. Enter your **Password**.
4. Press Enter or click **OK**.
5. On the **Configuration** tab, in the section **Settings Management** click **Settings Manager**.
6. In the **CUASFW** category, select **ComtecAuthentication**.
    - The minimum password length of a password can be specified with the setting MinimumPasswordLength (default 8).
    - When a user should change his password in case his current password is shorter than the minimum password length the setting EnforcePasswordRequirementsDuringLogin (default: True) can be checked.

4 User group management

Users that share the same permissions are organized in user groups. Permissions are granted to user groups and not to individual users. For more information on permissions, see "Permissions" on page 9.

4.1 User group hierarchy

A user group can inherit permissions from other user groups , enabling you to form a user group hierarchy. For example, a department can be assigned to a user group to indicate that the granted or inherited permissions in this user group only apply to the selected department and its sub-departments.

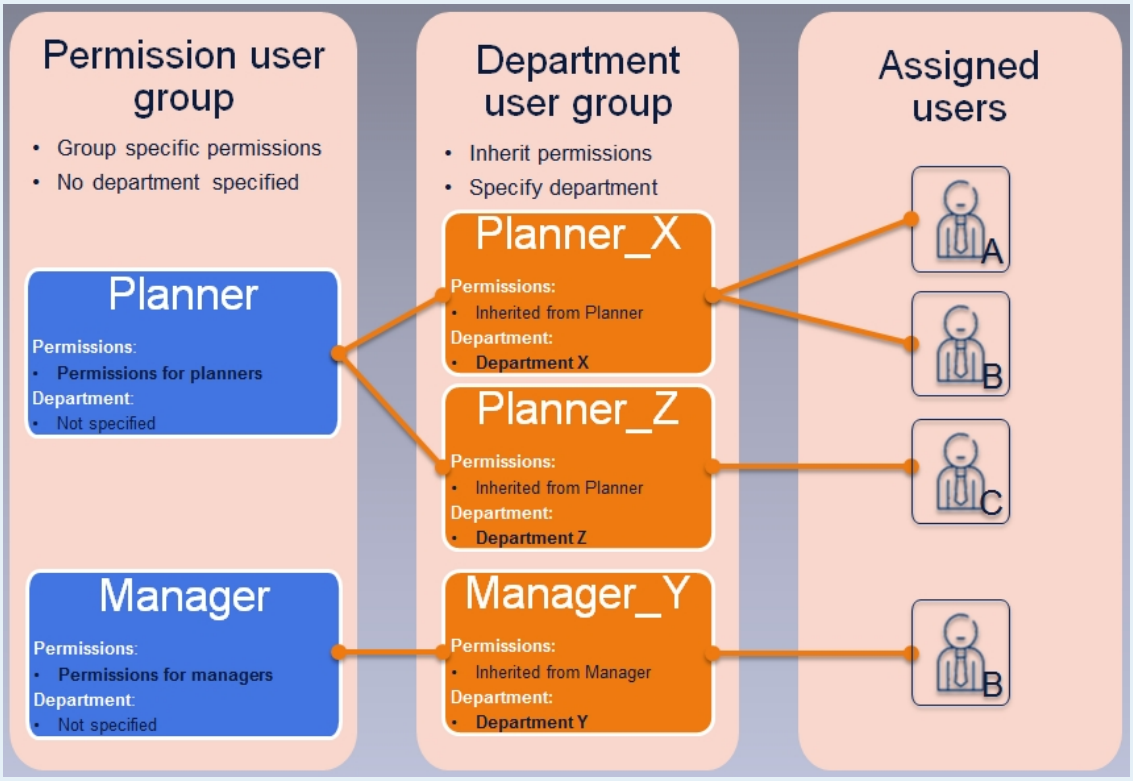
> Permissions inherited from another user group can **not** be revoked. Only additional permissions can be granted.

To prevent from having to assign permissions to all groups, it's advised to add a user group that is solely used for granting permissions, we call this a **Permission user group**. Then create user groups that inherit permissions from this permission group and specify the departments for which they apply to. We call this a **Department user group**. With this configuration it's easier to grant or revoke permissions.

After the user groups are configured, users are added to one or more user groups to receive the configured permissions in **ORTEC WS** applications.

Example

Users A and B are planners for department X, user B is also manager of department Y and user C is planner for department Z. This can be configured best by using the following configuration:



4.2 Create new user group

To grant permissions to a specific group of users (such as Planners, Managers, etc.), create a new user group.

1. Click the **All Groups** tab.
2. In the **User Groups** section in the left pane, right-click and select **New user group**.
3. Enter the name of the new user group.
4. Click **OK**.

4.3 Specify department for a user group

Specify a department for a user group to grant permissions only to those departments.

1. Click the **All Groups** tab.
2. In the **User Groups** section, select the user group.
3. Click the **Group parameters** tab.
4. Right-click the 'department' parameter and select **Set value**.

When no 'department' parameter is available, first create one via the **Parameters** tab.

5. Enter the **Name** of the department you want to search for and click **Search**.

   This action performs a full text search in the names of all departments.

6. In the **Results** section, select a department and click **OK**.

   If a non-leaf department is selected, all permissions specified for the user group are granted to all sub departments.

4.4 Add user(s) to a user group

1. Click the **All Groups** tab.
2. In the **User Groups** section, select the user group.
3. Click the **Group members** tab.
4. Click the **Add user** button.
5. (Optional) In the **Input parameters** section, enter (a part of) the user name
6. Click **Search**. Only users that aren't assigned to the selected user group are listed.
7. Select one or multiple users (using the Ctrl key) to be assigned to the selected user group.
8. Click **OK**.

   It's also possible to maintain user group assignments from the data entry window of the user data element that's accessible on the **User management** tab.

4.5 Remove user(s) from a user group

1. Click the **All Groups** tab.
2. In the **User Groups** section, select the user group.
3. Click the **Group members** tab. The users assigned to the selected user group, are listed.
4. Select one or multiple users (using the Ctrl key) to be removed from the user group.
5. Click the **Remove** button.

   It's also possible to maintain user group assignments from the data entry window of the user data element that's accessible on the **User management** tab.

4.6 Rename a user group

1. Click the **All Groups** tab.
2. In the **User Groups** section, right-click the user group and select **Rename group**.
3. Enter the new name of the new user group.
4. Click **OK**.

4.7 Delete a user group

Delete a user group only if it has no users assigned to it.

1. Click the **All Groups** tab.
2. In the **User Groups** section, right-click the user group and select **Delete group**.
3. Click **OK**.

4.8 Backup user group permissions

Backup the permissions granted to a user group. This backup can be used to restore permissions on other environments or as a template for a new user group in the current environment.

1. Click the **All Groups** tab.
2. In the **User Groups** section, right-click the user group and select **Export group to XML**.
3. In the file download window, click **Save** and enter a location where the file should be saved.
4. Click **Save**, then click **Close**.

> The backup file for a user group contains the permissions that are directly granted to the user group (not the inherited permissions) and the user groups he inherits from.

4.9 Restore user group permissions backup

A backup of a user group can be imported to restore the definition of granted permissions and user groups it inherits from in the file.

1. Click the **All Groups** tab.
2. In the **User Groups** section, right-click and select **Import group**.
3. In the Import groups window, click **Upload** and select the user group file to be imported.
4. To revoke permissions currently granted to the user group, select the checkbox **Remove not imported permissions**.
5. Click **OK**, then click **Close**.

> The user group name and user group inheritance defined in the backup file defines to which user group the permissions will be imported and from which user groups it inherits from. In case the user group name already exists, this user group will be adjusted with the imported data. Otherwise a new user group will be created.
> The file can be edited in editors like Notepad or any other XML editor to obtain the file that can be imported into another environment or as a template for a new user group.

```
<?xml version="1.0" encoding="utf-8" ?>
- <userGroups>
  - <userGroup name="Test_User_group_2">
    - <parentUserGroups>
        <parentUserGroup name="Test_User_group" />
      </parentUserGroups>
    - <userGroupPermissions>
        <userGroupPermission acObjectCode="gui.application.cwgs.CUASMANAGEMENTCONFIG" accessMode="Execute" condition="" />
      </userGroupPermissions>
    </userGroup>
  </userGroups>
```

5 Permissions

Permissions are granted to user groups and not to individual users. Users that share the same permissions are organized in user groups.

> For more information on user groups, see "User group management" on page 5. There, you can also find more information on:
>
> - Inherited permissions and how best to work with them in a user group hierarchy.
> - Backing up & restoring user group permissions.

Permissions are grouped in categories. Most of the categories correspond with how the menu actions in the client application are categorized.

> - It's possible that a permission is used in multiple applications and shown in multiple categories.
> - Some permissions are available for future purposes and aren't being used in the applications yet.
> - Some categories are deprecated. These are **Employee Self Service**, **Manager Self Service**, **ORTEC WS for Windows** and **Team Scheduling**.

Access modes

Each permission is about a certain object and about how to access it. Objects can be applications (such as the client application, the system configuration or access control application), menu actions or data entities.

For starting applications and using menu actions, there's the access mode **Execute**. For data entities, there are the following access modes:

- **Create**
  This mode allows the user to create a data entity.
- **Read**
  This mode allows the user to view the details of a data entity.
- **Update**
  This mode allows the user to update the details of a data entity.
- **Delete**
  This mode allows the user to delete a data entity.
- **List**
  This mode allows the user to retrieve a list overview of the data entities.

5.1 Grant permissions

1. Click the **All Groups** tab.
2. In the **User Groups** section, select the user group.
3. Click the **Group permissions** tab.
4. In the **Permissions** section, select the permission(s) to be granted.
5. Click **Grant** to grant the permission to the selected user group.

The background color indicates whether a permission is granted:

- Green for granted permissions.
- Lighter green for permissions that are inherited.
- No background color for permissions that are neither granted nor inherited.

5.2 Revoke permissions

1. Click the **All Groups** tab.
2. In the **User Groups** section, select the user group.
3. Click the **Group permissions** tab.
4. In the **Permissions** section, select the permission(s) to be revoked.
5. Click **Revoke** to revoke the permission from the selected user group.

5.3 Filter on granted

To only show permissions that are granted, inherited or neither granted nor inherited, use the **Filter on granted** feature.

1. Click the **All Groups** tab.
2. In the **User Groups** section, select the user group.
3. Click the **Group permissions** tab.
4. Click the button **Filter on granted** and select the options to filter:
   - **(Select all)**
     Shows all permissions.
   - **Granted**
     Shows the permissions that are directly granted to the selected user group.
   - **Inherited**
     Shows the permissions that are inherited from other user groups.
   - **Neither granted nor inherited**
     Shows the permissions that are neither directly granted to the selected user group nor inherited from other user groups.
5. Click **OK** to apply the filter to the permissions shown.

5.4 Filter on access mode

1. Click the **All Groups** tab.
2. In the **User Groups** section, select the user group.
3. Click the **Group permissions** tab.
4. Click the button **Filter on access mode** and select the access modes to filter.

The filter is applied real time to the shown permissions, there's no need to click OK to apply the filter.

5.5 Free text filter

1. Click the **All Groups** tab.
2. In the **User Groups** section, select the user group.
3. Click the **Group permissions** tab.
4. In the **Filter...** box at the top-right of the page, type a text to apply a free text filter.

> This action performs a full text search in all columns shown in the results list, e.g. User name, Full name, Description.

5.6 Access Control

The **Access Control** category contains permissions relevant for the **Access Control** application.

The following permissions are worth mentioning:

- The **Access Control \ Actions** category contains permissions for all actions that can be executed in the Access Control application.
- The **Access Control \ Authentication** category currently contains only the permission that allows the user to change the password of users other than yourself.

Permissions about user management in Access Control can be found in the **Data entry \ User** category.

5.7 Applications

The **Applications** category contains the login permissions for most of the applications of **ORTEC WS**. The following application permissions are available:

- :en-US:CSCS
- Access Control
- Adhoc Planner (departments)
- Dual Client
  The web application that is used in the **ORTEC WS WS for Windows** application to make web windows available in the application.
- Employee Self Service (deprecated)
- Employee Self Service App
- Manager Self Service (deprecated)
- ORTEC WS for Employees
- ORTEC WS for Managers
- ORTEC WS for Web
- Team Scheduler (departments)
- Team Scheduling (deprecated)
- Time and Attendance

5.8 Data entry

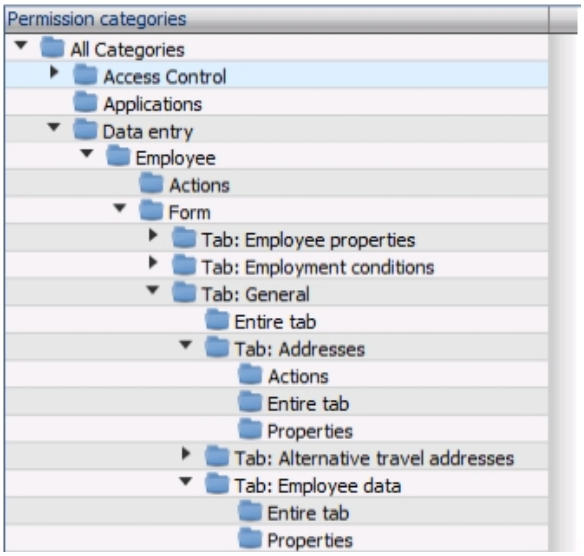
The **Data entry** category contains the permissions for data entities. When a default data entry window is used in an application the relevant permissions can be found in this category.

Action permissions

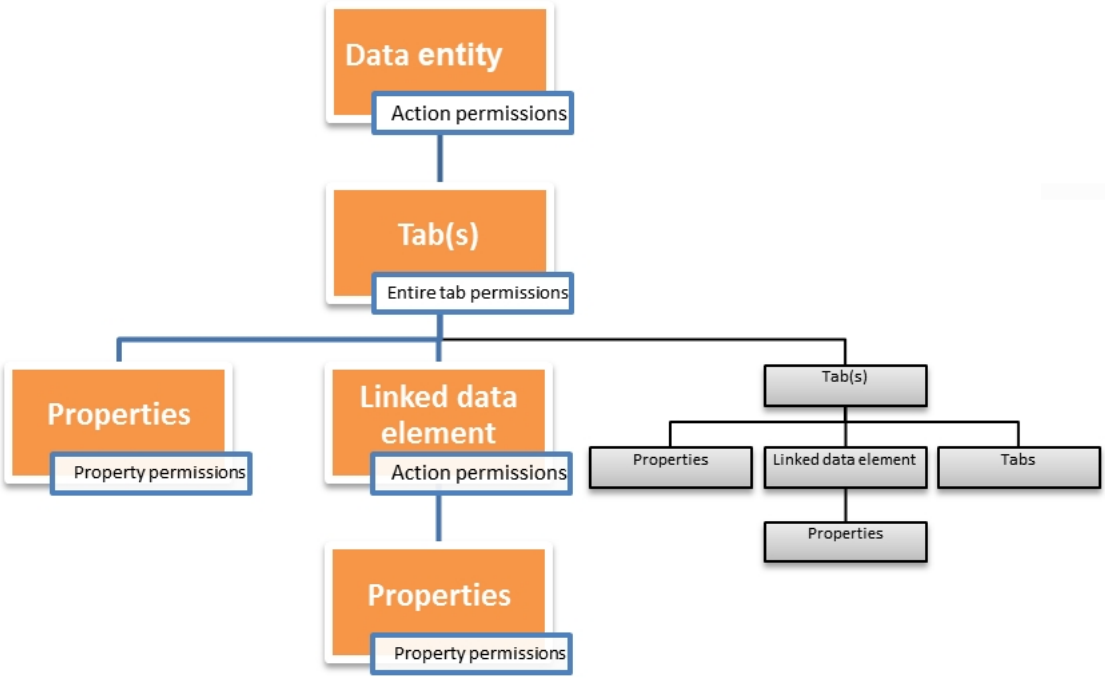
The action permissions can be found in the **Data entry \ <Data entity> \ Actions** categories. They are usually Create, Read, Update, Delete and List. For more information, see "Permissions" on page 9.

Form permissions

Form permissions are for the data entity window(s), like prohibiting to modify a certain property of the data entity or to view a whole tab. The form permissions can be found in the **Data entry \ <Data entity> \ Form** categories.



The following permission hierarchy applies:



Entire tab permissions

The following permissions can be granted to the tab:

- **Create**
  Currently this permission is not used in the applications. It will be removed in a later version.
- **Read**
  This permission specifies whether the tab is visible for the user.
- **Update**
  This permission allows the user to update the information shown in the components on the tab and any underlying tabs.

Properties permissions

The following permissions can be granted to the (linked) data entity properties shown on tab.

- **Create**
  This permission is required to enter a value for a property in case a new (linked) data entity is created by a create action.
- **Read**
  This permission is required to be able to view the value of a property.

  > The reading permissions for a property are not applied to the columns shown in the list overview of a (linked) data entity.

- **Update**
  This permission is required to be able to alter the value of a property.

5.9 ORTEC WS Ad Hoc Planning

The **ORTEC WS Ad Hoc Planning** category contains a permission relevant for the **ORTEC WS Ad Hoc Planning** application.

5.10 ORTEC WS for Employees

The **ORTEC WS for Employees** category contains the permissions relevant for the **ORTEC WS for Employees** application.

The categories found under the **ORTEC WS for Employees** category correspond with the different workspaces available in **ORTEC WS for Employees**.

5.11 ORTEC WS for Managers

The **ORTEC WS for Managers** category contains the permissions relevant for the **ORTEC WS for Managers** application.

The categories found under the **ORTEC WS for Managers** category correspond with the different workspaces available in **ORTEC WS for Managers**.

5.12 ORTEC WS for Team Schedulers

The **ORTEC WS for Team Schedulers** category contains permissions relevant for the **ORTEC WS for Team Schedulers** application.

5.13 ORTEC WS for Web

The **ORTEC WS for Web** category contains permissions relevant for the **ORTEC WS for Web** application.

5.14 Reports (Microsoft)

The **Reports (Microsoft)** category contains permissions for MS Reporting reports in case they are available in the different applications.

> Permissions are registered for reports which are uploaded in **ORTEC WS System Configuration**, through the post installation step 'Upload MS Reporting'.

5.15 Time and Attendance

The **Time and Attendance** category contains permissions relevant for the **Time and Attendance** module.

5.16 User interface

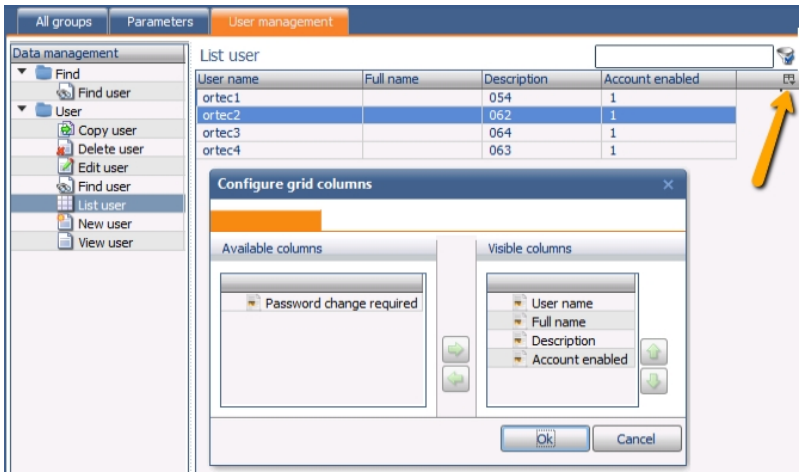
The **User interface** category contains general permissions for the user interfaces of the applications.

For the web based applications the following permissions are worth mentioning:

- **Save settings**
  With this permission the last used user interface settings are stored (when logging out) so they'll be used the next time the user logs in. Some examples of user interface settings that are stored are 'Filters', 'Last active tab', 'Last opened schedule', 'Resizing of grids', 'Manually configured columns in a grid', 'Size and position of pop-up windows (like MS Reporting window)'.

  > It's possible that an application is implemented in such a way that not all user interface settings are stored.

- **Configure grid columns**
  With this permission the user can configure which columns are visible in the list overviews.



6 Accountability

The **Access Control** application keeps track of what parts of the system have been accessed by which user. These logging records are not accessible from the application, only from the database tables. These tables can only be accessed by a user with direct access to the database and having basic SQL knowledge.

> The logging records are stored for 366 days.

The **acLoginSession** table contains information about the users who are currently accessing an application, the following information is available:

- **id_user**
  The id of the user who accessed the system.

  > Information about the user (for example the user name) can be found in the **[user]** database table.

- **created_datetime**
  The time stamp of when the user has logged in to an application.
- **application**
  The application the user is accessing.

The **acLoginSessionLog** table contains information about the users who have accessed an application, the following information is available:

- **userName**
  The user who accessed the system.
- **LogDatetime**
  The time stamp of the event that occurs when accessing an application.
- **eventType**
  The following types of events are logged
  - login: The user has logged in to the application
  - logout: The user has logged out from the application
  - invalidate: The user has been forced to log out from the application
  - expired:The user has not been active for a certain period (around 30 minutes)

    > This only holds for the web applications.

  - validationFailed: An application has discovered the log-in session of the user is not valid anymore.
- **eventData**
  Extra information related to the event, type of information depends on the event type.
- **application**
  The application the user accessed.

The **acFailedLoginLog** table contains information about the failed log-in attempts for an application.The following information is available:

- **userName**
  The user who accessed the system.

- **LogDatetime**

  The time stamp of the event that occurs when accessing an application.

- **eventType**

  The following types of failed log-in attempts are logged

  - UserDoesNotExist: The entered user name is not known in the application.
  - UserAccountDisabled: The **Enabled** checkbox is not set for the user data element.
  - IncorrectPassword: The entered password is incorrect.
  - AuthenticationProviderNotSupported: The used authentication provider is not supported anymore.
  - AccessDenied: The user does not have the permission to access the application.
  - PasswordChangeRequired: The user is forced to change his password.

    > This event can only occur for the Comtec authentication provider.

  - AnErrorHasOccured: Any other failures that occurs during the log-in attempt.

- **eventData**
  Extra information related to the event, type of information depends on the event type.
- **application**
  The application the user accessed.

Contact information

For further information contact ORTEC, either through your existing ORTEC representative or by using the appropriate contact details listed on www.ortec.com

Our website offers case studies, white papers, brochures, demos and much more.