



# Accounts

## Planon Software Suite

Version: L105

© 1997 - 2024 Planon. All rights reserved.

Planon and the Planon logo are registered trademarks of Planon Software Development B.V. or its affiliates. All other product and company names mentioned herein are trademarks or registered trademarks of their respective companies. Planon Software Development B.V., its affiliates and/or licensors own the copyright to all Planon software and its associated data files and user manuals.

Although every effort has been made to ensure this document and the Planon software are accurate, complete and up to date at the time of writing, Planon Software Development B.V. does not accept liability for the consequences of any misinterpretations, errors or omissions.

A customer is authorized to use the Planon software and its associated data files and user manuals within the terms and conditions of the license agreement between customer and the respective legal Planon entity as soon as the respective Planon entity has received due payment for the software license.

Planon Software Development B.V. strictly prohibits the copying of its software, data files, user manuals and training material. However, customers are authorized to make a back-up copy of the original CD-ROMs supplied, which can then be used in the event of data loss or corruption.

No part of this document may be reproduced in any form for any purpose (including photocopying, copying onto microfilm, or storing in any medium by electronic means) without the prior written permission of Planon Software Development B.V. No copies of this document may be published, distributed, or made available to third parties, whether by paper, electronic or other means without Planon Software Development B.V.'s prior written permission.

# About this Document

## Intended Audience

This document is intended for *Planon Software Suite* users.

## Contacting us

If you have any comments or questions regarding this document, please send them to: [support@planonsoftware.com](mailto:support@planonsoftware.com).

## Document Conventions

### **Bold**

Names of menus, options, tabs, fields and buttons are displayed in bold type.

### *Italic text*

Application names are displayed in italics.

### CAPITALS

Names of keys are displayed in upper case.

## Special symbols

	Text preceded by this symbol references additional information or a tip.
	Text preceded by this symbol is intended to alert users about consequences if they carry out a particular action in Planon.

# Table of Contents

Accounts.....	7
User group.....	8
Creating user groups and linking function profiles.....	8
User.....	9
Adding a new user.....	10
User settings.....	10
Creating a password.....	10
Changing a password.....	10
Setting user's start and end date.....	11
Using a reference date.....	11
Setting / resetting a password.....	12
Resetting UUID.....	13
Clearing forgotten password attempts.....	14
Linking a user to a person.....	14
Generalizing screen settings.....	15
Configuring user screen settings.....	15
Linking alternative e-mail addresses.....	15
Clearing user screen settings.....	16
Access keys.....	16
Usage instructions.....	17
Configuration.....	18
Product definitions.....	20
Linking product definitions to user groups.....	20
Linking user groups to product definitions.....	21
How product definitions work.....	22
Available product definitions.....	24

Unlinking the scheduler product definition.....	28
Solution license.....	29
How does solution licensing work?.....	29
Function profile.....	30
Creating function profiles.....	30
BO Rights.....	31
Linking fields.....	31
Linking actions.....	32
Linking status transitions.....	33
Linking extended actions.....	33
Specifying permissions.....	34
Transferring permissions.....	34
BO Rights report.....	37
Authorization.....	38
Activating authorization.....	40
Creating authorization filters.....	40
Creating action authorization filters.....	41
In/activating action filters.....	42
ProCenter filters for authorization.....	42
Linking authorization filters to user groups.....	43
Authorization settings.....	46
Separating data access and functional access (splitting role and data).....	46
Authorization methodology differences.....	46
Authorization links.....	49
Reference links.....	49
Creating a reference link.....	50
Association links.....	51
Creating an association link.....	52

---

Dos and don'ts of authorization links.....	53
Users.....	54
Field descriptions.....	55
Access key fields.....	55
Association link fields.....	55
Authorization link fields.....	56
BO Rights fields.....	56
Details fields.....	57
Function profile fields.....	59
Key pair fields.....	59
Product definition fields.....	60
Solution license fields.....	61
User fields.....	62
User settings - fields.....	64
Index.....	68

# Accounts

The **Accounts** navigation group holds important functionality in respect to creating users and providing access to specific functionality.

For more in-depth examples and descriptions, see [Authorization](#).

# User group

A group of users whose access rights are determined by a function profile. In Planon Software Suite, users are required to belong to at least one user group.

The function profile linked to a user group specifies the functionality that will be made available to that user group. Usually, this functionality is based on the tasks that are required for a particular job role.

Each user group must be linked to a function profile.

For each user group, you can configure which products can be used.

## Creating user groups and linking function profiles

Users must belong to a user group. The rights of users in a specific user group are determined by the function profile (and any authorization filter) linked to this user group. This section discusses the general procedure for creating user groups and linking function profiles.

### Procedure

1. Go to User groups.

**On this level you can add or delete user groups.**


2. On the action panel, click Add to add a user group.
3. Enter a name and description.

**If necessary, you can add a remark in the Comment field.**


**The Users section displays the users that belong to the selected user group. When you have just added a new user group, there are no users linked yet.**

4. Click Users on the action panel.

A dialog box with available users is displayed; here, you can select the users to be included.

 For more information on adding entirely new users to the list of available users, refer to [Adding new users](#).

**Move the required users to In Use section.**


 On the **User group details** level you can find detailed information on the individual users of the selected user group. The Show unlinked user accounts button on the elements list enables you to display users that are not linked to a user group (keep in mind that filtering and navigation restricts the result in the elements list).



5. Link a function profile to the user group by using the Function profiles field. Select the appropriate function profile and click OK.

**The function profile is now linked to the user group. On User groups level, the related permission type is now displayed in the elements panel.**


6. In the Additional security logging field, click Yes if you want to log the login and logout timings of the users (in the selected user group). This data will be stored in the security logging file. To enable this feature, you must first make the security logging settings. For more information, refer to Security logging.


 User groups can also be copied, by using the **Copy** option from the **User groups** action panel. Copying a user group may save a lot of time, if there are many users and there is a substantial overlap between two user groups. All users and action filters that are linked to the user group are copied to the new user group. You can only link one function profile to a user group. If needed, you can also link one or more authorization filters to a user group. For each combination of function profile and authorization filter(s) a user group is required (for example Security Region North, Security Region South).

For more information on creating function profiles, refer to [Creating function profiles](#). For more information on creating authorization filters and linking them to a user group, refer to [Creating authorization filters](#).

The following actions are subject to security logging:

- Adding, changing and deleting user groups
- Linking or unlinking users to user groups
- Updating function profiles that are linked to the user group


 For more information about this topic, [Security logging \(Administrator's Guide\)](#).

 System reports available in **Authorization** provide an overview of authorization per business object/user group. For more information, see [System reports](#).

For more information on linking user groups to **Self-Service** web definitions or **Planon Live** mobile web definitions, see [Linking user groups to web definitions](#) and [Linking user groups to web definitions / granting access to modules](#) respectively.


## User


A user in *Planon ProCenter* is part of a user group and is linked to a person. Users are registered in the **User group details** step. A user can be linked to one or more user groups, so that more rights can be assigned to the user.

 Users belonging to multiple user groups can access all launch groups and function profiles associated with these user groups.

In the **Users** step, you can:

- add a user
- link a user to a person
- link a user to a user group
- reset a user's password
- display unlinked user accounts


 In **User settings**, end users can maintain their own settings. By default, the same user data fields are available as in the current **User groups** TSI. There is, however, one difference: the **User settings** TSI allows the administrator to configure which user settings can be maintained by the end users.

 A user account will be visible based on the reference date that is applied on the start and end date of the account.

## Adding a new user

### Procedure

1. At User group details, select a relevant user group.
2. Click Add on the action panel.
3. Fill out the fields in the data section. For a description of these fields, refer to User fields.
4. Click Save.


 This user will be temporarily displayed in the elements list. If you refresh the elements list, the newly added user will disappear from the list. The reason is that the user needs to be linked to the user group first.

## User settings

This section lists a number of important and specific user settings and actions.

## Creating a password

A new password can be created for new accounts. When you save the new account, the new password is hashed and stored in the database.

 If the **Password never expires** field is set to **No**, then the expiry date is set to the current date plus the number of days as defined in the password expiry date.

## Changing a password

Users can change their own password.



Only users can change their own password, it cannot be changed by anyone else. This is to prevent misuse.

### Procedure

1. Go to User groups > User groups details > Users.
2. Select your user account.
3. On the action panel, click Change password.

**The Enter values dialog box appears.**

4. In the Old password text box, enter your old password.
5. In the New password text box, enter your new password.
6. In the Confirm password text box, retype your password to confirm.
7. Click OK.

**A warning message is displayed saying that your password is changed and that you can try logging in again with the new password.**

8. Click Proceed. Your password is changed.

**When you change a password, the password policy validations are applied.**



For more information about the password policy, [Password settings](#).

## Setting user's start and end date

To set a user's start and end date, proceed as follows:

### Procedure

1. At the User groups, select the relevant user group.
2. Select the Users selection level.
3. From the elements list, select the relevant user.
4. In the data panel, fill out the Start date field and, optionally, the End date field.
5. Click Save.

You have now set this user's start date (and, optionally, the end date).

## Using a reference date

Throughout **Accounts** you can set a reference date.

By setting a reference date, your elements list will be filtered by this date and only the users will be displayed that are valid on the reference date, i.e. users whose start date is earlier than or equal to the reference date and whose end date is later than or equal to the reference date.

By default, the system date is the reference date.

By clicking the **Reference date** button you can select any other date from a date picker, whether it is in the past or in the future. To distinguish a selected reference date from the current date, the label of the **Reference date** button assumes a different color.

The reference date is by default activated. You can deactivate the reference date by clicking **Deactivate reference date** in the toolbar.

## Setting / resetting a password

As an administrator, you can (re)set a user password in case the user has forgotten the password or it has expired or for any other reason.



You must use authorization to prevent the users from resetting the password of other users.

### Procedure

1. Go to User group details > Users.
2. Select the user for which you want to reset the password.
3. On the action panel, click Set password. The Enter values dialog box appears.
4. The Password field is already populated with a new password generated by the system.



You can also overrule the default generated password.

5. In the Force change on login field, if you select Yes, the user will be forced to change the password on logging in.

If **No** is selected, the user is allowed to use the 'system generated' password or the password provided by the administrator.



- For user accounts whose password never expires, the **Force change password** feature is not available.
- The new password should be communicated immediately to the relevant user, because after the **OK** button is clicked the password is encrypted and cannot be retrieved anymore.

6. In the Send email field, select Yes if you want to notify the user about a reset password by email.

#### This email can only be sent if:

- a mail merge template has been configured for the email that should be sent to the user, at User group details > Users.



See *Reports* for more information on creating mail merge templates for user reports.

- this mail merge template is selected in the relevant language fields of the **Reset password report** setting in System settings > Security.

- the user's email address is entered in the **Contact's email address** field at the Settings > User settings step.
- a language has been specified for the user in the **Planon ProCenter Language** field at User group details > User settings.

## Resetting UUID

### Data collection

Within the Planon application, data that is collected pertains to:

- License usage (as covered in contracts);
- System events (these are technical events such as server startup or unhandled errors, such as Java exceptions);
- Anonymous interactions of users with Planon that relate only to software usage and are used as input for product improvements by Planon.

No personal (PII/PSI) data and no customer data is ever collected.

Some data that is being collected is enriched with a user UUID. A UUID is a Universally Unique Identifier, which can be used to identify information across a computer system.

The user UUID in Planon is randomly generated for a Planon user and cannot in any way be used to identify a natural person. UUIDs are used by Planon to determine the unique number of users using a particular product in a chosen time frame and are thus only used in an aggregated form.

### Reset UUID

A system administrator of Planon can reset a user's UUID (the system then replaces the UUID field stored with the user with a newly generated random UUID) such that future actions of the user cannot be related to past actions of this user.

To enable resetting the UUID, you must add the **Reset UUID** action to the layout:

#### Procedure

1. Go to **Layouts** and add the action **Reset UUID** to the **Users** (Account) layout.



This is only required once.

Once this is done and you log off / log on again, you can use the action.

2. Go to Accounts > User groups > User group details > Users step, click **Reset UUID** to reset the UUID.

- This you can do for a single user or, by using **Action on selection**, for a selection of users/for all users.
- You can manually click the action or you can automate it by creating a scheduled task for it.

## Clearing forgotten password attempts

If a user has forgotten his/her password and the account is locked, the Planon application manager can reset the number of forgotten password attempts.

### Preconditions

For this functionality to work, the following configuration must be in place.

1. In System Settings > Security, enable the **Forgot password functionality**.
2. In Layouts > Users (Accounts) add the **No. of attempts forgotten password** field and the **Clear forgotten password attempts** action.

When the user has forgotten their password and has requested a new password 3 times, the system administrator can clear the number of attempts as follows.

### Procedure

1. Go to User groups > User groups details > Users.
2. Select the user account.
3. On the action panel, click Clear forgotten password attempts.

**This option will only be enabled if there is a value in the No. of attempts forgotten password field.**


**The No. of attempts forgotten password field will be reset and the user will be able to use the Forgot password? option again.**


 For more information on the **No. of attempts forgotten password** field, see [User fields](#).

## Linking a user to a person

Someone who is registered as a user in **User Groups** is not automatically linked to a corresponding person in **Personnel**.

You have to establish this link manually. Once this is done, all TSI fields in which you can enter a person from **Personnel** and for which a default value has been specified by means of the **&Person** macro, will automatically be populated with the name of the logged-in user.

 If you are working with multiple property sets, it is possible to link multiple users to a single person from the **Personnel** TSI. You can use one user account for multiple property sets. Each property set contains its own persons so that you can link a person to the user account in each of these property sets.

 For more information on setting macros as default values, see [Using macros to specify a default value](#) ( Field definer ). For general information on macros, see [Relative filters using macros](#) (Fundamentals).

## Procedure

1. Go to User group details > Users.
2. Select the user to whom you want to link a person from **Personnel** .
3. On the action panel, click Persons.
4. From the Available list, select the person you want to link to the selected user and move it to In use.



**You can link only one person to a user within a property set. If you want to link another person to the current user, you must first move the selected person from the In use list back to the Available list and then try to link another person.**

5. Click OK. You have now linked a person from **Personnel** TSI to the selected user.

## Generalizing screen settings

To set default screen settings for all users in a company who have not logged on before. This will result in all new users having the same user interface to work with.

### Procedure

1. Go to User groups > Users.
2. Click the Generalize screen settings toolbar button.  
A message appears.
3. Click OK to set the screen settings for all new users or click Cancel to cancel the action.

## Configuring user screen settings

### Procedure

1. Go to User groups > Users.
2. Select the user for whom you want to set the screen settings.
3. Descend to Settings.

For a description of the fields, see [User settings - fields](#).

4. Click Save.
5. Log out and log in to the Planon application .

You have now configured the user screen settings.

## Linking alternative e-mail addresses

When a user's e-mail address is changed (example, after getting married or when a company's domain name is changed), to avoid problems when synchronizing existing

meetings, the old e-mail address can be registered as an alternative e-mail address so that there is a connection between the old and new e-mail addresses.

### Procedure

1. Go to User settings
2. In the element list, select a user to whom you want to add alternative e-mail address.
3. On the action menu, click Link alternative e-mail addresses. The Alternative e-mail addresses dialog box appears.
4. Select the e-mail addresses that you want to link and move them to In use.
5. Click OK.

**The selected e-mail addresses are now linked as alternative e-mail addresses to the user and existing meeting appointments will be kept in sync.**

## Clearing user screen settings



User settings can occasionally become corrupted and the application can behave in an unusual manner. You can resolve this by using the **Clear user screen settings** action.

### Procedure

1. Go to User groups > Settings.
2. Select the user for whom you want to clear the stored screen settings.

**You can select multiple users by CTRL+clicking user or by clicking All at the bottom of the list and then clicking Action on selection.**

3. On the action menu, click Clear user screen settings.

The stored settings of the selected user are now cleared. This means that all user settings are reset to the default, which affects:

- The order of gadgets (in the Planon ProCenter )
- The adjustment/alignment of columns
- The position of pop-ups
- The last used user filter

The next time the user logs on, their user settings will be reset.

## Access keys

By generating a key pair, the Planon administrator can enable using [access keys](#). A [key pair](#) consists of private key and a public key that together accomplishes two functions:



authentication and encryption. The private key (used to generate the access key) and the public key (used to decrypt the access key) are stored in the database.

When a key pair is generated, the Planon administrator can create access keys and give these to the intended audience to grant (limited) access to Planon (see [Usage instructions](#)).



You can only create access keys via the Web client. The Access key login works for Self-Service, SDK and Kiosk clients. Consequently, you cannot select the **Access keys** BO in Enterprise Talk and SDI, nor is it possible to reference an **Access key** field in an expression in Reports or other places.

## Usage instructions

Before using access key functionality, please read the following (security) instructions thoroughly.

### General

- This functionality is meant to provide (read-only) access to information in Planon or a third-party application that needs access to data in Planon, such as: surveys, charts, etc.
- This functionality only works for the Self-Service, SDK and Kiosk clients.

### Self-Service and Kiosk clients

- As security measure, throttling is applied to restrict the number of authentication requests via the access key per time interval, per client. The throttle time interval is only checked per client computer.
- If you login with the access-key, your session is state-full, e.g. you stay logged on until you log off.

### SDK

- The SDK connector supports access key authentication via the HTTP header instead of extending the URL. The Authorization parameter is set with a custom planon type: AUTHORIZATION: PLANONKEY accesskey=<key>. With this implementation, the key cannot be retrieved when using HTTPs.
- If you log on with the access-key your session is stateless.

### Hardware requirements

- Make sure your application has enough memory to accommodate these logins (check with your system management to evaluate your current memory usage).

### Security

Because access keys allow you to provide users access to the Planon application, Planon expects customers to understand the impact and follow security guidelines responsibly.

It is important to acknowledge that anyone who has your access key has the same level of access to the resources that you do.

Because users may be inclined to think that it cannot do any harm, they will much easier share a link than they would share a user name and password. Planon, therefore **strongly** recommends being very strict when using this functionality:

- Keep in mind if you distribute an access key, all people using it will use the same account to access Planon.
- Do not provide/generate an access for your root user. Anyone who has the access key of your root user has unrestricted access to all the resources in the account.
- Do not distribute access key links freely, only share them on a need-to-basis.
- Only use this kind of access if you really cannot use a user name and password solution.
- Limit the ability to generate key pairs to a dedicated account.
- Set an expiry date of the access key pair.
- Limit (access) privileges of the account for which this functionality is configured.
  - It is best to remove Web Client access for this account.
  - Only enable those product definitions that are required.
  - If used for the SDK, then only enable access to the SDK. If used for Kiosk, then only enable access to Kiosk etc.
- Limit the rights of the account to that what you want to accomplish.
- Make a Planon Self-Service form for the account for which you are generating access keys only, do not use it for other purposes.

### **License**


When using access keys, Planon licenses will be consumed as usual. The type of license applicable determines the license usage, the number of concurrent users granted access, etc.:

- Named user: If the account is connected to a named user license, an unlimited number of people can login because they all use the same account.
- Hit count: each login and usage will consume hits and increment the hit count.
- Concurrent license: you can only login as many times as you have concurrent licenses.
- Watch out with configuration make sure the regular Planon users still have a license. Make an assessment of the number of concurrent logins you expect.

## **Configuration**

Before being able to use access keys, some configuration is required:

- You must generate key pair.
- You must add the **Access keys** step to **User groups**.

 This only needs to be done once.

- You must create the access keys and distribute these.

### Generating a key pair

1. Go to System Settings > Security.
2. Click the Key pairs tab and click Generate key pair.

**Planon will generate a key pair and will automatically populate the fields on the Key pairs tab. For information about these fields, see [Key pair fields](#).**

### Generating access keys

1. Go to Accounts > User groups.
2. Drill down to Settings > Access keys.
3. Click Add to add an access key and fill out the required fields.

**For more information about these fields, see [Access key fields](#).**

4. Click Save.

**The access key appears in the Access key field.**

5. Put your cursor in the field and copy its contents (CTRL+A and CTRL+C).
  - The access key is an alphanumeric string that appears in a single line.
  - You can generate multiple access keys.
6. Paste the content in a text editor to save it for later use.
7. Go to the form that you want to share and copy its URL.
8. Paste the URL in a new line in the text editor preceding the access key.
9. Add the string ?accesskey= to the URL.

**For the various clients, this resembles the following:**

- **PSS:** https://<planon-instance>.<planoninstallation.com>/case/BP/ PUB003/?accesskey=
  - **Kiosk:** https://<planon-instance>.<planoninstallation.com>/kiosk?accesskey=
  - **SDK:** https://<planon-instance>.<planoninstallation.com>/sdk/?accesskey=
10. Merge the URL and the access key into a single line.

**You can now test the resulting URL. To do so, open a different browser and paste the new URL in the address bar and press ENTER.**

**The form to which you are granting direct access appears.**



When sharing URLs via mail, chat or any other means of communication, invisible characters (zero-width space) may be added that invalidate the URL. When receiving a URL in such a way, pasting it in a text editor will remove these invisible characters.

## Product definitions

Each user (account) is linked to a user group. By using user groups, there are two ways of arranging user access to Planon products:

- Linking product definitions to user groups
- Linking user groups to product definitions



- Arranging access to Planon products (when added or deleted) is subject to security logging. For more information about this topic, see [Security logging](#) in the WebHelp.
- Adding products to user groups or vice versa can be restricted for products having a named license. For more information, see [Licensing](#).

## Linking product definitions to user groups

You can link product definitions to a user group. This allows you to specify which products will be accessible to a user group.

### IMPORTANT



How product definitions work:

- By default, no user group is assigned to a product definition. In general, this means that all user groups can access all available products. However, when using [OpenID connect authentication](#), this does not apply to WebDAV product definitions. Here, you must explicitly link a user (group) to a WebDAV product definition, or access to the WebDAV location is denied!
- If there is one product linked to a user group (or vice versa) then the user group will not have access to other Planon products.
- Ensure that you do not exclude yourself from the application! Always make sure that Planon supervisors have access to all products.
- To better understand the consequences of linking user groups to product definitions (or vice versa), please read the article about [How product definitions work](#).



In order to start the Planon application, it is mandatory to add the PSS2 product definition along with the PPWeb product definition to the selected user group.

## Procedure

1. On the User groups selection level, select a user group to which you want to link products.
2. On the action menu, click Product definitions.

The **Product definitions** dialog box appears.

3. Select one or more products from the Available list and move them to In use.

For example, select PSS2 in the **Available** list and click the right arrow to move it to **In use**.

4. Click OK.

The user group is linked to the selected product(s). The users of this user group can access the linked product(s).

## Linking user groups to product definitions

You can link user groups to product definitions. This allows you to specify which user groups can access a specific product.

### IMPORTANT



How product definitions work:

- By default, no user group is assigned to a product definition. In general, this means that all user groups can access all available products. However, when using [OpenID connect authentication](#), this does not apply to WebDAV product definitions. Here, you must explicitly link a user (group) to a WebDAV product definition, or access to the WebDAV location is denied!
- If there is one product linked to a user group (or vice versa) then the user group will not have access to other Planon products.
- Ensure that you do not exclude yourself from the application! Always make sure that Planon supervisors have access to all products.
- To better understand the consequences of linking user groups to product definitions (or vice versa), please read the article about [How product definitions work](#).

### Procedure

1. In User group details > Product definitions step, select a product to which you want to link a user group.
2. On the action menu, click User groups.

The **User groups** dialog box appears.

3. Select a user group from the Available list and move it to In use.

4. Click OK.

**The user group is linked to the product definition. Users of this user group will have access to the product whose product definition is linked.**

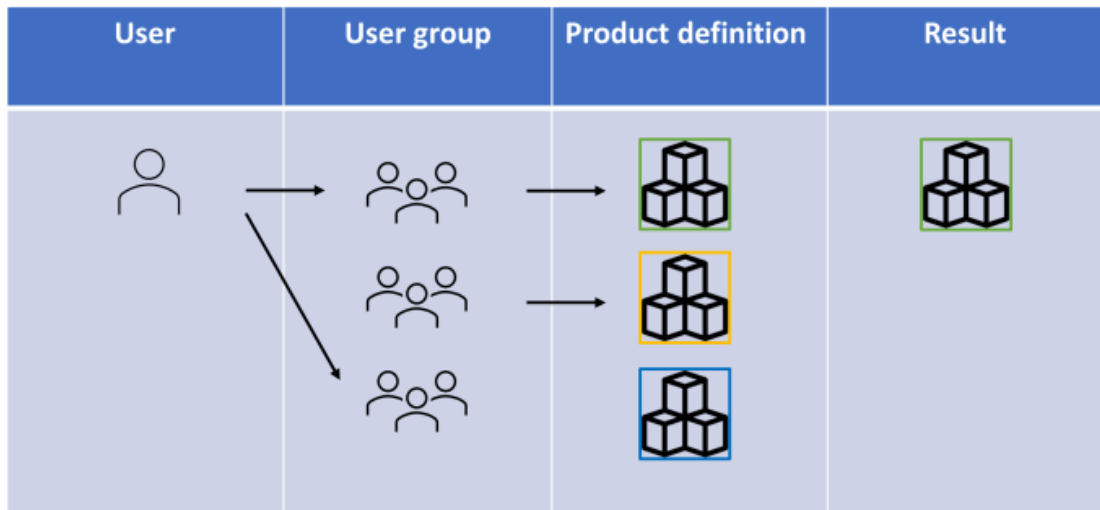
## How product definitions work

The following examples show the effect of linking user groups to products definitions (or vice versa).

Product definitions enable access to products. By linking user groups to product definitions (or vice versa), you can therefore determine who can access a specific product.

### Restrictive access

The following example illustrates that users are restricted to accessing products to whom their user groups are allowed access.



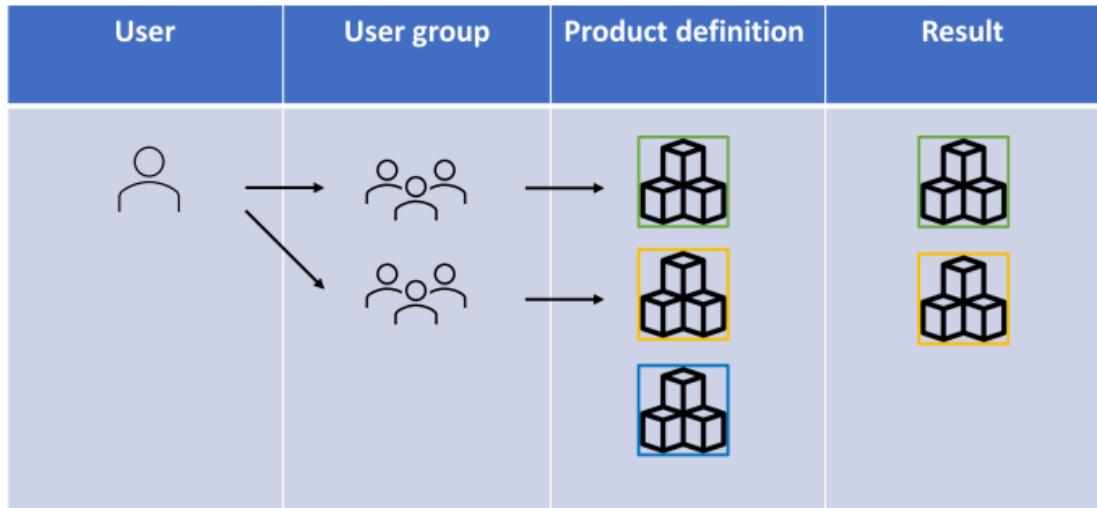
User 1 is linked to two user groups.

One user group is not linked to any product definition; users exclusively linked this user group have access to all products.

However, because user 1 is also linked to the first user group that is linked to product definition (green), the user only has access to product green.

### Extended access

The following example displays how linking a user to different user groups extends access to the products of those user groups.



User 2 is linked to two user groups.

User group 1 is linked to product definition (green), and user group 2 is linked to product definition (orange).

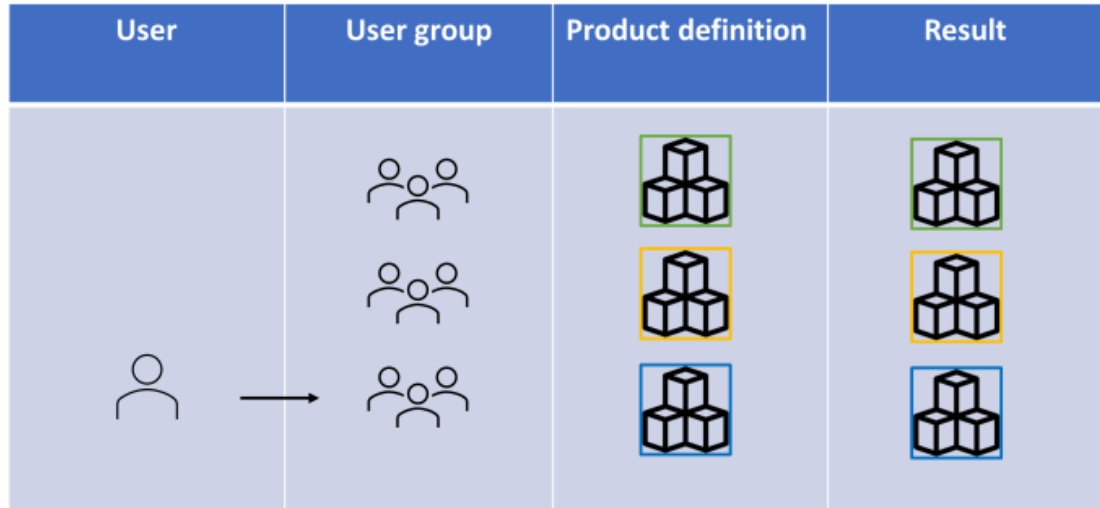
This user can access products green and orange.

## All access

This example illustrates that if no user group is linked to a product definition, a user linked to such a user group can access ALL products.



This situation does not apply to WebDAV product definitions. When using [OpenID connect authentication](#), you must explicitly link a user (group) to a WebDAV product definition, or users cannot access the WebDAV location!





User 3 is linked to the third user group, which is not linked to any product definition.

User 3 may therefore access all available products.

## Available product definitions

The following table lists the available product definitions and the products to which they provide access.

 For users to be able to use the products listed, make sure that the appropriate user group is linked to the corresponding product definition.

Product	Product definition / Name	Description
Analytics	Planon Analytics connector	<p>Extends the operational Planon system with a data lake and a data connector to external data analytics tools. This makes it easy to extract data for reporting, analytics and predictions with standard BI tools.</p> <p>For more information, see <a href="#">Connect for Analytics</a>.</p>
Apps	Apps Planon Apps	<p> Planon Apps has been phased out. If you upgrade your Planon software after December 01, 2021 to version L64 or higher (except for version L75), the Planon Apps will no longer work. Although Planon Apps will remain in the App stores until December 01, 2022, end-of-support policy applies. Planon has developed a new mobile self-service solution: the Planon Workplace Engagement App.</p>



Product	Product definition / Name	Description
		<p>Please contact your account manager for information about the possibilities of the new Workplace Engagement App and how to obtain it.</p>
		<p>Existing users who have not migrated yet can refer to <i>Planon Apps</i> for product information until December 01, 2022.</p>
AppSuite	<p>PMFS Planon Mobile Field Services</p>	<p><b>My jobs</b> module for field engineers to get and maintain jobs on their mobile devices. The app supports the whole workflow of job handling (starting, traveling, completing, pausing, ending jobs), scanning assets codes, meter readings, modifying activities and more. The product definition also includes the Service requests module to enable field engineers to add new jobs.</p> <p>For more information, see the <i>PMFS configuration guide</i>.</p>
AppSuite	<p>PMFS-PRO Planon Mobile Field Services with support for Stock</p>	<p>Same features as in PMFS, but with additional <b>Materials</b> module that supports a stock requests workflow and mobile stores.</p> <p>For more information, see the <i>AppSuite - configuration guide</i>.</p>
AppSuite	<p>PMAV Planon Mobile Asset Viewer</p>	<p>Graphical display of assets in an integrated viewer.</p> <p>For more information, see the <i>AppSuite - configuration guide</i>.</p>
AppSuite	<p>PMBV Planon Mobile BIM Viewer</p>	<p>BIM (Building Information Modelling) viewer provides 3D modeling representation of the assets and building elements in a building.</p> <p>For more information, see the <i>AppSuite - configuration guide</i>.</p>
AppSuite	<p>PMPV Planon Mobile Property Viewer</p>	<p>Provides easy access to property information you may need while working on a maintenance job. The search functionality enables users to</p>

Product	Product definition / Name	Description
AWM	AWMDataEngine Planon AWM Data Engine	find the correct building information via one or more search criteria.  For more information, see the <i>AppSuite - configuration guide</i> .
Connect for AutoCAD	EnterpriseServiceAPI Planon ProCenter Enterprise Service API	A plug-in that is integrated into AutoCAD and enables AutoCAD users to maintain Planon ProCenter data in their CAD drawings.
Connect for Outlook	JsonServices Planon JSON services	For more information, see <a href="#">Connect for AutoCAD</a> .
Connect for Outlook	Exchange Planon ProCenter Connect for Outlook	Allows users to use Microsoft Exchange clients such as Outlook / Web Access to invite attendees and create reservations in Planon ProCenter. Through Connect for Outlook, reservations in Planon ProCenter are synchronized with Exchange so the user can see the availability of rooms and attendees in one view in their calendars.  For more information, see <a href="#">Connect for Outlook</a> .
EventConnector	Event Connector	A gateway between third-party applications and Planon. It is designed to process messages that are sent by another application and which need to be processed in the Planon application, and vice versa. By using Event Connector, third party application messages can be received and processed through a

Product	Product definition / Name	Description
		<p>Decision Model to determine if/what further action is required.</p> <p>For more information, see <a href="#">Event Connector</a>.</p>
IDE	Integrated development environment	<p>Unlocks the ability to enable an Integrated Development Environment in your Planon application. By using the IDE, you can set up your own developer's workspace and create apps that interact with the Planon application via business rules.</p> <p>For more information, see <a href="#">Platform apps</a>.</p>
PSS2	PSS2 Planon ProCenter Self-Service	<p>Creating web forms to be linked to your Planon application.</p> <p>For more information, see <a href="#">Web configuration</a>.</p>
Resource Planner	EnterpriseServiceAPI Planon ProCenter Enterprise Service API	<p>Enables you to use a graphical planning tool. It gives access to one or multiple specially configured planboards, on which you can assign work to available resources quickly and easily.</p>
Scheduler/ Alerts	Scheduler Planon ProCenter Planned Services Scheduler	<p>Allows you to create and schedule jobs or notifications/alarms for events that occur and for which you need or want to be informed. Typically with a notification an email sent to a designated person; an alarms results in a visual notification in the user interface of the appropriate person.</p> <p>For more information, see <a href="#">Alerts</a>.</p>
Web Client	PPWeb Planon ProCenter Web Client  PSS2 Planon ProCenter Self-Service	<p>To enable access to the Planon application via an Internet browser.</p>
WebDAV	WebDAV	<p>When enabling OpenID connect authentication for WebDAV (Cloud</p>

Product	Product definition / Name	Description
	WebDAV_Audit WebDAV_Backup WebDAV_PEET WebDAV_TMS WebDAV_Webservices	<p>only) in the <a href="#">Environment Management gadget</a>, you must assign the various WebDAV product definitions to the appropriate user group(s).</p> <ul style="list-style-type: none"> <li>• WebDAV For access to images and documents.</li> <li>• WebDAV_Audit For access to audit logging.</li> <li>• WebDAV_Backup For access to database back-ups.</li> <li>• WebDAV_PEET For access to Enterprise Talk (PEET) folders.</li> <li>• WebDAV_TMS For access to Tailor Made Solution folders.</li> <li>• WebDAV_Webservices For access to Web services.</li> </ul> <p>For more information, see <a href="#">OpenID connect</a>.</p>
Web Services	PPWS Planon ProCenter Web Services	<p>A service to enable and implement a Service Oriented Architecture in which multiple enterprise applications can be linked to share data via an interfaces to connect these applications.</p> <p>For more information, see <a href="#">Web Services</a>.</p>

## Unlinking the scheduler product definition



When the scheduler product definition is removed from a user group, this change will only be reflected after restarting the application server (which includes a restart of the scheduler).

## Solution license

A license type that is based on a fixed number of named users per solution (a set of modules). An administrator can provide solution access to users by linking user groups to solutions (or vice versa). Users in a user group that are not linked to a solution cannot use the modules included in that solution.

The **solution license** list is displayed at following locations in the Planon application:

- User groups > User group details > Solution licenses.
- System settings > License > License usage > Solution licenses.

## How does solution licensing work?

- In **Solution licenses**, user groups can be linked to solution licenses to provide access to the modules included in the solution. The modules disclosed are listed on the product list that comes with the license key.
- Only users linked to the solution license can use the modules in the solution.
- It is not possible to add more (unique) users than specified in the solution license.
- If the number of linked users is greater than the license describes, a user group should be removed from the solution license. Alternatively, you can also remove users from other user groups to be able to add a new user group to the solution license.
- Planon checks against these criteria, when:
  - Linking the solution license to a user group.
  - Linking a user group to a solution license.
  - Adding users to a user group.



Linking or unlinking a solution license to a user group is subject to security logging. For more information about this topic, see [Security logging](#) (Administrator's Guide).

# Function profile

A function profile is used to define a certain role that a user group can have, for example security officer, and specify the rights for functionality. Function profiles always refer to functionality and not to data!

Function profiles are reusable: the same function profile can be used at different locations, for example in different regions. The rights for functionality are the same, but the rights for data can vary per location (region).

For example: the security function profile can be used for the security officers of property north and those of property south. On a functional level, the rights are the same, but the rights for data differ (region north and south).

For each business object you can specify which fields, actions and status transitions should be accessible. In Planon Software Suite, three authorization levels can be distinguished:

- No access to business object;
- Read-only access to business object;
- Business object can be modified.



Access to a business object is read-only by default. Fields can be made modifiable individually.

## Creating function profiles

As a prerequisite for creating function profiles, the first step is to enable authorization for the required business objects.

For more information on enabling authorization, refer to [Authorizing business objects](#).

Per function profile, you can specify a default level of permission for a business object:

- Invisible
- Read only
- Full functionality

### Procedure

1. Go to Accounts > Function profiles.
2. On the action menu, click Add.

Or, if you want to re-use an existing function profile, click **Copy**.

3. Complete the fields in the data section. For a description of these fields, see Function profile fields.
4. Click Save. You can now proceed to specify business object permissions for this function profile.

The following topics are subject to security logging:

- Updating function profiles when linked to user group
- Changing the **Default permission type** field



For more information about this topic, see [Security logging](#) (Administrator's Guide).

## BO Rights

After creating function profiles, you can specify the permissions you want to set per business object for a particular function profile.

### Specifying permissions

#### Procedure

1. On the Function profiles level, select the function profile for which you want to specify permissions and then navigate to the BO Rights level.
2. Per business object, complete the fields in the data section. For a description of these fields, refer to BO Rights fields.
3. Click Save.

If you have selected **Invisible**, **Read only**, or **Full functionality**, you have now completed specifying the permissions for the selected function profile.

If you have selected **Specific** for one or more business objects, you should continue configuring the function profile permissions, by:

- [Linking fields](#)
- [Linking actions](#)
- [Linking status transitions](#)
- [Linking extended actions](#)
- [Specifying permissions](#)



System reports available in **Authorization** provide an overview of authorization per business object/user group. For more information, see [System reports \(Authorization\)](#).

## Linking fields

You can determine per business object which fields should be available for a specific function profile.

### Procedure

1. On the BO Rights level, select a business object from the element list for which you want to specify the fields that should be available.
2. On the action menu, click Fields.

**The Fields dialog box appears. This dialog box allows you to select the fields you want to make available to the business object.**

3. Use the arrow buttons to move items from the Available list to the In use list, or vice versa .

The **Available** list displays the data fields that are available for use with the selected business object. The **In Use** list displays the data fields that are to be included in the function profile. These data fields will then be available to the user group to which the function profile is linked. Use the arrow buttons to add or remove fields.



When adding or removing data fields, you should always consider the following:

- When adding a reference data field, such as Person, it is advised to define at least read permissions on the principal fields such as **Code** and **Name** of the referenced business object as well.
- Not adding these fields to the function profile can result in missing fields and columns in the quick search feature of the relevant dialog box and it can also cause the tree within the dialog box to have an irregular appearance.
- Some data fields should not be removed from the function profile. These include fields indicating a hierarchy, such as the **ParentOrderGroupRef** field in the **Order Group** business object. If the **ParentOrderGroupRef** field is not included in the function profile, the tree view will display the objects without any hierarchy.

4. Click OK. The selected fields are linked to the function profile.



Linking fields to business objects is subject to security logging. For more information about this topic, see [Security logging](#) (Administrator's Guide).

## Linking actions

You can determine per business object which actions should be available for a specific function profile.

### Procedure




1. On the BO Rights level and, select a business object from the element list for which you want to specify the actions that should be available.
2. On the action menu, click Actions.

**The Actions dialog box appears. This dialog box allows you to select the actions you want to make available to the business object.**

 If you want to grant a user dearchiving rights, you must also grant save rights.

3. Use the arrow buttons to move items from the Available list to the In use list, or vice versa.
4. Click OK.

**The selected actions are added to the function profile.**

 Linking actions to business objects is subject to security logging. For more information about this topic, see [Security logging](#) (Administrator's Guide).

## Linking status transitions

You can determine per business object which status transitions should be available for a specific function profile.


### Procedure

1. On the BO Rights level, select a business object from the elements list for which you want to specify the status transitions that should be available.
2. On the action menu, click Status transitions.

**The Status transitions dialog box appears, which allows you to select the status transitions you want to make available to the business object.**

3. Use the arrow buttons to move items from the Available list to the In use list, or vice versa. By default, no status transition is accessible.
4. Click OK.

**The selected status transitions are linked to the business object.**

 Linking status transitions to business objects is subject to security logging. For more information about this topic, see [Security logging](#) (Administrator's Guide).

## Linking extended actions

You can determine per business object which extended actions should be available for a specific function profile.

### Procedure

1. On the BO Rights level, select a business object from the elements list for which you want to specify the extended actions that should be available.
2. On the action menu, click Extended Actions.

**The Extended Actions dialog box appears. This dialog box allows you to select the extended actions you want to assign to the business object.**

3. Use the arrow buttons to move items from the Available list to the In use list, or vice versa.
4. Click OK.

The extended actions are linked to the business object.



Linking extended actions to business objects is subject to security logging. For more information about this topic, see [Security logging](#) (Administrator's Guide).

## Specifying permissions

After linking actions/fields/extended actions/status transitions, you can continue to specify permissions for these items.



This only needs to be done for business objects whose permission type is **Specific**.

### Procedure

1. On the BO Rights level, select the business object for which you want to specify permissions and then navigate to the Details level.
2. The Details level contains multiple steps. Select the appropriate step. For a description of the fields on this step, refer to Details fields.
3. Click Save.

**You have now completed specifying permissions for the selected function profile.**

## Transferring permissions

Function profiles will very often need the same permissions for a fixed set of business objects.

Similarly within a single function profile multiple business objects can have the same permissions for certain (extended) actions. If you had to manually assign these permissions to other business objects and function profiles, this would result in a lot of repetitive work. To avoid this, you can first define the function profile details (fields, (extended) actions and status transitions) for a single business object and then you use the Transfer permission details action to transfer them in one go to one or more business objects in one or more function profiles. Although you can both add and delete

the function profile details of an individual business object, you have to transfer the added and removed details separately to the other business objects and/or function profiles.

## Procedure

1. On BO Rights level, select the business object whose permission details you want transfer.



The list only displays the business objects for which **Is authorized** is enabled in Field definer . System fields are never shown because they cannot be authorized.

2. On the action menu, click Transfer permission details.

The **Transfer permission details** wizard appears. Complete the wizard steps; these steps are outlined in the wizard's **Selection step** panel. The steps displayed depend on the selected BO's permission type.

For the following permission types, proceed with [Step 9](#):

- Invisible
- Read only
- Full functionality

For permission type *Specific*, the **Define transfer action** step is selected.

3. Indicate whether you want to change the target's permission type to *Specific*.
4. Depending on whether you want to transfer either added details or removed details from the selected BOs and function profiles, select the Add or Delete option.



If you need both to add and delete details, the transfer must be done twice.

5. Click Next.

**The Select the field(s) step appears. Select the field(s) that you want to add to the business objects and function profiles.**



Use the SHIFT + CTRL keys to select multiple fields.

A search bar is available for searching in the **Available** list. If there are no fields to be added, just click **Next**.

The **Select the action(s)** step appears.

6. Select the action(s) you want to add to the business objects and function profiles. If there are no actions to be added, just click Next.

**The Select status transition(s) step appears.**

7. Select the status transition(s) you want to add to the business objects and function profiles. If there are no status transitions to be added, just click Next.

The **Select Extended action(s)** step appears.

8. Select the extended action(s) you want to add to the business objects and function profiles. If there are no extended actions to be added, just click Next.

The **Select the business object(s)** step appears.

9. Select the business object(s) to which you want to add the above details.
  - Select **Show all business objects** to display all the authorized business objects.
  - Select **Show related business objects** to display all the related (authorized) business objects. Related business objects are all business objects that have the same base business object as the business object selected in [Step 1](#).
10. Select the functional profile to which you want to add the above details. Click Next.

The **Confirm** step appears.

11. This screen displays a summary of the selected details.
  - Click **Complete** to finish the transfer.
  - Click **Previous**, if you want to make changes in any of the previous steps.

The selected details are transferred to the selected business objects and function profiles.

The following changes take place when the details are transferred:

- If an added field is transferred, all its permissions are also transferred. If the field already exists in the destination business object, then its permissions are overwritten.

If the selected field is not a system field in the original business object, but is a system field in the destination business object, then it will not be transferred.

- If a field, an action, a status transition with exactly the same system name is present in the destination business object or if an extended action with exactly the same *Planon Software Suite* class name is present in the destination business object, then they will be set to *In use* (if not already).

If this is not the case, the transfer of details to that business object is skipped and the transfer continues with the next detail/business object.



If you have selected the **Delete** option, all function profile details that are not in use for the selected business object are now displayed in the **Available** column.

When deleting details, the following changes take place when the details are transferred:

- If a field, an action, a status transition with exactly the same system name is present in the destination business object or if an extended action with exactly the same *Planon Software Suite* class name is present in the destination business object, then they will be set to **Not in use** (if it was **In use** before.)

If this is not the case, the transfer of details to that business object is just skipped and the transfer continues with the next detail/business object.

## BO Rights report

This section describes the system report that is available in Function profiles > BO Rights. By clicking **Edit report settings** in the action menu, you can determine the information to be displayed.

---

Parameters	Description
Title	Enter a text that will replace the default report title.
Subtitle	Enter a text that will be placed beneath the title.
Fields	Select this check box to include in the report the fields available to the function profile.

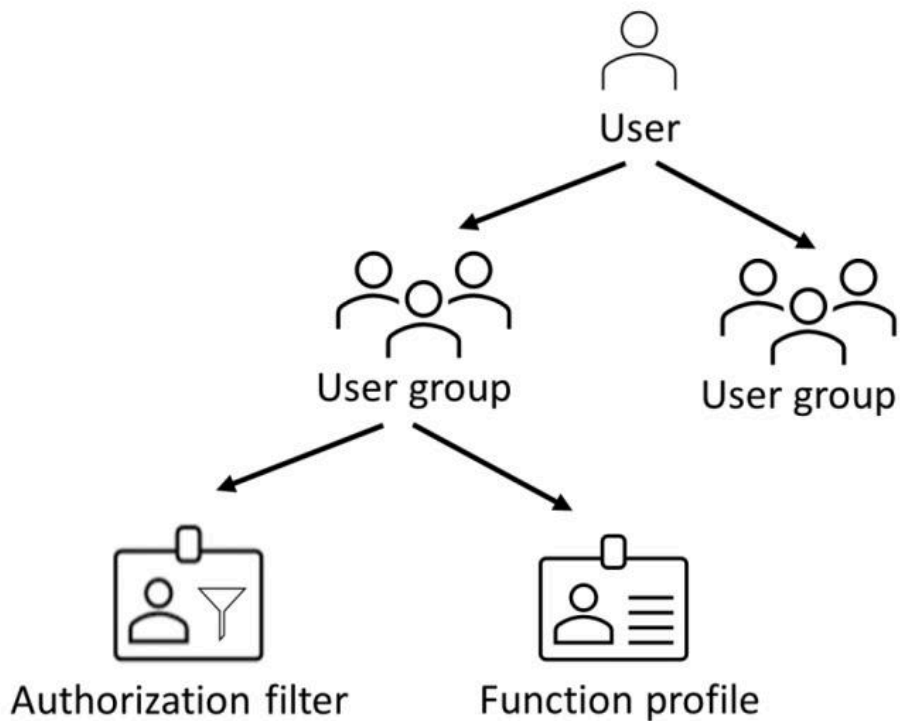
---

# Authorization

In Planon Software Suite authorization is based on the principle of separating data and functionality. An administrator can therefore create:

- User groups, which can be used in two ways:
  - To combine data and functional access
  - To separate data and functional access
- Function profiles to specify the functionality (such as data fields, actions and status transitions) to be made available to certain users.
- Authorization filters to limit users to accessing specific data.

By linking a function profile and authorization filters to a user group you can determine the rights of the users of this particular user group.



---

## Authorization filter

Access to data:

- No access

## Function profile

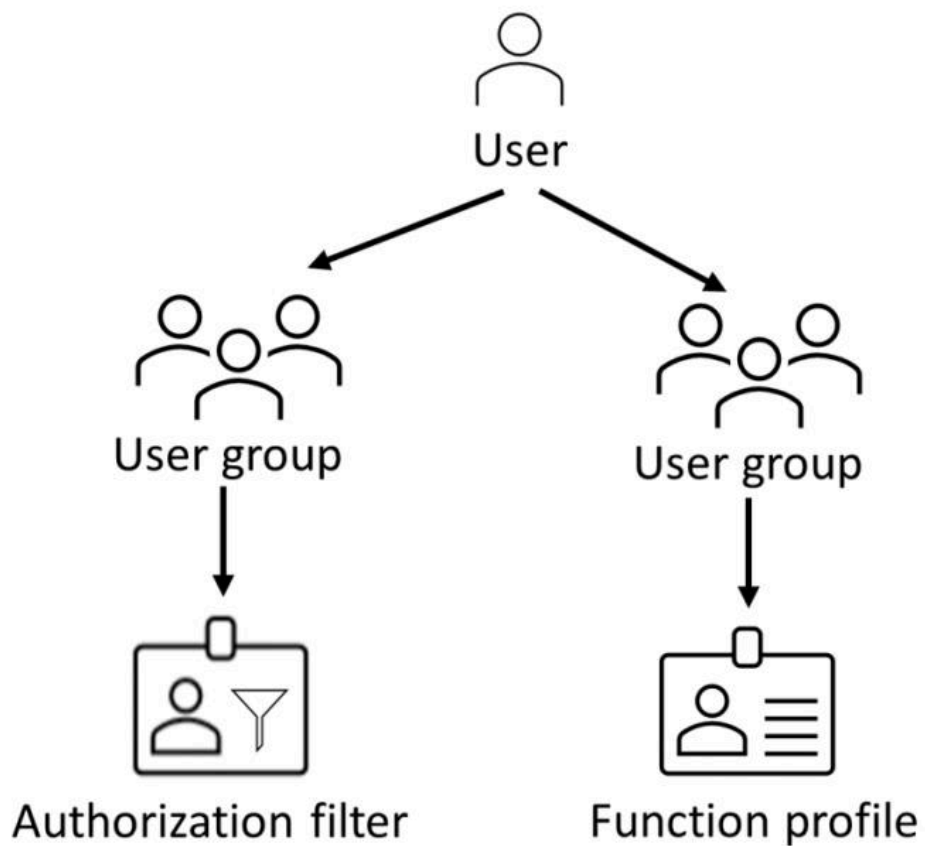
Access to functionality:

- Fields

Authorization filter	Funtion profile
<ul style="list-style-type: none"> <li>• Read-only access</li> <li>• Modify</li> </ul>	<ul style="list-style-type: none"> <li>• Status transitions</li> <li>• Actions</li> </ul>

When using this type of profile, the combination of user groups grants access to specific data. By linking users to multiple user groups, access to data is expanded.

Or, alternatively, you can separate functional access and data access by applying [split role and data](#):



Authorization filter	Funtion profile
Access to data: <ul style="list-style-type: none"> <li>• No access</li> <li>• Read-only access</li> </ul>	Access to functionality: <ul style="list-style-type: none"> <li>• Fields</li> <li>• Status transitions</li> </ul>

Authorization filter	Funtion profile
<ul style="list-style-type: none"> <li>• Modify</li> </ul>	<ul style="list-style-type: none"> <li>• Actions</li> </ul>

When using this profile, the combination of user groups grants specific access to data. When using authorization links, this type of combining profiles acts restricting as is explained in [Separating data access and functional access](#).


For more information on the concepts used in Authorization, see [Authorization concepts](#).

## Activating authorization

Authorization is inactive by default and it is therefore necessary to activate it before authorization can take place. It is only necessary to activate authorization once.

### Procedure

1. Go to **Accounts** > Authorization.
2. On the top right corner, click the slider  to activate or deactivate authorization.


 Activating/deactivating authorization is subject to security logging. For more information about this topic, see [Security logging](#) (Administrator's Guide).


## Creating authorization filters

An authorization filter allows a Planon administrator to specify the data users are allowed to view, modify, and perform actions on.

For example, if an organization has two properties in two different regions North and South. The personnel in North are only allowed to access data belonging to property North, whereas the personnel in South are only allowed to access data belonging to property South. To accomplish this filtering of data, two authorization filters could be created.

An **Authorization** button is available on the TSI to enable or disable entire authorization feature.

 The use of authorization filters is optional.

 While creating authorization filters, you cannot include fields exceeding 2000 characters.




### Procedure

1. Go to Filters > Authorization filters step.



2. On the action panel, click Add.
3. Select a business object for which you want to create the filter, for example Visitor and click OK.
4. In the Filter field, set the filter criteria by selecting the fields to be filtered on. On each data field, select an operator and then add a corresponding filter parameter.
5. Click Save.

**The authorization filter is now ready for use.**

	If an authorization filter is applied to a business object's subtype, it is only effective for that particular subtype. The other types (i.e. the main object and other subtypes) will all be visible and unfiltered. If an authorization filter is applied to a main business object, it is only effective for that main type and all subtypes will be visible and unfiltered.
	Updating authorization filters (when linked to a user group) is subject to security logging. For more information about this topic, see <a href="#">Security logging</a> .
	For more information on defining and using filters, refer to <a href="#">Fundamentals</a> . For more information on creating user-defined business objects, refer to <a href="#">Field definer</a> .

## Creating action authorization filters

By using action authorization filters, Planon administrators can specify the actions available for the selected user group based on the authorization filter criteria.

For example, if an organization has many properties, for users of the UK property an action authorization filter is created. All user in UK properties are authorized to add, cancel and modify actions but only few users are authorized to delete. Hence, two action filters could be created on same action authorization filter and user group but for different actions.

### Procedure

1. Go to Authorization > Filters.

**On the Action authorization step, you can assign a user group to the action authorization filter.**

2. Go to the Action authorization selection step.
3. On the action menu, click Add.
4. Select a authorization filter for which you want to create the action filter and click OK.

**You can also add the authorization filter directly in the Authorization filter popup.**

5. Click OK.
6. Select the action that is allowed for the authorization filter and user group, click OK.



You can create multiple filters for different actions on the same authorization filter and same user group.

7. In the User group field, select the user group for which you want the filter to be applied, click OK.
8. Click Save.

The action authorization filter is now ready to use.

## In/activating action filters

When creating or working on existing action authorization filters, you can make a filter activate/inactive.

Making them active/inactive allows you to test the filter without having to enable/disable authorization altogether.

### Procedure

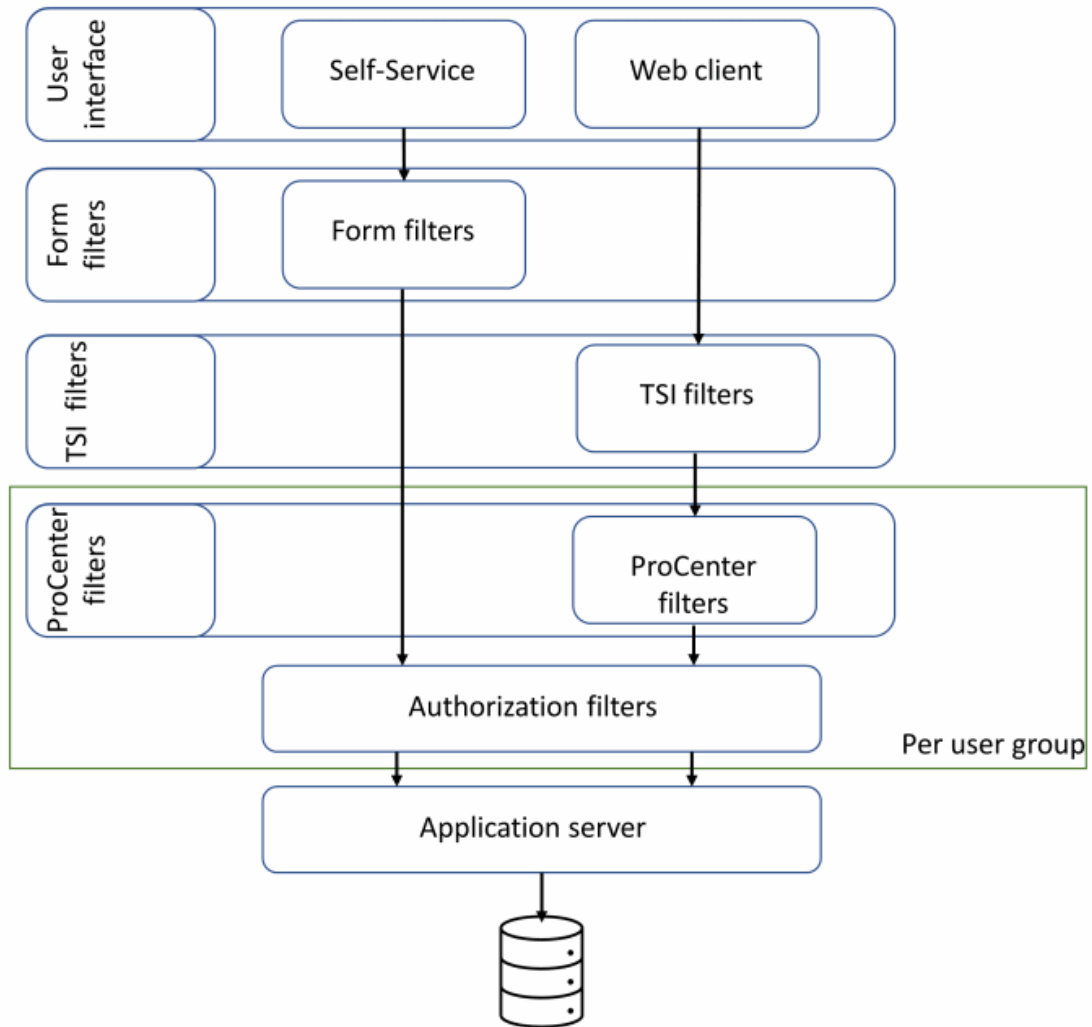
1. On the Action authorization step, you can use the quick search on top of the elements panels to filter on Activated = Yes.
2. Select the required filter in the list and, in the data panel, set:
  - **Activated** to **No** if you want to disable the filter
  - **Activated** to **Yes** if you want to enable the filter


Toggling this setting allows you to test whether your changes have the required effect without having to switch off authorization entirely.

## ProCenter filters for authorization

ProCenter filters are similar to authorization filters except that they are limited to **Web Client** TSIs. Other products such as **Kiosk**, **Apps** and **Self-Service** will not be affected by the ProCenter action filters. After you create a ProCenter filter, you can then create action filters with it. A **ProCenter action filter** button is available on the TSI to enable or disable all ProCenter action filters. It is also possible to enable or disable individual ProCenter action filters.

The ProCenter action filter and other filters are depicted in the image given below:



 If **Authorization** or **Split role and data** is turned off, ProCenter action filters are also automatically disabled and cannot be activated until both these settings are enabled.

## Linking authorization filters to user groups

Authorization filters can be linked to user groups in order to specify the data the user group is authorized to access. Proceed as follows to link an authorization filter to a user group.

### Procedure

1. Go to Authorization > Filters selection level.

Here you can add or delete actions, business objects and authorization filters. Action authorization filters are linked to a user group in order to specify the actions (e.g. **Read**, **Save**,

Delete etc.) that can be performed on the filtered data from the authorization filter.



- In the **Business objects** selection level, the field **Is authorized?** of a business object must be set to **Yes**, in order to add an authorization filter on it.
- Adding, deleting, updating action filters is subject to security logging. For more information about this topic, see [Security logging](#) (Administrator's Guide).

2. In the **Action authorization** selection step, click Add on the action menu.
3. Select the required authorization filter in the Authorization filter field.
4. Select the required action in the Actions field.
5. Select the User group to which you want to link the action filter.

The selected action determines what users are allowed to do with the data (view, modify, copy etc).

For example: a **Read** filter (action=Cancel) is set on the property business object (property=North). This filter is linked to the Security North user group. This means that the users from the Security North user group are allowed to view but not modify the information from property North. In addition, users belonging to Security North will not be able to view properties from other regions.



- It is not possible to link the **Add** action to an authorization filter, since this action is included as part of the **Save** action (the **Add** action is used when the user clicks **Save**). Therefore, a filter on the **Save** action suffices.
- After you have unlinked an authorization filter from a user group, you need to refresh the cache of the webserver to deactivate the working of the filter.



If no authorization filter has been linked to a user group, then users belonging to that user group will have access to all data from the business objects of the linked function profile. The rights to access this data will then at least be read-only.

### Combining filters

Authorization filters are combined in the following way:

- Authorization filters combined in a single user group. Combining two authorization filters in a single user group is only possible if they are linked to different actions. The result is the sum of both filters: the user gets fewer rights. For example: the filters Region North and Orders worth less than €5000 have been linked to a user group. The members of this user group only see the orders of region North that are worth less than €5000.
- If a user is a member of two user groups, the authorization filters in both user groups are combined and the user gets more rights. For example: a user who is member of the user groups Service Desk

North and Service Desk South will be able to view all data of both regions North and South.

**Applying authorization to status transitions:**

You can also apply authorization to status transitions of various user groups by using Authorization filters. For example, the following table explains what authorization conditions can be set on each status of the **Person** business object:

---

<b>Status</b>	<b>Example conditions</b>
Approved	<b>Approval by</b> field must be filled in with the logged in user(&Person)
Administratively completed	<b>Costs incl. VAT</b> field must contain a value greater than 0.
Question to requestor	<b>Question</b> field must contain a value.
In preparation	<b>Coordinator</b> field must contain a value.

---

# Authorization settings

Arranging authorization based on combining user groups and linking function profiles may cause a burden of having to maintain a large number of groups, profiles and filters.

You can decrease this potential maintenance burden by separating data access and functional access. By clearing the link between user group and function profile it is now possible to establish such a separation as will be explained in the following sections.

It is possible to reuse data or functional user groups for different users.

## Separating data access and functional access (splitting role and data)

### Procedure

1. Go to Accounts > Authorization settings.
2. Assuming Authorization is already set to Yes, set Split role and data to Yes also.
3. Create data user groups and functional user groups.
4. Link users to functional user groups and data user groups.

The result of the **Split role and data** setting is that in Authorization > User groups, the **Function profile** field is no longer a mandatory field. Consequently, it is possible to have user groups without linked function profiles.

By linking an authorization filter to a user group without a function profile, you can grant data access to a specific data set (data access).

Applying authorization in this manner has functional implications, as is explained in [Authorization methodology differences](#).



After setting **Split role and data** to **Yes**, it will be difficult / near to impossible to revert this change.

## Authorization methodology differences

Users can be assigned to multiple user groups. If a user is linked to two user groups, one with filters and one without filters, the functional/data access is different:

<b>Combining data and functional access</b>	<b>Separating data and functional access</b>
the access rights of users expands, granting full access/allowing all actions.	Access rights of users is decreased, limiting the access/available actions.

When using authorization links, and a user is linked to two user groups, one with links and one without links, the functional/data access is different:

<b>Combining data and functional access</b>	<b>Separating data and functional access</b>
The link is only applied to the data set of the linked user group	The link is applied to the data set of both user groups.

**Examples**

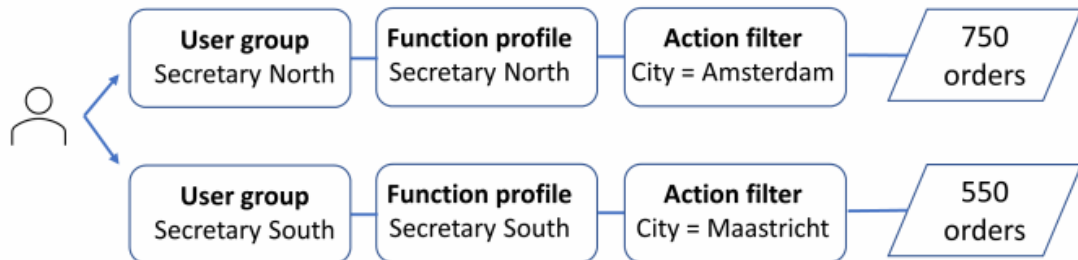
The following scenarios will further help understand the authorization methodology differences.

Imagine three users having access to all, or parts of the following data:

<b>Data set Amsterdam</b>		
<b>Total number of orders</b>	<b>Orders &gt; €1000</b>	<b>Orders &lt; €1000</b>
750	250	500

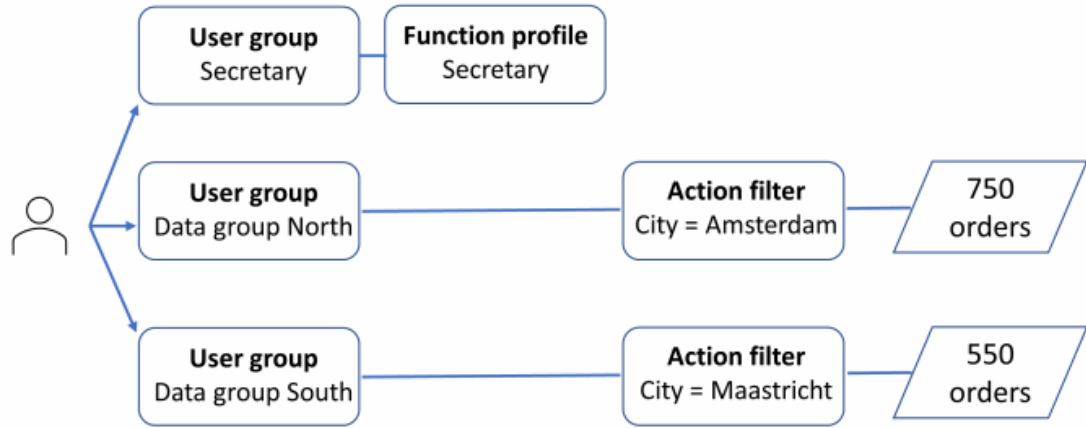
<b>Data set Maastricht</b>		
<b>Total number of orders</b>	<b>Orders &gt; €1000</b>	<b>Orders &lt; €1000</b>
550	300	250

**Combining functional and data access:**



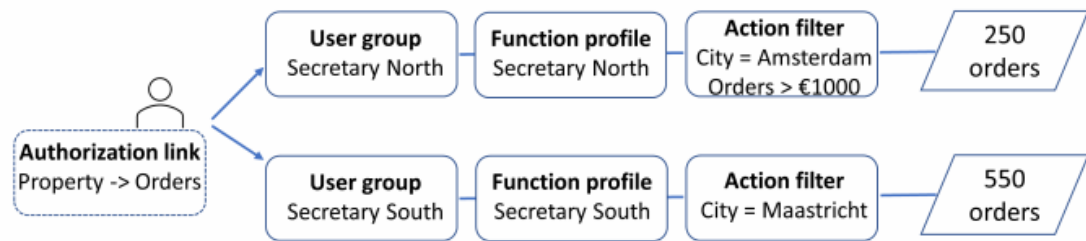
Each user group has its own function profile and action filter.

**Separating functional and data access:**



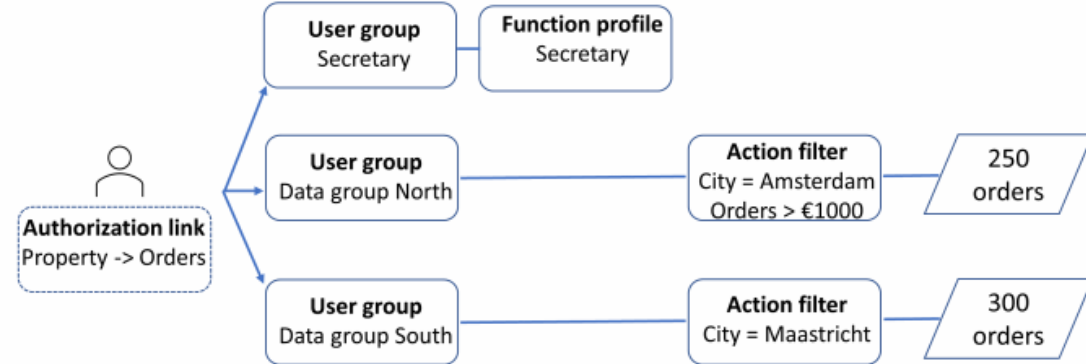
Only a single function profile is required, splitting role (fields, actions, etc.) and data access.

**Combining functional and data access (and using authorization links):**



The filter is only applied to one data set, limiting data access for this data set only.

**Separating functional and data access (and using authorization links):**



The filter is taken into account for both data sets, limiting the data access.

**i** System reports available in **Authorization** provide an overview of authorization per business object/user group. For more information, see .



# Authorization links

An authorization link is a link between two business objects that affects the data set to be displayed to the user.

An authorization link limits the data set displayed to the user for reasons of security or usability.

There are two kinds of authorization links:

- [Reference links](#)
- [Association links](#)

## Example

The difference between these two types of links is best explained by an example:

### Reference link

- There is a reference field on BO Orders, where you can specify a property. You can make a reference link, which means that if the user has an authorization filter on properties, they will only see the orders where the reference field has a value from the list of authorized properties.

### Association link

- There is an M-to-N ('many-to-many') link between BO Standard orders and BO Properties. This means one standard order can be linked to many properties, not just one, as would be the case with a reference field. When the user has an authorization filter on BO Properties, to show only the properties with a specific code, the user can see records of BO Standard order when any of the properties linked to the standard order match the filter on properties.

## Reference links

A reference authorization link (or, shorter: *reference link*) is used to link two business objects thereby allowing the user to only view those records of the business object for which the reference link was created.

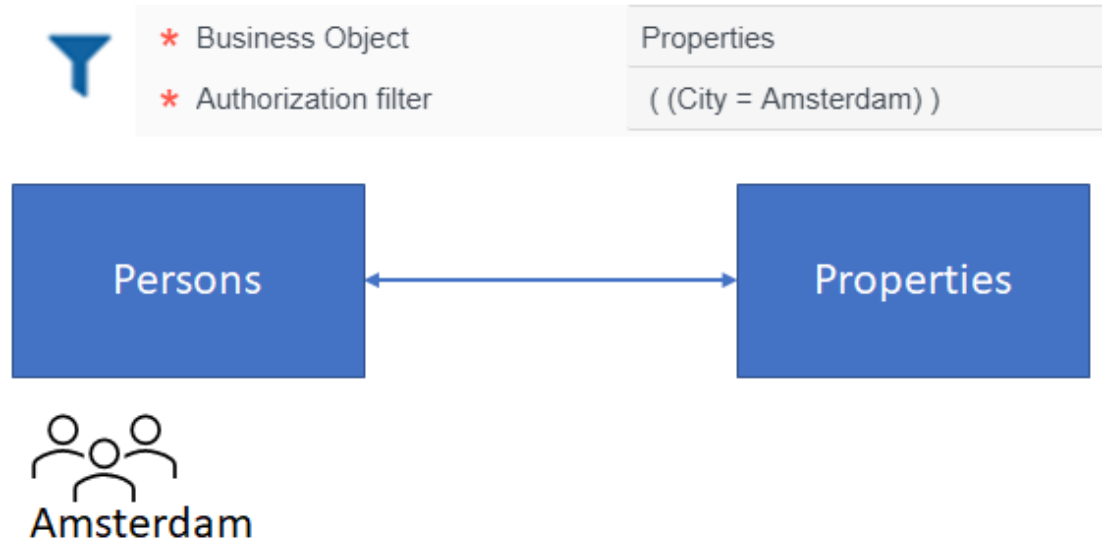
When a user creates a reference link on a business object, the authorization filter of the linked business object (the latter business object in the link) affects the record set of the business object on which the reference link is created.

An authorization filter determines whether a user should be able to see, modify and execute actions for a certain business object, based on its properties. A reference link however, is always created on the **Read** action of the business object.



For more information on creating authorization filters, see [Creating authorization filters](#).

When two business objects are linked, the second business object appears as a reference field on the first. For example, by using reference links, the user can see persons linked to only those properties/building which the user is authorized to see:



You can create reference links only for configurable base business objects. In addition, reference links can also be used for free integer reference fields, but not for free string fields.



Reference links can be defined only for base business objects on which the authorization filter is set on the **Read** action.



- A reference link created on the base business object also gets implicitly applied to its subs.
- Adding, deleting, updating authorization links is subject to security logging. For more information about this topic, see [Security logging](#).
- When you combine a reference link and an authorization filter, your result set may include records for which the value you are filtering on is empty. This is intentionally done to show records that would otherwise never be shown (so you can correct it).

## Creating a reference link

### Procedure

1. Go to Authorization links > Business objects > Reference business objects.

2. Select the business object for which you want to create the reference link.



Reference links can also be applied on business objects for which **Is Authorized** is set to **No**.

3. Go to the Authorization links step.
4. On the action menu, click Add and select the business object that you want to reference.

In the **General** section, specify the information. For a description of these fields, refer to [Authorization link fields](#).

5. Click Save. The Link field displays the reference authorization link created between the two business objects, that is the link between the source business object and the target business object.



In **Authorization links**, the **Quick search** enables you to set a filter on the **Business object field definition**, **Is active (Y/N)**, and **System name** for filtering the business objects.



You cannot create circular references between business objects using authorization links. That is, if you have already created an authorization link between **Personnel** and **Property**, you cannot create another authorization link vice versa, that is between **Property** and **Personnel**.

It is also not possible to create self-referenced authorization links, for example: an authorization link from **Property** to **Property**.

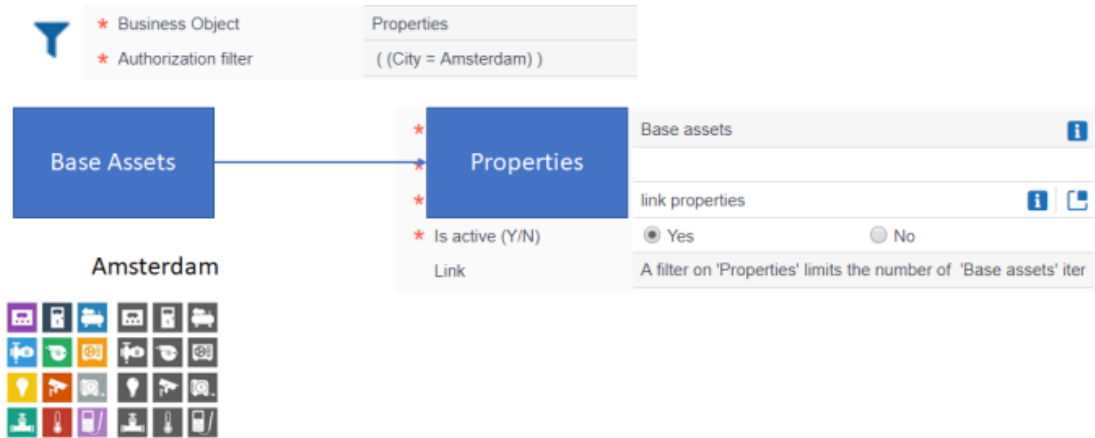
## Association links

When two business objects are linked using an m-to-n relation, the second business object (N, on which the Authorization filter is created) can be made available as an **Association link** to the first (M).

An **Association link** limits the results of the second business object. For example, by using an authorization Association link, you limit users to see only the simple and multiple assets of a property that they are authorized to see.

In M-to-N linked business objects, an association link can be created only from the business object that is on the M side to a business object on the N side. For example, considering Base assets and properties,

- You can create an association link from Base assets (M) to Properties (N) as assets can be filtered based on a filter on Properties.
- You cannot create an association link from Properties (N) to Base assets (M) because properties cannot be filtered based on a filter on assets.



**Association links** do not support multiple select free fields (MSFF) links. Association links are available for the following business objects:

- Activities
- Base assets
- Budget categories
- Customers
- Delivery addresses
- Distribution points
- Maintenance plans
- Parcel
- PPM profiles
- Properties
- Purchase organization
- Resource planner configurations
- Standard orders

## Creating an association link

### Prerequisite

Enable the **Split role and data** field in the **Authorization settings**.

### Procedure

1. Go to Authorization links > Business objects > Association links.
2. Select a business object for which you want to create an association link and click the Authorization links level.
3. On the action panel, click Add.

4. Complete the fields in the data section. For a description of these fields, refer to Association link fields.
5. Click Save.

**An association link is created for the selected business object. The Link field displays the association link created between the two business objects.**

## Dos and don'ts of authorization links

Authorization links can give rise to intensive database queries when the data is retrieved. Therefore, the following guidelines are recommended to avoid any performance issues when authorization links are used:

### **Filtering on a non-indexed field**

Authorization links created between business objects with non-indexed fields, involved in the query, may have a performance penalty. In the Planon Software Suite, mostly all fields in relations (table) starting with FK\_ are indexed. The code field is also indexed mandatorily. For example, the field **Unit of length** in the business object **Spaces**, with the table name FK\_PLC\_MEASUREMENT\_SYSTEM.

### **Enabling filtering on a BO that is defined on a view**

All relation (table) variables which start with PLN\_VW\_ are views in a database schema. An authorization link querying on a view created for relations with a complex relationship can have a performance penalty. For example, creating an authorization link on BaseMaintenanceActivityDefinition to BaseAssetRef. This link queries on the PLN\_VW\_ASSET.

### **Making a user available in multiple user groups**

An authorization link may result in a complex query, if a user is in multiple user groups. This can cause a performance penalty.

### **Making a long authorization link**

If an authorization link is created on a business object, which in turn is a part of an authorization link of another business object and likewise, this may result in a slower performance.

# Users

The navigation group **Users** that is available in **Accounts** is a configuration of the **Account** web definition.

The screenshot displays the 'Users' management interface. On the left, there is a search bar with the text 'User name' and a 'Search' button. Below the search bar are buttons for '+ Add user' and 'Show inactive user acco...'. A table lists users with columns for 'User name', 'Person', 'Department', and 'User account groups'. The first user, 'ADAMS', is highlighted. On the right, a detailed view for 'ADAMS' is shown, including fields for 'User name', 'Start date', 'End date', 'Time zone', 'User account groups', 'Comment', and 'Personnel data'.

User name	Person	Department	User account groups
ADAMS	047 Harry Adams	ICT	Accelerator Asset & Maintenance Mgt solution, Accelerator Integrated Services Mgt solution, Platon Solutio... Rundis, Accelerator Real Estate Mgt solution, Requestor, Accelerator Sustainability Mgt solution, Accelerator ... Space & Workplace Mgt solution
AMM			Accelerator Asset & Maintenance Mgt solution, AMM-solution
BALLEY	138 Sunny Ballely	Facility Management	Accelerator Integrated Services Mgt solution, ISM - Trade person soft services
BYERS	051 Bob Byers	Procurement	Accelerator Asset & Maintenance Mgt solution, Buyer
CAMBON	085 Virginia Cameron	Corporate Real Estate	Accelerator Real Estate Mgt solution, REM - Real estate manager
CLARKE	011 Lucas Clarke	Corporate Operational Audit	Lease accounting - Contractor, Accelerator Real Estate Mgt solution
COYTING	278 Conline		Accelerator Asset & Maintenance Mgt solution, Contractor
ECCLESTONE	470 Mitch Ecclestone		Accelerator Asset & Maintenance Mgt solution, AMM - Maintenance engineer
EDWARDS	082 Tina Edwards	Corporate Real Estate	Accelerator Real Estate Mgt solution, REM - Portfolio manager
EMERSON	020 Matt Emerson	Maintenance Management	Accelerator Asset & Maintenance Mgt solution, AMM - Maintenance engineer
EVANS	110 Terry Evans	Facility Management	Accelerator Integrated Services Mgt solution, ISM - Service management specialist

The information displayed and the actions available here, are all configured in the **Account** web definition.

# Field descriptions

## Access key fields

---


Field	Description
User	Enter the user for whom you want to generate an access key.
End date-time	Enter an expiry date-time for the access key.  After this date people will no longer be able to log in with this key.
Access key	This field will contain the access key that is generated when clicking <b>Save</b> . You can copy and paste this key.
Access key valid?	Indicates whether key is still valid with the current environment's encrypted master key. If this field is <b>No</b> , access via this key will be denied.
Description	Here you can enter additional information, such as the reason for generating the access key, the user whom you shared the access key with, etc..
Name	Enter a meaningful name that helps identify this access key.

---

## Association link fields

---

Fields	Description
Business object definition	The selected business object (N) is automatically filled in.
System name	Specify a system name.
Link 'Association' definition	Select a business object definition to which the selected business object will be an association link.

Fields	Description
Is active (Y/N)	According to M-to-N relation, select the M business object for the selected N business object.  Click <b>Yes</b> to enable the link. By default, the field is set to <b>No</b> .
	<div style="border: 1px solid #0070C0; padding: 5px;">  To activate the association link, the <b>Split role and data</b> field must be set to <b>Yes</b> in the <b>Authorization settings</b>.         </div>
Link	The <b>Link</b> field displays the association link created between the two business objects. This is a read-only field.


## Authorization link fields

Field	Description
System name	Specify a system name.
Business object field definition	<p>Select a referenced business object for which an authorization filter is created with a link to <b>Read</b> action. The selection pop-up displays all reference fields on the business object which you selected on the first level.</p> <p>For example, select the <b>Properties</b> business object that has an authorization filter applied on it with a link to the <b>Read</b> action set in <b>Authorization &gt; Filters &gt; Action filters</b> step.</p> <p>Only the reference fields of type <i>Integer</i> are supported in authorization links. The reference fields of type <i>String</i> and <i>Free string</i> are not supported.</p>
Is active Y/N	Click <b>Yes</b> to enable the link.

## BO Rights fields

Field	Description
Name	Displays the name of the selected business object.
Function profile	Displays the name of the function profile for which you are specifying permissions.
Business object definition	Displays the system name of the user-defined business object for which you are specifying permissions.



Field	Description
Permission type	<p>Displays the default permission type assigned to the function profile.</p> <p>Per authorized business object you can change the value to one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Invisible</b></li> </ul> <p>Select this option if you do not want to make the business object available for the selected function profile.</p> <ul style="list-style-type: none"> <li>• <b>Read only</b></li> </ul> <p>Select this option if you want to make the business object available in read-only mode for the selected function profile.</p> <ul style="list-style-type: none"> <li>• <b>Specific</b></li> </ul> <p>Select this option if you want to make specific settings for:</p> <ul style="list-style-type: none"> <li>• Fields</li> <li>• Actions</li> <li>• Status transitions</li> <li>• Extended actions</li> </ul> <p>If you select <b>Specific</b>, a message will be displayed prompting you to indicate whether the initial permission should be <b>Read only</b>.</p> <p>If you click <b>Yes</b>, the permissions for fields, actions, status transitions and extended actions will initially be read only. You can change these settings on the <b>Details</b> level as required. (See <a href="#">Specifying permissions</a>).</p> <p>If you click <b>No</b>, the details will not be accessible.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Changing a business object's permission type is subject to security logging. For more information about this topic, see <a href="#">Security logging</a> in the WebHelp.</p> </div>

## Details fields

### Fields

Field	Description
Right	Displays the business object for which you are specifying permissions.

---

Field	Description
Field	Displays the name of the field selected.
Permissions	<p>Select the specific permission type that you want to apply to the selected field. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>No edit allowed</b> (default value)</li> </ul> <p>Renders the field as read only.</p> <ul style="list-style-type: none"> <li>• <b>Edit allowed</b></li> </ul> <p>Renders the field as modifiable.</p> <ul style="list-style-type: none"> <li>• <b>Edit and transfer allowed</b></li> </ul> <p>Renders the field as modifiable. You can save the business object once with a value in this field that is not within your authorization filter, thus allowing you to change the value once. For example, for changing the owner of a problem.</p> <p>Adding, deleting and updating field permissions is subject to security logging. For more information about this topic, see <a href="#">Security logging</a> in the WebHelp.</p>

---

#### Actions

---

Field	Description
Right	Displays the business object for which you are specifying permissions.
Action	<p>Displays the selected action.</p> <p>In <a href="#">Linking actions</a> you have previously determined which actions are available in the elements list.</p>

---

#### Status transitions

---



Field	Description
Right	Displays the business object for which you are specifying permissions.
Action	<p>Displays the selected action.</p> <p>In <a href="#">Linking status transitions</a> you have previously determined which actions are available in the elements list.</p>

---

#### Extended actions

Field	Description
Right	Displays the business object for which you are specifying permissions.
User extension - client	Displays the selected action. In <a href="#">Linking extended actions</a> you have previously determined which extended actions are available in the elements list.

## Function profile fields

Field	Description
System name	Enter a name for the function profile.
Description	Enter a description of the function profile.
Default permission type	<p>Select the permission type that will be used for all business objects when a new function profile is created or when a business object is set to <b>Authorized</b>.</p> <ul style="list-style-type: none"> <li>• <b>Invisible</b></li> <li>• <b>Read only</b></li> <li>• <b>Full functionality</b></li> </ul> <p>This setting only affects newly authorized business objects. If you set a business object to <b>Authorized</b> in <b>Field definer</b> or if you add a field to a business object, the permission type specified here will automatically be applied.</p> <div style="border: 1px solid #0070C0; padding: 5px;"> <p> Example - The function profile for a Planon administrator should have the value Full functionality, so that each authorized business object is automatically added to the administrator function profile with full functionality. For a function profile requiring read only properties, the default value should be <b>Read only</b>.</p> <p> You can later still fine-tune the specific authorization per business object. (See <a href="#">BO Rights</a>).</p> </div>

## Key pair fields

Field	Description
Generated?	Indicates whether a key pair has been generated.
Access key valid?	Indicates whether key is still valid with the current environment's encrypted master key. If this field is <b>No</b> , access via this key will be denied.
Generated on	Displays the date and time of generating the key pair.

## Product definition fields

Fields	Description
Product	Displays the (short name of the) product.
Description	Displays the description of the product.
Transferred to archive?	Indicates whether the product is archived.
Accounts	Specifies the number of accounts linked to the selected product definition.
Number of licenses	The number of available licenses (in total) for this product definition.
Unlimited named license	Indicates whether the product definition is linked to an unlimited named license.
User group detail	Displays the user groups that have been linked to the license.
Threshold	<p>Allows you to specify a percentage based threshold.</p> <p>When setting a threshold and the number of users vs the number of licenses becomes greater than the allowed threshold percentage, the <b>Threshold reached?</b> field will be set to <b>Yes</b>.</p>



Fields	Description
Threshold reached?	<p>Conversely, when the number of users vs number of licenses becomes less than the threshold percentage, the <b>Threshold reached?</b> field will be set to <b>No</b>.</p> <p>Indicates whether the percentage based threshold is reached (<b>Yes</b>) or not (<b>No</b>).</p> <p>It is possible to create an alert on the status of this field. This will allow system administrators to be updated when the threshold is reached so steps can be taken to obtain more licenses or change the configuration where needed.</p>

## Solution license fields

Fields	Description
Code	The code of the license.
Name	The license name.
Users	The number of users linked to the license.
Number of licenses	The number of available licenses (in total) for this license.
User group detail	Displays the user groups that have been linked to the license.
Threshold	<p>Allows you to specify a percentage based threshold.</p> <p>When setting a threshold and the number of users vs the number of licenses becomes greater than the allowed threshold percentage, the <b>Threshold reached?</b> field will be set to <b>Yes</b>.</p> <p>Conversely, when the number of users vs number of licenses becomes less than the threshold percentage, the <b>Threshold reached?</b> field will be set to <b>No</b>.</p>

Fields	Description
Threshold reached?	<p>Indicates whether the percentage based threshold is reached (<b>Yes</b>) or not (<b>No</b>).</p> <p>It is possible to create an alert on the status of this field. This will allow system administrators to be updated when the threshold is reached so steps can be taken to obtain more licenses or change the configuration where needed.</p>

## User fields

Fields	Users selection step
User name	Specify a user name.
Description	Enter a relevant description of the user.
Start date	Specify the date when the user is allowed to log on. If end users try to log on to the system on an earlier date, they will receive a message stating that their account is not yet active.
End date	Specify the date when the user is no longer allowed to log on.
	<div style="border: 1px solid red; padding: 5px;"> <p> Users are no longer allowed to log in from the end date onwards.</p> </div> <div style="border: 1px solid blue; padding: 5px; margin-top: 5px;"> <p> To ensure that you are not locked out accidentally, users are not allowed to set an end date for themselves.</p> </div>
Previous log on date-time	Displays the last log on date-time (in UTC time).
Previous log on date-time (user)	Displays the last log on date-time in the time zone of the user account (the logged in user).
Password	This field is only displayed if you add a new user. Specify a password for this user. You can change the password using the <b>Change password</b> option on the action panel.
Password expiry date	Specify a password expiry date. On this date, the user password will expire.


---


## Fields

## Users selection step

Password never expires

If you select **Yes**, the **Password expiry date** field is grayed out and the user password will never expire.

 If the **Password never expires** field is set to **No**, then the expiry date is set to the current date plus the number of days as defined in the password settings.

 For more information on [Password settings](#) (System settings).

No. of attempts forgotten password

This field will be automatically populated with a number whenever the user clicks **Forgot password?** on the login screen. The maximum number of attempts is 3, after which the user account will be locked and you have to reset this field. For more information on resetting forgotten password, see [Clearing forgotten password attempts](#).

Department

Select the department to which the user is linked.

Telephone

Enter the user's telephone number.

Photo


Allows you to display a photo of the user.

Address

Select the user's address from the list.

Property set

This is a mandatory field.  
Select a default property set in which the selected user is allowed to work.

 By default, a user group has all rights in all property sets. By means of an authorization filter on the **Property set** business object, you can restrict the number of property sets and the corresponding rights of a user group.

Time zone



This field is not visible by default. If the use of multiple time zones has been activated in user's system, this field is mandatory. You can use this field to link a relevant time zone to a user.

Person details


Displays the details of the persons linked through the **Persons** link. It displays details like: code, first name, full name, department code, phone number and email.



Fields	Users selection step
User group details	Displays the details of the user groups linked through the <b>User Groups</b> link. It displays details such as system name, description and the user's permission type.
Product definition details	Displays the product definitions that are linked to the user's user group.

## User settings - fields

Fields	Description
<b>General</b>	
User	Displays the name of the selected user.
Translator	<p>Select <b>Yes</b> to set the user as a translator.</p> <p>As translator the user is allowed to overwrite custom (user-defined) translations.</p> <p>User-defined translations get status '2' in the application.</p> <p>Typically, when importing a new language file, user-defined translations remain unaffected. However, when importing a language file as 'translator', the user-defined fields are overwritten by the translations in the language file.</p>
Language	<p>Select a language for the user.</p> <div data-bbox="602 1325 1317 1514" style="border: 1px solid #00a0e3; padding: 5px;"> <p> When you do not specify a language for a user, the application does not know which language to display when the user logs on. In the application it is specified that when this occurs, the first available language will be displayed.</p> </div>
Theme	<p>Select a theme for the user.</p> <div data-bbox="602 1577 1317 1734" style="border: 1px solid #00a0e3; padding: 5px;"> <p> To see the <b>Themes</b> field, you must first add it to the TSI. To allow users to change their theme themselves, see <a href="#">Web Configuration &gt; Allowing users to choose a theme</a></p> </div> <p>The following themes are available in Planon:</p> <ul style="list-style-type: none"> <li>• Classic</li> </ul>



Fields	Description
	<ul style="list-style-type: none"> <li>• Planon light: a default light theme (background is mostly bright, fonts are mostly black)</li> <li>• Planon dark: a default dark theme (background is mostly dark, fonts are mostly white)</li> <li>• High contrast: provides the best possible contrast for visually impaired people.</li> <li>• Custom light: customized light theme based on the primary and secondary colors selected in System Settings &gt; Themes.</li> <li>• Custom dark: customized dark theme based on the primary and secondary colors selected in System Settings &gt; Themes.</li> </ul>
	<div style="border: 1px solid black; padding: 5px;">  The <b>Custom light</b> and <b>Custom dark</b> themes are displayed only if the <b>Custom theme activated?</b> field is set to <b>Yes</b>.         </div>
Use 24-hour notation	Select <b>Yes</b> to set the 24 - hour clock in the user's application.
Displayed unit of length	Select a unit of length. The available options are <i>meters</i> and <i>feet</i> .
Reply email address	Select an email address for email correspondence. You can only select a single email address.
Sender's email address	Select an email address from the list to be added as a sender's email address.
Contact's email address	Select or add an email address that must be used as the user's Exchange email address. This field is used by the Connect for Outlook feature in order to link the Outlook user to a user account in Planon.
Bcc email address	Select an email address to be added as a Bcc email address.
Field name size (in pixels)	Specify the field name size. By default, a field name size of 200 pixels is specified.
Show labels of toolbar buttons	Select <b>Yes</b> to display the labels of toolbar buttons.

Fields	Description
Autoselect first item in list?	Select <b>Yes</b> to automatically highlight and select the first item in the elements list.
Anonymized?	This field indicates if the user's data have been anonymized. Anonymization is related to the <b>General Data Protection Regulation (GDPR)</b> functionality in Planon.  <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  For more information, see <a href="#">GDPR</a>. </div>
Alternative e-mail addresses for Exchange	Displays the alternative e-mail addresses linked to the user.  <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">  For more information on adding alternative e-mail address, see <a href="#">Linking alternative e-mail addresses</a>. </div>
Keep session alive?	Set this field to <b>Yes</b> if you want to keep the application open to its user. The user in question will not be logged out of the application and will be able to continue work even if the general setting on <a href="#">Keeping sessions alive</a> is switched off.  If it is set to <b>No</b> , the application will <i>behave</i> according to the <a href="#">Web application settings</a> in System Settings.
Enable additional accessibility support?	When enabled ( <b>Yes</b> ) this field will add tab focus and tab index to disabled buttons in the Web client.  These will allow for easier navigation of the web client for visually impaired users (for example by using screen reading software).  When the setting is disabled ( <b>No</b> ), the regular power user focus behavior will apply.  Note that this setting requires a log out/log in to apply changes.
Show menu when hovering over level	When enabled ( <b>Yes</b> ), this field ensures that the steps under a level are displayed when hovering over a level.  If you add this field to the <b>My Account</b> definition, users can determine this setting for themselves.
<b>Planon AppSuite</b>	
Block AppSuite user & retract all data from device?	Use this field to block an engineer's access to AppSuite and retract all data from the mobile device. The data is sent to the back-office. Jobs will later be reassigned to the field engineer. This setting is

---

Fields	Description
<b>PMFS Live app - Work assignments</b>	useful for re-installing the app without losing the data on the device or when switching between MDM tools.
Enable work assignment 'envelopes'?	Select <b>Yes</b> in this field to enable the 'mobile envelopes' functionality for the selected user. This setting will then be applied to send work assignments to the PMFS Live app . Enabling the 'mobile envelopes' functionality automatically means that work assignments are no longer sent to <b>Planon AppSuite</b> , for the selected user(s). By default, this field is set to <b>No</b> .

---

# Index

## A

- Access key fields 55
- Access key valid? 59
- Access keys: configuration 18
- Access keys: generating 19
- Access keys: introduction 16
- Access to Planon products 20
- Accounts
  - Association link fields 55
  - Authorization link fields 56
  - BO Rights fields 56
  - Details level fields 57
  - Field descriptions 55
  - Function profile fields 59
  - Introduction 7
  - User fields 62
- Action authorization filter 43
- Action authorization filter: create 42
- Action filter: create 41
- Actions: link to business objects 32
- Alternative e-mail address
  - link 15
- Association - authorization link 52
- association link 49
- Association link 52
- Association links 51
- Authorization Association link 51
- Authorization filter
  - combine filters 43
  - link to user group 43
- Authorization filter: create 40
- Authorization filters 38
- Authorization levels 30, 32
- authorization link 49
- Authorization link 50
- Authorization links 49
- Authorization links: dos and don'ts 53
- Authorization report: BO Rights 37
- Authorization: activate 40
- Authorization: data access 46
- Authorization: functional access 46

- Authorization: set user start and end date 11
- Authorization: system reports 46

## B

- Business object permissions: specify 31

## C

- clients 17

## D

- Data access and functional access
  - separate 46
  - split role & data 46
- Data access and functional access:
  - separate 46

## E

- Extended actions: link to business objects 33

## F

- Fields: link to business objects 31
- Forgotten password: clearing attempts 14
- Function profile 30
  - link to user group 8
- Function profile: create 30
- Function profile: include actions 30
- Function profile: include fields 30
- Function profile: include status transitions 30
- Function profiles 38
- Function profiles: transfer to other BOs 34

## H

- Hardware requirements 17
- How product definitions work 22

## K

- Key pair
  - generate 19
- Key pair: fields 59
- Kiosk 17

## L

- License 17

**M**

M-to-N 49  
m-to-n relation 51

**N**

New passwordset  
  create 10  
New users: add 20

**P**

Password  
  email notification 12  
  reset 12  
  set 12  
Password settings 10  
Password: change 10  
Permissions: specify 34  
ProCenter filters 42  
Product definition  
  fields 60  
  unlinking scheduler 28  
product definition - user group 22  
Product definitions 20  
  Analytics 24  
  AppSuite 24  
  AWM 24  
  Connect for AutoCAD 24  
  Connect for Outlook 24  
  EventConnector 24  
  IDE 24  
  PSS2 24  
  Resource Planner 24  
  Scheduler/Alerts 24  
  Web Client 24  
  Web Services 24

**R**

Reference - authorization link 50  
Reference date 11  
Reference date active 11  
reference link 49  
Reference link 49  
Reset UUID 13

**S**

SDK 17

Security 17  
Security logging 31, 32, 33, 33  
Self-service 17  
Solution license 29  
  fields 61  
Solution license: definition 29  
Status transition: link to business  
objects 33

**U**

User 9  
User group 8  
  create 8  
  link authorization filter 43  
  link function profile 8  
user group - product definition 22  
User groups: link to products 21  
User screen settings: configure 15  
User screen settings: delete 16  
User screen settings: generalize 15  
User settings 10  
  fields 64  
User: add new user 10  
User: link to a person 14  
Users  
  Account  
    Web definition 54