Authorization

Planon Software Suite

Version: L105

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.

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

ℹ	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

Authorization

This section describes some concepts and instructions for implementing authorization.

For more information on applying authorization to user/user groups as well as more generic descriptions regarding authorization principles, see Accounts.

Authorization concepts

To understand authorization in Planon Software Suite, it is important to understand the various concepts involved. This section discusses the following concepts and explains how they are connected:

- Access key
- Authorization filter
- Business object
- Constraint
- Foreign key
- Function profile
- Key pair
- Navigation groups
- Property set
- TSI
- User
- User group

Access key

An access key is an encrypted URL for an account that can be used to grant access to Planon functionality. Access keys are intended to enable multiple logins of the same account to limited functionality.

Authorization filter

An authorization filter is used to specify the data a user group is authorized to view and perform actions on. The same authorization filter can be used by several user groups.

For example: the Security, Catering and Service Desk user groups for Region North of a building complex are to access the same data and will therefore have the same authorization filter linked to them.

Business object

A business object (BO in short) is a logical unit of functionality and data that refers to a facility management concept, For example, work order, request, budget type, etc.

In Planon, there are two type of BOs, **system BO** and **user-defined BO (UDBO**). A system BO offers standard sets of fields and statuses to work with. An UDBO on the other hand, is highly customizable. You can create your own fields, actions, statuses and status transitions. Still, a UDBO is always based on a system BO. For example, you can create the user-defined business objects **Customer** and **Supplier**, based on the **Personnel** business object.

BOs are managed in **Field definer**. The system BOs and UDBOs are distinguished here. Each BO or UDBO has its own set of fields and statuses. Fields contain data. For a BO, you can create any number of UDBOs.

You can authorize a business object to restrict users from using the BO. Authorizing a BO provides a means to determine if or in what way users can access data (no access, read access, read-write access) and what actions can be performed .

❗ By default, business objects are not authorized. This means that all users have full access to these business objects: all fields are accessible and all actions can be performed.

Constraint

Constraints are used to limit the type of data that can go into a database table. This ensures the accuracy and reliability of the data in a table.

Common constraints:

Constraint	Value
UNIQUE	Ensures that all values in a column are unique.
FOREIGN KEY	Uniquely identifies a row/record in another table.
CHECK	Ensures that all values in a column satisfy a specific condition.

Foreign key

A field in a relational database table that links two records together and which is used to reference the unique key in another table.

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.

Key pair

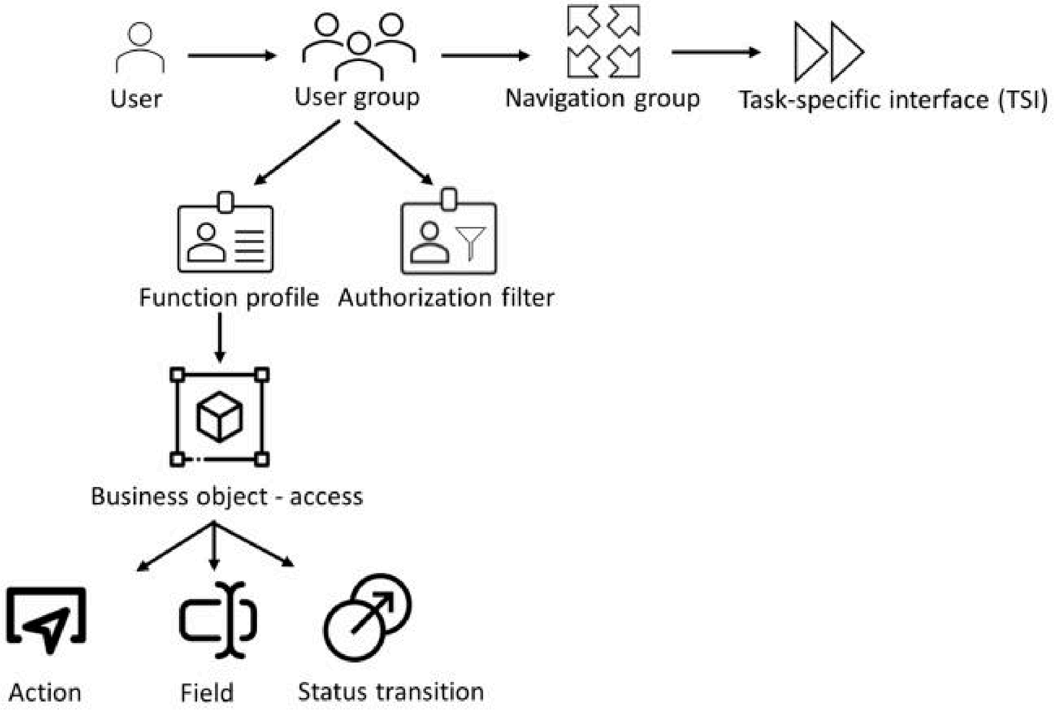
A key pair consists of a private key and a public key. These keys are used for decryption/encryption of the access key.

Navigation groups

Navigation groups in the Navigation Panel are used to make TSIs available per user group. In other words: navigation groups are needed to make TSIs available to users.

You can link a navigation group to several user groups.

The following diagram displays the link between the concepts described in this section.



See also:

- Navigation panel

Property set

A property set is a set of data comprising specific properties (buildings). Depending on the authorizations of their user group, users can work in or view one or multiple property sets. Property sets are authorizable business objects, which means you can authorize users groups to access one or more property sets and perform certain actions.

TSI

A TSI (Task Specific Interface) contains selection levels and selection steps with several (predefined) business objects. A TSI offers various user groups with the required functionality to perform specific tasks and activities.

A selection level displays a BO's elements list. A selection level includes multiple layouts that determine how a BO or UDBO is presented to the end user. Each layout determines how fields, tabs, actions and status transitions are displayed. For the end users, TSIs are available in the **Navigation panel**.

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.

> ℹ 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

> ℹ 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.

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

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.

Configuring Authorization

This section provides you with information on how to proceed when configuring authorization for the various user groups in your organization. The Basic authorization part describes the standard configuration procedure. In the Advanced Authorization part the use of authorization filters (optional) is explained. In addition, this section describes how to authorize pick lists and the use of standard orders.

> We recommend reading the Scenarios section at the end of this manual before you actually begin authorizing, since this section provides important information on the consequences of various authorization configurations.

> Exporting/Importing of user groups and function profiles, authorization filters, and authorization links is coveredy by **Configuration Transfer**. Please refer to *Configuration Transfer* for more information.

Basic authorization

Basic authorization involves:

- Activating authorization
- Authorizing business objects

The following sections provide more detailed information on these steps.

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).

Authorizing business objects

By default, authorization is disabled for business objects. This means that all users can read all fields of a business object and that they can perform all actions. If authorization is enabled for a business object, it has read-only access by default for all users; the rights for fields, actions, status transitions and extended actions can be restricted or extended per user group.

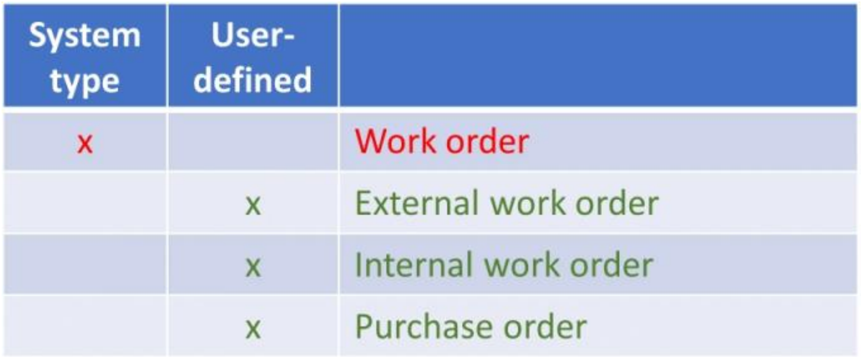
- We recommend authorizing business objects only if there is a business requirement. Minimal authorization makes maintenance easier and performance better.
- For more information on how to set rights for fields, actions, status transitions and extended actions, refer to BO Rights (Accounts).

To enable authorization for business objects

Procedure

1. Go to **Field definer** > **Business objects**.
2. Select the business object for which you want to enable authorization.

For the user-defined subtypes of the **Orders** business object, authorization has to be enabled. For system order types, authorization cannot be enabled! (Refer to the following figure).



System type	User-defined	
x		Work order
	x	External work order
	x	Internal work order
	x	Purchase order

See also Creating user-defined business objects (Field definer).

3. On the action panel, click Under construction.
4. In the data panel, set the Is Authorized option to Yes and click Save.
5. On the action panel, click Completed.

Authorization has now been enabled for this business object.

Please pay attention to the following:

- If an authorized business object is set to **Not authorized**, the rights for this business object will be removed from the existing function profiles!
- If an authorized user-defined business object is set to *Under construction* in Field definer , the business object will be removed from the list of business objects in the Function profiles launch item as soon as the list is refreshed. However, if the **Refresh list** button is not clicked, the object will remain in the list. Subsequently selecting the business object and then attempting to add fields to it can then cause an error.

Authorizing the use of standard orders

There are many reasons for applying authorization to standard orders. The following example merely serves as an example of this functionality.

The Planon administrator in Company X has added users to a 'Front Desk' user group, who will only be allowed to add requests. They are denied the right to add work orders. To prevent these users from adding work orders, the Planon administrator has excluded the **Add** action from the **Work Orders** business object in the 'Front Desk' function profile. However, this action alone does not suffice. Users from the ‘Front Desk’ user group will still be able to circumvent authorization by using standard orders in the **Work Orders** TSI. By selecting the **Add standard** option from the action menu, they can open the **Standard order** dialog box and select any type of standard order, including standard work orders.

For more information on adding orders that are based on a standard order, refer to *Work Orders* .

Additional authorization is therefore required to prevent users from the 'Front desk' user group to add a work order that is based on a standard order.

You need to take the following measures:

1. In **Field definer** , make sure the Is Authorized option for the Standard work orders business object is set to Yes.
2. In the Authorization > Function Profiles launch item, select the relevant function profile and remove the Standard work order business object’s Read action from the function profile. You can do this by moving the Read action from the In use list to the Available list in the Actions dialog box.

   For detailed information on configuring authorization, refer to Configuring Authorization.

   After you have made the above settings, users from the 'Front Desk' user group will no longer be able to view nor select standard orders in the **Standard order** dialog box. The **Standard order** dialog box will only show standard requests.

Authorizing the configuration and use of pick lists

Authorization for pick lists takes place on two levels, since both the configuration and the use of pick lists can be subjected to authorization.

Moreover, there are two types of pick lists whose configuration and use can be authorized:

- Pick list (descriptive)

- Pick list (code-descriptive)

To facilitate two types of authorization for two types of pick lists, multiple pick list related business objects are available. Depending on your authorization requirements, you have to enable authorization for one or more pick list related business objects in the **Field definer** launch group.

For more information on enabling authorization for the business objects that are involved in the configuration of pick lists, refer to Authorizing pick list configuration. For more information on enabling authorization for the business objects that are involved in the use of pick lists, refer to Authorizing end users to use configured pick lists.

Enabling authorization for a business object is step 2 in the Basic Authorization process. For general information on the complete authorization process, refer to Basic authorization.

Authorizing pick list configuration

You can authorize user groups to configure pick lists. To bring this about, you have to enable authorization for the following business objects in the **Field definer** launch group > **Field definer** launch item. Note that authorization on pick list configuration has to be enabled separately for the pick list dialog boxes and for the pick list items.

Enabling authorization for pick lists

Enabling authorization for pick list items

Enabling authorization for pick lists

1. In **Field definer** , put the Pick lists business object under construction.
2. Enable the option Is authorized for the relevant sub-business object in the data section: Pick lists (code-descriptive) and/ or Pick lists (descriptive).

   You have now enabled authorization for the dialog boxes that contain configured pick lists.
3. Select the Completed option in the action menu and click Save.

Enabling authorization for pick list items

1. In **Field definer** , put the Pick list items (descriptive) and/or the Pick list items (code, descriptive) business object under construction.
2. Enable the option Is authorized for the relevant business object in the data section.

   You have now enabled authorization on the items included in the configured pick lists.
3. Select the Completed option in the action menu and click Save.

This is step 2 in the Basic Authorization process. For general information on the complete authorization process, refer to Basic authorization.

Note that if you want to authorize the configuration of **Pick lists (code/ descriptive)**, you also have to authorize the configuration of the **Pick list items (code-descriptive)**. The same applies to **Pick lists (descriptive)** and **Pick list items (descriptive)**.

A person with an authorization to configure pick lists of one or both types, is allowed to configure pick lists in the **Supporting data** launch group > **Pick lists** launch item.

For more information on configuring pick lists in the **Supporting data** launch group, refer to Supporting data documentation.

Configured pick lists of either type (descriptive, or code-descriptive) can be linked to free fields in the **Field definer** launch item.

For more information on linking pick lists to free fields in the **Field definer** launch group, refer to Field definer documentation.

Finally, you can authorize end users to use all or some of the items in these pick lists. For more information on authorizing the use of pick lists, refer to Authorizing end users to use configured pick lists.

Enabling authorization for configured pick lists

Enabling authorization for configured pick lists

1. In the **Field definer** launch group, put the Configured pick lists (descriptive) and/or Configured pick lists (code, descriptive) business object under construction.
2. Enable the option Is authorized for the relevant business object in the data section.
3. Select the Completed option in the action menu and click Save.

This is step 2 in the Basic Authorization process. For general information on the complete authorization process, refer to Basic authorization .

An end user who is authorized to use certain pick lists, can select items from these pick lists in a data field.

Authorizing end users to use configured pick lists

Once you have configured pick lists in **Supporting data** and linked them to a field in **Field definer** , you can authorize the use of these pick lists. In other words, you can make them available to specific user groups. To bring this about, you have to enable authorization for the **Configured pick lists** business objects in **Field definer** .

Advanced authorization

Advanced authorization involves:

- Creating authorization filters
- Deciding whether to use TSIs or TSIs with Authorization

The following topics describe more advanced authorization options.

Using TSI authorization

When you are configuring Planon Software Suite, it is not always necessary to use Authorization. Consider the following example:

Within an organization, the following job roles can be distinguished:

- Security officers: are allowed to add visitors and modify visitor data.
- Service Desk staff: are allowed to view but not modify visitor data.
- Caterers: have no access to visitors at all.

In order to implement this structure, two possible configurations can be used:

- Using TSIs without authorization
- Using a TSI in combination with authorization

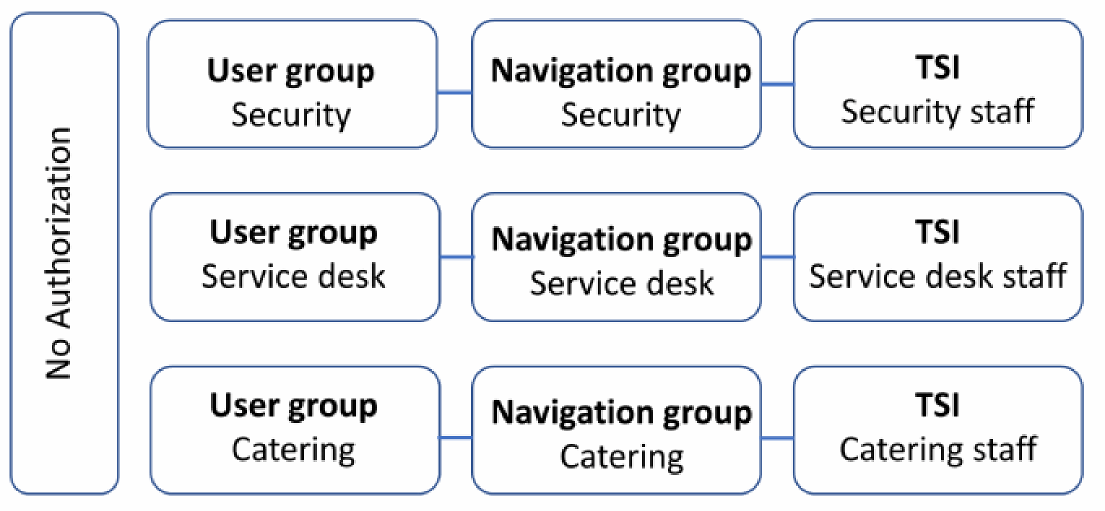
If the data in question includes critical or confidential information that should never be accessible to end users, then a TSI should be used in combination with authorization. If on the other hand, no such data is used, there is no need to use authorization and the solution would then simply involve several TSIs.

Using TSIs without authorization could enable users to access data fields they are not authorized to access using dialog boxes or reports. For an entirely secure solution, we strongly recommend using a TSI in combination with authorization.

Below, both configurations are represented graphically.

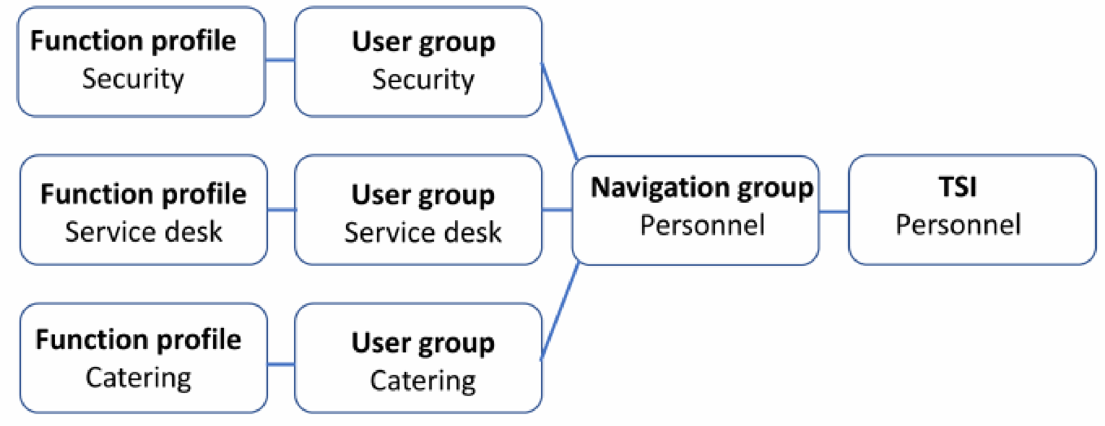
TSI

This involves defining three TSIs, based on **Personnel** :



TSI and authorization

This involves defining one TSI based on **Personnel** and three different function profiles:



See also:

- TSIs
- Navigation panel

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) is a European legislation that aims to protect EU citizens from privacy and data breaches in an increasingly data-driven world. Companies processing or storing personal data need to comply with the GDPR legislation.

The legislation is aimed at the following subjects:

- Breach notification
- Right to access
- Right to be forgotten
- Data portability
- Privacy by design
- Data protection officers

ℹ For more information, see .

To be GDPR-compliant, Planon provides companies/users with the possibility to:

- change personal data.
- limit access to personal data using authorization filters and function profiles.
- show their privacy policy in the user menu.
- Anonymize (automatically) personal data stored in Planon based on criteria specified in their privacy policy. For example, auto-anonymizing personal data of visitors after a month.
- Anonymize the entire database.

Anonymizing data

Following GDPR legislation, personal data referred to in the application must either be deleted or anonymized.

Planon features two anonymization actions that work differently. The process of anonymization can involve either scrambling data or purging data. This section describes the differences between these two actions:

- Anonymize
- Anonymize database action

Anonymize action

Planon features the anonymization action in the **Persons**, **External requestors**, **Addresses**, **Accounts** and **Visitors** business objects. Anonymizing a business object will scramble its data and the action is irreversible. All the references to this business object will stay intact but pressing the **i**-icon for the referenced anonymized business object will show the scrambled values.

Anonymizing is an irreversible and destructive action, which is important to understand before clicking the **Anonymize** action. A warning will appear and the user must explicitly click **Yes** to confirm the action.

The **Anonymize** action is available for the following business objects:

- Visitors
- Addresses
- Persons
- External requestors
- Accounts
- Contracting parties

What does the action do?

When clicking the **Anonymize** action, the record will (seem to) disappear from the user interface. Related personal data on related ordes will be scrambled.

In general, the following table shows the anonymized values per type of field after using the **Anonymize** action:

Type	Anonymized value
Text	*****
Number	0

Type	Anonymized value
Decimal	0,0
Date	1-1-1970
Date-time	1-1-1970 00:00:00

- Anonymizing accounts is subject to logging. For more information, see the Administrator's Guide.
- The **Anonymize** action is schedulable by using an action definition and a schedule in Alerts to automate the anonymization process.
- On the above business objects, you can apply the **Anonymize** action via **Action on selection**.

Anonymize database action

Following GDPR legislation, it is not allowed to have privacy related information available on non-production systems.

Anonymize database

For this reason, a generic **Anonymize database** action is available in **System Settings** > **Security** to scramble/purge the information for the above business objects.

The **Anonymize database** action is designed to anonymize data in non-production environments in one go. It is specifically designed to be used in either of the following situations:

- Shipping the database elsewhere to prevent sending potential sensitive and personal information to a third party, for example to Planon Support.
- Moving a production database to a non-production environment, where there is no need in having potential sensitive and personal information available. After anonymizing the database, default test data could be onboarded for use in test cases.

- By clicking the generic **Anonymize database**, all instances of the business objects mentioned earlier, except for Accounts will be anonymized.
- This functionality is available only for non-production environments.
- To start generic anonymization, the general setting **Stop end user access** must be enabled.

Database procedure

Instead of using the **Anonymize database** on a non-production environment, you can also anonymize the whole database by creating a backup of the production database and executing the following database procedure:

```
PLN_ANONYMIZE_ALL
```

What does the action do?

When using the **Anonymize database** action, the following actions will be carried out:

- All history is deleted.
- Fields that are part of database constraints ('check' or 'unique' constraints) are skipped and are not anonymized, the value remains as is. Examples of these are:
    - Visitor status: has a check constraint to make sure it contains a valid status.
    - The uniqueness constraint of fields, such as Code, within a property set for certain business objects.
- Date/Time fields get the value 1970-01-01 00:00:00.
- Number and Decimal fields are cleared when they are part of a foreign key and not mandatory.
- Number and Decimal fields are skipped when they are part of a foreign key and mandatory.
- Number and Decimal fields get the value 0 when they are not part of a foreign key.
- Text fields are cleared when they are not mandatory.
- Text fields get the value * when they are mandatory.

Accounts in database procedure

The database procedure allows the following accounts to remain usable so the database remains accesible:

- SUPERVISOR
- CLOUDADMIN
- AWMDATAENGINEADMIN
- EVENTCONNECTORADMIN

- EXCHANGEADMIN
- SCHEDULERENGINEADMIN

In addition, the accounts linked to the user group specified in the System settings > General > Planon administrator group field will also retain access.

Anonymize history

Following GDPR legislation, any personal data stored, even in history records, must be anonymized. In Planon, when a business object with personal information is updated, a history record is created containing this personal information. To comply with GDPR, a generic **Anonymize history** action is available in history-aware business objects that enable you to anonymize this history.

The **Anonymize history** action is available in the **Action on selection** menu on all the root business objects that have history, for example, **Orders** and **Contracts**. The action can be performed manually, but is also schedulable.

When the **Anonymize history** action is triggered, all person, address, external requestors, visitors (also external) and account fields in a business object for which history is enabled are hashed with a '*******' string.

Examples of business objects for which anonymization of history records is possible are shown below:

- Orders
- Contracts
- Assets
- Planned maintenance
- Questionnaire
- Spaces and moves scenario planning

Privacy statement

Planon features a **Help** menu in the top-right corner to provide access to customers to link their Privacy Policy statement. The menu lists the **Privacy statement** option which allows you to view the privacy statement of your company to comply with GDPR regulation.

GDPR mandates that the Privacy Policy statement must be easy to find. The law insists that the information provided to customers about how their personal data is processed must be concise, transparent, intelligible and easily accessible.

You can specify the privacy statement in System settings > General > Privacy Statement . If there is no privacy statement specified, the option will not be visible in the menu.

The Privacy Policy statement must document and describe the following items:

- For what purpose do you need to process personal data?

- Is the personal data shared with any other parties?
- How long will the information be retained?

  As per the rule, you can only process personal data as long as it is required for a specific purpose in which the personal data will be collected. For some specific type of information, such as employee illness/absence information, you must adhere to specific limits.
- How can users alter personal data that they have submitted?
- How can people revoke their consent and remove their personal data from your system?

No Web client

Typically, the Privacy statement can be published as a web content web definition or an external URL which can be linked in the **Privacy statement** field.

However, to make this functionality available to those who do not have access to the Web client, the configured Privacy statement will now also be available under the homepage in the user menu.

My account

The **My account** button in the Planon ribbon allows you to edit your personal data and account settings. In **My user account**, you can view your **User name**, **Password expiry date** and change your password with the **Change password** option.

> Planon application managers can add or remove fields in this window in the Web Configuration TSI. For more information, see Making My account settings for end users.

In **My account settings**, click the **Edit** button to change the following settings:

- **Use 24-hour notation**

  With this setting, you can toggle between the 24-hour clock notation and the 12-hour clock notation (with AM and PM). The 24-hour clock notation represents time continuously from 00:00 (midnight) to 23:59 (11:59 PM) without the use of AM or PM indicators, employing a 24-hour format to express the time of day. The 12-hour clock notation, along with AM (Ante Meridiem) and PM (Post Meridiem), divides the day into two 12-hour segments to denote time. The selected time notation is used throughout the application.
- **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.
- **Language**

  Select the language in which you want to display the application.
- **Displayed unit of length**

Select the unit of length you want to use in the application: meters or feet. The selected unit of length is used throughout the application.

- **Autoselect first item in list?**

  Select **Yes** to automatically highlight and select the first item in the elements list.

- **Theme**

  Select the theme you want to use: Planon light, Planon dark or High contrast.

> ℹ To view the changes, click the **Save and log off** button.

The name displayed in the **My Account** list is either derived from the account or the person linked to the account. This table shows the name that is displayed.

Account		Person		Displayed
User name	**Description**	**First name**	**Last name**	
WEASLY	Adam Weasly	Adam	Bilt	Adam Bilt
WEASLY	Adam Weasly	Adam		Adam
WEASLY	Adam Weasly		Bilt	Bilt
WEASLY	Adam Weasly			Adam Weasly
WEASLY		Adam	Bilt	Adam Bilt
WEASLY		Adam		Adam
WEASLY			Bilt	Bilt
WEASLY				WEASLY

The photo displayed on the **My Account** menu is determined based on this table.

Account - Photo	Person - Photo	Photo displayed in 'My Account'
Y	Y	Person-Photo
Y	N	Default image
N	Y	Person-Photo

Account - Photo	Person - Photo	Photo displayed in 'My Account'
N	N	Default image

If no photo is selected in the **Photo** field, a default image appears. This placeholder displays one or two characters. This example shows which characters might appear in the default image.

Account - User name	Person - First name	Person - Surname	Displayed
WEASLY	Adam	Bilt	AB
WEASLY	Adam		A
WEASLY		Bilt	B
WEASLY			W

If **First Name** and **Surname** do not contain any value, then it means the fields are empty (none of them are system mandatory) or no person is linked to the account.

Help menu

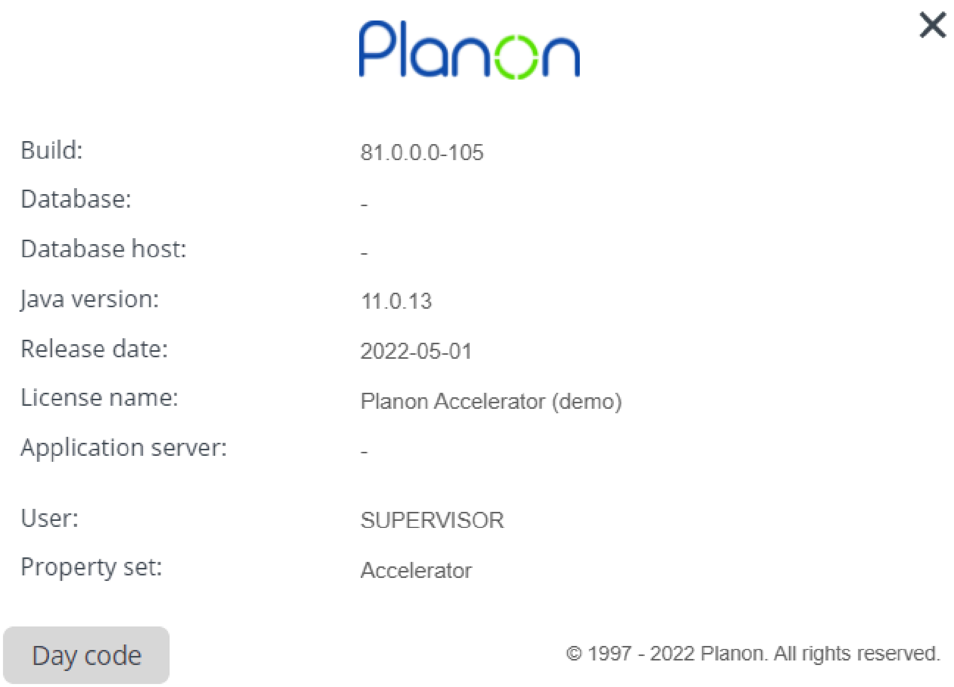
Planon features a **Help** button in the top-right corner that opens a menu providing access to information about the software and privacy statement of your company (GDPR legislation).

The options listed in the **Help** menu are:

- **TSI Help**: Enables you to view help information related to the TSI that is active on the screen. The option is visible only if a document/web page related URL is specified in TSI Help URL. If there is no URL specified, the option will not be visible in the menu.
- **WebHelp**: Enables a user to start and view the Planon WebHelp. The WebHelp is displayed in the language of the version of the WebHelp specified in the Help URL field (System settings).
- **Privacy statement**: Enables you to view the privacy statement of your company to be compliant with GDPR regulation. The privacy statement can be specified in **General settings** TSI > **Privacy Statement**. If there is no privacy statement specified, the option will not be visible in the menu. For more information about the Privacy Policy statement, see Privacy statement.
- **About**: Enables you to get information about the version of Planon you are using.

For information about the history of installed versions of Planon in your environment, see Creating a product version overview.

  - This information is important in the communication with Planon or to assess whether an update should be considered (based on the release date)



Build:	81.0.0.0-105
Database:	-
Database host:	-
Java version:	11.0.13
Release date:	2022-05-01
License name:	Planon Accelerator (demo)
Application server:	-
User:	SUPERVISOR
Property set:	Accelerator

© 1997 - 2022 Planon. All rights reserved.

- **Keyboard shortcuts**: Enables you to view the available keyboard shortcuts in Planon. For more keyboard shortcuts, refer to Shortcut keys (Fundamentals).

Authorization on the log-on date

When a user logs on, the system will verify the user's name and password. Additionally, the system will also check whether he or she is allowed to log on at this particular point in time, by checking the personal start date and end date. These dates are compared to the system date (of the server).

If a user's start date is later than the system date on which he or she tries to log on, the logging on process is stopped. The same principle applies to a situation where the user's end date is earlier than the system date on which he or she tries to log on.

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.

User Screen Settings

In your user screen, you can perform certain actions such as:

- resizing dialog boxes,
- selecting options in dialog boxes,
- opening a TSI
- and so on.

  The results of these actions are stored as user screen settings in the database and are specific for each user. As you log on, the last stored user screen settings are loaded into the application. This enables you to view data in a form that is convenient to you.

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.

Security

Data security involves balancing the protection of confidentiality, integrity and the availability of data while maintaining a focus on efficient policy implementation without hampering organization productivity. In Planon, you can use Authorization to bring about this balance by granting/restricting access to data. For the sake of traceability, changes to data-senstive areas is subject to logging.

Access to security-sensitive data

Some parts of the application deal with security-sensitive data. By being more security aware Planon has stepped up to its responsibility of providing customers the possibility to tighten data security.

Data security is beyond the scope of functional application management, the domain of the Planon application manager. Planon recommends to create a dedicated *system administrator* profile for someone who is in charge of system security and responsible for all changes that affect security (such as unauthorized access).

What kind of data/access are we talking about?

In general, this affects areas where you configure or can access:

- Technical configuration
- Sensitive information (folders, passwords, URLs, and more)

A system administrator should be assigned the responsibility of managing:

- ProCenter Modules
    - Web content
    - External content
    - Environment Management gadget
    - Cloud exo gadget
- System settings
    - Connect for Outlook
    - External data storage
    - File locations
    - General
    - Outgoing email
    - Reporting
    - Security

    - Trusted services
    - Web application
- System information
    - User sessions
    - User groups
    - Authorization
- Planon Live - Workplace engagement app
    - External links

These are areas to which only the system administrator and not the application manager should have access.

Configuring access to security-sensitive data

In Planon, data access can be maintained by creating two separate launch panels for user groups/function profiles. In addition to functional business objects, system business objects have also been made authorizable, which means that you can make them available/unavailable at will.

Authorization for system business objects is configured at the Authorization > Business objects level.

In contrast to Field definer , here, all business objects are displayed and not only those that are configurable. The system business objects that can be made authorizable display fewer details than those that are configurable and only the **Is authorized** field can be changed.

> When authorizing system business objects, be careful not to exclude yourself from accessing this funtionality. The system business objects are recognizable by their gray-colored icon.

Authorizing system business objects

Preparation:

- Create two separate user groups & function profiles, one for the application manager and one for the system administrator.
- The application manager has **Default permissions** as **Invisible** and the system administrator has **Full functionality**.

1. Go to Authorization > Business objects level and select a system business object that you want to make authorizable.
2. Set it Under construction and set Is authorized to Yes.
3. Set the business object back to Completed and log out/log in.

- The system administrator can still access and change data for the business object.

- The application manager cannot view or change data for the business object.

Security logging

To be able to monitor and safeguard the data integrity of your application, Planon has enabled security logging. This will help ensure that:

- Computer security records are stored in sufficient detail.
- Policy breaches can be monitored and appropriate action can be taken.

Logging of events is done in a file; its name and location is configurable. Logging can be switched on/off as required.

The following events are logged:

- Authentication changes
- (Failed) User actions
  - User login failed is logged
  - User login failed (locked) is logged
  - First time user login is logged
  - User login failed (inactive start / end date)
  - User account will be locked (multiple wrong logins, end date arrived, password expired)
- Password settings
- Logging in/out of Planon administrators
- Authorization changes

ℹ For more information of configuring security logging, see Security logging.

Scenarios

This section describes various scenarios that illustrate the consequences of using different authorization configurations.

In Authorization, you have configured, the following:

Situation 1: A user has the rights to modify the **Space** field, but is not authorized to view the **Property** field.

Situation 2: A user has rights to modify the **Space** field, and only authorized to view the **Property** field and not change it.

If the user modifies the Space field, the following will happen:

For situation 1: Planon will skip the **Property** field and not change it. Planon will not give an error message. When the user tries to save, an error message may be displayed.

For situation 2: Planon will change the **Property** field, even though the user is not authorized to change this field manually.

In Authorization, you have configured that a user is not authorized to view work orders:

Consider the following situation:

A standard request with standard suborders has been defined. If the user that is not authorized to view work orders wants to apply this standard request, the following happens: all the fields that are part of the request are filled, but the suborders are not created (even if the user indicated that he wanted to create the suborders).

In Authorization, you have configured that a user is not authorized to view some work orders fields:

Consider the following situation:

The user wants to apply a standard work order or standard request. What will happen? Planon tries to populate fields that cannot be populated because the user is not authorized to view them. In that case, Planon populates all fields for which the user is authorized and skips the ones the user is not authorized to view. Planon will not give an error message. Note: If a user has read-only rights to a field, Planon is still authorized to populate it.

In Authorization, you have configured the following:

Situation 1: a user has read-only access to the **Department** field of the **Person** business object.

Situation 2: a user has no access to the **Department** field of the **Person** business object.

If the user selects a person in department "FM" and chooses the **Copy** action, the following will happen:

For situation 1: the **Department** field of the new object (person) will be populated with the value "FM", even though the user is not authorized to change the value of this field manually.

For situation 2: the **Department** field of the new object (person) will be left empty (but the user does not see this field!).

Combining user groups

In the following section, some examples are given of the prevailing authorization if users belong to more than one user group.

- If the **Read** action is available in User Group 1 but not available in User Group 2, the **Read** action will be available for a user who is in both user groups.
- If the **Property** field of the work order business object is not available in User Group 1 but modifiable in User Group 2, it will be modifiable for a user who belongs to both user groups.
- Suppose User Group 1 has no filter on the **Read** action for Property (=users from this group are able to view all properties) and User Group 2 has a filter on the **Read** action that allows viewing properties in Amsterdam only. A user who belongs to both user groups will be able to view all properties.
- Suppose User Group 1 has a filter that allows reading properties in London only and User Group 2 has a filter on the **Read** action that allows viewing properties in Amsterdam only. A user who belongs to both user groups will be able to view the properties in both Amsterdam and London.
- Suppose User Group 1 has no filter on the **Read** action for Property (=users from this group can view all properties) and a filter on the **Save** action that allows modifying properties in London only. User Group 2 has a filter that allows viewing properties in the Netherlands and modifying properties in Amsterdam only. A user belonging to both user groups will be able to view all properties and can modify properties in Amsterdam and London.
- Suppose User Group 1 has a filter that allows viewing properties in the Netherlands and modifying properties in Amsterdam only. User Group 2 has a filter that allows viewing properties in Amsterdam and modifying properties in Amsterdam only. A user belonging to both user groups will be able to view properties in both Amsterdam and in the rest of the Netherlands and modify properties in Amsterdam only.

System reports - Authorization

The following sections describe the system reports that are available for **Authorization**.

On **User groups** level, a system report is available that can list various properties of a user group and its function profile. For more information, see User groups report.

On Function profiles > BO Rights level, a system report is available providing per authorized business object and function profile a clear overview of the:

- Permission type
- Available actions
- Possible status transitions
- Available extended actions
- Available fields (optional)

  For more information, see BO Rights report.

User groups report

This section describes the system report that is available in Authorization > User groups. 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.
Show actions	Select this check box to include in the report the actions available to the user group.
Show authorization links	Select this check box to include in the report the authorization links available to the user group.
Show statuses	Select this check box to include in the report the statuses available to the user group.
Show permission types	Select this check box to include in the report the permission types available to the user group.

Parameters	Description
Show action filters	Select this check box to include in the report the action filters available to the user group.

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.

Index