iPCA
Management

iPoint-systems gmbh
Ludwig-Erhard-Straße 58
72760 Reutlingen

Tel +49 7121 14489 60
Fax +49 7121 14489 89
info@ipoint-systems.de

Director: Jörg Walden
Amtsgericht Reutlingen · HRB 353830
USt.-Id.Nr. DE813135964

Imprint

This document is part of the product family iPoint Compliance Agent.

iPoint-systems gmbh

Ludwig-Erhard-Strasse 58

72760 Reutlingen

Germany

Phone: +49 7121 14489 60

Fax: +49 7121 14489 89

Table of Contents

1 Introduction

1.1 General

This document is for the application administrators for iPoint Compliance Agent.

This documentation describes the management of roles and users and the advanced configuration of the application.

Information about the usage of the products is available in the corresponding documents.

Parts of this documentation are describing optional function. These optional functions are marked as “optional” in the documentation.

Some functions are only available with specific rights owned by the login user. If a required functionality is not available for you, please contact your internal administrator.

2 Support

For any questions about the application, please contact your in-house administrator.

This administrator will check and answer your enquiry.

If you in-house administrator cannot solve the problem, he will contact iPoint-systems gmbh to get a solution for it.

It is important that only the in-house administrator contacts iPoint-systems gmbh as this is the only way to get a fast response and to avoid doing the work twice.

3 New functions

Version	Description
13.25	Renamed permissions • COMPONENT to IHS_NUMBER_COMPONENT • MATERIAL to IHS_NUMBER_MATERIAL • SEMICOMPONENT to IHS_NUMBER_SEMICOMPONENT • ARTICLE to IHS_NUMBER_ARTICLE • MIXTURE to IHS_NUMBER_MIXTURE
13.24	Added permissions for administration of LCM requests and for bulk import of LCM requests (only for LCM web application) Added permissions for access to and administration of Plants master data panel Added permissions for access to and administration of Projects master data panel
13.20	Added permissions for editing of IHS number in the IMDS and SAM-M datasheets Added permissions for RoHS Letter creation for VP
13.15	Added permission for publishing SVHC information in VP(s) into an external portal
13.08	Added permission for export of SDS files to an external SDS service provider (optional) Added permission for publishing of SDS files to an external interface (optional)
13.05	Added permissions for control of the display of contact details in 'Received' and 'Sent' panels (based on GDPR regulation)
13.03	Added permission for requesting and answering external advice for SEP request (optional)
13.02	Added permissions for regions and region types management (optional) Added permissions for handling of regions at MDSs (optional) Added permissions for storage classes master data management (optional)
13.00	Added permission for control of the priority of the DB job Added search feature for permission tree
12.27	Renamed permissions for access UN Number and Hazard Class master data panels Added permissions for access Technical and physical management master data panels
12.24	Added permissions for creation of new version of MDS/module Improved and moved permissions for sort out module
12.21	Added permissions for event manager for SAM-M module
12.18	Added permissions for access UN Number and Hazard Class master data panels
12.17	Added permission for MDS bulk deactivation (optional) Added permission for RRR product model deletion Added permissions for company and contact exports (optional)
12.10	Added filter for active users to the user search
12.09	Added permission for MDS bulk transfer (optional)
12.05	Added more granular permissions for IHS companies management Added more granular permissions for IHS contacts management Added permissions for deletion of article and mixture

Version	Description
	Added permission for deletion of SAM-M substance Added permission to import supplier contacts Added permissions for chemistry manager (feature itself is not released yet)
12.03	Added permissions for copy of article and mixture Added permission for copy of SEP request Added permissions for SEP requests Added permission for administration of contacts of IHS companies Added permissions for conversion of the VP to DS (optional) Added permissions for VPM charts (optional) Added permissions for iPCA web (optional) Added permissions for request charts (optional)
12.00	Reworked permission handling and renamed permissions for deletion of MDSs/modules Added permissions for read-only access to Parts list and DS List Added permission for releasing the RRR product model
11.12	Added function to exclude user from automatic password expiration Added function to exclude user from automatic user deactivation
11.11	Added permission for load of MDS in the Sent panel
11.09	Added permissions for VPM PDM import configuration panel Added permissions for IHS module, IHS database interface and IHS matching tables management Added permissions for product definition lookup Added permission to change the process type of a request
11.05	Added permission for quality check of the datasheet
11.00	Added function to export permissions vs. roles matrix
10.24	Added permission for administration of the document management module Added permissions for reactivation of article and mixture Added permission for RRR extended library edit Added permission for creation of a product model from article
10.13	Added several permissions for iPCA, SAMM and SEP features
10.01	Added permissions for creation of VP from CSI results (optional) Added permissions for physical deletion of VPs and deletion of jobs linked to VP (optional) Added permission for physical deletion of DB jobs including their content Added permission for re-check of already processed received MDSs (optional) Added permission for search of SAM-M documents
10.00.006	Added permission for creation and copy of the user account
9.14	Added permission for REACH report Added permission for starting usage and CSI analysis for VPs
9.12	Added permissions for setting archive status for articles and mixtures
9.10	Added more granular permissions for upload to IMDS

Version	Description
9.06	Added permissions for VPM (optional) Added permissions for Problem solving MDS flag (optional)
9.04	Added permissions for copy and forward Added permissions for automated user deactivation (optional)
9.03	Added permission for SPM multi edit
9.00	Added password security visualization and password validity (optional) Added phoneNo. and signature to restricted user management (optional) New permissions for Program Tracking System and SEP
8.08	New permissions for scheduling CSI and usage list background jobs (optional)
8.05	New permissions for MSP (optional)
8.00	New permissions in the scopes of CSI, job management and RRR
7.5	Added permissions for printing and display of basic substances IMDS Contact name can be stored to a user
6.2	New sub permission for SEARCH_INBOX New sub permission for CHECK_MDB
6.00	Signature for the user New permissions for management of events, REACh and the check configurations General Layout changes
5.4	Added type information for all privileges Added visualization of user type Added function to export of user list Changed display of user tree Changed display of roles Added dropdown for selection of Organization Unit of user Added new permissions for administration of own substance group types, substance groups, compliance checker and to see database jobs
5.1	Added configuration of application Added function to copy the user Added new permissions for administration of companies, own substances and norms
5.00	Added new permission for JAMA module
4.07	Added new permissions for MACSI module and publishing of the datasheet

4 Management

The management allows administrator of the application to manage users, roles and some special configuration parameters of the application.

The management can either be accesses from inside the application iPCA/IHS (menu "**Extras → Management**") or by using the link on the start page for the web based products like iPCA/SCM. A user without management permission is only allowed to change his data (see **chapter 4.1.1.6**).

When starting the management, small window pops-up (see **Figure 1**). By click on the "**OK**" button, the management is opened in a new window.

By ticking the checkbox "**Activate admin mode?**" and entering the correct password, the management with extended configuration of the application will opened. Please note, that the password is available to iPoint only. When entering wrong or no password, a notification will be shown (see **Figure 2**) and the standard management will be loaded.

PLEASE NOTE: The change of the configuration of the application should be done by users with special training.

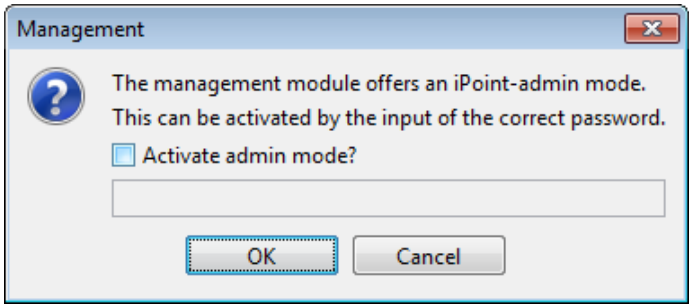

Figure 1 Pop-up window shown prior the management being loaded

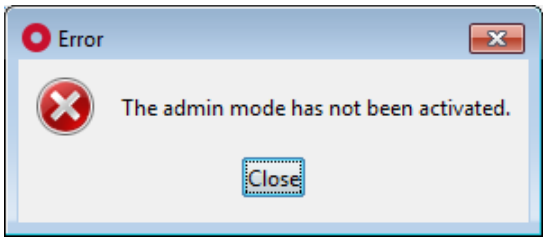

Figure 2 Notification informing that the management in extended mode has not been activated

4.1 User management

4.1.1 Users

The management is activated through tab "**Users**" (see **Figure 3**).

The users tab is split into four areas:

1. Search mask (orange) – see **chapter 4.1.1.1**
2. Overview of existing users (blue) – see **chapter 4.1.1.2**
3. Interactive area showing details of a user selected in area 2 (green) – see **chapter 4.1.1.3**
4. Actions (black) – see **chapter 4.1.1.4**

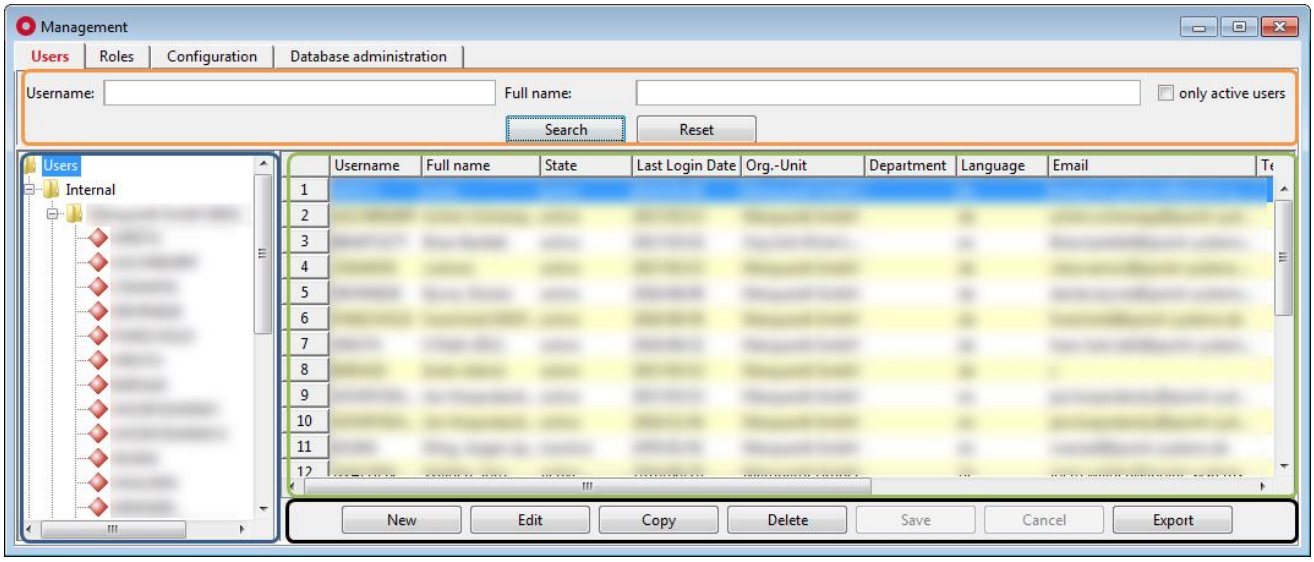

Figure 3 Overview of users

4.1.1.1 Search mask

Enables the quick search for a user by either username or full name or by the status of the user account. Matches will be shown in reference to the entered search criteria.

The following actions are available:

- **Search**
  Perform searches based on criteria entered into the search fields
- **Reset**
  Remove entered search criteria from search fields

4.1.1.2 Overview of existing users

The list of users is split by associated organization units and sorted by the user name. It is also split into internal and external users.

To get the details about a particular user, their name must be selected. Then in the interactive area on the right side, all information about the selected user is displayed.

To get just a list of users assigned to a particular organization unit, the organization unit must be selected.

If an organization unit is not valid anymore its background and the background of assigned users is greyed-out. These users are set as inactive. In order to activate them, they have to be assigned to an active organization unit otherwise it is recommended to delete these users.

Depending on the permissions, which are associated to a user (by roles), the user, from a license point view, could be:

- Concurrent user
- Named user
- Admin user

The symbol is shown in front of the user name to make it easy to recognize the assigned roles.

4.1.1.3 Interactive area

This part of the "**Users**" window displays either the list of all existing users or a list of users assigned to a selected organization unit (see **Figure 3**) or a detail of a user selected in the tree on the left side of the window (see **Figure 4**).

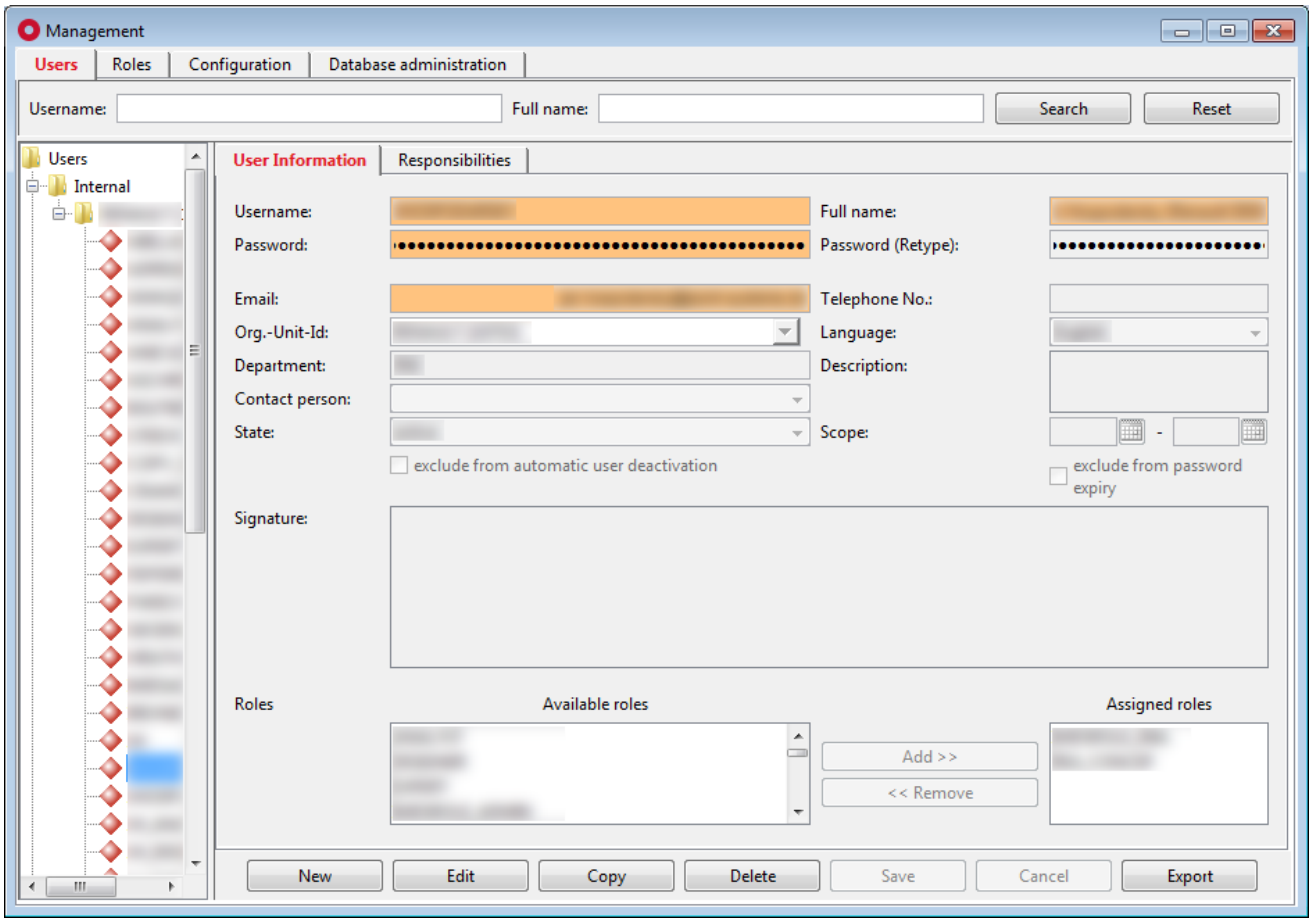

Figure 4 Details of a selected user

4.1.1.4 Actions

The following actions are available:

- **New**
  Create a new user
- **Edit**
  Edit details of a selected user
- **Copy**
  Create a new user by copying a selected user

- **Delete**
  Delete a selected user
- **Save**
  Save created user or save update to existing user
- **Cancel**
  Cancel the editing or created user without saving
- **Export**
  Export the list of users

4.1.1.4.1 Creating a user

A new user can be created by click on the "**New**" button. This loads an empty mask for user to be defined (see **Figure 5**). Fields highlighted in orange are mandatory and must be filled out. If these fields are not filled out, then a new user cannot be created.

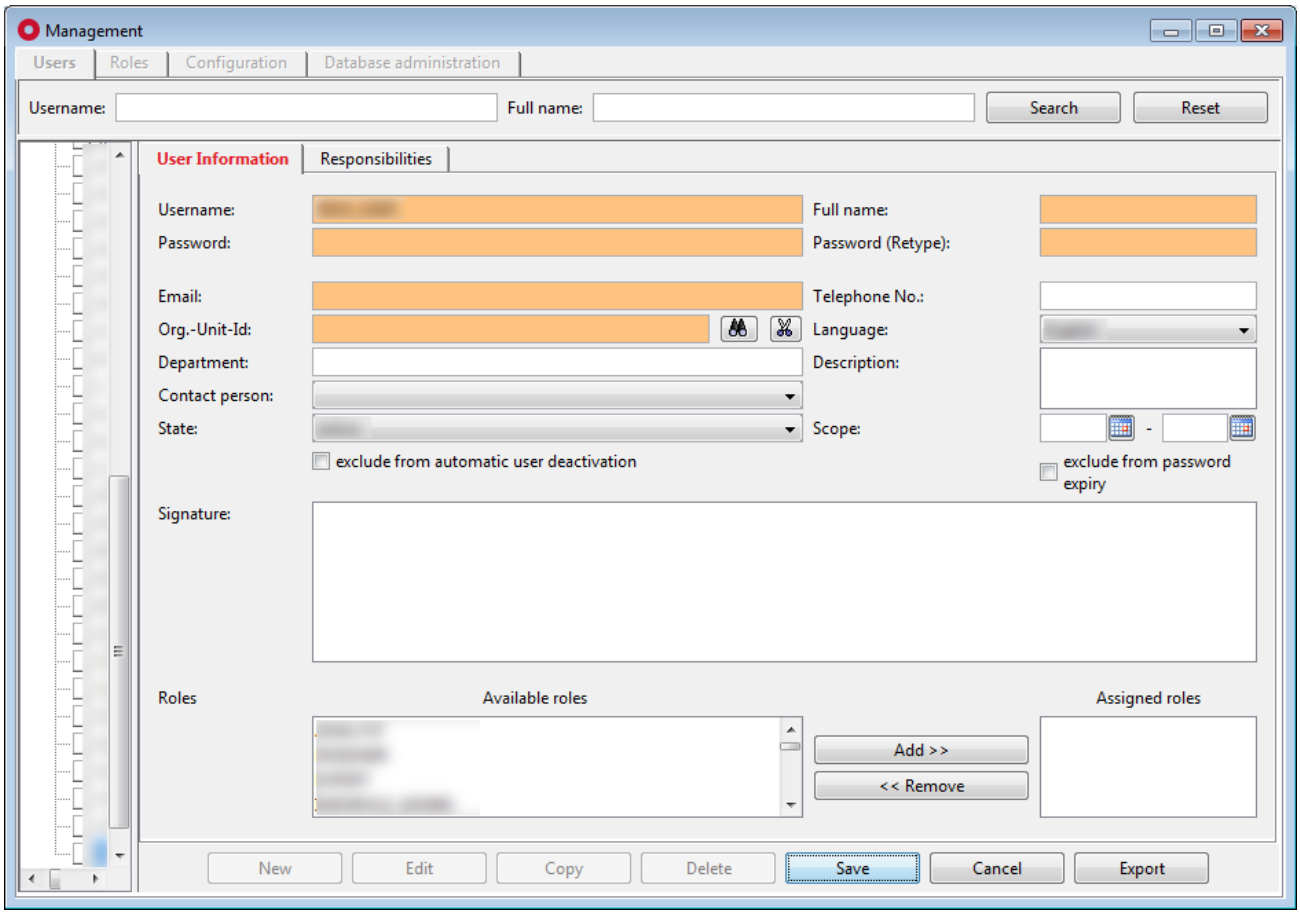

Figure 5 Creating a user

Following information must/could be defined:

- **Username**
  It must be unique.
  The maximum length is 30 characters.
  On save, the entered value is automatically converted to capital letters.
  PLEASE NOTE: Due to security reasons, username must not contain the strings "**imds**" and "**ipca**".
- **Full name**
  The complete name of a user, e.g. "**John Smith**".
- **Password / Password (Retype)**
  User's password. When typing, instead of characters bullets are shown.
  The password must have minimum length of 4 characters must be different for the previously used password.
  Further criteria depend upon the configuration by your company administrator.
- **Email**
  Email address of a user must be entered in valid format (e.g. info@ipoint-systems.de).
  It is used as a sender for emails created within the system.
- **Telephone No.**
  User's telephone number.
- **Org.-Unit-Id**
  IMDS organization unit to which is a user is assigned to. It could be your own company (internal) or an external organization unit.
  If it is an internal user all of the internal organization units are displayed in a drop-down list from which the corresponding entry can be selected.
  If the user is from an external company, then that company/org.unit can be selected by searching via the company search dialog which opens by clicking the search button. To revert/delete the entry a delete button is available.
- **Language**
  Selected language will be used as
  - an application language in case of automatic login (SSO)
  - a correspondence language for some generated emails
  - a standard language for background jobs, e.g. import
- **Department**
  Name of the department a user works in.
- **Contact person**
  IMDS contact name which is used for to upload new own datasheet from iPCA to IMDS.
- **Description**
  Any comment about a user.

- **State**
  Flag to set a user as active or inactive.
  PLEASE NOTE: In case the user account is set to "**inactive**", values from couple of attributes are removed (for more details see **chapter 7**).
- **Scope**
  Definition of the period of validity for a user account, e.g. for temporary employees
  PLEASE NOTE: In case the user account is set to "**inactive**" automatically on login of the user whose user account validity is expired, values from couple of attributes are removed (for more details see **chapter 7**).
- **Exclude from automatic user deactivation**
  If checked the user is excluded from the automatic user deactivation after n-day of inactivity (for more details see **chapter 5**)
- **Exclude from password expiry**
  If checked the user is excluded from the password expiration (for more details see **chapter 6**)
- **Signature**
  User's signature. This is attached to the datasheet rejection email checked in SCM/USC.
- **Roles**
  Roles define what functions of iPCA are available to a user. At least one role needs to be assigned to a user for the account to the valid. On the left-hand side all available roles are listed. Using the "**Add >>**" button a role can be added to a user. Using the "**<< Remove**" button an assigned role will be withdrawn from a user.
  PLEASE NOTE: User gets all permissions cumulated from all assigned roles.

Once all required details are defined a new user can be created by clicking the "**Save**" button. To cancel the creation of a user, click the "**Cancel**" button.

PLEASE NOTE: The "**Responsibilities**" tab can be used only if a Product Release Process module (PRP) is activated.

4.1.1.4.2 Editing a user

The details of a selected user can be changed by clicking on the "**Edit**" button. This loads a mask populated with details of a user (see **Figure 4**) and they could be changed.

Once all changes are done, they can be saved by clicking on "**Save**" button. To cancel changes, click the "**Cancel**" button.

4.1.1.4.3 Copying a user

A new user can be created by copying an existing user selected in the user overview by click on the "**Copy**" button. This loads a mask populated with details of the original user.

The username of a copied user is automatically given the prefix "**COPY_**" and the original password is removed so it will need to be defined.

Once all changes are done, they can be saved by click on the "**Save**" button. To cancel changes, click the "**Cancel**" button.

4.1.1.4.4 Deleting a user

An existing user can be deleted by click on the "**Delete**" button. This will bring up a small pop-up window (see **Figure 6**). By clicking on the "**Yes**" button a user will be deleted. By clicking on the "**No**" button, the user will be kept.

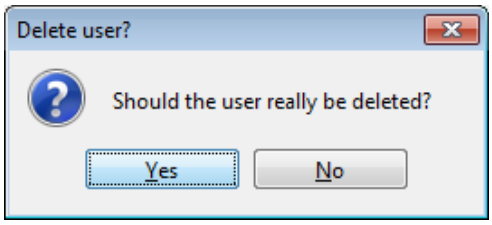

Figure 6 Confirmation of deletion of a user

4.1.1.4.5 Export of users

Existing users can be exported in a CSV or an XLS(X) file by clicking on the "**Export**" button.

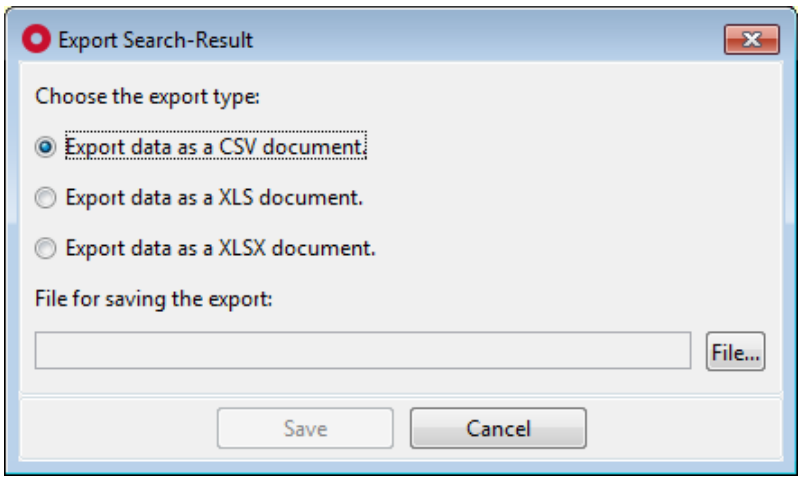

Figure 7 Export of users

The user is then asked to choose a desired output format and define the location, where the exported file is to be stored (see **Figure 7**). To learn more details about export function, please see the IHS user manual (see **chapter 6.4.4**).

4.1.1.5 Password security and validity

4.1.1.5.1 Password security

A company administrator has the option to define some criteria for user passwords, allowing the security of the passwords to be set. This level is visualized below in the "**Password**" field (see **Figure 8**).

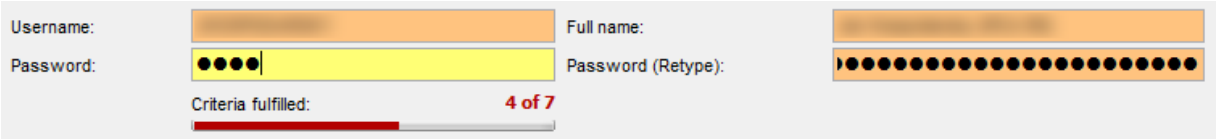

Figure 8 Password security

The defined criteria are displayed as a "tip" as long as the cursor is hovering over the field "**Password strength**". Only passwords which fulfill all defined criteria can be saved, otherwise an error message is shown listing all the missed criteria (see **Figure 9**).

Figure 9 Notification shown if password does not meet security requirements

4.1.1.5.2 Password validity

If a password validity period has been defined by a company administrator, the validity in days is displayed below the field "**Password (Retype)**" (see **Figure 10**). As soon as this period expires the user has to change the password after the next login. The validity period is then reset.

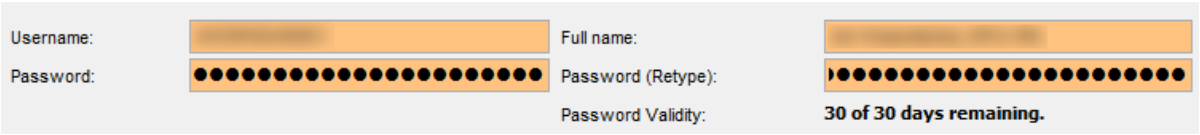

Figure 10 Password validity

4.1.1.6 Editing of own data

A user without management permission can change only their individual data (see **Figure 11**). This can be done from iPCA/IHS application by navigating to the menu "**Extras → Management**".

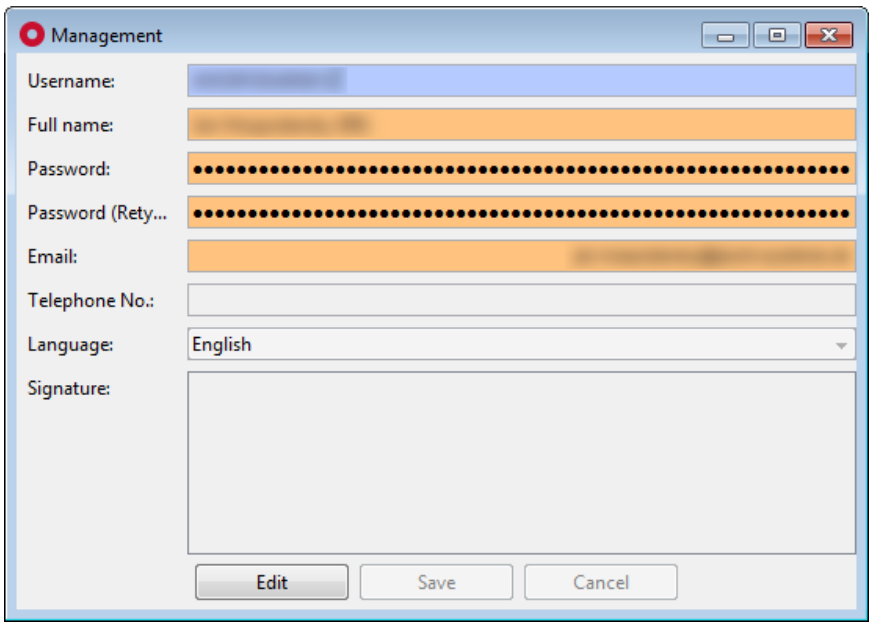

Figure 11 Editing of own data

By clicking on the "**Edit**" button the following data is able to be changed:

- **Full name**
  A complete name of a user, e.g. "**John Smith**"
- **Password / Password (Retype)**
  User's password. When typing, instead of characters bullets are shown. The password must have minimum length of 4 characters and must be different for the previously used password. Further criteria depends upon the configuration by your company administrator.
- **Email**
  Email address of a user must be entered in valid format (e.g. info@ipoint-systems.de). It is used as a sender for emails within the system.
- **Telephone No.**
  User's telephone number. This is not a mandatory fieldyet it will be beneficial if quick contact needs to be made.
- **Language**
  Selected language will be used as a default for a user when launching iPCA.
- **Signature**
  User's signature. This is attached to the datasheet rejection email checked in SCM/USC.

Once all changes are done, they can be saved by click on the "**Save**" button. To cancel changes, click the **Cancel**" button.

4.1.2 Roles

The role tab contains permissions, which can be enabled or disabled to specify what features in the application are available to a user.

Upon the activation of the "**Roles**" tab, an overview is shown (see **Figure 12**).

The roles tab is split into three areas:

1. Overview of existing roles (blue) – see **chapter 4.1.2.1**
2. Interactive area showing details of a role selected in area 2 (green) – see **chapter 4.1.2.2**
3. Actions (black) – see **chapter 4.1.2.3**

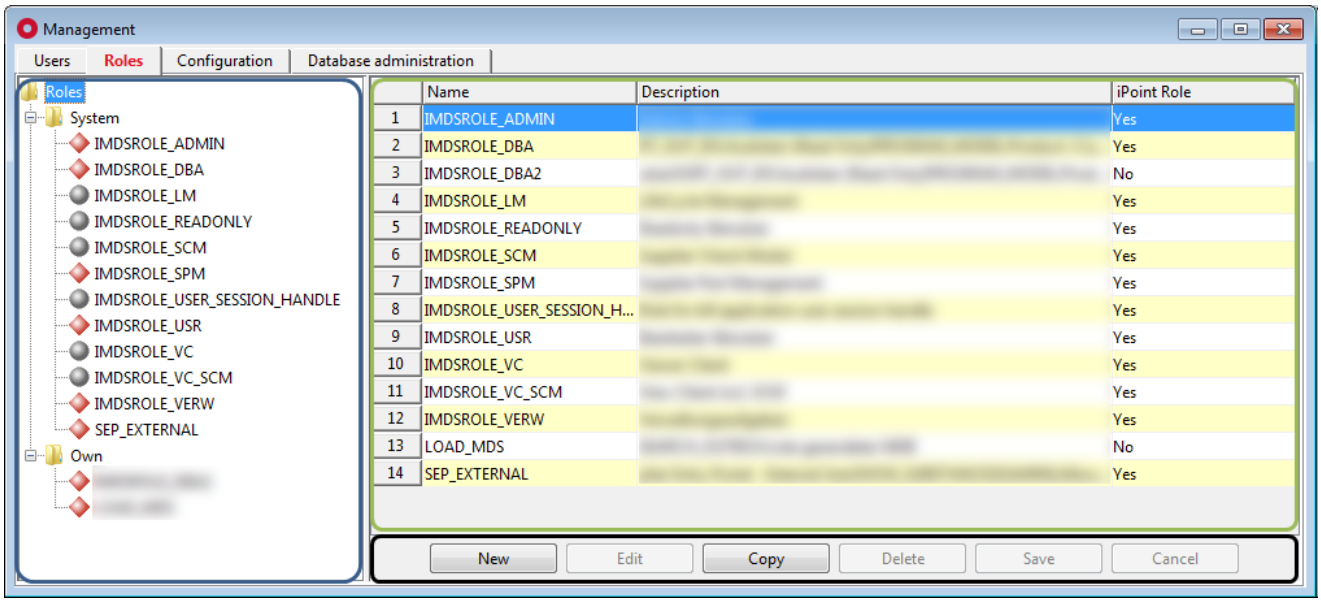

Figure 12 Overview of roles

When creating roles, two strategies can be chosen:

- **User specific roles**
  Roles describing all permissions for a specific user or group of users, e.g. "**admin**", "**purchasing**", etc.
- **Module specific roles**
  Roles describing a small specific task, e.g. MDS approved with all rights to accept/reject datasheet.

PLEASE NOTE: The administrator must take care that a user does not get permissions, which interfere with the assignment of different roles. The behavior of the application cannot be predicted, if the user has contradictory permissions like as detailed below.

- iMDS_IHS → READ_ONLY
- iMDS_IHS → EDIT

4.1.2.1 Overview of existing roles

The list of roles is divided into two groups:

- **System**
  Roles are defined by iPoint-systems (see **Table 1**). These roles cannot be changed and are subject of change in future releases of iPCA.
- **Own**
  Roles defined by a customer so they are fully editable and can be changed anytime required.

Role Name	Description
IMDSROLE_ADMIN	The role for iPCA user with some administrator rights
IMDSROLE_DBA	The role for iPCA user with full administrator rights and access to database administration
IMDSROLE_LM	The role for LCM user
IMDSROLE_READONLY	The role for iPCA read only user
IMDSROLE_SCM	The role for SCM user
IMDSROLE_SPM	The role for SPM user
IMDSROLE_USER_SESSION_HANDLE	The role for kill application user session handle
IMDSROLE_USR	The role for iPCA user
IMDSROLE_VC	The role for web client read only user
IMDSROLE_VC_SCM	The role for web client user
IMDSROLE_VERW	The role for iPCA user with user administrator rights
PTSROLE_CHAMPION	The role for PTS user with rights to create requests over the complete lifecycle of the request
PTSROLE_CHAMPION_SV	The role for PTS user with rights to create requests over the complete lifecycle of the request and for champions team
PTSROLE_DATA_COLLECTOR	The role for PTS user with rights to collect data from suppliers for parts
PTSROLE_REQUESTOR	The role for PTS user with rights to create requests for assemblies
PTSROLE_VALIDATOR	The role for PTS user with rights to validate incoming IMDS data
SEP_EXTERNAL	The role for SEP external user

Table 1 Details of system roles from iPoint

To get the details about a particular role, it must be selected. Then in the interactive area on the right-hand side, all information about the selected role is displayed.

The symbol shown in front of the role tells what type of license it is:

- Concurrent
- Named
- Admin

4.1.2.2 Interactive area

This part of the "**Roles**" window displays either the list of all existing roles (see **Figure 12**) or details of a selected role in the tree on the left-hand side of the window (see **Figure 13**).

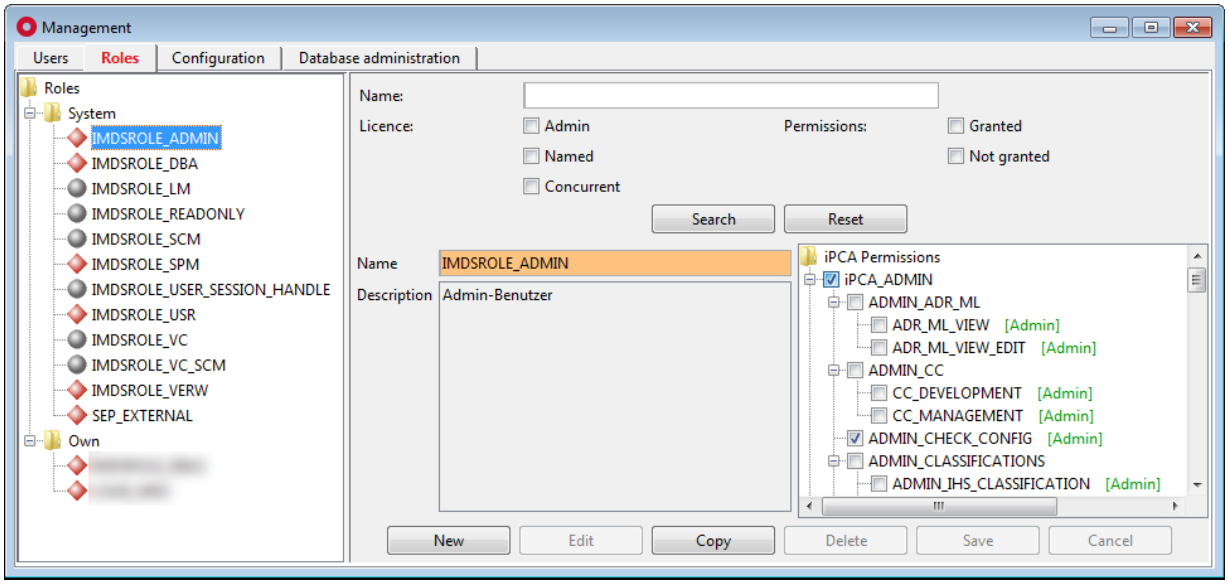

Figure 13 Details of selected role

If the role is viewed, the search panel allowing to search for permissions is enabled.

This allows to search for the permissions based on their licence type and/or name and/or fact whether they are granted in the particular role or not.

When searching by permission name (leading and trailing wildcard is supported), only permissions that contain searched text are displayed in the permission tree. However, if it happens that there don't exist the permission with searched text, but its parent contains the searched text, this is displayed together with all its permissions.

If the new role is being created or existing role is being edited or copied, the search panel is disabled.

4.1.2.3 Actions

Following actions are available:

- **New**
  Create a new role
- **Edit**
  Edit details of a selected role
- **Copy**
  Create a new role by copy of a selected role
- **Delete**
  Delete a selected role
- **Save**
  Save created role or update of existing role
- **Cancel**
  Cancel the editing or creating of a role without saving
- **Export**
  Export the permission & roles matrix

4.1.2.3.1 Creating a role

A new role can be created by click on the "**New**" button. This loads an empty mask allowing for the role to be defined (see **Figure 14**). Fields highlighted in orange are mandatory and must be filled out. If they are not filled out a new role cannot be created.

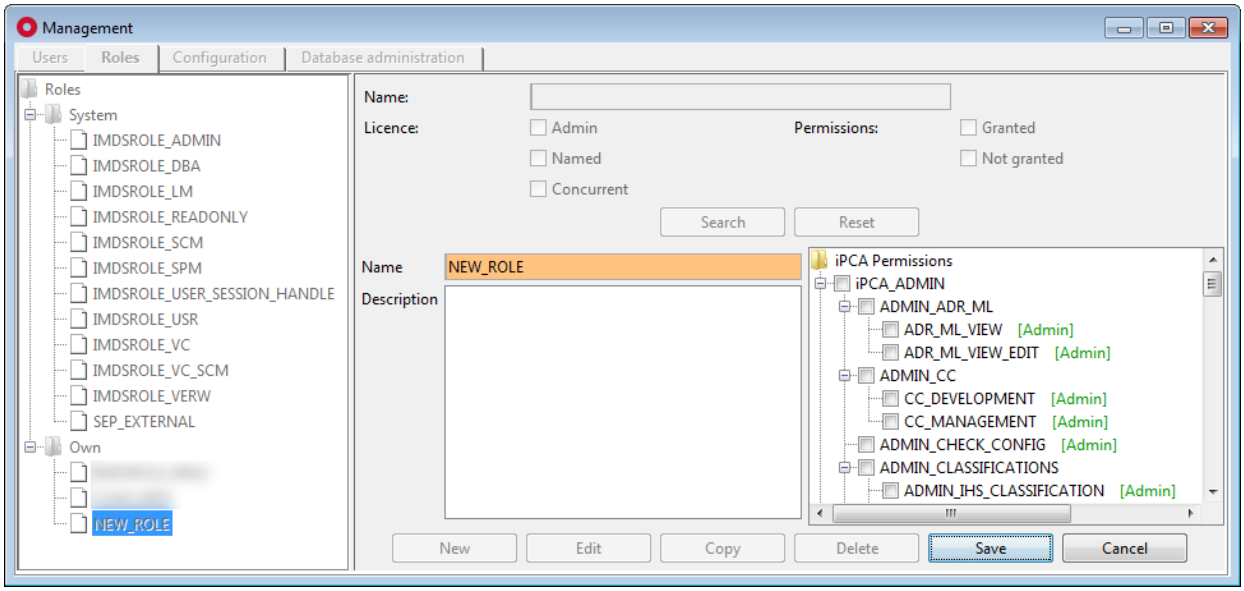

Figure 14 Creating a role

The following information can/must be defined:

- **Name**
  It must be unique. When saving, it is converted automatically into capital letters.
- **Description**
  Any comments or explanations about a role.
- **Permissions**
  Assignment of permissions to the role is detailed in **chapter 4.1.3.2**.

In situation where the name of the role already exists, a notification will be shown (see **Figure 15**).

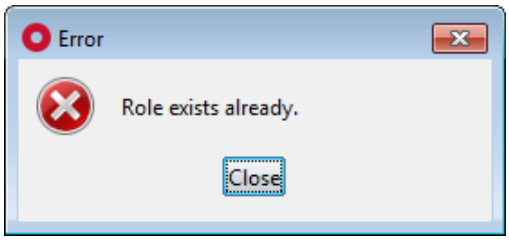

Figure 15 Notification shown if role with the same name already exists

Once all required details are defined a new role can be created by clicking on the "**Save**" button. To cancel the creation of a role, click on the "**Cancel**" button.

4.1.2.3.2 Editing a role

Details of a role selected in the role overview of can be changed by click on the "**Edit**" button. This loads a mask populated with details of a role (see **Figure 13**) which can be edited.

Once all the changes are done, they can be saved by click on the "**Save**" button. To cancel changes, click the "**Cancel**" button.

PLEASE NOTE: Roles assigned the to role group "**System**" are from iPoint-systems and cannot be changed.

4.1.2.3.3 Copying a role

New role can be created by copying an existing role. This is done by selecting a role in the role overview and clicking on the "**Copy**" button. This loads a mask populated with details of original role.

Once all changes are done, they can be saved by clicking on the "**Save**" button. To cancel changes, click the "**Cancel**" button.

4.1.2.3.4 Deleting a role

Existing role can be deleted by clicking on the "**Delete**" button. This opens a small pop-up window (see **Figure 16**). By clicking on the "**Yes**" button a role will be deleted. By clicking on the "**No**" button, the role will be kept.

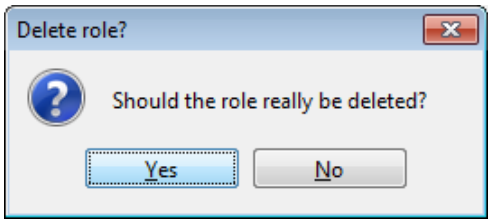

Figure 16 Confirmation of delete of a role

In situation where a role is assigned to at least one user a notification is shown (see **Figure 17**). A list of users with particular role assigned can be retrieved by click on the "**Details >>**" button. By clicking on the "**Yes**" button a role will be deleted and revoked from affected user(s). By clicking on the "**No**" button, the role will be kept.

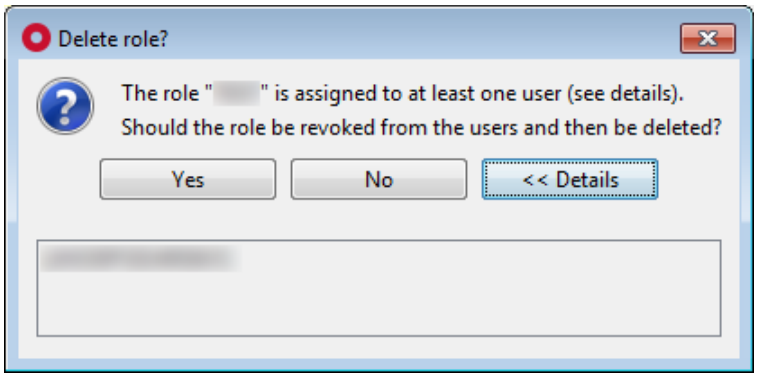

Figure 17 Confirmation of deleted role assigned to at least one user

4.1.3 Permissions

4.1.3.1 Introduction

The permissions define what features in the application are available to a user.

Permissions are assigned to users through roles and they are cumulative.

Example:

Role "**A**" has the permission "**iPCA_ADMIN**" but not the permission "**iMDS_IHS**"

Role "**B**" does not have the permission "**iPCA_ADMIN**" but has the permission "**iMDS_IHS**"

When both roles are assigned to a user, he/she has both permissions.

Some permissions or permission groups listed in the following chapters may not be available in the permission tree if the module related license has not been purchased by your company.

When a permission, which is not available under your purchased is assigned to a role (e.g. if "**iMDS_LM**" is not licensed), the assignment will have no effect.

All permissions are marked whether they are of named, concurrent or admin type.

4.1.3.2 Assignment of permissions

The assignment of permission to a role is done by marking the permission ☑ .

If the permission has sub-permissions underneath and the parent permission is checked/unchecked, sub-permissions are checked/unchecked accordingly.

When all sub-permissions are unchecked, the parent permission is automatically unchecked.

4.1.3.3 Overview of permissions

The permissions are divided into several groups:

- **iMDS_IHS**
  Permissions specific to working with the in-house system, e.g. search, edit, do reports, etc. (see **chapter 4.1.3.3.1**)
- **iMDS_LM**
  Permissions specific to working with Lifecycle Management module (see **chapter 4.1.3.3.2**)
- **iMDS_SCM**
  Permissions specific to working with Supplier Check / User Guided Supplier Check module (see **chapter 4.1.3.3.3**)
- **iMDS_SPM**
  Permissions specific to working with Supplier Parts Management module (see **chapter 4.1.3.3.4**)
- **iMDS_VC**
  Permissions specific to working with web client (see **chapter 4.1.3.3.5**)
- **iPCA_ADMIN**
  Permissions for the management of the application (see **chapter 4.1.3.3.6**)
- **iPCA_GENERAL**
  Permissions that are used for IMDS and SAM-M part of the application (see **chapter 4.1.3.3.7**)
- **PTS**
  Permissions for the management of the Program Tracking System (see **chapter 4.1.3.3.8**)
- **RRR/LCA**
  Permissions specific to working with RRR / Lifecycle Assessment modules (see **chapter 4.1.3.3.9**)

- **SAMM**
  Permissions specific to working with Substances, Articles and Mixtures Management module (see **chapter 4.1.3.3.10**)
- **THIN_CLIENT**
  Permissions specific to working with some parts of IHS application over thin client (see **chapter 4.1.3.3.11**)

4.1.3.3.1 iMDS_IHS

Permission Name	Description
ADMIN	The permissions to manage IHS application
ADMIN_EVENT	The permission to create and edit LCM and SPM events for all users
ADMIN_IACM	The permission to manage internal article codes for components/semi components
ADMIN_MAT_IACM	The permission to manage internal article codes for materials
ADMIN_MDB	The permission to edit MDS/modules (own and received) of whole own company regardless from the assigned organization unit to the user.
ADMIN_SUBSTITUTION	The permission to edit and to create substitution rules in the edit mask or during the copy process (e.g. creation of a flatbill).
BLACKLIST	The permissions for Blacklist module
BLACKLIST_EDIT	The permission to edit blacklist entries for BoM import
BLACKLIST_VIEW	The restriction to access blacklist entries for BoM import in read only mode
CHECK	The permissions for managing checks in IHS
CHECK_MDB	The permissions to check and accept or reject MDS
ALL_OTHER_ORG_UNITS	The permission to check MDS which were sent to all other organization units of the company. (own and organization unit of company are not included, depending on permissions OWN_ORG_UNIT and/or COMPANY_ORG_UNIT).
COMPANY_ORG_UNIT	The permission to check MDSs which were sent to the any organization unit of own company
OWN_ORG_UNIT	The permission to check MDSs which were sent to the organization unit the user is assigned to
CHECK_QUALITY	The permission to use the quality checker
CHECK_RECOMMENDATION	The permission to use the recommendation checker
CREATE_CHECK_CONFIG	The permission to create, edit and delete an own check configurations

Permission Name	Description
IMDS_AUTOMATED_INBOX_CHECK	The permissions for automated inbox check (AIC)
IMDS_AIC	The permission for automated inbox check (AIC)
IMDS_AIC_VIEW	The restriction to access automated inbox check (AIC) in read only mode
ADMIN_IMDS_AIC	The permission to edit automated inbox check (AIC)
AIC_WHITELIST_VIEW_EDIT	The permission allows to view and edit AIC Whitelist
AIC_WHITELIST_VIEW	The permission allows to view the AIC Whitelist
CHEMISTRY MANAGER	The permissions for IMDS regulator information
CHEMISTRY_MANAGER_MULTI_REQUEST	The permission for request functions for IMDS regulatory information for accepted and published MDS for multiple MDS/Modules from search result list
CHEMISTRY_MANAGER_REQUEST	The permission for request functions for IMDS regulatory information for accepted and published MDS
CHEMISTRY_MANAGER_VIEW	The permission to see IMDS regulatory information for own MDS/modules
CHEMISTRY_MANAGER_VIEW_EDIT	The permission to edit IMDS regulatory information for own MDS/modules
COMPLIANCE_CHECKER	The permission group for CSI checks
CC_CHECK	The permission to check MDS using released compliance checker groups
CC_CHECK_CONFIG	The permission to make the rule groups available in different check configurations
CC_CYCLIC_JOB	The permission to create reoccurring CSI check jobs
CC_EXPORT	The permission to export the rule groups into the exchange format
CC_IMPORT	The permission to import rule groups in the exchange format
CC_INSPECTOR	The permission to check MDS using all compliance checker groups (even if not yet released)
CC_MONITORING	The permission to set the monitoring option for a scheduled CSI job
CC_RESULT_TO_VPM	The permission to create VP from the results of the IMDS CSI analysis
CC_SCHEDULE_JOB	The permission to schedule background jobs in CSI wizard (start date and time)

Permission Name	Description
EDIT	The permissions to work in the IHS application
ADD_DOCUMENTS	The permission to access and manage tab “Documents” in MDS/Module.
BULK_UPDATE	The permission to use Bulk update module
CREATE	The permissions to create, edit and copy MDS/modules
COPY	The permissions to copy MDS/modules
COPY_COMPONENT	The permission to copy component MDS/module
COPY_MATERIAL	The permission to copy material MDS/module
COPY_ONLY_MDS_WITH_FORWARDING_ALLOWED	The permission to copy received MDS only if the checkbox "Forwarding allowed" is checked
COPY_SEMI_COMPONENT	The permission to copy semi-components MDS/module
CREATE_COMPONENT	The permission to create and edit copy component MDS/module
CREATE_SEMI_COMPONENT	The permission to create and edit semi-component MDS/module
CREATE_MATERIAL	The permission to create and edit material MDS/module
FORWARD	The permissions to forward MDS/modules
FORWARD_COMPONENT	The permission to forward component MDS/module
FORWARD_MATERIAL	The permission to forward material MDS/module
FORWARD_SEMI_COMPONENT	The permission to forward semi-components MDS/module
NEW_VERSION	The permissions to create a new version
NEW_VERSION_COMPONENT	The permission to create new version of component MDS/module
NEW_VERSION_MATERIAL	The permission to create new version of material MDS/module
NEW_VERSION_SEMI_COMPONENT	The permission to create new version of semi-component MDS/module
DELETE	The permission to delete MDS/modules
DELETE_MDSS_INTERNALLY_RELEASED	The permission to delete MDSs/modules that are internally released in IMDS online system

Permission Name	Description
DELETE_MDSS_NON_INTERNALLY_RELEASED	The permission to delete MDSs/modules that are not internally released in IMDS online system
EXTERNAL_EXPORT	The permission to export MDS (JAMA, Roundtrip)
FLATBILL	The permission to create a flatbill
IHS_NUMBER	The permissions to edit the IHS item number
IHS_NUMBER_COMPONENT	The permission to edit the IHS item number in the IMDS datasheet of type component
IHS_NUMBER_MATERIAL	The permission to edit the IHS item number in the IMDS datasheet of type material
IHS_NUMBER_SEMI-COMPONENT	The permission to edit the IHS item number in the IMDS datasheet of type semicomponent
PROTOTYPE_MDS	The permission to create a Prototype MDS
READY	The permission to set/reset the status “IHS ready” for MDS/module
REPLACE_MSP	The permission to show MSP in a tree and to replace an MDS with a MSP (if possible)
SHOW_MSP	The permission to show available MSP in a tree
EXCHANGE	The permissions to share data (roundtrip, IMDS, etc.)
CSV_IMPORT	The permission to start an CSV import
ERP_IMPORT	The permission to access information about ERP imports
ERP_STATISTICS	The permission to access ERP import statistics
ERP_STATUS	The permission to access the status overview of the ERP imports
EXPORT	The permission to export search result lists
IMPORT_EXPORT_OVERVIEW	The permission to open the import/export overview
MDS_BULK_TRANSFER	The permission to access MDS bulk transfer import panel
NXP_IMPORT	The permission to import part from NXP
PDM_BOM_IMPORT_DIRECT	The permission to perform PDM BoM import (direct)
PDM_BOM_REQUEST	The permission to request a PDM BoM

Permission Name	Description
PDM_BOM_REQUEST_ADMIN	The permission to manage PDM master data
PDM_BOM_REQUEST_USER	The permission to start PDM BoM download
ROUNDTRIP_EXPORT	The permissions to export a MDS via the Roundtrip interface
ROUNDTRIP_IMPORT	The permissions to import a MDS via the Roundtrip interface
SAFE_USE_INFORMATION_IMPORT	The permission to import safe use information documents
UPLOAD	The permissions to upload MDSs/modules from iPCA to IMDS
IMDS_BULK_UPLOAD	The permission to upload/send/propose multiple MDS at once
IMDS_UPLOAD	The permission to upload (upload, release, send, propose) MDSs/modules to IMDS
IMDS_UPLOAD_PUBLISH	The permission to publish a MDS in IMDS
IMDS_UPLOAD_PROPOSE	The permission to upload an MDS/module to IMDS and propose it
IMDS_UPLOAD_RELEASE	The permission to upload an MDS/module to IMDS and release it internally
IMDS_UPLOAD_SEND	The permission to upload an MDS/module to IMDS and send it
IMDS_UPLOAD_RESET	The permission to cancel upload of an MDS/module to IMDS
VALIDATION_VIEWDATA	The permission to view the imported data for the validation of part numbers and supplier codes
JAMA_JAPIA	The permission to create and edit JAMA/JAPIA datasheets including import and export
MACSI	The permission to create and edit MACSI datasheets and upload them to the MACSI portal
MNS	The permissions for MNS module
MNS_EDIT	The permission to edit multi numbers (MNS)
MNS_IMPORT	The permission to import multi number (MNS) files
OTHER	The permissions for miscellaneous operations
ANALYSIS	The permissions for analysis
COMPARE	The permission to compare multiple MDSs/Car Models/VPMs

Permission Name	Description
SHOW_ANALYSIS	The permission to perform an analysis
USAGE_ANALYSIS_SCHEDULE	The permission to schedule jobs in usage analysis (start date and time)
EVENT	The permission to create and edit LCM and SPM events for the own user
IMDS_INBOX_HISTORY	The permission to access history of the received MDS
MDS_PRINT	The permission to print a MDS/module with “Print Report”
PRODUCT_CHAIN_MODULE	The permission to change "Product Chain" information
OPEN_LARGE_MDS	The permission to completely open a large datasheet regardless of configuration parameter FILTER_NODE_COUNT_TRESHOLD
RECHECK_SUPPLIER_MDSS	The permission to start re-check of received supplier MDSs from received panel
REPORTS	The permission to access reports
SUBSTANCE_SEARCH_WITH_PORTFOLIO	The permission to perform usage analysis with cross-check to portfolio system
SUPPLIER_MDS_CHECK_RESULTS_REPORT	The permission to access MDS check result report
PROGRAM_MODEL	The permissions for access to Car/Product model screen and work with it
PROGRAM_MODEL_ROADMAP_EXPORT	The permission to create roadmap export for Car/Product model
PROGRAM_MODEL_SEARCH	The permissions to perform a search in Car/Product model screen
PROGRAM_MODEL_SUPPLIER_LIST	The permissions to open MDS List for Car/Product model
REACH_FOR_PRODUCTS	The permissions for REACh for Products
REACH_ANALYSE	The permission to perform evaluation analysis for REACh
REACH_EDIT	The permission to edit REACh data
REACH_VIEW	The restriction to use REACh in read only mode
REACH_REQUEST	The permission to create, edit, delete or send REACh request
READ_ONLY	The restriction to use the application in a read only mode
SEARCH	The permissions to perform search
IHS_MUST_NOT_ENTER_SEARCH_CRITERIA	The permission to perform search without entering any search criteria

Permission Name	Description
SEARCH_COMPONENT	The permission to search for components
SEARCH_INBOX	The permissions to use the search for the received MDS and to restrict, which received MDS are shown. If user does not have any of following permissions, the tab “Received” is not visible for him
LOAD_MDS_RECEIVED	The permission to load MDSs from the Received panel
RECEIVED_INCLUDE_CONTACT_DETAILS	The permission enables to see "Contact person" and "Email Address" columns in the result grid in the "Received" panel.
TO_ALL_OTHER_ORG_UNITS	The permission to search for MDSs, which were sent to all other organization units of the company (own and organization unit of company are not included, depending on permissions TO_OWN_ORG_UNIT and/or TO_COMPANY_ORG_UNIT)
TO_COMPANY_ORG_UNIT	The permission to search for MDSs, which were sent to the any organization unit of own company
TO_OWN_ORG_UNIT	The permission to search for MDSs, which were sent to the organization unit the user is assigned to
SEARCH_MATERIAL	The permission to search for materials
SEARCH_MDS_MODULE	The permission to search for MDSs/modules
SEARCH_RECEIVED_VP	The permission to search for received MDS in VPs
SEARCH_SEMI_COMPONENT	The permission to search for semicomponents
SEARCH_SENT	The permissions to use the search for the sent MDS. If user does not have any of following permissions, the tab “Sent” is not visible for him
LOAD_MDS_SENT	The permission to load MDSs from the search result in "Sent" tab
SENT_INCLUDE_CONTACT_DETAILS	The permission enables to see "Contact person" and "Email Address" columns in the result grid in the "Sent" panel.
SEARCH_OUTBOX	The permission to search for sent MDS
SEARCH_SUBSTANCE	The permission to search for substances
SEARCH_VOLUME	The permissions to search for with unlimited row fetch count

Permission Name	Description
COMPLETE_MDS	The permission to search for component, semicomponent, material, MDS/module with unlimited row fetch count
COMPLETE_RECEIVED	The permission to search for received MDSs with unlimited row fetch count
COMPLETE_SENT	The permission to search for sent MDSs with unlimited row fetch count
COMPLETE_USAGEANALYSIS	The permission to search in usage analysis with unlimited row fetch count
SHOW_SUBSTANCES	The permissions to shown/hide basic substances in the tree. If all basic substances should be displayed both permissions have to be selected (default selection).
SHOW_GADSL_SUBSTANCES	The permission to see the basic substances, which are marked as declarable or prohibited by the GADSL list
SHOW_OTHER_SUBSTANCES	The permission to see the basic substances, which do not have GADSL marking
SPECIAL	The permissions for special operations
EDIT_SUBSTANCES_NORMS	The permission to edit own substances and norms
EDIT_TRANSFER_KENNZ	The permission to send a MDS to recipients one by one
MATERIAL_ANALYSIS	The permission to perform material analysis
PDM_EXPORT_LIST	The permission to start a PDM export list
PROBLEM_SOLVING	The permissions to define and edit problem solving flag
MDS_PROBLEM_SOLVING	The permission to edit problem solving flag in MDS
RECOM_SPM_UPDATE_REPORT	The permission to request updates those MDS, which do not meet the current recommendations
REPLACE	The permission to manually assign MDS to missing positions
VALIDITY	The permission to use the validity report

Table 2 Permissions for iMDS_IHS

4.1.3.3.2 iMDS_LM

Permission Name	Description
LM	The permission to use LCM module
LM_ADMIN	The permission to administer all LCM requests This permission is currently used only by LCM web application
LM_DELETE	The permission to delete LCM request
LM_IMDS_UPLOAD	The permission to upload and update an IMDS request in IMDS online system
LM_IMPORT	The permission to perform import to create LCM requests This permission is currently used only by LCM web application
LM_MANAGE_DOCUMENTS	The permission to add, edit and delete documents for a LCM request
LM_READ_ONLY	The restriction to use the LCM module in a read only mode
LM_SHOW_MDS_DETAILS	The permission to open a datasheet assigned to LCM request directly from the request

Table 3 Permissions for iMDS_LM

4.1.3.3.3 iMDS_SCM

Permission Name	Description
SCM	The permission use SCM/USC module
SCM_READ_ONLY	The restriction to use the SCM/USC module in a read only mode
SHOW_MDS_DETAILS	The permission to open a datasheet (only for web client)

Table 4 Permissions for iMDS_SCM

4.1.3.3.4 iMDS_SPM

Permission Name	Description
SPM	The permission to use SPM module
SPM_ASSIGN_MDS	The permission to assign MDS to a SPM request
SPM_BULK_EDIT	The permission for editing more than one SPM requests at once
SPM_COPY	The permission to copy SPM request
SPM_DELETE	The permission to delete SPM request
SPM_EDIT	The permission to edit SPM request
SPM_IMDS_UPLOAD	The permission to send a request to IMDS online system, i.e. to create IMDS requests
SPM_READ_ONLY	The restriction to use the SPM module in a read only mode
SPM_REQUEST_FROM_EXISTING_MDS	The permission to create SPM request from received MDS
SPM_SHOW_MDS_DETAILS	The permission to open a datasheet assigned to the SPM request directly from the request

Table 5 Permissions for iMDS_SPM

4.1.3.3.5 iMDS_VC

Permission Name	Description
VC	The permission to use IHS in a web client

Table 6 Permissions for iMDS_VC

4.1.3.3.6 iPCA_ADMIN

Permission Name	Description
ADMIN_CC	The permissions for CSI management
CC_MANAGEMENT	The permission to maintain compliance checker rules, rule groups, etc.
CC_DEVELOPMENT	The permission to create own rules and rule groups
ADMIN_CHECK_CONFIG	The permission to edit existing check configurations and to create and edit new configurations
ADMIN_CLASSIFICATIONS	The permission to manage material classifications
ADMIN_IHS_CLASSIFICATION	The permission to view the VDA Classifications and managing own material classifications.
EDIT_IMDS_CLASSIFICATION	The permission to change ISO classification for selected VDA classification provided by IMDS.
ADMIN_COMPANIES	The permissions to manage master data for companies
EXAMINATION_OFFICE_MANAGEMENT	The permission to define an examination office. Furthermore the user can give an organization based approval for SAM-M object. Detailed information can be found in the SAM-M usermanual.
IHS_COMPANIES_MANAGEMENT	The permission to create and edit own companies (IHS Companies and Legal Units)
IHS_COMPANIES_MANAGEMENT_CREATE	The permission to create companies in the company master data panel located under Extras > Master Data > Companies / legal units / contacts
IHS_COMPANIES_MANAGEMENT_DELETE	The permission to delete companies in the company master data panel located under Extras > Master Data > Companies / legal units / contacts
IHS_COMPANIES_MANAGEMENT_EDIT	The permission to edit and save companies in the company master data panel located under Extras > Master Data > Companies / legal units / contacts

Permission Name	Description
IHS_COMPANIES_MANAGEMENT_VIEW	The permission to view companies and access the company search located under: Extras > Master Data > Companies / legal units / contacts
IHS_CONTACT_MANAGEMENT	The permission to create and edit companies's contacts
IHS_CONTACT_MANAGEMENT_CREATE	The permission to create new company contacts
IHS_CONTACT_MANAGEMENT_DELETE	The permission to delete company contacts
IHS_CONTACT_MANAGEMENT_EDIT	The permission to edit company contacts
IHS_CONTACT_MANAGEMENT_VIEW	The permission to search and view company contacts
ADMIN_DB	The permission to see tab “Database administration” in the management. This will enable to see DB user sessions and installed DB jobs.
ADMIN_DMM	The permission to access the configuration dialog of the document management module (DMM)
ADMIN_EXTERNAL_IHS_DB	The permission to administrate the external IHS DB interface
ADMIN_EXTIHS_EDIT	The permission to administrate the configuration of external IHS DB interface
ADMIN_EXTIHS_SHOW	Permission for only viewing the configuration of external IHS DB interface
ADMIN_GEO_ORG_DATA	The permission to manage region and organization master data
ADMIN_IHS_SUBSTANCES_NORMS	The permission to manage own substances and norms
ADMIN_IHS_SUBSTANCEGROUPS_TYPES	The permission to manage substance group types and substance groups
ADMIN_IHS_WASTE_CATALOGUES	The permissions to administrate the waste catalogues
ADMIN_IHS_WASTE_CATALOGUE	The permission to edit the waste catalogue entries
ADMIN_IHS_WASTE_CATALOGUE_GROUPS	The permission to edit the waste catalogue group entries
ADMIN_HAZARD_CLASSIFICATION	The permissions to access to the master data dialogs which are needed for the hazard classification management
HAZARD_CLASSIFICATION_VIEW	The permission to search and view master data of hazard classification
HAZARD_CLASSIFICATION_VIEW_EDIT	The permission to search and edit master data of hazard classification
ADMIN_JOBS	The permissions for job management

Permission Name	Description
JOB_ACCESSORY	The permission to allow search for frontend and backend (e.g. DWH) jobs
JOB_ADMIN	The permission to allow delete, cancel and view results of all jobs. If the user has this permission no other of the following permissions is necessary.
JOB_CANCEL	The permission to cancel active jobs, which are created/started by the actual user.
JOB_DELETE	The permission to allow delete own, finished jobs.
JOB_PHYSICALLY_DELETE	The permission to physically delete DB job from the database including its content
JOB_PRIORITY_CHANGE	The permission to change the priority of the DB job
JOB_RESULT	The permission to view and save the result of own jobs.
JOB_START_USERJOB	The permission to start predefined jobs for the user
ADMIN_LM	The permission to access LCM Parameter screen
ADMIN_PASSWORD_MANAGEMENT	The permission to access Password Security parameter screen
ADMIN_PHYS_TECH_PROPERTIES	The permissions to access to the master data dialogs which are needed for the Technical-/Physical properties management
PHYS_TECH_PROPERTIES _VIEW	The permission to search and view master data of Technical-/Physical properties management
PHYS_TECH_PROPERTIES _VIEW_EDIT	The permission to search and edit master data of Technical-/Physical properties management
ADMIN_REACH	The permissions for REACh masterdata management
ADMIN_REACH_APPLICATION	The permission to manage applications master data for REACh
ADMIN_REACH_LEGAL_UNIT	The permission to manage master data for legal units
ADMIN_REACH_REQUEST	The permission to manage REACh requests parameter
ADMIN_REGIONS	The permissions for regions and region types masterdata management
REGION_VIEW	This permission enables the user to view the existing regions in iPCA
REGION_VIEW_EDIT	This permission enables the user to create, edit or disable regions
REGION_TYPES_VIEW	This permission enables the user to view the existing region types

Permission Name	Description
REGION_TYPES_VIEW_EDIT	This permission enables the user to create, edit or disable region types
ADMIN_REPORTS	The permissions to administrate the reports
ADMIN_REACH_REPORT	The permission to access REACH report
ADMIN_ROHS_REPORT	The permission to access RoHS report
ADMIN_SEP	The permissions to edit the SEP Parameter panel
ADMIN_SEP_PDM_INTERFACE	The permission to manage PDM interface for SEP
ADMIN_SPM	The permission to access SPM Parameter screen
ADMIN_STORAGE_CLASS	The permissions to access the master data dialog for storage class management
ADMIN_STORAGE_CLASS_VIEW	This permission enables the user to search and view master data of storage classes
ADMIN_STORAGE_CLASS_VIEW_EDIT	This permission enables the user to search and edit master data of storage classes
ADMIN_USC_REJECT_REASONS	The permission to manage USC standard reject reasons
ADMIN_USER_DEACTIVATION	The permission to manage automated user deactivation
ADMIN_WEB_CLIENT	The permissions to administrate the iPCA Web Module
ADMIN_WEB_CLIENT_INTERFACE	The permission for administration access for the iPCA Web Module
CONFIG_TOOL	The permissions to manage own or company check configurations
CONFIG_COMPANY	The permission to edit configuration for own company
CONFIG_ORGANISATION	The permission to edit configuration of own organization units
CONFIG_USER	The permission to change the user own configuration
EDIT_REJECT_REASON_TEXTS	The permission to edit messages for reject reasons
KILL_MY_OWN_SESSION	The permission to cancel search in standard search screens
KILL_FOREIGN_SESSION	The permission to cancel and kill a database connection of other users. A database administration role must be mapped to the user himself.
MANAGE_IPCA_RRR_PARTTYPE	The permission to use the part types matching
USER_MANAGEMENT	The permission to control access rights for all users

Permission Name	Description
USER_MANAGEMENT_CREATE_USER	The permission to create or copy user accounts
WMS_MANAGEMENT	The permission to configure workflows

Table 7 Permissions for iPCA_ADMIN

4.1.3.3.7 iPCA_GENERAL

Permission Name	Description
EXPORT	The export permissions
SUPPLIER_COMPANY_EXPORT	The permission to export companies and organization units from iPCA
SUPPLIER_CONTACT_EXPORT	The permission to export companies and organization units with their contacts from iPCA
EXTERNAL_IHS_DB	The permissions for exteral IHS module
EXTIHS_EDIT_MATCH	The permission to access and manage data in the the external IHS matching table
EXTIHS_SHOW_MATCH	The permission to access external IHS matching table in read only mode
IMPORT	The import permissions
SUPPLIER_CONTACT_IMPORT	The permission to import supplier contacts
MASTER_DATA	The permissions to access and manage "Master Data" panels
PLANTS_VIEW	The permission to access Plants master data panel in read-only mode
PLANTS_VIEW_EDIT	The permission to access Plants master data panel and administer the data
PROJECTS_VIEW	The permission to access Projects master data panel in read-only mode
PROJECTS_VIEW_EDIT	The permission to access Projects master data panel and administer the data
REGIONS	The permissions for handling of region information at MDS
REGION_MDS_VIEW	The permission to view region information at MDS
REGION_MDS_VIEW_EDIT	The permission to edit region information at MDS

Permission Name	Description
PRODUCT_DEFINITION_LOOKUP	The permission group to access Organization Structure related data (Divisions, Business Units, Product Group, Plants)
PRODUCT_DEFINITION_LOOKUP_VIEW	The permission that adds a section to several panels of the application (e.g. search, detail views) to lookup or filter by Organization Structure related data
PRODUCT_DEFINITION_LOOKUP_VIEW_EDIT	The permission that enables import of Organization Structure related data (Divisions, Business Units, Product Groups)
REPORTS	The permissions for reports
ROHS_LETTER	The permissions for RoHS Letter creation
ROHS_LETTER_ARCHIVE	The permission to archive the RoHS Letter
ROHS_LETTER_COMPLIANCE_DATE	The permission to set the compliance date for the RoHS Letter
ROHS_LETTER_FORMAT	The permission to save the RoHS Letter as Word document
ROHS_LETTER_PRINT	The permission to create and print the RoHS Letter
REQUESTS	The permissions for requests
REQUEST_CHARTS	The permissions for equests charts
REQUEST_HISTORY_CHARTS	The permission to access charts based on historic figures of Request Data
REQUEST_REPORT_CHARTS	The permission to access charts based on the current set of selected Request Data
SORT_OUT	The permission to sort out MDS/modules, mixtures, articles, organisation units and companies
SORT_OUT_BULK	The permission to access MDS bulk deactivation feature (IMDS only)
SORT_OUT_VIEW	The permission to access hidden MDS/modules, articles, mixtures organisation units and companies in read only mode
SORT_OUT_VIEW_EDIT	The permission to sort out MDS/modules, organisation units and companies
VIRTUAL_PRODUCT_MODEL	The permissions to work with VPM
VPM_ADMIN	The permission for administration and supervisor tasks
VPM_ANALYSIS	The permission to start usage and CSI analysis for VPs

Permission Name	Description
VPM_CHARTS	The permission group to access VP charts
VPM_ACTUAL_CHARTS	The permission for charts based on the current set of Virtual Product Model Data
VPM_HISTORY_CHARTS	The permission for charts based on historic figures of Virtual Product Model Data
VPM_REPORT_CHARTS	The permission for charts based on the current set of selected Virtual Product Model Data
VPM_DS_LIST	The permissions to manage DS list
VPM_DS_ANALYSIS	The permission to trigger analysis for selected entry in DS list
VPM_DS_CREATE	The permission to create DS
VPM_DS_CREATE_IMDS_MDS	The permission to create IMDS datasheet
VPM_DS_CREATE_SAMM_MDS	The permission to create SAM-M datasheet
VPM_DS_LOAD	The permission to load DS/request for selected entry in DS list
VPM_DS_REPLACE	The permission to replace DS/request for selected entry in DS list
VPM_DS_RRR	The permission to trigger RRR analysis for selected entry in DS list
VPM_DB_VIEW	The permission to view the DS list
VPM_MAIN	The permissions to use VPM
VPM_CHANGE_LOG	The permission to access VP change log
VPM_CONVERT_TO_IMDS_DS	The permission to convert the VP to IMDS MDS/module
VPM_CONVERT_TO_SAMM_DS	The permission to convert the VP to SAM-M article
VPM_COPY	The permission to copy existing VP
VPM_CREATE	The permission to create new VP
VPM_IMPORT	The permission to create new VP by import
VPM_MANUAL	The permission to create new VP manually
VPM_DELETE	The permission to delete existing VP
VPM_DELETED_VP_REPORT	The permission to see Deleted VP Report

Permission Name	Description
VPM_DELETE_JOBS	The permission to see checkbox to delete jobs related to the VP in the VP delete dialog
VPM_EDIT	The permission to edit details of VP
VPM_LINK	The permission to link VP to another VP
VPM_PHYSICALLY_DELETE	The permission to physically delete VP from database
VPM_PUBLISH_SVHC	The permission to publish SVHC information to an external portal
VPM_VIEW	The restriction to use the VPM in a read only mode
VPM_PARTS_LIST	The permissions to manage parts list
VPM_PARTS_ADD	The permission to add a new part to the parts list
VPM_PARTS_COPY	The permission to copy an existing part in the parts list
VPM_PARTS_DELETE	The permission to delete an existing part from the parts list
VPM_PARTS_EDIT	The permission to edit an existing part from the parts list
VPM_PARTS_VIEW	The permission to view the part list
VPM_PDM	The permissions to manage PDM VP import configuration panel
VPM_PDM_ADMIN	The permission to access and manage data in the PDM VP import configuration panel
VPM_PDM_VIEW	The permission to access PDM VP import configuration panel in read only mode

Table 8 Permissions for iPCA_GENERAL

4.1.3.3.8 PTS

Permission Name	Description
ACCESS_TO_ADMINISTRATION_PANEL	The permission to access administration panel
ACCESS_TO_CHAMPION_ASSIGNMENT	The permission to access champion assignment
ACCESS_TO_DATA_COLLECTOR_ASSIGNMENT	The permission to access data collector assignment

Permission Name	Description
ASSEMBLIES	The permissions for assembly managements
CREATE_ASSEMBLIES	The permission to create assemblies
DELETE_ASSEMBLIES	The permission to delete assemblies
EDIT_ASSEMBLIES	The permission to edit assemblies
VIEW_ASSEMBLIES	The permission to see assemblies
CHANGE_RESPONSIBLE_CHAMPION	The permission to change responsible champion
COMPONENTS	The permissions for component management
CREATE_COMPONENTS	The permission to create components
DELETE_COMPONENTS	The permission to delete components
EDIT_COMPONENTS	The permission to edit components
VIEW_COMPONENTS	The permission to see components
PROGRAMS	The permissions for Program Management
CREATE_PROGRAMS	The permission to create programs
DELETE_PROGRAMS	The permission to delete programs
EDIT_PROGRAMS	The permission to edit programs
VIEW_PROGRAMS	The permission to see programs
PTS_ACCESS_TO_UNASSIGNED_SUPPLIERS	The permission to access the unassigned suppliers
PTS_SEARCH_REQUESTS_BY_SELECTED_REGIONS	The permission to search requests by selected regions
REPORTS	The permissions for report management
ACCESS_TO_CHAMPIONS_WORKLOAD_REPORT	The permission to access champions workload report
ACCESS_TO_DC_WORKLOAD_REPORT	The permission to access DC workload report
ACCESS_TO_SOC_REPORT	The permission to access SoC report
REQUESTS	The permissions for request management
ADD_BOM_FILES	The permission to add BoM files

Permission Name	Description
CHANGE_REQUEST_STATUS	The permission to change request status
CREATE_REQUESTS	The permission to create requests
DELETE_REQUESTS	The permission to delete requests
EDIT_FOREIGN_REQUESTS	The permission to edit foreign requests
EDIT_OWN_REQUESTS	The permission to edit own requests
IMPORT_BOM_FILES	The permission to import BoM files
LOCK_REQUESTS	The permission to lock requests
REJECT_REQUESTS	The permission to reject requests
VIEW_REQUESTS	The permission to see requests
SEARCH	The permissions for search
SEARCH_FOR_ASSEMBLIES	The permission to search for assemblies
SEARCH_FOR_CONTROL_FILES	The permission to search for control files
SEARCH_FOR_PARTS	The permission to search for parts
SEARCH_FOR_PLANTS	The permission to search for plants
SEARCH_FOR_PROGRAMS	The permission to search for programs
SEARCH_FOR_REQUESTS	The permission to search for requests
SEARCH_FOR_SUPPLIERS	The permission to search for suppliers
USE_PS_APPLICATION	The permission to PTS

Table 9 Permissions for PTS

4.1.3.3.9 RRR/LCA

Permission Name	Description

Permission Name	Description
CALCULATE_LCA	The permission to perform LCA calculations
CALCULATE_RRR	The permission to calculate a RRR product model
DELETE_RRR_PRODUCT_MODEL	The permission to delete RRR product model
EDIT_LCA_LIBRARY	The permission to change LCA libraries
EDIT_PRODUCT_MODEL	The permission to change a RRR product model
EDIT_RRR_EXTENDED_LIBRARY	The permission to use the extended version of the recycling profile library editor
EDIT_RRR_LIBRARY	The permission to edit RRR libraries (e.g. material library)
MANAGE_IPCA_RRR_PARTTYPE	The permission to preselect an EOL profile before starting the RRR client
READ_LCA_RESULTS	The permission to open existing LCA results
READ_RRR_RESULTS	The permission to open existing RRR results (e.g. reports)
RELEASE_PRODUCT_MODEL	The permission allowing to release RRR product model

Table 10 Permissions for RRR/LCA

4.1.3.3.10 SAMM

Permission Name	Description
ADD_DOCUMENTS	The permission to access and manage tab “Documents” in Mixture/Article
ADMIN	The permissions to manage the SAMM application
ADMIN_EVENT	The permission to create and edit SEP events for all users
ANALYSIS	The permissions for analysis of SAM-M data
SHOW_ANALYSIS	The permission to perform an analysis
USAGE_ANALYSIS_SCHEDULE	The permission to schedule jobs in usage analysis (start date and time)
BLACKLIST	The permissions for Blacklist module

Permission Name	Description
BLACKLIST_EDIT	The permission to edit blacklist entries for BoM import
BLACKLIST_VIEW	The permission to view blacklist entries for BoM import
COMPLIANCE_CHECKER	The permission group for CSI checks
CC_CHECK	The permission to check MDS using released compliance checker groups
CC_CHECK_CONFIG	The permission to make the rule groups available in different check configurations (e.g. USC)
CC_CYCLIC_JOB	The permission to create reoccurring CSI check jobs
CC_EXPORT	The permission to export the rule groups into the exchange format
CC_IMPORT	The permission to import rule groups in the exchange format
CC_INSPECTOR	The permission to check MDS using all compliance checker groups (even if not yet released)
CC_MONITORING	The permission to set the monitoring option for a scheduled CSI job
CC_RESULT_TO_VPM	The permission to create VP from the results of the SAM-M CSI analysis
CC_SCHEDULE_JOB	The permission to schedule background jobs in CSI wizard (start date and time)
EDIT	The permissions for edit of SAM-M objects and data
ARTICLE_DETAILS	The permissions for articles
ARTICLE_ADR_CONFIRM_MIGRATED	The permission that activates checkbox on Transport tab of Article that allows to approve that UN Number data was migrated
ARTICLE_COMPLIANCE	The permission to see compliance panel for article
ARTICLE_COMPLIANCE_INFO	The permission to see the compliance info panel for articles
ARTICLE_DISPOSAL	The permission to see disposal panel for article
ARTICLE_DOCUMENTATION	The permission to see documentation panel for article
ARTICLE_DOCUMENTATIONS	The permissions for actions in documentation panel for articles
ARTICLE_DOCUMENT_NAME	The permission to edit the documents name.

Permission Name	Description
ARTICLE_FROZEN_DOCUMENT_NAME	The permission to edit the documents name even if the document is read only
ARTICLE_HAZARD_CHARACTERISATION	The permission to see hazard characterization panel for article
ARTICLE_USAGE_SCOPE	The permission to see waste and usage scope panel for article
SAMM_ARTICLE_HISTORY	The permission to show the history tab for articles in the REACh worksheet
CREATE	The permissions to create new SAM-M objects
COPY_ARTICLE	The permission to copy articles
COPY_MIXTURE	The permission to copy mixtures
CREATE_ARTICLE	The permission to create article
CREATE_MIXTURE	The permission to create mixture
CREATE_SEP_REQUEST	The permission to create SEP requests
CREATE_SURFACES	The permission to define a mixture as a surface
COPY_SEP_REQUEST	The permission to copy SEP requests
REACTIVATE_ARTICLE	The permission to reactivate a deactivated article
REACTIVATE_MIXTURE	The permission to reactivate a deactivated mixture
DELETE	The permissions for deletion of articles/mixtures/substances which are not internally released
DELETE_ARTICLE	The permission to delete articles
DELETE_MIXTURE	The permission to delete mixtures
DELETE_SUBSTANCE	The permission to delete substances
EDIT_SEP_REQUEST	The permissions to access SEP (Supplier Entry Portal)
ASSIGNED_RULE_GROUPS	The permission to see group tab for SEP requests
DOCUMENTS	The permission to see documents tab for SEP requests
MAIN_DATA	The permission to see SEP request main details
PROCESS_TYPE_CHANGE	The permission to change the process type of a request

Permission Name	Description
IHS_NUMBER	The permissions to edit the IHS item number
IHS_NUMBER_ARTICLE	The permission to edit the IHS item number in the SAM-M datasheet of type article
IHS_NUMBER_MIXTURE	The permission to edit the IHS item number in the SAM-M datasheet of type mixture
MIXTURE_DETAILS	The permissions for mixtures
MIXTURE_ADR_CONFIRM_MIGRATED	The permission that activates checkbox on Transport tab of Mixture that allows to approve that UN Number data was migrated
MIXTURE_CLASSIFICATION_AND_LABELLING	The permission to see classifications and labeling panel for mixture
MIXTURE_COMPLIANCE	The permission to see compliance panel for mixture
MIXTURE_COMPLIANCE_INFO	The permission to see the compliance info panel for mixtures
MIXTURE_DOCUMENTATION	The permission to see documentation panel for mixture
MIXTURE_DOCUMENTATIONS	The permissions for actions in documentation panel for mixtures
MIXTURE_DOCUMENT_NAME	The permission to edit the documents name
MIXTURE_FROZEN_DOCUMENT_NAME	The permission to edit the documents name even if the document is read only
MIXTURE_DISPOSAL	The permission to see disposal panel for mixture
MIXTURE_GHS_CLASSIFICATION_AND_LABELLING	The permission to see GHS classification and labeling panel for mixture
MIXTURE_HAZARD_CHARACTERISATION	The permission to see hazard characterization panel for mixture
MIXTURE_TRANSPORT	The permission to see transport panel for mixture
MIXTURE_USAGE_SCOPE	The permission to see waste and usage scope panel for mixture
SAMM_MIXTURE_HISTORY	The permission to show the history tab for mixtures in the REACh worksheet
REACH_REQUEST	The permission to create, edit, delete or send REACh request
REPLACE_MSP	The permission to show MSP in a tree and to replace an MDS with a MSP (if possible)
SEP_REQUESTS	The permission group for handling SEP requests
SEP_ACCEPT_REJECT_REQUEST	The permission to accept or reject a SEP request
SEP_CANCEL_REQUEST	The permission to cancel a SEP request

Permission Name	Description
SEP_DELETE_REQUEST	The permission to delete a SEP request
SEP_RE-REQUEST	The permission to request a SEP request again
SEP_SDS_EXPORT	The permission to export SDS files to an external SDS service provider
SEP_SDS_PUBLISH	The permission to publish SDS files to an (public) portal
SEP_SEND_REQUEST	The permission to dispatch a SEP request respectively SEP email
SEP_SET_EXT_ADVICE	The permission to request external advice from a third party
SEP_SET_EXT_ADVICE_COMPLETE	The permission to answer a request for an external advice
SHOW_MSP	The permission to show available MSP in a tree
VALIDITY_MANAGEMENT	The permission to change "valid until" date of already released products
IPC1752_EXPORT	The permission to export a structure (like an article) to an IPC1752 XML file
IMPORT	The permission to be able to do imports
COMMODITY_IMPORT	The permission for commodity import
SUPPLIER_IMPORT	The permission for supplier import
MDS_PRINT	The permission to print a safety data sheet
MNS	The permissions for MNS module
MNS_EDIT	The permission to edit multi numbers (MNS)
MNS_IMPORT	The permission to import multi number (MNS) files
OTHER	The permissions for miscellaneous operations
EVENT	The permission to create and edit SEP events for the own user
PROGRAM_MODEL	The permissions for access to Car/Product model screen and work with it
CREATE_PRODUCT_FROM_ARTICLE	The permission to create a product from an article
PROGRAM_MODEL_ROADMAP_EXPORT	The permission to create roadmap export for Car/Product model
PROGRAM_MODEL_SEARCH	The permissions to perform a search in Car/Product model screen

Permission Name	Description
PROGRAM_MODEL_SUPPLIER_LIST	The permissions to open MDS List for Car/Product model
RELEASE	The permissions to release articles and mixtures
RELEASE_ARTICLES	The permissions to release article
RELEASE_MIXTURES	The permissions to release mixture
REPORTS	The permission to access SAMM reports
SEARCH	The permission for searching special SAM-M objects
SEARCH_ARTICLE	The permissions for search of articles
IHS_ARTICLE_RELEASE_STATES	The permission to see the articles based on their IHS release state
ARCHIVED_ARTICLE	The permission to set IHS release status "Archived" for an article
LOCKED_ARTICLE	The permission to set IHS release status "Locked" for an article
NOT_RELEASED_ARTICLE	The permission to set IHS release status "Not released" for an article
PROHIBITED_ARTICLE	The permission to set IHS release status "Prohibited" for an article
RELEASED_ARTICLE	The permission to set IHS release status "Released" for a mixture
RESTRICTED_ARTICLE	The permission to set IHS release status "Restricted" for an article
SEARCH_DOCUMENTS	The permissions to search documents
SEARCH_MIXTURE	The permissions for search of mixtures
ALL_ORG_UNIT_ASSIGNED_DATA	The permission to see mixtures, which are assigned to any organisation unit
IHS_MIXTURE_RELEASE_STATES	The permission to see the mixtures based on their IHS release state
ARCHIVED_MIXTURE	The permission to set IHS release status "Archived" for a mixture
LOCKED_MIXTURE	The permission to set IHS release status "Locked" for a mixture
NOT_RELEASED_MIXTURE	The permission to set IHS release status "Not released" for a mixture
PROHIBITED_MIXTURE	The permission to set IHS release status "Prohibited" for a mixture
RELEASED_MIXTURE	The permission to set IHS release status "Released" for a mixture

Permission Name	Description
RESTRICTED_MIXTURE	The permission to set IHS release status "Restricted" for a mixture
ONLY_RELEASED_FOR_OWN_ORG_UNIT	The permission to see mixtures, which are released and assigned to users organisation unit
OWN_ORG_UNIT_ASSIGNED_DATA	The permission to see mixtures, which are assigned to users organisation unit
SEARCH_SURFACES	The permission to search for surfaces
SEARCH_SEP_REQUEST	The permission to search for SEP requests
SEARCH_SUBSTANCE	The permission to search substances
SEP	The permission to access SEP (Supplier Entry Portal)
SEP_CYCLE_TIME	The permission to create SEP CYCLE TIME report
SHOW_SUBSTANCES	The permissions to shown/hide basic substances in the tree. If all basic substances should be displayed both permissions have to be selected.
SHOW_CONFIDENTIAL_SUBSTANCES	The permission to see confidential substances
SHOW_OTHER_SUBSTANCES	The permission to all other substances
VIEW	The restriction to see SAM-M objects and data in read only mode: Important note: This permission overwrites all other REACh edit permissions.

Table 11 Permissions for SAMM

4.1.3.3.11 THIN_CLIENT

Permission Name	Description
SHOW_CAR_MODEL	The permission to see Car/Product model in the thin client
SHOW_JOB_HISTORY	The permission to see job history in the thin client

Table 12 Permissions for THIN_CLIENT

4.2 Application configuration

Some configuration parameters for the applicable can be changed in the "**Configuration**" tab (see **Figure 18**).

The configuration tab is split into four areas:

1. Search mask (orange) – see **chapter 4.2.1.1**
2. Result list (blue) – see **chapter 4.2.1.2**
3. Interactive area with details of a configuration parameter selected in result list (green) – see **chapter 4.2.1.3**
4. Actions (black) – see **chapter 4.2.1.4**

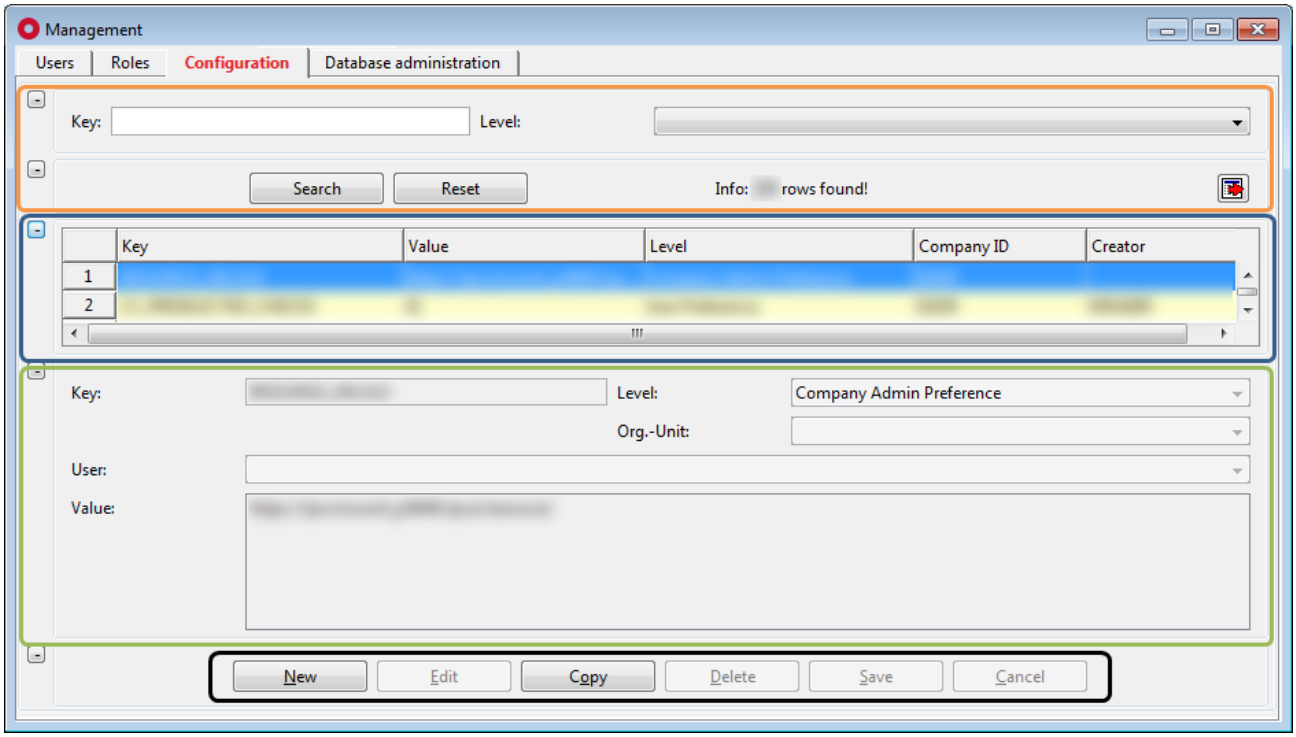

Figure 18 Configuration tab

4.2.1.1 Search mask

Enables the configuration parameter to be quickly found; which key matches with the search criteria entered into the search fields.

The drop-down list "**Level**" contains three values representing the types of the configuration parameters:

- Company Admin Preference
- Organization Admin Preference
- User Preference

The following actions are available:

- **Search**
  Perform search based on search criteria entered into the search fields
- **Reset**
  Remove entered search criteria from search fields

4.2.1.2 Result list

The result list displays configuration parameters and its details as per defined search criteria.

Please beware that configuration parameters shown in the result list may be also of different level than defined in the search mask.

The logic is defined below:

- **Company Admin Preference**
  Returns configuration parameters with levels "**Company Admin Preference**", "**Organization Admin Preference**" and "**User Preference**"
- **Organization Admin Preference**
  Returns configuration parameters with levels "**Organization Admin Preference**" and "**User Preference**"
- **User Preference**
  Returns configuration parameters with level "**User Preference**"

Upon selection of the particular configuration parameter, its details are shown also in the interactive area (see **chapter 4.2.1.3**).

4.2.1.3 Interactive area

This part displays details of a configuration parameter selected in result list or details of a new configuration parameter which is being defined.

4.2.1.4 Actions

Following actions are available:

- **New**
  Create a new configuration parameter
- **Edit**
  Edit details of a selected configuration parameter (not possible for each configuration parameter)

- **Copy**
  Create a new configuration parameter by copy of a selected configuration parameter
- **Delete**
  Delete a selected configuration parameter
- **Save**
  Save created configuration parameter or update of existing configuration parameter
- **Cancel**
  Cancel the editing or creating of a configuration parameter without saving

PLEASE NOTE: Do not create, edit or delete a configuration parameter without knowledge of administration!

4.2.1.4.1 Creating a configuration parameter

New configuration parameter can be created by clicking on the "**New**" button. This will load an empty mask for definition of a configuration parameter (see **Figure 19**). Fields highlighted in orange are mandatory and must be filled out. If these are not filled out then a new configuration parameter cannot be created.

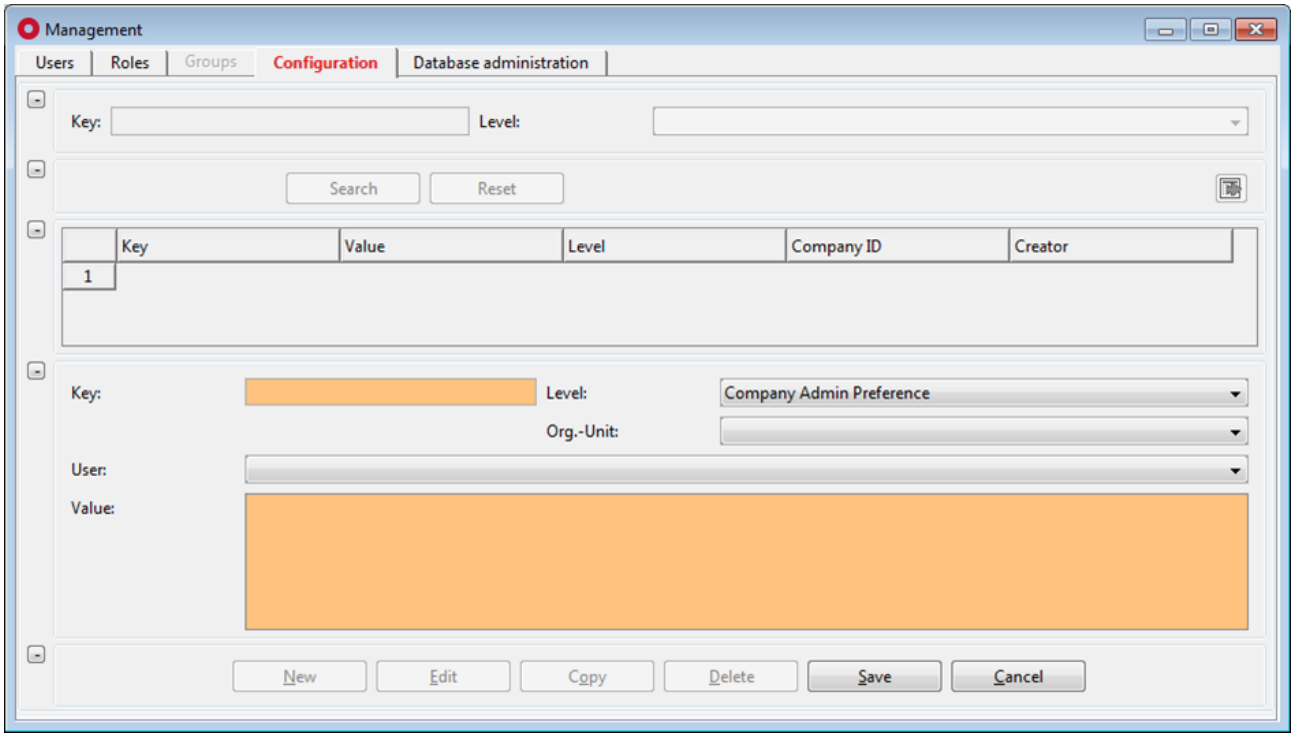

Figure 19 Creating a configuration parameter

The following information must/could be defined:

- **Key**
  Name of a configuration parameter.
- **Level**
  Level of the configuration parameter. Default value is "**Company Admin Preference**".
- **Org.-Unit**
  Organisation Unit for which the configuration parameter is valid.
- **User**
  User for which the configuration parameter is valid.
- **Value**
  Value of a configuration parameter.

In the situation where newly created configuration parameter has exactly the same values as already existing configuration parameter a notification is shown (see **Figure 20**).

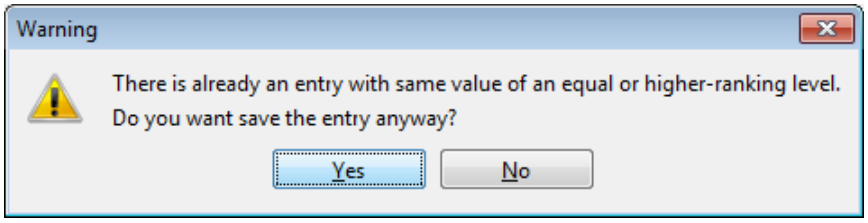

Figure 20 Notification shown if configuration parameter with the same values exists already

A user is then able to make a decision, if newly created configuration parameter can be saved as is or not.

Once all required details are defined a new configuration parameter can be created by clicking on the "**Save**" button. To cancel creation of a configuration parameter, click the "**Cancel**" button.

4.2.1.4.2 Editing a configuration parameter

The details of a selected configuration parameter can be changed by clicking on the "**Edit**" button. Once all changes are done, they can be saved by clicking on the "**Save**" button. To cancel changes, click the "**Cancel**" button.

PLEASE NOTE: It is not possible to edit all configuration parameters shown in the result list. Some of the configuration parameters are configurable from iPCA only.

4.2.1.4.3 Copying a configuration parameter

New configuration parameter can be created by copying an existing configuration parameter selected in the result list by clicking on the “**Copy**” button.

Once all changes are done, they can be saved by clicking on the “**Save**” button. To cancel changes, click the “**Cancel**” button.

4.2.1.4.4 Deleting a configuration parameter

Existing configuration parameter can be deleted by clicking on “**Delete**” button. This opens a small pop=-up window (see **Figure 21**). By clicking on the “**Yes**” button a configuration parameter will be deleted. By clicking on the “**No**” button, the configuration parameter will be kept.

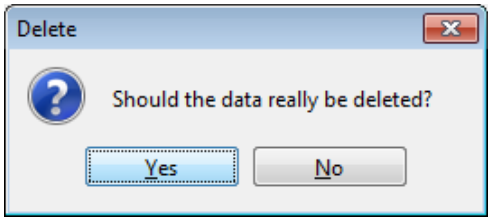

Figure 21 Confirmation of deletion of a configuration parameter

4.3 Database administration

Provides an overview about user sessions and system jobs.

There are two sub-tabs available:

- User Sessions
- User Scheduler Jobs

4.3.1 User Sessions

Provides an overview about user sessions in the application (see **Figure 22**).

The user sessions tab is split into two areas:

1. Search mask (orange) – see **chapter 4.3.1.1**
2. Result list (blue) – see **chapter 4.3.1.2**

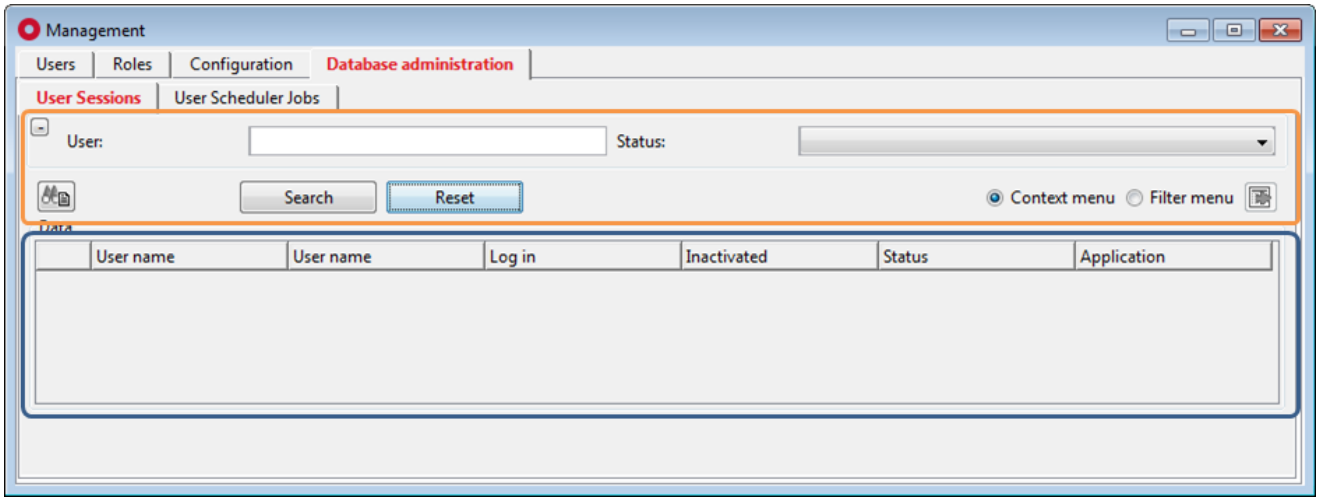

Figure 22 User Sessions tab

4.3.1.1 Search mask

Enables the quick search for a user by either username or status. Matches will be shown in the reference to the entered search criteria.

Drop-down list "**Status**" contains five values representing the possible statuses of the user session:

- active
- invalid
- inactive
- down
- maintenance

The following actions are available:

- **Search**
  Perform searches based on criteria entered into the search fields
- **Reset**
  Remove entered search criteria from search fields

4.3.1.2 Result list

The result list displays user session and its details as per defined search criteria.

It is not possible to do any action from the result list.

4.3.2 User Scheduler Jobs

Provides an overview about system jobs (see **Figure 23**).

The user scheduler jobs split into two areas:

1. Search mask (orange)
2. Result list (blue)

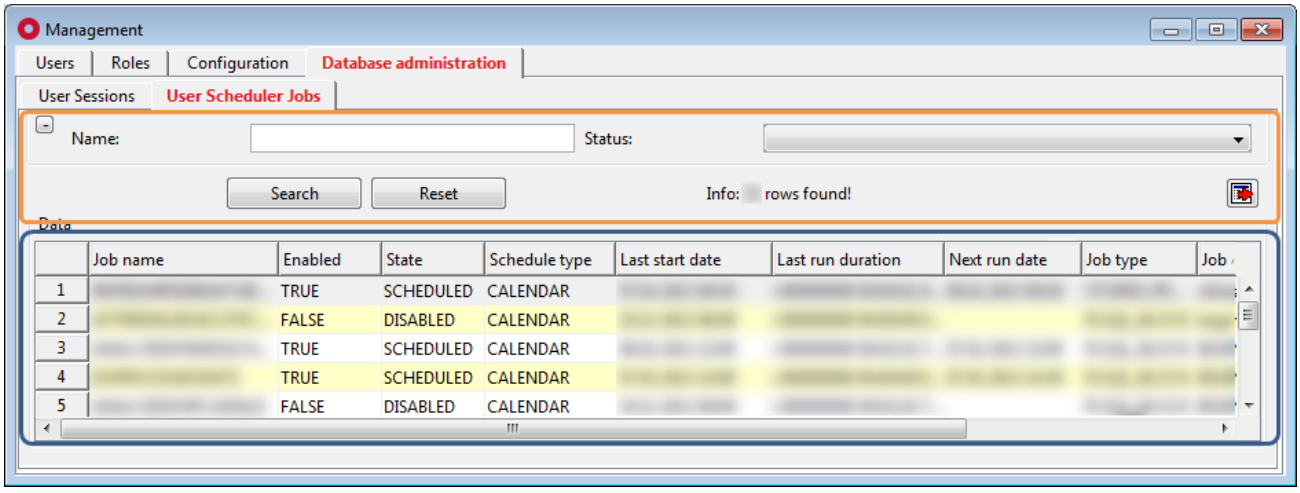

Figure 23 User Scheduler Jobs

4.3.2.1 Search mask

Enables the quick search for a job by either name or status. Matches will be shown in reference to the entered search restrictions.

Drop-down list "**Status**" contains nine values representing the possible statuses of the system jobs:

- DISABLED
- RETRY SCHEDULED
- SCHEDULED
- RUNNING
- COMPLETED
- BROKEN
- FAILED
- REMOTE
- SUCCEEDED

The following actions are available:

- **Search**
  Perform searches based on criteria entered into the search fields
- **Reset**
  Remove entered search criteria from search fields

4.3.2.2 Result list

The result list displays system jobs and its details as per defined search criteria.

It is not possible to do any action from the result list.

5 User deactivation (optional)

This optional module allows automatic deactivation of the user account after defined days of inactivity in iPCA and submission of appropriate notifications to the user and/or to company application administrators.

The panel for edit of user deactivation parameters can be accessed from menu "**Options → Parameter → User Deactivation**".

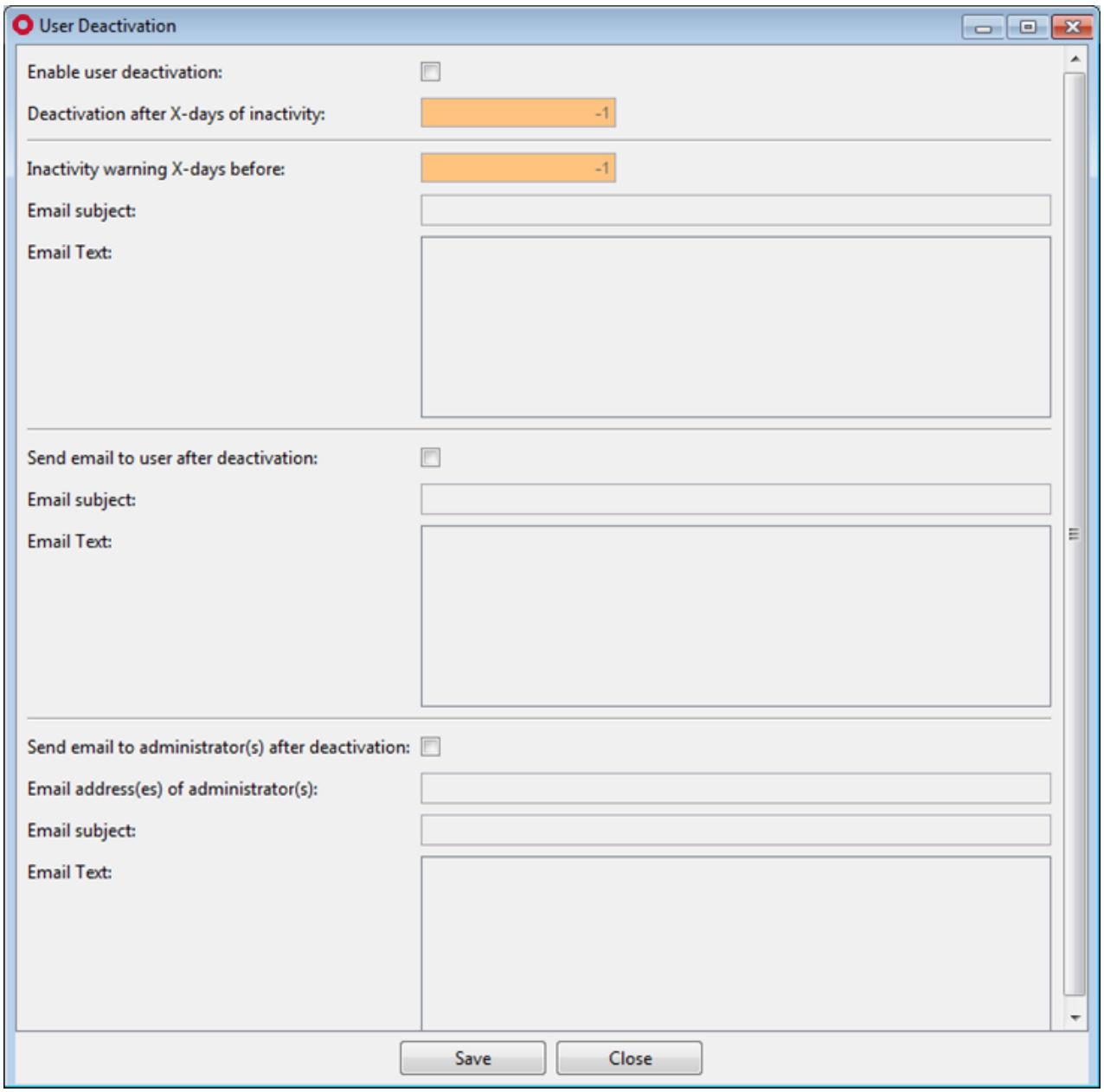

Figure 24 User Deactivation parameters screen

Following information must/could be defined:

- **Enable user deactivation**
  If this checkbox is checked, a background process will check the inactivity period for every user of the system. If a user's inactivity exceeds the defined limit defined in parameter "**Deactivation after X-days of inactivity**", his account will be deactivated (set to inactive).
  PLEASE NOTE: In case the user account is set to "**inactive**" automatically by this process, values from couple of attributes are removed (for more details see **chapter 7**).
- **Deactivation after X-days of inactivity**
  Defines the number of days after which the user account is deactivated, if user did not log into the application within this period.
  Possible values are from 1 to 1000.
- **Inactivity warning X-days before:**
  Defines the number of days before the email is send to affected user before the deactivation of his user account.
  Possible values are from 1 to 1000.
  If set to "**-1**", the notification email is not send.
- **Email subject**
  The subject of the warning email send prior to deactivation of the user account.
- **Email text**
  The body of the warning email send prior to deactivation of the user account.
- **Send email to user after deactivation**
  If this checkbox is checked, the email is send to the user upon deactivation of his user account.
- **Email subject**
  The subject of the email sent to the user upon deactivation of his user account.
- **Email text**
  The body of the email sent to the user upon deactivation of his user account.
- **Send email to administrator(s) after deactivation**
  If this checkbox is checked, the email is send to the email address(es) defined in the field "**Email address(es) of administrator(s)**" upon deactivation of any user account.
- **Email address(es) of administrator(s)**
  The email addresses of company administrators who receive summary email upon deactivation of at least one user. Email separator is a semicolon "**;**".
- **Email subject**
  The subject of the email sent to the administrator(s) upon deactivation of at least one user.

- **Email text**
  The body of the email sent to the administrator(s) upon deactivation of at least one user.
  This email contains cumulated information about all deactivated users on the particular day.
  The body of the email is automatically extended with details of deactivated user accounts:
    - User name
    - Full name
    - Email
    - Last Login Date
    - Roles

PLEASE NOTE: Only user with activated permission "**ADMIN_USER_DEACTIVATION**" can access user deactivation management.

Below iPoint technical users are automatically excluded from the user deactivation (this setting cannot be changed):

- AIMDSAD
- IFLOWBPM
- IMDSAD
- INFOPATH_WS
- SAP_JCO
- ZBMAT_INTERFACE

6 Password security (optional)

This optional module allows define the password validity and the company wide security criteria for user passwords.

The panel for edit of password security parameters can be accessed from menu "**Options → Parameter → Password Security**".

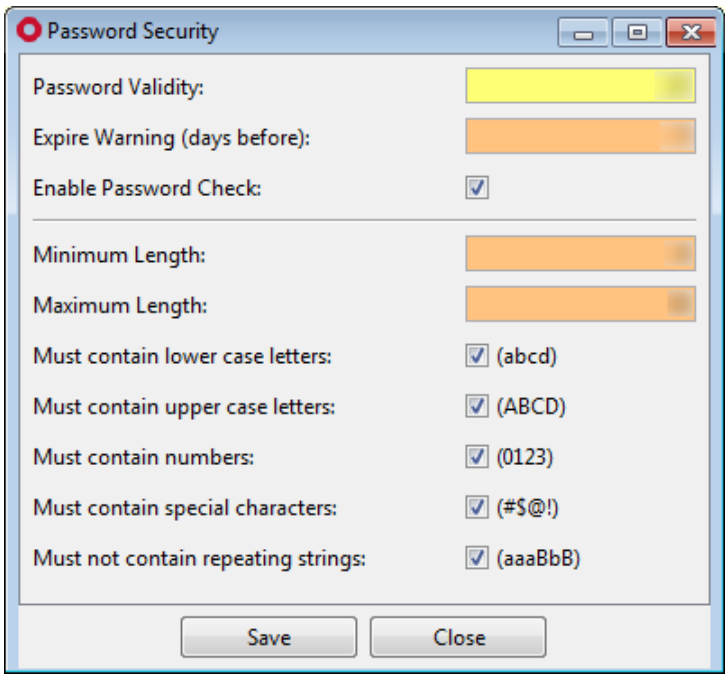

Figure 25 Password Security parameters screen

Following information must/could be defined:

- **Password Validity**
  Defines the number of days after which a password must be changed (see **Figure 26** and **Figure 27**).
  Possible values are from 1 to 365.
  If set to "**-1**", password validity check is disabled.
  PLEASE NOTE If this parameter is set for the first time, every user has to change his password on the next login.

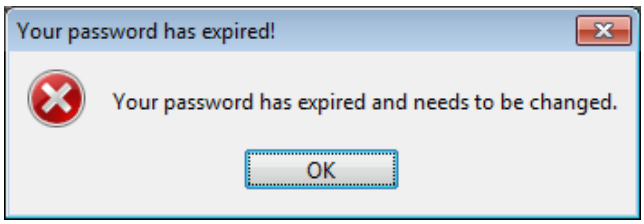

Figure 26 Notification that password has expired and must be changed

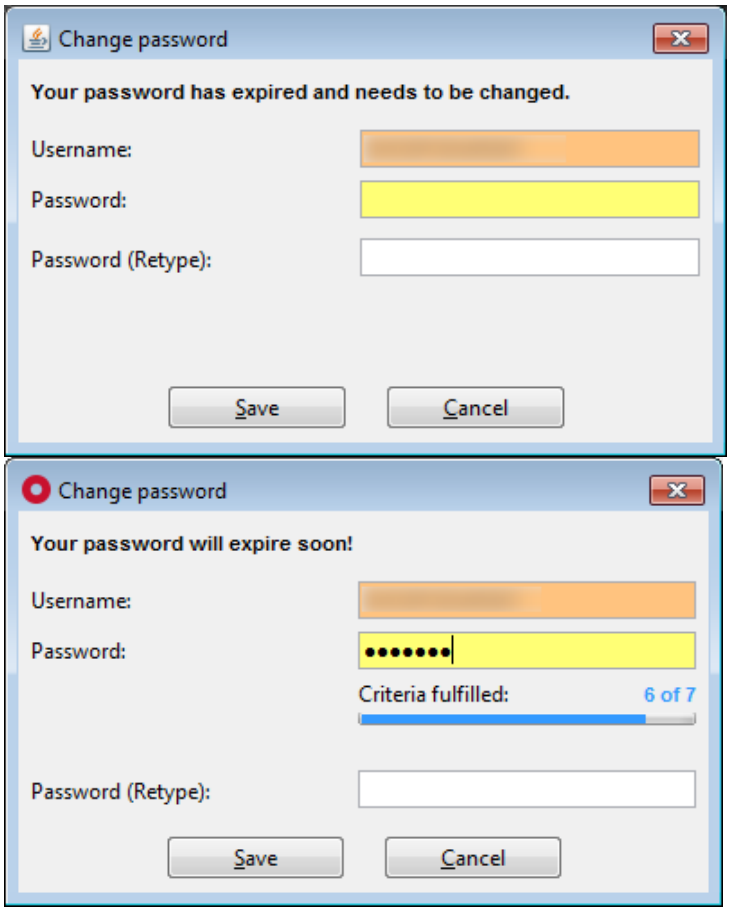

Figure 27 Panel for change of the password during login (without / with criteria)

- **Expire Warning (days before)**
  Defines the number of days the user is notified before expiration of his password (see **Figure 28**). The warning will pop up on every login until the password has been changed. By clicking on "**Yes**" the user has the option to change his password immediately. In case of click on "**No**", user can change his password either on next login of by editing of own user data (see chapter **0**).
  Possible values are from 1 to 365.
  If set to "**-1**", the notification about oncoming expiration of the password is not show to the user.

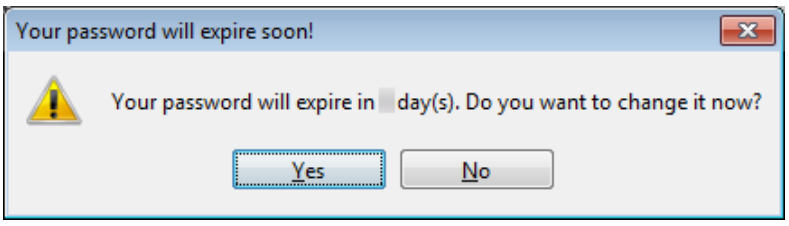

Figure 28 Dialog panel notifying that password will expire in n-days allowing its change

- **Enable password check**
  If this checkbox is checked, password must fulfil security criteria under this checkbox, which are activated
- **Minimum Length**
  Defines minimum length for a password.
  Possible values are from 4 to 99.
- **Maximum Length**
  Defines maximum length for a password.
  Possible values are from 4 to 99.
  If set to "**-1**", the length of the password is not limited.
  PLEASE NOTE: Value defined in this field cannot be smaller than the value in field "**Minimum Length**"
- **Must contain lower case letters**
  If this checkbox is checked, password must contain at least one lower case letter, e.g. abcd
- **Must contain upper case letters**
  If this checkbox is checked, password must contain at least one upper case letter, e.g. ABCD
- **Must contain numbers**
  If this checkbox is checked, password must contain at least one number, e.g. 0123
- **Must contain special characters**
  If this checkbox is checked, password must contain at least one special character, e.g. #$@!
- **Must not contain repeating strings**
  If this checkbox is checked, password must contain at least one upper case letter, e.g. ABCDE

Below iPoint technical users are automatically excluded from the password expiration (this setting cannot be changed):

- AIMDSAD
- IFLOWBPM
- IMDSAD
- INFOPATH_WS

- SAP_JCO
- ZBMAT_INTERFACE

7 Deletion of attributes on inactivation of the iPCA user account

Based on a regulation EU 2016/679 of the European Parliament, so called General Data Protection Regulation (GDPR), below iPCA user account attributes are deleted upon the profile is inactivated:

- Password
- Email
- Telephone No.
- Department
- Description
- Contact person

PLEASE NOTE: The deletion is handled by a background process that run every hour.

The iPCA user profile can be set to inactive by:

- manual edit of the user account
- deactivation job (optional)
- login of user whose account validity expired
- synchronization with user directory, e.g. LDAP
- synchronization with external system, e.g. SAP

8 Glossary

Term	Explanation
AIC	Automated Inbox Check: The pre-checking of supplier datasheets for mandatory company specific requirements
CSI	Compliance Substance Inspector
DMM	Document Management Module
iPCA	iPoint Compliance Agent
IHS	In House System
LCA	Life Cycle Assessment: The calculation from cradle to grave for products about environmental impact
LCM	Life Cycle Management (also shown as LCM). The management of data requests from customers
MCP	Material Compliance Portal
MNS	Multi Number Support
MSP	Multi Sourced Parts
PDL	Product Definition Lookup
PI	Parts Inventory
PTS	Program Tracking Support: The complete process management for programs from the request to the acceptance and statistics
PRP	Product Release Process
RRR	Recyclability, Reusability, Recoverability: The calculation of the material treatment at end-of-life of a product
SAMM	Substance, Articles, Material Management The acronym to process and manage material and substance related data
SCM	Supply Check Module: The pre-checking of supplier datasheets for IMDS recommendations
SDS	Safety Data Sheet
SEP	Supplier Entry Portal
SPM	Supply Part Management: The process to requests data from supplier

Term	Explanation
USC	User Guided Supplier Check: The pre-checking of supplier data for IMDS rules, quality, content and compliance
VC	Viewer Client: The acronym for the thin web client
VPM	Virtual Product Model: Module for handling IMDS and non-IMDS product information

Table 13 Glossary of terms used in the user manual

9 Table of tables

10 Table of figures

11 Change History

Version	Date	Description
4.02.002	24.07.2006	Complete revision
4.07	26.02.2007	Added chapter 4.1 “Common Overview” Added permissions · IMDS_Upload_Publish · MACSI
5.00	20.05.2007	Added permission JAMA_JAPIA
5.1	21.05.2007	Added configuration of application New function · Copy of user New access rights · Admin_IHS_Companies · Admin_IHS_Substances_Norms · Imds_Inbox_History · Edit_Substances_Norms
5.01.007	19.06.2007	Added new permission · Recom_SPM_Update_Report · Material_report (Optional)
5.4	11.012008	Added type information for all privileges Added visualization of user type Added export of User list Changed display of user tree Changed display of roles Added dropdown for selection of Organization Unit of user Added new permissions · Admin_ihs_substancegroups_types · Admin_jobs · Cc_management · Cc_check · Cc_inspector · Bulk_update · Admin_inbox
6.1	25.10.2008	Changes for Release 6.0 Change to iPCA
6.2	10.12.2008	Permission Admin_Inbox, replaced with new permissions: · To_Own_Org_Unit · To_Company_Org_Unit · To_All_Other_Org_Units Added new sub permissions for check of MDSs: · Own_Org_Unit · Company_ Org_Unit

Version	Date	Description
		· All_Other_Org_Units
6.3	15.01.2009	Added Note for Userright „Analysis“
7.5	15.10.2009	Added Contact name to user data
7.17	01.09.2010	New permissions Mds_Print and Show_Substances
		New permission Edit_Imds_Classification
7.18 7.08.009	20.09.2010	New permission Admin_Substitution Permissions Admin_Iacm deleted
8.00	20.12.2010	Chapter 4.5.4 renamed to iPCA_ADMIN Added new permissions: · Job_Admin · Job_Cancel · Job_Delete · CC_Development · Cc_Cyclic_Job · Cc_Check_Config · Cc_Export · Cc_Import Added new permission groups: · Admin_CC · RRR Removed permission for Honda
8.01	01.02.2011	Added several permissions
8.05	14.03.2011	New permissions for MSP (optional)
8.08	22.08.2011	Added permissions for CSI and usage list scheduling (optional)
8.09	15.10.2011	Added permission JOB_RESULT
	28.10.2011	Permission Analysis changed to group – permission itself now renamed to Show_Analysis
9.00	30.01.2012	Add Password Security visualization (optional) Add phoneNo. and signature to restricted user management New permissions for Program Tracking System and SEP
9.03	31.01.2013	Changes for selection/display of organization unit for internal or external users Added permission for SPM multi edit
9.07	07.07.2013	Added permissions added to the application since version 9.03.000 (optional)
9.10	16.08.2013	Added more granular permissions for upload to IMDS Renamed permission for multi SPM edit - SPM_BULK_EDIT
9.12	11.11.2013	Added permissions for setting archive status for articles and mixtures Minor adjustments of the texts and descriptions of some permissions

Version	Date	Description
9.14	28.02.2014	Added permission for starting usage and CSI analysis for VPs Added permission for REACH report
10.00.006	23.05.2014	Added permission for creation and copy of the user account
10.01.000	06.06.2014	Added permissions for creation of VP from CSI results (optional) Added permissions for physical deletion of VPs and deletion of jobs linked to VP (optional) Added permission for physical deletion of DB jobs including their content Added permission for re-check of already processed received MDSs (optional) Added permission for search of SAM-M documents
10.13.000	03.12.2014	Added several permissions for iPCA, SAMM and SEP features
10.24.000	15.09.2015	Migration of the user manual to new iPoint style Updated big number of figures (due to change of the iPoint logo in iPCA) Fixed some typos Added permission for administration of the document management module Added permissions for reactivation of article and mixture Added permission for RRR extended library edit Added permission for creation of a product model from article
11.00.000	08.10.2015	Added function to export permissions vs. roles matrix Fixed some typos Minor improvements in some paragraphs
11.05.000	22.12.2015	Added permission for quality check of the datasheet Renamed permission for recommendation check of the datasheet
11.08.000	21.03.2016	Moved permission group “VIRTUAL_PRODUCT_MODEL” under the new permission parent group “iPCA_GENERAL” Fixed broken references Fixed some typos
11.09.000	10.05.2016	Added permissions IHS database interface and IHS matching tables management (chapter 4.1.3.3.6) Added permissions for VPM PDM import configuration panel (chapter 4.1.3.3.7) Added permissions for product definition lookup (chapter 4.1.3.3.7) Added permission to change the process type of a request (chapter 4.1.3.3.10) Changed page orientation to landscape for chapter 4.1.3.3 and all subchapters
11.11.000	23.05.2016	Renamed permission “LOAD_MDS” to “LOAD_MDS_RECEIVED” (chapter 4.1.3.3.1) Added permission group “SEARCH_SENT” containing new permission “LOAD_MDS_SENT” and moved permission “SEARCH_OUTBOX” (chapter 4.1.3.3.1)

Version	Date	Description
11.12.000	11.08.2016	Updated Figure 4 (chapter 4.1.1.3) Updated Figure 5 and added details about options “exclude from automatic user deactivation “ and “exclude from password expiry” (chapter 4.1.1.4.1) Updated Figure 7 (chapter 4.1.1.4.5) Added permissions for AIC Whitelist (chapter 4.1.3.3.1) Added permission “LM_DELETE” (chapter 4.1.3.3.2) Added permissions for imports (chapter 4.1.3.3.10) Updated Figure 22 (chapter 4.3.1) Updated Figure 23 (chapter 4.3.2)
12.00.000	20.09.2016	Added permissions “DELETE_MDSS_INTERNALLY_RELEASED” and “DELETE_MDSS_NON_INTERNALLY_RELEASED” (chapter 4.1.3.3.1) Added permissions “VPM_DS_VIEW” and “VPM_PARTS_VIEW” (chapter 4.1.3.3.7) Added permission “RELEASE_PRODUCT_MODEL” (chapter 4.1.3.3.9)
12.01.000	19.10.2016	Added information about iPoint technical users that are removed from automatic user deactivation (chapter 5) Added information about iPoint technical users that are removed from password expiration (chapter 6)
12.03.000	10.11.2016	Added permissions for iPCA web administration and for management of contacts of IHS companies (chapter 4.1.3.3.6) Added permissions in chapter 4.1.3.3.7 for • VP to DS conversion • VP charts in the iPCA web • requests charts in iPCA web Added permissions in chapter 4.1.3.3.10 for • SEP requests • copy of article and mixture
12.05.000	19.12.2016	Added permissions in chapter 4.1.3.3.6 for • IHS companies management • IHS contacts management Added permissions in chapter 4.1.3.3.10 for • deletion of article and mixture • deletion of SAM-M substance • import supplier contacts Added permissions for chemistry manager (feature itself is not released yet) (chapter 4.1.3.3.1)
12.09.000	03.03.2017	Added permission “MDS_BULK_TRANSFER” (chapter 4.1.3.3.1)
12.10.000	13.03.2017	Updated Figure 3 (chapter 4.1.1) Added hint about search by the user account state (chapter 4.1.1.1) Added information about maximum length of the “Username” (chapter 4.1.1.4.1) Updated Figure 12 (chapter 4.1.2) Updated Figure 22 (chapter 4.3.1)

Version	Date	Description
12.16.000	19.06.2017	Permission “SUPPLIER_CONTACT_IMPORT" moved from “SAM-M → IMPORT” to “iPCA_GENERAL → IMPORT” (chapter 4.1.3.3.7)
12.17.000	26.06.2017	Added permission “SORT_OUT_BULK” (chapter 4.1.3.3.1) Added permissions “SUPPLIER_COMPANY_EXPORT” and “SUPPLIER_CONTACT_EXPORT” (chapter 4.1.3.3.7) Added permission “DELETE_RRR_PRODUCT_MODEL” (chapter 4.1.3.3.9)
12.18.000	14.07.2017	Added permissions “ADR_ML_VIEW” and “ADR_ML_VIEW_EDIT” (chapter 4.1.3.3.6) Added permissions “ARTICLE_ADR_CONFIRM_MIGRATED” and “MIXTURE_ADR_CONFIRM_MIGRATED” in the (chapter 4.1.3.3.10)
12.21.000	04.09.2017	Added permissions “ADMIN_EVENT” and “EVENT” (chapter 4.1.3.3.10)
12.24.000	22.09.2017	Added permissions for creation of new version of the MDS/module (new permission group “NEW_VERSION”) (chapter 4.1.3.3.1) Permissions moved from “iMDS_IHS → EDIT → SORT_OUT” and from “SAM-M → EDIT → SORT_OUT ” to “iPCA GENERAL → SORT_OUT“ and renamed (chapter 4.1.3.3.7) • SORT_OUT_ADMIN → SORT_OUT_VIEW_EDIT • SORT_OUT_BULK • SORT_OUT_RO → SORT_OUT_VIEW
12.27.000	22.11.2017	Renamed permissions (chapter 4.1.3.3.10) • ADMIN_ADR_ML → ADMIN_HAZARD_CLASSIFICATION • ADR_ML_VIEW → HAZARD_CLASSIFICATION_VIEW • ADR_ML_VIEW_EDIT → HAZARD_CLASSIFICATION_VIEW_EDIT Added permissions “PHYS_TECH_PROPERTIES_VIEW” and “PHYS_TECH_PROPERTIES_VIEW_EDIT” (chapter 4.1.3.3.10)
13.00.000	15.12.2017	Added permission “JOB_PRIORITY_CHANGE” (chapter 4.1.3.3.6) Updated Figure 12 (chapter 4.1.2.2) Updated Figure 13 (chapter 4.1.2.3.1)
13.02.000	18.01.2018	Added permissions in chapter 4.1.3.3.6 for management of regions and region types • REGION_VIEW • REGION_VIEW_EDIT • REGION_TYPES_VIEW • REGION_TYPES_VIEW_EDIT Added permissions in chapter 4.1.3.3.6 for management of storage classes master data • ADMIN_STORAGE_CLASS_VIEW • ADMIN_STORAGE_CLASS_VIEW_EDIT Added permissions in chapter 4.1.3.3.7 for handling of regions at MDS • REGION_MDS_VIEW • REGION_MDS_VIEW_EDIT
13.03.000	24.01.2018	Added permissions in chapter 4.1.3.3.10 for requesting and answering external advice for SEP request

Version	Date	Description
		• SEP_SET_EXT_ADVICE • SEP_SET_EXT_ADVICE_COMPLETE
13.05.000	15.03.2018	Added information about deletion of few attributes on inactivation of the iPCA user account (chapter 4.1.1.4.1) Added permissions in chapter 4.1.3.3.1 for control of the display of contact details in 'Received' and 'Sent' panels (based on GDPR regulation) • RECEIVED_INCLUDE_CONTACT_DETAILS • SENT_INCLUDE_CONTACT_DETAILS Added information about deletion of few attributes on inactivation of the iPCA user account (chapter 5) Added new chapter 7
13.08.000	05.04.2018	Added permission in chapter 4.1.3.3.10 • SEP_SDS_EXPORT • SEP_SDS_PUBLISH
13.15.000	29.06.2018	Added permission VPM_PUBLISH_SVHC (chapter 4.1.3.3.7)
13.20.000	03.09.2018	Added permissions in chapter 4.1.3.3.1 for control of editing of the IHS item number in the IMDS datasheets • COMPONENT • MATERIAL • SEMICOMPONENT Added permissions in chapter 4.1.3.3.10 for control of editing of the IHS item number in the SAM-M datasheets • ARTICLE • MIXTURE Added permissions in chapter 4.1.3.3.7 for creation of the RoHS letter for VP • ROHS_LETTER_ARCHIVE • ROHS_LETTER_COMPLIANCE_DATE • ROHS_LETTER_FORMAT • ROHS_LETTER_PRINT
13.24.000	29.11.2018	Added permissions for LCM web application in chapter 4.1.3.3.2 • LM_ADMIN • LM_IMPORT Added permissions for access to and administration of Plants master data panel in chapter 4.1.3.3.7 • PLANTS_VIEW • PLANTS_VIEW_EDIT Added permissions for access to and administration of Projects master data panel in chapter 4.1.3.3.7 • PROJECTS_VIEW • PROJECTS _VIEW_EDIT
13.25.000	14.01.2019	Renamed permissions in chapter 4.1.3.3.1 • COMPONENT to IHS_NUMBER_COMPONENT

Version	Date	Description
		• MATERIAL to IHS_NUMBER_MATERIAL • SEMICOMPONENT to IHS_NUMBER_SEMICOMPONENT Renamed permissions in chapter 4.1.3.3.10 • ARTICLE to IHS_NUMBER_ARTICLE • MIXTURE to IHS_NUMBER_MIXTURE
14.00.000	01.03.2019	Corrected description of the “Language” attribute in the user profile (chapter 4.1.1.4.1)