© PROXESS GmbH

DOCUMENTATION

PROXESS ADMINISTRATOR CONSOLE

Status: PROXESS 10

Table of Contents

Copyright notice, disclaimer

PROXESS has made every effort to guarantee the completeness, accuracy and timeliness of the information contained in this document. We reserve the right to make changes to this document without notice. PROXESS does not assume any liability for technical defects in this documentation. Furthermore, PROXESS does not assume liability for damages that can be attributed directly or indirectly to the delivery, performance and use of this documentation.

This documentation contains proprietary information that is subject to copyright. Without prior written permission from PROXESS, this documentation may not be translated, distributed, copied or reproduced in any other form either in whole or in part. The software described in this documentation is subject to a licensing agreement. The use and reproduction are only permitted within the bounds of this agreement.

PROXESS is not liable to any person or entity for any losses or damages that are allegedly or actually and directly or indirectly incurred in connection with the use of or impossibility of using the instructions contained in these documents. PROXESS reserves the right to change this document without prior notice, without being obligated to inform any persons of such changes or modifications.

All of the trademarks, product names and company names mentioned in this book may be registered trademarks of the respective owners or manufacturers. All brands and other names that do not belong to the PROXESS software are also the property of the respective owner if no special mention is made of protected rights in individual cases.

All mentioned software products are trademarks of the respective manufacturers:

- PROXESS® is a registered trademark of PROXESS GmbH.
- Adobe and Acrobat are trademarks of Adobe Systems Incorporated which may be registered in some jurisdictions.
- CFM Twain is a registered trademark of Computer für Menschen GmbH.
- Internet Explorer, Microsoft Windows, MS Word, MS Excel, MS Powerpoint and Microsoft SQL Server are registered trademarks of Microsoft Corporation.
- Microsoft Dynamics NAV is a registered trademark of Microsoft Corporation.
- Lucene is a free software project from the Apache Software Foundation.
- Caché is a registered trademark of InterSystems Corporation.
- Oracle product names and the Oracle logo are registered trademarks of Oracle Corporation.
- SAP/R3 is a registered trademark of SAP Software AG.
- Google Chrome is a registered trademark of Google Inc.

General information

A note for female users:

For better legibility, we are omitting the explicitly separate mention of male and female users in this documentation. However, we want to expressly point out that we always refer to both women and men in this documentation.

Highlights in the text

Highlights are used in this documentation as follows:

Bold	Refers to menu commands, buttons, field names, options, program names and program groups. Examples: the **New** command, in the **Name** field
"Quotation marks"	Refer to menu titles, folder names and dialog fields. Examples: the "User" menu, the "Smartcards" folder, the "Set password" dialog field
UPPERCASE LETTERS	Are reserved for the representation of keys. Examples: RETURN key, ALT key
(Brackets)	Show that a placeholder symbol is meant. Examples: (%) (_) during the PROXESS search

Tips

	This symbol shows you particularly convenient options for the operation or useful additional information. Tips are always represented as they are in this paragraph.

Warning information

	This symbol is displayed for actions that could result in significantly more work or might even lead to data loss or other material damages. Warnings are shown by this symbol: **You should read the warnings very carefully before you continue working.**

Print documentation

In addition to the online help that you are currently using, you can also open and print this program documentation as a PDF file with the free Acrobat Reader.

You can find the respective PDF help files in the program group **PROXESS/Documentation**.

Please see the Acrobat Reader Online Manual for information on how to use Acrobat Reader.

Activating the system—step by step

If you are using **PROXESS in the security certificate mode**, a few preparatory steps must be performed in the PROXESS Administrator Console before starting the system and working with PROXESS for the first time.

You can see how the individual steps are performed when you follow the entered links.

First step: Install PROXESS software	One time	
Second step: Request system certificate	One time	==> Transfer of the request to PROXESS GmbH ==> PROXESS sends the signed request file back to the applicant
Third step: Activate and install the system certificate - Activation - Installation	One time	
Fourth step: Create the first supervisor smartcard - Preparation - Creation	One time	==> Transfer of the data from the supervisor certificate to PROXESS ==> Creation and transfer of the licensing files by PROXESS

Fifth step: Import licensing files	One time	==> First PROXESS system start by supervisor
Sixth step: Initializing database signing	One time	==> **Now the system is unlocked!** ==> Now user registration and other administration are possible
Seventh step: Create additional supervisor smartcards - Preparation - Creation - Assignment	Always in running operation	Recommendation: create at least one more supervisor smartcard

Organizational analysis as a prerequisite

Before setting up a PROXESS system, you have to clarify a few organizational questions. Ideally, you have performed an advance organizational analysis and answered the questions below:

As administrator, you need the following information for the system setup:

- Which archive databases are needed?
- Which document types are needed in the respective archive databases?
- Which index fields are needed in each archive database?
- Which index fields should be encrypted?
- Which index fields should be mandatory fields?
- Should any index fields be provided with a validation rule?
- Should particular searches be fixed by means of search conditions?
- Which fields should be linked to a dynamic search criterion?
- Which file types should be archived and which programs for processing, viewing and printing will the users apply?
- Are file templates needed in conjunction with certain programs (e.g., Winword)?
- On which storage media and how long should documents be archived?

For the PROXESS supervisor's tasks in the PROXESS Administrator Console, it is necessary to know:

- Which users and groups are needed?
- Which rights to databases and document types do the users and groups get?
- Which databases should be encrypted as high-security databases?
- Which users should function as database area administrators?

You can start the configuration and setup of PROXESS only when you have this information.

What is the PROXESS Administrator Console?

The PROXESS Administrator Console supports the central system administration.

You can perform these tasks with the PROXESS Administrator Console:

- User management and rights management
- Management of smartcards for supervisors
- Creation and activation of the system certificate and the supervisor certificates
- Database signing, field and file encryption
- Management and configuration of archive databases
- Setup of fields, document types and file types
- Setup of index and search masks
- Configuration of validation rules, template files, and search and sorting criteria

The PROXESS Administrator Console is provided as a "snap-in" for the Microsoft Management Console (MMC).

Also see:
Activating the system—step by step
Organizational analysis
Before the first login

PROXESS administrator—tasks and rights

PROXESS administrators are all members of the "Admin" PROXESS user group. Administrators log into the system with the short PROXESS user name and password. In the PROXESS Admin Console, it is not possible for a Windows Active Directory user to log in.

The administrator's tasks are:

- Creating new archive databases
- Configuration of fields, document types and file types (incl. encryption options on a field and file level)
- Creation and configuration of document masks
- Configuration of validation rules, sorting criteria, thesauruses, etc.
- System administration (creating and managing external storage media, cache management, external SQL database administration, etc.)

The supervisor or the database area administrator assigned by the supervisor handles the task of user management and the allocation of access rights to databases and document types. Any user who is a member in the "Administrators" group is an administrator.

When a new database is created, the administrator automatically gets an access right to this database. The access right is needed to execute the above-mentioned administrative tasks. However, the access right for the database does not automatically provide access to the documents in this database. For this purpose, separate access rights on a document type level must be granted.

What can't the administrator do?
Access rights to databases and document types are granted by the supervisor or database area administrator. The administrator can only view the rights, not grant or revoke them.

Also see:

Access rights—concept and overview

An overview of administrator categories

PROXESS separates the administrative sectors of access rights management by a PROXESS supervisor from the technical administration by the PROXESS administrator. The PROXESS supervisor is responsible for the "Who?" of archival access and the PROXESS administrator for the "What?" All of the administrator's tasks can also be performed by the supervisor. To relieve supervisors, they can assign database area administrators to certain databases. These administrators can then handle the user access rights management in their own database areas.

An overview of the rights:

Supervisor	Database area administrator	Administrator
• System initialization • User management • Access rights management • Encryption of field contents or files	• is assigned by the supervisor • Management of access rights, reset of passwords, user blocking in their own database area	• Creation of new archive databases • Management of fields, document types and file types • Management of document masks • Management of validation rules, template files, and search and sorting criteria • System administration (creating and managing external storage media, cache management, external SQL DB administration, etc.)

Database area administrator

The supervisor can grant supervisor privileges to a database area administrator. **The supervisor gives the database area administrator the right to manage one or multiple databases.**

The administration right for a database makes it possible to grant or revoke access rights to documents for other PROXESS users. Additionally, area administrators can create passwords and disable them and block and unblock user accounts for users with access rights to "their" database.

As the area administrator for a database, only the databases that the supervisor has unlocked will be displayed. Area administrators can have all existing user and group memberships displayed but can only make changes to a limited extent. Database area administrators can grant users and groups access rights to the database they manage only if these users and groups don't have any access rights to other databases which the administrators don't also manage. Likewise, only users who have no access rights to other databases can be added to a group with an access right to the managed database. If database area administrators manage multiple databases, they can freely assign users and groups within their administration area and grant access rights.

The purpose of this rule is to prevent area administrators from misusing their authorizations and, by changing passwords, get access to an archive with another user login to which they have not received access. At the same time, this is intended to relieve supervisors of daily routine tasks in user management, such as "Reset password".

In addition to basic access to an archive database, database area administrators are responsible for granting the corresponding document type rights of one or more databases within their administration area.

Also see:

User management—concept and overview

Access rights—concept and overview

Managing database rights

Managing document type rights

Supervisor

PROXESS separates the administrative sectors of access rights management by a PROXESS supervisor from the technical administration by the PROXESS administrator. The PROXESS supervisor is responsible for the "Who?" of archival access (user and group rights), the PROXESS administrator for the "What?" (database fields, document types, thesauruses, etc.). All of the PROXESS administrator's tasks can also be performed by the PROXESS supervisor. The supervisor always uses a smartcard and PIN for identification by the system.

The security concept of PROXESS sees a company's management in the role of the supervisor, who uses a personal smartcard for authentication to manage security-relevant functions in the system. These functions/authorizations include, among others, activating the encryption of field contents or files and setting up or changing user and group authorizations.

If certain employees should take over expanded administrative tasks and the management of access rights for particular areas, the supervisor can give them this role. This means that the human resources director, for example, can take over management of access rights for the "Personnel" database (Database area administrator). If needed, this also allows the supervisor to grant any rights to the original PROXESS administrator. This makes system operation possible "as usual".

A supervisor is any registered person in PROXESS who is a member of the "SUPERVISORS" group and to whom a valid supervisor smartcard has been assigned.

Also see:

User management—concept and overview

Access rights—concept and overview

System setup for operation in certificate mode

(!)	Which mode is used depends on how the PROXESS professional setup set is installed. Either the certificate mode or the OEM mode can be activated here. **It is not possible to switch from certificate mode to OEM mode or vice versa at a later time.**

If you have installed **PROXESS in the security certificate mode**, a few preparatory steps must be performed in the PROXESS Administrator Console before starting the system and working with PROXESS for the first time.

AFTER the software installation and BEFORE the first login, you must:

Request, activate and install a PROXESS system certificate for your system one time

Prepare and create your first supervisor smartcard

Import your individual PROXESS system license (created by PROXESS GmbH)

Initialize the database signing

You can see how the individual steps are performed when you follow the links in the table.

First step: Install PROXESS software	One time	
Second step: Request system certificate	One time	==> Online transfer of the request to PROXESS GmbH ==> PROXESS sends the signed file back to the applicant
Third step: Activate and install the system certificate Activation/installation	One time	

Dokumentation PROXESS Admin Console

|		
Fourth step: Create the first supervisor smartcard Preparation/creation	One time	==> Transfer of the data from the supervisor certificate to PROXESS ==> Creation and transfer of the licensing files by PROXESS
Fifth step: Import licensing files	One time	==> First PROXESS system start by the supervisor
Sixth step: Initializing database signing	One time	==> **Now the system is unlocked!** ==> Now user registration and other administration are possible
Seventh step: Create additional supervisor smartcards Preparation/creation/ assignment	Always in running operation	We recommend that you create at least one additional supervisor smartcard for security reasons.
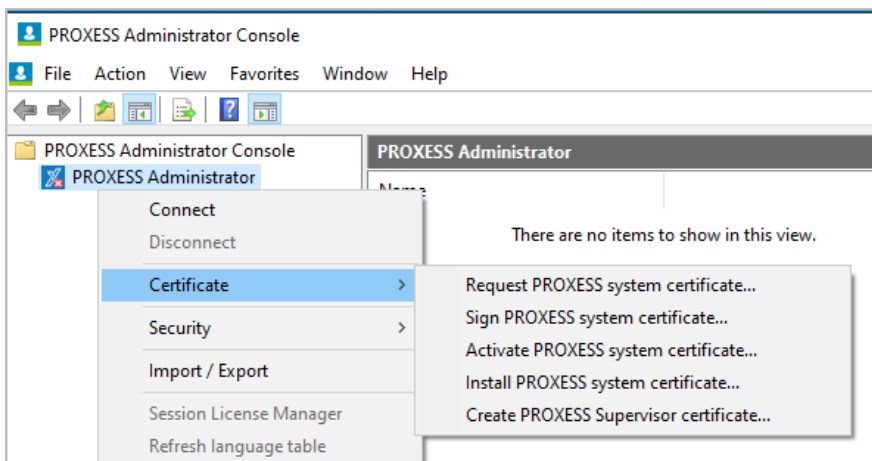
Fig.: Necessary steps for the PROXESS system certificate
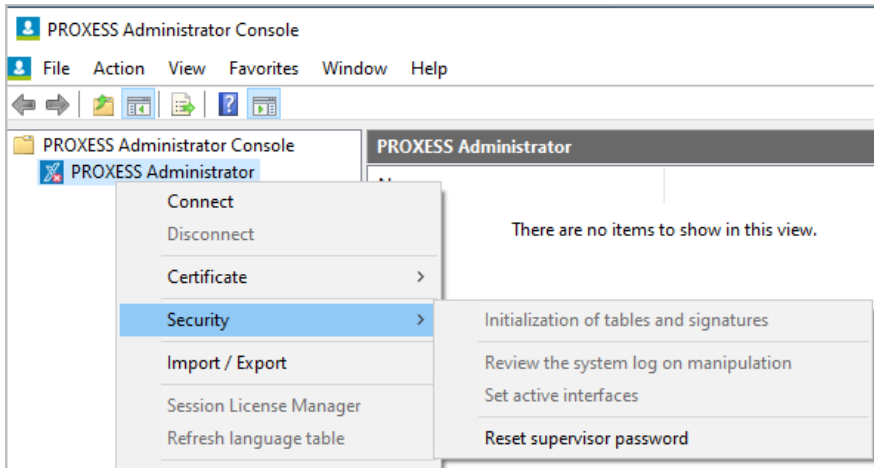
Fig.: Functions for the necessary database signing and for the optional encryption for high-security databases

System setup for operation in OEM mode

If the system is operated in OEM mode, no system certificate needs to be requested. A setup of high-security databases with a special file and field encryption is not available. Although these certificate options are displayed, they have no application in OEM mode.

After the installation in OEM mode, the system is immediately operational and available with a default database.

⊙	hich mode is used depends on how the PROXESS professional setup set is installed. Either the certificate mode or the OEM mode can be activated here. It is not possible to switch from certificate mode to OEM mode or vice versa at a later time.

System log

The system log should be checked regularly for manipulations:

◦

The list below provides an overview of all PROXESS events recorded in the system log. You can use the provided SQL scripts to evaluate the log. (See: Database security (logging).

SQL table: SystemMetaLog
SQL database: PROXESS MasterDB
function: Log all configuration events

Event	Event ID	Explanation
eDBCREATE	1	Database: create new
eDBUPDATE	2	Database: change description
eDBDELETE	3	Database: clear
eDBRGRANT	4	Database: assign rights
eDBRREVOKE	5	Database: revoke rights
eDBRREMOVE	6	Database: clear rights
eDBPURGE	7	Database: configure deletion behavior
eDBLOG	8	Database: activate event log
eDTCREATE	9	Document type: create new
eDTUPDATE	10	Document type: change properties
eDTDELETE	11	Document type: clear
eDTRGRANT	12	Assign document type rights
eDTRREVOKE	13	Document type: revoke rights
eDTRREMOVE	14	Delete document type rights
eDT_FIELDNEW	15	Document type: create new field
eDT_FIELDUPDATE	16	Document type: change properties field
eDT_FIELDDELETE	17	Document type: clear

eDT_DEL_KFT	18	Document type retention period: Exception clear for a file type
eFTCREATE	19	File type: create new
eFTUPDATE	20	File type: change properties
eFTDELETE	21	File type: clear
eFT_FILEASSIGN	22	File type: create link to the template file
eFT_FILEREMOVE	23	File type: remove link to the template file
eEDCREATE	24	Editor: create new
eEDUPDATE	25	Editor: change properties
eEDDELETE	26	Editor: delete
eFIELDCREATE	27	Field: create new
eFIELDUPDATE	28	Field: change properties
eFIELDDELETE	29	Field: clear
eUDISABLE	30	Users: lock/unlock
eUG_ASSIGN	31	Users: assign to a group
eUG_REMOVE	32	Users: remove from a group
eUNEW	33	Users: create new
eUMODIFY	34	Users: change properties
eUDELETE	35	Users: clear
eUPASSCHANGE	36	Users: password changed by administrator
eUMY_PASSCHANGE	37	Users: change their own password
eGNEW	38	Group: create new
eGMODIFY	39	Group: change properties
eGDELETE	40	Group: clear
eVRNEW	41	Validation rule: create new

eVRUPDATE	42	Validation rule: change properties
eVRDELETE	43	Validation rule: clear
eVRASSIGN	44	Validation rule: create field link
eVRCANCEL	45	Validation rule: cancel field link
eVRTHES	46	NOT occupied
eCERTNEW	47	Certificate: create new
eCERTUPDATE	48	Certificate: change properties
eALLGRANT	49	Bulk rights (give the admin group all rights)
eMASTERKEY	50	Master key: create new
eSIGNDOCS	51	Sign: high-security database
eSIGNMETA	52	Sign: metadata
ePROFILENEW	53	Profile: create new
ePROFILEDELETE	54	Profile: clear
ePROFILEUPDATE	55	Profile: change properties

The log itself is protected against manipulation by hash values and a link from the relevant protocol entry to its respective predecessor and successor.

Also see:
Database logging (security)

File encryption

File encryption in PROXESS means that the contents of the files archived in PROXESS are encrypted. The file encryption must first be initialized by the supervisor in the PROXESS Administrator Console. The initialization of the file encryption is a one-off process and can't be reversed. Whether you initialize the file encryption depends on whether you decided on system operation with security options or system operation without security options.

The file encryption can be controlled through the properties of a document type only after the initialization. This setting is performed in the PROXESS Administrator program. The file encryption for document types can only be set in the PROXESS databases that were previously activated as high-security databases.

Setting the option "File encryption" for a document type in the PROXESS Administrator program does not result in a retroactive encryption of already archived files of this document type. The files are only encrypted from the time at which the administrator has activated the file encryption for a document type.

Initializing the file encryption

As supervisor, use your smartcard to connect with the registered "PROXESS Administrator".
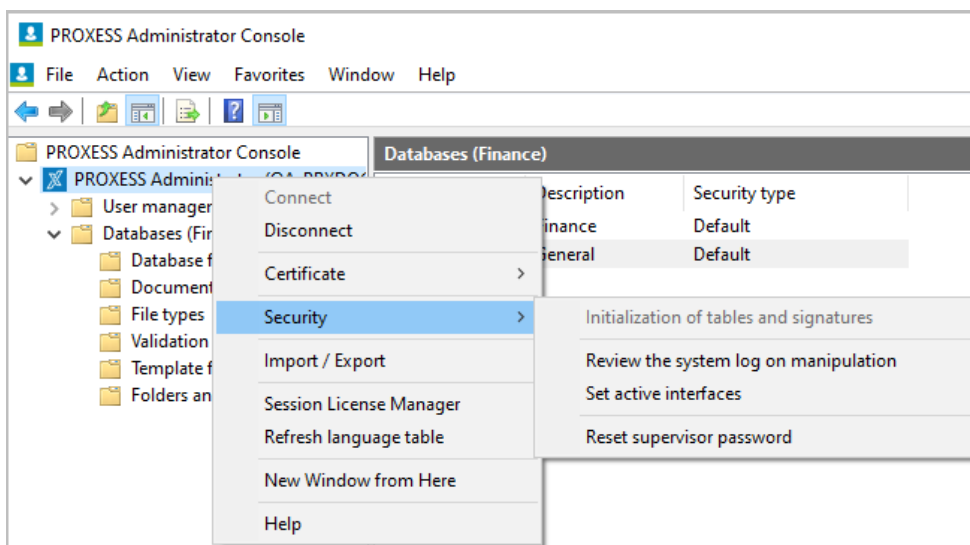In the "Action/security" menu, select the command **Initialize file encryption**.

Fig.: "Action/security" menu

Select a printer to print out "PROXESS master key—file encryption". For security reasons, select a local printer or a printer not accessible to the public. (Don't select a PDF printer or similar, since there is a risk that your password file will be overwritten accidentally.)
Confirm your selection with the **Initialize** command.
Your changes will only take effect after you **restart the PROXESS system**.

Warning information

> ⊘ **Store the resulting printout "PROXESS master key—file encryption" in a safe place. This printout contains a key password for the algorithm of the file encryption. Without this password, it isn't possible to decrypt encrypted files, for example after changing hardware, and to show them in the original format again. If the master key file encryption is lost, data will be lost!**

Dokumentation PROXESS Admin Console

Restore file encryption

Restoring the file encryption is required e.g., after replacing system hardware.

As supervisor, use the smartcard to connect with the registered "PROXESS Administrator".
In the "Actions/security" menu, select the command **Restore the file encryption**.
Enter the password of the printout "PROXESS master key—file encryption".
Confirm your entry with the command **Restore**.
Your changes will only take effect after you **restart the PROXESS system.**

Also see:
Activate high-security database

Database signing (administrative database)

When the administrative database is signed, metadata such as the administrative data of users, groups and rights are protected against unauthorized access from the outside (e.g., via external SQL tools). If a user's group membership is manipulated and changed through an external SQL command, for example, the PROXESS system detects this manipulation and blocks the relevant user account. Database signing thus makes unauthorized access and manipulations of the administrative data visible.

The initialization of the database signing is a prerequisite for operating PROXESS. It also has to be initialized if you don't want to select additional encryption options, i.e., to choose system operation without security functions. If the database signing hasn't been initialized yet, no users can log on to the system or connect to a database.

You need supervisor privileges for the functions "Initialize database signing", "Restore database signing" and "Initialize and sign metadata" described below.
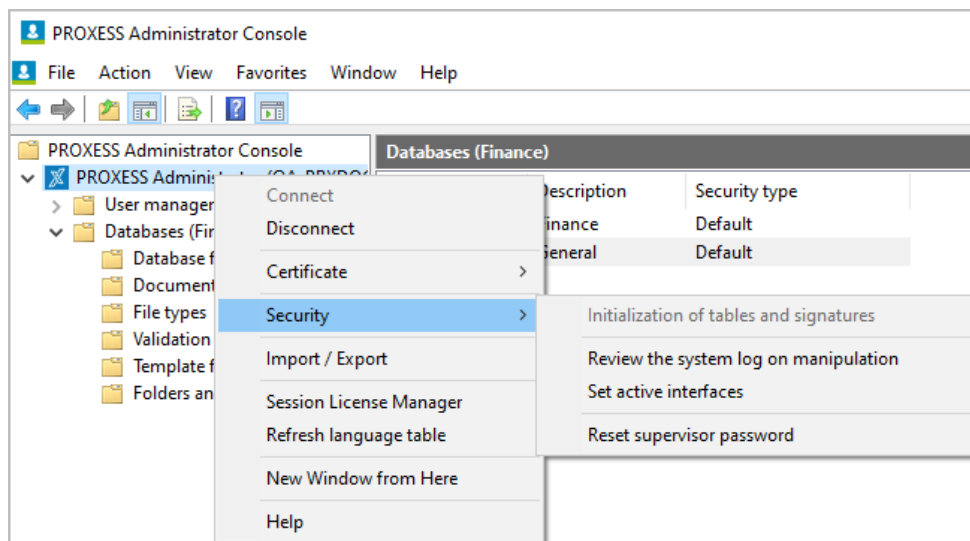

Fig.: "Action/security" menu

Initializing database signing

Select a printer to print out "PROXESS master key—database signing key". For security reasons, select a local printer or a printer not accessible to the public. (Don't select a PDF printer or similar, since there is a risk that your password file will be overwritten accidentally.)
Confirm your selection with the **Initialize** command.
Your changes will only take effect after you **restart the PROXESS system**.

Warning information

⊘ **Store the resulting printout "PROXESS master key—database signing" in a safe place. This printout has a key password that is required for the potential recovery of the database signing, e.g., after a hardware replacement. Without this password, the user will be unable to autonomously restore the system operation. In that case, the database signing must be re-initialized by PROXESS GmbH for a fee.**

Restore database signing

Dokumentation PROXESS Admin Console

Restoring the database signing is required e.g., after replacing system hardware.

As supervisor, use the smartcard to connect with the registered "PROXESS Administrator".

In the "Actions/security" menu, select the command **Restore database signing**.

Enter the password of the printout "PROXESS master key—database signing key".

Confirm your entry with the command **Restore**.

Your changes will only take effect after you **restart the PROXESS system**.

Initialize and sign metadata

This function is only required when you update from PROXESS 5.0 to PROXESS 5$^+$.   This command adds new database fields from the administration database to the database signing. You do not need to execute this command if you are installing PROXESS 5$^+$ for the first time.

Also see:

Activate high-security database

Field encryption

In PROXESS, field encryption means that individual database field contents of an archive database which has been activated as a high-security database in PROXESS are encrypted. Database field contents are the entered search criteria of a document. In a personnel database, this could be e.g., the personnel number and name of an employee. If you want such information to be protected especially well, activate field encryption for these fields. This setting is performed in the PROXESS Administrator program.

The field encryption must first be initialized by the supervisor in the PROXESS Administrator Console. The initialization of the field encryption is a one-off process and can't be reversed. Whether you initialize the field encryption depends on whether you decided on system operation with security options or system operation without security options.

The field encryption can be controlled through the properties of a PROXESS default field in the PROXESS administrator program after the initialization. Setting the option "Encrypted" for a standard field in PROXESS Administrator does not result in the retroactive encryption of already entered and archived field contents. Only default fields of high-security databases can be encrypted.

Initialize field encryption

As supervisor, use your smartcard to connect with the registered "PROXESS Administrator" in the PROXESS Administrator Console.
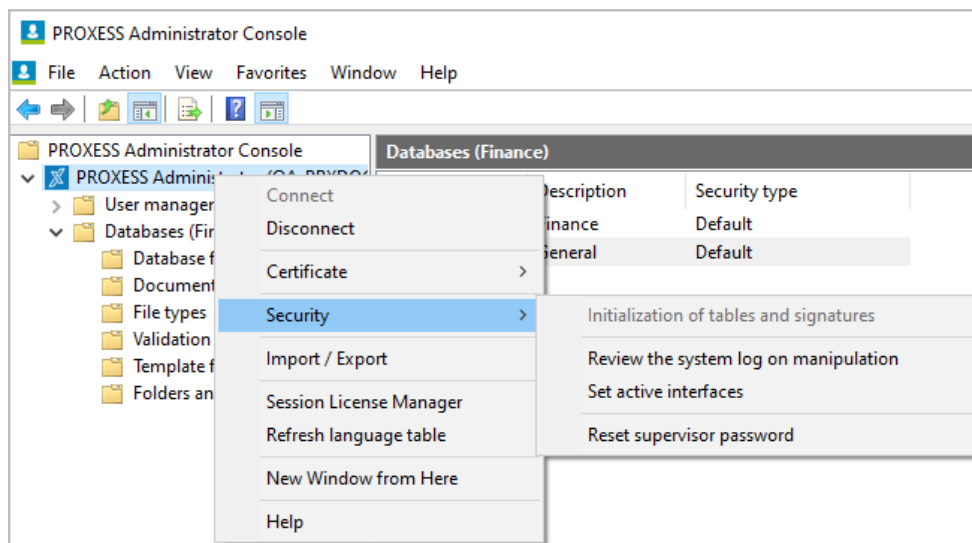In the "Action/security" menu, select the command **Initialize field encryption**.

Fig.: "Action/security" menu

Select a printer to print out "PROXESS master key—field encryption". For security reasons, select a local printer or a printer not accessible to the public. (Don't select a PDF printer or similar, since there is a risk that your password file will be overwritten accidentally.)
Confirm your selection with the **Initialize** command.
Your changes will only take effect after you **restart the PROXESS system**.

Warning information

⊘ **Store the resulting printout "PROXESS master key—field encryption" in a safe place. This printout contains a key password for the algorithm of the field encryption. Without this password, it isn't possible to decrypt encrypted field values, for example after changing hardware, and to show them in the original format again. If the master key field encryption is lost, data will be lost!**

Restore field encryption

Restoring the field encryption is required e.g., after replacing system hardware.

- As supervisor, use the smartcard to connect with the registered "PROXESS Administrator".
- In the "Actions/security" menu, select the command **Restore field encryption**.
- Enter the password of the printout "PROXESS master key—field encryption".
- Confirm your entry with the command **Restore**.
- Your changes will only take effect after you **restart the PROXESS system**.

Also see:
Activate high-security database

Dokumentation PROXESS Admin Console

Activate high-security database

Content-related information about the archived document (contents of the document fields) and administrative information about the archived documents, such as lifespan, retention period and storage medium are entered in the document data sets of a PROXESS archive database. If you want this information to receive special protection, it is recommended that you activate a database as a high-security database.

By activating it as a high-security database, the document data sets in this PROXESS archive database are signed in the underlying SQL database. This means that the PROXESS system can recognize manipulative interference from the outside, on the SQL level, and can display it to the user.

Example: If an SQL command is used to assign a document to another document type, the display and processing of the affected document is blocked with warning indicators. Only a supervisor can remove this block.

The corresponding entries in the full-text database are also protected from unauthorized access by encryption.

Before you can activate a database as a high-security database, these <u>conditions</u> must be met:

The database signing must have already been initialized (see Database signing).

The desired database must be entered as a high-security database in the active PROXESS licensing file. This entry can only be performed by the manufacturer (PROXESS). If needed, contact your sales partner or PROXESS GmbH directly.

The activation of a database as a high-security database is a one-off process and can't be reversed. If you perform the activation at a time when the system has already been in use and documents have already been stored in this database, they will be signed retroactively. Depending on the number of existing documents, this retroactive signing can take a long time. Before the signing starts, you will receive information about the number of existing documents.

<u>**Step-by-step instructions**</u>

As supervisor, use the smartcard to connect with the registered "PROXESS Administrator".

Mark the database that you want to activate as a high-security database. You don't have to be connected to the database.

In the "Action" menu (alternatively via the context menu), select the function "Activate high-security database".
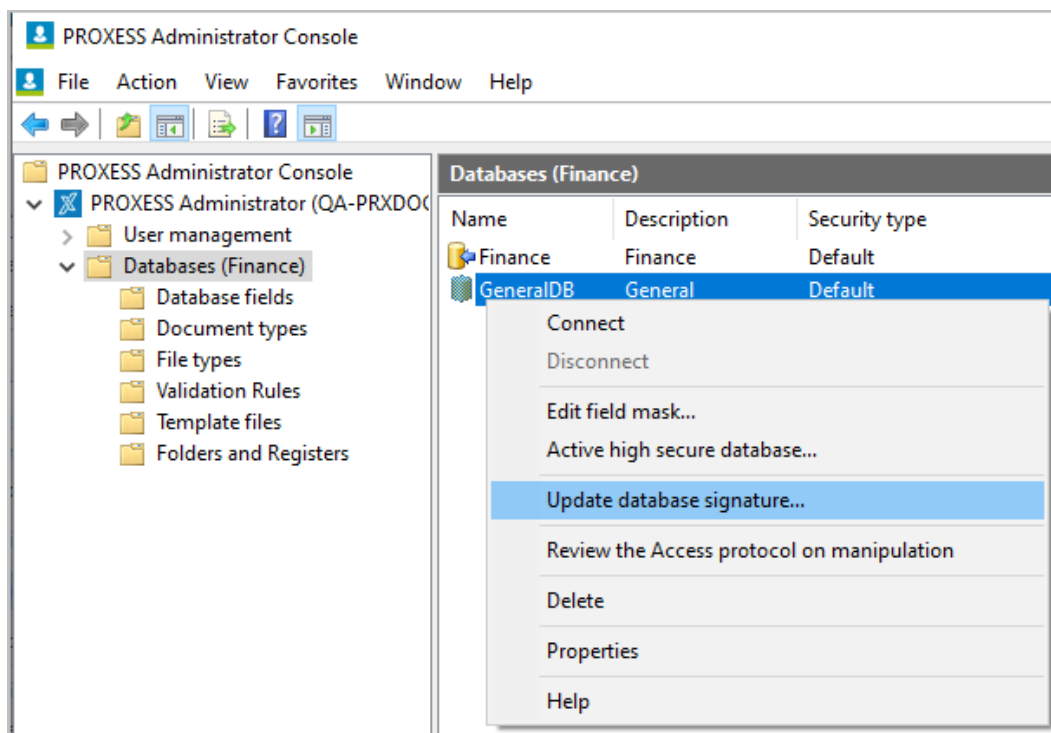
Fig.: Activation of the "Personnel" database as a high-security database

A notice appears to show how many documents in this database have to be signed retroactively. Since it isn't possible to permanently delete any deleted documents in PROXESS, these data sets will also be signed retroactively and counted.
Start the process with the **Yes** command.

If you have successfully activated a database as a high-security database, the menu item "Activate high-security database" will be deactivated. The security type of the database gets the status "High".

Database security (logging)

1.   Access log

All access to archived documents and files is captured in this log. The log records the PROXESS user name, time of day and date and the type of access.   The type of access is distinguished in "New", "Read", Change" or "Clear". For each database, the log can be activated/deactivated by the supervisor or database administrator.

The log itself is protected against manipulation by hash values and a link from the relevant protocol entry to its respective predecessor and successor.

Activate and set up access log

Connect to the system as a supervisor or database area administrator.

Select the desired database.

In the "Action" menu, choose the menu item "Properties" (alternatively via the context menu).
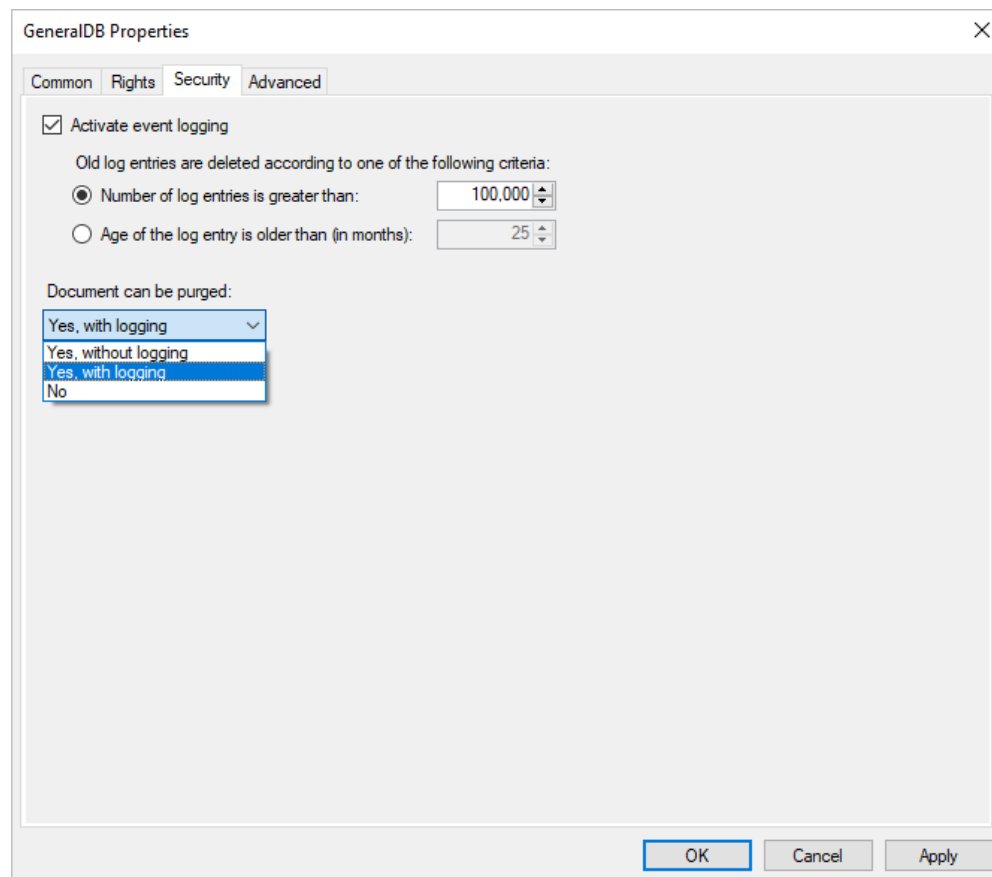
Now select the "Security" tab:

Fig.: Settings for logging on a database level with the sample "Personnel" DB

Possible settings for access logs:

Activate event logging	Here you can activate/deactivate the logging of user access to the documents for the selected database. By default, the logging is not activated.
Clear log entries...

if the amount exceeds .... or

if older than ... months | For performance reasons, you can set the automatic deletion of older log entries either based on volume or time.

Values between 100,000 and 1,000,000 are permitted here.

Values of 25 months or more are permitted here. |

The supervisor or database administrator should regularly check the consistency of the logging:
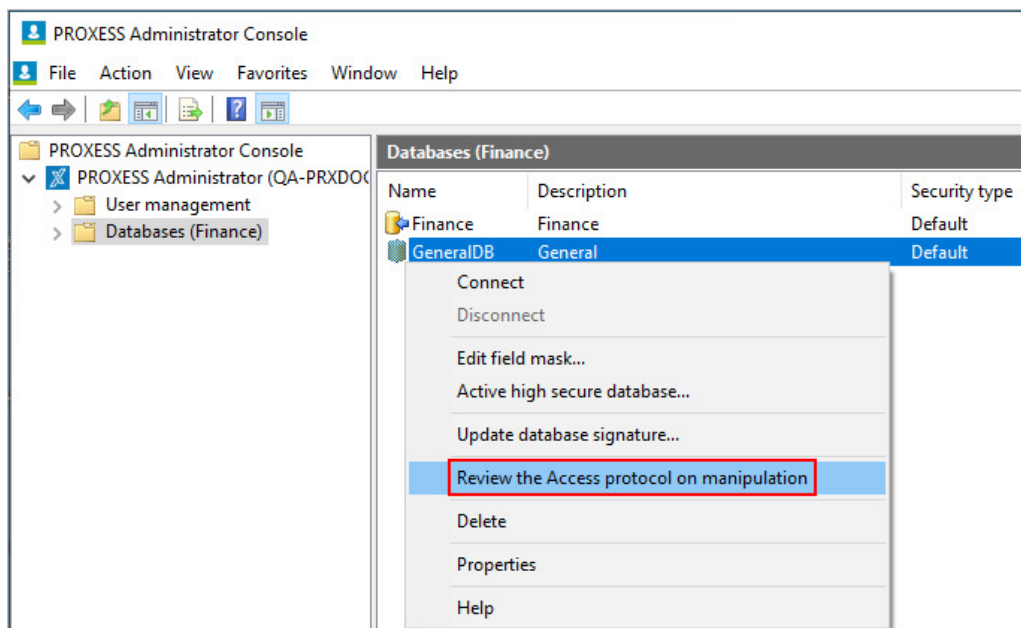
Statistical evaluations of the access logs:
You can filter and represent user access to documents and files with the provided PROXESS Report Console. The evaluations are based on the access log activated here.
The evaluations can be exported as xls or csv files. You can find more information in the module documentation for the PROXESS Report Console.

Examples of business and organizational evaluations:

- Number of document accesses per user group with the goal of allocating the PROXESS DMS costs.
- Time-specific statistics of the document accesses per user group for particular completed actions, etc.
- Frequency of accesses/changes in respect to a certain document type (e.g., purchase agreements).

Logging of deletion processes

Although users with deletion rights can mark archived documents for deletion, they can't permanently remove them from the system for security reasons. The earmarked documents in PROXESS can only be permanently deleted or restored by a PROXESS administrator. To take account of the various legal regulations for various document types in respect to the storage and destruction of company documents (e.g. for personnel documents), you can apply settings for the deletion behavior and the logging of the deletion process for each archive database.

Configuration for the deletion logging:

Connect to the system as a supervisor or database area administrator and select the desired database. In the "Action" menu, choose the menu item "Properties" (alternatively via the context menu). Now select the "Security" tab (see fig. above):

Possible settings for logging the deletion process:

Permanently clear documents….	
No	It is not possible to permanently delete documents. All documents are provided in the system with a possibility of recovery. However, documents deleted by a user can't be searched for and are no longer shown in retrieval.
Yes, with logging	Documents that are permanently deleted by the administrator are noted in the deletion log. The deletion entry includes the executing PROXESS user, the time of the deletion and all contents of the document at the time of deletion.
Yes, without logging (Default setting)	Permanent deletion of documents by the administrator is possible; no entries about the document contents are made in the deletion log.

Tip

	You can find the deletion log as the "LogInfo" SQL table in the respective database and it can be viewed with common SQL tools.

System log

Changes in metadata and main settings are recorded in a central system log. The processes recorded in the system log include, among other things, the creation or deletion of fields, document types or of users and groups. A list of all events captured in the system log can be viewed in the chapter <u>List of log events in the system log</u>.

Similarly to the access log, the log entries here are secured against manipulation by means of hash values and a link to predecessors and successors. The system log can make manipulative access to the system settings visible. **The system log can <u>not</u> be deactivated.**

You should regularly review/evaluate the system log to detect manipulative alterations. Connect to the system as a supervisor for this purpose. Select your PROXESS system and, in the Action/Security menu, choose the function: **Review the system log for manipulation**.
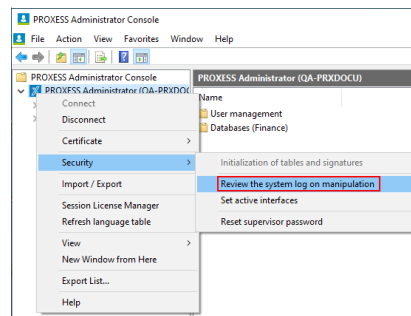
Fig.: Security menu

Statistical evaluations of the system logs:
The scope of the program includes SQL scripts that you can use to execute evaluations of the changes to the PROXESS system settings.   With these evaluations, you can trace configuration changes related to databases, document types, etc. The query results can be saved e.g., as a CSV file.

Examples of possible evaluations:

- Which user has granted which rights to a certain database to which users or groups?
- Which user has added which other users to a certain group at which time?
- Which user has granted which document type rights to whom in a specific database?
a) Filtered for a particular document type
b) Additionally filtered for just a particular group

Also see:
List of log events in the system log

Security functions—concept and overview

The PROXESS security concept includes four main functions:

Supervisor authentication through smartcard and PIN: You need supervisor privileges to grant rights, to delegate management tasks and to activate other optional security functions.
Database signing: PROXESS creates a signature across relevant database fields, thus offering protection against manipulations of the database entries. This function is obligatory for the PROXESS administrative database and optional for individual PROXESS archive databases.
Field encryption: Individual fields in a database are saved with encryption (optional).
File encryption: Files of a certain document type are saved with encryption (optional).

You can decide on system operation <u>with</u> or <u>without security functions</u>. This depends on your need for security or how much protection is needed for the archived documents. Personal documents such as payrolls or application documents are sensitive information, for example, and should thus be seen as more in need of protection than received merchandise invoices.

System operation without security functions

If you decide on system operation without security functions, only two standard security functions have to be activated and used.

This includes the supervisor's <u>Login via smartcard and PIN</u>. This is necessary to carry out the user and access rights management or to assign area administrators for the additional user and access rights management in this area. The supervisor (usually a member of senior management) can assign the human resources manager as the area administrator for the personnel archive, for example. Specifically, the human resources manager receives management rights for the "Personnel" archive database.

<u>Database signing</u> is the second required condition even for system operation without security functions. It results in the signing of the PROXESS administrative database in the underlying SQL database. These administrative data are stored in the PROXESS DB. This also includes user management data, among other things. The signing of the corresponding data sets makes manipulative interventions at the SQL level transparent.

Example: If a PROXESS user without access to the "Personnel" archive database, via an SQL command, becomes the member of a group that has access rights to the "Personnel" archive database, the system detects the manipulation and blocks the user account.

System operation with security functions

If you decide on a system operation with security functions. additional security functions are offered in PROXESS.

When you activate a PROXESS archive database as a <u>high-security database,</u> this initially starts the encryption of the links to PROXESS documents saved in the full-text database. Additionally, this fulfills the prerequisite that SQL field contents and contents of the files archived in PROXESS can be encrypted. However, the SQL field contents are not actually encrypted until this is configured on a database level in the PROXESS Administrator program.

Other conditions for configuring fields or files as encrypted include the initialization of the <u>file and field encryption</u>. **During the initialization of the file and field encryption, passwords are created for the encryption algorithm and printed out. You absolutely must have these passwords in the event of a system restoration or hardware change. It is not possible to make the encrypted data and files legible again without passwords.**

In both cases, before the system is activated, PROXESS GmbH will provide you with a declaration in which you will be informed about the importance of the certificate and encryption passwords. This declaration must be signed and returned to PROXESS GmbH before activating the system.

This table summarizes the information:

Security function	System operation without security functions	System operation with security functions	Effect
Login via smartcard and PIN	Yes	Yes	Required to execute the user management and access rights management
Signing of the PROXESS administrative database	Yes	Yes	Metadata protection for user management Consistency check of the user data High-security database
	No	Yes	Prerequisite for the encryption of standard fields and file encryption per document type in this database Activation of the full-text DB encryption Entry in license required
File encryption	No	Yes	Serves to protect the document data sets in the SQL DB Configuration per default field Only possible in high-security DBs
Field encryption	No	Yes	Serves to protect the PROXESS file contents Configuration per document type Only possible in high-security databases

Also see:

Logging

Activating the system—step by step instructions

Licensing files

PROXESS requires two licensing files. You will get these licensing files via e-mail from PROXESS GmbH after you have completed the PROXESS certification process and transferred the file with the *.dmp* extension via online form (https://www.PROXESS.de/lizenzantrag.html) to PROXESS in the course of creating the first PROXESS supervisor smartcard.

You will receive two files:

Lizenz.txt	Module license file: Specification of the unlocked PROXESS modules and the maximum simultaneously logged-in PROXESS users.
LizenzSec.txt	Customer license file: Specifications of the certification request and the first supervisor smartcard, entry of the high-security databases

Both files must be located in the stated license directory. The information regarding the valid license directory is provided in the program "PROXESS Registry Setup" and "PROXESS Storage Manager Explorer". In the default setting, this is the working directory of the PROXESS server, (e.g., C:\Programme\PROXESS\LizenzSigned.txt and C:\Programme\PROXESS\LizenzSec.txt).
If no specifications are entered, PROXESS will use this directory.

After the licensing files are imported, you can activate the database signing.

Also see:
Activation of PROXESS—step by step

Prepare PROXESS supervisor smartcard

Requirements:

- You have already completed the certification process
- You have a valid system certificate file (pfx file) (see Activate PROXESS system certificate)

Step by step:

Connect the PROXESS smartcard reader to the computer via the USB interface.

Insert a new "blank" smartcard into the reader.

Start the program Gemalto Classic Client Toolbox via Start/Programs.
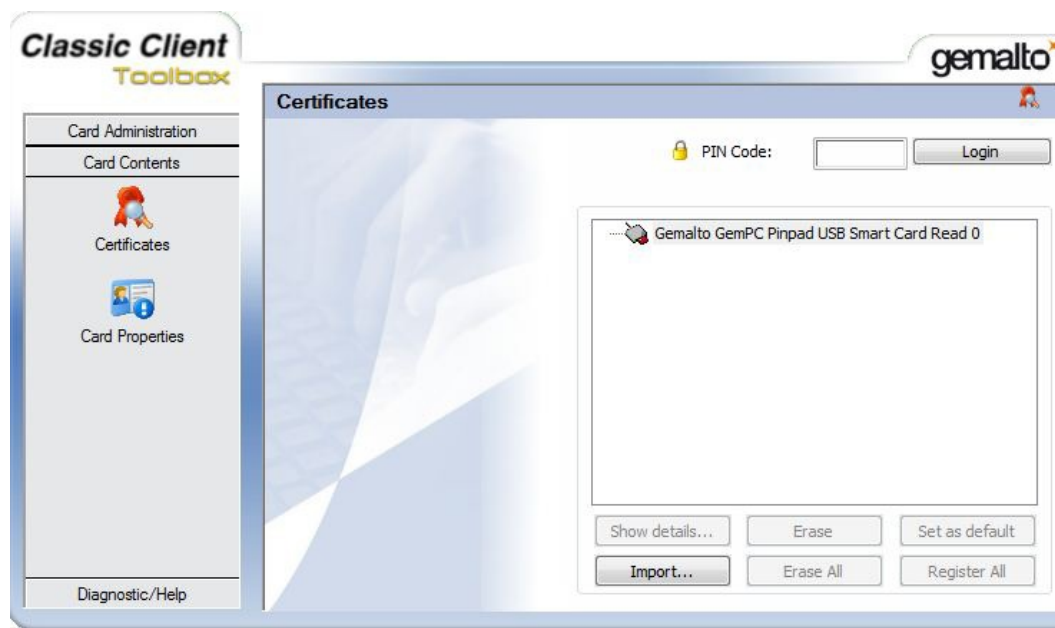
In the "Card contents" menu, choose the command **Certificates**.

Fig.: Dialog box for the Gemalto Classic Client Toolbox to import the key file (.pfx)

In the option "Import/Import from File", choose the **Open** command.

In the output folder that you have already selected, choose the file with the .pfx extension, which you created during the certification process in the menu item "Activate PROXESS system certificate".

Enter the password of your PROXESS system certificate request in the following dialog. (You can find this password on the printout of the PROXESS system certificate request.)

Confirm your entry with the **Verify** command.

After a successful review, your certificate to be imported is displayed in the selection list.

Select the certificate and enter the PIN of the inserted smartcard. (At delivery, this is: 1234).

Dokumentation PROXESS Admin Console

You should subsequently change the standard PIN into an individual PIN in the program Gemalto Classic Client Toolbox in the "PIN management" menu (see PIN management of PROXESS supervisor smartcards).

Confirm your entries with the **Import** command. You will get a confirmation that the certificate was imported successfully.

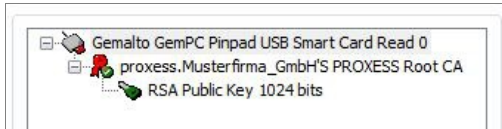Now the imported key is displayed in the "Certificates" menu and assigned to your PROXESS system certificate.

Fig.: Display after successful transfer in the "Certificates" menu

Now you can create a PROXESS supervisor smartcard.

Also see:
PIN management of PROXESS supervisor smartcards
Activating the system—step by step

Create PROXESS supervisor smartcard

Requirements:

- You need supervisor privileges for this action.
- Connect the PROXESS smartcard reader to your computer via the USB interface.
- You will need a prepared smartcard. You can learn how to prepare a smartcard in the chapter "Prepare PROXESS supervisor smartcard".

Step by step:

Start the PROXESS Administrator Console and mark the node PROXESS Administrator ("server name") in the console root.

In the "Action" menu, using the context menu or via the action panel on the right, select the menu item "Certificates" and select the command **Create PROXESS supervisor certificate**.

Select an output folder for the creation of the certificate files and a printer to print out your PROXESS supervisor certificate.

Confirm your entries with the **Create** command.

The following files are created in the selected output folder:

proxess-sv_Musterfirma_GmbH_SN0f4898a9.pfx	Result file for the activation of the PROXESS supervisor certificate.
proxess-sv_Musterfirma_GmbH_SN0f4898a9.dmp	File with individual smartcard data. This file is later sent to PROXESS GmbH and integrated into the individual customer license. This step is only required for the first PROXESS supervisor smartcard.

Warning information

⊗	**Select a secure output folder and a secure (local) printer to prevent unauthorized access. In case of unauthorized use of these documents, the PROXESS system might become insecure. Store the created PROXESS supervisor certificate and created files in a secure location.**

When the files are created, you will be prompted to enter your PIN. Note the display of your smartcard reader. (At delivery, the PIN is: 1234). You should subsequently change this standard PIN into an individual PIN in the program Gemalto Classic Client Toolbox in the "PIN management" menu (see "PIN management of PROXESS supervisor smartcards").

Start via Start/Programs/the program Gemalto Classic Client Toolbox.

In the "Card contents" menu, choose the command **Certificates**.

In the option "Import/Import from File", choose the **Open** command.
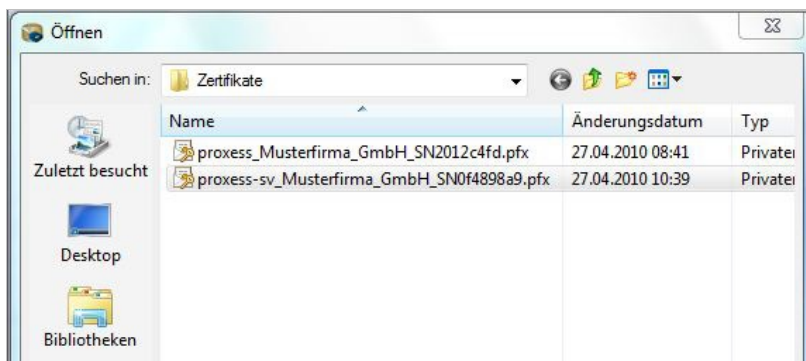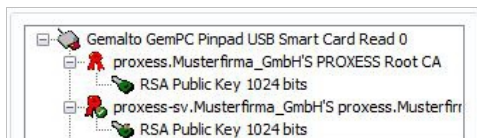
Fig.: Selection of the PROXESS supervisor certificate for import (sample name)

You can recognize the PROXESS supervisor certificate by the file name "proxess-**sv**_SN<Serial number>.pfx".

Select the PROXESS supervisor certificate and confirm your selection with the **Import** command.

Now you have to enter the password of your PROXESS supervisor certificate in the following dialog. You can find this password on the printout of your PROXESS supervisor certificate.

After a successful review, your certificate is offered in the selection list.

Select the certificate and start the import with the **Import** command. You will get a confirmation that the certificate was imported successfully.

Check: Now the imported key is displayed in the "Certificates" menu and assigned to your supervisor certificate.

Fig.: Display after successful transfer of the PROXESS supervisor certificate in the "Certificates" menu

If this is the first PROXESS supervisor smartcard, transfer the .dmp file from the above-selected output folder to PROXESS GmbH. PROXESS GmbH will enter your valid smartcard data into your PROXESS customer license. After a short processing time, you will receive an e-mail with your individual PROXESS license files "Lizenz.txt" and "LizenzSec.txt" from PROXESS GmbH.

The step of transferring the individual PROXESS license files is eliminated for all other PROXESS supervisor smartcards.

In the next step, you can install the PROXESS software and activate the license files.

Tip

	If you want to activate PROXESS archive databases as high-security databases, they must first be entered into your license file by PROXESS GmbH. For this purpose, please tell us the exact name of the archive database(s) (database name). Usually this is already discussed in advance with your PROXESS system advisor during the installation/update.

Also see:
Activating the system—step by step

Activate PROXESS system certificate

As soon as you have received the countersigned file of the certificate request (cer file) from PROXESS GmbH, you can activate your certificate. Activation means that you enable your system to assemble the parts of your certificate (pvk file and cer file) into a functional certificate (pfx file).

Step by step:
Start the PROXESS Administrator Console and mark the branch "PROXESS Administrator" in the console root. In the "Actions" menu, click "Certificates" and select the command **Activate PROXESS system certificate**.

The following dialog box appears:
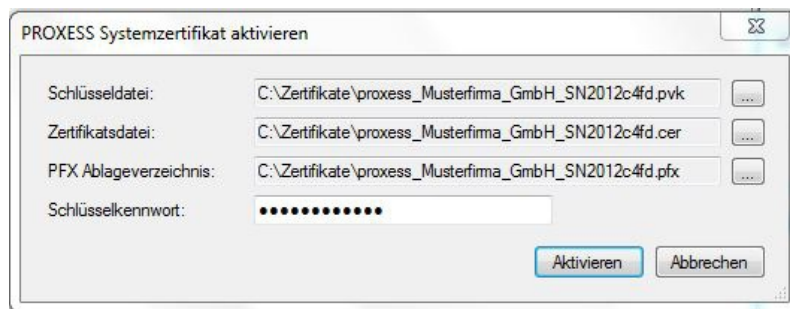
Fig.: Dialog field to activate the PROXESS system certificate

First select the storage location of the private key file (pvk file). When all the required files are in the same directory, the information for the PFX storage directory is entered automatically.

Enter the storage place for the cer file countersigned by PROXESS on the certificate file line and select the **Activate** command. You will get a confirmation that the activation was completed successfully.

Directory content after successful activation:

proxess_ExampleCompany_GmbH_SN2012c4fd.req*	Request file of the PROXESS system certificate. This file was sent to PROXESS GmbH in the preceding step "Request PROXESS system certificate".
proxess_ExampleCompany_GmbH_SN2012c4fd.pvk*	Private key file. This file is the main cryptographic secret for creating the supervisor smartcards and must therefore be stored securely.
proxess_ExampleCompany_GmbH_SN2012c4fd.cer*	Individual PROXESS system certificate. PROXESS GmbH has transmitted this file to you.
proxess_ExampleCompany_GmbH_SN2012c4fd.pfx*	Result file for the activation. This is the basic file to create supervisor smartcards and must therefore be stored securely.

* Sample file names

Warning information

Dokumentation PROXESS Admin Console

	Unauthorized use of the files marked in red (.pvk and .pfx) can result in third parties gaining access to the system. You should therefore store these files in a secure location.

You can install the PROXESS system certificate in the next step.

Also see:

Request PROXESS system certificate

Install PROXESS System certificate

Request PROXESS system certificate

At the start of the certification process, you create a system certificate request that you must send to PROXESS GmbH. Two files are generated during the creation of the system certificate request. The file with the extension **req** contains the certification request. The file with the extension **pvk** contains a private key. This contains the main cryptographic secret of the smartcard creation and may not fall into the hands of third parties, including those of PROXESS GmbH. The request is also issued as a paper printout.

Step by step:

Start the PROXESS Administrator Console and mark the branch "PROXESS Administrator" in the console root. In the "Actions" menu, click "Certificates" and select the command **Request PROXESS system certificate**.

Enter your company information in the following dialog box:

Fig.: Dialog box to request a PROXESS system certificate

Output folder	Two files are created with the request: - The file with the extension req contains the certification request. - The file with the extension pvk contains a private key. Both files are stored in the directory entered here. For security reasons, the manufacturer recommends a protected local directory.
Printer	Select a printer to print out the system certificate request. For security reasons, the manufacturer recommends a local printer.

Warning information

> ⊗ **The printout of the PROXESS system certificate request contains a password that is subject to the strictest secrecy. Unauthorized parties can get access to protected archive data by knowing this password. Please keep this request under lock in a safe place. PROXESS GmbH recommends using a local printer for the printout.**

Confirm your input by clicking the **Request** button.

In the following dialog box, you will be prompted to secure your private key by entering the password from the system certificate request. You can find this password on the printout of the system certification request.
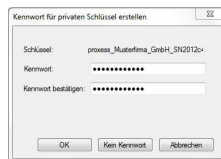
Figure: Entry dialog for the password for the private key

Confirm your input with **OK**. The protected system certification request is now created and stored in the above output folder.
You will get a confirmation that the process was completed successfully.

Send the created system certification request (**req** file) to PROXESS via the online form:
https://www.PROXESS.de/zertifikatsantrag.html.

After a brief processing time, PROXESS will send you an e-mail with the digitally countersigned system certificate (file with the extension **cer**). This can be used only in conjunction with your already created private key and can thus be securely transferred by e-mail.

Now you can activate the PROXESS system certificate.

_____

Also see:

Activate PROXESS system certificate

Install PROXESS system certificate

You need your PROXESS system certificate (pfx file) for this step. First, the steps "Request PROXESS system certificate" and "Activate PROXESS system certificate" must already be completed. By entering the command "Install PROXESS system certificate", you are designating the pfx file as the valid certificate file for your PROXESS system.

Step by step:

Start the PROXESS Administrator Console and mark the branch "PROXESS Administrator" in the console root. In the "Action" menu, click "Certificates" and select the command **Install PROXESS system certificate**.

The following dialog box appears:
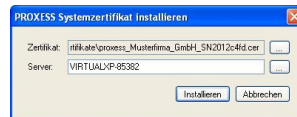
Fig.: Dialog field to install the PROXESS system certificate

Select your PROXESS system certificate as the certificate. You transferred this to PROXESS GmbH in the step "Request PROXESS system certificate" and received it back from the company in a digitally countersigned e-mail.

Please enter the IP addresses or the name of your PROXESS server in the "Server" field. In a distributed system, this is the computer on which the PROXESS Document Manager is installed.

Confirm your input by clicking the **Install** button.

You will get a confirmation that the action was completed successfully.

You can prepare and create a supervisor smartcard in the next step.

Also see:

Prepare PROXESS supervisor smartcard

Create PROXESS supervisor smartcard

Dokumentation PROXESS Admin Console

Certificates—concept and overview

A one-off certification process must be performed before the first PROXESS system start. You will also create the first PROXESS supervisor smartcard of the system. You will carry out the necessary steps of the certification process with the help of the PROXESS Administrator Console. Different certificate files and certificate documents will be created in this process. These are required for the secure running operation of the system, for a system transfer to new hardware or to restore a system after hardware failure. (See: Activating the system—step by step)

The following documents and files are created in the course of the certification process:

- **Request file of the PROXESS system certificate (.req):** file that is sent to PROXESS GmbH as a certificate request (example: proxess_ExampleCompany_GmbH_SN2012c4fd.req)
- **PROXESS system certificate request**: printout created during the request for the PROXESS system certificate
- **Private key (.pvk)**: file created during the request for the PROXESS system certificate (example: proxess_ExampleCompany_GmbH_SN2012c4fd.pvk)
- **PROXESS system certificate (.cer):** file that is created when PROXESS GmbH has countersigned the system certificate (example: proxess_ExampleCompany_GmbH_SN2012c4fd.cer)
- **PROXESS system certificate (.pfx):** file created during the activation of the system certificate (example: proxess_ExampleCompany_GmbH_SN2012c4fd.pfx)

When the PROXESS supervisor smartcards are created, this also results in certificate files and documents:

- **PROXESS supervisor certificate (.pfx):** (example: proxess-sv_ExampleCompany_GmbH_SN0f4898a9.pfx)
- **PROXESS supervisor certificate**: printout of the PROXESS supervisor certificate
- **File with individual smartcard data (.dmp):** This file is sent to PROXESS GmbH and integrated into the individual customer license. This step is only required for the first PROXESS supervisor smartcard (example: proxess-sv_ExampleCompany_GmbH_SN0f4898a9.dmp)

Warning information:

> **Without these files and documents, it isn't possible to create additional smartcards for the administration at a later date. Additionally, it must be ensured that these files and documents don't fall into the hands of third parties, or else the security of the archived documents can no longer be guaranteed. The files (.pvk, .cer, .pfx) should be transferred to a separate data carrier (e.g., memory stick, CD/DVD) and stored in a secure location (safe or notary public). It must be ensured that the data carriers are readable. PROXESS GmbH is explicitly unable to create valid duplicates of the smartcard. Without the above-mentioned files and documents, it also isn't possible for PROXESS GmbH to create additional smartcards at a later date.**

Also see:

Activating the system—step by step

Set Active Interface

The Unicode character set is supported in PROXESS 8.0 and subsequent versions. For reasons of downward compatibility, the older code page character set can also still be used. Use the function **Set Active Interface** to determine which character set should be used for the communication between the PROXESS server and PROXESS clients.

Step by step:

As supervisor, use your smartcard to connect with the registered "PROXESS Administrator" in the PROXESS Administrator Console.
In the "Action/Security" menu, select the command **Set Active Interface** (alternatively in the context menu).
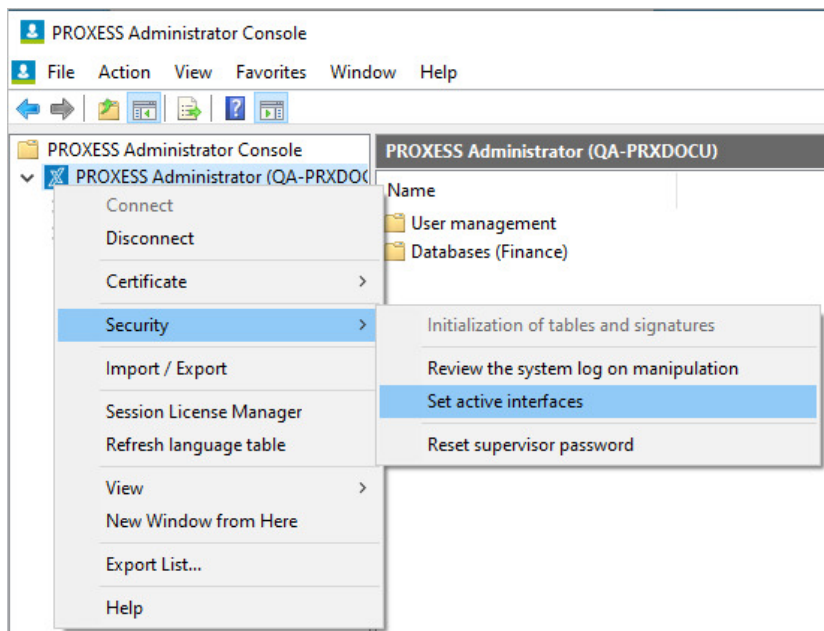
Fig.: Context menu server/security

You have the following setting options.

Only code page-based	The code page character set covers the characters of most European languages. When this setting is active, only PROXESS clients up to version 5^+ R2 can log onto the PROXESS server.
Just Unicode-based	The Unicode character set includes the characters of all languages known worldwide. It is supported by PROXESS 8.0 and later versions. When this setting is active, only PROXESS clients with version 8.0 or later can log onto the PROXESS server.

Both	With this setting, PROXESS clients with all PROXESS versions can log on. **Warning information** <table><tr><td>⚠️</td><td>**Use this setting only temporarily, e.g., in a conversion phase from an older PROXESS version to PROXESS 8.0.** **When both interfaces are activated, documents may be overwritten unintentionally with the old code page character set.** Then unknown characters are reset with substitute characters, such as "?". This will make the documents illegible. To track this overwritten text, you should activate the document history in the PROXESS administrator during the conversion phase.</td></tr></table>

Importing/exporting metadata

⊘	**You need supervisor rights for this function.**

You can export metadata to a file (XML format) and import it from a file or a system into another database/another system. As a system administrator, this saves you a lot of manual work during setup, for example when multiple databases have a similar structure.

These metadata can be exported/imported:

- Users
- Groups
- Database fields
- Document types
- File types
- Template files
- Validation rules
- Search and sorting categories

Step by step:

Select the branch of your PROXESS system and select the **Import/export** command in the context menu.

Open the "**File**" menu.
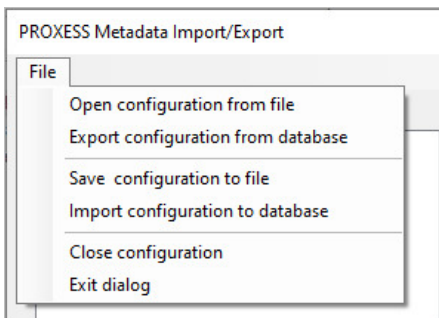
Fig.: Overview of functions for the PROXESS Metadata Exchange dialog

Depending on whether you want to import or export, the following functions are available.

Open configuration from file	Use this to open an existing PMX file (PROXESS Metadata Exchange) with the Explorer menu. Use this function if you want to import metadata.
Export configuration from database	Select the desired database. All metadata are read. You can see the readout of the current metadata on the right in the "Log" window. (See figure below).

Dokumentation PROXESS Admin Console

Save configuration to file	With this command you can save the above-selected values to a PMX file. First go to "Metadata" in the left area of the window to decide which metadata are written into the export file.
Import configuration to database	Select the desired database for the import. In this dialog you can also create a new database at the same time. In this dialog you can also select which metadata should be imported. (See figure below)
Close configuration	This returns you to an empty dialog box.
Exit dialog	Close the box here.
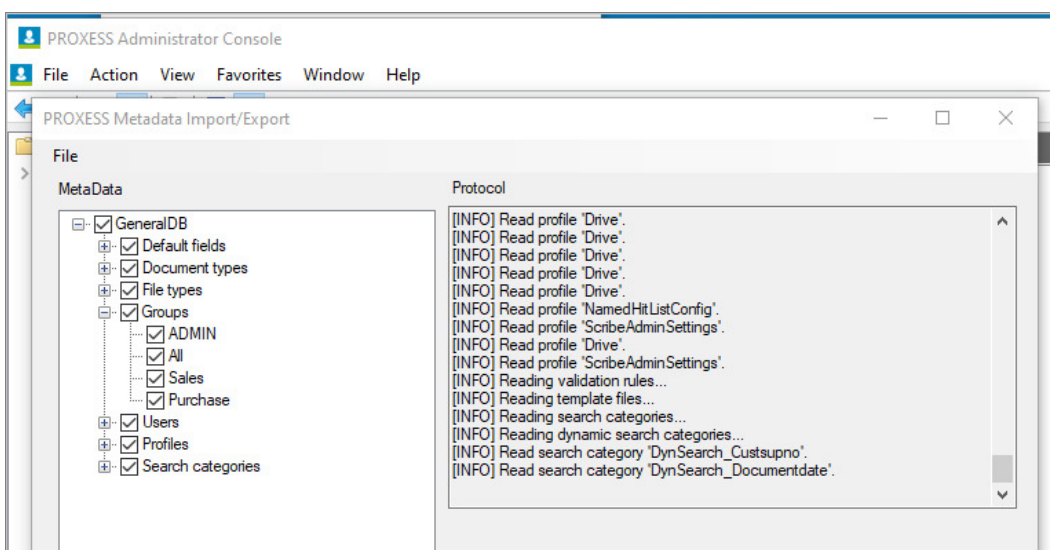
Fig.: Readout and configuration of the metadata file for export

Dokumentation PROXESS Admin Console
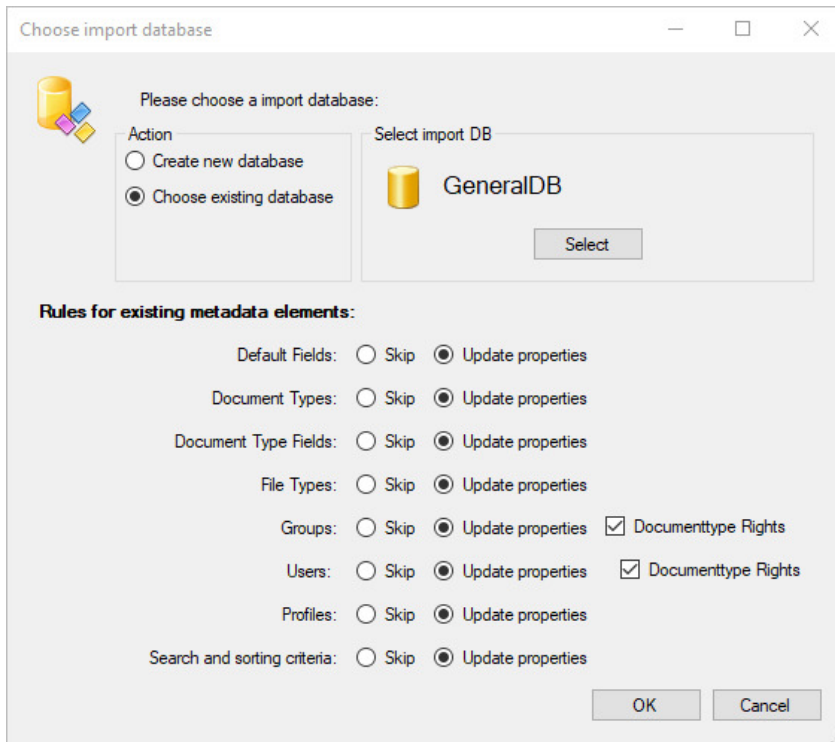
Fig.: Configuration dialog for the import of metadata

Dokumentation PROXESS Admin Console

Connect database

To manage a database, you first have to connect to this database.

If you have already successfully logged on to the PROXESS server, you are automatically reconnected to the database from your last session. If you want to manage a different database, you first have to connect to this database.

Step by step:

–
Select the database that you want to connect to.

In the "Action" menu (alternatively via the context menu), select the function "Connect".

You can identify the currently connected database by the blue arrow symbol.
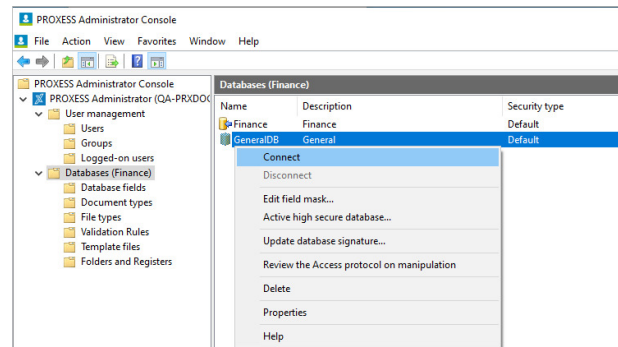
Fig.: Connecting to the "Personnel" database

Login

When you start the PROXESS Administrator Console for the first time, the PROXESS login dialog appears. During subsequent starts, you will connect to the already registered PROXESS system via the menu item Action/Connect (alternatively via the context menu).

Figure: Login mask of the PROXESS Administrator Console

The PROXESS Administrator Console offers you two options for logging in: A login via smartcard and a login with a user name and password. It is not possible to log in with a Windows Active Directory user account. Depending on the type of login you select and your user profile, you will be granted different rights to perform functions within the PROXESS Administrator Console.

First option: login with smartcard and PIN entry

Logging in with a smartcard and PIN entry is reserved exclusively for PROXESS users with supervisor privileges.

Make sure that the entries for the server connection are correct (see table). Connect the smartcard reader to your computer and select the **smartcard** command. An action window from the smartcard reader will appear on your screen. At the same time, a display in the smartcard reader will prompt you to enter a valid supervisor PIN and confirm with ENTER.

It is not necessary to enter a user name and password when logging in with a smartcard.

Second option: log in with a user name and password

Users, administrators and database area administrators log in with a user name and password. The login with a user name and password is not associated with supervisor privileges.

Name	In this field, enter your user name or apply the name that is still provided from the previous session. During the first login, you use the user name that was created during the installation. The program stores the provided user name so that you can continue to use it during the next login.
Password	Enter your password here. During the first login, you use the password that was created during the installation. Only a supervisor can change passwords within the PROXESS Administrator Console. Changing your own password is possible e.g. in the "PROXESS" program or in "PROXESS Administrator".

Dokumentation PROXESS Admin Console

Server name	Enter the name of the desired PROXESS server here. The syntax depends on the network in which you installed PROXESS. The PROXESS Administrator Console stores the PROXESS server name so that you can continue to use it during the next login.
Protocol	Select the network protocol for connecting to the server here. Keep in mind that the possible selections for the protocol sequence depend on the installed network components. When the PROXESS server and the provided module are installed on a computer, select the "Local server" setting.

The PROXESS server connection is stored. You only need to adjust it if something about the settings changed or if you want to work with another server.

Enter the login information and select the **Log in** command.

Straight after the login, you are connected to the database from the last session:
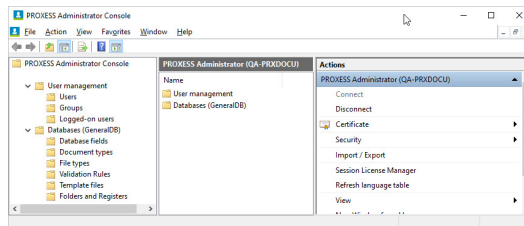
Fig.: Dialog after successful login

_____

Also see:

Change password

Windows Active Directory Integration

User concept: AD users versus PROXESS users

As system administrator, you should organizationally divide all users who work with PROXESS into two user categories.

1. Users with Windows authentication
The system administrator adopts the user data from the Windows Active Directory for these users to avoid double administration in Windows and PROXESS. Users transferring from AD select the authentication option "Windows" in the login dialog of the respective module when logging into PROXESS. Then the Windows login information is automatically transferred to PROXESS. Here, it is recommended to suppress the login dialog for AD users in the respective module settings after the first login.

Members of this category, however, do not have any access to high-security databases—e.g., those for which high security and encryption are activated. This aims to prevent a situation where AD users automatically receive access rights to particularly sensitive documents and data in PROXESS simply by being assigned to an AD group, without these having to be explicitly declared in PROXESS. In practice, this will probably affect the majority of users who, for example, are not members of senior management or HR, and so do not need any access to specially protected data. For these users, Windows Active Directory integration can help to avoid double administration, thus making work easier for the system administrator. This also enables automatic login to the PROXESS modules for the user.

All steps for the Windows Active Directory Integration in PROXESS are described in this chapter.

Warning information

⊘	**Authentication via Windows does not enable access to "secured" databases, meaning those with activated high security and encryption. Only the correspondingly authorized users of the internal PROXESS user administration can access these databases.**

2. Users with PROXESS authentication
Members of this category can access high-security databases (e.g., employee database) if they have been granted the necessary access rights in PROXESS. In practice, this will most likely be limited to a smaller circle of users (e.g., senior management/HR department). These users are created and managed directly in PROXESS. When logging in to PROXESS, the user selects the authentication option "PROXESS" and enters their PROXESS user name and password.

You can find all explanations about the internal PROXESS group and user management in the "User management" chapter.

Warning information

⊘	**Avoid users with a "double identity" as Windows AD users and PROXESS users. Users should generally log into all PROXESS modules with one and the same authentication to ensure that they get a consistent basis for the data and access.**

Please be sure to first read the remarks in the preceding chapter: User management—concept and overview.

Dokumentation PROXESS Admin Console

Step by step: Windows Active Directory Integration

First step: Create Windows authentication group

Create a Windows authentication group for PROXESS in the management of the Windows Active Directory. You can select a random name for this. Select e.g., the group name "PROXESS" or another name, as in the example below. In this group, all Windows users who should work with PROXESS are collected. **For that reason, add all Windows users to this group who should work with PROXESS and should log into PROXESS via the automatic Windows authentication.** A good strategy is to work on a group level and add all Windows groups that should work with PROXESS. This ensures that all members of such a group are automatically added to the authentication group. Management via groups also makes the later administration and maintenance of the system easier for you. Then any newly added users, due to their Windows group membership, automatically also become members of the authentication group for PROXESS. A Windows group hierarchy is not adopted in PROXESS. Users of the groups and subgroups are adopted on equal levels.

Example:
Based on the PROXESS demo system "Let's be fast" (LBF), here is an example with fictitious Windows groups.

First, in the management of the Windows Active Directory, create a Windows group with the name "LBF Everyone". In our example, this will be the Windows authentication group for PROXESS.

In the next step, add the Windows groups "LBF Sales", "LBF Purchasing", "LBF Financial Accounting", "LBF Senior Management" to the newly created group "LBF Everyone". Now you have added all users for later AD integration into the main authentication group for the PROXESS system.

Warning information

ⓘ	**The membership of a Windows user in the authentication group is a mandatory condition for the subsequent assignment of PROXESS access rights to this user.**

Second step: Activate Windows authentication in PROXESS

Now open the program **PROXESS Registry Setup** in the PROXESS program group and select this new group in the Document Manager/User Login menu under "Authentication group". First you must activate the "Windows domain" option in the section "External user system". (Also see the documentation on the PROXESS Registry Setup)
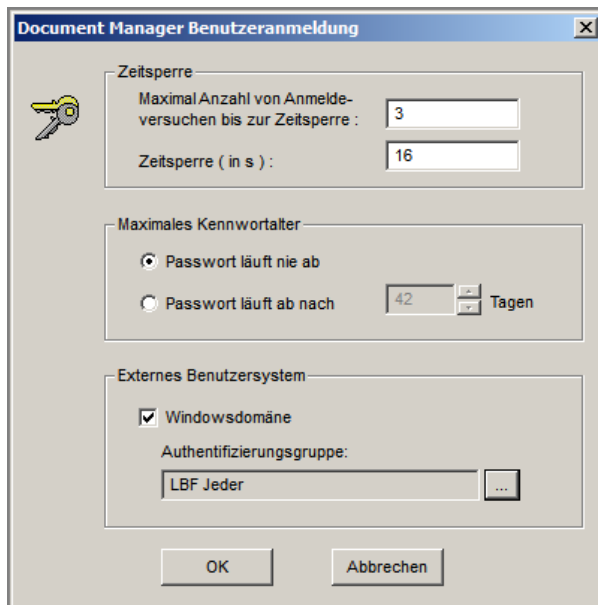
Fig.: Settings for the external user system in the PROXESS Registry Setup

Example: Select the group "LBF Everyone" created in step 1 as the authentication group.

Warning information

⛔	**For the PROXESS authentication group, be sure that you never fall back on existing internal Windows user groups such as "Everyone". Since PROXESS regularly synchronizes the user groups, this will lead to performance problems with a large amount of user accounts.**
	To avoid this, create a PROXESS group as described in item 1, which you can then select as an authentication group in the above dialog.

Third step: Register Windows groups and add users to PROXESS

Now connect to the desired PROXESS system in the PROXESS Administrator Console again and select the "Groups" node. In the "Action" menu, choose the menu item **Register Windows group.**
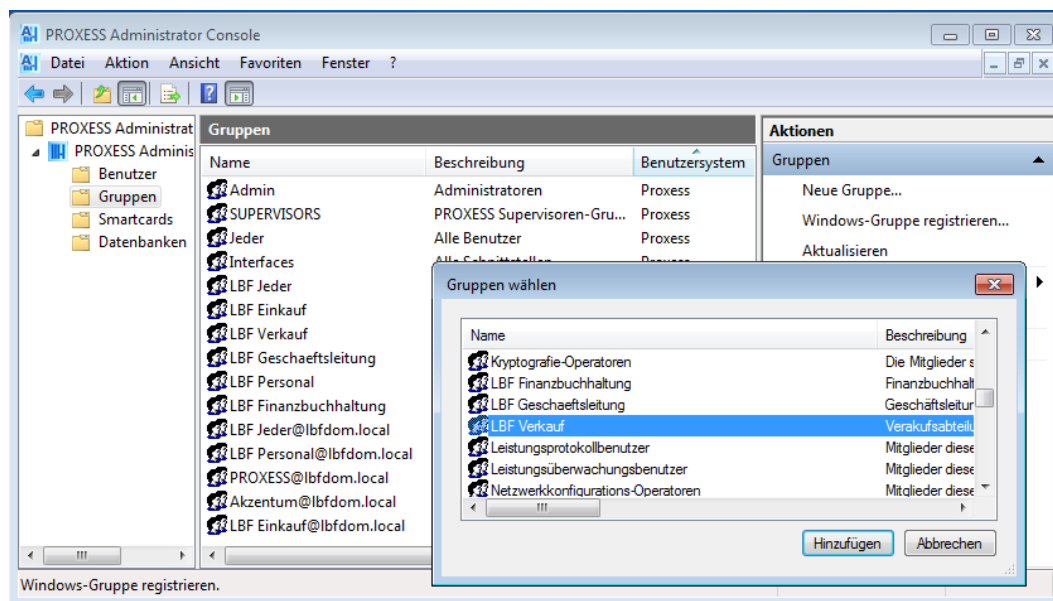
Fig.: Registration of a Windows AD group in PROXESS

Now select all the Windows groups that should be added for working with PROXESS. When the first Windows group is registered, all user data from these group members are adopted into the PROXESS user list. With the first registration of a Windows group, the main Windows authentication group and its members are also automatically adopted into the user management of the PROXESS Administrator Console. Users and groups transferred from Windows will be marked with the entry "Windows" in the "User system" column in the overview.

Example:
Select the Windows groups "LBF Sales", "LBF Purchasing", "LBF Financial Accounting", "LBF Senior Management" for registration in PROXESS. The group "LBF Everyone" is automatically adopted as well. Now the PROXESS system automatically adopts all login information of the group members. You can review this in the PROXESS user overview.

Fourth step: Assign PROXESS rights

Now assign the desired PROXESS access rights to the registered Windows groups. (See chapter: Access rights)

Warning information

⊘	**In the relevant group, you can only assign rights to members who are also members of the above-mentioned Windows authentication group (see above).**

Fifth step: Add a new Windows user

When the above-mentioned steps 1–4 are completed as in the example, new Windows users are automatically adopted into the PROXESS user management via their group memberships. By being added to a Windows group, this user will also automatically receive the PROXESS access rights assigned to this group. The prerequisite for this is again that the user's Windows group is part of the Windows authentication group.

Summary: This means that a separate user and rights management is no longer required for PROXESS.

Dokumentation PROXESS Admin Console

Logged-on users

Select the branch "Logged-on users" under the "Users" node.

Now you will see a list of all currently logged-in users in the middle pane. You can also export this list as a TXT file.

User management—concept and overview

Only registered users can work with PROXESS. In order to perform user management tasks, you must be a <u>supervisor</u> or <u>database area administrator</u>.

The PROXESS user management tasks are:

- Creation of a system-wide user concept
- Implementation of the concept through the creation of user accounts and groups
- Management and maintenance of user accounts and groups
- Setup and maintenance of access permissions

Active directory users versus PROXESS users

As system administrator, you should organizationally divide all users who work with PROXESS into two user categories.

<u>1. Users with Windows authentication</u>
The system administrator adopts the user data from the Windows Active Directory for these users to avoid double administration in Windows and PROXESS. Users transferring from AD select the authentication option "Windows" in the login dialog of the respective module when logging into PROXESS. Then the Windows login information is automatically used for login to PROXESS. Here, it is recommended to suppress the login dialog for AD users in the respective module settings after the first login.

Members of this category, however, do <u>not</u> have any access to high-security databases—e.g., those for which high security and encryption are activated. This aims to prevent a situation where AD users automatically receive access rights to particularly sensitive documents and data in PROXESS simply by being assigned to an AD group, without these having to be explicitly declared in PROXESS. In practice, this will probably affect the majority of users who, for example, are not members of senior management or HR, and so do not need any access to specially protected data. For these users, Windows Active Directory integration can help to avoid double administration, thus making work easier for the system administrator. This also enables automatic login to the PROXESS modules for the user.

All steps for the Windows Active Directory Integration in PROXESS are described <u>here</u>.

All steps for the Windows Active Directory Integration in PROXESS are described in the chapter "Windows Active Directory Integration".

Warning information

⊘	Authentication via Windows does not enable access to "secured" databases, meaning those with activated high security and encryption. Only the correspondingly authorized users of the internal PROXESS user administration can access these databases.

<u>2. Users with PROXESS authentication</u>
Members of this category can access high-security databases (e.g., employee database) if they have been granted the necessary access rights in PROXESS. In practice, this will most likely be limited to a smaller circle of users (e.g., senior management/HR department). These users are created and managed directly in PROXESS. When logging in to PROXESS, the user selects the authentication option "PROXESS" and enters their PROXESS user name and password.

You can find all explanations about the internal PROXESS group and user management in the "User management"

Dokumentation PROXESS Admin Console
chapter.

Warning information

⊘	Avoid users with a "double identity" as Windows AD users and PROXESS users. Users should generally log into all PROXESS modules with one and the same authentication to ensure that they get a consistent basis for the data and access.

Also see:

Access rights—concept and overview

Delete user

For security reasons, user accounts in PROXESS can only be blocked, not deleted.

In contrast to the permanent deletion of a user account, this keeps the user information visible in existing documents after the users are blocked.

Dokumentation PROXESS Admin Console

Create users

Use this function only if you want to create users of the user category "PROXESS Authentication" (also see User administration tasks). To create users in the "Windows Authentication" category, please follow the instructions in the chapter Windows Active Directory Integration.

The creation of users is supported by an assistant that enables you to create as many users as you like simultaneously and assign properties to them.

First step: Create user data

Connect to your PROXESS system via the PROXESS Administrator Console as a supervisor.

Select the directory "Users".

Select the **New User** command in the action panel on the right, in the "Action" menu or using the context menu.

The user assistant opens (see below).

Enter the user data and confirm your entries with the **Add** command.

Now the created user appears in the right window area.

Use the context menu to access the dialog **Advanced properties** of the user.

This enables you to add more users.
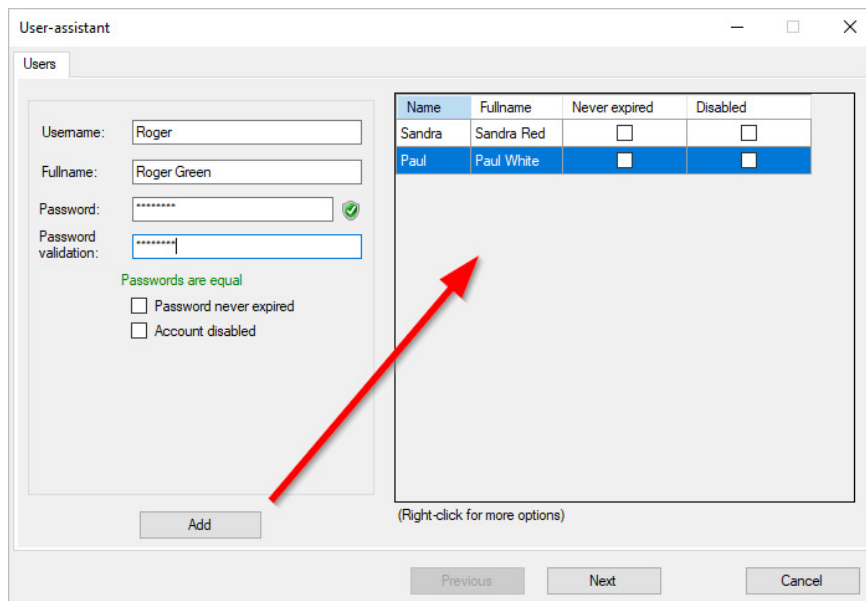
Fig.: Dialog field to create a new user account

Explanations of the user data:

User name	Here you enter a nickname for the new user, e.g., a common short name in your company. The new user will use this name to log into PROXESS.
Full name	Here you enter the user's full name. This can be the first and last name or a functional description. The full name appears in the status bar after logging into PROXESS.

Password/ password confirmation	You have to assign a password to the new user. The following password rules apply: - The password field may not be empty. - The password must have at least eight characters. - The password may not be identical to the user name. - The password must contain at least one number or a special character. All symbols aside from a–z, A–Z and 0–9 are considered special characters. - The password must contain at least one lowercase and one uppercase letter. A green symbol next to the password field indicates that all conditions have been met and the password is valid.
Password never expires	If you activate this check box, the password for this user will remain valid indefinitely. If the check box is not activated, the password will expire after a period of time. After the first login, users will be requested to change their password within the next 14 days. If they do so, the validity period configured in the "PROXESS Registry Setup" program will be valid for the new password (see below). Important: An "empty password" will also expire if this is activated in the system.
Account is locked	A user account can be blocked temporarily or permanently. This lets you comfortably carry out system operations, for example. Users can't be deleted, since your user data may be linked to archived documents. For that reason, you can block the accounts of employees who have left the company here. You can remove the block on a user account at any time.

Warning information

⊘	**For security reasons, user accounts can only be blocked, not deleted.** In contrast to the permanent deletion of a user account, this keeps the user information visible in existing documents after the users are blocked.

Tip

🔆	The validity period of user passwords can be limited in PROXESS. This system function must first be activated system-wide in the "PROXESS Registry Setup" program. You can change the relevant settings in the option field **Maximum password age** under the menu item Document Manager/User Registration. The option **Password never expires** is the default setting after the installation. Setting the option **Password expires after n days** (n: maximum password age in days) activates the verification of the password process.

Tip

🔆	You are unable to see which password a user is currently using. You can reset current passwords if users have forgotten their password. Users can also change passwords themselves in the PROXESS Standard Client and PROXESS Web Client.

Second step: Adding users to groups

You can assign users to one or more groups or perform a multiple assignment.

1. Individual assignment

Choose a user in the dialog box below. The currently selected user will always be displayed in the info field under "Currently selected user for individual assignment".

In the right column with the header "Not member of", mark the desired group that you want to assign. You can also mark multiple groups

at once and assign them simultaneously.

Select the **Assign command.** Now the assigned group(s) is/are shown in the middle column "Member of".

You can similarly remove individual users from one or more groups simultaneously.
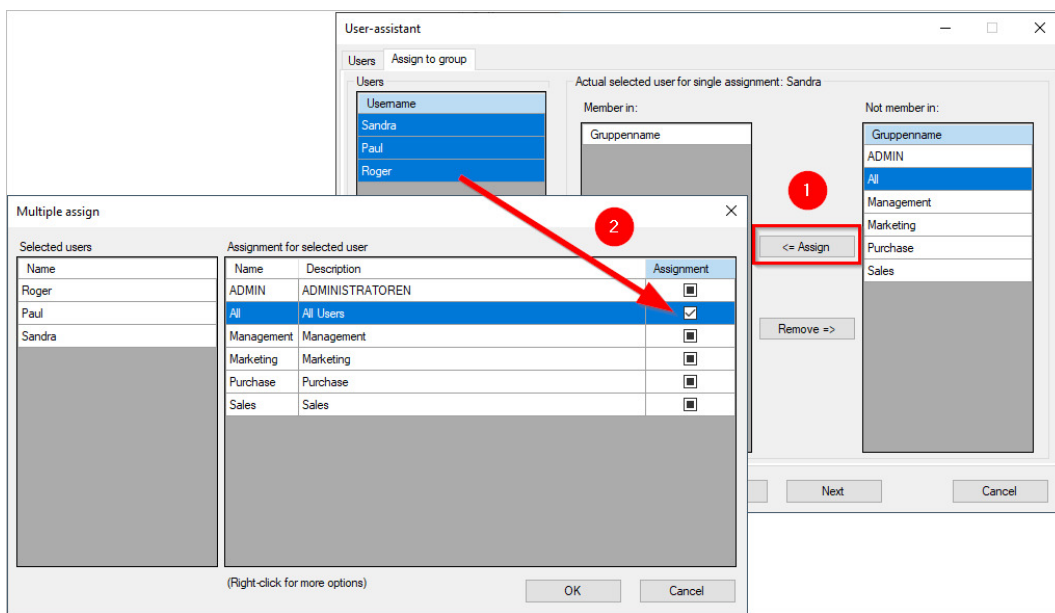
2. Multiple assignment

Select multiple users simultaneously.

Use the right mouse button to access the multiple assignment.

The dialog box "Multiple assignment" will appear at the bottom.

Select the desired groups and conditions.

Confirm your selection with **OK**.

You have the following options for the multiple assignment:

☑ **Check mark placed**	The selected users are added to this group.
◼ **Green or black box**	The selected users are not added to this group. If they are already a member of this group, however, they will not lose their group membership. I.e., the current status is retained.
☐ **Empty check box**	The selected users are removed from the group.

If all users are assigned to the group, click the **Next** button.

A confirmation dialog appears. Confirm your settings here with the **Create** button to actually add the new users.
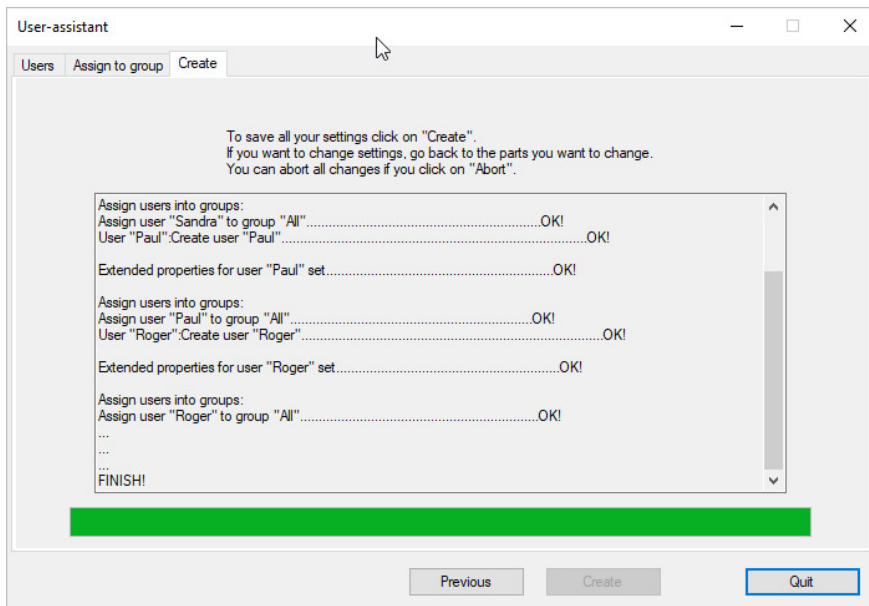
You will receive a log and confirmation that all settings were saved successfully.

Dokumentation PROXESS Admin Console

Manage user properties

Connect to your PROXESS system via the PROXESS Administrator Console.

Select the directory "Users" and choose the desired users. Double-click to open the Properties dialog. Alternatively, select **Properties** in the action panel on the right, in the "Action" menu or by using the context menu.

The following dialog box appears:

Fig.: General user properties of the user "Andrea Stern".

General properties

The **general properties** for a user include the short and full name, password expiration period and the blocking/unblocking of the user account. You can change these properties if needed. For users in the user category "Windows authentication", however, the fields user name and full user name are deactivated. These properties can only be changed via the Windows Active Directory. The changes applied there are automatically adopted into the PROXESS user properties.

Warning information

|	
⊘	Users can't be deleted, only blocked. This ensures that user-specific logs in the system (e.g., for the creation or processing of documents) won't get lost. You can hide blocked users through a filter function so that only active users are displayed.

Group membership of a user

Under the "**Member of**" tab, you can define the user's group memberships. A user can be a member of one group, several groups or none:
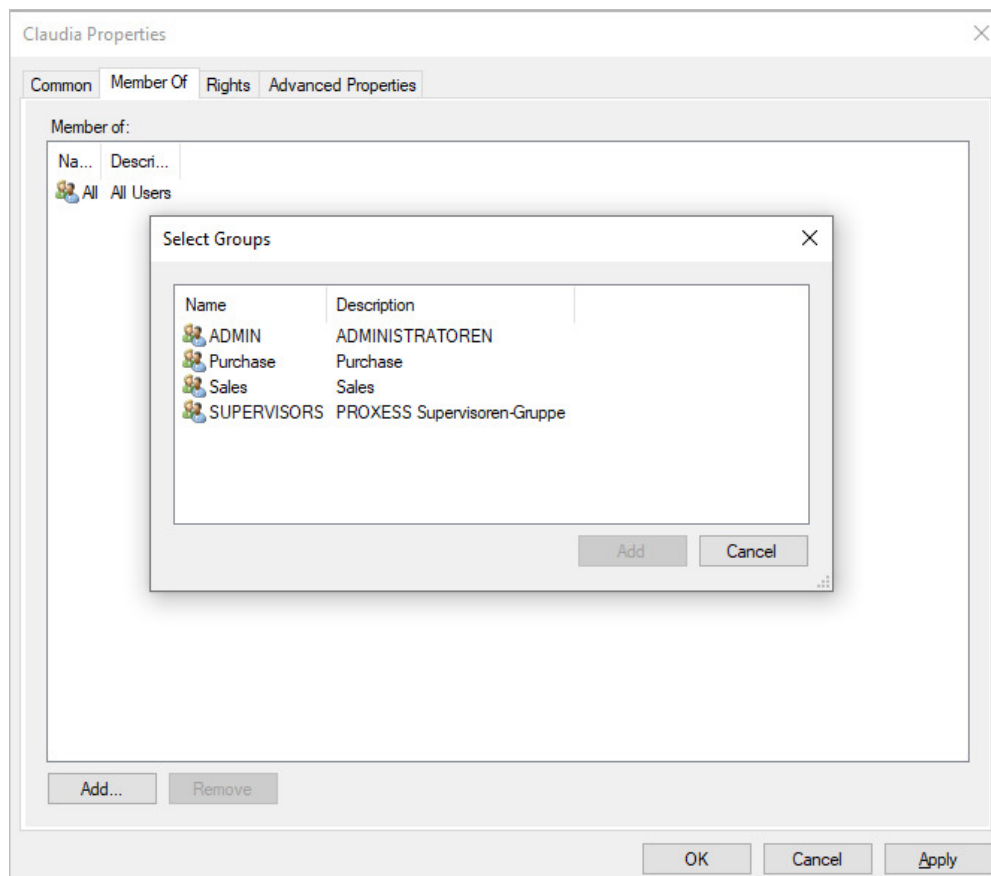
User rights

All access and action rights of the user of the connected archive database are shown under the "**Rights**" tab. Of course this presumes that you have previously connected to a database. The management of access rights is explained in the chapter "Access rights".

Dokumentation PROXESS Admin Console
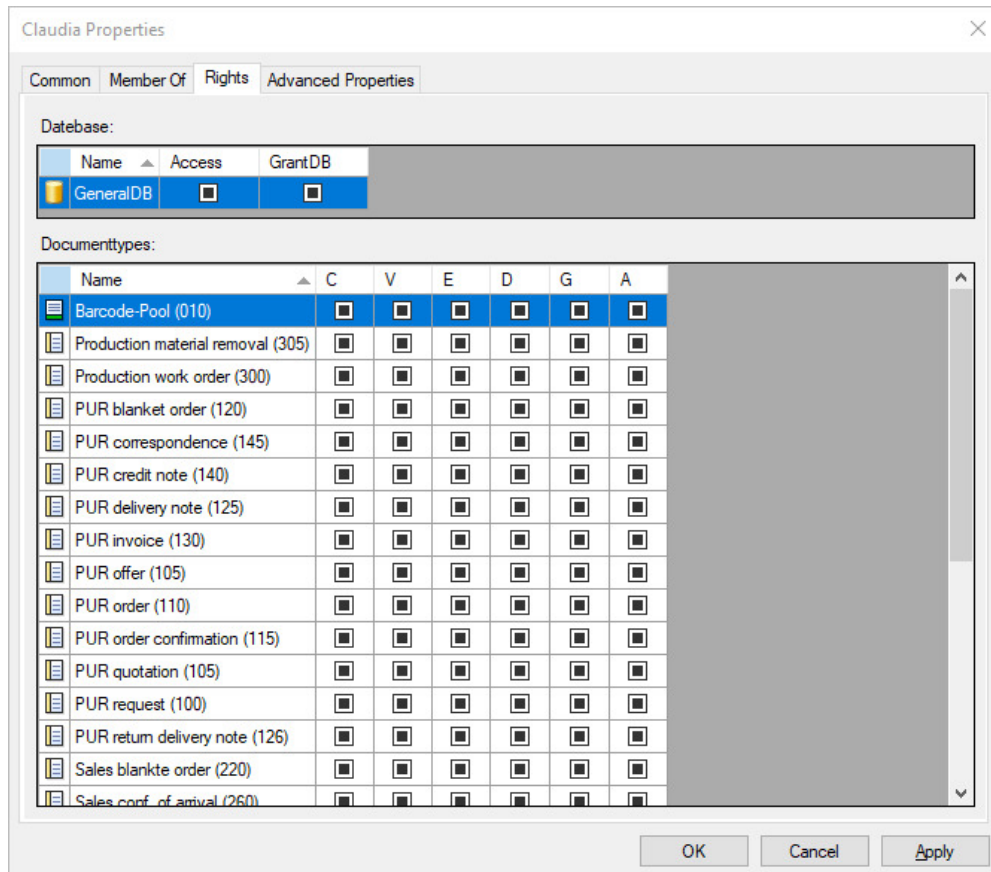
Tip

	It has proven effective in practical experience to grant rights on a group level and assign users according to the groups. If a user is a member of a group, the user will also get the corresponding rights. This is why the assignment of members to groups should be based on which rights a user should get.

Advanced properties

All contact and address data of a user are managed in PROXESS under the "**Advanced properties**" tab. These values can be used for the configuration of **External thesauruses**, for example.

You can pre-allocate the properties of the respective user here. The properties entered in the AD user management are automatically adopted here. Under **Display name**, enter the name that should be displayed when the user sends e-mails. Under **E-mail address**, enter the user's valid e-mail address. The associated SMTP settings are automatically entered by the system.

Also see:

Access rights—concept and overview

Managing database rights

Managing document type rights

Dokumentation PROXESS Admin Console

Export user list

With the **Export list** command in the context menu of the user node, you can export the displayed user list as a TXT
file (also see: Filter and display blocked and active users)

Filter and display blocked or active users

You can filter all users with these properties to get an overview of your active and blocked users.

To do this, mark the "User" directory. Now select the command **Filter** in the action panel on the right, in the "Action" menu or by using the context menu.

The following dialog appears:

Fig.: Filter users according to active/blocked

By default, all users in the user list are shown on the right. If you only want to see e.g., active users in the user list, place the check mark for Active, as shown above.

With the **Export list** command in the context menu of the user node, you can export the displayed list as a TXT file.

Create a group

Groups consolidate users who are intended to receive the same rights. This means you don't have to assign rules individually to every user. You can do this on a group basis instead. Whether you work with groups or individual users depends on the number of PROXESS users at your company and on the specifications from the organizational analysis.

First step: Create groups

Select the "Groups" directory and choose the command **New group** in the action panel on the right, in the "Action" menu or using the context menu.

Enter a group name and description for your new group.

Confirm your entries with the **Add** command. Now the new group is displayed in the right area of the window.

You can remove a marked user from the list via the context menu.

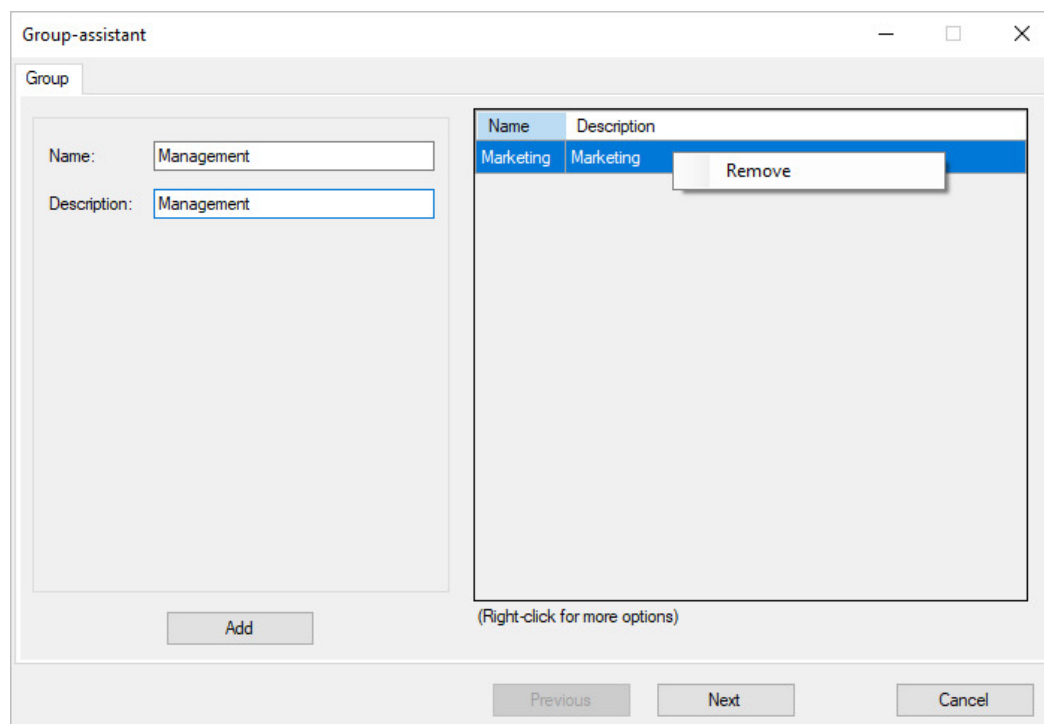This enables you to create multiple groups at once.

Fig.: Create groups

Second step: Add users to the group

You can assign groups to one or more users or perform a multiple assignment.

1. Individual assignment

Choose a group in the dialog box below. The currently selected group will always be displayed in the info field under "Currently selected group for individual assignment".

In the right column with the header "Not member of", mark the desired users that you want to assign. You can also mark multiple users at once and assign them simultaneously.

Dokumentation PROXESS Admin Console

Select the **Assign command.** Now the assigned user(s) is/are shown in the middle column "Member of".

You can similarly remove users from a group.

2. Multiple assignment

Select multiple groups simultaneously.

Use the right mouse button to access the multiple assignment.

The dialog box "Multiple assignment" will appear at the bottom.

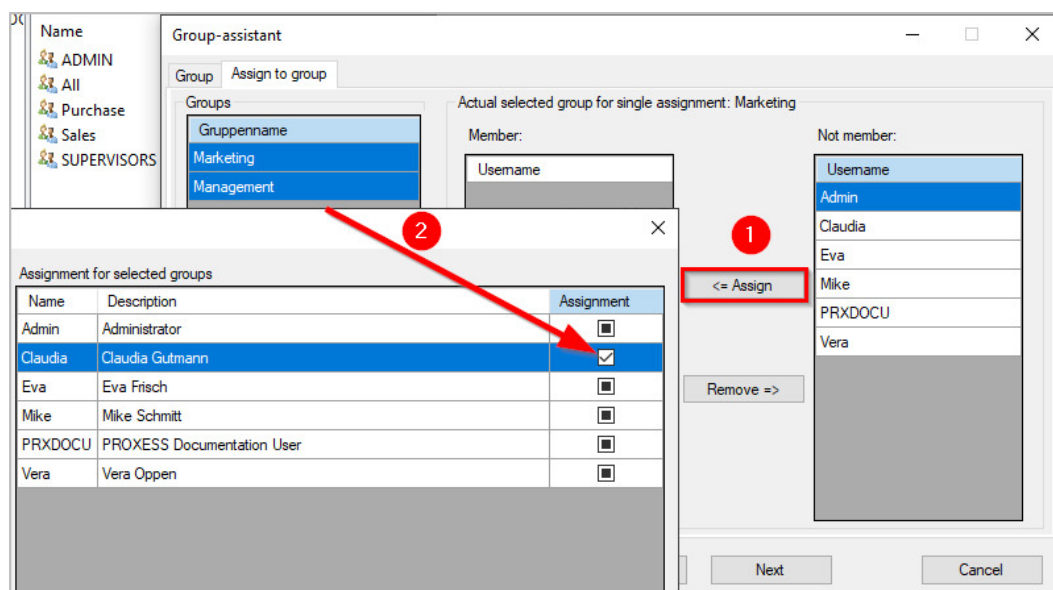Select the desired users and conditions.

Confirm your selection with **OK**.

Fig.: Assigning users to one or multiple groups

You have the following assignment options:

✅ **Check mark placed**	The selected users are added to these groups.
⬛ **Green or black box**	The selected users are not added to this group. If they are already a member of this group, however, they will not lose their group membership. I.e., the current status is retained.
☐ **Empty check box**	The selected users are removed from the group.

Third step: Assign database rights

Here you can also grant access rights to the databases to individual groups (1) or perform a multiple assignment (2) as above.
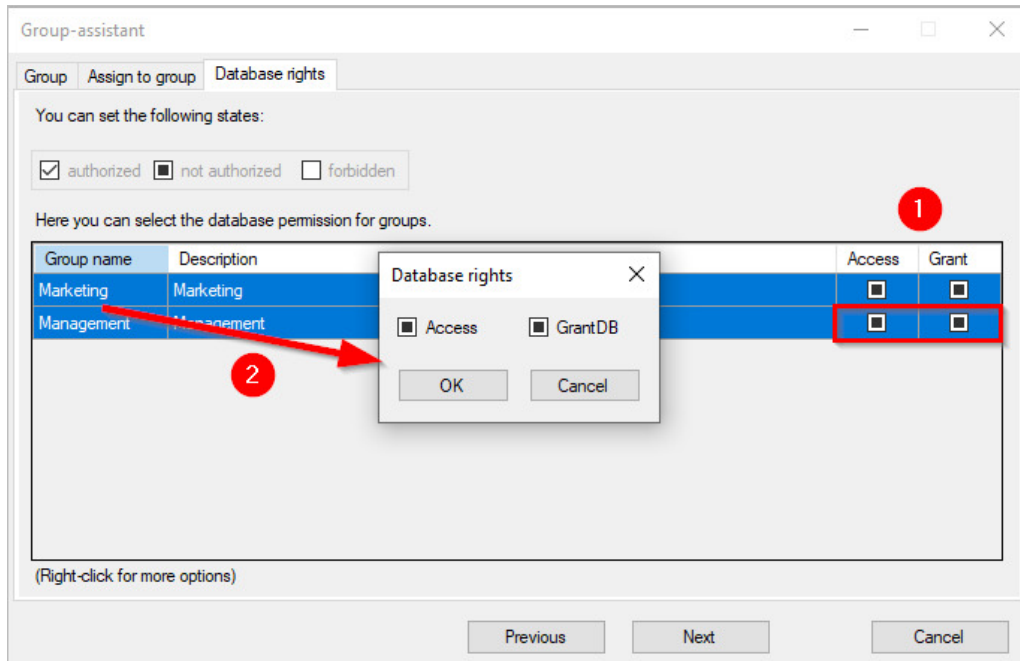
Fig.: Assign database rights to one or multiple groups

Fourth step: Grant document type rights

In the final step, the document type rights are assigned to the newly created groups.

Here you also have the option to mark only a single document type and grant the rights on a group level.
If you mark multiple groups at once, you have the option to grant rights to the document type to all marked groups simultaneously via the context menu.
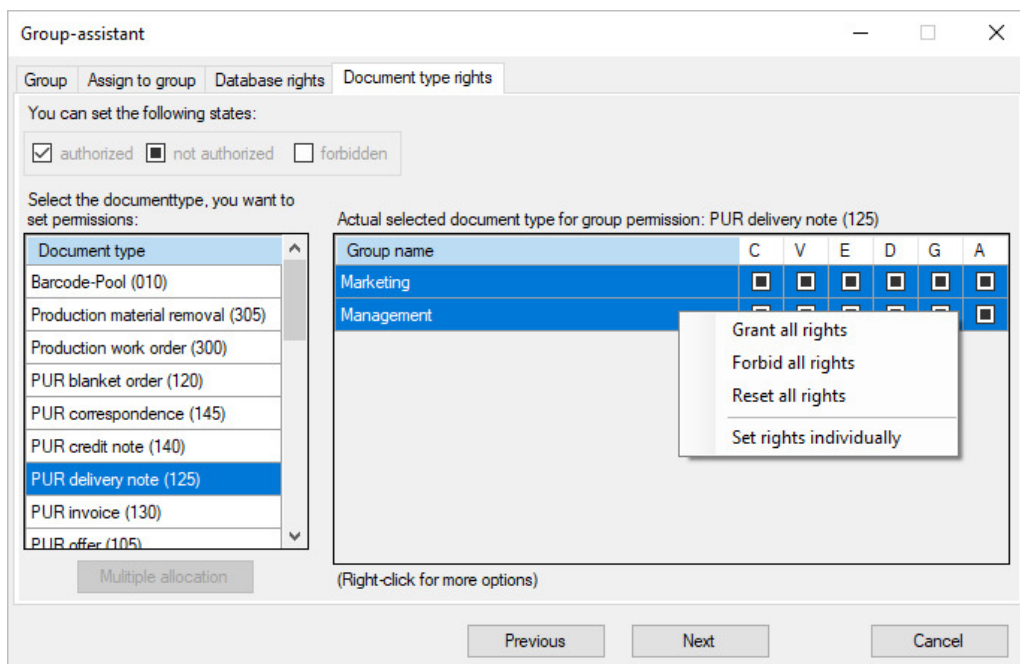

Fig.: Granting rights for a single document type

Please mark multiple document types for multiple assignments.

Then select the command **Multiple assignment** in the context menu.

Dokumentation PROXESS Admin Console

This dialog box appears: Multiple assignment for document type rights.

In the right area of the window, now grant the rights that should apply to all document types at once.
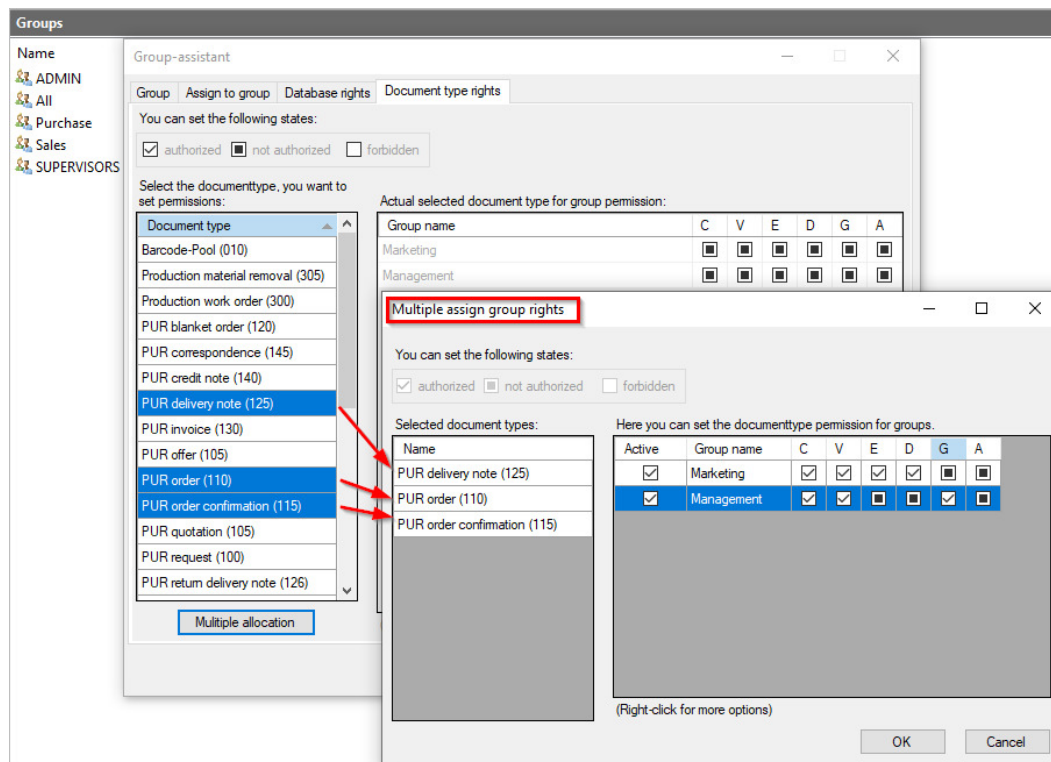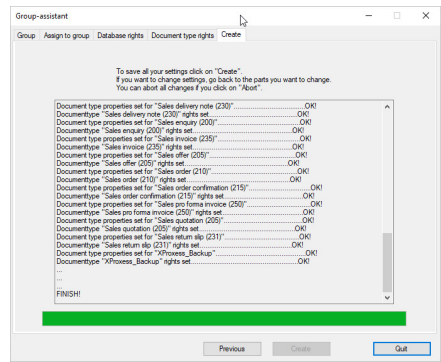

Fig.: Multiple assignment for document type rights

With the **Create** command, all of the applied settings are saved.

If you want to **edit** the settings, just switch to the respective tab.

The created groups can be discarded with the **Cancel** command.

-

Overview of functions for groups

Select the "Groups" directory in the user management and open the context menu:

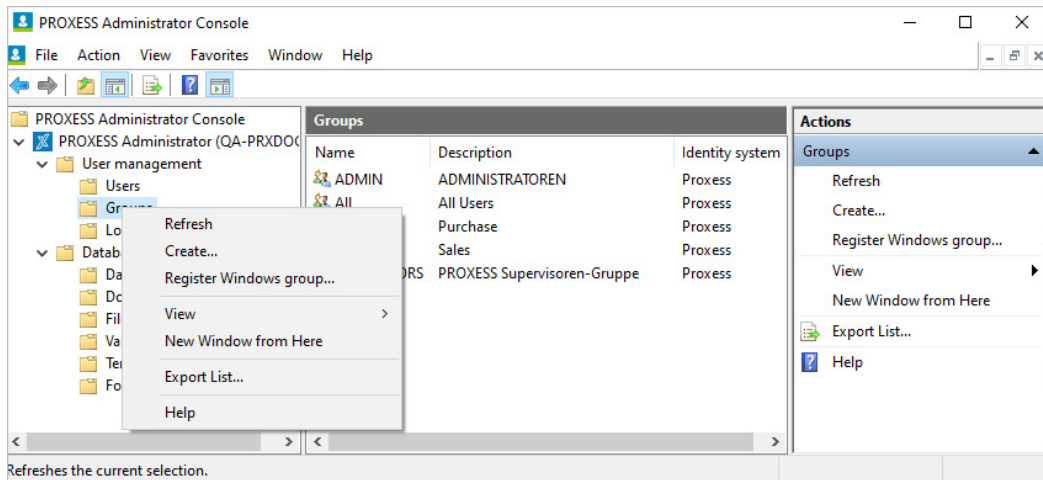*Fig.: Overview of functions for group administration*

New Group...	Creates a new user group
Register Windows group	Opens the Windows user management to adopt the existing Windows user groups and their members in the PROXESS Administrator Console
Update	Updates the current display
View	Contains commands to adopt the current window layout (e.g., to display columns)
Open new window here	Opens a new window starting from this node. This command can help get a better overview of an extensive range of adjustments. If you work simultaneously in several windows, the **Update** command is useful.
Export list...	With the **Export list** command in the context menu of the middle area of the window, you can export the displayed list as a TXT file. You can e.g., export a list of all users, all logged-in users or a database list.
Help	Opens online help

Manage PROXESS group

No users can be added or deleted in groups in the "Windows Authentication" category here. These properties can only be changed via the Windows Active Directory. The changes applied there are automatically adopted into the PROXESS group properties.

Connect to your PROXESS system via the PROXESS Administrator Console as a supervisor.
Select the "Groups" directory and choose the desired group. In the "Action" menu, choose the **Properties** command.

The following dialog box appears:

Fig.: Properties of the "Human Resources" group

The general properties for a group include the group name and description. You can change these properties at any time if needed. No new group is created by changing the two entries. The fields "Group Name" and "Description" are deactivated for groups in the "Windows Authentication" category. These properties can only be changed via the Windows Active Directory. The changes applied there are automatically adopted into the PROXESS group properties.

You can define which users are members of this group under the "Members" tab. A user can be a member in no group or in multiple groups.

Fig.: List of group members

With the **Add** command, you can see a list of all users who aren't a member in this group yet and can assign them according to the group.

If you mark one or more users simultaneously, you can use the **Remove** command to remove group members from the group.

Your changes only go into effect with the **OK** or **Apply** command.

All access and action rights of the user of the connected archive database are shown under the "**Rights**" tab. This presumes that you have previously connected to a database. The management of access rights is explained in the chapter "Access rights".

Tip

	It has proven effective in practical experience to grant rights on a group level and assign users according to the groups. If a user is a member of a group, the user will also get the corresponding rights. This is why the assignment of members to groups should be based on which rights a user should get.

Also see:

Access rights—concept and overview

Managing database rights

Managing document type rights

Change PROXESS password

Setting or changing passwords is only possible here for users of the "PROXESS" authentication category.   User properties such as the user name and password for "Windows Active Directory users" can only be processed through the Windows Active Directory. Then these changes are automatically adopted in PROXESS.

Connect to your PROXESS system via the PROXESS Administrator Console as a supervisor or database area administrator.

Select the directory "Users" and choose the desired users.

Choose the command **Set password** in the action panel on the right, in the "Action" menu or using the context menu.
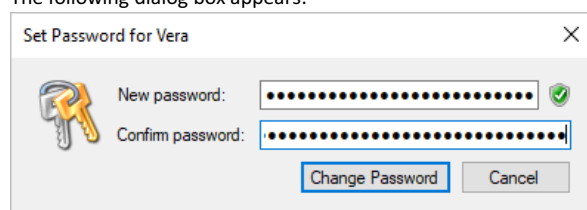
The following dialog box appears:

Fig.: Setting or changing the password for a PROXESS user

Here you can assign a new password.

The following rules apply to the assignment of a password:
- The password field may not be empty.
- The password must have at least eight characters.
- The password may not be identical to the user name.
- The password must contain at least one number or a special character. All symbols aside from a–z, A–Z and 0–9 are considered special characters.
- The password must contain at least one lowercase and one uppercase letter.

A green symbol next to the password field indicates that all conditions have been met and the password is valid.

Tip

	For security reasons each user, after logging in for the first time with a reset password, should change this password into an individual one again. Users can change their passwords in the PROXESS program.

Also see:
Managing users (password never expires)

Dokumentation PROXESS Admin Console

PIN management of PROXESS supervisor smartcards

As a PROXESS supervisor, a user logs into PROXESS with a supervisor smartcard and PIN. The supervisor is authorized to manage users and groups, grant and revoke access and management rights and activate PROXESS security options such as field encryption.

The preset standard user and admin PIN of a supervisor smartcard is "1234".   Smartcards and PINs are managed via the program Gemalto Classic Client Toolbox.

Warning information

⊘	**For security reasons, PROXESS GmbH strongly recommends changing the two standard PINs into individual PINs.**
	In order to prevent the uncontrolled or unauthorized activation of the security options in PROXESS, we urgently recommend against sharing the smartcard with third parties.

Each PROXESS supervisor smartcard has an admin PIN and a user PIN. The user PIN is used by supervisors to log into the PROXESS system with their smartcard. The admin PIN is used exclusively for the internal management of the smartcard. Logging into the program Gemalto Classic Client Toolbox with the admin PIN makes it possible not only to change the user PIN and admin PIN but also to unblock a user PIN that has been blocked due to multiple incorrect entries. In that sense, the admin PIN of a smartcard can be compared to the PUK code of a cell phone SIM card.

Recommendation: To ensure that the smartcard can be unlocked at a later time, a smartcard administrator should be responsible for changing admin PINs before issuing supervisor smartcards.

Changing the smartcard user PIN

Insert the smartcard in the smartcard reader and connect the smartcard reader to your computer.
Start the Gemalto/Classic Client Toolbox program and select **PIN management** in the "card administration" menu.
Mark the connected smartcard reader and select the **Change PIN** command.
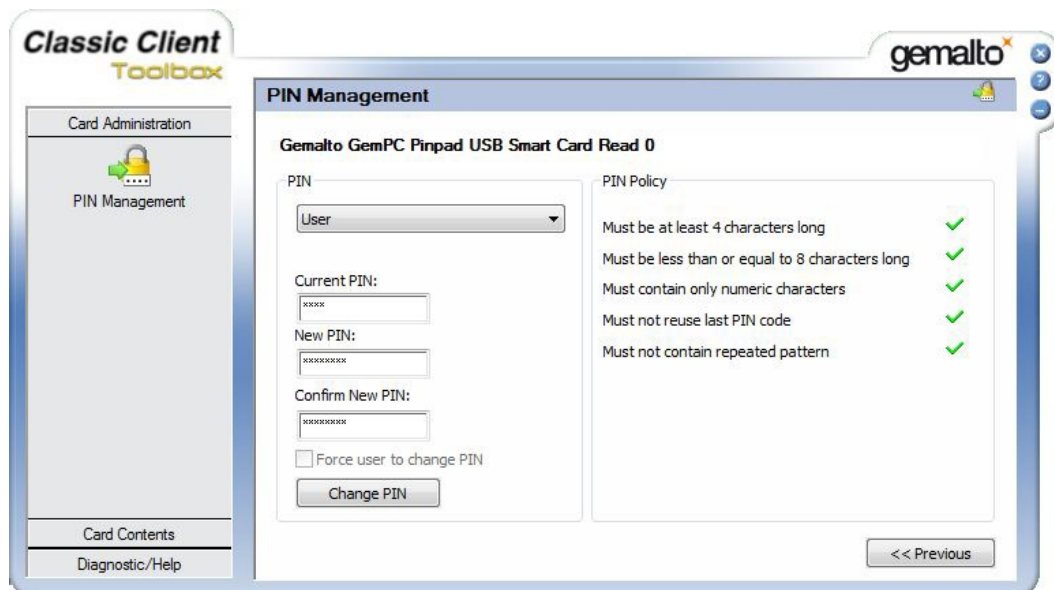

Fig.: Dialog box to change a smartcard user PIN

Select the **User** option for the PIN selection.

Now enter the current and new user PIN via the computer keyboard. In the course of entering the new PIN, the PIN security guideline is checked. This means that your new PIN is reviewed to ensure that it follows the security requirements regarding length, character contents and repeated characters. The result is indicated with red crosses or green check marks. All criteria have to be met for a PIN to be changed.

The **Change PIN** command applies the change. You will get a confirmation that your change was completed successfully.

Changing the smartcard admin PIN

Proceed as under "Changing the smartcard user PIN", but select the **Admin** option in the "PIN" selection field.

Unblocking the smartcard user PIN

Proceed as under "Changing the smartcard user PIN", but select the **Unblock PIN** command.

In contrast to the PIN change, only the **User** option is possible in the **PIN** field of the dialog box. In the **Admin PIN** field here, enter the corresponding admin PIN of the inserted smartcard. Compliance with the PIN security guidelines is reviewed here as well (see above). The **Unblock PIN** command applies the change. You will get a confirmation that your change was completed successfully.

Warning information

⊘	**A supervisor smartcard with an admin PIN that has been blocked due to multiple incorrect entries can no longer be unblocked. It should be changed to the "Withdrawn" status in the PROXESS Administrator Console and replaced with a new supervisor smartcard.**

Withdraw smartcard

If you want to permanently withdraw a supervisor's <u>supervisor privileges</u> or if the card should be permanently blocked (e.g., if it is lost), select the option "**Withdraw smartcard**".

The option "<u>Block smartcard</u>", in contrast, is used when the supervisor privileges should be revoked only for a specific time. You can block a user's card as a precaution, for example, if the user is on vacation or handling other tasks at the company for a certain time period (e.g., a stay abroad).

As supervisor, use your smartcard to connect with the registered PROXESS system.

Select the "Smartcards" folder and mark the desired user in the list. In the "Action" menu (alternatively via the user's context menu), select the function **Withdraw**.
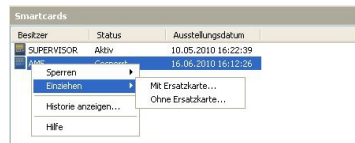
The following dialog box appears:

Fig.: Withdrawing the smartcard with/without replacement card for the user AME

The option "**With replacement card**" makes it possible to immediately assign a new, already prepared and created <u>smartcard</u> to the user. The option "**Without replacement card**" doesn't offer this option. In both cases a reason must be entered for the smartcard history.

Warning information

⊖	To ensure that the user can log in again with their user name and password, the user may not be a member of the "SUPERVISORS" group (see: <u>Manage groups</u>).

Block smartcard

The smartcard is blocked when the supervisor privileges should be revoked only for a specific time. You can block a user's card as a precaution, for example, if the user is on vacation or handling other tasks at the company for a certain time period (e.g., a stay abroad).

If you want to permanently withdraw a supervisor's supervisor privileges or if the card should be permanently blocked (e.g., if it is lost), select the option "Withdraw smartcard".

As supervisor, use your smartcard to connect to the registered PROXESS system.

Select the "Smartcards" folder and mark the desired user in the list. In the "Action" menu (alternatively via the user's context menu), select the command **Block/set block**.
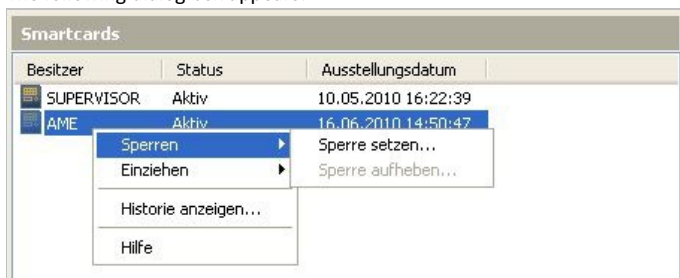
The following dialog box appears:

Fig.: Blocking of smartcard for the user AME
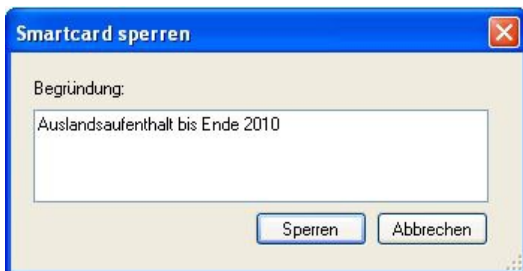
Enter a reason for the block:

Fig.: Reason for blocking the smartcard of user AME

The entered reason appears in the history of the smartcard. To access this, select the "Smartcards" folder again and mark the desired user in the list. In the "Action" menu (alternatively via the user's context menu), select the command **Show history**.

Dokumentation PROXESS Admin Console
Fig.: History of the smartcard of user AME

Assign smartcard

The action "Assign smartcard" is not carried out for the first supervisor smartcard. The first supervisor smartcard is already entered in the individual license file.

However, supervisor privileges aren't limited to a single user. For corporate reasons (e.g., for substitution rules), it can be expedient to grant supervisor privileges to two or even more people. You can also store a second supervisor smartcard as a replacement card in a safe place (e.g., notary public, bank safe).

If a supervisor logs in with a smartcard and PIN, no user name has to be entered. By assigning the PROXESS supervisor smartcard to a user, however, the user's actions can still be verified. The assignment lets PROXESS monitor which action the user is performing (e.g., the creation or deletion of documents, granting of access rights or the new creation of a user).

Before you can assign a new PROXESS supervisor smartcard, this smartcard must have already been prepared and created (also see "Prepare PROXESS supervisor smartcard" and "Create PROXESS supervisor smartcard").

As supervisor, use your smartcard to connect to the registered PROXESS system.

Mark the "Smartcards" folder and select the command **Assign smartcard** in the "Actions" menu (alternatively: context menu).
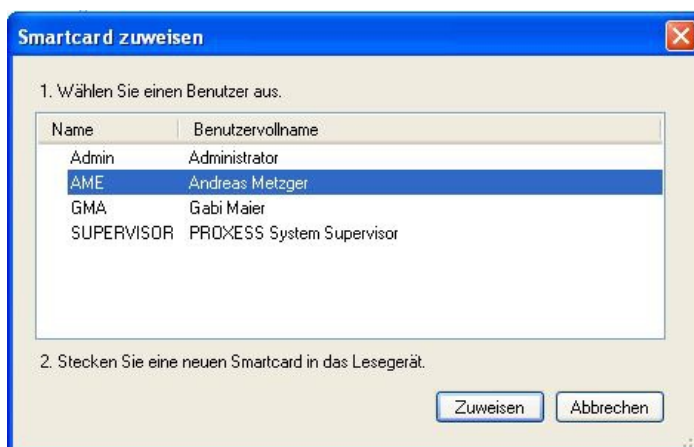
The following dialog box appears:

Fig.: Dialog box "Assign smartcard"

Mark the user to whom you want to assign the smartcard and select the **Assign** command.
Now the user appears in the "Smartcards" list in the "Smartcards" folder.

Warning information

> To ensure that the user can log into the system with the smartcard and PIN, the user must be a member of the "SUPERVISORS" group (see: Manage groups).

Dokumentation PROXESS Admin Console

Create file type

Archived files are assigned to a file type in PROXESS. File types are identified by a name and an extension. For every file type, programs can be specified that PROXESS users can use to view and process the archived files for this file type. Typical examples of file types are scanning, Word files or COLD files.

Step by step:

Connect to the desired database.

Select the "File type" branch in the database.

Select the command **New** in the context menu.
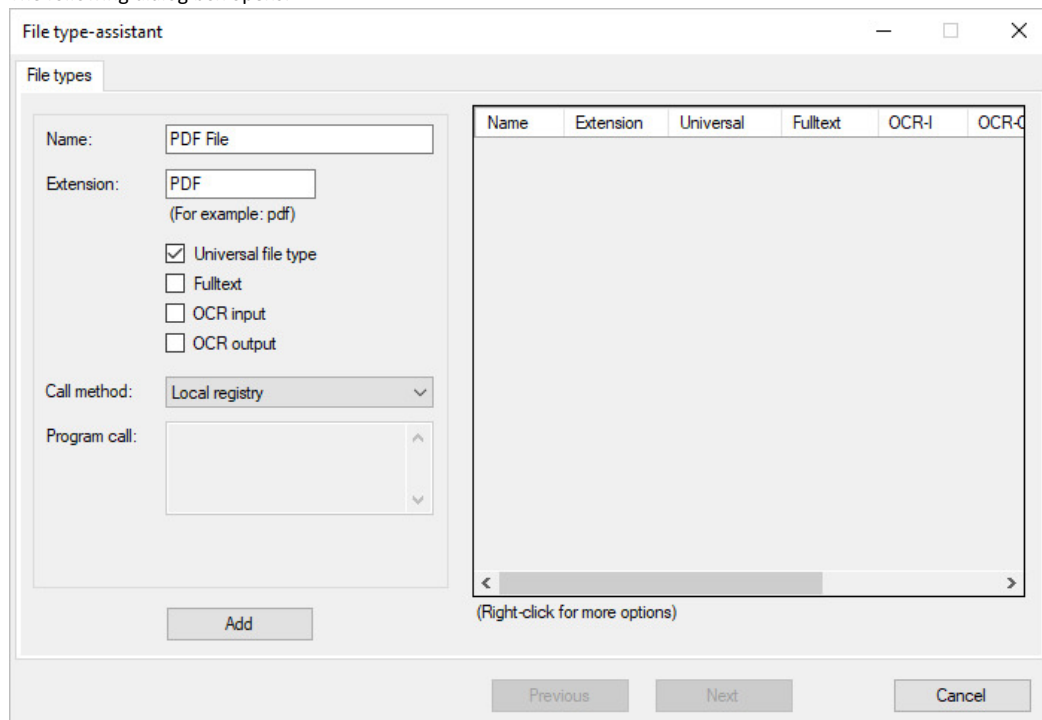
The following dialog box opens:

Fig.: Dialog box to create a new file type

Now select a name for the file type and the extension.

Explanations of the properties of a file type:

Name	Here you can change the name of the file type. The change will also apply to files that have already been archived in PROXESS.
Extension	This file extension generally corresponds to the usual file extension for the desired file-type application for processing the file.

Dokumentation PROXESS Admin Console

Universal file type	If this option is selected when the user creates a new file, the system will select the appropriate program from the local registry on the basis of the file extension and, if an entry is found there, the correct file extension will automatically be added to the file. This option is very useful, for example, if different files are selected and imported during an import from Windows Explorer.
Enable full text indexing	This is where the file type for the full text search is activated and unlocked. Requirement. (Also see: Properties of document types)
Activate OCR	Here you activate the file type for the OCR function.
For OCR input	Here you can activate the file type for OCR text recognition. However, the recognition process must be initiated manually in the PROXESS Client.

Example: You activate the "Scanning" file type for OCR input. |
| **For OCR output** | Here you can activate the file type for the output of recognized OCR text.

Example:
You activate the "Text file" file type for the OCR output and thus the recognized text is saved in exactly this file type. |

_____

Also see:
Link file type with application
Link file type with template file

Dokumentation PROXESS Admin Console
Link file type with application

To ensure that PROXESS starts the right application for a selected file type for creating, viewing and printing files, you link each file type with an application or program.

Double-click the file type to get to the properties window.

Select the "File type applications" tab here.
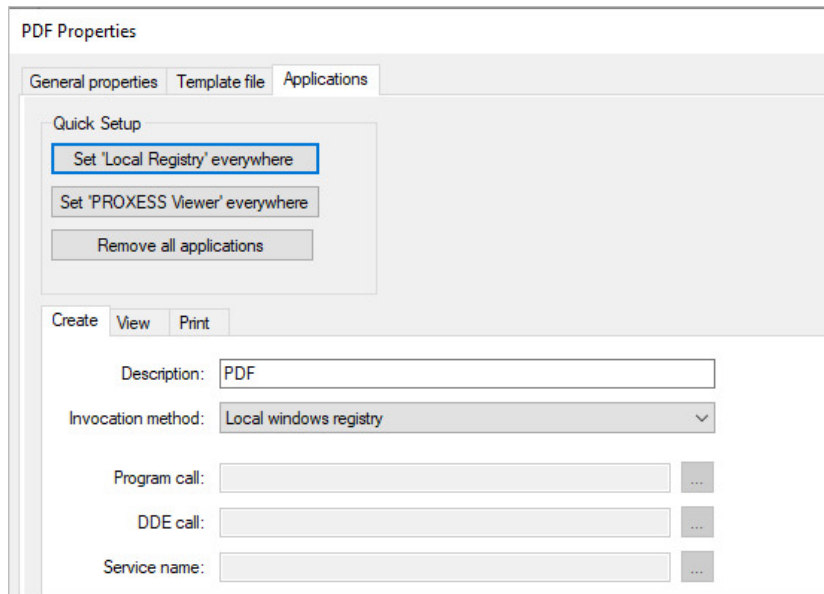
With the **Quick setup**, you can apply the standard settings with a single click for "Create", "View" and "Print" files.

You can select the following access methods for the three functions **Create, View and Print**:

Program call	Here you can manually store the program call for the application (e.g., Winword) that should open for Create, View and Print.
	If you have installed a program at your workplace that is linked with the file name extension of this file type, the syntax for the program call is automatically inserted from the system registration.
DDE	This option applies to all DDE-capable programs, e.g., for Microsoft Word or Excel.
	If you have installed a program on your computer that is linked with the file name extension of this file type, the syntax for the DDE call is automatically inserted from the system registration.

Dokumentation PROXESS Admin Console

Local registry	The **Local registry**Option is used to quickly and automatically integrate applications. It ensures that each client computer from the system registration searches for a program associated with the file name extension for this file type. This method makes sense for computers with very different installations. Another advantage: you don't need to detect the correct access method but are using already available system information. When you use the **Local registry**option, you don't have to fill in the input fields. **Tip** This is the correct setting for the universal file type.
Scan	For scanned documents, you only have to activate the **Scan**option, since PROXESS's own DLLs are used for the access. The input fields stay blank.
Diaclip	Activate the Diaclip option for the Diaclip PROXESS module. Additionally, enter one or more parameters in the field **Program call**. The correct syntax: App=notepad.exe %1 Tiff=\\<Server>\<Path>\<Filename>.TIF XOffset=0 YOffset=0 FontWidth=144 FontHeight=240 LineHeight=240 CountLines=1 MaxLines=72 is automatically entered by the system so that you only have to add the appropriate values. (Also see: Parameters for Diaclip)

Properties of file types

File types are identified by a title and an extension. They are associated with programs which the user applies to view and process the respective file type in PROXESS. Examples of file types are scanning or Word files or COLD files.

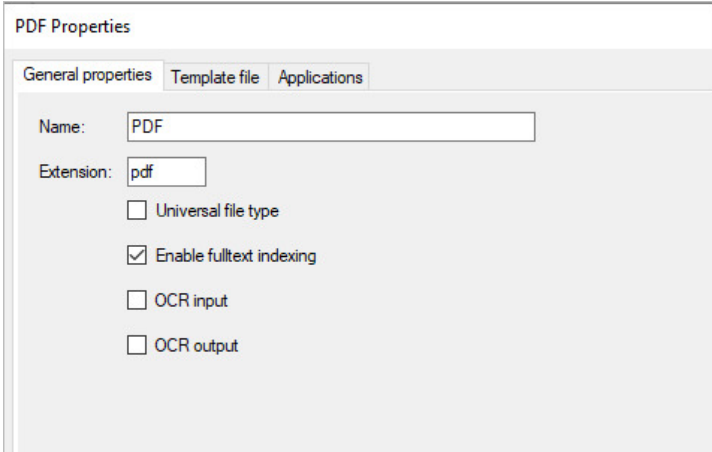Double-click the file type to get to the respective properties window:

Fig.: Properties of the "PDF" file type

Name	Here you can change the name of the file type. The change will also apply to files that have already been archived in PROXESS.
Extension	This file extension generally corresponds to the usual file extension for the desired file-type application for processing the file.
Universal file type	If this option is selected when the user creates a new file, the system will select the appropriate program from the local registry on the basis of the file extension and, if an entry is found there, the correct file extension will automatically be added to the file. This option is very useful, for example, if different files are selected and imported during an import from Windows Explorer.
Enable full text indexing	This is where the file type for the full text search is activated and unlocked. Requirement. (Also see: Properties of document types)
Activate OCR	Here you activate the file type for the OCR function.
For OCR input	Here you can activate the file type for OCR text recognition. However, the recognition process must be initiated manually in the PROXESS Client. Example: You activate the "Scanning" file type for OCR input.

Dokumentation PROXESS Admin Console

For OCR output	Here you can activate the file type for the output of recognized OCR text. Example: You activate the "Text file" file type for the OCR output and thus the recognized text is saved in exactly this file type.

Dokumentation PROXESS Admin Console

Universal file type

The universal file type makes it easier to import files e.g., from Windows Explorer.

If the universal file type is selected when importing a file with the PROXESS Windows Client, the corresponding program is automatically read from the local registry on the basis of the file extension in Windows Explorer.

This avoids the need to enter and configure all possible file types separately.

For that reason, it is recommended to create a universal file type.

Step by step:

Connect to the desired database.

Mark the **File types** node in the branch **Managing the database**.

Now select the command **New** in the context menu.
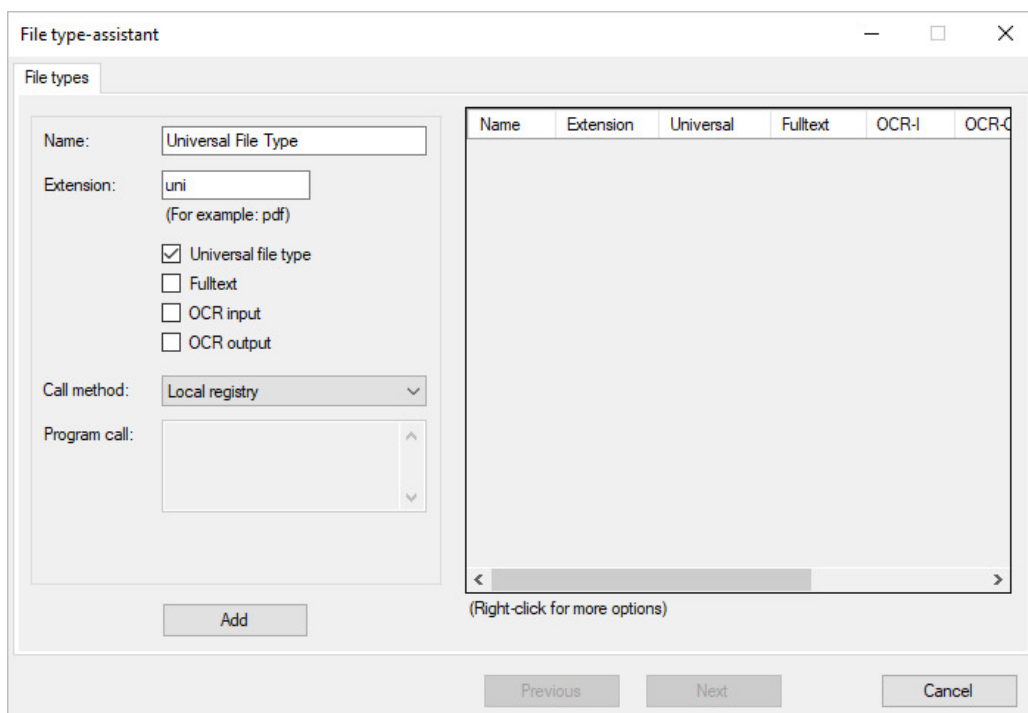
The dialog "Create file type" appears:

Fig.: Dialog box to create a universal file type

In principle, you can use any name and any extension. We recommend the entries listed above.

Activate the property **Universal file type**.

Confirm your entries with the **Create** command.

General database properties

Mark the "Databases" branch in the console root of the PROXESS Administrator Console.
Mark the database to be managed and select the **Properties** command and **General** tab in the context menu ("right mouse button").
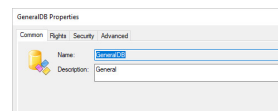

Fig.: General database properties of the "Personnel" database

Here you can change the **description** of the database.

The **name** of the database can't be changed, since it must correspond to the database name in the underlying SQL database.

_____

Also see:
Managing database rights
Database security (logging)

Delete database

If you no longer need a database, e.g., a test database, you can delete it again. This is only possible if users are no longer connected to this database. A warning appears that you must confirm to perform the actual deletion.

Step by step:

Select the "Databases" branch in the left pane.

Mark the database that you want to delete in the database list.

In the "Action" menu (alternatively via the context menu), select the function "Clear".

Observe and confirm the warning if you want to actually delete the database.
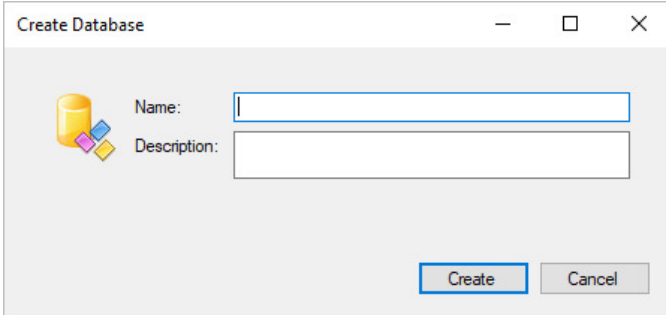
Warning information

⊘	A deleted database can't be restored. All documents that are stored in this database will also be deleted irreparably.

Create new database

You need supervisor privileges for this function.

Select the database node and select the function **Create new...** in the action panel or via the context menu.

Now you can assign a name and description for the new database (for the new archive).

Name	Name of the database that is also used in the SQL database. Enter a name with a maximum of eight characters here. The first character must be a letter. You can't use keywords that are reserved for internal purposes in the database. Once saved, the name can no longer be changed.
Description	Description or explanation of the database. This can be changed at any time.
Create in DBMS	Here you can connect with the Database Management System (DBMS) (see dialog box below) to physically create the PROXESS database in the underlying SQL database system. If the PROXESS database manager and PROXESS Administrator Console are installed on a computer, the SQL connection settings are already adopted in the dialog.
Create	**You can only create the database in the PROXESS Administrator Console after the new database was created as an SQL database.**
Cancel	This lets you exit the dialog without saving the entries.

Fig.: Connection dialog of the DBMS

Update database signature

This is an internal administrative function that becomes necessary if changes were made to the PROXESS database tables with SQL Tools due to maintenance activities (e.g., if a field was extended subsequently). This kind of intervention requires an update of the database signature for the affected documents. This is the only way to ensure that the documents can continue to be displayed for the user.

Warning information

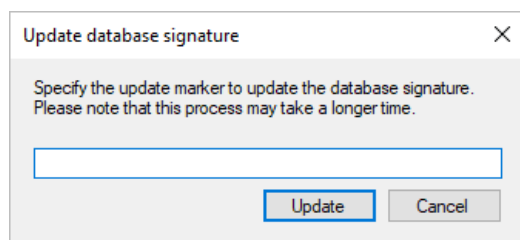|	
⛔	**Always perform these maintenance tasks in connection with your PROXESS service partner. If the work is performed incorrectly, the relevant documents will no longer be displayed in the system and database entries will be falsified.**

Step-by-step instructions:

During maintenance work, use the SQL command to mark the "Datahash" column with any arbitrary entry (e.g., Update).

Connect to the registered "PROXESS Administrator" in the PROXESS Administrator Console with supervisor privileges.

Select the appropriate database.

In the "Action" menu, choose the command **Update database signature** (alternatively through the context menu of the selected database).

The following dialog box opens:

Enter the marker entry used above (e.g., "Update").

Select the **Update** command.

_____

Also see:
Database signing
Security functions—concept and overview

Dokumentation PROXESS Admin Console

Managing database rights

In order for users to work in a sub-archive, i.e., a database, to retrieve information or add documents, they need access rights to this database. After receiving a basic access right for a database, access rights to the document types in this database are also necessary (see Managing document type rights).

Note

To manage database rights, you have to be logged in as a supervisor. As a database area administrator or (system) administrator, you will only see the databases displayed that were already unlocked for you by the supervisor. You can have all existing user and group rights displayed but can make no changes.

Mark the "Databases" branch in the console root of the PROXESS Administrator Console.
Mark the database to be managed and select the **Properties** command and **Rights** tab in the context menu ("right mouse button").

The following dialog box appears:

Fig.: Database rights for the "Personnel" database

You can see the name of the selected database in the title bar. The table lists all existing users and groups.

These two database rights are differentiated:

Access	Makes it possible to connect to a database. For successful access to archived documents, an access right to document types is also needed.
Manage	Makes it possible to grant or revoke access rights to other PROXESS users within this database. When users get the administration right to a database, they become database area administrators.

There are three statuses when assigning rights:

☑ **Check mark placed**   Right granted

☐ **Green check box**   Right not granted (= default setting). However, a user may have
(or grayed-out check box in the   corresponding rights through group membership.
classic Windows design)

☐ **Empty check box**   Right explicitly revoked (= forbid). "Forbidding" a right for an individual
                                             user overrides the right that the user would have due to group
                                             membership.

No right can be granted or revoked to the group of SUPERVISORS and the supervisors themselves. Supervisors per se have access and administration rights to all databases.

Administrators automatically get an access right to the databases that they created in the PROXESS Administrator program. This enables the administrators to perform the necessary management tasks, such as the creation of document types and fields in this database. The access right to a database alone does not enable access to the archived documents of this database. This requires additional access rights on a document type level and document level. Furthermore, administrators don't receive an administration right to the created databases, i.e., they are unable to grant user rights.

By clicking a check box, you activate the different conditions. All selected changes only go into effect with the **OK** or **Apply** command.

Also see:

Access rights—concept and overview

Database area administrator

Create database field

You can define the search and index fields for an archive using the database fields. It is strongly recommended that you define these fields in advance in an organizational meeting.

Step by step:

To create a new field, connect to the desired database and select the node Database fields under Database in the left pane.

If you haven't created any fields for a database yet, you will first see the two **PROXESS core fields Doc Des and DocsDocTypeName**. The two fields DocDes (document name) and DocsDocTypeName (document type) are always available automatically in every database. You can rename these two fields, but all other properties are fixed and can't be changed.

In the action panel on the right (alternatively via the context menu), select the command **New**.
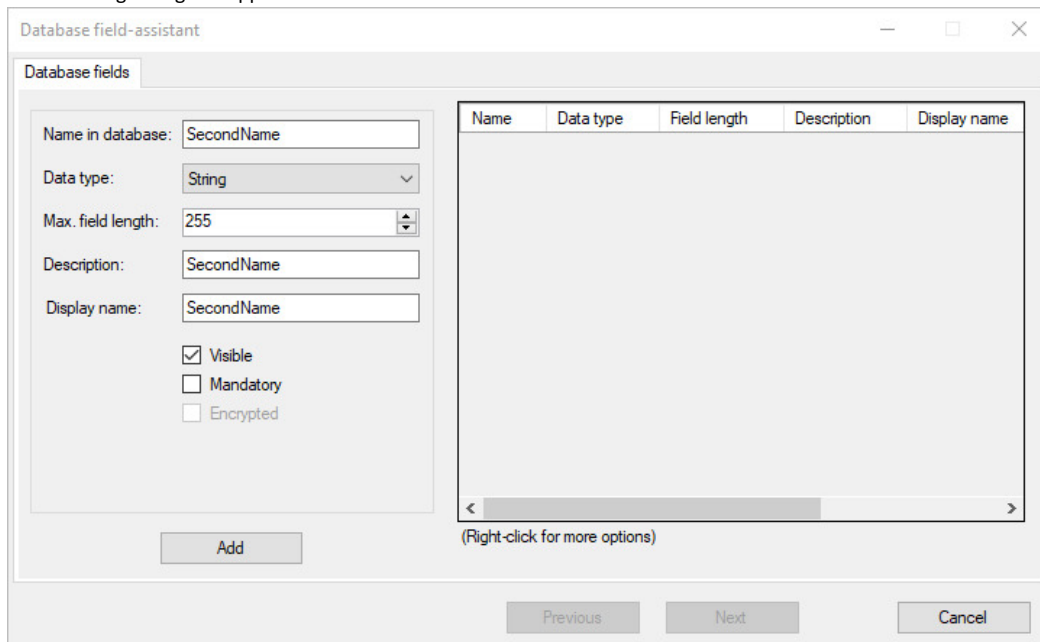
The following dialog box appears:

Fig.: Create a new database field "Last name"

Field name	Here you assign a name for the new field. This name must meet the requirements of the underlying SQL database. If you use any characters that are not allowed in the SQL database, the entry turns red and can't be saved. You can't use certain keywords that are reserved for internal database purposes, for example. You can later add a descriptive field name for the user mask.
Data type	This is where you select a data type. The selection of available data types depends on which database or interface is being used. For Microsoft SQL Server, for example, you can use the types STRING (alphanumeric characters), INTEGER (natural number), DATETIME (date and time) and DOUBLE (floating point value). **Once it has been set, the data type can no longer be changed.**
Field length	If you have selected STRING as the data type, you also specify the maximum field length. This can be between 1 and 255 characters. The user can't enter more than the number of characters defined here in this field. Like the data type, the field length can't be changed later.

Fixed length	This option can only be selected for fields of the STRING type. Here you define a fixed field length for the respective database entry. Unused characters are then filled with blanks if necessary. The fixed length allows you to slightly optimize storage space in the database. For current databases, however, this advantage is negligible, so that the manufacturer recommends not enabling this option.
Encrypted	Activate the checkbox to encrypt field contents of this properties field in the SQL database. The activation is only possible if your supervisor has previously activated this database as a high-security database in the PROXESS Administrator Console. As a member of the administrator group, you can activate the field encryption even without supervisor privileges. (See note below). Encrypted fields are marked with this symbol ⬛: **Warning information**
	⛔ Encrypted fields lead to certain restrictions: For one, only exact equivalence searches are possible (i.e., no more "% searches"), for another, the system performance can deteriorate. This depends on the amount of data to be encrypted and the hardware you use.
Create	With this you create a new field with the entered data. Once saved, these properties can no longer be changed. However, you can configure the properties that are visible for the user.

Tip

💡	In PROXESS, certain **core fields** are generated automatically and shown in the document mask. These include the user who created the document, the date of creation and the date of the last edit of the document. These fields are displayed in the PROXESS Client in the document mask in the Core fields tab. The document's archiving period is also automatically displayed there.

Also see:

PROXESS Metadata Exchange

Database field properties

Connect to the desired database. Select the Database fields node in the left pane. In the middle pane, you can see a list of the existing database fields.
Select the desired field and choose **Properties** in the action panel on the right (alternatively via the context menu).

The following dialog opens:

Fig.: Properties of the "Branch" database field

General settings	
Field name in database	The field name in the database was assigned when the field was created (see: Create database field). It can't be changed afterwards.
Validation rule	Here you can see whether a validation rule is linked to the field.
Display name	Name of the field in the search and index mask.
Field description	Additional information for the user in the status bar.
Indexed	This checkbox informs you whether a particular field is indexed in the database—to speed up the search—or not. The fields **Document title** and **Document type** are already indexed automatically. You can create an index when you configure dynamic sorting criteria. If you want to index a field for another reason, you can do this directly in the database. You can find detailed information on indexing in the documentation on your SQL database.
Visible	If this option is activated, this field is visible to the user in the default mask.
Mandatory field	Select the checkbox to define a field as mandatory. Then the users can't save their entries in the application until they have filled in the mandatory field. Mandatory fields should only be created for particularly important data, such as invoice number, which are indispensable for processing and searching for documents.
Encrypted	The activation of this option is only possible if your supervisor has previously activated this database as a high-security database. You can activate the field encryption as a member of the administrator group.

Delete database field

The organizational analysis should ensure that only the required database fields with the desired properties are created. If a field was created by mistake or has an incorrect name in the database, an incorrect data type or an incorrect length, you can also delete it again if necessary.

Step by step:

Connect to the desired database.

Select the "Database Fields" command.

Now all database fields are displayed in the middle pane.

Select the field to be deleted.

Select the command **Clear** in the context menu.

Warning information

⊖	**Since deleting the field means that any data that may already be saved will also be deleted, a security prompt appears, which you must confirm in order to actually delete.**

Create document type

PROXESS groups similar documents together in the form of document types. Some examples of this are: incoming invoice, outgoing invoice, delivery note, order confirmation, letter, contract, order, etc. A document type defines a series of properties, such as access rights, retention periods/media and the respective indexing mask. You should have analyzed the definition of your company-related document types in advance in an organizational analysis. Many document types will be derived from your company's integrated ERP and accounting systems.

Step by step

Connect to the desired database.

Select the document type node.

In the context menu (or the action panel on the right), select the command **New**.

The following dialog box appears:

Fig.: Create a new document type

Now assign a name to the document type. In an organizational analysis, you should have determined in advance which document types you create and with which properties.

Decide whether the document type should be a clipboard and whether it can be researched with a full-text search.

You can find explanations of the properties in the next chapter under: Properties of document types

Managing document type rights

Document types are the organizational backbone of a PROXESS archive database. Each archived document must be assigned to a document type. Document types are created and configured in the "PROXESS Administrator" program.

Requirements for the rights assignment:
For a user in PROXESS to see documents of a certain document type and work with them, it is necessary for this user to have an access right for this document type.

	Groups and users don't get automatic access rights to newly created document types by the system. This is why an initial assignment of rights by the supervisor is mandatory to enable users and groups to work with the document type.

To manage document type rights, mark the entry for your PROXESS system in the console root and select the action **Connect.** Log in as supervisor with smartcard and PIN.

Double-click the branch to view all databases of the connected PROXESS system.

Connect to the desired database by marking the desired database and selecting the **Connect** command in the "Actions" menu.

Tip

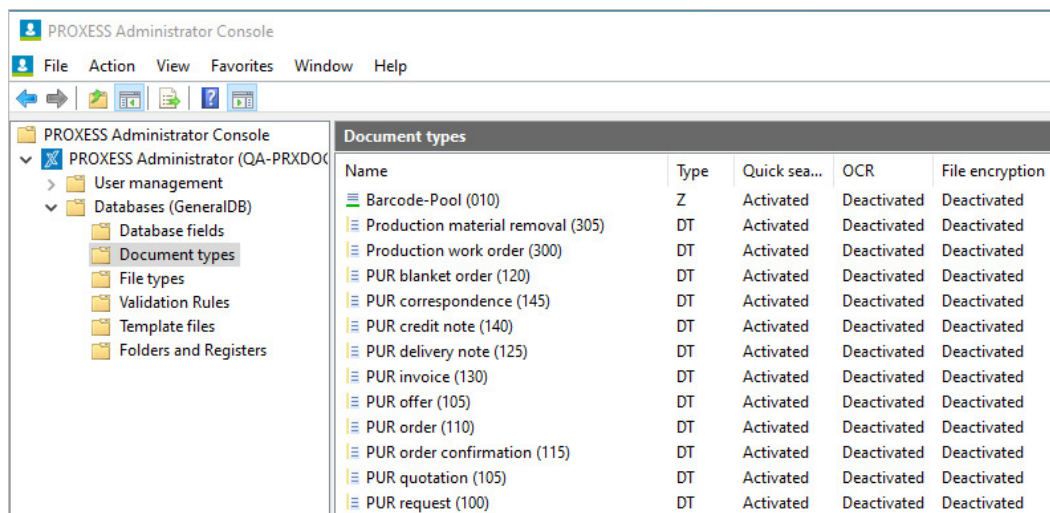|	The currently active, connected database is displayed in brackets in the left pane in the databases branch for your information.

Fig.: Connected to the "Dynamics" database

The document types and existing document type rights available in this database are "loaded" only after a database has been successfully connected and can now be managed.

–

–

First option: Grant document type rights via the document type

Dokumentation PROXESS Admin Console

Select the "Document types" node.

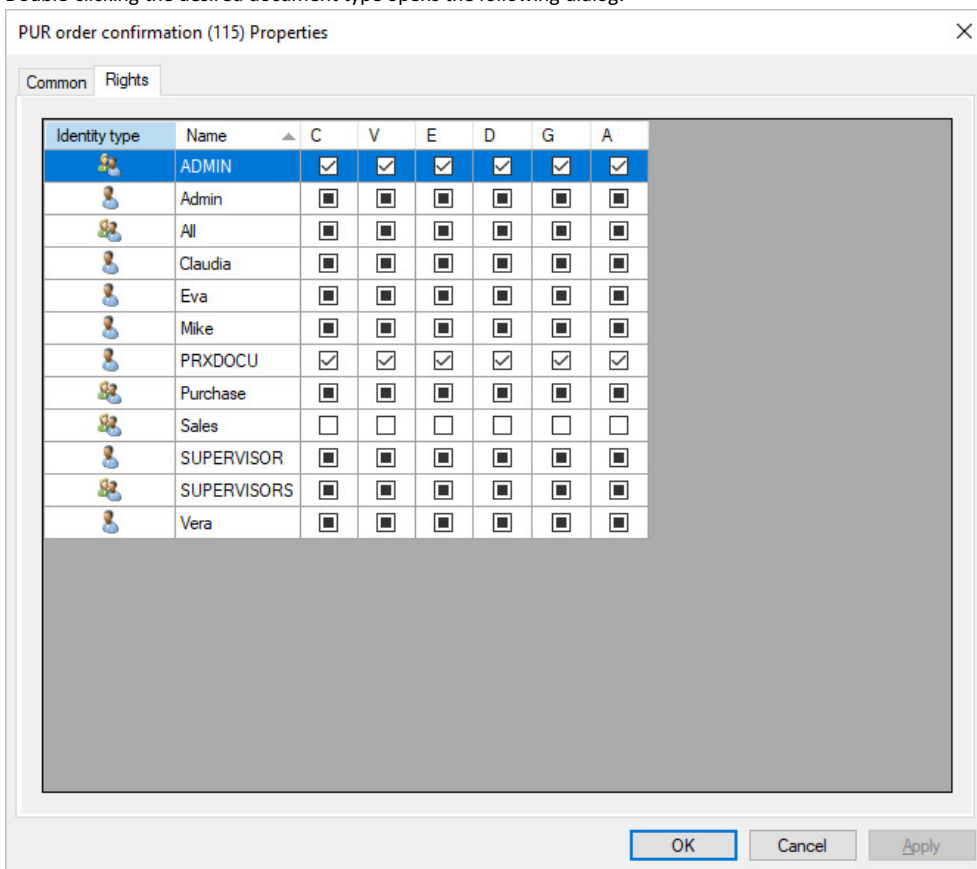Double-clicking the desired document type opens the following dialog:

Fig.: Overview of all rights for the doc type "Credit-Deb"

–

There are six different action rights on the document type level:

Create (E)	If the checkbox is activated, the user gets the right to create new documents of this type.
View (A)	If the checkbox is activated, the user/the group has the right to view documents of this type. This is the prerequisite for determining whether documents of this type can be retrieved in a search and displayed in the list of results.
Process (B)	If the checkbox is activated, users have the right to process documents of this type. They can thus change properties fields as well as all files for this document.
Delete (L)	If the checkbox is activated, the user has the right to delete documents of this type. Deletion is only a corrective measure and should not be the rule for archiving. The right to delete should therefore be used very sparingly. **Important note: PROXESS users are not able to restore deleted documents.**

Grant document rights (Z)	If the checkbox is activated, users have the right to themselves grant rights for individual documents of this type. This is advantageous for editing processes that pass through the hands of multiple users. A department manager who e.g., wants to grant a case worker insight into a confidential memo can do this without generally having to authorize this user for the document type memo. Or the other way around: If the confidential document should only be accessible to a very small group of people, the grant user can deny other people authorized for this document type access to this particular document. This means that users with this right can expand or limit the rights structure you create so that an overview of the effectively applicable rights to a document is only possible in the document window of PROXESS.
Grant document type rights (V)	If the checkbox is activated, the user is allowed to grant the action rights New, View, etc., to other users for this document type. Only supervisors and database area administrators can grant this right. This option makes sense if the company has only set up a database archive and thus can't perform a legal differentiation on the database level. This is generally the case for smaller PROXESS systems.

The action rights build on each other. You can e.g., assign only the right to view to users. If you want to assign the right to delete, this requires the right to view and must also be assigned.

Rights statuses:

☑ **Check mark placed**	Right is granted
▣ **Green check box** (or grayed-out check box in the classic Windows design)	Right not granted (= default setting). However, a user may have corresponding rights through group membership.
☐ **Empty check box**	Right explicitly revoked (= forbid). "Forbidding" a right for an individual user overrides the right that the user would have due to group membership.

Click the check box to change the respective rights status.

Second option: Change document type rights via the group/the users:

Select the "User management" node.

Mark the Groups branch. (Alternatively you can also grant the rights on a user level. In this case, mark the User branch.)
In the middle pane, select the desired group whose rights you want to manage and select the **Properties** command in the "Actions" menu. Select the **Rights** tab.
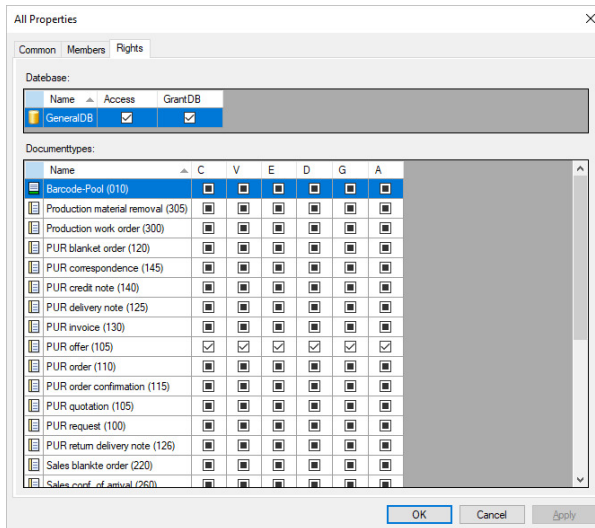
Fig.: Dialog box to manage rights for the group "Human resources" in the "Personnel" database

Now proceed as described under the "First option: Grant document type rights via the document type".

Tip

If you want to grant the same rights for multiple document types/multiple users or groups, you can simplify your work. Mark the respective document types or groups or users and select the command **Grant multiple rights** in the context menu. Grant the desired rights as usual and confirm your entries with **Apply**.
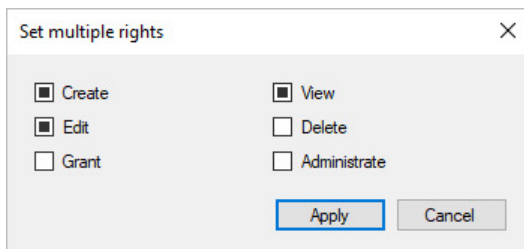

Fig.: Simultaneous processing of the rights for multiple document types/multiple users or groups

Also see:

Access rights—concept and overview

Connect database

Dokumentation PROXESS Admin Console

Properties of document types

PROXESS groups similar documents together in the form of document types. Some examples of this are: incoming invoice, outgoing invoice, delivery note, order confirmation, letter, contract, order, etc. A document type defines a series of properties, such as access rights, retention periods/media and the respective indexing mask. You should have analyzed the definition of your company-related document types in advance in an organizational analysis. Many document types will be derived from your company's integrated ERP and accounting systems.

Step by step:

Select your desired database and desired document type. Double-click to open the properties window of the document type.
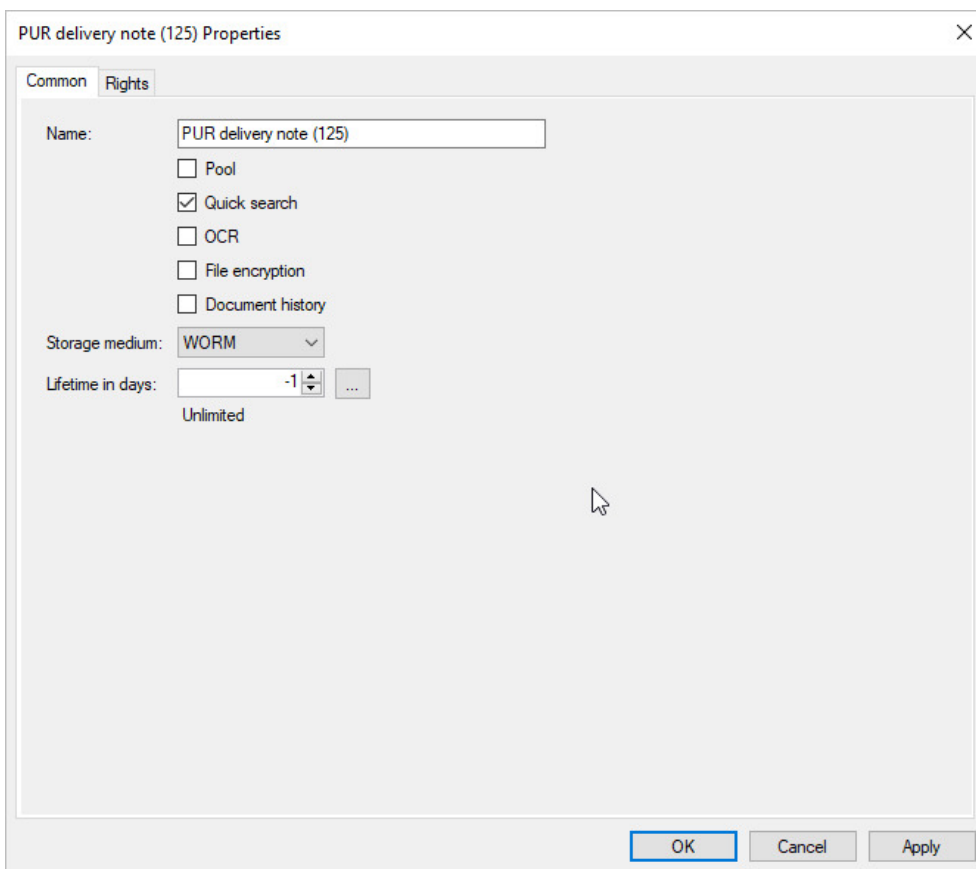

Fig.: Determine properties of a document type (here: delivery note cred.)

Name	Here you enter the name/description of the document type.

Clipboard	The document type can be created here as a clipboard. Clipboards are modifiable document types. Documents in clipboards usually require further editing and will be assigned to a final document type later. Example: An example of a clipboard is the **barcode pool** or a general scan pool. During bar code scanning with the PROXESS Scan Link, the scanned documents are first archived with the recognized bar code in the document type "barcode pool". After the final indexing, e.g., via the ERP data, they are assigned to their final document type (e.g., delivery note). **Warning information** ⊘ You create a clipboard just like a normal document type. This means that in the standard setting, all index fields are displayed in the indexing mask. If users enter information into these fields in the clipboard, this information may later be invisible when the document type is changed. **To avoid such processing errors, it is best to reduce the visible fields in clipboards to the absolute minimum. For scanned incoming e-mail, for example, the barcode number is usually sufficient.**
Full text	This activates the full text search for the document type. I.e., 1.) Index field entries are retrievable via the full-text search. 2.) File contents saved with this document type can now be activated for the full-text search. To ensure that the file contents are retrievable, each file type must additionally be activated for the full-text search.
OCR	The document type is released in PROXESS User for OCR processing. You can then process all files with this document type using the integrated text recognition function. For processing large volumes of documents, PROXESS offers interfaces to other OCR and ICR software.
File encryption	Here you can activate document types for encryption. Files that are archived with this document type are encrypted by the system. You can activate document types for file encryption only in high-security databases. Activation as a high-security database is performed in advance via the PROXESS Administrator Console with supervisor privileges. For users in the system, an encrypted document type behaves in the same way as a normal document type.
Document history	Here you can activate the document history. All of the changes to the properties fields (index fields) of a document are logged in the document history in the form of a "history file". In order to view the document history, the user must have the "Process" right for this document type. The document history supplements the "Versioning" function, where changes to the archived files are listed. If the option is activated later, all changes from the time of activation are logged. Default setting for clipboards: deactivated Default setting for document types: activated

Dokumentation PROXESS Admin Console

Storage medium	Documents can be archived on various media (e.g., hard drive, WORM, DVD). The media selection will depend not only on the available hardware, but also on the necessary archiving period for the documents. Documents with the same lifespan and storage medium will be written to a shared volume. (See the documentation on the Storage Manager Explorer on this topic.) **Tip** The default settings for storage media are linked to the document type. However, since documents sometimes consist of different files, it can be expedient to define deviation values depending on the file type. This lets you control, for example, that note files for the actual document are stored on a shorter-lived medium.
Lifespan in days	For many document types there are legal regulations as to how long these documents must be archived. There are company-specific regulations for other document types. Here you can define the lifespan and thus the archiving period of a document type. Documents with the same lifespan and storage medium will be stored together organizationally and written to a shared volume. (See the documentation on the Storage Manager Explorer on this topic.) **Incidentally, documents with expired lifespans are not deleted automatically but can be regularly queried by the administrator via the PROXESS Windows Client/Sorting Criteria and marked there for permanent deletion.**

Also see:
Managing document type rights

Dokumentation PROXESS Admin Console

Set up document type mask

A wide range of document types are archived within a database. The requirements for the indexing can be very different. Index fields such as document number and supplier address are useful for an incoming invoice, for example, whereas fields such as sender, subject and recipient are of use for an e-mail. In the document type "barcode pool", only the bar code field is usually required.

To meet these different requirements, you can define the indexing and search masks for each document type. Here the starting point is always the default mask, which you should have defined in advance as the basis (see: Set up default mask).

Tip

	Perform an organizational analysis for your company in advance and define which document types and which index fields you need for each document type. Your PROXESS project partner will assist you with this.

Step by step:

Mark the desired document type and select the **Edit field mask** function in the context menu.

The field mask editor opens:

Fig.: Field mask editor for the "e-mails" document type

All the fields in the list are initially grayed out. Grayed out fields are default fields and have default properties.

Now mark the fields that you want to convert into document type fields and select the **Document type field** button. These fields will now be displayed in black and can be edited. This means that you can change the display name, the stored validation rule and the position on the mask. You can also hide the field or define it as a mandatory field.

Now, for each field, change the properties and position on the field mask as desired.

(See the explanations in Set up default field mask on this topic)

Examples for the **e-mails** document type:

Mark "Page 1" in the list and select the command **Delete page** in the context menu. Now all fields from page 1 and page 2 will automatically be combined on one page.

Convert the barcode field into the document type field and deactivate the "Visible" function. Now the fields will no longer appear on the mask.

With the **AutoLayout** function in the context menu, you can realign the fields on the page.

Set up default mask

You can use the **Field mask editor** to determine the position and size of the index fields in the search and indexing mask for Windows users. In the first step, a default mask is defined for the entire database or the entire archive. Later, you can set up masks that deviate from this for specific document types (see: Set up document type mask).

Tip

	Before you set up the default mask, make sure that all required fields have already been created (see: Create database field).

To access the field mask editor for the default mask, mark the desired database and use the context menu to select the command **Edit field mask** (alternatively via the action panel on the right)**.**
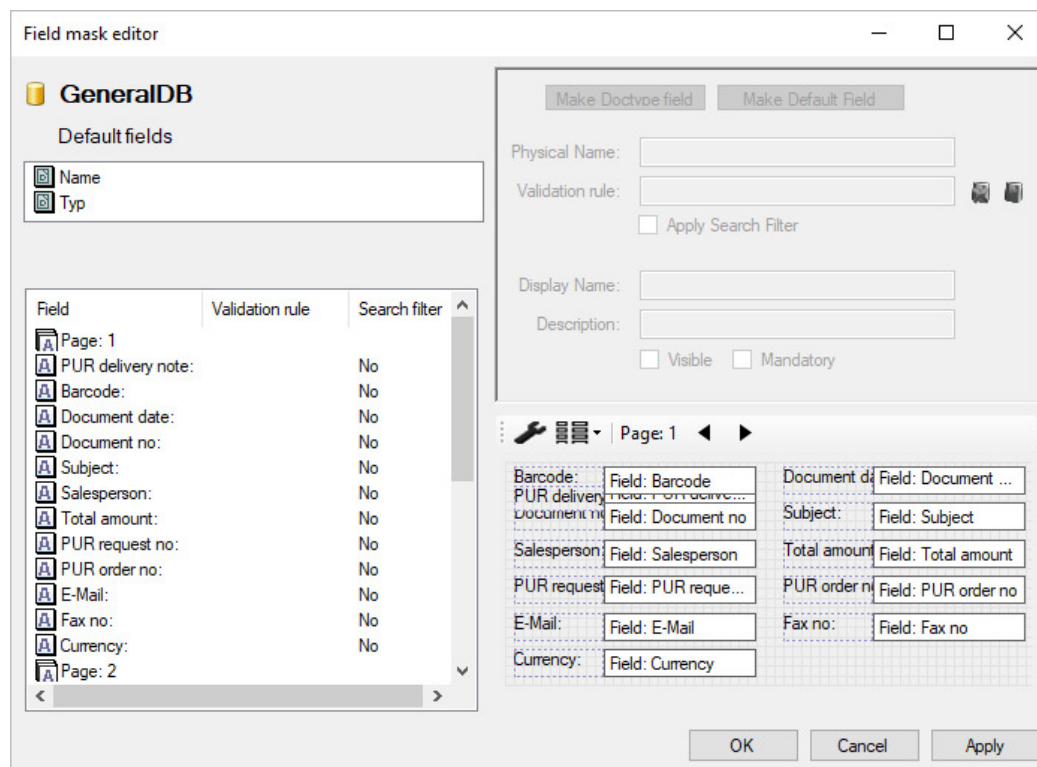
Fig.: Field mask editor for the default mask of the TestDB database

In the left pane, you can see the list of the existing fields and their allocation to the page tabs in the mask. The sequence of the fields in the list also determines their tab position for the user.

In the top right pane, you can find several field properties:

Document type field/default field	This option is deactivated for the default mask.
Name in the database	Name of the field in the underlying SQL database. This name corresponds to the field name that you assigned when you created the field and can no longer be changed later.

Validation rule	Shows the assigned validation rule for the field. Here you can assign or remove a validation rule to the field (also see: Assign validation rule to a database field)
Display name	Field name displayed in the search mask. This was assigned during the creation of the field and can be changed any time.
Description	A short description of the field displayed in the status bar in the Windows Client.
Visible	Fields can be hidden for a better overview. This makes sense, for example, if certain fields are only used for a single document type.
Mandatory	Here you can make the field a "mandatory" field for indexing.

The fields are displayed with position and size on the mask in the **bottom right pane**.

The currently marked field and its coordinates on the mask are shown **at the bottom of the dialog**.

Change the page position and tab position:
Mark the field in the list and drag and drop it to the desired area. You can mark multiple fields at once.

Set up a new page and position fields on this page
You can create a new page with the context menu in the field list. You can either drag and drop the fields onto this page or place them on the page via the context menu.

Move fields to another page
1. Mark the field and select the **Move to...** command in the context menu.
2. Mark the field in the selection list on the left and **drag and drop it within the selection list**
3. Mark the field in the selection list on the left and **drag and drop it onto the tab of the new page**

Creating a mask with the auto-layout function
All created fields are in the list on the left. On the mask, these fields are all superimposed first. You should thus use the auto-layout function for the initial template structure:
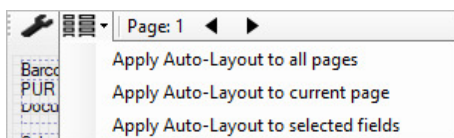
Select **Apply auto-layout to all pages**.

Now the fields are arranged expediently in succession on the mask:
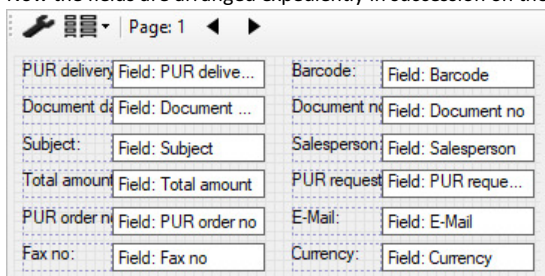
Individual pages or individual fields or groups of fields can also be positioned with the **Auto-layout** function on the

mask. This makes sense if you process existing masks at a later time. You can find the **Auto-layout** function in the context menu of the page or the fields. In the positioning, you can either let the system act completely autonomously or firmly define the number of columns and rows.   A maximum of 21 fields can be displayed on one page (three columns with seven fields each).
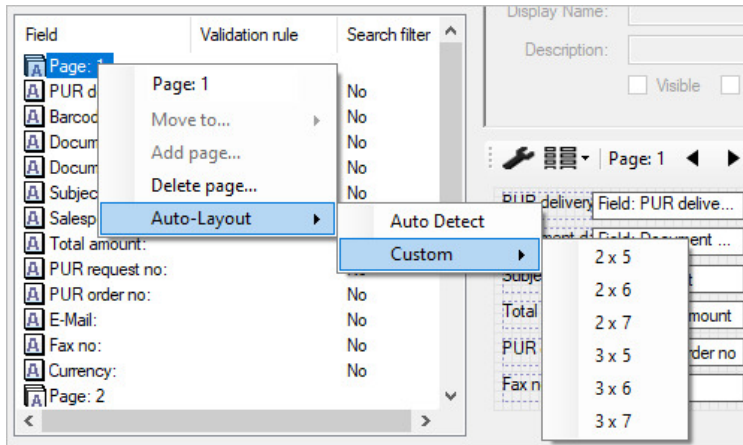

Fig.: Individually defining the auto-layout for page 1

Positioning individual/multiple fields via drag and drop:

Mark the field or the desired fields and drag and drop it to the desired position. Blue guides and a grid will help you in this process. You can change this grid in the Editor settings ✎ . The position of each field is also displayed numerically at the bottom of the screen.

Editor settings
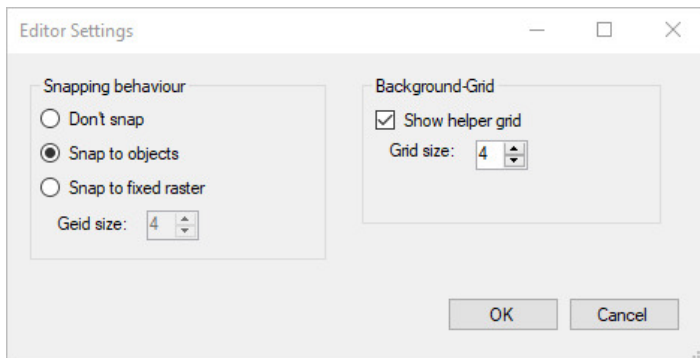
Don't snap	The position for fields and field descriptions can be selected freely without help from the grid
Snap to objects	When moving fields and labels with the mouse, the fields are automatically snapped to useful positions, which makes it possible, for example, for all fields to be placed exactly vertically below each other
Snap to fixed grid	When moving with drag and drop, the fields snap in at certain pixel intervals. Orientation to other objects on the page is disabled.
Interval	Definition of the fixed grid pattern.
Show background grid	A background grid is displayed for the setup. This will no longer appear on the search and index mask later.

Dokumentation PROXESS Admin Console

Interval	Here you can determine the size of the background grid.

Dokumentation PROXESS Admin Console

Key controls for

customizing the field mask

Using the cursor keys, it is possible to position the fields exactly on the page.

To do this, select one or more fields.

The following combinations are supported in connection with the cursor keys:

Cursor key only	The selected elements are moved in the desired direction by one size unit (approx. 1.5 pixels).
Ctrl + cursor keys	The selected elements are moved in the desired direction by two size units.
Alt + cursor keys	The selected elements are moved in the desired direction by four size units.
Shift + cursor keys	The size of the selected elements is increased or decreased by moving the right or lower edge of the elements. The size is changed by one size unit.
Shift + Ctrl + cursor keys	The size of the selected elements is changed by two size units.
Shift + Alt + cursor keys	The size of the selected elements is changed by four size units.

What are search criteria?

Search criteria provide the user with an additional search method in PROXESS. This method is prepared here. The purpose of this search method is to provide the user with something familiar, a kind of hierarchical filing structure similar to index cards.

You have two options for this:

Static search criterion
You define the desired search criterion manually and store an**SQL query**to the relational database.

Dynamic search criterion
Here you simply state the field that should be evaluated. The search branch will automatically construct itself depending on the archived documents.

The user can also apply Advanced Search to combine multiple search criteria in one query.

Examples of search criteria

Notes about the SQL condition

The SQL condition is the core of a search criterion. If the PROXESS user starts a search for sorting and search criteria, the search criteria control the database query.

The search condition is part of an SQL Where clause. This can have a maximum of 255 characters. The SQL syntax depends on which database server you are using (e.g., MSQL or Oracle). The basic form of a search condition is always:

[field name] = [value].

In the SQL condition, you can not only use the fields that you have created yourself but also the automatically created core fields Document category, Document name as well as Creation and change date, Creation author and Change author. You can find the names of these database fields in the docs table of the database.

Examples for SQL search conditions

1. Search for a specific document type

SQL search condition: DocsDocTypeName = "[Document type name]"
You can apply this condition independently of the system configuration.

2. Search for the creation date

SQL search condition: DATEPART (year, dateofcreate)
The argument that specifies the desired part is in parentheses. You can also use a link as an SQL condition.

3. Search for creation date (time period):
SQL search condition: createdate between '03.11.1997 20:00' and '03.12.1997 16:00'

4. Search for the author of a document
Determine the corresponding user ID through ISQL/w with the following query in the main PROXESS database: *select userid*10000,shortname from users*
Divide the result by 10000 (e.g., 2,000.00/10000)
Enter SQL search condition, e.g., creator = $0.0002

5. Search for double barcodes
SQL search condition: Barcode IN (SELECT barcode FROM docs GROUP BY barcode
HAVING COUNT(barcode) > 1)

6. Search for empty documents:
SQL search condition: docid not in (select docid from files)

7. Search for all cross-reference documents:
SQL search condition: docid in (select sourcedoc from seealso)

8. Search for empty documents that aren't cross-reference documents:
SQL search condition: docid not in (select docid from files) and docid not in (select sourcedoc from seealso)

9. Search for documents created in the last 30 days:
SQL search condition: datepart (dy,createdate) > (datepart(dy,getdate()) - 30)

Tip

All search criteria for a sorting criterion are connected with OR and the result with AND.

Formal: (A or B or C or ...N) and (AA or BB or CC or...NN) and ...

The system won't check whether a search condition has correct and meaningful syntax. If you aren't certain, test the search criterion in PROXESS.

Dokumentation PROXESS Admin Console

Dynamic search criterion

With a dynamic search criterion, you simply specify the field that should be evaluated. The search branch will automatically construct itself for the user depending on the existing documents in the archive.

Step by step:

Connect to the desired database and select the branch Search criteria under Database.

Select the command **New dynamic criterion** in the context menu.
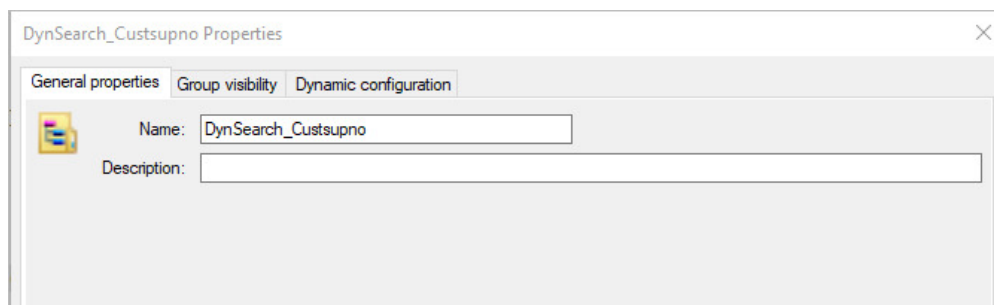
This dialog box appears:

Fig.: Creating a dynamic search criterion

Enter a name and (optionally) a description for the new search criterion.

Select whether an **index** should be placed on the field to speed up the search. If there are many records in the database with many different entries in this field, an index improves the performance. On the other hand, if there are only a few possible entries in a field, e.g., five country codes per 100,000 records, an index tends to slow down the performance. Too many indexes in a database also reduce the performance
Select the **Create** command.

Now the new dynamic search criterion appears in the list.

For the configuration and to assign rights to the search criterion, open the search criterion by double-clicking.

Group visibility

Select the **Group visibility** tab and add the user groups that should get access to the dynamic search criterion via the PROXESS Client. After creating a search and sorting criterion, this is not initially released to any user group. The assignment of rights is only possible on the level of the PROXESS user groups and not for individual users.

Dynamic configuration

In the **Dynamic configuration** tab, you have the following options for settings.

Hierarchy levels of the display	In text fields, you can decide whether the search criteria should be formed fully dynamically or whether you want to specify the classification and number of levels. If the counter for the hierarchy levels is set to 0, this means that the levels and level descriptions are derived from the actual document archive. **This is generally the most useful setting, since it results in the clearest presentation.** Sample application: For a postal code field, for example, this configuration results in a selection of search criteria from all actually existing postal codes. If you would like to divide this list into postal code groups (0s, 1s, 2s, 3s, 4s, etc.) for the sake of clarity, set the desired number of levels here (in this example 1). The system allows up to 50 levels. However, such deep nesting is rarely necessary in practical use.
Tab names	When you define the hierarchy levels, you can also determine the tab titles. You can enter the characters or character strings into the field, in succession in the desired sequence without separators. Since such tab titles are often structured the same way as in index card systems, you can use the checkboxes to fill them in quickly. Duplicate tab titles are not possible; the system checks the list and reports any multiple entries. With little effort, you can thus create a very differentiated selection of search criteria.
Digits	If you want to use digits from 0–9 as tab titles, select this check box. If there are two hierarchy levels, e.g., it becomes tab 0 with sub-tabs 00 through 09, then tab 1 with sub-tabs 10 through 19, and so on, up to tab 9 with sub-tabs 90 through 99.
All upper-case letters **All lower-case letters**	For an alphabetical tab order of the search criteria, you can differentiate between upper- and lower-case letters. However, this differentiation is only important if you are using an Oracle database. For MS SQL Server it is sufficient to select the checkbox **All upper-case letters**. Lower-case letters are automatically sorted here, if lower-case letters are available in the database.
German special characters	If an alphabetical order should contain umlauts and "ß", select this checkbox. In combination with upper-case letters, upper-case special characters are sorted, in combination with lower-case letters, lower-case special characters are sorted.
Other special characters	A selection of additional special characters is stored, e.g., paragraph marks. You can add further special characters, e.g., Danish letters, with the ASCII code. You can find the ASCII code in the Windows table of symbols.

Static sorting and search criterion

With a static search criterion, users define the desired search criterion manually and store an **SQL query** to the relational database.

Step by step:

Connect to the desired database and select the branch Search criteria under Database.

Select the command **New static criterion** in the context menu.
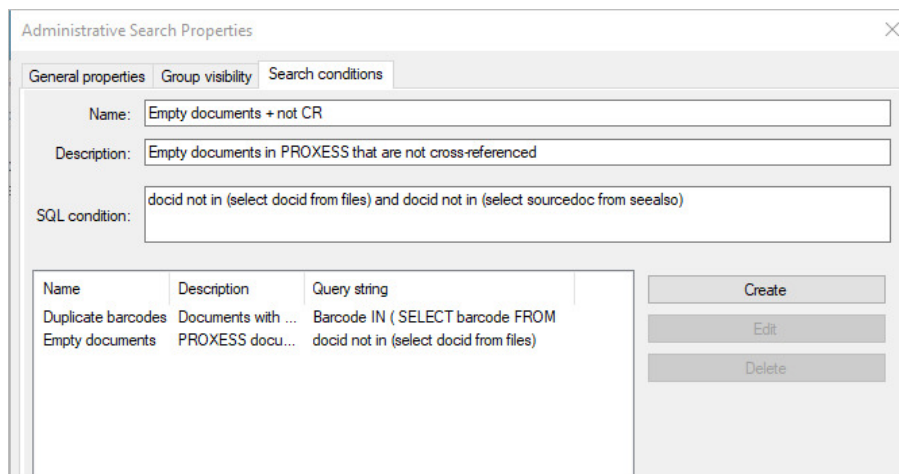
This dialog box appears:

Fig.: Creating a new static search criterion

Enter a name and (optionally) a description for the new search criterion.

Select the **Create** command.

The new static sorting criterion now appears in the list.

To define different static search criteria with an SQL search condition, open the sorting criterion now by double-clicking it.

Fig.: Defining static search criteria with an SQL query

In the above dialog, you can already see some examples of SQL search conditions. You can find more examples in the topic Examples of search criteria.

Notes about the SQL condition

Dokumentation PROXESS Admin Console

The SQL condition is the core of a search criterion. If the PROXESS user starts a search for sorting and search criteria, the search criteria control the database query.

The search condition is part of an SQL Where clause. This can have a maximum of 255 characters. The SQL syntax depends on which database server you are using (e.g., MSQL or Oracle). The basic form of a search condition is always:

[field name] = [value].

In the SQL condition, you can not only use the fields that you have created yourself but also the automatically created core fields Document category, Document name as well as Creation and change date, Creation author and Change author. You can find the names of these database fields in the docs table of the database.

Group visibility

Select the Group visibility tab and add the user groups that should get access the sorting criterion via the PROXESS Client. After creating a search and sorting criterion, this is not initially released to any user group.   The assignment of rights is only possible on the level of the PROXESS user groups and not for individual users.
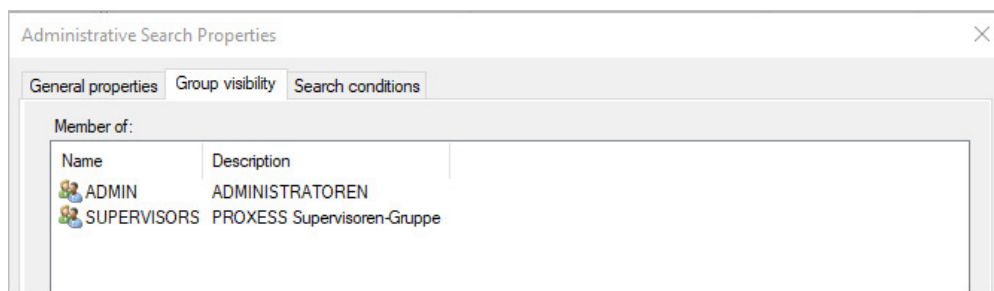

Fig.: Group visibility of the sorting criterion "Administrative search"

External thesaurus

Depending on the user currently logged in, external thesauruses make it possible to display individual selection lists in a field for the creation of documents and to retrieve documents.

Using freely definable SQL queries, the value lists are determined online from external systems such as an external SQL database. This makes it possible, for example, to use user and rights information online from the leading ERP system and thus avoid double data maintenance.

Example:
Administrator A is responsible for order processing in the "North" region. The assignment of employees to a region is found in an external SQL data source of the ERP system. You can now create and configure an external thesaurus so that administrator A, due to his PROXESS user properties, can only call up documents from the "North" region. Other selection options in the "Region" field are not displayed to the user.

Step by step:
In the "Database" node, select the entry "**Validation rules**". In the action panel on the right (alternatively via the context menu), select the command **New**.
Select the **External thesaurus** entry.

The following dialog appears:

Description	Unique name for the external thesaurus rule
Provider	Name of the validation provider (here: SQL provider as interface to the SQL database)

Dokumentation PROXESS Admin Console

Data source	The dialog to specify the connection parameters to the external data source opens. (E.g., to the ODBC source) Enter the login information for a database user here. The DB user entered here must be at least a DB owner or have the rights of a DB owner. The respective connection string is created automatically when the **OK** button is clicked. (See below)
Behavior	Specifies the behavior of the PROXESS client if the value list for the current user determined by the SQL query is blank (either the person isn't entered as a user in the external database or no value is assigned to the user) Example above: The logged-in user doesn't exist in the external database or no region is assigned to the logged-in PROXESS user. There are two options for such cases: a) No search is performed, i.e., no documents are shown in the hitlist. b) All hits are shown (example: documents from all regions are displayed)
sql	By clicking the text, you can enter a freely definable SQL query with replacement variables (see below)
sqldef	By clicking the text, you can enter a default SQL query that is performed when the result of the actual SQL query is blank.
sep	Here you enter the used separator between the entries in the values list.

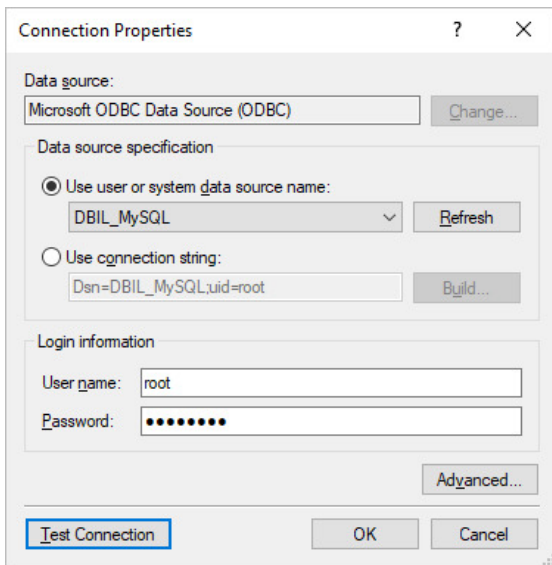## Definition of an ODBC data source

*Fig.: Defining an ODBC data source for an external thesaurus*

Step by step:

1. Select the name of the data source.
2. Enter the login information for the data source.
3. After clicking the **Build** button, the dialog "SQL server login" appears

Dokumentation PROXESS Admin Console

4. Here you select the database server name and, with the **Options** button, select the database to be used as the external source.

5. Accept the remaining values from the default setting and confirm the entries with **OK**.

6. The **Test connection** command enables you to check the connection data.

Defining the SQL query

By clicking the text "Enter SQL query here", you open the dialog box:
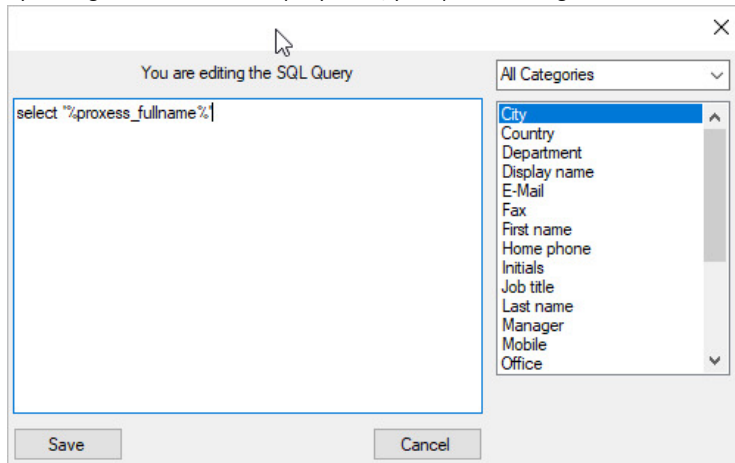
Now enter the desired SQL query. By double-clicking a value in the selection list on the right, the associated replacement variable is entered into the SQL statement at the cursor position.

Example above:
SQL statement: select REGION from ST_Region where '%proxess_name% = '%sn%'

An SQL table is accessed with an assignment of the respective logged-in PROXESS user to certain regions (North, South, East, West).

Testing an external thesaurus

In the "Databases/thesauruses" node, mark the desired external thesaurus and select the **Test** command in the context menu.

The test dialog opens:
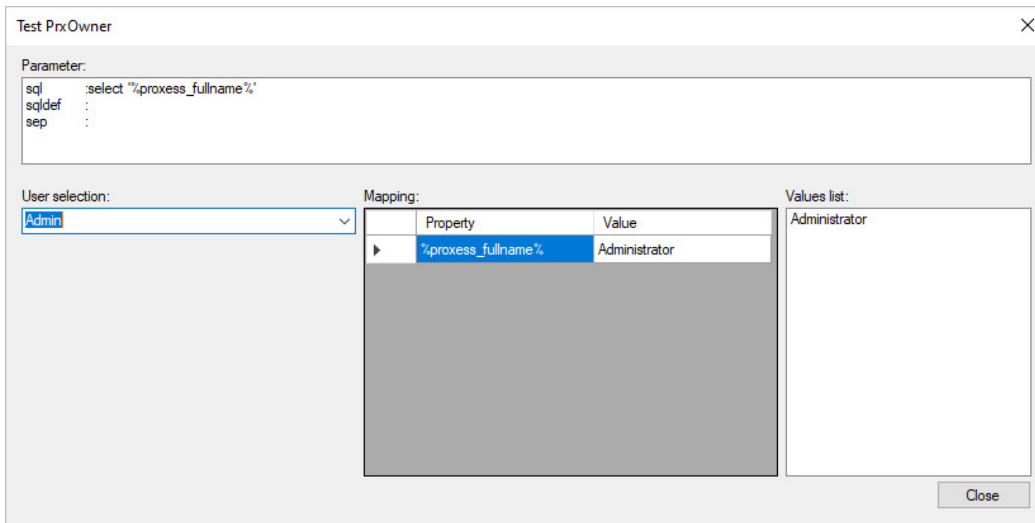
Dokumentation PROXESS Admin Console

Fig.: Test dialog for external thesauruses

In the example above, the user "krocker@letsbefast.de" is assigned the regional entries "East" and "West". I.e., he only sees the documents in which the "Region" field is filled with one of the two values.

Parameters	Line-by-line display of the configured parameters for the query.
User selection	Here you can select the user for whom the value list resulting from the SQL query should be displayed. If a default parameter (sqldef) is defined, its query result is displayed if the result is blank for the user.
Property values	Display of all replacement variables used in the parameters and their values for the selected user
Values list	The values list determined by the SQL query for the selected user. This list is displayed to the user.

Important security information for high-security databases:

Authorizations in secured databases may only be administered by the PROXESS supervisor or a database manager authorized by him or her. This is ensured by the system in the area of database and document type rights. **If external thesauruses are used as an implementation of content-based access rights, however, protection against manipulation of the external data source cannot be guaranteed by the system.** This relates precisely to the principle of being able to use authorization information from third-party systems that are not under the control of PROXESS. **For that reason, the system operator is responsible for securing this information.**

Create validation rule

Validation rules are input help for fields. In PROXESS there are:

- Thesauruses for text fields
- Periods for date fields
- Maximum and minimum values for decimal and integer fields
- External thesauruses

Validation rules, such as a pull-down list with a selection of possible entries for a field, make it possible to exclude typos or implausible entries as far as possible.

First, a validation rule is created. In a second step, the rule is linked with one or more database fields (see: Database field properties).

Step by step:

In the Database node, select the entry "**Validation rules**". In the action panel on the right (alternatively via the context menu), select the command **New**.
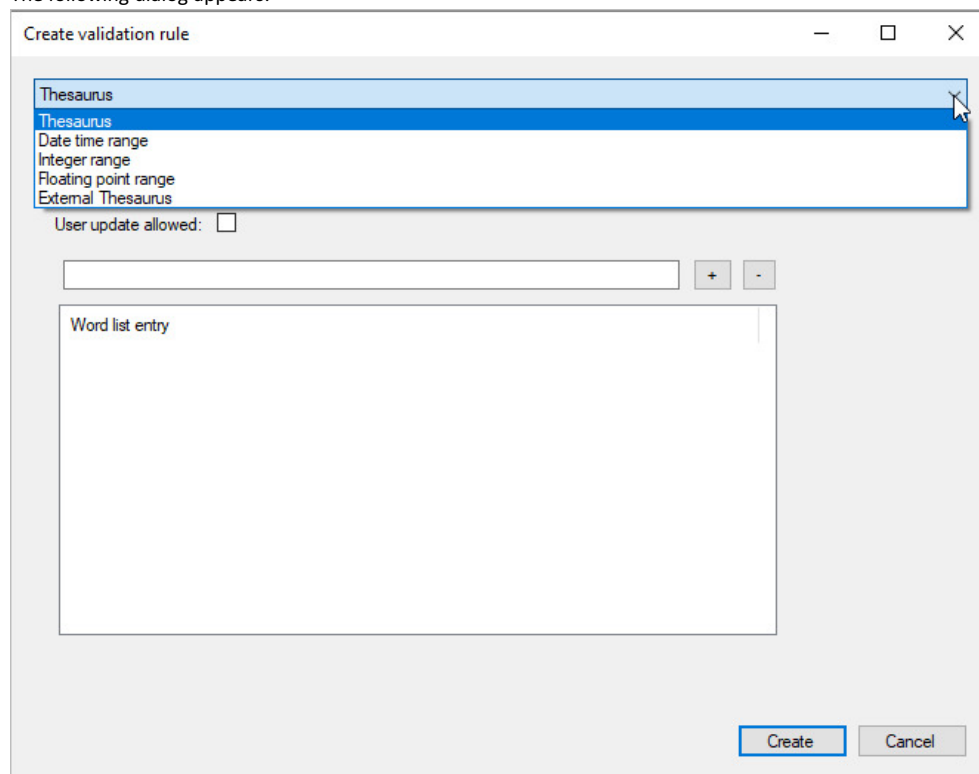
The following dialog appears:

Fig.: Selection of a new validation rule

The following settings are possible:

Dokumentation PROXESS Admin Console

Thesaurus (for text fields)	Here you can assign a **name to the thesaurus**. You can also specify fixed field entries, which you can see in the form of a selection list, via the **Word list**. In the **Maximum word length** field, you can specify the maximum characters for an entry. The option "**User input permitted**" can be used to specify whether users can fill the list or expand it with new entries themselves, or if they are restricted to the predefined entries.
Date range, integer range, floating point number range	In addition to the name of the thesaurus, you can define upper and lower limits for user input.
External thesaurus	Value lists from external systems, such as from a PROXESS-external SQL database, can be defined using external thesauruses. This access to external databases makes it possible, for example, to use user and rights information online from the leading ERP system and thus avoid double data maintenance.

You can link the created validation rule with a database field here:

Assigning a validation rule to a database field

Validation rules are input help for various data types:

- Thesauruses for text fields
- Periods for date fields
- Maximum and minimum values for decimal and integer fields

Validation rules, such as a pull-down list with a selection of possible entries for a field, make it possible to exclude typos or implausible entries as far as possible.

First validation rules are created (see: Create validation rule) and linked to fields in a second step. Compliance with the linked rule is then already checked during the user entry.

Warning information

> **If you link fields with a validation rule after documents have been created, you ensure that the rule takes all of the already existing field entries into account. Otherwise there will be error messages while processing these documents.**

Assigning a validation rule to a default database field

In the Database node, select the entry Fields. Mark the field to be linked. Now select the command **Properties** in the action panel on the right (alternatively via the context menu).
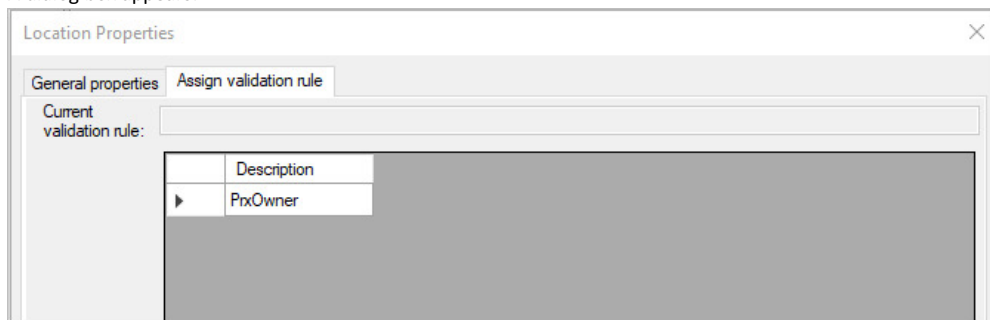
A dialog box appears:

Fig.: Assigning the validation rule "Subsidiary" to the "Branch" field

You can find a general overview in the "General settings" tab. Here you can already see whether a validation rule has been linked to the field.

Is the rule visible or not?
Often the upper and lower limits are specified as validation rules to avoid typos in the entries. However, even if you don't want to bother the user by specifying entry limits, you don't have to omit the validation rules. In this case, just select the option "Rule not visible".

In the "Assign validation rule" tab, you can use the command **Set from selection** to assign the currently marked entry in the list of the existing validation rules. You can also cancel the assignment with the **Unset** command. Save your entries.

Assigning a validation rule to a document type field

Dokumentation PROXESS Admin Console

Select your desired database and mark the desired document type.

Now select the field mask editor with the command **Edit field mask** in the context menu.

Once you have converted a default field into a document type field here, you can assign a validation rule to the field. However, in that case this assignment only applies to the selected document type.
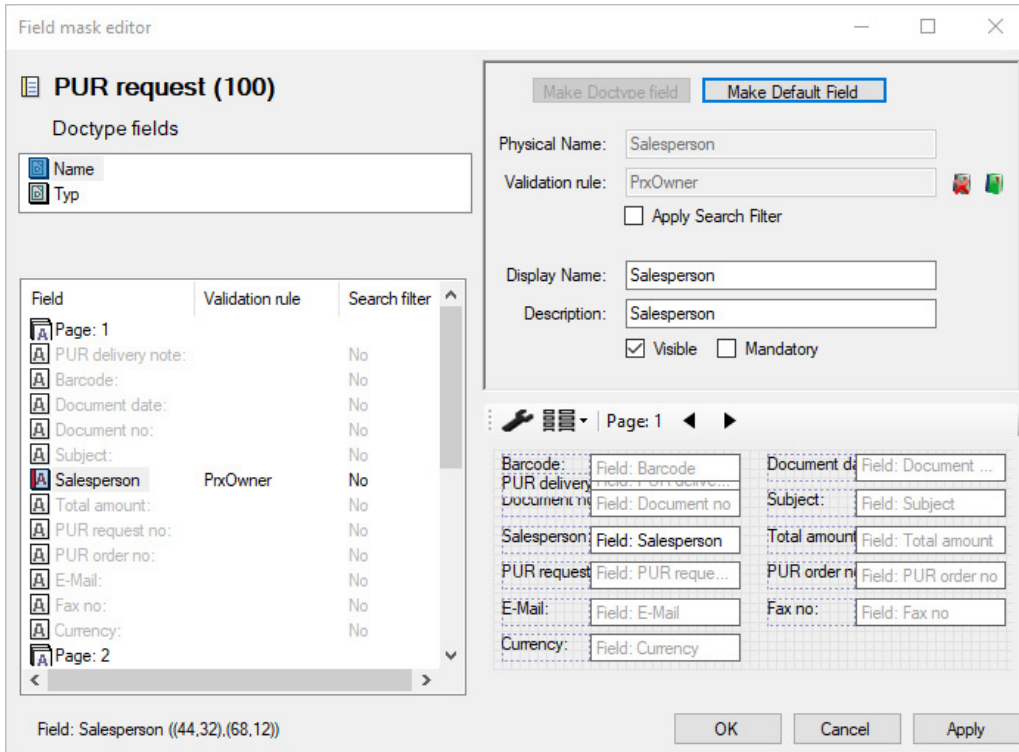

Fig.: Assigning a validation rule "Department" to the "Department" document type field

Dokumentation PROXESS Admin Console

Parameters for Diaclip files

The "Diaclip" option in the File type applications makes it possible to represent COLD files with a background image (e.g., the company letterhead).

You can use various parameters to determine and adjust the background image.

First, state which TIF file should be set as the background. PROXESS already provides white background TIF files in DIN A3 and A4. If you want to use a company form, scan it and copy the TIF file, preferably into the system directory.
In the Program call field, enter one or more parameters and assign a value to them.
Syntax: [Parameter] = [Value]
Enter a blank space as a separator between the equality conditions. It doesn't matter whether there are blank spaces within an expression, nor does the letter case matter.
The parameters can have any arbitrary sequence. If a parameter occurs more than once in the line, only the one furthest to the right is considered.

Overview of parameters and values:

Parameter	Explanation	Value
App	You only need this parameter in the **New** tab. It indicates which application is used to create the DClip file. The user only applies this option in PROXESS if DClip files are created manually. But this usually happens automatically with COLD files. You can enter e.g., Notepad.	[Program name].EXE%1 %1 is used to indicate the path and is understood on all platforms.
TIFF	Defines the background TIFF and is absolutely necessary.	[Path name]\[file name].TIF If the front end is in the same directory, the file name suffices.
XOFFSET YOFFSET	Specifies the page dimensions. X and Y are interpreted according to the German standard.	Page dimension in TWIPS
FontWidth	Regulates the spacing between the letters.	Width in TWIPS
FontHeight	Specifies the font size	Height in TWIPS
LineHeight	Specifies the line spacing	Spacing in TWIPS
CountLines	Specifies when a page break should be inserted	Value 0 = the page break is created by a form feed Value 1 = the page break is inserted after a maximum number of lines
MaxLines	Specifies the maximum number of lines on a page. This is only used if CountLines has the value 1.	Whole number e.g., 72 for DIN A4 page

The table shows the conversion factors for common units of measurement in Windows:

Unit of measurement	Twips	pt	inch	cm
1 Twip =	1	1/20	1/1,440	1/567
1 pt =	20	1	1/72	0.35
1 inch =	1,440	72	1	2.54
1 cm	567	28.35	0.39	1

The Cold files for Diaclip generally don't include formatting information. Then the values defined here are used for page margins and font sizes. If a file includes formatting instructions, they are applied.

Tip

Dokumentation PROXESS Admin Console

	To set up forms, you must know the font size that is usually applied for printing. Then set the font height and width accordingly.

Dokumentation PROXESS Admin Console

Create template file

You can use Windows files to create templates, such as forms or letterheads. These template files are then available for data type management. Working with template files is a convenience feature; it is not required by the system.

Example:

If the same kinds of documents, such as company letters, are repeatedly created at your company, you can use a template file to create a file type that will call up your text processing specifications together with the letterhead.

Step by step:

Create the required template files with the desired application (e.g., WinWord). Only now can you integrate the template file in PROXESS:

Connect to the desired database.

In the Template file branch, select the **New** command via the context menu or action panel.
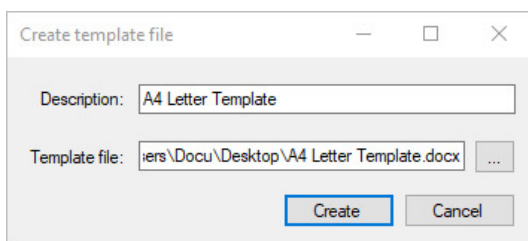

Fig.: Creating a new template file

Assign an identifier for the template file in PROXESS.

Use Explorer to select the prepared template file.

You can save your specifications with the **New** command.

Link template file with file type

Created <u>template files</u> can be linked with an existing <u>file type</u>. This means that when a new file is created, for example, the stored template file is opened.

A classic example of a template file is a Word template for a company letter.

Step by step:

Connect to the desired database and select the desired file type in the branch **Databases/file types**.

Now select the **Properties** command via the context menu or the action panel on the right.
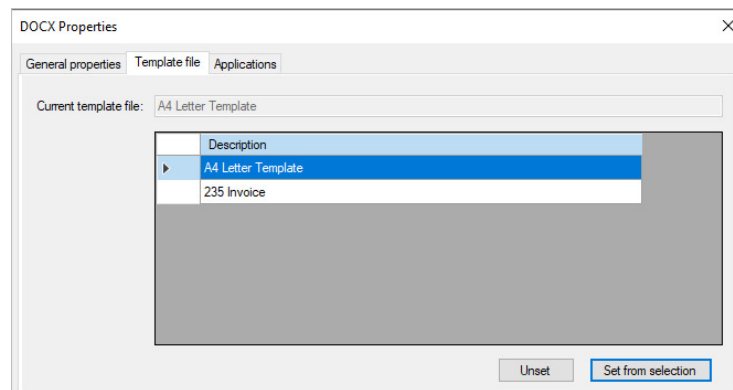
Select the "Template file" tab:

Fig.: Link template file to application

Under **Current template file**, you can see whether a link was already established.

Select the desired template from the list.

Use the **Create** command to establish the link from the template file to the file type.

You can cancel the link at any time with the **Delete** command. This has no retroactive effect on already archived files.

Dokumentation PROXESS Admin Console

Access rights—concept and overview

Why are there rights?
In an electronic archive, documents are more easily and quickly accessible to users company-wide than in a paper archive. It is all the more important to determine who should have access to which documents. In PROXESS, this is done through user rights to databases, document types and individual documents. Rights can be assigned not just to individual users but also to groups. This saves valuable working hours in systems with several hundred users.

Must and can
You must assign rights in each case, since the system won't grant any rights to new users and groups by default. The system offers numerous differentiation options to assign rights. Whether and to what extent you use these depends on the number of PROXESS users and on your company's document and task structure.

Rights management levels

Level 1: Database rights
PROXESS supports setting up and managing various archive databases. This makes it possible for you to keep large sectors like Procurement or Payroll entirely separate. Users and groups first need the relevant database access rights before they can work with these archive databases.

Level 2: Document type rights
You can control the access options available to users within an archive database via document type rights. These cover the following distinct action rights: View, New, Edit and Clear, as well as "Grant document rights" and Grant document type rights. Generally speaking, you can choose any combination of these actions, whereby View is obviously the necessary foundation for the other action rights.

Level 3: Individual document rights
Rights to individual documents can also be granted in the four categories "View", "New", "Edit" and "Clear". The purpose of this is to give users the option to decide for themselves in individual cases whether other users should receive access to a specific document. This respects the decision-making competence of the company employees and thus enables more efficient workflows without the need for intervention by the supervisor or area administrator. It is only valid for individual documents, so it does not replace the rights hierarchy set by the supervisor, rather simply expands it. Users grant rights to individual documents themselves in the PROXESS Standard Client.

Example
You grant user A the access right to the "Job" database. In this database, you give him the right to access the document types Offer, Job, Purchase agreement, Customer invoice and Complaint.
The user may not only view the offers but also create, edit and delete them.
The user may view, create and edit orders but not delete them.
The user may only view and create purchase agreements.
The user may only view customer invoices and complaints.
For customer invoices, user B gets the right to assign rights. To enable user A to edit invoice 4711 for a particular process, user B gives user A the "processing right" for this invoice.
This way user A can see all customer invoices but only process invoice 4711.

Rights statuses and prioritization of rights

Normally, "Right granted" and "Right not granted" are all that are needed to work with rights management. However, overlaps and contradictions may arise when a user is a member of multiple groups. For this reason, you can also work with the right "Forbid" in rights management, in order to quickly and safely withdraw a right that a user possesses through group membership.

Dokumentation PROXESS Admin Console

This is why the system differentiates between three basic rights statuses and represents them as follows:
There are three statuses when assigning rights:

Check mark placed	Right is granted
Green check box (or grayed-out check box in the classic Windows design)	Right is not granted (= default setting). However, a user may have corresponding rights through group membership.
Empty check box	Right is explicitly revoked (= forbid). "Forbidding" a right for an individual user overrides the right that the user would have due to group membership.

Example:
You want to revoke access to the "Wages" database for user X. This user is a member of 10 different groups.

If you only had to make do with the two rights statuses "Authorization" and "No authorization", the following would need to be done:
Control the rights for each of these 10 groups. Three groups have the right to the wage database. Remove user X from the three authorized groups.

The additional right status "Forbid" reduces this process to one work step:
You just revoke access to the "Wages" database for user X explicitly. This means that all the rights that the user has from the group membership are automatically canceled.

Prioritization of rights
There are a few simple rules that prioritize rights. These rules are graded by strength; i.e., the first is stronger than the second, and the second stronger than the third:

User rights take precedence over group rights
Forbidding takes precedence over "authorization"
"Authorization" takes precedence over "No authorization"

Possible constellations of rights can be represented by a combination table. If you aren't entirely sure of the effects of your specifications, it can help to create an overview first before you assign rights in the PROXESS Administrator.
The following table shows the combination options for a user X who is a member in two groups. Depending on how many user groups there are, of course the options increase. The right column shows the respective result for user X resulting from the prioritization of rights.

Case	User X	Group 1	Group 2	Can user X see object Y?
1	Not authorized	Not authorized	Not authorized	No
2	Not authorized	Not authorized	Authorized	Yes
3	Not authorized	Authorized	Authorized	Yes

4	Not authorized	Authorized	Forbidden	No
5	Authorized	Authorized	Authorized	Yes
6	Authorized	Authorized	Forbidden	Yes
7	Authorized	Forbidden	Forbidden	Yes
8	Forbidden	Forbidden	Forbidden	No
9	Forbidden	Forbidden	Not authorized	No
10	Forbidden	Not authorized	Not authorized	No

Fig.: Combination table to clarify possible constellations of rights

You aren't able to derive the different action rights (View, Edit, Clear, Assign right) from this table. In case 4, for example, the user's rights might include all four actions, but the right of group 1 is only for viewing and the right of group 2 is for viewing, creating and editing. Here the prioritization of rights again decides which actions the user may perform.

Action rights

Action rights state what a user may do with documents. On the document type level, six action rights are distinguished and five action rights for individual documents. The assignment of rights on the document type level is performed via the PROXESS Administrator Console. The assignment of rights on the individual document level is performed via the PROXESS Standard Client.

New	If the checkbox is activated, the user gets the right to create new documents of this type/new files within a document.
View	If the checkbox is activated, the user has the right to view documents of this type/the relevant document. This is the prerequisite for determining whether documents of this type can be retrieved in a search and displayed in the list of results.
Edit	If the checkbox is activated, users have the right to edit documents of this type/the relevant document. They can thus change properties fields as well as all files for this document.
Clear	If the checkbox is activated, the user has the right to delete documents of this type/the relevant document. Clear is only a corrective measure and should not be the rule for archiving. The right to delete should therefore be used very sparingly. **Important note: PROXESS users are not able to restore deleted documents. They will need the help of a PROXESS administrator for this.**

Dokumentation PROXESS Admin Console

Grant document rights	If the checkbox is activated, the user has the right to grant action rights for individual documents of this type/the respective document. This is advantageous for editing processes that pass through the hands of multiple users. A department manager who e.g., wants to grant a case worker insight into a confidential memo can do this without generally having to authorize this user for the document type memo. Or the other way around: If the confidential document should only be accessible to a very small group of people, the grant user can deny other people authorized for this document type access to this particular document. This means that users with this right can expand or limit the rights structure you create so that an overview of the effectively applicable rights to a document is only possible in the document window of PROXESS.
Grant document type rights	If the checkbox is activated, the user is allowed to grant the action rights New, View, etc., to other users for this document type. Only supervisors and database area administrators can grant this right. This option makes sense if the company has only set up a database archive and thus can't perform a legal differentiation on the database level. This is generally the case for smaller PROXESS systems. Of course this action right is only accessible on the document level.

Also see:

Managing database rights

Managing document type rights

Index