

Parks > Authorization Manager



# **Parks Authorization Manager (PAM)**

## Demo Manual

PAM-10-001 - 20/02/2019



## Contents

<b>1 Introduction</b>	<b>6</b>
1.1 Notation information	6
1.2 Security information	6
1.3 Additional information	7
1.3.1 Help	7
1.3.2 Internet information	7
1.3.3 How to obtain programme licences	7
1.3.4 Customer support	7
1.4 The user interface	8
1.5 General operation	11
<b>2 Using the application</b>	<b>12</b>
2.1 Databases	12
2.2 Features for checks and analysis	12
2.2.1 Scan folder permissions	12
2.2.2 Searching account permissions	19
2.2.3 Show effective user groups	23
2.2.4 Verify user access to a folder	24
2.2.5 Search users and groups in Active Directory	26
2.2.6 View active permission groups	28
2.3 Planning new file system structures	28
2.3.1 Working with companies	31
2.3.2 Working with base folders	36
2.3.3 Working with folder templates	39
2.3.4 Working with organization folders	45
2.3.5 Migrating files and folders	59
2.4 Application settings	65
2.5 Additional functions	69
2.5.1 Selecting objects in Active Directory	69
2.5.2 Showing the network environment	70
2.5.3 Showing group members	70
2.5.4 Working with the clipboard	71
2.6 Conclusion	72
<b>3 Appendix</b>	<b>73</b>

3.1 Frequently asked questions .....	73
3.1.1 No connection drives in file dialogues .....	73
3.2 Uninstalling Parks Authorization Manager .....	73

## List of Figures

Figure 1: Main programme window .....	9
Figure 2: Configure permission scan .....	13
Figure 3: Scan folder permissions .....	14
Figure 4: Memory exception .....	16
Figure 5: Export scan result .....	17
Figure 6: PDF export .....	19
Figure 7: Search effective user permissions .....	20
Figure 8: Search objects .....	22
Figure 9: Show effective user groups .....	24
Figure 10: Check user access to a folder .....	25
Figure 11: Active directory search .....	27
Figure 12: View active permission groups .....	28
Figure 13: Folder types and example structure .....	29
Figure 14: Company properties .....	32
Figure 15: Organization units in a company .....	33
Figure 16: Importing organization units .....	35
Figure 17: Creating a base folder .....	38
Figure 18: Creating a folder template .....	41
Figure 19: Folder permissions .....	43
Figure 20: Creating a new permission group .....	44
Figure 21: Creating an organization folder (organization data) .....	46
Figure 22: Creating an organization folder (folder settings) .....	47
Figure 23: Creating an organization folder (preview) .....	48
Figure 24: Organization folder permissions .....	49
Figure 25: Organization folder .....	50
Figure 26: Permissions of an organization folder .....	51
Figure 27: Folder structure of an organization folder .....	52
Figure 28: Create protected folder .....	53
Figure 29: Analysing the permissions of an organization folder .....	55
Figure 30: Importing organization folders .....	57
Figure 31: Update organization folders .....	58

Figure 32: Copy files and folders .....	60
Figure 33: Current copy operation .....	62
Figure 34: Copy preview .....	64
Figure 35: Copy history .....	65
Figure 36: Application settings: tab "General" .....	66
Figure 37: Application settings: tab "Settings" .....	67
Figure 38: Application settings: tab "Network" .....	68
Figure 39: Selecting objects in Active Directory .....	69
Figure 40: Group membership .....	71

# 1 Introduction

PAM for Windows enables you to maintain, analyse and document your NTFS file system permissions and Active Directory groups.

Permissions in the NTFS file system and Active Directory groups can be administered, analysed and documented with the programme. Helpful tests and analysis – e.g. folder permission scan, determination of effective permissions for a user, the checking of access permission of a user to a particular folder – give you a quick overview of your existing folder structures and permissions.

To ease administrative work the folder templates can be defined for departments or projects. PAM will then automatically generate the required folder structure, prepare permission groups in Active Directory and enter these groups in the folder access control lists. If required, the programme will prepare secured network shares, via which the staff member can access the folders. Furthermore, it is possible to set up an Access Based Enumeration so that users can only see the files for which they have access rights.

This manual contains a description of all programme functions as well as information about configuration.

 Note on the demo version: The demo version is available to you for 30 days after the first start of the program for test purposes. Some features are limited in the demo version, some features are only available in the licensed version. The restrictions are indicated in the appropriate places in this manual.

## 1.1 Notation information

The following symbols are used in the manual:

-  Gives valuable practical tips
-  Gives additional information
-  Should be particularly noted
-  Gives information about required administrative permissions

## 1.2 Security information

The programme works with information from the Active Directory of your Windows Domain – e.g. to get information about permission groups – and it can read and change file and folder permissions.



Administrative rights for your Windows Domain are necessary in order to test certain programme functions. Please make sure you have such rights.

After starting the application your permission groups can be seen via the menu **Actions | Show active permission groups....**

### 1.3 Additional information

Various sources of information are available should you have any questions about the application.

#### 1.3.1 Help

An online help application can be started via the menu **Help | Overview....** In addition, a context-based help can be obtained by pressing the **F1** button in each window.

#### 1.3.2 Internet information

Current product information can be found on our Internet homepage under <http://www.parks-informatik.de/pam>.

#### 1.3.3 How to obtain programme licences

We hope we can convince you of the productivity of our product. If you register your version on our homepage you will receive an updated version with extended functions:

- You can use as many databases as you wish, e.g. for different customers or computer centres.
- You can fully analyse and export the permissions of any one folder in your network.
- You can import existing folders and scan their permissions.
- You can define folder templates and base folders for your company for the automatic creation of new department or project drives.
- You can add or delete new members to Active Directory permission groups via the Group Membership dialogue (see chapter 2.5.3).

#### 1.3.4 Customer support

Should errors occur during operation and you are unable find a solution under „Help“ or in the User Manual, please send an email to [support@parks-informatik.de](mailto:support@parks-informatik.de). We will do our utmost to help you quickly. Email can also be sent via the menu **Help | E-Mail to Customer support....**



Programme runtime information and problems are documented in a protocol file. The file can be found in the `%USERPROFILE%\parksapps\logs` folder.

Copy this folder path into the Windows Explorer address list. The stored protocol files there have the name `PamWindows.log`. If you have problems with PAM, just send us the file and – even better – also screenshots per email with a short description of the problem. This will enable us to help you quickly.

You are missing a function or you have further suggestions to improve our product? We would be very pleased to hear from you!



Please check if a new version of the programme is available via the menu **Help | Search for updates....** It could be that a particular problem has already been solved in a newer programme version.

When sending an email to Customer Support please include your *product and application versions* – which you will easily find via the menu **Help | About...** as well as the *operating system of your computer* (e.g. Windows XP, Windows 7) and *the server with which you work* (e.g. Windows Server 2008).

### The sample data

To enable you to start work directly without complex preparatory work, the demo programme generates several master data itself during the first start-up.



Press **F6** in the master data area of the main window to see all the objects generated by the programme.

## 1.4 The user interface

The main window (fig. 1) appears after starting the programme.

The main window is divided up into several areas.

On the right-hand side you can see the welcome dialogue with an introductory text and reference to the documentations available. Click the links to open the documents, to start a scan or to create an Organization folder.



The documentation is locally installed as PDF documents. A programme is needed to open the documents (e.g. Adobe Reader).

# Parks Authorization Manager (PAM)

## Demo Manual

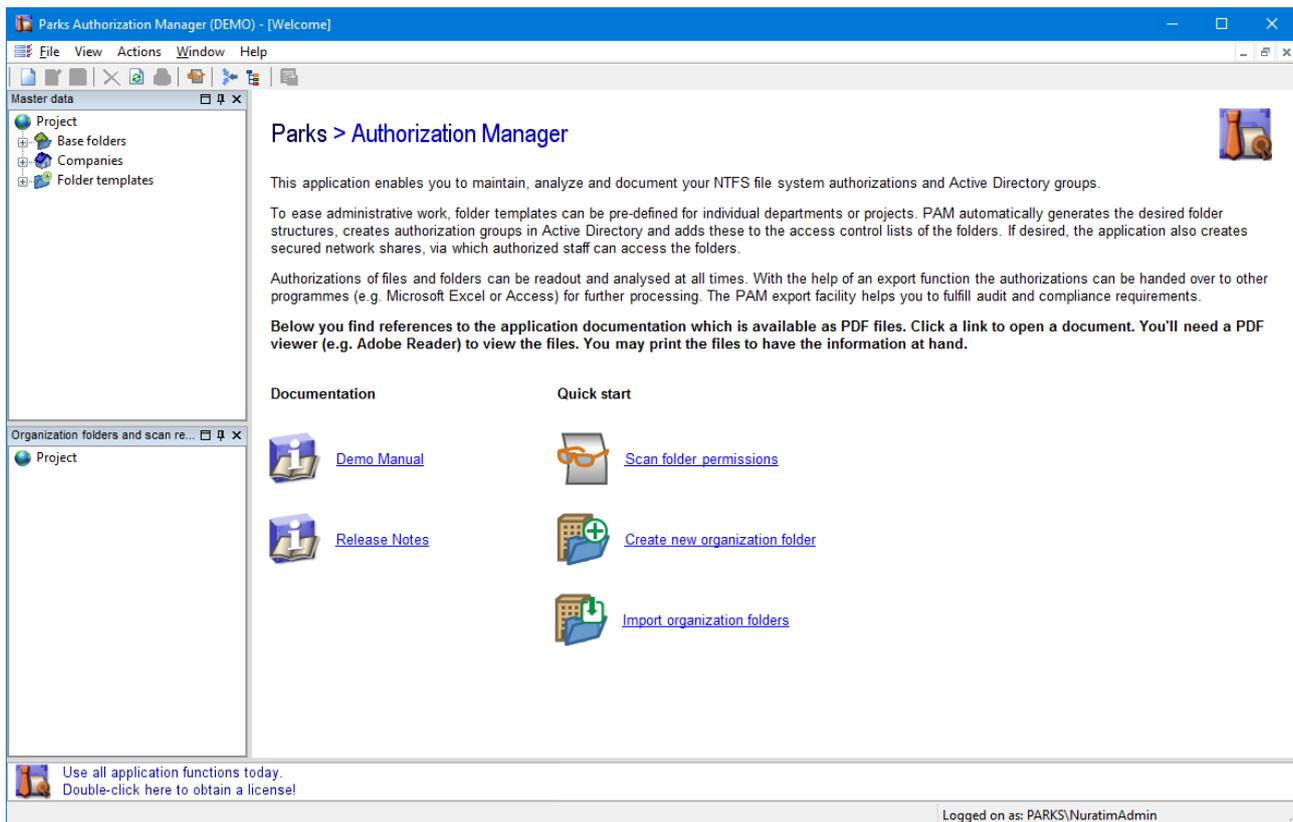


Figure 1: Main programme window

When you have closed the welcome dialogue by clicking the window closing symbols, these can be displayed again via the menu **Help | Welcome dialogue**.

On the left-hand side of the main window you can see the areas **Master data** and **organization folders and scan results**.

The **Master data** area holds all the information you need when you use PAM to plan and administer your folder structure. After programme installation only the company mentioned in the start configuration is included.

The **Organization folders and scan results** area contains all generated or imported organization folders as well as saved permission scan results.

The planning and administration of organization structures – along with the corresponding master data and organization folders – is described in chapter 2.3.

The display of the various areas is controlled via the menu **View**. They can be faded-in and faded-out there. All areas are organised in tree-like structures and the trees can be fully opened with the help of the **F6** button.

The areas **Scan result**, **Search result** and **Network environment** are normally not displayed. Scan results are automatically displayed after completion of a folder scan (see chapter 2.2.1), search results from the programme after a permission search (see chapter 2.2.1). You can display the network environment yourself via the menu **View** (see chapter 2.5.2).

The following overview describes the symbols used in various areas of the main window:



### **Project**

All data in a PAM data bank belong to one project (see chapter 2.1). Each data bank is a completed, logical database (comparable to a client).



### **Company**

Companies are used to maintain folder structures and permissions in your PAM database. Each company has several organization units, which can be administered in various categories (see below).

Working with companies is being described in chapter 2.3.1.



### **Category**

Categories are used to bunch an abundance of organization folders (see below) for a clearer arrangement.

The categories *Departments*, *General*, *User* and *Projects* are automatically generated in each database. The categories can be separately administered for each database via the application settings (see chapter 2.4).



### **Organization unit**

An organization unit corresponds to an administration unit in your company, e.g. a department or a project. They always belong to one company and are also centrally administered there (see chapter 2.3.1).



### **Base folder**

A base folder is a central folder in your file system that contains all organization folders (see below) of a category. You can e.g. define a base folder for all the departmental folders of your company.

Working with base folders is being described in chapter 2.3.2.



### **Folder template**

A folder template contains a folder structure for all organization folders (see below) of a category. Here you can e.g. generate the structure of a departmental folder in a set pattern. You define the Active Directory groups for each folder, which PAM automatically generates. The users are then allocated to the groups.

With the help of folder templates you get a homogeneous folder structure and fixed, free definable name conventions for the Active Directory groups.

Working with folder templates is being described in chapter 2.3.3.



### **Organization folder**

An organization folder is the specific characteristic of a folder for any one organization unit of your company. It is generated with the use of a folder template. By using place holders for the names of the organization units, an Active Directory group is generated

for each organization folder.

Working with organization folders is being described in chapter 2.3.4.



### Scan result

When you analyse the file system permissions, you can store the result in the database so that these can be recalled at a later stage (e.g. for a comparison).

Analysing file system permissions is being described in chapter 2.2.1.



### Permissions

Here you get a complete overview of the permissions of any one organization folder.

Most symbols in the trees have short descriptions: go over the symbol with the mouse to receive additional information for identification.

## 1.5 General operation

All programme functions can be reached via the menu. The most often used functions have keyboard short cuts stored behind the menu points for use without the mouse.

Some functions can be reached directly with a click on to the picture in the toolbar under the menu. A description of the function appears by moving the mouse pointer across the picture.

You can also click on to the objects in the tree and – by pressing the right side of the mouse – a context menu appears showing the functions available for the chosen object.

### Dialogue windows

Dialogue windows are mostly resizeable. Just move the mouse pointer on the borders and resize the window size at will.

The application uses different background colours for edit widgets. Widgets with blue background are mandatory and have to be filled in. Widgets with white background are optional and may be left blank. Grey background is used for values that are not editable. They can mostly be set upon create of an object only.

Blue text with underline contains a hyperlink. By clicking the text with the left mouse button, a context-dependent function will be executed.

## 2 Using the application

Parks Authorization Manager (PAM) gives you useful functions to analyse, organise and optimize your file system folder structures and permissions. With PAM you can simplify your daily tasks that you would perform using Windows Explorer or the Active Directory user management tools.

### 2.1 Databases

 In the demo version only one demo database can be used. Several databases, e.g. for different customers, can be created, edited and deleted in the licensed version.

The programme stores all information required for the administration of your permissions in a local database file.

On starting, the programme opens the demo database automatically.

 A PAM database can administer an Active Directory domain structure, i.e. a domain and all trusted, associated domains. They can be regarded as a sort of client.  
If you are a service provider for several customers, then you use a database per customer.

### 2.2 Features for checks and analysis

This chapter gives you information about about useful programme features for checks and analysis, e.g. scan of folder permissions, determine the effective permissions of a Windows user, check of a user's access to a folder and many more.

#### 2.2.1 Scan folder permissions

 In the demo version the number of files and folders to be analyzed is limited to 200.  
After purchasing a license you can analyze any number of local and network drives with the Professional Edition of this program.

The analysis of a selected folder and its subfolders offers a detailed overview of its permissions and permission groups.

PAM offers two analyse possibilities, the method **Scan folder permissions** and the method **Scan current permissions**.

With the method **Scan folder permissions** you can select any one folder and directly start the permission scan. This possibility makes sense if you wish to get a quick overview of the permissions of a particular folder. You can export the scan result into a text file or store them in a database.

The method **Scan current permissions** is based on already generated organization folders in PAM and is useful if you archive the scan result in the database and for instance wish to compare them. The scan result can be stored in the database.

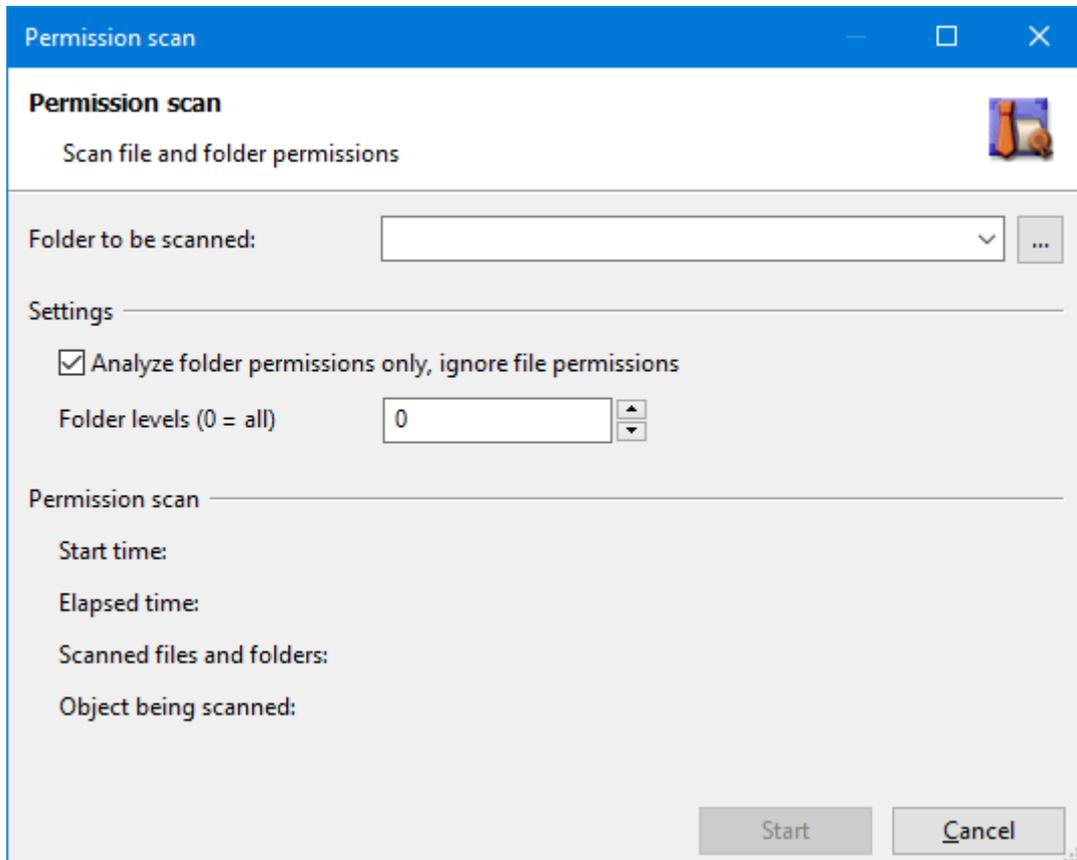


Figure 2: Configure permission scan

This chapter deals with the first method, Scan folder permissions, which you can run through as follows:

1. Click **Actions | Scan folder permissions** in the menu to start an analysis (fig. 2).
2. Enter the folder to be analysed and the corresponding path or select them via the push button ... behind the entry field.
3. Optionally it is possible to specify how many folder levels you wish to analyse. The default value is 0, with this all existing levels will be analysed. If you for instance enter a 2, only two folder levels will be analysed, i.e. the folder to be examined and the folder directly one level underneath.

You can also limit the scan to folder permissions only, in this case, file permissions will be ignored.

4. Click the button **Start**. The programme begins with the folder scan. After completion of the scan, the dialogue shows several statistics regarding the analysed folders.

5. Click the button **Close**.

The programme will then show you the area **Scan result** on the left-hand side of the main window. The window contains the scanned folder tree. The analysed permissions of the selected folder can be seen on the right-hand side (fig. 3). In a Matrix layout all associated permissions per group are shown.

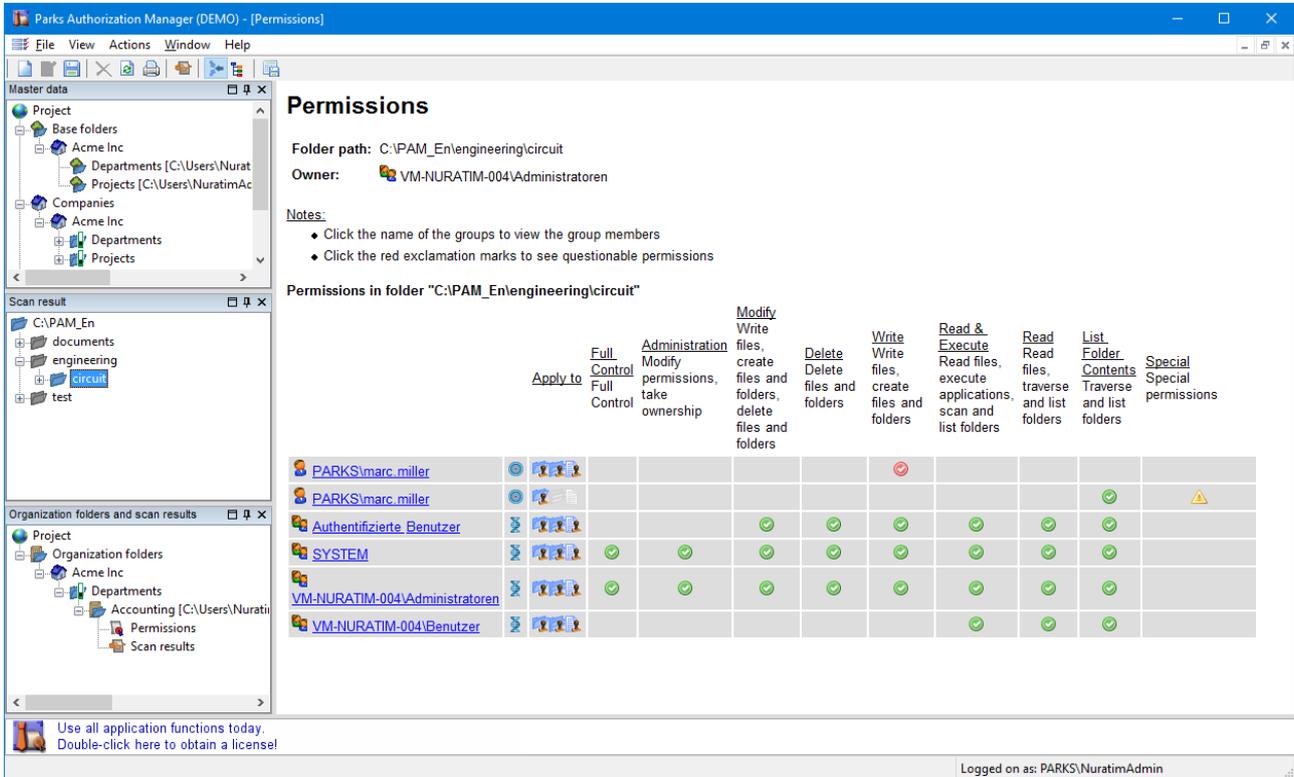


Figure 3: Scan folder permissions

User and group names are displayed by default in domain format. You can change this view to LDAP format. Changing the view between LDAP and domain formats is done via menu *View > Account display format* or the corresponding button in the toolbar.

**i** LDAP format is only possible if Active Directory is available. Local groups will always be shown in domain format.

In the two columns behind the account name, inheritance information is displayed. The narrow column indicates whether an existing directory has obtained its permissions via inheritance (helix) or whether it has explicit permissions (target).

The column *Apply to* indicates whether the permissions refer only to this folder or also to sub-folders and/or files.

**💡** By clicking on to a permission group (blue underlined) you open a window in which you can see the group members.

You may see red or yellow icons. The red icons with exclamation mark show permissions that usually should not be assigned (e.g. *modify permissions* for non-administrative users).



If you see a red folder in the permission scan result window, you do not have access rights for that folder and PAM cannot analyse it further. This can be seen as an indicator for a permission misconfiguration.

If an account does not have the permissions fully, e.g. Read or Write, the permissions will be shown as Special permissions (yellow icon with exclamation mark). By clicking the red and yellow icons with exclamation mark, the application will show you the elementary permissions affected.

Red icons with check mark permissions, that have explicitly being denied.



In the permission scan result, you can search for permissions for specific accounts (see chapter 2.2.2 for details).

### Tips for an effective folder scan

By observing a few tips, the effectiveness of the extensive amount of storage space needed to carry out a folder scan can be increased:

1. Do not analyse the complete C: drive

While the Windows folder, user documents and settings and the programme installation folders can contain plenty of files, the informative value of the analysed permissions is very low as normally only user-related permissions are set up there or the operating system pre-determined these permissions and they cannot be changed.

2. Analyse business data and organization folders

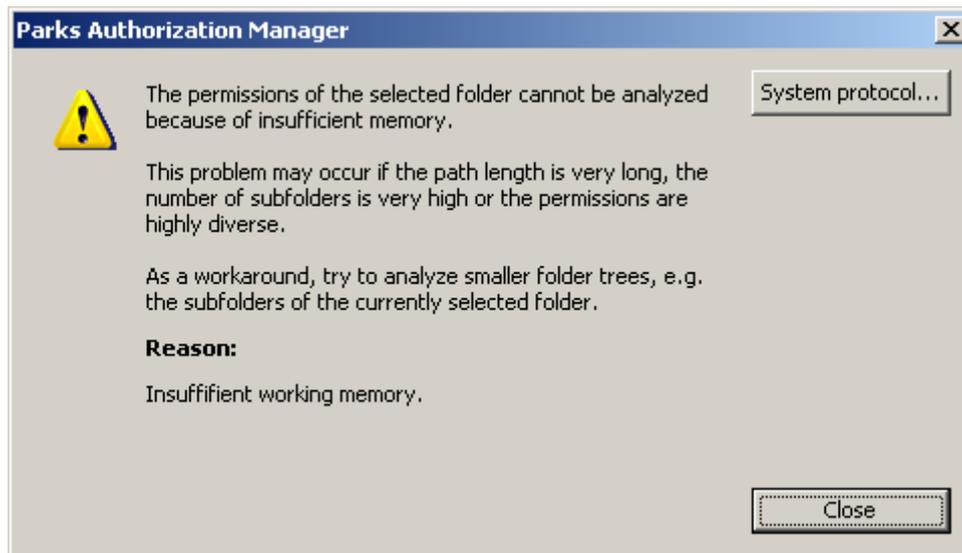


Figure 4: Memory exception

Concentrate on project and departmental drives when analysing, the permissions of which, if necessary, can later be revised with PAM. An error message will appear if there is not enough storage space available for the analysis (fig. 4). In this case, several smaller analysis should be carried out – e.g. analysis of single sub-folders.

### Save permission scan result in the database

You can save the result of a permission scan in the database and load it at a later time for reporting. So you need to perform another scan only if you have modified permissions.

The permission scan result is saved as follows:

1. Click into the scan result area in the main window with the mouse.
2. Click the main menu **File | Save**.
3. In the dialogue, enter a name for the permission scan result and click **Ok** to save the result in the database.

**Note:** The name of the permission scan result must not already exist in the database.

The saved permission scan result will be shown in the area *Organisation folders and scan results* in the main window.

### Load permission scan result from the database

A permission scan result can be loaded from the database as follows:

1. Click the name of the permission scan result in the area *Organisation folders and scan results* in the main window.

The scan result will be loaded from the database and displayed in the area *Scan result* of the main window. In this area, you can search for permissions for specific accounts (see chapter 2.2.2 for details).

## Export scan result

You can also export the result of the permission scan into a text file and then evaluate these with other programmes (e.g. Excel or databases).

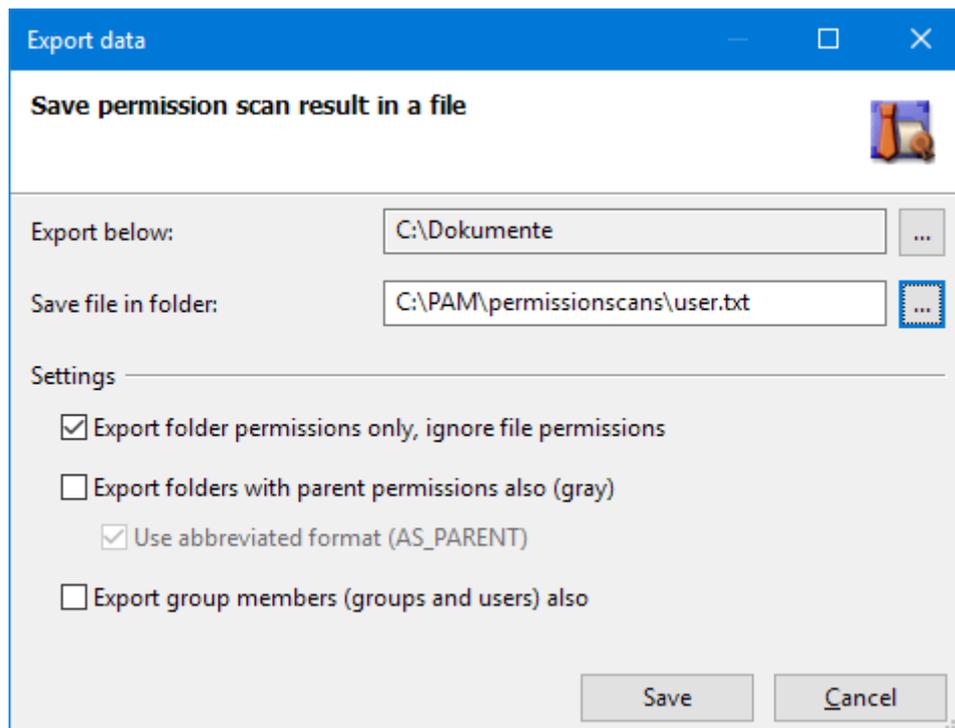


Figure 5: Export scan result



A connection to Active Directory is necessary for the export.



An export file will be available as a text file (\*.txt) or comma separated values file (\*.csv). The data will be exported in UTF-8 character encoding.

Each line in the file contains eight fields, which are separated by semi-colons.

The single fields are:

- file or folder path
- file type („directory“ or „file“)
- an indicator, if the permission is an allowed (“A”) or denied (“D”) one,

- permissions inherited or explicit assigned to this folder,
- permissions applied to „ThisFolder“ and/or „Subfolders“ and/or „Files“,
- permission,
- level,
- the user group that is authorized

#### Example of a record:

```
"C:\PAM\  
Test";"directory";"A";"Explicit";"ThisFolderOnly";"MODIFY";"0";"NUR  
ATIM\Domain Admins"
```

The scan results are exported as follows:

1. Click into the scan result area in the main window with the mouse.
2. Click the menu **File | Export | Scan result...**
3. You can narrow down the exported data and select a folder by clicking the button ... behind **Export below**. The program will then export data below the selected folder only.
4. Enter a path and file name or click the button ... to select a path.
5. Activate the option if you would like to export folder permissions only.

**Note:** If you only analyzed folder permissions in the permission scan, there will not be any file permissions to be exported in the scan result.

6. If you would like to export all permissions, not modified permissions only (= blue folders), click the corresponding button.

When exporting all accounts will be written to the file. To keep paths with same permissions as their parent more concise, click the option **Use abbreviated format (AS\_PARENT)**. In this case, a single line will be exported for the path: the permission field will contain the value AS\_PARENT, the account field will be left empty.

7. If you like to export group members (other groups and users) too, click the button **Export group members (groups and users) also**. The output file will contain a nesting level field. The level is 0 for groups and users assigned directly, and > 0 for each members level.
8. Click **Save** to export the data.

### Export permission scan result as PDF file

You can export a permission scan result as a PDF file.

To export a permission scan result as a PDF file report:

1. Click into the scan result area in the main window with the mouse.

2. Click the menu **File | Export as PDF...** or select the corresponding context menu function of a scan result (figure 6).
3. You can narrow down the exported data and select a folder by clicking the button ... behind **Export below**. The program will then export data below the selected folder only.
4. Enter a path and file name or click the button ... behind **Save file in folder** to select a path.
5. Click **Save** to start the PDF export. The progress bar will give you a hint how long the export will run.

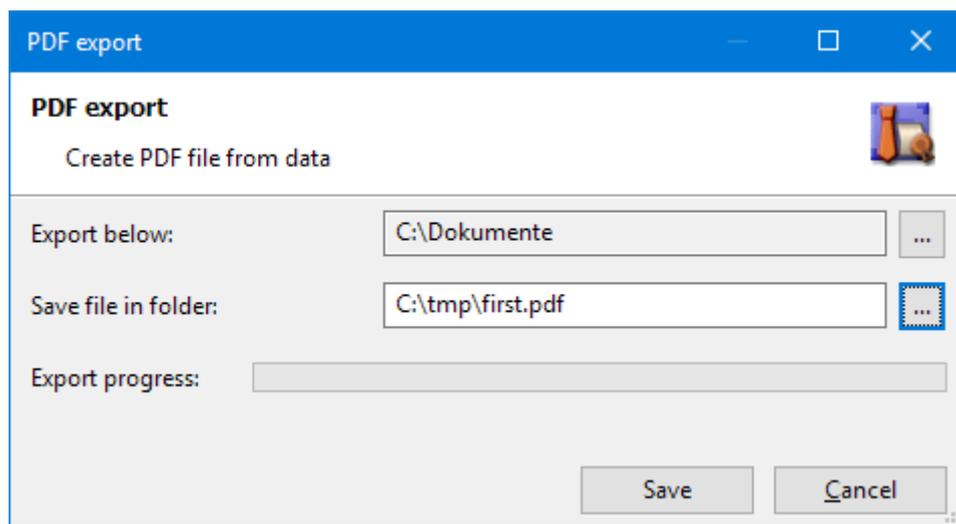


Figure 6: PDF export

## 2.2.2 Searching account permissions

If you have performed a permission scan or loaded a permission scan result from the database, you can search for specific account permissions.

First, you can search for effective user account permissions. That means that all paths will be shown with an explicit permission assignment for the specific account or any group it is a member in. Second, you can search user and group accounts by name. The search result will then show all paths with matching account names.

Each search method will act as a filter on the permission scan result, showing the search result in another window.

### Search effective user permissions

Using this function, you can search permissions of a specific Active Directory user. In addition, permission of user groups in which the account is a member will be searched too. This is an easy way to find a user's effective permissions in the file system.

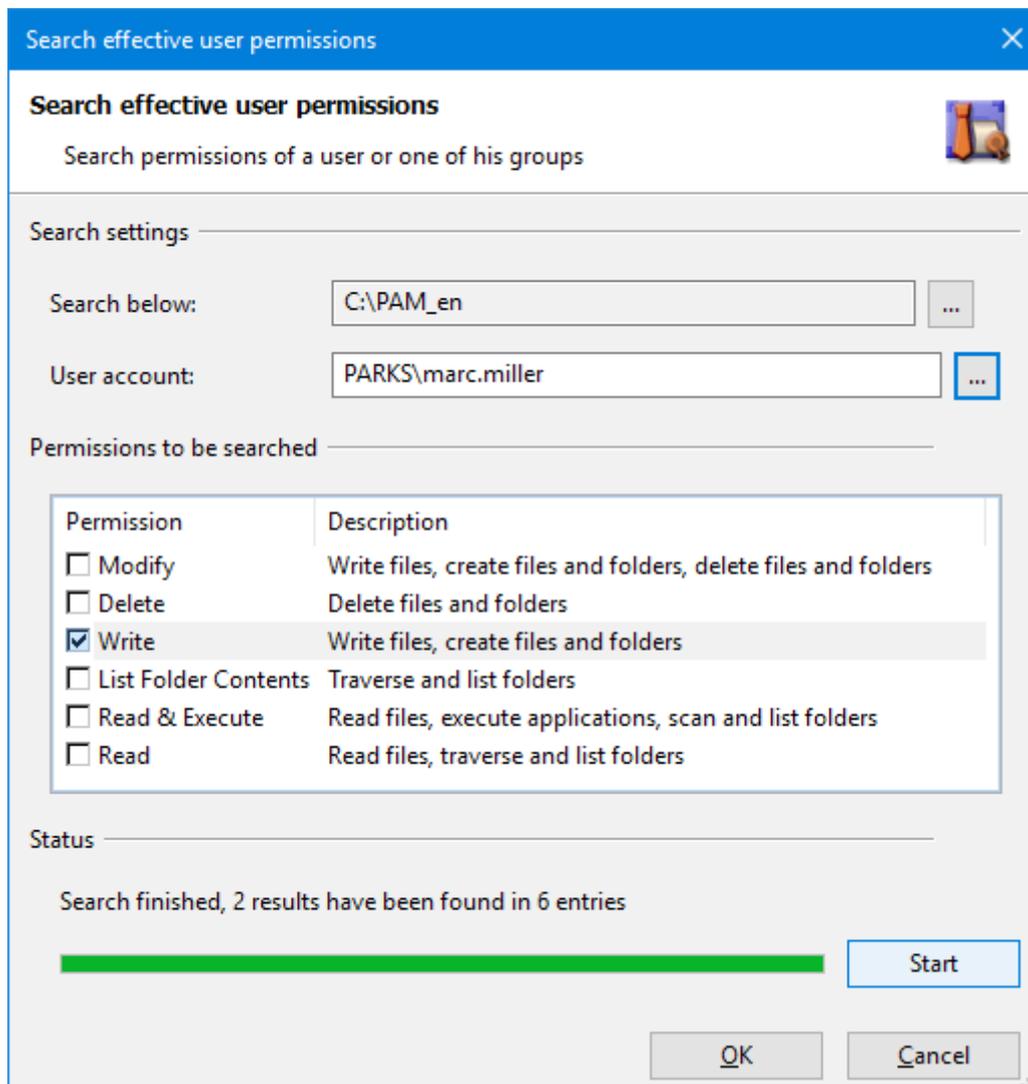


Figure 7: Search effective user permissions

1. To start the search open the context menu in the area *Scan result* or click the main menu **Actions | Search effective user permissions**.
2. **Optional:** Modify the path Search below. The search will only consider paths below the path to make the search effective even using very large scan results.  
When the dialogue is opened, the path will be the selected path in the scan result tree.
3. Enter the name of the user account using the format DOMAIN\ACCOUNT or click the button ... behind the widget to select an account in Active Directory.
4. Select the permissions that the account should have.
5. Click **Start** to start the search.

The programme starts the search and shows the progress in the progress bar. After the search is finished, click the button **Ok** to show the results that have been found. Click **Cancel** to discard the search result.

If the search delivers too much result entries, you can modify the search parameters and re-start the search by clicking **Start**, until a suitable result has been found.

The result will be shown in the main window area *Search result*, with the same style as a permission scan result. After selecting an entry in the tree, accounts and permissions will be shown on the right side of the main window. You can export the search result as text or CSV file.

If you click the root entry of the search result tree, you will get all paths and permissions. To keep the representation concisely, a maximum of 100 paths will be shown. Click other paths in the tree to see their permissions.

### Search accounts by name

A specific search in the scan results for permission groups holding a certain permission can be made. The search dialogue can be reached via the context menu in the area Scan result **Search users and groups by name...** or also via the main menu **Actions | Search users and groups by name...**, when the scan result window is activated (fig. 8).

Four search methods are available for specific searches:

1. For a *Default* search a part-word belonging to any one word is entered.  
**Example:** A search for “Adm” will find “Administrator” and “Domain Administrator”.
2. If the *Wildcards* search is used, then the symbols \* and ? are used to ignore part words (\*) or single characters during the search. This search complies with the usual functionality when searching in file systems.  
**Example:** A search for “Ad?in” will find “Admin” and other names with any digit/letter as third character.
3. The *Prefix* search can be used to search for objects with a prefix. The entered text must be at the beginning of the object name.  
**Example:** A search for “Adm” will find “Administrator”, but will not find “Domain Administrator”.
4. A search using *Regular expressions* permits flexible – but also complex – search queries.

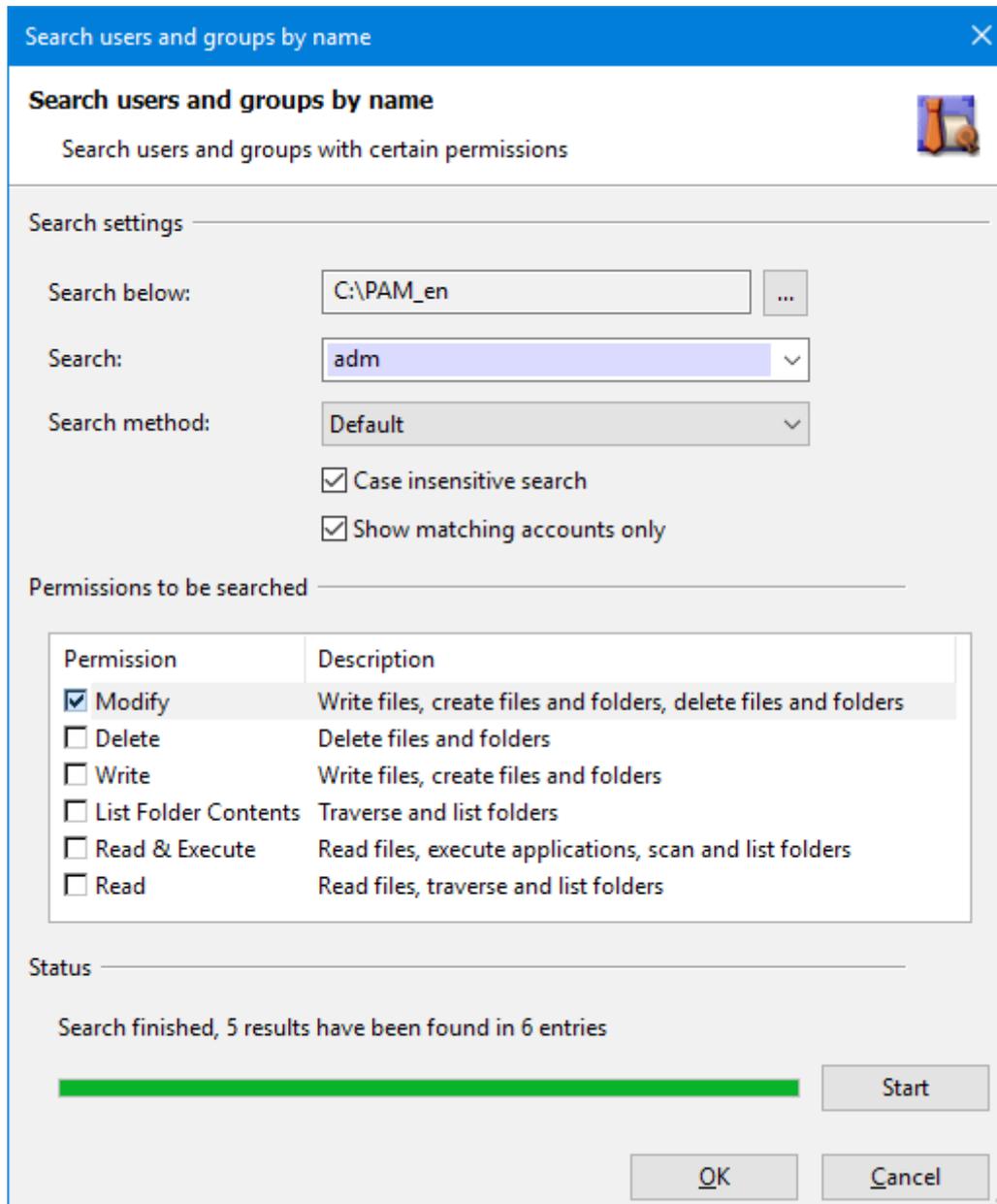


Figure 8: Search objects

1. To start the search open the context menu in the area *Scan result* or click the main menu **Actions | Search users and groups by name**.
2. **Optional:** Modify the path Search below. The search will only consider paths below the path to make the search effective even using very large scan results.

When the dialogue is opened, the path will be the selected path in the scan result tree.

3. Enter the name or search string that is suitable for the selected search method.
4. **Optional:** Modify the search options for case-insensitive searching or the display of the accounts found. In general, all accounts that have permissions for a path will be shown. If you want to see accounts that match the search only, click the option **Show matching accounts only**.
5. Select the permissions that the account should have.
6. Click **Start** to start the search.

The programme starts the search and shows the progress in the progress bar. After the search is finished, click the button **Ok** to show the results that have been found. Click **Cancel** to discard the search result.

If the search delivers too much result entries, you can modify the search parameters and re-start the search by clicking **Start**, until a suitable result has been found.

The result will be shown in the main window area *Search result*, with the same style as a permission scan result. After selecting an entry in the tree, accounts and permissions will be shown on the right side of the main window. You can export the search result as text or CSV file.

If you click the root entry of the search result tree, you will get all paths and permissions. To keep the representation concisely, a maximum of 100 paths will be shown. Click other paths in the tree to see their permissions.

### 2.2.3 Show effective user groups

In this dialogue all user groups for one particular user can be displayed. The function shows you the groups a user works with as soon as he logs into a particular work place.

1. To see the effective user groups of a particular user first click the menu **Actions | Show effective user groups** (fig. 9).
2. Select a user by clicking the button ... behind the entry field.
3. **Optional:** Select a computer by clicking the button ... behind the entry field, which is to be used as login computer for the user.
4. Start the query by clicking the button **Show**.
5. The programme will then show you all the user groups in which the above selected user is a member when he logs into the selected computer.
6. By clicking the button **Copy**, all displayed information can be copied into the clipboard. Instructions on using the clipboard can be found in chapter 2.5.4.

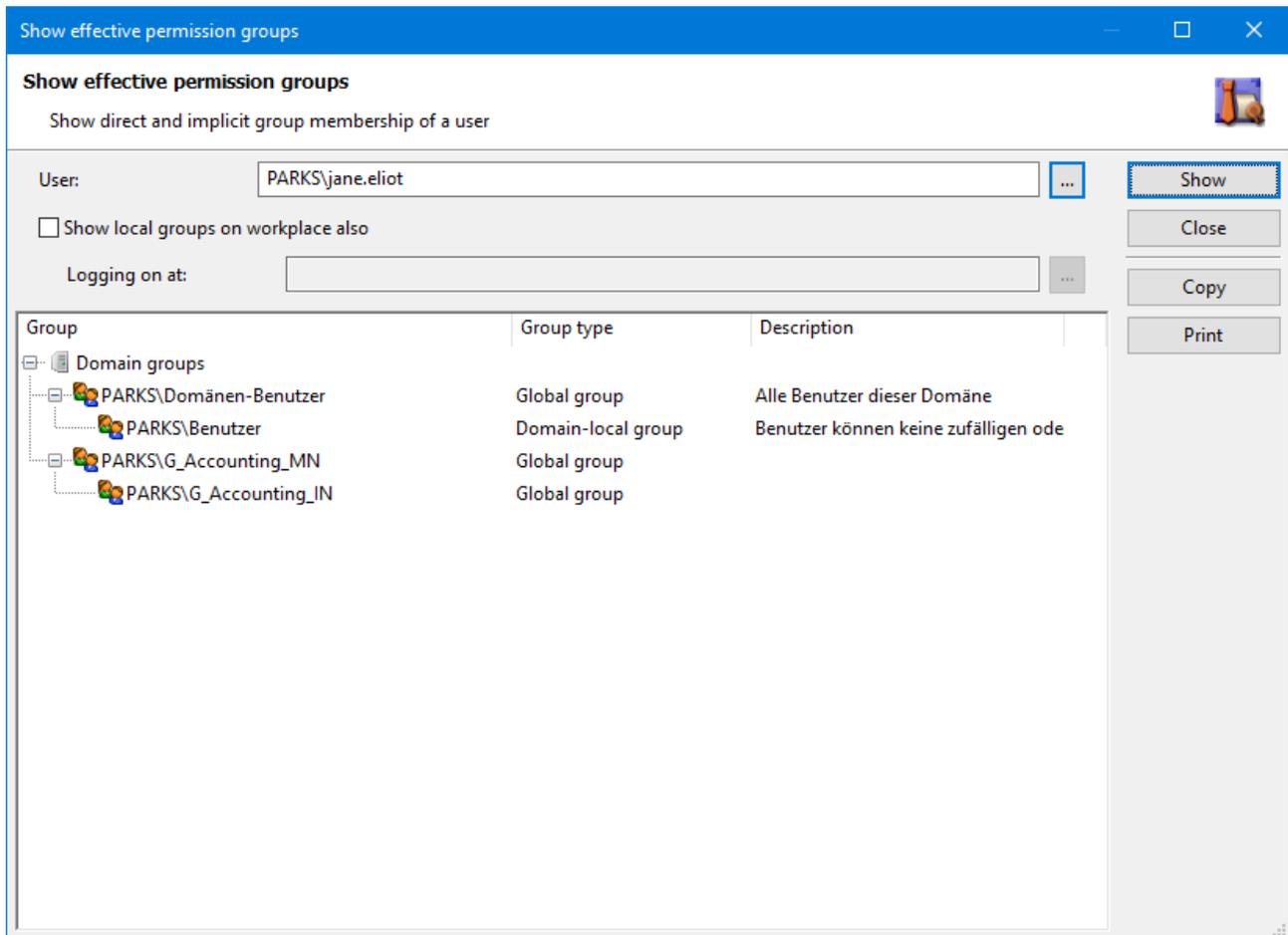


Figure 9: Show effective user groups

## 2.2.4 Verify user access to a folder

With the help of this function you can find out if a particular user has or has not access rights to a particular folder.

The test results will show you the folders in a path where access is denied and will give you an info as to why (e.g. if the user is not a member of an appropriate permission group). The problem can be further analysed by direct access to the folder via Windows Explorer.

1. To carry out an access test, click on the menu **Actions | Check folder access...**(fig. 10).
2. Select the corresponding user.
3. Select the folder in which the access permissions are to be checked.
4. Select at least one permission which the user should have in the folder.
5. Click the button **Check now**.

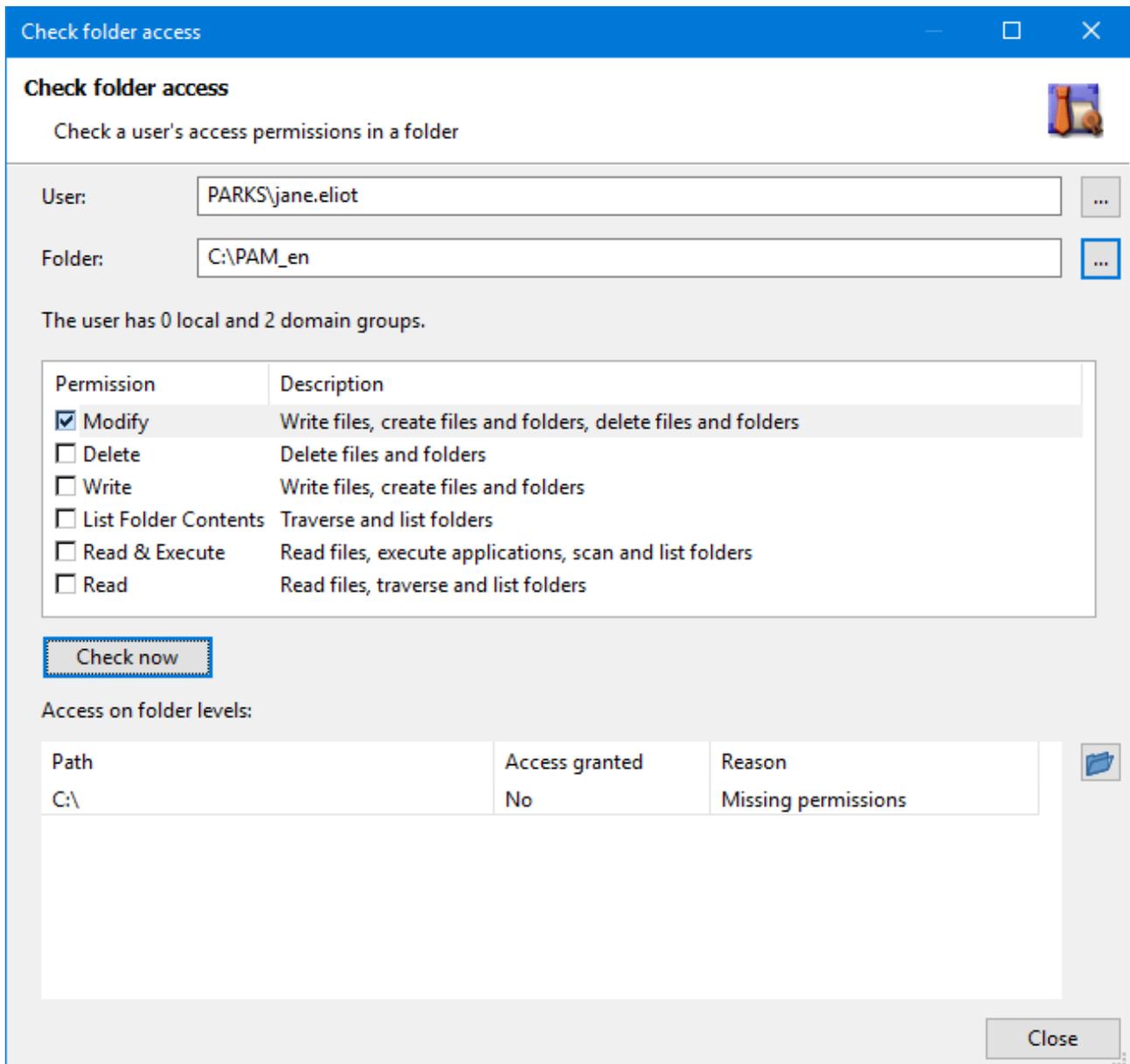


Figure 10: Check user access to a folder

In the list **Access on folder levels** all the permissions of the selected user will be checked and determined as to whether access is allowed or not in each folder level up to the target folder. Furthermore, the reason for the results of each level will be determined.



If access to a path is not allowed, select the chart line and click the button with the blue folder. The programme will then start the Windows Explorer, with which you can see and correct the permissions of the folder if necessary.

## 2.2.5 Search users and groups in Active Directory

The programme offers a function which will give you information about users and user groups in Active Directory. Via a search function you can determine users and user groups directly in Active Directory.

1. Click in menu **Actions | Search for users and groups in Active Directory...** (fig. 11).
2. Select in dialogue Active Directory Search the relevant domain.
3. (optional) Select in the **Search below** field via the button ... a particular organization unit.
4. The standard value in the **Search scope** stands at **Recursive**. With this, the programme also runs through the organization unit directly underneath. **One Level** in the **Search scope** means that a search will only be made in this selected organization unit.
5. Select in the field **Objects to be searched** for between **Users** and **User groups**.
6. Enter the name or name part in the **Search** field.
7. Enter the search algorithm in the **Search method** field. As well as the standard search, a prefix search, a place holder search, a search with regular words and a special LDAP search (LDAP filter syntax) are at your disposal.
8. Click the button **Start search**.

The programme starts the search process. The results will be listed in the **Search result** window. The account, the full name and – if available – the family name, the first name and the department will be shown.

Five search methods are available for specific searches:

1. For a *Default* search a part-word belonging to any one word is entered.  
**Example:** A search for “Adm” will find “Administrator” and “Domain Administrator”.
2. If the *Wildcards* search is used, then the symbols \* and ? are used to ignore part words (\*) or single characters during the search. This search complies with the usual functionality when searching in file systems.  
**Example:** A search for “Ad?in” will find “Admin” and other names with any digit/letter as third character.
3. The *Prefix* search can be used to search for objects with a prefix. The entered text must be at the beginning of the object name.  
**Example:** A search for “Adm” will find “Administrator”, but will not find “Domain Administrator”.
4. A search using *Regular expressions* permits flexible – but also complex – search queries.
5. The special LDAP search is based on the LDAP filter syntax.

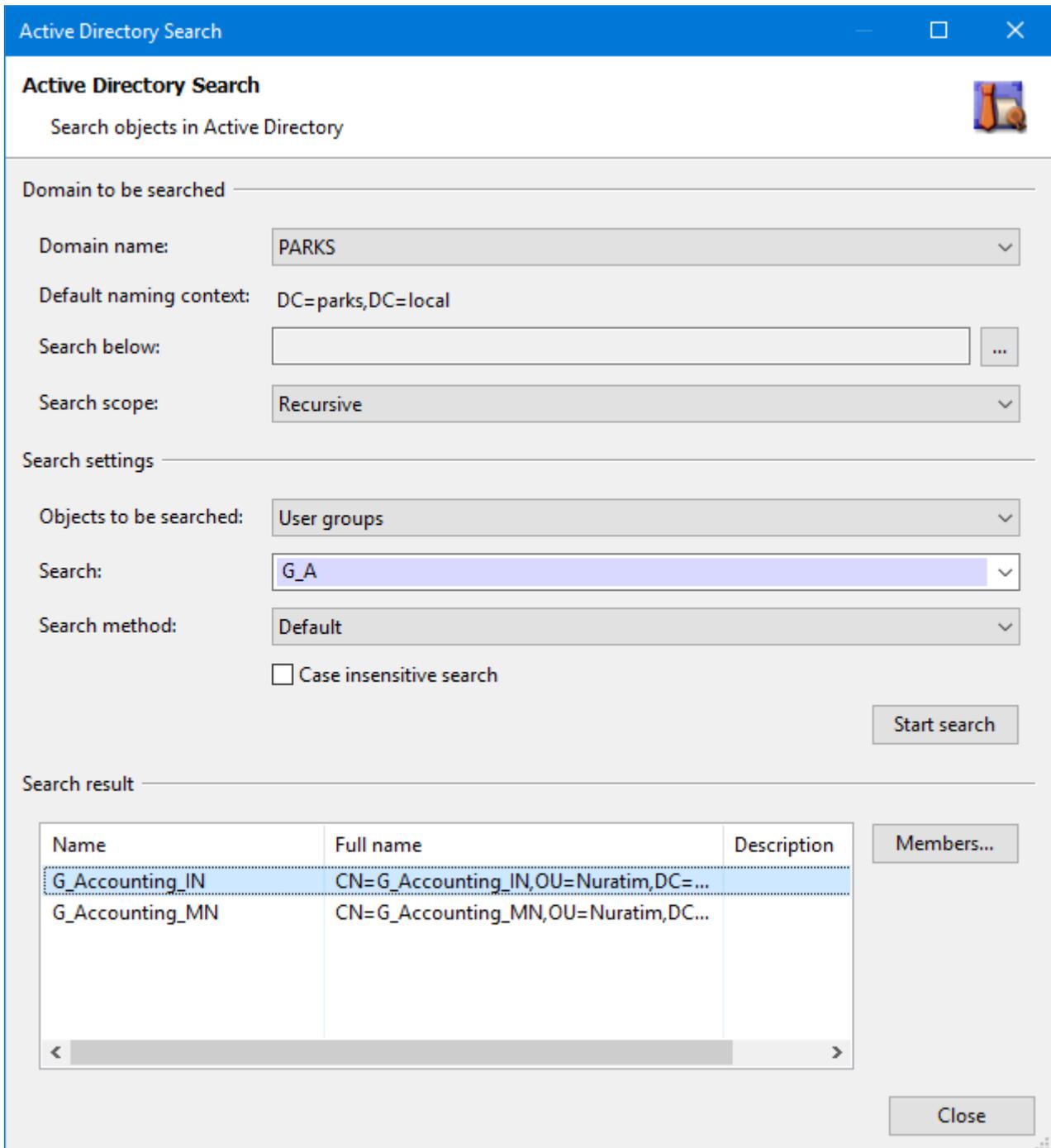


Figure 11: Active directory search

If you have searched for user groups, you can select a group in the result list and click the button Members... to display all group members (see chapter 2.5.3).

## 2.2.6 View active permission groups

Click the menu **Actions | Show my permission groups...**, to see information about your log-in names and your active permission groups (fig. 12).

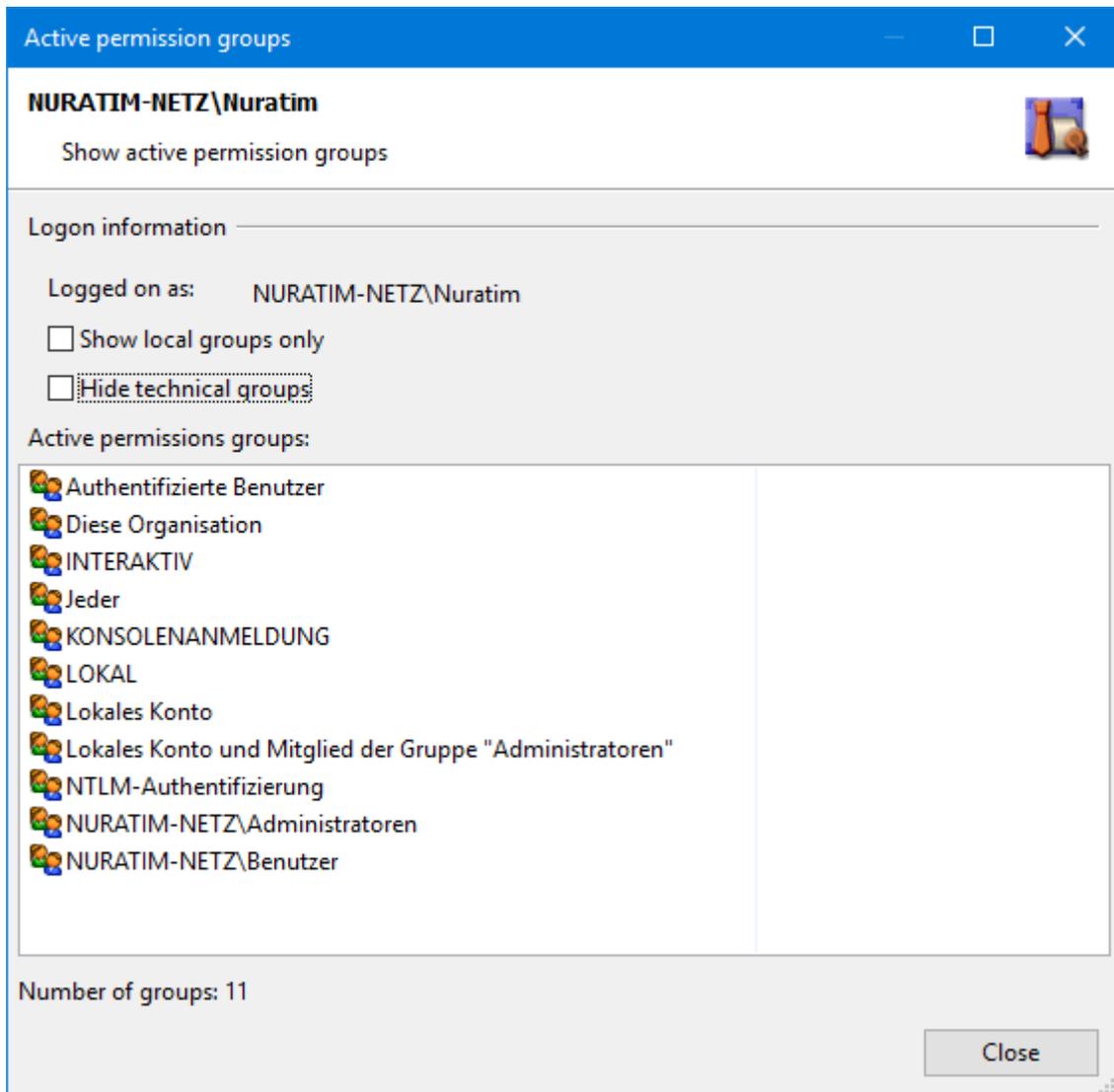


Figure 12: View active permission groups

## 2.3 Planning new file system structures

Requirements change over the years, projects and restructuring in the organisation necessitate adaptations. New folders are set up, Active Directory groups for permissions generated and allocated to users. A difficult and unclear chaos results out of what was once an originally well-thought-out structure:

- the folder structure of similar folders (e.g. for departments) is no longer consistent,
- it is no longer directly visible which Active Directory group is connected to which folder rights,
- the name regulations for the Active Directory groups are not always adhered to,
- when requested by users, it becomes difficult for administrators to allocate the correct Active Directory groups without causing unwanted side effects.

You have seen how to get an overview of your file systems with the help of the analysis functions in chapter 2.2. In the following chapters you will see how Parks Authorization Manager will enable you to build up and keep your file system permanently consistent.



Figure 13: Folder types and example structure

Figure 13 will show you the recommended structure for your folders. This structure guarantees that no more than four levels of a file system are provided with permissions (“best practice” recommendation).

The dark blue folder levels can be administered by PAM; the functions necessary to do so will be described in the following chapters.

PAM uses a 4 level folder system for structuring file systems:

#### ■ **Business data folder**

The business data folder is the basis for all user data. It separates the data from the operating system data.

The business data folder will not be administered by PAM but will be created and receive permissions beforehand.

#### ■ **Base folder**

The business data folder contains a number of base folders. These are folders that contain protected folders of a specific category, e.g. departments or projects.

#### ■ **Organization folder**

A base folder contains a series of organization folders. The folders can orientate themselves on organization units but can also be defined for other data requiring special permissions, e.g. for special licensed software applications for installation folders.



When defining organization folders orientate yourself to the company structure, i.e. departments or projects in your company.

#### ■ **Process folder**

Each organization folder can contain process folders, which have protected areas with their own permissions.



When defining organization folders orientate yourself to the process organisation, i.e. defined business processes within an organization unit. Typical process folders are e.g. protected folders for departmental or project leaders.

These folder types can be used to design and later set up your new folders. PAM will do the following for you:

1. create the folder structure,
2. create the user groups in Active Directory,
3. register the user groups in the corresponding folders,
4. copy the data out of the old folders into the new folders.

First create a company in PAM, in which you then add the base folders and folder templates. You can then create organization folders with this information. The following chapters will give you details of how to do so.

### 2.3.1 Working with companies

Companies are base objects to that are used to maintain file system structures and permissions. Each database must have at least one company. The first company is created with the help of the configuration assistant.

A company should also be created immediately after the creation of a new database.



In general you will use one company per database. If you use PAM in an enterprise setting with multiple Active Directory domains, you can use a company for each domain to represent organizational responsibilities in PAM.

#### Creating a new company

1. To create a new company click on to the menu **File | New | Company....**
2. Enter a name for the company.
3. (optional) Enter a description.
4. Click **OK** to save the company.



In the demo version only 2 companies can be created. With the licensed version (Parks Authorization Manager for Windows - Professional) you can create any number of companies.

#### Modifying a company

1. First select the required company in the **Master data** or **Organization folders** area of the main window (see chapter 1.4).
2. Then click the menu **File | Properties...** to open the company.

The tab **Companies** in the dialogue (fig. 14) contains the master data of the company:

- **Name** – the name of the company
- **Description** – an additional description (optional)

The tab organization units contains the organization units of the company:

- **Name** – the name of the organization unit (cannot be edited)
- **Display name** – the name of the organization unit for use e.g. in reports (optional, editable)

If no display name has been specified, the application uses the name of the organization unit.

- **Description** – an additional description (optional)

Organization units are the basis of all organization folders, the permissions of which you can administer and analyse with the programme (fig. Fehler: Verweis nicht gefunden).

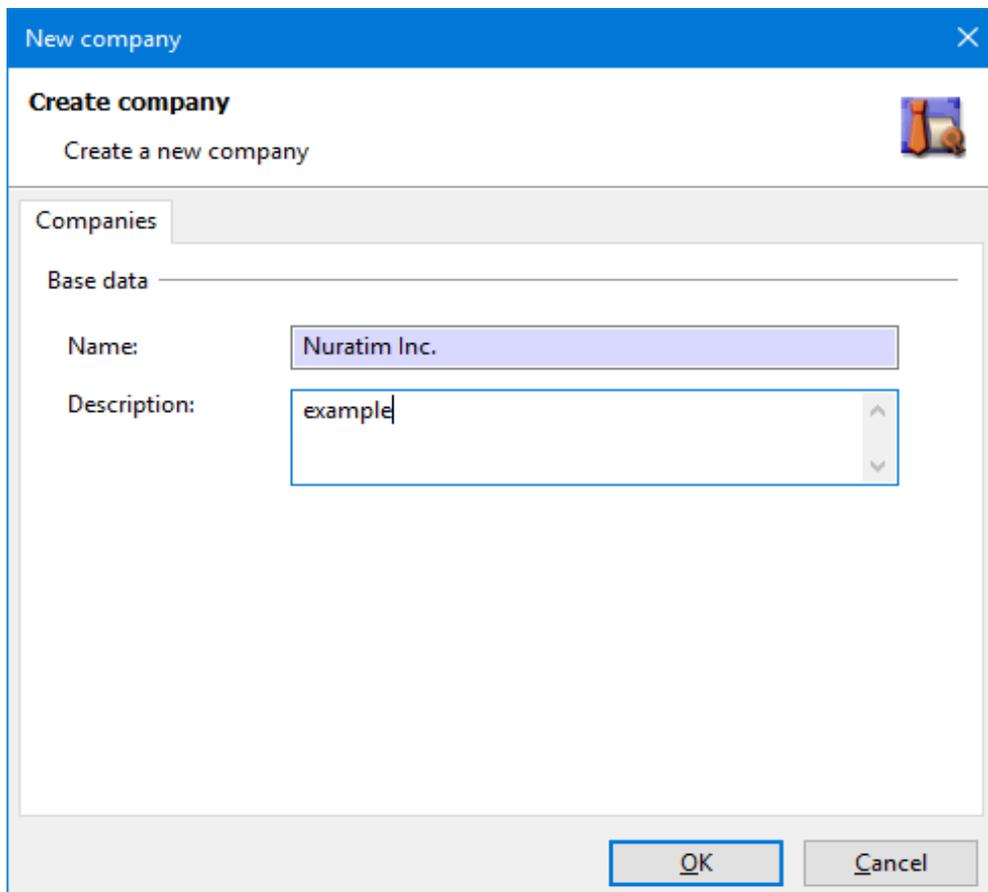


Figure 14: Company properties

Organization units are stored in categories. The categories **Departments**, **General**, **Projects** and **Users** are pre-defined in each database. The category list can be administered in the application settings (chapter 2.4).



The display name name is used in reports and can be changed at any time, e.g. after a company restructuring etc.

The name of the organization unit is being used when creating Active Directory user groups. A place holder in the group name will be replaced by the name of the organization unit (see “Editing folder permissions” in chapter 2.3.3).

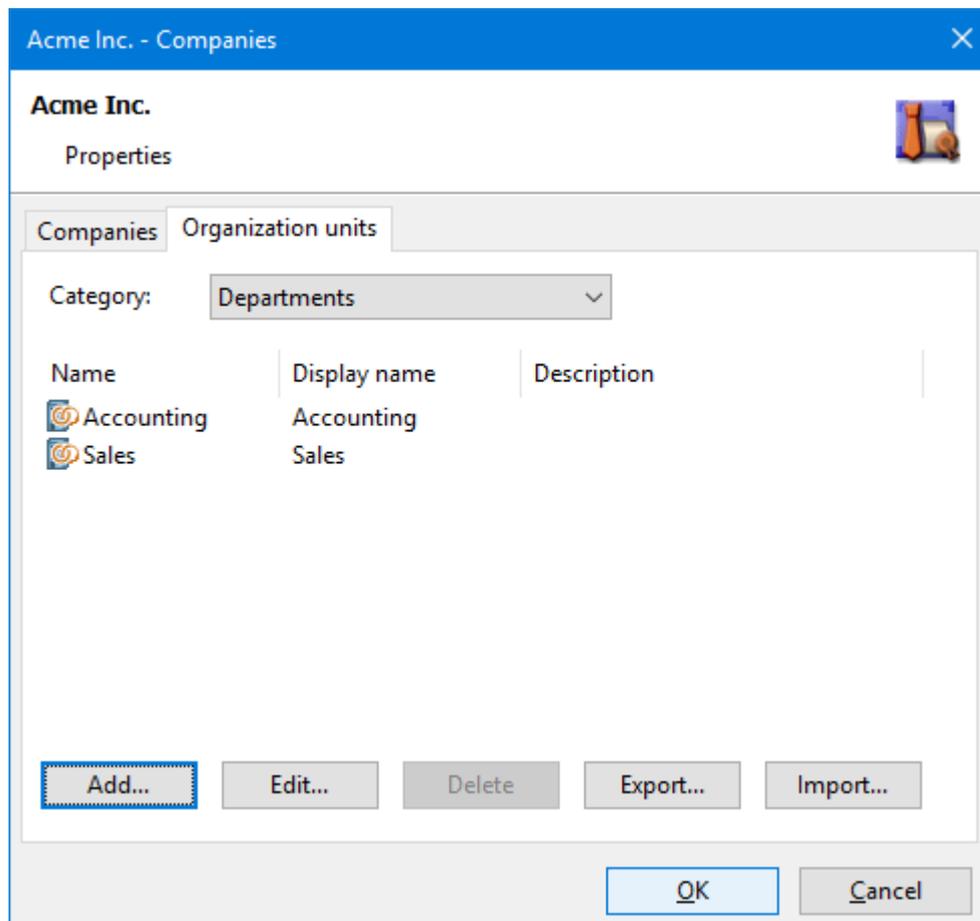


Figure 15: Organization units in a company

### Deleting a company

1. First select the required company out of the **Master data** or **organization folders** of the main window.
2. Then click the menu **File | Delete** and confirm the query.



A company can only be deleted after the dependent data of the company (organization folders, folder templates, base folders) have already been deleted.

### Renaming a company

1. First select the required company out of the **Master data** or **organization folders** of the main window.
2. Then click the menu **File | Rename**.

3. Enter a new name for the company.
4. Click **OK** to save the company.

### Creating an organization unit

1. First select the required category in the selection list. The programme then displays all existing organization units of this category.
2. Then click the **Add...** button.
3. Enter a name for the new organization unit.  
Note: The name cannot be modified later.
4. (optional) Enter a display name.
5. (optional) Enter an additional description.
6. Select the category of the new organization unit.
7. Click **OK** to save the organization unit.



If you need to create multiple organization units, you can also use the import function (see below).

### Editing an organization unit

1. First select the required category in the selection list. The programme then displays all existing organization units of this category.
2. Select an organization unit from the list.
3. Then click **Edit...**
4. Edit the display name and/or the description.
5. Click **OK** to save the organization unit.

### Deleting an organization unit

1. First select the required category in the selection list. The programme then displays all existing organization units of this category.
2. Select an organization unit from the list.
3. Click the **Delete** button and confirm the query to delete the organization unit.

### Exporting organization units

1. First select the required category in the selection list. The programme then displays all existing organization units of this category.
2. Then click **Export...**
3. Select the folder for the output file and enter a file name.
4. Click save to create the output file.

### Importing organization units

1. First select the required category in the selection list. The programme then displays all existing organization units of this category.
2. Then click **Import...**
3. Select the category for which the new organization units are to be created (fig. 16).
4. Enter the path of the input file or select a file by clicking the button ... behind the edit field.
5. Click **OK** to import the organization units.
6. After the import the programme will show you how many organization units have been imported.

Organization units that already existed will not be imported again.

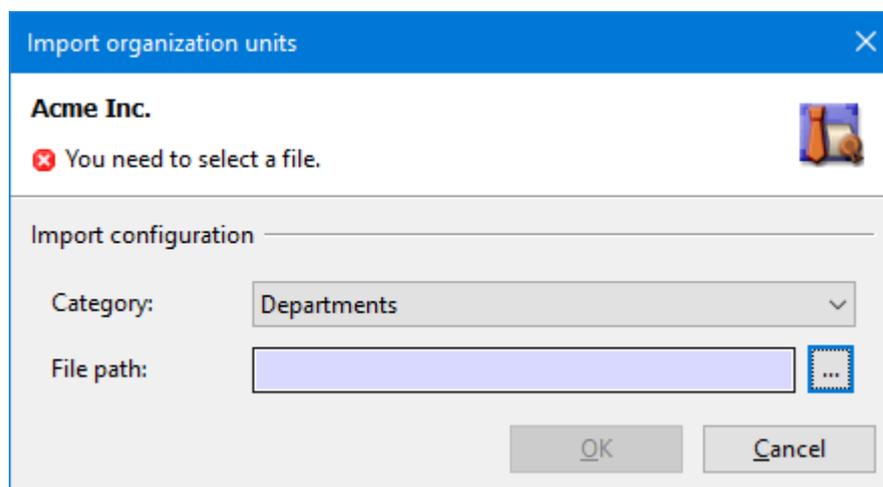


Figure 16: Importing organization units



You can create an import file for organization units with any text editor.

Each line in the file contains the information of an organization unit in four fields, that need to be separated by semicolon.

The fields are:

- Name
- Display name
- Description
- Category (will be filled in during exporting; will be ignored in import)

**Example:**

Controlling; Acme Inc. Controlling;Department at Site 12;



If you have already created some organization units, just export them to a file, edit the file and import the modified organization units again.

### 2.3.2 Working with base folders

Base folders are folders in which new organization folders for a category are created. You can define a base folder in which all new departmental folders are stored and you may also issue several base folders for any one category, if e.g. you administer different data servers.

#### Creating a base folder



In the demo version only 4 base folders can be created. With the licensed version (Parks Authorization Manager for Windows - Professional) you can create any number of base folders.

1. To create a new base folder click the menu **File | New | Base folder...**
2. Enter a name for the new base folder (fig. 17).
3. (optional) Enter an additional description.
4. (optional) Select the company for which the base folder is to be created.
5. (optional) Select the category of the organization folders that shall be created in this base folder later.
6. Enter the directory path to be used as base folder or select a folder by clicking ... behind the edit field.

Note: You can select a network folder or a local folder. The folder will be created if it does not already exist.

7. Click **Full access for domain administrators** if you want an administrators group full access to the folder (recommended).

If you do not want to use the domain default group because of distributed or delegated work in Active Directory click ... behind the edit field to select a different user group in Active Directory. The selection dialogue will be described in chapter 2.5.1.

8. Click **Full access for local administrators** if you want to grant full access to the local administrators group (recommended).

With this setting, local administrators can log in to the machine even if network is not available to access the data.

9. Click **Share the folder in the network** if a network share shall be created for the base folder.

(optional) Edit the name of the network share.

(optional) Activate access based enumeration of sub folders of the base folder (see below for a description).

10. Click **OK** to save the base folder.

The programme will create the folder in the file system (if it does not already exist) and will configure its permission settings to your selected configuration.



**Access based enumeration** is a useful feature to enforce the need-to-know principle in the file system to enhance security and privacy.

When accessing a folder using a share, users see only files and folders that they have at least read permission to. Files and folders, that they are not allowed to read, will be invisible.

Activating this feature is useful e.g. if the name of a file or folder only can promote unwanted information (e.g. folder "Employee Lay-off").

As a rule of thumb, access based enumeration should be enabled for all departmental or project base folders.



The programme removes all inherited permissions from the base folder, i.e. only the permissions defined in PAM will be active.

Therefore be careful to configure the administrator group permissions correctly.



You can create multiple base folders for a category, e.g. if you want to distribute the folders across multiple file servers.

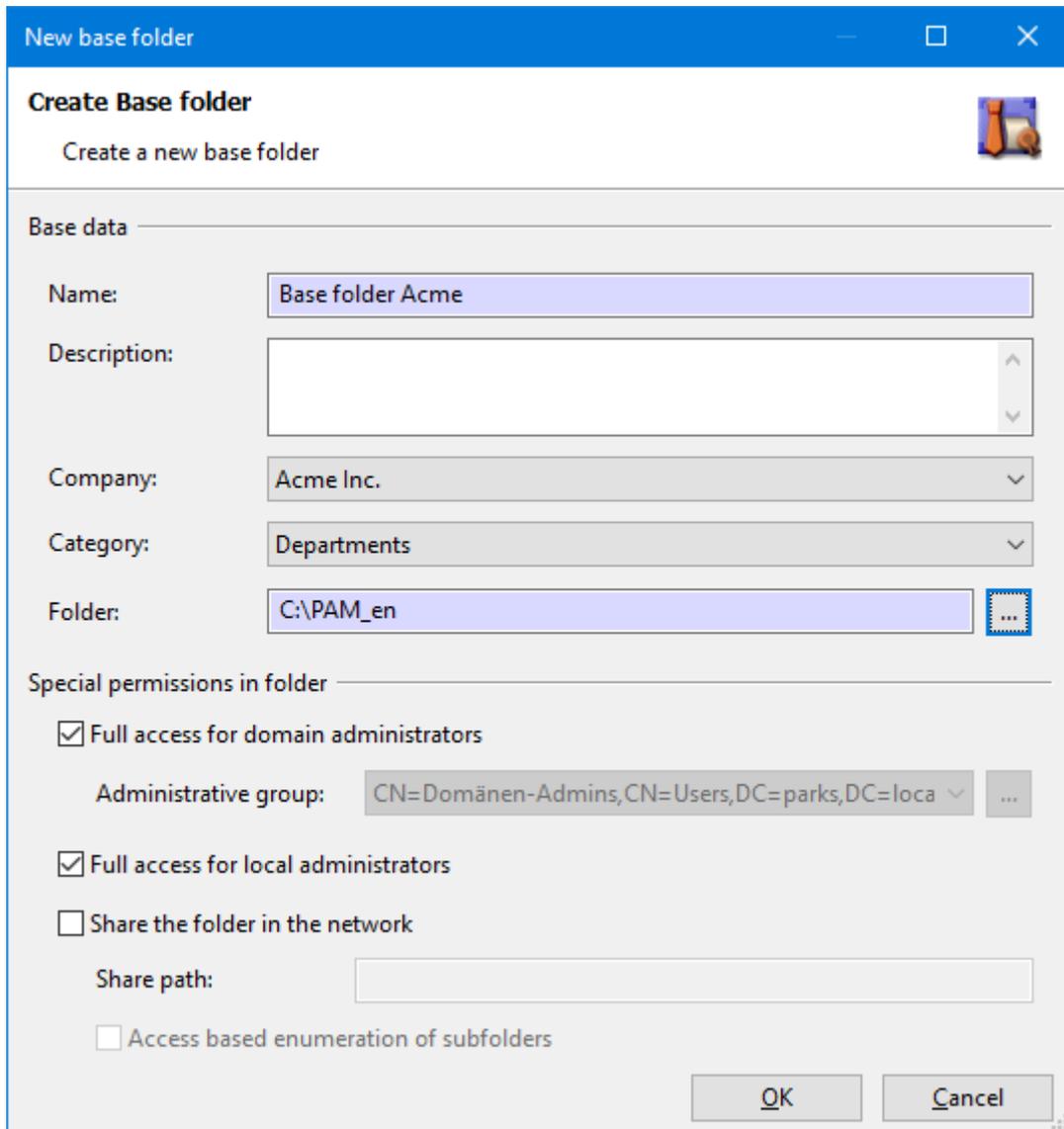


Figure 17: Creating a base folder

### Modifying a base folder

1. First select the required base folder in the **Master data** area of the main window.
2. Then click the menu **File | Properties...** to open the base folder.
3. Edit the description of other information of the base folder.
4. Click **OK** to save the base folder.

## Deleting a base folder

1. First select the required base folder in the **Master data** area of the main window.
2. Then click the menu **File | Delete** and confirm the query.



The base folder can only be deleted if the dependent data of the base folder has already been deleted (organization folders).

## Renaming a base folder

1. First select the required base folder in the **Master data** area of the main window.
2. Then click the menu **File | Rename**.
3. Enter a new name for the base folder.
4. Click **OK** to save the base folder.

### 2.3.3 Working with folder templates

A folder template defines how an organization folder shall look in the file system. It contains a folder structure that can be defined freely. For each folder, Active Directory groups with permissions can be specified.

Folder templates are being used as a template if an organization folder is to be created (see 2.3.4). The file system folder structures and Active Directory user group will be created based on its definitions.

Using folder templates, you can define your own standards for file system structures and group naming conventions in Active Directory that will be enforced by PAM.

## Creating a folder template



In the demo version only 4 folder templates can be created. With the licensed version (Parks Authorization Manager for Windows - Professional) you can create any number of folder templates.

1. To create a new folder template first click the menu **File | New | Folder template....**
2. Enter a name for the new folder template (fig. 18).
3. (optional) Enter an additional description.
4. (optional) Select the company for which the folder template is to be created.
5. Click **Full access for domain administrators** if you want an administrators group full access to all organization folders created using this template (recommended).

If you do not want to use the domain default group because of distributed or delegated work in Active Directory click ... behind the edit field to select a different user group in Active Directory. The selection dialogue will be described in chapter 2.5.1.

6. Click **Full access for local administrators** if you want to grant full access to the local administrators group (recommended).

With this setting, local administrators can log in to the machine even if network is not available to access the data.

7. Edit the folder structure in the field **Subfolders and permissions** (see below).
8. Click **OK** to save the folder template.

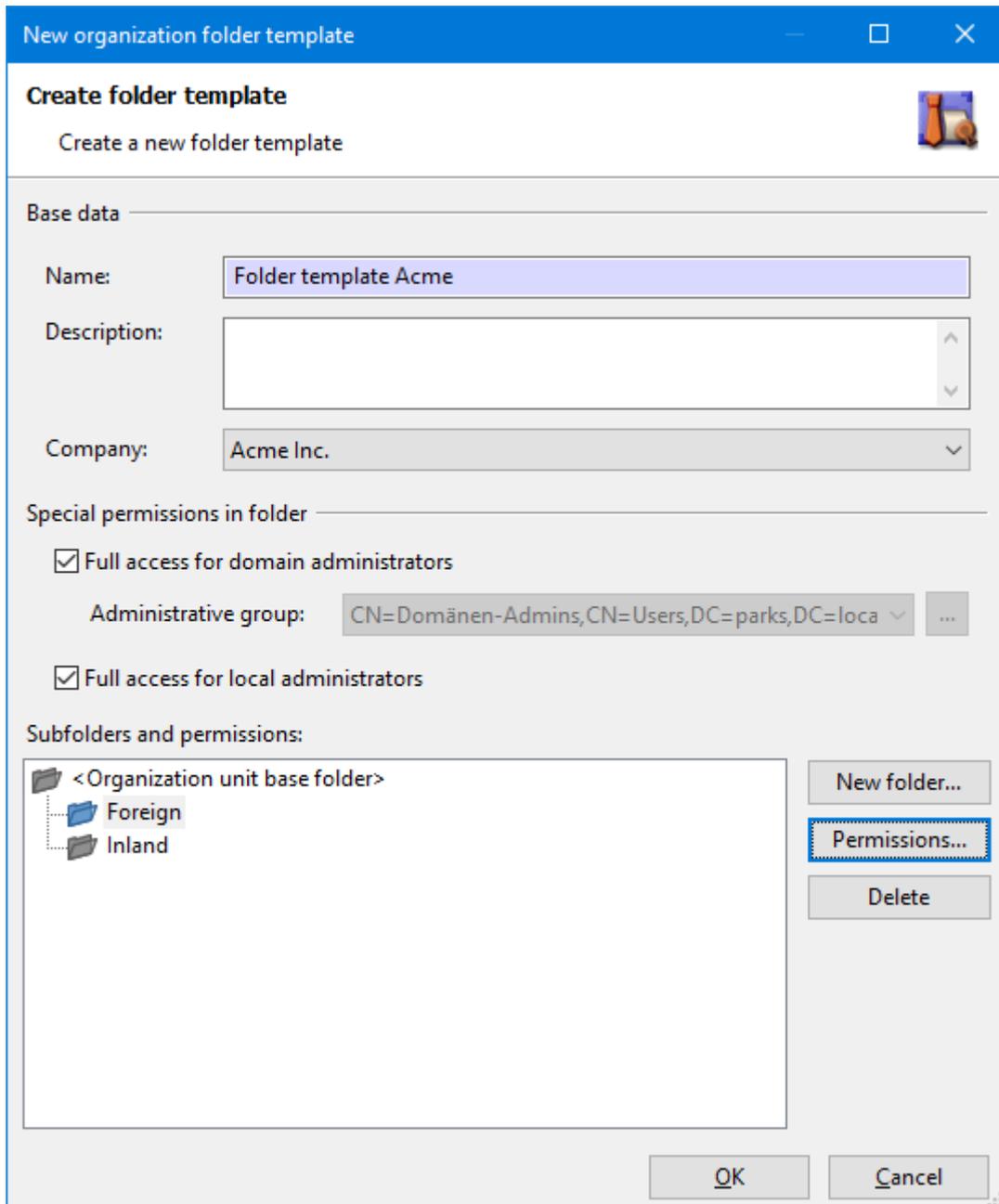


Figure 18: Creating a folder template

### Managing folders and permissions

The edit field **Subfolders and permissions** (fig. 18) contains the folder structure, that will be created and configured if a new organization folder is being created based on this folder template (see 2.3.4).

The folder symbol can be displayed grey or blue. Grey means that the folder does not have permissions assigned to it, it will inherit the permissions of the parent folder.

Blue folders have permissions that can be edited by clicking the button **Permissions...**

The “Organization unit base folder” is the organization folder itself. It can contain multiple sub-folders.



The base folder has no permissions at the beginning. However, permissions should be set up (folder symbols must be blue), as without permissions no access to the folders is possible. If no permissions are set, then at least the button **Full access for domain administrators** should be activated to enable the domain administrators to have access to the folders.

### Creating a new folder

1. First select the folder in the tree that will be the parent of the new folder.
2. Click the button **New folder...**
3. Enter the name of the new folder.
4. Click **OK** to save the new folder.

### Deleting a folder

1. Select the folder to be deleted in the tree.
2. Click the button **Delete** and confirm the query to delete the folder.



When deleting a folder, all folders below will be deleted as well.  
The base folder at the root of the tree cannot be deleted.

### Editing folder permissions

1. First select the folder in the tree whose permissions are to be edited.
2. Click the button **Permissions...** to open the folder permission dialogue (fig. 19).

In the dialogue you see the relative path of the folder within the folder template.

The list Groups and permissions contains the Active Directory groups and the permissions that they will provide to users.

Groups and permissions can be edited by using the buttons **New group...**, **Permissions...** and **Delete**.

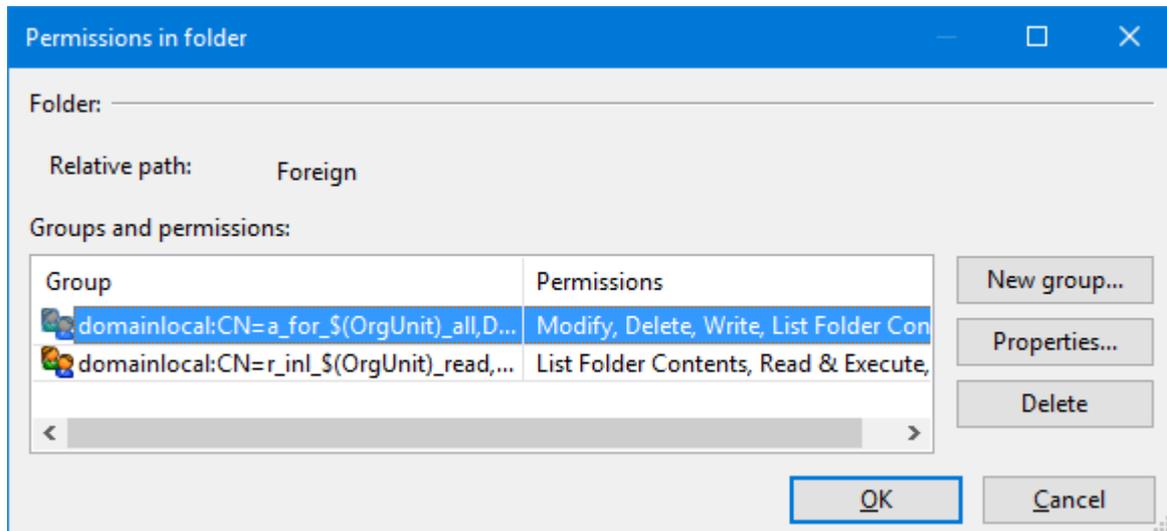


Figure 19: Folder permissions

### Creating a new group

1. Click the button **New group...** to create a new group for the folder (fig. 19).
2. Select the Active Directory domain where the new group is to be created (fig. 20).
3. Select the scope of the group.
4. Select the container in Active Directory, where the group is to be located.
5. Enter the name of the group using your favourite naming convention.



When you create an organization folder based on the folder template, you will need to specify the organization unit which will use the folder (see chapter 2.3.1).

By using placeholders in the names of the permission groups you will be able to use the name of the organization unit in the group name. Therefore you will be seeing for each group in Active Directory to which organization unit it belongs to.

Use the placeholder **\$(OrgUnit)** in the name of the permission group. This placeholder will be replaced by the name of the organization unit when creating the permission group in Active Directory.

Example: Define a group with the name `O_$(OrgUnit)_R` with read permissions. When you create an organization folder for the organization unit *Controlling* using this folder template, PAM will create a permission group named `O_Controlling_R` in Active Directory which you can later assign users to.

Just use your favourite naming convention and use the placeholder, PAM will do the other work for you.

You can also select an existing group from Active Directory if you click the button ... behind the edit field.

6. Select the permissions to be granted to the group in the file system folder.

You can select special permissions using the button **Advanced...** Use the **Delete** button to remove all permissions that have already been assigned. You can then assign new permissions.

For some permissions, PAM will automatically extends them according to the operating system rules. If you e.g. select Read & Execute, the permissions *Read* and *List Folder Contents* will be activated to.

7. Click **OK** to save the permission group.

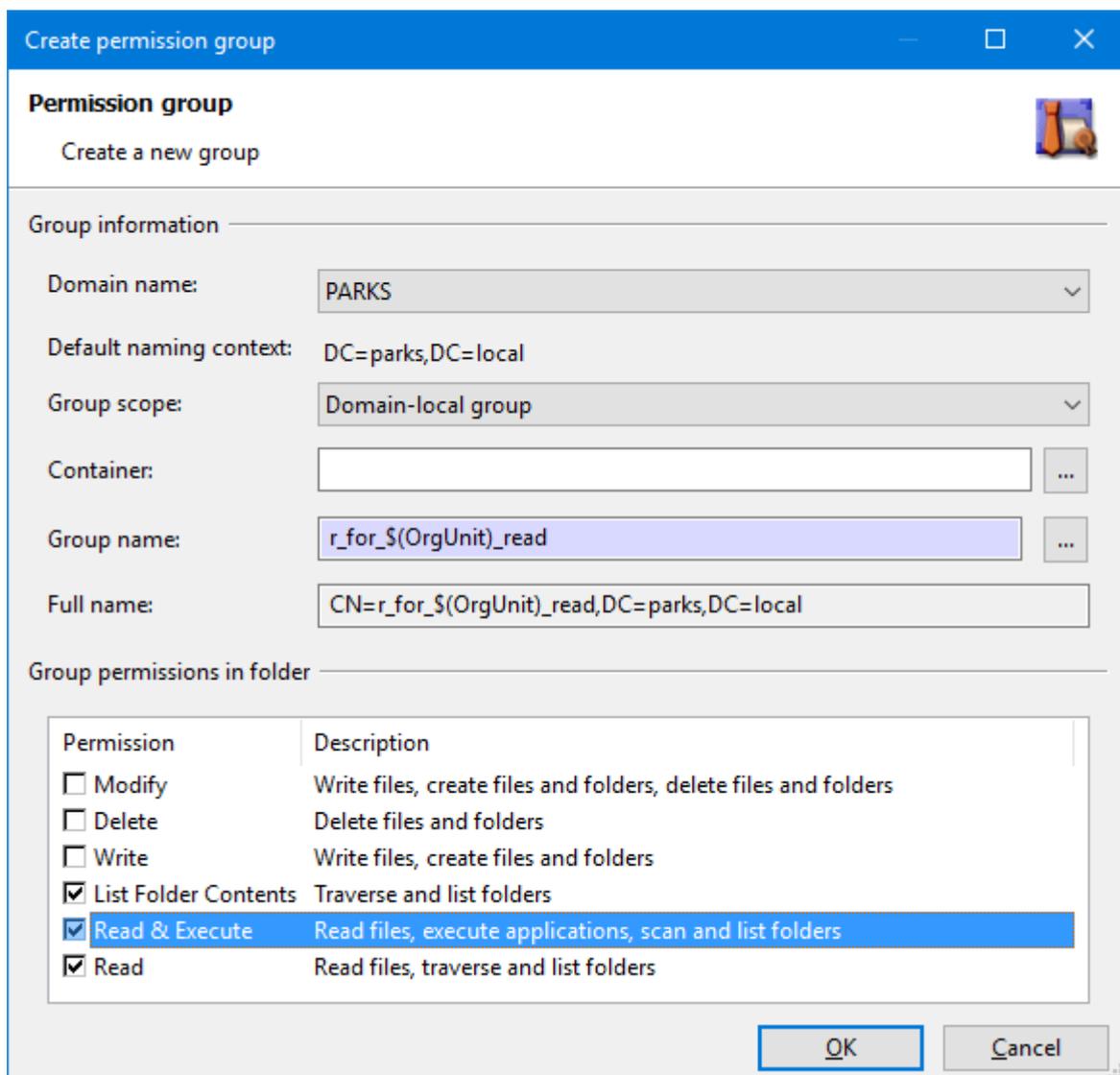


Figure 20: Creating a new permission group

### Editing a permission group

1. Select the permission group to be edited in the list (fig. 19).

2. Click the button **Permissions...** to edit the group.
3. Modify the permissions or other values (fig. 20). You can select special permissions using the button **Advanced...** Use the **Delete** button to remove all permissions that have already been assigned. You can then assign new permissions.
4. Click **OK** to save the permission group.

### Deleting a permission group

1. Select the permission group to be edited in the list (fig. 19).
2. Click the button **Delete** and confirm the query to delete the group.

### Deleting a folder template

1. First select the required folder template in the **Master data** area of the main window.
2. Then click the menu **File | Delete** and confirm the query.



The folder template can only be deleted after the dependent data has already been deleted (organization folders).

### Renaming a folder template

1. First select the required folder template in the **Master data** area of the main window.
2. Then click the menu **File | Rename**.
3. Enter a new name for the folder template.
4. Click **OK** to save the folder template.

## 2.3.4 Working with organization folders

This chapter describes how organization folders are managed. These folders contain the files of an organization unit. An organization folder will be created in a base folder (see chapter 2.3.2), its folder structure and permissions are based on a folder template (see chapter 2.3.3). When creating an organization folder, PAM creates the folder structure in the file system, creates the permission groups in Active Directory and inserts them into the access control lists of the file system folders.

### Creating an organization folder



In the demo version only 6 organization folders can be created. With the licensed version (Parks Authorization Manager for Windows - Professional) you can create any num-

ber of organization folders.

1. Click the menu **File | New | Organization folder** to open the wizard for creating an organization folder.
2. On the first page of the wizard, select the company, the category and the organization unit for which the folder is to be created (see fig. 21).
3. Click the button **Next >** to continue with the next wizard page.

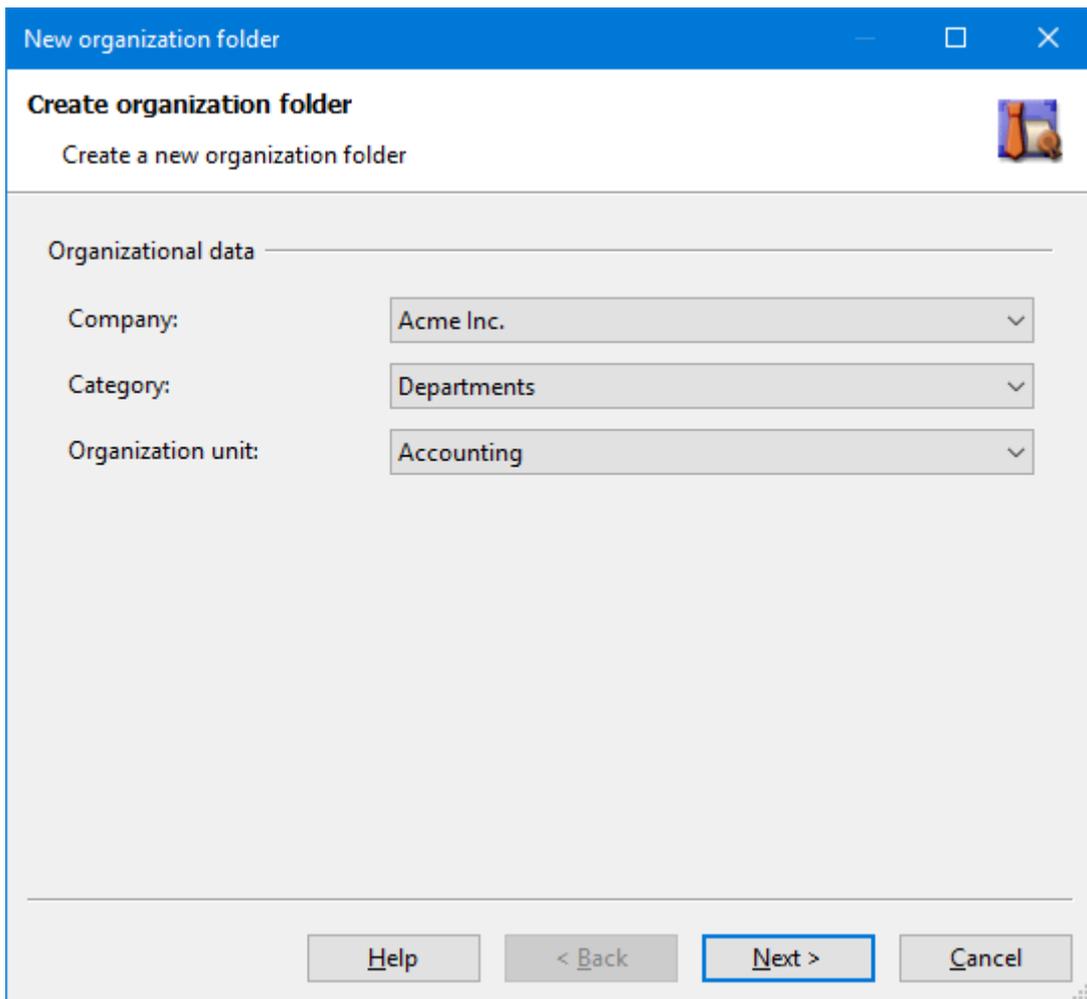
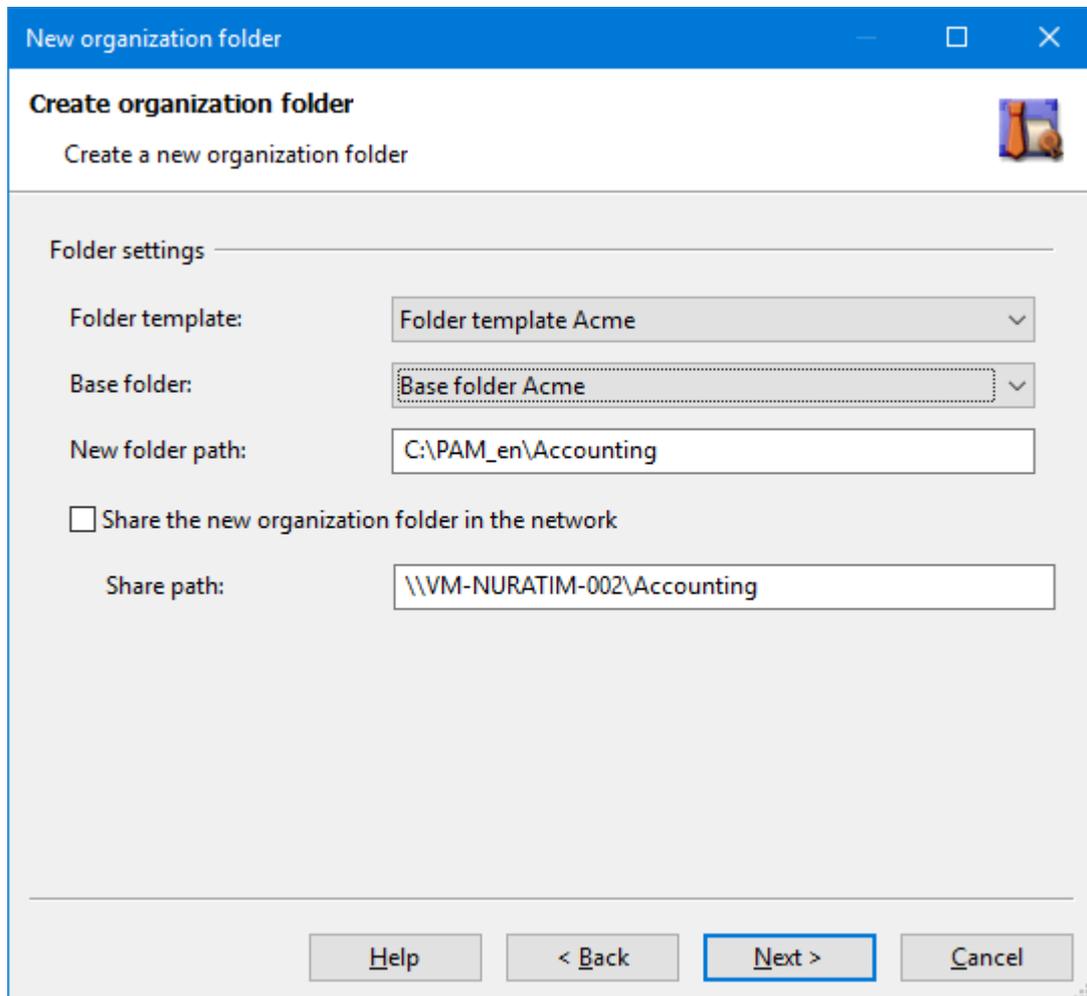


Figure 21: Creating an organization folder (organization data)

4. On the second page of the wizard, select the folder template and the base folder in which the folder is to be created.
5. (optional) Click the checkbox and modify the path of the network share if you want to share the organization folder in the network.



It is recommended to share the base folder in the network and enable access based enumeration, to avoid sharing all organization folders manually.



The screenshot shows a Windows-style dialog box titled "New organization folder". The main heading is "Create organization folder" with a sub-heading "Create a new organization folder". Under "Folder settings", there are four fields: "Folder template:" with a dropdown menu showing "Folder template Acme"; "Base folder:" with a dropdown menu showing "Base folder Acme"; "New folder path:" with a text box containing "C:\PAM\_en\Accounting"; and "Share path:" with a text box containing "\\VM-NURATIM-002\Accounting". There is an unchecked checkbox labeled "Share the new organization folder in the network". At the bottom, there are four buttons: "Help", "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

Figure 22: Creating an organization folder (folder settings)

6. Click the button **Next >** to continue with the next wizard page. This page shows a preview of the folders and permissions that will be created (see fig. 23).
7. (optional) Click the button **Print** to get a printed report of the folder to be created.
8. Click the button **Finish** to create the new organization folder.

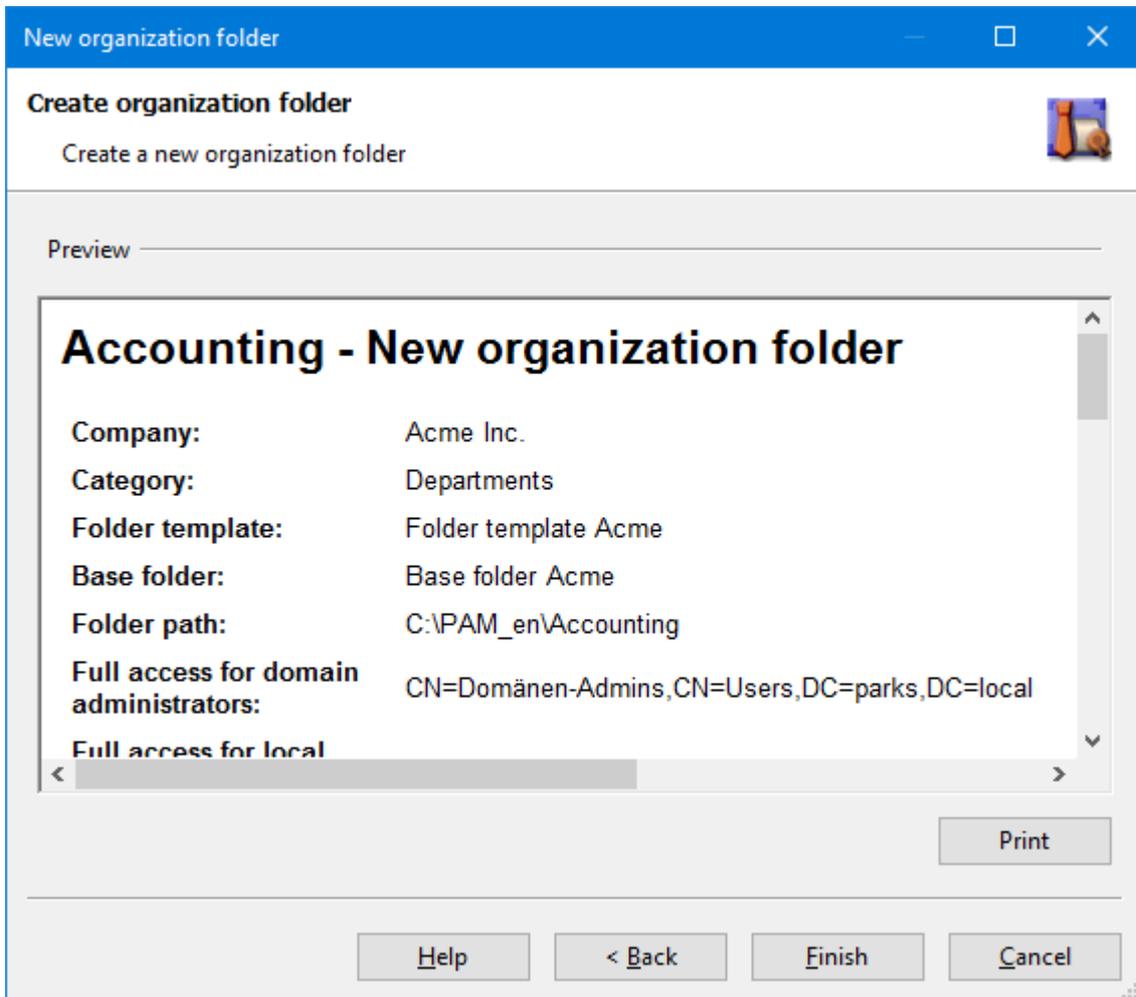


Figure 23: Creating an organization folder (preview)



In this demo programme, the new folder will be created in your folder *My Documents* and can be deleted later without problems.

After the successful creation of the new organization folder the programme creates a new entry in the tree-like organization folder area at the top left of the main window. Click into this tree with the mouse and press the **F6** button to open up the tree.

The new organization folder *Accounting* can now be seen in the tree. Click on to **Permissions** under the organization folder and the programme will show you all permissions in a window on the right side of the main window.

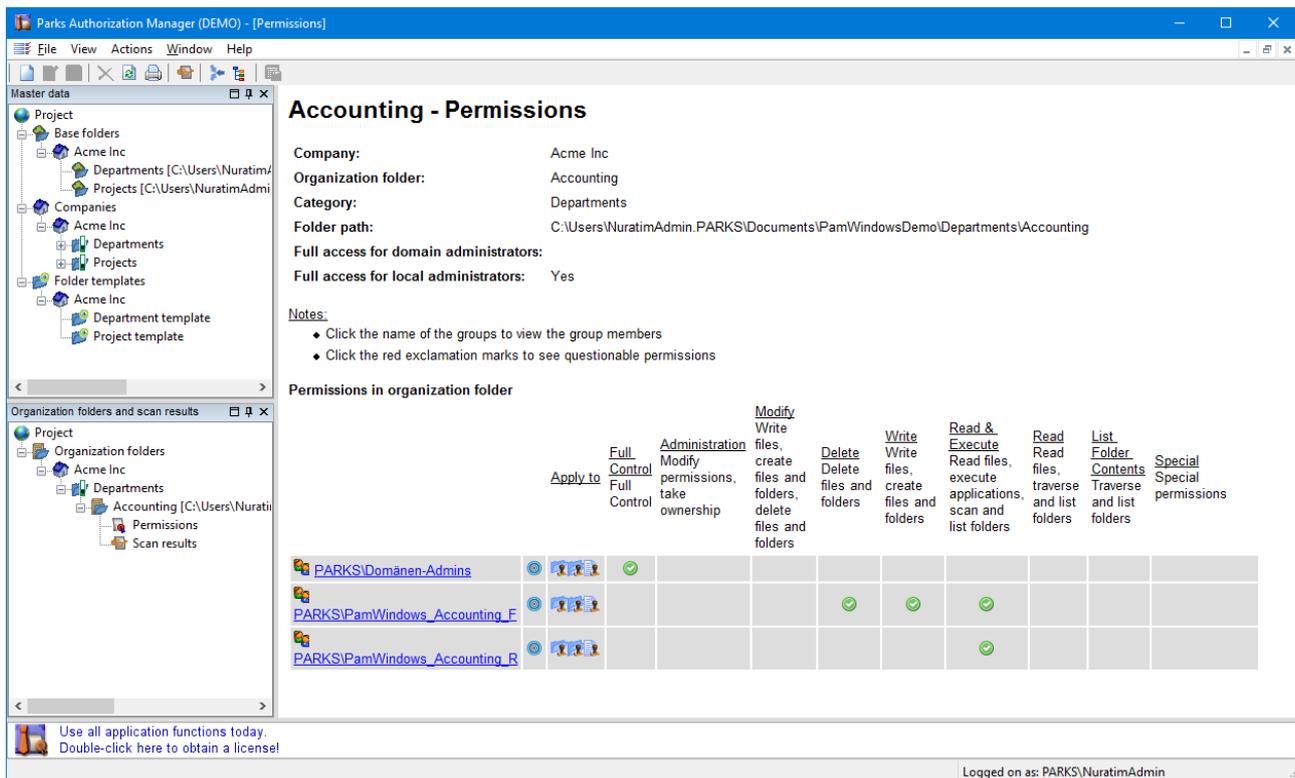


Figure 24: Organization folder permissions

The permission window shows the permissions of each user or group (fig. 24).



By clicking on to a permission group (blue underline) the administrative programme for permission groups is started. Here you can administer the user assignments.

Permissions of the Accounting folder can also be seen in the windows explorer.

With the help of the organization folder assistant departmental or project folders can be easily created without having to make manual settings in Active Directory.

## Editing an organization folder

1. First select the required folder in the **Organization folder** area of the main window.
2. Then click the menu **File | Properties...** to open the organization folder.

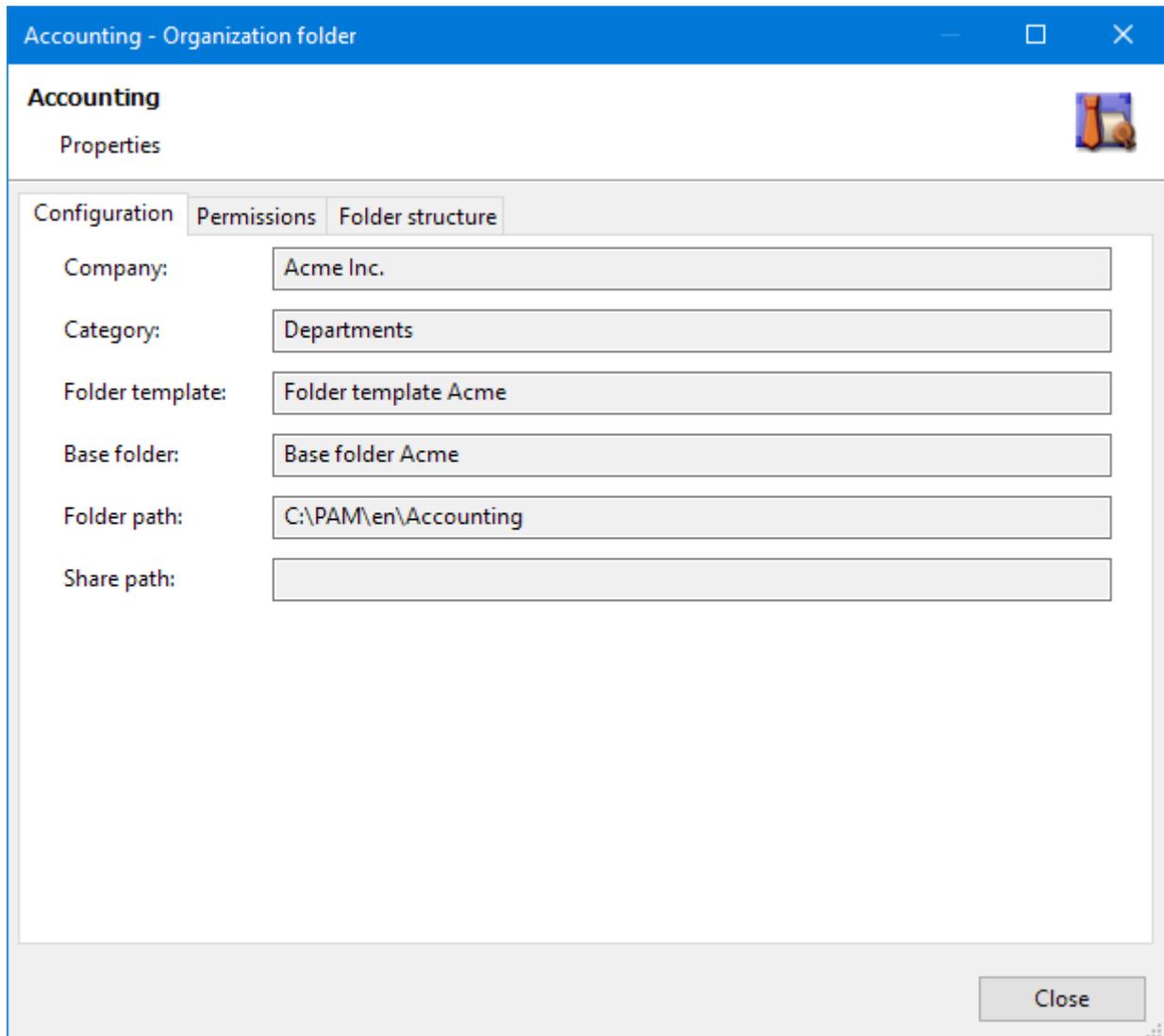


Figure 25: Organization folder

The tab **Configuration** in the dialogue contains the master data of the organization folder (see fig. 25):

- **Company** – the company to which the folder belongs to
- **Category** – the category of the folder
- **Folder template** – the folder template that has been used when creating the folder
- **Base folder** – the base folder in which the organization folder is located
- **Folder path** – the file path of the organization folder
- **Share path** – the network share (optional)

The tab **Permissions** contains the permissions of the organization folder (Figure 26). For each permission there will be an entry in the list with:

- **User group** – the name of the user group
- **Folder path** – the relative path below the organization folder, where the user group is authorized
- **Permissions** – the permissions of the user group in the folder

You can select a user group and click the button **Members...** to view all members of the group (see chapter 2.5.3).

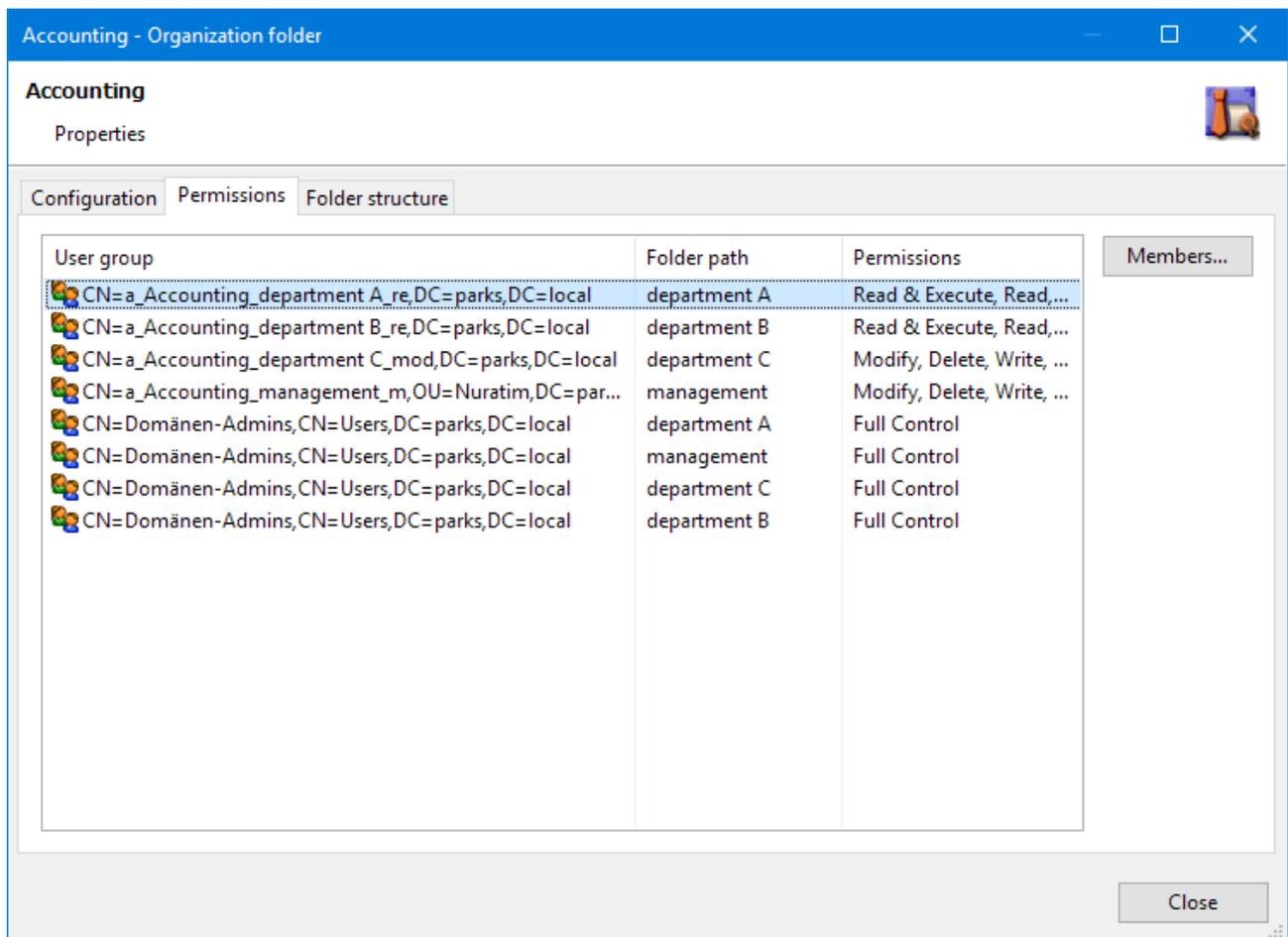


Figure 26: Permissions of an organization folder

In the **Folder structure** tab you see the structure of the directory folders in this organization folder. The folders are displayed in a tree structure, showing their subfolders and coloured either grey (same permissions as the parent directory) or blue (different permissions) depending on the access permissions.

You can use a number of functions to modify the folder structure of the organization folder. For example, you can create process folders (see chapter 2.3) with special authorizations.

You can use the following functions to work with the folder structure:

- **Refresh** – Reloads the folder structure, e.g. after changes
- **New folder...** - Creates a new folder in the selected directory
- **Protected folder...** - Creates a new folder with special permissions in the selected directory (see below)

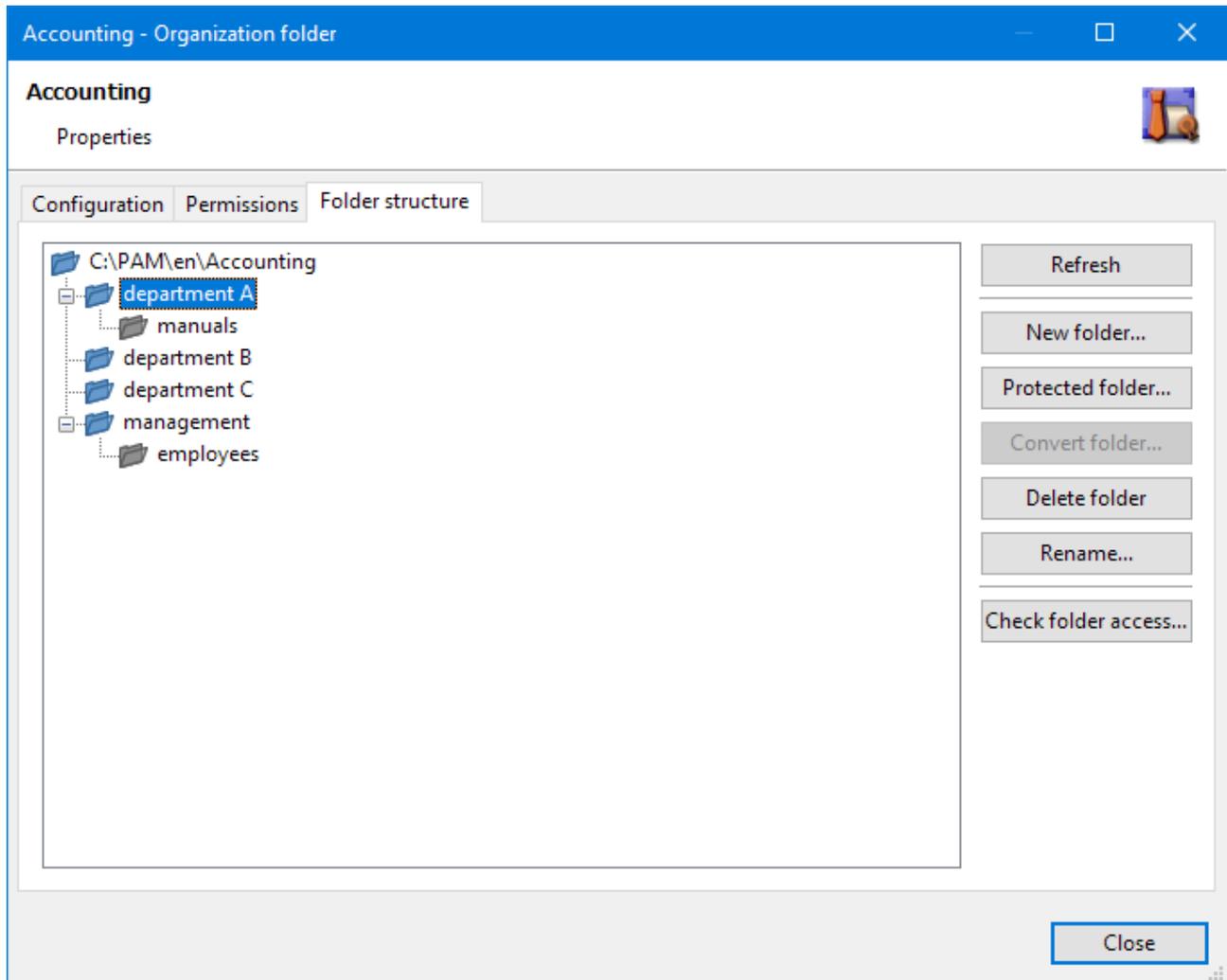


Figure 27: Folder structure of an organization folder

### Create a protected folder

You can create a new folder with special permissions for an existing organizational folder. For this folder, you can select an existing user group to map the permissions, or have the program create a new user group.

If you want to use an existing group:

1. Enter a name for the new folder
2. Select the desired group in the Active Directory
3. Select the appropriate permissions for the group
4. Click **OK** to create the new folder with the desired access rights

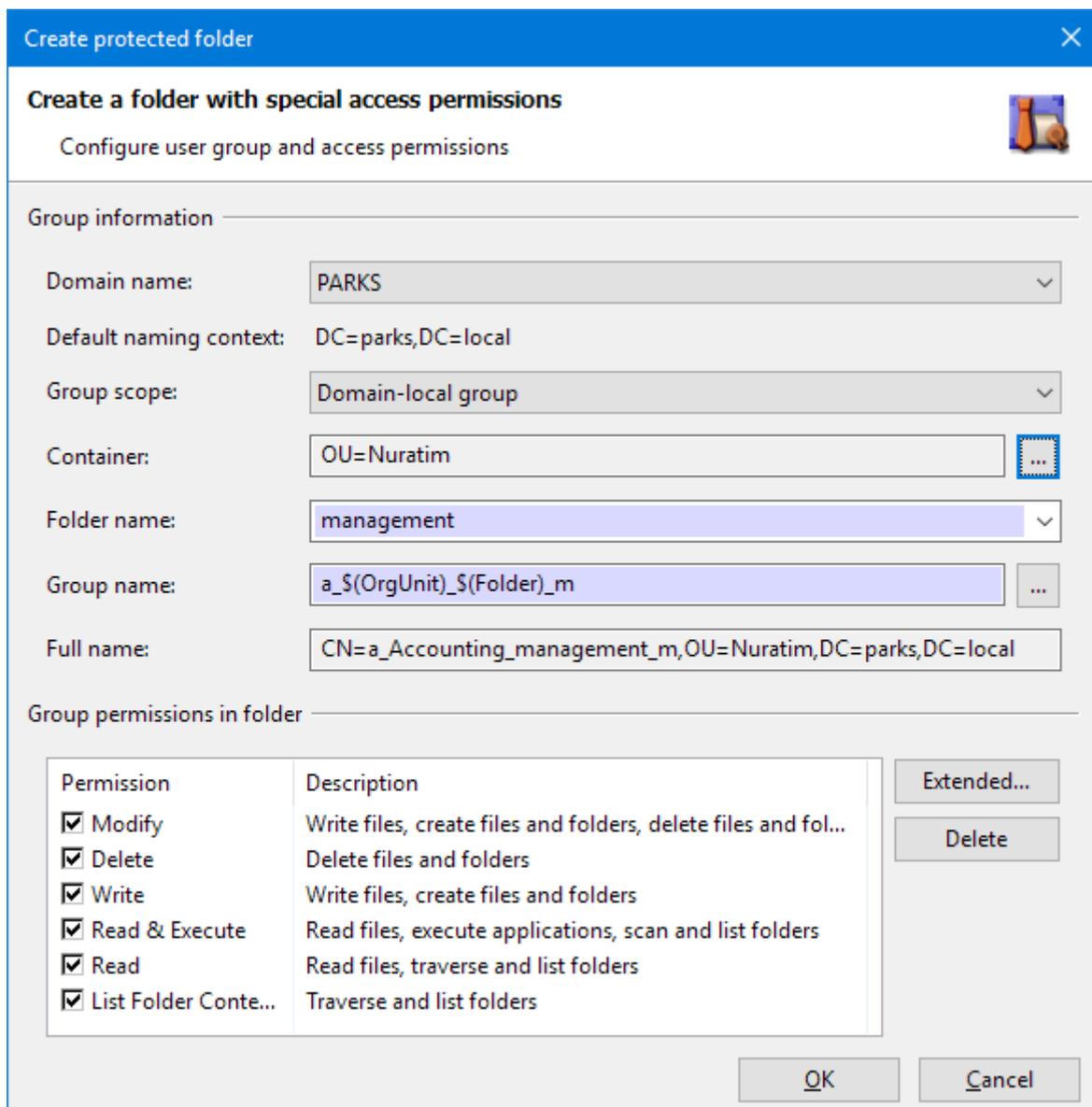


Figure 28: Create protected folder

If you want the program to create a new group:

1. Select the Active Directory domain in which user groups are defined
2. Select the group scope (usually domainlocal)
3. Select the Active Directory container in which the new user group is to be created
4. Enter a name for the new folder
5. Enter the name of the group in your desired naming notation

You can use placeholders for the name of the folder and the selected organizational unit to create a uniform group naming notation. Simply use the placeholders "\$ (OrgUnit)" for the selected organizational unit and "\$ (Folder)" for the name of the folder. The placeholders are replaced by the concrete values in the full name of the group.

6. Select the appropriate permissions for the group
  7. Click **OK** to create the new folder with the desired access rights
- **Convert folder...** - Converts the selected folder into a folder with special permissions
  - **Rename...** - Assigns a new name to the selected folder
  - **Check access...** - Checks whether a specific user has access to the selected folder (see chapter 2.2.4)

### Deleting an organization folder

1. First select the required organization folder under **Organization folders** of the main window.
2. Then click **File | Delete** and confirm the query.

### Analysing the permissions of an organization folder

1. First select the required organization folder under **Organization folders** of the main window.
2. Click the menu **Actions | Scan current permissions...** to start the permission scan (see fig. 29).
3. Execute the permission scan as described in chapter 2.2.1.

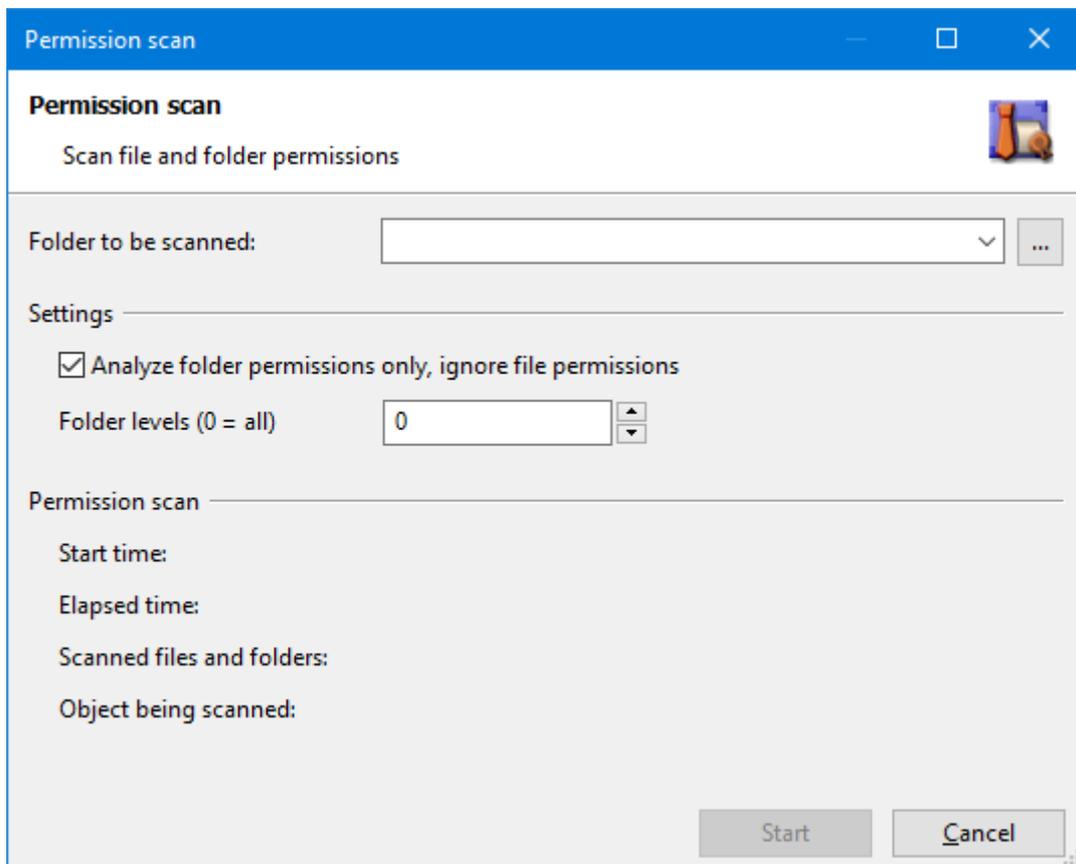


Figure 29: Analysing the permissions of an organization folder

## Importing organization folders

 In the demo version, a maximum of 3 organization folders can be imported. With the licensed version (Parks Authorization Manager for Windows - Professional) you can import any number of organization folders.

You can import existing file system folders as organization folders. If you want to redesign your file system, as an example, you can import your existing folders and analyse their permissions and compare them with your redesigned definitions. During import, PAM reads the folders and permissions of the existing folder without modification.

1. Click the menu **File | Import | Organization folders...** to start the wizard for folder import.
2. On the first page select the company to which the folder belongs to.
3. On the second page of the wizard you define the categories needed for the organization folders. If you select a category here, it will be used as the default category on the configuration page.

If you want to define new categories, just click the **Add** button, enter the name of the category and close the dialog clicking **OK**.

4. Configure the folders to be imported on the next page (Figure 30: Importing organization folders). In the table, enter the organization folder, its category, organization unit and folder path in each row.

Another option is importing the subdirectories of a folder as organization folders. This is useful if you already have directories with e.g. departmental folders. Just click the button **Import...** and select the folder. The subfolders will be added to the table, you just need to add the categories.

- a) **Category:** Select one of the categories defined on page 2 (if not already configured).
- b) **Organization unit:** If there are already organization units defined for the selected category, they will be shown in the list. It is also possible to enter the name of a new organization unit.
- c) **Folder:** Select the folder to be imported as an organization folder by clicking the button ....
- d) **Imported:** No will be shown as an information if you entered the table row data manually. If you imported the folder in the row, Yes will be shown.

Click the button **New entry** to create a new table row. To delete one or more rows, select the rows while holding down the *Ctrl* key and clicking the *category* column, then click **Delete rows**.

After you have finished editing all table rows, you can start the import on the next wizard page.

5. Click **Finish** to start the organization folder import. After successful import, you will see the import statistics.

After the import the new organization folders will be shown in the *Organization folders and scan results* area of the main window. If new categories or organization units have been created, they will be shown in the *Master data* area.

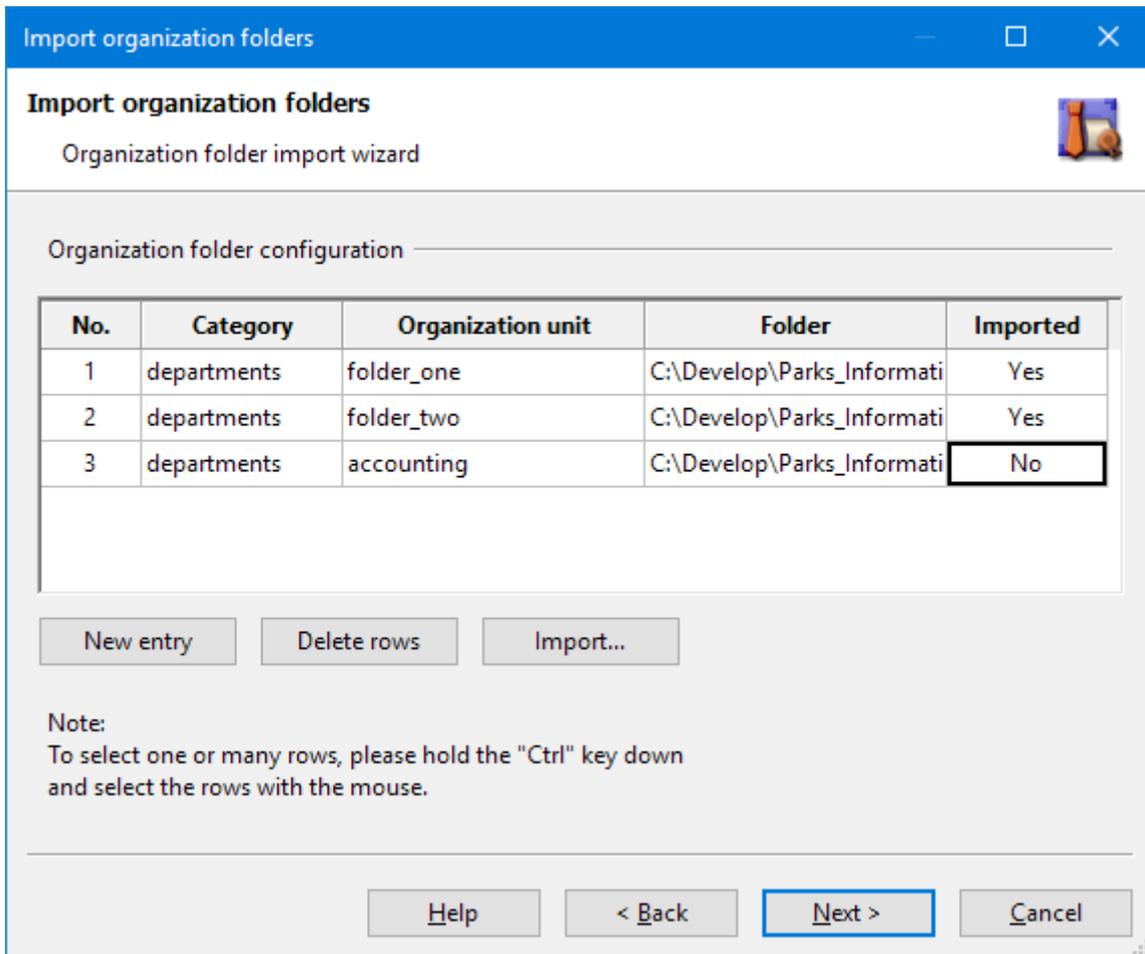


Figure 30: Importing organization folders

## Updating existing organization folders

Chances are that requirements change and existing folder templates have to be modified to meet the current expectations, e.g. a new folder with permissions is needed.

If you have already created organization folders using the template and want to update them to match the new template definitions respectively link new imported organization folders to an existing template:

1. Select the respective folder template in the **Master data** area of the main window.
2. Open the context menu using the right button of the mouse.
3. Click the context menu **Update organization folders...**
4. If you would like to link imported organization folders to an existing folder template activate the option **Use folder template also with imported organization folders**. The imported organization folders will be listed in addition.

5. If you want to see imported organisation folders only, click the button **Select imported organization folders only**.
6. Select all organization folders to be updated in the list (fig. 31).
7. Click the button **Update** to have the file system structure and permissions of the organization folders be updated.

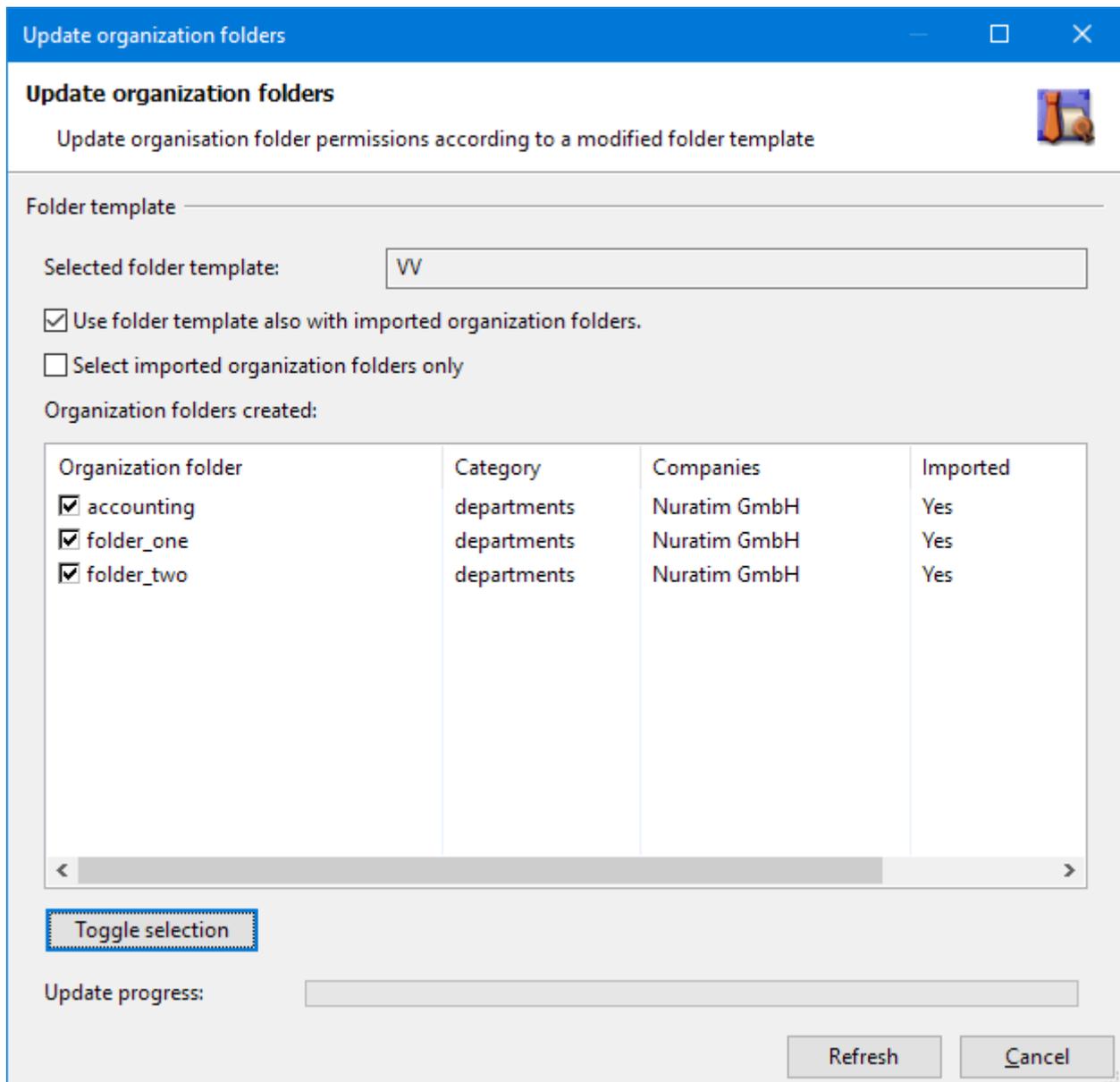


Figure 31: Update organization folders



You can toggle the selected items by clicking **Toggle selection**. If you e.g. want to select all items, do not click all items manually but click **Toggle selection**.

### 2.3.5 Migrating files and folders

The copy function helps you transfer files and folders from one folder into a new folder. If e.g. you set up new organization folders with PAM during a server migration or during a file system reorganization, it is easy to copy the data from the old folder into the new folder.

While doing so you have special options which make life easier compared to the classical copying with the Windows Explorer:

- At the beginning you define both a source folder and a destination folder. Now you can select subfolders out of these folders and copy the files (also recursive). All the copied files are registered during the copying process and at the same time the function ensures that files, which have already been copied, are not copied again at some other stage. This option is referred to as *copy history* in the following paragraphs.

This enables you to restructure complete folder hierarchies safely without having to manually recognise and eliminate duplicates.

- Unwanted file types can be eliminated from the copying process.

You start the copying function via the menu **Actions | Copy files and folders...**, or via the corresponding context menu function by choosing an organization folder.

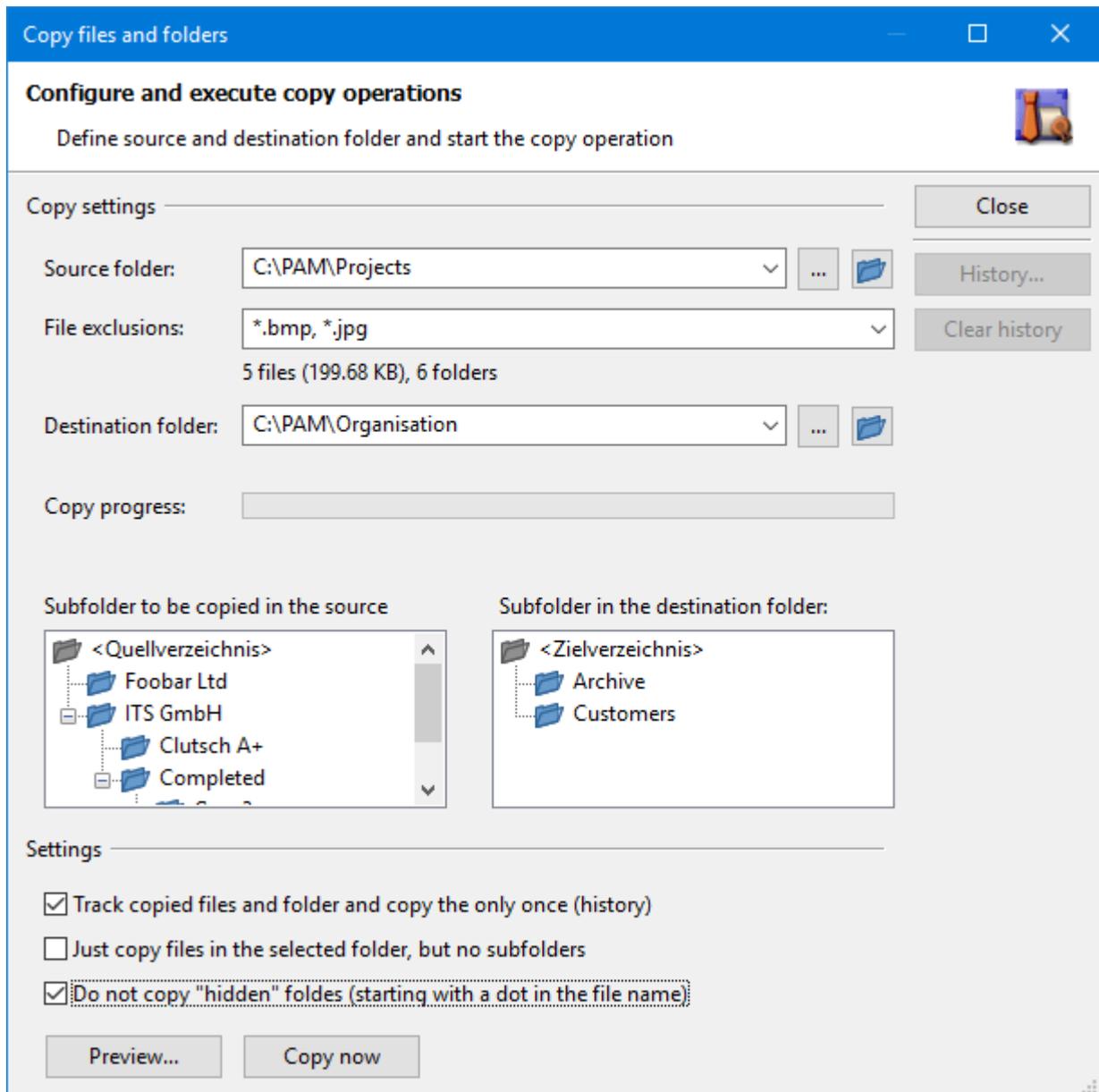


Figure 32: Copy files and folders

To copy files and folders proceed as follows:

1. Enter the source folder or select a folder with the help of the push button „...“. After typing in the name press the Enter button: the programme then analyses the folder structure and shows a statistic of the available file sizes.

**Hint:**

- The folders selected last will be stored in your user settings. These can be shown with the help of the input selection list.

- If you wish to first look at the data in the folders, start the Windows Explorer by clicking the push button with the blue folder icon.
2. (Optional) Enter a sample of the file types you do not wish to copy. You can use the place holder \* in the sample. Several samples are separated with commas.  
**Example:** To avoid copying audio files enter as sample „\*.mp3, \*.wav“  
Then press the enter button again, the programme actualises the statistic.
  3. Enter the destination folder or select a folder with the help of the push button „...“  
The programme has now analysed the folder structure of the source and destination folders and shows these as two trees.
  4. (Optional) Select the subfolders of the source and destination folders in the tree between which the data is to be transferred. If you do not select anything here, then the previously selected source and destination folders will be used.  
**Hint:** If you wish to set up new folders in the destination folder just start the Windows Explorer. Carry out the required operations and then press the input key in the destination folder entry field so that the programme can actualise the folder structure in the tree.
  5. (Optional) If you click the push button **Preview...** the programme will show the files to be copied in advance.
  6. The copy function is started by clicking the push button **Copy now...**
  7. After copying the progress bar in the main window shows you how many files out of the source folder have been transferred into the destination folder. You can now select further subfolders or copy other source folders.

## Start the copy function

When you have configured all copy settings open a new window by clicking the **Copy now...** button, in which you can see and check the current copying process.

 In the demo version, a maximum of 25 files can be copied. With the licensed version (Parks Authorization Manager for Windows - Professional) you can copy any number of folders and files.

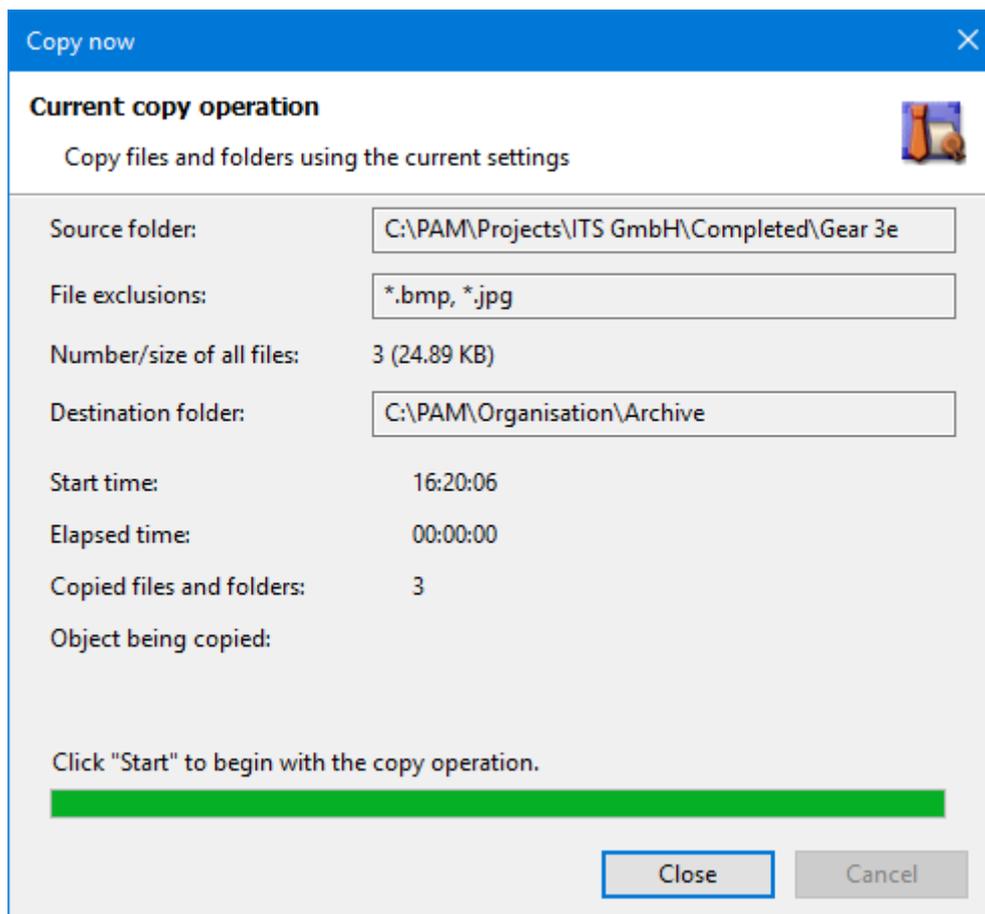


Figure 33: Current copy operation

When all inputs are correct, start the copying process with the help of the **Start** button (not shown in figure above; you can see the **Close** button at the same place. This is automatically activated at the end of each copying process).

During the copying process you can see the start time, the time already needed and the number of copied files.

## Copying options

Various options are available for each copying process:

1. Register copied files and folders and copy them only once (copy history)

If this option is activated the programme registers the files copied and will not copy them again even if the same source folder is selected. This means you have the possibility of newly structuring your folder hierarchy without having to worry about duplicate files.

Further information about the copy history can be found below.

2. Copy only the files in selected folders, but not in subfolders

When you activate this option, the recursive copying of subfolders is turned off. Only the source folder files will be copied.

3. Do not copy “hidden” folders (i.e. with a dot at the beginning of the name)

Internal programme folders, e.g. from version control systems, often have a dot at the beginning. Activate this option to avoid copying such folders.

## Copy preview

You can reach the copy preview by pressing the **Preview...** button in the copy main window.

The copy preview gives you an overview of all the data which will be copied under the current settings. This includes the complete source and destination folders, the excluded files and a statistic. The list shows all files with (relative) sources, destinations and sizes.

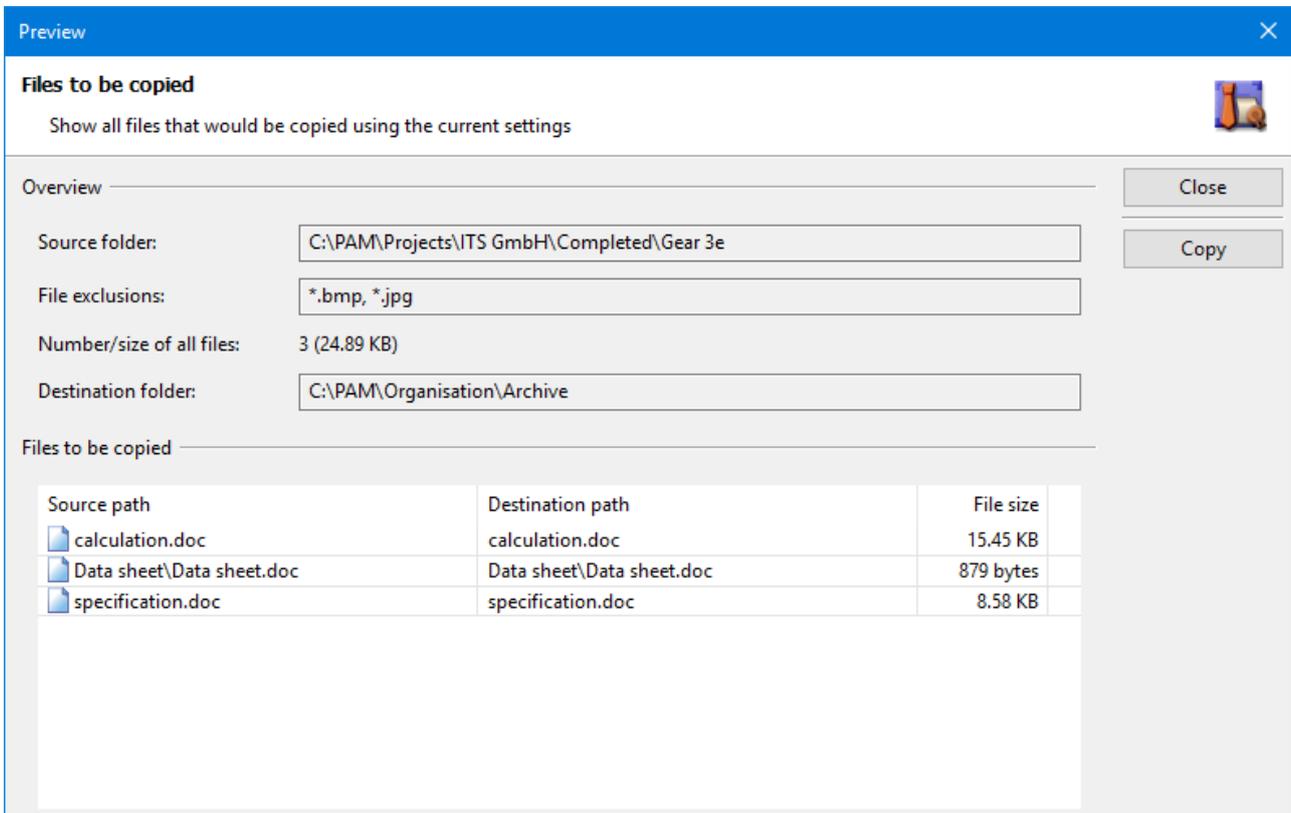


Figure 34: Copy preview

With the **Copy** button the contents of the table can be copied into the clipboard (see below).

## Copy history

The copy history can be opened by pressing the **History...** button in the main copy window.

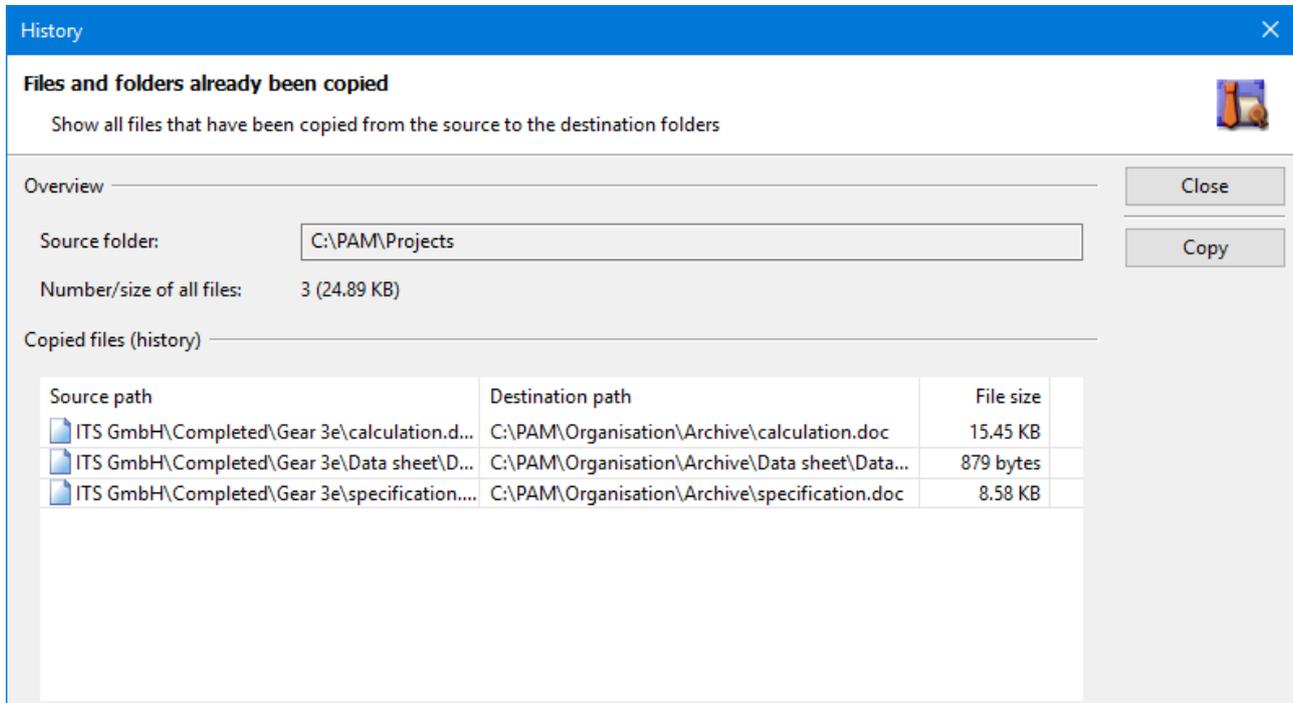


Figure 35: Copy history

The source and destination paths as well as the size of all files copied to date can be seen in the history.

You can reach the copy history only after the first copy process, the button is deactivated up till then.

The contents of the table can be copied into the clipboard with the **Copy** button (see below).



The history is used for one copying process only. A new history is set up as soon as you select a new source file or file exclusions.

The copy history is also erased if you close the copy main window. You can erase the data yourself at any time with the help of the button **Clear history**.

## 2.4 Application settings

Information about projects, databases, categories and network can be found and general configurations carried out in the general programme settings. General programme settings can be reached via **File | Settings...**

### General tab

The project names and descriptions can be changed under the tab **General**. In addition, details about the path and name of the active database are also shown (fig. 36).

The categories needed for the creation of the organization unit can also be extended or deleted here. The following categories are normally pre-installed: Departments, General, Users and Projects. Categories are used to structure organization units.

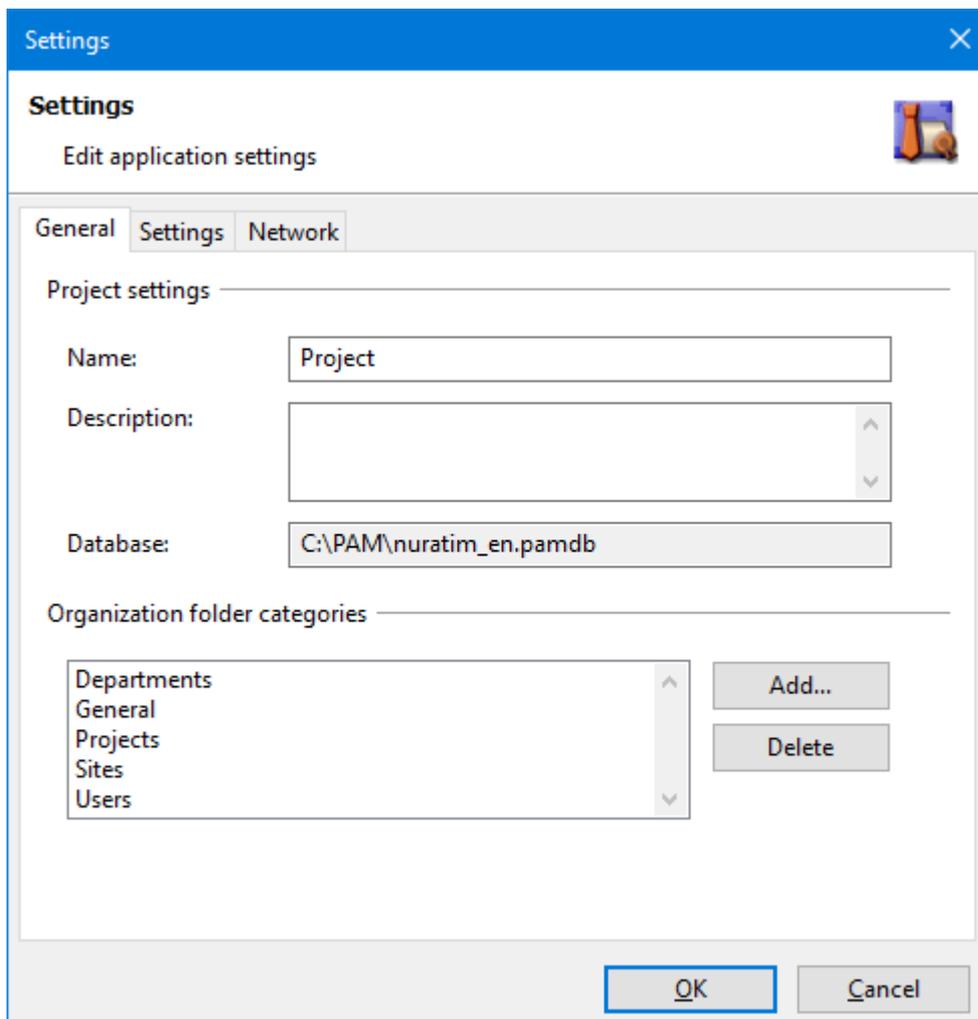


Figure 36: Application settings: tab “General”

Additional categories can be added or existing categories deleted at all times. A new window, in which the name of the category is entered, is opened via the **Add...** button. To delete a category from the database, first select an existing category, then click the **Delete** button and confirm the query.

### Settings tab

It can be determined within the tab **Settings** in which colours the permission differences in the scan result are to be shown (fig. 37). If **Just mark extensions to parent permissions** is selected, then only those folders and files containing **more** permissions than the parent folders will be shown in a different colour.

If **Mark all permission changes** is selected, then all folders and files showing different permissions to the parent folders will be coloured differently.

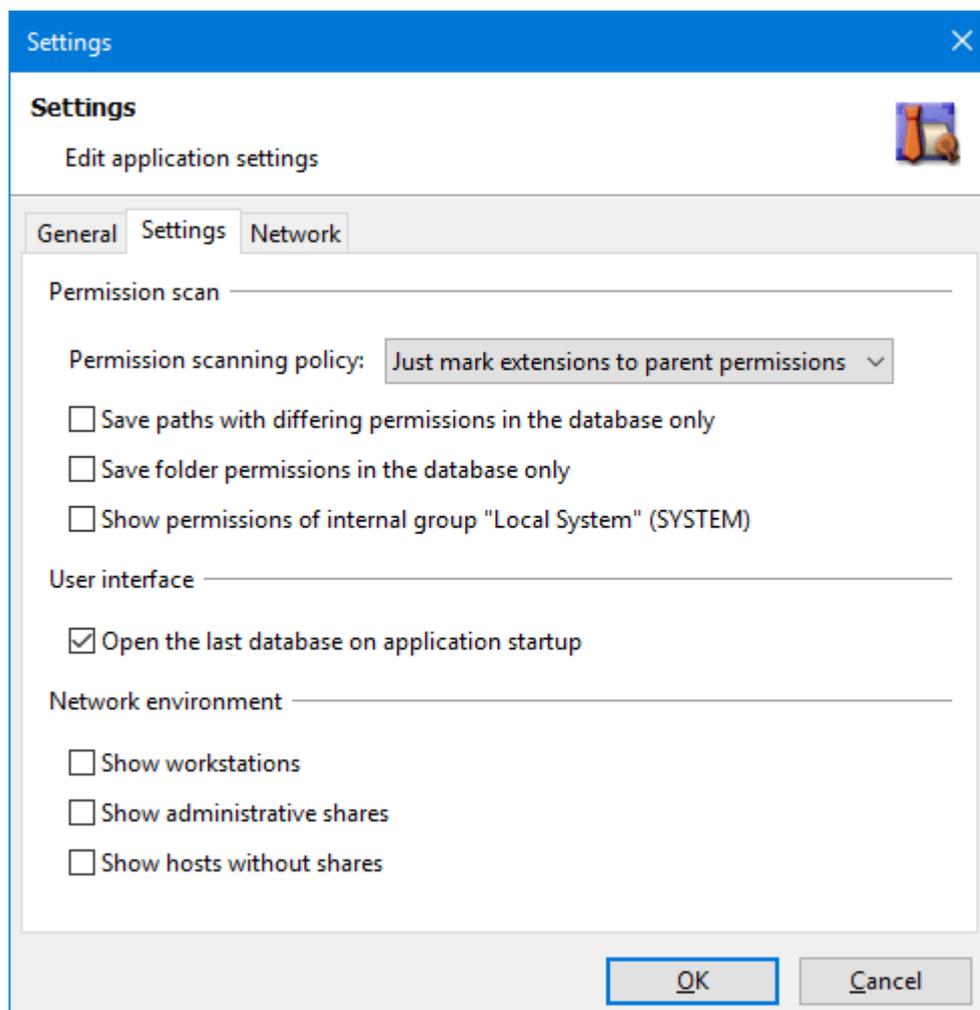


Figure 37: Application settings: tab "Settings"

In addition, the settings for the user interface can also be set. It can be determined whether the database last opened should be automatically opened when the programme is newly started. Otherwise the user must make a connection to an explicit database.

### Network tab

Domain system Information can be seen under the tab **Network**. The domain name, the primary domain server, the computer operating system and the standard name context are displayed.



The standard name context can only be displayed when the Active Directory is available.

In addition, it can also be defined whether a local log-on should be possible if the network resp. the domain server cannot be reached. During a local log-on the user cannot undertake any actions which have an affect on the network. Only actions on the local computer are possible.

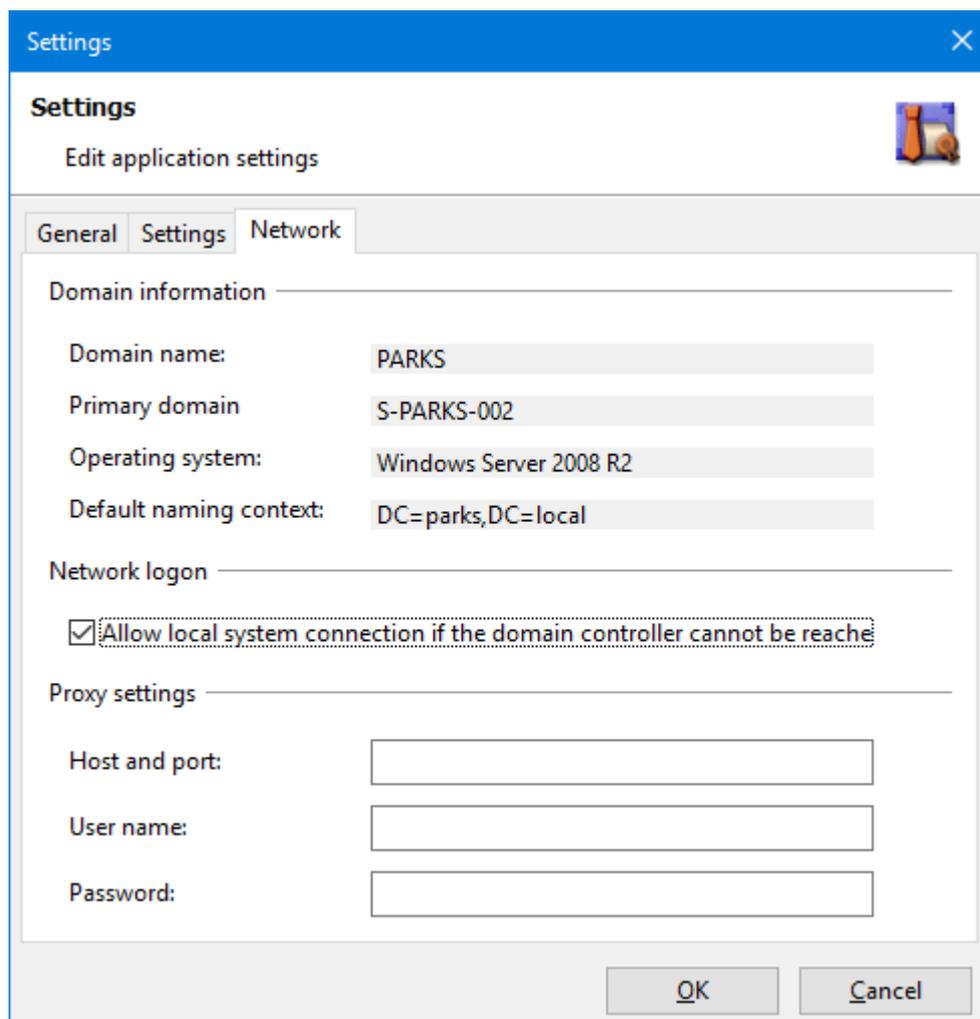


Figure 38: Application settings: tab “Network”

Programme updates can be downloaded into networks without direct access to internet with the help of *Proxy settings*. To do so, the IP-Adress of the proxy server, followed by a colon and the port number must be entered into the text field *Host and port* (e.g. “192.168.1.1:8080”). The

proxy authentication data must be entered in the text control *User name* and *Password* if they are necessary for the proxy access. The password is stored encrypted on the hard disk.

## 2.5 Additional functions

This chapter describes additional functions that are used in multiple places in the programme.

### 2.5.1 Selecting objects in Active Directory

This dialogue is used to select a user group in Active Directory. You can reach this dialogue via the following functionalities:

- base folder: select administration group (domain administrator).
- folder template: select administration group (domain administrator).
- folder template: group name of permission groups
- show effective user groups: select users.
- check access to a folder: select users.

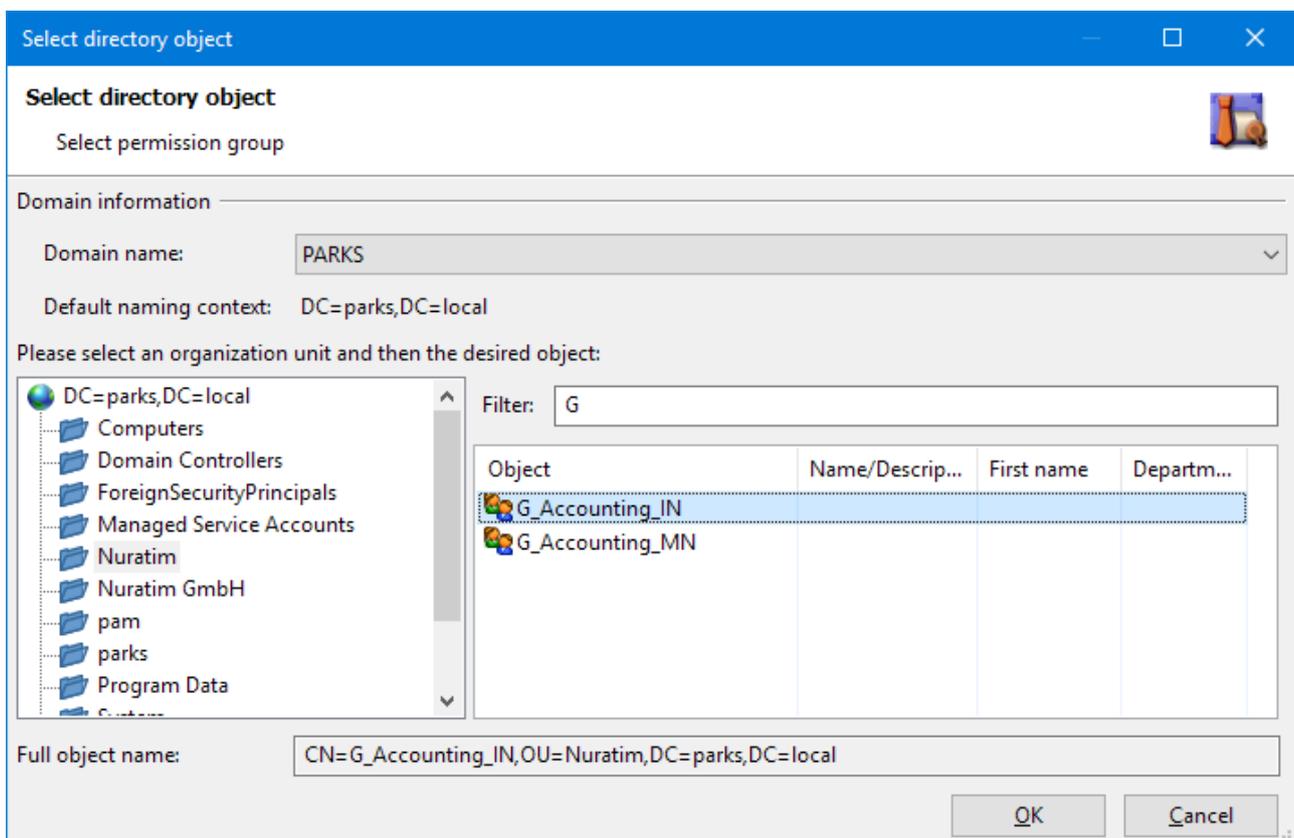


Figure 39: Selecting objects in Active Directory

Proceed as follows to select a user group resp. a folder object in this dialogue (Fig. 39):

1. Select a domain in the field **Domain name**.
2. Select an **Organization unit** in the left window of Active Directory. All objects in this organization unit will be displayed in the right-hand window.
3. Select a user group resp. a folder object in the right-hand window.
4. If the object list is unclear you can enter an object or partial name in the **Filter** field (observe upper case/lower case writing as the filter is case-sensitive). The list will then only show the objects containing this name.
5. The complete object name will be displayed in LDAP spelling in the **Complete object name** field.
6. Click the **OK** button to use the object.

### 2.5.2 Showing the network environment

By clicking the menu **View | Show network environment** you can turn on/turn off the display of computers in your network. You will see the names and descriptions of the server and optionally the workplaces with defined shares.

Click on to the computer or share and open the context menu with the right-hand mouse button. You can e.g. carry out selective permission scans here (see chapter 2.2.1).



The display of the network environment can be adapted to your requirements via programme settings (see chapter 2.4).

### 2.5.3 Showing group members



Adding and deleting members is not possible in the demo version. With the licensed version (Parks Authorization Manager for Windows - Professional) you can add and delete members and groups directly in the Active Directory.

In this dialogue the members of an Active Directory group will be shown hierarchically, i.e. the members of all other groups included will also be shown.

By clicking the **Copy** button the displayed information can be copied into the clipboard (see chapter 2.5.4).

You can filter the result by typing in the **Search (user or group name)**. All hits are displayed in black font. The non-applicable entries are grey. You can also print the group membership (**Print** button) or export it as a PDF report (**Export...** button).

In this dialog you can **add** or **delete** group members directly in the Active Directory to the selected group. When you press the **Add...** button the *Select Directory Object* dialog opens (see chapter 2.5.1). Here you can select groups or users from the Active Directory and assign them to the group.

 In Active Directory, it is not possible to add domain local groups to global groups.

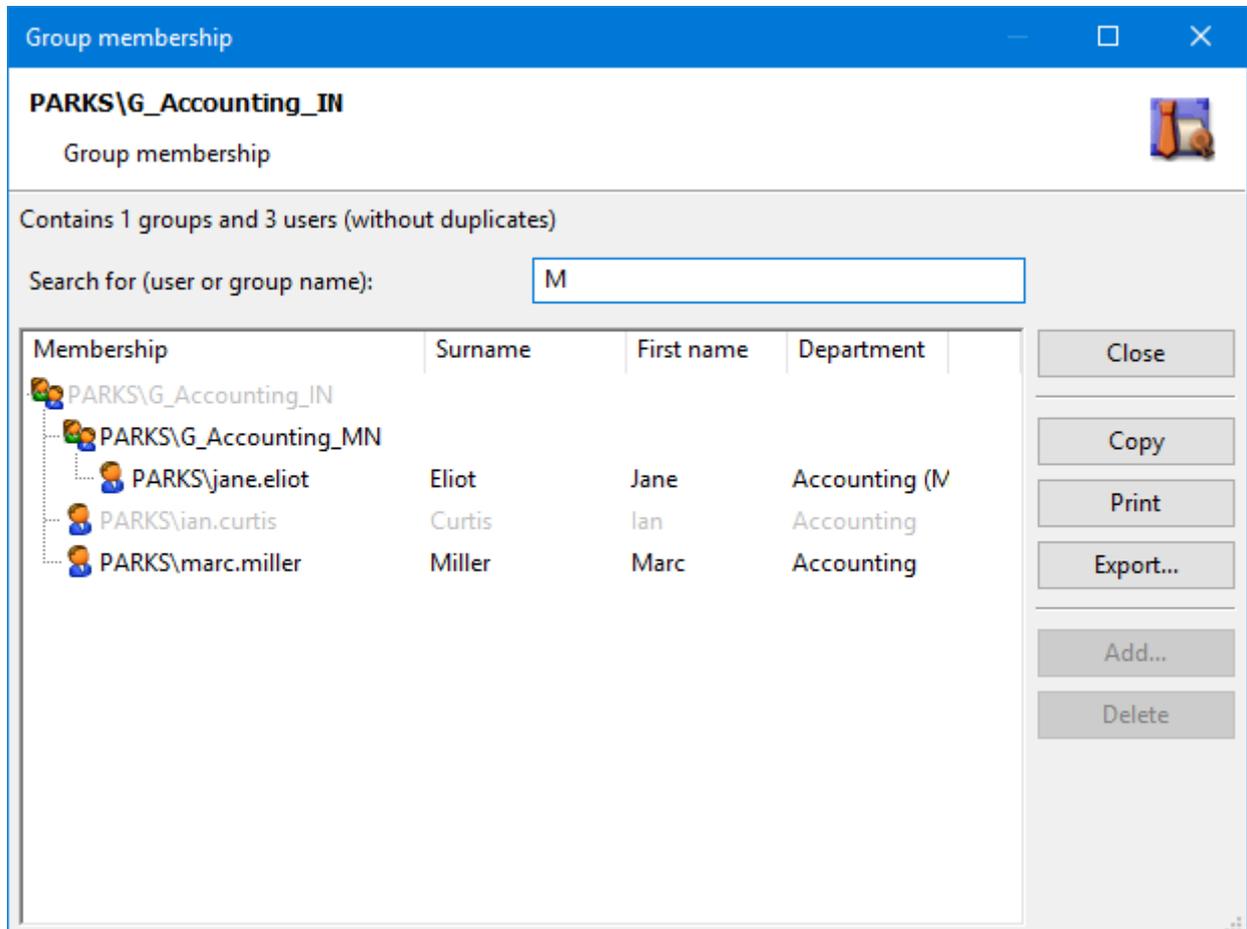


Figure 40: Group membership

## 2.5.4 Working with the clipboard

In various dialogues the displayed contents can be copied into the clipboard by clicking the **Copy** button. The data format is described in the corresponding dialogue descriptions of this manual.

After copying, the clipboard always contains two formats: text data in CSV format, which you can copy into the text editor, and a formatted table in HTML format for word processing programme.



Depending on the target programme settings, it is not enough to use the key combination **Ctrl+V** to insert, you must use the function “**Insert Contents**”, with which you can select the required format in the clipboard. Some programmes allow the configuration of the preferred insertion format (text or HTML) in the settings.

## 2.6 Conclusion

We hope we have been able to give you a first impression of the productivity of our product Parks Authorization Manager (PAM) with this manual and we would be very pleased to welcome you as a customer in the near future.

Further information about the product can be found on our homepage in Internet under <http://www.parks-informatik.de/pam>

## 3 Appendix

### 3.1 Frequently asked questions

#### 3.1.1 No connection drives in file dialogues

If the user account control (UAC) is active in Windows, you are working, even as an administrative user, with two so called tokens. The token with restricted rights will be active during logon and also when connecting network drives. All connected drives are therefore connected with the restricted token.

When PAM is started as an “elevated application” (blue UAC dialog), Windows will switch to the administrative token, which does not have any information about connected network drives.

**Solution:**

1. Use UNC path notation to access network drives in PAM.
2. Modify the registry or use a group policy to have connected drives be available also in “elevated mode”.

### 3.2 Uninstalling Parks Authorization Manager

Please use our Uninstallation programme to remove the programme – this can be reached via **Control Panel | Software**.

The programme can also be removed via **Start | Program Files | Parks Authorization Manager (Demo) | Uninstall Parks Authorization Manager (Demo)**.

The created sample folders can be found under your **My Documents** folder. Here please delete the folder **PamWindowsDemo**.

If organization folders have been created by following these instructions, then the permission groups created by the programme must also be deleted. To do so, delete all groups with the prefix *PamWindows* from the Active Directory.