



# PERMISSION ANALYZER

## Quick Start

*Protect your data and get in control!*

*Scan your network, filter NTFS permissions,*

*validate your access control design*

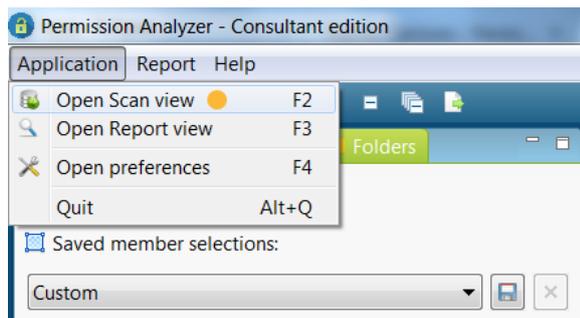
*and trace user or group access.*

## SCANNING THE NETWORK

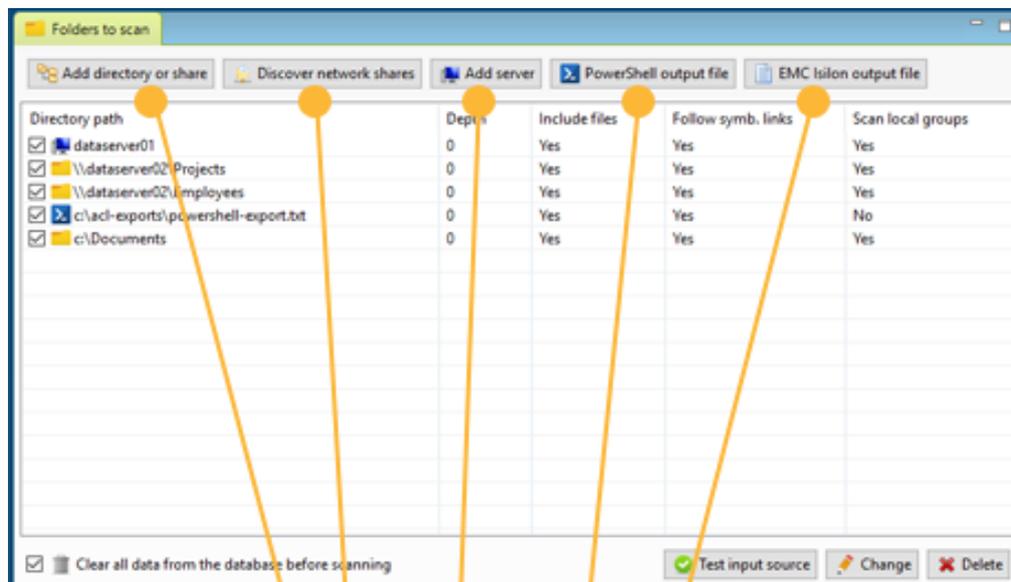


Permission Analyzer has two key functionalities: network scanning and overview creation. During the scanning process, all necessary information is stored in the corresponding local database.

### Adding directories



Open **Scan View** via the menu and determine which directories and LDAP Organizational Units (OU) need to be scanned by Permission Analyzer. LDAP OU's are used to supplement user data from the ACL with a username and nested group information.



Add particular network shares or local directories to scan. Or scan all network shares by adding a server or let PowerShell do the scanning and import the results from a txt file

## Scanning Active Directory OU's

Permission Analyzer will automatically detect your domain and Active Directory connection and will ask for a username and password to read information from the AD. Open the application **preferences** to add more LDAP connections, such as various domain controllers or a global catalog. The default connection will use a bind user to read information from the Active Directory. The application asks for a username and password during the scan, which can be saved encrypted in the application preferences.

LDAP connection	LDAP base container	Search scope	Object types
<input checked="" type="checkbox"/> Global Catalog	CN=Dev,OU=Distribution Groups,DC=gp,DC=gl,DC=...	Container and sub containers	Users and groups
<input checked="" type="checkbox"/> Primary domain controller	OU=Management,DC=mydomain,DC=com	Container and sub containers	Users and groups

## Starting scan

Permission Analyzer will refresh the database with the current network statistics when a scan is initiated. Only items that are **checked** will be scanned by Permission Analyzer. A scan may be initiated automatically by the application using the **-scan** startup parameter. The application will then commence a scan with the current configurations and subsequently close. An LDAP or directory scan may be initiated using the **-scanLDAP** or **-scanDirectories** parameters.

## FILTERS AND OVERVIEWS



Create filters and include or exclude particular members, simple or special permissions and folders or files. Save your filters as Selection or save and re-use them as report.



The simplest filter displays the permission privileges for a specific group or user (hereafter to be referred to as **member**). The filter takes into account the nested group membership of the selected member.

It is possible to select a group from which all members are included or excluded in the overview. Simply add a specific group or LDAP OU in the **All members from group or OU** section. This will not filter for the group itself but for **all** the members of that group. Nested group membership will automatically be taken into account for each group member when determining permissions. This will allow you to monitor whether someone from a specific group has too many permission privileges in certain folders.

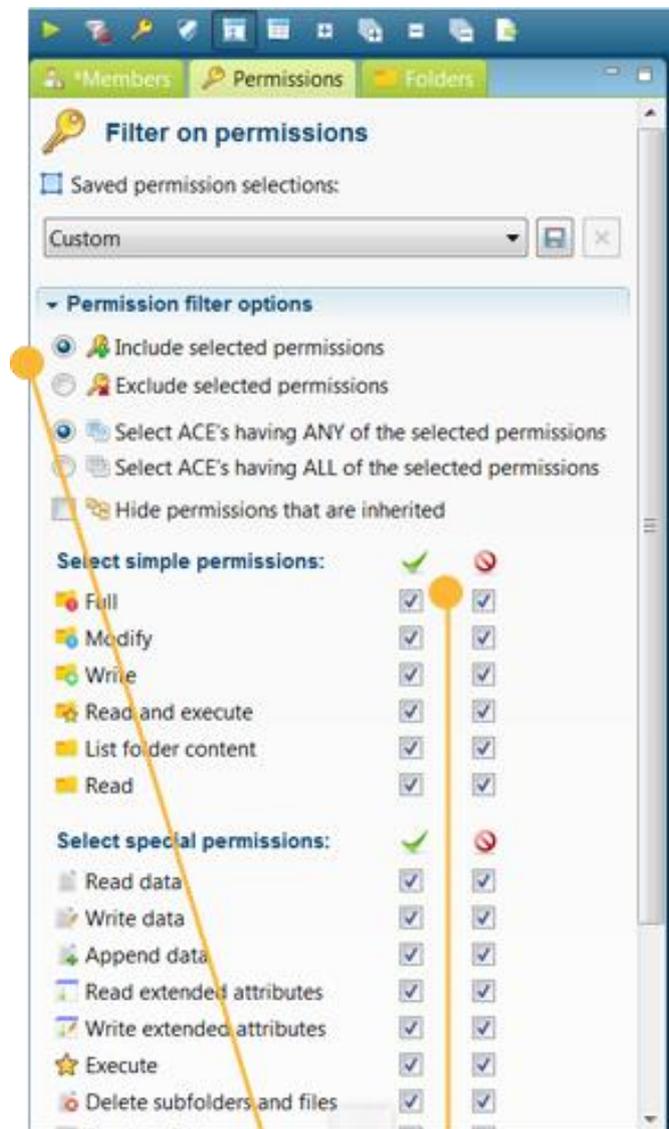
In addition to including members in searches, you are also able to **exclude** one or more members from searches, e.g. by excluding everyone from the Domain Admins group.

## Filtering for permission privileges

All permission privileges are automatically shown for each search. However, a filter can be created to **include** or **exclude** certain privileges from a search. The filter overview distinguishes between Windows simple permissions, special permissions or permissions that allow or deny something.

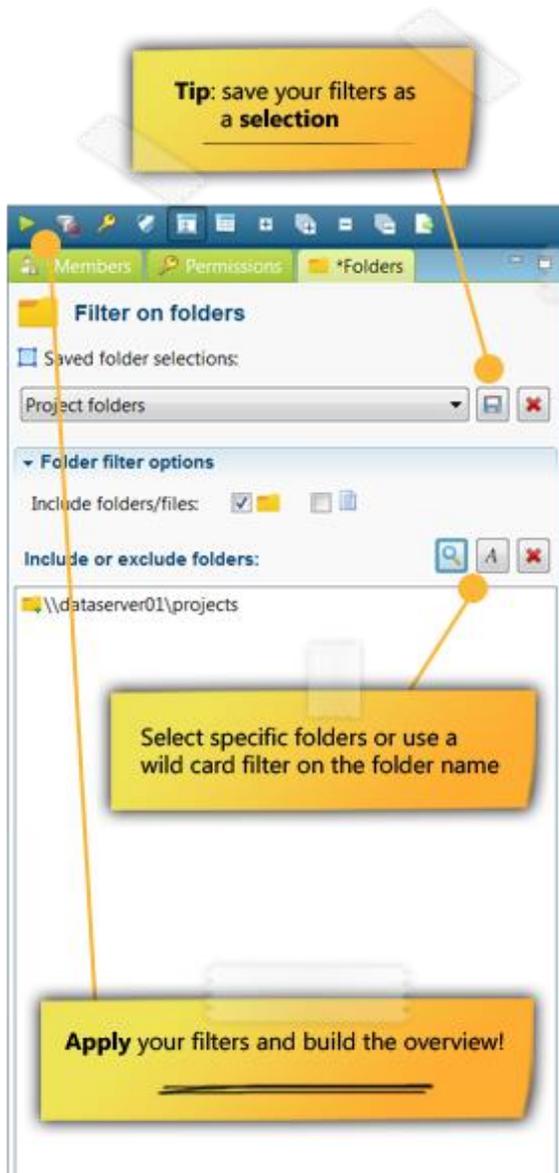
When filtering permission privileges you can indicate whether a member should have **all** privileges or **at least one** of those you have selected. The former can be used to filter for members with specific permissions (such as FULL), while the latter can be used to display a series of permissions.

If necessary, configure the filter to only display **explicit** permissions.



Select the 'allow' and/or 'deny' permissions that you want to include or exclude.

## Filtering for directories and files



Search results can be scoped to exclude certain directories or files. Adding a directory will automatically include all subdirectories and files. You will also be able to search for the name of a file or directory using a wildcard.

**Tip:** To retrieve a directory or file in the main window, use the Quick File Search box.



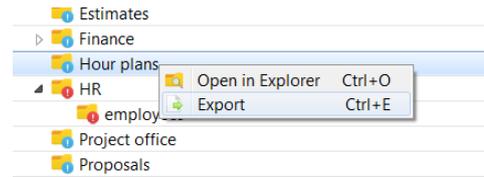
A set of filters can be saved as a **Selection**, making a large number of frequently used filters easily retrievable and usable. A selection will bundle filters of the same type (members, permissions or folders). The total number of filters for an overview can be saved as a Report.

Apply your filters by pressing the Run

## Overview of permissions

After applying the filters, all retrieved permissions will be shown in a tree structure, grouped in directories and files. Each item will contain a label with the relevant permission and a number of columns showing which special permissions apply e.g. permissions of various members, as each row is a sum of all retrieved permissions. The background color of the permissions indicates whether a permission was granted directly or if it was inherited from a folder above: white for implicit 'allow' permissions, green for explicit 'allow' permissions, light red for implicit 'deny' permissions and dark red for explicit 'deny' permissions.

**Tip:** Each directory within the search results can be exported to an HTML report or CSV file by opening the context menu with the right mouse button. Directories can also be opened directly with **Windows Explorer**.



There are four tabs at the bottom of the search result screen: one which allows you to zoom in on a directory to review which permissions and members have been found including their effective and inherited permissions, one that provides details on the Access Control List of the directory selected, one that shows the provenance of permissions for a particular member and another tab which allows you to retrieve all users and groups from the overview including all their explicit permissions.

The file tree displays an aggregated view of all the permissions that match the filter. It shows a label with the relevant permission and a number of columns showing which special permissions apply e.g. permissions of various members, as each row is a sum of all retrieved permissions. Use the tabs at the bottom of the screen to view more details on the selected directory or file.

Path	Permission	Special Permissions
\\dataserver01\data	Read and execute	...
Archive	Read and execute	...
Clients	Read and execute	...
Departments	Read and execute	...
Employees	Read and execute	...
Finance	None	...
2015	None	...
Projects	None	...
Results	None	...
Clients	None	...
MCE Hospital	Modify	...
Trade Bank LC	Read and execute	...
E-mail proposal.bt	Read and execute	...
Evaluation.docx	Read and execute	...
Notes 20150608.docx	Read and execute	...
Notes 20150714.docx	Read and execute	...
Notes 20150829.docx	Read and execute	...
Profits.xlsx	Read and execute	...
Proposal.pdf	Read and execute	...
results.zip	Read and execute	...
Screenshot.png	Read and execute	...
2016	None	...
Offerings	None	...
IT Solutions	Modify	...

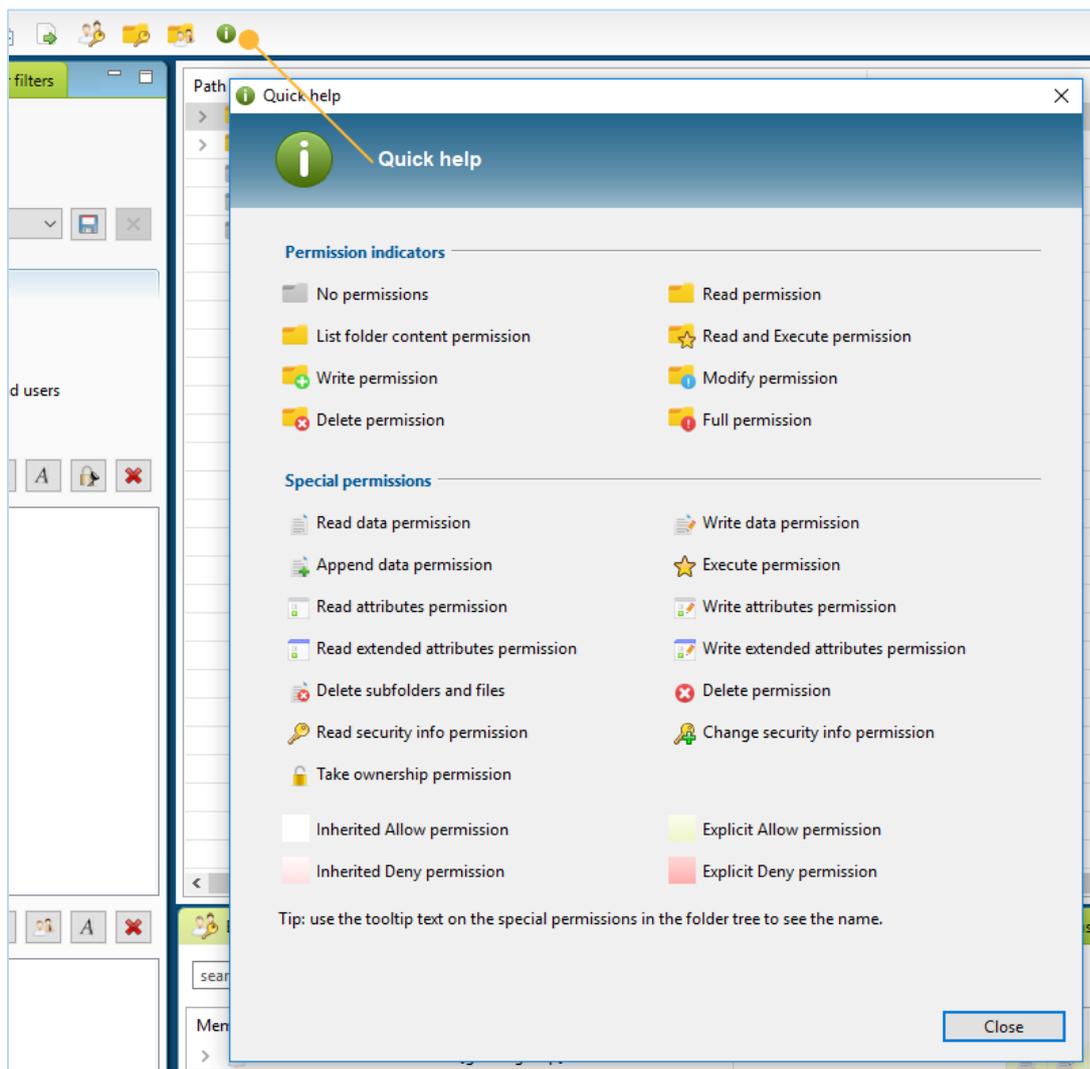
**Effective permissions** | **ACL on the file system** | **Trace the origin of permissions** | **All matching users and groups** |  Apply filter on the list

This tab displays all the members that are found on the selected file. For each member, the effective permissions are displayed and unfolding a member will display all the applicable explicit Access Control Entries and (if applicable) members of a group. To view the inherited permissions for a particular user or group, you can put a member in the Trace tab using the context menu.

Member	Permission	Inheritance flags	From folder
TESTDOMAIN\PWaxman	Modify		
TESTDOMAIN\Domain Users [global group]	Read and execute (n...	This folder, subfold...	\\dataserver01\data
TESTDOMAIN\Consultants [global group]	Modify	This folder, subfold...	MCE Hospital
TESTDOMAIN\RRounthwaite	Modify		
TESTDOMAIN\SPurcell	Modify		
TESTDOMAIN\SShridhar	Modify		

The folder tree should make it clear at a glance where the unwanted rights are and what rights are granted explicitly. The tree shows all rights per directory, initially this will mainly be FULL rights of the Administrators, but as more filters are applied, the tree will show the purposeful rights. The icon for the directory indicates which access right it involves. Press the green info icon in the toolbar to quickly get an overview of icons.

The icons to the right of the directories indicate which special rights apply to the directory (a summation of all Access Control Entries on the directory that match the filter criteria). The background color indicates whether these special rights are inherited from a parent folder (white background), or directly assigned to the directory (green background). A red background indicates a 'Deny' right.



## REPORTS AND EXPORT



*Save your filters as report and export them to HTML or CSV and e-mail. Use different report types, such as permissions tracing and group memberships, effective permissions or plain Access Control List information of your directories.*

Current sets of filters can be saved as a new report using the menu [Report] > [Create new report]. Reports can be exported to **HTML** or **CSV** files or can be reloaded within the program to change the filters or review results.

**Create a new report**

If you have selected a filter selection as a filter, then that selection will show up as an option when creating the report. Using the selection will create a reference to the filter selection within the report and any modifications to the filter selection will result in all reports automatically applying the modified selection. Unchecking the option in the report will result in the report saving a copy of the filters and not change according to the filter selection.

Report name:

Report description:

Report type:

Expand groups:  Do not expand  Expand direct memberships  Expand nested memberships

File type:   Use simple presentation

Target file path:

Custom template path:

E-mail recipient:

Link to filter sets: No filter sets have been selected

**Filters for this report:**

<input checked="" type="checkbox"/>	Include (nested) group membership
<input checked="" type="checkbox"/>	Include member TESTDOMAIN\Product designers [global group]
<input checked="" type="checkbox"/>	Include member TESTDOMAIN\Sales [global group]
<input checked="" type="checkbox"/>	Include member TESTDOMAIN\Intranet Admins [global group]
<input checked="" type="checkbox"/>	Include all members from the group TESTDOMAIN\Freelancers [global group]
<input checked="" type="checkbox"/>	Include member TESTDOMAIN\Intranet Developers [global group]
<input checked="" type="checkbox"/>	Include member TESTDOMAIN\Freelancers [global group]
<input checked="" type="checkbox"/>	Include folder \\dataserver01\projects
<input checked="" type="checkbox"/>	Include folder \\dataserver01\data

### Report types

Permission Analyzer supports nine report types, each of which displays search results differently:

- **Folders/files** and the sum of their permissions
- **Folders/files** and all users with their effective permissions

- **Folders/files** and their Access Control List, like Windows Explorer
- **Folders/files** and the ACL with expanded groups showing direct members and their effective permissions
- **Folders/files** and the ACL with expanded groups showing nested members and their effective permissions
- **Users and groups** and all their explicit permissions. This report is laid down per user/group instead of directory/file. For each user or group the directories and explicit rights are displayed, including permissions from nested group memberships.
- **Groups** that match the filter criteria and their direct members
- **Groups** that match the filter criteria and their nested members
- **Groups** that have permissions in the folder tree and their direct members
- **Groups** that have permissions in the folder tree and their nested members
- **Users** that match the filter criteria and their direct group memberships
- **Users** that match the filter criteria and their nested group memberships

Some reports show a relatively extensive amount of information per user and group. That's why we recommend making your filters as specific and targeted as possible, to exclude any unnecessary information. This prevents reports from being crowded with irrelevant information.

**Tip:** put a placeholder in the *Target file path* to include the current date in the path `c:\permission reports\[date:yyyy-MM-dd]_report.html`. This will preserve old report files. See [Java date formats](#).

## E-mail

A report can be configured with an e-mail address, allowing it to be sent to that address at every export opportunity. An **SMTP** server, however, must be configured to accommodate the address and can be set up in the application settings. The option will also allow you to indicate whether you want the report to be included as an **attachment** and to include a message in the e-mail. The e-mail template may contain the following fields: `[report_name]`, `[report_path]`, `[report_description]` and `[report_threshold]`.

## Running reports automatically

Use Permission Analyzer to run reports automatically using the following parameters:

- **-report "myReport" "myReport2"**: run one or more reports by name.
- **-allReports**: run all reports.

Permission Analyzer will close automatically after all reports have been exported.

See [Scheduling jobs](#) feature for more command-line options.

## EXAMPLE: FOLDERS/FILES AND THEIR ACCESS CONTROL LIST

Instead of adding up all the rights, Access Control Entries are displayed separately per directory or file in this report. It provides an overview of the Access Control List (ACL) per directory or file and contains all Access Control Entries (ACE) that match the search criteria. Each ACE has a set of permissions and a member and match the data in the **Windows Security tab** on the file properties. Only the directories and files that match the search criteria will be included in the report.

**PERMISSION ANALYZER - ACL REPORT** Report date: 12 september 2017 20:35  
Directories and files found: 9

The ACL report displays permission information that corresponds with the Access Control Lists on the file system. Only the members that match the selected filter criteria are displayed in the report.

**Filters applied:**

- include (nested) group membership
- include member TESTDOMAIN\Rudy Owen [Rudy Owen]
- hide permissions that are inherited from a parent folder
- include folder %dataserver0\projects

**Column visibility:**

- File path
- Members
- Permission text
- Special permission
- ACE flags
- Inherited from folder

Show 50 entries Search

Member	Permission	ACE flags
%dataserver0\projects\Applications (1 member) (TESTDOMAIN\Clayton) (Inherit ACL: yes)	Read and execute (explicit)	This folder, subfolders and files
%dataserver0\projects\Applications\Deployment artifacts (1 member) (TESTDOMAIN\Clayton) (Inherit ACL: yes)	Modify (explicit)	This folder, subfolders and files
%dataserver0\projects\Applications\Planning (1 member) (TESTDOMAIN\Clayton) (Inherit ACL: yes)	Modify (explicit)	This folder, subfolders and files
%dataserver0\projects\Applications\Proposals\2015\EX Insurances (1 member) (TESTDOMAIN\Clayton) (Inherit ACL: yes)	Read and execute (explicit)	This folder, subfolders and files
%dataserver0\projects\Applications\Source (1 member) (TESTDOMAIN\Clayton) (Inherit ACL: yes)	Modify (explicit)	This folder, subfolders and files
%dataserver0\projects\Applications\Technical designs (1 member) (TESTDOMAIN\Clayton) (Inherit ACL: yes)	Modify (explicit)	This folder, subfolders and files

## EXAMPLE: USERS AND GROUPS AND ALL THEIR EXPLICIT PERMISSIONS

This report is laid down per user/group instead of directory/file. For each user or group the directories and explicit rights are displayed. It displays all explicit permissions, including permissions from nested group memberships. The column **Via ACL member** shows the origin of permissions per group or user, indicating through which (nested) group a user or group has inherited those permissions. Only users and groups that appear in the search results will be included in the report. This report shows a relatively extensive amount of information per user and group. That's why we recommend making your filters as specific and targeted as possible, to exclude any unnecessary information. This prevents reports from being crowded with irrelevant information.

PERMISSION ANALYZER - EXPLICIT PERMISSIONS BY MEMBERS REPORT Report date: 16 september 2017 14:14  
Members found: 4

The user/group permission report displays explicit permissions ordered by user or group. Only the users, groups and permissions that match the selected filter criteria are displayed in the report.

**Filters applied:**

- Include (nested) group membership
- Include all members from the group TESTDOMAIN\Consultants [global group]
- Only include folders
- Include folder \dataserver01\data

**Column visibility:**

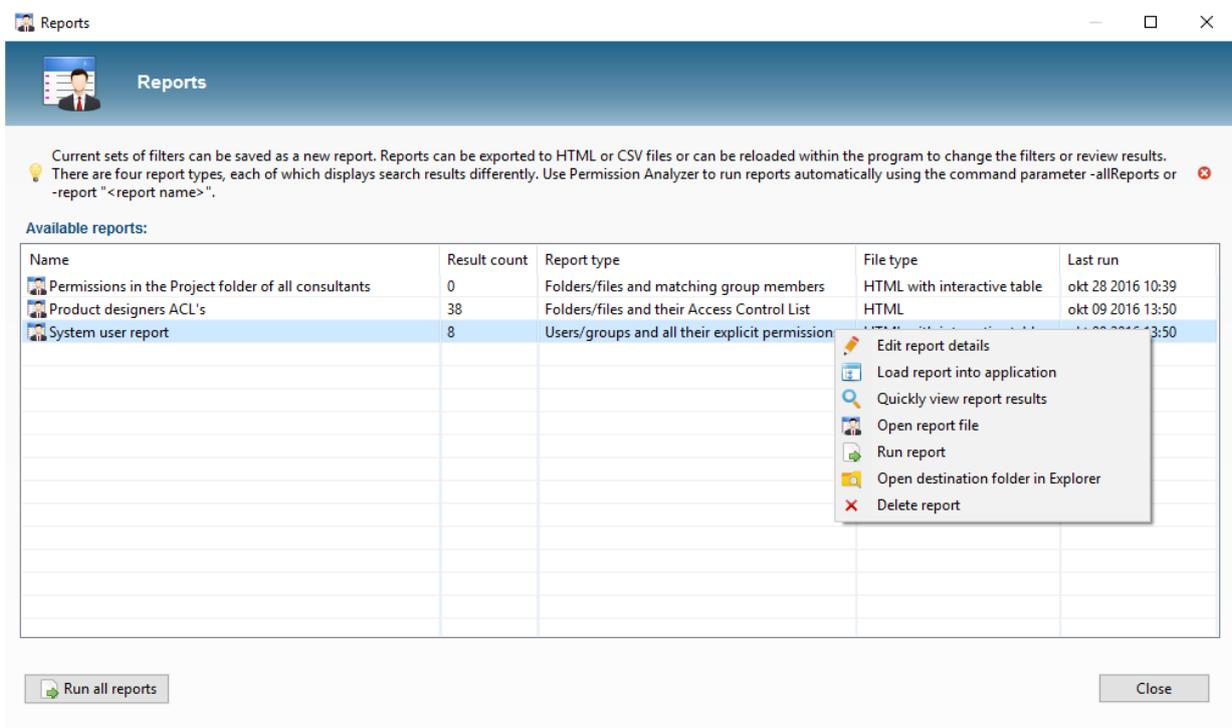
- Members
- File path
- Permission text
- Special permission
- ACE flags
- Owner
- Inherit ACL

Show 50 entries Search:

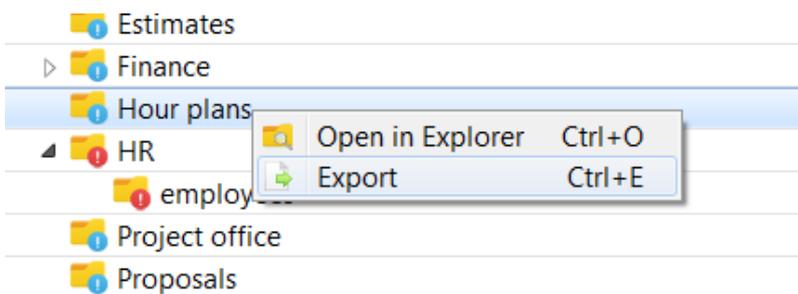
Member and files	Via ACL member	Permission	Read data	Write data	Append data	Execute	Read attributes	Write attributes	Read extended attributes	Write extended attributes	Delete subfolders and files	Delete	Change permissions	Take ownership	Owner
TESTDOMAIN\Purcell [Sean Purcell] (5 ACEs)															
\dataserver01\data	TESTDOMAIN\Domain Users [global group]	Read and execute (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											
\dataserver01\data\Finance\2015\Projects\Results\Clients\MCE Hospital	TESTDOMAIN\Consultants [global group]	Modify (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											
\dataserver01\data\Finance\2015\Projects\Results\Clients\Trade Bank LC	TESTDOMAIN\Consultants [global group]	Read and execute (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											
TESTDOMAIN\Rounthwaite [Robert Rounthwaite] (3 ACEs)															
\dataserver01\data	TESTDOMAIN\Domain Users [global group]	Read and execute (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											
\dataserver01\data\Finance\2015\Projects\Results\Clients\MCE Hospital	TESTDOMAIN\Consultants [global group]	Modify (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											
\dataserver01\data\Finance\2015\Projects\Results\Clients\Trade Bank LC	TESTDOMAIN\Consultants [global group]	Read and execute (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											
TESTDOMAIN\Waxman [Peter Waxman] (3 ACEs)															
\dataserver01\data	TESTDOMAIN\Domain Users [global group]	Read and execute (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											
\dataserver01\data\Finance\2015\Projects\Results\Clients\MCE Hospital	TESTDOMAIN\Consultants [global group]	Modify (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											
\dataserver01\data\Finance\2015\Projects\Results\Clients\Trade Bank LC	TESTDOMAIN\Consultants [global group]	Read and execute (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											
\dataserver01\data\Finance\2016\Offerings\IT Solutions	TESTDOMAIN\Product designers [global group]	Modfr (explicit)	<input checked="" type="checkbox"/>	TESTDOMAIN\Clayton											

## Managing reports

A list of all reports can be requested via the menu: [Report] > [Manage Reports]. You will subsequently be able to review and modify all reports, run them manually or import them into the application.



## Quick export



Folders can be easily exported using the filters selected and will not require generation of a report. Simply open the context menu of a folder

using the right mouse button and select Export. This option will also allow you to select the report type, file type and whether you wish to send an e-mail.

## 3.5 DEFINING POLICIES



*Save your filters as policies and receive e-mail notifications if your policy report contains unwanted permissions.*

A policy is a collection of filters that display unwanted permissions. This collection can be saved as a policy where an e-mail notification is sent if the report contains more than a certain number of directories and files. That number can be configured via the **Policy alert threshold** value in the policy details. Here's the difference between a policy report and a standard report: a policy report defines a combination of filters that should not yield any results. If any results are found, however, an e-mail notification is sent out. Running a policy report automatically from time to time will allow you to check for any unwanted permissions within the network.

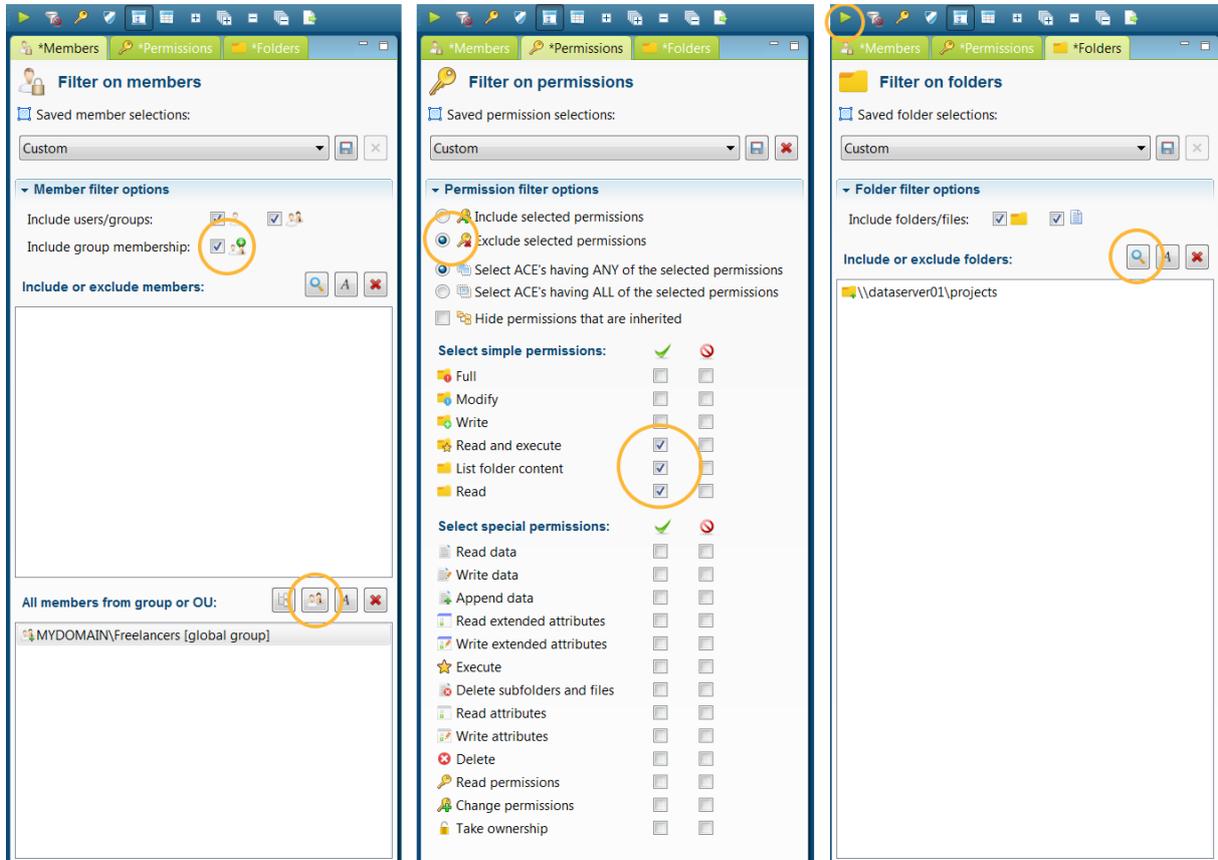
A **SMTP** server should be configured to facilitate any e-mail notifications. Go to settings to configure the server. You will also be able to indicate whether you want the report to be included as an **attachment** and to include a message in the e-mail. The e-mail template may contain the following fields: [report\_name], [report\_path], [report\_description] and [report\_threshold].

### Example

If, in your access control design you determined that all freelancers within your network should be unable to modify project information and you would like to verify that policy with current permissions within the network. All freelancers are located in a communal group; project information is kept in the projects folder on a data server. First you will have to define the filters that make up the policy:

- Select Freelancers from the Members tab and add this group to the bottom selection list (see screenshot). This will not filter for the group itself but for **all** the members of that group. Nested group membership will automatically be taken into account for each group member when determining permissions.
- In the Permissions tab select the Exclude option and select all reading privileges. These, after all, are privileges that Freelancers have been granted and as such should be excluded from the policy report.

- In the Folders tab select the \\dataserver01\projects folder. Your search results will then be scoped to that specific folder.



Review your search results by applying the filters using the **Apply filters** button. If necessary, add new filters, e.g. an Exclude filter for one or more users. Ideally, the result field will remain empty, meaning that no unwanted permissions have been found and that your policy has been implemented completely. Should you have any search result items that appear as exceptions, then simply raise the threshold value for e-mail notification in the report. The threshold value determines the number of files or folders notifications that are sent and can be configured in the *Policy alert threshold* field. For a policy you will only want a notification if a minimum number of files is found, so you would set the value at 1 or more. Once your search results are satisfactory, save your filters as a new policy:

Create a new policy
— □ ×



## Create a new policy

If you have selected a filter selection as a filter, then that selection will show up as an option when creating the report. Using the selection will create a reference to the filter selection within the report and any modifications to the filter selection will result in all reports automatically applying the modified selection. Unchecking the option in the report will result in the report saving a copy of the filters and not change according to the filter selection. ✖

**Policy name:**

**Report description:**

**Report type:**

**File type:**

**Target file path:**   

**Custom template path:**   

**E-mail recipient:**

**Policy alert threshold (file/folder count):**  

**Link to filter sets:** No filter sets have been selected

**Filters for this report:**

 Include (nested) group membership
 Include all members from the group TESTDOMAIN\Freelancers [global group]
 Exclude ACE's that have any of the following permissions:
 Read (allow)
 List folder content (allow)
 Read and execute (allow)
 Include folder \\dataserver01\projects

The way a policy report is shown depends on the report type you. If you selected the report type **Folders/files and matching group members**, it may look like the figure below. The report below shows that John Doe has Modify privileges in the “project\Change requests” through the “Project Office” group. It also shows Jane Murphy has full privileges within the “projects\Development” folder, as she is part of the “Testers” group. These results show you who has acquired more permissions than is desirable and where additional permissions have been granted.

Directories and files found: 10 PERMISSION ANALYZER - TRACE REPORT

The Trace report displays permission information for all members that match the selected filter criteria. For each member the report will show all applicable Access Control Entries and where they come from, meaning via what group membership.  
All permissions excluding Read permissions for everyone in the group Freelancers scoped to the projects folder.

**Filters applied:**

- Include (nested) group membership
- Include all members from the group MYDOMAIN\Freelancers [global group]
- Exclude ACE's that have any of the following permissions:
  - Read and execute (allow)
  - List folder content (allow)
  - Read (allow)
- Include folder \dataserver01\projects

**Column visibility:**

- File path
- Members
- Permission text
- Special permission
- ACE flags
- Via group

Show 200 entries Search:

Member	Permission	Read data	Write data	Append data	Execute	Read attributes	Write attributes	Read extended attributes	Write extended attributes	Delete subfolders and files	Delete	Read permissions	Change permissions	Take ownership	Via group	ACE flags
<b>\dataserver01\projects\Change requests</b>																
MYDOMAIN\jdoe [John Doe]	Modify (explicit)	<input checked="" type="checkbox"/>	MYDOMAIN\Project Office [global group]	This folder, subfolders and files												
<b>\dataserver01\projects\Development</b>																
MYDOMAIN\jmurphy [Jane Murphy]	Full (explicit)	<input checked="" type="checkbox"/>	MYDOMAIN\Testers [domain local group]	This folder, subfolders and files												
<b>\dataserver01\projects\Development\Calculation application</b>																
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)	<input checked="" type="checkbox"/>	MYDOMAIN\Testers [domain local group]	This folder, subfolders and files												
<b>\dataserver01\projects\Development\Calculation application\appidcertstorecheck.exe</b>																
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)	<input checked="" type="checkbox"/>	MYDOMAIN\Testers [domain local group]	This file only												
<b>\dataserver01\projects\Development\Calculation application\Design</b>																
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)	<input checked="" type="checkbox"/>	MYDOMAIN\Testers [domain local group]	This folder, subfolders and files												
<b>\dataserver01\projects\Development\Calculation application\Design\cifs.sys</b>																
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)	<input checked="" type="checkbox"/>	MYDOMAIN\Testers [domain local group]	This file only												
<b>\dataserver01\projects\Finance</b>																
MYDOMAIN\jdoe [John Doe]	Special (explicit)	<input checked="" type="checkbox"/>	(direct)	This folder, subfolders and files												
<b>\dataserver01\projects\HR</b>																
MYDOMAIN\jdoe [John Doe]	Full (inherited)	<input checked="" type="checkbox"/>	MYDOMAIN\HR Admins [global group]	This folder, subfolders and files												
<b>\dataserver01\projects\HR\employees</b>																
MYDOMAIN\jdoe [John Doe]	Change permissions (explicit)	<input checked="" type="checkbox"/>	(direct)	This folder and subfolders												
MYDOMAIN\jdoe [John Doe]	Full (inherited)	<input checked="" type="checkbox"/>	MYDOMAIN\HR Admins [global group]	This folder, subfolders and files												
<b>\dataserver01\projects\Proposals</b>																
MYDOMAIN\jdoe [John Doe]	Modify (explicit)	<input checked="" type="checkbox"/>	(direct)	This folder, subfolders and files												

Showing 1 to 11 of 11 entries Previous **1** Next