PERMISSION ANALYZER

USER MANUAL 2.4

Protect your data and get in control!

Scan your network, filter NTFS permissions,

validate your access control design

and trace user or group access.

PERDEMIASOFTWARE
Get in control

1. What is Permission Analyzer? 4
1.1 Main features 4
Scanning the NTFS file systems and Active Directory 4
Viewing server permissions and applying filters 4
Tracing user and group permissions 4
Creating HTML and CSV exports and security audit policies 5
2. Architectural setup 6
2.1 Using the embedded database 6
2.2 Using a central database 7
2.3 Using scan agents 8
3. Features 10
3.1 Scanning the network 10
Configuring LDAP connections 10
Adding directories and LDAP OU's 12
Starting scan 13
3.2 Filters and overviews 13
Filtering for users and groups 14
Filtering for permission privileges 15
Filtering for directories and files 16
Overview of permissions 16
Displaying Ownership ratio 19
3.3 Tracing permissions 20
3.4 Reports and export 23
Report types 24
E-mail 24
Report templates 24
Filter selections 25
Running reports automatically 25
Managing reports 31
Quick export 31
3.5 Defining policies 32
Example 32
Creating policies using the wizard 35

Running policies automatically 36
3.6 Scheduling jobs 36
3.7 Modifying permissions 38
3.8 Data protection 39
3.9 External database 40
3.10 Other features 41
Showing member info 41
Configuring LDAP attributes 43
Update service 43
4. Using PowerShell scripts 43
5. Licensing model 47
6. FAQ 49
6.1 Technical questions 49
6.2 Functional questions 52
6.3 Licensing questions 55
7. Application version history 57

1. What is Permission Analyzer?

Permission Analyzer reports NTFS permissions from the file system combined with user and group data from the Active Directory. All data is stored in a local or remote database and can be utilized to create overviews of permissions based on many filter criteria. You will be able to monitor permissions for entire user groups and receive notifications if undesired permissions are found within your network.

1.1 MAIN FEATURES

Scanning the NTFS file systems and Active Directory

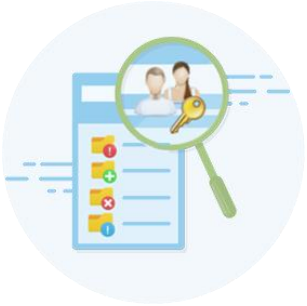
Configure the directories and LDAP Organizational Units to scan. All directory information and group memberships from LDAP are saved in a local database file. Run the scan whenever you like or schedule an automated scan. Permission Analyzer supports an external database, allowing multiple workstations to share the same information source.

Viewing server permissions and applying filters

All information is saved on a database, allowing you to conduct targeted search queries in seconds, instead of scanning the whole network every time you want to apply a new filter. Add filters for specific members, all members of a group or LDAP OU, permissions or folders.

Tracing user and group permissions

The main overview provides an aggregated summary of all server permissions found and may contain the permissions of multiple users or groups. The application offers different views on the search results, like the effective permissions per user/group, the plain ACL information like Windows Explorer, the origin of permissions for a specific user or group (via which group membership or parent folder they have been inherited), and a view of all the matching users/groups that have been found including their (possible unwanted) permissions. Use these views to zoom in on your search results.



Creating HTML and CSV exports and security audit policies

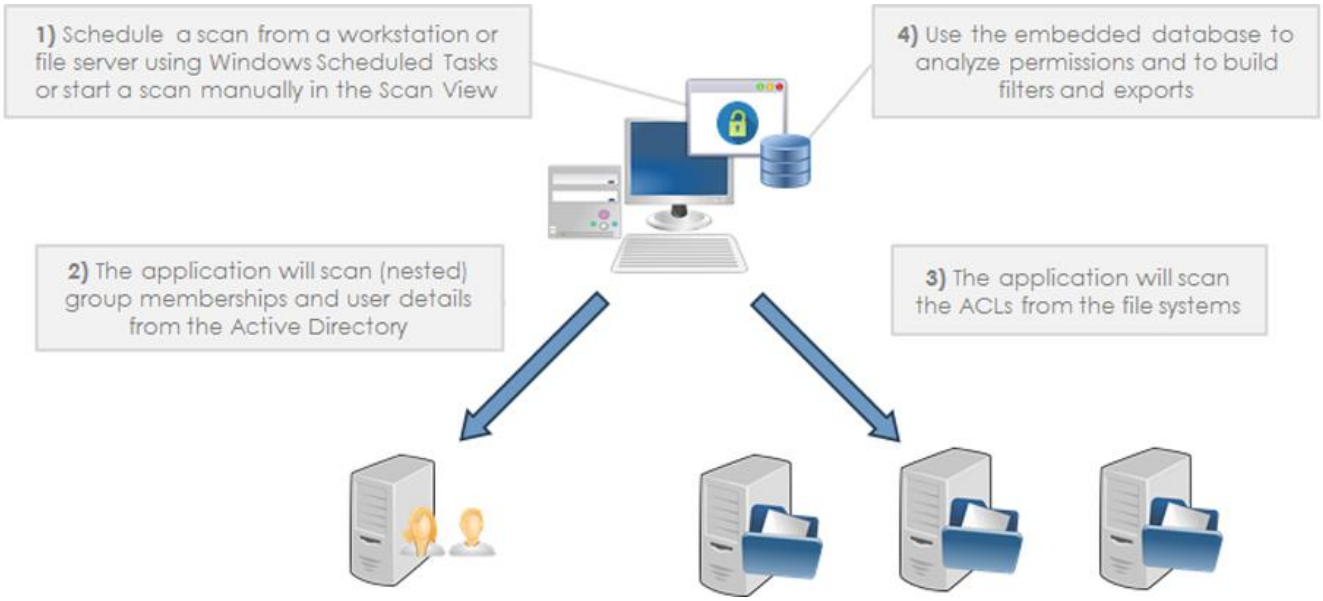
Save your filters as report and export them to HTML or CSV and e-mail. Use Permission Analyzer to run reports automatically using command-line parameters. Save your filters as policies and receive e-mail notifications if your policy report contains unwanted permissions.

2. Architectural setup

Permission Analyzer supports different setups by either using the embedded database, or a central database server to share the scanned network data, filter definitions and reports between workstations.

2.1 USING THE EMBEDDED DATABASE

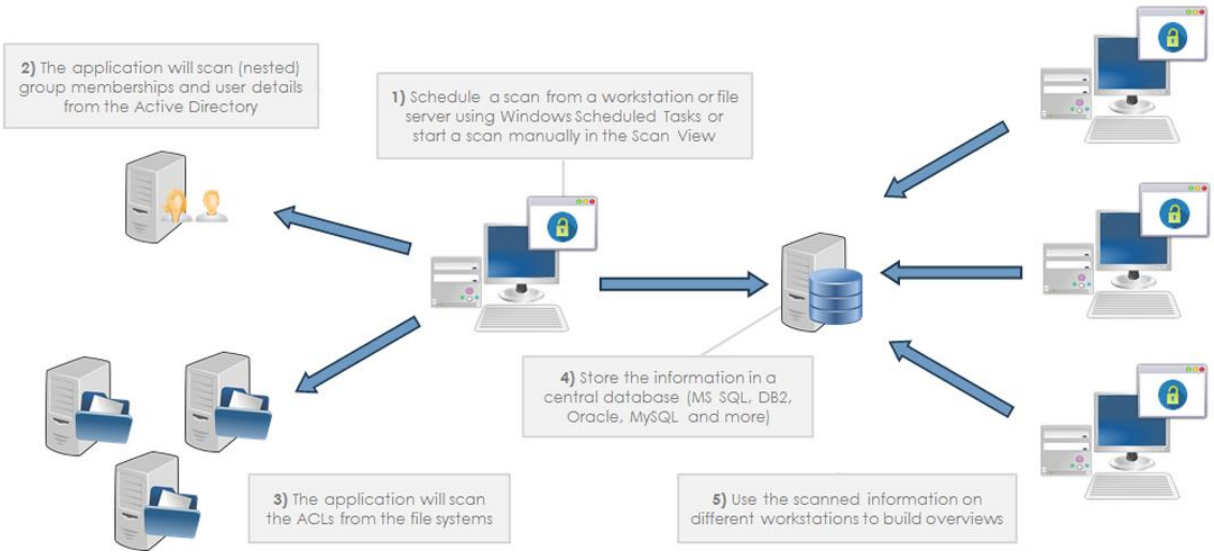
The default setup depends on a single workstation or server. The scanning is done from a single machine and the information is stored in a local database file. The disadvantage of this setup is that the scanned information cannot be shared and that the workstation or server will have to scan all the remote file systems, which has the overhead of reading remote NTFS permissions over the network:



The performance depends a lot on the network setup and hardware. Scanning local files using a local database scans about 25,000 files per minute and takes 1 MB database storage per 1000 files or directories. When scanning a NAS or using a remote database, much of the performance depends on the network environment. See Using scan agents to scan remote file systems more efficiently.

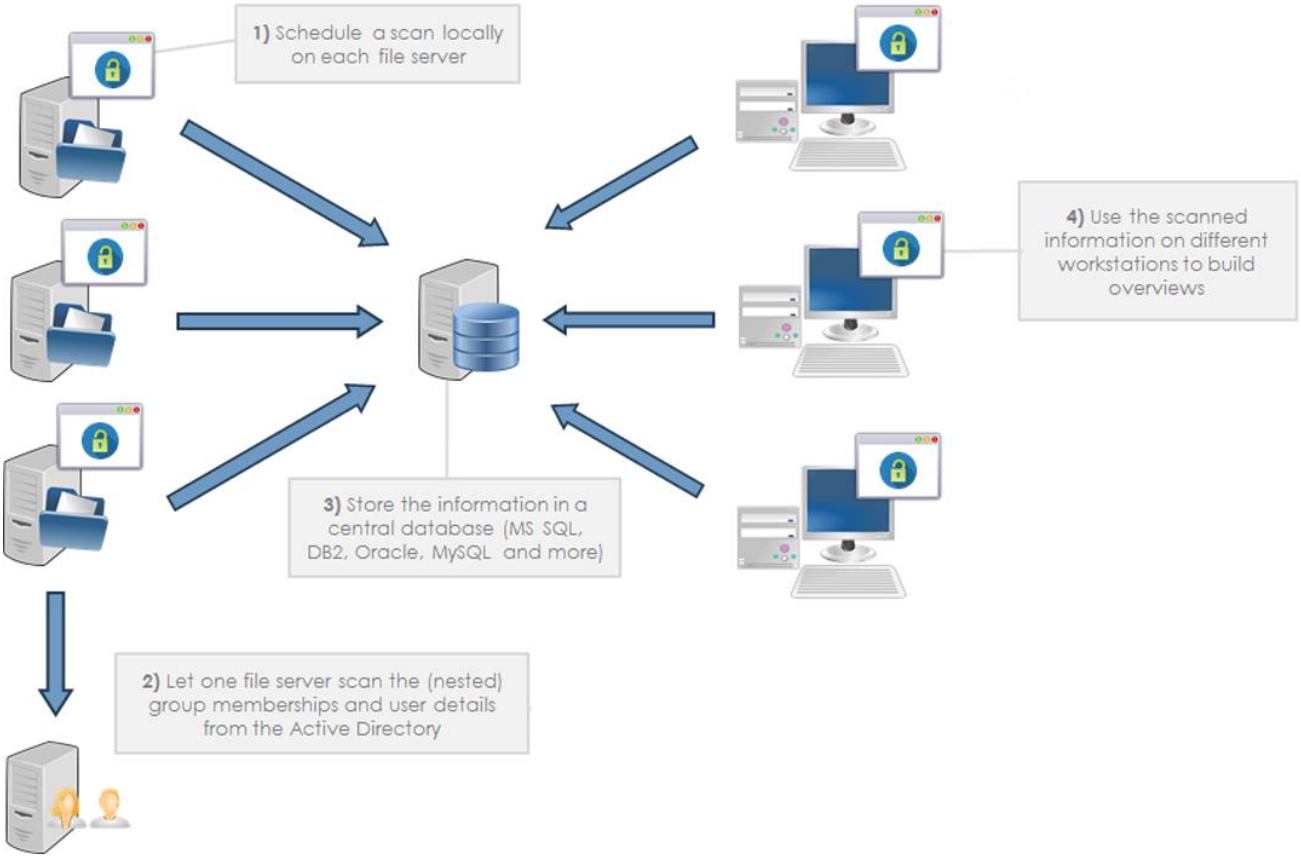
2.2 USING A CENTRAL DATABASE

The second setup has a shared (external) database, which means that other team members / workstations can use the scanned information from the database to create overviews. The application supports Oracle, MSSQL, DB2, MySQL, PostgreSQL, H2 and Derby out of the box. User reports, policies and filter sets are stored in the database, so when you use a central database you can share that information between all the clients/workstations. Note that each workstation requires a license, Permission Analyzer is licensed on "per-installation" basis. The Basic and Standard Edition don't support the use of an external database.

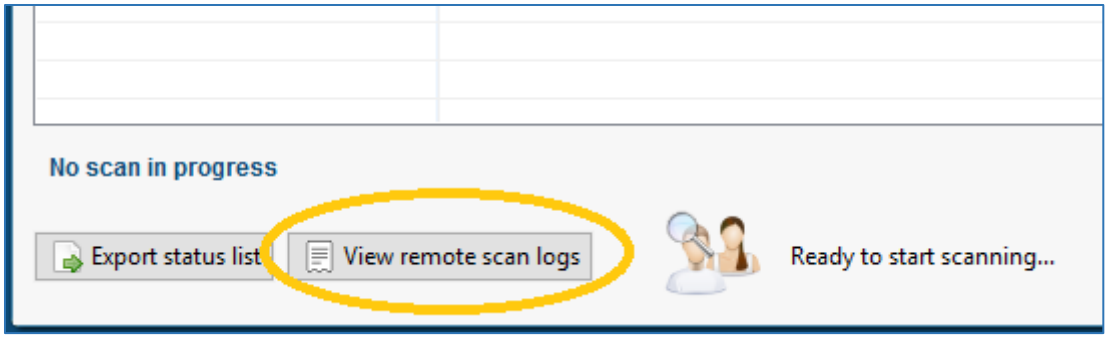


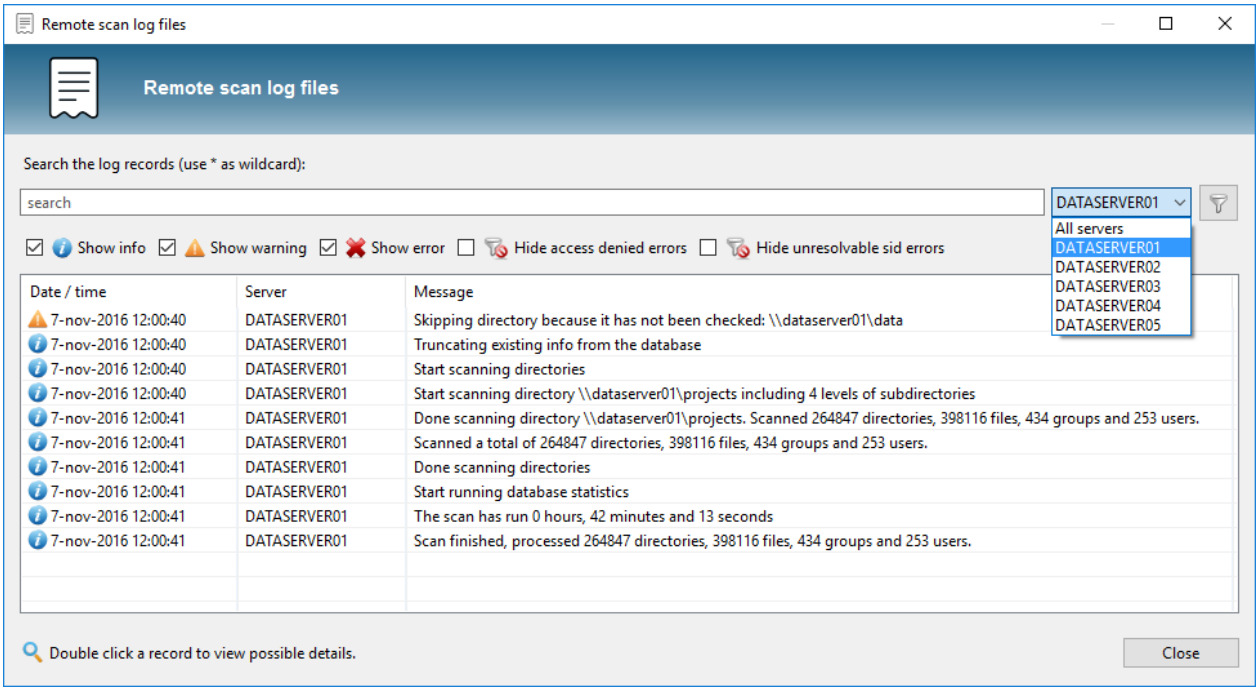
2.3 USING SCAN AGENTS

The third setup may prevent the reading of remote permissions over the network and makes it possible to scan the file systems simultaneously. Instead of scanning a remote file system from a workstation, every file server will scan its own local permissions and submits the information to a central database. Reading local permissions is a lot faster and the file servers can scan their permissions simultaneously. The file servers only require a (cheaper) Scan Agent license, which doesn't support reporting, but only scanning the network. A Scan Agent is the same application installation (and download from the website), but it is activated with a Scan Agent license. This will only activate the scanning features of the application.



Every scan agent can be scheduled using Windows Scheduled Tasks in combination with the application parameter "-scan". A Scan Agent stores the status messages in the central database, which is also the way in which to communicate with an agent. You can view the scan results of every agent in a centralized view of either one of the scan agents or your workstation:





3. Features

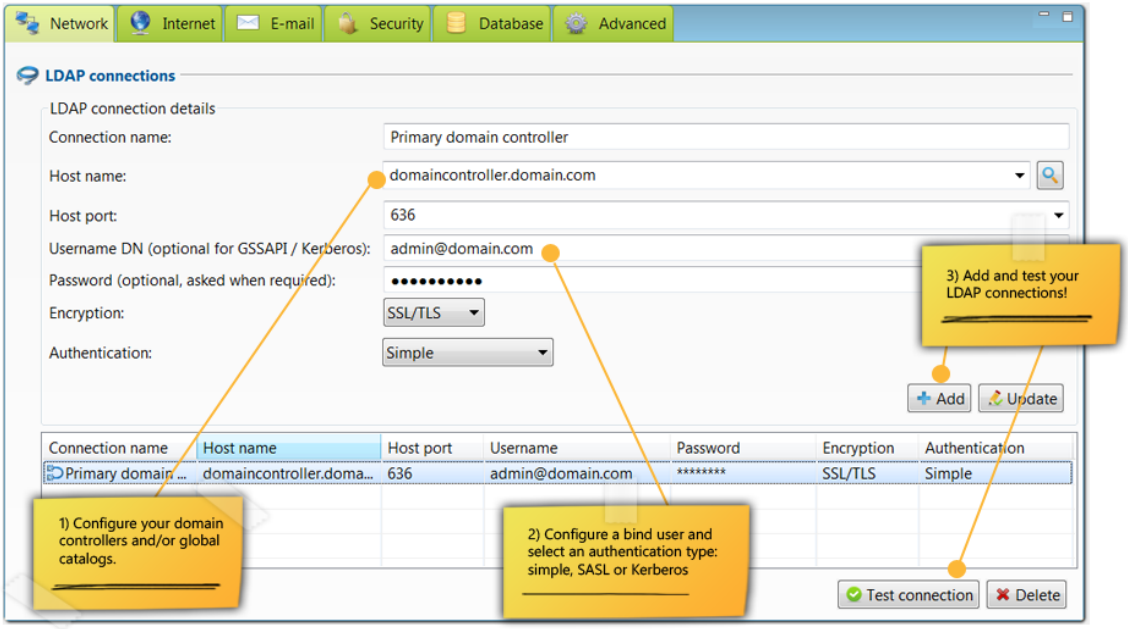
3.1 SCANNING THE NETWORK

Specify directories or network shares to scan and configure depth. Add (nested) group membership information to the database by selecting particular LDAP Organizational Units to scan.

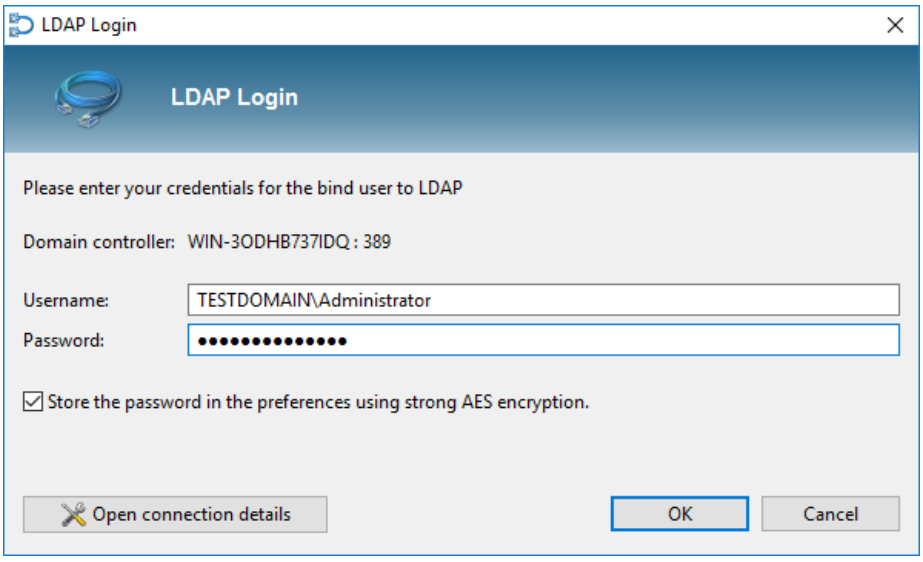
Permission Analyzer has two key functionalities: network scanning and overview creation. During the scanning process, all necessary information is stored in the corresponding local database. A major advantage of this feature, firstly, is that the network need not be overloaded with each overview that is run. Secondly, any overview results are available within a matter of seconds. The database contains the Access Control List of each folder (or file), group and user data from the LDAP, such as usernames, and data on (nested) group relations. In addition, Permission Analyzer supports a series of external databases, allowing data to be centralized and shared between multiple workstations. Please see chapter on External Database.

Configuring LDAP connections

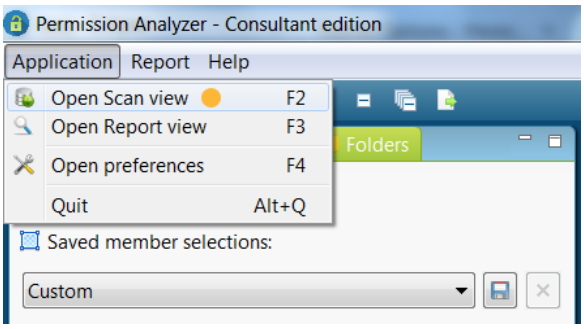
Permission Analyzer will automatically detect your domain and Active Directory connection and will ask for a username and password to read information from the AD. Open the application **preferences** to add more LDAP connections, such as various domain controllers or a global catalog. Permission Analyzer supports multiple authentication protocols, such as (bind) username and password, Digest-MD5, Cram-MD5 or Kerberos. In addition, users can choose between plain, SSL/TLS or STARTTLS security protocols.



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. See the chapter Data protection for more details about securing the data and preferences.



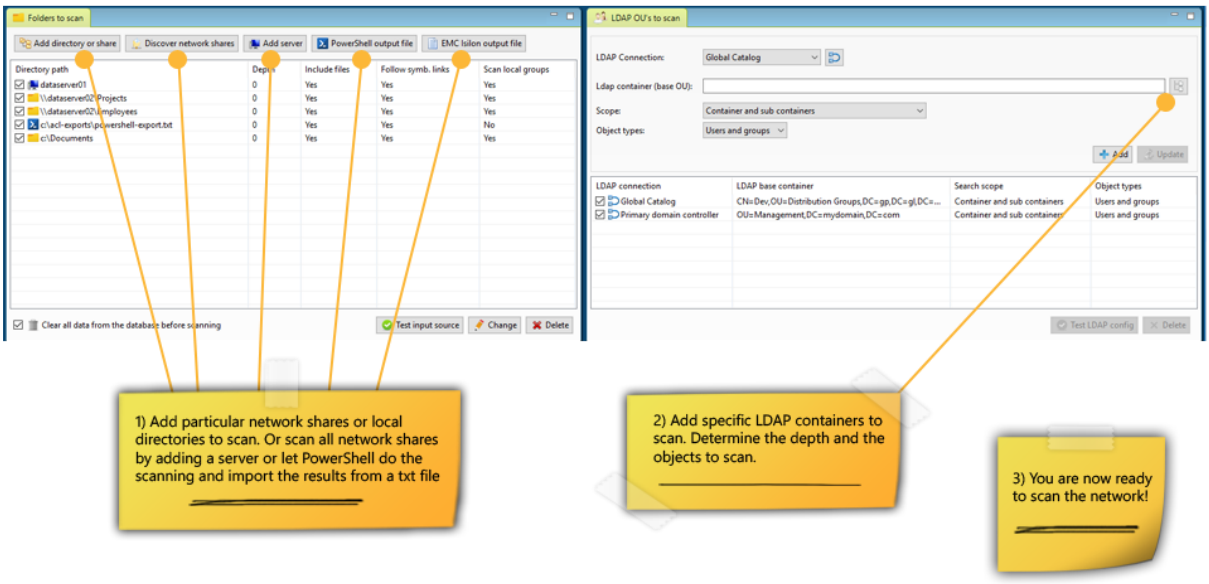
Adding directories and LDAP OU's



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 for the relevant member.

Directories can be limited by setting up a depth limit for the number of subdirectories, file scanning and scanning of local groups on the server of the directory. LDAP OU's can also be configured with a depth limit as well as selected scanning of users and/or groups. Permission Analyzer will at all times ensure that a comprehensive overview of nested group data is available by assessing the **member** and **memberOf** attributes of each user or group. As such, the scan may expand beyond the selected OU.

Note: because a universal group can have members from domains other than the domain where the group object is stored and can be used to provide access to resources in any domain, only a global catalog server is guaranteed to have all universal group memberships that are required for authentication. On the other hand, the global catalog stores the membership (the member attribute) of only universal groups. The membership of other groups can be ascertained at the domain level. Therefore, if applicable, make sure you add both the domain controllers as your global catalogue to ensure a complete overview of group memberships. Permission Analyzer will make sure that no duplicate memberships are stored.

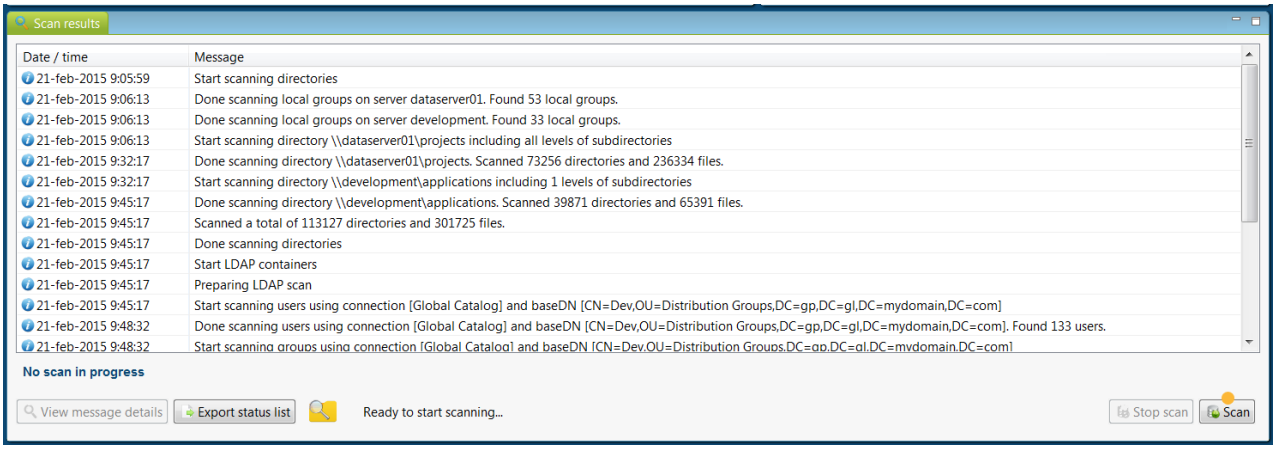


Starting scan

Permission Analyzer will refresh the database with the current network statistics when a scan is initiated. You will also be able to choose to refresh the databases or LDAP OUs only. This will result in the application leaving user and group data unchanged in the former and the directory data in the database unchanged in the latter. Only items that are **checked** will be scanned by Permission Analyzer.

A scan may be initiated automatically by the application using the scan 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.

You will be able to review the results of the final scan in the status list or in the *Last_status_messages.csv* file in the application directory.

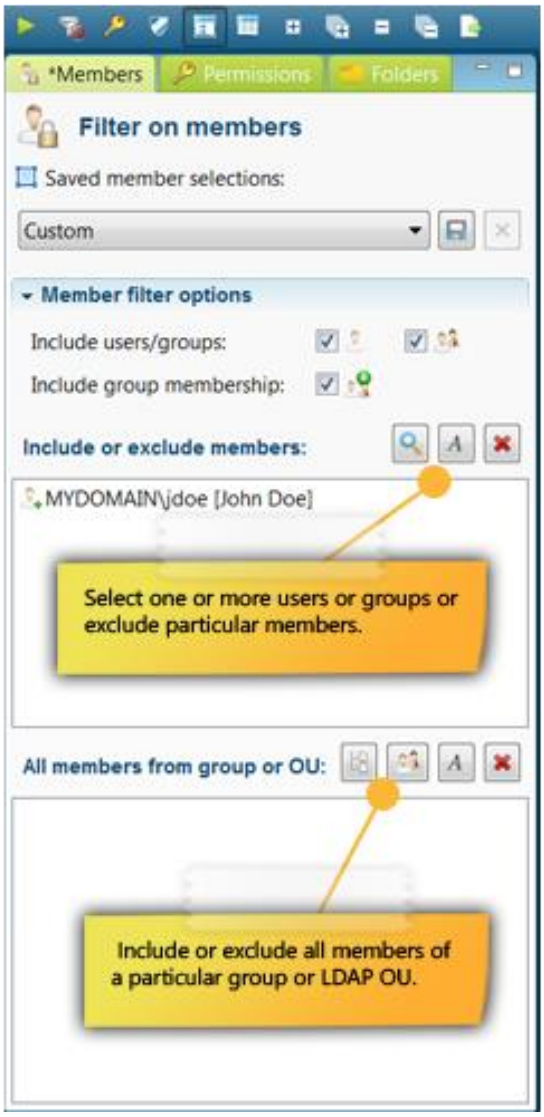


3.2 FILTERS AND OVERVIEWS

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.

Following the network scan, the database may be used to carry out search queries. Permission Analyzer offers an extensive set of filters for you to obtain specific information. The search results are represented in the **tree** structure or **table** of directories and files. An **aggregated** list of privileges is shown for each of the directories or files, as the search result(s) may contain privileges of multiple users or groups. You will be able to zoom in on the aggregated privileges using the Trace options at the bottom of the result window. The filters are divided into three categories, namely Members, Permissions and Folders. Each category can be found as a tab on the left of the outline.

Filtering for users and groups



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.

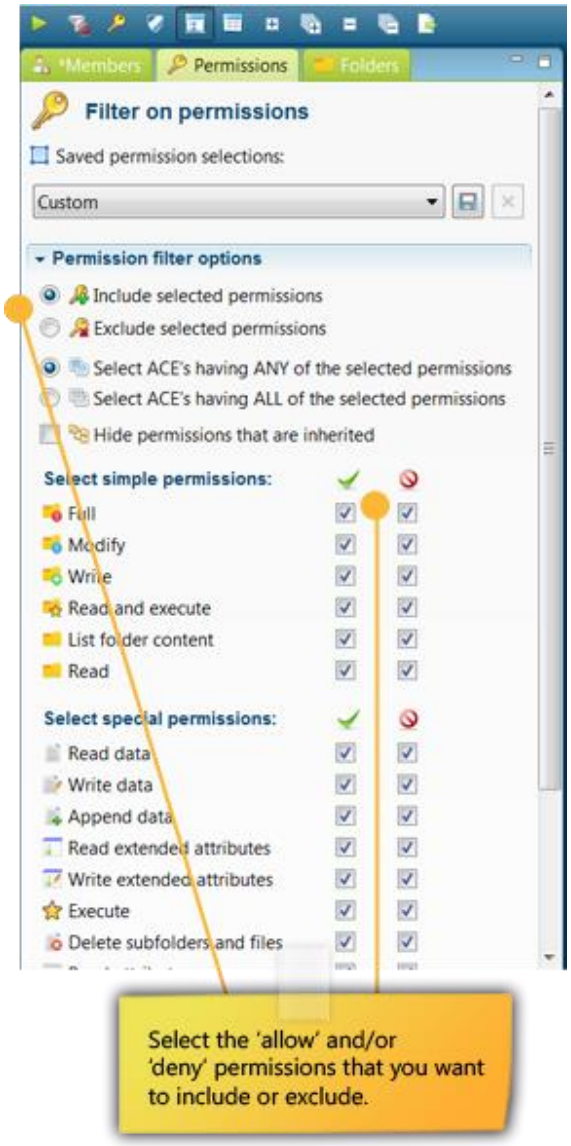
In addition to including members in searches, you are also able to **exclude** one or more members from searches, e.g. by excluding everyone from the Domain Admins group.

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.

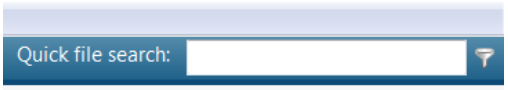
If necessary, configure the filter to only display **explicit** permissions.



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.

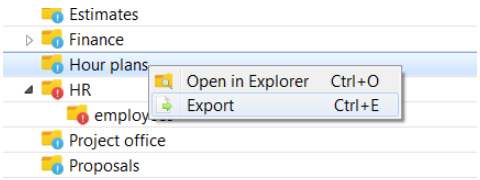


A set of filters can be saved as a **Selection**, making a large number of frequently used filters easily retrievable and usable. A selection will bundle filters of the same type (members, permissions or folders). The total number of filters for an overview can be saved as a Report. Filters can be modified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

Overview of permissions

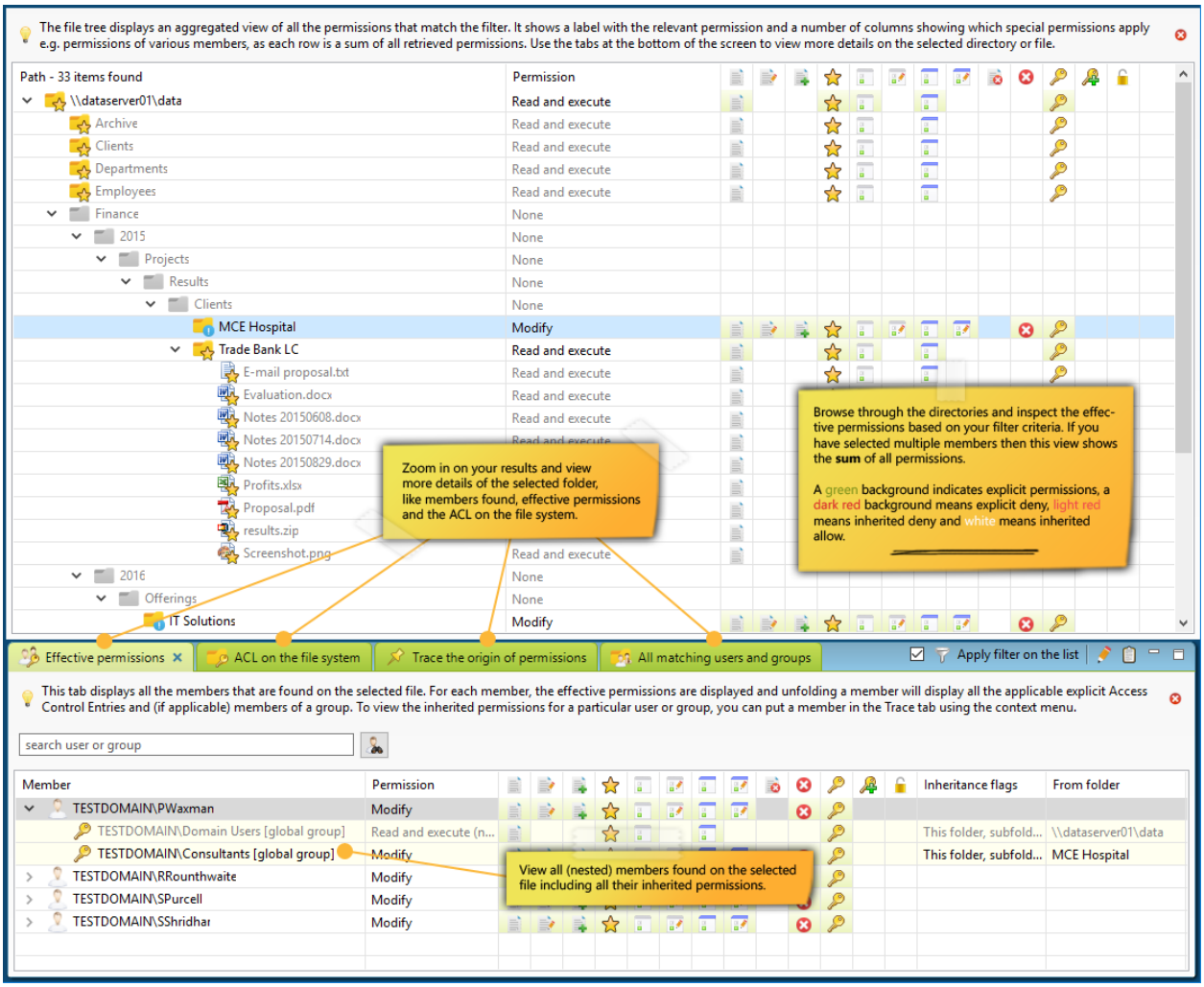
After applying the filters, all retrieved permissions will be shown in a tree structure, grouped in directories and files. The toolbar also contains an option to have results displayed in a table rather than a tree structure. Each item will contain a label with the relevant permission and a number of 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**.



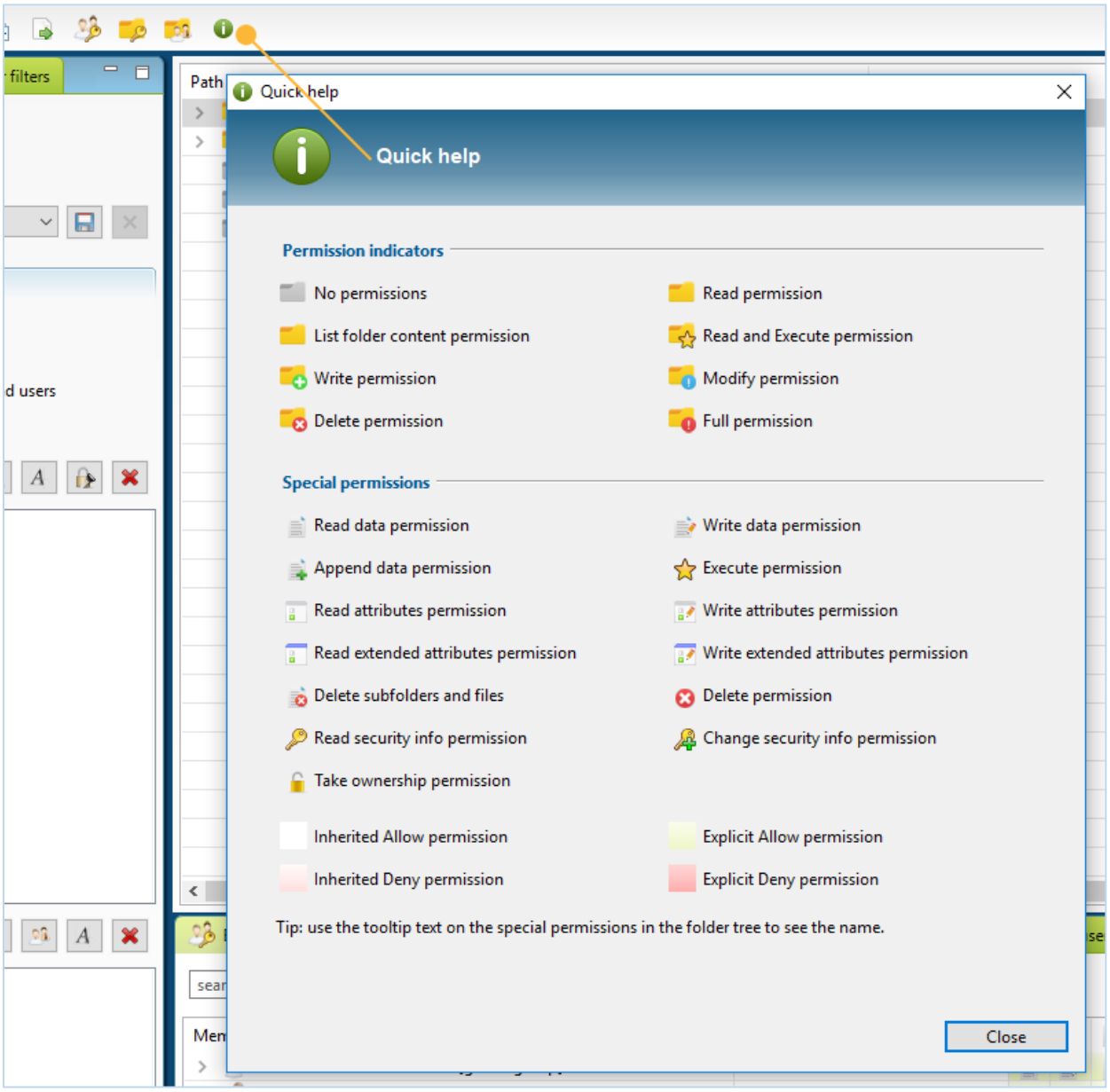
There are four tabs at the bottom of the search result screen: one which allows you to zoom in on a directory to review which permissions and members have been found including their effective and inherited permissions, one that provides details on the Access Control List of the directory selected, one 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. For more details see the Modifying permissions and Tracing permissions features.

Tip: drag tabs to a second screen or to another location within the application to view both tabs simultaneously.



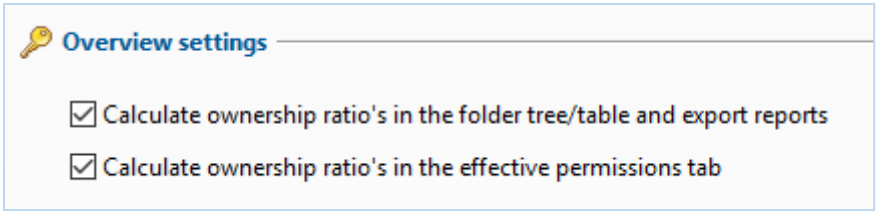
The folder tree should make it clear at a glance where the unwanted rights are and what rights are granted explicitly. The tree shows all rights per directory, initially this will mainly be FULL rights of the Administrators, but as more filters are applied, the tree will show the purposeful rights. The 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.



Displaying Ownership ratio

The application provides an option to calculate “ownership ratio” per directory. This option is disabled by default, but can be activated in the Advanced tab of the application settings:



The ownership ratio consists of two values:

- **Total ownership ratio**: The number of users and groups that matches the filter criteria and also has rights to the folder, relative to the total number of users that has rights to the folder. In other words, to what extent is my filter selection owner of a folder?

- **Group ownership ratio**: The number of users and groups that matches the filter criteria and also has rights to the folder, relative to the total number of groups and users in the filter selection. In other words, which section of my filter selection actually has rights to a folder?

The values can be used to gain insight into the owner of folders and files, to what extent are the users and groups owner of the filtered data. The following calculation is used:

- *All filtered members* = All users that match the filter criteria (regardless of the selected directory)

- *All folder members* = All users that have rights to the folders (without using filters)

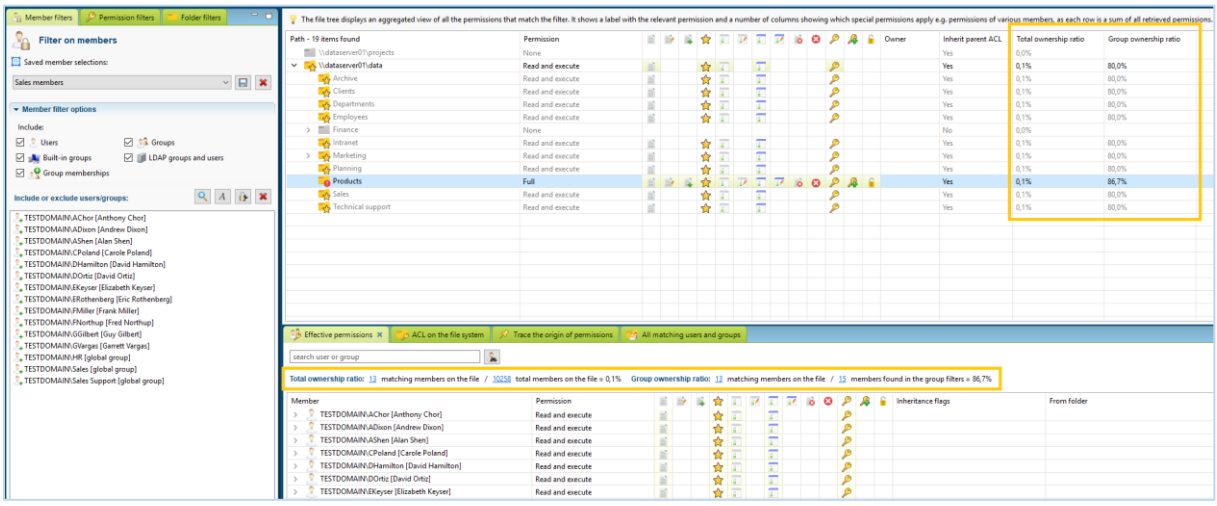
- *Matching folder members* = All users that match the filter criteria and have rights to the selected folder

Total Ownership ratio = *Matching folder members / All filtered members*

Group Ownership ratio = *Matching folder members / All folder members*

The ownership ratio can become visible in three spots, in the folder tree, in the HTML/CSV reports and in the Effective Permissions tab at the bottom of the folder tree.

Example:



We see here that the *Products* folder has been selected, this folder has a Total ownership ratio of **0.1%** and a Group ownership ratio of **86.7%**. These values can be found in the folder tree and the Effective permissions tab. In the tab we see how the values are calculated and by clicking on one of the values it's possible to see which users/groups it involves.

We see that we have filtered on 15 members (users and groups). 13 of these members actually have rights to the Products folder. In total 10,258 members have rights to the folder, so that Total ownership ratio is very small, namely 13 / 10,258 * 100 = **0.1%**.

If we look at how many users in our selection have rights to the folder then we come to a group ownership ratio, namely 13 / 15 * 100 = **86,7%**.

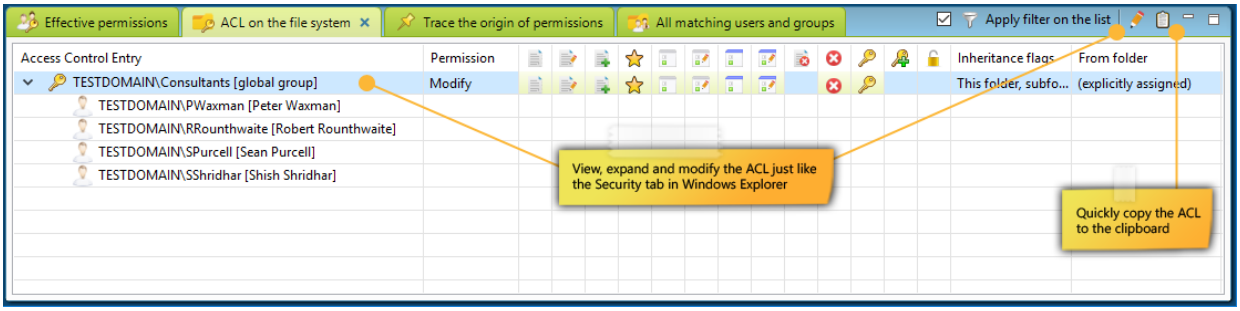
3.3 TRACING PERMISSIONS

Zoom in on your search results and trace the origin of permissions that have been found. See if permissions are inherited from a (indirect) group membership or parent folder.

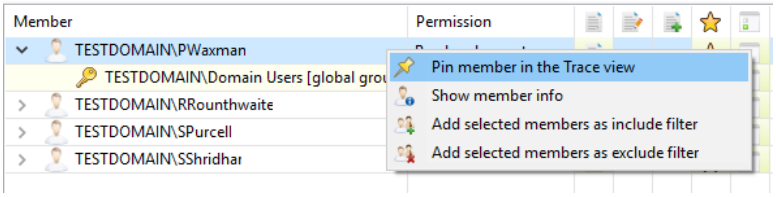
To review a directory for all found permissions, see the tabs at the bottom of the search result screen. Each directory in the main search result screen represents the **sum** of all permissions found. Should the filter criteria yield multiple members, then you may use one of the tabs to view more details about particular members. The first tab with **Effective permissions** displays members for whom permissions have been found on the selected directory or file. Each member can be expanded to view the provenance of

their effective permissions, e.g. through which (nested) group membership the permissions were granted.

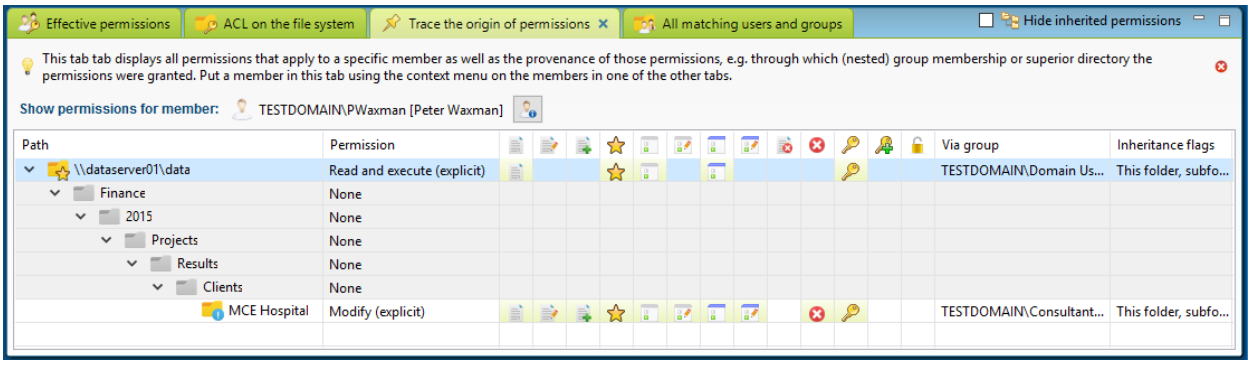
The second tab displays the **Access Control List on the file system**, this tab corresponds with the Security tab on the file properties dialog in Windows Explorer. Only the members that match the filter criteria are displayed, unless the option "*Apply filter on the list*" is unchecked to view the entire Access Control List. Permissions can be modified or the results can be copied to the clipboard using the toolbar buttons in the tab:



The **Trace** tab is used to pin a particular member and to view all applicable permissions for the selected folder. The view subsequently displays all permissions that apply to that specific member as well as the provenance of those permissions, e.g. through which (nested) group membership or superior directory the permissions were granted. This feature allows you to easily track the cause of undesirable permissions and resolve such cases by modifying the permissions. The context menu of a member in one of the other tabs has the option to add the member to the Trace tab.

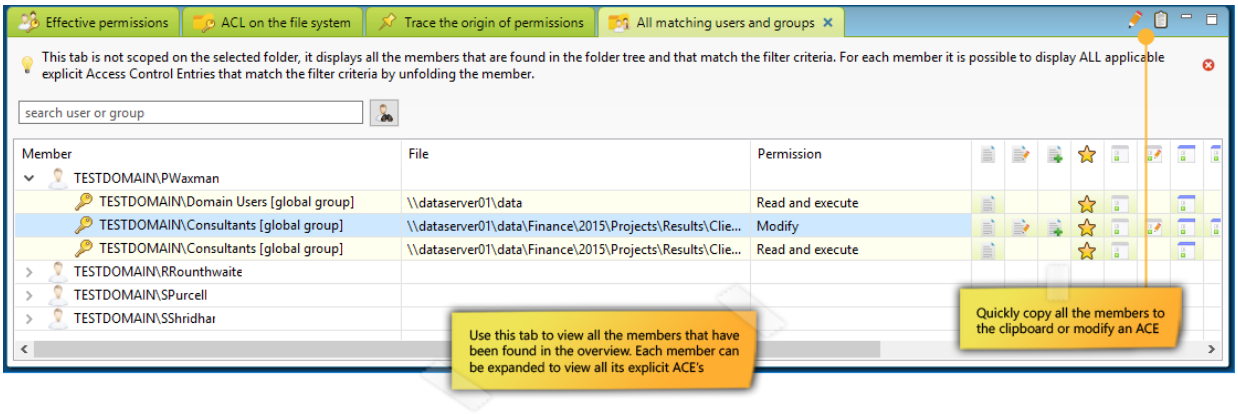


Tip: Use the info button to get the group membership information of the member selected:



The final tab **All matching users and groups** can be used to extract all users and groups from the overview. This is useful when the filter criteria yield multiple members

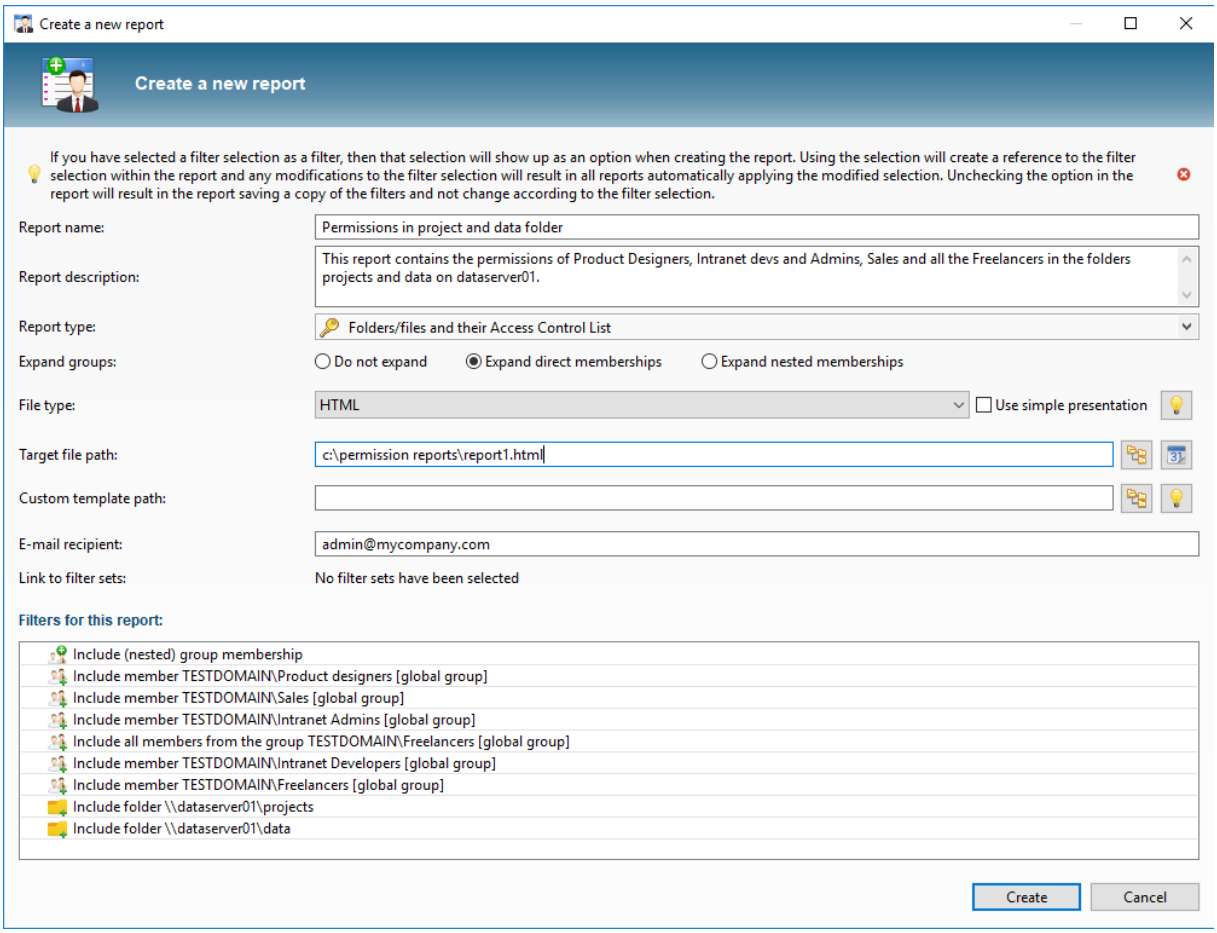
and you want to have a overview of unique users and groups that have been found. Each member can be expanded to view **all** the explicit permissions on every directory for that member, including the ones granted through nested group memberships:



3.4 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. The HTML format includes search, paging and sorting options.



Report types

Permission Analyzer supports twelve 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]`.

Report templates

You will also be able to use modified templates to generate the report. Permission Analyzer comes with a number of default templates for HTML and CSV, which can be modified according to your specifications. The templates are located in *<application dir>\plugins\Permission_Analyzer_2.xxxx.jar* – the file can be opened with any ZIP application. Here are examples of the default HTML template for files and the sum of permissions or the CSV template for files and their ACL's.

Filter selections

If you have selected a filter selection as a filter, then that selection will show up as an option when generating 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.

Running reports automatically

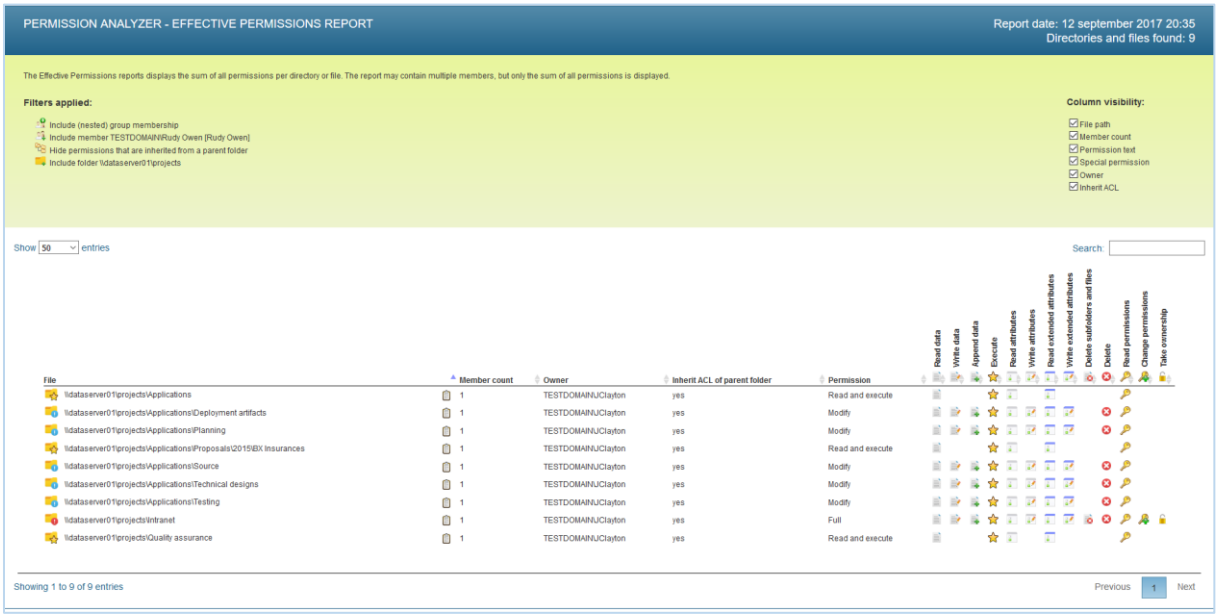
Use Permission Analyzer to run reports automatically using the following parameters:

- **-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.

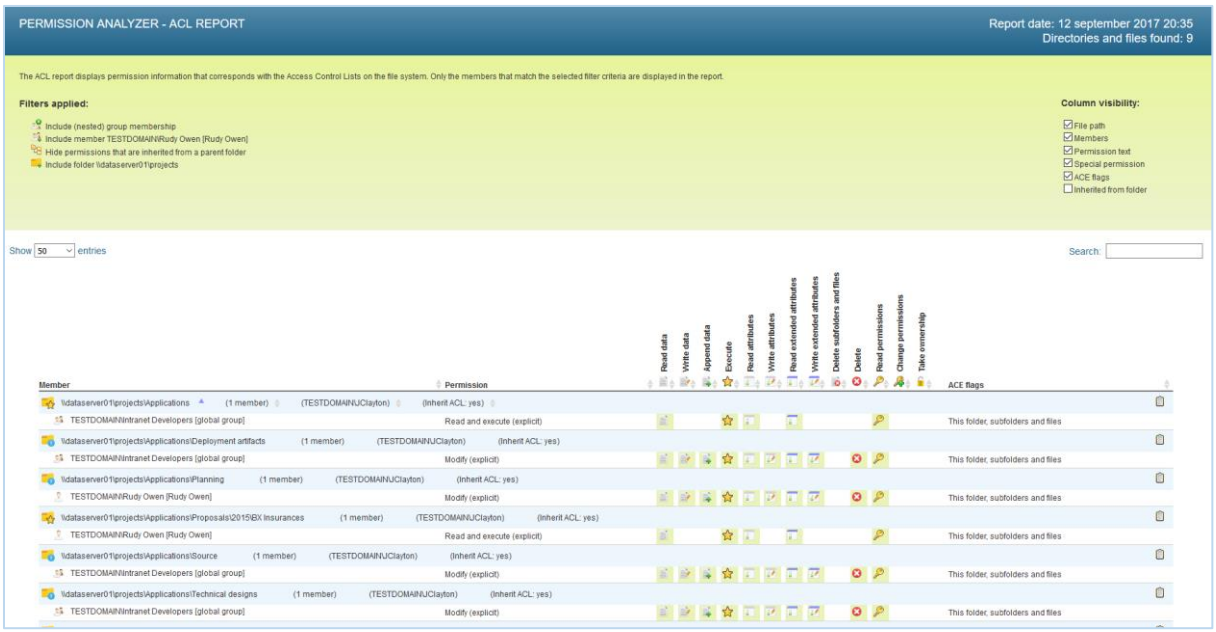
FOLDERS/FILES AND THE SUM OF THEIR PERMISSIONS

This report type shows a sum of all permissions found per directory or file and takes into account the priorities used by Windows (privileges that deny something will, for example, have a higher priority than privileges that grant access).



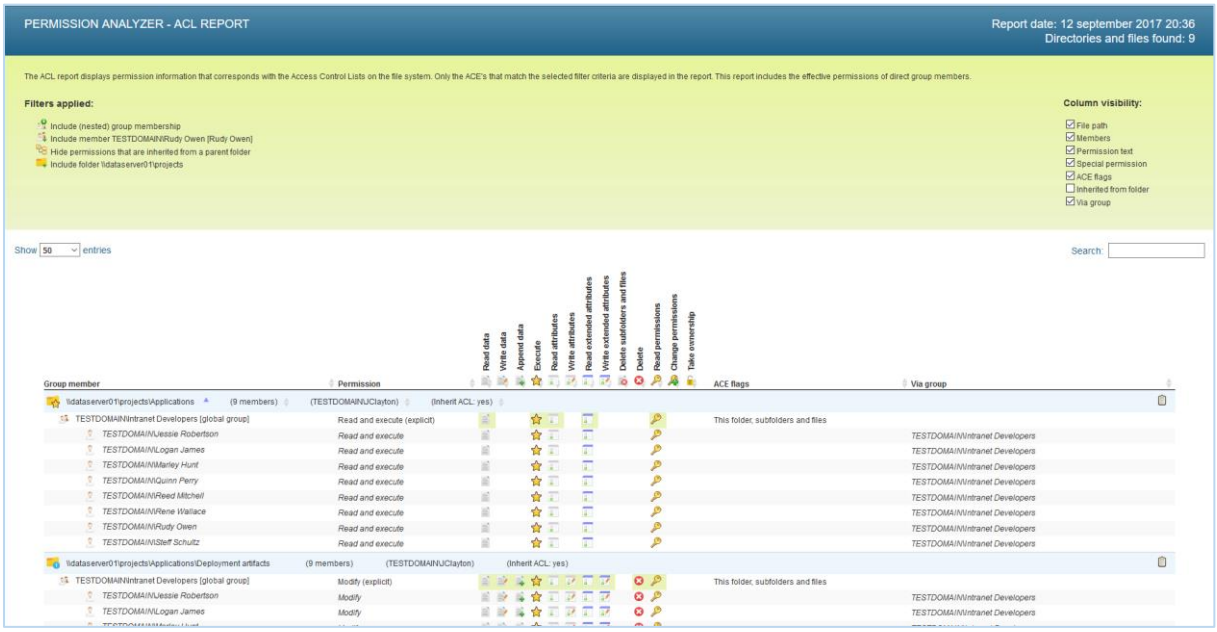
FOLDERS/FILES AND THEIR ACCESS CONTROL LIST

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.



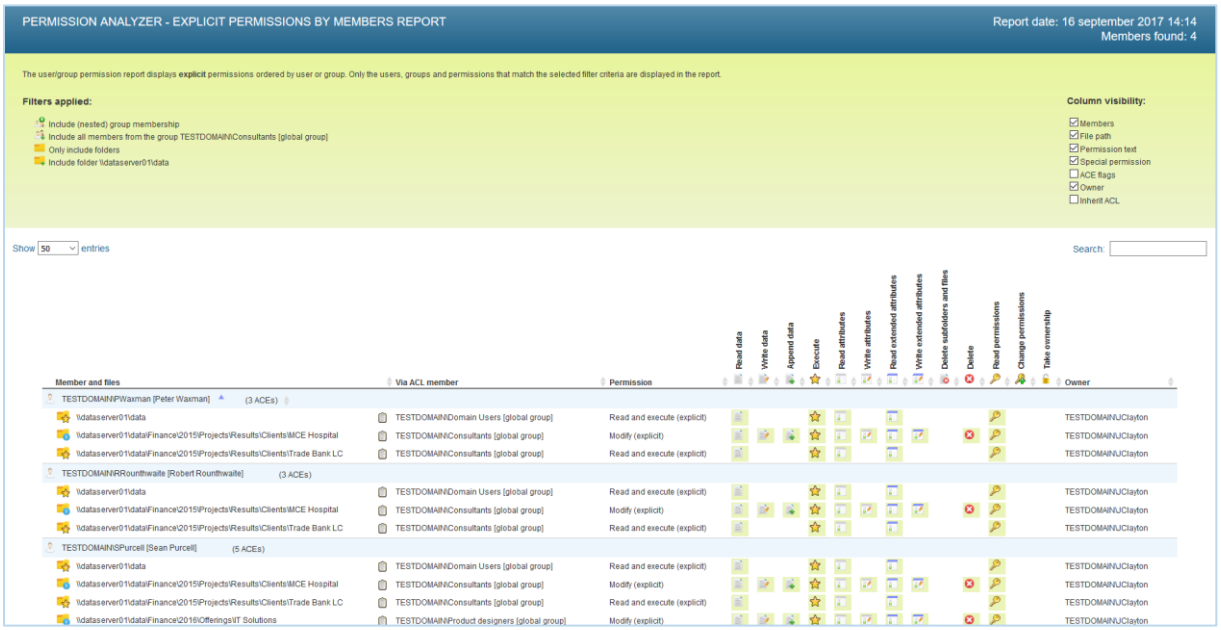
FOLDERS/FILES AND THE ACL WITH EXPANDED GROUPS SHOWING DIRECT MEMBERS AND THEIR EFFECTIVE PERMISSIONS

Same as previous report type, but the report groups in the report popped up so that the direct group members are visible. A similar report type is available to display the nested group members.



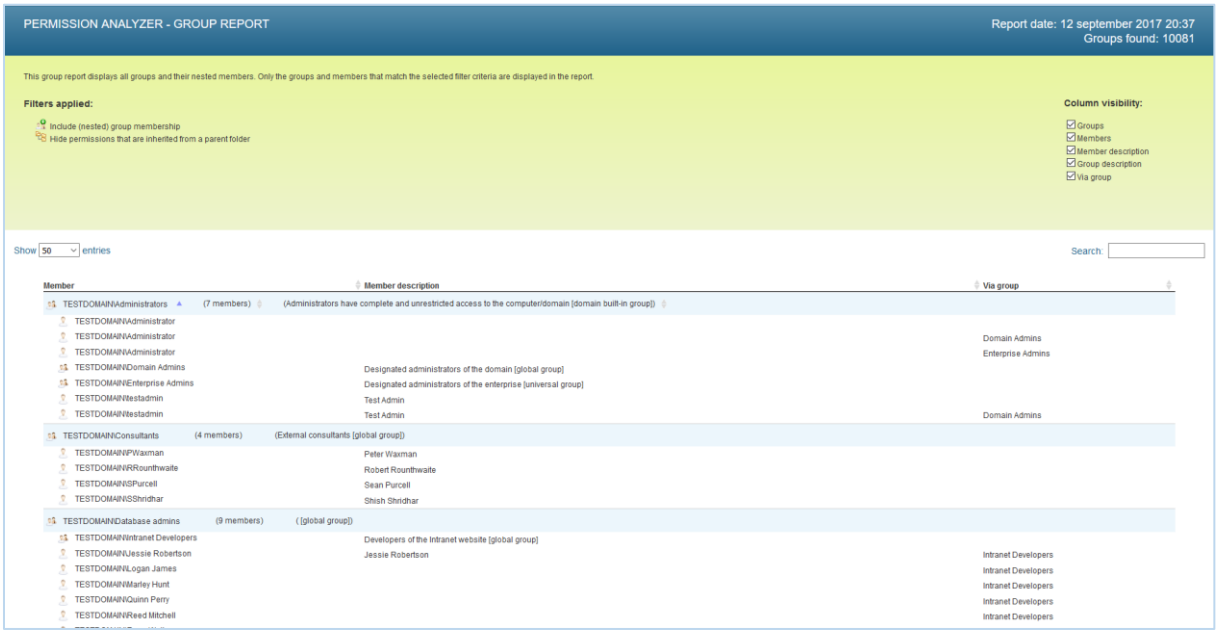
USERS AND GROUPS AND ALL THEIR EXPLICIT PERMISSIONS

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.



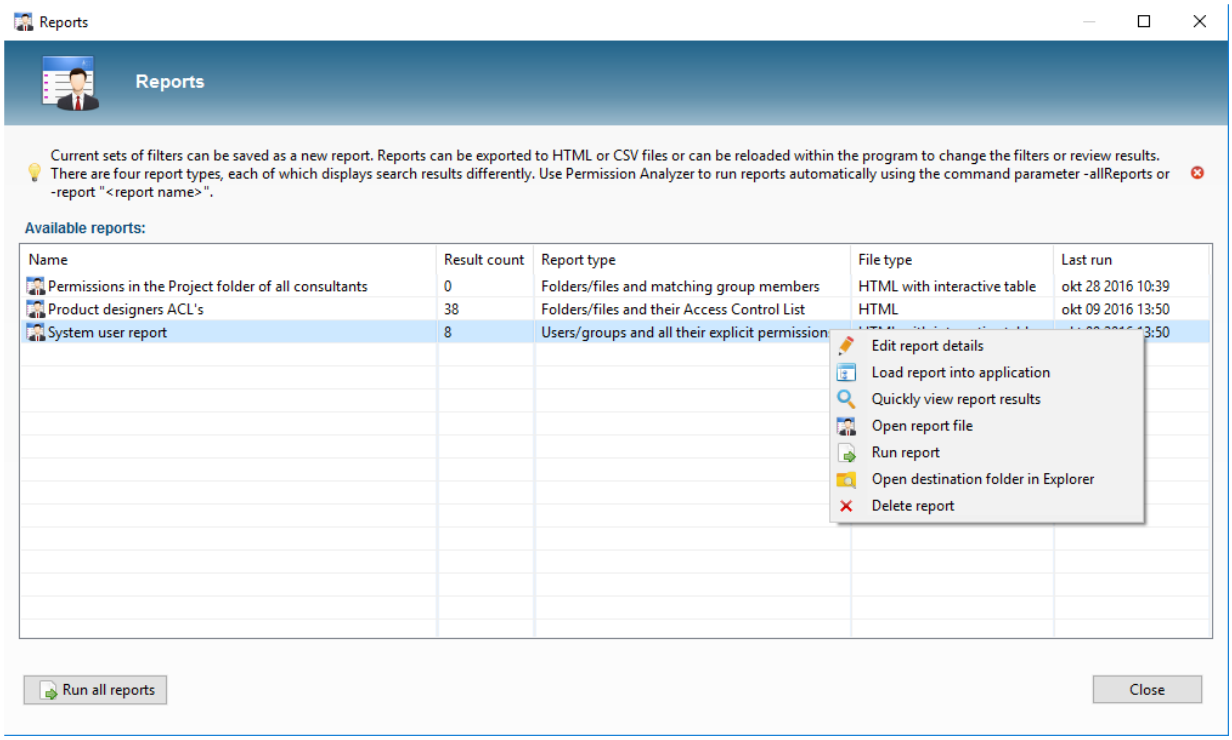
GROUPS AND MEMBERS

This report is separate from the rights and shows exclusively the groups found as well as their group members. A similar report type is available to display the nested group members. A separate report type will only display the groups that actually have permissions in the (filtered) folder tree.

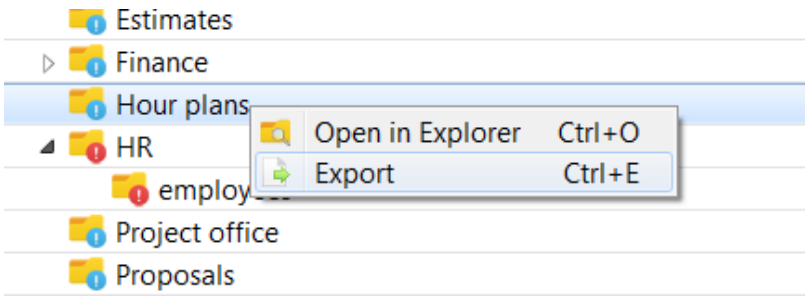


Managing reports

A list of all reports can be requesting 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.

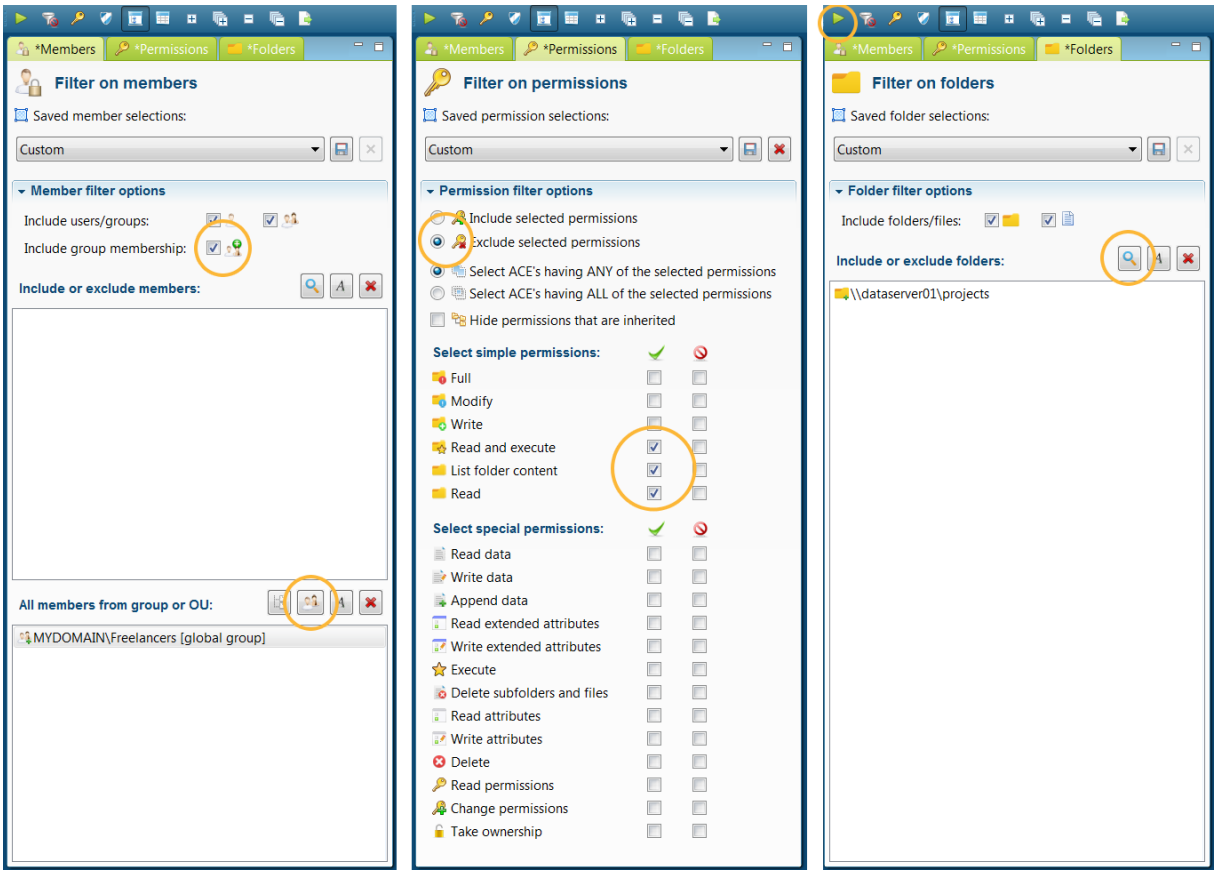
A policy is a collection of filters that display unwanted permissions. This collection can be saved as a policy where an e-mail notification is sent if the report contains more than a certain number of directories and files. That number can be configured via the ***Policy alert threshold*** value in 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. Also see the Scheduling Jobs and Reports and Export features.

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]`.

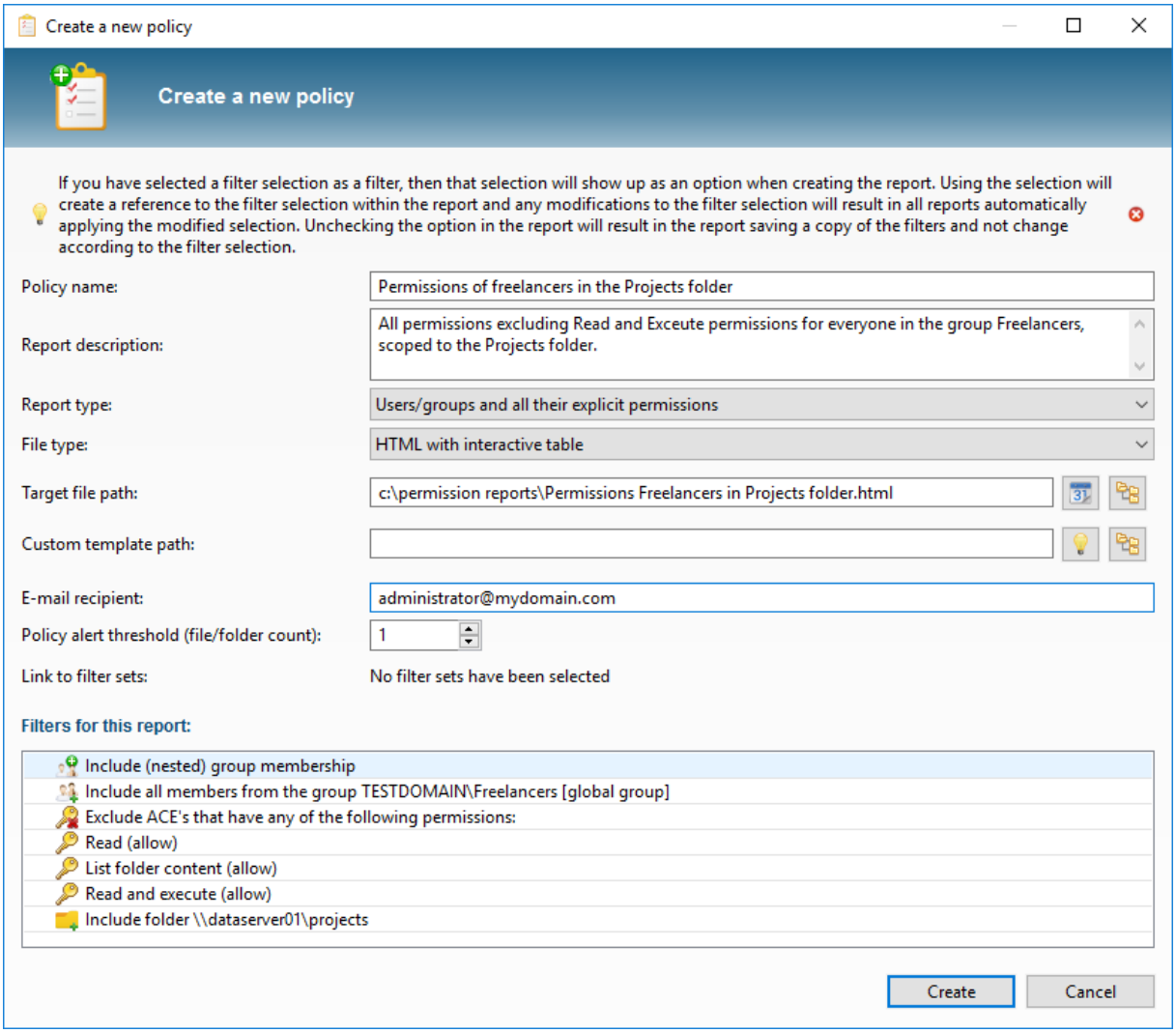
Example

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 \\datasever01\projects folder. Your search results will then be scoped to that specific folder.



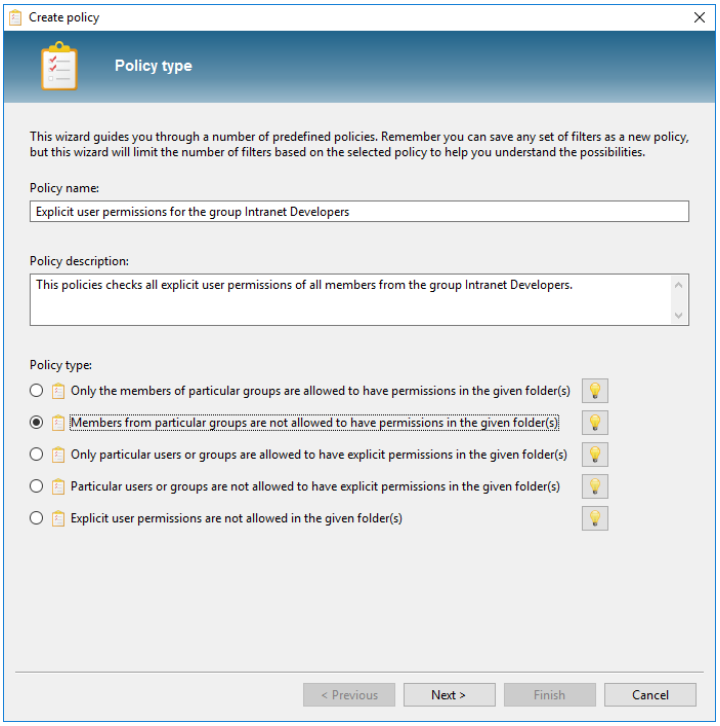
Review your search results by applying the filters using the **Apply filters** button. If necessary, add new filters, e.g. an Exclude filter for one or more users. Ideally, the result field will remain empty, meaning that no unwanted permissions have been found and that your policy has been implemented 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:



The way a policy report is shown depends on the report type you selected – see Reports and Export feature. 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.

Creating policies using the wizard

Permission Analyzer offers a wizard to help you creating the first policies. It offers a predefined set of policies and guides you through the necessary filters. You can find this wizard in the menu [Policies] > [Open the policy wizard]:



Running policies automatically

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

- **-policy “myPolicy” “myPolicy2”**: run a specific policy by name.
- **-allPolicies**: run all policies.

Permission Analyzer will close automatically after all policies have been run. See Scheduling jobs feature for more command-line options.

3.6 SCHEDULING JOBS

Use command-line parameters to run a network scan or report export automatically. Let Permission Analyzer check all your policies and send out e-mail notifications by running the application with parameters and Windows Scheduler.

Permission Analyzer is able to run network scans and export reports automatically. Simply use Windows Scheduled Tasks and a combination of application parameters:

PARAMETER	FUNCTION
-scan	Automatically initiate a network scan with the current configuration, after which the application closes down. Only checked directories and LDAP OUs will be scanned. Review results of an automatic scan in the status list in Scan View or via the Last_status_messages.csv file in the application directory.
-scanDirectories	Only scans (checked) directories and files and does not change LDAP data in the database. Review results of an automatic scan in the status list in Scan View or via the Last_status_messages.csv file in the application folder.
-scanLdap	Automatically initiates a scan of all selected LDAP OUs. Directory data in the database remains unchanged.
-password	If the application is secured with a password, than this parameter, combined with a scan or report parameter, can be used to initiate the application.
-report	Exports a specific report (by name) and can include sending out an e-mail notification. Multiple reports can be exported by inputting the parameter several times: -report “All permissions

	for John Doe" -report "All explicit permissions in the projects folder".
-allReports	Exports all reports and sends out all required e-mails if that option has been enabled for a report. Export files are automatically overwritten.
-policy	Runs a specific policy (by name) and can include sending out an e-mail notification. Multiple policies can be exported by inputting the parameter several times.
-allPolicies	Runs all policies.
-data	Overrules the default workspace folder that holds all the application preferences. You can create different configurations (domain settings, credentials, OU's and folders to scan, database path) by specifying another workspace location. For example: Permission Analyzer.exe -data "c:\workspaces\customerA"

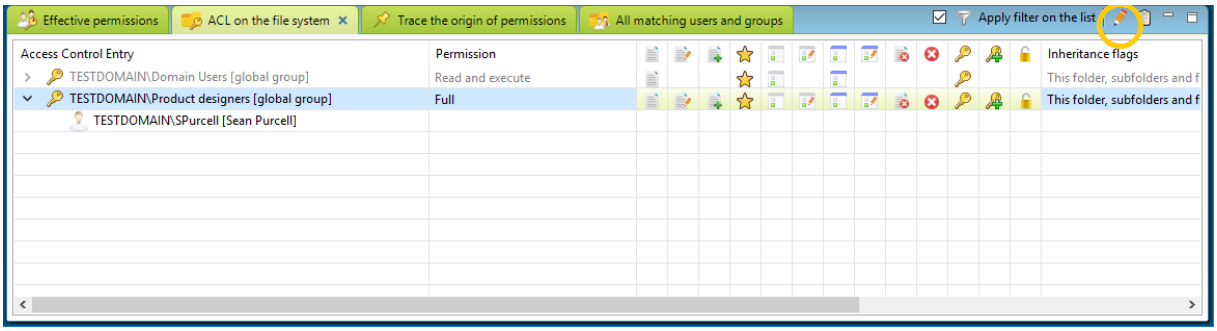
The following two parameters are only applicable when you use the -scan parameter to execute an automated scan. A scan will normally only scan the directories and LDAP containers that have been checked in the Scan View. The following two parameters can be used to overrule the checkboxes:

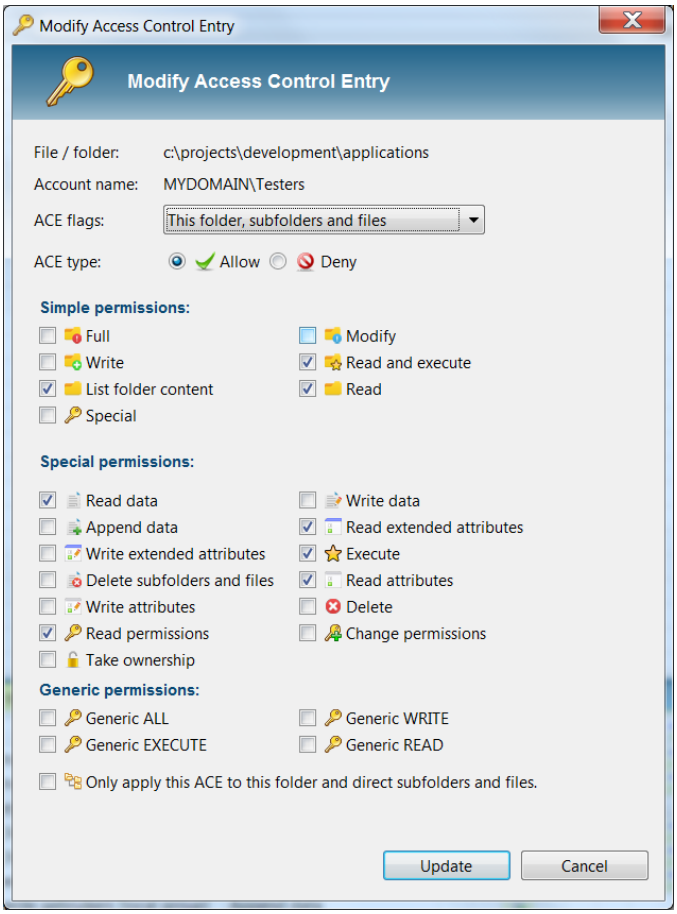
PARAMETER	FUNCTION
-forceScanAllLdapContainers	Scans all LDAP containers in combination with the -scan parameter, even if they are unchecked.
-forceScanAllDirectoryContainers	Scans all directories in combination with the -scan parameter, even if they are unchecked

3.7 MODIFYING PERMISSIONS

Change the permissions of a directory directly from within the application. Changes are directly applied to the file system and the database is updated with the changes made.

At the bottom of the search result screen is a tab that allows you to review and modify the Access Control List (ACL) of the selected directory or file. The ACL tab corresponds to the **Security tab** in Windows' file properties. Permission Analyzer in some cases will show more items in the ACL, as Windows does not show generic permissions. You will be able to only show Access Control Entries (ACE) that meet the filter criteria by ticking the checkbox "*Apply filter on ACL list*". In addition the ACL tab toolbar contains a button to directly modify the selected ACE on the file system. Permission Analyzer uses the same Windows mechanisms as the Security tab. When modifying permission through Permission Analyzer, however, information in the database is updated immediately.





3.8 DATA PROTECTION

Permission Analyzer can be secured with an application password. The password is required to open up the application and may be used to encrypt the local database using strong AES encryption.

All Permission Analyzer settings (such as LDAP connections) are automatically saved using an encryption with a built-in hidden* key. Users, however, can opt to protect their settings and access to the application with their own passwords. The application will subsequently only be accessible after start up once the correct password is entered. Passwords themselves are not saved; only a 'one-way' hash code of the password is stored. Permission Analyzer uses an advanced hash algorithm (**PBKDF2WithHmacSHA1**), making it impossible to crack or retrieve passwords.

Alternatively, you can also choose to encrypt the local database completely with both your own password as well as an **AES** encryption. This will however result in database interaction becoming 2.5 times slower.

Please keep in mind that if you encrypt the application with a password, you will have to enter the password when running automatic scans or have reports exported via Windows Scheduled Tasks. Use the application parameter ***-password mypassword***.

* Permission Analyzer's application code is encrypted and it is very difficult, but not impossible, to retrieve textual values, such as a built-in password.

3.9 EXTERNAL DATABASE

Permission Analyzer is supplied with an embedded database to store directory and group membership information. It supports a central company database, so that workstations can use the same information source or so you can create your own queries and integration.

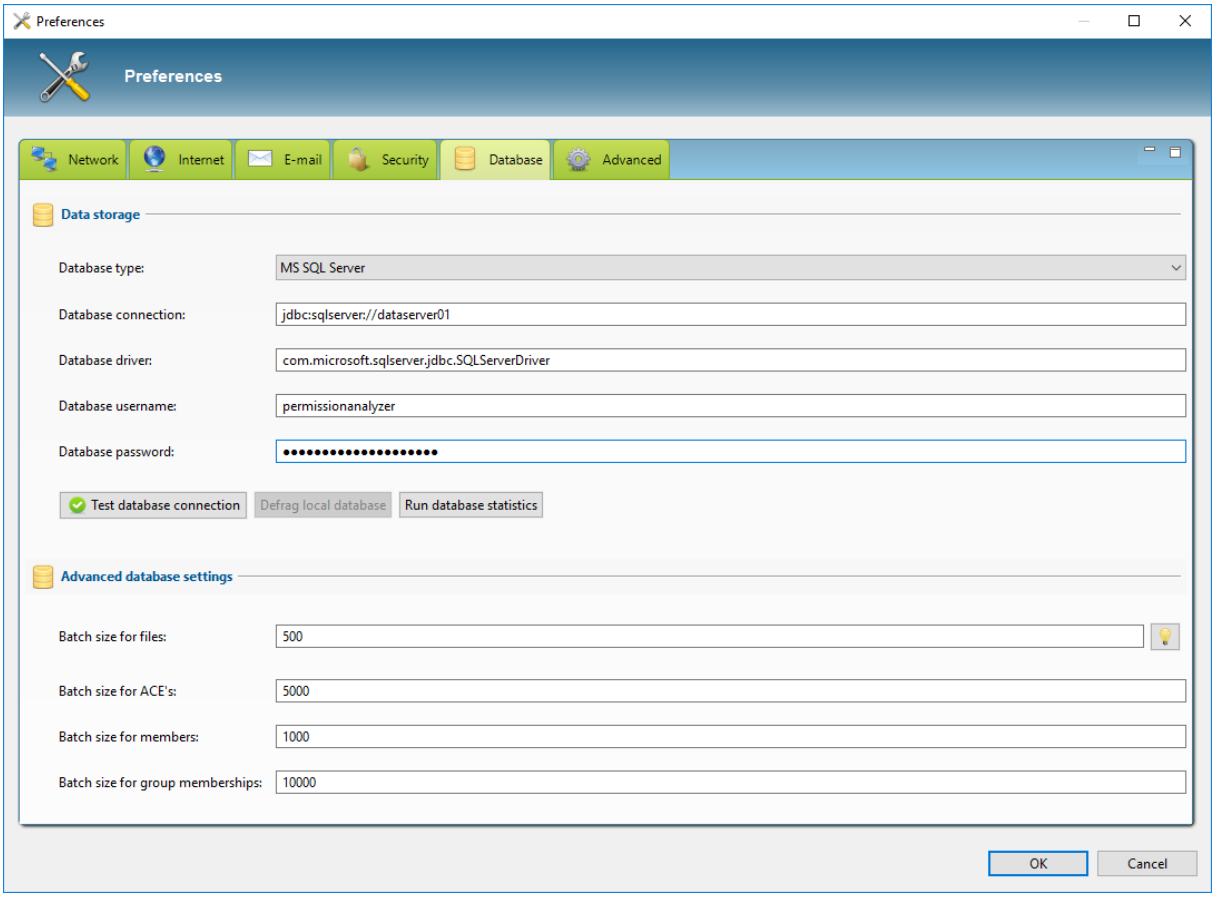
Although Permission Analyzer is supplied with a local database (H2), which is simply a file in the application directory, you can choose to use a central database to share, say, scanned information, between installations of Permission Analyzer or to run your own queries on the database. Permission Analyzer supports Oracle, DB2, MS SQL, MySQL, PostgreSQL, Derby and H2. Please note that this feature is only supported by the **Advanced** and **Enterprise** editions.

First download the Driver Pack and overwrite the External_DB_Drivers_1.0.0.jar file in the plugins directory of Permission Analyzer. Then restart the application using the **-clean** parameter. Run one of the following SQL scripts on your central database to create the tables for Permission Analyzer:

- Oracle create script
- DB2 create script
- MSSQL create script
- MySQL create script
- PostgreSQL create script
- Derby create script
- H2 create script

Once the database has been created, open **Settings**. In the **Database** tab you will then be able to select an external database and enter the connection details.

The batch size in the advanced database settings indicates the number of records that is being sent to the database at once. It is a tradeoff between speed, memory usage and the size of transaction logs in the database. The larger the batch size, the more memory and required space for the transaction log it will need.

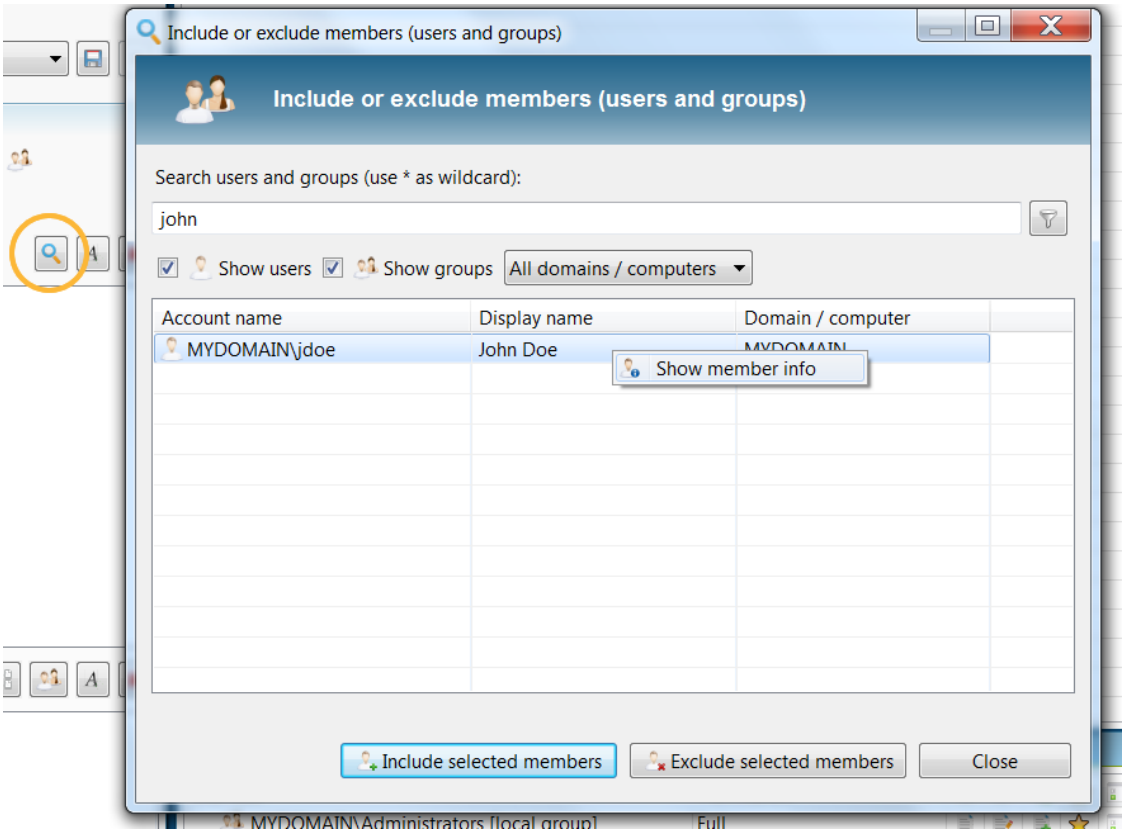


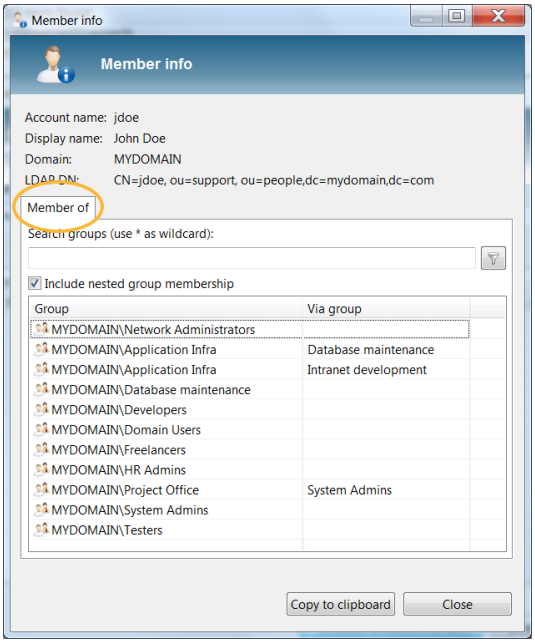
3.10 OTHER FEATURES

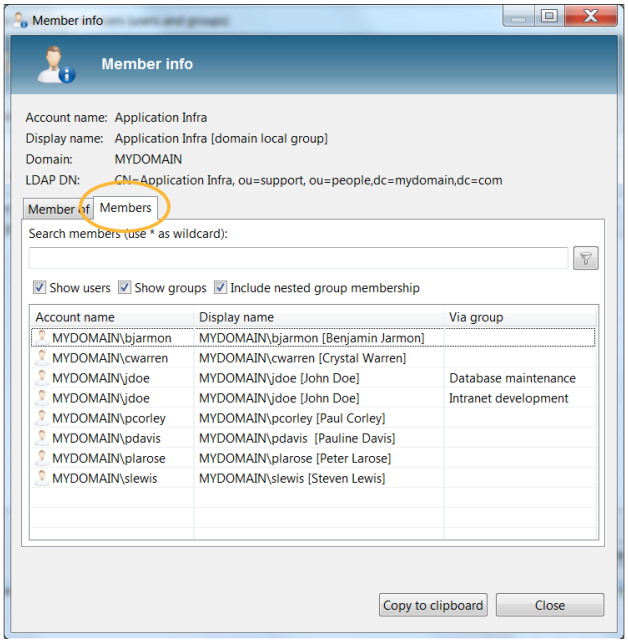
View member info and search for nested group memberships, modify LDAP attributes that are being used and make use of the update service delivered by Permission Analyzer.

Showing member info

You will be able to request the details of a member or group at various points throughout the application: in the ACL view, Trace view, Member filters or search window for member selection. The member dialogue window shows both **memberOf** data as well as the **members** in the case of a group. In both cases **nested** memberships will also be shown.

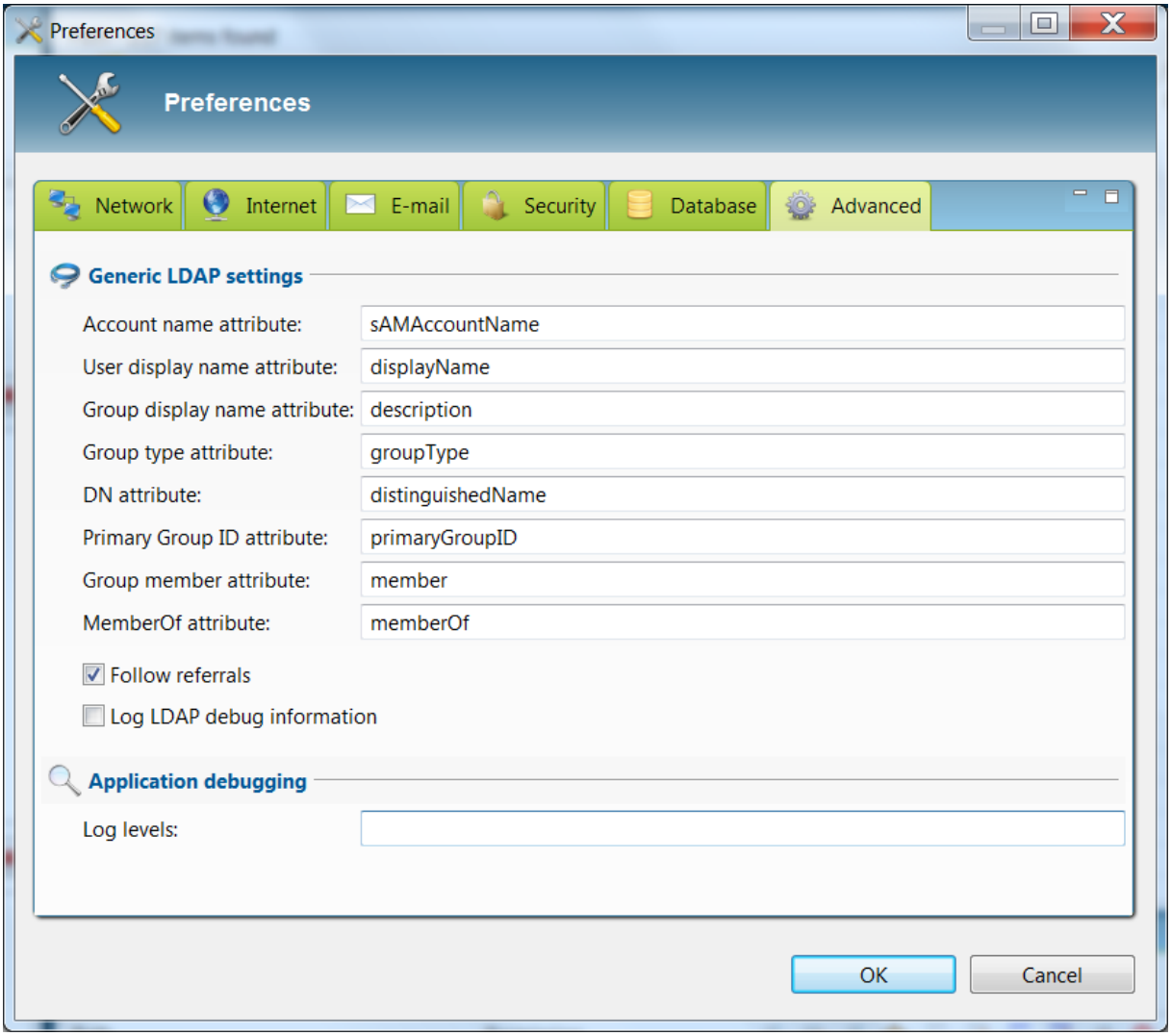

Include or exclude members (users and groups)
Include or exclude members (users and groups)
Search users and groups (use * as wildcard):
john
Show users
Show groups
All domains / computers
Account name
Display name
Domain / computer
MYDOMAIN\jdoe
John Doe
Show member info
Include selected members
Exclude selected members
Close


Member info
Member info
Account name: jdoe
Display name: John Doe
Domain: MYDOMAIN
LDAP DN: CN=jdoe, ou=support, ou=people,dc=mydomain,dc=com
Member of
Search groups (use * as wildcard):
Include nested group membership
Group
Via group
MYDOMAIN\Network Administrators
MYDOMAIN\Application Infra
Database maintenance
MYDOMAIN\Application Infra
Intranet development
MYDOMAIN\Database maintenance
MYDOMAIN\Developers
MYDOMAIN\Domain Users
MYDOMAIN\Freelancers
MYDOMAIN\HR Admins
MYDOMAIN\Project Office
System Admins
MYDOMAIN\System Admins
MYDOMAIN\Testers
Copy to clipboard
Close


Member info
Member info
Account name: Application Infra
Display name: Application Infra [domain local group]
Domain: MYDOMAIN
LDAP DN: CN=Application Infra, ou=support, ou=people,dc=mydomain,dc=com
Member of
Members
Search members (use * as wildcard):
Show users
Show groups
Include nested group membership
Account name
Display name
Via group
MYDOMAIN\bjarmon
MYDOMAIN\bjarmon [Benjamin Jarmon]
MYDOMAIN\cwarren
MYDOMAIN\cwarren [Crystal Warren]
MYDOMAIN\jdoe
MYDOMAIN\jdoe [John Doe]
Database maintenance
MYDOMAIN\jdoe
MYDOMAIN\jdoe [John Doe]
Intranet development
MYDOMAIN\pcorley
MYDOMAIN\pcorley [Paul Corley]
MYDOMAIN\pdavis
MYDOMAIN\pdavis [Pauline Davis]
MYDOMAIN\plarose
MYDOMAIN\plarose [Peter Larose]
MYDOMAIN\slewis
MYDOMAIN\slewis [Steven Lewis]
Copy to clipboard
Close

Configuring LDAP attributes

Permission Analyzer makes use of a number of standard LDAP attributes to retrieve member information and group relations. These attributes can be modified if you wish to use other fields. By enabling the option "Follow referrals" the application automatically resolves LDAP referrals sent by the domain controllers. The option is default disabled because it may cause errors when those referrals cannot be reached (they point to other domain controllers for example).



Update service

Check for updates quickly at any time via [Help] > [Check for updates]. If there is no Internet connection available you can use the offline update package on the Download page, which can be downloaded from a different machine. This package contains all the required artifacts to update your application to the latest version.

4. Using PowerShell scripts

PowerShell is a native Microsoft scripting solution, which allows you to scan the ACL's of directories and files. PowerShell scripts are executed on the remote server (if necessary) and the result is saved locally. So instead of scanning the network using Permission Analyzer, you can use a PowerShell script to export all the ACL information to a text file which can be imported into Permission Analyzer.

Execute a command-line and type "powershell", you should see a command prompt that starts with "PS". Copy and paste one of the following scripts to the command-line to export permissions:

PowerShell script to export the ACL of all (sub)directories and files to a text file:

(you can also use a network share as path, this will run the script locally on the remote server)

```
Get-ChildItem "C:\MyFolder" -Recurse | Sort-Object FullName | %{
$Path = $_.FullName
$IsDirectory = $_.PsIsContainer
(Get-Acl $Path) | Select-Object `
    @{n='Path';e={ "$Path, d=$IsDirectory" }},
      @{n='Access';e={ [String]::Join("`n", $( $_.Access | %{
            "$($_.IdentityReference), $($_.AccessControlType),
$($_.IsInherited), $($_.InheritanceFlags), $($_.PropagationFlags),
$($_.FileSystemRights)" })) }}
} | Format-list | Out-File -FilePath C:\temp\permission_export.txt -
Encoding UTF8
```

PowerShell script to exclude files (and only export directories):

```
Get-ChildItem "C:\MyFolder" -Recurse | Sort-Object FullName | ?{
$_.PsIsContainer } | %{
$Path = $_.FullName
$IsDirectory = $_.PsIsContainer
(Get-Acl $Path) | Select-Object `
    @{n='Path';e={ "$Path, d=$IsDirectory" }},
      @{n='Access';e={ [String]::Join("`n", $( $_.Access | %{
            "$($_.IdentityReference), $($_.AccessControlType),
$($_.IsInherited), $($_.InheritanceFlags), $($_.PropagationFlags),
$($_.FileSystemRights)" })) }}
} | Format-list | Out-File -FilePath C:\temp\permission_export.txt -
Encoding UTF8
```

PowerShell script to exclude inherited permissions:

```
Get-ChildItem "C:\MyFolder" -Recurse | Sort-Object FullName | %{
$Path = $_.FullName
$IsDirectory = $_.PsIsContainer
(Get-Acl $Path) | Select-Object `
    @{n='Path';e={ "$Path, d=$IsDirectory" }},
      @{n='Access';e={ [String]::Join("`n", $( $_.Access |
?{!$_.IsInherited} | %{
            "$($_.IdentityReference), $($_.AccessControlType),
$($_.IsInherited), $($_.InheritanceFlags), $($_.PropagationFlags),
$($_.FileSystemRights)" })) }}
} | Format-list | Out-File -FilePath C:\temp\permission_export.txt -
Encoding UTF8
```

The resulting text file has the following format:

```
Path   : <path>
Access : <member>, <Allow/Deny>, <inherited ACE>, <inheritance flags>,
<propagation flags>, <permissions>
         <member>, <Allow/Deny>, <inherited ACE>, <inheritance flags>,
<propagation flags>, <permissions>
```

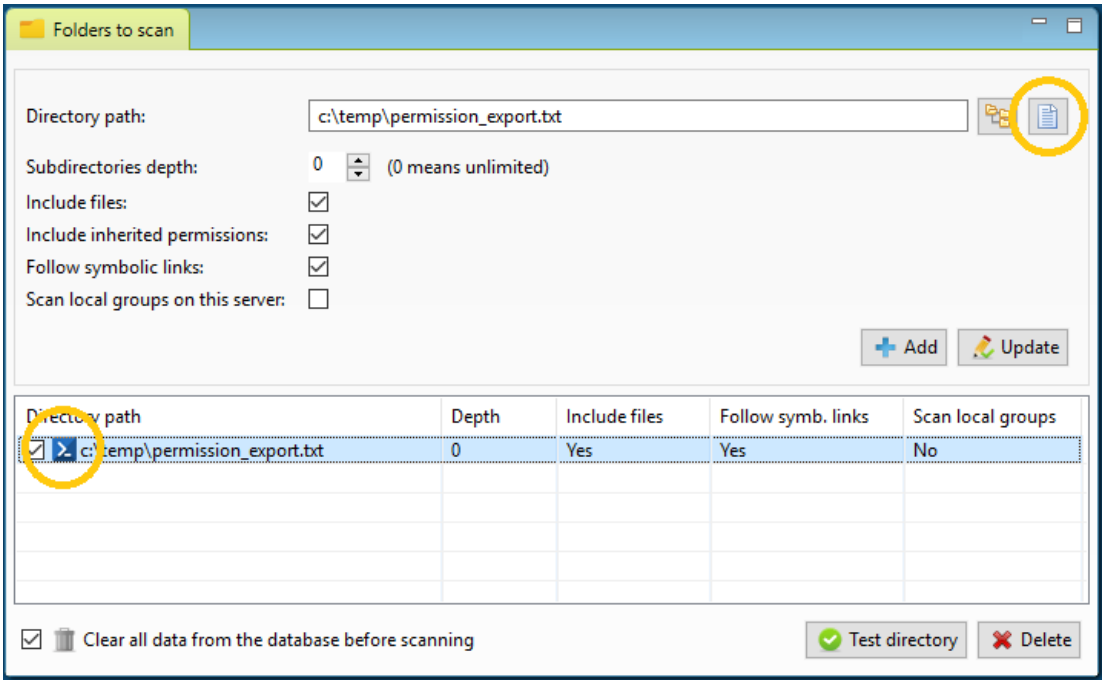
For example:

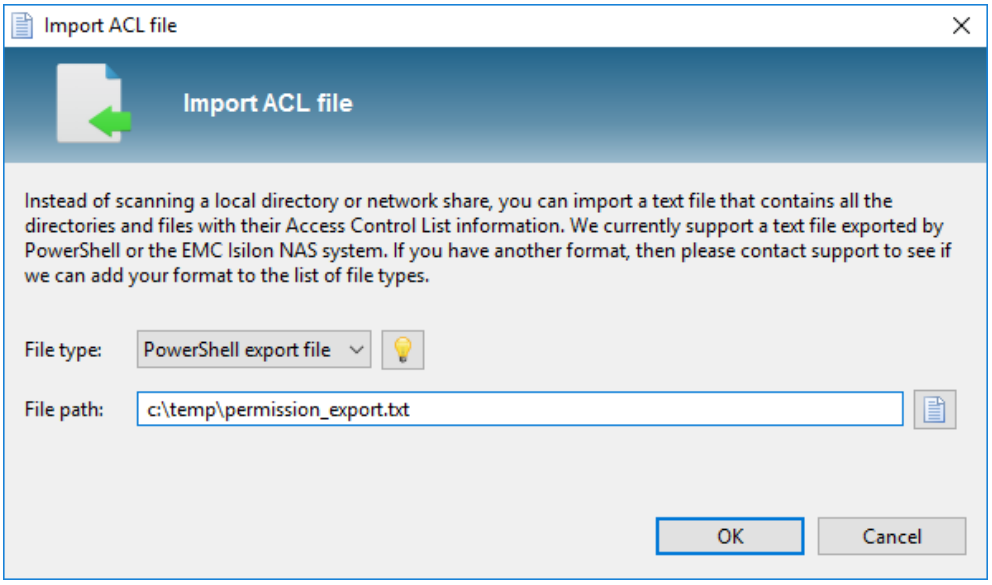
```
Path   : \\server01\Data\Projects\Finance, d=True
Access : YOURDOMAIN\Domain Admins, Allow, True, None, None, FullControl,
Synchronize
         YOURDOMAIN\pbrandon, Allow, True, ContainerInherit, InheritOnly,
ReadAndExecute, Synchronize
         YOURDOMAIN\gwatson, Allow, True, None, None, FullControl,
Synchronize
         YOURDOMAIN\Project Office, Allow, True, ContainerInherit,
ObjectInherit, InheritOnly, Modify, Synchronize
         YOURDOMAIN\Finance Auditors, Allow, True, None, None, FullControl,
Synchronize

Path   : \\server01\Data\Projects\Finance\Results, d=True
Access : YOURDOMAIN\Domain Admins, Allow, True, None, None, FullControl,
Synchronize
         YOURDOMAIN\pbrandon, Allow, True, ContainerInherit, InheritOnly,
ReadAndExecute, Synchronize
         YOURDOMAIN\gwatson, Allow, True, None, None, FullControl,
Synchronize
         YOURDOMAIN\Project Office, Allow, True, ContainerInherit, None,
None, Modify, Synchronize
         YOURDOMAIN\Finance Auditors, Allow, True, None, None, FullControl,
Synchronize
```

Importing the PowerShell results

The text file that has been created can be imported into Permission Analyzer:





You can now scan the content of the text file the same you would scan a directory or share. Use the same command line options ("-scan") to scan the text file periodically using Windows Scheduled Tasks. Note that Permission Analyzer scans ACL's more than twice as fast as the provided PowerShell scripts.

Tip: Zip the text file to save storage and import the zip file directly into Permission Analyzer, the application will recognize the zip extension.

Permission Analyzer also supports files exported from a **EMC Isilon NAS**. See the Help button in the import dialog for more information.

5. Licensing model

Permission Analyzer's licensing model operates on an installation basis and consists of a number of editions based on company size, varying in the features they offer. Each **installation** of Permission Analyzer will require a separate license. The number of users and groups per edition will constitute the maximum number to be scanned by Permission Analyzer. These numbers are the sum of the unique members found in the Access Control Lists on the file system and the LDAP Organizational Units you select to determine (nested) group membership. This does not necessarily have to encompass the entire domain, but can be limited to certain OUs. Only those members and groups will then be available to the application, supplemented by the members attributed to a directory directly.

Licenses will be valid for **1 year** and automatically entitle the purchaser to tech support and updates. A license can be moved three times by deactivating an active license and reactivating it on a new device.

Permission Analyzer's **trial** version is limited to 2 root directories (unlimited depth of sub directories), 3 member filters and the export to HTML/CSV is limited to a depth of 3 sub directories. If you'd like to try out one of the editions, then just fill out the trial request form.

Notes:

(1) The number of servers that are scanned on directories, files and local groups. This does not relate to the number of domain controllers.

(2) Encryption is only supported for the local H2 databases supplied with the edition. Please consult the product documentation for information on encryption of other (external) databases.

(3) You will be able to use any database with a JDBC interface. Permission Analyzer automatically supports Oracle, DB2, MS SQL, MySQL, PostgreSQL, Derby and H2. Also see External Database.

TRIAL	BASIC	STANDARD
-	$ 149[99]	$ 249[99]
2 root directories	Unlimited directories	Unlimited directories
1 file server [1]	1 file server [1]	5 file servers [1]
Unlimited users	500 users	3000 users
Unlimited groups	100 groups	1000 groups
-	-	Database encryption [2]
-	-	-
DOWNLOAD	PURCHASE	PURCHASE

ADVANCED	ENTERPRISE	SCAN AGENT
$ 349[99]	$ 499[99]	$ 24[99]
Unlimited directories	Unlimited directories	Unlimited directories
15 file servers [1]	Unlimited file servers [1]	1 file server [1]
15,000 users	Unlimited users	Unlimited users
5,000 groups	Unlimited groups	Unlimited groups
Database encryption [2]	Database encryption [2]	Database encryption [2]
External DB support [3]	External DB support [3]	External DB support [3]
PURCHASE	PURCHASE	PURCHASE

6. FAQ

6.1 TECHNICAL QUESTIONS

How is Permission Analyzer installed?

The download of Permission Analyzer is a zip file that can be unpacked anywhere. The application runs from the extracted directory and no installation is needed. Please note that Windows has additional restrictions on the "Program Files" directory and that Permission Analyzer can possibly only be run as an Administrator. To avoid these problems, it's best that the application is extracted outside of the Program Files directory. To uninstall the application only the application folder needs to be deleted.

Why does the application not start?

Access denied on the workspace directory

Permission Analyzer writes data into the directory where it has been installed. If the directory is located in Program Files, Windows may decide to block the writing operations of the application. If this is the case, run Permission Analyzer as an Administrator. Right click Permission Analyzer.exe and select Run as Administrator.

What exactly is retrieved from the Active Directory?

Permission Analyzer makes use of the Active Directory to retrieve additional member attributes that are not available from the file system, e.g. the displayName and (nested) group membership. The application's scan screen will show specific Active Directory Organizational Units (OU) to be scanned and Permission Analyzer will limit the scan to those OUs. The scan will only search for items outside the OUs if they occur in the **member** or **memberOf** attributes of members in the OU. This is done to obtain a complete overview of group membership for each member of the OU(s).

Note: because a universal group can have members from domains other than the domain where the group object is stored and can be used to provide access to resources in any domain, only a global catalog server is guaranteed to have all universal group memberships that are required for authentication. On the other hand, the global catalog stores the membership (the member attribute) of only universal groups. The membership of other groups can be ascertained at the domain level. Therefore, if applicable, make sure you add both the domain controllers as your global catalogue to ensure a complete overview of group memberships. Permission Analyzer will make sure that no duplicate memberships are stored. Active Directory uses the following default ports:

389: LDAP without SSL

636: LDAP with SSL

3268: Global Catalog without SSL

3269: Global Catalog with SSL

Do I have to install the product directly on a domain controller?

No, you can run Permission Analyzer from any server or workstation within your domain, as long as you have enough permissions to read the security properties of the directories to scan and the OUs in the Active Directory.

What kind of setups are supported?

Permission Analyzer can easily be run from a workstation with a supplied database in the application folder. From the workstation different file servers can be scanned, just like the Active Directory for group information. In addition, you can use an extensive setup with scan agents and a central database to share information.

Instead of scanning a remote file system from a workstation, a Scan Agent can be used to perform a scan on the file server. Each Scan Agent will add the scanned information to the central database. A Scan Agent is a normal installation of Permission Analyzer but is activated with a cheaper Scan Agent license, with which only the scanning features of the application are activated. The progress and status messages of each Scan Agent can be viewed on, for example, a central workstation. A Scan Agent stores the status messages in the central database, which is also the way in which to communicate with an agent. Starting an agent can, as with the normal installation of Permission Analyzer, be scheduled via Windows Scheduled Tasks and application parameters such as scan.

See also Architectural setup.

Can the application scan unix/linux shares?

Yes, the application can scan shares that support the NFSv4 ACL Model using the SMB protocol. Make sure ACL's are enabled on the machine that hosts the network shares. For example, for OSX you can execute the following:

```
sudo defaults write
/Library/Preferences/SystemConfiguration/com.apple.smb.server
AclsEnabled -bool YES
```

Is there any limitation on the subfolder level or length of the file path?

In the Windows API (with some exceptions), the maximum length for a path MAX_PATH, which is defined as 260 characters. Reading the file path is no problem, but getting the security descriptor of the file fails when the file path exceeds the MAX_PATH length. Permission Analyzer has a workaround to support long file paths anyway! Whenever necessary it converts the long file path to its 8.3 short notation (file names with ~1 etc) before reading the security properties. The long file path is stored in the database along with the security info retrieved by the short path. This way you still have a readable long path including the security info.

What is stored in the database?

When performing a network scan a snapshot is made of the file system in combination with group information from the Active Directory. The database contains file names, access control entries and user and group information. The database also contains filters, reports, policies, which can be shared with several work stations by using a central database. The storage occupies approx. 1 MB per 1,000 directories/files.

The searches, reviews and reports in the "Report View" strictly use the database to show the results. The directories on the network and the Active Directory will only be accessed while running a network scan.

Can I change the location of the embedded database?

Yes, just move the files **H2DB.h2.db** and **H2DB.trace.db** to another location on your hard disk and change the database path in the settings of the application.

What databases are supported?

By default, the application uses a supplied H2 database which is included, in the form of a database file in the application directory. In the preferences in the application the following databases can also be used: Oracle, MSSQL, DB2, MySQL, PostgreSQL and Derby. By using an external database server the scanned information, reports, and filters can be shared between workstations, and potential Scan Agents can scan a local file system in parallel and save the information in the database. The application supports basically any database with a JDBC driver, contact support if the desired database is not listed.

How long does it take to scan the files?

This depends a lot on the network performance, the file servers or local file system and whether or not an external database is used. Scanning local files with a local database

scans about 25,000 files per minute and occupies 1 MB database storage per 1,000 files. As the database size increases the scanning speed drops, since with each new row the database needs to update a number of growing indexes.

Tip: use Scan Agents on the file servers to increase speed.

Does the application require an Internet connection?

No, you can use an Internet connection to activate your license automatically, but you can also use our form on the website to create an offline activation file based on your license.

I've discovered a bug. How can I report it?

A dialog window can be opened within the application, allowing you to send a direct message to our tech support team. The dialog window also allows you to send the application log in zip format. Go to [Help] > [Contact support]. Make sure you've configured a valid SMTP server in the application settings before sending out the e-mail.

6.2 FUNCTIONAL QUESTIONS

Can group members be included in the reports?

Yes, the recent version of Permission Analyzer has a number of new reports with which groups 'unfolded' in the HTML or CSV report are included. At this point the following report types can be selected:

Folders/files and the sum of their permissions
A list of directories and files that meet the filter criteria. Per directory, only the effective rights of all Access Control Entries that are found on the basis of the filters.

Folders/files and their Access Control List
Instead of adding up all the rights, Access Control Entries (users and groups) are displayed separately per directory or file in this report.

Folders/files and the ACL with expanded groups showing direct members and their effective permissions
Same as previous report type, but the report groups in the report popped up so that the direct group members are visible.

Folders/files and the ACL with expanded groups showing nested members and their effective permissions
Same as the previous report type, but in addition to direct group members also the nested members of a group are displayed.

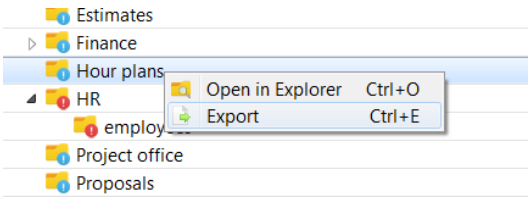
Users/groups and all their explicit permissions
This report is laid down per user/group instead of directory/file. For each user or group the directories and explicit rights are displayed.

Groups and members
This report is separate from the rights and shows exclusively the groups found as well as their group members. A separate report type will only display the groups that actually have permissions in the (filtered) folder tree.

For more information, see also the Reports.

How can I export the overviews?

The application supports exporting to HTML or CSV. A quick export can be done via the context menu of a directory or the Export button in the application toolbar:



In order to create a periodic export a report can be used. A random set of filters can be saved as a new report. In a report, among other things, the file format, the destination path and the way of presenting are configured. A report can be loaded at any time in the application or be exported to HTML or CSV. See also Reports and command-line parameters.

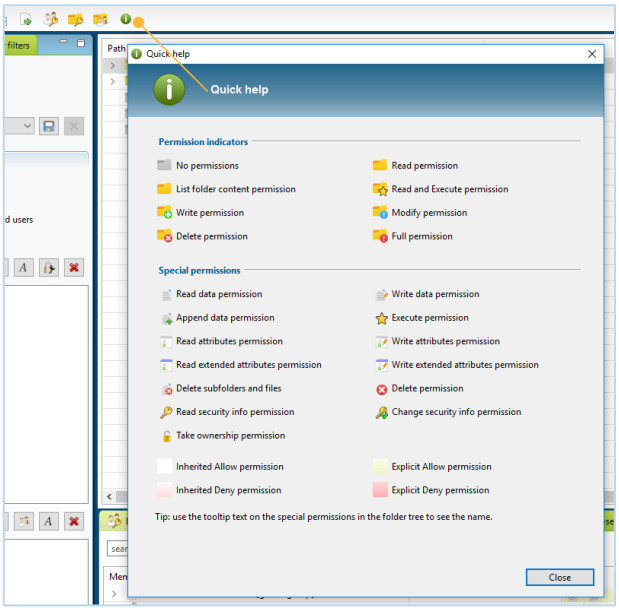
Can I schedule a scan and/or export on a daily basis?

A set of filters can be saved as a new report, where the file path (with possible timestamp) can be configured per report. Using Windows Scheduled Tasks and different application parameters Permission Analyzer can be launched automatically, a scan can be run and reports can be exported. See command-line parameters.

Do you support nested group memberships?

Yes, group memberships are stored in the database during the network scan, from the Active Directory. The reviews show the standard rights of nested group memberships, these rights can be excluded with the check mark "Include group memberships" on the Members tab on the left of the outline. By unchecking this option the explicit rights of a user or group are displayed.

What are those icons and colors in the folder tree?



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.

What filters can I apply?

Permission Analyzer provides a highly comprehensive collection of filters. The filters are divided into three categories, namely Members, Permissions and Folders. Each category can be found as a tab on the left of the outline. In the Member tab a list of users/groups can be added as an Include or Exclude keyword filter. That way only the rights for those users appears in the folder tree. It is even possible to select a group from which all members are included or excluded in the overview. The nested groups of each group member are included in the overview. This allows a quick bulk review to be done on a large group of users. The folder tree shows at a glance where the unwanted rights are. With the tabs at the bottom of the folder tree it's possible to see which users have been found. The filters can be added as an Include filter or Exclude filter.

Can I get all the folders that are not accessible by a particular account?

The Exclude filter on a username will only exclude that user from the overview. However, in order to show the directories to which a user has no rights, the nested group memberships of the outline should also be excluded. See following PDF for some simple steps to take to add the groups of a user as Exclude: Filter for folders not accessible by a particular user.pdf

6.3 LICENSING QUESTIONS

How many licenses do I need?

A Permission Analyzer license is tied to one machine, either a server or a workstation. From one machine different servers can be scanned, multiple licenses apply to different workstations with an installation of Permission Analyzer, or in the case of Scan Agents (a cheaper license option) where Permission Analyzer is installed on each file server to run a local scan and add the information to a central database. You should select the appropriate edition of Permission Analyzer based on the number of groups and users you are scanning on the file system and Active Directory.

What edition do I need?

The edition of Permission Analyzer depends on the number of users and groups that is scanned in the Active Directory (the Organizational Units selected in the scan window of the application). The following list gives an indication of the edition that could apply:

- **Basic**: 1 file server / 500 users / 100 groups.
- **Standard**: 5 file servers / 3,000 users / 1,000 groups and support for encryption of the included (embedded) database supplied.
- **Advanced**: 15 file servers / 15,000 users / 5,000 groups and support for an external database such as MS SQL Server.
- **Enterprise**: Unlimited file servers, users and groups plus support for an external database such as MS SQL Server.
- **Scan Agent**: Suited for local scan of a single file server.

How can I move my license?

A license is linked to an installation of Permission Analyzer. That's why it's important to deactivate an old, previous installation. This can be done automatically online or

manually through the website. Open [Help] > [License information] and select [Deactivate license]. You will now be able to activate the license on another device.

How can I get a written quote?

You can easily create a quote yourself in the order process. To do so, place the desired products in the shopping cart, proceed to checkout, enter the required data in the order form and select your preferred payment type. As usual, you can review all of the information you entered again on the confirmation page. Then, instead of completing the order using the button at the bottom of the confirmation page, click the “Save as quote only” link.

We will then process the information you entered and send you an e-mail confirmation. This e-mail contains your quote details, a link to the login page of the “My Account” area in the Customer Care Center and a PDF attachment with the non-binding quote.

You now have 14 days to review and edit the quote in the “My Account” area in the Customer Care Center. Log in with your user ID and password and click the ‘Quote overview’ tab. There you will find an overview of your quotes where you can view the details, delete the quote or order the products in the respective quote by clicking ‘Process as order’. You will then be redirected to the order process automatically via a secure connection.

As you have already entered your information, we can process your order immediately. A description of the subsequent steps is given in the answer to the question ‘What will happen after I place my order online?’

If you do not place an order within 14 days, the quote will be deleted automatically after this 14-day period.

What is Permission Analyzer’s ordering process like?

Permission Analyzer’s orders are processed by our sales agent Share-It, one of the biggest software sales agents worldwide. Share-It supports the following payment methods: credit card (Visa, MasterCard, American Express, JCB and Diner’s Club, as well as Maestro debit cards issued in the UK), wire transfer, check, PayPal and WebMoney. When you pay by credit card you will immediately receive the license file(s) by e-mail.

The trial version is very limited. Can I test a full version?

Sure! Just fill out our online form to request a trial license for a specific edition.

Can I sign up as a reseller?

Yes, you can register as a reseller or affiliate through our sales agent, Share-It. As an affiliate, you can market Permission Analyzer by placing links on your website to the relevant product pages on the publisher's website. You will receive a commission for each sale of these products via your website. As a reseller you will be able to quickly and easily place online orders for your customers for products by "Perdemia". As a reseller, you can log in to the publisher's website without having to re-enter your personal information for every order.

Register as affiliate
Register as reseller

7. Application version history

2.3.6 **2018-06-25**

- Added a new report type "Folder/files and users with their effective permissions". It is similar to the ACL report, but it hides group information and shows all users directly under the folder/file.
- Added the option to configure your own logo in the HTML reports (set your logo in the application preferences).
- Added a simplified version of most of the HTML reports, suitable for management overviews. Just select the checkbox "Simple presentation" in the report details, it will leave out some of the columns, checkboxes and filter information.
- Special permissions are default hidden in the HTML reports.
- Added a preference to configure the CSV separator, since Excel expects a semicolon while the default character is a comma.

2.3.5 **2018-02-13**

- Added a new filter option to invert the matching folders in the overview. Enabling this checkbox in the Folder filter panel will display all the folders that do not match the filter criteria. This can be useful to create an overview of all folders that do not have a particular member in the ACL list. For example, include a member filter Administrators, and check the option Invert matching folders. This will display all folders that don't have the Administrators group on them. The exclude member filter will not work in this case, because it will just exclude the Administrators permissions from the overview, but the folders will still appear since they have other permissions that match the filter.

2.3.4 **2017-09-16**

- Added a wizard to create new policies
- Performance improvements in the Report View when using an external database
- Reorganized the list of items to scan (servers, local directories, shares, etc.)

- Added a new filter for disabled users
- Added two new report types:
  - *Groups that have permissions in the folder tree and their direct members*
  - *Groups that have permissions in the folder tree and their nested members*

2.3.3 **2017-01-29**

- Added file owners to the overviews, including a filter on the account name of an owner
- Added the option to display ownership ratio in the overview (this is default disabled because of the performance impact, but can be enabled in the preferences)
- Added the option to change the ownership and file inheritance in the context menu of the folder tree
- Added two new report types: "Groups and nested members" and "Groups and direct members"
- Added the option to add a server name in the scan list (instead of a directory or network share). The application will scan all the shares of that server, except the hidden drives like c$ and the shares admin$, print$ and ipc$. Use the command-line parameter "-includeSharedDrives" to scan hidden drives like c$ as well.

2.3.2 **2016-11-14**

Added efficiencies in the scanning process, making scanning much faster.

2.3.1 **2016-11-05**

Added the feature to import a text file generated by a given PowerShell script.

2.3.0 **2016-10-07**

- Created a better separation between reports and policies, including a dialog that shows the current status of all your policies.
- Added a wizard to create a new policy
- Renamed the report types and added a new report type that orders the data by user/group

2.2.1 **2016-08-14**

Added two new tabs in the Report View. One tab with the members of the selected directory and their effective permissions and one tab that displays all users and groups that have been found in the directory tree, including their ACE's.

2.2.0 **2016-06-19**

- Support for Scan Agents that run locally on the file server and submit their information to a central database. The previous version would always truncate the existing data from the database, this is now configurable in the Scan View.
- A new checkbox has been introduced in the Scan View to exclude inherited permissions from the scan. So besides excluding them in the overview, they can now be excluded from the database completely. This means the database will be a lot smaller (and faster) in that case.
- The export reports contain a new column with the number of members per directory.
- Uchecking the member column in the HTML report will now hide the whole ACE row.
- The HTML reports have a new icon to copy the file path quickly to the clipboard.

2.1.2 **2016-05-06**

Added support for long file paths (Windows MAX_PATH limitation).

2.1.1 **2016-04-03**

A new panel has been added to display all members that have been found in the results after the filters are applied.

2.1.0 **2016-02-13**

A new audit dashboard with 18 charts showing statistics about your network users and groups, permissions and files.

2.0.0 **2015-10-10**

A complete renewal of version 1.x