Enterprise Permission Reporter

Version 3.5.0.2

Manual

NETsec

14 August2012

What is EPR? 4
Installation 5
Where do I install EPR? 5
Store reports to file 5
Proposals 5
System Requirements 5
Setup 6
Configuration 7
Store System 8
Notification 9
Service Configuration 10
EPR Structure 11
File System Report Definitions 13
The First Report 13
Filtering, Sorting, Exporting 20
Filtering 20
Exporting 21
Sorting 21
Delta Reports 22
Scheduling 28
Monthly Compliance Report 28
Weekly Delta Report to Data Owners 29
Active Directory Report Definition 33
Tasks: 33
The First Report 34
Weekly Delta Report to the Head of the IT-Department 38
Membership Watch Report 42
Tasks: 42
The First Report 42
Licensing 46
Trial License 46
Add a License 46

Support **47**
Blogs **47**

What is EPR?

EPR (Enterprise Permission Reporter) is our NTFS and Active Directory permissions reporting solution. EPR will assist you to meet all challenges you may face regarding regulatory compliances such as HIPAA, FDA, PCI or SOX.

EPR lets you control, document and review all your file system, Active Directory permissions with ease. With EPR it is also possible to watch for membership changes within AD groups.

Installation

Where do I install EPR?

You can install EPR on any server or workstation within your Windows domain. The computer you install EPR on must have access to the network if you plan on tracking permission changes on remote computers.

Store reports to file

If you test EPR you can use CSV files to store the reports, however if you wish to use EPR in production we strongly recommend an SQL Server / SQL Express to store the report data.

Proposals

- Permissions
  - The account running EPR and the EPRScheduleService should be able to:
    - Read all files and folder that are to be analyzed
    - Read all Active-Directory object security descriptors that are to be analyzed
    - Write the results to the medium you want to store the Reports (SQL-database or CSV File)
- Store type File
  - You should use File as a testing and evaluation Mode. File will lack Features such as sorting and may have significant performance differences to SQL.

System Requirements

Enterprise Permission Reporter does not need to run on a Domain Controller or specific server. We recommend placing Enterprise Permission Reporter on a machine of the domain with high bandwidth, so that the access right assessment occurs quickly when analyzing over LAN.

It is also possible to install EPR in a virtual environment. Here is a complete list of what is necessary for the successful usage of EPR.

1. Processor
   a. A minimum of a dual-core processor is required
      i. Note: EPR will run on single core systems; however it will take longer to process the information gathered during the reports.
   b. We recommend a quad-core processor.
2. Memory
   a. A minimum of 2 GB RAM is required to run EPR
   b. We recommend 4 GB RAM to run EPR fluidly, especially if you analyze a lot of folders concurrently.
3. Disk Space

    a. EPR requires about 200 MB of HDD space, excluding the generated reports which vary in size.
4. Operating System
    a. EPR is supported on the following Operating Systems:
        i. Windows Vista
        ii. Windows 7
        iii. Windows 8
        iv. Windows Server 2003 SP2
        v. Windows Server 2003 R2
        vi. Windows Server 2008
        vii. Windows Server 2008 R2
        viii. Windows Server 2012
5. Other Requirements
    a. .NET Framework 4
    b. All recommended Windows Updates
6. SQL Server Versions
    a. All SQL Editions 2008 and above are supported (including Express)
7. Service Account Settings
    a. Service Account is also in the Role db_creator (When using the SQL Server to save your reports)

If you plan on using EPR with an SQL Database, you will need to have an SQL Server 2008 or newer installed within the domain. If you wish to send summary emails you will need to have an SMTP service (e.g. Microsoft Exchange Server) installed within your domain.

Setup

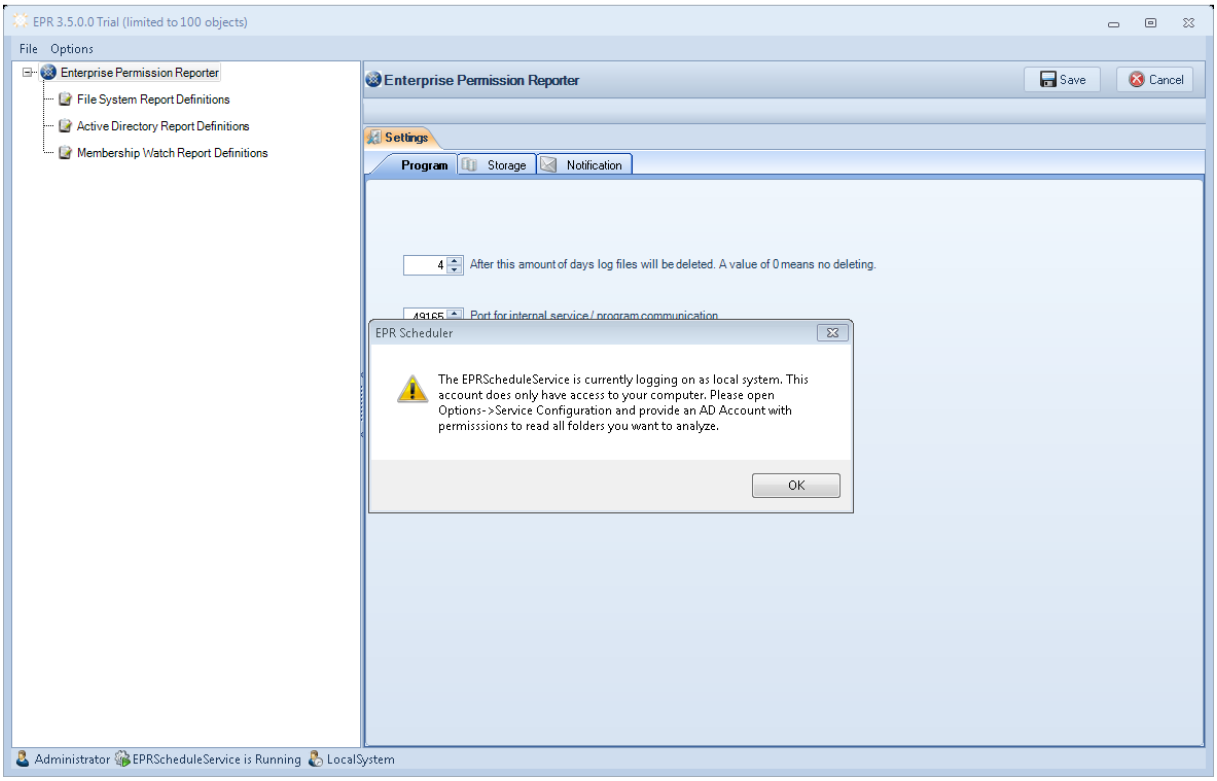
This will install and register all the components necessary to run Enterprise Permission Reporter on your server or workstation. Setup will create a folder NETsec\Enterprise Permission Reporter in the start menu, and place a shortcut onto your desktop. After the first program start there will be additional subfolders profiles and reports. No special modifications are made to the registry.

Setup will also create a Service called "EPRScheduleService", which will execute any scheduled report. Please check which account the service is logging in as. You can check this setting under Options->Service Configuration.

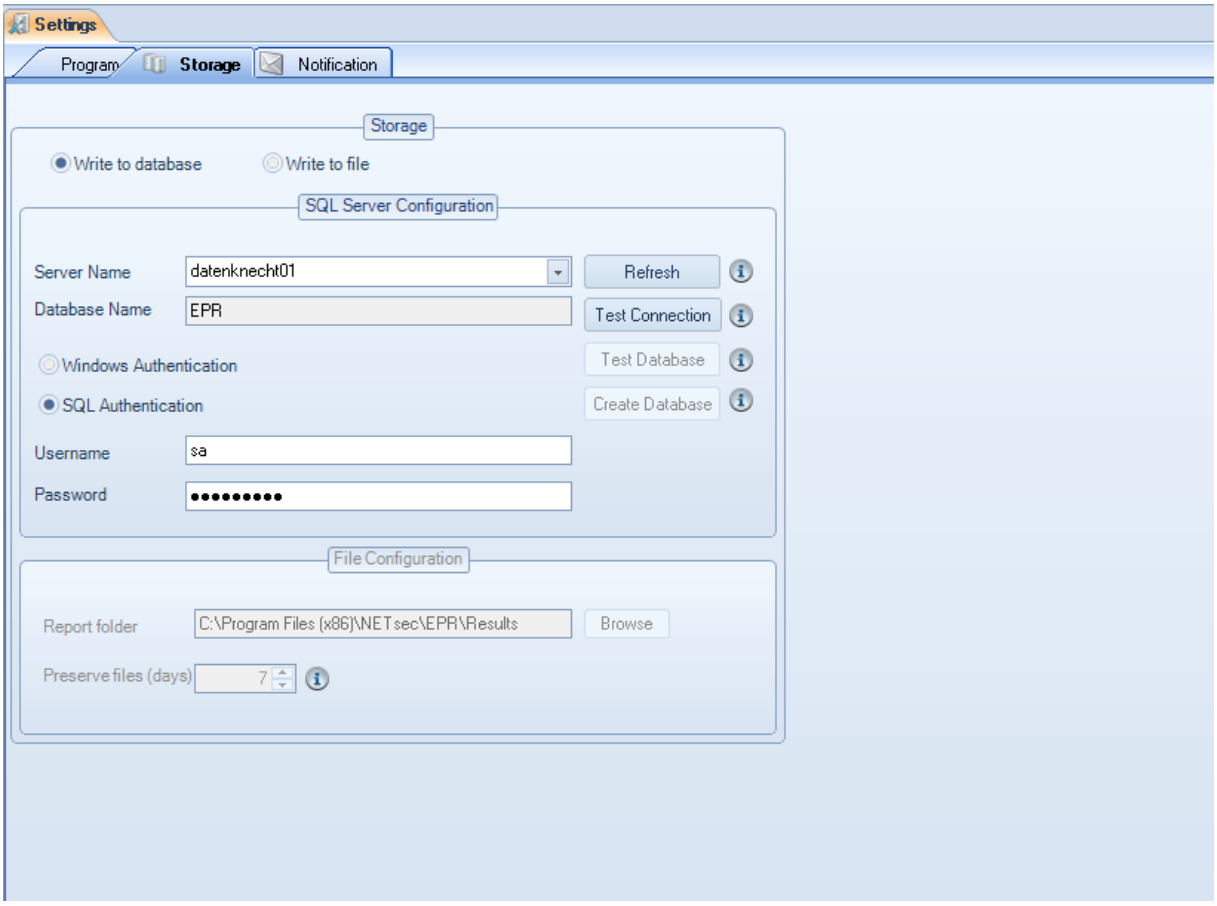
Configuration

When starting EPR for the first time, you should take a minute to set the "General Settings". This includes Store System and Mail Configuration. Once you have set the General Settings, these will act as default to every new Report Definition you create.

This is what EPR looks like when you start it up the first time:



Store System

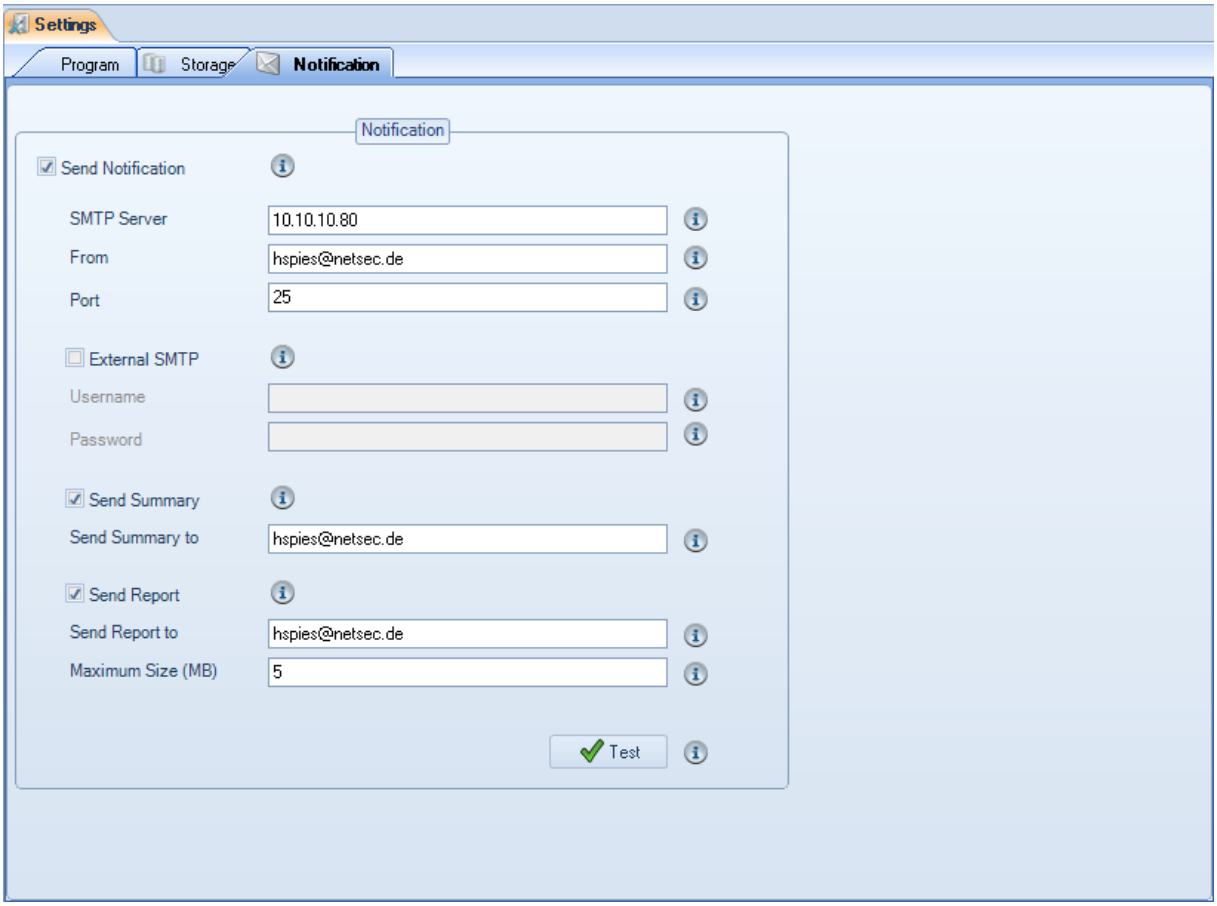


We support both store types, file and SQL, but we recommend that File Storage to be used for testing and evaluation purpose. Large reports usually generate too much data for a file, and require a SQL database to store this information.

You can either enter the SQL Server name by keyboard, or click "Refresh" to get a list of all SQL Servers in your network (having sql browser service running). Once you have selected the desired SQL server and configured the authentication method, you can test the connection. This will check if you are able to authenticate to the selected SQL server and tell if any connection issues occurred. If this is successful, you can now click "Test Database". This will check for the existence of an EPR database on the selected SQL server. If the database is not present, it will ask, if it can create it.

Please Note: The database has to be created by the software, as we use several stored procedures and user-defined tables.

Notification



EPR is able to send emails via SMTP. If you are using MS Exchange, you will need to enable the machine running EPR to send anonymous SMTP messages (look for thechnet articles about "How To Allow anonymous access or relaying in Exchange)

External SMTP:

You are also able to use an SMTP server which requires authentication (i.e. external) such as Hotmail, by providing corresponding credentials.

Send Summary:

This will send a summary of the report after every run, including timestamps, if it succeeded or not, and number of results. This may be interesting for the administrator monitoring the application.

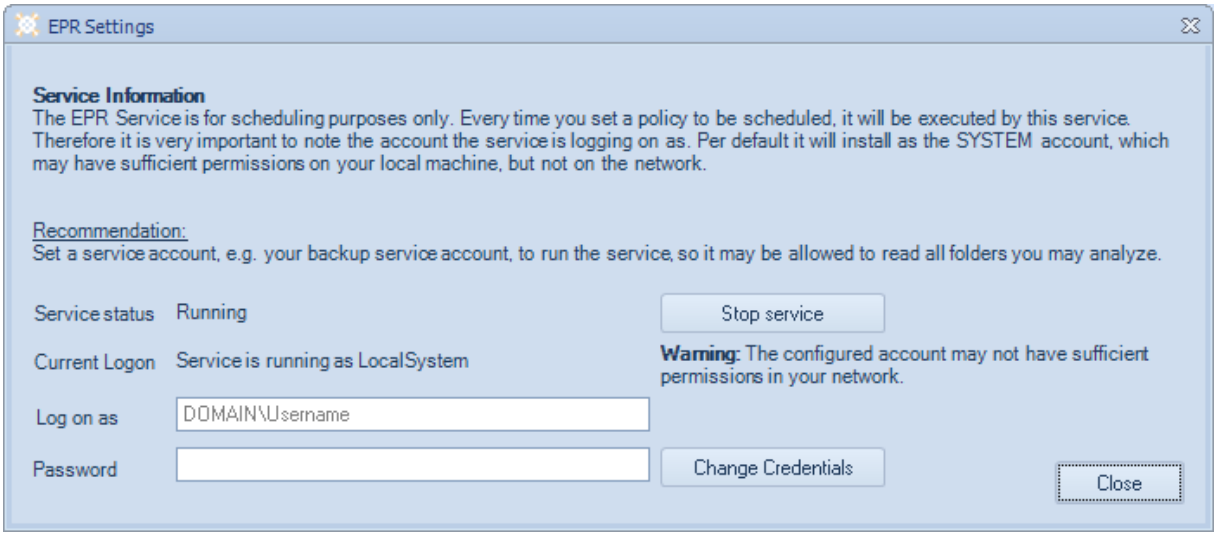
Send Report:

This feature will send the whole report as a CSV File attached to an email to the given sender. You may consider setting a maximum size of that file depending on your mailing environment. (By default: **10MB**)

The Test Button checks if your settings are correct.

Service Configuration

After setting up the general settings, the last configuration aspect is the Service Configuration. We open this up by clicking Options->Service Configuration:



After a fresh install, the service runs as LocalSystem. You should consider changing the account running the service, as any scheduled report will run under permissions of this account. Your LocalSystem Account will not have permission to analyze folder permissions in your network. We recommend using a Service Account with Domain Administrator access for this.

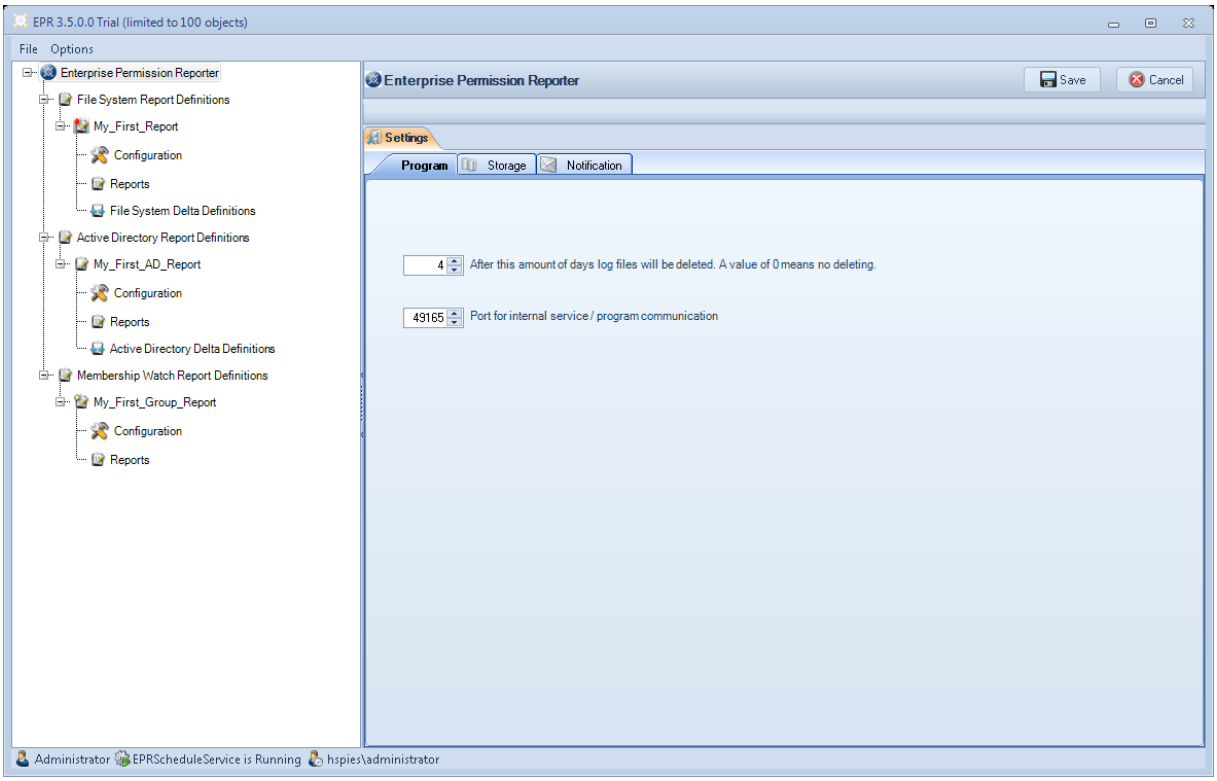
Minimal requirements regarding the EPR Service Account

1. member of the domain user group
2. member of the local adminstrator group of the machine EPR is running on
3. db-owner of the EPR database
4. appropriate access permissions to all resources he wants to do reports about

EPR Structure

The main element in EPR is the Report Definition. This element describes what should be reported, where the results should be stored, and what should be send. A Report Definition may also contain several reports (one Report equals one Run of the Definition) and many Delta Definitions.

Here is a simple overview on how the tree in EPR is built:



- Enterprise Permission Reporter
  - File System Report Definition
    - "ReportName1"
      - Configuration
      - Reports
        - "UniqueReportID"
          - Functional Application Manager
          - System Manager
          - Technical Application Manager
      - File System Delta Definitions
        - "ReportName1"
          - Configuration
          - Report
            - "UniqueReportID"
              - Functional Application Manager
              - System Manager

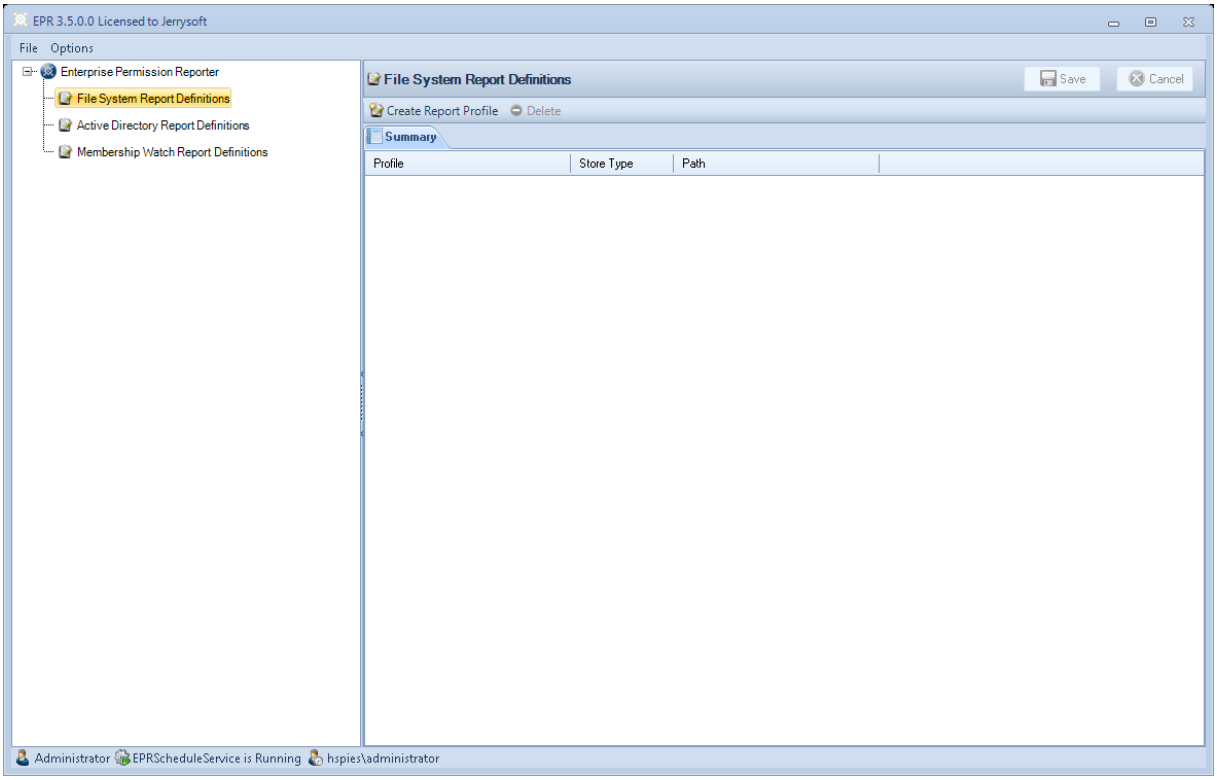
                - Technical Application Manager
            - "ReportName2"
            - …
            - "ReportNameN"
    - "ReportName2"
    - …
    - "ReportNameN"
- Active Directory Report Definitions
    - "ReportName1"
        - Configuration
        - Reports
            - "UniqueReportID"
                - Functional Application Manager
                - System Manager
                - Technical Application Manager
        - Active Directory Delta Definitions
            - "ReportName1"
                - Configuration
                - Reports
                    - "UniqueReportID"
                        - Functional Application Manager
                        - System Manager
                        - Technical Application Manager
            - "ReportName2"
            - …
            - "ReportNameN"
    - "ReportName2"
    - …
    - "ReportNameN"
- Membership Watch Report Definitions
    - "ReportName1"
        - Configuration
        - Reports
            - "UniqueReportID"
    - "ReportName2"
    - …
    - "ReportNameN"

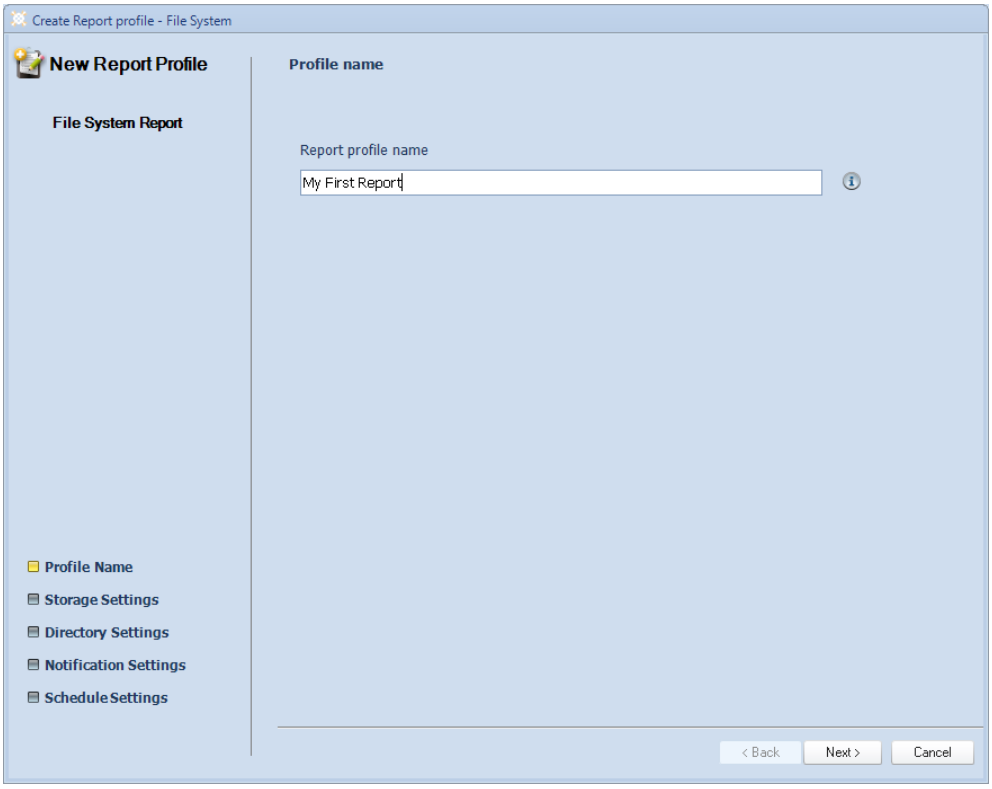
File System Report Definitions

In this section, we want to walk you through the most common tasks you want to achieve with the File System Report.

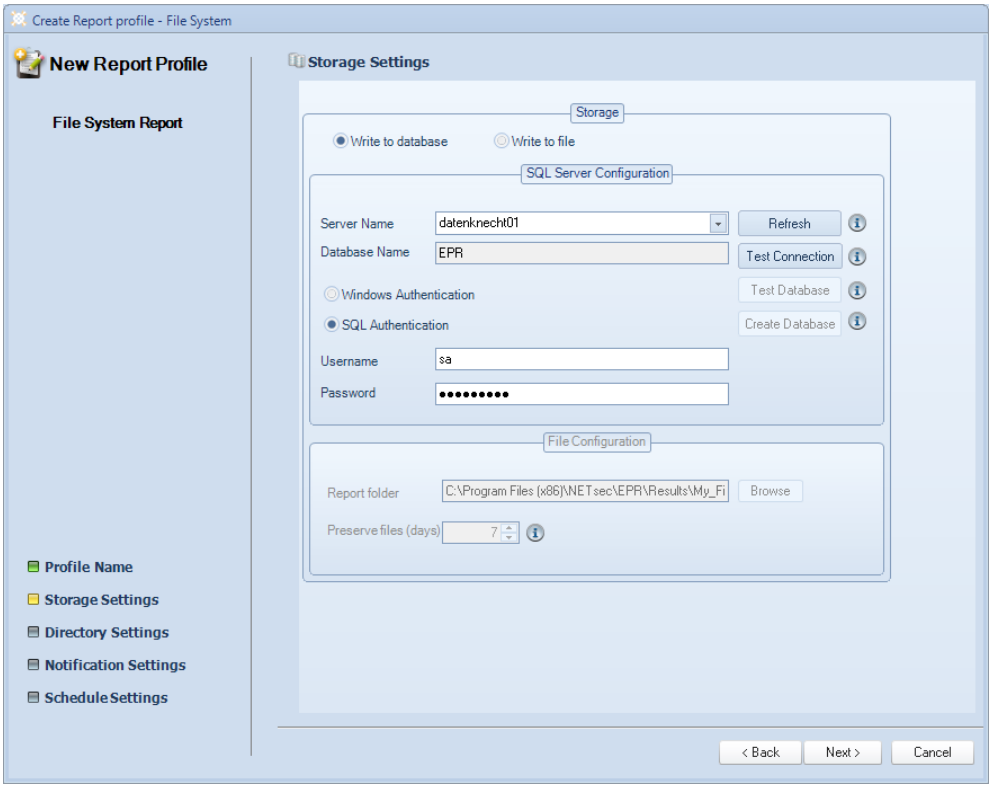
The First Report

Let's start off with your first report; given that you are running the application on your domain-computer, a short analysis of your Users Folder can be interesting. Let's start off by creating a new Report Definition by selecting "File System Report Definitions" and clicking "Create Report Profile" in the action pane of using the context menu:

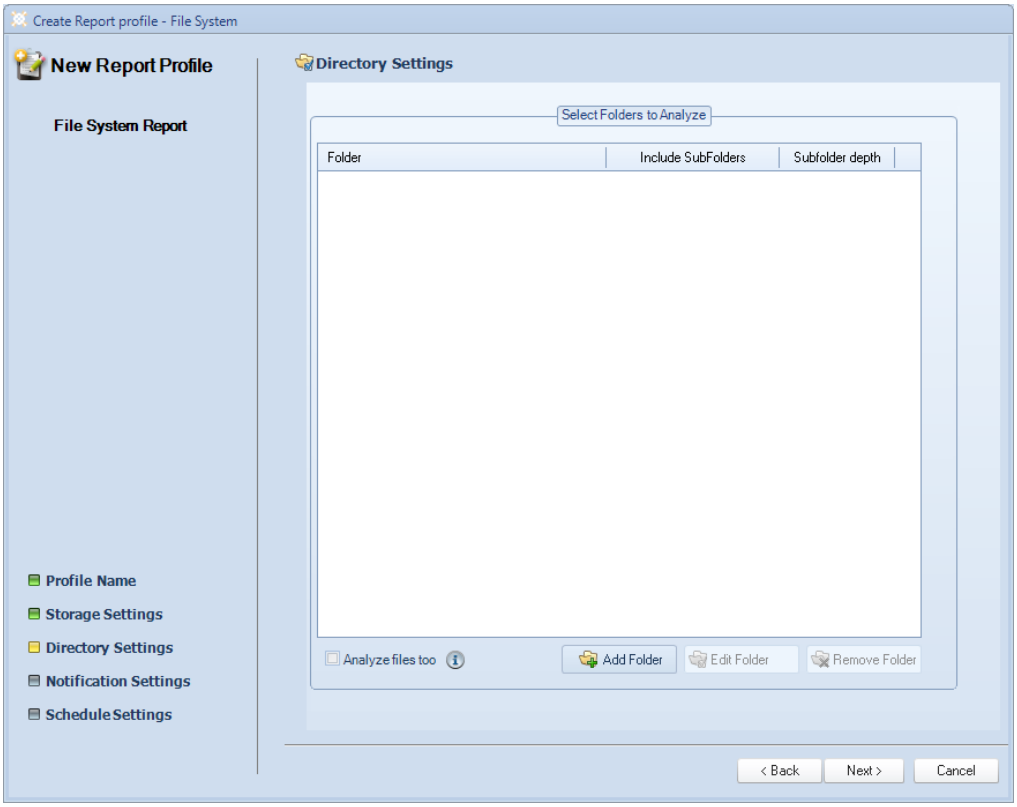




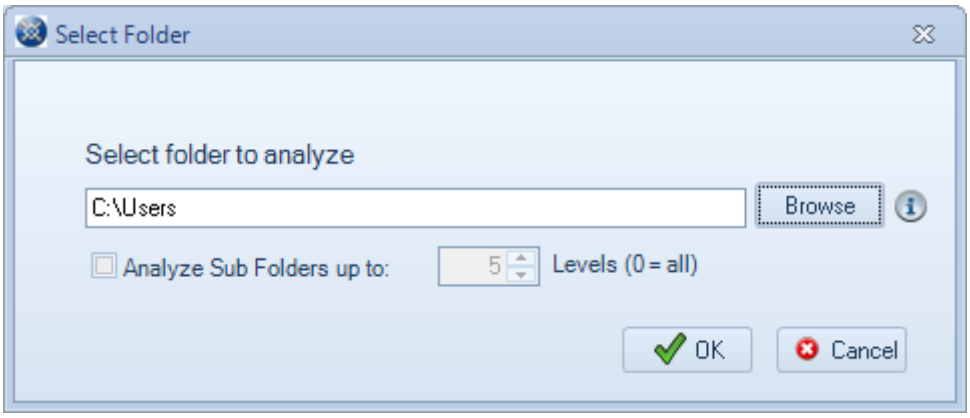
After providing a name, we click next.



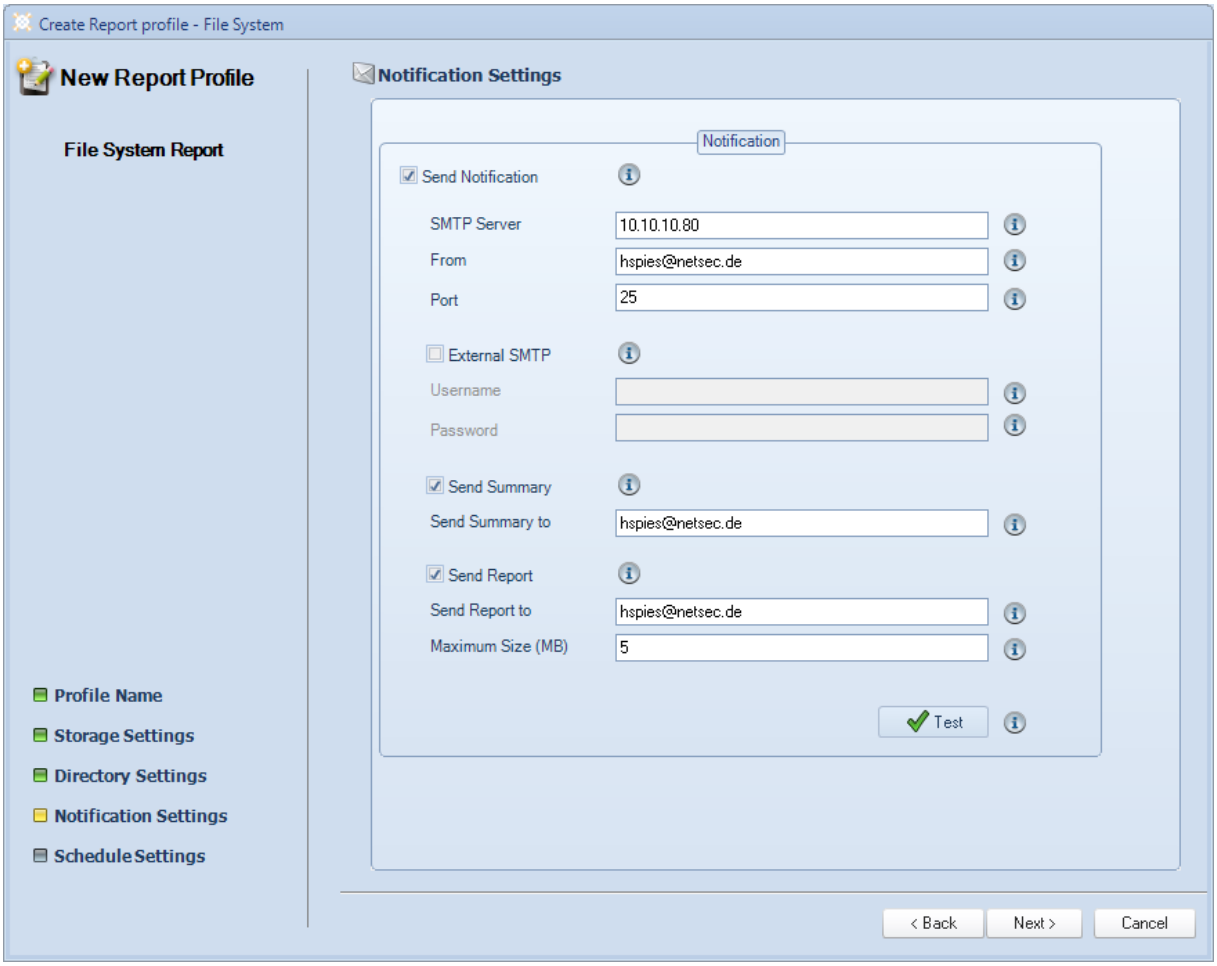
Here we find our default settings set up earlier. I assume we can leave this as it is and click next:



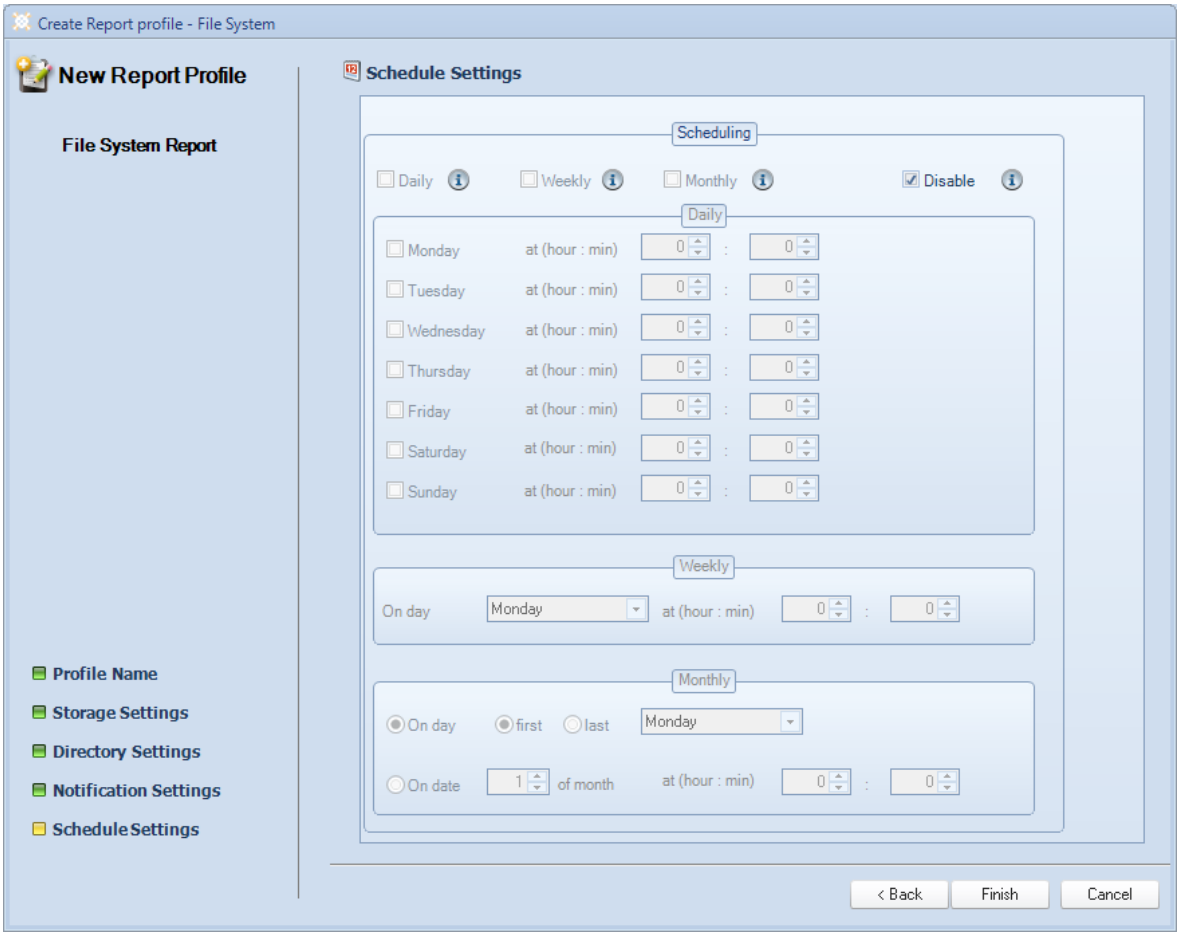
Here we can add all the Folders we want to Analyze by clicking "Add Folder":



We can either type in the UNC Path of the desired older or use the Browse button. After selecting the desired folder, choose whether or not you want to include subfolders. We are also able to limit the subfolder levels EPR will analyze. The default value is 5, setting 0 means unlimited number of subfolders. For our first report, using Level 5 should do the trick. After acknowledging with OK we can hit next.



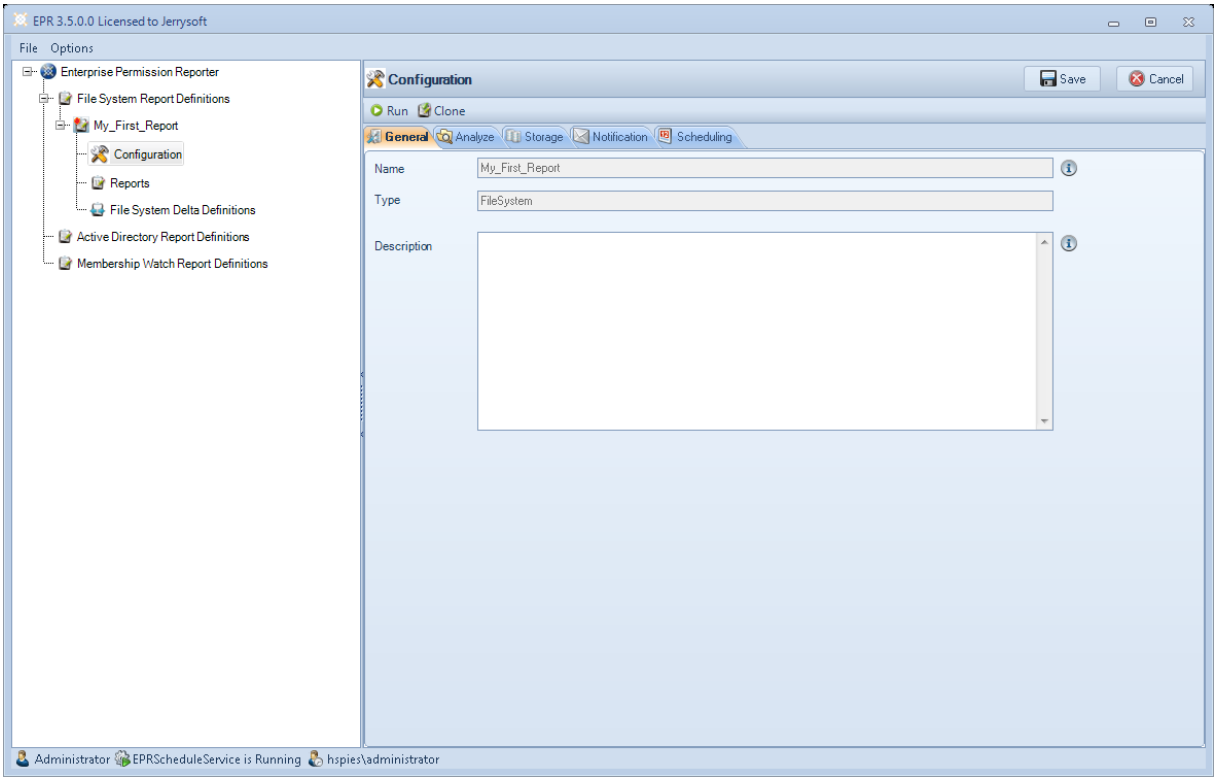
Similar to our Store type, the default settings earlier apply to the Status Notification. Assuming the default is correct, we can go ahead clicking next.



The last Wizard Page is for Scheduling. You can set up Daily, Weekly or Monthly schedules. For our first report we do not need any scheduling, so we can finish the wizard.

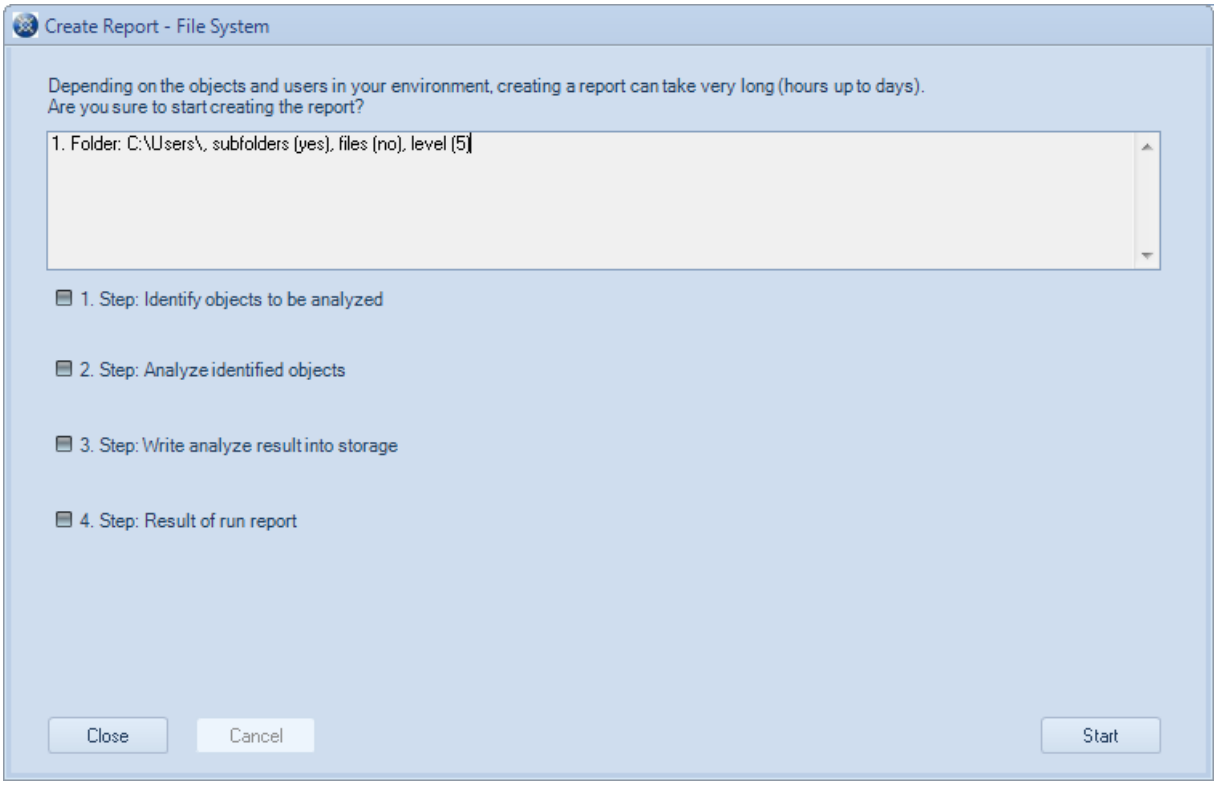
(Note: Scheduling will be described in "Monthly Compliance Report")

We now see our first simple report selected in the EPR menu structure:

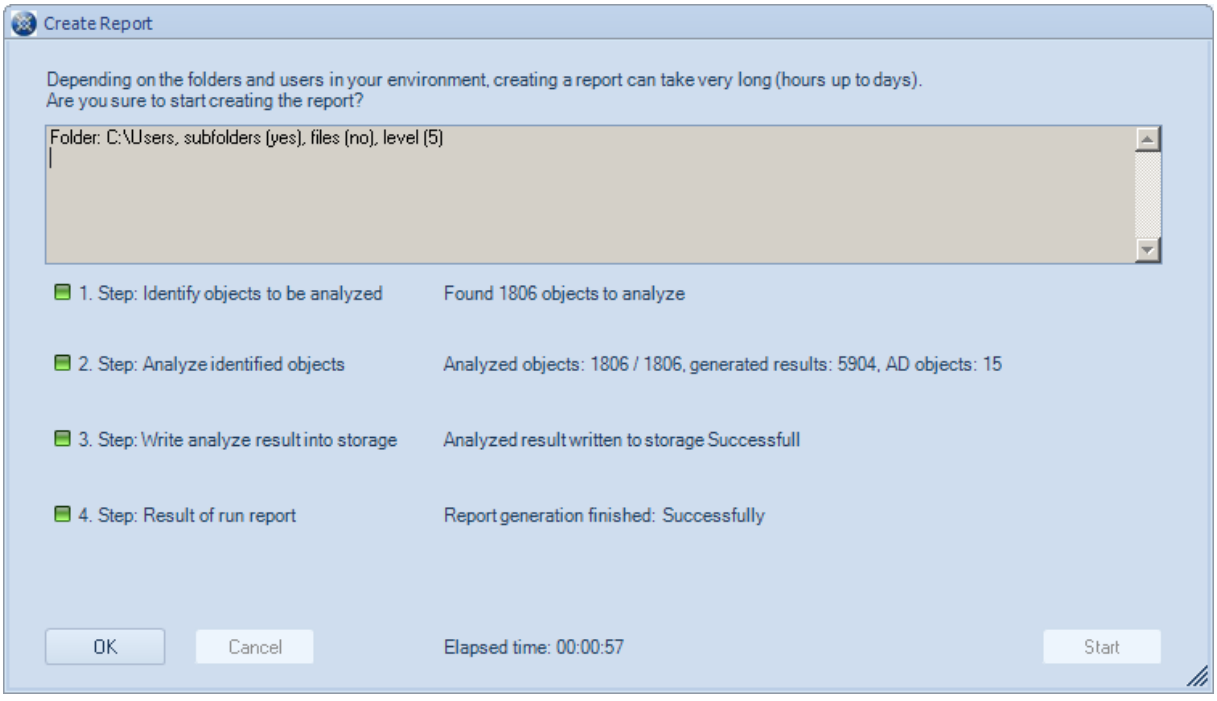


The Configuration node shows us each wizard page we just went through as a tab on the right side. We may change anything we just configured, as long as we do not have any reports created for this definition. This would prevent the Report Definition from withstanding any compliant check and also negate any results existing inside the report.

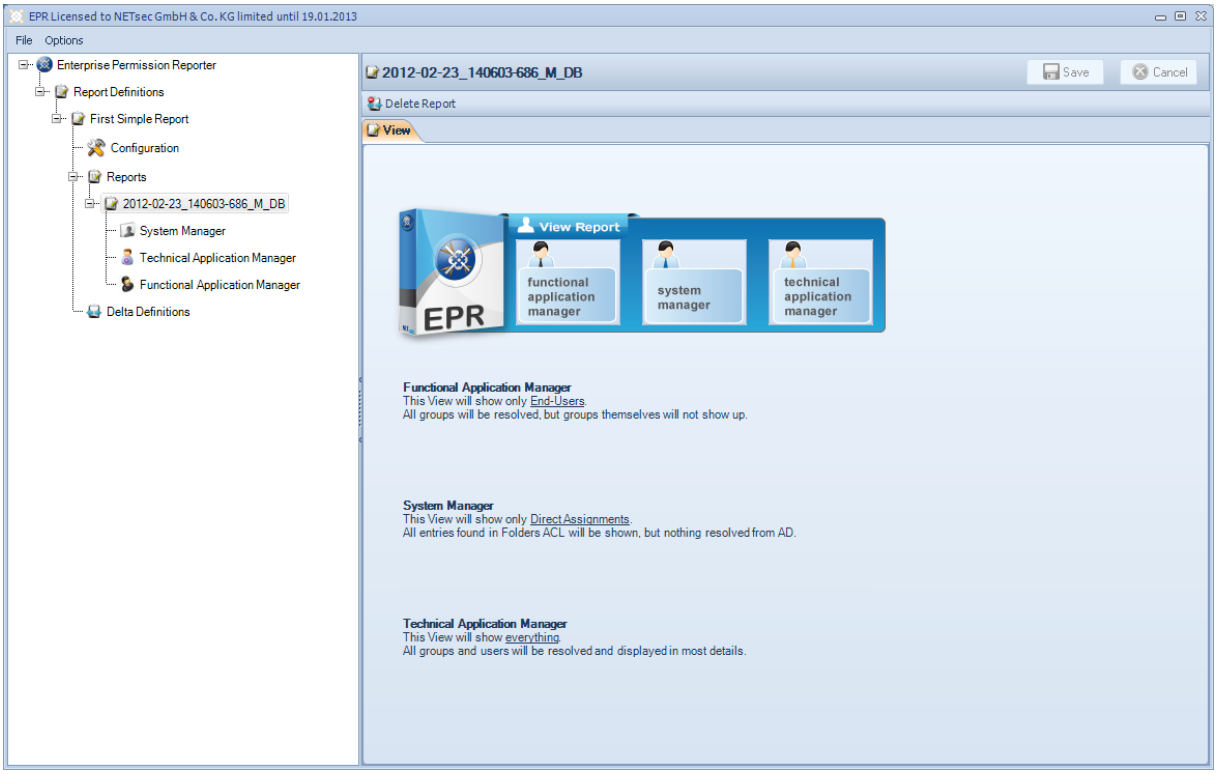
Now run the report you just created:



We now can see the settings we provided and click Start when we are ready:



After the report generation is finished, we can close this form by clicking OK. We now see our freshly created report selected in the EPR menu structure:



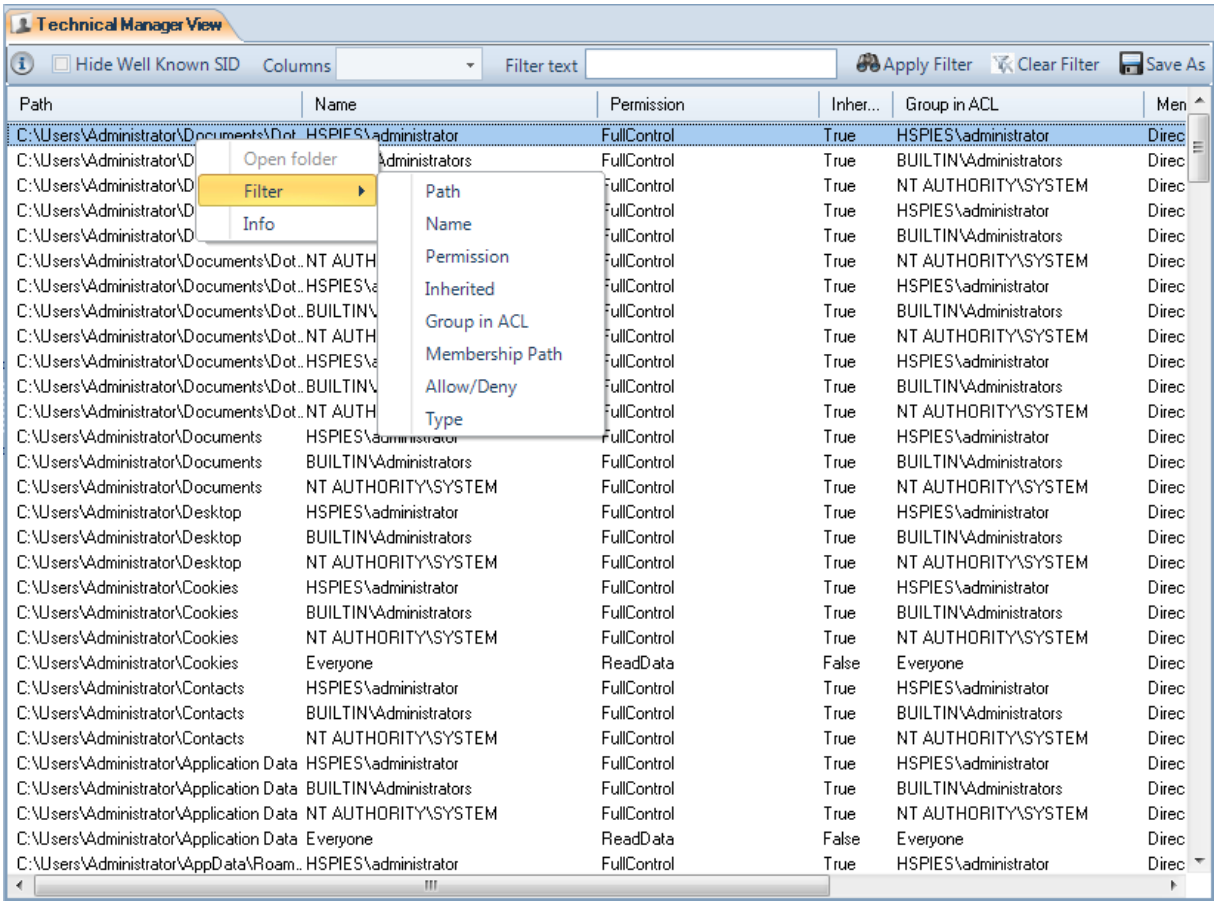
Viewing a report can be done using 3 different views, each including their own filters:

- Functional Application Manager
  - This view will show only End-Users.
    All groups will be resolved, but groups themselves will not show up.
- System Manager
  - This view will show only Direct Assignments.
    All entries found in folders ACL will be shown, but nothing resolved from AD.
- Technical Application Manager
  - This view will show everything.
    All groups and users will be resolved and displayed in the most detail.

Filtering, Sorting, Exporting

Filtering

No matter what type of report you view using EPR, you are always able to filter and export what you see. There are 2 ways to apply a filter:



First, you can select the column you want to filter, enter a filter text and then hit Apply Filter.

Second, you can select a row showing a value you want to filter, right-click to open the Context Menu, go to Filter, and then select the desired row which you want to filter for the value of the selected row.

The most common filter is the upper left checkbox "Hide Well Known SIDs" (WKSID), which will simply filter out all entries of the type WKSID.

When you feel the need of returning to the unfiltered entries, just click "Clear Filter" to delete any filter you may have applied.

Exporting

Once you have a display of the desired entries, you may click "Save As" to get a CSV version of just the data in your current view, which then can be supplied to anyone asking for particular permission reports.

Sorting

EPR is built for very large result-amounts. To keep up with even millions of entries in one single report, we developed EPR to use a complex paging mechanism to stay fast in terms of usability. This is why sorting is only

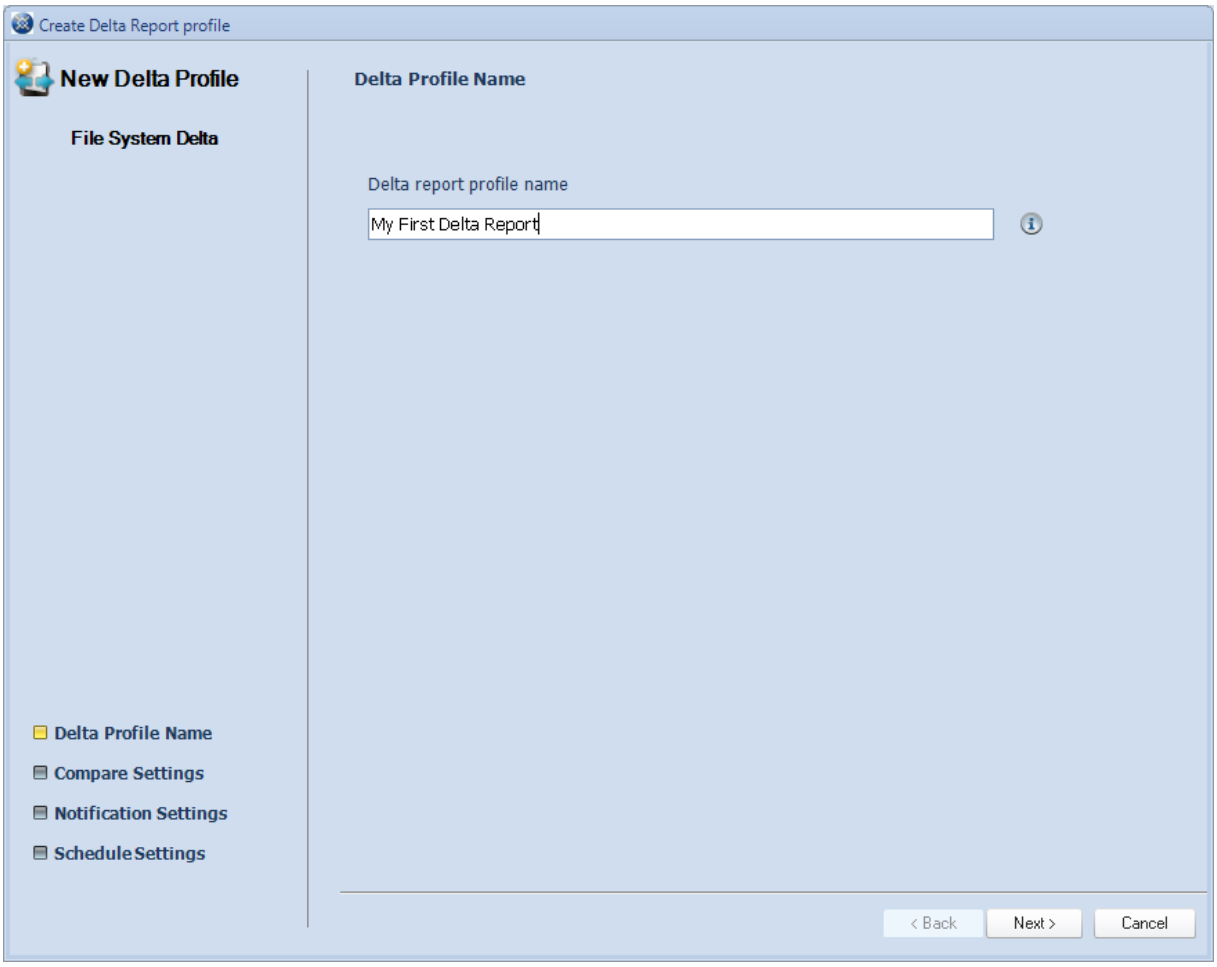
enabled when the Store type is SQL. The current page size of EPR is 50,000 entries. Your current view has to be below that to allow sorting; otherwise our paging-mechanism would fail to retrieve the correct sorted data from the SQL server.

Once that is considered, sorting functions the same way it does in any other Application: click the column once for ascending sorting, and another time for descending sorting.

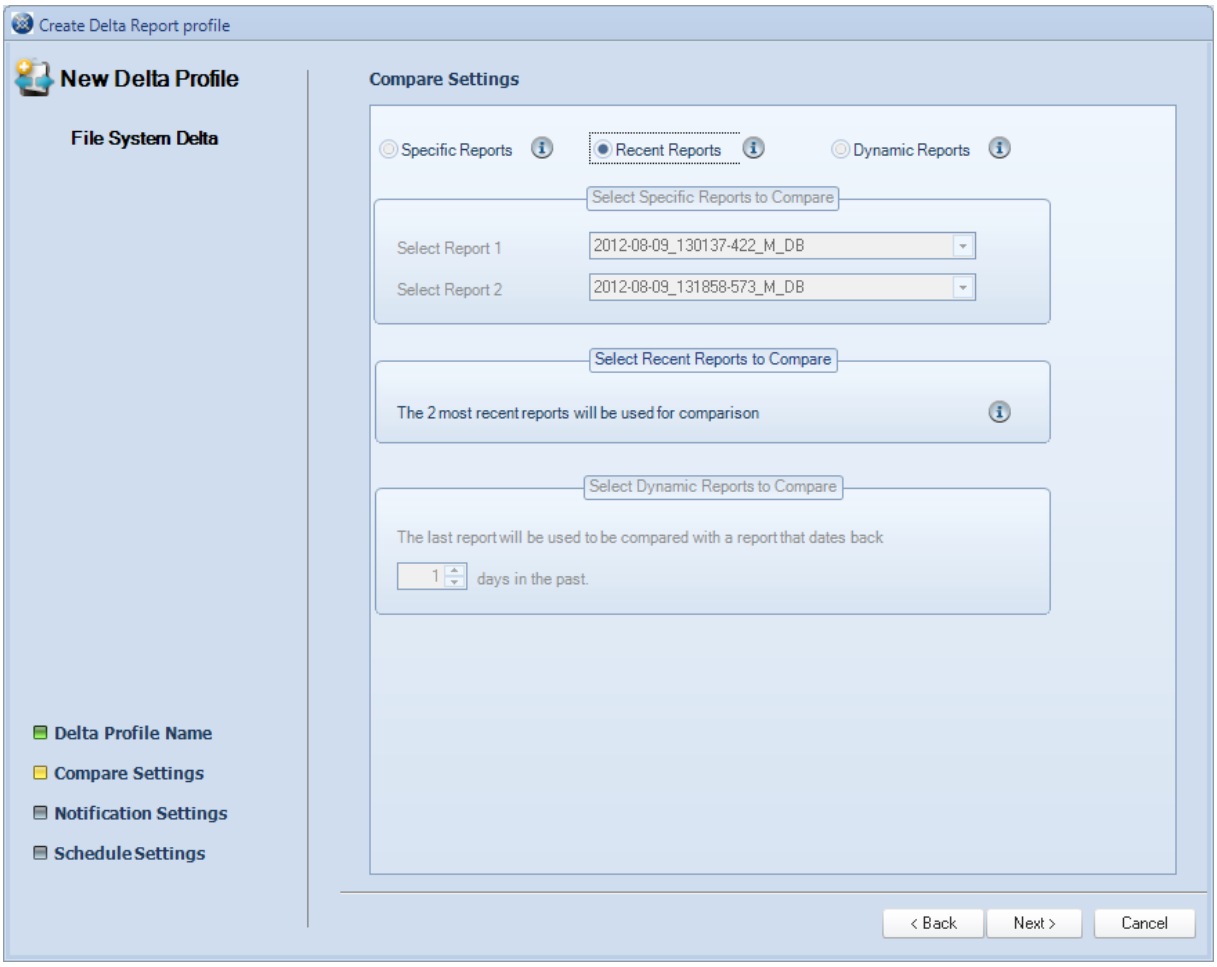
Delta Reports

To better understand this section, please read "The First Report" first.

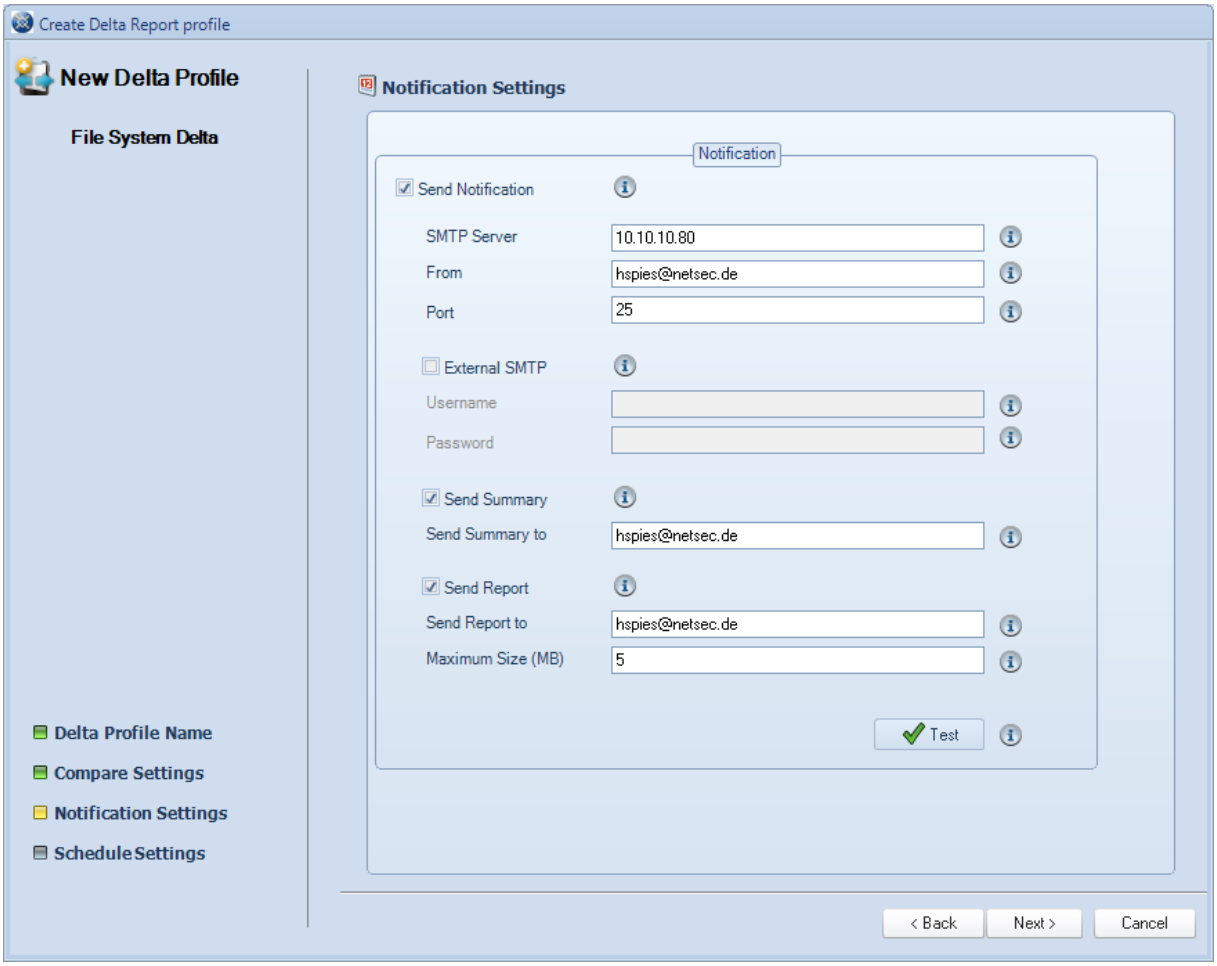
I have just granted access an additional user modify permissions on my users folder. First of all we need to create a new report in our Definition to recognize the change, so we hit Run again. After the report is finished, we need to first create a new Delta Report Definition within our Report Definition. To do so, we select the Delta Definitions Node and click Create:



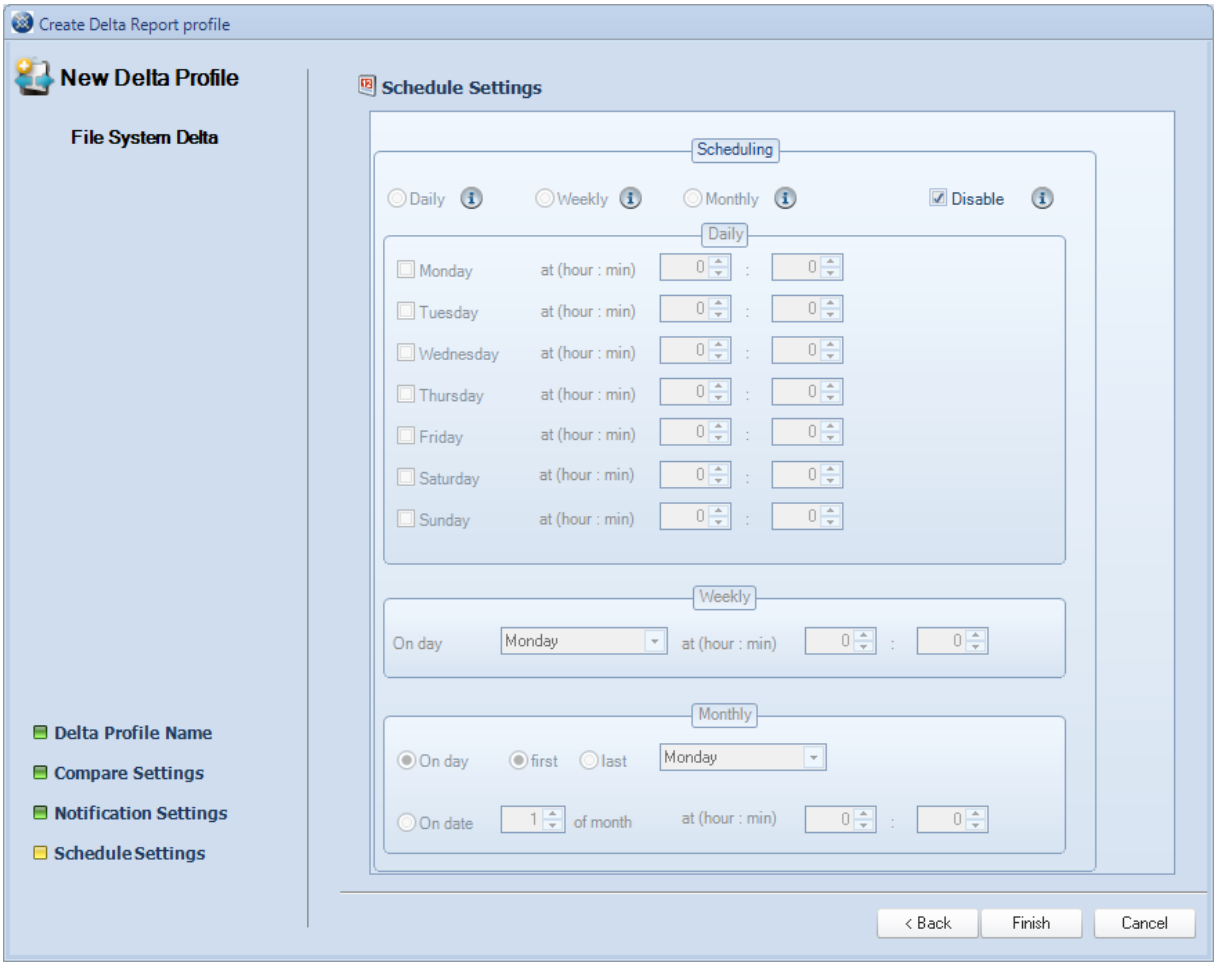
After providing a name, we select the reports to compare after clicking next:



Here we have 3 options on how to select the reports to be compared. In our case we could either select the specific reports like in the screenshot or select "Recent Reports", which would compare the last 2 created reports. Using "Dynamic Reports" enables us to compare the most current report with the last report of a day that is X days in the past. We continue with Next:

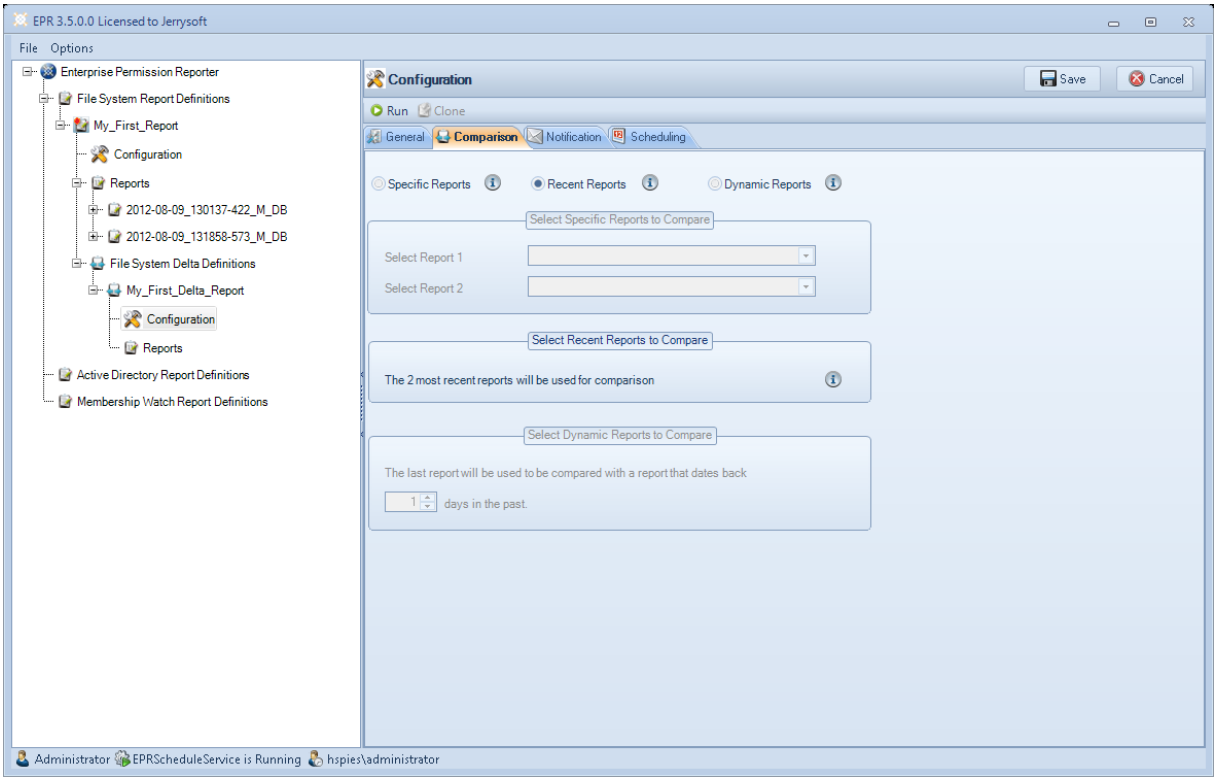


Here we find the Mail Notification form again filled in with our default values. We can change the Subject or To-Addresses here. Clicking Next leads us to the Scheduling form:



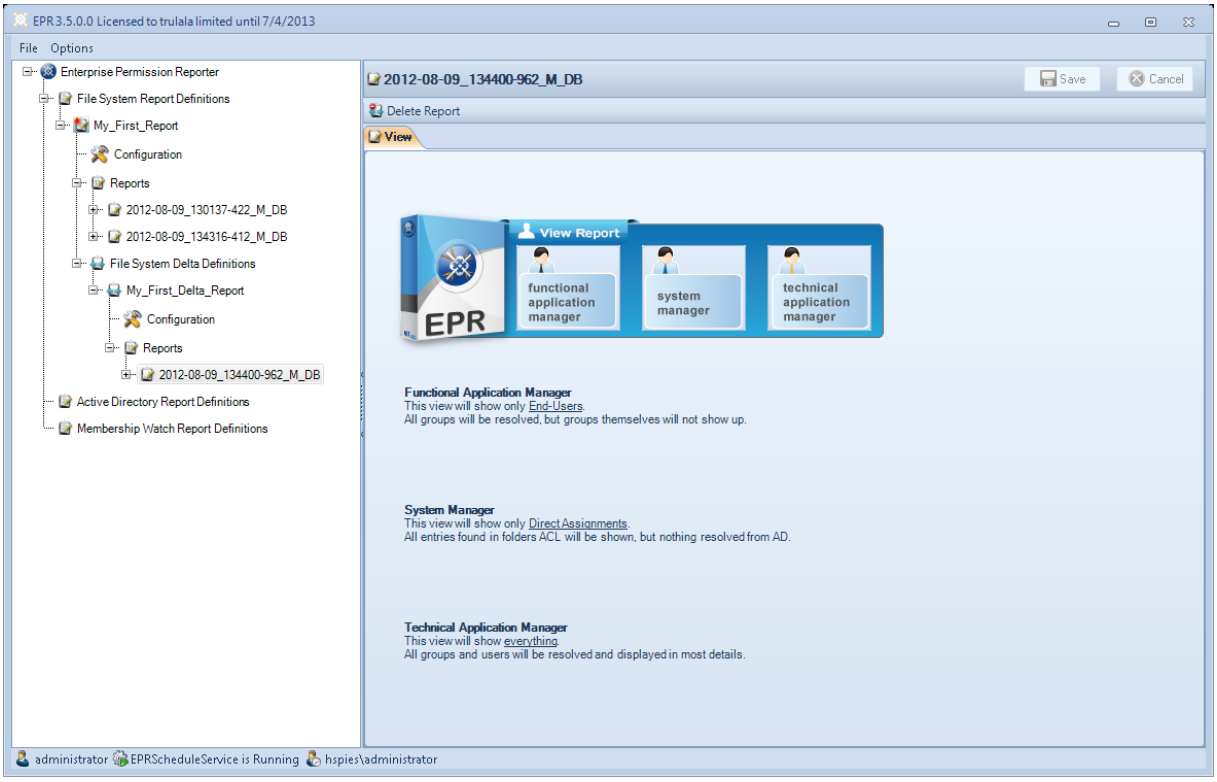
This would only make sense using Recent or Dynamic report selection, so leave it disabled and click Finish.

We find the newly created Delta Report Definition selected in the menu structure:

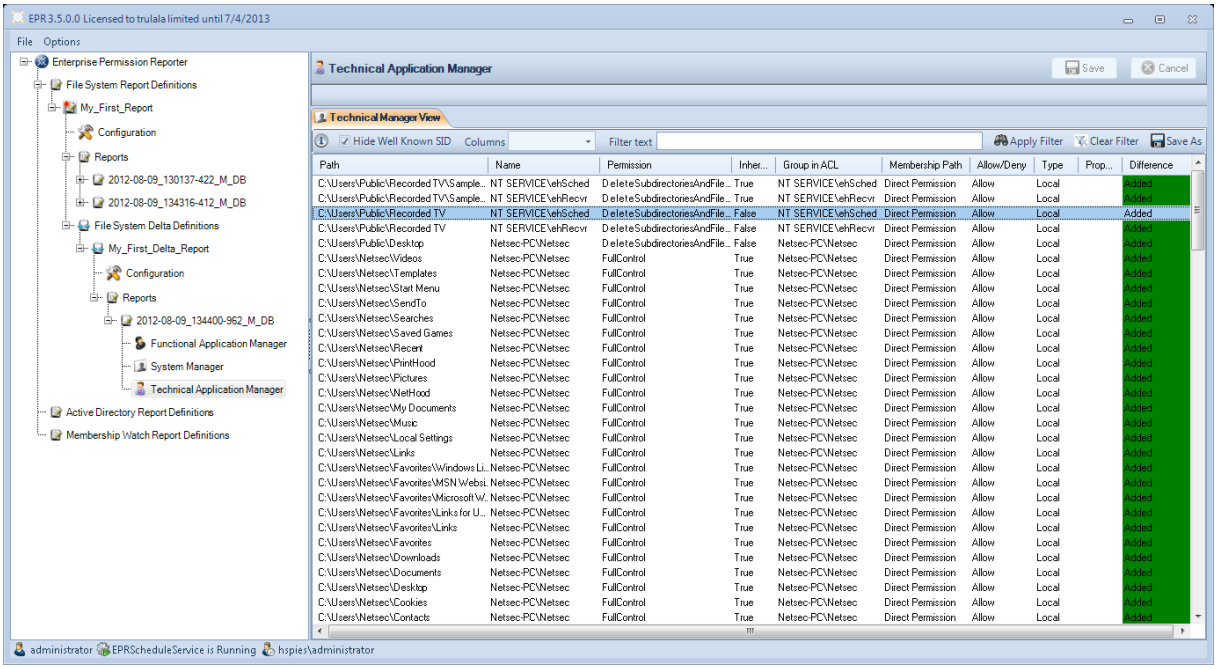


We can straight go ahead and click Run to generate the Delta Report:

After creation finished and clicked on OK, we are presented the new report and the 3 views:



Selecting the technical view, we can see all the change entries for the user I just added:



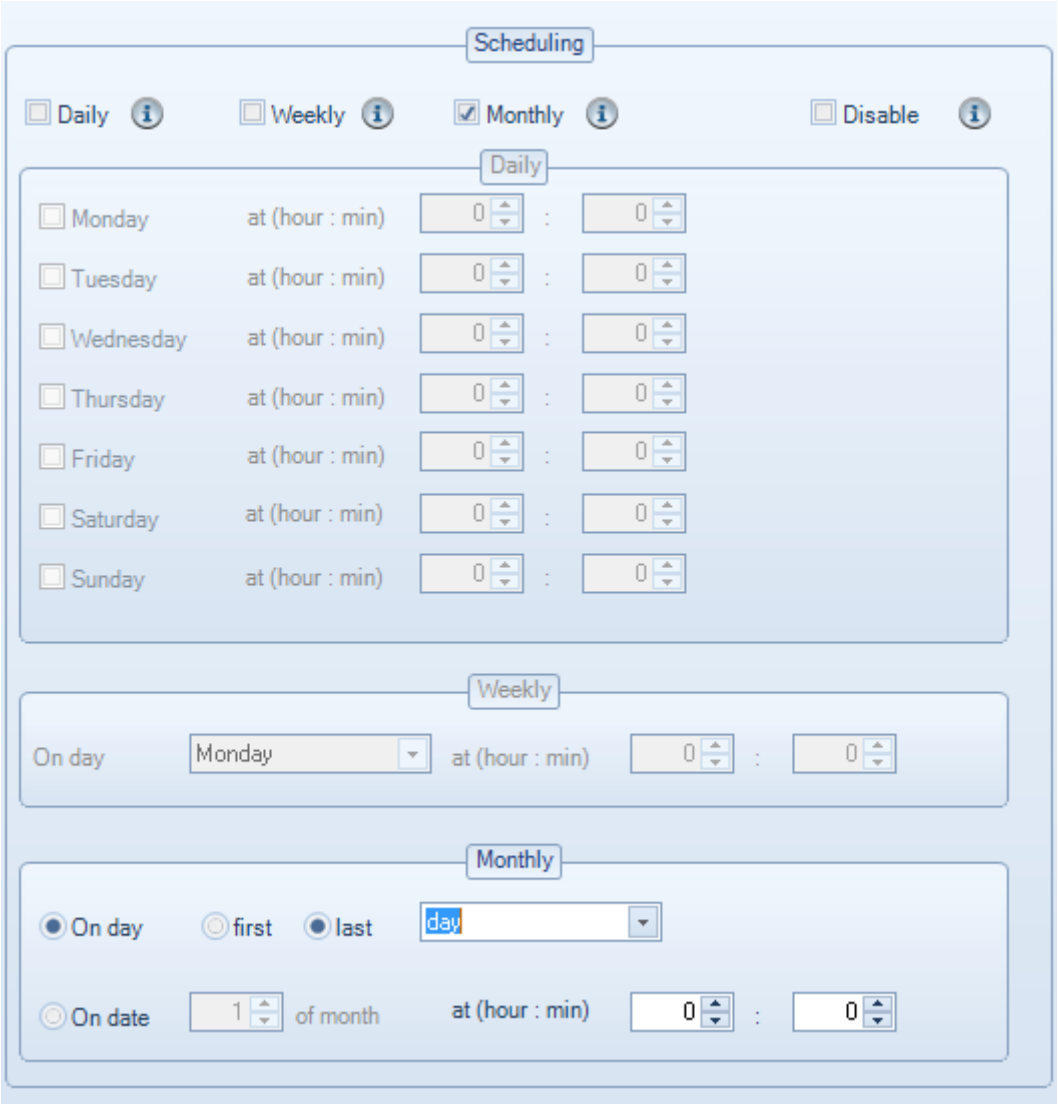
Scheduling

Monthly Compliance Report

To better understand this section, please read "The First Report" and "Delta Reports" first.

This task enables you to keep track of your whole permissions for compliance purposes on a monthly basis.

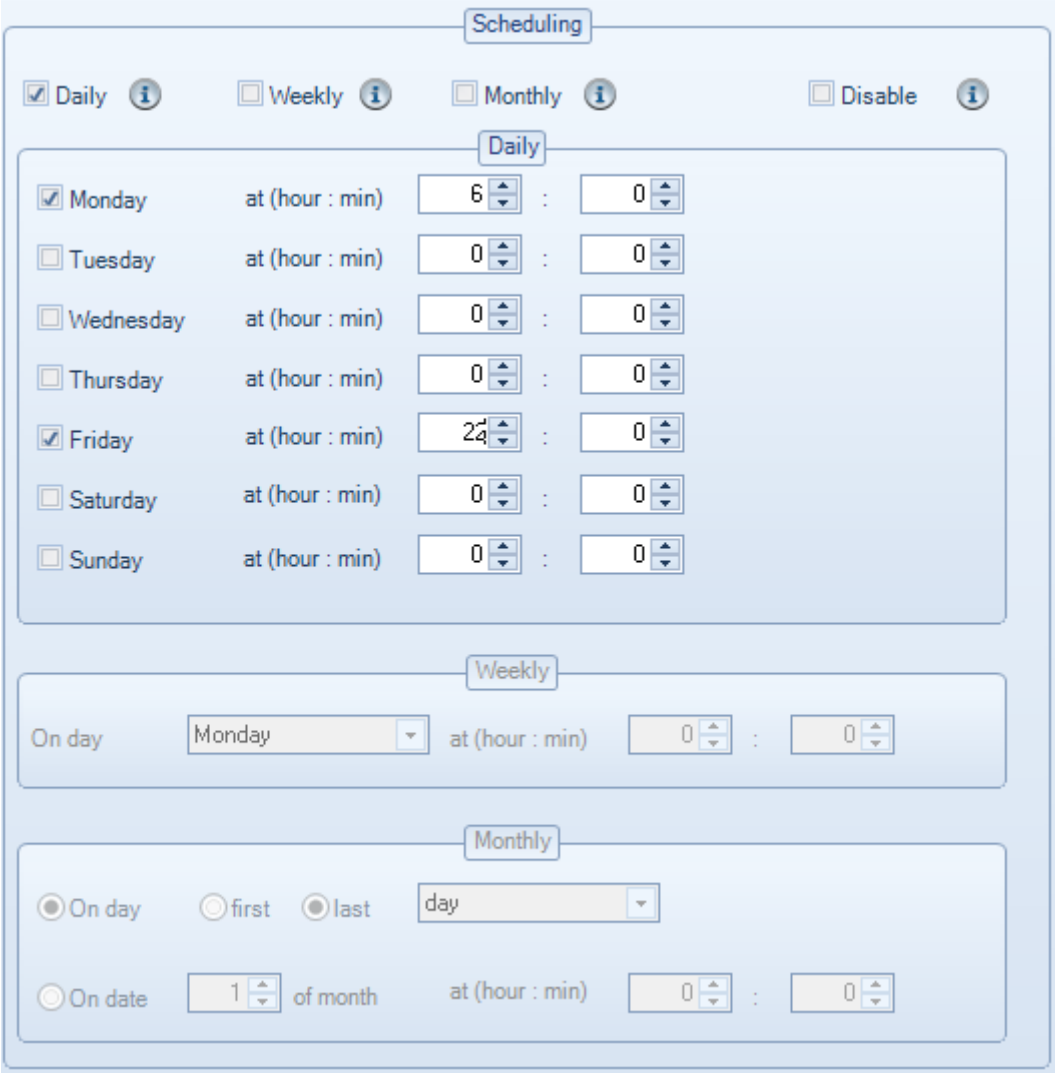
To do this, create a new Report Definition, add all Folders to analyze, and schedule it monthly:



Weekly Delta Report to Data Owners

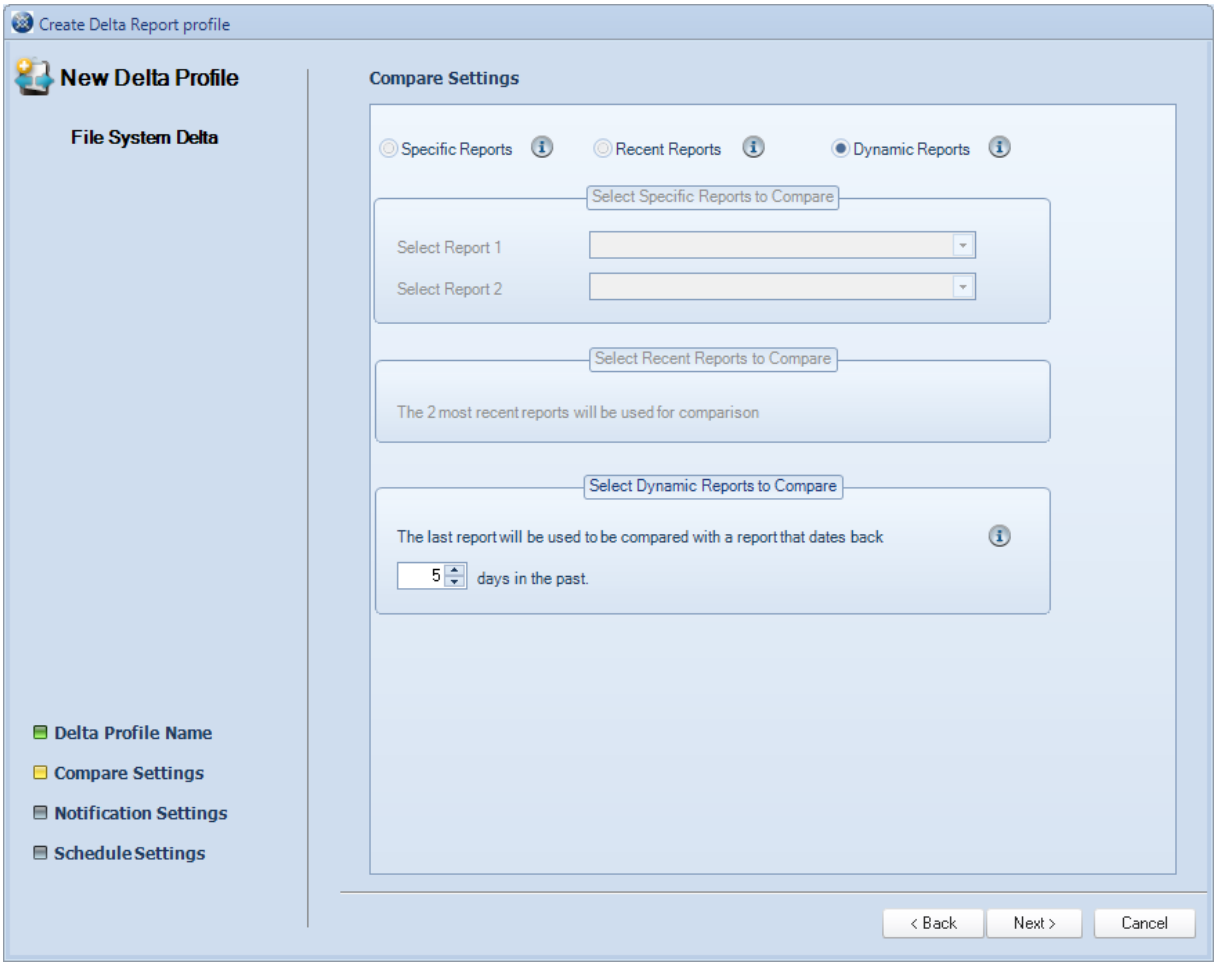
To better understand this section, please read "The First Report" and "Delta Reports" first.

This task aims to the delivery of a CSV file per email to every data owner wishing to get a weekly change of permissions report for the folders they own. First, you need to create a new Report Definition matching your needs in regards of the folders that are to be analyzed. Now, you need to schedule this report to run twice a week, once at the start, and once at the end of the week, like this:



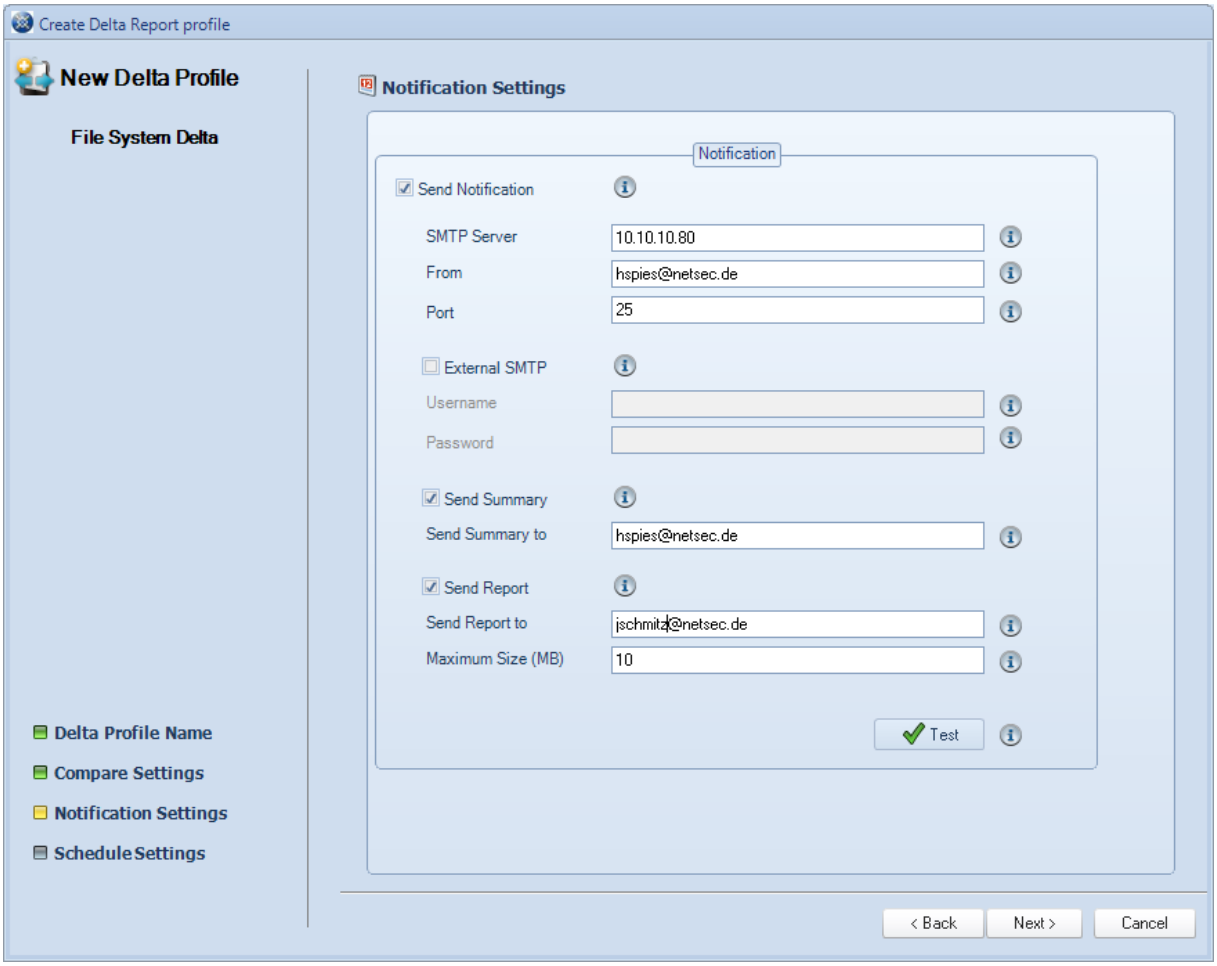
(Please Note: This will make the EPR Service execute a new report every Monday at 6 am and Friday at 10 pm**)**

With the comparable reports scheduled, we now go ahead and create a new Delta Definition for this Report Definition:

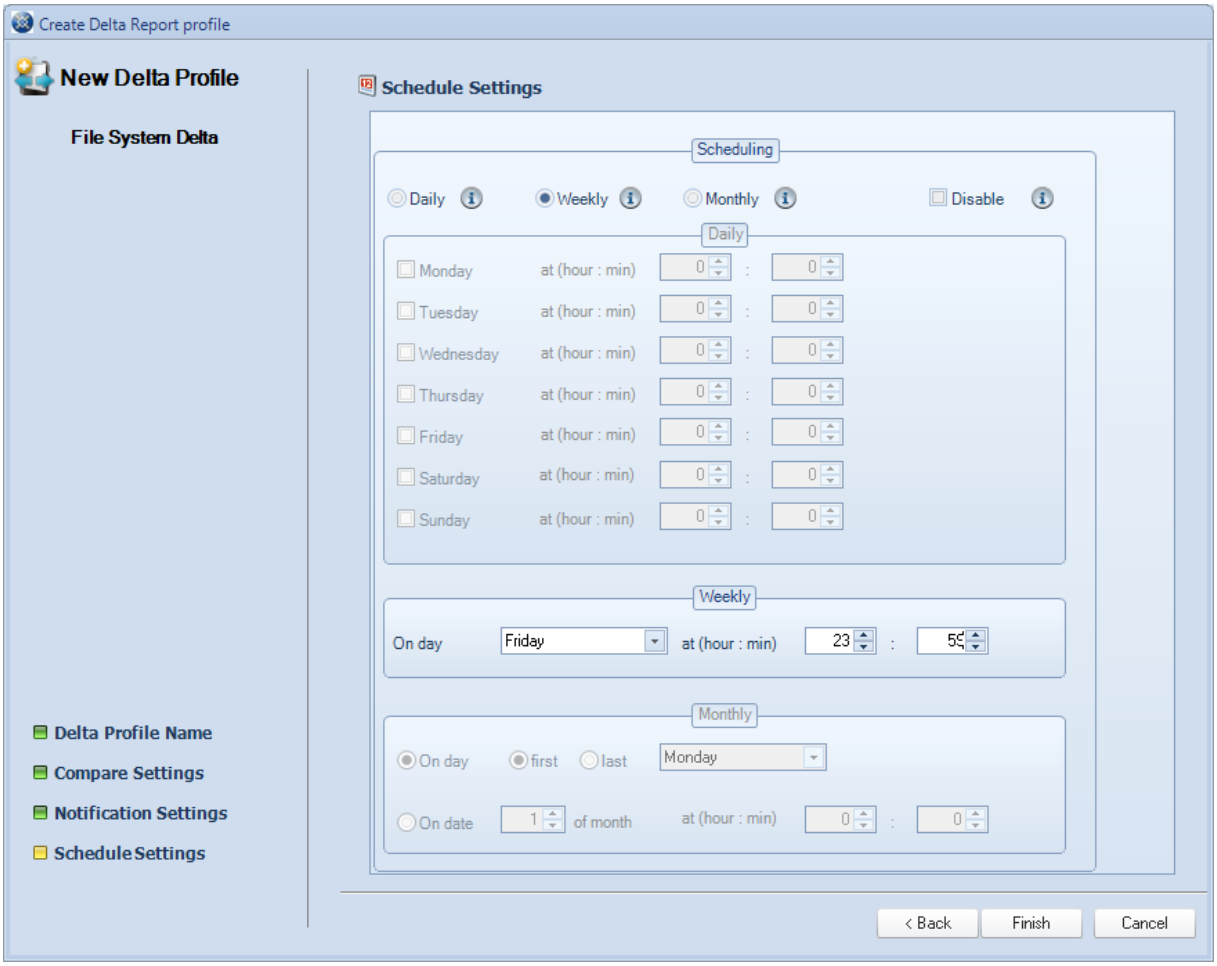


We plan to schedule this Delta Report on Friday, 2359h, so the report must be dynamic selected 5 days in the past.

In most cases you will want to send a summary to you, the administrator, and the report as a CSV file to the data owner, whose folders we are analyzing:



Last but not least, we need to configure a schedule for this delta report to match our schedule of the comparison report:



That’s it, now we have successfully configured a Weekly Delta Report which reports permission changes to the data owner

Active Directory Report Definition

One of the new features in EPR is the possibility to report all permissions of a chosen AD object.

All features for File System Reports are also valid for the Active Directory Reports (Scheduling, Notifications)

Tasks:

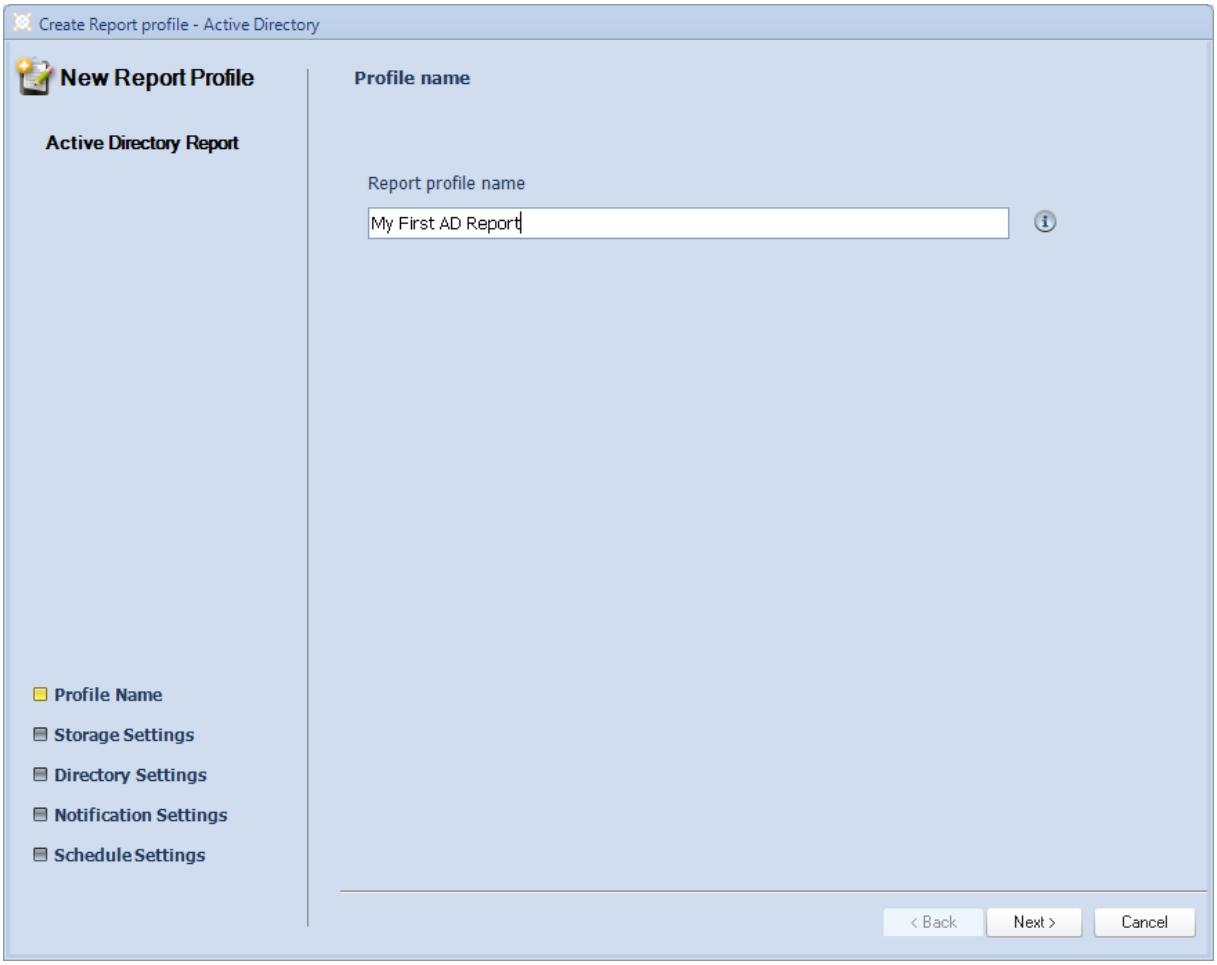
In this Section, we want to walk you through the most common tasks you may want to achieve with the Active Directory Report.

Let's start off with your first report; Given that you are running the application on your domain-computer, a short analysis of an OU to see which permissions are given is a good first report.

To complete this task, please first read "Filtering, Sorting, Exporting", "Delta Reports" and "Scheduling".

The First Report

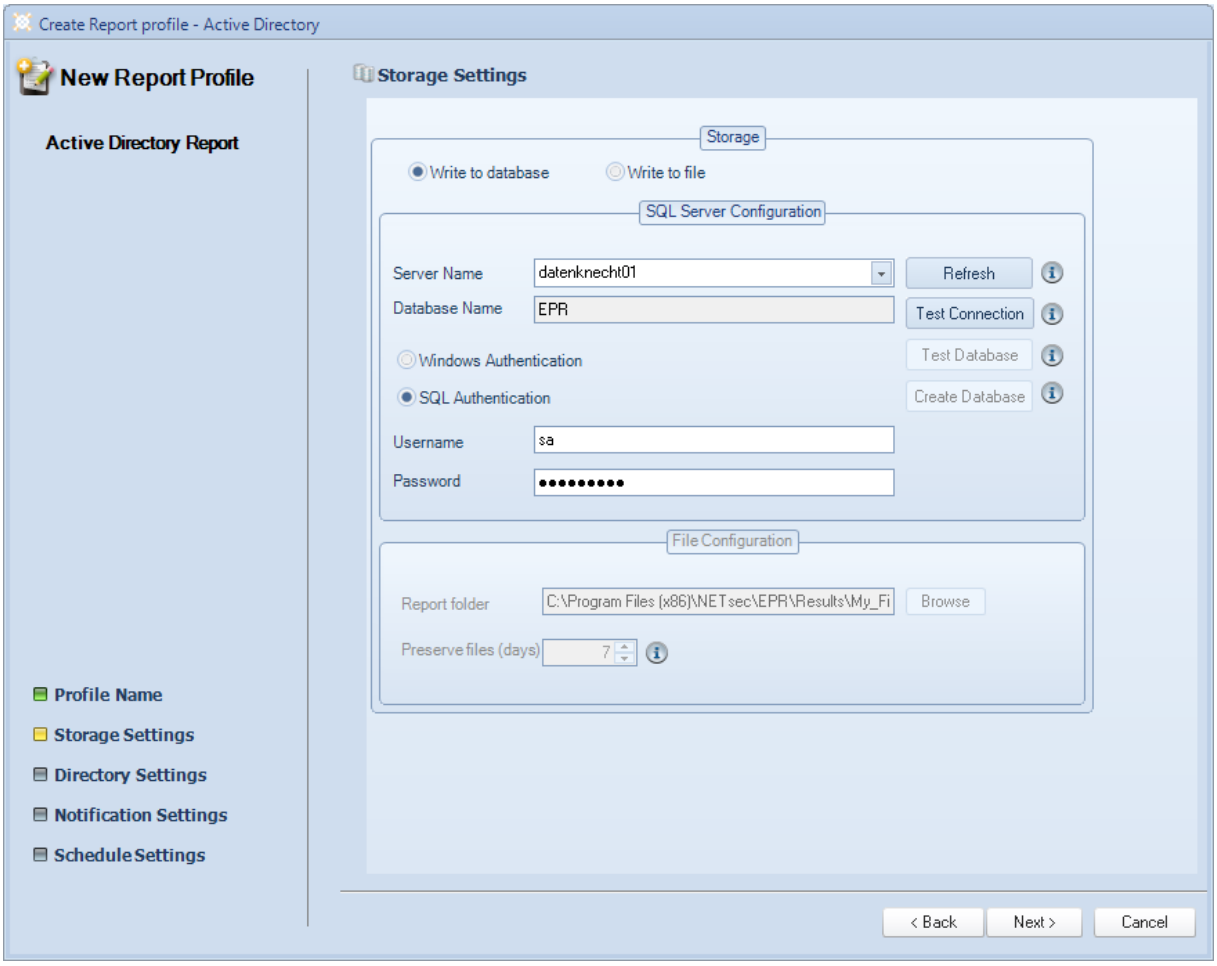
To create an Active Directory Report Definition click "Create Report Profile". The following window will open:



Here, you can give your Report Definition a name.

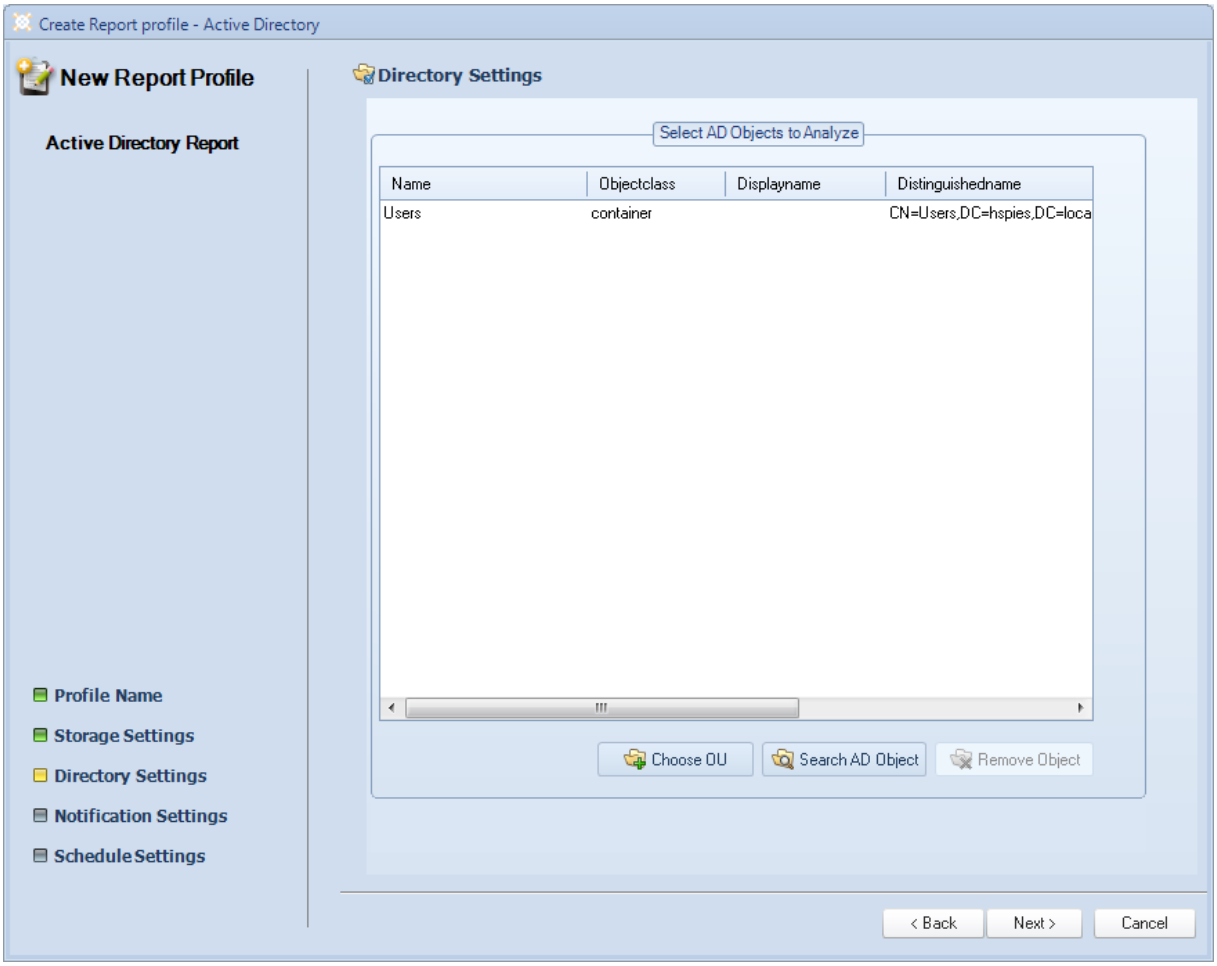
When this is done click next to continue.

Here you can choose where the reports will be saved.

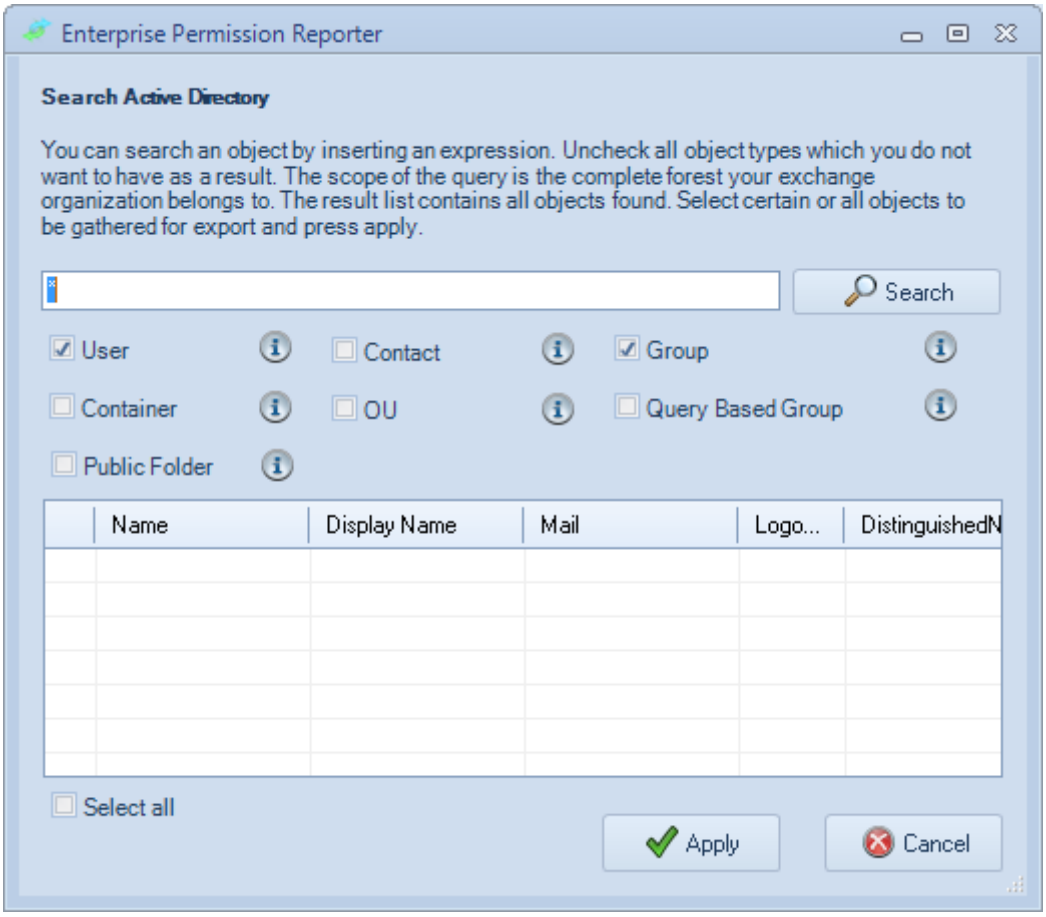


Click next to continue.

Here you can choose an OU or an AD object which you want to report on.



If you click onto "Search AD Object" you can enter a keyword to find your AD object.



In the next window, you can enter your Notification Settings.

When this is done, you can decide if you want to schedule your report.

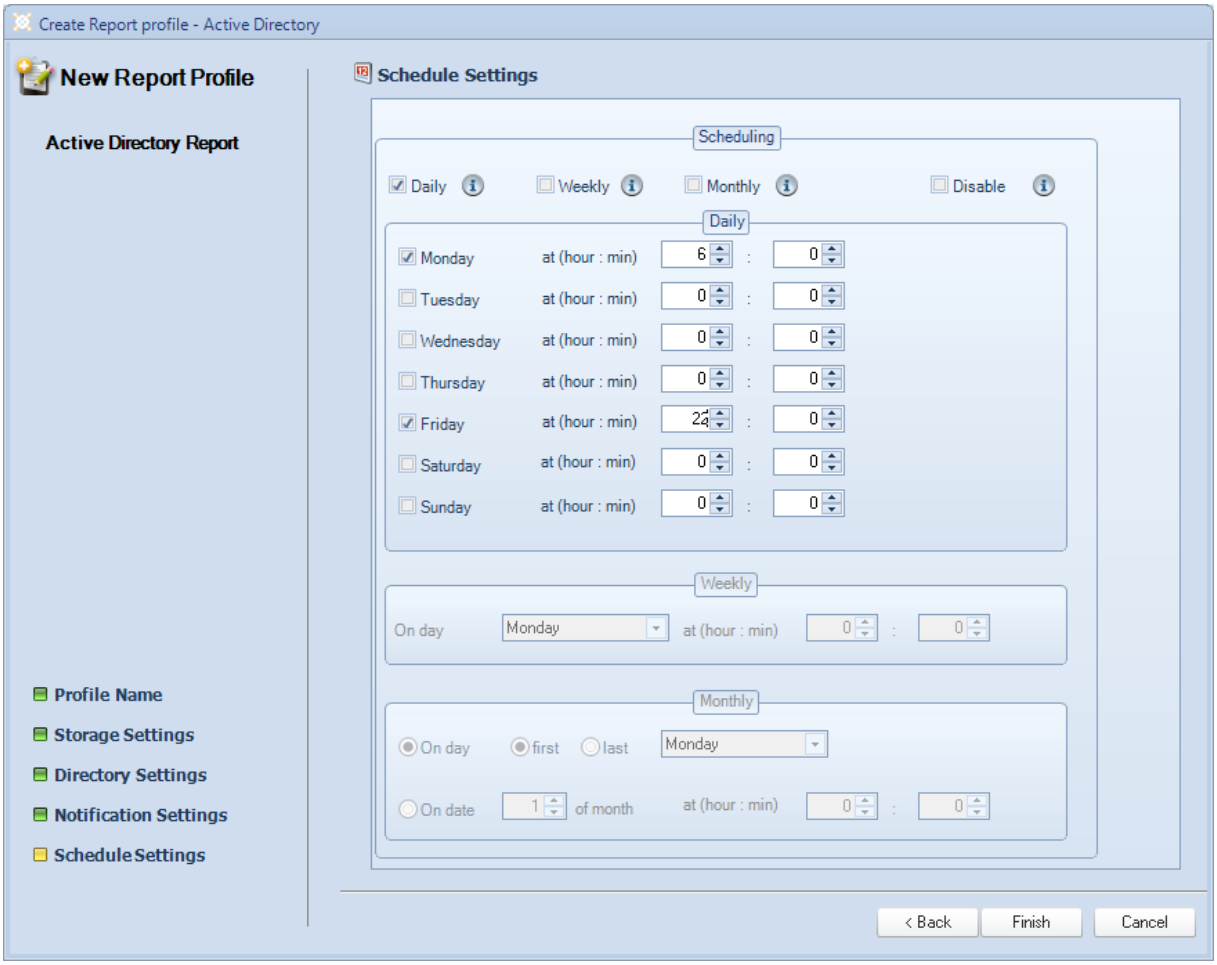
When the first Report is created, you can choose between three different views just like the File System Reports.

Weekly Delta Report to the Head of the IT-Department

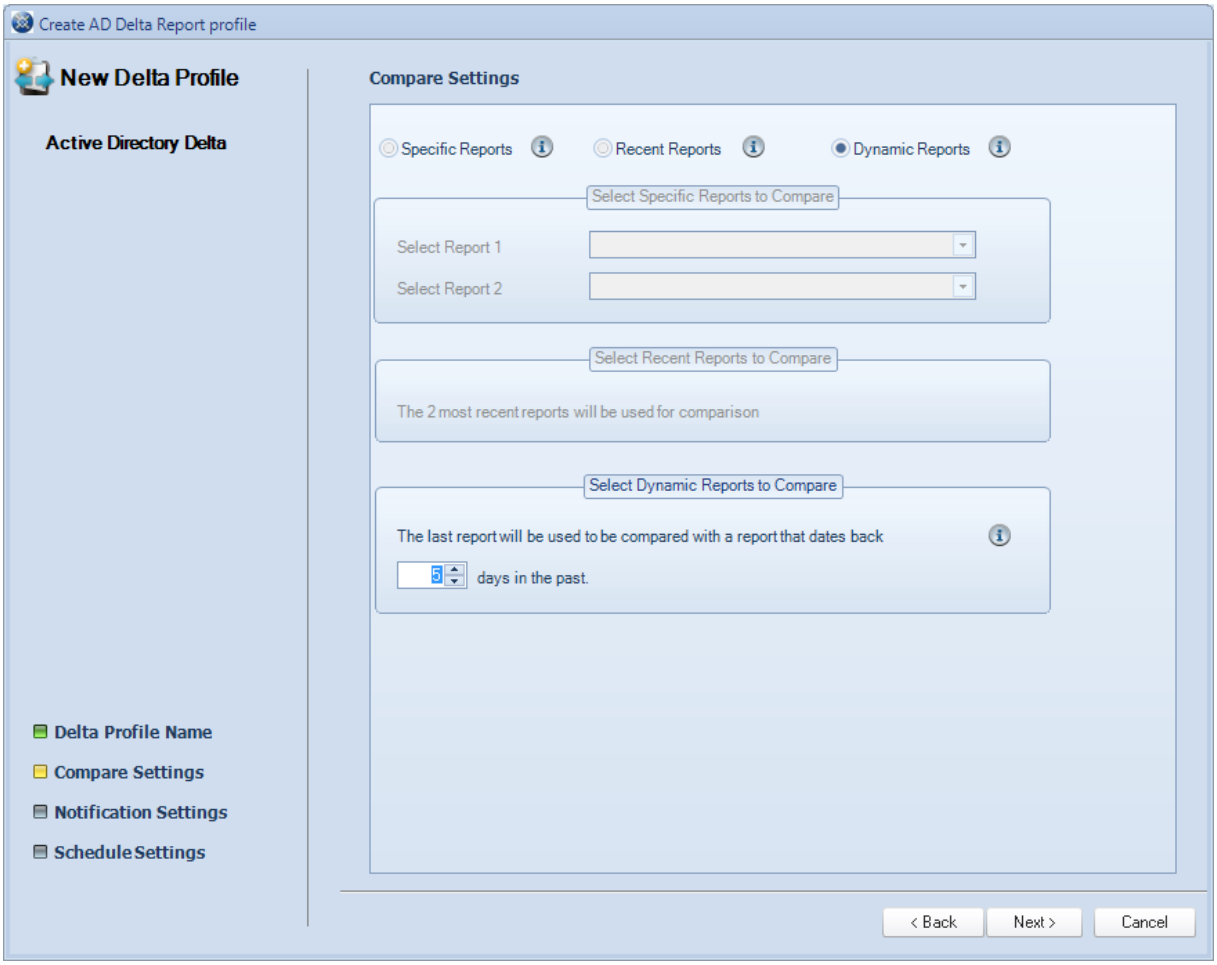
To better understand this section please read "The First Report", "Delta Reports" and "Scheduling" first.

This will report permission changes to the selected AD object on a weekly basis to the Head of the IT Department.

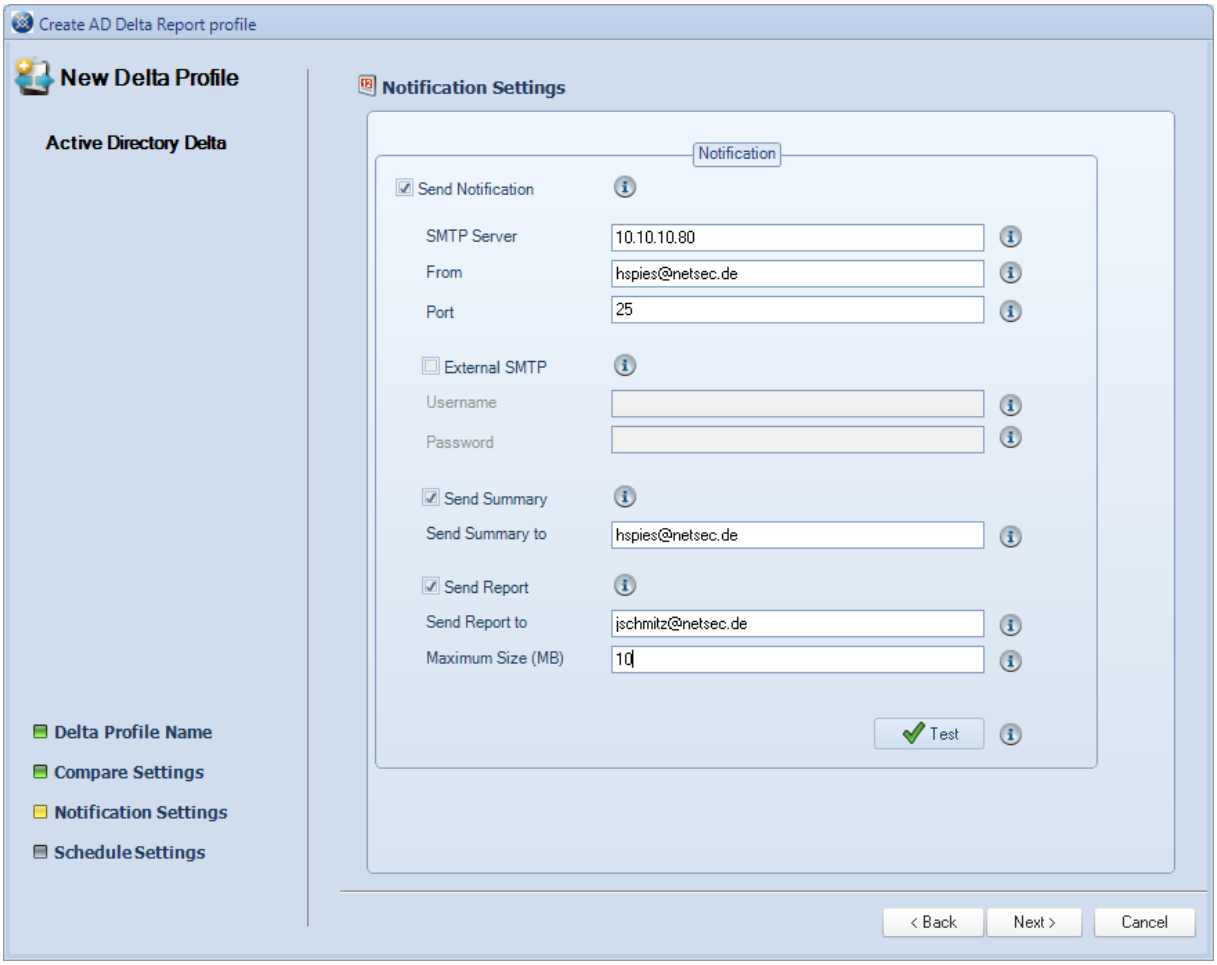
First, we need to create a report for the AD object we want to watch, in this example we used the container "Users" and schedule it to run Mondays at 6 AM and Fridays at 10 PM



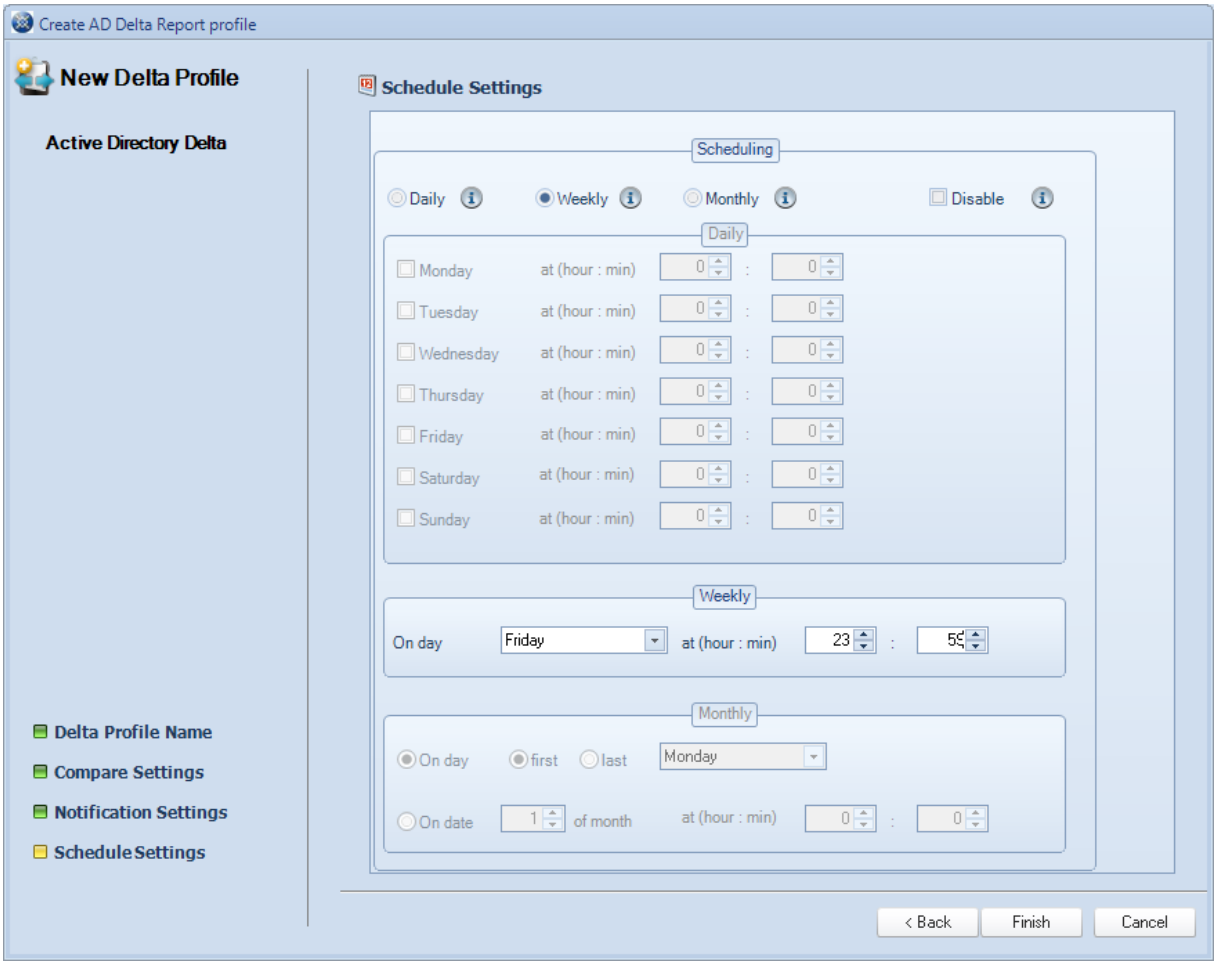
After that, we need to configure the Delta Report to compare the reports generated on Monday and Friday. The report must be a dynamic report 5 days back.



Here we change who gets the report sent to them, in this case we want the Head of the IT Department to receive this so they know who has permission within the container User.



As with File System we let the Delta Report run Friday at 23:59



After the Delta Report runs, the Head of the IT Department will have report automatically sent to them.

Membership Watch Report

The Membership Watch Reports can give you a quick report if anything was changed in a chosen group.

Tasks:

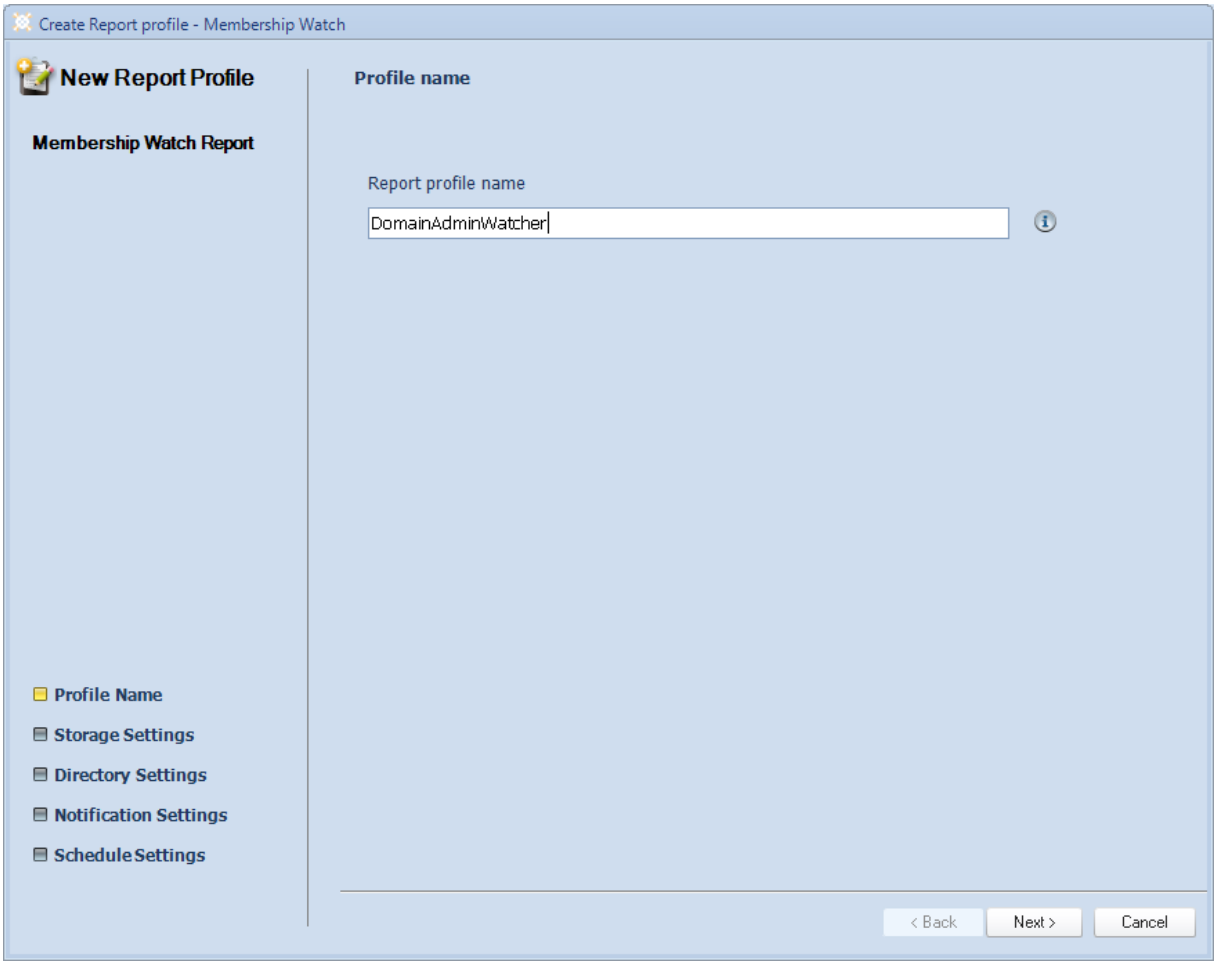
The Membership Watch Report can help you, to monitor mission critical groups (e.g. Domain Admins).

To complete these tasks, please first read "Filtering, Sorting, Exporting", "Delta Report" and "Scheduling".

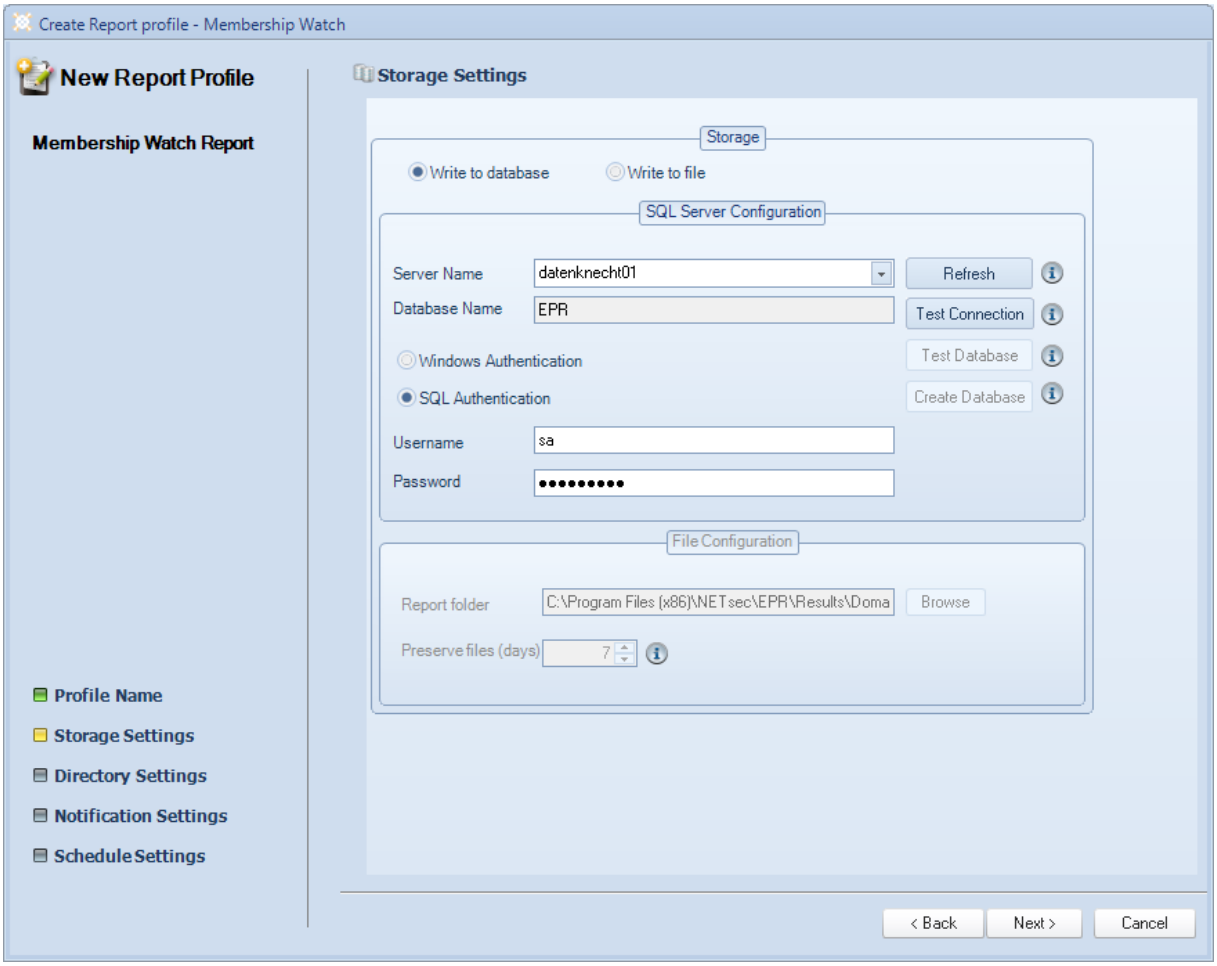
The First Report

To create a Membership Watch Report, click onto "Create Report Profile".

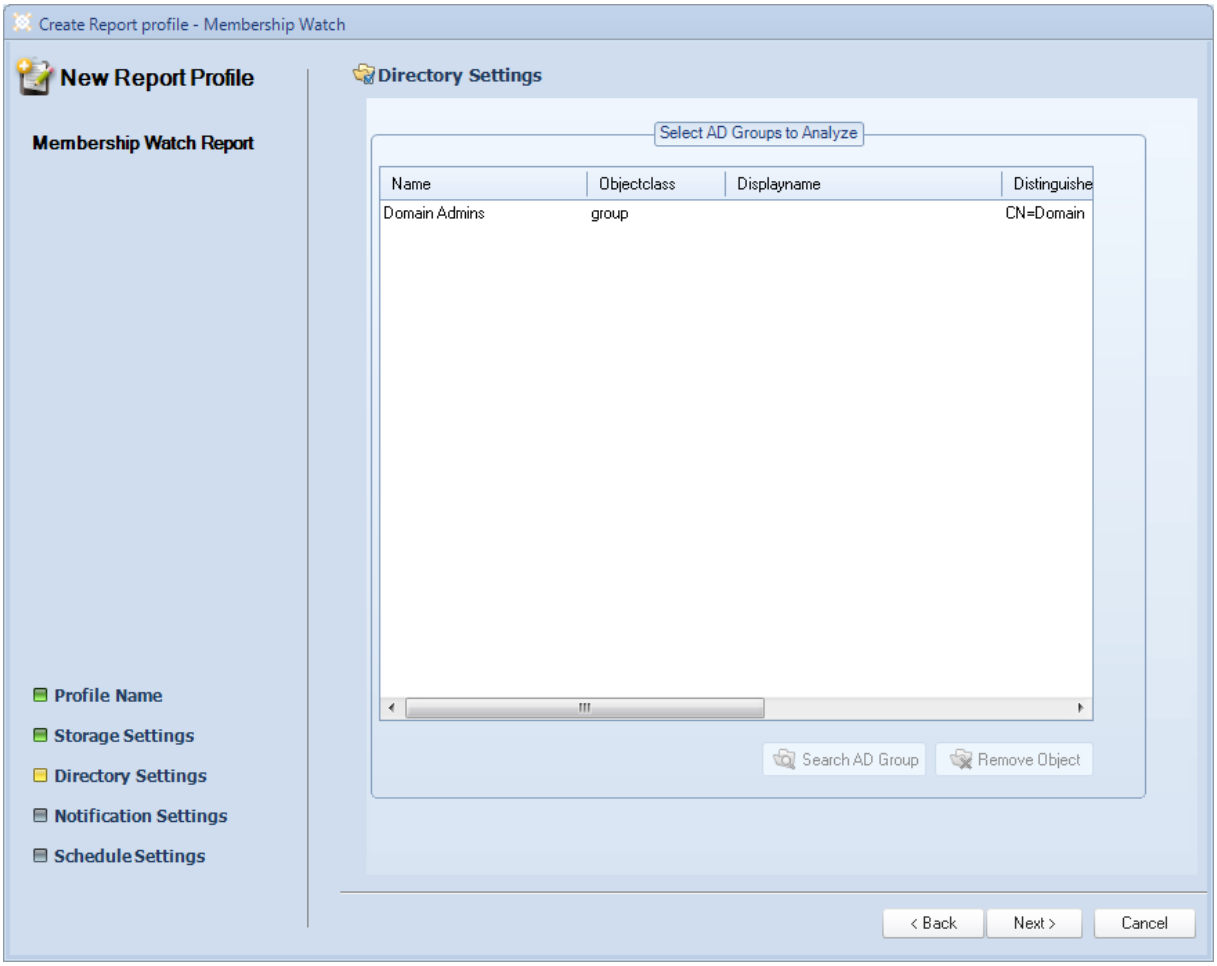
At first you have to enter a name for your Report Definition.



In the second step, you can decide where to save your reports (Database or File).



After this is done, you can choose an AD Group which you want to report.



When you click next, you can setup your Notification Settings.

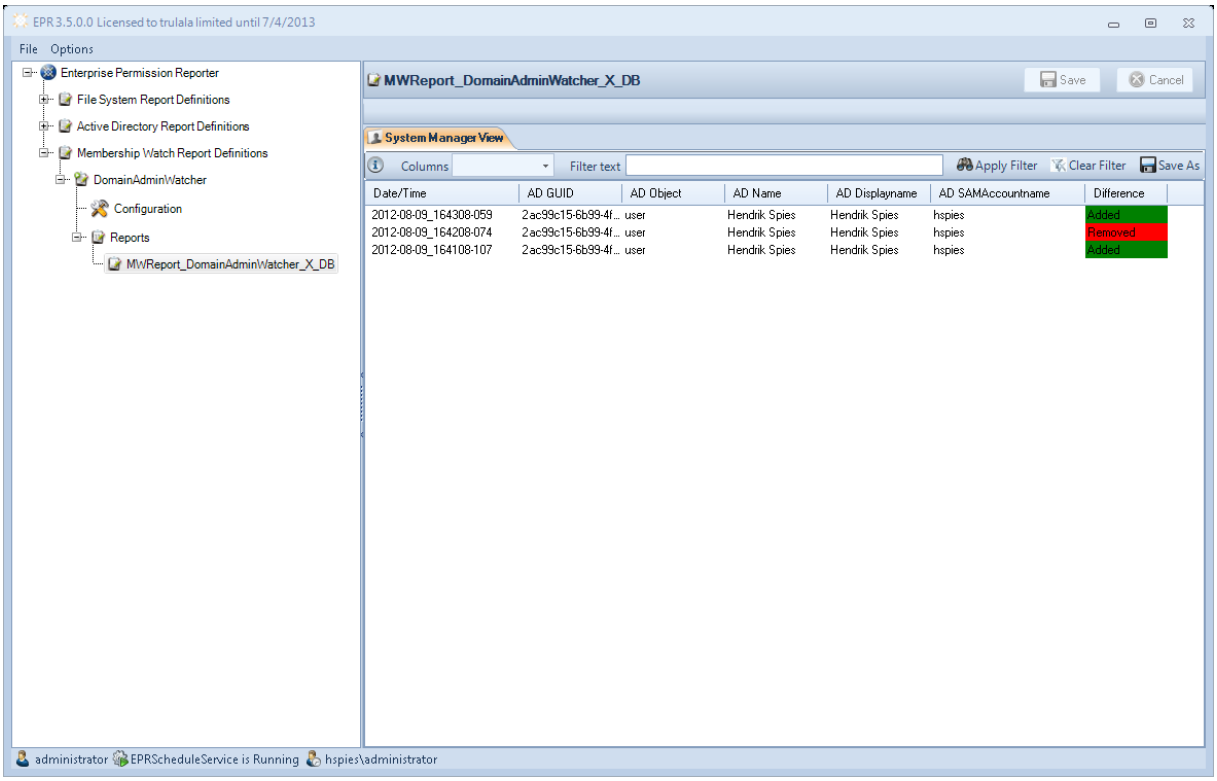
Afterwards, you have the possibility to set the interval the scheduling is running. The standard time is 1 Minute.

Notice: A Report will only be created if any changes were made in the AD Group.

When a change was made, you can get a summary near to real-time if you set the Notification Settings correctly.

Attention: If you configured a Membership Watch Report let 10 minutes go ahead before you do first changes.

During our example we removed someone from the Domain Administrators group and re-added them.



Licensing

Trial License

To use EPR in Trial

A trial license will allow you to analyze up to 100 folders in the File System Report.

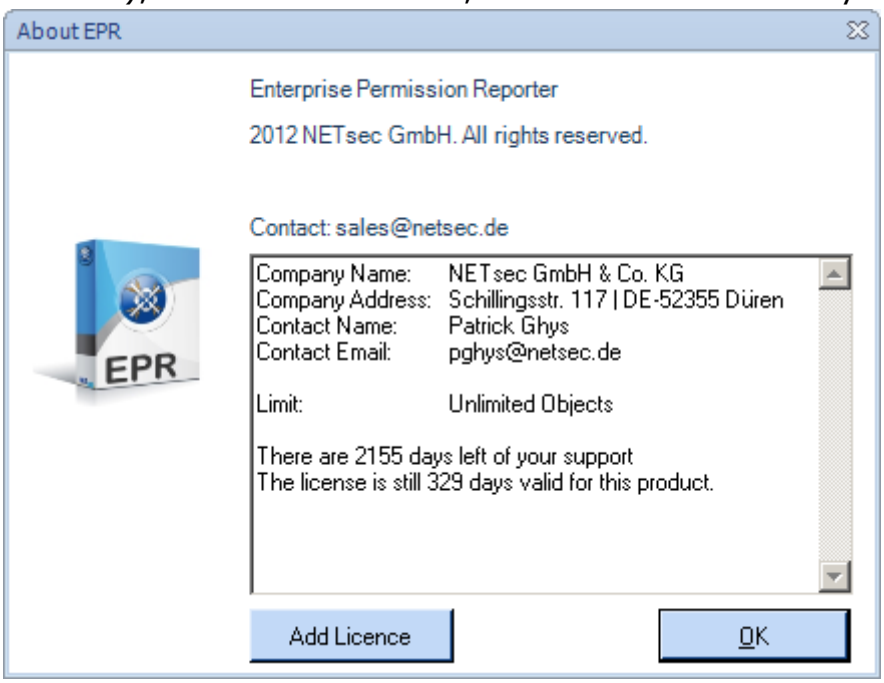
A trial license will allow you up to analyze up to 100 Active Directory Report.

A trial license will allow you to analyze 100 changes in the Membership Watch Report.

All functionality is available to you even though it is a trial. The trial license is automatically activated unless you replace it with a purchased license.

Add a License

To add a License you have bought, simply open the About Box (Options->About), click "Add License", and select the lic-File you got:



Support

EPR Technical Support is happy to help you in any regard.

Please contact us via email: Support@NETsec.de

or by Phone: +49 2421 998 78 20

Blogs

You find additional information on our blog
www.tools4activcedirectory.com