



EPR 3.0

Manual

NETSEC

02. April 2012

| | |
|---|-----------|
| General..... | 3 |
| What is EPR? | 3 |
| Where do I install EPR? | 3 |
| What's new?..... | 4 |
| Small & Medium Businesses | 5 |
| Large Businesses or Enterprises | 5 |
| Proposals..... | 5 |
| System Requirements..... | 5 |
| Setup..... | 6 |
| Configuration | 6 |
| Store System: | 7 |
| Notification: | 9 |
| Service Configuration | 10 |
| EPR Structure..... | 10 |
| Tasks..... | 12 |
| Simple, first Report..... | 12 |
| Filtering, Sorting, Exporting | 20 |
| Filtering | 20 |
| Exporting..... | 21 |
| Sorting..... | 21 |
| Delta Report..... | 21 |
| Scheduling..... | 28 |
| Monthly Compliance Report..... | 28 |
| Weekly Delta Report to Data owners..... | 28 |
| Licensing | 33 |
| Trial License | 33 |
| Add a License..... | 33 |
| Support | 33 |

General

What is EPR?

EPR (Enterprise Permission Reporter) is our NTFS 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 permissions with ease.

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. If you choose to SQL Express be aware that the setup will automatically install SQL Express on the local machine.

What's new?

The new version of EPR has several enhanced features compared to the old version and has been completely redesigned.

EPR 2.0 Feature List

- Generate Just-In-Time Based Reports for your File system
 - Includes EVERY Permission set to the folders
 - Breaks down every access to user level, including nested Groups
- Store your Reports in XML – Data will be stored in Excel-Friendly XML Files on your File system

EPR 3.0 Feature List

- Generate Just-In-Time or Scheduled based Reports for your File system
 - Includes EVERY Permission set to the folders
 - Breaks down every access to user level, including nested Groups
- Generate Just-In-Time or schedule based reports on the changes between two certain reports
 - Scheduled delta reports enables you to report permission changes within a week, month, or any other timespan
- Store your Reports in
 - XML – Data will be stored in Excel-Friendly XML Files on your File system
 - SQL – Data will be stored in any SQL Server in your Network

Small & Medium Businesses

If you are a small or medium sized business (<1000 users) we recommend that you use CSV files to store the reports, however if you wish to use an SQL Server / SQL Express to store the report data you are welcome to do so.

Large Businesses or Enterprises

If you are a large business or enterprise (>1000 users) we recommend that you use an SQL Server / SQL Express to store your reports, however you are not required to do so.

Proposals

- Permissions
 - The account running EPR and the EPRScheduledService should be able to:
 - Read all Folders that are to be analyzed
 - Read Active-Directory
 - Write the Store you want to Store the Reports (SQL 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 XP SP3
 - ii. Windows Vista
 - iii. Windows 7
 - iv. Windows Server 2003 SP2
 - v. Windows Server 2003 R2
 - vi. Windows Server 2008
 - vii. Windows Server 2008 R2
5. Other Requirements
 - a. .NET Framework 2.0 +
 - b. All recommended Windows Updates
6. SQL Server Versions
 - a. All SQL Editions 2008 and above are supported (Including Express)

If you plan on using EPR with an SQL Database, you will need to have an SQL Server 2008 or up installed within the domain. If you wish to send summary emails you will need to have a Microsoft Exchange Server installed within your domain.

Setup

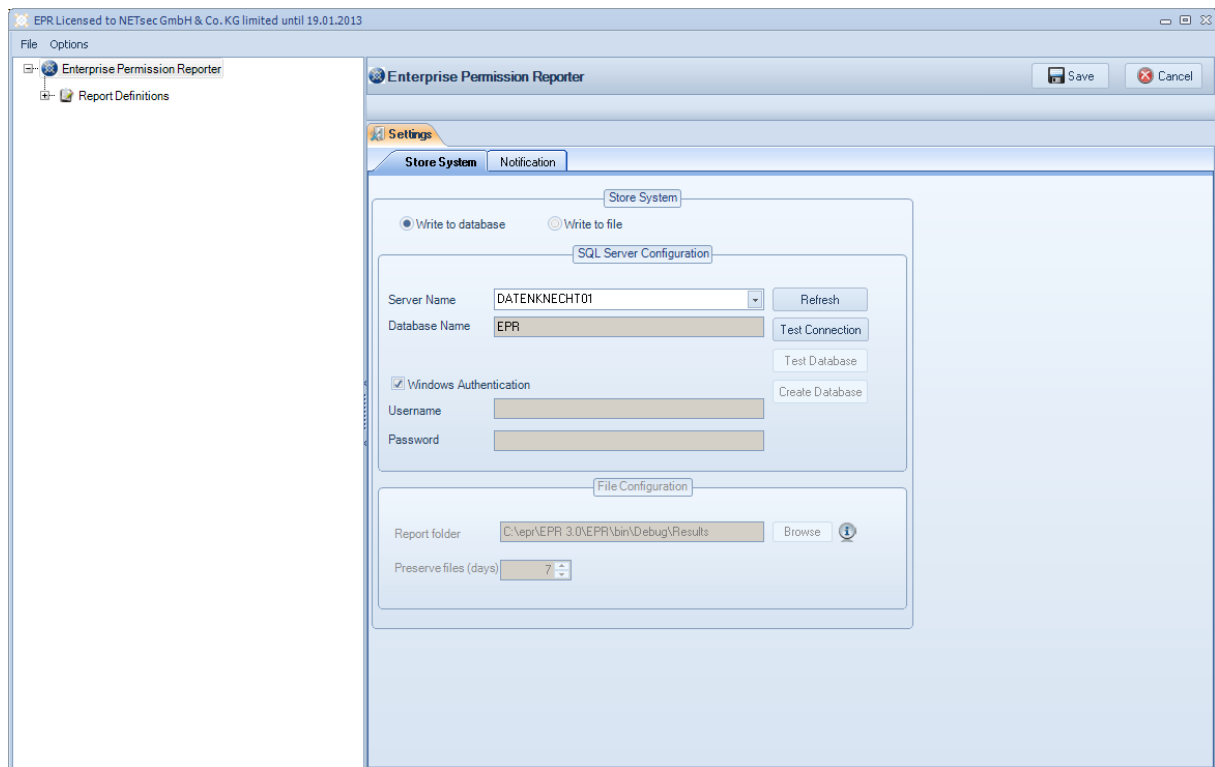
This will install and register all the components necessary to run Enterprise Permission Reporter on your server or workstation. Setup will create a folder NETsec\Enterprise Permission Reporter in the start menu, and place a shortcut onto your desktop. After first program start there will be additional 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 take special care to the Account the service is logging in as. You may review this setting under Options->Service Configuration.

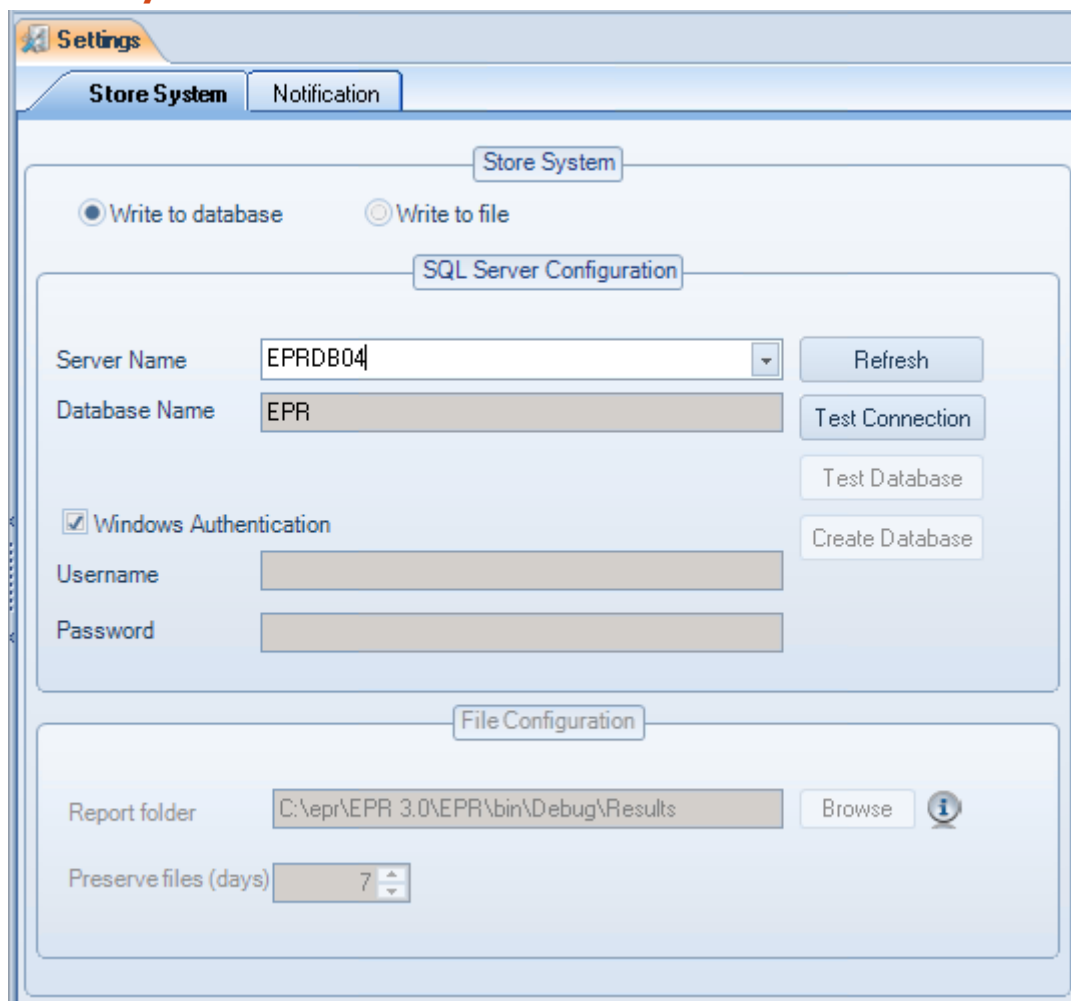
Configuration

When starting EPR for the First time, you should take a minute to setup the "General Settings". This includes Store system and Mail configuration. Once you have set up the General Settings, these will be set 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 do support both store types, file and SQL, but we consider File to be only used for a fast test and evaluation phase, as heading on to larger result amounts a SQL Database is the best choice in cases of performance, reliability and compliance conformity.

You can either enter the SQL Server name by Keyboard, or hit "Refresh" to get a List of all SQL Servers in your network. Once you have selected the desired SQL Server and configured the authentication method, you can go ahead a "Test Connection". This will check if you are able to authenticate to the given Server name and tell if any connection issues exist. After this is successful, you can now hit "Test Database". This will check for the existence of the EPR Database on the given Server. If the Database is not present, it will ask you to create it. Please Note that the Database has to be created by the Software, as we use several stored procedures and user-defined tables.

Notification:

The screenshot shows the 'Settings' window with the 'Notification' tab selected. The 'Notification' sub-tab is also active. The settings are as follows:

- ☒ Send Notification (info icon)
- SMTP Server: devexchange10 (info icon)
- From: EPR@dev.netsec.de (info icon)
- Port: 25 (info icon)
- ☐ External SMTP (info icon)
- User Name: pghys (info icon)
- Password: (info icon)
- ☒ Send Summary (info icon)
- Send Summary to: pghys@netsec.de (info icon)
- Subject: Summary for PR Test (info icon)
- ☒ Send Report (info icon)
- Send Report to: pghys@netsec.de (info icon)
- Subject: Report XXX 1 (info icon)
- Maximum Size: 50 (info icon)
- Test button (green checkmark icon) (info icon)

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.

External SMTP:

You are also able to use an external SMTP, such as Hotmail, by providing corresponding credentials.

Send Summary:

This will send a summary of the Report after every run, including Timestamps, success, and number of Results. This may be interesting for the administrator monitoring the application.

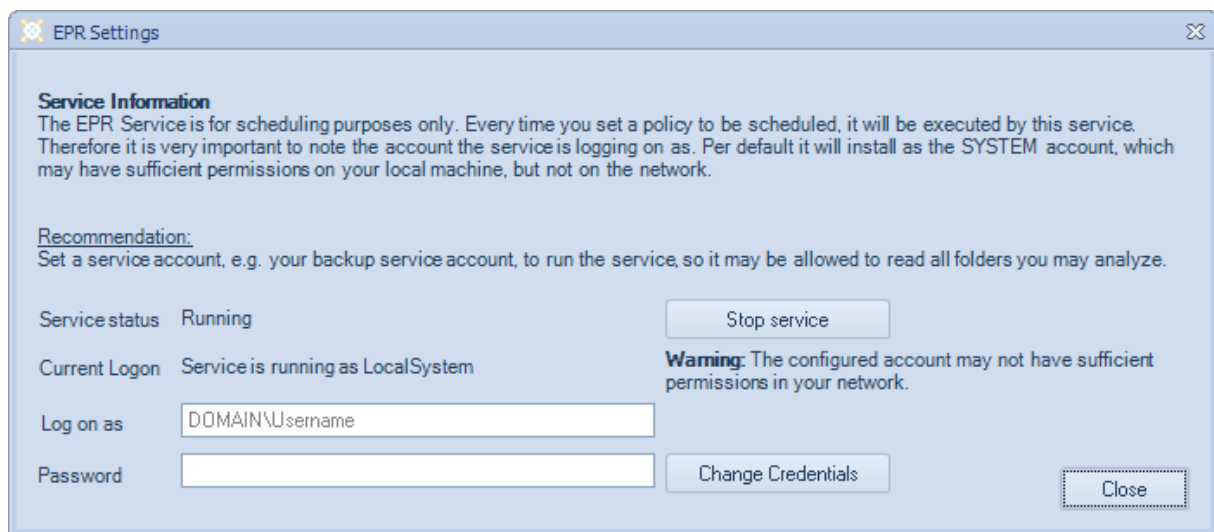
Send Report:

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.

Using the Test Button you can check if your settings are correct.

Service Configuration

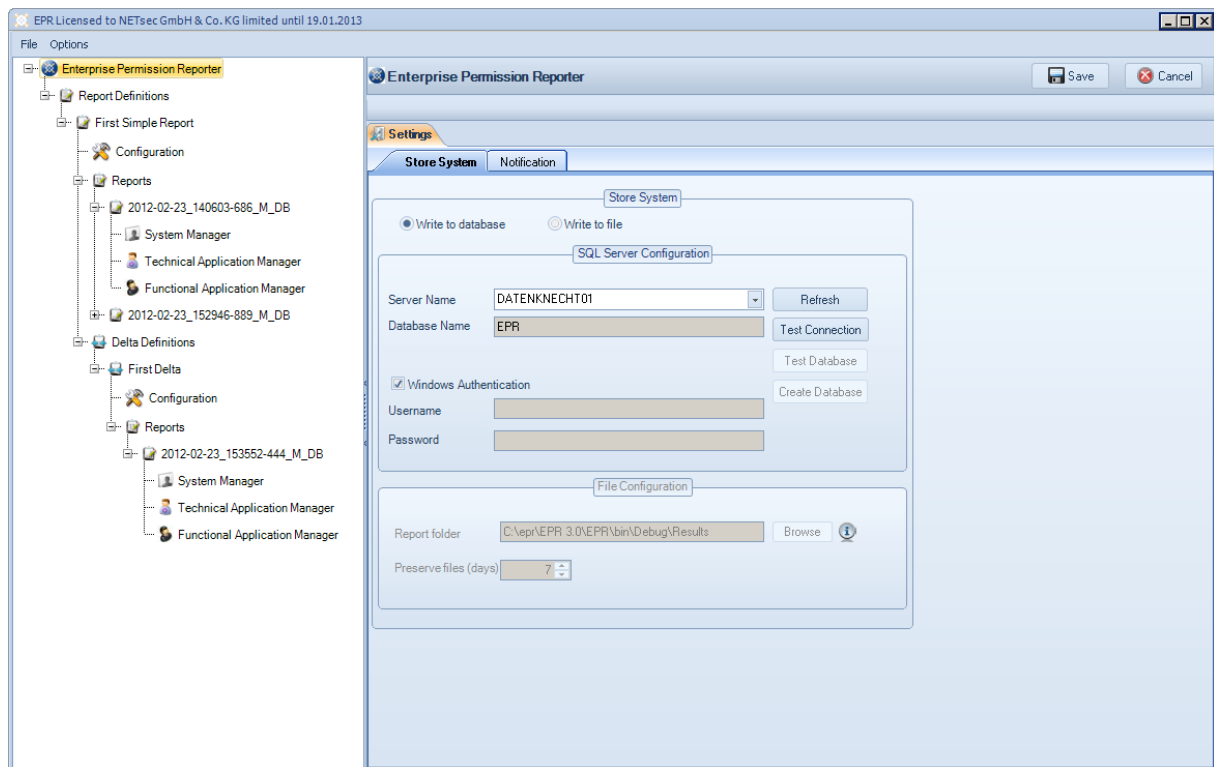
After setting up the general settings, the last configuration aspect is the Service Configuration. We open this up by clicking Options->Service Configuration:



After a fresh install, the service runs as LocalSystem per Default. You should now consider changing the account running the service, as any scheduled report will run under permissions of this account. Your LocalSystem Account will not have sufficient permissions in your network. We recommend using your Backup Service Account for this.

EPR Structure

The Main Element in EPR is the Report Definition. This element describes what should be reported, where it 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.



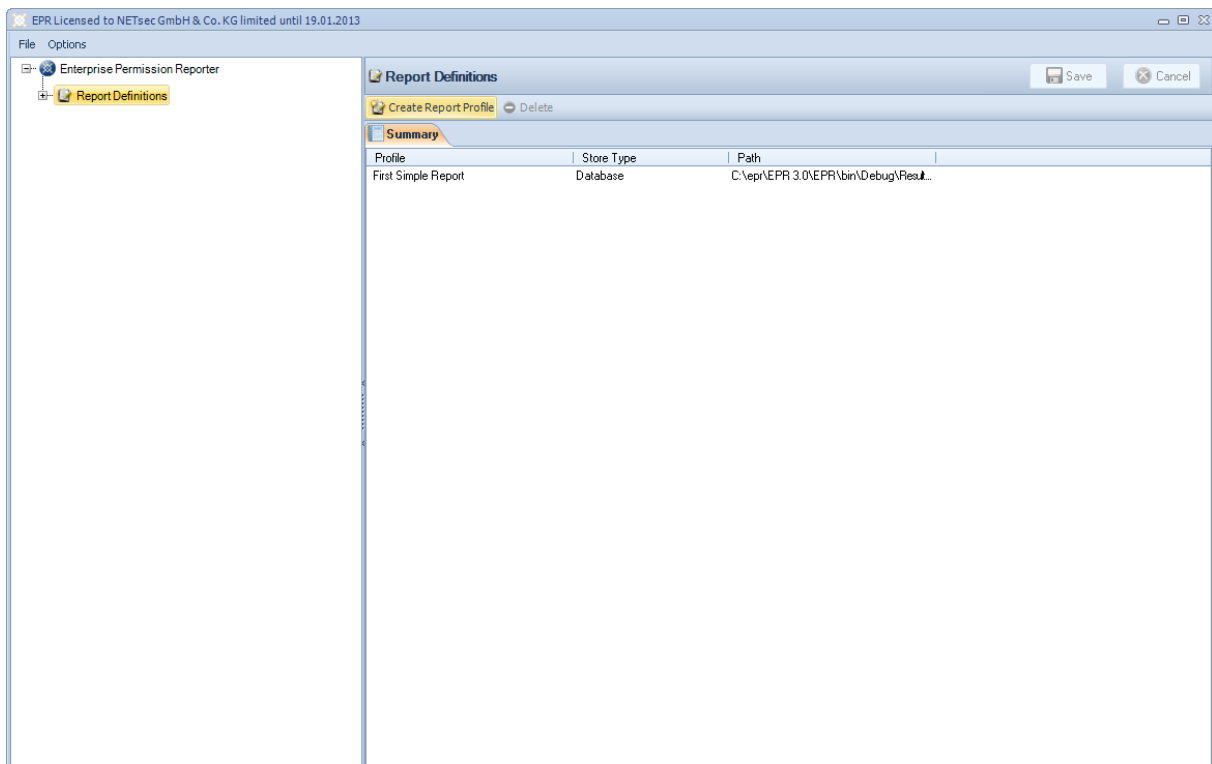
- Report Definition
 - Configuration
 - Reports
 - Report
 - System Manager
 - Technical Application Manager
 - Functional Application Manager
 - Delta Definitions
 - Delta Report
 - Configuration
 - Reports
 - Report
 - System Manager
 - Technical Application Manager
 - Functional Application Manager

Tasks

In this Section, we want to walk you through the most common Tasks you may want to achieve with EPR.

Simple, first Report

Let's start off with your first Report. Given that you are running the application on your Domain-Computer, a short analyze of your Users Folder might be Interesting. Let's start off by creating a new Report Definition by selecting "Report Definitions" and clicking "Create Report Profile" in the action pane of using the context Menu:



The screenshot shows a software window titled "Create Report Definition". Inside, there's a section titled "New Report Definition" with a sidebar on the left containing five options: "Report Definition" (selected), "Storage Settings", "Directory Settings", "Status Notification Settings", and "Schedule Settings". The main area is titled "Report Definition Name" and contains the instruction "Enter Report Definition Name". Below this is a text input field labeled "Report definition name" which contains the text "Simple First Report". To the right of the input field is an information icon. At the bottom right of the window are three buttons: "< Back", "Next >", and "Cancel".

After providing a Name, we click next.

Create Report Definition

New Report Definition

- Report Definition
- Storage Settings
- Directory Settings
- Status Notification Settings
- Schedule Settings

First Simple Report

Store System

☒ Write to database ☐ Write to file

SQL Server Configuration

Server Name: DATENKNECHT01

Database Name: EPR

☒ Windows Authentication

Username:

Password:

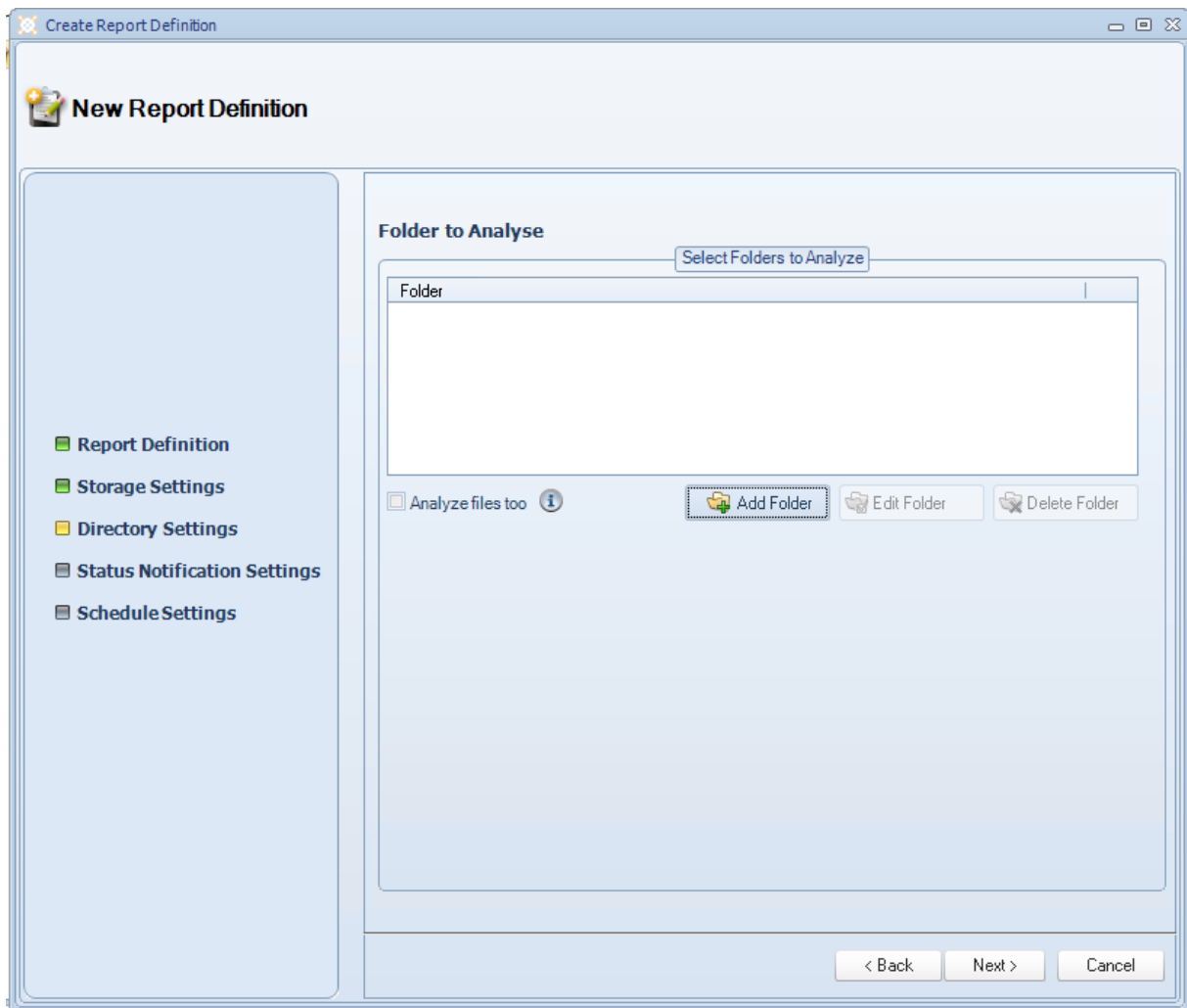
File Configuration

Report folder: C:\ep\r\EPR 3.0\EPR\bin\Debug\Results\First Simp

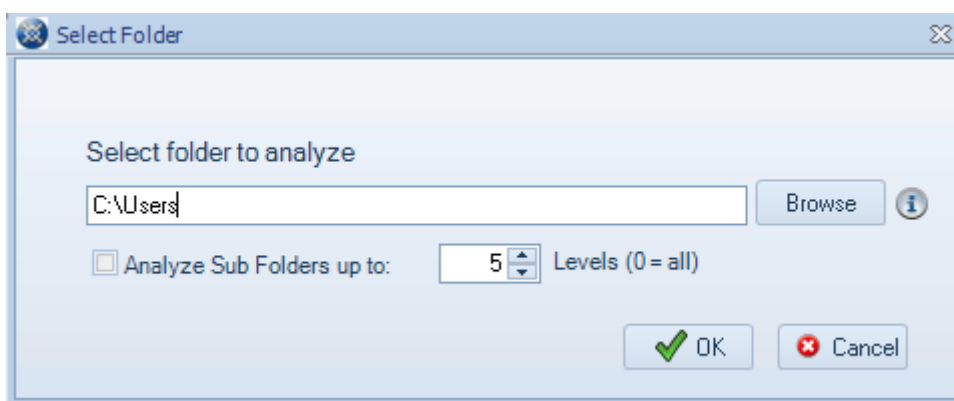
Preserve files (days): 7

< Back Next > Cancel

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 might want to Analyze by clicking “Add Folder”:



We can either type in the UNC Path of the desired Folder or use the Browse Button. After selecting the desired Folder, we should consider including subfolders. Doing so we are also able to limit the subfolder levels EPR shall analyze. The Default value is 5, setting 0 means unlimited

subfolders. For our first Report, using Level 5 should do the trick. After acknowledging with OK we can hit next.

Create Report Definition

New Report Definition

- Report Definition
- Storage Settings
- Directory Settings
- Status Notification Settings**
- Schedule Settings

Status Notification Email

Notification

☒ Send Notification ⓘ

SMTP Server: devexchange10 ⓘ

From: EPR@dev.netsec.de ⓘ

Port: 25 ⓘ

☐ External SMTP ⓘ

User Name: pghys ⓘ

Password: ⓘ

☒ Send Summary ⓘ

Send Summary to: pghys@netsec.de ⓘ

Subject: Summary for PR Test ⓘ

☒ Send Report ⓘ

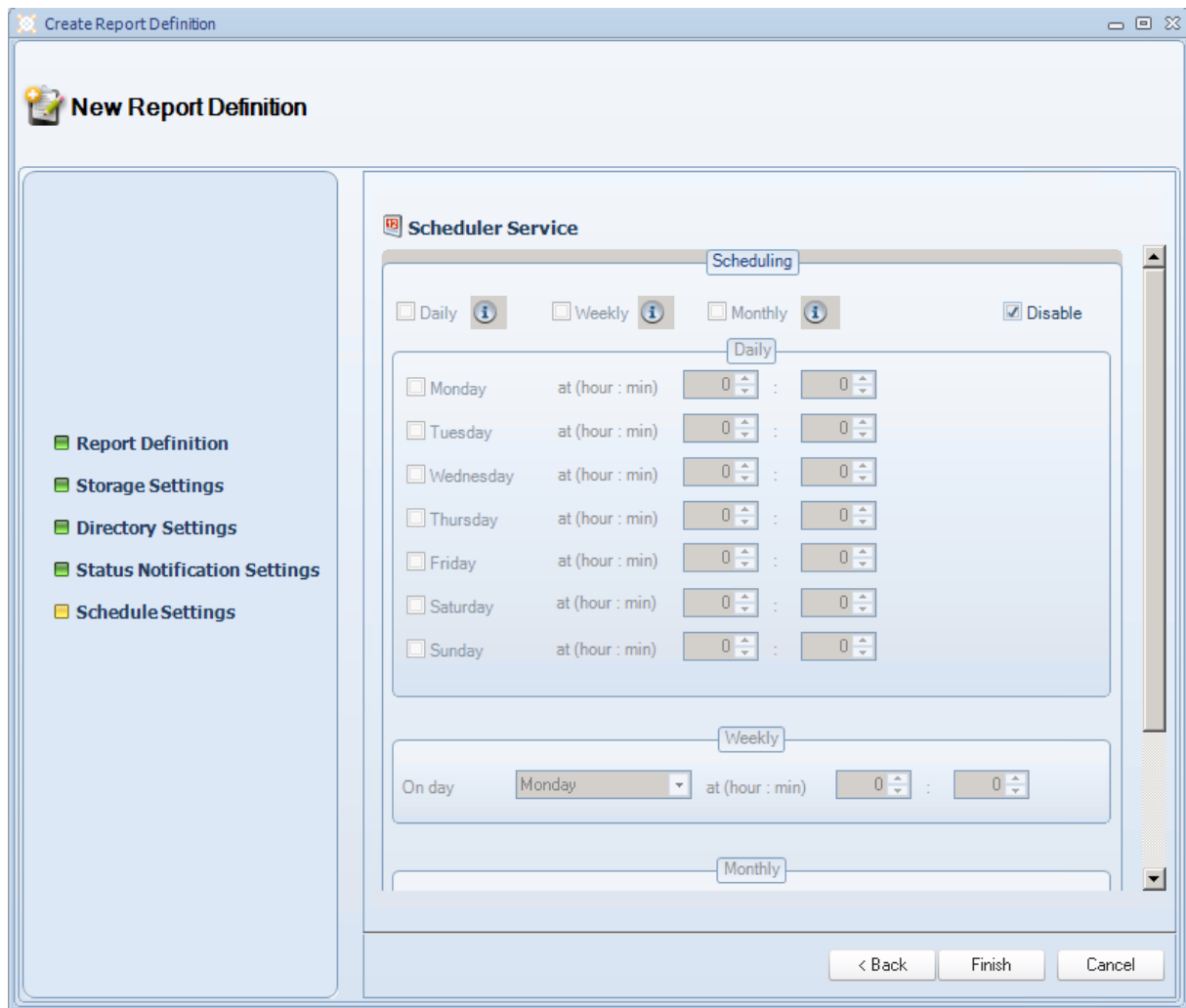
Send Report to: pghys@netsec.de ⓘ

Subject: Report XXXY 1 ⓘ

Maximum Size: 50 ⓘ

< Back Next > Cancel

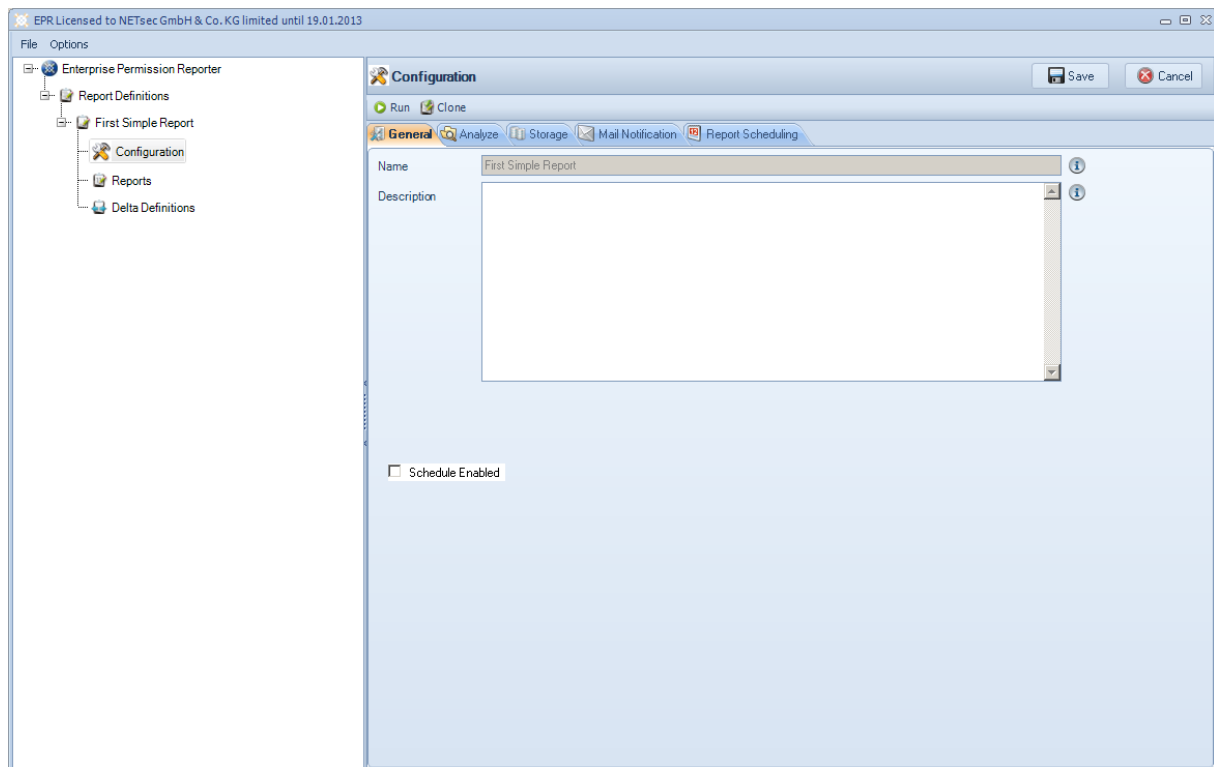
Similar to our Store type, the default Settings earlier apply to the Status Notification. Assuming the default is correct, we can go ahead clicking next.



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.

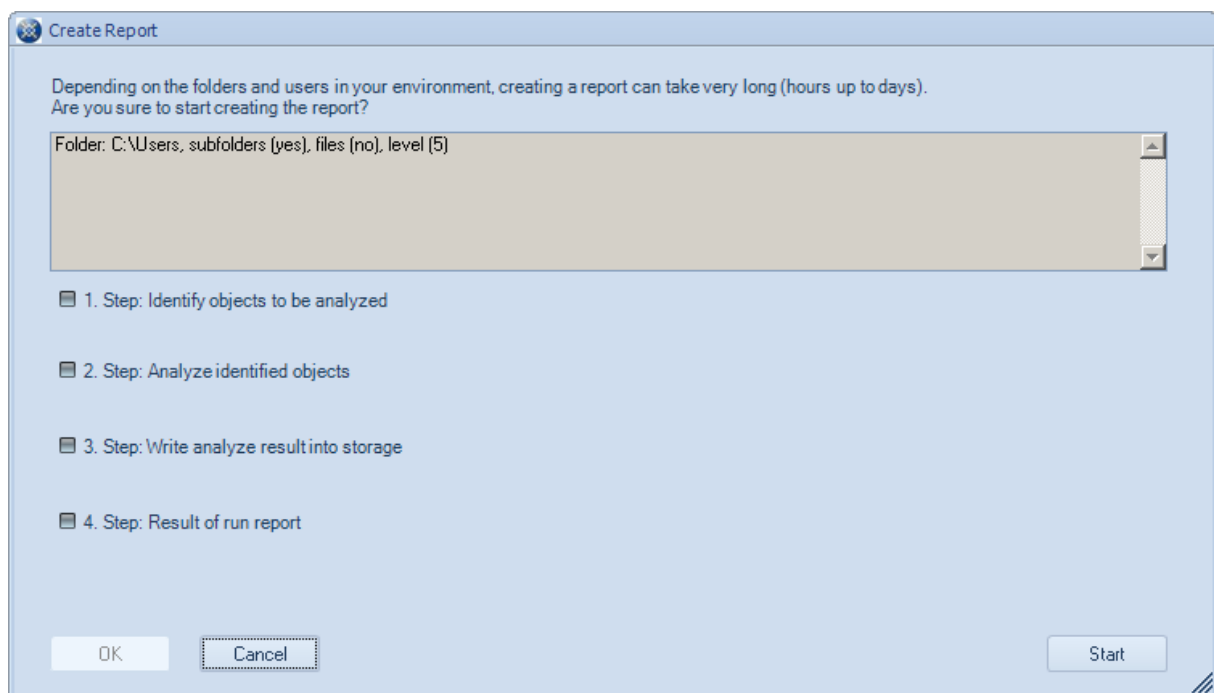
(Note: Scheduling will be described in "Monthly Compliance Report")

We now see our First Simple Report selected in the EPR Menu Structure:

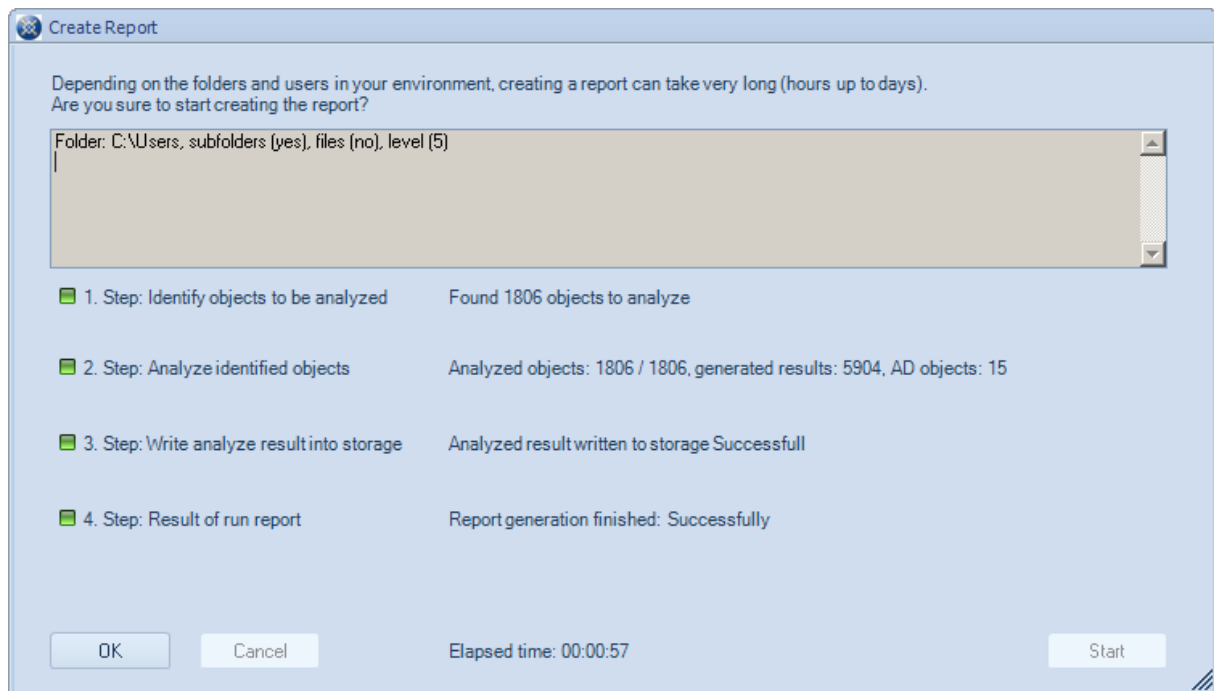


The Configuration Node shows us each Wizard Page we just went through as a Tab on the right side. We may change anything we just configured, as long as we do not have any Reports created for this Definition. This would prevent the Report Definition from withstanding any compliant check and also negate any Results existing inside the Report.

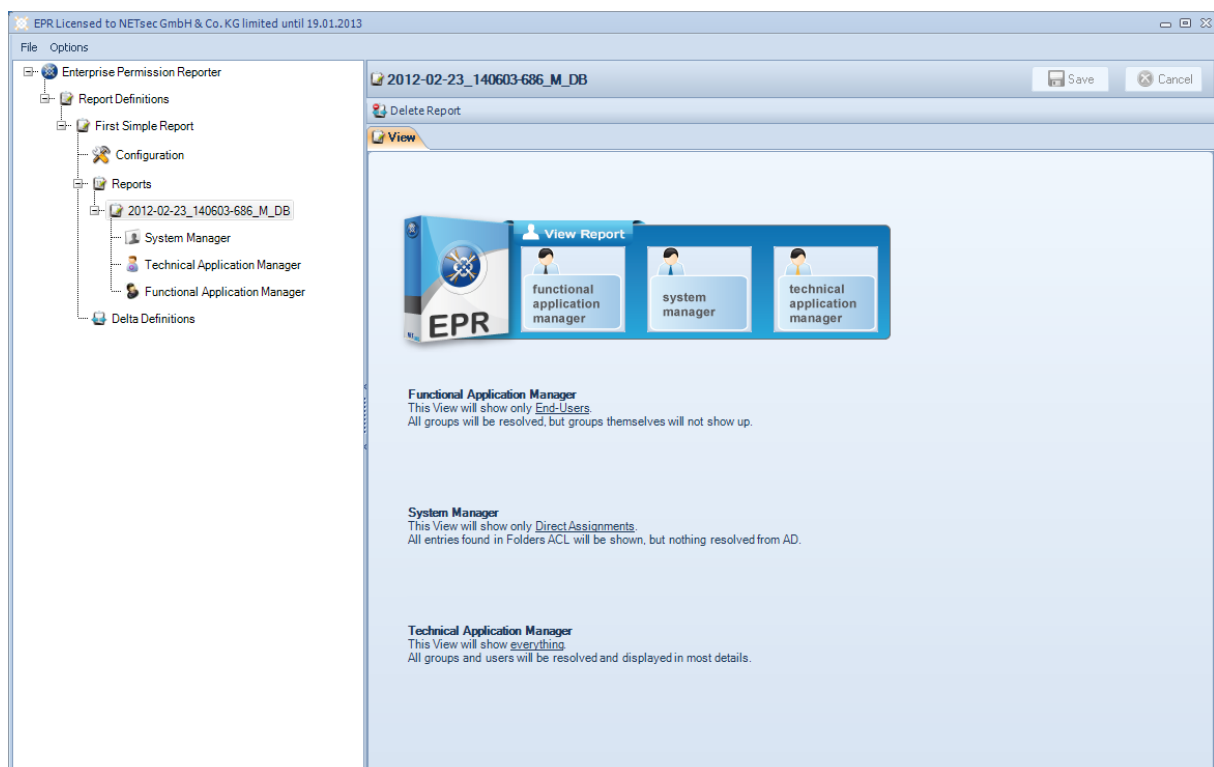
As we are ready to go, we may now hit Run to start up the first Report:



We now might check the settings we provided and click Start whenever 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:



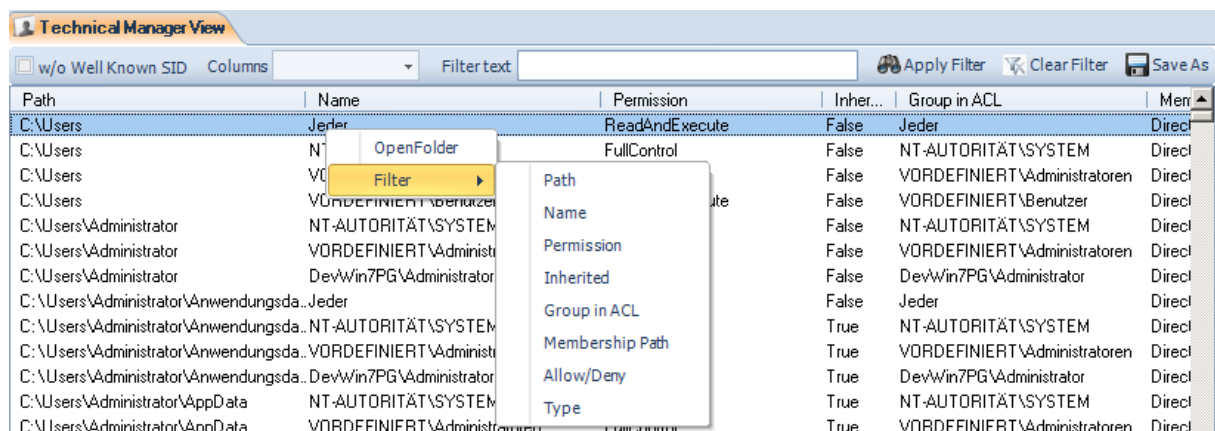
Viewing a Report can be done using 3 different Views, each including their own filters:

- Functional Application Manager
 - o This View will show only End-Users.
All groups will be resolved, but groups themselves will not show up.
- System Manager
 - o This View will show only Direct Assignments.
All entries found in Folders ACL will be shown, but nothing resolved from AD:
- Technical Application Manager
 - o 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 may view using EPR, you are always able to Filter and Export what you see. To apply a Filter you can go 2 ways:



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 "without Well Known SIDs", 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 Report

To walk through this section, please go through "Simple, 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:

Create Delta Report Definition

New Delta Report Definition

- Delta Report Definition
- Report Comparing
- Notification Settings
- Schedule Settings

Delta Report Definition Name

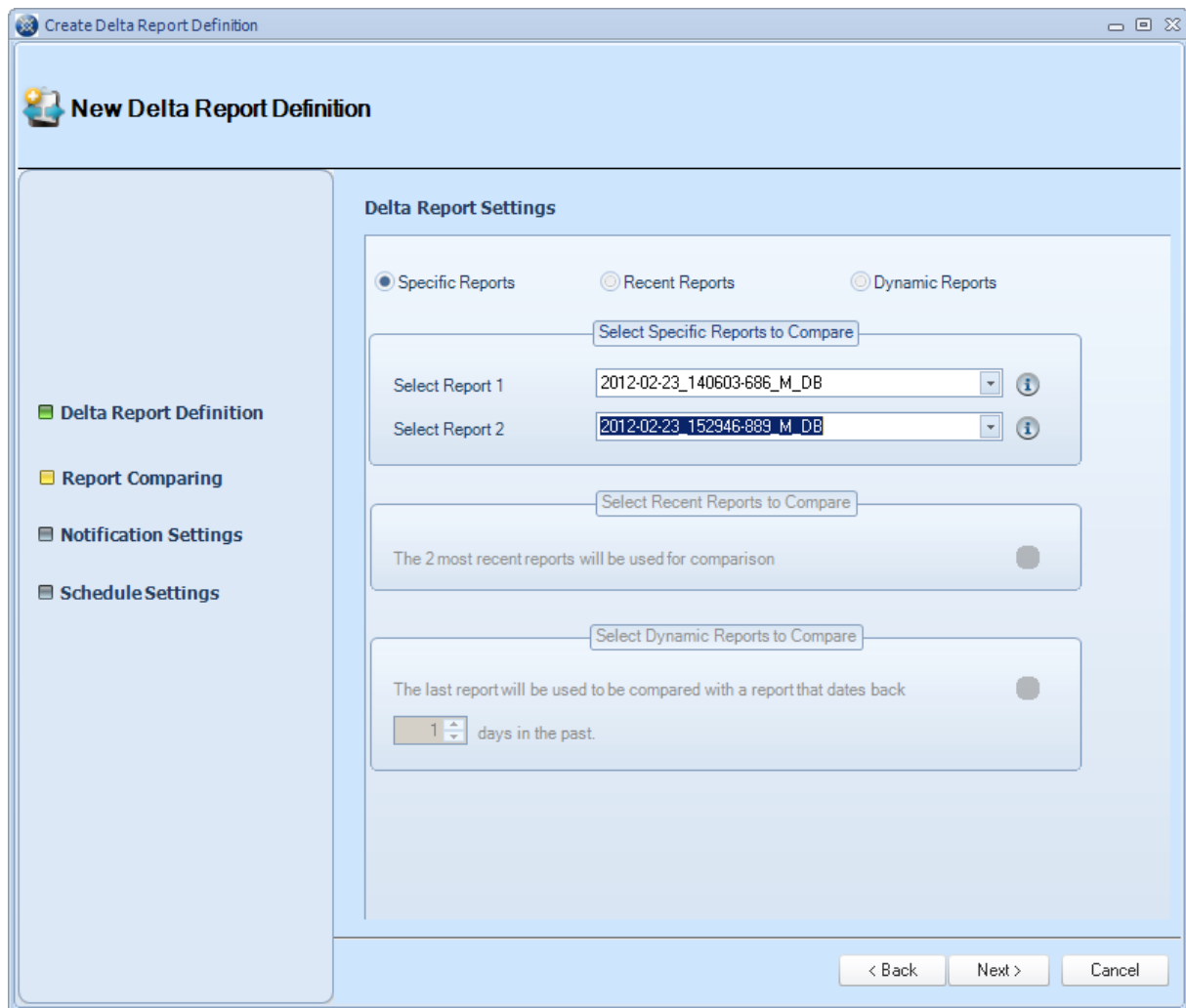
Enter Delta Report Definition Name

Delta Report Name

First Delta

< Back Next > Cancel

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:

Create Delta Report Definition

New Delta Report Definition

- Delta Report Definition
- Report Comparing
- Notification Settings
- Schedule Settings

Send Email Summary

Notification

☒ Send Notification ⓘ

SMTP Server: devexchange10 ⓘ

From: EPR@dev.netsec.de ⓘ

Port: 25 ⓘ

☐ External SMTP ⓘ

User Name: pghys ⓘ

Password: ⓘ

☒ Send Summary ⓘ

Send Summary to: pghys@netsec.de ⓘ

Subject: Summary for PR Test ⓘ

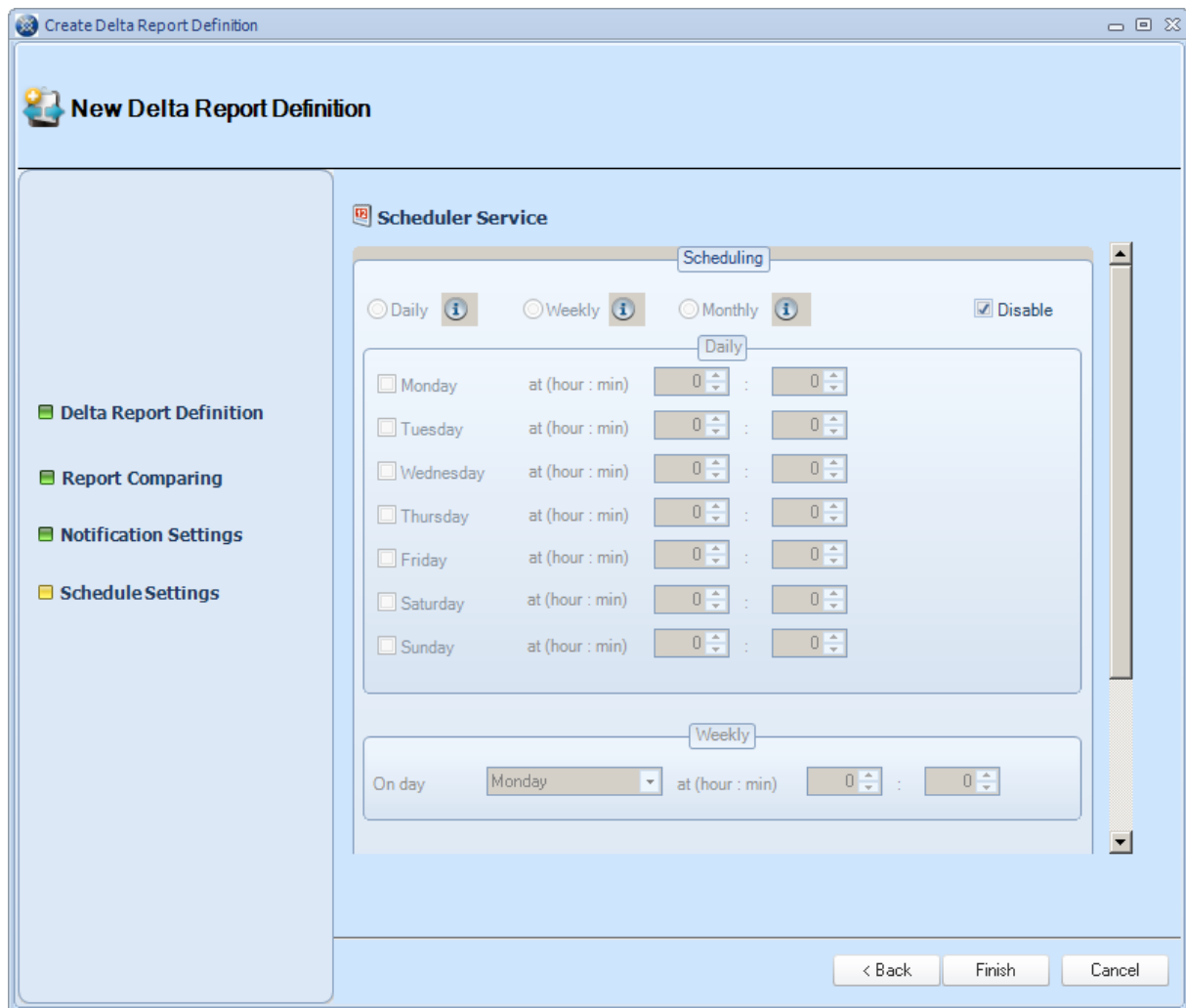
☒ Send Report ⓘ

Send Report to: pghys@netsec.de ⓘ

Subject: Report XXXY 1 ⓘ

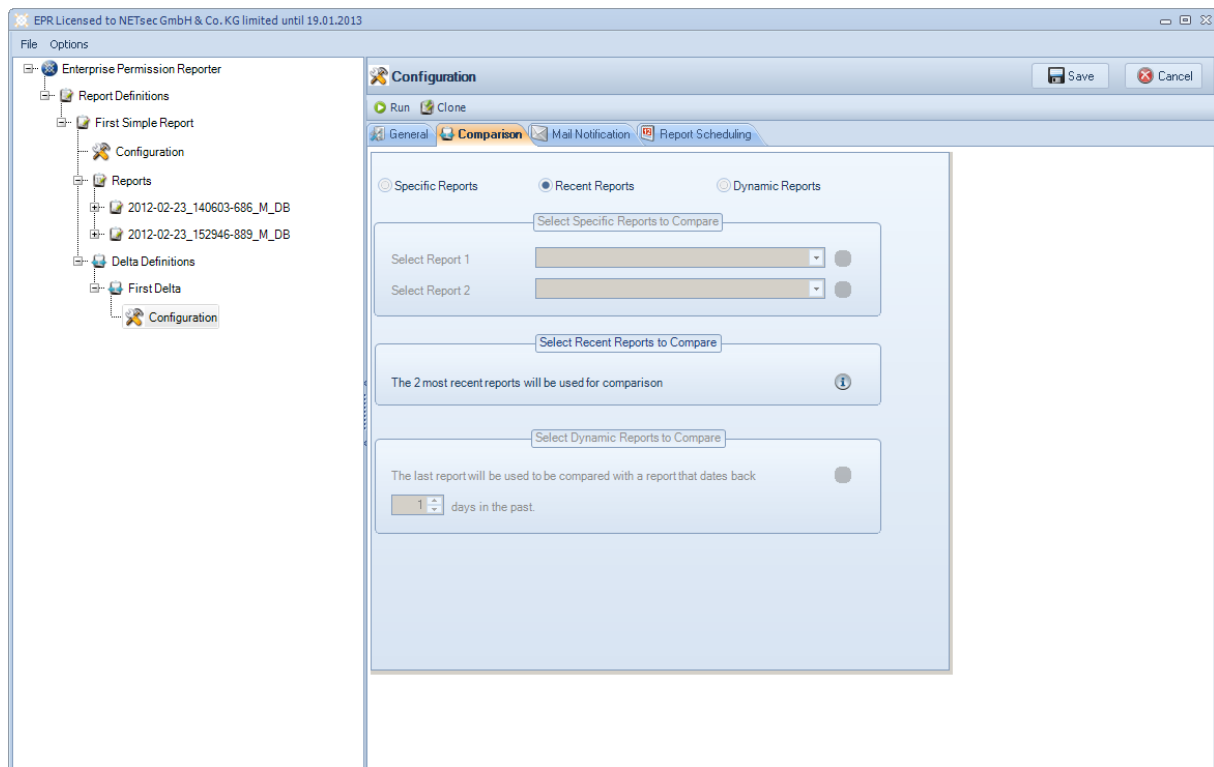
< Back Next > Cancel

Here we find the Mail Notification form again filled in with our Default Values. We might consider changing the Subject or To-Addresses here. Clicking Next leads us to the Scheduling form:

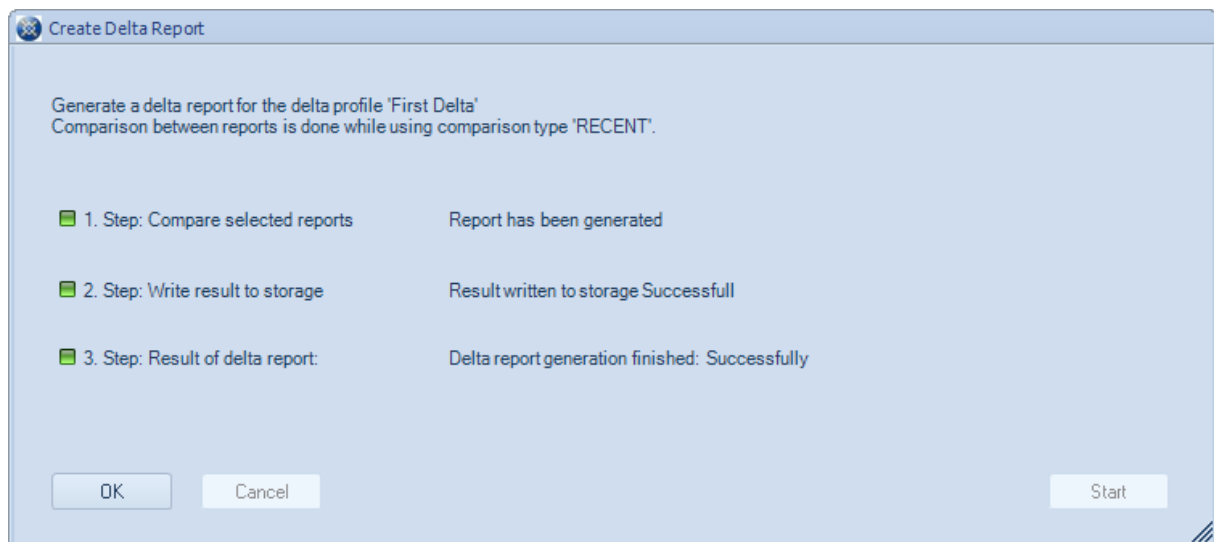


This would only make sense using Recent or Dynamic report selection, so we leave it disabled and click Finish.

Again we find the just created Delta 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:

Scheduling

Monthly Compliance Report

To walk through this task, please go through “Simple, first Report” and “Delta Report” 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:

The screenshot shows a 'Scheduling' window with three tabs: 'Daily', 'Weekly', and 'Monthly'. The 'Monthly' tab is selected. At the top, there are checkboxes for 'Daily', 'Weekly', 'Monthly' (checked), and 'Disable'. Each has an information icon. Below the tabs, the 'Daily' section is active, showing a list of days from Monday to Sunday, each with a checkbox and a time selector 'at (hour : min)' with two spinners set to 0. The 'Weekly' section shows 'On day' set to 'Monday' and a time selector set to 0. The 'Monthly' section shows 'On day' selected with 'first', 'last', and 'day' options, and a time selector set to 0. Below that, 'On date' is selected with a spinner set to 1 and 'of month' text, and a time selector set to 22.

Weekly Delta Report to Data owners

To walk through this task, please go through “Simple, first Report” and “Delta Report” first.

This Task aims to the delivery of a CSV File per email to every Data owner wishing to get a weekly change Report on Permissions 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, one time at the start, and one time at the end of the Week, like this:

The screenshot shows a 'Scheduling' window with three tabs: 'Daily', 'Weekly', and 'Monthly'. The 'Daily' tab is selected. At the top, there are radio buttons for 'Daily' (selected), 'Weekly', and 'Monthly', along with a 'Disable' checkbox. Below the 'Daily' tab, there is a table of days of the week with checkboxes and time selectors. Monday and Friday are checked, and both are set to run at 22:00. The 'Weekly' tab shows a single day selector set to 'Monday' at 00:00. The 'Monthly' tab shows options for 'On day' (selected), 'first', or 'last', with a day selector set to 'Monday' at 00:00, and an option for 'On date' (1 of month) at 00:00.

| Day | at (hour : min) |
|--|-----------------|
| <input checked="" type="checkbox"/> Monday | 22 : 0 |
| <input type="checkbox"/> Tuesday | 0 : 0 |
| <input type="checkbox"/> Wednesday | 0 : 0 |
| <input type="checkbox"/> Thursday | 0 : 0 |
| <input checked="" type="checkbox"/> Friday | 22 : 0 |
| <input type="checkbox"/> Saturday | 0 : 0 |
| <input type="checkbox"/> Sunday | 0 : 0 |

Weekly

On day: Monday at (hour : min) 0 : 0

Monthly

☒ On day ☐ first ☐ last Monday at (hour : min)

☐ On date 1 of month 0 : 0

Please note that this will make the Service execute a new Report every Monday and Friday each on 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 second Report shall 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:

The screenshot shows a software window titled "Create Delta Report Definition". Inside, there's a section titled "New Delta Report Definition" with a sidebar on the left containing four items: "Delta Report Definition" (selected), "Report Comparing", "Notification Settings", and "Schedule Settings". The main area is titled "Send Email Summary" and contains the following fields:

- Port: 25
- ☐ External SMTP
- User Name: pghys
- Password: (empty)
- ☒ Send Summary
- Send Summary to: pghys@netsec.de
- Subject: Summary for Weekly Delta (Development)
- ☒ Send Report
- Send Report to: hwkremer@netsec.de
- Subject: Weekly Permission Changes (Development)
- Maximum Size: 20

At the bottom right of the main area is a "Test" button with a green checkmark icon. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

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

The screenshot shows a software window titled "Create Delta Report Definition". On the left is a sidebar with four items: "Delta Report Definition", "Report Comparing", "Notification Settings", and "ScheduleSettings". The main area is titled "Scheduler Service" and contains a "Scheduling" tab. Under this tab, there are three radio buttons: "Daily", "Weekly" (which is selected), and "Monthly", along with a "Disable" checkbox. Below the "Daily" section, there is a table for scheduling on specific days of the week. Below the "Weekly" section, there is a field for "On day" set to "Friday" and a time field set to "23 : 59". At the bottom right are three buttons: "< Back", "Finish", and "Cancel".

| Day | at (hour : min) |
|------------------------------------|-----------------|
| <input type="checkbox"/> Monday | 0 : 0 |
| <input type="checkbox"/> Tuesday | 0 : 0 |
| <input type="checkbox"/> Wednesday | 0 : 0 |
| <input type="checkbox"/> Thursday | 0 : 0 |
| <input type="checkbox"/> Friday | 0 : 0 |
| <input type="checkbox"/> Saturday | 0 : 0 |
| <input type="checkbox"/> Sunday | 0 : 0 |

Weekly Scheduling:
 On day: Friday at (hour : min) 23 : 59

That's it. We do now report permission changes on a weekly basis fully automatically.

Licensing

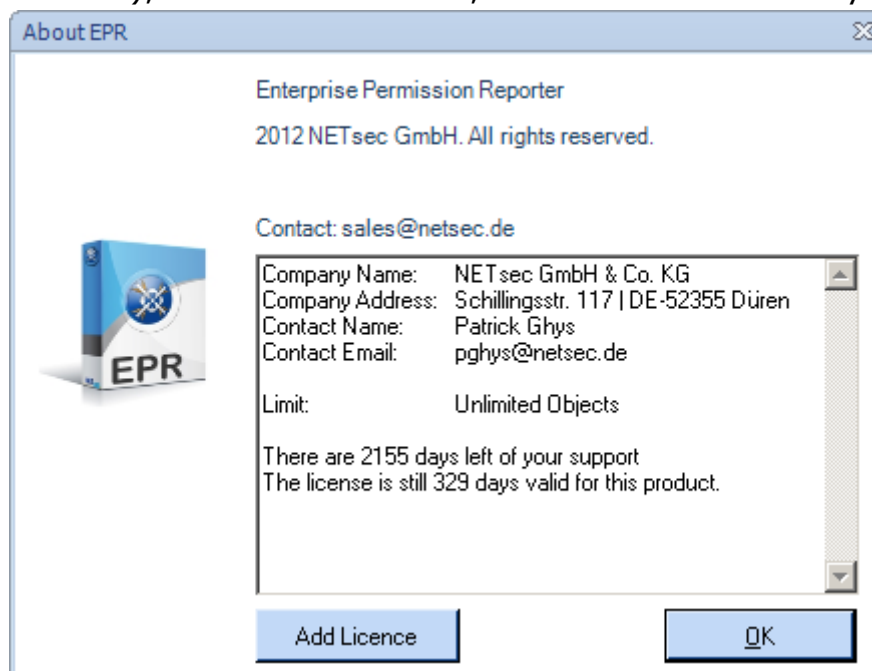
Trial License

To use EPR in Trial

A trial license will allow you to analyze up to 100 folders. 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