PERMISSION REPORTER® V4.0

Quickstart Guide

NETsec

September 2015

1 Einleitung

Mit NETsec Permission Reporter haben Sie die Möglichkeit, die NTFS- und Freigabeberechtigungen Ihrer Windows File Ressourcen zu erfassen und in einer SQL Datenbank zu speichern. Die so ermittelten Daten können als Dokumentation der vergebenen Berechtigungen genutzt werden oder, falls die Daten zu verschiedenen Zeitpunkten erfasst wurden, auch zum Erkennen/Dokumentieren der erfolgten Änderungen.

Mit den folgenden Seiten möchten wir den Einstieg in den NETsec Permission Reporter erleichtern.

Sollten Sie während der Testphase auf Probleme stoßen steht Ihnen unser Support Team gerne per Mail unter support@netsec.de zur Verfügung.

2 Anforderungen

2.1 Empfehlung

Wir empfehlen, NETsec Permission Reporter auf einer separaten (virtuellen) Maschine zu verwenden.

Des Weiteren ist eine Auflösung von 1920 x 1080p empfehlenswert, um ein vernünftiges Arbeiten mit der Benutzeroberfläche zu gewährleisten.

2.2 Mindestanforderungen an das System

Betriebssystem:	Windows Server 2008 64bit / Windows Vista 64bit
Arbeitsspeicher:	4 GB
Freier Speicherplatz:	500 MB
.NET Framework:	4.5
CPU:	x64

2.3 Anforderungen an die Datenbank

Microsoft SQL:

- Server 2005 oder neuer
- LocalDB 2012 mit verfügbarer Standard-Instanz (v11.0)

Die LocalDB sollte nur für Testszenarien verwendet werden, da diverse Limitierungen bestehen und benutzerkontextfreie Nutzung nicht möglich ist.

2.4 Anforderungen an das Service Konto

Auf der Maschine auf der der Service läuft:

- Mitglied der lokalen Administratorgruppe (kein vordefiniertes Konto)
- Recht: Anmelden als Dienst (engl. Logon as a Service-Privileg)

Auf der zu analysierenden Maschine (Fileserver):

- Mitglied der lokalen Administratorgruppe

Datenbankrechte:

- Schreibberechtigung
- Leseberechtigung
- Änderungsberechtigung

2.5 Anforderung an das GUI Konto

Als GUI-Konto ist das Konto zu verstehen, welches die Anwendung ausführt.

Auf der lokalen Maschine:

- Mitglied der lokalen Administratorgruppe
  (Nicht zwingend die zu analysierende Maschine)

Zum Zeitpunkt des Anlegens einer Zieldatenbank:

- Berechtigung, auf der Serverinstanz Datenbanken anzulegen

Nach dem Anlegen einer Zieldatenbank:

- Allgemeine Leseberechtigung in den Zieldatenbanken der Analysen

Besonderheit bei einer LocalDB:

- GUI-Benutzer muss dem Service-Konto entsprechen. Grund hierfür ist die benutzerkontextabhängige Datenbanknutzung

3 Installation & Upgrade

1. Anmeldung mit dem GUI-Konto
2. Starten der MSI-Datei (PermissionReporterSetup.4.*.msi)

Sofern bereits eine Installation von Permission Reporter vorliegt, sollte der Service (Permission Reporter Service) für den Zeitraum des Upgrades beendet werden.

Achtung: Dieser Vorgang unterbricht auch laufende/geplante Analysen von Permission Reporter! Stellen Sie sicher, dass keine Analysen laufen.

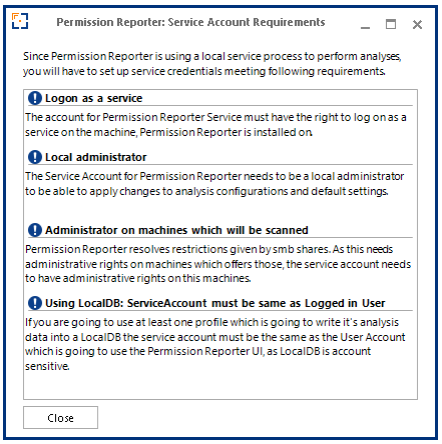
4 Erster Start

Beim ersten Start von Permission Reporter werden einmalige Überprüfungen durchgeführt und Empfehlungen ausgesprochen.

Darüber hinaus können dem Programm Standardeinstellungen übergeben und bei Bedarf eine lokale Datenbank installiert werden.

4.1 Service Account

Permission Reporter wird im Falle des ersten Starts darauf hinweisen, dass der Service im Maschinen-Kontext ausgeführt wird (.\LocalSystem).



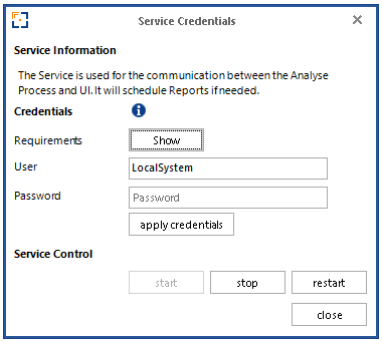
Wie unter 2.4 (Anforderungen an das Service Konto) beschrieben empfiehlt sich die Verwendung eines Service-Kontos für Permission Reporter. Daher wird im Rahmen des ersten Starts ein Wechsel der Credentials notwendig.

Dieser sollte den angezeigten Anforderungen an einen Service Account für Permission Reporter entsprechen.

Nachdem Sie von den Anforderungen Kenntnis genommen haben, gelangen Sie in einen Dialog, welcher die Eingabe gültiger Credentials erwartet.

Bitte geben Sie den Benutzernamen im Format *Domäne\Benutzer* oder *Benutzer@Domäne* an.

Nach einem Klick auf „*apply credentials*“ folgt eine Erfolgsmeldung welche Sie danach schließen können. Der Service wird nach Übernahme der Credentials neugestartet um im übergebenen Kontext arbeiten zu können.



4.2 LocalDB 2012

Beim ersten Start von Permission Reporter wird das laufende System auf eine installierte Version von Microsoft SQL-Express 2012 LocalDB überprüft.

Sofern auf dem System keine installierte Version festgestellt werden kann, wird im Rahmen des ersten Starts eine Installation dieser Software angeboten.

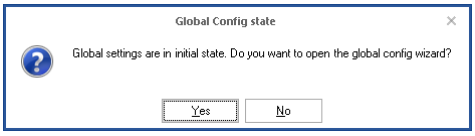
Diese Installation ist für Testszenarien empfohlen in denen kein SQL-Server für Analysedaten zur Verfügung steht.

Falls die Installation von LocalDB 2012 durchgeführt wollen soll, startet ein entsprechender Installationsdialog.

4.3 Globale Einstellungen

Permission Reporter verfügt über globale Einstellungen, welche programmweit gültige Einstellungen wie die Dauer des Beibehaltens von Logfiles, aber auch Firmendaten beinhalten. Weiterhin werden im Rahmen der globalen Einstellungen Standardauswahlen für später zu erzeugende Analyse-Vorlagen (Profile) vorgenommen.

Da es sich um den ersten Start handelt, wird das Festlegen von globalen Einstellungen durch Permission Reporter empfohlen.

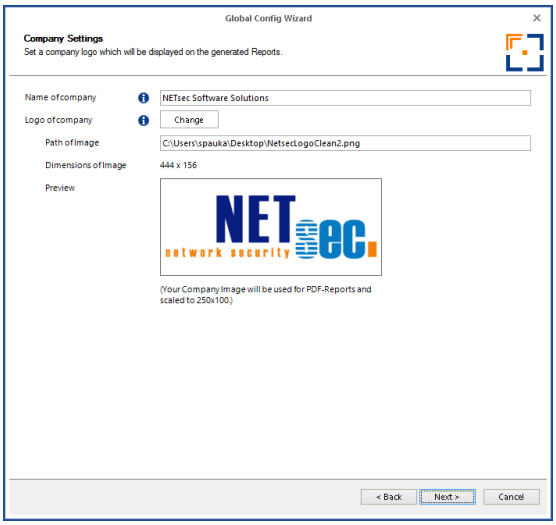


Der „*Global Config Wizard*" (dt. Assistent) hilft Ihnen bei der Konfiguration der Standardeinstellungen. Die einzelnen Einstellungen werden im Folgenden näher erläutert.

4.3.1 Firmeneinstellungen

Auf der ersten Seite des Assistenten können Sie den Namen Ihrer Firma sowie ein Bild mit Ihrem Firmenlogo angeben, welche später in den generierten Reports erscheinen.

Diese Angaben sind optional und nicht zwingend erforderlich.

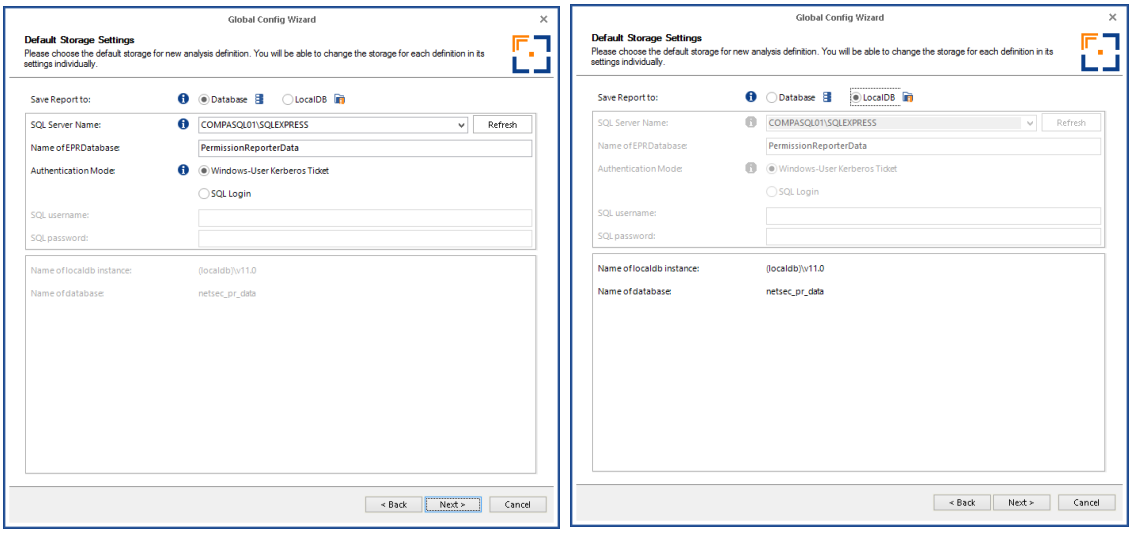


4.3.2 Datenbankeinstellungen

Auf der Seite zu den „*Default Storage Settings*“ können Sie Standardeinstellungen für anzulegende Profile vornehmen. Hierbei können Sie einen SQL-Server sowie eine Datenbank auswählen.

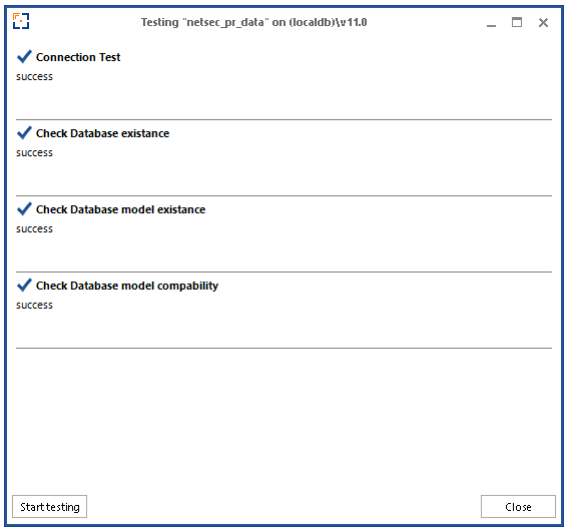
Eine ausgewählte Datenbank ist nur dann für Permission Reporter nutzbar, wenn sie

- Von Permission Reporter in einer vergangenen Sitzung erstellt wurde.
- Nicht existiert und von Permission Reporter angelegt werden kann.

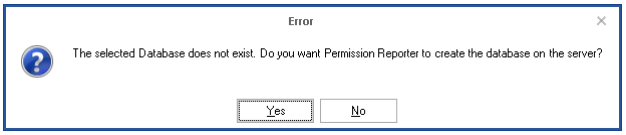


Sollten Sie sich dagegen für die Nutzung der LocalDB entscheiden, beachten Sie bitte, dass dies nur möglich ist, sofern der Benutzer der UI dem Service Account entspricht (2.5 Anforderung an das GUI Konto).

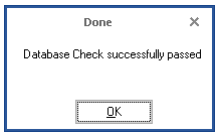
Nach der Auswahl des Servers und der Datenbank wird eine Datenbankvalidierung vorgenommen.



Sollte noch keine Datenbank existieren, wird Permission Reporter anbieten, diese zu erstellen.

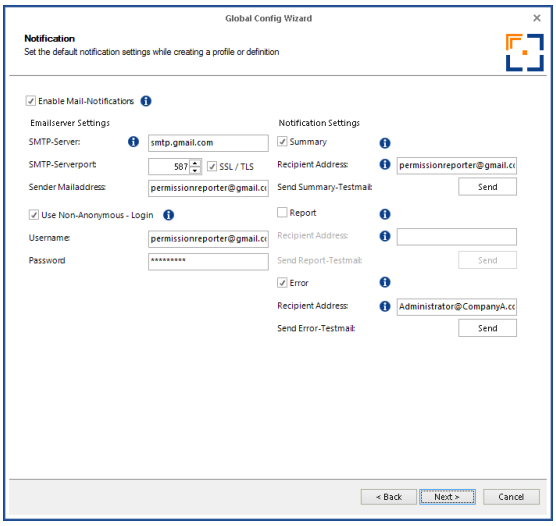


Nach der Erstellung, wird ein weiteres Mal eine Validierung der Datenbank vorgenommen.



4.3.3 Benachrichtigungseinstellungen

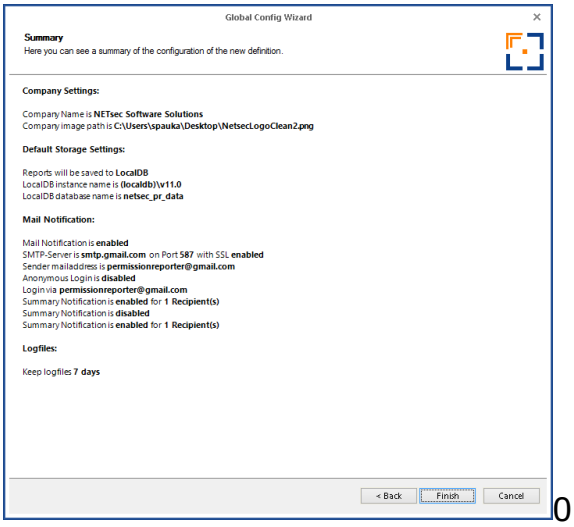
Permission Reporter kann nach durchgeführten Analysen per E-Mail Benachrichtigungen über dessen Verlauf versenden. Hierzu benötigt Permission Reporter Daten über den zu verwendenden SMTP Server und die hierfür eventuell erforderlichen Anmeldedaten.



Sie können die Funktionalität des E-Mail-Versands mittels der angebotenen Testmail Buttons überprüfen.

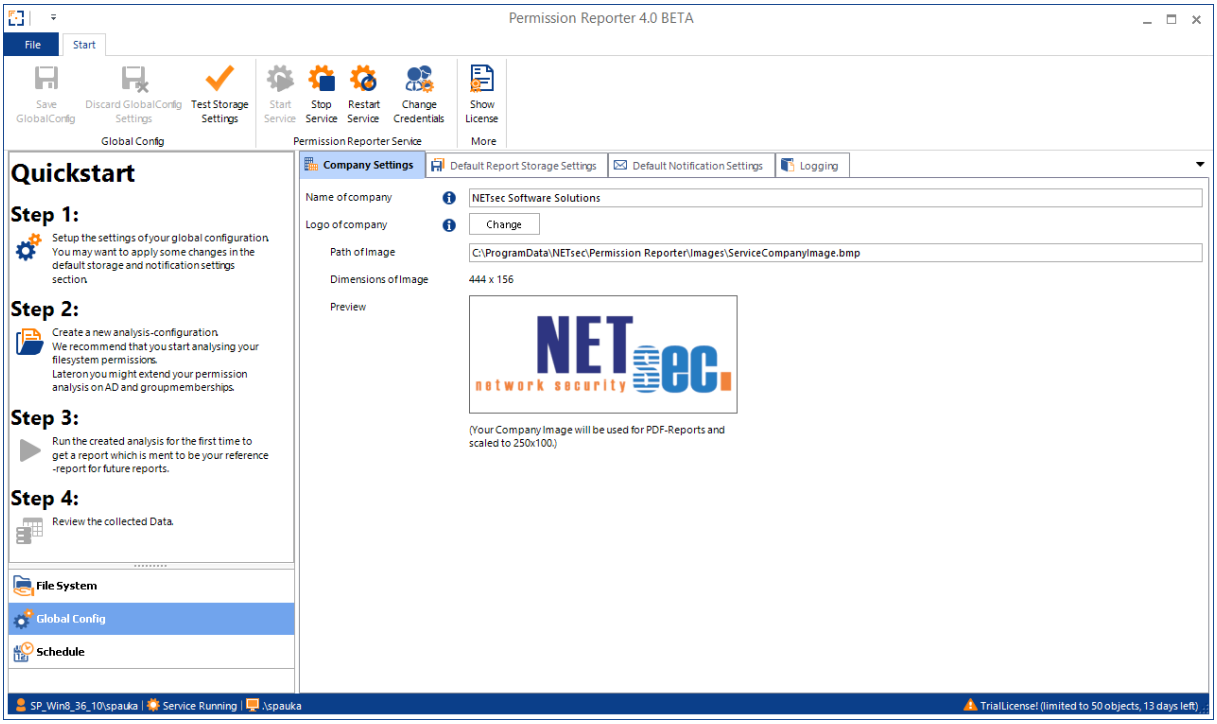
4.3.4 Zusammenfassung

Abschließend wird eine Übersicht über die von Ihnen gewählten Einstellungen gezeigt.



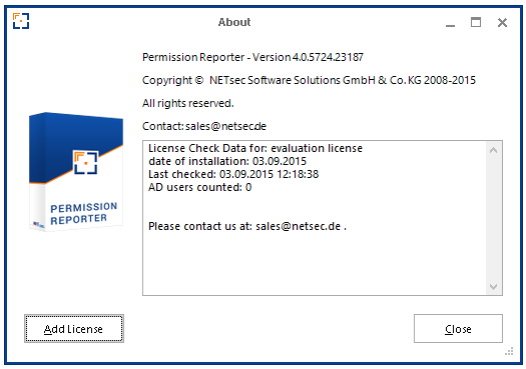
Nach dem Beenden des Assistenten gelangen Sie in die grafische Oberfläche der Software.

Zu diesem Zeitpunkt befinden Sie sich in den Globalen Einstellungen, in denen ein Quickstart Menü bereitgestellt wird um die ersten Schritte in Permission Reporter zu erleichtern.



5 Lizenz

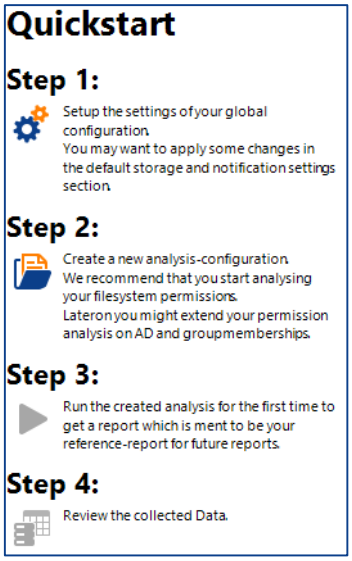
Sofern Sie eine Lizenz für Permission Reporter besitzen, können Sie diese mit einem Klick auf „*Show License*“ und „*Add License*“ in folgendem Dialog einspielen.



Sollten Sie Permission Reporter zu Testzwecken ohne Lizenz nutzen, ist der Umfang einer Analyse auf 50 Objekte des Dateisystems beschränkt.

6 Erstellen eines Profils

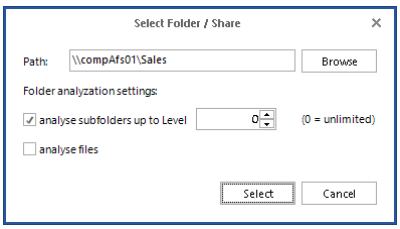
In sogenannten Profilen wird gespeichert, welcher Pfad zu untersuchen ist und auf welche Dateisystemobjekte sich die Analyse beziehen soll.



Durch einen Klick auf das Symbol im „*Step 2*“ des angebotenen Quickstart-Elements, gelangen Sie zu einem Erstellungs-Assistenten für ein solches Profil.

Auf der ersten Seite können Sie einen Namen und eine Beschreibung für das Profil eingeben.

Auf der folgenden Seite wählen Sie einen Ordner oder eine Freigabe als Einstiegspunkt für die Analyse.

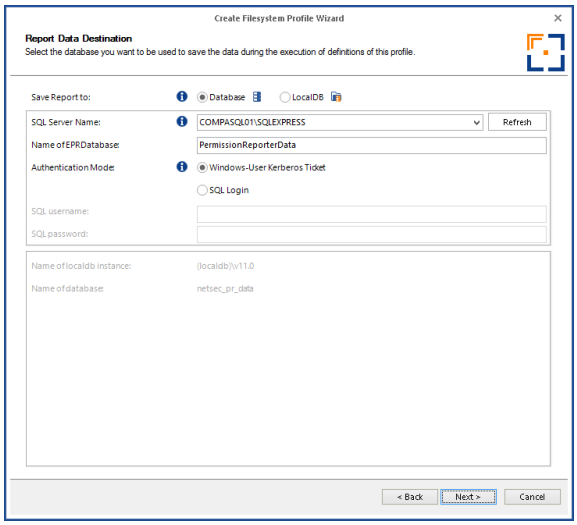


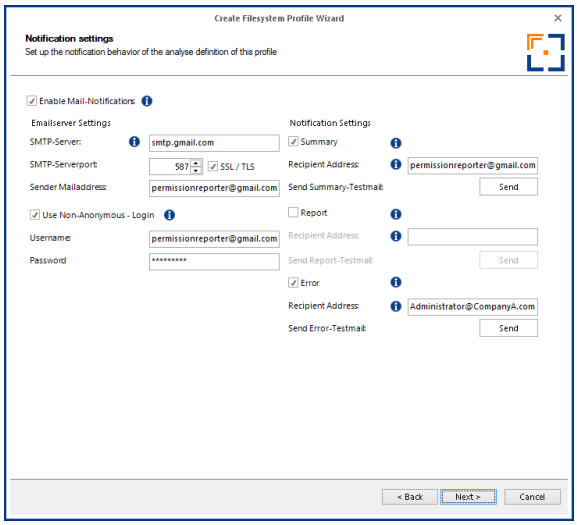
Neben der reinen Auswahl eines Pfades entscheiden Sie hier, ob und bis zu welchem Verzweigungsgrad Unterordner und Dateien analysiert werden sollen.

Beachten Sie hierbei, dass die getroffene Auswahl für dieses Profil nicht mehr veränderbar ist.

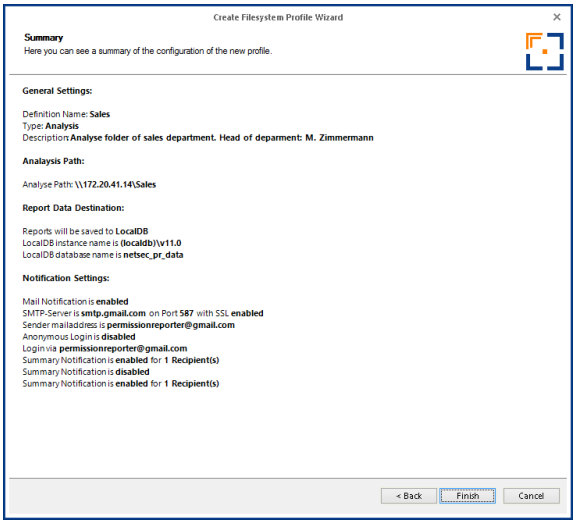
Sollten Sie sich für die Analyse von Dateien entscheiden, bedenken Sie, dass hierdurch in der Regel weitaus mehr Objekte des Dateisystems analysiert werden müssen und somit die Ausführungszeit für eine Analyse deutlich steigen wird.

Anschließend können Anpassungen im Hinblick auf Datenbank und Benachrichtigungen vorgenommen werden.

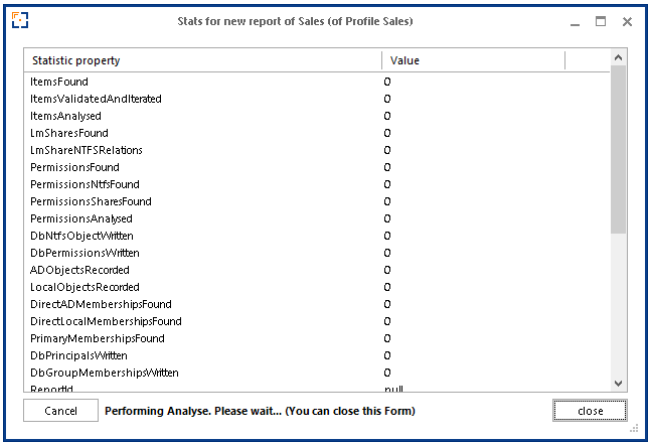




Abschließend wird ein Übersichtsbildschirm mit den vorgenommenen Einstellungen präsentiert.

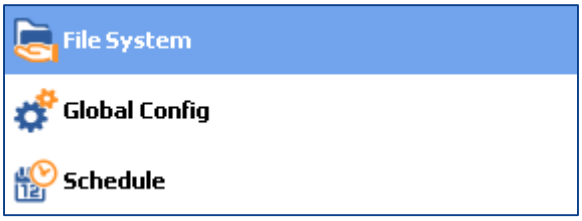


Durch einen Klick auf das Bild im Quickstart „*Step 3*“ wird eine Analyse für das von Ihnen soeben angelegte Profil gestartet und Sie haben die Möglichkeit, den Status der laufenden Analyse im entsprechenden Dialog mit zu verfolgen oder aber sich weiter mit der Oberfläche von Permission Reporter vertraut zu machen.



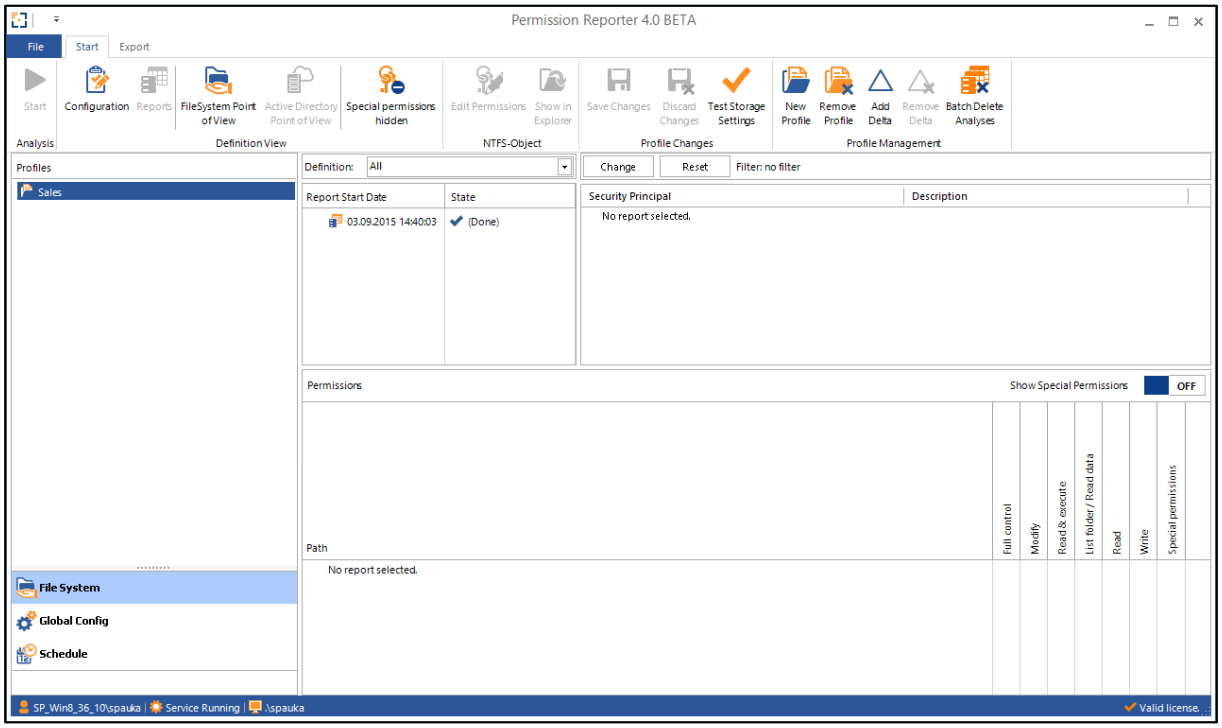
7 Durchgeführte Analysen betrachten

Um das Ergebnis einer Analyse (sogenannte Reports) betrachten zu können, wählen Sie im Navigationsbereich (unten links) den Menüpunkt „*File System*“. Es folgt eine Auflistung alle verfügbaren Profile oberhalb des Navigationsbereiches.

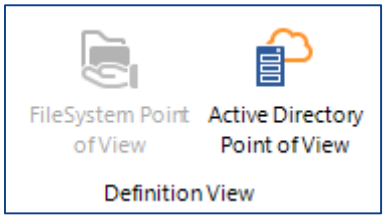


Im oberen Abschnitt unter „*Start*“ besteht nun die Möglichkeit von „*Configuration*“ auf „*Reports*“ zu wechseln. Ist der Wechsel vollzogen, so wird die aktive Auswahl ausgegraut.

Neben der Liste alle Profile erscheint eine Auflistung von bereits durchgeführten Analysen.



Sie können bei der Betrachtung der Analyse zwischen folgenden Perspektiven wählen.

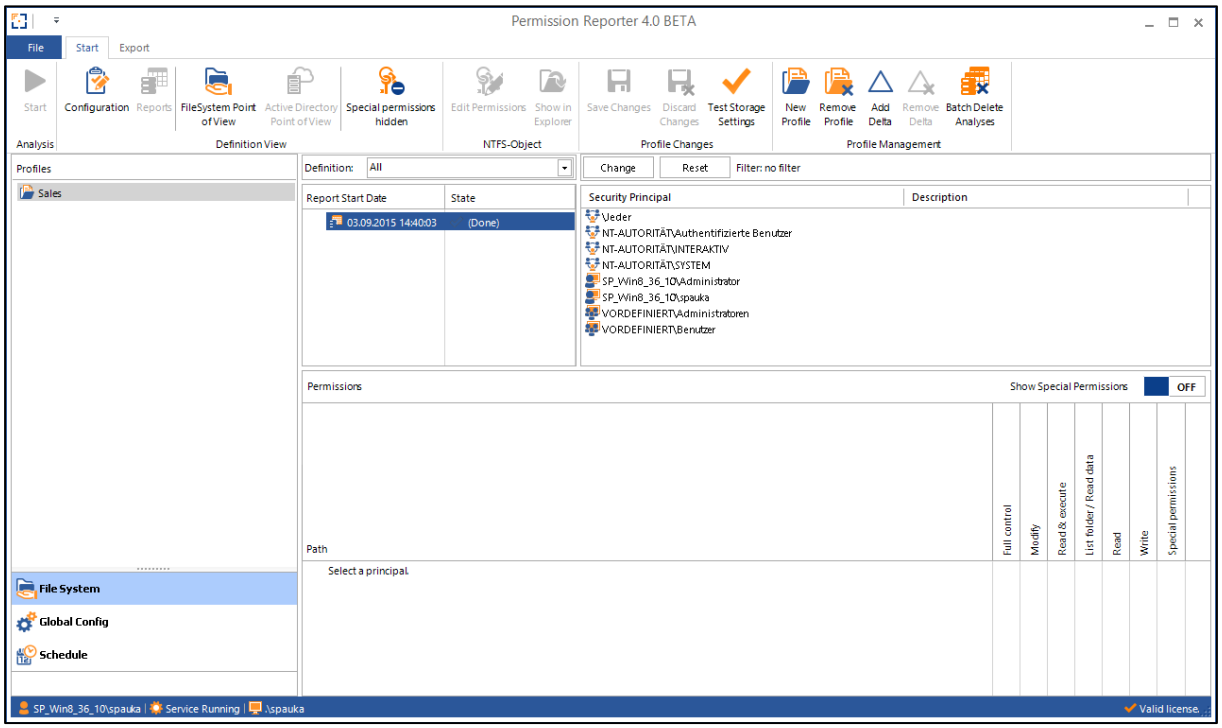


7.1 File System Point of View

Stellt die in der Analyse gefundenen Objekte des Dateisystems bereit und zeigt Ihnen nach Auswahl, die - *für das ausgewählte Objekt* - gültigen Berechtigungen in Form der DACL (Discretionary Access Control List).

7.2 Active Directory Point of View

Stellt Ihnen zuerst die in der Analyse gefundenen Sicherheitsprinzipale zur Auswahl und daraufhin die analysierten Dateisystemobjekte mit den jeweiligen Berechtigungen.



7.3 PDF Reports

Entsprechend der Auswahl von Objekten des Dateisystems und/oder Sicherheitsprinzipalen wird die Generierung von verschiedenen Reports im PDF Format angeboten.