IT-Security

Permission analysis in Docusnap

TITLE	IT-Security
AUTHOR	Docusnap Consulting
DATE	8/29/2019
VERSION	1.0 | valid from 8/22/2019

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of itelio GmbH. All rights reserved.

CONTENTS

1. INTRODUCTION 4
1.1 GENERAL REQUIREMENTS 5
2. FILE SYSTEM (CIFS/DFS/WINDOWS) 6
2.1 REQUIREMENT 6
2.2 NTFS ANALYSIS 7
2.3 ANALYSIS - FILE SYSTEM 9
2.3.1 SURFACE AREA 9
2.3.2 REPORTS 13
2.3.3 ORIGIN OF ENTITLEMENT 22
2.3.4 FURTHER TOPICS 24
3. SHAREPOINT 28
3.1 REQUIREMENTS 28
3.2 ANALYSIS 28
4. EXCHANGE 29
4.1 REQUIREMENT 29
4.2 ANALYSIS 30

1. INTRODUCTION

The issue of permissions is essential for companies. Often it is difficult to get a structured and clean overview of which shares and directories have which permissions, or which shares and directories a certain user or group of people may access.

With the help of IT security in Docusnap, these questions can be answered in the areas of file system, Exchange and SharePoint.

In the file system area, share and NTFS permissions are used so that you can also determine the effective permissions of a user here. In addition, permissions for SharePoint servers, Exchange mailboxes, mailbox folders and public folders can be inventoried and analyzed.

This HowTo describes the implementation of the authorization analysis in Docusnap with all its functions and possibilities as well as application examples.

- Chapter 2 describes the authorization analysis for file systems in full - this includes, among others
  - Conditions for implementation
  - Directory reports, which output the permissions on shares / folders
  - User reports that output permissions for selected users / groups
  - Time-controlled execution of these reports
- Chapter 3 describes the authorization analysis of your SharePoint environment.
- Chapter 4 Authorization Analysis of the Exchange Infrastructure

1.1 GENERAL REQUIREMENTS

IT security can be analyzed in the areas of file system, Exchange and SharePoint. All of these areas require a full Active Directory inventory. The further necessary inventories can be found in the following table.

File system (Windows, CIFS, DFS)	exchange	SharePoint
Active Directory Inventory (resolving SIDs and group affiliations)	Active Directory Inventory (resolving SIDs and group affiliations)	Active Directory Inventory (resolving SIDs and group affiliations)
Windows, CIFS, DFS (releases and their release permissions)	Exchange inventory (mailboxes, public folders etc.)	SharePoint inventory (websites, document libraries etc.)
NTFS analysis		

Table 1 - IT Security Requirements

An overview of the required ports and permissions can be found in the How-To Whitepaper Docusnap Inventory in the Docusnap Knowledge Base.

2. FILE SYSTEM (CIFS/DFS/WINDOWS)

2.1 REQUIREMENT

The successful permission analysis for file systems (NTFS, ReFS) requires the following inventories:

- Active Directory
- Windows, CIFS, DFS

Active Directory

An up-to-date Active Directory inventory is essential for authorization analysis. In the course of the NTFS analysis SIDs are determined. These SIDs can be resolved to users and groups through the Active Directory inventory. The user and group structures are also known (group memberships).

In step 3 - Active Directory - of the Active Directory inventory, you can define an OU filter. Afterwards, only the selected OUs and the user and groups located there are inventoried. Please note that this setting may result in some SIDs not being resolved. Check the Advanced option - Inventory all users and groups.

Be sure to take a complete inventory of trusted domains as well. This is the only way to ensure that all SIDs can be resolved in the event that authorizations have been assigned here.

Windows - CIFS - DFS

The later NTFS analysis aims at drives or shares. In order for these to be available for selection, the systems and services above them must also be inventoried: Windows, CIFS and DFS. In the course of these inventories, the release authorizations are inventoried. These form the first part of the authorizations.

The following chapter describes the NTFS analysis, which inventories the second part of the permissions - the NTFS permissions.

2.2 NTFS ANALYSIS

NTFS analysis is used to read the NTFS authorizations and store them in the database. The NTFS analysis does not have archive data, which means that you can always only analyze the current status.

The wizard for performing the NTFS analysis is located in the IT Security section, which can be accessed via the main navigation bar.

In **step 1 - Company selection** - select the corresponding company

Step 2 - Authentication - requires a domain user with sufficient permissions to connect the shares and read the permissions.

In **step 3 - Systems** - you can now select the systems to be analyzed using their drives. If you activate the option **Use shares for Windows systems**, all shares of the Windows systems are listed in addition to the CIFS and DFS, which you can analyze afterwards.

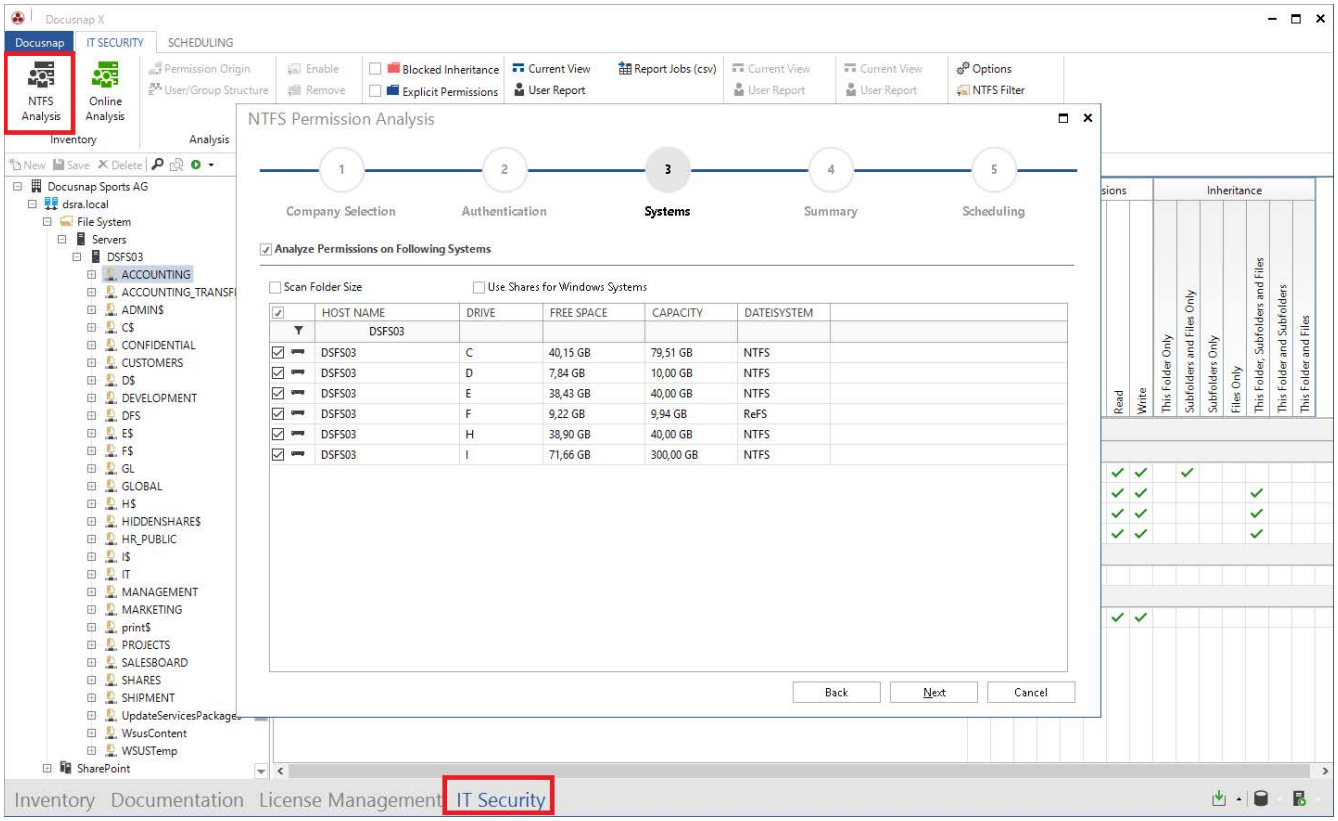

Figure 1 - Starting NTFS analysis

Below you will find a list describing the advantages and disadvantages of the NTFS permission inventory variants - drives and shares.

	disk drives	**releases**
advantages	The complete drive is analyzed. If new releases are detected, e.g. by the Windows Inventory, they are automatically evaluated in the IT security.	Explicit selection of the required releases. Thus, a reduction of the required database memory as well as a reduction of the runtime is realized.
drawbacks	The amount of data is increased by the complete analysis of the drive. Unused releases such as C$, ADMIN$ can be evaluated.	The selection of releases is not dynamic. New releases must be explicitly selected.

Table 1 - Drives vs. shares

2.3 ANALYSIS - FILE SYSTEM

After the data has been collected, it can be analyzed in the next step. Both the Docusnap interface and reports are available for analysis.

2.3.1 SURFACE AREA

The Docusnap interface offers you the first possibility to analyze the authorization assignment on the file system. You start the analysis of authorizations using the tree structure in the IT security area. Navigate through **your company - your domain - file system to the** corresponding system. Below you will now find the shares and folders that have been inventoried.

In the main area, the NTFS permissions (directly set and inherited) and the release permissions are displayed. You can also use the user group search to display effective permissions.

If blocked inheritances or **directly set permissions are** to be visible in the hierarchical structure, this can be activated in the ribbon in the **Display** area.

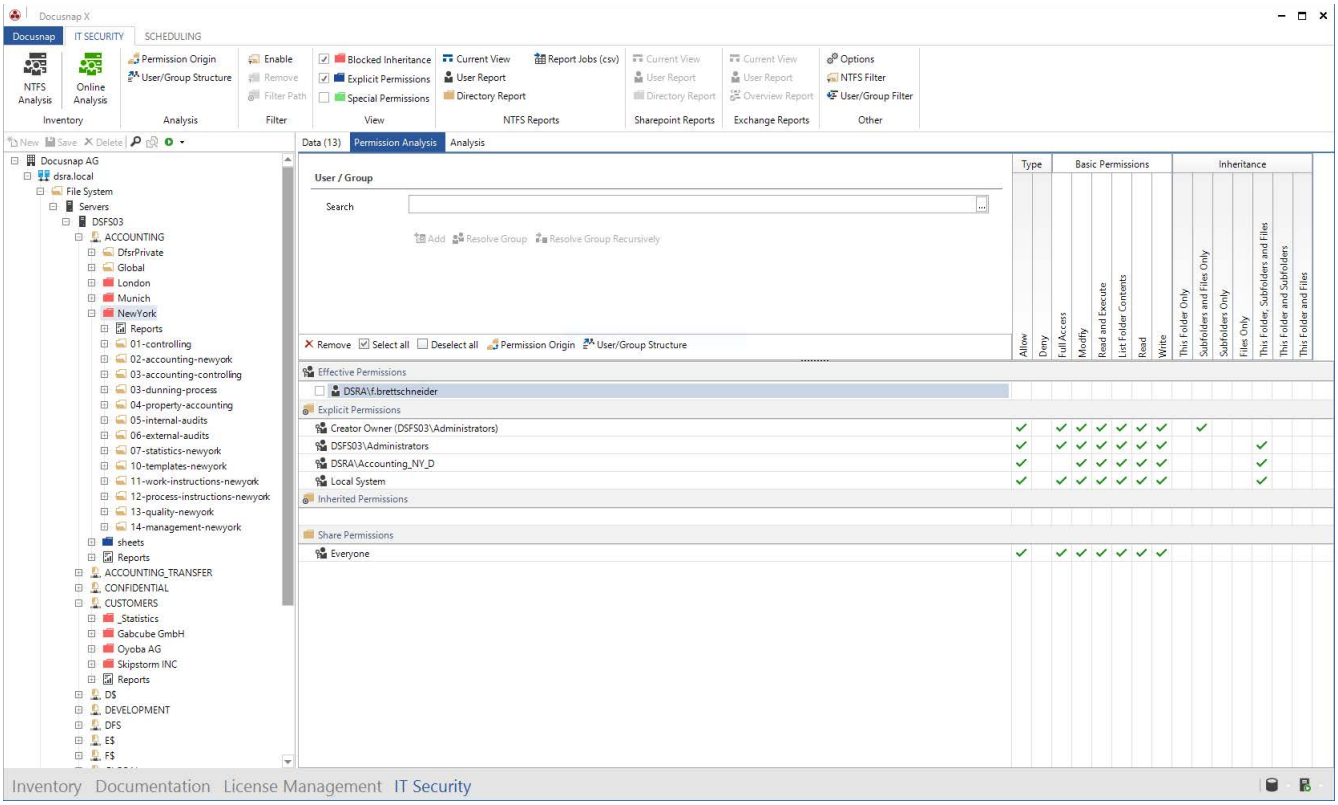

Figure 2 - NTFS analysis hierarchical structure

2.3.1.1 USER-GROUP SEARCH

In the main area, the NTFS permissions (directly set and inherited) and the release permissions are displayed. To evaluate the effective permissions of selected users and/or groups, you can add them using the search area.

Type the name of the user or group in the **search box**. You are then offered the appropriate users and groups from the Active Directory and the local systems for selection. Groups can be dissolved (recursively).

Later, you can also generate a user/group report for the selected users or groups.

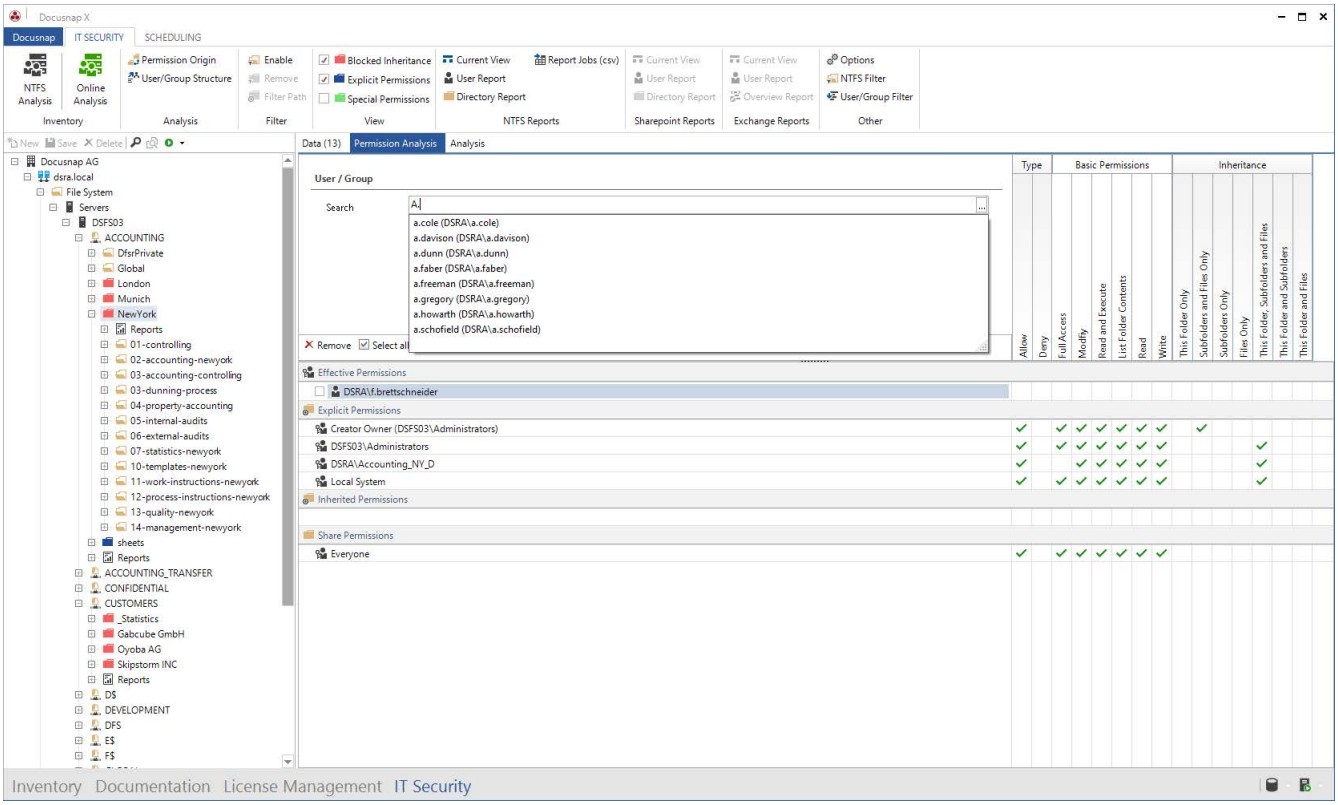

Figure 3 - User - Group Selection

You can perform an **advanced search for** users and groups using the button at the end of the search field. The inventoried ADS properties of the users and groups are now available for selection here. Logical AND and OR operations can be performed.

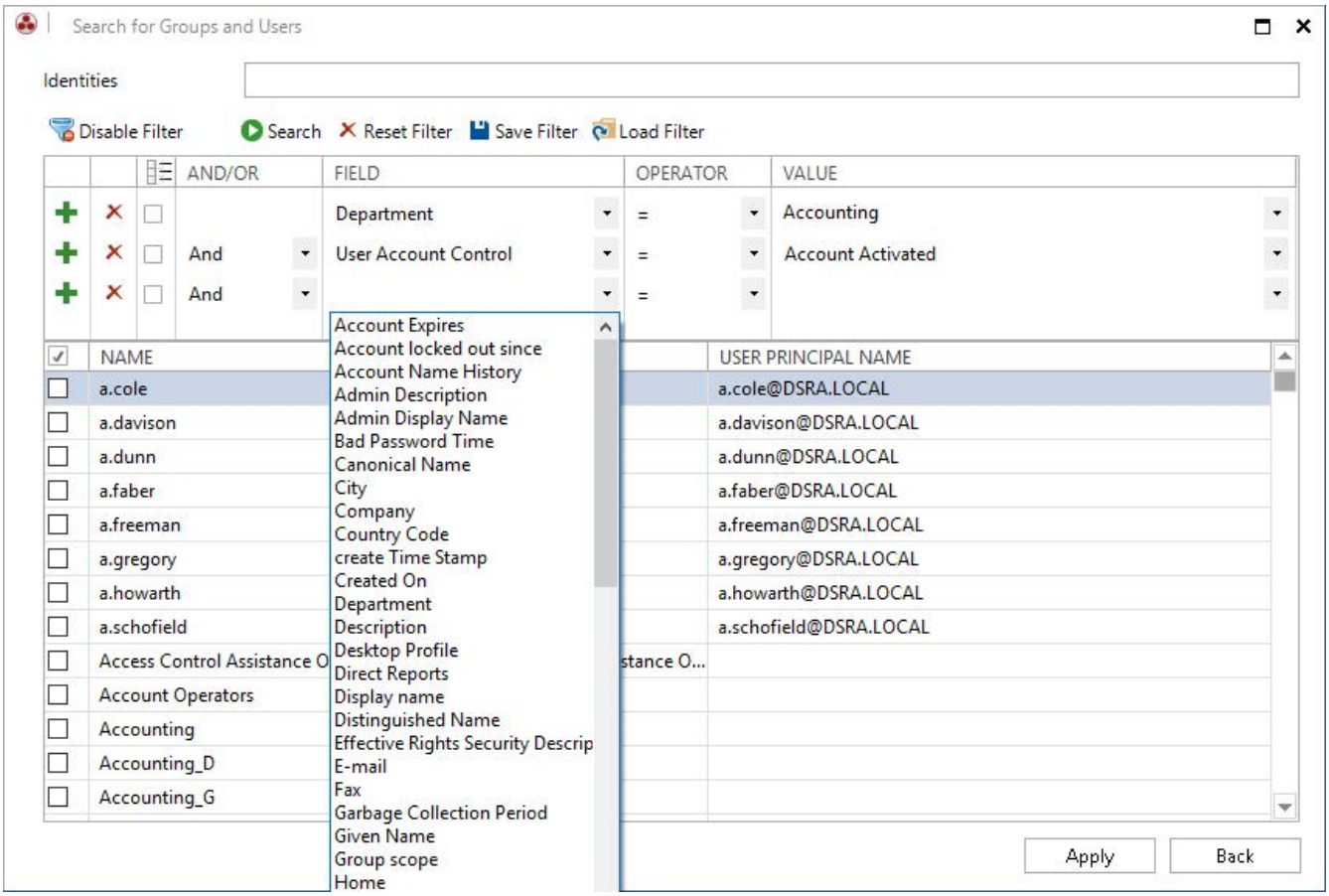

Figure 4 - Advanced Users - Group Search

2.3.1.2 AUTHORIZATION FILTER

You can use the permission filter to define a minimum permission that a user or group must have on a share that is displayed within the tree structure. In this way, you can determine all folders to which a selected user or group has corresponding permissions.

To do this, activate the filter within the ribbon. Then select the appropriate permission that the user or group must have in order for the folders to be displayed in the tree structure.

The activated filter also affects the user report. Within the user report, only those folders are displayed that are now also listed in the tree structure.

Hint:

A user has read permissions on the share. The user receives change authorizations for the subfolder.

Activate the filter and choose Change - the previously mentioned subfolder will not be listed! The user needs change authorizations or more on the complete path.

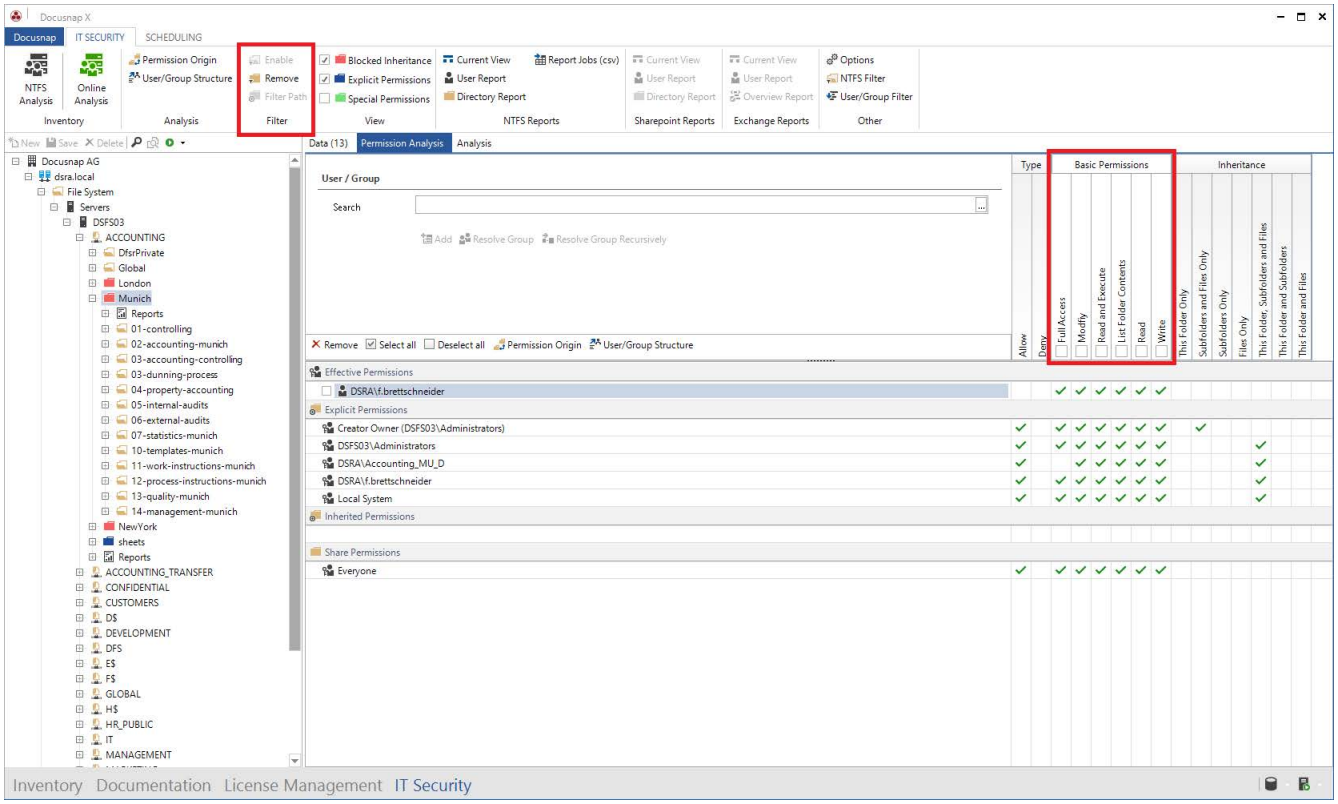

Figure 5 - Permission filter

2.3.2 REPORTS

The following reports are available for analyzing the file system.

- directory report
- user report
- directories
- releases

A distinction is made between complex evaluations (directory and user reports) and simple representations of ACLs (directories and releases). For complex evaluations, e.g. effective authorizations are calculated and group memberships are dissolved.

directory report	**user report**	**directories**	**releases**
Evaluation of effective and NTFS permissions from the point of view of the share / directory	Evaluation of effective and NTFS permissions from the point of view of the user / group	Display of NTFS permissions	Display of share and subdirectories
Execution of complex evaluations - dissolving group memberships (optional)	Execution of complex evaluations - dissolving group memberships (optional)	Representation of the ACLs of the directories	Representation of the ACLS of the shares and directories

2.3.2.1 DIRECTORY REPORT

The directory report shows the current permissions (share, NTFS, effective) from a share / folder. Within the wizard, you also have the choice of how many directory levels are to be taken into account during creation.

You determine the starting point of the directory report by selecting the appropriate share / folder within the tree structure. After you have made your selection, call the wizard for creating the **directory report in the** ribbon.

The following selection of options is available. All options are described again in the user manual - which can be accessed via the F1 key.

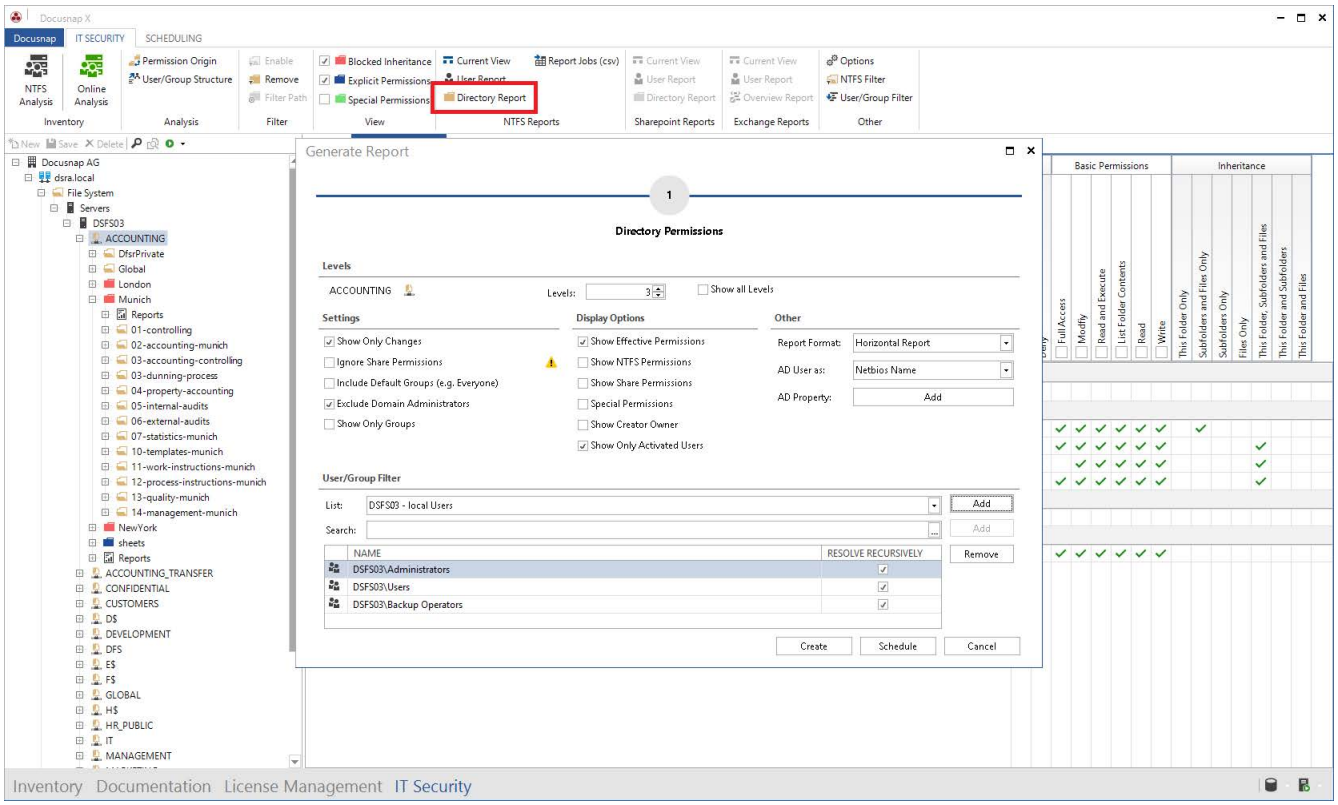

Figure 6 - Create directory report

- plains
  - Number of levels analyzed within the report
- Display changes only
  - Folders with inherited permissions only are **not** displayed in the report.
  - Only if the effective permissions have been changed (inheritance blocked, permissions set directly), these folders are listed in the report.
- Show groups only
  - The report does not break down the authorized groups recursively.
  - Only the authorized groups and directly authorized users are listed.

- view options
  - Select the appropriate permissions to list in the report.
  - Best practice:
    - For non-IT-savvy persons, list only the effective authorizations.

- Other
  - Choose between the available report formats
    - Horizontal
    - Vertical
    - Excel
  - Representation of the respective users
  - Selection of additional ADS properties - e.g. department
- User/Group Filter
  - Exclude specific users and groups from the display in the directory report
  - See the User/Group Filters chapter for information on how to perform pre-built exclusions.

The following figure shows the horizontal directory report.

Legend						
Effective Permissions						
Full Access (F)	Modify (M)	Read and Execute (RX)	List FolderContent (L)	Read (R)	Write (W)	

Account: Docusnap AG

Domain	dsra.local

Servers

Host	\\DSFS03						
Share	ACCOUNTING	08.01.2019 09:24:09	Effective Permissions				
			F	M	RX	L	R	W
a.faber				x	x	x	x	x
a.schofield				x	x	x	x	x
DSFS03\Administrator			x	x	x	x	x	x
f.brettschneider				x	x	x	x	x
h.lawrence				x	x	x	x	x
h.stephenson				x	x	x	x	x
s.friedmann				x	x	x	x	x
Directory	ACCOUNTING\London	DSFS03\Administrators	Effective Permissions					
			F	M	RX	L	R	W
a.schofield				x	x	x	x	x
DSFS03\Administrator			x	x	x	x	x	x
h.lawrence				x	x	x	x	x
Directory	ACCOUNTING\Munich	DSFS03\Administrators	Effective Permissions					
			F	M	RX	L	R	W
a.faber				x	x	x	x	x
DSFS03\Administrator			x	x	x	x	x	x
f.brettschneider			x	x	x	x	x	x
s.friedmann				x	x	x	x	x

Figure 7 - Directory (Resource) report

2.3.2.2 USER REPORT

The User Report displays the corresponding permissions for the selected resources and folder levels for selected users or groups.

Before a user report can be created, you must add a selected user or group using the search box. You can then open the Create User Report Wizard.

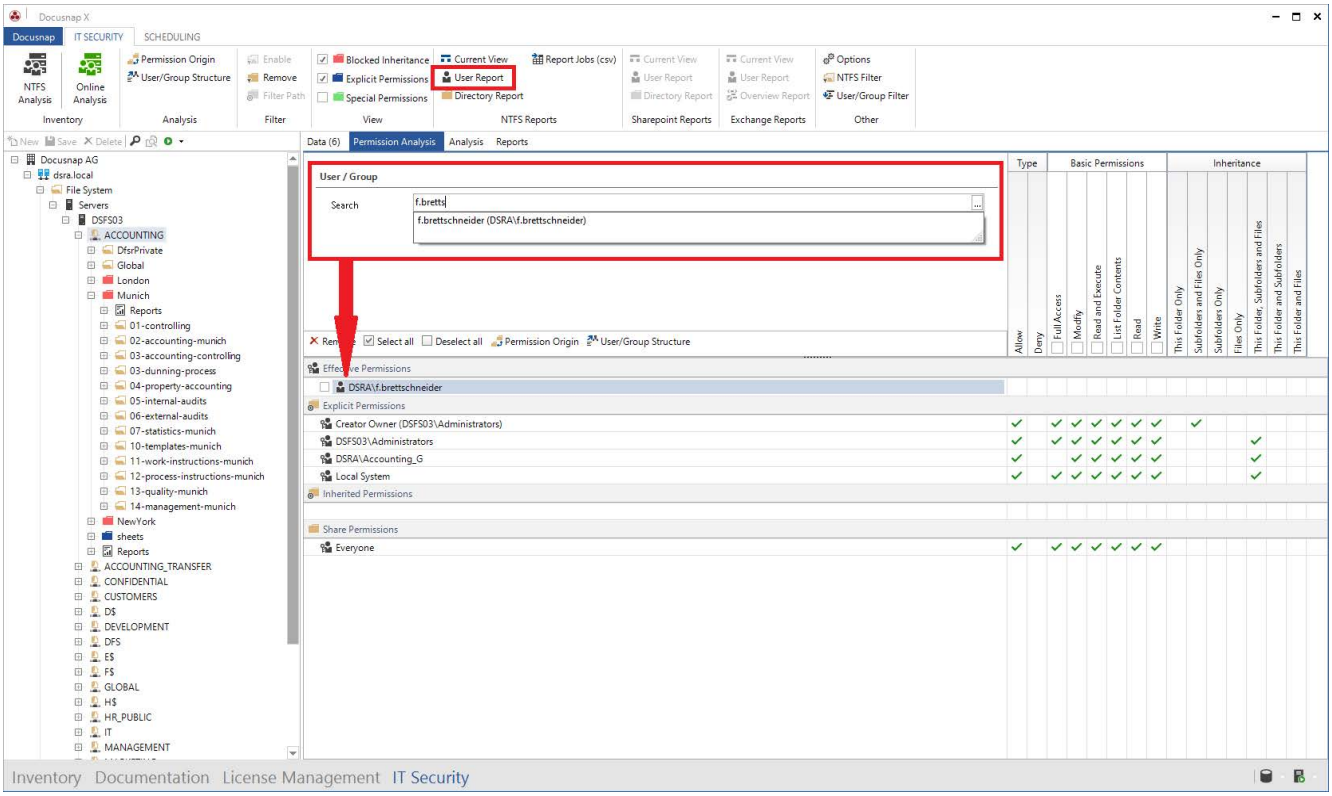

Figure 8 - Add user

The following options are available in the wizard:

- plains
  - Number of levels analyzed within the report
- Display changes only
  - Folders with inherited permissions only are **not** displayed in the report.
  - Only if the effective permissions of the selected user have been changed (inheritance blocked, permissions set directly), these folders are listed in the report.
- Display subfolders without permissions
  - Should folders to which the selected user / group has no permissions be listed in the report?

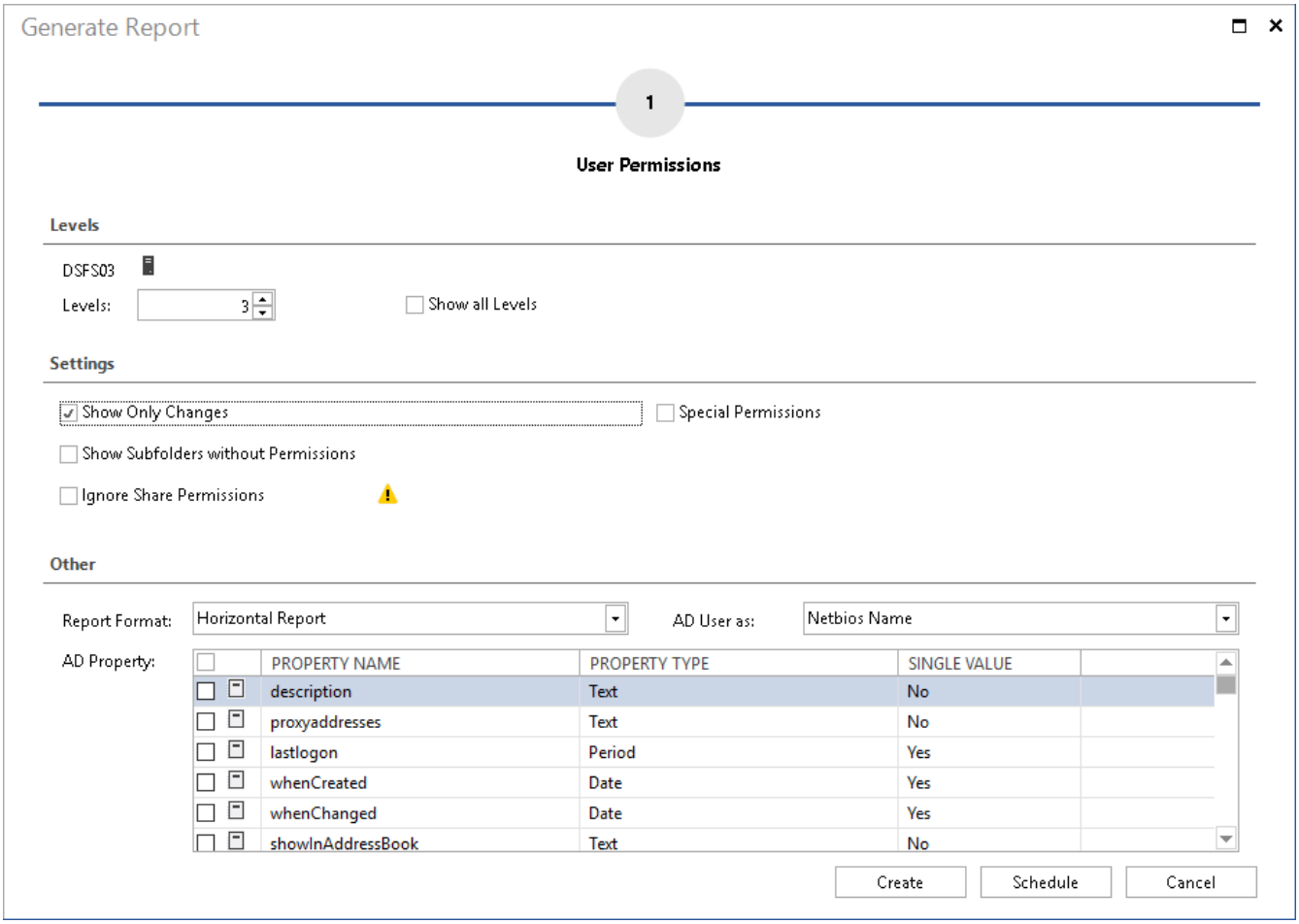

Figure 9 - User report options

								Effective Permissions				
								Full Access (F)	Modify (M)	Read and Execute (RX)	List Folder Content (L)	Read (R)	Write (W)
Account: Docusnap AG												
Domain	dsra.local											
Servers												
Host	DSFS03											
Share	ACCOUNTING			08.01.2019 09:24:09				Effective Permissions				
								F	M	RX	L	R	W
DSRA\f.brettschneider					User				x	x	x	x	x
Directory	ACCOUNTING\Munich			DSFS03\Administrators				Effective Permissions				
								F	M	RX	L	R	W
DSRA\f.brettschneider					User			x	x	x	x	x	x
Share	ACCOUNTING_TRANSFER			08.01.2019 09:24:09				Effective Permissions				
								F	M	RX	L	R	W
DSRA\f.brettschneider					User				x	x	x	x	x
Share	CONFIDENTIAL			08.01.2019 09:24:09				Effective Permissions				
								F	M	RX	L	R	W
DSRA\f.brettschneider					User					x	x	x	
Share	CUSTOMERS			08.01.2019 09:24:09				Effective Permissions				
								F	M	RX	L	R	W
DSRA\f.brettschneider					User								

Figure 10 - User report

Hint:

As you can see from the previous screenshot, the **Development** folder is listed, although it appears that the selected user has no permissions. However, the user has **special permissions** on the folder. You can enable the display of special permissions in the User Report Creation Wizard.

2.3.2.3 RELEASE/DIRECTORY REPORT

The tree structure contains additional reports for releases and directories. These reports do **not** reflect **effective permissions.** The reports give you release and NTFS permissions.

When you select Release as well as Report directories, the following setting options are available to you with regard to the scope of the reports:

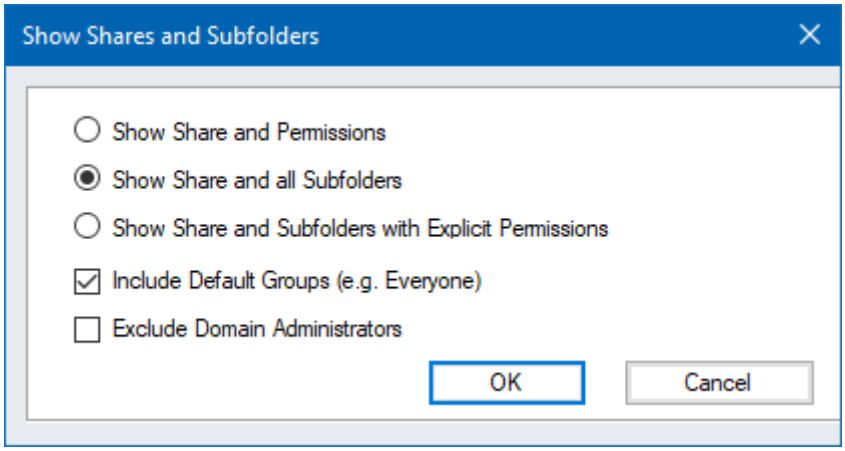

Figure 11 - Share report options

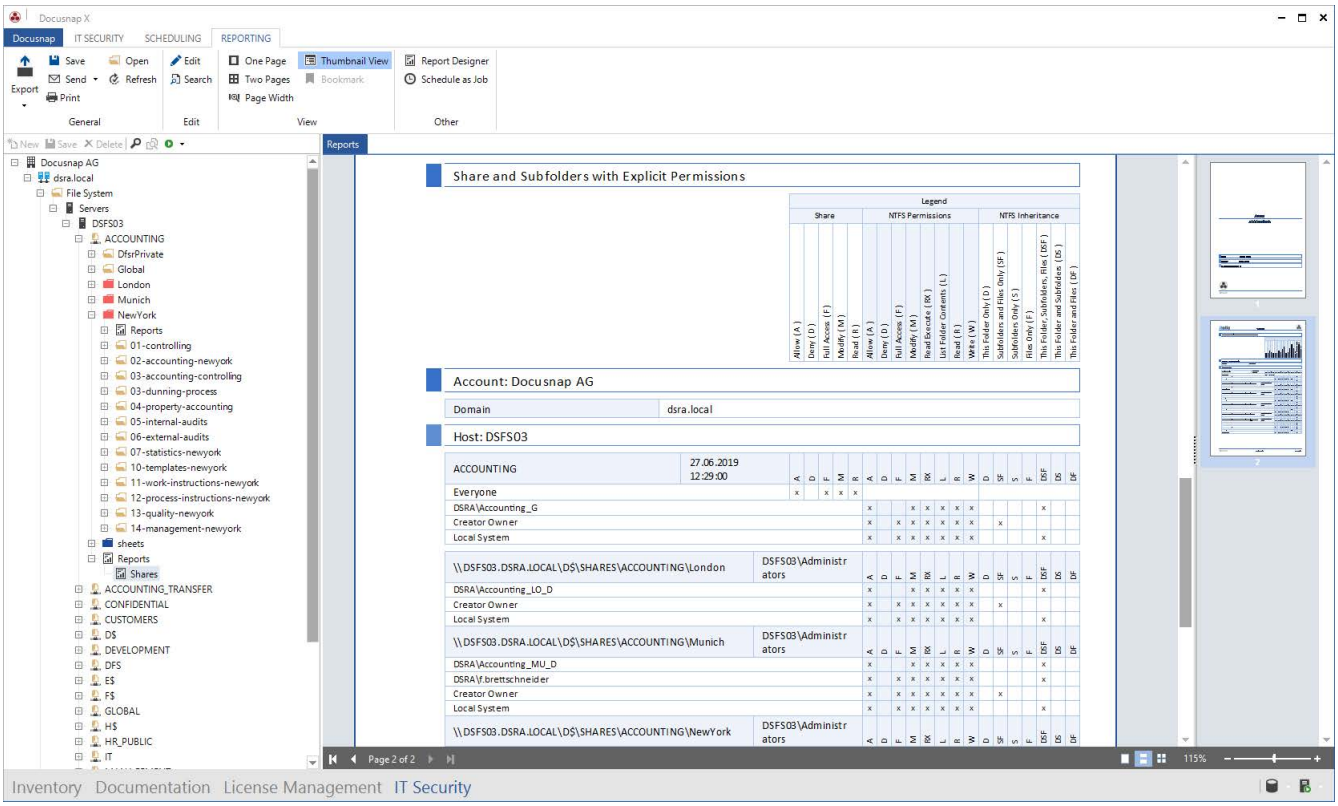

Figure 12 - Share report

2.3.2.4 CREATE AND SEND REPORTS ON A SCHEDULED BASIS

The reports described above can also be scheduled and sent by e-mail. In this way, you can send the responsible persons an overview of the assigned authorizations at regular intervals - fully automatically!

You will find the **Schedule** button within the wizard for both the user and directory reports. You can now specify where the report is to be stored in the file system (step 2) and to whom the report is to be sent by e-mail (step 3). Please also note the file formats, which you can adjust below the **advanced options.**

The report created on the file system can then be found in the following path:

- Your company\Your domain\Servername\Release name

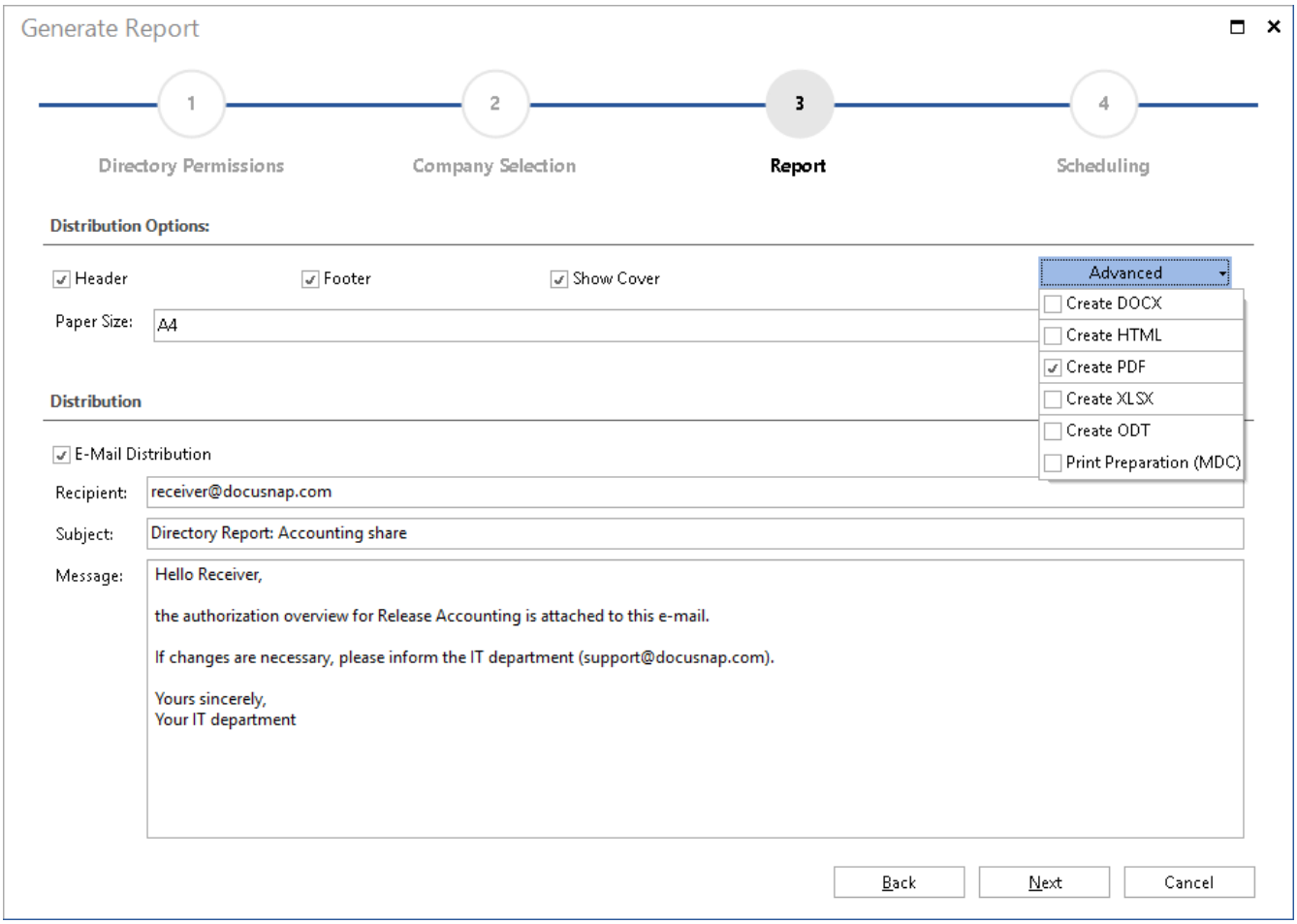

Figure 13 - Send permission reports by e-mail

You can also create and send the release and directory report time-controlled after creation via the **Plan as order** button:

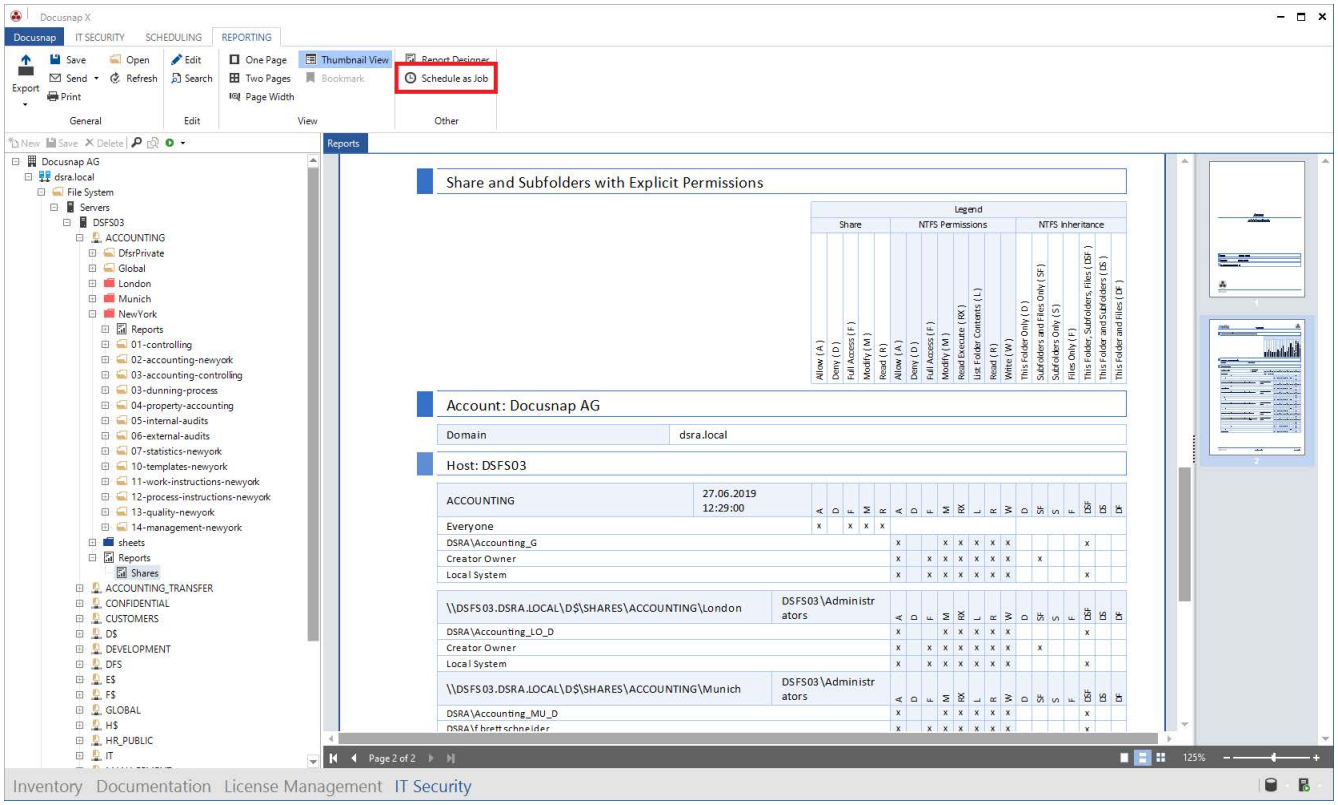

Figure 14 - Schedule Share and directory reports as job

2.3.3 ORIGIN OF ENTITLEMENT

If the analysis in the user interface or within a report reveals an authorization that you would not have expected, you can use Docusnap to check the origin of this authorization.

Why does the user have the appropriate permissions on this resource?

You can clarify this question using the authorization origin. First add the user using the search field and choose the authorization origin in the next step:

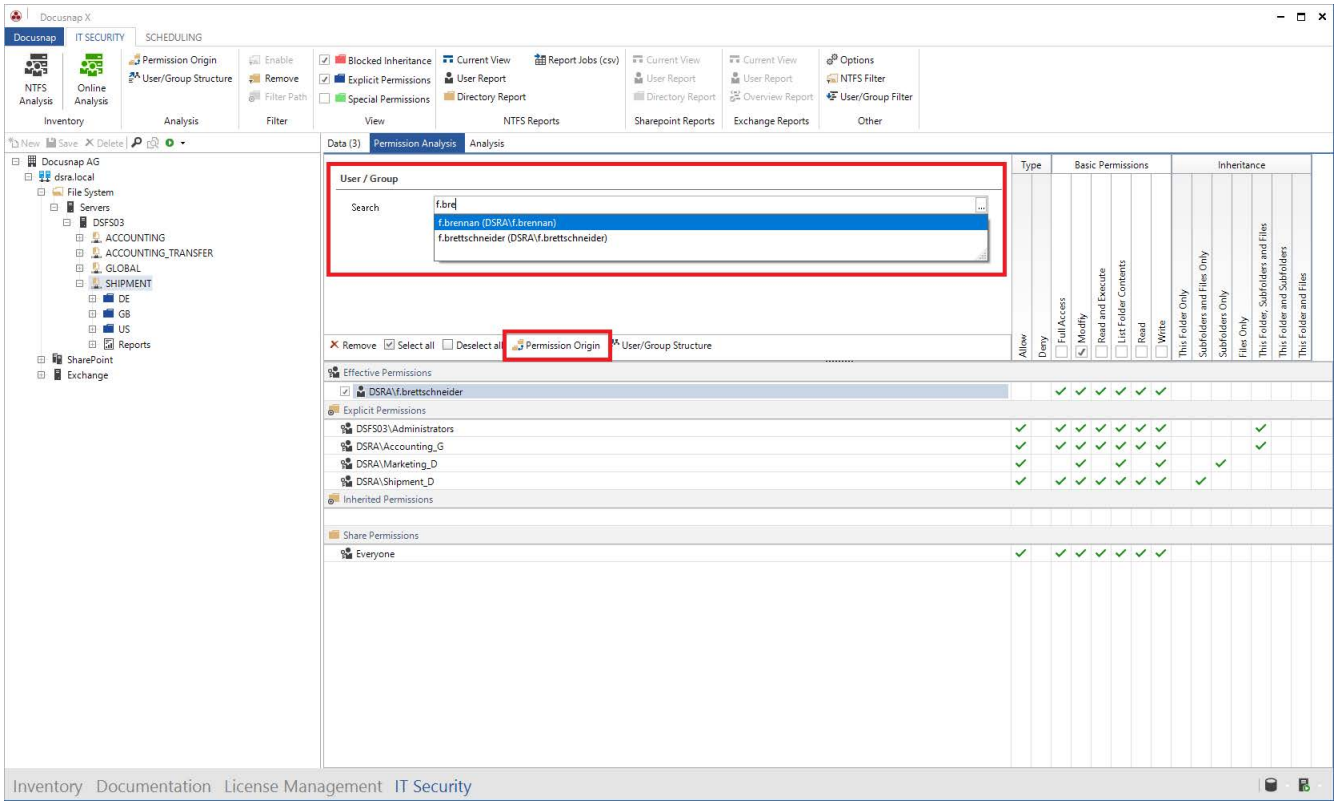

Figure 15 - Call permission origin

Now the origin of the NTFS as well as the release authorization and the resulting effective authorizations are derived.

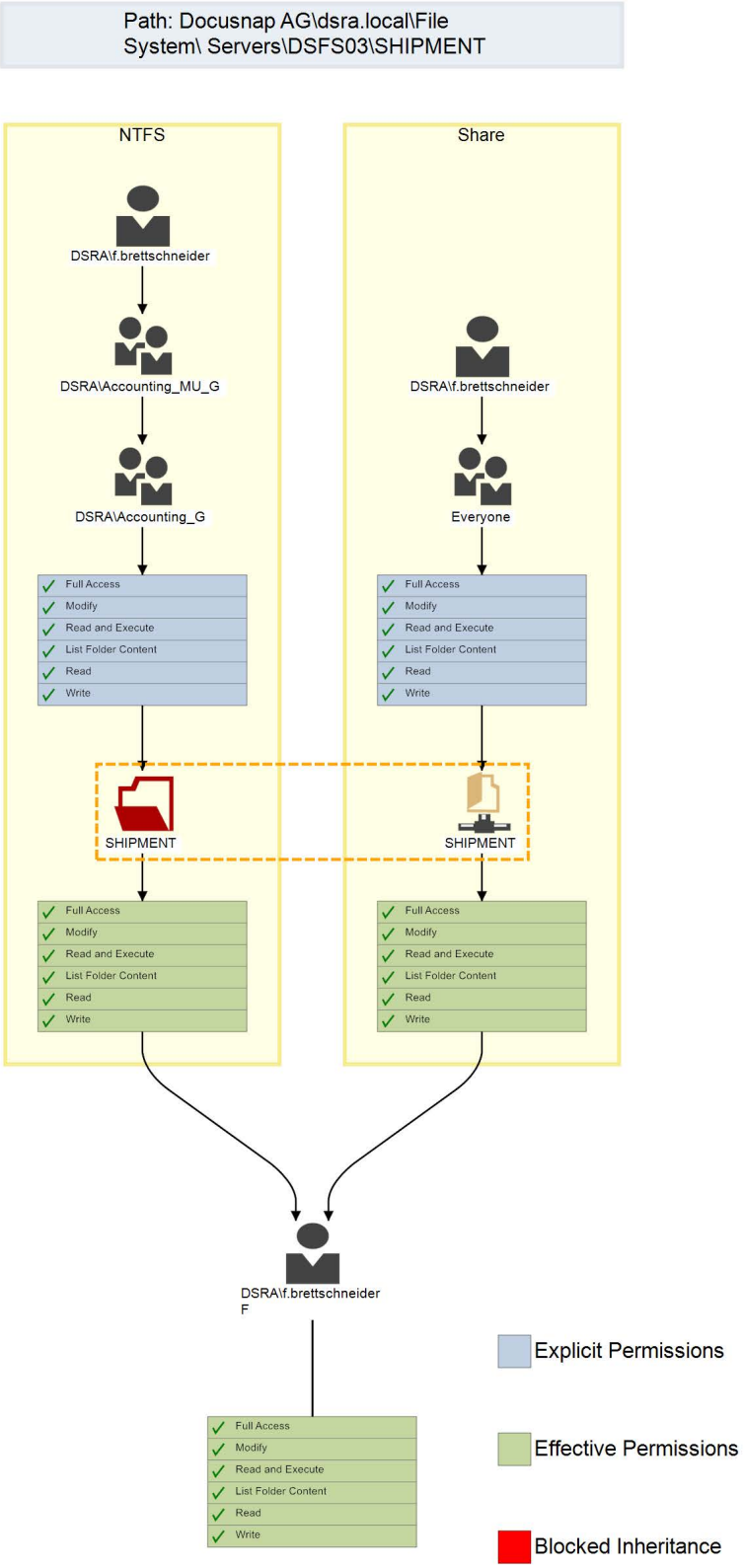

Figure 16 - Check permission origin

2.3.4 FURTHER TOPICS

The following section deals with further topics.

2.3.4.1 LIMIT FOLDER LEVELS

With the help of the option **Limit folder levels** you can define how deep the NTFS analysis should inventory permissions. The fewer levels are considered, the less time and storage space is required (keyword SQL Express - 10 GB database limitation). In return, you may miss out on changes to the authorization structure.

You can set a limit for the folder levels in the IT security **options**.

The first level are the releases. If you limit the inventory to three levels, the share, the first folder and its subfolders will be inventoried. Underlying structures are ignored.

- Enable (Level 1)
  - Folder (Level 2)
    - Subfolder (Level 3)

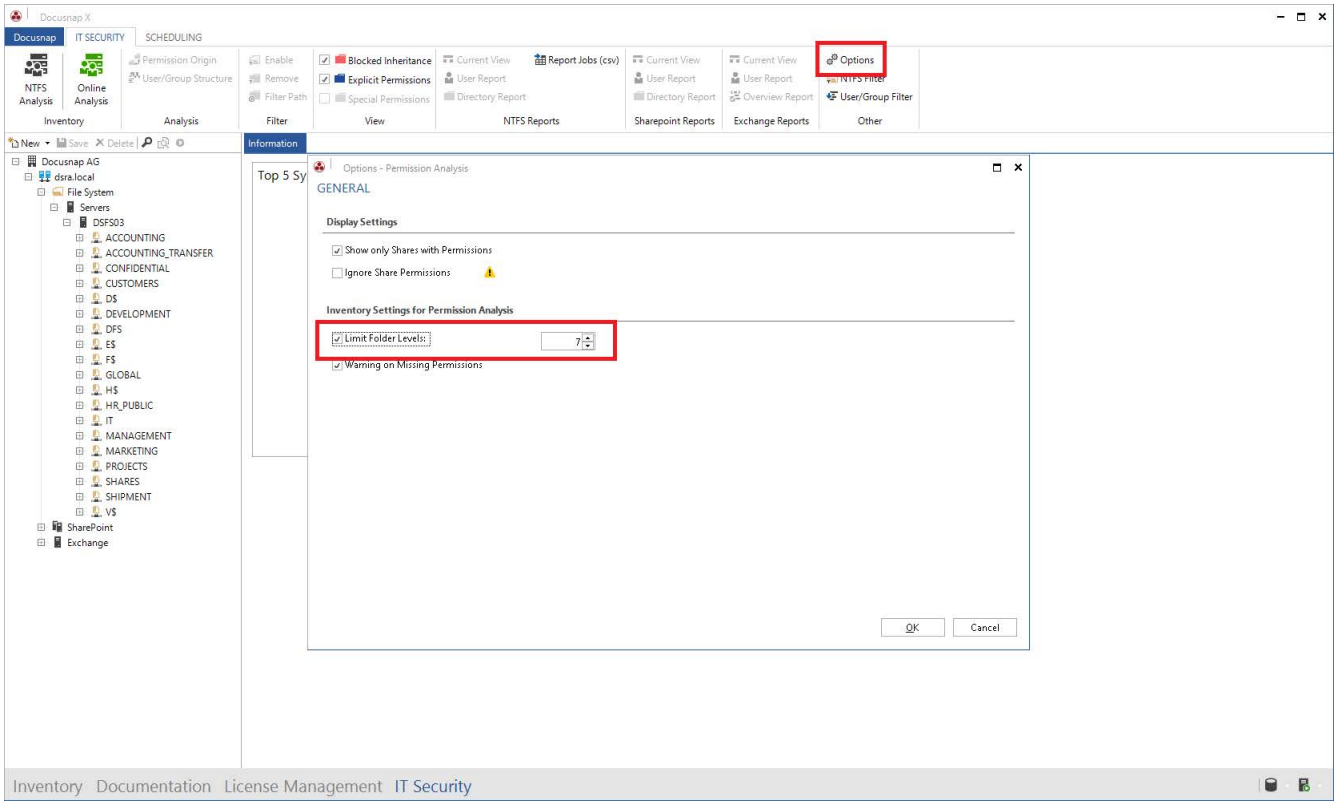

Figure 17 - Limit folder levels

2.3.4.2 NTFS FILTER

You can use the NTFS filter to restrict the directories to be read. It is possible to specify directories that are to be inventoried. You can also exclude directories that are not required in the authorization analysis. You can also define a combination of directories to include and directories to exclude.

You call the **NTFS filter** via the control of the same name in the **Miscellaneous** area.

The following operators are available:

- **Contains**: The specified condition must be contained in the directory - **the directory will then be inventoried.**
    - **If this operator is used, only the specified shares / directories are explicitly inventoried.**
- **Does not contain**: The specified condition must not be contained in the directory - **the directory will then not be inventoried.**

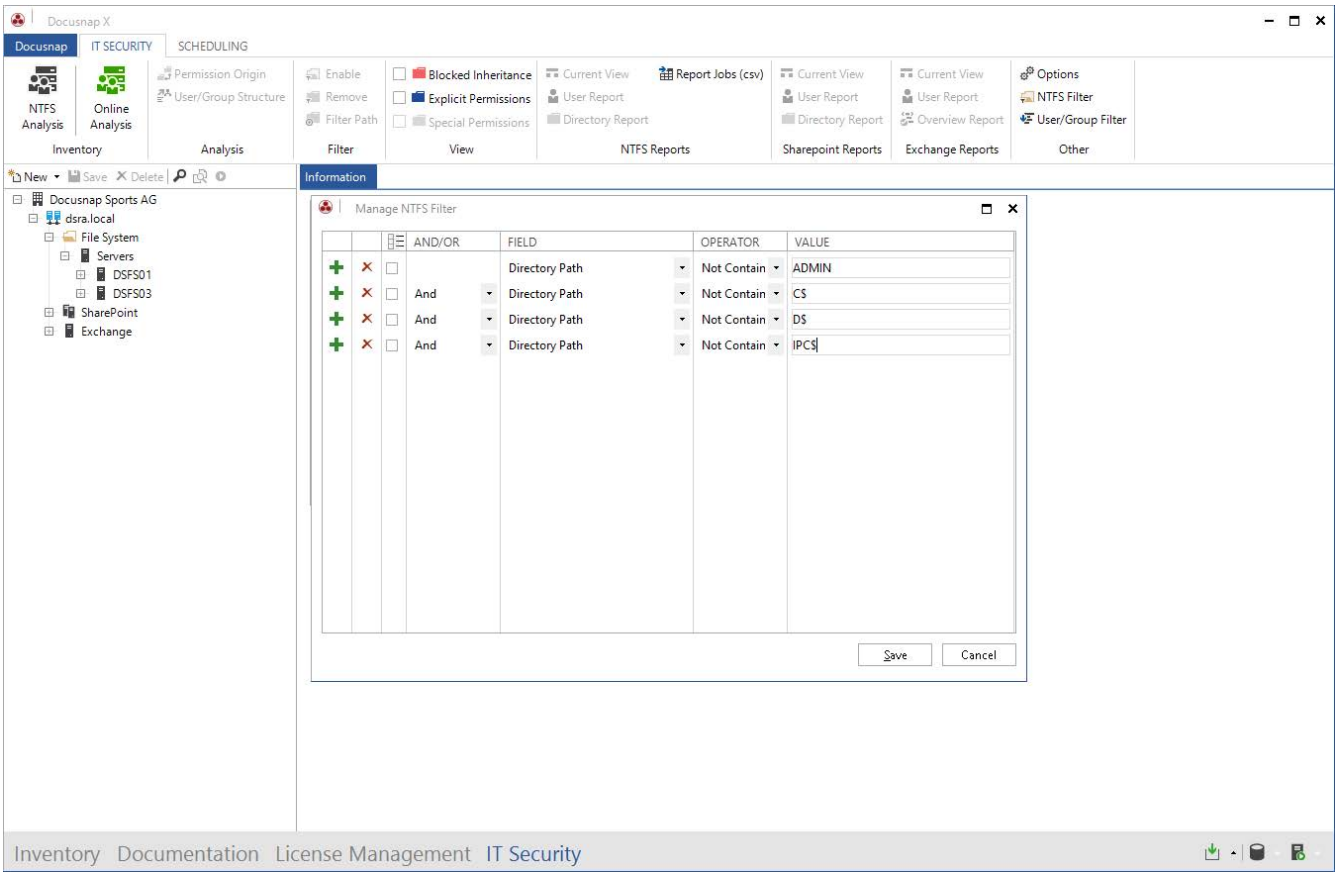

Figure 18 - Creating NTFS filter

2.3.4.3 ONLINE ANALYSIS

In addition to the so-called offline analysis - the inventory of the authorization via the previously discussed NTFS analysis - you can also perform an online analysis.

To do this, activate the online analysis using the control of the same name. In this course Docusnap tries to establish a connection to all inventoried Windows and CIFS systems as well as DFS shares.

This is useful if you need to "just do it fast" check the share and NTFS permissions of a less critical system. Here, too, you can use the **display options to** highlight folders in color whose inheritance has been deactivated or whose permissions have been set directly in addition to the inheritance.

Note that you cannot determine effective authorizations when using the online analysis. For this reason, no reports are available here.

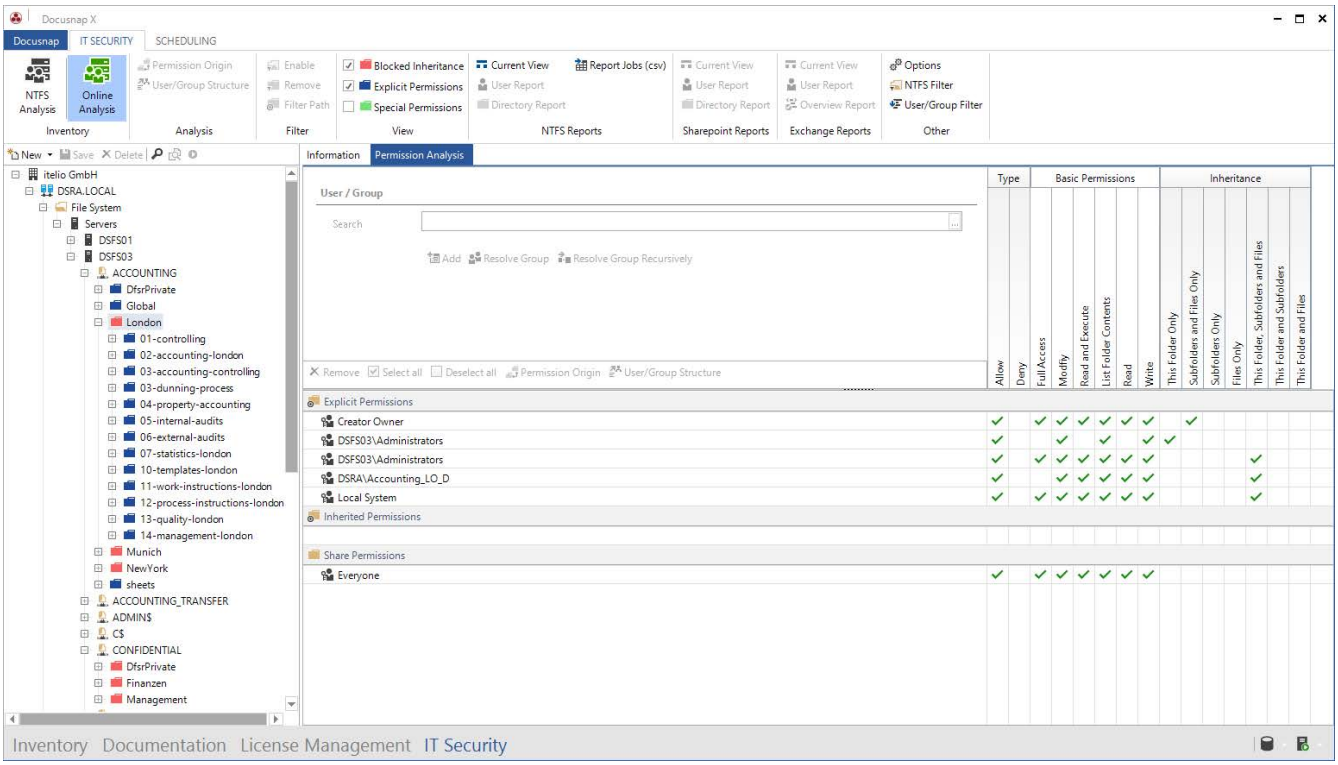

Figure 19 - Online analysis

2.3.4.4 REPORTING JOB (CSV)

If you want to create an extensive number of directory reports automatically at regular intervals, you can do this conveniently and quickly with a CSV file. Create a CSV file with the columns Domain, Host, Share/Path and Mail (sending the reports by mail).

Further information can be found in the corresponding HowTo in our Knowledge Base: Report Jobs (CSV).

2.3.4.5 USER/GROUP FILTER

When creating the directory report, there is a specific option to exclude domain administrators and other selected users and groups from the report. If you want to exclude these selected groups of people from the report on a recurring basis, you can do this using the **user/group filter** from the ribbon.

Click the New button to create a new filter, which will then be available to you when creating the directory report. In the **Search** area, add the group or user to the filter.

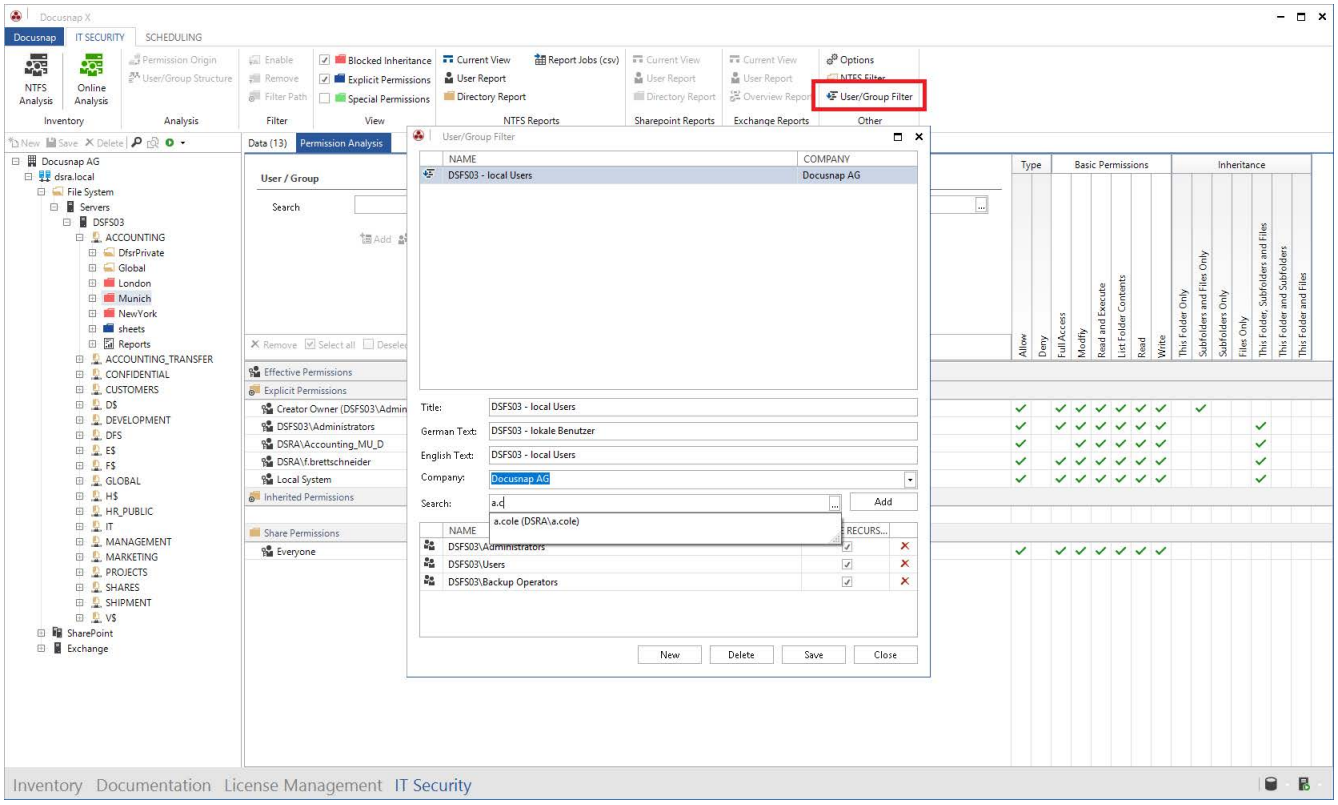

Figure 20 - User Group Filter

3. SHAREPOINT

3.1 REQUIREMENTS

To be able to evaluate the permissions of your SharePoint environment, an inventory of the SharePoint is required first. The permissions are automatically part of the inventory.

For a complete evaluation to be possible, the use of the farm administrator is assumed. You can find an overview of the set authorizations, for example for Web applications, in the tree structure.

3.2 ANALYSIS

Similar to the authorization analysis in file systems, it is also possible to perform evaluations for SharePoint environments. The user report and the directory report are also available. The current view of the matrix in the main window can also be generated.

The authorization analysis for SharePoint systems deals with the particularities of the underlying authorization concept. Only the individual authorizations are used here. Aggregation in authorization levels is not evaluated.

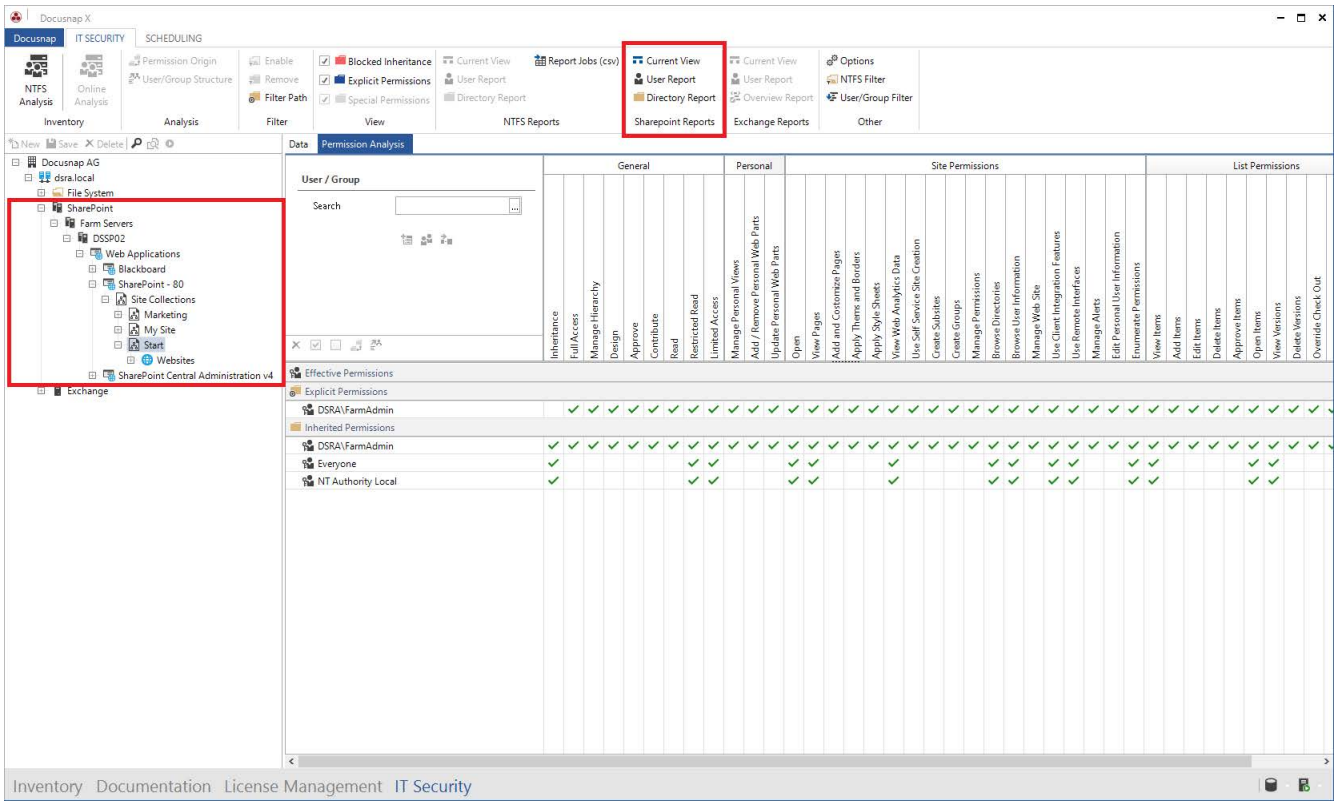

Figure 21 - SharePoint permission analysis

4. EXCHANGE

4.1 REQUIREMENT

In order to be able to evaluate Exchange permissions, you must first perform an inventory. The authorizations must be part of the inventory. These can be enabled in the Exchange Scan Wizard - Step 3 - Advanced Options. The authorizations are inventoried by default.

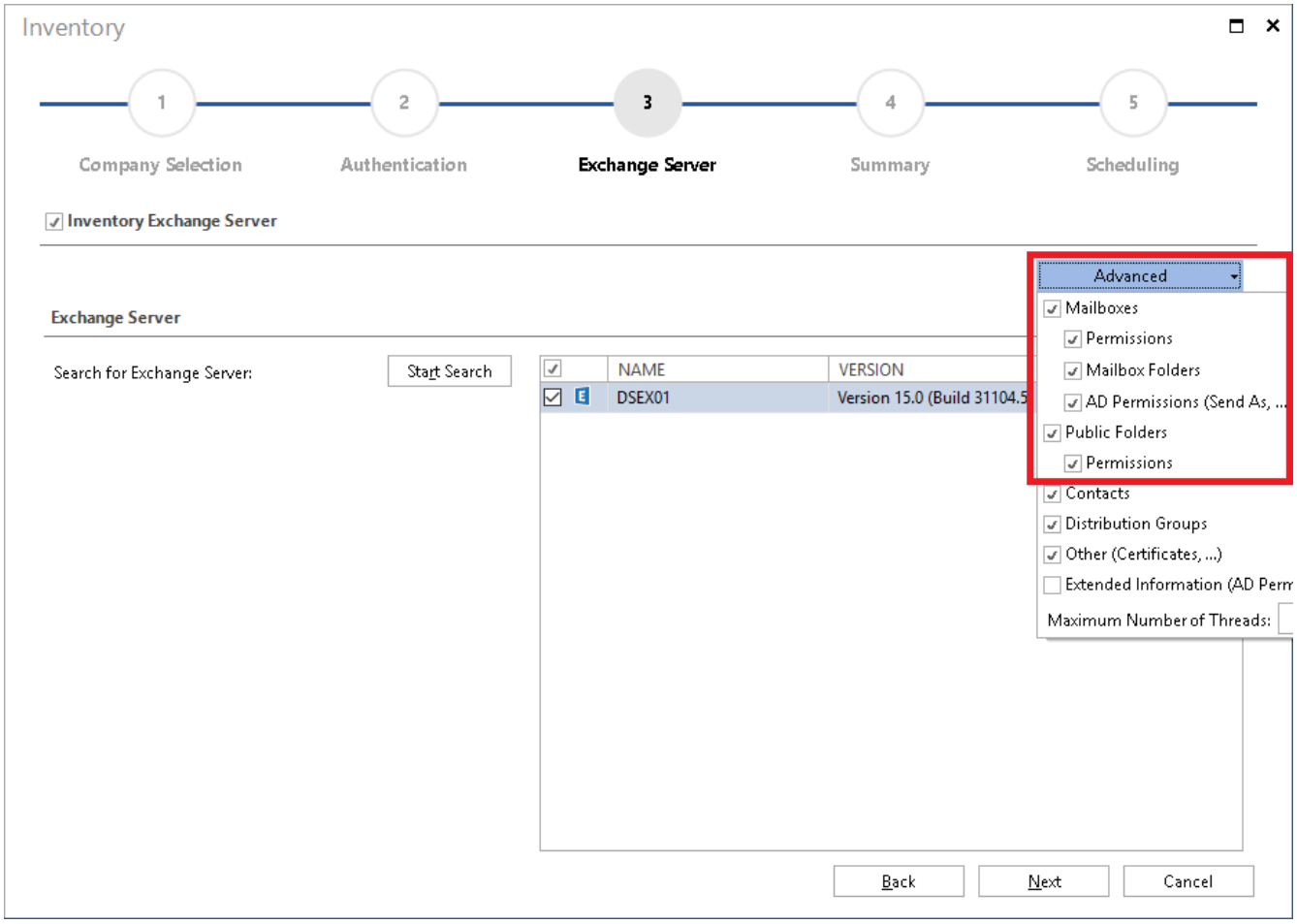

Figure 22 - Advanced Exchange inventory options

4.2 ANALYSIS

As with authorization analysis in file systems, it is also possible to perform evaluations for Exchange environments. The user report and the overview report (analogous to the directory report) are available. The current view of the matrix in the main window can also be generated.

The authorization analysis for Exchange systems deals with the special features of the underlying authorization concept. Both mailboxes and public folders can be viewed.

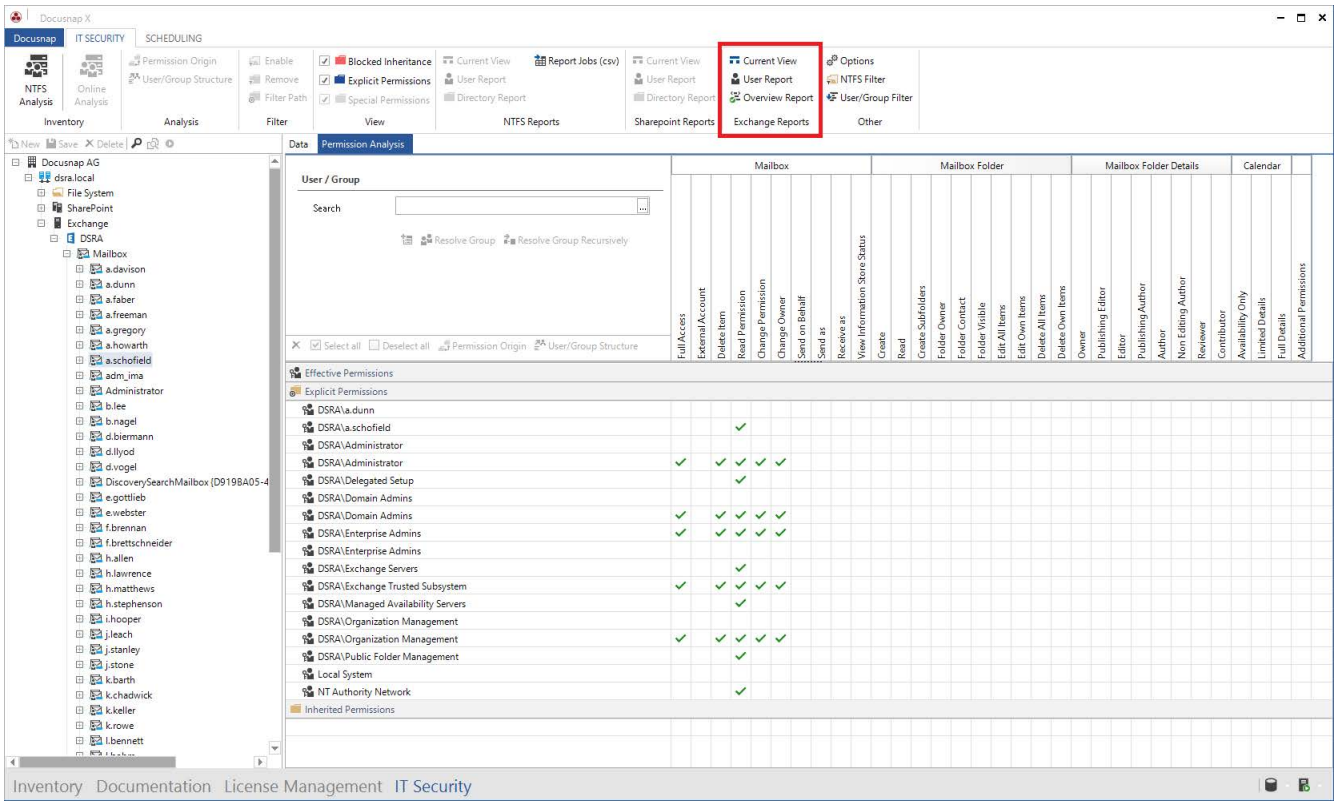

Figure 23 - Exchange permission analysis

LIST OF FIGURES

FIGURE 1 - STARTING NTFS ANALYSIS 7
FIGURE 2 - NTFS ANALYSIS HIERARCHICAL STRUCTURE 9
FIGURE 3 - USER - GROUP SELECTION 10
FIGURE 4 - ADVANCED USERS - GROUP SEARCH 11
FIGURE 5 - PERMISSION FILTER 12
FIGURE 6 - CREATE DIRECTORY REPORT 14
FIGURE 7 - DIRECTORY (RESOURCE) REPORT 15
FIGURE 8 - ADD USER 16
FIGURE 9 - USER REPORT OPTIONS 17
FIGURE 10 - USER REPORT 18
FIGURE 11 - SHARE REPORT OPTIONS 19
FIGURE 12 - SHARE REPORT 19
FIGURE 13 - SEND PERMISSION REPORTS BY E-MAIL 20
FIGURE 14 - SCHEDULE SHARE AND DIRECTORY REPORTS AS JOB 21
FIGURE 15 - CALL PERMISSION ORIGIN 22
FIGURE 16 - CHECK PERMISSION ORIGIN 23
FIGURE 17 - LIMIT FOLDER LEVELS 24
FIGURE 18 - CREATING NTFS FILTER 25
FIGURE 19 - ONLINE ANALYSIS 26
FIGURE 20 - USER GROUP FILTER 27
FIGURE 21 - SHAREPOINT PERMISSION ANALYSIS 28
FIGURE 22 - ADVANCED EXCHANGE INVENTORY OPTIONS 29
FIGURE 23 - EXCHANGE PERMISSION ANALYSIS 30

INDEX OF TABLES

No entries could be found for a table of figures.

© itelio GmbH - www.itelio.com