



IT-Security

Permission analysis in DocuSnap

TITLE	IT-Security
AUTHOR	Docusnap Consulting
DATE	10/18/2022
VERSION	2.3 valid from September 28, 2022

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	PERMISSION ORIGIN	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.

As of 15.09.2020, it is not possible to perform an authorization analysis on the inventoried Exchange Online data.

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 (On Premise)

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 [HowTo 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. During 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 if authorizations have been assigned here.

Windows - CIFS - DFS

The later NTFS analysis aims at drives or shares. For these to be available for selection, the systems and services above them must also be inventoried: Windows, CIFS and DFS. During 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 status.

The wizard for performing the NTFS analysis is located in the IT Security section, which can be accessed via the 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 analysed via their drives or shares (use shares for Windows systems).

Furthermore, you have the option of limiting the folder levels that are to be used for the NTFS analysis. This should be considered, as this setting has a considerable influence on the required database size (SQL-Express -10 GB).

In order to inventory new drives or shares of systems in already time scheduled ntfs analysis you can activate the option **For scheduled NTFS analysis....**New drives or shares from selected systems are then also inventoried.

If a filter is entered in the Drives column, newly found drives or shares are only inventoried if they match the filter.

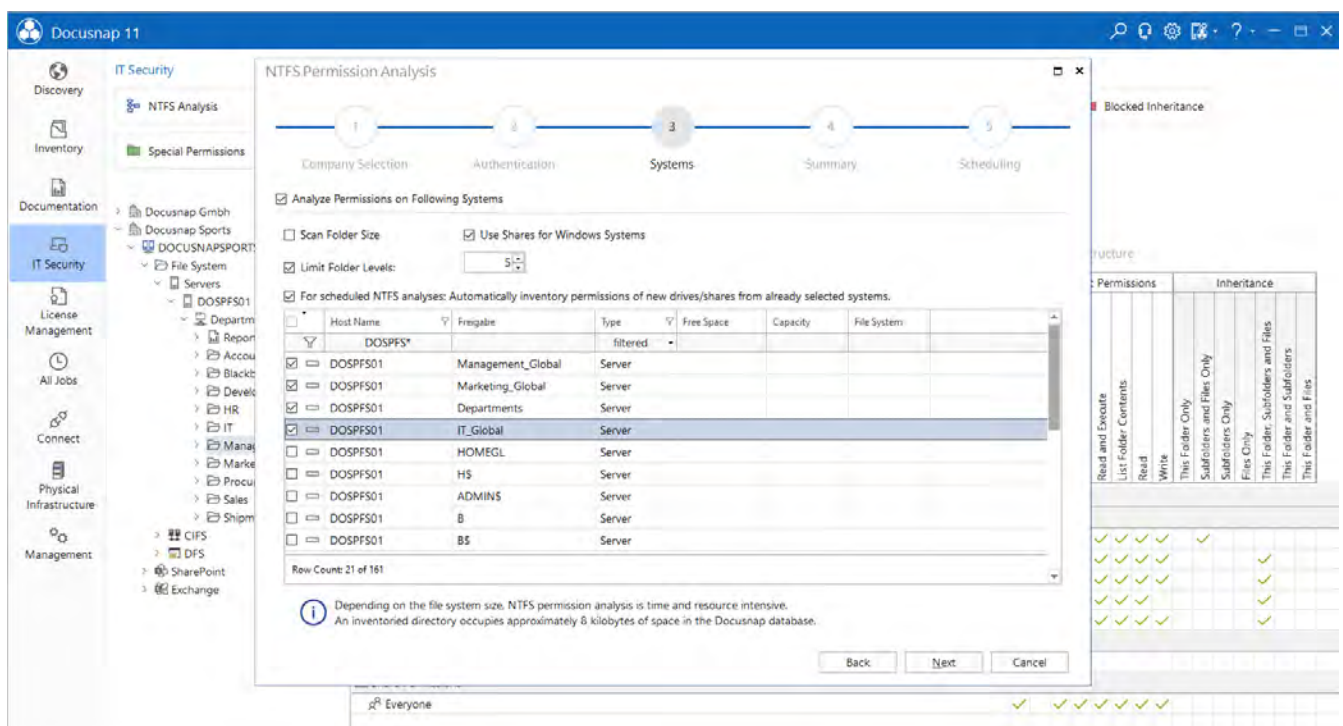


Figure 1 - Starting NTFS analysis

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 **explicit set permissions** are to be visible in the hierarchical structure, this can be activated in the ribbon in the **Display** area.

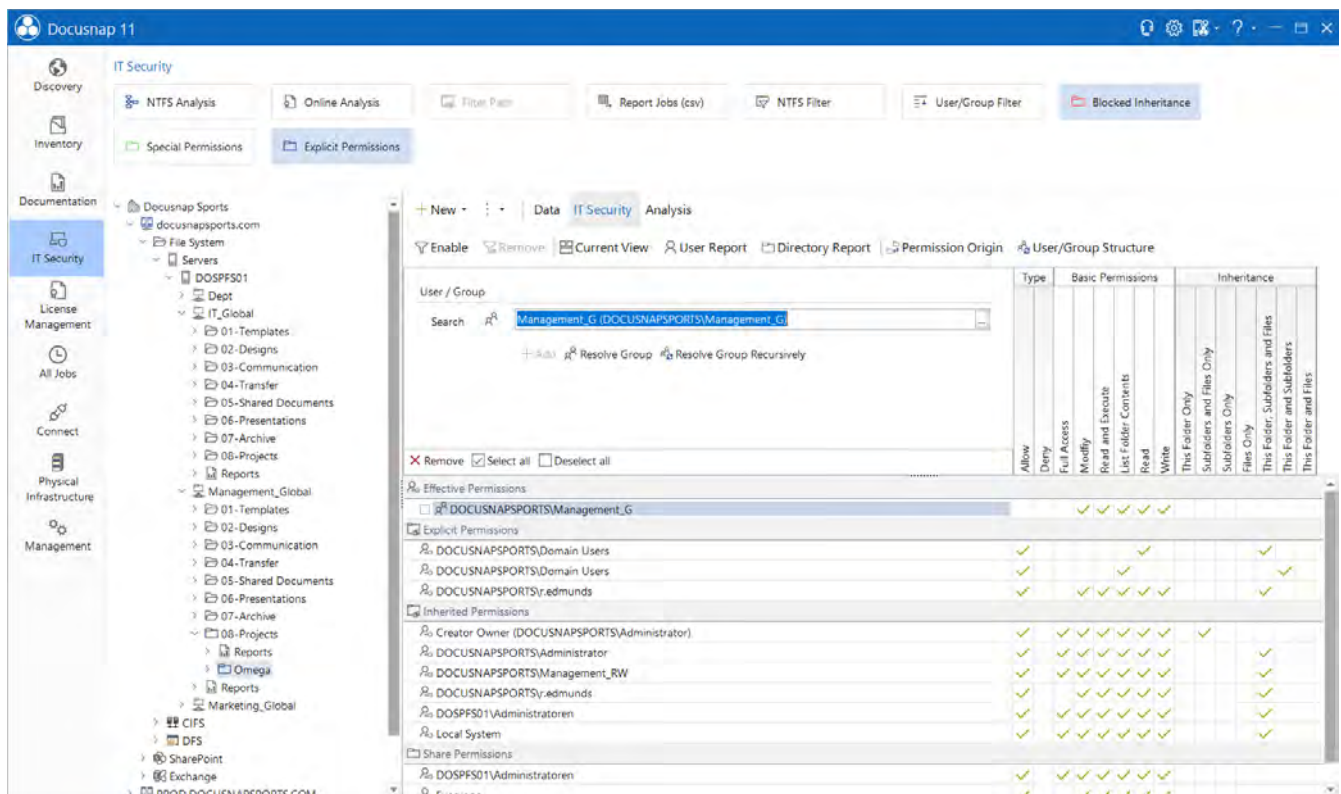


Figure 2 - NTFS analysis hierarchical structure

2.3.1.1 USER-GROUP SEARCH

In the data 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.

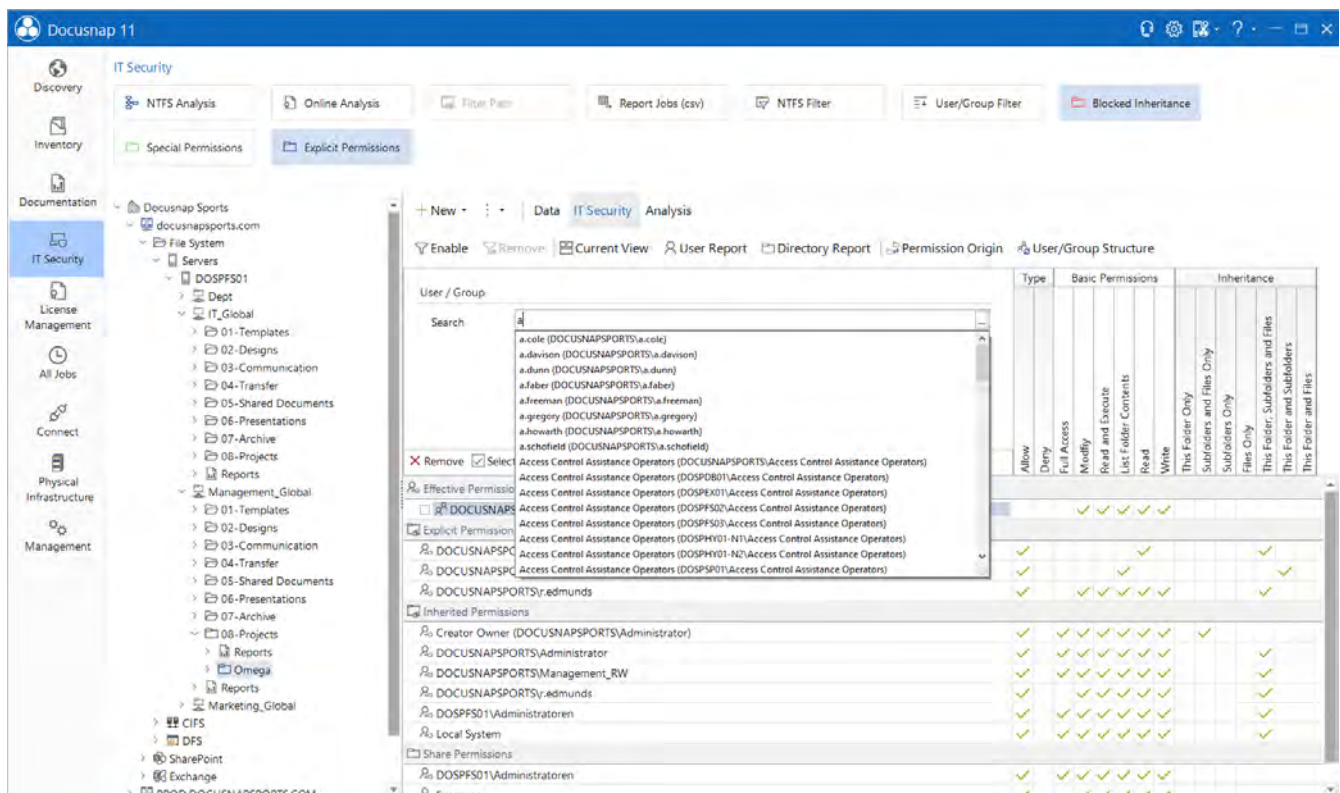


Figure 3 - User - Group Selection

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.

Search for Groups and Users

Identities

Disable Filter

Search

Reset Filter

Save Filter

Load Filter

		AND/OR	FIELD	OPERATOR	VALUE
+	×		Department	Contains	Accounting
+	×	And	User Account Control	=	Account Activated
+	×	And		=	

☒ Name
☐ a.cole
☐ a.davison
☐ a.dunn
☐ a.faber
☐ a.freeman
☐ a.gregory
☐ a.howarth
☐ a.schofield
☐ Access Control Assistanc...
☐ Account Operators
☐ Accounting
☐ Accounting_D
☐ Accounting_G
☐ Accounting_LO_D
☐ Accounting_LO_G
☐ Accounting_MU_D
☐ Accounting_MU_G
☐ Accounting_NY_D
☐ Accounting_NY_G
☐ Accounting_U
☐ Administrator
☐ Administrator

Account Expires

Account locked out since

Account Name History

Admin Description

Admin Display Name

Bad Password Time

Canonical Name

City

Company

Country Code

create Time Stamp

Created On

Department

Description

Desktop Profile

Direct Reports

Display name

Distinguished Name

Effective Rights Security De

E-mail

Fax

Garbage Collection Period

Given Name

Group scope

Home

Home drive

Home folder

Home Phone Number (Oth

Initials

IP Phone

User Principal Name

cole a.cole@DOCUSNAPSPORTS.COM

davison a.davison@DOCUSNAPSPORTS.COM

dunn a.dunn@DOCUSNAPSPORTS.COM

faber a.faber@DOCUSNAPSPORTS.COM

freeman a.freeman@DOCUSNAPSPORTS.COM

gregory a.gregory@DOCUSNAPSPORTS.COM

howarth a.howarth@DOCUSNAPSPORTS.COM

schofield a.schofield@DOCUSNAPSPORTS.COM

ccess C...

ccount ...

ccounti...

ccounti...

ccounti...

ccounti...

ccounti...

ccounti...

ccounti...

ccounti...

ccounti...

ccounti...

ccounti...

ccounti...

Administrator@DOCUSNAPSPORTS.COM

Administrator@DOCUSNAPSPORTS.COM

Apply

Back

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.

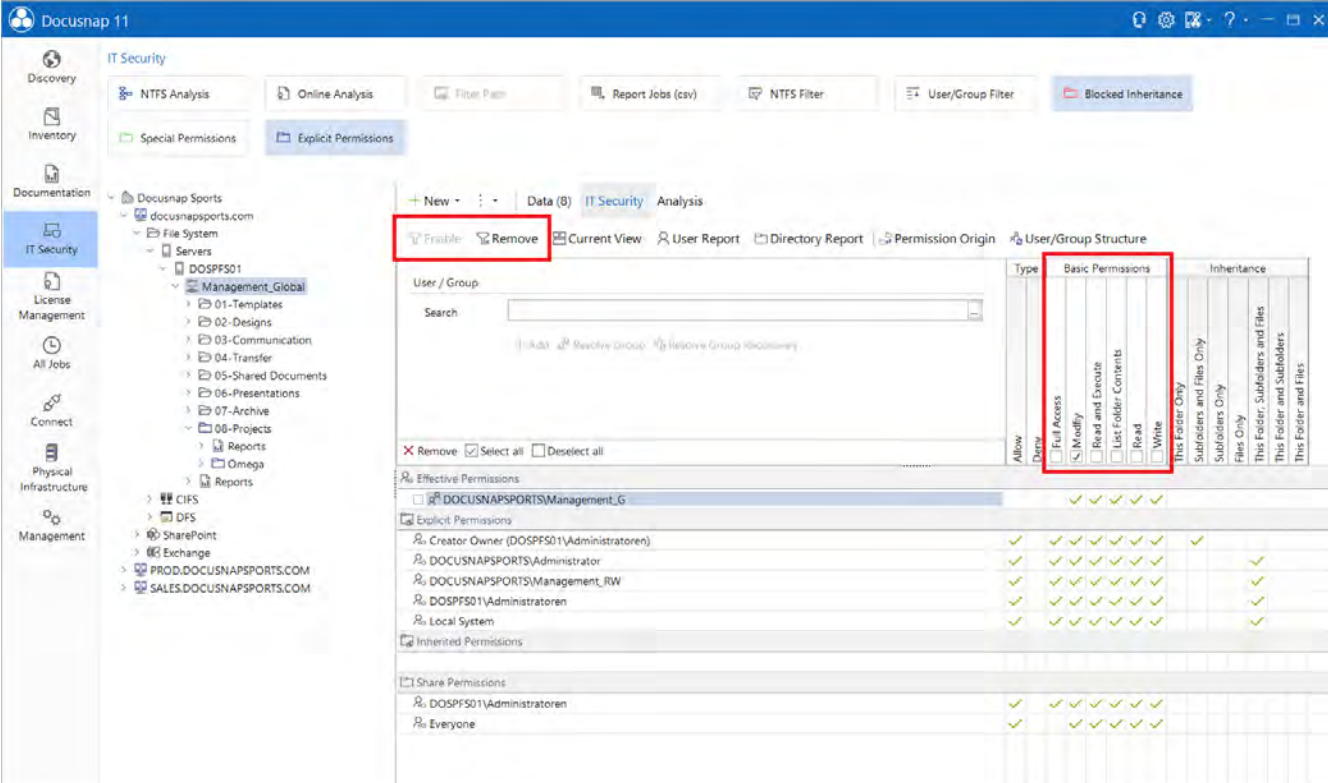
To do this, activate the filter within the field of action. Then select the appropriate permission that the user or group must have for the folders to be displayed in the tree structure.

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.



The screenshot shows the Docusnap 11 IT Security interface. On the left is a navigation pane with categories like Discovery, Inventory, Documentation, IT Security, License Management, All Jobs, Connect, Physical Infrastructure, and Management. The main area is titled 'IT Security' and contains several tabs: NTFS Analysis, Online Analysis, Filter Path, Report Jobs (csv), NTFS Filter, User/Group Filter, and Blocked Inheritance. The 'NTFS Filter' tab is active, showing a 'Filter' button (highlighted with a red box) and a 'Remove' button. Below these buttons is a table with columns: User / Group, Type, Basic Permissions, and Inheritance. The 'Basic Permissions' column is highlighted with a red box and contains checkboxes for: Full Control, Modify, Read and Execute, List Folder Contents, Read, and Write. The table lists various users and groups, including 'DOCUSNAPSORTS\Management_G', 'DOCUSNAPSORTS\Administratoren', 'DOCUSNAPSORTS\Administrator', 'DOCUSNAPSORTS\Management_RW', 'DOCUSNAPSORTS\Administratoren', and 'Local System'. The 'Inheritance' column shows the inheritance status for each user/group.

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 considered 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 field of action.

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

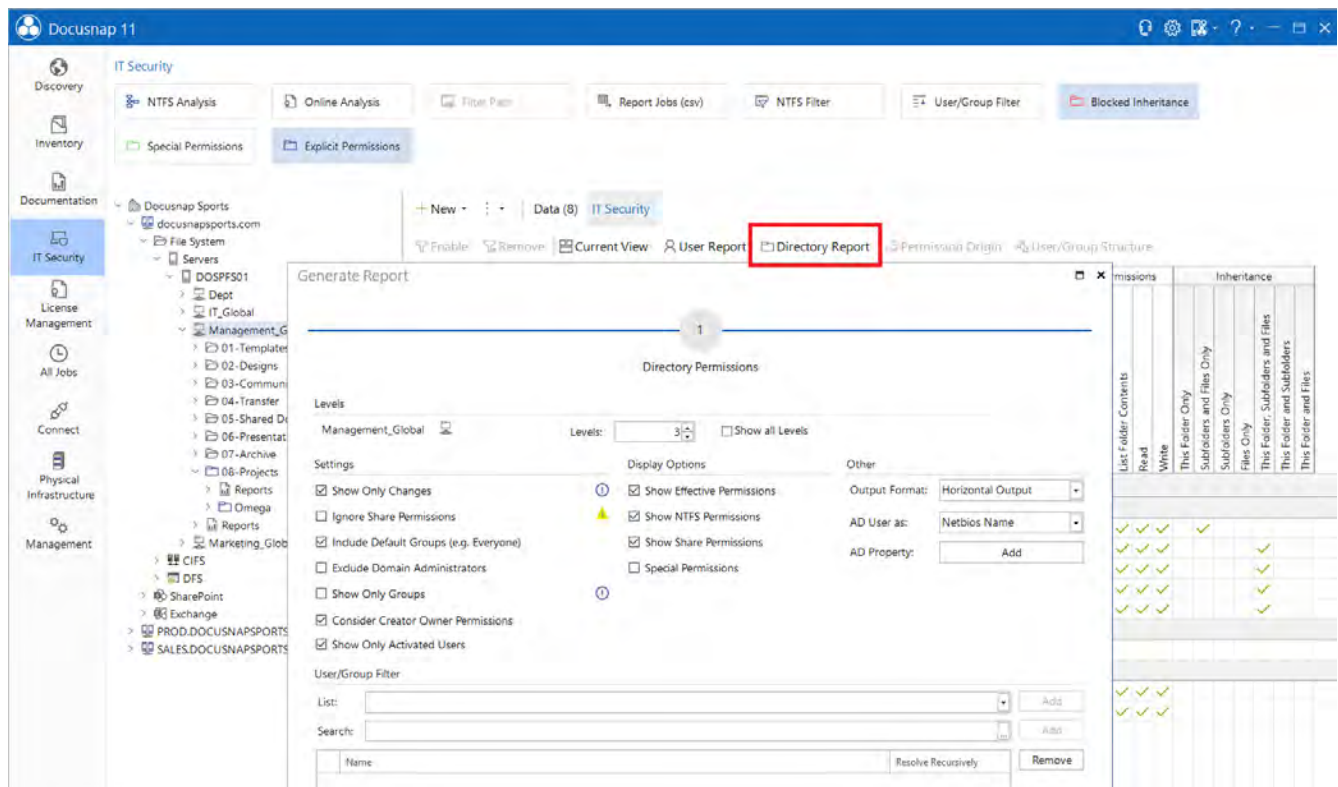


Figure 6 - Create directory report

- **Levels**
 - 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.
- **display 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
 - CSV
 - 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.

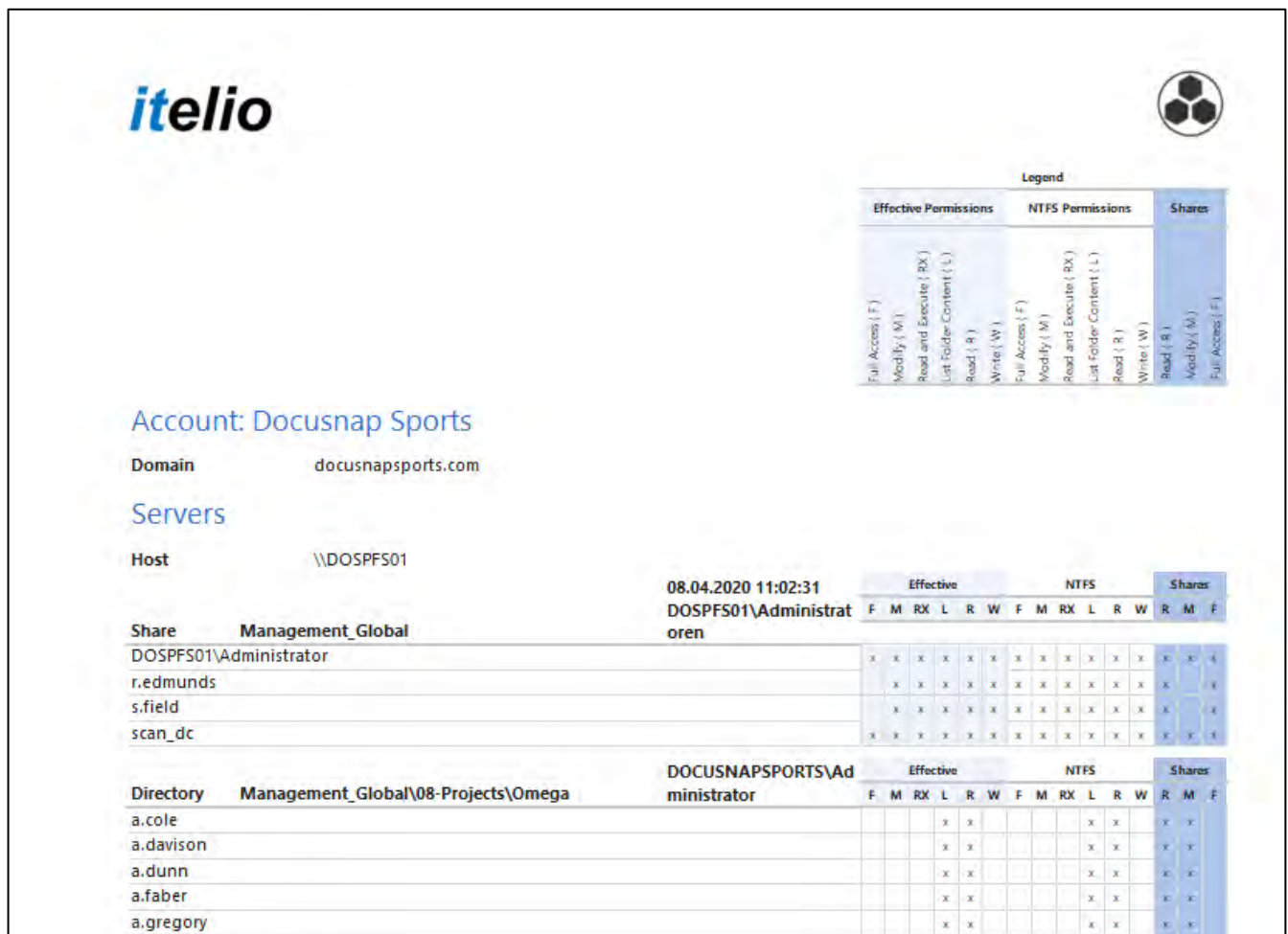


Figure 7 - Directory (Resource) report

2.3.2.1.1 CUSTOMIZE DEFAULT SETTINGS

In the options - IT Security you have the possibility to customize the default settings for the directory report generation. The options selected here will be set as default in the future when you create a new directory report.

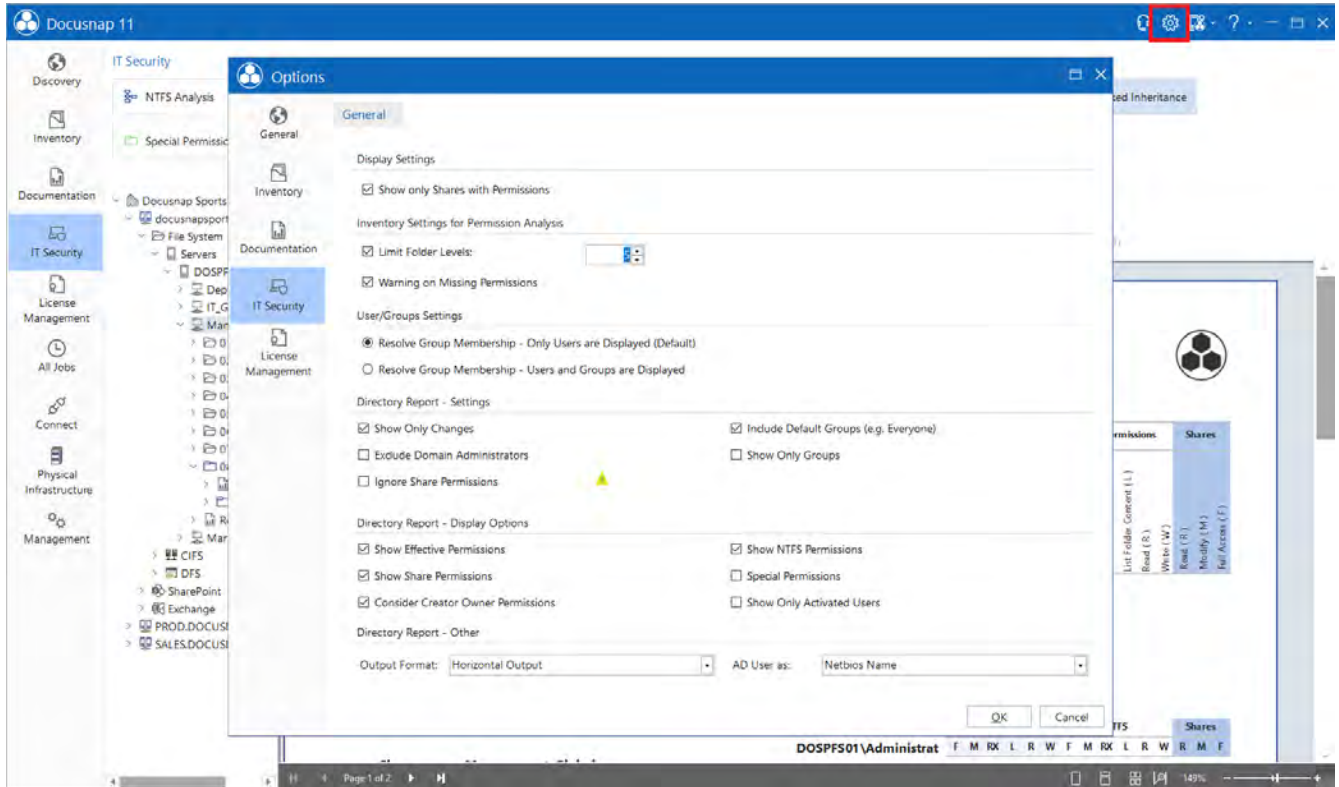


Figure 8 - Adjust default settings for the directory report

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.

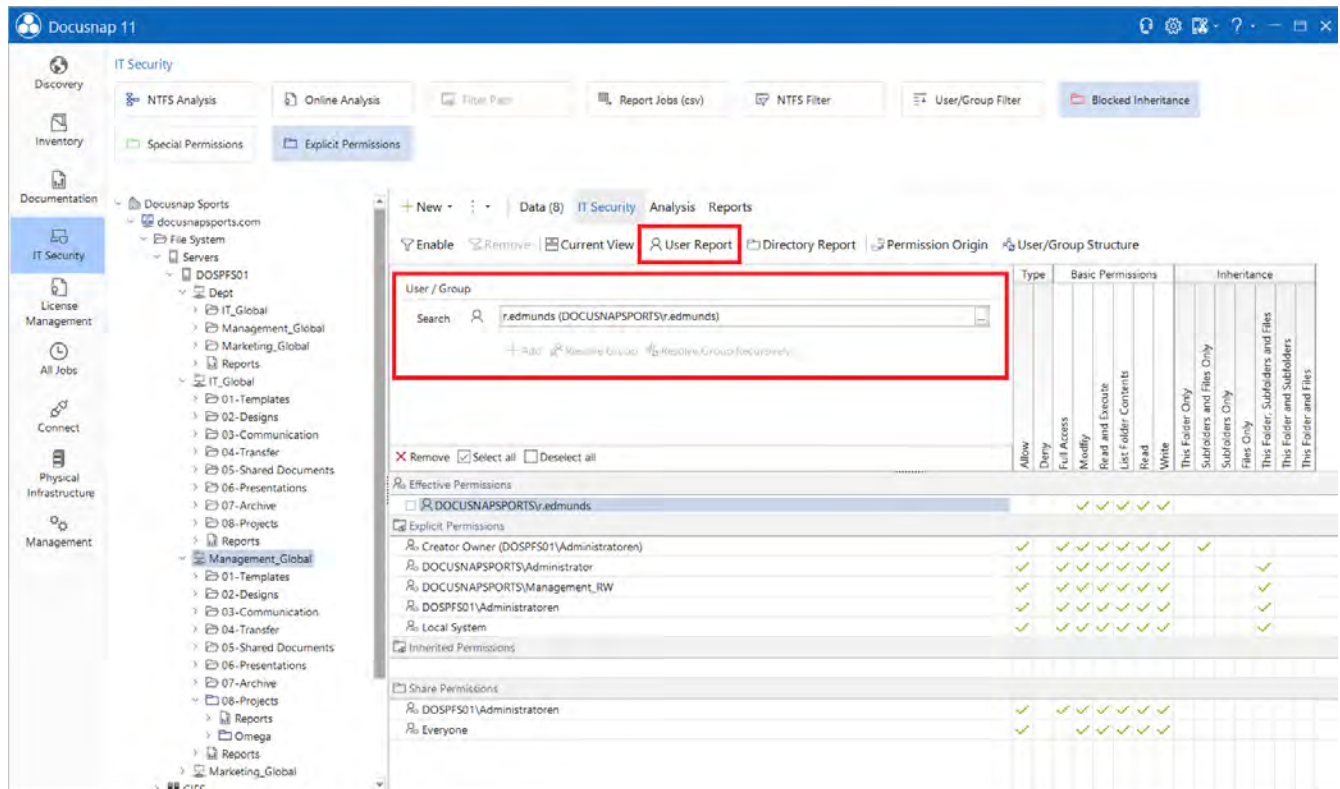


Figure 9 - Add user

The following options are available in the wizard. Detailed explanations can be found in the user manual - F1.

- **Levels**
 - Number of levels analyzed within the report
- **Show only changes**
 - 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.
- **Show subfolders without permissions**
 - Should folders to which the selected user / group has no permissions be listed in the report?

Generate Report
□ ×

1

User Permissions

Levels

Management_Global
📁

Levels:

3

Show all Levels

Settings

☒ Show Only Changes

☐ Special Permissions

☒ Consider Creator Owner Permissions

☐ Show Subfolders without Permissions

☐ Ignore Share Permissions

Other

Output Format:

Horizontal Output

AD User as:

Display Name

AD Property:

	Property Name	Property Type	Single Value	
<input type="checkbox"/>	accountexpires	Period	Yes	
<input type="checkbox"/>	accountNameHistory	Text	No	
<input type="checkbox"/>	activationSchedule	Text	Yes	
<input type="checkbox"/>	activationStyle	Number	Yes	
<input type="checkbox"/>	adminDescription	Text	Yes	

Row Count: 109 of 109

Create

Schedule

Cancel

Figure 10 - User report options

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 regarding the scope of the reports:

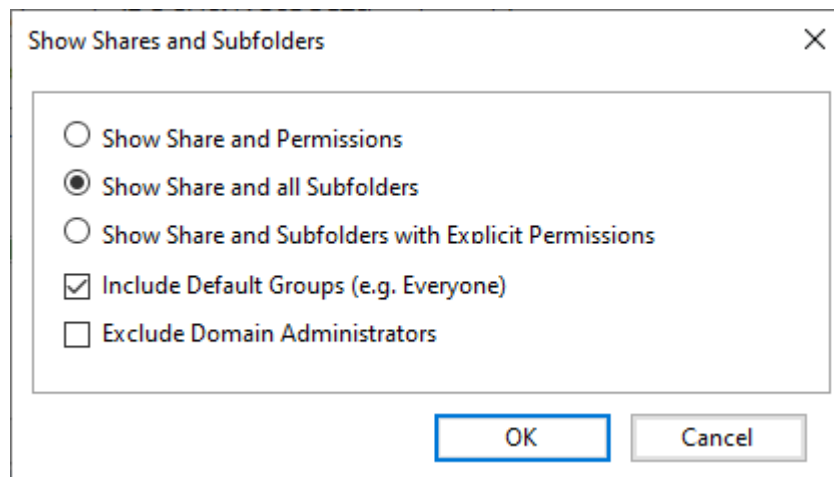


Figure 11 - Share report options

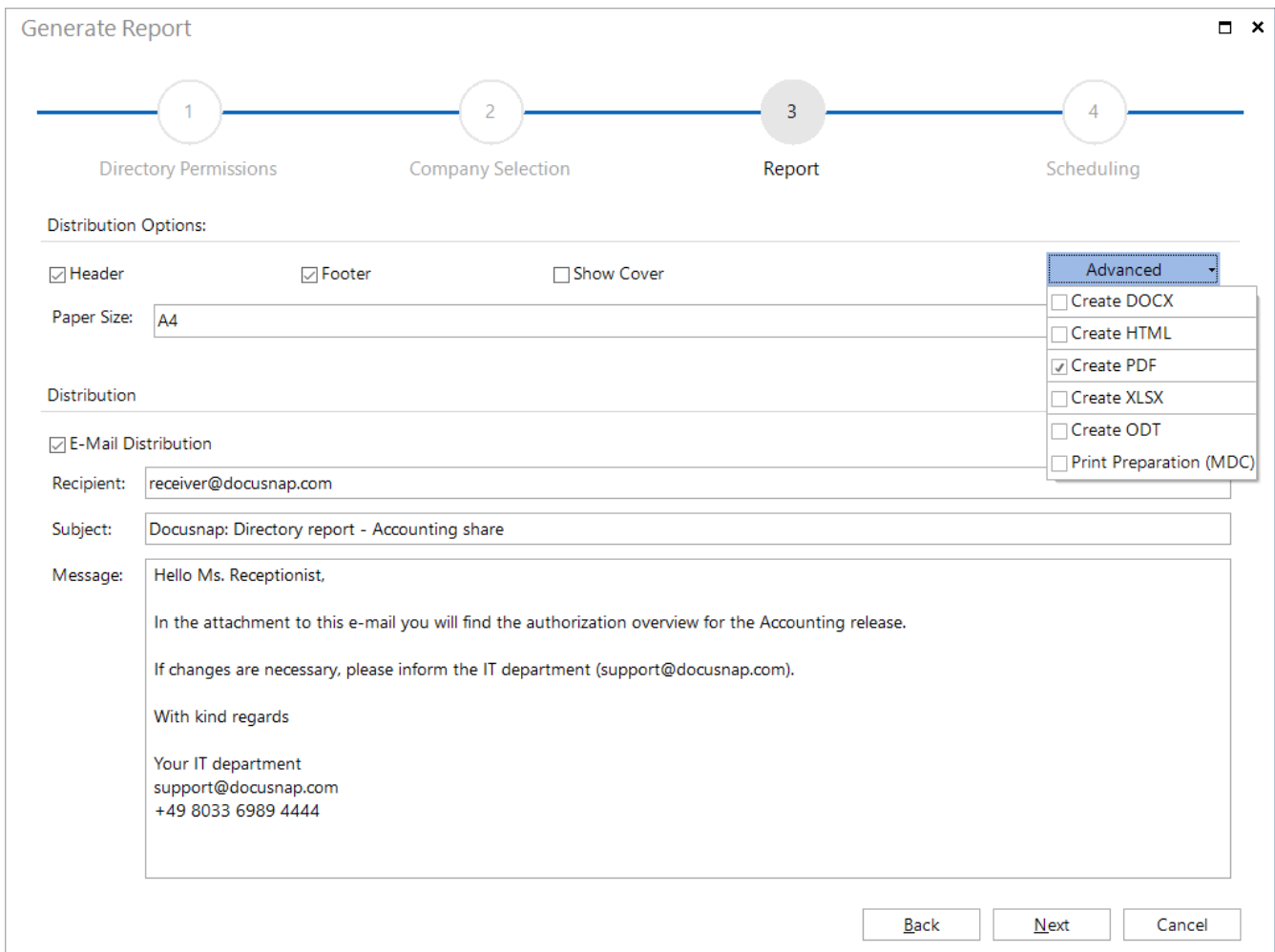
2.3.2.4 CREATE AND SEND REPORTS ON A SCHEDULED BASIS

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



Generate Report

1 Directory Permissions 2 Company Selection 3 **Report** 4 Scheduling

Distribution Options:

☒ Header ☒ Footer ☐ Show Cover

Paper Size: A4

Distribution

☒ E-Mail Distribution

Recipient: receiver@docusnap.com

Subject: Docusnap: Directory report - Accounting share

Message:

Hello Ms. Receptionist,

In the attachment to this e-mail you will find the authorization overview for the Accounting release.

If changes are necessary, please inform the IT department (support@docusnap.com).

With kind regards

Your IT department
support@docusnap.com
+49 8033 6989 4444

Advanced

- ☐ Create DOCX
- ☐ Create HTML
- ☒ Create PDF
- ☐ Create XLSX
- ☐ Create ODT
- ☐ Print Preparation (MDC)

Back Next Cancel

Figure 12 - Send permission reports by e-mail

You can also create and send the share and directory report time-controlled after creation via the **Schedule as Job** button:

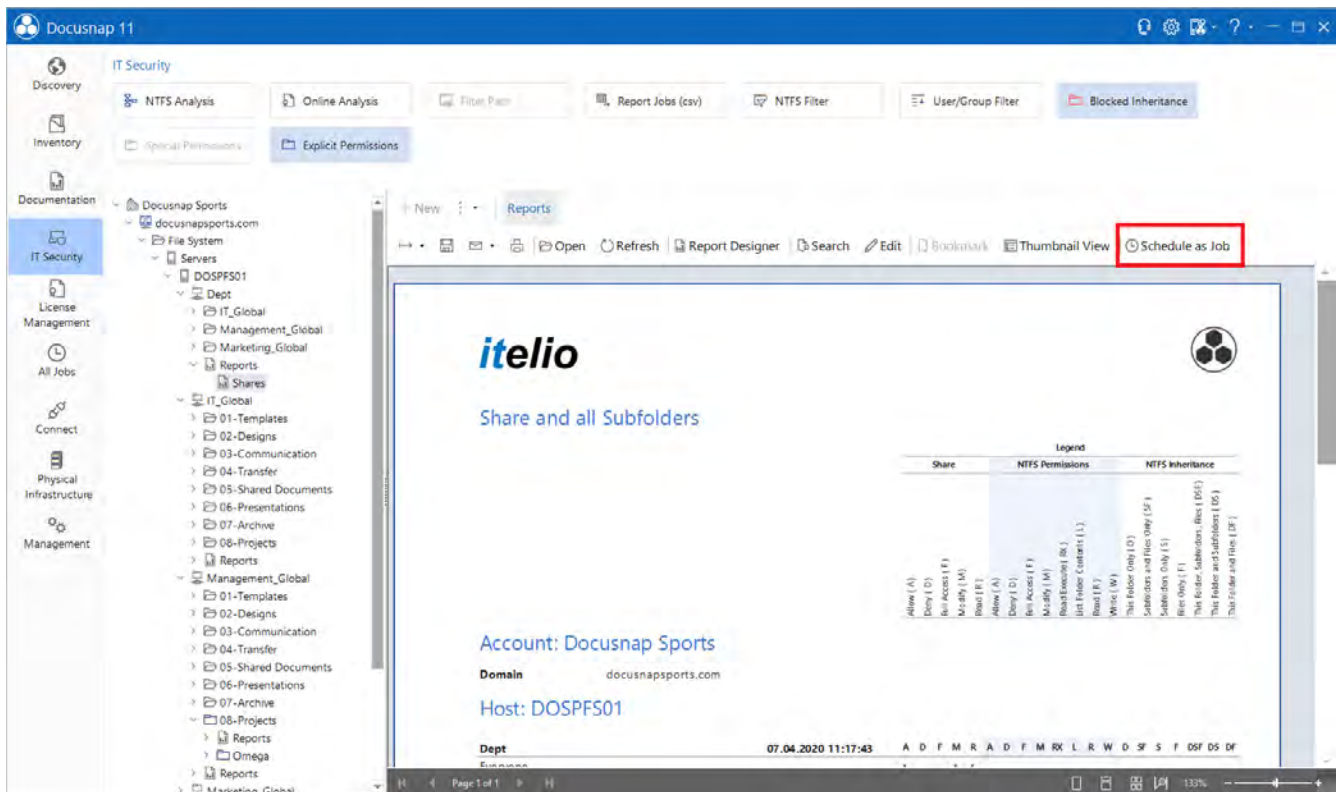


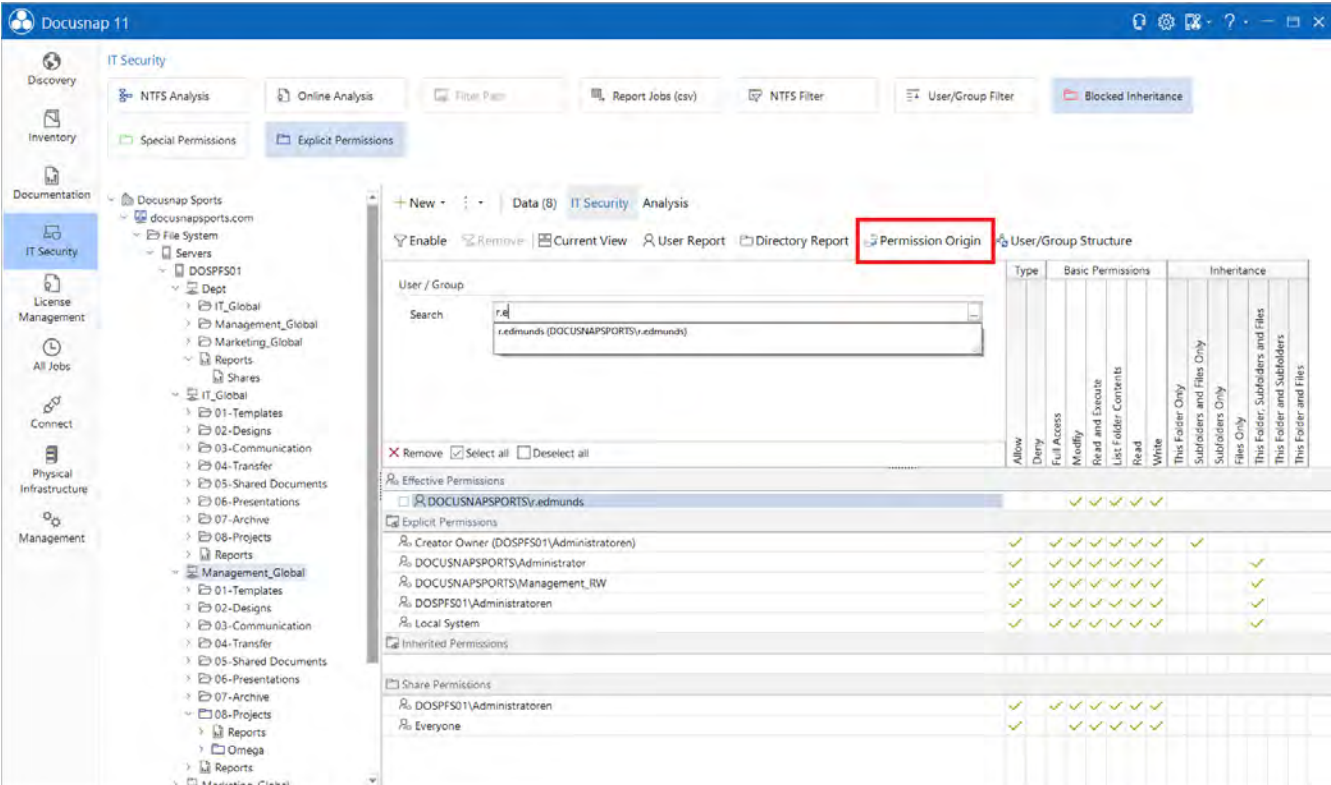
Figure 13 - Schedule Share and directory reports as job

2.3.3 PERMISSION ORIGIN

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

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

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



The screenshot shows the Docusnap 11 interface with the 'IT Security' tab selected. The 'Permission Origin' sub-tab is active, highlighted with a red box. The search field contains 'r.edmunds (DOCUSNAPSORTS\y.edmunds)'. The 'Effective Permissions' section shows a list of permissions for the selected user, including 'Creator Owner (DOSPFS01\Administratoren)' and 'DOCUSNAPSORTS\Administrator'. The 'Explicit Permissions' section shows a list of permissions for the selected user, including 'DOCUSNAPSORTS\Management_IRW' and 'DOSPFS01\Administratoren'. The 'Inherited Permissions' section shows a list of permissions for the selected user, including 'Local System' and 'DOSPFS01\Administratoren'.

Type	Basic Permissions	Inheritance
Allow		
Deny		
Full Access		
Modify		
Read and Execute		
List Folder Contents		
Read		
Write		
This Folder Only		
Subfolders and Files Only		
Subfolders Only		
Files Only		
This Folder, Subfolders and Files		
This Folder and Subfolders		
This Folder and Files		

Figure 14 - Call permission origin

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

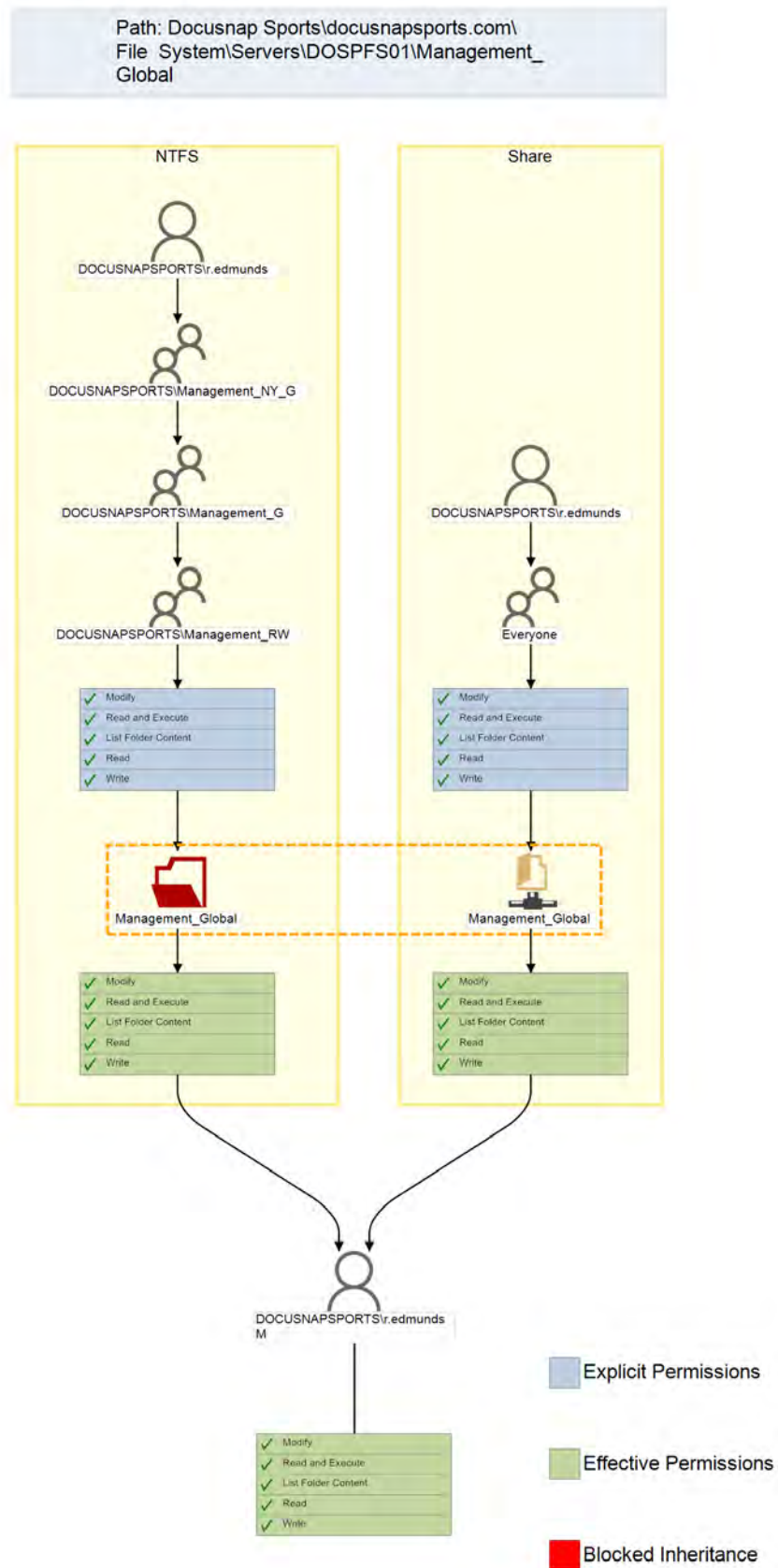


Figure 15 - Check permission origin

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.

The first possibility to limit the folder levels you have already learned around NTFS analysis. In this case, the limitation only applies to the specific NTFS analysis that you want to perform or schedule.

Within the **Options - IT Security** you have the possibility to limit the folder levels in general or to adjust the preselection that the folder levels are not limited.

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.

- Share (Level 1)
 - o Folder (Level 2)
 - Subfolder (Level 3)

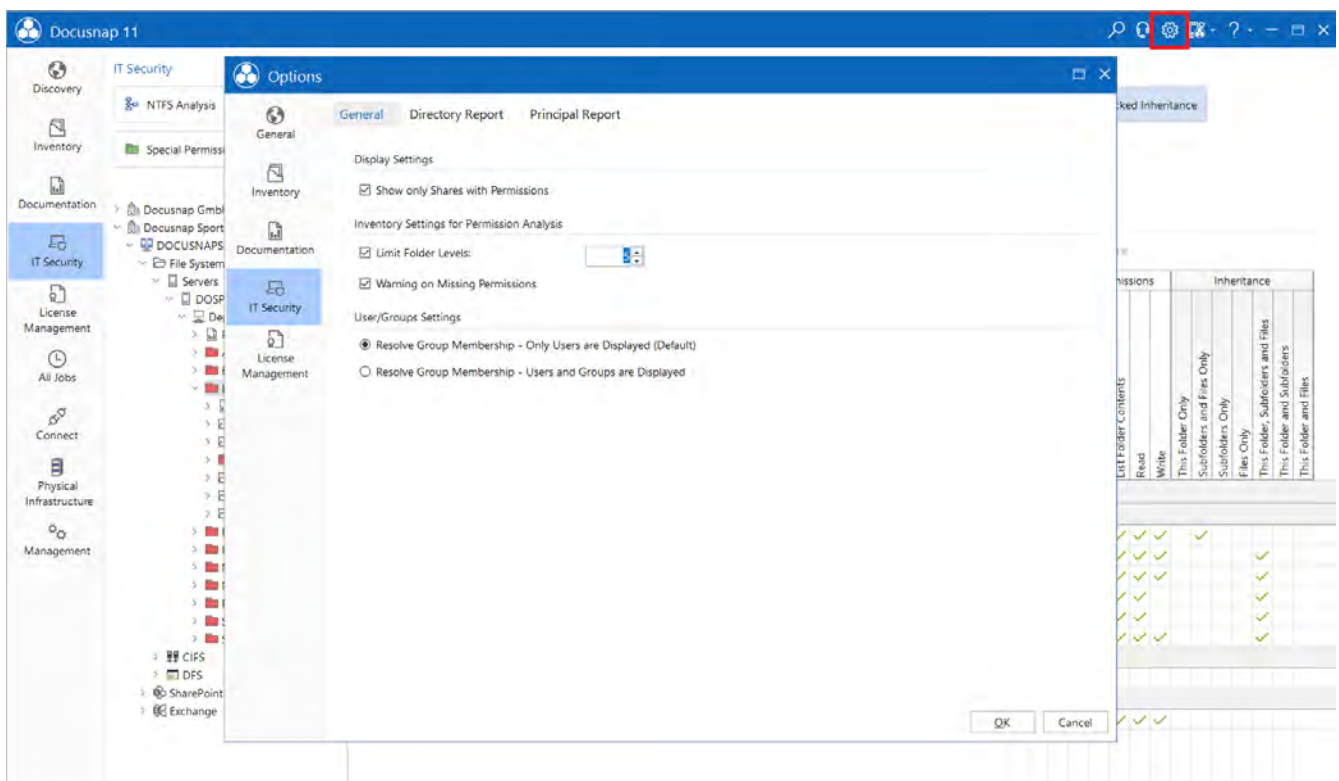


Figure 16 - Limit folder levels

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.

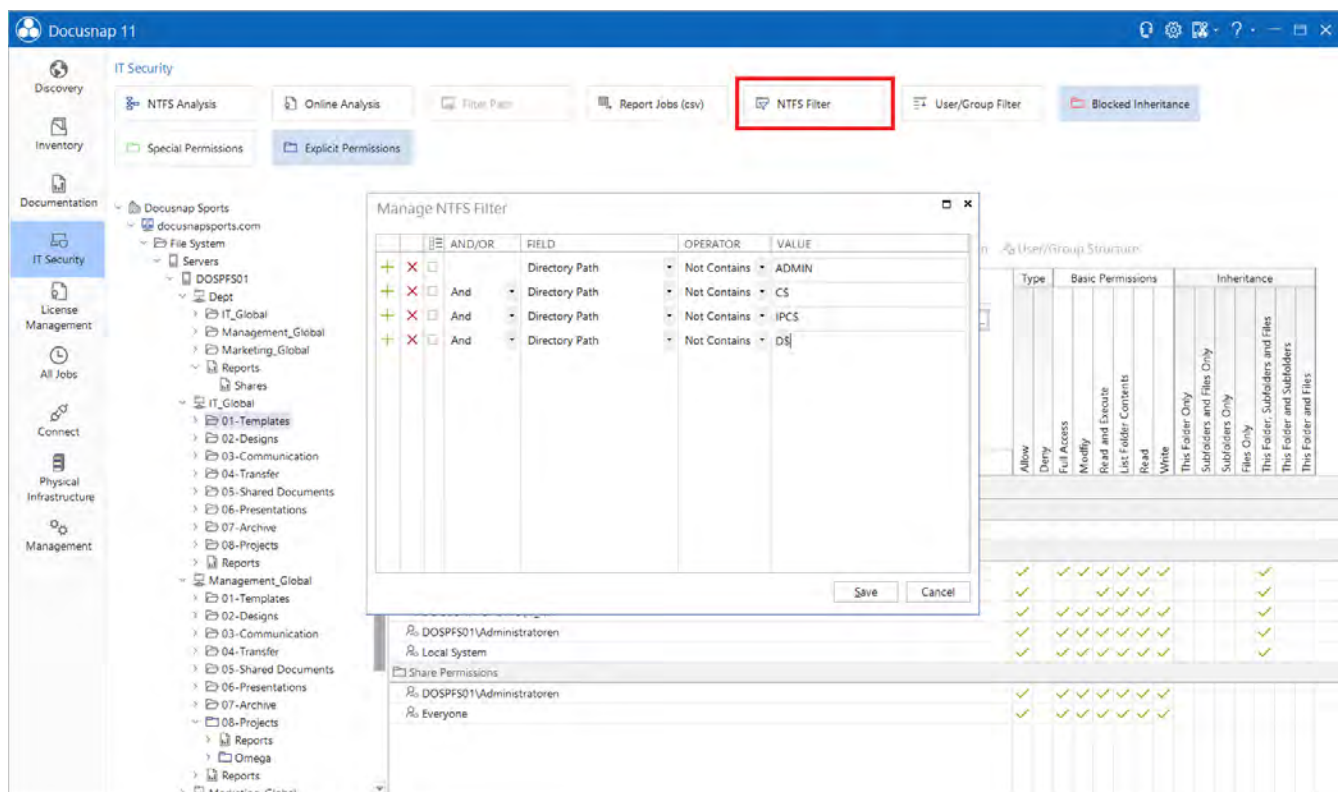


Figure 17 - Creating NTFS filter

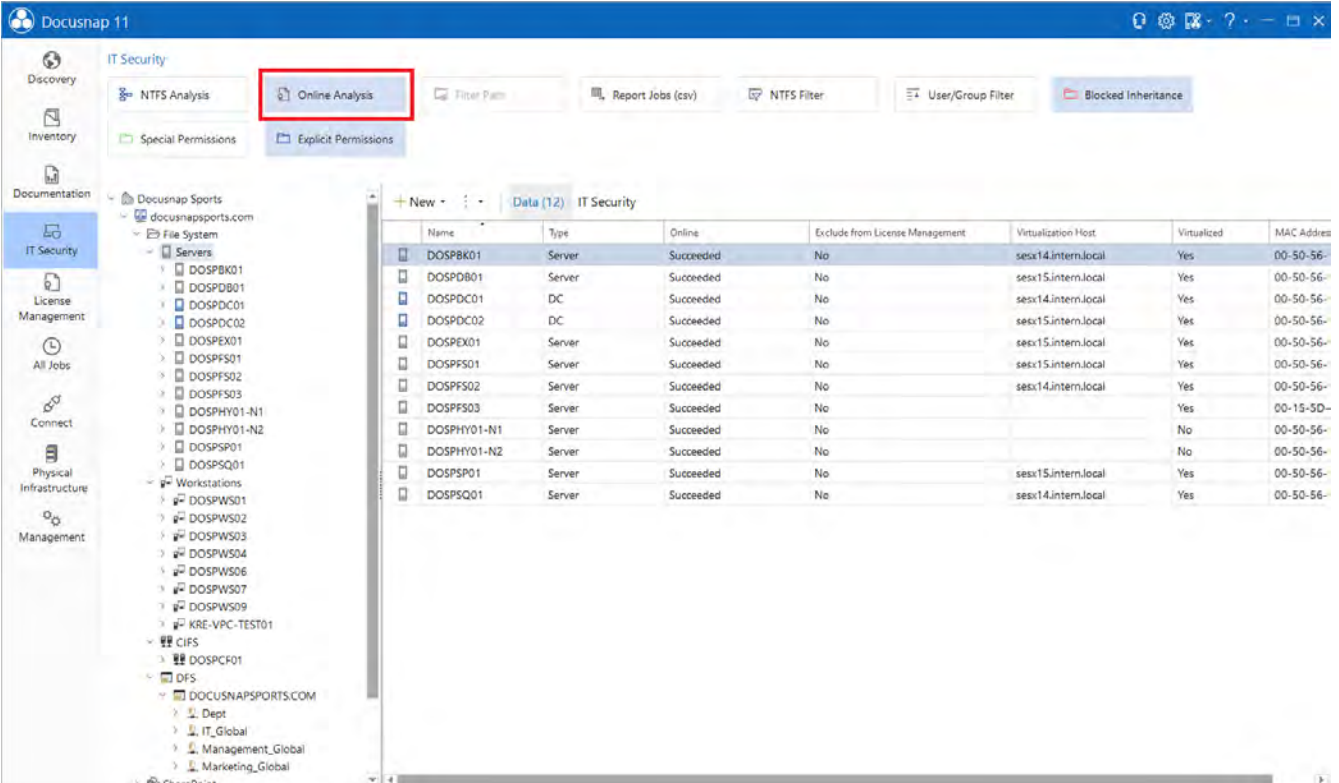
2.3.4.3 ONLINE ANALYSIS

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 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.



The screenshot shows the Docusnap 11 IT Security interface. The 'Online Analysis' tab is selected and highlighted with a red box. The main window displays a table of systems with the following columns: Name, Type, Online, Exclude from License Management, Virtualization Host, Virtualized, and MAC Address. The table contains 17 rows of data, including servers, DCs, and workstations.

Name	Type	Online	Exclude from License Management	Virtualization Host	Virtualized	MAC Address
DOSPBK01	Server	Succeeded	No	sesx14.intern.local	Yes	00-50-56-
DOSPD801	Server	Succeeded	No	sesx15.intern.local	Yes	00-50-56-
DOSPD01	DC	Succeeded	No	sesx14.intern.local	Yes	00-50-56-
DOSPD02	DC	Succeeded	No	sesx15.intern.local	Yes	00-50-56-
DOSPEX01	Server	Succeeded	No	sesx15.intern.local	Yes	00-50-56-
DOSPPS01	Server	Succeeded	No	sesx15.intern.local	Yes	00-50-56-
DOSPPS02	Server	Succeeded	No	sesx14.intern.local	Yes	00-50-56-
DOSPPS03	Server	Succeeded	No		Yes	00-15-5D-
DOSPHY01-N1	Server	Succeeded	No		No	00-50-56-
DOSPHY01-N2	Server	Succeeded	No		No	00-50-56-
DOSPSQ01	Server	Succeeded	No	sesx15.intern.local	Yes	00-50-56-
DOSPSQ01	Server	Succeeded	No	sesx14.intern.local	Yes	00-50-56-

Figure 18 - 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.

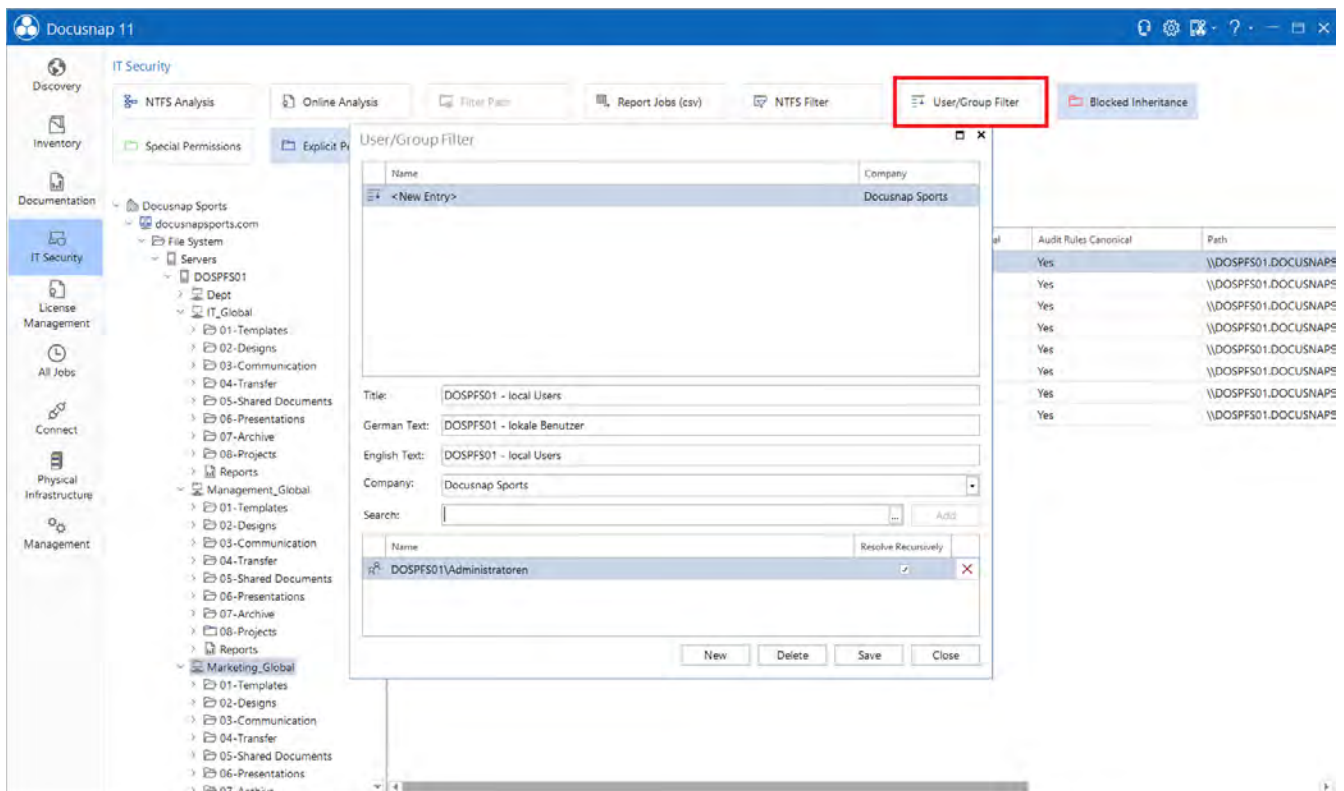


Figure 19 - User Group Filter

3. SHAREPOINT

3.1 REQUIREMENTS

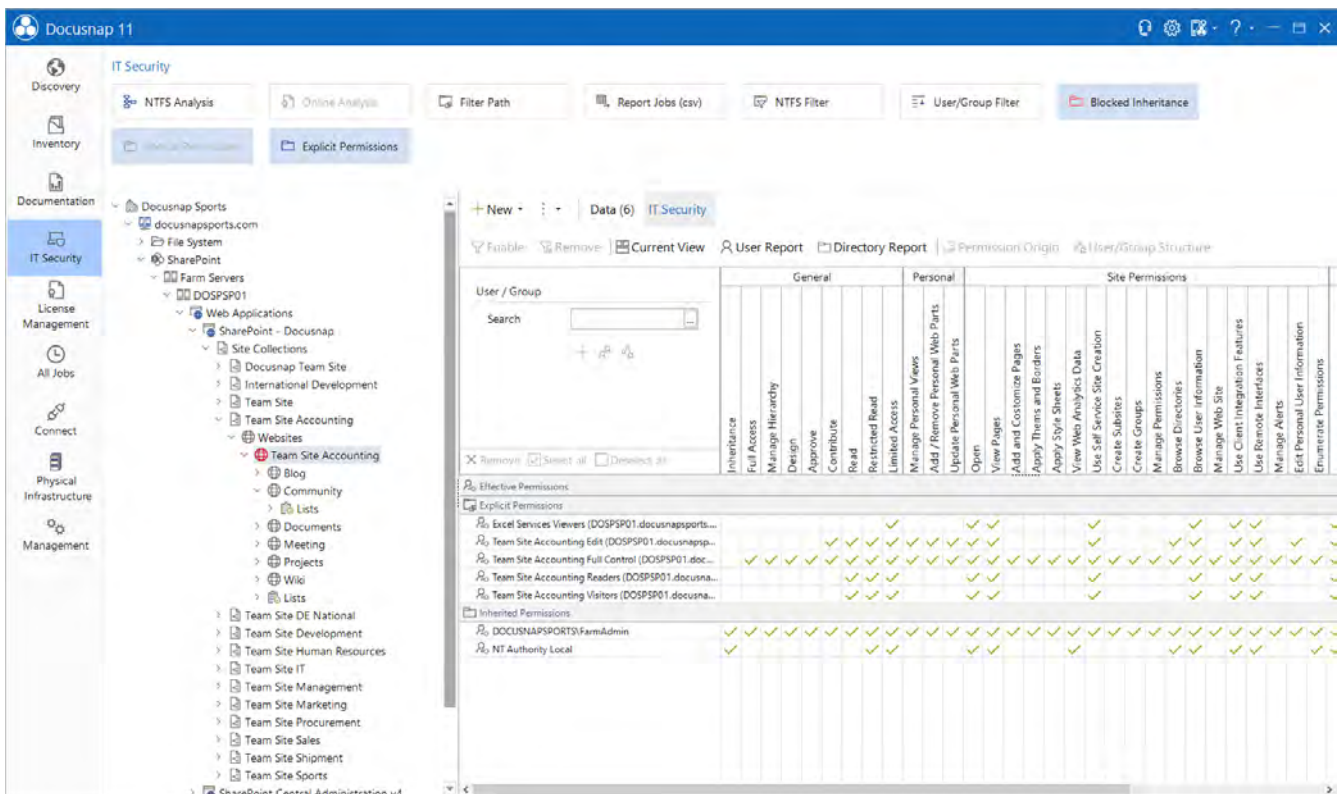
To be able to evaluate the permissions of your SharePoint environment, an inventory of the SharePoint is required first. The permissions are automatically part of the inventory.

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.



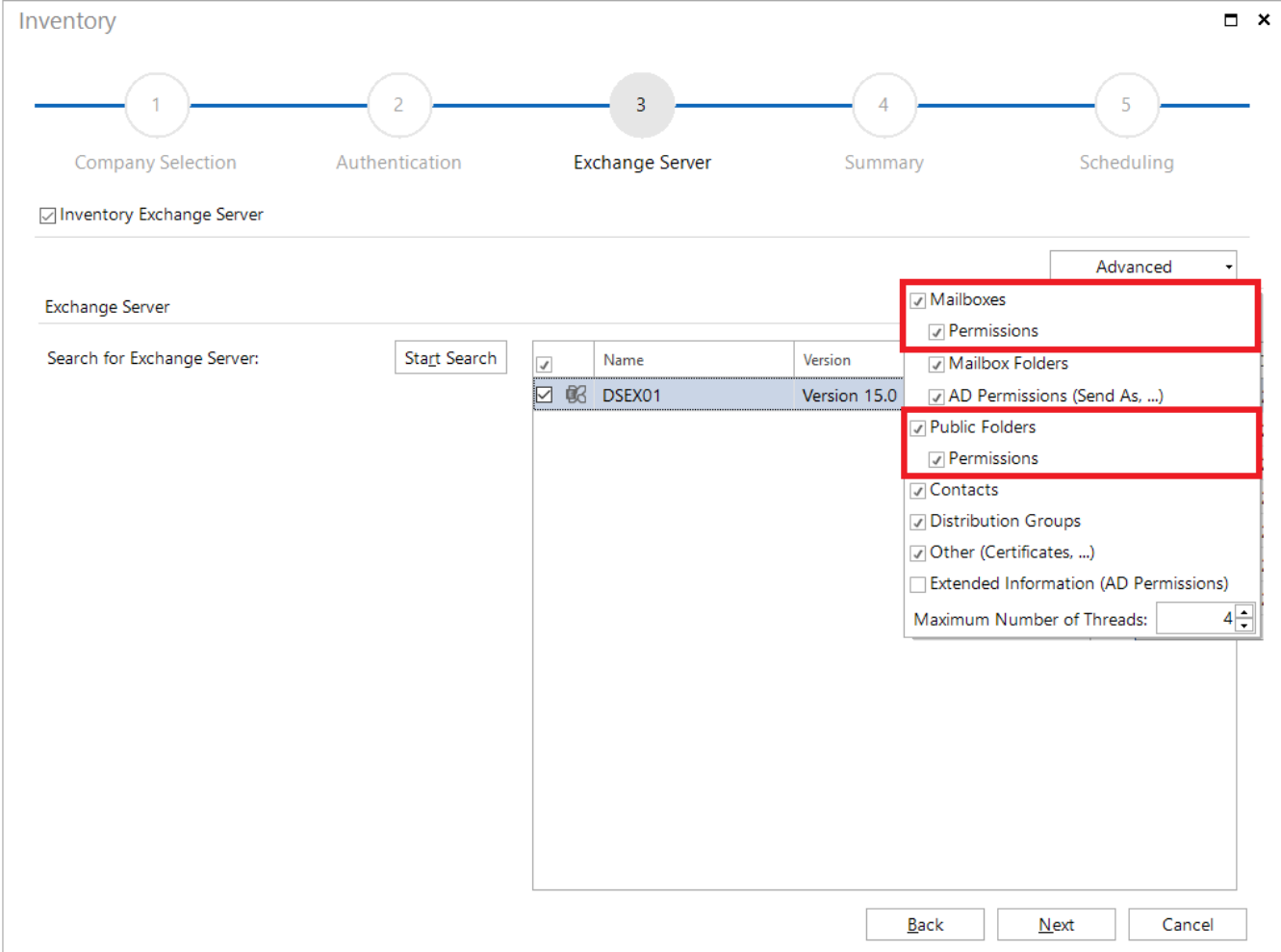
The screenshot displays the Docusnap 11 IT Security application. The left sidebar shows a navigation menu with categories like Discovery, Inventory, Documentation, IT Security (selected), License Management, All Jobs, Connect, Physical Infrastructure, and Management. The main window is titled 'IT Security' and contains a toolbar with buttons for NTFS Analysis, Online Analysis, Filter Path, Report Jobs (csv), NTFS Filter, User/Group Filter, and Blocked Inheritance. Below the toolbar, a tree structure on the left lists the SharePoint environment hierarchy, including 'Docusnap Sports', 'docusnapsports.com', 'File System', 'SharePoint', 'Farm Servers', 'DOSPPSP01', 'Web Applications', 'SharePoint - Docusnap', 'Site Collections', 'Docusnap Team Site', 'International Development', 'Team Site', 'Team Site Accounting', 'Websites', 'Team Site Accounting', 'Blog', 'Community', 'Lists', 'Documents', 'Meeting', 'Projects', 'Wiki', 'Team Site DE National', 'Team Site Development', 'Team Site Human Resources', 'Team Site IT', 'Team Site Management', 'Team Site Marketing', 'Team Site Procurement', 'Team Site Sales', 'Team Site Shipment', 'Team Site Sports', and 'SharePoint Central Administration.v4'. The main pane shows a 'Data (6) IT Security' view with a search bar and a table of permissions. The table has columns for 'User / Group', 'General', 'Personal', and 'Site Permissions'. The 'User / Group' column lists various users and groups, including 'Excel Services Viewers (DOSPPSP01.docusnapsports.com)', 'Team Site Accounting Edit (DOSPPSP01.docusnapsports.com)', 'Team Site Accounting Full Control (DOSPPSP01.docusnapsports.com)', 'Team Site Accounting Readers (DOSPPSP01.docusnapsports.com)', 'Team Site Accounting Visitors (DOSPPSP01.docusnapsports.com)', 'Docusnap Team Site FarmAdmin', and 'NT Authority Local'. The 'General' column lists permissions like 'Inheritance', 'Full Access', 'Manage Hierarchy', 'Design', 'Approve', 'Contribute', 'Read', 'Restricted Read', 'Limited Access', 'Manage Personal Views', 'Add / Remove Personal Web Parts', 'Update Personal Web Parts', 'Open', 'View Pages', 'Add and Customize Pages', 'Apply Themes and Borders', 'Apply Style Sheets', 'View Web Analytics Data', 'Use Self Service Site Creation', 'Create Subsites', 'Manage Groups', 'Manage Directories', 'Browse User Information', 'Manage Web Site', 'Use Client Integration Features', 'Use Remote Interfaces', 'Manage Alerts', 'Edit Personal User Information', and 'Enumerate Permissions'. The 'Personal' and 'Site Permissions' columns are currently empty. The table shows green checkmarks indicating that most users have full control over the site.

Figure 20 - SharePoint permission analysis

4. EXCHANGE

4.1 REQUIREMENT

To be able to evaluate Exchange permissions, you must first perform an inventory. The permissions must be part of the inventory. These can be enabled in the Exchange Scan Wizard - Step 3 - Advanced Options.



Inventory

1 Company Selection 2 Authentication 3 Exchange Server 4 Summary 5 Scheduling

☒ Inventory Exchange Server

Exchange Server

Search for Exchange Server:

<input checked="" type="checkbox"/>	Name	Version
<input checked="" type="checkbox"/>	DSEX01	Version 15.0

Advanced

- ☒ Mailboxes
- ☒ Permissions
- ☒ Mailbox Folders
- ☒ AD Permissions (Send As, ...)
- ☒ Public Folders
- ☒ Permissions
- ☒ Contacts
- ☒ Distribution Groups
- ☒ Other (Certificates, ...)
- ☐ Extended Information (AD Permissions)

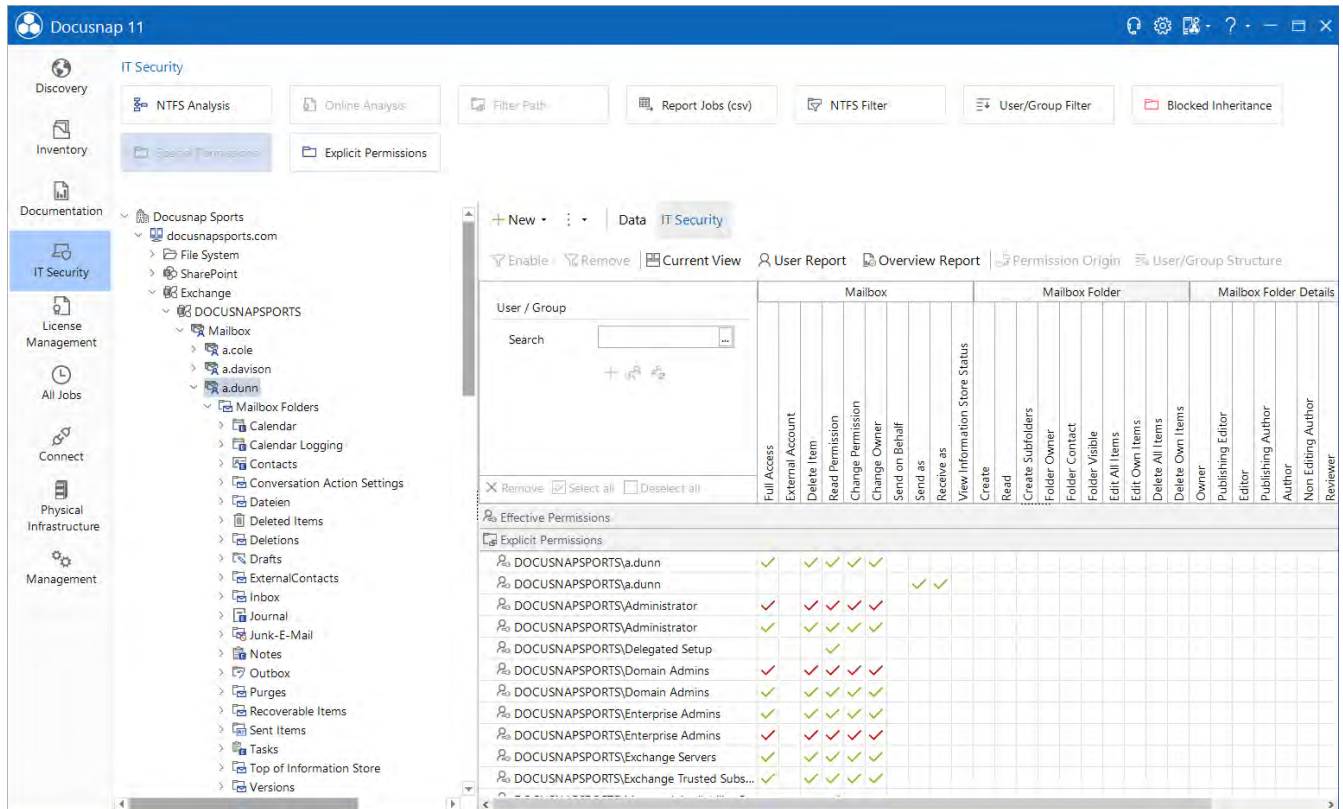
Maximum Number of Threads: 4

Figure 21 - 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.



The screenshot shows the Docusnap 11 IT Security interface. The left sidebar contains navigation options: Discovery, Inventory, Documentation, IT Security (selected), License Management, All Jobs, Connect, Physical Infrastructure, and Management. The main window displays a table of permissions for various users and groups across different Exchange components.

Table 1: Mailbox Permissions

User / Group	Full Access	External Account	Delete Item	Read Permission	Change Permission	Change Owner	Send on Behalf	Send as	Receive as	View Information Store Status
DOCUSNAPSPTS\j.dunn	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Administrator	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Delegated Setup	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Domain Admins	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Enterprise Admins	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Exchange Servers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Exchange Trusted Subs...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 2: Mailbox Folder Permissions

User / Group	Create Subfolders	Folder Owner	Folder Contact	Folder Visible	Edit All Items	Edit Own Items	Delete All Items	Delete Own Items	Owner	Publishing Editor	Publishing Author	Non-Editing Author	Reviewer
DOCUSNAPSPTS\j.dunn	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Administrator	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Delegated Setup	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Domain Admins	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Enterprise Admins	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Exchange Servers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DOCUSNAPSPTS\Exchange Trusted Subs...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 22 - 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 - ADJUST DEFAULT SETTINGS FOR THE DIRECTORY REPORT	16
FIGURE 9 - ADD USER	17
FIGURE 10 - USER REPORT OPTIONS	18
FIGURE 11 - SHARE REPORT OPTIONS.....	19
FIGURE 12 - SEND PERMISSION REPORTS BY E-MAIL	20
FIGURE 13 - SCHEDULE SHARE AND DIRECTORY REPORTS AS JOB	21
FIGURE 14 - CALL PERMISSION ORIGIN	22
FIGURE 15 - CHECK PERMISSION ORIGIN.....	23
FIGURE 16 - LIMIT FOLDER LEVELS.....	24
FIGURE 17 - CREATING NTFS FILTER.....	25
FIGURE 18 - ONLINE ANALYSIS	26
FIGURE 19 - USER GROUP FILTER	27
FIGURE 20 - SHAREPOINT PERMISSION ANALYSIS.....	28
FIGURE 21 - ADVANCED EXCHANGE INVENTORY OPTIONS	29
FIGURE 22 - EXCHANGE PERMISSION ANALYSIS	30

VERSION HISTORY

Date	Description
08/22/2019	Document created
06/01/2020	Revision of the HowTo for Docusnap 11
06/01/2022	Screenshot update
09/27/2022	Revision of Chapter 2.2 – NTFS Analysis
