Docusnap X – User Management

Managing User Access to Docusnap

TITLE	Docusnap X – User Management
AUTHOR	Docusnap Consulting
DATE	12/18/2018
VERSION	1.1 | valid from September 26, 2018

This document contains proprietary information. The reproduction and distribution of this document as a whole or in part as well as the utilization and disclosure of its contents to third parties without the express authorization by itelio GmbH are prohibited. Offenders will be held liable for the payment of indemnification. All rights reserved.

TABLE OF CONTENTS

1. Purpose of this Document

By default, every Docusnap user has unlimited access to the full functionality of the application.

The User Management feature in Docusnap, however, allows you to establish a granular permission assignment scheme by using a user roles concept.

Through this scheme, you can define which features and information can be accessed by which user.

This HowTo document describes the following use cases:

- 1st level support employees should only have reading access to the information available in Docusnap
  - Chapter 3.2
- The Client Management team should have no access to the server systems in Docusnap
  - Chapter 4
- Our apprentices should not see the passwords stored in Docusnap
  - Chapter 5
- Permission assignment in Docusnap should be documented
  - Chapter 8

2. Introduction

Depending on your requirements, the User Management structure can be very complex. The following section contains an introduction listing the most important aspects that are to be observed beforehand and provide more detailed information.

Why?

Why do you want / need to enable the User Management feature and restrict the access to Docusnap, certain features, or pieces of information?

What?

What is to be restricted?

- Restrict access to Docusnap
- Restrict access to certain features
- Restrict access to certain pieces of information

Who?

Which persons should have access to which features and information?

- Docusnap users

How?

How can you implement these restrictions?

- Docusnap Roles
- Permission Categories

2.1 Important Terms

Docusnap users

Add users or ADS groups (recommended) to the Docusnap User Management. Create corresponding ADS groups and add them to the Docusnap User Management. Examples:

- Docusnap_Admins
- Docusnap_View_Only
- Docusnap_Documentation

Docusnap Roles

Roles are assigned to the groups previously added to User Management. These roles define the access rights to features and information within Docusnap. By default, ten predefined roles are available. For a description of the predefined roles and their functionality, refer to our User Manual.

Refer to chapter 7 to learn how to add and manage roles.

Permission Categories

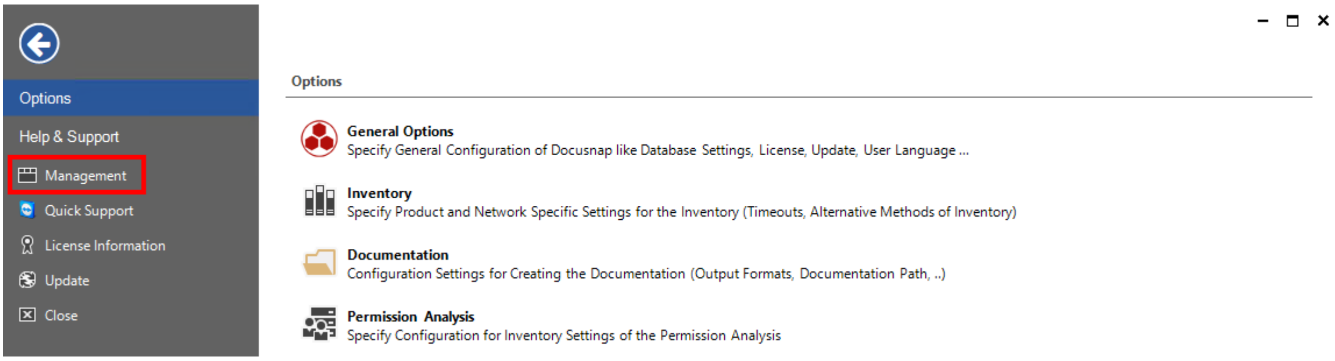
Permission categories help you restrict the access to additional information (passwords, contracts, comments, etc.) in Docusnap. Permission categories are linked to roles. This way, you can use the Docusnap roles also to control the access to additional information.

To begin, please read the HowTo document which provides a detailed description of additional information in Docusnap.

3. User Management in Docusnap

3.1 Docusnap Roles

Roles define the access rights to features and information in Docusnap. To find the predefined roles, go to Docusnap > Management – General tab – Docusnap Roles.



Options

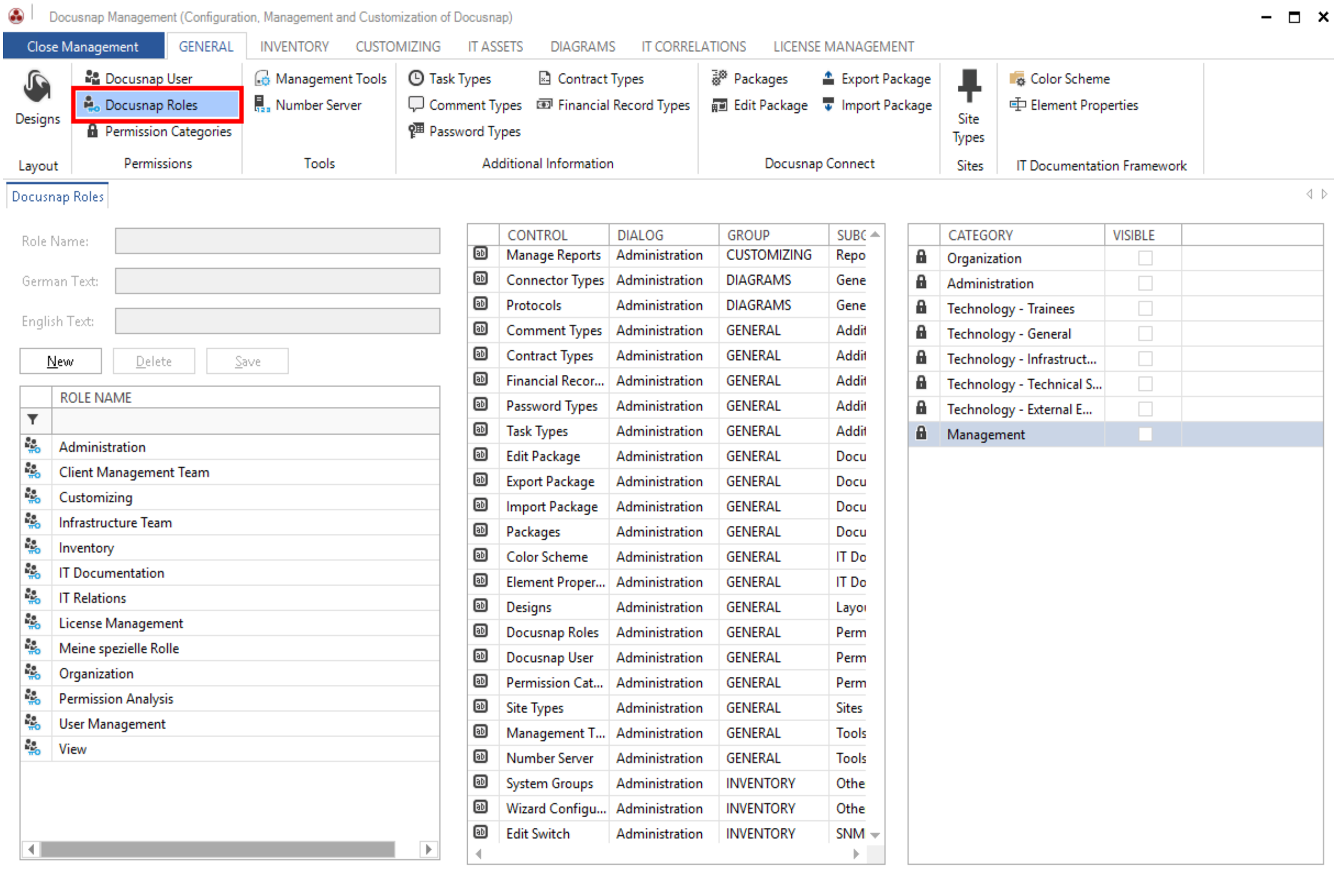
General Options
Specify General Configuration of Docusnap like Database Settings, License, Update, User Language ...

Inventory
Specify Product and Network Specific Settings for the Inventory (Timeouts, Alternative Methods of Inventory)

Documentation
Configuration Settings for Creating the Documentation (Output Formats, Documentation Path, ..)

Permission Analysis
Specify Configuration for Inventory Settings of the Permission Analysis

Fig. 1 – Accessing Docusnap Management



Role Name:

German Text:

English Text:

New | Delete | Save

ROLE NAME
Administration
Client Management Team
Customizing
Infrastructure Team
Inventory
IT Documentation
IT Relations
License Management
Meine spezielle Rolle
Organization
Permission Analysis
User Management
View

CONTROL	DIALOG	GROUP	SUBC
Manage Reports	Administration	CUSTOMIZING	Repo
Connector Types	Administration	DIAGRAMS	Gene
Protocols	Administration	DIAGRAMS	Gene
Comment Types	Administration	GENERAL	Addi
Contract Types	Administration	GENERAL	Addi
Financial Recor...	Administration	GENERAL	Addi
Password Types	Administration	GENERAL	Addi
Task Types	Administration	GENERAL	Addi
Edit Package	Administration	GENERAL	Docu
Export Package	Administration	GENERAL	Docu
Import Package	Administration	GENERAL	Docu
Packages	Administration	GENERAL	Docu
Color Scheme	Administration	GENERAL	IT Do
Element Proper...	Administration	GENERAL	IT Do
Designs	Administration	GENERAL	Layou
Docusnap Roles	Administration	GENERAL	Perm
Docusnap User	Administration	GENERAL	Perm
Permission Cat...	Administration	GENERAL	Perm
Site Types	Administration	GENERAL	Sites
Management T...	Administration	GENERAL	Tools
Number Server	Administration	GENERAL	Tools
System Groups	Administration	INVENTORY	Othe
Wizard Configu...	Administration	INVENTORY	Othe
Edit Switch	Administration	INVENTORY	SNM

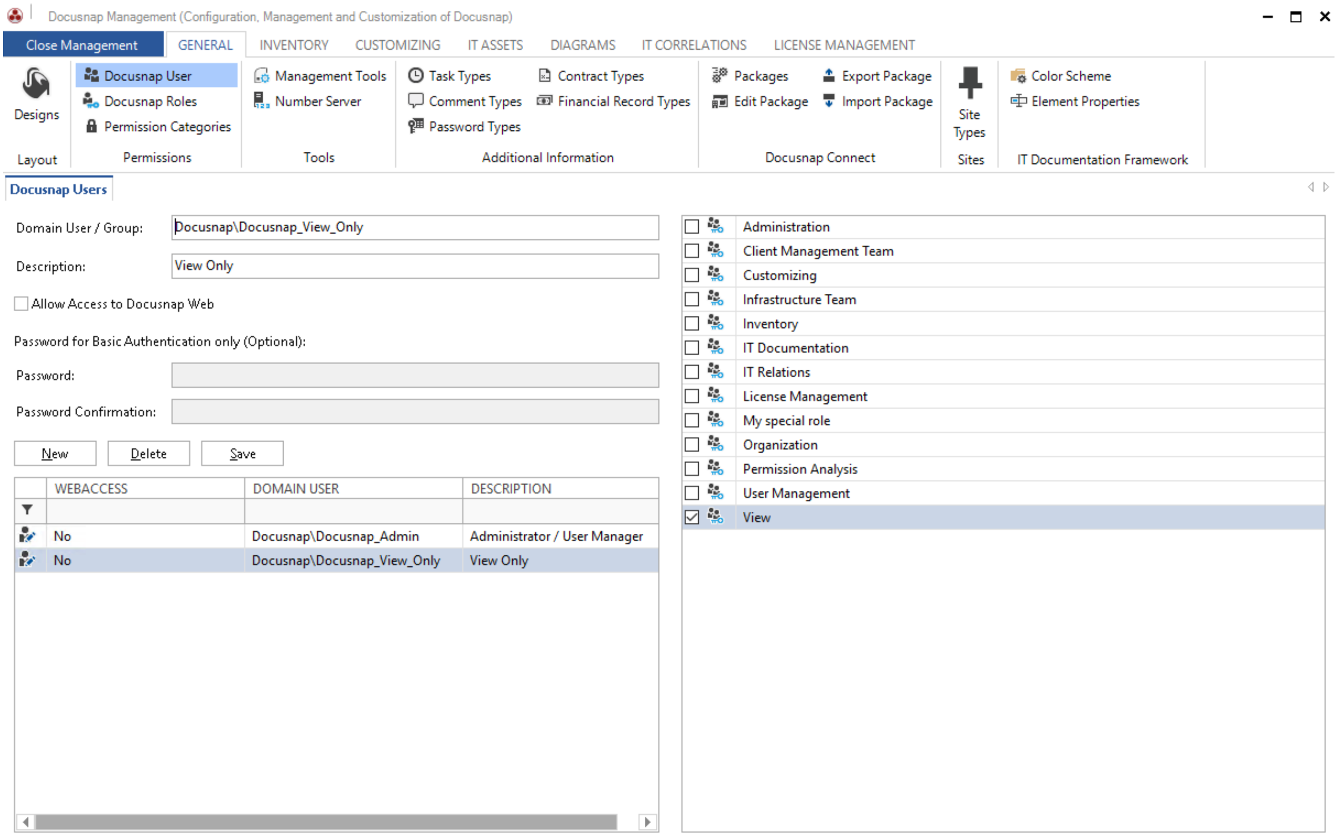
CATEGORY	VISIBLE
Organization	□
Administration	□
Technology - Trainees	□
Technology - General	□
Technology - Infrastruct...	□
Technology - Technical S...	□
Technology - External E...	□
Management	□

Fig. 2 – Docusnap Roles

3.2 Docusnap Users

In the **Docusnap Users** area, you can add users and groups (local and ADS groups) to the Docusnap User Management. As a best practice, we recommend that you use custom (user-defined) ADS groups. These ADS groups allow you to manage the access to features and information in Docusnap.

After having added a group, you can assign a role to this group. The assigned role defines the features and information accessible to the group members.



Domain User / Group: Docusnap\Docusnap_View_Only

Description: View Only

☐ Allow Access to Docusnap Web

Password for Basic Authentication only (Optional):

Password:

Password Confirmation:

WEBACCESS	DOMAIN USER	DESCRIPTION
No	Docusnap\Docusnap_Admin	Administrator / User Manager
No	Docusnap\Docusnap_View_Only	View Only

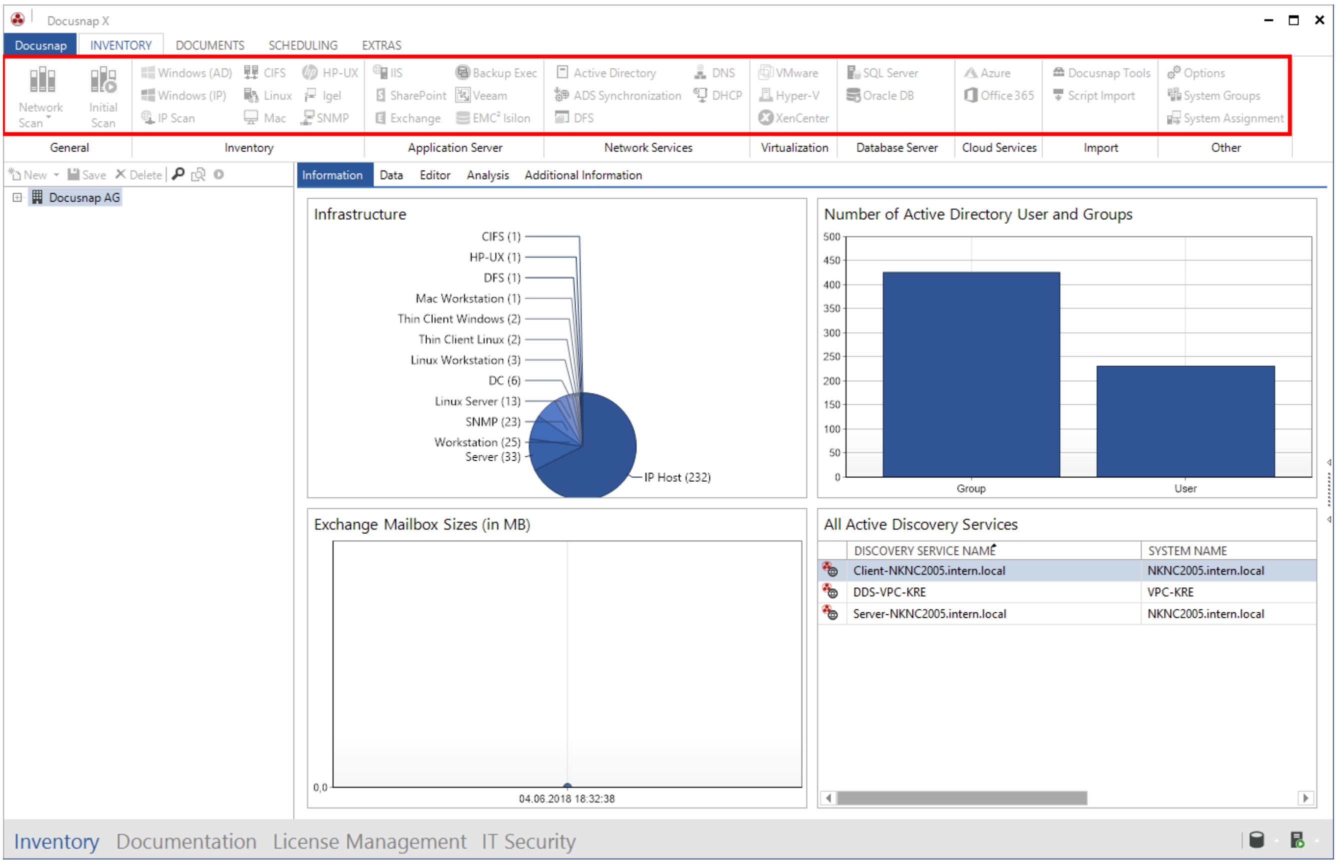
☐ Administration
☐ Client Management Team
☐ Customizing
☐ Infrastructure Team
☐ Inventory
☐ IT Documentation
☐ IT Relations
☐ License Management
☐ My special role
☐ Organization
☐ Permission Analysis
☐ User Management
☑ View

Fig. 3 – Docusnap Users

To add an ADS group to User Management, click the **New** button. Docusnap initially suggests to add the current user – with administrator rights. You can confirm this prompt or instead add your Docusnap_Admin group to User Management. It is important that there is at least one user who has administrator rights (Administration + User Management) in Docusnap. If you do not specify a user who has administrator rights in Docusnap, the application can no longer be managed.

Adding a user group enables User Management in Docusnap. This means that only persons who are known to User Management can open Docusnap.

To implement the application example mentioned before – **1st level support employees should only have reading access to the information available in Docusnap** – you need an ADS group with the desired members. Add this group in User Management and select the **View** role – see Fig. 3.

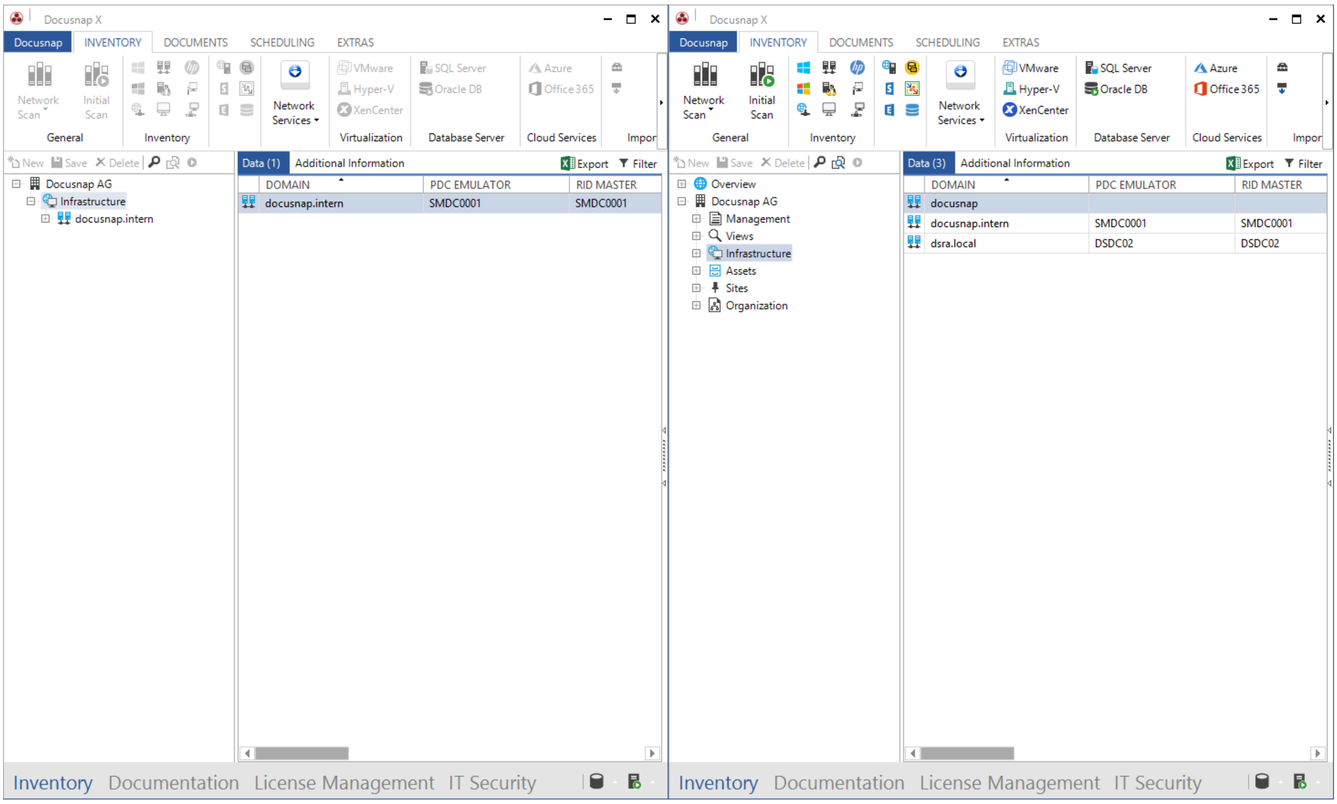


DISCOVERY SERVICE NAME	SYSTEM NAME
Client-NKNC2005.intern.local	NKNC2005.intern.local
DDS-VPC-KRE	VPC-KRE
Server-NKNC2005.intern.local	NKNC2005.intern.local

Fig. 4 – View role – Restricted access to features

4. Restricting Access to Types and Objects in the Data Explorer

By restricting the access to types and objects, you can achieve that not all information can be accessed by everybody. Example: who may access server information?



Docusnap AG
Infrastructure
docusnap.intern

Data (1)

DOMAIN	PDC EMULATOR	RID MASTER
docusnap.intern	SMDC0001	SMDC0001

Overview
Docusnap AG
Management
Views
Infrastructure
Assets
Sites
Organization

Data (3)

DOMAIN	PDC EMULATOR	RID MASTER
docusnap		
docusnap.intern	SMDC0001	SMDC0001
dsra.local	DSDC02	DSDC02

Fig. 5 – Restricted view of objects in the Data Explorer

To define the access to types and objects, proceed as described below. This section covers the following use case: The Client Management team should have no access to the server systems in Docusnap.

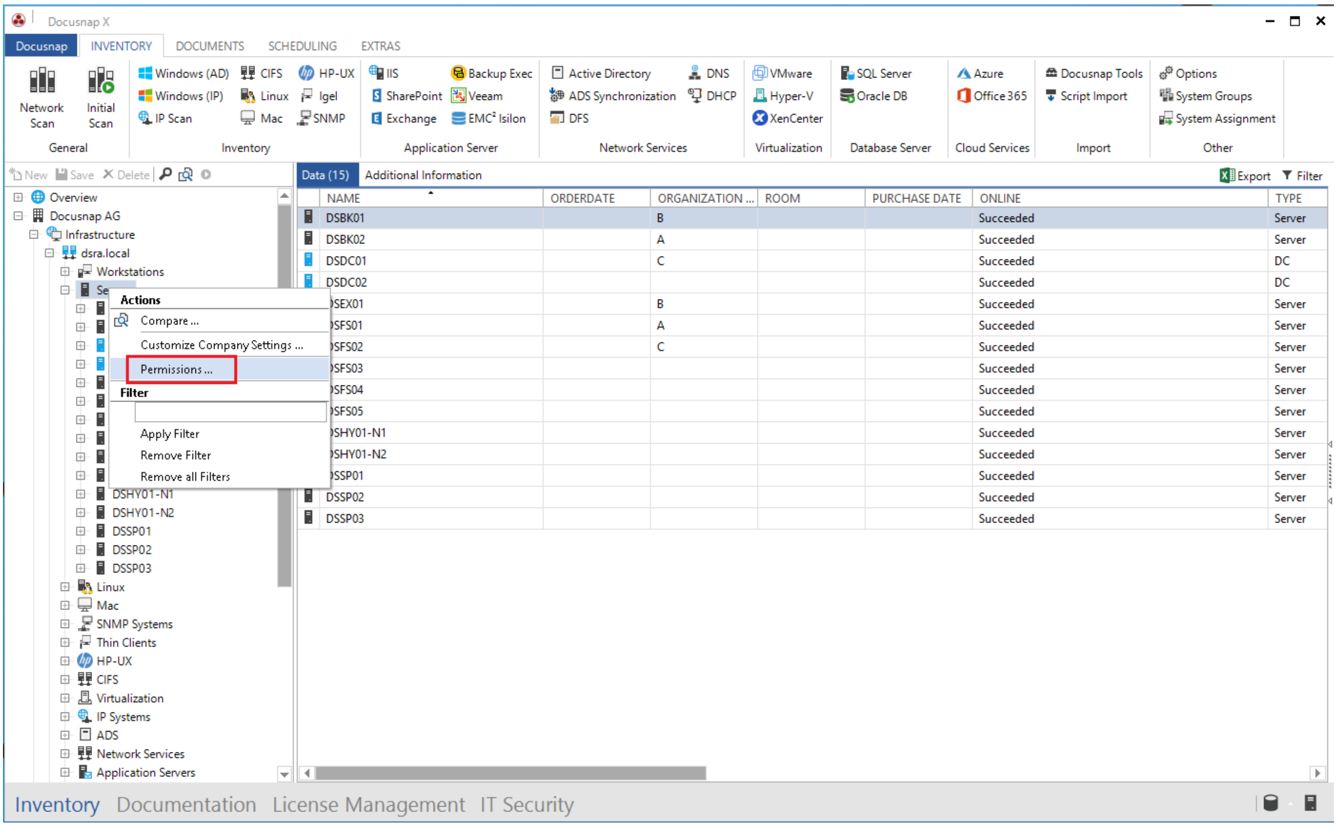
To implement this use case, at least two ADS groups must have been added to User Management and corresponding roles must have been assigned to them. Example:

- Docusnap_Admins – Administration role
- Docusnap_Client_Management – Organization role

Go to the Docusnap main screen and highlight Servers in the Data Explorer. Right-click and select *Permissions*.

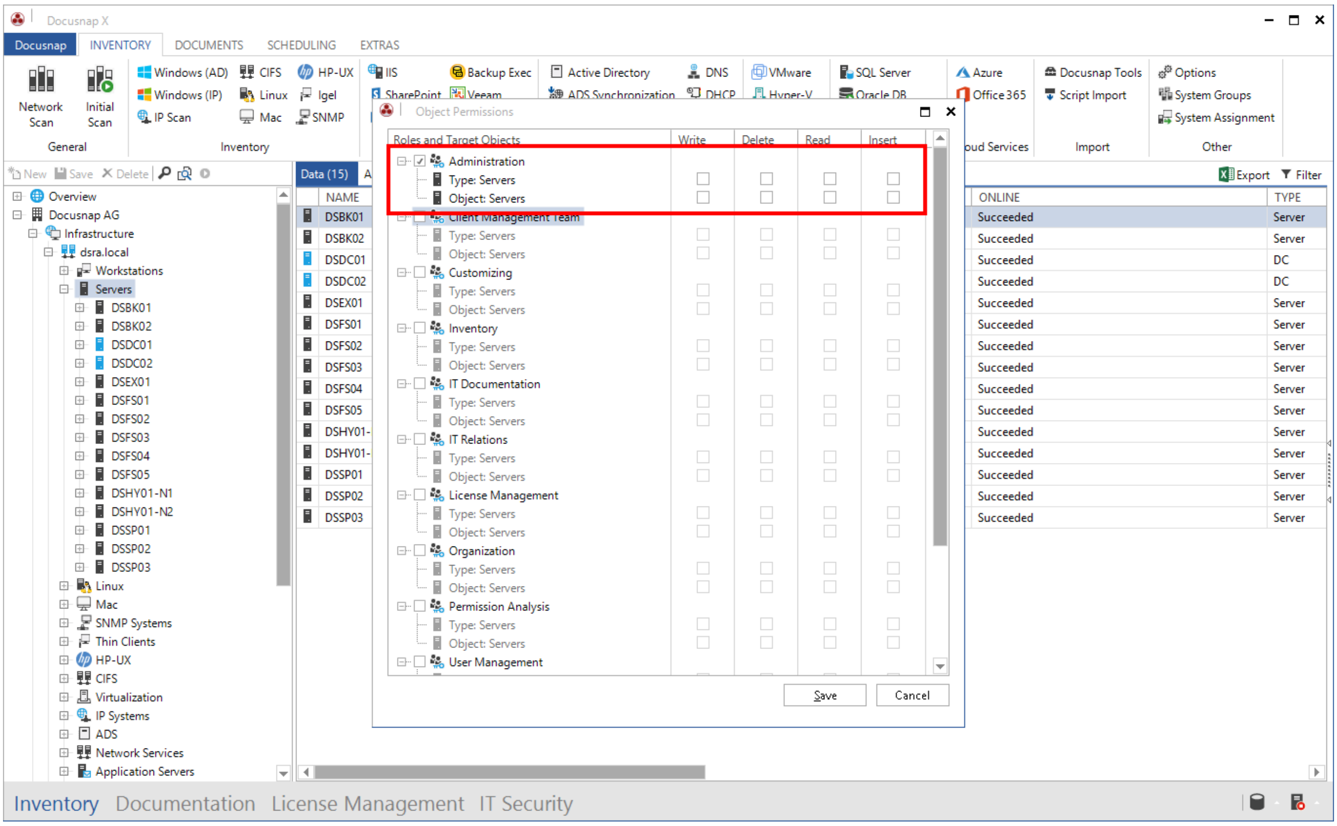
The **Object Permissions** windows opens (Fig. 7), listing all available Docusnap roles. Now, select the role(s) you need. The member of the selected role(s) will continue to see the Servers type or object in the tree structure of Docusnap.

The members of the roles you do not select in this dialog, will no longer see the Servers type or object.



NAME	ORDERDATE	ORGANIZATION ...	ROOM	PURCHASE DATE	ONLINE	TYPE
DSBK01		B			Succeeded	Server
DSBK02		A			Succeeded	Server
DSDC01		C			Succeeded	DC
DSDC02					Succeeded	DC
DSEX01		B			Succeeded	Server
DSFS01		A			Succeeded	Server
DSFS02		C			Succeeded	Server
DSFS03					Succeeded	Server
DSFS04					Succeeded	Server
DSFS05					Succeeded	Server
DSHY01-N1					Succeeded	Server
DSHY01-N2					Succeeded	Server
DSSP01					Succeeded	Server
DSSP02					Succeeded	Server
DSSP03					Succeeded	Server

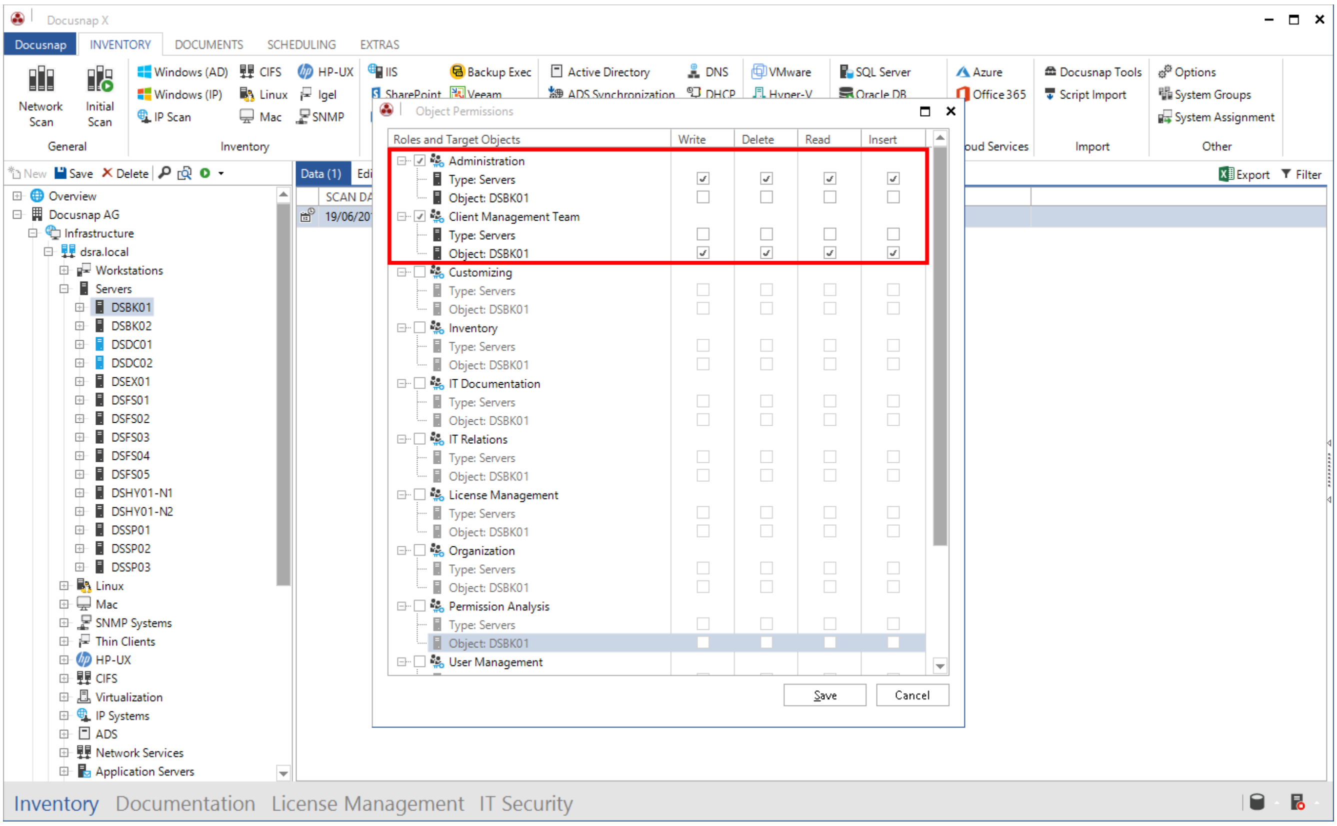
Fig. 6 – Opening the Object Permissions dialog



Roles and Target Objects	Write	Delete	Read	Insert
☑ Administration				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Client Management Team				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Customizing				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Inventory				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ IT Documentation				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ IT Relations				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ License Management				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Organization				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Permission Analysis				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ User Management				

Fig. 7 – Setting permissions

4.1 What is the Difference between Type and Object?



Object Permissions

Roles and Target Objects	Write	Delete	Read	Insert
☑ Administration				
Type: Servers	☑	☑	☑	☑
Object: DSBK01	☐	☐	☐	☐
☑ Client Management Team				
Type: Servers	☐	☐	☐	☐
Object: DSBK01	☑	☑	☑	☑
☐ Customizing				
Type: Servers	☐	☐	☐	☐
Object: DSBK01	☐	☐	☐	☐
☐ Inventory				
Type: Servers	☐	☐	☐	☐
Object: DSBK01	☐	☐	☐	☐
☐ IT Documentation				
Type: Servers	☐	☐	☐	☐
Object: DSBK01	☐	☐	☐	☐
☐ IT Relations				
Type: Servers	☐	☐	☐	☐
Object: DSBK01	☐	☐	☐	☐
☐ License Management				
Type: Servers	☐	☐	☐	☐
Object: DSBK01	☐	☐	☐	☐
☐ Organization				
Type: Servers	☐	☐	☐	☐
Object: DSBK01	☐	☐	☐	☐
☐ Permission Analysis				
Type: Servers	☐	☐	☐	☐
Object: DSBK01	☐	☐	☐	☐
☐ User Management				

Fig. 8 – Object Permissions – Type vs. Object

In the Object Permissions dialog, you have the choice between two options: Type and Object.

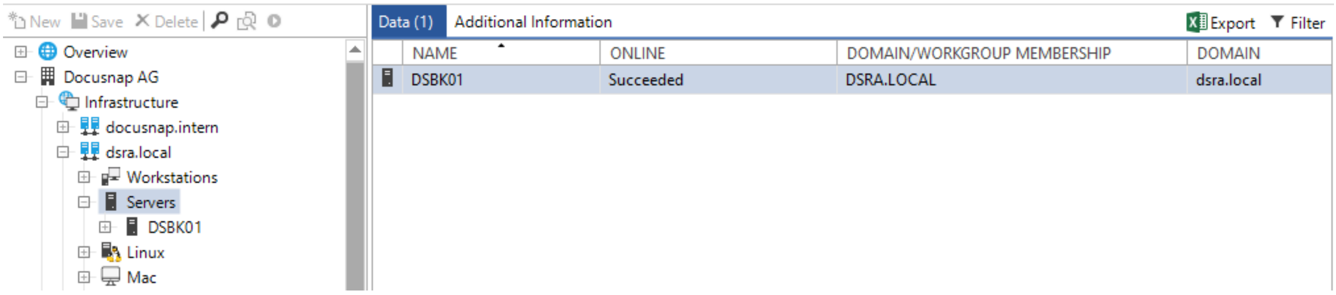
The Object Permissions dialog shown in Fig. 8 was opened through a server object, here DSBK01:

Type: Servers

Type represents all server objects within Docusnap. Now, select the Administration role and enable all checkboxes for Type: Servers. Members of this role will continue to see the Server objects within the tree structure.

Object: DSBK01

This object represents the explicitly selected DSBK01 Server object. Now, select a role and enable the checkboxes for Object: DSBK01. Members of this role will only see the DSBK01 server object within the Data Explorer.



NAME	ONLINE	DOMAIN/WORKGROUP MEMBERSHIP	DOMAIN
DSBK01	Succeeded	DSRA.LOCAL	dsra.local

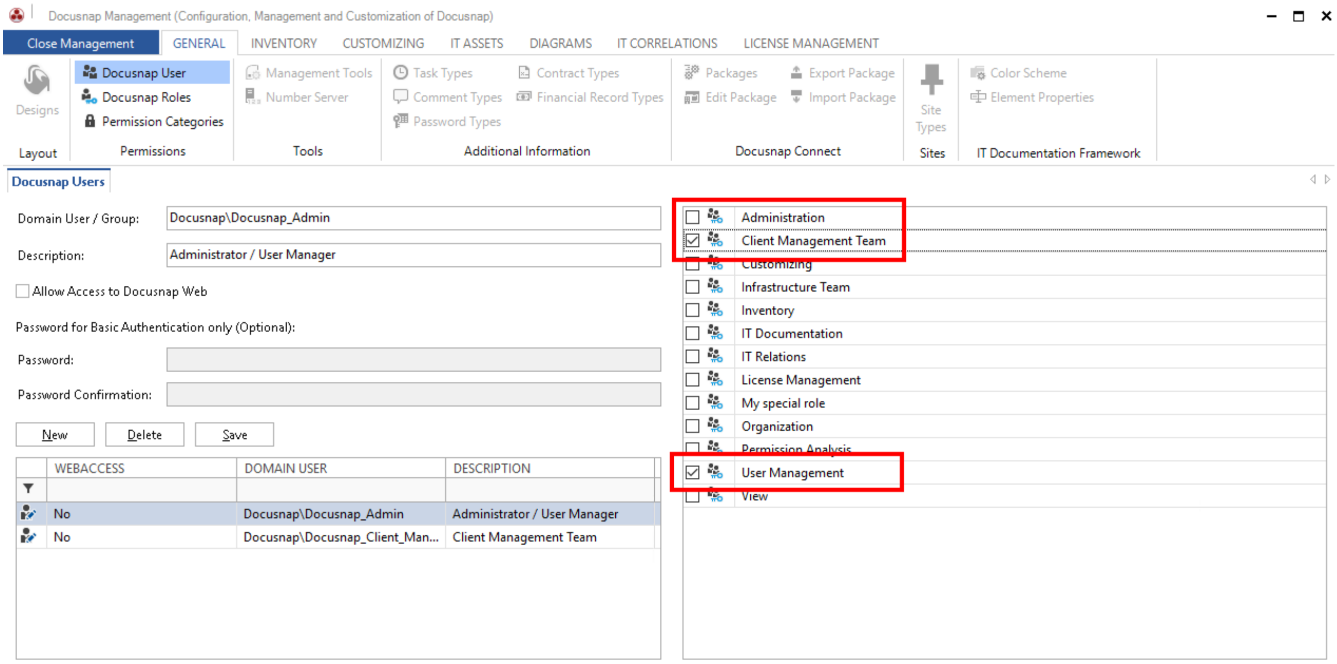
Fig. 9 – Setting object permissions – restricted access to information

4.2 Best Practice for Setting Permissions to Types and Objects

Setting up restrictions for information may require some effort and be hard to check. For this reason, we recommend the procedure presented below to set up permissions to information. With this procedure, you can directly check the permissions specified without the need to start Docusnap as a different user.

Start Docusnap and assign the following to the user or to the user's group: the **User Management** role and in addition the role whose access you want to restrict. You also need to de-select the Administration role for this user or group because an administrator is always permitted to see everything in Docusnap (cf. chapter 6).

- See chapter 7 to learn how to add and manage roles.



Domain User / Group: Docusnap\Docusnap_Admin

Description: Administrator / User Manager

☐ Allow Access to Docusnap Web

Password for Basic Authentication only (Optional):

Password:

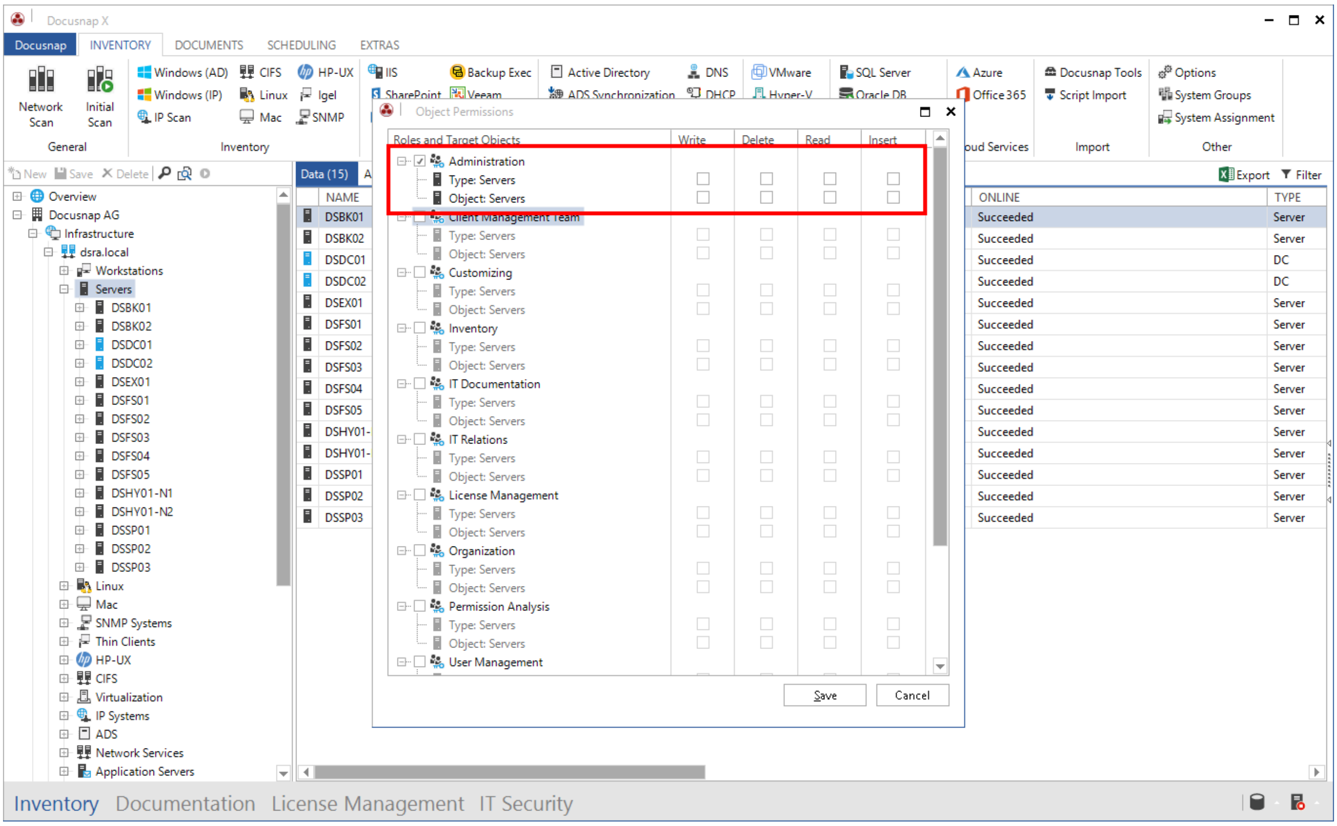
Password Confirmation:

WEBACCESS	DOMAIN USER	DESCRIPTION
No	Docusnap\Docusnap_Admin	Administrator / User Manager
No	Docusnap\Docusnap_Client_Man...	Client Management Team

☐ Administration
☑ Client Management Team
☐ Customizing
☐ Infrastructure Team
☐ Inventory
☐ IT Documentation
☐ IT Relations
☐ License Management
☐ My special role
☐ Organization
☐ Permission Analysis
☑ User Management
☐ View

Fig. 10 – Assigning roles

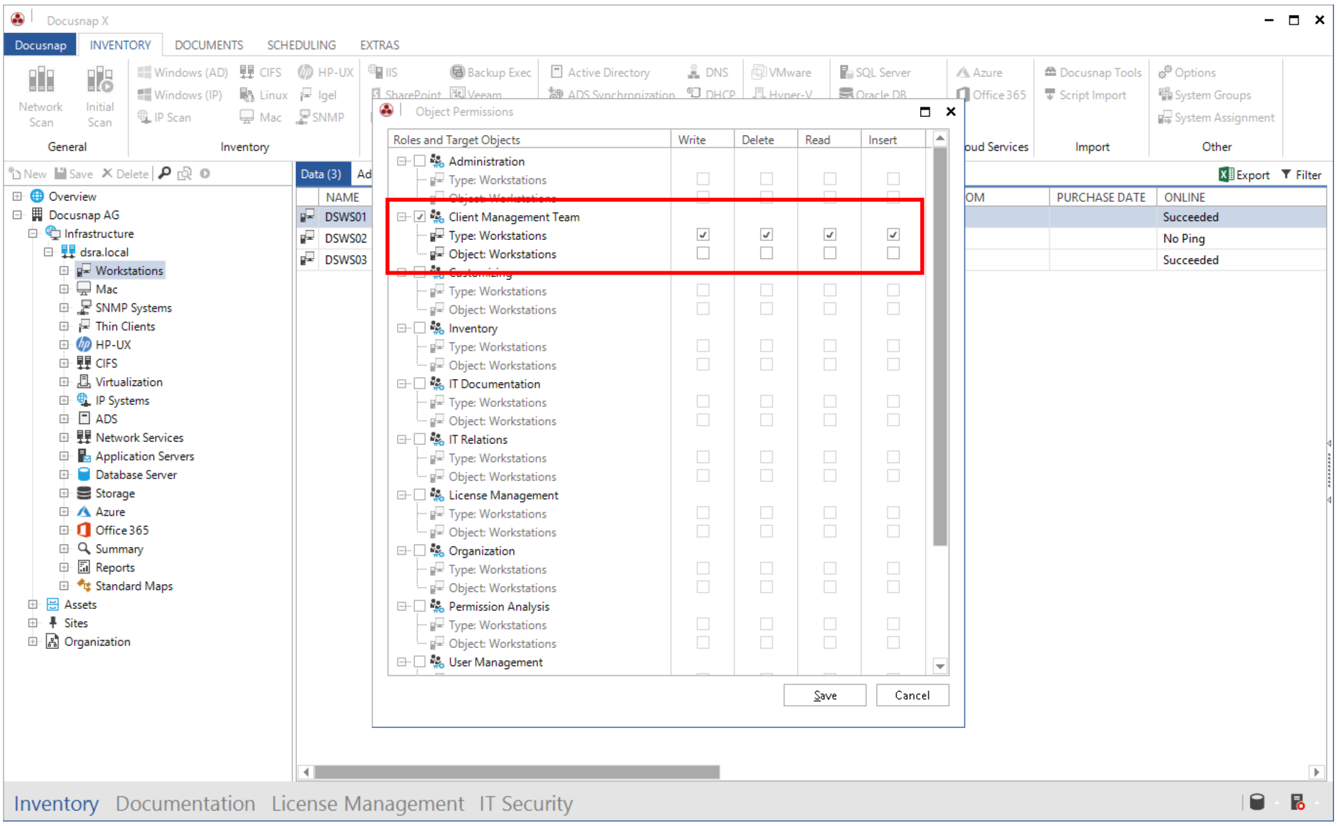
Go to the Docusnap main screen. While you are changing from the Management area to the main screen, the role change becomes effective. Now, make the desired changes in the main screen.



Roles and Target Objects	Write	Delete	Read	Insert
☑ Administration				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Client Management Team				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Customizing				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Inventory				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ IT Documentation				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ IT Relations				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ License Management				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Organization				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Permission Analysis				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ User Management				

NAME	ONLINE	TYPE
DSBK01	Succeeded	Server
DSBK02	Succeeded	Server
DSDC01	Succeeded	DC
DSDC02	Succeeded	DC
DSEX01	Succeeded	Server
DSFS01	Succeeded	Server
DSFS02	Succeeded	Server
DSFS03	Succeeded	Server
DSFS04	Succeeded	Server
DSFS05	Succeeded	Server
DSHY01-	Succeeded	Server
DSHY01-	Succeeded	Server
DSSP01	Succeeded	Server
DSSP02	Succeeded	Server
DSSP03	Succeeded	Server

Fig. 11 – Setting permissions to Servers



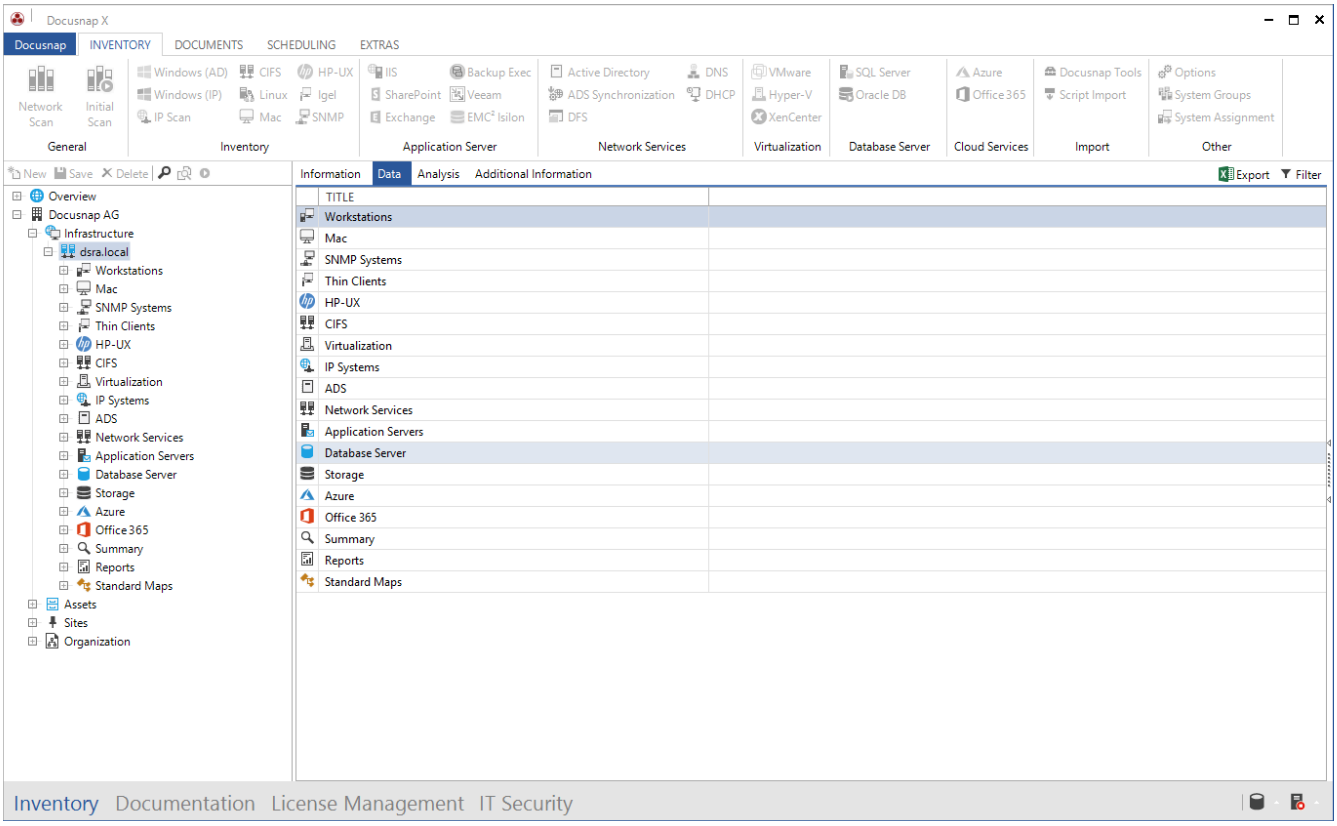
Roles and Target Objects	Write	Delete	Read	Insert
□ Administration				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
☑ Client Management Team				
Type: Workstations	☑	☑	☑	☑
Object: Workstations	□	□	□	□
□ Customizing				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ Inventory				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ IT Documentation				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ IT Relations				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ License Management				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ Organization				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ Permission Analysis				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ User Management				

NAME	PURCHASE DATE	ONLINE
DSWS01		Succeeded
DSWS02		No Ping
DSWS03		Succeeded

Fig. 12 – Setting permissions to Workstations

Once you have closed the Object Permissions dialog, the changes become effective. This way, you can check whether the changes have been made as desired.

After you have mad all desired changes, assign the Docusnap role(s) to the user or the corresponding ADS group again. Afterwards, you have access to the usual features again.



TITLE
Workstations
Mac
SNMP Systems
Thin Clients
HP-UX
CIFS
Virtualization
IP Systems
ADS
Network Services
Application Servers
Database Server
Storage
Azure
Office 365
Summary
Reports
Standard Maps

Fig. 13 – Checking the specified permissions

5. Permission Categories

Permission categories help you restrict the access to data that is stored in Docusnap as additional information (passwords, contracts, comments, etc.). Permission categories are assigned to Docusnap roles. When creating additional information, you select a corresponding category. This ensures that additional information can only be viewed by particular persons.

To begin, please read the following HowTo document which provides a detailed description of additional information in Docusnap: Additional information.

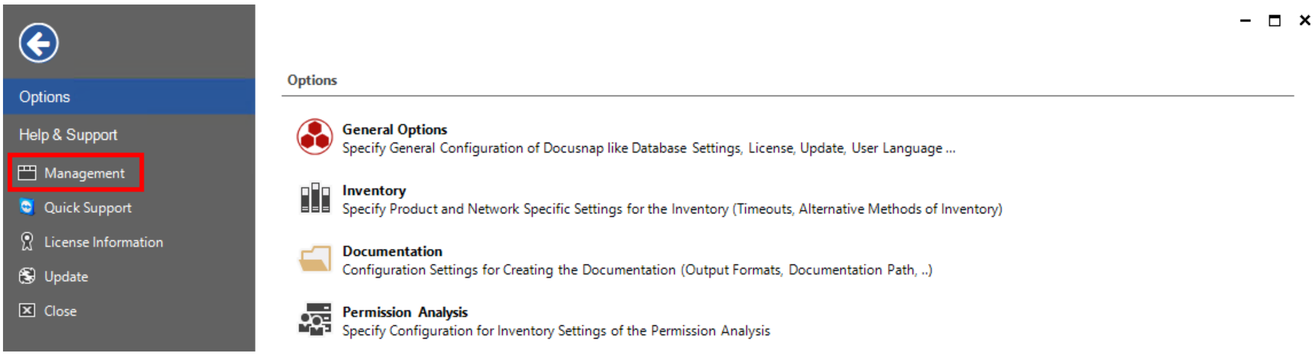
The following shows a possible application example:

- Our apprentices should not see the passwords stored in Docusnap

5.1 Managing Permission Categories

To find permission categories, go to Docusnap > Management – General tab – Permission Categories.

To create more permission categories, click the New button. The newly created permission categories will be available for the creation of additional information.



Options

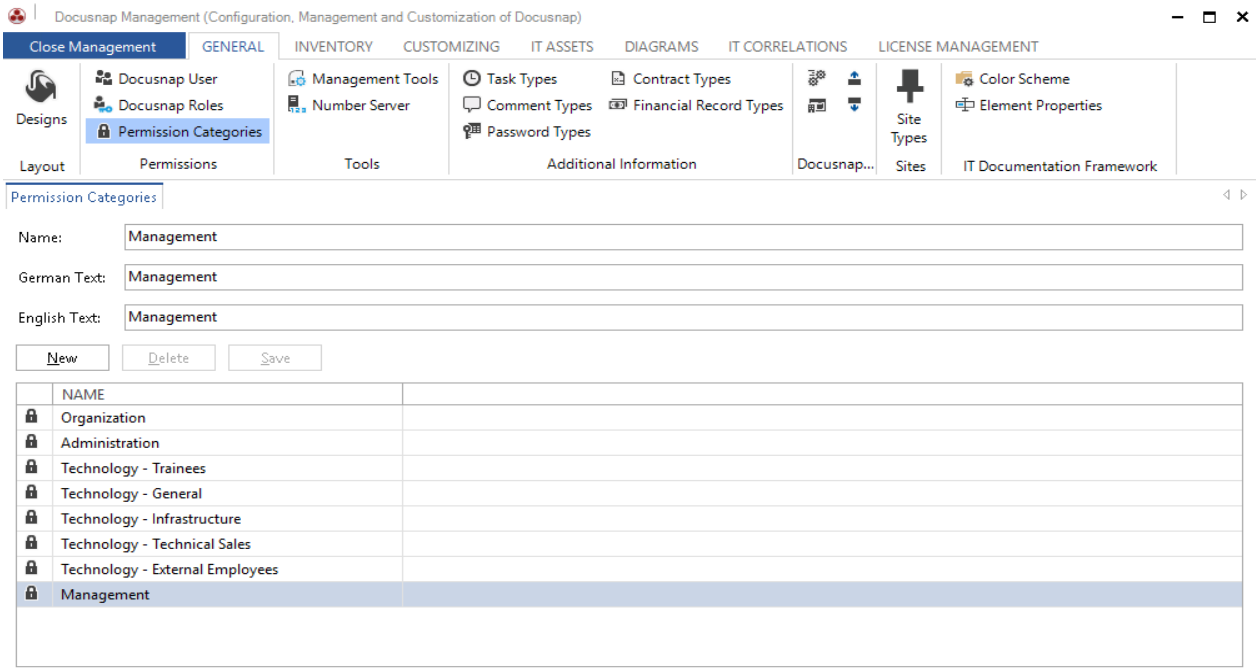
General Options
Specify General Configuration of Docusnap like Database Settings, License, Update, User Language ...

Inventory
Specify Product and Network Specific Settings for the Inventory (Timeouts, Alternative Methods of Inventory)

Documentation
Configuration Settings for Creating the Documentation (Output Formats, Documentation Path, ..)

Permission Analysis
Specify Configuration for Inventory Settings of the Permission Analysis

Fig. 14 – Accessing Docusnap Management



Name: Management

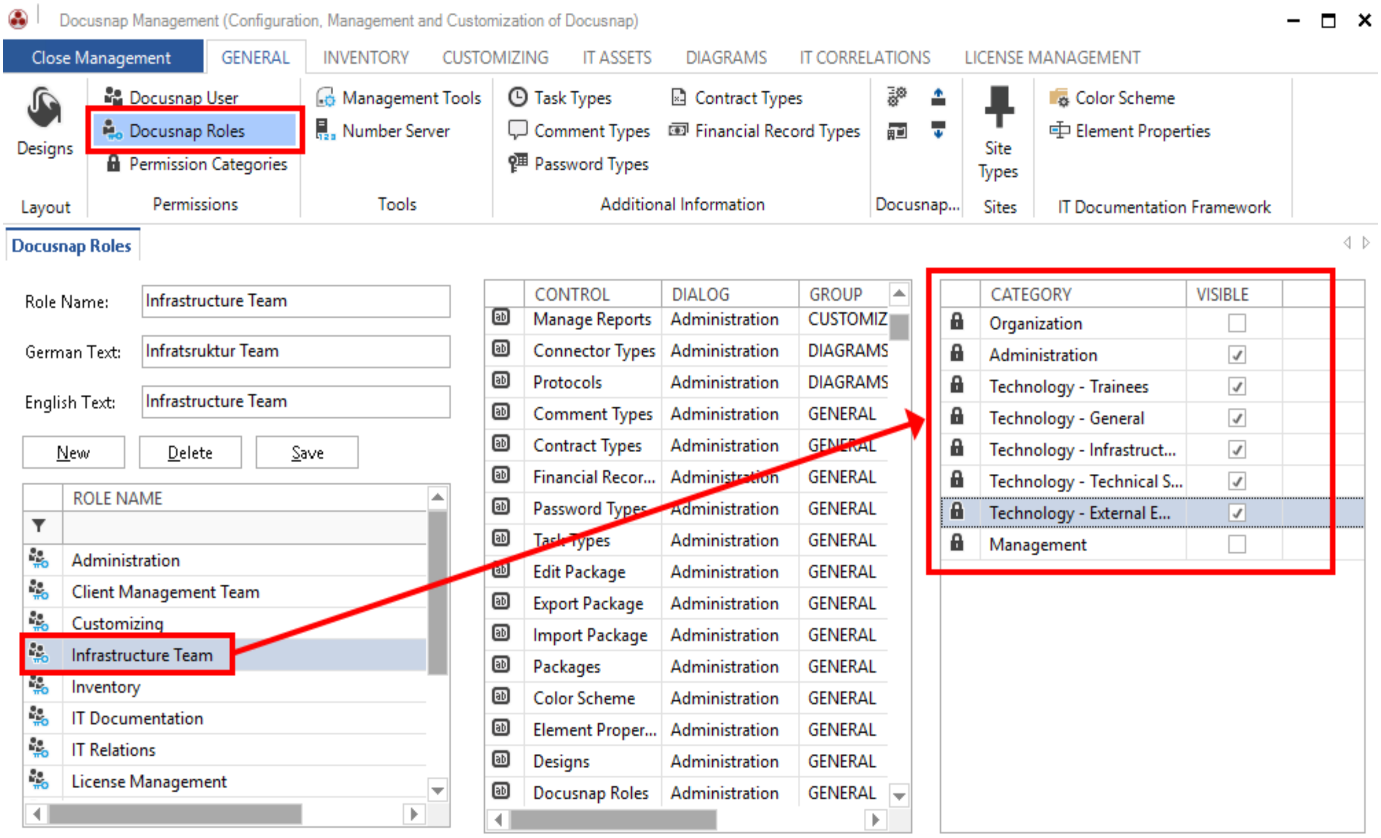
German Text: Management

English Text: Management

NAME
Organization
Administration
Technology - Trainees
Technology - General
Technology - Infrastructure
Technology - Technical Sales
Technology - External Employees
Management

Fig. 15 – Permission Categories

In order to be able to use permission categories, you must assign them to the desired Docusnap roles. This assignment is made in the Docusnap Roles area.



Role Name: Infrastructure Team

German Text: Infratsruktur Team

English Text: Infrastructure Team

ROLE NAME
Administration
Client Management Team
Customizing
Infrastructure Team
Inventory
IT Documentation
IT Relations
License Management

CONTROL	DIALOG	GROUP
Manage Reports	Administration	CUSTOMIZ
Connector Types	Administration	DIAGRAMS
Protocols	Administration	DIAGRAMS
Comment Types	Administration	GENERAL
Contract Types	Administration	GENERAL
Financial Recor...	Administration	GENERAL
Password Types	Administration	GENERAL
Task Types	Administration	GENERAL
Edit Package	Administration	GENERAL
Export Package	Administration	GENERAL
Import Package	Administration	GENERAL
Packages	Administration	GENERAL
Color Scheme	Administration	GENERAL
Element Proper...	Administration	GENERAL
Designs	Administration	GENERAL
Docusnap Roles	Administration	GENERAL

CATEGORY	VISIBLE
Organization	□
Administration	☑
Technology - Trainees	☑
Technology - General	☑
Technology - Infrastruct...	☑
Technology - Technical S...	☑
Technology - External E...	☑
Management	□

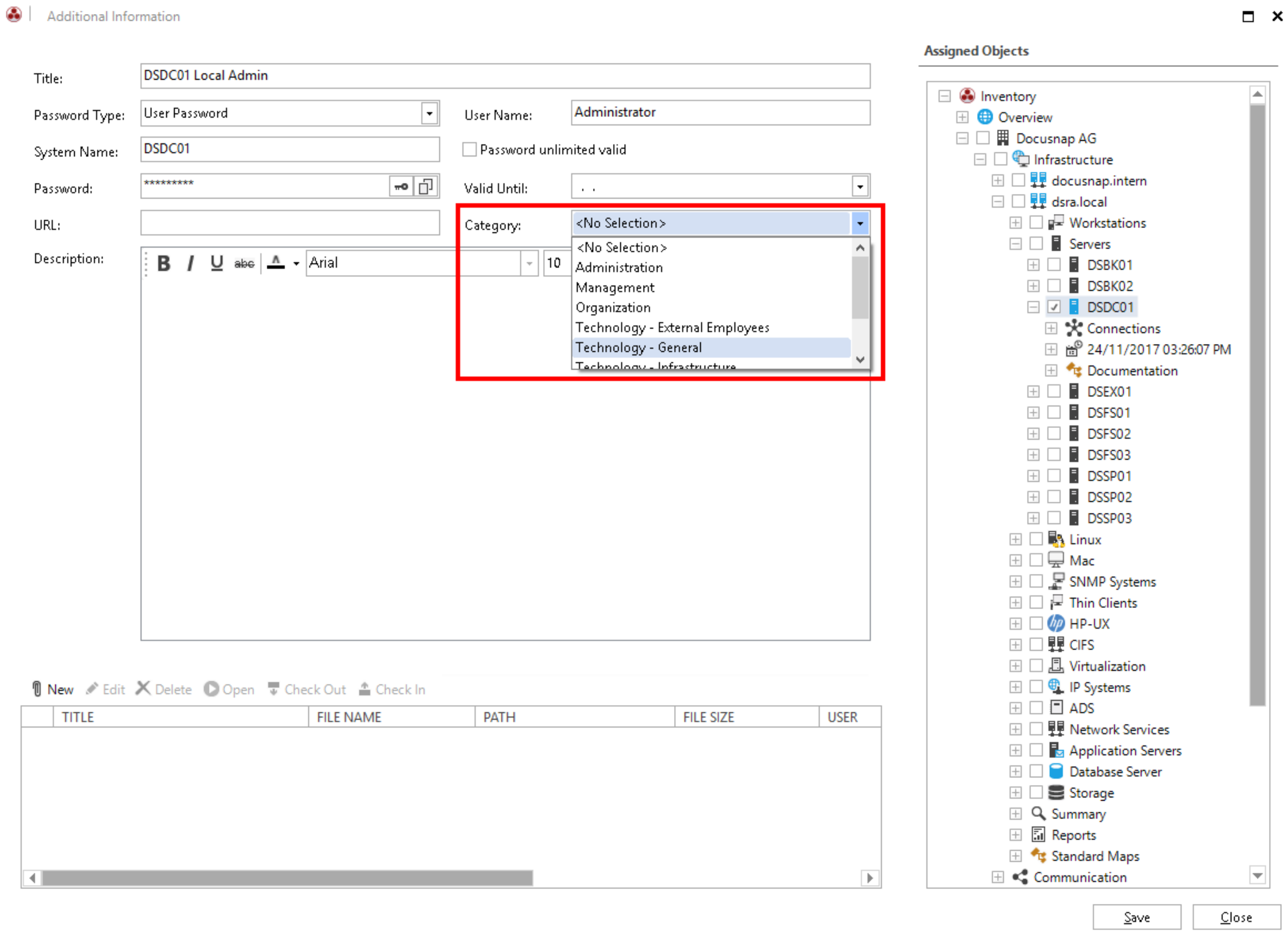
Fig. 16 – Assigning permission categories to Docusnap roles

5.2 Creating Additional Information Using Permission Categories

Create a new piece of additional information – e.g. a password. The dialog includes a selection list called **Category**. You can select a suitable permission category from this selection list.

Additional information to which no permission category has been assigned can be viewed by any user in Docusnap.

Additional information with a permission category assigned can only be viewed by users with a role to which a corresponding permission category has been assigned.



Additional Information

Title: DSDC01 Local Admin

Password Type: User Password

User Name: Administrator

System Name: DSDC01

☐ Password unlimited valid

Password: *********

Valid Until: . .

URL:

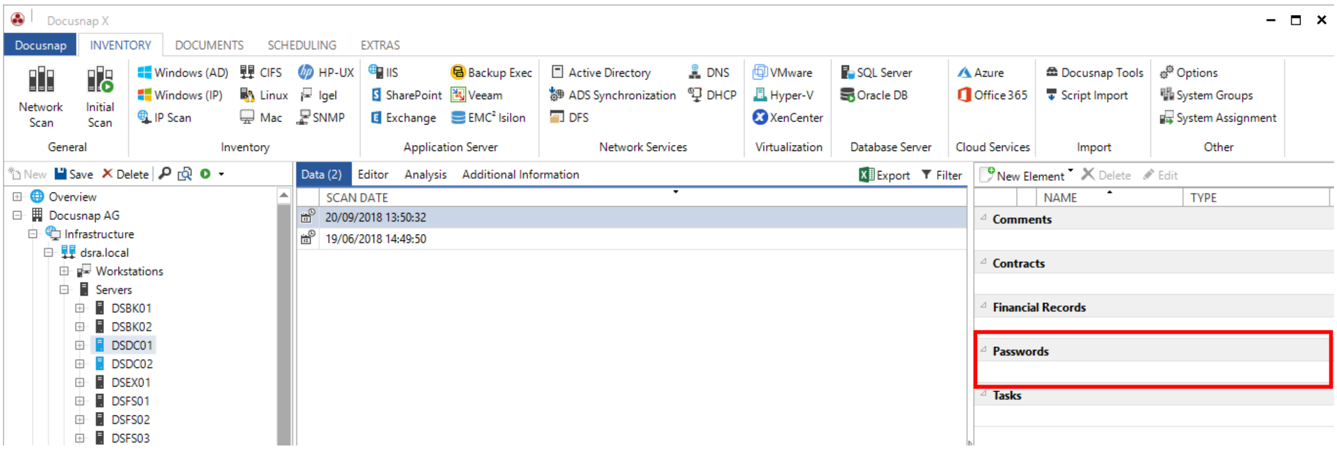
Category: <No Selection>

- <No Selection>
- Administration
- Management
- Organization
- Technology - External Employees
- Technology - General
- Technology - Infrastructure

Description:

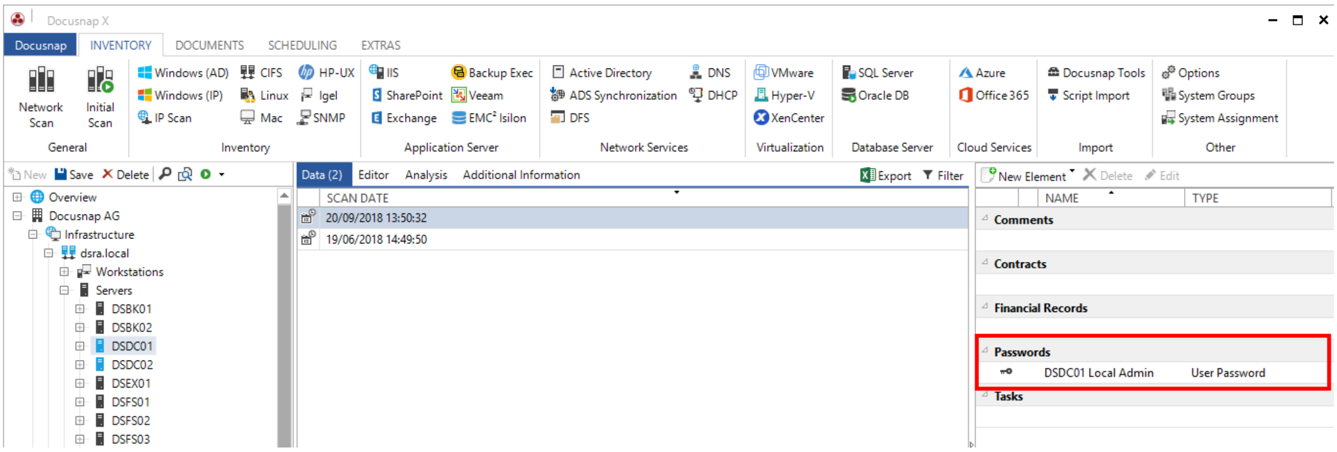
TITLE	FILE NAME	PATH	FILE SIZE	USER

Fig. 17 – Permission categories available for additional information



SCAN DATE
20/09/2018 13:50:32
19/06/2018 14:49:50

Fig. 18 – View as seen by a user without a permission category assigned



SCAN DATE
20/09/2018 13:50:32
19/06/2018 14:49:50

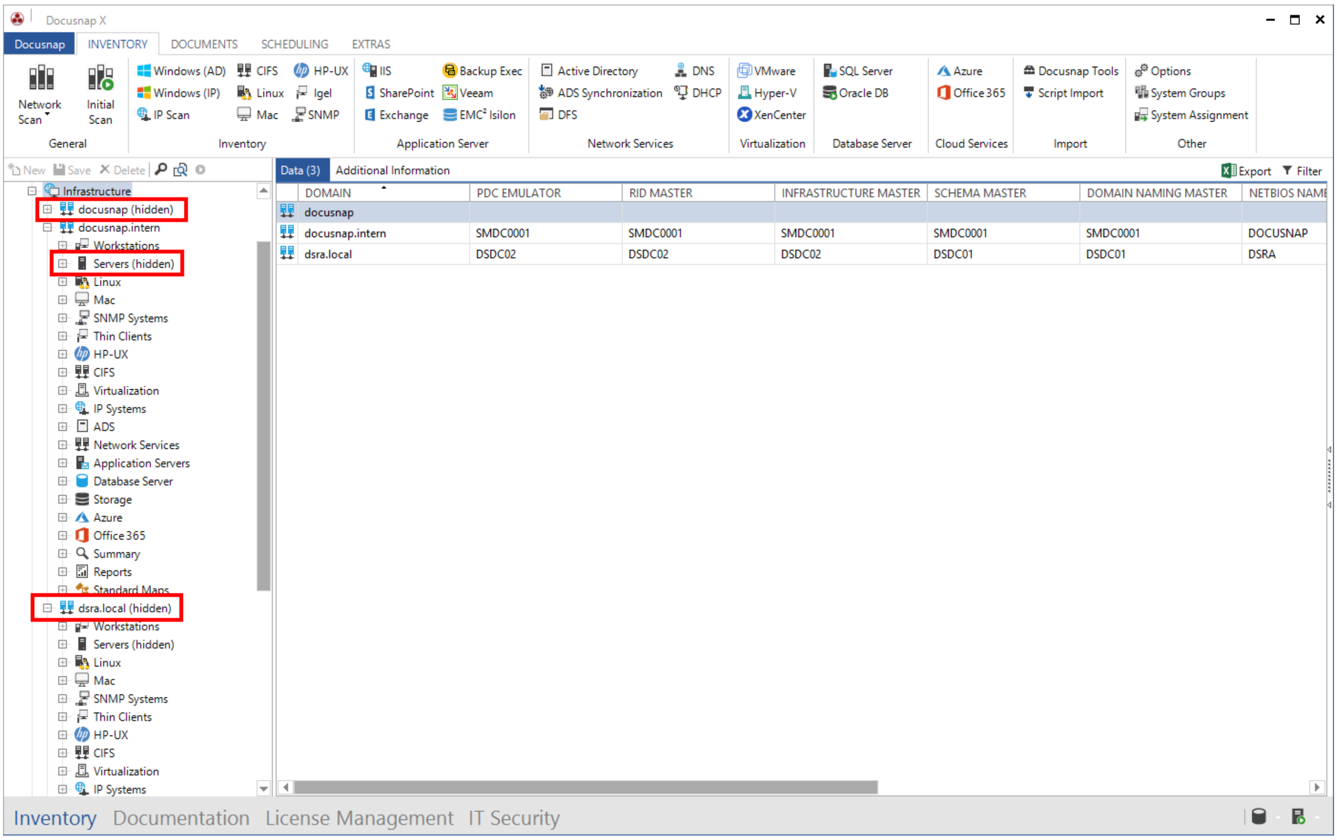
NAME	TYPE
DSDC01 Local Admin	User Password

Fig. 19 – View as seen by a user with a permission category assigned

6. Special Role: Administration

The Administration role in Docusnap is designed for users who may “see and do everything”.

For example, if you configure additional information or objects available in the Data Explorer in such a way that the members of the Administration role cannot access them, this setting has no effect, i.e. the members of this role still have access to this information or these objects. This situation is identified by the word (hidden) next to the corresponding object.



DOMAIN	PDC EMULATOR	RID MASTER	INFRASTRUCTURE MASTER	SCHEMA MASTER	DOMAIN NAMING MASTER	NETBIOS NAME
docusnap						
docusnap.intern	SMDC0001	SMDC0001	SMDC0001	SMDC0001	SMDC0001	DOCUSNAP
dsra.local	DSDC02	DSDC02	DSDC02	DSDC01	DSDC01	DSRA

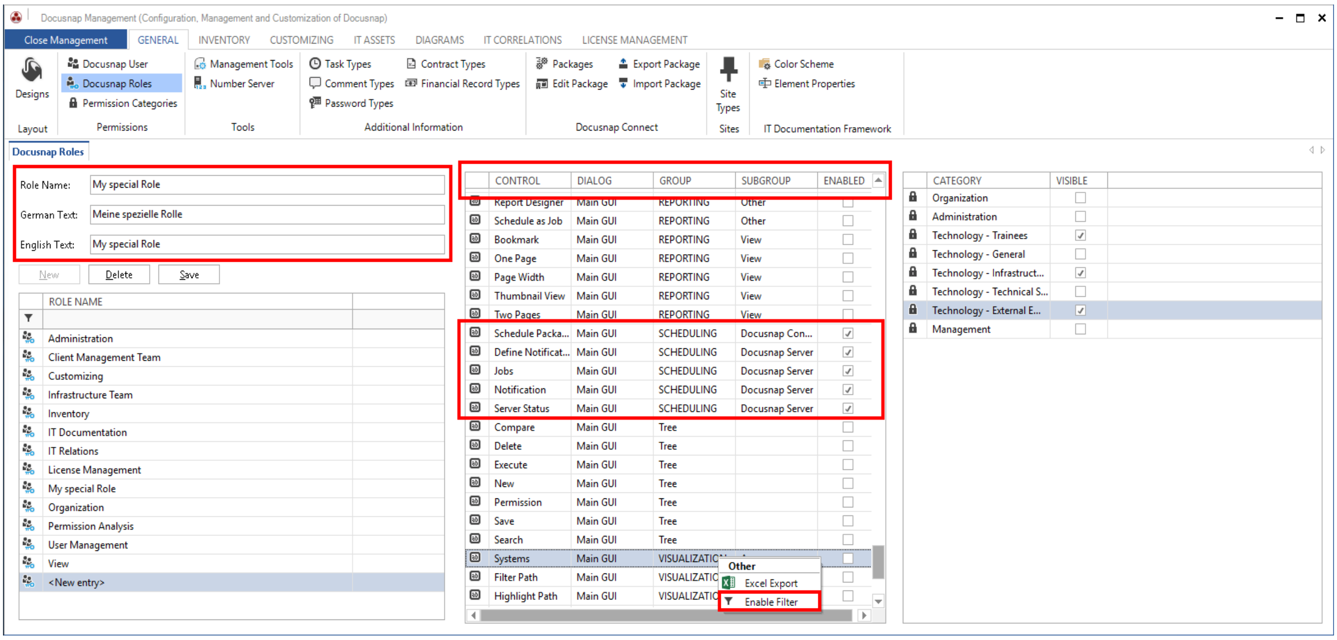
Fig. 20 – Special role: Administration

7. Adding Docusnap Roles

Under Docusnap > Management – General tab – Docusnap Roles, you can create your own Docusnap roles. This allows you to make exactly those features available to the users that these need for their work.

Please note that existing roles can neither be edited nor copied!

However, you can use the newly created roles to restrict the access to information as desired.



Role Name: My special Role

German Text: Meine spezielle Rolle

English Text: My special Role

ROLE NAME
Administration
Client Management Team
Customizing
Infrastructure Team
Inventory
IT Documentation
IT Relations
License Management
My special Role
Organization
Permission Analysis
User Management
View
<New entry>

CONTROL	DIALOG	GROUP	SUBGROUP	ENABLED
Report Designer	Main GUI	REPORTING	Other	□
Schedule as Job	Main GUI	REPORTING	Other	□
Bookmark	Main GUI	REPORTING	View	□
One Page	Main GUI	REPORTING	View	□
Page Width	Main GUI	REPORTING	View	□
Thumbnail View	Main GUI	REPORTING	View	□
Two Pages	Main GUI	REPORTING	View	□
Schedule Packa...	Main GUI	SCHEDULING	Docusnap Con...	☑
Define Notificat...	Main GUI	SCHEDULING	Docusnap Server	☑
Jobs	Main GUI	SCHEDULING	Docusnap Server	☑
Notification	Main GUI	SCHEDULING	Docusnap Server	☑
Server Status	Main GUI	SCHEDULING	Docusnap Server	☑
Compare	Main GUI	Tree		□
Delete	Main GUI	Tree		□
Execute	Main GUI	Tree		□
New	Main GUI	Tree		□
Permission	Main GUI	Tree		□
Save	Main GUI	Tree		□
Search	Main GUI	Tree		□
Systems	Main GUI	VISUALIZATIO		□
Filter Path	Main GUI	VISUALIZATIC		□
Highlight Path	Main GUI	VISUALIZATIC		□

CATEGORY	VISIBLE
Organization	□
Administration	□
Technology - Trainees	☑
Technology - General	□
Technology - Infrastruct...	☑
Technology - Technical S...	□
Technology - External E...	☑
Management	□

Fig. 21 – Creating custom roles

Once you have created a new role, you can select the desired controls in the center panel.

Initially, the controls are sorted by dialog, group, and subgroup.

Dialog
This column indicates the Docusnap area where the control is located, e.g. the main GUI.

Group
This column identifies the functional group to which the control belongs, e.g. Reporting.

Subgroup
This is a further subdivision, e.g. Reporting – View

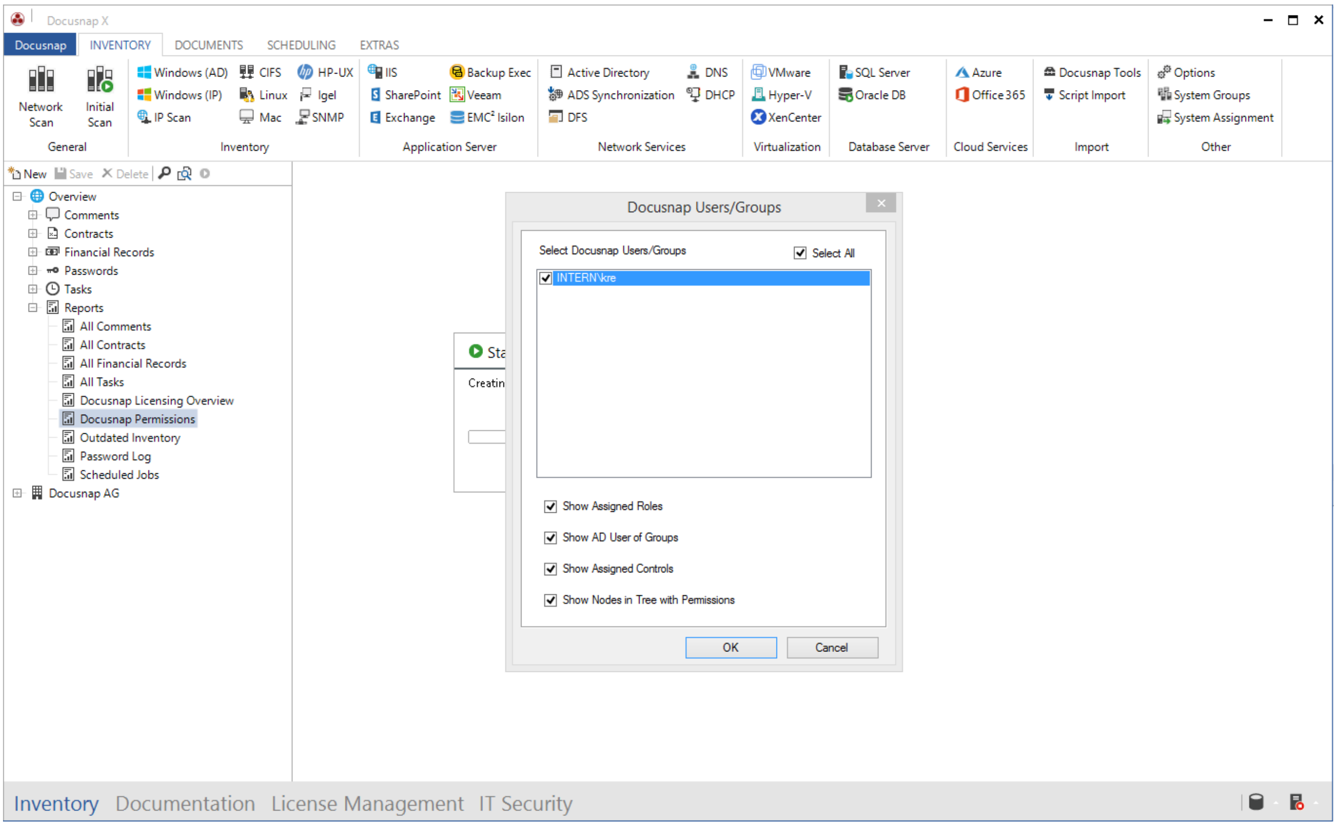
8. Documenting the User Management Settings

Permission management in Docusnap is comprehensive and can soon become very complex. To enable you to check and document the implementation of these permissions, a report listing the permission settings is available in Docusnap.

The **Docusnap Permissions** report can be found under **Overview – Reports**. Once you have opened the report, you are prompted to select the users or groups that you added to the Docusnap User Management.

The other options allow you to specify the level of detail for the report:

Show Assigned Roles	The report will include the Docusnap roles associated to the selected users and groups.
Show AD User of Groups	The report will resolve the stored AD group from User Management.
Show Assigned Controls	The report will list the controls available to the selected users or groups.
Show Nodes in Tree with Permissions	The report will list objects and types that the users or groups may view.



Docusnap Users/Groups

Select Docusnap Users/Groups ☑ Select All

☑ INTERN\kre

☑ Show Assigned Roles

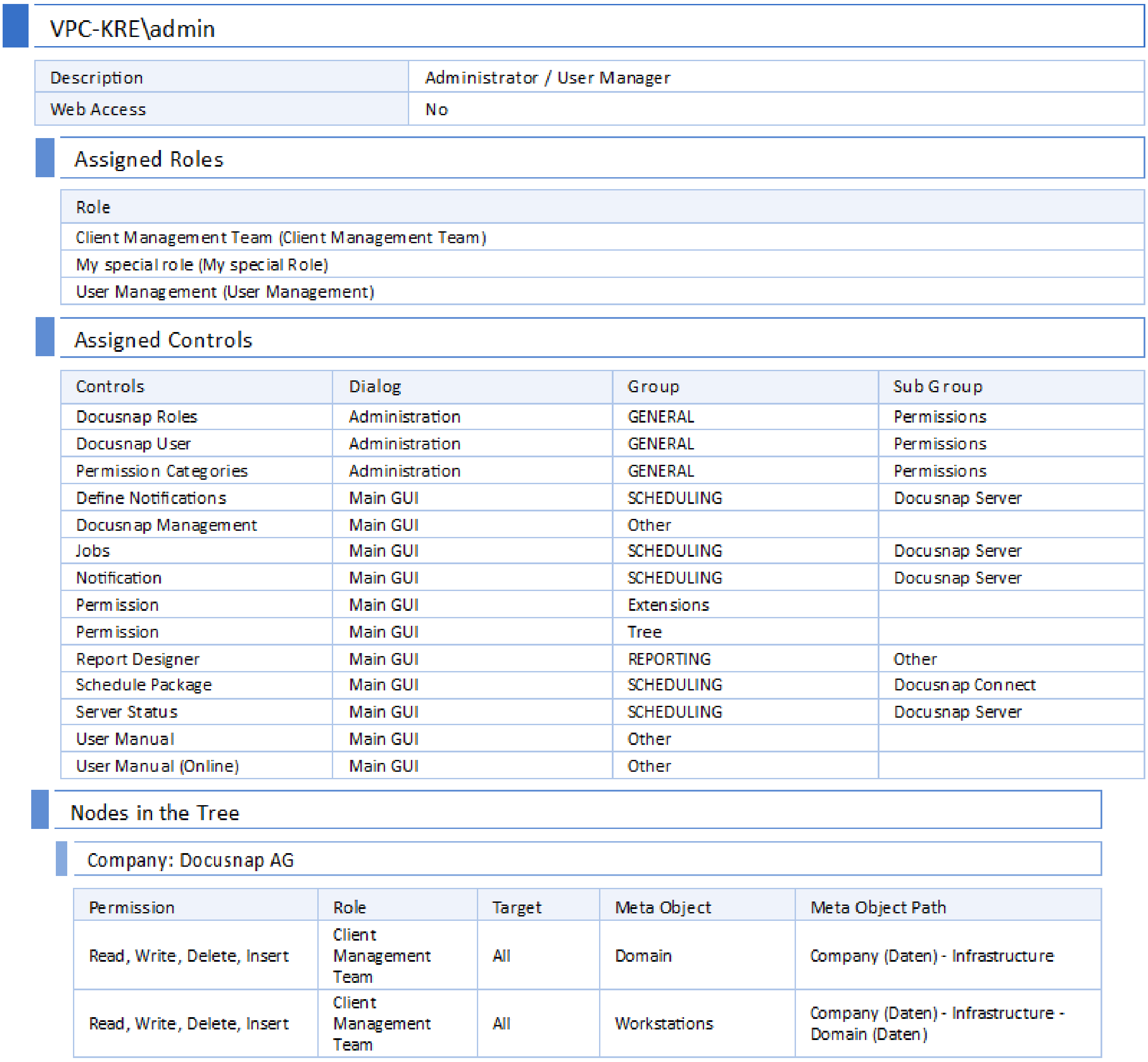
☑ Show AD User of Groups

☑ Show Assigned Controls

☑ Show Nodes in Tree with Permissions

OK Cancel

Fig. 22 – -Calling the Docusnap Permissions report



VPC-KRE\admin

Description	Administrator / User Manager
Web Access	No

Assigned Roles

Role
Client Management Team (Client Management Team)
My special role (My special Role)
User Management (User Management)

Assigned Controls

Controls	Dialog	Group	Sub Group
Docusnap Roles	Administration	GENERAL	Permissions
Docusnap User	Administration	GENERAL	Permissions
Permission Categories	Administration	GENERAL	Permissions
Define Notifications	Main GUI	SCHEDULING	Docusnap Server
Docusnap Management	Main GUI	Other	
Jobs	Main GUI	SCHEDULING	Docusnap Server
Notification	Main GUI	SCHEDULING	Docusnap Server
Permission	Main GUI	Extensions	
Permission	Main GUI	Tree	
Report Designer	Main GUI	REPORTING	Other
Schedule Package	Main GUI	SCHEDULING	Docusnap Connect
Server Status	Main GUI	SCHEDULING	Docusnap Server
User Manual	Main GUI	Other	
User Manual (Online)	Main GUI	Other	

Nodes in the Tree

Company: Docusnap AG

Permission	Role	Target	Meta Object	Meta Object Path
Read, Write, Delete, Insert	Client Management Team	All	Domain	Company (Daten) - Infrastructure
Read, Write, Delete, Insert	Client Management Team	All	Workstations	Company (Daten) - Infrastructure - Domain (Daten)

Fig. 23 – Excerpt from the Docusnap Permissions report

LIST OF FIGURES

VERSION HISTORY

Date	Description
January 02, 2018	First draft created
January 04, 2018	Version 1.0 completed
October 24, 2018	Changed Screenshots

© itelio GmbH - www.itelio.com