Docusnap – User Management

Managing User Access to Docusnap

TITLE	Docusnap – User Management
AUTHOR	Docusnap Consulting
DATE	11/20/2020
VERSION	2.0 | valid from May 01, 2020

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 authorization assignment also affects access to Docusnap Web. Please note that the selected authentication method for Docusnap Web will only be effective when user management is activated. For more information on the authentication methods for Docusnap Web, please refer to the corresponding HowTo - Docusnap Web.

This HowTo document describes the following use cases:

- Eemployees 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

Other examples of groups and resulting Docusnap roles could be

- 1st level Docusnap
- 2nd level Docusnap
- 3rd level Docusnap

- Client Management
- Server Management
- network management

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.

Permission Categories

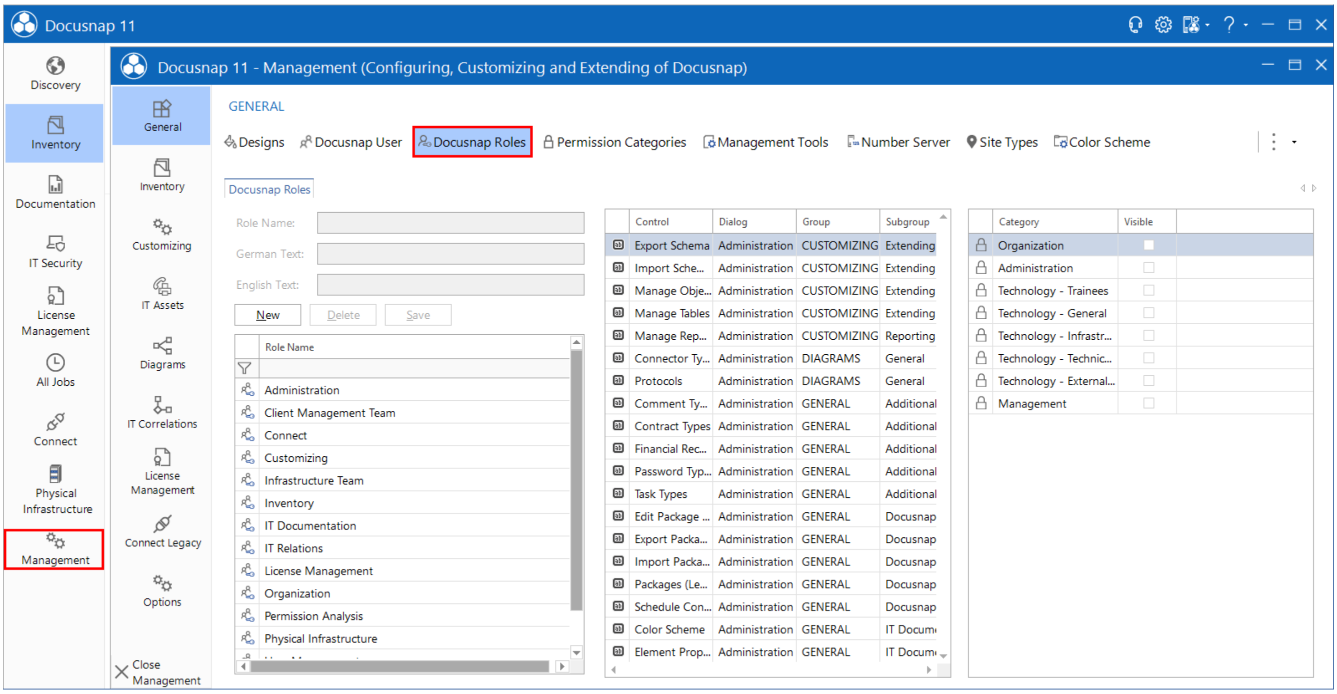
Permission categories help you restrict the access to additional information (passwords, contracts, comments, etc.) in Docusnap. Permission categories are linked to roles. This way, you can use the Docusnap roles also to control the access to additional information.

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 Management – General – Docusnap Roles.



Role Name
Administration
Client Management Team
Connect
Customizing
Infrastructure Team
Inventory
IT Documentation
IT Relations
License Management
Organization
Permission Analysis
Physical Infrastructure

Control	Dialog	Group	Subgroup
Export Schema	Administration	CUSTOMIZING	Extending
Import Sche...	Administration	CUSTOMIZING	Extending
Manage Obje...	Administration	CUSTOMIZING	Extending
Manage Tables	Administration	CUSTOMIZING	Extending
Manage Rep...	Administration	CUSTOMIZING	Reporting
Connector Ty...	Administration	DIAGRAMS	General
Protocols	Administration	DIAGRAMS	General
Comment Ty...	Administration	GENERAL	Additional
Contract Types	Administration	GENERAL	Additional
Financial Rec...	Administration	GENERAL	Additional
Password Typ...	Administration	GENERAL	Additional
Task Types	Administration	GENERAL	Additional
Edit Package ...	Administration	GENERAL	Docusnap
Export Packa...	Administration	GENERAL	Docusnap
Import Packa...	Administration	GENERAL	Docusnap
Packages (Le...	Administration	GENERAL	Docusnap
Schedule Con...	Administration	GENERAL	Docusnap
Color Scheme	Administration	GENERAL	IT Docum
Element Prop...	Administration	GENERAL	IT Docum

Category	Visible
Organization	□
Administration	□
Technology - Trainees	□
Technology - General	□
Technology - Infrastr...	□
Technology - Technic...	□
Technology - External...	□
Management	□

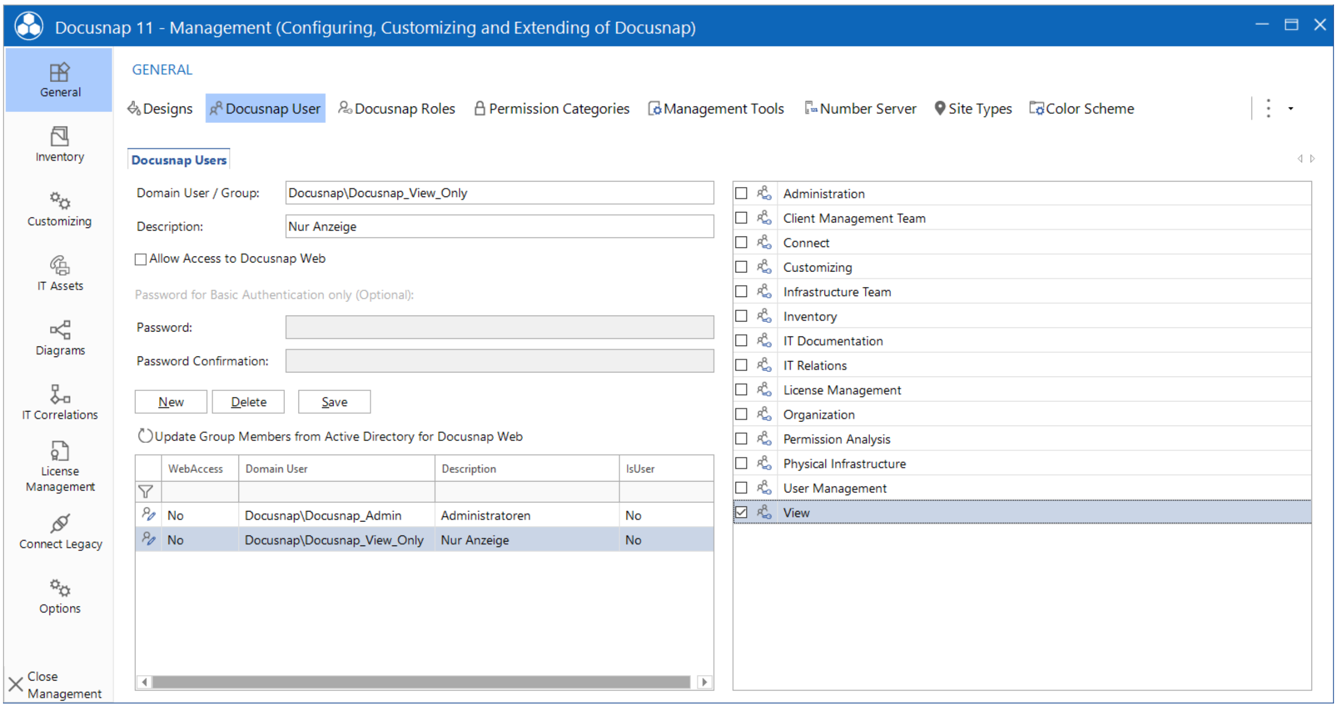
Fig. 1 – Accessing Docusnap Management

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.

The column **IsUser** indicates whether this is a user or an AD group. If this column remains empty, Docusnap cannot resolve it, please check the spelling again. A resolution can only take place if the Docusnap system itself is also in the domain.



Domain User / Group: Docusnap\Docusnap_View_Only

Description: Nur Anzeige

□ Allow Access to Docusnap Web

Password for Basic Authentication only (Optional):

Password:

Password Confirmation:

Update Group Members from Active Directory for Docusnap Web

WebAccess	Domain User	Description	IsUser
No	Docusnap\Docusnap_Admin	Administratoren	No
No	Docusnap\Docusnap_View_Only	Nur Anzeige	No

- □ Administration
- □ Client Management Team
- □ Connect
- □ Customizing
- □ Infrastructure Team
- □ Inventory
- □ IT Documentation
- □ IT Relations
- □ License Management
- □ Organization
- □ Permission Analysis
- □ Physical Infrastructure
- □ User Management
- ☑ View

Fig. 2 – 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 – 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.

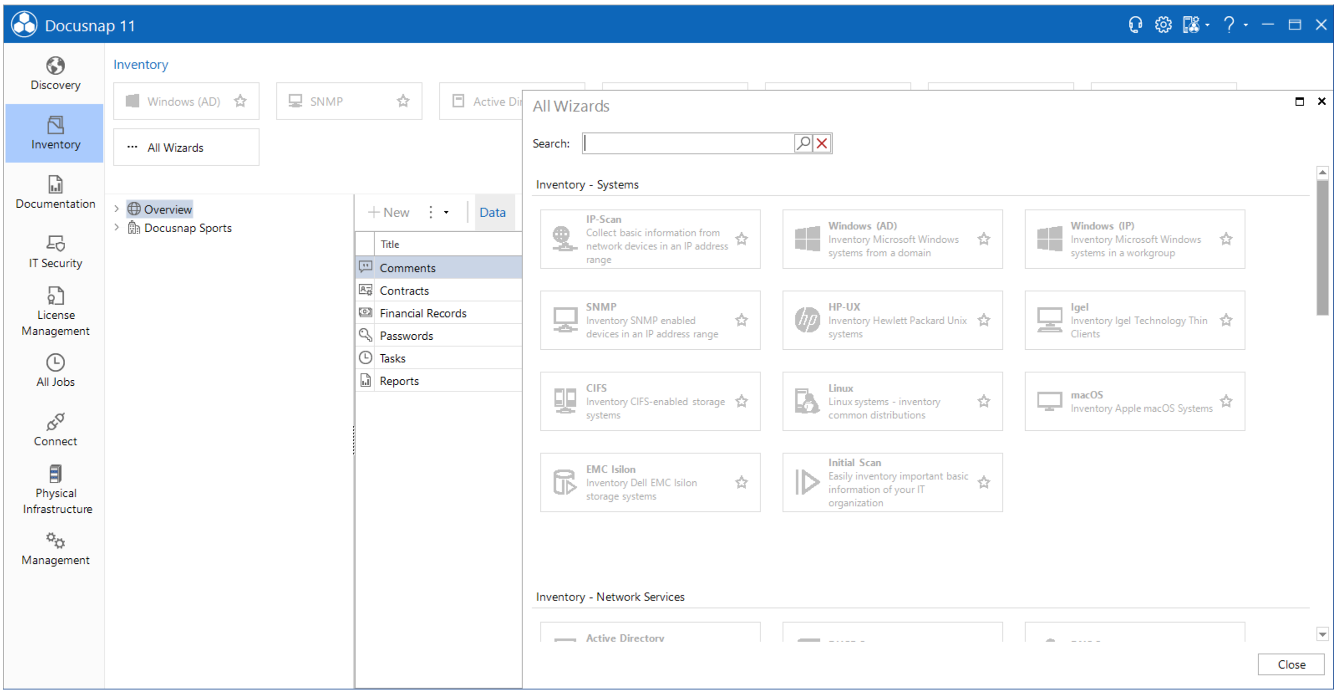

Docusnap 11
Discovery
Inventory
Documentation
IT Security
License Management
All Jobs
Connect
Physical Infrastructure
Management
Inventory
Windows (AD)
SNMP
Active Di
All Wizards
Overview
Docusnap Sports
New
Data
Title
Comments
Contracts
Financial Records
Passwords
Tasks
Reports
All Wizards
Search:
Inventory - Systems
IP-Scan
Collect basic information from network devices in an IP address range
Windows (AD)
Inventory Microsoft Windows systems from a domain
Windows (IP)
Inventory Microsoft Windows systems in a workgroup
SNMP
Inventory SNMP enabled devices in an IP address range
HP-UX
Inventory Hewlett Packard Unix systems
Igel
Inventory Igel Technology Thin Clients
CIFS
Inventory CIFS-enabled storage systems
Linux
Linux systems - inventory common distributions
macOS
Inventory Apple macOS Systems
EMC Isilon
Inventory Dell EMC Isilon storage systems
Initial Scan
Easily inventory important basic information of your IT organization
Inventory - Network Services
Active Directory
Close

Fig. 3 – View role – Restricted access to features

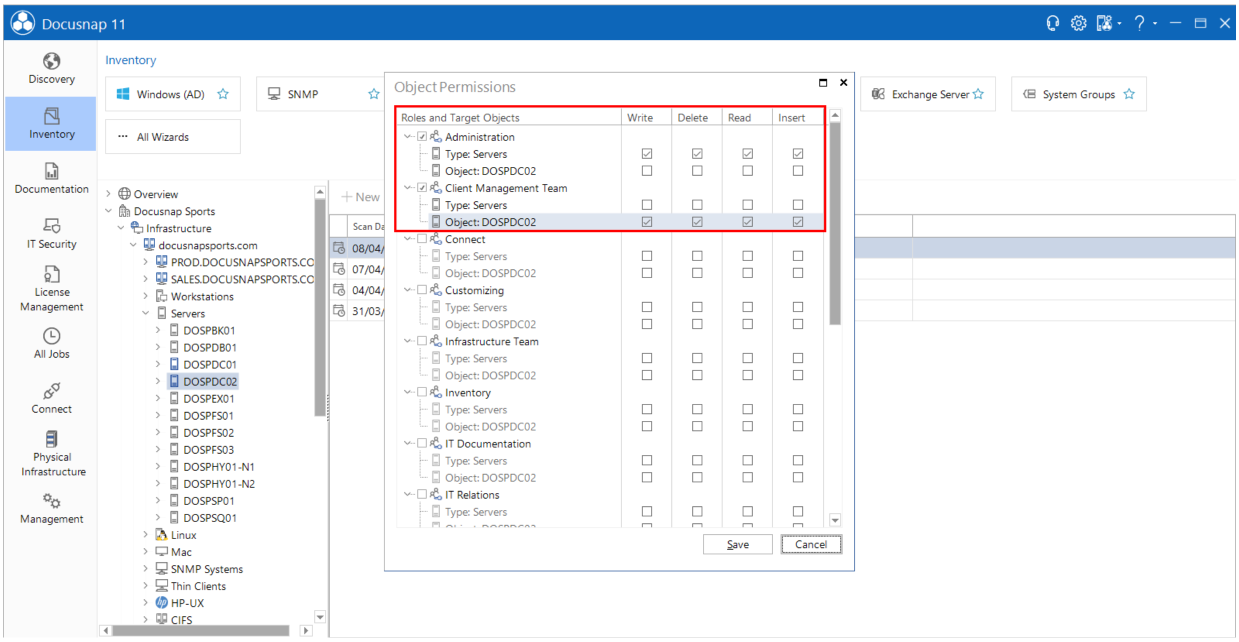
4. Restricting Access to Types and Objects in the Data Explorer

In addition to being able to limit the functions in Docusnap for users and groups, you also have the option of restricting access to types and objects within the data tree - e.g. Who can access the server information?

Here you can restrict which Docusnap roles can view certain types and objects and restrict to what extent Docusnap roles can edit these types and objects - Who can delete server objects?

4.1 Difference between types and objects

In the Permissions Object dialog, you have two options: Type and Object. You open this dialog by right-clicking on an object / heading in the Docusnap data tree.



Object Permissions

Roles and Target Objects	Write	Delete	Read	Insert
☑ Administration				
Type: Servers	☑	☑	☑	☑
Object: DOSPDC02	□	□	□	□
☑ Client Management Team				
Type: Servers	□	□	□	□
Object: DOSPDC02	☑	☑	☑	☑
□ Connect				
Type: Servers	□	□	□	□
Object: DOSPDC02	□	□	□	□
□ Customizing				
Type: Servers	□	□	□	□
Object: DOSPDC02	□	□	□	□
□ Infrastructure Team				
Type: Servers	□	□	□	□
Object: DOSPDC02	□	□	□	□
□ Inventory				
Type: Servers	□	□	□	□
Object: DOSPDC02	□	□	□	□
□ IT Documentation				
Type: Servers	□	□	□	□
Object: DOSPDC02	□	□	□	□
□ IT Relations				
Type: Servers	□	□	□	□

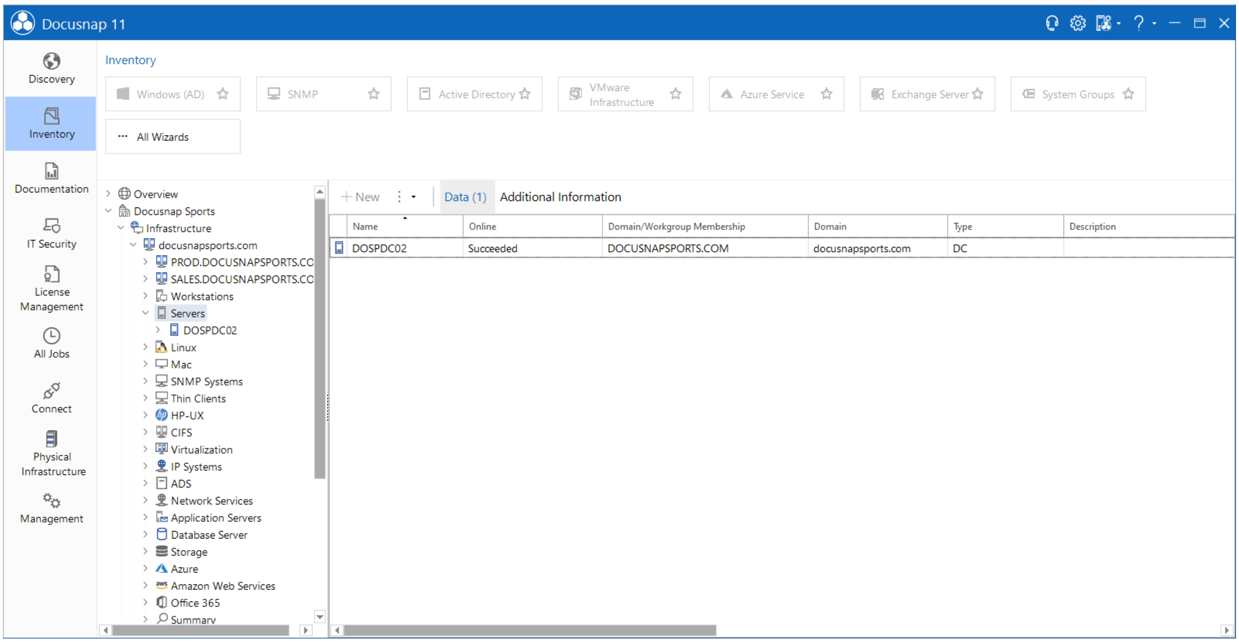
Fig. 4 – Object Permissions – Type vs. Object

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 **DOSPDC02**:

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 **DOSPDC02** Server object. Now, select a role and enable the checkboxes for **Object: DOSPDC02**. Members of this role will only see the DOSPDC02 server object within the Data Explorer.



Name	Online	Domain/Workgroup Membership	Domain	Type	Description
DOSPDC02	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	DC	

Fig. 5 – Setting object permissions – restricted access to information

4.2 Restrict the visibility of types and objects

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.

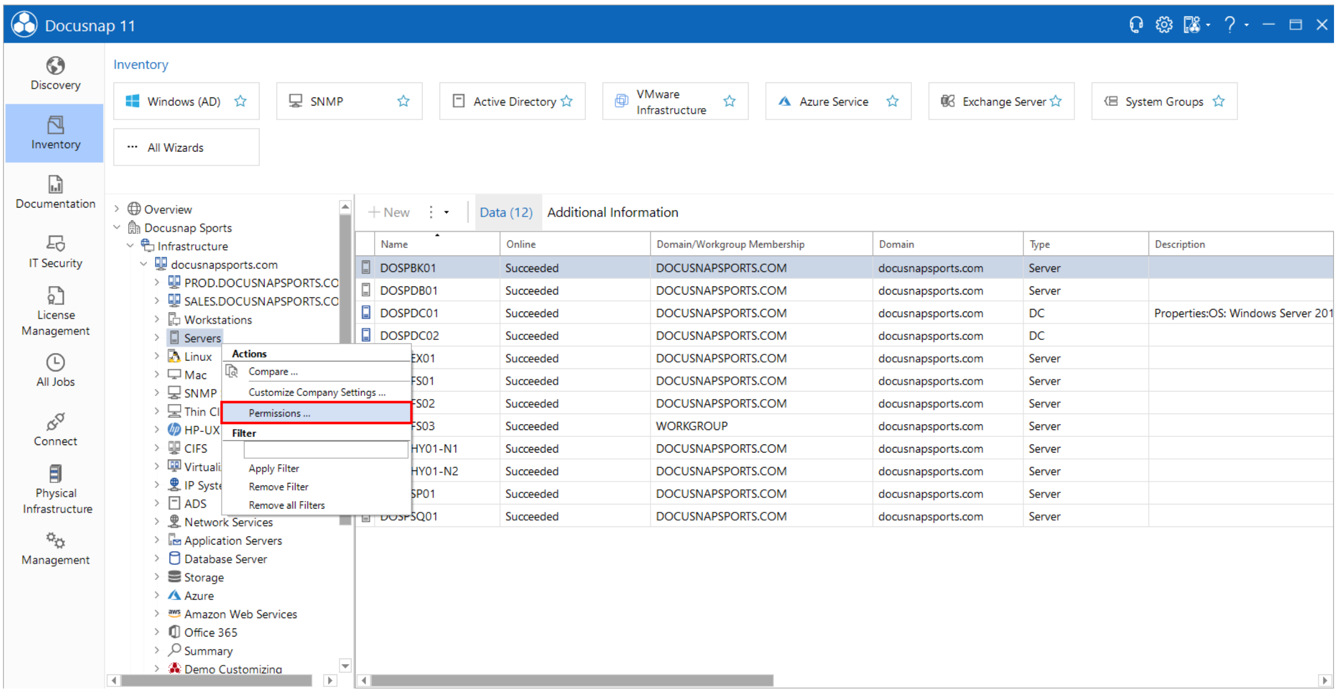
To implement this use case, at least two ADS groups must have been added to User Management and corresponding roles must have been assigned to them. Example:

- 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.

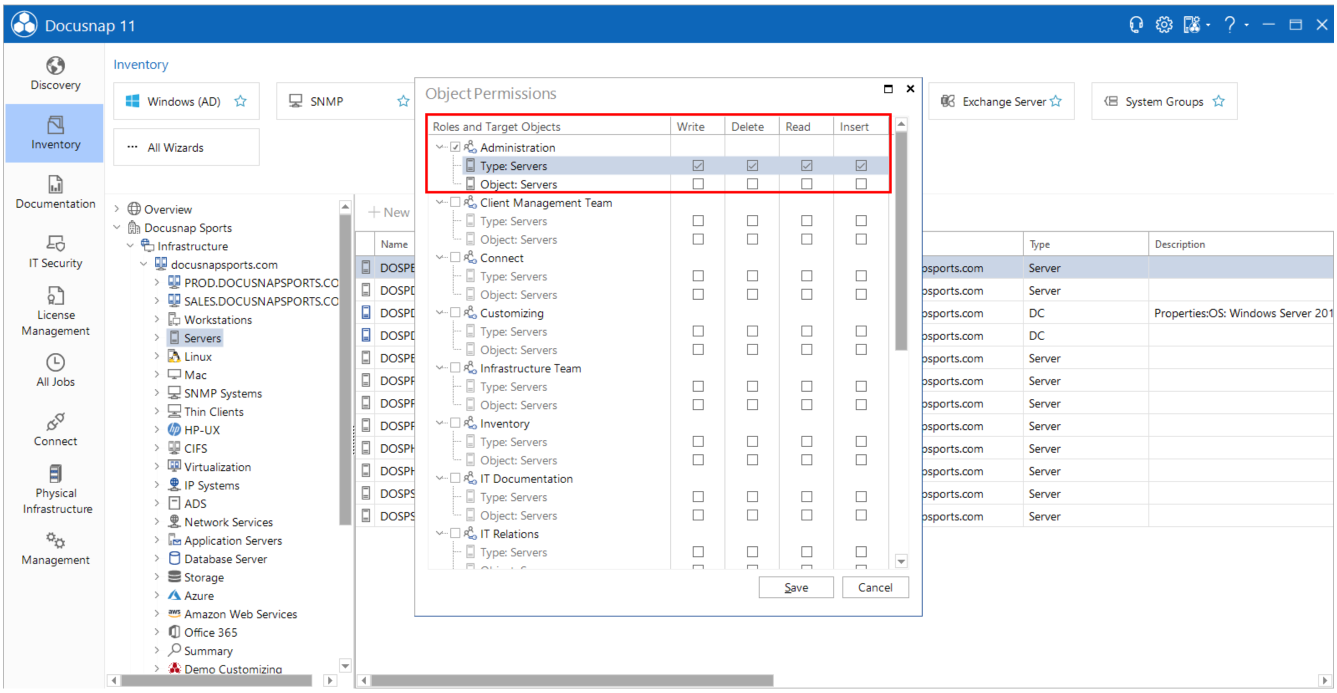
The **Object Permissions** windows opens, listing all available Docusnap roles. Now, select the role(s) you need. The member of the selected role(s) will continue to see the Servers type or object in the tree structure of Docusnap.

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



Name	Online	Domain/Workgroup Membership	Domain	Type	Description
DOSPBK01	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Server	
DOSPDB01	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Server	
DOSPDC01	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	DC	Properties:OS: Windows Server 201
DOSPDC02	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	DC	
EX01	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Server	
FS01	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Server	
FS02	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Server	
FS03	Succeeded	WORKGROUP	docusnapsports.com	Server	
HY01-N1	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Server	
HY01-N2	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Server	
SP01	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Server	
DOSPSQ01	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	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	□	□	□	□
□ Connect				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Customizing				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Infrastructure Team				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ Inventory				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ IT Documentation				
Type: Servers	□	□	□	□
Object: Servers	□	□	□	□
□ IT Relations				
Type: Servers	□	□	□	□

Name		Type	Description
DOSPE	psports.com	Server	
DOSPD	psports.com	Server	
DOSPD	psports.com	DC	Properties:OS: Windows Server 201
DOSPD	psports.com	DC	
DOSPE	psports.com	Server	
DOSPF	psports.com	Server	
DOSPF	psports.com	Server	
DOSPF	psports.com	Server	
DOSPH	psports.com	Server	
DOSPH	psports.com	Server	
DOSPS	psports.com	Server	
DOSPS	psports.com	Server	

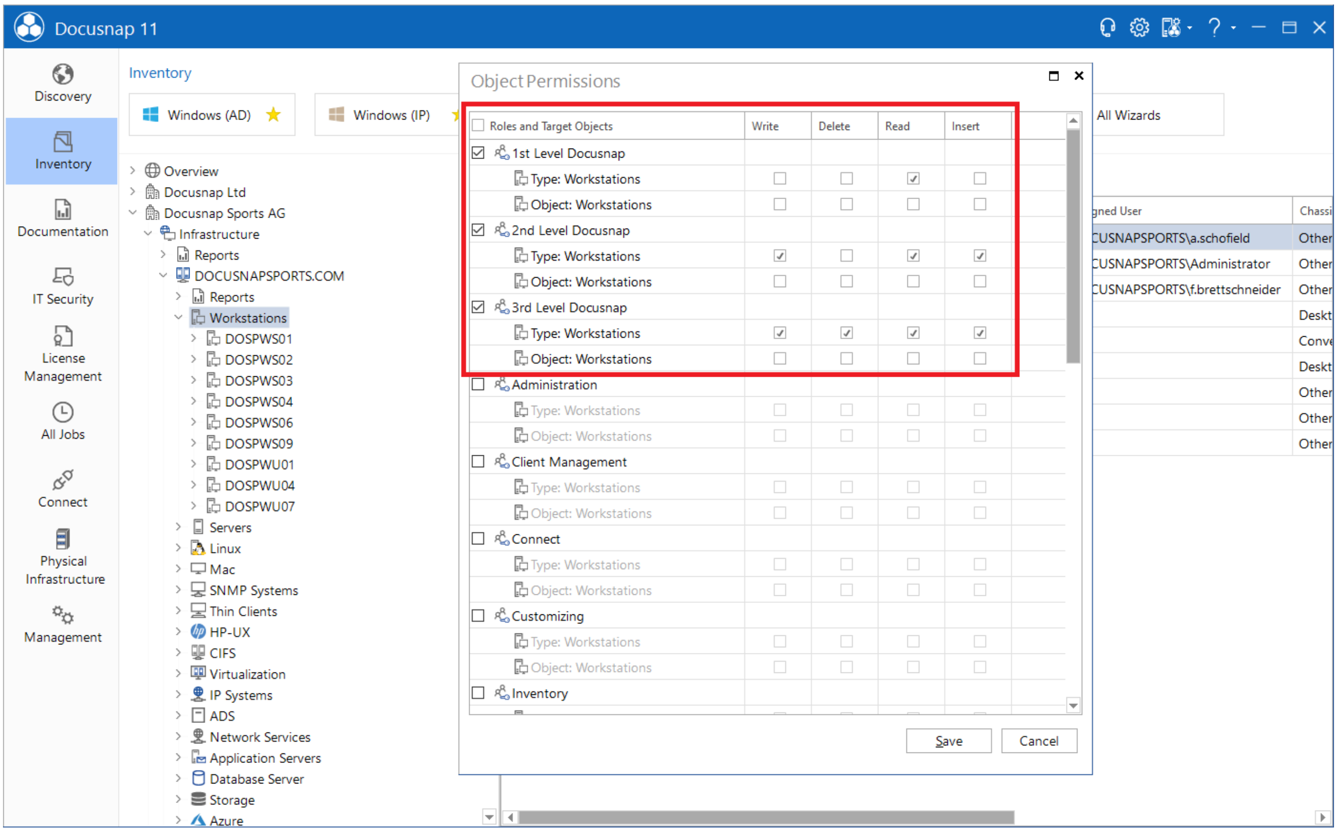
Fig. 7 – Setting permissions

4.3 Restrict the editing options of types and objects

You can define who can make which changes to existing objects within the Docusnap database, e.g. who should be allowed to edit and delete objects.

The following screenshot shows the new roles added to Docusnap with their respective permissions on workstation type objects

- 1st Level Docusnap can only view the objects
- 2nd Level Docusnap Can edit the objects
- 3rd Level Docusnap Can edit and delete objects

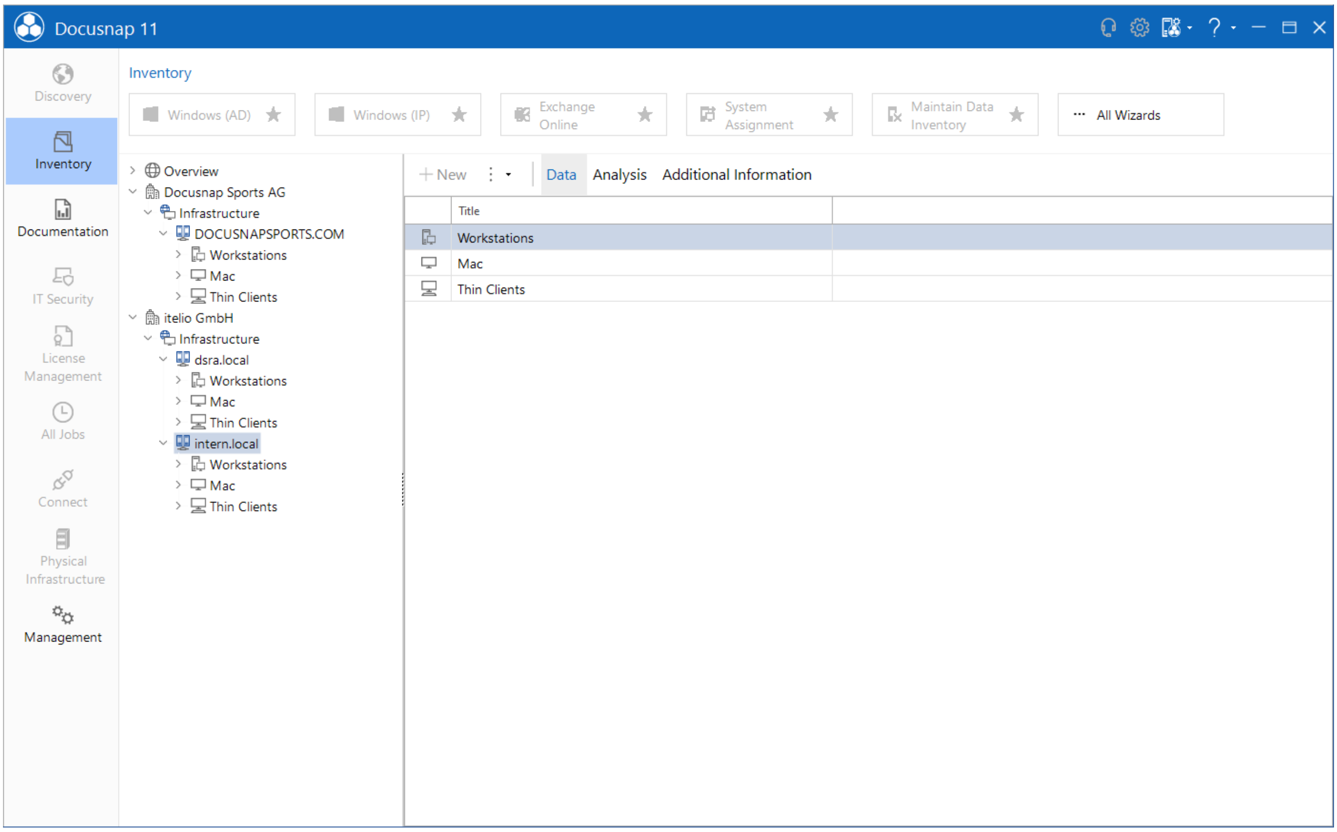


□ Roles and Target Objects	Write	Delete	Read	Insert
☑ 1st Level Docusnap				
Type: Workstations	□	□	☑	□
Object: Workstations	□	□	□	□
☑ 2nd Level Docusnap				
Type: Workstations	☑	□	☑	☑
Object: Workstations	□	□	□	□
☑ 3rd Level Docusnap				
Type: Workstations	☑	☑	☑	☑
Object: Workstations	□	□	□	□
□ Administration				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ Client Management				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ Connect				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ Customizing				
Type: Workstations	□	□	□	□
Object: Workstations	□	□	□	□
□ Inventory				

Fig. 8 – Setting permissions for editing objects

4.4 Tenant separation for Docusnap Permissions

If you assign the two types of permissions described above, they are valid for all tenants by default. So, if you have more than one tenant you have also set the permissions for all of them.

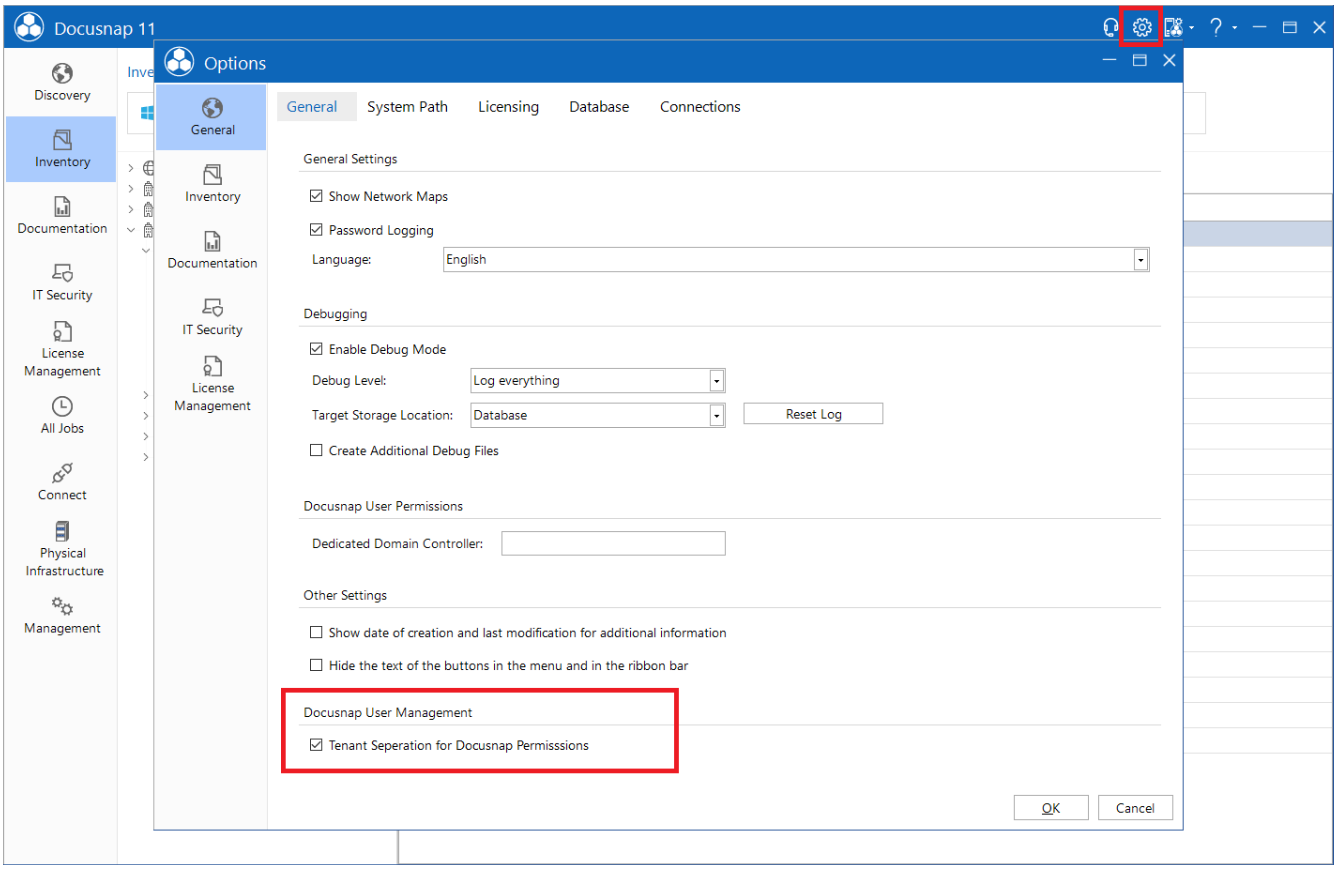


Title
Workstations
Mac
Thin Clients

Fig. 9 – Permissions set for one tenant are also applied to the others

If you want to assign specific permissions for the existing tenants, you can activate this in the General Options - Tenant separation for Docusnap Permissions.

After you have activated the option, permissions assigned for a tenant are not assigned directly to the additional tenant(s).



General Settings

☑ Show Network Maps

☑ Password Logging

Language: English

Debugging

☑ Enable Debug Mode

Debug Level: Log everything

Target Storage Location: Database

□ Create Additional Debug Files

Docusnap User Permissions

Dedicated Domain Controller:

Other Settings

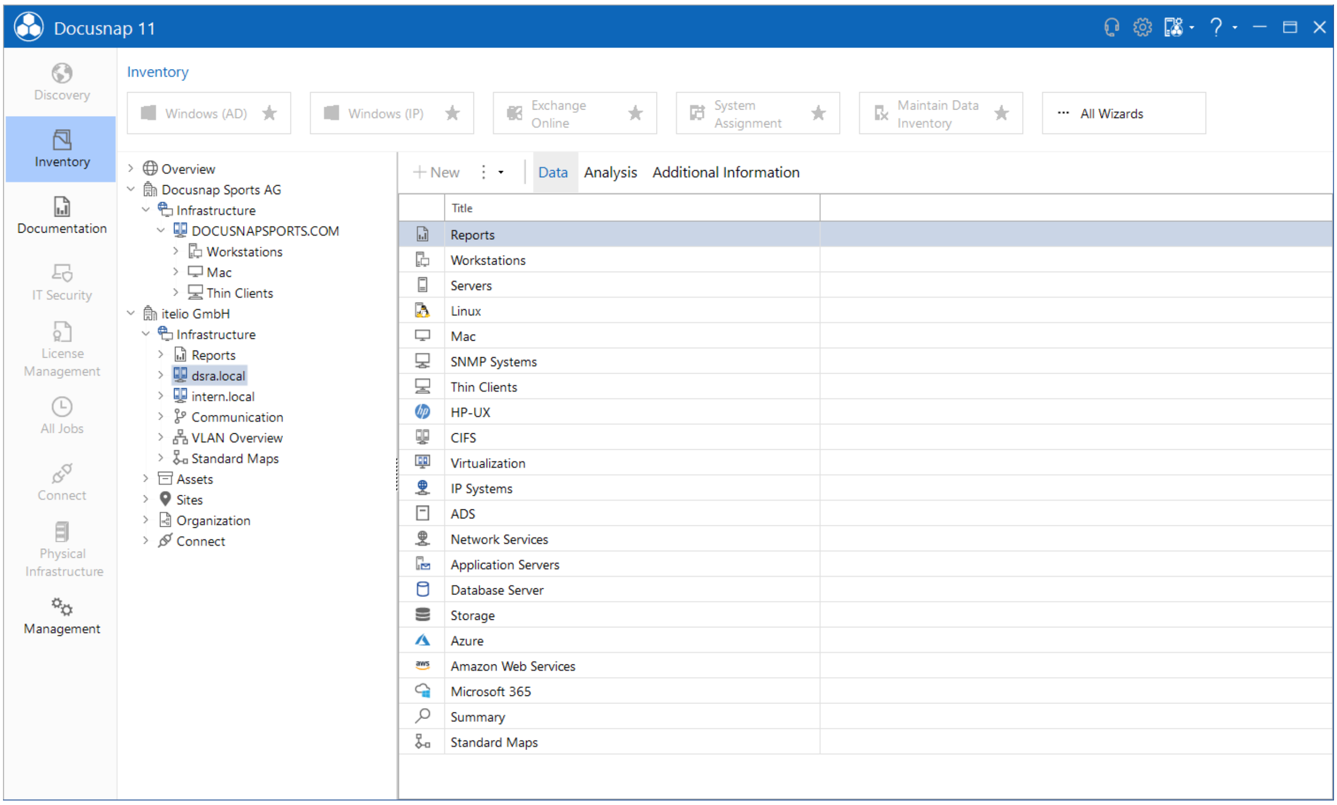
□ Show date of creation and last modification for additional information

□ Hide the text of the buttons in the menu and in the ribbon bar

Docusnap User Management

☑ Tenant Seperation for Docusnap Permisssions

Fig. 10 – Activating tenant separation for Docusnap permissions



- Overview
- Docusnap Sports AG
  - Infrastructure
    - DOCUSNAPSPORTS.COM
      - Workstations
      - Mac
      - Thin Clients
- itelio GmbH
  - Infrastructure
    - Reports
    - dsra.local
    - intern.local
    - Communication
    - VLAN Overview
    - Standard Maps
  - Assets
  - Sites
  - Organization
  - Connect

Title
Reports
Workstations
Servers
Linux
Mac
SNMP Systems
Thin Clients
HP-UX
CIFS
Virtualization
IP Systems
ADS
Network Services
Application Servers
Database Server
Storage
Azure
Amazon Web Services
Microsoft 365
Summary
Standard Maps

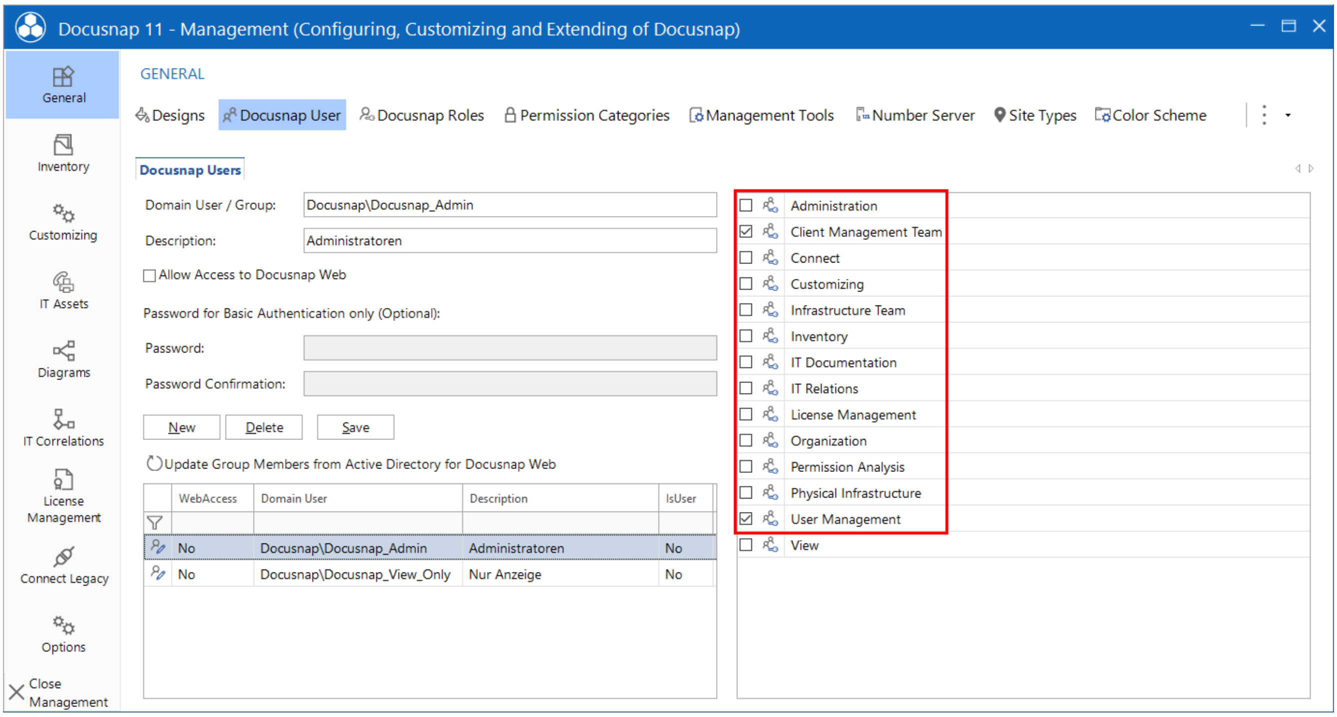
Fig. 11 – Authorizations can now be assigned to a specific tenant

4.5 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: Administratoren

□ Allow Access to Docusnap Web

Password for Basic Authentication only (Optional):

Password:

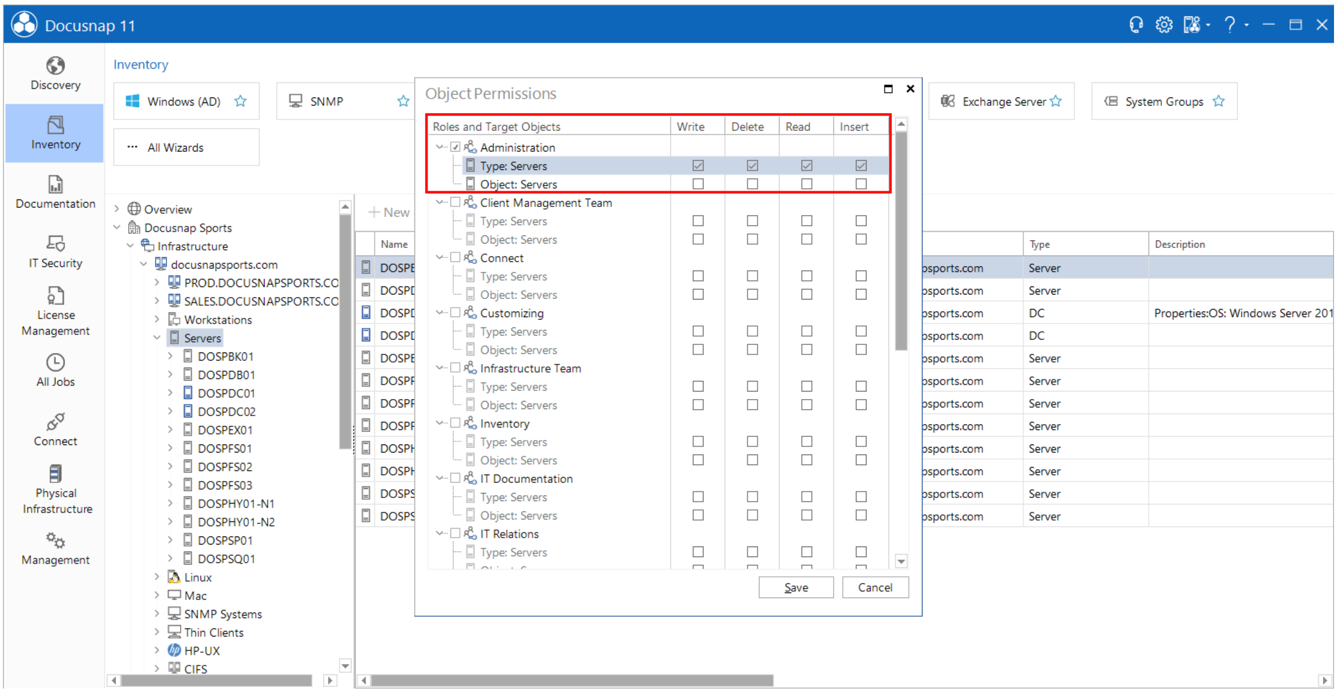
Password Confirmation:

WebAccess	Domain User	Description	IsUser
No	Docusnap\Docusnap_Admin	Administratoren	No
No	Docusnap\Docusnap_View_Only	Nur Anzeige	No

- □ Administration
- ☑ Client Management Team
- □ Connect
- □ Customizing
- □ Infrastructure Team
- □ Inventory
- □ IT Documentation
- □ IT Relations
- □ License Management
- □ Organization
- □ Permission Analysis
- □ Physical Infrastructure
- ☑ User Management
- □ View

Fig. 12 – Assigning roles

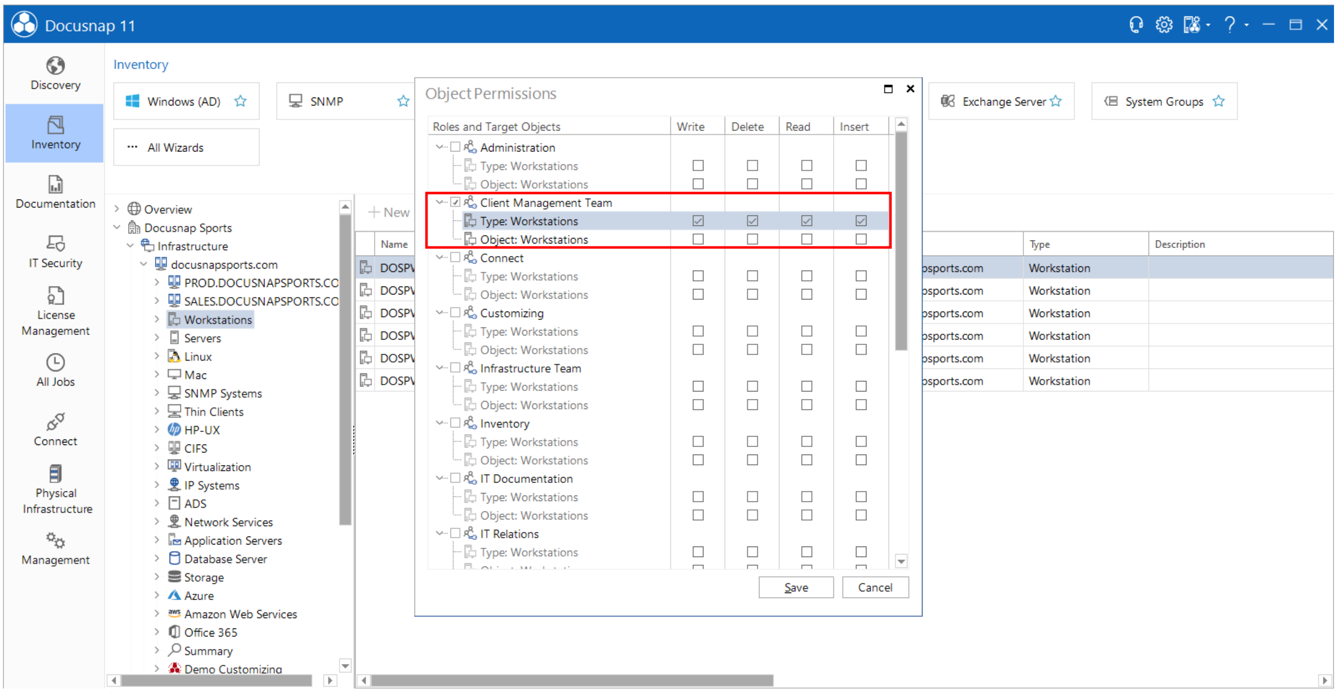
Go to the Docusnap main screen. While you are changing from the Management area to the main screen, the role change becomes effective. Now, make the desired changes in the main screen.



Roles and Target Objects	Write	Delete	Read	Insert
☑ Administration				
Type: Servers	☑	☑	☑	☑
Object: Servers	☐	☐	☐	☐
☐ Client Management Team				
Type: Servers	☐	☐	☐	☐
Object: Servers	☐	☐	☐	☐
☐ Connect				
Type: Servers	☐	☐	☐	☐
Object: Servers	☐	☐	☐	☐
☐ Customizing				
Type: Servers	☐	☐	☐	☐
Object: Servers	☐	☐	☐	☐
☐ Infrastructure Team				
Type: Servers	☐	☐	☐	☐
Object: Servers	☐	☐	☐	☐
☐ Inventory				
Type: Servers	☐	☐	☐	☐
Object: Servers	☐	☐	☐	☐
☐ IT Documentation				
Type: Servers	☐	☐	☐	☐
Object: Servers	☐	☐	☐	☐
☐ IT Relations				
Type: Servers	☐	☐	☐	☐

Name		Type	Description
DOSPE	psports.com	Server	
DOSPD	psports.com	Server	
DOSPD	psports.com	DC	Properties:OS: Windows Server 201
DOSPD	psports.com	DC	
DOSPE	psports.com	Server	
DOSPF	psports.com	Server	
DOSPF	psports.com	Server	
DOSPF	psports.com	Server	
DOSPH	psports.com	Server	
DOSPH	psports.com	Server	
DOSPS	psports.com	Server	
DOSPS	psports.com	Server	

Fig. 13 – Setting permissions to Servers



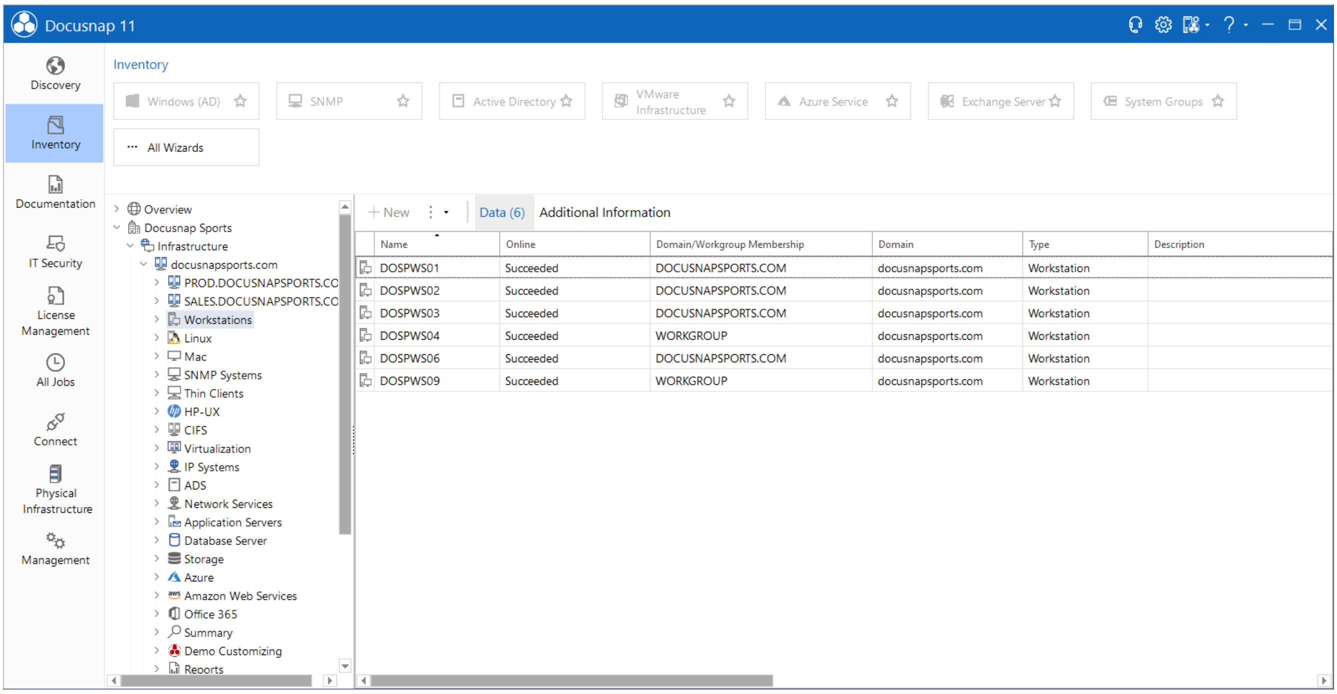
Roles and Target Objects	Write	Delete	Read	Insert
☐ Administration				
Type: Workstations	☐	☐	☐	☐
Object: Workstations	☐	☐	☐	☐
☑ Client Management Team				
Type: Workstations	☑	☑	☑	☑
Object: Workstations	☐	☐	☐	☐
☐ Connect				
Type: Workstations	☐	☐	☐	☐
Object: Workstations	☐	☐	☐	☐
☐ Customizing				
Type: Workstations	☐	☐	☐	☐
Object: Workstations	☐	☐	☐	☐
☐ Infrastructure Team				
Type: Workstations	☐	☐	☐	☐
Object: Workstations	☐	☐	☐	☐
☐ Inventory				
Type: Workstations	☐	☐	☐	☐
Object: Workstations	☐	☐	☐	☐
☐ IT Documentation				
Type: Workstations	☐	☐	☐	☐
Object: Workstations	☐	☐	☐	☐
☐ IT Relations				
Type: Workstations	☐	☐	☐	☐

Name		Type	Description
DOSPV	psports.com	Workstation	
DOSPV	psports.com	Workstation	
DOSPV	psports.com	Workstation	
DOSPV	psports.com	Workstation	
DOSPV	psports.com	Workstation	
DOSPV	psports.com	Workstation	

Fig. 14 – 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.



Name	Online	Domain/Workgroup Membership	Domain	Type	Description
DOSPWS01	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Workstation	
DOSPWS02	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Workstation	
DOSPWS03	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Workstation	
DOSPWS04	Succeeded	WORKGROUP	docusnapsports.com	Workstation	
DOSPWS06	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Workstation	
DOSPWS09	Succeeded	WORKGROUP	docusnapsports.com	Workstation	

Fig. 15 – 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.

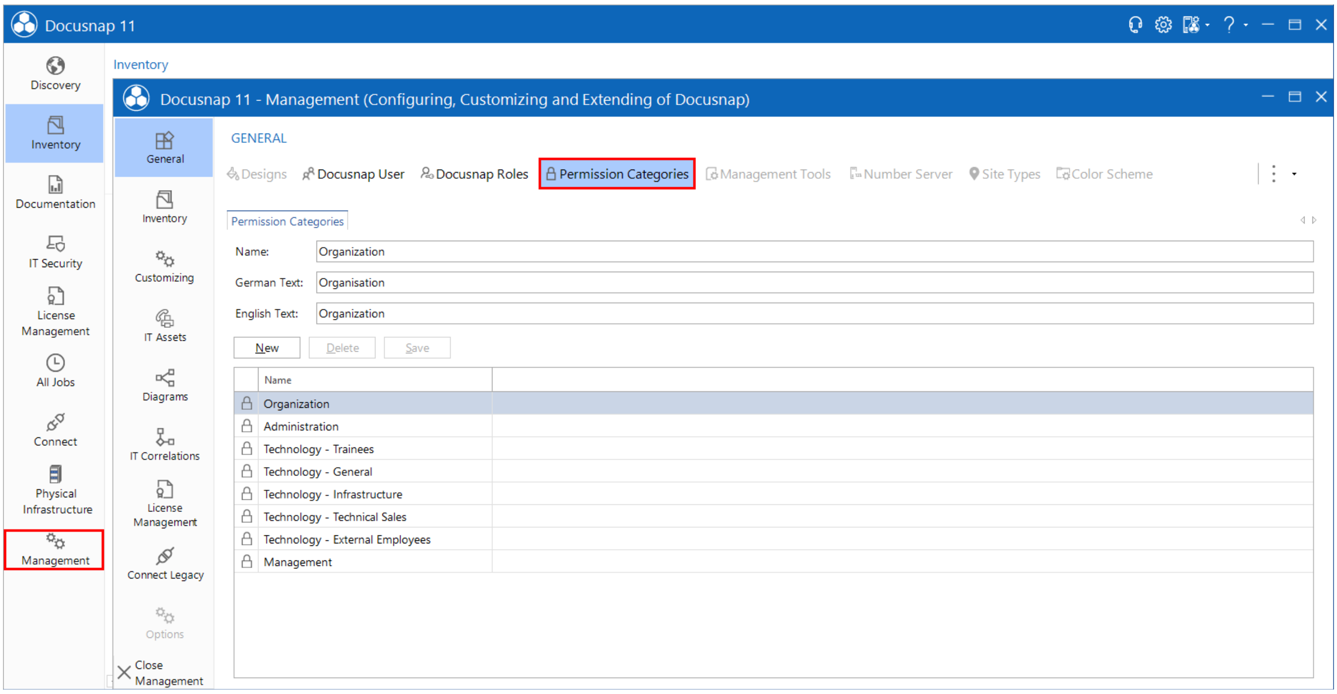
The following shows a possible application example:

- 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.



Name: Organization

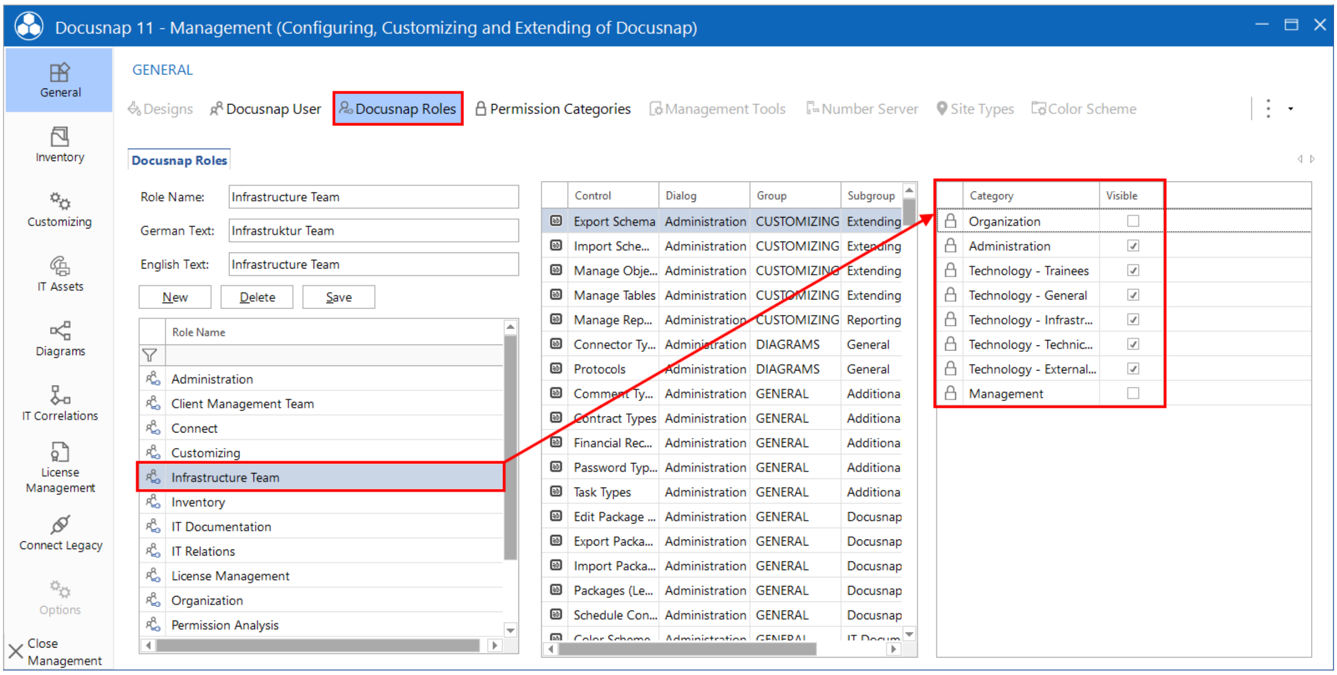
German Text: Organisation

English Text: Organization

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

Fig. 16 – Accessing Docusnap Management

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: Infrastruktur Team

English Text: Infrastructure Team

Role Name
Administration
Client Management Team
Connect
Customizing
Infrastructure Team
Inventory
IT Documentation
IT Relations
License Management
Organization
Permission Analysis

Control	Dialog	Group	Subgroup
Export Schema	Administration	CUSTOMIZING	Extending
Import Sche...	Administration	CUSTOMIZING	Extending
Manage Obje...	Administration	CUSTOMIZING	Extending
Manage Tables	Administration	CUSTOMIZING	Extending
Manage Rep...	Administration	CUSTOMIZING	Reporting
Connector Ty...	Administration	DIAGRAMS	General
Protocols	Administration	DIAGRAMS	General
Comment Ty...	Administration	GENERAL	Additiona
Contract Types	Administration	GENERAL	Additiona
Financial Rec...	Administration	GENERAL	Additiona
Password Typ...	Administration	GENERAL	Additiona
Task Types	Administration	GENERAL	Additiona
Edit Package ...	Administration	GENERAL	Docusnap
Export Packa...	Administration	GENERAL	Docusnap
Import Packa...	Administration	GENERAL	Docusnap
Packages (Le...	Administration	GENERAL	Docusnap
Schedule Con...	Administration	GENERAL	Docusnap
Color Scheme...	Administration	GENERAL	IT Docum...

Category	Visible
Organization	☐
Administration	☑
Technology - Trainees	☑
Technology - General	☑
Technology - Infrastr...	☑
Technology - Technic...	☑
Technology - External...	☑
Management	☐

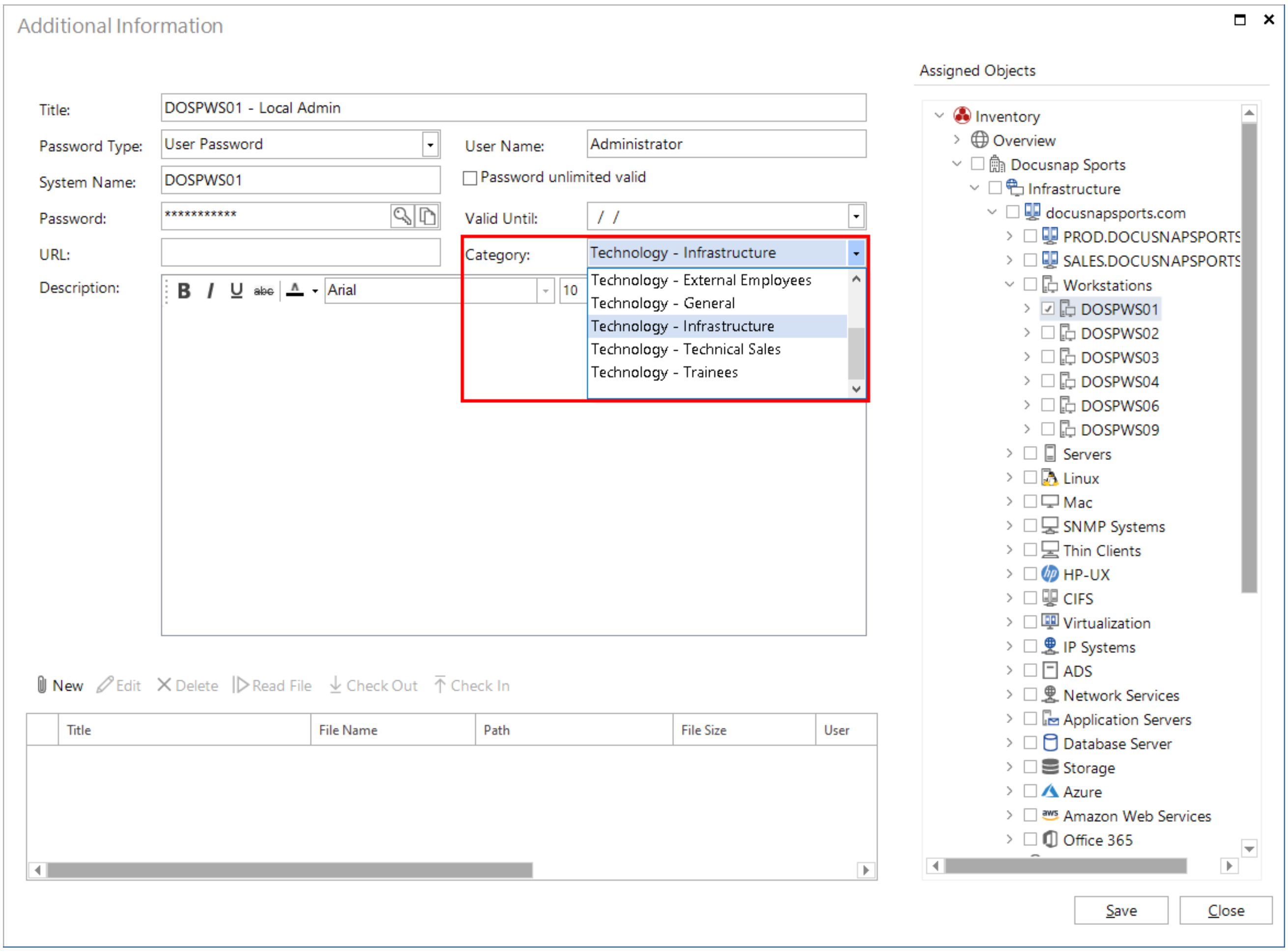
Fig. 17 – Assigning permission categories to Docusnap roles

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: DOSPWS01 - Local Admin
Password Type: User Password
User Name: Administrator
System Name: DOSPWS01
☐ Password unlimited valid
Password: ***********
Valid Until: / /
URL:
Category: Technology - Infrastructure
Description:

Fig. 18 – Permission categories available for additional information

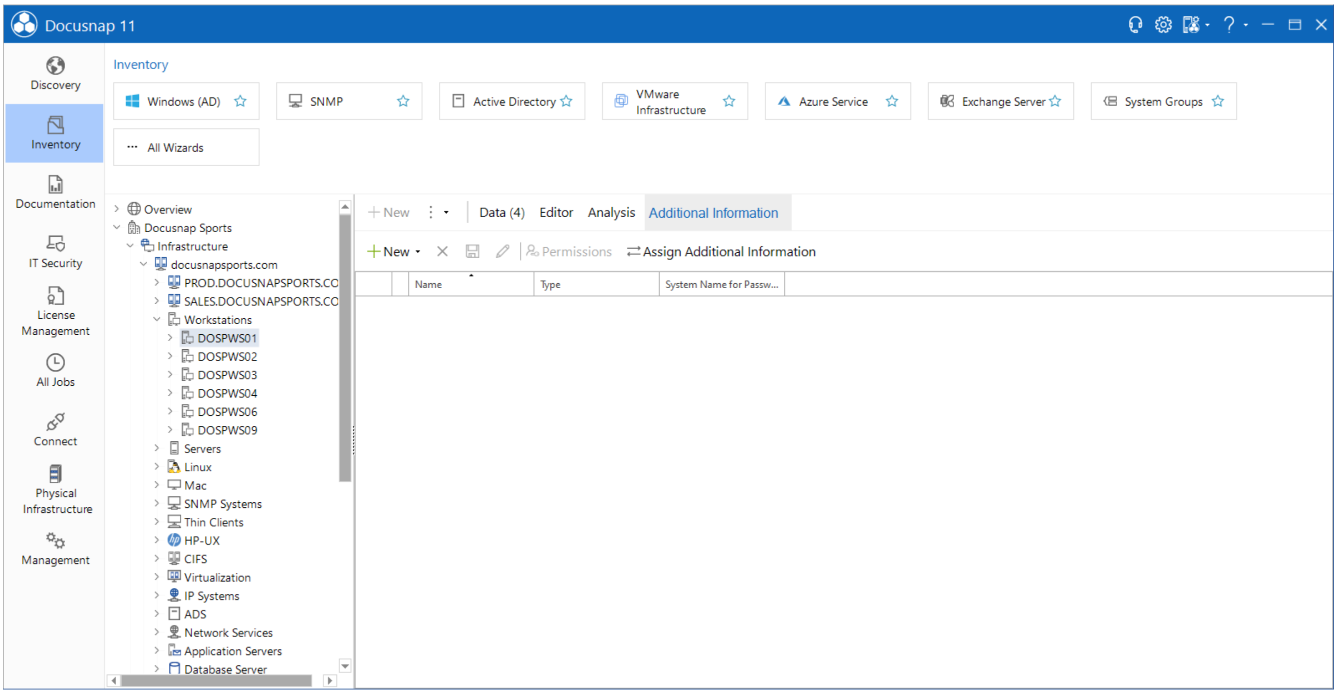
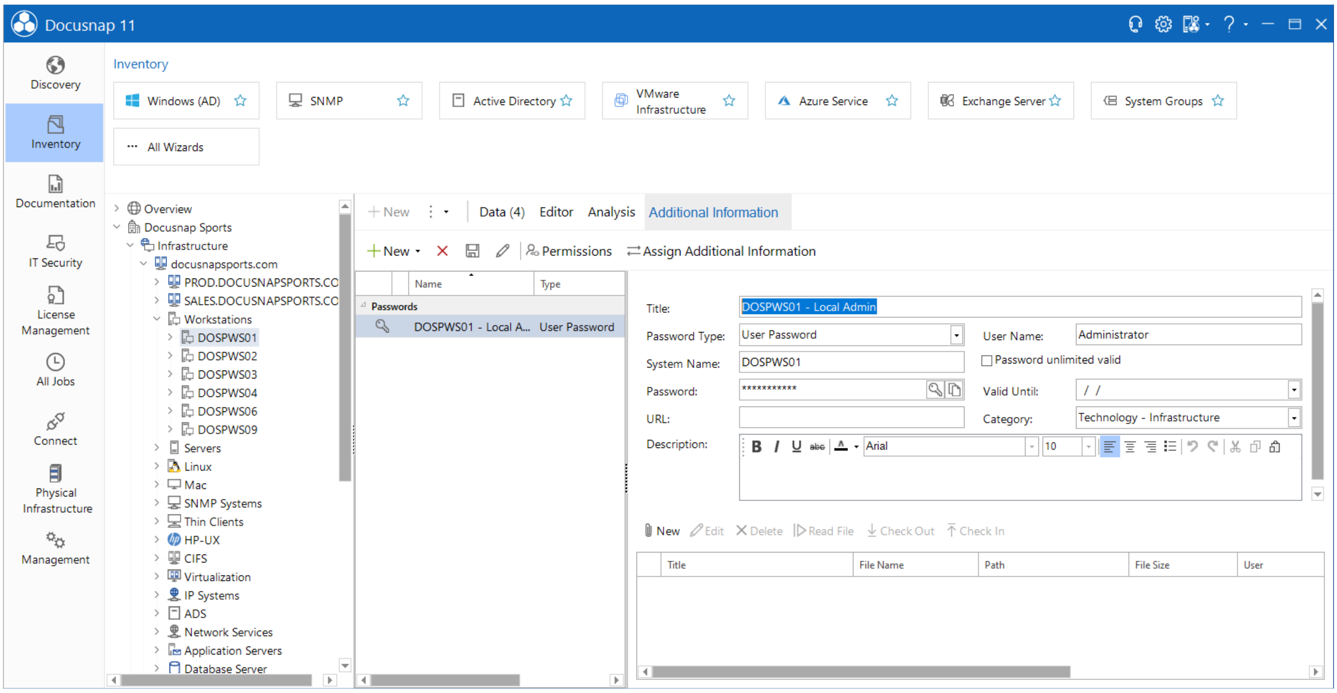


Fig. 19 – View as seen by a user without a permission category assigned



Name	Type
Passwords	
DOSPWS01 - Local A...	User Password

Title: DOSPWS01 - Local Admin

Password Type: User Password

User Name: Administrator

System Name: DOSPWS01

□ Password unlimited valid

Password: ***********

Valid Until: / /

URL:

Category: Technology - Infrastructure

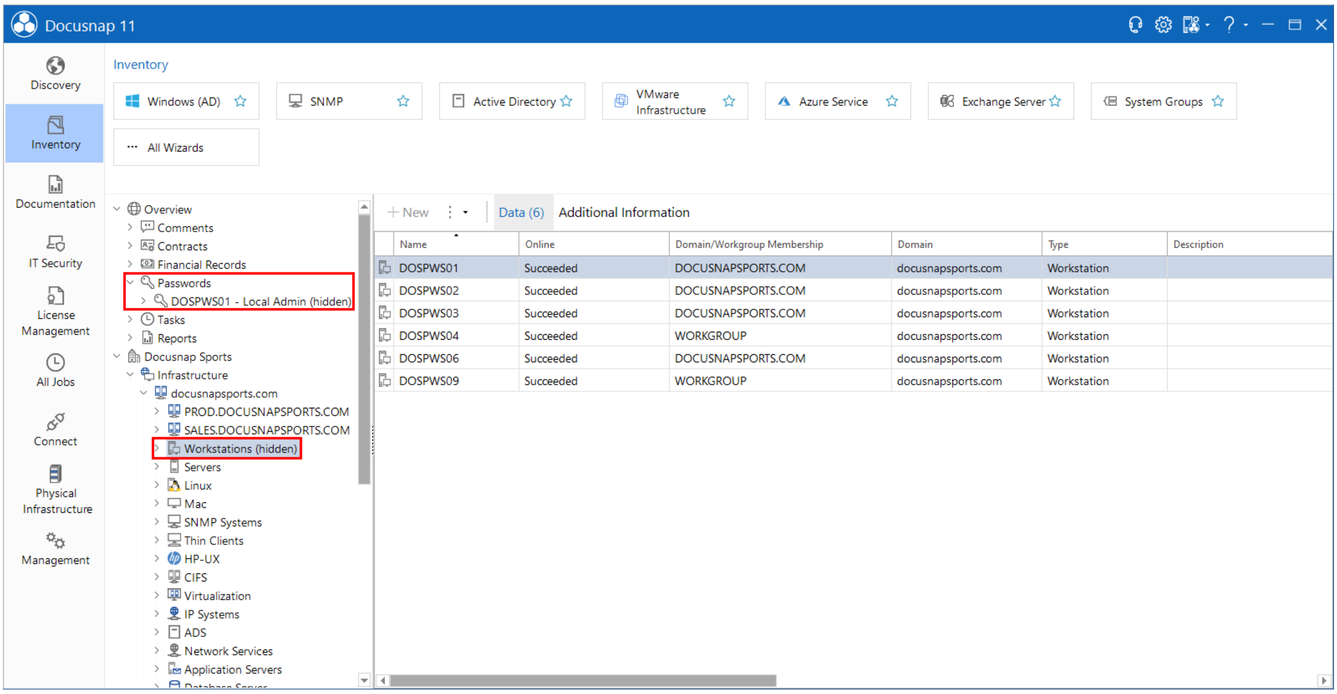
Description:

Fig. 20 – 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.



Name	Online	Domain/Workgroup Membership	Domain	Type	Description
DOSPWS01	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Workstation	
DOSPWS02	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Workstation	
DOSPWS03	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Workstation	
DOSPWS04	Succeeded	WORKGROUP	docusnapsports.com	Workstation	
DOSPWS06	Succeeded	DOCUSNAPSPORTS.COM	docusnapsports.com	Workstation	
DOSPWS09	Succeeded	WORKGROUP	docusnapsports.com	Workstation	

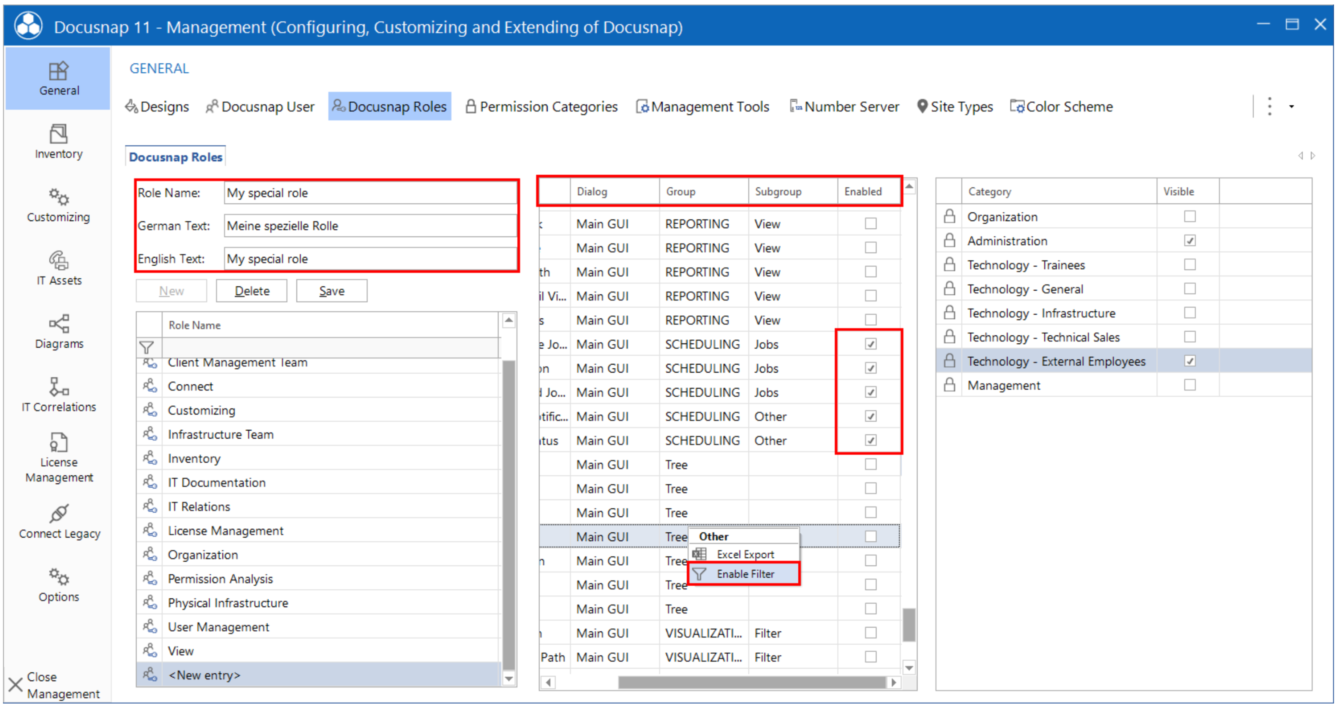
Fig. 21 – Special role Administration

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.



Docusnap 11 - Management (Configuring, Customizing and Extending of Docusnap)

Role Name: My special role

German Text: Meine spezielle Rolle

English Text: My special role

Role Name
Client Management Team
Connect
Customizing
Infrastructure Team
Inventory
IT Documentation
IT Relations
License Management
Organization
Permission Analysis
Physical Infrastructure
User Management
View
<New entry>

	Dialog	Group	Subgroup	Enabled
k	Main GUI	REPORTING	View	☐
	Main GUI	REPORTING	View	☐
th	Main GUI	REPORTING	View	☐
il Vi...	Main GUI	REPORTING	View	☐
s	Main GUI	REPORTING	View	☐
e Jo...	Main GUI	SCHEDULING	Jobs	☑
on	Main GUI	SCHEDULING	Jobs	☑
l Jo...	Main GUI	SCHEDULING	Jobs	☑
tific...	Main GUI	SCHEDULING	Other	☑
tus	Main GUI	SCHEDULING	Other	☑
	Main GUI	Tree		☐
	Main GUI	Tree		☐
	Main GUI	Tree		☐
	Main GUI	Tree		☐
n	Main GUI	Tree		☐
	Main GUI	Tree		☐
	Main GUI	Tree		☐
n	Main GUI	VISUALIZATI...	Filter	☐
Path	Main GUI	VISUALIZATI...	Filter	☐

Category	Visible
Organization	☐
Administration	☑
Technology - Trainees	☐
Technology - General	☐
Technology - Infrastructure	☐
Technology - Technical Sales	☐
Technology - External Employees	☑
Management	☐

Fig. 22 – 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 User Management report can be found under Overview – Reports - Docusnap. Once you have opened the report, you are prompted to select the users or groups that you added to the Docusnap User Management.

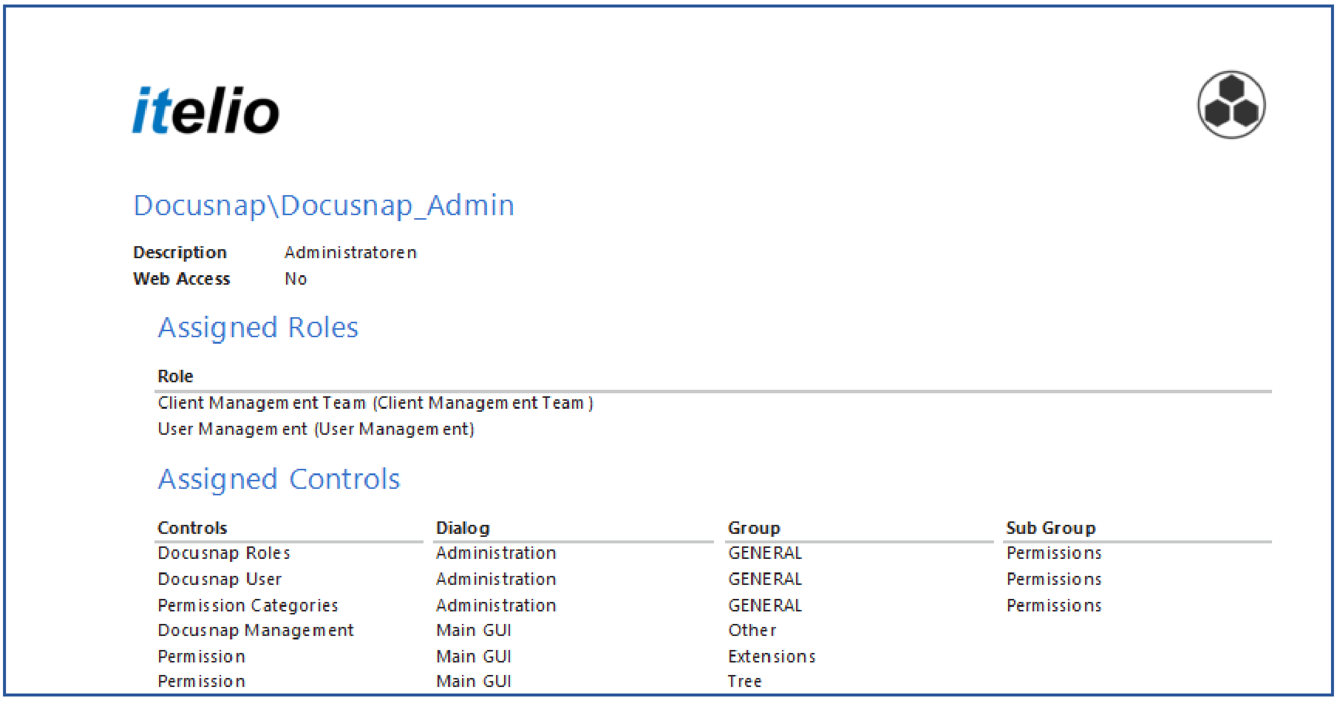
The other options allow you to specify the level of detail for the report:

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.



itelio

Docusnap\Docusnap_Admin

Description Administratoren
Web Access No

Assigned Roles

Role
Client Management Team (Client Management Team)
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
Docusnap Management	Main GUI	Other	
Permission	Main GUI	Extensions	
Permission	Main GUI	Tree	

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
April 27, 2020	Version 2.0 - Revision of the HowTos for Docusnap 11