



User Management

Managing User Access to DocuSnap

TITLE	User Management
AUTHOR	Docusnap Consulting
DATE	12/12/2023
VERSION	4.0 valid from November 13, 2023

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	4
2. Introduction	5
2.1 Important Terms	6
3. User Management in Docusnap	7
3.1 Docusnap Roles	7
3.2 Docusnap Users	7
4. Restricting Access to Types and Objects in the Data Explorer	8
4.1 Difference between types and objects	8
4.2 Restrict the visibility of types and objects	9
4.3 Restrict the editing options of types and objects	9
4.4 Tenant separation for Docusnap Permissions	11
4.5 Best Practice for Setting Permissions to Types and Objects	11
5. Permission Categories	12
5.1 Managing Permission Categories	12
5.2 Creating Additional Information Using Permission Categories	13
6. Special Role: Administration	14
7. Adding Docusnap Roles	14
8. Documenting the User Management Settings	15

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:

- 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

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.

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.

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.

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.

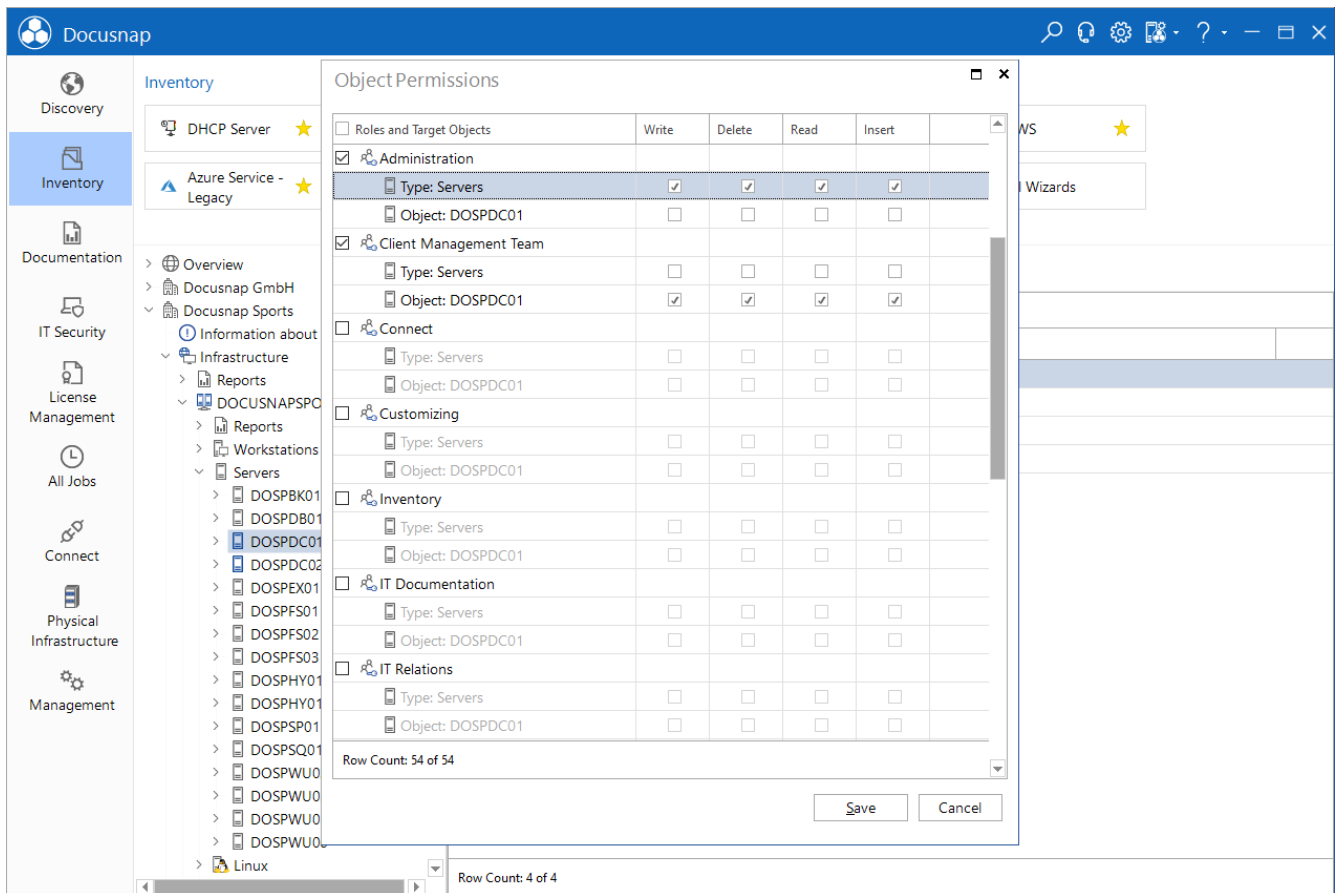


Fig. 1 – Object Permissions – Type vs. Object

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 DOSPDC01:

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: DOSPDC01

This object represents the explicitly selected DOSPDC01 Server object. Now, select a role and enable the checkboxes for Object: DOSPDC01. Members of this role will only see the DOSPDC01 server object within the Data Explorer.

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** window 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.

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

The screenshot shows the 'ObjectPermissions' dialog box in the Docusnap application. The dialog is titled 'ObjectPermissions' and has a close button (X) in the top right corner. It contains a table with columns for 'Roles and Target Objects', 'Write', 'Delete', 'Read', and 'Insert'. The table lists several roles, each with a 'Type' and 'Object' (both 'Workstations'). The '3rd Level Support' role is highlighted in blue, and its 'Type: Workstations' row has all four permission checkboxes checked. Other roles like '1st Level Support', '2nd Level Support', 'Administration', 'Client Management Team', 'Connect', and 'Customizing' have various combinations of checked and unchecked checkboxes. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons. The background shows the Docusnap interface with a left sidebar and a main content area.

Roles and Target Objects	Write	Delete	Read	Insert
<input checked="" type="checkbox"/> 1st Level Support				
Type: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Object: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> 2nd Level Support				
Type: Workstations	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Object: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> 3rd Level Support				
Type: Workstations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Object: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Administration				
Type: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Object: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Client Management Team				
Type: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Object: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Connect				
Type: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Object: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Customizing				
Type: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Object: Workstations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Fig. 2 – 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.

If you want to assign specific permissions for the existing tenants, you can activate this in the

- 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).

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.

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.

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 made 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.

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.

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.

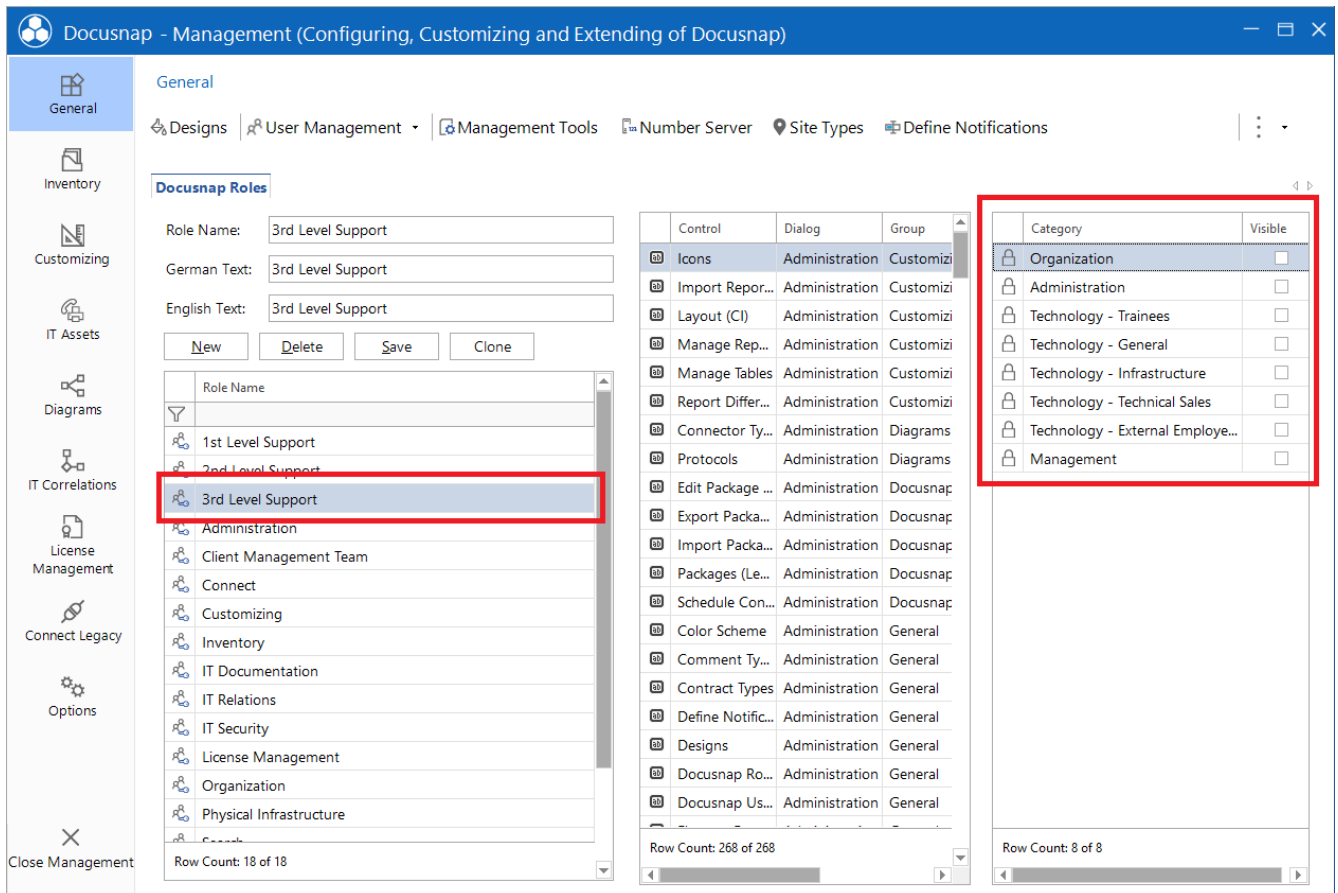


Fig. 3 – Assigning permission categories to Docusnap roles

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.

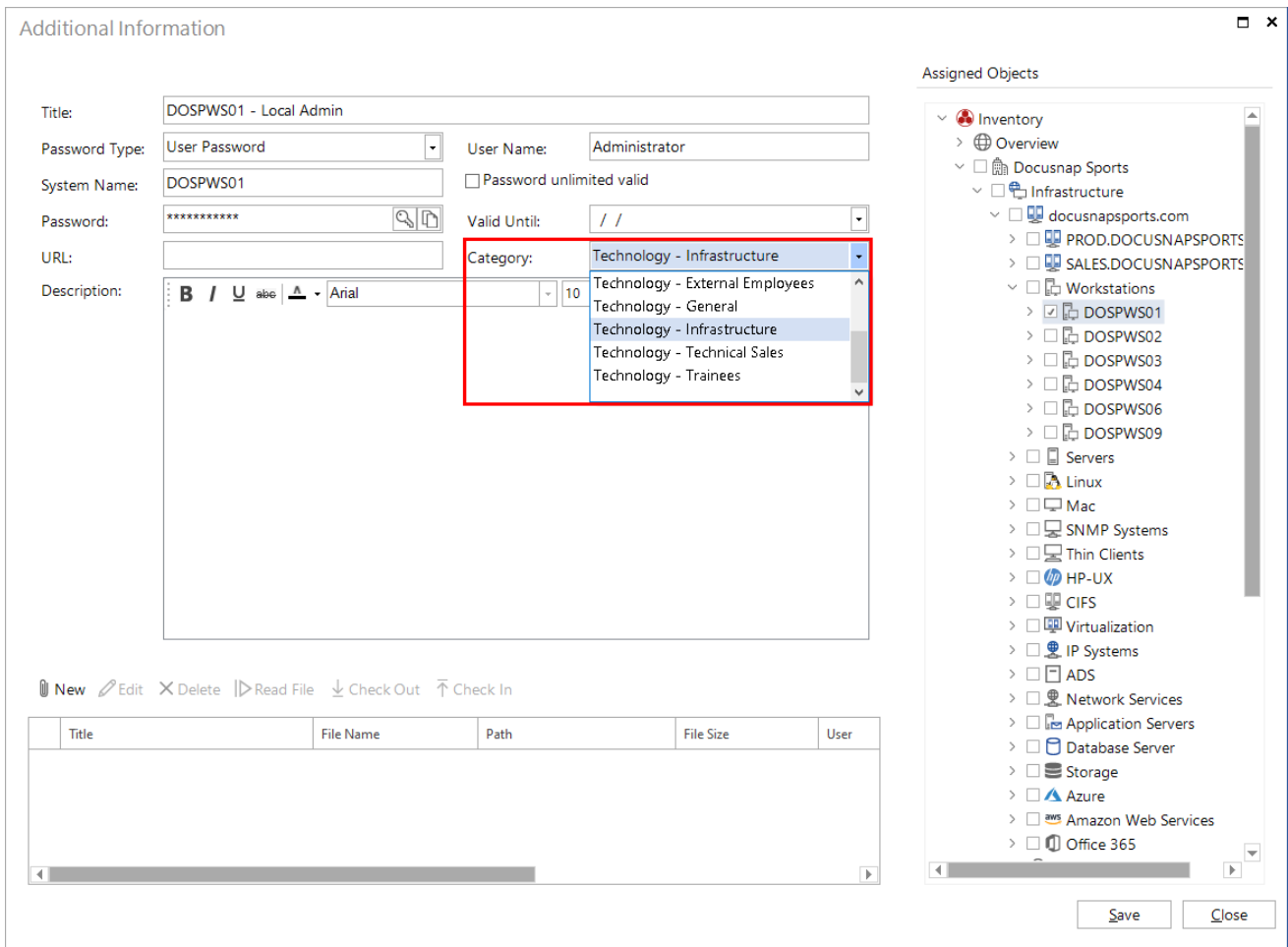


Fig. 4 – Permission categories available for additional information

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.

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.

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

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.

LIST OF FIGURES

FIG. 1 – OBJECT PERMISSIONS – TYPE VS. OBJECT 8

FIG. 2 – SETTING PERMISSIONS FOR EDITING OBJECTS10

FIG. 3 – ASSIGNING PERMISSION CATEGORIES TO DOCUSNAP ROLES12

FIG. 4 – PERMISSION CATEGORIES AVAILABLE FOR ADDITIONAL INFORMATION13

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 HowTo for Docusnap 11
December 16, 2022	Version 3.0 – Revision of the HowTo for Docusnap 12
November 13, 2023	Version 4.0 – Revision of the HowTo for Docusnap 13
