Docusnap Web

Configuring a Company-Specific Access to Docusnap Web

TITLE	Docusnap Web
AUTHOR	Docusnap Consulting
DATE	11/20/2020
VERSION	2.0 | valid as of October 01, 2020

TABLE OF CONTENTS

1. Introduction

With Docusnap it is possible to access the Docusnap database via browser. This allows database access (with read permission) and the output of plans and reports for any employee or customer without the need to install a Docusnap client.

Please note that client-specific access to the database, both via the client and via Docusnap Web, may incur license costs for the Microsoft SQL Server and this must be checked in advance.

Docusnap uses a role-based user administration that enables you to restrict the data to be accessed by users and groups to the desired level.

This HowTo shows how to restrict access to Docusnap Web using the user administration.

1.1 Installing and Configuring Docusnap Web

As it is assumed that Docusnap Web has already been installed and fully configured, the installation and configuration of the application will not be discussed in this HowTo document.

A corresponding HowTo, which describes the installation and configuration, can be found in our Knowledge Base.

1.2 Application Example – Restricting the Access to Docusnap Web

This example describes how to ensure for a Docusnap environment with two clients that Client A and Client B only have access to their own Docusnap data.

2. Docusnap Web – Authentication Scheme

2.1 Configuring the Authentication Scheme

In step four of the Docusnap Server configuration wizard, *Server API*, you can specify the valid authentication methods for accessing Docusnap Web:

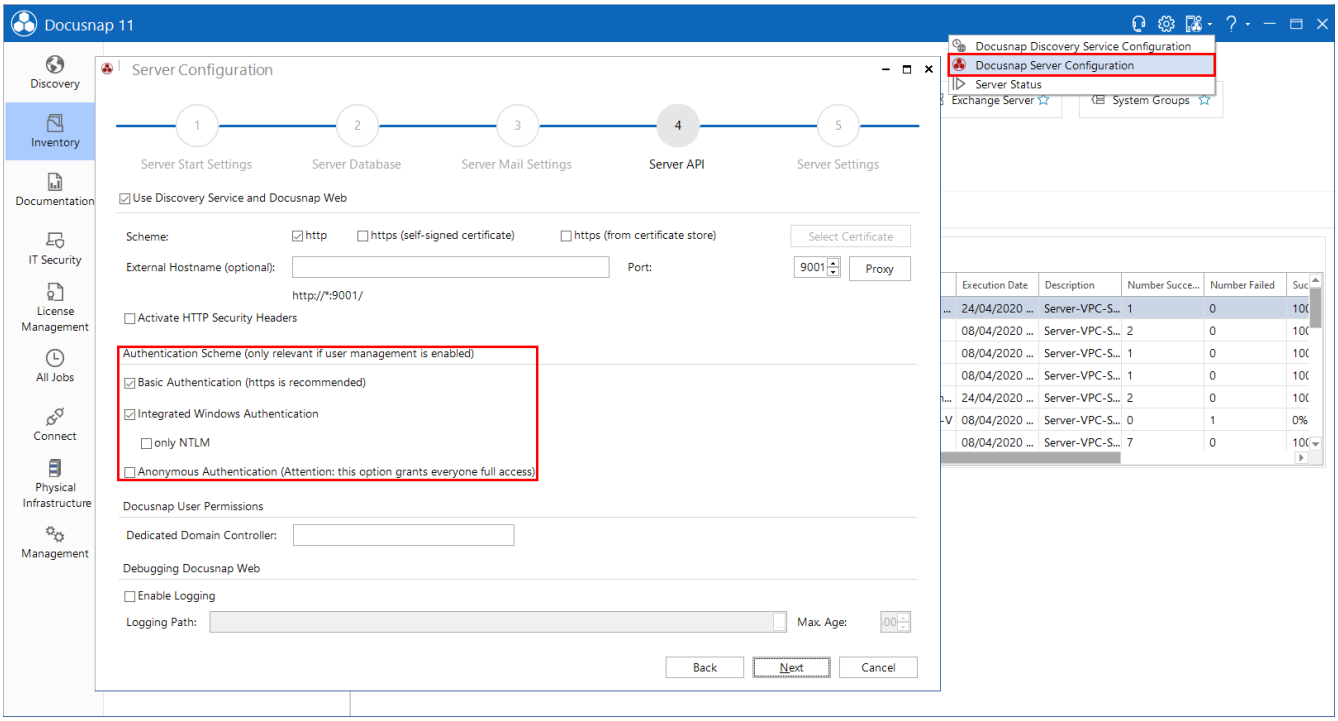

Figure 1 – Configuring the authentication scheme

2.2 Anonymous Authentication

If you select **Anonymous Authentication**, all other authentication methods are disabled automatically. There will be no permission checks, i.e. every user has unlimited access to Docusnap Web. This is especially worrisome if the server API and thus Docusnap Web is accessible from outside, as you use Docusnap Discovery Services for inventorying decentralized environments.

2.3 Basic Authentication

Basic Authentication means that the user must enter his/her username and password each time he/she wants to access Docusnap Web. The user password is sent to Docusnap Web as plain text, i.e. in unencrypted form.

With this method, you can grant users outside your own domain access to Docusnap Web. In productive use, however, it is strongly recommended, to use HTTPS for the access to Docusnap Web to make sure that the password is encrypted before transmission.

2.4 Integrated Windows Authentication

This method is recommended to grant users within your own domain access to Docusnap Web. ADS security groups and users as well as local users (not recommended) can be granted access directly in Docusnap. In contrast to the Basic Authentication method, Integrated Windows Authentication uses the ADS for user account management.

Please note that Single Sign-On cannot be guaranteed in every environment.

2.5 Combined Use of Integrated Windows Authentication & Basic Authentication

It is possible to use both methods in a combined authentication scheme. This way, you can set up easy access for internal users and controlled access for external users.

3. Docusnap user management

This chapter briefly explains the Docusnap User Management feature on which the content of this HowTo document is based. Only the functionality required for this example will be discussed. You can find further information in our Knowledge Base in the HowTo: Docusnap User Management.

3.1 User Management Overview

By default, User Management is disabled, i.e. every user can access all features and data of the Docusnap database. Creating the first user automatically enables the User Management feature. From this time on, users can only access features for which they have explicitly been granted permission. Access to data is still unlimited at this point, but once you have set permissions to specific object classes or objects, permission checks will be carried out.

You can open the Docusnap Roles and Docusnap User dialogs from the General tab of the Docusnap Management:

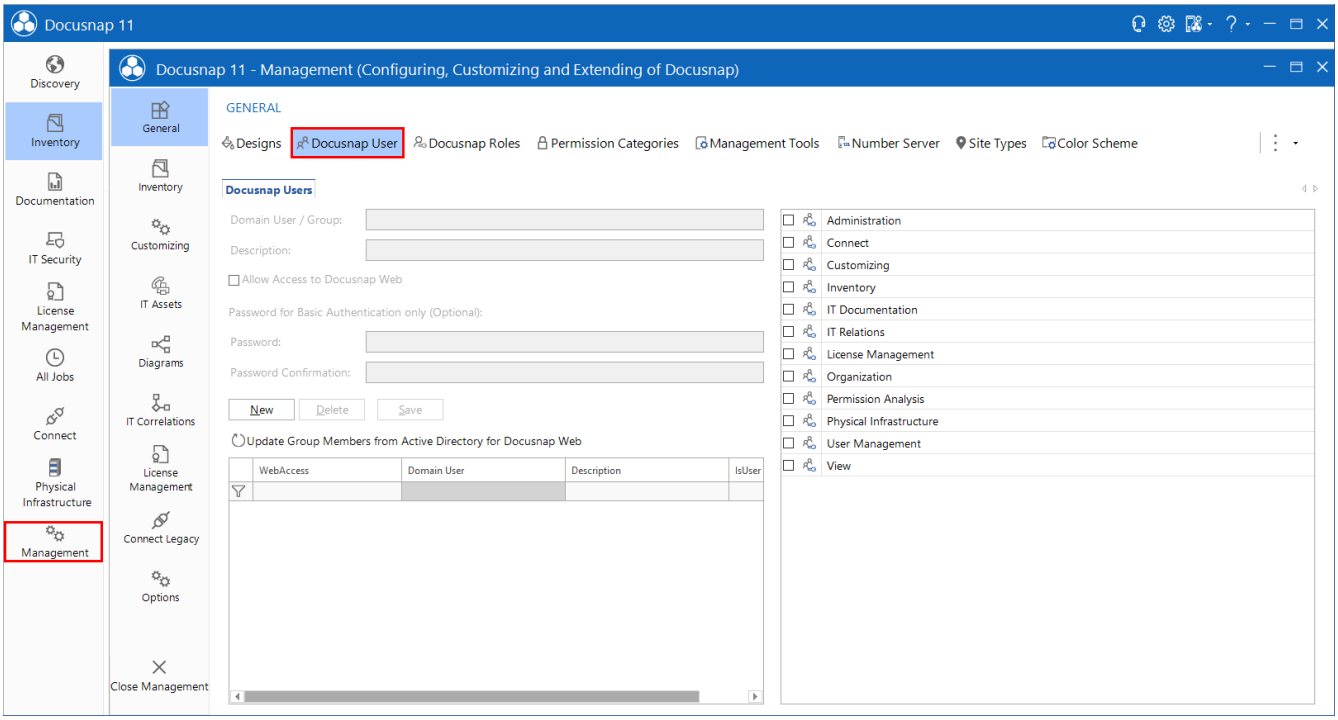

Figure 2 – Docusnap User Management

3.1.1 Docusnap Roles

The Docusnap User Management feature allows you to restrict the access to any user interface controls. Roles are used to make this a straightforward process. A role is a collection of access rights to the Docusnap controls. Docusnap comes with standard roles, so that you can easily limit the access for users to read-only (View role). These standard roles cannot be modified by the end customer. In this dialog, you can define additional roles to which you can freely assign any desired user permissions.

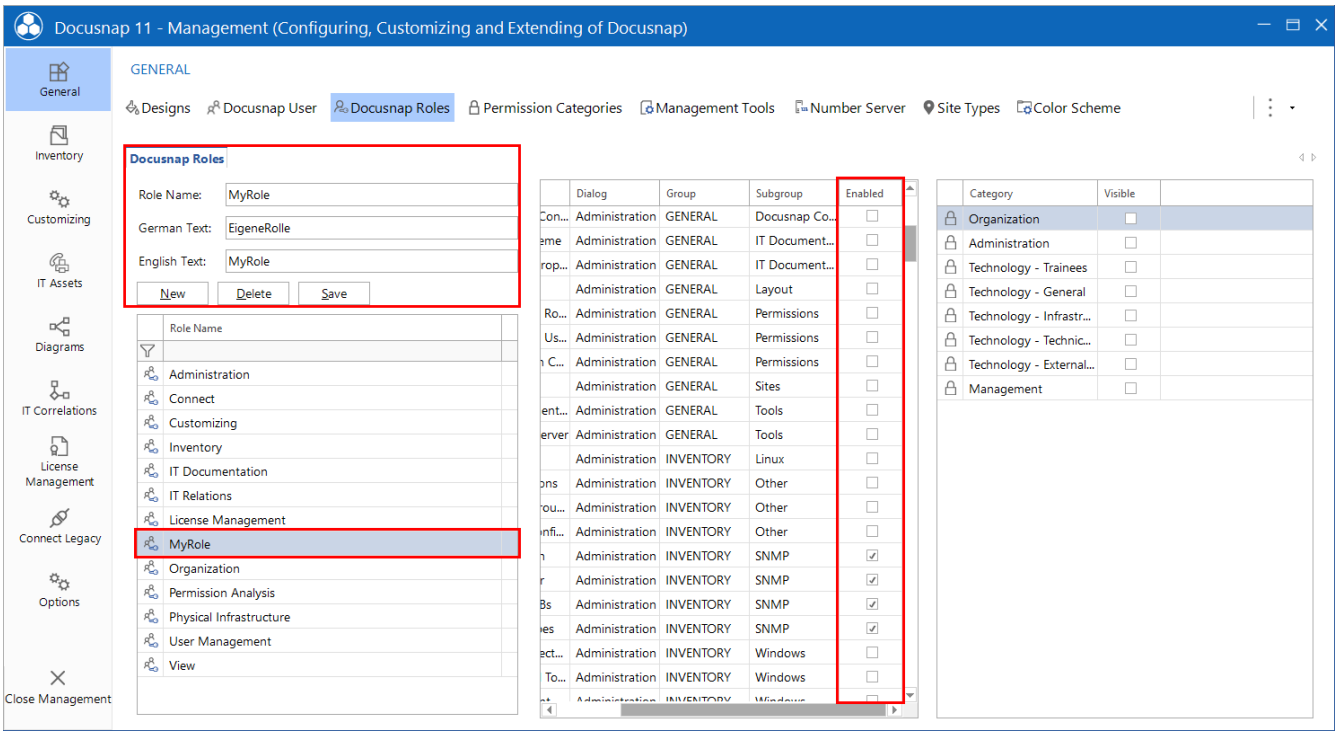

Figure 3 – Creating custom roles

3.2 Docusnap User

Open the Docusnap Users dialog to grant ADS users or ADS groups access to the Docusnap Client or to Docusnap Web. In addition, you can create new users to grant them access to Docusnap Web through the Basic Authentication method.

The access to Docusnap / Docusnap Web is managed by assigning roles. A user who has not been assigned a role cannot access the respective features or data.

Important: Make sure that you yourself or an ADS group of which you are a member is registered in the Docusnap User Management and that you or the respective ADS group have/has been assigned the Administration role. Otherwise, all controls will be grayed out when you start Docusnap the next time and you will no longer be able to use the application!

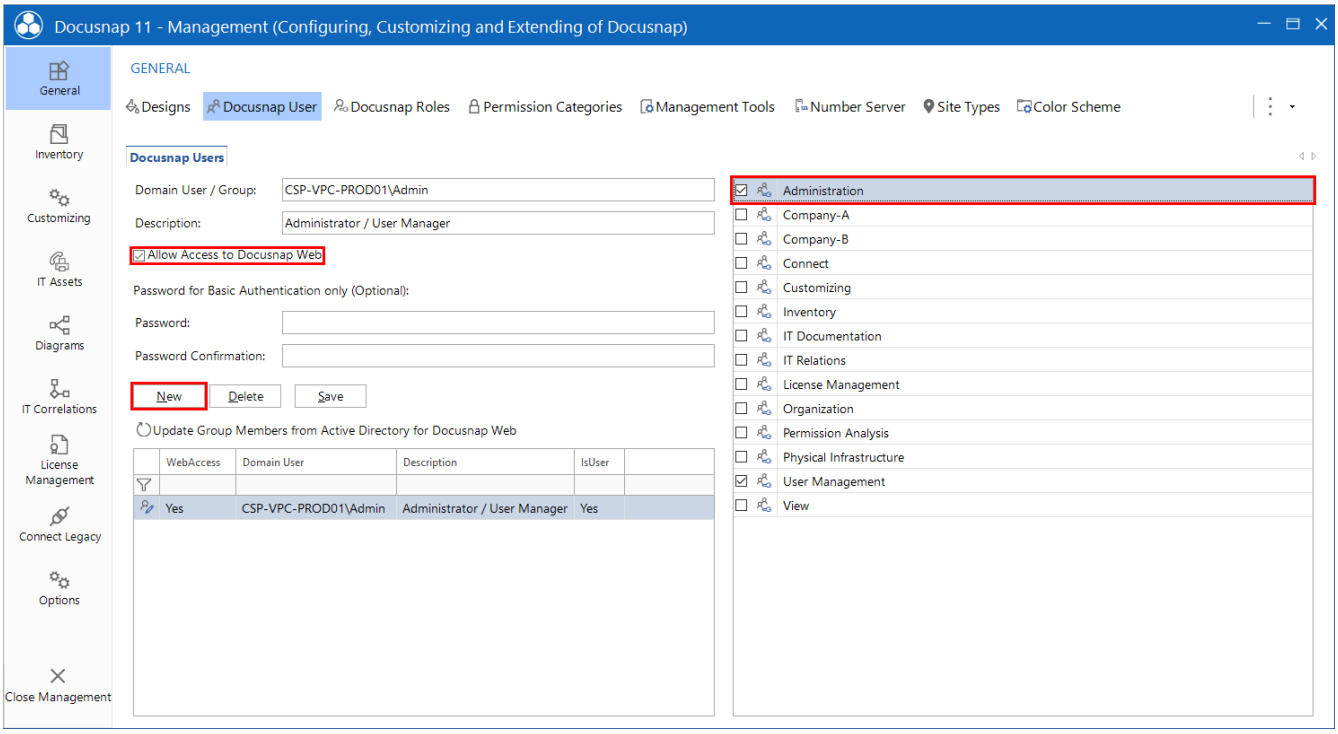

Figure 4 – Creating Docusnap users with the Administration role

3.3 Docusnap User Management – Object Classes and Objects

Once the Docusnap User Management feature has been enabled, you can restrict the access not only to features, but also to database data. Now, it is possible to select an item in the tree view and select additional permission settings from the context menu.

In this example, the Server DOSPDC01 was selected, and with a right-click, the Object Permissions dialog was launched. Users with the Administration role are granted full access to the Server type object class. This right will now apply to all objects of the Server type. Alternatively, it could have been assigned exclusively to the object DOSPDC01. In this case, the assignment would have no effect on the access rights of the Administration role to other objects of the Server type:

5

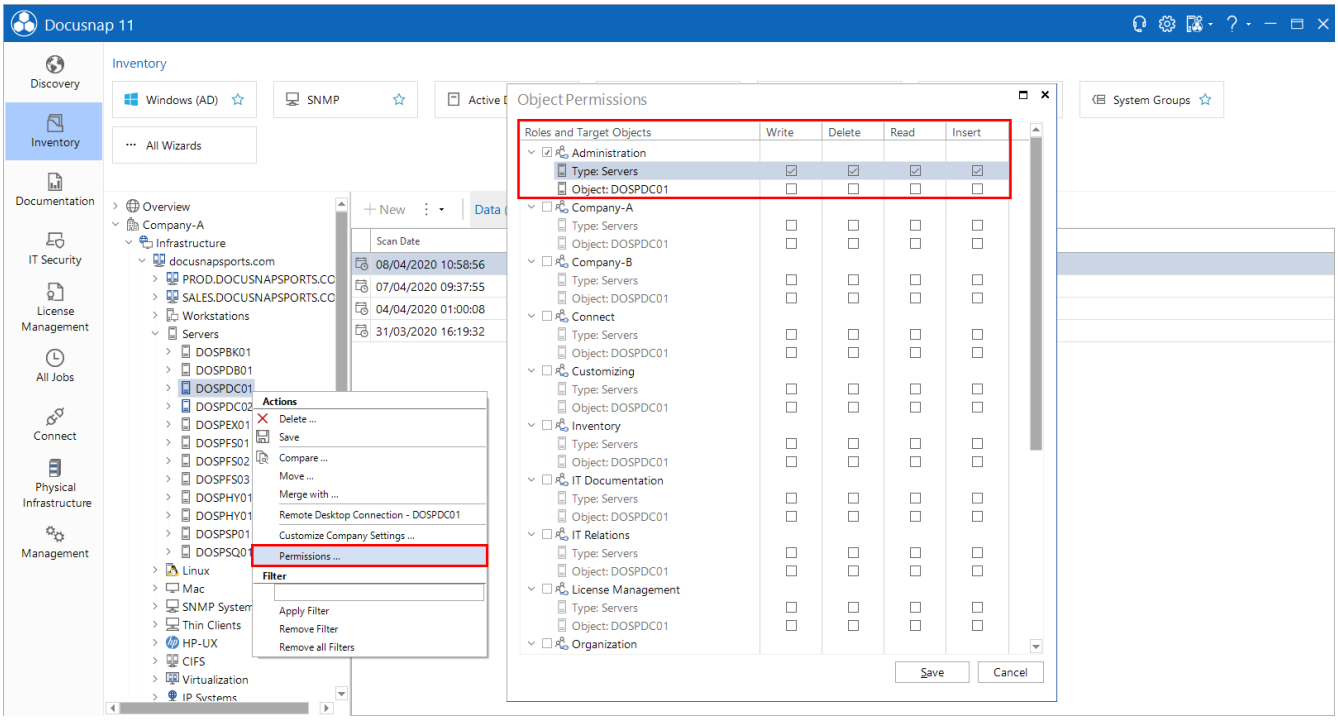

Figure 5 – Assigning access rights to Server objects to users with the Administration role

4. Configuring Docusnap Web Access Rights – Example

After this brief description of the relevant Docusnap User Management features, we will now show how they are implemented in the application example.

4.1 Requirement

You want to grant two customers (called "Company-A" and "Company-B") access to parts of your Docusnap database. You must make sure to both minimize the administrative effort and to define the permissions in such a way that both customers can only access their own data. Both must not be able to access data of the respective other company.

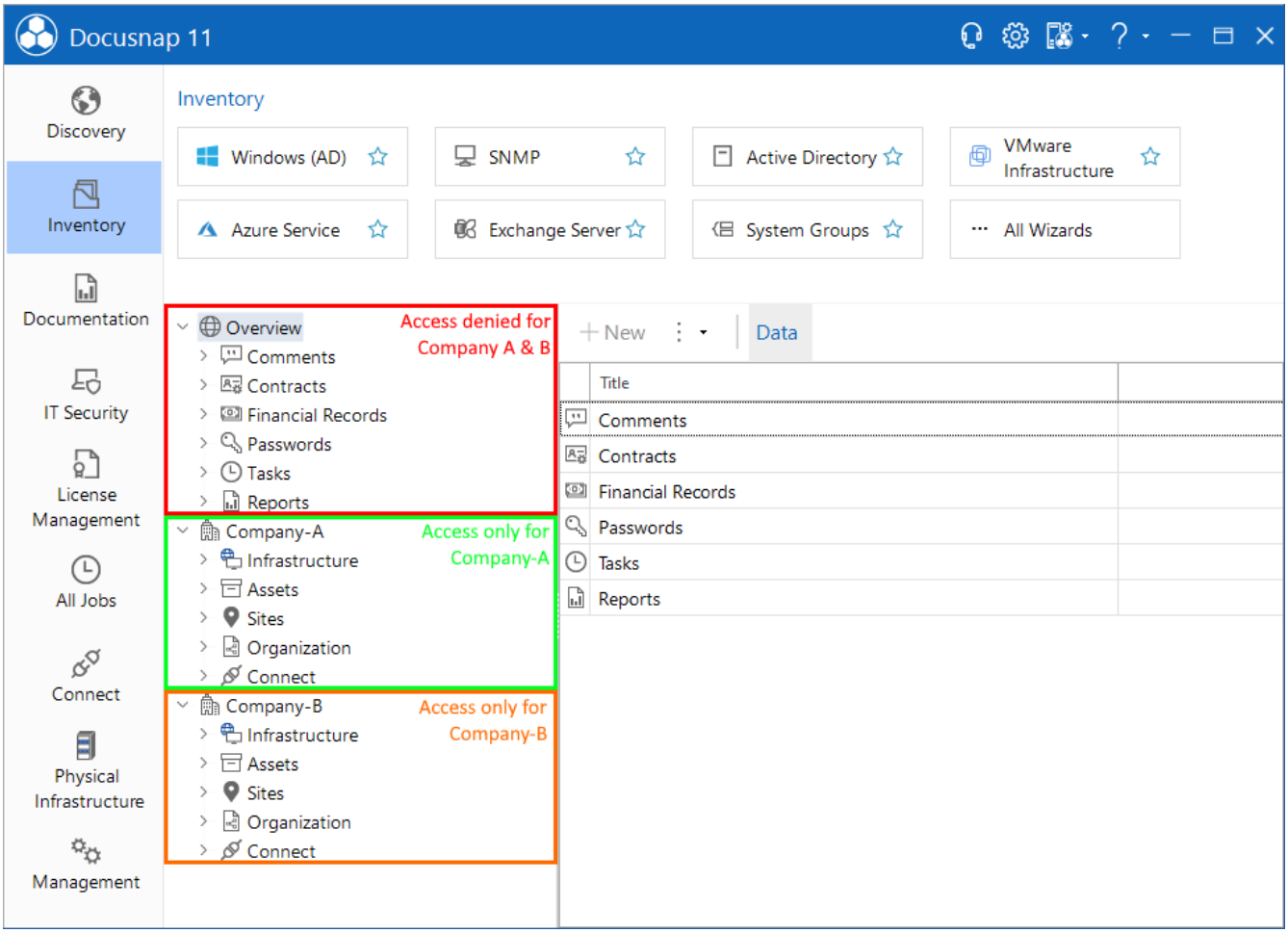

Figure 6 – Permission example – Requirement

4.2 Basic Setup of the Docusnap User Management

In this example, both Basic- and Integrated Windows Authentication will be used as the Docusnap Web authentication scheme. Docusnap User Management is enabled, and the user defined for you has been assigned the Administration and User Management role. For the access to Docusnap Web, users "Company-A" and "Company-B" have been created and set to "Basic Authentication". Both have been assigned the password "test".

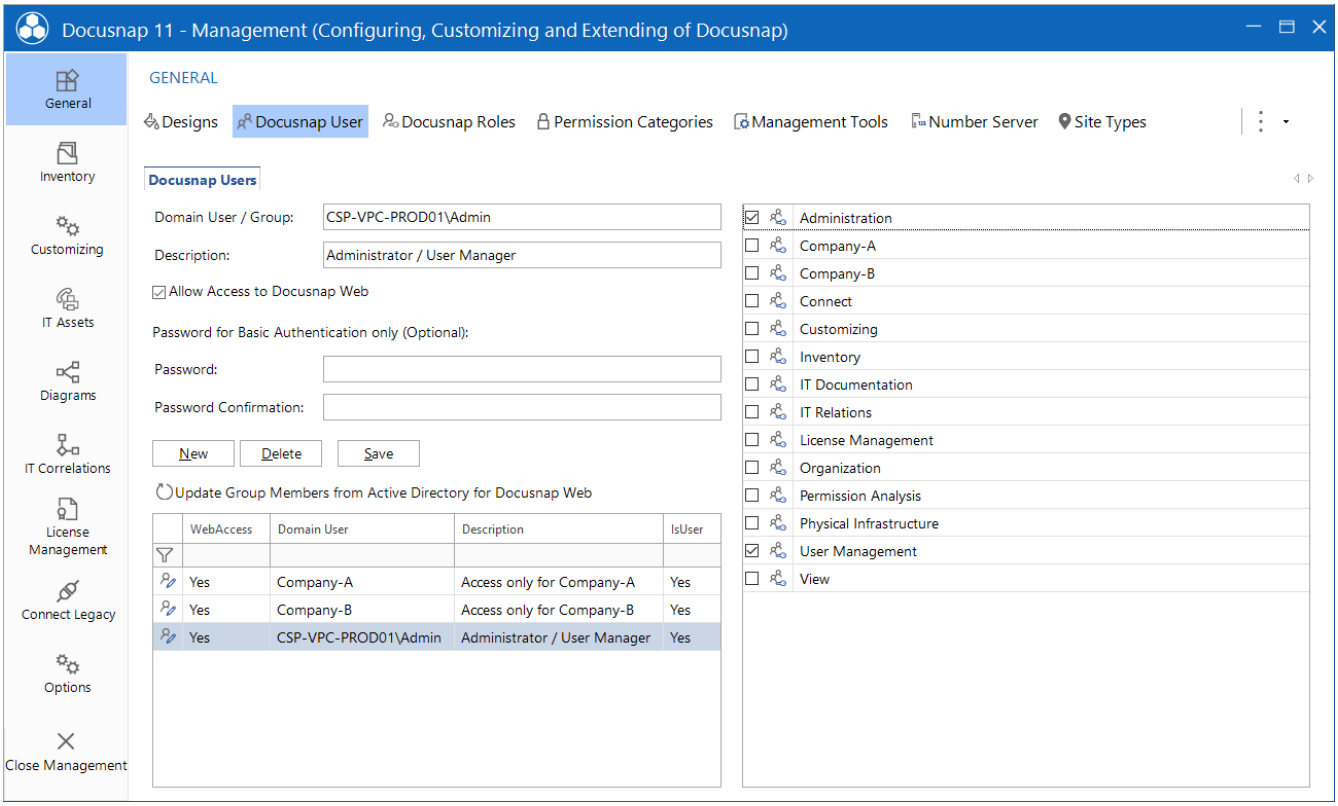

Figure 7 – Permission management – Basic settings

4.3 Testing the Basic Settings

Perform an initial connection test by logging in as the user "Company-B" (Basic Authentication). The login attempt was successful, and the user may access Docusnap Web, but currently this applies to the data of all companies:

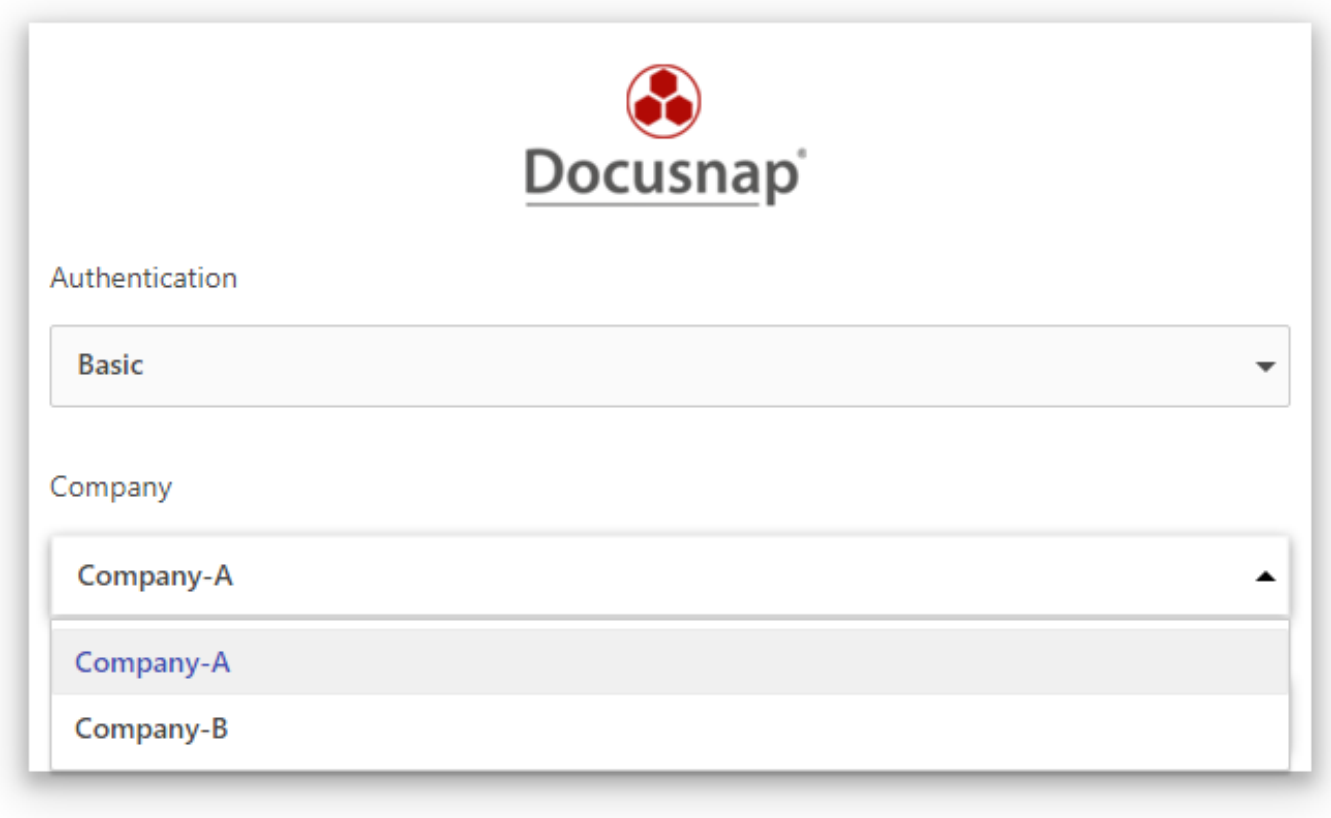

Figure 8 – Docusnap Web access is working (user can access all companies)

4.4 Step One – General Restriction of Access Rights

In the first step, access to the Overview object type is restricted in such a way that only users with the Administration role are granted access.

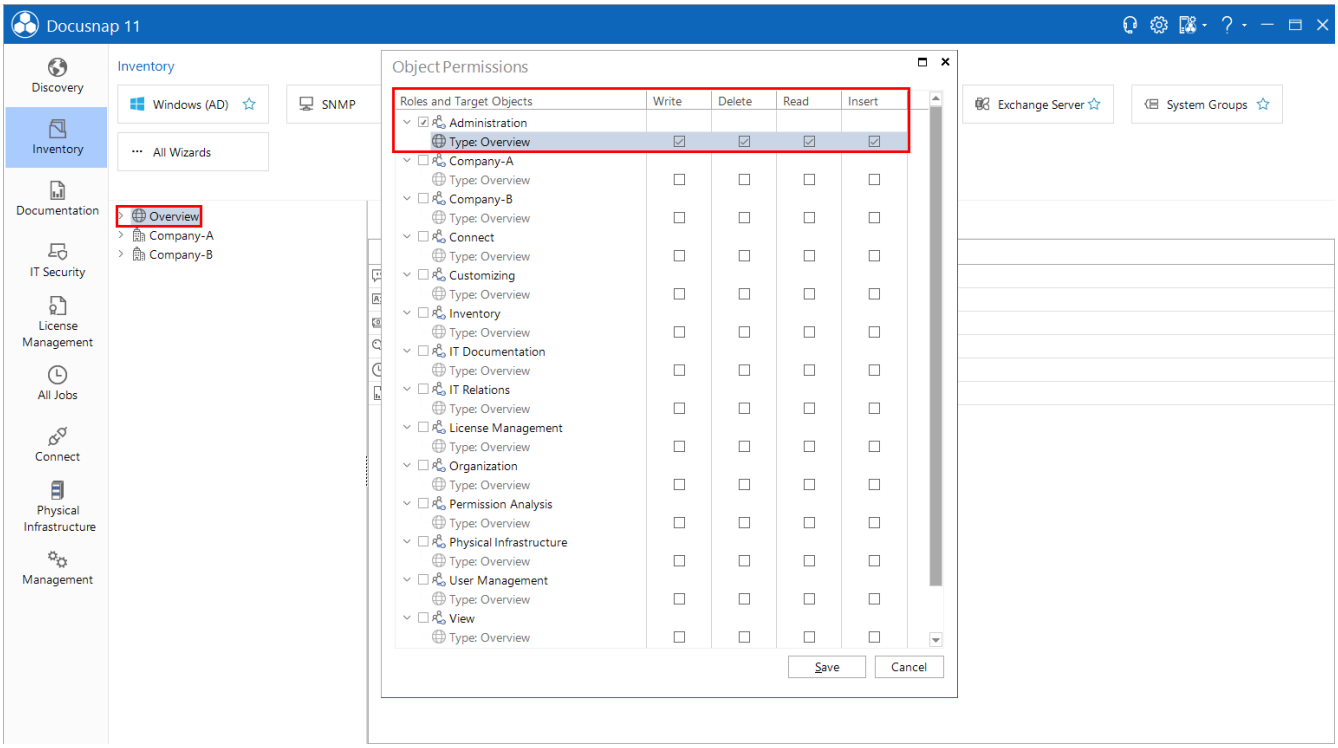

Figure 9 – Restricting access to the Overview object type (Administration role only)

Now, the right to access the Company object type is also restricted to the Administration role:

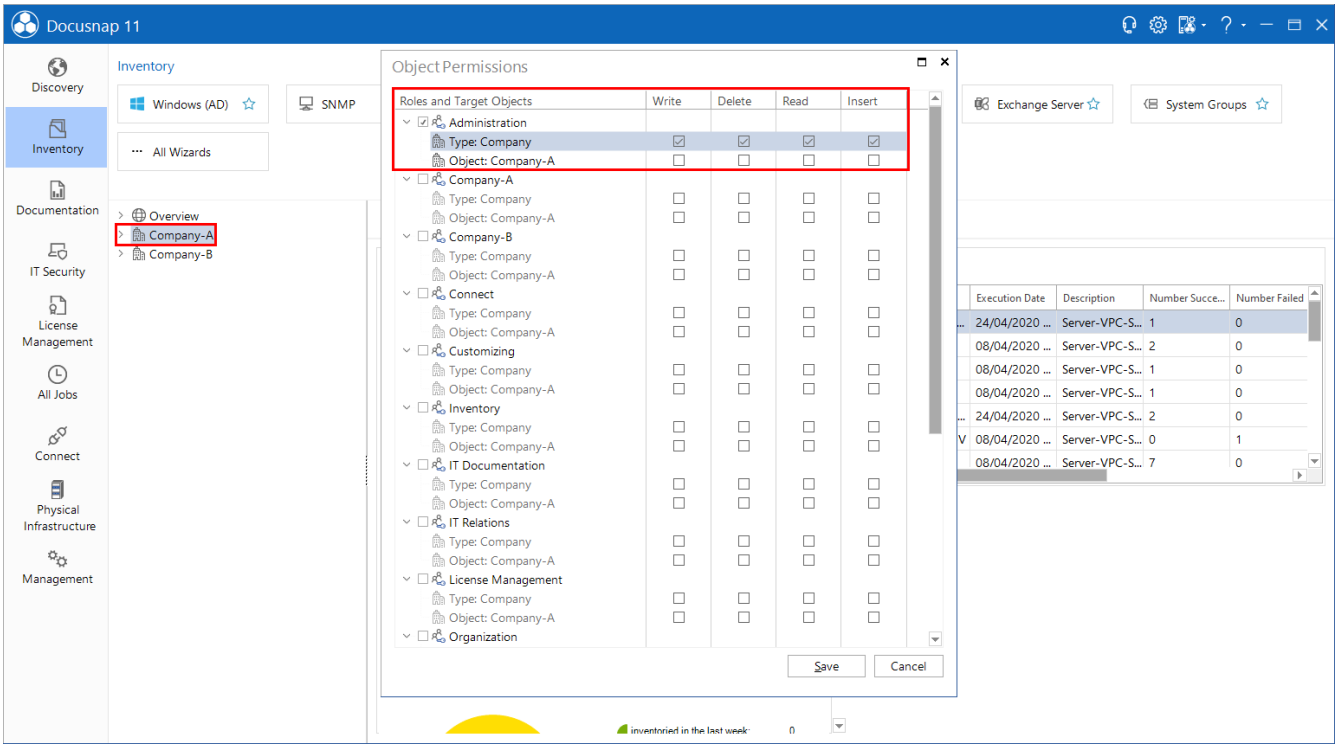

Figure 10 – Restricting access to the Company object type (Administration role only)

4.5 Testing the Changes Made in Step One

Perform a new connection test by logging in as the user “Company-B”:

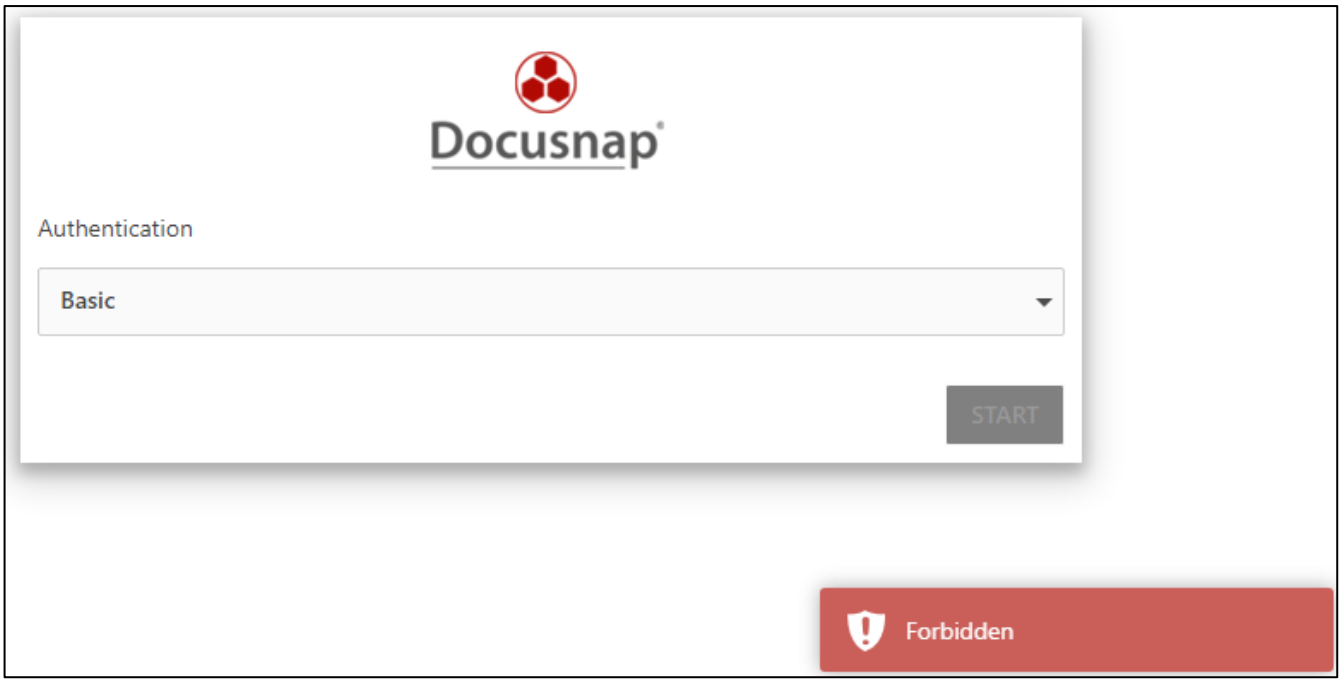

Figure 11 – Login attempt after access rights editing

4.5.1 Why Did the Login Attempt Fail?

Due to the permission adjustments, only users with the Administration role can access objects of the Company object class. The access rights of the users Client A and Client B have been completely removed.

4.6 Step Two – Granting Companies Access Rights to their Data

Now, a new role will be created for each user and assigned to the respective Company. Here, no controls will be assigned to the roles. The roles are only used to define access rights to customer data.

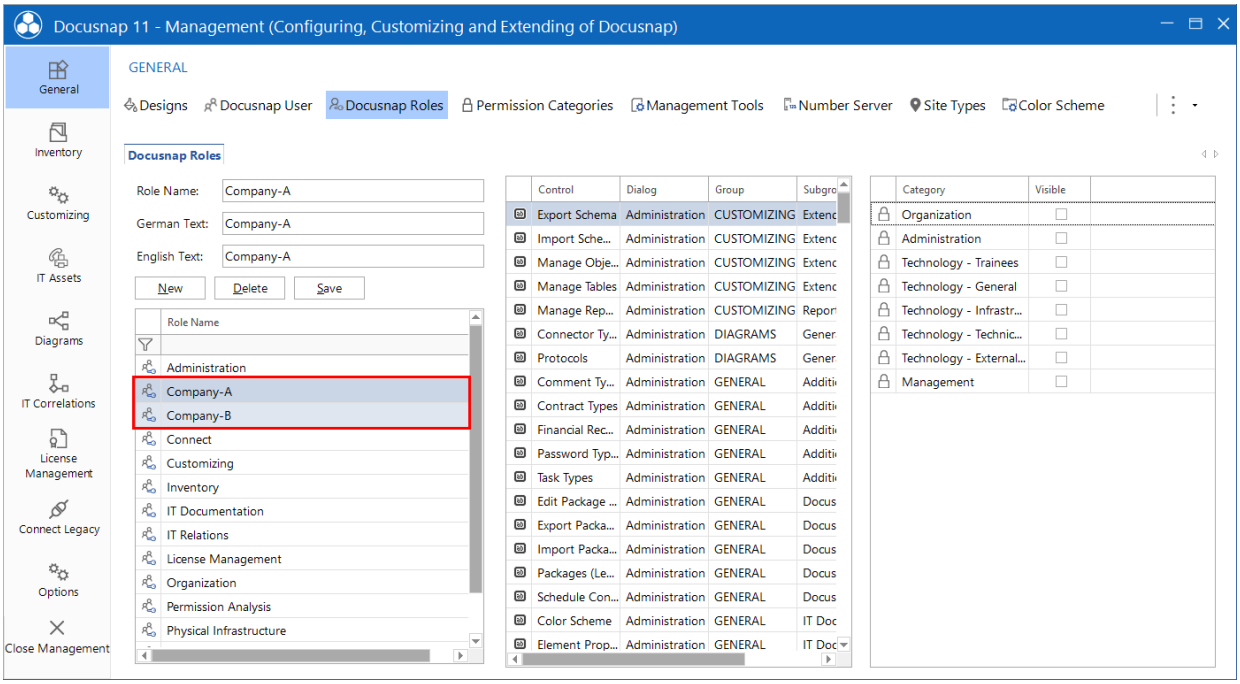

Figure 12 – Creating the Company-A and Company-B roles

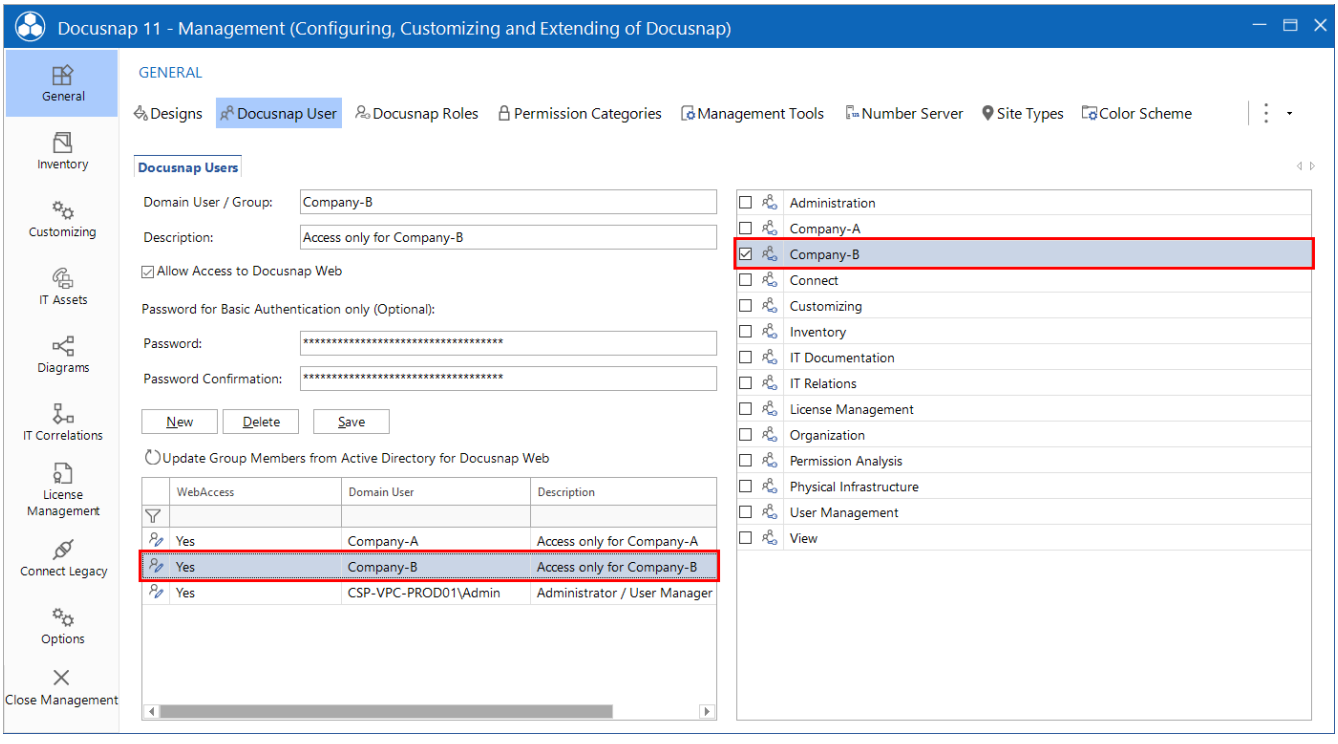

Figure 13 – Assigning the respective role to the user

Now, each company has been granted the required access rights. The Company-A role is granted View permission to the Company-A object. The rights for the Company-B role are assigned accordingly. Please note that the rights only refer to a object, not to the entire object class!

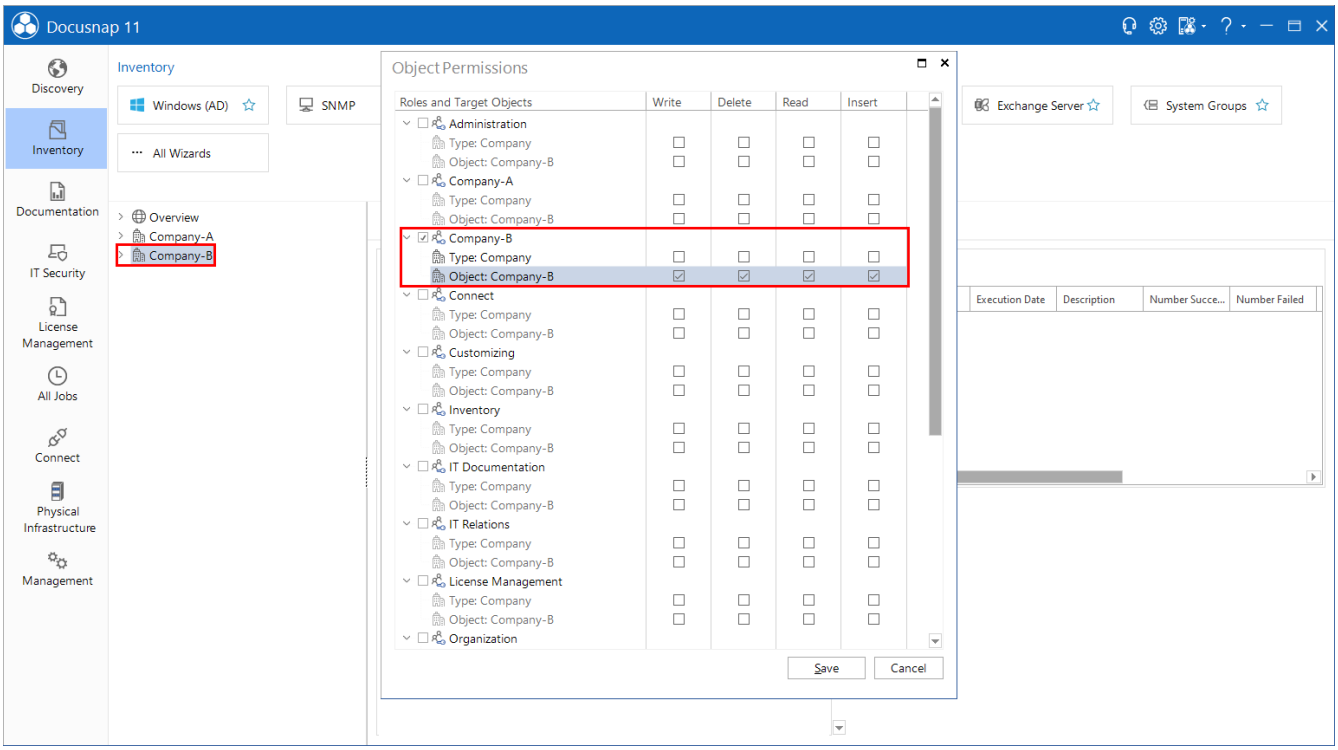

Figure 14 – Granting permissions to the new company roles

4.7 Testing the Changes Made in Step Two

Now, user "Company-B" can only access the data of the Company-B object.

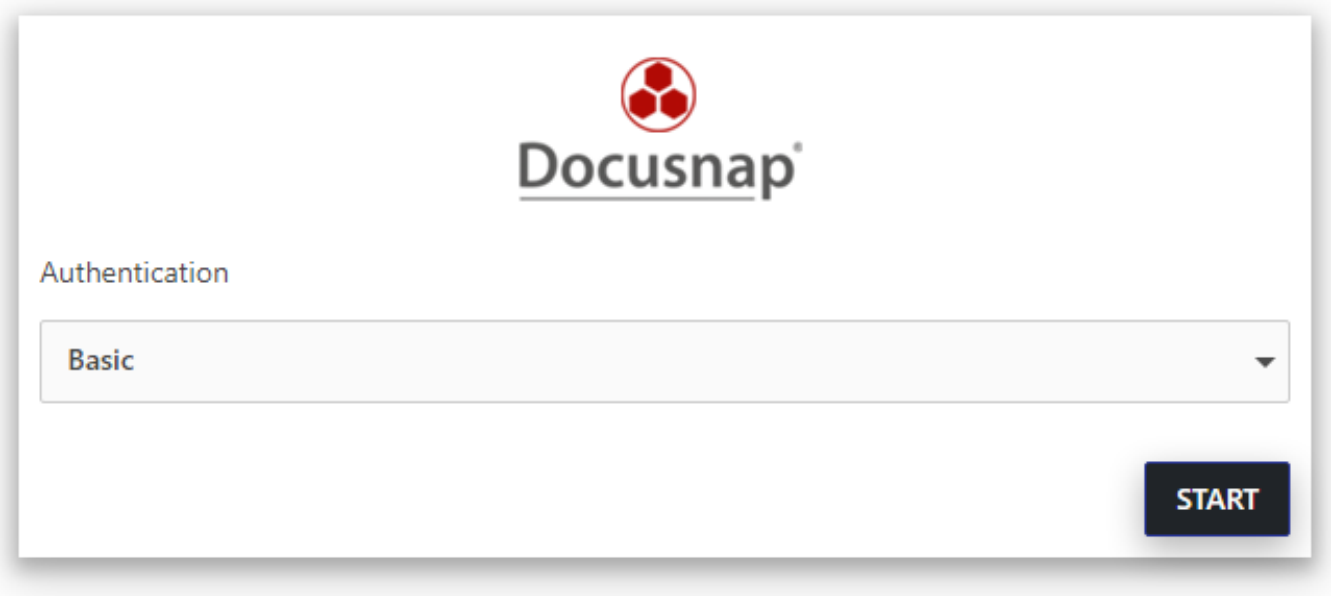

Figure 15 – Successful login after access rights editing

4.8 Next Steps

If you later create a new user, say "Company-C", with Basic Authentication, this user will by default have no permission to access the Docusnap database. Only after you have created a role for this user and set corresponding rights to an object of the Company type, the new user will be able to access the data. The permissions granted to the two existing users do not need to be adapted in this case.

LIST OF FIGURES

VERSION HISTORY

Date	Description
October 11, 2016	Version 1.0 – This description applies to Docusnap version 10.0.464.11.
October 31, 2016	Version 1.01 – Screenshots have been updated – Version 10.0.488.1
October 19, 2018	Version 1.1 – Screenshots have been updated – Version 10.0.1183.4
October 24, 2018	Version 1.2 – Screenshots have been updated – 1. Introduction: License notice has been added
May 04, 2020	Version 2.0 - Revision of the HowTos for Docusnap 11