



Docusnap Web

Configuration of Docusnap Web

TITLE	Docusnap Web
AUTHOR	Docusnap Consulting
DATE	June 2, 2025
VERSION	4.1 valid as of June 2, 2025

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.	Introduction	4
2.	Activating Docusnap Webserver	5
2.1	Starting the Docusnap Server configuration	5
2.2	Configuring Docusnap Server – Server API	6
2.3	Docusnap Web – functional test on the Docusnap Server system	7
2.4	Configuration of the service principal name (SPN)	8
2.5	Optional step: Customizing the Server API setting	9
3.	Docusnap Web – Known issues with self-signed certificates	10
4.	Administering user access to Docusnap Web	11
4.1	Enabling user management	11
5.	Using the ONC path in Docusnap Web	13

1. Introduction

In Docusnap, you can use a browser on any device to read most of the data in your Docusnap database and create plans and reports.

Perform a basic Docusnap installation. In our HowTo document called Docusnap – Installation and Configuration, you will find a detailed description of the installation and configuration of Docusnap X including the database deployment.

2. Activating Docusnap Webserver

2.1 Starting the Docusnap Server configuration

If you selected Docusnap Server at the time of the initial installation, Docusnap Web is already active and can be accessed via the default port 9001. If Docusnap Server is not yet active, you can activate it via **Discovery Services– Docusnap Server Configuration**.

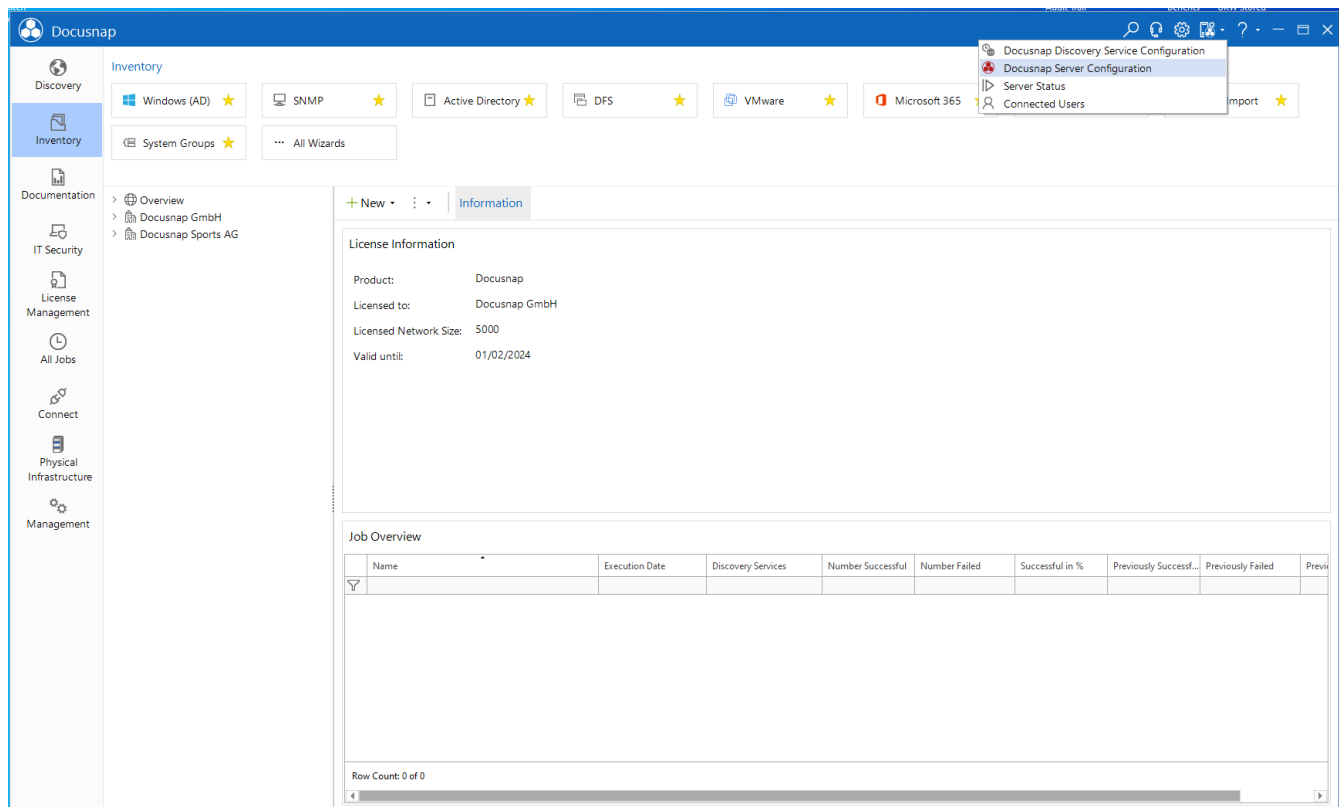
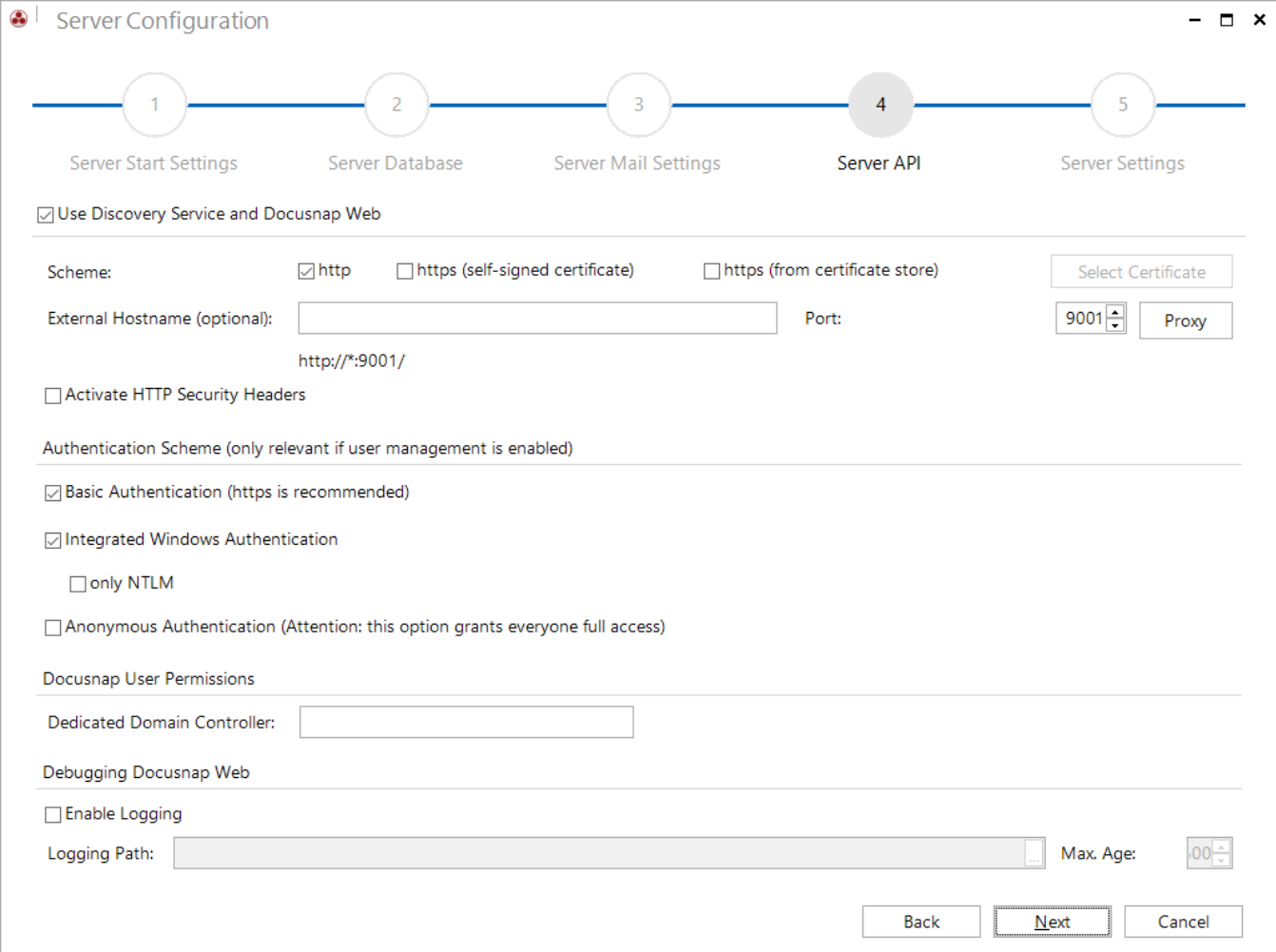


Fig. 1 – Configuring Docusnap Server

2.2 Configuring Docusnap Server – Server API

In this dialog, you configure all settings relevant to the use of Docusnap Web:



Server Configuration

1 Server Start Settings 2 Server Database 3 Server Mail Settings **4 Server API** 5 Server Settings

☒ Use Discovery Service and Docusnap Web

Scheme: ☒ http ☐ https (self-signed certificate) ☐ https (from certificate store) Select Certificate

External Hostname (optional): Port: Proxy

http://*:9001/

☐ Activate HTTP Security Headers

Authentication Scheme (only relevant if user management is enabled)

☒ Basic Authentication (https is recommended)

☒ Integrated Windows Authentication

☐ only NTLM

☐ Anonymous Authentication (Attention: this option grants everyone full access)

Docusnap User Permissions

Dedicated Domain Controller:

Debugging Docusnap Web

☐ Enable Logging

Logging Path: Max. Age:

Back Next Cancel

Fig. 2 – Docusnap Server – API

Use Discovery Service and Docusnap Web pane

- Enable the Use Discovery Service and Docusnap Web checkbox
- Select the http or https protocol
- If you want to use https, select the certificate or create one yourself (https is recommended)
- Optionally, specify an external host name and/or the desired proxy setting
- Select the port (default: 9001) - Set firewall policy!
- **HTTP Security Headers:** If desired, the HTTP Security Headers can be activated. As a result, however, the embedded reports, plans and documents are no longer displayed in the web client due to the higher security requirement.

Authentication Scheme pane

Please note: If you did not configure any users for Docusnap Web in the Docusnap User Management, **Docusnap Web will be available to all users**, regardless of the configured authentication settings. 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.

- Basic Authentication – Required if users outside your ADS need to access the Web client.
- Integrated Windows Authentication (The availability of single sign-on depends on the browser, i.e. this feature is not guaranteed)
- Anonymous Authentication – Full access for all users when the Docusnap User Management is enabled.

Debugging Docusnap Web pane

The Enable Logging option found on this pane is only intended for the Docusnap Support team; it is not relevant to normal operation.

2.3 Docusnap Web – functional test on the Docusnap Server system

Once you have completed the configuration of Docusnap Server and the service is available, Docusnap Web is ready for use. To test the functionality of Docusnap Web, enter the URL **<https://NameOfDocusnapServer:9001>** in your browser. We recommend performing the functional test from a client system, not locally on the Docusnap server.

2.4 Configuration of the service principal name (SPN)

In Active Directory (AD), the Service Principal Name (SPN) is a unique identifier for a service running on a specific server. SPNs are primarily used in the context of Kerberos authentication. They allow clients to uniquely identify a service and obtain a Kerberos ticket to authenticate to that service.

Kerberos authentication is the preferred login method for Docusnap Web. NTLM is used as a fallback mechanism.

Docusnap Web is provided through the Docusnap Server Service, which can be run either as **Local System** or under a **service user** account.

If the **Docusnap Server Service** is run as **Local System**, no additional SPN configuration is required. The appropriate SPNs are automatically registered when the computer object is created in AD (e.g., `HOST/NameOfDocusnapServer`, `HOST/NameOfDocusnapServer.Domain.local`).

If a **service user** is used to run the **Docusnap Server Service**, an SPN must be configured for this user and Docusnap Web to enable Kerberos authentication:

- `setspn -S HTTP/NameOfDocusnapServer.Domain.Local NameOfServiceUser`
- Example: `setspn -S HTTP/SRV-Docusnap.intern.local SVC-Docusnap`

If this SPN configuration is not performed, NTLM will be used for authentication. If NTLM is disabled, logging in to Docusnap Web will not be possible.

Additionally, SPN configuration is required if Docusnap Web is accessed using a name that differs from the server's hostname (e.g., a DNS alias):

- If the **Local System** account is used:
 - `setspn -S HTTP/DocusnapWebAlias NameOfDocusnapServer`
- If a **service user** is used:
 - `setspn -S HTTP/DocusnapWebAlias NameOfServiceUser`

2.5 Optional step: Customizing the Server API setting

If you operate more than one Docusnap installation, the URL of the system on which Docusnap Server was configured should be changed – for all Docusnap installations – from the default value, i.e. `http://localhost:9001`, to the host name or IP address actually used.

Options – General Options – Connections – Server API Connection

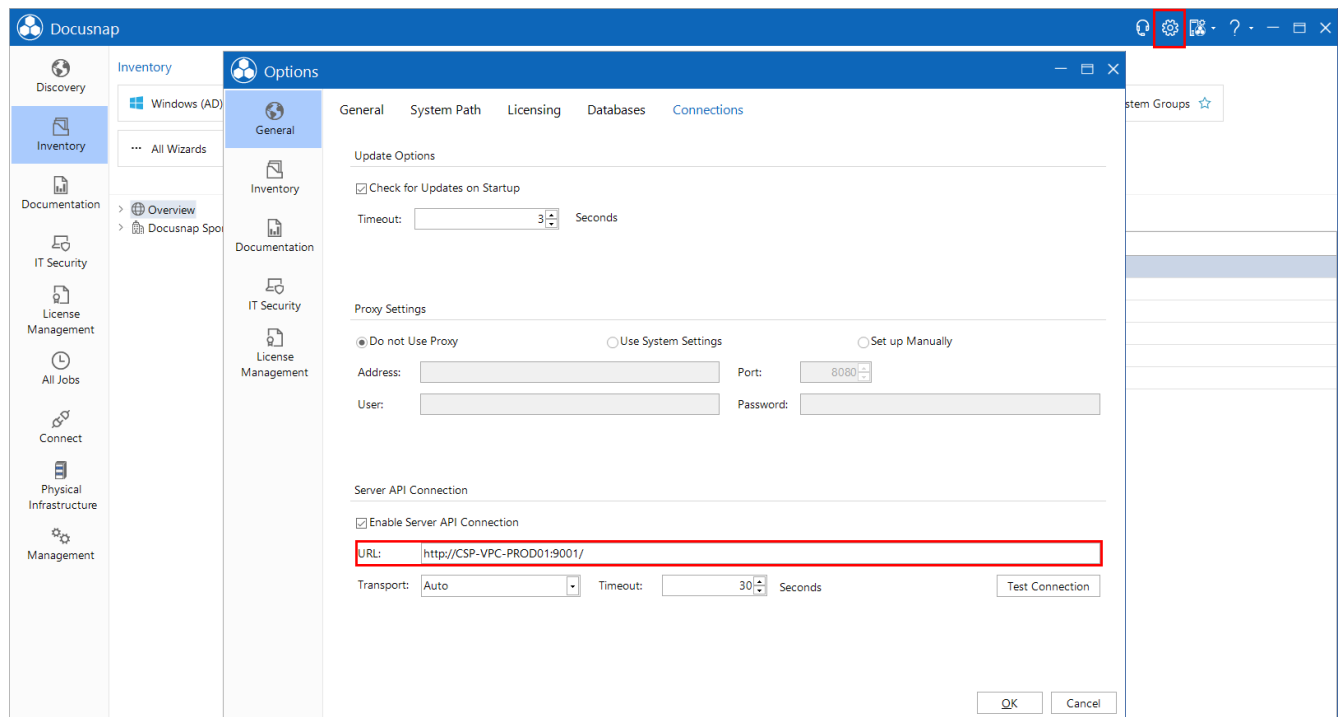


Fig. 3 – Connection options – Customizing the server API

3. Docusnap Web – Known issues with self-signed certificates

When calling Docusnap Web, you must accept the self-signed Docusnap Server certificate. This step caused problems in the Firefox browser. All other tested browsers accepted the certificate in our tests.

A security alert is displayed. Confirm the prompt. When you close this dialog, the Docusnap Web Client starts.

Whether these prompts are displayed or not depends on the certificate used to establish the https connection to the Docusnap Server API.

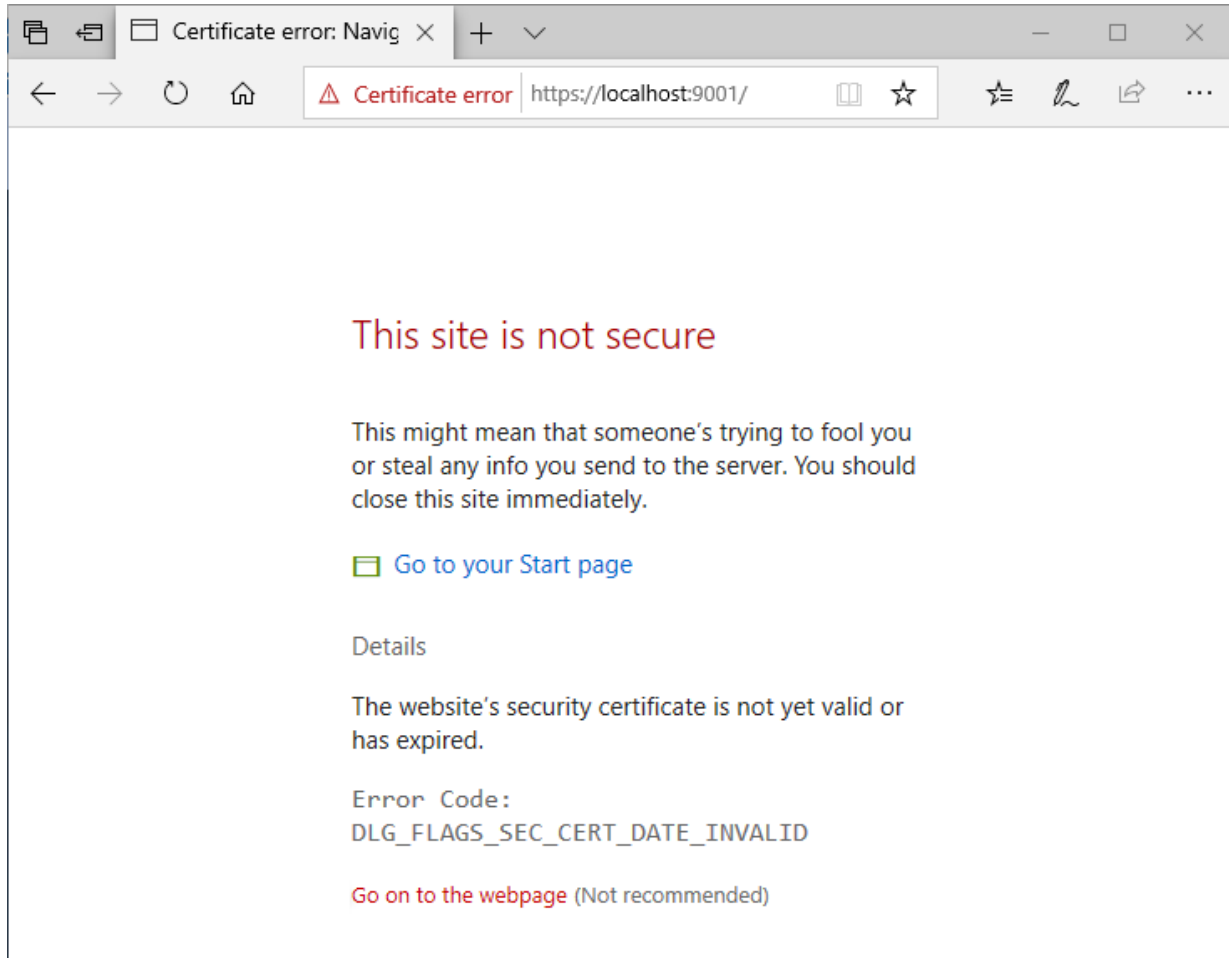


Fig. 4 – Operating system security alert –Browser Microsoft Edge

4. Administering user access to Docusnap Web

The authentication scheme for accessing Docusnap Web can be configured in the Docusnap Server settings under "Server API." By default, the "Basic" and "Integrated" authentication schemes are enabled.

Important: Without enabling user management, Docusnap Web cannot be used with this configuration! In this case, you must either enable user management (recommended) or configure the authentication scheme to "Anonymous" (not recommended).

4.1 Enabling user management

To switch to the Docusnap User Management, click *Management – General*.

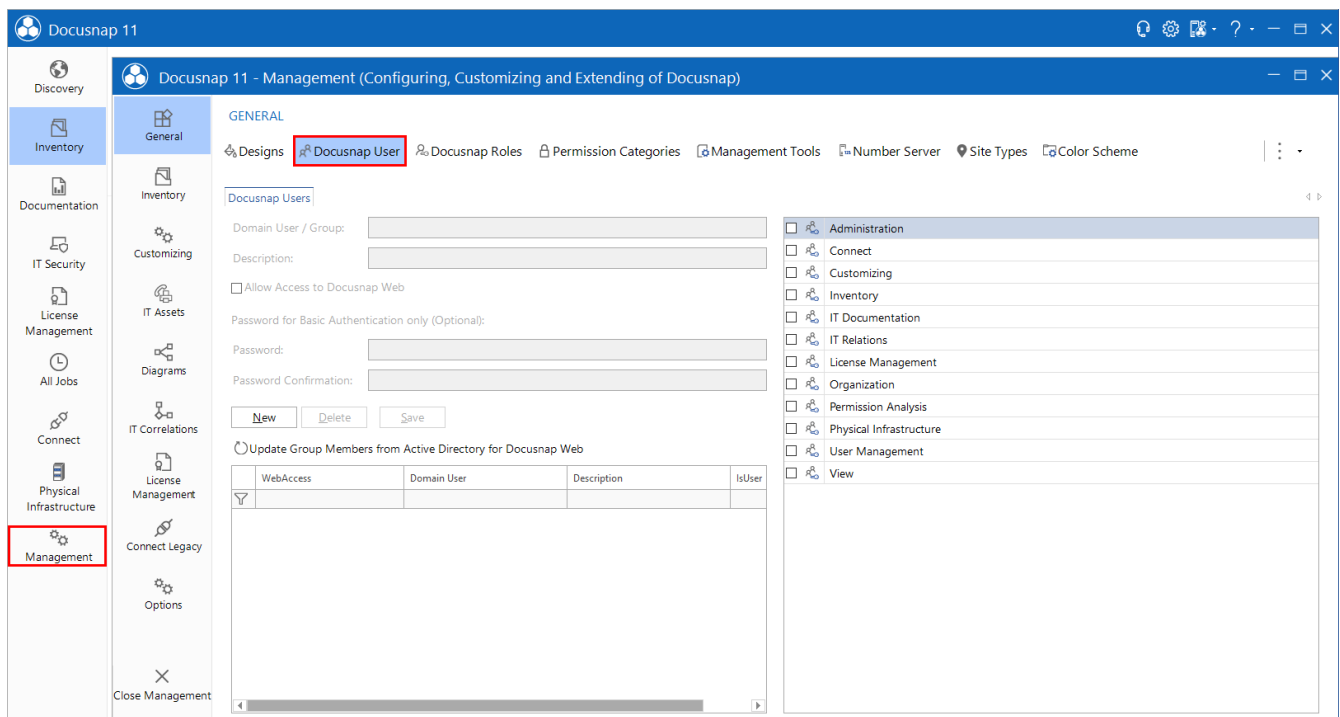


Fig. 5 – User Management

User Management allows you to manage the following:

- Domain User / Group – either from the current domain or the local system
- Description
- Allow Access to Web Client
- Password for Basic Authentication only
- Docusnap Roles

For further information on the Docusnap User Management functionality, please refer to the online manual. The corresponding manual chapter can be accessed directly by pressing F1 – provided that the Docusnap system has Internet access.

If you select **Integrated Windows – Authentication** or **Basic Authentication**, you need to make sure to create the corresponding users or groups in User Management and enable the **Allow Access to Docusnap Web** checkbox.

The Basic Authentication scheme requires you to enter a password for accessing the Web Client.

If you want to add users that should have access to the Web Client only, there is no need to assign them a role.

IMPORTANT: Users / groups who are supposed to work with the Docusnap Client must be assigned corresponding user roles!

5. Using the ONC path in Docusnap Web

The ONC (Object Numbering Convention) is a coded path to a concrete object in the Docusnap trees. Each object in Docusnap is uniquely identifiable via this.

The ONC path can be generated during the creation of a Docusnap Connect Package - optionally the ONC column can be output.

Another possibility is to select the desired object in the data tree and press CTRL + C.

For more information on the ONC path, see the Docusnap User Manual - Docusnap and External Programs. For more information about Docusnap Connect, see the HowTo Docusnap Connect Export and Import.

The ONC path can also be used to navigate to the selected object in Docusnap Web. To do this, enter the path in the URL line.

Example: `http://localhost:9001/ONC/[1,1]\[1,2]\[2,4]\[2,5]\[6,6]`

After confirming the URL, it is necessary to authenticate, after which the desired content is opened in Docusnap Web

VERSION HISTORY

Date	Description
August 05, 2016	Version 1.0 – Initial draft
August 08, 2016	Version 1.1 – Port customization and certificate handling sections added
August 09, 2016	Version 1.2 – Corrections (resulting from feedback from Development)
September 02, 2016	Version 1.3 – Adaptations to RTM version of Docusnap X
September 14, 2016	Version 1.4 – Screenshot with Docusnap X status bar; handling of private certificates updated
June 01, 2018	Version 2.0 – Release of Docusnap Webserver – complete revision of the HowTo document
January 27, 2020	Version 2.1 – Version removed from title; screenshot update; ONC path added
Mai 04, 2020	Version 3.0 - Revision of the HowTos for Docusnap 11
November 13, 2023	Version 4.0 - Revision of the HowTos for Docusnap 13
June 2, 2025	Version 4.1 - Revision of the HowTo - Chapter 2.4 added