



DocuSnap – DocuSnap Web
Installing and Customizing DocuSnap Web

TITLE Docusnap – Docusnap Web
AUTHOR Docusnap Consulting
DATE May 04, 2020
HOW-TO VERSION 3.0 | valid as of October 01, 2020
LANGUAGE English

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
1.1	Installation of Docusnap – preparation	4
1.2	Docusnap webserver – current architecture	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	Optional step: Customizing the Server API setting	8
3.	Changing from IIS to Docusnap Webserver	9
4.	Docusnap Web – Known issues with self-signed certificates	10
5.	Administering user access to Docusnap Web	11
5.1	Enabling user management	11
6.	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.

1.1 Installation of Docusnap – preparation

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.

For trouble-free use of Docusnap Web we recommend Windows Server 2012 or higher.

1.2 Docusnap webservice – current architecture

The diagram below shows the architecture of the Docusnap Webservice.

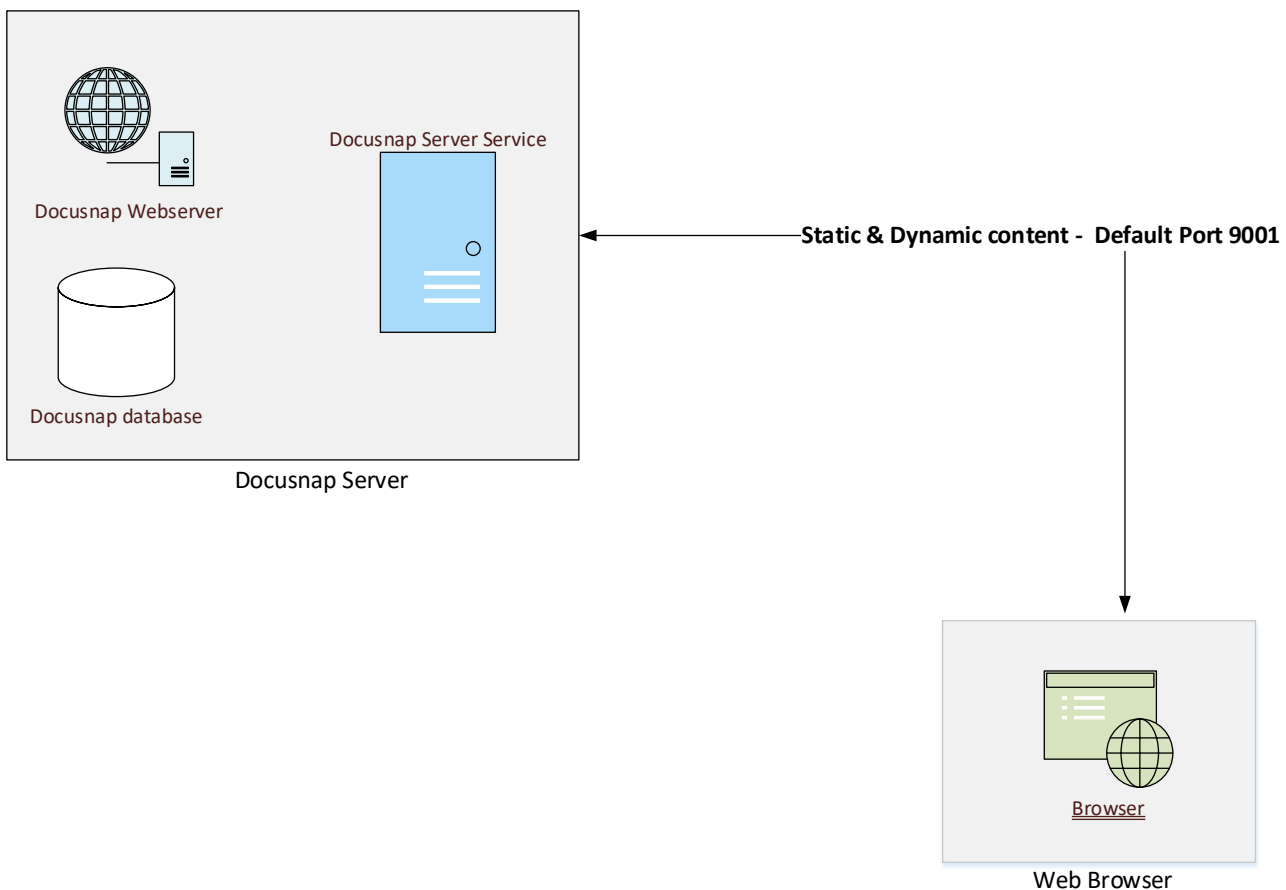


Fig. 1 – Docusnap Webservice architecture

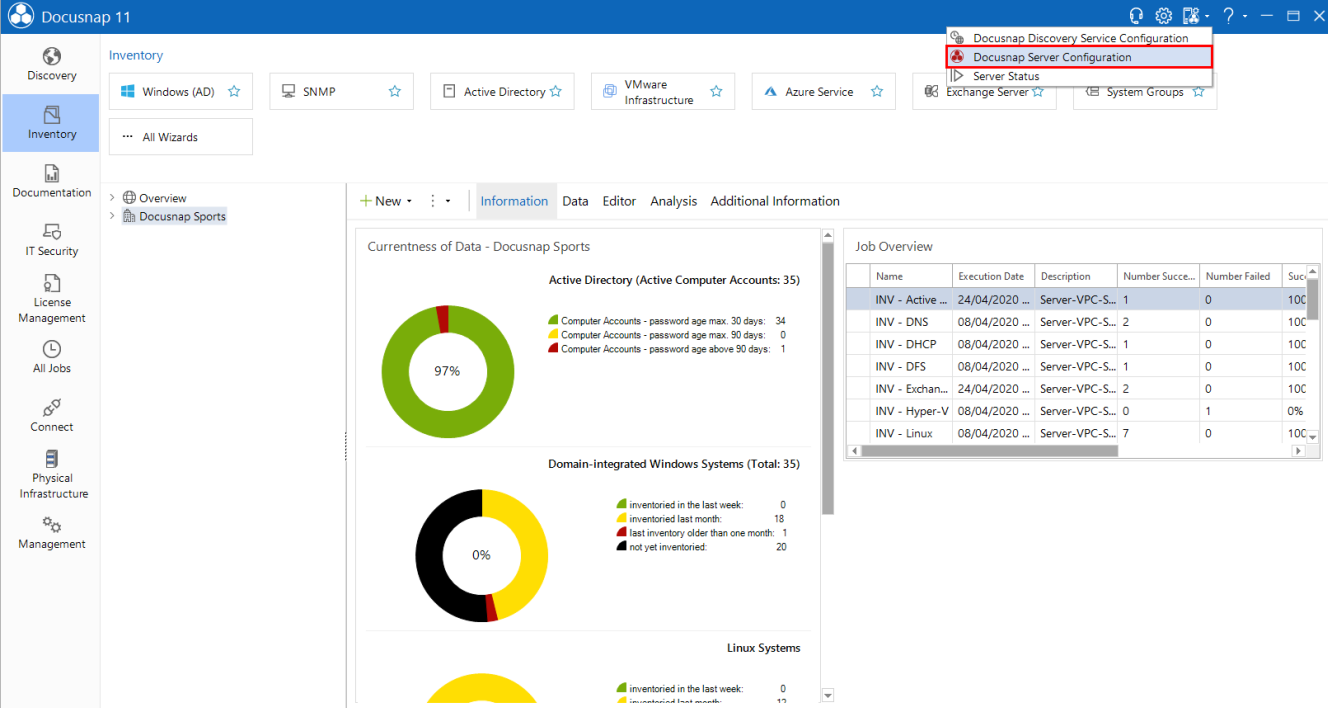
Important: The default port for Docusnap Web is 9001. The single port can be configured in Docusnap using a central setting.

Make sure that the remote Docusnap Web devices can access your Docusnap system via this port.

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**.



The screenshot shows the Docusnap 11 web interface. In the top right corner, a dropdown menu is open, highlighting 'Docusnap Server Configuration'. The main dashboard displays the following data:

Currentness of Data - Docusnap Sports

Active Directory (Active Computer Accounts: 35)

- Computer Accounts - password age max. 30 days: 34
- Computer Accounts - password age max. 90 days: 0
- Computer Accounts - password age above 90 days: 1

Domain-integrated Windows Systems (Total: 35)

- inventoried in the last week: 0
- inventoried last month: 18
- last inventory older than one month: 1
- not yet inventoried: 20

Linux Systems

- inventoried in the last week: 0
- inventoried last month: 15

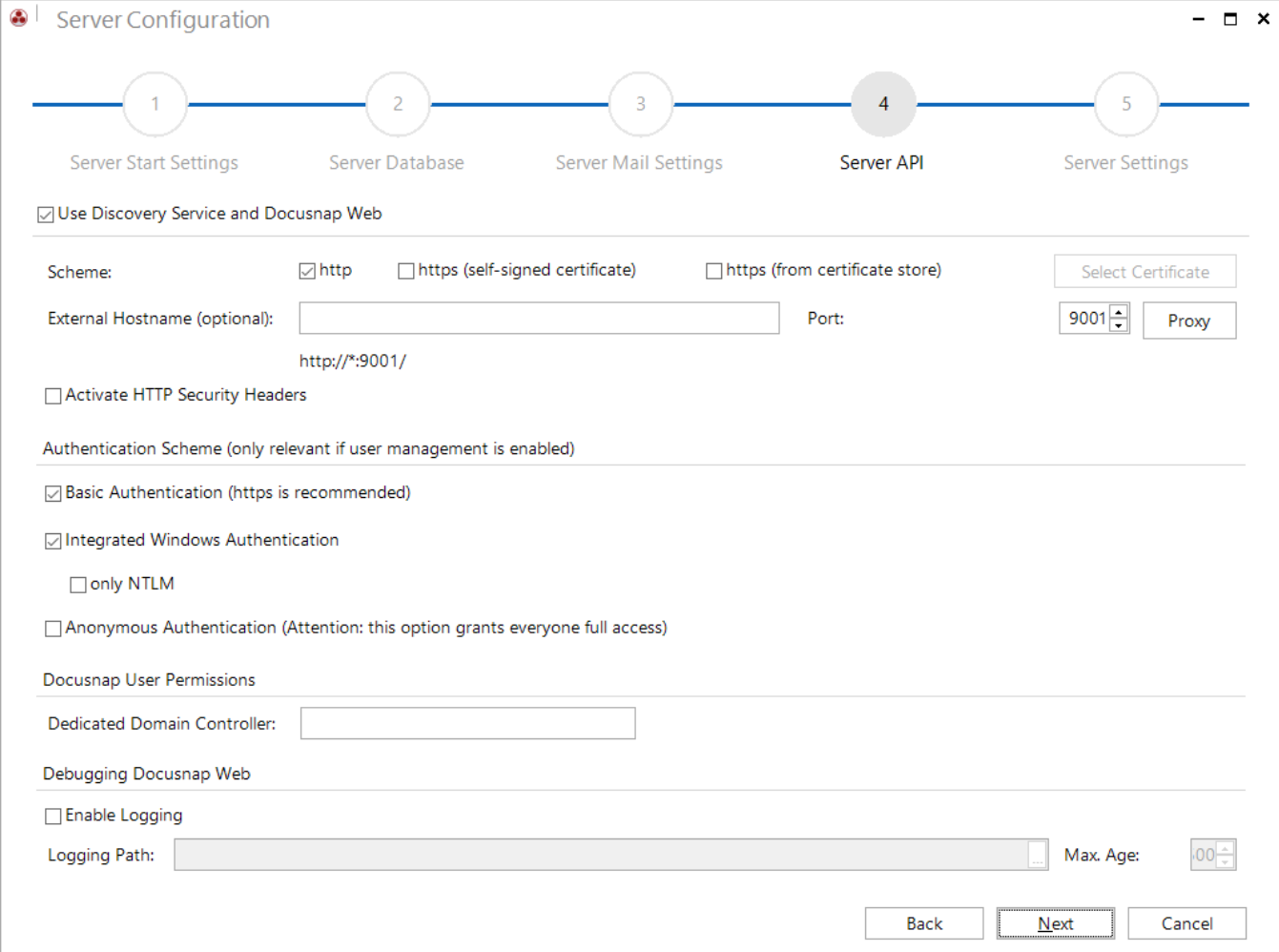
Job Overview Table:

Name	Execution Date	Description	Number Succe...	Number Failed	Suc...
INV - Active ...	24/04/2020 ...	Server-VPC-S...	1	0	100
INV - DNS	08/04/2020 ...	Server-VPC-S...	2	0	100
INV - DHCP	08/04/2020 ...	Server-VPC-S...	1	0	100
INV - DFS	08/04/2020 ...	Server-VPC-S...	1	0	100
INV - Exchan...	24/04/2020 ...	Server-VPC-S...	2	0	100
INV - Hyper-V	08/04/2020 ...	Server-VPC-S...	0	1	0%
INV - Linux	08/04/2020 ...	Server-VPC-S...	7	0	100

Fig. 2 – 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)

External Hostname (optional): Port:

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:

Fig. 3 – 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 (self-signed certificates are only recommended for testing)
- Optionally, specify an external host name and/or the desired proxy setting
- Select the port (default: 9001)
- **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.

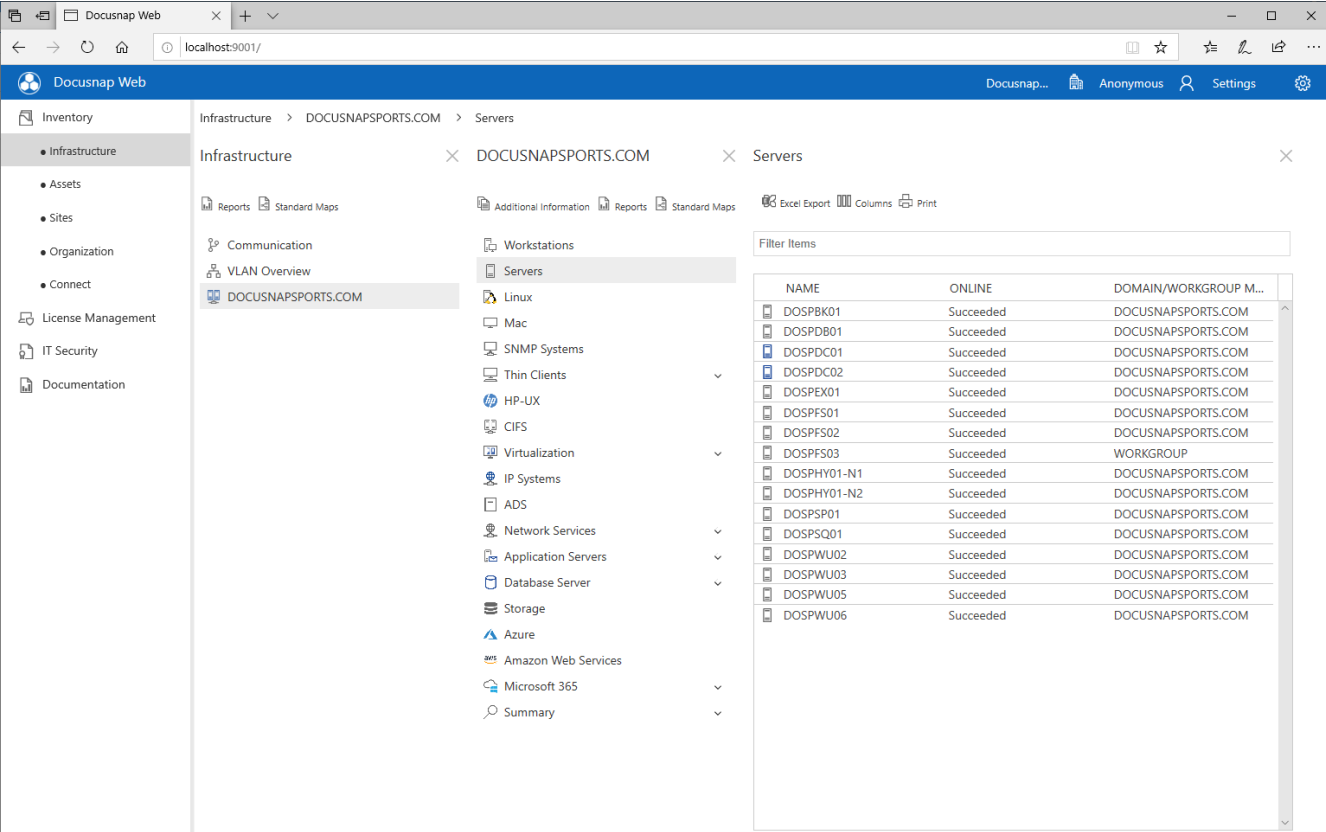
- Basic Authentication – Required if users outside your ADS need to access the Web client.
- Integrated Windows Authentication (The availability of single sign-on depends on the browser, i.e. this feature is not guaranteed)
- Anonymous Authentication – Full access for all users when the Docusnap User 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 <http://localhost:9001> in your browser:



NAME	ONLINE	DOMAIN/WORKGROUP M...
DOSPDK01	Succeeded	DOCUSNAPSPORTS.COM
DOSPDB01	Succeeded	DOCUSNAPSPORTS.COM
DOSPDC01	Succeeded	DOCUSNAPSPORTS.COM
DOSPDC02	Succeeded	DOCUSNAPSPORTS.COM
DOSPEX01	Succeeded	DOCUSNAPSPORTS.COM
DOSPF01	Succeeded	DOCUSNAPSPORTS.COM
DOSPF02	Succeeded	DOCUSNAPSPORTS.COM
DOSPF03	Succeeded	WORKGROUP
DOSPHY01-N1	Succeeded	DOCUSNAPSPORTS.COM
DOSPHY01-N2	Succeeded	DOCUSNAPSPORTS.COM
DOSPS01	Succeeded	DOCUSNAPSPORTS.COM
DOSPSQ01	Succeeded	DOCUSNAPSPORTS.COM
DOSPWU02	Succeeded	DOCUSNAPSPORTS.COM
DOSPWU03	Succeeded	DOCUSNAPSPORTS.COM
DOSPWU05	Succeeded	DOCUSNAPSPORTS.COM
DOSPWU06	Succeeded	DOCUSNAPSPORTS.COM

Fig. 4 – Docusnap Web: functional test

2.4 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

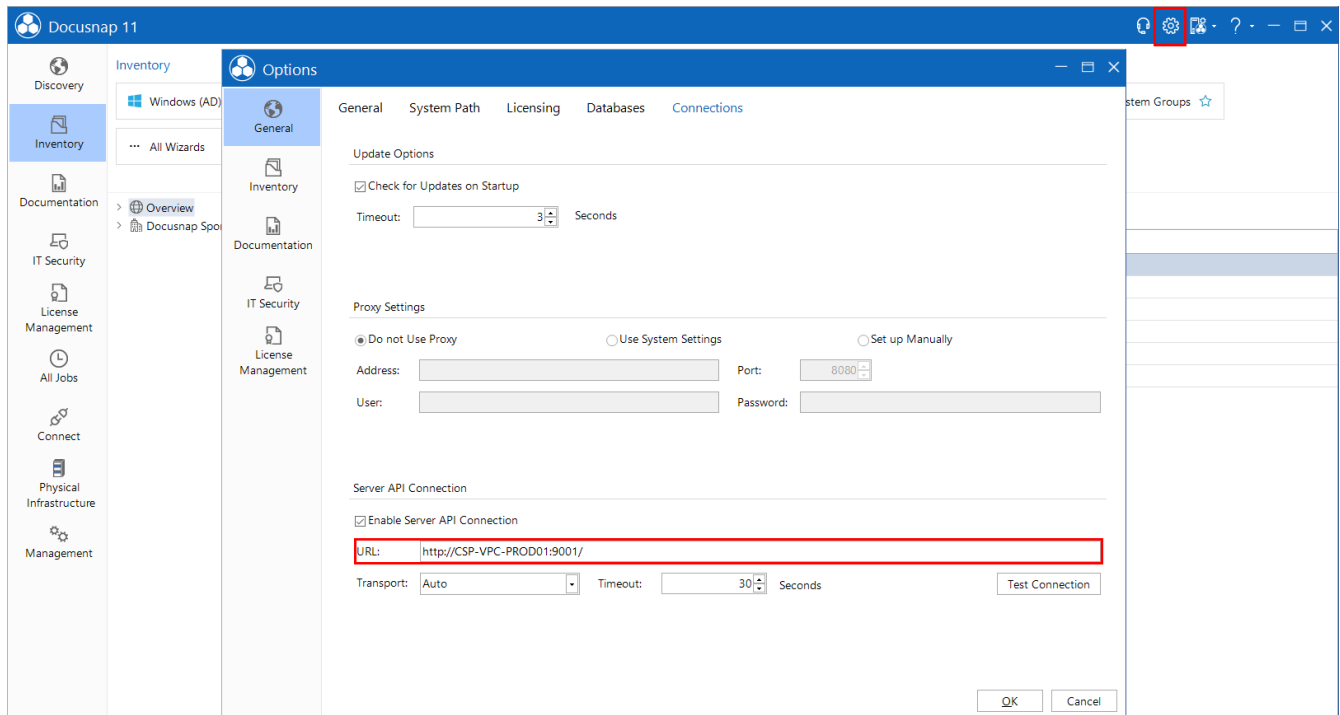
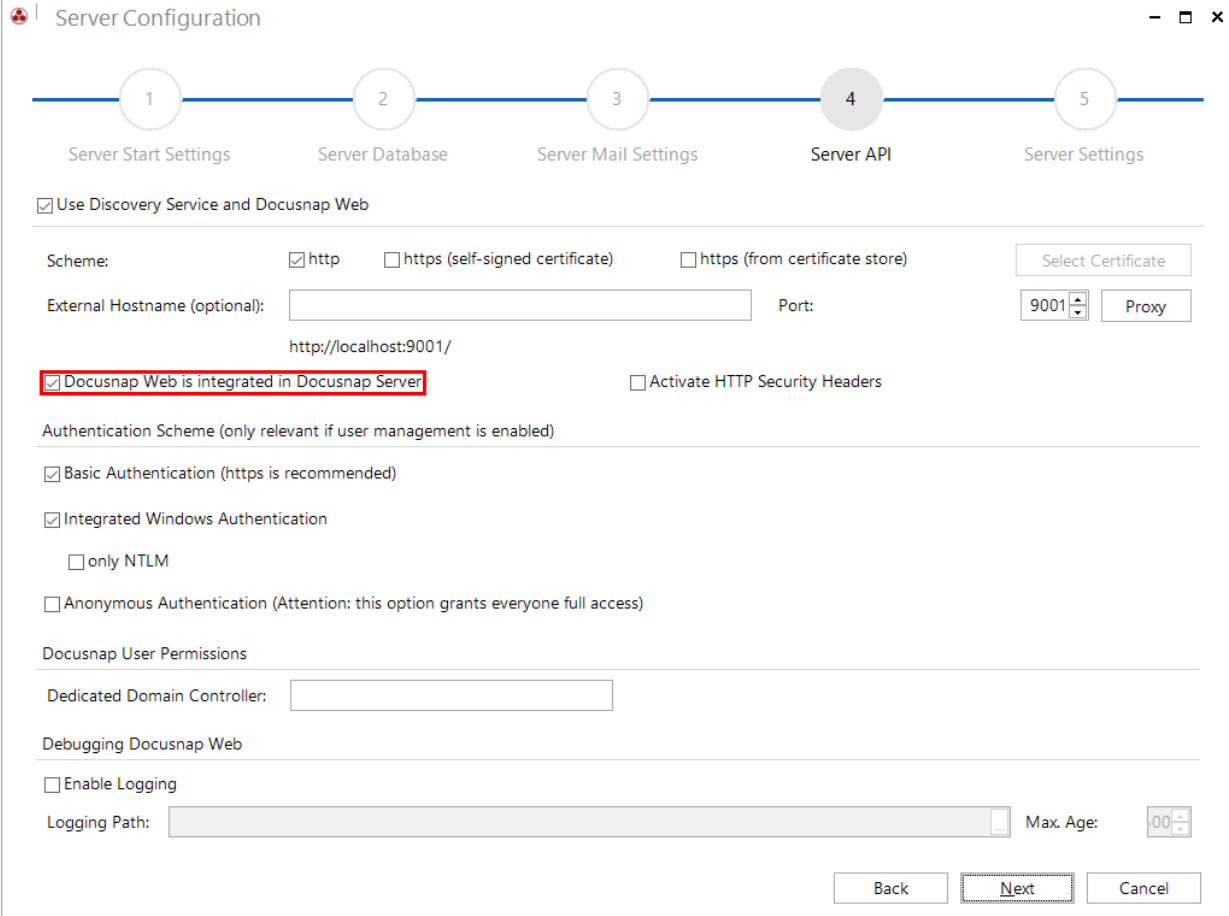


Fig. 5 – Connection options – Customizing the server API

3. Changing from IIS to Docusnap Webserver

Until May, 2018, Docusnap needed the Internet Information Server Role for providing the static web items.

For new Docusnap installations, the Docusnap Webserver is now installed automatically. For legacy installations with IIS, the IIS server is enabled under the configured port (default: 8181) after the update. However, the Docusnap Server configuration allows you to enable the Docusnap Webserver for legacy installations as well.



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)

External Hostname (optional): Port:

http://localhost:9001/

Docusnap Web is integrated in Docusnap Server 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:

Fig. 6 – Enabling Docusnap Webserver for legacy installations – Option only available in legacy installations

When you restart Docusnap Server, the Docusnap Webserver is active and the Docusnap Web contents will also be output via port 9001 (default port for the Docusnap API). From then on, the IIS role is no longer required and you no longer need to enable port 8181 (default port for IIS).

Please note that the development of Docusnap Web IIS has been discontinued so that it is no longer available in Docusnap.

4. 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.

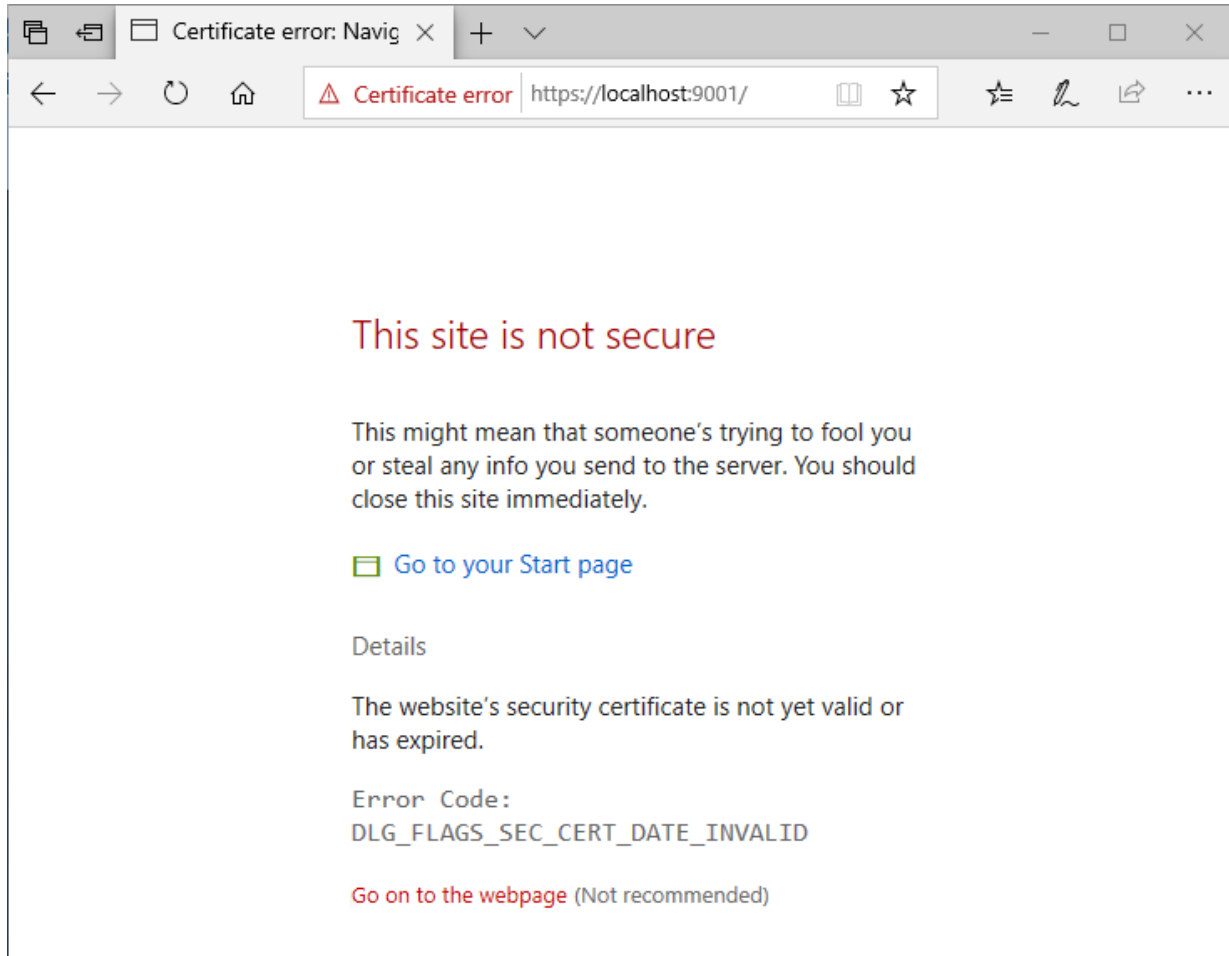


Fig. 7 – Operating system security alert –Browser Microsoft Edge

5. Administering user access to Docusnap Web

The authentication scheme for the access to Docusnap Web can be changed while you configure the Docusnap Server in the *Server API* step. This requires that User Management has been enabled. Otherwise, Docusnap Web will be accessed using *Anonymous Authentication* – this means that *everybody* would have access to the Docusnap Web Client.

5.1 Enabling user management

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

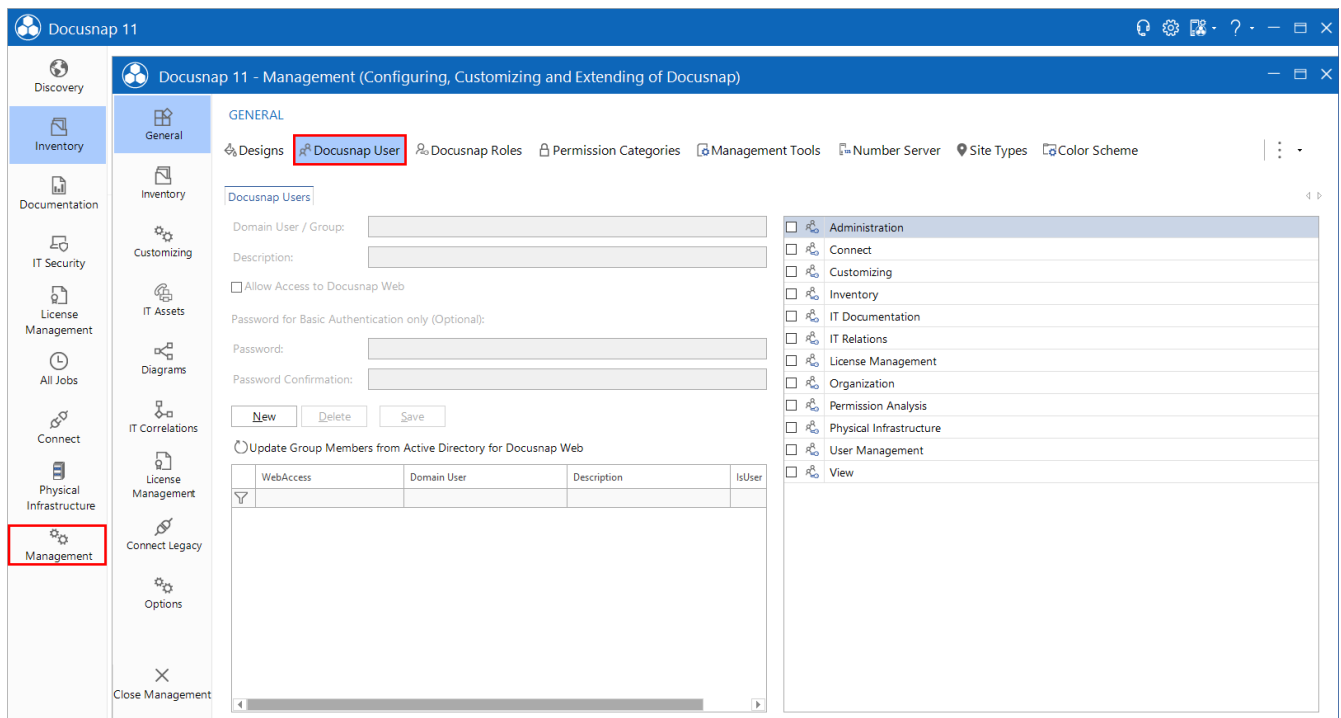


Fig. 8 – User Management

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!

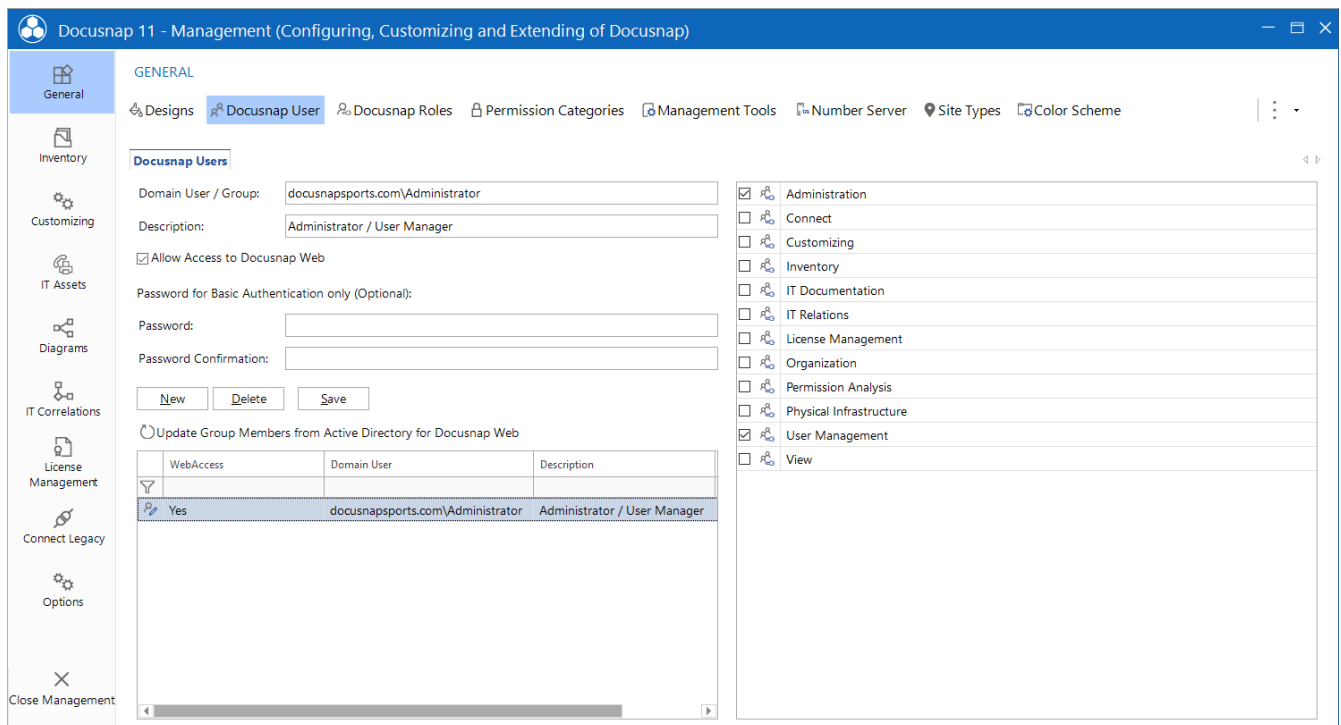


Fig. 9 – Adding users when using the Integrated Windows Authentication scheme

6. 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

LIST OF FIGURES

FIG. 1 – DOCUSNAP WEBSERVER ARCHITECTURE.....	4
FIG. 2 – CONFIGURING DOCUSNAP SERVER	5
FIG. 3 – DOCUSNAP SERVER – API	6
FIG. 4 – DOCUSNAP WEB: FUNCTIONAL TEST	7
FIG. 5 – CONNECTION OPTIONS – CUSTOMIZING THE SERVER API	8
FIG. 6 – ENABLING DOCUSNAP WEBSERVER FOR LEGACY INSTALLATIONS – OPTION ONLY AVAILABLE IN LEGACY INSTALLATIONS	9
FIG. 7 – OPERATING SYSTEM SECURITY ALERT –BROWSER MICROSOFT EDGE.....	10
FIG. 8 – USER MANAGEMENT.....	11
FIG. 9 – ADDING USERS WHEN USING THE INTEGRATED WINDOWS AUTHENTICATION SCHEME.....	12

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
