



Docusnap X – Docusnap Web

Installing and Customizing Docusnap Web

TITLE	Docusnap X – Docusnap Web
AUTHOR	Docusnap Consulting
DATE	7/12/2017
VERSION	1.3 valid as of September 06, 2016
LANGUAGE	English

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.

All rights reserved.

TABLE OF CONTENTS

1.	Introduction	4
1.1	Overview of the Topics in this HowTo Document – Docusnap Web	4
1.2	Docusnap Web Installation – Prerequisites	4
1.3	The Architecture of Docusnap Web	5
2.	Installing Docusnap Web	6
2.1	Installing Docusnap Web – Automatic Installation	6
2.2	Installing Docusnap Web – Manual Installation	7
2.2.1	Installing Docusnap Web – Manual Installation – Installation Procedure	7
2.3	Docusnap Web – Logging On for the First Time	9
3.	Optional Step: Customizing the Ports for the Web Server and the Docusnap Server API	11
3.1	Introduction	11
3.2	Configuring the IIS (Static Website) Access with http – Port 80	11
3.4	Configuring the Docusnap Server API Access with https – Port 443	15
3.4.1	Customizing the Server API Connection	16
3.5	Docusnap Web – Testing the Connection with a Different System	17
4.	Managing User Access to Docusnap Web	20
4.1	Enabling User Management	20
4.2	Configuring the Authentication Scheme for Docusnap Web	22
4.2.1	Anonymous Authentication	22
4.2.2	Basic Authentication	22
4.2.3	Integrated Windows Authentication	22

1. Introduction

In Docusnap X, it is possible to obtain read-access to the data in your Docusnap database and to create plans and reports using a web browser on any mobile terminal device.

1.1 Overview of the Topics in this HowTo Document – Docusnap Web

- Chapter 2 – Automatic and manual installation of Docusnap Web
- Section 3 – Best practice: setup of the web server ports and the Docusnap Server API
- Chapter 4 – Managing user access to Docusnap Web

1.2 Docusnap Web Installation – Prerequisites

- Docusnap must have been installed and configured completely

The procedures are described in a separate HowTo document called “Docusnap X Installation and Configuration” that is available for download in the [HowTo area](#) of our website.

- Configuration of the Docusnap Server service

– For the installation of Docusnap Web, at least Windows 8 / 2012 or higher is required!

1.3 The Architecture of Docusnap Web

You need to install an IIS web server on the Docusnap system and create a static website. This website connects to the Docusnap Server service to access your Docusnap database. In the browser, you can query the desired contents from the database and view them on your mobile device.

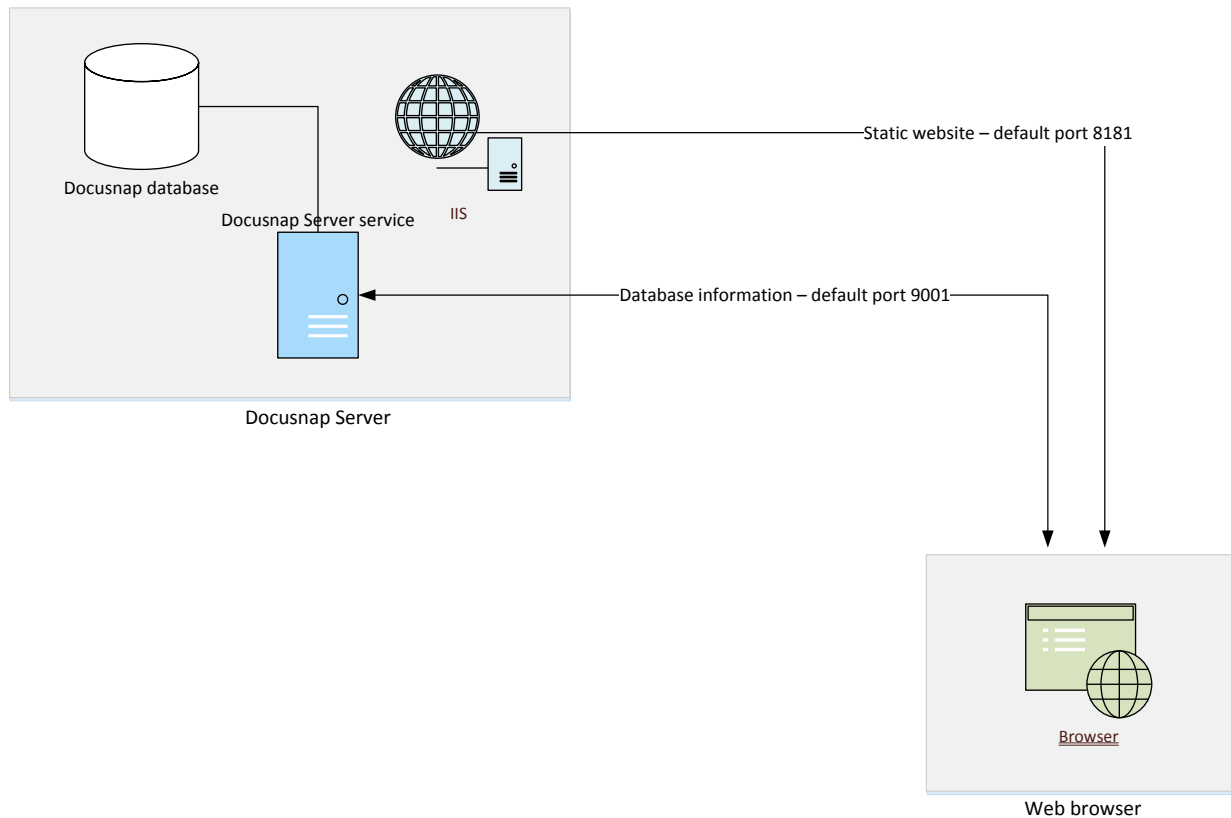


Fig. 1 – Overview of the Docusnap Web architecture

Important: The static website can only be viewed in the browser if a special port has been opened for access to the IIS web server. Another port is required to access the Docusnap Server API. Information from the Docusnap database will be loaded into the browser using this interface.

Make sure that the Docusnap web devices are able to access the Docusnap main system using these ports!

The default port for the IIS web server is 8181, the Docusnap Server API is by default accessed via port 9001. Chapter 3 explains how you can change these ports to port 80 (http) and port 443 (https).

2. Installing Docusnap Web

2.1 Installing Docusnap Web – Automatic Installation

Once the basic installation of Docusnap X is complete, a configuration dialog opens *when you start Docusnap X for the first time*. If you select “Install Docusnap Web”, the system automatically installs all IIS components and creates the Docusnap website that will be accessible by anonymous users via port 8181.

For this installation type, *no additional steps* are required. This means that a default installation of Docusnap Web without any additional steps is performed.

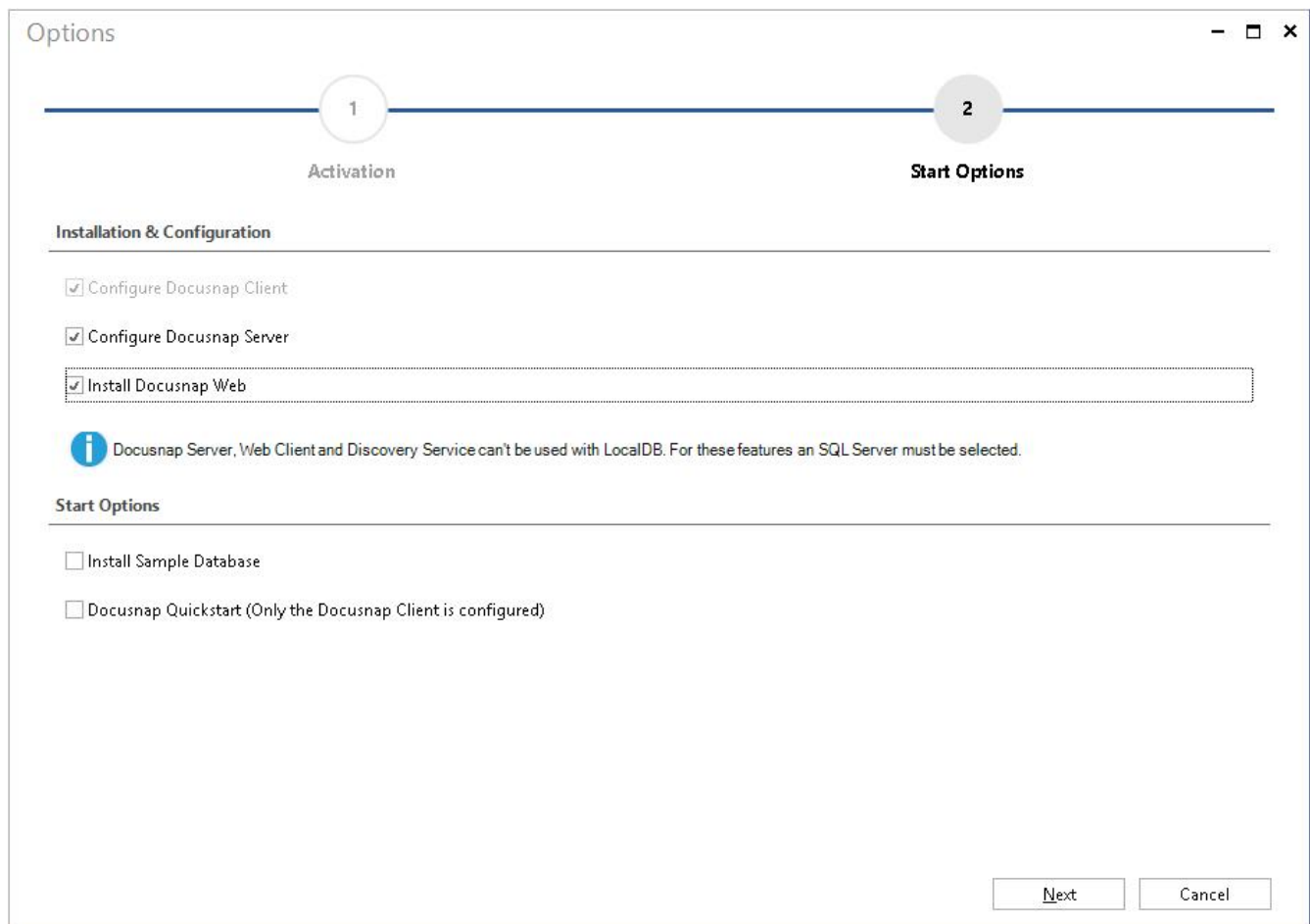


Fig. 2 – Docusnap X , first start, configuration wizard

2.2 Installing Docusnap Web – Manual Installation

If you did not select the *Install Docusnap Web* option when starting Docusnap X for the first time, you can perform the installation later on. To do so, follow the steps described below.

2.2.1 Installing Docusnap Web – Manual Installation – Installation Procedure

The *DocusnapWebSetup.exe* setup file resides in the Setup subdirectory of the Docusnap X program directory.

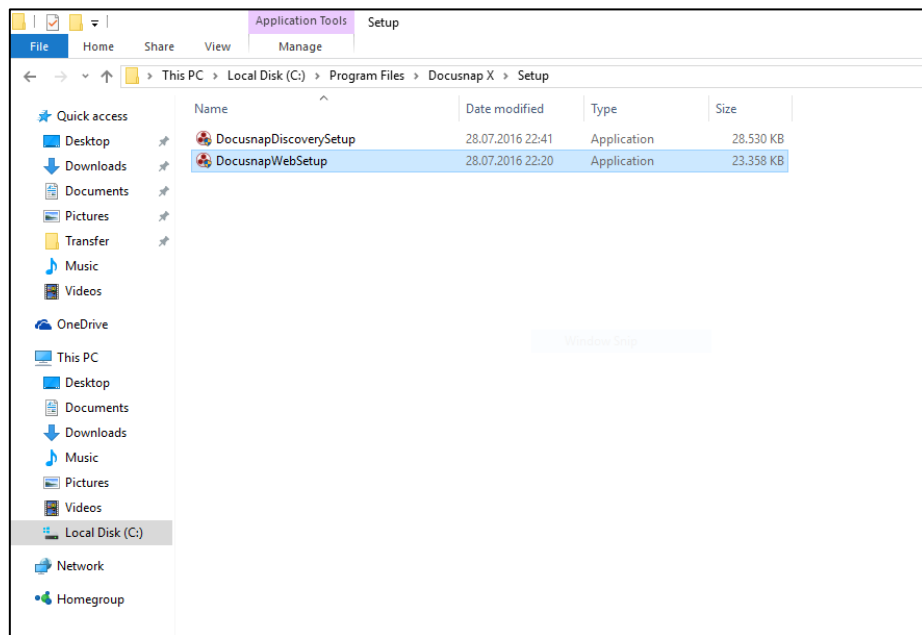


Fig. 3 – Setup file location in the file system

The following figure shows the steps of the setup dialog. The installation of the IIS components and the creation of the Docusnap website are performed in the background. The installation might take some minutes.

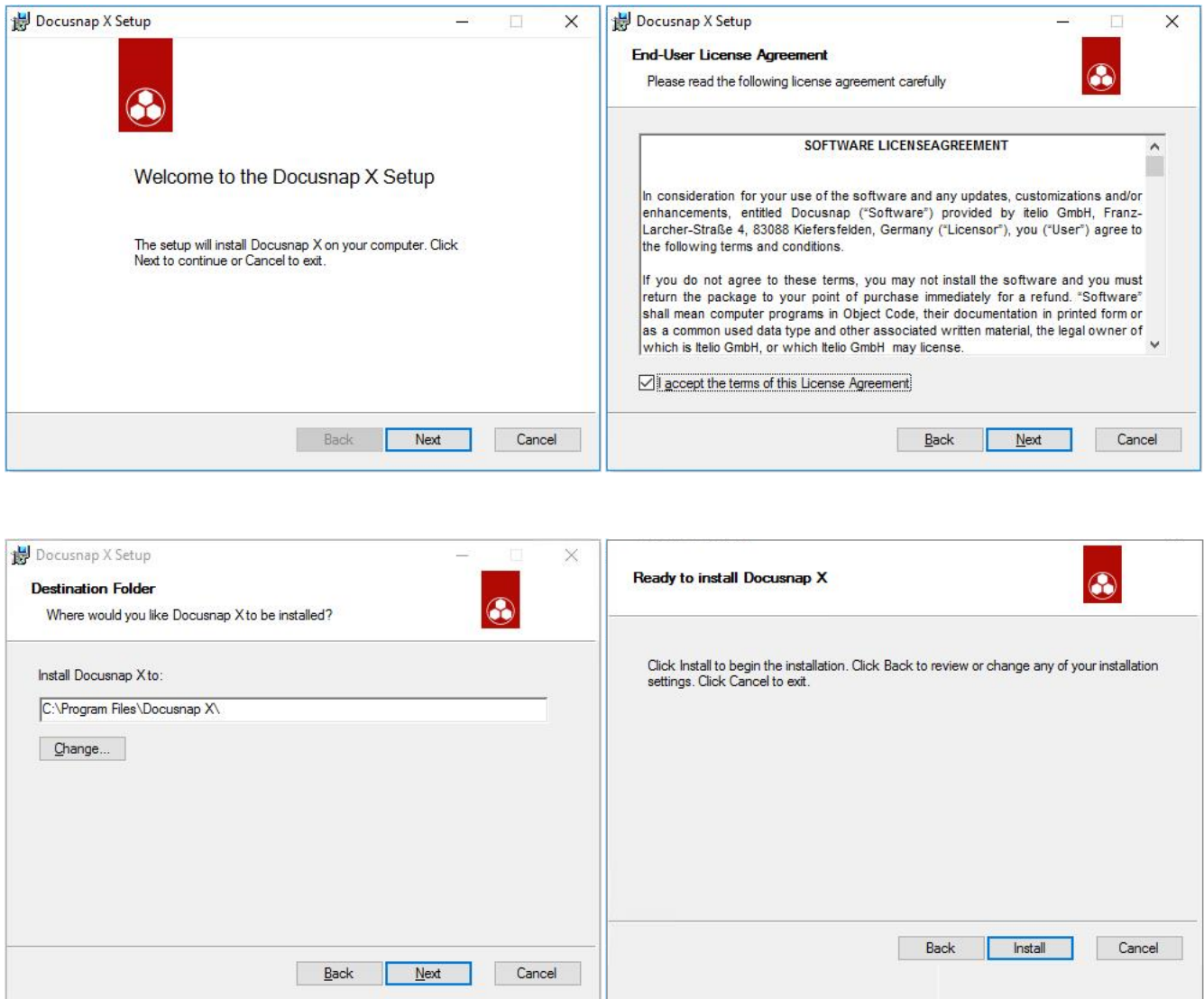


Fig. 4 – Docusnap Web setup – Installation steps

2.3 Docusnap Web – Logging On for the First Time

The Docusnap Web login dialog is displayed in your browser. Docusnap Web is called locally using the following URL: <http://localhost:8181>

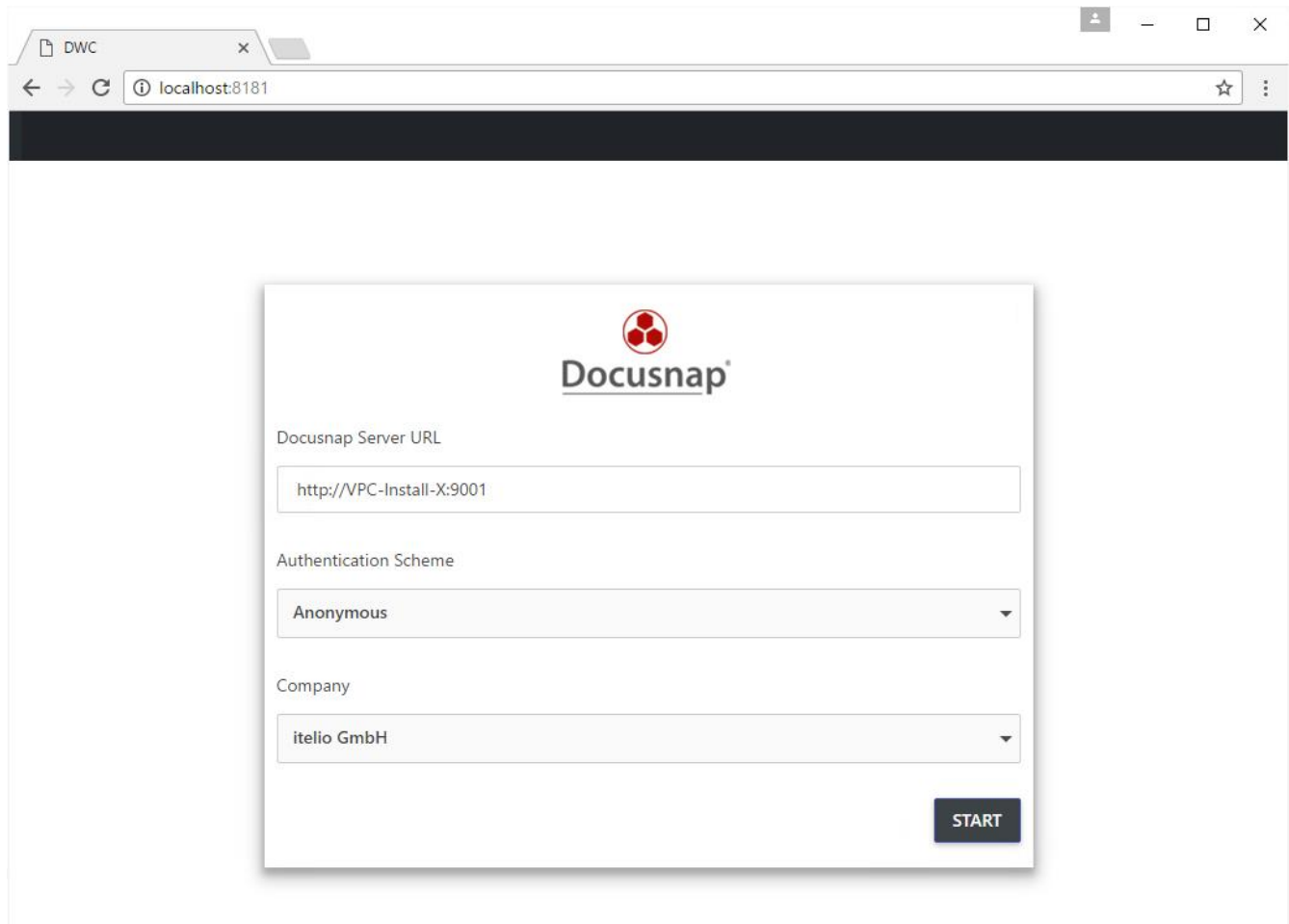


Fig. 5 – Docusnap Web login dialog

In the login dialog, you can specify the Docusnap Server from which the data will be retrieved. Depending on the authentication scheme, you will be prompted to enter your credentials and specify the desired company (tenant).

In the *Docusnap Server URL* field, specify the protocol to be used (http or https) and the port that must be open for accessing the Docusnap Server API.

If no customizations have been made, the Docusnap Server API will be reached by using the following URL:

```
http://HOSTNAME:9001
```

To determine the URL of the server API, select *General Options - Connections - Server API Connection* in Docusnap.

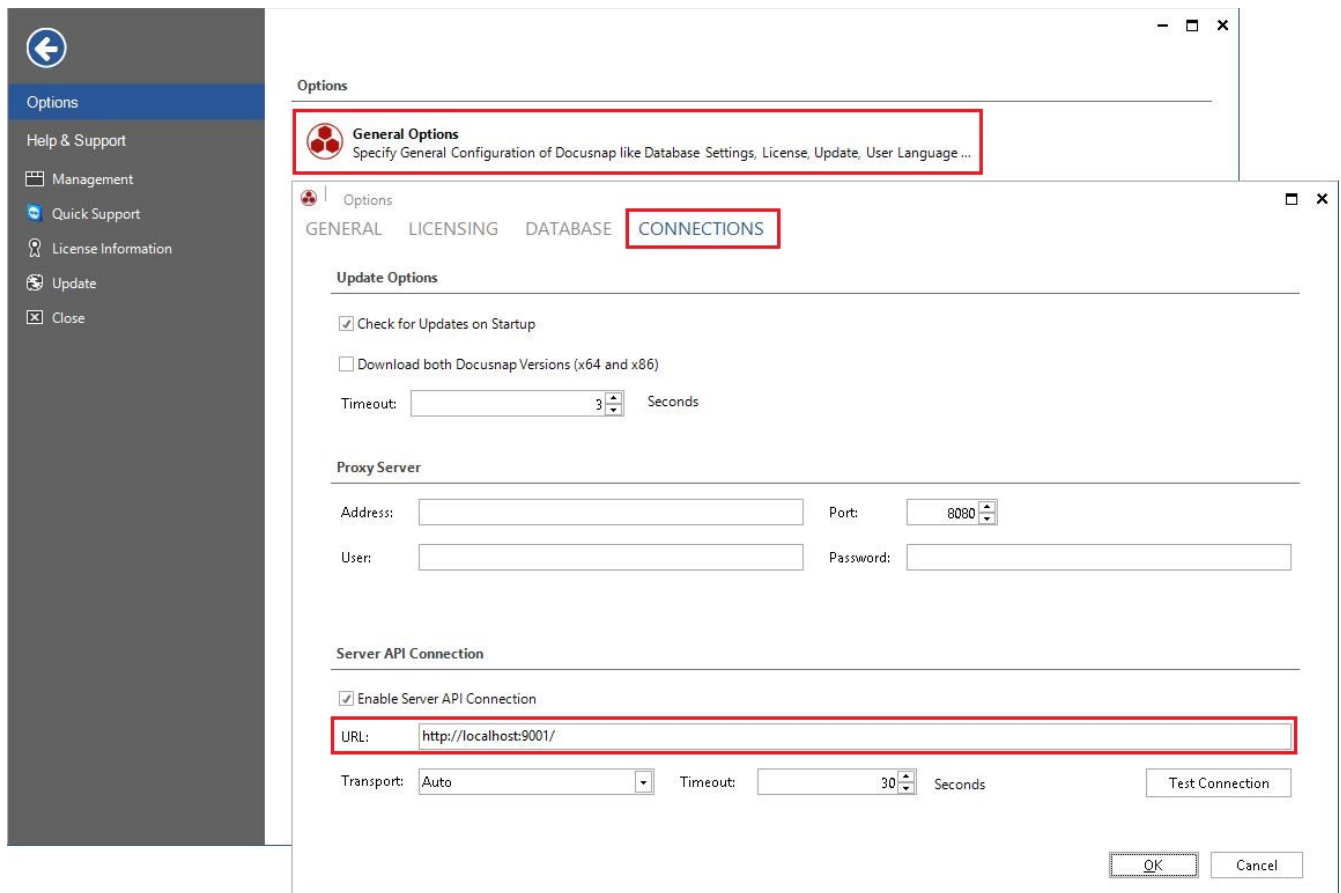


Fig. 6 – Docusnap Server API - Determining the URL

3. Optional Step: Customizing the Ports for the Web Server and the Docusnap Server API

3.1 Introduction

In some production environments, port 8181 (IIS access – static website) and port 9001 (access to the Docusnap Server API) might not be enabled. This optional chapter describes how to change the access to the Docusnap IIS web server to port 80 (http) and the access to the Docusnap Server API to port 443 (https) based on the default configuration. Communicating via these ports should be possible in most environments. In addition, querying the database via the browser even increases the security as the data transferred will be encrypted through the use of https.

3.2 Configuring the IIS (Static Website) Access with http – Port 80

Once Docusnap has been installed successfully, an ISS server resides on the system that hosts two websites:

- Default Web Site (port 80)
- Docusnap Web (port 8181)

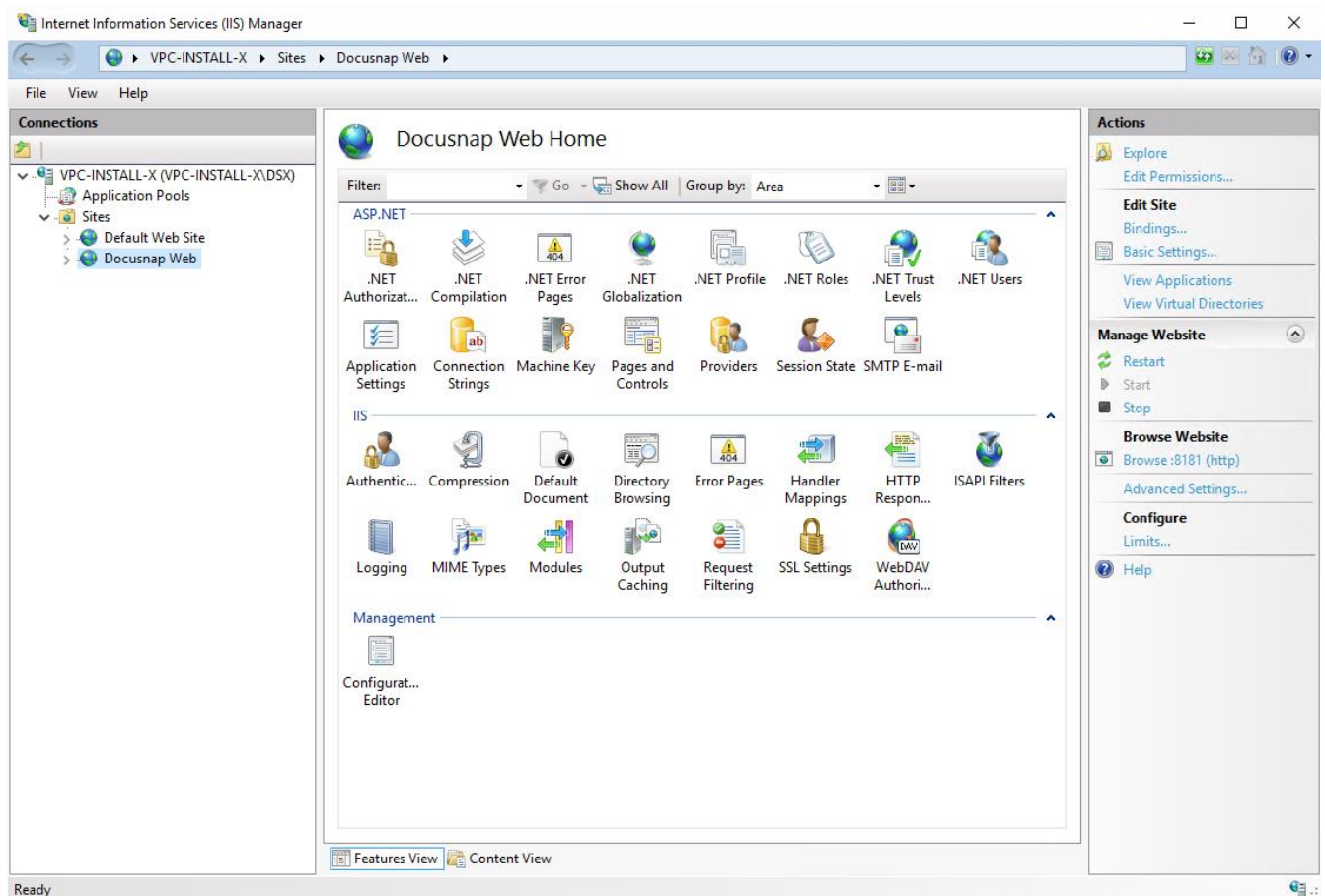


Fig. 7 – IIS Manager – Existing websites

In the first step, right-click *Default Web Site* – *Edit Bindings* and change the port from 80 to 81. In the next step, configure Docusnap Web to port 80 which is now available:

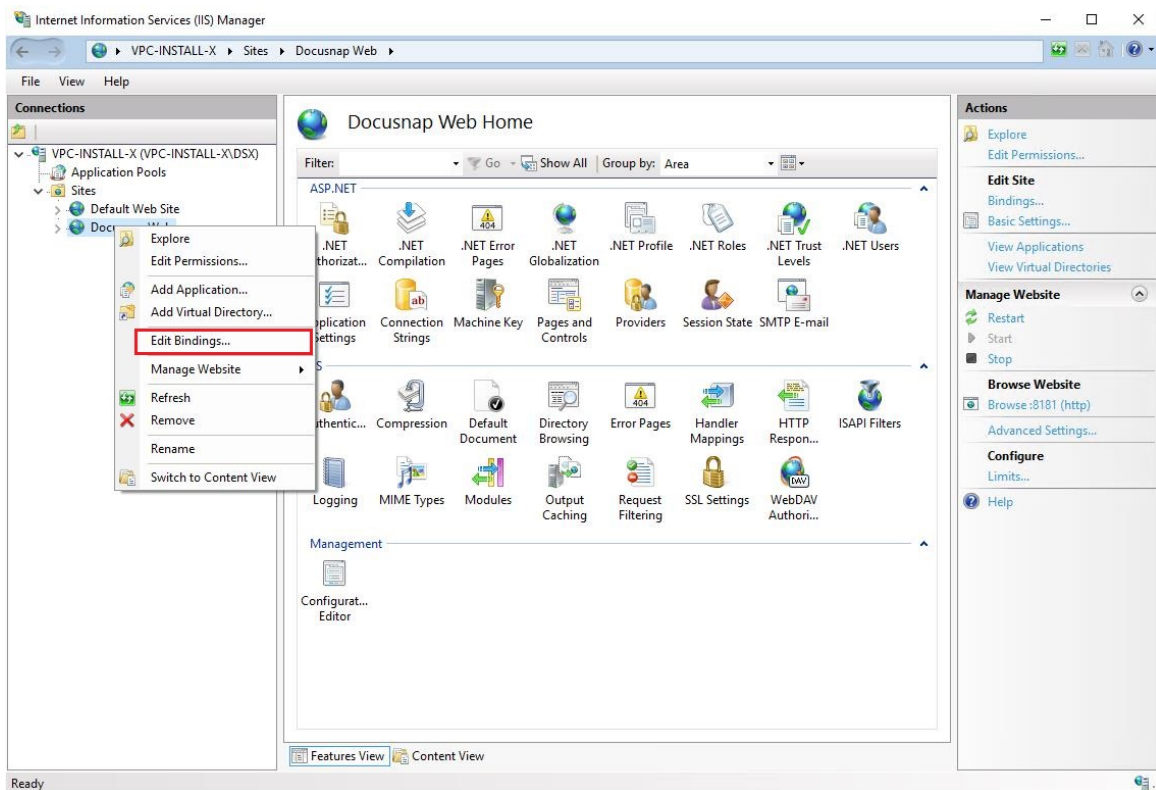


Fig. 8 – IIS Manager – Starting the Edit Bindings dialog

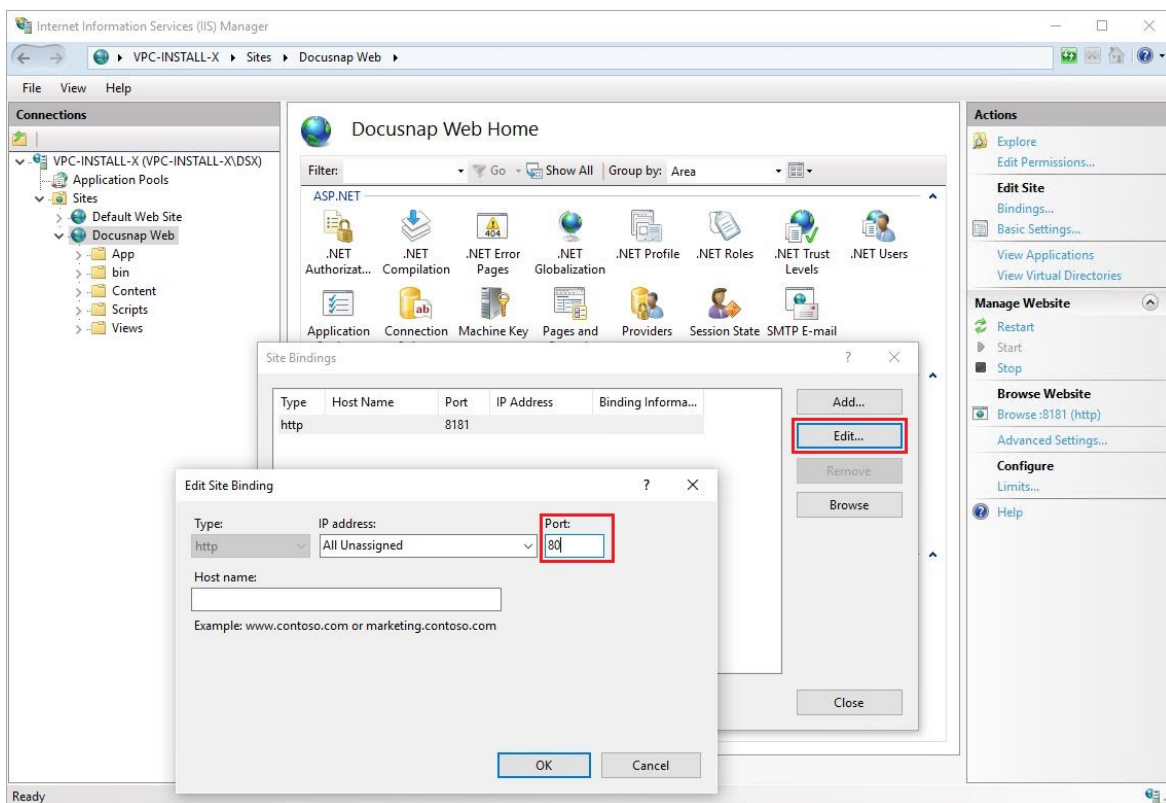


Fig. 9 – IIS Manager - Setting Docusnap Web to port 80

These changes will only become effective after a restart of the IIS Server. This can be done in the right panel of the IIS Manager under *Actions – Manage Website*.

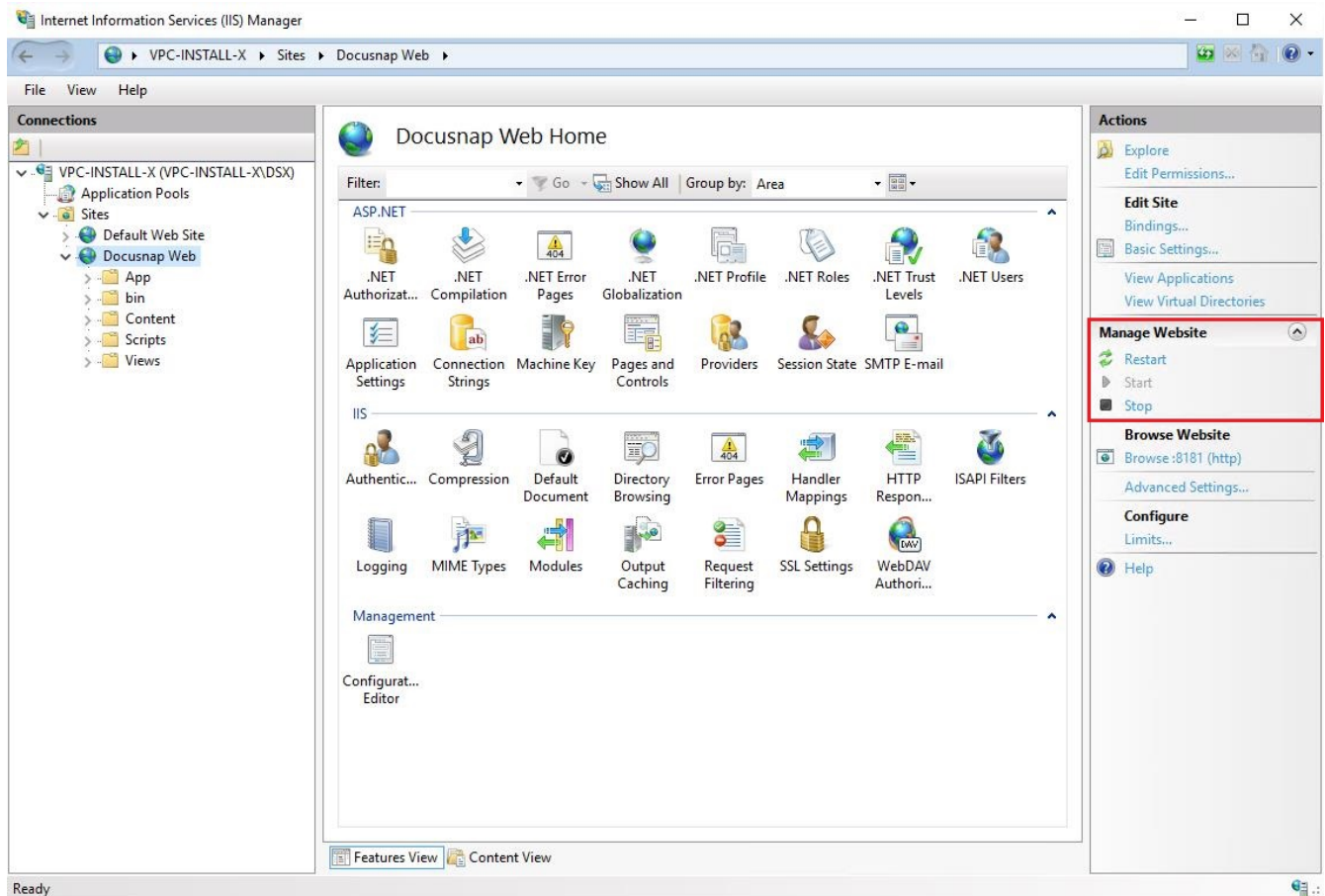


Fig. 10 - Restarting the IIS Server

As an alternative, open a CMD console with administrator rights and enter the *iisreset* command.

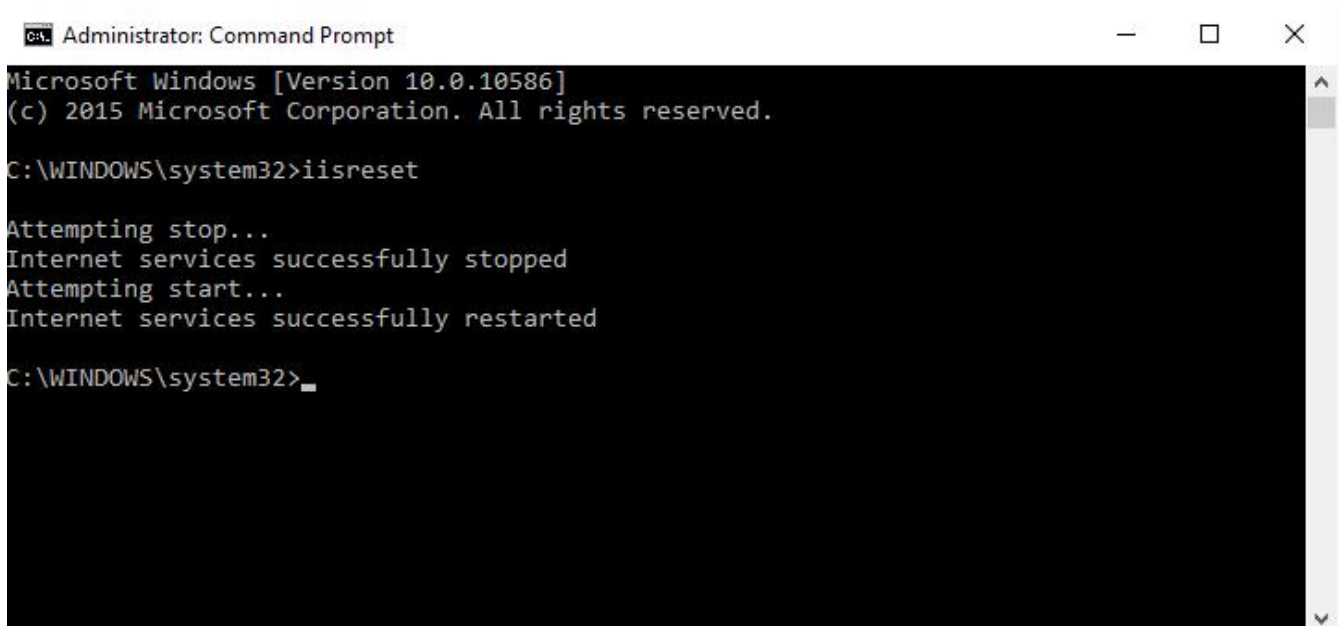


Fig. 11 - iisreset

Now, the Docusnap Web client can be called by entering *http://hostname*.

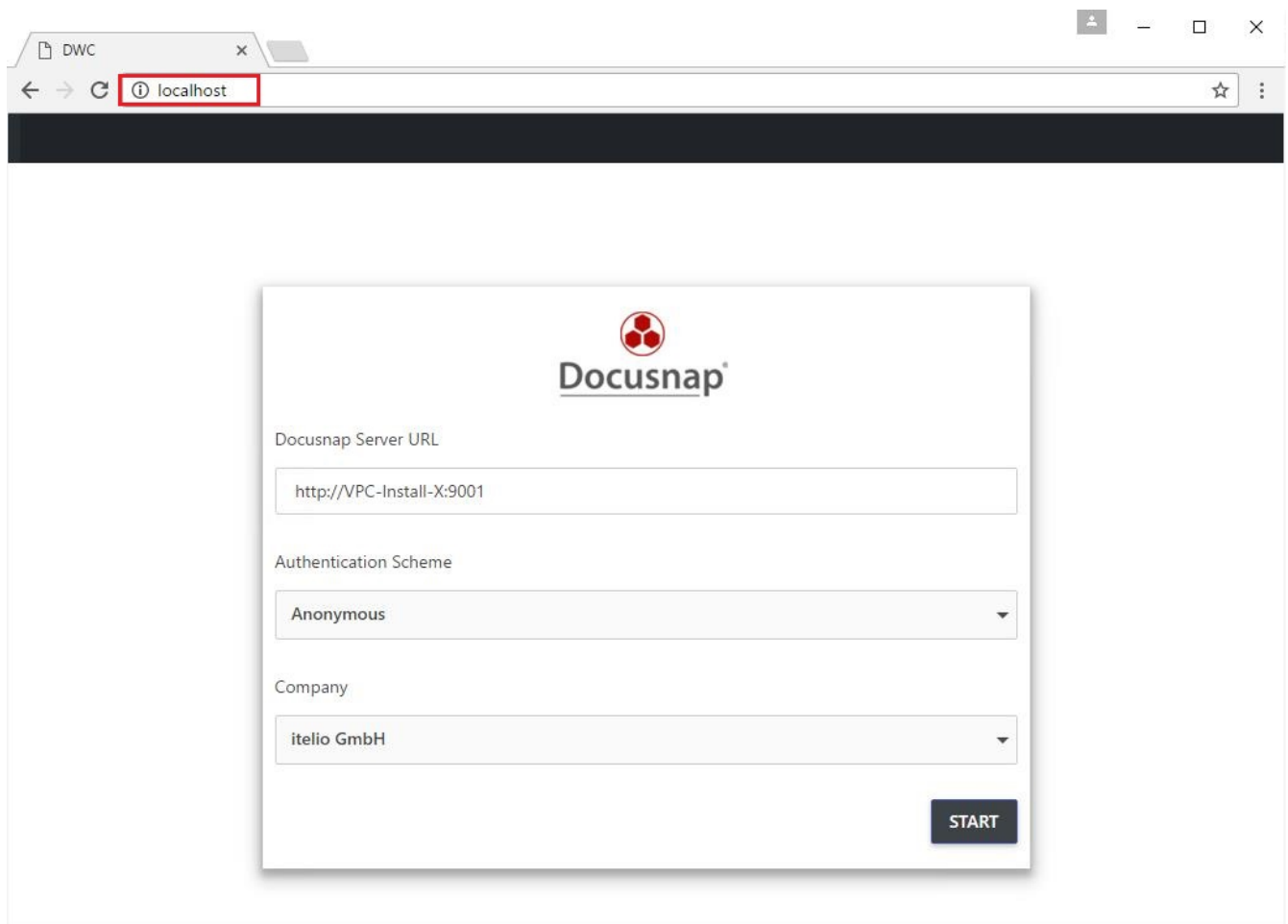


Fig. 12 – Opening the web client after the change

3.4 Configuring the Docusnap Server API Access with https – Port 443

When *changing from http to https*, a certificate is required for encryption. This example shows how to create a self-signed certificate in Docusnap and how to configure the Docusnap Server API for https using port 443. These steps will be performed in the Docusnap Server Configuration dialog.

Only the settings in step 4 – *Server API* need to be changed.

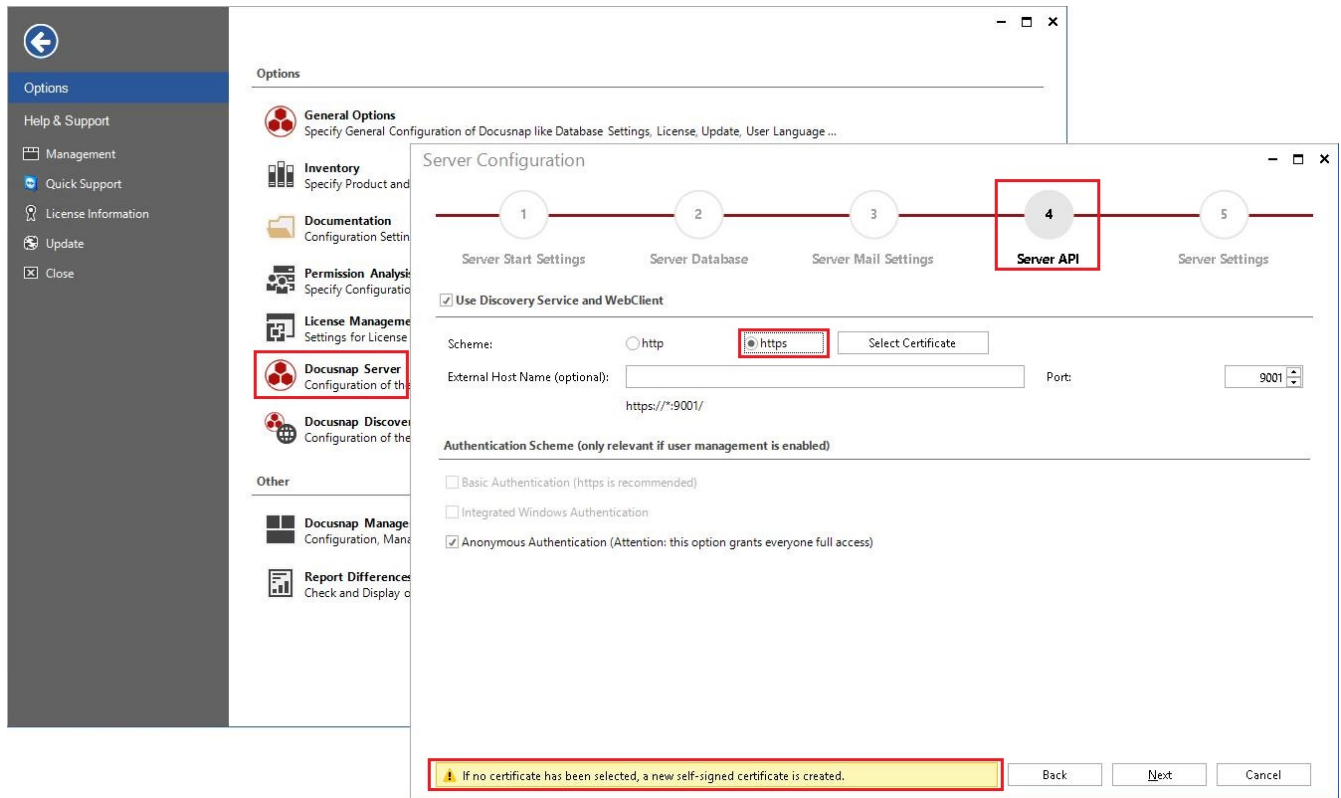


Fig. 13 – Docusnap Server Configuration – Server API

Here, configure the following settings:

- *Schema*
 - o Access via http or https
- *Select Certificate* – if you set https as the schema.
 - o You can select an existing certificate.
 - o If no certificate exists, the system will create a new, self-signed certificate during the configuration process.
- *Authentication Scheme*
 - o Authentication for accessing Docusnap Web
 - o For details, see the next chapter.

Once you have configured all properties and completed the configuration, the certificate will be installed. Confirm this by clicking Yes.

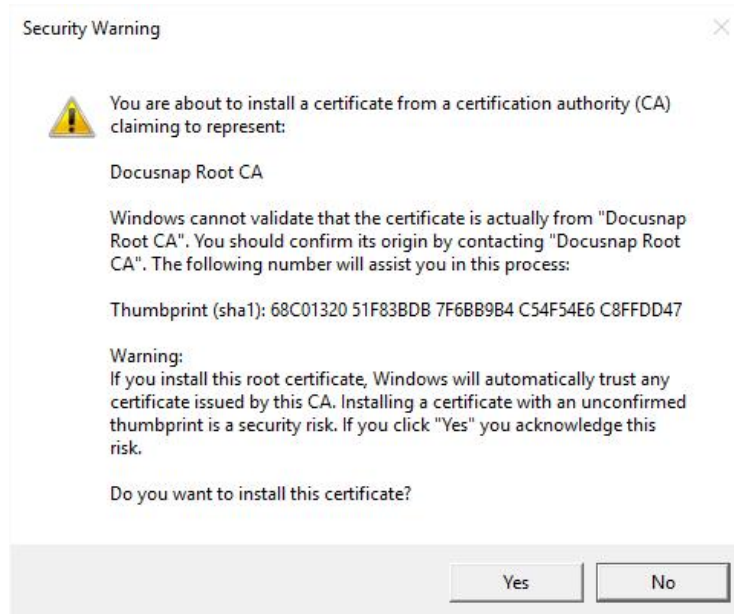


Fig. 14 - Operating system security alert – Installation of the certificate

3.4.1 Customizing the Server API Connection

Due to the change made to the Server API authentication scheme, you must customize the Server API connection URL in the next step to match the authentication scheme.

Click *General Options – Connections – Server API Connection* to change this setting. You can test the connection by clicking the **Connection Test** button.

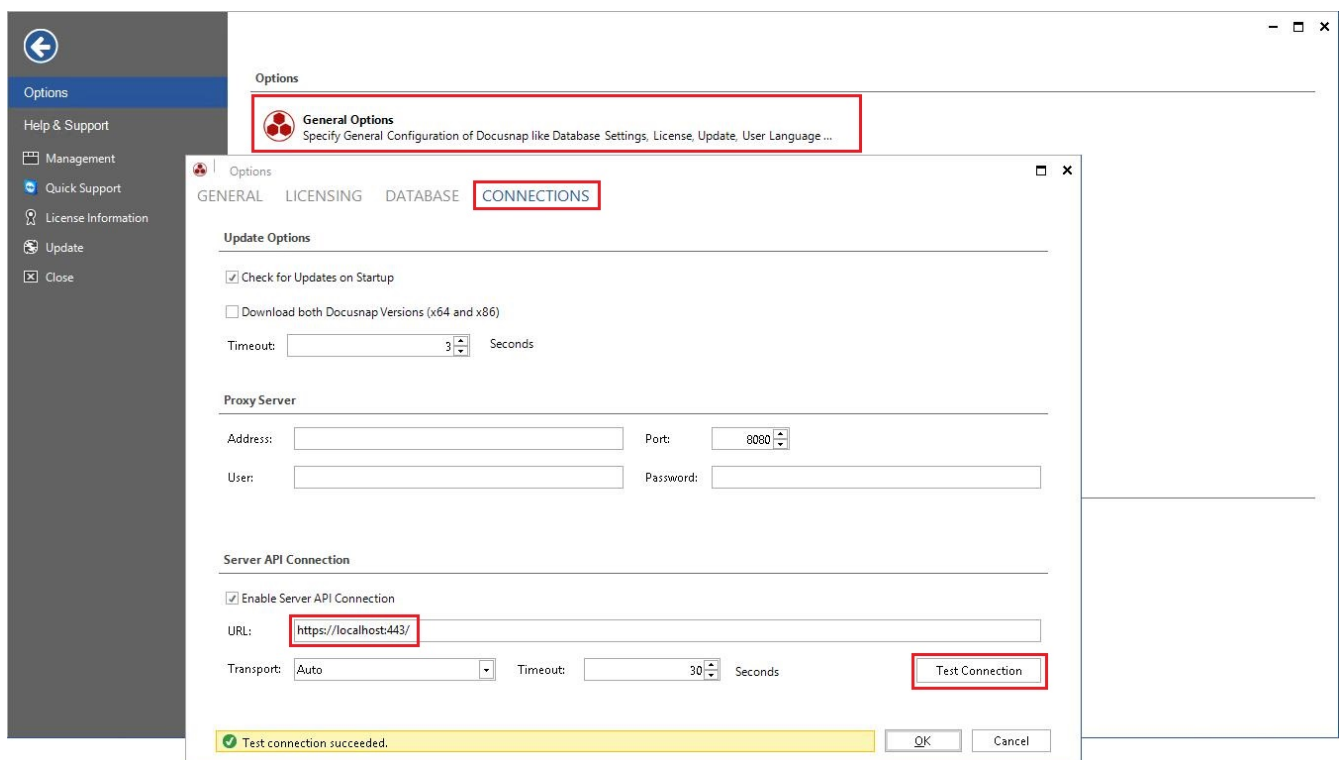


Fig. 15 – Customizing and testing the Server API connection

When you close the dialog, the Docusnap status bar will indicate that two Discovery services are active and connected via https. This completes the transition to https (port 443). In some cases, you might need to restart the Docusnap Server service.

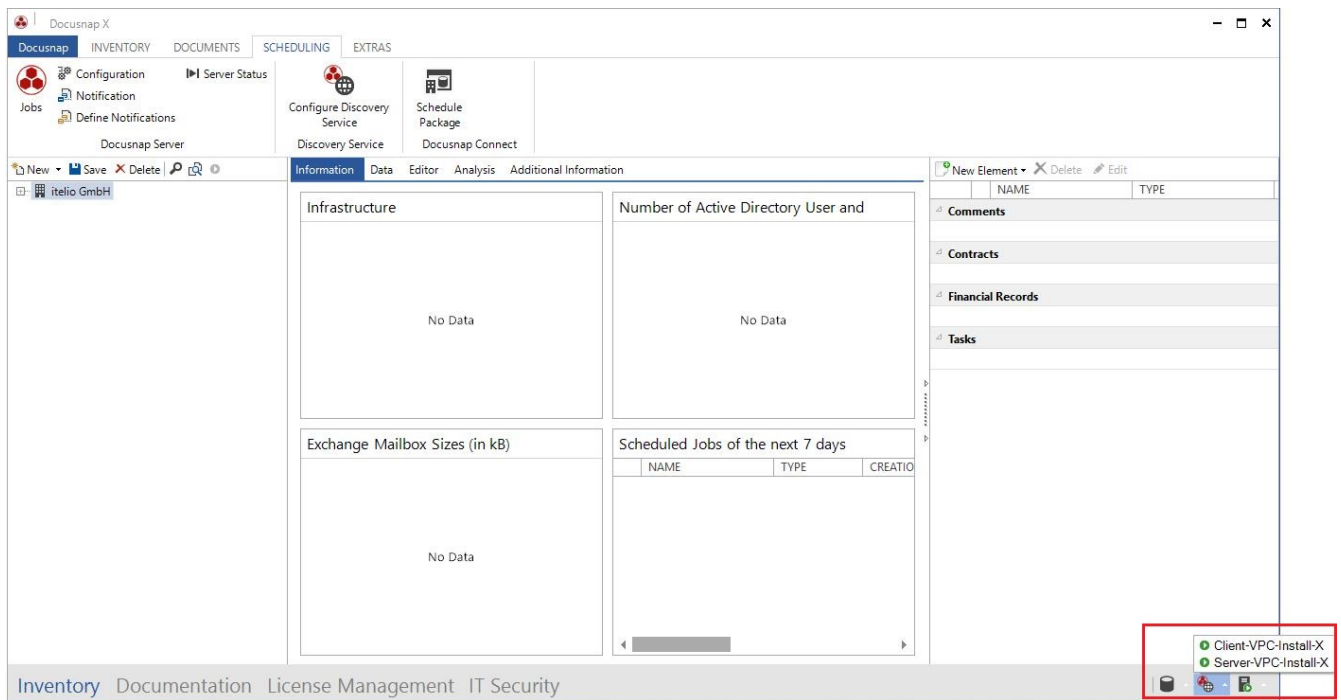


Fig. 16 – Status of the Discovery services

3.5 Docusnap Web – Testing the Connection with a Different System

Now, test the changes you made by using a different system in your network. This Windows system will be able to resolve the host name of the Docusnap computer. Enter the appropriate URL in the “Docusnap Server URL” field. The https protocol will be used automatically. Port 443 is the default https port. So there is no need to specify it explicitly.

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:

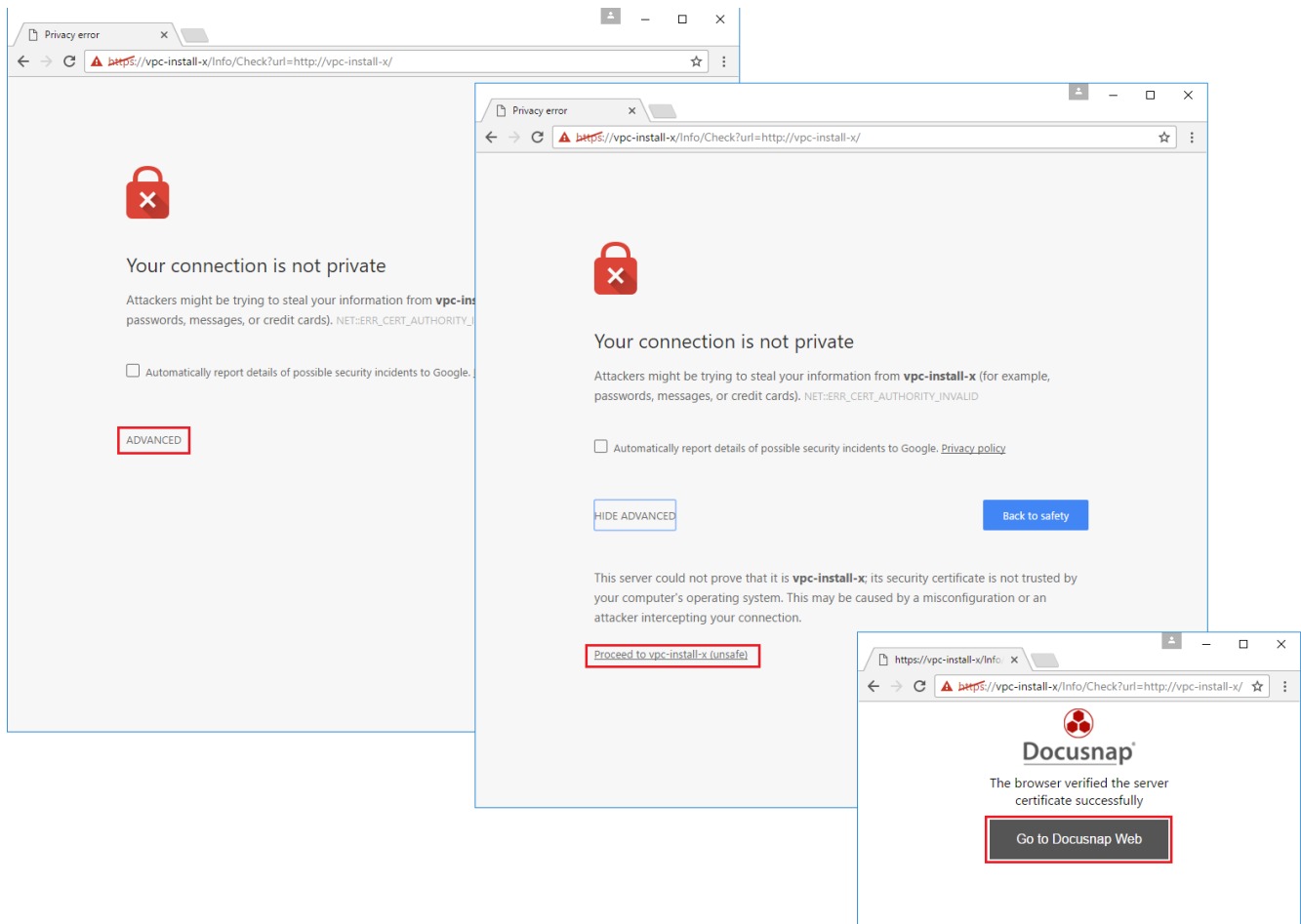


Fig. 17 – Docusnap Web – Connection test

A security alert is displayed. Click Yes to confirm. When you close this dialog, the Docusnap Web Client starts.

Depending on the certificate used to establish the https connection to the Docusnap Server API, a security alert might be displayed.

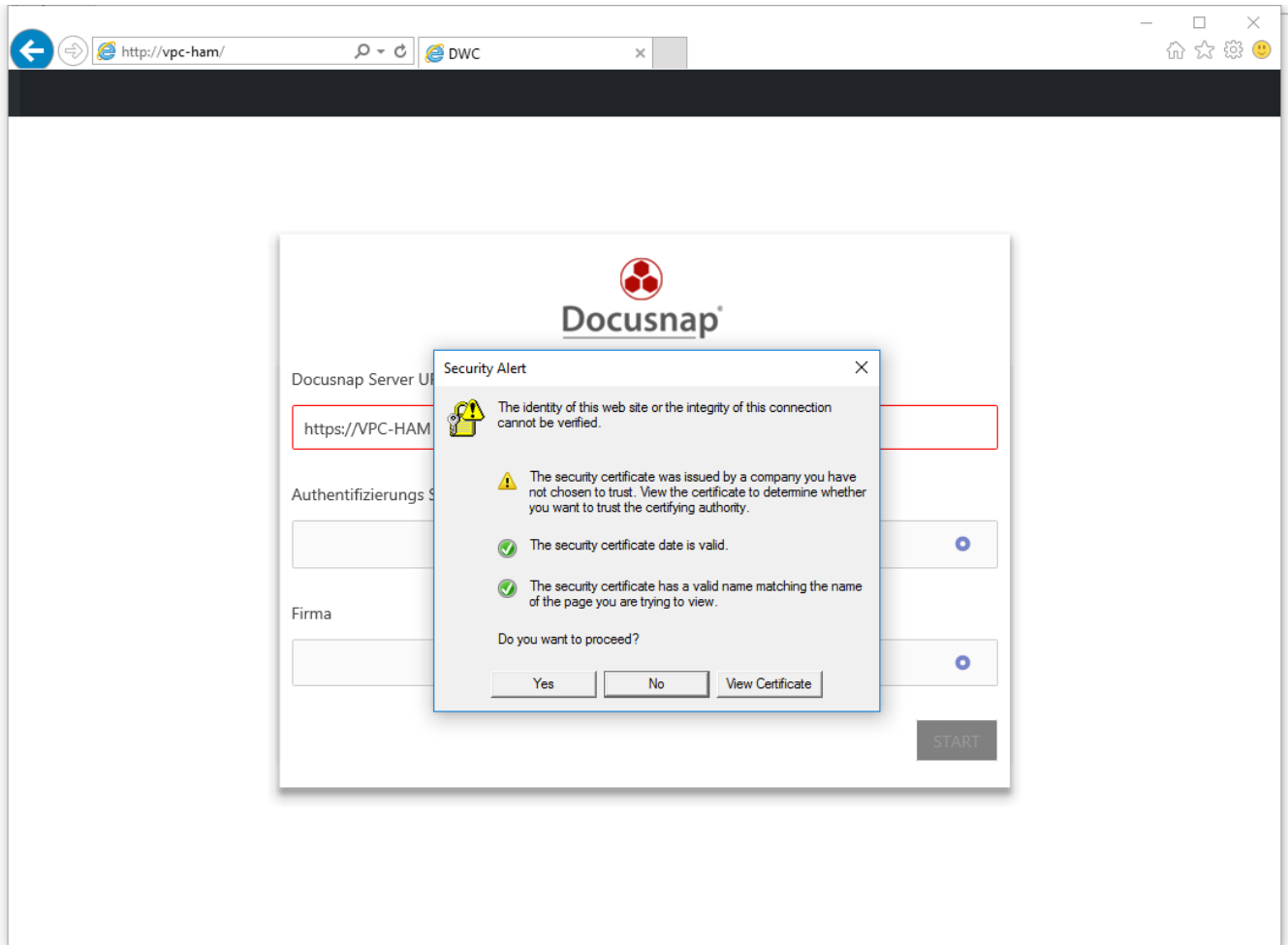


Fig. 18 – Operating system security alert

4. Managing User Access to Docusnap Web

As explained above, the authentication scheme for accessing Docusnap Web can be changed during the configuration of the Docusnap Server (Server API). 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.

4.1 Enabling User Management

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

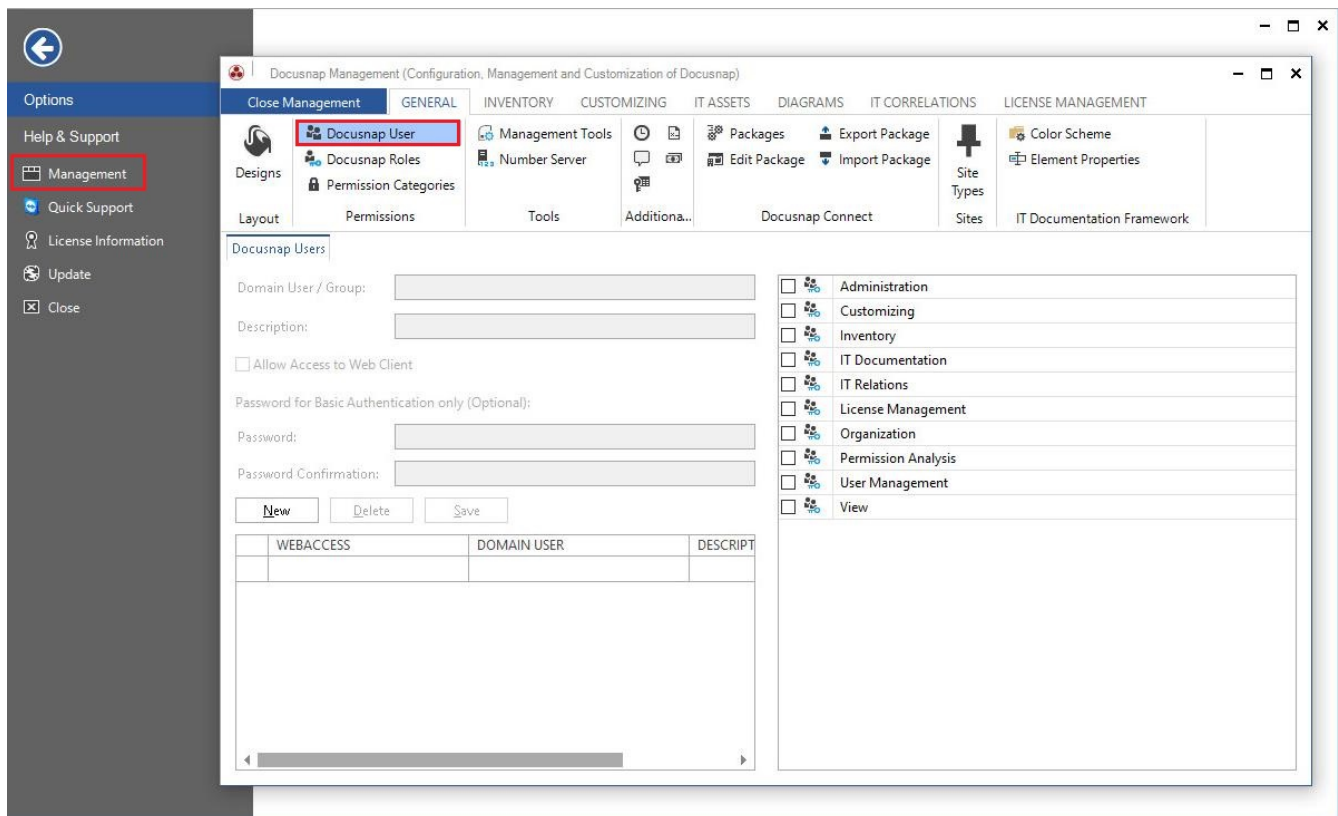


Fig. 19 – User Management

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](#)

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

The Basic Authentication scheme requires you to enter a password for accessing the Web Client. With the Integrated Windows Authentication scheme, no password is required.

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 who are supposed to work with the Docusnap Client must be assigned corresponding user roles!

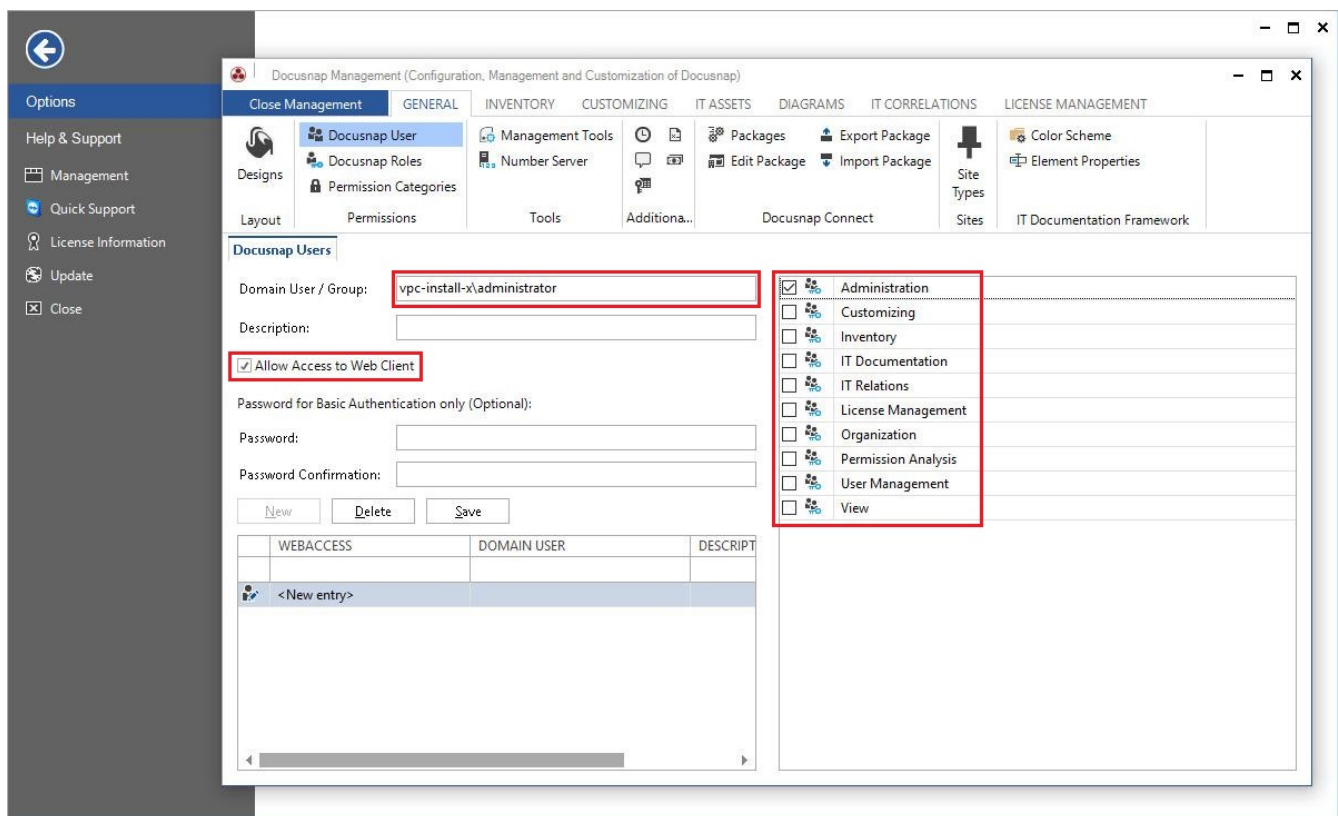


Fig. 20 – Adding users when using the Integrated Windows Authentication scheme

4.2 Configuring the Authentication Scheme for Docusnap Web

To change the authentication scheme for the access to the Web Client, open the Docusnap Server Configuration dialog – step 4 - Server API.

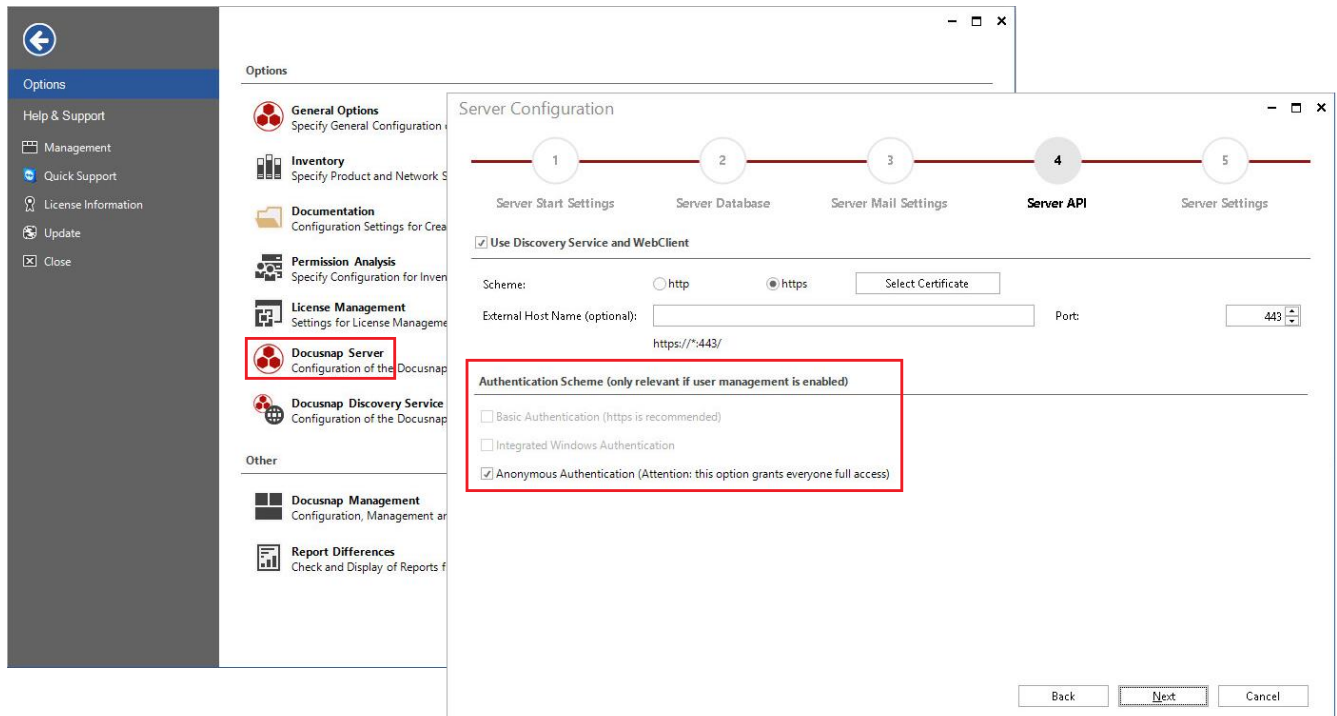


Fig. 21 – Selecting the authentication scheme

4.2.1 Anonymous Authentication

If you select this authentication scheme, no authentication will be performed by the IIS. Each user who is able to reach this system via the network can open the Docusnap Web Client.

4.2.2 Basic Authentication

If you select this authentication scheme, users can access Docusnap Web only after having entered their credentials (i.e. user name and password). Since this data is transmitted as plain text, https should be configured for the Docusnap Server API when using this authentication scheme. Use this scheme in the following cases:

- Anonymous Authentication is not desired
- Integrated Windows Authentication is not possible (e.g. the system is a member of a work group or is located outside the Intranet)

4.2.3 Integrated Windows Authentication

With this scheme, the system checks whether the logged-on domain or system user is enabled in the Docusnap User Management and whether that user has the permission to access Docusnap Web. For opening Docusnap Web, no credentials need to be entered here. This authentication scheme is the most complex one, but ensures maximum security. Restricting the access to Docusnap in this way was already possible in the previous Docusnap versions. In Docusnap X, this functionality was extended to include Docusnap Web.

LIST OF FIGURES

FIG. 1 – OVERVIEW OF THE DOCUSNAP WEB ARCHITECTURE	5
FIG. 2 – DOCUSNAP X , FIRST START, CONFIGURATION WIZARD	6
FIG. 3 – SETUP FILE LOCATION IN THE FILE SYSTEM	7
FIG. 4 – DOCUSNAP WEB SETUP – INSTALLATION STEPS.....	8
FIG. 5 – DOCUSNAP WEB LOGIN DIALOG	9
FIG. 6 – DOCUSNAP SERVER API - DETERMINING THE URL	10
FIG. 7 – IIS MANAGER – EXISTING WEBSITES	11
FIG. 8 – IIS MANAGER – STARTING THE EDIT BINDINGS DIALOG.....	12
FIG. 9 – IIS MANAGER - SETTING DOCUSNAP WEB TO PORT 80	12
FIG. 10 - RESTARTING THE IIS SERVER	13
FIG. 11 - IISRESET.....	13
FIG. 12 – OPENING THE WEB CLIENT AFTER THE CHANGE	14
FIG. 13 – DOCUSNAP SERVER CONFIGURATION – SERVER API.....	15
FIG. 14 - OPERATING SYSTEM SECURITY ALERT – INSTALLATION OF THE CERTIFICATE	16
FIG. 15 – CUSTOMIZING AND TESTING THE SERVER API CONNECTION	16
FIG. 16 – STATUS OF THE DISCOVERY SERVICES	17
FIG. 17 – DOCUSNAP WEB – CONNECTION TEST	18
FIG. 18 – OPERATING SYSTEM SECURITY ALERT	19
FIG. 19 – USER MANAGEMENT	20
FIG. 20 – ADDING USERS WHEN USING THE INTEGRATED WINDOWS AUTHENTICATION SCHEME	21
FIG. 21 – SELECTING THE AUTHENTICATION SCHEME	22

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

