Net at Work
Building IT-Excellence.

NoSpamProxy Web Portal 13.2

Installation Manual

- Protection
- Encryption
- Large Files

Imprint

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn

Trademarks

13 February 2020

Contents

1. Introduction

The Web Portal is an extension for NoSpamProxy Encryption and NoSpamProxy Large Files

Certificate-Free Encryption with the Web Portal

If you are using NoSpamProxy Encryption, you can install the Web Portal via a separate setup. The Web Portal is used for encrypted communication with partners who do not have their own encryption key such as certificates or PGP keys. Messages can be sent to the recipient via encrypted PDF documents. Replies to the message are composed directly via the web portal and sent back to the sender of the original email. The Web Portal communicates with the intranet role and can thus receive all the information it needs to function properly.

Passwords for PDF Mail

The passwords for PDF Mail can now be stored in the Partner node of the Management Console. These passwords are replicated to all connected gateway roles and web portals. If the password is changed, the partner will receive an email notification of this change. If no password is available for PDF Mail, the outgoing email will be queued.

Large Files

Large Files allows you to easily and securely send large files without media interruption directly from Outlook. Users can also send large files that exceed the limitations of the email application without media interruption with a single click. Using Large Files is as easy as sending conventional file attachments. In contrast to common cloud-based file transfer services the data is provided by the customer's own web server and transmitted in encrypted form via SSL. The security level of the solution meets critical business requirements at all times.

2. Prerequisites and Preparation for Installation

Prerequisites

The following prerequisites exist for the installation of the Web Portal:

- Windows Server 2008 R2 or later.
- .NET Framework 4.7.2 (will be installed during installation, if required).
- Microsoft SQL Server. During the installation, you can either install the free Microsoft SQL Server 2012 Express Edition or use an existing SQL Server. The Web portal supports Microsoft SQL Server 2008 or later in the Express, Standard, or Enterprise editions.

If NoSpamProxy and Microsoft Exchange are installed on the same server, make sure that Exchange supports the respective version of the .NET Framework before installing or upgrading. The Exchange Server Supportability Matrix offers an overview of supported versions.

Preparations

Depending on the planned installation environment, different preparations are necessary.

- **Open ports on the firewall**
  If you are using a firewall, the port provided for the NoSpamProxy Web Portal must be open. This is usually port 443.
- **IIS on a Gateway Role**
  If the IIS is installed on the same system as one of the gateway roles, please deactivate the SSL loopback check. The procedure is described in the Microsoft Knowledge Base http://support.microsoft.com/kb/896861. Please use 'Method 1' to set up an exception for the connection to this address. 'Method 2' is not recommended as it would disable an essential security feature of your server.
- **Web Portal in the DMZ / not part of the domain**
  If the Web Portal is installed on a computer in the DMZ or if it is not part of the domain, please deactivate the UAC Remote Restrictions. The procedure is described in the Microsoft Knowledge Base http://support.microsoft.com/kb/951016.

3. Help and Support

Net at Work provides you with help and support for the installation and the operation of NoSpamProxy.

- **Training videos**
  The Training videos provide an overview of different areas and show step by step configurations, in the concrete application case.
- **Blog**
  Our blog Blog provides you with information on new product versions, suggested changes for your configuration, compatibility issues and more. You can also find the latest blog posts on the start page of the NoSpamProxy management console.
- **Knowledge Base**
  The Knowledge base contains further technical information on special issues.
- **Support**
  You can also visit our Support website for additional information and contact options. .

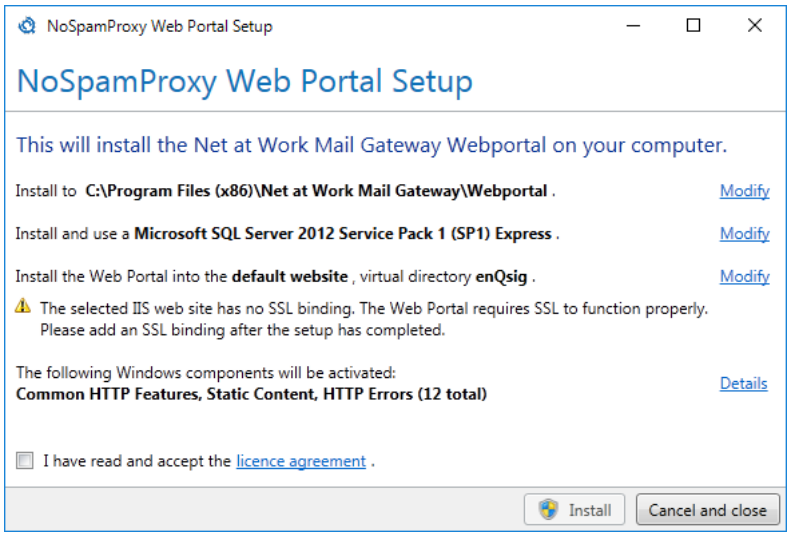
4. Installing the Web Portal

This chapter describes the installation of the NoSpamProxy Web Portal.

See chapter Upgrades for information on available upgrades. Otherwise, complete functionality cannot be guaranteed.

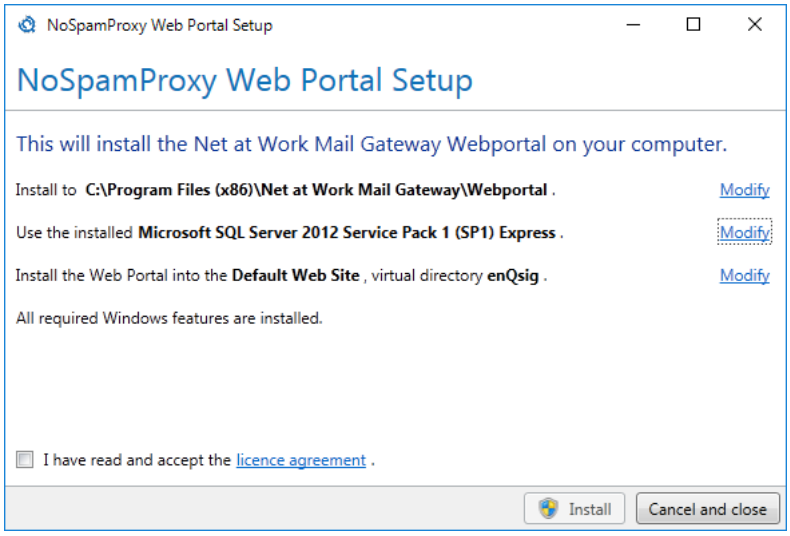
Starting the Installation

Close all Windows applications before starting the installation. Upon startup, the installation routine determines the existing system configuration and automatically proposes default settings for the installation. (Picture 1). You can change the respective settings at the end of each line by clicking on **Modify** and change it if necessary.



Picture 1: Summary of installation options for first-time installation

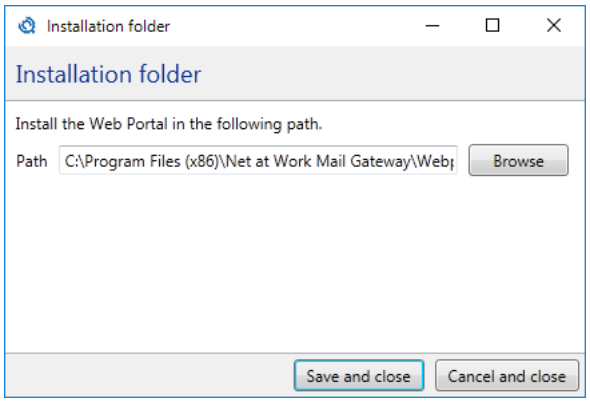
If you reinstall the Web Portal or the Internet Information Services (IIS), the overview displays differing settings. (Picture 2).



Picture 2: Summary of installation options in case IIS are already configured

Installation Folder

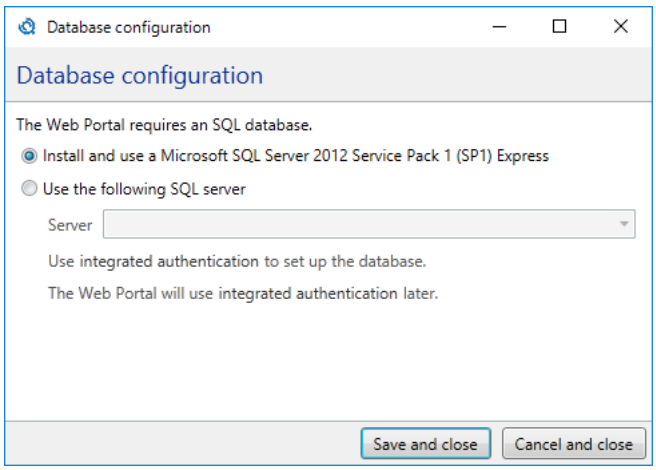
Specify the installation folder for the Web Portal (Picture 3).



Picture 3: Selection of the installation folder

Configuring the Database

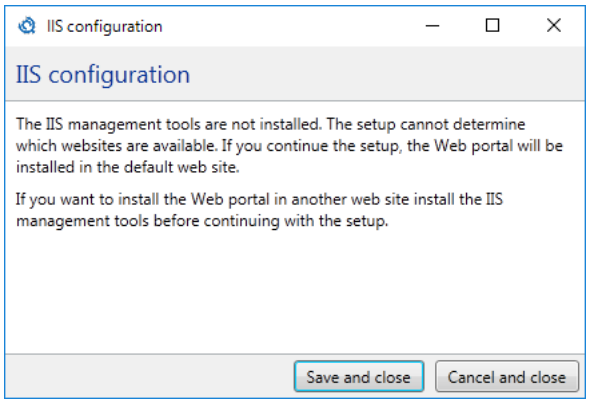
The Web Portal requires a database. An existing SQL Server instance can be used; alternatively, the setup installs a Microsoft SQL Server 2012 Express Edition (Picture 4).



Picture 4: Database selection

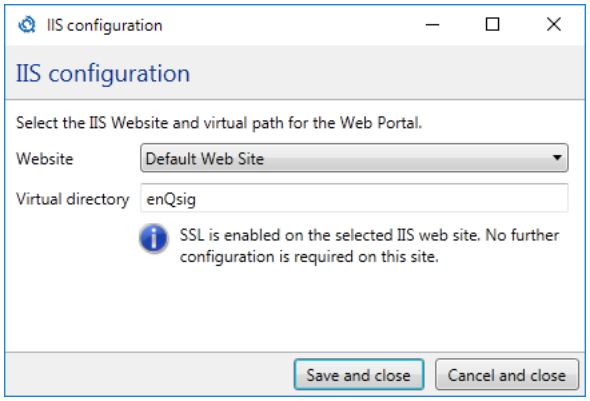
IIS Configuration

If you want to install the Web Portal into a specific website or virtual directory, you need the 'IIS Management Tools'. If not yet installed, the setup offers you the installation of the 'IIS Management Tools' into the virtual directory "enQsig" within the standard website (Picture 5).



Picture 5: Indicates that the default settings must be used

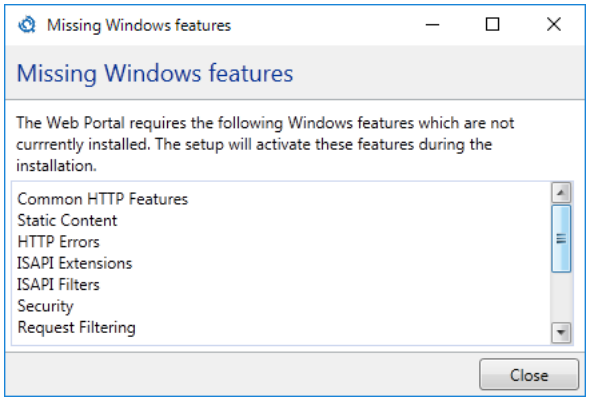
If you want to install the Web Portal on another website or virtual directory, you must first cancel this installation and install the 'IIS Management Tools'. Then select the website and the virtual directory (Picture 6). For each of the selected websites you will be notified whether SSL is already configured or whether further steps are necessary .



Picture 6: Open Server Certificates Selection of the website and the virtual directory into which the Web Portal is to be installed

Missing Windows Features

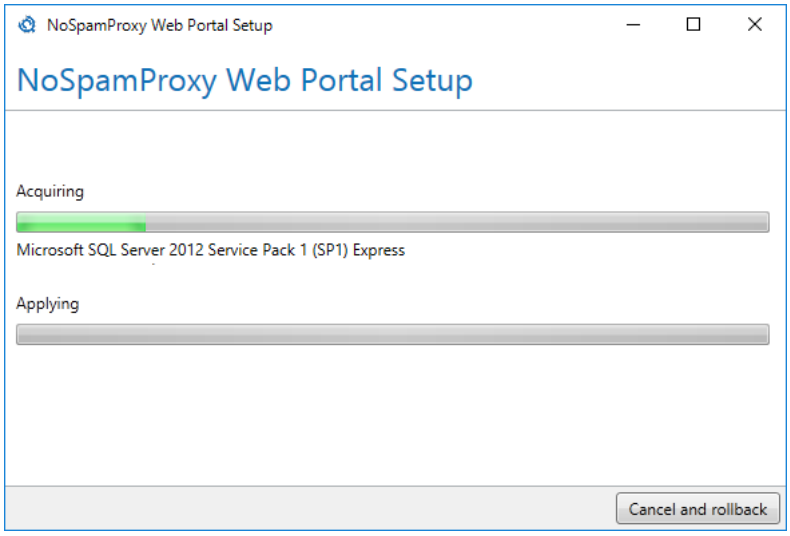
In case Windows features are missing for the installation, they are automatically activated. Via **Details** you can view all Windows features that will be activated when the installation is complete.



Picture 7: Windows features which will be activated

Installation Procedure

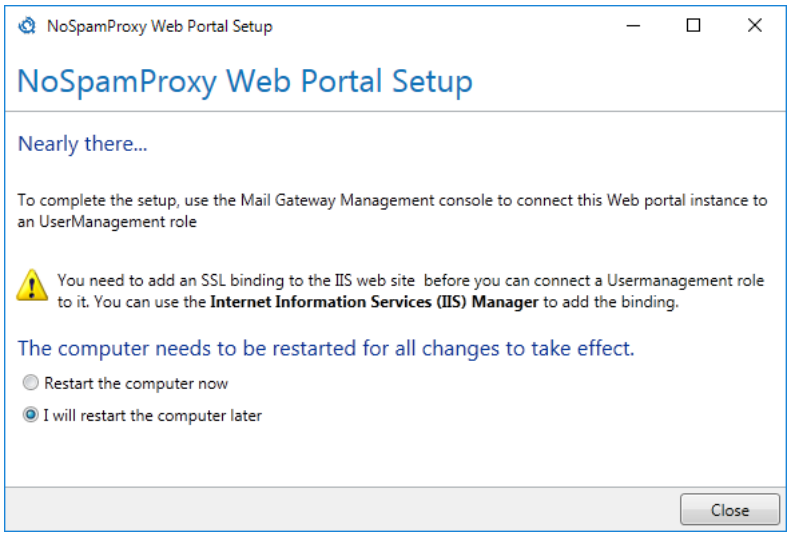
After reading and accepting the license terms, you can use **Install** to start the installation. All the steps shown in the overview will be carried out (Picture 8).



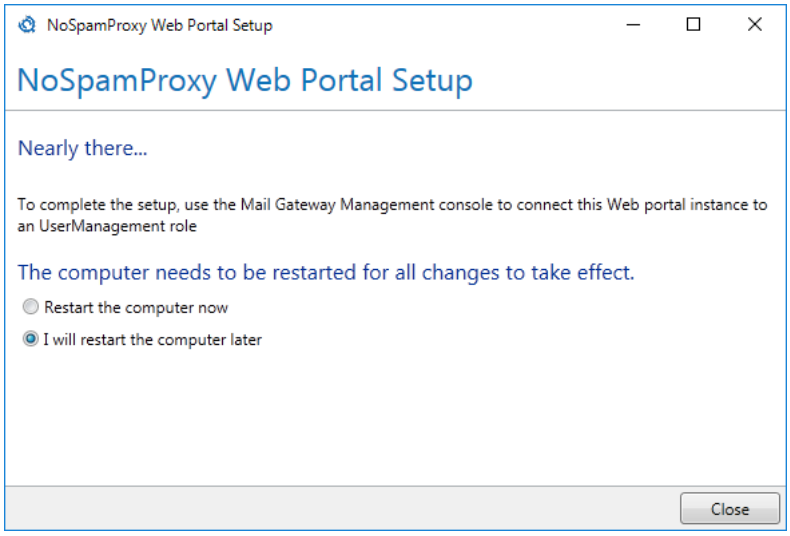
Picture 8: The progress of the installation

Completion of the Installation

After successful installation, the application will inform you about further steps to be taken. It may be necessary to configure an SSL access for the Web Portal, (Picture 9) or, if the configuration has already been carried out, to restart the computer. (Picture 10).



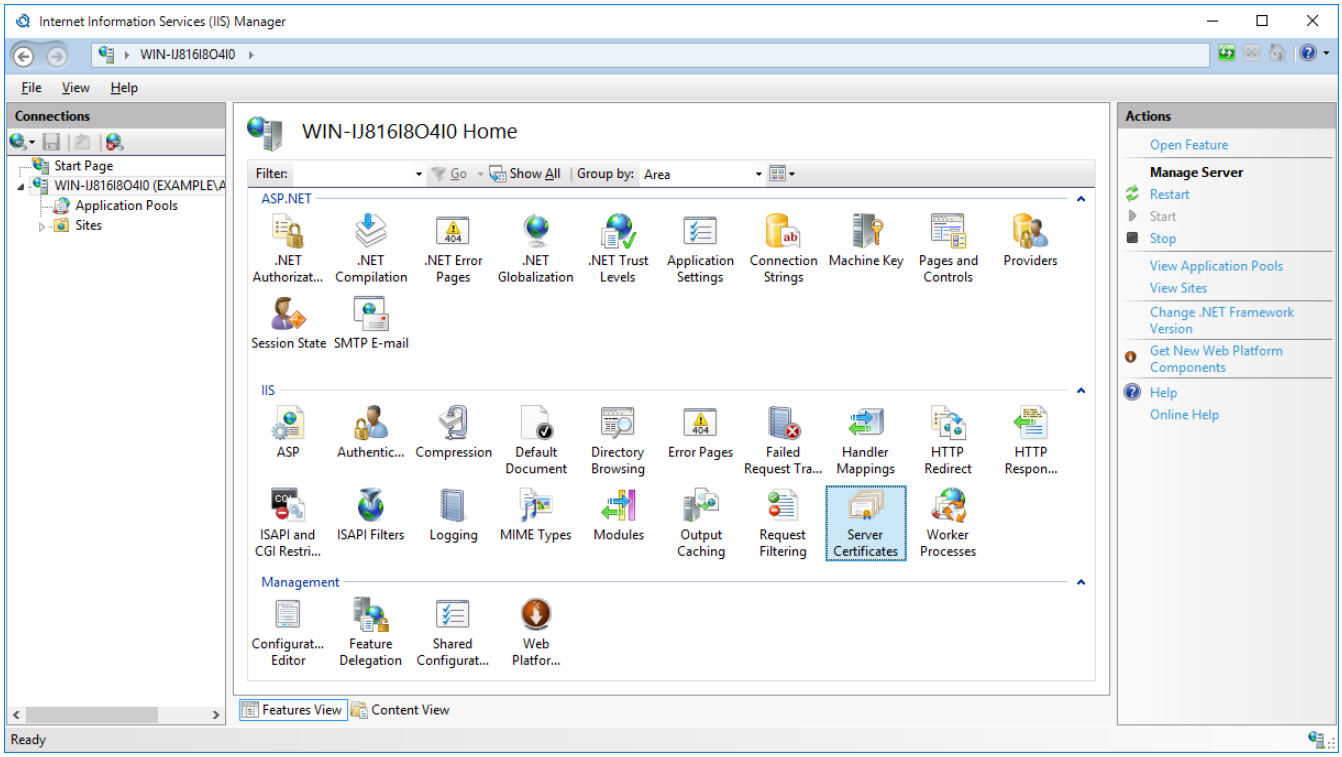
Picture 9: Completion of installation without SSL binding



Picture 10: Completion of installation with successful SSL binding

5. Installing an SSL Certificate in the IIS

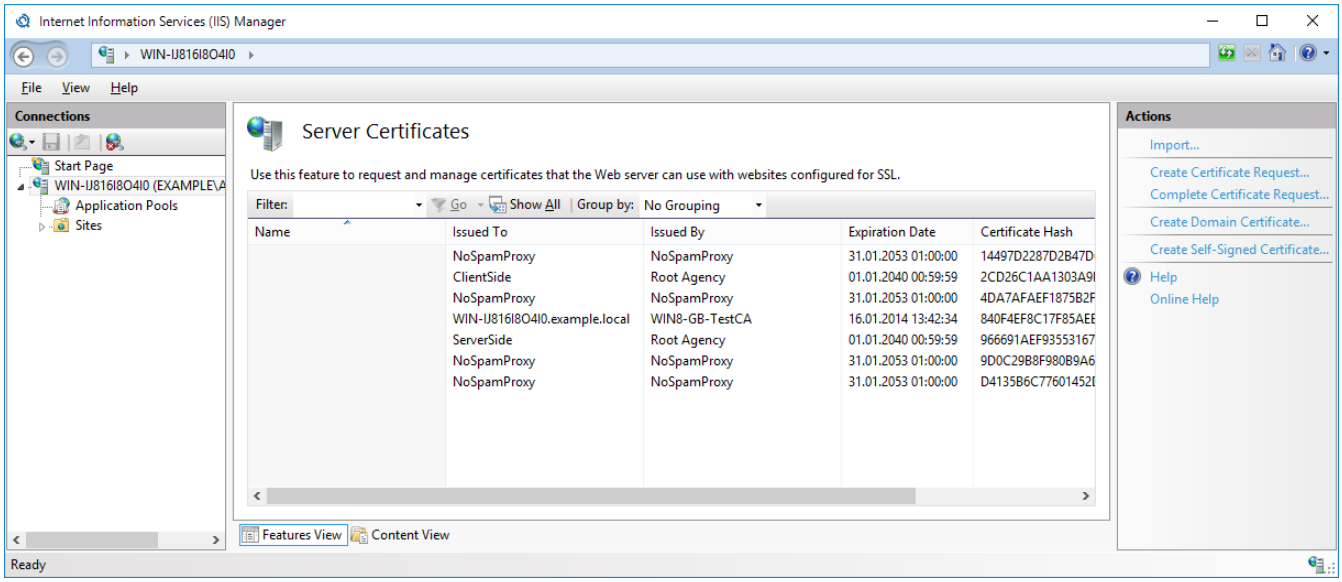
To configure SSL access for the Web Portal, open the Internet Information Services (IIS) Manager. (Picture 11). Choose "Server Certificates" by double-clicking. The list of server certificates opens. (Picture 12). Check whether your own certificate for SSL access is displayed here.



Picture 11: The IIS Manager

Locating an Existing Certificate

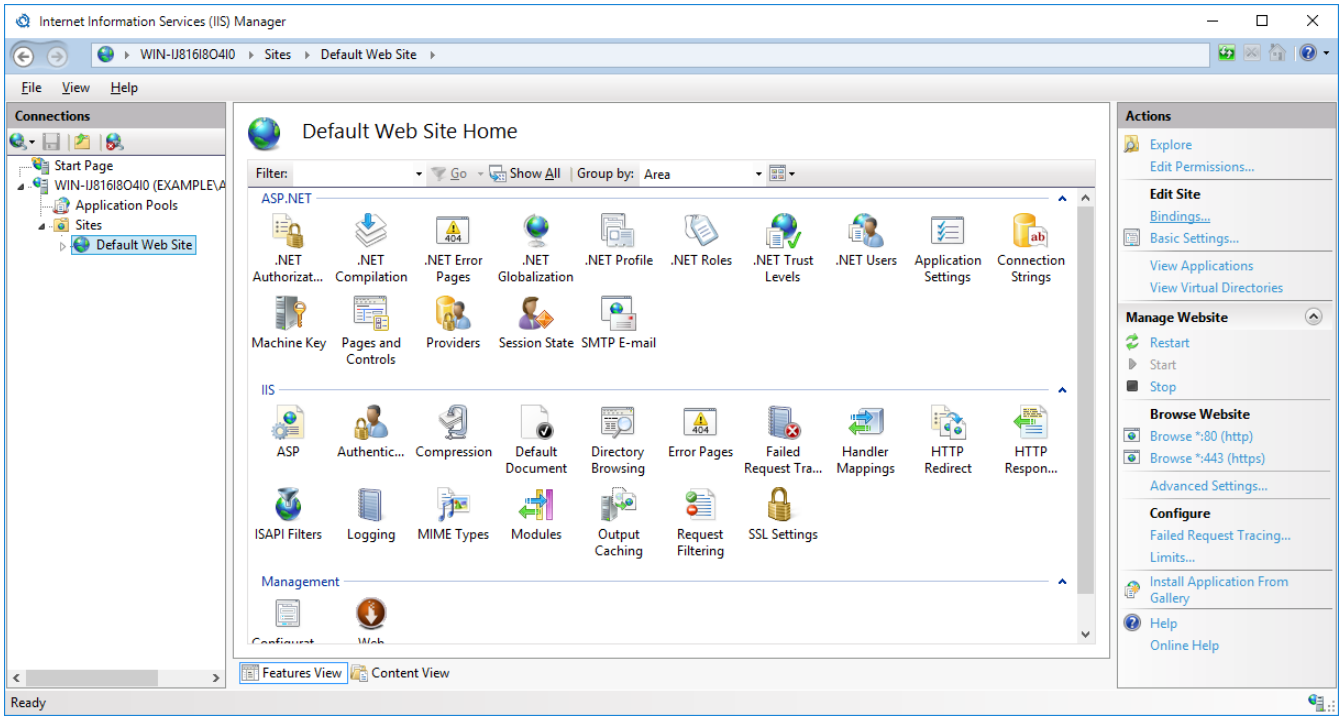
Server certificates must be stored in the certificate store of the local computer account. They are located in the **Personal** store . All certificates that can be used for SSL are listed under **Server Certificates** of the IIS Manager (Picture 12). Make sure your certificate is listed.



Picture 12: List of all server certificates

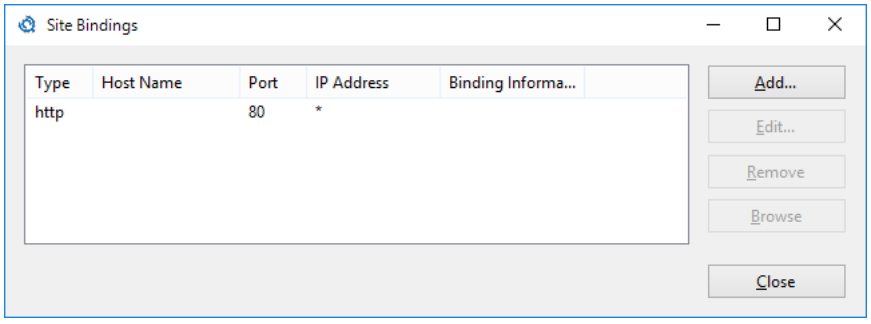
Make sure that the SSL certificate you are using contains, among other things, the exact FQDN that you use to call the Web portal. For example, if you want to operate the Web portal using the URL `https://portal.example.com/enqsig`, the name must appear as `portal.example.com` in the SSL certificate. Furthermore, make sure that the issuer of this certificate is registered on the server of the Intranet role as a trusted root certificate authority. You can access the list of trusted root certificate authorities in the certificate store of the local computer account. To verify this, open Internet Explorer on the server of the Intranet Role and enter the URL of the Web Portal, here `https://portal.example.com/enqsig`. The page must open without error messages. If this is the case, the connection to the Web portal in the Intranet Role can also be successfully added.

In the IIS Manager tree, select from the menu bar under **Sites** the web site into which the Web Portal has been installed. For a standard installation, it is called **Default Web Site**. (Picture 13) Right-click to select **Edit Bindings**, or go to the **Actions** menu and select the option **Bindings**.



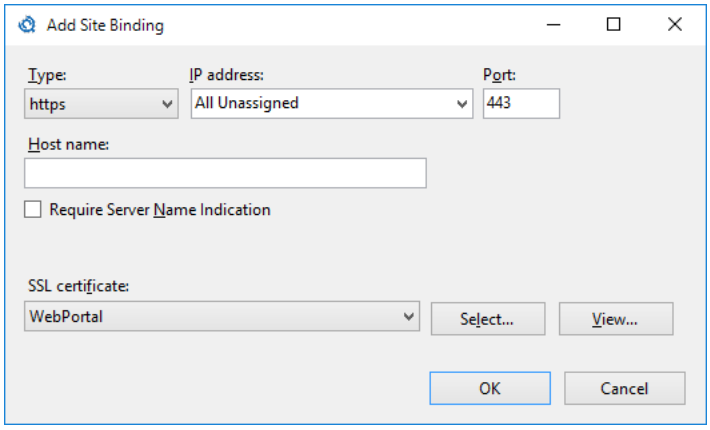
Picture 13: Configuring the Web Portal website

Click **Add** to add a new binding (Picture 14).



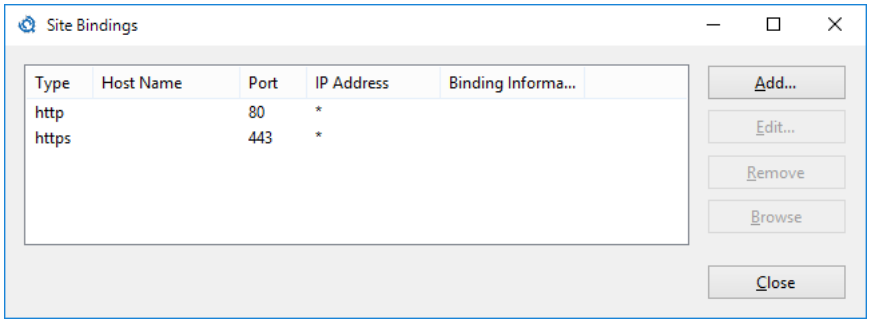
Picture 14: List of all bindings

Select a specific IP address, port 443, and the previously verified SSL certificate, if any.



Picture 15: Creating a new HTTPS binding

Upon closing of the dialog, the new site binding appears in the list of all website bindings. (Picture 16).



Picture 16: List of all bindings with the newly created HTTPS binding

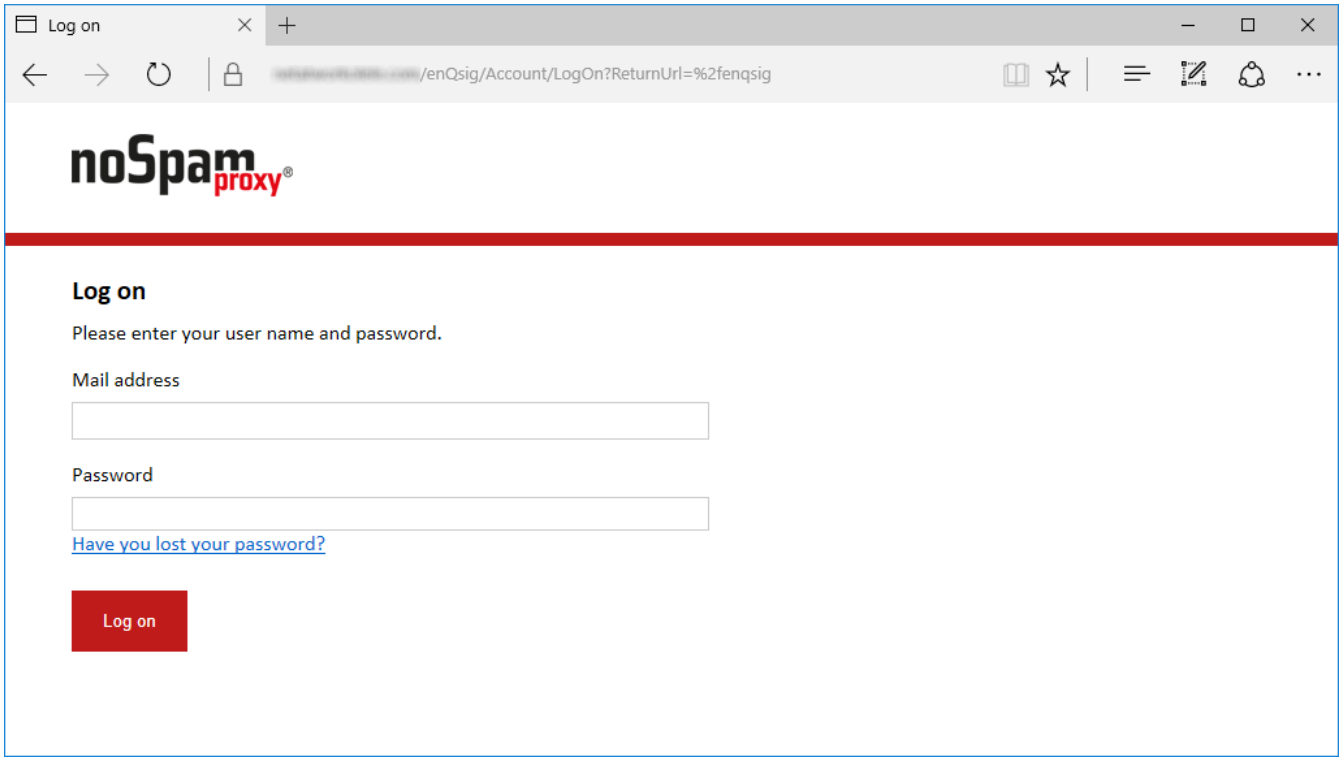
6. After Installation

Once the installation is complete, you can access the web site of the Web Portal from the address specified during installation. For a standard installation, this is

`https://<NameOfComputer>/enqsig`

If the page can not be reached, please check the configuration of the Internet Information Services. Then, see chapter Error Handling.

If the installation was successful, the login page of the Web Portal appears . (Picture 17)



Picture 17: The logon screen of the Web Portal

Now connect the Web Portal to your Intranet Role. To do this, open the NoSpamProxy Management Console. Open **Configuration/NoSpamProxy Components**. Go to the **Web Portal** section and configure the connection.

If you want to use the Large Files for uploaded files, and if you want these files to be scanned for viruses by the Cyren service, an additional step is necessary. This must not be executed until a connection to the Intranet Role has been established. Open a browser and navigate to the following page: `https://computername/enqsig/admin/configurecyren`. On this page, enter the user name and password of an administrator account. This action configures the Cyren service. The portal is now ready for use.

7. Upgrades

If you are updating from a previous version of the Web Portal, please note the points listed below.

- In most cases, you must perform manual steps before and after the installation, otherwise complete functionality of the Web portal cannot be guaranteed. See the steps in section Upgrade Paths. The sections are cumulative, which means you have to follow the sections from your currently installed version to the current version.
- Check the configuration of your Web Portal after each program update.

Upgrade Paths

Depending on the version you are updating from to the current version of the Web Portal, you must perform different steps.

Updating from Version 12.1 to Version 12.2

When updating from version 12.1 to version 12.2, all settings and user information are retained during the update.

Updating from Version 12 to Version 12.1

When updating from version 12 to version 12.1, all settings and user information are retained during the update.

Updating from Version 11.1 to Version 12

When updating from version 11.1 to version 12, all settings and user information are retained during the update.

Updating from Version 11 to Version 11.1

Version 11.1 of SQL Server requires version 2008. Please update your SQL Server 2005 to version 2008 or later before starting the NoSpamProxy update.

When updating from version 11 to version 11.1, all settings and user information are retained during the update.

Updating from Version 10.1 to Version 11

When updating from version 10.1 to version 11, all settings and user information are retained during the update.

Updating from Version 10 to Version 10.1

When updating from version 10 to version 10.1, all settings and user information are retained during the update.

8. Error Handling

Login page not available - Error 500.21

If the HTTP error 500.21 is displayed instead of the login page, ASP. NET 4.7.2 is probably not installed or registered correctly in the IIS.

Before re-registering the ASP.NET Framework 4.7.2 on your Internet server, make sure that the framework is compatible with any other Internet sites hosted on this server. Back up your system, particularly the IIS configuration, before proceeding.

If NoSpamProxy and Microsoft Exchange are installed on the same server, make sure that Exchange supports the respective version of the .NET Framework before installing or upgrading. The Exchange Server Supportability Matrix offers an overview of supported versions.

Perform a re-registration of the ASP.NET Framework using the following command:

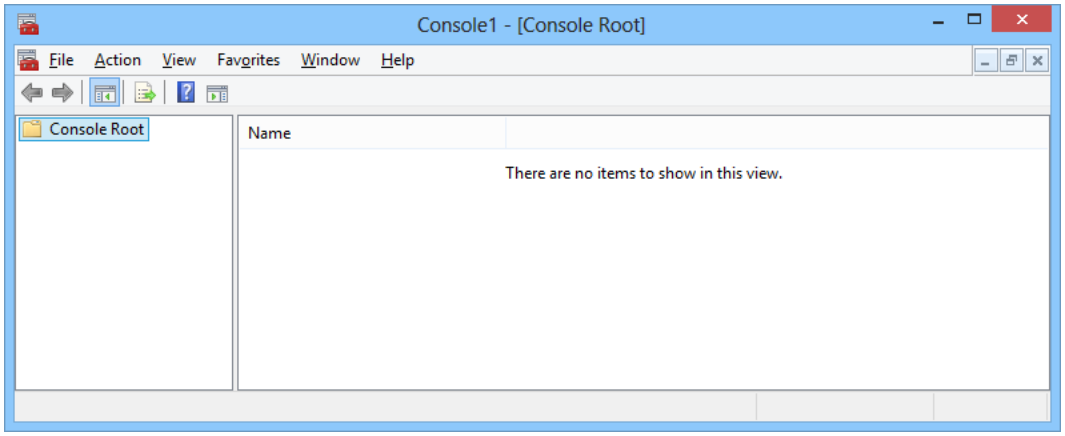
```
%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i
```

9. Appendix

Viewing the Certificate Store of the Local Computer

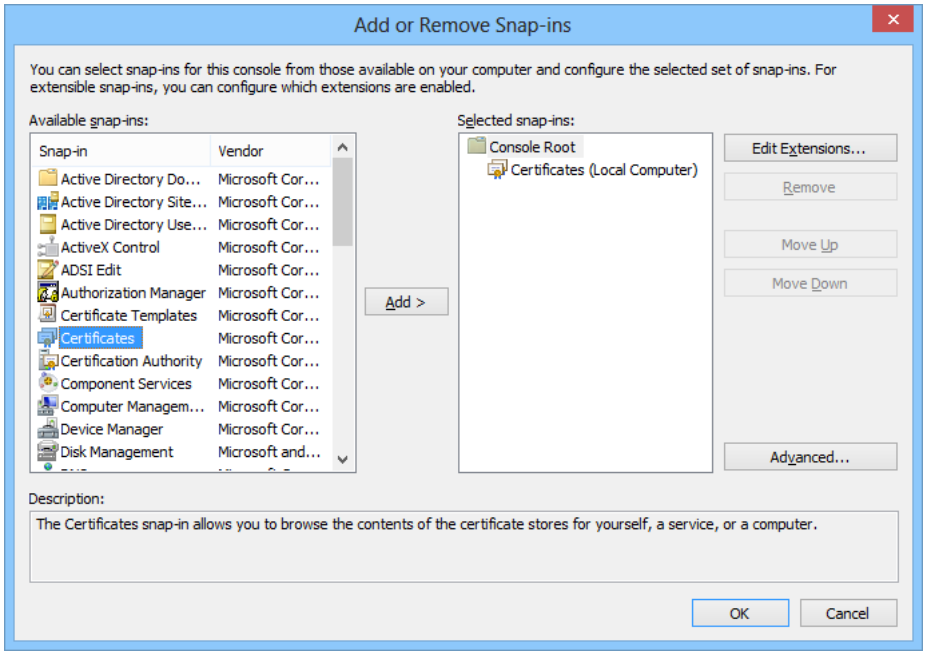
The following steps are necessary to view the certificates of the local computer:

Start a new MMC console (Start -> Run -> mmc. exe) (Picture 18).



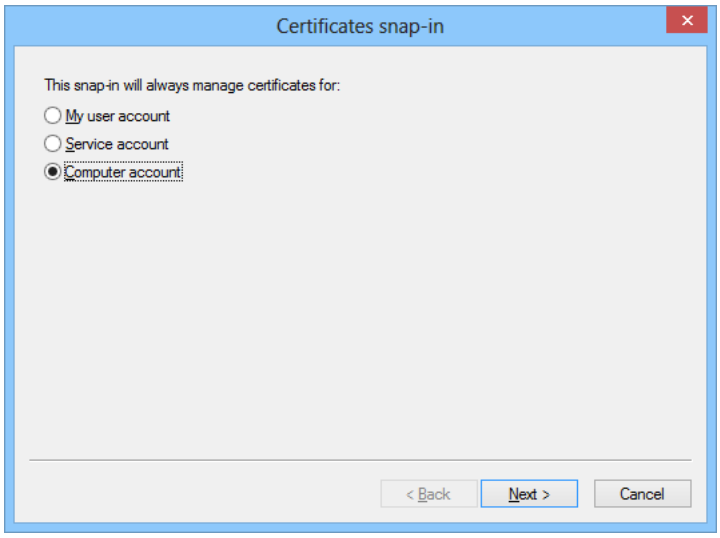
Picture 18: An empty MMC

In the **File** menu , click **Add/Remove Snap-in**. Select the **Certificates** snap-in and click **Add** (Picture 19).

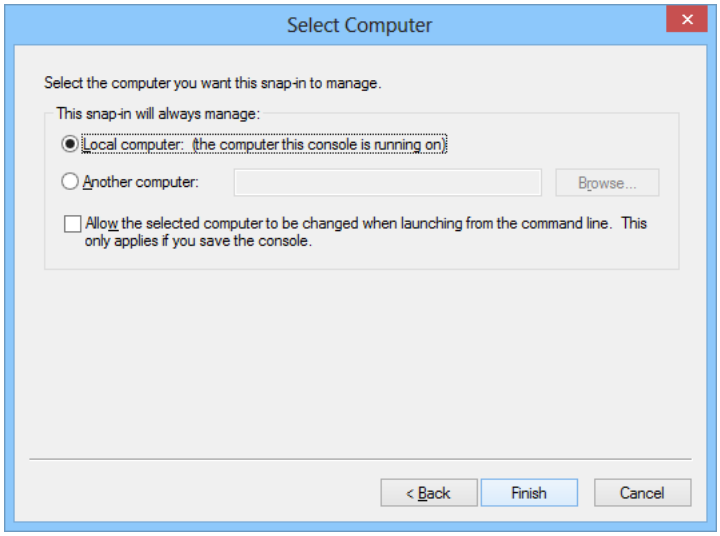


Picture 19: Dialog for adding snap-ins

The configuration wizard for the snap-in **Certificates** appears . Select the **Computer account** (Picture 20), then **Local computer** (Picture 21) then click **Finish**.



Picture 20: Computer account selection



Picture 21: Local computer selection

Close the dialog **Add or Remove Snap-ins** by clicking **OK**. In the window **Console Root**, click **Certificates (Local Computer)** to view the certificate store of the computer.