Net at Work
Building IT-Excellence.

NoSpamProxy 13.2

Connection to digiSeal server 2.0

- Encryption
- Large Files

Imprint

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

Trademarks

13 February 2020

Contents

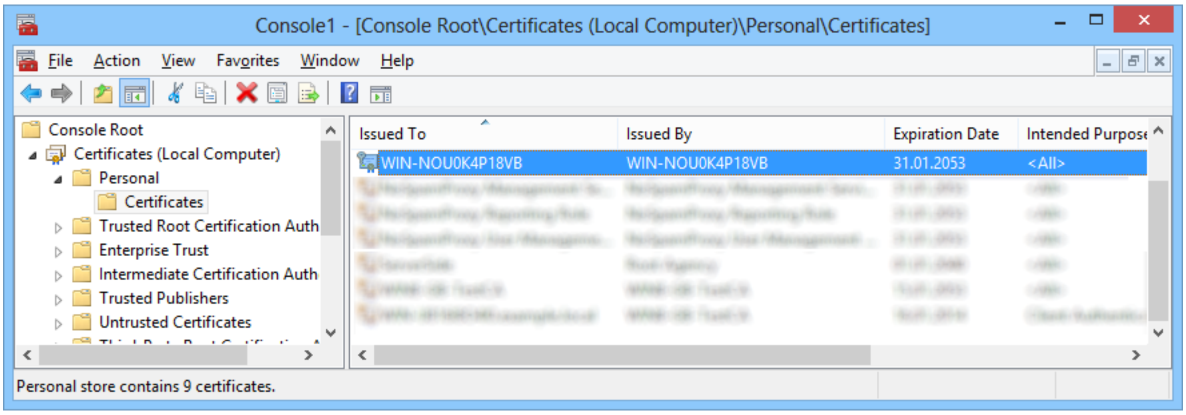
1. System Requirements

The digiSeal server and NoSpamProxy Encryption can be operated simultaneously on one single system. They can also be installed on different workstations. By default, communication between the digiSeal server and NoSpamProxy Encryption takes place via TCP/IP, Port 2001. In order to use this port it may be necessary to create exception rules in existing firewalls on the participating workstations.

2. Certificate Configuration

Communication between NoSpamProxy Encryption and the digiSeal server is encrypted using certificates. By default, the certificate with the name " `CN=<ComputerName>, CN=Net at Work Mailgateway` " is used. If the two services are located on two different computers, this certificate must first be transferred from NoSpamProxy Encryption to the digiSeal server.

To do this, open the Certificate store of the local computer account. Go to **Personal** and select the certificate with the name of your workstation (Picture 1).



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Auth
Enterprise Trust
Intermediate Certification Auth
Trusted Publishers
Untrusted Certificates

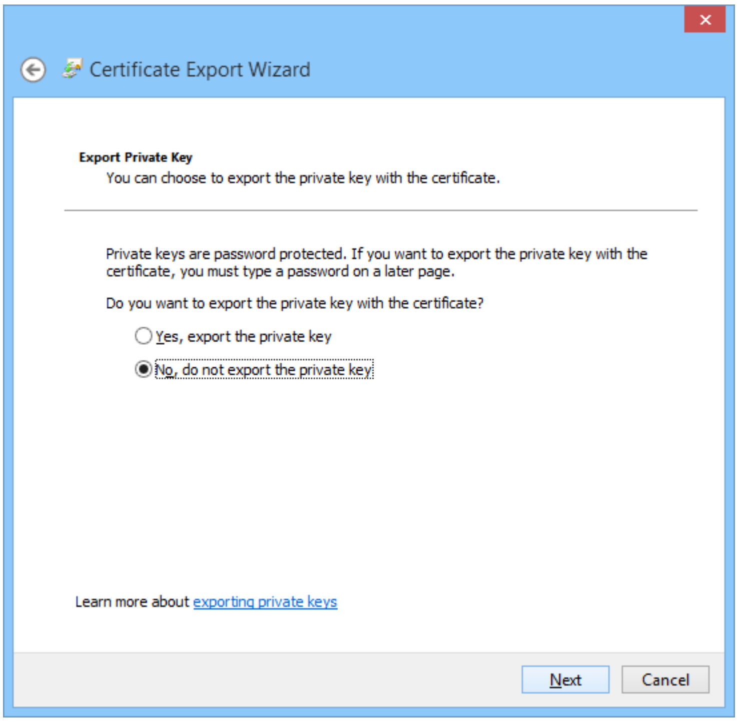
Issued To	Issued By	Expiration Date	Intended Purpose
WIN-NOU0K4P18VB	WIN-NOU0K4P18VB	31.01.2053	<All>

Personal store contains 9 certificates.

Picture 1: The certificate of the Gateway Role

On the certificate, select **All Tasks**, then **Export**. The Certificate Export Wizard opens.

Click **Next**, then select the export of this certificate without private key (Picture 2).



Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

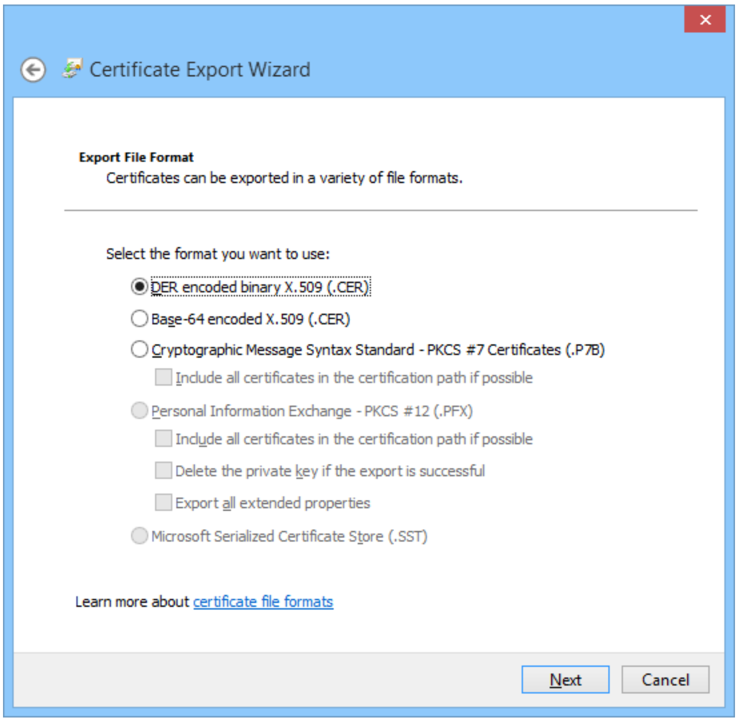
○ Yes, export the private key

● No, do not export the private key

Learn more about exporting private keys

Picture 2: Export without private key

Now select the DER format as file format (Picture 3).



Export File Format

Certificates can be exported in a variety of file formats.

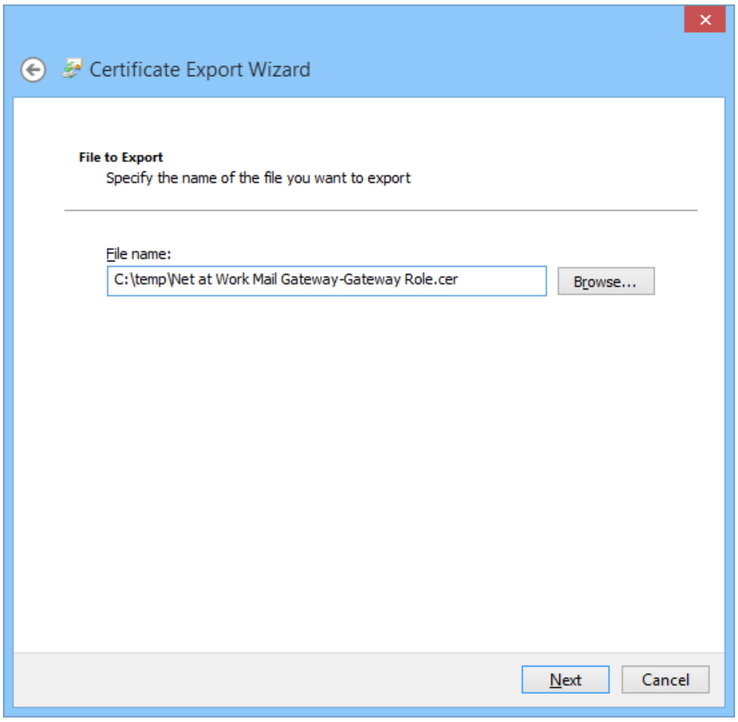
Select the format you want to use:

- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
- ○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Picture 3: Selecting the DER file format

Finally, specify the storage location (Picture 4). Confirm the selected settings and exit the wizard by clicking **Finish**.



File to Export

Specify the name of the file you want to export

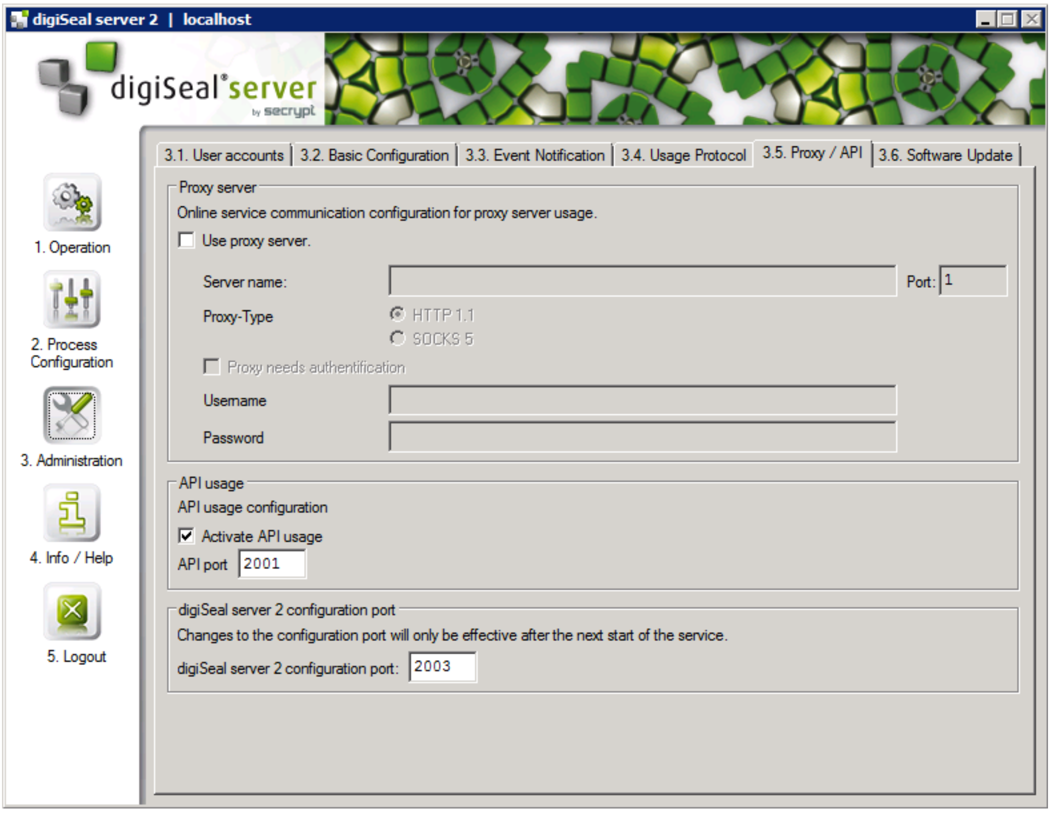
File name:

C:\temp\Net at Work Mail Gateway-Gateway Role.cer

Picture 4: Saving the exported certificate

If the digiSeal server is located on a remote server, copy the file with the certificate to it.

Make sure that the API is enabled on the digiSeal server (Picture 5).



Proxy server

Online service communication configuration for proxy server usage.

□ Use proxy server.

Server name: Port: 1

Proxy-Type ● HTTP 1.1 ○ SOCKS 5

□ Proxy needs authentification

Username

Password

API usage

API usage configuration

☑ Activate API usage

API port 2001

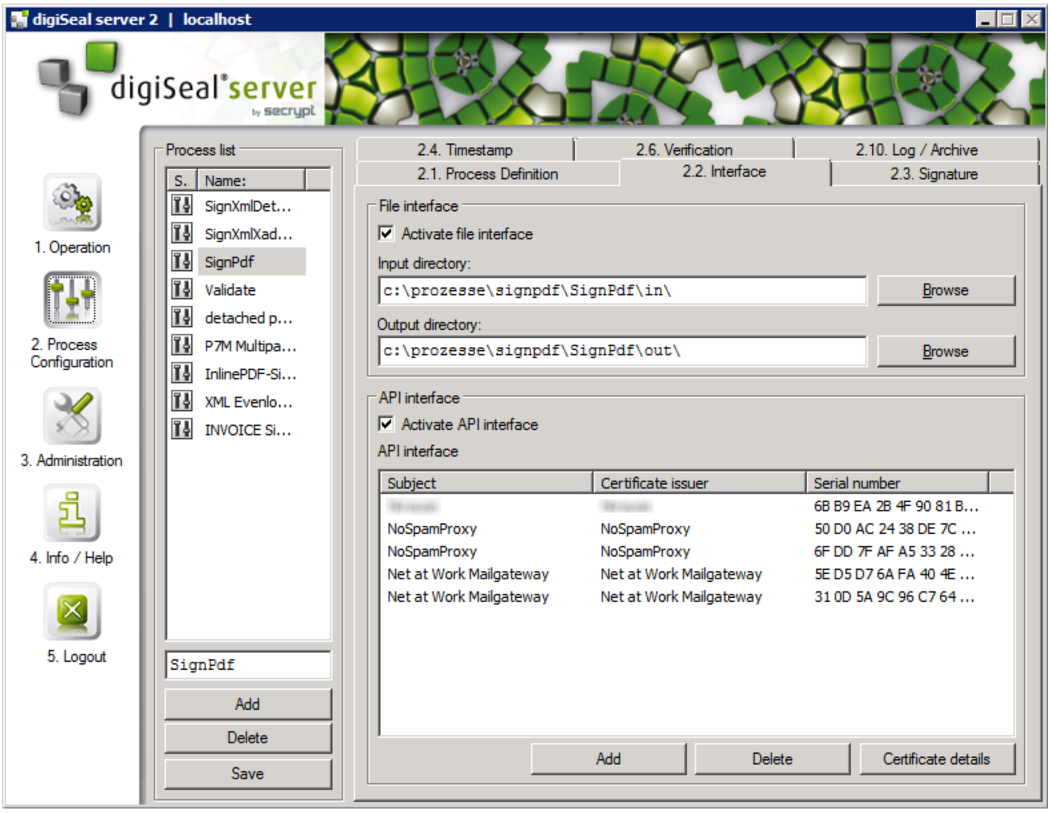
digiSeal server 2 configuration port

Changes to the configuration port will only be effective after the next start of the service.

digiSeal server 2 configuration port: 2003

Picture 5: Activating the API interface

Activate the API for each process to be used by NoSpamProxy Encryption. To do this, make sure that the **Activate API interface** checkbox is ticked. The interface is only enabled for applications that use a certificate listed in the **API Interface list**. The previously exported certificate must be included in this list (Picture 6).



Process list

S.	Name:
	SignXmlDet...
	SignXmlXad...
	SignPdf
	Validate
	detached p...
	P7M Multipa...
	InlinePDF-Si...
	XML Evenlo...
	INVOICE Si...

SignPdf

File interface

☑ Activate file interface

Input directory:

c:\prozesse\signpdf\SignPdf\in\

Output directory:

c:\prozesse\signpdf\SignPdf\out\

API interface

☑ Activate API interface

API interface

Subject	Certificate issuer	Serial number
[redacted]	[redacted]	6B B9 EA 2B 4F 90 81 B...
NoSpamProxy	NoSpamProxy	50 D0 AC 24 38 DE 7C ...
NoSpamProxy	NoSpamProxy	6F DD 7F AF A5 33 28 ...
Net at Work Mailgateway	Net at Work Mailgateway	5E D5 D7 6A FA 40 4E ...
Net at Work Mailgateway	Net at Work Mailgateway	31 0D 5A 9C 96 C7 64 ...

Picture 6: Activating the API interface on the set up process

3. NoSpamProxy Configuration

NoSpamProxy Encryption requires a number of files from the digiSeal server directory. Copy the files „ `dsServerAPI.dll` “, „ `dsServerAPI.dll.p7s` “ and „ `dsServerAPI.signature` “ from the digiSeal server program directory to the directory „ `%ProgramFiles%\Net at Work Mail Gateway\Gateway Role` “. Now restart the Gateway Role.

Consult the NoSpamProxy Manual to set up the options in the interface for using the digiSeal server. Pay special attention to the following points:

Under **Configuration** / **Connected Systems**: Configure the **Connection to the digiSeal server**.

Under **Configuration** / **User notifications**: Configure the **Email notifications** and the **Administrative email addresses**.

Under **Configuration** / **Rules**:

- Add the action **digiSeal server: Sign attachments on outbound emails** to a new or existing outgoing rule and configure it as described in the manual.
- Add the action **digiSeal server: Verify and enforce attachment signatures on inbound emails** to a new or existing incoming rule and configure it as described in the manual.

4. Archiving

The two digiSeal server actions of the NoSpamProxy rules provide data for the archive interface of NoSpamProxy if you have configured an archive connector there. During archiving, the emails, signatures and verification protocols are transferred to the configured archive connector. Details on this topic can be found in the NoSpamProxy Manual under **Archive interface**. An archive connector for new archive systems that have not yet been supported can be implemented by Net at Work after consultation with you.

5. Qualified Signature Incidents

It is not always possible to complete the signing or verification of documents correctly. For example, in some cases the connection to the digiSeal server cannot be established, or the digiSeal server cannot reach an OCSP server. In these cases, the email is accepted by NoSpamProxy Encryption but not forwarded to the recipient. Instead, the affected emails are cached. As a result, the administrator will receive an email alerting him or her of the issue, if so configured.

In the interface, these emails are displayed under **Monitoring** / **Emails on hold**. All incidents are displayed in a list. The administrator can decide per incident whether the email is to be delivered again by NoSpamProxy Encryption or whether the incident is to be deleted.

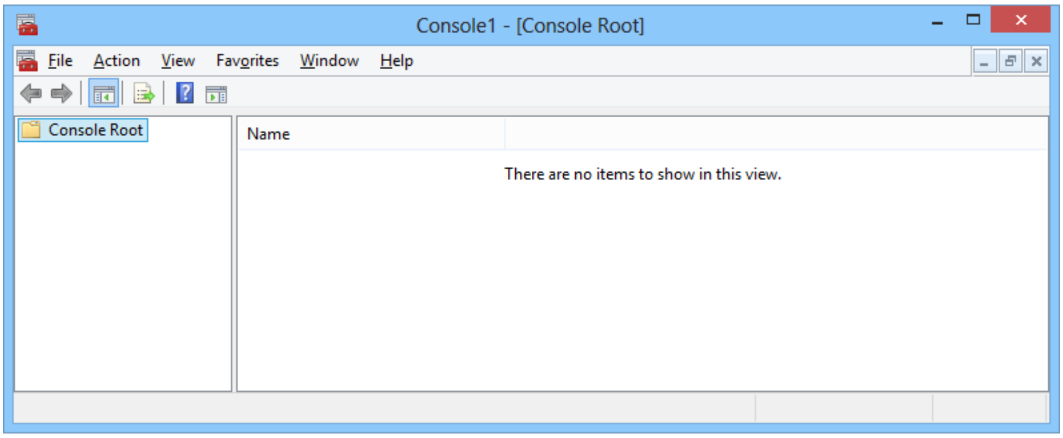
A detailed description of how to use the above settings can be found in the NoSpamProxy Manual.

6. Appendix

Displaying the Certificate Store of the Local Workstation

To view the certificates of the local workstation, the following steps are necessary:

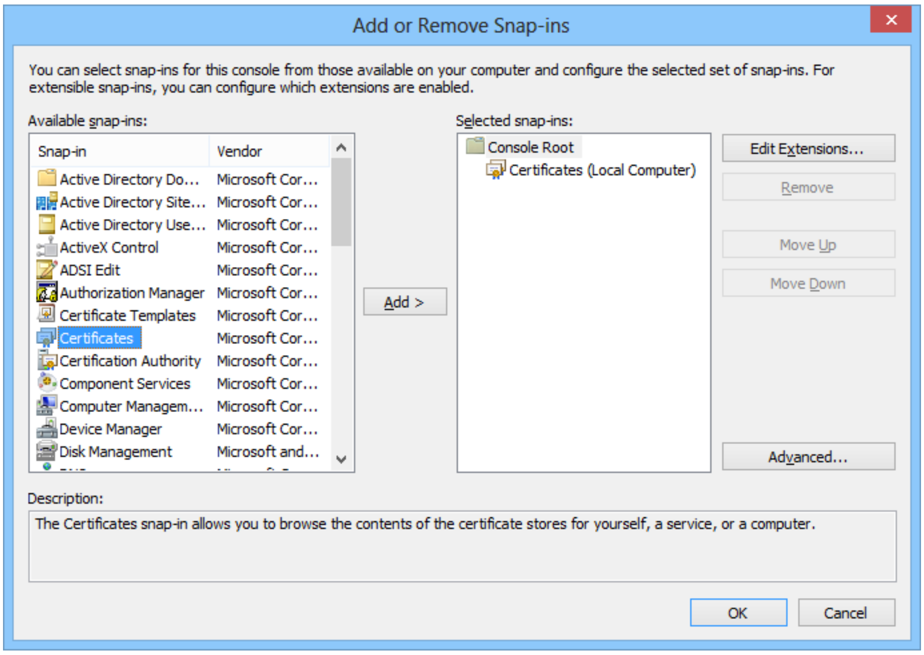
Launch a new MMC console (Start -> Run -> mmc.exe) (Picture 7).



There are no items to show in this view.

Picture 7: An empty MMC console

In the menu **File**, click **Add/Remove Snap-in**. Select the **Certificates** Snap-In and click **Add** (Picture 8).



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

Selected snap-ins:

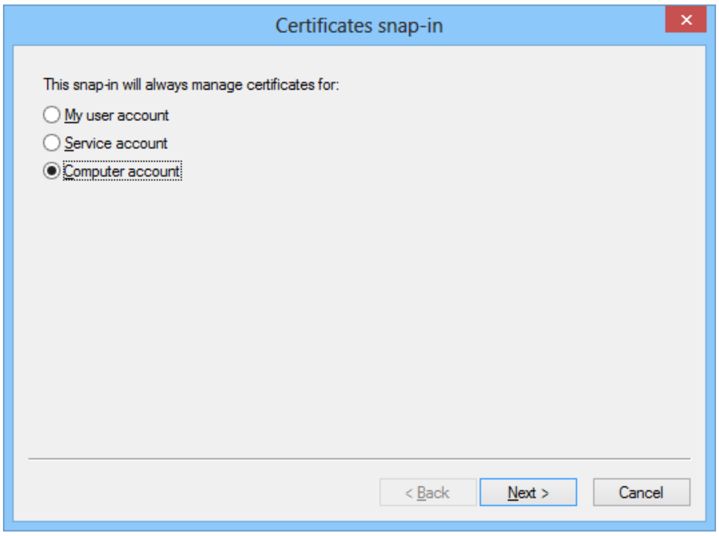
- Console Root
  - Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Picture 8: Dialog for adding snap-ins

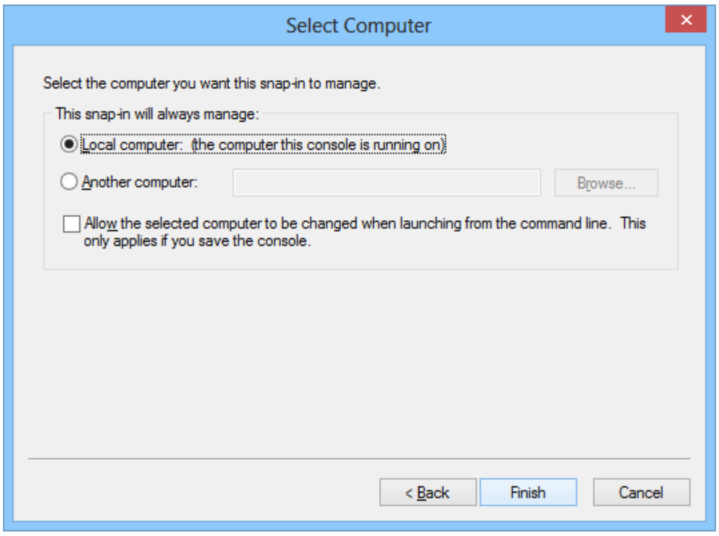
The configuration wizard for the snap-in **Certificates** appears . Select **Computer account** (Picture 9), then **Local computer** (Picture 10) and click **Finish**.



This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Picture 9: Computer account selection



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Picture 10: 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 stores for the computer.

7. Help and support

Net at Work offers many forms of help and support for the installation and the operation of NoSpamProxy.

- **Training videos**
  Training videos provide an overview of different areas and include step-by-step configuration tutorials as well as practical examples.
- **Blog**
  The Blog provides daily updated alerts for new product versions, suggested changes to your configuration, warnings on compatibility issues and more help. To make sure you do not miss any important advice, you can also find the latest news from the blog on the start page of the NoSpamProxy configuration console.
- **Knowledge Base**
  The Knowledge Base contains additional information on specific issues.
- **Support**
  If you require additional support, please visit our support website.