

noSpam[®] proxy SERVER

Version 14

Einbindung in digiSeal server 2.0

Legal information

All rights reserved. This document and the applications described therein are copyrighted products of Net at Work GmbH, Paderborn, Federal Republic of Germany. This document is subject to change without notice. The information contained in this document does not constitute an assumption of warranty or liability on the part of Net at Work GmbH. The partial or complete reproduction is only permitted with the written permission of Net at Work GmbH.

Copyright © 2022 Net at Work GmbH

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

Microsoft®, Windows®, Microsoft Exchange®, SQL Server®, SQL Server Express®, Windows Server 2008®, Windows Server 2012®, Windows Server 2012 R2®, Windows Server 2016®, Microsoft .NET Framework®, Microsoft Report Viewer®, Microsoft Office®, Microsoft 365®, Office 365®, Microsoft Outlook®, Microsoft Visual Studio® and Azure® are registered trademarks of Microsoft Corporation. NoSpamProxy® and 32Guards® are registered trademarks of Net at Work GmbH. All other trademarks used belong to the respective manufacturers or owners.

THIS DOCUMENT WAS LAST EDITED ON MARCH 31, 2023.

Content

System requirements	1
Configuring the certificates	2
Configuring NoSpamProxy	7
Archiving	8
Qualified signature incidents	9
Viewing the local certificate store	10
Help and support	13

System requirements

The digiSeal server and NoSpamProxy Encryption can be installed on a single system or on different computers.



NOTE: Since the communication between the digiSeal server and NoSpamProxy Encryption takes place by default via TCP/IP, port 2001, you may have to create exception rules for this port on the participating computers in existing firewalls.

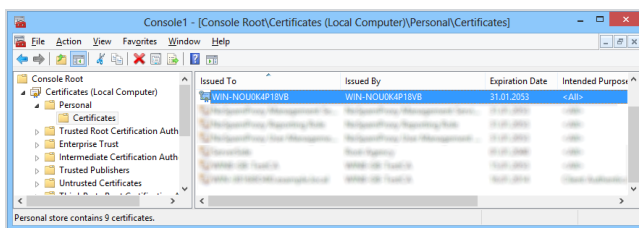
Configuring the certificates

The 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 installed on different computers, this certificate must first be transferred from NoSpamProxy Encryption to the digiSeal server.

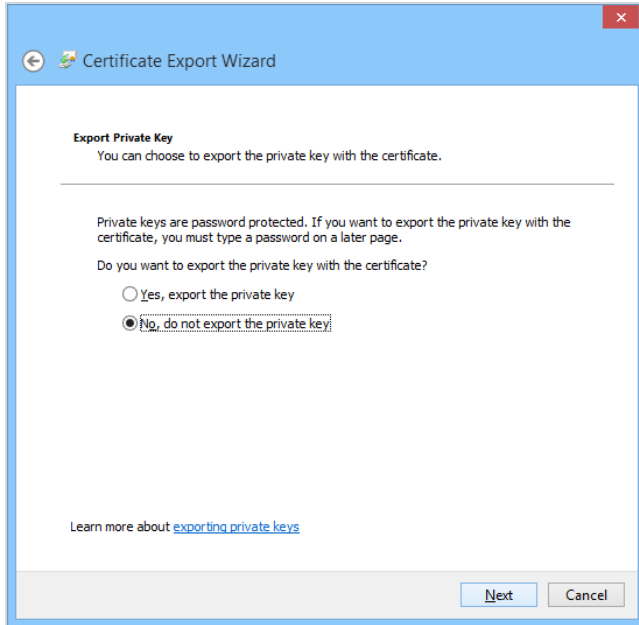
Proceed as follows:

1. Open the certificate store of the local computer account.
2. Go to **.Persönliche Zertifikate/Personal**.
3. Select the certificate with the name of your computer.

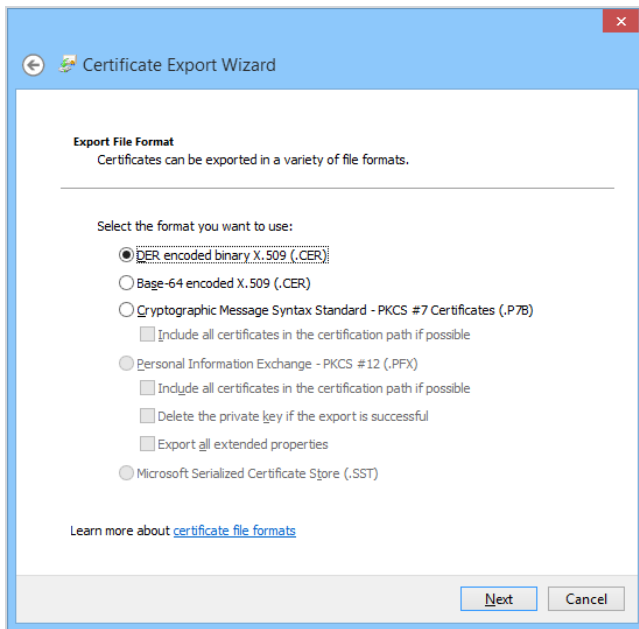


4. On the certificate, select **Alle Aufgaben/All Tasks** and then **Exportieren/Export**.

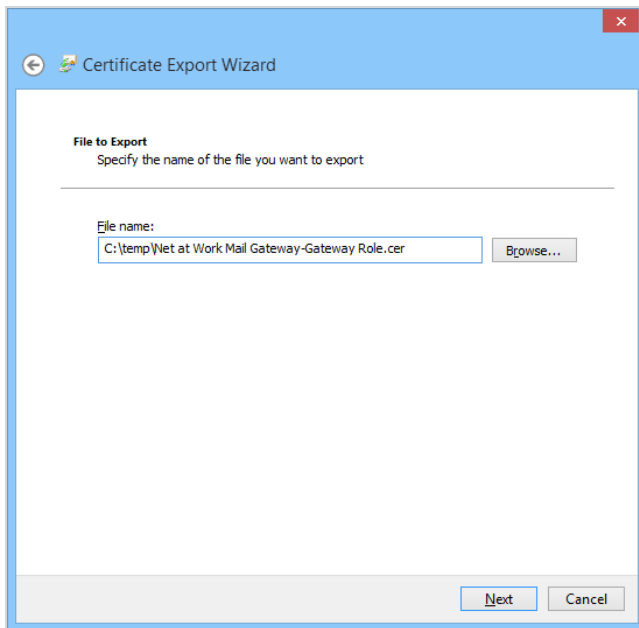
5. Click **Weiter / Next** and then select **Export ohne privaten Schlüssel / Export without private key**.



6. Select DER format as the file format.



7. Specify the storage location.



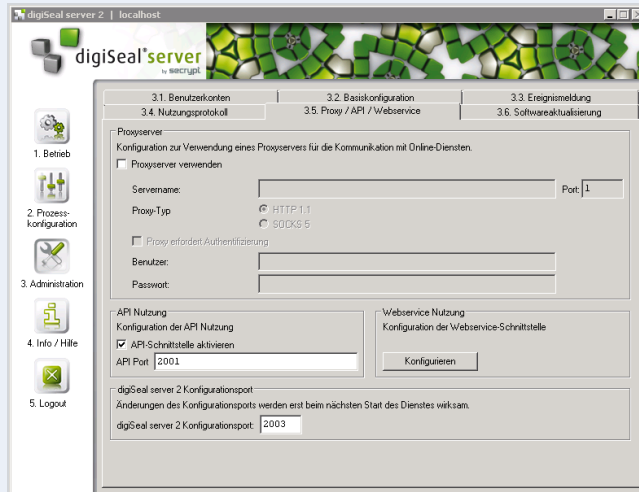
8. Confirm the selected settings and click **Beenden / Finish**.



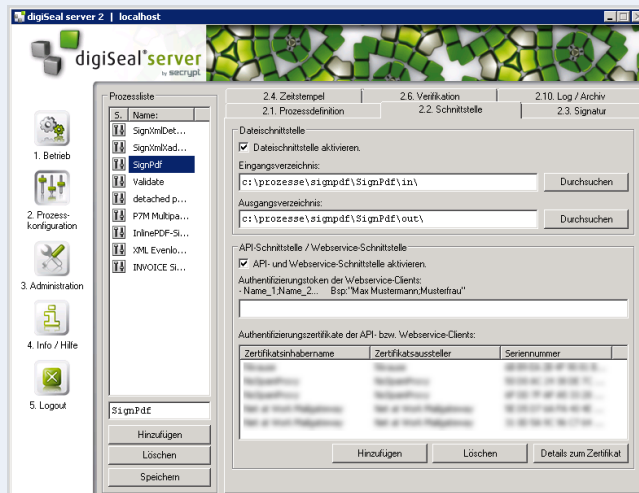
NOTE: If the digiSeal server is located on a remote server, copy the file with the certificate there.



NOTE: Make sure that the API is activated on the digiSeal server.



Enable the API for each process to be used by NoSpamProxy Encryption. To do this, make sure that the Enable API Interface checkbox is checked. The interface is only enabled for programs that use a certificate that is listed in the API Interface list. The previously exported certificate must be added to this list.



Configuring NoSpamProxy

NoSpamProxy Encryption requires some files from the digiSeal server directory.

1. Copy the following files from the digiSeal server program directory to the **%ProgramFiles%\Net at Work Mail Gateway\Gateway Role** directory:
 - **dsServerAPI.dll**
 - **dsServerAPI.dll.p7s**
 - **dsServerAPI.signature**
2. Restart the Gateway Role.
3. Follow the instructions under **digiSeal-server-Verbindung** and **Qualifizierte Dokumentensignatur mit dem digiSeal server** to set up the options in the interface for using the digiSeal server. Pay particular attention to the following points:
 - **Configuration > Connected systems**| Configure the connection to the digiSeal server.
 - **Configuration > User notifications**| Configure email notifications and administrative email addresses.
 - **Configuration > Rules**| Add the action **digiSeal server: Sign attachments to outbound emails** to a new or existing outbound rule and configure it as described.
 - **Configuration > Rules**| Add the action **digiSeal server: Verify and enforce attachment signatures on inbound emails** to a new or existing inbound rule and configure it as described.

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 audit trails are transferred to the configured archive connector.



NOTE: Details can be found under [Archivkonnektoren](#). An archive connector for new, previously unsupported archive systems can be implemented by Net at Work in consultation with you.

Qualified signature incidents

Signing or reviewing documents cannot always be completed correctly. For example, it may happen that

- the connection to the digiSeal server cannot be established or
- the digiSeal server cannot reach an OCSP server on the Internet.

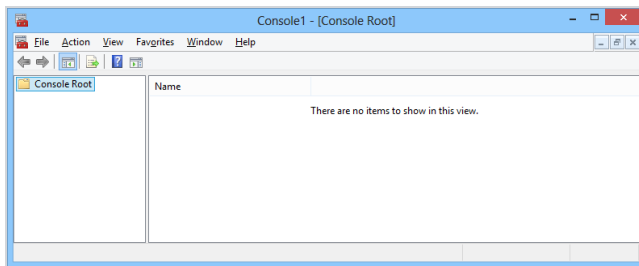
In these cases, the email is accepted by NoSpamProxy Encryption but not forwarded to the recipient. Instead, the affected emails are stored temporarily.

In this case, the administrator receives an email, if configured. In the user interface, these emails are displayed under **Angehaltene E-Mails**. The administrator can decide per incident whether the email should be delivered again by NoSpamProxy Encryption or whether the incident should be deleted.

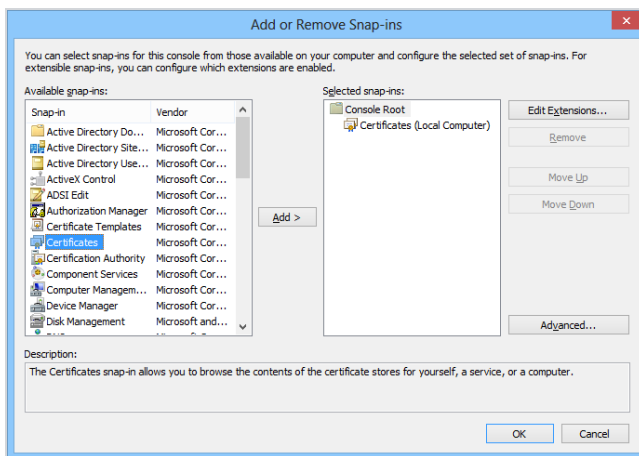
Viewing the local certificate store

To view the certificates of the local computer, follow these steps:

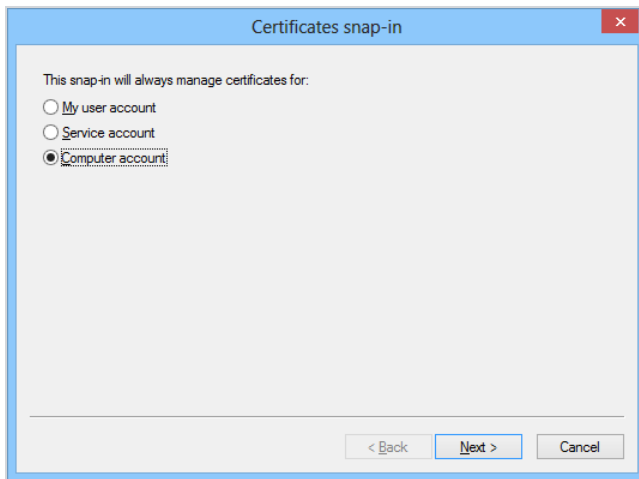
1. Start a new NoSpamProxy Command Center.



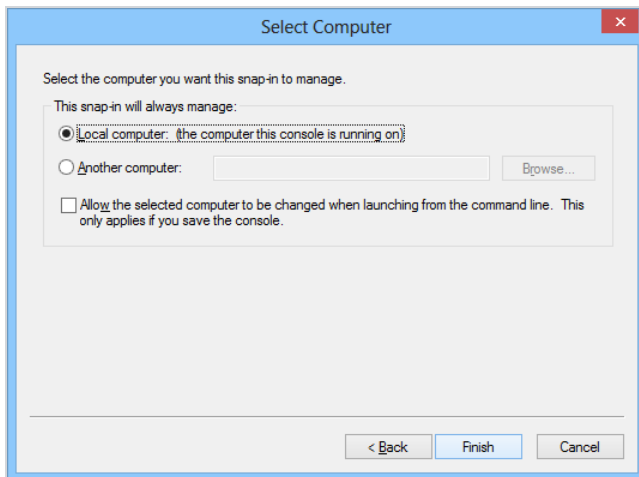
2. Under **File/File**, click **Snap-In hinzufügen/entfernen/Add/Remove Snap-in**.
3. Select the **Certificates** snap-in and click **Add**.



4. In the configuration wizard, select the **Computer-Konto / Computer account**.



5. Select **Lokaler Computer / Local computer**.



6. Click **Finish**.
7. Click **OK** to close the dialog.
8. Go to **.Konsolenstamm / Console Root**.

9. Click **Zertifikate (Lokaler Computer) / Certificates (Local Computer)** to view the certificate stores for the computer.

Help and support

Knowledge Base

The [Knowledge Base](#) contains further technical information on various problems.

Website

The [NoSpamProxy website](#) contains manuals, white papers, brochures and other information about NoSpamProxy.

NoSpamProxy Forum

The [NoSpamProxy forum](#) gives you the opportunity to exchange information with other NoSpamProxy users, get tips and tricks and share them with others.

Blog

The [blog](#) offers technical support, tips on new product versions, suggestions for changes to your configuration, warnings about compatibility problems and much more. The latest news from the blog is also displayed on the start page of the NoSpamProxy Command Center.

YouTube

On our [YouTube](#) channel you will find tutorials, how-tos and other product information that will make working with NoSpamProxy easier.

NoSpamProxy Support

You can reach our support team

- by phone at [+49 5251304-636](tel:+495251304636)
- by email at support@nospamproxy.de.

