noSpam proxy® SERVER

Version 14

Einbindung in digiSeal server 2.0

Net at Work
Building IT-Excellence.

Legal information

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

THIS DOCUMENT WAS LAST EDITED ON NOVEMBER 27, 2023.

Content

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.

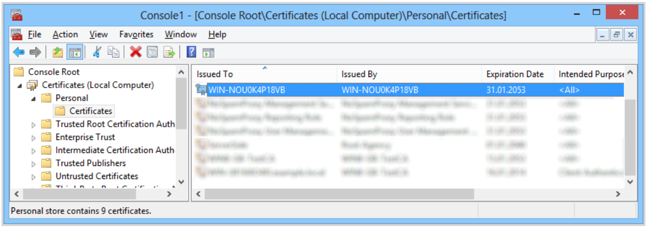
Configuring the certificates

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.



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

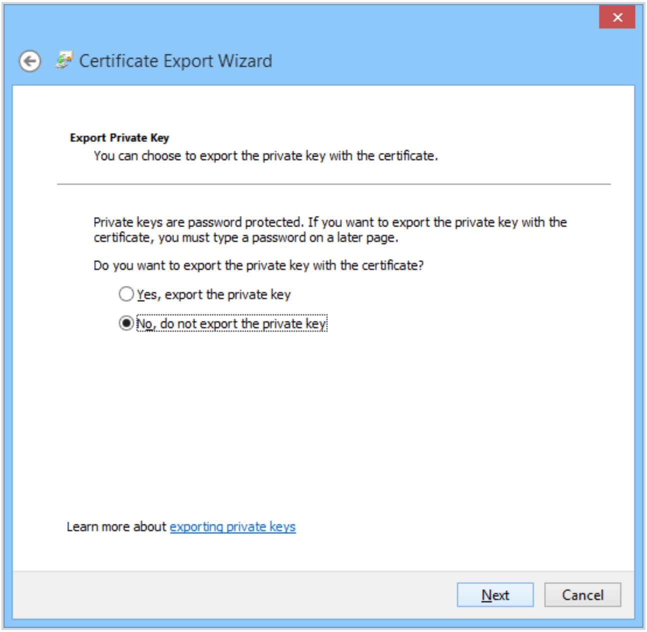
- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Auth
    - Enterprise Trust
    - Intermediate Certification Auth
    - Trusted Publishers
    - Untrusted Certificates

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

Personal store contains 9 certificates.

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**.



Export Private Key
You can choose to export the private key with the certificate.

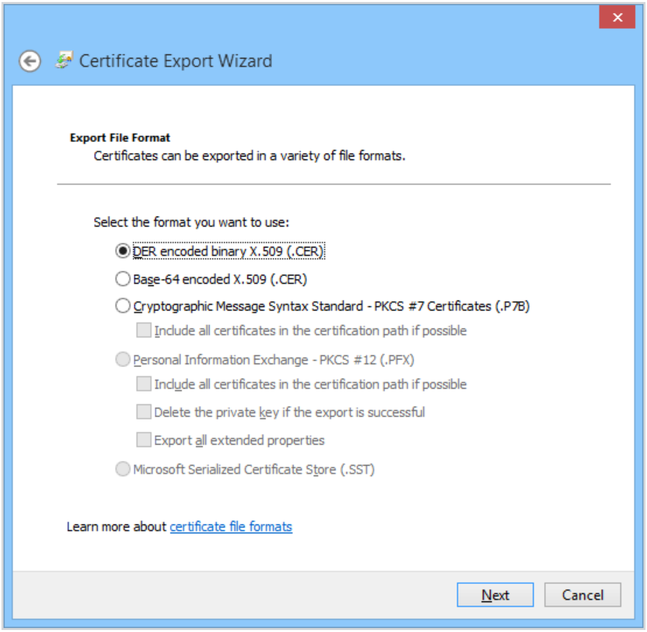
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

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

6. Select DER format as the file format.



Certificate Export Wizard

Export File Format

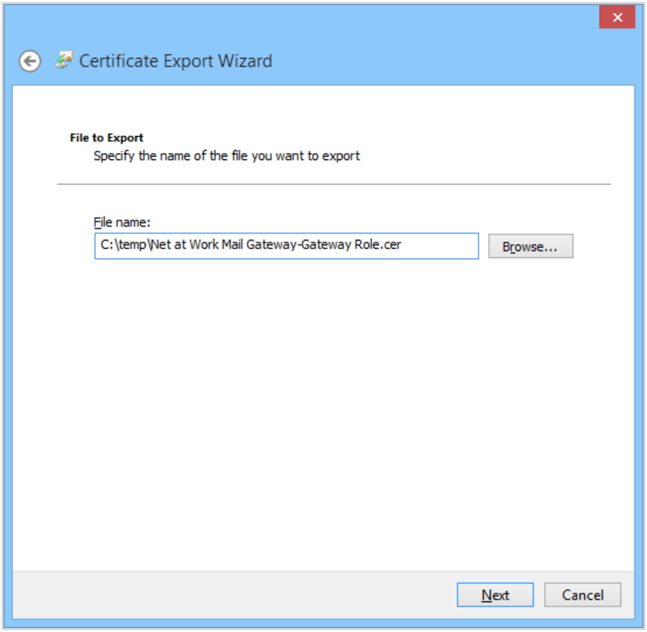
Certificates can be exported in a variety of file formats.

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

7. Specify the storage location.



Certificate Export Wizard

File to Export

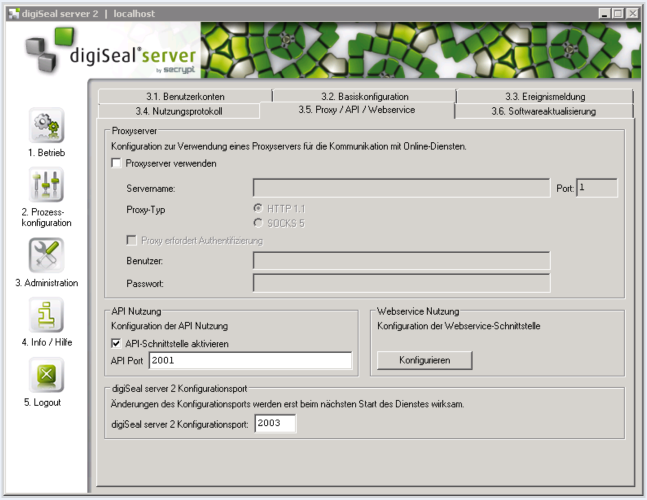
Specify the name of the file you want to export

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

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.



Proxyserver

Konfiguration zur Verwendung eines Proxyservers für die Kommunikation mit Online-Diensten.

□ Proxyserver verwenden

Servername: Port: 1

Proxy-Typ ● HTTP 1.1 ○ SOCKS 5

□ Proxy erfordert Authentifizierung

Benutzer:

Passwort:

API Nutzung

Konfiguration der API Nutzung

☑ API-Schnittstelle aktivieren

API Port 2001

Webservice Nutzung

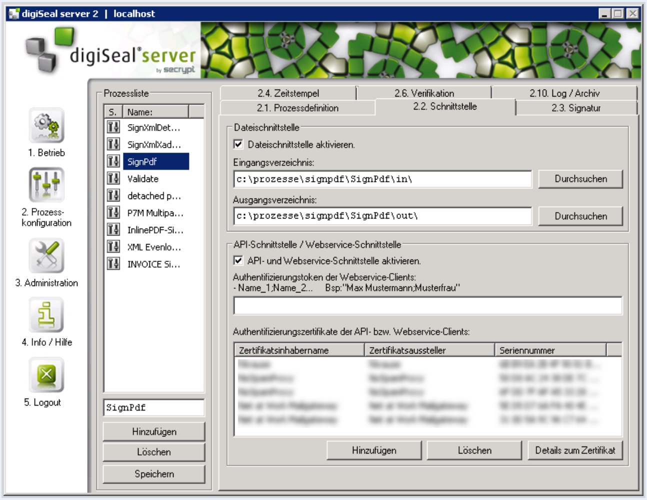
Konfiguration der Webservice-Schnittstelle

digiSeal server 2 Konfigurationsport

Änderungen des Konfigurationsports werden erst beim nächsten Start des Dienstes wirksam.

digiSeal server 2 Konfigurationsport: 2003

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.



Prozessliste

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

SignPdf

Dateischnittstelle

☑ Dateischnittstelle aktivieren.

Eingangsverzeichnis: c:\prozesse\signpdf\SignPdf\in\

Ausgangsverzeichnis: c:\prozesse\signpdf\SignPdf\out\

API-Schnittstelle / Webservice-Schnittstelle

☑ API- und Webservice-Schnittstelle aktivieren.

Authentifizierungstoken der Webservice-Clients:
- Name_1;Name_2... Bsp:"Max Mustermann;Musterfrau"

Authentifizierungszertifikate der API- bzw. Webservice-Clients:

Zertifikatsinhabername	Zertifikatsaussteller	Seriennummer
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

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.

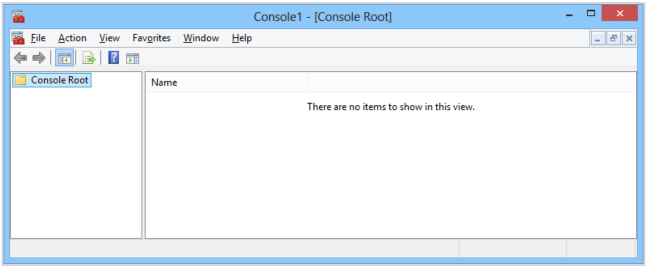
In these cases, the email is accepted by NoSpamProxy Encryption but not forwarded to the recipient. Instead, the affected emails are stored temporarily.

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:

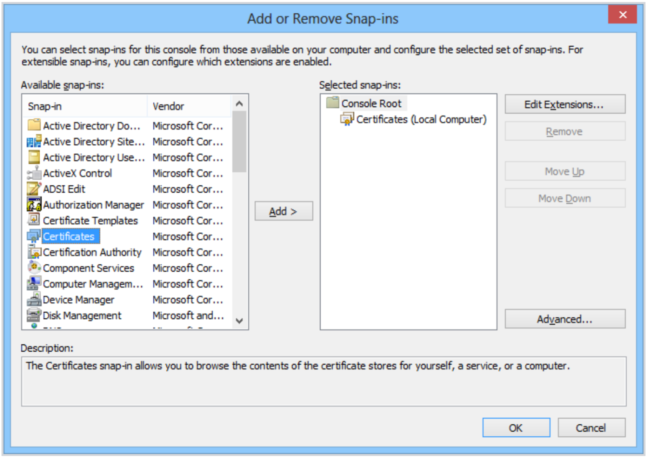
1. Start a new NoSpamProxy Command Center.



There are no items to show in this view.

2. Under **File/File**, click **Snap-In hinzufügen/entfernen/Add/Remove Snap-in**.

3. Select the **Certificates** snap-in and click **Add**.

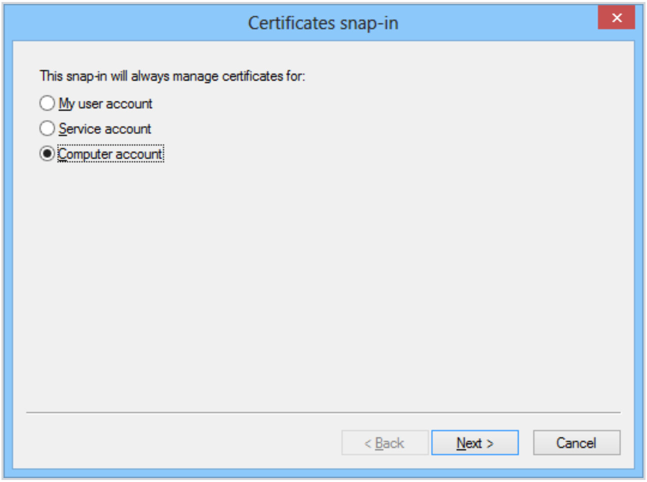


You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

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...

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

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



Certificates snap-in

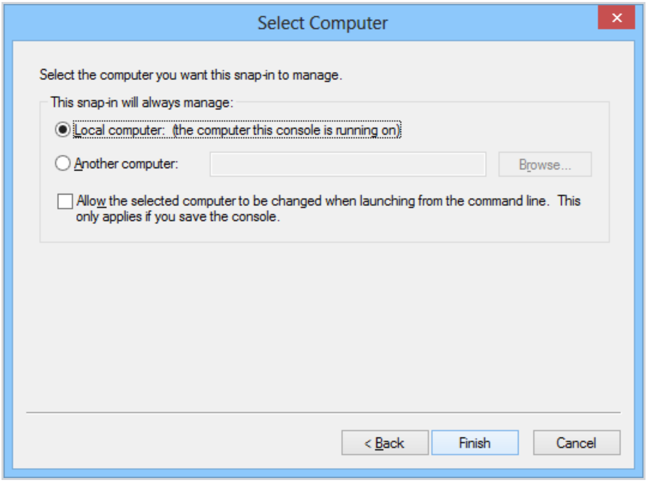
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

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



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.

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**
- by email at **support@nospamproxy.de**.