

Version 15

Einbindung in digiSeal server 2.0



Rechtliche Hinweise

Alle Rechte vorbehalten. Dieses Dokument und die darin beschriebenen Programme sind urheberrechtlich geschützte Erzeugnisse der Net at Work GmbH, Paderborn, Bundesrepublik Deutschland. Änderungen vorbehalten. Die in diesem Dokument enthaltenen Informationen begründen keine Gewährleistungs- und Haftungsübernahme seitens der Net at Work GmbH. Die teilweise oder vollständige Vervielfältigung ist nur mit schriftlicher Genehmigung der Net at Work GmbH zulässig.

Copyright © 2023 Net at Work GmbH

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

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® und Azure® sind eingetragene Handelsmarken der Microsoft Corporation. NoSpamProxy® und 32Guards® sind eingetragene Handelsmarken der Net at Work GmbH. Alle anderen verwendeten Handelsmarken gehören den jeweiligen Herstellern beziehungsweise Inhabern.

DIESES DOKUMENT WURDE ZULETZT AM 11. DEZEMBER 2024 ÜBERARBEITET.

Inhalt

Systemanforderungen	1
Konfigurieren der Zertifikate	2
Konfigurieren von NoSpamProxy	8
Archivierung	10
Vorfälle der qualifizierten Signatur	. 11
Anzeigen des lokalen Zertifikatsspeichers	12
Hilfe und Unterstützung	15

Systemanforderungen

Der digiSeal server und NoSpamProxy Encryption gemeinsam auf einem System oder auf verschiedenen Computern installiert werden.

HINWEIS: Da die Kommunikation zwischen dem digiSeal server und NoSpamProxy Encryption standardmäßig über TCP/IP, Port 2001 erfolgt, müssen Sie für diesen Port auf den beteiligten Computern gegebenenfalls Ausnahmeregeln in vorhandenen Firewalls erstellen.

Konfigurieren der Zertifikate

Die Kommunikation zwischen NoSpamProxy Encryption und dem digiSeal server wird mit Hilfe von Zertifikaten verschlüsselt.

Standardmäßig wird dafür das Zertifikat mit dem Namen CN=<ComputerName>, CN=Net at Work Mailgateway verwendet. Sind die beiden Dienste auf unterschiedlichen Computern installiert, muss dieses Zertifikat zunächst von NoSpamProxy Encryption zum digiSeal server übertragen werden.

Gehen Sie folgendermaßen vor:

- 1. Öffnen Sie den Zertifikatsspeicher des lokalen Computer-Kontos.
- 2. Gehen Sie zu Persönliche Zertifikate/Personal.
- 3. Wählen Sie das Zertifikat mit dem Namen Ihres Computers aus.

Console1 -	[Console Root\Certificates (Lo	cal Computer)\Personal\Certifi	cates]	- 🗆 🗙
Eile Action View Favorites Window	w <u>H</u> elp			_ 8 ×
🗢 🏟 🖄 📰 🔏 🖏 🗶 🖬 🕒				
Console Root	Issued To	Issued By	Expiration Date	Intended Purpose ^
Certificates (Local Computer)	WIN-NOU0K4P18VB	WIN-NOU0K4P18VB	31.01.2053	<all></all>
Personal Personal Trusted Root certification Auth Enterprise Trust Intermediate Certification Auth Trusted Publishes Untrusted Certificates	 HolpsonProg. Management Inc. HolpsonProg. Reporting Table HolpsonProg. Table Reports HolpsonProg. Table HolpsonProg. Table<th>Asligani Proy Hangamari Seri, Asligani Proy Rapming Tele Solgani Proy Ter Hangamari - Boli Tani Ca Mille (di TualCa Wile) Se TualCa</th><th>9 (8 ,00) 9 (8 ,00) 9 (8 ,00) 9 (8 ,00) 9 (8 ,00) 9 (8 ,00) 9 (8 ,00)</th><th>×</th>	Asligani Proy Hangamari Seri, Asligani Proy Rapming Tele Solgani Proy Ter Hangamari - Boli Tani Ca Mille (di TualCa Wile) Se TualCa	9 (8 ,00) 9 (8 ,00) 9 (8 ,00) 9 (8 ,00) 9 (8 ,00) 9 (8 ,00) 9 (8 ,00)	×
Personal store contains 9 certificates.				

4. Wählen Sie auf dem Zertifikat die Aktion Alle Aufgaben/All Tasks und dann Exportieren/Export. 5. Klicken Sie Weiter/Next und wählen danach den Export ohne privaten Schlüssel.

	×
📀 🔗 Certificate Export Wizard	
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 <u>exporting private keys</u>	
Next Cancel	1

6. Wählen Sie als Dateiformat das DER-Format aus.



7. Legen Sie den Speicherort fest.



8. Bestätigen Sie die gewählten Einstellungen und Klicken Sie Beenden/Finish.

HINWEIS: Wenn sich der digiSeal server auf einem entfernten Server befindet, kopieren Sie die Datei mit dem Zertifikat dorthin.

n

Ð

HINWEIS: Stellen Sie sicher, dass auf dem digiSeal server die API aktiviert ist.

	3.1. Benutzerkonten	1 3.2 Basis	configuration	3.3. Ereign	ismeldung
3 <mark>0</mark>	Proxyserver	0.0.1100/7741	, masterine of I	3.6. Suriwalea	iktualisielung
Betrieb	Konfiguration zur Verwendung ein	nes Proxyservers für die Kommur	nikation mit Online-Dienst	en.	
	Proxyserver verwenden				
1±T	Servername:				Port: 1
rozess-	Proxy-Typ	C HTTP 1.1			
iguator	Prosu enfordert Authentifiz	isuna			
\times	Benutzer				1
ministration	Passwort				-
		1			
곱	API Nutzung Konfiguration der API Nutzung		Webservice Nutzung Konfiguration der We) hservice-Schnittstelle	
nfo / Hilfe	API-Schnittstelle aktivieren				
	API Port 2001		Konfigurieren		
	- diciSe al server 2 K onlice rationen	~			
Logout	Änderungen des Konfigurationsp	orts werden erst beim nächsten !	Start des Dienstes wirksa	m.	
	digiSeal server 2 Konfigurationsp	vt 2003			

Aktivieren Sie die API für jeden Prozess, der von NoSpamProxy Encryption verwendet werden soll. Stellen Sie dazu sicher, dass das Häkchen für API-Schnittstelle aktivieren gesetzt ist. Die Schnittstelle wird nur für Programme aktiviert, die ein Zertifikat verwenden, das in der Liste API-Schnittstelle aufgeführt ist. In diese Liste muss das zuvor exportierte Zertifikat aufgenommen werden.



Konfigurieren von NoSpamProxy

NoSpamProxy Encryption benötigt einige Dateien aus dem digiSeal server Verzeichnis.

- Kopieren Sie die folgenden Dateien aus dem digiSeal server Programmverzeichnis in das Verzeichnis %ProgramFiles%\Net at Work Mail Gateway\Gateway Role:
 - dsServerAPI.dll
 - dsServerAPI.dll.p7s
 - dsServerAPI.signature
- 2. Starten Sie die Gatewayrolle neu.
- Folgen Sie den Hinweisen unter <u>digiSeal-server-Verbindung</u> sowie unter <u>Qualifizierte Dokumentensignatur mit dem digiSeal server</u>, um die Optionen in der Oberfläche für die Benutzung des digiSeal servers einzurichten. Beachten Sie im Besonderen die folgenden Punkte:
 - Konfiguration > Verbundene Systeme | Konfigurieren Sie die Verbindung zum digiSeal server.
 - Konfiguration > Benutzer-Benachrichtigungen | Konfigurieren Sie die E-Mail-Benachrichtigungen und die Administrativen E-Mail-Adressen.
 - Konfiguration > Regeln| Fügen Sie die Aktion digiSeal server: Signiere Anhänge an ausgehenden E-Mails zu einer neuen oder bestehenden ausgehenden Regel hinzu und konfigurieren Sie diese wie beschrieben.
 - Konfiguration > Regeln| Fügen Sie die Aktion

digiSeal server: Überprüfen und Erzwingen von signierten Anhängen auf eingehenden E-Mails| zu einer neuen oder bestehenden eingehenden Regel hinzu und konfigurieren Sie diese wie beschrieben.

Archivierung

የገ

Die beiden digiSeal server-Aktionen der Regeln von NoSpamProxy stellen Daten für die Archivschnittstelle von NoSpamProxy bereit, falls Sie dort einen Archivkonnektor konfiguriert haben. Bei der Archivierung werden die E-Mails, Signaturen und Prüfprotokolle an den konfigurierten Archivkonnektor übergeben.

HINWEIS: Details hierzu finden Sie unter <u>Archivkonnektoren</u>. Ein
Archivkonnektor für neue, bisher nicht unterstützte Archivsysteme
kann in Absprache mit Ihnen durch Net at Work implementiert
werden.

Vorfälle der qualifizierten Signatur

Nicht immer kann das Signieren oder Überprüfen von Dokumenten korrekt abgeschlossen werden. Es kann beispielsweise vorkommen, dass

- die Verbindung zum digiSeal server nicht hergestellt werden kann oder
- der digiSeal server keinen OCSP-Server im Internet erreichen kann.

In diesen Fällen wird die E-Mail von NoSpamProxy Encryption zwar angenommen, aber nicht an den Empfänger weitergeleitet. Stattdessen werden die betroffenen E-Mails zwischengespeichert.

Der Administrator erhält in diesem Fall - sofern konfiguriert - eine E-Mail. In der Oberfläche werden diese E-Mails unter <u>Angehaltene E-Mails</u> angezeigt. Der Administrator kann pro Vorfall entscheiden, ob die E-Mail erneut durch NoSpamProxy Encryption zugestellt werden soll oder ob der Vorfall gelöscht wird.

Anzeigen des lokalen Zertifikatsspeichers

Um die Zertifikate des lokalen Computers anzuzeigen, gehen Sie folgendermaßen vor:

1. Starten Sie ein neues NoSpamProxy Command Center.

-				Console	1 - [Console Root]		- 🗆 🗙
Eile Action	<u>V</u> iew Fa	av <u>o</u> rites	Window	<u>H</u> elp			_ 6 ×
⇐ ⇒ 🗖 🗟	? 🎫						
📔 Console Root		Name					
					There are no items to show in th	is view.	

- 2. Klicken Sie unter Datei/File auf Snap-In hinzufügen/entfernen/Add/Remove Snap-in.
- Wählen Sie das Zertifikate/Certificates Snap-In aus und klicken Sie Hinzufügen/Add.

Active Directory Do	Vendor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	^	Sgected shap-ins:	(Local Computer)	Edit Extensions Remove Move Up
ADSI Edit Certificate Templates Certificates Certificates Component Services Computer Managem Device Manager Disk Management	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor		<u>A</u> dd >		Move <u>D</u> own
escription:		~	L		Au <u>v</u> ariceu

4. Wählen Sie im Konfigurationsassistenten das Computer-Konto/Computer

account.

5. Wählen Sie Lokaler Computer/Local computer.

Select Computer	×
Select the computer you want this snap in to manage. This snap in will always manage: [
O Another computer:	B <u>r</u> owse
Allow the selected computer to be changed when launching from the comm only applies if you save the console.	and line. This
< <u>B</u> ack Finish	Cancel

- 6. Klicken Sie Beenden/Finish.
- 7. Klicken Sie OK, um den Dialog zu schließen.
- 8. Gehen Sie zu Konsolenstamm/Console Root.

9. Klicken Sie Zertifikate (Lokaler Computer)/Certificates (Local Computer), um die Zertifikatsspeicher für den Computer anzuzeigen.

Hilfe und Unterstützung

Knowledge Base

Die Knowledge Base enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

Website

Auf der **NoSpamProxy-Website** finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

NoSpamProxy-Forum

Das <u>NoSpamProxy-Forum</u> gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

Blog

Das <u>Blog</u> bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite des NoSpamProxy Command Center angezeigt.

YouTube

In unserem <u>YouTube-Kanal</u> finden Sie Tutorials, How-tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

NoSpamProxy-Support

Unser Support-Team erreichen Sie

- per Telefon unter <u>+49 5251304-636</u>
- per E-Mail unter <u>support@nospamproxy.de</u>.



