

Windows-Firewall Ausnahmen für Docusnap konfigurieren

© itelio GmbH

Inhaltsverzeichnis

1 Windows Firewall Konfiguration - Grundlagen	3
1.1 Übersicht - benötige Firewall Ausnahmen	3
2 Windows 7	4
2.1 Windows 7 - Windows Firewall Konfiguration per Befehl starten	4
2.2 Windows 7 - Windows Firewall Konfiguration interaktiv starten	5
2.3 Windows 7 – Windows-Firewall Ausnahmen festlegen	7
3 Windows Vista	9
3.1 Windows Vista – Windows Firewall Konfiguration per Befehl starten	9
3.2 Windows Vista – Windows Firewall Konfiguration interaktiv starten]]
3.3 Windows Vista – Windows-Firewall Ausnahmen festlegen	13
4 Windows XP (ab SP2)	14
4.1 Windows XP – Windows Firewall Konfiguration starten	14
4.2 Windows XP – Windows-Firewall Ausnahme festlegen	15
4.3 Windows XP – per GPO zusätzliche Ausnahme aktivieren – GPO Editor starten	16
4.4 Windows XP – per GPO zusätzliche Ausnahme aktivieren	17
5 Windows Firewall Konfiguration - Active Directory	18
5.1 Grundlagen: Firewall – Gruppenrichtlinien/Verwaltungskonsole (GPMC)	18
5.2 AD Windows Firewall Konfiguration – GPMC starten	19
5.3 AD Windows Firewall – Gruppenrichtlinienobjekt für die Domäne erstellen	20
5.4 AD Windows Firewall - Zuvor erstelltes Gruppenrichtlinienobjekt bearbeiten	21
5.5 AD Windows Firewall - Ausnahme für Datei- und Druckerfreigabe aktivieren	23
5.6 AD Windows Firewall – Remotever waltungsausnahme aktivieren	24

1. Windows Firewall Konfiguration - Grundlagen

Damit der Scan von Windowssystemen mit aktivierter Firewall mit Docusnap gelingt, sind zwei Firewall Ausnahmen zu überprüfen bzw. zu konfigurieren. Diese Einstellungen können per Gruppenrichtlinien erzeugt und verwaltet werden. Für einen schnellen Test wird die manuelle Konfiguration der Windows-Firewall ebenfalls vorgestellt. Die Beispiele – manuelle Konfiguration wurden für Windows 7, Vista und XP entworfen.

1.1 Übersicht - benötige Firewall Ausnahmen

Es erfolgt nun eine kurze Beschreibung der zu treffenden Ausnahmen. Die Beschränkung der Ausnahmen auf bestimmte IP Bereiche kann nur über die Konfiguration von Gruppenrichtlinienobjekten (GPO) erfolgen.

Datei und Druckfreigabe

Ermöglicht die Datei- und Druckerfreigabe. Windows-Firewall öffnet hierzu UDP-Port 137 und 138 und TCP-Port 139 und 445. Durch Aktivieren dieser Richtlinieneinstellung öffnet Windows-Firewall diese Ports, sodass das Windows-System Druckaufträge und Zugriffsanforderungen für freigegebene Dateien empfangen kann.

Hinweis: Diese Einstellung lässt Windows-Firewall eingehende ICMP-Echoanforderungen (eine vom Dienstprogramm Ping gesendete Meldung) zu, und zwar auch dann, wenn die Richtlinieneinstellung "Windows-Firewall: ICMP-Ausnahmen zulassen" sie blockieren würde.

Hinweis Sicherheit: Es sollte festgelegt werden, für welche IP-Adressen oder Subnetze die eingehenden Meldungen zulässig sind.

Remoteverwaltungsausnahme zulassen

Entspricht im wesentlichen der Windows 7 / Vista Ausnahme Windows-Verwaltungsinstrumentation (WMI) und ermöglicht die Remoteverwaltung des Windowssystems mit Verwaltungsprogrammen, wie z. B. Microsoft Management Console (MMC) und Windows-Verwaltungsinstrumentation (WMI). Windows-Firewall öffnet hierzu TCPPort 135 und 445. Dienste verwenden diese Ports normalerweise für die Kommunikation mithilfe von Remoteprozedur aufrufen (RPC) und DCOM (Distributed Component Object Model).

Darüber hinaus ermöglicht diese Richtlinieneinstellung den Programmen SVCHOST.EXE und LSASS.EXE unerbetene eingehende Meldungen zu empfangen und ermöglicht gehosteten Diensten, zusätzliche dynamisch zugewiesene Ports zu öffnen.

Hinweis Sicherheit: Es sollte festgelegt werden für welche IP-Adressen oder Subnetze diese eingehenden Meldungen zulässig sind.

2. Windows 7

2.1 Windows 7 – Windows Firewall Konfiguration per Befehl starten

Der einfachste Weg die Firewall-Konfiguration zu starten ist per Befehl firewall.cpl

Folgende Varianten für die Befehlseingabe sind möglich:





> Programme/Dateien durchsuchen Eingabe: firewall.cpl> Ausführen Eingabe: firewall.cpl

Alternativ kann der Befehl auch in einem Konsolenfenster erfolgen.

2.2 Windows 7 – Windows Firewall Konfiguration interaktiv starten





> Klicken und

Systemsteuerung auswählen



> System und Sicherheit anklicken



> Auf Windows-Firewall klicken

2.3 Windows 7 - Windows-Firewall Ausnahmen festlegen



> Ein Programm oder Feature durch die Windows-Firewall zulassen anklicken

 System und Sicherneit + Windows-Firewall + Zuge 	lassene Pro	ogramme	• 🔛	Systemsteuerung	g aurchsuchen
Kommunikation von Programmen durch	die Windo	ws-Firewall zulasse	n		
Klicken Sie zum Hinzufügen, Ändern oder Entferi	nen zugela:	ssener Programme und	Ports auf "Eir	nstellungen ändern".	
Welche Risiken bestehen, wenn die Kommunikat	ion von Pro	orammen zugelassen		Einstellungen ände	ern
wird?					Contraction of the local division of the loc
U Ihrer Sicherheit werden einige Einstellu	ngen vom S	Systemadministrator ver	rwaltet.		
Zugelassene Programme und Features:					10
Name	Domäne	Heim/Arbeit (Privat)	Öffentlich	Gruppenrichtlinie	-
Routing und RAS				Nein	
Schlüsselverwaltungsdienst				Nein	
Secure Socket Tunneling-Protokoll				Nein	
SNMP-Trap				Nein	
Tragbare Drahtlosgeräte				Nein	
Verbindung mit einem Netzwerkprojek				Nein	
Windows Media Player				Nein	
☐ Windows Media Player -Netzwerkfreig				Nein	
☐ Windows Media Player-Netzwerkfreig				Nein	-
Windows-Firewallremoteverwaltung				Nein	
Windows-Peer-zu-Peer-Zusammenarb				Nein	
Windows-Remoteverwaltung				Nein	
Windows-Verwaltungsinstrumentation				Nein	-
			De <u>t</u> ail	s Entferner	a [
-			Anderes	Programm zulassen	
			O	K Abbrech	ien

> Einstellungen ändern schaltet, entsprechende Benutzerrechte vorausgesetzt, die Bearbeitung von Programmen und Features frei. Windows 7 kennt drei unterschiedliche Netzwerktypen (Domäne, Heim/Arbeit, Öffentlich). Die Firewall Ausnahmen werden separat für jeden Typ definiert. Für die verwendeten Netzwerk Typen sind folgenden Ausnahmen per Haken in der Liste Zugelassene Programme und Features zu setzen:

- Datei- und Druckerfreigabe
- Windows-Verwaltungsinstrumentation (WMI)

Die neuen Einstellungen nun per Klick auf die OK Schaltfläche übernehmen. Diese Firewall Einstellungen ermöglichen Docusnap den Rechner zu scannen.

3. Windows Vista

3.1 Windows Vista – Windows Firewall Konfiguration per Befehl starten

Der einfachste Weg die Firewall-Konfiguration zu starten, ist per Befehl firewall.cpl.

Folgende Varianten für die Befehlseingabe sind möglich:





> Suche starten Eingabe: firewall.cpl

> Ausführen Eingabe: firewall.cpl

Alternativ kann der Befehl auch in einem Konsolenfenster erfolgen.

Windows-Firewall		
Windows-Firewall ein- oder ausschalten	Windows-Firewall	
Programm durch die	Die Windows-Firewall kann dazu beitragen, Hacker oder böswillige Zugriff auf den Computer über das Internet bzw. ein Netzwerk zu e	e Software daran zu hindern, erlangen.
kommunizieren lassen	Wie kann eine Firewall zum Schutz des Computer beitragen?	
	Einige Einstellungen werden durch eine Gruppenrichtlinie ges	teuert.
	Ø Der Computer wird durch die Windows-Firewall gesch	ützt.
	Windows-Firewall ist an.	Einstellungen ändern
	Eingehende Verbindungen, die keine Ausnahmen besitzen, werd	en geblockt.
	Eine Benachrichtigung anzeigen, wenn ein Programm geblockt wird:	Ja
	Netzwerkstandort:	Öffentliches Netzwerk
	Was sind Netzwerkstandorte?	
Siehe auch		
Sicherheitscenter		
Netzwerkcenter		

> Mit Klick auf Programm durch die Windows-Firewall kommunizieren lassen gelangt man in die Ausnahmen Konfiguration.

3.2 Windows Vista – Windows Firewall Konfiguration interaktiv starten





> Klicken und

Systemsteuerung auswählen



> Programme durch die Windows-Firewall kommunizieren anklicken



> Programm durch die Windows-Firewall kommunizieren lassen anklicken

3.3 Windows Vista – Windows-Firewall Ausnahmen festlegen

Windows-Firewalleinstellungen
Allgemein Ausnahmen Erweitert
Ausnahmen kontrollieren, wie Programme durch die Windows-Firewall kommunizieren. Fügen Sie eine Programm- oder Portausnahme hinzu, um Kommunikation durch die Firewall zu gestatten. Die Windows-Firewall verwendet momentan Einstellungen für den Netzwerkstandort "Öffentlich". <u>Risiken durch das Aufheben von Blockierungen</u> Markieren Sie das entsprechende Kontrollkästchen, um eine Ausnahme zu aktivieren:
Programm oder Port
SNMP-Trap
Tragbare Drahtlosgeräte
Verbindung mit einem Netzwerkprojektor herstellen
VMware Authd
Windows Live Sync
Windows Media Player
Windows Media Player-Netzwerkfreigabedienst
Windows-Firewallremoteverwaltung
Windows-Peer-zu-Peer-Zusammenarbeits-Foundation
Windows Remoteverwaltung
Windows-Teamarbeit
Windows-Verwaltungsinstrumentation (WMI)
Programm hinzufügen Port hinzufügen Eigenschaften Löschen
✓ Benachrichtigen, wenn ein neues Programm geblockt wird
OK Abbrechen Ü <u>b</u> ernehmen

> In der Liste Programm oder Port sind folgende Ausnahmen per Haken anzuwählen:

- Datei- und Druckerfreigabe
- Windows-Verwaltungsinstrumentation (WMI)

Nun die gewählten Einstellungen mit der Schaltfläche Übernehmen und dann OK bestätigen. Diese Firewall Einstellungen ermöglichen Docusnap den Rechner zu scannen.

4. Windows XP (ab SP2)

4.1 Windows XP – Windows Firewall Konfiguration starten

Der schnellste Weg um die Firewall-Konfiguration aufzurufen ist per Befehl firewall.cpl



- > per Eingabeaufforderung
- > über Start > Ausführen

4.2 Windows XP – Windows Firewall Konfiguration interaktiv starten

👺 Windows-Firewall	<
Allgemein Ausnahmen Erweitert	
Eingehende Netzwerkverbindungen mit Ausnahme cer unten aufgelisteten Programme und Dienste wercen geblockt. Durch Hinzufügen weiterer Ausnahmen funktionieren die entsprechenden Programme eventuell besser, aber das Sicherheitsrisiko kann sich erhöhen.	
Programme und <u>D</u> ienste:	
Catei- und Druckerfreigabe Nicrosoft Office Outlook Netzwerkdiagnose für Windows XP Femotedesktop Femoteunterstützung LPnP-Framework	
Programm Port Bearbeten Löschen	
Benachrichtigen, wenn Programm durch Windows-Firewall geblockt wird	
weiche misiken destehen dem Zulassen von Ausnahmen?	
OK Abtrechen	1

> Auf den Reiter Ausnahmen klicken. In der Liste Programm oder Dienste ist folgende Ausnahme per Haken anzuwählen:

• Datei- und Druckerfreigabe

Mit der Schaltfläche OK bestätigen. Die Windows-Firewall kann nun geschlossen werden.

4.3 Windows XP – per GPO zusätzliche Ausnahme aktivieren – GPO Editor starten

🚡 Gruppenrichtlinie		_O×
Datei Aktion Ansicht ?		
Richtlinien für Lokaler Computer Softwareeinstellungen Softwareeinstellungen	Einstellung Windows-Firewall: Alle Netzwerkverbindungen schützen Windows-Firewall: Keine Ausnahmen zulassen Windows-Firewall: Programmausnahmen festlegen Windows-Firewall: Ausnahmen für lokale Programme zulassen Windows-Firewall: Remoteverwaltungsausnahme zulassen Windows-Firewall: Ausnahme für Datei- und Druckerfreigabe zula Windows-Firewall: ICMP-Ausnahmen zulassen Windows-Firewall: ICMP-Ausnahmen zulassen Windows-Firewall: Benachrichtigungen nicht zulassen Windows-Firewall: Benachrichtigungen nicht zulassen Windows-Firewall: Drotokollierurg zulassen Windows-Firewall: Uncastantwert auf Multicast- oder Broadcasta Windows-Firewall: Portausnahmen festlegen Windows-Firewall: Ausnahmen für lokale Ports zulassen	Status Nicht konfiguriert
	Erweitert A Standard /	
		1

>In Windows XP Firewall Ausnahmen fehlt die in Windows Vista und Windows 7 vorhandene Ausnahme Windows Verwaltungsinstrumentation (WMI)

Diese Ausnahme wird in Windows XP per Gruppenrichtlinien Einstellung aktiviert. Deshalb wird in den lokalen Gruppenrichtlinien Einstellungen die Firewall Ausnahme Remoteverwaltungsausnahme zulassen konfiguriert. Das Programm wird mit gpedit.msc gestartet. (per Eingabeaufforderung oder über Start > Ausführen)

Die zu aktivierende Gruppenrichtlinie befindet sich in: Richtlinien für Lokaler Computer Computerkonfiguration Administrative Vorlagen Netzwerk Netzwerkverbindungen Windows – Firewall Domänenprofil

4.4 Windows XP – per GPO zusätzliche Ausnahme aktivieren

Eigenschaften von Windows-Firewall: Remoteverwaltungsaus 🎴 🗙
Einstellung Erklärung
🗿 Windows-Firewall: Remoteverwaltungsausnahme zulassen
C Nicht <u>k</u> onfiguriert
<u>Aktiviert</u>
C Deaktiviert
Unerbetene eingehende Nachrichten zulassen von:
localsubnet
Syntax:
Geben Sie "*" ein, um Meldungen von allen Netzwerken zuzulassen,
oder geben Sie eine durch Komma getrennte Liste ein, die eine
Ziffer oder folgende Kombination enthält:
IP-Adressen, wie z. B. 10.0.0.1
Subnetzbeschreibungen, wie z. B. 10.2.3.0/24
J Die ∠eichenfolge "localsubnet"
Unterstützt auf: Mindestens Microsoft Windows XP Professional mit SP 2
Vorherige Einstellung Nächste Einstellung
OK Abbrechen Ü <u>b</u> ernehmen

>Die Gruppenrichtlinie Windows Firewall: Remoteverwaltungsausnahme zulassen aktivieren und die Reichweite der Einstellung im Eingabefeld festlegen. Dann Fenster mit Klick auf die OK Schaltfläche schließen.

Unerbetene eingehende Nachrichten zulassen von:

- Ein Stern im Eingabefeld schaltet die Firewall für jeden beliebigen Rechner frei
- Die Ausnahme gilt nur für ein bestimmtes Subnetz
- (z.B. volles Class C Netzwerk 192.168.100.0/24)
- Das lokale Subnetz kann auch über die Zeichenfolge localsubnet freigeschaltet werden
- Die Ausnahme auf einen bestimmten PC beschränkt werden (z.B. 192.168.100.10)

Die Anwendung kann jetzt geschlossen werden. Die Windows-Firewall Ausnahmen für Windows XP sind nun vollständig konfiguriert.

5. Windows Firewall Konfiguration – Active Directory

5.1 Grundlagen: Firewall – Gruppenrichtlinien/Verwaltungskonsole (GPMC)

Um die Firewall-Konfiguration für mehrere Rechner durchzuführen, wird empfohlen die benötigten Einstellungen per GPO vorzunehmen. Die Einstellungen sind ab XP SP2 gültig. Es ist nicht nötig für Vista und Windows 7 Rechner gesonderte Windows-Firewall Ausnahmen zu definieren.

Das folgende Beispiel zeigt wie mit dem Microsoft Tool Gruppenrichtlinien-Verwaltungskonsole (GPMC) eine domänenweite Einstellung vorgenommen wird. GPO Einstellungen können lokal (L), standortweit (S), domänenweit (D) und auf der Organisationsebene (OU) vorgenommen werden. Dabei überschreiben nachfolgende Einstellungen zuvor festgelegte Werte. Die Reihenfolge lautet L, S, D, OU.

Die Gruppenrichtlinien Verwaltungskonsole kann auf der Microsoft Webseite kostenlos geladen werden. Dieses Tool ändert in diesem Beispiel die Firewall Einstellungen für alle in der Domäne vorhandenen Systeme und sollte nur mit Bedacht verwendet werden.

5.2 AD Windows Firewall Konfiguration – GPMC starten



> Der einfachste Weg um die Verwaltungskonsole aufzurufen ist per Befehl gpmc.msc
 (Eingabeaufforderung oder über Start > Ausführen)

5.3 AD Windows Firewall -

Gruppenrichtlinienobjekt für die Domäne erstellen

Scuppenrichtlinienve	erwaltung					_ 🗆 ×
හිදී Datei Aktion Ansid	:ht <u>E</u> enster <u>?</u>					_ 8 ×
← → 🗈 🖪	📽 🙆 😫 🖬					
Gruppenrichtlinienverwi Gesamtstructur: dsi Gesamtstructur: dsi Gesam	altınıq idemo.local iruppenrichtliniengbjekt hier ers orhandenes Gruppenrichtliniend tererbung deaktivieren iruppenrichtlinienmodellierungs- jeue Organisationseinheit juchen törenencontroller änglern intfernen kitve Directory-Benutzer und -O insicht leues Fenster ktualisieren Eigensghaften jilfe	dsdemo.local Verknüpfte Gruppenrichtlinie tellen und verknüpfen bijek: verknüpfen Computer	nobjekte Gruppenrichtlinienverer Gruppenrichtlinienobjekt 쥸 Default Domain Policy 중 Windows-Firewall Ausnahme	bung Delegi Erzwungen Nein Nein	erung Verknüpfung sktiviert Ja Ja	Status d Aktiviert Aktiviert
		•				

> Per Rechtsklick auf die gewünschte Domäne gelangt man zur Auswahl
 Gruppenrichtlinenobjekt hier erstellen und verknüpfen...

5 Gruppenrichtlinienverwaltung				_ 🗆 ×
හිදු Datei Aktion Ansicht Eenster ?				_ 8 ×
양을 Gruppenrichtlinienverwaltung 금 슈 Gesemtstruktur: dsdemo.local 금 및 Domänen	dsdemo.local Verknüptte Gruppenrichtlinienobjekte Gruppenrichtlinienvererb	ung Delegi	erung	1
Default Domain Policy	Verknüpfu A Gruppenrichtlinienobjekt	Erzwungen	Verknüpfung aktivier	Status d
Windows-Firewall Aus	☆ 1 🚲 Defaul Domain Policy	Nein	Ja	Aktiviert
CIFS DOCUSNAP DOCUSNAP DOCUSNAP DOCUSNAP DOCUSNAP DOCUSNAP DOCUSNAP DOCUSNAP DOCUSNAP Name: Ware: DOCUSNAP Name: DOCUSNAP Name: DOCUSNAP DOCUSNAP Name: DOCUSNAP DOCUSNAP Name: DOCUSNAP DOCUSNAP Name: DOCUSNAP DOCUSNAP Name: DOCUSNAP DOCUSNAP DOCUSNAP DOCUSNAP Name: DOCUSNAP DOCUSNAP Name: DOCUSNAP	penrichtlinienobjekt X Indows Eirewal-Ausnahmer	n en	Ja	AKUVIA

> Einen entsprechenden Namen für das Gruppenrichtlinenobjekt festlegen

5.4 AD Windows Firewall -

Zuvor erstelltes Gruppenrichtlinienobjekt bearbeiten



> Mit einem Rechtsklick das zuvor erstellte Gruppenrichtlinienobjekt anwählen und die Option Bearbeiten auswählen

5.4 AD Windows Firewall –

Zuvor erstelltes Gruppenrichtlinienobjekt bearbeiten



> Nun öffnet sich der Gruppenrichtlinienobjekt-Editor

Die zu aktivierenden Gruppenrichtlinien befinden sich in:

```
Richtlinien für Lokaler Computer
Computerkonfiguration
Administrative Vorlagen
Netzwerk
Netzwerkverbindungen
Windows – Firewall
Domänenprofil
```

5.5 AD Windows Firewall -

Ausnahme für Datei- und Druckerfreigabe aktivieren

Eigenschaften von Windows-Firewall: Ausnahme für Datei- und <mark>?</mark> 🗙
Einstellung Erklärung
😭 Wincows-Firewall: Ausnahme für Datei- und Druckerfreigabe zulassen
Nicht konfiguriert
Aktivert
O <u>D</u> eaktiviert
Unerbetene eingehende Nachrichten zulassen von: Iocalsubnet Syntax: Geben Bie "*" ein, um Meldungen von allen Netzwerken zuzulassen, oder geben Sie eine durch Komma getrennte Liste ein, die eine Ziffer oder folgende Kombination enthält: IP-Adressen, wie z. B. 10.0.0.1 Subnetzbeschreibungen, wie z. B. 10.2.3.0/24
Unterstützt auf: Mindestens Microsoft Windows XP Professional mit SP 2
Vorherige Einstellung Nächste Einstellung
OK. Abbrechen Übernehmen

> Windows-Firewall: Ausnahme für Datei- und Druckerfreigabe zulassen aktivieren

In diesem Beispiel wird die Firewall Ausnahme mit Beschränkung auf das lokale Subnetz aktiviert.

5.6 AD Windows Firewall – Remoteverwaltungsausnahme aktivieren

nschaften v	on Windows-Firewall: Remoteverwaltungsaus 🎦 🗙
nstellung Erk	lárung
🗿 Windows-F	iiewall: Remoteverwaltungsausnahme zulassen
0 Nicht <u>k</u> onfi	puriert
• <u>A</u> ktiviert	
Deaktiviert	
Unerbetene e	ingehende Nachrichten zulassen von:
la a a la chur a t	
liocaisubnet	
Syntax:	
Geben Sie ''*	ein, um Meldungen von allen Netzwerken zuzulassen,
oder geben S	e eine durch Komma getrennte Liste ein, die eine
Ziffer oder fol	jende Kombination enthält:
IP-Adresser	, wie z. B. 10.0.0.1
Subnetzbes	chreibungen, wie z. B. 10.2.3.0/24
Die Zeichei	ilolge "localsubnet" 📃
Unterstützt auf	Mindestens Microsoft Windows XP Professional mit SP 2
Vorherige Ein	stellung Nächste Einstellung
	OK Abbrechen Übernehmen

> Windows-Firewall: Remoteverwaltungsausnahme definieren aktivieren

Für dieses Beispiel wird die Firewall Ausnahme mit Beschränkung auf das lokale Subnetz gesetzt.

