

Docusnap X - Windows Firewall Ausnahmen

Windows Firewall Ausnahmen für Docusnap konfigurieren



TITEL	Docusnap X - Windows Firewall Ausnahmen
AUTOR	Docusnap Consulting
DATUM	18.12.2018
VERSION	1.2 gültig ab 26.09.2018

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die itelio GmbH zugestanden. Zuwiderhandlung verpflichtet zu Schadenersatz. Alle Rechte vorbehalten.

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of itelio GmbH. All rights reserved.



INHALTSVERZEICHNIS

1. Einleitung	4
2. Grundlagen	5
2.1 Benötigte Firewall Ausnahmen	5
3. Windows Firewall Konfiguration – Active Directory	6
3.1 Verwaltungskonsole (GPMC)	6
3.2 GPMC starten	7
3.3 Gruppenrichtlinienobjekt erstellen	8
3.4 Gruppenrichtlinienobjekt bearbeiten	9
3.5 Ausnahme für Datei- und Druckerfreigabe aktivieren	11
3.6 Remoteverwaltungsausnahme aktivieren	12
3.7 Gruppenrichtlinienobjekt bearbeiten – weitere Möglichkeiten	13
3.7.1 Datei- und Druckerfreigabe aktivieren - Ping	15
3.7.2 Windows Verwaltungsinstrumentation (WMI) aktivieren	18
4. Windows 10 – Windows Firewall Konfiguration (lokal)	21
4.1 Ausnahme festlegen	23



1. Einleitung

Docusnap inventarisiert Windows Systeme mit Hilfe der Standardschnittstelle Windows Management Instrumentation (WMI). Ist auf einem Windows System die Windows-Firewall aktiviert, wird hierdurch unter Umständen das Auslesen verhindert. Dieses Dokument beschreibt die notwendigen Anpassungen von Firewall-Einstellungen bei Windows Systemen.

Im Kapitel WINDOWS FIREWALL KONFIGURATION – ACTIVE DIRECTORY wird beschrieben wie die erforderlichen Windows-Firewall Ausnahmen über Gruppenrichtlinien mit Hilfe des Active Directory organisationsweit konfiguriert werden können. Dies ist die von uns empfohlene Methode.

Im Kapitel WINDOWS 10 - WINDOWS FIREWALL KONFIGURATION (LOKAL) wird am Beispiel von Windows 10 beschrieben wie *lokale* Gruppenrichtlinien zu konfigurieren sind. Die Anpassung der *lokalen* Gruppenrichtlinien ist nur in Arbeitsgruppen oder zu Testzwecken sinnvoll.



2. 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.

2.1 Benötigte Firewall Ausnahmen

Es erfolgt nun eine kurze Beschreibung der zu treffenden Ausnahmen.

Datei- und Druckerfreigabe

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

<u>Hinweis:</u> Diese Einstellung lässt die 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.

Remoteverwaltungsausnahme zulassen

Entspricht im Wesentlichen der Windows Firewall Ausnahme Windows-Verwaltungsinstrumentation (WMI) und ermöglicht die Remoteverwaltung des Windowssystems mit Verwaltungsprogrammen, wie z. B. Microsoft Management Console (MMC) und Windows-Verwaltungsinstrumentation (WMI). Die Windows Firewall öffnet hierzu TCP-Port 135 und 445. Dienste verwenden diese Ports normalerweise für die Kommunikation mithilfe von Remoteprozeduraufrufen (RPC) und DCOM (Distributed Component Object Model).

Sicherheitshinweis

Es wird empfohlen, die Einstellung per Gruppenrichtlinie zu verteilen, damit erlaubte IP-Adressen oder Subnetze für diese Ausnahmen gesetzt werden können.



3. Windows Firewall Konfiguration – Active Directory

3.1 Verwaltungskonsole (GPMC)

Um die Firewall Konfiguration für mehrere Rechner durchzuführen, wird empfohlen, die benötigten Einstellungen per Gruppenrichtlinie vorzunehmen.

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.

Sofern die Gruppenrichtlinien-Verwaltungskonsole nicht bereits installiert ist, kann diese kostenlos bei Microsoft heruntergeladen werden. Im folgenden Beispiel werden hiermit die Firewall Einstellungen für alle in der Domäne vorhandenen Systeme geändert. Ein vorheriger Test in einer Testumgebung oder der Einsatz der Einstellungen nur auf eine spezielle Test- Organisationsebene *(OU)* im Active Directory wird dringend empfohlen.

Die Remoteserver-Verwaltungstools, welche die GPMC enthalten, können für die Windows Client-Betriebssysteme bei Microsoft heruntergeladen werden:

Bei Windows Server-Betriebssystemen (ab 2008) ist die GPMC bereits enthalten, muss aber gegebenenfalls über den Server-Manager nachinstalliert werden.



3.2 GPMC starten

Starten Sie den Windows-Ausführen-Dialog (Windows-Taste+R) und geben gpmc.msc ein.

L.	Gruppenrichtlinienverwaltung
📓 Datei Aktion Ansicht Fenster ?	
	Gruppenrichtlinienverwaltung
Gesamtstruktur: docusnap.intern	Inhalt
Domanen	A
docusnap.intern	Name
Activate SecurityCenter	🔬 Gesamtstruktur: docusnap.intem
Default Domain Policy	
S-Script	
Firewall Exception	
KDP - Allow	
Windows Firewaii-Ausnanmen	
a docusnap	
Domain Controllers	
EnrestGroups	
MPORT	
b 🖬 Loop	
Microsoft Exchange Security Groups	
▷ I RES_DOM	
iservice_accounts	
⊳ 📴 TestOÜ	
Gruppenrichtlinienobjekte	
WMI-Filter	
b i Starter-Gruppenrichtlinienobjekte	
b i Standorte	
💱 Gruppenrichtlinienmodellierung	
🔀 Gruppenrichtlinienergebnisse	

Abbildung 1 - Gruppenrichtlinienverwaltung



3.3 Gruppenrichtlinienobjekt erstellen

Per Rechtsklick auf die gewünschte *Domäne* oder eine *OU* gelangt man zur Auswahl *Gruppenrichtlinienobjekt hier erstellen und verknüpfen*.

<u>s</u>		Gru	ppenrichtlinienverwa	Itung
🛃 Datei Aktion Ansicht Fenster ?				
🗢 🏟 📶 🗙 🔍 📗				
Gruppenrichtlinienverwaltung Cesamtstruktur: docusnap.intern Ce	Firewall Exception Bereich Details Einstellungen Delegie	erung		
a 🚔 docusnap.intern	Verknüpfungen			
Activate Gruppenrichtlinienobj	ekt hier erstellen und verknüpfen	o.intem		
Default Vorhandenes Gruppen	richtlinienobjekt verknüpfen	hisationseinheiten sind r	nit dem Objekt verknüpft:	
DS-Scrip Vererbung deaktivierer Firewall	n	Erzwungen	Verknüpfung aktiviert	Pfad
RDP - AI Gruppenrichtlinienmo	dellierungs-Assistent	Nein	Ja	docusnap.intem
Window Neue Organisationseir S COUNT Suchen S docusne Domäinencontroller än S Domain Entfernen S ForestGr Active Directory-Benut S Loop Microso S Microso Aktualisieren S RES_DO Eigenschaften	iheit idern tzer und -Computer nen			
 B service - FestOÜ Hilfe F Gruppenrichtlinienobjekte 	Gruppen, Benutzer und Computer:	jekts gelten nur für die f	olgenden	
WMI-Filter	Name			
Starter-Gruppenrichtlinienobjekte Standorte	& Authentifizierte Benutzer			
Gruppenrichtlinienmodellierung				

Abbildung 2 - Gruppenrichtlinienobjekt hier erstellen und verknüpfen

Einen "sprechenden" Namen für das Gruppenrichtlinienobjekt festlegen.

E.		Gruppenrichtlinienverwaltung
🛃 Datei Aktion Ansicht Fenster	?	
🗢 🔿 🔲 🞑 🔀 🖬		
Gruppenrichtlinienverwaltung	Gruppenrichtlinienve	rwaltung
a 🚔 docusnap.intern	Name	^
Activate SecurityCen	A Gesamtstruktur: docusna	plintem
Default Domain Polic		
Neues (Gruppenrichtlinienobjekt	×
Name:		
Windows Firewall-Ausnah	men	
Quell-Starter-Gruppenrichtli	nienobjekt:	
(Kein)		~
	ОК	Abbrechen
▷ 1 Loop▷ 1 Microsoft Exchange \$		

Abbildung 3 - Neues Gruppenrichtlinienobjekt



3.4 Gruppenrichtlinienobjekt bearbeiten

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

<u>-</u>	Gruppenrichtlir	ienverwaltung		-
🔜 Datei Aktion Ansicht Fenster				
🗢 🔿 🙋 📰 🙆 👔				
Gruppenrichtlinienverwaltung A Gesamtstruktur: docusnap.inter A Bomänen	bcusnap.intern tatus Verknüpfte Gruppenrichtlinienobjekte Gru	ppenrichtlinienvererbung) Delegierung	
 docusnap.intern Activate SecurityCen Default Domain Polic DS-Script Firewall Exception 	Verk Gruppenrichtlinienobjekt 1 Default Domain Policy 2 Firewall Exception 3 DS-Script 4 RDP - Allow	Erzwungen Verku Nein Ja Nein Ja Nein Ja Nein Ja	nüpfung aktiviert Objek Aktivi Aktivi Alle E Aktiv	ttstatus WMI-Filter iert Keine iert Keine înstellung Docusnap iert Keine
RDP - Allow	5 🗊 Windy	Ja	Aktiv	iert Keine
 Windows Firewall-At COUNTRIES docusnap docusnap internation Domain Controllers EXPORT EXPORT ForestGroups IMPORT Loop Microsoft Exchange ! RES_DOM Service_accounts TestOÜ Gruppenrichtlinienol Starter-Gruppenricht Standorte Gruppenrichtlinienmodelliei Gruppenrichtlinienmodelliei Gruppenrichtlinienmodelliei 	6 Activa Beateren Firzwungen Verknüpfung ak Bericht speicher Löschen Umbenennen Aktualisieren	Ja tiviert	Aktivi	ert Keine
< >				

Abbildung 4 - Gruppenrichtlinienobjekt bearbeiten



Der Gruppenrichtlinienobjekt-Editor öffnet sich:



Abbildung 5 - Gruppenrichtlinienobjekt-Editor

Die zu konfigurierenden Gruppenrichtlinien befinden sich unter:

- > Computerkonfiguration
 - ➢ Richtlinien
 - Administrative Vorlagen
 - > Netzwerk
 - Netzwerkverbindungen
 - Windows-Firewall
 - o Domänenprofil



3.5 Ausnahme für Datei- und Druckerfreigabe aktivieren

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

🛃 Windows-Firewall: Eingehende	e Ausnahme	e für Datei- und Druckerfreigabe zulassen 🛛 – 🗖 📕	X						
📷 Windows-Firewall: Eingehende Ausnal	Windows-Firewall: Eingehende Ausnahme für Datei- und Druckerfreigabe zulassen								
Vorherige Einstellung Nächste Einste	llung								
O Nicht konfiguriert Kommentar:			^						
 Aktiviert 									
 Deaktiviert 			Υ.						
Unterstützt auf:	Mindestens	Windows XP Professional mit SP 2	^						
			\vee						
Optionen:		Hilfe:							
			_						
Unerbetene eingehende Meldungen von d Adressen zulassen:	iesen IP- ^	Ermöglicht die Datei- und Druckerfreigabe. Windows-Firewall öffnet hierzu UDP-Port 137 und 138 und TCP-Port 139 und 445.	^						
localsubnet Syntax:		Durch Aktivieren dieser Richtlinieneinstellung öffnet Windows- Firewall diese Ports, sodass der Computer Druckaufträge und Zugriffsanforderungen für freigegebene Dateien empfangen							
Geben Sie "*" ein, um Meldungen von aller Netzwerken zuzulassen	n	kann. Sie mussen die IP-Adressen oder Subnetze angeben, für die diese eingehenden Meldungen zulässig sind. In der Windows-	2						
oder geben Sie eine durch Komma getrenn ein die eine	te Liste	Kontrollkästchen "Datei- und Druckerfreigabe" aktiviert und Administratoren können es nicht deaktivieren.							
beliebige Anzahl oder Kombination folgen Elemente enthält:	der	Wenn Sie diese Richtlinieneinstellung deaktivieren, blockiert Windows-Firewall diese Ports, sodass der Computer keine							
IP-Adressen wie 10.0.0.1		Dateien und Drucker treigeben kann. Fails ein Administrator versucht, einen dieser Ports zu öffnen, indem der Port der lokalen Portausnahmeliste binzufügt wird öffnet Windows-Firewall	1						
Subnetzbeschreibungen wie 10.2.3.0/24	~	diesen Port nicht. In diesem Fall wird das Kontrollkästchen							
<	>		~						
		OK Abbrechen Übernehme	an						

Abbildung 6 - Ausnahme für Datei- und Druckerfreigaben aktivieren und Bereich einschränken



3.6 Remoteverwaltungsausnahme aktivieren

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

Se Windows-Firewall:	Eingehend	e Remoteverwaltungsausnahme zulassen 🛛 – 🗖 📕	×
📷 Windows-Firewall: Eingehende Remote	everwaltungsa	ausnahme zulassen	
Vorherige Einstellung Nächste Einste	llung		
 Nicht konfiguriert Aktiviert Deaktiviert Unterstützt auf: 	Mindenters		^ ~
Optionen:	Mindestens	Hilfe:	<u> </u>
Unerbetene eingehende Meldungen von d Adressen zulassen: Iocalsubnet Syntax: Geben Sie "*" ein, um Meldungen von aller Netzwerken zuzulassen, oder geben Sie eine durch Komma getrenn ein, die eine beliebige Anzahl oder Kombination folgen Elemente enthält: IP-Adressen wie 10.0.0.1 Subnetzbeschreibungen wie 10.2.3.0/24	iesen IP- ^	Ermöglicht die Remoteverwaltung des Computers mit Verwaltungsprogrammen, wie z. B. Microsoft Management Console (MMC) und Windows-Verwaltungsinstrumentation (WMI). Windows-Firewall öffnet hierzu TCP-Port 135 und 445. Dienste verwenden diese Ports normalerweise für die Kommunikation mithilfe von Remoteprozeduraufrufen (RPC) und DCOM (Distributed Component Object Model). Darüber hinaus ermöglicht diese Richtlinieneinstellung unter Windows XP Professional mit mindestens SP2 und Windows Server 2003 mit mindestens SP1 den Programmen SVCHOST.EXE und LSASS.EXE unerbetene eingehende Meldungen zu empfangen und ermöglicht gehosteten Diensten, zusätzliche dynamisch zugewiesene Ports zu öffnen, normalerweise im Bereich 1024 bis 1034. Unter Windows Vista können mit dieser Richtlinieneinstellung nicht die Verbindungen mit SVCHOST.EXE und LSASS.EXE kontrolliert werden. Wenn Sie diese Richtlinieneinstellung aktivieren, gestattet Windows-Firewall dem Computer, unerbetene eingehende	~
		OK Abbrechen Übernehme	en

Abbildung 7 - Remoteverwaltungsausnahme aktivieren und Bereich einschränken



3.7 Gruppenrichtlinienobjekt bearbeiten – weitere Möglichkeiten

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

<u></u>		Gruppenri	chtlinienverwaltu	ing		
📓 Datei Aktion Ansicht Fenster	?					
🗢 🔿 🙋 📆 🙆 📔 🖬						
Gruppenrichtlinienverwaltung	docusna Status V	Nap.intern Verknüpfte Gruppenrichtlinienobjekte Verk Gruppenrichtlinienobjekt	Gruppenrichtlinienve	rerbung Delegierung	Objektstatus	WMI-Filter
Activate SecurityCen Default Domain Polic DS-Script Firewall Exception		1 Default Domain Policy 2 Firewall Exception 3 DS-Script 4 RDP - Allow	Nein Nein Nein Nein	Ja Ja Ja Ja	Aktiviert Aktiviert Alle Einstellung Aktiviert	Keine Keine Docusnap Keine
 RDP - Allow Windows Firewall-At COUNTRIES docusnap docusnap internation Domain Controllers EXPORT ForestGroups IMPORT Loop Microsoft Exchange ! RES_DOM service_accounts TestOÜ Gruppenrichtlinienol Standorte Gruppenrichtlinienmodelliei Gruppenrichtlinienmodelliei Gruppenrichtlinienmodelliei 	₹	5 Rearbeiter 6 Active Bearbeiter Verknüpfu Bericht sp Löschen Umbenen Aktualisier	ng aktiviert eichern nen en	Ja	Aktiviert Aktiviert	Keine Keine
< >						

Abbildung 8 - Gruppenrichtlinienobjekt bearbeiten



Der Gruppenrichtlinienobjekt-Editor wird geöffnet:

9	Group Policy Ma	anagement Editor						- 🗆 X
File Action View Help								
🗢 🌩 🖄 🔜 🗟 🖬								
Windows Firewall [DSDC01.DSRA.LOCAL] Policy	Name	Group	Profile	Enabled	Action	Override	Program	Local Address
Computer Configuration		There are no item	is to show in	this view.				
⊿ Policies								
Software Settings								
Windows Settings								
Scripts (Startun/Shutdown)								
A Security Settings								
Account Policies								
Local Policies								
Event Log								
Restricted Groups								
System Services								
Registry								
File System								
Wired Network (IEEE 802.3) Policies								
Windows Firewall with Advanced Security								
Windows Firewall with Advanced Security								
New Rule								
Conne Filter by Profile b								
Network list out out								
Viceless Network								
Public Key Po								
▷ Software Rest								
Network Acce Refresh								
Application C Export List								
Advanced Aux Help								
Advanced Ad Thep	1							
Administrative Templates: Policy definitions (ADMX)	f							
Preferences								
⊿ 🐁 User Configuration								
Policies								
Preferences								
< III >								
New Rule								

Abbildung 9 - Gruppenrichtlinienobjekt-Editor

Die zu konfigurierenden Firewall Einstellungen befinden sich unter:

- ➢ Computerkonfiguration
 - ➢ Richtlinien
 - Windows Einstellungen
 - Sicherheitseinstellungen
 - > Windows Firewall mit erweiterter Sicherheit
 - > Windows Firewall mit erweiterter Sicherheit
 - o Eingehende Regeln
 - Neue Regel



3.7.1 Datei- und Druckerfreigabe aktivieren - Ping

Nach der Auswahl "Neue Regel" wird der Firewall Assistent gestartet. Wählen Sie hier den vordefinierten Regelsatz:

- "Datei- und Druckerfreigabe"



Abbildung 10 - Auswahl des vordefinierten Regelsatz Datei- und Druckerfreigabe



Im nächsten Schritt wird ausgewählt, welche Aktionen im Bereich der Datei- und Druckerfreigabe aktiviert werden sollen. Hier werden folgende Regeln aktiviert:

- Datei- und Druckerfreigabe (ICMP Echoanforderung ICMPv6-In) und
- Datei- und Druckerfreigabe (ICMP Echoanforderung ICMPv4-In)

J		Group Policy Management Editor						_ 🗆 X
File Action View Help								
🔶 🄿 🙍 🖬 🗟 🖬								
Windows Firewall [DSDC01.DSRA.LOC	AL] Policy	Name Group	Profile	Enabled	Action	Override	Program	Local Address
4 👰 Computer Configuration		There are a	no itoms to show i	n this view				
⊿ 🧮 Policies		There are i	no items to show i	in unis view.				
Software Settings	*	New Inbound Rule Wizard			x			
Windows Settings	Predefined Rules							
Scripts (Startun/Shutde								
A Security Settings	Select the rules to be creat	ted for this experience.						
Account Policies	Steps:							
Local Policies		Which rules would you like to create?						
👂 📠 Event Log	Hule Type							
Restricted Groups	Predefined Rules	The following rules define network connectivity requirements for t	he selected predefin	ed group.				
System Services	Action	the existing rule will be overwritten.	a is checked, the co	riterits of				
Registry								
File System		Rules:						
4 🦳 Windows Eirewall w		Name	Rule Exists	Profile				
A P Windows Firewa		File and Printer Sharing (LLMNR-UDP-In)	No	All				
📰 Inbound Rul		File and Printer Sharing (Echo Request - ICMPv6-In)	No	AI				
Cutbound R		✓ File and Printer Sharing (Echo Request - ICMPv4-In)	No	All				
🌆 Connection		File and Printer Sharing (Spooler Service - RPC-EPMAP)	No	All				
🧮 Network List Manac		File and Printer Sharing (Spooler Service - NPC)	No	All				
Wireless Network (I		File and Printer Sharing (NB-Name-In)	No	AI				
Public Key Policies		File and Printer Sharing (SMB-In)	No	AI				
Software Restriction		File and Printer Sharing (NB-Session-In)	No	All				
Network Access Pro Application Control								
Application Control		< 111		>				
Advanced Audit Policies								
Policy-based QoS								
Administrative Templates:								
Preferences								
a 兆 User Configuration					_			
Policies		< Back	Next >	Cancel				
Preferences								
<	>							

Abbildung 11 - Aktivierung der Regel zur Freigabe von ICMP-Echoanforderungen



Der nächste Schritt besteht darin die Option "Verbindung zulassen" auszuwählen, welche im Standard bereits aktiviert ist.



Abbildung 12 - Abschluss der Regelaktivierung - Verbindung zulassen



3.7.2 Windows Verwaltungsinstrumentation (WMI) aktivieren

Neben der Aktivierung der Datei- und Druckerfreigabe - speziell der Ping-Befehl, wird auch die Freischaltung für eingehende WMI-Abfragen benötigt. Hierfür starten Sie wieder den Firewall Assistenten und wählen folgenden vordefinierten Regelsatz aus:

- "Vordefiniert" - "Windows Verwaltungsinstrumentation (WMI)"



Abbildung 13 - Auswahl des vordefinierten Regelsatz Windows Verwaltungsinstrumentation



Im nächsten Schritt aktivieren Sie die Regel

- Windows Verwaltungsinstrumentation (WMI-In)

Die weiteren Regeln werden nicht benötigt. Die übrigen Schritte zur Aktivierung der Regel sind analog der vorherigen Regel durchzuführen:

- Verbindung zulassen

J			Group Policy Management Ec	litor					_ 0	x
File Action View Help										
🗢 🔿 🙍 🗔 🗟 🖬										
I Windows Firewall [DSDC01.DSRA.LOC	AL1 Policy	Name	6	iroun	Prof	le Enabled	Action	Override	Program	Local
🖌 🖉 Computer Configuration	@		New Inbound Rule Wizard			×	Allow	No	Any	Any
⊿ Policies	Predefined Rules						Allow	No	Any	Any
Windows Settings	Select the piles to be one	ad for this av								
Name Resolution Policy	Select the fulles to be crea	Select the rules to be created for this experience.								
Scripts (Startup/Shutdo	Steps:									
⊿ Security Settings	Rule Type		Which rules would you like to create?							
Account Policies	Predefined Rules		The following rules define network connectivity require	ements for the sel	ected predefined arour	,				
b 🖬 Event Log	Action		Rules that are checked will be created. If a rule alread	by exists and is ch	ecked, the contents of					
Restricted Groups			the existing rule will be overwritten.							
Image: System Services			Rules:							
▶ Karing Parameters			Name	Rule Exists	Profile	De				
File System Wired Network (IEEE			Windows Management Instrumentation (ASync-Ir	n) No	All	Int				
⊿ G Windows Firewall w			Windows Management Instrumentation (WMI-In)	No	All	Int				
a 🔐 Windows Firewa			Windows Management Instrumentation (DCOM-Ir	n) No	All	Int				
式 Inbound Rule										
Connection 1										
Network List Manag										
↓ Wireless Network (IE)										
Public Key Policies										
Software Restriction			<			>				
Network Access Pro Network Access Pro Application Control										
Application Control B R JP Security Policies of										
Advanced Audit Pol										
Policy-based QoS										
Administrative Templates: I				< Back	Next > Ca	ncel				
Preferences				, but						
Policies		-								
Preferences										
	>	×								

Abbildung 14 - Aktivierung der Regel zur Freigabe eingehenden WMI Abfragen



	Group Policy Management	Editor					_ □	x
File Action View Help								
🗢 🏟 🔁 🖬 🔒 🛛 🖬								
Windows Firewall [DSDC01.DSRA.LOCAL] Policy	Name	Group	Profile	Enabled	Action	Override	Program	Local
🔺 👰 Computer Configuration	🕑 Windows Management Instrumentation (WMI-In)	Windows Management Instr	All	Yes	Allow	No	%System	Any
⊿ 🛗 Policies	🕑 File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	Yes	Allow	No	Any	Any
Software Settings	File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	Yes	Allow	No	Any	Any
⊿ Windows Settings								
Name Resolution Policy								
Scripts (Startup/Shutdown)								
⊿ Security Settings								
Account Policies								
b a Event Lee								
Event Log								
System Services								
N Registry								
File System								
Wired Network (IEEE 802.3) Policies								
Windows Firewall with Advanced Security								
Windows Firewall with Advanced Security								
🗱 Inbound Rules								
🗱 Outbound Rules								
🌆 Connection Security Rules								
Network List Manager Policies								
Wireless Network (IEEE 802.11) Policies								
Public Key Policies								
Software Restriction Policies								
Network Access Protection								
Application Control Policies								
Advanced Audit Policy Configuration								
Advanced Addit Policy Configuration								
Administrative Templates: Policy definitions (ADMX f								
Preferences								
Super Configuration								
Policies								
Preferences								
< III >	<							>

Abbildung 15 - Abschluss der Firewall Konfiguration



4. Windows 10 - Windows Firewall Konfiguration (lokal)

Die Firewall Konfiguration kann direkt über den Befehl firewall.cpl aufgerufen werden.



• Suchen – Eingabe: firewall.cpl



Abbildung 16 - Windows 10 - Suche - Eingabe firewall.cpl

Alternativ kann der Befehl auch in einem Konsolenfenster ausgeführt werden:



Abbildung 17 - Windows 10 - Eingabeaufforderung firewall.cpl





4.1 Ausnahme festlegen

Eine App oder ein Feature durch die Windows-Firewall zulassen anklicken.

@	Wind	ows-Firewall	- 🗆 🗙
(→ ↑ → Systemsteuer	rung → Alle Systemsteuerungselemente → Windows	5-Firewall v C	Systemsteuerung durchsuchen 🔎
 Systemsteuerung Sinder Systemsteuerung Sinder Systemsteuerung Sinder Systemsteuerung Sinder Systemsteuerung Benachrichtigungs- einstellungen ändern Benachrichtigungs- einstellungen ändern Standard wiederherstellen Erweiterte Einstellungen Problembehandlung für 	 Alle Systemsteuerungselemente * Windows Den PC mithilfe der Windows-Firewall s Mithilfe der Windows-Firewall kann verhindert werde bzw. über ein Netzwerk Zugriff auf den PC erhalten. Zu Ihrer Sicherheit werden einige Einstellungen Firewalleinstellungen aktualisieren Die zum Schutz des Computers empfohlenen Einstellungen werden nicht von der Windows-Firewall verwendet. Was sind die empfohlenen Einstellungen? 	rirewall rirewall rirewall rirewall	Systemsteuerung aurchsuchen D
Netzwerk	Domänennetzwerke Netzwerke am Arbeitsplatz, die zu einer Domäne ge	Verbunden 🕥	
	Status der Windows-Firewall:	Aus	
	Eingehende Verbindungen:	Alle Verbindungen mit Apps blockieren, die nicht in der Liste zugelassener Apps vorhanden sind	
	Aktive Domänennetzwerke:	intern.local	
	Benachrichtigungsstatus:	Benachrichtigen, wenn eine neue App von der Windows-Firewall blockiert wird	
Siehe auch	Private Netzwerke	Nicht verbunden 🕑	
Wartungscenter	Gast oder öffentliche <u>N</u> etzwerke	Nicht verbunden 📀	
Netzwerk- und Freigabecenter		,	

Abbildung 18 - Windows 10 - Windows-Firewall - App oder Feature zulassen

 (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall → Zugelassene Apps v (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall → Zugelassene Apps v (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall → Zugelassene Apps v (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall → Zugelassene Apps v (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall → Zugelassene Apps v (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall → Zugelassene Apps v (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall zulassen (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall zulassen (→ ↑ → Systemsteuerung → Alle Systemsteuerung durchsuchen (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall zulassen (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall zulassen (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall zulassen (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall zulassen (→ ↑ → Systemsteuerung → Alle Systemsteuerungselemente → Windows-Firewall zulassen (→ ↑ → Systemsteuerung → Systemsteuerungselemente → Systemsteueru	
Kommunikation von Apps durch die Windows-Firewall zulassen Klicken Sie zum Hinzufügen, Ändern oder Entfernen zugelassener Apps und Ports auf "Einstellungen ändern". Welche Risiken bestehen, wenn die Kommunikation einer App zugelassen wird?	P
Kommunikation von Apps durch die Windows-Firewall zulassen Klicken Sie zum Hinzufügen, Ändern oder Entfernen zugelassener Apps und Ports auf "Einstellungen ändern". Welche Risiken bestehen, wenn die Kommunikation einer App zugelassen wird?	
Klicken Sie zum Hinzufügen, Ändern oder Entfernen zugelassener Apps und Ports auf "Einstellungen ändern". Welche Risiken bestehen, wenn die Kommunikation einer App zugelassen wird?	
Welche Risiken bestehen, wenn die Kommunikation einer App zugelassen wird?	
wird?	
■ Zu Ihrer Sicherheit werden einige Einstellungen vom Systemadministrator verwaltet.	
Zugelassene Apps und Features:	
Name Domäne Privat Öffentlich Gruppenrichtlinie ^	
Verwaltung virtueller TPM-Smartcards	
✓ Visual Studio 12 - Remotedebugger-Erken	
☑ Wi-Fi Direct-Netzwerkerkennung □ □ ☑ Nein	
Windows Media Player D Nein	
Windows Media Player-Netzwerkfreigabe	
Windows Media Player-Netzwerkfreigabe	
Windows-Firewallremoteverwaltung Nein	
Windows-Peer-zu-Peer-Zusammenarbeits	
Windows-Remoteverwaltung D Nein	
Windows-Remoteverwaltung (Kompatibili	
🗹 Windows-Verwaltungsinstrumentation (W 🗹 🗌 🗌 Nein	
Details Entfernen	
Ande <u>r</u> e App zuassen	
OK Abbrechen	
JA ADDIELTIEI	

Abbildung 19 - Windows 10 - Windows-Firewall Zugelassene Apps und Features



Einstellungen ändern schaltet, entsprechende Benutzerrechte vorausgesetzt, die Bearbeitung von Programmen und Features frei. Windows 10 kennt drei unterschiedliche Netzwerktypen (Domäne, Privat und Öffentlich). Die Firewall Ausnahmen werden separat für jeden Typ definiert. Für die verwendeten Netzwerktypen sind folgende Ausnahmen per Haken in der Liste *Zugelassene Apps und Features* zu setzen:

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

Die neuen Einstellungen werden über die Schaltfläche *OK* übernommen. Diese Firewall Einstellungen ermöglichen Docusnap den Rechner zu scannen.



ABBILDUNGSVERZEICHNIS

ABBILDUNG 1 - GRUPPENRICHTLINIENVERWALTUNG	7
ABBILDUNG 2 - GRUPPENRICHTLINIENOBJEKT HIER ERSTELLEN UND VERKNÜPFEN	8
ABBILDUNG 3 - NEUES GRUPPENRICHTLINIENOBJEKT	8
ABBILDUNG 4 - GRUPPENRICHTLINIENOBJEKT BEARBEITEN	9
ABBILDUNG 5 - GRUPPENRICHTLINIENOBJEKT-EDITOR	10
ABBILDUNG 6 - AUSNAHME FÜR DATEI- UND DRUCKERFREIGABEN AKTIVIEREN UND BEREICH EINSCHRÄNKEN	11
ABBILDUNG 7 - REMOTEVERWALTUNGSAUSNAHME AKTIVIEREN UND BEREICH EINSCHRÄNKEN	12
ABBILDUNG 8 - GRUPPENRICHTLINIENOBJEKT BEARBEITEN	13
ABBILDUNG 9 - GRUPPENRICHTLINIENOBJEKT-EDITOR	14
ABBILDUNG 10 - AUSWAHL DES VORDEFINIERTEN REGELSATZ DATEI- UND DRUCKERFREIGABE	15
ABBILDUNG 11 - AKTIVIERUNG DER REGEL ZUR FREIGABE VON ICMP-ECHOANFORDERUNGEN	16
ABBILDUNG 12 - ABSCHLUSS DER REGELAKTIVIERUNG - VERBINDUNG ZULASSEN	17
ABBILDUNG 13 - AUSWAHL DES VORDEFINIERTEN REGELSATZ WINDOWS VERWALTUNGSINSTRUMENTATION	18
ABBILDUNG 14 - AKTIVIERUNG DER REGEL ZUR FREIGABE EINGEHENDEN WMI ABFRAGEN	19
ABBILDUNG 15 - ABSCHLUSS DER FIREWALL KONFIGURATION	20
ABBILDUNG 16 - WINDOWS 10 - SUCHE - EINGABE FIREWALL.CPL	21
ABBILDUNG 17 - WINDOWS 10 - EINGABEAUFFORDERUNG FIREWALL.CPL	21
ABBILDUNG 18 - WINDOWS 10 - WINDOWS-FIREWALL - APP ODER FEATURE ZULASSEN	23
ABBILDUNG 19 - WINDOWS 10 – WINDOWS-FIREWALL ZUGELASSENE APPS UND FEATURES	23

VERSIONSHISTORIE

Datum	Beschreibung
03.01.2017	Erstellung des How-Tos
24.10.2018	Screenshots und Inhalt auf Windows 10 aktualisiert



support@docusnap.com | www.docusnap.com/support © itelio GmbH - www.itelio.com