

Windows Firewall Exceptions

Configuring Windows Firewall Exceptions for Docusnap

TITLE	Windows Firewall Exceptions
AUTHOR	Docusnap Consulting
DATE	21/04/2015

The reproduction and distribution of this document as a whole or in part as well as the utilization and disclosure of its contents to third parties without the express authorization by itelio GmbH are prohibited. Offenders will be held liable for the payment of indemnification. All rights reserved.

TABLE OF CONTENTS

1. INTRODUCTION	4
2. BASICS	5
2.1 REQUIRED FIREWALL EXCEPTIONS	5
3. WINDOWS FIREWALL CONFIGURATION – ACTIVE DIRECTORY	6
3.1 MANAGEMENT CONSOLE (GPMC)	6
3.2 STARTING GPMC	7
3.3 CREATING A GROUP POLICY OBJECT	8
3.4 EDITING A GROUP POLICY OBJECT	9
3.5 ENABLING EXCEPTIONS FOR FILE AND PRINTER SHARES	11
3.6 ENABLING A REMOTE ADMINISTRATION EXCEPTION	12
4. WINDOWS 8 - WINDOWS FIREWALL CONFIGURATION (LOCAL)	13
4.1 DEFINING EXCEPTIONS	14

1. INTRODUCTION

For the inventory of Windows systems, Docusnap uses the standard Windows Management Instrumentation (WMI) interface. If the Windows Firewall is enabled on a Windows system, it may be impossible for Docusnap to scan the system. This document explains the necessary adjustments of firewall settings for Windows systems.

The chapter named WINDOWS FIREWALL CONFIGURATION – ACTIVE DIRECTORY describes how the required Windows Firewall exceptions can be configured by defining corporate group policies using the Active Directory. This is the method recommended by itelio.

The chapter named WINDOWS 8 - WINDOWS FIREWALL CONFIGURATION (LOCAL) describes an example of how to configure *local* group policies for Windows 8. Adjusting the *local* group policies only makes sense in the context of workgroups or for testing purposes.

2. BASICS

To make sure that Windows systems with the firewall enabled can be scanned successfully by Docusnap, you need to check or configure two firewall exceptions. These settings can be set up and administered using group policies. To enable you to quickly check your environment, we will also describe how to manually configure your Windows firewall.

2.1 REQUIRED FIREWALL EXCEPTIONS

The following is a brief description of the exceptions to be configured.

File and Printer Sharing

Allows you to share files and printers. For this purpose, the Windows Firewall opens UDP ports 137 and 138 as well as TCP ports 139 and 445. Once you enable these policy settings, the Windows Firewall opens these ports so that the Windows system can receive print jobs and access requests for shared files.

<u>Note:</u> This setting lets inbound ICMP echo requests (messages sent by the Ping utility) pass through the Windows Firewall, even if the "Windows Firewall: Allow ICMP Exceptions" policy setting normally blocked them.

Allow Remote Administration Exception

Essentially corresponds to the Windows Management Instrumentation (WMI) Windows Firewall exception and enables remote administration of the Windows system using management programs such as Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). For this purpose, the Windows Firewall opens TCP ports 135 and 445. Services normally use these ports for RPC (Remote Procedure Call) and DCOM (Distributed Component Object Model) communication.

Security notice

We recommend that you distribute the setting by means of a group policy. This way, you can globally set allowed IP addresses or subnets for these exceptions.

3. WINDOWS FIREWALL CONFIGURATION – ACTIVE DIRECTORY

3.1 MANAGEMENT CONSOLE (GPMC)

To configure the firewall for multiple computers, it is advisable to define the required settings by means of a group policy.

The following example shows how to define a domain-wide setting using the Microsoft Group Policy Management Console (GPMC) tool. GPO settings can be made at the local (L), site (S), domain (D), and organisational unit (OU) levels. Subsequent settings always overwrite the previously defined values. The hierarchy is L, S, D, OU.

If the Microsoft Group Policy Management Console has not been installed on your system, you can download it for free from Microsoft. The following example shows how to change the firewall settings for all systems in the domain. It is strongly recommended to previously test this measure in a test environment or to implement the settings only in a dedicated test OU (*organisational unit*) in the Active Directory.

The remote server management tools including the GPMC can be downloaded from the Microsoft website for the Windows client operating systems.

For Windows 7: http://www.microsoft.com/de-de/download/details.aspx?id=7887

For Windows 8: http://www.microsoft.com/de-DE/download/details.aspx?id=28972

For Windows 8.1: http://www.microsoft.com/de-DE/download/details.aspx?id=39296

Windows server operating systems (2008 and higher) already include the GPMC, but it might be necessary to install it subsequently via the Server Manager.

For more information on the group policy management console and its options, please refer to: https://technet.microsoft.com/de-de/library/cc753298.aspx

3.2 STARTING GPMC

Open the Windows Run dialog (Windows key+R) and type *gpmc.msc*.

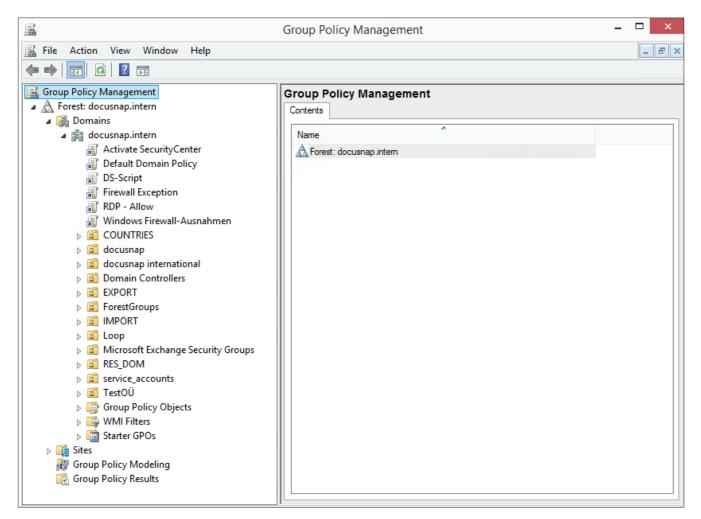


Fig. 1 – Group Policy Management

3.3 CREATING A GROUP POLICY OBJECT

Right-click the desired domain or OU and select the Create a GPO in this domain, and Link it here option.

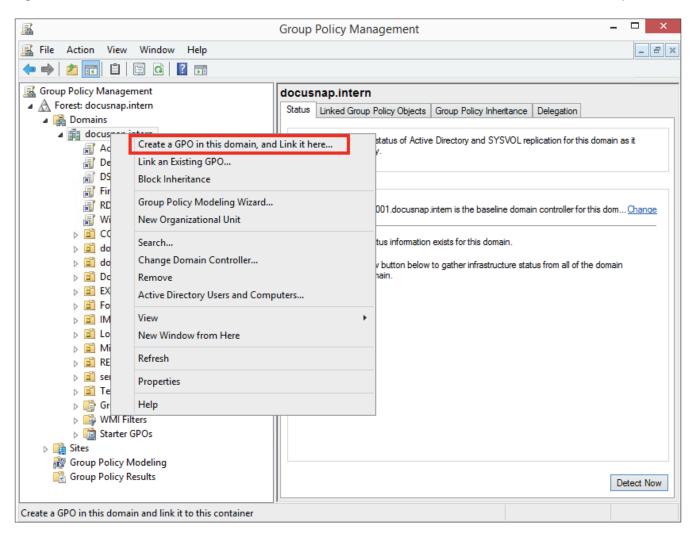


Fig. 2 – Create a GPO in this domain, and Link it here... option

Enter a descriptive name for the GPO.

Ne	ew GPO	
Name:		
Windows Firewall-Exceptions		
Source Starter GPO:		
Source Starter GPO: (none)		~
Source Starter GPO: (none)	ОК	∨ Cancel

Fig. 3 – New GPO dialog

3.4 EDITING A GROUP POLICY OBJECT

Right-click the previously created group policy object to select it and select Edit.

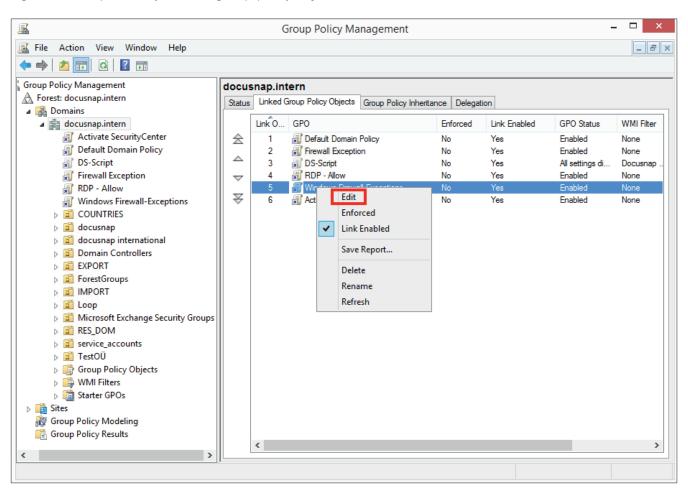


Fig. 4 – Editing a group policy object

The Group Policy Management Editor window opens:

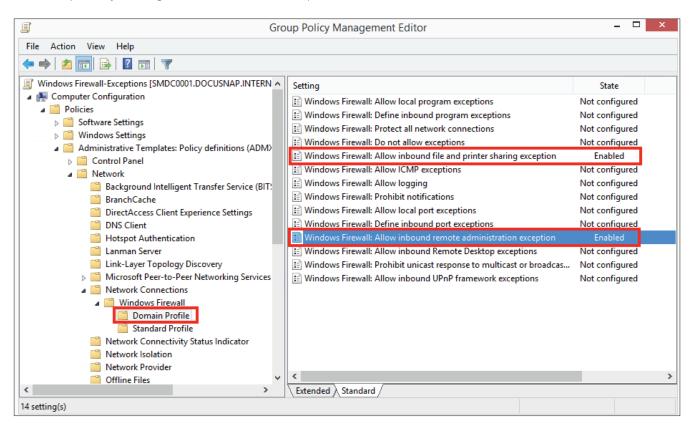


Fig. 5 – Group Policy Management Editor window

The group policies to be configured are located in the following path:

- Computer Configuration
 - > Policies
 - Administrative Templates
 - > Network
 - Network Connections
 - ➢ Windows Firewall
 - o Domain Profile

3.5 ENABLING EXCEPTIONS FOR FILE AND PRINTER SHARES

In this example, enabling the firewall exception is restricted to the local subnet.

Se Windows Firewa	all: Allow inb	ound file and printer sharing exception 🛛 – 🗖 🔜	×
🔚 Windows Firewall: Allow inbound file	and printer sha	ring exception Previous Setting Next Setting	
 Not Configured Comment: Enabled 			^
O Disabled Supported on:	At least Window	vs XP Professional with SP2	~
Options:		Help:	~
Allow unsolicited incoming messages from addresses:	m these IP 🔺	Allows inbound file and printer sharing. To do this, Windows Firewall opens UDP ports 137 and 138, and TCP ports 139 and 445.	^
Syntax: Type "*" to allow messages from any netw	york or	If you enable this policy setting, Windows Firewall opens these ports so that this computer can receive print jobs and requests for access to shared files. You must specify the IP addresses or	
else type a comma-separated list that contains any number or combination of these:		subnets from which these incoming messages are allowed. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is selected and administrators cannot clear it.	
IP addresses, such as 10.0.0.1 Subnet descriptions, such as 10.2.3.0/2	24	If you disable this policy setting, Windows Firewall blocks these ports, which prevents this computer from sharing files and printers. If an administrator attempts to open any of these ports	
The string "localsubnet" Example: to allow messages from 10.0.0.1	t,	by adding them to a local port exceptions list, Windows Firewall does not open the port. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is cleared and administrators cannot select it.	
10.0.0.2, and from any system on the	>	If you do not configure this policy setting, Windows Firewall	~
		OK Cancel Apply	

Fig. 6 – Enabling an exception for file and printer shares and restricting its scope

3.6 ENABLING A REMOTE ADMINISTRATION EXCEPTION

For this example, enabling the firewall exception is restricted to the local subnet.

🐖 Windows Firev	wall: Allow inbound remote administration exception 🛛 – 🗖	x
Windows Firewall: Allow inbound r	remote administration exception Previous Setting Next Setting	
O Not Configured Comment:		^
Enabled		
 Disabled 		× .
Supported on:	At least Windows XP Professional with SP2	^
		~
Options:	Help:	
Allow unsolicited incoming messages f addresses: Iocalsubnet Syntax: Type "*" to allow messages from any ne else type a comma-separated list that c any number or combination of these: IP addresses, such as 10.0.0.1 Subnet descriptions, such as 10.2.3.0 The string "localsubnet" Example: to allow messages from 10.0.1 10.0.0.2, and from any system on the <	etwork, or ontains 0/24 administrative tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object Model (DCOM). Additionally, on Windows XP Professional with at least SP2 and Windows Server 2003 with at least SP1, this policy setting also allows SVCHOST.EXE and LSASS.EXE to receive unsolicited incoming messages and allows hosted services to open additional dynamically-assigned ports, typically in the range of 1024 to 1034. On Windows Vista, this policy setting does not control connections to SVCHOST.EXE and LSASS.EXE. If you enable this policy setting, Windows Firewall allows the computer to receive the unsolicited incoming messages associated with remote administration. You must specify the IP	
	OK Cancel Apply	

Fig. 7 – Enabling a remote administration exception and restricting its scope

4. WINDOWS 8 - WINDOWS FIREWALL CONFIGURATION (LOCAL)

The firewall configuration can be opened directly by entering the *firewall.cpl* command.

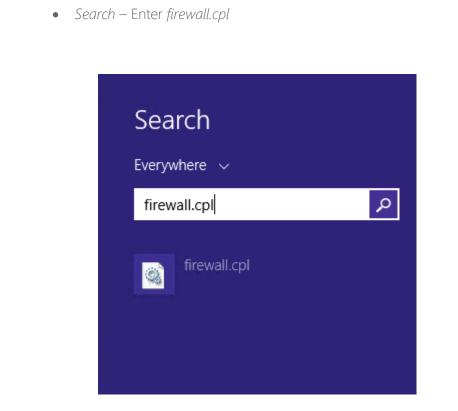


Fig. 8 - Windows 8 - Search - Enter firewall.cpl

Alternatively, you can enter the command from a console window:

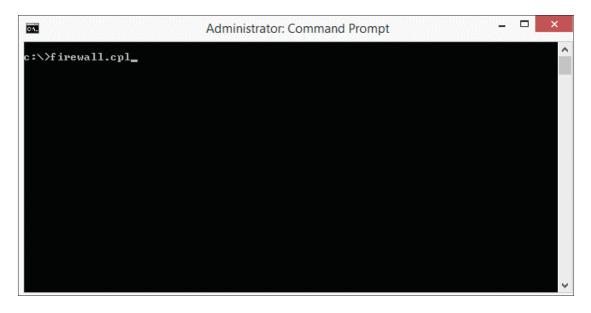


Fig. 9 - Windows 8 - command prompt for firewall.cpl

4.1 DEFINING EXCEPTIONS

Click Allow an app or feature through Windows Firewall.

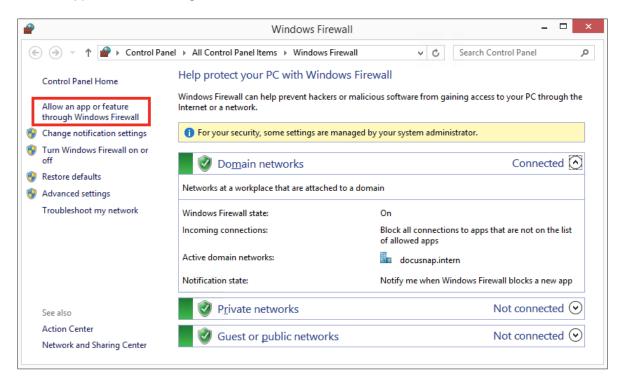


Fig. 10 - Windows 8 – Windows-Firewall - Allow an app or feature through Windows Firewall option

	Allowed	apps					_ 1	×
€ ⋺ - ↑		ed apps			/ 🖒 Searc	h Cor	ntrol Panel	Q,
	Allow apps to communicate through Window	us Eirouu	all					^
	To add, change, or remove allowed apps and ports, click C							
		nange sett	ings.					
	What are the risks of allowing an app to communicate?			(🕑 Change settin	ngs		
	For your security, some settings are managed by your	r system ac	Iministrato	or.]	- 1
	Allowed apps and features:							- 1
	Name	Domain	Private	Public	Group Policy	^		
	✓ @{microsoft.windowscommunicationsapps_17.5				No			
	☑ @{microsoft.windowscommunicationsapps_17.5	~	✓		No			
	☑ @{Microsoft.WindowsReadingList_6.3.9654.20349	~	~		No			
	Any Inbound	\checkmark	\checkmark	~	No			
	BranchCache - Content Retrieval (Uses HTTP)				No			
	BranchCache - Hosted Cache Client (Uses HTTPS)				No			
	BranchCache - Hosted Cache Server (Uses HTTPS)				No			
	BranchCache - Peer Discovery (Uses WSD)				No			
	Browser Choice	\checkmark	✓	~	No			
	CheckPoint.VPN	\checkmark	✓	~	No			
	Connect to a Network Projector				No			
	Core Networking	✓	✓	~	No	\checkmark		
				Details	Remov	e		. 1
				A	llow another app	p	_	~
				C	OK Car	ncel		

Fig. 11 – Windows 8 – Windows-Firewall: Allowed apps window

Click *Change settings* to edit the apps and features listed here. This is only possible if you have adequate rights. Windows 8 manages three different types of networks: Domain, Private, and Public. You need to define the firewall exceptions separately for each type. Define the following exceptions for the network types in use by setting the corresponding checkmarks in the *Allowed apps and features* list.

- File and Printer Sharing
- Windows Management Instrumentation (WMI)

Click the *OK* button to apply the new settings. The firewall settings thus defined allow Docusnap to scan the computer.

LIST OF FIGURES

IG. 1 – GROUP POLICY MANAGEMENT	7
IG. 2 – CREATE A GPO IN THIS DOMAIN, AND LINK IT HERE OPTION	8
-IG. 3 – NEW GPO DIALOG	8
-IG. 4 – EDITING A GROUP POLICY OBJECT	9
-IG. 5 – GROUP POLICY MANAGEMENT EDITOR WINDOW	.10
IG. 6 – ENABLING AN EXCEPTION FOR FILE AND PRINTER SHARES AND RESTRICTING ITS SCOPE	. 11
IG. 7 – ENABLING A REMOTE ADMINISTRATION EXCEPTION AND RESTRICTING ITS SCOPE	.12
- IG. 8 - WINDOWS 8 - SEARCH – ENTER FIREWALL.CPL	.13
FIG. 9 - WINDOWS 8 - COMMAND PROMPT FOR FIREWALL.CPL	.13
FIG. 10 - WINDOWS 8 – WINDOWS-FIREWALL - ALLOW AN APP OR FEATURE THROUGH WINDOWS FIREWA OPTION	
	14

