

# **Docusnap - Windows Firewall Exceptions**

Configuring Windows Firewall Exceptions for Docusnap



TITLE	Docusnap - Windows Firewall Exceptions
AUTHOR	Docusnap Consulting
DATE	11/3/2020
VERSION	1.2   valid from October 01, 2020

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 Docusnap GmbH. All rights reserved.



# CONTENTS

1. Introduction	4
2. Basics - 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 10 - Windows Firewall configuration (local)	13



### 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 Docusnap.

The chapter named WINDOWS 10 - WINDOWS FIREWALL CONFIGURATION (LOCAL) describes an example of how to configure local group policies for Windows 10. Adjusting the local group policies only makes sense in the context of workgroups or for testing purposes.



### 2. Basics - Required firewall exceptions

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.

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 organizational 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 (*organizational 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.

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



# 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	w GPO	
Name:		
Windows Firewall-Exceptions		
Source Starter GPO:		
Source Starter GPO: (none)		

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 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.

See Windows Firev	vall: Allow inb	ound file and printer sharing exception $ \square$ ×
📷 Windows Firewall: Allow inbound f	ile and printer sha	aring exception Previous Setting Next Setting
Not Configured     Comment:     Enabled		^
<ul> <li>Disabled</li> <li>Supported on:</li> </ul>	At least Windov	vs XP Professional with SP2
Options:		Help:
Allow unsolicited incoming messages for addresses:	rom 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 ne else type a comma-separated list that co	etwork, 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 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
any number or combination of these: IP addresses, such as 10.0.0.1		clear it. If you disable this policy setting, Windows Firewall blocks these
Subnet descriptions, such as 10.2.3.0 The string "localsubnet"	/24	ports, which prevents this computer from sharing files and printers. If an administrator attempts to open any of these ports by adding them to a local port exceptions list, Windows Firewall does not open the port. In the Windows Firewall component of
Example: to allow messages from 10.0.0 10.0.0.2, and from any system on the	).1, V	Control Panel, the "File and Printer Sharing" check box is cleared and administrators cannot select it.
	,	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 Fi	ewall: Allow inbound remote administration exception 🛛 – 🗖	X
📷 Windows Firewall: Allow inbou	d remote administration exception Previous Setting Next Setting	
O Not Configured Comment:		^
Enabled		
<ul> <li>Disabled</li> <li>Supported c</li> </ul>	At least Windows XP Professional with SP2	×
		~
Options:	Help:	
Allow unsolicited incoming messag addresses: Iocalsubnet Syntax: Type "*" to allow messages from an else type a comma-separated list th any number or combination of thes IP addresses, such as 10.0.0.1 Subnet descriptions, such as 10.2 The string "localsubnet" Example: to allow messages from 10 10.0.0.2, and from any system on the	Allows remote administration of this computer using administrative tools such as the Microsoft Management Cor (MMC) and Windows Management Instrumentation (WMI), do this, Windows Firewall opens TCP ports 135 and 445. Server typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object M (DCOM). Additionally, on Windows XP Professional with at I SP2 and Windows Server 2003 with at least SP1, this policy set also allows SVCHOST.EXE and LSASS.EXE to receive unsolicit incoming messages and allows hosted services to open additional dynamically-assigned ports, typically in the range 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 addresses or subnets from which these incoming messages allowed. If you disable or do not configure this policy setting, Window	nsole To rices odel east etting ed e of t are ws ↓

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



### 4. Windows 10 - Windows Firewall configuration (local)

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



Search – Enter firewall.cpl



Fig. 8 - Windows 10 - Search - Enter firewall.cpl

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







Click Allow an app or feature through Windows Firewall.

2	Windows Firewall	_ □
🔄 🌛 👻 🋧 🔗 > Control Pa	nel 🔸 All Control Panel Items 🔸 Windows Firewall	v 🖒 Search Control Panel 🔎
Control Panel Home	Help protect your PC with Windows F	Firewall
Allow an app or feature through Windows Firewall	Windows Firewall can help prevent hackers or ma Internet or a network.	alicious software from gaining access to your PC through the
Change notification settings	i For your security, some settings are manage	ed by your system administrator.
Turn Windows Firewall on or off	Do <u>m</u> ain networks	Connected 🕥
Restore defaults		
Advanced settings	Networks at a workplace that are attached to a c	domain
Troubleshoot my network	Windows Firewall state:	On
	Incoming connections:	Block all connections to apps that are not on the list of allowed apps
	Active domain networks:	docusnap.intern
	Notification state:	Notify me when Windows Firewall blocks a new app
See also	P <u>r</u> ivate networks	Not connected $\overline{oldsymbol{arphi}}$
Action Center	Guest or public networks	Not connected 📀
Network and Sharing Center		

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

	Anowed	apps					
€	All Control Panel Items > Windows Firewall > Allow	ed apps		~	C Searc	ch Control Panel	)
	All and a second second second by Miles day		-11				
	Allow apps to communicate through window	vs Firew	an				
	To add, change, of femove allowed apps and ports, click c	nange seu	ings.		<b>N</b> - 1	_	
	What are the risks of allowing an app to communicate?				🖉 Change settin	ngs	
	1 For your security, some settings are managed by you	r system ac	Iministrato	or.			
	Allowed apps and features:						
	Name	Domain	Private	Public	Group Policy	^	
	☑ @{microsoft.windowscommunicationsapps_17.5				No		
	@{microsoft.windowscommunicationsapps_17.5	<ul><li>✓</li></ul>	<ul><li>✓</li></ul>		No		
	@{Microsoft.WindowsReadingList_6.3.9654.20349	✓	✓		No		
	Any Inbound	$\checkmark$	<b>~</b>	✓	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	✓	<b>~</b>	✓	No		
	CheckPoint.VPN		<b>~</b>		No		
	Connect to a Network Projector				No		
	Core Networking	✓	✓	✓	No	~	
				Details	Remov	e	
				A	low another ap	p	
				0	K Car	ncel	

Fig. 11 - Windows 10 – 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 10 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

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



#### **VERSION HISTORY**

Date	Description
01/03/2017	HowTo Creation
10/24/2018	Screenshots updated and modified content to Windows 10

