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

CONTENTS

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.

Note: 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*.

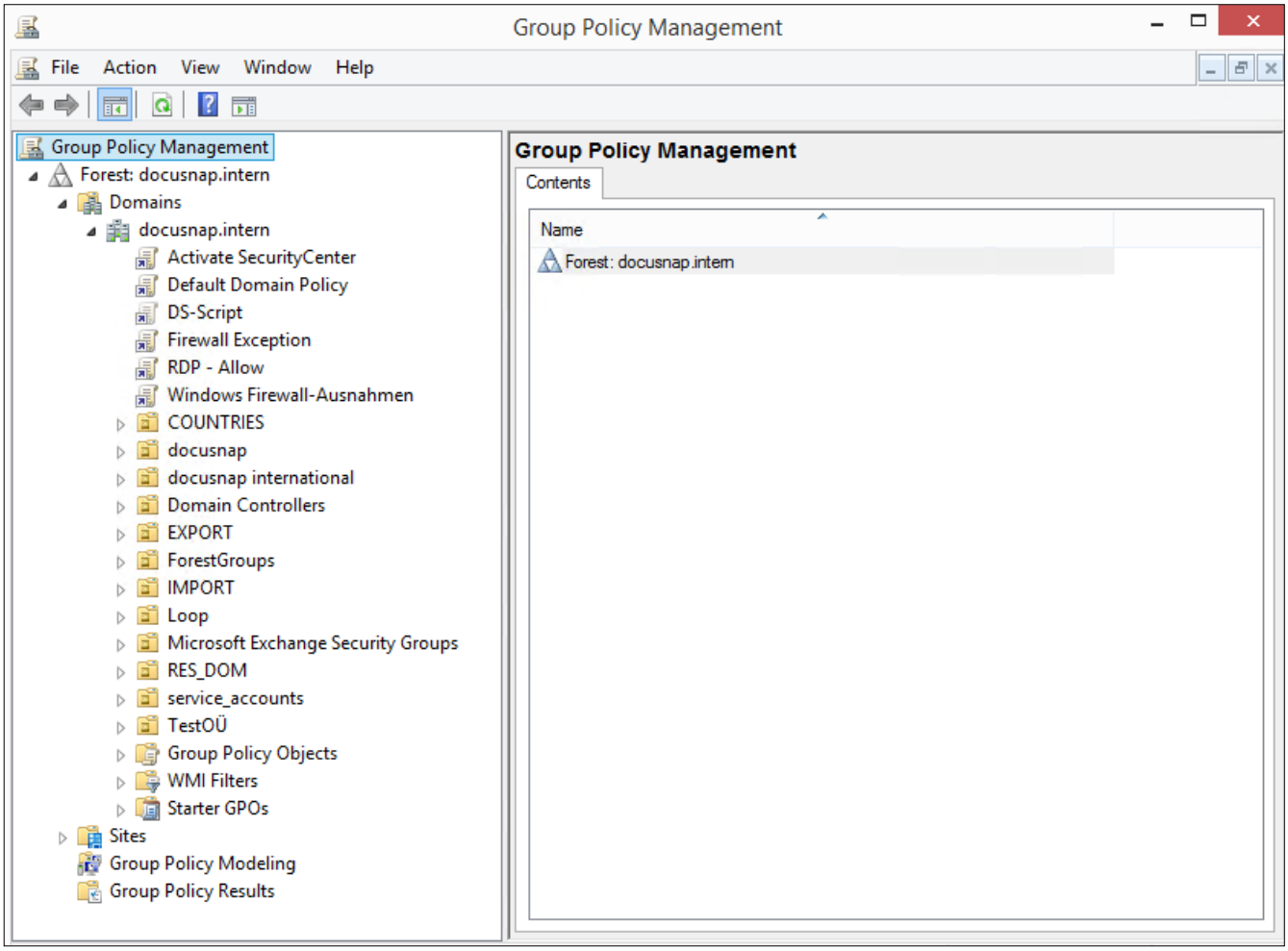

Fig. 1 - Group Policy Management

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.

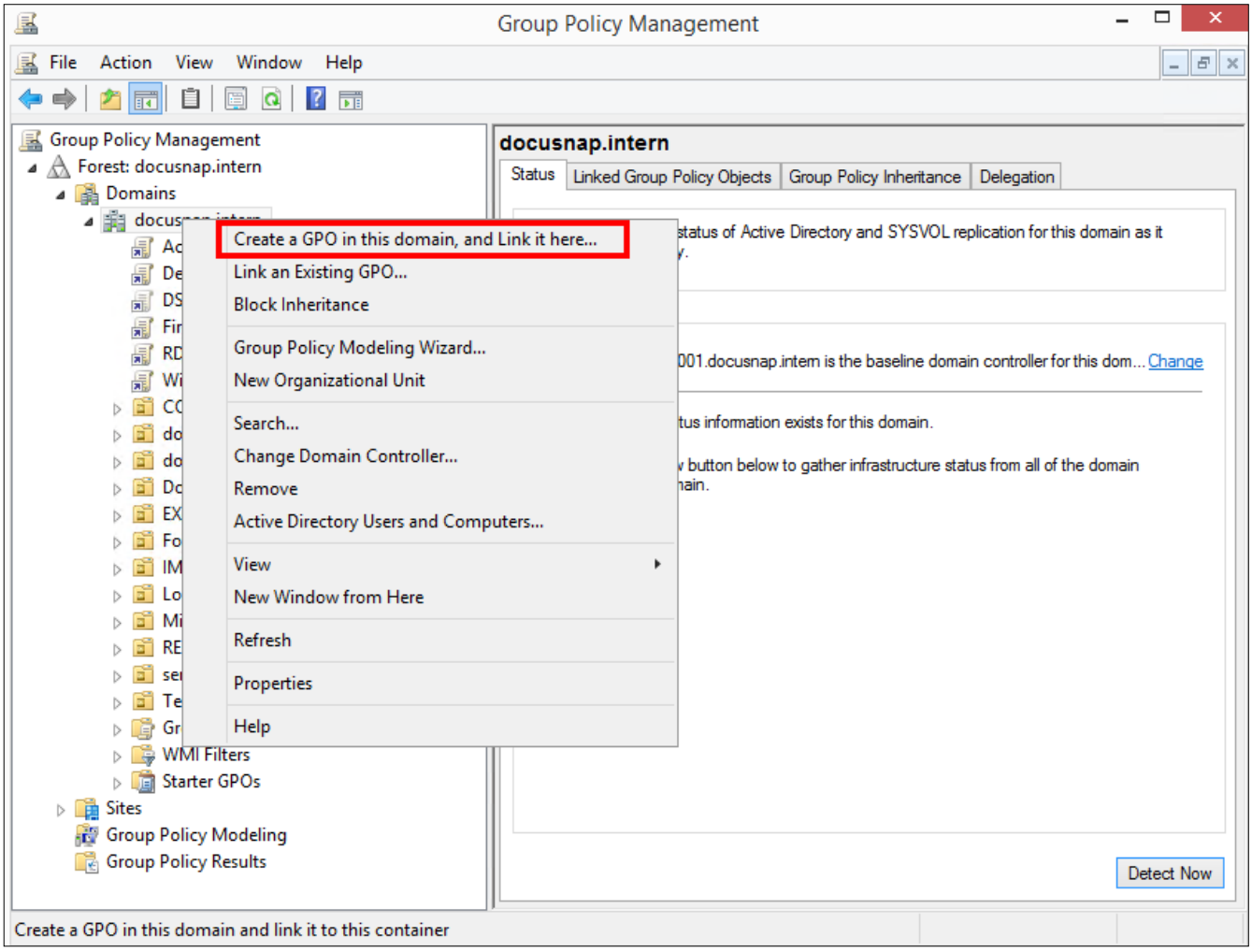

Fig. 2 - Create a GPO in this domain, and Link it here... option

Enter a descriptive name for the GPO.

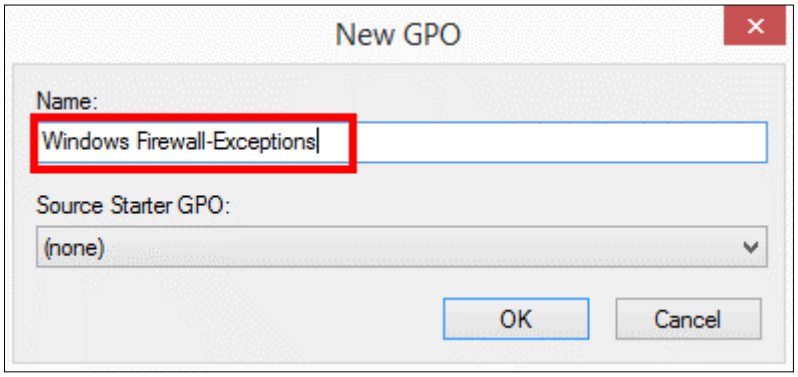

Fig. 3 - New GPO dialog

3.4 Editing a Group Policy Object

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

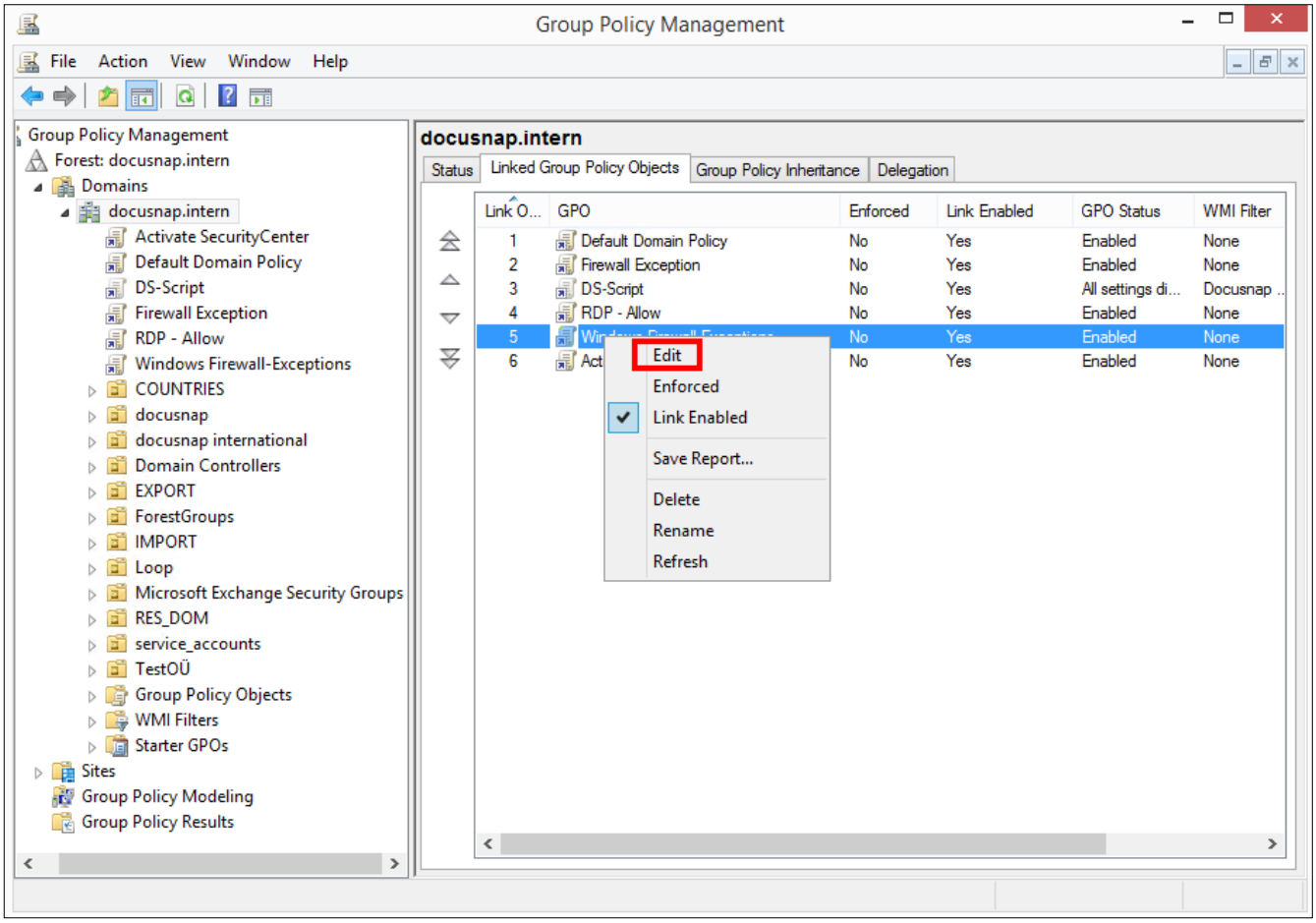

Fig. 4 - Editing a group policy object

The Group Policy Management Editor window opens:

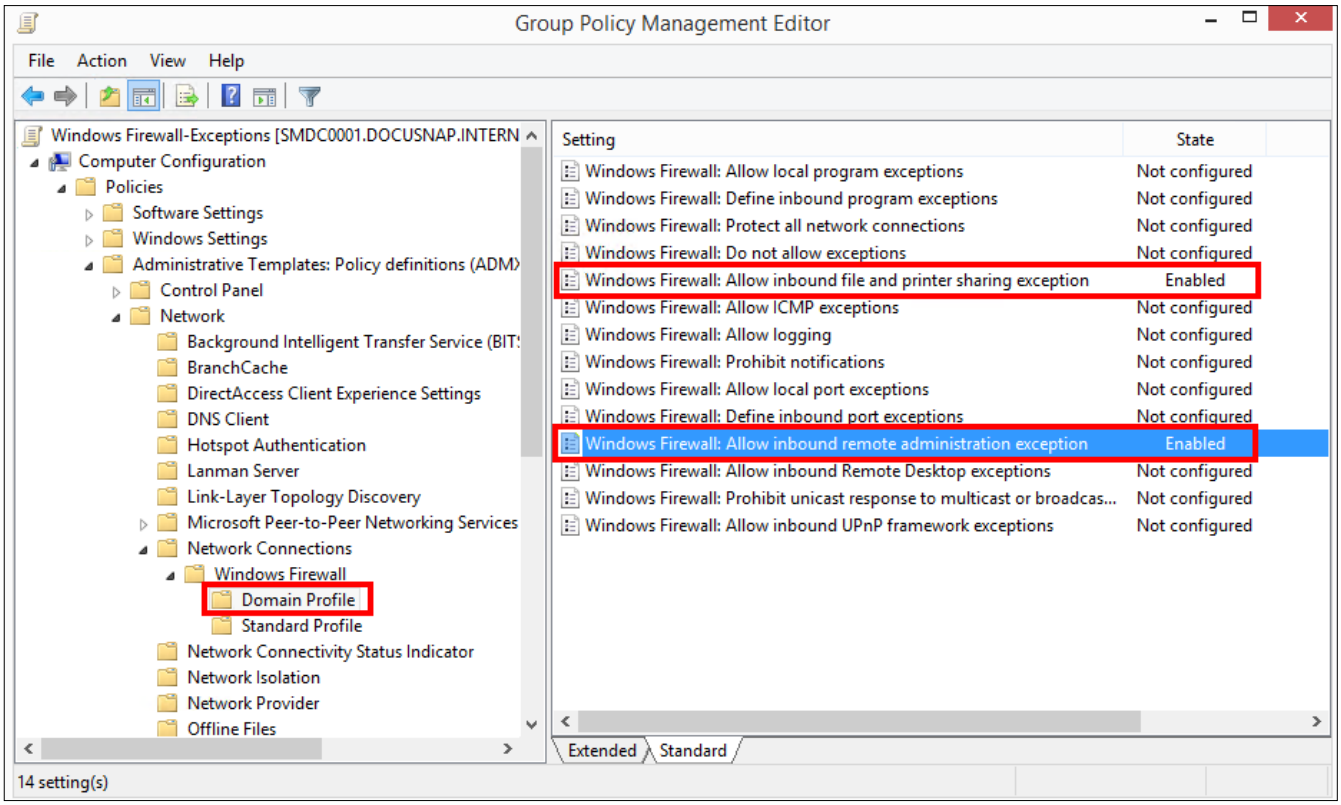

Fig. 5 - Group Policy Management Editor window

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

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

3.5 Enabling exceptions for file and printer shares

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

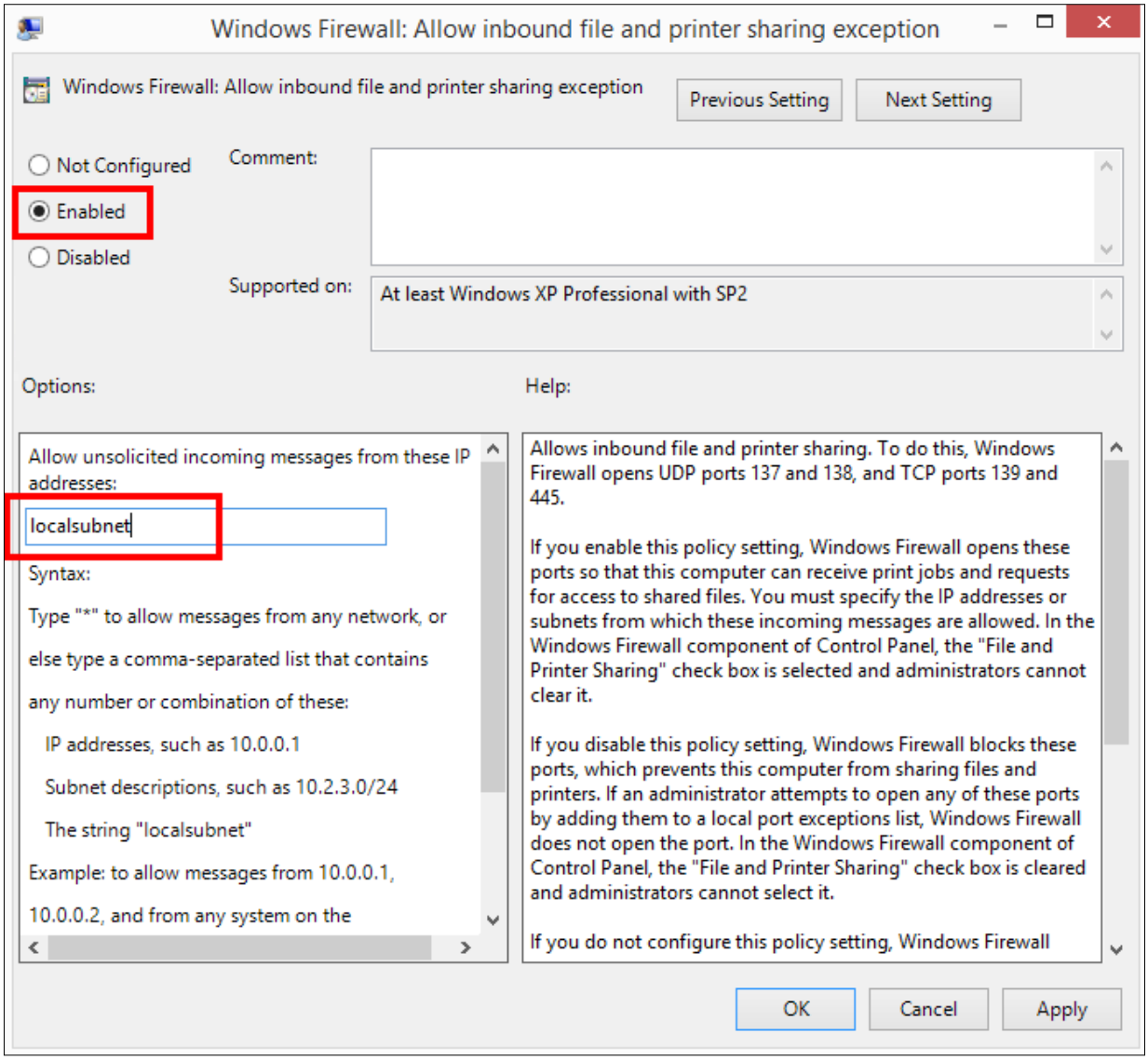

Fig. 6 - Enabling an exception for file and printer shares and restricting its scope

3.6 Enabling a remote administration exception

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

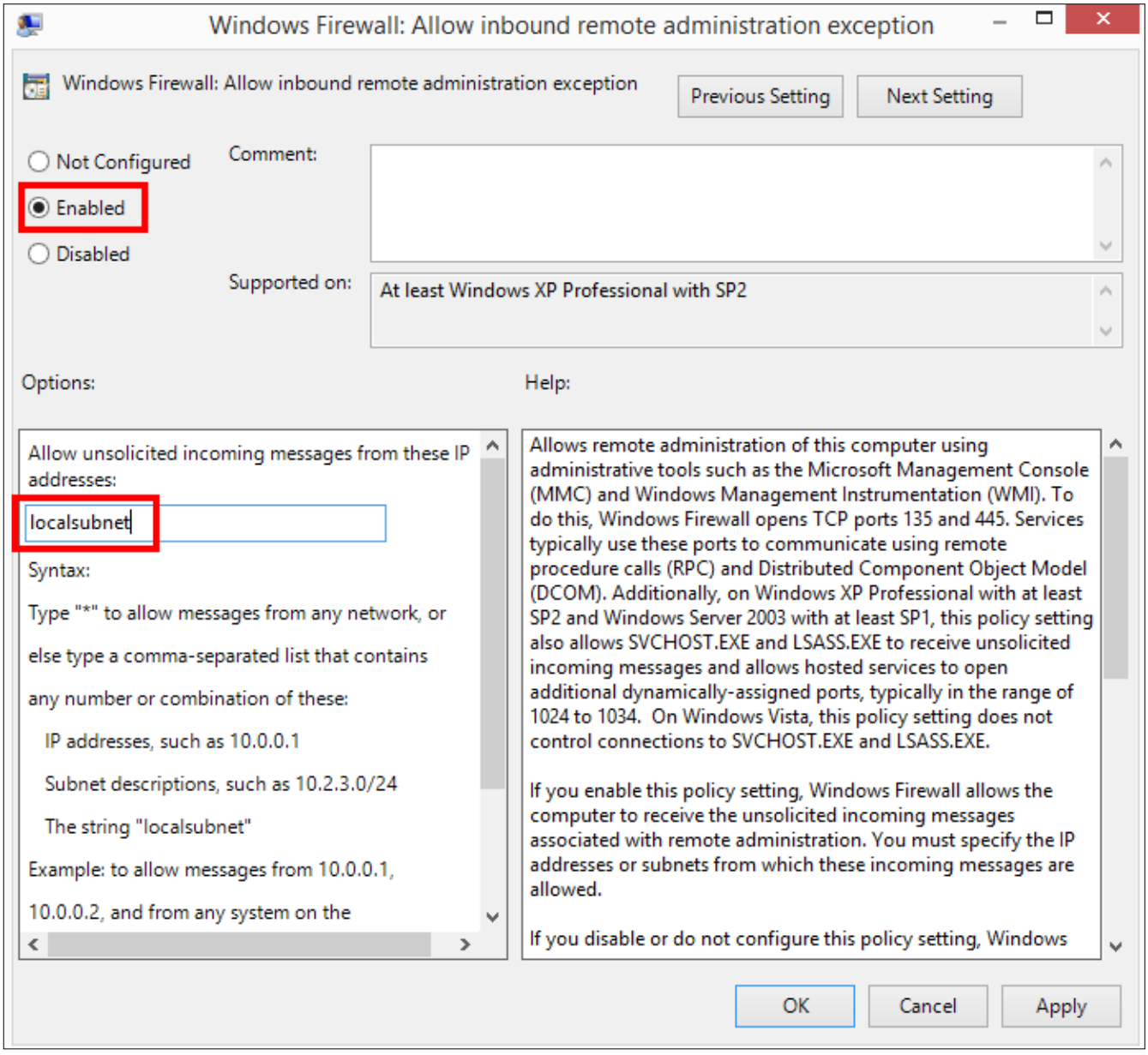

Fig. 7 - Enabling a remote administration exception and restricting its scope

4. Windows 10 - Windows Firewall configuration (local)

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

- *Search* – Enter **firewall.cpl**

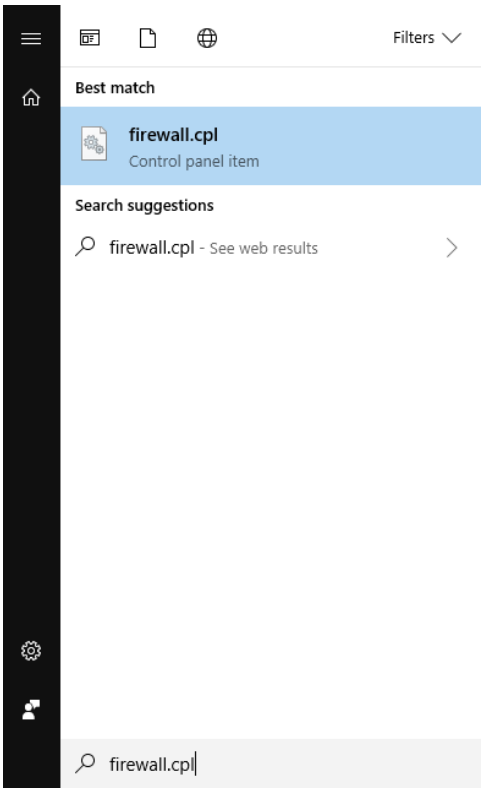

Fig. 8 - Windows 10 - Search – Enter firewall.cpl

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

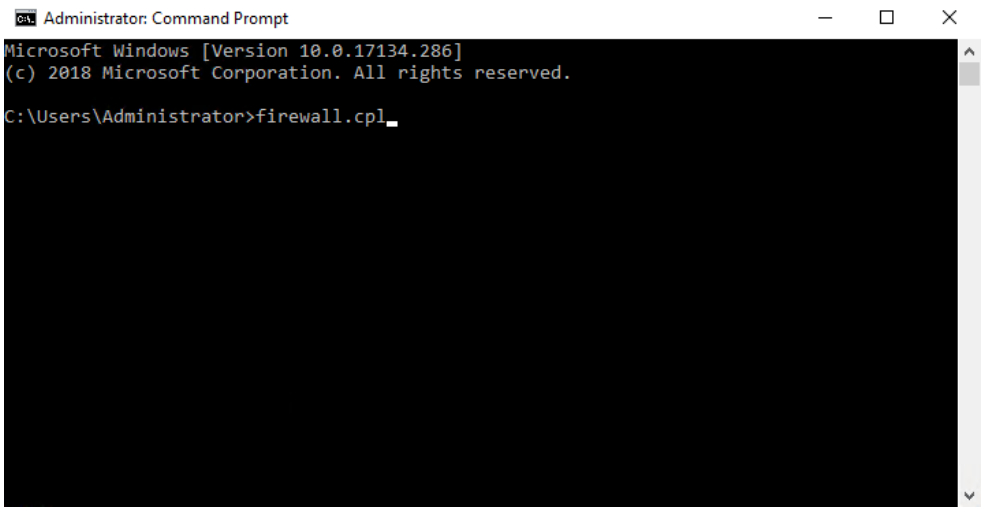

Fig. 9 - Windows 10 - command prompt for firewall.cpl

Click Allow an app or feature through Windows Firewall.

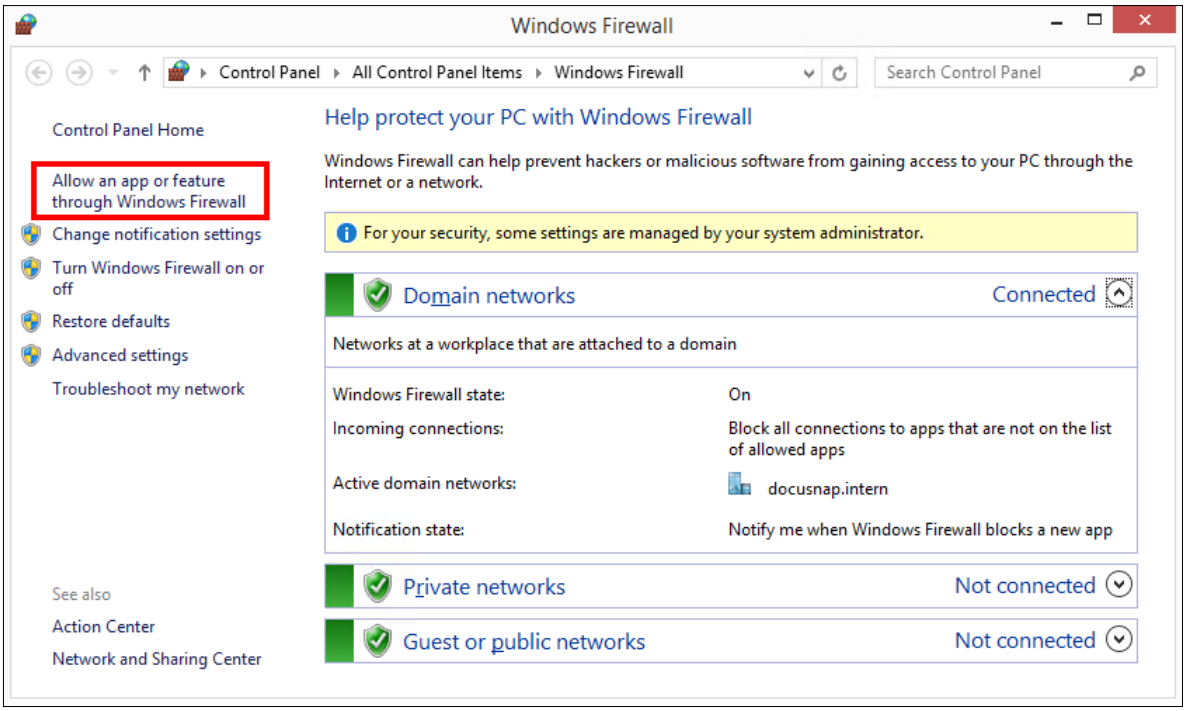

Fig. 10 - Windows 10 – Windows-Firewall - Allow an app or feature through Windows Firewall option

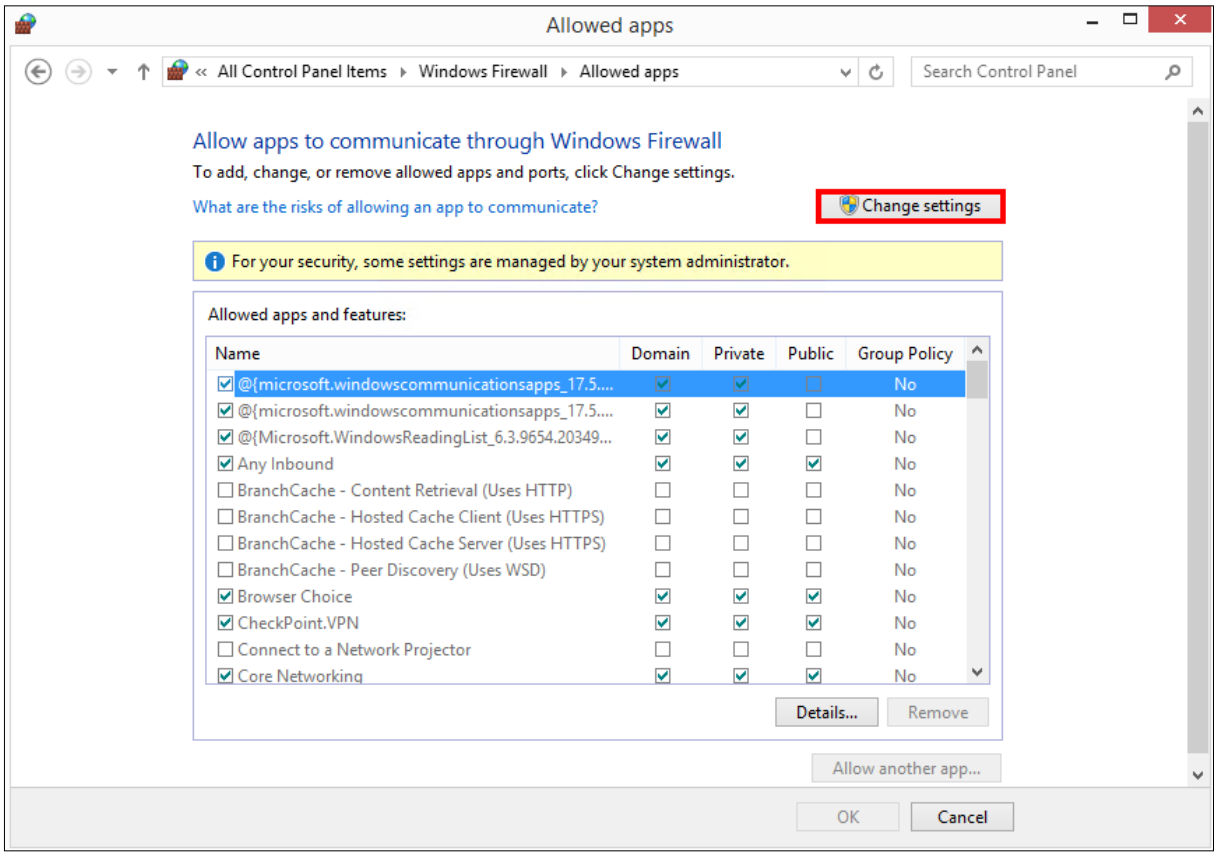

Fig. 11 - Windows 10 – Windows-Firewall: Allowed apps window

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

VERSION HISTORY

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

