



Windows-Firewall-Ausnahmen

Windows-Firewall-Ausnahmen für DocuSnap konfigurieren

TITEL	Windows-Firewall-Ausnahmen
AUTOR	Docusnap Consulting
DATUM	14.04.2015

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	AUSNAHMEN FÜR DATEI- UND DRUCKERFREIGABE AKTIVIEREN	11
3.6	REMOTEVERWALTUNGSAusNAHME AKTIVIEREN	12
4.	WINDOWS 8 - WINDOWS FIREWALL KONFIGURATION (LOKAL)	13
4.1	AUSNAHMEN FESTLEGEN	14

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 8 - WINDOWS FIREWALL KONFIGURATION (LOKAL) wird am Beispiel von Windows 8 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.

Hinweis: 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-Verwaltungskontrolle (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-Verwaltungskontrolle 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:

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

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

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

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

Weitere Informationen zur Gruppenrichtlinien-Verwaltungskontrolle und ihren Möglichkeiten findet man unter: <https://technet.microsoft.com/de-de/library/cc753298.aspx>

3.2 GPMC STARTEN

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

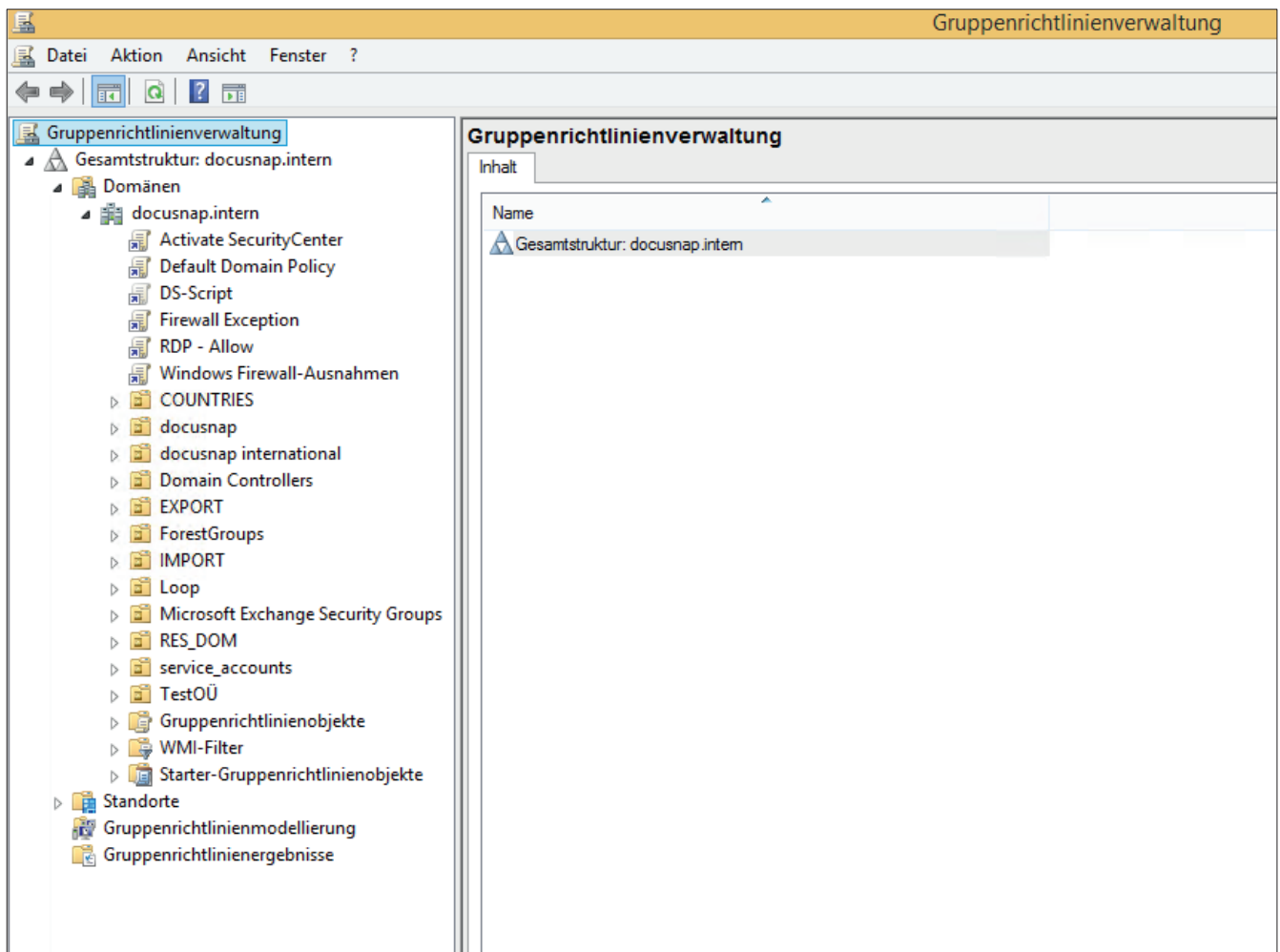


Abbildung 1 - Gruppenrichtlinienverwaltung

3.3 GRUPPENRICHTLINIENOBJEKT ERSTELLEN

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

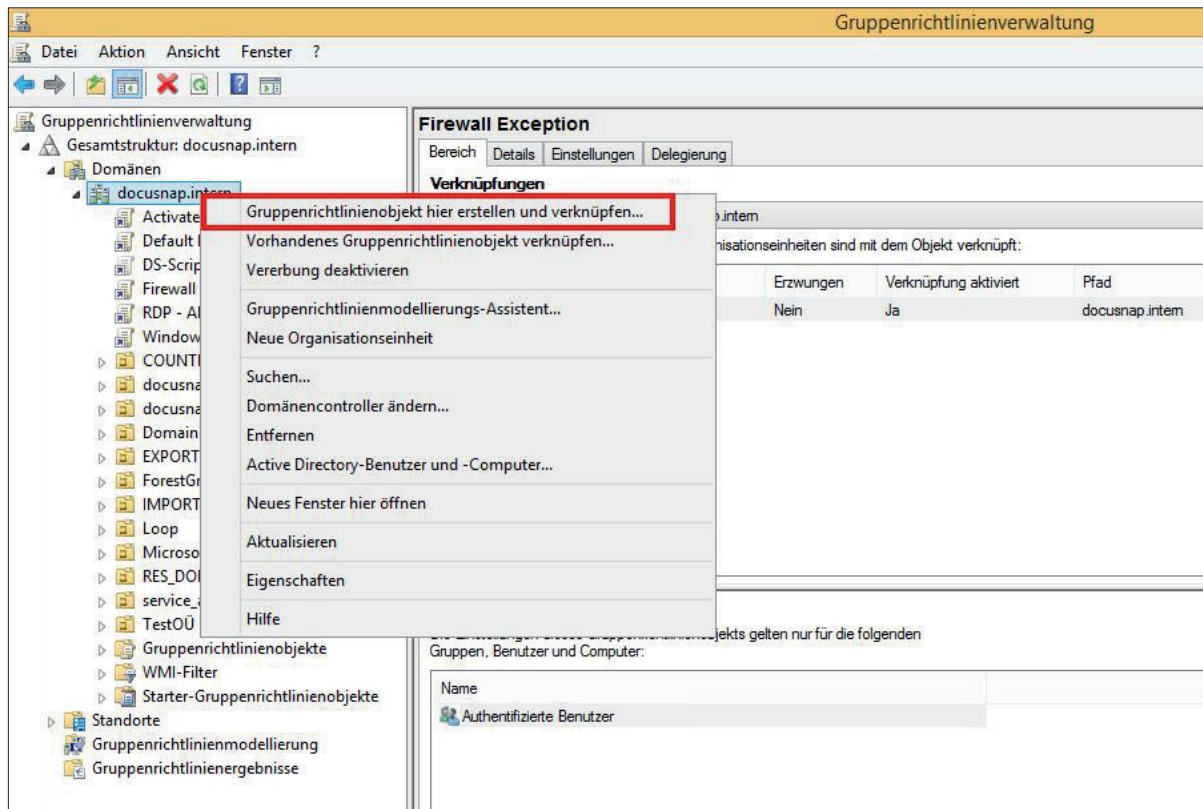


Abbildung 2 - Gruppenrichtlinienobjekt hier erstellen und verknüpfen

Einen „sprechenden“ Namen für das Gruppenrichtlinienobjekt festlegen.

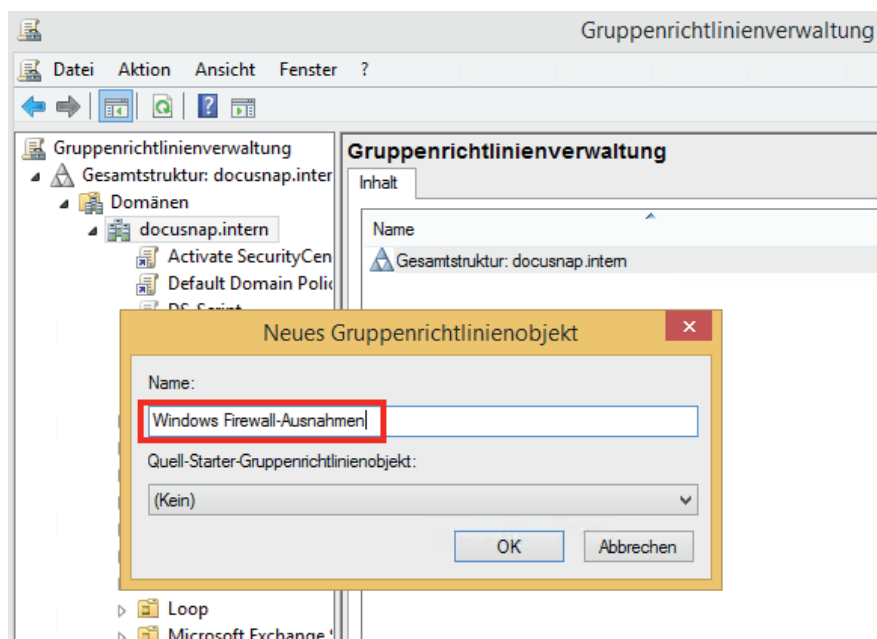


Abbildung 3 - Neues Gruppenrichtlinienobjekt

3.4 GRUPPENRICHTLINIENOBJEKT BEARBEITEN

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

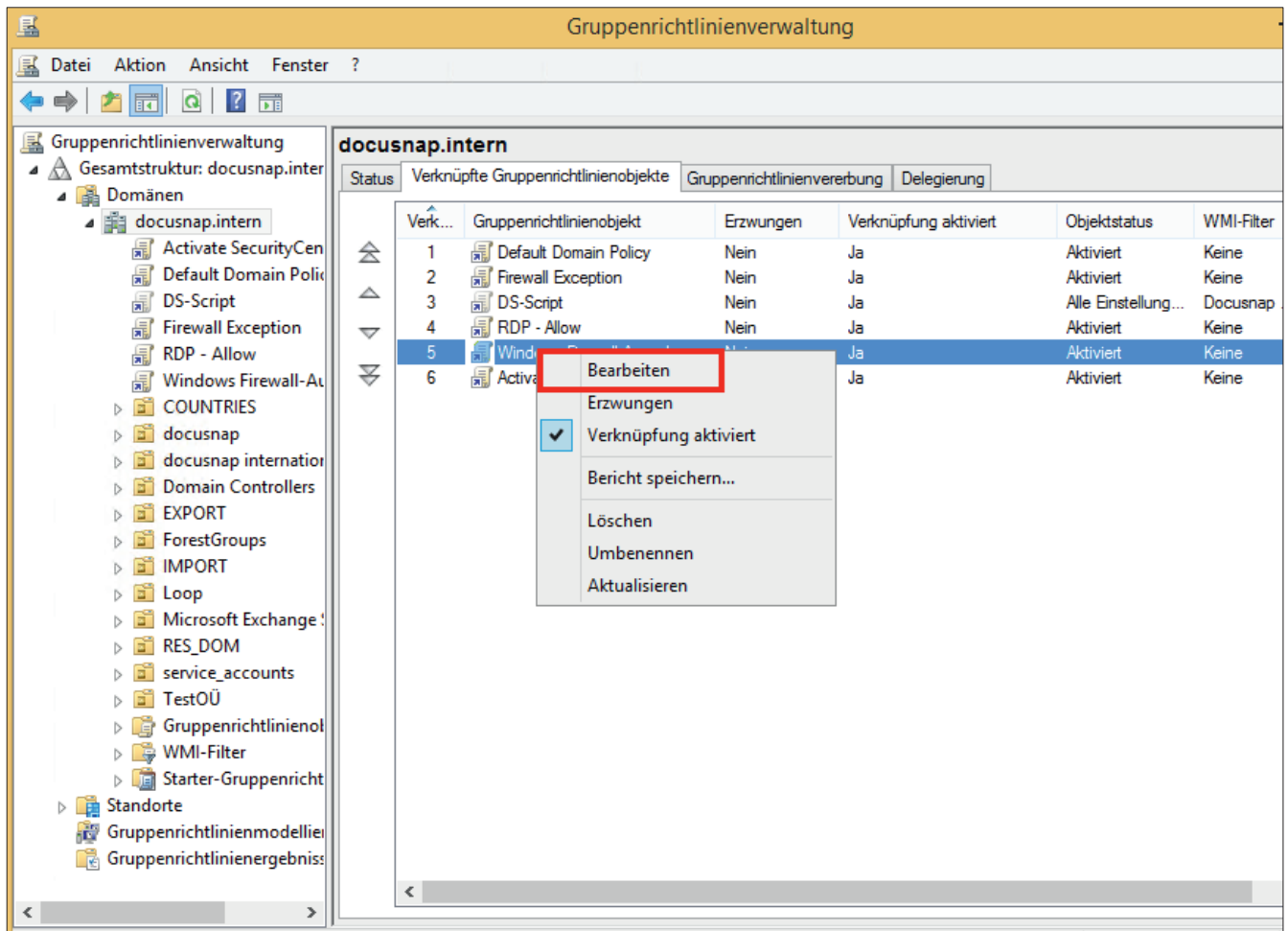


Abbildung 4 - Gruppenrichtlinienobjekt bearbeiten

Der Gruppenrichtlinienobjekt-Editor öffnet sich:

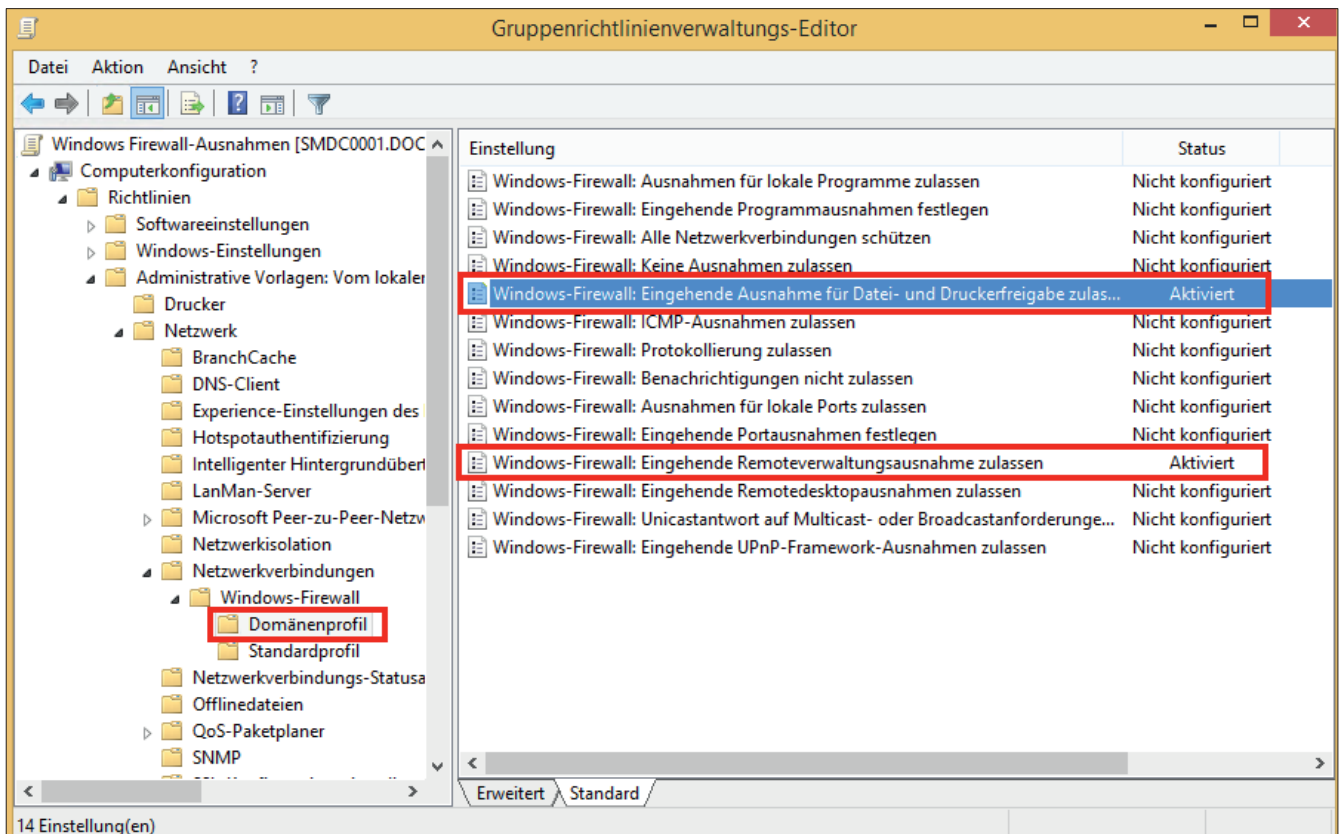


Abbildung 5 - Gruppenrichtlinienobjekt-Editor

Die zu konfigurierenden Gruppenrichtlinien befinden sich unter:

- Computerkonfiguration
 - Richtlinien
 - Administrative Vorlagen
 - Netzwerk
 - Netzwerkverbindungen
 - Windows-Firewall
 - Domänenprofil

3.5 AUSNAHMEN FÜR DATEI- UND DRUCKERFREIGABE AKTIVIEREN

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

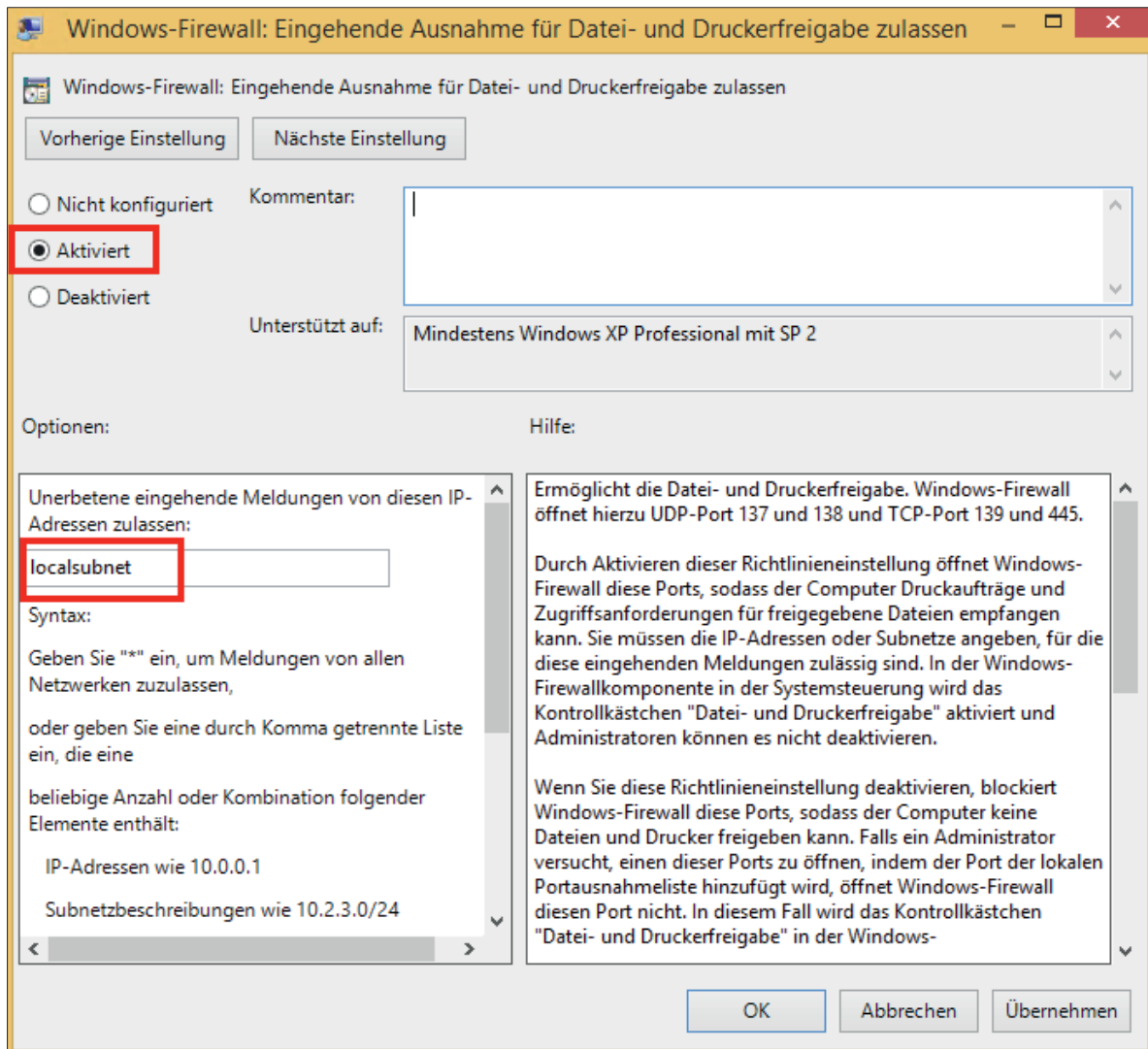


Abbildung 6 - Ausnahme für Datei- und Druckerfreigaben aktivieren und Bereich einschränken

3.6 REMOTEVERWALTUNGSAusNAHME AKTIVIEREN

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

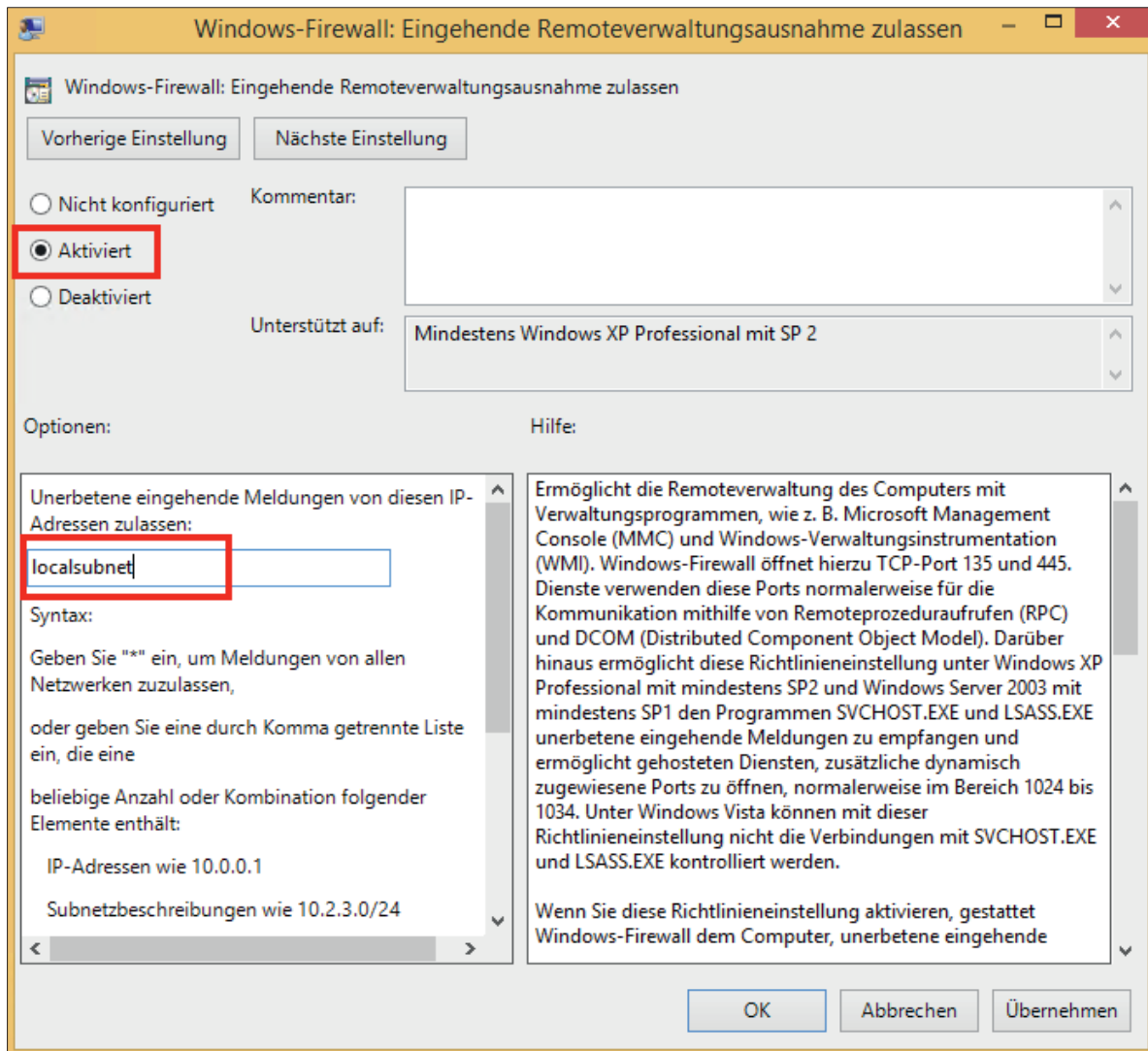


Abbildung 7 - Remoteverwaltungsausnahme aktivieren und Bereich einschränken

4. WINDOWS 8 - WINDOWS FIREWALL KONFIGURATION (LOKAL)

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



- Suchen – Eingabe: *firewall.cpl*

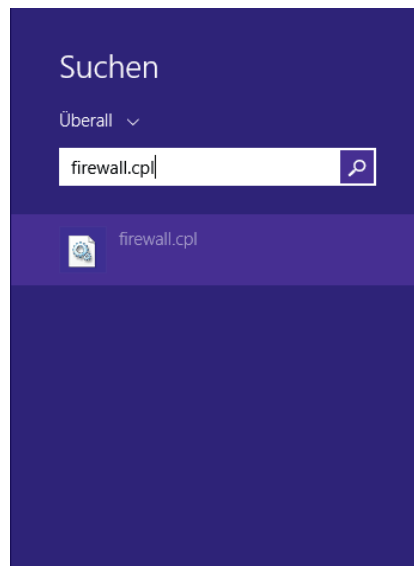


Abbildung 8 - Windows 8 - Suche - Eingabe firewall.cpl

Alternativ kann der Befehl auch in einem Konsolenfenster ausgeführt werden:

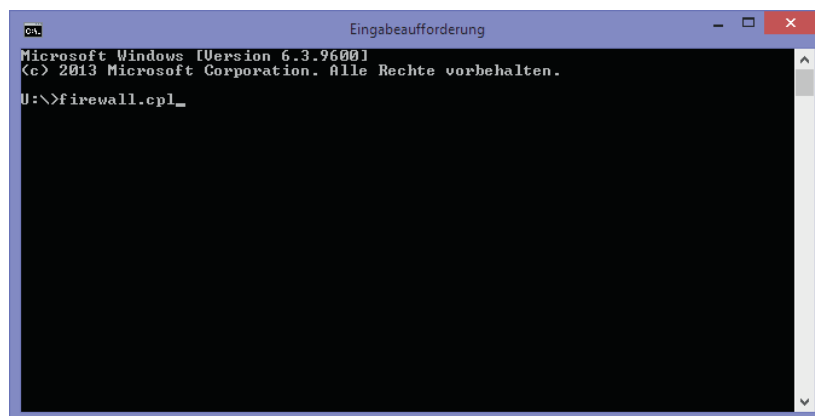


Abbildung 9 - Windows 8 - Eingabeaufforderung firewall.cpl

4.1 AUSNAHMEN FESTLEGEN

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

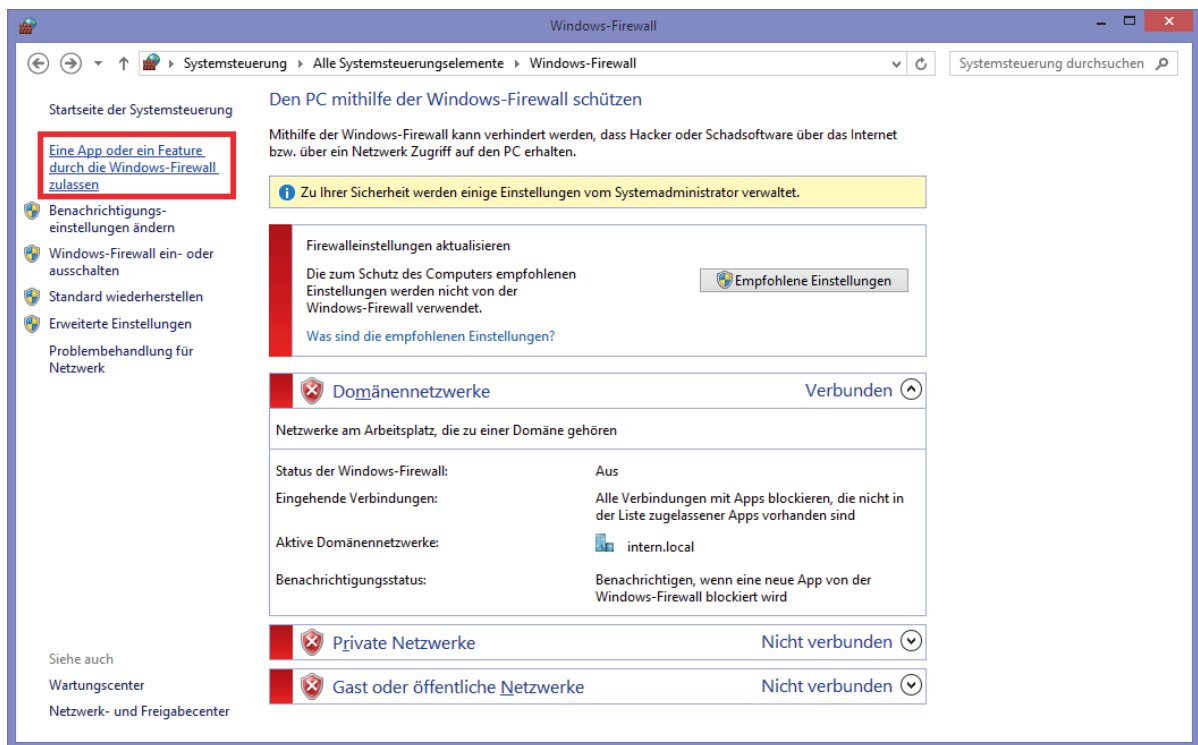


Abbildung 10 - Windows 8 - Windows-Firewall - App oder Feature zulassen

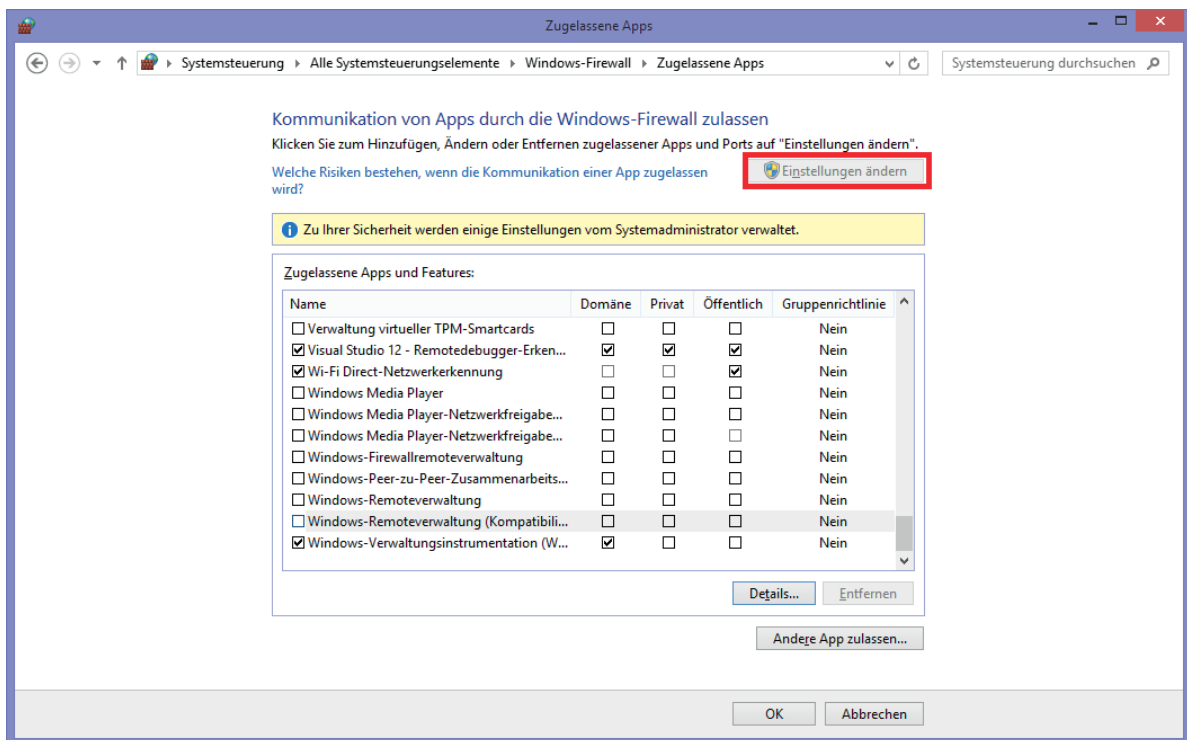


Abbildung 11 - Windows 8 – Windows-Firewall Zugelassene Apps und Features

Einstellungen ändern schaltet, entsprechende Benutzerrechte vorausgesetzt, die Bearbeitung von Programmen und Features frei. Windows 8 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 - WINDOWS 8 - SUCHE - EINGABE FIREWALL.CPL	13
ABBILDUNG 9 - WINDOWS 8 - EINGABEAUFFORDERUNG FIREWALL.CPL.....	13
ABBILDUNG 10 - WINDOWS 8 - WINDOWS-FIREWALL - APP ODER FEATURE ZULASSEN	14
ABBILDUNG 11 - WINDOWS 8 – WINDOWS-FIREWALL ZUGELASSENE APPS UND FEATURES.....	14



Docusnap[®]

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