

## Windows XP SP2 Konfiguration für LOGINventory

### Überblick:

In Windows XP (vor SP2) war die Internetverbindungsfirewall (ICF Internet Connection Firewall) auf allen DFÜ-Verbindungen aktiv, sobald die ICF erfolgreich gestartet wurde.

Beim Boot von Windows XP SP2, wird eine Standard Windows Firewall Richtlinie angewandt, die es den Computern nur erlaubt, grundlegende Netzwerkfunktionen auszuführen. Dazu gehören DHCP (Dynamic Host Configuration Protocol), und DNS (Domain Name Service), die es den Computern erlauben mit den Domänen Controllern zu kommunizieren, um Updates der Gruppenrichtlinien zu erhalten.

Sobald der Windows Firewall (WF) Dienst gestartet ist, wird dessen Konfiguration benutzt, und die Standard Windows Firewall Richtlinie deaktiviert.

Diese Standard Windows Firewall Richtlinie kann nicht konfiguriert oder deaktiviert werden.

Die Standard Konfiguration des Windows Firewall in Workgroups erlaubt folgende eingehenden Verbindungen:

- Remote Desktop von überall ( „\*“ )
- File- und Printservice vom eigenem Subnetz ( „LocalSubnet“ )

Ist der PC mit Windows XP SP2 Mitglied einer Domain, so ist lediglich der Remote Desktop zugelassen.

**LOGINventory** benutzt folgende Methoden zur Inventarisierung beim IP-Scan:

- Ping (ICMP)
- Remote Registry basierend auf File- und Printservice
- WMI basierend auf RPC (optional)

Handlungsbedarf besteht demnach also in Domains, wenn über Subnet-Grenzen hinweg gescannt oder WMI eingesetzt werden soll.

## Konfiguration der Windows Firewall durch GPOs

In einem Firmennetzwerk, das ADS (Active Directory Services) benutzt, können Gruppenrichtlinien dazu verwendet werden, die Windows Firewall einzurichten. Dazu gibt es neue Gruppenrichtlinien, die es einem Netzwerkadministrator erlauben, die Windows Firewall zu konfigurieren.

Updates von Gruppenrichtlinien werden von den Mitgliedscomputern der Domain selbst veranlasst, so dass dieser Verkehr nicht von der Firewall blockiert wird.

Sobald diese Gruppenrichtlinien in einem Netzwerk aktiviert sind, können manche lokalen Einstellungen für die Windows Firewall nicht mehr geändert werden. Dies gilt auch für lokale Administratoren.

Diese Gruppenrichtlinien können für zwei unterschiedliche Profile konfiguriert werden.

- **Domänen Profil**  
Die Einstellungen dieses Profils werden verwendet, sobald der Computer mit dem Firmennetzwerk verbunden ist.
- **Standard Profil**  
Wenn der Computer sich nicht im Firmennetzwerk befindet, wird dieses Profil verwendet. Da der Computer, in diesem Fall nicht mehr kontrolliert werden kann, sollte dieses Profil stärker eingeschränkt sein.

## Konfiguration für LOGINventory:

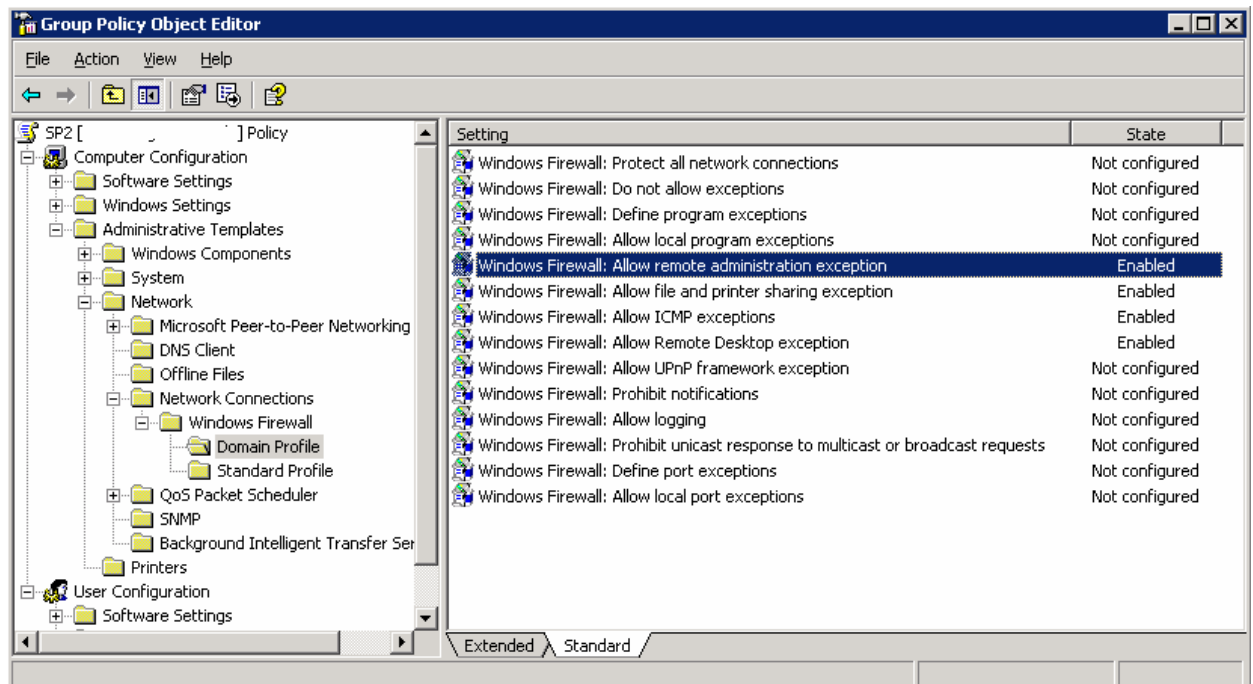
Zuerst müssen die GPOs mit den neuen Gruppenrichtlinien der Windows Firewall auf den aktuellen Stand gebracht werden:

- Melden Sie sich an einem Windows XP-SP2 PC als Benutzer mit Rechten zum Erstellen von GPOs an (z.B. Domain-Admin).
- Starten Sie MMC, fügen Sie das Snap-In „Gruppenrichtlinie“ hinzu und „Durchsuchen“ Sie die Domain, um die gewünschte OU zu finden.

Jetzt kann die Windows Firewall mit Hilfe einer neuen GPO (z.B. „SP2“) konfiguriert werden.

Für die problemlose Zusammenarbeit mit LOGINventory empfehlen wir folgende Einstellungen:

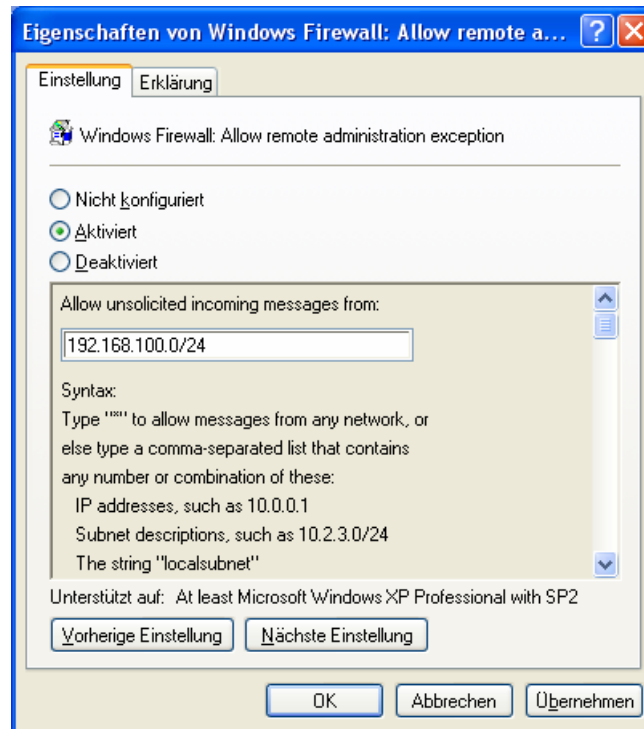
Navigieren Sie zu: „Computer Configuration / Administrative Templates / Network / Network Connections / Windows Firewall / Domain Profile“.



Im Folgenden werden diese Einstellungen der Windows Firewall kurz beschrieben.

- **Windows Firewall: Allow remote administration exception - enabled**

Um diese Einstellung zu ändern, wählen Sie Eigenschaften im Kontextmenu.



Diese Einstellung erlaubt es ihnen zu bestimmen, ob Computer mit Windows XP SP2 mittels Applikationen, die die TCP Ports 135 und 445 (z.B. MMC, WMI) benutzen, Remote administriert werden können.

Dienste, die über diese Ports kommunizieren, benutzen RPC Calls und DCOM um Zugriff auf Remote Hosts zu bekommen. Die Windows Firewall fügt SVCHOST.EXE und LSASS.EXE in die Liste der ausgenommenen Programme hinzu, und erlaubt diesen Diensten zusätzliche dynamische Ports, normalerweise im Bereich von 1024 bis 1034, Freizuschalten.

**Allow incoming messages from systems in these subnets:**

Hier wird konfiguriert aus welchen IPv4 Subnets eingehende Verbindungen akzeptiert werden.

Idealerweise platziert man die Server in einem separaten Subnet, in unserem Beispiel „192.168.100.0/24“, und gibt dieses Subnet an.

Dadurch wird sichergestellt, dass nur Verbindungen aus dem gewählten IPv4 Adressbereich akzeptiert werden. Versuche aus anderen Netzen werden blockiert. „LocalSubnet“ erlaubt nur Verbindungen von IPv4 Adressen aus dem Subnet des Rechners

„\*“ erlaubt Verbindungen von jeder IPv4 Adresse.



Die RPC Schnittstelle ist ein beliebter Angriffspunkt für Viren wie z.B. „Blaster“ oder „Sasser“. LOGINquiry benötigt RPC zum Ermitteln der (optionalen) WMI-Informationen.

- **Windows Firewall: Allow file and printer sharing exception - enabled**

Um diese Einstellung zu ändern, wählen Sie Eigenschaften im Kontextmenu.

Diese Einstellung erlaubt es ihnen festzulegen, ob die Ports für die Datei und Druckerfreigabe geöffnet sind. Ist diese Einstellung aktiviert, werden folgende Ports geöffnet:

UDP 137, UDP 138, TCP 139 und TCP 445

**Allow unsolicited incoming messages from:**

Hier wird ebenfalls konfiguriert aus welchen IPv4 Subnets eingehende Verbindungen akzeptiert werden; in unserem Beispiel „\*“ (alle Netze).



Diese Schnittstelle hatte in der Vergangenheit keine einzige bekannte Schwachstelle.

LOGINquiry ermittelt fast alle Informationen über diesen Weg.

---

- **Windows Firewall: Allow ICMP exceptions - enabled**

Um diese Einstellung zu ändern, wählen Sie Eigenschaften im Kontextmenu.

Wenn diese Einstellung aktiviert ist, müssen zusätzlich noch die erlaubten ICMP Pakete definiert werden.

Die meisten Einstellungen der Windows Firewall beziehen sich auf eingehenden, dagegen betreffen mehrere Optionen von **Allow ICMP exceptions** auch ausgehenden Verkehr.



Sobald eine andere Einstellung der Windows Firewall den TCP Port 445 öffnet (z.B. *File and Printer sharing*), sind eingehende ICMP Verbindungen erlaubt, auch wenn Allow ICMP exceptions deaktiviert ist.

LOGINquiry verwendet „Ping“ zum Erkennen eines vorhandenen PCs.

---

- **Windows Firewall: Allow remote Desktop exception - enabled**

Um diese Einstellung zu ändern, wählen Sie Eigenschaften im Kontextmenu.

Ist diese Einstellung aktiviert, sind Remote Desktop Verbindungen erlaubt, und der TCP Port 3389 ist geöffnet.

**Allow unsolicited incoming messages from:**

Hier wird ebenfalls konfiguriert aus welchen IPv4 Subnets eingehende Verbindungen akzeptiert werden; in unserem Beispiel „\*“ für alle Netze.



Dies Schnittstelle wird von keinem LOGINventory Modul direkt verwendet; kann jedoch z.B. über MMC - Taskpad aufgerufen werden.

---

Weiterführende Informationen zu diesem Thema:

[Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2](#)