

# LOGINventory5

## Trouble Shooting Guide

© 2012 Schmidt's LOGIN GmbH  
Munich

Phone +49 89 44 888 70  
[www.LOGINventory.com](http://www.LOGINventory.com)  
[info@LOGINternet.de](mailto:info@LOGINternet.de)

## Table of Content

<b>1</b>	<b>Installation .....</b>	<b>3</b>
1.1	Installation ended prematurely because of an error.....	3
1.2	Internal Error 2738 .....	3
1.3	Multiple LOGINventory installation.....	3
1.4	Error opening file for writing .....	3
<b>2</b>	<b>Scanning .....</b>	<b>4</b>
2.1	Prerequisites for Scanning .....	4
2.2	Common Scan Errors.....	5
<b>3</b>	<b>Miscellaneous Problems .....</b>	<b>8</b>
3.1	Manual Inventory.....	8
3.2	Uninstalling LOGINventory.....	8
3.3	Start and Go .....	8
3.4	Display of Software not installed .....	8
3.5	'Your Database is not case-sensitive! This can cause problems ...' .....	9
3.6	LOGINfoW failed to initialize properly .....	10
<b>4</b>	<b>Windows XP SP2/3 Firewall Configuration.....</b>	<b>11</b>
4.1	Introduction.....	11
4.2	Configuration using Group Policy Objects .....	11
4.3	Configuration for LOGINventory.....	12
4.4	Configuration of the Windows Firewall using NETSH.....	16
<b>5</b>	<b>Windows 7, Vista and 2008 Server Configuration .....</b>	<b>18</b>
5.1	Introduction.....	18
5.2	Local configuration of Windows Vista or later .....	19
5.3	Configuration by using Group Policy Objects .....	22
5.4	Applying Group Policy Settings to PCs.....	31
<b>6</b>	<b>Remote Assistance .....</b>	<b>32</b>
6.1	Unsolicited Remote Assistance.....	32
6.2	Remote Assistance Group Policies.....	32
6.3	Remote Assistance in LOGINventory Management Console .....	35
<b>7</b>	<b>SNMP .....</b>	<b>36</b>
7.1	Installation of additional components .....	36
7.2	Test explicit credentials via Net-SNMP .....	36
7.3	Define default setting for Net-SNMP .....	37
7.4	Test default credentials .....	37
7.5	Use SNMP v1/v2c with LOGINventory.....	38

## 1 Installation

During the LOGINventory installation you may encounter unforeseen problems. The reasons for the abort of the installation are different. Following you find an explanation of the various messages which indicate the potential cause for a failed installation.

### 1.1 Installation ended prematurely because of an error

LOGINventory web interface is installed by the Microsoft Installer service, so the user 'System' must have read access to the install source directory for the installation to work.

### 1.2 Internal Error 2738

This message indicates a missing Windows Scripting Host (WSH). You can download the current WSH version from the Microsoft Download Center at

<http://www.microsoft.com/downloads/en/default.aspx>

### 1.3 Multiple LOGINventory installation

If you use multiple installations, it is important to refresh all existing LOGINventory installations in the event of an update!

For execution within logon script, always the most current version of LOGINfo.exe is required.

Since LOGINventory version 5.5 Build 5153 all LOGINfo\*.exe programs in DATA directory (if available) will be automatically updated during installation.

### 1.4 Error opening file for writing ...

- (DbgHelp.dll) LOGINventory is still installed onto this system and one of its applications is in use, maybe by another user on this system. Close all applications and restart the setup again.
- (LVBext.dll) LOGINventory is still installed onto this system and the WebInterface has been used, therefore IIS still access LOGINventory libraries.  
Workaround: Execute the command 'iisreset'<sup>1</sup> and restart the setup again.

---

<sup>1</sup> Open a 'Command Prompt', as administrator if necessary, and execute the command  
`iisreset`

## 2 Scanning

### 2.1 Prerequisites for Scanning

The following prerequisites may be checked to assure proper scans:

Due to the limited networking capabilities of Windows 95, 98, ME, XP Home, Vista Home and Windows 7 Home, LOGINventory is unable to remotely scan such PCs. However, by executing LOGINfo.EXE locally (for example via start-up script) it is possible to inventory these computers, too (see section 3.1 of the LOGINventory Manual for detailed explanation).

For scanning remote computers, valid logon credentials as a local administrator on the remote PC are required.

Typically, this is no problem in a domain environment when logged on with an account which is a member of the 'Domain Admins' group. Otherwise user name and password must be specified within LOGINquiry. For domain accounts the user name must be prefixed with the domain name (e.g.: MYDOMAIN\myadministrator).

In a workgroup environment user name and password are always required. The user account must have administrative privileges on the target, otherwise ERROR 5 or ERROR 1326 (access denied) occurs.

Microsoft integrated a new security mechanism into **Windows XP** and later that automatically maps every connection to the 'Guest' user on network access, even if the Guest account is deactivated. This feature can be turned off in the **local security policy** by setting

Local Policies

→ Security Options

→ Network access: Sharing and Security model for local accounts

to value 'Classic'.

'**Client for Windows Networks**' and '**File and Printer Sharing**' must be enabled.

Administrative shares (**C\$, D\$** ...) are required for gathering disk space if no WMI is used.

It must be possible to connect to a Windows workstation share using

```
NET USE * \\PCname\IPC$ /USER:domain\adminaccount password
```

or

```
NET USE * \\PCname\IPC$ /USER:localadminaccount password
```

**Regedit** respectively **Regedit32** remote registry access should work:

- Start REGEDIT
- Select File / Connect Network Registry
- Enter the object name to select:  
The result of

```
NBTSTAT [-a 'PCname'] or
```

```
NBTSTAT [-A 'PC-IP-address'] (i.e. 192.168.1.2)
```

- should list [PCname] within NetBIOS name table.

On Windows XP or later Remote WMI access can be checked by **WMIC**, e.g.:

```
WMIC /NODE:remotepc-FQDN /USER:domain\adminaccount /PASSWORD:secret CPU
```

### 2.1.1 Ports and Protocols

**LOGINventory uses the following protocols and ports for scanning:**

- ICMP Echo Request (if Ping doesn't work - SNMP connect is tried only)
- TCP Port 139 (NetBIOS Session Services)
- UDP Port 137 and 138 (NetBIOS Name Server, NetBIOS Datagram)
- TCP Port 445 (RPC + WMI)
- UDP Port 161 (SNMP)

In most cases the first two (Ping and TCP/139) are sufficient for Windows PCs. When using SNMP, the device generally must also answer Ping; it is also possible but not recommended to configure LOGINquiry for retrieving SNMP data from devices not answering Ping.

## 2.2 Common Scan Errors

Scanned computers do not necessarily have to be members of a domain; however, local administrative rights are needed for scanning everywhere. Parameters such as 'user name', 'user account', 'logon domain' and 'logon server' will only be identified, if a user is logged in while scanning.

All error codes that are displayed during the scan process and have a value higher than '4' are normal Windows error codes. They will be described if you enter

```
NET HELPMSG
```

on the command prompt.

You will find detailed descriptions about the Windows error codes on the pages of 'Microsoft Tech-Net' at

<http://technet.microsoft.com/en-us/default.aspx>.

Following you will find descriptions of the most common scan errors and how they can be resolved.

### 2.2.1 ERROR 1: No WMI: Inventory successful, but without WMI information

Verify that the Windows Management Instrumentation service is running by 'services.msc' or search the System Log for DCOM errors. In case of Windows XP-SP2 please read chapter 4 of this Trouble Shooting Guide or disable the firewall for testing purposes.

Use 'dcomcnfg.exe' and select:

- *Component Services*
  - *Computers*
    - *My Computer*
      - *Properties*
        - *Default Properties*

to check whether DCOM is enabled and access rights are properly configured (Compare settings to a machine where WMI works).

Compare settings of  
*Component Services*  
 → *Computers*  
 → *My Computer*  
 → *DCOM Config*  
 → *Windows Management and Instrumentation*  
 → *Properties* (right mouse button)  
 → *Security*

to a machine where WMI works.

Repeat the same procedure for  
 → *Microsoft WMI Provider Subsystem Host*  
 → *Properties* (right mouse button)  
 → *Security*

if available.

Stop the WMI service and delete the directory  
`%systemroot%\system32\wbem\Repository`

Restart WMI. The folder is recreated on the next access.

Ensure that

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\EnableDCOM`

has the value '= Y' and is of type REG\_SZ.

On Windows XP or later you can check via command line, whether you have WMI access to a remote PC:

```
C:\> WMIC /NODE:remotepc-FQDN /USER:domain\adminaccount /PASSWORD:secret CPU
```

You will find some more trouble shooting information about WMI here:

<http://www.microsoft.com/technet/scriptcenter/resources/wmifaq.mspx>

### 2.2.2 ERROR 5: Access is denied

Invalid user name or password

Either the scanning account is not a member of the local Administrators group or the Sharing and Security model for local accounts is not set to 'classic' on Windows XP. The Local Security Policy 'Limit local account use of blank passwords to console login only' could be another technical reason.

### 2.2.3 ERROR 22: The device does not recognize the command

The Remote Registry Service is not running on the target PC (default setting on Vista) or there might be a problem with the access rights of the registry on the client machine.

The latter can happen when scanning with LOGINquiry in a domain environment if only a local account is specified and not a domain account (e.g. MYDOMAIN\Administrator).

Try to connect the registry of the client over the network using 'Regedit.exe'. Check if you have access to the following registry key:

`HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0`

If not, please notice the subsequent articles:

<http://support.microsoft.com/?scid=kb;en-us;892192>

<http://support.microsoft.com/?scid=kb;en-us;314837>

#### **2.2.4 ERROR 40: Unknown error**

SNMP connection failure.

Either the SNMP read community specified is invalid or the target is not reachable via SNMP at all.

#### **2.2.5 ERROR 51 / ERROR 53: Network path not found**

Microsoft file- and print server is not available.

Normal using Windows 9x, XP Home, Vista Home or 7 Home, since the appropriate API not present.

Refer to a problem in name resolving. Check your configuration for DNS, HOSTS, WINS, LMHOST and NetBIOS.

#### **2.2.6 ERROR 1223: The operation was canceled by the user.**

The inventory of this asset has been canceled by a STOP statement in LOGINfo.ini.

#### **2.2.7 ERROR 1326: Logon failure: unknown user name or bad password**

This error will mainly occur if the PC is not a member of a domain but of a workgroup. It is equivalent to ERROR 5 in case of Workgroup.

Ensure that in LOGINquiry the domain prefixes the username: e.g. 'Domain\Administrator'.

#### **2.2.8 ERROR 1395: Out of License**

Your installation is licensed for a particular number of asserts. No more assets can be inserted at this time because there are already as many assets as the database can accept.

#### **2.2.9 ERROR 1460: This operation returned because the timeout period expired**

The maximum time between client responses or the total time for a scan was reached.

You can adjust timeouts in LOGINfo.ini; default settings are:

```
!SET TOTALTIMEOUT=1800
!SET INACTIVITYTIMEOUT=300
!SET SNMPCONNECTTIMEOUT=10
```

Sometimes an active network component detects an 'Outbreak' attack from a LOGINquiry PC by mistake. In this case please significantly reduce the number of concurrent scans in LOGINquiry options (to 1 ... 3); if timeouts are gone please contact your network administrator.

Please read also Chapter [2.1](#) of this Trouble Shooting Guide about scanning prerequisites.

## 3 Miscellaneous Problems

### 3.1 Manual Inventory

You may create your own .LI5 files similar to those written by LOGINquiry or LOGINfo.exe, put them in the data directory and run LOGINsert to process them. Be aware, that the filename is very important:

```
[COMPUTERNAME]@[YEAR][MONTH][DAY]T[HOURL][MINUTE][SECOND].LI5
```

You can download an example for such a file under

<http://www.loginter.net/files/manual-inventory-sample.zip>.

In this file, the only mandatory line in the file is PCNAME, all others are optional.

Starting with version 5 you can easily create and edit these files with the new module **LIEditor**, which can be found in Start Menu in:

```
LOGInventory5  
→ Tools  
→ LIEditor
```

### 3.2 Uninstalling LOGINventory

When uninstalling LOGINventory, not all components will be removed: collected data, scan-range definitions and registry keys (including LOGINventory license information) remain unaffected.

In LOGINventory5 you are able to remove these components too, by checking the corresponding option in the un-install process.

For more information please visit our support forum (English and German language) or send an email to

<mailto:support@loginternet.de>.

### 3.3 Start and Go

It is possible to start the LOGINventory Management Console along with the command line parameter /q:<pcuid> to immediately set the focus to the asset <pcuid>.

Example:

```
MMC 'c:\Program Files\LOGIN\LOGINventory5\LOGINventory5.msc' /q:MyPcName
```

### 3.4 Display of Software not installed

Starting with version 5, this feature has been integrated into the standard 'Software / Packages' and 'Software / Hotfixes' node.

- The column 'Installed' shows if a certain package has been found on a single computer (or not)!
- In addition you may reduce the view to computers without this software by entering 'no' into filter bar of column 'Installed'; this filter defaults to 'yes'.

### 3.5 'Your Database is not case-sensitive! This can cause problems ...'

Per default, only Oracle and PostgreSQL database will be installed with a case-sensitive default collation by their installation procedure as required by LOGINventory5.

MS-Jet is always case-insensitive.

#### 3.5.1 MySQL

If you are using MySQL you can change the default collation even after MySQL installation by modifying the file 'my.ini':

- Go to section [mysqld]
- Add or modify:  

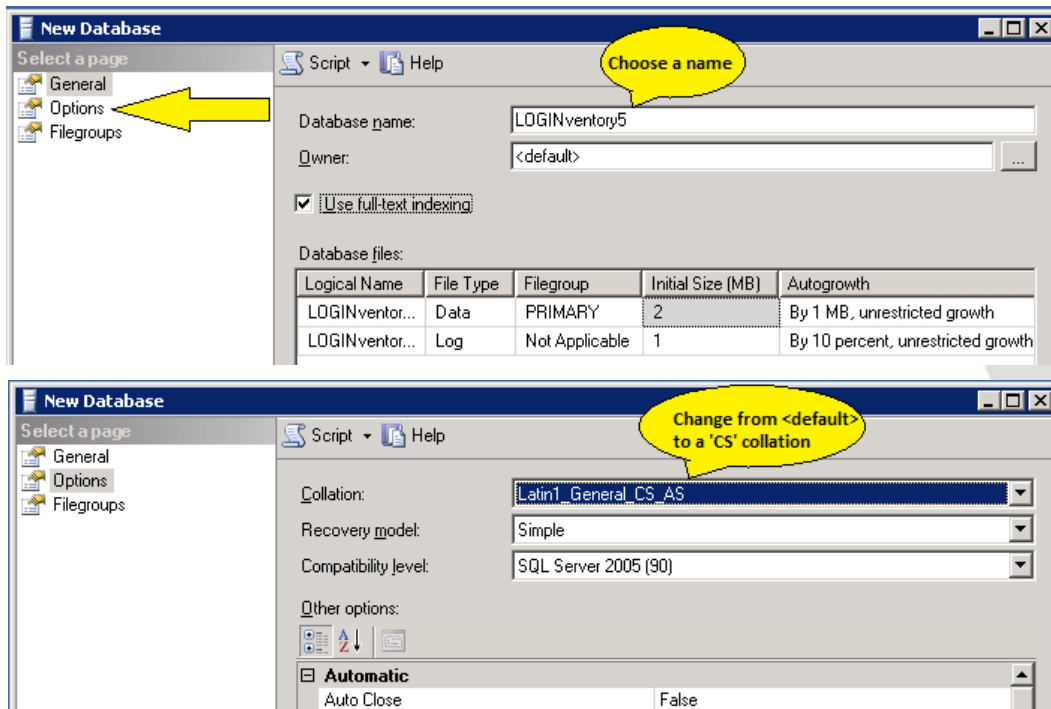
```
default-collation=latin1_general_cs
```

Save the file and restart MySQL services.

From now on, every new database will use this case sensitive collation. Existing databases will not be affected by this modification.

#### 3.5.2 Microsoft SQL Server 2005 / 2008

If you are using MS-SQL Server you cannot easily change the default server collation (SQL\_Latin1\_General\_CP1\_CI\_AS for an English server) after installation; however you can always create a new database via SQL Server Management Studio and specify in 'Options' the collation: 'Latin1\_General\_CS\_AS'. For an existing one you can change it the same way.



After creation do not forget to allow access for the appropriate users.

If you want to change the default collation for SQL Server 2008, please read:

<http://msdn.microsoft.com/en-us/library/ms179254.aspx>.

After changing the default collation, every new database will use the new default collation. Existing databases will not be affected.

### 3.6 LOGINfoW failed to initialize properly

LOGINfoW.exe or LOGINfo.exe has been started within login script from a network share:

```
\\server\share\Loginfow.exe \\server\share\data
```

While this was working without any problems under Windows XP, this cause the following error under Windows 7: 'The application failed to initialize properly (0xc000000F)'

This is a known problem in Windows 7. A supported hotfix is available from Microsoft:

<http://support.microsoft.com/kb/978869>.

## 4 Windows XP SP2/3 Firewall Configuration

### 4.1 Introduction

Windows XP SP2 introduces a start-up Windows Firewall policy to perform packet filtering. This allows the computer to perform basic networking start-up tasks, including DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name System). Using these services the computer may communicate with a domain controller to obtain Group Policy updates.

Once the Windows Firewall /ICS service was started, it uses its own configuration and removes the start-up policy. The start-up policy settings cannot be configured or uninstalled.

The default configuration of the Windows Firewall policy in workgroups allows the following incoming connections:

- Remote Desktop from everywhere ( '\*' )
- File and Print Service from the local subnet ('localsubnet').

If the Windows XP SP2 PC is a member of a domain, only Remote Desktop connections are allowed.

**LOGINventory** performs an inventory using the following methods during an IP scan:

- Ping (ICMP)
- Remote Registry based on File and Print Services
- WMI based on RPC (optional)

**If you want to scan other subnets or use WMI, the Windows Firewall must be configured in Domains.**

### 4.2 Configuration using Group Policy Objects

To centralize the configuration of large numbers of computers in an organization network that uses the Active Directory® Service, Windows Firewall settings for computers running Windows XP SP2/3 can be deployed through Computer Configuration Group Policy. A new set of Computer Configuration Group Policy Windows Firewall settings allows network administrators to configure Windows Firewall operational modes, excepted traffic, and other settings using a Group Policy Object.

Group Policy updates are requested by the domain member computer. This is therefore treated as solicited traffic that is not hindered to pass even if the Windows Firewall is enabled.

When you configure Windows Firewall in an organization network using Group Policy, some of the local Windows Firewall configuration options can be grayed out and marked as unavailable, even for local administrators.

When using the new Windows Firewall Group Policy settings, you can configure two different profiles:

- **Domain Profile**  
Set of Windows Firewall settings needed for networked computers containing the organization's domain controllers.
- **Standard Profile**  
This is the Windows Firewall settings needed when a computer is not connected to the network that contains an organization's domain controllers. Because laptops can be directly connected to the Internet, standard profiles should contain more restrictive settings than the domain profile.

### 4.3 Configuration for LOGINventory

You have to update Group Policy Objects with the New Windows Firewall Settings first:

- Log on to the Windows XP SP2/3 computer, as a member of
  - the Domain Administrator's security group or
  - the Enterprise Administrator's security group or
  - the Group Policy Creator Owner's security group.
- From the Windows desktop, click 'Start', click 'Run', type `mmc`, and then click OK.
- Go to
  - File
    - Add/Remove Snap-in...
- Click on the 'Add'- Button to open a list of Available Standalone Snap-ins list, click on Group Policy Object Editor, and then click Add. In the Select Group Policy Object dialog box, click Browse.

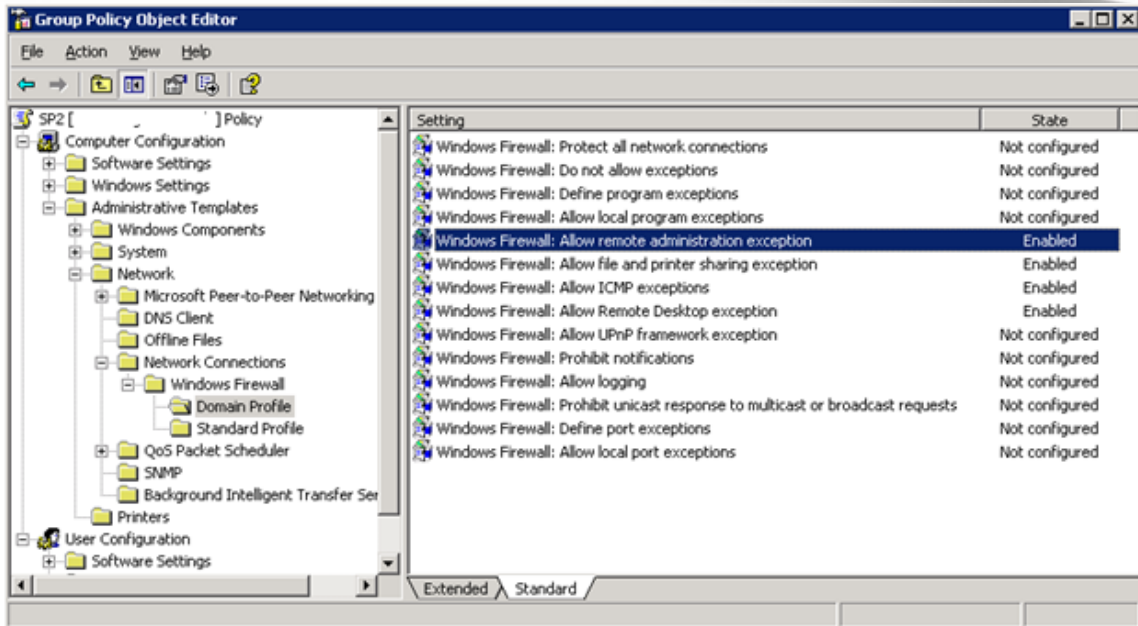


Now you can configure the windows Firewall using a new Group Policy Object (i.e. 'SP2').

For using LOGINventory we recommend these settings:

Navigate to:

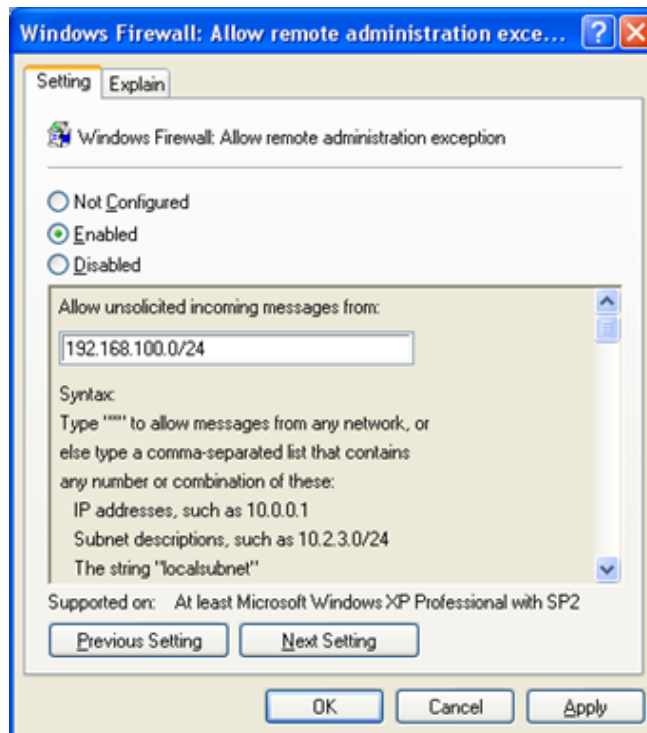
- Computer Configuration*
  - *Administrative Templates*
    - *Network*
      - *Network Connections*
        - *Windows Firewall*
          - *Domain Profile.*



The next steps provide a short description of how to configure these settings.

#### 4.3.1 Allow remote administration exception

To change these settings, select *Properties* in the Context menu.



This setting allows you to specify whether computers running Windows XP SP2/3 can be remotely administered by applications that use TCP ports 135 and 445 (such as MMC and WMI).

Services that communicate over these ports use Remote Procedure Calls (RPC) and Distributed Component Object Model (DCOM) to access remote hosts.

In effect, Windows Firewall adds SVCHOST.EXE and LSASS.EXE to the program exceptions list and allows those services to open additional, dynamically assigned ports, typically in the range of 1024 to 1034.

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

We recommend that you allow only traffic originating from the server subnet address (e.g. 192.168.100.0/24).

The sources can be:

- 'localsubnet'. This allows connections only from the computer's subnet.
- '\*': This allows connection from any network (not recommended)



The RPC interface is a well-known target for viruses such as 'Blaster' or 'Sasser'.

LOGINquiry uses the RPC interface to collect some (optional) WMI information, but it is not essential.

#### 4.3.2 Allow file and printer sharing exception

To change these settings, select *Properties* in the Context menu.

This setting specifies whether the ports for file- and printer sharing are open. Enabling this will open the following Ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445

**Allow unsolicited incoming messages from:**

Type \* to specify traffic originating from any source IPv4 address or a comma separated list of sources, e.g. '\*' (all networks).



There is no known security risk for this interface.

LOGINquiry collects most of its information this way.  
This setting is required!

### 4.3.3 Allow ICMP exceptions

To change these settings, select *Properties* in the Context menu.

The setting '**Windows Firewall: Allow ICMP exceptions**' allow you to configure specific types of ICMP messages so they will be treated as excepted traffic (unsolicited traffic that has been specified as allowed). When you select *Enabled*, you must also specify the specific types of ICMP messages that are allowed. Selecting *Enabled* overrides the local ICMP settings of the Windows Firewall.

Other Windows Firewall policy settings affect only incoming messages, but several of the options of the **Windows Firewall: Allow ICMP exceptions** setting also affect outgoing communication.



If any policy setting opens TCP port 445, Windows Firewall automatically allows inbound ICMP Echo messages, even if the *Allow ICMP exceptions* setting is disabled. Policy settings that can open TCP port 445 include *File and printer sharing exception*, *Remote administration exception*.  
Required, and already configured via the *File and printer sharing exception*.

### 4.3.4 Allow remote Desktop exception

To change these settings, select *Properties* in the Context menu.

Enable this setting will allow 'Remote Desktop connections' and will also open TCP port 3389.

#### Allow unsolicited incoming messages from:

Type \* to specify traffic originating from any source IPv4 address or a comma separated list of sources, e.g. "\*" (all networks).



This interface will **not** be used by any LOGINventory module. However, it can be used by any applications invoked from MMC task pad.  
Not required!

Please confirm the following services are running and start automatically:

- Server
- Remote Registry

For more information, see:

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

## 4.4 Configuration of the Windows Firewall using NETSH

For individual configuration of a single PC, Windows Firewall settings may be defined by using the 'NetSh' command.

Open a command window and type:

```
C:\>netsh firewall show opmode
```

You'll get as result something like:

```
Domain profile configuration (current):
-----
Operational mode           = Disable
Exception mode             = Enable

Standard profile configuration <current>:
-----
Operational mode           = Disable
Exception mode             = Enable

Local Area Connection firewall configuration:
-----
Operational mode           = Disable
```

This command output shows that Windows Firewall is currently disabled and needs to be enabled. To do this, use the following command:

```
C:\>netsh firewall set opmode enable
```

The next steps provide a short description of how to configure these settings.

### 4.4.1 Allow remote administration exception

To change these settings type:

```
C:\>netsh firewall set service remoteadmin enable subnet
```

This setting allows you to specify whether computers running Windows XP SP2/3 can be remotely administered by applications that use TCP ports 135 and 445 (such as MMC and WMI).

Services that communicate over these ports use remote procedure calls (RPC) and Distributed Component Object Model (DCOM) to access remote hosts. In effect, Windows Firewall adds SVCHOST.EXE and LSASS.EXE to the program exceptions list and allows those services to open additional, dynamically assigned ports, typically in the range of 1024 to 1034.

The sources can be

- the local subnet 'subnet' (as in our example)
- one or more IPv4 addresses or IPv4 address ranges separated by commas.

#### 4.4.2 Allow file and printer sharing exception

To change these settings type:

```
C:\>netsh firewall set service fileandprint enable *
```

This setting specifies whether the ports for file- and printer sharing are open. Enabling this will open the following Ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445

The sources can be

- the local subnet 'subnet'
- one or more IPv4 addresses or IPv4 address ranges separated by commas (as in our example)

Please confirm the following services are running and start automatically:

- Server
- Remote Registry

## 5 Windows 7, Vista and 2008 Server Configuration

### 5.1 Introduction

In Windows XP Service Pack 2, Microsoft shipped a vastly improved -- at the time -- client-based firewall solution. The Windows XP firewall in SP2 was enabled by default, which meant that computers were instantly granted better protection from attack. However, the firewall in XP SP2 was missing some key features that have been included in Vista Windows Firewall.



As Windows Server 2008 is built from the same code base as Windows Vista, all described settings are valid for Windows Vista and Windows Server 2008, even if only Windows Vista is mentioned

The Vista Windows Firewall knows three different configuration sets:

- Domain Profile
- Private Profile
- Public Profile

The 'Domain Profile' is automatically applied in Active Directory domain environments. In this Troubleshooting Guide we will describe the necessary configuration steps for using LOGINventory.

The default configuration of the Windows Firewall policy in 'Domain Profile' and 'Private Profile' allows the following incoming exceptions:

- Core Networking
- Network Discovery
- File and Printer Sharing

**LOGINventory** performs an inventory using the following methods during an IP-Scan:

- Ping / ICMP (obligatory) (obligatory)
- Remote Registry based on File and Print Services (obligatory)
- WMI based on RPC (optional)

By default, the 'Remote Registry' service is not started automatically. This needs to be changed. In order to take a complete inventory from a Vista PC, the Windows Firewall configuration must be adjusted to fulfill these requirements.

#### 5.1.1 Windows 7 and Vista Editions

**Windows 7 Home** and **Vista Home** versions cannot be scanned remotely due to missing APIs (just like **Windows XP Home**), but you may execute the program LOGINfo.exe locally. This needs no special configuration.

In this document the term '**Windows Vista and later**' covers

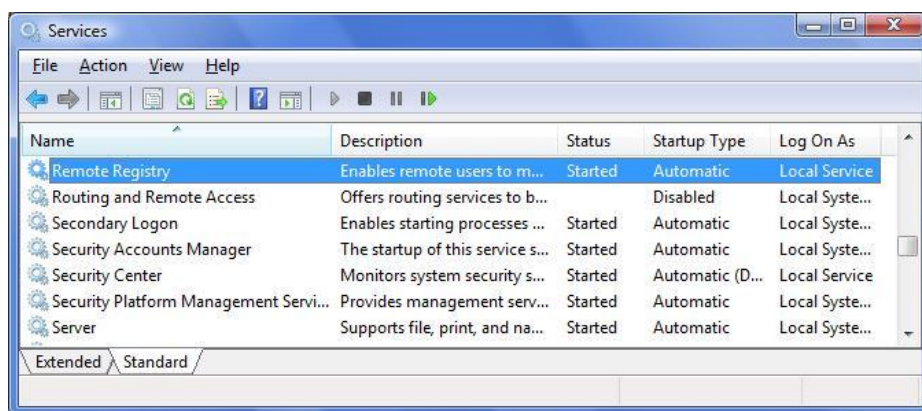
- **Vista Business,**
- **Vista Enterprise,**
- **Vista Ultimate,**
- **Windows 7 Professional,**
- **Windows 7 Enterprise** and
- **Windows 7 Ultimate** as well as
- **Windows Server 2008** including R2.

## 5.2 Local configuration of Windows Vista or later

The first method, which you could consider the 'traditional' or basic management method, will be familiar to anyone who has managed Windows XP in the past.

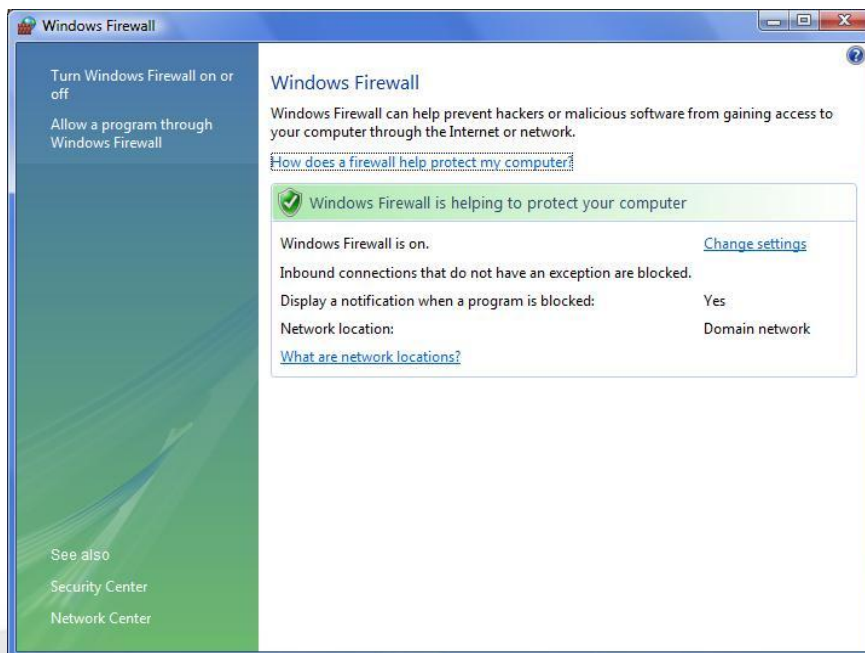
First of all, make sure that the services 'Server' and 'Remote Registry' are started automatically, by navigating to:

- Start
  - Control Panel
  - Administrative Tools
  - Services



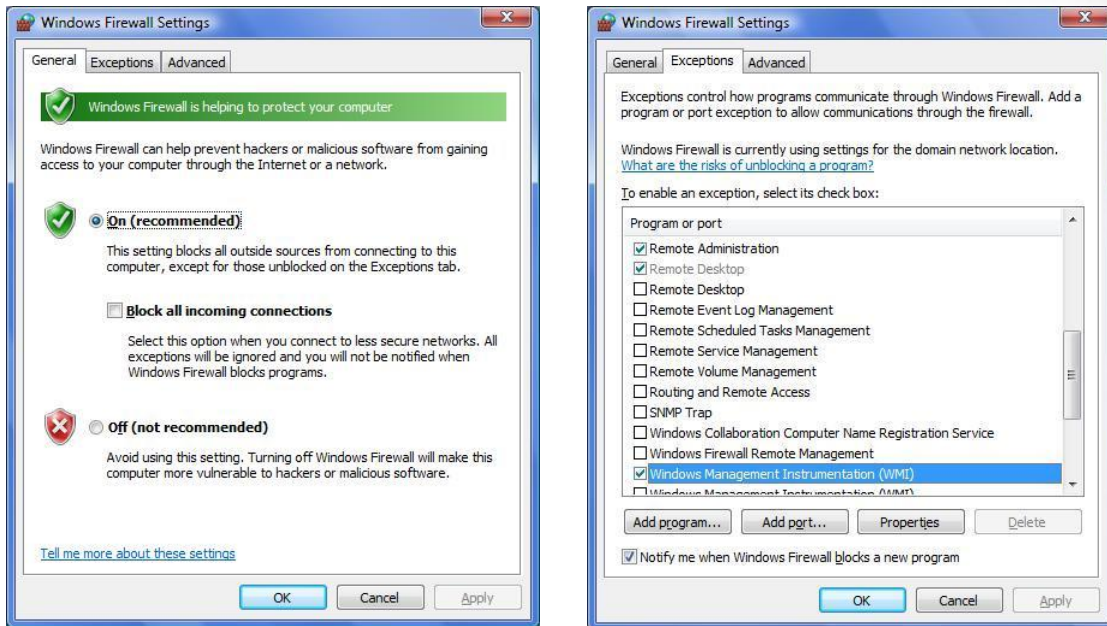
In Vista, the Windows Firewall management interface can be found at

- Start
  - Control Panel
  - Windows Firewall:



To change your firewall settings, select the Change settings option.


This option opens up the Windows Firewall Settings window. When you open this window, the General tab is selected.




The Exceptions tab provides a way for you to exclude specific services or TCP/UDP ports from being subject to blocking by Windows Firewall.

On a Vista or later PC to be inventoried you should enable the following exceptions:

- Remote Administration
- Windows Management Instrumentation (WMI)
- File and printer Sharing
- Remote Desktop



The Remote Desktop interface is not used by any LOGINInventory module. However, it may be used by any applications invoked from MMC task pad.



Windows 7 editions do not have a predefined rule named 'Remote Administration'. Please use 'Remote Service Administration' instead

## 5.2.1 Windows Vista or later in Workgroups

If you want to run LOGINventory on Windows Vista or later in a Workgroup environment, e.g. on computers not joined to a Domain, you have to consider that User Account Control (UAC) protects remote connections per default:

When a user who is a member of the local administrators group on the target remote computer establishes a remote connection, it **will not connect as a full administrator**. The user has no elevation potential on the remote computer, and the user cannot perform administrative tasks.

Only when a user who has an **Active Directory Domain user** account connects remotely to a Windows Vista or later computer and the domain user is a member of the Administrators group, it will run with a full elevated administrator access token on the remote computer, and UAC will not be in effect.

To disable UAC remote restrictions, follow these steps:

- Start **regedit**
- Navigate to following registry subkey:  
`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
- If the **LocalAccountTokenFilterPolicy** registry entry does not exist, follow these steps:
  - On the **Edit** menu, point to **New**, and then click **DWORD Value**.
  - Type **LocalAccountTokenFilterPolicy**, and then press ENTER.
- Set **LocalAccountTokenFilterPolicy** to 1 (= build an elevated token)
- Exit Registry Editor.

If this value does not exist it defaults to '0' (= build a filtered token).

For more information please read:

<http://support.microsoft.com/kb/951016>.

### 5.3 Configuration by using Group Policy Objects

To centralize the configuration of large numbers of computers in an organization network that use the Active Directory® service, Windows Firewall settings for computers running Windows Vista or later can be deployed through Computer Configuration Group Policy. A new set of Computer Configuration Group Policy Windows Firewall settings allows a network administrator to configure Windows Firewall operational modes, excepted traffic, and other settings using a Group Policy Object.

Group Policy updates are requested by the domain member computer. This is therefore treated as solicited traffic that is not dropped even when the Windows Firewall is enabled.

When you configure Windows Firewall in an organization network using Group Policy, some of the local Windows Firewall configuration options can be greyed-out and marked as unavailable, even for local administrators.

When using the new Windows Firewall Group Policy settings, you can configure three profiles:

- Domain Profile
- Private Profile
- Public Profile

We will now focus on the 'Domain Profile' settings and will enable the following exceptions:

- Remote Administration
- Windows Management Instrumentation (WMI)
- File and printer Sharing
- Remote Desktop

First you have to create a new Group Policy Object, e.g. 'Vista':

- Log on to a Windows Vista or later computer
  - either as a member of the Domain Administrators security group, or
  - the Enterprise Administrators security group, or
  - the Group Policy Creator Owners security group.
- From the desktop, click 'Start', click 'Run', type `GP.MSC`, and then click OK.

In the Group Policy Management tree navigate to

*'Your Forest'*  
→ *'Your Domain'*  
→ *'Your OU'*

where the 'Vista' GPO should be created.

If you right-click the OU and select 'Create a GPO in this domain and link it here' the Group Policy Object Editor will start after specifying a meaningful name, e.g. 'Vista'.

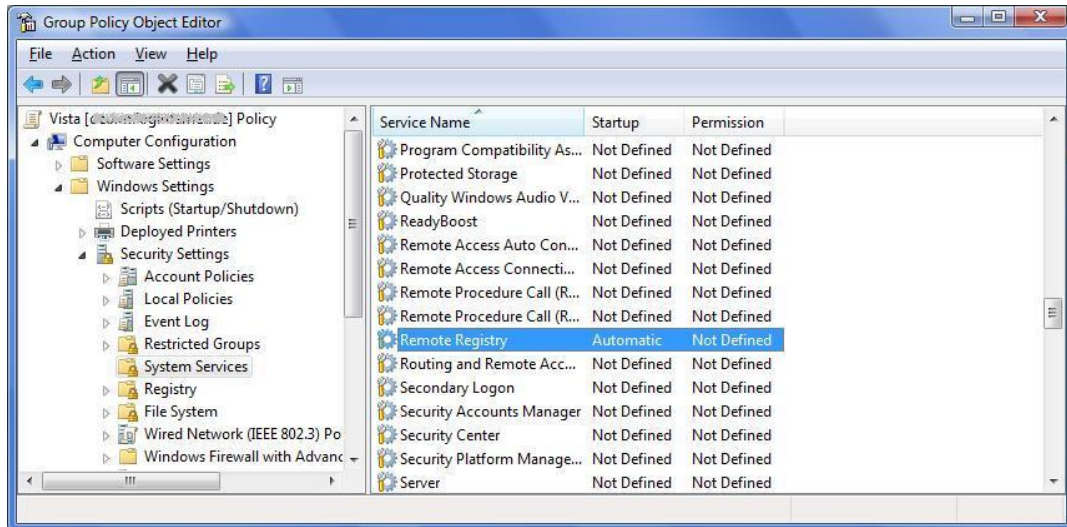
### 5.3.1 Autostart Remote Registry

In the Group Policy Object Editor navigate to  
*Computer Configuration*

→ *Windows Settings*

→ *Security Settings*

→ *System Services*



- Double-click on 'Remote Registry'
- Define this policy
- Select 'Automatic'
- Click 'OK'



### 5.3.2 Windows Firewall exceptions

In the Group Policy Object Editor navigate to

*Computer Configuration*

→ *Windows Settings*

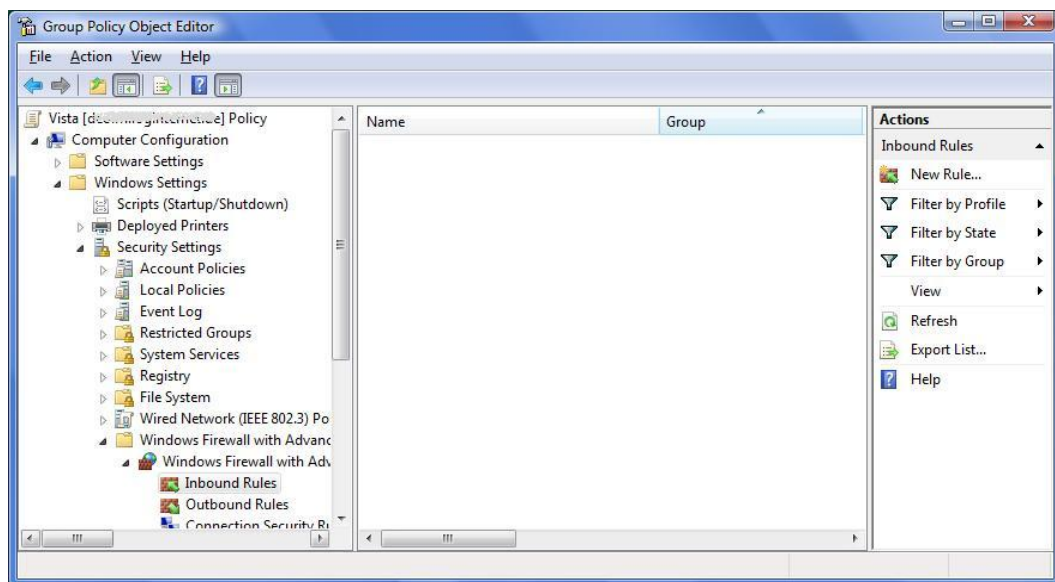
→ *Security Settings*

→ *Windows Firewall with Advanced Security*

→ *Windows Firewall with Advanced Security*

→ *Inbound Rules.*

You will probably see no Inbound Rule defined.



#### 5.3.2.1 Remote Administration exception

The Remote administration exception allows you to specify whether computers running Windows Vista can be remotely administered by applications that use TCP ports 135 and 445 (such as MMC).

Services that use these ports to communicate are using Remote Procedure Calls (RPC) and Distributed Component Object Model (DCOM) to access remote hosts. In effect, Windows Firewall adds SVCHOST.EXE and LSASS.EXE to the program exceptions list and allows those services to open additional, dynamically assigned ports, typically in the range of 1024 to 1034.

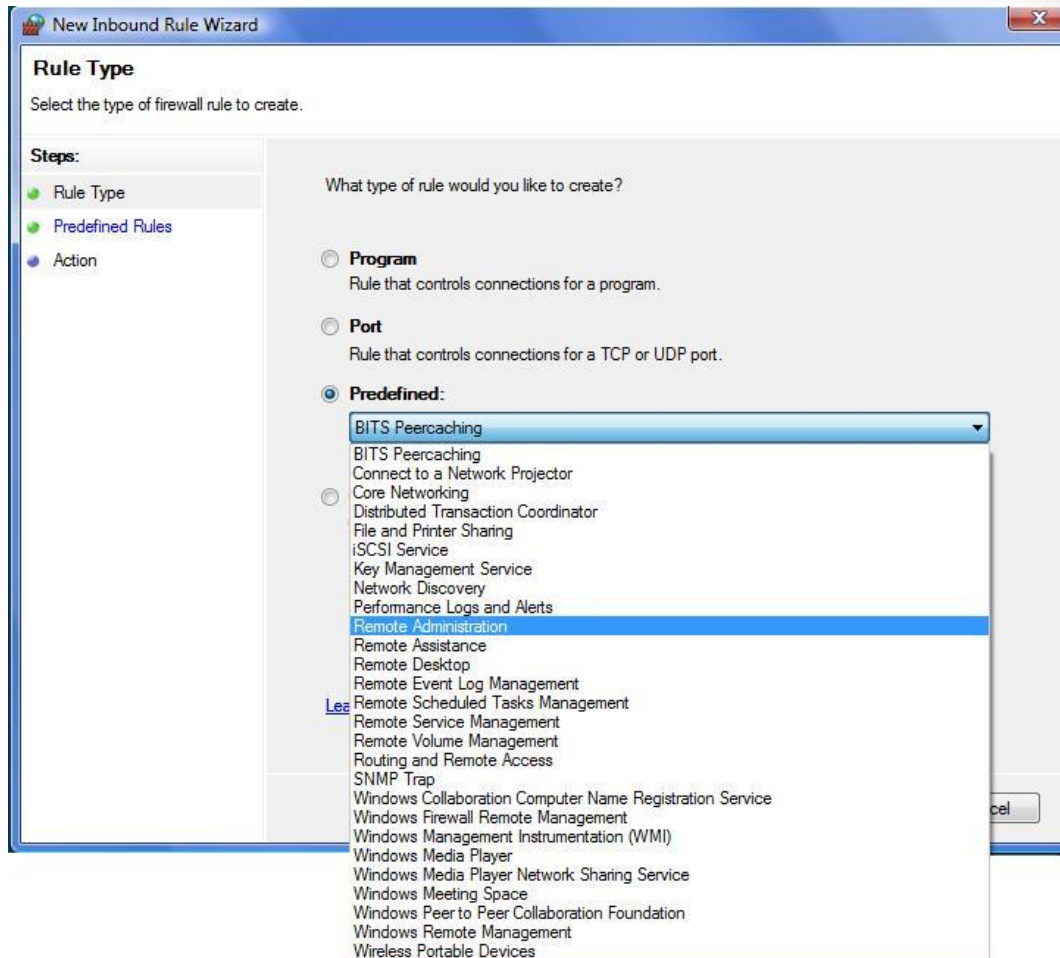


The RPC interface is a well-known target for viruses such as 'Blaster' or 'Sasser'.

By configuring this exception in the Domain Profile only it is not enabled if the parent Active Directory Domain cannot be connected.

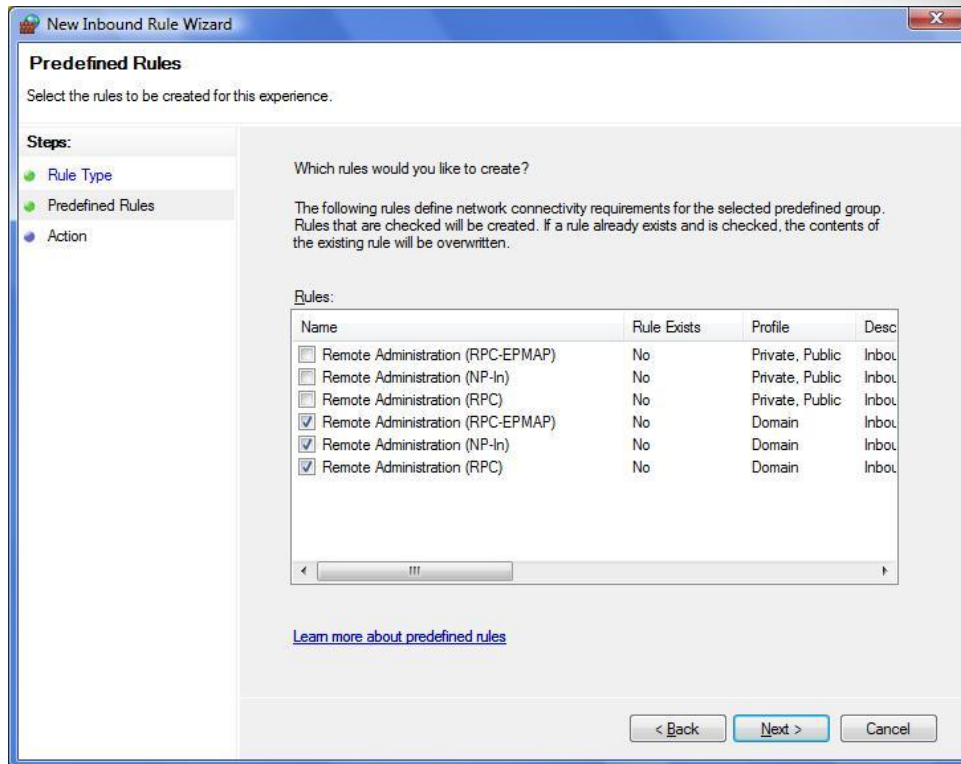
Click 'New Rule' in the Actions Pane, and the 'New Inbound Rule Wizard' will start.

Now click 'Predefined' and select 'Remote Administration' from the predefined rules pull down menu.

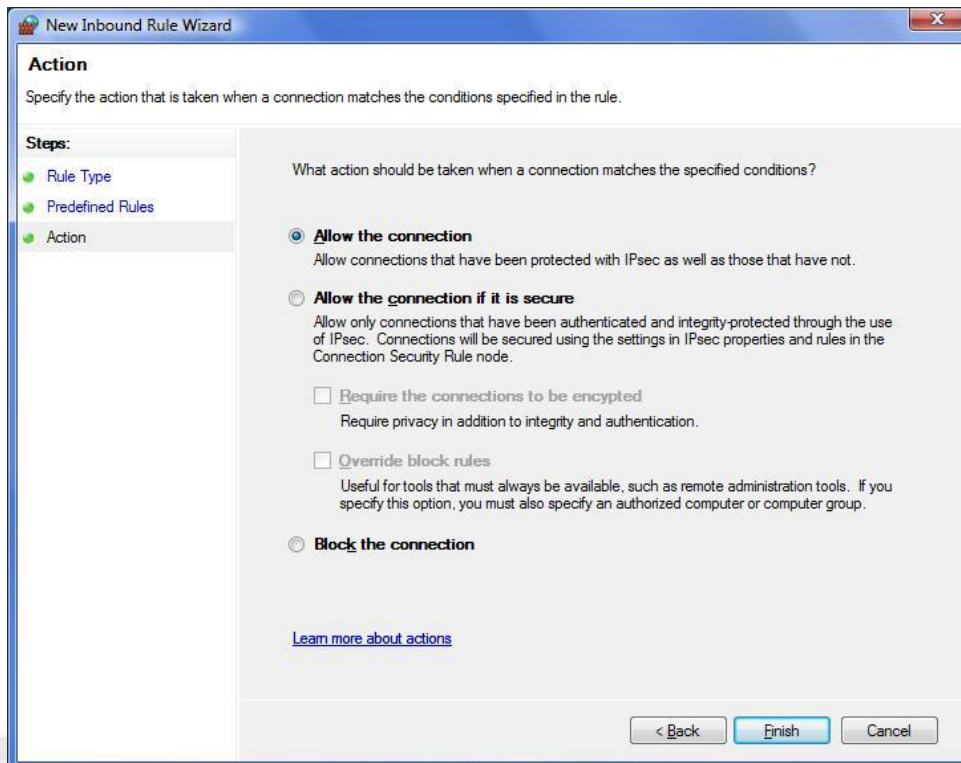


Windows 7 editions do not have a predefined rule named 'Remote Administration', but it is available on Windows Server 2008 (R2).

This exception is needed for the Domain Profile only, so please uncheck Private and Public Profile.



Finally, you select 'Allow the connection' and click on 'Finish'.



### 5.3.2.2 WMI exception

To enable this exception in Domain Profile, repeat the steps above and select *Windows Management Instrumentation (WMI)* from the predefined rules menu.



By configuring this exception in the Domain Profile only, it will be enabled only if the parent Active Directory Domain can be connected.

### 5.3.2.3 File and Printer Sharing exception

To enable this exception in Domain Profile, repeat the steps above and select *File and Printer Sharing* from the predefined rules menu.



By configuring this exception in the Domain Profile only, it will be enabled only if the parent Active Directory Domain can be connected.

### 5.3.2.4 Remote Desktop exception

To enable this exception in Domain Profile, repeat the steps above and select *Remote Desktop* from the predefined rules menu.



If Remote Desktop connections are allowed, TCP port 3389 is opened.

When you're done creating your new rules, they will appear in the list of rules on the main firewall configuration window.

### 5.3.3 Additional settings to run LOGINventory on Windows Vista or later

If you want to install and run LOGINventory module LOGINquiry on Windows Vista or later, we recommend the following additional settings to let it act just like on previous Windows versions.

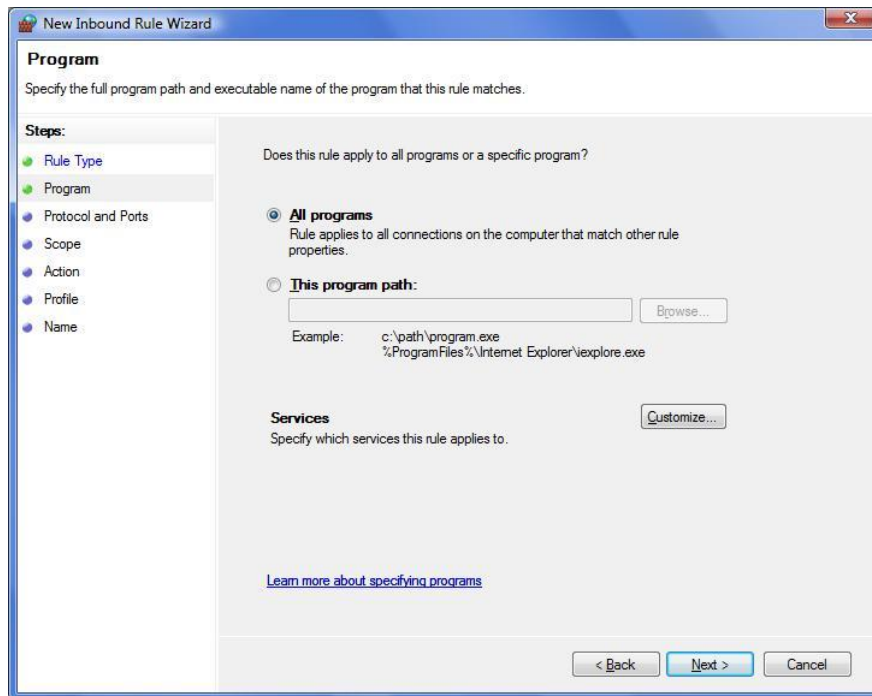
- Define ICMPv4 Exceptions (required)
- Disable Virtualizing of failed file and registry writes
- Disable Admin Approval mode for Administrators

You may define these policy settings within the same Group Policy Object which is used to assure proper client scanning, or within a separate one.

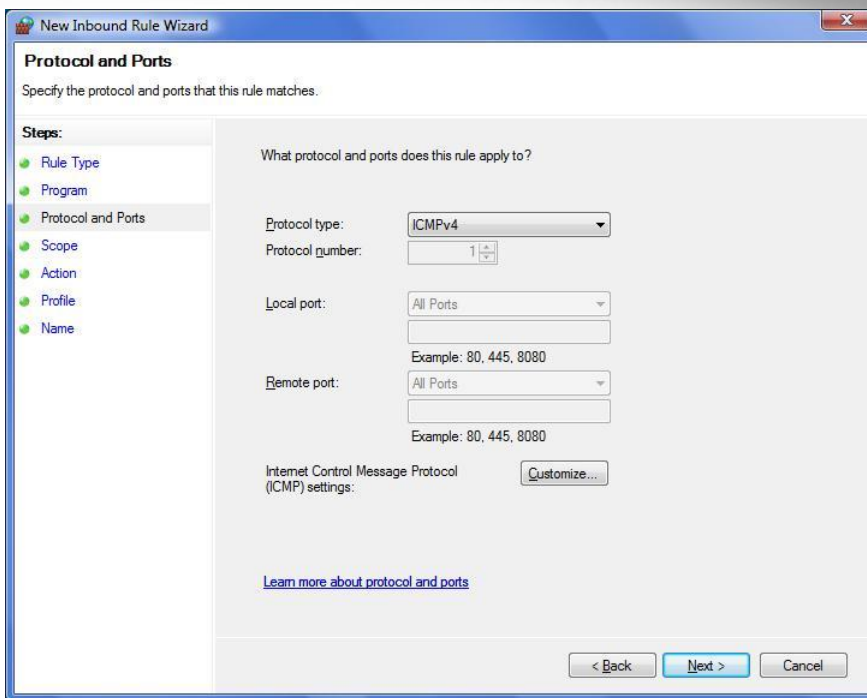
### 5.3.3.1 ICMPv4 exceptions

Different from the former Windows XP SP2 firewall, ICMP exceptions are no longer predefined nor allowed.

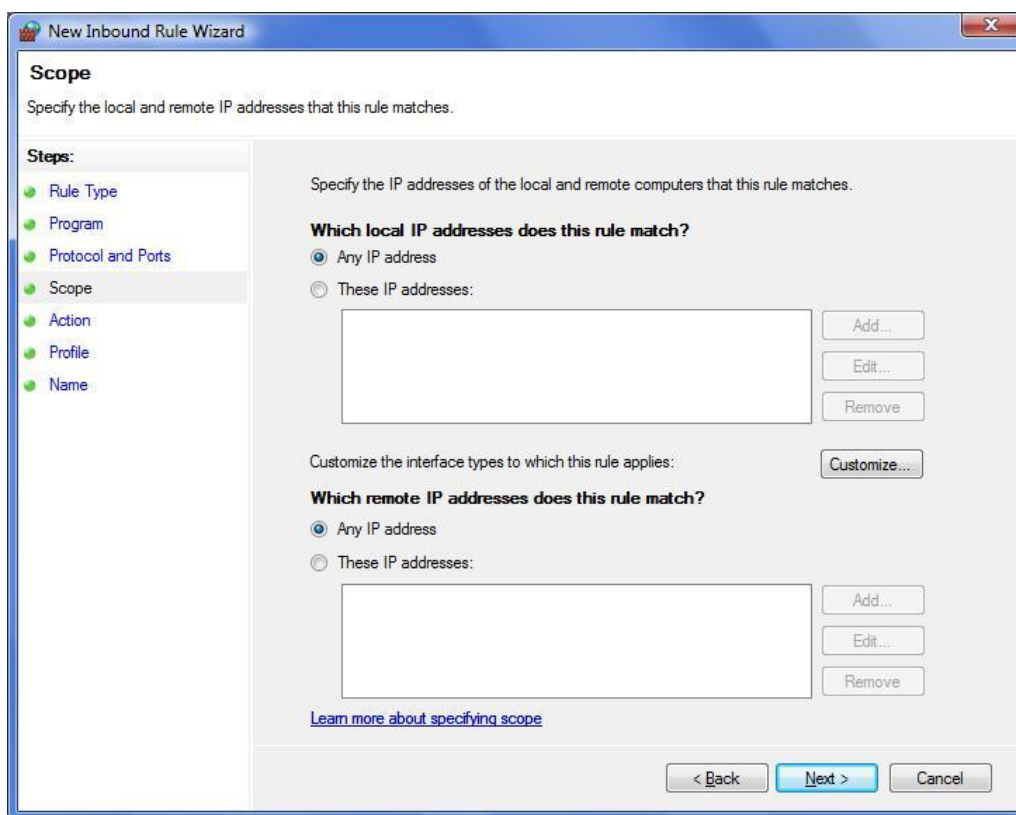
To define this exception, start the 'New Inbound Rule Wizard' again by clicking 'New Rule', but now choose 'Custom' and on the next menu 'All programs'; continue with 'Next'.



Now select protocol type 'ICMPv4' from Protocol type pull down menu, continue with 'Next'.

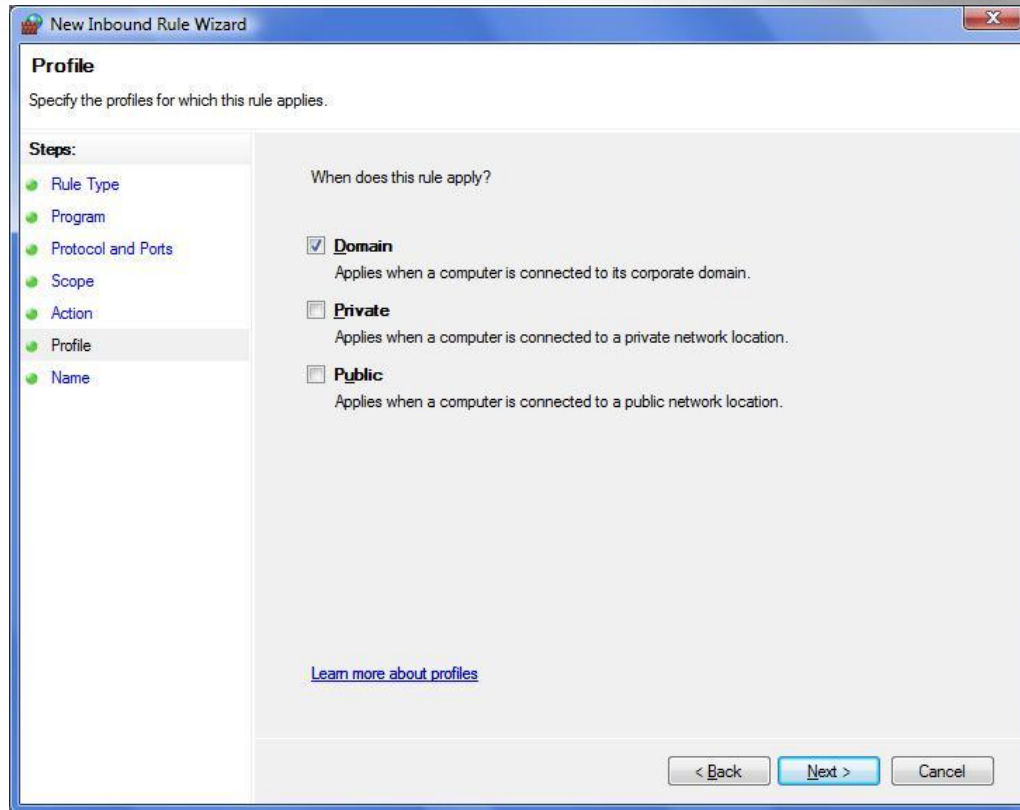


You have to allow PING from and to any address you may want to take an inventory.



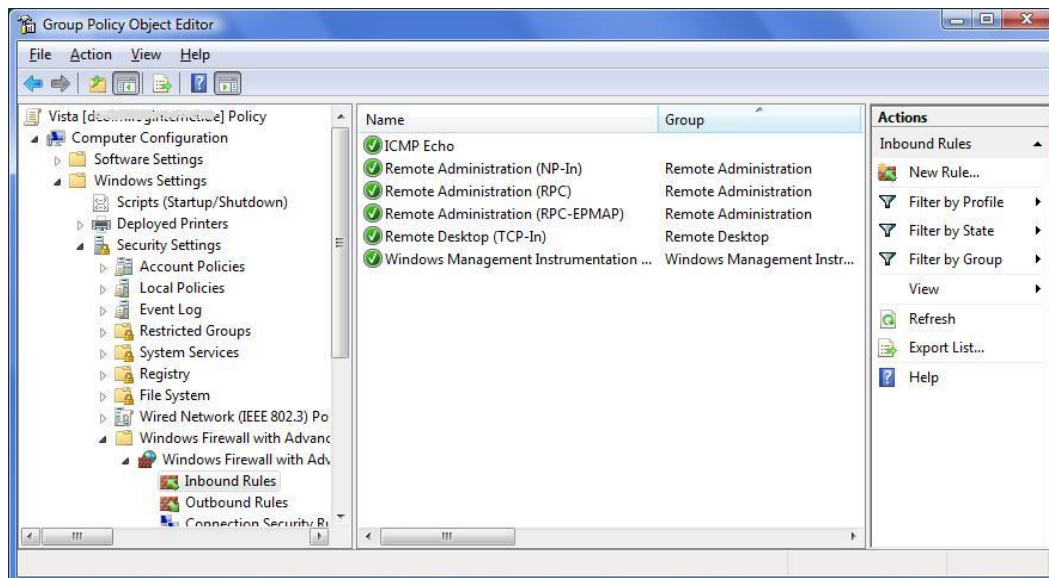
As usual, you have to allow the connection on the next menu page.

Now you will be asked: 'When does this rule apply?' In 'Profile' please only select 'Domain':



On the final menu page you have to specify a name for this rule, e.g. 'ICMP Echo' and press 'Finish'.

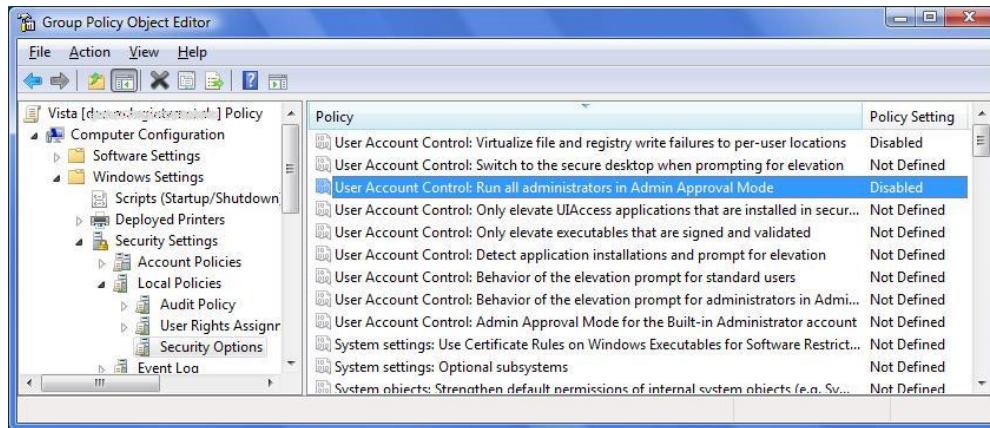
Now you should have defined the following rules:



### 5.3.3.2 Adjusting User Account Control (UAC)

In Group Policy Object Editor – which is still running – navigate to *Computer Configuration*

- *Windows Settings*
- *Security Settings*
- *Local Policies*
- *Security Options*



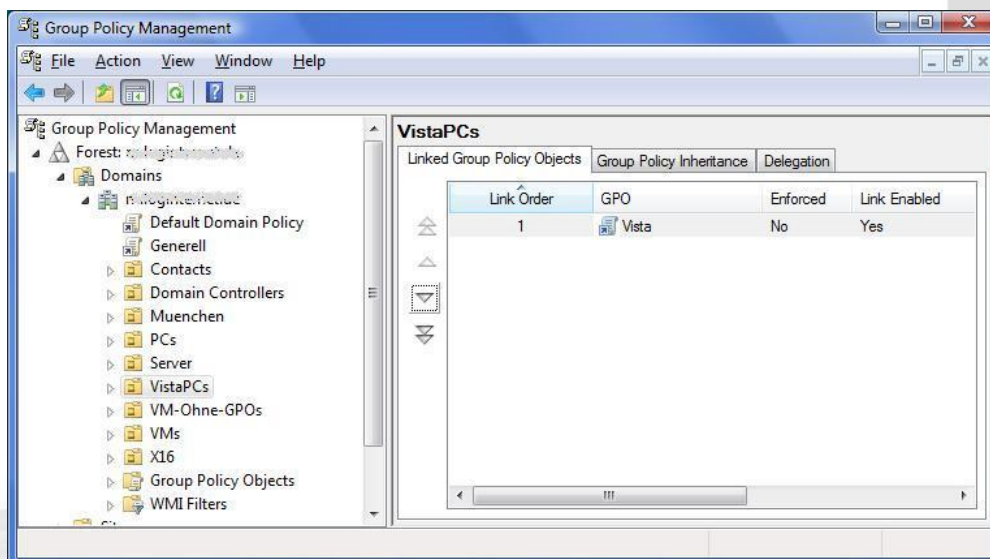
**Deactivate** both of the next settings:

- User Account Control: Virtualize file and registry write failures to per-user locations
- User Account Control: Run all administrators in Admin Approval Mode

### 5.4 Applying Group Policy Settings to PCs

The new created Group Policy Object 'Vista' is now ready and linked to the desired OU e.g. 'VistaPCs'. Every PC residing under this OU will now start using the GPO settings from your just now created GPO 'Vista'.

By default, Group Policies are updated when the PC starts up and subsequently in the background every 90 minutes, with a random offset of 0 to 30 minutes.



## 6 Remote Assistance

Remote Assistance provides a way for users to get the help they need and makes it easier and less costly for corporate helpdesks to assist their users.

### 6.1 Unsolicited Remote Assistance

Unsolicited remote assistance is initiated by an Expert user and is used to offer Remote Assistance to a Novice user. The Expert should know the Novice's machine name or IP address to view the novice's desktop. If the Expert needs to share control of the Novice's machine, the Expert can request control and the Novice can accept or deny the request.

LOGINventory5 is able to invoke an unsolicited Remote Assistance session to a selected PC if it is running on a Windows Vista or later operating system (e.g. Windows Server 2008, Windows 7, etc...). The operating system of the Novice user can be Windows XP or later.

For this feature to work you must fulfill some prerequisites:

- The Expert must be member of a 'Helpers' group
- Unsolicited Remote Assistance must be allowed on the target PC
- Both PCs and users (Expert and Novice) must be member of an AD domain

In AD Domain you can reach this target by defining a GPO:

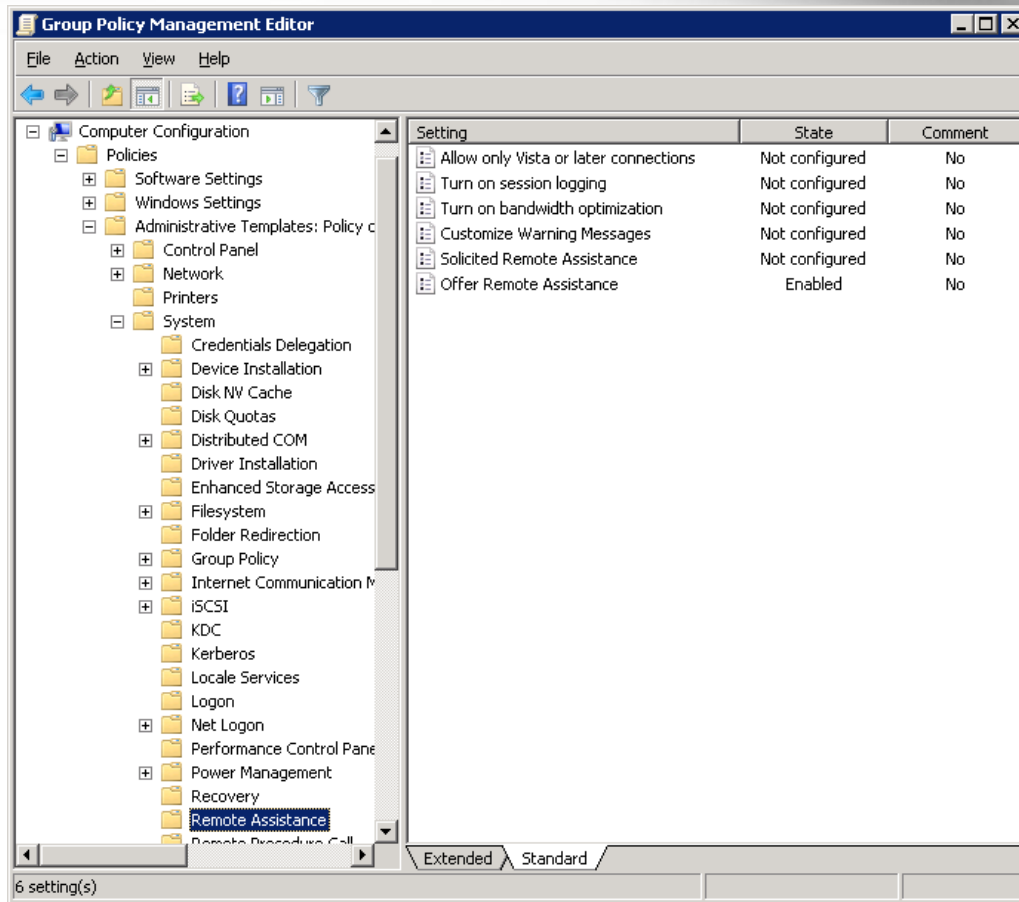
### 6.2 Remote Assistance Group Policies

Remote Assistance may be configured using the group policies located in the following container:

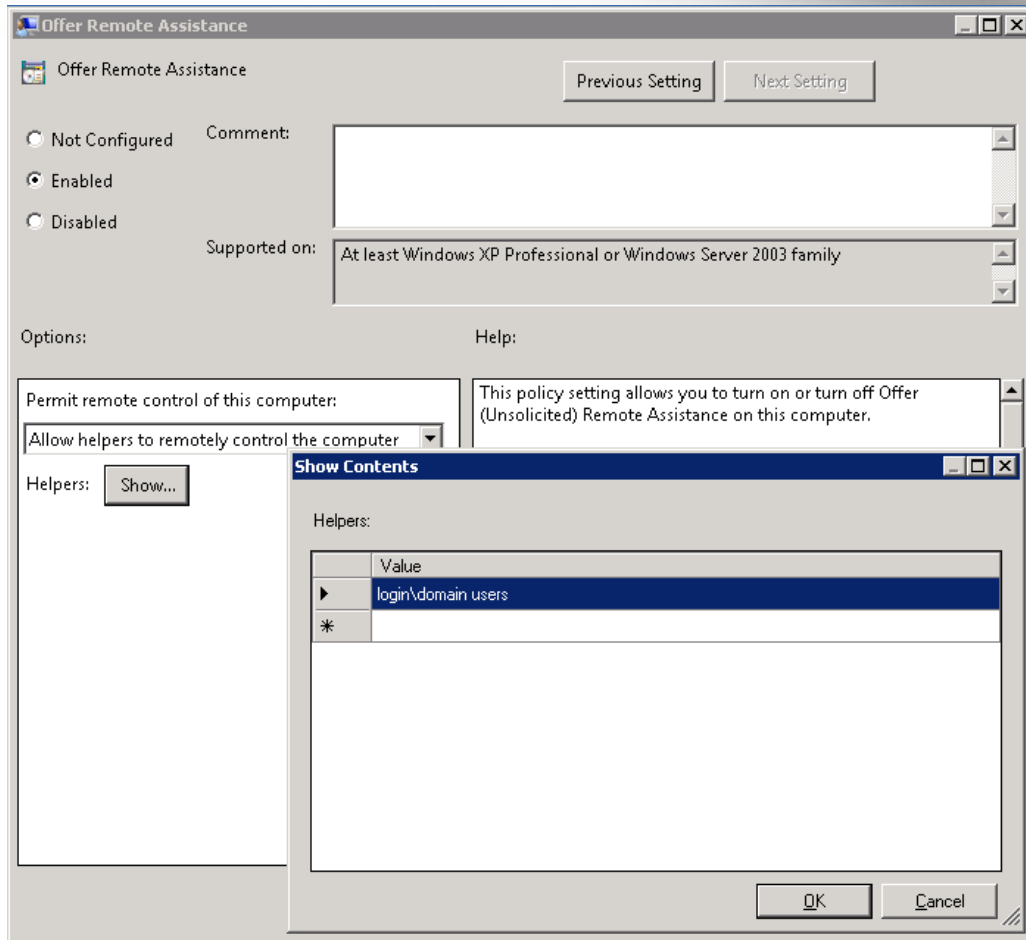
*Computer Configuration*  
→ *Administrative Templates*  
→ *System*  
→ *Remote Assistance*

The policies write registry values to the following area of the registry:

`HKLM\Software\Policies\Microsoft\Windows NT\Terminal Services`



To define the appropriate 'Offer Remote Assistance' Policy, create (or edit) a Group Policy and navigate to 'Remote Assistance' policy as show in the above picture, then double-click on 'Offer Remote Assistance'.



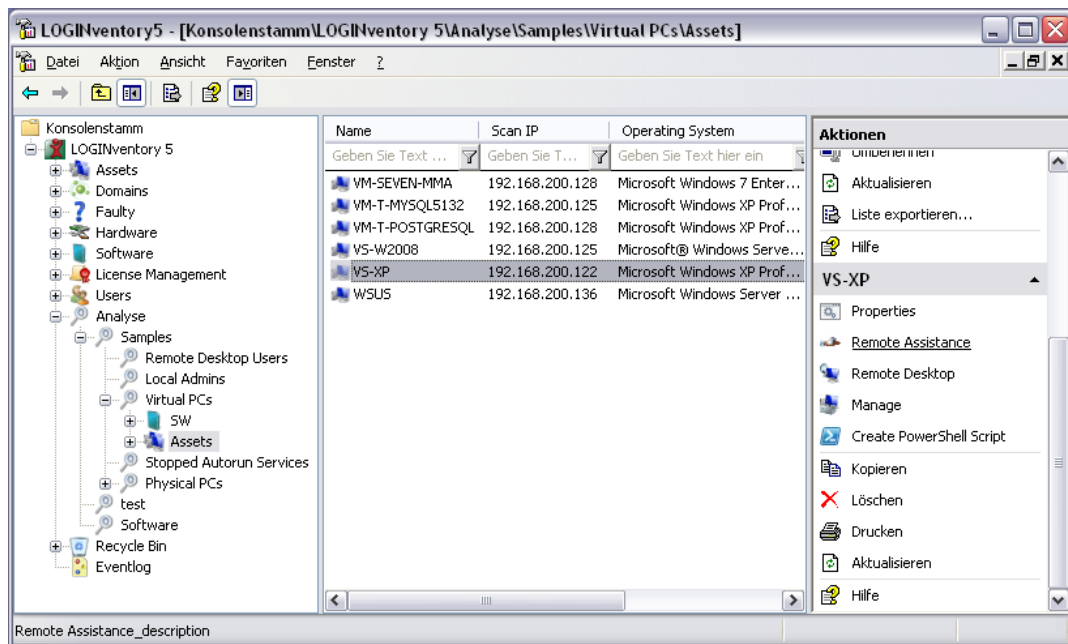
Switch on 'Enabled' and after this you have to define who has permissions to offer assistance by click on the 'Show...' button. In our example we have chosen to allow all 'login\domain users' to act as Helpers. You may adjust this to your needs.

After you have applied this policy to a group of computers, the defined Helpers group(s) are able to offer Remote Assistance to these computers.

### 6.3 Remote Assistance in LOGINventory Management Console

Remote Assistance is available as an action in the Actions pane, if the focus is set on a PC.

You will be able to offer Remote Assistance to the selected PC, if all prerequisites described previously in this chapter are fulfilled.



With LOGINventory version 5.0, User Account Control (UAC) must be switched off for Remote Assistance to work; otherwise you will receive the error:

*'The requested operation requires elevation'.*

This has been fixed in version 5.1.

## 7 SNMP

For testing the SNMP functionality, you could use the freeware tool 'Net-SNMP'.

Using this description, you'll see how to test the SNMP connection and how to set-up a configuration of SNMP v1/v2c for the automatic use in LOGINquiry.

Further information about configuration of SNMP v3 you'll find in the [installation manual](#).

### 7.1 Installation of additional components

Log on as local administrator on your LOGINventory PC.

Download and install the following with default configuration in this order:

1. Net-SNMP from: <http://www.net-snmp.org/download.html>
2. ActivePerl (optional – if scripting is desired)  
<http://www.activestate.com/activeperl/downloads>



**Note:**

There are different downloads available depending on your platform (x86, AMD64).

### 7.2 Test explicit credentials via Net-SNMP

Assumed the device you want to inventory, activated SNMP V1 (or V2c), used the community 'public' and had an IP address like '192.168.1.2', you could open a command prompt and enter:

```
snmpwalk -v1 -c public 192.168.1.2 system
```

or

```
snmpwalk -v2c -c public 192.168.1.2 system
```

Check the output for any errors.



**Hint:**

The command `snmpwalk` with the OID 'system' can be used to check the connection to the device. If you receive no information, SNMP is not installed or not started or not configured.



**Caution:**

Net-SNMP commands are case-sensitive!

### 7.3 Define default setting for Net-SNMP

Open the configuration file from Net-SNMP, using a text editor. If you installed Net-SNMP with default settings, you'll find this file as

```
'C:\usr\etc\snmp\snmp.conf'
```

Usually there are some existing lines even after a fresh install:

```
mibdirs C:/usr/share/snmp/mibs
persistentDir C:/usr/snmp/persist
tempFilePattern C:/usr/temp/snmpdXXXXXX
```

Now enter the following lines and save the file:

```
# LOGINventory: Default credentials sample
defVersion 1
defCommunity public
```

Using the configuration file from Net-SNMP will define the parameter as default values.

This way, you may set the SNMP communities you want to read in the configuration file.

You'll find a description of valid SNMP parameters at:

*Start Menu*

→ *All Programs*

→ *Net-SNMP*

→ *Net-SNMP Help*

+ *Configuration*

→ *snmp.conf*

### 7.4 Test default credentials

At the LOGINventory computer open a command prompt and enter:

```
snmpwalk 192.168.2.1 system
```

Check the output for any errors. You should get the same result as above.

## 7.5 Use SNMP v1/v2c with LOGINventory

Open a command prompt and navigate to the LOGINventory program directory, e.g.

```
CD /D C:\Program Files\LOGIN\LOGINventory5
```

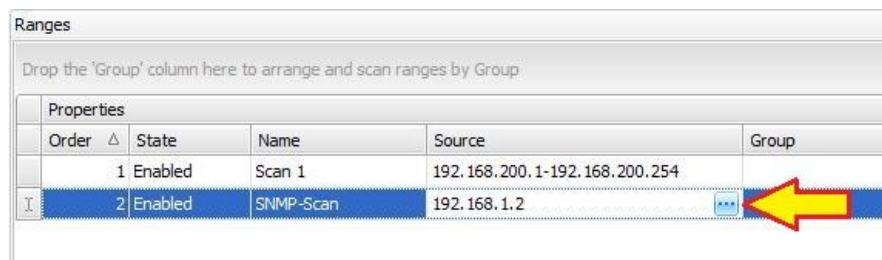
Start LOGINfoR and specify using of default Net-SNMP credentials only

```
LOGINforR !192.168.2.1 C:\temp /SNMP /NETSNMPCONF
```

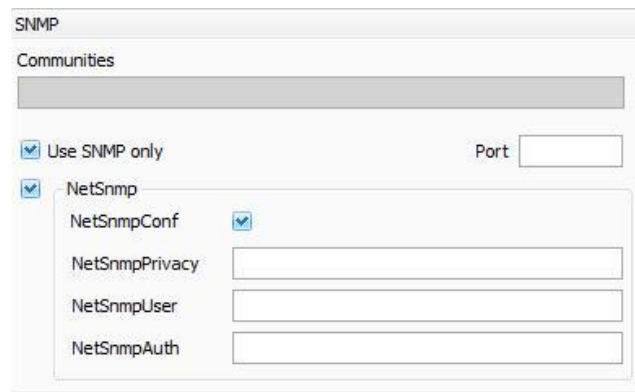
In this example the resulting .LI5 file will be placed in C:\temp. You can open this file with a text editor and look near the end for a line containing SCANRESULT.

If this is 1 or 2, everything is OK and you can specify scan range properties in LOGINquiry accordingly.

Open the property page for the scan range, using the '...' button.



select the 'Advanced' property page and there, activate the options 'NetSnp' and 'NetSnpConf'.



When you start a scan via LOGINquiry, the resulting .LI5 file is placed in the standard DATA directory and LOGINsert is started afterwards.



For configure SNMP v3 you'll find a description in the [installation manual](#).