

Windows XP SP2 Configuration for LOGINventory

Overview:

Prior to Windows XP SP2, Internet Connection Firewall (ICF) was active on connections which it was enabled when the ICF/Internet Connection Sharing (ICS) service was successfully started.

SP2 introduces a startup Windows Firewall policy to perform stateful packet filtering. This allows the computer to perform basic networking startup tasks. These use Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) to configure the computer and to communicate with a domain controller to obtain Group Policy updates.

Once the Windows Firewall (WF)/Internet Connection Sharing (ICS) service is started (running?), it uses its own configuration and removes the startup policy. Startup policy settings cannot be configured.

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.

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 (mandatory)
- WMI based on RPC (optional)

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

Configuration of the Windows Firewall using Group Policy Objects

To centralize the configuration of large numbers of computers in an organization network that use the Active Directory® directory service, Windows Firewall settings for computers running Windows XP SP2 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 grayed out and unavailable, even for local administrators.

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

- **Domain Profile**
This is the set of Windows Firewall settings that are needed when a computer is connected to the network that contains an 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.

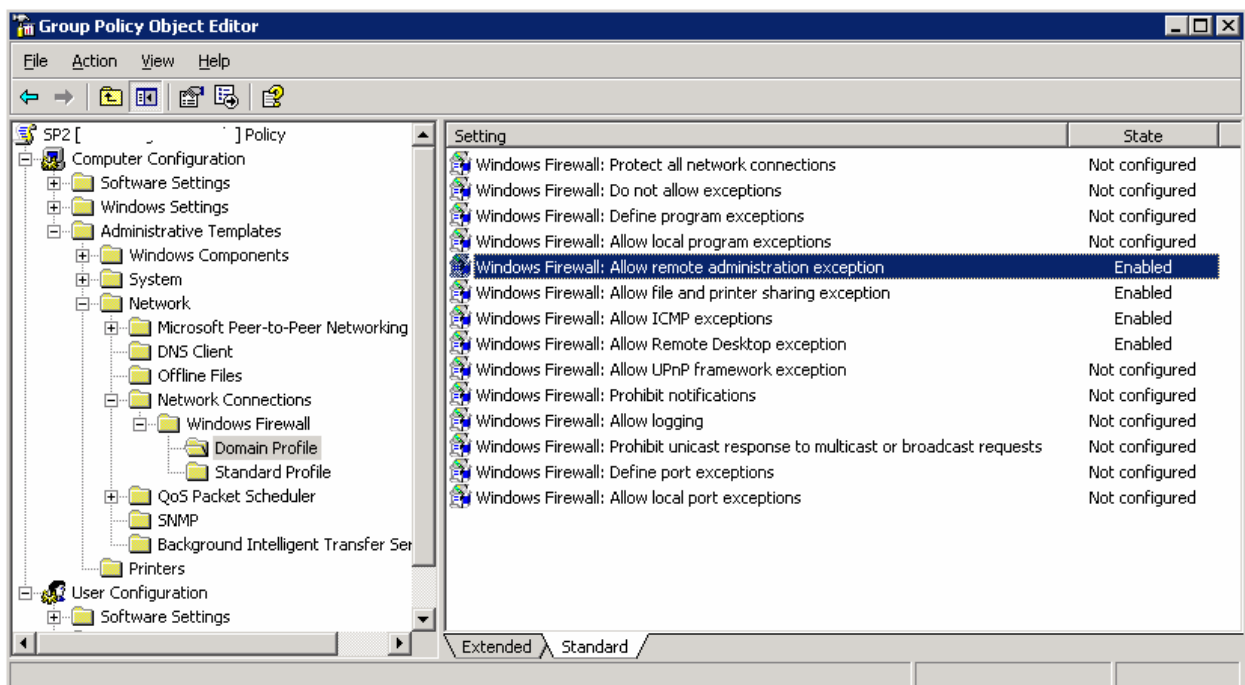
Configuration for LOGINventory:

First you must update Group Policy Objects with the New Windows Firewall Settings:

1. Log on to the Windows XP SP2 computer (either as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group).
2. From the Windows XP desktop, click Start, click Run, type mmc, and then click OK.
3. 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”).

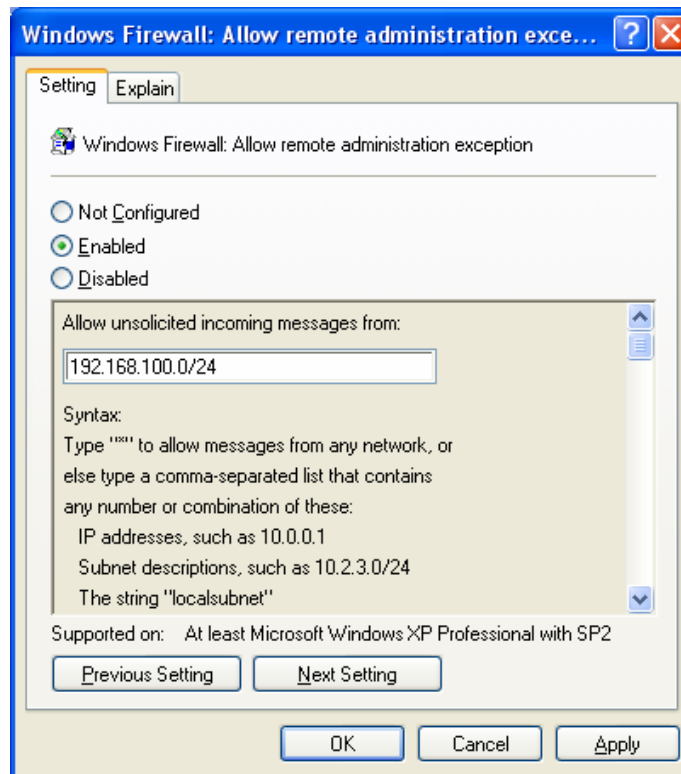
To start doing this, navigate to: “Computer Configuration / Administrative Templates / Network / Network Connections / Windows Firewall / Domain Profile”.



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

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

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



The **Windows Firewall: Allow remote administration exception**. This setting allows you to specify whether computers running Windows XP SP2 can be remotely administered by applications that use TCP ports 135 and 445 (such as MMC and WMI). 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.

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*, or one or more IPv4 addresses or IPv4 address ranges separated by commas. *LocalSubnet* allows connections only from the computer's Subnet.



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.

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

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

The **Windows Firewall: Allow file and print sharing exception**. This setting specifies whether or not the ports for file and printer sharing are open. Enabling this will open the following Ports:

UDP 137, UDP 138, TCP 139 and TCP 445

Allow unsolicited incoming messages from:

In **Allow unsolicited incoming messages from**, type * to specify traffic originating from any source IPv4 address or a comma separated list of sources. In our example "*" (all networks).



There is no known security risk with this interface.
LOGINquiry collects most of its information this way. This setting is Required.

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

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

The **Windows Firewall: Allow ICMP exceptions**. This setting allows 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*.

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

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

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

Allow unsolicited incoming messages from:

In **Allow unsolicited incoming messages from**, type * to specify traffic originating from any source IPv4 address or a comma separated list of sources. In our example 192.168.100.0/24



This interface is not used by any LOGINventory module. However, it can be used by applications invoked from MMC-Taskpad.
Not required.

For more information, see:

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