Agilent Technologies

Configuring Windows Firewall for Agilent MassHunter GC/MS Acquisition Software

The purpose of this document is to provide instructions on configuring Windows Firewall settings that allow Agilent MassHunter GC/MS Acquisition Software to work properly through a firewall. The instructions in this document apply to Windows 7.

Windows Firewall can help protect your computer from being accessed by hackers or malicious software through a network or the Internet. For this reason, Agilent recommends that you do turn *on* Windows Firewall and allow trusted programs, such as the ones required by MassHunter GC/MS Acquisition Software, to communicate through the firewall.

1 Turn on Windows Firewall

Windows Firewall is installed automatically with Windows Operating System. However, it may or may not be turned on depending on what you selected during **Set Up Windows** after the initial power on of your band new computer.

It is recommended that you select **Use recommended settings** in **Set Up Windows** (**Figure 1**).

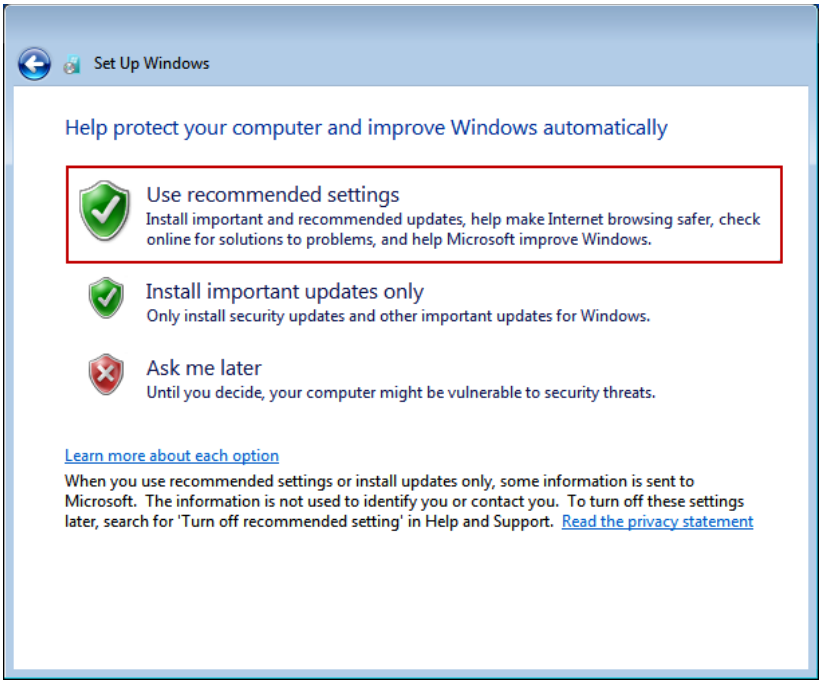

Figure 1 Set Up Windows after initial PC power on

When the **Use recommended settings** option is selected, the default firewall settings are:

- The firewall is on.
- The firewall is on for all network locations (Home or work, Public, or Domain).
- The firewall is on for all network connections.
- The firewall is blocking all inbound connections except those that you specifically allowed.

If you choose the **Ask me later** option in Setup Windows, Windows Firewall is turned *off* by default.

IMPORTANT: It is recommended that Windows Firewall be turned *on* to protect your computer.

To turn Windows Firewall on, perform the following steps.

1. Log on to your computer with administrator privileges.
2. Click on **Start > Control Panel > System and Security > Windows Firewall**. If you do not see **System and Security** in Control Panel, you can alternatively click **Windows Firewall**.
3. If you get a **Windows Firewall** window that looks like **Figure 2**, it means that the computer is being managed by your IT department. You will not be able to make changes to the firewall settings on your own. Please contact your IT department for assistance before continuing.

Figure 2 Windows Firewall managed by your IT department

4. If you get a **Windows Firewall** window that looks like **Figure 3**, click **Turn Windows Firewall on or off** on the left pane.

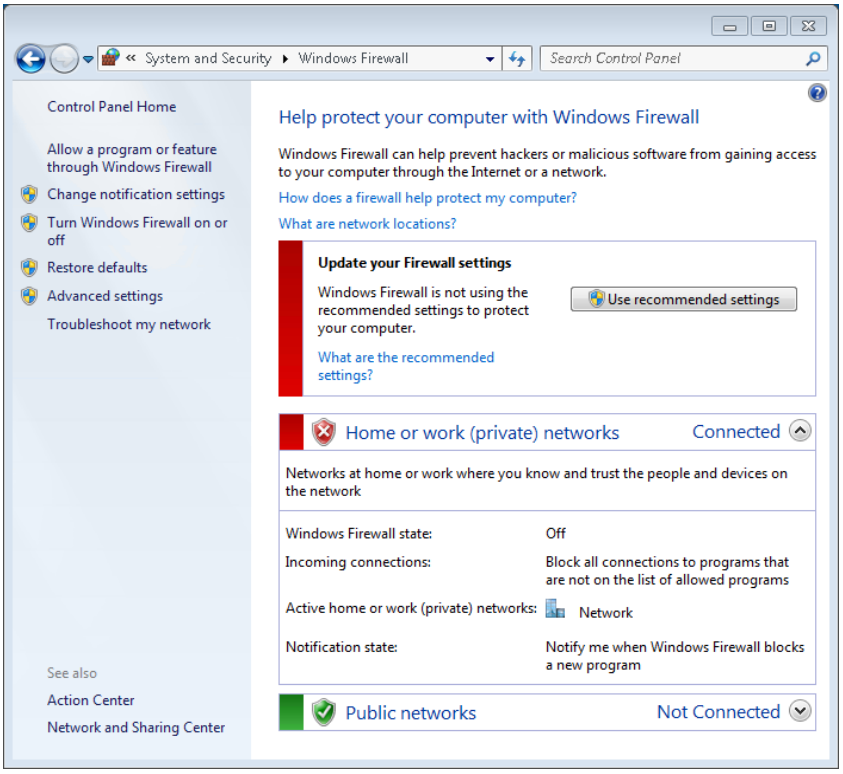

Figure 3 Windows Firewall off

5. In the **Customize Settings** window, select **Turn on Windows Firewall** and make sure **Notify me when Windows Firewall blocks a new program** check box is checked for each type of the network location that you use (**Figure 4**). Do *not* check **Block all incoming connections, including those in the list of allowed programs**.

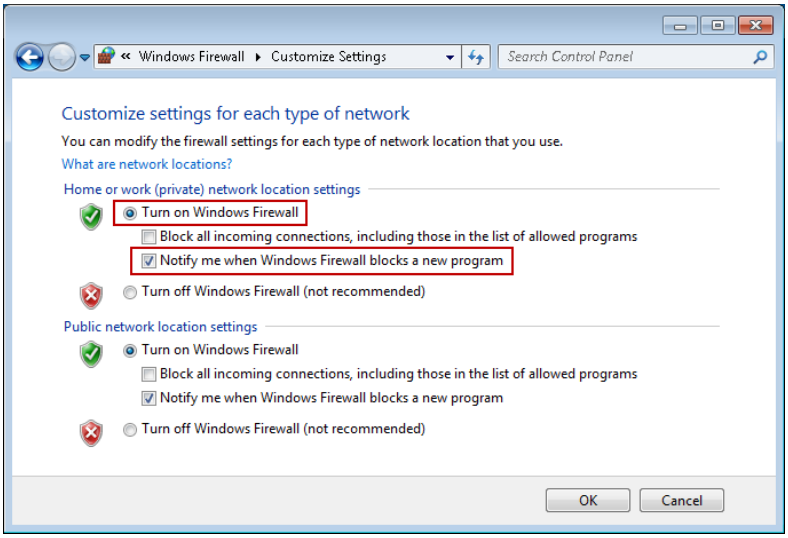

Figure 4 Customized Settings window

6. Click **OK**. Windows Firewall is now turned on with the recommended settings (**Figure 5**).

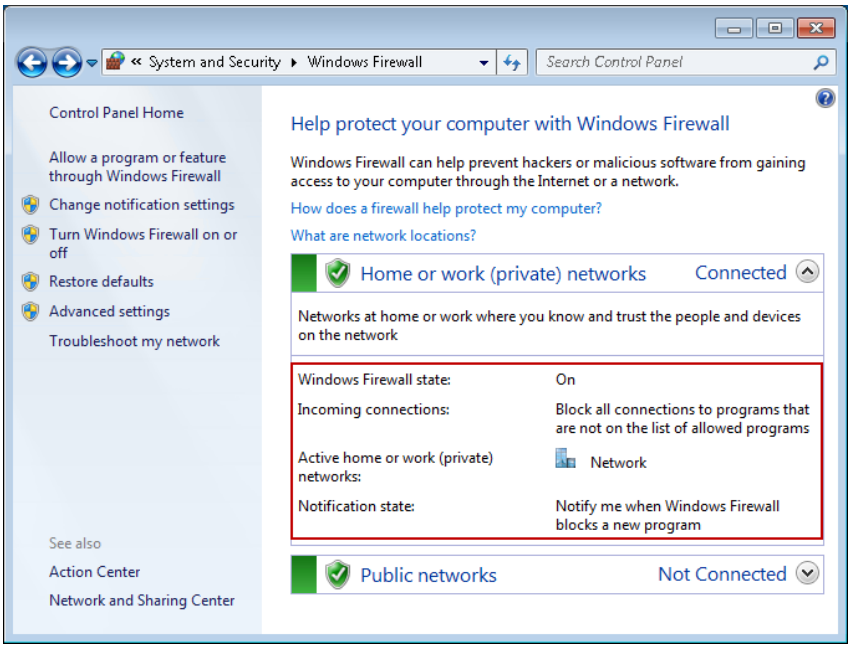

Figure 5 Windows Firewall on

With the **Notify me when Windows Firewall blocks a new program** option selected, when you run a program that is not on the allowed list, the **Windows Security Alert** window (**Figure 6**) appears prompting you to allow the blocked program through the firewall.

You should click **Allow access** if the program is from a trusted source. Refer to **Table 1** for a list of programs that need to be allowed through the firewall in order for Agilent MassHunter Acquisition software to work properly.

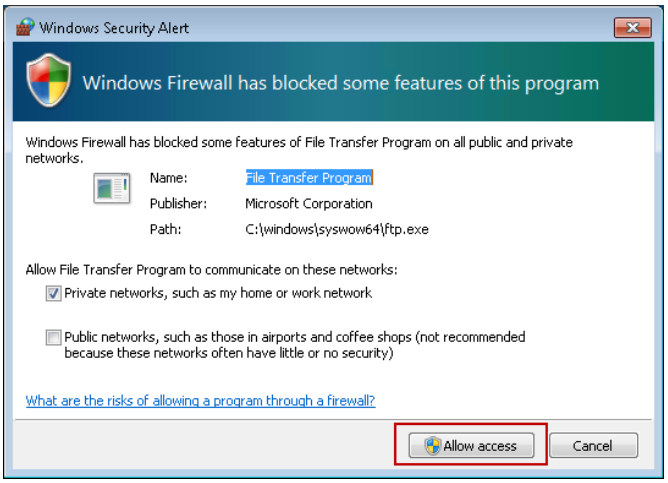

Figure 6 Notification of program blocked by Windows Firewall

2 Allow Programs and Features Through Windows Firewall

When Agilent MassHunter GC/MS Acquisition Software is installed on the computer, the software and all of its required components are automatically put on the list of allowed programs and features that can communicate through Windows Firewall.

If you are having issues communicating with GC/MS instruments through the firewall, you should verify that the required programs (see **Table 1**) for MassHunter GC/MS Acquisition software are properly added to the Windows Firewall allowed list.

Table 1 Programs required on Windows Firewall Allowed or Exceptions List

Programs	Paths
File Transfer Program	C:\windows\system32\ftp.exe
File Transfer Program	C:\windows\syswow64\ftp.exe
GCDriverEvents	N/A
httpdmsd tool	C:\GCMS\msexe\httpdmsd.exe
instrument control and calibration	C:\GCMS\msexe\msinsctl.exe
MSD Firmware Update	C:\GCMS\firmware\5973N\msupdate.exe
rpcinfo tool	C:\GCMS\msexe\rpcinfo.exe

If the required programs are not on the list, you will need to add them manually.

To add a program to the allowed list, perform the following steps.

1. In the **Windows Firewall** window (**Figure 3**) on the left pane, click on **Allow a program or feature through a firewall** and the **Allowed Programs** window appears.
2. In the **Allow Programs** window (**Figure 7**), if the program is in the **Allowed programs and features** list (also known as the Exceptions list), be sure to check the box next to the program and network location(s) you want to allow communication. Then click **OK**.

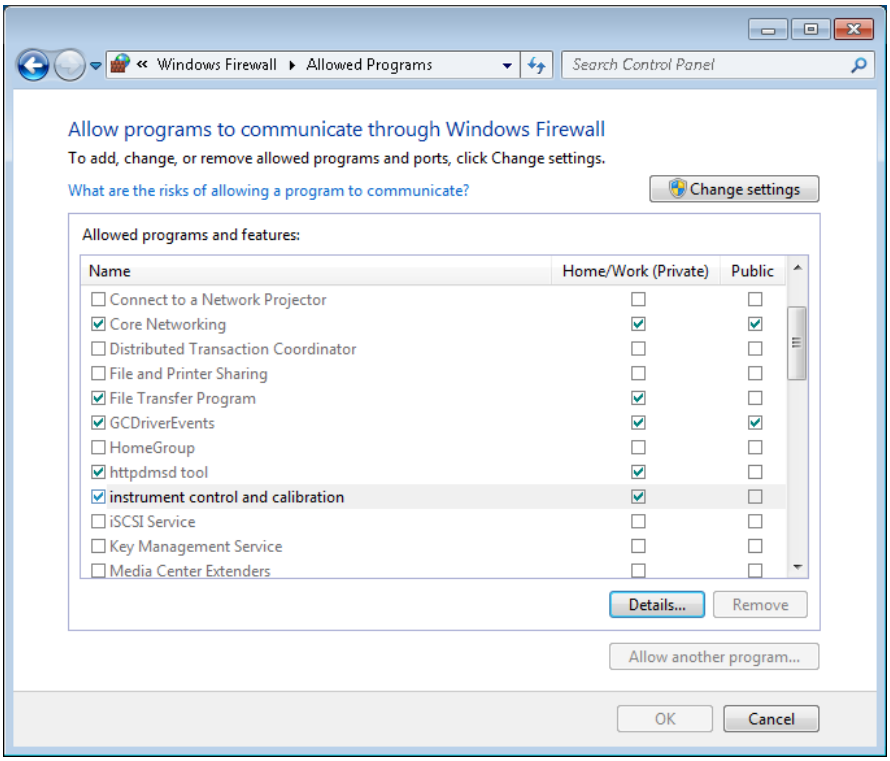

Figure 7 Allowed Programs window

3. If the program is not on the list of **Allowed programs and features**, you can add it to the list by performing the following steps:
    a) Click **Change settings** and then select **Allow another program** (Figure 7) and the **Add a Program** window (Figure 8) appears.

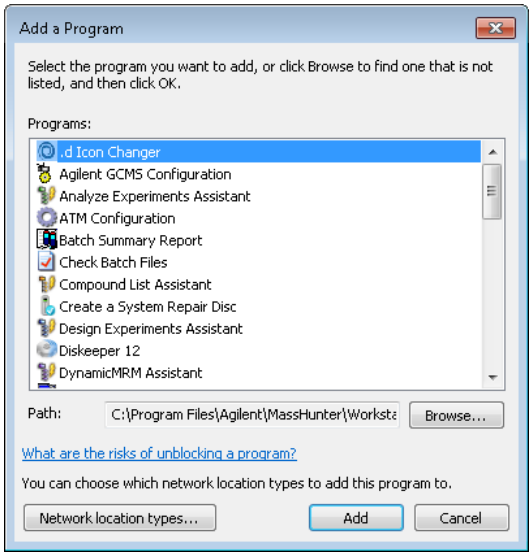

Figure 8 Add a Program window

b) Click **Browse** to open the **Browse** window.

c) In the **Browse** window (**Figure 9**), navigate to the path where the program is located (refer to **Table 1**), select the program file you want to add, and click **Open**.

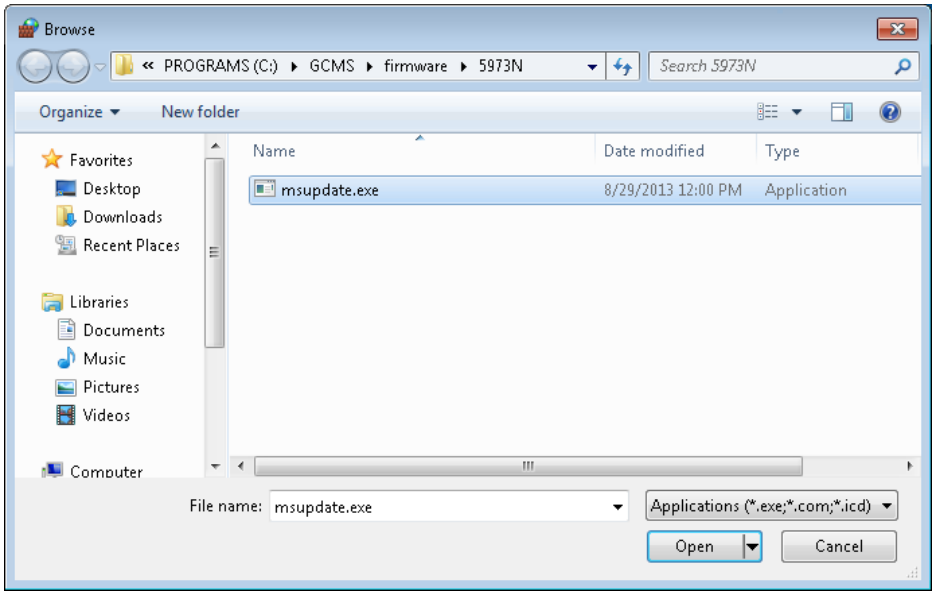

Figure 9 **Browse window**

d) In the **Add a Program** window (**Figure 10**), verify that the program file you have selected is shown in the **Path** field, and then click **Add**.

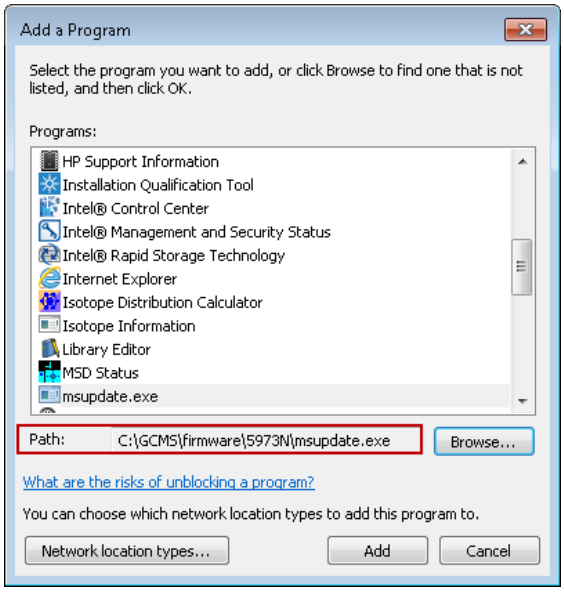

Figure 10 **Adding a program to Windows Firewall Allowed list**

e) You should now see the program on the Allowed list with a check mark next to it (**Figure 11**).

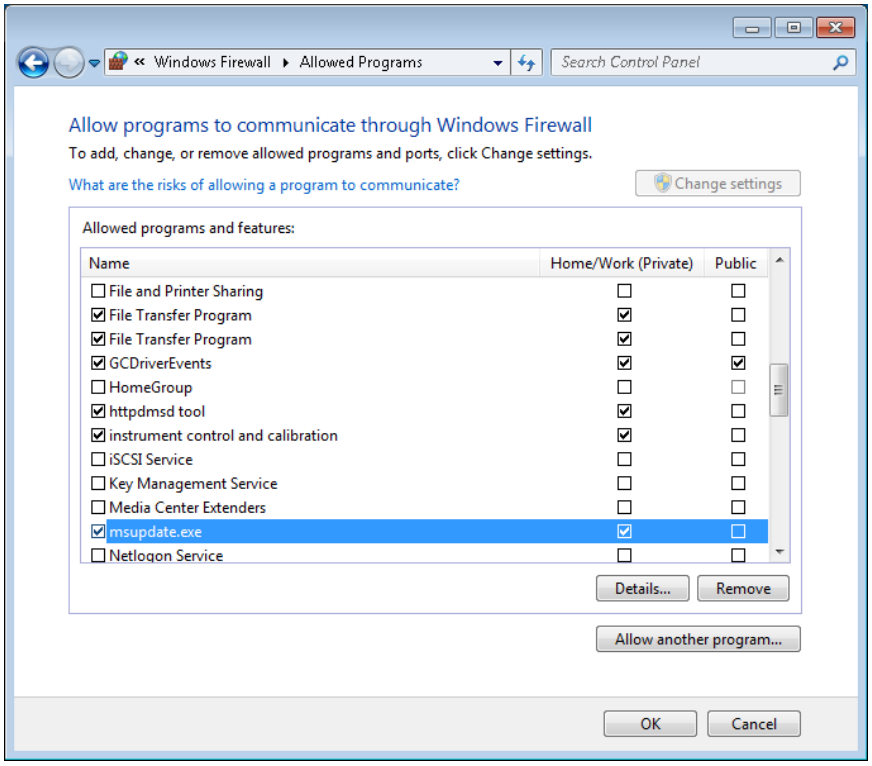

Figure 11 Program is added to Windows Firewall Allowed list