Quick Start Guide:
Utilizing GCOS with Windows XP Service Pack 2

P/N 702288 Rev. 1

For research use only.
Not for use in diagnostic procedures.

Trademarks

Affymetrix®, GeneChip®, AX®, HuSNP®, GenFlex®, Flying Objective™, CustomExpress®, CustomSeq®, NetAffx™, Tools To Take You As Far As Your Vision®, The Way Ahead™, Powered by Affymetrix™, GeneChip-compatible™, and Command Console™ are trademarks of Affymetrix, Inc.

All other trademarks are the property of their respective owners.

Limited License

Subject to the Affymetrix terms and conditions that govern your use of Affymetrix products, Affymetrix grants you a non-exclusive, non-transferable, non-sublicensable license to use this Affymetrix product only in accordance with the manual and written instructions provided by Affymetrix. You understand and agree that, except as expressly set forth in the Affymetrix terms and conditions, no right or license to any patent or other intellectual property owned or licensable by Affymetrix is conveyed or implied by this Affymetrix product. In particular, no right or license is conveyed or implied to use this Affymetrix product in combination with a product not provided, licensed, or specifically recommended by Affymetrix for such use.

Patents

Arrays: Products may be covered by one or more of the following patents and/or sold under license from Oxford Gene Technology: U.S. Patent Nos. 5,445,934; 5,700,637; 5,744,305; 5,945,334; 6,054,270; 6,140,044; 6,261,776; 6,291,183; 6,346,413; 6,399,365; 6,420,169; 6,551,817; 6,610,482; 6,733,977; and EP 619 321; 373 203 and other U.S. or foreign patents.

Use of the GeneChip® WT Amplified Double-Stranded cDNA Synthesis and Amplification Kit in accordance with the instructions provided is accompanied by a limited license to U.S. Patent Nos. 5,716,785; 5,891,636; 6,291,170; and 5,545,522. Users who do not purchase this Kit may be required to obtain a license under these patents or to purchase another licensed kit.

Copyright

© 2005-2006 Affymetrix Inc. All rights reserved.

INTRODUCTION

Microsoft® released Windows XP Service Pack 2 in August 2004. Workstations that have the auto-update feature of Windows XP enabled will have the Service Pack 2 applied automatically. Service Pack 2 enables software features that help to enhance the ability of computers running Windows XP to avoid malicious attacks, especially those from viruses and worms.

The technologies include these improvements:

- Network protection
- Memory protection
- E-mail handling
- Web browsing security
- Computer maintenance

As part of the Network protection enhancements, Windows XP Service Pack 2 installs a Windows software firewall and enables access control restrictions in Distributed Component Object model (DCOM) settings.

The changes in DCOM settings and the installation of the firewall will directly impact GeneChip Operating Software (GCOS) in the following areas:

Ability to control the GCS 3000 / GCS 3000 HR Scanner

The GeneChip Operating Software communicates with the Affymetrix GCS 3000 family of scanners using TCP/IP. The firewall installed as part of the Microsoft Windows XP SP2 enhancements will block TCP/IP traffic between the workstation and the scanner. This will prevent the workstation from communicating properly with the GCS 3000 scanners.

Ability to receive status messages from the GCOS Server

The GeneChip Operating Software communicates with the GeneChip Operating Software (GCOS) Server using DCOM. The firewall installed as part of the Microsoft Windows XP SP2 enhancements will block traffic on DCOM port 135 as part of the security enhancements. This will prevent the workstation from communicating properly with the GCOS Server. In addition, SP2 changes machine-wide DCOM permissions.

This prevents GCOS executables on the GCOS Server from providing status messages to the GCOS client. The application impacted by the update to DCOM permissions includes Data Transfer Tool and any custom user interface that makes use of the CAB creation SDK.

To enable communication with the scanner and/or GCOS server, the Windows XP firewall has to be disabled. In addition to communicate with the GCOS Server, the DCOM permissions have to be reset to allow the software to receive status messages from the GCOS Server. Section 1 and Section 2 provide instructions to disable the Windows firewall and reset the DCOM permissions to those available under Windows XP Service Pack 1a.

Follow the instructions in Section 1 – Disabling the XP SP2 firewall, if you have a GCS 3000 scanner or a GCOS Server.

Follow the instructions in Section 2 – Changing DCOM permissions only if you have a GCOS Server.

If you have a stand alone analysis workstation then the instructions in this document do not apply to you.

Section 1: Disabling the Windows Software Firewall

The Windows firewall will block all “unsolicited (on un-authenticated)” traffic on the network interface card(s) from the internet/external network. It however allows all traffic that is initiated locally from the workstation. The SP2 firewall blocks all traffic on TCP and UDP ports. In doing so the firewall blocks all DCOM communications arriving at TCP port 135. This will prevent the software from communicating with the GCOS Server. The software firewall blocks all network traffic that occurs between the scanner and the workstation over TCP. To re-enable the GCOS functionality for the scanner and /or the GCOS server, the firewall has to be configured to allow the instrument control drivers and DCOM to receive traffic from outside the workstation.

NOTE: It is necessary to have local administrative rights to make changes to the Windows firewall or Windows DCOM permissions.

Enabling Scanner-Workstation Functionality Through a Firewall

1. Open the Windows Control Panel and click **Security Center** (Figure 1).

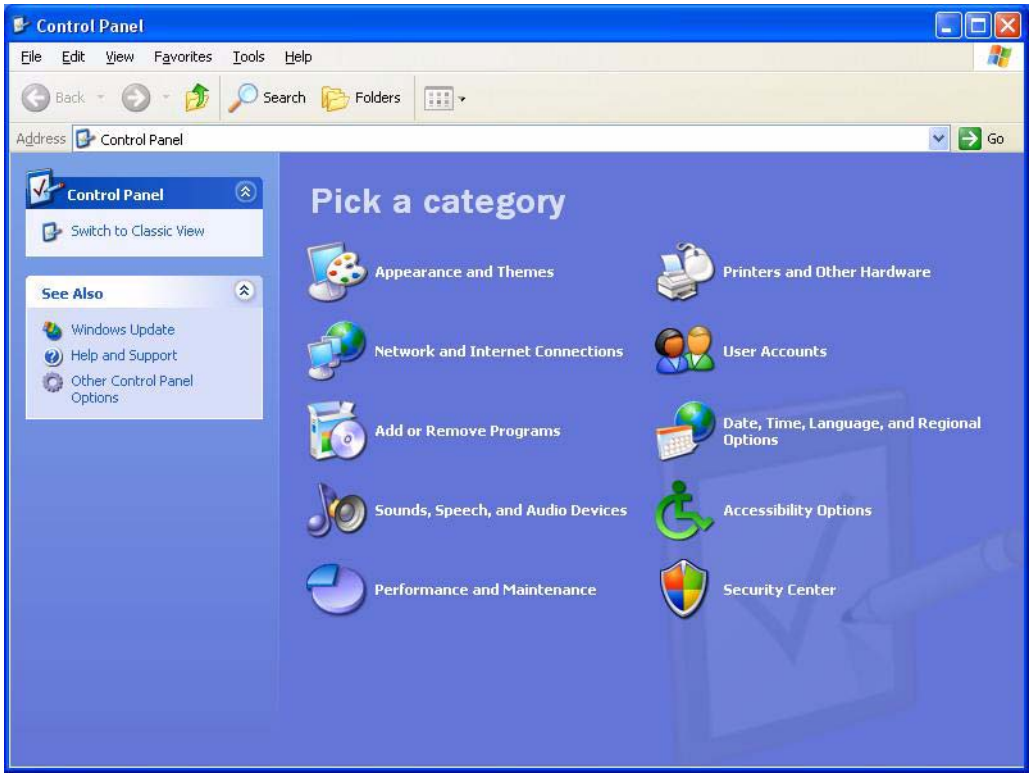

Figure 1 Windows Control Panel

The Windows Security Center window opens. It is from this window that you are allowed to configure the Windows Firewall (Figure 2).

Figure 2 Windows Security Center window

2. Click **Windows Firewall** to open the dialog box for changing the firewall settings (Figure 3).

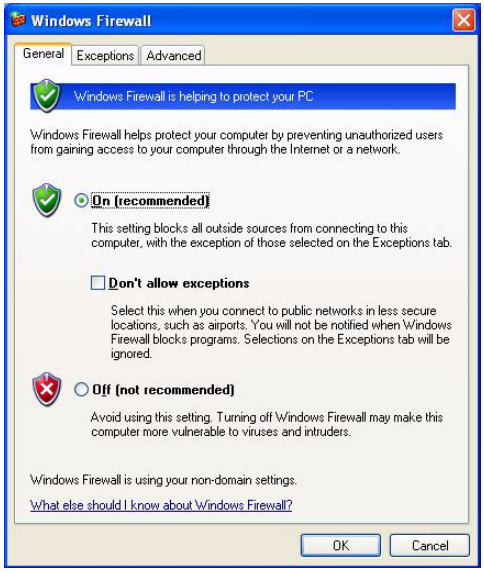

Figure 3 Windows Firewall dialog box

3. Click the **Exceptions** tab (Figure 4).

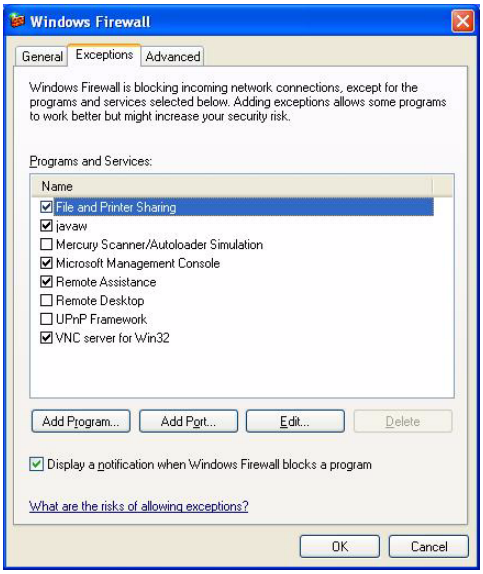

Figure 4 Windows Firewall dialog box

4. Click **Add Program** to add a program that will be allowed to receive network traffic over TCP/IP (Figure 5).

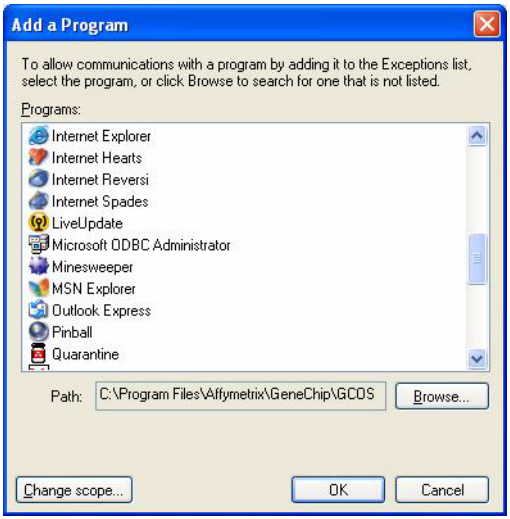

Figure 5 Add a Program dialog box

5. Click **Browse** and change the directory to the GCOS install directory.
6. Select **MerScanCom.exe** from the GCOS directory and click **Open** (Figure 6).

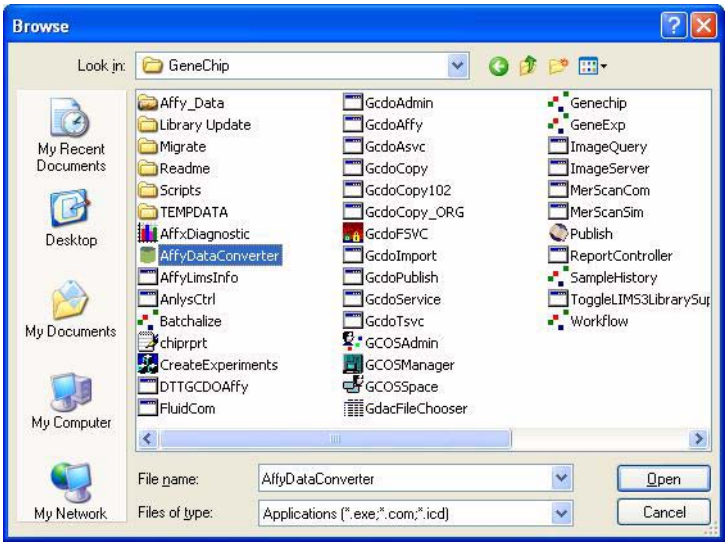

Figure 6 Browse dialog box

7. Click **Open** and select **MerScanCom.exe**.
8. Click **OK** on the next screen (see Figure 7).

This allows the scanner instrument control library to receive data packets from the scanner through the firewall.

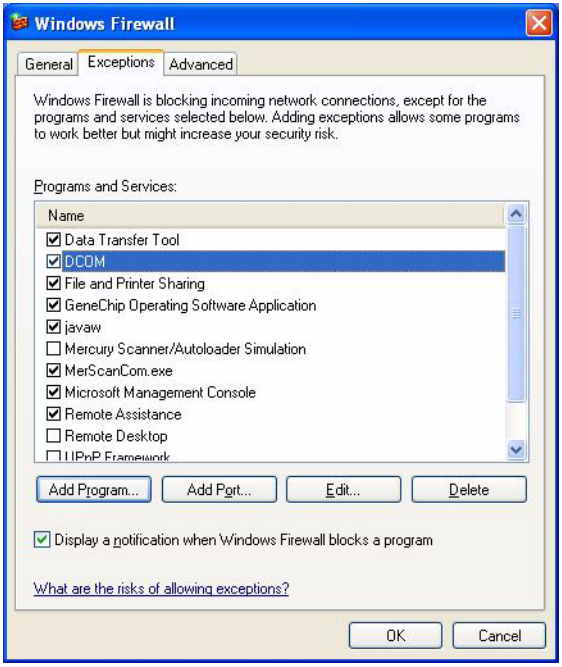

Figure 7 Windows Firewall dialog box

Enabling Status Events From CAB Creation Component on GCOS Server

Follow the steps if you have a GCOS Server and use the CAB creation functionality of Data Transfer Tool. To re-enable the CAB creation utility on the server to send status events back to the GCOS client workstation perform the following steps on the GCOS client workstation:

1. Open the Windows Control Panel and click **Security Center** (Figure 8).

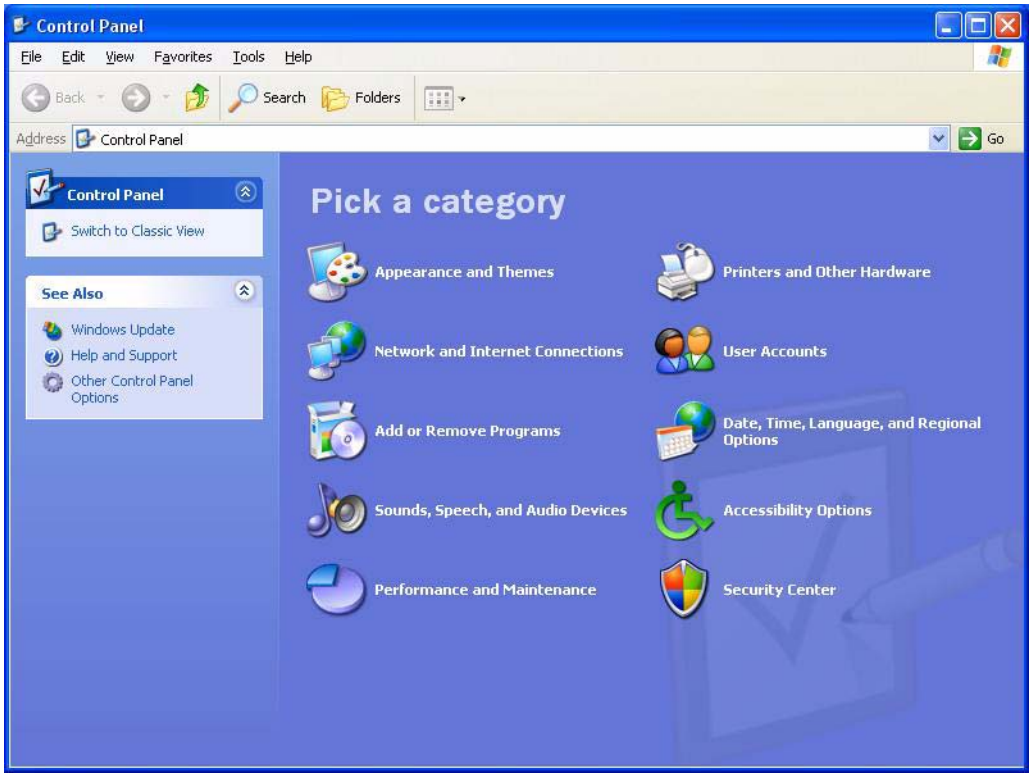

Figure 8 Windows Control Panel

The Windows Security Center dialog box appears. It is from this dialog box that you configure the Windows Firewall (Figure 9).

Figure 9 Windows Security Center dialog box

2. Click **Windows Firewall** to open the dialog box for changing the firewall settings (Figure 10).

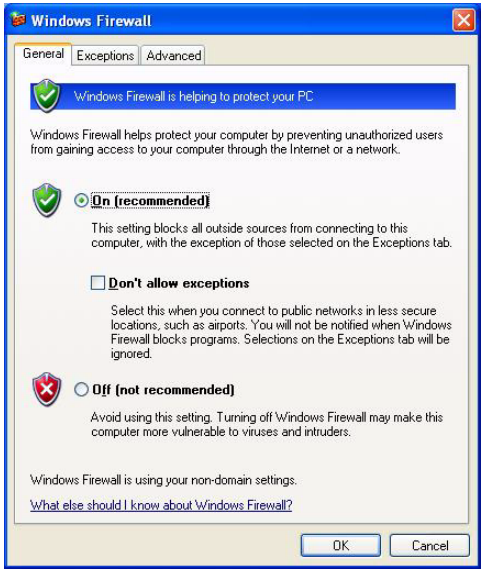

Figure 10 Windows Firewall dialog box

3. Click the **Exceptions** tab (Figure 11).

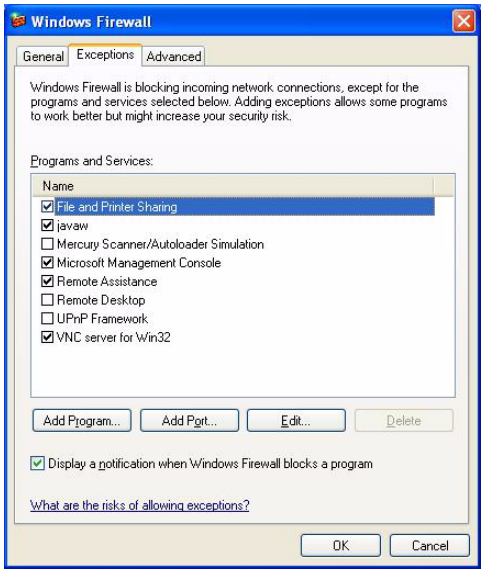

Figure 11 Windows Firewall dialog box - Exceptions tab

4. Click **Add Port** to configure DCOM.

5. Type **DCOM** in the **Name** field and **135** in the **Port number** field as shown in Figure 12. Click **OK** to close the dialog box.

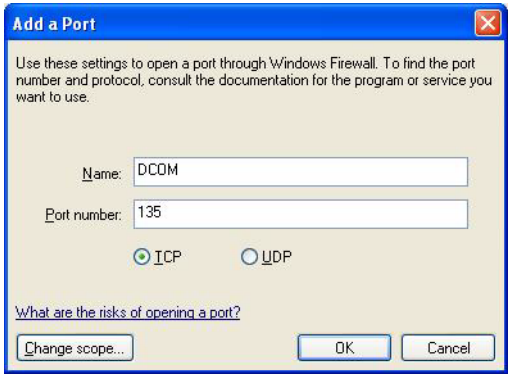

Figure 12 Add a Port dialog box

6. Click **OK** in the Windows Firewall dialog box (Figure 13).

   This allows the CAB creation component on the GCOS Server to communicate through the firewall with the Data Transfer Tool on the client.

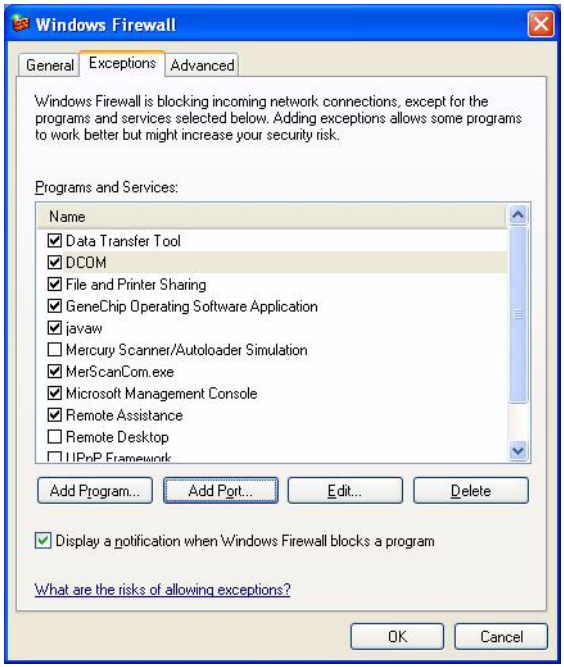

Figure 13 Windows Firewall dialog box - Exceptions tab

Section 2: Changing DCOM permissions

XP Service SP2 updates the DCOM settings to enhance network security. The changes in DCOM settings impact default impersonation and authentication level. The permissions have to be updated to allow anonymous requests coming from CAB creation application on the GCOS Server. It is not possible to limit change for authentication and impersonation for a single component (i.e., to allow anonymous requests only from the CAB creation application that resides on the server). The DCOM permissions for entire workstation must to be changed to enable DTT to receive status messages from the CAB creation component located on the server.

The two steps required to re-enable un-authenticated requests include:

1. Set the DCOM security on the client machine, and
2. Open up the firewall to DCOM (as explained in Section 1)

Perform the instructions in the following steps:

1. Select **Start** → **Run** and enter **DCOMCnfg** in the Run dialog box. Click **OK** (Figure 14).

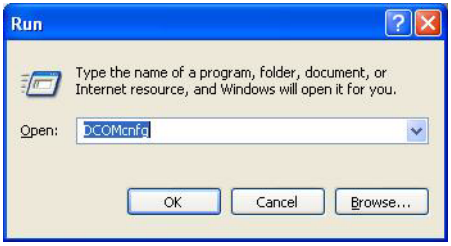

Figure 14 Run dialog box

The Component Services dialog box appears. It is from this dialog box that DCOM permissions can be updated (Figure 15).

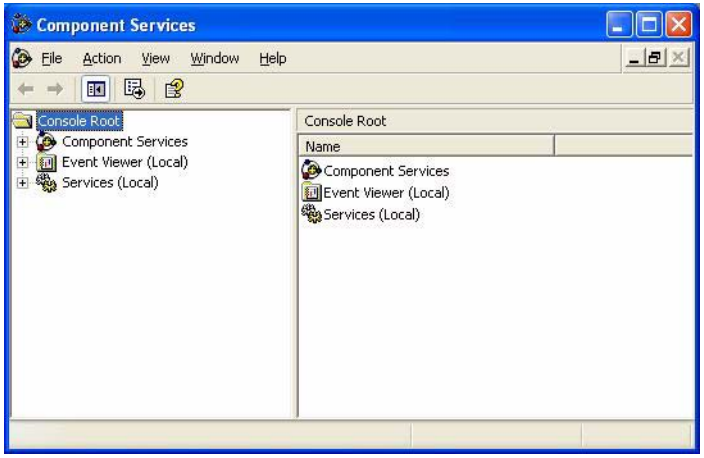

Figure 15 Component Services dialog box

2. Double-click the **Component Services** node under the **Console Root** to view the **Computers** folder.
3. Select the **Computers** node to view **My Computer** in the right pane of the window.
4. Right-click **My Computer** and select **Properties** from the shortcut menu that appears (Figure 16).

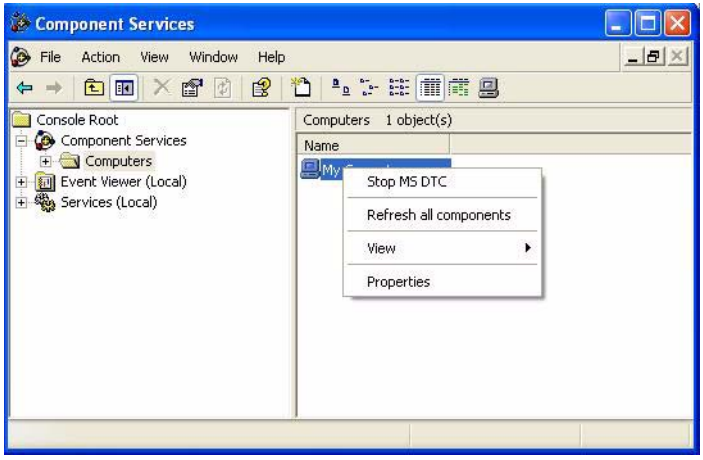

Figure 16 Component Services dialog box

5. In the My Computer Properties dialog box, click the **Default Properties** tab (Figure 17).

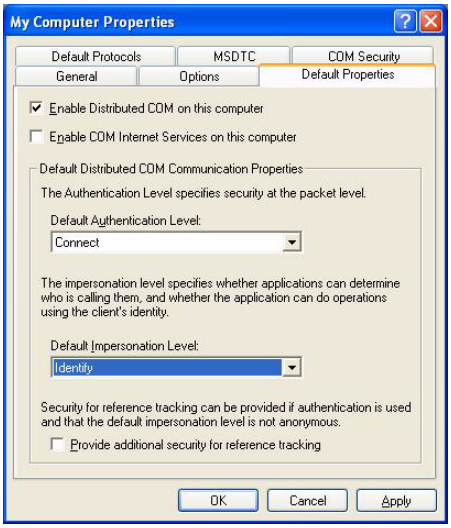

Figure 17 Computer Properties dialog box - Default Properties tab

6. Change the **Default Authentication Level** from **Connect** to **None** and change the **Default Impersonation Level** from **Identify** to **Anonymous** (Figure 18).

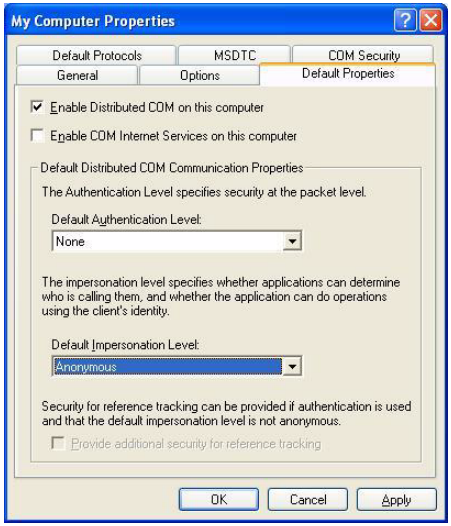

Figure 18 Computer Properties dialog box

7. Click **Apply**.

8. Click **OK** to close the dialog.
9. Click **Start** → **Run** and enter **gpedit.msc** (Figure 19). Click **OK**.

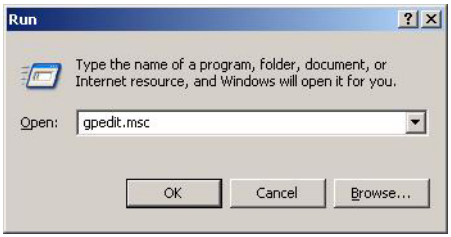

Figure 19 Run dialog box

This starts the Windows Group Policy console (Figure 20).

10. In the left pane select **Local Computer Policy** → **Computer Configuration** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Option**. The list of policies is displayed in the right pane (Figure 20).

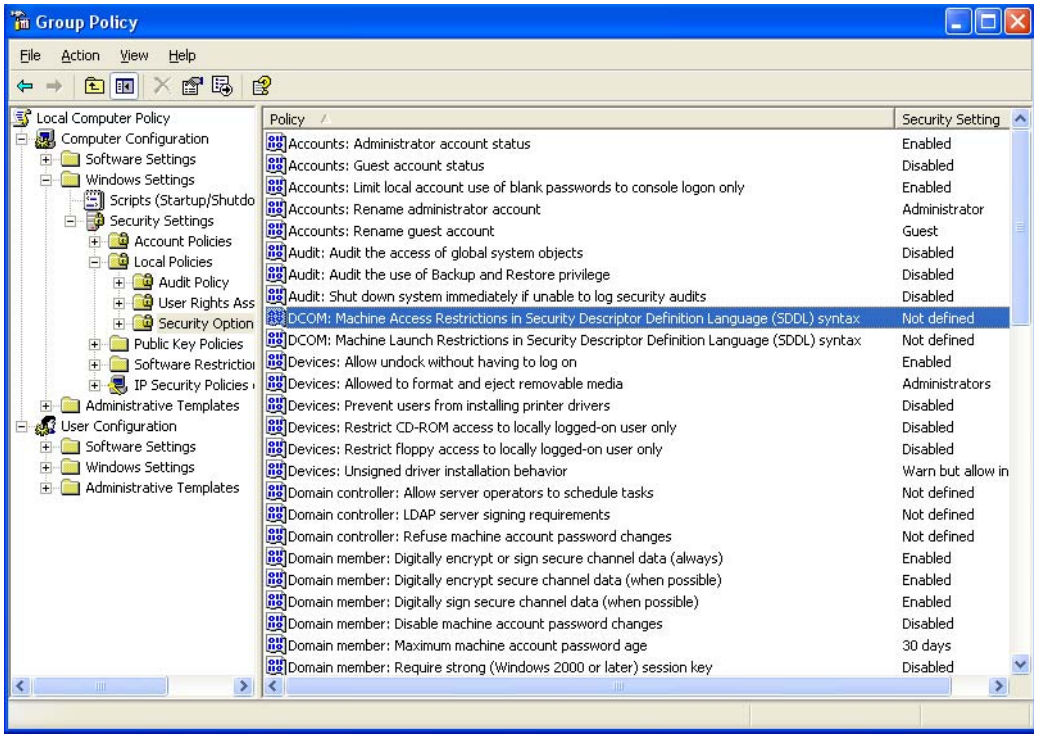

Figure 20 Group Policy window

11. In the right pane double-click "**DCOM: Machine Access Restrictions ...**" The Machine Access Restrictions dialog box appears (Figure 21).

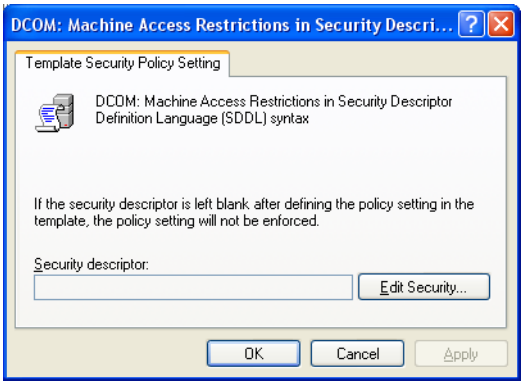

Figure 21 Machine Access Restrictions dialog box

12. Click **Edit Security**. The Access Permissions dialog box appears (Figure 22).

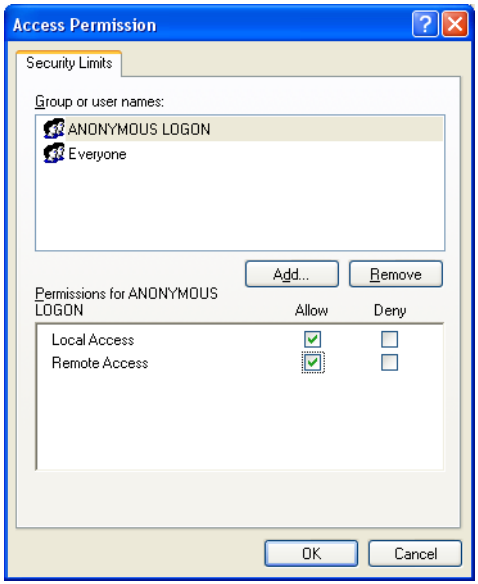

Figure 22 Access Permissions dialog box

13. Select the **Allow** option for both **Local Access** and **Remote Access** for both the **ANONYMOUS LOGON** and **Everyone**.

14. Click **Add**.
The Select Users or Groups dialog box appears (Figure 23).

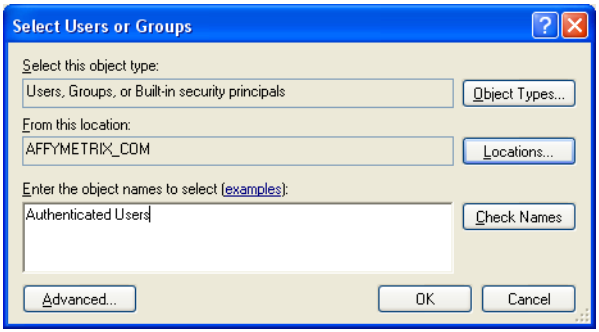

Figure 23 Select Users or Groups dialog box

15. Type **Authenticated Users** and click **OK**.

16. Select the **Allow** option for all permissions for the **Authenticated Users** user.

17. Click **OK** in the Access Permissions dialog box and Machine Access Restrictions dialog box to apply the changes.

18. Double-click "**DCOM: Machine Launch Restrictions ...**"
The Machine Launch Restrictions dialog box appears (Figure 24).

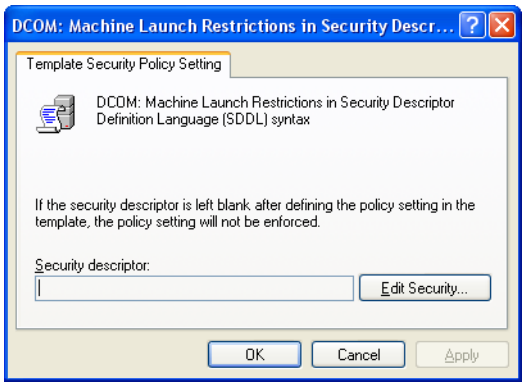

Figure 24 Machine Launch Restrictions dialog box

19. Click the **Edit Security** button.
The Launch Permissions dialog box appears (Figure 25).

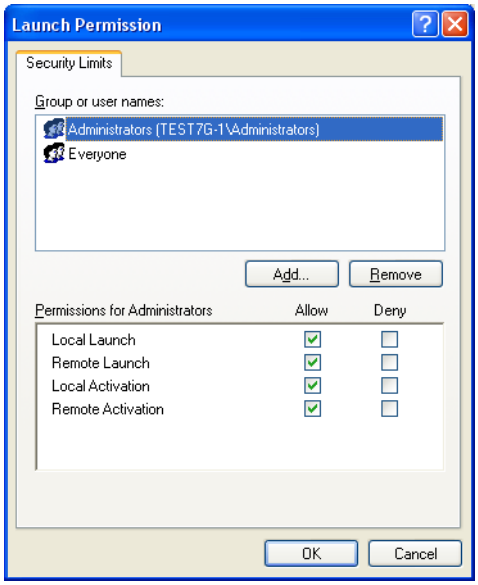

Figure 25 Launch Permissions dialog box

20. Select the **Allow** option for all permissions for the **Everyone** user.

21. Click **Add**.
The Select Users or Groups dialog box appears (Figure 26).

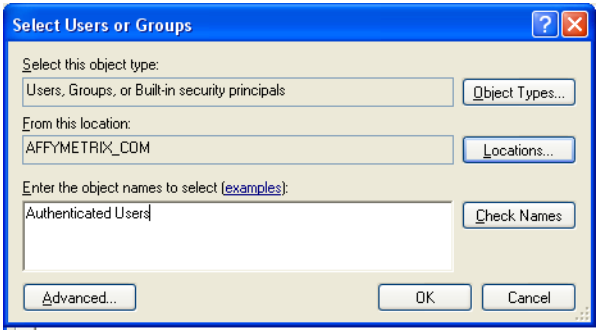

Figure 26 Select Users or Groups dialog box

22. Type **Authenticated Users** and click **OK**.

23. Select the **Allow** option for all permissions for the **Authenticated Users** user.

24. Click **OK** in the both the Launch Permissions and Machine Launch Restrictions dialogs boxes to apply the changes.

    For more information on DCOM security go to www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx

25. Reboot the workstation.

Contact Information

Affymetrix, Inc.
3420 Central Expressway
Santa Clara, CA 95051
USA

E-mail: support@affymetrix.com
Tel: 1-888-362-2447 (1-888-DNA-CHIP)
Fax: 1-408-731-5441

Affymetrix UK Ltd
Voyager, Mercury Park,
Wycombe Lane, Wooburn Green,
High Wycombe HP10 0HH
United Kingdom

E-mail: supporteurope@affymetrix.com
UK and Others Tel: +44 (0) 1628 552550
France Tel: 0800919505
Germany Tel: 01803001334
Fax: +44 (0) 1628 552585

Affymetrix Japan, K. K.
Mita NN Bldg
16 Floor, 4-1-23 Shiba,
Minato-ku, Tokyo 108-0014
Japan

Tel: (03) 5730-8200
Fax: (03) 5730-8201