

Microsoft Windows XP SP2 and Firewall Technical Note for the GeneChip® GCS-3000 Targeted Genotyping System

The note describes required changes to the Windows Firewall on the GTGS and GCOS Workstations, and required DCOM group policy changes on the GCOS workstation, if the computers are using Windows XP Service Pack 2

Microsoft released Windows XP Service Pack 2 in August 2004. On April 14, 2005 Microsoft unblocked the auto-update feature for XP Service Pack (SP) 2. Workstations that have the auto-update feature of Windows XP enabled will have Service Pack 2 applied automatically. Service Pack 2 enables software features that will help to enhance the ability of computers running Windows XP to withstand 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 various areas.

Section 1: If you choose to keep the firewall on for the GTGS Lab Workstations, you will need to follow the instructions in Section 1. HTTP port 80 and SQL Server port 1433 will need to be opened on the Post-Amp Lab Workstation. If these ports aren't opened, the Pre-Amp Lab Workstation will not be able to run GeneChip® Targeted Genotyping Analysis software (GTGS), since the application is being accessed from the Post-Amp Workstation. No adjustments are needed for the Pre-Amp Lab Workstation.

Section 2: If you choose to keep the firewall on for a GCOS workstation that has been updated to Windows XP Service Pack 2, you will need to follow the instructions in **Section 2**. The GeneChip® Operating Software (GCOS) communicates with GTGS on another computer using DCOM. Microsoft Windows XP SP2 enhancements will block traffic on DCOM port 135 and communication with GcdoAffy.exe, due to the Windows Firewall. This will prevent the GCOS workstation from communicating properly with GTGS workstations. Section 2 describes how to adjust the Firewall to enable communication between GTGS and GCOS.

Section 3: If the GCOS workstation has been updated to Windows XP Service Pack 2, you will need to follow the instructions in Section 3. Service Pack 2 enhancements create a group policy for DCOM that by default prevents GTGS from communicating with GCOS over the network. Section 3 describes how to adjust the DCOM group policy to enable communication between GTGS and GCOS.

Note: If a GCOS workstation has been upgraded to XP Service Pack 2, please also refer to the support documentation at http://www.affymetrix.com/support/technical/product_updates/gcos_xpsp2.affx

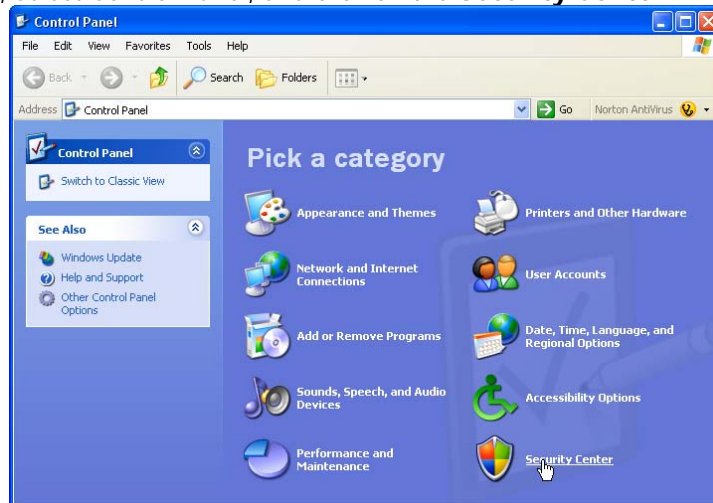
NOTE: A computer's firewall settings may automatically change when a computer is added to a domain, or when Norton AntiVirus is activated.

NOTE: It is necessary to have local administrative rights to manage these settings.

Section 1: Adjust the Windows Firewall settings for the GTGS Post-Amp Lab Workstation

Note: No Firewall adjustments are needed for the GTGS Pre-Amp Lab Workstation

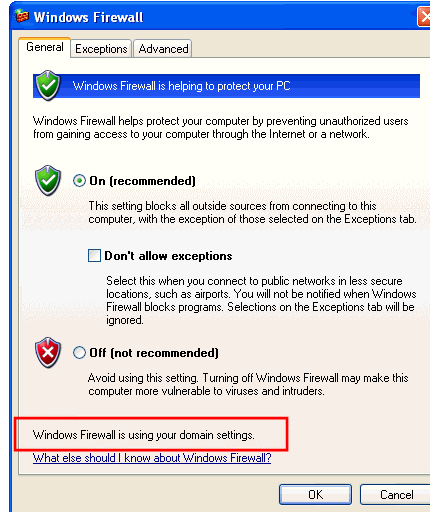
1. Log into the GTGS Post-Amp Lab Workstation as **Administrator** on **this computer**.
2. From the Start Menu, select Control Panel, and click on the **Security Center**.



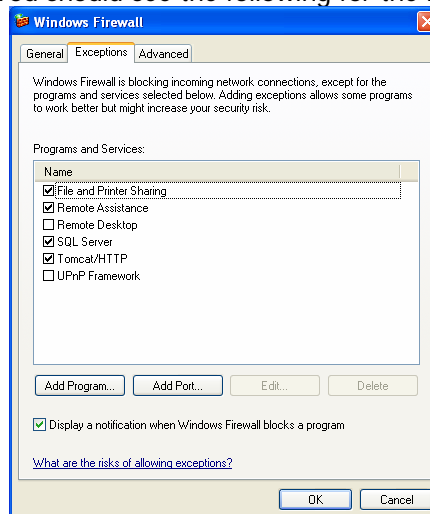
3. Within the Windows Security Center window, select **Windows Firewall**.



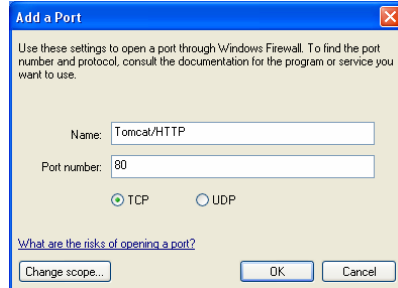
- In the **General** tab, if you wish the firewall to be on, then **On (recommended)** should be selected, with **Don't allow exceptions UNCHECKED**. If this is not the case, there are three possible reasons (and suggestions):



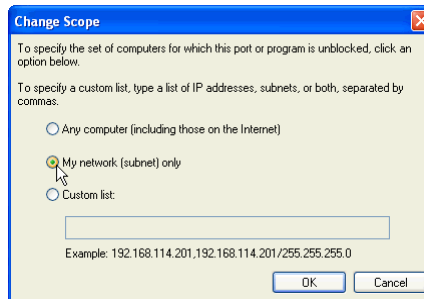
- Reason #1: If the highlighted text in the General tab screenshot says “Windows Firewall is using your domain settings”, then it is possible that adding this computer to the domain changed the settings.
 - If domain settings are used and the firewall is “On”, but “Don't allow exceptions” is **CHECKED**, then uncheck it. If this option is not available, talk to your System Administrator to make necessary changes to allow exceptions.
 - If domain settings are used and the firewall is “Off”, you can assume the site's network policy discourages firewall settings for this computer. You can stop reading this Technical Note, as it doesn't apply to your configuration.
 - Reason #2: Installing Norton AntiVirus with default settings can turn off Windows Firewall. Unless the System Administrator wants to keep the firewall off, click “On (recommended)”, and make sure “Don't allow exceptions” is **UNCHECKED**.
 - Reason #3: The firewall may be off if you or the System Administrator have manually turned off the firewall per the System Administrator's request. If this is the case, you can stop reading this Technical Note, as it doesn't apply to your configuration.
- Switch to the **Exceptions** tab. You should see the following for the Post-Amp Workstation:



6. **File and Printer Sharing** should be **CHECKED**, and entries for **SQL Server** and **Tomcat/HTTP** must be present and **CHECKED**. If this is the case, you can stop reading the steps in this section, as your configuration for the GTGS Post-Amp Workstation is already correct. However, adding the computer to the domain may have changed the entries. If the entries need to be re-added, do the following:
7. Check **File and Printer Sharing**.
8. Select **Add Port**.



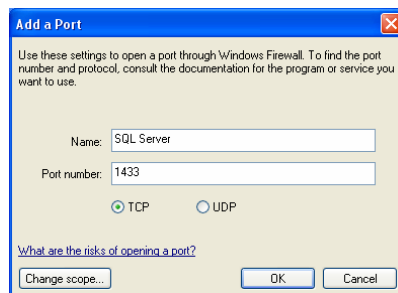
9. Enter **Tomcat/HTTP** for the Name, **80** for the Port number, and make sure **TCP** is selected.
10. Click **Change Scope**.



11. Select **My Network (subnet) only** and click **OK**.

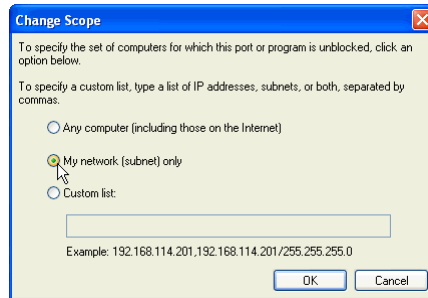
NOTE: Talk to your System Administrator if you're unsure whether the Pre-Amp and Post-Amp Lab Workstations are on the same subnet.

12. Click **OK** in the **Add Port** window to add the Tomcat/HTTP exception.
13. Select **Add Port**.



14. Enter **SQL Server** for the Name, **1433** for the Port number, and make sure **TCP** is selected.

15. Click **Change Scope...**



16. Select **My Network (subnet) only** and click **OK**.

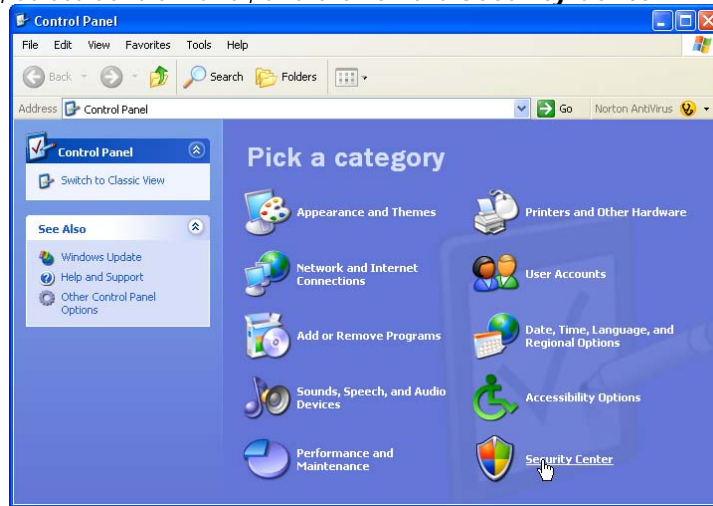
NOTE: Talk to your System Administrator if you're unsure whether the Pre-Amp and Post-Amp Lab Workstations are on the same subnet.

17. Click **OK** in the **Add Port** window to add the SQL Server exception.

18. Click **OK** to close Windows Firewall.

Section 2: Configure Windows Firewall and DCOM settings on the GCOS Workstation to allow GCOS to communicate with GTGS

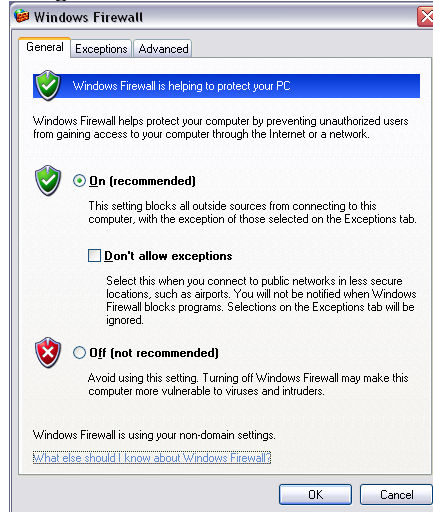
1. Log into the GCOS Instrument Workstation as **Administrator** on **this computer**.
2. From the Start Menu, select Control Panel, and click on the **Security Center**.



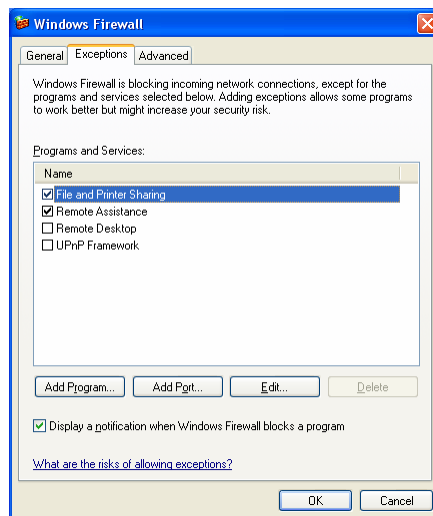
3. Within the Windows Security Center window, select **Windows Firewall**.



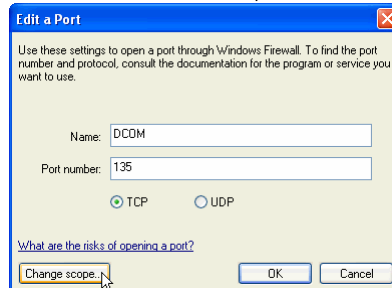
4. Click on **Windows Firewall** to open the dialog for changing the firewall settings. If it is "On", make sure that "Don't allow exceptions" is not checked. If it is "Off", then you do not need to do any further steps in this section, because no firewall configuration is needed.



5. Select the **Exceptions** tab. If there is a DCOM entry, select **Edit...** If there is no DCOM entry, select **Add Port...**

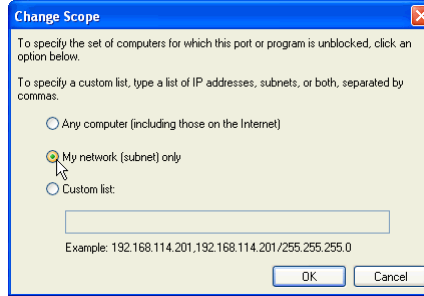


6. For the Name field , enter **DCOM**. For the Port number, enter **135**.

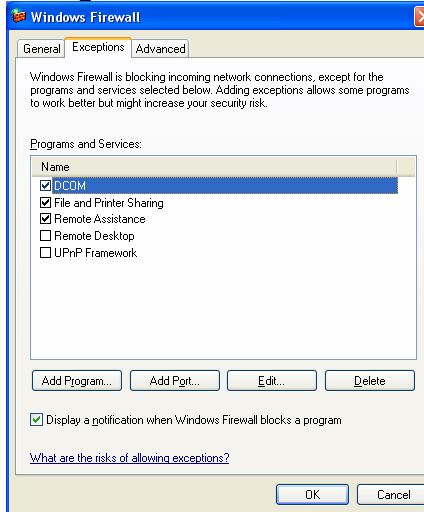


7. Click **Change scope...**

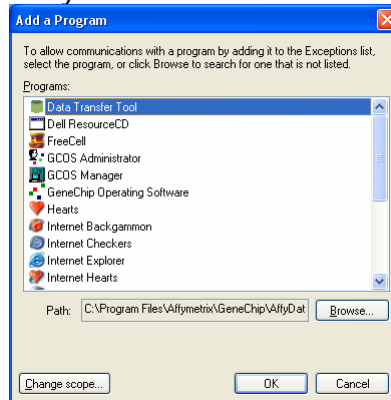
8. Select **My network (subnet) only**, and click **OK**.



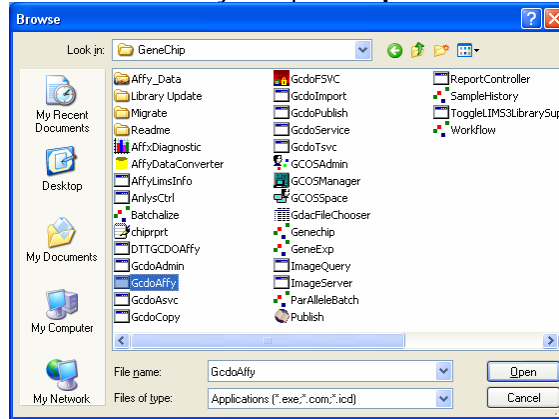
9. From the Exceptions tab, click **Add Program...**



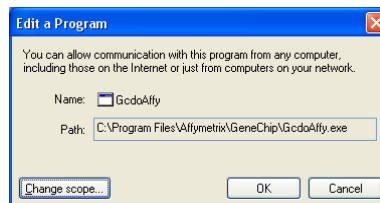
10. Select **Browse** and change the directory to the GCOS install directory.



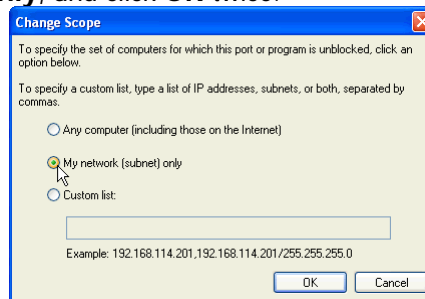
11. Select **GcdoAffy.exe** from the GCOS directory and press **Open**.



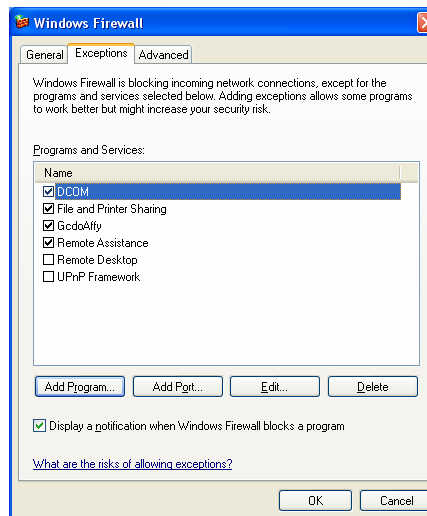
12. Click **Change scope...**



13. Select **My network (subnet) only**, and click **OK** twice.



14. When done, the Exceptions tab should show at least the following entries:

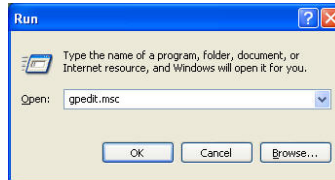


15. Click **OK** to close the Windows Firewall control panel.

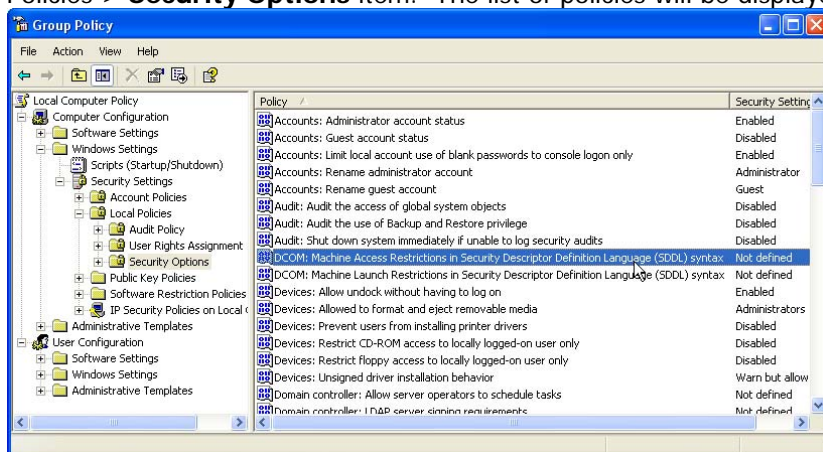
Section 3: Configure the DCOM group policy on the GCOS Workstation to allow GCOS to communicate with GTGS

Note: This step is only necessary for GCOS workstations running Windows XP Service Pack 2.

1. Log into the GCOS Instrument Workstation as **Administrator** on **this computer**.
2. Select the Windows **Start** menu and select **Run**. Enter **gpedit.msc** and click **OK**. This will start the Windows Group Policy console.

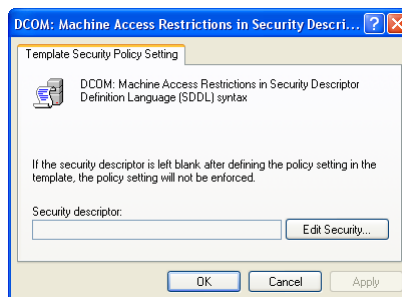


3. In the left pane select the Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > **Security Options** item. The list of policies will be displayed in the right pane.

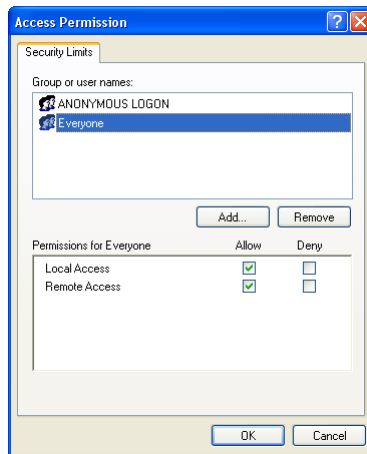


Note: If there are no DCOM entries in this window, then you do not have to do any of the configuration steps in this section.

4. In the right pane double click on the **DCOM: Machine Access Restrictions ...** item. The Machine Access Restrictions dialog will appear.



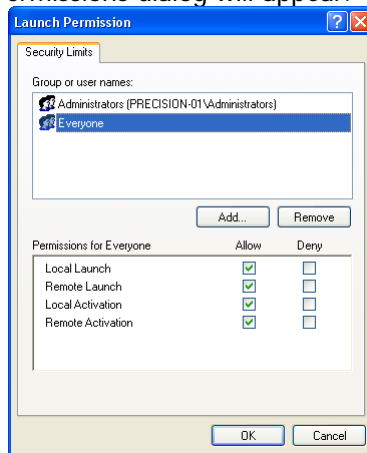
5. Click **Edit Security...** The Access Permissions dialog will appear.



6. Select the **Everyone** user. Verify that the "Allow" option is checked for both Local Access and Remote Access.
7. Click **OK** in the both the Access Permissions and Machine Access Restrictions dialogs to apply the changes.
8. Now double click on the **DCOM: Machine Launch Restrictions ...** item. The Machine Launch Restrictions dialog will appear.



9. Click **Edit Security...** The Launch Permissions dialog will appear.



10. Select the **Everyone** user. Check the "Allow" option for all permissions.
11. Click **OK** in the both the Launch Permissions and Machine Launch Restrictions dialogs to apply the changes.
12. Restart the workstation.