Application Note 8:

X Series Recorders
DCOM Settings and XP Firewall

DCOM Configuration

Introduction

This document is intended to provide a check-list of PC settings when running on Windows XP (service pack 2) which may require changing in order to get DCOM communications working on a client network. The DCOM section of this document can be applied to both Windows 2000 and Windows XP, the firewall settings will only apply to Windows XP (SP2) as other versions of windows are not currently supported.

DCOM may be required for either connecting with a remote Trend Server database or Communications Server or where OPC communications to an X-Series recorder are required.

DCOM is a Microsoft technology which allows software components or applications to exchange data via a network, if nothing blocks this communication it just works! Unfortunately networks and network attached devices often require security systems to block any unwanted or (potentially) malicious network traffic.
Current Windows operating systems have default security settings set to what is considered “safe” for the majority of users, unfortunately this often blocks DCOM (and OPC) traffic.
To allow DCOM traffic a number of Windows security and Firewall (if used) settings need to be checked and changed if necessary. The following changes should work for most applications, however if the client network has additional security systems (firewall, router etc.) these may also require changing.

***** Please Note *****

It is not the responsibility of your supplier, or a fault with the equipment supplied if DCOM does not function correctly on a particular PC or Network. This is likely caused by Network or PC policies or other installed applications that are out of the control of your supplier. In the event of additional problems, please refer to your Network Administrator

Check List

1. Check the DCOM settings on both client and server:
   1.1. The client will generally work with the default settings, but the server will almost always require the settings changed.

   See Appendix A DCOM Configuration for more details

2. If the Windows (or other) firewall is used:
   2.1. Create a firewall exception rule to allow DCOM traffic (port 135) on both client and server.
   2.2. Ensure that the “File and Printer Sharing” firewall exception is enabled on both client and server.
   2.3. Create a firewall exception rule to allow the application “TrendServerPro.exe” to access the network on both client and server.
   2.4. Create a firewall exception rule to allow the service “Database Server” (DSapserv.exe) to access the network on both client and server.
   2.5. Create a firewall exception rule to allow the service “CommsSrv” (CommsSrv.exe) to access the network on both client and server.

   See Appendix B Windows Firewall for more details.

3. Check to see if the client and server are in a domain. If they are not in a domain, then the following applies:
   3.1. Simple File Sharing (SFS) should be switched off.
   3.2. The server machine must have the same user account configured as the client machine that is currently trying to run the Trend Server software. The password for the user account must be the same on both machines.

   See Appendix C Domains: SFS and user accounts.

4. If after the above the actions the remote client still isn’t communicating:
   4.1. Try restarting both client and server; a restart should not be necessary if only the firewall or simple file sharing option have changed, but a restart is needed to ensure that any DCOM configuration changes have been applied.
   4.2. Temporarily switch off any firewall; if a firewall is in use, it must be restored after testing; switching the firewall off will eliminate it is as a possible problem source.
   4.3. Check network security settings and ensure DCOM traffic (port 135) is being allowed; this will require some input from someone familiar with the network architecture being used.

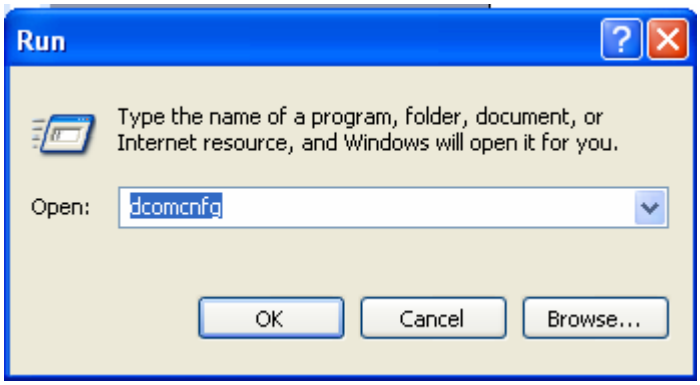
5. If after all the above actions the remote client still isn’t communicating:
   5.1. Attempt to establish a direct connection between the client and server, this can either be by using a network cross-over cable and assigning a static IP address to both client and server, or by using a DHCP equipped router to form a simple network.
   5.2. If the client will communicate only with a direct connection (as above) the security settings used on the client network need to be reviewed to ensure DCOM traffic is being allowed.
   5.3. As a final check that DCOM traffic is not being blocked by the client network, a port scanner may be used to check the state of and access to port 135; this is not recommended for anyone unfamiliar with network technology. A basic (and safe) port scanner (PortQry) is available for down-load from Microsoft’s web site; a search on Microsoft.com for Portqry will locate the instructions for down-load and use, down-loading from any third party web site is not recommended.

Appendix A DCOM configuration

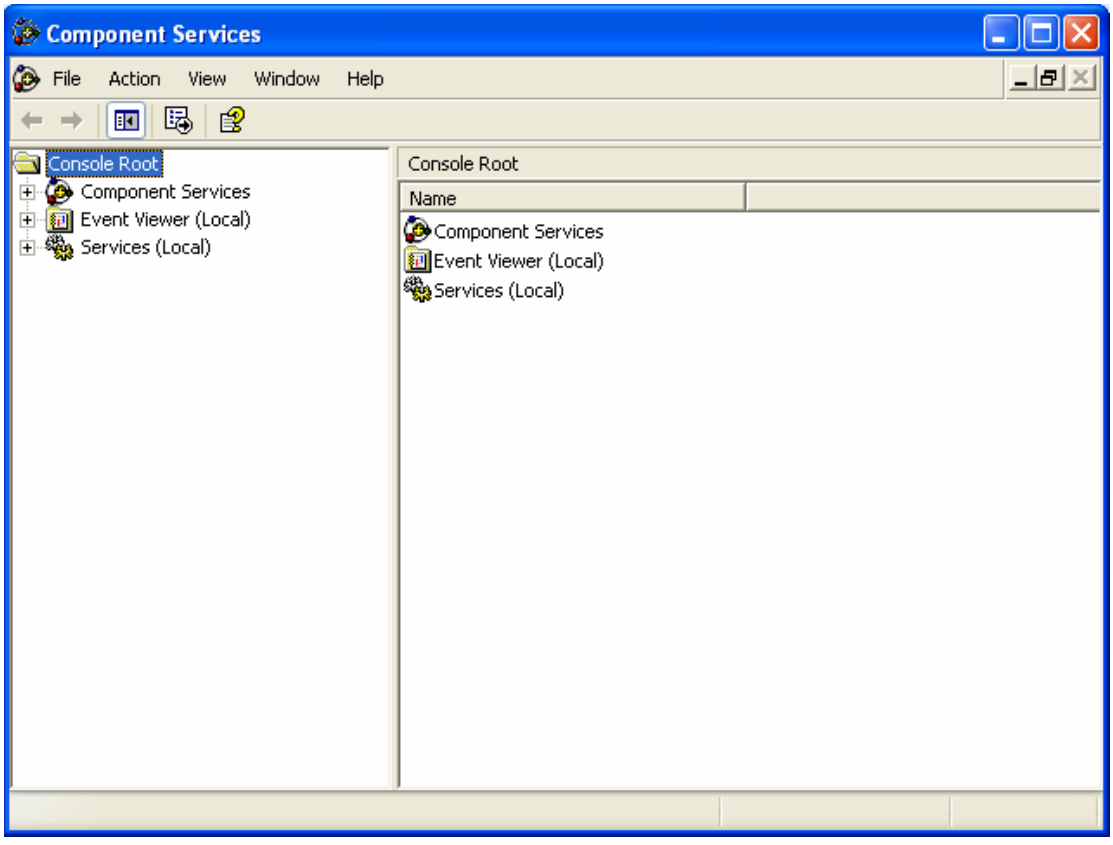
These instructions and example dialogs have been produced from Windows XP (SP2), if you are using another version of Windows or the dialog boxes differ from those shown please seek advice before continuing.

This needs to be carried out on any PC where remote DCOM access is required.

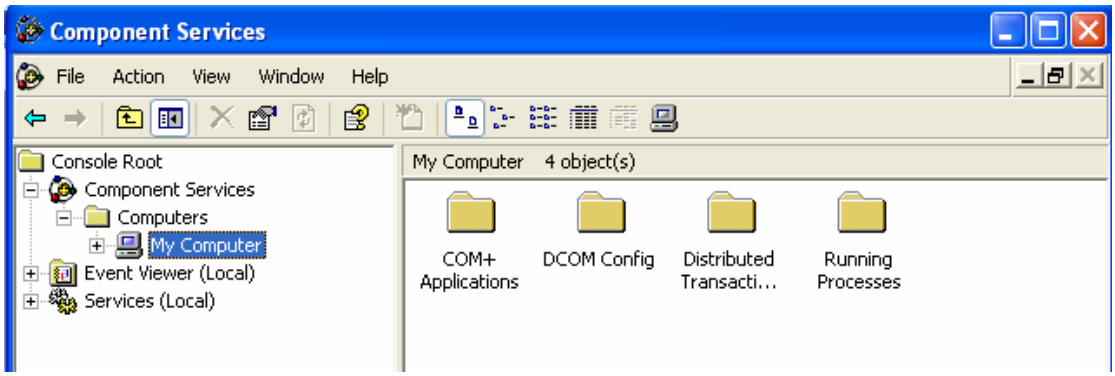
Step A.1) From the Start menu, select “Run…” and enter dcomcnfg in the run dialog box:



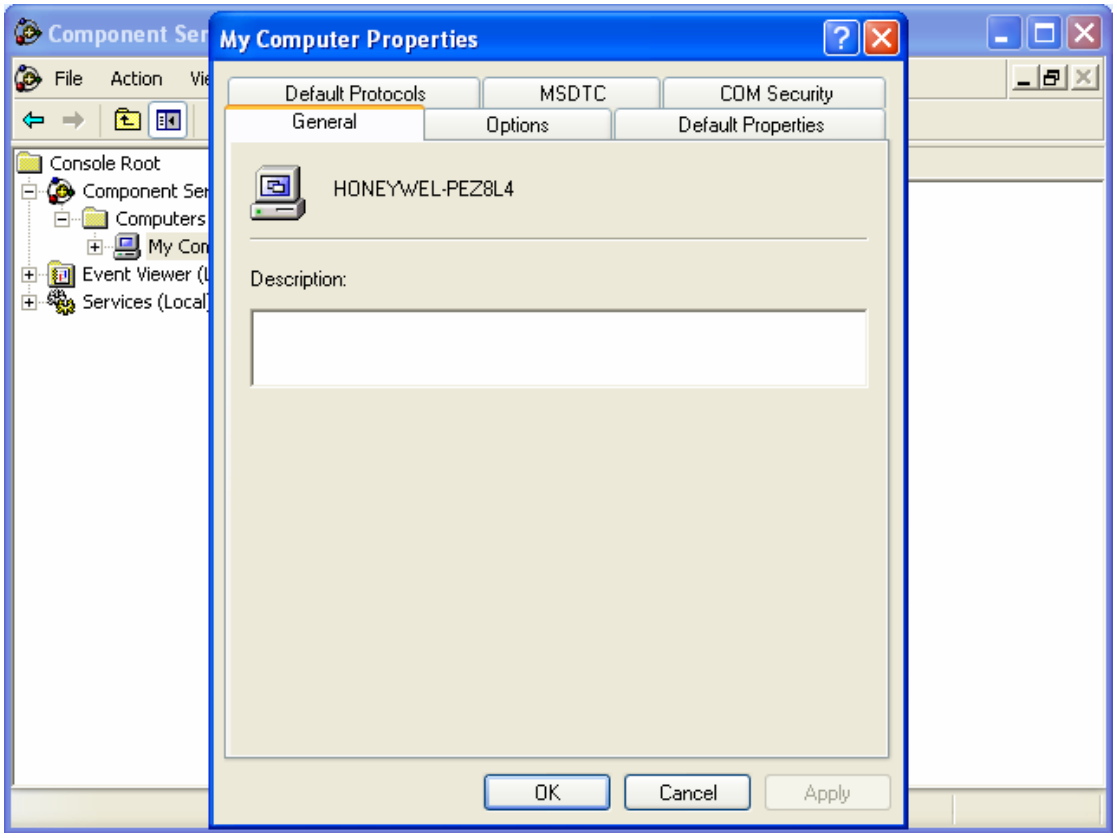
This will open the component services dialog box:



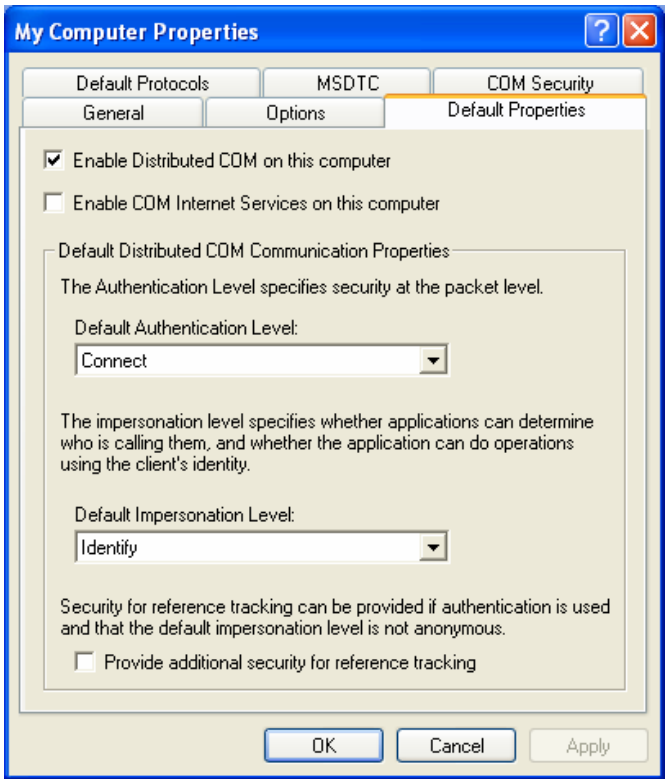
Step A.2) Open the Component services tree to allow “My Computer” to be selected:



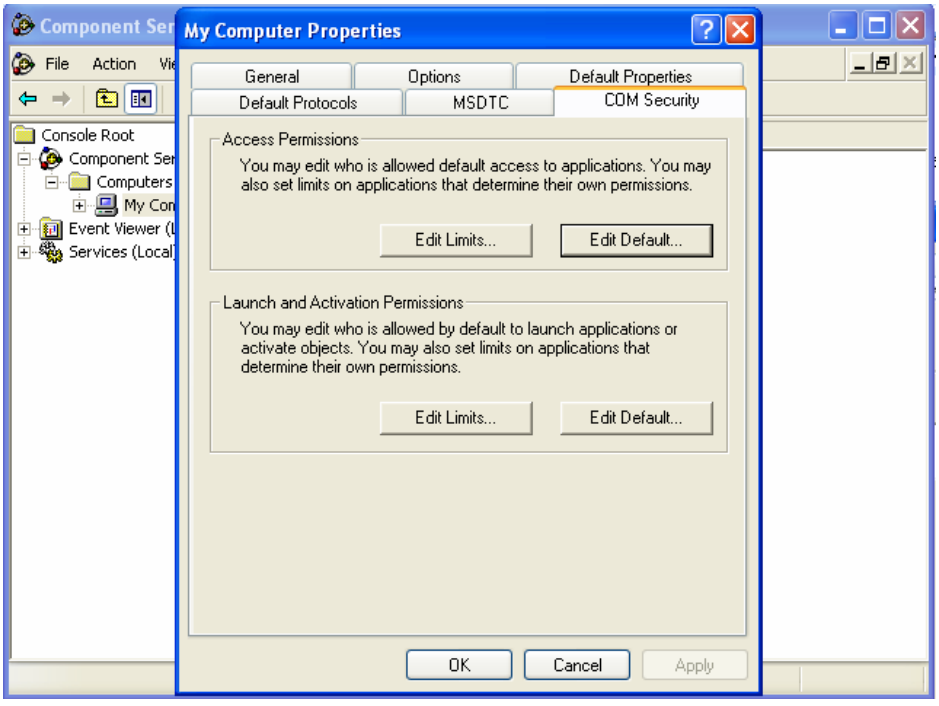
Step A.3) Right click on “My Computer” to show the context menu, and select “Properties”:



Step A.4) First thing to check is that DCOM has been enabled on the PC, this is done by selecting the Default properties tab and checking that Enable distributed COM on this computer is checked.

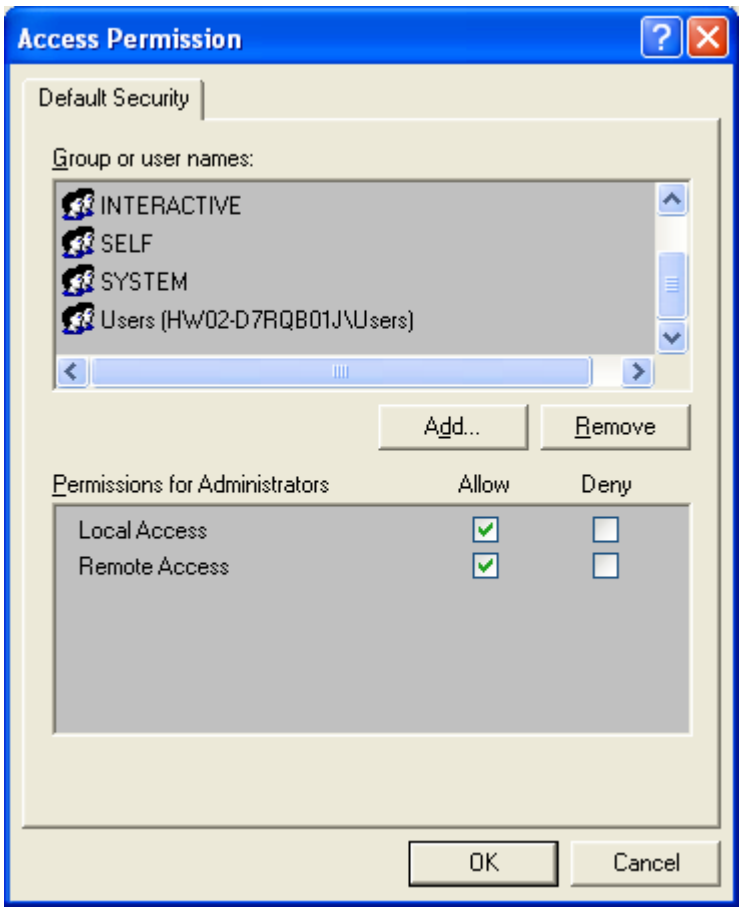


Step A.5) Select the “COM Security” tab:



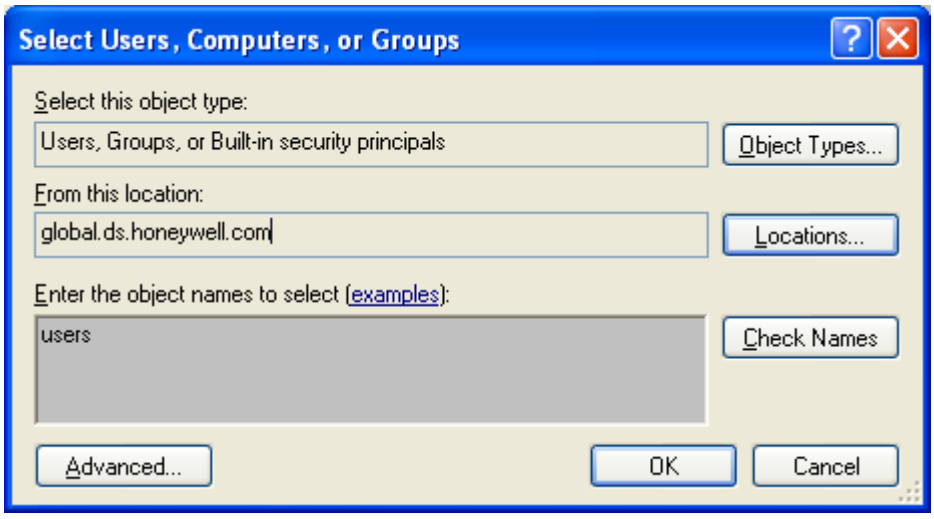
The next series of steps are aimed at ensuring that recognised users are permitted to remotely connect to databases and commincations servers running on this machine.

Step A.6) Select the “Edit Default…” button from the Access Permissions section of the dialog box of the step above in order to see the following dialog box.



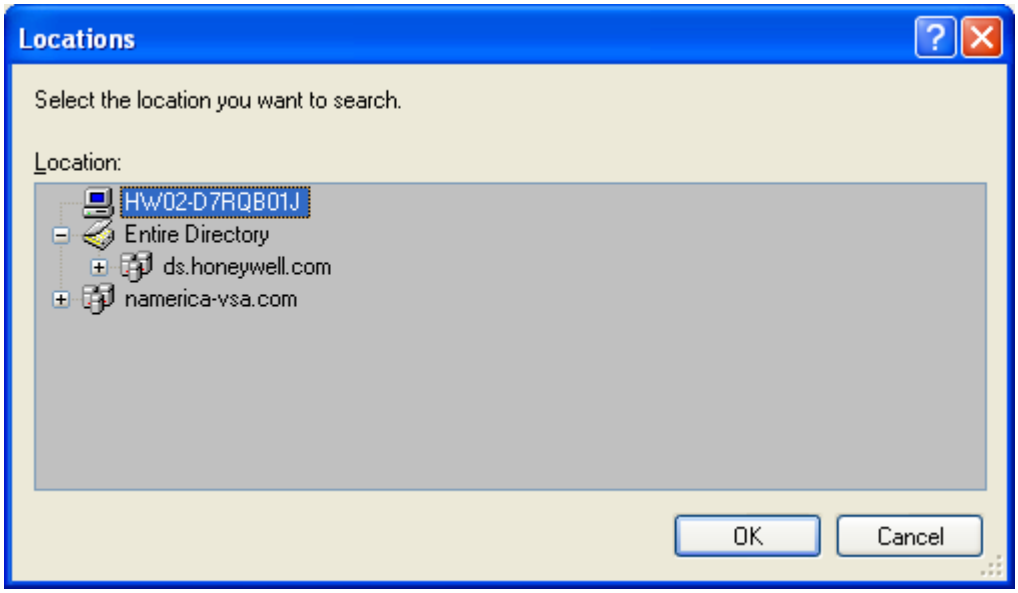
Ensure that the “Users” group for the machine appears in the list titled “Group or user names:” and also make sure that both the “Local Access” and “Remote Access” options for “Allow” are ticked in the bottom-half of the dialog box. If the “Users” entry is missing from the list of groups or users then see Step A.6.1 below for how to add it to the list, otherwise Select OK to commit any modifications that have been made to the settings.

Step A.6.1) To add the “Users” group, click the “Add…” button in order to be presented with the following dialog box:



Enter “users” in the bottom field of the box and then ensure that the name of the computer appears in the “From this location:” field then click OK to commit the addition of the users group.

If the dialog is not presented showing the computer name in the “From this location:” field then it will be necessary to click on the “Locations…” button in order to be presented with the following dialog box:

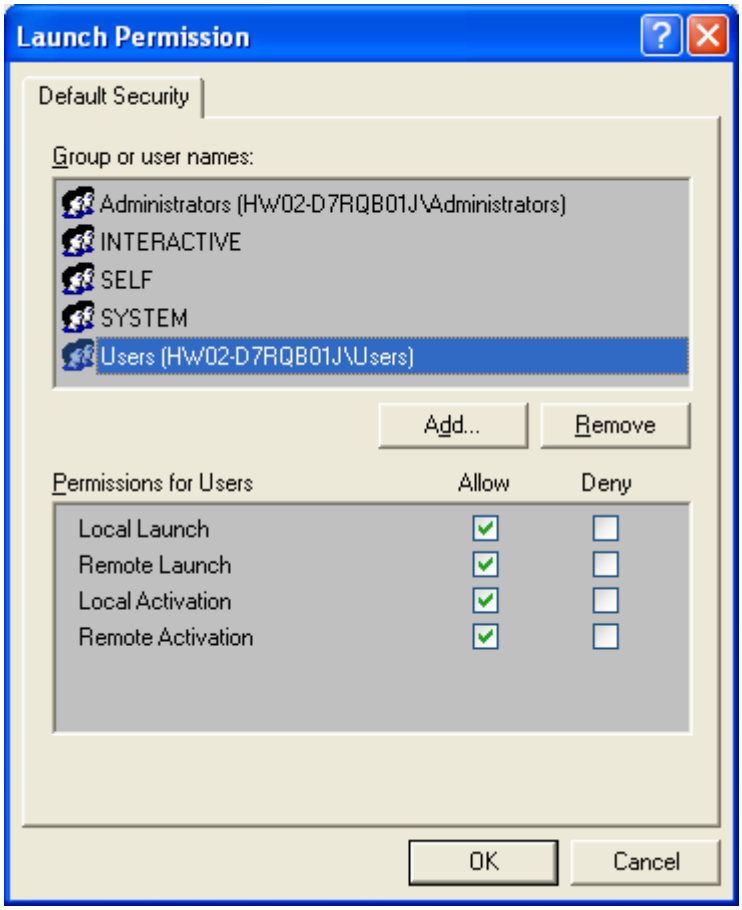


Typically the computer will be the top entry in the list of locations. Make sure that it is selected then click OK to return to the Access Permissions box.

“Users” will now appear in the “Group or User names” window of the default security tab in the Access Permissions box.

Ensure Step A.6 is completed, click ok to return to the “My Computer Properties” box

Step A.7) The final step is to ensure that the users group has appropriate launch and activation permissions on this computer, which is done by clicking on the “Edit Default…” button from the “Launch and Activation Permissions” section of the dialog box of the “Com Security” tab in the “My Computer Properties” box to display the following dialog box.



Ensure that the “Users” group appears in the “Group or user names:” list in the top half of the dialog box, referring to Step A.6.1 if necessary. Verify that in the “Permissions for Users” section that the Allow box is ticked for all four options of “Local Launch”, “Remote Launch”, “Local Activation” and “Remote Activation”. Click OK once this has done and the the DCOM configurations panel can now be closed.

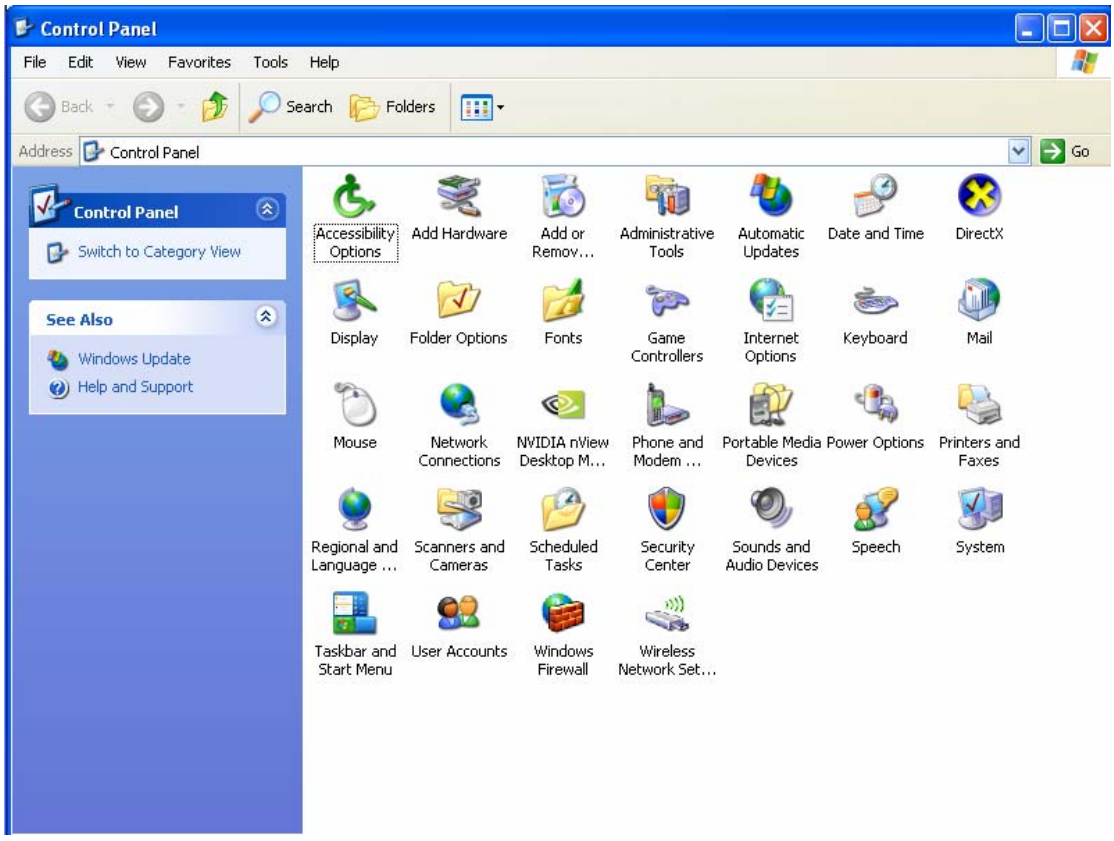
Select “Apply” and then OK to close the “My Computer Properties” box

Step A.8) The system must be restarted in order for the new DCOM settings to take effect.

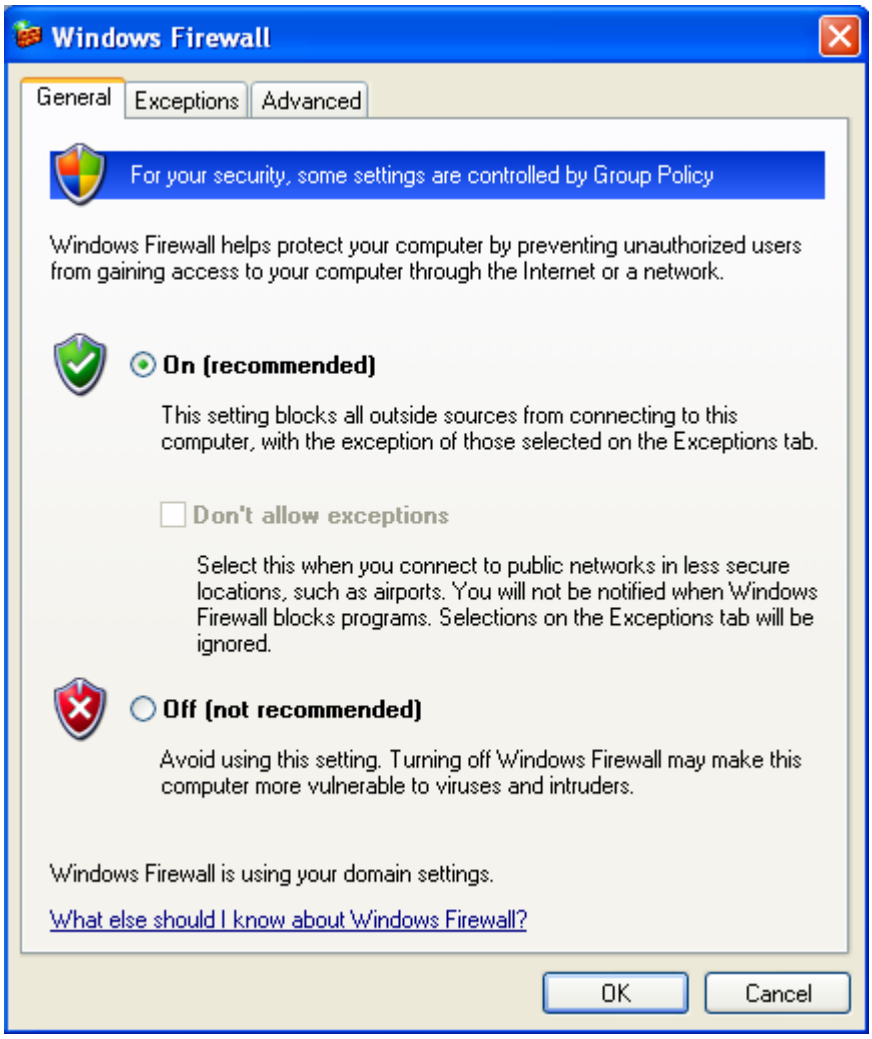
Appendix B Windows XP Firewall

With the advent of Windows XP (SP2) the Windows firewall is now enabled by default. To establish DCOM communications between a client and server the Firewall needs to either be turned off (not recommended) or Exception rules to allow DCOM traffic need to be created.

Step B.1) From the Start menu, select Settings and then Control Panel, the Windows Control Panel (similar to this) will then be shown,

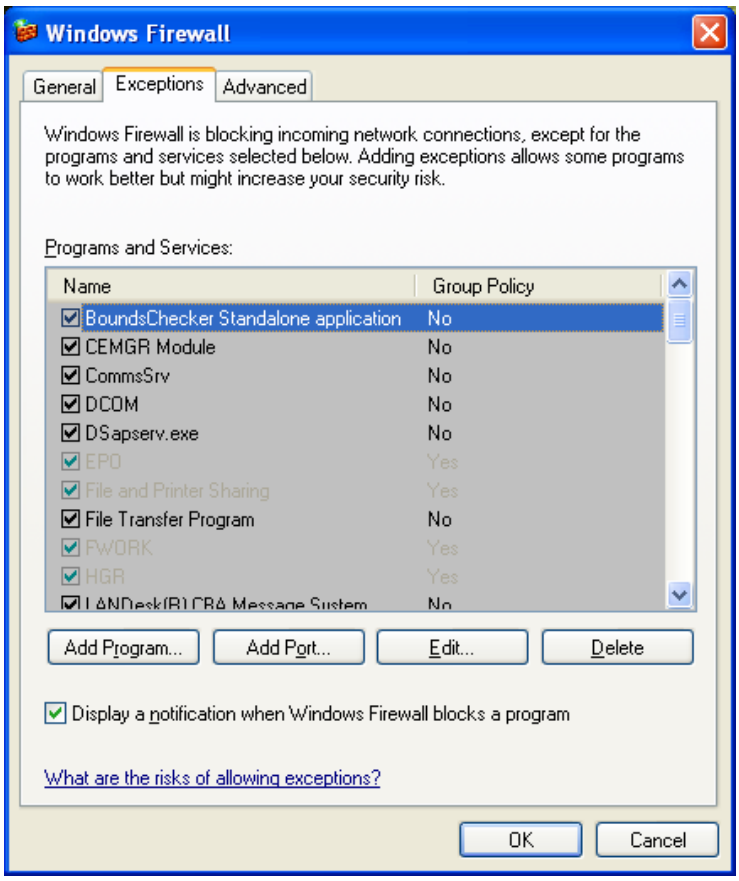


Step B.2) Select Windows Firewall and the following will be shown,

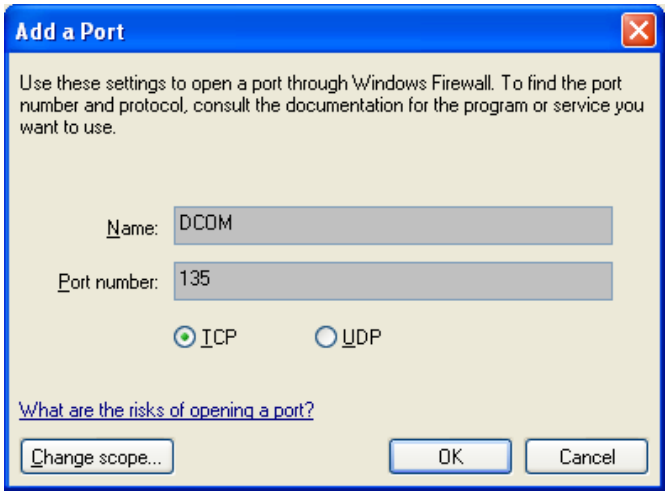


If the Firewall is currently turned off (and the PC is otherwise protected) it can be left turned off and no exception rules need to be created. Otherwise, exception rules must be created to permit general DCOM connections, and then specifically to permit database, communications and trending applications.

Step B.3) The first rule to add will be to permit the port connection for DCOM. Navigate to the “Exceptions” settings but clicking on the “Exceptions” tab in order to see something similar to the following:

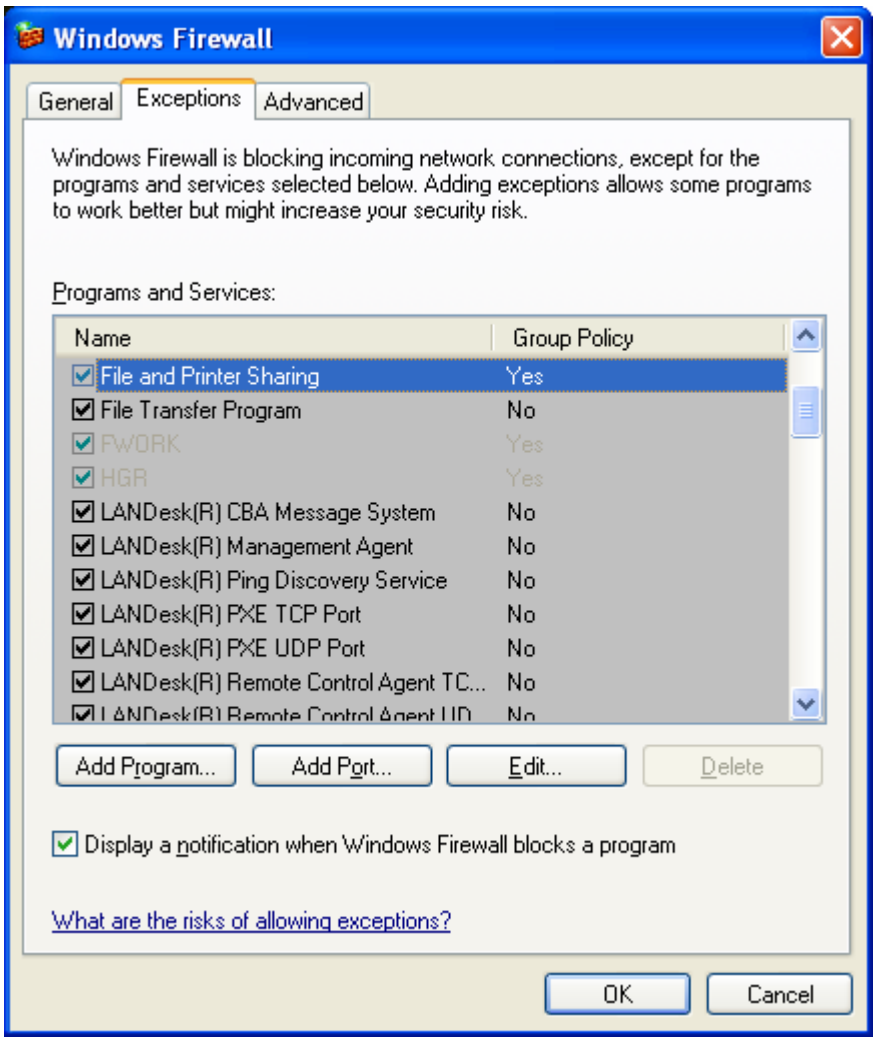


Now click on “Add Port…” button in order to be presented with the following dialog box:

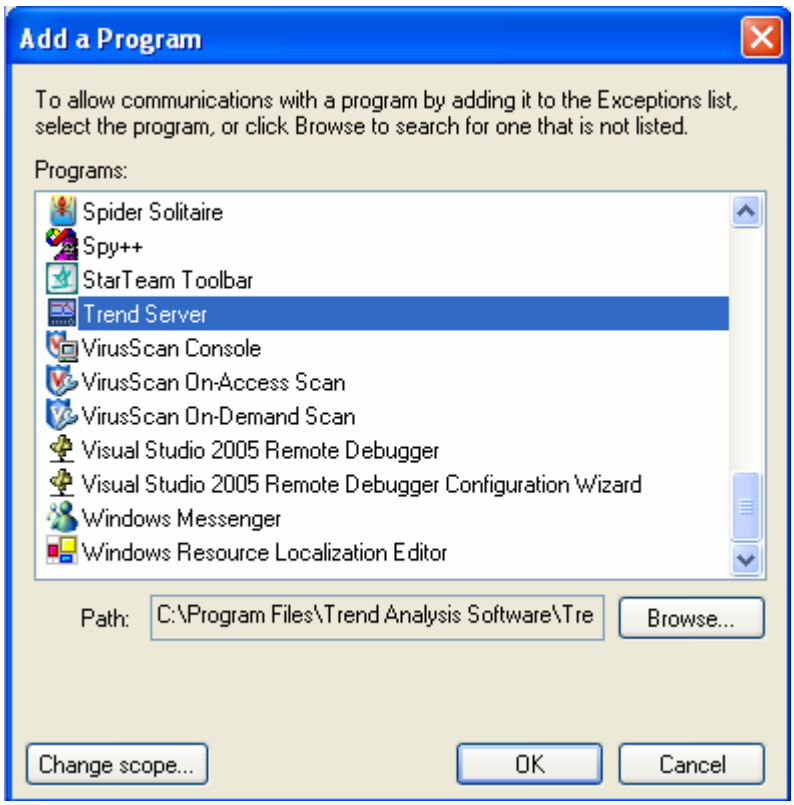


Enter “DCOM” in the “Name:” field and “135” in the “Port number:” field. Ensure that the “TCP” radio button is selected and then click on the OK button to add the rule and return to the Windows Firewall box.

Step B.4) Ensure that the “File and Printer Sharing” is switched on, which is the highlighted option in the screenshot below.



Step B.5) Add the Trend Server application to the list of programs. Start by clicking on the “Add Program…” button in order to see the following dialog box:



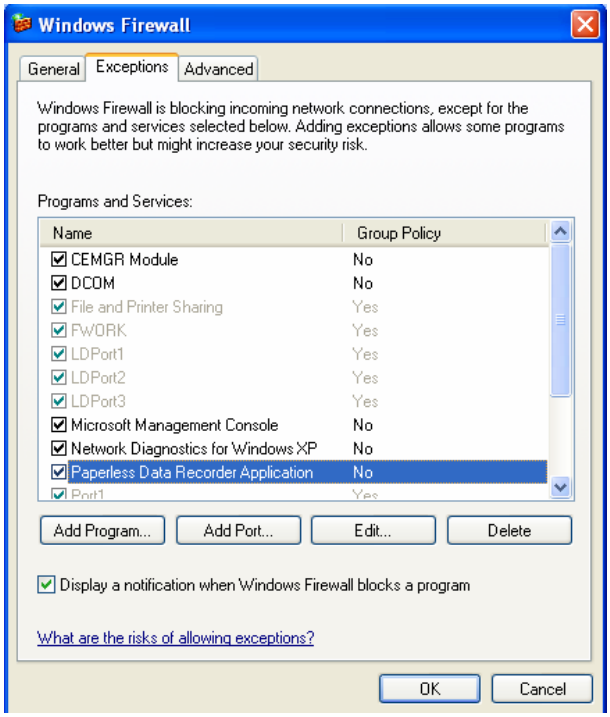
If Trend Server is in the list of programs then select it and press the OK button to create the Exception Rule. If Trend Server is not in the list then use the “Browse…” button to locate where the TrendServerPro.exe file has been installed, highlight it and select Open to create the Exception Rule.

Step B.6) Where the PC is being used as either a communications server or a database server and the main Trend Server application is not always used, these applications will also need to have firewall rules created (Dsapserv.exe or CommSrv.exe). To create these rules use the browse button to navigate to where these files have been installed. The Communications Server is installed in the same location as Trend Server and the Database Server can be found one directory level higher-up. Where the firewall is concerned, it is the top-level application which needs the rule. Other applications or software components will inherit a firewall access from it’s parent.

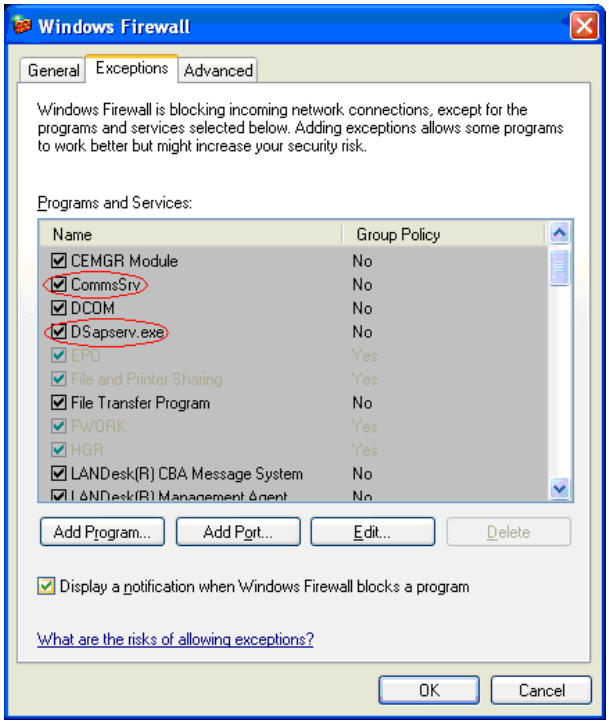
The name of the main application may vary depending on which version has been installed, if there is any doubt the browse button can be used to locate where the application has been installed.

When the new program has been located click OK to return to the Windows Firewall box

Step B.7) There will now be two new rules, one called DCOM and another called Paperless Data Recorder Application. If not, return to Step B.3 and repeat to add “DCOM” port or Step B.5 to add the “Paperless Data Recorder Application” program



Also, if a database server and a communications server have been configured, their rules should appear in the list too:



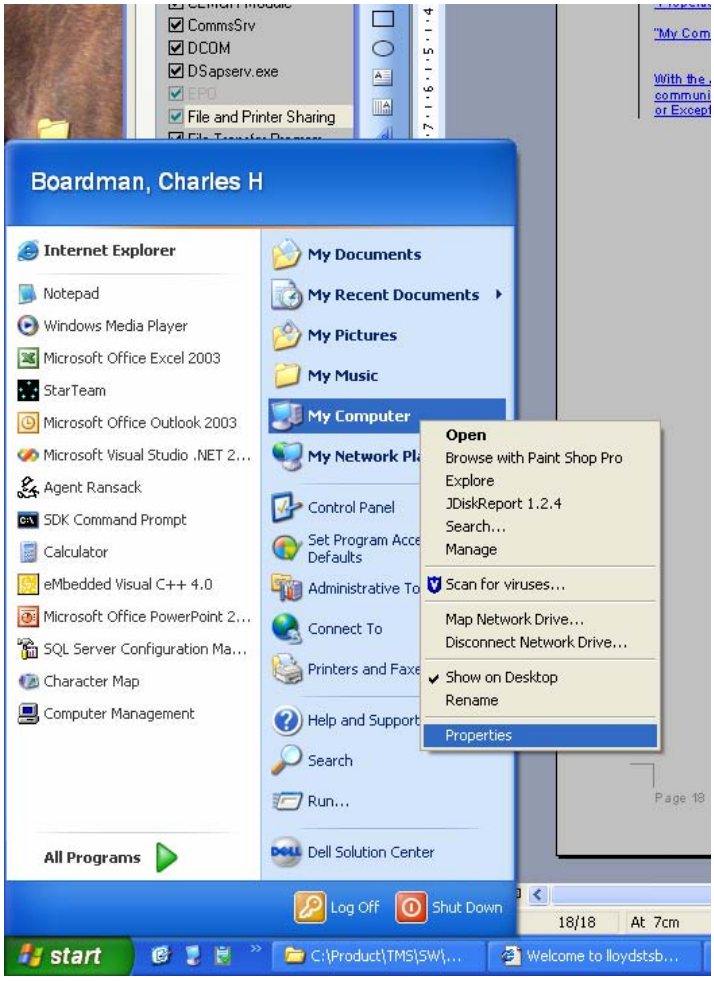
Click OK to finish the Windows Firewall setup

Appendix C Domains: SFS and user accounts

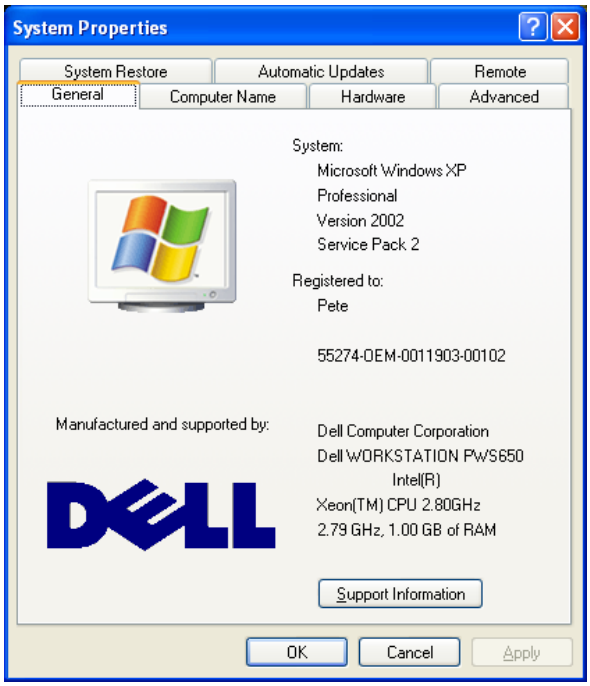
When trying to connect two computers, that are not in the same domain, the authentication for DCOM connections is executed differently. Consequently other aspects of the computer configuration other than the DCOM settings will affect the ability to connect to remote databases and communications servers.

Step C.1) The first step is to verify whether or not a machine is within a domain. This can be done by holding down the right mouse button over “My Computer” to present the context menu, and to select the “Properties” option from that menu.

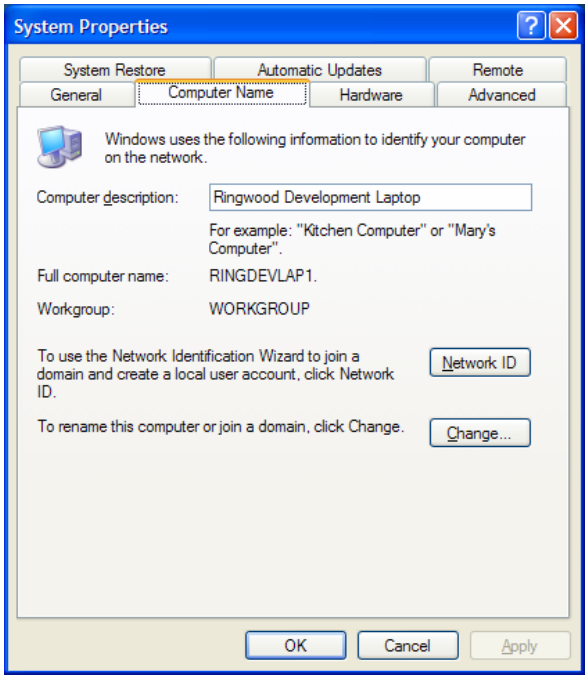
“My Computer” is usually found either on the Desktop and/or in the Start menu:



The “System Properties” window will be displayed, that looks much like the following:



Now select the “Computer Name” tab to see something similar to the following:

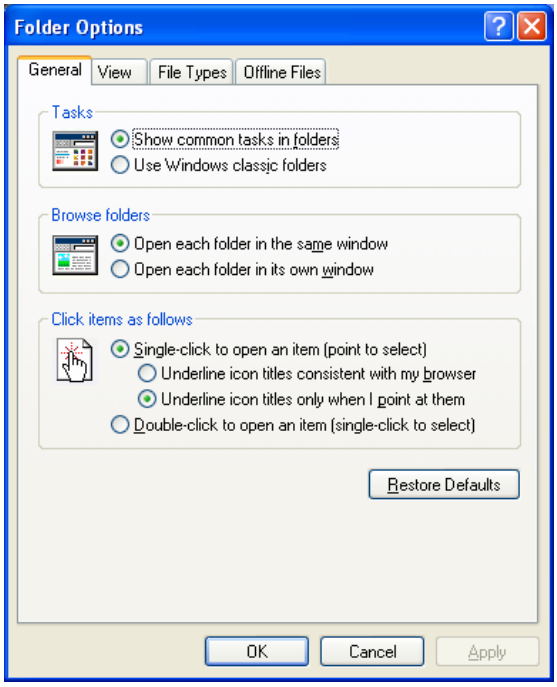


The key information to look out for is the field below the “Full computer name:” field. If the computer is in a domain, then the field will be called “Domain:” otherwise it will state “Workgroup:”. If the field is “Domain:” indicating that the machine is currently within a domain, then the rest of this Appendix is not applicable. Click OK to close the box

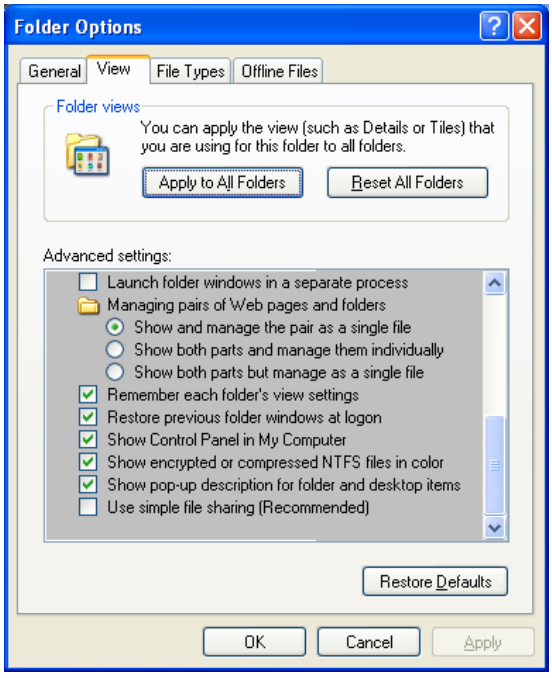
The above screenshot is from a computer that is not in a domain. Note the field below “Full computer name:” is indeed “Workgroup:”.

Step C.2) Switching off Simple File Sharing (SFS) is simple to achieve and does not require a restart of the machine in order to take effect. Go to any open Windows Explorer or open “My Computer” if an explorer is not already open.

Go to the “Tools” menu and select the “Folder options…” menu item. This will present a dialog box as follows:



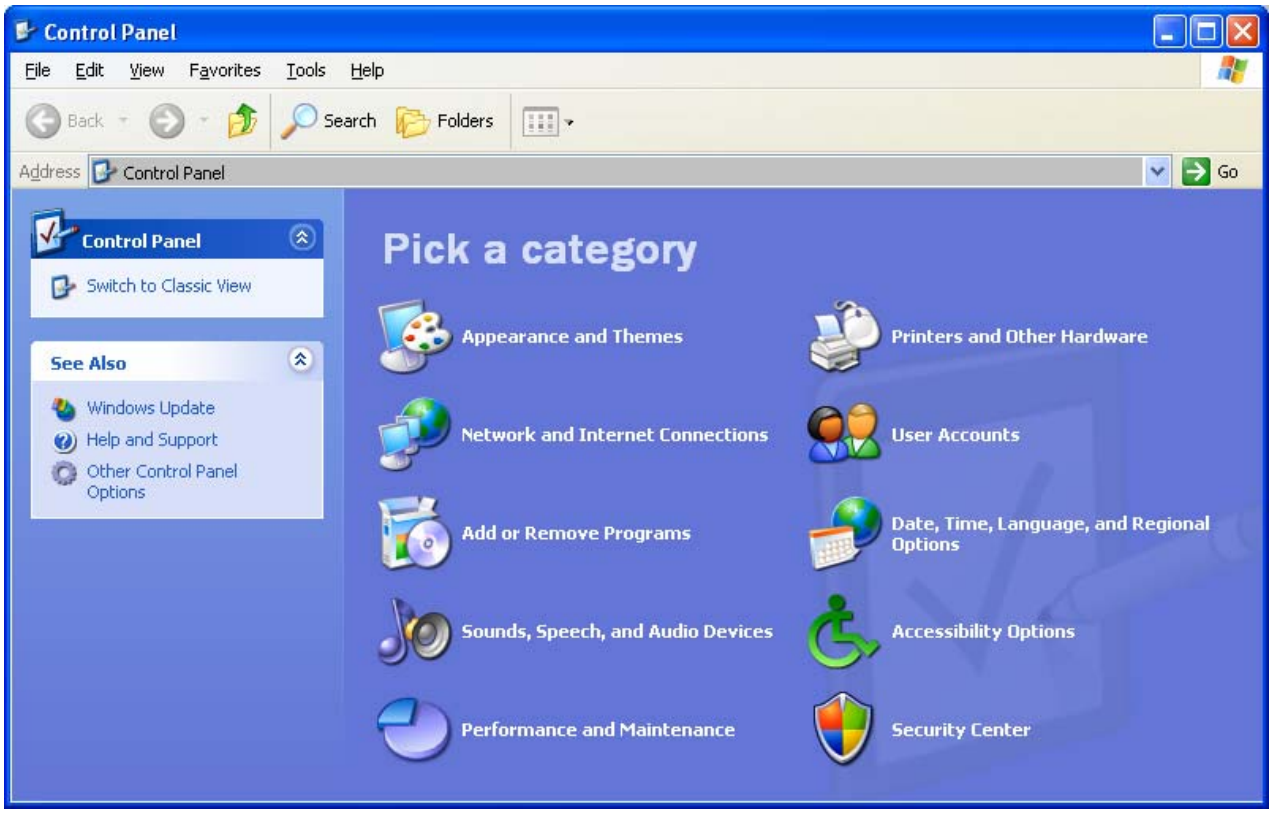
Select the “View” pane in order to be able to see some advanced settings. The “Folder Options” window will change to look something like the following:



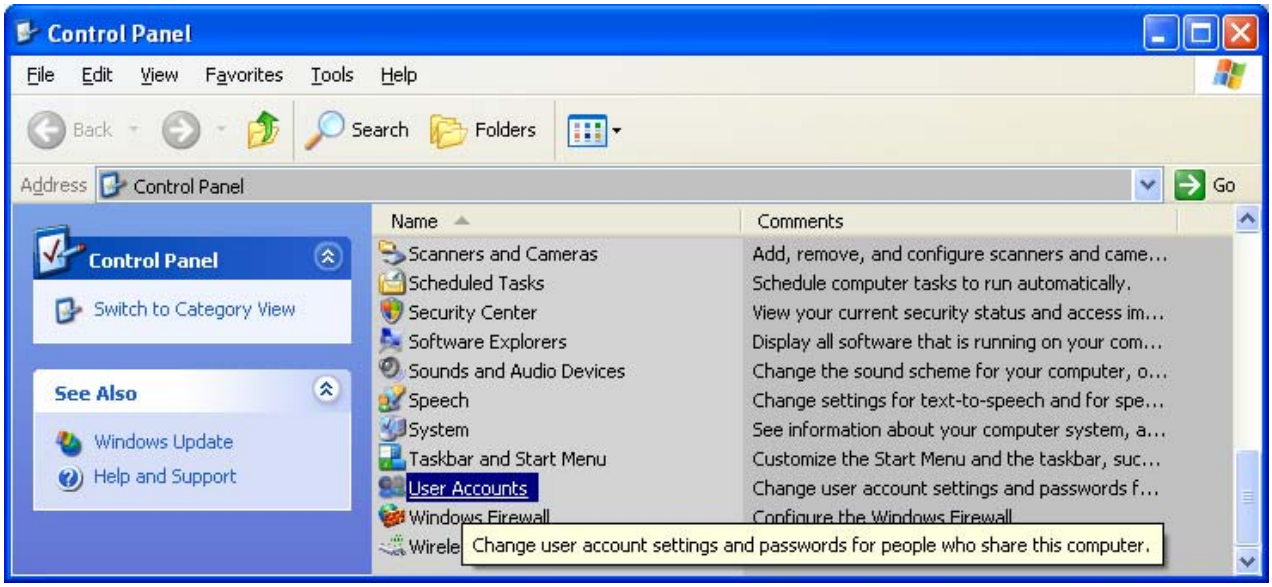
Scroll to the bottom of the “Advanced settings:” area of the window and make sure that the “Use simple file sharing (Recommended)” option is not enabled. It has been disabled in the example screenshot above.

Step C.3) For another machine to be able to remotely connect to a database server or communications server on the current machine, it is necessary for the machines to share common user accounts. At this point, establish which users are likely to log on to either the client or server machine and who will want to be able to connect to remote databases or communication servers.

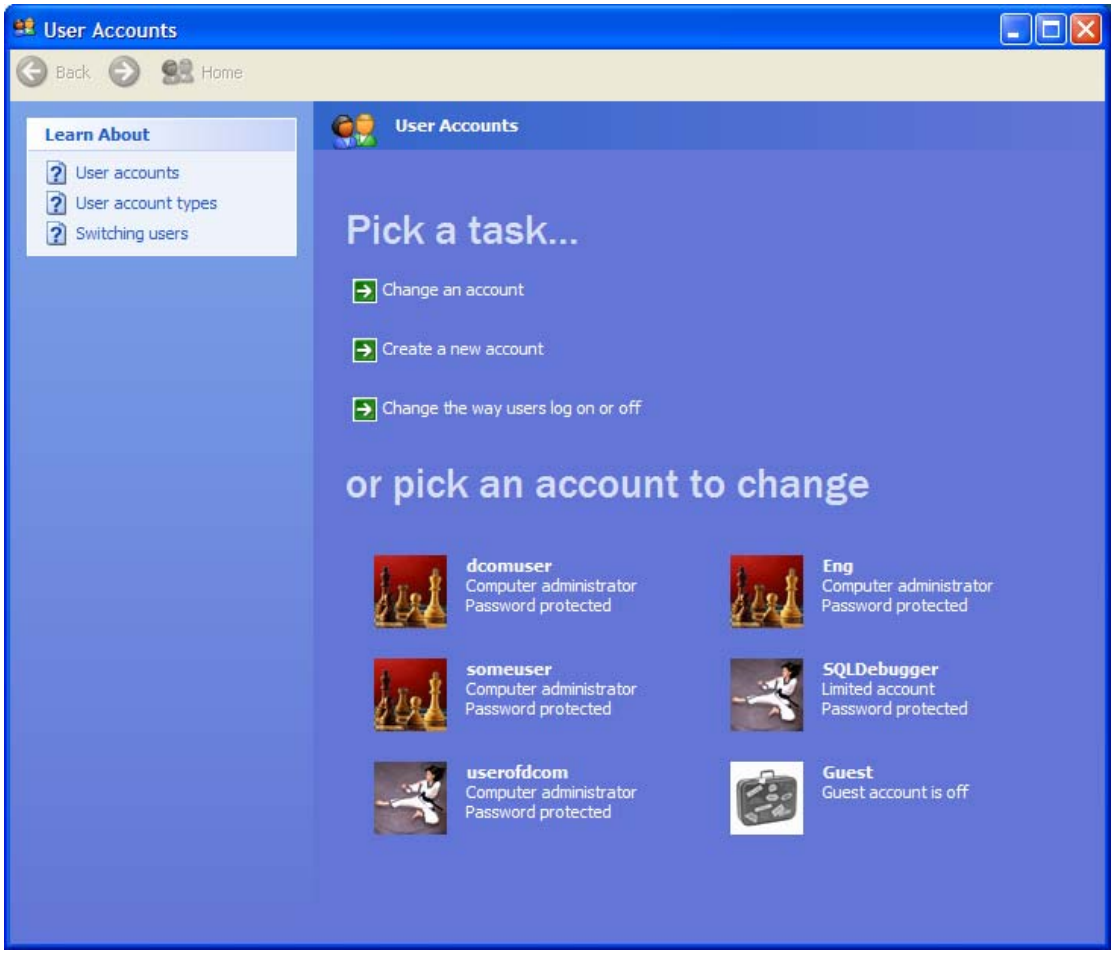
The first thing to do is verify that all of those users have an account on the client and server machines being used. For this, open the Control Panel and one of two possible windows will be presented:



The above is the Category View of the Control Panel and below is the Classic View of the Control Panel:

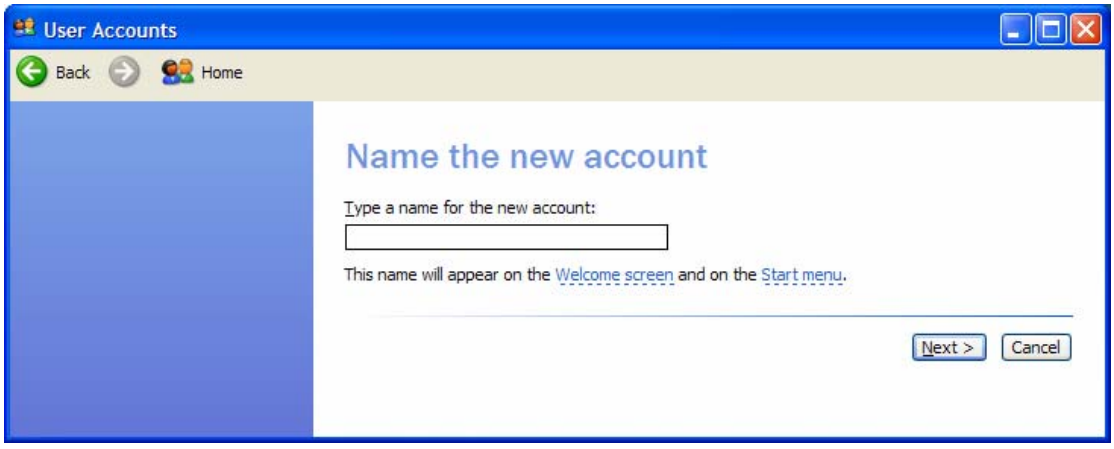


Whichever view of the Control Panel is displayed, open the “User Accounts” entry and a window similar to the following should be displayed:

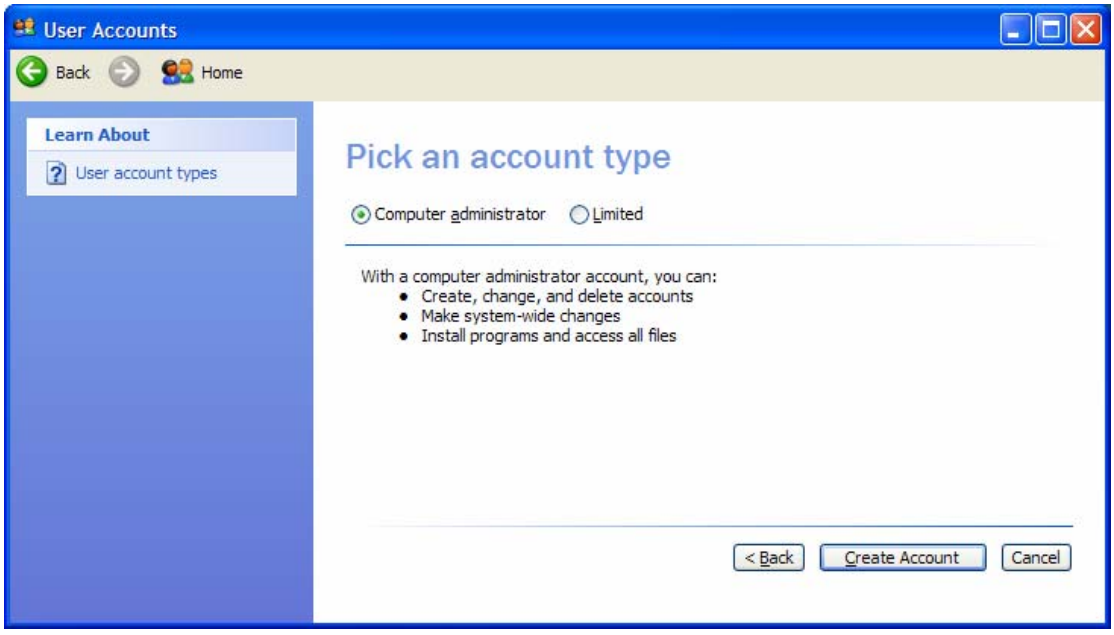


Observe that the bottom part of the window lists the users of the machine, so it should be quite easy to check whether the necessary users all have an account on the machine.

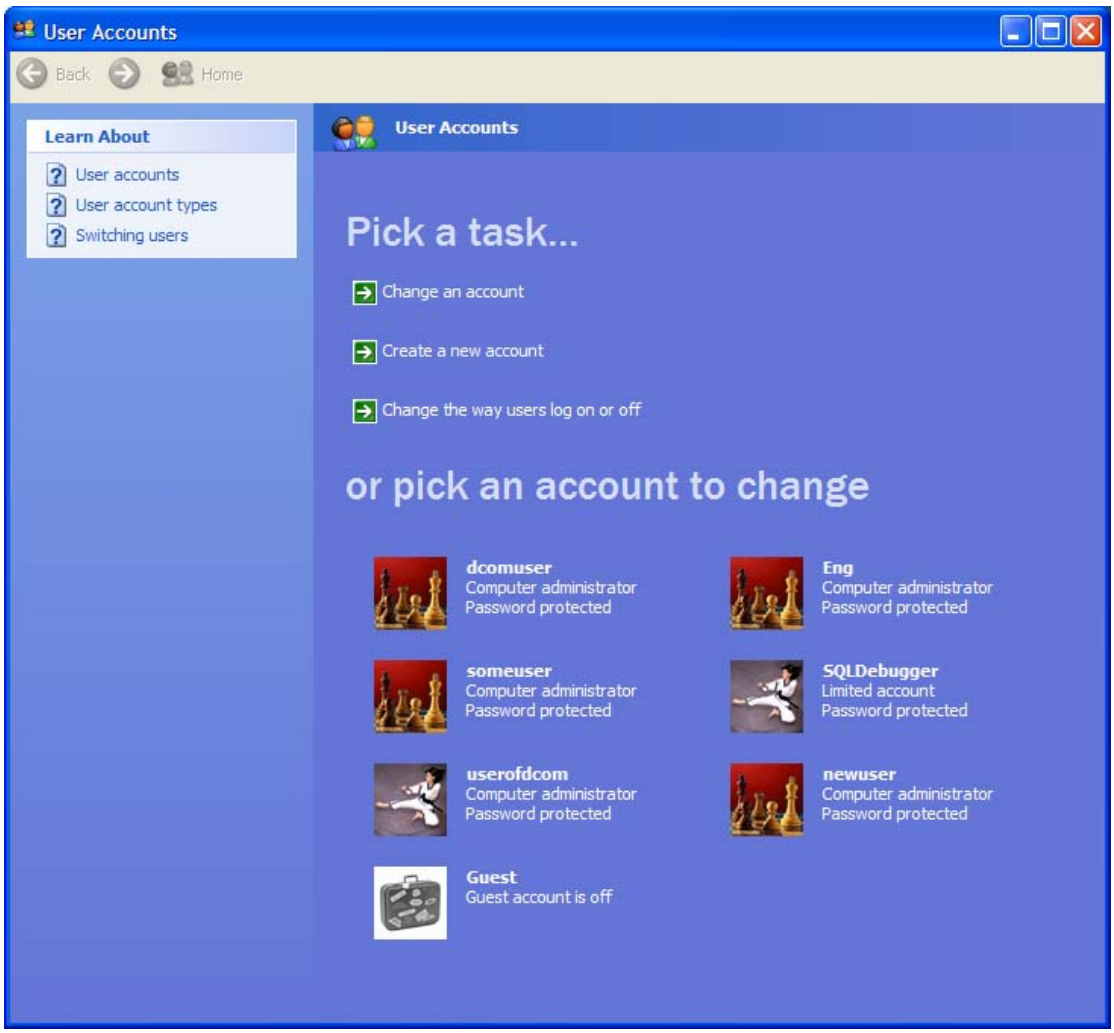
Step C.4) If a user is not listed then it will be necessary to add a new account. So click on “Create a new account” to be presented with the following:



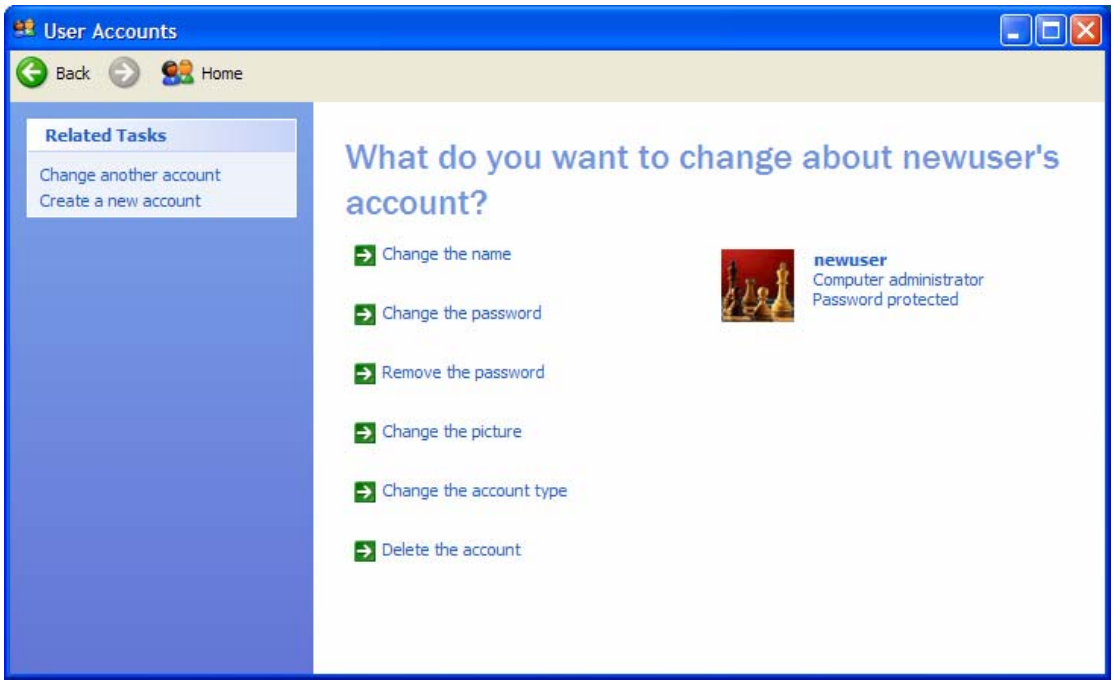
Enter the user name for the account and click on “Next >” button to see the following:



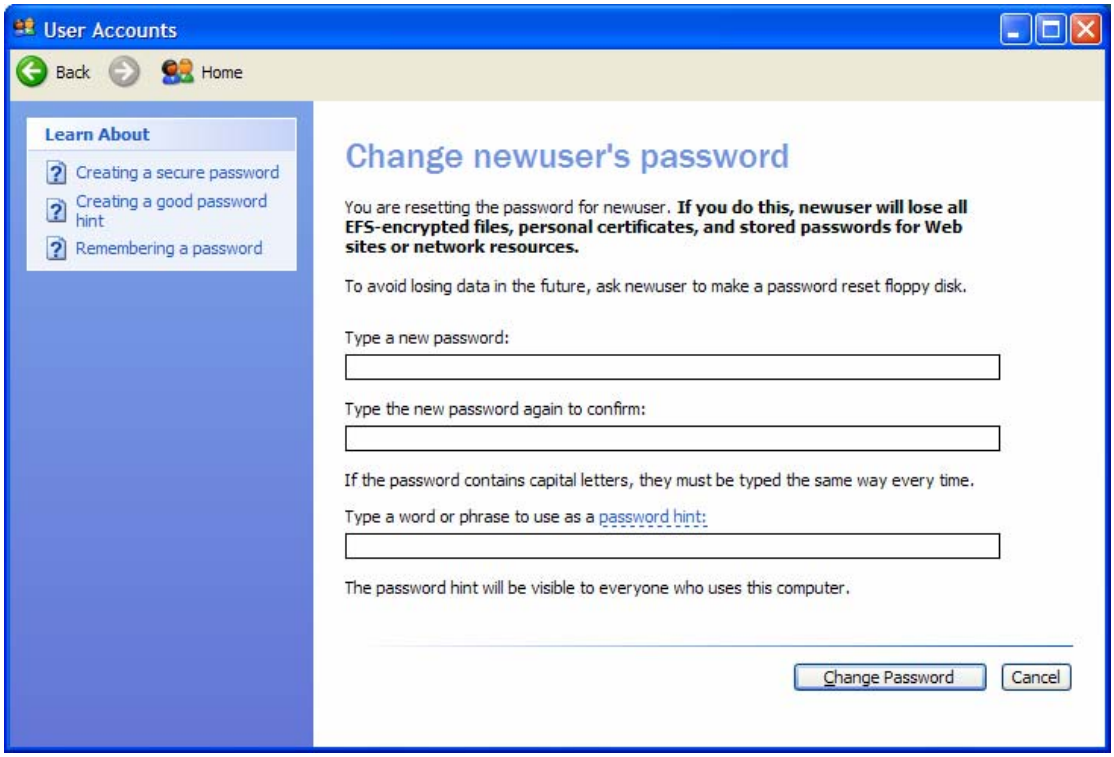
Make sure that “Computer administrator” is the chosen account type and then click on the “Create Account” button. The “User Accounts” window will be displayed once more, this time with the new user added to the list at the bottom of the window, as follows:



Step C.5) Ensure that the password for the user account is the same on all machines. To change a password, select the account from the “User Accounts” window to get an option window as follows:



Then simply select the “Change the password” option to get the following window:



Specify the new password, committing the change by selecting “Change Password”.

Step C.6) Restart the machine in order to be sure that all new and modified user account settings take affect with respect to successfully achieving DCOM connections.