

Establishing OPC Communication on Windows XP SP2 and Windows 2003 SP1

July 4, 2006

Users will often experience difficulties with OPC Communication on Windows XP SP2 and Windows 2003 SP1 due to advanced security settings. This document describes how to disable these security settings to allow OPC Communication.

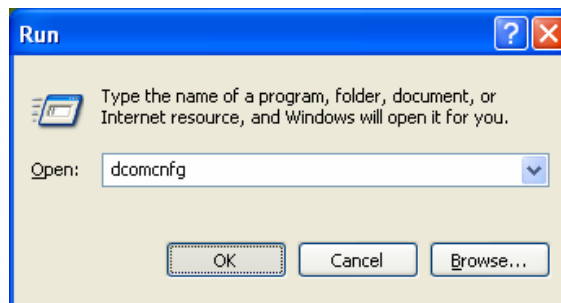
DCOM Security Settings

OPC uses ActiveX COM and DCOM to communicate, so we must open our DCOM permissions to allow this.

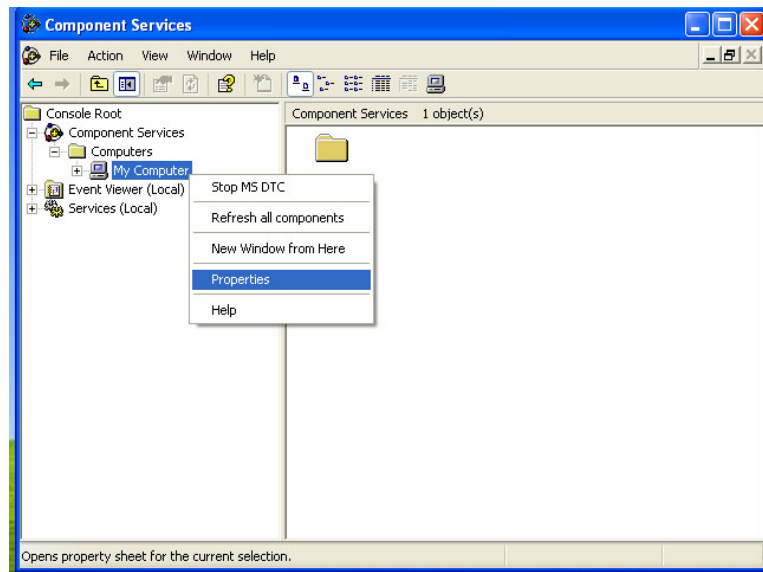
1. Go to 'Start->Run'



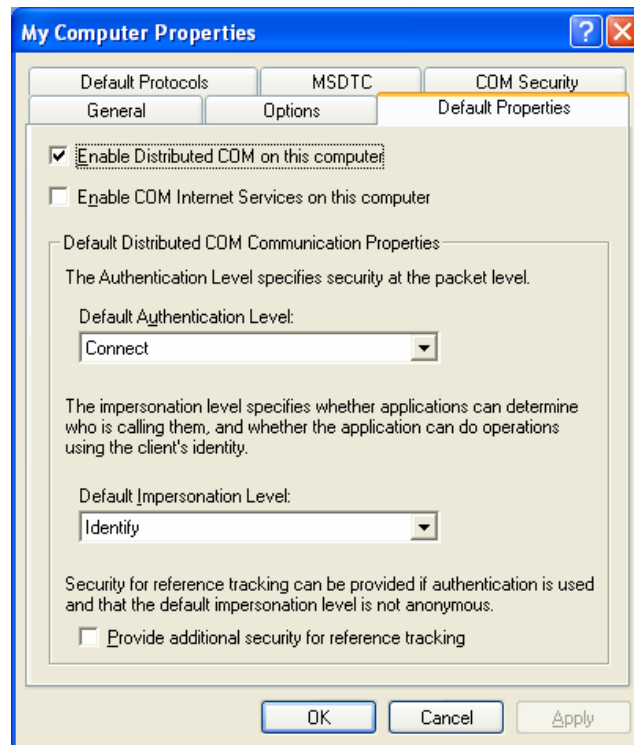
2. Type in 'dcomcnfg' and click OK.



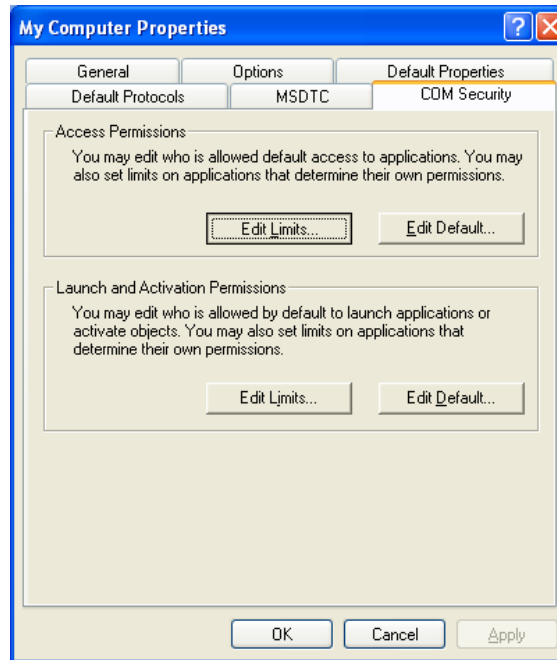
3. Go to 'Console Root->Component Services->Computers->My Computer'. Right-click on 'My Computer' and select 'Properties'.



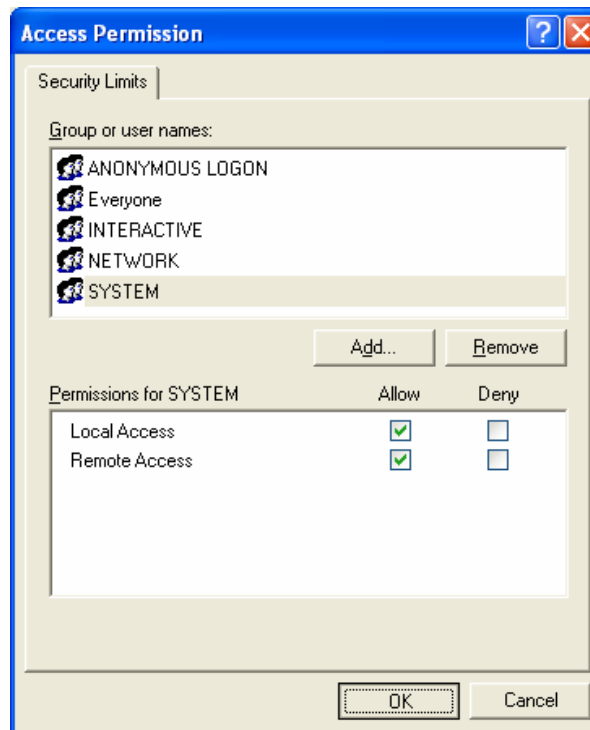
4. Go to the 'Default Properties' tab and ensure that your Window matches the one shown below:



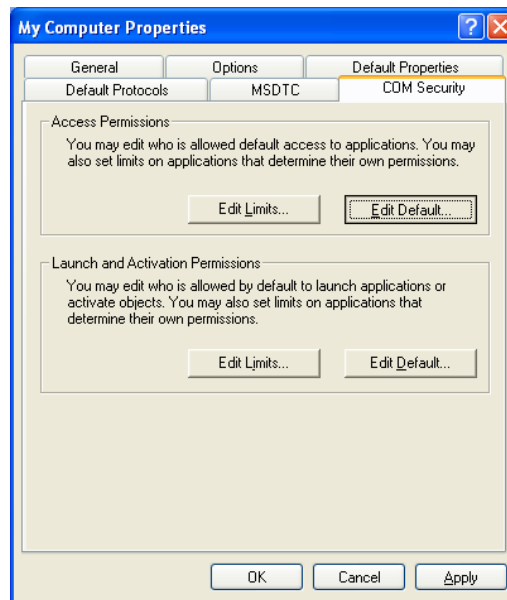
5. Go to the 'COM Security' tab. Under 'Access Permissions', click on the 'Edit Limits' button.



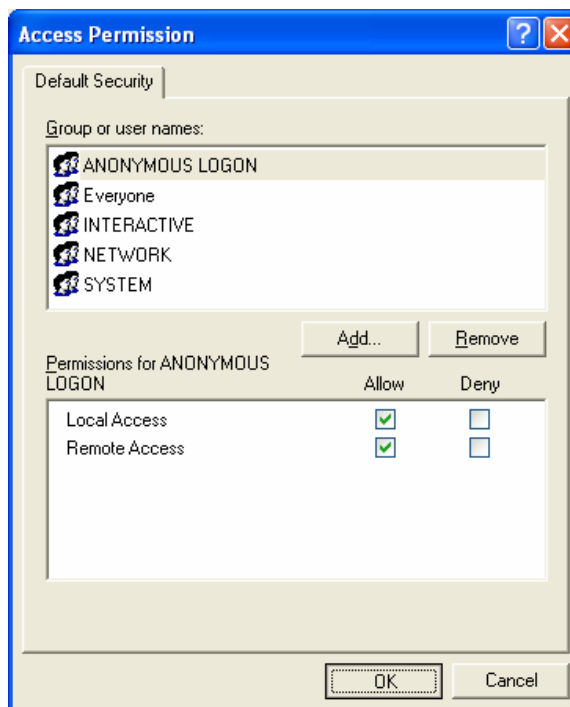
6. Ensure that you have allowed permissions to 'Anonymous Logon', 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.



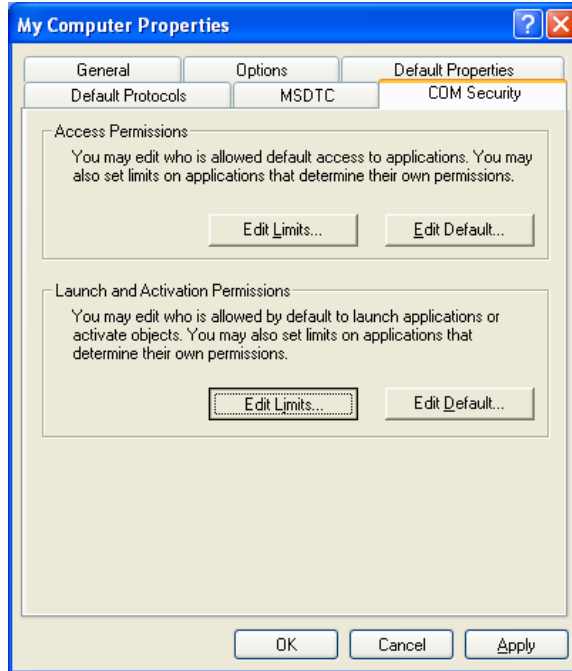
7. Under 'Access Permissions', select the 'Edit Default' button.



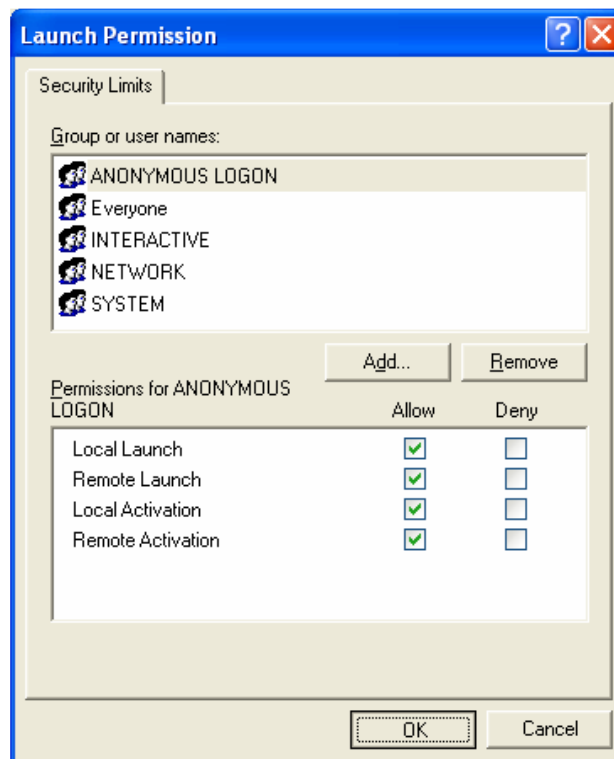
8. Ensure that you have allowed permissions to 'Anonymous Logon', 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.



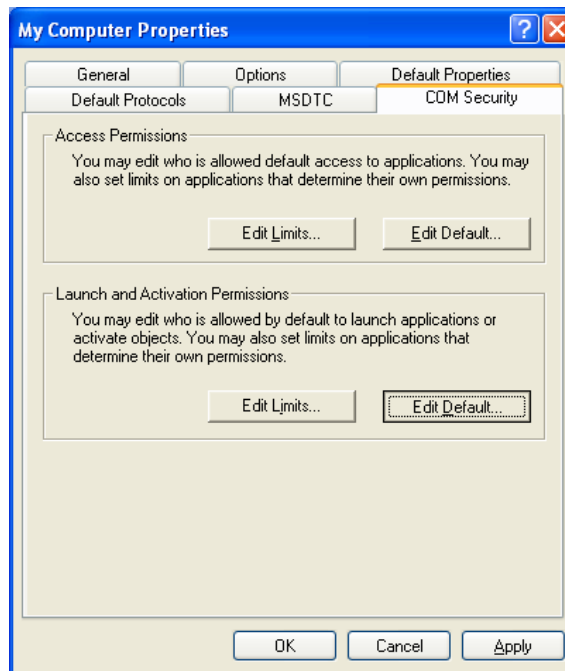
9. Under 'Launch and Activation Permissions', select 'Edit Limits'.



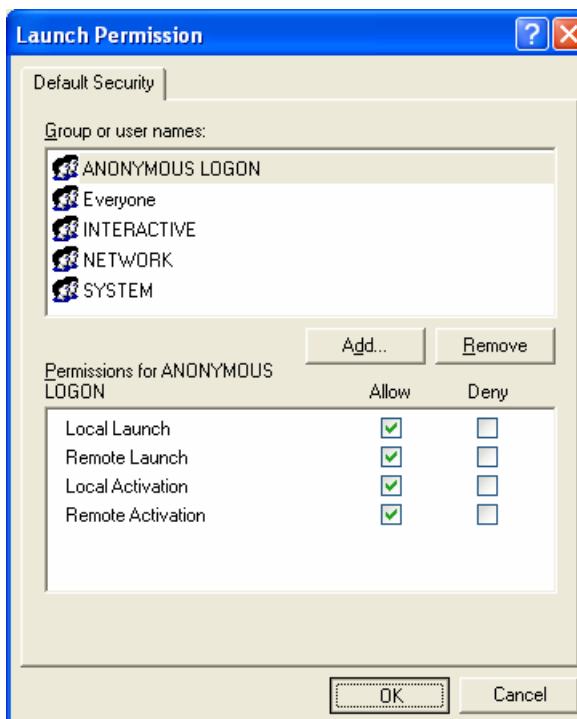
10. Ensure that you have allowed permissions to 'Anonymous Logon', 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.



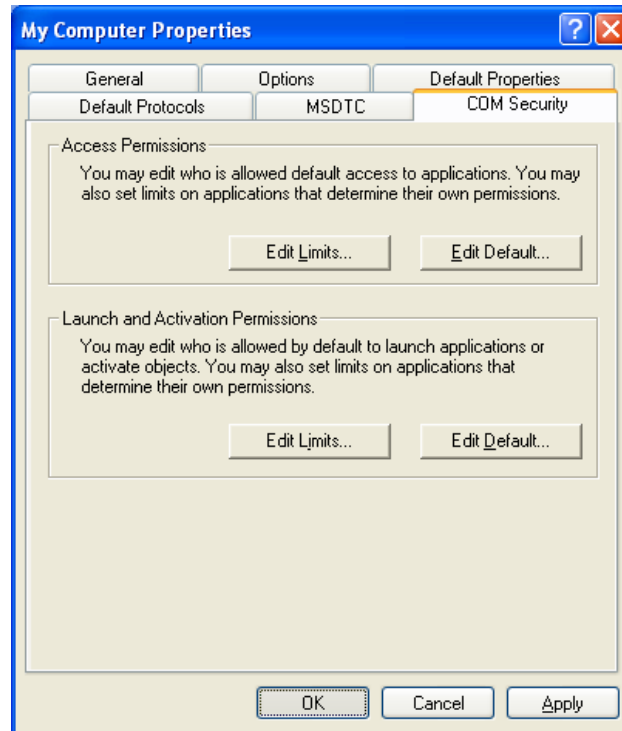
11. Under 'Launch and Activation Permissions' select 'Edit Default'.



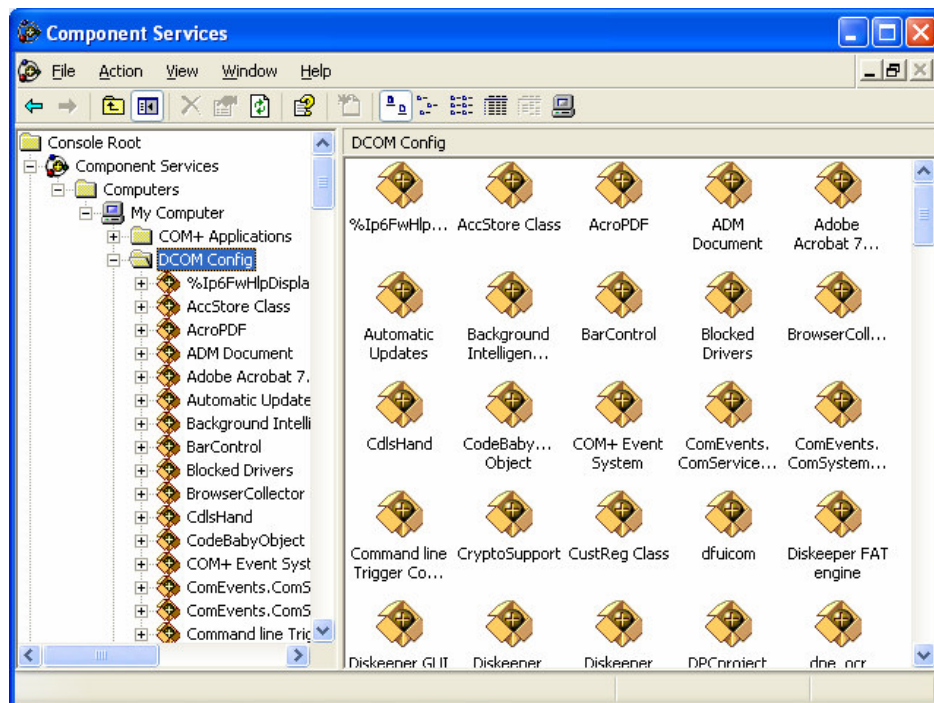
12. Ensure that you have allowed permissions to 'Anonymous Logon', 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.



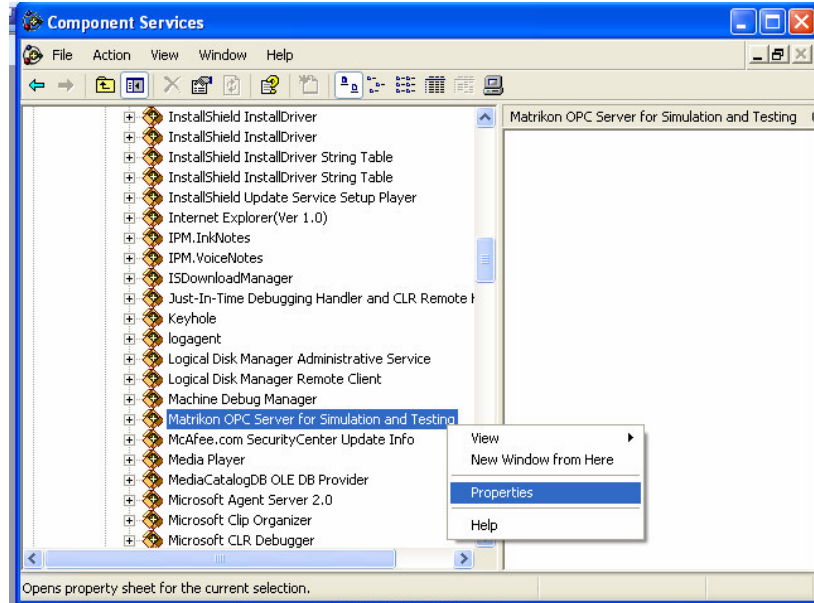
13. We have successfully configured the default DCOM settings. Click OK to return to the Component Services window.



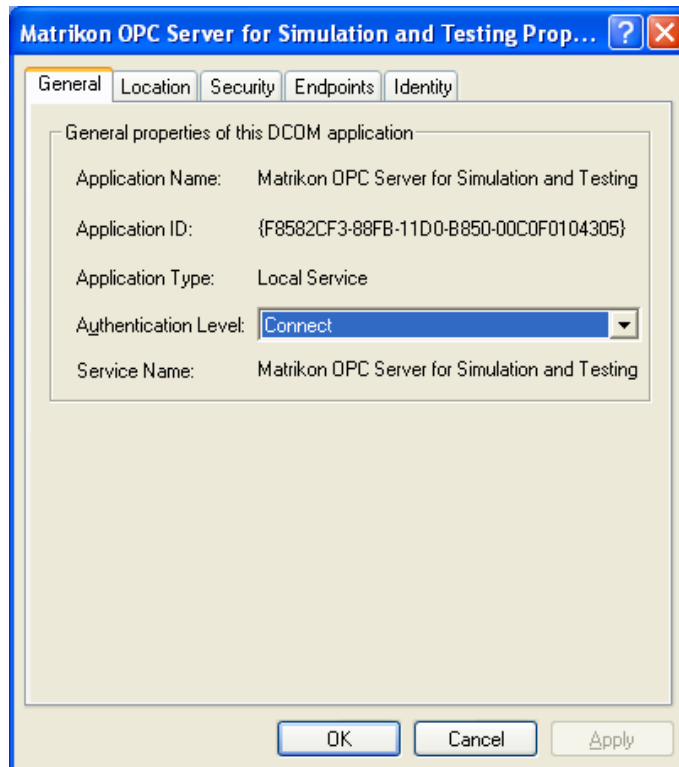
14. Under 'My Computer', open the folder labelled 'DCOM Config'



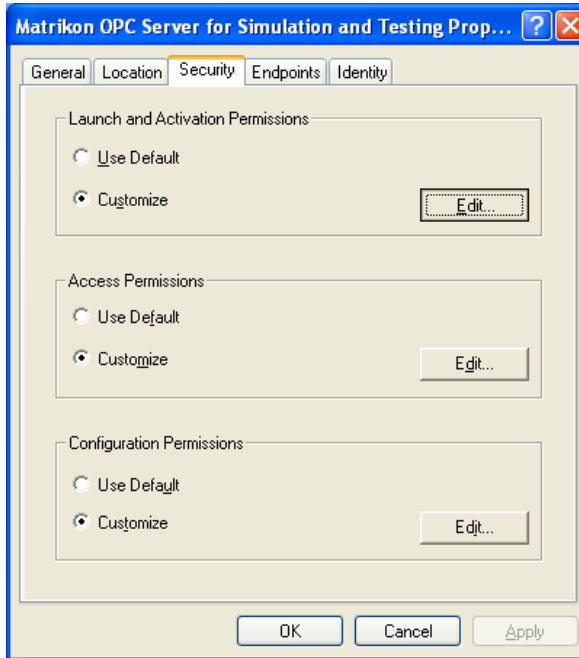
15. Browse to your OPC Server, right-click on it, and select 'Properties'.



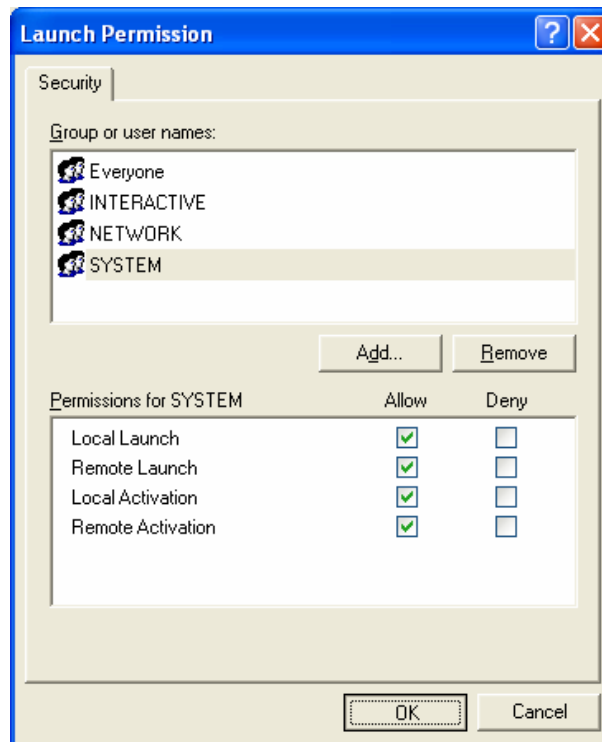
16. Under the 'General' tab, set the Authentication Level to 'Connect'.



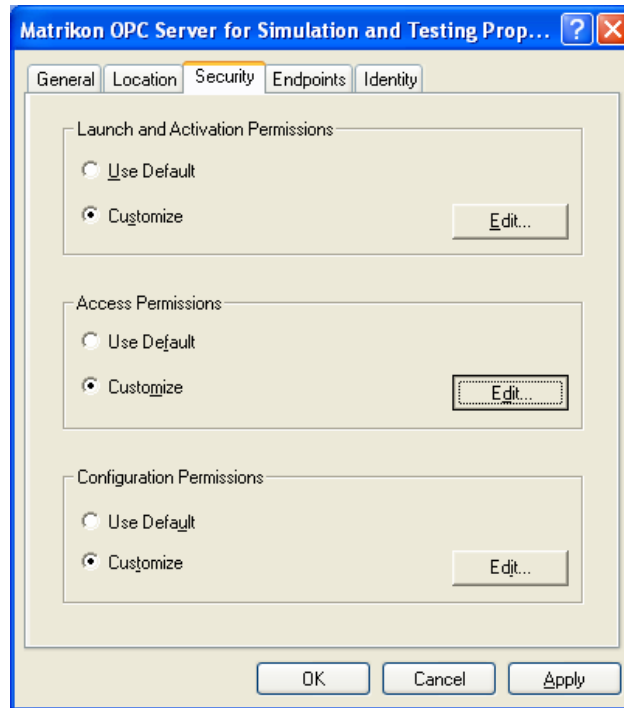
17. Go to the 'Security' tab. Under 'Launch and Activation Permissions', select the 'Customize' button. Then click Edit.



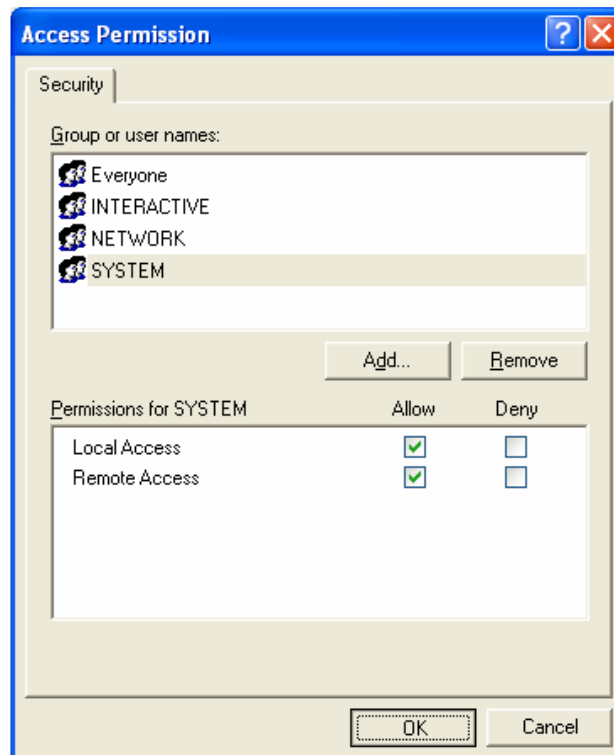
18. Ensure that you have allowed permissions to 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.



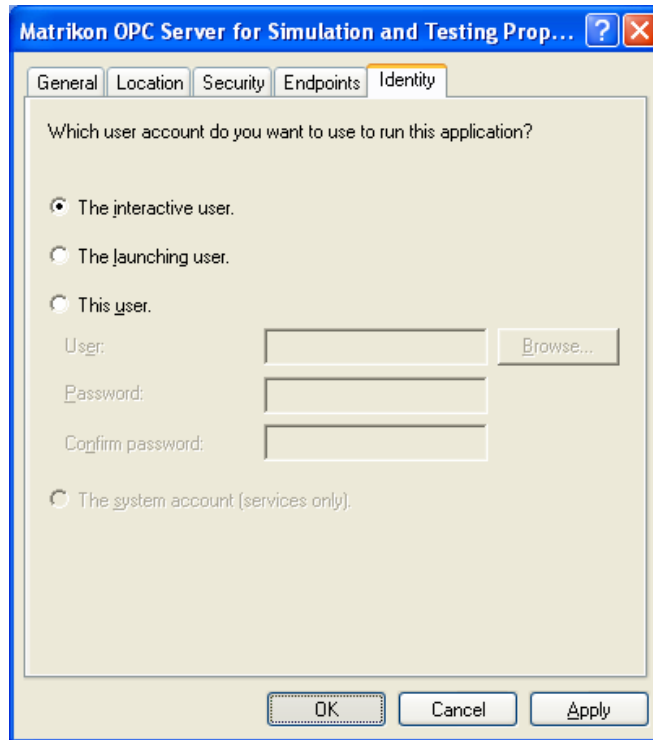
19. Under 'Access Permissions' choose the 'Customize' button. Then click Edit.



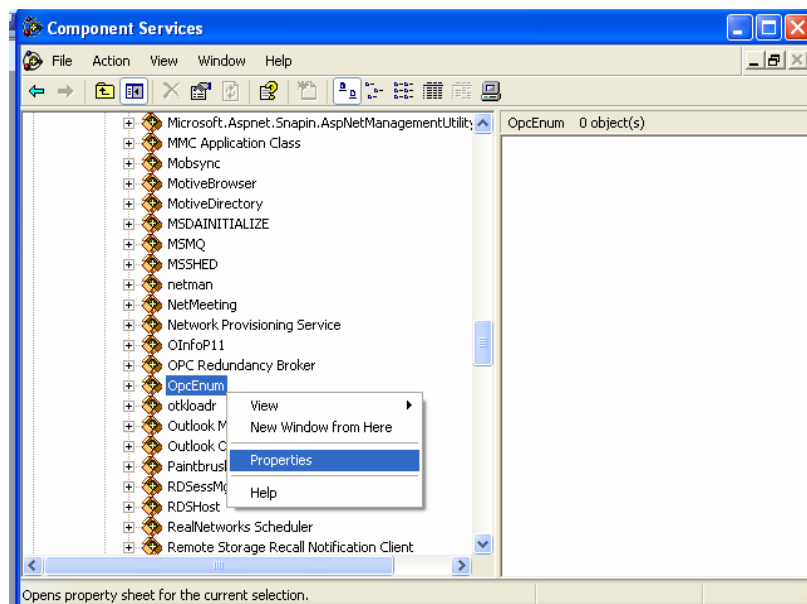
20. Ensure that you have allowed permissions to 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.



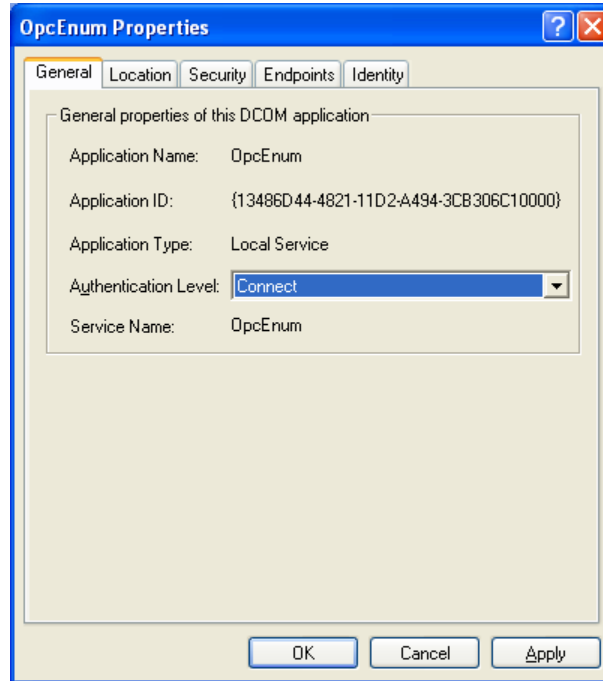
21. Go to the 'Identity' tab. Ensure that your server is either running as 'The interactive user' OR, if it is running as a service, 'The system account'. Click OK to return to the Component Services window.



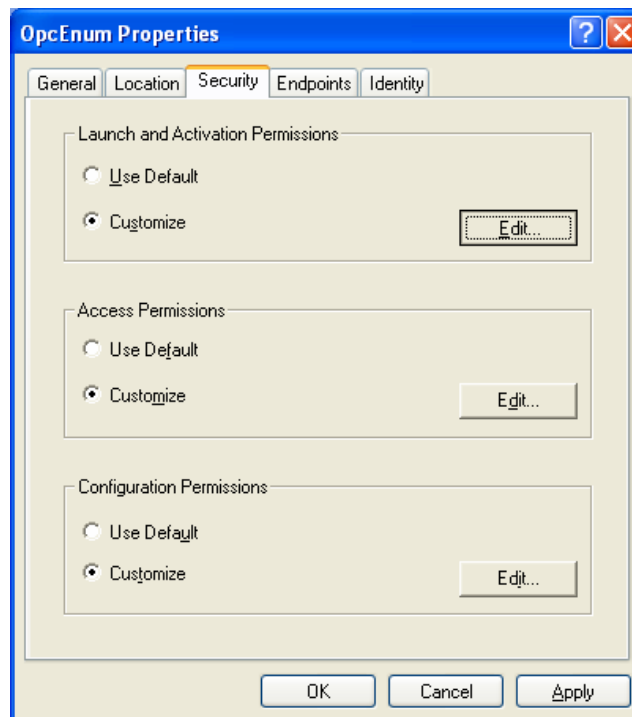
22. In the 'DCOM Config' folder browse to 'OpcEnum'. Right click on it and select 'Properties'.



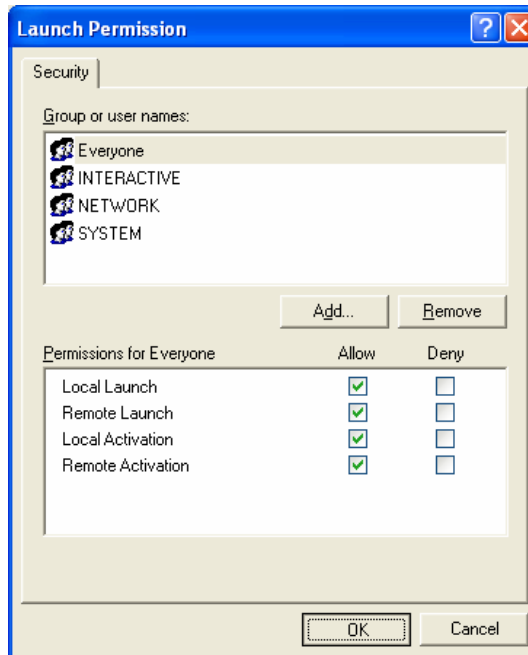
23. Under the 'General' tab ensure that the Authentication Level is set to 'Connect'.



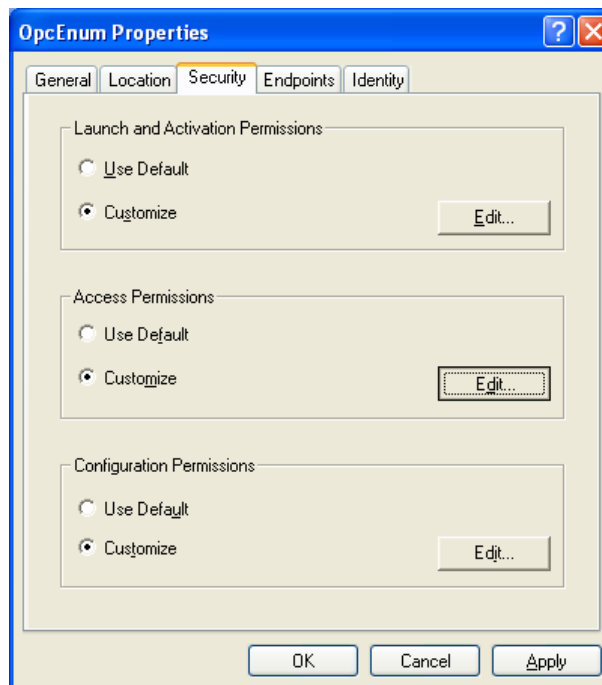
24. Go to the 'Security' tab. Under 'Launch and Activation Permissions', select the 'Customize' button. Then click Edit.



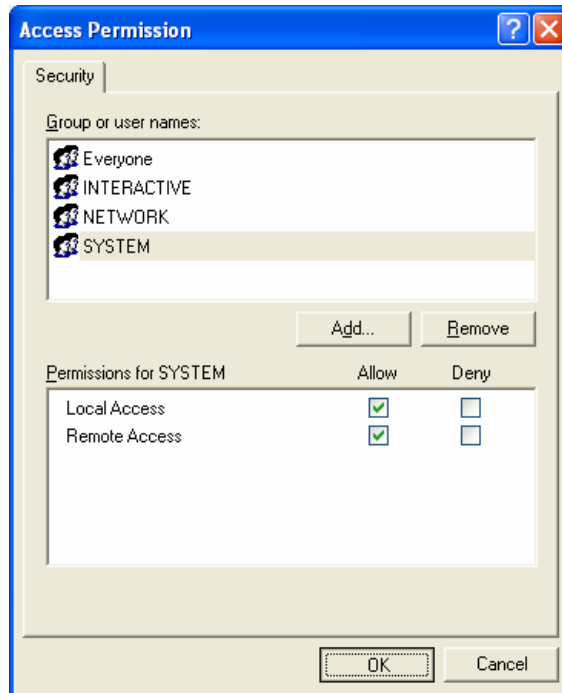
25. Ensure that you have allowed permissions to 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.



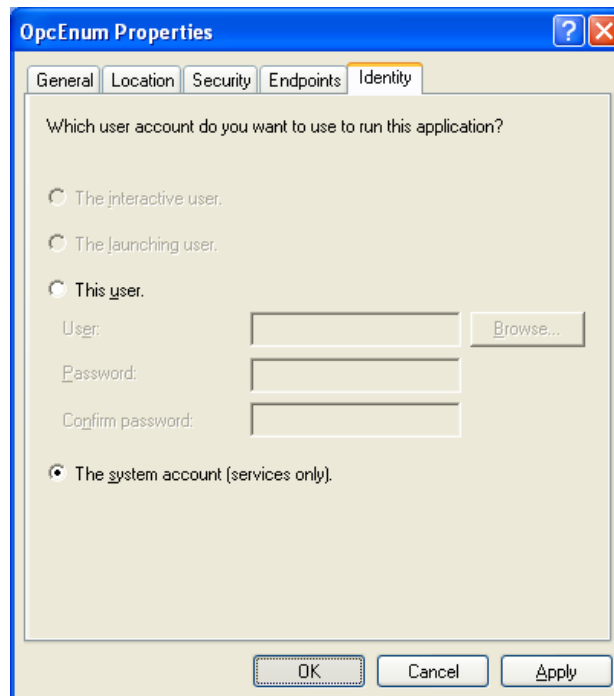
26. Under 'Access Permissions' select the 'Customize' button. Then click Edit.



27. Ensure that you have allowed permissions to 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.



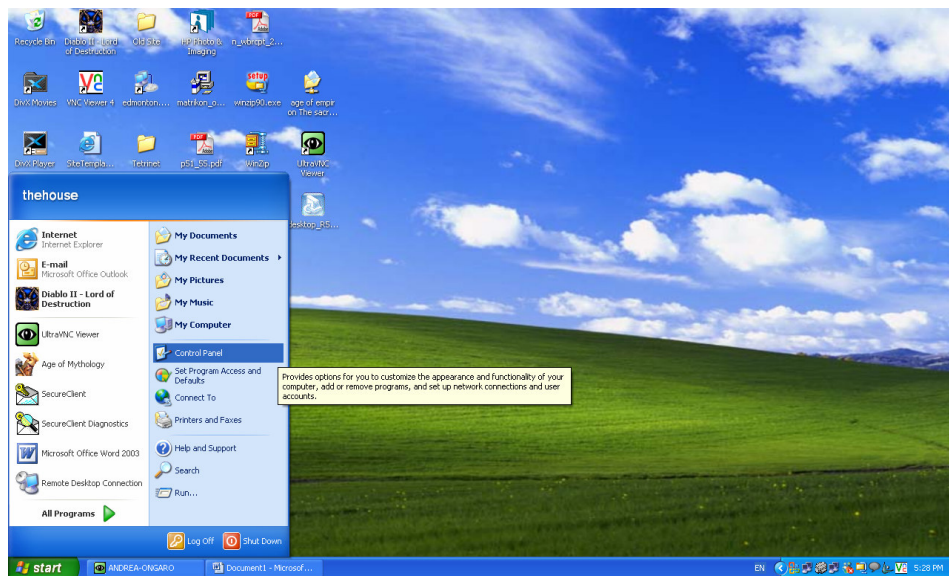
28. Go to the 'Identity' tab. The user should be set to 'The system account', as OpcEnum runs as a service. Click OK. The DCOM settings on this machine are now correct.



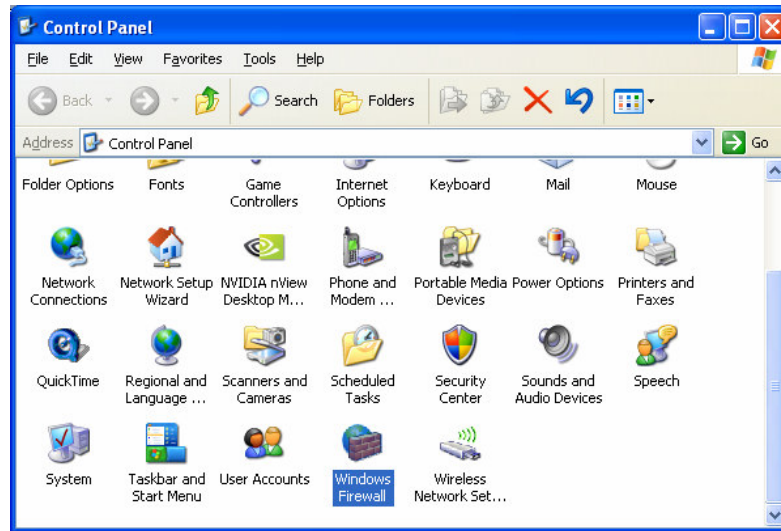
The Windows Firewall

If the Windows Firewall is up and running, it will interfere with communication between applications on the system. There are ways to specify which applications are allowed through the Firewall – if you wish to do so, documents are available from the OPC Foundation which describe the procedure (www.opcfoundation.org). Otherwise disable the firewall by walking through the following steps:

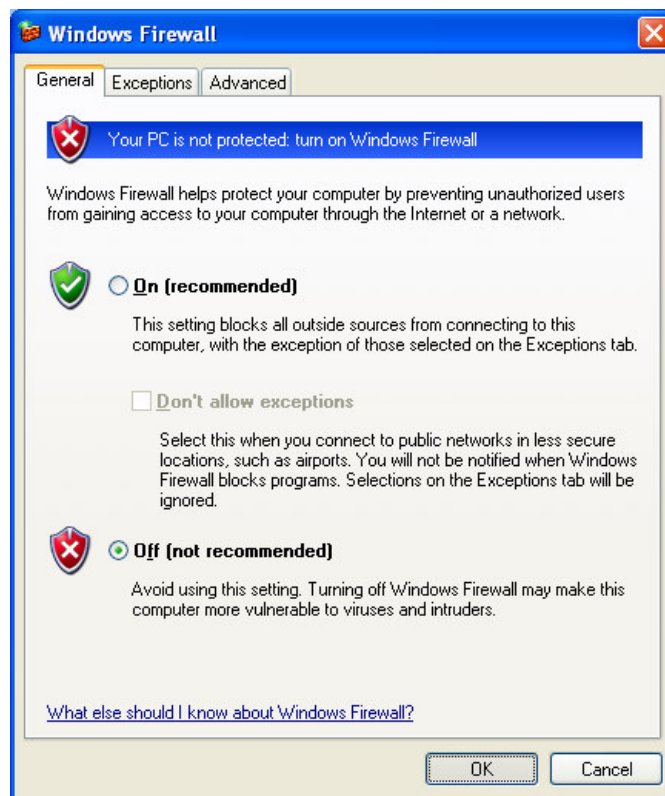
1. Go to ‘Start->Control Panel’ as shown:



2. Double click on the 'Windows Firewall' icon.



3. Set the Windows Firewall to 'Off' as shown, and click OK. The Firewall will no longer block OPC Communication.

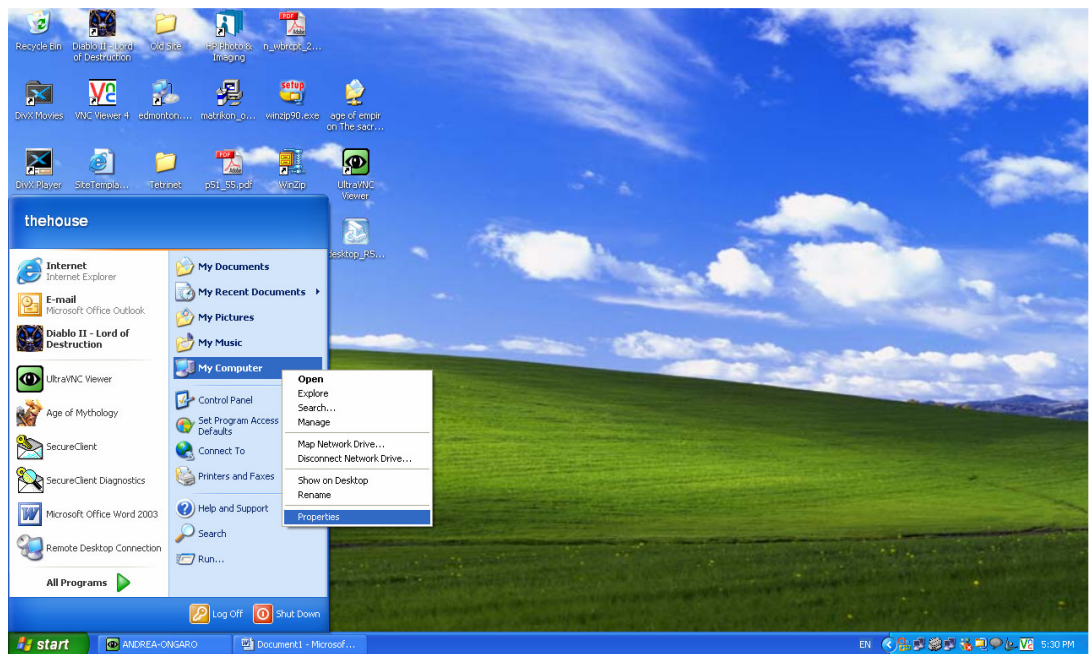


Data Execution Prevention

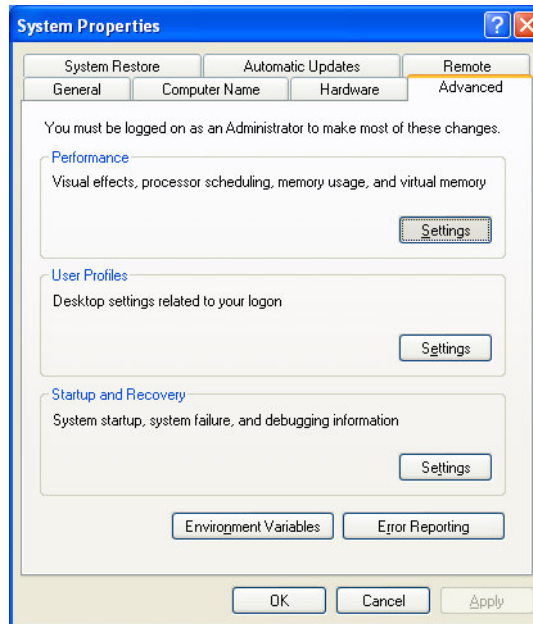
Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system. In Microsoft Windows XP Service Pack 2 (SP2) and Microsoft Windows XP Tablet PC Edition 2005, DEP is enforced by hardware and by software.

DEP will also prevent many installations from running, and has been known to cause other software issues. Please disable it as per the following steps:

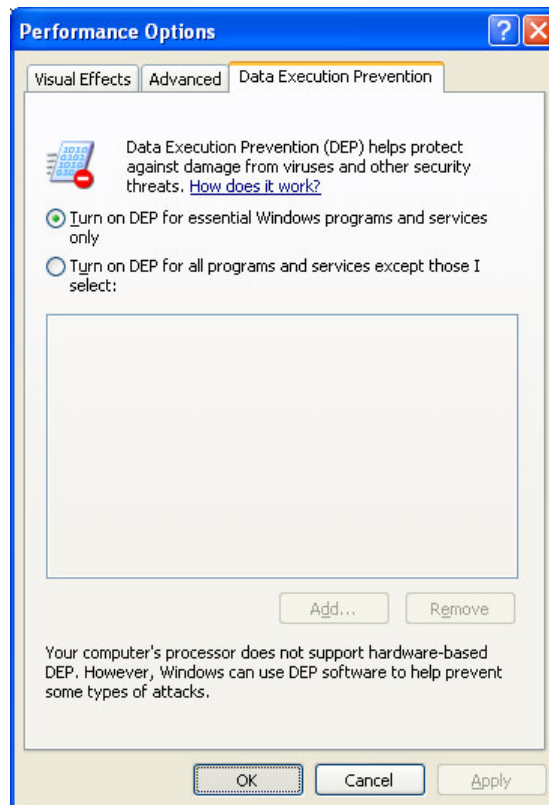
1. From your Start menu, right-click on 'My Computer' and select 'Properties'



2. Go to the 'Advanced' tab. Under 'Performance', hit the Settings button.



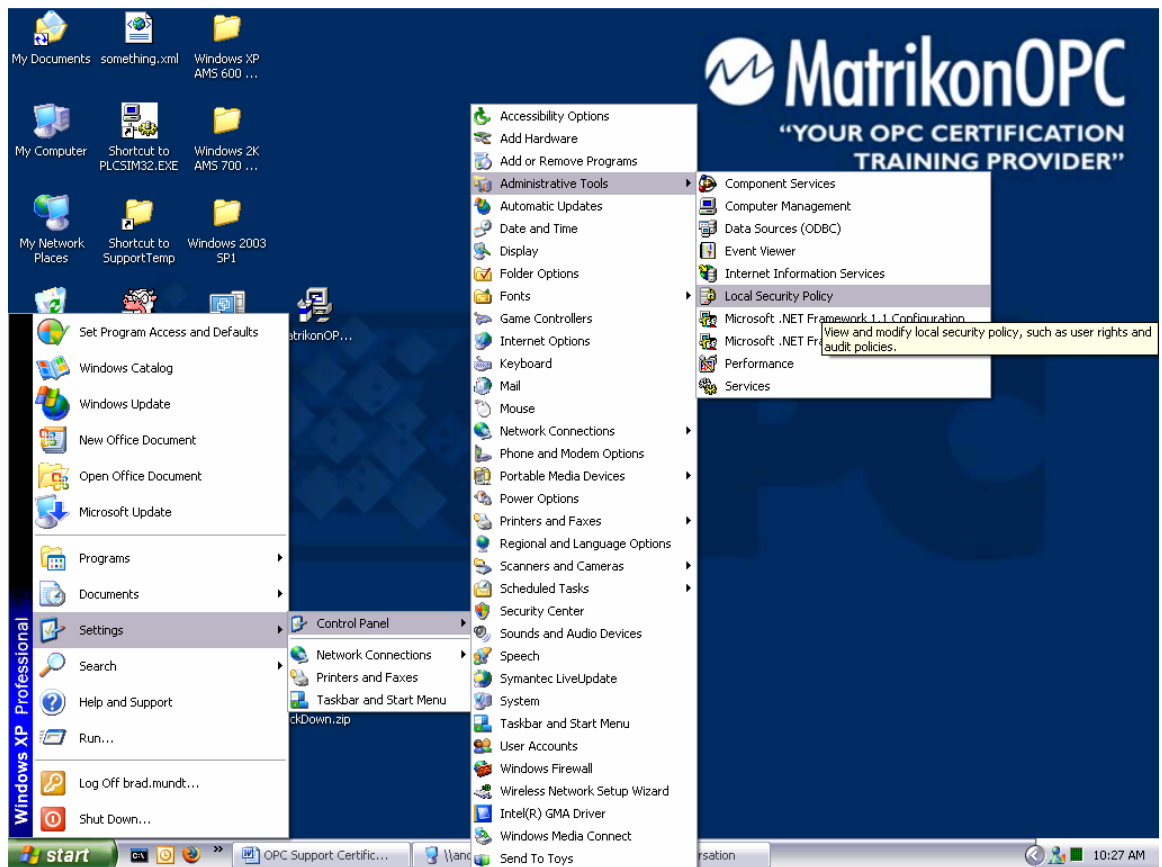
3. Select the 'Turn on DEP for essential...' button, as shown. Click OK. At this point it may be necessary to restart the machine.



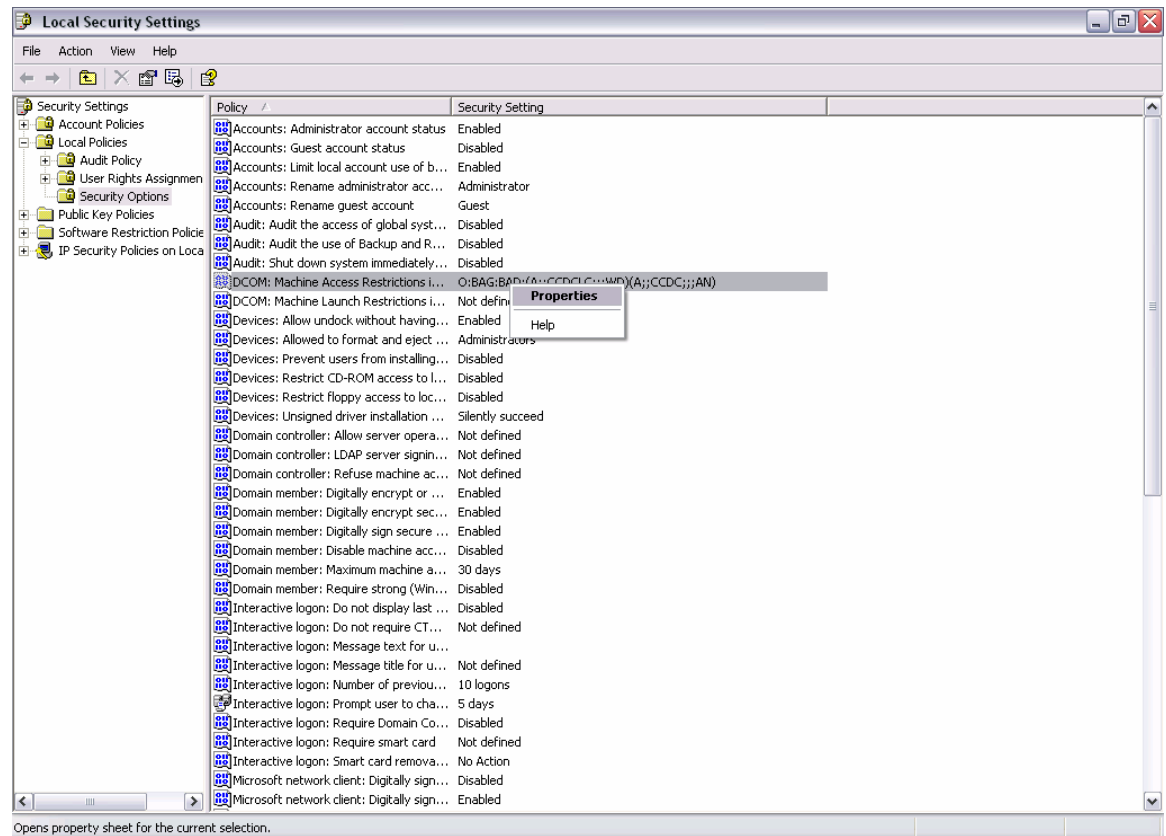
Local Security Policy

If you are using workgroups instead of domains the following steps may need to be taken in order to establish communication. Please note that these changes may compromise the security of your system – speak with your network administrator if you have any concerns.

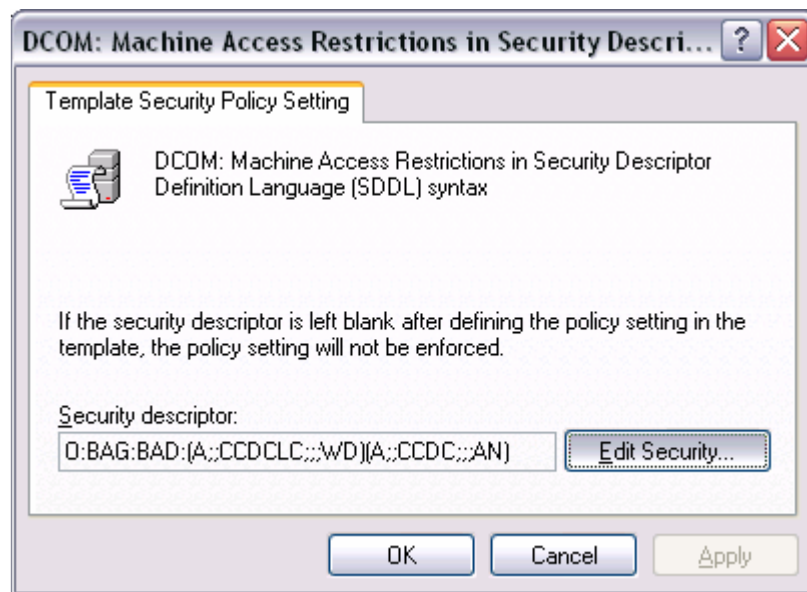
1. Go to ‘Start->Settings->Control Panel->Administrative Tools->Local Security Policy’.



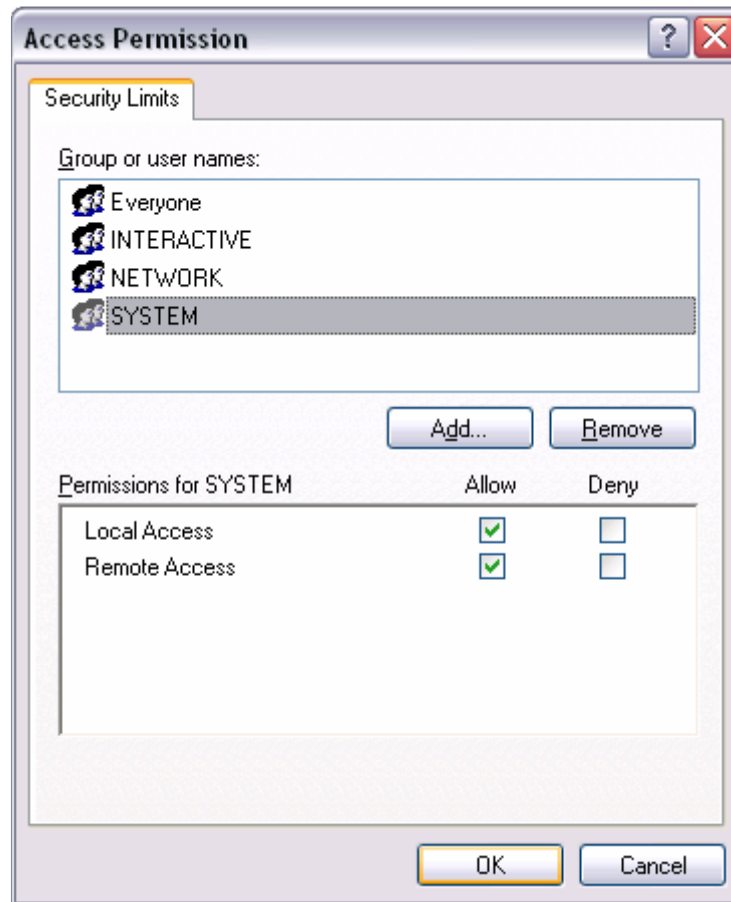
- Go to 'Security Settings->Local Policies->Security Options'.
- Right-click on 'DCOM: Machine Access Restrictions...' and select 'Properties'.



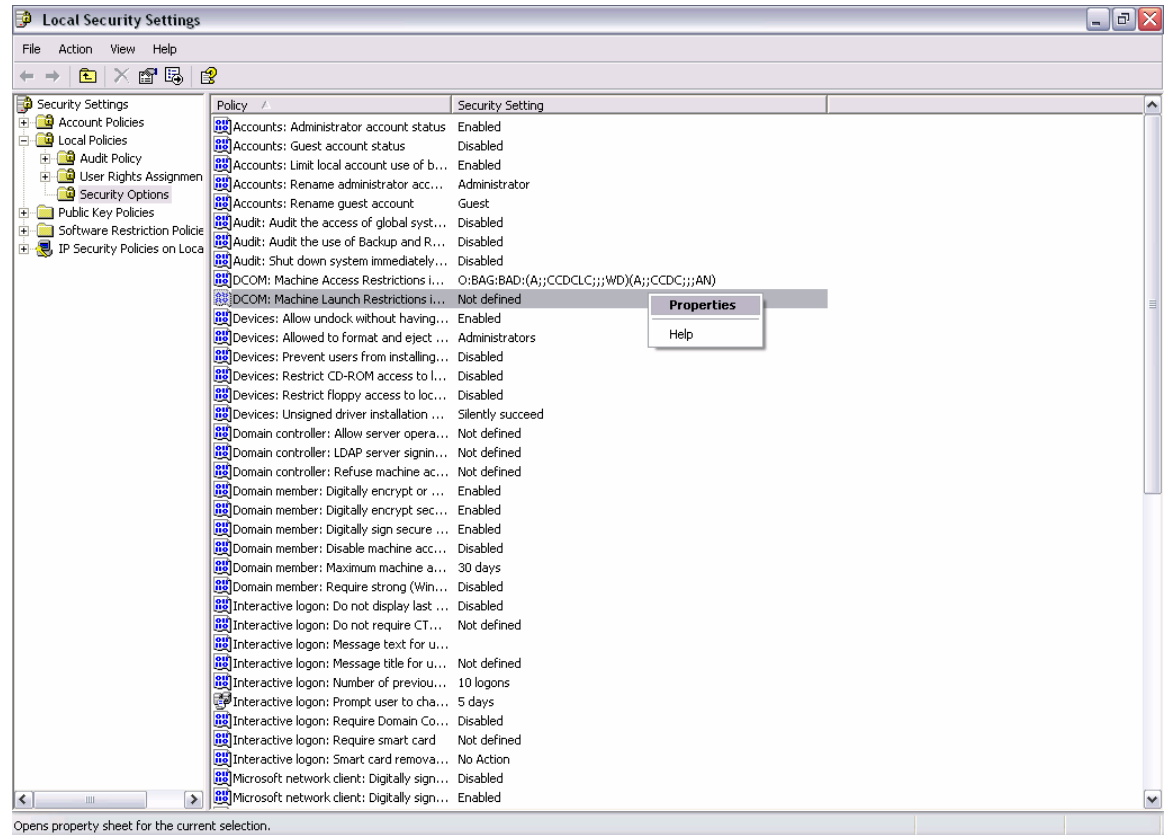
- Hit the 'Edit Security' button, as shown.



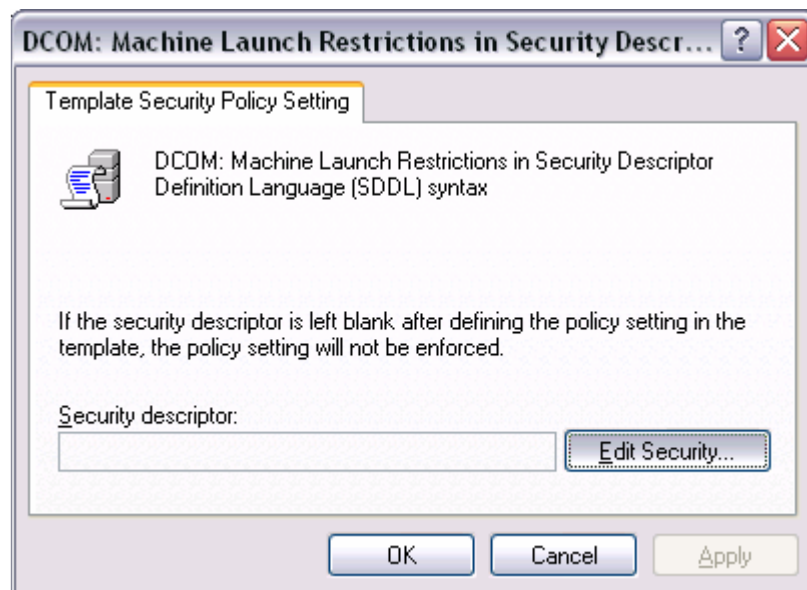
5. Ensure that 'Everyone', 'Interactive', 'Network', and 'System' are added into the allowed Group or User Names, as shown. Click OK to return to the main security policy window.



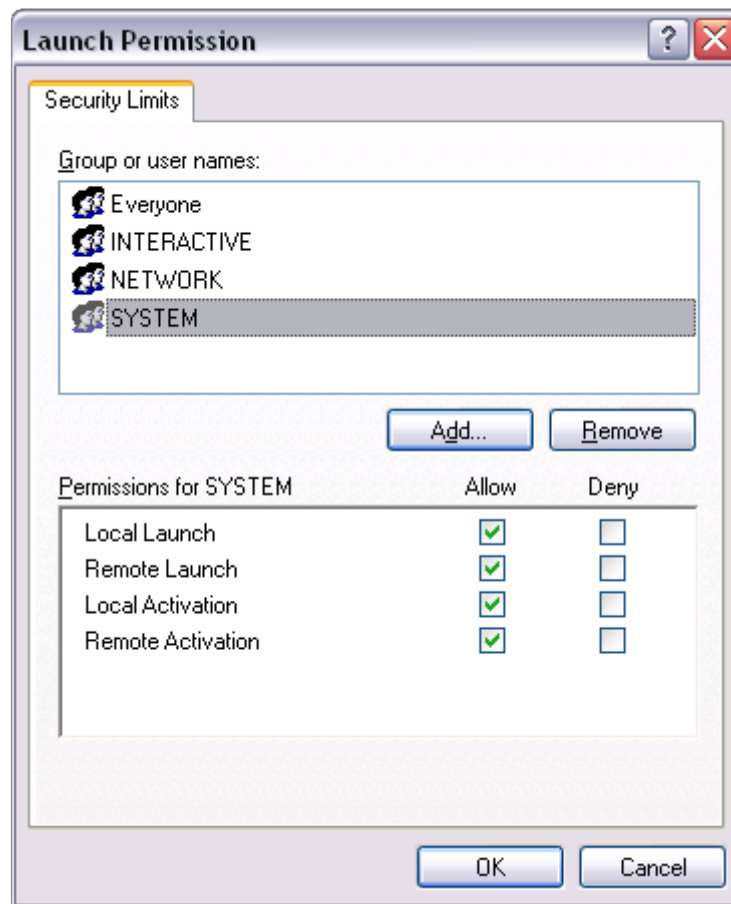
- Right-click on 'DCOM: Machine Launch Restrictions...' and select 'Properties'.



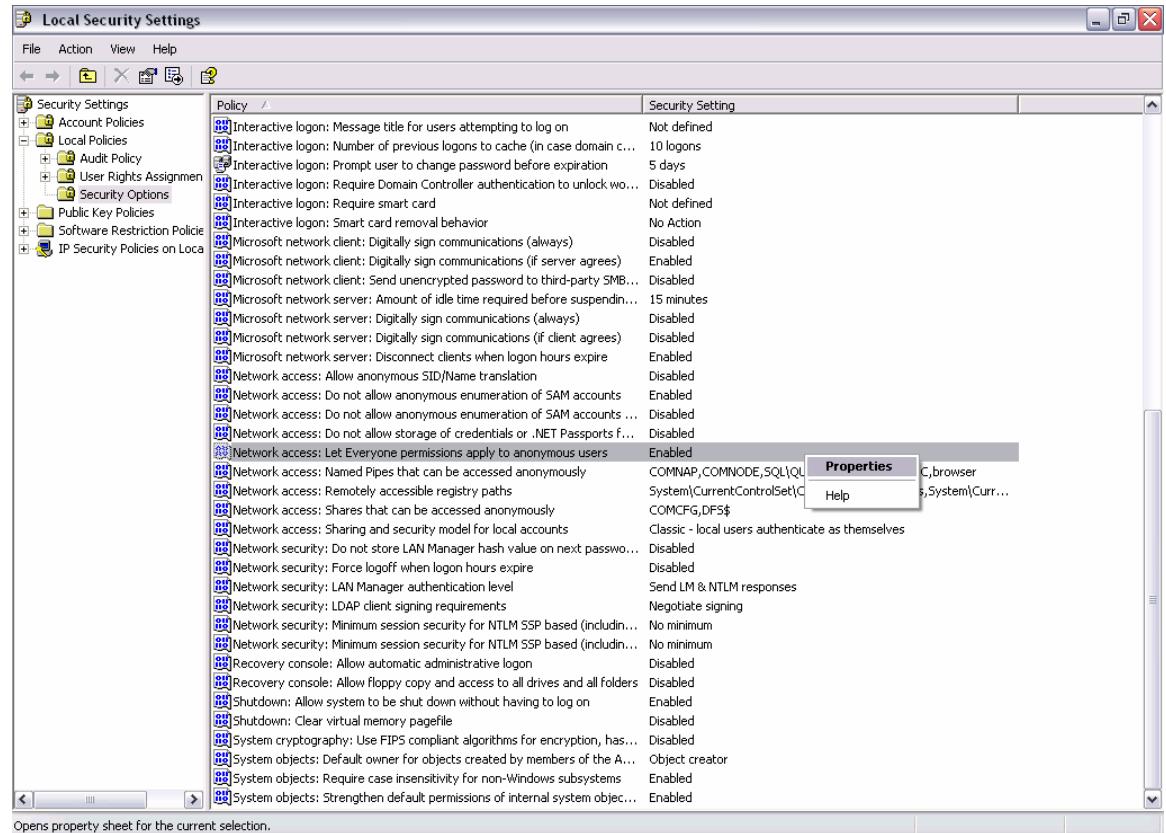
- Hit the 'Edit Security' button, as shown.



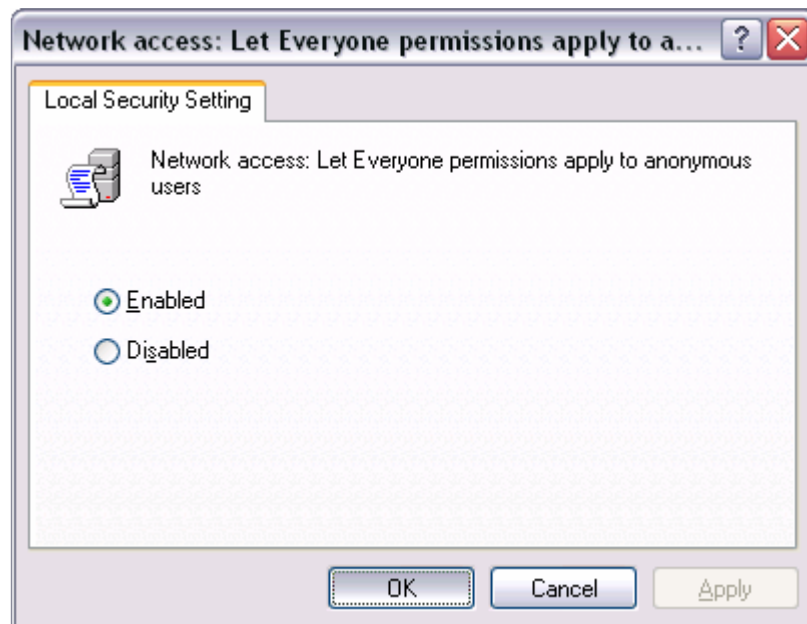
8. Ensure that 'Everyone', 'Interactive', 'Network', and 'System' are added into the allowed Group or User Names, as shown. Click OK to return to the main security policy window.



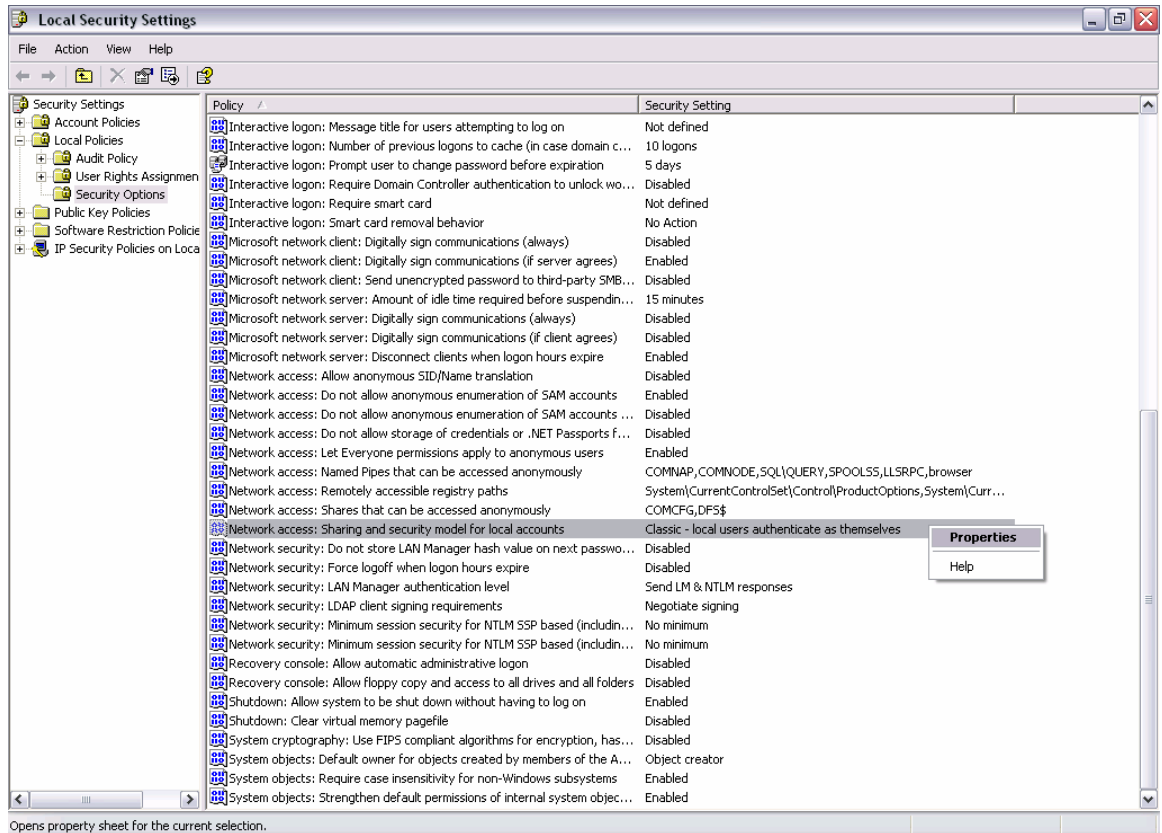
9. Browse to 'Network access: Let Everyone permissions apply to anonymous users'. Right click on it, and select 'Properties'.



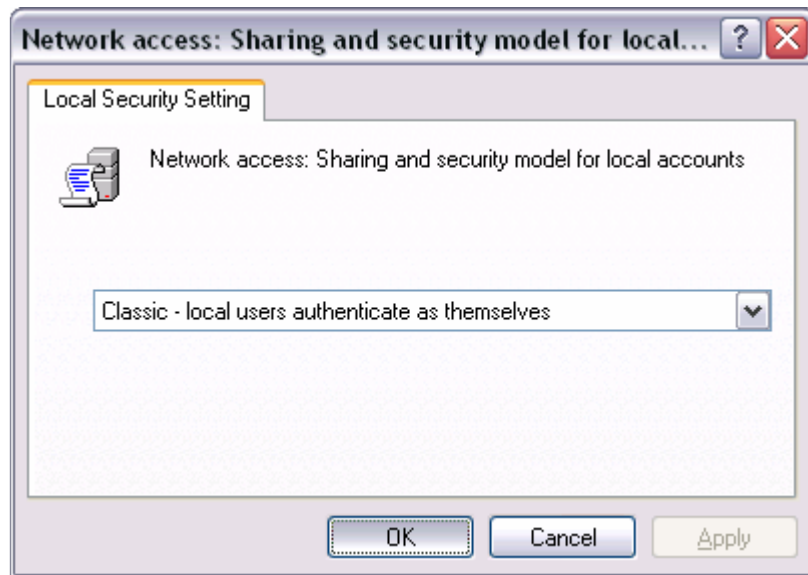
10. Select 'Enabled' and click 'OK'.



11. Browse to 'Network access: Sharing and security model for local accounts'. Right-click on it and select 'Properties'.



12. Select 'Classic – local users authenticate as themselves' and click OK.



Your **DCOM** is now setup to accept all incoming connections.

NOTE: DCOM has limitations for connectivity when operating on separate domains/workgroups. These steps may work but, depending on individual networks, additional settings and components may be required. Please contact OPC Support for additional information.

Phone: (91) 94444-43373

E-Mail: osn-in@flsaindia.co.in