Windows 7 Professional 64 bit Configuration for MassLynx Security

1. Purpose

This document outlines the procedure to configure Microsoft Windows 7 Professional 64 bit operating system in order for installations of MassLynx with Security to function correctly

2. Scope

It is assumed that the Engineer configuring the PC is familiar with Windows 7 Professional 64 bit operation and its general operational use. It is also assumed that Windows 7 Professional 64 bit for the IBM M5x PC has been configured correctly for Instrument Control.

Refer to Service Note "Configuring Windows 7 for Ethernet Instrument Communication with Empower or MassLynx" for details.

3. Hardware/Software Required

- Current or High Spec IBM M5x (Host) PC
- Windows 7 Professional 64 bit with valid license

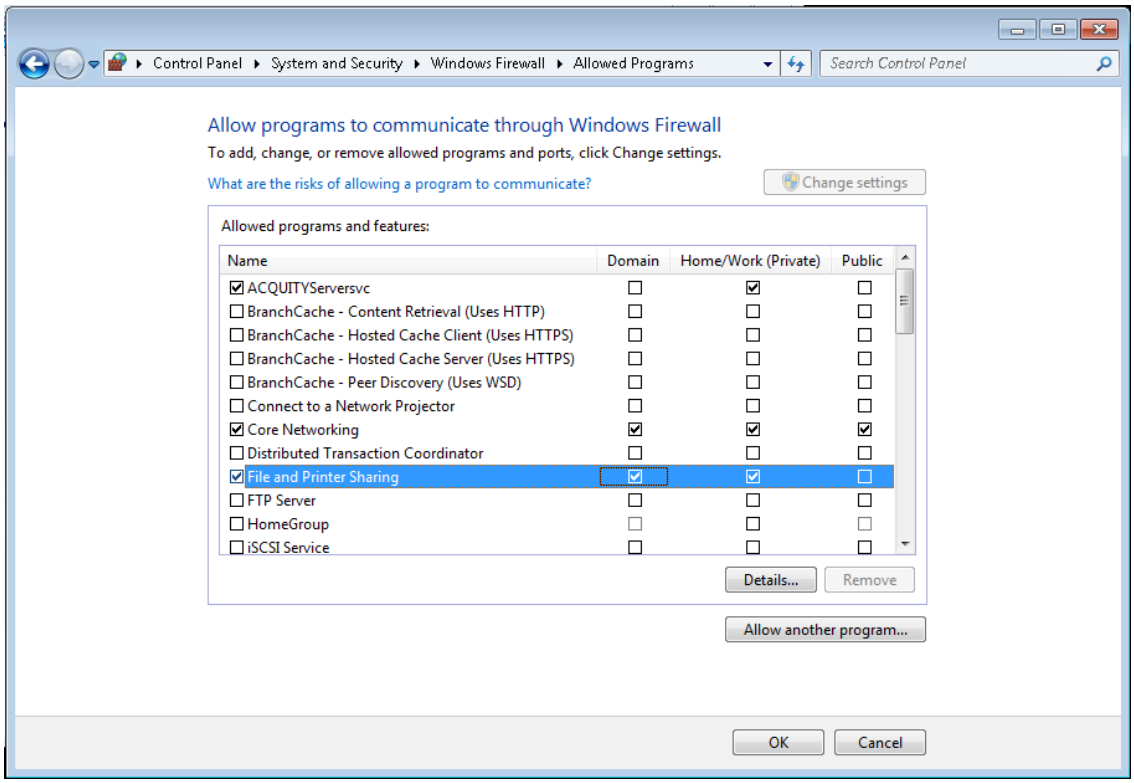
4. Document Index

5. Configuration of Windows 7 Professional 64 bit for Secure Installation of MassLynx

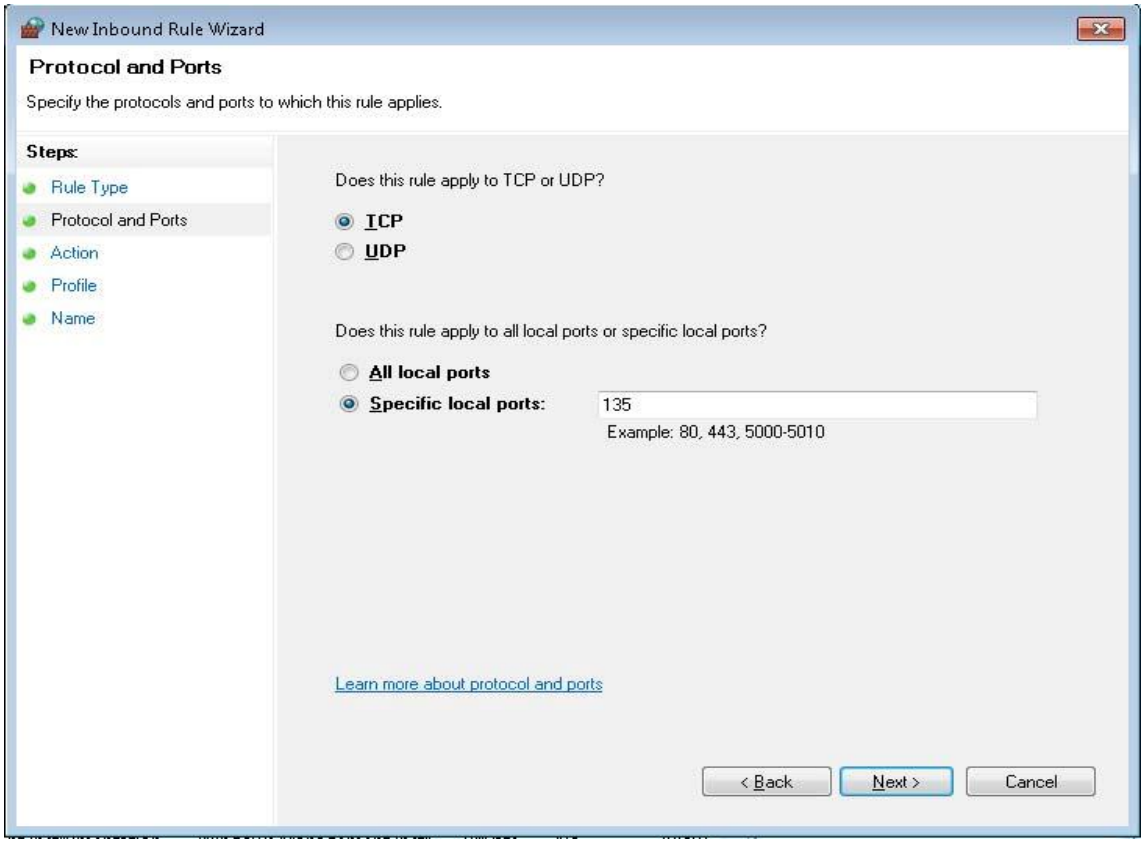
The changes detailed below are required to allow a secure installation of MassLynx to function correctly.

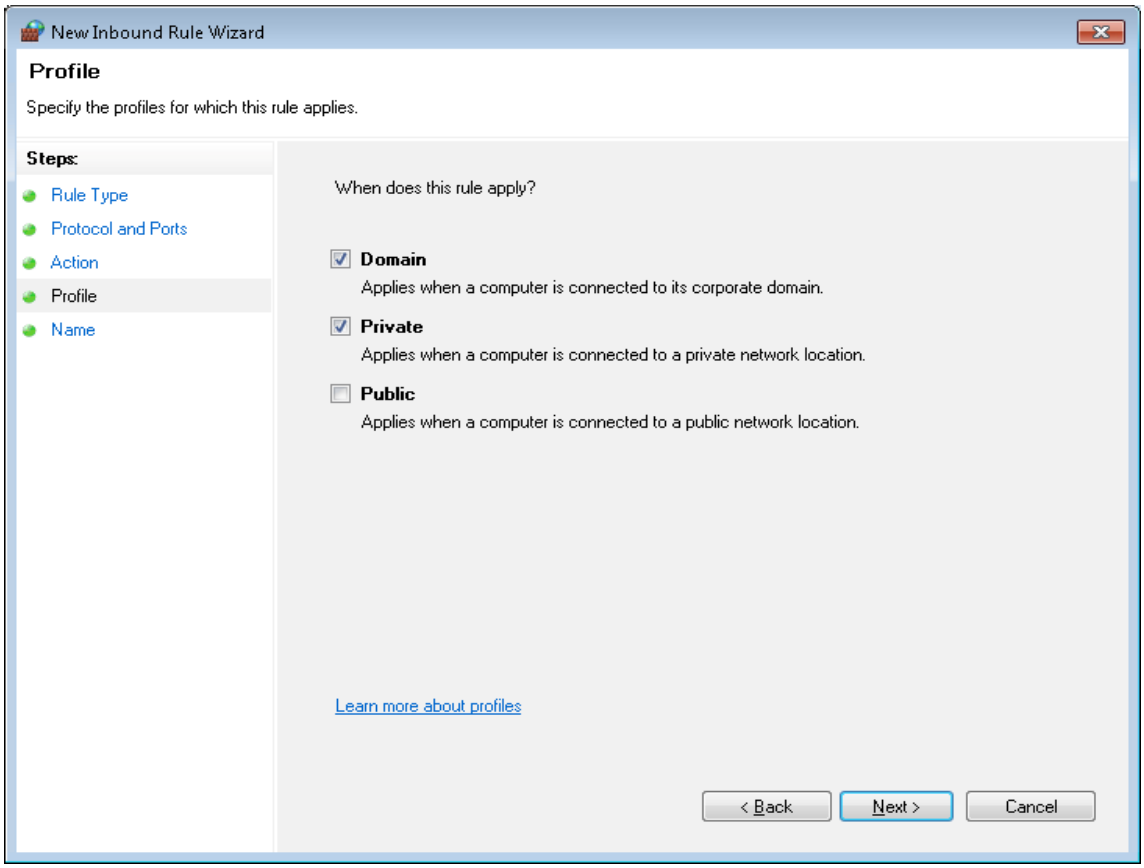
5.1 Enabling file and print sharing and allowing RPCs on port 135 through Firewall

Close down any currently open applications and go to **Control Panel -> System and Security -> Windows Firewall -> Allowed Programs**. Check the "File and Printer Sharing" option and Domain and Private network permissions as shown below and click **OK**



Now, go to **Control Panel -> System and Security -> Windows Firewall** and Advanced Settings. Create a new rule in Inbound Rules by clicking **Action -> New Rule** which opens New Inbound Rule Wizard. Select "**Port**" as Rule Type, select "**TCP**" and enter "**135**" to Specific local ports as Protocol and Ports, select "Allow the connection" as Action, check only "Domain" and "Private" in Profile section, enter "**RPC**" as Name and finally click **Finish** to create the new RPC Inbound rule

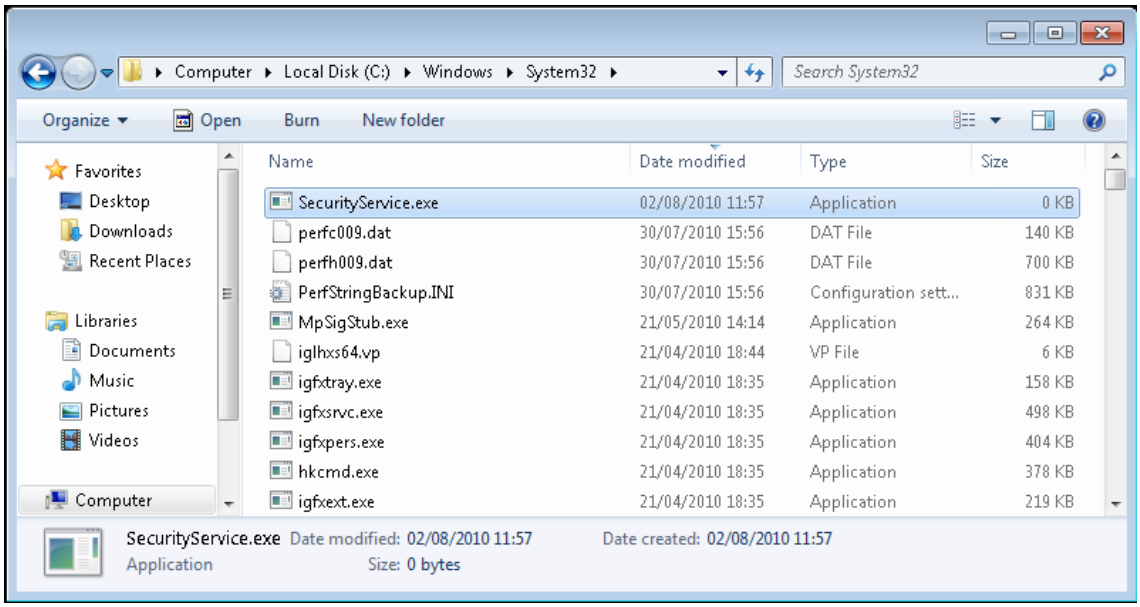

New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
135
Example: 80, 443, 5000-5010
Learn more about protocol and ports
< Back
Next >
Cancel


New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location.
Public
Applies when a computer is connected to a public network location.
Learn more about profiles
< Back
Next >
Cancel

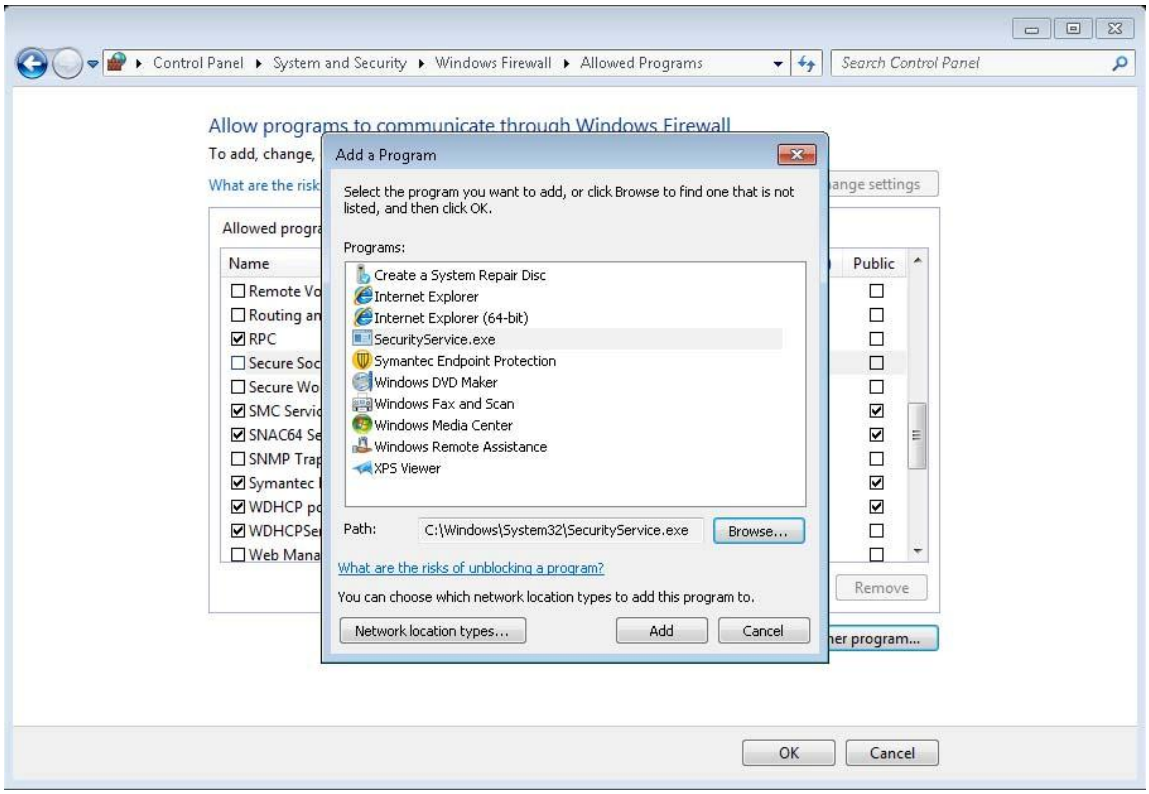
5.2 Allowing security services through the Firewall

Locate the folder "C:\Windows\System32". Create a new **Text Document** called "New Text Doument.txt". Now create a dummy executable for the security service by renaming the text file as "**SecurityService.exe**"

[Note: make sure that files are listed with extension, otherwise go to **Organize -> Folder** and search options. Click on **View** tab and uncheck "**Hide Extensions for known file types**" option and click **OK**]

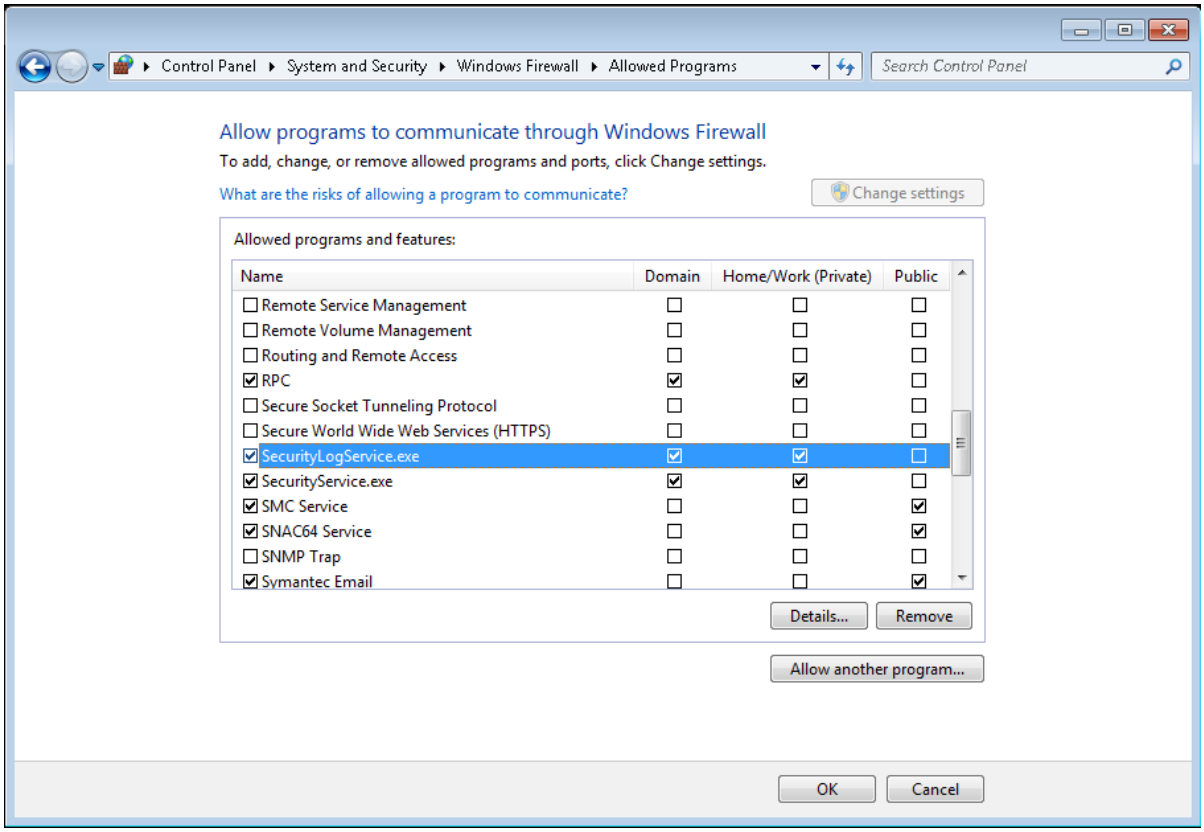


Now, go to **Control Panel -> System and Security -> Windows Firewall -> Allowed Programs** and click on Allow another program... which opens the Add a Program dialog. Here browse and select the executable "C:\Windows\System32\SecurityService.exe" and click **Add**



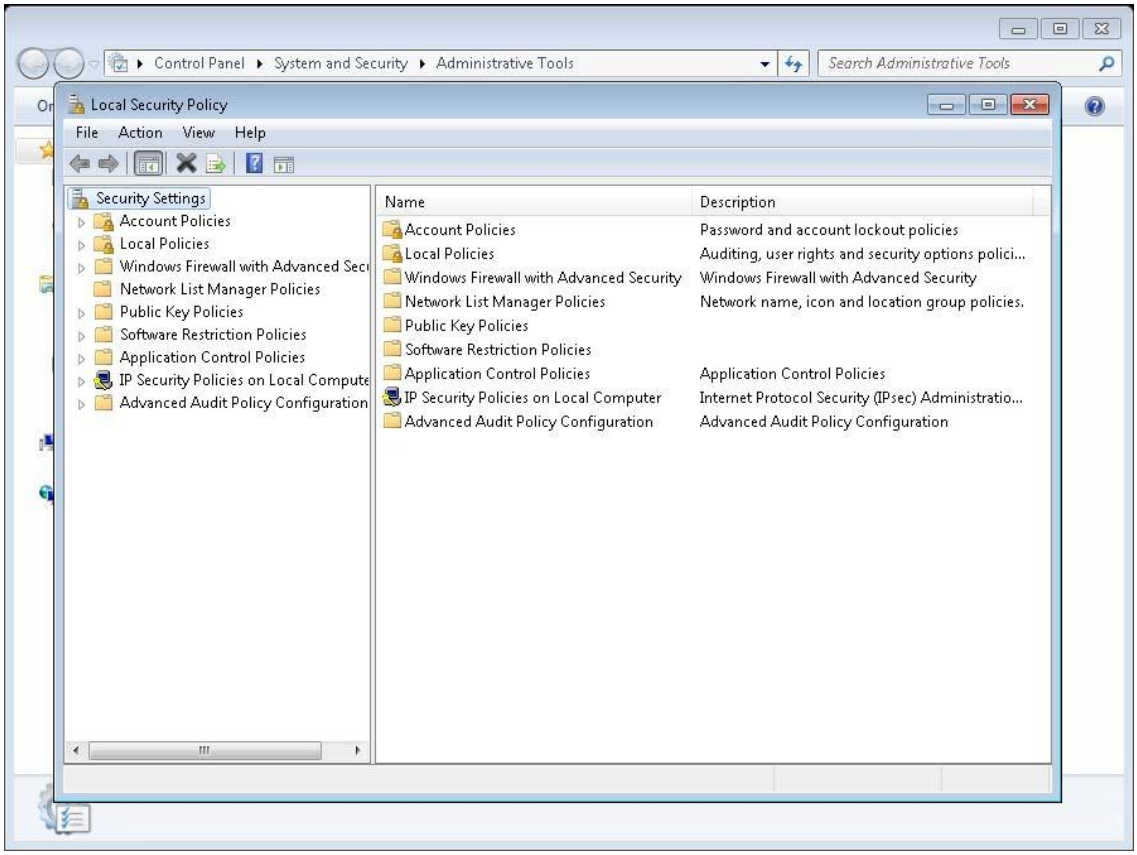
Check "Domain" and "Private" network permissions to SecurityService.exe and click **OK** to close the firewall. Once successfully added, delete SecurityService.exe file from "C:\Windows\System32" folder. [Note: **Failure to remove the dummy securityservice.exe file may prevent MassLynx from being installed correctly at a later stage**.]

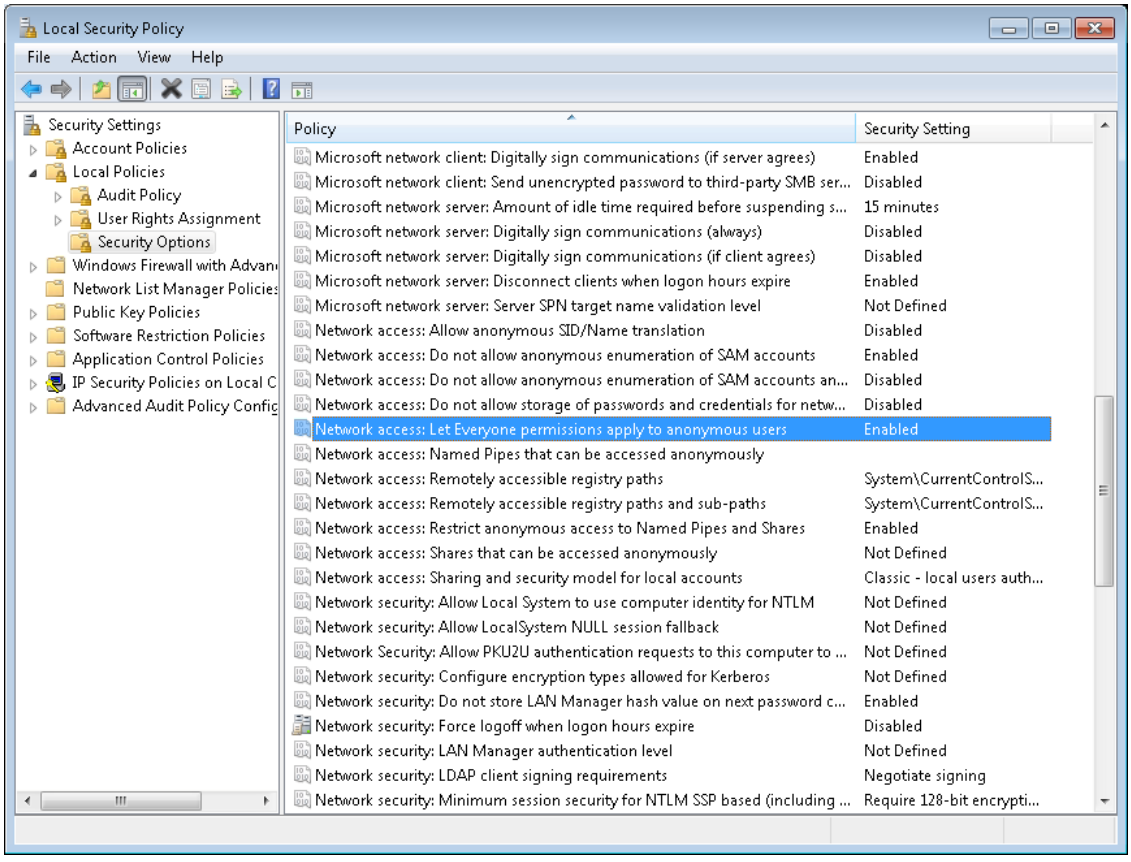
For a log server the executable "**C:\Windows\System32\SecurityLogService.exe**" must also be added to the Allowed Programs list. A dummy file should be created, added to the Allowed Programs list, then deleted in the same way as for the securityservice.exe



5.3 Configuring Local Policy

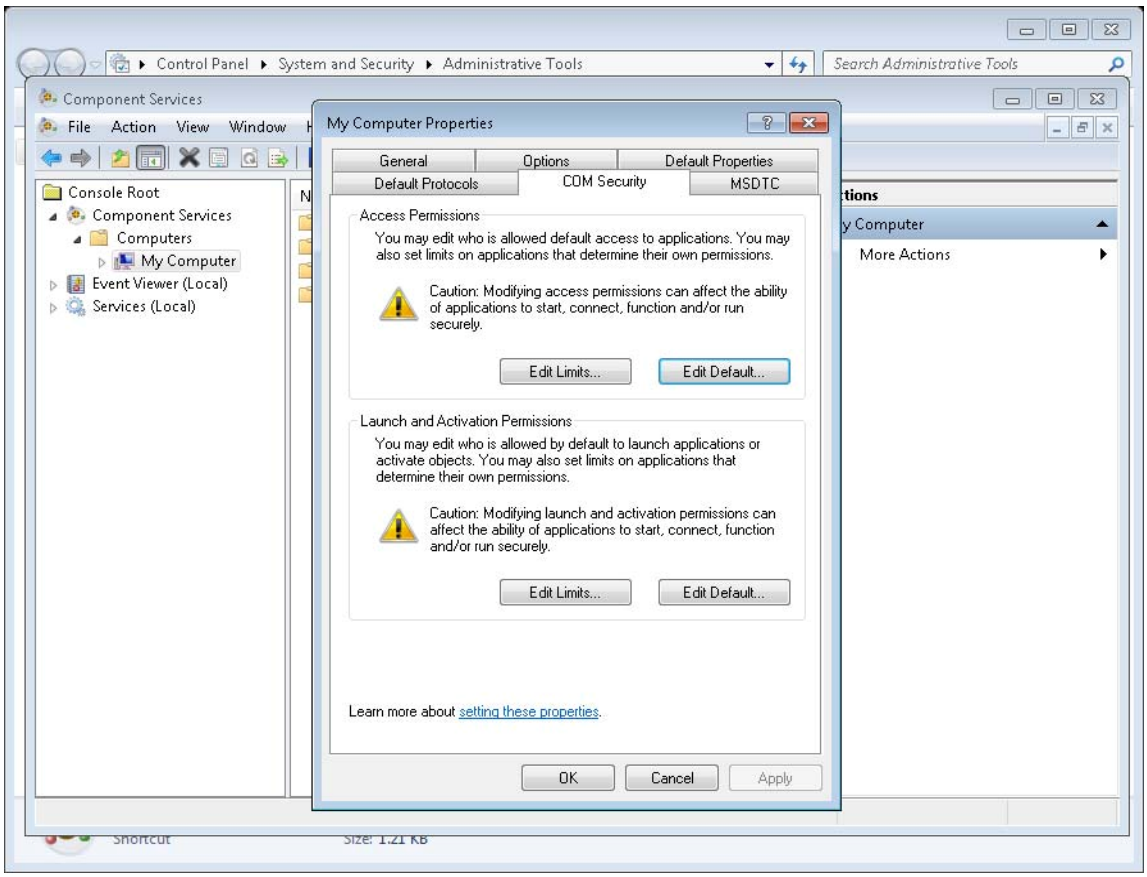
Go to **Control Panel -> System and Security -> Administrative Tools** and open "**Local Security Policy**". Expand **Local Policies -> Security Options** and select "**Network access: Let Everyone Permissions apply to anonymous users"** policy. From Action click Properties, select the "**Enabled**" option and then click **Ok**.


Control Panel ▸ System and Security ▸ Administrative Tools
Search Administrative Tools
Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Name
Description
Account Policies
Password and account lockout policies
Local Policies
Auditing, user rights and security options polici...
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security
Network List Manager Policies
Network name, icon and location group policies.
Public Key Policies
Software Restriction Policies
Application Control Policies
Application Control Policies
IP Security Policies on Local Computer
Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration
Advanced Audit Policy Configuration

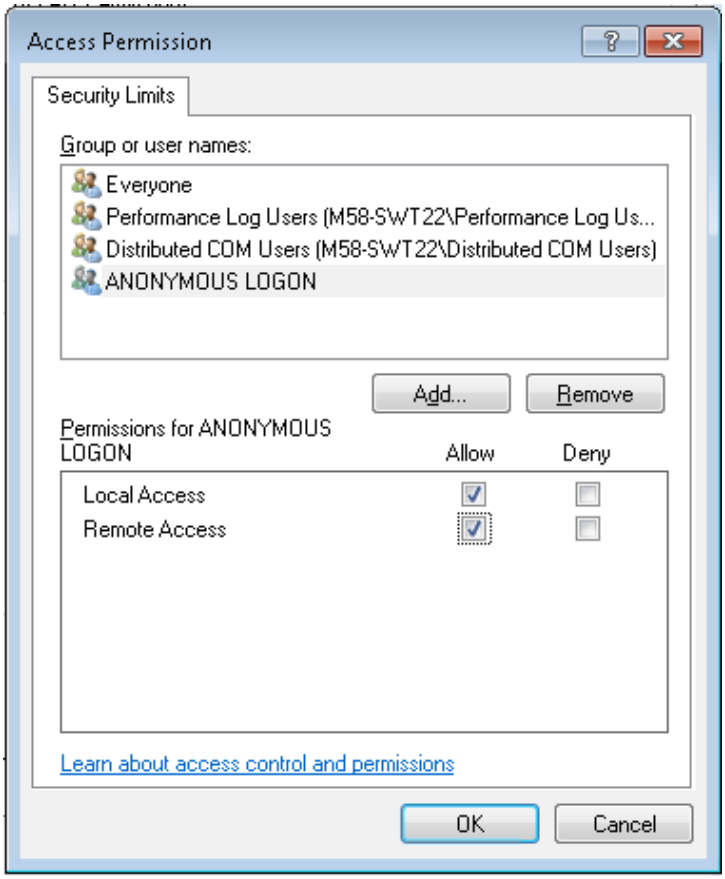

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advan
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local C
Advanced Audit Policy Config
Policy
Security Setting
Microsoft network client: Digitally sign communications (if server agrees)
Enabled
Microsoft network client: Send unencrypted password to third-party SMB ser...
Disabled
Microsoft network server: Amount of idle time required before suspending s...
15 minutes
Microsoft network server: Digitally sign communications (always)
Disabled
Microsoft network server: Digitally sign communications (if client agrees)
Disabled
Microsoft network server: Disconnect clients when logon hours expire
Enabled
Microsoft network server: Server SPN target name validation level
Not Defined
Network access: Allow anonymous SID/Name translation
Disabled
Network access: Do not allow anonymous enumeration of SAM accounts
Enabled
Network access: Do not allow anonymous enumeration of SAM accounts an...
Disabled
Network access: Do not allow storage of passwords and credentials for netw...
Disabled
Network access: Let Everyone permissions apply to anonymous users
Enabled
Network access: Named Pipes that can be accessed anonymously
Network access: Remotely accessible registry paths
System\CurrentControlS...
Network access: Remotely accessible registry paths and sub-paths
System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes and Shares
Enabled
Network access: Shares that can be accessed anonymously
Not Defined
Network access: Sharing and security model for local accounts
Classic - local users auth...
Network security: Allow Local System to use computer identity for NTLM
Not Defined
Network security: Allow LocalSystem NULL session fallback
Not Defined
Network Security: Allow PKU2U authentication requests to this computer to ...
Not Defined
Network security: Configure encryption types allowed for Kerberos
Not Defined
Network security: Do not store LAN Manager hash value on next password c...
Enabled
Network security: Force logoff when logon hours expire
Disabled
Network security: LAN Manager authentication level
Not Defined
Network security: LDAP client signing requirements
Negotiate signing
Network security: Minimum session security for NTLM SSP based (including ...
Require 128-bit encrypti...

5.4 Configuring remote DCOM

Go to **Control Panel -> System and Security -> Administrative Tools** and open "**Component Services".** Expand to My Computer and go to Properties from Action menu. Select **COM Security** Tab



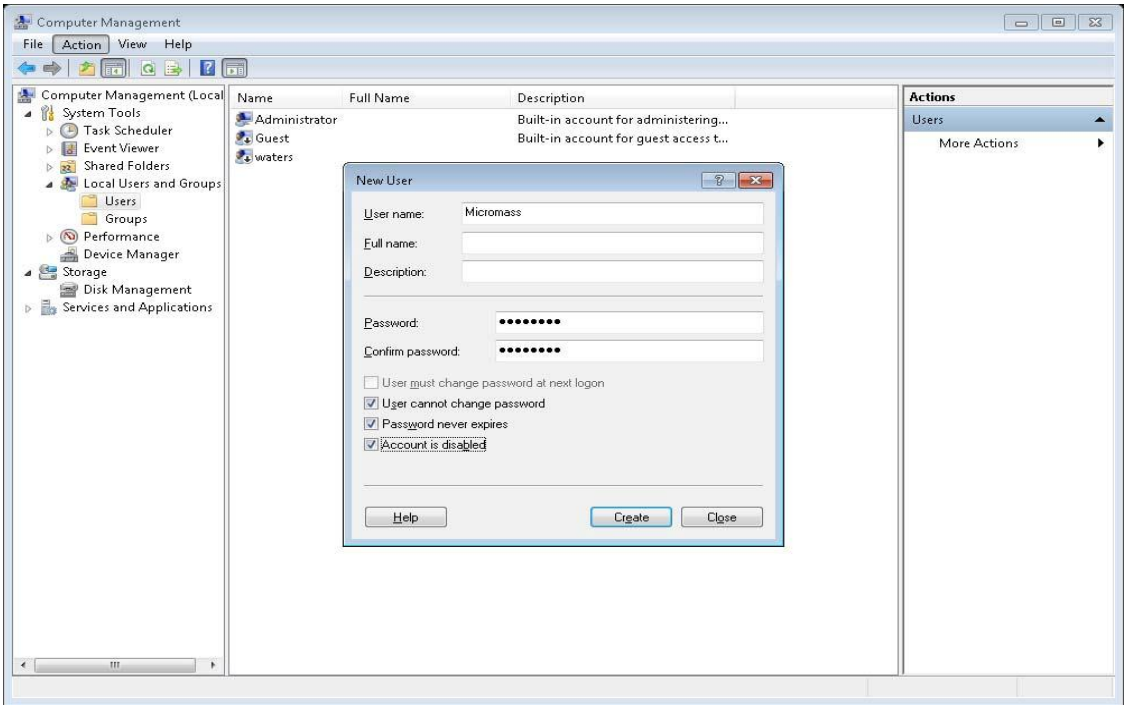
Click on "**Edit Limits**" of Access Permissions section and allow "**Remote Access**" to Anonymous Logon and Click **OK**. Click on "**Edit Limits**" of Launch and Activation Permissions and allow "**Remote Launch**" and "**Remote Activation**" for "Everyone" group and click **Ok**. Finally, click **Apply** and **Ok** button


Access Permission
Security Limits
Group or user names:
Everyone
Performance Log Users (M58-SWT22\Performance Log Us...
Distributed COM Users (M58-SWT22\Distributed COM Users)
ANONYMOUS LOGON
Add...
Remove
Permissions for ANONYMOUS LOGON
Allow
Deny
Local Access
Remote Access
Learn about access control and permissions
OK
Cancel


Launch and Activation Permission
Security Limits
Group or user names:
Everyone
Administrators (M58-SWT22\Administrators)
Performance Log Users (M58-SWT22\Performance Log Us...
Distributed COM Users (M58-SWT22\Distributed COM Users)
Add...
Remove
Permissions for Everyone
Allow
Deny
Local Launch
Remote Launch
Local Activation
Remote Activation
Learn about access control and permissions
OK
Cancel

5.5. Adding User Account

Go to **Control Panel -> System and Security -> Administrative Tools** and Open the **Computer Management**. In the Computer Management window, expand to Users. Click **Action -> New User** which opens the New User dialog. Enter the details User name as "**Micromass**", Password as "analysis", Deselect the "**User must change password at next logon**", select the "**User cannot change password**" and select the "**Password never expires**" options. Then click **Create** button to create the ***Micromass*** user account



Double click on the newly created ***Micromass*** account. Click on the **Member Of** tab. Verify that the Micromass user is a member of the **Users** group click **OK** to close down the Properties box

Note:

The local '**Micromass**' account is only required to complete the initial installation of MassLynx with security (used to apply the checksums). Once a successful installation has been completed the local '**Micromass**' account can be deleted.