Configuring Windows 10 for MassLynx Security

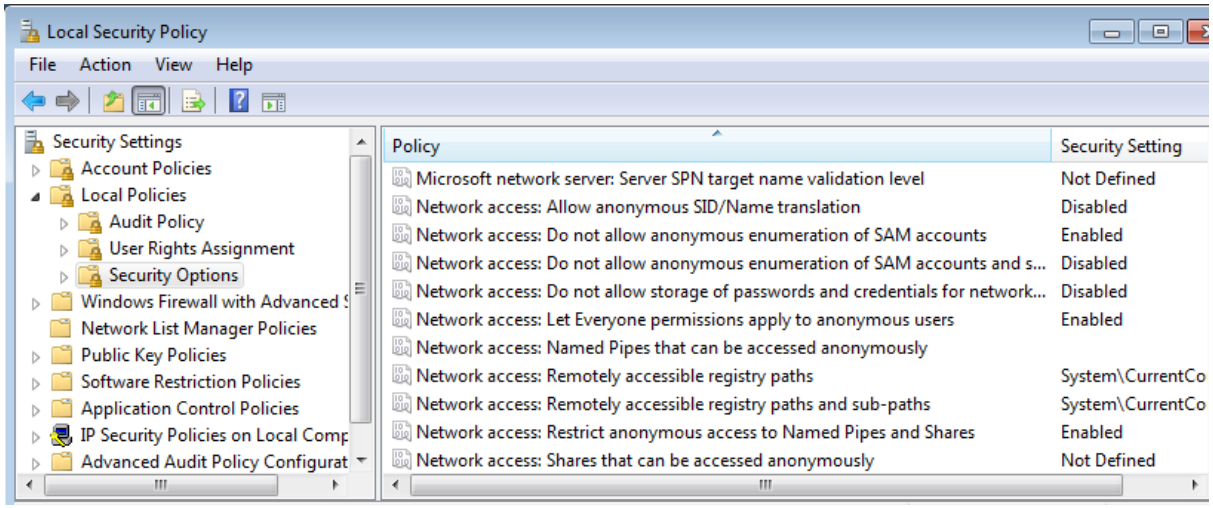
A. Configuring Local Policy

1. In the Search window, enter '**secpol**'.

Alternatively, in the Search window, enter '**Control**', choose **Control Panel -> System and Security -> Administrative Tools** and then open '**Local Security Policy**'.

3. Expand **Local Policies -> Security Options** and select '**Network access: Let Everyone Permissions apply to anonymous users'** policy.

4. Select the '**Action'** menu, click '**Properties'**, select the '**Enabled**' option and then click '**Ok'**.



B. Configuring remote DCOM

1. In the Search window, enter '**dcomcnfg**'.

Alternatively, in the Search window, enter '**Control**', choose **Control Panel -> System and Security -> Administrative Tools** and then open "**Component Services".**

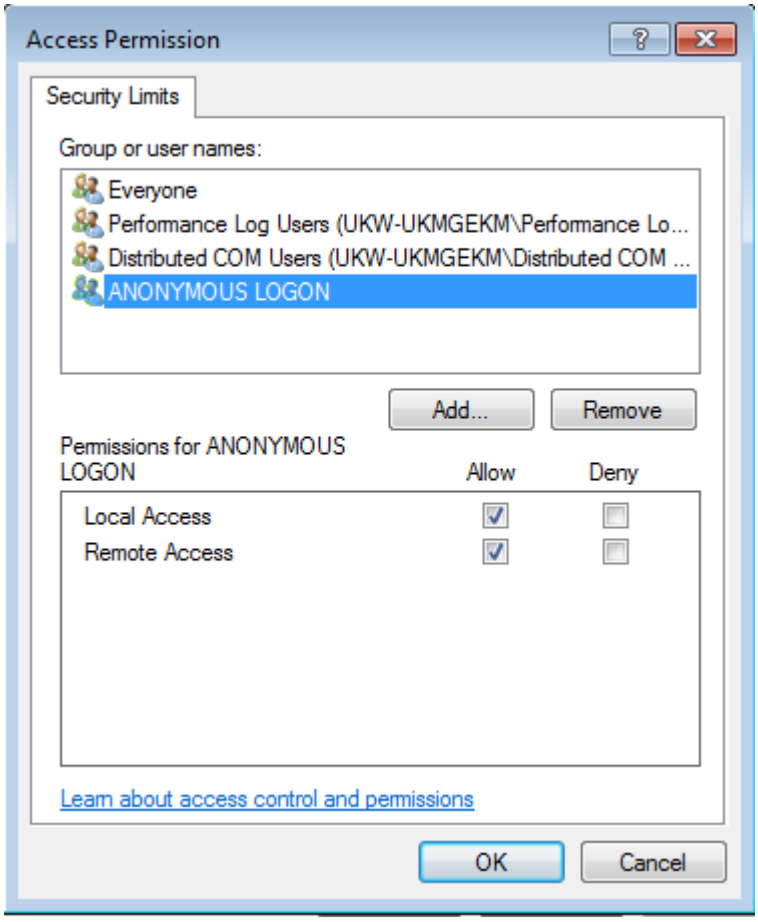
2. In the middle panel, double-click '**Computers**', then right-click on '**My Computer**' and choose '**Properties**' from the dropdown.

Alternatively, in the Console Root, expand **'Component Services'**, expand '**Computers**', highlight '**My Computer'**, select the '**Action'** menu and then choose '**Properties**'.

3. Select the '**COM Security'** tab.

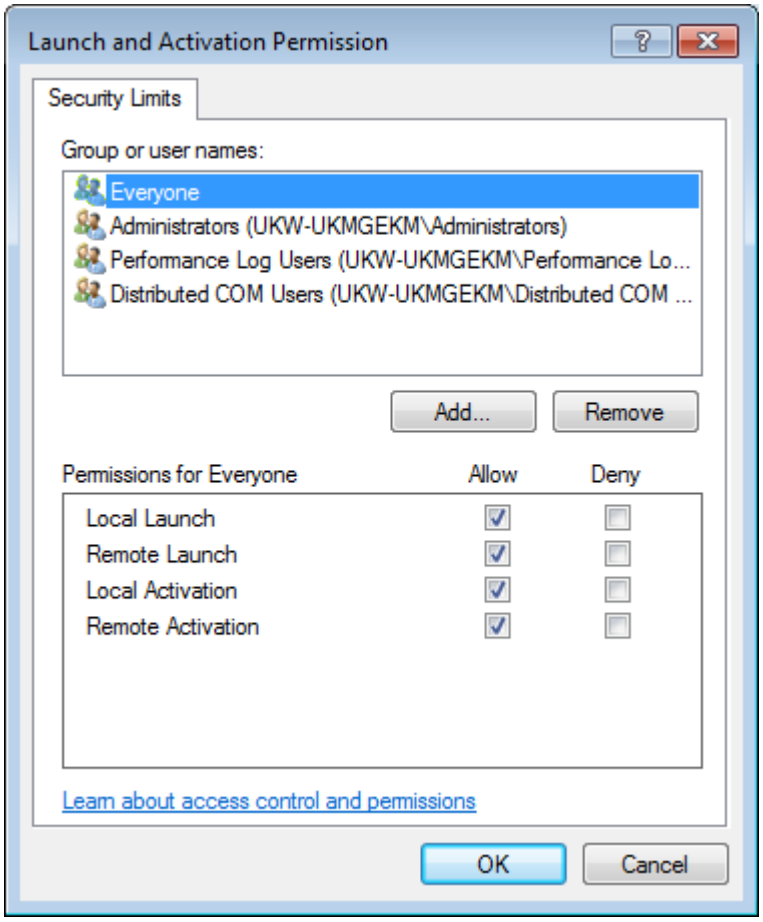
4. In the '**Access Permissions'** area, click '**Edit Limits**'.

5. Under '**Group or user names'**, highlight '**Anonymous Logon**' and ensure that '**Allow**' is selected for the '**Remote Access**' permission, and then Click **OK**.



6. In the '**Launch and Activation Permissions**' area, click '**Edit Limits**'.

7. Under '**Group or user names'**, highlight '**Everyone**' and ensure that the '**Remote Launch**' and '**Remote Activation** permissions are both selected, and then click **Ok**.



C. Adding the Security Services as Exceptions to the Firewall

If the Windows 10 Firewall is enabled on a MassLynx security PC, and if remote logging is being used, configure the Firewall as described below, after installing MassLynx security. This will allow MassLynx to log events to the remote audit log file (.mlevt) on the MassLynx logserver.

1. In the Search window, enter '**Control**', choose **Control Panel -> System and Security -> Windows Firewall -> Allow a Program through Windows Firewall.**

2. Click on '**Allow another program...**' which opens the '**Add a Program'** dialog. Browse and select the following executable:

'C:\Windows\SysWOW64\SecurityService.exe'

The service will be displayed in the list of exceptions as '**SecurityService Module**'.

3. Check '**Domain**' and '**Private**' network permissions to SecurityService.exe and click **OK** to close the firewall.

4. On the logserver, repeat steps 1-3, adding the following executable to the Firewall:

'C:\Windows\ SysWOW64\SecurityLogService.exe'

The service will be displayed in the list of exceptions as '**NT service for event database.exe**'.