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'.

| 🛓 Local Security Policy | | |
|------------------------------------|---|------------------|
| File Action View Help | | |
| 🗢 🧼 🙎 📰 🗟 🛛 🖬 | | |
| Security Settings | Policy | Security Setting |
| Account Policies | B Microsoft network server: Server SPN target name validation level | Not Defined |
| Local Policies | B Network access: Allow anonymous SID/Name translation | Disabled |
| Audit Policy | B Network access: Do not allow anonymous enumeration of SAM accounts | Enabled |
| Security Ontions | B Network access: Do not allow anonymous enumeration of SAM accounts and s | Disabled |
| Windows Eirewall with Advanced | 📓 Network access: Do not allow storage of passwords and credentials for network | Disabled |
| Network List Manager Policies | 🛞 Network access: Let Everyone permissions apply to anonymous users | Enabled |
| Public Key Policies | 🔯 Network access: Named Pipes that can be accessed anonymously | |
| Software Restriction Policies | 📖 Network access: Remotely accessible registry paths | System\CurrentCo |
| Application Control Policies | 🖾 Network access: Remotely accessible registry paths and sub-paths | System\CurrentCo |
| IP Security Policies on Local Comp | 📖 Network access: Restrict anonymous access to Named Pipes and Shares | Enabled |
| Advanced Audit Policy Configurat | 圆 Network access: Shares that can be accessed anonymously | Not Defined |
| ۰ III • • • | ٠ (III | • |

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.

| Access Permission | | ? × | | |
|---|-------|------------|--|--|
| Security Limits | | | | |
| Group or user names: | | | | |
| Everyone Performance Log Users (UKW-UKMGEKM\Performance Lo Distributed COM Users (UKW-UKMGEKM\Distributed COM | | | | |
| and ANON TMOUS LOGON | | | | |
| | Add | Remove | | |
| Permissions for ANONYMOUS | Allow | Deny | | |
| Local Access Remote Access | | | | |
| | | | | |

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.

| Launch and Activation Permission | | | | | |
|---|---|--------|--|--|--|
| Security Limits | | | | | |
| Group or user names: | | | | | |
| See Everyone | | | | | |
| Administrators (UKW-UKMGE | & Administrators (UKW-UKMGEKM\Administrators) | | | | |
| Performance Log Users (UKW-UKMGEKM\Performance Lo Distributed COM Users (UKW, UKMGEKM) Distributed COM | | | | | |
| Bisinduled COM Users (DRW-DRINGERM Distributed COM | | | | | |
| | | | | | |
| | Add | Remove | | | |
| Permissions for Everyone | Allow | Deny | | | |
| Local Launch | V | | | | |
| Remote Launch | V | | | | |
| Local Activation | v | | | | |
| Remote Activation | \checkmark | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Learn about access control and permissions | | | | | |
| | ОК | Cancel | | | |

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'.