Product	Version	Theme	Environment	Date	Department	Person	Language
SPM_PLM	Vx.x	Firewall ports	Windows		After Sales	Technical Support	EN

Subject:

Firewall configuration tips

Description:

This document describes the Windows security settings to check in order to have SEE Electrical PLM Applications working with a 3 tiers installation when a firewall is activated.

Our proposed solution:

You need to have Windows administrative rights to modify the firewall properties on all the computers used by SEE Electrical PLM
Check also if some firewall rules apply above the ones you are working on (domain administration).

Important : the COM+ service representing the SEE Electrical PLM application server should not be running

Generally, you need to check the communication settings:

1) On the computer where your SQL server is installed:
   - the ports are used by SQL server. See the details in the "How to set SQL Server Ports" document
2) On the computer where your Application server is installed:
   - the ports used for the COM+ communication. See the details in the "How to set COM+ ports" document
   - the firewall configuration
3) On the client computers where SEE Electrical PLM – Hub clients are installed:
   - the COM+ communication settings
   - the firewall settings
4) On the computer where the Flex LM server is installed
   - the firewall settings for FlexLM

1 - Configuring the computer where the SQL server is installed

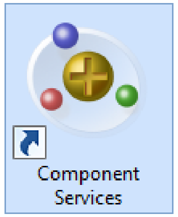
Add a rule into the firewall interactively
or by batch commands:

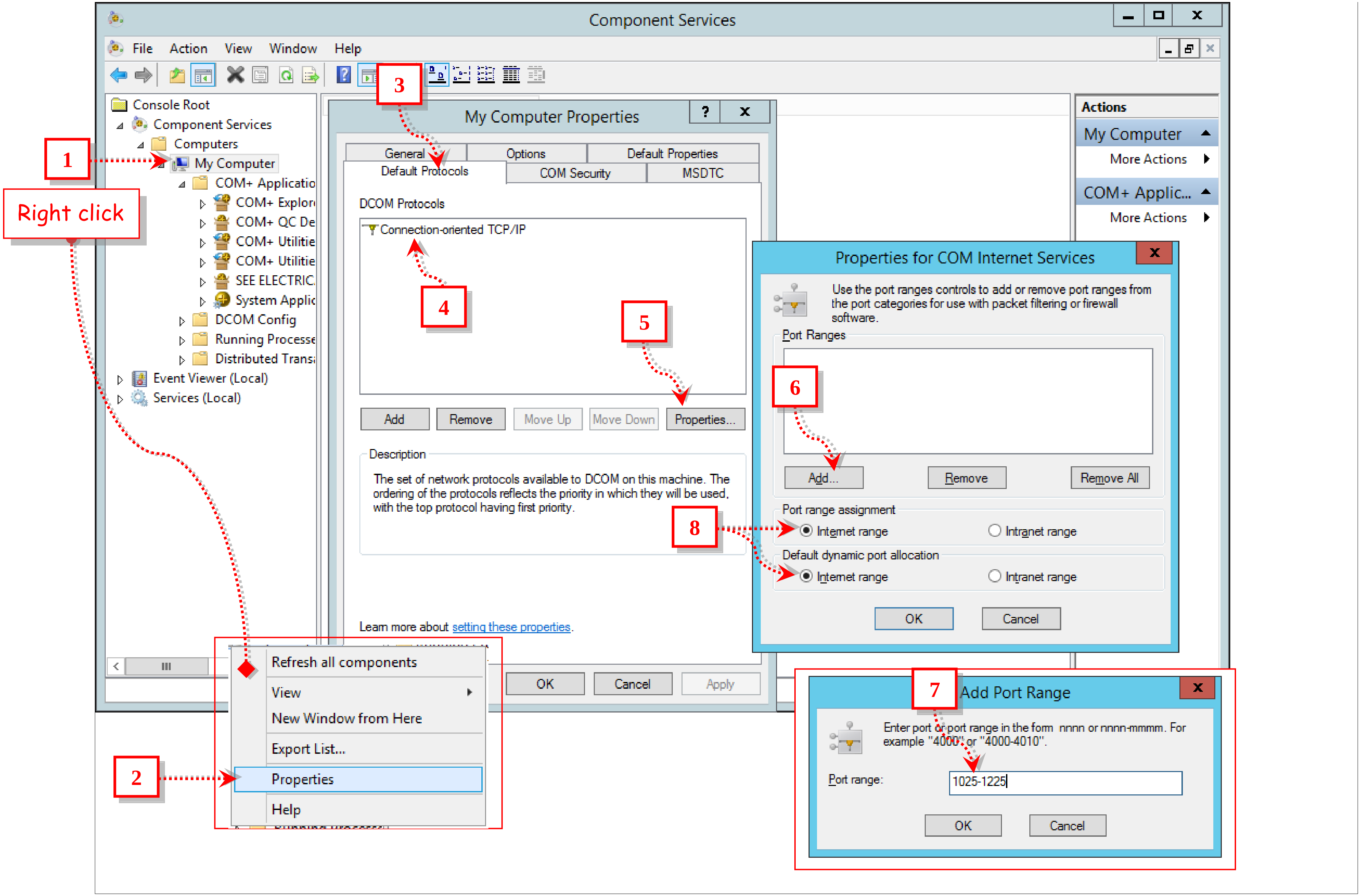
```
@echo ========= SQL Server Ports ===================
@echo Enabling SQLServer default instance port 1433
netsh advfirewall firewall add rule name="SQLServer communication" dir=in action=allow protocol=TCP localport=1433
```

2 - Configuring the computer where the Application server is installed

Define the Com+ port ranges (here we choose ports 1025 to 1225)
Open windows Component Services :

Control Panel\All Control Panel Items\Administrative Tools





The set of network protocols available to DCOM on this machine. The ordering of the protocols reflects the priority in which they will be used, with the top protocol having first priority.

Learn more about setting these properties.

Use the port ranges controls to add or remove port ranges from the port categories for use with packet filtering or firewall software.

Port range assignment

● Internet range ○ Intranet range

Default dynamic port allocation

● Internet range ○ Intranet range

Enter port or port range in the form nnnn or nnnn-mmmm. For example "4000" or "4000-4010".

Port range: 1025-1225

After modification
Click on OK to all this windows

Add a rule into the firewall interactively
or by batch commands:

```
@echo ========= Com+ Port ===================
@echo Enabling Com+ Port 1025-1225
netsh advfirewall firewall add rule name="Com+ Port 1025-1225" dir=in action=allow protocol=TCP localport=1025-1225
@echo Enabling Com+ Port 135
netsh advfirewall firewall add rule name="Com+ Port 135" dir=in action=allow protocol=TCP localport=135
```

3 - Configure client computers running Topology

Add a rule into the firewall interactively
or by batch commands:

```
@echo ========= SEE Electrical PLM – Topology ===================
@echo Enabling exe SEE Electrical PLM ® - Topology (TCP)
netsh advfirewall firewall add rule name="SEE Electrical PLM - Topology" dir=in action=allow protocol=TCP
program="C:\program files (x86)\ige+xao\see electrical plm - topology v4r7\see_soft\exe\seetopology.exe"
```

4 - On the client computer where the Flex LM server is installed

For a Flex lm server, you need to open, with protocol type TCP, the ports specified in the *.lic file delivered to you by IGE+XAO.

For instance:

```
-------
# IGE+XAO Group - Licenses File Description
SERVER serverID  001234567890 18000
--------
USE_SERVER
VENDOR see_lm port=18001
VENDOR see_lm2 port=18002
```

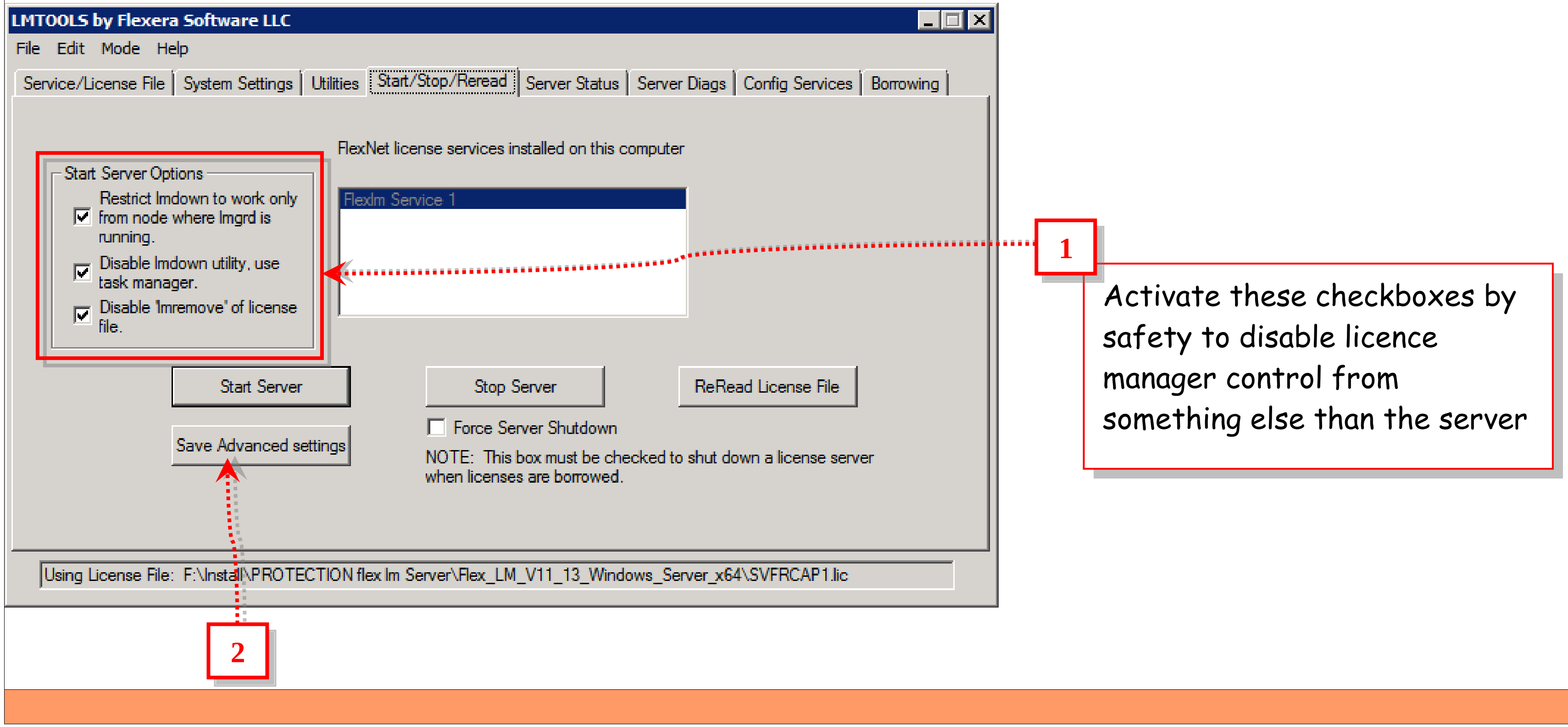
In this example you need to open Port 18000, 18001, 18002 with protocol type TCP.

Add a rule into the firewall interactively
or by batch commands:

```
@echo ========= Flex LM ports ===================
@echo Enabling Flex LM port 27000
netsh advfirewall firewall add rule name="Flex LM default port 27000" dir=in action=allow protocol=TCP localport=27000
@echo Enabling Flex LM port 18000-18002
netsh advfirewall firewall add rule name="Flex LM port 18000-18002 define into licence file" dir=in action=allow
protocol=TCP localport=18000-18002
```

Important Remark:
We recommend to set FlexLM Server Options with this configuration

From the LMTOOLS application on the licence server, go to Stop/Start/Reread tab and click the Advanced settings button. On the left side will appear Start Server Options.



LMTOOLS by Flexera Software LLC
File Edit Mode Help
Service/License File | System Settings | Utilities | Start/Stop/Reread | Server Status | Server Diags | Config Services | Borrowing
Start Server
Stop Server
ReRead License File
Save Advanced settings
1
2

Start Server Options

☑ Restrict lmdown to work only from node where lmgrd is running.

☑ Disable lmdown utility, use task manager.

☑ Disable 'lmremove' of license file.

FlexNet license services installed on this computer

Flexlm Service 1

□ Force Server Shutdown

NOTE: This box must be checked to shut down a license server when licenses are borrowed.

Using License File: F:\Install\PROTECTION flex lm Server\Flex_LM_V11_13_Windows_Server_x64\SVFRCAP1.lic

Activate these checkboxes by safety to disable licence manager control from something else than the server