Null sessions are used for various unauthenticated legacy communications purposes. They can be exploited through the various shares that are on the computer. Null Sessions is not a bug but a valid method used to allow systems to ask for resources from other systems without having to specify a username or password first. The problem is a considerable amount of information can be obtained through this type of connection including a list of user accounts on the host, password policies, domain information, etc.

For Creo Workflow, Clients and Servers all authenticate for their communication. As long as a client mounts unto a Server by specifying a user name and password then you will not have any problem disabling Null Sessions.

Creo recommends disabling this feature by doing the following:

Windows 2000:

- Select **Start > Run** and type **GPEdit.MSC**.
- Select **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security options**.
- Double click the value **Additional Restrictions for Anonymous Connections** and under Local Policy select **No access without explicit anonymous permissions**.
- Close and restart GPEdit.MSC and verify the **Effective Setting** for **Additional Restrictions** = **Local Setting**. If they do no match your Domain may be trying to push a lesser policy to you clients.

Windows 2003:

- Select **Start > Run** and type **GPEdit.MSC**.
- Select **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security options**.
- Modify the following Values:

Value	Setting
Network Access: All 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 and shares	Disabled
Network Access: Restrict Anonymous Access to Named Pipes and Shares	Enabled