ACP ThinManager Tech Notes

Remote ThinManager Connections

Use the **F1** button on any page of a ThinManager wizard to launch Help for that page.

Visit www.thinmanager.com/TechNotes4/01_Intro/Manuals.shtml to download the manual, manual chapters, or the abridged ThinManual.

Microsoft workstations have different permission levels than Windows servers. This can make it difficult to connect ThinManager on a workstation like Vista to the ThinManager Server on a Windows 2003 Server for remote administration.

Here are steps that can help.

1) Turn off the firewall on the workstation. This will allow two-way communication between the workstation ThinManager and the server ThinManager Server.

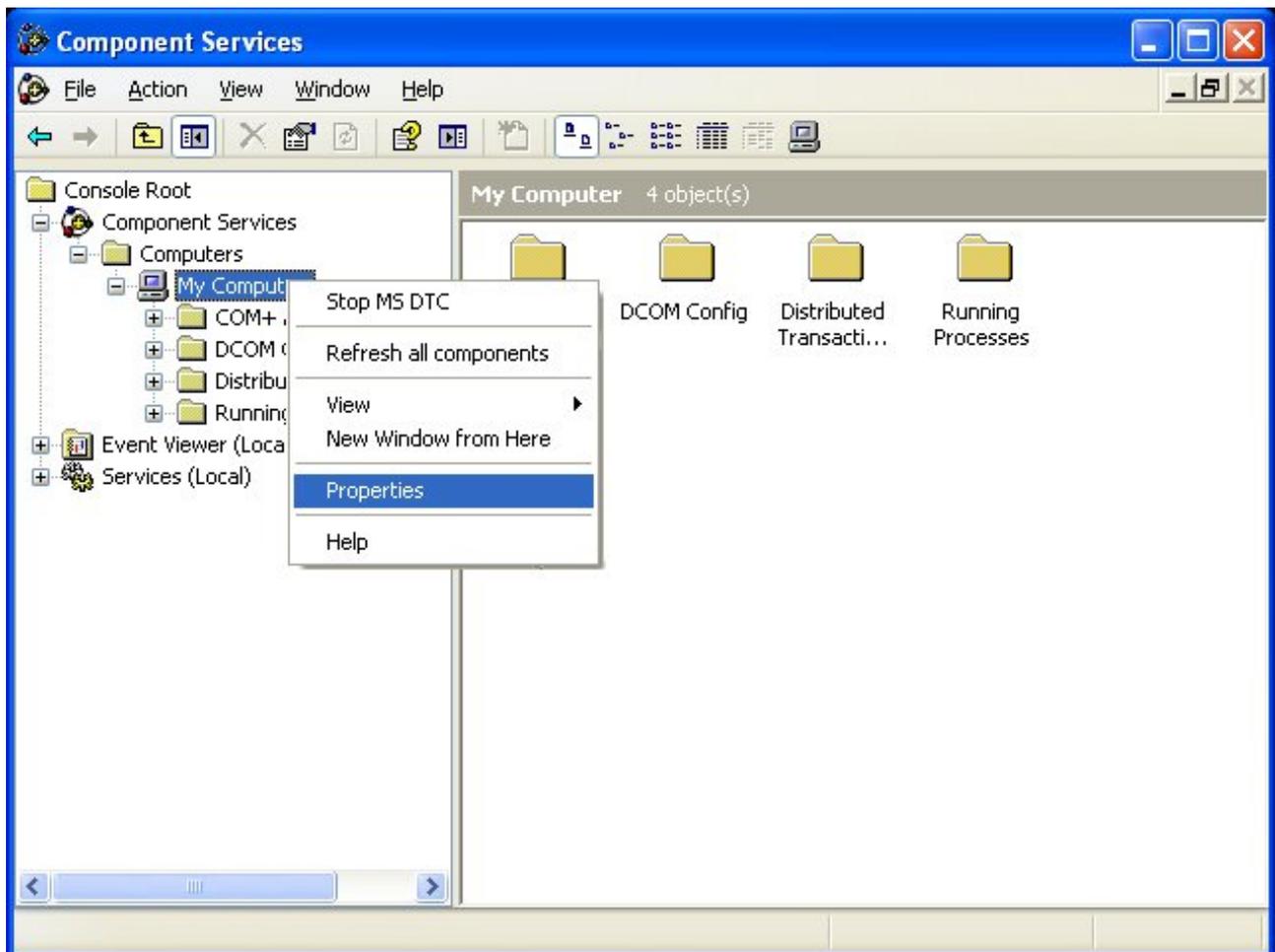2) Open the **Component Services** console by typing `dcomcnfg.exe` at a command prompt.

Figure 1 - Component Services

3) Expand the tree, right click on **My Computer**, and select *Properties* to launch **My Computer Properties.**

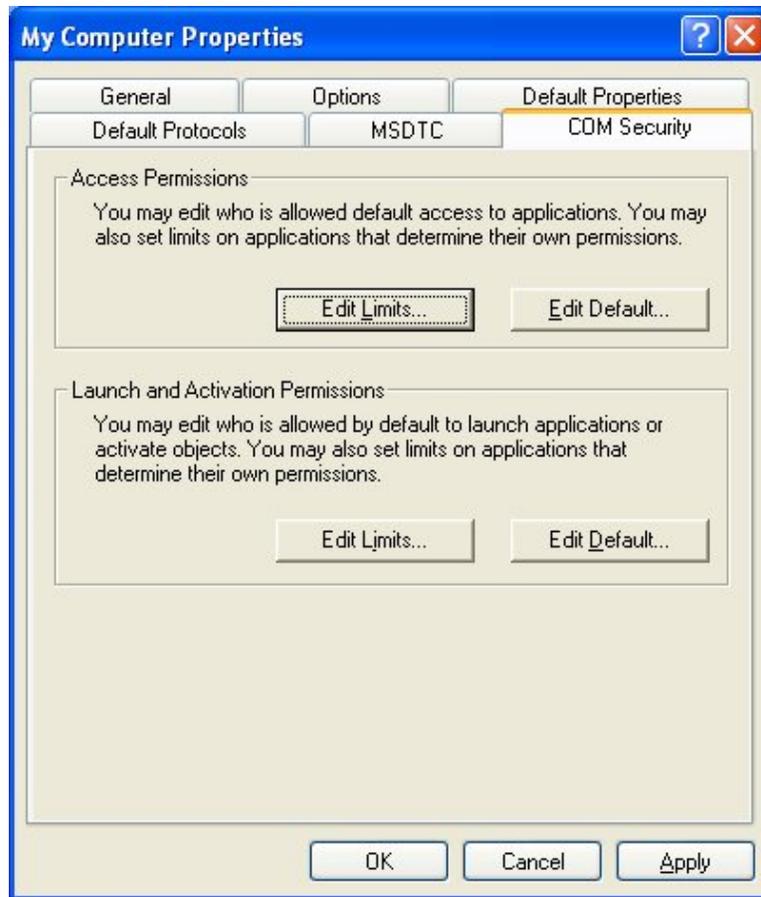**Automation Control Products**
www.thinmanager.com
Revised 1/26/2011

Figure 2 - COM Security Properties

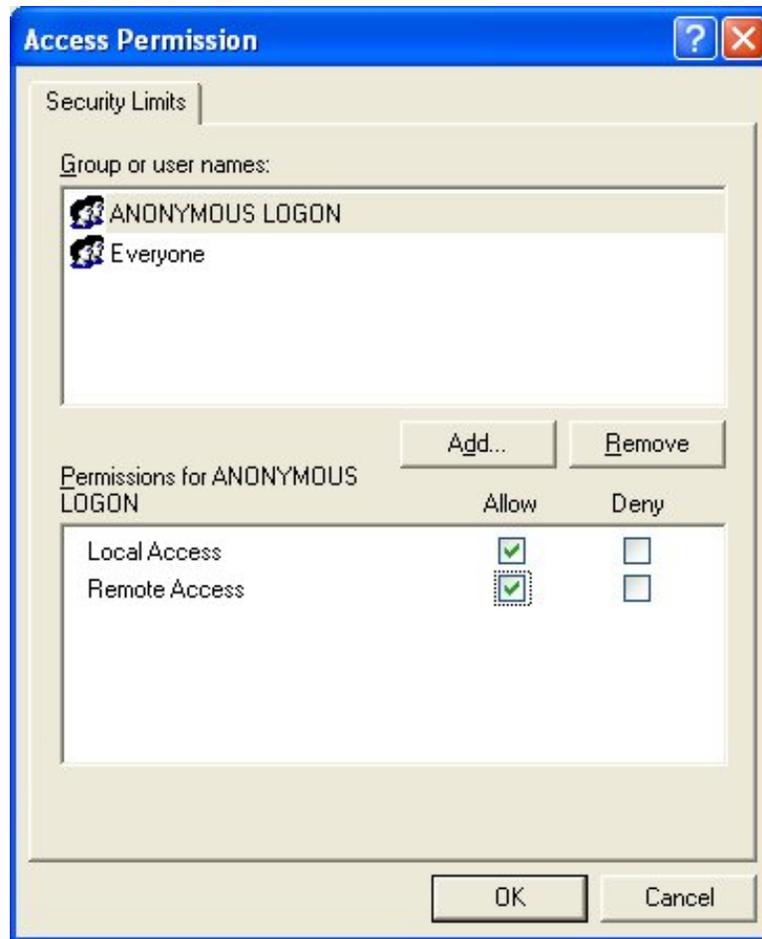4) Select the **COM Security** tab and select the **Edit Limits** button.

Figure 3 - Access Permissions

5) Make sure that the **ANONYMOUS LOGON** is allowed *Local Access* and *Remote Access*.

Remote Connection Login Request

When you try to connect to a remote ThinManager you may receive a Login Prompt.

Figure 4 - Login Prompt

If your user name and password don't work make sure that the user account has been granted Local Access and Remote Access on the remote ThinManager Server as shown in Figure 3.
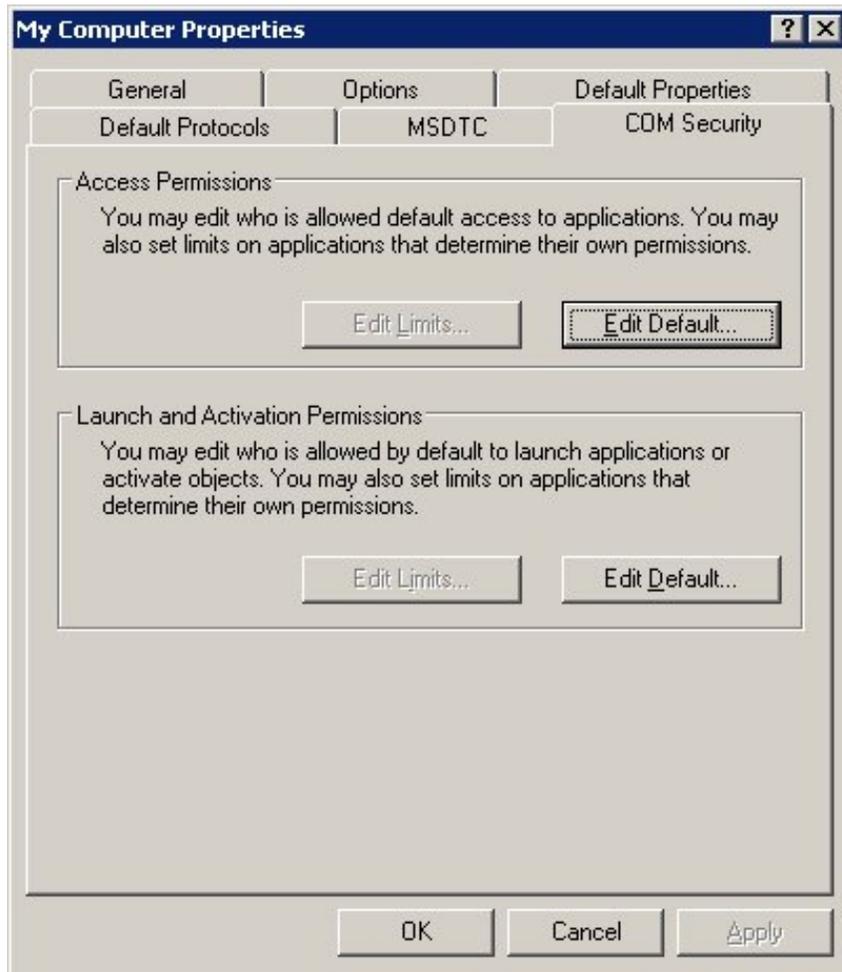
When Edit Limits are Disabled

Figure 5 - COM Security Properties

Some setups and configurations disable the *Edit Limit* buttons of the **COM Security** settings. This requires a change to the Local Security Policy.

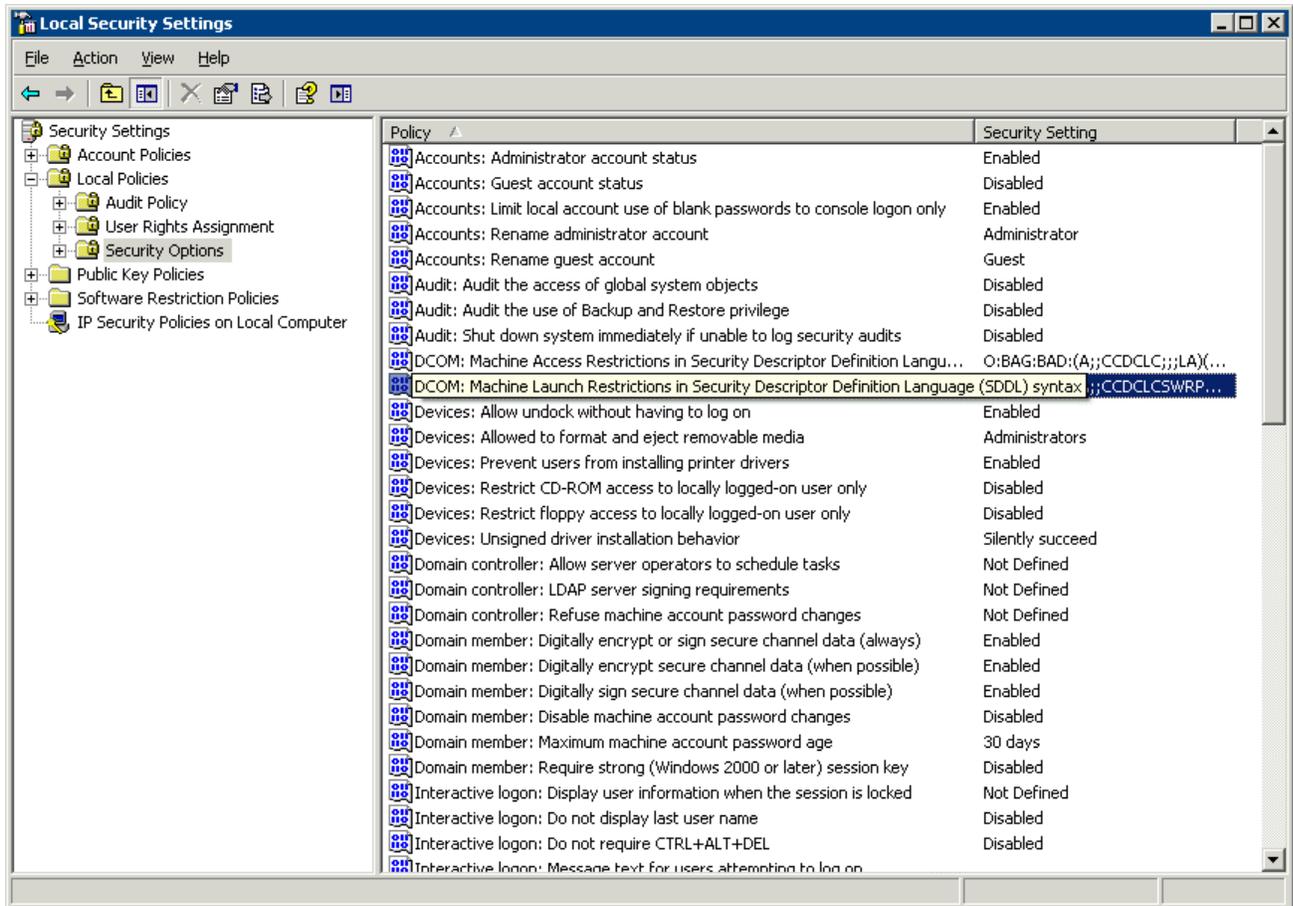Launch the Local Security Policy by typing `secpol.msc` at a command prompt.

Figure 6 - Local Security Policy

Expand the tree the tree to **Security Settings>Local Policies>Security Options**.

Double click on the **DCOM:Machine Launch Restrictions in Security Descriptor Definition Language (SDDL)** syntax policy to launch the policy setting window.
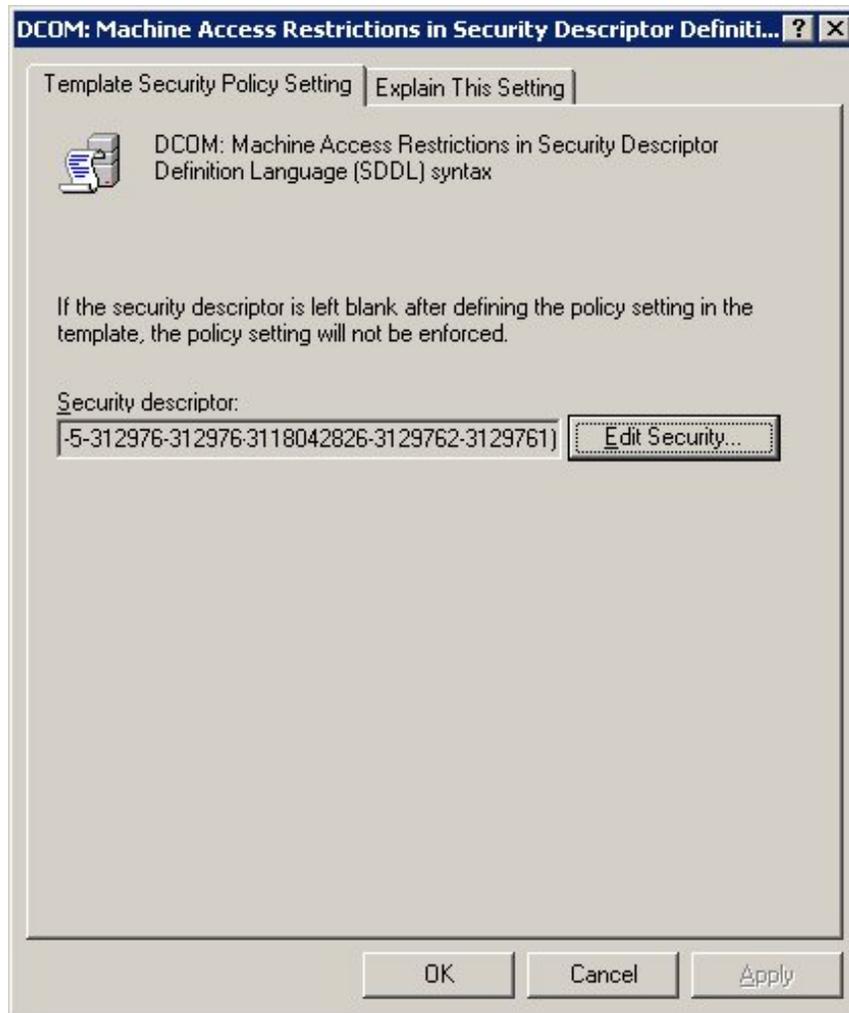
Figure 7 - DCOM Property Window

Select the **Edit Security** button to launch the **Access Permissions** window.
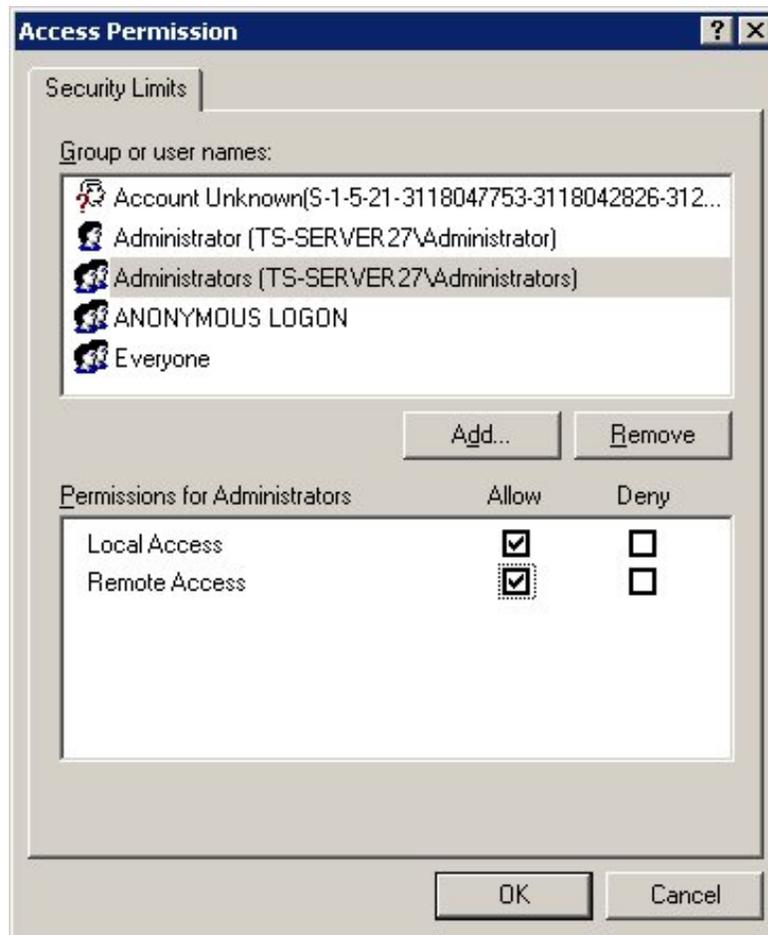
Figure 8 - Access Permission Window

Make sure that the ANONYMOUS LOGON is allowed *Local Access* and *Remote Access*. You may also add other Window groups and grant them the permissions.