

Remote ThinManager Connections

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

Visit <u>www.thinmanager.com/TechNotes4/01_Intro/Manuals.shtml</u> 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.

Discomponent Services	
🖗 File Action View Window Help	_ 8 ×
← → È 📧 × 📽 🖉 😫 🚥 🎽 📲 🗄 🗰 🗰 🗰 🕮	
Console Root Component Services Computers COM+ COM+ COM+ COM+ COM+ COM+ COM+ COM+	

Figure 1 - Component Services

 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



ly Computer Proper	ties	?
General	Options	Default Properties
Default Protocols	MSDTC	COM Security
Access Permissions You may edit who also set limits on aj	is allowed default access pplications that determine Edit Limits	to applications. You may their own permissions. Edit Default
You may edit who activate objects. Y determine their ow	is allowed by default to lau 'ou may also set limits on a n permissions.	unch applications or applications that
	Edit Limits	Edit <u>D</u> efault

Figure 2 - COM Security Properties

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



Access Permission		? 🛛
Security Limits		
<u>G</u> roup or user names:		
ANONYMOUS LOGON		
🕵 Everyone		
	A <u>d</u> d	Remove
Permissions for ANONYMOUS LOGON	Allow	Deny
Local Access		
Hemote Access		
1		
	OK	Cancel

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.

ОК
Cancel



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

General	Options	Default Properties
Default Protocols	MSDTC	COM Security
Access Permissions		
You may edit who also set limits on a	o is allowed default access applications that determine	to applications. You ma their own permissions.
	Edit Limits	Edit Default
aunch and Activat. You may edit who activate objects. determine their ov	ion Permissions o is allowed by default to lau You may also set limits on a wn permissions.	unch applications or applications that
Launch and Activat You may edit who activate objects. determine their ov	ion Permissions o is allowed by default to law You may also set limits on a wn permissions. Edit Limits	unch applications or applications that Edit <u>D</u> efault
Launch and Activat You may edit who activate objects." determine their ov	ion Permissions o is allowed by default to lar You may also set limits on a wn permissions. <u>Edit Li</u> mits	unch applications or applications that Edit <u>D</u> efault
Launch and Activat You may edit who activate objects.' determine their ov	ion Permissions o is allowed by default to lau You may also set limits on a wn permissions. Edit Limits	unch applications or applications that Edit <u>D</u> efault
Launch and Activat You may edit who activate objects.' determine their ov	ion Permissions o is allowed by default to lau You may also set limits on a wn permissions. <u>Edit Limits</u>	unch applications or applications that Edit <u>D</u> efault

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.



http://www.communications		
<u>File Action View H</u> elp		
🚱 Security Settings	Policy A	Security Setting
🗄 📴 Account Policies	👸 Accounts: Administrator account status	Enabled
	BAccounts: Guest account status	Disabled
	BAccounts: Limit local account use of blank passwords to console logon only	Enabled
User Rights Assignment	👸 Accounts: Rename administrator account	Administrator
English Security Options	🕮 Accounts: Rename guest account	Guest
H	👸 Audit: Audit the access of global system objects	Disabled
TP Security Policies on Local Computer	👸 Audit: Audit the use of Backup and Restore privilege	Disabled
The Security Policies on Local Computer	BAudit: Shut down system immediately if unable to log security audits	Disabled
	BOCOM: Machine Access Restrictions in Security Descriptor Definition Langu	O:BAG:BAD:(A;;CCDCLC;;;;LA)(
	BCOM: Machine Launch Restrictions in Security Descriptor Definition Language	(SDDL) syntax (;;CCDCLCSWRP
	👸 Devices: Allow undock without having to log on	Enabled
	👸 Devices: Allowed to format and eject removable media	Administrators
	👸 Devices: Prevent users from installing printer drivers	Enabled
	💐 Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
	💐 Devices: Restrict floppy access to locally logged-on user only	Disabled
	👸 Devices: Unsigned driver installation behavior	Silently succeed
	🕴 Domain controller: Allow server operators to schedule tasks	Not Defined
	🕴 Domain controller: LDAP server signing requirements	Not Defined
	🔀 Domain controller: Refuse machine account password changes	Not Defined
	🔀Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
	👸 Domain member: Digitally encrypt secure channel data (when possible)	Enabled
	💐Domain member: Digitally sign secure channel data (when possible)	Enabled
	👸 Domain member: Disable machine account password changes	Disabled
	👸 Domain member: Maximum machine account password age	30 days
	💐Domain member: Require strong (Windows 2000 or later) session key	Disabled
	👸 Interactive logon: Display user information when the session is locked	Not Defined
	👸 Interactive logon: Do not display last user name	Disabled
	Interactive logon: Do not require CTRL+ALT+DEL	Disabled
	1880 Interactive logon: Message text for users attempting to log on	<u> </u>

Figure 6 - Local Security Policy

Expand 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.



DCOM: Machine Access Restrictions in Security Descriptor Definiti ? 🗙
Template Security Policy Setting Explain This Setting
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax
If the security descriptor is left blank after defining the policy setting in the template, the policy setting will not be enforced.
Security descriptor:
-5-312976-312976-3118042826-3129762-3129761)
OK Cancel Apply

Figure 7 - DCOM Property Window

Select the *Edit Security* button to launch the Access Permissions window.



ss Permission		
curity Limits		
roup or user names:		
🖗 Account Unknown(S-1-5-21	-3118047753-3118	3042826-312
Administrator (TS-SERVER)	27\Administrator)	
Machinistrators (TS-SERVER	(27\Administrators)	
🖉 ANONYMOUS LOGON		
🥵 Everyone		
	Add	Remove
	Agg	Temove
ermissions for Administrators	Allow	Deny
Local Access	\checkmark	
Remote Access	$\mathbf{\nabla}$	
		-

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.