This document covers the computer configuration steps necessary to use the ASTRA V software application to communicate with Wyatt Technology instruments (DAWN HELEOS/TREOS, ViscoStar & Optilab rEX) via a TCP/IP network.

Distributed Component Object Model (DCOM)

ASTRA V and its monitoring tool (DiagnosticManager) use DCOM to communicate with Wyatt Technology instruments via TCP/IP. With the release of Windows XP Service Pack 2 and Vista, Microsoft modified the security permission level requirements for communication with networked devices using DCOM. This document explains how to modify the permissions to allow communication with Wyatt Technology instruments via TCP/IP.

1. Configuring Requirements
2. Accessing DCOM Default Settings, refer to the corresponding operating system
    - **Windows XP SP2**
    - **Windows VISTA**
3. Modifying DCOM Properties
4. Alternative Method to Edit COM Security Limits

Firewalls

If the client computer running ASTRA has an enabled firewall, a few specific TCP ports must be open for communication with Wyatt Technology instruments via TCP/IP. The software application installer will add the necessary firewall exceptions to the Windows Firewall.

If a firewall other then the Windows Firewall is used, see “ReadMe – Firewall Configuration (M6001 Rev B)” for detailed instructions.

1. Configuration Requirements

It is not necessary to follow these instructions if either of the following is true:

- Analyzing existing data (not collecting or monitoring instrument data)
- Only collecting instrument data from the following Wyatt Technology instruments:
    - DAWN EOS
    - DAWN DSP
    - DAWN DSP-F
    - miniDAWN
    - WyattQELS

Any of the following require adjusting the default DCOM configuration:

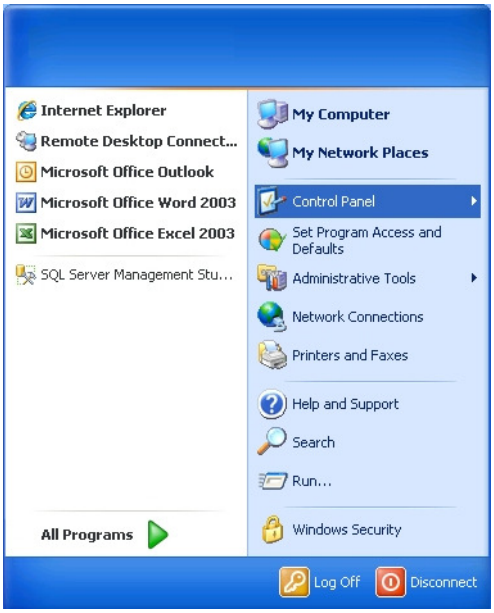
- Collecting and/or monitoring instrument data from one or more of the following Wyatt Technology instruments:
    - DAWN HELEOS
    - DAWN TREOS
    - ViscoStar
    - Optilab rEX

    Note: The DAWN HELEOS/TREOS instrument has an embedded QELS option. The QELS option has the same requirements as the DAWN host.
- Using one of the following Windows operating systems:
    - XP Service Pack 2 or higher
    - Vista

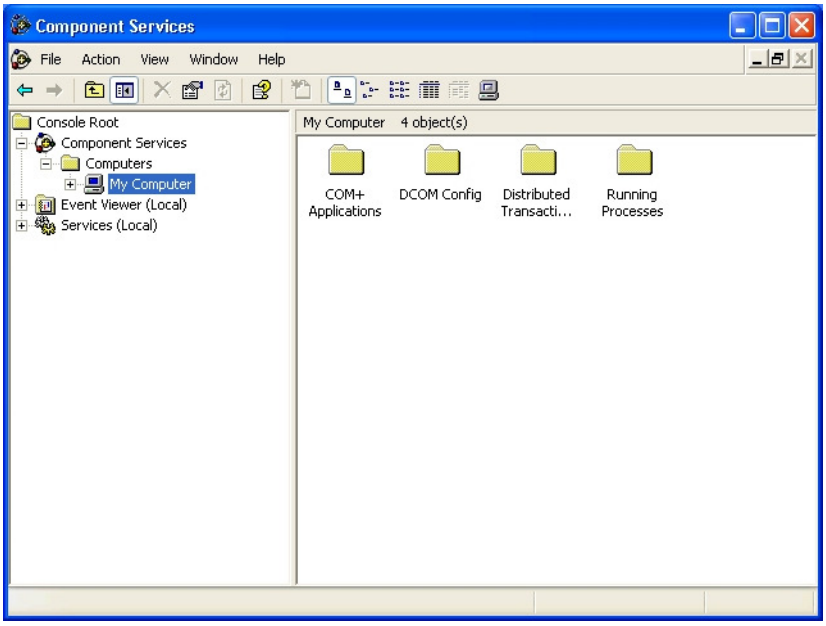
Note: Administrative privileges will be required for the active Windows user log on to modify the configuration parameters.

2. Accessing DCOM Default Settings Windows XP SP2

A. From the Start menu, choose Control Panel.

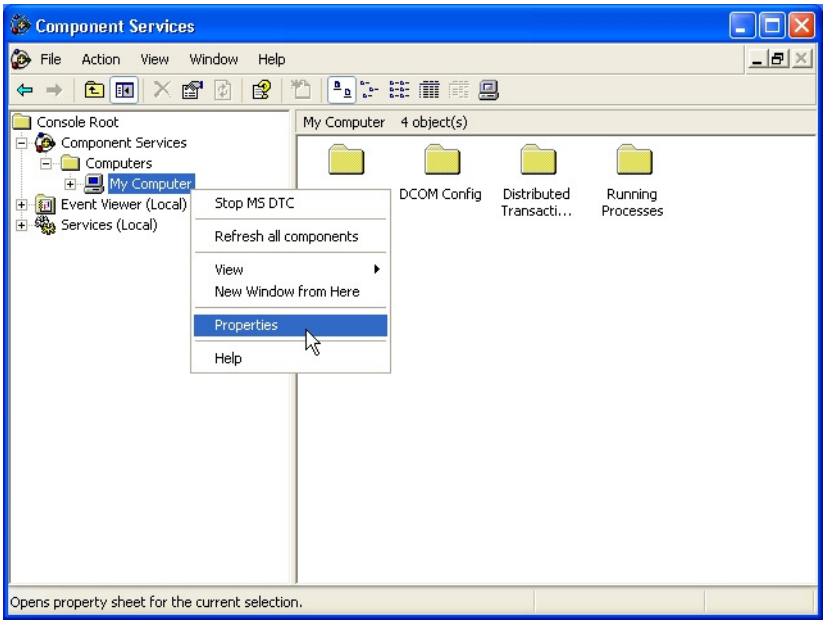


B. From the Control Panel, select Administrative Tools, then select Component Services.



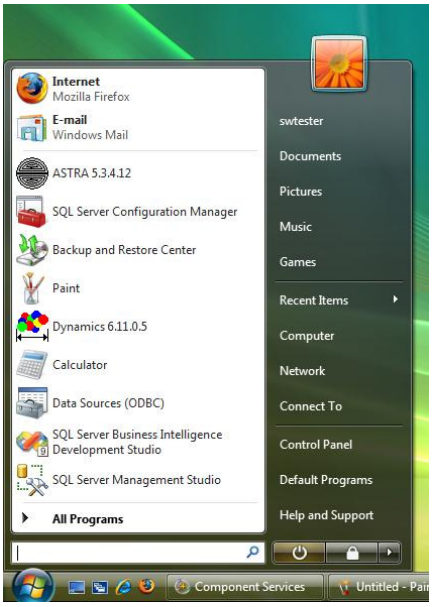
C. Expand the Component Services tree on the left pane to display “My Computer” as shown in the image above.

D. Right-click on the “My Computer” entry and select Properties.

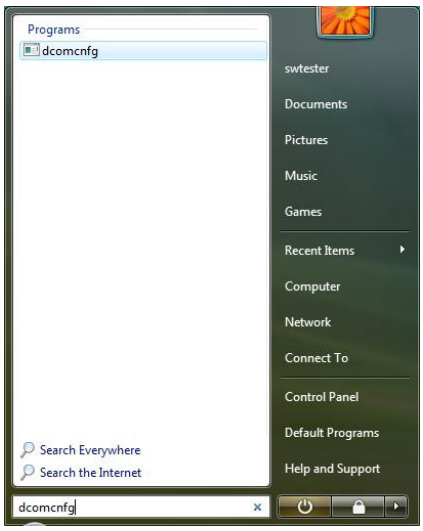


2. Accessing DCOM Default Settings Windows VISTA

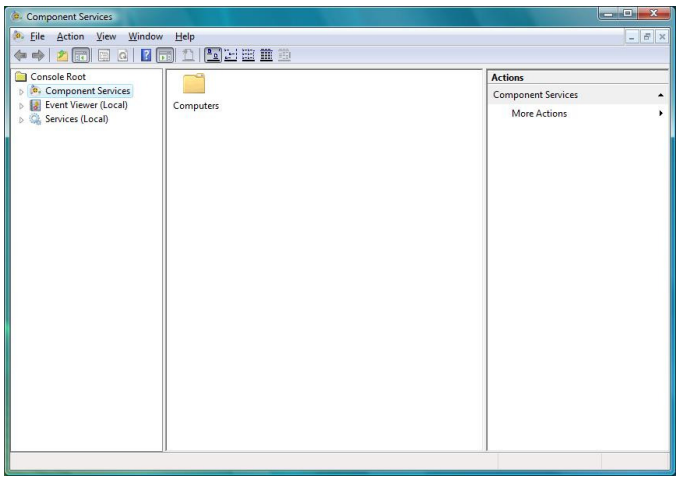
A. Click the VISTA ‘start’ button, typically in lower left corner, this should bring up the Start Bar.



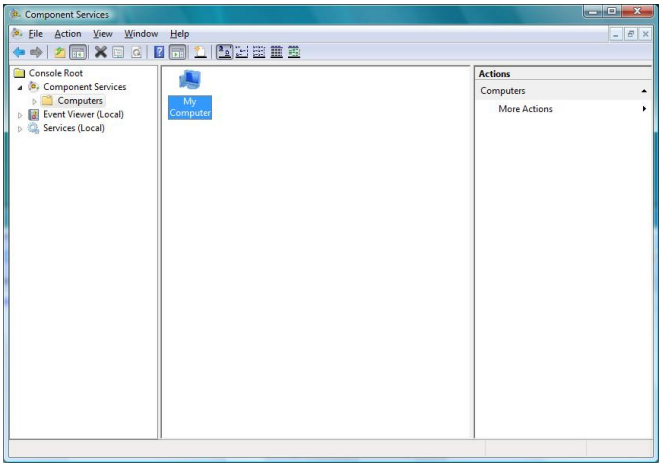
B. In the text box type ‘dcomcnfg’ then press enter.



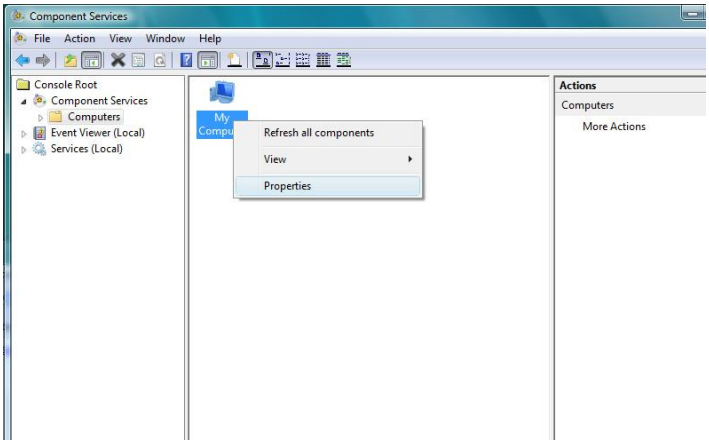
C. Double click on the ‘Computers’ Icon



D. Expand the Component Services tree on the left pane to display “My Computer” as shown in the image above.

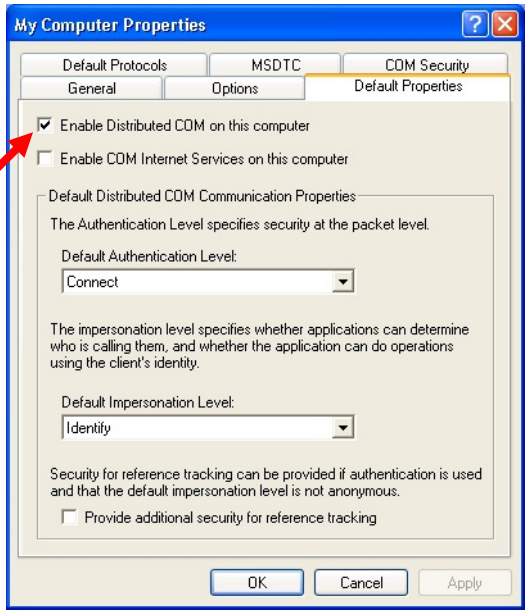


E. Right-click on the “My Computer” entry and select Properties.



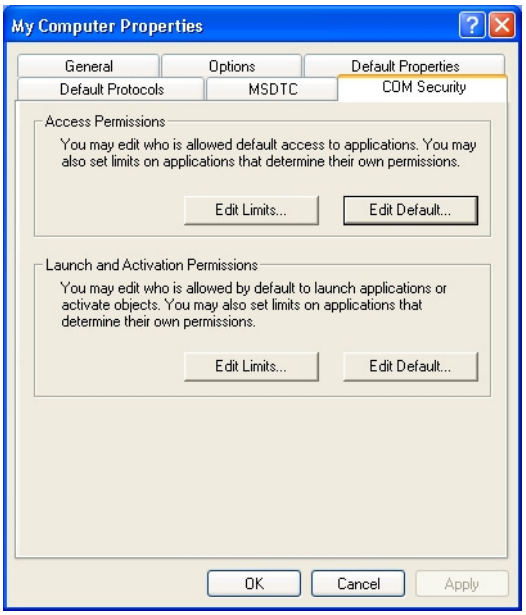
3. Modifying DCOM Properties

A. My Computer Properties for the Component Services will be displayed. Ensure that Distributed COM is enabled.

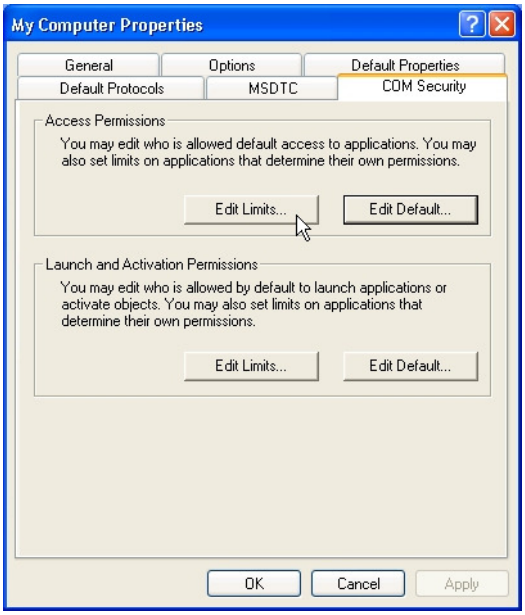


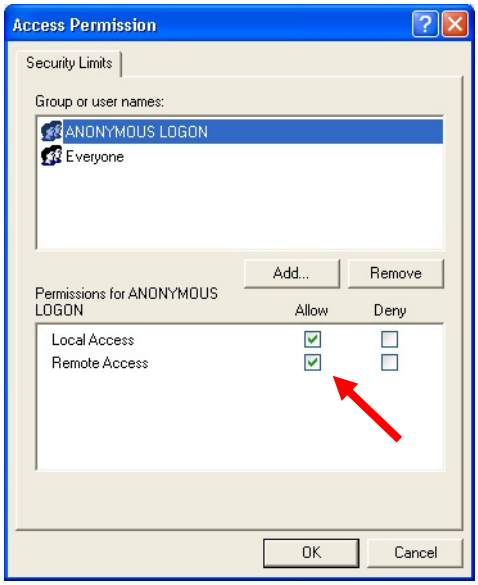
B. Select the COM Security Tab on the My Computer Properties dialog.

Note: If the "Edit Limits…" buttons are disabled see "3. Alternative Method to Edit COM Security Limits".



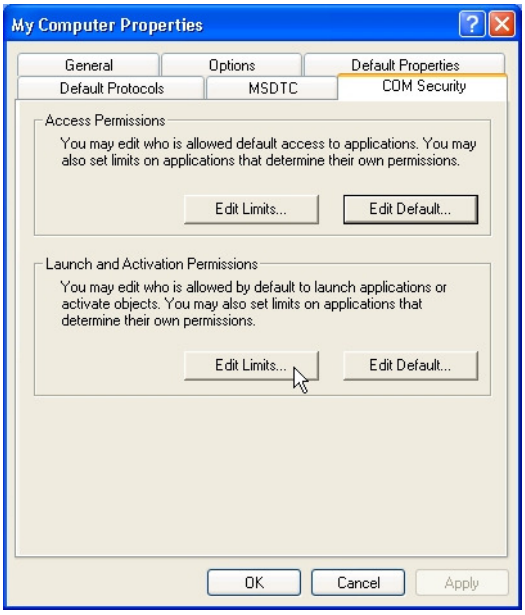
C. Press Edit Limits for Access Permissions, to display Access Permission dialog.

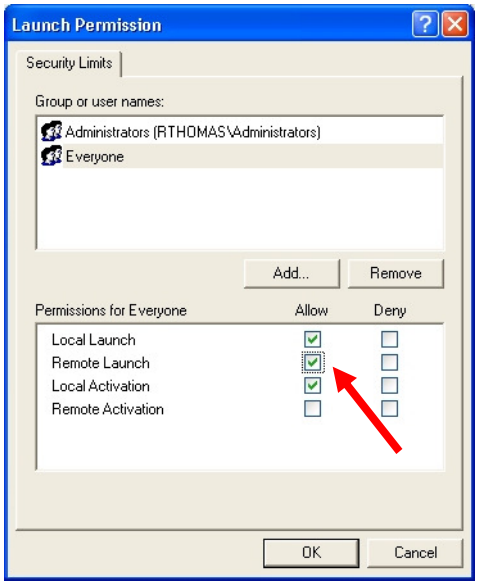




D. In the Access Permission dialog, select “ANONYMOUS LOGON”, then enable “Allow” for Remote Access. Press OK to apply the change and close the Access Permission dialog.

E. Press Edit Limits for Launch Permissions, to display Launch Permission dialog.





F. In the Launch Permission dialog, select “Everyone”, then enable “Allow” for Remote Launch. Press OK to apply the change and close the Launch Permission dialog.

G. Press OK to apply the changes and close the My Computer Properties dialog.

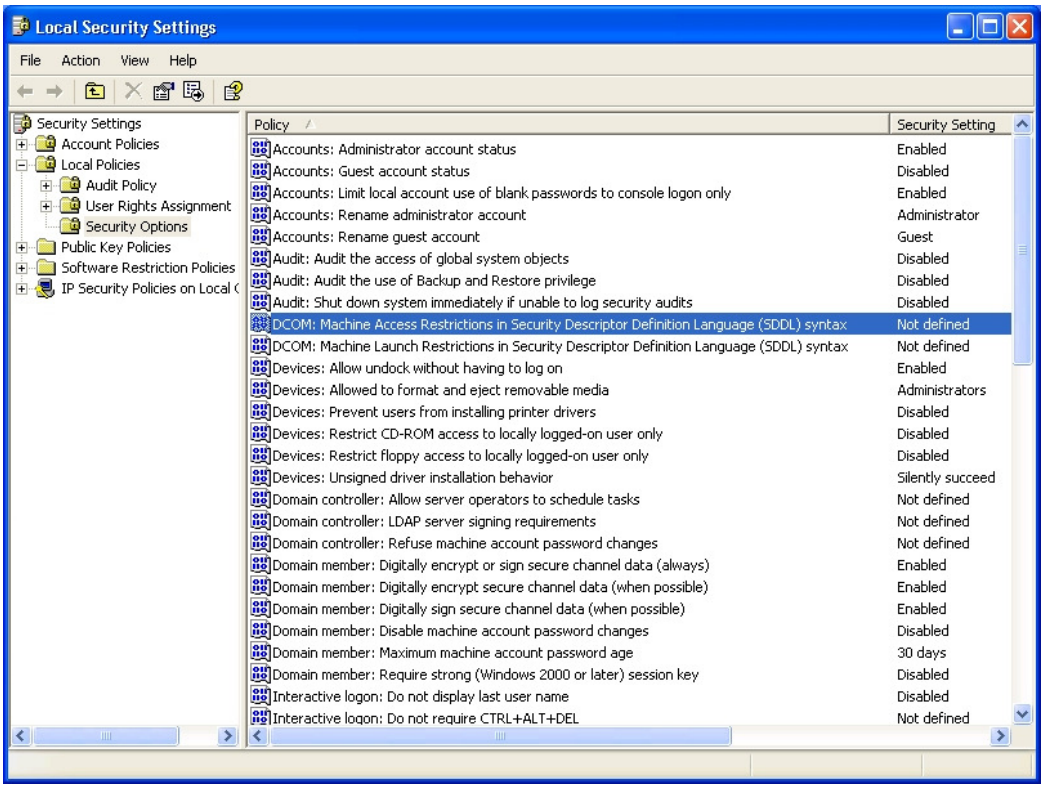
H. Close the Component Services window.

4. Alternative Method to Edit COM Security Limits

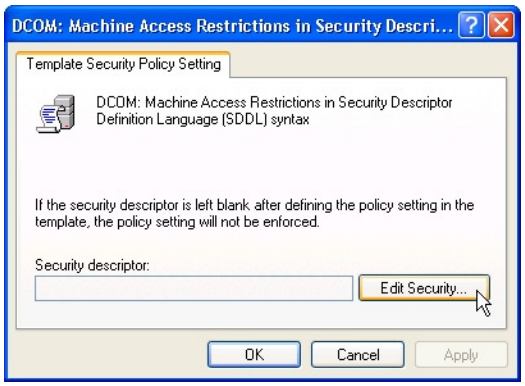
The “Edit Limits…” buttons can be disabled via Local security policy settings. If they are disabled the settings can be adjusted via the Local Security Policy.

A. From the Start menu, choose Control Panel, then select Administrative Tools, then select Local Security Policy.

B. Expand the Security Settings tree on the left pane to display “Security Options” as shown.



C. Right-click “DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax” and select Properties to display the Template Security Policy Setting for Access Restrictions.



D. Press the “Edit Security…” button to display the Access Permission dialog.

E. Follow the instructions for steps 2(H) above.

F. Press OK to apply the changes and close the Template Security Policy Setting for Access Restrictions.

G. Right-click “DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax” and select Properties to display the Template Security Policy Setting for Launch Restrictions.

H. Press the “Edit Security…” button to display the Launch Permission dialog.

I. Follow the instructions for steps 2(J) above.

J. Press OK to apply the changes and close the Template Security Policy Setting for Launch Restrictions.

K. Close the Local Security Policy window.