Kiosk Mode
For Instruments Using Windows Platform

Roger C. Lee
Brookhaven National Lab

ICALECPS 2009
Control System Cyber-Security Workshop
Oct. 11, 2009

Why is kiosk necessary

How to implement

Limitations

WHY KIOSK

- These instruments are just like a Windows desktop PC
  - They have all the security vulnerabilities of a desktop
  - Need to prevent unauthorized use
- Instrument may be used in a remote, unattended location for data acquisition
  - No keyboard or mouse
  - Must be running when accelerator is in operation
- Still want to have local use
  - Access to controls and display for system commissioning or diagnostics
- Want to be able to reboot the instrument remotely
  - Use remote AC reset to restore operation
  - No user interaction needed

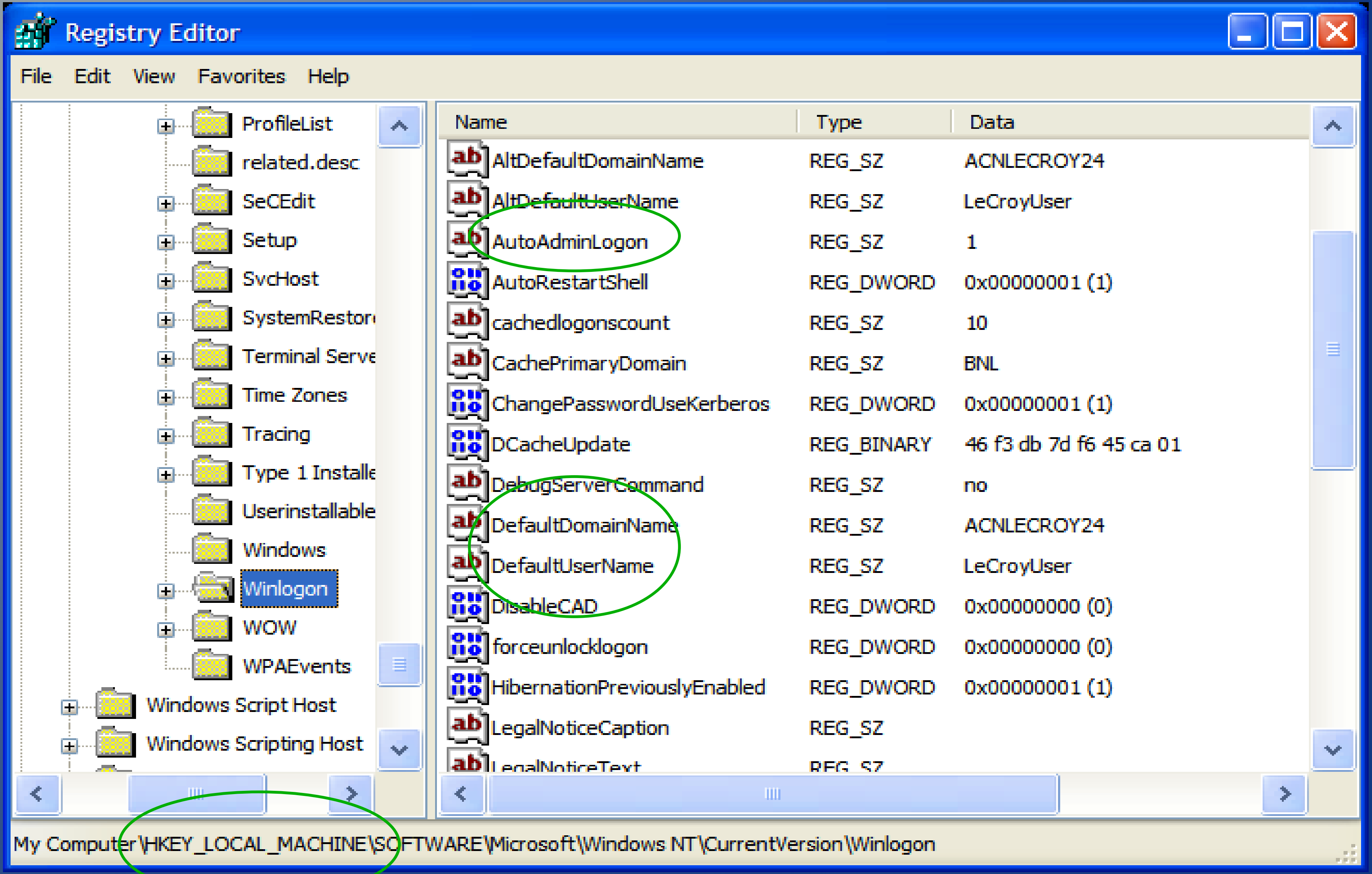
IMPLEMENTATION

How to allow local use of the instrument
and
provide cyber security.

1) Auto log-on
2) Run the instrument application at start up
3) No access to task manager

To automatically log on this account, instead of being prompted for credentials, follow these steps.

1. Locate the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
2. In the right pane open the string value “AutoAdminLogon”. If it doesn’t exist – create it.
3. Change the value of “AutoAdminLogon” from “0” to “1”.
4. In the same pane, add another string value called “DefaultUserName”.
5. Change the value for “DefaultUserName” to the name of the account you created for limited access.
6. Add another string value called “DefaultPassword”.
7. Change the value for “DefaultPassword” to the password you created for the limited account. If no password was set you can leave this blank.
8. Close the registry editor.

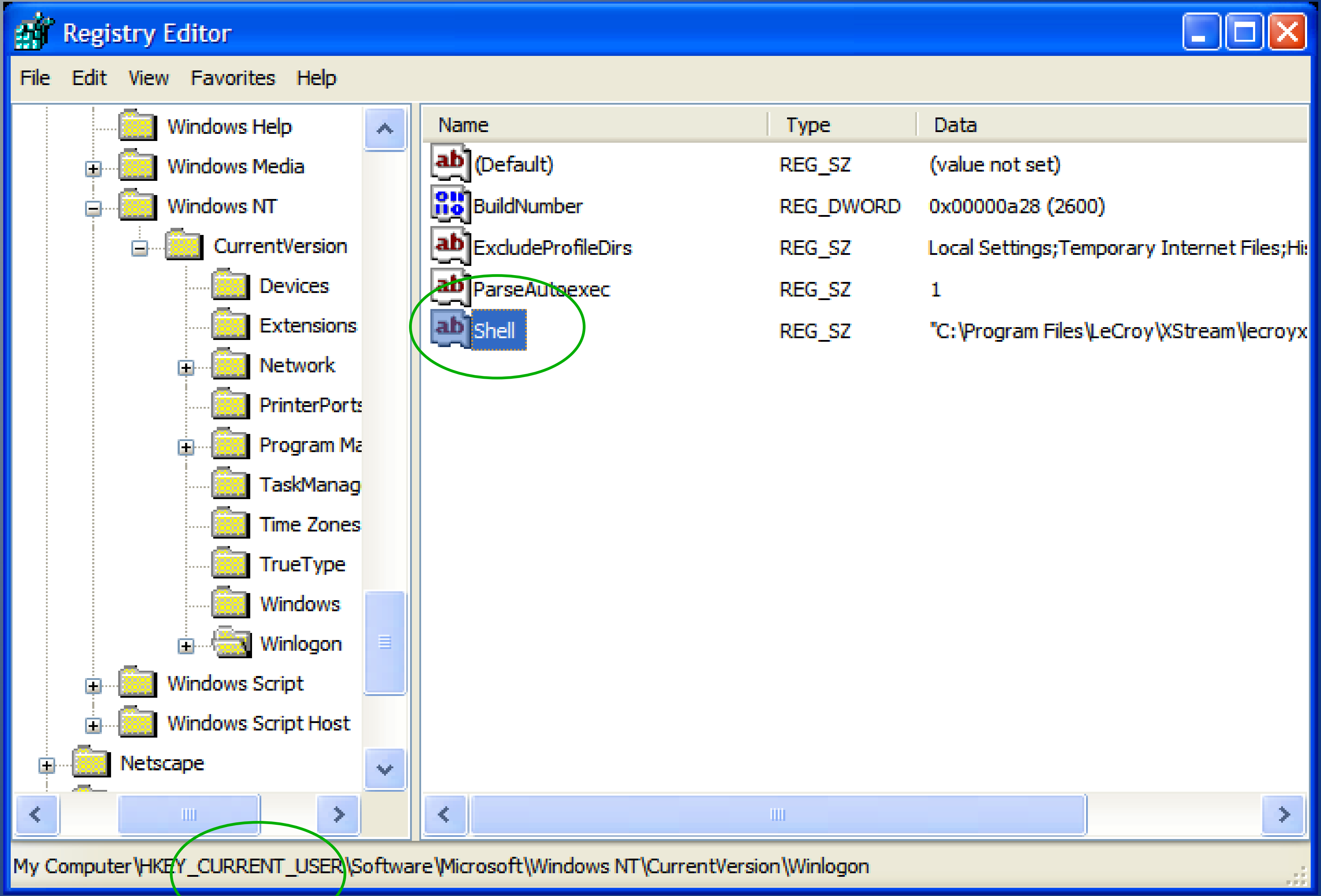


Name	Type	Data
AltDefaultDomainName	REG_SZ	ACNLECROY24
AltDefaultUserName	REG_SZ	LeCroyUser
AutoAdminLogon	REG_SZ	1
AutoRestartShell	REG_DWORD	0x00000001 (1)
cachedlogonscount	REG_SZ	10
CachePrimaryDomain	REG_SZ	BNL
ChangePasswordUseKerberos	REG_DWORD	0x00000001 (1)
DCacheUpdate	REG_BINARY	46 f3 db 7d f6 45 ca 01
DebugServerCommand	REG_SZ	no
DefaultDomainName	REG_SZ	ACNLECROY24
DefaultUserName	REG_SZ	LeCroyUser
DisableCAD	REG_DWORD	0x00000000 (0)
forceunlocklogon	REG_DWORD	0x00000000 (0)
HibernationPreviouslyEnabled	REG_DWORD	0x00000001 (1)
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

These steps will force the specified program to be run instead of the normal windows shell.

1. From an account with administrative rights, create a new account and give it administrative rights as well.
2. Log off and onto the new account you just created. (This account must have admin rights)
3. Open the registry editor by clicking Start – Run – and typing “regedit” in the space.
4. Locate the registry key HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon.
5. In the right pane – create a new string value and name it “Shell”.
6. Change the value for the newly created string to the application executable you wish to solely run on this account including the path.
7. Close the registry editor.

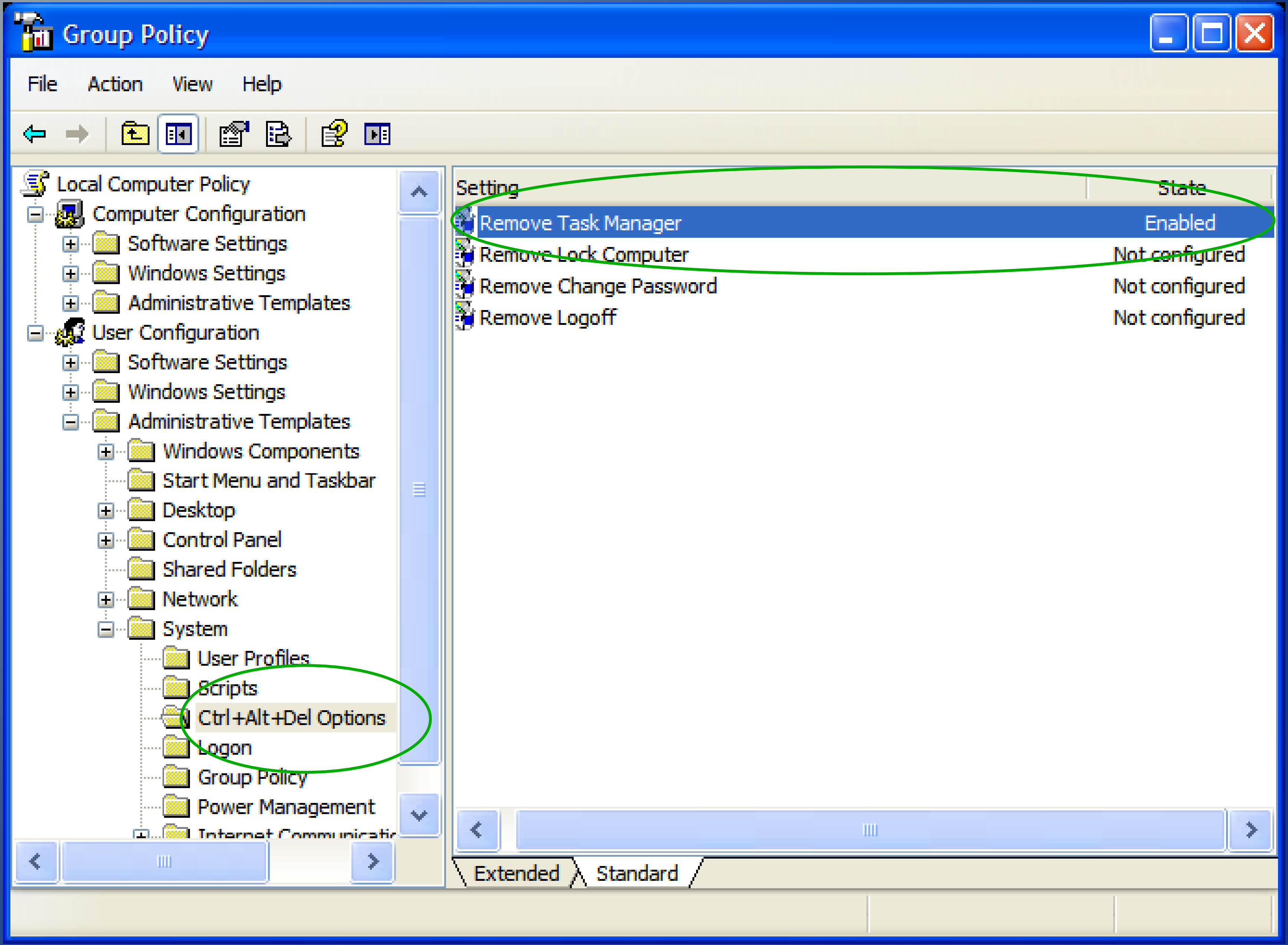


Name	Type	Data
(Default)	REG_SZ	(value not set)
BuildNumber	REG_DWORD	0x00000a28 (2600)
ExcludeProfileDirs	REG_SZ	Local Settings;Temporary Internet Files;Hi
ParseAutoexec	REG_SZ	1
Shell	REG_SZ	"C:\Program Files\LeCroy\XStream\lecroyx

My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

These last steps will disable the task manager so that no additional programs can be run or closed.

1. Click Start – Run – and type “gpedit.msc” in the space.
2. In the left pane expand the key called “User Configuration”.
3. Under “User Configuration” expand “Administrative Templates”.
4. Under “Administrative Templates” expand “System”.
5. Under “System” open the folder called “Ctrl+Alt+Del Options”.
6. Double click “Remove Task Manager” and change the setting from “Not Configured” to “Enabled”.
7. Close the policy editor.



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Windows Components
      - Start Menu and Taskbar
      - Desktop
      - Control Panel
      - Shared Folders
      - Network
      - System
        - User Profiles
        - Scripts
        - Ctrl+Alt+Del Options
        - Logon
        - Group Policy
        - Power Management
        - Internet Communicatic

Setting	State
Remove Task Manager	Enabled
Remove Lock Computer	Not configured
Remove Change Password	Not configured
Remove Logoff	Not configured

Limitations

The running application may provide access to the internet or the task bar.

After a “Remote Desktop” session it is necessary to log-on or reboot the device.

“Trials, Tribulations, and Pitfalls Using Commercial Instruments for Data Acquisition”