Configure Windows 7 for WiRES-X

Setting up Windows 7 for remote Wires-X operation

This document suggests how Windows 7 should be set up to operate unattended. I.e., 24x7x365. There are many “features” in Windows that assume an operator is sitting in front of the monitor. Many of these features can cause you to lose control of the computer.

The suggested modifications are classified as:
Critical: Essential for remote operation - it won’t run for long without this change.
Recommended - Good luck if you don’t make this change
Optional - You could get by without this change, mostly.

Typed user inputs shown in **bold**.

Important Note: These instructions assume that you have selected View By: Small Icons in the Control Panel.

What about Windows 10?

I don’t run Windows 10 and never plan to do so - I have an issue with my operating system being a social media machine that wants to market (or sell) me. So Win7 will be the end of the line for me.

That said, many of the techniques described in this document will apply to other versions of Windows. I will, however, accept instructions for other versions of Windows and post them (with credit given), but these won’t be coming from me.

Document Update History

Rev	Date	Change
1	25-Mar-2016	Initial Release
2	31-Mar-2016	Added info on preventing WinX installation

Table of Contents

Prepare Windows for Changes

Create a shell link that you can run as administrator. This shell window will be needed for several of the steps below.

- Create a command window and place it on your desktop
    - Point the mouse somewhere on the desktop
    - Right-click and select “New” then “Shortcut”
    - In the “Create Shortcut” dialog, enter **C:\Windows\system32\cmd.exe**
    - Click “Next”
    - Name the shortcut **Shell Window**
    - Click Finish

Automatically Log-in on Power-up (Critical)

This permits the computer to automatically log in to the user account when it is started - most likely because of a power failure or a Windows Update reboot.

Note: This opens up a security vulnerability. It is recommended that the WiRES-X node computer only be used for the node.

- Right-click the Shell Window and select “Run as administrator”
- A User Accounts window will open
    - Enter **netplwiz**.
    - Click the node account - this is typically the account that was generated when Windows was installed.
    - Uncheck “Users must enter a user name and password to use this computer” (See, we said it opened up a vulnerability.)
    - Click “OK”
    - Enter the user name of the account that will be automatically logged in.
    - Enter the password for the account (twice).
    - Click “OK”
- Test the automatic log in by shutting Windows down then starting it again. You should not be required to enter a password to get to the user screen

Set BIOS to Boot When Power is Applied (Critical)

This varies from computer to computer, so you’re on your own for this one.

Enter the BIOS or computer setup and enable a selection that causes the computer to automatically boot when power is applied.

Eliminate “Safe Start” Screen on Boot (Critical)

After an unplanned shutdown (i.e., power failure), Windows is unhappy. When it restarts it will probably give you a dialog box wanting to know if you should do a normal or “safe” boot. It will stay at this prompt until power is removed or the end of time (whichever comes first). Needless to say, you just lost complete control of your computer.

- Open the Shell Window with administrator privileges
    - Right click Shell Window and select “Run as administrator”
    - Click “Yes”
    - At “C:\windows\system32” type **bcdedit /set {current} bootstatuspolicy ignoreallfailures**
    - The computer should respond with “The operations completed successfully.”
    - Type **exit** to close the window

Prevent dialog box on crash from preventing WiRES-X reboot (Recommended)

Similar to above, WiRES-X (or any program that crashes) may present a modal dialog box asking if the program should close or if you want to troubleshoot it. That prevents YMAN from automatically restarting WiRES-X. This is not labeled as critical since you can login remotely and respond to the dialog box that’s preventing the restart.

- Right click Shell Window and select “Run as administrator”
- Click “Yes”
- Type gpedit.msc
- Expand Computer configuration then expand Administrative Templates
- Expand Windows Components
- Select Windows Error Reporting
- Double click“Prevent display of the user interface for critical errors”
- Select Enabled
- Click on OK
- Close all windows

Automatically Close and Restart WiRES-X (Recommended)

A task is set in the scheduler to periodically shut down WiRES-X. We then depend on YMAN to detect that it was shutdown and restart it. Why? Software can slowly collect errors as it runs (and some software more than others). There may be memory leaks, buffer overflows, etc. that slowly corrupt the software until it no longer functions properly. It is recommended to restart WiRES-X periodically before these errors accumulate to a degree that the software no longer functions properly. This is not critical because you can remotely log in to restart WiRES-X if necessary.

Note: If the computer is hosting a room, all occupants will need to rejoin the room when the restart occurs.

- From Control Panel -> Administrator tools choose Task Scheduler
- Select Action -> Create Task…
- In the “General” tab
    - Enter Name: **Restart WiRES-X**
    - If desired, add an appropriate description
    - Click “Run whether user is logged on or not”
    - Click “Run with highest privileges”
    - Select “Configure for: Windows 7….”
- Select the “Triggers” tab
    - Click on “New..”
    - Select “Begin the task: On a schedule”
    - Select an interval, i.e. “daily”
    - Select a date and time the computer should reboot, i.e. **Monday 12:45 AM**
    - Click OK
- In the “Actions” tab
    - Click “New..”
    - Click “Start a program”
    - Enter the following in “Program/script: **taskkill**
    - Enter the following in “Add arguments (optional):” **/F /IM Wires-X.exe**
    - Click “OK”
    - Click “OK”
    - Enter the user password
    - Click “OK”
- Test the reboot task
    - Click on “Task Scheduler Library”
    - In the center window click on the task you just created
    - Right click the task then select “Run”. You can also edit the task by clicking on “Properties”.

Automatically Reboot Windows (Recommended)

Similarly to WiRES-X, it may be beneficial to periodically restart Windows. This also provides Windows an opportunity to install any security updates it has downloaded.

- From Control Panel -> Administrator tools choose Task Scheduler
- Select Action -> Create Task…
- In the “General” tab
    - Enter Name: **Restart Windows**
    - If desired, add an appropriate description
    - Click “Run whether user is logged on or not”
    - Click “Run with highest privileges”
    - Select “Configure for: Windows 7….”
- Select the “Triggers” tab
    - Click on “New..”
    - Select “Begin the task: On a schedule”
    - Select an interval, i.e. “weekly”
    - Select today’s date and time the computer should reboot, i.e. “12:45 AM”
    - Enter the number of weeks between reboot, i.e., “1”
    - Select the day of the week, i.e. “Monday”
    - Click OK
- In the “Actions” tab
    - Click “New..”
    - Click “Start a program”
    - Click “Next”
    - Enter the following in “Program/script:” **shutdown**
    - Enter the following in “Add arguments (optional):” **-r -f**
        - The “-r” causes a reboot
        - The “-f” forces a reboot, otherwise a program that hangs could prevent the reboot
    - Click “OK”
    - Click “OK”
    - Enter the user password
    - Click “OK”
- Test the reboot task
    - Click on “Task Scheduler Library”
    - In the center window click on the task you just created
    - Right click the task then select “Run”. You can also edit the task by clicking on “Properties”.

Install Security Updates (Critical)

Normally it’s a bad idea for an unattended machine to get updates from Microsoft. You could consider just disabling automatic updates.

I suggest setting Control Panel -> Windows Updates -> Change Settings to:

- Install updates automatically (recommended)
- Every Monday at 3:00 AM
- Set the Windows reboot (above) to every Monday at 2:00 AM
- Disable “Give me recommended updates the same way I receive important updates”

Disable Timed Computer Shut Down (Critical)

Normal settings may cause the computer to sleep after a given period of keyboard inactivity. If this is done, the computer will be off and will have to be restarted manually or it will restart after a power failure.

- Control Panel -> Power Options
- Select “Balanced (recommended)”
- Select “Change plan settings”
- Set “Put the computer to sleep: to Never
- Click on “Save Changes”

“Safe” Remote Desktop Access

Remote Desktop normally uses port #3389 for access. Naturally this port is one of the first that will be investigated by any evil hacker. If the port is changed to a non-standard number, then it is unlikely our evil hacker will ever find it. To change the port you must modify Windows registry. You can really screw up your computer by making incorrect changes, so be careful. You have been warned!

- Enable RDP access
    - Open the Control Panel
    - Click on “System and Security”.
    - Under “System”, click “Allow Remote Access”
    - Under “Remote Desktop”, select “Allow connections from computers running any version of Remote Desktop (less secure)”

- Click on the Windows flag that is used to start programs
- In the text box, type **regedit**. This opens up the registry editor.
- Click “Yes” to use administrative privileges.
- Change the registry key that defines the RDP port number.
    - Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp by clicking on the various folders on the left-hand side
    - In the right-hand window, right-click on “PortNumber”, then select “Modify…”
    - In the window that opens up, click on “Decimal”
    - Under “Value data:” enter the new port number. I.e., 46191
    - Click “OK”
    - In the registry editor, click File -> Exit.
- It is necessary to open the selected port in the Windows firewall.
    - Open the firewall: Start->Control Panel->Windows Firewall
    - Select Advanced Settings
    - Select “Inbound Rules”
    - Select Action -> New Rule
    - Click on Port then “Next >”
    - Click on TCP
    - Click on “Specific local ports:” then enter the port number you chose. I.e., 46191
    - Click on “Next >”
    - Check all boxes then press “Next >”
    - Enter the name i.e., **RDP_UDP-46191**
    - Click on “Finish”

    - Repeat the above except select UDP instead of TCP and use a different name i.e., **RDP_TCP-46191**
- Restart the computer for the changes to take effect
- On another computer, access the remote desktop using: ComputerIP-or-URL:PortNumber. I.e., 192.168.0.32:46191
- Make sure your router also has this port number open if you wish to access the computer from outside your network.

Using Remote Desktop

TBD

Disable Hibernation (Optional)

Hibernation is not needed and simply creates a big file for your disk to store.

To make hibernation unavailable, follow these steps:

- Click Start, and then type cmd in the Start Search box.
- In the search results list, right-click Command Prompt, and then click Run as Administrator.
- When you are prompted by User Account Control, click Continue.
- At the command prompt, type powercfg.exe /hibernate off, and then press Enter.
- Type exit, and then press Enter to close the Command Prompt window.

Network Management - Open Ports to the Right Machine (Critical)

It is critical that your network router open incoming ports to this computer. I suggest setting up your router to assign a fixed IP address to this computer based on it's own ethernet or Wi-Fi MAC address.

- Determine the computer's MAC addresses by typing **ipconfig /all** in a shell window.
- Look for the "Physical Address" under the appropriate adapter. This is the MAC address of that adapter.
- Follow your router's instructions to assign a fixed IP address to a computer based on the determined MAC address.
- Follow your router's instructions to forward the following ports to the IP address chosen above:
    - 46,100
    - 46,110
    - 46,112
    - 46,114
    - 46,120
    - 46,122
    - 46,191 (or whatever port # you chose for the WiRES-X embedded web server
- Follow your router's instructions to forward UDP and TCP for the port you chose for the Windows Remote Desktop (See "Safe" Remote Desktop Access above).

Personalizations (Optional)

Disable all Windows-generated sounds

- Control Panel -> Sound -> Sounds: Sound Scheme = No Sounds
- Control Panel -> Sounds Deselect "Play Windows Startup Sound"

Eliminate the screen saver

- Control Panel -> Personalizations: Select Screen Saver None

Blank the screen after a certain amount of time

- Control Panel -> Power Options
- Select Balanced then click on Change plan settings
    - Set turn of display to 10 minutes
    - Make sure "Put the computer to sleep:" is set to Never
    - Click on Save changes

Improve computer performance - particularly for remote access

- Control Panel -> System -> Change Settings -> Advanced -> Performance "Settings…+
- Select "Adjust for best performance"
- Press OK and close the dialog boxes.

Prevent Unwanted Installation of WinX (Optional)

Microsoft has been aggressively promoting Windows 10 such that many people who didn't want it have installed it by mistake. Because of the complaints, Microsoft provided a mechanism to prevent unwanted "upgrades" to WinX, but these measures required editing the registry. Fortunately Steve Gibson at Gibson Research Corporation has provided a free tool to disable Windows Update from upgrading your Win7 or Win8.1 computer to WinX. This is a simple tool and I highly recommend it. You can learn about it here: https://www.grc.com/never10.htm

To do

Command line commands for Win7, i.e., taskmgr

Disclaimer

This document was authored by K9EQ. You use the information in this document at your own risk. Whatever happens to your radio including failure to function, malfunction, generation of interference, spontaneous combustion, electric shock, emotional stress, divorce, loss of friends, clinical depression and tying up repeaters complaining about K9EQ and his documents, before or after viewing this document is your responsibility.

While there is absolutely no blame on our part for any error we make, no matter how stupid or unkind, your suggestions or corrections to this document are appreciated and will be considered for inclusion in the next version.

Copyright