

Configure Windows 7 for WiRES-X

Setting up Windows 7 for remote Wires-X operation

DO NOT COPY AND POST THIS DOCUMENT TO ANOTHER SITE.

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.

Microsoft announced that on 15 January, 2020 that they were ending support for Windows 7. What should a node operator do? “Upgrade” to Win10? Stick with Win7? This issue is now addressed.

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.

Document Update History

Rev	Date	Change
4	13-Jan-2020	Added information regarding Microsoft's end of support for Win7
3	5-Oct-2019	Corrected minor errors with Firewall. Added section on Network Management. TeamViewer warning added.
2	31-Mar-2016	Added info on preventing WinX installation
1	25-Mar-2016	Initial Release

Table of Contents

[Document Update History](#)

[Table of Contents](#)

[Prepare Windows for Changes](#)

[Automatically Log-in on Power-up \(Critical\)](#)

[Set BIOS to Boot When Power is Applied \(Critical\)](#)

[Eliminate “Safe Start” Screen on Boot \(Critical\)](#)

[Prevent dialog box on crash from preventing WiRES-X reboot \(Recommended\)](#)

[Automatically Close and Restart WiRES-X \(Recommended\)](#)

[Automatically Reboot Windows \(Recommended\)](#)

[Install Security Updates \(Critical\)](#)

[Disable Timed Computer Shut Down \(Critical\)](#)

[“Safe” Remote Desktop Access](#)

[Using Remote Desktop](#)

[Disable Hibernation \(Optional\)](#)

[Network Management - Open Ports to the Right Machine \(Critical\)](#)

[Personalizations \(Optional\)](#)

[Support of Win7 After Microsoft Doesn't](#)

[Purchase “Upgrade” to Windows](#)

[“Upgrade” Windows 10 Without a Purchase](#)

[Stay with Win7 and Take Your Chances](#)

[Stay with Win7](#)

[Cheat with Win7](#)

[Win10 “Upgrade” Good or Bad Idea?](#)

[To do](#)

[Disclaimer](#)

[Copyright](#)

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

Note: Use of TeamViewer is NOT recommended. This is a popular and POWERFUL tool for system administrators and provides an EXTREME level of control over the remote computer. However it does interfere with the operation of WiRES-X.

Google Chrome Remote Desktop has been used successfully, but beware that Google installs a lot of code, and thus overhead, on your computer to support this. In addition to The Goog tracking the computer, you may not want this overhead on a small system.

MNWiS uses RDP exclusively because it is efficiently integrated with the OS. However, it may not be supported by some “home” versions of the OS. We don't have the resources to try all of the options out there. Please let us know of your experiences.

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.

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 >”
 - Click on “Allow the Connection” then press “Next >”
 - Check all boxes then press “Next >”
 - Enter the name i.e., **RDP_TCP-46191**
 - Click on “Finish”
 - Repeat the above starting with “Select Action -> New Rule” except select UDP instead of TCP and use a different name i.e., **RDP_UDP-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.

Support of Win7 After Microsoft Doesn't

Microsoft general support for Win7 ends 15 Jan 2020. Extended support is available, but that service is designed for big companies with deep pockets. Win7 probably runs most of the WiRES-X nodes, so this presents a problem for the community. What to do? The options we'll discuss are:

1. Upgrade to Windows 10 by making a donation to the Microsoft fund.
2. Upgrade to Windows 10 without making a donation.
3. Stay with Windows 7 and take our chances.
4. Stay with Windows 7 and mitigate potential issues from the removal of support.
5. Cheat and continue to get Windows 7 updates.

Purchase "Upgrade" to Windows

You can go to Microsoft online, pull out your credit card, download Windows 10 and install it on your computer. For a time Microsoft made the "upgrade" free. That time has ended so they are "officially" requiring you to purchase the "upgrade" should you want it. What I have learned in life is that Hams are cheap, er, I mean frugal. I really doubt anyone wants this option, but it's there should you want it.

Why does he keep putting "upgrade" in quotes? Keep reading.

"Upgrade" Windows 10 Without a Purchase

It turns out that it's possible to "upgrade" your computer to Windows 10 without whipping out your credit card. While Microsoft says you need to purchase the "upgrade", there are techniques that allow you to perform the "upgrade" at no cost. Note that these methods are not sanctioned by Microsoft and could go away or fail at any time should they decide to make a change. In other words, "You pays your money and you takes your chances".

The process for "upgrading" without a purchase is as follows:

1. This upgrade only works if you already have a valid Win7 or Win8/8.1 license.
2. Download the Windows 10 "upgrade" tool from microsoft at: <https://grc.sc/win10>
3. **You will be converting your Win7 license to a Win10 license. YOU CANNOT GO BACK!!!! Therefore make a complete disk image of your hard drive before you go any further. This might be a great time to clone your hard drive to a brand new SSD and keep the old one for backup or recovery. You've been warned!**
4. Run the "upgrade" utility. See the instructions at: <https://www.bleepingcomputer.com/news/microsoft/you-can-still-upgrade-to-windows-10-for-free-heres-how/>
5. Follow [these instructions](#) for adjusting Win10 to run reliably.
6. You will have a digital license that's good for the life of the hardware.

Stay with Win7 and Take Your Chances

After all, how many times has your node been hacked? Win7 has worked fine and will continue to work fine. The updates and patches mostly address security issues regarding Win7. If you don't care about security issues then you don't need to do anything.

Keep in mind that security issues on your node computer could impact other computers on your network. You could isolate your node computer on a "guest" network so it can't communicate with your other computers. See K9EQ's take on security (below).

Stay with Win7

There are things we can do so that any potential security issues with Win7 are very unlikely to have an impact. In fact these are smart things to do even if you are on Win10. After all the security issues existed before Microsoft patched them. In some cases the security issues have existed for many, many years. It's unlikely Microsoft was the first to spot the problem!

Many of the security issues are not the result of a problem with the operating system, but come as a result of defects in application software and bad decisions made by the user of the computer. The rules below are intended to mitigate almost all of the potential risk from security vulnerabilities.

1. **If you didn't ask for it, don't click on it.** Only do things YOU decided to do, not things someone else decided you should do. This particularly applies to email.
2. **Don't install ANY applications that you don't absolutely need!** My recommendation is to have at least two computers. One computer for important stuff (banking, stocks, etc.) and one for fun stuff. Leave the important computer off and don't install unnecessary applications on it. Use the fun computer to play.
3. **Don't run any antivirus software except for that from Microsoft!** Antivirus software drills deep down into your operating system and become a security risk. Keep in mind that these companies quit making money if the security problems go away. They are bloated with all kinds of s**t you don't need and can kill the performance of your computer. Just use the free Microsoft tool. It works just fine.
4. **Don't run as administrator.** Have a user account and an admin account. I know it's a pain to keep typing in the admin password when you want to change things, but 70% of the attacks are mitigated by NOT running as an administrator!
5. **Don't run any software unless it's needed.** I suggest that you have a dedicated node computer and only run your Amateur Radio software on it. No email. No web surfing. Just WiRES-X and perhaps things like Ham Radio Deluxe.
6. **Shut down any services you don't need.** Why have computer sharing turned on when you're not sharing between computers? It just opens more holes of which attackers can take advantage.
7. **Keep all software up to date.** Developers do fix problems and that does reduce the security risk.
8. Follow the instructions in this document to increase the reliability of your node, particularly if it is running at a remote site.

Many people have run WinXP for years after support was dropped without issues. In fact WinXP is still running today in gas pumps, ATMs, and other places where there's a screen. This works because these systems don't "surf the web". They only communicate point-to-point and that doesn't give the bad guys and gals much of an opportunity to hack in. We're doing the same thing by just using the node to talk to the WiRES-X servers. It's really unlikely WiRES-X servers are going to be run by nefarious Russians.

Cheat with Win7

As with WinXP, it is possible to continue to get Win7 updates after the official end of support. Eventually these tricks will fail.

You're on your own with this. My personal preference is to lock Win7 down and not take any new updates.

Should you want to investigate continuing to receive updates, check here:

<https://hothardware.com/news/windows-7-extended-security-updates-january-2020-bypassesu>.

Win10 “Upgrade” Good or Bad Idea?

You may have noticed I’ve been putting “upgrade” in quotes. That’s because as far as WiRES-X is concerned, it isn’t an upgrade. We’re just getting more stuff we don’t need. Microsoft clearly plans on using Win10 as a platform to generate revenue by selling products and services to you. Do you really need Candy Crush? Try to get rid of it!

It also occurs to me that it might be nice to not get updates. Most of my problems running a WiRES-X node have come as a result of Windows 7 updates that have screwed the system up. For some reason when an update gets load but not installed, things quit working right until the update is finally installed. I’m looking forward to not having to deal with those 2nd Tuesday updates!

To do

- Command line commands for Win7, i.e., taskmgr
- Installing Windows easily:
http://answers.microsoft.com/en-us/windows/forum/windows_7-update/windows-7-update-solution/f39a65fa-9d10-42e7-9bc0-7f5096b36d0c
- Testing computer hardware: <http://www.memtest86.com>
- Microsoft update download: <https://support.microsoft.com/en-us/kb/119591>
- Microsoft security update bulletins: <https://technet.microsoft.com/en-us/security/bulletins.aspx>
- Sep 2016: <https://technet.microsoft.com/en-us/library/security/ms16-sep>
- Microsoft security tools: <https://technet.microsoft.com/en-us/library/security/ms16-sep>
- Microsoft update catalog (needs IE):
<http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB3175443>
-

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

This document is Copyright 2016-2020 by K9EQ and HamOperator.com. All rights reserved. You may use this document as you wish providing its use does not violate any law or Yaesu published instructions. If you transmit this document to another person by any means, it must remain unaltered from the original. Encourage others to obtain this document via direct download from <http://www.hamoperator.com> - and thus ensuring retrieval of the latest version. You may modify your own version with your own notes, but are then prohibited from distributing that version.

DO NOT COPY AND POST THIS DOCUMENT TO ANOTHER SITE. It is constantly being updated and freezing the document in time would be a disservice to the community. Rather link to this document at:

<http://www.hamoperator.com/Fusion/FusionFiles/K9EQ-Fusion-PDF-0017-Win7.pdf>

This URL will not change.