Windows Hardening

Research and apply hardening techniques to the Windows OS.

In this article, we'll explore ways to make the most of Windows operating system configurations to make our Windows computer safe.

Windows Quirks To Consider

Windows has many settings and options spread across an array of separate menus within the operating system. Microsoft tries to make sure that old software and hardware will continue to function with new versions of Windows software. While maintaining compatibility has its benefits, it also creates some inconsistent rules.

Because of these version differences, keep in mind that there is no one-stop-shop for hardening all versions of Windows. In this article, we will walk through a basic hardening checklist that should inspire some further research. Follow along and see which ones you haven't implemented yet!

Basic Windows Hardening Checklist

This section is a guide to enable basic security features and hardening measures and to help build your confidence to move onto more advanced hardening. As you work your way through this list, it's a good security habit to research each item before you go through with it.

Account Setup

Force Accounts to Have Passwords

- Open the "Run" app by searching for it or using `Win+ r`.
- Type `netplwiz` into the dialog box and click "OK".
- Check the box labeled "Users must enter a user name and password to use this computer." in the "User Accounts" window.

Limit Administrator Privileges to only Necessary Accounts

- From the same "User Accounts" window, you can set whether or not accounts have administrator privileges.

- Select an account that you want to add or remove administrator privileges from, then click "Properties".
- In the new window, switch to the "Group Membership" tab, and select "Standard User" or "Administrator" as appropriate.
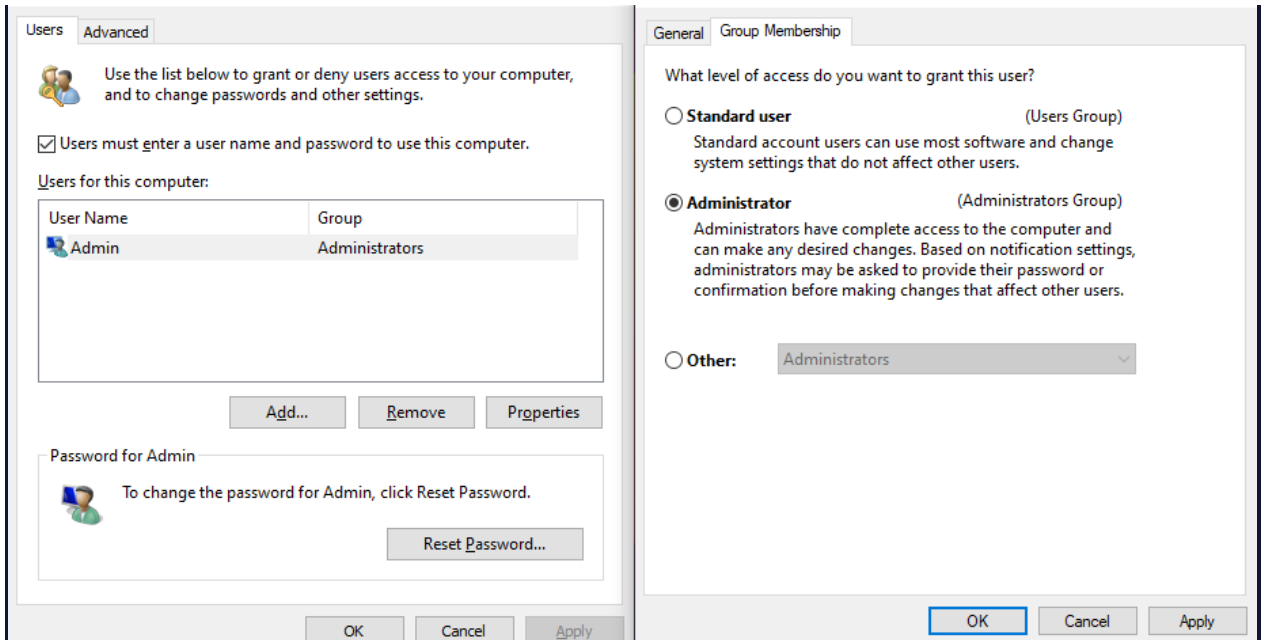
Require Log In on Screensaver

- Open the "Settings" app.
- Go to the "Accounts" section.
- Go to the "Sign-in options" section in the sidebar.
- Under the "Require sign-in" header, select "When PC wakes up from sleep"

Windows Security Features

Turn on Windows Firewall

- Open the "Windows Security" app.
- Go to "Firewall & network protection".

- Ensure that the domain, private, and public networks all have their firewall enabled.

⟨ɪ⟩ Firewall & network protection

Who and what can access your networks.

🔲 **Domain network**

Firewall is on.

🔲 **Private network** (active)

Firewall is on.

🔲 **Public network**

Firewall is on.

Turn on Windows' Built-In Antivirus

This serves the same general purpose as 3rd-party antivirus software, providing scans and real-time protection against malicious software.

- Open the "Windows Security" app.
- Go to "Virus & threat protection".
- Go to "Virus & threat protection settings".
- Turn on "Real-time protection", "Cloud-delivered protection", "Automatic sample submission", and "Tamper Protection".

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

Submit a sample manually

Tamper Protection

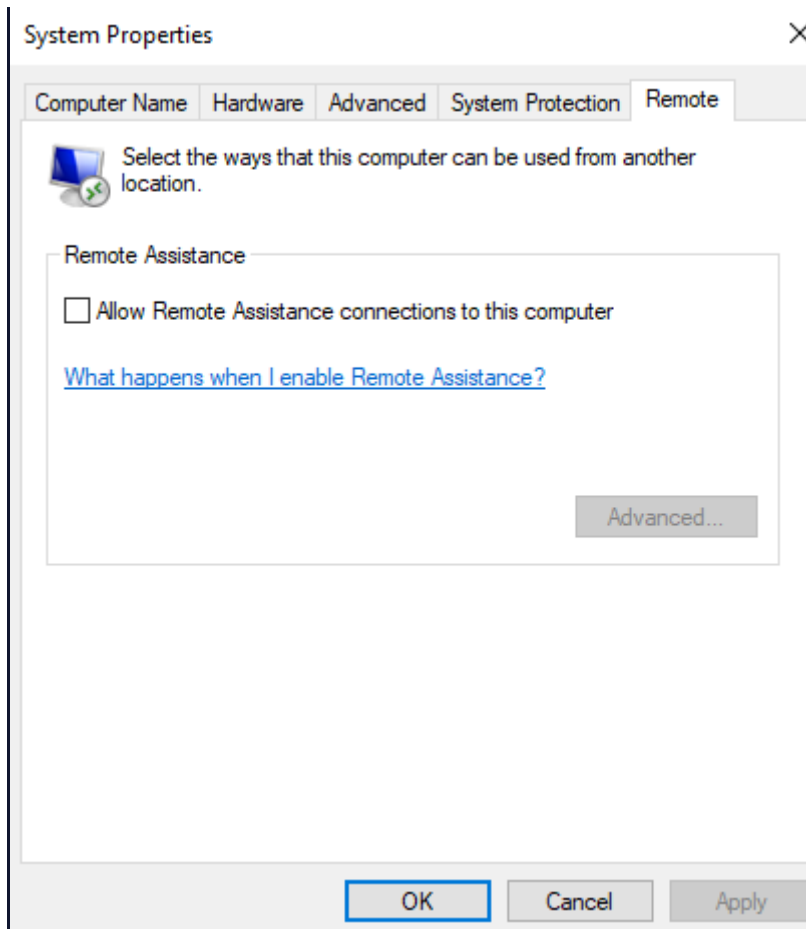Prevents others from tampering with important security features.

On

Miscellaneous Best Practices

Disable Remote Access

- Open the "Control Panel" app.
- Go to "System and Security" (You may need to change the view settings to "view by category").
- Go to "System".
- Go to "Remote settings"

- Under the "Remote" tab, uncheck the "Allow Remote Assistance connections to this computer" box.

System Properties ×

Computer Name | Hardware | Advanced | System Protection | Remote

Select the ways that this computer can be used from another location.

Remote Assistance

☐ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Advanced...

OK | Cancel | Apply

- Depending on your version of Windows, there may be another similar feature you need to disable:
- Open the "Settings" app.
- Go to "System".
- Go to "Remote Desktop".
- If your version of windows has the remote desktop feature, turn it off.

Allow Automatic Microsoft Software Updates

- Open the "Settings" app.
- Go to "Update & Security".
- Go to "Advanced Options".
- Turn "Receive updates for other Microsoft products when you update Windows" on.

Advanced Windows Hardening Techniques

Once you've completed the basics of hardening your OS, you may want to move on to more advanced hardening. These are methods that require additional resources and/or research. Some measures spend more computer resources, slowing down your system, or cause networking issues in certain environments. Always be sure to do your research on the benefits, drawbacks, and potential complications of a technique before choosing to apply it!

Uninstall Unused Programs

There's no point having programs that you don't use sitting around on your computer; at best, they take up space, and at worst they provide extra tools for attackers to make use of. It's good to scan through the list of programs in case any of them were downloaded accidentally. Be careful to distinguish from critical programs for the OS.

Encryption

- Some versions of Windows come with options for encrypting the hard drive, such as [Bitlocker](#).
- Self-encrypting drives are hard drives with built-in encryption.

Backups

- Some versions of Windows have the option of automatic backups using File History, and an extra hard drive.
- There are many cloud-based backup services available to consumers such as OneDrive and DropBox.
- Creating local backups using an external hard drive is also an option, and there are many ways to do it.

Add Extra Security Software

While Windows' built-in antivirus is usually adequate, it may not be enough in special situations, such as when securing a not so tech-savvy family member's computer. In these cases, it's worth it to invest in additional security software that offer a full suite of protection and features. Kaspersky and Bitdefender are two well-regarded names in consumer security software, but you can look at a variety of recent guides to determine what suite will meet your needs.

Additional Resources

- [InfoSec Institute has a general list](#) of Windows hardening techniques to look into.
- [Hacker Noon has a fantastic article](#) on windows 10 hardening, but many of the things covered in it are beyond what is required for the average individual.

Congratulations — you just took the first step towards improving the security of your computer's operating system!