LIFARS
your digital world, secured

Windows 10 Hardening-Non-Enterprise Environment

Windows 10 Hardening-Non-Enterprise Environment

A security guide on how to secure Windows 10 for non-enterprise environment. Hardening is performed using mostly native Windows tools and Microsoft tools. This documentation contains all the hardening steps which are necessary to make Windows 10 more secure.

Let Us Begin:

Windows recognizes the User who is sitting at the keyboard with a User Login. The owner can be defined with different categories of Logins, such as administrator, Standard user, child user or guest and give them different permissions to access.

Standard, Child and Guest User can be categorized under *Non-Privileged user.* A Non-Privileged User can be a Microsoft account, but with strong passphrase used as a PIN code. This user might also have rights to install apps from Windows store and bypass Firewall rules, hence be conscientious of such semi-admin.

The difference between Admin and Non Privileged user can also be understood as below:

'Under normal circumstances, non privileged users can change their own passwords, while the superuser can change any user's password. (Using enhanced security, it's also possible to deny users the ability to change their own passwords.)'

Windows 10 Machine Hardening is done separately for Admin Users and Non-Privileged Users, since the privileges are different. To start with the Process, follow the below defined steps with Path defined for:

User Feasibility:

- **Password Complexity**

  A strong Password is the most basic defense mechanism to adhere to, when securing your system from vulnerabilities. This can be done using the Built-in Local security policy. Keep a strong password. Enable, Password must meet complexity requirement and Store password using reverse encryption. Select the other settings to secure your system

  Path: Start (enter secpol.msc)-> Local security Policy->Account Policy -> Password Policy

- Disable all **Live Tiles** from your System.

  Path: Start Menu -> Type "gpedit.msc"-> Local Computer Policy > User Configuration > Administrative Templates > Start Menu and Taskbar > Notifications

- Turn **User Account Settings** to max from Control settings.

  Path: Control Panel->All Control Panel Items->User Accounts->Change User Account Control Settings.

- Uninstall unnecessary apps from Control settings.

  Path: Control Panel->Programs

Although Microsoft Defender is enough as an antivirus, yet protections need to be enabled. For better security, below settings needs to be assured on Windows Security

- ·Under **Virus and Threat Protection** settings, turn on all the settings except automatic sample submission.

  Path: Start > Settings > Update & Security >Windows Security -> Virus & threat protection ->Manage settings -> Controlled folder access -> Manage Controlled folder access-> Protected

- **Ransomware protection**

  Under Ransomware Protection (*Start -> Type Ransomware Protection*) turn on controlled access folders, adjust protected folders to reflect your habits

- **Firewall and network protection**

  Under Firewall and Network Protection settings (present under windows defender), turn on firewall for all profiles, set public profile as default

- **Update of OS**

  To make your Operating system bullet proof and minimize a computer's OS exposure to threats and to mitigate possible risks, keeping your operating system updated with latest build is a very basic measure.

  Path: Control Panel -> All control panel items ->Windows Update

Apps and Browser control

- **Update of Browsers**

  Keeping your browser up-to-date and installing the latest version acts like a defense mechanism and avoid any malicious code running on your system.

- **Update of Other applications**

  Microsoft provides regular updates to protect your system from various attacks. Apps on your system can be updated from below path:

  Path: Start screen-> Microsoft store-> Account Menu (upper right corner) -> update apps automatically ON

- Under **Check apps and Smartscreen** setting, select either Warn or Block
- Under **Isolated browsing** turn on Windows Defender Application Guard

  Note: This is incompatible with Vmware Workstation

- ·Under **Exploit protection** enable all features (in case of problems mandatory ASLR can be left in disable state – incompatible with VMware Workstation)

  In order to *Add program*: e.g browser. Settings for Chrome, Firefox and Opera can be found at section Configure Anti-Exploit technology from https://hardenwindows10forsecurity.com/

- · Enable **Data Execution Protection.** Refer the below path

  Path: (This PC->Properties->Advanced System Settings->Performance settings choose turn on DEP for all programs)

- Turn on **Memory Integrity** settings

  Path: Settings->Update & Security->Windows Security->Device Security->Core isolation->Memory integrity

  Note: Problem with VMware, hence VMware needs to be turned off

Networking

- **Protocol Settings**

  Path: Control Panel->Network and Sharing Center->Change Adapter Settings and disable unused protocols.

  Enable only Internet Protocol version 4 (TCP IPv4) and Disable IPv6.

- **Dword 32 bit**

  Path: HKLM->SYSTEM->CurrentControlSet->Services->TCPIP6->Parameters, create DWORD 32 bit entry DisabledComponents,

  Set value to 0xFF

- Disable **Remote Desktop Redirector Bus device**

  Path: Control Panel\Device Manager\System Devices\Remote Desktop Device Redirector Bus

- Disable **UPnP**

  Path: HKLM->Software->Microsoft->DirectplayNATHelp->DPNHUPnP, new DWORD UPnPMode, set value to 2

- Enable **Firewall logging**

  Path: Start->Windows Administrative Tools->Windows Firewall with Advanced Security->Windows Firewall Properties

  On each tab (domain, private, public) customize logging. Log successful and dropped connections, size limit 32767KB (max allowed)

- Disable **Automatic proxy setup**
  Path: Settings->Network and Internet->Proxy

Turn off ‘Automatically detect’ settings

Block Apps and Features:

Block the below apps and Features to make your system more secure.

- · **OSArmor**

  ○ Install OSArmor using the Link https://www.novirusthanks.org/products/osarmor/

  ○ Open Configurator, check everything on main and anti-exploit protections tab. Also Verify and block specific locations on advanced tab

- **Windows Apps sideloading**

  Path: Settings->Update and security->for developers-> choose Microsoft Store appsBlock Windows Apps sideloading

- Disable **Autoplay**

  Path: Settings->Devices->Autoplay turn off

- Disable **Autorun**

  Path: HKEY_Current_User ->Software ->Microsoft ->Windows ->CurrentVersion->policies ->Explorer->NoDriveTypeAutoRun.

  Change value of NoDriveTypeAutoRun to 0xFF

- · Disable **Remote assistance**

  Path: This PC ->Properties ->Advanced System Settings->Remote tab

  Disable remote assistance from the above path.

- **Internet Explorer 11**

  Path: Control Panel->Programs and Features->Turn Windows features on or off Uncheck Internet Explorer 11

  Apart from this, Disable all the other another unused services.

Logging

- **Log processes**

  Path: Gpedit.msc-> Local Computer Policy->Computer Configuration->Windows Settings->Security Settings->Local Policies->Audit Policy

  Verify the above path for Audit process tracking for success and failure

- **Log file size**

  Path: Event viewer->right click on logs->properties

  Select at least 204800 KB as Log file size

User Settings

- **File extensions**

  Path: Explorer->View check file name extensions

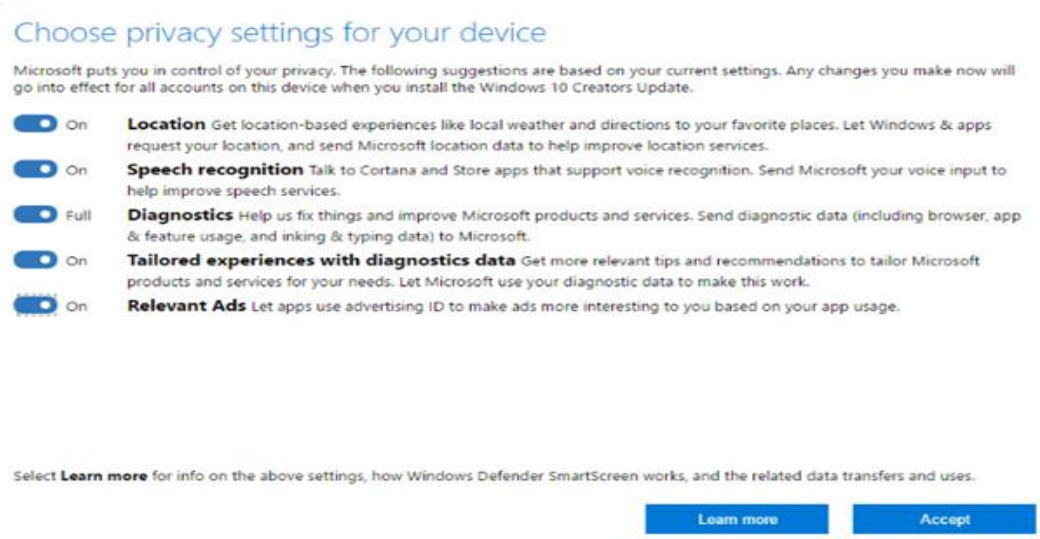
  Select Show File extensions

- **Lock screen**

  Path: Settings->Personalize->Lock Screen->Screen

  Select the Time out setting 5 or 10 minutes

Privacy



- ·Navigate to *Settings->Privacy review* and disable the features not required.

- **Encrypt disk**

  Encrypt your disk drive using Bitlocker, or preferably VeraCrypt full disk encryption

- **KeePass**

  KeePass can be used to manage passwords for Windows. It officially supports MacOS and Linux Operating System. It can be downloaded from link https://keepass.info/download.html

- **GnuPG with OutLook**

  Using Gnu Privacy Guard for Secure Mails in OutLook is a better option considering security of your system. This can be downloaded from https://www.gnupg.org/%28en%29/download/index.html

This basic hardening improves resiliency of Windows 10 for Home users with minimum amount of work to set it up with maximize the protection.