

This document is a Work-In-Progress and may contain errors, typo's, etc..
Please email shaun@copscorp.com.au with any corrections or to request any additions or changes

Reset Passwords

Windows

Method 1: Tools

Medicat

PC Unlocker

Method 2: Manual

Exploit Utilman.exe

- Hold **Shift** key + click **Restart**
Continue to hold shift until the screen goes black
Windows should reboot in to the **Recovery Environment**
- Click **Troubleshoot**
- Click **Advanced**
- Click **Command Prompt**
- Navigate to the System32 directory
`cd c:\windows\system32`
Depending on the number logical volumes the computer has connected at the time, the volume that contains the Windows directory may be mounted to a different drive letter, but it's usually mounted as C:

How to find the correct drive letter that contains the Windows directory
If **C:** does not contain the **Windows** directory, then you can repeat the following steps with different letters to locate which drive does:

- Run **D:**
 - Run `dir`
 - Check the output of `dir` for both the **Users** and **Windows** directories
- Backup Utility Manager
`copy utilman.exe utilman.exe.bak`
- Replace Utility Manager with Command Prompt
`copy cmd.exe utilman.exe`
- Reboot
`wpeutil reboot`

Create Temporary Local Admin Account

- Click the **Utility Manager** icon
Command Prompt should now open instead of the Utility Manager
- Enter the following commands:
`net user temp /add`
`net localgroup administrators temp /add`
`exit`

Reset User Password

- Sign in to the new **temp** user account
*If you don't see the **temp** user account, restart Windows and check again*
- Run **netplwiz**
- Select the target user account
- Click **Reset Password**
- Enter new password or leave empty for no password
- Click **OK**
- Sign Out

Remove Temporary Local Admin Account

- Sign in to an admin user account
not the temp user account
- Run **netplwiz**
- Select the **temp** user account
- Click **Remove**
- Click **Yes**
- Click **OK**

Restore Utilman.exe

- Hold **Shift** key + click **Restart**
Continue to hold shift until the screen goes black
Windows should reboot in to the **Recovery Environment**
- Click **Troubleshoot**
- Click **Advanced**
- Click **Command Prompt**
- Navigate to the System32 directory
`cd c:\windows\system32`
Depending on the number logical volumes the computer has connected at the time, the volume that contains the Windows directory may be mounted to a different drive letter, but it's usually mounted as C:

How to find the correct drive letter that contains the Windows directory
If **C:** does not contain the **Windows** directory, then you can repeat the following steps with different letters to locate which drive does:

- Run D:
 - Run `dir`
 - Check the output of `dir` for both the `Users` and `Windows` directories
- Restore Utility Manager


```
copy utilman.exe.bak utilman.exe
```

System Service

Windows

Software

- **Restart Windows**

Force Restart Windows now to provide a clean environment before proceeding

```
shutdown -r -f -t 00
```
- **System Restore**
 - Check System Restore configuration

Make sure System Restore is Enabled on C: and set the allocation to 7%
 - Create a new System Restore point


```
COPS - Pre System Service
```
- **Task Manager**
 - Disable unwanted startup items
- **Wintoys**
 - Install Wintoys


```
winget install wintoys
```

or

```
winget install 9P8LTPGCBZXD
```

or

```
ms-windows-store://pdp/?ProductId=9P8LTPGCBZXD
```
 - Performance Tab
 - Ultimate performance power plan

Turn ON if Desktop

Turn OFF if Laptop
 - HAGS (hardware-accelerated GPU scheduling) | Turn ON
 - VBS (virtualization-base security) | Turn ON
 - Startup apps | Disable unwanted startup items
 - Search indexing | Turn ON

- Delivery optimization | Turn ON
 - Network adapter onboard processor | Turn ON
- Health Tab
 - Fast startup | Turn ON
 - Drive optimization | Turn ON and run (click config icon and optimise each drive)
 - Storage sense | Turn ON and run (click config icon and click 'Run Storage Sense now')
 - Cleanup | Run 'Junk' + 'Microsoft Store' + 'DNS'
 - System updates | Set to 'Default'
 - App updates | Turn ON
 - Graphics driver | Click 'Restart'
 - Icons cache | Click 'Rebuild'
- Tweaks Tab
 - Desktop | Turn ON 'This PC' + 'Recycle Bin'
- Updates
 - Update Windows
old Windows 10 builds can use the Windows 10 Update Assistant to jump to the latest build
 - Update Apps via Winget
 - Update Apps via Microsoft Store
 - Update Office Apps
"C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RClient.exe"
/update user forceappshutdown=true
- Drivers
 - Update Drivers using SDIO
 - Verify Drivers using verifier
- System Maintenance/Repair
 - Open a Terminal as Administrator
Run wt or powershell or cmd
 - Run the following commands:
winget source reset --force
winget source update
winget upgrade --all --silent
sfc /scannow
dism /online /cleanup-image /startcomponentcleanup
/resetbase
dism /online /cleanup-image /restorehealth
sfc /scannow
defrag /c /o
chkdsk c: /r /scan /perf

- Disk Cleanup
 - Run `cleanmgr /sageset:10`
 - Click Clean up system files
 - Tick all checkboxes EXCEPT:
 - System error memory dump files
 - System error minidump files
 - Windows error reports and feedback diagnostics
 - User file history
 - Click OK
 - Run `cleanmgr /sagerun:10`
- Memory Diagnostics
 - Run Windows Memory Diagnostics
 - Click 'Restart now and check for problems (recommended)'
 - After Windows boots back up, check results:
 - Event Viewer - Windows Logs - System - Filter Current Log... - Event sources - Tick 'MemoryDiagnostics-Results' - Click OK
- Create a new System Restore point
 - COPS - Post System Service

Hardware

- Check all buttons and ports are free from debris and working functioning correctly
- Air compress out system as required
- Wipe down device and clean surfaces
- Add a Serviced by COPS sticker or replace old worn stickers as required

Data Transfer

Windows

Backup

Windows

- Restart Windows
 - Force Restart Windows now to provide a clean environment befor proceeding*
 - `shutdown -r -f -t 00`
- [OPTIONAL] Create a new System Restore point

Antivirus

- Disable the Antivirus
 - Some of our extraction tools prompt false positives in the majority of security software*

Transfer Drive

- Create a Job folder on the Transfer Drive *naming convention:*
Job#5000
 - Create a new folder with the current job number to save User Data to

User Profiles

- Copy `C:\Users\` folder to the Job folder on the Transfer Drive

Web Browsers

 For each installed web browser complete the following:

- **Export Bookmarks**
naming convention:
Web Browser - Google Chrome - Bookmarks - 2024-07-15.html
or
web-browser_google-chrome_bookmarks_2024-07-15.html
 - Google Chrome URL: `chrome://bookmarks`
 - Microsoft Edge URL: `edge://favorites`
 - AVG Secure Browser URL: `secure://bookmarks`
 - Mozilla Firefox Hotkey: `Ctrl+Shift+0`
 - Microsoft Internet Explorer: `%USERPROFILE%\Favorites`
- **Export Passwords**
naming convention:
Web Browser - Google Chrome - Passwords - 2024-07-15.csv
or
web-browser_google-chrome_passwords-2024-07-15.csv
 - Google Chrome URL: `chrome://password-manager` or `chrome://settings/passwords`
(older Chrome versions)
 - Microsoft Edge URL: `edge://wallet/passwords` or `edge://settings/passwords`
(older Edge versions)
 - AVG Secure Browser URL: `secure://password-manager` or
`secure://settings/passwords` (older Secure Browser versions)
 - Mozilla Firefox URL: `about:logins`
 - Microsoft Internet Explorer: use Nirsoft IE PassView
- **Sync Accounts**
Try to sync each browser with their relevant accounts if available
Manual exports of Bookmarks + Passwords is good, but syncing the entire browser is better

- Google Chrome: Google Account
 - `chrome://sync-internals`
 - Check Enabled: Sync Feature Enabled = true
 - Check Account: Username
 - Checked Synced: Last Synced = Just now
 - Check Not Actively Syncing: Sync Cycle Ongoing = false
 - Force Sync (if required): `chrome://extensions` - enable Developer mode - click Update
- Microsoft Edge: Microsoft Account
 - `edge://sync-internals`
 - Check Enabled: Sync Feature Enabled = true
 - Check Account: Username
 - Checked Synced: Last Synced = Just now
 - Check Not Actively Syncing: Sync Cycle Ongoing = false
 - Force Sync (if required): `edge://extensions` - enable Developer mode - click Update
- AVG Secure Browser: AVG Account
- Mozilla Firefox: Mozilla Account

Programs

- **Export Installed Programs List**
naming convention:
 Installed Programs - Nirsoft Uninstallview - 2024-07-15.html
 or
 installed-programs_nirsoft-uninstallview_2024-07-15.html
 - Use Nirsoft UninstallView, save all as Horizontal HTML
- **Export Winget**
naming convention:
 Winget - Export - 2024-07-15.json
 or
 winget_export_2024-07-15.json
 - Open a Terminal as Administrator
 Run `wt` or `powershell` or `cmd`

- Check Winget is installed `winget -v` (this will throw an error if winget is unavailable)
- Update Winget `winget source update`
- Export Winget's list of installed programs `winget export -o "REPLACE-WITH-TARGET-FILE"`
(*update REPLACE-WITH-TARGET-FILE with the target winget export file on the transfer drive*)
- Optionally export a list of all programs that Winget does cannot re-install at the same time with this extended command
`winget export -o "REPLACE-WITH-TARGET-FILE" > "winget_unavailable.txt"`
- [ALTERNATIVE] Create Winget Install Script using 3rd party site
winstall.app
winget.run

Licenses *naming convention:*

License Keys - Nirsoft Product Key Scanner - 2024-07-15.html

or

license-keys_nirsoft-product-key-scanner_2024-07-15.html - use Nirsoft Product Key Scanner or Nirsoft ProduKey, save all as Horizontal HTML

Emails / Calendars / Contacts

- Extract Passwords and Server Settings
 - Nirsoft Mail PassView
 - Nirsoft WinMailPassRec
 - Nirsoft PstPassword
- Backup any accounts set up as POP
 - *How to export emails to file in Outlook*
- Export Calendars
- Export Contacts

Drivers

- Export Drivers
naming convention:
TRANSFERDRIVE:\\Job#5000\Drivers - 2024-07-15\
or
TRANSFERDRIVER:\\Job#5000\drivers_2024-07-15\
- Open PowerShell as an Administrator and run the following script:
`Export-WindowsDriver -Online -Destination "REPLACE-WITH-TARGET-FOLDER"`
update REPLACE-WITH-TARGET-FOLDER with the target drivers folder on the transfer drive

Other

- Check C: Drive for unusual files/folders to transfer
copy to Job folder copying the C: Drive file structure (Transfer-Drive:\Job#5000\C\FolderToSave)

Prepare New Device (*if required*)

- **Create a Local Account during Windows 10/11 Out of Box Experience (OOBE)**
 - **Option 1: No Internet Connected**
Bypass Network Registration
 - *Open Command Prompt: Shift+F10 (may require pressing Fn on some devices)*
 - *Run command: OOBE\BYPASSNRO (this will restart the OOBE if successful)*
 - *Proceed through OOBE like normal until you get to the Network Selection screen*
 - *Select I don't have an internet connection (if this button is not available the bypass didn't work, proceed to Option 2)*
 - *Select Continue with limited setup*
 - *Create a Local Account: COPS (no password)*
 - *Complete the OOBE as normal*
 - **Option 2: Internet Connected**
Force Local Account Creation
 - *Proceed though OOBE like normal until you get to the Login with a Microsoft Account screen*
 - *Open Command Prompt: Shift+F10 (may require pressing Fn on some devices)*
 - *Run command: start ms-cxh:localonly*
 - *Create a Local Account: COPS (no password)*
 - *Complete the OOBE as normal*
- Note regarding Windows 10/11 S Mode
In some cases you won't be able to open the Command Prompt, you may only see it's black box flash up on the screen and quickly disappear. This is could be a indication of the Windows 10/11 install being in S Mode (Store Mode), which disables access to terminals

(i.e. Command Prompt) and execution of non Microsoft Store apps. If you encounter this, you will not be able create a Local Account during the OOBE, and you will need to complete the OOBE with the customer's Microsoft Account. After the OOBE is complete and you've reached the Windows Desktop environment, you may need to Switch Out of S Mode to proceed with the Data Transfer, as S Mode restricts us from running our tools if required.

- [OPTIONAL] Switch Out of S Mode
WARNING: SWITCHING OUT OF S MODE IS A PERMANENT CHANGE AND CANNOT BE REVERTED

- *Connect to the internet*

- *Run `ms-windows-store://pdp/?productid=BF712690PMLF&OCID=windowssmodesupportp`*

- *Follow the prompts to Switch Out of S Mode
(this will change the Windows edition installed to Windows 10/11 Home or Pro as per it's installed license)*

- **Configure System Restore**

- **Check installed Windows' Edition**

- *Run `winver`*

- **Create a new System Restore point**

COPS - Fresh Windows 10/11 Home/Pro Install (use 10 or 11 and Home or Pro as per winver)

- **Connect to the Internet** (if not already)

- **Check Windows is activated**

TODO: `ms-settings:activation` or `ms-settings:activation?activationSource=SMC-Article-12440`

- **Configure Time/Date**

- **Configure Windows Update**

- Open Windows Update

Run control update

- Click Resume updates if updates are currently paused

- Disable Get the latest updates as soon as they're available

- Advanced options

- Enable Receive update for other Microsoft products

- Disable Get me up to date

- Enable Notify me when a restart is required to finish updating

- Delivery Optimization

- Enable Allow downloads from other devices

- Select Devices on my local network

- **Update Microsoft Store Apps**

- Open Microsoft Store

- Run `ms-windows-store`:
 - Click Downloads
 - Click Check for updates
 - Click Update all
- **Update Winget Apps**
 - Open a Terminal
 - Run `wt` or `powershell` or `cmd`
 - Run the following commands:


```
winget source update
winget upgrade --all --silent
```
- **Update Windows**

```
control update
```
- **Update Office apps**
 - Run `"C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RClient.exe" /update user forceappshutdown=true`
- **Check Drivers**

Bangs(!) exclamation marks in Device Manager indicates missing, incorrect, or corrupt drivers

 - Open Device Manager to check for Bangs(!)
 - Run Snappy Driver Installer Origin (SDIO) as an Administrator
 - Select TODO: Create a new system restore point
 - Select all missing/incorrect/corrupt drivers (as per bangs! in Device Manager)
 - Click Install
- **[OPTIONAL] Update Outdated Drivers**
- **Verify Drivers**
 - **Turn On Windows Verifier:**
 - Run verifier
 - Select Create standard settings
 - Click Next
 - Select ☐ Automatically select all drivers on this computer
 - Click Finish
 - Restart Windows shutdown `-r -f -t 00`
 - *Windows Verifier works by stressing out drivers as they're loaded (it is expected that the computer's performance will be impacted while verifier is enabled)*
 - *If Windows loads into the desktop OK and does not crash with Verifier enabled, then all is good and you can proceed to turn it off*

- *If Verifier induces a crash, Windows should produce a Blue Screen of Death (BSOD) with a STOP Code error and information on the driver that crashed, you can use this information to identify the faulty driver that caused the crash and replace it*
- **Turn Off Windows Verifier:**
 - Run verifier
 - Select Delete existing settings
 - Click Finish
 - Restart Windows shutdown -r -f -t 00

Restore

- **Install Programs**
 - you can use the winget install script for this if you made one - *install programs before restoring the user profile, as otherwise some required registry entries may not exist yet*
- **Restore User Profiles**
 - make Administrator, make default user, set no password and set password does NOT expire
- **Copy over any C: Drive files/folders that were backed up**
- **Restart Windows** (this should log in to the restored user profile)
 - open a command prompt window (or similar) as Administrator to ensure account has admin privileges
- **Install Printer Drivers**
 - If you can not install the printer drivers + software without the printer present, save the printer package installer to C:\COPS\ and create a shortcut to it on the customer's desktop
- **Check Web Browsers and restore Bookmarks and Passwords from backups as required**
- **Activate software using extracted keys or accounts as required**
- **Configure email accounts as required**
- **Install additional drivers as required**
- **Move any USB Dongles from the old device (Wireless mice, wifi, blue adapters, etc...)**
- **Update Apps**
 - via Microsoft Store
 - via Winget
- **Update Windows**
- **Update Office apps** (if installed)
- **Restart Windows**
- **Remove 'COPS' user account**
 - Run netplwiz - Select COPS - Click Remove
 - Delete C:\Users\COPS\ folder

Windows may prevent you from removing this folder if it's currently accessing it in the background, if this happens just restart Windows

and try to remove it again

- Empty Recycle Bin
- **System Maintenance/Repair**

- Open a Terminal as Administrator
Run `wt` or `powershell` or `cmd`
- Run the following commands:
`winget source reset --force`
`winget source update`
`winget upgrade --all --silent`
`sfc /scannow`
`dism /online /cleanup-image /startcomponentcleanup`
`/resetbase`
`dism /online /cleanup-image /restorehealth`
`sfc /scannow`
`defrag /c /o`
`chkdsk c: /r /scan /perf`

Useful Tip

You can queue up multiple commands in PowerShell by pressing **Shift+Enter** to add a new line before pressing **Enter** to execute the all of the queued up commands one after another

- **Restart Windows**
- **Create a new System Restore point** COPS - Completed Data Transfer

Virus/Malware Removal

Windows

Pre Scans

- [**IMPORTANT**] **Air Gap Device**
Ensure device is disconnected from all networks before RKill is run successfully and RATs (Remote Access Tools) removed, to ensure malicious actors do not re-connect to the device while it's still compromised
- Enable System Restore (set to 7% allocation if enough free disk space)
- [**OPTIONAL**] **Create a new System Restore point**
COPS - Pre Virus/Malware Removal
This System Restore point will be wiped out in a later step (post-virus/malware removal), as malware can persist in old System Restore points
- **Restart Windows**
Force Restart Windows now to provide a clean environment before proceeding
`shutdown -r -f -t 00`

- **COPS Folder**
Create C:\COPS\ folder on the system
 - [OPTIONAL] Add C:\COPS\ to the installed antivirus's exclusion list
 - Trend Micro
 - Windows Security
- **Disable Antivirus**
 - Trend Micro
 - Windows Security
- **RKill**
 - Copy RKill folder from your USB Tool to the COPS folder
RKill can't run from a write-blocked drive, so you'll usually need to copy the executables out first
 - [**IMPORTANT**] Run any RKill executable as Administrator
 - Wait for RKill to complete, it will then generate a report RKill.txt on the current user's desktop
 - Move RKill.txt from %USERPROFILE%\Desktop to COPS folder
- **Revo Uninstaller**
- **Disk Cleanup**
 - Run `cleanmgr /sageset:10`
This will open the Disk Cleanup utility to create settings for Profile 10
 - Click **Clean up system files**
 - Select all checkboxes except for the following system error options:
System error memory dump files
System error minidump files

Useful Tip
You can click on an option, and then use the UP + DOWN arrows + Space Bar to quickly check or uncheck options

 - Click OK
 - Run `cleanmgr /sagerun:10`
This will run the Disk Cleanup utility to using Profile 10's settings

Scans

- Connect to Internet
- [OPTIONAL] AdwCleaner
AdwCleaner crashes out of UVK's automation, so run it now instead if you want to use it
- [OPTIONAL] Spybot - Search & Destroy
Spybot is a thorough malware removal tool, but it can take a very long time to complete it's scans
- [OPTIONAL] Windows Defender Offline Scan

- [OPTIONAL] Create a new System Restore point COPS - Pre Virus/Malware Removal
 - Ultra Virus Killer (UVK)
 - Install UVK
 - Open UVK
 - Do not disable Hybrid Shutdown if asked when opening UVK
 - Do Update UVK if asked when opening UVK
 - Click System Repair
 - Select the following repair actions: (*left menu*)
- Useful Tip
 You can click on an option, and then use the UP + DOWN arrows + Space Bar to quickly check or uncheck options
- **Pre-Repair Actions**
 - 1. Set technician power settings
 - 2. Kill all non system processes
 - 3. Delete all restore points
 - 4. Create a system restore point
 - 5. Free physical memory
 - 6. Backup the registry
 - 7. Un-immunize all areas
 - 8. Disable the User Account Control
 - 9. Enable the legacy (F8) boot menu
 - 10. Enable Windows Recovery Environment
 - 11. Prevent rebooting until all is done
 - **Third-Party Built-in Apps**
 - 12. Ultra Adware Killer scan
 - 13. MalwareBytes AntiMalware scan
 - 14. Super AntiSpyware scan
 - 15. RogueKiller scan
 - 16. Kaspersky TDSSKiller scan
 - 17. Avast! Browser Cleanup
 - **Reset Actions**
 - 18. Reset the DNS cache
 - 19. Reset the Windows Store
 - 20. Reset all print jobs
 - **Fixes for Common Windows Problems** *n/a*
 - **File System Related Actions**
 - 21. Rebuild icon cache
 - **Essential Installes/Updates**
 - [If Google Chrome is installed]
 - 22. Insall/Update Chrome
 - 23. Install uBlock Origin for Chrome
 - [If Mozilla Firefox is installed]
 - 24. Install/Update Firefox
 - 25. Install uBlock Origin for Firefox
 - 26. Install uBlock Origin for Edge
 - 27. PatchMyPC - Update all apps
 - **Privacy Cleanup**
 - 28. Clear all browsers history (all users)
 - 29. Delete browsers cookies (all users)
 - **Maintenance Actions**
 - 30. Empty all users temp folders
 - 31. Empty browsers cache (all users)
 - 32. Unattended disk cleanup
 - **System Repair and Optimization** *n/a*
 - **Windows Troubleshooters** *n/a*
 - **Post-Repair Actions**
 - 33. Restore the previous UAC state
 - 34. Restore previous immunization
 - 35. Delete all restore points (post repair)
 - 36. Create restore point (post repair)
 - 37. Reset power settings
 - 38. Uninstall Malwarebytes Antimalware
 - 39. Uninstall Super AntiSpyware
 - 40. Uninstall RogueKiller
 - 41. Uninstall this application
 - 42. Restore normal boot
 - Select the following loadout settings: (*right menu*)
 - 1. Third party

- full scans 2. Use unattended mode
- Click Run selected fixes/apps

Post Scans

- [OPTIONAL] Create a new System Restore point COPS - Pre Windows Update
- Update Windows (no preview updates)
- Update Apps via Microsoft Store
- Update Apps via Windows Package Manager (winget)
winget source update
winget upgrade --all --silent

Useful Tip

You can queue up multiple commands in PowerShell by pressing **Shift+Enter** to add a new line before pressing **Enter** to execute the all of the queued up commands one after another

- [OPTIONAL] Create a new System Restore point COPS - Pre Driver Update
- Update Drivers (SDIO)
- Verify Drivers
 - **Turn On Windows Verifier:**
 - Run verifier
 - Select Create standard settings
 - Click Next
 - Select Automatically select all drivers on this computer
 - Click Finish
 - Restart Windows (shutdown -r -f -t 00)
Windows Verifier works by stressing out drivers as they're loaded (it is expected that the computer's performance will be impacted while verifier is enabled)
If Windows loads into the desktop OK and does not crash with verifier enabled, then all is good and you can proceed to turn it off
 - **Turn Off Windows Verifier:**
 - Run verifier
 - Select Delete existing settings
 - Click Finish
 - Restart Windows
shutdown -r -f -t 00
- **System Maintenance/Repair**
 - Open a Terminal as Administrator
Run wt or powershell or cmd
 - Run the following commands:


```

winget source reset --force
winget source update
winget upgrade --all --silent
sfc /scannow
dism /online /cleanup-image /startcomponentcleanup
/resetbase
dism /online /cleanup-image /restorehealth
sfc /scannow
defrag /c /o
chkdsk c: /r /scan /perf

```

Useful Tip

You can queue up multiple commands in PowerShell by pressing **Shift+Enter** to add a new line before pressing **Enter** to execute the all of the queued up commands one after another

- Create a new System Restore point COPS - Post Virus/Malware Removal

Android

Pre Scans

- **Remove Intrusive Full-Screen Pop-Ups**

These relentless pop-ups make the device impossible to work with, so deal with these first (*if applicable*)

More Info

These full screen pop-ups/ads aren't a sign of an injection, but merely a malicious use of the native Android notification system.

Users don't intentionally give these apps permission to do this, but it's often caused by Tapjacking or simply users ignorantly agreeing to permission prompts.

- Open Play Store
 - Install Ad Virus Cleaner - ROX Security
- Open ROX Security
 - Tap Scan
 - Wait for the scan to complete
 - Tap on Pop-up Ad Detector
 - Tap on Give Permissions

This will open a required permissions settings panel

 - Enable ROX Security
 - Tap < (*back button*)
 - Wait for an intrusive full-screen pop-up
 - Tap ||| (*app switch button*)

- Switch back to Rox Security Rox Security should have logged recent app activity under it's Pop-up Ad Detector
- Tap : *(kebab button)* next to the offending app
 - Tap Show in Play Store
 - Verify the app is not important
If the app is published by Google or the device's manufacturer (i.e. Samsung) think twice before removing
 - Tap Uninstall
- Uninstall ROX Security when done
- **Safe Mode**
Reboot the device in Safe-Mode *(if available)*
- **Malicious or Suspicious Apps**
 - Remove any remote access apps *(i.e. AnyDesk, TeamViewer, etc..)*
These are used by scammers to access devices remotely
 - Remove any malicious or bloatware apps
The following are common types of apps that are unnecessary often load their own malware
 - Any free 3rd-party "Cleaner" apps
 - Any free 3rd-party "QR Scanner" apps
 - Any free 3rd-party "PDF Reader" apps *(excluding Adobe Acrobat Reader)*
 - Any free 3rd-party "File Manager" apps
 - Remove any "Crypto" apps *(after verifying the customer does not genuinely use them)*
Scammers often load on crypto apps to try and steal currencies the device has access to
- **Web Browsers**
Clear Cache + Data for all Web Browsers installed on the device.
The following steps are for Google Chrome, but other apps are managed that same way
 - Open Settings
 - Tap Apps
 - Tap Chrome
 - Tap Storage
 - Tap Clear cache
 - Tap Clear data

1st Party Scans

- Play Protect Scan
- [If Samsung Device]
 - Samsung Device Care Scan

3rd Party Scans

- Install and Run at least 3 of the following free malware scanners:
 - Malwarebytes Mobile Security
 - AVG AntiVirus & Security
 - Bitdefender Antivirus
 - Sophos Intercept X for Mobile
 - Avira Security Antivirus & VPN
 - Trend Micro Mobile Security & Antivirus
 - ESET Mobile Security Antivirus
 - TotalAV Mobile Security *untested if can be used without an account*
 - Panda Dome Antivirus and VPN *untested if can be used without an account*
 - Avast Antivirus & Security *untested if can be used without an account*

Updates

- Update Apps via **Play Store**
- [If Samsung Device]
 - Update Apps via **Galaxy Store**
- Update **Android OS**
This may take multiple updates and reboots, as customers often neglect updating their devices

Backup / Export

Windows

macOS

Backup Device

- Use Time Machine

iOS

Export Messages

- imessage-exporter

Export Photos

- Connect the iOS device to a macOS device
You may need to unlock the iOS device and tap **Trust** if prompted
- Open **Image Capture** app
- Click on the iOS device
The connected iOS device should show up under **DEVICES** on the left
- Change **Import To:** folder
Make a Job# folder to import the photos/videos to
- Click **Download All**

Backup iCloud Photos

- Submit Apple Privacy Data Request
 - Sign in Apple's Data and Privacy page with the customer's Apple Account
 - Click Request a copy of your data
 - Tick iCloud Photos
 - Click Continue
 - Choose the largest bundle/zip size (*this will make downloading the files easier, as you can only download 3 of the part files at a time*)
- Check confirmation email
Apple will send a confirmation email to the customer's Apple Account email address, if this does not come through now then you may have issues receiving the download link email later
- Wait for the download link email
Apple will have to compile and zip up all of the data you requested, this can take many days
- Open download link
- Download all .zip files Apple prepared for download
- Unzip all .zip files
- Combine the unzipped data in to one folder

Android

OS Install Media Creation

Windows

Download

- Download from massgrave.dev

Verify

- Verify checksums against [rg-adguard.net](https://github.com/0x00adguard)

Flash

- Flash image to USB using Rufus
`winget install rufus.rufus`

Inject Drivers

- **Prep**
 - Have a folder with extracted drivers ready to go
`C:\drivers\` for this example
 - Create an empty directory ready to mount the Windows image to for editing
`C:\mount\` for this example
 - Have a Windows image ready to go
`F:\sources\install.wim` for this example
- **Mount**
 - Open Powershell as admin
 - Find index of the Windows image you want to mount
`Get-WindowsImage -ImagePath F:\sources\install.wim`
 - Mount the Windows image
`Mount-WindowsImage -Path C:\mount\ -ImagePath F:\sources\install.wim -Index 1`
- **Add Drivers**
 - `Add-WindowsDriver -Path C:\mount\ -Driver C:\drivers\ -Recurse -ForceUnsigned`
- **Unmount**
 - `Dismount-WindowsImage -Path C:\mount\ -Save`

Sideload

Android

Download

- Download desired .APK from 3rd party source or directly from the Google Play store using Aurora Store
- [If you can only download an App Bundle (.APKS, .XAPK, .APKM)]
 - Use AntiSplit M to merge the bundle components back in to a .APK file

Upload

- Connect the Android device to a computer
- Navigate to it's mounted file system (*i.e. in **This PC***)
- Open **Downloads** folder
- Copy **.APK** file in to the **Downloads** folder

Install

- Enable Sideloading
Depending on the manufacturer of the device, you may need to enable Sideloading before you can install .APK files
Samsung
- Open **Files** app
- Navigate to **Downloads** folder
- Tap on the **.APK** file
- Tap **Install**

USB Tool

Ventoy

Medicat

Bootable Tools

Windows Tools

COPS Extras (scripts, etc..)

Reference

Apps

Windows

App	Install	Description	Use Case
7-Zip			
AMD Adrenalin			
AltSnap			
Apple Devices	<code>winget install "Apple Devices"</code>		

App	Install	Description	Use Case
Apple iTunes	<code>winget install Apple.iTunes</code>		DEPRECATE- DUse Apple Devices instead
Audacity			
balenaEtcher			
BandiView			
BandiZip			
Bitwarden			
Chocolatey	<code>winget install Chocolatey.Chocolatey</code>		DEPRECATE- DUse Winget instead
Cinebench	<code>winget install Maxon.CinebenchR23</code>		
Clear Disk Info	<code>winget install Carifred.ClearDiskInfo</code>		
CPUID CPU-Z	<code>winget install CPUID.CPU-Z</code>		
CPUID	<code>winget install CPUID.HWMonitor</code>		
HWMonitor			
CrystalDiskInfo	<code>winget install CrystalDewWorld.CrystalDiskInfo</code>		DEPRECATE- DUse Clear Disk Info instead
CrystalDiskMark	<code>winget install CrystalDewWorld.CrystalDiskMark</code>		
DaVinci Resolve			
Disk Drill	<code>winget install CleverFiles.DiskDrill</code>		
Display Driver Uninstaller (DDU)	<code>winget install Wagnardsoft.DisplayDriverUninstaller</code>		
DropBox			
eM Client	<code>winget install eMClient.eMClient</code>		
Exact Audio Copy (EAC)			
Everything			
FFmpeg			
FileBot			
FileZilla			
ForensiT	<code>winget install ForensiT.Transwiz</code>		DEPRECATED- Copy %USERPROFILE% instead
Transwiz			

App	Install	Description	Use Case
Furmark	winget install Geeks3D.FurMark.2		
Gimp	winget install GIMP.GIMP.3		
Git	winget install Git.Git		
GitHub Desktop	winget install GitHub.GitHubDesktop		
Google Chrome	winget install Google.Chrome		
Google Drive	winget install Google.GoogleDrive		
GPU-Z	winget install TechPowerUp.GPU-Z		
HandBrake	winget install HandBrake.HandBrake		
HashCheck Shell Extension	winget install idrassi.HashCheckShellExtension		
HD Tune Pro	winget install EFDSOFTWARE.HDTunePro	HDD / SSD Priority	Benchmark drive speed over time with graph
HexChat	winget install HexChat.HexChat		
HWiNFO	winget install REALiX.HWiNFO		
iMazing	winget install DigiDNA.iMazing		
iMazing Converter	winget install DigiDNA.iMazingHEICConverter		
ImgBurn	winget install LIGHTNINGUK.ImgBurn		
Inkscape	winget install Inkscape.Inkscape		
Intel HD Graphics			
Intel PresentMon	winget install Intel.PresentMon.beta		
iPerf	winget install ar51an.iPerf3	Measuring TCP, UDP and SCTP bandwidth performance	Test network throughput
JDownloader	winget install AppWork.JDownloader		

App	Install	Description	Use Case
Libre Office	<code>winget install</code> <code>TheDocumentFoundation.LibreOffice</code>		
MASMicrosoft Activation Scripts	<code>irm</code> <code>https://get.activa</code> <code> iex</code>	Open-source Windows and Office activator	Change Windows Editions
MediaInfo	<code>winget install</code> <code>MediaArea.MediaInfo.GUI</code>		
MakeMKV	<code>winget install</code> <code>GuinpinSoft.MakeMKV</code>		
Microsoft Office	<code>winget install</code> <code>Microsoft.Office</code>		
Microsoft OneDrive			
Microsoft PC Health Check	<code>winget install</code> <code>Microsoft.WindowsPCHealthCheck</code>		
Microsoft PowerToys			
Microsoft Visual Studio Code	<code>winget install</code> <code>Microsoft.VisualStudioCode</code>		
Microsoft Windows Terminal	<code>winget install</code> <code>Microsoft.WindowsTerminal</code>		
Microsoft Verifier			
MiniTool	<code>winget install</code>		
Partition Wizard	<code>MiniTool.PartitionWizard.Free</code>		
Mozilla Firefox	<code>winget install</code> <code>Mozilla.Firefox</code>		
Mozilla Thunderbird	<code>winget install</code> <code>Mozilla.Thunderbird</code>		
NirSoft	<code>winget install</code>		
BlueScreenView	<code>NirSoft.BlueScreenView</code>		
NirSoft Product Key Scanner			
NirSoft ProduKey			
Nvidia App			
NVIDIA GeForce Experience			DEPRECATE- DUse NVIDIA App instead
OpenOffice			
Papa's Best STL Viewer			
Proton VPN			
qBittorrent			

App	Install	Description	Use Case
Raspberry Pi Imager			
ReNamer			
RevoUninstaller	<code>winget install RevoUninstaller.RevoUninstaller</code>		
Rufus	<code>winget install Rufus.Rufus</code>		
SD Card Formatter			
Scoop			DEPRECATE- DUse Winget instead
Snappy Driver Installer (SDI)	<code>winget install samlab-ws.SnappyDriverInstaller</code>		DEPRECATE- DUse Snappy Driver Installer Origin (SDIO) instead
Snappy Driver Installer Origin (SDIO)	<code>winget install GlennDelahoy.SnappyDriverInstallerOrigin</code>		
Sublime Text	<code>winget install SublimeHQ.SublimeText.4</code>		
TeamViewer	<code>winget install TeamViewer.TeamViewer</code>		
Trend Micro Internet Security	<code>winget install "Trend Micro Internet Security"</code>		
Trend Micro Maximum Security	<code>winget install "Trend Micro Maximum Security"</code>		
UltraViewer	<code>winget install DucFabulous.UltraViewer</code>		
Ultra Virus Killer (UVK)			
UniGetUI <i>formerly WingetUI</i>	<code>winget install MartiCliment.UniGetUI</code>	A GUI for the common CLI package managers for Windows	

App	Install	Description	Use Case
uTorrent			DEPRECATE- DUse qBittorrent instead
VLC Media Player	<code>winget install VideoLAN.VLC</code>		
Win32 Disk Imager	<code>winget install Win32diskimager.win32diskimager</code>		
WinDirStat	<code>winget install WinDirStat.WinDirStat</code>		DEPRECATE- DUse WizTree instead
Winget	<code>irm asheroto.com/winget iex</code>		
WinRAR	<code>winget install RARLab.WinRAR</code>		
WizTree	<code>winget install AntibodySoftware.WizTree</code>		
yt-dlp	<code>winget install yt-dlp.yt-dlp</code>		

macOS

App	Install	Description	Use Case
Apple Image Capture		Download photos/videos from digital cameras or iOS devices	Useful for backing up photos/videos from iOS devices, even if their iCloud account isn't working, as it treats the iOS device like a digital camera and simply imports the local copies on the device
Microsoft Remote Desktop			DEPRECATE- DUse Microsoft Windows App instead
Microsoft Windows App			

App	Install	Description	Use Case
Raycast	<code>brew install</code> <code>--cask raycast</code>		
Rectangle	<code>brew install</code> <code>--cask</code> <code>rectangle</code>		
yabai	<code>brew install</code> <code>koekeishiya/formulae/yabai</code>		
AeroSpace	<code>brew install</code> <code>--cask</code> <code>nikitabobko/tap/aerospace</code>		
FlashSpace	<code>brew install</code> <code>flashspace</code>		
Spectacle			DEPRECATE- DUse Rectangle instead
Alfred			DEPRECATE- DUse Raycast instead

iOS

Android

App	Description	Use Case
Appwatch	Snitch on app activity	DEPRECATEDUse Rox Security instead
Aurora Store	Alternative Google Play Store app	Install apps from the Play Store repository without needing to log in with a Google Account, and can download .APKs from the Play Store for later sideloading
Rox Security	Multi-tool for identifying unusual/unwanted app behaviour, including snitching on app activity	Identify apps that are responsible for intrusive full-screen pop-ups

Commands

Windows

Command	Description	Use Case
\	Opens %SYSTEMDRIVE% folder	Quick access to C:\
appwiz.cpl	Opens Programs and Features control panel window	
calc	Opens Calculator app	
charmap	Opens Character Map app	
chrome	Opens Google Chrome app <i>(if installed)</i>	
cmd	Opens Command Prompt app <i>(if installed)</i>	
code	Opens Visual Studio Code app	
compmgmt.msc	Opens Computer Management snap in	
control	Opens Control Panel	
control folders	Opens File Explorer Options window	
control keyboard	Opens Keyboard Properties window	
control printers	Opens Bluetooth & devices settings window	Quick access to Printers & scanners
control update	Opens Windows Update settings window	
desk.cpl	Opens Display settings window	Quick access to Resolution + Multi-Monitor settings
devmgmt.msc	Opens Device Manager snap in	Check Drivers
diskmgmt.msc	Opens Disk Management snap in	Check connected drives
diskpart	Opens Microsoft DiskPart command line interface	
documents	Opens current user's Documents folder	
downloads	Opens current user's Downloads folder	
dxdiag	Opens DirectX Diagnostic Tool app	

Command	Description	Use Case
eventvwr.msc	Opens Event Viewer snap in	
explorer	Opens Windows Explorer	
firefox	Opens Mozilla Firefox app (<i>if installed</i>)	
firewall.cpl	Opens Windows Defender Firewall control panel window	
fonts	Opens Fonts folder	
gpedit.msc	Opens Local Group Policy Editor snap in	
iexplore	Opens Internet Explorer app	
inetcpl.cpl	Opens Internet Properties window	Quick access to Proxy server settings
joy.cpl	Opens Game Controllers window	Use to test game controller inputs
lusrmgr.msc	Opens Local Users and Groups snap in	Powerful control over User Accounts and Groups, but does not work on Windows Home editions
main.cpl	Opens Mouse Properties window	
manage-bde c: -off	Run in a terminal to decrypt and disable BitLocker on C: drive	
manage-bde -status	Run in a terminal to show BitLocker status of all drives	
mdsched	Opens Windows Memory Diagnostic app	
mmc	Opens empty Microsoft Management Console snap in	
mmsys.cpl	Opens Sound window	
mrt	Opens Microsoft Windows Malicious Software Removal Tool app	

Command	Description	Use Case
msconfig	Opens System Configuration window	Quick access to Safe boot or Windows boot entries
msedge	Opens Microsoft Edge app	
msinfo32	Opens System Information	
mstsc	Opens Remote Desktop Connection app	Less powerful control over User Accounts, but does work on Windows Home editions
ms-windows-store:	Opens Microsoft Store app	
ncpa.cpl	Opens Network Connections control panel window	
netplwiz	Opens User Accounts window	
notepad	Opens Notepad app	
onedrive	Opens current user's OneDrive folder	
osk	Opens On-Screen Keyboard	
pictures	Opens current user's Pictures folder	
powercfg.cpl	Opens Power Options control panel window	
powershell	Opens Powershell app	
regedit	Opens Registry Editor app	Useful for creating shortcuts to Microsoft Store apps
resmon	Opens Resource Monitor app	
services.msc	Opens Services snap in	
shell:appsfolder	Opens Applications folder	
shell:mycomputerfolder	Opens This PC folder	
shell:recyclebinfolder	Opens Recycle Bin folder	
shell:startup	Opens Startup folder	
shutdown /h	Hibernate computer	
shutdown /l	Log off	
shutdown /r /fw /t 00	Restart Windows and boot in to BIOS / UEFI	
Run as Administrator		

Command	Description	Use Case
<code>shutdown /r /o /t 00</code>	Restart Windows and boot in to Recovery Environment	
<code>shutdown /r /f /t 00</code>	Force Restarts Windows immediately	
<code>shutdown /s /f /t 00</code>	Force Shuts down Windows immediately	
<code>snippingtool</code>	Opens Snipping Tool app	
<code>sysdm.cpl</code>	Opens System Properties window	Quick access to System Restore
<code>taskmgr</code>	Opens Task Manager app	
<code>taskschd.msc</code>	Opens Task Scheduler snap in	
<code>timedate.cpl</code>	Opens Date and Time window	
<code>verifier</code>	Opens Driver Verifier Manager app	
<code>videos</code>	Opens current user's Videos folder	
<code>vlc</code>	Opens VLC Media Player app (<i>if installed</i>)	
<code>winver</code>	Opens About Windows window	Quick way to check installed Windows edition (<i>Home/Pro/Enterprise</i>), version, and build
<code>wt</code>	Opens Windows Terminal app	
<code>%APPDATA%</code>	Opens current user's AppData\Roaming folder	
<code>%LOCALAPPDATA%</code>	Opens current user's AppData\Local folder	
<code>%SYSTEMDRIVE%</code>	Opens the root folder of the system drive	
<code>%TEMP%</code>	Opens current user's Temp folder	
<code>%USERPROFILE%</code>	Opens current user's profile folder	
<code>%WINDIR%</code>	Opens Windows folder	

Hotkeys

Windows

Resources

Hardware

iFixIt - Electronics Skills	Learn general device repair and electronics skills
iFixIt - Repair Guides	Repository of repair guides for specific devices
Repair Wiki	Guides for troubleshooting more specific or niche device issues
Keyboard Checker	Keyboard tester
HardwareTester - Midi Tester	Test MIDI input devices
HardwareTester - Gamepad Tester	Test Gamepads / Controllers
HardwareTester - Microphone Tester	Test Microphones
PassMark - CPU Benchmarks	Compare CPU's
PassMark - Videocard Benchmarks	Compare Videocards
PassMark - Memory Benchmarks	Compare Memory Modules
PassMark - Hard Drive Benchmarks	Compare HDD's / SSD's
AirPrint	List of Printers that support AirPrint

Networking

Port Forward	Repository of router port forwarding guides and ports for common software
Router Passwords	Repository of default router usernames/passwords and IP addresses
SpeedTest	Test internet connection download, upload, ping speeds

Security

Bitwarden Password Generator	Great password generator to create unique Passphrases
Have I Been Pwned	

Software

winstall	Make winget install scripts to batch install software
Ninite	Make standalone batch software installers
Adobe PDF Tools	Free to use PDF tools, use Incognito/Private mode to exceed free 'try' limits
Photopea	Free Photoshop alternative that runs in the web browser
PrintFriendly	Convert various file formats to PDF
Watermark Remover	AI watermark removing tool, use Incognito/Private mode to exceed free 'try' limits
Monkeytype	Typing test website
keybr	Typing practice website

Scripting / Coding

SS64.com	Quick reference from terminal shell commands, particularly helpful for CMD / Batch commands
----------	---

Phonetic Alphabet

The NATO Phonetic Alphabet can be very useful when trying to provide remote support over the phone

A	Aplha	N	November
B	Bravo	O	Oscar
C	Charlie	P	Papa
D	Delta	Q	Quebec
E	Echo	R	Romeo
F	Foxtrot	S	Sierra
G	Golf	T	Tango
H	Hotel	U	Uniform
I	India	V	Victor
J	Juliett	W	Whiskey
K	Kilo	X	X-ray
L	Lima	Y	Yankee
M	Mike	Z	Zulu

Miscellaneous

How to Hard Refresh Web Browsers

A hard refresh clears your browser cache for a specific page, which forces it to load the most recent version of that page. This could include new scripts, styles or features.

Important: Clicking the “Refresh” arrow on your browser address bar is not a hard refresh. Here’s how you can clear your cache through a hard refresh on any browser:

- Google Chrome
Windows: **Ctrl** and then press **F5**
macOS: **Cmd** + **Shift** + **R**
- Firefox
Windows: **Ctrl** + **F5**
macOS: **Cmd** + **Shift** + **R**
- Safari (Mac)
Empty Cache: Go to Safari > Empty Cache, or hit **Opt** + **Cmd** + **E**
Refresh: Click the refresh button on the address bar or press **Cmd** + **R**
- Internet Explorer/Microsoft Edge (Windows)
Ctrl + **F5**

How to Manually Clear the Print Queue (Windows)

- Open a terminal as Administrator
- Run the following commands:

```
net stop spooler
del %SYSTEMROOT%\System32\spool\PRINTERS\* /Q
net start spooler
```

How to Generate Battery Report (Windows)

- Open a terminal as Administrator
- Export Battery Report

```
powercfg /batteryreport /output c:\batt.html
```
- Open Battery Report

```
start c:\batt.html
```

How to Reset Page File (pagefile.sys) (Windows)

A page file (also known as a “paging file”) is an optional, hidden system file on a hard disk. Page files enable the system to remove infrequently accessed

modified data from physical memory to let the system use physical memory more efficiently for more frequently accessed data.

More Info

Page files extend how much **Committed Memory** (also known as “virtual memory”) is used to store modified data. This can be checked in **Task Manager > Performance > Memory > Committed** This committed memory value should represent Total Physical Memory + Page File size

Method 1: Registry

- Run **regedit** as Administrator (Shift + Enter)
- Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management**
- Open **ClearPageFileAtShutdown** (Double-Click)
 - Change Value data to 1
 - Click OK
- Close Registry Editor
- Restart Windows
`shutdown /r /f /t 00`

Method 2: Group Policy

- Run **gpedit.msc** as Administrator (Shift + Enter)
- Navigate to **Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**
- Open **Shutdown: Clear virtual memory pagefile** (Double-Click)
 - Select Enabled
 - Click OK
- Close Local Group Policy Editor
- Run a terminal as Administrator
`wt` or `powershell` or `cmd`
- Run the following command:
`gpupdate /force`
- Restart Windows
`shutdown /r /f /t 00`

Method 3: Manual

Disable Page File

- Open System Properties
`sysdm.cpl`
- Click Advanced tab
- Performance
 - Click Settings... button

- Click Advanced tab
- Virtual Memory
 - Click Change... button
 - Take note of the current settings (we'll need to re-apply these later)
 - Uncheck Automatically manage paging file size for all drives
 - Select C: drive
 - Select No paging file
 - Click Set
 - Click Yes
 - Click OK
- Restart Windows
`shutdown /r /f /t 00`

Re-Enable Page File

- Open System Properties
`sysdm.cpl`
- Click Advanced tab
- Performance
 - Click Settings... button
 - Click Advanced tab
 - Virtual Memory
 - Click Change... button
 - Re-Apply Settings as they were before disabling
 - Click OK
- Restart Windows
`shutdown /r /f /t 00`

How to Reset Hibernation File (hiberfil.sys) (Windows)

Windows uses the hiberfil.sys file to store a copy of the system memory on the hard disk when the hybrid sleep setting is turned on. If this file is not present, the computer cannot hibernate.

More Info

The hiberfil.sys hidden system file is located in the root folder of the drive where the operating system is installed. The Windows Kernel Power Manager reserves this file when you install Windows. The size of this file is approximately equal to how much random access memory (RAM) is installed on the computer.

Disable Hibernation

`powercfg -h off`
 or

```
powercfg.exe /hibernate off
```

Re-Enable Hibernation

```
powercfg -h on
```

or

```
powercfg.exe /hibernate on
```

How to Install / Repair Winget

- Connect to the internet
- Open a terminal as Administrator
- Run `irm asheroto.com/winget | iex`
- Wait for script to complete
- Close + Re-open the terminal
winget should now be working again
- Run `winget -v` to test