COPS Guide - Data Transfer (Windows)

contributors: shaun@	*updated: 05-AUG-2024*

Backup

- Restart Windows
  > *Force Restart Windows (`shutdown -r -f -t 00`) now to provide a clean slate for proceeding*
- [OPTIONAL] Create a new System Restore point
- Disable Antivirus
  > *(Some of our extraction tools prompt false positives in most security packages)*
- Create a Job# number folder on a Transfer Drive
  > *Create a new folder with the current job number (ie. 'Job#5000') to save User Data to*
- User Profile
  > *use Forensit Transwiz, Fast Pack (no compression), use default filename, no password*
- Web Browsers
  > *For each web browser installed export the following:*
  - Export Bookmarks *(ie. 'Web Browser - Google Chrome - Bookmarks - 2024-07-15.html')*
    > *Google Chrome URL: `chrome://bookmarks`*
    > *Microsoft Edge URL: `edge://favorites`*
    > *Mozilla Firefox Hotkey: `Ctrl+Shift+O`*
    > *Microsoft Internet Explorer: Copy Favorites folder (%USERPROFILE%\Favorites)*
  - Export Passwords *(ie. 'Web Browser - Google Chrome - Passwords - 2024-07-15.csv')*
    > *Google Chrome URL: `chrome://password-manager/passwords` or `chrome://settings/passwords` (older versions)*
    > *Microsoft Edge URL: `edge://wallet/passwords` or `edge://settings/passwords` (older versions)*
    > *Mozilla Firefox URL: `about:logins`*
    > *Microsoft Internet Explorer: Use Nirsoft IE PassView*
- Installed Programs *(ie. 'Installed Programs - 2024-07-15.html')*
  > *use Nirsoft UninstallView, save all as Horizontal HTML*
- License Keys *(ie. 'License Keys - 2024-07-15.htmal')*
  > *use Nirsoft ProduKey and Nirsoft Product Key Scanner*
- Emails
  - 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*
- Check C: Drive for unusual files/folders
  > *copy to Job folder copying the C: Drive file structure (TransferDrive:\Job#5000\C\FolderToSave)*
- [OPTIONAL] Create Winget Install Script
  > *https://winstall.app/ - Select Desired Programs - Generate Script - Download both Batch (.bat) and PowerShell (.ps1) scripts*
- Drivers *('TransferDrive:\Job#5000\Drivers - 2024-07-24')*
  > *Open PowerShell as Administrator and run (update with your export folder location):*
  > `Export-WindowsDriver -Online -Destination REPLACE-WITH-EXPORT-FOLDER`
- Enable Antivirus

Prepare New Device (if required)

- Bypass Network Registration in Windows 11 Out of Box Experience
  > `Shift+F10` to open Command Prompt:
  > Enter the command: `OOBE\BYPASSNRO`
  > Select 'I don't have an internet connection'
  > Select 'Continue with limited setup' (to create)
  > Create a Local Account named 'COPS' (no password)
- Configure System Restore
- Create a new System Restore point 'COPS - Fresh Windows 11 Install'
- Connect to the Internet after Windows logs into the COPS user account
- Configure Time/Date
- Configure Windows Update
- Update Apps via Microsoft Store
- Update Apps via Winget
- Update Windows
- Update Office apps
- Check for Device Manager for bangs(!)
  > *Check for missing or faulty drivers, and install/update as required (SDIO)*
- [OPTIONAL] Update remaining Drivers (SDIO)
- [If you installed/updated any drivers:] Verify Drivers (verifier)
  - **Turn On Windows Verifier:**
    - Run `Win+R` : `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 `Win+R` : `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 Profile using Transwiz
  > 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 priviledges
- 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
- Update Windows
- Update Office apps if present
- Restart Windows
- Remove 'COPS' user account
  - Run: `netplwiz` - Select COPS - Click Remove
  - Delete C:\Users\COPS\ folder
  - Empty Recycle Bin
- Windows Maintenance (run the following commands as Admin)

  ```
  winget source update
  winget upgrade --all --silent
  sfc /scannow
  dism /online /cleanup-image /startcomponentcleanup /resetbase
  dism /online /cleanup-image /restorehealth
  sfc /scannow
  ```

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