PCGenesis It Issues / Tips

Steve Phillips

- Printing Issues
  - Printing problems with PCGenesis
  - Double sided printing, won't print landscape only portrait or will not print at all.
  - What is the cause
    - A print driver acts as the translator who helps your technology to communicate more effectively.
    - Newer printer drivers tend to take control of a print job coming from a program (Word, Excel, etc)
    - Generic or universal driver will correct the problem
    - So when the print job leaves PCGenesis and goes to a printer with a regular print driver it chokes it does know what to do. But with a generic or universal print driver it basely let the print job start printing without trying to make any changes. It seems to correct the print problem every time. It is no magic just change the driver.
    - Where do I find the generic or universal driver? You can find the print driver for your printer on the web.
      - HP printers https://support.hp.com/us-en/drivers/printers
      - XEROX http://dnd.support.xerox.com/support/enus.html
      - Ricoh printers https://www.ricoh-usa.com/en/support-and-download
      - Brother printers https://www.brother-usa.com/brother-support/driver-downloads
    - How to install a generic or universal driver
      - It is recommended that you create another printer with a generic or universal driver for your printer and name it PCGenesis Check Printer. By doing this you will have printer (PCGenesis Check Printer) that you can direct PCGenesis print jobs and the other you Send print jobs to Word, Excel, etc.
    - Redirected printers
    - PCGenesis doesn't like redirected printers
      - What causes these redirected printers
      - The cause is printer check box on the Remote Desktop box is checked
- Window Server 2008
  - On January 14, 2020, support for Windows Server 2008 and 2008 R2 will end
  - The price is reasonable
    - 1 - Windows Server 2019 Standard -License - 16 cores - academic - OLP:Academic - Single Language $225.78
    - 10 - Microsoft - Windows Server 2019 -License - 1 user CAL - academic - OLP: Academic - Single Language $7.99 each $79.90
    - 5 - Windows Remote Desktop Services 2019 - License - 1 user CAL - academic - OLP: Academic - Win -Single Language $23.27 ea $116.35
    - Microsoft controls the price so it is same price at each reseller.
  - PCGenesis works great in Window Server 2019
  - More memory the better
  - Add terminal services (Remote Desktop Services)
    - License CALS come in packs of 5

    - Must be a stand-alone file server (Auditors prefer that it is stand-alone)
    - If you server only needs upgrading the server software you may not have to remove PCGenesis drive (K:\) to upgrade your server
        - If C:\ has 500k to 1GB or more of space
        - If K: is a stand-alone partition of at least 500 GB
- Remote Desktop
    - Classic Shell
    - Local Printing
    - Redirected printer
        - Cause and fix
    - Access to your desktop, documents and downloads
- PCGenesis Window Size (Windows Server 2008 x64 R2)
    - Connect to the remote machine using Window's standard "Remote Desktop Connection" application
    - but under Advanced -> Display tab choose a normal resolution like 1280x768.
    - Once you connect, click on the little icon (a screen with a sync symbol) in the uppermost lefthand corner of the window, where you find the options for maximize, minimize, etc. You'll see an option "zoom". Choose 200% for example. You'll find the right setting depending on your resolution and the resolution of the remote system.
- PCGenesis Window Size (Windows Server 2019)
    - https://jussiroine.com/2019/04/making-remote-desktop-fun-again-dynamic-resizing-and-resolution-changes-while-connected/
- Backup - PCGenesis
    - Tech B1: PCGenesis Full System Recovery Check List
    - Cobian Backup 11 (Gravity)
        - https://www.cobiansoft.com/
        - Jump Drive, External hard drive or off-site server
        - Free
- Dual Monitors

  Here are SIX good reasons to have dual monitors:
    - Published studies indicate that having a dual monitor in a workplace setting can increase productivity by 20 to 50 percent. For example, if you're a computer programmer, it should be obvious that having your source code on one side and your program on the other side of a dual monitor display would be very helpful.
    - Real multi-tasking requires enough screen space to keep two or more apps in full view simultaneously. If you have ever tried to size and align windows on a single monitor, you'll appreciate the ability to have several apps fully open at the same time. Customer service reps and web designers are additional examples of people that would benefit from dual monitors.
    - Cutting and pasting between documents is much easier when you don't have to alt-tab between them and scroll up or down so much. If you create newsletters or PowerPoint presentations, you'll identify with this.
    - Picture and video editing is a whole new experience with dual monitors. You can have all of your editing tools on one screen while you work on the project in the other. You can compare before and after views of the same work, or supersize panoramic pictures.

    - Comparing products is easier when you have dual monitors. You can show two video cameras' specs side by side in separate browser windows, for example.
    - Video and gaming take on a whole new dimension with dual monitors. You can view much more of a virtual world and see bad guys coming from a distance. Some gamers like to have Skype or another chat app open on a second screen.
- Windows 8 and 10 offer some new multi-monitor features, such as the ability to use different backgrounds on each monitor, span multiple screens with your background image
    - Cost is reasonable
    - $115-$140
    - Most newer desktops coming with video port (HDMI) or you can add a video expansion card
    - Easy to install
- TeamViewer
    - **TeamViewer** is the premier software solution for remote support, remote access, and online collaboration. In fact, we believe it is the best, most powerful, and most intuitive solution on the market, and many analysts, industry experts, and, most importantly, our customers would agree.
    - Auditor approve using TeamViewer
        - Transmission is Encrypted, requires 3 logins, desktop Remote Desktop and PCGenesis
    - Free or subscription
        - The free version of TeamViewer works but are subject to locked out because of use
        - Subscription cost $528 per year and you can use on 3 computers (Office desktop, home desktop and your laptop. Much faster and better screen control than the free version.
- Ransomware
    - Jump Drive Backup
        - full backup of K:*.*
        - backup of K:\SECOND*.* and K:\PCGSQLdb*.*
        - a copy of the *Technical System Operations Guide*, *Section A: PCGenesis Configuration, Topic 1: New Server Installation Checklist*. (Important information is available in *Section B* and *Section C* as well.)
- How Does Ransomware Spread?
    - Ransomware is most typically distributed through spam email attacks. The spam email will have an attachment disguised as a legitimate file or will include a URL link in the body of the email. If the former method is used, the ransomware program is activated as soon as the attachment is opened and within seconds, starts to encrypt files on the device. If the attack vector is a link, upon clicking it the user is taken to a web page where the ransomware is delivered to the device unbeknownst to the user. The malicious programs or sites often use exploit kits to detect if there are security vulnerabilities in the device's operating system or applications that can be used to deliver and activate the ransomware. Additionally, cyber criminals may utilize existing exploits as seen in the recent WannaCry attack, which took advantage of a well-documented Windows vulnerability known as EternalBlue.
- Reducing the Risk of Ransomware Impacting Your Business

- **Educate the weakest link.** The vast majority of ransomware requires someone to take action to activate the payload. Educating employees about how to recognize and defend against cyber attacks is vital. Many attacks will use email and social engineering techniques to trick the employee into downloading malware or divulging their username and password. As such, training should focus on these common attack vectors. Exercises where employees are sent faux "phishing" emails are effective in coaching users to distinguish between a genuine supplier communication and a phishing email with the subject line "Invoice Attached - please open."
- **Patch, patch, patch. Then patch again.** As demonstrated by the recent WannaCry and Petya attacks, failing to implement a rigorous approach to patching known security vulnerabilities can leave an enterprise exposed. Even months after the EternalBlue vulnerability was exploited for the WannaCry and NotPetya ransomware attacks, it's estimated that at least 38 million PCs remain unpatched.[8] It's relatively simple for cybercriminals to identify unpatched devices and software on an enterprise's network, and once identified, to take advantage of known vulnerabilities.

Make your email account more secure

- At Google, we take online security seriously. To protect your Google Account, we strongly recommend following the steps below regularly.
- Note: If you're a journalist, activist, or someone else at risk of targeted online attacks, learn about the Advanced Protection Program.

Step 1: Do a Security Checkup

- Go to Security Checkup to get personalized security recommendations for your Google Account, including:
  - *Add or update account recovery options*
  - Turn on 2-Step Verification
  - *Remove risky access to your data*
  - *Turn on screen locks*

Step 2: Update your software

- If your browser, operating system, or apps are out-of-date, the software might not be safe from hackers. Keep your software updated to help protect your account.
- *Update your browser*
- *Update your operating system*
- *Update your apps*

Step 3: Use unique, strong passwords

- It's risky to use the same password on multiple sites. If your password for one site is hacked, it could be used to get in to your accounts for multiple sites.
- Make sure to create a strong, unique password for each account.
- *Manage your passwords*
- *Help protect your password from hackers*

Step 4: Remove apps & browser extensions you don't need

- As more apps are installed on a device, it can become more vulnerable. Install only essential apps and browser extensions on devices that have access to sensitive information. Avoid installing unknown apps or apps from unknown sources to protect your device and personal info.
- Learn how to:

- Delete or disable apps on Android devices
- Uninstall extensions on Chrome
- Uninstall apps or extensions on Chromebooks
- Note: For info on removing apps and extensions from other devices and browsers, visit the applicable support site.

Step 5: Protect against suspicious messages & content

- Hackers can use emails, text messages, phone calls, and web pages to pretend to be institutions, family members, or colleagues.
- *Avoid suspicious requests*
- *Avoid suspicious emails*
- *Avoid suspicious web pages*
- If you notice suspicious activity on your account let someone know