

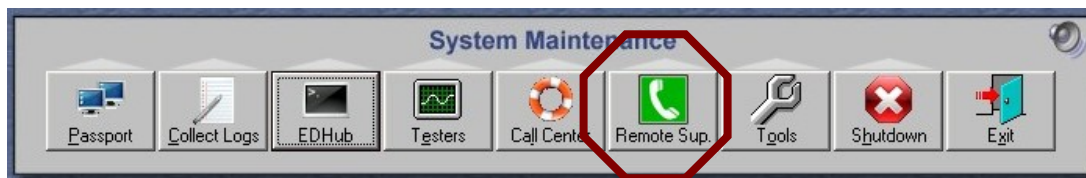
PA-DSS Quick Reference: Important Things To Remember

1. **Installing a Passport® POS is an important first step in your site's PCI compliance.** Gilbarco's Passport POS with Version 8.02/8.03 software meets the strict security standards required to achieve The PCI Security Council's Payment Application Data Security Standard (PA-DSS) validation. Be sure to also apply the store operational practices that are required for PCI compliance.

- Secure reports and system passwords.
- Review the Self-Assessment and other PCI educational tools at www.pcisecuritystandards.org.



2. **Use only Gilbarco-approved software on your Passport system.** Passport with PA-DSS uses the industry's latest virus protection technology. Protect your POS and your business by installing only trusted software on the Passport system. An "Approved Launcher" allows you to update some drivers for devices such as printers or UPS. You assume security risk if you install drivers not approved by Gilbarco.
3. **Keep your passwords in a safe place!** Your ASC will ask you to program your site's secure passwords at the end of Passport version 8.02/8.03 upgrade. You can set up one password that only the manager knows, or set up the manager's secure password and also provide security passwords for one or more trusted employees. Either way, the ***Security Manager Report*** is your record of the security passwords. ***Be sure to protect this Report and know how to get to the passwords when they are needed during any hour of operation.*** Gilbarco and your technician will not know these passwords, yet they are required for certain tasks (see 4 and 5). Consider having at least one other trusted employee with a security password so that person can act in the event the manager is not available.
4. **Yes, you can still print unmasked Network Account Transaction Reports.** Network Transaction Reports are important when you need to negotiate disputes and unpaid transactions with the network. You can print these reports two ways. Mask the sensitive cardholder data. Or, if supported by your payment network, show the full data you may need in a way that is PA-DSS validated. You will need to enter the **Secure Reports Password** created by your store management to print unmasked reports. The ***PA-DSS Implementation Guide*** (MDE- 4743) contains detailed instructions concerning the setup and maintenance of this Secure Password and other valuable PCI procedures. Ask your Installing Technician to review this document with you before leaving the site.
5. **Invitation is required for Help Desk support..** To protect your system from access by non-authorized personnel, someone at your store must enable Gilbarco's Help Desk to gain access to your system for Remote Diagnostics. It's easy to do: Simply press the ***Enable Dial-In*** button located under **Remote Support** button in the System Maintenance application, which you can access by pressing CTL-ALT-P.



In addition, a Manager or Cashier may need to enter the **Secure Password** that you have programmed (and only you know) to allow our Help Desk to remotely access the most secure part of the system.

6. **If your main Server goes offline, you still have network and fuel support.** If your main site server (COMBO) goes offline for any reason, you can still control fuel, continue CRIND® sales, and remain online with the network while your server issues are being addressed. Any secondary Cashier Workstations you have will remain online as well.
7. **Some prompting and processes have changed when the customer is using the PIN Pad.** Some Cashier Workstation PIN Pad prompts have changed as a result of our new architecture. The process for handling Manual Card Entry is also different. Your updated reference documents detail these changes. See MDE-4835.
8. **Don't pull the plug on the EDH.** The new EDH now functions more like a server/computer than our previous Dispenser Hub. As a result, we have safer methods to restart or reboot the EDH if required by our Help Desk. To restart the EDH, under System Maintenance, select EDHub, then either select Stop/Start EDH or Reboot EDH.

