
PDG Commerce

PABP Security Implementation Guide

**PDG Software, Inc.
1751 Montreal Circle, Suite B
Tucker, Georgia 30084-6802**

Copyright ©1998 - 2008 PDG Software, Inc.; All rights reserved.

PDG Software, Inc. ("PDG Software") retains all ownership rights to the software programs (referred to herein as "Software") offered by PDG Software and related documentation. Use of the Software and related documentation is governed by the license agreement accompanying the Software and applicable copyright law.

THIS DOCUMENTATION IS PROVIDED "AS-IS" WITHOUT WARRANTY OF ANY KIND. IN NO EVENT SHALL PDG SOFTWARE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, ARISING FROM ANY ERROR IN THIS DOCUMENTATION.

PDG Software, Inc.
<http://www.pdgsoft.com>

December 2008

PDG Commerce follows Visa’s Payment Application Best Practices (PABP) and operates in a secure environment according to the requirements of the Payment Card Industry (PCI).

Introduction

This guide provides instructions to ensure that your PDG Commerce program is maintained in a secure configuration in compliance with the PABP and PCI requirements. Merchants accepting credit card payments in an online storefront are responsible for maintaining a secure environment according to the current standards.

This document provides instructions and recommendations for installing and configuring PDG Commerce on your server to ensure that your storefront meets the appropriate guidelines.

Standard Terminology

CISP: Acronym for ‘Cardholder Information Security Program’. It is a program designed by Visa that aims to secure Visa cardholder data wherever it resides, requiring that members, merchants, and service providers maintain the highest information security standards. CISP compliance is required of all entities that store, process, or transmit Visa cardholder data.

PCI DSS: Acronym for ‘Payment Card Industry Data Security Standard’. It offers a single approach to safeguarding sensitive data for all card brands.

PABP: Acronym for ‘Payment Application Best Practices’. Applications such as PDG Commerce can be certified “PABP Compliant”. Using PABP compliant applications according to their documentation will assist merchants in being “PCI Compliant”. It is ultimately the merchant’s responsibility to ensure that their network, various other business software and hardware along with access control procedures, meet or exceed the requirements set forth in the PCI DSS.

PA-DSS: Acronym for ‘Payment Application Data Security Standard’. This is a program similar to PABP but is recognized by all five major credit card brands in an effort to standardize security requirements.

PAN: Acronym for ‘Primary Account Number’. This is the credit card number.

Cardholder data: The PAN, cardholder name, service code, and expiration date. If you are storing the PAN, the other cardholder data elements must be stored encrypted. PDG Commerce does not store the PAN, so encrypting the additional data elements is optional for our merchants.

Sensitive Authentication data: This data includes full magnetic strip, CVC2/CCV2/CID and PIN/PIN block. It cannot be stored subsequent to authorization (not even if encrypted).

Encryption: The process of transforming information (referred to as plaintext) using a process to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. PDG Commerce stores confidential information in an encrypted format. If you wish to encrypt additional data such as emails or order logs, you can do so by following the directions in our *Encryption Set Up Guide* at <http://www.pdgsoft.com/docs/Encryption.pdf>

SSL: Acronym for ‘Secure Socket Layer’. The standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. A web server requires an SSL Certificate to create an SSL connection. Typically when accessing a webpage over an SSL Connection in a browser, you will see a small padlock icon. This signifies that the information submitted is protected by a SSL certificate.

SFTP/SSH: Acronyms for ‘Secure File Transfer Protocol/Secure Shell’. These network protocols allow data to be exchanged using a secure channel between two networked devices over an insecure network, such as the Internet.

Additional CISP/PCI Information

You can find additional information about CISP, PABP, PCI, etc. at the following sites:

<https://www.pcisecuritystandards.org>

http://usa.visa.com/merchants/risk_management/cisp.htm

PCI Compliance

Below is a summary of the core of the PCI DSS. It is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized. Merchants should download and review the complete PCI DSS Requirements as it is your responsibility to maintain “PCI Compliance”. You will need to ensure that your hosting, internal networking (intranet), access control procedures, other software and hardware, etc. all operate together in a manner that is PCI Compliant. The complete PCI DSS guide can be found at <https://www.pcisecuritystandards.org>

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security.

Installation

PDG Commerce is installed on your web server. You and your hosting company and/or PCI consultant, should work to ensure that the software is maintained in a secure environment. All access to the server and web site should be properly

restricted. This access includes, but is not limited to, SFTP/SSH, remote access, control panel, payment gateway, email, and database accounts. Account information should be provided to as few individuals as possible, and passwords should be changed on a regular basis. The web server should be kept up to date with the latest available software patches.

Please review the *PDG Commerce Installation Guide* for installation instructions, as well as an explanation of permissions that should be set on all PDG Software files to restrict access properly.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

PDG Commerce should be installed and configured following the instructions provided in the *PDG Commerce Install Guide*. You should set up a secure network where all cardholder data is stored behind a firewall. PDG Commerce does not store any cardholder data. Any credit card information collected from your web site is sent to your payment gateway processor over an SSL connection. Your credit card processor is then responsible for storing and protecting this data.

PDG Commerce provides several features to assist you in securing access to your Commerce Administrator. The Commerce Administrator is available via Secure Socket Layer (SSL) access. You should use the IP Black List section of your PDG Commerce Administrator to enter the IP addresses of your office and personal computers, as well as any other computers that will need to access the program. All other IP addresses will be denied access to the program, even with a valid username and password. You may also need to enter the IP address of PDG Software or your authorized PDG Commerce reseller for troubleshooting purposes, which you should disable after the situation is resolved.

PDG Commerce provides the ability to modify certain program configuration files, such as the `shopper.conf` file, via non-console access. You should work with your hosting company to ensure that non-console access is provided through secure means, such as SSH or SFTP, VPN, or SSL/TLS, and that this access is recorded appropriately.

PDG Commerce does not prevent the implementation of a two-factor authentication mechanism such as RADIUS or TACACS with tokens, or VPN with individual certificates.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PDG Commerce requires the use of complex passwords. Upon logging into a new installation of PDG Commerce, you are required to create a unique user name and password. The user name must be 5 characters long and the password must be a minimum of 8 characters with at least one upper case, one lowercase letter and one number/special character. When you are setting up other passwords for appli-

cations such as SFTP, database, network password, etc. you should also verify they are unique and complex.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PDG Commerce does not store the PAN. If you are storing this information from another source, you should verify that it is encrypted to the standard necessary to meet the PCI-DSS requirements.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

If you are collecting credit card information from your web site, you are required to have and use a SSL certificate on the payment page. PDG Commerce will only send credit card information to a gateway processor via a SSL connection.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

PDG Commerce is designed to operate securely with anti-virus software on both the local computer and the web server. PDG Software recommends using any number of widely available and proven security products on your computers.

Requirement 6: Develop and maintain secure systems and applications

The PDG Commerce software is based on secure coding guidelines, according to Visa's Payment Application Best Practices (PABP) requirements. If you have any questions about the development process in respect to these requirements, please contact PDG Software.

PDG Commerce is tested for security issues prior to releases being made public. PDG Commerce does not provide software updates via remote access on an automated basis. Patches are provided for download on the PDG Software web site. Merchants with a premium support contract or who purchase a per incident ticket may request that PDG technical staff install the latest patch via SFTP/SSH or remote desktop access. You should provide a user account specifically created for PDG technical staff, which is disabled after the patch has been installed. Please note that these updates are provided to the PDG Commerce software residing on your web server at your request. Patches are never automatically installed, and are never installed to your personal or office computer.

You should verify that your other systems and applications are up to date. This includes local PC's, server operating systems, web sever software, database programs, anti-virus, anti-spyware, and firewall applications.

PDG Commerce does not provide an option for wireless payment applications. If you choose to make secure order information available to your employees in a wireless environment, you should ensure that all credit card data is encrypted and/or authentication is required to access the data.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Although PDG Commerce does not store cardholder data, it still offers the ability to restrict access to various areas in the PDG Administrator based upon the user login. If you have someone entering product information you can restrict them to that specific area, disallowing them access to orders, shipping, general administrator options, etc. Should you be storing cardholder data for another source, you should verify that employees have access 'as-needed'.

Commerce Administrator accounts are only provided to PDG technical staff by the merchant or authorized employees as needed for troubleshooting. You should create a user account specifically for PDG technical staff that is not used for any other purpose. You may choose which sections of the Commerce Administrator are accessible, and may delete the account after use. PDG technical staff may store the password if needed, in an encrypted format behind a firewall. PDG technical staff cannot obtain account information unless you provide it.

Requirement 8: Assign a unique ID to each person with computer access

PDG Commerce allows you to create a separate login ID and password for each of your employees who need access to the PDG Administrator. Your employees should be instructed to **never** share their login information with someone else.

PDG Commerce requires users to create unique usernames and complex passwords to access the Commerce Administrator. Passwords must contain eight characters, a combination of upper and lower case characters, and at least one special case character (numbers or punctuation). Merchants will be required by PDG Commerce to change passwords every 90 days. When a password is changed, the new password cannot match any of the previous four passwords. Six incorrect attempts to access the Commerce Administrator will result in a locked account, which will remain locked for 30 minutes. After 15 minutes of inactivity, Commerce Administrator users will be returned to the login page, and required to log in again to access the Commerce Administrator.

PDG Commerce Administrator passwords are assigned to a user account and email address. This information is encrypted in a file located in the PDG_Commerce directory on the server. If the merchant forgets her password, PDG Commerce will provide a one time use password to the email address assigned to the account.

Requirement 9: Restrict physical access to cardholder data

If you are storing cardholder data, you should verify that it is stored in a physically secure area. Areas with computers or printed data that stores credit card numbers should be secured (locked). You should use a shredder to dispose of printed materials that contain cardholder data when it is no longer needed.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PDG Commerce provides an activity log for the PDG Administrator.

The following occurrences result in an event written to the audit log:

- Any time a user accesses any portion of the Commerce Administrator or makes a change to the Commerce Administrator.
- Any time a user attempts to log into the Commerce Administrator and fails.
- Any time a user attempts to access a portion of the Commerce Administrator to which he does not have access.
- Any time a user performs an action that causes the program to create or delete a system-level object.

Each time a user attempts to access the audit log, PDG Commerce validates that the current user is the main account for the Commerce Administrator. For each event written to the audit log, the username, type of event, date and time, success or failure indication, origin of event, and name of the affected data are recorded.

PDG Commerce does not provide configuration options for the format of the audit log. You can change the name of the file in the 'shopper.conf' file. The log file may be deleted from the PDG_Commerce folder, located on the server. Access to this folder should be appropriately restricted. A copy of the audit log should be saved for your records on a location other than the server before the log is deleted. A new log file will be created the next time a user accesses the Commerce Administrator.

PDG Commerce logs follow the requirements of sections 10.2 and 10.3 of the Payment Card Industry Data Security Standard (PCI-DSS). It is the merchant's responsibility to ensure that SFTP/SSH and file access to the server is recorded appropriately according to the PCI-DSS document requirements (sections 10.2 and 10.3).

The logs should be reviewed regularly to detect attempts at unauthorized access. You should also maintain logs for other business applications you may use, such as your web server, SFTP/SSH sessions, Windows Events.

Requirement 11: Regularly test security systems and processes

You should refer to the PCI-DSS for detailed guidance for the testing standards appropriate to your Merchant Level.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Using the information from this guide and the PCI-DSS documentation, you should implement a security policy making all employees responsible for protecting customer data to which they have access.

How to securely remove security keys:

Prior to PDG Commerce V5 security keys and secure information were set automatically. The user being able to set the security key for PDG Commerce V5 is one of the improvements in V5. The software then uses this key as part of the encryption key for user passwords, sensitive configuration information as well as session management. The user can change or update the security key at any time as long as they have Administrator privileges, the current, and are logged into the PDG Administration Panel. If the user needs to delete or completely remove the security key, then they can delete the `pdg3.dat` and `.ustats` files (located in the PDG_Commerce folder in the cgi-bin folder). Once these files are removed the system will lose all of its user accounts and sensitive configuration settings.

Once the files are deleted and the user tries to log in again, they will be forced to create a new Administrative user account and re-enter all sensitive configuration information (this includes database, real-time shipping, payment gateway and other secure information).

Upgrading from previous version of PDG Commerce

If you have upgraded to PDG Commerce from a previous version or from PDG Shopping Cart, you may have order log files from the previous version in the PDG_Commerce or PDG_Cart folder located on the server. While it is a recommended security practice to delete these files often, previous versions of PDG Software did have the option to store credit card data in the order logs. Please note that PDG Software has never stored the CCV code.

Release versions of PDG Commerce also remove any existing debug files. Debug logs do not store credit card data.

PDG Commerce V5 does not store any secure card data. The information is collected and sent via a secure connection to your payment gateway for processing.

If you are upgrading from an older version of PDG Commerce you may have been storing card data like credit card number and expiration date. If you still have PDG Commerce V4 or earlier you can login to the PDG Administration Panel and look under 'Commerce Options' to determine if you were storing card data. If you are storing card data you should follow the steps below once you complete the upgrade.

If you have already upgraded then you should remove the card data from your website. The first step is to login to your PDG Commerce V5 Administration Panel. Then go to the 'Orders' section and select 'Orders & Reports'; then click on the 'Logging Settings' tab. From this page you can see what order files are being maintained and the file names as well. You will see 3 different file types: csv, xml and text. All these files can contain secure card data. Please record the files name being used.

Now that we have identified the files to delete we will repeat the steps below for each file:

- 1) download secure delete/wipe software. PDG Software recommends **SDelete** (downloadable from Microsoft) on Windows servers and **Wipe** (wipe.sourceforge.net) for Unix servers. This software is used to make the data on the disk non-recoverable once it is deleted.
- 2) download and store files in a secure manner if they are needed. If you are not sure how to do this contact your PCI/security consultant.
- 3) follow the secure delete/wipe software instructions and remove the files that were identified.
- 4) once the files are deleted PDG Commerce V5 will create new files with the names that were listed in the 'Logging Settings' section. The new files will NOT contain any sensitive card data because PDG Commerce V5 does not store sensitive card-data.

Appendix

Security Checklist for users of PDG Commerce

While PDG Software has designed this document to contain a list of items that should be verified when using PDG Commerce, it should not be considered comprehensive. Web security requires constant communication between you, your server administrator, and the provider of any software applications utilized on your web server. **PDG Software, Inc. does not guarantee that this list will make any site absolutely secure.** This checklist is not intended to provide a complete security check for your site, though it is an excellent starting point.

Each of the items below should be confirmed with your site administrator, server administrator, and any other parties necessary. If you are unsure of the appropriate party to contact for each portion of the checklist, please contact PDG Software for assistance.

- PDG Software updates - Verify that PDG Commerce has been upgraded to the most recent version available. The most recent versions of PDG Commerce include a considerable number of security features to help protect you and your web store.
- Operating system updates - Verify that all operating system patches and upgrades have been installed to the server where your site resides. Failure to do so can result in the compromise of your entire web server.
- Web server updates - Verify that all web server software programs (including web server, SSL modules, etc.) have the appropriate patches and upgrades in place.
- Windows permission, IIS, and Web Service Extensions settings - For Windows 2000/2003 servers, confirm that IIS, file permissions, and web service extensions (Windows Server 2003 and newer) have been set per the PDG Commerce documentation found at <http://www.pdgsoft.com/security.htm>.
- UNIX .htaccess protection - For UNIX servers, confirm that you have the appropriate .htaccess file located within your PDG_Commerce directory. Additional information regarding .htaccess can be found at http://www.pdgsoft.com/unix_security.htm.
- Placement of PDG_Commerce directory and order log files - PDG Commerce allows users to choose from a number of locations to store the PDG_Commerce directory, including the option of storing it outside of the site's document root directory so that it is unavailable via URL queries. The three locations that PDG Commerce will attempt to locate the PDG_Commerce directory are one directory above the document root, within the document root, or within the cgi directory in which the PDG Commerce executables are stored.
 - It is not required that your order log files be created and stored within the PDG_Commerce directory. You may supply a full server path to a protected directory, or you may use ../ to specify a path relative to the PDG_Commerce directory.
- GPG encryption - PDG Commerce is compatible with GnuPrivacy Guard (GPG). GPG offers encryption for sending and storing sensitive data. Please review the PDG Commerce Encryption Guide for instructions.
- SSL (Secure Socket Layer) web certificates - SSL certificates issued by PDG Software partners such as GoDaddy, VeriSign, Thawte, and GeoTrust encrypt all data as it is in transit from a customer's web browser to your web server. Please review the

PDG Commerce User Guide for instructions for adding SSL to your PDG Commerce program.

- Passwords - All passwords, including your PDG Commerce Administrator password, as well as your password for online payment gateways and SFTP/SSH/web access accounts, should contain a minimum of eight characters, include a combination of upper and lower case characters, and at least one special character (number or punctuation). Avoid using common information as passwords or usernames. Passwords should also be changed on a periodic/frequent basis. **Do not use the same password for all accounts.**
- File naming - Similar to choosing a password, merchants should also use caution when determining the names of order log and payment gateway log files. **Default file names should never be used for order log files.** Select a file name that cannot be easily guessed and would not be apparent to an unauthorized user.
- Authorized users - Verify that only authorized users have access to your web site and Commerce Administrator. Do not share your passwords with any unauthorized individuals. Verify that all former employee access is terminated immediately after employment has ended and that any site passwords they may have had access to are changed. If it is necessary to provide your account information to a third party, be sure to change the password as soon as the situation is resolved.
- Archiving previous orders - Download and remove secure order information from your server on a regular basis. PDG Commerce will automatically create new log files with the same names on the next order any time you download and delete your order log files.
- Payment gateway setup - If you are utilizing an online payment gateway to accept credit cards or checks online, be sure that you adhere to the setup process referenced in the PDG Commerce User Guide and your payment service provider's instructions.
- Disposal of printed materials - Be sure to dispose of any printed secure order information in the appropriate manner (e.g., shredding).
- Removing welcome page - The commerce.html page located in the document root directory of your web site is for familiarizing yourself with PDG Commerce. this file should be removed, renamed, or relocated as you acquaint yourself with PDG Commerce to make it more difficult for a malicious web user to determine which software is being utilized on your web site.
- Renaming executables - The commerce.cgi or commerce.exe executable file in use on your web site may be renamed to any name (based on your server configuration, it may be necessary to maintain the .cgi or .exe file extension) to make it more difficult for a malicious web user to identify the software being utilized on your web site. It is important that your web pages reflect the new name or your customers will encounter "file not found" errors when attempting to purchase items on your web site.
 - When upgrading to new minor version patches of the PDG Commerce program, you will need to rename the commerce.cgi or commerce.exe executable file in the upgrade to the name you are using on your web site.
- Firewall - Install and maintain a working network firewall to protect sensitive data that is available via the Internet.
- Web access logs - Verify with your hosting company or server administrator that access logs are being created for all queries to your web site. In the unfortunate event that the server or your web site is compromised and an unauthorized user gains access, these files will assist in determining how the user was able to bypass your security settings.

