
PDG Commerce
version 5

Installation Guide

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

Copyright ©1998 - 2009 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>

May, 2009

Contents

Chapter 1	Installation Overview	7
	Installation Process	7
	Configuration	7
	Integration of PDG Commerce	8
Chapter 2	Installation Preparation	9
	Definitions	9
	Preparing for Installation	10
	Installation Notes	10
	System Requirements for PDG Commerce	11
	Downloading PDG Commerce	11
Chapter 3	Installation	13
	Unzipping the Archive	13
	Web Server Installation	14
	Account Setup	16
	Database Setup	17
	Setting Up the Database	19
	Using PDG Commerce	19
Chapter 4	Setting Permissions	21
	Windows Permissions	21
	Unix Permissions	22
	Verify Permissions	23
Chapter 5	Appendix	25
	File Transfer Formats	25
	Security Checklist for PDG Commerce	26

Installation Overview

Installation Overview for PDG Commerce

Adding PDG Commerce to your web site consists of three main activities. These are installation, configuration, and integration of PDG Commerce.

Installation Process

The installation process includes:

- Downloading PDG Commerce files
- Uncompressing PDG Commerce files
- Copying PDG Commerce files to your web server
- Setting security permissions for files
- Basic database configuration

Configuration

Configuration consists of using the Merchant Administrator to configure PDG Commerce's many options including the addition and maintenance of products. Configuration is only touched upon in this guide.

Integration of PDG Commerce

Integrating PDG Commerce consists of adding PDG Commerce functionality to your web site, and modifying PDG Commerce's templates to match your web site design and layout. At your request, PDG technical staff will create a *skin set* for you that incorporates your web site's look and feel into a set of templates that can display PDG Commerce data. This skin set can be based on an existing page on your web site, or a new page design or template of your choice. An initial skin set is created as a courtesy. Additional skin sets can be provided for a fee.

You can also create your own skin set by modifying any of the included templates. A final option for embedding PDG Commerce is to use your own existing pages, and modify the forms and links to point to the appropriate PDG Commerce commands.



Installation Preparation

Preparing to Install PDG Commerce

This guide explains the process for installing PDG Commerce on your web server. If you would prefer that PDG technical staff install the software for you, please contact PDG Software. Installations are provided as a courtesy for your free trial of the program or with a retail price purchase. If you are purchasing through an authorized PDG Commerce reseller, you may request installation from the resell company, or you may purchase an installation performed by PDG technical staff.

Definitions

This section refers to several terms used to describe the file transfer process. The following definitions explain terms used throughout this chapter.

SFTP: SFTP stands for Secure File Transfer Protocol, and refers to a program used to connect your computer to your hosting company's web server securely. This program allows you to transfer files to and from your web site. Your hosting company can assist you in setting up your SFTP program.

Local System: The local system is your computer. When using an SFTP program, you will be able to transfer files from your computer to the web server. The *local system* refers to the files located on your computer.

Remote System: The remote system is your hosting company's web server, on which your web site resides. The *remote system* refers to the files located on your web site.

Preparing for Installation

PDG Software recommends that you run through the following checklist before beginning installation. If you do not have the information necessary or require assistance with these items, you should contact your hosting company.

- Make sure you know the operating system of the server on which your web store resides.
- Verify that your web site's host server meets the hardware/software requirements explained in the next section.
- You will need a basic understanding of zip/unzip utilities, and secure file transfer protocol (SFTP).
- Have your SFTP or remote desktop username and password available so that you can access your web store's host server.
- You will need to create a database on your web server. You will need to record the database server address, database name, user name, and password.
- You will need an SSL (Secure Socket Layer) certificate installed on your web site, and will need to know the complete URL to the secure server.

Installation Notes

It cannot be stressed strongly enough how important it is that your PDG Commerce site have the proper permissions set, not only for security reasons, but also to ensure proper operation. Many errors in functional operation can be traced to having improper permissions on the directories or files, particularly the PDG_Commerce directory.

Note: PDG Commerce is compliant with the PCI PA-DSS (Payment Applications Data Security Standards). It is the merchant's responsibility to ensure that permissions are set properly according to this guide to be secured. The permissions outlined in this document also provide compliance with the appropriate portions of the Payment Card Industry Data Security Standard (PCI PA-DSS).

The file permissions for the PDG_Commerce directory (and all files and subdirectories it contains) are 700 (UNIX) for the web user account. If the site will be updated by multiple users, you may need to create a user group to access the files. In that case, permissions should be 770 to allow appropriate access for the group. If that does not provide adequate access for the server and your staff, permissions can be 777. Please note that there may be some security implications based on the hosting environment. You should work with your PCI consultant to ensure that the hosting environment is compliant with the PCI PA-DSS requirements.

Note that PDG Commerce is a server-side program. No client-side version of it exists. To operate properly, it is necessary to have a web site hosted on a server, and the pages must be viewed through that server. Simply previewing them in your HTML editor on your local machine is not enough, because program data will not be available.

System Requirements for PDG Commerce

Before installing PDG Commerce, verify that your web server meets the appropriate requirements.

The following requirements must be met in order for PDG Commerce to function properly. You should contact your hosting company to ensure that the server on which your site resides is capable of operating PDG Commerce.

- Your web server must be CGI compliant. Most major web servers, including Apache and IIS, are compliant. The CGI directory on your web server must be able to execute compiled binary scripts.
- At least 35 MB of hard drive space must be available in the CGI directory. Please note that 70 MB of hard drive space is recommended.
- Ability for the Web server to access and write to the CGI directory and subdirectories for retaining logs and invoice numbers.
- MySQL, Microsoft Access, or MS SQL Server should be installed and you should verify it is operational and running properly.

Your customers will need to use a web browser that supports client-side cookies, JavaScripts, and flash in order for PDG Commerce to display and function properly while visiting your web store. This will not be an issue for your customers unless they have disabled this functionality.

Downloading PDG Commerce

If you have everything you need from the checklist, and your hosting server meets the requirements, you should be ready to install PDG Commerce. The first step is to download the software from the PDG Software web site, <http://www.pdgsoft.com>.

When you download PDG Commerce, you are retrieving an archive. An archive is a compressed, or zipped, collection of files. The installation archives include the executables and files which comprise PDG Commerce, and the Installation manual in Adobe Acrobat format (PDF).



Completing a new installation

This chapter will guide new users of PDG Commerce in the installation of the software. Prior to beginning the steps outlined throughout, you should make sure that you have downloaded the correct version of PDG Commerce for your web server's operating system.

Unzipping the Archive

If you have not already done so, download PDG Commerce from the PDG Software web site, <http://www.pdgsoft.com>.

Next, extract the archive files using a zip/unzip utility such as WinZIP. Your extracted archive should have the following structure:

- PDG_Commerce_V5
 - Your_CGI_Directory
 - PDG_Commerce
 - additional files
 - Your_Document_Directory
 - CommConfig
 - PDGCommTemplates
 - PDGEditorTemplates
 - PDG Images
 - commerce.html

Along with the “Your_CGI_Directory” and “Your_Document_Directory” sub-directories, there will also be some PDF files. The PDF files will include this

installation guide and the license agreement. All of these PDF files can be viewed using Adobe Acrobat Reader.

Web Server Installation

PDG Commerce requires a web server and a database to run properly. PDG Commerce for Microsoft Windows is distributed ready to work with Microsoft Access, Microsoft SQL Server, or MySQL databases. For PDG Commerce for UNIX, you must have access to a MySQL database. It is your responsibility to have access to a functioning webserver and a database.

Before installing PDG Commerce, you should set up a database. This is done through your hosting control panel. Once the database is set up, record the connection information, which you will need during PDG Commerce installation. If you require assistance creating a database on your web site, you should contact your hosting company or system administrator for assistance.

Note: Most files may be uploaded to your web server in automatic transfer mode. In this mode, your SFTP program determines which transfer format to use based on the file extension. When noted in this guide, you must change the transfer mode to binary instead of automatic. If you are not sure how to change the transfer mode, you should obtain assistance from the provider of your SFTP program.

Transfer the 'Your_CGI_Directory' Contents

Using an SFTP program:

1. Start a session and connect to your web site's location on its host server.
2. In the local system view of your SFTP window, locate the directory containing the PDG Commerce files that you extracted. Open the PDG_Commerce_V5 folder, then open the Your_CGI_Directory folder.
3. Find the CGI directory on the remote system view of your SFTP window. This may be named cgi-bin, cgi, cgi-local, etc. If a CGI directory does not exist on the server, you will need to create one.
4. Transfer the four executable files in binary format from the local to the remote system. For a UNIX server, these files are commconfig.cgi, commerce.cgi, redirect.cgi, and img-uploader.cgi. For a Windows server, these files are CommConfig.exe, Commerce.exe, redirect.exe, and img-uploader.exe. These files must be uploaded in binary transfer format.
5. Transfer the PDG_Commerce directory and its contents in automatic format from the local to the remote system. You should transfer the entire folder to the CGI directory on the remote system.

Transferring the 'Your_Document_Directory' Files

Continuing with your SFTP session:

1. In the local system view of your SFTP window, locate the directory containing the PDG Commerce files that you extracted. Open the PDG_Commerce_V5 folder, then open the Your_Document_Directory folder.
2. In the remote system view of your SFTP window, locate the document directory of your web site. This is the folder that contains the home page of your web site. This folder is often named public_html, htdocs, httpdocs, or www.
3. Transfer the PDGCommTemplates, PDGEditorTemplates, CommConfig, and PDGImages folders from the local to the remote system in automatic format.
4. Transfer the commerce.html file in automatic format from the local to the remote system.

Adjusting Files

At this point, all of the files necessary for PDG Commerce to function are now on your Web store's server. However, you may need to make a few changes to complete installation.

If the CGI directory on your site is not named cgi-bin, you will need to make the following changes to your Commerce installation. If the CGI directory is named cgi-bin, you may skip this section.

Continuing with your SFTP session:

1. In the local system view of your SFTP window, locate the commerce.html file in the Your_Document_Directory folder. Select it and click the 'View' or 'Edit' button in your SFTP program to open the file in a text editor.
2. Use the "Find and Replace" option of your text editor to replace cgi-bin with the correct CGI directory name.
3. Save the changes and then upload the file from the local to the remote system in automatic transfer format, overwriting the existing file.
4. In the local system view of your SFTP window, locate the CommConfig folder in the Your_Document_Directory folder, and open it. Find the index.html file in this folder, and click the 'View' or 'Edit' button in your SFTP program to open the file in a text editor.
5. Use the "Find and Replace" option of your text editor to replace cgi-bin with the correct CGI directory name.
6. Save the changes and then upload the file from the local to the remote system in automatic transfer format, overwriting the existing file. **Make sure that you are uploading the file to the CommConfig directory on the remote system.**

Setting Permissions

For Web server applications, there are two types of permissions. There are file permissions and there are web server permissions. File permissions indicate which user accounts on the server have access to which files. Web server permissions indicate which directories and files the web server will allow users to browse or read with their browser. Please note that Windows and UNIX servers use different types of settings for file permissions.

The file permissions for the PDG_Commerce directory (and all files and subdirectories it contains) are Modify (Windows) and 700 (UNIX) for the web browser account. If the site will be updated by multiple users, you may need to create a user group to access the files. In that case, permissions should be 770 to allow appropriate access for the group. If that does not provide adequate access for the server and your staff, permissions can be 777. Please note that there may be some security implications based on the hosting environment. You should work with your PCI consultant to ensure that the hosting environment is compliant with the PCI PA-DSS requirements.

Web server permissions **must** be set to prevent reading and browsing of your PDG_Commerce directory. For Windows servers, these permissions are set in IIS. For UNIX servers, these permissions are set using an .htaccess file.

See Chapter 4 of this guide for details on setting permissions.

Account Setup

After the PDG Commerce program has been installed and permissions have been set properly, you will need to configure the primary user account. To create the account, open a web browser, and enter the following address, changing `www.webstorename.com` to your web site's domain name.

`https://www.webstorename.com/commerce.html`

On the page that is displayed, click the "Administration" link in the blue box on the left side. Click the "Enter Your Commerce Administrator" link on the following page. The next page will prompt you to enter the appropriate data required to create your primary user account.

User Name

In this field, enter the user name you would like to use to access the primary account. User names must be unique. Common words such as temp, test, and admin. This account will be for your use only. You will create additional accounts for all other users of your PDG Commerce program.

Password

In this field, enter the password you would like to use to access the primary account. You must create a complex password for the account, including uppercase and lowercase letters, and at least one special character (number or punctuation mark). The password must be at least eight characters long.

Confirm Password

In this field, enter your password again to confirm it. If the “Password” and “Confirm Password” field entries do not match, the account will not be created and you will be required to enter the data again.

Email

Each account must have a valid email address assigned to it. You should enter your email address in this field. You should not use a generic address, as this user account will not be shared. Please note that a valid email address is required.

Secret Phrase

You must enter a secret phrase that will be used to secure your user account. It must be between 16 and 255 characters long, and should contain a combination of lowercase letters, uppercase letters, numbers, and punctuation marks.

Note: You *must* save the secret phrase for your account in a secure place where you can locate it if needed. If you forget your username or password in the future, and do not have access to the email address for the purpose of resetting the password, you will need the secret phrase to create a new account. If you forget the secret phrase, data will be lost from your Commerce Administrator settings, which you will then have to re-enter with a new account.

Database Setup

After you have successfully created the primary user account for PDG Commerce, you will be prompted to establish the connection between PDG Commerce and your blank database. To do that, enter the following fields as appropriate. Please note that some fields may not appear on the page, as they are dependant on your server’s operating system.

Database Driver Type (Windows only)

Select the appropriate database driver type from the drop down menu. If you are not sure which type of database you are using, contact your hosting company for assistance.

DSN (Windows Only)

This is the name of the data source file, which will contain the complete database for your Web site. This field is not required. If you decide to use it, you must create a system DSN on the server.

SQL Server or MySQL Server

This field is used to specify the name of the database server if you are using an MS SQL or MySQL database. This field should contain the IP address or the name (without https://) of the database server. If you are using the provided Microsoft Access database, leave this field blank.

SQL Server Database or MySQL Server Database

This field is used to specify the name of the MS SQL or MySQL database you are using. If you are using the provided Microsoft Access database, leave this field blank.

MS Access database filename (Windows only)

This field is used to specify the name of the MS Access database. The default is commerce.mdb. If you are using an MS SQL or MySQL database, leave this field blank.

Login Name

This field is used to specify your MS SQL or MySQL login name. If you are using the provided Microsoft Access database, leave this field blank.

Password

This field is used to specify your MS SQL or MySQL password. If you are using the provided Microsoft Access database, leave this field blank.

MySQL Socket (UNIX only)

You should leave this field blank for a default MySQL configuration. If the MySQL socket file exists in a different location on the server, enter the location and file name in this field.

Setting Up the Database

After entering your database connectivity information, click the ‘Submit Changes’ button. If the information was entered correctly, a button will now appear at the top of the page called ‘Install the Commerce Database (version 3.00)’. Click this button to install the appropriate PDG Commerce tables into your database.

If the database has been configured correctly, the following message will appear:

You have the correct database for this version of Commerce

Once you see this message, click the “Make Live” link at the top right of the page.

Using PDG Commerce

At this point, you are ready to begin using PDG Commerce. To access the PDG Commerce Welcome page, enter the following address in a web browser:

<https://www.webstorename.com/commerce.html>

Where www.webstorename.com is replaced with your web site’s address. The Welcome page provides links to several portions of your PDG Commerce program to help you get started.



The PDG Commerce program must have both file and web server level permissions set correctly to operate properly on your web site.

For Windows machines, the PDG_Commerce folder and its subdirectories must have modify file level permissions set for the web browser account. If your hosting company does not provide an option for you to set these yourself, you should contact them for assistance and provide them with the following settings information.

Windows Permissions

If you are using Windows 2003, follow the steps below. Otherwise, download the appropriate guide for your version of Windows from <http://www.pdgsoft.com/security.htm>.

File system permissions

The file permissions must be set for the Internet Guest Account (e.g., IUSR_[computer name]) so that the web server and executables can read, write, modify, and delete the configuration files located within the PDG_Commerce directory. For this specific directory, you'll need to allow full control for the Internet Guest Account. You will also need to make sure that the Internet Guest Account has read and execute permissions for the files in the CGI directory. This is typically enabled by default.

Web Server permissions

In the IIS window, navigate to the cgi directory. Right-click this folder and select Properties. On the main tab of the resulting page, verify that read, write, index this resource, and directory browsing are disabled. On this same page, verify that the script resource for the cgi directory is set to “scripts and executables.”

In the IIS window, go to the “manage service extensions” area and create a service extension that will tell IIS to execute the PDG Commerce files. Create a new service and add the following files as permitted executables: within the cgi directory, commerce.exe, commconfig.exe, redirect.exe, and img-uploader.exe.

If you do not have the option to set these permissions, you should provide your hosting company with the **PDG Software Windows Permissions Guide**, and request that they set the permissions for you.

Unix Permissions

File system permissions

You can set permissions using your SFTP client. If you are unfamiliar with how to do this, try selecting a file or folder and looking for “Properties” or “CHMOD.” If you are not sure how to access the appropriate settings, consult the provider of your SFTP program.

Locate the CGI directory on the remote system, and set permissions to 755. Open the CGI directory, and set the four executable files (commconfig.cgi, commerce.cgi, img-uploader.cgi, and redirect.cgi) to 755 permissions. Set the PDG_Commerce folder to 700 permissions. Open the PDG_Commerce folder, and set the AdminTemplates, EmailTemplates, Intro, and ProdText folders to 700 permissions. Set all additional files in this folder to 600 permissions.

Please note that it may be necessary to set folders to 770 or 777 permissions and the PDG_Commerce files to 660 or 666 permissions, based on the user configuration provided by your hosting environment. There may be some security implications based on the configuration of your web server. You should work with your PCI consultant to ensure that the hosting environment is compliant with the PCI PA-DSS document.

Web Server permissions

For most UNIX servers, server level permissions can be set with an `.htaccess` file. This is a text file that can be placed in a directory. When the web server receives a request for a document in that directory, it checks for an `.htaccess` file and verifies access.

PDG Commerce includes an `.htaccess` file that blocks all browser requests to the `PDG_Commerce` directory. This file was uploaded during installation. This file should block any attempts to browse your data. If it does not, you should contact your hosting company to ensure that the use of `.htaccess` files is enabled on the server.

Verify Permissions

To ensure that the permissions have been set properly for your PDG Commerce installation, you should attempt to access a link on your web site. If the permissions are set properly, this link will return a “forbidden” or “file not found” error. If text is displayed when you view this link, then the permissions have not been set properly and your PDG Commerce program is not secure.

To verify permissions, you should attempt to view one of the PDG Commerce configuration files through a web browser. This file should not be visible. You should use the following links, replacing `www.webstorename.com` with your web site’s domain name.

`http://www.webstorename.com/cgi-bin/PDG_Commerce/shopper.conf`

`https://www.webstorename.com/cgi-bin/PDG_Commerce/shopper.conf`



Additional information for installation of PDG Commerce

Included in this appendix are two sections of additional data that you may find useful in the process of installing the PDG Commerce program on your web server. First is a list of file transfer formats used for installation based on the file extension. Second is the PDG Commerce Security Checklist, which provides a starting point for ensuring that your web store is properly secured.

File Transfer Formats

When uploading PDG Commerce to your web site, you must transfer files in either ASCII or binary format. The following is a list of file extensions used by PDG Commerce, and the required transfer type.

- .html and .htm - ASCII
- .js - ASCII
- .css - ASCII
- .gif and .jpg - binary
- .conf - ASCII
- .txt - ASCII
- .exe - binary
- .cgi - binary
- .xml - ASCII
- .Email - ASCII
- .htaccess - ASCII
- .conf - ASCII
- .lic - ASCII

Security Checklist for PDG Commerce

While PDG Software has designed this section to contain a list of items that should be verified when using PDG Commerce, it should not be considered comprehensive. **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.
- 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 2000/2003/2008 servers, confirm that IIS, file permissions, and web service extensions (Windows 2003 and 2008) 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 - You can use encryption to secure your customers' data. PDG Commerce is compatible with GnuPrivacy Guard (GPG). GPG offers 128-bit 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, password for online payment gateways, and FTP/web access accounts should contain a minimum of eight characters, include a combination of upper and lower case char-

acters, 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.

