# AbleCommerce Gold

Version 7.0.91.8643
Release Label: Gold R11

## Secure Implementation Guide
PCI DSS 3.1

Revision: 1.0
October 8th, 2015

# Copyright



**Able Solutions Corporation**
PO Box 2671
Titusville, FL
32781

Phone: 1-360-571-5839
Toll Free: 1-800-292-7192 (USA Only)
Fax: 1-360-546-3532
Email: support@ablecommerce.com
Website: http://www.ablecommerce.com

# Revision History

**Revision 1.0 – Oct 8th, 2015**

- Initial publication.

The contents of this guide will be reviewed and updated periodically, at least once per year.

# Table of Contents

# Introduction

## *Scope and Target Audience*

This guide covers AbleCommerce Gold, and is intended for merchants and integrators who wish to implement the application in accordance with guidelines set by the Payment Card Industry (PCI).

## *PCI Data Security Standard (PCI DSS)*

In 2006 American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International formed the Payment Card Industry Security Standards Council. The main purpose of the council is to produce and maintain the Data Security Standard (DSS). This is a set of rules and requirements that when followed will help prevent fraud, hacking, and other threats to private cardholder data. The main objectives of the PCI DSS are as follows:

- Build and Maintain a Secure Network
  - Install and maintain a firewall configuration to protect cardholder data
  - Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - Protect stored cardholder data
  - Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Use and regularly update anti-virus software
  - Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Restrict access to cardholder data b y business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Track and monitor all access to network resources and cardholder data
  - Regularly test security systems and processes
- Maintain an Information Security Policy
  - Maintain a policy that addresses information security

You can find and review the complete specification by visiting the URL below.

https://www.pcisecuritystandards.org/

This guide is intended to help merchants implement the AbleCommerce application in a way that is compliant with version 3.1 of the PCI DSS.

## *Payment Application DSS (PA-DSS)*

The Payment Application Data Security Standard was originally created by Visa (as Payment Application Best Practices – PABP) as an aid to software providers to help build secure payment applications. PA-DSS validation proves that an application can be implemented in a way that is compliant with the PCI DSS.

AbleCommerce has been designed and certified to meet all of the requirements of the PA-DSS version 3.1. This does not automatically make you, the merchant, PCI DSS compliant. It is necessary that the recommendations and instructions in this guide are followed.

For additional information about PA-DSS, or to view AbleCommerce in the official list of validated applications, please visit the URL below.

https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

## *PCI Compliance and Validation*

The PCI Security Standards Council is not a compliance organization. They do not require compliance, but individual payment networks may. Visa is one such example. They require you to comply with the PCI DSS, and you must complete some degree of validation based on the annual transaction volume processed. All merchants who handle Visa payments are required to perform at least some level of validation. The URL below directs you to Visa's Cardholder Information Security Program (CISP) and has complete details and validation procedures.

http://www.visa.com/cisp

A qualified security assessor is the only one who can validate your PCI compliance. A current list of assessors is maintained by the PCI and can be found at this URL:

https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

ControlCase performed the PA-DSS certification for AbleCommerce Gold. They can be contacted via any one of the following:

Control Case, LLC
http://www.controlcase.com/
11700 Plaza America Drive
Suite 810
Reston, VA 20190 USA
Phone: 202-450-7781
FAX: 703-738-7241

## *Versioning Methodology*

The version of AbleCommerce described in this document is Gold R11 which is a simplified naming convention, or Release Label, used to easily determine the version of the software that is installed.

The exact version of AbleCommerce Gold R11 is **7.0.91.8643**

We use the following schema for versioning: *Major.Security.Minor.Build*

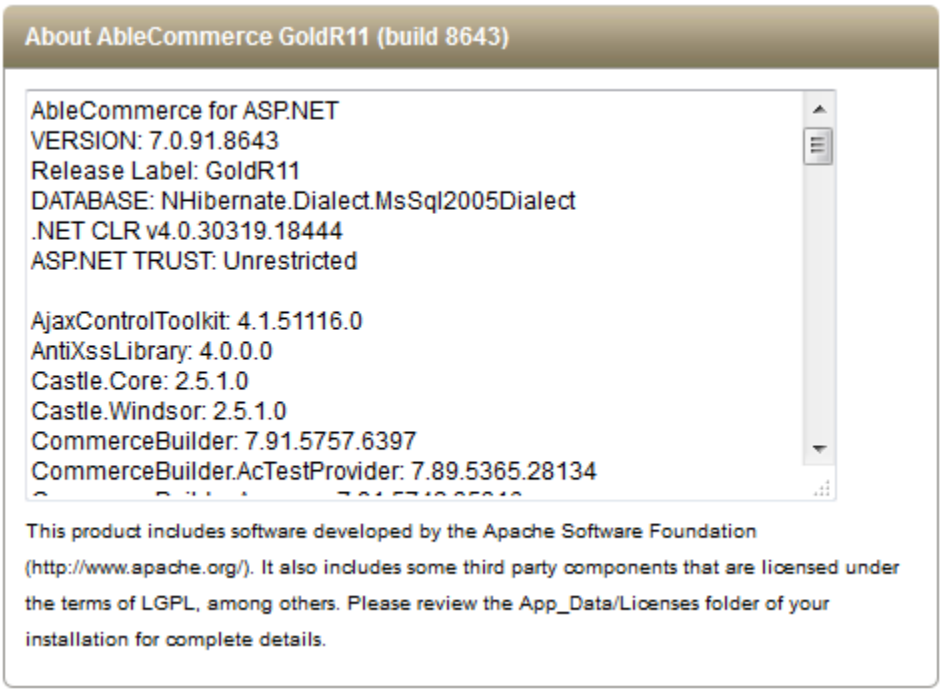
**Major**: If the AbleCommerce software is rewritten, or if methods for encrypting data are changed, the major version will be incremented by 1. A major release could have security impact.

**Security**: If there is a change that has to do with security, or more specifically, a change required by the PCI Data Security Standard council, the security versioning will be incremented by 1.

**Minor**: If new features are added to the software, or defects are fixed, the minor version will be incremented by 1 digit. A minor version update could indicate a security impact.

**Build**: A patch is used to fix a specific defect in the software. Each patch will generate a new build number. A patch fixes a single issue only and may result in a newer version of one or more of the core encrypted source files, and/or specific Asp.Net file(s) needed to fix the issue.

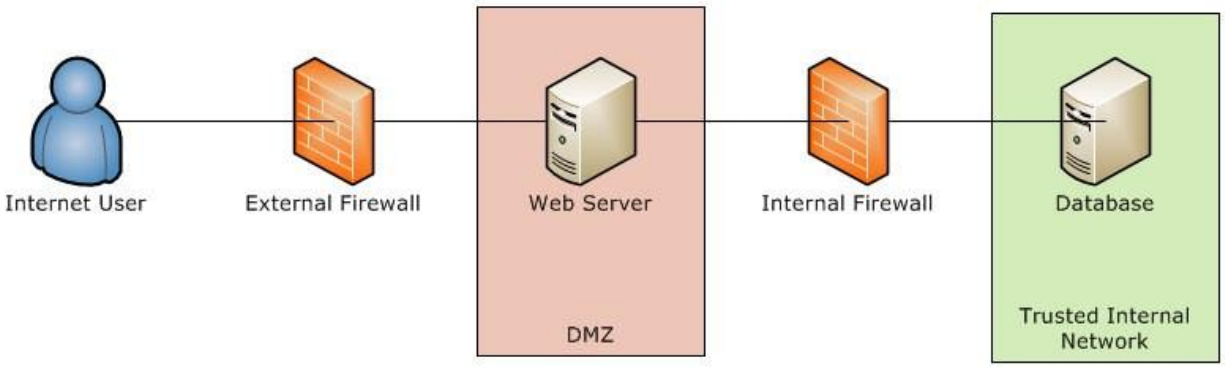
After installation, you can find the exact version and build of AbleCommerce by going to the *Help > About* page from the Merchant Administration.



# Installation of AbleCommerce

## *Server Environment*

To achieve compliance with the DSS, you must ensure that your server environment is properly designed. Among the requirements, you must not store cardholder data on a server that is publicly accessible. It will be necessary to segment your network and use a proper firewall configuration to prevent unauthorized access to your servers. A suitable network configuration is demonstrated in the figure below.




You must not store cardholder data on a server accessible from the Internet in order to remain compliant with the DSS. For example, you should not have your database and web server on the same machine.

Traffic between the DMZ and the trusted internal network is allowed when required for business reasons. You must still use a firewall to filter and regulate this traffic, limit it only to the required protocols and prevent any unnecessary communication. Internet traffic should not be permitted to the internal trusted network.

You should also disable all unnecessary services and protocols on your servers to reduce the possible attack surface. Possible examples may include services like SMTP or FTP, and protocols like NetBIOS.

## *Minimum System Requirements*

The hardware and software requirements for AbleCommerce Gold are as follows:

**Memory:**

- 2 GB for development environment
- 4 GB or higher for production environment

**Operating System:**

- Microsoft Windows 2008 R2, 2012 R2, or 2014 Server
- Microsoft Windows personal computers (optional, for development only)

**Website Software**:

- Microsoft Internet Information Server (IIS) 7.0 or 7.5

**Optional Software**:

- Microsoft Visual Studio (for development and testing purposes only)

**Application Software**:

- Microsoft Asp.Net 4.5.1

**Disk:**

- 70 MB minimum; more depending on storage needs for assets such as images

**Database:**

- A new blank database using either Microsoft SQL Database Server 2008 R2, 2012, or 2014
- Express versions of SQL Server are supported for development and testing only

**Browser:**

- Internet Explorer
- Firefox
- Google Chrome
- Safari
- Mobile Devices

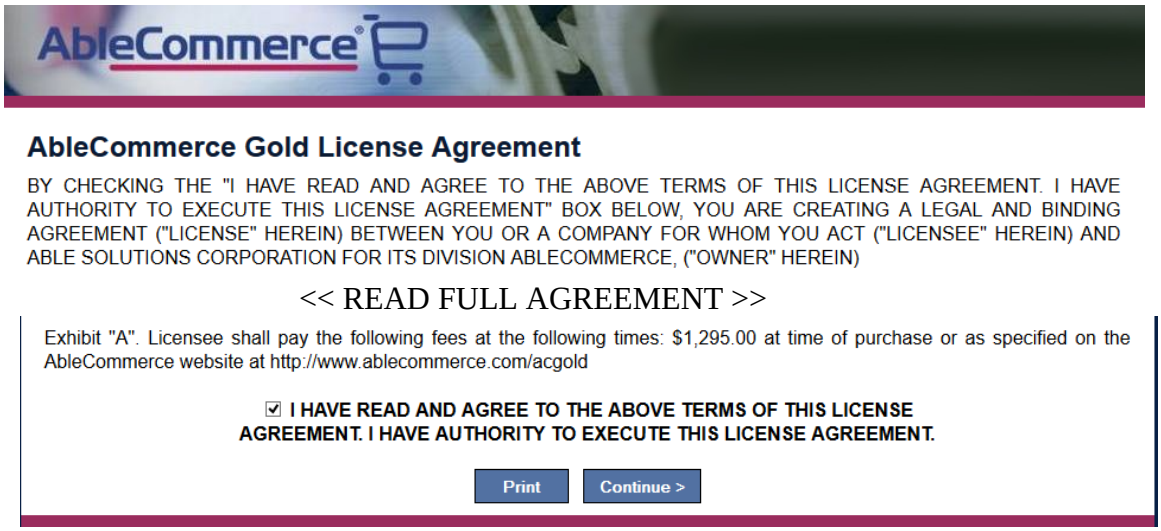
The most recent service packs and security fixes must be applied for the operating system and database. For additional details about recommended minimum system requirements refer to the AbleCommerce online help documentation at http://help.ablecommerce.com

## *Application Deployment*

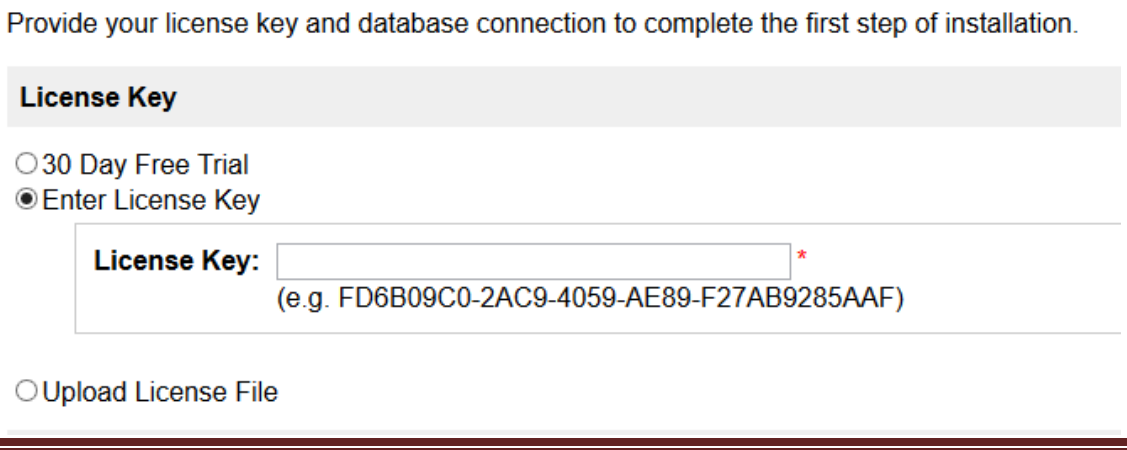
Follow the standard procedure for deployment of the application files to the web server.

1. Copy all program files to the desired location in your website.
    a. (Optional) Open the AbleCommerce.sln file with a development application like Visual Studio to load the application on your local computer.
    b. Open the **default.aspx** page located in the **/install/** folder using a web browser.

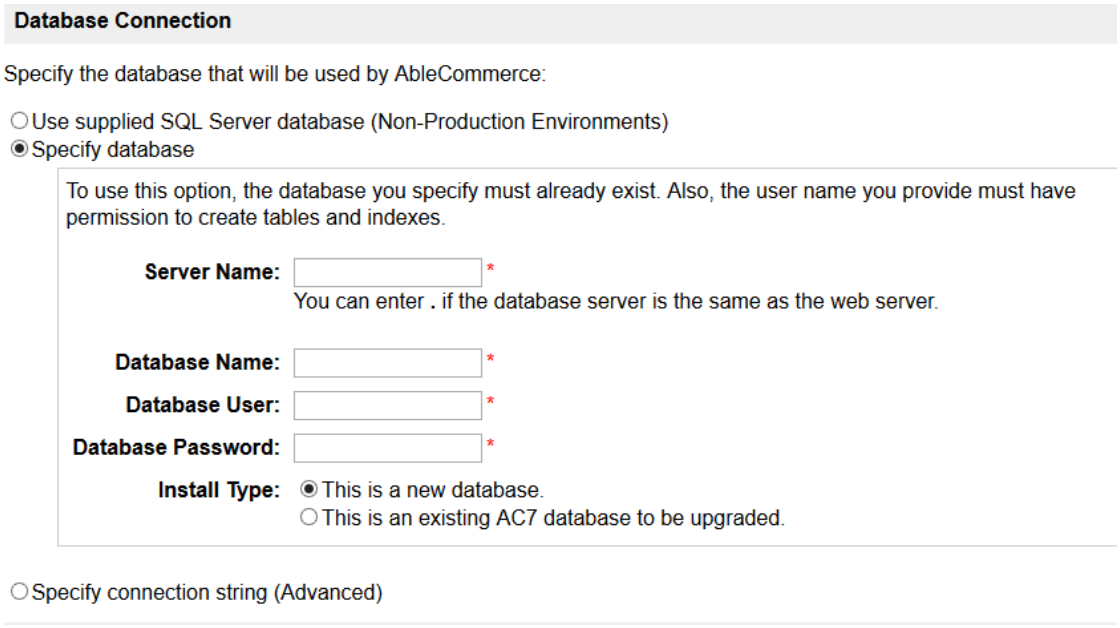
2. Begin the web-based installation by reading the license agreement.




3. You must check the box to accept the terms of the license agreement and continue.
4. On the next page, you will need to enter a license key or use the 30 Day Free Trial Option. License Keys requests must be submitted through your order.



5. Next, you will be asked to provide your database connection information which includes the server IP, database name, database user, and password.




You can use this form to provide the SQL username and password for connecting to the database. You should NOT use the "sa" super user account.

NOTE: In a PCI DSS compliant installation, you cannot choose the option to use supplied SQL Server database. That option uses a local user instance of SQL Express, which violates the best practices for database storage. Instead you must have Microsoft SQL Server installed on a separate server that is not accessible from the internet.

6. You may also use Windows authentication (recommended) to connect to the database. To do this, select the option "Specify Connection string (Advanced)"

   For Windows authentication the connection string should take this format:

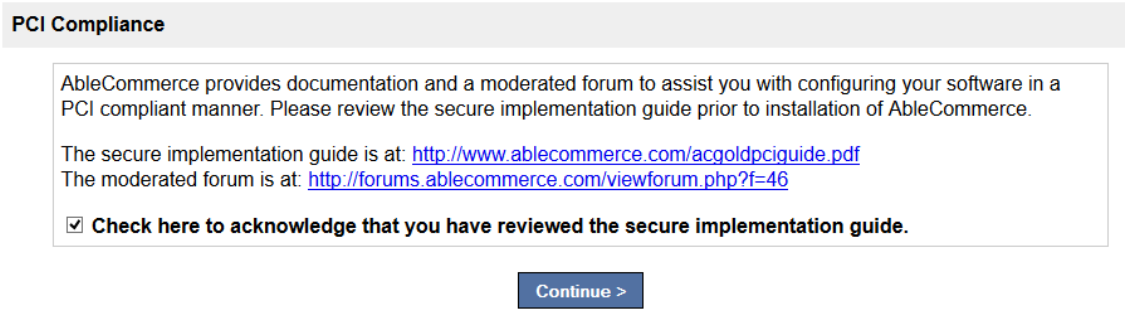
   Server=serverAddress;Database=databaseName;Trusted_Connection=yes;

   When using this method to connect, you must be sure that the user identity of the ASP.NET process has been given permissions to access the database.

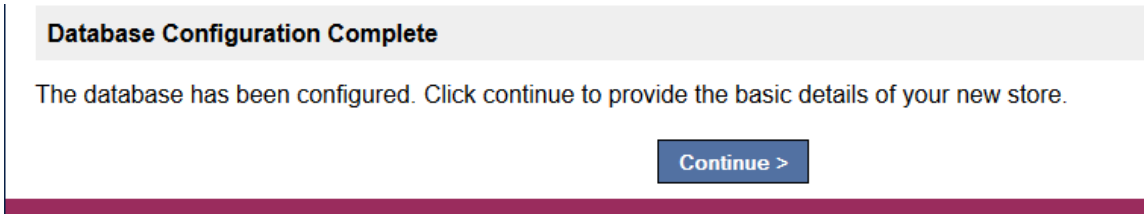
   When you submit the page AbleCommerce will verify a connection can be established to your database. If not, you will remain at the installation screen with an error message that identifies the problem. This provides some measure of protection from supplying invalid credentials.

7. The last section on this page will ask you to review this secure implementation guide. You should download the referenced PDF so you will always have it available. There is also a link to our moderated forum where you can ask specific questions relating to PCI compliance.

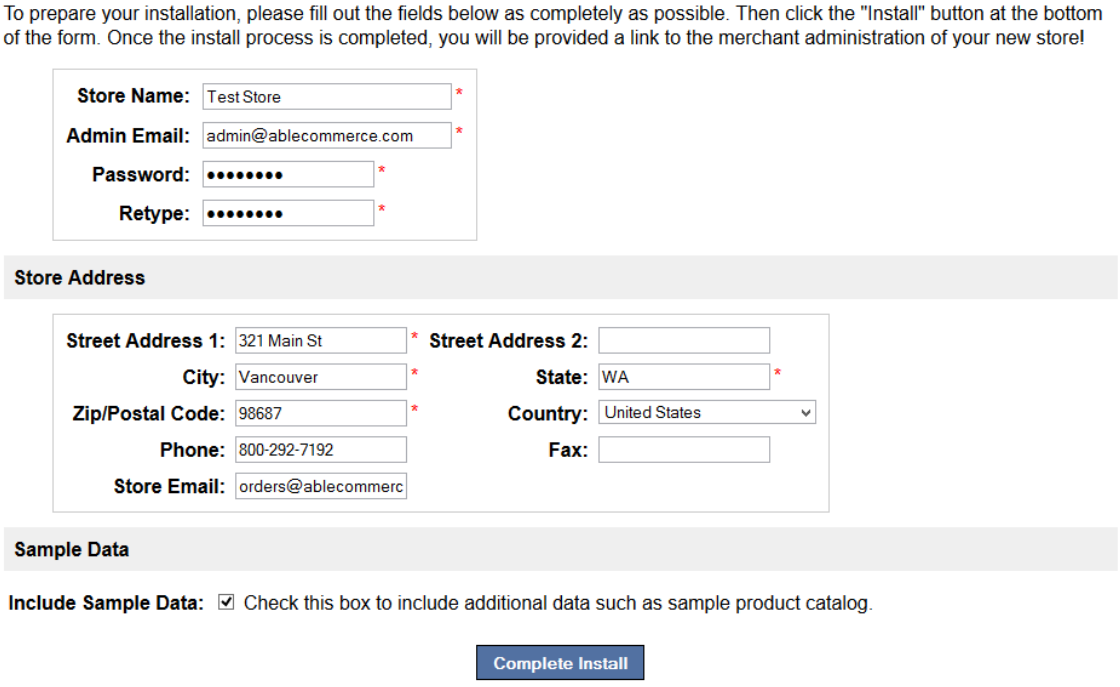
Check the box to acknowledge and press Continue.




8. The next step of the installation will be configuration of the database.



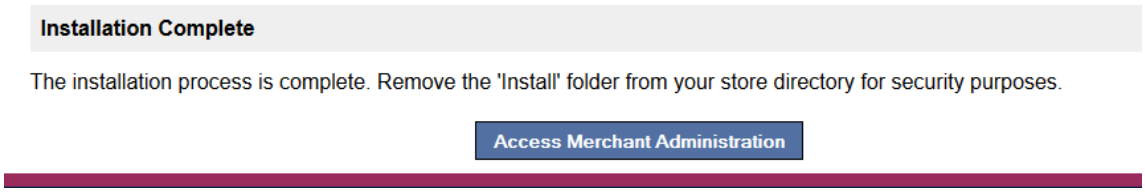

9. When this is completed, press Continue.
10. Proceed to the second part of the web-based installation. You will be asked to provide the admin email and initial password, as well as your information to setup your store. Required fields are indicated by a red astericks.




At this stage, there is no password policy in force. It is your responsibility to choose a strong initial password for this admin user. At a minimum, it should be 7 characters long and use a mix of upper and lower alphabetic and numeric characters. This user

will become a member of the “super user” account having access to every page within the application, including audit logs and encryption keys.

11. Press the Complete Install button when finished.




12. Press the Access Merchant Administration button to complete the web-based installation. This will redirect you to the Merchant Menu login page.


13. Use your admin email and password to login.

Application deployment is complete and you can now move on to post-deployment configuration.

# Post-Deployment Configuration

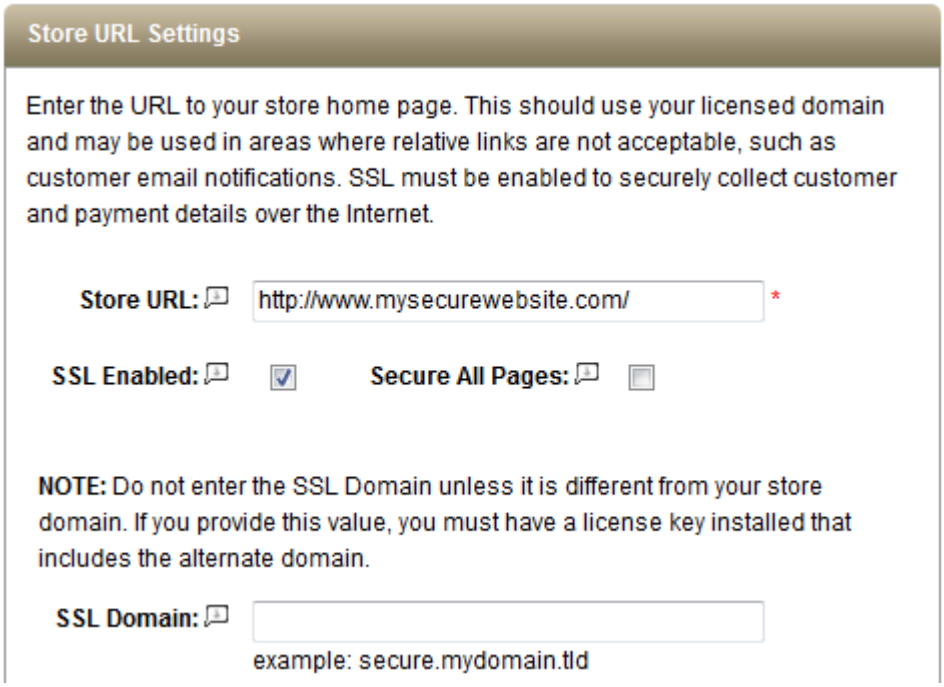
## *Enable Secure Sockets Layer (SSL)*

SSL protects data that is transmitted between a browser and your web server. It is critical that you have SSL enabled on your web server, and this should be among the first steps taken after deployment. You will need to have a certificate issued for a domain that is included in your AbleCommerce license. Usually this is the same as the store domain.

AbleCommerce does not support any production installation that does not have SSL enabled. Additionally, our application will never display credit card details, even to super users, unless SSL is enabled.

To meet the requirements of PCI DSS 3.1, you must enable TLS 1.1 or higher. To do this, you may want to reference this website https://www.nartac.com/Products/IISCrypto/. IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Servers. Additionally, the PCI Security Council has provided a supplemental guide for information on Migrating from SSL and early TLS here - https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf

Enabling SSL on the web server is outside the scope of this guide. Once your web server is properly configured, you must enable the feature within AbleCommerce. Access the merchant administration and go to Configure -> Security -> System Settings.



The SSL configuration form is demonstrated above. You have the option of using an alternate domain, if your certificate is issued for something other than your regular store domain. When you submit the form it will provide you with a link to test the SSL enabled admin. You should verify the test link to ensure you do not lock yourself out of the admin website.

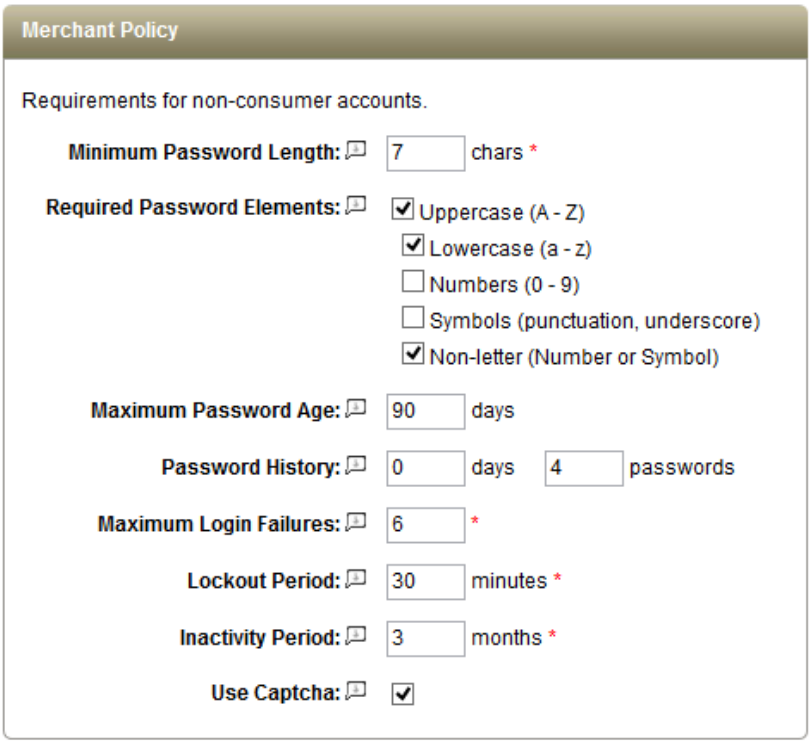
Once SSL is enabled, the admin site will automatically run under the https context. Secure customer areas like login and account settings will also use https so that private data is not transmitted in the clear.

## *Set a Password Policy*

AbleCommerce allows you to specify separate password policies for administrators and consumers. The DSS requirements specify the following minimums for your administrator password policies:

- Minimum of 7 characters
- Must use numeric and alphabetic characters
- Password history should maintain the last 4 passwords
- Passwords must expire at least every 90 days
- Account must be locked after 6 attempts
- Account lockout must last at least 30 minutes or until re-enabled by administrator.

To configure the password policies, access the AbleCommerce merchant admin and go to Configure -> Security -> Passwords. The figure below demonstrates how to configure the policy to meet the minimum requirements:




For DSS compliance you cannot set the policy to anything less restrictive, but for increased security you can make the policy more restrictive than the minimum. For instance you could choose to require a longer password, require non letter characters, or lower the maximum password age.

These password policies also apply to any other applications, systems, and accounts that are related to your cardholder data environment.

## *Additional Password Considerations*

In order to achieve PABP compliance, AbleCommerce Gold has introduced some features that you must be aware of in regards to user accounts:

- User passwords are stored in a one-way SHA1 hash. Passwords cannot be decrypted or recovered, they can only be reset.
- All accounts, including the admin accounts, can become locked out due to too many login attempts or disabled due to inactivity.

Additionally, you are advised to use strong passwords for all other systems and applications, including but not limited to your database passwords and your payment gateway merchant accounts. This also applies to accounts that are not regularly used, such as the default “sa” super- user account within your SQL Server database. Default accounts that are not in use should also be disabled whenever possible.

## *Configure a Payment Gateway*

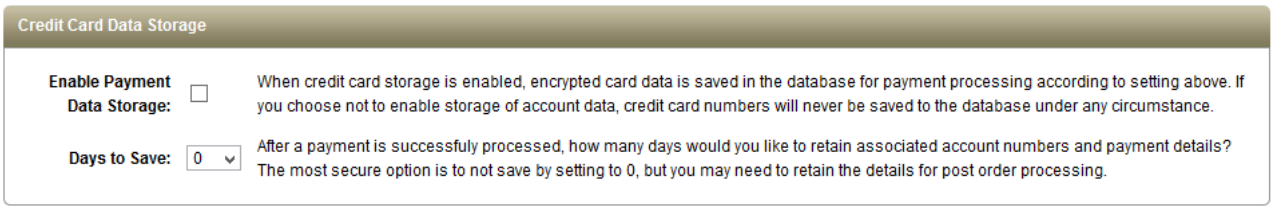
A payment gateway allows AbleCommerce to communicate with third party payment processors to handle credit card and eCheck transactions for your store. Use of a payment gateway will help you avoid the need to store credit card numbers in your database. This is also the only way to gain the benefit of the Card Security Code (CVV2), which helps reduce fraudulent transactions.

To configure a payment gateway, access the merchant administration and go to Configure -> Payments -> Gateways. Then click the "Add Gateway" button. A screen will display all of the gateways that are currently available to be configured. You will need to have a merchant account with one of these third party providers. Click the provider you wish to configure and then enter your merchant account details.

Before you can enable the optional payment storage feature, which will allow the user to store his or her payment profiles, you must have the Authorize.net CIM gateway configured. This is the only payment gateway which supports Recurring Billing Profile management.

## *Disable Credit Card Storage*

The available payment gateways included with AbleCommerce do not require credit card details once a transaction has been successfully authorized. For enhanced security, you should consider disabling card storage all together. This can be accomplished from the merchant administration by going to Configure -> Security -> System Settings. You can uncheck the "Enable Credit Card Storage" box to prevent AbleCommerce from ever storing a card number to your database.



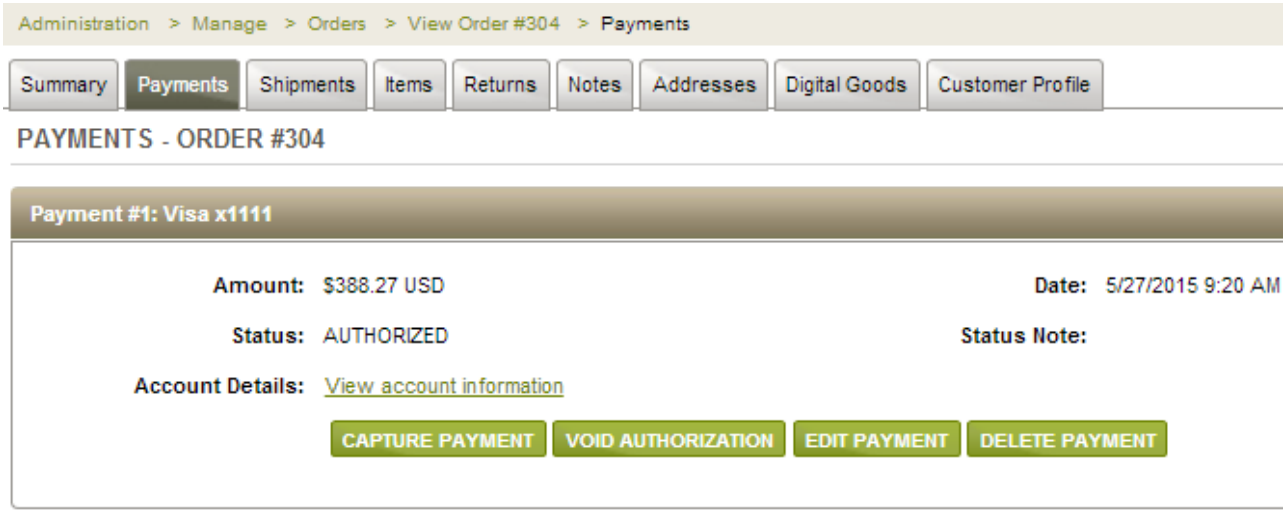

The benefit to this approach is that you gain the security of never recording a customer's card information. However you should be aware of the following:

- If the transaction fails to authorize for any reason, you will not be able to use the "retry" feature from merchant admin as the card data will not be available.
- You cannot access the card data for offline processing – you must have a payment gateway configured if you disable credit card storage.

Be sure to inspect the setting for Account Data Lifespan if you do not disable credit card storage. The recommended value is 0, which means as soon as a payment is completed the encrypted account data will be wiped from the database. AbleCommerce will not allow you to retain the card data longer than 30 days after a payment is completed.

## *Viewing Credit Card Data*

If you choose to store the payment card data, there is a single location where it can be viewed. You must be logged in as a user with minimum permissions of an Order Manager, and view the Payments tab of the Order details page.




Click on the "View account information" link next to Account Details. If SSL encryption is enabled, then you will be shown the Account Name, Number, Expiration Month, and Year. Under no circumstance does AbleCommerce store or show the CVV code.

Additionally, when the View account information link is clicked, a record of this action will be stored in the Audit Log. The user's identity, IP address, date/time, and order reference is logged.

## *Set Encryption Key*

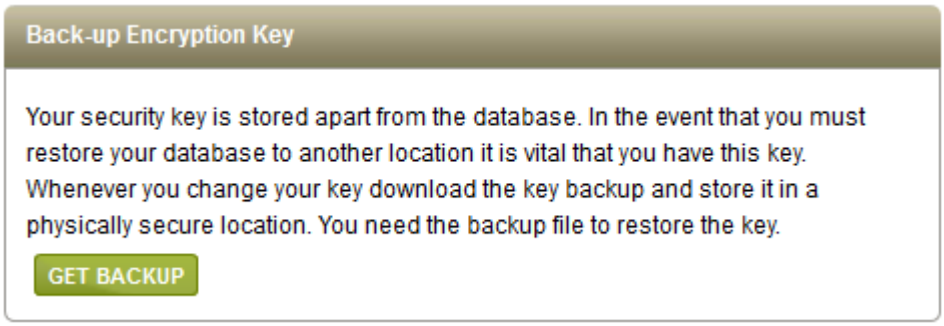
Sensitive data (such as credit card numbers) that must be stored to the database is protected with Advanced Encryption Standard (AES) cryptography. AES is a keyed encryption – you need a secret password to encrypt and decrypt the data. AbleCommerce Gold introduces a new interface for managing this key so that your sensitive data cannot be read by anyone who does not know the key.

When you deploy AbleCommerce, it does not have a key set. If you are storing credit card data it is important that you set the encryption key after deployment. To manage your encryption key you must be logged in as an AbleCommerce super user. Go to Configure -> Security -> Encryption Key to access the key management interface.


To set your encryption key, fill in at least 20 characters of random text. This will help initialize the key generator and produce a unique random key. The default key size is 256 bits using the Rijndael encryption algorithm.

You should change the key at least once per year, but every 90 is recommended.

Whenever you change the key it is very important to create a backup. If your web server crashes, the encrypted data in your database will unrecoverable without a restorable key backup. Once a key is set, the backup form will appear to the right of the Change Encryption Key section:




Click the Get Backup button to display the download links. You must download both key backup file. This should be saved to a physically secure location, for instance recorded to CD and placed in a locked cabinet.

On this same page is a form to restore a key backup. A restore needs to be done if the application is moved to a different web server.

## *Email Security*

As distributed, AbleCommerce does not include credit account details in any of the email notifications. Email is not a secure method of transport and should not be used. Use of unencrypted email could lead to data compromise. Merchants and/or developers implementing AbleCommerce should not attempt to customize this as a feature unless an email encryption solution is also implemented.

## *Audit Log*

AbleCommerce includes security audit logging. This feature is automatically enabled during the installation and cannot be disabled at any time. To view the audit log, you must be logged in as an AbleCommerce super user. Go to Reports -> System -> Audit Log to view the security information being logged.

The Audit log contains a login record of any user with administrative access. You can view the date and time the user logged in, as well as the username (email), and originating IP address. Any attempt at a login will be recorded. This includes all failed logins, password changes, and account lockouts.

If you store credit card information, the Audit log will also show any attempt to view the credit card data which can only be performed securely from the order payment page. In the audit log, a reference will be made to the order number and the administrative user who viewed the information.

# Additional Instructions

## *Employee Training and Monitoring*

The greatest threat to your data comes from your own employees. Be sure to give your employees proper instruction with regard to your policies regarding cardholder data. Create a set of written policies and procedures to keep maintain the integrity of your secure environment. Restrict the number of employees who have access to the cardholder data to only those who have a business need.

In AbleCommerce, all user accesses of credit card data are written to the write only audit log. This log can only be viewed by super user admins. This log can help you monitor employee activities and identify suspicious behavior.

## *Key Management Responsibilities*

Maintaining the encryption key for AbleCommerce is an important task because it impacts the security of your data. Only super users can access the key management interface. As a merchant, you must ensure that users responsible for the encryption key sign a written statement that they understand and accept the duties and responsibilities as custodian(s) of the key. The key custodians should be fully familiar with the requirements of the PCI DSS.

**Secure Key Storage**

Secure key storage encompasses operational storage, backup storage and archival storage. Each of the three respective components plays a vital role in secure key storage for PCI DSS compliance.

Operational storage consists of system components that require immediate access and availability to the key for specific applications within the boundaries of system components as defined by the PCI DSS. These keys, which may be stored locally, must have strong physical security controls and logical security controls. The use of a single authentication and authorization right that could be utilized by multiple users should be prohibited. For users that do have access to keys within the operational storage environment, the system components must have acceptable audit and logging trails enabled and various dual controls as needed.

Backup Storage consists of secure key storage where keys are backed up to a secure and physical source of media, which is independent from the keys used in the operational storage environment. This allows for the retrieval of keys in the event of the operational storage environment being compromised.

Archive Storage consists of the secure key storage where an archive for the keying material shall provide both integrity and access control. Integrity is required in order to protect the archived material from unauthorized modification, deletion or insertion. Access control is needed to prevent unauthorized disclosure.

**Key Custodian Responsibilites**

- Be sure to maintain appropriate key backups and store the backup key securely using the concept of split knowledge and dual control of keys described in the next section.

- Change your key regularly. Every 90 days is recommended.

- You should also change the key any time an employee with access to the key leaves your company.

- Always replace the key if you know or suspect it has been compromised by any means.

**Split Knowledge and Dual Control of Keys**

To comply with PCI DSS requirements, you must adhere to the concept of split knowledge and dual control of keys by ensuring that multiple personnel are required to undertake specific actions and respond to requests regarding effective key management procedures. It should be standard practice within your organization to ensure that a single individual or person does not have full control of the key-management lifecycle. Various persons should be involved in different stages of the following key-management lifecycle activities:

- Key Generation
- Key Distribution
- Key Archiving
- Key Renewal
- Key Retirement
- Key Revocation
- Key Deleting / Destruction
- Key Recovery

Responsibilites for activities above and secure key storage will fall on the Key Custodian or Key Management department.

**Sample Key Custodian Form**

This document is an example Key Custodian form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities. Any user who has access to any encryption keys used in conjunction with the AbleCommerce application must agree and sign a document such as this.

A key custodian is responsible for maintaining the confidentiality and integrity of keys in their custody. A key custodian must protect access to all encryption keys in their custody.

I, _____ , as an employee of _____ hereby agree that I:

1) Have read and understood the policies and procedures associated with key management and agree to comply with them to the best of my ability.

2) Agree to never compromise the security of the keys in my custody by divulging any information about key management practices, related security systems, passwords, or other private information associated with the company's systems to any unauthorized persons.

3) Agree to immediately report any suspicious activity that may compromise key security

Printed Name: _____

Title: _____

Date: _____

Signature: _____

**Retirement and Destruction of Old Keys**

The end of the key life will ultimately result in key deregistration, which is the scheduled process initiated when there is no compelling business requirement (legal or compliance) for retaining the keys.

When copies of the encrypted keys are made, care should be taken to provide for their eventual destruction. All copies of the key backups shall be destroyed once they are no longer required (e.g. for archival or reconstruction activity) in order to minimize the risk of a compromise. Any media on which the encrypted key backup is stored shall be erased in a manner that removes all traces of the keying material to preclude its recovery by either physical or electronic means.

**Replacement of Known or Suspected Compromised Keys**

If a key has been compromised, it must be expeditiously and properly revoked in a manner that will mitigate or eliminate the impact on the cardholder environment or any supporting system components.

The process for compromised keys includes immediate removal of all instances of keys that have been affected. This includes keys in operational storage and usage. Immediately replace affected key with a new key that allows business operations to continue as normal.

## *Purging Old Cardholder Data*

Once you have established your cardholder retention period, you will need to purge any database backups of the credit card numbers that no longer fall into this timeframe. The credit card account number is stored in the database, within a table named "ac_Payments" and in a column named "EncryptedAccountData".

Instructions on purging data can be found at the page below –

http://help.ablecommerce.com/index.htm#faqs/ablecommercegold/how_do_i_remove_sensitive_credit_card_data_.htm

## *Wireless Communications*

If you use wireless networking to access sensitive card holder data, it is your responsibility to ensure your wireless security configuration follows the PCI DSS requirements.

- Personal firewall software should be installed on any mobile and employee-owned computers that have direct access to the internet and are also used to access your network.
- Change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.
- Encrypt wireless transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS.
- Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:
    - Use with a minimum 104-bit encryption key and 24 bit-initialization value
    - Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
    - Rotate shared WEP keys quarterly (or automatically if the technology permits)
    - Rotate shared WEP keys whenever there are changes in personnel with access to keys
    - Restrict access based on media access cod e (MAC) address.
- Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny any traffic from the wireless environment or to control any traffic if it is necessary for business purposes.

## *Access Control*

You must carefully control access to cardholder data. This covers all places where sensitive data may be stored, including databases, servers, and PCs. Follow these rules:

- Always provide unique usernames for each person who needs access.
- Always use strong passwords that meet the requirements of the PCI DSS.

## *Remote Access*

If you enable remote access to your network and the cardholder data environment, you must implement two-factor authentication. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates. You should make sure that any remote access software is securely configured by keeping in mind the following:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses
- Use strong authentication or complex passwords for logins
- Enable encrypted data transmission
- Enable account lockout after a certain number of failed login attempts
- Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed
- Enable any logging or auditing functions
- Restrict access to customer passwords to authorized reseller/integrator personnel
- Establish customer passwords according to PCI DSS requirements 8.1, 8.2, 8.4, 8.5

## *Non-Console Administrative Access*

If you use tools to remotely access the application, you should encrypt all communication with technologies like SSH, VPN, or SSL/TLS. For example, Microsoft Terminal Services can be configured to use encryption and this should be set to the “high” level. This will ensure that the RDP data is bi-directionally encrypted with a 128 bit key.

## *Encrypted Config Files*

The database.config and encryption.config files are saved in an encrypted form, so that your connection string and encryption key remain protected. If you are installing AbleCommerce to a web farm or clustered environment, you must take additional steps so that this file encryption will work properly. The standard AbleCommerce installation guide contains details on how to implement the application in a clustered environment.

## *Notes for Integrators*

If you are a third party developer who integrates with AbleCommerce or customizes it on behalf of others, you may have occasions where it is necessary to troubleshoot a problem with one of your clients. In these events, please note the following:

- Sensitive authentication data should only be collected when needed to solve a specific problem.
- Sensitive data should be stored in specific, known locations with limited access.
- Only collect the minimum amount of data needed to solve the problem.
- Sensitive data must be encrypted while it is stored
- Sensitive data must be securely deleted immediately after use

## *Application Debug Logging*

Payment gateway integrations provided by AbleCommerce all support optional application debug logging. The debug log files generated by our integrations never include sensitive card data. Sensitive data such as credit card number and CVV2 are redacted. Third party developers who create new payment integrations are strongly advised to follow the same procedure. Debug logs must not contain sensitive data in order to achieve PCI DSS compliance.

## *Log File Location and Off-site Storage*

The **general application log files** are created and saved to the “app.log” file within the \Website\App_Data\Logs\folder. This log file stores error messages and warnings that are only applicable to the general use of the software.

The **security audit log files** are created and saved to the “audit.log” file within the \Website\App_Data\Logs\folder. This log file only stores information about security issues related to viewing of payment data, account lockouts, and admin users.

If you want to store your security audit log files to a centralized log server, use the following steps:

1. From your Microsoft SQL database server, use Microsoft scheduler to create a batch file that will run with the following command.

```
bcp "SELECT  databasename.tableowner.AuditEventId, StoreId, EventDate,
EventTypeId, Successful, UserId, RelatedId, RemoteIP, Comment FROM
ac_AuditEvents WHERE     (EventDate > DATEADD(dd, - 1, GETDATE()))"
queryout ablecommerce_auditlog.txt -c -T
```

For more information on this command see:
https://technet.microsoft.com/en-us/library/ms189569%28v=sql.105%29.aspx

For information on task scheduler see the following:
https://technet.microsoft.com/en-us/library/dd834883.aspx

2. To copy this file to a remote location using the task scheduler, create a batch file using the commands below. This will copy the data to a remote location and increment the file number to preserve older copies.

```
@echo off
set Source=C:\test\ablecommerce_auditlog.txt
set Destination=E:\remote\ablelogs
set Filename=ablecommerce_auditlog
set a=1

:loop
if exist %Destination%\%Filename%(%a%).txt set /a a+=1 && goto :loop
copy %Source% %Destination%\%Filename%(%a%).txt
pause
```

## *Service Releases*

From time to time, the software will need to be patched to correct any new issues that arise. These patches will be distributed to AbleCommerce customers for free. You should visit http://help.ablecommerce.com/index.htm#upgrades/acgold/hot_patches_gold.htm for the latest information and downloads. From the linked page above, you can enter your email address to be notified of any new updates.

Additionally, AbleCommerce has a dashboard alert system where any issue of importance will be published. To view the dashboard, simply login to the Merchant Menu and view the section named “Software News Feed” from the main Dashboard page.

You may also sign-up for our “Software Support and News” mailing list by logging into your AbleCommerce account and adding the option to your user profile.

## *System Hardening*

System hardening is the process of securely configuring computer systems, to eliminate as many security risks as possible. While default security configurations for many products have improved greatly over the years, some options and settings favor ease of use over security, exposing vulnerabilites that can be used to compromise a system. The resources below offer guidance on secure configurations and hardening procedures.

To help those that are not security experts, a number of security organizations have established system-hardening guidelines and recommendations, which advise how to correct these weaknesses. Examples of sources for guidance on configuration standards include, but are not limited to:

www.nist.gov – National Institute of Standards Technology (NIST)
www.sans.org – SysAdmin Audit Network Security (SANS) Institute
www.cisecurity.org – Center for Internet Security (CIS)
www.iso.org – International Organization for Standardization (ISO)

System configuration standards must be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.

**Additional Resources:**

The following resources relate specifically to securing Windows servers that meet the minimum system requirements of AbleCommerce Gold software for PCI compliance.

Windows Servers 2008 or 2012

- Hardening the Microsoft Windows Server 2008 operating system - https://technet.microsoft.com/en-us/library/Cc995076.aspx
- Server Hardening: Windows Server 2012 https://technet.microsoft.com/en-us/security/jj720323.aspx
- Configure Web Server Security (IIS7) https://technet.microsoft.com/en-us/library/Cc731278(v=WS.10).aspx
- Security in the .NET Framework https://msdn.microsoft.com/en-us/library/fkytk30f(v=vs.110).aspx
- Securing SQL Server v 2008 R2 https://msdn.microsoft.com/en-us/library/bb283235(v=sql.105).aspx
- Securing SQL Server v 2012 https://msdn.microsoft.com/en-us/library/bb283235(v=sql.110).aspx
- Securing SQL Server 2014 https://msdn.microsoft.com/en-us/library/bb283235(v=sql.120).aspx

## *System Inventory*

PCI DSS 3.1 requires that organizations must **maintain an inventory of system components that are in the scope of PCI DSS**. System components include network devices, computing devices, and applications. This includes virtual components such as virtual machines, virtual switches/routers, etc.

Included within this documentation should be a description mapped to each piece of hardware and software components detailing its function and usage. Depending on the size of the organization, keeping an accurate and up-to-date inventory can be a daunting task. Periodic and proactive review and maintenance of system inventories can alleviate some of the stress associated with this requirement, but it is critical that adequate resources be allocated for this task.

**Testing Procedures:**

- Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.

- Interview personnel to verify the documented inventory is kept current.