

AbleCommerce v7.0

**Secure Implementation Guide
PA/PCI DSS v1.2**



**Revision: 1.3
April 30, 2010**

Copyright

©2010 Able Solutions Corporation. All rights reserved.

AbleCommerce is a division of Able Solutions Corporation. CommerceBuilder is a registered trademark of Able Solutions Corporation.

The information contained herein is supplied without representation or warranty of any kind, is subject to change without notice and does not represent a commitment on the part of Able Solutions Corporation.

Able Solutions Corporation, therefore, assumes no responsibility and shall have no liability, consequential or otherwise, of any kind arising from this material or any part thereof, or any supplementary materials subsequently issued by Able Solutions Corporation.

We have made every effort to ensure the accuracy of this material. If you have any questions or comments, please contact us using one of the methods below.

AbleCommerce.com

PO Box 873249

Vancouver, WA

98687-3249

Phone: 1-360-571-5839

Toll Free: 1-866 -571-5888 (USA Only)

Fax: 1-360-546-3532

Email: info@ablecommerce.com

Web: <http://www.ablecommerce.com>

Revision History

Revision 1.2 – April 30, 2010

- Updated example network configuration to make the implied firewall between web server and database more apparent.
- Updated to reflect PA/PCI DSS version 1.2.
- Updates to System Requirements

Revision 1.1 – March 3, 2009

- Reviewed; no changes to guide implemented.

Revision 1.0 - February 19, 2008

- Initial publication.

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

Introduction

Scope and Target Audience

This guide covers AbleCommerce 7.0, 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 by 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 1.2 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 1.2. 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

Chief Security Officers performed the PA-DSS certification for AbleCommerce 7.0. They can be contacted via any one of the following:

Chief Security Officers

<http://chiefsecurityofficers.com/>

9821 N. 95th Street, Suite 105

Scottsdale, AZ 85258

Phone: 888-237-3899

FAX: 480-275-4818

Email: info@chiefsecurityofficers.com

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.

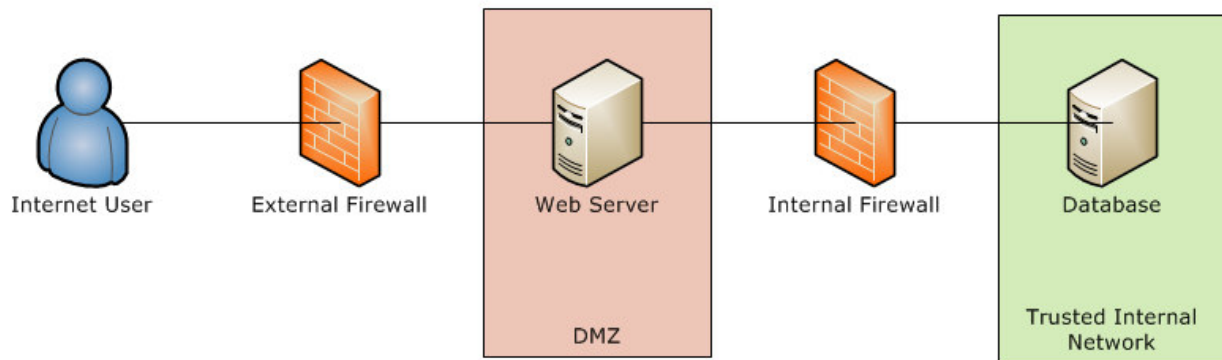


Figure 1 - Server Environment

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 7.0 are as follows:

Memory:

- 1 GB for development environment
- 2 GB or higher for live environment

Operating System:

Microsoft Windows 2000, 2003, or 2009 Server

Disk:

50 MB minimum, more depending on storage needs

Database:

Microsoft SQL Server 2000, 2005, or 2008
(Express versions of SQL Server are supported.)

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 this URL:

<http://help.ablecommerce.com>

Application Deployment

Follow the standard procedure for deployment of the application files to the web server. When you reach the web based installation you will be asked to provide your database connection information.

Database Connection

Specify the database that will be used by AbleCommerce:

Specify database

To use this option, the database you specify must already exist. Also, the user name you provide must have permission to create tables and indexes.

Server Name:
You can enter . if the database server is the same as the web server.

Database Name:

Database User:

Database Password:

Database Type:

Specify connection string (Advanced)

Use supplied SQL Server 2005 database

Figure 2 - Specify Database Connection

In a PCI DSS compliant installation, you cannot choose to use the supplied SQL Server 2005 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.

The screen shown in Figure 2 above is used if your database is set up to accept SQL Logins. 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.

You may also use Windows authentication (recommended) to connect to the database. To do this, select to specify the connection string:

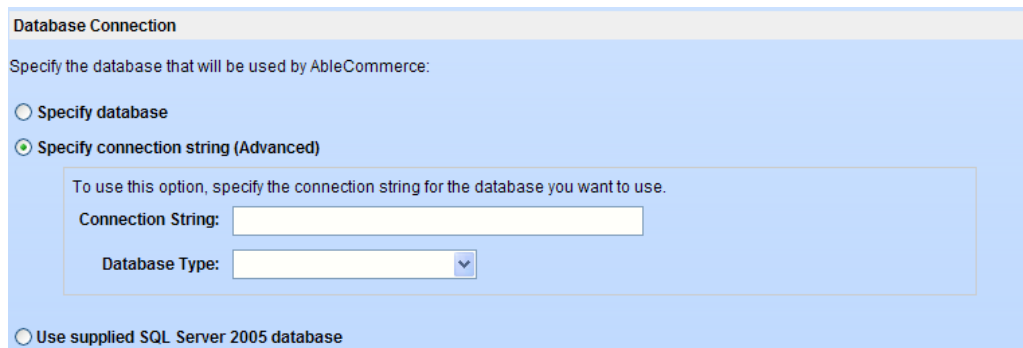


Figure 3 - Specify Connection String

For Windows authentication the connection string should take the format of:

```
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.

When you proceed to the second page of the web based installation, you are asked to provide the admin email (username) and initial password:

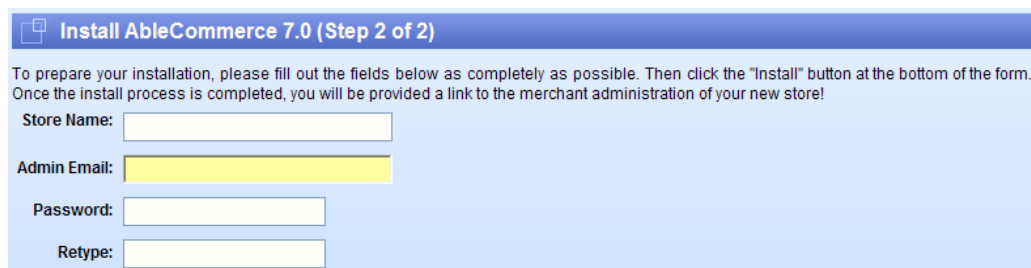


Figure 4 - Create Admin Account

For the “Admin Email” field, pick an email address that will be created as the super user for the application. This user will have complete access to the application, including encryption keys and audit logs.

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

Once you submit the second step of web based installation, application deployment is complete and you can 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.

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 -> General.

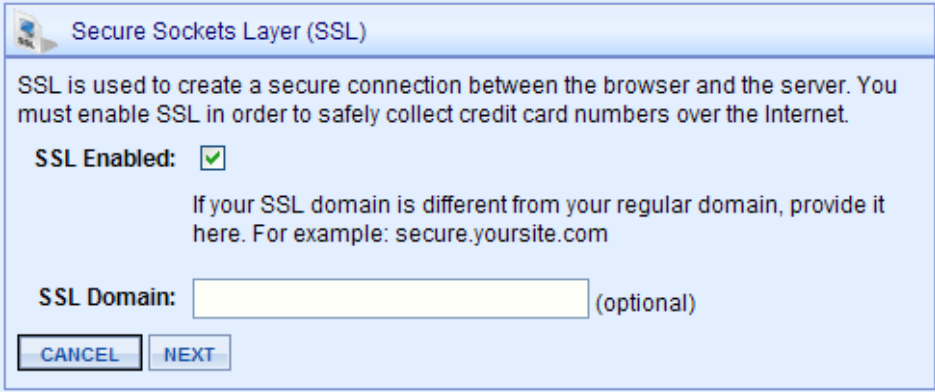


Figure 5 - Enable SSL

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 -> Password Policy. The figure below demonstrates how to configure the policy to meet the minimum requirements:

The screenshot shows the 'Merchant Policy' configuration window for non-consumer accounts. The settings are as follows:

Setting	Value	Unit
Minimum Password Length	7	chars
Required Password Elements	<input checked="" type="checkbox"/> Uppercase (A - Z) <input checked="" type="checkbox"/> Lowercase (a - z) <input checked="" type="checkbox"/> Numbers (0 - 9) <input type="checkbox"/> Symbols (punctuation, underscore) <input type="checkbox"/> Non-letter (Number or Symbol)	
Maximum Password Age	90	days
Password History	0 days, 4	passwords
Maximum Login Failures	6	
Lockout Period	30	minutes
Inactivity Period	3	months

A 'SAVE CHANGES' button is visible in the bottom right corner.

Figure 6 - Minimum Password Policy

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 7.0 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.

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 -> General. 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:

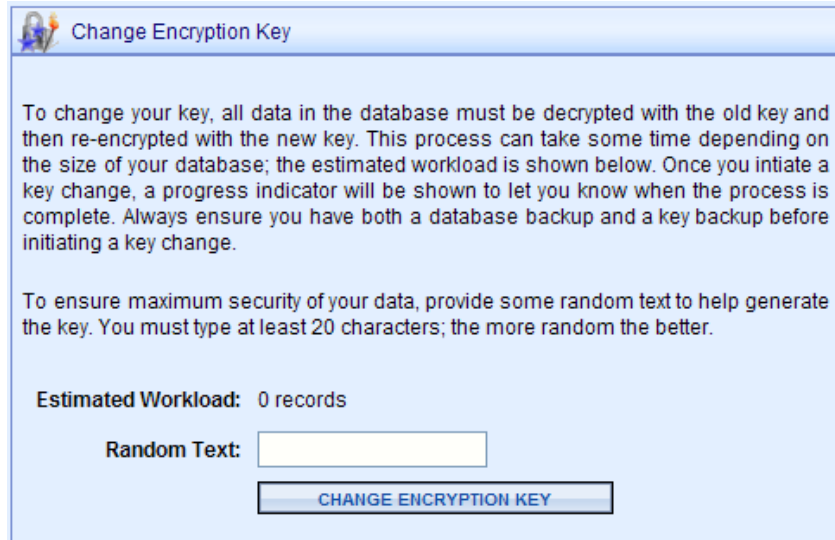
- If the transaction fails to authorize for any reason, you will not be able to use the “retry” feature from merchant admin as the card data will not be available.
- You cannot access the card data for offline processing – you must have a payment gateway configured if you disable credit card storage.

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.

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 7.0 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.



Change Encryption Key

To change your key, all data in the database must be decrypted with the old key and then re-encrypted with the new key. This process can take some time depending on the size of your database; the estimated workload is shown below. Once you initiate a key change, a progress indicator will be shown to let you know when the process is complete. Always ensure you have both a database backup and a key backup before initiating a key change.

To ensure maximum security of your data, provide some random text to help generate the key. You must type at least 20 characters; the more random the better.

Estimated Workload: 0 records

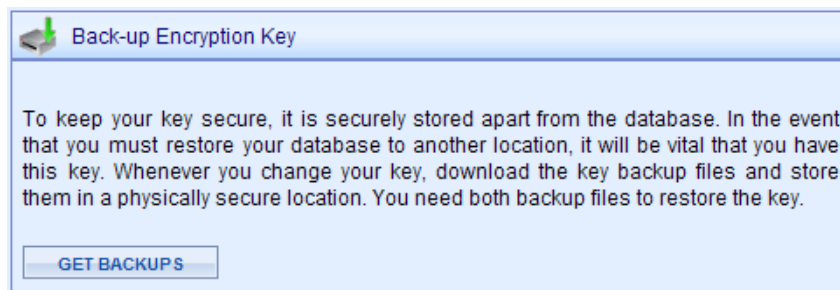
Random Text:

[CHANGE ENCRYPTION KEY](#)

Figure 7 - Set Encryption Key

To set your encryption key, fill in at least 20 characters of random text. This will help initialize the generator and produce a unique random key. You should change the key at least once per year.

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:



Back-up Encryption Key

To keep your key secure, it is securely stored apart from the database. In the event that you must restore your database to another location, it will be vital that you have this key. Whenever you change your key, download the key backup files and store them in a physically secure location. You need both backup files to restore the key.

[GET BACKUPS](#)

Figure 8 - Backup Encryption Key

Click the Get Backups button to display the download links. You must download both key backup files. They 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.

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.

Also be sure to maintain appropriate key backups and store the backup keys securely. AbleCommerce provides for the key backup to be split into two parts so that you may have two people each retain part of the key. This would prevent any one person from being able to reconstruct the entire key.

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.

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 code (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

Debug Logging

Payment gateway integrations provided by AbleCommerce all support optional 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.