

AbleCommerce®

Secure Implementation Guide

for

PCI DSS 3.2.1
Compliance

Version 9.0

Revision: 1.0

April 30th, 2019



GO GREEN! Please don't print this document.

Copyright

© 2018-2019 Able Solutions Corporation. All rights reserved.

AbleCommerce 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.

Able Solutions Corporation

Mailing address:

13609 NE 6th Ave
Vancouver, WA 98685-2809

Phone: 1-360-571-5839
Toll Free: 1-800-292-7192 (USA Only)
Fax: 1-360-546-3532

Email: info@ablecommerce.com
Website: <http://www.ablecommerce.com>

Revision History

Revision 1.0 – April 30th, 2019

- Initial publication

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

Table of Contents

Copyright	2
Revision History	4
Introduction.....	7
Scope and Target Audience.....	7
PCI Data Security Standard (PCI DSS).....	7
Payment Application DSS (PA-DSS)	8
PCI Compliance and Validation.....	8
Versioning Methodology	9
Installation of AbleCommerce.....	10
Server Environment	10
Minimum System Requirements.....	11
Application Deployment	12
1. Extract Files and start Installation.....	12
2. Configure and Connect to the Database.....	13
3. Download and Review the PCI Secure Implementation Guide	15
4. Create an Admin account and set up store	16
Post-Deployment Configuration	20
Enable SSL (Secure Sockets Layer).....	20
Set the Password Policy	22
Enable CAPTCHA.....	24
To Enable or Disable Google reCAPTCHA	24
Email Server Configuration	26
Setup User Authentication	28
To Enable Multi-Factor Authentication	29
Setup Multi-Factor Authentication for Admin Users.....	30
Login using Multi-Factor Authentication	32
Encryption Key	33
Create the Encryption Key	34
Backup the Encryption Key	35
Restoring an Encryption Key.....	35
Management and Protection of Keys	36
Payment Data Storage.....	36
To Enable Payment Storage	37
To Disable Payment Storage.....	38
Purging Cardholder Data from the Database	38
Processing Credit Card Payments	39
Install a Payment Gateway.....	40
Configure a Payment Gateway.....	40
Using a Customer Information Manager (CIM).....	40
Viewing Payment Data	41
To View Account Information for a Payment.....	42

Audit Logging	43
Find a Card Viewing Event in the Audit Log	43
PCI DSS Requirements and Responsibilities	44
Employee Training and Monitoring	44
Key Management Responsibilities	44
Secure Key Storage	45
Key Custodian Responsibilities	45
Split Knowledge and Dual Control of Keys	45
Key Custodian Sample Agreement	46
Retirement and Destruction of Old Keys	47
Replacement of Known or Suspected Compromised Keys	47
Network Segmentation	48
Wireless Communications	48
Use of Third-Party Service Providers / Outsourcing	49
Remote Access	49
Non-Console Administrative Access	49
Encrypted Files	50
Notes for Integrators	50
Application Debug Logging	50
Log File Location and Off-site Storage	50
Using a Centralized Log Server	51
System Hardening	51
Additional Resources	52
System Inventory	52
AbleCommerce Upgrade Manager	53
Glossary of Terms for AbleCommerce	55

Introduction

Scope and Target Audience

This guide covers the AbleCommerce installation and setup, 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 purpose of the council is to produce and maintain the Data Security Standard (DSS). The DSS is a set of rules and requirements that when followed will help prevent fraud, hacking, and other threats to private cardholder data. The 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 3.2.1 of the PCI DSS.

Payment Application DSS (PA-DSS)

The Payment Application Data Security Standard was 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 3.2.1. The application's certification does not automatically make you, the merchant, PCI DSS compliant. It is also necessary that the recommendations and instructions in this guide be implemented and 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 expect 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, maintained by the PCI, can be found at this website:

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

Dara Security has performed the PA-DSS certification for AbleCommerce. You may contact them using any one of the following methods:

Dara Security

<http://www.darasecurity.com/>

10580 N. McCarran Blvd.

Suite #115-337

Reno, NV 89503 USA

Phone: +1 775-622-5386

Email: info@darasecurity.com

Versioning Methodology

The version of AbleCommerce described in this document is AbleCommerce 9, which is a simplified naming convention used to readily determine the software version that is validated for PA-DSS.

AbleCommerce versioning has four levels: *Major.Minor.Revision.Wildcard*

The exact version of AbleCommerce is **9.0.x.x** where X is a numeric value only.

Major: If AbleCommerce software is rewritten, significantly changed, or if methods for encrypting data change, the major version will be incremented. A major version indicates the version of PA-DSS the application is validated for.

Minor: If new features are added to AbleCommerce, which may simultaneously include several bug fixes, the minor version will be incremented by one digit for each released upgrade. A minor version update may have a security impact requiring a re-certification for PA-DSS.

Revision: Used by the AbleCommerce license manager to determine eligibility for upgrades and patches. A revision update will not have a negative impact on PA-DSS requirements, but it will have a dependency on the installed license key.

Wildcard: These changes increment the build number. Build changes include bug fixes and have no negative impact on PA-DSS requirements.

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

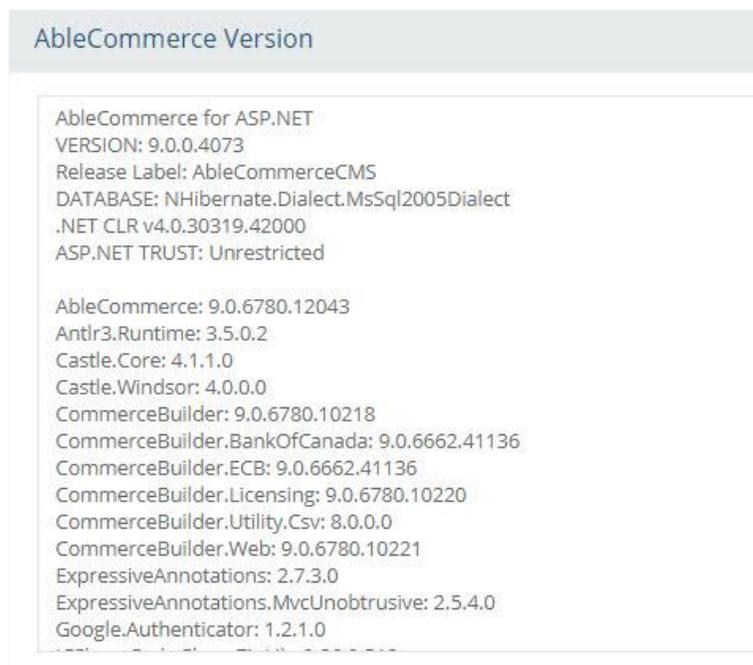
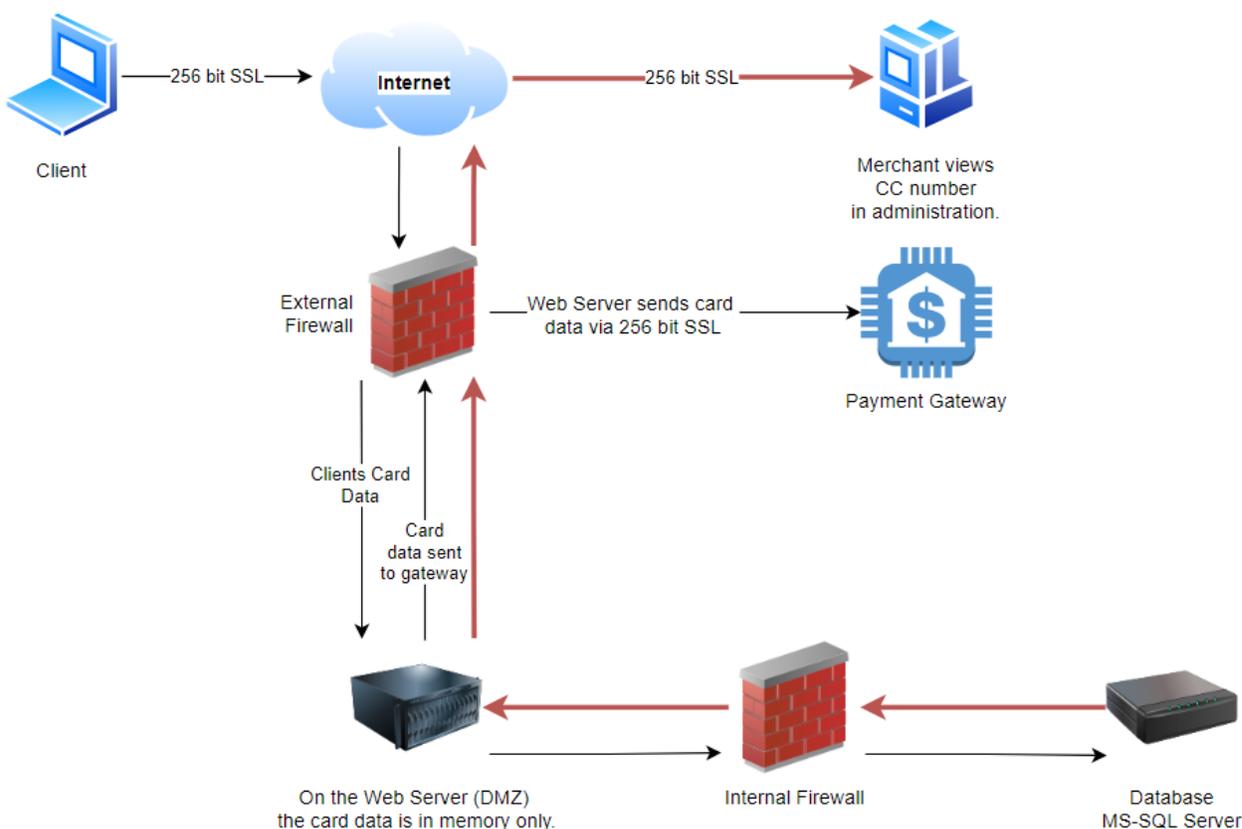


Figure 1 - About AbleCommerce

Installation of AbleCommerce

Server Environment

To achieve compliance with the DSS, you must ensure that your server environment is designed and implemented correctly. 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 and card data flow configuration is demonstrated in the figure below.



Card data is stored to database server when card data storage is set to 1 or more days.

You must not store cardholder data on a server accessible from the Internet 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 are as follows:

Memory

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

Operating System

- Microsoft Windows 2008 R2, 2012 R2, 2016, 2019 Server
- Microsoft Windows personal computers (optional; for development only)

Website Software

- Microsoft Internet Information Server (IIS) 7.0, 7.5, or 8.0

Optional Software

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

Application Software

- Microsoft Asp.Net 4.6.2

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, 2014, 2016, or 2017.
- 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 to the operating system and database. For additional details about recommended minimum system requirements refer to the AbleCommerce online help site and documentation at <http://help.ablecommerce.com>

Application Deployment

Follow the standard procedure for a new deployment of the AbleCommerce application to a web server and SQL server.

1. Extract Files and start Installation

Once the application files are placed in the website, the installation is completed by accessing the IP or domain.

- a) Copy the extracted application to the root folder of your website.

The root folder is also called the document root. It is the folder where the website files for a domain name are stored.
e.g. c:\inetpub\wwwroot\{copy application files and folders starting here}\website\

- b) Open a browser and access your website URL.

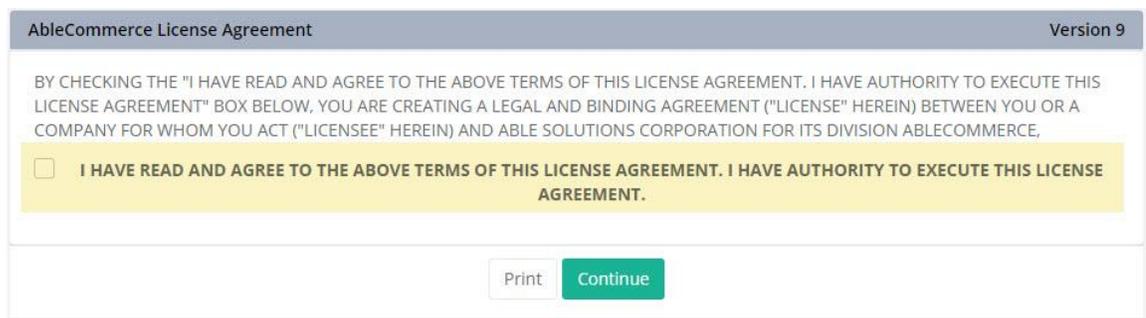
The installation will launch automatically.
e.g. http://my-website.xyz

- c) Select the type of the installation.



The image shows a dialog box titled "Installation Options". It contains two radio button options: "Install a development version (key not required)" which is selected, and "Install with a license key".

- d) The license agreement page will be shown. Please read the agreement and print if needed.



The image shows a dialog box titled "AbleCommerce License Agreement" with "Version 9" in the top right corner. The main text reads: "BY CHECKING THE 'I HAVE READ AND AGREE TO THE ABOVE TERMS OF THIS LICENSE AGREEMENT. I HAVE AUTHORITY TO EXECUTE THIS LICENSE AGREEMENT' BOX BELOW, YOU ARE CREATING A LEGAL AND BINDING AGREEMENT ('LICENSE' HEREIN) BETWEEN YOU OR A COMPANY FOR WHOM YOU ACT ('LICENSEE' HEREIN) AND ABLE SOLUTIONS CORPORATION FOR ITS DIVISION ABLECOMMERCE,". Below this text is a yellow highlighted box containing a checkbox and the text: "I HAVE READ AND AGREE TO THE ABOVE TERMS OF THIS LICENSE AGREEMENT. I HAVE AUTHORITY TO EXECUTE THIS LICENSE AGREEMENT." At the bottom of the dialog box are two buttons: "Print" and "Continue".

- e) When finished, check the box to accept the terms of the license agreement.
- f) Press the **Continue** button.

2. Configure and Connect to the Database

A license key is not required for the installation. You may choose to install a free developer version.

- a) In the **License Key** section, enter a production license key, or select the option to use the free development version.

Registration

Register for developer version

Install a License Key

License Key

Enter a development or production license. [Login to your account](#) and request a license key through your online order invoice.

If you are behind a firewall and unable to access the [ablecommerce.com](#) website for key registration, then request a pre-registered key. For more information, see [installing license keys](#).

Upload License File

- b) In the **Database Connection** section, provide the required elements to connect to a new blank database.

Specify a database

To use this option, the database you specify must already exist as a new blank database, or one that is compatible for upgrade. Also, the database user provided must have permission to create or modify tables and indexes.

Server Name
 *

You can enter a period (.) if the database server is on the same server.

Database Name
 *

Database User
 *

Database Password
 *

Install Type:

This is a new (blank) database.

This is an existing AbleCommerce Gold database to be upgraded.

There are two database connection options available:

OPTION 1 - Use SQL Server Authentication

If you have a database and SQL Server Authentication login, select the “Specify database option” and enter the following information into the fields provided:

- Server Name – enter the database server name or IP address
- Database Name – enter the name of the new blank database
- Database User – enter the SQL server authentication username
- Database Password – enter the password for the user above.

OPTION 2 - Use Windows Authentication (recommended)

To connect using Windows authentication, select the option “Specify Connection string (Advanced)” and enter the database connection string.

The connection string should take this format:

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

When using the Windows Authentication method to connect, make certain that the user identity of the ASP.NET process has been given permissions to access the database.

- c) Select the default option for **Install Type**: This is a new (blank) database

Connecting to the Database
Best Practices for PCI Compliance

Database Location

In a PCI DSS compliant installation, you cannot choose the option to use the supplied SQL Server database. That option uses a local user instance of SQL Express, which violates the best practices for database storage.

You must have Microsoft SQL Server installed on a separate server that is not accessible from the internet.

Database Login

Using SQL Server Management Studio, create a login and authorize that login to access a database as a user. Logins can be either Windows Authentication logins, which use credentials from Windows, or SQL Server Authentication logins, which store the authentication information in SQL Server and are independent of your Windows credentials. Use Windows Authentication whenever possible.

You should NEVER provide the credentials of the “sa” superuser account to connect.

3. Download and Review the PCI Secure Implementation Guide

In the PCI Compliance section, a link is provided to this guide. Download and keep this secure implementation guide for reference. A link to the AbleCommerce moderated forum is also shown. Use the forum to ask specific questions relating to PCI-DSS compliance.

Payment Card Industry (PCI-DSS) Compliance

AbleCommerce provides documentation and a moderated forum to assist you with configuring your software in a PCI compliant manner. Please review the secure implementation guide prior to installation of AbleCommerce.

The secure implementation guide is at: [http://www.ablecommerce.com/AbleCommerce Secure Implementation Guide.pdf](http://www.ablecommerce.com/AbleCommerce%20Secure%20Implementation%20Guide.pdf)

The moderated forum is at: <https://www.ablecommerce.com/forums/topics/3-PCI-Certification-and-Implementation-Questions>

Check here to acknowledge that you have reviewed the secure implementation guide.

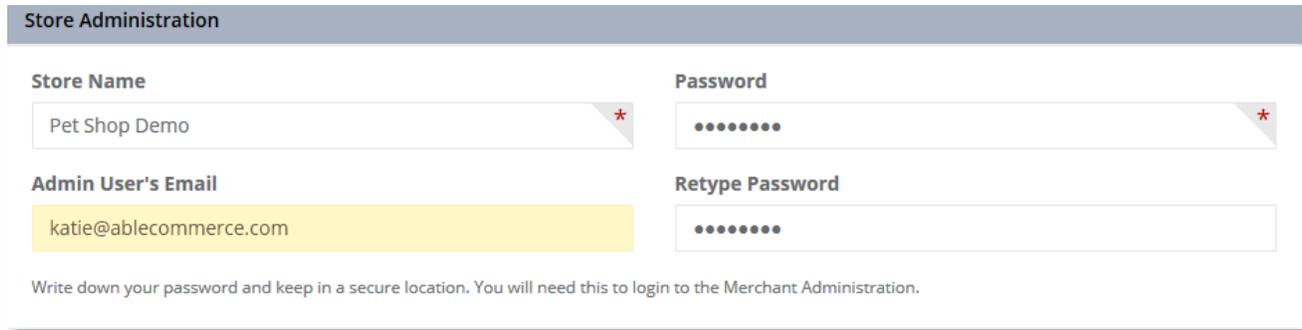
- a) Check the box to acknowledge that you have reviewed the guide.
b) Press the **Continue** button.

When you submit the page, AbleCommerce verifies a connection to your database. If the process is unsuccessful, you will remain at the installation screen with an error message that identifies the problem. This step provides some measure of protection from supplying invalid credentials.

- c) If database configuration is successful, you will proceed to the final part of the installation.

4. Create an Admin account and set up store

The final installation steps include creating the superuser account and initial store contact information. All information entered here may be changed after installation.



Store Administration

Store Name
Pet Shop Demo *

Password
..... *

Admin User's Email
katie@ablecommerce.com

Retype Password
.....

Write down your password and keep in a secure location. You will need this to login to the Merchant Administration.

- a) Enter a name for the store.
- b) Enter an email address for the Admin user.

The Super Admin user will have the highest security rights within the store. This user will become the “superuser” account, having access to every page within the application, including audit logs, encryption keys, and rights to create additional admin users
This account must belong to a single person. Sharing of admin user accounts is prohibited.

- c) Enter a password for the admin user.

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 seven characters long and use a mix of upper and lower alphabetic and numeric characters.

- d) Re-enter the password as confirmation.
- e) Enter the primary address for the store and an email address.

Store Address	
Address <input type="text" value="770 Easy Commerce Drive"/> *	Country <input type="text" value="United States"/>
Apt. Suite, etc. <input type="text"/>	Phone <input type="text" value="360-555-1234"/>
City <input type="text" value="Vancouver"/> *	Fax <input type="text" value="360-555-4321"/>
State <input type="text" value="WA"/> *	Store Email <input type="text" value="orders@ablecommerce.com"/> *
Zip code <input type="text" value="98685"/> *	<p>The information collected here establishes the default warehouse for the store. You can change the store name or address from the Configure > Shipping > Warehouse page later.</p>

This information will be used to establish your store’s default warehouse, physical location, or origin point for fulfillment and delivery.

f) Select the option to include Sample Data.

Sample Data
Include Sample Data <input checked="" type="checkbox"/> Check this box to include additional data such as small sample catalog.
<input type="button" value="Complete Install"/>

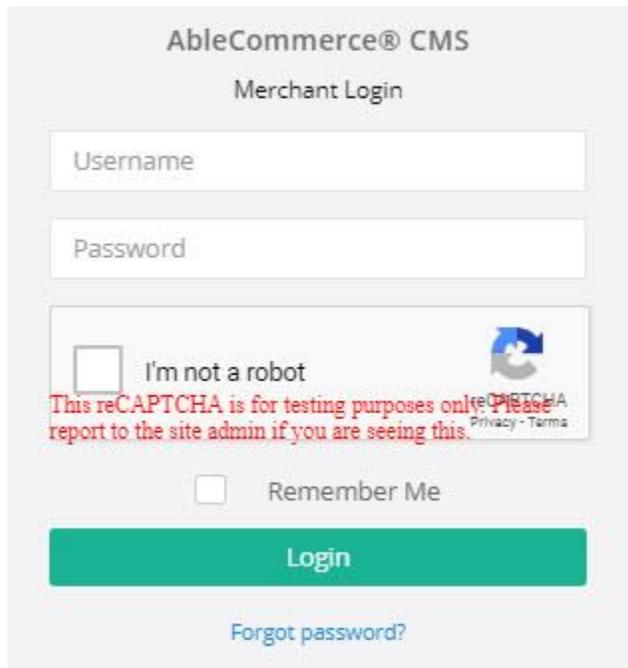
The Sample Data option includes a small catalog with product examples. The email templates and other features are installed and pre-configured so the store will be operational after installation.

g) Press the **Complete Install** button.

Installation Complete
<p>The installation process is complete.</p>
<input type="button" value="Access Merchant Administration"/>

h) Press the **Access Merchant Administration** button to complete the web-based installation.

i) Next, you will be redirected to the **Merchant Login** page. *Bookmark this page.*

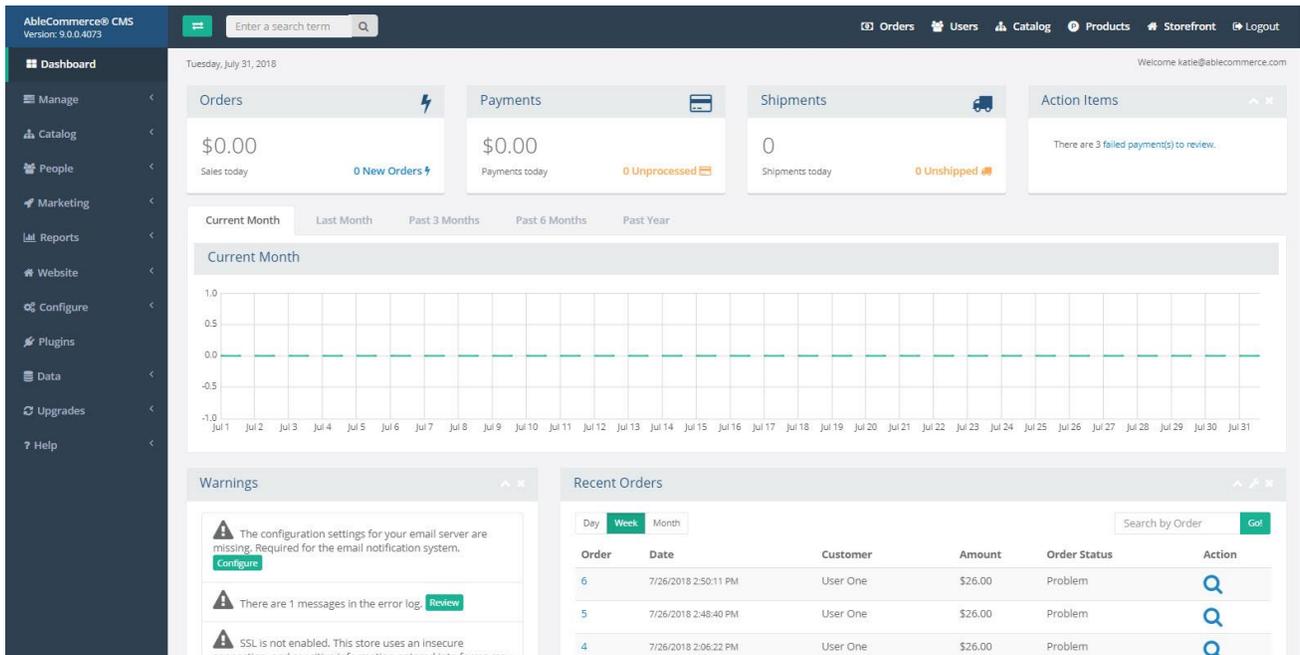


j) Use the superuser account created during the installation to log in.

k) A test version of CAPTCHA is in use. Check the box to confirm you are not a robot.

l) Press the **Login** button.

m) You should now be viewing the AbleCommerce **Merchant Dashboard**.



Order	Date	Customer	Amount	Order Status	Action
6	7/26/2018 2:50:11 PM	User One	\$26.00	Problem	View
5	7/26/2018 2:48:40 PM	User One	\$26.00	Problem	View
4	7/26/2018 2:06:22 PM	User One	\$26.00	Problem	View

Figure 2- Merchant Dashboard

Application deployment is complete.

Next, complete post-deployment configuration.

Post-Deployment Configuration

Enable SSL (Secure Sockets Layer)

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

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 an SSL certificate issued for a fully-qualified-domain-name (FQDN) which needs to match the domain name that is registered to your AbleCommerce license.

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

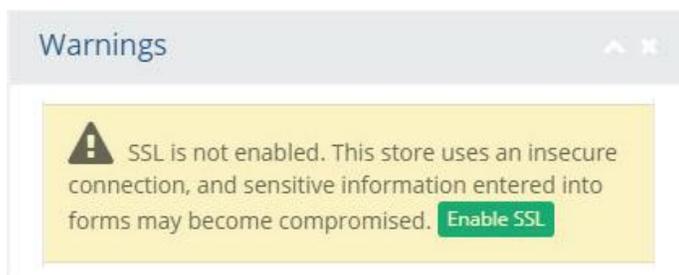
Requirements for TLS 1.2

TLS 1.2 is the Transport Layer Security Protocol designed to protect the privacy of information communicated over the Internet. To meet the requirements of PCI DSS 3.2, you must use TLS 1.2 or higher for all secure communications.

Enabling SSL on the web server is outside the scope of this guide. Once your web server is properly configured, you must enable the SSL feature within AbleCommerce.

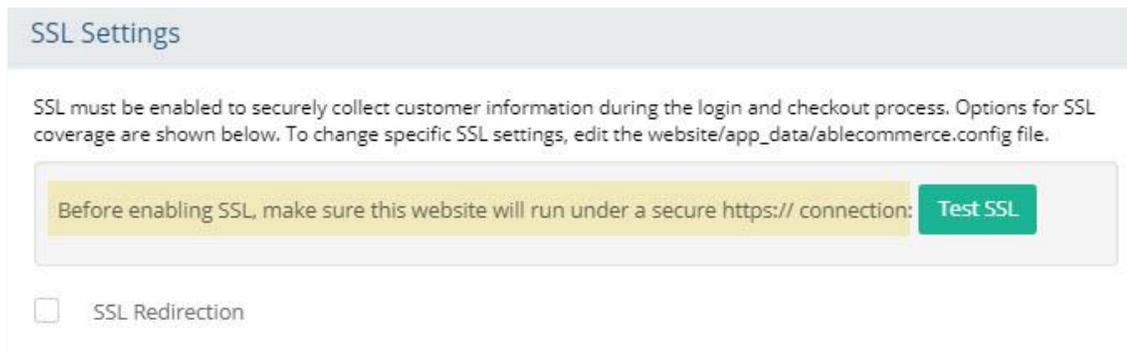
1. **Login** to the AbleCommerce Merchant Administration

The Merchant Dashboard will have a notification when SSL is not enabled. Press the Enable SSL button from the **Warnings** panel.



2. Or, using the menu, go to **Configure > Security > SSL Settings**

3. Press the **Test SSL** button to launch the Secure Connection Test window.



AbleCommerce provides a Test SSL button. Use this to confirm the website is able to run under a secure connection before saving your settings. If the website is unable to make an SSL connection, the installation will be disabled. **Do not skip this important next step.**

4. Click the **https test link** to *confirm the page opens without any warnings or errors.*
5. If successful, close the page and press the **CLOSE** button to complete the test.

If the https test page loaded **with an error**, then you must contact your website administrator before enabling the SSL feature. Failing to do so will result in your site becoming inaccessible.

6. Check the box labeled “**SSL Redirection**” to open the configuration panel.



7. There are two SSL settings available -
 - a. The option to **Secure all pages** will force https security over the entire installation, including the merchant administration and customer-facing storefront.

Select the radio option: **Secure all pages** (*recommended*)
 - b. The option to **apply SSL to defined paths and pages** includes settings to secure only those pages that collect sensitive information and the entire merchant administration. A list showing the definition of each path and SSL state is shown on-screen.

The default settings meet the minimum requirement for PCI DSS compliance. Individual settings can be added or changed in the ablecommerce.config file.

8. When finished, press the **Save Settings** button in the bottom-right corner of the footer.

Set the Password Policy

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

Strong passwords are the first line of defense into a network since a malicious individual will often first try to find accounts with weak passwords.

The PCI Security Council requires the following password requirements for all users:

PCI DSS Requirement	
8.2.3	Passwords must meet the following: <ul style="list-style-type: none">• Require a minimum length of at least seven characters• Contain both numeric and alphabetic characters
8.2.4	Change user passwords at least once every 90 days.
8.2.5	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
8.2.6	Set passwords for first-time use and upon reset to a unique value for each user and change immediately after the first use.

AbleCommerce allows you to specify different password policies for administrators and consumers.

Merchant Password Policy

Password and login requirements for the administrator accounts.

Minimum Password Length 7 chars

Required Password Element

- Uppercase (A - Z)
- Lowercase (a - z)
- Numbers (0 - 9)
- Symbols (punctuation, underscore)
- Non-letter (number or symbol)

Maximum Password Age 30 days

Password History 10 days 4 passwords

Maximum Login Failure 6

Lockout Period 30 minutes before retry

Inactivity Period 3 months before account is disabled

Figure 3- Merchant Password Policy

For PCI compliance, you cannot set the policy to anything less restrictive, but for increased security, you can make the policy more restrictive than the minimum requirements.

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 comply with the Payment Card Industry's best practices and requirements, AbleCommerce has introduced some features that apply to all user accounts:

→ User passwords are stored in a one-way SHA256 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. The admin accounts are automatically disabled due to inactivity.

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

To locate the password policy configuration page, use the menu and go to **Configure > Security > SSL Settings**.

The **Merchant Password Policy** configuration screen is shown to the left.

The merchant's configuration policy applies to all administrator accounts.

The installation sets the default values and complies with PCI DSS requirements.

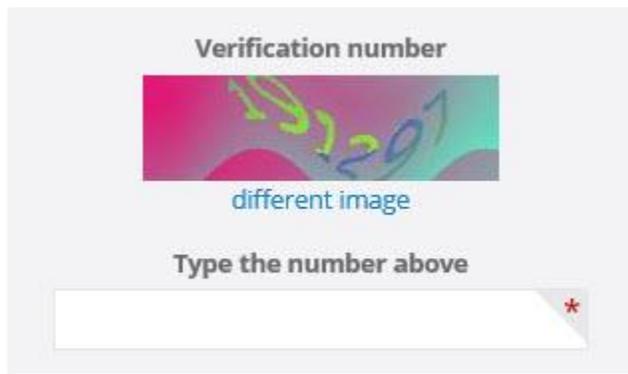
No changes are necessary.

Enable CAPTCHA

A CAPTCHA is a type of challenge–response test used in computing to determine whether or not the user is human. AbleCommerce includes two options for CAPTCHA.

❖ Standard image CAPTCHA

The standard CAPTCHA option will display a 6-digit verification number embedded within an image. The user is required to enter the number from the image into the form field provided. This option requires no additional configuration.

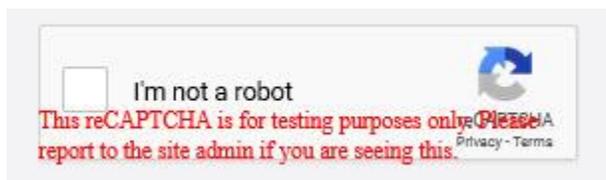


❖ Google reCAPTCHA service

The AbleCommerce installation sets up a test account for the Google reCAPTCHA service. To continue using this option, you will need to obtain your own service keys by registering or sign in at the following link -

<https://www.google.com/recaptcha/admin#list>

The Google reCAPTCHA option will display a simple checkbox that the user must click or press during the log in process.



To Enable or Disable Google reCAPTCHA

To use Google's reCAPTCHA service, you must have completed [site registration](#) with Google and obtained a Site and Secret key. At the time of this writing, the service is available at no cost.

1. Using the menu, go to **Configure > Security > Passwords**
2. Find the **CAPTCHA Services** section.

CAPTCHA Services

Select CAPTCHA Type:

Use standard image CAPTCHA

Use Google reCAPTCHA service

 **Configure Google reCAPTCHA**

To use Google reCAPTCHA, [sign in or register](#) to obtain your Secret and Site keys which need to be entered into the fields below. To do that, register a new site using the reCAPTCHA v2 option. Enter one or more domains for the site registration and save your changes. Expand the Keys section under "Adding reCAPTCHA to your Site" and copy the Site and Secret keys to the form below.

Site Key

Secret Key

Theme

Size

3. The installation sets the default option to “Use Google reCAPTCHA service”.

Option A) To set up Google reCAPTCHA, **continue to step 4.**

Option B) To disable Google reCAPTCHA, select the radio-option labeled “Use standard image CAPTCHA”. This option requires no further setup.

CAPTCHA Services

Select CAPTCHA Type:

Use standard image CAPTCHA

Use Google reCAPTCHA service

4. Enter the Site Key obtained from your registration of this website.
5. Enter the Secret Key.
6. Press the **Save Settings** button in the lower-left corner of the footer.

Email Server Configuration

Several security features depend on the operation of the email server, such as sending a request to reset a password. The configuration of the email server is also required before user authentication services can be used.

As distributed, AbleCommerce does not include sensitive information or account details in any of the email notifications. Email is not a secure method of transport and should not be used for such a purpose. 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.

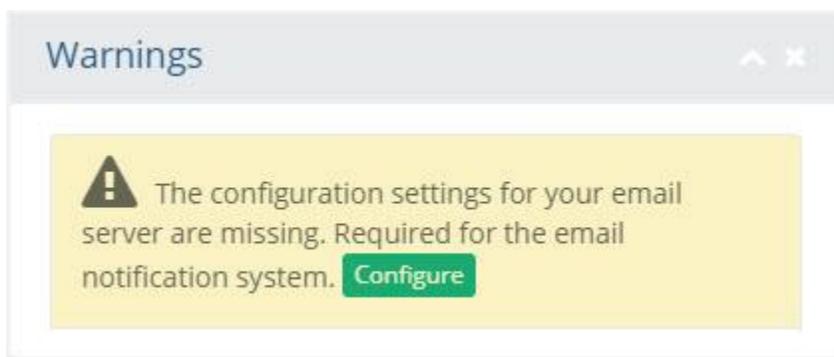
Email, instant messages, SMS, and chat are not secure methods of communication.

E-mail, instant messaging, SMS, and chat can be easily intercepted by packet-sniffing during delivery across internal and public networks. Do not utilize these messaging tools to send account numbers, or any sensitive information, unless they are configured to provide strong encryption. Additionally, if you request account numbers, or any sensitive information, with end-user messaging technologies, you must provide a tool or method to protect this information using strong cryptography or render the information unreadable before transmission.

PCI DSS Requirement

4.2 Never send unprotected PANs by end-user messaging technologies (for example, email, IM, SMS, chat, etc.)

After a new installation, the Merchant Dashboard will have a notification if the email server has not been configured. Press the **Configure** button from the Warnings panel.



Or, using the menu, go to **Configure > Email > Settings**.

To enable the email systems in AbleCommerce, you may need to contact the person who can provide the settings to your email server.

The **Email Server Configuration** page in AbleCommerce is shown below.

Email Server Configuration

To enable the email system, enter applicable SMTP server settings below. You may need to acquire this information from your system administrator.

SMTP Server

SMTP Port

25

Enable Secure SMTP

Enable Email Authentication

SMTP Username

SMTP Password

Save Email Settings

Figure 4- Email Server Configuration

Email server configurations vary, and it is not in the scope of this document to provide detailed information on how to acquire your email settings. The [AbleCommerce Merchant Guide](#) provides additional information and instructions for setting up the email system.

After your email settings have been entered, press the **Save Email Settings** button.

A new **Test Message** section will appear below the configuration form. Enter a valid email address and press the **Send** button to generate a test message.

Test Message

You can generate a test message to check your server configuration. Provide the address where the message should be sent and press send.

Enter Email

Send

Confirm the email is received before continuing. If the email server is improperly configured, an error message will be displayed on-screen. This information is helpful for troubleshooting.

Setup User Authentication

Assigning a unique identification (account) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by and can be traced to, known and authorized users and processes.

By ensuring each user is uniquely identified— instead of using one account for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.

To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones

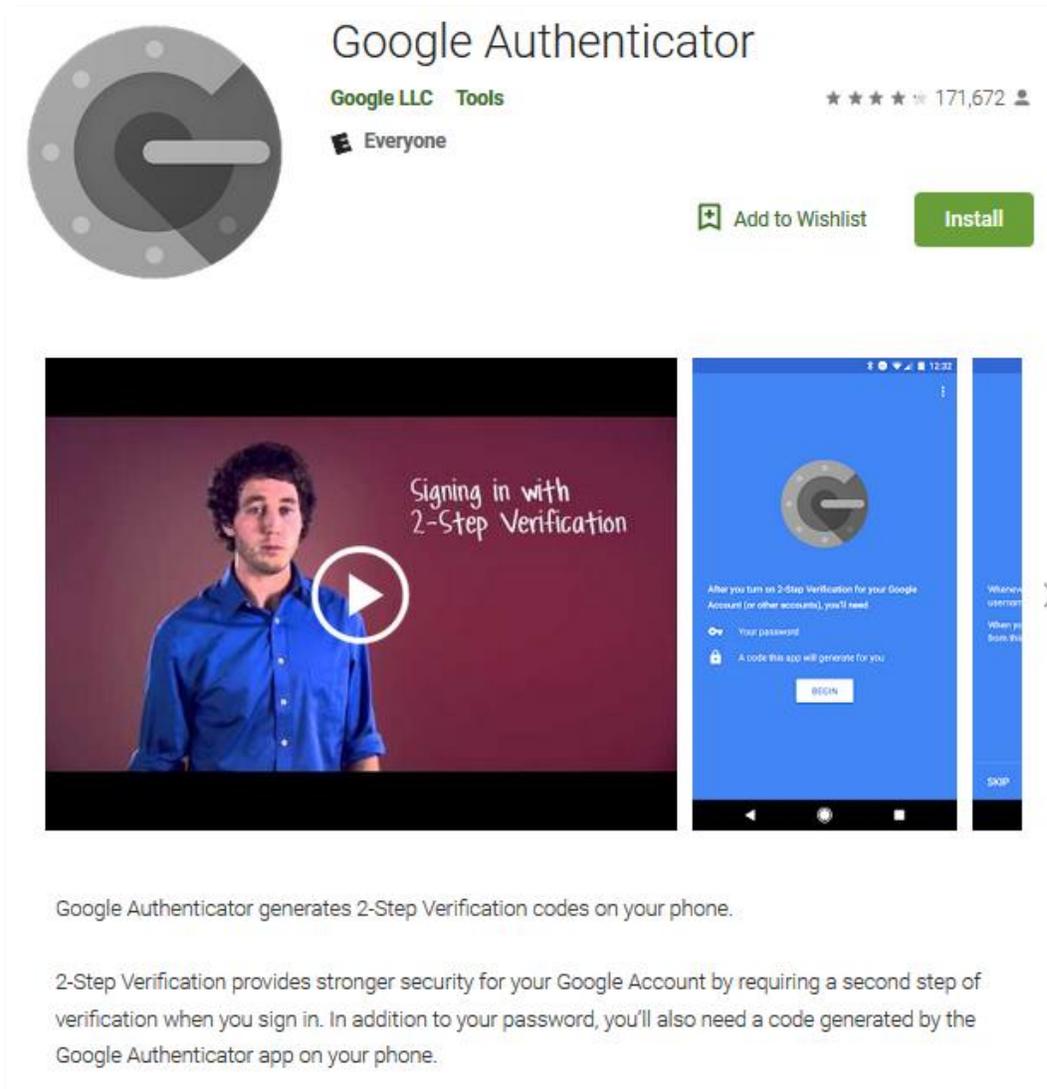
The PCI Security Council requires that users are identified and authenticated before gaining access to system components:

PCI DSS Requirement	
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.
8.1.3	Immediately revoke access for any terminated users.
8.1.4	Remove/disable inactive user accounts within 90 days.
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the session
8.3.1	Incorporate multi-factor authentication for non-console access into the CDE for personnel with administrative access.

Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted.

Multi-factor authentication provides additional assurance that the individual attempting to gain access is whom they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

AbleCommerce satisfies the multi-factor authentication (MFA) requirement with its Google Authenticator integration.



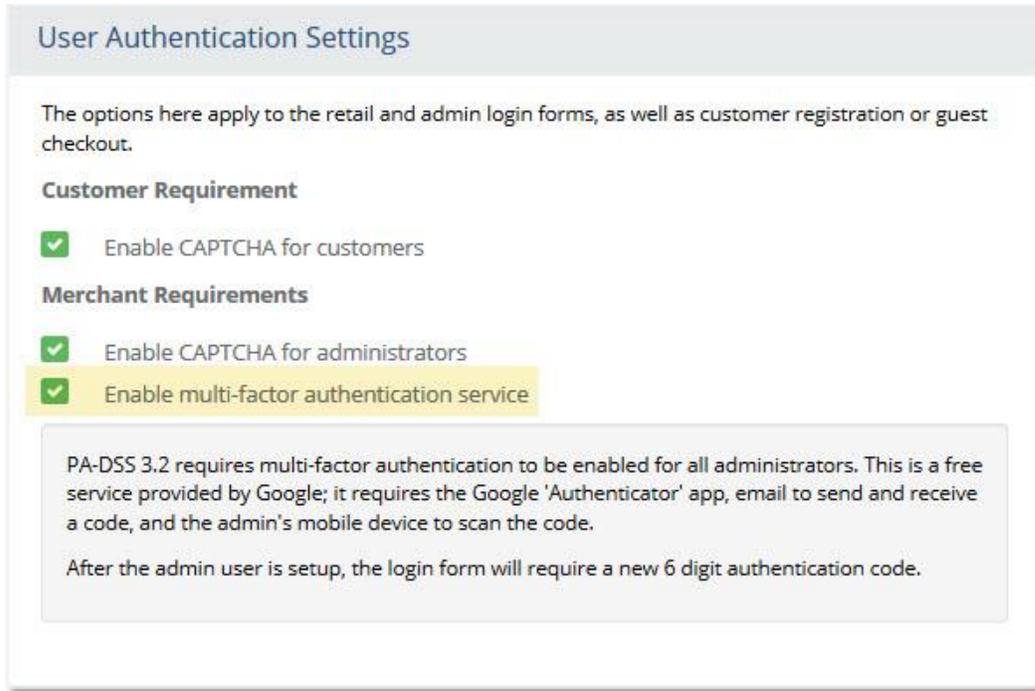
The Google Authenticator app, available from play.google.com, generates a 2-step verification code from your mobile phone. For the initial setup, an email is generated with a barcode embedded image. The user will scan the image which instantly creates the account within the Authenticator app.

Once an account is created, the merchant will be able to view an ever-changing code from the app. Using their personal device, the admin user can retrieve the code and log in to the AbleCommerce Administration.

To Enable Multi-Factor Authentication

Make certain the email system is enabled and functioning before continuing. This feature relies on an email, containing a barcode, which must be scanned to complete the setup.

1. Each AbleCommerce Admin user must first download and install the Google 'Authenticator' app to his or her personal mobile device.
2. Using the menu, go to **Configure > Security > Passwords**
3. Find the **User Authentication Settings** section.



User Authentication Settings

The options here apply to the retail and admin login forms, as well as customer registration or guest checkout.

Customer Requirement

Enable CAPTCHA for customers

Merchant Requirements

Enable CAPTCHA for administrators

Enable multi-factor authentication service

PA-DSS 3.2 requires multi-factor authentication to be enabled for all administrators. This is a free service provided by Google; it requires the Google 'Authenticator' app, email to send and receive a code, and the admin's mobile device to scan the code.

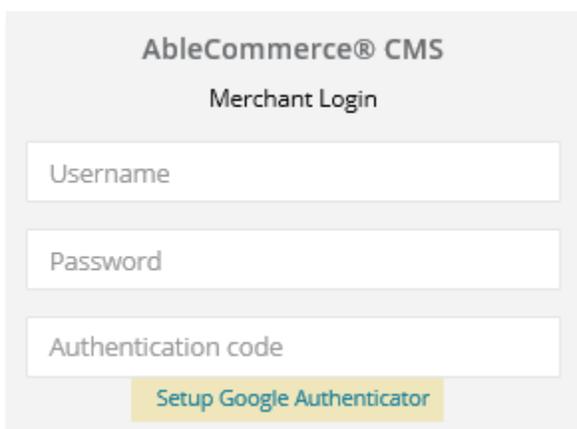
After the admin user is setup, the login form will require a new 6 digit authentication code.

4. Check the box to “**Enable multi-factor authentication service**”.
5. Press the **Save Settings** button in the bottom-right corner of the footer.

Setup Multi-Factor Authentication for Admin Users

Once enabled, all admin users must log in through the Merchant Login form. It will not be possible for the AbleCommerce Admin user to use the customer-facing storefront login form when MFA is enabled.

1. From the Merchant Login page, use the “**Setup Google Authenticator**” link to begin setup.



AbleCommerce® CMS

Merchant Login

Username

Password

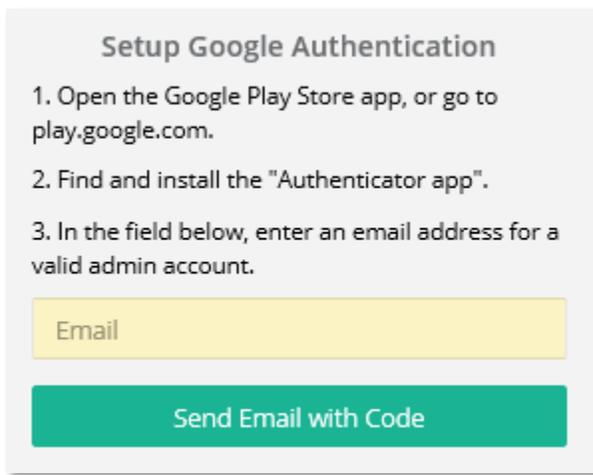
Authentication code

[Setup Google Authenticator](#)

- The first steps are to find the **Google Authenticator** app and have the user install it on their personal mobile device.

Each new Admin user needs to install the Google Authenticator app available from play.google.com.

- The **Google app** provides a link to **Begin Setup**. Initiate the setup by pressing this link.
- Next, the user will need to enter the email address that is associated with his or her unique admin account into the form provided.



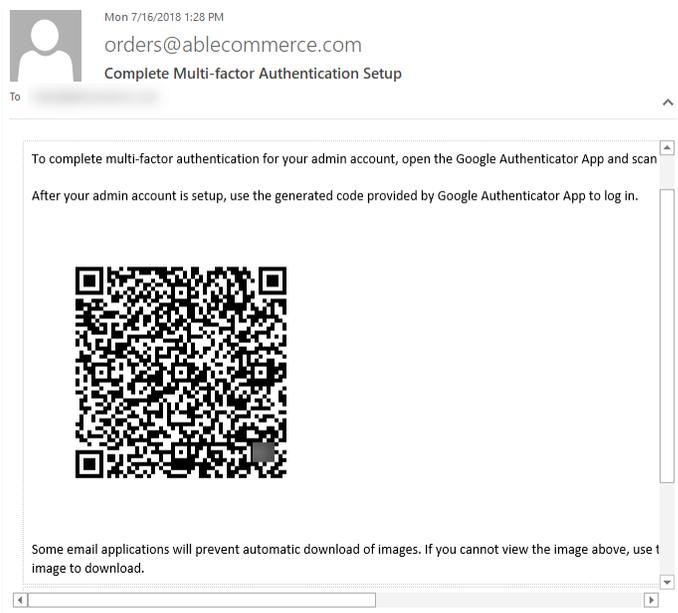
Setup Google Authentication

1. Open the Google Play Store app, or go to play.google.com.
2. Find and install the "Authenticator app".
3. In the field below, enter an email address for a valid admin account.

Email

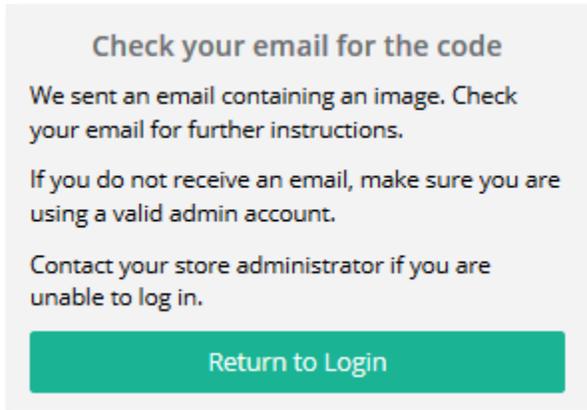
Send Email with Code

- Press the **Send Email with Code** button to continue. AbleCommerce will dispatch an email with the final configuration instructions.



- When the user receives this email, a **barcode** will be displayed as an embedded image which then **must be scanned** with the user's personal mobile device.
- The Google Authenticator app offers two options to input the code:

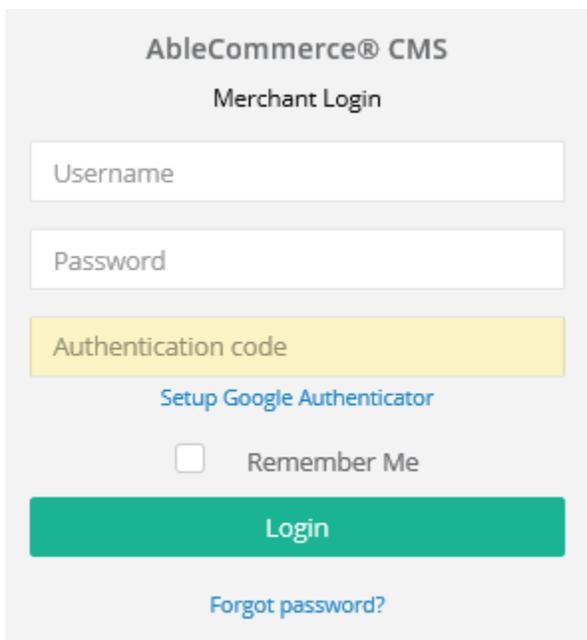
- a. Scan Barcode – use this option by pointing your phone at the barcode image
 - b. Manual Entry – use this option for hand-entry of an extremely long key code
8. If successful, the scanned image will activate the account within the Google Authenticator app.
 9. At this point, the user should see a **6-digit code that is continuously updating** within the app. This code will be used in conjunction with the Admin user’s login credentials.
 10. Press the **Return to Login** button to continue.



Login using Multi-Factor Authentication

The Admin login page is available by direct link. The AbleCommerce system administrator should provide this link to each new Admin user.

1. Access the **Merchant Login** page.



2. **Enter** a username, password, and **active 6-digit Google Authenticator code** into the form provided.

3. Press the **Login** button. If successful, the Admin user will be directed to the Merchant Administration.

Encryption Key

Sensitive data, such as credit card numbers and passwords, that is stored to the database needs to be protected with Advanced Encryption Standard (AES) cryptography. AES is a keyed encryption – which means you need a secret password to encrypt and decrypt the data.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

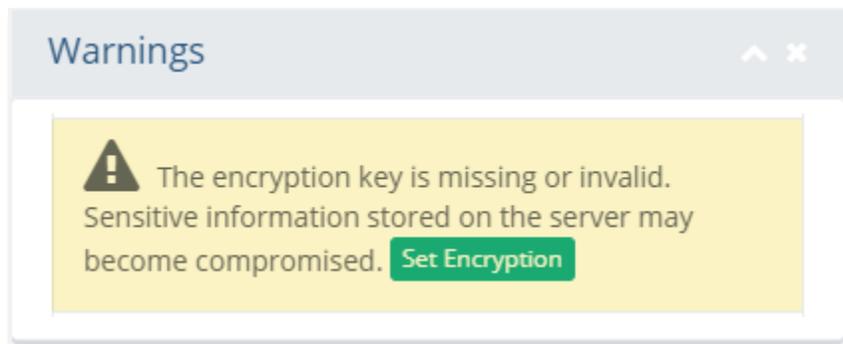
The Rijndael cipher -- a mash of the Belgian creators' last names Daemen and Rijmen -- was selected as the proposed algorithm for AES in October 2000 and published by NIST as U.S. FIPS PUB 197. The Advanced Encryption Standard became effective as a federal government standard in 2002. It is also included in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3 standard, which specifies block ciphers for the purpose of data confidentiality.

In AbleCommerce, there is only one key to manage which is being used for data encryption. This key is called the data encryption key, or DEK. This key is set and managed from within the AbleCommerce security configuration pages. The DEK is protected by a second key called the Key Encryption Key, or KEK. The KEK is managed and protected through [Microsoft .NET application data protection](#).

At no time is the data encryption key (DEK) transmitted, saved, or displayed in plain text.

After installation, AbleCommerce does not have the encryption key set. It is important that you set the encryption key immediately after deployment. This is especially important if you plan to store credit card data.

The Merchant Dashboard will have a notification if the encryption key is not set.



Create the Encryption Key

Use this procedure to create or change an encryption key.

1. Press the Set Encryption key button from the Warnings panel of the Dashboard.
2. Or, using the menu, go to **Configure > Security > Encryption**
3. To set the encryption key, find the **Change Encryption Key** section.

Change Encryption Key

To change your encryption 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.

Before initiating a key change, make sure to **backup the current encryption key and database.**

Estimated Workload: 0

Enter at least 20 characters of random text

rgj693nfsg7934vhlqmp90nx./zaqjfyelokhnpwbxofdhtypamtu

Change Encryption Key

4. **Enter** at least 20 characters of **random text** into the field provided.

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.

5. Press the **Change Encryption Key** button.
6. A confirmation page will appear.
7. Please **confirm** to continue.
8. The encryption key file will be updated with a notice displayed on-screen showing the time and date the key was last updated.

PCI Compliance

Sensitive account data is encrypted within the database using a secret key. Without this key, the data cannot be read. You must update your encryption key on a regular schedule, **at least once per year but every 90 days is recommended.**

Encryption Key Last Updated: 7/17/2018 12:42 PM

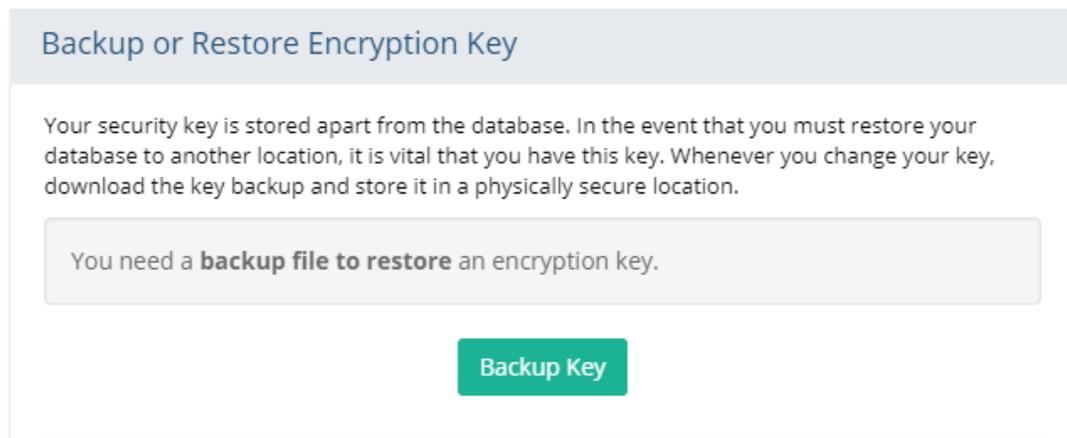
The encryption key should be changed at least once per year, but every 90 days is recommended.

Backup the Encryption Key

Use this procedure to backup an encryption key. For first-time deployment, there will only be one option - Backup Key. You must create a key before the backup option will be available.

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.

1. To back up the encryption key, find the **Backup or Restore Encryption Key** section located in the menu at **Configure > Security > Encryption**.



2. Press the **Backup Key** button to begin.
3. A confirmation page will appear.
4. Please **confirm** to continue.
5. The encryption key file will be updated.

Restoring an Encryption Key

Use this procedure to restore an encryption key. This is required if you move the installation to a different server.

1. Find the **Backup or Restore Encryption Key** section located in the menu at **Configure > Security > Encryption**.
2. Press the **Restore Key** button to begin.
3. A Backup File option will appear. *Choose the latest key backup when performing a restore.*
4. Press the **Restore Key** button again and re-encrypt the data using the restored key. **This action cannot be undone.**

Management and Protection of Keys

Encryption keys must be strongly protected because those who obtain access will be able to decrypt data. Procedures need to be put in place to protect keys used to secure stored cardholder data against disclosure and misuse.

A crypto period is the time span during which a particular key can be used for its defined purpose. Periodic changing of the encryption keys when the keys have reached the end of their crypto period is imperative to minimize the risk of someone's obtaining the encryption keys and using them to decrypt data.

Keys that are no longer used or needed or keys that are known or suspected to be compromised should be revoked and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept, they should be carefully protected.

Security policies and operational policies for protecting stored cardholder data need to be documented, in use and known to all affected parties.

For additional information, review the section [Key Management Responsibilities](#) below.

Payment Data Storage

AbleCommerce does not enable payment data storage by default. This action can only take place by an authorized Admin user. Before turning on this feature, you must understand the responsibility of protecting the cardholder's data.

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full account number is not needed, and not sending unprotected using end-user messaging technologies, such as e-mail and instant messaging.

A formal data retention policy identifies what data needs to be retained, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only cardholder data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code.

Understanding where cardholder data is located is necessary so it can be properly retained or disposed of when no longer needed. In order to define appropriate retention requirements, an entity first needs to understand their own business needs as well as any legal or regulatory obligations that apply to their industry, and/or that apply to the type of data being retained.

Identifying and deleting stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed.

Remember, if you don't need it, don't store it!

PCI DSS Requirement

- 3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:
- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements.
 - Specific retention requirements for cardholder data.
 - Processes for secure deletion of data when no longer needed.
 - A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

To Enable Payment Storage

Minimize the risk by keeping this setting off. Unless you have a business need to store credit card numbers, the payment storage feature should remain disabled.

1. Using the menu, go to **Configure > Security > System Settings**
2. Find the **Credit Card Data Storage** section.



Credit Card Data Storage

When payment data storage is enabled, the credit card information is encrypted and saved for future payment processing.

Enable Payment Data Storage

Days To Save

3. Check the box **“Enable Payment Data Storage”**.
4. This will give you the option to select the number of **Days to Save**.
5. Choose the least amount of days necessary to store the cardholder’s data. A value of ‘0’ will purge the information immediately after each transaction is completed.
6. Press the **Save Settings** button in the lower-right corner of the footer.

To Disable Payment Storage

1. Find the **Credit Card Data Storage** section located in the menu at **Configure > Security > System Settings**
2. To disable, uncheck the **Enable Payment Data Storage** box.
3. Press the **Save Settings** button.

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

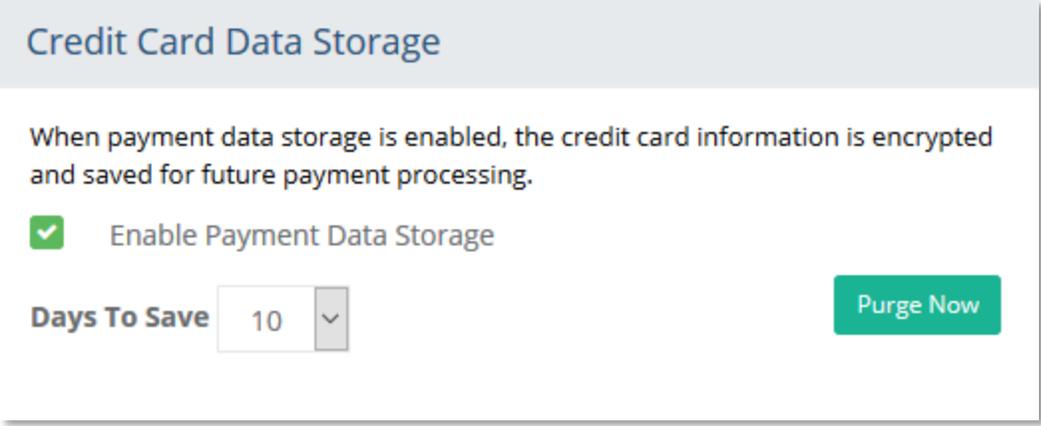
- If the transaction fails to authorize for any reason, you will not be able to use the "retry" feature from merchant admin as the card data will not be available.
- You cannot access the card data for offline processing – you must have a payment gateway configured if you disable credit card storage.

The setting for Days to Save is important if payment storage is enabled. The recommended value is 0, which means as soon as a payment is completed the encrypted account data will be removed. AbleCommerce does not have an option longer than 60 days to retain the card data after a payment is completed.

Purging Cardholder Data from the Database

Once you have established your cardholder retention period, you will need to purge the credit card numbers before taking a **database backup**.

The maintenance routine will automatically remove any stored card data that exceeds the number of days to save. Purging is a manual action and should be performed before manually backing up the database.



The screenshot shows a settings panel titled "Credit Card Data Storage". Below the title, there is a descriptive text: "When payment data storage is enabled, the credit card information is encrypted and saved for future payment processing." Below this text, there is a checked checkbox labeled "Enable Payment Data Storage". To the right of the checkbox, there is a "Purge Now" button. Below the checkbox, there is a "Days To Save" label followed by a numeric input field containing the value "10" and a dropdown arrow.

1. Find the **Credit Card Data Storage** section located in the menu at **Configure > Security > System Settings**
2. To purge all saved credit card data, press the **Purge Now** button located to the far right.
3. A warning message will appear indicating that all credit card data for processed and unprocessed orders will be deleted.

You should make sure that *all orders are processed* before continuing.

Are you sure you want to
purge all credit card data for
processed and unprocessed
orders?

You will not be able to recover!

Cancel

OK

4. To continue, press **OK**.
5. A confirmation indicating the number of records purged will be shown.

The steps above describe how to purge credit card data before taking a backup of the AbleCommerce database.

The document linked below describes how to purge credit card data from after taking a backup of the AbleCommerce database.

[FAQ: How to remove sensitive credit card data from a data backup](#)

These steps ensure that any database backups do not contain card number data. This is required by the PCI Payment Standards Security Council if you are storing credit card information.

Processing Credit Card Payments

Accepting and processing credit card payments through the AbleCommerce store requires the installation and activation of a payment gateway. A payment gateway allows AbleCommerce to communicate with third-party payment processors to handle the credit card transactions for your store. The payment processor, or service, will then deposit funds into the merchant's bank account. Use of a payment gateway will help you avoid the need to store credit card numbers. This is also the only way to gain the benefit of the Card Verification Code (CVC or CVV) service, which helps reduce fraudulent transactions.

AbleCommerce offers several payment gateway integrations without the need to install additional software or plug-ins. One popular payment gateway is Authorize.net. This payment processor, along with AbleCommerce, supports many features including the secure Customer

Information Manager (CIM). Authorize.net with CIM will eliminate the need to store sensitive credit card information in the database.

Instead, Authorize.net is able to store the details of the customers' credit cards and AbleCommerce is able to transmit the information using a secure ID or token. At this time, Authorize.net is the only payment gateway offered that supports the CIM feature.

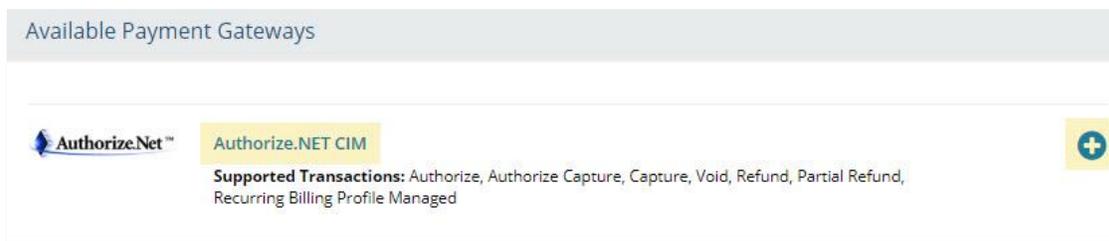
There are several other payment gateways available such as PayPal's Braintree, Chase Paymentech Orbital, PayPal standard IPN, Express Checkout, and Website Payments Pro, as well as the E-Payment Integrator which offers an additional 90 payment gateways choices.

Install a Payment Gateway

1. Go to the **Plugins** page using the menu.
2. Find a payment gateway and press the **Install** button.
3. Wait a moment for the page to refresh.
4. Confirm the gateway installed.

Configure a Payment Gateway

1. Go to **Configure > Payments > Gateways** page using the menu.
2. Within the **Available Payment Gateways** section, find a payment gateway to configure.



3. Press the linked name or the blue + icon to access the configuration page for the chosen payment gateway.
4. Each gateway requires different configuration details to complete the setup. Reference the [documentation](#) of each payment gateway for assistance.

Using a Customer Information Manager (CIM)

Before you can enable the feature which allows a registered user to save and reuse payment profiles, you must have the Authorize.net CIM gateway configured.

1. Go to **Configure > Store > General** page using the menu.
2. Find the **Checkout Options** section.

Checkout Options

- Use a One-Page-Checkout system
- Allow users to create orders with multiple shipping addresses
- Allow users to enter special delivery instructions
- Give registered users the option to save credit cards

3. Enable the option to “**Give registered users the option to save credit cards**”.
4. Press the **Save Settings** button.

Customer Information Manager (CIM)

The Authorize.Net Customer Information Manager (CIM) allows you to store customers' sensitive payment information on Authorize.Net's secure servers, simplifying your compliance with the Payment Card Industry Data Security Standard (PCI DSS) as well as the payments process for returning customers and recurring transactions.



Viewing Payment Data

The display of full account numbers on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that full account number viewing is only displayed for those with a legitimate business need to see the information minimizes the risk of unauthorized persons gaining access to this data.

Cardholder data and sensitive authentication data are defined as follows:

Account Data

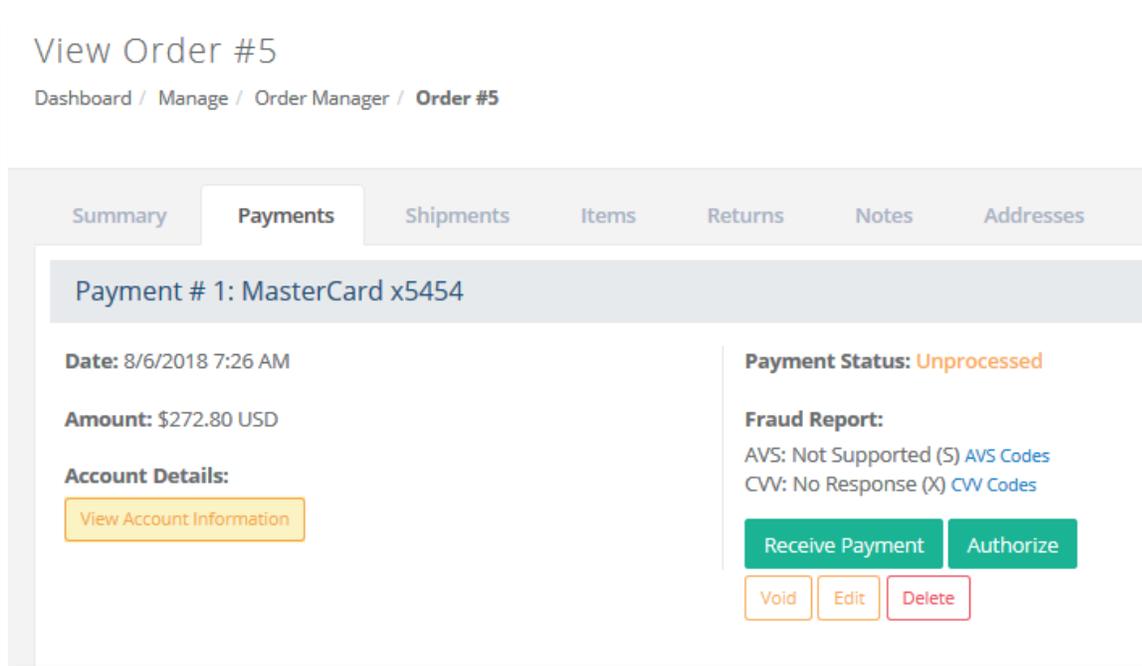
Cardholder Data includes:	Sensitive Authentication Data includes:
<ul style="list-style-type: none"> • Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code 	<ul style="list-style-type: none"> • Full track data (magnetic-stripe data or equivalent on a chip) • CAV2/CVC2/CVV2/CID • PINs/PIN blocks

If you have decided 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.

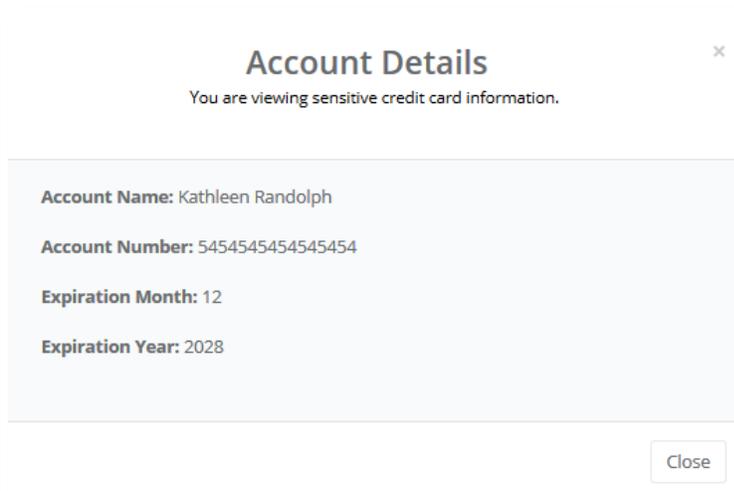
To View Account Information for a Payment

The payment method and last 4 digits are shown on-screen. This is usually enough information for any post-order processing.

1. Go to **Manage > Orders** page using the menu.
2. Find and **View** the order that you want to view the payment information for.
3. Click on the **Payments** tab.



4. To view the full credit card number, press the **View Account Information** button.



A pop-up is displayed with the following account details shown: account name, account number (PAN), expiration month and year.

Additionally, when the **View Account Information** button is pressed, a record of the action will be stored in the Audit Log. The user's identity, IP address, date/time, and order reference are logged.

- If SSL is not enabled, the button to **View Account Information** will not be available.
- Under no circumstances will AbleCommerce save, store, or show the CVV code.

PCI DSS Requirement	
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

Audit Logging

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 superuser.

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.

Find a Card Viewing Event in the Audit Log

1. Go to the **Reports > System > Audit Log** page using the menu.
2. At the top of each column are clickable headings that will change the sort order.

Additionally, the report includes the ability to filter events to a specific day or time period.

Show events from to [Report](#)

3. In the **Event** column, find **“View Card Data”**. The record should look similar to this:

Date	Event	Success	User	Re IP Address	Comment
8/6/2018 7:29:35 AM	View Card Data	X	katie@ablecommerce.com	127.0.0.1	Payment information for Order# 5 viewed

4. The date, time, user’s email and originating IP address are recorded. In the **Comment** column, a reference to the order number is shown.

PCI DSS Requirements and Responsibilities

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 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.

Documentation should be examined and personnel interviewed to verify that security policies and operational policies for protecting stored cardholder data are in place. Personnel need to be aware of and following security policies and documented operational procedures for managing the secure storage of cardholder data on a continuous basis.

The write-only Audit log also 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.

Anytime an admin user views the full credit card number, an event is written to audit log. This log can only be viewed by superuser admins. The event log can help you monitor employee activities and identify suspicious behavior.

PCI DSS Requirement

3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.

Key Management Responsibilities

The key custodians should understand and formally acknowledge their key-management responsibilities. This process will help ensure individuals that act as key custodians commit to the role and understand and accept the responsibilities.

There should be very few who have access to the encryption keys; limit to those who have key custodian responsibilities. Storing keys in the fewest locations helps an organization to keep track of and monitor all key locations and minimizes the potential for keys to be exposed to unauthorized parties.

Maintaining the encryption key for AbleCommerce is an important task because it impacts the security of your data. The encryption key must be strongly protected because those who obtain

access will be able to decrypt data. Only a super admin user can access the key management interface. The persons responsible for this important task are called your key custodians.

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

Cryptographic keys must be stored securely and in the fewest locations helps an organization to keep track of and monitor all key locations and minimizes the potential for keys to be exposed to unauthorized parties.

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 an 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 of 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 to protect the archived material from unauthorized modification, deletion or insertion. Access control is needed to prevent unauthorized disclosure.

Key Custodian Responsibilities

- ✓ 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

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

Key Custodian Sample Agreement

The document below 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.

Sample Key Custodian Form

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 report any suspicious activity that may compromise key security immediately.

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 the affected key with a new key that allows business operations to continue as normal.

In summary, the manner in which your keys are managed is a critical part of the continued security of the encryption solution. A good key management process, whether it is manual or automated, is based on industry standards and addresses all requirements of PCI DSS.

PCI DSS Requirement	
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.
3.5.4	Store cryptographic keys in the fewest possible locations.
3.6.1	Generation of strong cryptographic keys.
3.6.3	Secure cryptographic key distribution.
3.6.4	Cryptographic key changes for keys that have reached the end of their crypto period, as defined by the key owner, and based on industry best practices and guidelines.
3.6.5	Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised.
3.6.7	Prevention of unauthorized substitution of cryptographic keys.

3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, without adequate network segmentation, the entire network is in the scope of the PCI DSS assessment. To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE.

If network segmentation is in place and being used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon a number of factors, such as a given network's configuration, the technologies deployed, and other controls that may be implemented.

Wireless Communications

If wireless technology is used to store, process, or transmit cardholder data, or if a wireless local area network (WLAN) is part of, or connected to the cardholder data environment, the PCI DSS requirements and testing procedures for wireless environments apply and must be performed.

Before wireless technology is implemented, an entity should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

PCI DSS Requirement	
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission

Use of Third-Party Service Providers / Outsourcing

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

Parties should clearly identify the services and system components which are included in the scope of the service provider's PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which the responsibility of the service provider's customers to include in their own PCI DSS reviews.

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.

Encrypted 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 correctly. The standard AbleCommerce installation guide contains details on how to implement the application in a clustered environment.

All AbleCommerce **config files** are in the \Website\App_Data\ folder.

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

The payment gateway integrations available in 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 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.

The app.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 audit.log file only stores information about security issues related to the viewing of payment data, account lockouts, and admin users.

Using a Centralized Log Server

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
```

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

vulnerabilities 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 software for PCI compliance.

Windows Servers

- 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>
- Server Hardening: Windows Server 2016 <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](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](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](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](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](https://msdn.microsoft.com/en-us/library/bb283235(v=sql.120).aspx)
- Securing SQL Server 2016 [https://msdn.microsoft.com/en-us/library/bb283235\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/bb283235(v=sql.120).aspx)

System Inventory

PCI DSS 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 in this document 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.

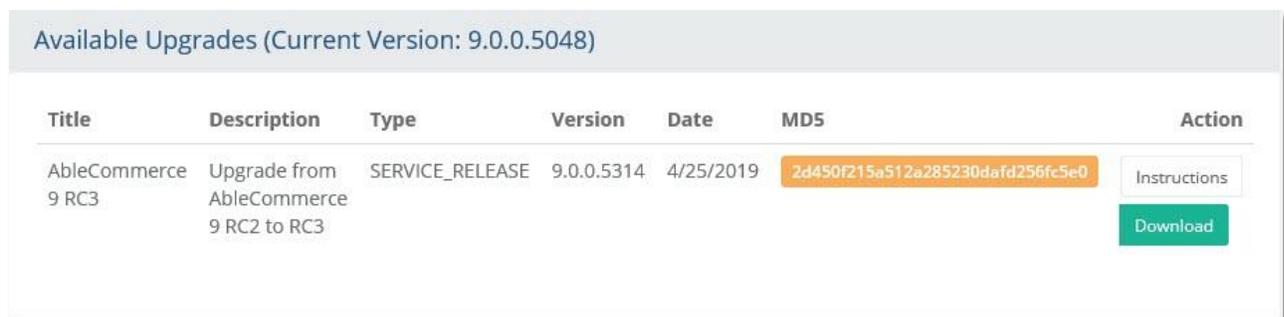
AbleCommerce Upgrade Manager

From time to time, the software will need to be patched to correct any new issues that arise. These service releases, or patches, will be distributed directly to AbleCommerce customers through their secure Merchant Dashboard.

AbleCommerce makes this process easy by providing a built-in Upgrade Manager to assist merchants. The upgrade manager reviews the installation's version number and displays the applicable secure downloads available.

For each download, the merchant may review the documentation which will always include detailed installation instructions, any pre or post-installation requirements, and a change log.

1. Login to the AbleCommerce Merchant Administration.
2. Using the menu, go to **Upgrades > Available Upgrades**
3. If there are any applicable downloads for the installation, they will appear here.



The screenshot displays the 'Available Upgrades (Current Version: 9.0.0.5048)' section of the merchant dashboard. It features a table with columns for Title, Description, Type, Version, Date, MD5, and Action. A single upgrade is listed: 'AbleCommerce 9 RC3' with a description of upgrading from RC2 to RC3, a version of 9.0.0.5314, and a date of 4/25/2019. The MD5 hash is highlighted in orange. Action buttons for 'Instructions' and 'Download' are visible for this upgrade.

Title	Description	Type	Version	Date	MD5	Action
AbleCommerce 9 RC3	Upgrade from AbleCommerce 9 RC2 to RC3	SERVICE_RELEASE	9.0.0.5314	4/25/2019	2d450f215a512a285230dafd256fc5e0	Instructions Download

Figure 5- Sample Upgrade

To view any upgrades that were previously installed, press the **Upgrade Log** button.

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

Glossary of Terms for AbleCommerce

Account – an id for any user in the system where the email address and/or username must have unique values to qualify that person as having a single source identity.

Encryption Key – this is the cryptographic key used to secure sensitive information within the AbleCommerce application.

Group – each admin user has a group assignment which determines access privileges to specific pages within the application.

Merchant Dashboard – the home page for AbleCommerce merchant administration.

Patch – a download that typically addresses a single important issue.

Service Release – service release is a cumulative upgrade consisting of several issues that will be fixed with a single download.

Superuser – the top-level administrators of the AbleCommerce system with access to all functions.