

INSTALLATION OF THE

CRE SECURE

PAYMENT MODULE V 1.0

FOR

ZEN CART 1.2 TO 1.3.X SERIES

INSTALLATION OF THE CRE SECURE MODULE FOR ZENCART

Customers who wish to install the CRE Secure payment module may do so by following these instructions. Provided all of these instructions are followed, merchants will be able to achieve PCI Compliance via the CRE Secure process.

Product Release Information

Product: CRE Secure Payments Module for Zencart

Release Number: 1.1

Release Date: Monday, November 16, 2009

Customer Support: For more information or support, please visit our website or email us at software@cresecure.com. Or Support: support@cresecure.com

Introduction

This guide describes how to install and get started with the CRE Secure Payments Module. Once installation is complete, further instructions are provided for the CRE process that will lead to completion of all requirements for PCI Compliance. If you wish to become PCI Compliant through the CRE Secure process, it is critical that that you follow all instructions exactly as specified. Skipping any of the steps described may prevent you from becoming PCI Compliant through this process.

CRE Secure payment module benefits

- (1) Simple path to PCI Compliance
- (2) No credit card information touches the merchant site
- (3) Expensive PCI Compliant hosting is not required.
- (4) Responsibility for PCI Compliance is almost completely outsourced.
- (5) Simple paperwork only is required to complete the compliance process*.
- (6) HTML Clone technology maintains the merchant customer experience.

*Note you may need to arrange scans of your site. Please check with your acquiring bank that holds your merchant account to be certain

Who is this process for?

Merchants already using Zen Cart versions 1.2 to 1.3.x can install the module. Please note that if you have questions about the installation process you can email us at support@cresecure.com. Support for your Zen Cart application falls under your existing support agreement with Zencart.



Minimal System Software Requirements.

To use the CRE Secure Payment module for Zencart you must already have an installation of a supported version of Zencart running on your server.

What other pre-requisites are there?

There are three additional pre-requisites for using the CRE Secure Payment module that you must be aware of before you start:

Pre-requisite 1.

To use the CRE Secure Payment module and complete your PCI Compliance, you must set-up an account on the CRE Secure service. This must be done prior to configuring the module as you will need several codes provided by the CRE Secure service to complete the set-up and process credit card transactions.

You will need details of your merchant account for the set-up. When you have those details, go here to [get started on the CRE Secure system](#).

Note: this is an essential step in completing compliance and the CRE Secure Payment module will not work without it.

Pre-requisite 2.

Once your module is installed you will also need to make a decision about any credit card data you may have stored in the database of your existing store. Many merchants keep credit card numbers on hand for their customers for reference purposes. Many keep them just out of habit. The PCI Security standards require that no credit card data be stored in your system unless major security requirements are implemented.

The CRE Secure process requires that all credit card data in your system be either deleted or permanently masked. Without this step, you cannot become PCI Compliant. If you are OK with this please proceed and after installation we will show you how to treat your stored data appropriately.

Pre-requisite 3.

For PCI Compliance you must be SSL enabled on your site so you will need to order an SSL certificate from your host.

Installation

Step 1.

First, download the CRE Secure Payment Module for Zen Cart V 1.0 from www.cresecure.com to your local machine. After the files are unzipped, then FTP all the files to the primary location of your Zen Cart site. (Usually to the root directory) The files will then automatically migrate to their appropriate location in your Zen Cart application.



When all files have been FTP'd now go to the Administration area of your store. Click on the `Modules' link in the navigation on the left. The Modules link should take you to the page where you install, edit etc your payment modules.

The CRE Secure payment module should now be listed in your payment modules. It will show as `Credit Card via CRE Secure'.

*****NOTE - IMPORTANT SECURITY REQUIREMENT*****

If you have ANY other payment modules (Other than the Paypal modules referred to below) presently installed in your store that are able to process, transmit or store credit card information via your server, (i.e Direct Payment modules) YOU MUST FIRST UNINSTALL THOSE MODULES.

ALL Other payment modules that you may have been using to *process credit cards through your website* cannot be used with CRE Secure as they are a security problem and will expose your shopping cart to the risk of hackers intercepting your customers' cardholder data.

Paypal Website Payments Standard DOES NOT process credit cards through your ecommerce server (this happens on Paypal servers). The Paypal Express check-out product also does not process cards through your store but in many instances it is shipped with the Website Payments PRO (WPP) module which DOES process credit cards on your store so you must be careful and only install Express Check-out and NOT WPP.)

Uninstalling all other modules will reduce your security risk substantially, but the best possible defense against this risk is to DELETE any unnecessary modules ENTIRELY from your system. This is easily done by simply going to the modules folder in your directory where your cart is installed (usually the root directory) and deleting all modules other than CRE Secure.

Note that if you are using Paypal Website Payments PRO or Paypal Payflow PRO as your payment gateway, these can be selected when you set up your gateway as part of your account set-up on cresecure.com. You do not need to install any other module other than CRE Secure to use these gateways

Click to select the CRE Secure payment module, then in the column on the right hand side of the screen, click `install' to install the module. The module will now be installed.

Step 2. Configuring the Module



Check for Updates

Mon, 16 Nov 2009 14:46:15 -0500GMT [75.164.136.109] Admin Home | Online Catalog | Support Site | Version | Logoff
 Configuration | Catalog | Modules | Customers | Locations / Taxes | Localization | Reports | Tools | Gift
 Certificate/Coupons | Extras

PAYMENT MODULES

Modules	Sort Order	Orders Status	Action
Authorize.net (SIM)	authorizenet	●	ⓘ
Authorize.net (AIM)	authorizenet_aim	●	ⓘ
Authorize.net - eCheck	authorizenet_echeck	●	ⓘ
Credit Card - Offline Processing	cc	●	ⓘ
Cash on Delivery	cod	●	ⓘ
Credit Card via CRE Secure	cresecure	●	ⓘ
The Zen Cart FREE CHARGE CARD	freecharger	●	ⓘ
Linkpoint/YourPay API	linkpoint_api	●	ⓘ
Check/Money Order (not configured - needs pay-to)	moneyorder	●	ⓘ
Nochex APC	nochex_apc	●	ⓘ
PayPal IPN - Website Payments Standard	PayPal	●	ⓘ
PayPal Website Payments Pro	PayPal	●	ⓘ
PayPal Express Checkout	PayPal	●	ⓘ

Credit Card via CRE Secure

Enable CRE Secure Payment Module
Do you want to accept payments through the CRE Secure Payment System?
 True
 False

CRE Secure Account ID
The Account ID used for the CRE Secure payment service

CRE Secure API Token
The API Token used for the CRE Secure payment service

Enable Sandbox Mode
Set to 'True' for sandbox test environment or set to 'False' for production environment.
 True
 False

Accepted Credit Cards
The credit cards you currently accept. Selections are American Express, Citibank Financial, DinersCart Blanche, Discover, JCB, MasterCard, RevolutionCard.

Set Pending Order Status
For Pending orders, set the status of orders made with this payment module to this value. Default is 'Preparing [CRE Secure]'.

Once you have installed the CRE Secure Payment module you can now configure it by clicking on 'Edit'. To ensure you complete the CRE Secure process and become PCI Compliant, the following options shown on this screen need to be set:

- CRE Secure Account ID (circled) - The Account ID used for the CRE Secure payment service. This is the Account ID you will be provided with when you connect your existing or new Merchant Account to CRE Secure.
- CRE Secure API Token (circled) - The API Token used for the CRE Secure payment service. This is the API Token you will be provided with when you connect your existing or new Merchant Account to CRE Secure.
- Accepted Credit Cards - The credit cards you currently accept.
- Payment Zone - Enable a payment zone for this module.
- Set Pending Order Status - For Pending orders, set the status of orders made with this payment module to this value. Default is 'Preparing [CRE Secure]'.
- Set Completed Order Status- for Completed orders, set the status of orders made with this payment module to this value.
- Sort Order - Sort order of payment display. Lowest is displayed first.

What if I encounter problems?

For problems or questions relating to installation you can email support@cresecure.com.

COMPLETION OF STEPS NECESSARY FOR PCI COMPLIANCE


Now that your CRE Secure Payment module is installed and configured there are several additional steps required to complete your path to PCI Compliance.

Step 3. Removal of Stored Credit Card Data.

The first of these is to decide what you wish to do with any credit card data you may have stored in the database of your existing store. As indicated above this is a required step in the CRE Secure process and must be completed before you can become PCI Compliant.

To assist in this process we have created a tool that will allow you to purge or mask your stored credit card data when you are ready. The tool may be found in the Administration area of your store. Go to your admin area then to `Modules' then click on your *Credit Card via CRE Secure* module. On the right hand side you will see a CRE Secure image and at the bottom there is a link that says `credit card purge utility'.

PAYMENT MODULES

Modules		Sort Order	Orders Status	Action	Credit Card via CRE Secure
Authorize.net (SIM)	authorizenet	●		ⓘ	<input type="button" value="remove"/> <input type="button" value="edit"/>
Authorize.net (AIM)	authorizenet_aim	●		ⓘ	
Authorize.net - eCheck	authorizenet_echeck	●		ⓘ	
Credit Card - Offline Processing	cc	0 ●	default	ⓘ	
Cash on Delivery	cod	●		ⓘ	
Credit Card via CRE Secure	cresecure	10 ●	default	ⓘ	 Checkout with Confidence Universal Payment System See for yourself why CRE Secure is the best option for online retailers who want a PCI Compliant, designer-friendly way to accept credit cards. Click Here to Learn More >> Version 1.1 <input type="button" value="Credit Card Purge Utility >>"/>
The Zen Cart FREE CHARGE CARD	freecharger	0 ●	default	ⓘ	
Linkpoint/YourPay API	linkpoint_api	●		ⓘ	
Check/Money Order (not configured - needs pay-to)	moneyorder	0 ●	default	ⓘ	
Nochex APC	nochex_apc	●		ⓘ	
PayPal IPN - Website Payments Standard	PayPal	●		ⓘ	
PayPal Website Payments Pro	PayPal	●		ⓘ	
PayPal Express Checkout	PayPal	●		ⓘ	

Module Directory: /home/wgstest/public_html/zen/includes/modules/payment/

Enable CRE Secure Payment Module
True

CRE Secure Account ID

CRE Secure API Token

Enable Sandbox Mode
False

Accepted Credit Cards
American Express, MasterCard, Visa

Set Pending Order Status
default

Set Completed Order Status
default

Sort Order
10

Click on this link and you will be taken to the following page:



Check for Updates

Tue, 15 Dec 2009 15:15:13 -0500GMT [75.164.136.109]

Admin Home | Online Catalog | Support Site | Version | Logoff

Configuration | Catalog | Modules | Customers | Locations / Taxes | Localization | Reports | Tools | Gift Certificate / Coupons | Extras

CREDIT CARD PURGE UTILITY TOOL

To achieve PCI Compliance you will need to mask all credit card number information stored in the database. You must now make a decision about the method used to mask the credit card information. If you do not do this YOU WILL NOT BE ABLE TO ACHIEVE PCI COMPLIANCE.

WARNING: Once this process is complete, you will no longer be able to see the entire credit card number.

- Remove All Credit Card Info
- Mask All Except Last 4 Digits of Credit Card Info (XXXXXXXXXXXX1234)
- Mask Middle 6 of Credit Card Info (123456XXXXXX1234)

Submit



E-Commerce Engine Copyright © 2003-2009 Zen Cart™
Zen Cart v1.3.8a/v1.3.8

Note the options presented on the page allow you to:

- Remove all credit card data
- Mask Middle six of credit card data
- Mask first 12 of credit card data

Select your preferred option and then click `Submit`

Any credit card data stored in your database will now be treated according to your selection. Choosing any of the three selections will conform to the requirements of the PCI Standard as you are no longer storing usable cardholder data. Note that the masking or removal process CANNOT BE REVERSED.

Step 4. Update your Administration Password.

PCI Compliance requires that you use complex passwords to access areas containing sensitive information. We strongly recommend that at this point you go into your admin area and change your existing password to a complex one. This is a password with no fewer than 8 characters, a mix of numbers and characters and a mix of upper and lower case letters.

Step 5. The Self-Assessment Questionnaire.

The Payment card Industry Council has defined a number of different store levels and requirements for those levels to become PCI Compliant. The following table outlines the requirements for Visa:

Level / Tier	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region ²	<ul style="list-style-type: none"> • Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") • Quarterly network scan by Approved Scan Vendor ("ASV") • Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	<ul style="list-style-type: none"> • Annual Self-Assessment Questionnaire ("SAQ") • Quarterly network scan by ASV • Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	<ul style="list-style-type: none"> • Annual SAQ • Quarterly network scan by ASV • Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	<ul style="list-style-type: none"> • Annual SAQ recommended • Quarterly network scan by ASV if applicable • Compliance validation requirements set by acquirer

All card brands allow Level 3 and 4 merchants to complete their compliance via a Self Assessment Questionnaire (SAQ) provided by the Council. This also applies to many Level 2 merchants, but you should check with your card brands to ensure you are clear on this. NOTE that the numbers of transactions that determine your merchant level are for EACH CARD BRAND. (Mastercard for example may require Level 2 merchants to validate their compliance via an audit process.)

The PCI Council has provided 5 categories of Self-Assessment Questionnaires (SAQ's) so merchants can self – assess their PCI Compliance. The 5 categories are shown briefly in the table below. Details of each SAQ category for your reference can be found by clicking on the links.

Merchants who use the CRE Secure process are able to qualify to use the [simplest Self Assessment Questionnaire, SAQ category A.](#)

To complete the requirements for your PCI Compliance [go to here](#) to download and fill-out the SAQ - A 'Attestation of Compliance'.

IMPORTANT.

Once you have downloaded the SAQ-A, you will find that many of the answers have been pre-filled for you by CRE Secure. These answers are based on the assumption that you have followed **all** requirements of the CRE Secure process described above. If you have **NOT** followed all requirements you must re-evaluate those answers before submitting your SAQ.

Please fill in the remaining blanks with the appropriate information and answer the questions that have been left un-checked, for example, you need to attest that you have read the PCI – DSS documentation and fill in your business details.

One of the questions will ask you to verify that your outsourced vendor is PCI Compliant. CRE Secure has been audited and verified as a PCI Compliant Service provider. Please see our [verification document here](#). You can also find us on the [official Visa list](#) of certified PCI Compliant service providers. Companies listed are in alphabetical order.

Finally, sign and date the document and send it to your acquirer (your Merchant Bank) via the route specified by each of them. Please contact your acquirer for details on where you must send the SAQ. Your acquirer is the financial institution with whom you have your Merchant Account. If you do not know who that is, call the ISO who set up your original Merchant Account, or if it was set-up originally through CRE Secure you can email us at support@cresecure.com.

SAQ Validation Type	Description	SAQ: V1.2
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Stand-alone terminal merchants, no electronic cardholder data storage	B
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.	D

A Note about Scans.

Most merchants filing SAQ-A are not required to have scans done on their website servers. However, some banks *will* require you to get quarterly scans of your site in addition to the steps we have outlined above.

Please check with your bank on whether you need to get these scans. If you do need scans, you can [go here](#) to arrange them.

Even if you are not required by your bank to get scans we would still suggest them as they are a good security precaution for your website. Provided you have followed all of the instructions we have provided you, no credit card information will be flowing through your site, so even if hackers get into your server they cannot compromise any cardholder data. But while CRE Secure can quickly get you PCI Compliant and protect you against credit card theft, we cannot prevent hackers from getting into your server and wreaking other kinds of havoc. Taking basic security measures on your site is a good idea. Regular scans can assist you in identifying areas you need to improve in your hosting security.

Completion of PCI Compliance.

Once you have completed all the steps above you will have finalized all that is required to become PCI Compliant via the Self – assessment method. No other steps are necessary. Note that you must attest to your bank that you are compliant with all PCI requirements on an annual basis.

OVERVIEW OF PCI COMPLIANCE

CRE Secure takes security very seriously and is particularly concerned about the security of our merchant's stores and their customer's credit card data. The Payment Card Industry (PCI) Council, an organization comprised of the major card companies, Visa, Mastercard, American Express, JCB and Discover Card, has developed new security requirements for the handling of cardholder information in payment software and applications.

The security requirements contained in the PCI Data Security Standard (DSS) apply to all members, merchants, and service providers that store, process or transmit cardholder data.

All merchants, regardless of the size of their business or the number of credit card transactions they process, are required by the PCI Council to be compliant with the PCI – DSS security requirements by July 1st 2010.

The PCI DSS standards are summarized in 12 Requirements:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect Stored Data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc):

PCI DSS

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

- ◆ Open Web Application Security Project (OWASP)

<http://www.owasp.org>

Much of the information below is based on the requirements of the documents above and will at times refer to specific sections in them. Please keep this in mind as you go through the following.

The CRE Secure payment module

Chain Reaction Ecommerce is committed to ensuring the safety of cardholder data and assisting merchants to become PCI Compliant. The CRE Secure payment module for Zencart has the following features:

- (1) The CRE Secure payment module does not allow the storage of credit card information in the database or elsewhere, as can be done with other payment modules.
- (2) The CRE Secure payment module does not process or transmit any credit card information. Instead, it calls the CRE Secure hosted payment page from CRE Secure's PCI Compliant systems when required by the merchant customer for the entering of credit card information.
- (3) Provided merchants utilize the installation and set-up process described in this document, the module will ensure that no credit card information is seen or handled by the merchant or touched by the merchant website.
- (4) The CRE Secure hosted page called by the payment module, utilizes CRE Secure's exclusive HTML Clone™ technology to maintain the look and feel of the merchant site and the quality of the customer experience.

As outlined above the CRE Secure payment module as well as the CRE Secure payment system, have been validated to the PCI – DSS standards. This means that provided merchants follow the CRE Secure process, they will become PCI Compliant using a system that has been independently validated by our Visa-Certified Quality Security Assessors (QSAs) as meeting all requirements of PCI Compliance. This validation will remain current and enable you to become compliant provided you do not modify the module in any way that would impact the handling of credit card information in your application, or, fail to follow any of the steps outlined in this document.

HTML Clone™ technology.

There are a number of payment systems on the market that use a `hosted' type of payment process. But the CRE Secure™ Payment process is the only one that presents customers with a hosted page that looks almost exactly like all the other pages in the merchant store. The customer experience is consistent from the beginning to the end of the transaction process.



When customers are sent off to some ugly page that looks nothing like your store as happens with some systems, this jarring experience for the customer can cost abandoned carts and lost sales.

The combination of functions in the CRE Secure Payment System allows customers to pay with a credit card without merchants needing to worry about capturing, transmitting or storing credit card information in their store. The customer credit card information is never seen by the merchant or touches the store. And, all this happens while maintaining a great customer experience.

This means that merchants using CRE Secure as set-out in this document do not have to host their stores in a high security PCI Compliant environment and comply with all of the PCI 12 steps as described above. All that is required to complete PCI Compliance process is to fill out and sign a brief Self Assessment Questionnaire (SAQ) version A and send it to the Merchant Account bank. (See instructions above)

PCI Compliant Delivery of Updates.

The CRE Secure Payment Module must be kept current to conform to PCI requirements. Updates and patches will be made available via the corporate website at www.cresecure.com. Customers who wish to update their application must go to the CRE Secure site and first login with the user name and password they set when they first acquired the application. Upon successful login, customers may access the download area and access the update or patch. Downloads take place via https to ensure security and chain of trust.

Patches will cover issues such as routine bug fixes or known problems within the products.

When security issues are identified in the product they are fixed immediately. Depending on severity, these will be released either in one of the regularly scheduled patches or, if sufficiently urgent, as a separate mini-patch that will be released as quickly as possible after it has been identified. Patch release dates are communicated to CRE Secure customers via the corporate website, press releases and also via Customer Support and Sales directly to customers.

Terms CRE Secure™ Payments, HTML Clone™, process and all logos are trademarks of Chain Reaction Ecommerce, Inc. 2009. All rights reserved; www.cresecure.com