



Installation and PCI Compliance Guide

For the

**CRE SECURE
Payment Module**

For

MAGENTO

Versions 1.2.1 to 1.4.xx



INSTALLATION OF THE CRE SECURE PAYMENT MODULE FOR MAGENTO

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 Magento

Release Number: 1.0

Release Date: Wednesday, January 6, 2010

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 Secure process that will lead to completion of all requirements for PCI Compliance. If you wish to become PCI Compliant through our 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 the CRE Secure 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 Magento versions 1.2.1 to 1.4.xx can install the module. Please note that if you have questions about the module installation process you can email us at support@cresecure.com. Support for your Magento application falls under your existing support agreement with Magento.



Minimal System Software Requirements

What other software must be installed first?

Before you can install this product, your web server will need the following:

Magento
PHP 4.0 or greater
The Apache Web server
MySQL database
The Linux Operating System
Installation

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.

If you are storing any credit card information in your ecommerce store in electronic form, you will need to either delete or render that information unusable for transaction purposes. Be mindful that any back-ups that you might have of this card data will also need to be treated if held in any electronic format. (Details of masking procedures are set out below). Note that CRE Secure will have a credit card vault system available soon that will allow you to store card data for later use for card-on-file or recurrent transactions. Please check with CRE Secure to determine availability.

The CRE Secure process requires that all credit card data in your system be either deleted or permanently masked. Without this step, you cannot complete your PCI Compliance via SAQ-A. If you are not prepared to do this, we cannot help you 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

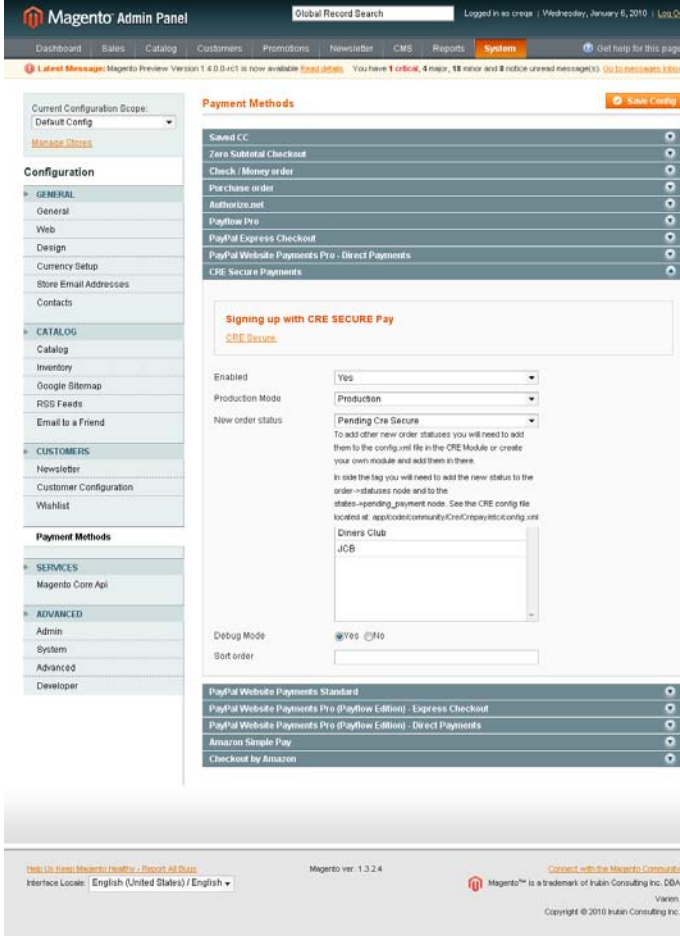
Step 1.

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

When all files have been FTP'd now go to the Administration area of your store. Click on the 'System' link in the navigation on the top, then select 'Configuration>Payment Methods'. The Payments link should take you to the page where you install, edit etc your payment methods.

The CRE Secure payment module should now be listed in your payment modules. It will show as 'CRE Secure Payments'.

Step 2. Configuring the Module



The screenshot shows the Magento Admin Panel interface. At the top, there is a navigation bar with 'System' selected. The left sidebar contains a 'Configuration' menu with 'Payment Methods' highlighted. The main content area displays a list of payment methods, including 'CRE Secure Payments'. Below this list, there is a configuration section for 'Signing up with CRE SECURE Pay' with the following fields:

- Enabled: Yes
- Production Mode: Production
- New order status: Pending Cre Secure
- Debug Mode: Yes (No)
- Sort order: [empty]

The 'New order status' field has a tooltip that reads: 'To add other new order statuses you will need to add them to the config.xml file in the CRE Module or create your own module and add them in there. In side the tag you will need to add the new status to the order->statuses node and to the status->pending_payment node. See the CRE config file located at: app/code/community/Cre/Crepayments/config.xml'.

Click to select the CRE Secure Payments module, then configure to enable the module, production or sandbox, order status, title and business name. Next enter your CRE Secure



Merchant ID and API Token, from your profile on CRE Secure. Then decide on the credit card types, debug mode and sort order. The module will now be installed.

What if I encounter problems?

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

*****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

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 Secure process and must be completed before you can become PCI Compliant.

There are three best options for treating any stored cardholder data you may have:

- Remove all credit card data
- Mask Middle six digits of credit card data
- Mask all except last four digits of credit card number

We would strongly suggest that you treat your stored data in one of the ways described above. If you really do not need to store the data the best option is to just permanently delete it from your system. If you go this route, remember to delete and back-ups stored in electronic format.

Choosing any of the three options will conform to the requirements of the PCI Standard as you will no longer be storing usable cardholder data. Note that whatever masking or removal process you use must be carried out so it 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.	<u>A</u>
2	Imprint-only merchants with no electronic cardholder data storage	<u>B</u>
3	Stand-alone terminal merchants, no electronic cardholder data storage	<u>B</u>
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	<u>C</u>
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.	<u>D</u>

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.

INTRODUCTION TO 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 (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 and the Secure process

CRE Secure is committed to ensuring the safety of cardholder data and assisting merchants to become PCI Compliant. The CRE Secure payment module has been engineered to the standards of the Payment Application Data Security Standards (PA – DSS), required by the Payment Card Industry Council. The payment module 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 facilitates the handing off of all customer credit card information to a CRE Secure systems hosted page outside the merchant website.
- (3) Provided merchants utilize the CRE Secure process, the module will ensure that no credit card information is seen or handled by the merchant.



- (4) The CRE Secure hosted page called by the payment module, utilizes CRE Secure 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 PA – 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 CRE Secure module in any way that would impact the handling of credit card information in the application, or, fail to follow any of the steps of the CRE Secure process.

HTML Clone™ technology.

There are a number of options on the market that use a `hosted' type of payment process. But the CRE Secure 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 with CRE Secure's exclusive, patent-pending HTML Clone technology.

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