

**INSTALLATION OF THE**

**CRE SECURE**

**PAYMENT MODULE V 1.0**

**FOR**

**OSCOMMERCE 2.2 MILESTONE 2 AND RC 2A**



## INSTALLATION OF THE CRE SECURE™ V 1.0 PAYMENT MODULE ONLY

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 RapidPCI™ process.

### Product Release Information

Product: CRE Secure Payments Module

Release Number: 1.0.0

Release Date: June 1, 2009

Customer Support: For more information or support, please visit our website or email us at [software@cresecure.com](mailto:software@cresecure.com). Or Support: [support@cresecure.com](mailto: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 RapidPCI™ process that will lead to completion of all requirements for PCI Compliance. If you wish to become PCI Compliant through our RapidPCI™ process, it is critical that that you follow all instructions exactly as specified. Skipping any of the steps described will prevent you from becoming PCI Compliant through the RapidPCI™ 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 Oscommerce versions 2.2 MS 2 to 2.2 RC can install the module. Please note that if you have questions about the installation process you can email us at [support@cresecure.com](mailto:support@cresecure.com). Support for your Oscommerce application falls under your existing support agreement.



## Minimal System Software Requirements

What other software must be installed first?

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

Oscommerce 2.2 MS 2+  
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 obtain PCI Compliance via the CRE RapidPCI™ process, you must connect your Merchant Account to the CRE Secure system. This must be done prior to your configuring the module as you will need several codes provided by the CRE Secure system to complete the set-up and make the module operational.

If you already have a merchant account, go here to [connect to the CRE Secure system](#). If you do not have a merchant account yet, go to [apply for an account](#) and connect to CRE Secure.

Note that new Merchant Accounts may take several days to be approved by the bank. You will not be able to complete the set-up of your store and the RapidPCI™ process until you have been approved and receive your codes.

Note: this is an essential step in the CRE RapidPCI™ process 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. If you wish to continue storing credit cards you cannot become compliant using the CRE RapidPCI™ process.

The CRE RapidPCI™ 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 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 Oscommerce v 1.0 from [www.cresecure.com](http://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 Oscommerce site. (Usually to the root directory) The files will then automatically migrate to their appropriate location in your Oscommerce application.

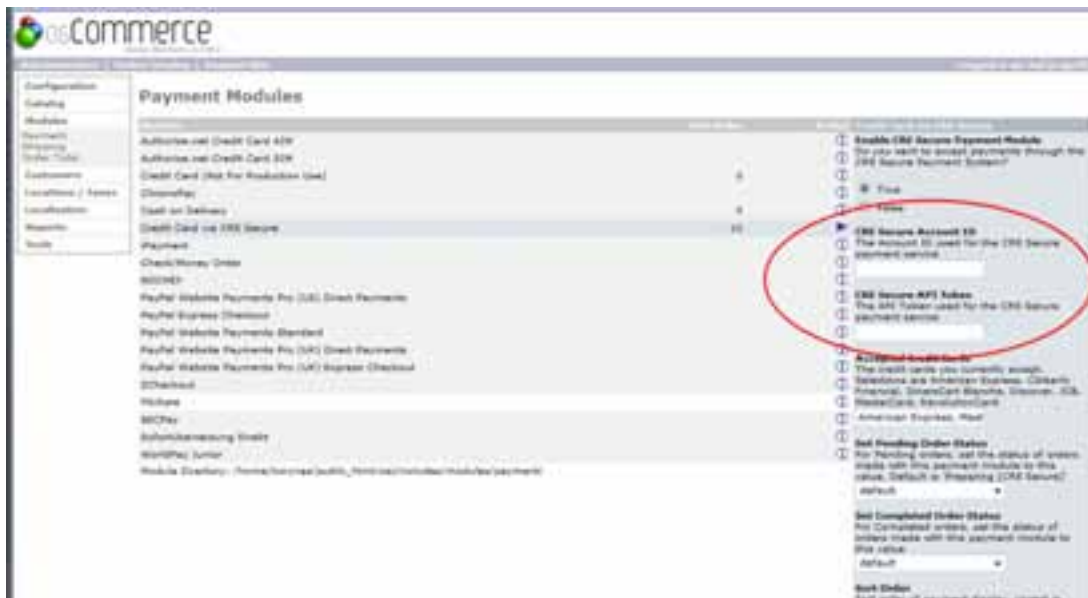
When all files have been FTP'd now go to the Administration area of your store. Click on the 'Modules' link in the navigation on the left. The Modules link should take you to the page where you install, edit etc your payment modules.

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

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

Once you have installed the CRE Secure Payment module you can now configure it by clicking on 'Edit'. To ensure you complete the CRE RapidPCI™ 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](mailto: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 RapidPCI™ 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'.



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



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.**

You now have only one more step to complete the RapidPCI™ process and become fully PCI Compliant!

The Payment card Industry Council has defined a number of different store levels and requirements for those levels to become PCI Compliant. Most CRE merchants would be designated a Level 4 store, which means stores that process less than 20,000 transactions per year.

#### **Introduction to the PCI-DSS Self Assessment Questionnaire. (SAQ)**

According to payment brand rules, all merchants and their service providers are required to comply with the PCI Data Security Standard in its entirety (PCI-DSS). To facilitate this process for merchants 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 below:

We recognize that this can be a complex process for merchants so our RapidPCI™ process has been designed to ensure that merchants who follow all requirements of the RapidPCI™ Process as described above, 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 most 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 **RapidPCI™ 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 few questions that have been left un-checked, for example, you need to attest that you have read the PCI – DSS and fill in your business details.

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](mailto: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 href="#">A</a>
2	Imprint-only merchants with no electronic cardholder data storage	<a href="#">B</a>
3	Stand-alone terminal merchants, no electronic cardholder data storage	<a href="#">B</a>
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	<a href="#">C</a>
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.	<a href="#">D</a>

**Step 6.** Please read the next section on 'A Note about Scans' below. Provided you do not require scans, if you have completed all steps above, you have not only completed the installation and set-up of your store but your store will now be fully PCI Compliant!

### A Note about Scans.

As indicated above, the major credit card brands (Visa, Mastercard etc.) also categorize merchants according to the number of transactions they carry out each year. For this purpose they have four levels of categorization, levels 1-4.

The lowest category, Level 4, means that you process fewer than 20,000 transactions per year for each of the credit card brands. So, if you do less than 20,000 transactions for each of Visa, Mastercard etc, you are categorized as a Level 4 store.

Level 4 stores are required to comply with the requirements of whichever SAQ is applicable to them PLUS some other requirements depending on which SAQ they use. Full details of store Levels as categorized by Visa are shown below:



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 <sup>2</sup>	<ul style="list-style-type: none"> <li>• Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")</li> <li>• Quarterly network scan by Approved Scan Vendor ("ASV")</li> <li>• Attestation of Compliance Form</li> </ul>
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	<ul style="list-style-type: none"> <li>• Annual Self-Assessment Questionnaire ("SAQ")</li> <li>• Quarterly network scan by ASV</li> <li>• Attestation of Compliance Form</li> </ul>
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	<ul style="list-style-type: none"> <li>• Annual SAQ</li> <li>• Quarterly network scan by ASV</li> <li>• Attestation of Compliance Form</li> </ul>
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"> <li>• Annual SAQ recommended</li> <li>• Quarterly network scan by ASV if applicable</li> <li>• Compliance validation requirements set by acquirer</li> </ul>

CRE research shows that many small to medium merchants who use our software, are Level 4 stores.

Some merchants will also be required to get quarterly scans of their hosting environment. For example, some of our merchants are Level 2 and 3 stores based on the table above. In their case, even if they follow our RapidPCI™ process and submit SAQ – A, they WILL in addition, be required to have quarterly scans of their hosting environment. Note that passing scans on your servers does not mean that you are required to have all of the expensive security measures of full

PCI Compliance on your servers. (These security measures are explained in more detail at the end of this document in the section headed 'Introduction to PCI Compliance'

You will though need to implement some basic security requirements to pass those scans and our partner Controlscan can help you with this. If you are a Level 2 or 3 store go to [Controlscan](#) to arrange regular scans of your hosting environment. Controlscan Inc. will assist you with the right scanning package and will advise you on any changes necessary to your hosting environment in order to pass the scans.

NOTE. It is most likely that if you are categorized as a Level 4 store you will not be required to get scans. HOWEVER, all merchants should check with their Merchant Account financial institution to determine if you are required to have scans. The banks set their requirements in this area and there may be differences from one bank to another. In most cases, level 4 stores using the Rapid PCI process will not be required to have scans. But you must check with your merchant account bank to be sure of your position on this requirement.

## INTRODUCTION TO PCI COMPLIANCE

Chain Reaction Ecommerce 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 CRE Secure payment module coupled with the RapidPCI™ process, will enable merchants to become PCI Compliant. If all installation and configuration requirements are followed carefully, merchants will find that their completion of the PCI Compliance process will be simple and easy to carry out.

### Difference between PCI Compliance and PA-DSS Validation

There are two sets of standards set by the PCI Council. In simplest form, these standards apply as follows:

**PA – DSS** – Applies to the software vendor *who builds* the software that handles cardholder data.

**PCI – DSS** – Applies to the merchant or service provider *who operates* the software that handles cardholder data.

The software vendor in this case would be CRE Secure Payments LLC. We are the company that is the developer of your CRE Secure payment module. As our module processes and transmits cardholder information we are required to certify our software to the PCI Council's PA – DSS standards.

The merchant is you, our customer, who will be using the CRE Secure payment module software. All merchants are required to operate their software in accordance with the PCI – DSS security requirements

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 October 1<sup>st</sup> 2009.

The PCI DSS requirements cover all system components within the CRE Secure environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

*All merchants are required to meet and address these standards for the handling, management and transmission of credit card data as laid down by the Payment Card industry Council.*

As a software vendor, CRE Secure Payments LLC (CRE) is required by the PCI Council to be "PA-DSS Validated." In addition, as merchant transactions connect to payment processors and acquiring banks through the CRE Secure payment system, we are required by the PCI Council to be PCI Compliant.

CRE has undertaken an assessment and certification compliance review with the Visa -certified independent assessment firm, Coalfire Systems Inc. ([www.coalfiresystems.com](http://www.coalfiresystems.com)) to ensure that our ecommerce software and systems conform to industry best practices and PCI Standards when handling, managing and storing payment-related information.



PA-DSS is the standard against which the CRE Secure payment module has been tested, assessed, and validated. The CRE Secure module has been validated to perform to the PCI Council standards required for the handling, managing and storing of payment-related information and in so doing will enable merchants to become PCI Compliant, provided that the module is used as described in the CRE RapidPCI™ process.described above.

PCI Compliance is an assessment of the merchants' actual server (or hosting) environment. Obtaining "PCI Compliance" is the responsibility of you, the merchant and your hosting provider, working together, using a PCI compliant server architecture, with proper hardware & software configurations and access control procedures.

The PA-DSS Validation referred to above ensures that the CRE Secure payment module will enable you to achieve and maintain PCI Compliance with respect to how the CRE Secure payment module handles user accounts, passwords, encryption, and other payment data related information. The CRE RapidPCI™ process has been designed to make compliance as easy as possible by moving most of the requirements to CRE Secure instead of you the merchant having to deal with them.

### **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):

- ♦ PA –DSS Data Security Standard  
[https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

PCI DSS  
[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](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 RapidPCI™ process

As already stated, Chain Reaction Ecommerce is committed to ensuring the safety of cardholder data and assisting merchants to become PCI Compliant. The CRE Secure payment module has achieved validation to the Payment Application Data Security Standards (PA – DSS), as required by the Payment Card Industry Council. The following features have been engineered into the payment module to ensure that it will comply with these requirements:

- (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 RapidPCI™ process, the module will ensure that no credit card information is seen or handled by the merchant.
- (4) The CRE Secure hosted page accessed 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.

If you wish to process credit cards in your online store, your merchant account financial institution will require you to use a shopping cart that is certified to PA-DSS requirements.

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 RapidPCI™ 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 application 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 RapidPCI™ process.



## 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 your customers with a hosted page that looks almost exactly like all the other pages in your store. So the customer experience is consistent from the beginning to the end of the transaction process.

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

The combination of functions in the CRE Secure Payment System allows your customers to pay you with a credit card without you needing to worry about capturing, transmitting or storing credit card information in your store. In fact you never even see the customer credit card information. And, all this happens while maintaining a great customer experience.

This means that you do not have to host your store in a high security PCI Compliant environment and comply with all of the 12 steps as described above. All you need to do to complete your PCI Compliance process is to fill out and sign a brief Self Assessment Questionnaire (SAQ) version A and fax it to your Merchant Account bank. (See instructions above)

You may not even require any scans of your hosting environment as long as you are processing less than 20,000 transactions in your store per year, per card brand. (See above installation instructions if you process more than 20,000 transactions per year, per brand.)

Scans are certainly a useful security precaution. However you may not be required to carry them out under the PCI rules. (Note however you should always check with your acquiring bank on the question of scans as they set the rules.)

As long as you complete the steps exactly as outlined above in the CRE RapidPCI™ process, you do not need to do anything else to be PCI Compliant! Oscommerce and CRE Secure have done it all for you!

## 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](http://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 downloads 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™, RapidPCI™ process and all logos are trademarks of Chain Reaction Ecommerce, Inc. 2009. All rights reserved; [www.cresecure.com](http://www.cresecure.com)