CoLinear Systems, Inc.

Response PCI/PA-DSS Implementation Guide

Response version 10

v10

Table of Contents

Response V10 PCI/PA-DSS Implementation Guide....3
Introduction:....3
Scope and Target Audience....3
History:....3
Payment Card Industry Data Security Standard (PCI DSS)....3
Payment Application Data Security Standard (PA-DSS)....4
PCI Compliance and Validation....4
Installation of Response Version 10....5
Server Environment....5
Minimum System Requirements....6
Memory:....6
Operating System:....6
Disk:....6
Database:....6
Application Deployment....6
Installation of the sql server / application server....6
Response Version 10 Secure Implementation Guide....7
Workstation configuration....9
Update to Response PCI compliant build 5095 or greater (IF needed)....9
Post-Deployment Configuration....10
Legacy Credit Card Data....10
Details on Purge Sensitive Data....11
Debug Logging / Test Mode....12
Set a Password Policy....13
Additional Password Considerations....13
Configure Credit Card System File....14
Encryption Utility....14
Key Management Responsibilities....15
Re-Key of Credit Card based sensitive data....16
Batch Order Import....17
Email Security....17
Wireless Communications....17
Access Control....17
Remote Access....18

Non-Console Administrative Access 18
Notes for Integrators 18
Maintenance to Implementation guide 18
FAQ: 20

Response V10 PCI/PA-DSS Implementation Guide

Introduction:

Scope and Target Audience

This guide covers Response Version 10 , and is intended for merchants and integrators who wish to implement the application in accordance with guidelines set by the Payment Card Industry (PCI).

History:

Payment Card Industry 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 (PCI SSC). The main purpose of the council is to produce and maintain the Data Security Standard (DSS). This is a set of rules and requirements that when followed will help prevent fraud, hacking, and other threats to private cardholder data. The main objectives of the PCI DSS are as follows:

- Build and Maintain a Secure Network
  - Install and maintain a firewall configuration to protect cardholder data
  - Do not use vendor-supplied defaults for system passwords and other
  - security parameters
- Protect Cardholder Data
  - Protect stored cardholder data
  - Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Use and regularly update anti-virus software
  - Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Restrict access to cardholder data by business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Track and monitor all access to network resources and cardholder data
  - Regularly test security systems and processes
- Maintain an Information Security Policy
  - Maintain a policy that addresses information security

You can find and review the complete specification by visiting the URL below.

https://www.pcisecuritystandards.org/tech/index.htm

This guide is intended to help merchants implement the Response Version 10 application in a way that is compliant with version 1.1 of the PCI DSS.

Payment Application Data Security Standard (PA-DSS)

PA-DSS was created by Visa 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 (Payment Card Infrastructure).

Response Version 10 has been designed to meet all of the requirements of the PABP. This does not automatically make you, the merchant, PCI DSS compliant. It is necessary that the recommendations and instructions in this guide are followed.

PCI Compliance and Validation

The PCI Security Standards Council (PCI SSC) is not a compliance organization. They do not require compliance, but individual payment networks may. Visa is one such example. They require you to comply with the PCI DSS, and you must complete some degree of validation based on the annual transaction volume processed. All merchants who handle Visa payments are required to perform at least some level of validation. The URL below directs you to Visa's Cardholder Information Security Program (CISP) and has complete details and validation procedures.

(QA - Vendor)

T3i Security

3651 Peachtree Pkwy.
Suite E 347
Suwanee, GA 30024

Security Council Board

PCI Security Standards Council, LLC

PCI Security Standards Council, LLC
401 Edgewater Place
Suite 600
Wakefield, MA USA 01880

Installation of Response Version 10

Server Environment

To achieve compliance with the DSS, you must ensure that your server environment is properly designed. Among the requirements, you must not store cardholder data on a server that is publicly accessible. It will be necessary to segment your network and use a proper firewall configuration to prevent unauthorized access to your servers. A suitable network configuration is demonstrated in figure 1 below.

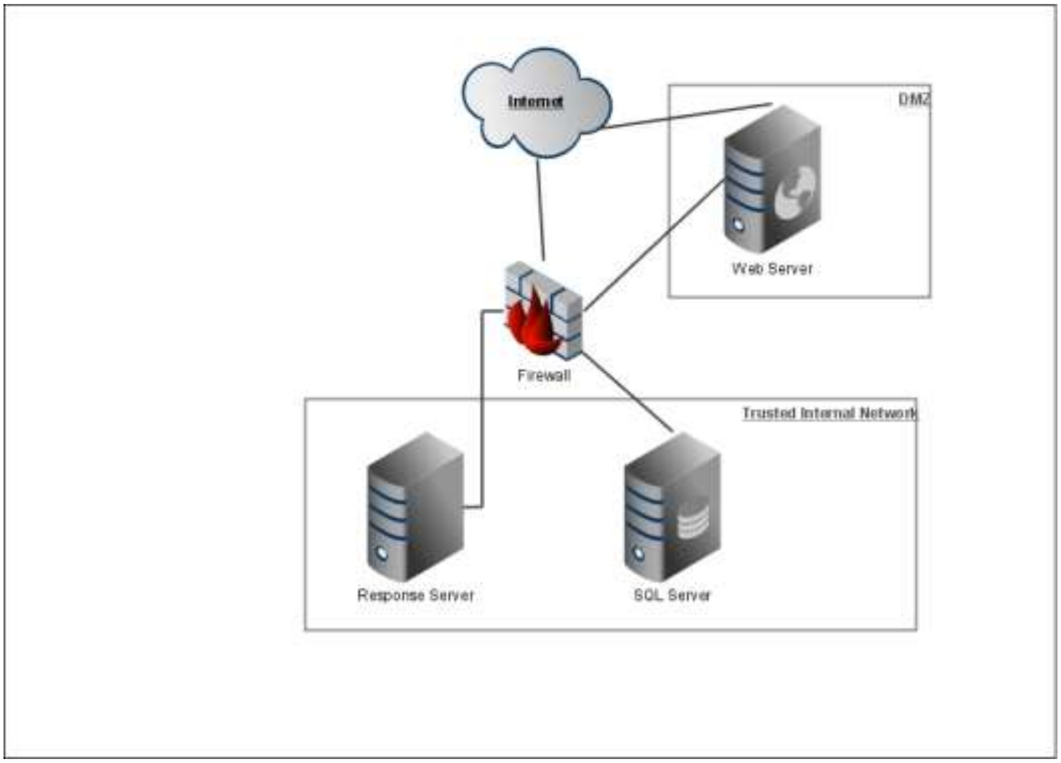


Figure 1 – Server Architecture

You must not store cardholder data on a server accessible from the Internet in order to remain compliant with the DSS. For example, you should not have your database and web server on the same machine (see figure 1). The Response database houses encrypted credit card data, but never needs to be installed on a computer accessible to the outside internet at large. The data base (Microsoft SQL Server) must be installed behind a firewall at all times, and never be accessible outside of a Virtual private network installation.

Traffic between the DMZ and the trusted internal network is allowed when required for business reasons. You must still 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 Response Version 10 are as follows:

Memory:

1 GB or higher

Operating System:

- Microsoft Windows 2000 Server
- Microsoft Windows 2003 Server
- Microsoft Windows 2008 Server

Disk:

300 MB minimum, more depending on storage needs

Database:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008

The most recent service packs and security fixes must be applied for the operating system and database. For additional details about recommended minimum system requirements refer to the Response Version 10 online help documentation at this URL:

http://support.colinear.com/doc/!-Deployment%20(new%20systems)/Response10x_System_Requirements.doc

Application Deployment

Installation of the sql server / application server

For deployment of Response software, you will need to follow these instructions:

Extract contents of the installation from the following link:
http://support.colinear.com/download/response10_demo.zip

If you intend to install SQL Server 2005 Express, then run the InstallAll.bat file with administrator privileges. This will install all requirements except for the users necessary for your Microsoft SQL database. You will need to setup a separate login within SQL Server Management Studio for each user in the SQL Server logins portion.

If you are not installing SQL Server Express Edition on the same computer, you will only need to run Setup.exe with administrator privileges. This will install the necessary files register the runtime drivers and associate the datatypes (.vd7) as executables.

You will need to install SQL Server in a manner outlined by Microsoft if you wish to install that separately. This guide is intended to give the example if wish to install SQL on the same machine as Response.

With the setup file run you will need to run the attachdatabases.vd7 utility found under your installation directory \r4w\DB directory. Enter in your login parameters for server name:

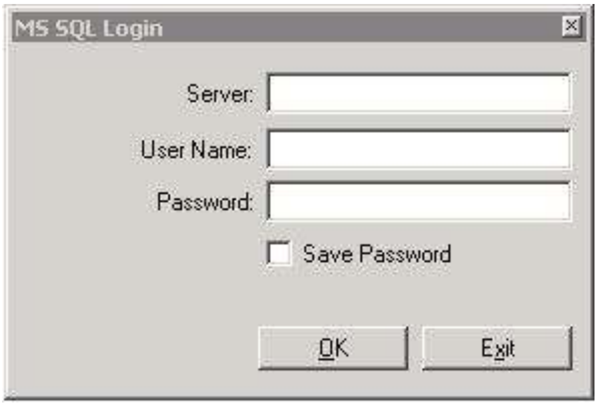
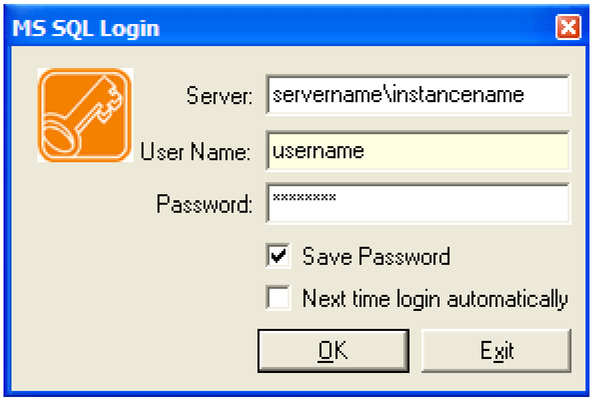


Figure 2 – Attach Databases SQL Login

This will attach the databases stored from your r4w\DB directory. Once the operation completes, the following dialogs will attach the required database files and log the attachment for the SQL login entered above. You will need to be sure to start the SQL browser if using the express edition under SQL Server configuration manager. You will also need to enable the TCP/IP protocol service for the client to connect to the database over the network.



Server: servername\instancename

User Name: username

Password: ********

☑ Save Password

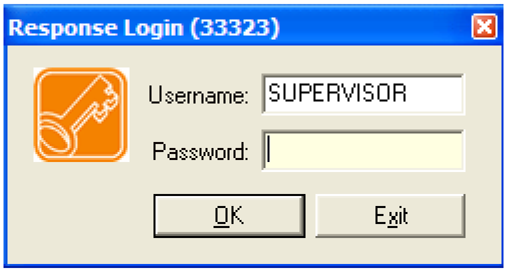
□ Next time login automatically

Figure 3 - Specify Database Connection

Response Version 10 Secure Implementation Guide

In a PCI DSS compliant installation, you can choose to use the supplied SQL Server 2005 database as long as it resides on a computer that is not accessible over the internet. That option uses a local user instance of SQL Express, which violates the best practices for database storage. Instead you must have Microsoft SQL Server 2000/2005/2008 installed on a separate server that is not accessible from the internet.

The screen shown in Figure 3 above is used if your database is set up to accept SQL Logins. You can use this form to provide the SQL username and password for connecting to the database. You should NOT use the “sa” super user account, but setup your SQL logins to allow specific users. This is accomplished under SQL Server Management Studio’s security/logins subdirectory. Each Response client installation should have a unique username and password for that client machine. Minimum password policies must include 8 character passwords containing a minimum of a single special character, and a single numeric character.

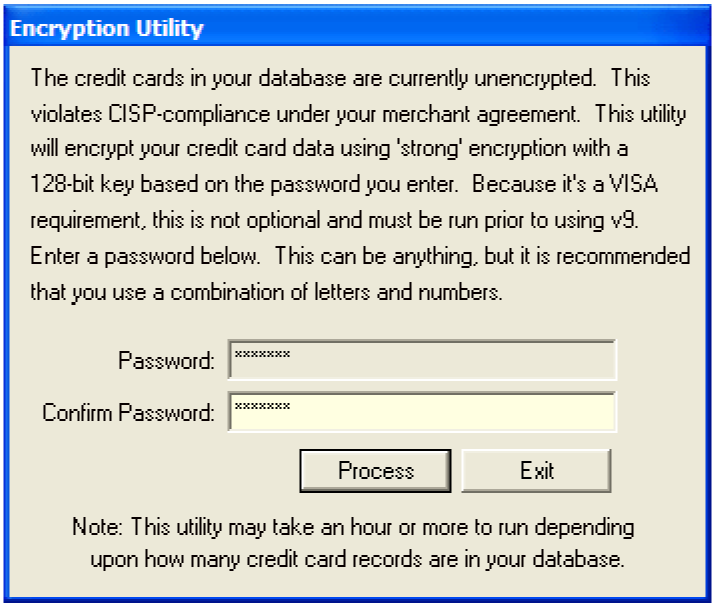


Response Login (33323)

Username: SUPERVISOR

Password:

Figure 4 – Default Supervisor Account



Encryption Utility

The credit cards in your database are currently unencrypted. This violates CISP-compliance under your merchant agreement. This utility will encrypt your credit card data using 'strong' encryption with a 128-bit key based on the password you enter. Because it's a VISA requirement, this is not optional and must be run prior to using v9. Enter a password below. This can be anything, but it is recommended that you use a combination of letters and numbers.

Password: *******

Confirm Password: *******

Note: This utility may take an hour or more to run depending upon how many credit card records are in your database.

Figure 5 – Initial encryption to Credit Card data.

For the “Supervisor” user, you will need to login with the default password: response for the post-deployment configuration procedures. At this stage, there is no password policy in force. It is your responsibility to choose a strong initial password for the super user (for the 5095 update discussed below). At a minimum it should be 7 characters long and use a mix of upper and lower alphabetic and numeric characters. Upon first login, you are met with our initial Credit Card encryption utitlity. This will only setup single-key encryption with our former 3DES algorithm. This will not be a necessary password to hold, until after you do this again for our 5095 build. Once you process this encryption utility, the server application deployment is complete and you can move on to the workstation configuration.

Workstation configuration

Setting up a workstation depends on the sharing of the colinear\r4w directory located in the directory the application installed (usually C:\program files\). The permissions for sharing of this folder should be set to allow only users and groups who will need to use the Response application.

On each workstation, the client will install by accessing the directory shared by from r4w

\\ResponseServerName\r4w\client\responsev10client.exe

…where ResponseServerName is the name of your primary response server you ran the setup.exe file on.

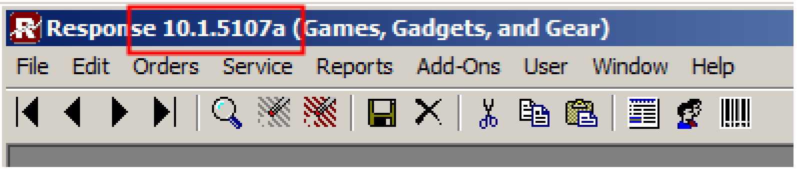
Once installed you will run the client from the programs menu / colinear / response 10 shortcut from the start button. This will present you with the login to the database. You will need to be sure to login with the login setup for that database user name. Once entered, check the “Save Pasword” and “next time login automatically” check boxes listed in Figure 3. This will default that client installation with that username. Be aware you will still need to setup a user within Response from the Supervisor account, but the merger between database user and Response user addresses critical forensic evidence in the need to view changes made to the database. You may further choose to lock this change within the permissions set in the following registry file:

HKEY_CURRENT_USER\Software\CoLinear\Response

By using the c:\windows\system32\regedit32.exe registry editor. Bear in mind this change will not allow the dynamic change of each client installation. Once you install each of your workstation clients in this manner, the server application deployment is complete and you can move on to updating to our initial PA-DSS compliant build 5095 if you are not already there.

Update to Response PCI compliant build 5095 or greater (IF needed)

Once you have installed Response you may need to update to our PCI compliant build #5095 or greater. When you open Response the application window title bar shows you the build #. This example shows Response version 10.1 the build # is 5107a



Response 10.1.5107a (Games, Gadgets, and Gear)

The latest build and instruction for installing it can be found here:
http://support.colinear.com/download/r10/10xbuilds.htm

Procedure for updating will be to verify the corresponding md5 hash number found on the CoLinear update site next to the 5095 build:

http://support.colinear.com/download/r10/10xbuilds.htm

The MD5 number will need to be entered upon extraction of the update file included in the .zip archive [to be fixed].

Review release notes and follow instructions provided. Questions should be directed to support@colinear.com.

Once updated, login password will be changed for the supervisor password, and will now have a password in all capitals = ”RESPONSE”. You will need to change this according to your post-deployment password business requirements. Your post deployment guideline will follow. You will need to run the Key management encryption within the PCI Security Management module to properly re-Encrypt your credit card data.

Note that this is only temporary in order to setup the constructs to enable dual – key control as described in the post – deployment configuration. The main reason for this is to allow for an available amount of time that this procedure can run, as this will tie up existing card data already in place when you run the dual – key encryption utility.

Post-Deployment Configuration

Ensure password policies / deletion previous auth data / setting up key management.

RCK (Response Connectivity Kit) users.

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 of RCK. You will need to have a certificate issued for a domain to allow this for visitors to your website. Setting up and enabling is outside the scope of this guide, and securing your web server should be handled by your web developer. Once SSL is enabled, the admin site will automatically run under the https context. Secure customer areas like login and account settings will also use https so that private data is not transmitted in the clear. Firewall rules are necessary to apply to your RCK server. RCK can be installed within your company’s firewall, but there only needs to be an internal IP address allowed to access the Database server machine.

Legacy Credit Card Data

While magnetic stripe data, card validation values or codes, and PINs or PIN block data are not (and never have been) stored within the database/software, Response Version 10 has tools available to securely delete sensitive data should the need arise. To securely delete the data, we will overwrite it with dummy text and then remove it from the database. This will ensure the data does not reside anywhere on disk or in memory when it is removed (See figure 6). This is intended for upgraded systems, as new systems will not have any existing credit card data. The locations where we store Legacy data is as follows:

<u>Database</u>

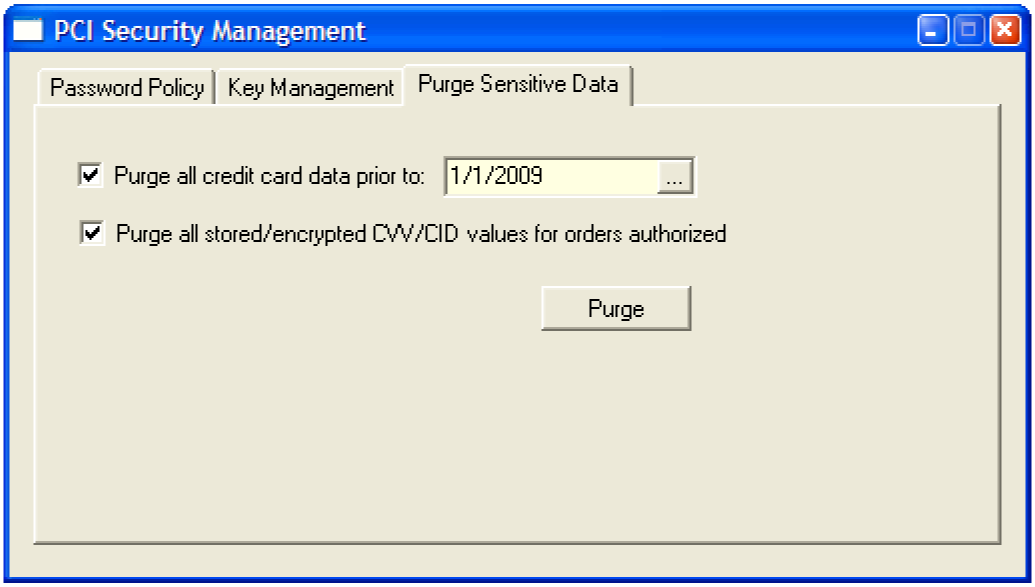
- Custcard
- Crtrans.cc_encrypted

- Crtrans.credit_card_num
- Crtrans.expiration
- Crtrans.cvv2
- Oshiptrn.expires
- Oshiptrn.credit_card_#
- Oshiptrn.cc_encryted
- Sysoent.cc_encrypted
- Sysoent.credit_card_#
- Sysoent.expires
- Sysoent.cvv_encrypted
- Sysoent.cvv2

All of the above fields are accessible by the secondary process module. If your company is using this module for creating transactional emails, be aware that you will not be able to send any credit card numbers in full – only card numbers as hashed numbers (######******####). The first 6 and last 4 are available – but it is advised to only show the last 4 for the email. Under no circumstances should the encrypted card data be sent through a transactional email. The secondary process should be locked for use by any response users except for managers/key custodian/CCView/supervisor security groups.

To purge go to

File → Supervisor Options → Security Setup → PCI Security Management:



☑ Purge all credit card data prior to: 1/1/2009

☑ Purge all stored/encrypted CVV/CID values for orders authorized

Figure 6 – Purge Sensitive Data tab

Details on Purge Sensitive Data

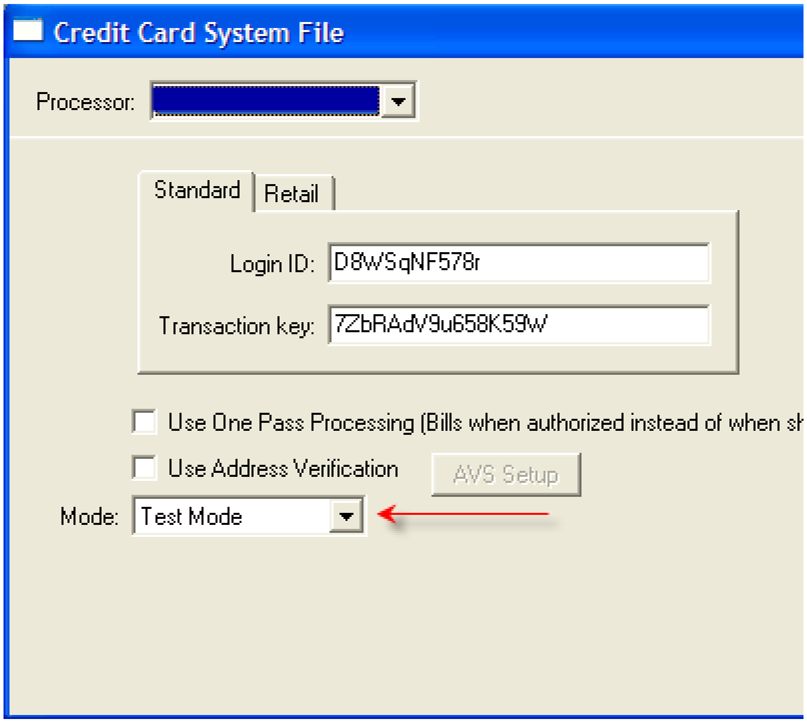
When you press the Purge button it does the following:

- removes the prior credit cards in the CUSTCARD table based on custcard.last_used date.

- Prior to build 5104 the purge routine wipes out the encrypted card number AND the masked number so you won't have any reference. In final build 5104 and greater the routine will only wipe the encrypted number and leave the masked number.
- You will still see the credit card transactions (CRTRANS data) in service lookup. This is, for example to see how much was charged or credited. But you won't see any relevant card data within the credit card transaction record.
- The PCI purge routines remove the card data from the transactions. You should still run “purge ECC transactions” to remove the CRTRANS records completely.

Debug Logging / Test Mode

Payment gateway integrations provided by Response Version 10 all support optional debug logging within the credit card setup utility. The debug log files generated by our integrations will not include sensitive credit card data. This functionality should be used only when setting up a new credit card processor. Once debugging your credit card setup for your processor, you will need to address using the purge sensitive data utility to destroy sensitive data. Be advised that this will destroy all existing data. Debug logging should be used on a test installation on a separate server to ensure existing live data is not compromised (See Figure 7). In order to practice in a PCI compliant manner, you will need to complete this process by wiping all your old data using the Purge sensitive data utility in Figure 6. Only then can you complete this and changing your credit card system file to “Live” mode to authorize/capture credit card funds.



Processor:

Login ID: D8WSqNF578r

Transaction key: 7ZbRAdV9u658K59W

☐ Use One Pass Processing (Bills when authorized instead of when sh

☐ Use Address Verification

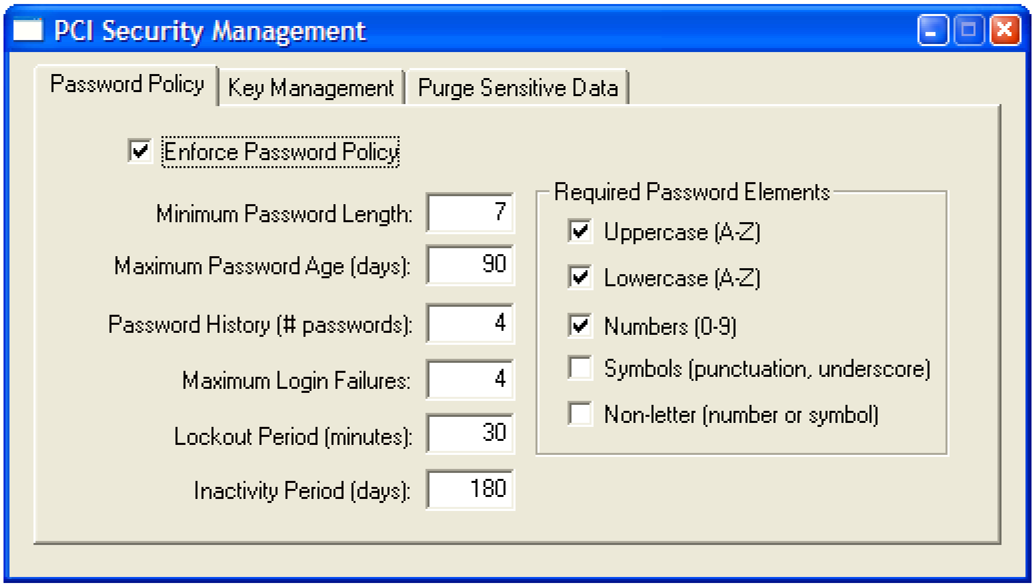
Mode: Test Mode

Figure 7 – Debug Logging / Test Mode

Set a Password Policy

Response Version 10 allows you to specify separate password policies for administrators and consumers. The DSS requirements specify the following minimums for your administrator password policies (see Figure 8):

- Minimum of 7 characters
- Must use numeric and alphabetic characters
- Password history should maintain the last 4 passwords
- Passwords must expire at least every 90 days
- Account must be locked after 4 attempts
- Account lockout will disable the users password entirely, and will have to be reset by a manager/supervisor



☑ Enforce Password Policy

Minimum Password Length: 7
Maximum Password Age (days): 90
Password History (# passwords): 4
Maximum Login Failures: 4
Lockout Period (minutes): 30
Inactivity Period (days): 180

Required Password Elements
☑ Uppercase (A-Z)
☑ Lowercase (A-Z)
☑ Numbers (0-9)
☐ Symbols (punctuation, underscore)
☐ Non-letter (number or symbol)

Figure 8 - Minimum Password Policy

To configure the password policies, access the Response Version 10 merchant admin and go to File / Supervisor Options / security setup / PCI Security Management. Figure 8 above demonstrates how to configure the policy to meet the minimum requirements.

For DSS compliance you cannot set the policy to anything less restrictive, but for increased security you can make the policy more restrictive than the minimum. For instance you could choose to require a longer password, require non letter characters, or lower the maximum password age.

These password policies also apply to any other applications, systems, and accounts that are related to your cardholder data environment.

Additional Password Considerations

In order to achieve PA-DSS compliance, Response Version 10 has introduced some features that you must be aware of in regards to user accounts:

- User passwords are stored in a one-way hash. Passwords cannot be decrypted or recovered, they can only be reset.
- All accounts, including the admin accounts, can become locked out due to too many login attempts or disabled due to inactivity.
- Passwords that are locked out are not recoverable, and will need to be reset by a supervisor.

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

Configure Credit Card System File

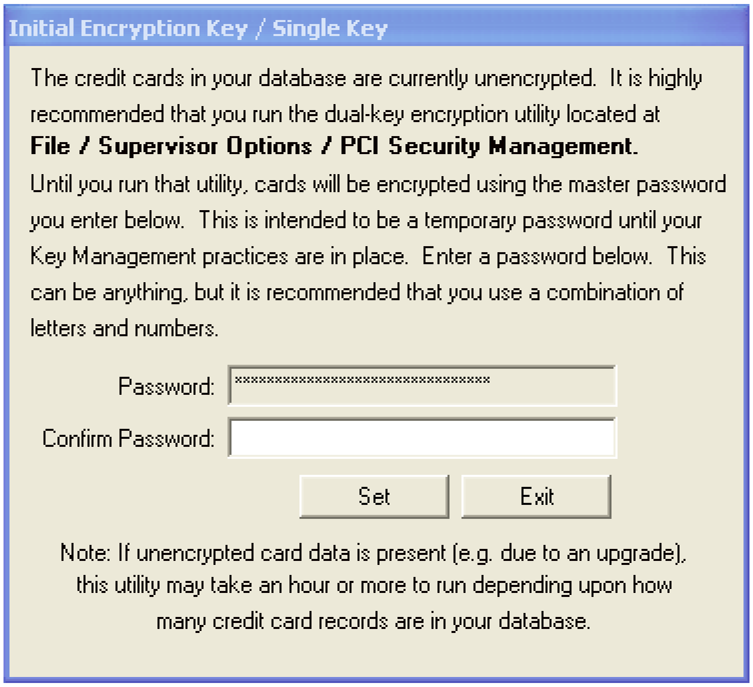
Configure your Processor to configure a payment gateway, access the merchant administration and go to Orders → Authorize / Deposit / Gift Cards → Auto Credit Card Processing → Configure Setup File. A screen will display all of the gateways that are currently available to be configured. You will need to have a merchant account with one of these third party providers. Click the provider you wish to configure and then enter your merchant account details. More information on setting this up can be found based on your 3rd party processor:

- Transfirst
- Orbital
- Authorize.net
- Litle
- Paymentech

The test mode for your Credit Card setup utility is only used for setting up your credit card processor information. As a mandatory security practice, your systems administrator is required to disable this debug mode altogether from this module. Security setup module will allow authorized users to disable this drop down box, as well as the rest of the forms within the credit card setup utility.

Encryption Utility

Sensitive data (such as credit card numbers) that must be stored to the database is protected with Advanced Encryption Standard (AES) cryptography. AES is a keyed encryption – you need a secret password to encrypt and decrypt the data. Response Version 10 introduces a new interface for managing this key so that your sensitive data cannot be read by anyone who does not know the key. When you deploy Response Version 10 it does not have a key set. If you are storing credit card data it is important that you set the encryption key after deployment. To manage your encryption key you must be logged in as a Response Version 10 supervisor. Go to Supervisor Options → Encryption Utility to access the Utility. To set your encryption key, fill in at least a 20 character password and press the Process button (See Figure 8).



Initial Encryption Key / Single Key

The credit cards in your database are currently unencrypted. It is highly recommended that you run the dual-key encryption utility located at **File / Supervisor Options / PCI Security Management.** Until you run that utility, cards will be encrypted using the master password you enter below. This is intended to be a temporary password until your Key Management practices are in place. Enter a password below. This can be anything, but it is recommended that you use a combination of letters and numbers.

Password: ********************************

Confirm Password:

Note: If unencrypted card data is present (e.g. due to an upgrade), this utility may take an hour or more to run depending upon how many credit card records are in your database.

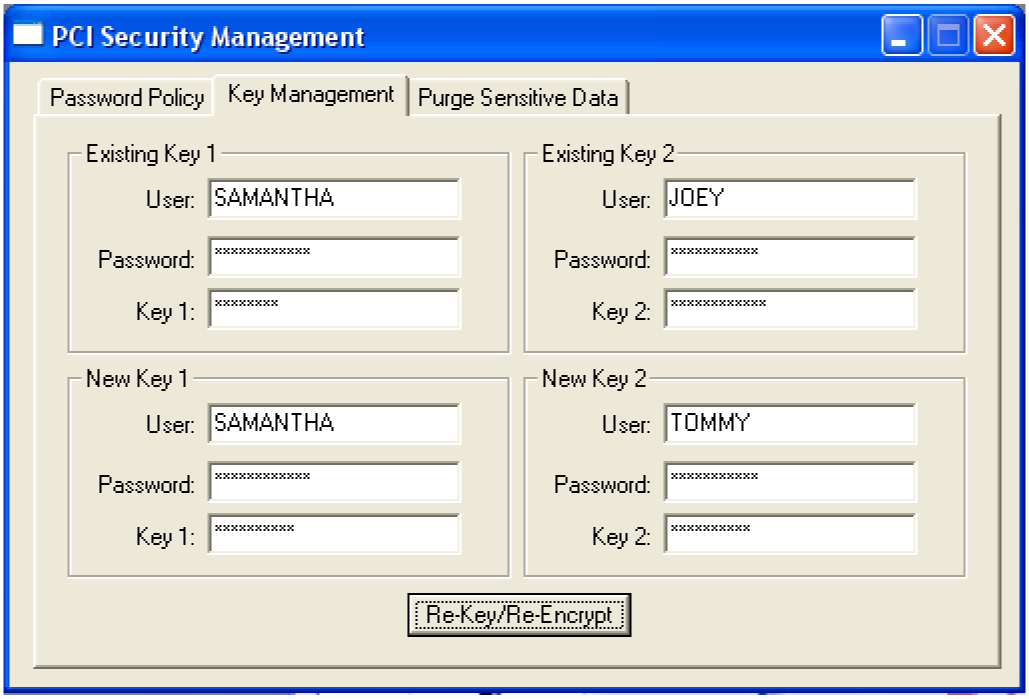
Figure 9 – Encryption Utility

This utility ensures dual-access control over the encryption/re-encryption to the client credit card data. The main thing to enforce here is that if ever one of these keys are lost, then the credit card data will not be allowed to be decrypted out of the database as a batch. This utility is meant to run with ample enough time to encrypt all your customer credit card data. Companies with years of data, may want this to run overnight as a precaution to not lock any users out of accessing existing credit card data. Be sure that the key custodians know the importance of not losing their key in the case of re-encryption. Otherwise a locked storage is recommended for access to a non-admin account. Initial setup of this key control will only allow the new key 1 & 2 to be entered, as subsequent changes to the encryption key will need to have the custodians presented at once to submit their user password, and existing key code. Be aware, we will not be able to recover your credit card data once these keys are used.

Key Management Responsibilities

Maintaining the encryption key for Response Version 10 is an important task because it impacts the security of your data. Only super users can access the key management interface. As a merchant, you must ensure that users responsible for the encryption key sign a written statement that they understand and accept the duties and responsibilities as custodian(s) of the key. The key custodians should be fully familiar with the requirements of the PCI DSS. Also be sure to maintain appropriate key backups and store the backup keys securely. Response Version 10 provides for the key backup to be split into two parts so that you may have two people each retain part of the key. This would prevent any one person from being able to reconstruct the entire key.

Change your key regularly. Every 90 days is recommended. You should also change the key any time an employee with access to the key leaves your company. Always replace the key if you know or suspect it has been compromised by any means. You have the ability as a supervisor to revoke a key. If further actions need to be handled in changing key custodians, retirement of a key is necessary (See Figure 8).



Existing Key 1
User: SAMANTHA
Password: ************
Key 1: ********

Existing Key 2
User: JOEY
Password: ***********
Key 2: ************

New Key 1
User: SAMANTHA
Password: ************
Key 1: **********

New Key 2
User: TOMMY
Password: ***********
Key 2: **********

Figure 8 – Key management

Secure transfer methods for sending and receiving of encrypted credit card data is managed through each of our processors over secure socket layer (SSL/TLS).

Re-Key of Credit Card based sensitive data

In order to rekey your Credit card data containing the encrypted Credit Card numbers – you will need to use the PCI Security Management module from Figure 8. This is where the Existing Key 1 / Key 2 will come into play. You will be required to bring both Key custodians to a login with knowledge of the Key password data. You will be allowed to change key custodians at this time, or rekey the existing data with new keys using the same key custodian users.

Note the example in Figure 8 in how we are re-keying the Credit Card data. Key custodian 1 (Samantha) has entered her user password and both her existing key and the new key to encrypt card holder data. The 2nd key custodian (Joey) is retiring his responsibility to Tommy. Joey will enter his user password and existing key, and Tommy will enter his user password and the new key to encrypt cardholder data by. In this example, mind you everyone entering in password/key data must be in the 'key custodian' security group. Depending on the size of your customer's card data accumulated – this may take quite some time to complete. Be sure to allow for ample amounts of time for this to run, as it will lock out new customers to be entered in with credit card numbers through order entry/order import.

Your company may wish to support an internal policy / procedural plan to change this key in set time increments. A minimum set interval recommended to re-encrypt your card holder data is 12 months.

Batch Order Import

The Response Batch order import utility requires an unencrypted plain text file to import orders thru this method. Users must handle those files with due care. Once the data is transferred into the Response database the CC data is encrypted, both in the temporary exceptions to review tables and in the permanent order tables after order generation. The text files should be removed after completion, or the user may choose to encrypt the text file for storage. Their method of encryption/decryption of the text data can be any they choose. Response does not do this for them.

Email Security

As distributed, Response Version 10 does not include credit account details in any of the email notifications. Email is not a secure method of transport and should not be used. Use of unencrypted email could lead to data compromise. Merchants and/or developers implementing Response Version 10 should not attempt to customize this as a feature unless an email encryption solution is also implemented.

Response Version 10 Secure Implementation Guide

Wireless Communications

If you use wireless networking to access sensitive card holder data, it is your responsibility to ensure your wireless security configuration follows the PCI DSS requirements.

Personal firewall software should be installed on any mobile and employeeowned computers that have direct access to the internet and are also used to access your network:

- Change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords and SNMP community strings.
- Disable SSID broadcasts.
- Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPAcapable.
- Encrypt wireless transmissions by using WiFi protected access (WPA or WPA2) technology.

Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address.

Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny any traffic from the wireless environment or to control any traffic if it is necessary for business purposes.

Access Control

You must carefully control access to cardholder data. This covers all places where sensitive data may be stored, including databases, servers, custodian key codes, and PCs. Follow these rules:

- Always provide unique usernames for each person who needs access.
- Always use strong passwords that meet the requirements of the PA DSS.

Remote Access

If you enable remote access to your network and the cardholder data environment, you must implement two-factor authentication. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates. You should make sure that any remote access software is securely configured by keeping in mind the following:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses
- Use strong authentication or complex passwords for logins
- Enable encrypted data transmission
- Enable account lockout after a certain number of failed login attempts
- Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed
- Enable any logging or auditing functions
- Restrict access to customer passwords to authorized reseller/integrator personnel
- Establish customer passwords according to PCI DSS requirements 8.1, 8.2, 8.4, 8.5

Non-Console Administrative Access

If you use tools to remotely access the application, you should encrypt all communication with technologies like SSH, VPN, or SSL/TLS. For example, Microsoft Terminal Services can be configured to use encryption and this should be set to the “high” level. This will ensure that the RDP data is bi-directionally encrypted with a 128 bit key.

Notes for Integrators

If you are a third party developer who integrates with Response Version 10 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:

- 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

Maintenance to Implementation guide

Instructions and frequently asked questions to our implementation guide will be maintained by our live document. Any and all detail instructions / questions to this implementation guide (including company specific examples) is maintained on our live document at http://support.colinear.com/doc/Implemention_guide_FAQ.doc

We will update this guide as appropriate on a bi-annual basis concerning notice and updates relevant from our Implementation Guide FAQ. The revision number is implemented by the year in the header of this Implementation guide.

FAQ:

Q: What does the information look like in the database?
A: Credit card number fields will show the first 6 digits plus some “xxx” characters plus the last 4 digits. The encrypted data is stored in a separate field and looks something like:
0xDEC1A121EF98A68A256D7EFC8FEB1DF473E96DBDD0A906B7000000000000

Q. I just used dbexplorer and I can see part of every credit card number - with mostly x’s filled in, though - in the credit_card_# field. But they’re definitely not “encrypted.”
A: We use the “old” credit card number field to store the partial/masked credit card data. The real/encrypted data is stored elsewhere and is restricted from viewing in dbexplorer.

Q. When I start a Response session I see an error
Encryption self test failed…… and it tells me more about Windows 2000 and service pack 4 etc. My machine is running windows XP, Win Vista, Win7. What can I do to fix this?
Answer:
The "microsoft enhanced cryptographic service provider" is what we use for encryption. If it’s not found in the operating system, Response produces the Encryption self test failure message.

A few suggestions for the machine. These are old but still relevant for Win XP, Vista and Windows 7!

Install the latest version of Internet Explorer (meaning IE 7 or 8, told you these were old) or at the very least you need to install the IE High Encryption Pack (googe that for more information)

FYI, our encryption self test encrypts known text and expects a specific result. If the result does not match or is blank, we know that encryption does not work on that machine. We use the "Microsoft Enhanced Cryptographic Provider v1.0" which is built into later versions of Internet Explorer (5.5 and greater we think) so applying IE High Encryption Pack should fix you up.

If that doesn’t work here are a couple more suggestions........

search for RSAENH.DLL - this is the Windows DLL we use for encryption. Maybe you have a bad/stale copy, or may not have it at all. Windows installs that DLL as part of the OS and part of Internet Explorer versions 6+. If it’s not there, maybe try installing IE 8x again.

or.....

In a couple of instances we found out the person’s Windows profile was corrupt. When they fixed the profile Response worked fine again. That profiles could be local or roaming we’re not sure

Or….

If you’re connecting to your client workstations over an RDP protocol (remote desktop), your network admin will need to allow for the encryption to pass through terminal services by way of the following:

Change the properties of the RDP-tcp connection on each of the RD Session Host Servers
Server Manager>
Roles>
Remote Desktop Services>
RD Session Host Configuration>
Double-click RDP-tcp

Set Security Layer - Negotiate
Set Encryption Level - Client Compatible
Click OK, Done

Let us know if you still need help!

Q. I need to find the whole CC number on a canceled order?

A. Create a new order for the customer and choose from previously used CC #'s. Select the #, even though it's still encrypted. Then switch over to customer service lookup. You can find the order (even in T status) then press the ZOOM button next to the CC number. Then you will be prompted for the manager login to display the whole CC number. FYI, this isn't supposed to be easy to get.

TECH: Document modification history

- 2nd qtr 2010: document created
- 08/04/2010: document modified
- 10/29/2010: document name changed from implementation_guide.doc to
- PA-DSS_implementation_guide.doc
- 10/29/2010: page 11; added section with details on purge sensitive data
- 04/29/2011: standardize document format of original *PA-DSS_implementation_guide.doc* and publish in .pdf format
- 6/21/2011: page 18, info on plain text files used by Batch order impord
- 11/4/2011: page 9,10, updated instructions to install build 5095 or greater
- 11/4/2011: page 21, added FAQ section