Fi-Soft Merchant Edition SP 2.0

PA-DSS 2.0 Implementation Guide

Version 1.0

Date: 09/12/11

Commerce. Anywhere.™

Confidential Information

The information contained in this document is confidential and has been prepared to establish internal policies and procedures. Do not copy or distribute without the written permission of Fi-Soft.

Guidelines for use of This Template:

This document is intended for use with Fi-Soft Merchant Edition SP software. Fi-Soft Merchant Edition SP software is compatible with QuickBooks Pro and Premier Versions 2006 or newer, and QuickBooks Enterprise Solutions version 6.0 or newer.

Fi-Soft Merchant Edition SP software is for use only in a Windows operating system environment. Refer to the Fi-Soft Merchant Edition SP User Guide for more details.

Table of Contents

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. Fi-Soft MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER Fi-Soft NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to, PA-DSS and DSS.

The retailer may undertake activities that may affect compliance. For this reason, Fi-Soft is required to be specific to only the standard software provided by it.

About this Document

This document describes the steps that must be followed in order for your Fi-Soft Merchant Edition SP installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 1.2 dated October, 2008).

Fi-Soft instructs and advises its customers to deploy Fi-Soft applications in a manner that adheres to the PCI Data Security Standard (v1.2). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various “Benchmarks”, should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

If you do not follow the steps outlined here, your Fi-Soft Merchant Edition SP installations will not be PA-DSS compliant.

Revision Information

Name	Title	Date of Update	Summary of Changes

Note: This PA-DSS Implementation Guide must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. Fi-Soft will distribute the IG to new customers via:

Fi-Soft website (www.fi-soft.com)

Distributed with Fi-Soft Merchant Edition software initial download or purchase

Executive Summary

Fi-Soft Merchant Edition SP 2.0 has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 2.0. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc. 361 Centennial Parkway Suite 150 Louisville, CO 80027	Coalfire Systems, Inc. 150 Nickerson Street Suite 106 Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Payment Application as a PA-DSS validated Application operating in a PCI Compliant environment.

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):

- Payment Applications Data Security Standard (PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

- Open Web Application Security Project (OWASP)
  http://www.owasp.org

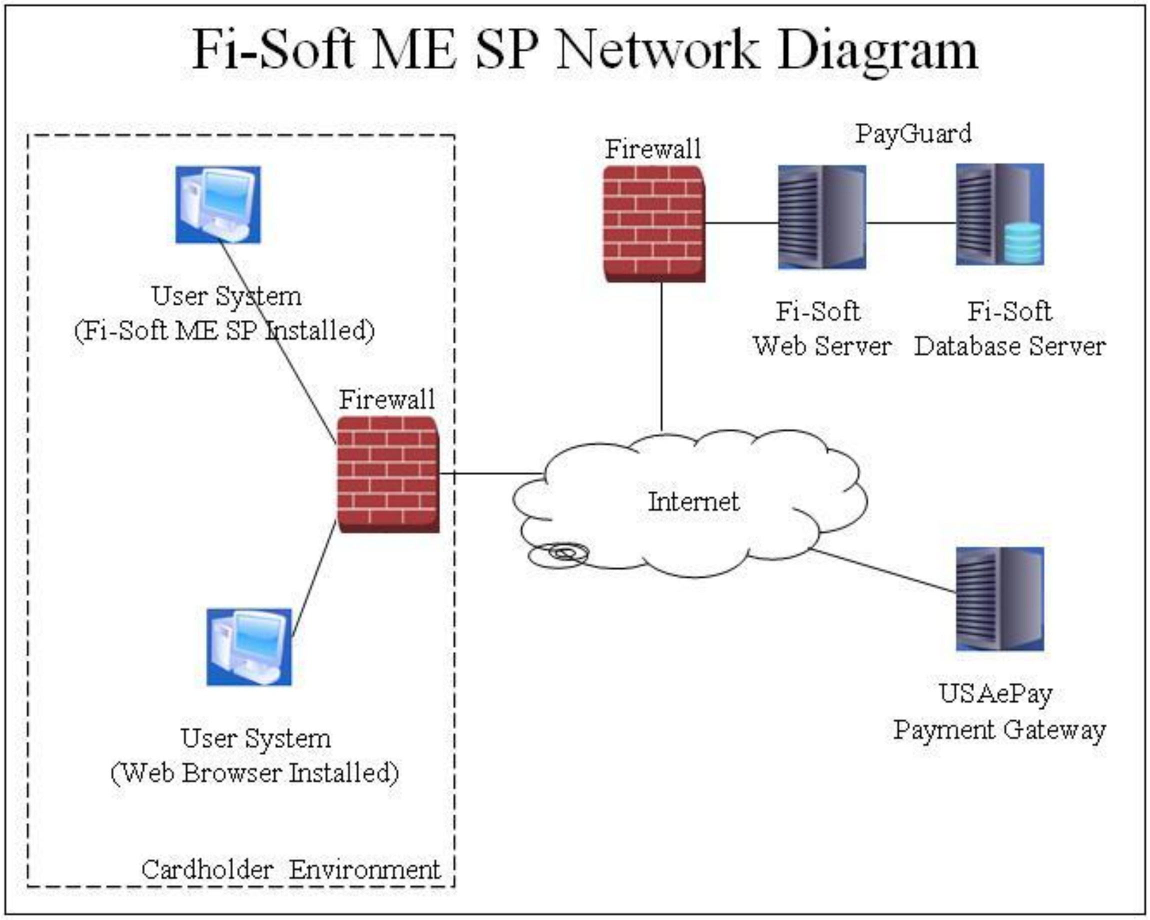
Application Summary

Payment Application Name:	Fi-Soft Merchant Edition SP
Payment Application Version:	2.0
Application Description:	Payment processing software. For use on the web and Windows operating systems.
Application Target Clientele:	Small and mid-sized businesses
Components of Application Suite (i.e. POS, Back Office, etc.)	Desktop software – Installed on merchants Windows based desktop/server systems.

	Web software – Hosted by Fi-Soft.
Required Third Party Payment Application Software:	USAePay Payment Gateway
Database Software Supported:	MS SQL 2008
Other Required Third Party Software:	USAePay Payment Gateway
Operating System(s) Supported:	The latest supported versions of: Windows XP Windows Vista Windows 7 Windows Server 2003 Windows Server 2008
Application Functionality Supported	Select one or more from the following list: ☐ **POS Suite** ☐ **POS Admin** ☐ **Shopping Cart & Store Front** ☐ **POS Face-To-Face** ☐ **Payment Middleware** ☐ **Others (Please Specify):** ☐ **POS Kiosk** ☐ **Payment Back Office** ☐ **POS Specialized** ☐ **Payment Gateway/Switch**
Payment Processing Connections:	Payment processing is done through the USAePay payment gateway.
Description of Versioning Methodology:	Version standards for Fi-Soft Merchant Edition follows the below scheme: Product Name X.Y.z X– Major version Y – Minor version z– Internal builds cycle number For the outside world the product will be informed by the Major and Minor numbers. For example: Fi-Soft Merchant Edition SP 2.2, Fi-Soft Merchant Edition SP 3.0, etc. Changes in the major version number (X) A change in the major version number is done for when there is a large change in the functionality, performance, or behavior of the underlying product.

	Changes in major version number will be relatively infrequent. Normally major releases will follow a yearly cycle. Sometime market demands may push 2 major releases in a year also. Changes in major version number will be restricted to those requiring an update or recertification to applicable payment security standards (currently PA-DSS). Changes in the minor version number (Y) Changes in the minor version number indicate a release that has additional functionality and changes/extensions to the product. These changes and extensions will be designed to deliver the functionality that Fi-Soft users require in a growing and changing industry (e.g. improved performance and compatibility), and to address any issues identified in previous releases (e.g. improved ease of use). Depending on the product a minor release can be expected every few months. Internal builds – cycle number (z) During the development and testing cycle, product builds will be identified with last number (z). This denotes the number of builds created by the team from starting the new version development (say from Fi-Soft Merchant Edition 2.5 [assuming 2.5 is last in 2.0 series] to Fi-Soft Merchant Edition 3.0). Using this number, the product team will be maintaining the source in the source control system with labeling for easy retrieval. For example, Fi-Soft Merchant Edition 3.0.1, Fi-Soft Merchant Edition 3.0.41 Pre-release versions Apart from the above scheme, a system for denoting pre-release versions as follows. Programs that are in an early stage are often called "alpha" software. After they mature but are not yet ready for release, they will be called as "beta" software.
List of Resellers/Integrators (If Applicable):	Available upon request.

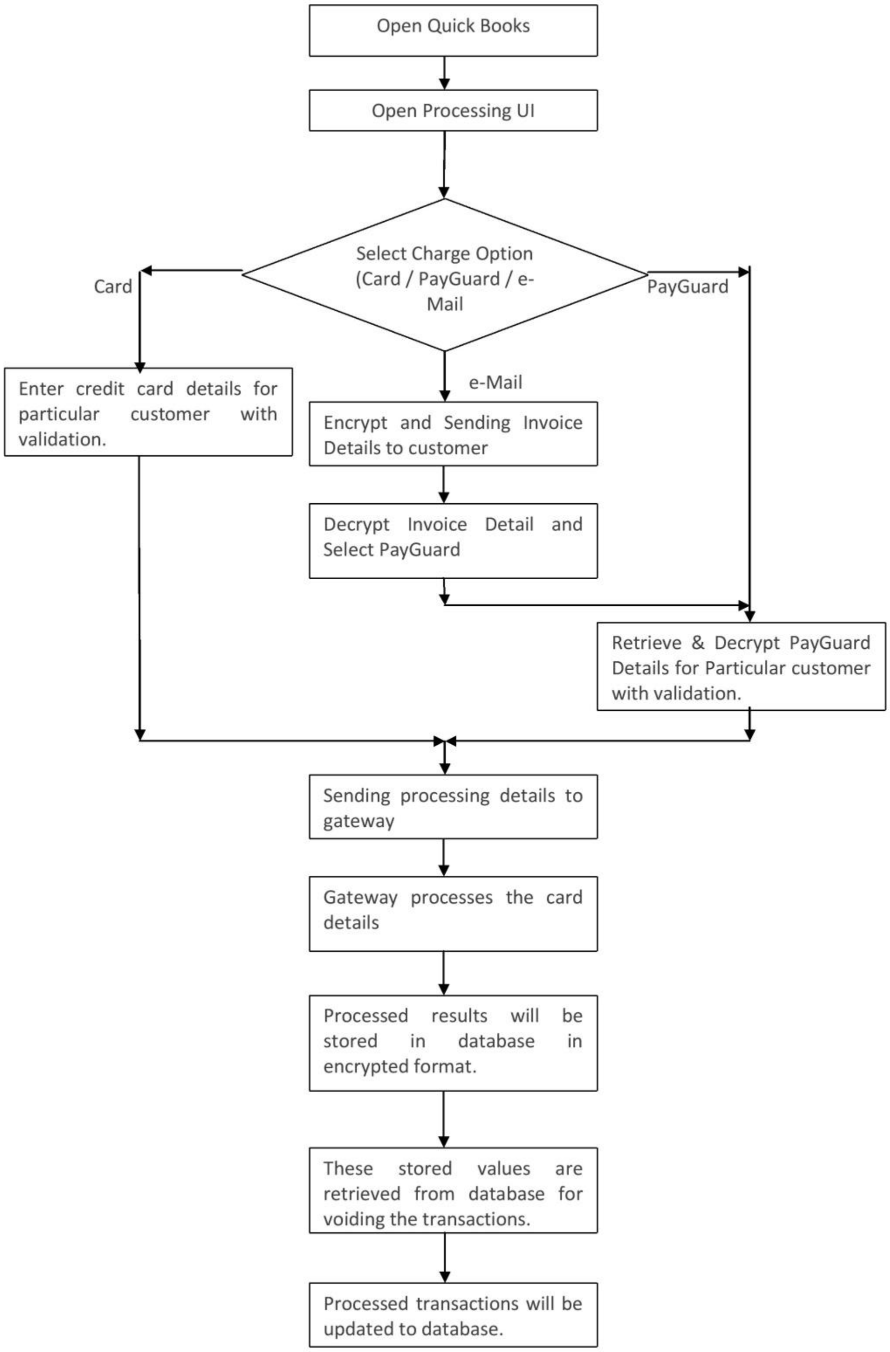
Typical Network Implementation



Fi-Soft Dataflow Diagram

Data flow diagram- For Card Data Flow

Charging the Card


Open Quick Books
Open Processing UI
Select Charge Option (Card / PayGuard / e-Mail
Card
PayGuard
e-Mail
Enter credit card details for particular customer with validation.
Encrypt and Sending Invoice Details to customer
Decrypt Invoice Detail and Select PayGuard
Retrieve & Decrypt PayGuard Details for Particular customer with validation.
Sending processing details to gateway
Gateway processes the card details
Processed results will be stored in database in encrypted format.
These stored values are retrieved from database for voiding the transactions.
Processed transactions will be updated to database.

Difference between PCI Compliance and PA-DSS Validation

As a software vendor, our responsibility is to be "PA-DSS Validated."

We have performed an assessment and certification compliance review with our independent assessment firm, to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining "PCI Compliance" is the responsibility of the merchant and your hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that the Payment Application will help you achieve and maintain PCI Compliance with respect to how Payment Application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application 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.

The 12 Requirements of the PCI DSS:

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*

Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- Sensitive Authentication Data requires special handling
- Remove Historical Cardholder Data
- Set up Good Access Controls
- Properly Train and Monitor Admin Personnel
- Key Management Roles & Responsibilities
- PCI-Compliant Remote Access
- Use SSH, VPN, or SSL/TLS for encryption of administrative access
- Log settings must be compliant
- PCI-Compliant Wireless settings
- Data Transport Encryption
- PCI-Compliant Use of Email
- Network Segmentation
- Never store cardholder data on internet-accessible systems
- Use SSL for Secure Data Transmission
- Delivery of Updates in a PCI Compliant Fashion

Implement a manual process within your environment to adhere to PCI DSS password requirements

- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- Enable Windows audit logging for the folders related to the Fi-Soft Merchant Edition application. See Microsoft Knowledge base article http://support.microsoft.com/kb/310399

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a)

Previous versions of Fi-Soft Merchant Edition SP did not store sensitive authentication data. Therefore, there is no need for secure removal of this historical data by the application as required by PA-DSS v2.0.

Sensitive Authentication Data requires special handling (PA-DSS 1.1.5.c)

Fi-Soft does not store Sensitive Authentication data for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with sensitive authentication data (swipe data, validation values or codes, PIN or PIN block data):

- Collect sensitive authentication data only when needed to solve a specific problem
- Store such data only in specific, known locations with limited access
- Collect only the limited amount of data needed to solve a specific problem
- Encrypt sensitive authentication data while stored
- Securely delete such data immediately after use

Purging of Cardholder Data (PA-DSS 2.1)

Fi-Soft Merchant Edition SP does not store cardholder data and therefore there is no data to be purged by the application as required by PA-DSS v2.0.

Any cardholder data you store outside of the application must be documented and you must define a retention period at which time you will purge (render irretrievable) the stored cardholder data.

Cardholder Data Encryption Key Management (PA-DSS 2.5.c and 2.6.a)

Fi-Soft Merchant Edition SP does not store cardholder data in any way nor does it provide any configurability that would allow a merchant to store cardholder data, therefore no encryption of cardholder data is required for PA-DSS v2.0.

Removal of Cryptographic material (PA-DSS 2.7.a)

Previous versions of Fi-Soft Merchant Edition SP never used encryption and therefore there is no cryptographic data to be securely removed as required by PA-DSS v2.0.

Set up Strong Access Controls (3.1.a and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process.

3.1.a: You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts.

All authentication credentials are provided by the application. For both the completion of the initial installation and for any subsequent changes (for example, any changes that result in user accounts reverting to default settings, any changes to existing account settings, or changes that generate new accounts or recreate existing accounts), the following 10 points must be followed per PCI 8.1, 8.2, and 8.5.8-15:

1. The application must assign unique IDs for user accounts. (8.1)
2. The application must provide at least one of the following three methods to authenticate users: (8.2)
    a. Something you know, such as a password or passphrase
    b. Something you have, such as a token device or smart card
    c. Something you are, such as a biometric
3. The application must NOT require or use any group, shared, or generic accounts or passwords.(8.5.8
4. The application requires passwords to be changed at least every 90 days (8.5.9)
5. The application requires passwords must to be at least 7 characters (8.5.10)
6. The application requires passwords to include both numeric and alphabetic characters (8.5.11)
7. The application keeps password history and requires that a new password is different than any of the last four passwords used. (8.5.12)
8. The application limits repeated access attempts by locking out the user account after not more than six logon attempts. (8.5.13)
9. The application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (8.5.14)
10. The application requires the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes.

These same account and password criteria from the above 10 requirements must also be applied to any applications or databases included in payment processing to be PCI compliant. Fi-Soft Merchant Edition SP as tested in our PA-DSS audit, meets, or exceeds these requirements for the following additional required applications or databases:

USAePay Payment Gateway

[Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.]

3.2: Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

Properly Train and Monitor Admin Personnel

It is your responsibility to institute proper personnel management techniques for allowing admin user access to cardholder data, site data, etc. You can control whether each individual admin user can see credit card PAN (or only last 4).

In most systems, a security breach is the result of unethical personnel. So pay special attention to whom you trust into your admin site and who you allow to view full decrypted and unmasked payment information.

Log settings must be compliant (PA-DSS 4.1.b, 4.4.b)

4.1.b: Fi-Soft Merchant Edition SP has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled. Disabling or subverting the logging function of Fi-Soft Merchant Edition SP in any way will result in non-compliance with PCI DSS.

Implement automated assessment trails for all system components to reconstruct the following events:

10.2.1 All individual user accesses to cardholder data
10.2.2 All actions taken by any individual with root or administrative privileges
10.2.3 Access to application audit trails managed by or within the application
10.2.4 Invalid logical access attempts
10.2 5 Use of the application's identification and authentication mechanisms
10.2.6 Initialization of the application audit logs
When the backend database for a Payment application is MS SQL Server, "the audit log is entirely contained within the SQL Server database and is initialized at database creation.
10.2.7 Creation and deletion of system-level objects within or by the application
The creation and deletion of system-level objects are to be logged by Windows. This logging is standard logging in Windows. You must maintain the log settings of these objects in The Windows Operating System.

Record at least the following assessment trail entries for all system components for each event from 10.2.x above:

10.3.1 User identification
10.3.2 Type of event
10.3.3 Date and time
10.3.4 Success or failure indication
10.3.5 Origination of event
10.3.6 Identity or name of affected data, system component, or resource.

In order to ensure proper functioning of logs, you must verify that your firewall has TCP port 443 open in a bidirectional flow.

Disabling or subverting the logging function of Fi-Soft Merchant Edition SP in any way will result in non-compliance with PCI DSS.

4.2.3 Access to application audit trails managed by or within the application

Fi-Soft Merchant Edition SP provides Merchant Admin reports that record user level changes which are made. These reports can be accessed within the Fi-Soft Merchant Edition Portal by the Merchant Admin.

Administrative level reports are only available to the Fi-Soft Admin. We recommend that you log into the Fi-Soft Merchant Edition SP web portal on a weekly basis and export the available logs into excel format using the link provided in the software. Logs should be stored in a secure location.

Services and Protocols (PA-DSS 5.4.c)

SSL

HTTPS

USAePay Payment Gateway

PCI-Compliant Wireless settings (PA-DSS 6.1.f and 6.2.b)

Fi-Soft Merchant Edition SP does not support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1:

2.1.1: Change wireless vendor defaults per the following 5 points:

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions
2. Default SNMP community strings on wireless devices must be changed
3. Default passwords/passphrases on access points must be changed
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks
5. Other security-related wireless vendor defaults, if applicable, must be changed

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.
Note: The use of WEP as a security control was prohibited as of June 30, 2010.

Never store cardholder data on internet-accessible systems (PA-DSS 9.1.b)

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)

PCI-Compliant Remote Access (10.2)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism. The means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase
2. Something you have, such as a token device or smart card

3. Something you are, such as a biometric

PCI-Compliant Delivery of Updates (PA-DSS 10.3.1)

Fi-Soft Merchant Edition SP delivers patches and updates in a secure manner:

As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise.

We do this by:

Membership in the Intuit Solution Provider Program

Members of the Intuit Developer Network

Once we identify a relevant vulnerability, we work to develop & test a patch that helps protect Fi-Soft Merchant Edition SP against the specific, new vulnerability. We attempt to publish a patch within 10 days of the identification of the vulnerability. We will then contact vendors and dealers to encourage them to install the patch. Typically, merchants are expected to respond quickly to and install available patches within 30 days.

We do not deliver software and/or updates via remote access to customer networks. Instead, software and updates are available by selecting the "Upgrade" menu option in the Fi-Soft Merchant Edition SP software.

- Patches are delivered over HTTPS and requires merchants to log into the Fi-Soft Merchant Edition SP portal.

- Integrity testing of patches or updates prior to installation is done by MD5 hash verification.

PCI-Compliant Remote Access (10.3.2.b)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop (RDP)/Terminal Server, PCAnywhere, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for PCAnywhere it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)
- Allow connections only from specific IP and/or MAC addresses
- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13
- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet
- Enable logging for auditing purposes
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Data Transport Encryption (PA-DSS 11.1.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSL or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with Fi-Soft Merchant Edition SP.

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b)

Fi-Soft Merchant Edition SP does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

Non-console administration (PA-DSS 12.1)

Fi-Soft Merchant Edition SP or server allows non-console administration, so you must use SSH, VPN, or SSL/TLS for encryption of this non-console administrative access.

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

- Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with Fi-Soft Merchant Edition SP.

Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
- Call in outside experts as needed.

Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Windows XP, Vista (32 & 64 bit), Windows 7, Windows Server 2003, Windows Server 2008. All operating systems require the latest Service Pack(s). All latest updates and hot-fixes should be tested and applied.
- 256 MB of RAM minimum, 2GB or higher recommended for Payment Application
- 30 MB of available hard-disk space
- TCP/IP network connectivity
- Internet Explorer 8 (or later), or Mozilla Firefox 4 (or later). All latest updates and hot-fixes should be tested and applied

Payment Application Initial Setup & Configuration

For setup and configuration, refer to the Fi-Soft Merchant Edition SP User Guide.