



**WinMAC (Online and Offline)  
FCMS (Full, Lite, and Reports)  
FTPCR  
CCAC  
APS-MBT100-\*\*\*  
PIL  
MCC87**

---

**Secure Implementation Guide  
(Covering CISP, PCI-DSS, and PABP requirements)**

Revision 1.0  
April 2008

© Magnetic Automation Corporation. [www.ac-magnetic.com](http://www.ac-magnetic.com)

Copyright 1990-2008 Magnetic Automation Corporation

The information contained herein is provided “As Is” without warranty of any kind, express or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. There is no warranty that the information of the use thereof does not infringe a patent, trademark, copyright, or trade secret.

Magnetic Automation Corporation shall not be liable for any direct, special, incidental, or consequential damages resulting from the use of any information contained herein, whether resulting from breach of contract, breach of warranty, negligence, or otherwise, even if Magnetic Automation has been advised of the possibility of such damages. Magnetic Automation Corporation reserves the right to make changes to the information contained herein at anytime without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Magnetic Automation Corporation.

# Table of Contents

1. Payment Systems Security
  - 1.1. Introduction
  - 1.2. Visa CISP Overview
  - 1.3. The PCI Data Security Standard
  - 1.4. Payment Application Best Practices (PABP)
  - 1.5. Payment Security Chain of Command
    - 1.5.1. Card Associations
    - 1.5.2. Acquirers
    - 1.5.3. Merchants
  - 1.6. Understanding “PABP” versus “PCI Compliance”
  - 1.7. Payment Card Industry Data Security
2. Merchant Requirements for Compliance
3. Payment Application Best Practices (PABP) Security Validation
  - 3.1. Do Not Store Magnetic Stripe, CVVS/CVC2 or PinBlock (PVV) Data
  - 3.2. Protect Stored Cardholder Data
    - 3.2.1. ICVerify
  - 3.3. Provide Secure Password Features
  - 3.4. Log Application Activity
  - 3.5. Develop Secure Applications
  - 3.6. Protect Wireless Transmissions
  - 3.7. Test for Application Vulnerabilities
  - 3.8. Facilitate Secure Network Implementation
  - 3.9. Cardholder Data Must Never Be Stored on a Server Connected to the Internet
  - 3.10. Facilitate Secure Remote Software Updates
  - 3.11. Facilitate Secure Remote Access to Application
  - 3.12. Encrypt Sensitive Traffic Over Public Networks
  - 3.13. Encrypt All Non-Console Administrative Access
  - 3.14. Maintain Instructional Documentation and Training Programs for Customers, Resellers, and Integrators
  - 3.15. Operational Considerations
4. FTP Central Reports (FTPCR)
  - 4.1. Overview
  - 4.2. Setting Up a Secure Connection Between FTPCR and FCMS computers
5. Hardening Your System
  - 5.1. Important Countermeasures
  - 5.2. Configuring Windows Firewall for FCMS/WinMAC and ICVerify
6. Resources on the World Wide Web
  - 6.1. Card Association Links
  - 6.2. Security Organizations
  - 6.3. Associated Technologies
7. References
  - 7.1. References

# 1. Payment Systems Security

## 1.1. Introduction

In the past decade, the methods of processing credit card data have grown more sophisticated and also dangerous. Payment systems have moved more away from paper into real-time electronic processing and settlement. Typically, systems were in a closed loop configuration and attacks on mom-and-pop merchant networks were virtually unheard of at that time. Now, with the move towards virtually all processing being done in real-time over the Public Internet, a severe gap has been created that has led to several high-profile breaches over the recent timeframe.

Merchants and Vendors must now apply significant resources to information system security and network security in order to prevent a breach and fines.

Starting in June 2001, VISA began to mandate that all cardholder data must be protected wherever it resides. This program of protecting cardholder data is known as Cardholder Information Security Program or CISP.

## 1.2 Visa CISP Overview

In order to achieve CISP Compliance, all members, merchants, and service providers must adhere to the PCI Data Security Standard. Mandated since June 2001, the program is intended to protect VISA cardholder data, wherever it resides, ensuring that members, merchants, and service providers maintain the highest information security standard.

## 1.3 The PCI Data Security Standard

The Payment Card Industry (PCI) Data Security Standard consists of (12) PCI DSS requirements. The PCI DSS requirements are organized into (6) logical groups identified as control objectives. The latest PCI DSS standard as of today is Version 1.1, Release: September 2006 and is available from [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

The PCI DSS is maintained by the PCI Security Standards Council. From their website: "The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection."

“The PCI Security Standards Council’s mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.”

## 1.4 Payment Application Best Practices (PABP)

Secure payment applications, when implemented in a CISP-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data or CVV2, and the damaging fraud resulting from these breaches.

Validated applications must be capable of being implemented in a CISP-compliant manner. Software vendors are expected to provide product documentation to instruct their customers on secure product implementation. This documentation should clearly delineate vendor and customer responsibilities for meeting CISP requirements.

PABP is a qualification, much like the PCI DSS, but structured for payment applications.

Currently, VISA only encourages, but does not require an application to become PABP validated.

## 1.5 Payment Security Chain of Command

The main job of information systems security typically lies with the IT department, but all association rules apply to the system in regards to storing, processing, and transmitting cardholder data.

### 1.5.1 Card Associations

A card association such as Visa or MasterCard, are those who define and ultimately enforce the rules on card use.

From VISA’s website: “The Visa USA Operating Regulations are rules that govern the use of the Visa payment system.” Visa has provided, for more than a decade, a comprehensive merchant rules guide that can be downloaded from this location:  
([http://usa.visa.com/download/merchants/rules\\_for\\_visa\\_merchants.pdf](http://usa.visa.com/download/merchants/rules_for_visa_merchants.pdf))

## 1.5.2 Acquirers

An acquirer is an organization licensed as a member of Visa / MasterCard as an affiliated bank or bank/processor alliance that is in the business of processing credit card transactions for businesses (acceptors) and is always acquiring new merchants.

From Visa's website: "Members are responsible for ensuring the CISP compliance of their merchants, service providers, and their merchants' service providers. Although there may not be a direct contractual relationship between merchant service providers and acquiring members, all members remain responsible for any liability that may occur as a result of CISP non-compliance. Acquirers must include a CISP compliance provision in all contracts with merchants and non-member agents."

## 1.5.3 Merchants

A merchant is someone or a business that displays any or all Credit Card Symbol and accepts those cards. The merchant is the end receiving the payment for goods or services. **It is ultimately the Merchant's responsibility to achieve CISP/PCI Compliance.**

## 1.6 Understanding "PABP" versus "PCI Compliance"

As a software vendor, our responsibility is to be "PABP Compliant."

While this is not currently required by Visa USA, as an industry leader in the parking industry, we felt it was important to take a position and obtain this certification.

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

**Note: We want to stress that obtaining "PCI Compliance" falls on you (the merchant) using PCI compliant architecture with proper hardware and software configurations and access control procedures.**

## 1.7 Payment Card Industry Data Security

To be in compliance with this standard, all of your company's Internet connections, assigned IP addresses, and all Internet connected servers (Web, email, DNS, etc.) must have no level 3, 4 or 5 severity vulnerabilities in their most recent security audit. Audits must be conducted at least every 90 days. Various firms can assist with your scans, including Verizon Business Cybertrust, ControlScan, or other firms.

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 following high level 12 Requirements comprise the core 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

## 2. Merchant Requirements for Compliance

According to Visa, 65 percent of all merchants will be PCI compliant by the end of 2007. If an organization does not know that they need to be PCI compliant, or if an organization just doesn't want to be bothered by having to obtain PCI compliance, it soon will not matter. The goal is to have all merchants, regardless of their merchant level, to be compliant with PCI DSS.

Notes on fines: From Visa's website "If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Fine the acquiring member
- Impose restrictions on the merchant or its agent
- Permanently prohibit the merchant or its agent from participating in Visa programs

Members receive protection from fines for merchants or service providers that have been compromised but found to be CISP-compliant at the time of the security breach. Members are subject to fines up to \$500,000 per incident for any merchant or service provider that is compromised and not CISP-compliant at the time of the incident."

See <http://www.visa.com/cisp> and contact your bank, processor, or acquirer for more information.

## 3. Payment Application Best Practices Security Validation

The following sections outline the validation used against Magnetic Automation Corporation's WinMAC, WinMAC-FCMS, FCMS, CCAC, APS-MBT-100-\*\*\*, and MCC87. It also outlines configuration and developer notes associated with secure implementation as defined by the Visa Payment Application Best Practices.

We offer three credit processing options: Real-time and Real-time with Automatic Batch Failover. For further information on the two modes, please refer to the WinMAC and/or FCMS documentation.

### 3.1 Do Not Store Magnetic Stripe, CVVS/CVC2 or PinBlock (PVV) Data

The aforementioned software and hardware does not retain or store magnetic stripe, CVVS/CVC2, or PinBlock (PVV) data.

*PABP References (1.1, 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6)*

**Transaction Logs:** Magnetic Automation does not store sensitive authentication data in transaction logs.

**History files:** Magnetic Automation does not store sensitive authentication data in history files.

**Debug logs:** Under production settings, Magnetic Automation does not output sensitive authentication data in debug logs.

**Audit logs:** Magnetic Automation does not store sensitive authentication data in audit logs.

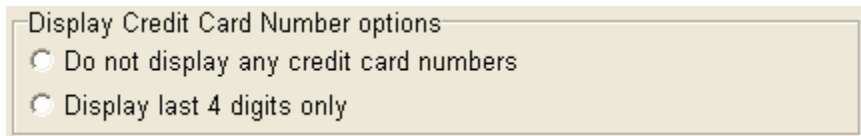
**Database schema's and tables:** Magnetic Automation does not store sensitive authentication data inside the database. Exception: In Automatic Batch Failover mode, the encrypted PAN and expiration date are stored using RC4 Stream Cipher. See below for explanation. This can be disabled.

**1.1.6** Magnetic Automation Corp's policy is to collect as little information as possible and required to help solve any particular support problem. In most cases sensitive data is not required when troubleshooting. If however any sensitive data is required and forwarded to our company for support purposes, it is handled in accordance with PABP/PCI requirements and securely removed when no longer needed.

## 3.2 Stored Data Protection

### *PABP Reference (2.1)*

**Mask displayed account numbers:** Magnetic Automation masks all digits when the Credit Card is swiped. When manually entering the card number into the WinMAC or WinMAC-FCMS software, the digits is displayed only to the cashier in order to visually verify what they are typing is correct. On the receipt to the customer, the merchant has the option to display the last four digits or no digits at all. This setting is available in WinMAC / WinMAC-FCMS and FCMS under “System Setup”.



**Figure 1: Display Credit Card Number Options in WinMAC**

**Render PAN unreadable when it is stored and Encrypt stored sensitive data:**

### *PABP Reference (2.2)*

The PAN and expiration date is only stored when Auto Batch Failover feature is enabled. We store the PAN using RC4 Stream Cipher and a complex key in the Auto Batch Database. We do not store Track1 or Track2 data from the Mag-stripe.

The data encryption algorithm is based on the RC4 symmetric stream cipher with RSA Public Key Encryption. The keys are generated using the Microsoft CryptAPI and the RSA Cryptographic Service Provider. The Protected Storage Service must be running in order for the encryption/decryption algorithms to execute.

If a key container does not exist, a new container is created under the user-profile – it is not machine specific. The initial key blob size is a random byte size between 140 to 160 bytes. We then generate a random number that is equal to the key blob length (i.e. 140) up to 32 random numbers. We use this random number to perform a bit swap on the initial key blob (i.e. bit position 0 becomes 139, etc). The total key blob size ultimately ends up being 255 bytes because we then pad the key blob with additional entropy with what is leftover. This key blob is then stored in the database – it is not the actual key, but it is representation of the key that is securely encrypted using the method above. The key container actually contains the key based on the user-profile, so you must always use the same user to run FCMS if in auto-batch mode. Once all transactions have been completely de-batched; a new key is generated and a new key blob

is stored in the database if the auto-batch condition occurs additional times.

Some examples of RC4 based cryptosystems include:

1. WEP
2. WPA
3. SSL
4. Secure Shell
5. BitTorrent protocol encryption

Users may access the Auto Batch Database from the Database menu in FCMS, but only the last four numbers of the card number are displayed. The reason for access is to allow the deletion of cards that may be bad or invalid since in Automatic Batch Failover, there is no real-time authorization. Access to the Auto Batch Database does not give any user access to the full credit card PAN and access can be restricted via user privilege in FCMS.

**Only** when Automatic Batch Failover feature is turned on is the PAN and Expiration Date stored for future processing. Note: Processing is automatic and requires no human interaction. A visual indicator listing the total amount of money batched so far and an “Offline” indicator is displayed when in Automatic Batch mode. The user can also set a threshold so that the system will only batch up to that amount of money. The maximum amount of money allowed to batch is \$10,000.

## ICVerify

For example, when using ICVerify, the credit card processing requests are passed to the ICVerify Multi-User application via a REQ/ANS file interface in a pre-defined directory (i.e. C:\MAC\ICVERIFY\REQDIR). Within a few seconds, the REQ file is picked up and deleted by the ICVerify application. Depending on your Internet connection, a response is generated by the application in a timely fashion. The following lists the REQ and ANS file format:

### REQ File Format

<Message Type>, <User ID/Clerk>, <Not Used>, <Account Number>, <Exp Date + Track Data (if available)>, <Amount>

### ANS File Format (Response)

<Y/N + Auth Code + Unique ID> Y = Approved, N = Declined. If Declined, reason is sent.

The WinMAC/WinMAC-FCMS, FCMS, and CCAC “poll” the directory waiting for the ANS file to be presented. Once the ANS file is presented, it is open and read by the aforementioned applications and deleted. Each REQ and ANS file are uniquely named by Station ID (i.e. ICVER001.REQ). If there was an application problem or the application restarts while either a REQ or ANS file exists in the “polling” directory, it will be automatically deleted from the system upon restart of either WinMAC or FCMS.

ICVerify is also a PABP Validated application and version 4.0.3 is the latest version available. All data is transmitted using 128-bit SSL Encryption to the credit card processor and is stored in a SQL database using AES 256-bit encryption with secure password features. Please refer to ICVerify documentation for more information.

### 3.3 Provide Secure Password Features

**Require a unique username and complex password for access to PC's, Servers, and databases where payment applications reside**

*PABP Reference (3.2)*

WinMAC / WinMAC-FCMS and FCMS are software applications and do not control the usernames and/or passwords for the PC's and Servers. This must be handled at the merchant level sysadmin support. Please refer to ICVERIFY User Guide on how to properly change passwords regularly and maintain PCI Compliance. The following lists the DOs and DONTs of machine security and are not all inclusive:

- Do not use the default Windows XP 'Administrator' account without a strong, complex password.
- Assign strong, complex passwords to default accounts even if that will not be used.
- Disable unused accounts
- Remove inactive accounts after 90 days

Per PCI DSS 8.5.8 to 8.5.15, the following lists how to create a complex password:

- Do not use group, shared, or generic accounts and passwords
- Change user passwords at least 90 days
- Require a minimum password length of at least 7 characters
- Use password 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
- Limit repeated access attempts by locking out the user ID after not more than six attempts
- Set the lockout duration to thirty minutes or until the administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

### 3.4 Log Application Activity

All application activity is logged into the "Alarm/Event Log". Additionally, all transactions per cashier are stored in the Shift Database.

**System Log**

Log Type Filter:  Alarm + Event  Alarm  Event

System Type Filter:  All  Revenue  Access  Count/Control  License Plate

Search for: [ ] Filter Condition: [ ] Year: 2007 Month: October

Log Type	Date	Time	Station	Station No.	Log Id.	Description	User Name
Event	10/9/2007	9:00 AM	Facility	0	658	User views logs	MAC
Event	10/9/2007	8:54 AM	Facility	0	756	User views table setup	MAC
Event	10/9/2007	8:53 AM	Facility	0	756	User views table setup	MAC
Event	10/9/2007	8:53 AM	Facility	0	601	User logs on	MAC
Alarm	10/9/2007	8:53 AM	Facility	0	401	Cannot find FCMS hardware dongle key. System shuts down.	System
Event	10/9/2007	8:53 AM	Facility	0	400	System starts up	System
Event	10/4/2007	3:44 PM	Facility	0	600	User exits to Windows	MAC
Event	10/4/2007	3:41 PM	Facility	0	1035	User views payment setup	MAC
Event	10/4/2007	3:41 PM	Facility	0	1060	User views keycard payment collection	MAC
Event	10/4/2007	3:41 PM	Facility	0	1061	User prints keycard payment collection	MAC
Event	10/4/2007	3:41 PM	Facility	0	1060	User views keycard payment collection	MAC
Event	10/4/2007	3:40 PM	Facility	0	1035	User views payment setup	MAC
Event	10/4/2007	3:39 PM	Facility	0	1020	User views access billing group	MAC
Event	10/4/2007	3:39 PM	Facility	0	1020	User views access billing group	MAC
Event	10/4/2007	3:39 PM	Facility	0	601	User logs on	MAC
Event	10/4/2007	3:38 PM	Facility	0	400	System starts up	System
Event	10/4/2007	3:05 PM	Facility	0	600	User exits to Windows	MAC
Event	10/4/2007	2:52 PM	Facility	0	1009	User views keycard account database	MAC
Event	10/4/2007	2:52 PM	Facility	0	601	User logs on	MAC
Alarm	10/4/2007	2:52 PM	Facility	0	401	Cannot find FCMS hardware dongle key. System shuts down.	System
Event	10/4/2007	2:51 PM	Facility	0	400	System starts up	System
Event	10/3/2007	10:58 AM	Facility	0	600	User exits to Windows	MAC

**Figure 2: System Log**

**Shift Transaction**

Search for: [ ]

Filter Condition: [End Date]>=10/9/2007 AND [End Date]<=10/9/2007

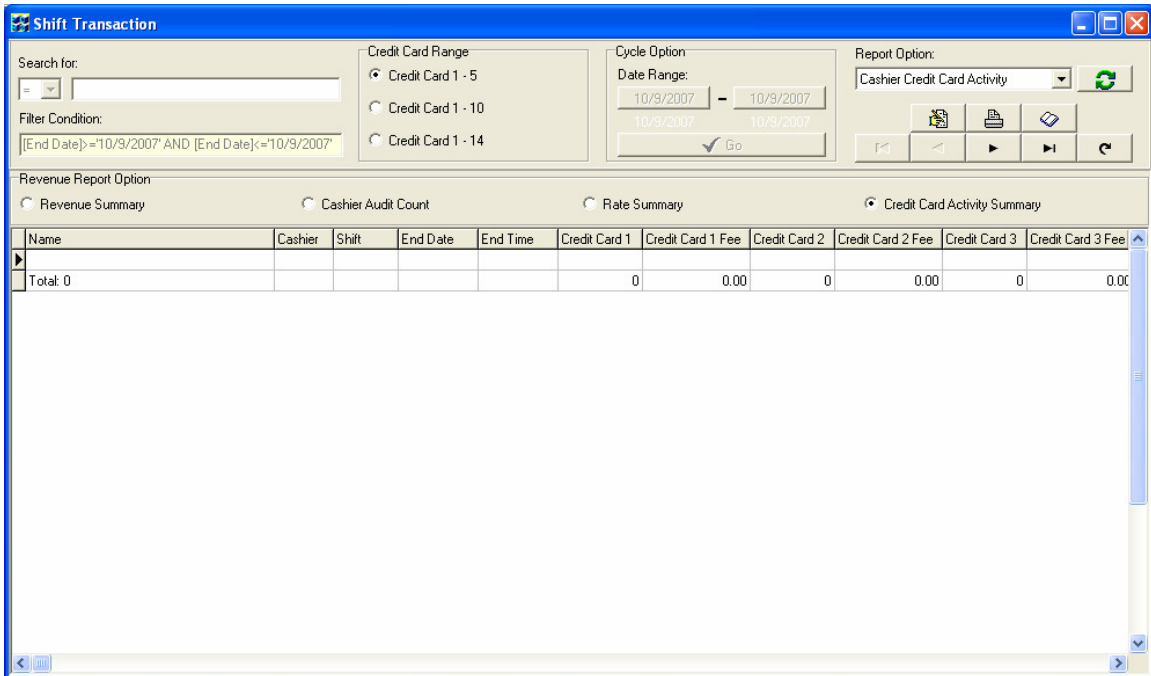
Cashier Information: Cashier: [ ] Shift: [ ] Name: [ ]

Cycle Option: Date Range: 10/9/2007 - 10/9/2007

Report Option: Shift Transaction

Cashier	Shift	End Date	End Time	Area	Station	Start Date	Start Time	Hour Stay	Minute Stay	Time Break	Transaction	Total Fee	Keycard	Keycard Fee	Val

**Figure 3: Shift Reports**



**Figure 4: Cashier Credit Card Activity**

*PABP Reference (4.1) - Validated Architecture*

FCMS and WinMAC provide extensive logging for security audits at both the internal and external level. External and internal Security logging is set to ON by default.

### 3.5 Develop Secure Applications

*PABP Reference (5.1)*

FCMS and WinMAC are provided as POS Parking applications for the management and collection of parking revenue. All of our flagship products take full (native) advantage of the latest operating system platforms. WinMAC and FCMS run on the Microsoft Windows platform. The MCC87 and APS are a proprietary embedded platform.

*PABP Reference (5.2.1) - Validated Architecture*

**All changes/patches are tested via QA:** Magnetic Automation Corporation tests all application changes internally via set QA procedures prior to releasing any code into a beta or production release.

*PABP Reference (5.2.4) – Validated Architecture*

**Custom code review:** As per company policy, all software developed by Magnetic Automation Corp complies with industry best practices and standards.

### 3.6 Protect Wireless Transmissions

*PABP References (6.1, 6.2)*

WinMAC, WinMAC-FCMS, FCMS, APS-MBT100-\*\*\*, and MCC87 can be operated over wireless networks and the reseller/installer/integrator must adhere to the following guidelines:

- Removal of All Default Keys from Wireless Equipment
- Use of appropriate encryption technologies such as VPN firewalls, 128-bit or greater SSL/TLS, 128-bit WEP (Wired Equivalent Protection) and WPA. WEP by itself is not PCI Compliant and WPA must at least be used.
- Regular key rotation
- Proper use of firewalls (Access Control Lists, IP and Port Restrictions, MAC Filters, etc)

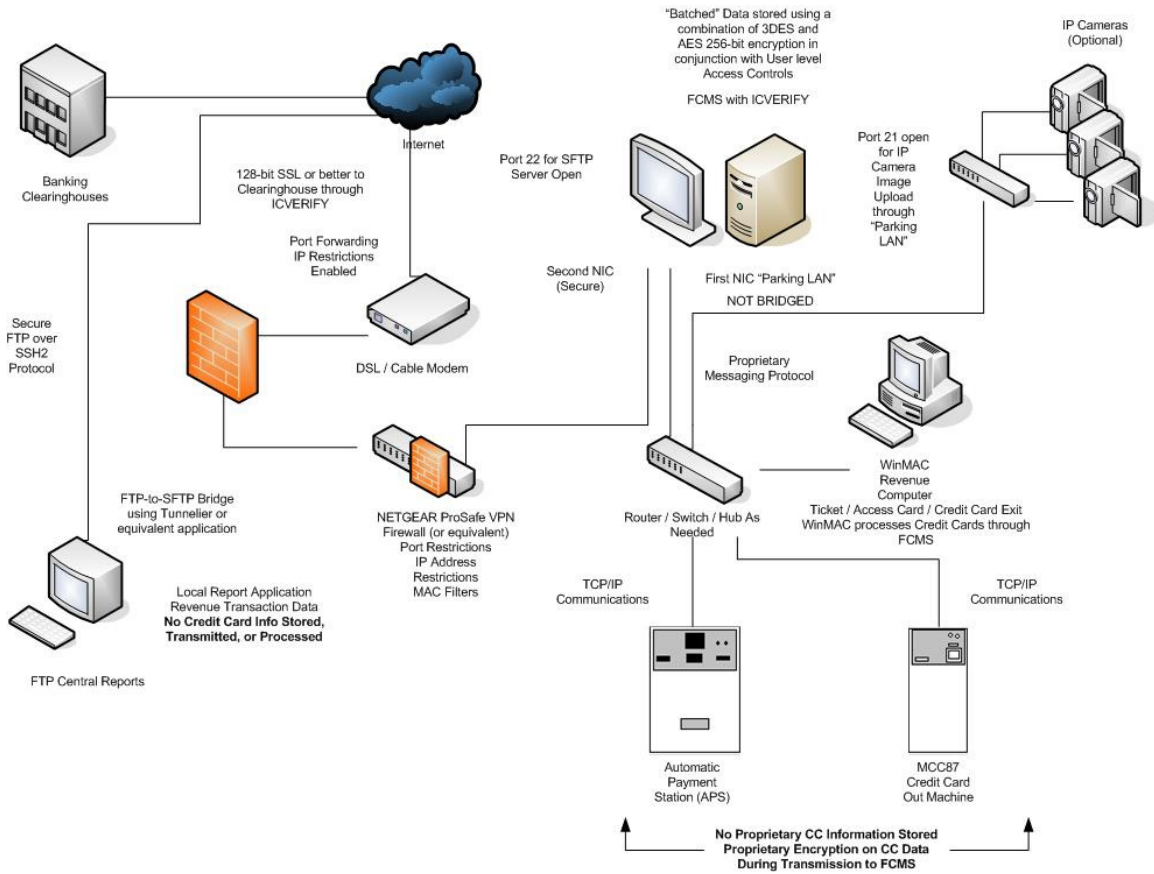
### 3.7 Tests for Application Vulnerabilities

*PABP Reference (7.1)*

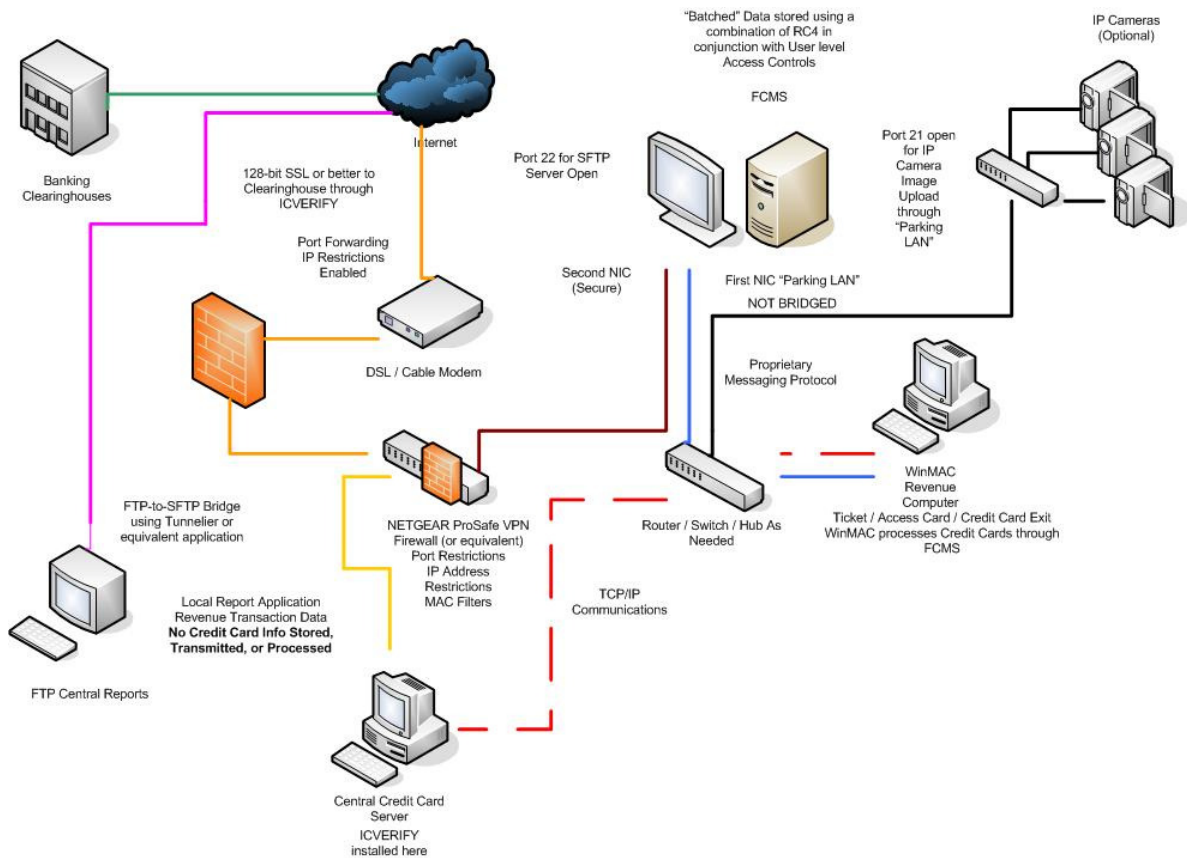
In addition to on-going internal testing, Magnetic Automation monitors outside security sources such as CERT and Microsoft Security Bulletins to check for product vulnerabilities. If vulnerability is found in any of the aforementioned products, merchants will be informed and a timely correction will be provided.

### 3.8 Facilitate Secure Network Implementation

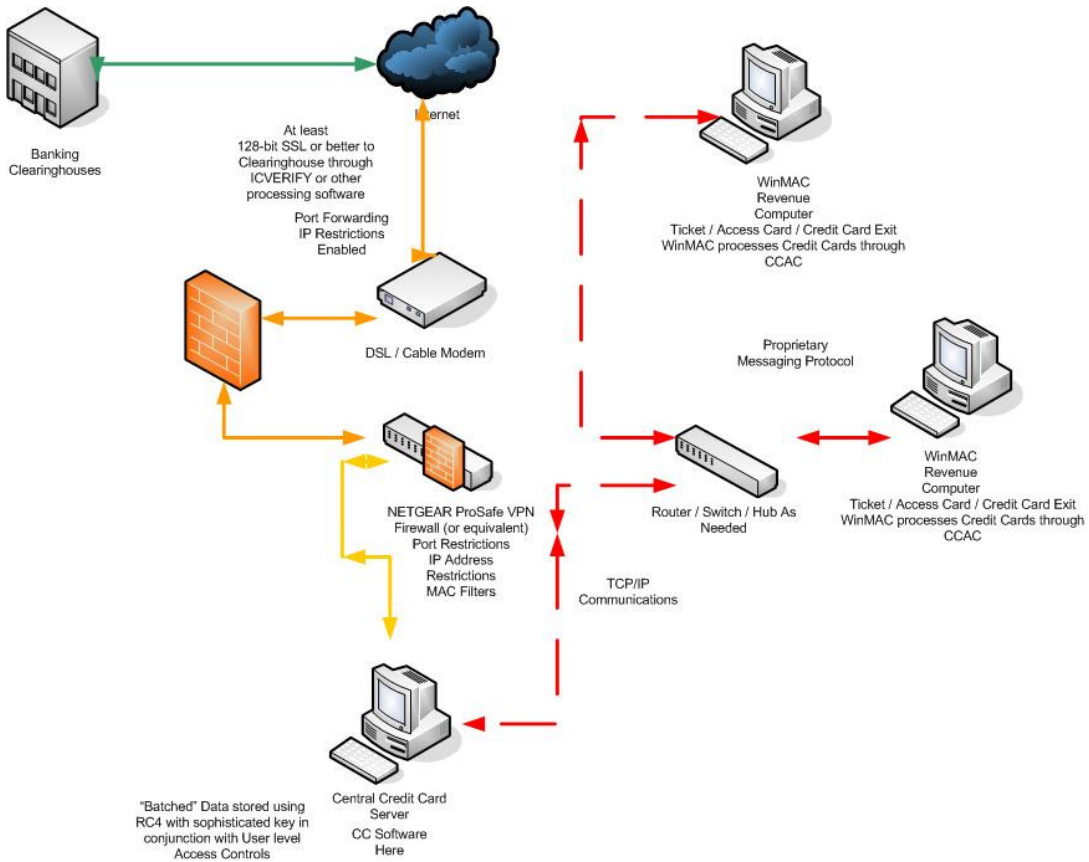
The following diagrams demonstrate how merchants can facilitate a secure network implementation when utilizing differing configurations:



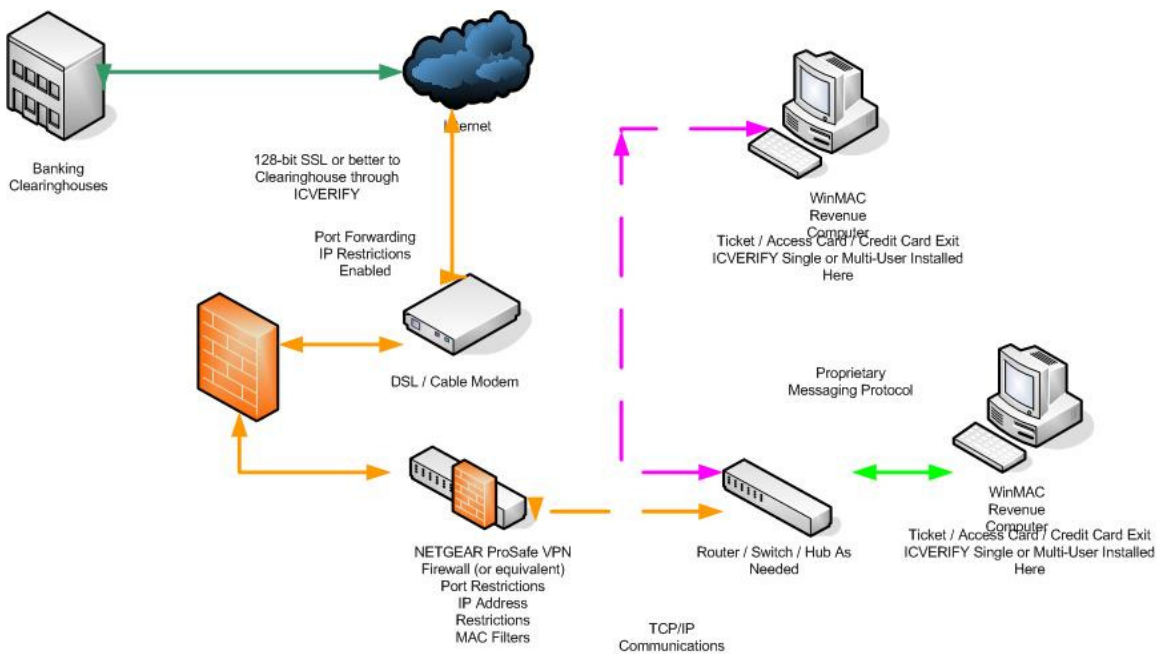
**Figure 5: Central Credit Card Processing Scenario through FCMS**



**Figure 6: Central Credit Card Processing Through Credit Card Server**



**Figure 7: Central Credit Processing Through Credit Card Center (No FCMS)  
All revenue data is retained on WinMAC PCs (No Centralized Management)  
Credit Card Data Stored on CCAC**



**Figure 8: WinMAC with ICVERIFY Single or Multi-User**

When the credit card information is transmitted from an exit station (WinMAC, PIL, APS, MCC87, MCC77), the PAN is encrypted using XOR encryption and is decrypted using the subsequent XOR encryption.

### 3.9 Cardholder Data Must Never Be Stored on a PC Directly Connected To the Internet

The aforementioned products are designed to run on a "Parking LAN" and not directly connected to the Internet. It is strongly recommended that the FCMS server and/or WinMAC (when used without FCMS for Central Credit Card processing) must not be directly connected to the Internet and should be segregated by using a VPN Firewall and/or Proxy Server to only accept connections from a restricted list of IP Addresses and/or Ports. WinMAC and FCMS run on the local, private network and not in either the DMZ or on a server directly connected to the Internet.

### 3.10 Facilitate Secure Remote Software Updates

*PABP Reference (10.1)*

Magnetic Automation does not facilitate the automatic download of updates. Updates are available on a CD from the Revenue Department by contacting (321) 635-8585. On occasion and by request only, updates may be sent via e-mail.

### 3.11 Facilitate Secure Remote Access to Application

*PABP Reference (11.1)*

Secure remote access to the FCMS server application and WinMAC / WinMAC-FCMS application is available by using an encrypted AES-256 bit VPN tunnel such as Hamachi. The only time secure remote access is used by the applications is by using the FTPCR (FTP Central Reports) application. While natively the FTPCR uses the insecure FTP protocol, it is tunneled over the Internet using AES 256-bit encryption used by Hamachi. Hamachi is a free program produced by LogMeIn and they also a premium product version. It is your responsibility to ensure the security of your connections.

### 3.12 Encrypt Sensitive Traffic over Public Networks

*PABP Reference (12.1, 12.2)*

The aforementioned applications are designed for installation on private/closed networks - not public networks. Therefore, sensitive traffic is not communicated over the public network. The WinMAC / WinMAC-FCMS and FCMS applications

do not send unencrypted PANs via email. WinMAC / WinMAC-FCMS and FCMS utilize ICVERIFY for processing credit card transactions. Please refer to ICVERIFY documentation on how the data is transmitted over the public Internet.

### 3.13 Encrypt All Non-Console Administrative Access

#### *PABP Reference 13.1*

WinMAC / WinMAC-FCMS, FCMS, APS-MBT100-\*\*\*, and MCC87 do not allow for remote Administrative Access. If Remote Desktop Support and Management take place over a public network or via telephone lines, a product that utilizes session encryption is recommended. Remote Desktop Tools that provide encryption options include:

- Symantec pcAnywhere v9.0 and higher. For configuration information, see:
  - *Appendix A: Security Features* in the v9.0 pcAnywhere User Guide
  - *Chapter 7: Securing Symantec pcAnywhere* in the v10.0 pcAnywhere User Guide
  - *Chapter 9: Securing your computer and sessions* in the v11.0 pcAnywhere User Guide
- Use of a Secure Web-based product like GoToMyPC.com. For security information, see the GoToMyPC Security White Paper located at [https://www.gotomypc.com/downloads/pdf/m/GoToMyPC\\_Personal\\_Security\\_White\\_Paper.pdf](https://www.gotomypc.com/downloads/pdf/m/GoToMyPC_Personal_Security_White_Paper.pdf)
- Citrix MetaFrame Secure Access Manager 2.0 – Not a Remote Desktop solution itself. Rather, it is a single portal which other Remote Desktop applications can be used for multiple sites, see <https://www.citrix.com/English/PS/products/product.asp?familyID=19&productID=184>

Regardless of the tool or encryption method, usernames, and complex passwords should be required for all remote access to the WinMAC or FCMS applications. Further, Remote Desktop Support and Management host software should only be run in cases when remote access is needed, if connectivity to the host software takes place over a public network or telephone line. An alternative, and recommended, approach when connecting via public network or telephone line is to use a two-factor authentication for user login to the remote access software at the site. An example of this would be the use of the Serial ID in versions of pcAnywhere v10.0 or later. A serial ID is required on both the host and client PCs for a remote session. This is in addition to the username and complex password.

There are other security mechanisms that are available with each Remote Desktop Support and Management tool. We can work with you to help you facilitate the best secure remote access plan that provides the right level of security.

## 3.14 Maintain Instructional Documentation for Customers and Integrators

This document serves as the ultimate source of documentation on secure implementation of Magnetic Automation hardware and software. All of the Magnetic Automation specifications are delivered to our integrators after signing a NDA.

## 3.16 PABP Operational Considerations

Once the entire system is "installed", please be sure you understand how various admin, login, and other actions are handled by WinMAC, FCMS, the CCAC, APS-MBT1000-\*\*\*, and MCC87. You will need to train yourself and customer service personnel on how to properly use the system. In some cases, with increased security comes slightly decreased "user friendliness". For instance, if you lose your password, we can recover it for you if you call us, but you may lose other user information in the process.

### **Admin Passwords (i.e. Supervisor)**

For admin users, unique & complex passwords must be required and enforced. Complex password is defined as 7 chars: uppercase + lowercase + number + symbol. The default setting is to just require strong passwords on the admin (supervisor) user in Windows.

### **Physical Key Control and Alarms**

It is important to ensure that all alarms are hooked up on the unmanned machines such as the MCC87, APS, and PIL, where applicable. The MCC87 uses a custom key available from Magnetic Automation. The APS/PIL uses a two lock system to prevent theft with five points so the data and your money stay secure. It is important to not disable the APS/PIL alarm because you would lose notification if the door was illegally opened and this could violate your PCI compliance. Ensure that you have a responsible individual who can manage key control to your hardware.

## 4. FTP Central Reports

### 4.1 Overview

FTP Central Reports is designed to run a customer provided PC running Windows 2000/NT/XP. The following lists FTP Central Reports functions:

1. Access up to 255 of Magnetic Automation products FCMS, FCMS-Lite, FCMS-Report, and WinMAC.
2. FTP username and password protection
3. Query daily transaction files, fee tables, validation accounts, and keycard account files manually.
4. Modify cashier passwords, supervisor passwords, fee tables, validation table, miscellaneous table, validation account, keycard account, keycard access group, keycard access level, and keycard billing group manually.
5. Update cashier passwords, supervisor passwords, fee tables, validation table, miscellaneous table, validation account, keycard account, keycard access group, keycard access level, and keycard billing group manually.
6. Allow selecting single source fee tables, validation accounts, and keycard account files to update multiple destination locations.
7. Provide reports
  - Single or multiple location revenue summary report by date range.
  - Shift transaction report, shift summary report, shift detailed report, cashier summary report, cashier revenue summary, cashier audit counts, cashier rates summary, and cashier credit card activity report.
  - Ticket entry transaction report, ticket exit transaction report, lane load report, lane activity report, lane volume report, ticket value report, duration and length of stay report, validation summary and detailed report, credit card summary and detailed report, miscellaneous summary and detailed report.
  - Keycard entry transaction report, keycard exit transaction report, lane load report, lane activity report, lane volume report, keycard activity report, duration and length of stay report, keycard group activity report, and keycard payment collection report.
  - System log report.
8. Application username and password protection.
9. Support user interface texts programmable.
10. Software License protected by dongle key.

#### **4.2 Setting up a Secure Connection between FTP Central Reports and FCMS Computers**

When using FTP Central Reports to connect to a FCMS computer which processes, stores, or transmits credit data, you must use a verified, secure connection and not an unencrypted transmission channel.

## 5. Hardening Your System

Hardening your system is very important and at a minimum the following guidelines must be followed in order to ensure there is the lowest possible attack footprint on the system. Hackers rely on poking at the weakest parts of the system and if you do not follow these guidelines, then you could be putting you and your customers at risk.

Every new PC hardware purchased as part of WinMAC or FCMS comes with an Antivirus Suite, out-of-box, in order to ensure that at a minimum your system is protected from viruses. Prior to shipping any new PC hardware, we run the Microsoft Baseline Security Analyzer (<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>) to check, repair, and scan any vulnerability known to the MBSA tool.

### 5.0 Software Install List

The following lists the software installed on the WinMAC Fee Computers as of May 1, 2008:

Name	Version	Description
ADAM 5000/6000 TCP	2.36.02	ADAM Module Utility for Gate Control
BDE	5.0	Borland Database Engine
Broadcom Advanced Control Suite	8.64.05	Integrated utility that provides useful information about the network adapter in your computer
FreshDiagnose	5.30	Tool for diagnosing and benchmarking computer
HASP Device Drivers	UNK	Software driver for hardware key
Intel® Graphics Media Accelerator Drivers	UNK	Software driver for graphics card
LogonStudio	UNK	Desktop Customization Tool
Microsoft Baseline Security Analyzer	2.1 BETA	Software scanning tool for vulnerabilities
Multi-Media Keyboard	UNK	Software driver for multimedia keyboard
Realtek AC'97 Audio	5.35	Software driver for multimedia audio
WinMAC / WinMAC-FCMS	8.0.2.6	WinMAC Fee Computer

The following lists the software installed on the FCMS computers as of May 1, 2008:

Name	Version	Description
BDE	5.0	Borland Database Engine

FCMS/Lite/Report	4.0.8.5	Facility Central Management System
MBSA	2.1 BETA	Microsoft Baseline Security Analyzer
Nport Administration Suite	1.8	Moxa TCP/IP RS232 Converter Config Tool
NVIDIA Drivers	UNK	Graphic Card Drivers
qCoscom	1.6	Tool for configuring MCC87 and APS
Sentinel Protection Installer	7.8.2	Software driver for hardware key

*Note: All PCs (WinMAC and FCMS) are shipped with Windows XP Pro SP2 and the latest windows updates, as of shipping, installed.*

The following lists the Windows XP Updates (at a minimum) installed on all PCs as of April 25, 2008. All PCs come loaded with Windows XP SP2 by default.

MS07-008	Installed	Security Update for Windows XP (KB928843)	Critical
MS05-018	Installed	Security Update for Windows XP (KB890859)	Important
MS07-067	Installed	Security Update for Windows XP (KB944653)	Important
MS06-030	Installed	Security Update for Windows XP (KB914389)	Important
MS06-041	Installed	Security Update for Windows XP (KB920683)	Critical
MS06-002	Installed	Security Update for Windows XP (KB908519)	Critical
MS08-008	Installed	Security Update for Windows XP (KB943055)	Critical
MS07-035	Installed	Security Update for Windows XP (KB935839)	Critical
MS06-069	Installed	Security Update for Flash Player (KB923789)	Critical
MS05-033	Installed	Security Update for Windows XP (KB896428)	Moderate
MS06-018	Installed	Security Update for Windows XP (KB913580)	Low
MS05-047	Installed	Security Update for Windows XP (KB905749)	Important
MS06-015	Installed	Security Update for Windows XP (KB908531)	Critical
MS06-009	Installed	Security Update for Windows XP (KB901190)	Important
MS07-050	Installed	Security Update for Internet Explorer 7 for Windows XP (KB938127)	
Critical			
MS08-020	Installed	Security Update for Windows XP (KB945553)	Important
MS08-002	Installed	Security Update for Windows XP (KB943485)	Important
MS07-031	Installed	Security Update for Windows XP (KB935840)	Critical
MS06-068	Installed	Security Update for Windows XP (KB920213)	Critical
MS05-049	Installed	Security Update for Windows XP (KB900725)	Important
890830	Installed	Windows Malicious Software Removal Tool - April 2008 (KB890830)	
MS08-021	Installed	Security Update for Windows XP (KB948590)	Critical
MS05-007	Installed	Security Update for Windows XP (KB888302)	Important
MS07-064	Installed	Security Update for Windows XP (KB941568)	Critical
MS06-075	Installed	Security Update for Windows XP (KB926255)	Important
MS07-013	Installed	Security Update for Windows XP (KB918118)	Important
MS05-037	Installed	Security Update for JView Profiler (KB903235)	Critical
MS07-056	Installed	Security Update for Outlook Express for Windows XP (KB941202)	
Critical			
MS06-057	Installed	Security Update for Windows XP (KB923191)	Critical
MS05-036	Installed	Security Update for Windows XP (KB901214)	Critical
MS07-020	Installed	Security Update for Windows XP (KB932168)	Critical
MS05-045	Installed	Security Update for Windows XP (KB905414)	Moderate
MS07-068	Installed	Security Update for Windows XP with Windows Media Format Runtime 9	
(KB941569)	Critical		
MS06-036	Installed	Security Update for Windows XP (KB914388)	Critical
MS06-052	Installed	Security Update for Windows XP (KB919007)	Important

MS07-021	Installed	Security Update for Windows XP (KB930178)	Critical
942763	Installed	Update for Windows XP (KB942763)	
MS07-011	Installed	Security Update for Windows XP (KB926436)	Important
MS05-032	Installed	Security Update for Windows XP (KB890046)	Moderate
MS05-051	Installed	Security Update for Windows XP (KB902400)	Important
MS06-022	Installed	Security Update for Windows XP (KB918439)	Critical
MS05-013	Installed	Security Update for Windows XP (KB891781)	Important
MS06-050	Installed	Security Update for Windows XP (KB920670)	Important
MS07-034	Installed	Cumulative Security Update for Outlook Express for Windows XP (KB929123)	Important
MS07-017	Installed	Security Update for Windows XP (KB925902)	Critical
MS06-006	Installed	Security Update for Windows Media Player Plug-in (KB911564)	Important
MS06-078	Installed	Security Update for Windows Media Player 6.4 (KB925398)	Critical
MS05-026	Installed	Security Update for Windows XP (KB896358)	Critical
MS08-024	Installed	Cumulative Security Update for Internet Explorer 7 for Windows XP (KB947864)	Critical
MS08-007	Installed	Security Update for Windows XP (KB946026)	Critical
MS05-009	Installed	Security Update for Windows Messenger (KB887472)	Moderate
MS08-025	Installed	Security Update for Windows XP (KB941693)	Important
MS08-001	Installed	Security Update for Windows XP (KB941644)	Critical
MS06-065	Installed	Security Update for Windows XP (KB924496)	Moderate
MS04-043	Installed	Security Update for Windows XP (KB873339)	Important
MS07-047	Installed	Security Update for Windows Media Player 9 (KB936782)	Important
MS07-019	Installed	Security Update for Windows XP (KB931261)	Critical
MS06-070	Installed	Security Update for Windows XP (KB924270)	Low
MS05-043	Installed	Security Update for Windows XP (KB896423)	Critical
MS07-012	Installed	Security Update for Windows XP (KB924667)	Important
MS06-014	Installed	Security Update for Windows XP (KB911562)	Critical
MS07-042	Installed	Security Update for Windows XP (KB936021)	Critical
MS06-025	Installed	Security Update for Windows XP (KB911280)	Important
MS06-066	Installed	Security Update for Windows XP (KB923980)	Important
MS05-040	Installed	Security Update for Windows XP (KB893756)	Important
MS06-053	Installed	Security Update for Windows XP (KB920685)	Moderate
MS07-058	Installed	Security Update for Windows XP (KB933729)	Important
MS05-041	Installed	Security Update for Windows XP (KB899591)	Moderate
MS05-048	Installed	Security Update for Windows XP (KB901017)	Important
MS06-008	Installed	Security Update for Windows XP (KB911927)	Important
MS07-004	Installed	Security Update for Windows XP (KB929969)	Critical
MS07-022	Installed	Security Update for Windows XP (KB931784)	Important
MS07-006	Installed	Security Update for Windows XP (KB928255)	Important
MS08-023	Installed	Security Update for ActiveX Killbits for Windows XP (KB948881)	Critical
MS07-065	Installed	Security Update for Windows XP (KB937894)	Moderate
MS06-063	Installed	Security Update for Windows XP (KB923414)	Important
MS04-041	Installed	Security Update for Windows XP (KB885836)	Important
MS04-044	Installed	Security Update for Windows XP (KB885835)	Important
MS06-064	Installed	Security Update for Windows XP (KB922819)	Low
MS07-061	Installed	Security Update for Windows XP (KB943460)	Critical
MS07-007	Installed	Security Update for Windows XP (KB927802)	Important
MS07-009	Installed	Security Update for Windows XP (KB927779)	Critical
MS05-042	Installed	Security Update for Windows XP (KB899587)	Moderate

## 5.1 Important Countermeasures

The following are some important countermeasures in order to reduce the attack surface of your WinMAC Fee Computer or FCMS.

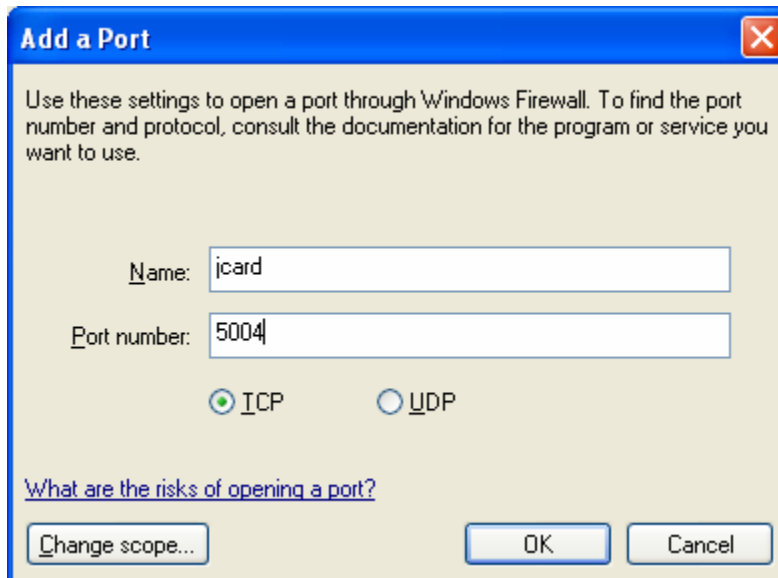
- Keep computers up-to-date on service packs and hotfixes with automated tools for testing and deployment
- Install and configure distributed firewall software or organizational IPsec policies
- Deploy and maintain antivirus software
- Deploy and maintain antispymware software
- Use an unprivileged account for day-to-day tasks. You should only use an account with administrator privileges to perform tasks that require elevated privileges.

## 5.2 Configuring Windows Firewall

At a bare minimum, you should run the Windows Firewall. However, you cannot expect it to work perfect “out-of-box” and exceptions need to be configured for FCMS, WinMAC, CCAC, or ICVERIFY. Other firewall solutions are available but it is impossible for this document to cover all of them.

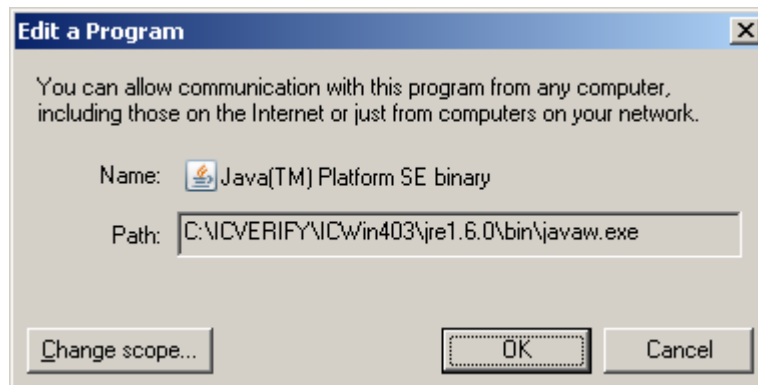
The exceptions configured for your firewall may depend on your clearinghouse. For example, TSYS has migrated from the WorldCom VirtualNet 1.0 gateway to the TNS VirtualNet 2.0 gateway. The new gateway uses TCP sockets to communicate rather than HTTPS connections. You may need to open a separate TCP route through your firewall to accommodate TSYS traffic. In the case of TSYS, they use port 5004 (as of writing).

In order to configure exceptions for ICVerify, you need to add an exception for **jcard**. The program **jcard** uses an internal port of 4445 and you do not need to open this port on your external firewall. However, you do need to add **jcard** to the list of exceptions accompanied with your Clearinghouse’s port number in order to properly process transactions. If you do not configure this correctly, you may have “timeout” transactions.

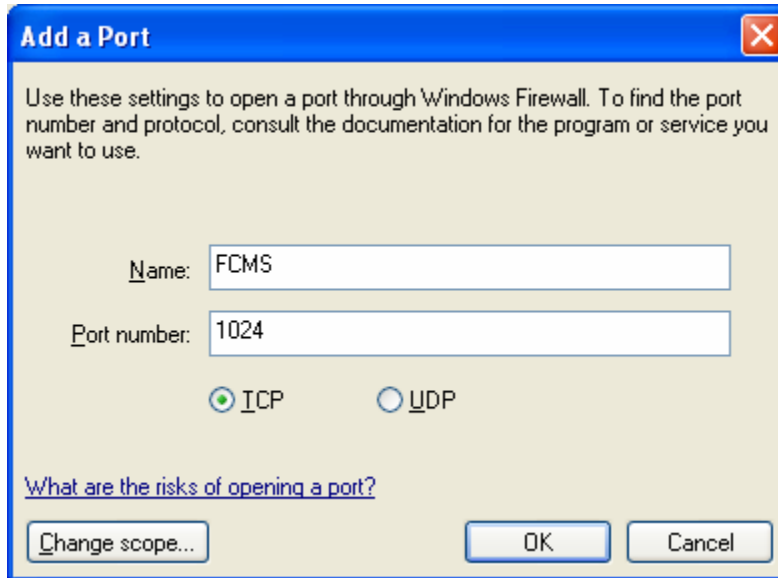


Add a Port to your Windows Firewall Exceptions (TSYS Example)

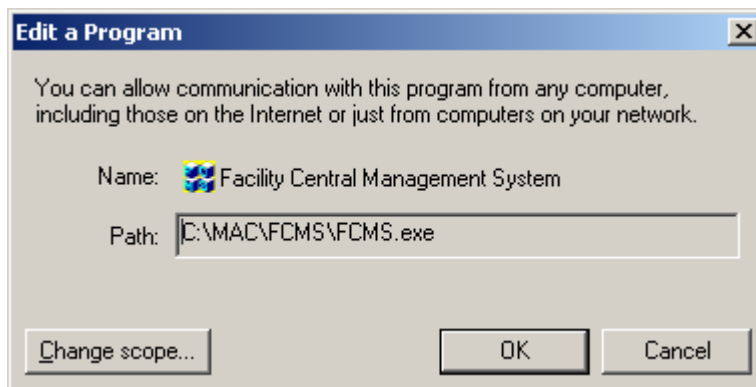
Additionally, you need to add the Java Sun Software to your exception list.



In order to configure FCMS and WinMAC for Windows Firewall, you need to add an exception for port 1024 to the local machine's exception list. Additionally, you need to add "Facility Central Management System" to the exception list for programs.



Add FCMS/WinMAC/CCAC to your Windows Firewall Exceptions



Add FCMS to the Windows Firewall Program Exception List

## 5. Resources on the World Wide Web

### 5.1 Card Association Links

Visa:

<http://www.visa.com/cisp>

Master Card:

<http://www.mastercard.com>

[http://www.mastercardmerchant.com/datasecurity/data\\_protection.html](http://www.mastercardmerchant.com/datasecurity/data_protection.html)

American Express:

[http://home.americanexpress.com/homepage/merchant\\_ne.shtml](http://home.americanexpress.com/homepage/merchant_ne.shtml)

### 5.2 Security Organizations

CERT: <http://www.cert.org>

Security Authorities: Bureau of Industry and Security:

<http://www.bis.doc.gov>

FBI CyberSecurity: <http://www.fbi.gov/cyberinvest/cyberhome.htm>

U.S. Secret Services: [http://www.secretservice.gov/financial\\_crimes.shtml](http://www.secretservice.gov/financial_crimes.shtml)

INTERPOL: <http://www.interpol.int/Public/TechnologyCrime/default.asp>

### 5.3 Associated Technologies

ICVERIFY:

<http://www.icverify.com>

Microsoft Windows XP Security Guide:

<http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx>

## 6. References

### 6.1 References

This document heavily references the Visa PABP and CISP websites located at [www.visa.com/cisp/](http://www.visa.com/cisp). In many instances, configuration notes and suggestions are derived from the most current Magnetic Automation manuals included on a CD with your product or from our websites.