PCI Guidance for Restaurant Manager

Versions 15.1- 18.0

Software, Installation, Server Network, Wireless, & Operations

Last Update: 12/13/2011

Contents

Notice 3

About this Document........ 3

Introduction 3

Difference between PCI Compliance and PA-DSS Validation 4

The 12 Requirements of the PCI DSS: 4

Restaurant Manager Application Settings 5

Log Files with Sensitive Data........ 5

Unencrypted Data 5

Credit Card Data Retrieval........ 6

Customer/Frequent Diner Credit Cards 7

Log Settings (PA-DSS 4.2.b) 7

Encryption 8

Removal of Cryptographic material (PA-DSS 2.7.a)........ 8

Passwords........ 9

Passwords 10

Master Password 10

Administrator Passwords 10

Sensitive Authentication Data Requires Special Handling (PA-DSS 1.1.5.c) 14

Beyond Restaurant Manager 15

Access Controls Outside RM........15

Log settings must be compliant (PA-DSS 4.2.b)........15

PCI Hardware Access (9.1) 16

PCI-Compliant Remote Access (11.2 and 11.3.b) 16

Remote Access (recommended by ASI) 17

Restricting inbound and outbound internet access 18
Server/Workstation Hardening Guidance 18
Cardholder Data via Email 18
PCI-Compliant Wireless settings (PA-DSS 6.1.b and 6.2.b) 19
Hardware 19
Wireless Configuration (PCI DSS Requirements 1.3.9, 2.1.1, 3.4, 4.1) 20
WPA 20
WPA-capable handheld hardware 20
Firewall Guidance (PCI DSS Requirement 1.3.9) 21
Write-On Configuration 22
Data Transport Encryption (PA-DSS 12.1.b) 22
Non-console administration (PA-DSS 13.1) 22
Internet Access (for OO, Write On Phone, and RM Browser) 22
DMZ Computer port forwarder setup 23
OO Server Setup 25
WO Phone Client Setup 27
RMBrowser Setup 28
Appendix: Notes 29
Additional Source Information 29
PCI Data Security Standard 8.5.8 through 8.5.15 General Guidelines 29
Revision History 30
10/27/10 Revision History 30
11/1/10 Revision History 30
12/7/10 Revision History 30
12/13/11 Revision History 30

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. ASI 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 ASI 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, ASI 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 RESTAURANT MANAGER 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).

ASI instructs and advises its customers to deploy ASI 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 RESTAURANT MANAGER installations will not be PA-DSS compliant.

Introduction

Restaurant Manager Version 18 is ASI's 4rd version PABP certified of RM for PCI compliant. It is important to note that installing RM Version 18 does not in itself make a restaurant PCI compliant. There are PCI requirements that extend beyond the RM software. Resellers need to take steps while configuring the server machine, network, and wireless infrastructure in order to adhere to PCI Guidelines. This document talks about areas inside RM that relate to PCI compliance, but also outlines those areas beyond RM that require attention from a PCI perspective. RM related topics include logging, data retention policies, encryption, passwords, and configuration settings.

Topics beyond RM itself involve system level configuration settings, some of which may require additional hardware, and others may require operational changes to store procedures. It is the job of the reseller to ensure the end user is fully aware of these requirements, and that failure to follow these recommendations will result in the store not being PCI Compliant, therefore compromising credit card data security.

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*

Restaurant Manager Application Settings

Log Files with Sensitive Data

Historical data must be securely deleted (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the software) – removal is absolutely necessary for PCI compliance and to satisfy the PA-DSS requirement 1.1.4.a (Remove Historical Sensitive Authentication Data –PA-DSS)

Unencrypted Data

Certain log files created in prior version up to version 15.1 may contained sensitive, unencrypted card data. These log files pose a serious security threat and are listed below:

- ERROR.TXT
- CCAUDIT.TXT
- RMCCAUDT.TXT
- CCSWIPE.TXT

To prevent a security breach after an upgrade, it is imperative that these log files be deleted from the main RM folder as well as any backup folders, drives, CD's, tapes, or any other backup media. These files should be deleted BEFORE upgrading to v18.

ASI provides a utility called CCPurge.EXE that erases these log files. In addition, CCPurge will erase any credit card information stored in database files PMT<mmyy>.DBF. CCPurge.EXE can be downloaded from ASI's web site, and should be executed in the main RM folder as well as any backup folders.

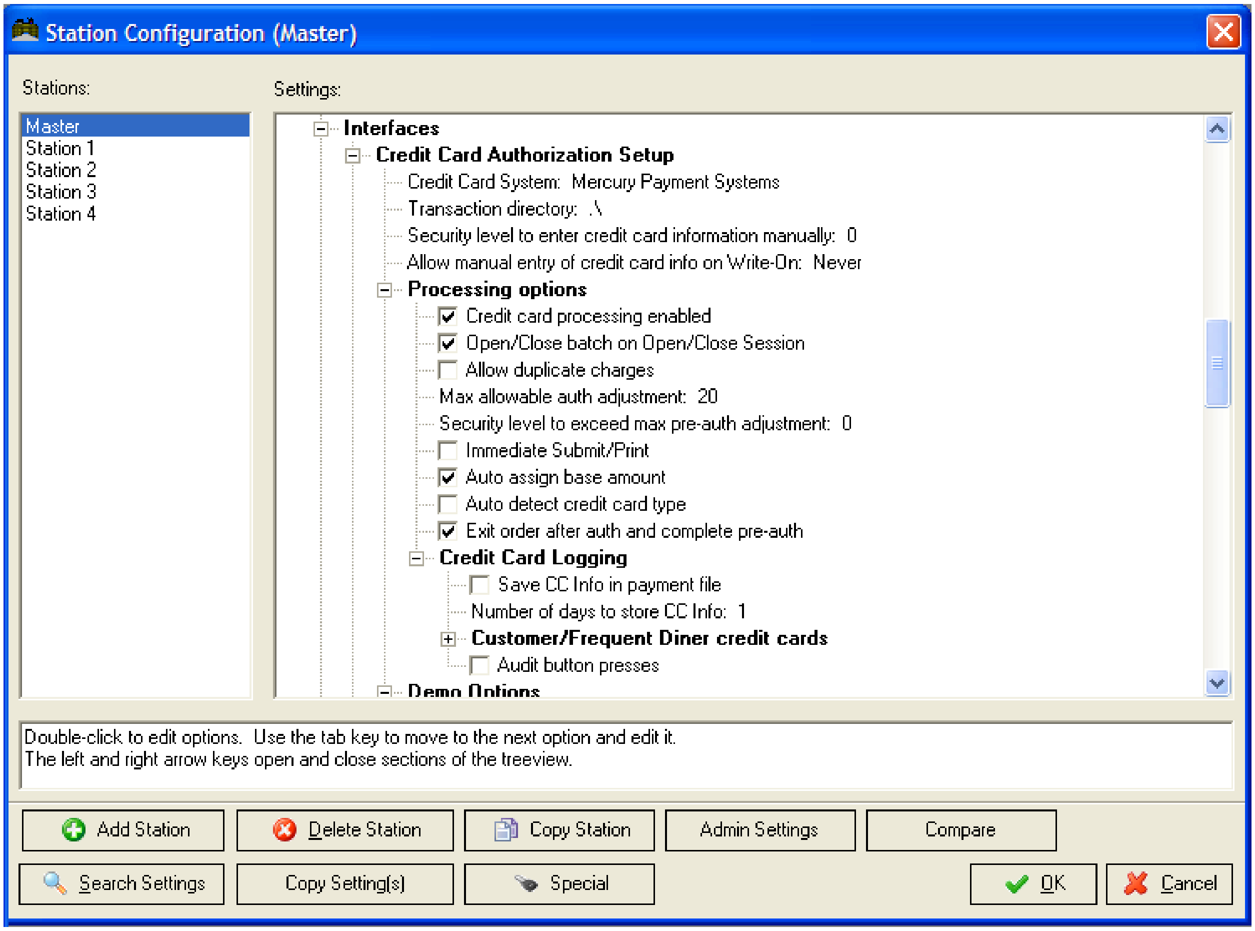
Note: after upgrading to RM version 18, the system will continue logging to the above mentioned files; however, all credit card information is masked and therefore does not pose a security risk. Hence, once a system is upgraded to v18, these files can be retained only in the live rmwin directory on the system without posing a security risk.

Credit Card Data Retrieval

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

Restaurant Manager provides several options for logging credit card information. The options are located in RM BackOffice >Setup >Station Configuration, Admin Settings (Admin Password) Miscellaneous > Credit Card Authorization Setup > Processing Options under "Credit Card Logging." Each option is described below.



```
⊟ Interfaces
   ⊟ Credit Card Authorization Setup
        Credit Card System:  Mercury Payment Systems
        Transaction directory:  .\
        Security level to enter credit card information manually:  0
        Allow manual entry of credit card info on Write-On:  Never
      ⊟ Processing options
           ☑ Credit card processing enabled
           ☑ Open/Close batch on Open/Close Session
           □ Allow duplicate charges
           Max allowable auth adjustment:  20
           Security level to exceed max pre-auth adjustment:  0
           □ Immediate Submit/Print
           ☑ Auto assign base amount
           □ Auto detect credit card type
           ☑ Exit order after auth and complete pre-auth
         ⊟ Credit Card Logging
              □ Save CC Info in payment file
              Number of days to store CC Info:  1
            ⊞ Customer/Frequent Diner credit cards
              □ Audit button presses
      ⊟ Demo Options
```

Double-click to edit options. Use the tab key to move to the next option and edit it.
The left and right arrow keys open and close sections of the treeview.

- ***Save CC Info in Payment File***

This option is provided to facilitate locating and/or fixing credit card issues arising during the course of business. For example, if a customer calls to dispute a charge. Card numbers are saved in the database PMT<mmyy>.DBF. The stored card numbers are masked to reduce the security threat, but it is still advisable to retain the card information for the minimum time necessary (i.e., for as long as there is a business need, but no longer).

- ***Number of days to store CC Info***

Use this option to limit the number of days Restaurant Manager will retain credit card information in PMT<mmyy>.DBF. Card information older than the number of days specified in this option, are purged at the beginning of each session (i.e. business day). Set this to a value that represents the business need to store this info, but no longer.

Customer/Frequent Diner Credit Cards

- ***Save/Restore customer/frequent diner credit card info***

This option can be used to save and restore credit card information for repeat customers. It is primarily useful in delivery-style operations where customers place their order by phone and give their credit card information verbally. If you choose to enable this option, you must decide how long you wish to retain unused card information. Refer to the next option.

- ***Number of days to keep unused card info***

This option defines how long the system will retain credit card information after a customer's last order. If a customer does not order again for the number of days specified, their credit information is automatically purged from the system.

The default setting is 90 days. Although you can enter a larger value, it is recommended that you set this option no bigger than 365 (1 year). Set this to a value that represents the business need to store this info, but no longer.

- ***Save/Restore Swiped Cards***

This option controls whether "swiped" credit cards are retained for future use. Note that PCI standards dictate that POS systems cannot store full credit card swipes or track 2 information for any reason what so ever. Therefore, only the card number and expiration are stored for future use. That means if the card is used in the future, it will be processed as a manually entered card, and hence will be subject to higher fees. If you expect the cardholder to present the card on future visits, it is preferable to set this option to "NO" and swipe the credit card on each future visit in order to obtain the best discount rate on future credit card transactions.

- ***Audit button presses***

This option logs button presses to the credit card audit file CCAUDIT.TXT. None of the information is sensitive therefore it does not compromise credit card security when this option is enabled; however, it can result in a LOT of stored data; therefore, this option should only be used when additional diagnostics are required for troubleshooting purposes.

Log Settings (PA-DSS 4.2.b)

Restaurant Manager 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 Restaurant Manager in any way will result in non-compliance with PCI DSS.

Credit card data retrieval is preformed at the POS using the [Retrieve Credit Card info] function within CC options and can only be used with an employee who has been assigned an administrator password. The use of this function is recorded in the file CARDVIEW.TXT located in the rmwin directory. This file is for auditing purposes only. The file shows the date, time, credit card type, and the last 4 digits of the card viewed and the employee number performing the operating.

Users can use PWLOG.dbf file as an additional method to track employees performing the credit card data retrieval at the POS. Restaurant Manager records every keystroke perform at the POS and records it in the PWLOG.dbf. The PWLOG.dbf can be viewed at the POS using the [View Button Log] function button on the Main Status POS screen of any module. This file does not contain any sensitive data but does show the employee number of the employee performing the keystrokes.

ENCRYPTION

In Restaurant Manager version 18, all sensitive information such as passwords and credit card data are encrypted using a Triple-DES encryption algorithm. Like any other encryption algorithm, Triple-DES uses an encryption key to encrypt and decrypt the data.

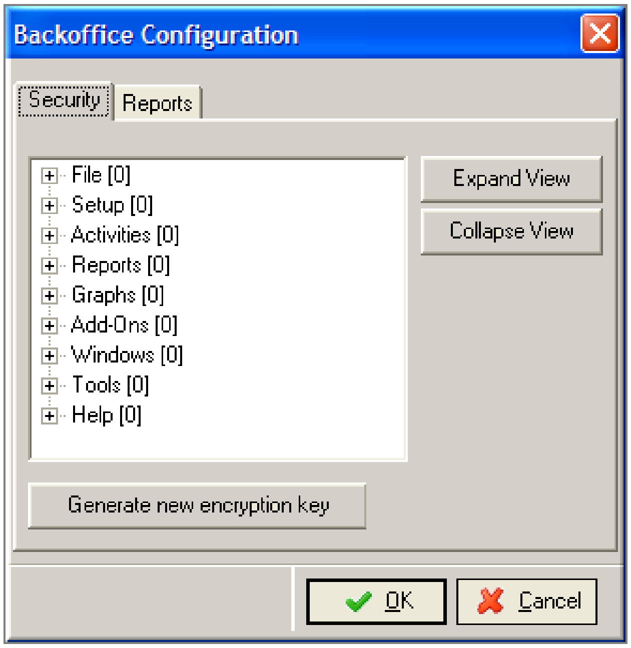
REMOVAL OF CRYPTOGRAPHIC MATERIAL (PA-DSS 2.7.A)

Restaurant Manager encrypts cardholder data on versions 15.1 to 18. The following must be done on these versions:

- All cryptographic material (encryption keys and encrypted cardholder data) must be securely removed.
- To securely remove this material you must run the ccPurge.exe. This is an automated process in Restaurant Manager when performing upgrades on RM versions prior to 15.1.
- This removal is absolutely necessary for PCI DSS Compliance
- Re-encrypt historic data with new keys by using the process of generating a new key described in this section.

In Restaurant Manager version 18, all sensitive information such as passwords and credit card data are encrypted using a Triple-DES encryption algorithm. Like any other encryption algorithm, Triple-DES uses an encryption key to encrypt and decrypt the data.

The encryption key is securely stored in the file KEY.DES, located in the RM working folder. It is important that this file not be deleted or tampered with as it will cause all encrypted data in the system to become un-readable. You should also make sure to include this file in any system backups. Restoring a backup without this file would cause passwords and stored credit cards to be un-readable. To ensure that credit card information is not compromised, ASI recommends changing the encryption key at least once per year. This is a simple process that must be done while the session is closed and takes no more than a few minutes. From the RM BackOffice go to Setup > Backoffice. Press the button “Generate new encryption key.” Under the Security tab. The system will automatically generate a random encryption key and update the necessary system and data files, re-encrypting all encrypted data with the new key



PASSWORDS

ASI Resellers, end users, and third party participants (i.e. outside network specialists) are advised to control access using unique usernames and PCI DSS compliant complex passwords, to any servers/computers, and databases with payment applications and cardholder data.

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. The following should be followed:

- Do not use administrative accounts for application logins (PA-DDS 3.1c).
- Assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts (PA-DDS 3.1c).
- Assign strong application and system passwords whenever possible (PA-DDS 3.1c).
- Create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15 (PA-DDS 3.1c).
- Changing the "out of the box" settings for unique user IDs and secure authentication will result in non-compliance with the PCI DSS (PA-DDS 3.2c).

The PCI standard requires the following password complexity for compliance (often referred to as using "strong passwords"):

- Do not use group, shared, or generic user accounts (PCI DSS 8.5.8)
- Passwords must be changed at least every 90 days (PCI DSS 8.5.9)
- Passwords must be at least 7 characters (PCI DSS 8.5.10)
- Passwords must include both numeric and alphabetic characters (PCI DSS 8.5.11)
- New passwords cannot be the same as the last 4 passwords (PCI DSS 8.5.12)

PCI user account requirements beyond uniqueness and password complexity are listed below:

- If an incorrect password is provided 6 times the account should be locked out (PCI DSS 8.5.13)
- Account lock out duration should be at least 30 min. (or until an administrator resets it) (PCI DSS 8.5.14)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session (PCI DSS 8.5.15)

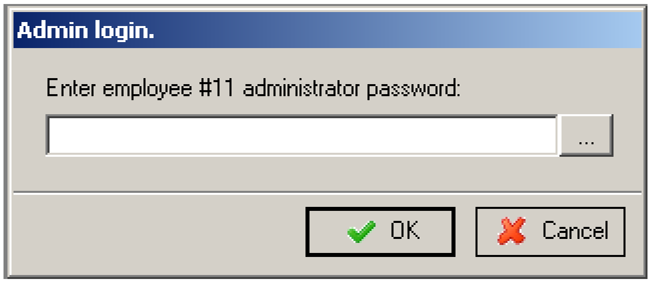
The following sections outline how you can configure RM to meet PCI DSS requirements

PASSWORDS

All passwords in version 18 are encrypted. In previous versions, it was possible to use DBU, or other database utility to view passwords stored in Employee.dbf and Config.dbf, these passwords are now encrypted. If DBU (or other utility) is used to change any of the passwords stored in these files, those passwords will be rendered unusable until they are reset.

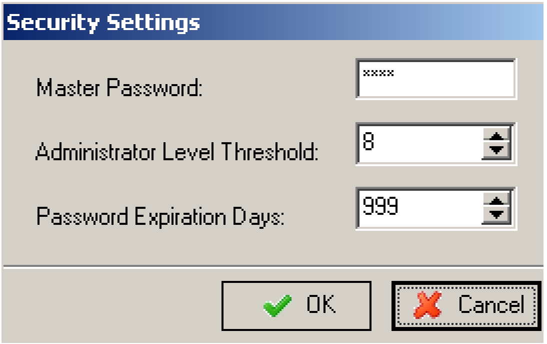
MASTER PASSWORD

The "Master Password" in Restaurant Manager allows access to all back office as well as Point of Sale functions. It is highly recommended that the master password not be used (PA-DDS 3.1c & PCI DSS 8.5.8). By default, the Master password on a new system is 0000. When setting up a new system, you should change the Master password to something other than the default value. It is also recommended that you change the master password at least every 90 days.



Admin login.

Enter employee #11 administrator password:



Security Settings

Master Password: ****

Administrator Level Threshold: 8

Password Expiration Days: 999

Because the master password is encrypted, the program PASS0000.EXE, must not be used as in previous versions. After upgrading from a version pre v15.1 and if the executable remains: it should be removed from the system. If you do execute PASS0000.EXE, or otherwise manually change or corrupt the master password on the system, it will render the master password unusable. (PA-DDS 3.2c). If this happens, you will only be able to reset the master password with assistance from ASI Tech Support. Open a help desk ticket with the subject, "Reset v18 master password".

ADMINISTRATOR PASSWORDS

Version 18 relies on the concept of Administrators. They have access to settings and operations normal users do not. Those items include:

1. Set or Change master password, located in Setup -> Security Configuration screen. User must also be a level 9.

2. Set or Change other employee’s administrator password, accessible using “Edit Administrator Password Info” button in Employee Setup. User must also be equal or higher security level than the one being changed.
3. Modify PCI Security Configuration settings, in new Setup -> Security Configuration. User must also be a level 9.
4. Access the Backoffice Configuration screen.
5. Access sensitive credit card configuration settings in RMCCWIN.
6. Add or Delete employees from the database.

Choosing these options in the RM BackOffice or RMCCWIN will cause an admin password prompt to appear, or a notice that the user does not have adequate permission.

Admin passwords are set in the RM BackOffice under Employee Setup, click on Edit Administrator Password Info”.

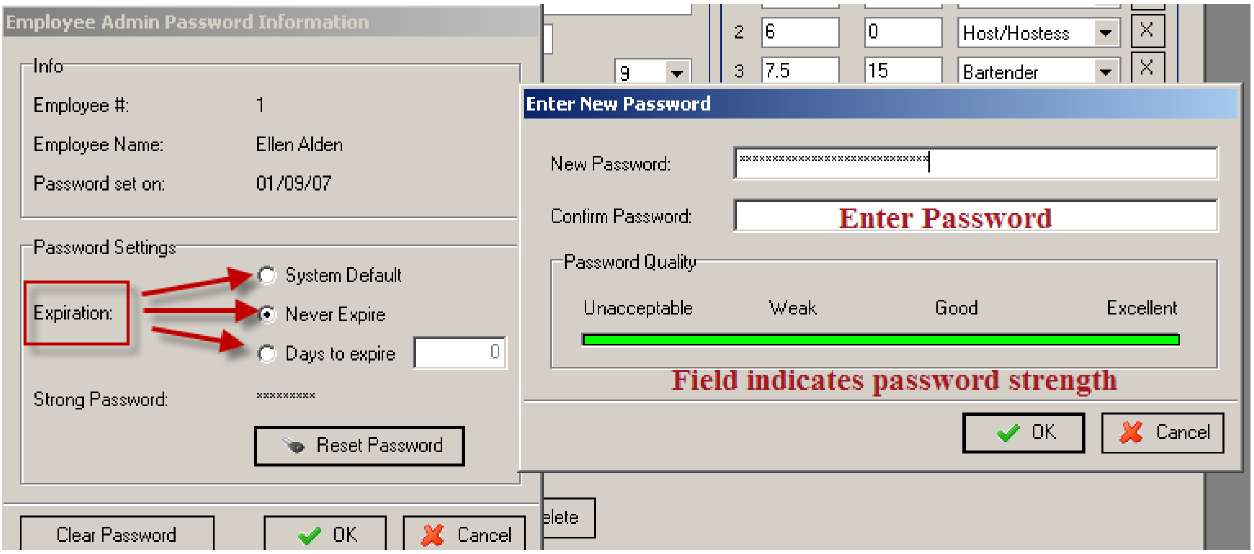
NOTE: It is always the admin password of the LOGGED-IN user that is required. This can be confusing when an admin is trying to change the admin password of another admin. It is their own password that should be entered, not the one of the employee he is editing.

NOTE: You are allowed only six attempts to enter an administrator password. Failures to enter the correct administrator password will block additional attempts for thirty minutes (PCI DSS 8.5.13 & PCI DSS 8.5.14)

- ***ADMIN PASSWORDS ARE “STRONG” PASSWORDS***

A “strong” password is an industry term to denote that the password is complex enough to reduce the chances of it being guessed using brute force methods. The rules for strong passwords are:

1. MUST be 7 characters or longer (PCI DSS 8.5.10)
2. MUST contain both letters and numbers (PCI DSS 8.5.11)
3. Should contain both upper and lower case letters
4. Should contain symbols (e.g. characters above numbers on keyboard)
5. Password should not be similar or contain the same numbers found in the employee password.


Employee Admin Password Information

Info

Employee #: 1

Employee Name: Ellen Alden

Password set on: 01/09/07

Password Settings

Expiration: ○ System Default ● Never Expire ○ Days to expire 0

Strong Password: *********

Enter New Password

New Password: ******************************

Confirm Password: Enter Password

Password Quality

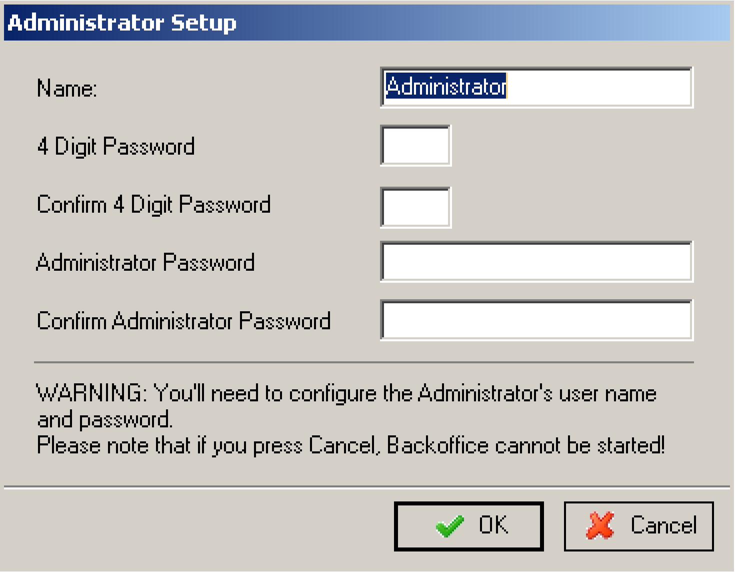
Unacceptable Weak Good Excellent

Field indicates password strength

The last 2 are not required, but add additional password security, and make an admin password quality “excellent”.

- ### *Creating the first Administrator Account*

After installing Restaurant Manager, start RM BackOffice (rmwin.exe) and you will be immediately prompted to create the first admin account, a level 9 user with access to all PCI-sensitive settings in the system. ASI recommends this account be a user tied to the reseller. It is from this user account that the reseller can continue configuring the credit card settings, and creating additional admin passwords for store personnel.


Administrator Setup

Name: Administrator

4 Digit Password

Confirm 4 Digit Password

Administrator Password

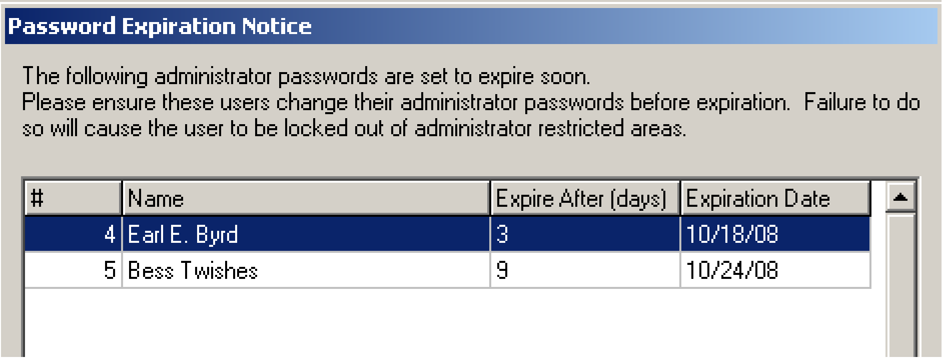
Confirm Administrator Password

WARNING: You'll need to configure the Administrator's user name and password.
Please note that if you press Cancel, Backoffice cannot be started!

Resellers may wish to restrict the level 9 security level for reseller use, and have store personnel be level 8 and below. Admins, by default, are defined as level 8 and above, configurable from within RM BackOffice.

- ***ADMIN PASSWORD EXPIRATION***

Admin passwords expire in 90 days by default. After expiration, the user can no longer gain access to the admin restricted areas of RM. That user needs to have his password reset to regain admin access.



Password Expiration Notice

The following administrator passwords are set to expire soon.
Please ensure these users change their administrator passwords before expiration. Failure to do so will cause the user to be locked out of administrator restricted areas.

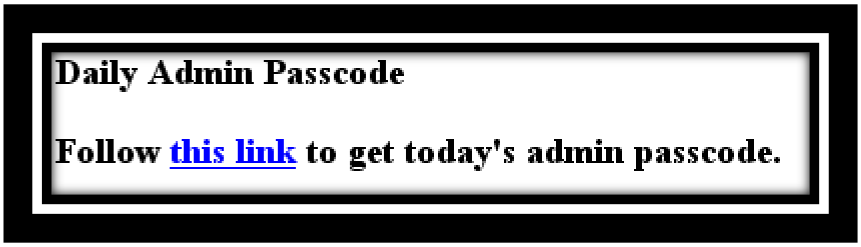
#	Name	Expire After (days)	Expiration Date
4	Earl E. Byrd	3	10/18/08
5	Bess Twishes	9	10/24/08

EXPIRATION WARNING: The RM BackOffice program will warn of impending admin password expirations upon Backoffice login. If any admin passwords will expire within the next 10 days, or have already expired, an expiration dialog will appear listing the employees affected.

- ***RESETTING ADMIN PASSWORDS***

If admin passwords are forgotten, or left to expire, they will need to be reset. That can be done through the following means:

1. **By a fellow admin**- Another admin at equal or higher security level who does still have access can change the password of the user whose admin password is unusable.
2. **By the reseller** – If all store admins have forgotten their password or let them expire, then the reseller's own admin user can be used to reset the admin password of the highest security level store employee to allow them to regain admin access.
3. **By calling ASI** – If all admin users have lost access, the only way to regain access is to call ASI Tech Support and get the RM Admin Daily Passcode and follow the instructions given by the ASI technician
4. **Accessing the ASI web site**- go to the Reseller page then Tech Support > Patches & Utilities > Daily Admin Password. Here you will find a link to get today's daily passcode. In the entry fields, you will need to enter your name and the site's name. The user is transported to a page with today's Admin Passcode.



Daily Admin Passcode

Follow this link to get today's admin passcode.

After retrieving the Daily Passcode:

- Re-start Rmwin and enter in the code into the password field when prompted.
- Go to "**Employee- Setup**", select the employee, and click on the **[Edit Administrator Password Info]** button to change the admin passcode.

Password fields left inactive for a period of 15 minutes will automatically time out. You will have to begin the process again if you exceed the time frame of inactivity (PCI DSS 8.5.15).

NOTE: New passwords cannot be the same as the last 4 passwords (PCI DSS 8.5.12).

- ***PCI COMPLIANT SETTINGS***

To be PCI compliant:

1. The default Password Expiration Days ***MUST*** be set to 90 or lower. 90 days is the default setting (PCI DSS 8.5.9).
2. All administrators MUST have their Expiration setting set to "System Default". This is the default setting.

Note that RM allows expiration settings other than what PCI requires. This is to accommodate sites that are not required to be PCI compliant (e.g. sites that do not accept credit cards). It is the responsibility of resellers, and ultimately store management to ensure that the store uses PCI compliant settings if required.

SENSITIVE AUTHENTICATION DATA REQUIRES SPECIAL HANDLING (PA-DSS 1.1.5.C)

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

These guidelines must be followed for all software used for processing credit cards

Note: For PCI compliance, any cards that were viewed at the POS using the [Retrieve Credit Card info] function within CC options are logged in the file CARDVIEW.TXT. This file is for auditing purposes only and shows the date, time, employee #, credit card type, and the last 4 digits of the card viewed.

Beyond Restaurant Manager

ACCESS CONTROLS OUTSIDE RM

ASI Resellers, end users, and third party participants (i.e. outside network specialists) are advised to control access using unique usernames and PCI DSS compliant complex passwords, to any servers/computers, and databases with payment applications and cardholder data.

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. The following should be followed:

- Do not use administrative accounts for application logins (PA-DDS 3.1c).
- Assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts (PA-DDS 3.1c).
- Assign strong application and system passwords whenever possible (PA-DDS 3.1c).
- Create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15 (PA-DDS 3.1c).
- Changing the "out of the box" settings for unique user IDs and secure authentication will result in non-compliance with the PCI DSS (PA-DDS 3.2c).

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.]

LOG SETTINGS MUST BE COMPLIANT (PA-DSS 4.2.B)

If allowed, any third party software used for remote access or credit card processing must have logging turned on and configured per PCI DSS 10.2 and 10.3 as follows:

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 all assessment trails
10.2.4 Invalid logical access attempts
10.2 5 Use of identification and authentication mechanisms
10.2.6 Initialization of the assessment logs
10.2.7 Creation and deletion of system-level objects.

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

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.

Disabling or subverting the logging function of Restaurant Manager in any way will result in non-compliance with PCI DSS.

PCI Hardware Access (9.1)

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder environment. Guidance- Without physical access controls, unauthorized persons could potentially gain access to the building and to sensitive information, and could alter system configurations, introduce vulnerabilities into the network, or destroy or steal equipment.

PCI-Compliant Remote Access (11.2 and 11.3.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 Logmein Central 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). *Please note that ASI is recommending that Symantec pcAnywhere, Tight VNC, or Remote Desktop or similar products not be used to access accounts*. However, if you choose to use one of these methods of remote access you should implement the following:

- Remote Desktop Top (RDP/Terminal Services)- use the high encryption setting on the server
- PCAnywhere/Tight VNC (or similar) – use 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 PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to 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 PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

REMOTE ACCESS (RECOMMENDED BY ASI)

The nature of our business requires remote access to a store network and server machine for support purposes. Such remote access is allowed, but only if proper protection and security methodologies are employed. Those methodologies include two-factor authentication and time-restricted access.

Below are two possible methods ASI offers for solutions regarding two factor authentication satisfaction:

- **LOGMEIN CENTRAL (PREFERRED)**

(PCI DSS Requirement 8.3) Access authentication shall employee two factors of protection. The built-in protection of the access software (such as LogMeIn Free, Pro, etc) which employs a unique username and complex password can be one factor of protection. But a second factor of protection shall also be used. ASI recommends using LogMeIn Central with individual security tokens (e.g. emailed passwords) or cell phone notifications to satisfy two factor authentications. LogMeIn Central provides preference settings under the Security tab where you define the authentication parameters for every time a client site is accessed for each user account.

In addition, you will need to configure the following in LogMeIn Central to satisfy PCI DSS criteria:

1. Unique user accounts. Users cannot share remote access credentials.
2. Accounts of terminated employees are immediately disabled.
3. Strong passwords at least 7 characters long with letters and numbers as minimum complexity.
4. Remote access passwords must be changed every 90 days.
5. Automatic idle disconnect after 15 min of inactivity.
6. Logs are retained for at least one year, showing who remote controlled into what computer at what time and from what IP the connection originated.
7. Six incorrect login attempts on a user account locks out that account for a minimum of 30 minutes in order to slow down brute-force guessing.
8. Remote access logs need to be reviewed regularly for abuse.

- ***VPN WITH LOGMEIN***

  (PCI DSS Requirement 8.3) Access authentication shall employee two factors of protection. The built-in protection of the access software (such as LogMeIn) which employs a unique username and complex password can be one factor of protection. But a second factor of protection shall also be used. In this method, ASI suggests using VPN with individual security tokens (e.g., Secure ID's, certificates, or public keys). Therefore, access to a store would first require establishing a VPN connection, and then starting up a secure remote access connection (i.e. LogMeIn or similar) through the VPN.

  i. ***VPN – access*** shall only be granted to users or vendors with business justification through a formal access granting process that is documented and tracked. In addition to the unique (to the user) username and complex password required to access servers within the payment processing environment, VPN users will need to have individually assigned access tokens.

  ii. ***LogMeIn or other access software*** (PCI DSS) – Access accounts shall be set up for every user (person) with access rights to the store.

Any "always-on" connections from a computer to a VPN should be secured by using a personal firewall (PCI DSS 1.3.9). The firewall should be configured to meet specific standards and not be alterable by employees.

- ***ACCESS ENABLED ONLY DURING UPDATE TIME PERIOD***

(PCI DSS Requirement 8.5.6) Vendor access accounts shall be disabled except during the time period when access is required. Prior to the necessity for access, an onsite trusted individual will enable access for the person requesting access. Following the access session, all access accounts will then be disabled.

RESTRICTING INBOUND AND OUTBOUND INTERNET ACCESS (PCI DSS Requirement 1)

The RM server machine shall have restricted inbound and outbound internet access though use of firewall services between the server machine and the internet. Access shall be limited to those needed by RM and related applications, such as credit card authorization, automatic anti-virus updates, and network time synchronization as examples.

The server machine shall be used solely as a server and not for other user functions, especially internet activities such as email or web browsing. Those should be done from a separate machine on a separate subnet with isolated access to the internet.

SERVER/WORKSTATION HARDENING GUIDANCE (PCI DSS Requirements 2.2, 6.1, 6.2)

Unnecessary and insecure services and protocols shall be removed or not installed on the server machine. This includes such services as NetBIOS, file-sharing, Telnet, unencrypted FTP, and others.

CARDHOLDER DATA VIA EMAIL (PCI DSS Requirement 4.2)

RM does not implement any mechanism for emailing of cardholder data. Reseller shall instruct end users not to email any cardholder data as part of doing business with their customers.

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

Restaurant Manager does *offer* wireless technologies with the WriteOn products. 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:

However, in sites not using WriteOn technology, a merchant may implement wireless access within the cardholder data environment. If such is the case, 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:

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.

2.1.1:

- All wireless networks implement strong encryption (e.g. AES)
- Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions
- Default SNMP community strings on wireless devices were changed
- Default passwords/passphrases on access points were changed
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)
- Other security-related wireless vendor defaults, if applicable

4.1.1:

- Industry best practices are used to implement strong encryption for the following over the wireless network in the cardholder data environment (4.1.1):
  - Transmission of cardholder data
  - Transmission of authentication data
- Payment applications using wireless technology must facilitate the following regarding use of WEP:
  - For new wireless implementations, it is prohibited to implement WEP as of March 31, 2009.
  - For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

Hardware

- **Required Specs**
  - 802.11n
  - WPA2 encryption (as opposed to just WPA)
- **Suggested Specs-** Gigabit port with gigabit networking to the server
- **Recommended Hardware-**
  - Basic Models
    - Netgear WN802T (access point, to connect to existing router)
    - Netgear WNDR3700 (router/access point combo)
  - Pro Model for Larger Sites-

- Netgear WNDAP350 (access point, plenum rated, 802.3af PoE support for remote placement and remote management). Use with one of the following:
  - Netgear WMS5316 Wireless Management System (for up to 16 access points, centrally managed)
  - Netgear WNDAP330 is non-plenum rated alternative

WIRELESS CONFIGURATION (PCI DSS REQUIREMENTS 1.3.9, 2.1.1, 3.4, 4.1)

Wi-Fi Configuration Guidance (PCI DSS Requirements 2.1.1 & 4.1) PCI requirements for wireless networks are extensive. All the following services and settings are required. Note that some of the requirements are hardware dependent. It is possible that new or different hardware will be required in order to satisfy PCI requirements. The Netgear access points/routers mention in the hardware section points are PCI-capable. The Netgear ME103, widely used for new Write-On installations in 2003-2004, is not.

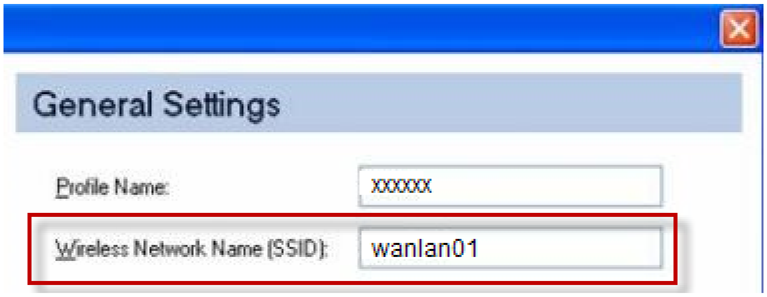
WPA

The wireless infrastructure must use WPA2 encryption. WEP encryption is no longer allowed Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks. Therefore WPA2-capable wireless infrastructure (access point) is a requirement. On most Netgear products, you will find the encryption options under the Security Settings of your wireless network. Settings on various models will vary. On some models you want to select the “WPA/WPA2-TKIP” option, on other models you will have to select WPA2 as Network Authentication and the select TKIP as Data Encryption type.

WPA-CAPABLE HANDHELD HARDWARE

All handheld hardware must be WPA-enabled if any mobile MSRs are in use in the installation. Since the ASI custom driver for the Socket wireless card does not support WPA, no consumer handhelds with the Socket card can be used in an installation that is also using MSR-capable handhelds such as the iPod Touch with MSR attachment. If you add an Ipod Touch with MSR to an existing installation, the entire site must be converted to WPA-capable handhelds in order to satisfy PCI compliance requirements.

1. ***Non-Default SSID* –** The ESSID of the wireless network must be changed from the default setting from the manufacturer. On most Netgear product the ESSID setting is on the Wireless Settings page for the wireless network. Change it to something that’s unique for each installation.

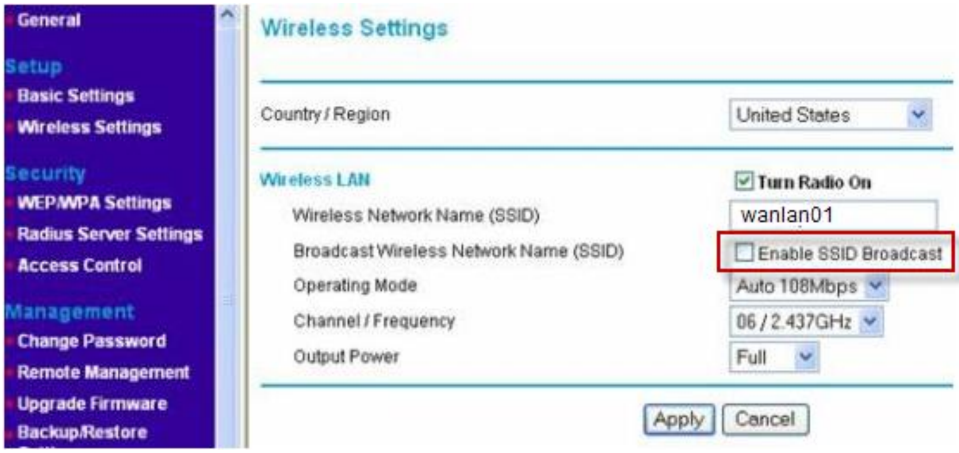


General Settings

Profile Name: xxxxxx

Wireless Network Name (SSID): wanlan01

2. ***Disable SSID Broadcast-*** The broadcast of the ESSID in the beacon must be disabled. On Netgear products, uncheck Broadcast Wireless Network Name (SSID) typically found in the main configuration page for the wireless network,



Wireless Settings

Country / Region: United States

Wireless LAN: ☑ Turn Radio On

Wireless Network Name (SSID): wanlan01

Broadcast Wireless Network Name (SSID): □ Enable SSID Broadcast

Operating Mode: Auto 108Mbps

Channel / Frequency: 06 / 2.437GHz

Output Power: Full

3. ***MAC address filtering –*** MAC address filtering must be used on the wireless network to disallow all clients except those specifically listed as trusted handheld client hardware.
   - **Net Gear WN802T (AP)**- under Security on the main menu, select Access Control**.** The Access Control menu will display. . Enable the “Turn Access Control On” option. Add entries listing the MAC address of each handheld hardware unit in use at the store. Do not forget to delete entries of units removed from service at the store.
   - **Net Gear WNDR3700 (Router/AP)**- From the main menu, select Wireless Settings and then click Setup Access List to display the Wireless Card Access List screen. Enable the “Turn Access Control On” option. Add entries listing the MAC address of each handheld hardware unit in use at the store. Do not forget to delete entries of units removed from service at the store.
   - **Net GearWNDAP350 (AP)-** Under the Configuration tab, select Security on the main menu, select Advanced from the left panel, and then select MAC Authentication. The MAC Authentication screen displays. Enable the “Turn Access Control On” option. Add entries listing the MAC address of each handheld hardware unit in use at the store. Do not forget to delete entries of units removed from service at the store.

Firewall Guidance (PCI DSS Requirement 1.3.9)

Firewall services must be installed to limit and protect access to the server machine from any wireless network that would otherwise have free access to the store’s wired network.

- ### *Hardware*

The Net Gear WNDRP3700 can serve this purpose, if properly configured. By default the SPI is enabled and must remain this way. If not using the Net Gear WNDRP3700, then an additional firewall box must be purchased and installed. It must include Stateful Packet Inspection (SPI).

- **LOCATION**

The firewall shall be placed between the wireless network and the physical network to which the server machine is connected. The goal is to prevent any unnecessary network traffic on the wireless network from gaining access to the wired network. Only necessary packets are allowed, using only necessary ports.

- **SETTINGS- PORT/SERVICE RESTRICTION**

The Write-On handheld and Write-On Server process communicates through IP. The protocols it uses are HTTP (TCP port 9644). Therefore, only 9644 shall be allowed through the firewall. All others shall be disallowed. On the WNDR3700 unit this is accomplished by selecting Port Forwarding/Port Triggering under Advanced in the main menu.

WRITE-ON CONFIGURATION

ACCESS TO HANDHELD SERVER FROM INTERNET (PCI DSS Requirement 2.4)
The Write-On Server application shall not be accessible from the internet. Access shall be limited only to the local network (subnet).

NO ACCESS ALLOWED (PORT 80 CLOSED, AND NO ALTERNATE PORT USED) –Port 80 on the server shall not be accessible from the internet. Furthermore, no open port from the internet shall map to the Write-On Server's port 80.

DATA TRANSPORT ENCRYPTION (PA-DSS 12.1.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.

In Restaurant Manager version 18, all sensitive information such as passwords and credit card data are encrypted using a Triple-DES encryption algorithm.

NON-CONSOLE ADMINISTRATION (PA-DSS 13.1)

Although Restaurant Manager does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, must use SSH, VPN, or SSL/TLS for encryption of this non-console administrative access.

INTERNET ACCESS (FOR OO, WRITE ON PHONE, AND RM BROWSER)

For PCI compliance, any incoming connections must pass through a machine between your RM Server and Firewall. This machine will be located in a separate sub network called the

DMZ(demilitarized zone). The firewall only allows incoming connections to machines in the DMZ. These machines are then allowed to make connections to the internal network.

Since Online Ordering(see note), Central Manager (optionally), the Write-On Phone, and RMBrowser make connections from the outside network (via the internet) to your internal network, you will have to configure a machine in the DMZ to forward connections from the outside world to your internal RM Server. Central Manager is PCI certified when used in push mode only, so access from the internet to the store is not permitted.

We have tested the NetworkActiv AUTAPF port forwarder with the Write-On Phone and Online Ordering. You can download this program directly from the NetworkActiv web-site: http://www.networkactiv.com/ . You will need to purchase a license (currently $60). The free trial will suspend connections and present a warning dialog every half hour.

You may use other port forwarding or proxy server software on the DMZ machine and still be PCI compliant. However, ASI will not be able to help you configure or test other software.

Note: DMZ machines have been used in the past for Online Ordering. The bitvise Tunnelier software can be used an alternative to DMZ. Instructions to use the Bitvise Tunnelier program can be found in this document: Bitvise Tunnelier Installation Guide.

Use the following steps for port forwarding using NetworkActiv AUTAPF:

- Install NetworkActiv AUTAPF as a service.
- Set these recommended Miscellaneous settings:

  1. Miscellaneous Settings

     a. System Tray Settings Section

        i. Enable' "Show Icon in System Tray

        ii. Hide taskbar button when minimized

     b. Data Formatting Section

        i. Enable data rate in bits per second

     c. Previously running port forwarding operations (when program is started) section

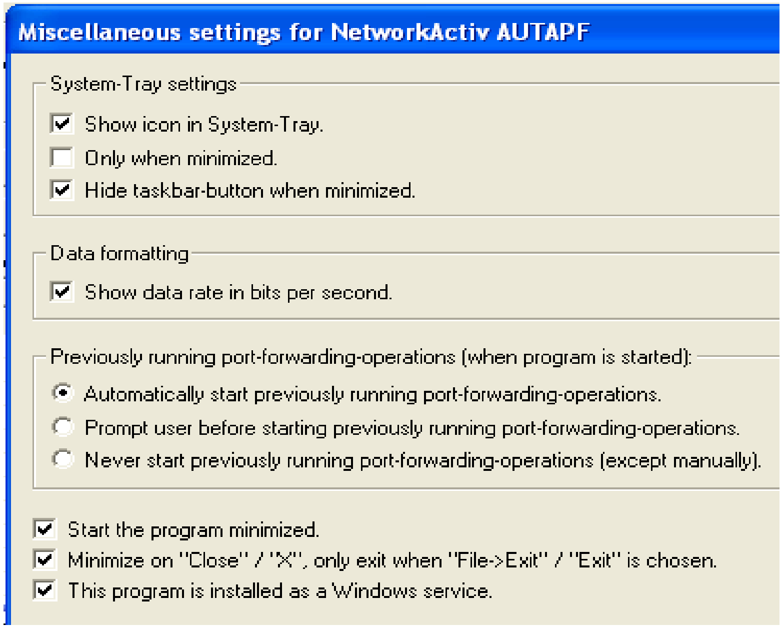
        i. Enable- "Automatically start previously running port-forwarding operations"

     d. Other Section

        i. Enable- Start the program minimized

        ii. Enable- Minimize on "Closed" / "X", only exit "File > Exit" / "Exit" is chosen.

        iii. Enable- This program is installed as a Windows Service



Miscellaneous settings for NetworkActiv AUTAPF

System-Tray settings

☑ Show icon in System-Tray.
□ Only when minimized.
☑ Hide taskbar-button when minimized.

Data formatting

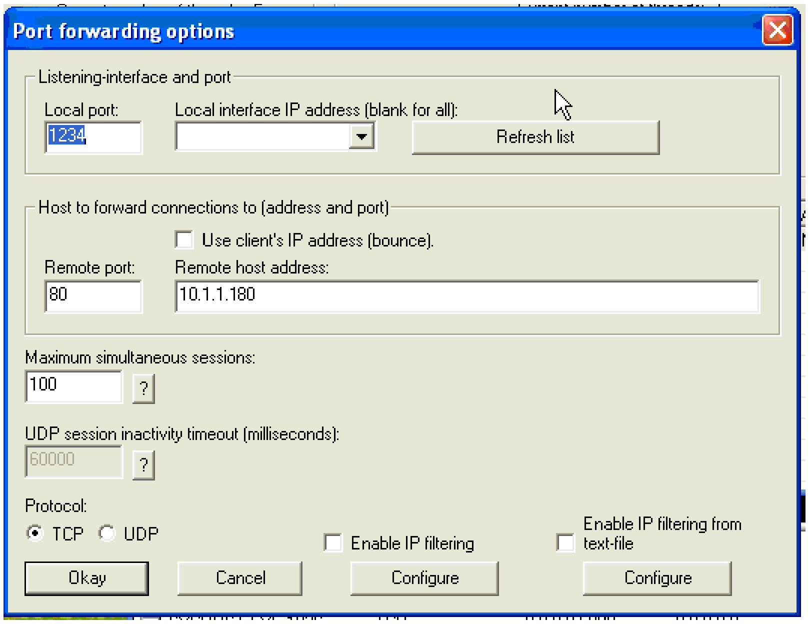
☑ Show data rate in bits per second.

Previously running port-forwarding-operations (when program is started):

● Automatically start previously running port-forwarding-operations.
○ Prompt user before starting previously running port-forwarding-operations.
○ Never start previously running port-forwarding-operations (except manually).

☑ Start the program minimized.
☑ Minimize on "Close" / "X", only exit when "File->Exit" / "Exit" is chosen.
☑ This program is installed as a Windows service.

2. Create a new port forwarding option filling out the following fields under the Port forwarding options:
   a. Local port: example:1234
   b. Remote port: 80
   c. Remote host address: use IP address of the server hosting RMServices.exe (i.e. 10.1.1.180)
   d. Protocol: TCP



Port forwarding options

Listening-interface and port

Local port: 1234

Local interface IP address (blank for all):

Host to forward connections to (address and port)

□ Use client's IP address (bounce).

Remote port: 80

Remote host address: 10.1.1.180

Maximum simultaneous sessions: 100

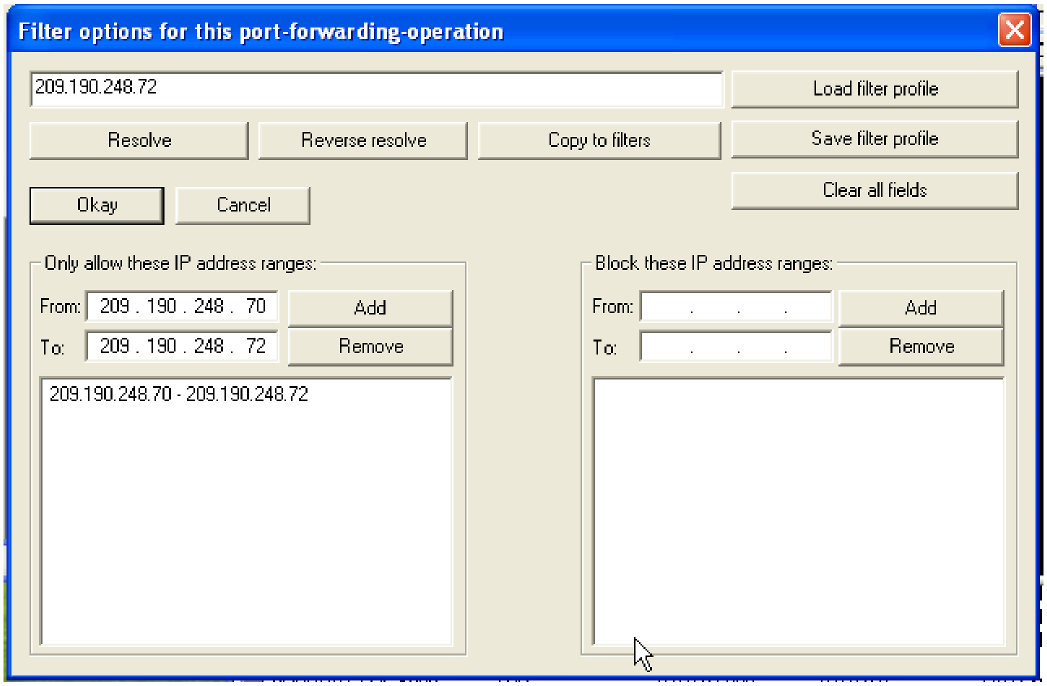
UDP session inactivity timeout (milliseconds): 60000

Protocol: ● TCP ○ UDP

□ Enable IP filtering

□ Enable IP filtering from text-file

You may want to “Enable IP Filtering” for an On Line Ordering installation. After the enabling this function you will then click on “Configure” and edit the filters similar to the screen shot below:



Filter options for this port-forwarding-operation

209.190.248.72

Only allow these IP address ranges:

From: 209 . 190 . 248 . 70

To: 209 . 190 . 248 . 72

209.190.248.70 - 209.190.248.72

Block these IP address ranges:

From: . . .

To: . . .

However, do not do “Enable IP Filtering” for Write-On Phone installations, as you cannot predict the IP address from where the Write-On Phone will be connecting. Also, this will make troubleshooting more difficult.

For On Line Ordering, the Test button will work correctly in the Order Routing Mode Setting box (see next section). However, the URL will not work from any machine other than the OO server itself.

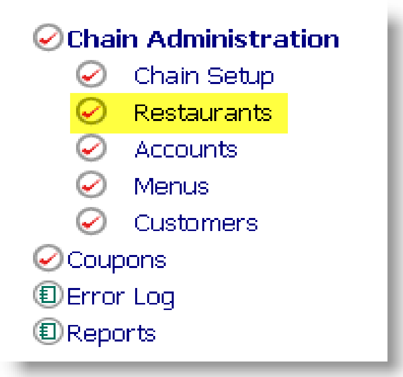
Under “Settings > Automatic Logging” > automatically log connection events, uncheck the “Do not log connection attempt from blocked IP addresses” option.

OO Server Setup

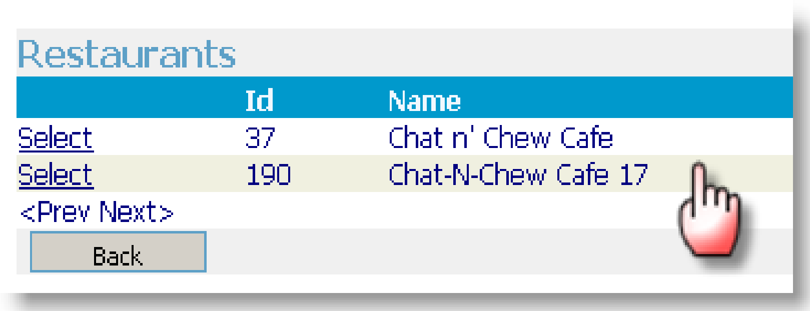
DMZ machines have been used in the past for Online Ordering. The Bitvise Tunnelier software can be used an alternative to DMZ. Instructions to use the Bitvise Tunnelier program can be found in this document: Bitvise Tunnelier Installation Guide. The following instructions below outline the steps for setting up OO when using a DMZ machine.

Log in to http://webordering.rmwservices.com/Asi.OO.Admin/Login.aspx .

1. Choose “Chain Administration | Restaurant”.



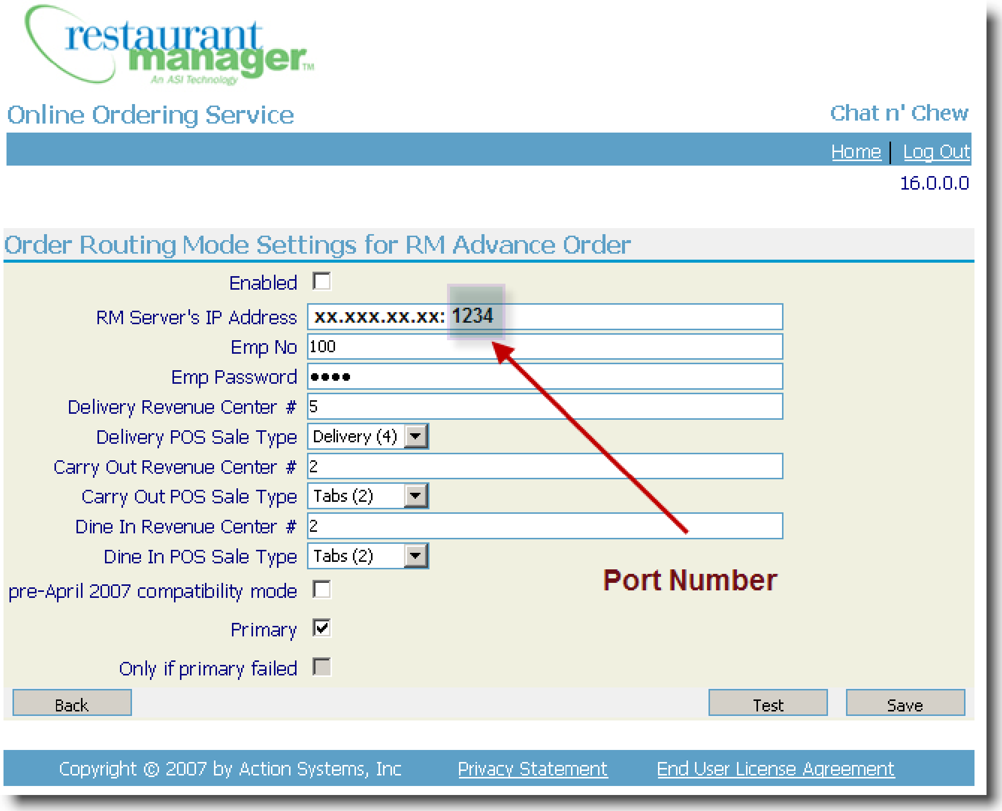
2. Click on the “Select” link for the appropriate restaurant.



Restaurants

	Id	Name
Select	37	Chat n' Chew Cafe
Select	190	Chat-N-Chew Cafe 17

3. Click on the “Select” link under “Order Routing Modes” for “RM Advance Order”:



Online Ordering Service

Chat n' Chew

Home | Log Out

16.0.0.0

Order Routing Mode Settings for RM Advance Order

Enabled	□
RM Server's IP Address	xx.xxx.xx.xx: 1234
Emp No	100
Emp Password	••••
Delivery Revenue Center #	5
Delivery POS Sale Type	Delivery (4)
Carry Out Revenue Center #	2
Carry Out POS Sale Type	Tabs (2)
Dine In Revenue Center #	2
Dine In POS Sale Type	Tabs (2)
pre-April 2007 compatibility mode	□
Primary	☑
Only if primary failed	□

Port Number

Copyright © 2007 by Action Systems, Inc   Privacy Statement   End User License Agreement

4. In the “RM Server’s IP Address” field, you will want to specify an IP address and a port. These will point to your DMZ computer. The port here should correspond to the port under AUTAPF’s “Listing-interface and port > Local port:” setting.

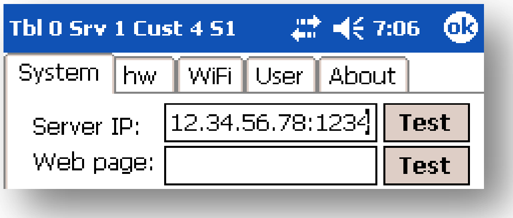
Note: No changes are required in OOLink

WO Phone Client Setup

Note that internal Write-On handhelds may go directly to the server machine via the internal network. This section is for setting up Write-On Phones that will access RMServices.exe via the internet.

In the “Options” dialog > “System” tab:

1. Enter the server IP address with the port at the end (i.e. xx.xx.xx.xx:1234).
2. Test the Server IP and port using the “Test” button next to the IP address field.



Tbl 0 Srv 1 Cust 4 S1   7:06

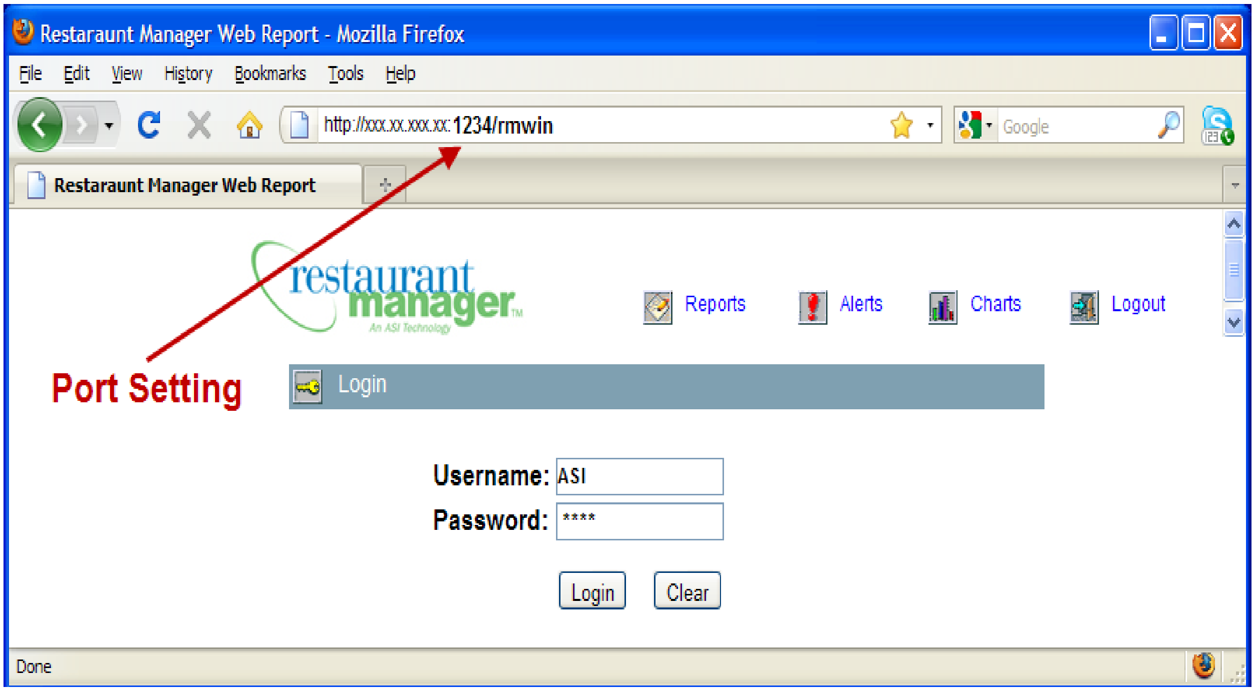
Server IP: 12.34.56.78:1234

Web page:

This IP address and port will point to your DMZ computer. The port here should correspond to the port under AUTAPF's "Listing-interface and port | Local port:" setting.

RMBROWSER SETUP

Simply point your web browser to your DMZ machine instead of the server where you currently have RMBrowser installed. The port forwarding will work transparently.



Restaraunt Manager Web Report - Mozilla Firefox

http://xxx.xx.xxx.xx:1234/rmwin

Port Setting

Login

Username: ASI

Password: ****

Appendix: Notes

Additional Source Information

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

PCI Data Security Standard 8.5.8 through 8.5.15 General Guidelines

The PCI standard requires the following password complexity for compliance (often referred to as using “strong passwords”):

- Do not use group, shared, or generic user accounts (8.5.8)
- Passwords must be changed at least every 90 days (8.5.9)
- Passwords must be at least 7 characters (8.5.10)
- Passwords must include both numeric and alphabetic characters (8.5.11)
- New passwords cannot be the same as the last 4 passwords (8.5.12)

PCI user account requirements beyond uniqueness and password complexity are listed below:

- If an incorrect password is provided 6 times the account should be locked out (8.5.13)
- Account lock out duration should be at least 30 min. (or until an administrator resets it) (8.5.14)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session (8.5.15)

Revision History

10/27/10 Revision History

1. added wording to comply with PA-DSS 1.1.4.a
2. section was added addressing PA-DSS 1.1.5.c
3. section was added to address PA-DSS 3.1.c within RM
4. section was added to address PA-DSS 3.1.c outside RM
5. section was added to address PA-DDS 3.2 within RM
6. section was added to address PA-DSS 3.1.c outside RM
7. section was added to address PA-DSS 4.2.b within RM
8. section was added to address PA-DSS 4.2.b outside RM
9. section was added to address PCI Data Security Standard 8.5.8 through 8.5.15 General Guidelines with RM
10. section was added to address PCI Data Security Standard 8.5.8 through 8.5.15 General Guidelines outside RM
11. section was added to address PA-DSS 6.1B &6.2.b
12. section was expanded to address remote access PA-DSS 11.2 and 11.3.b
13. section was added addressing firewall settings in a VPN network PA-DSS 10.1
14. additional section was added outlining Data Encryption PA-DSS 12.1.b

11/1/10 Revision History

1. section was adding addressing removal a cryptographic material (PA-DSS 2.7.a)

12/7/10 Revision History

1. section was added for new hardware recommendation. Removed wording for Symbol router that is no longer supported.
2. section on firewall was updated to reflect new hardware recommendations

12/13/11 Revision History

Updated document with ver 18 wording- there has been no structural changes since version 17