



**Payment Application Data Security Standard
(PA-DSS) Implementation Guidance
For Aldelo® For Restaurants Version 3.8.10 or Later**

PUBLISHED BY

Aldelo Systems Inc.
4641 Spyres Way, Suite 4
Modesto, CA 95356

Copyright © 1997-2009 by Aldelo Systems Inc.

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permissions of the publisher.

This manual is available through Aldelo Systems Inc. and resellers worldwide. For further information about other languages that the manual may be translated in, please contact Aldelo Systems Inc. or visit our Web site at www.aldelo.com. Send comments about this manual to contact@aldelo.com

Aldelo is the registered trademark of Aldelo Systems Inc. Other products or company names mentioned herein are the trademarks of their respective owners.

The example companies, organizations, products, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, logo, person, place or event is intended or should be inferred.

Table of Contents

Chapter 1 : Introduction to PA-DSS Compliancy.....	7
Chapter 2: PA-DSS Payment Application Environment Requirements	9
Remote Access.....	9
Non-Console Administration	9
Wireless Networks	9
Wireless Access Control	11
Transport Encryption	11
Manager Access	11
Network Segmentation.....	12
Information Security Policy / Program	14
Chapter 3: Aldelo® For Restaurants Configuration	15
Baseline System Configuration	15
Application Configuration	15
Installing Aldelo® For Restaurants.....	15
Chapter 4: Updates and References	17
Updates to Aldelo® For Restaurants.....	17
More Information	17

Chapter 1:

Introduction to PA-DSS Compliancy

Systems which process payment transactions necessarily handle sensitive cardholder account information. The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the Payment Application Data Security Standard (PA-DSS). The security requirements defined in the PA-DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PA-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 12 Requirements comprise the core of the PA-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

The remainder of this document describes the essential guidance for implementing Aldelo® For Restaurants in a PA-DSS compliant environment.

Chapter 2:

PA-DSS Payment Application Environment Requirements

Remote Access

The PA-DSS 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. Remote access should be disabled when not in use.

Non-Console Administration

Users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop Protocol (RDP)/Terminal Server, pcAnywhere, etc. to access other hosts within the payment processing environment. However, to be compliant, every such session must be encrypted with at least 128-bit encryption, although 256-bit encryption is preferred (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for pcAnywhere it means using symmetric or public key options for encryption. Additionally, the PA-DSS user account and password requirements will apply to these access methods as well.

Wireless Networks

The initial setup of your wireless network is beyond the scope of this document and should be only performed by an expert in wireless network security. However, general information on how to setup a wireless network may be found at <http://www.microsoft.com/athome/moredone/wirelesssetup.mspx>, while additional information and several useful tips on improving the security of a wireless network (in Windows XP) may be found at <http://www.microsoft.com/windowsxp/using/networking/security/wireless.mspx>.

Many wireless access points and wireless routers do not require the use of an administrator password to logon to the device or to configure it. Others may include default passwords right out of the box. When setting up

such devices, a strong password should be setup and used to provide secure access. The PA-DSS standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must include numeric, alphabetic, and special characters
- Passwords must be changed at least every 90 days
- New passwords cannot be the same as the last 4 passwords

Any default passwords should be disabled to prevent unauthorized access. Be sure to record your new password and to keep it in a safe place. Never write down the password on paper and leave it in an accessible location where it may be viewed by others. Treat your password as you would any other valuable possession. If it is lost, you may have to reset your wireless access point or wireless router to the factory default settings which would delete any previous configuration information, requiring you to again setup the device from scratch.

Almost all wireless access points and wireless routers constantly broadcast your Service Set Identifier (SSID). This is essentially a unique name for your wireless network to distinguish it from others. This name must be known to connect to your network. Broadcasting the name allows anyone to connect a device to your network without knowing its SSID. This makes setup extremely easy but it also allows anyone within range to connect to your wireless network. To enhance the security of your wireless network, you should disable the broadcasting of your SSID. See the documentation that came with your wireless access point or wireless router for instructions on how to accomplish this.

Wired Equivalency Privacy (WEP) is an encryption method designed to make it more difficult for unauthorized users to access your wireless network. Encryption is a system of subjecting information to an algorithm that uses a key to make that information unreadable to anyone who does not possess the same key, which is required to reverse the process (decryption). WEP has been in use for quite some time now and several weaknesses have been identified that allow hackers to gain access to WEP protected networks in a matter of minutes. As such, WEP is falling out of favor while Wi-Fi Protected Access (WPA) is becoming more popular. WPA provides better protection by allowing the use of much stronger encryption keys which are far more difficult to determine, even through the use of encryption code cracking software. WPA2 is a version of WPA that provides even stronger encryption. WPA2 can be found in the most recently manufactured hardware. To use WPA or WPA2, be sure to install the most recent downloadable updates to your operating system. No matter which method you decide to use, always use the latest and strongest encryption available to you to help ensure against data loss.

An additional level of security may be added by enabling Media Access Control (MAC) filtering to your network. A MAC address is unique 48 bit hexadecimal number that identifies a specific network adapter. Enabling MAC filtering allows you to restrict access to your network to only those devices whose MAC addresses you have manually entered into the wireless access point or wireless router. All others are denied access. Although it can be tedious to setup, especially if you have many wireless clients or they change frequently, MAC filtering adds another level of security to help stop hackers from invading your network.

Some, but by no means all wireless access points and wireless routers allow the user to adjust the power output of the transmitter. If yours does, you may want to decrease its transmitting power. Reducing the power reduces the distance the signal travels. Although you don't want to reduce the power so much that some of your wireless clients are unable to access your network, there is also no need to use so much power that your

transmitter's signal reaches far beyond the boundaries of your business. Reducing the transmitting power properly can help prevent access to your network by those within close proximity to your physical location.

With some wireless routers, you have the ability to perform administrative duties remotely by way of the Internet. If your wireless router has this capability, it should be disabled and not used. Use of this feature has the potential of allowing a hacker anywhere in the world to access your network. If you absolutely must use this feature, limit access to your router to communications originating from a specific IP address or range of IP addresses to prevent unauthorized access to your network.

Wireless Access Control

The PA-DSS standard requires the encryption of cardholder data transmitted over wireless connections. The following items identify the PA-DSS standard requirements for wireless connectivity to the payment environment:

- Firewall/port filtering services should be placed between wireless access points and the payment application environment with rules restricting access
- Use of appropriate encryption mechanisms such as VPN, SSL/TLS at 128 bit, WEP at 128 bit, and/or WPA
- If WEP is used, the following additional requirements must be met:
 - Another encryption methodology must be used to protect cardholder data
 - If automated WEP key rotation is implemented, key change should occur every ten to thirty minutes
 - If automated key change is not used, keys should be manually changed at least quarterly and when key personnel leave the organization
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed or disabled
- Access point should restrict access to known authorized devices (using MAC Address filtering)

Transport Encryption

The PA-DSS 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 sensitive cardholder data during transmission over public networks (this includes the Internet and Internet accessible demilitarized zone [DMZ] network segments).

Additionally, PA-DSS requires that cardholder information is never sent via e-mail without strong encryption of the data.

Manager Access

The Aldelo® For Restaurants passwords are administered by the Master (first or primary) Administrator. This Master Administrator therefore is responsible to perform periodic password changes.

Additionally, the Master Administrator should sign an official acknowledgement form created or issued by the merchant organization of those manager access responsibilities.

Examples of Manager Access Responsibilities:

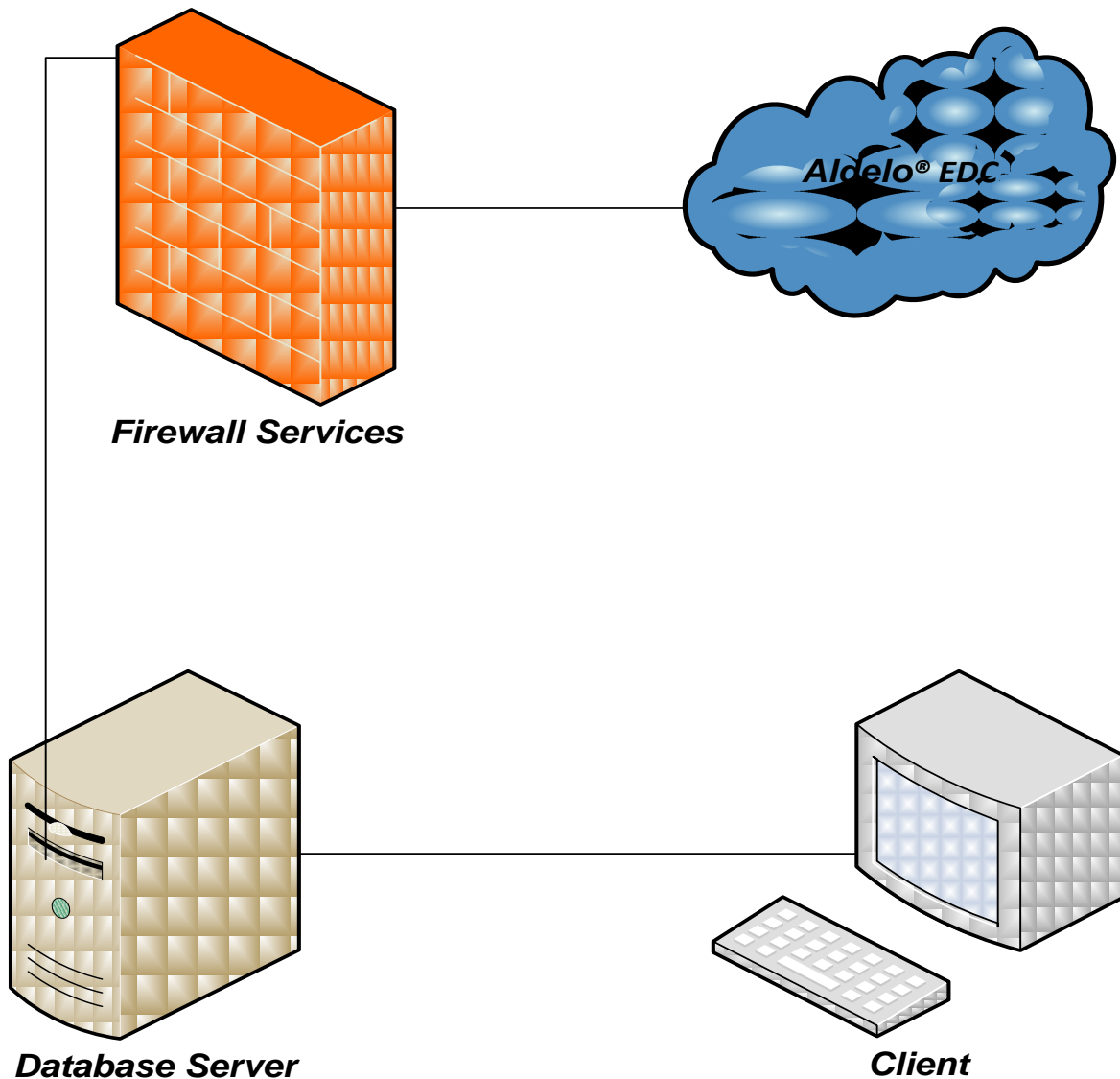
- Change the administrator account password periodically in compliance with PA-DSS requirements
- Periodically perform security audit and transactional log audits in compliance with PA-DSS requirements
- Maintain System updates, patches, and security perimeter configurations in compliance with PA-DSS requirements
- Manage user or process accounts in compliance with PA-DSS requirements

Network Segmentation

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

A simplified high-level diagram of an expected network configuration for a web based payment application environment is included:

Data Flow Diagram



Information Security Policy / Program

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

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

- Read the PA-DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PA-DSS requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the action plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PA-DSS Self Assessment Questionnaire.
- Call in outside experts as needed. Visa has published a Qualified Security Assessor List of companies that can conduct on-site PA-DSS compliance audits for Level 1 Merchants, and Level 1 and 2 Service Providers. MasterCard has published a Compliant Security Vendor List of SDP-approved scanning vendors as well.

Chapter 3: Aldelo® For Restaurants Configuration

Baseline System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PA-DSS compliance:

- Windows XP Professional with Service Pack 3
- Windows Vista Business, Enterprise, and Ultimate Editions
- Windows Server 2003 with SP1
- Windows Server 2008 with R2
- All latest updates and hot-fixes should be tested and applied
- 512 MB of RAM minimum, 1 GB or higher recommended
- 1 GB of available hard-disk space
- TCP/IP network connectivity

Application Configuration

Aldelo® For Restaurants requires certain Windows Operating System features to be installed prior to deploying. There are some prerequisites that must be met before Aldelo® For Restaurants may be installed on a system.

The following list describes the hierarchical order of deployment:

- **Step 1:** Ensure that the system to which Aldelo® For Restaurants will be deployed meets the Baseline System Configuration requirements
- **Step 2:** Install Aldelo® For Restaurants based on intended deployment strategies (Server or Client)

The following sections describe key concepts for deployment to a system running Windows XP Pro. Installation in Windows Vista, Windows Server 2003, or Windows Server 2008 should be comparable.

Installing Aldelo® For Restaurants

When the above considerations have been met, you are ready to install and setup Aldelo® For Restaurants. The first action is to install Aldelo® For Restaurants onto the system that will be hosting the application. Install this application just like you would any other program. For instructions on installing the software, please see the

section entitled “Installing Aldelo® For Restaurants” in Chapter 5 of either the Aldelo® For Restaurants User Guide or the Aldelo® For Restaurants User Manual. Once installed, the software may be configured.

Once the AFR Service is installed, all credit and debit card processing events are logged to the EDC Audit Log and AFR Service starts and stops are logged to the Windows Event Viewer.

Chapter 4:

Updates and References

Updates to Aldelo® For Restaurants

Updates to Aldelo® For Restaurants are made available from time to time and should immediately be installed if the update addresses a security issue. Aldelo Systems Inc. will have security related issues resolved within 10 business days of development confirming such issues. Updates will be posted to the www.aldelo.com website upon release and can be downloaded at any time with the proper credentials for the website.

More Information

A copy of the Payment Card Industry Data Security Standard (PCI DSS) from VISA's security website is available at the following Internet address:

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Additional information for merchants from VISA is available at the following Internet address:

http://usa.visa.com/business/accepting_visa/ops_risk_management/PA-DSS_merchants.html?it=il/business/accepting_visa/ops_risk_management/PA-DSS.html|Merchants

A listing of qualified security assessors from VISA is available at the following Internet address:

http://usa.visa.com/business/accepting_visa/ops_risk_management/PA-DSS_accessors.html?it=12/business/accepting_visa/ops_risk_management/PA-DSS_merchants%2Ehtml|Assessors

For Best Security Practices when installing Internet Information Services, please refer to the Microsoft website

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/596cdf5a-c852-4b79-b55a-708e5283ced5.mspx?mfr=true>

