ALDELO
Path to Simplicity

ALDELO® EDC

Payment Card Industry Data Security Standard (PCI-DSS) Implementation Guide

Aldelo® EDC Payment Card Industry Data Security Standard (PCI-DSS) Implementation Guide

Aldelo® EDC Version 7.0

PUBLISHED BY
Aldelo, LP
6800 Koll Center Parkway, Suite 310
Pleasanton, CA 94566
07/01/2016

This manual is available through Aldelo, LP and resellers worldwide. For further information, please contact Aldelo, LP or visit our website at www.aldelo.com. Send comments about this manual to contact@aldelo.com.

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.

For the sake of simplicity, all gender references are written only in the masculine. Any references to the masculine gender should be interpreted to include the feminine gender as well and vice versa, wherever applicable.

Reviewed by:	Date	Time
Jeff Moore / Dave Ventura	03/28/2013	12:47 PM
Jeff Moore / Dave Ventura	04/04/2013	12:06 PM
Jeff Moore / Dave Ventura	05/30/2013	08:25 AM
Jeff Moore / Dave Ventura	06/10/2013	09:20 AM
Dave Ventura	08/06/2015	08:12 AM
Jeff Moore / Dave Ventura	02/29/2016	10:47 AM
Jeff Moore / Dave Ventura	07/01/2016	04.05 PM

Table of Contents

Chapter 1: Introduction to PCI-DSS Compliance 10

Chapter 2: PCI-DSS Payment Application Environment Requirements 12
Access Control 12
Remote Access 13
Non-Console Administration 13
Transport Encryption 13
Encryption Key Management 14
Cardholder Data Retention 15
Key Custodian 15
Network Segmentation 16
Windows Restore Points 16
Information Security Policy / Program 18

Chapter 3: Payment Application Configuration 20
Baseline System Configuration 20
Application Configuration 20
Wireless Configuration 20
Installing Internet Information Services 21
Installing .NET Framework 4.6 21
Installing Microsoft Point of Service for .NET 21
Installing SQL Server 2008 22
Installing Aldelo® EDC 22
Database Setup 22
Store Settings 23
Security Settings 24
Users 24
Merchant Accounts 25
Application Requirements 26

Chapter 4: Updates and References 28
..... 28
Updates to Aldelo® EDC 28
Technical Support 28
More Information 28
Application Versioning Methodology 29

Chapter 5: PA-DSS v 3.2 Requirements 30

Chapter 1: Introduction to PCI-DSS Compliance

Systems that 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 Card Industry Data Security Standard (PCI-DSS). The security requirements defined in the PCI-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 are defined as any network devices, hosts, or applications 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.

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

Chapter 2: PCI-DSS Payment Application Environment Requirements

Access Control

The PCI-DSS requires that access to all systems in the payment processing environment be protected through the use of unique user accounts 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. Additionally, any default accounts provided with operating systems, databases, and/or devices should be removed/disabled/renamed as possible, or at least should have PCI-DSS compliant complex passwords and should not be used. Examples of default administrator accounts include "administrator" (Windows systems), "sa" (SQL/MSDE), and "root" (UNIX/Linux).

Please note that Aldelo® EDC does not use or contain any built-in application user accounts.

The PCI-DSS standard requires the following password complexity for compliance:

- Passwords must be at least 7 characters
- Passwords must include numeric, alphabetic (both upper and lower case), and special characters
- Passwords must be changed at least every 90 days
- New passwords cannot be the same as the last 4 passwords
- Do not use default user names and passwords, such as "Administrator" and "12345"
- Always use unique user names and passwords
- Users should never create shared usernames and passwords and each user must have a unique username and password that is appropriate to his system access level

PCI-DSS 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
- Account lock out duration should be at least 30 minutes (or until an administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session
- Forgotten passwords may be reset by answering three challenge questions (the answers to these questions are setup when the user account is created)

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI-DSS compliant.

Remote Access

The PCI-DSS standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment, access should be authenticated using a multi-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. When not in use, remote access must be disabled.

If remote access is used, the following guidelines must be adhered to:

- Change default settings in the remote-access software (for example, change default passwords and use unique passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses
- Use strong authentication and complex passwords for logins (See PA-DSS Requirements 3.1.1 through 3.1.11)
- Enable encrypted data transmission according to PA-DSS Requirement 12.1
- Enable account lockout after a certain number of failed login attempts (See PA-DSS Requirement 3.1.8)
- Establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed
- Enable the logging function
- Restrict access to your environments by vendors for support to authorized integrator/reseller personnel

Non-Console Administration

The EDC application itself does not support non-console access. All access is through an application-provided interface. However, you as a merchant may choose to access the underlying systems remotely.

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, 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 multi-factor authentication required for users connecting from outside the payment processing environment). Implement and use strong cryptography (such as SSH, VPN, or TLS) for encryption of any non-console administrative access to payment application or servers in the cardholder data environment. In addition, any non-console access must support the multi-factor authentication.

Transport Encryption

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 TLS 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, PCI-DSS requires that cardholder information is never sent via email without strong encryption of the data.

The Aldelo® EDC application uses TLS 1.2 for transmission of cardholder data to the processor. The application does not support the use of end-user messaging technology for the transmission of cardholder data.

Encryption Key Management

The application utilizes AES with a programmatic interface to generate 128-bit keys for securing the storage of the credit card number and expiration date in accordance with PCI DSS 3.4. Cardholder data is stored in the following locations only:

File Name	Table Name	Field Name	Card Data Element Stored	Encryption Used
Defined by Customer	EDC Transactions	TransactioninfoENC	Card Number	AES
Defined by Customer	EDC Transactions	TransactioninfoENC	Expiration Date	AES

Cardholder data is not stored in any other location and the application cannot be configured to do so. Keys generated by the application are stored in predefined locations by the application. These keys are stored securely in the fewest possible number of locations.

You must restrict access to the ability to perform change keys to the fewest number of key custodians necessary. These key custodians must acknowledge their role in securing the encryption keys and must sign a Key Custodian Agreement. A list of key custodian responsibilities is contained in the section titled Key Custodian, below.

Access to generate new keys is restricted to authorized application users through the use of RBAC, limiting access to the key and passwords change functions. These settings are available under each user's role definition.

The application does not grant access to stored encryption keys through an application interface, and users have no access to unencrypted keys through any interface. The application supports secure key distribution, as keys and passwords are encrypted prior to storage.

You may change your encryption keys as often as required. However, you should also adhere to the following key management processes to maintain you PCI DSS compliance:

- Change your encryption keys if they have been weakened, such as by the departure of a key custodian (this must happen immediately)

- Change your encryption keys if compromise is confirmed or suspected (this must happen immediately)

Note: The application prevents the use of replaced or retired keys, as replaced or retired keys and passwords cannot be used for further encryption. Replaced or retired encryption keys are destroyed by the application upon creation of new keys and passwords.

Note: The application prevents the unauthorized substitution of keys and password through the use of RBAC for application users. Access to change keys through the application is logged. In addition, to prevent a key or password from being modified outside of the application, a check is performed to confirm no changes have been made. If a key or password is modified, the application will inform you that the stored keys are corrupted and no longer useable.

Note: Installation of the new version of the application will force the re-encryption of all stored historical cardholder data and securely remove the previously used cryptographic data.

Cardholder Data Retention

The application will automatically purge all cardholder data upon batching and sending the data to your merchant processor.

As you may decide to retain cardholder data outside of the application using third party means (Excel spreadsheet, written hardcopy, etc.), you must understand that any cardholder data collected by you exceeding the defined retention period must be purged based upon business, legal, and/or regulatory requirements in order for you to achieve and meet your own PCI-DSS compliance requirements.

Key Custodian

The Aldelo® EDC encryption key is administered by the Master (first or primary) Administrator. This Master Administrator therefore is considered the Key Custodian of the Payment Application, and is responsible for performing periodic key changes (as well as their passwords) based on PCI-DSS compliance requirements.

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

Examples of Key Custodian Responsibilities:

- Change the administrator account password periodically in compliance with PCI-DSS requirements
- Change the Aldelo® EDC encryption key periodically in compliance with PCI-DSS requirements
- Periodically perform security audits and transactional log audits in compliance with PCI-DSS requirements
- Maintain System updates, patches, and security perimeter configurations in compliance with PCI-DSS requirements
- Manage user and/or process accounts in compliance with PCI-DSS requirements

Network Segmentation

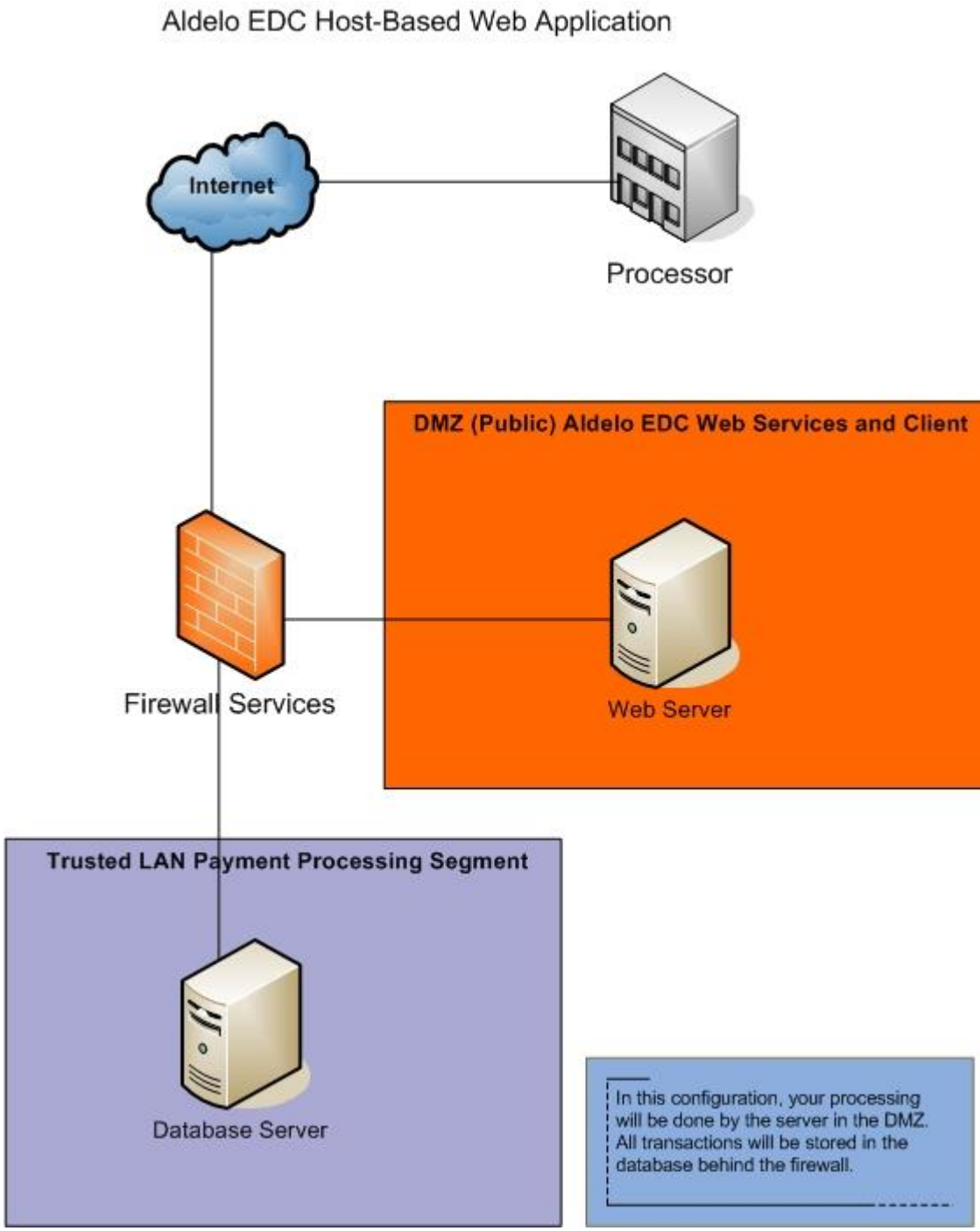
The PCI-DSS requires that firewall services be used (with NAT [Network Address Translation] or PAT [Port Address Translation]) to segment the network into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and 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 may be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

Windows Restore Points

Please note that Windows Restore Points must be disabled. Restore points may be disabled by following the instructions for your operating system as follows:

- Windows 7 – http://windows.microsoft.com/en-us/windows7/turn-system-restore-on-or-off
- POS Ready 7 – http://support.microsoft.com/kb/310405
- Windows 10 – Windows Restore Points are disabled by default in Windows 10.
- Windows Server 2014 – The Windows Restore Points feature is not available in Windows Server 2014 and therefore does not have to be disabled.

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



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 PCI-DSS in full and perform a security gap analysis to identify any gaps between existing practices in your organization and those outlined by the PCI-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 PCI-DSS Self-Assessment Questionnaire. The questionnaire is available at the following Internet address: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php
- Call in outside experts as needed. The PCI Council has published a Qualified Security Assessor List of companies that can conduct on-site PCI-DSS compliance audits for Level 1 Merchants, and Level 1 and Level 2 Service Providers. The PCI Council has also published a list of PCI-approved scanning vendors. This list is available at the following Internet address: https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

Chapter 3:
Payment Application Configuration

Baseline System Configuration

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

- Windows POSReady 7
- Windows 7 Professional
- Windows 10
- Windows Server 2014
- All latest updates and hot-fixes should be tested and applied
- CPU 2GHz
- 2GB of RAM minimum
- 2 GB of available hard-disk space
- TCP/IP network connectivity
- Broadband Internet Connection

Application Configuration

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

The following list describes the hierarchical order of deployment:

- **Step 1:** Ensure that the system to which Aldelo® EDC will be deployed meets the Baseline System Configuration requirements
- **Step 2:** Ensure that the System has Internet Information Services 5.0 or later installed
- **Step 3:** Install Aldelo® EDC based on intended deployment strategy (Server or Client)

The following sections describe key concepts for deployment to a system running Windows 7 Professional. Installation in Windows POSReady 7, Windows 10, and Windows Server 2014 should be comparable.

Wireless Configuration

Although Aldelo does not recommend wireless networks for use with Aldelo® EDC, customers who choose to setup a wireless network should choose a wireless technology that supports wireless encryption that does not use the default wireless encryption keys, passwords, and SNMP community strings. Your wireless network

must use industry best practices and comply with the IEEE 802.11i standard to implement strong encryption for authentication and transmission. The use of WEP as a security control is prohibited as of June 30, 2010 by the PCI Security Standards Council, LLC. You must install a firewall between any wireless networks and systems that store cardholder data, and configure firewalls to deny or, if such traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

Installing Internet Information Services

Aldelo® EDC requires Microsoft Internet Information Services (IIS) to be installed prior to deployment. IIS is included with the Windows 7 Professional, POSReady 7, Windows 10, and Windows Server 2014 operating systems.

If the System does not have IIS installed, it may be installed by using the Add/Remove Windows Components function from the Windows Control Panel. Be sure to have your Windows installation CD available when installing this component.

The following steps describe how to install IIS to a Windows 7 Professional System:

1. Click the "Windows Logo" button on the task bar to bring up the Start Menu.
2. Navigate to "Control Panel" to invoke the control panel list of features.
3. Double click the "Programs and Features" icon.
4. Within the "Programs and Features" screen, click the "Turn Windows Feature On or Off" option.
5. The UAC prompt will appear requesting your permission to continue.
6. In the "Windows Features" dialog, select the "Internet Information Services" option.
7. Click "OK."
8. Once the installation finishes, IIS is installed on Windows 7 Professional.

Installing .NET Framework 4.6

Aldelo® EDC requires Microsoft .NET Framework 4.6 to be installed on the System in order to operate. The .NET Framework 4.6 is acquired through Windows Update. Be sure to use the Windows Update feature to apply all updates to your system.

Installing Microsoft Point of Service for .NET

Aldelo® EDC supports the printing of transaction receipts to specialized POS printers. Aldelo® EDC uses Microsoft Point of Service (POS) for .NET peripheral integration methods to deliver printing instructions. The installation of this component is optional for merchants.

Microsoft POS for .NET 1.12 is available for download from Microsoft at the following location: http://www.microsoft.com/en-us/download/details.aspx?id=5355.

If POS for .NET printing integration is to be used, the underlying POS printer must support POS for .NET or OPOS 1.13 with appropriate drivers. For technical assistance regarding POS printer setup and integration with POS for .NET, please contact the respective printer manufacturers for assistance.

Installing SQL Server 2008

Aldelo® EDC requires SQL Server 2008 to be installed in order to function. Aldelo® EDC supports all SQL Server 2008 editions except the Compact Edition. SQL Server 2008 is used to store operational data for Aldelo® EDC. For most merchants, SQL Server 2008 Express installed as an Aldelo Instance is preferred since it is free and is adequate in most cases.

Microsoft SQL Server 2008 Express is available for download from Microsoft at the following location: http://www.microsoft.com/en-us/download/details.aspx?id=1695.

For instructions on how to properly install SQL Server 2008, please refer to the appropriate software installation documentation. For detailed installation instructions, please see the Aldelo® EDC User manual. Please follow all PCI-DSS compliance requirements when installing the database server.

Installing Aldelo® EDC

When the above considerations have been met, you are ready to install and setup Aldelo® EDC. The first action is to install Aldelo® EDC onto the system that will be hosting the application. Install this application just like you would any other program. Once installed, you are able to start configuration. The following sections describe each setup action in detail.

Database Setup

The first step in working with Aldelo® EDC is to setup a new database. Start by first connecting to the SQL Server 2008 that you are working with. To setup your database, follow the steps below.

1. Click “File” on the Aldelo® EDC menu bar.
2. Select “Database Setup” to bring up the screen where you configure your database connection settings and create new databases.
3. In the SQL Server field, enter the name and instance of the SQL Server 2008 that you wish to connect to. If it is located locally, you may use the word “(local)” or enter “.”
4. Once you have selected your SQL Server, fill in the authentication information. You can use either Windows Authentication or SQL Server Authentication. However, it is highly recommended that Windows Authentication be used to prevent your username and password from being sent in clear text as this is the case with SQL Server Authentication. The Aldelo Instance of SQL Server 2005 Express is set to Mixed Mode Authentication to give you the option of choosing your authentication type.
5. Click “Test” to ensure that the new settings are entered properly. If it fails, please review the SQL Server and Authentication fields previously specified.
6. Once the test is successful, select the “Create New Database” option.

7. Type the name of your database in the "Database Name" field. Do not enter spaces or special characters.
8. Click the "**…**" button in the "Data File Path" to allow the selection of the folder in which you wish to store the database. The default folder should be fine for most installations.
9. Click "Create" to run through the process of creating the database on the server. You should see a successful message once it completes.
10. Click "Select Existing Database."
11. Select the database that was just created.
12. Click "Connect" to create an association with the selected database for use. The "Current Data Source Link" information is updated to show the newly selected connection settings.

	**Tech Tip:** To implement the software in a DMZ environment, you must install Aldelo® EDC on the database machine for the purpose of creating the database. Once this is complete, you may remove Aldelo® EDC completely.

Store Settings

Once the database is created and connected, please go to the Store Settings menu option to start configuration. The following list will help you guide through this process:

1. Click "Setup" in the Aldelo® EDC menu bar.
2. Select "Store Settings" to display the Store Settings screen for configuration.
3. Enter the IP Address (or "localhost" if it's the same system) of the system hosting the Payment Application. Most installations will use "localhost". It is a good idea to give this station a static IP Address since this system is hosting a service that is accessed via an IP Address. As you may be instructed by your network administrator, you are able to add a port number to the IP address or computer name, for example "192.168.28.16:8080" or "computer_name:8080".
4. You can leave the "EDC Web Service Application Name" as the default name unless you manually change it in IIS. Only advanced networking professionals should change this.
5. "Use Secure Channel (TLS)" is used to secure communications between an application and Aldelo® EDC. This is highly recommended as it prevents any attempts to capture data traveling across the network or internet if used remotely. To use TLS, you must either purchase a TLS certificate from a trusted vendor or generate one using Windows. For more information on this, refer to the Microsoft help system or website.
6. Enter a password in the "Card Encryption Password" field. This password is used to encrypt all transactions that are stored in the database. Additionally, this field is the encryption key, and the Master Administrator (first administrator to the System) is considered the Key Custodian. As a Key Custodian, the administrator is responsible for periodically changing this key and the administrator's account password per PCI-DSS compliance requirements. Additionally, the Key Custodian should sign an acknowledgement of responsibilities form with the merchant.
7. "Audit Trail History Kept Days" is the number of days the system will keep recorded activities in the system. These can be viewed in the Reports section of the software. It is recommended that you keep a good history of your system audit logs. The minimum is 90 days but it is recommended that you keep them for 180 days or more.
8. "Batch Auto Close Time" is the time that the batch will automatically be processed.
9. "Auto Batch Close User Name" is the user account name that will perform the auto batch.

    a. The software must be running at all times for the Auto Batch function to work.
    b. The batch user must also have Batch and Sales security permissions assigned.
10. Click “Receipt” to go to the next tab.
11. Fill in the “Receipt Header Line 1” with what you would like to show at the top of the credit card slip.
12. Click “Done” to save the settings so you can move onto other first time setup tasks. You can always come back to this page to change more settings once you have the initial ones complete.

Security Settings

Before you are able to fully use the software, you must setup at least one user account. Each user account will have securities associated with it by assigning a security role to the user. These security roles must first be created before they can be assigned to any user. To create a security role, follow the steps below.

1. Click “Setup” on the Aldelo® EDC menu bar.
2. Select “Security Settings” to display the screen where all your security roles are listed.
3. Click “New” to allow you to create your first security role.
4. For the first security role, it is a good idea to call it something like “Admin”, “Owner”, or something to that affect. This user will have all rights in the software so make sure to check all checkboxes to allow full access to everything.
    a. Administrative access should only be given to one person. This employee should not share this access with any other employee or give out their username or password.
5. Click “Done” to save this security role.

Users

After you have created your first security role that has full access to the software, you want to assign that role to your first user. This user will be the administrator of the software since he or she will have full access to all the features of the software. To create the first user and assign the security account, follow the steps below.

1. Click “Setup” at the Aldelo® EDC menu bar.
2. Select “Users” to display the screen where all your user accounts are listed.
3. Click “New” to create a new user.
4. Fill in the “User Name” field with a user that describes who or what this user is. The first one should be the name of the person who will be administering the system. This should not be “Admin” or “Administrator” or the person’s title. It should be the actual name of the person.
5. Fill the in the “Password” and “Re-enter Password” fields with this user’s password. This will be the password used when you try to access something that is protected by the security settings. The password must be a complex password in that it must have 7 characters, upper and lower case, special characters, and numbers. Passwords automatically expire in 90 days and will automatically lock the user out after 6 attempts to guess the password. If the user does not change the password before the password expires, the account will be locked and the administrator will have to unlock the account before the password can be updated. These are PCI-DSS compliancy requirements. If your account is locked, it will automatically unlock after 30 minutes or can be reset by the administrator. The 30-minute reset does not apply to expired password locks. Passwords must also be historically unique and you cannot use the same password again within 4 changes of your password.

6. To assign the security role to this user, put a check in the box next to the security role you wish to assign to this user. The first user should have administrator rights so that he may have full access to the system.
7. Users will be forced to create challenge answers for use with resetting their password. These challenge answers should be personal and secret and must never be shared with others.

If the user is the Master Administrator, then this person will be considered the Key Custodian. Please see the Key Custodian sections mentioned previously for more details.

Merchant Accounts

Once you have your first user setup, you can now setup your merchant account. This is the core of the software and you must have a merchant account to complete this section. If you have not setup your merchant account yet with your merchant account provider, you can still setup other parts of the software and come back to it later. To setup a new merchant account, follow the steps below.

1. Click "Setup" on the Aldelo® EDC menu bar.
2. Select "Merchant Accounts" to display the list of Merchant Accounts you have. Normally you will have only one.
3. Click "New" to display a blank Merchant Account.
4. Fill in the "Account Name" field. This may be any name you wish and does not have to be the name of the account provider.
5. Select the "Account Type" as "Primary", "Secondary", "Gift", etc.
6. Select the "Merchant Service Provider." This is the actual company where you have your merchant account. As you change this field, the processor settings change as well.
7. Select the "Business Type."
    a. Restaurant: if the merchant is setup as a restaurant (Needs tip adjustments)
    b. Retail: if the merchant is setup as a retail store (No tip adjustments)
    c. MOTO: if the merchant is setup as a mail order/telephone order operation
8. Fill in the various fields that pertain to this merchant account type. This information is obtained from your merchant provider.
9. Mark the account as "Active Account."
10. Select "Enable Tracing." This allows you to track exactly what is going through the system and is very useful when troubleshooting issues.
11. Click "Done."

Once the merchant account is configured in the Payment Application, it is a best practice to use a live credit card to process a test transaction against the live merchant account. Once this live test is successful, make sure to close batch.

It is recommended that customers **do not** enable the "Demo" checkbox within the Merchant Account Setup screen. The "Demo" checkbox is reserved only for use under the supervision or guidance of Aldelo, LP's support engineers. When a merchant account is setup as "Demo," all transactions are simulated, and no request is sent to the processor. (Do not use the "Demo" feature unless instructed by an Aldelo, LP support engineer. When a test session ends, always close the current batch before switching back to "Live" mode)

	**Tech Tip:** If you need more information about any field in Aldelo® EDC, use the tool tips by keeping the mouse pointer over the field you have questions about. This displays a description of what the field is used for.

Application Requirements

The Aldelo® EDC application may operate on the following Microsoft Windows operating systems:

- Windows POSReady 7
- Windows 7 Professional
- Windows 10
- Windows Server 2014

The Aldelo® EDC application supports the following Microsoft Databases for storage:

- Microsoft SQL Server 2008
- Microsoft SQL Server 2014

The Aldelo® EDC application requires the following ports and services to function:

- TLS 1.2 over 443/TCP outbound to the processor
- TCP Port 8080 for internal communication by default, but this port number is customer-configurable
- 1433/TCP for Database communication (Internal Only)

The Aldelo® EDC application supports the following POI devices for MSR card and Chip acceptance:

- All pinpad devices are semi-integrated systems and are supported by your acquirer's bank.

Chapter 4:
Updates and References

Updates to Aldelo® EDC

Updates to Aldelo® EDC are made available from time to time and should immediately be installed if the update addresses a security issue. Aldelo, LP will have security related issues resolved within 10 business days of the development staff confirming such issues. Updates will be posted to the http://aldelo.com website upon release and can be downloaded at any time with the proper credentials for the website. To obtain the proper credentials, contact your Aldelo authorized reseller. All downloaded files are digitally signed for your protection. The user must maintain system updates, patches, and security perimeter configurations in compliance with PCI-DSS requirements.

Technical Support

Aldelo Technical Support is available 24/7 to assist customers with software related questions and provides remote support for advanced troubleshooting using LogMeIn Rescue. LogMeIn Rescue requires fully attended operations by the end user and does not allow for unattended support operations.

During application and support processes, the following criteria must be adhered to by you, the customer, and our resellers/integrators regarding to the collection of sensitive authentication data:

- Sensitive authentication data (pre-authorization) must only be collected when needed to solve a specific problem.
- Such data must be stored only in specific, known locations with limited access
- Collect only the minimum amount of such data that is needed to solve the specific issue
- Sensitive authentication data must be encrypted while stored
- Such data must be securely deleted immediately after use

Note: Aldelo support staff will never ask for nor collect sensitive authentication data for troubleshooting purposes.

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=l2|/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

For more information on generating TLS Certificates in Windows:

http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/maintain/featusability/c06iis.mspx

Application Versioning Methodology

The application versioning methodology for Aldelo® EDC is as follows: MAJOR.MINOR.BUILD

- A change in the first portion of the version number indicates a major change to the software
- A change in the second portion of the version number indicates a minor change to the software that may include security changes that affect PA-DSS
- A change in the third portion of the version number represents the internal build that does not include security changes that affect PA-DSS
- Wildcard elements are never used to represent security-impacting changes to the software

Chapter 5:
PA-DSS v 3.2 Requirements

PA-DSS v 3.2 Requirement	Requirement Fulfillment
1.1.4 Securely delete any magnetic stripe data, card verification values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations.	PIN data is never stored. Magnetic stripe data and verification codes are removed upon batching automatically by the software and are not permitted to exceed storage for more than 48 hours. Previous versions of the Aldelo® EDC application did not and could not be configured to store sensitive authentication data; therefore, a tool for removal of such data is not provided.
1.1.5 Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other sources received from customers, to ensure that magnetic stripe data card verification codes or values, and PINS or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only collected when necessary to resolve a problem. They must be encrypted while stored, and deleted immediately after use.	Sensitive authentication data is never stored as part of logged information. Aldelo agents will never collect sensitive data from customers for troubleshooting or debugging purposes.
4.1 At the completion of the installation process, the "out of the box" default installation of the payment application must log all user access (especially users with administrative privileges), and be able to link all activities to individual users.	All activities of all users are logged to the audit trail within Aldelo® EDC. All audit trails are automatically enabled and may not be disabled. Log files may be found at: C:\ProgramData\Aldelo\Aldelo EDC\Log\Eventlog.[current date].txt.
4.4 Payment application must facilitate centralized logging. Provide a description of which centralized logging mechanisms are supported, as well as instructions and procedures for incorporating the payment application logs into a centralized logging server.	All user activities are logged to the audit trail in Aldelo® EDC. To export the log, from the main screen of Aldelo® EDC, navigate to File Tab\Import & Export. Choose the data and settings to export from the Select Transform Options group box (make sure Audit Logs is selected) and click the navigation button . Navigate to your desired destination for the export file, create a name for it, and click the "Open" button to return to the Import & Export screen. Click the "Export" button to complete the file creation and exportation. For a detailed explanation, see the chapter titled Administrative Tasks in the Aldelo® EDC User Manual.

PA-DSS v 3.2 Requirement	Requirement Fulfillment
10.1 Implement two-factor authentication for all remote access to payment application that originates from outside the customer environment.	Aldelo® EDC does not allow remote access to the payment application that originates from outside the customer environment.
10.2.1 If payment application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes.	Payment application updates are not automatically sent to customers. Customers must obtain these from Aldelo, LP's secure website and the update installation is initiated by the user.