Slatwall 4.x.x

PA-DSS Implementation Guide

Version 1.0

ten24 Digital Solutions

Table of Contents

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. TEN24 DIGITAL SOLUTIONS 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 TEN24 DIGITAL SOLUTIONS 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.

About this Document

The purpose of this document is to describe the steps needed for a user to properly install Slatwall so that it will 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 3.1).

ten24 Digital Solutions advises its customers to deploy Slatwall and other ten24 Digital Solutions applications in a manner that adheres to the PCI Data Security Standard (v3.1). Along with deployment it is important that 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 improve security by enhancing intrusion detection and prevention, additional and more efficient system logging, and other general recommendations to secure networking environments. Some of these methods include enabling operating system auditing subsystems, utilization of a centralized logging server to handle system wide logging, disabling infrequently-used or frequently vulnerable networking protocols and implementing certificate-based protocols for access to servers by users and vendors.

Any time this document is updated it will be distributed to all customers and it will be available here: https://github.com/ten24/slatwall/blob/master/slatwall_implementation_guide.pdf

You must follow the steps outlined in this *Implementation Guide* in order for your Slatwall installation to support your PCI-DSS compliance efforts.

Executive Summary

Slatwall version 4.x.x has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 3.1. In order to validate our PA-DSS assessment, we worked together with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Trustwave Holdings, Inc
70 W. Madison St.
Suite 1050
Chicago, IL 60602

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. Alongside this information, this document provides best practices for installation, configuration, and ongoing management for use with Slatwall.

PCI Security Standards Council Reference Documents

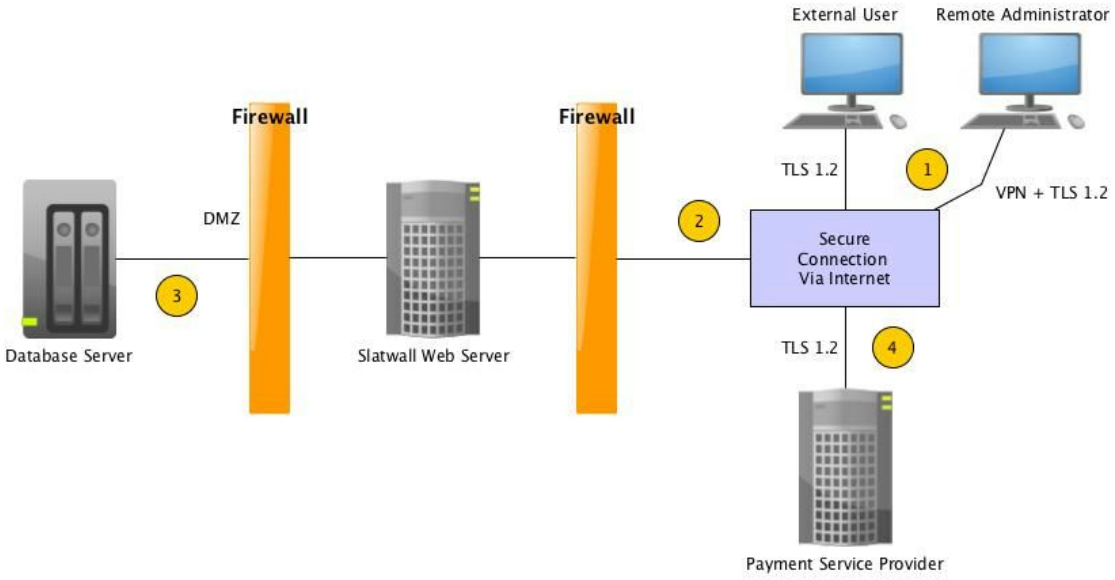
The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI-DSS, etc):

- Payment Applications Data Security Standard (PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
- Payment Card Industry Data Security Standard (PCI-DSS)
  https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Open Web Application Security Project (OWASP)
  http://www.owasp.org

Application Summary

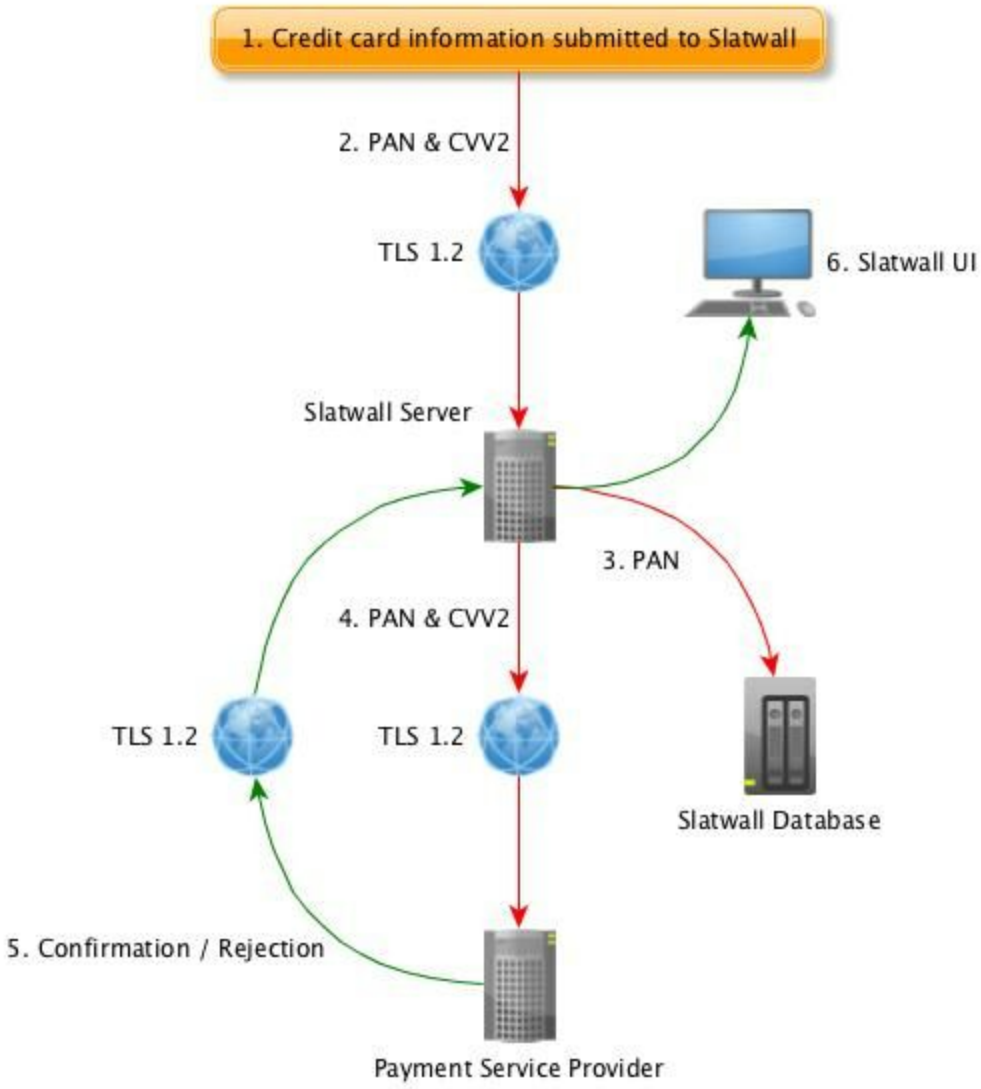
Application Name:	Slatwall
Application Version:	4.x.x
Application Description:	Slatwall is an extremely powerful and robust digital commerce management system. It is designed to work in a multitude of different business situations and helps to centralize your commerce activity by integrating into existing systems. Slatwall easily operates as an eCommerce shopping cart for your website but it can also do a lot more like Inventory Management, Vendor Ordering, Subscription Management, etc.
Application Target Clientele:	Midsize ecommerce businesses.
Database Software Supported:	MySQL, MS SQL, and Oracle
Other Required Third Party Software:	Coldfusion 9.0.1 + or Railo 4.0.1 +
Operating Systems Supported:	Windows, Mac OS X, and Linux
Description of Versioning Methodology:	Version numbers are in the form: Major.Minor.Patch

Typical Network Implementation



1. Remote Administrators and External Users connect to Slatwall via TLS 1.2. Remote Administrators also have the option of being able to connect to Slatawll via VPN.
2. Because Slatwall runs on a web Server it needs to connect to the internet. It is important though that all webservers have a firewall in place to protect this. It is also recommended that another firewall separates the web server from the rest of the network.
3. Slatwall stores client information and other data on a network database that is protected by another firewall.
4. Slatwall connects to a payment service provider via TLS 1.2 in order to process credit card information during transactions.

Dataflow Diagram



1. Credit Card Information is added to the order form by the user and submitted.
2. The PAN and CVV2 are submitted over TLS 1.2 to a server hosting Slatwall data.
3. If credit card storage is enabled, the PAN will be encrypted and stored in the database.
4. The PAN and CVV2 are then sent to a payment service provider for processing.
5. A confirmation or rejection is then sent form the payment service provider to Slatwall
6. The result is then displayed to the user via the Slatwall UI.

Difference between PCI Compliance and PA-DSS Validation

The Payment Card Industry (PCI) has created a set of security standards called PCI Data Security Standard (DSS) which is responsible for determining how cardholder information should be handled. This set of standards applies to all members, merchants, and service providers that store, process, transmit, or handle cardholder data.

PCI compliancy is the responsibility of the merchant and hosting provider in order to make sure that all components of the application system are secure. These components include the network device, host, and the parts of the application which are connected to a network segment that handles the cardholder data. Together, the merchant and hosting provider need to make sure that they cover all requirements of the PCI-DSS. These requirements include:

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

As the software vendor, ten24 Digital Solutions is held responsible for being “PA-DSS Validated.” PA-DSS is the standard against which Slatwall has been tested, assessed, and validated. This means that we have performed an assessment and complete a certification compliance review with Trustwave, to ensure that Slatwall adheres to industry standards when handling, managing and storing payment related information.

Considerations for the Implementation of Slatwall in a PCI Compliant Environment

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

- Sensitive Authentication Data requires special handling
- Historical Cardholder Data needs to be removed
- Key Management Roles & Responsibilities
- Log settings need to be compliant
- Admin personnel need to be properly trained an monitored
- PCI Compliant Wireless settings
- Never store cardholder data on internet-accessible systems
- PCI Compliant Remote Access
- Delivery of Updates in a PCI Compliant Fashion
- Data Transport Encryption
- PCI Compliant Use of Email

Sensitive Authentication Data Requires Special Handling

PCI Standards is important in ensuring that cardholder data and the integrity of the credit card industry as a whole are protected. Slatwall does not store magnetic stripe data, card validation codes, PINS, and PIN blocks. In Slatwall PAN is stored in following location:

Table – SwOrderPayment (Column: creditCardNumberEncrypted)

Table – SwAccountPayment (Column: creditCardNumberEncrypted)

Table – SwAccountPaymentMethod (Column: creditCardNumberEncrypted)

In order to comply with PA-DSS it is important that historical data is removed from previous versions of Slatwall. This is important to ensure PCI Compliancy.

We never store cvv2 data provided by customer

Purging of Cardholder Data

The following guidelines must be followed when dealing with cardholder data such as customers Personal Account Numbers (PAN) alone or along with any of the following: expiration date, cardholder name or service code:

- A customer defined retention period must be defined with a business justification.
- Cardholder data exceeding the customer-defined retention period must be purged.
- To purge cardholder data create script to update and null out PAN records from SwOrderPayment, SwAccountPayment and SwAccountPaymentMethod. Here is a sample script:
    - UPDATE SwOrderPayment
      SET creditCardNumberEncrypted = NULL
      WHERE DateDiff(day, SwOrderPayment.createdDateTime, getDate()) > 90
    - UPDATE SwAccountPayment
      SET creditCardNumberEncrypted = NULL
      WHERE DateDiff(day, SwAccountPayment.createdDateTime, getDate()) > 90
    - UPDATE SwAccountPaymentMethod
      SET creditCardNumberEncrypted = NULL
      WHERE DateDiff(day, SwAccountPaymentMethod.createdDateTime, getDate()) > 90

Cardholder Data Encryption Key Management

Slatwall does not store the PAN by default. If the merchant does decide to store the credit card number whoever, they will get encrypted with AES 128 bit encryption on a record by record basis using an unique salt that is stored in memory, not on disk. Only the last 4 digits of the PAN are stored in plain text so that it may be used for displaying purpose. If Slatwall's API is being used to submit cardholder data then any logging that is taking place on this communication needs to be written or configured so that it does not accidentally capture this data.

To re-encrypt the data with new key go to Config → Re-encrypt Database and follow the instructions on screen.

Access to Cardholder Data

By default only super users have access to PAN in Slatwall admin. In order to give access to PAN to personnel with legitimate business reason create a new permission group with specific access requirement and assign that permission group to required personnel. To create permission group go to Menu → Accounts → Permission Groups. There create a new permission group and check off the actions and fields that you want to grant access to this permission group.

Encrypted Storage of PAN

Card holder data is only stored in Database in encrypted format. There is no option for customer to store PAN in un-encrypted format.

Setup Secure Access

Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.

Setup Strong Access Controls

PCI-DSS requires that all user accounts with access to any system in the payment process must be unique and utilize a strong password. To be considered a unique user account, the account can only be associated to one user and cannot be controlled by any generic group accounts used by more than one user or process.

By default Slatwall assigns a unique id to all users and forces Admin accounts to use a complex password which get encrypted before being stored in the database. All authentication credentials are provided by Slatwall during the completion of the initial installation / administrator setup and also for any future changes to an account such as any changes to existing account settings, or changes that generate new accounts or recreate existing accounts. By default, Slatwall takes the following 8 items into consideration for Admin Accounts:

1. Slatwall must assign unique IDs for user accounts
2. Slatwall must NOT require or use any group, shared, or generic accounts or passwords.
3. Slatwall requires passwords to be changed at least every 90 days
4. Slatwall requires passwords must to be at least 7 characters and include both numeric and alphabetic characters.
5. Slatwall keeps password history and requires that a new password is different than any of the previous four passwords used.

6. Slatwall limits repeated access attempts by locking out the account after a max of 6 login attempts.
7. Slatwall sets the lockout duration to a minimum of 30 minutes or until an administrator logins in to unlock the account.
8. Slatwall requires the user log back into the system after 15 min of inactivity.

Log settings must be compliant

By default Slatwall's logging functionality meets PA-DSS compliancy. This logging is not configurable and may not be disabled. By disabling or subverting the logging functionality of Slatwall in any way will remove PCI-DSS compliancy.

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

10.2.1 All individual user accesses to cardholder data
10.2.2 All actions taken by any individual with root or administrative privileges
10.2.3 Access to application audit trails managed by or within Slatwall
10.2.4 Invalid logical access attempts
10.2 5 Use of Slatwall's identification and authentication mechanisms
10.2.6 Initialization of Slatwall audit logs
10.2.7 Creation and deletion of system-level objects within or by Slatwall

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

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

To remain PCI compliant, it is important that all log is kept in a centralized location. This helps to ensure that logging is handled efficiently and is easily available if needed. Slatwall Application logs are created in standard tab delimited format and can be read by any log analysis application. There are a variety of tools that can be used to help facilitate centralized logging such as Paper Trail and Splunk.

Slatwall Audit logs can also be exported by going to Tools Menu → Audits and then clicking on the Gear icon above the listing and then clicking export.

Properly Train and Monitor Admin Personnel

It is the responsibility of the merchant to institute proper personnel management techniques for allowing admin user access to sensitive data (cardholder data, site data, etc). Even some of the most secure systems can have leaks do to employee negligence or ignorance. Because

of this, it is important pay attention to whom you trust into your admin site and who you allow to have access to sensitive data and features.

PCI Compliant Wireless Settings

If the merchant installs Slatwall in a wireless environment (such as a front desk laptop connecting to a wireless router which connects to a server that hosts Slatwall) it is important that the merchant remains compliant with their wireless settings per PCI Data Security Standard.

PCI dictates that a firewall must be installed between any wireless networks and systems that store card data. All traffic coming through this firewall must be denied unless it is required for business purposes.

Requirements:

- 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 are updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)
- Industry best practices are used to implement strong encryption for the following over the wireless network in the cardholder data environment:
    - Transmission of cardholder data
    - Transmission of authentication data
- Wired Equivalent Privacy (WEP) is no longer an acceptable security measure over wireless networks and its use will result in a PCI non compliance.

Failure to follow these guidelines during implementation with wireless technology and Slatwall will result in PCI non-compliance.

Services and Protocols

In order to reach PA-DSS compliancy it is important that Slatwall does not require the use of any insecure services or protocols. The only protocol that Slatwall specifically needs is HTTPS. It is recommended that you disable all weak ciphers on server and only transmit secure data over TLS 1.2 or higher.

Never Store Cardholder Data on Internet-Accessible Systems

Never store cardholder data on Internet-accessible systems. An example of this would be utilizing a server for both your web server and your database server. Cardholder data storage components require a higher level of protection than public-facing application components. If

cardholder data is located within the DMZ, it is easier for an external attacker to access this information, since there are fewer layers to penetrate. For the same reason, web servers should never be stored on the same server as the data storage component. If a malicious individual were able to compromise an account on the web server, they could also have compromised the cardholder database with no additional effort required.

Create a separate network zone for database server with no publicly accessible open ports and only open access for required database port from web server to the database server. Check the network diagram in this document for reference.

PCI Compliant Remote Access

The PCI standard requires that if users are given remote access to the payment processing environment then a two-factor authentication mechanism should be required in order for them to gain access. This means that at least two of the following authentication methods should be used:

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

Remote access also needs to be implemented securely by doing the following:

- 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.
- Enable encrypted data transmission.
- Enable account lockout after a certain number of failed login attempts.
- Establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.
- Enable logging functionality.
- Restrict access to customer environments to authorized integrator/reseller personnel.
- SSH, VPN, or TLS 1.2 or higher is needed for encryption of administrative access

PCI Compliant Delivery of Updates

In order to meet PA-DSS compliancy ten24 constantly delivers necessary updates and patches in a timely manner. These updates are easily downloadable through the update functionality that is built into Slatwall.

1. Backup your Site Files & Database
2. Log into the admin
3. Slatwall requires passwords to be changed at least every 90 days
4. Navigate to Tools / Help >> Update Slatwall

5. You will see the current version you are on as well as the available versions to update to
6. From the dropdown you can select either the latest stable release, or latest bleeding edge release. In addition you can also define a custom branch on GitHub that you would like to update to by typing the name in
7. Select the appropriate option and click the "Update" button
8. Be patient because this can take several minutes. Once the action is complete you should be redirected to the main dashboard with an "Update Successful Message"
9. You can verify that your version of Slatwall was updated by navigating to Tools / Help >> About and reviewing the version number

All updates are heavily tested prior to them being released in order to sure proper functionality of Slatwall. It is the responsibility of the end user to download/update Slatwall in a timely manner once a new update has been provided. Updates are downloaded from github over https connection.

Data Transport Encryption

In order to remain PCI and PA-DSS compliant it is required that strong encryptions are used (at least 128 bit encryption strength) at the transport layer or at the data layer during transmission over to a public network. In order to utilize proper data transport encryption with Slatwall, the merchant needs to make sure that all data transfers are done over https instead of http. This should ensure that data being transported is properly encrypted. Verify to make sure only trusted certificates and key are in use and all non supported transmission protocols are disabled. Here is a sample tool to test your SSL connection: https://www.ssllabs.com/ssltest/

Non Console Access

Encrypt all non-console administrative access with strong cryptography, using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Note: Clear-text protocols such as Telnet or rlogin must never be used for administrative access.

PCI Compliant Use of End User Messaging Technologies

Slatwall by default does not allow or provide the capabilities for a user to send sensitive credit card information such as PANs through the use of messaging technology such as e-mail and instant message.

Maintaining an Information Security Program

On top of the security recommendations provided earlier in this documentation, it is important to stay knowledgeable of the best ways to protect the organization and sensitive card data. In order to do this, it is important to maintain a comprehensive approach to assessing and maintaining the security compliance of the environment.

This is a basic plan that merchants should follow in order to implement a security program:

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

Secure Procedures for Troubleshooting customer issues

It is always recommended to use secure procedures and practice when troubleshooting customer issues. Secure procedures and practice includes, but not limited to, the following:

- Never send sensitive credit card information such as PAN or password through the use of messaging technology such as e-mail and instant message.
- Never store or send CVV in any written communication
- Always use VPN or secure tunnel when accessing customer PCI environment
- Always login as an authenticated user to troubleshoot application issues

Initial Setup & Configuration

If assistance is needed with either installing, configuring, or locking down Slatwall please review the documentation at: http://docs.getslatwall.com/

Help can also be found on the Google Groups at:
https://groups.google.com/forum/#!forum/slatwallecommerce

Regardless of whether Coldfusion or Railo is being used, it is important that during installation the server gets locked down in order to improve security. The following links will help with how this task is accomplished.

Coldfusion:
http://www.adobe.com/content/dam/Adobe/en/products/coldfusion/pdfs/91025512-cf9-lockdownguide-wp-ue.pdf

Railo:
https://github.com/getrailo/railo/wiki/Railo-Lockdown-Guide

Other Considerations

Application does not explicitly use any port to connect to database over the network. A datasource is created in the Application Server that is being used (Adobe ColdFusion or Railo) and application communicates using that datasource. Typically the datasource is setup to communicate over the default ODBC port (1433 for SQL Server or 3306 for MySQL etc.).

Only required service for application is Application Server (Adobe ColdFusion, or Railo).

Required ports to run the application is 80 and 443

Version Methodology

The versioning methodology for Slatwall is X.X.X where the components are as follows:

1st digit - This is the major version number and would represent a significant enhancement or functionality change. This includes changes affecting cardholder data security or PA-DSS compliance.

2nd digit - This is the minor version number and would represent a minor enhancement to the application. This does not contain changes affecting cardholder data security or PA-DSS compliance.

3rd digit - This is the patch version number. When this is incremented, the release could involve defect patches. This digit would represent an internal non-compliance related change.

All elements are using numeric characters.

Change History

11/13/2014 - Chris Kundrat

06/03/2015 - Sumit Verma

09/04/2015 - Sumit Verma - Updated based on PA DSS standards requirement

02/24/2016 - Sumit Verma - Updated versioning info

03/12/2016 - Sumit Verma - Updated based on PA DSS QA feedback

03/24/2016 - Sumit Verma - Updated About this document, Non-Console Access and DMZ instruction.

04/04/2016 - Sumit Verma - Added instruction on how to export audit logs