PA-DSS

Implementation Guide

Table of Contents

- Revision History
- PA-DSS Requirements for Compliance
  - Implementation Guide Purpose
  - Implementation Guide Target Audience and Distribution
  - Implementation Guide Maintenance Policy
- Security Implementation Requirements
  - Remove historical sensitive authentication data
  - Delete any sensitive authentication data gathered for troubleshooting
  - Delete/Purge Cardholder Data after Customer-Defined Retention Period
  - PAN Value Management
  - CardHolder Data Encryption Key Management
  - Set up Strong Access Controls
  - Log Settings Must be Compliant
  - Application Versioning Methodology
  - PCI-Compliant Wireless Settings
  - Services and Protocols
  - Never store cardholder data on internet-accessible systems
  - PCI Compliant Remote Access
  - Data Transport Encryption
  - PCI Compliant Use of End User Messaging Technologies
  - Non console administration

Revision History

Date of Change	Version	Responsible	Summary of Change
January 22nd 2015	1.0	Cássio Corrêa	Initial
June 10th 2015	1.1	Cássio Corrêa	Removed unnecessaries points for the PA-DSS Standard version 3.1
July 2nd 2015	1.2	David Kelleher	Proof read and update for English content
July 6th 2015	1.3	Cássio Corrêa	Added Purpose, Target Audience and Maintenance Policy sections.
July 6th 2015	1.4	David Kelleher	Proof read and update for English content for revision 1.3
July 21st 2015	1.5	Cássio Corrêa	Replaced table format for text only
August 11th 2015	1.6	Cássio Corrêa	Applied TrustWave review corrections

PA-DSS Requirements for Compliance

Implementation Guide Purpose

This document is provided as an Implementation Guide to instruct merchants, resellers and integrators on secure product implementation and to document the secure configuration specifics mentioned throughout the PCI PA-DSS requirements documentation. The document delineates vendor, reseller/integrator, and customer responsibilities for meeting all compliance requirements. It is highly recommended that the vendor and reseller/integrator familiarize themselves and adheres to PCI-DSS standards.

Implementation Guide Target Audience and Distribution

This document is intended for merchants, resellers and integrators who place CloudWalk payment applications in service for processing credit card and debit card transactions.

The typical users, resellers and integrators include but are not limited to:

- Payment Systems Integrators;
- Payment Processors;
- Banks.

The Implementation Guide is distributed to integrator and resellers at the event of purchasing the CloudWalk product. The document is available on the CloudWalk Developer's portal for merchants access.

Implementation Guide Maintenance Policy

This Implementation Guide is subject to annual review and maintenance updates, which address the changes implied by new revisions of the PCI DSS and PCI PA-DSS standards as well as any software updates related to improvement of the security features in CloudWalk products.

Security Implementation Requirements

Remove historical sensitive authentication data

Previous versions of CloudWalk payment application do not store sensitive authentication data therefore is no need manual removal of historical data.
For non-CloudWalk application the customer must ensures that all historical data is deleted before the update of the application to be compliant with the PCI-DSS requirements.

Delete any sensitive authentication data gathered for troubleshooting

CloudWalk's application does not store any sensitive authentication data for any reason.

If the client need to store sensitive data the following guidelines must be attended when dealing with sensitive authentication data (swipe data, validation values or codes, PIN or PIN block data):

- Sensitive authentication data must only collected when needed to solve a specific problem;
- Such data must be stored only in specific, known locations with limited access;
- Only collect a limited amount of such data as needed to solve specific problem;
- Sensitive authentication data must be encrypted while stored;
- Such data must be securely deleted immediately after use.

Delete/Purge Cardholder Data after Customer-Defined Retention Period

The payment application does not store any historical data containing full cardholder data and do not store any sensitive authentication data. We do not recommend the storage of full cardholder data but if the client provide a service that need to store the cardholder data the following guidelines must be attended when dealing with cardholder data(PAN alone or with any of the following: expiry date, cardholder name or service code):

- After exceeding the customer-defined retention period the cardholder data must be securely deleted;
- All cardholder data must be securely delete when no longer required for legal, regulatory, or business purposes.

PAN Value Management

The CloudWalk payment application automatically truncates the PAN value in the format: '****** **** **** 1234**' in the storation. It's make the value unreadable anywhere it is stored thus only this truncated PAN can be displayed. CloudWalk payment application does not provide option to be possible to display the full PAN value or change the PAN value truncation process.

When dealing with the PAN value the following guidelines must be followed:

- The PAN must be render unreadable anywhere it is stored;
- By default on all display the PAN is truncated;
- Only personal with a legitimate business need can see the full PAN.

CardHolder Data Encryption Key Management

The CloudWalk payment application secure management of encryption keys is ensured with the use of approved PTS devices. The use of approved PTS devices is mandatory.

To handle the encryption keys management the following requirements must be attended:

- Strong cryptographic keys must be created;
- Secure distribution of the keys must be ensured;
- Secure storage of the cryptographic keys must be ensured;
- After the end of their cryptoperiod cryptographic keys must be changed;
- Retirement or replacement of the keys when the integrity of the keys have been weakened or are suspected of being compromised;

- Split knowledge and dual control for any clear-text cryptographic key management;
- Prevent unauthorized substitution of cryptographic keys.

Set up Strong Access Controls

CloudWalk payment application **do not provides or manage** a user system. The CloudWalk application commands are limited to payment processing functions only. No direct access or changes to the CloudWalk software or memory are implemented.
PCI DSS requires that all systems in the payment processing environment must protected through use of unique users and complex passwords according to the following guidelines:

- Does not use (or require the use of) default administrative accounts for other necessary software (for example, the payment application must not use the database default administrative account);
- Enforce the changing of all default application passwords for all accounts that are generated or managed by the application, by the completion of installation and for subsequent changes after installation. This applies to all accounts, including user accounts, application and service accounts, and accounts used by the vendor for support purposes;
- Assigns unique IDs for user accounts;
- Employs at least one method to authenticate all users;
- Does not require or use any group, shared, or generic accounts and passwords;
- Requires that passwords meet the following:
    - Require a minimum length of at least seven characters;
    - Contain both numeric and alphabetic characters.
- Requires changes to user passwords at least every 90 days;
- Keeps password history and requires that a new password is different than any of the last four passwords used;
- Limits repeated access attempts by locking out the user account after not more than six logon attempts;
- Sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID;
- Requires the user to reauthenticate to re-activate the session if a payment application session has been idle for more than 15 minutes.

Log Settings Must be Compliant

Since CloudWalk payment does not have user management, logs related to user interaction are not possible to be registered. The customer can access the logs related to the communication between the terminal and the CloudWalk server.

A customer that want to access the log functionality must send an email to CloudWalk support team to request access and instructions to use this functionality. That process is to generate an api token for the customer. Regardless of whether the customer request access the log events are always recorded. Allowing the user to access old logs when needed.

Application Versioning Methodology

CloudWalk payment application version has the format WW.XX.YY and is assigned according to the following rules:

- The first two digits "**WW**" represent the version when you have a **High Impact** change;
- The next two digits "**XX**" represent the version when you have a **Low Impact** change;
- The "**YY**" digits are used to indicate the use of **WILDCARDS.** It should be used when you have a **No Impact** change.

The characters used to define versions are the **numeric values 0-9 integers**. To separate the numerical values of the versions must be used the separator " **.** ".

PCI-Compliant Wireless Settings

CloudWalk only uses network over private APN network.
If the customer implement a wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed:

- Encryption keys must be changed from default at installation, and must be changed anytime with knowledge of the keys leaves the company or changes positions. Refer to wireless device manufacturer's documentation for change instructions;
- Default SNMP community strings on wireless devices must be changed. Refer to wireless device manufacturer's documentation for change instructions;
- Default passwords/passphrases on access points must be changed. Refer to wireless device manufacturer's documentation for change instructions;
- Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks. Refer to wireless device manufacturer's documentation for change instructions. Firmware updates should be performed for any wireless networking device that is capable, including routers, access points, gateways and switches;
- Other security related wireless vendor defaults, if applicable, must be changed. Refer to wireless device manufacturer's documentation for change instructions. Changes to vendor defaults settings should be performed for any wireless networking device that is capable, including routers, access points, gateways and switches.

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.
Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.

Services and Protocols

CloudWalk does not require nor permit the use of any insecure service or protocols. The payment application works isolated in an embedded point of sale device. CloudWalk only request the use of private APN GPRS connection.

Never store cardholder data on internet-accessible systems

CloudWalk does not require any external storage or on any other Internet system outside the boundaries of the secure storage embedded in the terminal. Cardholder data must never be stored in internet accessible systems (e.g, web server and database server must not be on same server).

PCI Compliant Remote Access

The CloudWalk application **does not** support remote access to the terminal.

If users may need to use third-party remote access software, special care must be taken. In order to be compliant, every such session must be encrypted with a strong encryption method (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). 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 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 PCI-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 PCI-DSS Requirement 3.1.9 through 3.1.10);
- Establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed;
- Enable the logging function;
- Restrict access to customer environments to authorized integrator/reseller personnel.

Data Transport Encryption

During transmission over public networks CloudWalk ensure the secure transmission encrypting the track2 data using **triple DES** algorithm with key size of 16 bytes, the pin block is encrypted using the **DUKPT** key management scheme with the **triple DES** algorithm. The client does not need or can influence in the data encryption. Others sensitive data are not transmitted over public networks.

PCI Compliant Use of End User Messaging Technologies

CloudWalk not allow or facilitate the sending of PANs via any end user messaging technology (for example, email, instant messaging, and chat).
If the user may need to send PANs by end-user messaging technologies the PAN must be always render unreadable or encrypted by a strong cryptography.

Non console administration

Although CloudWalk 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 SSLV3/TLS 1.0 or higher for encryption of this non console administrative access.