

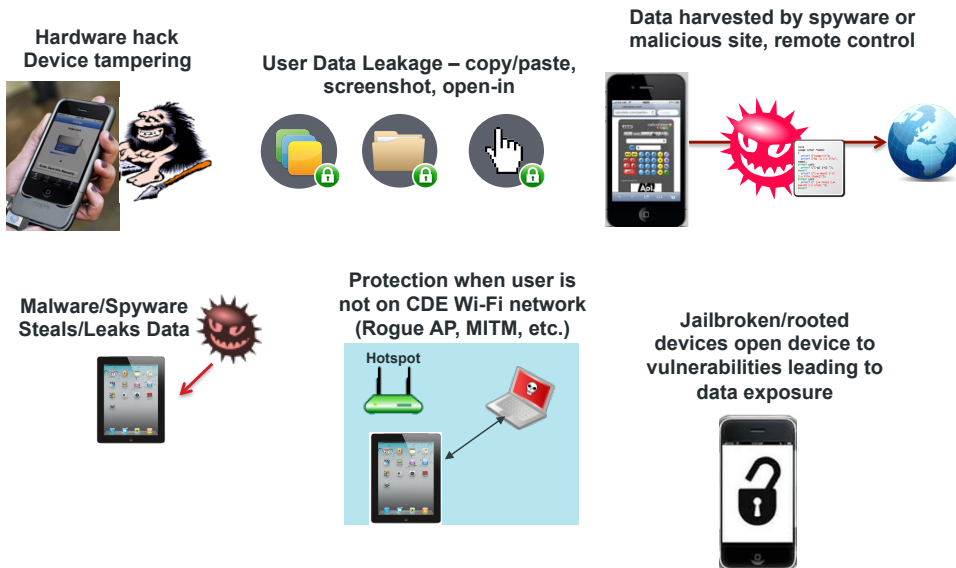
PCI Compliance and Mobile Devices

The Payment Card Industry (PCI) Security Standards Council has released the Data Security Standards (DSS) version 3.0 outlining revised requirements for payment data security, effective January 1st, 2014. Merchants and Service Providers that store, process, or transmit customer payment card data must adhere to the revised outlined requirements. Additionally, the PCI Council released the PCI Mobile Payment Acceptance Security Guidelines 1.0, which focuses on Mobile POS (Point-of-Sale) devices.

Many companies are moving to mobile to increase employee productivity, improve customer experience, and increase sales. As a result, the revised requirements in PCI DSS 3.0 include new requirements for mobile devices used in the Cardholder Data Environment (CDE) as well as Mobile POS. This document outlines best practices for achieving compliance with these mobile requirements and fortifying your mobile strategy. This is meant only as directional guidance, and each organization should seek the appropriate validation from their preferred PCI QSA (Qualified Security Assessor).

Payment card network mobile attacks

Attacks on payment card networks are broad, extensive, and sophisticated, as demonstrated by a recent breach at a retailer exposing more than 70 million credit and debit cards. These attacks can include:



415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com



- Interception – MITM (Man-in-the-Middle) attacks capturing data-in-transit
- Malware – Malware, keyloggers, and spyware capturing and stealing data from POS devices at the point of transaction
- Jailbreak/Root – Devices open to vulnerabilities leading to data exposure
- Data Leakage – Users copying sensitive data through copy/paste, screenshot, and open-in
- Unauthorized logical access – Brute force and dictionary attacks on mobile devices

Meeting PCI DSS 3.0 Mobile Requirements

This section describes the most important PCI DSS 3.0 mobile requirements and how MobileIron can address them.

2.2.4 Configure system (mobile device) security parameters to prevent misuse. MobileIron lockdown and restriction policies disable unnecessary services and features to prevent abuse. Additionally, strong password device lock policies can be enforced and monitored to prohibit brute force and dictionary attacks.

2.3 Encrypt all non-console administrative access using strong cryptography. MobileIron delivers strong authentication for administrative access from mobile devices over Wi-Fi, VPN, or AppTunnel. MobileIron can leverage either its built-in CA (Certificate Authority) or integration with a 3rd party CA to automatically deliver an authentication certificate with the configuration.

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

MobileIron enables strong encryption for wireless authentication and transmission with certificates that can be automatically deployed to the mobile devices.

8.3 Incorporate two-factor authentication for remote network access originating from the outside the network by personal and all third parties. MobileIron can additionally provide certificates to the mobile devices for use with the VPN or MobileIron AppTunnel, thus eliminating brute force attacks against remote access accounts and meeting two-factor authentication requirements.

10.5.4 Logs for external-facing technologies are written onto a secure, centralized, internal log server or media. MobileIron audits mobile device activity and centrally stores this log information to provide reporting on PCI policy violations.

12.3 Develop usage policies for critical technologies (mobile devices) and define proper use of these technologies. MobileIron provides the ability to prohibit use of certain devices and other technologies, while also requiring strong authentication through the use of certificates. Additionally, the MobileIron reporting and dashboard delivers an accurate inventory and device labeling to identify devices that are out of compliance.

Mobile POS (Point-of-Sale)

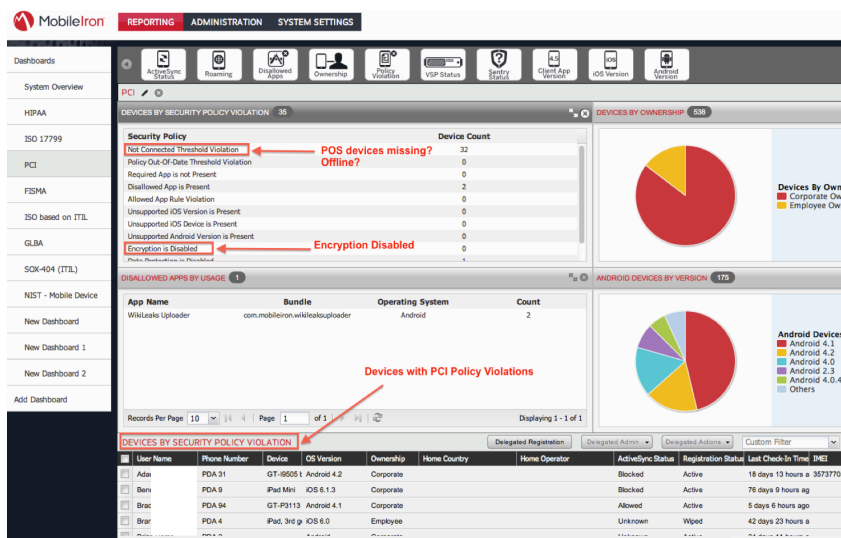
MobileIron allows PCI customers to achieve compliance with all of **PCI Mobile Payment Acceptance Security Guidelines 1.0** for Mobile POS (mPOS) devices.

Objective 1 - Prevent account data from being intercepted when entered into a mobile device. To ensure the account data entry channel is secured against injections and interception, MobileIron can identify malicious application and subsequent jailbreak and rooting activities. Additionally, MobileIron's automated quarantine action can wipe the POS App and its data in order to mitigate credit card exposure.

Objective 2 - Prevent account data from compromise while processed or stored within the mobile device. MobileIron controls copy/paste, screenshot, file sharing, and other possible data leakage vectors to prevent unintentional or side-channel data leakage.

Objective 3 - Prevent account data from interception upon transmission out of the mobile device. To mitigate MITM (Man-in-the-Middle), sniffing, and other data-in-transit attacks, MobileIron can deliver and enforce strong encryption and authentication credentials.

Objective 4 – Address security measures essential to the integrity of the mobile platform and associated application environment. MobileIron exceeds the recommendation to alarm when root or jailbreak actions have been taken. When MobileIron detects the rooting or jailbreaking of a device, the automated quarantine can block network access and perform a selective wipe by removing the POS application and its data from the device. This quarantine also keeps the device under management so that it can still be managed and located. Additionally, MobileIron lockdown and restriction policies provide further assurances for mobile device integrity, while alerting and reporting identify for the administrator any devices that fall out of PCI compliance.



The screenshot displays the MobileIron management console interface. At the top, there are navigation tabs for REPORTING, ADMINISTRATION, and SYSTEM SETTINGS. The main content area is divided into several sections:

- System Overview:** A sidebar on the left lists various dashboards and reports.
- PCI Compliance:** A central section titled "DEVICES BY SECURITY POLICY VIOLATION" shows a table of violations. Red arrows point to "Not Connected Threshold Violation" (32 devices) with the note "POS devices missing? Offline?" and "Encryption is Disabled" (1 device).
- Deviations:** A table below shows "DISALLOWED APPS BY USAGE" with one entry: "App Name: WillLeak Uploader, Bundle: com.mobilityiron.willleakuploader, Operating System: Android, Count: 2". A red arrow points to this entry with the note "Devices with PCI Policy Violations".
- Charts:** Two pie charts are present: "DEVICES BY OWNERSHIP" (Corporate Own vs Employee Own) and "ANDROID DEVICES BY VERSION" (Android 4.1, 4.2, 4.0, 2.3, 4.0.4, Others).
- Table:** A table at the bottom lists individual devices with columns for User Name, Phone Number, Device, OS Version, Ownership, Home Country, Home Operator, Active/Sync Status, Registration Status, and Last Check-In Time.

Conclusion:

Any business accepting credit cards on mobile devices must determine how to comply with the PCI DSS (Data Security Standard) 3.0 requirements while also maintaining the overall security of their mobile devices. MobileIron provides a comprehensive suite of options to allow companies to meet all of the PCI mobile requirements. MobileIron is also a participating organization in the PCI Security Standards Council. As a participating organization, MobileIron participates in Special Interest Groups (SIGs) and the PCI Mobile Task Force. This provides MobileIron the opportunity to represent our customers' voices at meetings as well as influence the published requirements.



PARTICIPATING ORGANIZATION