Mobile Device Management

(Check out the Demo or Sign up for a FREE 14 Days Trial)

Smartphones and tablets are generally delivered with preloaded consumer apps and are not ready for business use. This is where Mobile Device Management (MDM) software comes into play. MDM software erases the device, configures it, and makes it enterprise ready.

Provisioning Android Devices

Smartphones and tablets running the Android operating system are now delivered with the Android Enterprise framework built-in. MDM software such as Codeproof uses the Android Enterprise framework to remotely secure and manage these devices. To install MDM software, devices already in use are factory reset, then a QR code is scanned to load the MDM. This process erases all the preloaded apps and installs only IT administrator approved apps. This makes the device more secure and productive. One-time physical access to the device is required to load and set up MDM. From that point forward the device can be remotely managed through a cloud-based dashboard.

Provisioning Apple Devices

Apple devices can be provisioned with MDM software such as Codeproof using Apple Business Manager (ABM). ABM verifies ownership of the device and enables full remote management (also known as supervision mode). With ABM, MDM can be installed over the air without the need for physical access to the device. When the device is powered on and connected to a cellular data or Wi-Fi network it connects to the ABM server, and MDM is downloaded and installed on the device automatically. The device user cannot disable or otherwise stop MDM installation.

Common MDM Usage Scenarios

- **Application Deployment and Update**
  Application deployment and update is a cumbersome task for an organization with many devices. Using the MDM dashboard, the IT Administrator can approve the installation of public apps or upload and install enterprise developed and approved apps with a single set of commands. MDM can be used manually or automatically to perform app updates.

- **Kiosk Mode**
  Using MDM, devices can be configured for "kiosk mode" in which a very limited number of apps are loaded on the device, and the device is otherwise locked in other uses – no preloaded or sideloading of apps. Kiosk mode is frequently used for scenarios such as tablets used as payment terminals by retailers or for conference room scheduling in an office building. Such use scenarios often include wallpaper and lock screen customizations with organization logos.

- **Passcode Policy Enforcement**
  Using MDM, an IT administrator can quickly enable enterprise-grade passcode authentication on the device. This feature is available for both Android and iOS devices.

- **Lost or Stolen Device Tracking**
  MDM software typically includes various data loss prevention (DLP) tools, including the ability to remotely:
  - Lock a device with a new passcode
  - Locate a device
  - Data wipe the device

Privacy and Compliance

Many privacy and compliance regulations must be adhered to by organizations that make significant use of enterprise mobility capabilities for business functions, particularly with legal privacy mandates in industries such as healthcare. The MDM platform enables compliance with various privacy and security regulations and standards, including HIPAA, GDPR, ELD, FIPS, PCI, CJIS, etc.

Asset Inventory

MDM software can be used by an IT administrator to generate reports such as device inventory, apps installed, data usage, location history, and many others. It allows a better organization, usage monitoring, and management of mobile devices, improving security and employee productivity and reducing overall IT expenditures.

Other Key Features

Many MDMs include features such as data usage monitoring, contact management, and call blocking.

FAQ

What is Android Enterprise?

Android Enterprise is Google's enterprise grade remote device management framework. It is free and part of the Android operating system. MDM vendors use Android Enterprise APIs to secure and manage devices.

What Apple Business Manager?

Apple Business Manager (ABM) is a free device assignment portal for business customers who purchase Apple devices. Using ABM, customers can remotely assign MDM profiles to company owned Apple devices (i.e., zero-touch). Before purchasing Apple devices, organizations should establish an ABM account and get an ABM ID number. This allows remote management of devices using MDM out of the box.

How can I purchase MDM software?

Business customers can purchase MDM software through mobile carriers or directly from MDM software vendors. Most MDM software is available as a cloud-based subscription paid on a monthly or annual basis. MDM software is carrier and network agnostic. It is highly recommended that MDM be loaded at the time of device purchase, avoiding the need to take physical possession of the device to perform a factory reset and MDM installation at a later date.