

MDM – Mobile Device Management

Copyright © 2015 1Mobility

All Rights Reserved.

The information contained in this document is confidential. It is suitable only for use for its intended purpose and may not be disclosed to third parties or modified/changed without express written agreement of 1Mobility.

This document is the property of and is proprietary to 1Mobility. It shall not be duplicated nor used, in whole or in part, for any purpose other defined in the agreement between 1Mobility and Customer.

1Mobility believes the information in this publication is accurate as of its publication date; such information is subject to change without notice.

About 1Mobility

1Mobility has successfully established itself as a global company, offering cloud based, internationalized and scalable Enterprise Mobility Management (EMM) solution that monitors, manages and supports mobile devices across platforms (Android, iOS, BlackBerry, Windows), service providers and manufacturers.

1Mobility has a team of dedicated and talented professionals with over 8 years of innovative software development believes that “today, Enterprise Mobility though not mandatory, is a fact of business life for various obvious reasons like increased productivity, cost savings, competitive advantage and better customer engagement.”

Having serviced industries like Banking, Financial Services, Insurance, Technology, Education, Pharmaceutical, Communication & Media and Government and initial focus on the emerging markets, 1Mobility provides affordable solutions either cloud based or privately installed, enabling over-the-air distribution of mobile applications, configuration settings and security policies to corporate owned or employee owned (BYOD) devices through a central web console. No matter what type of organization it is, 1Mobility has affordable solutions and services for all, be it initial, advanced or matured enterprise mobility.

1Mobility offers following solutions

- Enterprise Mobility Management (EMM) through consulting, development and managed services
- Data Loss Prevention (DLP) of Mobile Data
- Compliance enforcement and monitoring
- Containerization
- BYOD Management



For further information, please visit the 1Mobility website at <http://www.1Mobility.com>

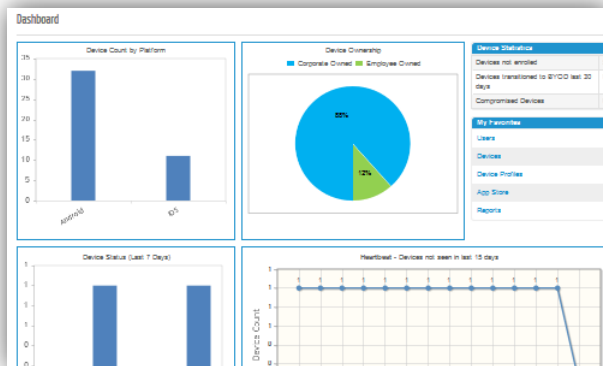
Mobile Device Management

Device Support

- ▶ 1Mobility supports the following Mobile OS / Platforms:
 - Apple iOS: 4+ (iPhone, iPad, iPod touch)
 - Android: 2.3+
 - Blackberry: between 5 & 7
 - Windows Phone 8+

Enroll

- ▶ **Device Ownership:** Enroll employee, corporate owned devices in your enterprise environment
- ▶ **Device Registration:** Enable IT to register existing devices one by one or in bulk. End users can add their own devices through DIY Portal, subject to approval by the administrators
- ▶ **User Authentication:** Authenticate users via 1Mobility or directory-based authentication (AD/LDAP)
- ▶ **EULA:** Create custom End User License Agreements (EULAs) for various groups and locations and mandate acceptance during enrollment
- ▶ **Restrictions:** Set up restrictions to block devices based on platform, version, etc. Non-compliant devices are not allowed to be enrolled.

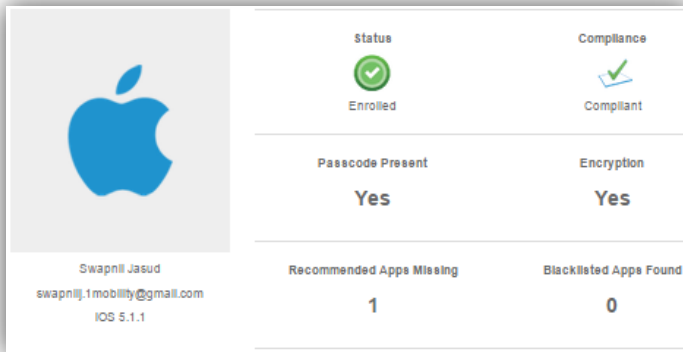


Secure

- ▶ **Password:** Require a device passcode with configurable complexity, length, lock and wipe rules
- ▶ **Encryption:** Enforce full device and storage card encryption
- ▶ **Restrictions:** Lock down an end user's ability to use specific device features, apps and web browsing
- ▶ **Compliance:** Set up rules for non-compliant activities and compromised devices with automated responses

Configure

- ▶ **Profiles:** Configure device settings and user credentials for accessing enterprise resources
- ▶ **Certificates:** Integrate with certificates for secure distribution and management of profiles
- ▶ **Accounts:** Provision access to corporate Email, Calendar, Contacts, Wi-Fi and VPN networks
- ▶ **Applications:** Distribute and manage internal/public/purchased apps via the App Catalog
- ▶ **Content:** Distribute corporate documents and secure mobile access using Content Locker

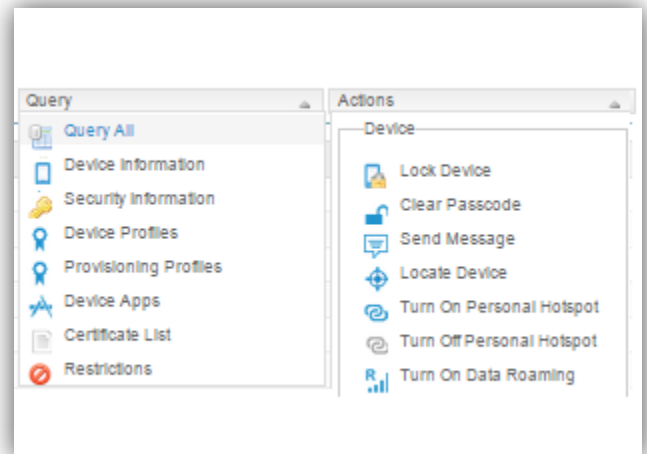


Monitor

- ▶ **Compliance Alerts:** Create email alerts with automated compliance rules to notify IT administrators and/or end users. Set up rules that define non-compliant events/activities and automated responses
- ▶ **Compliance Actions:** Automated compliance checks and their corresponding actions to secure data. For example, Delete Corporate Data, De-enroll Device etc.
- ▶ **Reporting:** On demand detailed compliance reports. Export device data to in CSV format to be consumed by other enterprise tools.

Manage

- ▶ **Queries:** OTA on-demand and automated capturing of device information.
- ▶ **Updates:** Real time broadcast of applicable security policies, compliance requirements, applications and configurations.
- ▶ **Commands:** Send commands on-demand or automated to devices to request info, lock, wipe a device and much more.
- ▶ **De-enrollment:** De-enroll devices from your environment, remove corporate data and wipe device.



Performed On	Command(s)	Status
05-Jan-15 03:25 PM IST	Managed Application List	✔ Success
05-Jan-15 03:25 PM IST	Device Apps	✔ Success
05-Jan-15 03:25 PM IST	Security Information	✔ Success
05-Jan-15 03:25 PM IST	Device Information	✔ Success
05-Jan-15 02:28 PM IST	Certificate List	✔ Success
05-Jan-15 02:28 PM IST	Device Lock	✔ Success
05-Jan-15 01:00 PM IST	Managed Application List	✔ Success
05-Jan-15 01:00 PM IST	Device Apps	✔ Success
05-Jan-15 01:00 PM IST	Device Information	✔ Success

Support

- ▶ **Messaging:** Send a customized message to one or more devices troubleshooting instructions.
- ▶ **Remote Diagnostics:** Perform remote diagnostics to identify device issues in real-time.
- ▶ **Remote Control:** Take remote control of an end user's device for troubleshooting via Team Viewer.
- ▶ **Do-It-Yourself:** Enable end users to clear their passcode, locate their device and more via DIY portal a.k.a. self-service portal.