PRODUCT SHEET

Advantal™

ADVANTAL'S MDM SOLUTION

Advantal's Mobile Device Management (MDM) Solution allows IT administrator to control, secure and enforce policies on smartphones or tablets. The intent of MDM is to optimize the functionality and security of mobile devices within the organization while simultaneously protecting the local network.

Advantal's Mobile device management relies on endpoint software called an MDM agent and an MDM server that will be installed in the data center.

Administrator's configure policies through the MDM server's management console, and the server then pushes those policies over the air to the MDM agent on the device. The agent applies the policies to the device by communicating with application programming interfaces (APIs) built directly into the device operating system. The document covers the features of the Mobile Device Management Solution.

- MDM Agent will start in background immediately after completing the installation. Application will also start automatically on phone restart.
- MDM Agent will be activated over the air.
- MDM Agent will start monitoring for the SIM card status in background.
- MDM Agent application will be installed on the devices. It will be an APK file for the Android devices. This application can be remotely pushed on devices via OTA.

MOBILE APPLICATION MANAGEMENT

- Create your own enterprise-authorized app catalog.
- Comprehensively manage both enterprise and Store (free/paid) apps as well as app licenses.

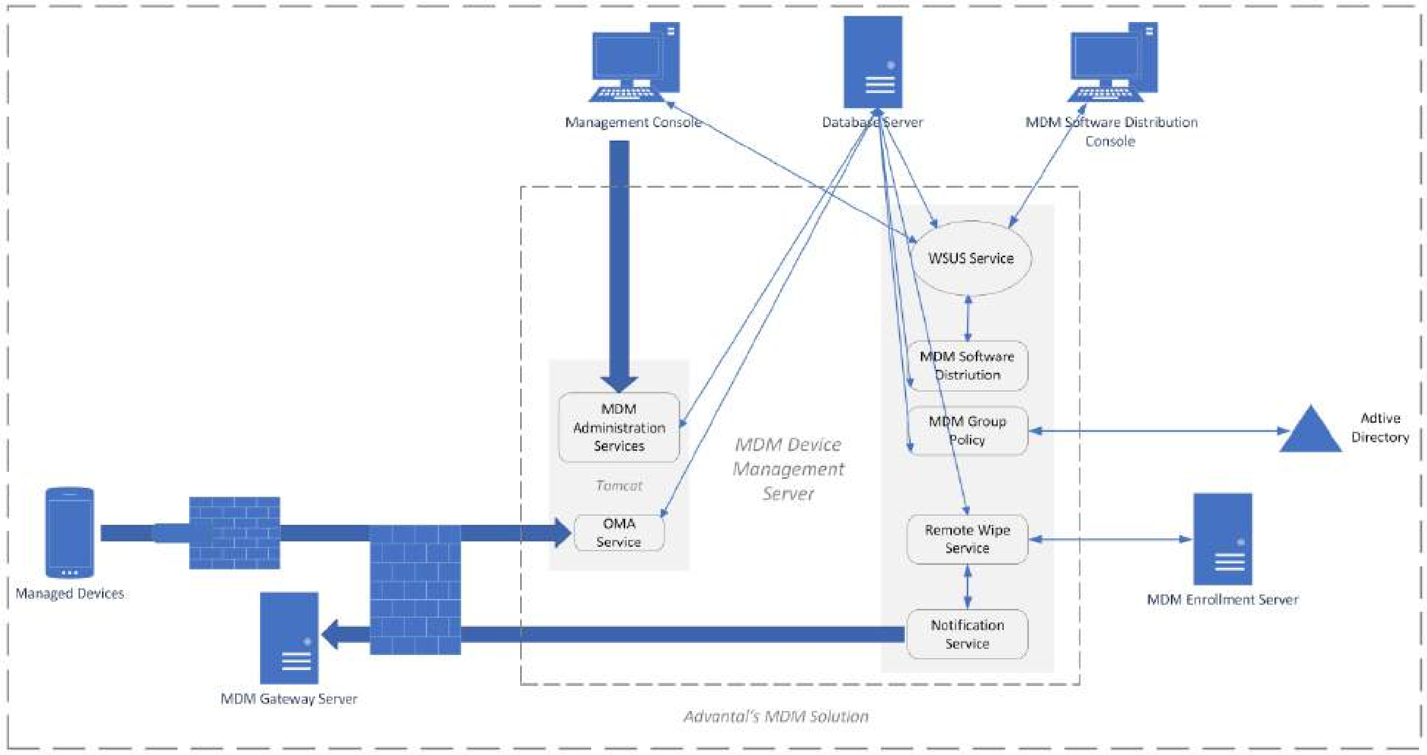
SECURITY MANAGEMENT

- Force passcodes to be set in accordance with your organization's security standards.
- Remotely lock devices to prevent misuse of misplaced or stolen devices.

ROBUST MDM SUPPORT

- Monitor devices for up-to-date device information.
- Diagnose device, user, or application issues from a centralized platform.

MDM DEPLOYMENT



SALIENT FEATURES

- Wipe out the existing phone contacts.
- Wipe out the existing call logs.
- Solution provides device inventory and device tracking.
- MDM Agent will block the Second SIM Slot in case the slot is available in device.
- MDM Solution permit only white listed applications to run on device.

Advantal™

- MDM Solution integrate with existing LDAP directory.
- MDM Solution integrates with Network Management System.
- Notification module of the MDM Solution sends SMS/EMAIL notifications to the administrators on policy violations.
- MDM Solution supports Grouping of devices based on organization hierarchy, Location based & Different Admin levels.

SALIENT FEATURES

- Device setup for custom user experience.
- Customize corporate branding through boot logo and dynamic wallpaper.
- Set custom lock screen messages.
- Set help text for modifying device settings.
- Manage lock screen features for fully managed and dedicated devices.
- Manage system updates.
- Retrieve device MAC addresses.
- Set default apps for specific activities.
- Solution must push customized notification on the device at group and individual level.
- MDM should be able to schedule software for the handset.

DEVICE MANAGEMENT

- Solution must provision for enforcement of GPS.
- Remotely reboot devices.
- Manage network radio settings.
- Manage system audio settings.
- Manage system clock settings.
- Standard certificate management.
- Advanced certificate management.
- Set policies for permission requests.
- Manage specific permission requests.
- Network Usage statistics for devices.
- Delegate certificate management.
- Block users from modifying WIFI settings.
- Able to integrate with VPN solutions.
- Block user from uninstalling apps.
- Control accessibility services settings.
- Enable/disable screen capture.
- Remotely reboot devices.
- Creation of Custom Report Users/ Groups for select details and for specific period of time.
- On Demand Compliance report and Compliance control for OS.
- Activity watermark with respective user id along with date and time during entire usage of phone.

DEVICE SETUP: DEVICE SECURITY

- Set advanced passcode restrictions
- Partial and complete wipe.
- Compliance enforcement.
- Access security Logs
- Disable all debugging
- Check device integrity
- Enforce verification of applications.
- Block external data transfer.
- Set lock screen restrictions.

APP STORE MANAGEMENT

- Manage app store web console.
- Silently distribute apps.
- Configure apps according to roles/privileges.
- Manage in house developed apps.
- Manage in house app store on devices.
- Customized managed IN HOUSE APP store layout.
- Deploy apps through package which is encrypted and more secure.

DEVICE CONTROL

- Bluetooth
- WIFI
- Camera
- SD Card
- USB Storage
- Software based Phone Reset

POLICY ENFORCEMENT

- GPS
- Camera
- Wi-Fi/ Hotspot/ tethering/ USB/ Bluetooth / NFC/Debugging options.
- Second SIM slot
- Block access to external storage media.
- Enforce clients to use remote storage by default while using camera app etc.

Mobile Device Management Features

MDM comes with various features that are mentioned below:

- MDM Agent will continuously monitor the APN settings. In case any APN is created or being used which is not available in the approved Army's APN List, application will put the phone in Flight Mode.
- MDM will seamlessly integrate with existing IAF captive LTE network and device ecosystem with LDAP & IAF 3 certification.
- MDM Solution will have customizable dashboard/watch-lists for end-point management like UEs not-registered, active/inactive status, network resource usage details etc.
- App installation/removal can be enabled only at server/admin through the web based management console.
- Password policy enforcement on devices can be done via MDM Solution.
- Solution supports geofencing or time-fencing features that enable you to limit where and when a device or certain applications can be used. For example, a device
- may automatically lock when it leaves a facility, or certain applications may only be accessible during lunch breaks or after hours.

Advantal™

- Remote wiping of devices can be activated from the solution by an authorized administrator through the web console. Remote wiping can also be activated based on policy enforcement.
- Wipe out existing phone memory data which includes images/ videos/ application data or any other file formats
- Wipe out the data on memory card which includes images/ videos/ application data or any other file formats.
- Move the device to Offline mode to ensure that there will be no network access hence no incoming/ outgoing calls (voice/ video), incoming /outgoing SMS. If user tries to change the profile to any other, the application will forcefully change the profile to Offline immediately. i.e., making the device unusable.
- Language of the application is English.

Contact for Support

Corporate Office
104, Vipul Trade centre, Sohna - Gurgaon Rd,
Sector 48, Gurugram, Haryana, India

Development Center
209, 1st Floor, Right Wing, MPSEDC STP Building,
Electronic Complex, Pardeshipura, Indore,
Madhya Pradesh, India

For Sales Assistance

sales@advantal.net

ashish.thakral@advantal.net

+91-731-4037720 | +91-9910097871

www.advantaltechnologies.com