BD-004 Requirement specification

Mobile device management system

This document discusses on the requirement for the mobile device management tool which will be used by the customer to manage the devices used across the company.

Table of Contents

Document Editing History

Color codes

Color	Description
	Content already existed in the document before
🟨	Content which has been added recently would be highlighted with yellow color

Glossary

S No.	Entity or Term used in the document	What it Means in the Document
1	MDM	Mobile device management tool which helps the administrator to manage the devices remotely.

1 Introduction

The mobile device management tool (MDM) would be used by the administrator of the customer to manage mobile devices across the company. It corresponds to many functionalities that can manage the mobile remotely by the administrator.

The MDM should work in addition to the mobile application that would be hosted on the mobile device. The MDM should work as a web application and can be accessed by the administrator from any location.

2 Scope

The scope of the document is to document the requirement specification for MDM in addition to the explanation of different functionalities of MDM and how they should work. This document explains the complete requirement specification of MDM at the administrator level.

The MDM management should work on the mobile network/ WiFi for accessing the mobile devices.

3 Goal

The goal of MDM is to manage the devices remotely from an administrator panel. The MDM should also help the administrator locating the device with its GPS coordinates. MDM would need to achieve the following functionalities as its goal.

1. Register the mobile device along with the user (User/Mobile licensing).
2. It would capable of managing the user login
    a. Locking the user
    b. Terminating the session of the user
    c. User login and logout logs
3. GPS coordinates
    a. It would help the administrator to locate where the user is located now
    b. All the details would be shown on the map.
4. User licensing:
    a. It would also be able to handle the user licensing
    b. If the user tries to login after exceeding the number of licenses on his device, this it will show a popup saying contact the administrator, licenses exceed.
    c. Administrator will also be able to view whether there are any users who were not able to login because of the licensing issue.
5. Sending messages
    a. The administrator would also be able to sending messages/ alerts to the user mobile.
6. Wiping the device:
    a. The administrators can also wipeout the device, if the user quits the company without informing.
7. Device status:
    a. The administrator can also monitor memory status, battery status etc., from the application.

4 Entities

The MDM has different entities or objects to work with:

1. Mobile device
2. Administrator
3. Mobile User

4. Super user

Mobile device: It is a hardware which can be of any configuration and running on any operating system (IOS, ANDROID, WINDOWS). The device can also be a tab or a mobile which also works on different operating system. The status of the mobile devices can be offline or online.

Offline: Is when the device is not under the coverage area/ or the device does not have access to the internet

Online: Is when the device is under the coverage area/ or the device is connected to the internet.

Note: Each customer can have multiple devices running with different operating system.

Administrator: The administrator of the customer would be the control manager who would control all the devices along with its users across the company. The administrator is authorized to create users, to distribute a license to a listed user until the administrator has reach the maximum number of licenses available for this customer. The administrator is authorized to disconnect the distributed license from the device of a user and redistribute the same license to another user with another device or to redistribute the same license to the same user with a new device. The devices that have been disconnected will end up on a blacklist and can't receive any license again unless overruled by the super administrator. The user that has been disconnected will NOT end up on a blacklist.

Mobile user: Mobile user is the one who would be the end user of the mobile device which works under the mobile network. The user would be using the mobile application in performing various tasks.

Super administrator: Super administrator is the administrator of the supplier of the application (ABS) that sets the maximum number of licenses for the application. The super administrator has the authorization to change the number of licenses, to block one or all licenses, to block one or all devices and to de-block the users and devices. The super administrator is authorized to create and erase an administrator.

5 Features of MDM

The MDM tool would work only under one user that is Administrator, Who would manage all the mobile device using the MDM tool. Below are the list of functionalities/ features that can be handled from MDM by an Administrator:

Note: The features/ functionalities are described as per the status of mobile device.

1. Mobile device registration

The administrator should also register the mobile device on the MDM tool with the mobile configuration details along with the device information. Until the device is registered with the MDM tool, the user or the device will not be able to make use of the mobile application installed on the device. Even if the user try to make use of the mobile application, it should warn that the "Device is not activated or it does not have a valid license".

As a note of user licensing structure, each device can be used by only one user. In the sense each device is allocated only to one user. And each device/ user must hold a valid license to run the mobile application. So, the number of devices the customer would like to use would be the number of licenses the customer should hold.

2. Handling licenses

   The administrator will also have accessibility of managing the licenses on the devices using the MDM tool. He can disconnect the license from one device and add the same license to a new device. And also he will not be able to add more than one license to a device.

   Once the license is disconnected from one device, the user belonging to that device will not be blocked. But will be capable of using the mobile application from a new device or existing device on which mobile application has not been installed.

   Before the user making use of the new device or existing device, the device needs to be registered with the MDM tool.

3. Managing login

   a. Locking the user, locking the device

      The administrator should be capable of locking the user or device, so that he cannot be able to login to the mobile application any more. Once the user is locked the user will not be able to login in any of the devices across the company. The administrator would need to unlock the user to make the user login again.

With lock or block I mean that the user or device cannot be used for running the mobile application anymore. User will not be allowed to login into the mobile application.

Once the user is locked he should not be able to upload or download the data from the application database on the server. He cannot login into the mobile application and whatever data flows from the device will not be uploaded to the central server.

b. Terminating the user session (Online)

   The administrator should be capable of terminating the user session when the device is connected to the network.

   Once the user session is terminated the user should not be able to upload or download the data from the central database of the application.

c. Displaying user logs

   The administrator should also see the user logs of the user in the administrator tool. The logs will contain all the actions performed by the user on the mobile application (Login, logout, upload, download, sync etc.,)

4. GPS coordinates
   The administrator tool should be capable of retrieving the GPS coordinates of the device across the company. The GPS coordinates should be shown in form of map in the administrator. The time interval in recording the GPS coordinates should be 5 minute. And also the administrator tool should store the complete history GPS coordinates, so that administrator can find on what path the user has taken in reaching the field. And the path must be shown in the form of map.

   The GPS coordinates of the device must be recorded irrespective of whether the device is online of offline. But when the device comes back to online the device should upload the latest history of GPS coordinates to the central server.

This should also help the administrator to have a look at what route was taken by the field inspector to visit the field.

5. Sending messages

   The administrator should be capable of sending messages/ alerts to the user on his/ her device using the MDM tool. Even though the messages are sent when the device is offline the messages must be retrieved by the device when it comes online. These messages can either be broadcasted to all the devices or can only be sent to specific device/ user.

6. Wiping the device

   The administrator should also be able to wipe the device and all its data. Even though the device is offline the device must be wiped off as soon as it comes online and not allowing user to perform any activities as soon as the device comes online.

7. Device status

   The administrator should also be able to view the status of device on the following details:

   a. Memory status
   b. Battery status
   c. Screen brightness status
   d. Total number of hours device used

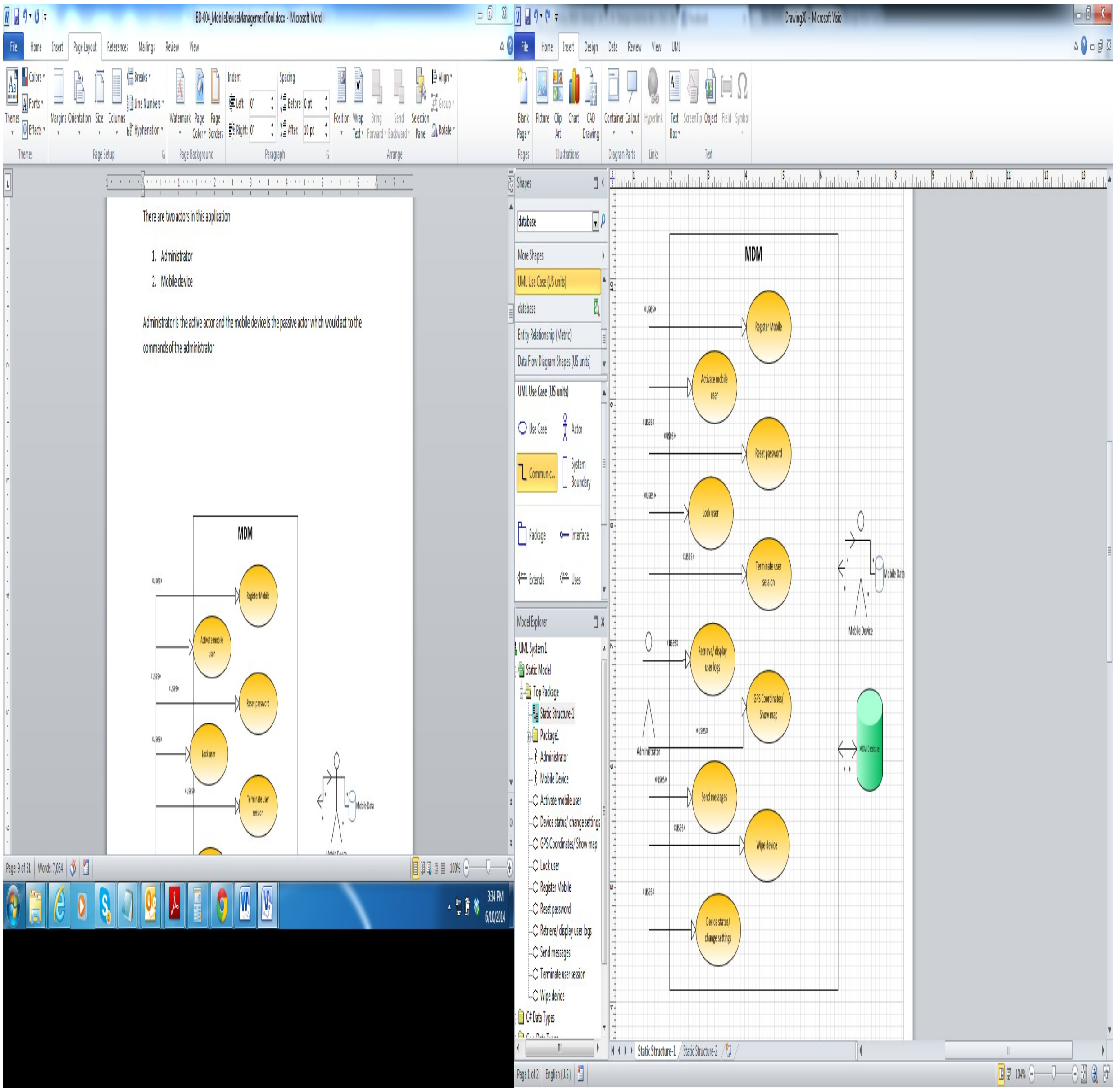
6 Use cases

There are two actors in this application.

1. Administrator
2. Mobile device
3. Super administrator

Administrator is the active actor and the mobile device is the passive actor which would act to the commands of the administrator

6.1 Administrator



There are two actors in this application.

1. Administrator
2. Mobile device

Administrator is the active actor and the mobile device is the passive actor which would act to the commands of the administrator

6.2 Mobile Device:

The mobile device along with the mobile user would be handling the following activities. And one of major constraints of the mobile device is that it can be disconnected from the mobile network, when the device is at a remote location.

The mobile device in the background must record the following details in its databases. And these processes would run on the mobile device in the background:

1. GPS Coordinates
2. User activity logs

Apart from that the device should always update the mobile database with the server instance as soon as it connects to the mobile network. By which the user or mobile device can handle the following activities

1. Lock user
2. Terminate user session
3. Receive administrator messages
4. Exchange details on user activities (GPS Coordinates, User activity logs)
5. Wiping the device

6.3 Super administrator:

Super administrator is a user from ABS who would interact with the customer. The super administrator will act on the top the administrator at the customer. He can perform the following activities:

1. Set licensing limits
2. Block licenses
3. Block/ unblock devices/ users
4. Delete/ Block administrator

Set licensing limits: This functionality in the MDM can only be accessed by the super administrator who can set the limit for the number licenses as per the agreement with the customer. He can either increase or decrease limit of number of licenses owned by the customer.

With the license we mean that each device which corresponds to one user will hold a license irrespective of whether the device is used all the time or not. If the device along with the corresponding user would plan to use the mobile application then it should hold a license to activate the mobile application.

Block licenses: This feature would be used to block all or some of the licenses hold by the customer on the mobile devices. Once the license is blocked the device and the user holding the blocked license cannot run the mobile application any more.

Block/ unblock devices or users: Similar to feature provided to the administrator the super administrator would have the rights to block the devices corresponding to the user. Once the device is blocked along with the user the device and user cannot be used for logging into the mobile application. And the mobile application cannot transfer any data back and forth from the central server.

Delete/ Block administrator: The super administrator would also have a capability to delete or block administrator. Once the administrator is deleted or blocked he cannot be able to access the MDM tool any more until and unless the administrator is activated or unblocked by the super administrator.

7 Functional workflows/ Activity diagrams

This section explains about the functional workflows for each and every feature that would be incorporated in MDM.

For all the features the login would be the common functionality by the administrator without with the administrator would not be able to operate on any of the features.

7.1 Registering the mobile

The super user should register the mobile before it is used for the web application. The device should be registered with the following details:

1. Device user
2. Device make
3. Device OS
4. Device OS version
5. Device screen size/ resolution
6. IMEI number
7. Mother board number etc.,

All these details should be mapped to the user license which cannot be used on any other device. And this functionality should be enabled only for the super user who is license administrator works from the vendor supplying the mobile application.

7.2 Handling licenses

The administrator can perform following activities under handling licenses:

1. Delete a license from device

   The administrator can delete a license from the device upon which the device cannot be used for using the mobile application. But still the user corresponding to the device can be mapped to a new device or existing device on which mobile application has not been installed.

2. Add an existing license to new device

   Before adding an existing license the device needs to be registered with the MDM tool. Upon which the device will then be mapped to a user who has no assigned device. And then the administrator will be able to add the existing license to the device so that the mobile application can be activated and used.

7.3 Managing Login

Locking user:

Terminating the user session:

Display user logs:

All the user logs - login, logout, Database sync, Upload etc., must be recorded and displayed as the user log for the administrator

7.4 GPS Coordinates

7.5 Sending messages

7.6 Wiping the device

7.7 Device status and change Device settings

The administrator would need to access the device settings and would be able to change the device settings if needed. The need for the change of the device settings is to save the battery or increase the data connectivity etc.,

8 Licensing activity workflow

To make the licensing structure of the application further clear, we would like to explain the licensing activity flow in the pictorial manner both from the administrator perspective and the device/ user perspective

Administrator:

The above workflow explains the scenario for the administrator trying to add/ register the new device. Once the device is add the administrator would map the device to the user upon which the mobile application would be installed on the device from Apple store or Google play store. Once the application is installed the application needs to be activated with the help of the license. Whenever the administrator tries to add a license to the device to activate the application, the MDM tool checks whether the licensing limit set by the super administrator exceeds or not, if not the system would allow to add the license to the device.

Device/ User:

In here we would like to explain scenario when the device is online and offline:

When device is online: The device retrieves the data corresponding to licensing information and user or device status. If the device has been removed with the license by the administrator using MDM tool, the device can no more be used to run the mobile application and hence cannot upload the mobile data to the customer server.

When device is offline: The user on the device performs normal activities unless the device comes back to online. Whenever the device comes back to online, the device retrieves the data corresponding to licensing information and user or device status. If the device has been removed with the license by the administrator using MDM tool, the device can no more be used to run the mobile application and hence cannot upload the mobile data to the customer server.

Note: Whenever the device comes to online. The licensing information and the user or device status is retrieved first from the customer server and then if everything is ok with the device and the user including the license, the data would then be uploaded from the device to the customer server.

9 Versioning of the Mobile Application:

We keep upgrading the mobile app based on the customer requirements and future enhancements. Each upgrade would get a different version number with the documentation on the new features of the upgrade.

We either need to upload the app to Google Play Store, Apple, Windows store to install the app on the mobile device or we need to install the mobile app by connecting the device to a PC and installing it – which is a very big process. Installing the mobile app manually from the customer server is difficult because we need have the device connected to the PC which can install the app to any device (Android and Windows we can install using a Windows PC, but for Apple we would need a MAC PC to make the installation of the mobile app onto the device). And hence we do not follow the manual procedure.

Instead we create a private channel for each customer on Google Store, Windows Store and Apple Store. By which each customer will have a location to access with the username and password to install the mobile app on the mobile for the corresponding store. The advantages of maintaining the private channel is:

1. As each customer might have a different version of the app, private channel will help in maintaining different versions of the app for different customers.

2. If the app is uploaded to the public store which can be accessed by anyone on the network, the app can be installed by anyone. And also the public store would be common for all the customers, by which we cannot maintain different versions of the app with each customer.

3. Maintaining the private channel in the corresponding app stores, will also help to avoid the manual intervention in installing the app on the device.

4. Whenever the new version of the app is uploaded to the customer private channel, the users corresponding to the customer can install the new version of the app without the intervention of the administrator.

With this scenario maintaining the versions of the app for different customers across the globe would not be so difficult. But with this we have an additional cost for each customer who needs to buy an account under the customer domain in Google, Windows and Apple (which cost less than 100$ per account and each customer needs to have only one account irrespective of number of users downloading the app and the number of different apps).

The above pictorial explains about how the private channel can be maintained for each customer. And how it can be advantageous instead of installing the app manually or hosting it on the public channel.