

ManageEngine 

Mobile Device Manager Plus

About us

Mobile Device Manager Plus is a mobile device management solution developed by ManageEngine. Mobile Device Manager Plus provides admins the power to perform device management from a single point. It is available on premise and also as a cloud based service. Mobile Device Manager Plus integrated with Desktop Central provides a complete desktop and mobile device management solution.

How we help?

With the ever growing use of mobile devices in enterprises, it has become inevitable to manage all the mobile devices coming into the company, to ensure the security of corporate data. Mobile Device Manager Plus provides a complete device management solution for managing both BYOD and corporate devices running on Android, iOS and Windows. It allows the user to group devices for better management, apply various restrictions on devices, distribute store and enterprise apps, blacklist apps, locate devices on demand, and much more.

Benefits of choosing Mobile Device Manager Plus

Mobile Device Manager Plus is a web based server that manages thousand of mobile devices from a central location. It automates the entire device management process from enrollment to retirement. Following are the benefits of using Mobile Device Manager Plus as your device management tool:

- It is an affordable web-based solution.
- Facilitates Over-The-Air device management.
- No formal training is required to work with the software, minimal network administration knowledge is sufficient.
- Enhances productivity of network administrators by reducing their workload.
- Reduces maintenance and support expenditures associated with manual device management.
- Increases device security thereby reducing business losses.

System requirements:

Following are the system requirements to use Mobile Device Manager Plus for managing mobile devices.

Hardware requirements for Mobile Device Manager Plus Server:

No. of Devices Managed	Processor Information	RAM Size	Hard Disk Space
1 to 250	Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MB cache	2 GB	5 GB*
251 to 500	Intel Core i3 (2 core/4 thread) 2.4 Ghz 3 MB cache	4 GB	10 GB*
501 to 1000	Intel Core i3 (2 core/4 thread) 2.9 Ghz 3 MB cache	4 GB	20 GB*
1001 to 3000	Intel Core i5 (4 core/4 thread) 2.3 GHz. 6 MB cache	8 GB	30 GB*
3001 to 5000	Intel Core i7 (6 core/12 thread) 3.2 GHz. 12 MB cache	8 GB	40 GB*
5001 to 10000	Intel Xeon E5 (8 core/16 thread) 2.6 GHz. 20 MB cache	16 GB	60 GB*

* May increase dynamically with the frequency of scanning.

NOTE: While managing more than 1000 devices it is recommended to install Mobile Device Manager Plus on a Windows Server Edition.

Software requirement for Mobile Device Manager Plus:

Mobile Device Manager Plus can be installed on a computer which satisfies the following requirements.

Desktop related operating systems

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

Server related operating systems

- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Supported browsers

Install any of the following browser on the computer to run Mobile Device Manager Plus console.

- Microsoft Internet Explorer 10 and later versions
- Mozilla Firefox 44 and later versions
- Google Chrome 47 and later versions

NOTE: Make sure that the screen resolution is 1024X768 or higher.

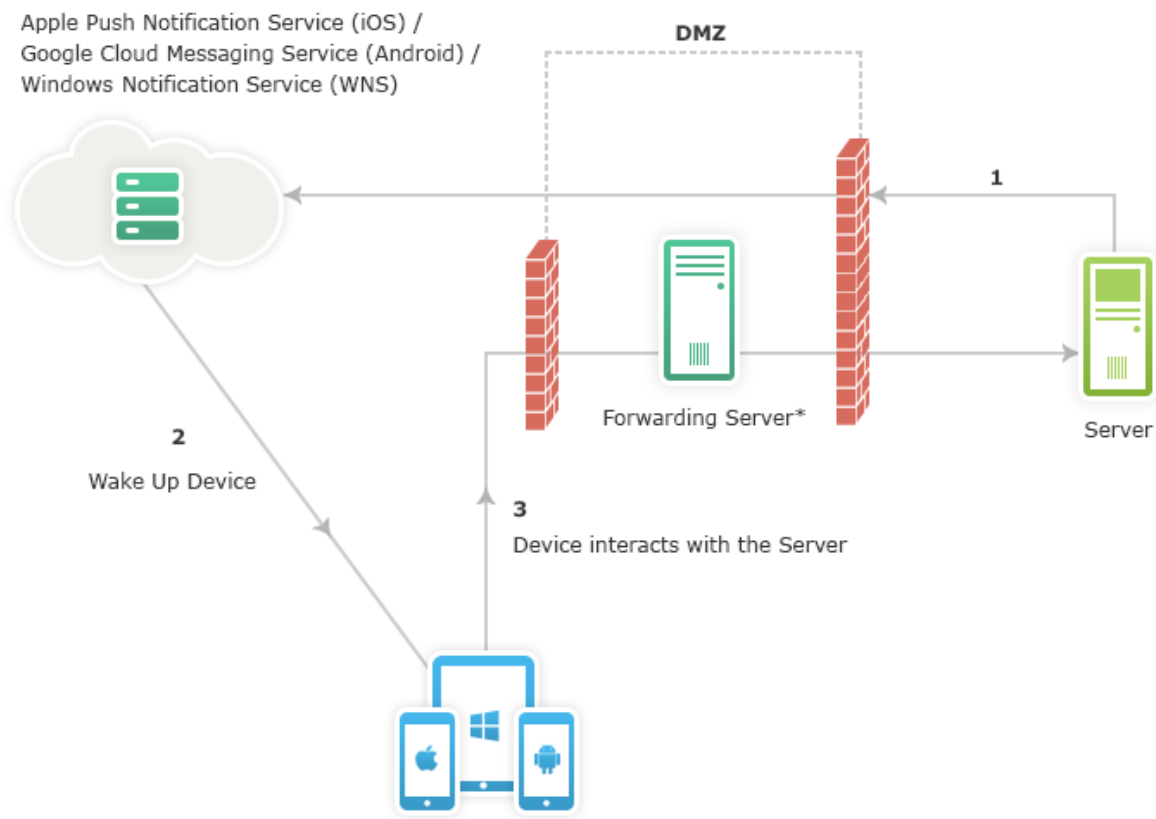
Mobile devices supported

The following are the devices that can be managed:

- iPhone, iPad and iPod Touch running iOS 4 and above.
- Smart Phones and Tablets running Android 2.2 and above.
- Windows Phone 8 and above.

Mobile Device Manager Plus architecture

The diagram shown below explains the architecture of Mobile Device Manager Plus.



Components:

The following are the architectural components of the Mobile Device Manager Plus.

- Server
- Forwarding Server
- APNs,GCM,WNS
- Mobile Devices

Server: Server is the main component of the architecture. All the devices can be managed from the server. The server should be reachable from a Public IP address to manage the

mobile devices. Hence, the server should be present on edge of the network.

Forwarding server: Forwarding Server is an optional component of architecture. It is configured to ensure that the server is not directly exposed to the internet. This keeps the server safe from threats and attacks.

NOTE: The NAT settings need to be configured to ensure that the devices are always in contact with the server.

APNs,GCM,WNS: These are mobile notification services that allow third party applications to send notifications to mobile devices. Mobile Device Manager Plus contacts these notification services to manage iOS,Android and Windows devices respectively.

NOTE: Proxy Settings need to be configured for Mobile Device Manager Plus to connect to the internet.

Another mandatory requirement before devices can be managed is to configure the Mail Server. The Mail Server needs to be configured to send e-mails related to enrollment, inventory and reports

Features of Mobile Device Manager Plus

Following are the key features offered by Mobile Device Manager Plus.

- Device Enrollment
- App Management
- Profile Management
- Asset Management
- Device Security
- E-mail Management
- Reports

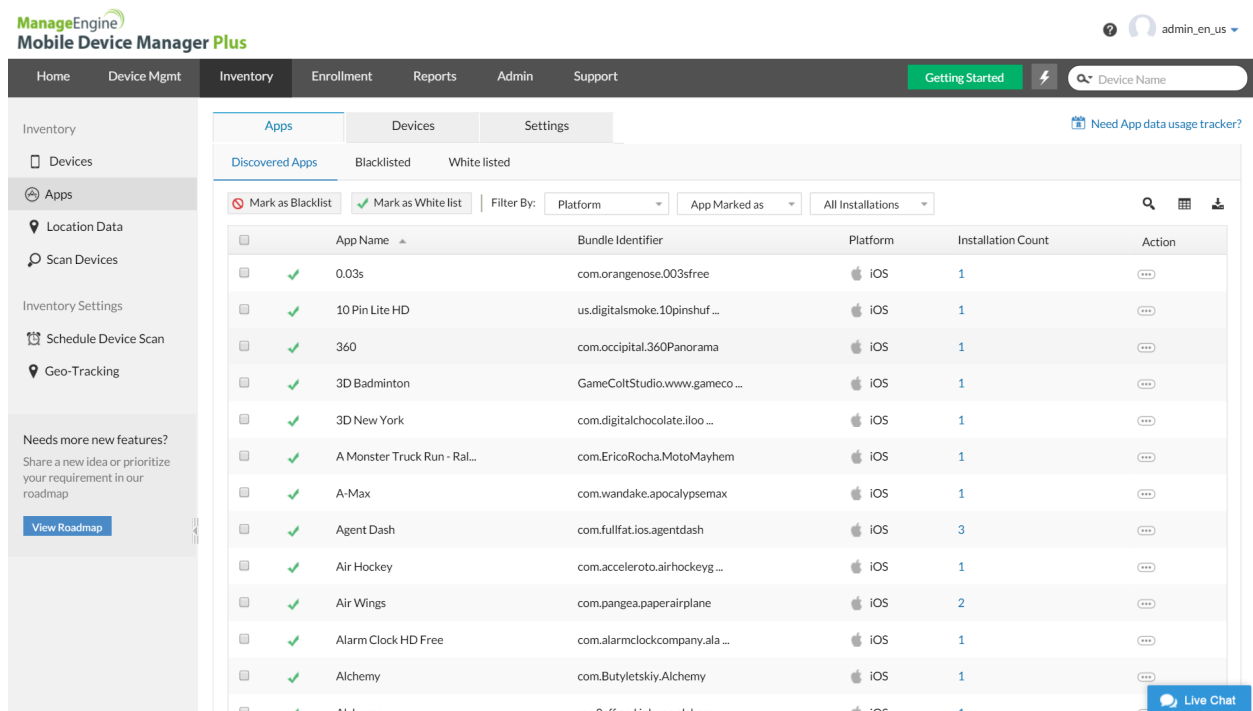
Device Enrollment:

Before the devices can be managed, they need to be enrolled into the server. As there will be large number of devices that are to be managed, Mobile Device Manager Plus offers the users different types of enrollment methods based on the types of devices to be enrolled.

User Name	Email	Platform	Owned By	Status	Remarks
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
user-37	user-37@zohocorp.com	iOS	Corporate	Enrolled	Successfully enrolled
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
dilip-2665	dilip.v@zohocorp.com	iOS	Corporate	Enrolled	Successfully enrolled
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
ANDREW	andrew@desktopcentral.com	iOS	Personal	Enrolled	Successfully enrolled
user-38	user-38@zohocorp.com	iOS	Corporate	Enrolled	Successfully enrolled
user-39	user-39@zohocorp.com	iOS	Corporate	Enrolled	Successfully enrolled

App Management:

As the apps present in the mobile devices make use of corporate data it is important to manage the apps in the devices as well. Mobile Device Manager Plus allows user to blacklist apps that should not be present in the mobile devices. Users can distribute both Enterprise and Store apps to the devices Over-The-Air.

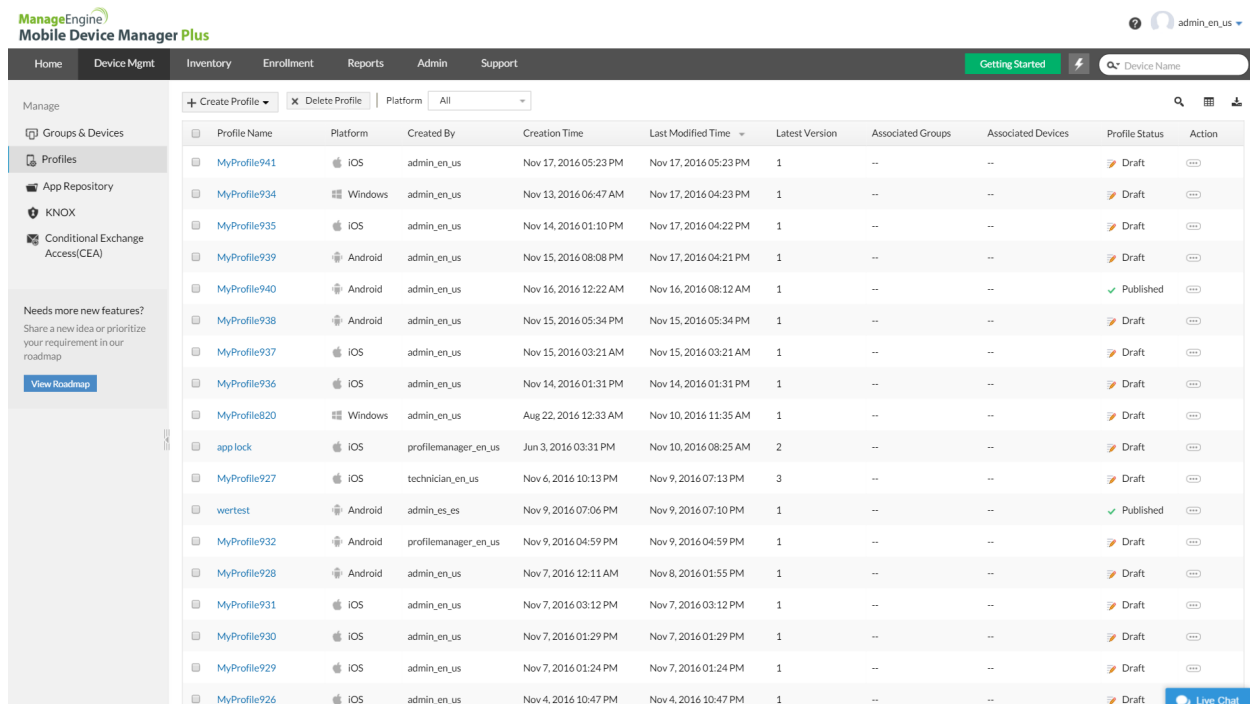


The screenshot displays the ManageEngine Mobile Device Manager Plus interface. The top navigation bar includes Home, Device Mgmt, Inventory, Enrollment, Reports, Admin, and Support. The user is logged in as admin_en_us. The main content area is titled 'Apps' and shows a list of discovered apps. The table below lists the apps with their details.

App Name	Bundle Identifier	Platform	Installation Count	Action
0.03s	com.orangenose.003sfree	iOS	1	...
10 Pin Lite HD	us.digitalsmoke.10pinshuf...	iOS	1	...
360	com.occipital.360Panorama	iOS	1	...
3D Badminton	GameColtStudio.www.gameco...	iOS	1	...
3D New York	com.digitalchocolate.iloo...	iOS	1	...
A Monster Truck Run - Ral...	com.EricoRocha.MotoMayhem	iOS	1	...
A-Max	com.wandake.apocalypsemax	iOS	1	...
Agent Dash	com.fullfat.Ios.agentdash	iOS	3	...
Air Hockey	com.acceleroto.airhockeyg...	iOS	1	...
Air Wings	com.pangea.paperairplane	iOS	2	...
Alarm Clock HD Free	com.alarmclockcompany.ala...	iOS	1	...
Alchemy	com.Butyletskyi.Alchemy	iOS	1	...
Alchemy	me.Duff.zed.iphone.alchem...	iOS	1	...

Profile Management:

Every device is not used to perform the same task, Mobile Device Manager Plus provides the user with an option to group devices based on departments and roles. Different restrictions and profiles can be applied to these groups. These profiles determine what features of the device can and cannot be accessed by the device user.



The screenshot displays the ManageEngine Mobile Device Manager Plus interface. The top navigation bar includes tabs for Home, Device Mgmt, Inventory, Enrollment, Reports, Admin, and Support. A search bar is present on the right with the text "Device Name". The left sidebar contains a "Manage" section with options for Groups & Devices, Profiles, App Repository, KNOX, and Conditional Exchange Access (CEA). The main content area shows a table of profiles with columns for Profile Name, Platform, Created By, Creation Time, Last Modified Time, Latest Version, Associated Groups, Associated Devices, Profile Status, and Action. The table lists various profiles, including "MyProfile941" through "MyProfile926", with statuses ranging from Draft to Published. A "Live Chat" button is visible in the bottom right corner.

Profile Name	Platform	Created By	Creation Time	Last Modified Time	Latest Version	Associated Groups	Associated Devices	Profile Status	Action
MyProfile941	iOS	admin_en_us	Nov 17, 2016 05:23 PM	Nov 17, 2016 05:23 PM	1	--	--	Draft	
MyProfile934	Windows	admin_en_us	Nov 13, 2016 06:47 AM	Nov 17, 2016 04:23 PM	1	--	--	Draft	
MyProfile935	iOS	admin_en_us	Nov 14, 2016 01:10 PM	Nov 17, 2016 04:22 PM	1	--	--	Draft	
MyProfile939	Android	admin_en_us	Nov 15, 2016 08:08 PM	Nov 17, 2016 04:21 PM	1	--	--	Draft	
MyProfile940	Android	admin_en_us	Nov 16, 2016 12:22 AM	Nov 16, 2016 08:12 AM	1	--	--	Published	
MyProfile938	Android	admin_en_us	Nov 15, 2016 05:34 PM	Nov 15, 2016 05:34 PM	1	--	--	Draft	
MyProfile937	iOS	admin_en_us	Nov 15, 2016 03:21 AM	Nov 15, 2016 03:21 AM	1	--	--	Draft	
MyProfile936	iOS	admin_en_us	Nov 14, 2016 01:31 PM	Nov 14, 2016 01:31 PM	1	--	--	Draft	
MyProfile820	Windows	admin_en_us	Aug 22, 2016 12:33 AM	Nov 10, 2016 11:35 AM	1	--	--	Draft	
app lock	iOS	profilemanager_en_us	Jun 3, 2016 03:31 PM	Nov 10, 2016 08:25 AM	2	--	--	Draft	
MyProfile927	iOS	technician_en_us	Nov 6, 2016 10:13 PM	Nov 9, 2016 07:13 PM	3	--	--	Draft	
wertest	Android	admin_es_es	Nov 9, 2016 07:06 PM	Nov 9, 2016 07:10 PM	1	--	--	Published	
MyProfile932	Android	profilemanager_en_us	Nov 9, 2016 04:59 PM	Nov 9, 2016 04:59 PM	1	--	--	Draft	
MyProfile928	Android	admin_en_us	Nov 7, 2016 12:11 AM	Nov 8, 2016 01:55 PM	1	--	--	Draft	
MyProfile931	iOS	admin_en_us	Nov 7, 2016 03:12 PM	Nov 7, 2016 03:12 PM	1	--	--	Draft	
MyProfile930	iOS	admin_en_us	Nov 7, 2016 01:29 PM	Nov 7, 2016 01:29 PM	1	--	--	Draft	
MyProfile929	iOS	admin_en_us	Nov 7, 2016 01:24 PM	Nov 7, 2016 01:24 PM	1	--	--	Draft	
MyProfile926	iOS	admin_en_us	Nov 4, 2016 10:47 PM	Nov 4, 2016 10:47 PM	1	--	--	Draft	

There are different restrictions that can be applied to iOS, Android and Windows devices.

For iOS devices:

Many restrictions such as CalDAV, Subscribed Calenders, WebClips etc are exclusively for iOS devices.

The screenshot displays the ManageEngine Mobile Device Manager Plus web interface. The top navigation bar includes links for Home, Device Mgmt, Inventory, Enrollment, Reports, Admin, and Support. A 'Getting Started' button and a search bar are also present. The breadcrumb trail indicates the current location: Device Mgmt > Profiles > Create Profile > MyProfile941. The main content area is titled 'Create Profile' and features a 'Define Profile' section with a 'Passcode' policy selected. The configuration options for the Passcode policy are as follows:

Setting	Value
Allow Simple Value	<input checked="" type="radio"/> Yes <input type="radio"/> No
Require Alphanumeric Value	<input type="radio"/> Yes <input checked="" type="radio"/> No
Minimum Passcode Length	Select
Minimum Number of Complex characters	Select
Maximum Passcode Age	days (1-730)
Auto-Lock the device when it is idle for	Select min
Number of Passcodes to be maintained in the history	(1-50)
Grace Period to Unlock Device without Passcode	Select
Maximum Number of Failed Attempts	Select

A 'Save' button is located at the bottom of the configuration area. The left sidebar lists various policy categories: Passcode, Restrictions, Wi-Fi, VPN, Email, Exchange ActiveSync, Certificate, LDAP, Web Content Filter, CalDAV, Subscribed Calendars, CardDAV, Web Clips, Kiosk Mode, Global HTTP Proxy, Access Point Name, and a link for 'Need a new policy?'. A 'Help' link is visible in the top right corner of the 'Define Profile' section.

For Android Devices:

The screenshot shows the 'Create Profile' page for an Android device. The breadcrumb trail is 'Device Mgmt > Profiles > Create Profile > MyProfile944'. The page title is 'Create Profile'. On the left, there is a sidebar with icons for 'Passcode', 'Restrictions', 'Wi-Fi', 'Email', 'Exchange ActiveSync', 'Kiosk', 'Wallpaper', and 'Global HTTP Proxy'. Below these is a link 'Need a new policy?'. The main area is titled 'Define Profile' and contains the following settings:

Minimum Passcode Requirement *	:	Select
Maximum Number of Failed Attempts ?	:	Select
Auto-Lock the device when it is idle for	:	Seconds
<small>[Note: 5 to 1800 seconds]</small>		
Number of Passcodes to be maintained in the history [1]	:	
Maximum Passcode Age [1]	:	Days
Force Passcode Policy After [?]	:	1 Hr
Unlock Device using Fingerprint [1]	:	<input type="radio"/> Allow <input checked="" type="radio"/> Restrict

At the bottom of the form are buttons for 'Save', 'Publish', and 'Cancel'. The footer contains the copyright notice '(C) Copyright 2016, ZOHIO Corp.' and a 'Live Chat' button.

For Windows devices:

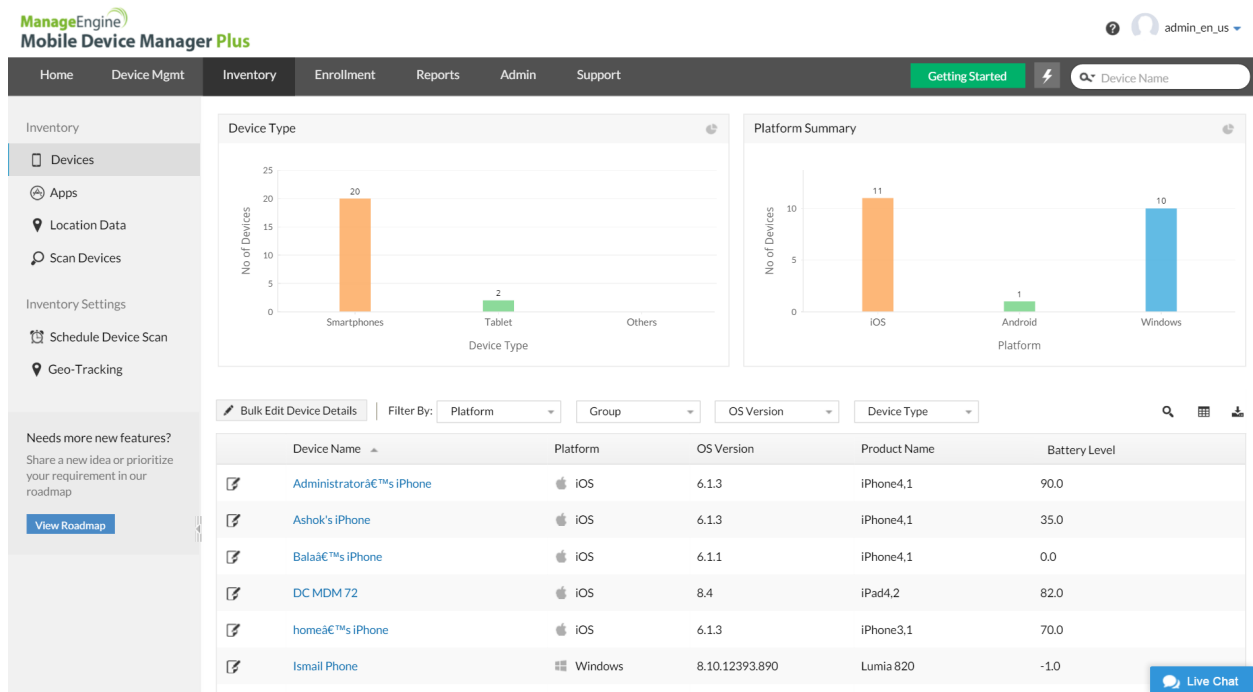
The screenshot shows the 'Create Profile' page for a Windows device. The breadcrumb trail is 'Device Mgmt > Profiles > Create Profile > MyProfile942'. The page title is 'Create Profile'. On the left, there is a sidebar with icons for 'Passcode', 'Restrictions', 'Email', 'Exchange ActiveSync', and 'Wi-Fi'. Below these is a link 'Need a new policy?'. The main area is titled 'Define Profile' and contains the following settings:

Passcode should contain *	:	Alphabets
Minimum Passcode Length	:	4
Minimum Number of Complex characters	:	0
Maximum Passcode Age	:	Days (1 to 730)
Auto-Lock the device when it is idle for	:	Minutes (1 to 999)
Number of Passcodes to be maintained in the history	:	
Maximum Number of Failed Attempts ?	:	(1 to 999)

At the bottom of the form are buttons for 'Save', 'Publish', and 'Cancel'. The footer contains the copyright notice '(C) Copyright 2016, ZOHIO Corp.' and a 'Live Chat' button.

Asset Management:

As the number of enrolled devices grows, keeping track of all the devices can become a cumbersome task. Details about the devices such as the IMEI number, UDID etc along with all the devices enrolled is listed. Details such as jailbroken or rooted devices and list of all the apps, which are crucial to device security are also provided.



Device Security:

Loss of devices can put the corporate data at risk, and to prevent this, various security features such as remote lock, remote alarm, reset password are provided. In case a device is lost, the device can be located on demand. As both BYOD and corporate device are being managed, it also provides two data wipe options.

Complete Wipe- This is most suitable for corporate devices which have only corporate data and can be wiped completely.

Corporate Wipe- Corporate wipe clears on the corporate data present in the device while leaving the users personal data intact. This is most useful for BYOD when an employee leaves the company.

The screenshot displays the ManageEngine Mobile Device Manager Plus interface. The top navigation bar includes Home, Device Mgmt, Inventory, Enrollment, Reports, Admin, and Support. A search bar on the right contains the text "Device Name". The main content area is titled "Device Details - Administrator's iPhone" and shows the last scan time as "Mar 27, 2015 05:36 PM".

The interface is divided into several sections:

- Device Summary:** Lists device information such as Device Name (Administrator's iPhone), Device Type (Smartphones), Model (MD235HN), Product Name (iPhone4,1), and IMEI Number (4025745ee77e418ca5ea7bc7207bbfee).
- Network Summary:** Lists network-related information such as Phone Number, Subscriber Carrier Network (Carrier), Bluetooth MAC (e0:c9:7a:8b:55:1b), WIFI MAC (e0:c9:7a:8b:55:1a), and Roaming Enabled (No).
- OS Summary:** Lists operating system information such as OS (iOS), OS Version (6.1.3), Build Version (10B329), and Serial Number (DNQ19JVDTC0).
- Memory Usage (GB):** A donut chart showing memory usage. The chart is divided into three segments: 28.6% (Free Space), 71.4% (Used Space), and 14 (Total Space). A legend indicates that red represents Used Space (GB) and green represents Free Space (GB).
- Security Info:** A table showing security settings: Hardware Encryption Caps (Yes), Jail Broken Devices (No), Passcode Compliant (Yes), Passcode Compliant With Profiles (Yes), and Passcode Enabled (No).

At the bottom of the page, there is a copyright notice: "(C) Copyright 2016, ZOHO Corp." and a "Live Chat" button.

E-mail Management:

E-mails are the preferred method of communication in the corporate sector. It is essential to prevent loss of corporate data exchanged through e-mail. Using Mobile Device Manager Plus, the user can grant access of the corporate e-mail account to particular devices. In addition to this, user can also restrict unapproved app from using the data.

The screenshot displays the ManageEngine Mobile Device Manager Plus web interface. The top navigation bar includes Home, Device Mgmt, Inventory, Enrollment, Reports, Admin, and Support. A 'Getting Started' button and a search field for 'Device Name' are also present. The user is logged in as 'admin_en_us'.

The main content area is divided into several sections:

- Summary Cards:** Shows 'Devices in Grace Period' (2), 'Restricted Devices' (4), 'Allowed Devices' (1), and 'Last Successful Sync' (Apr 21, 2016 06:57 PM).
- Devices in Grace Period (2):** Lists two users: 'user40 (serranodsdd)' and 'user5 (a5itedd)', both with their email addresses and last sync times (6 months ago and 8 months ago respectively).
- Conditional Exchange Access Policy:** Titled 'How the Policy Works?', it lists two points: 1. Policy applicable to All users. 2. New Devices have no Grace Period and are Quarantined by default. They should be enrolled with MDM, to access Exchange Server.
- Exchange Server Details:** Shows 'Server Name: exchangeserver10.domainname.com', 'Exchange Version: Exchange Server 2010', 'Default Access Level: Quarantine', and 'Total Mailboxes: 32'.

A note at the bottom of the policy section states: 'Note: New devices accessing Exchange Server or a device which gets restricted will receive a Mail from Exchange Server that must include [this content](#), for devices to enroll using Self Enrollment.'

At the bottom of the page, there is a copyright notice: '(C) Copyright 2016, ZOH0 Corp.' and a 'Live Chat' button.

Reports:

Mobile Device Manager Plus creates reports with various device details such as installed apps, blacklisted apps and device model. This helps in analysing and tracking all the devices in the network. Another feature that Mobile Device Manager Plus offers is customized reports-Users can create reports based on their requirements apart from all the reports that are already available.

The screenshot displays the ManageEngine Mobile Device Manager Plus interface. At the top left is the logo for ManageEngine Mobile Device Manager Plus. The top navigation bar includes links for Home, Device Mgmt, Inventory, Enrollment, Reports (which is the active page), Admin, and Support. On the right side of the navigation bar, there is a 'Getting Started' button, a search icon, and a search input field containing 'Device Name'. Below the navigation bar, there are three tabs: 'Predefined Reports' (selected), 'Schedule Reports', and 'Custom Reports'. The main content area is divided into four columns of report categories:

- App Reports**
 - ▶ Apps by Devices
 - ▶ Devices with/without Specific App
 - ▶ Blacklisted Apps Summary
 - ▶ Devices with Blacklisted Apps
 - ▶ New App detected
- Hardware Reports**
 - ▶ Devices by Model
- Enrollment Reports**
 - ▶ Devices by Enrollment Time
 - ▶ Inactive Devices
- Security Reports**
 - ▶ Rooted Devices
 - ▶ Devices by Storage Encryption
 - ▶ Jail Broken Devices
 - ▶ Devices by Passcode Type
 - ▶ Devices backed up in Cloud

At the bottom right of the page, there is a blue 'Live Chat' button.

Product trial and demo

ManageEngine provides the following trials and demo for further evaluation of the product.

- A fully functional, 30 days trial for unlimited devices:
<https://mdm.manageengine.com/free-trial.html>
- Help documents and other literature:
<https://www.manageengine.com/mobile-device-management/help.html>
- Online Demo: <http://demo.mobiledvicemanagerplus.com/>

Pricing

Mobile Device Manager Plus is licensed based on the number of mobile devices and technicians.