ManageEngine

Mobile Device Manager Plus

Admin Guide

Table of Contents

1. Need for MDM in a Corporate Setup

The rate at which the number of mobile devices are increasing in the corporate world, it has become imperative to have a system to manage these mobile devices. The services that need to be offered by such a device management software are multifold. There are different types of devices in the corporate sector and the device management solution should meet the needs of all the devices.

In today's corporate world, companies are moving towards the BYOD trend, where employees make use of personal devices for their work related tasks. Thus there is corporate data present on these devices that needs to be secured.

Many different issues can arise due to BYOD, which should be addressed by a MDM solution.

1. It is important to keep the corporate data safe on devices that have access to the data.
2. The company may prefer to restrict the use of certain features of the devices, like camera.
3. Preventing unauthorized apps from accessing the corporate data present in the devices.

Some organizations still make use of separate devices for corporate use to prevent the misuse of corporate data. These type of corporate owned devices have a different set of management requirements.

1. It is crucial for the company to monitor the location of these devices. This detail about the location of the device can be helpful to locate the devices when required.
2. It is preferred by companies, to be able to control the devices from which the corporate e-mail account can be accessed.
3. Some type of apps should not be present in a corporate device, thus the installation

of these apps should be restricted.

2. Introduction to ManageEngine Mobile Device Manager Plus

ManageEngine Mobile Device Manager Plus offers a wide range of functionalities that help in managing the mobile devices with ease. It can be used to manage Android, iOS, Windows and Chrome devices. Mobile Device Manager Plus has numerous features that address all the requirements of device management in the corporate and also the education sector.

The following features help in addressing the cases discussed above.

1. **containerization**- This feature helps to create a container in the personal device of the employees to store the corporate data. This helps in segregating the personal and corporate data in a single mobile device.
2. **Restrictions**- Mobile Device Manage Plus offers the admin control over some features of the device. Admins can restrict the use of these features on the devices which are a part of their organization.
3. **Geotracking**- Location Tracking feature allows the user to keep track of the location of the devices. This helps in ensuring the safety of the devices.
4. **Conditional Exchange Access**- This feature provided by Mobile Device Manage Plus allows the admin decide from which device the corporate e-mail account can be accessed. This helps in adding an extra layer of security for corporate data.
5. **Kiosk Mode**- When the kiosk mode is activated the device can access only a single app or selected few apps. This helps in ensuring that the device is not used for any other purpose than what it is intended for.
6. **Blacklisting Apps**- This feature functions as a medium to restrict the employee from installing certain apps to their devices. This is useful to prevent the use of the device for purposes other than the one it is intended for.
7. **Remote Troubleshoot-** Mobile Device Manager Plus now allows the admins to

remotely view/control mobile devices to ensure smooth functioning of devices, without actual contact with devices.

8. **Remote Wipe**- It is not always possible to prevent the device from theft or unauthorized access. Remote wipe feature helps us to wipe the devices from the MDM server without actual contact with the devices.

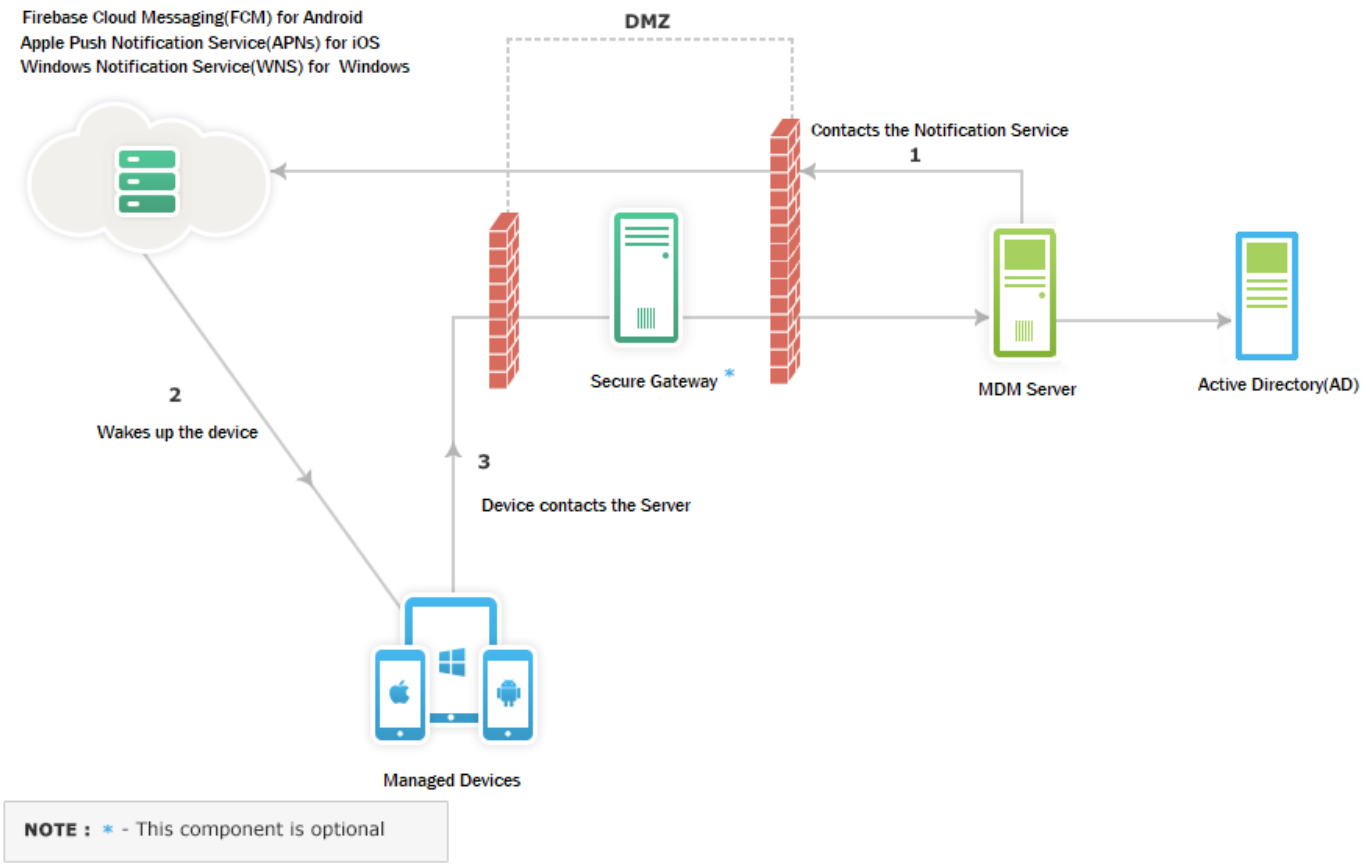
Click here know more about all the features of ManageEngine Mobile Device Manager Plus.

3. Architecture

ManageEngine Mobile Device Manage Plus is software that helps the IT admins manage devices from a single point. It helps in managing iOS, Android, Windows and Chrome device. It uses Apple Push Notification Service (APNs), Firebase Cloud Messaging Service (FCM) and Windows Notification Service (WNS) to manage all the devices wirelessly. It helps in performing Policy Management, Profile Management, Asset Management, App Management and Security Management of mobile devices.

MDM architecture provides the following advantages to the IT admins

1. It provides agentless and Over the Air (OTA) management of devices.
2. The deployed policies and profiles are applied immediately.
3. The communication to and from the devices is secured.



*- Secure Gateway is optional.

3.1 How it works

The following section explains how communication occurs between devices and the Mobile Device Manager Plus server.

1. Any communication from Mobile Device Manager Plus to the device is routed through Apple Push Notification service (APNs) via TCP **port 2195** for iOS devices and through FCM via TCP port 80 for Android Devices.
2. As per Apple iOS MDM protocol, all iOS devices maintain a dedicated TCP connection with APNs at TCP **Port 5223**. Mobile Device Manager Plus leverages this to wake up a device using APNs.
3. Device communicates with Mobile Device Manager Plus Server for available

instructions at **port 9383** using a secured connection.

4. Secure Gateway is an optional component that acts as an intermediary between the internet and the MDM server to ensure data security by not exposing the MDM server to the internet. The ports **8383 , 8031, 8443, 8027** need to be opened on the firewall while configuring the secure gateway.
5. Mobile Device Manager Plus also integrates with Active Directory to simplify user assignment and authentication processes.

3.2 Port Details

The following are the ports that are used for communication between the Mobile Device Manager Plus and the devices-

1. **TCP ports that need to be opened on the Mobile Device Manager Plus Server**
   9383 - Used for secured communication between the device and the Mobile Device Manager Plus.
2. **TCP Ports that need to be opened for managing iOS devices**
   2195, 443 - Should be opened on the proxy server/firewall for the Mobile Device Manager Plus Server to reach the APNs.

   5223 - This port should be opened on the device, if the mobile device connects to the internet through the WiFi. For better security, restrict connections on the IP range 17.0.0.0/8.
3. **TCP Ports that need to be opened for managing Android devices**
   443 - Used for secured communication between the Mobile Device Manager Plus server and the GCM server. This port should be opened on the proxy/firewall server as well as the mobile device.

   Port numbers **5228, 5229, 5230** should be open on the firewall, if the mobile device connects to the internet through WiFi. This enables communication between the mobile devices and the GCM.

4. Setup

Before we can start enrolling and managing devices with Mobile Device Manager

Plus the following configurations need to be performed.

1. NAT settings
2. Proxy Settings
3. Mail Server Settings
4. APNs Certificate

NOTE: Configuring APNs Certificates is mandatory only if iOS devices are to be managed, for managing Android and Windows devices this setup is not required. This section provides the steps to perform the various setup configurations.

4.1 NAT Settings

Mobile Device Manager Plus Server needs to be reachable at all times to manage mobile devices. Thus the server should be accessable by a public IP address to manage devices in LAN and the internet. To achieve this the NAT settings need to be configured appropriately. The user can follow any of the two approaches to configure the same.

1. Exposing the MDM server to the internet.
2. Exposing the secure gateway to the internet.

1. Exposing the MDM Server to the Internet
   In this configuration, the requests sent to the public IP address get redirected to the Mobile Device Manager Plus server.

   - **Devices in LAN**

   When the DNS name for both the public and private IP address is the same, the internal requests are directed from the internal DNS to the private IP address

instead of routing through the public IP address.

- **Devices on the Internet**

The DNS name is used to reach the public IP address which is then routed to the private IP address.

NOTE: To secure corporate data, self signed or third party certificates can be used. These certificates encrypt the communications to and from the server. These certificates use the Fully Qualified Domain Name (FQDN) to identify the server. Thus, **it is recommended to use FQDN instead of IP address.**

2. Exposing the Secure Gateway to the Internet
   A secure gateway can be created to act as an intermediary between the managed devices and the MDM server. This protects the MDM server from vulnerabilities. The secure gateway is exposed to the internet instead of the MDM server thus securing the MDM server from threats and attacks. This section explains how to set up the secure gateway.

Setting Up the Secure Gateway

Setting up the a secure gateway involves the following steps-

1. Configuring the secure gateway
2. Installing the certificates
3. Verifying the secure gateway

Configuring the Secure Gateway

1. **Download** the secure gateway.
2. Double click the exe to start installation.
3. Enter the following data-

- **Server Name**-Specify the FQDN/DNS/IP Address of the Mobile Device Manager Plus server.
- **HTTP Port Number**- Specify the port number that the secure gateway uses to contact the MDM server.
- **HTTPS Port Number**-Specify the port number that the managed devices use to contact the MDM server.

4. Click **Next.**

Installing the certificates

1. For a Self Signed Certificate copy the **server.crt** and **server.key** files located in the **ManageEngine\MDMServer\Apache\Conf** directory to the **ManageEngine\ME_Secure_Gateway_Server\nginx\conf** on the computer with the secure gateway installed.
2. For a Third Party Certificate follow the steps given below-
    1. Rename the third party certificate as **server.crt**.
    2. Rename the private key as **server.key**.
    3. Modify the file name of the intermediate certificate(if any) to **intermediate.crt**.
3. Copy the server.crt,server.key,intermediate.crt to the location where the secure gateway is installed **ManageEngine\ME_Secure_Gateway_Server\nginx\conf**.

4. Navigate to **ManageEngine\ME_Secure_Gateway_Server\conf\websetting.conf** and add the line **intermediate.certificate=intermediate.crt**.
5. The certificates have been successfully copied, click INSTALL to complete the installation.

Verifying the Secure Gateway

1. Secure gateway starts automatically. This can be verified by running **services.msc**

on the computer with the secure gateway.

2. Confirm if **ManageEngine Secure Gateway** has started.
3. The secure gateway has been successfully configured.

Whether using the secure gateway or MDM server, it is necessary to map a public IP address to the server chosen to allow the devices to contact the secure gateway. NAT configurations are performed to ensure the mapping of the server to the public IP address.

NOTE: Here's a video to help you configure the secure gateway!

Configuring NAT Settings

Follow the steps given below to configure the NAT settings-

1. Under the **Admin** tab select **NAT Settings** option.
2. The details about the **MDM Server** and the **Ports** are pre-filled.
3. Enter the **FQDN** (eg. mail.yourcompanyname.com) and **Server Port** details under **NAT Devices**.
4. Click **Save** to apply the configurations.

NOTE: The MDM server needs to be restarted for the changes to take effect.

Troubleshooting Tips

1. Verify if the certificates are copied to the correct location when third party certificates are used.
2. Ensure that the port 9383 is not used by any other application.

4.2 Proxy Settings

Mobile Device Manager Plus needs a connection to the internet to contact APNs, FCM and WNS servers and manage all the mobile devices. This connection can be established using this configuration.

Proxy Server can be configured in any of the following ways

- No connection to the internet
- Direct connection to the internet
- Manual configuration
- Automatic configuration using scripts

No Connection to the Internet

The proxy can be configured under this option if the server does not have access to the internet or if the organization works on a private network.

NOTE: Only Android and Windows devices can be managed with this setting. iOS devices require an internet connection to contact APNs. The following configuration options can be used in such cases.

Direct Connection to the Internet

If the server has direct connection to the internet the following configuration can be applied to the proxy settings.

Manual Configuration

The proxy server can be set up manually by entering the following information

- HTTP Proxy Host
- HTTP Proxy Port
- username
- password

Automatic Configuration using Scripts

The proxy server settings can be automated by using scripts. A script with all the specifications needs to be created. A Proxy Auto-Config (PAC) file defines how appropriate proxy server can be chosen for fetching a URL. Only the URL to this PAC file needs to be specified for this type of configuration.

The proxy server can be configured using scripts by providing the following details

- PAC URL
- Username
- Password

The following steps can be used to configure proxy server-

1.Under **Admin** tab select **Proxy Settings** option.

2.Click **Edit** under **Proxy** to open the setup options.

3.Choose the required configuration for the proxy server.

4.Enter the required details for the configuration.

5.Click **Save** to apply the configurations.

A message stating "HTTP proxy settings updated successfully" will be displayed.

4.3 Mail Server Settings

Mail Server Settings need to be configured to perform the following tasks-

- To send enrollment requests to users.
- To send notifications via e-mail.
- To send Inventory related details to users.
- To send e-mail reports.

Follow the steps given below to configure the mail server

1. Select **Mail Server Settings** from the **Admin** tab.
2. Enter the outgoing **Server Name** and **Port** details.
3. Enter the details of the user such as **Sender Name** and **E-mail Address**.
4. For the **E-mail Type** choose between SMTP and SMTPS.
5. Choose **Yes** if TLS is to be enabled.
6. Specify the **User Name** and **Password** if **Authentication** is enabled.
7. Click **Save** to apply the mail configurations.

A message stating "Mail Server Configuration applied Successfully" is displayed.

NOTE: A test e-mail can be sent to check if the mail server has been configured successfully. To send this test mail enter the receiver's email address under **Test e-mail Address.**

Gmail accounts can be used to configure the mail server. Follow the steps given here to configure the mail server using gmail.

4.4 APNs Certificate

Apple Push Notification Service (APNs) is the centrepiece of remote notification

feature.

To manage iOS devices APNs need to be created and added to Mobile Device Manager Plus.

The steps involved are:

1. Creating and signing CSR
2. Creating APNs
3. Creating APNs certificate

NOTE: It is not possible to enroll and manage iOS devices without adding the APNs certificate.

Creating and Signing CSR

1. Click the **Enrollment** tab and select **APNs Certificate** under **iOS** tab.
2. **Download** the Vendor Signed Document by clicking on **Download.**

Creating and uploading APNs

1. Open the Apple Push Certificates Portal and sign in using a corporate account.
2. Accept the conditions and click next to upload the Vendor Signed Certificate.
3. Upon receiving the confirmation of the creation of a new push certificate, download the certificate.
4. Upload the downloaded APNs by clicking on **Choose File** under **Locate APNs Certificate.**
5. Enter the **corporate e-mail ID** used while creating the APNs.
6. Enter the e-mail ID to which the notifications must be sent when the APNs expires.
7. Click on **Upload** to complete the process.

Upon successful addition of the APNs certificate, the page will be refreshed and will contain the details about the APNs certificate created.

NOTE: It is important to **use a corporate ID while creating the APNs certificate**. This is because the same apple ID is needed to renew the APNs on expiry. If a different apple ID is used, then all the devices that were enrolled previously will have to be re-enrolled to MDM.

Removing APNs Certificates

It may be required to remove the APNs certificates, in cases when-

1. The user forgets the Apple ID used to create the current APNs certificate.
2. The user wants to upload a new certificate after removing the current APNs certificate.
3. A new APNs certificate needs to be uploaded if the Apple ID used is changed.

Follow the steps given below to remove APNs certificate

1. Click the **Enrollment** tab and select **APNs Certificate** from **iOS** tab.
2. The details of the existing APNs certificate will be displayed.
3. Click on the **Remove APNs** button to remove the current APNs certificate.
4. The APNs certificate will be removed and the steps to add APNs certificate will be displayed.

Follow the same procedure to create and add the new APNs certificate.

NOTE: The communication between the MDM server and the managed devices should be secure at all times. ManageEngine Mobile Device Manager Plus supports Third Party Certificates to encrypt the communication. Follow these steps to use

Third Party Certificates to secure the communication.

After setting up ManageEngine Mobile Device Manager Plus, the next step is to bring the devices under management.This is achieved by using Enrollment.

5. What is Enrollment?

Enrollment of devices needs to be performed before the devices can be managed. Enrollment refers to adding the devices to the server and installing the Mobile Device Manager Plus (ME MDM) app on the devices to be managed.

5.1 Authentication

It is essential to provide some form of authentication while enrolling devices. This ensures that there are no unauthorized enrollments into the Mobile Device Manager Plus server. Mobile Device Manager Plus offers three types of authentication options to while performing enrollment.

1. OTP authentication
2. Active Directory authentication
3. Two Factor authentication

OTP Authentication: A unique passcode is generated with every enrollment and sent to the user by e-mail along with the enrollment details. This OTP is valid for 7 days and can be used only once.

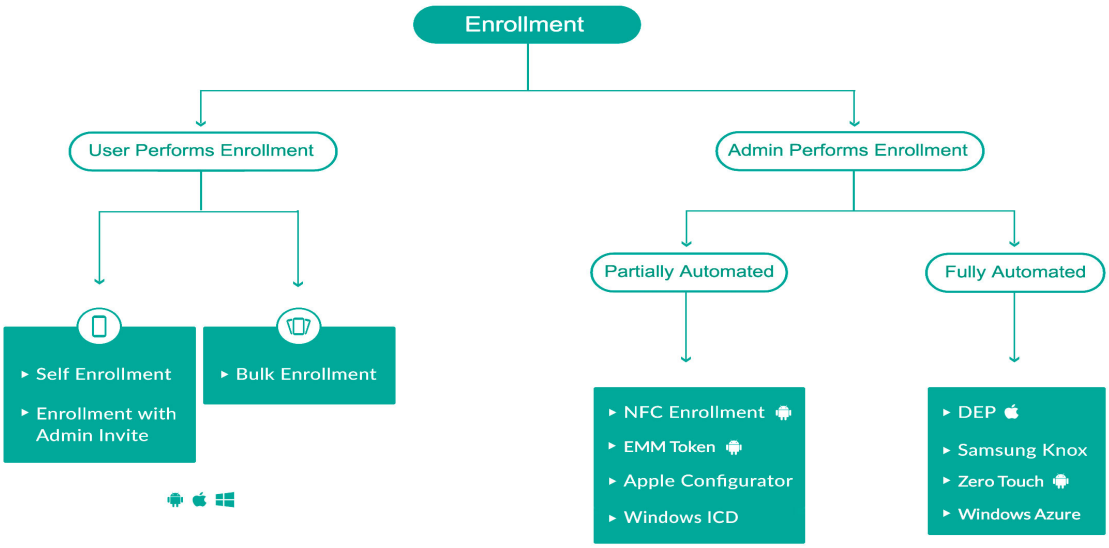
Active Directory Authentication: The user's domain login credentials are used for

authentication when AD authentication is selected.

Two Factor Authentication: This is considered to be the most secure method of authentication. When this option is selected, both the OTP and the domain credentials are required for enrolling the device.

6. Types of Enrollment

Mobile Device Manager Plus offers different types of enrollment option to meet the different needs of the user. The various enrollment options are based on various factors such as device type, number of devices to enroll. The following diagram gives the different types of enrollment.



7. Best Enrollment Methods for your Organization

This section helps in assessing which enrollment technique is most suitable for your corporate environment.

For BYOD:

1. If an organization has the following requirements, make use of **Enrollment with invites.**
    a. It does not have an Active Directory configured.
    b. Only a restricted subset of users have access to the corporate network and only these users have to enroll their devices.
    c. Contract employees, who are not present in the Active Directory are a part of the organization. Therefore, a request must be sent for enrolling devices.
    d. Evaluators assess products before an organization purchases these products. For an evaluator, this is a fuss free enrollment technique.

2. **Self Enrollment** is recommended when all the employees are present in the Active Directory and there is no condition on who can enroll a device.

For Corporate Devices:

1. For iOS devices,
    a. If a device is enrolled using **Apple Business Manager**, the device will never go unmanaged even if it is factory reset. Therefore, if an organization does not want the profiles applied to the devices to be removed or the device to be unmanaged by the user, then they can use this enrollment technique.
    b. DEP is available in a few countries, and if DEP is not available in your country use **Apple Configurator** to enroll devices.

    For the list of countries where DEP is supported, refer http://www.apple.com/business/dep/

2. For Android devices
    a. **Google Zero Touch Enrollment** can be used to enroll Android 7.0 and above corporate devices without any user intervention.
    b. **Samsung KNOX Device Enrollment** can be used to enroll Samsung devices

if the organization does not want the device to go unmanaged even when it is factory reset. The device enrolled using this enrollment method will never go unmanaged.

c. **EMM token Enrollment** can be used to enroll corporate devices running Android 6.0 and above with minimum user intervention and to provision the device as a device owner upon enrollment.
d. If the devices are not Samsung KNOX devices but support NFC, use **NFC enrollment** to enroll the devices.

For the list of supported Samsung devices, refer https://www.samsungknox.com/en/knox-supported-devices/my-knox

3. For Windows devices
   a. **Windows Azure Enrollment** automates the enrollment of corporate Windows 10 devices.
   b. If the organization has Windows 10 devices, then these devices can be enrolled using **Windows Imaging and Configuration Designer** with minimum user intervention.

It is a tedious task to send out invitations to all the employees in an organization.

Therefore, **Bulk Enrollment** can be used to send invites to multiple devices simultaneously.

8. Apple Business Manager

Apple Business Manager (ABM) is a portal provided by Apple that allows organizations to manage their devices and apps. ABM was formerly known as Apple's Device Enrollment Program. It provides a fast, streamlined way to manage corporate owned devices purchased directly from Apple or Apple authorized reseller.

Advantages of ABM

1. **Mandatory enrollment**- Using ABM for enrolling devices ensures mandatory and automatic enrollment based on the company's requirements upon device activation.
2. **Automated configurations**- The initial setup configurations can be performed over-the-air upon device activation. Large scale deployment of iOS devices can be performed seamlessly.

3. **Over-the-air supervision**- Supervision improves the control an organization can have over the devices. Extra restrictions, for example, on AirDrop, iMessage can be applied. Device supervision can be enabled wirelessly, during initial setup, when Apple Device Enrollment Program is used.
4. **Initial setup**- The initial setup of the device can be streamlined by skipping a few or all the initial steps.
5. **Device is always managed**- The devices once enrolled using Apple DEP will never go unmanaged, even if the device is factory reset. The device will be re-enrolled even if the device is erased.

Example: An organization that wants to ensure that the corporate devices are managed right out of the box and cannot be unmanaged can use Apple Business Manager to enroll their Apple devices.

Refer this document for the steps to perform enrollment using ABM.

9. Apple Configurator

Apple Configurator is a utility tool designed by Apple to enroll and manage corporate devices in an enterprise using a physical USB connection. This helps in directly enrolling multiple devices simultaneously to the Mobile Device Manage Plus server. Apple Configurator also helps configure a large number of iOS corporate devices with profiles, settings, apps and data using a physical connection to a mac machine.

Advantages of using Apple Configurator

1. **Automatic enrollment**- The devices are enrolled automatically to the Mobile Device Manager with little user intervention.
2. **Multiple device enrollment**- Multiple devices can be enrolled simultaneously using Apple Configurator.
3. **Supervise the device**- Supervision of devices refers to the extra restrictions and

control that the administrator can have over a device. Thus supervising corporate devices helps in better management of these devices.

4. **Enroll any device to ABM**- With Apple Configurator organizations can now also enroll devices that are not purchased from authorised resellers into their ABM portal and into Mobile Device Manager Plus.

Example: If the organization is located in a country that doesn't support ABM, Apple Configurator can be used to manage their corporate iOS devices.

Refer this document for the steps to perform enrollment using Apple Configurator.

NOTE: Mac devices are required to enroll devices using Apple Configurator.

10. Google Zero Touch Enrollment (ZTE) and Samsung Knox Mobile Enrollment

Similar to Apple Business Manager, Google and Samsung provide its users with Zero Touch Enrollment and KNOX Mobile Enrollment respectively. It allows IT admins to enroll multiple Android and Samsung devices in a Mobile Device Management solution without manually configuring each device. All the user has to do is, enter the reseller information into respective portals, who inturn add the devices into the portal by entering the order number.

NOTE: To perform this enrollment, the device should be purchased from a approved resellers.

Advantages of ZTE and Knox Mobile Enrollment

1. **No user interference**- This type of enrollment is completely automated and does not require any user interaction.
2. **Multiple device enrollment**- Many devices can be enrolled simultaneously as a CSV file with the device details is used to enroll the devices.
3. **Devices are always managed**- The devices enrolled using this method will never

go unmanaged, even after factory reset.

4. **Device Owner**- This type of enrollment helps us to provision the device as an Device Owner, a device administrator privilege that cannot be deactivated by the device user.

Example: An organization with a large number of corporate devices can use either ZTE or Knox Mobile Enrollment to enroll these devices simultaneously without any user intervention.

Click here for the steps to perform Samsung KNOX Mobile Enrollment.

Click here for the steps to perform Zero Touch Enrollment

11. EMM Token Enrollment

EMM token enrollment is the 3 step process to enroll and provision Android devices as device owner. On the device to be enrolled, admin enters the EMM token "afw#memdm" to automatically install the ME MDM app into the device and scan a QR code to complete the process.

Advantages of EMM Token Enrollment

1. **Easy Enrollment-** With EMM token enrollment the device is enrolled and ready for corporate use in just 2 steps.
2. **Time Saving**- The enrollment process is simple and does not consume too much time.
3. **No user intervention**-The user is not involved in the enrollment process, the admin directly enrolls the devices into the Mobile Device Manage Plus server.
4. **Device Owner**- This type of enrollment helps us to provision the device as an Device Owner, a device administrator privilege that cannot be deactivated by the device user.

Example: Organizations can use EMM token enrollment to simplify the enrollment of corporate devices not purchased from authorised resellers. EMM token enrollment also helps in provisioning devices running Android 6.0 and above as

device owner.

Click here for the steps to perform EMM token Enrollment.

12. NFC Enrollment

NFC Enrollment makes use of the ManageEngine NFC Enrollment App to enroll Android devices to the ManageEngine Mobile Device Manager Plus server. This type of enrollment is useful for enrolling corporate devices.

Advantages of NFC Enrollment

1. **Easy Enrollment-** NFC enrollment is a no fuss, easy to perform enrollment method. The device to be enrolled needs to be bumped with the device installed with the NFC Enrollment App, known as the admin device to perform the enrollment.
2. **Time Saving**- The enrollment process is simple and does not consume too much time. The device can be enrolled by just a single bump with the admin device.
3. **No user intervention**-The user is not involved in the enrollment process, the admin directly enrolls the devices into the Mobile Device Manage Plus server.
4. **Device Owner**- This type of enrollment helps us to provision the device as an Device Owner, a device administrator privilege that cannot be deactivated by the device user.

Example: An organization can make use of NFC enrollment to enroll and provision their corporate Android devices as device owner if these devices support NFC and are running on Android below 6.0.

Click here for the steps to perform NFC Enrollment.

NOTE: This Device Owner privilege is required for performing some extra device management tasks such as configuring Exchange ActiveSync for non-Samsung devices, silent installation of Play Store and Enterprise apps.

13. Windows Azure Enrollment

Similar to the other portals, Windows Azure Enrollment provides the admin an option to integrate with Mobile Device Manager Plus to automate the enrollment process of Windows 10 devices. All the user has to do is, enter the reseller information into portal, who inturn add the devices into the portal by entering the order number.

NOTE: To perform this enrollment, the device should be purchased from approved resellers.

Advantages of Windows Azure Enrollment

1. **No user interference**- This type of enrollment is completely automated and does not require any user interaction.
2. **Multiple device enrollment**- Many devices can be enrolled simultaneously as a CSV file with the device details is used to enroll the devices.
3. **Devices are always managed**- The devices enrolled using this method will never go unmanaged, even after factory reset.

Example: An organization with a large number of corporate Windows 10 devices can use Windows Azure Enrollment to enroll these devices simultaneously without any user intervention.

Click here for the steps to perform Windows Azure Enrollment.

14. Enrollment using Windows ICD

Windows Imaging and Configuration Designer (ICD) can be used to enroll multiple Windows 10 devices to the Mobile Device Manager Plus server. It is a fully automated enrollment options that can be used to enroll corporate devices into the Mobile Device Manager Plus server.

Advantages of Windows ICD Enrollment

1. **No user interference**- It is a completely automated enrollment technique that does not involve any user intervention.
2. **Multiple device enrollment**- Multiple devices can be enrolled into the server simultaneously.
3. **Also suitable for BYOD**- This method of enrollment can also be performed for BYOD without any extra effort.
4. **Apply Restriction on activation**- It allows the user to apply preconfigured restriction on the devices once the device is activated.
5. **App distribution on activation**- Apps can be distributed to the device immediately upon activation.

NOTE: This enrollment can be used to enroll only Windows 10 devices.

The steps to perform enrollment using Windows ICD are listed here.

TIP: Admins can create the PPKG file and send it to the users whose devices need to be enrolled.

15. Enrollment with Invitation

Enrollment using invites is the most popularly used method of enrolling mobile devices. It can be used to enroll iOS, Android and windows devices to the ManageEngine Mobile Device Manager Plus server.
The user receives the enrollment details as an e-mail from the administrator and completes the enrollment process.

Advantages of Enrollment with invites

1. **Easy procedure**- This is the simplest method to enroll mobile devices to the ManageEngine Mobile Device Manager Plus server. The user only needs to enter the enrollment details received in the e-mail into the Mobile Device Manager App.
2. **Suitable for BYOD**- This enrollment type is preferred when enrolling BYOD devices. This is because the user is the one to complete the enrollment process.

Example: A company which uses BYOD devices can make use of this enrollment. When a new employee joins the company, an e-mail can be sent to the user with the enrollment details and the device can be enrolled by the user.

NOTE: It is preferred to use either admin enrollment (Enrollment performed by admin) or the following types of enrollment in case the number of devices to be enrolled is large.
User Enrollment can be performed for Apple, Android and Windows devices.The steps to enroll Apple devices using invites is given here.
To perform enrollment of Android devices using invites, refer this document.
Windows devices can be enrolled using invites by following the given steps.

16. Bulk Enrollment

It becomes a tedious task for the IT Admin to enter the details of individual devices in the ManageEngine Mobile Device Manager Plus server and send the enrollment request. Thus, bulk enrollment is the required alternative. The IT admin needs to create a CSV file with the device and user details. An e-mail will be sent to all the users simultaneously. Thus multiple BYOD can be enrolled simultaneously using bulk enrollment.

Advantages of Bulk Enrollment

1. **Multiple device enrollment**-Large number of devices can be enrolled simultaneously by just creating a CSV file.
2. **Minimal admin interaction**-Since the enrollment is completed by the user, the admin only needs to create the CSV file for enrollment. There is no direct involvement of the admin in the enrollment process.
3. **Suitable for all types of devices**-Bulk enrollment can be used for all types of devices- iOS, Android and Windows.

Example: Employees bring different types of devices to an organization, Bulk Enrollment can be used to enroll these devices. Since all the types of devices can be added to the same CSV file, the type of device does not play a major role in bulk enrollment.

The steps to perform bulk enrollment are given here.

17. Self Enrollment

Self Enrollment is used mainly for BYOD. It does not require the admin to send an invite to the device user. The user enrolls the device by accessing the enrollment URL available on the server. The company provides the URL to the employees using internal forums, blogs mails, etc and the user then completes the enrollment process by using AD authentication.

Advantages of self enrollment

1. **No admin involvement**- There is no involvement from the admin side, the user accesses the enrollment URL and performs the enrollment.
2. **No unauthorized enrollment**-Even though the enrollment URL can be accessed by any person, AD authentication ensures that only authorized people can complete the enrollment process.
3. **Single user,multiple devices**- Self enrollment helps when a single user wants to enroll multiple devices. The user accesses the enrollment URL from the different devices and enrolls them.

Example: Self Enrollment is very useful in companies with a large number of employees using BYOD. The enrollment URL can be published and can be accessed by all the employees who want to enroll their devices.

NOTE: It is not possible to track the user or the devices in case of failed enrollment.

Follow the steps given in the document to perform self enrollment.

18. Managing Mobile Devices

Once the device has been enrolled into the ManageEngine Mobile Device Manager Plus server, the devices can be managed as per users requirements.
The following diagram helps in understanding the device management process and the features ManageEngine Mobile Device Manager Plus offers to manage devices.

1. Enrollment	• Enroll Devices
2. Inventory	• Details like IMEI number and UDID retrieved
3. Maintaining Groups	• Create Groups as per Requirements • Add devices to the appropriate Groups
4. Profiles	• Create Profiles with Restrictions • Apply Profiles to Groups / Devices
5. App Management	• Add apps to the Repository • Distribute apps to the Groups/Devices • Blacklist apps
6. Reports	• Reports generated based on criteria like jail broken devices etc
7. Device Security	• On demand Geo-Tracking • Remote Alarm to locate the devices • Reset password • Complete Wipe the device
8. Retiring Devices	• Revoke License • Corporate Wipe BYOD or Complete Wipe Corporate devices • Unmanage Device

Please refer the following for more details on ManageEngine Mobile Device Manager Plus.

1. https://www.manageengine.com/mobile-device-management/how-to.html
2. https://www.manageengine.com/mobile-device-management/knowledge-base.html
3. https://www.manageengine.com/mobile-device-management/faq.html

Feature Request: If there are features required for your organization, please raise a "Feature Request" and we will add it to our Roadmap.

Write to us at
On-Premises: mdm-support@manageengine.com
Cloud: mdmcloud-support@manageengine.com
For any queries Call our Toll free : +1-888-720-9500