

Device enrollment for iOS devices

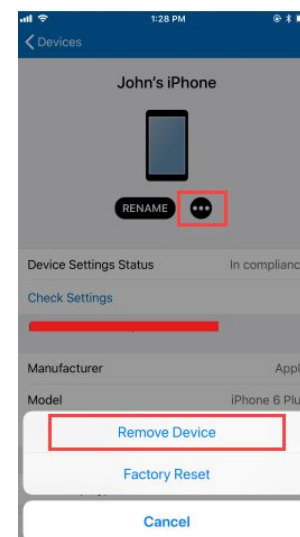
Device enrollment for iOS devices

Prerequisites for enrolment :

- Device OS should be updated to the latest version of iOS: 17.0 or above.
- Okta Verify application must be installed and configured as per the instructions provided.
- Devices should not be rooted/jail broken.
- Devices should not be enrolled with any other Mobile Device Management (MDM) solution. Follow the below steps to unenroll if your device is enrolled with any other MDM Solution.
- Configuration time will take around 20 minutes depending upon your wifi connection.

Steps to unenroll from existing MDM (Intune)

Open Intune Company Portal → Devices → Select your device → Tap on the Three dots → 'Remove Device'.



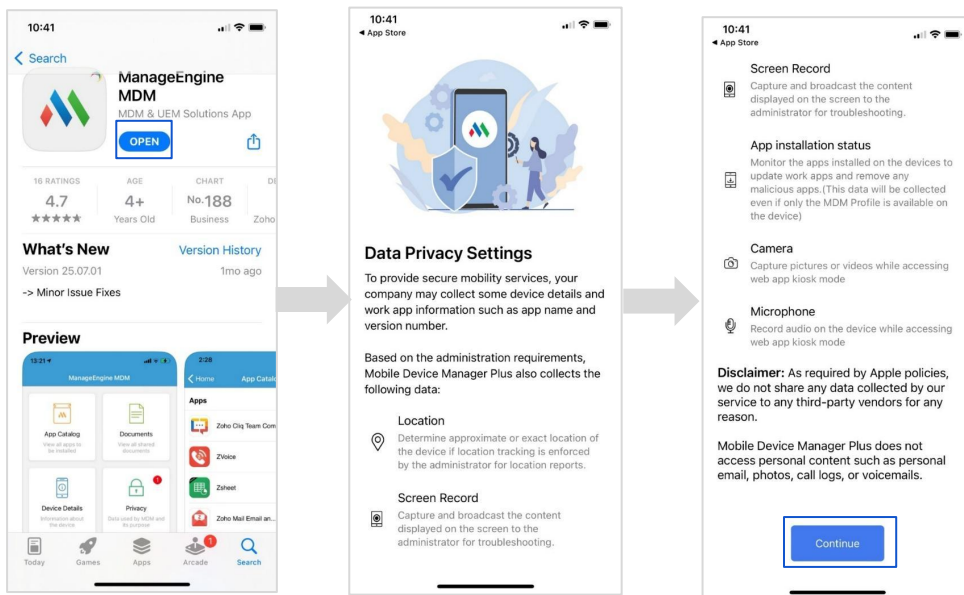
Steps to enroll to ManageEngine (1/4)

01

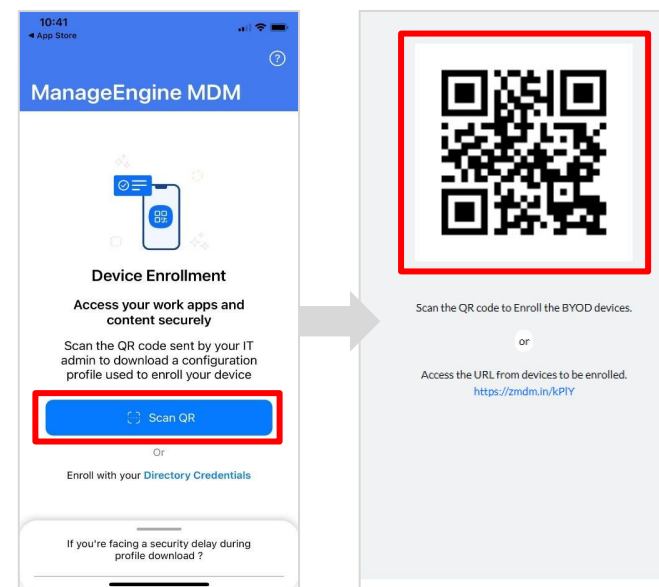
Install and configure Okta Verify application (If not done already).

02

Install 'ManageEngine MDM' application from App Store and open and click on continue.



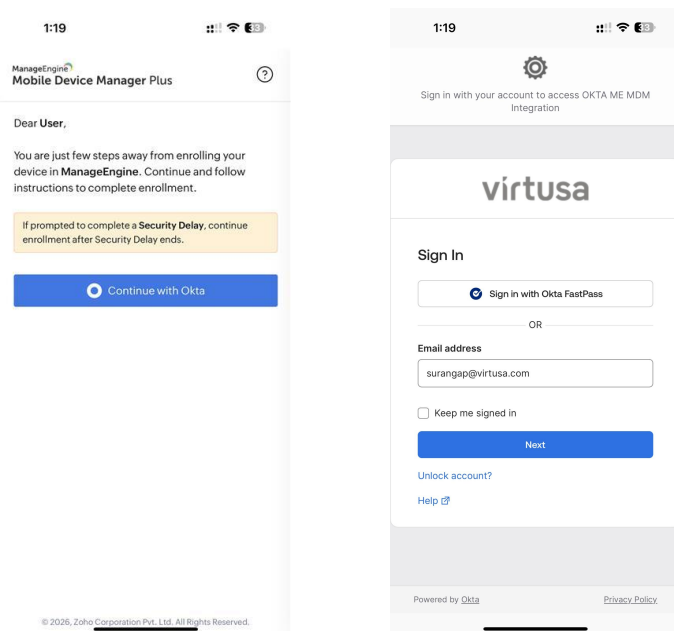
OR Scan the QR Code from the Device Camera or inbuilt QR Scanner OR access the Enrolment link [Https://zmdm.in/kPIY](https://zmdm.in/kPIY) from the Safari browser



Steps to enroll to ManageEngine (2/4)

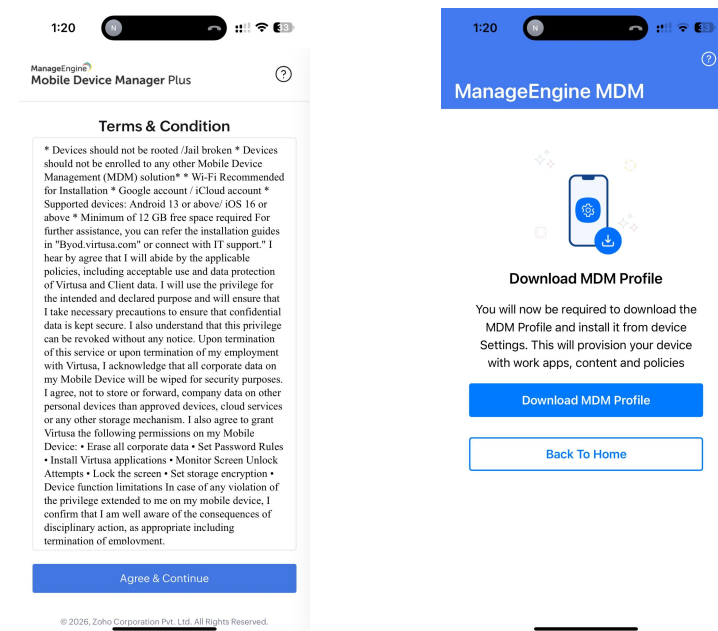
03

Okta Verify login page will open. Click 'Continue with Okta' to complete Okta verification.



04

Agree to the terms and conditions and click 'Download MDM Profile'

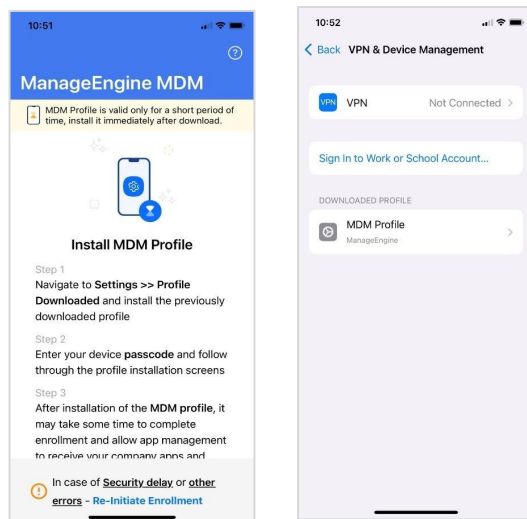


Steps to enroll to ManageEngine (3/4)

05

Once the profile is downloaded, open the settings app on your device and select the downloaded MDM profile at the top of the settings listing.

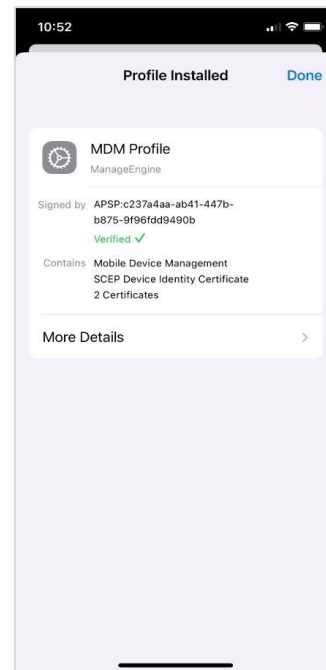
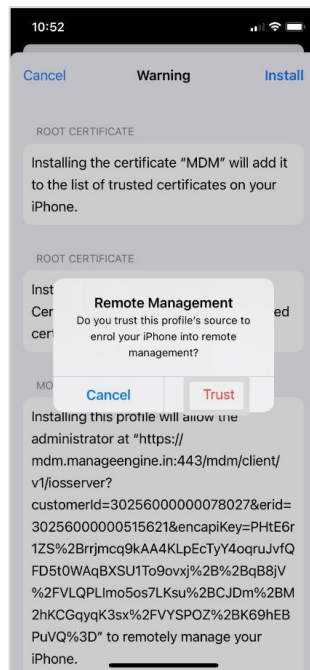
If you can't find it, navigate to the Settings > General > VPN & Device Management section in your device and select the downloaded profile.



Steps to enroll to ManageEngine (4/4)

06

Tap Install in the upper-right corner and enter your device passcode if prompted to complete the installation process. When prompted, "Do you trust this profile's source to enroll your iPhone into remote management?", choose Trust.

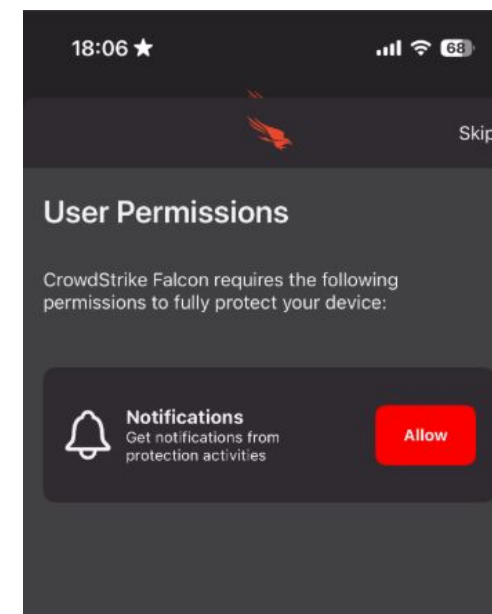


07

Once the MDM profile is installed, the device is automatically enrolled in MDM. All mandatory Virtusa apps will prompt to install. Tap Install. If Admin configured any policies and configurations after enrolment, MDM will apply all relevant policies and configurations to the device.

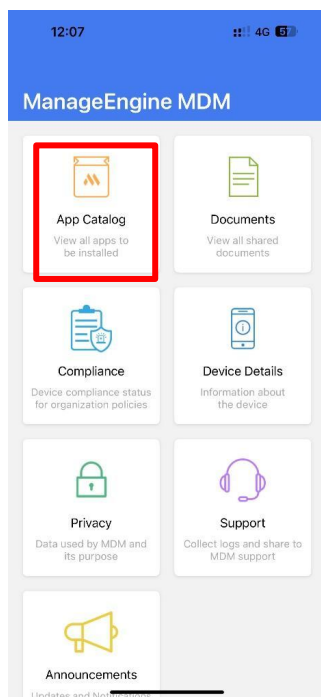
Additional notes

- Verify all the Mandatory apps installed in the device. Mandatory apps include:
 - Sheets
 - Slides
 - Gemini
 - Google
 - Calendar
 - Meet
 - Drive
 - Docs
 - Chat
 - Gmail
 - Chrome
 - Okta Verify
 - Edge
- Open **CrowdStrike** application. It will be automatically configured once all the mandatory applications are installed and synced with ME.
- Click '**Allow**' for enabling notifications.

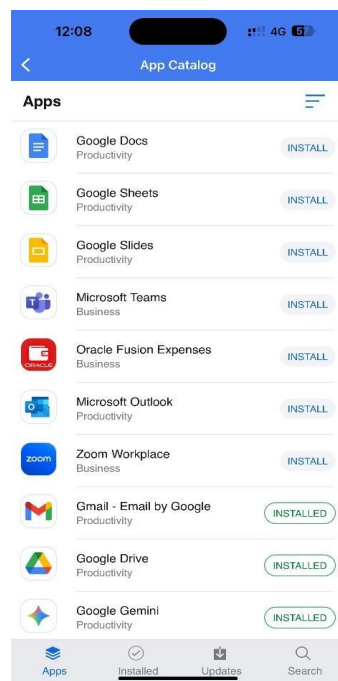


Teams App configuration steps:

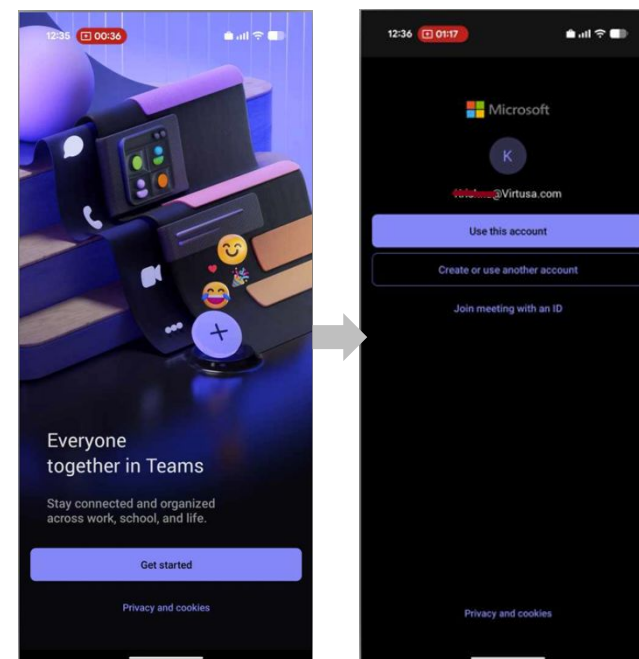
- Open the **ME MDM application** in your mobile and click on **'App Catalog'**.



- Install Teams, Outlook, MS Authenticator, Intune Company Portal App if need to access Teams or Outlook.



- Configure the MS Authenticator app.
- Open Teams application, click **"Get Started"**.
- Enter your Virtusa account credentials and configure.



iOS Gmail login process

ME MDM device enrollment

01

You can refer to the “**Virtusa - Mobile Device Enrollment guide**” for step by step process.

02

Once the enrolment is finished, Virtusa apps will be installed automatically. You can access the downloaded apps in your phone's work profile section.

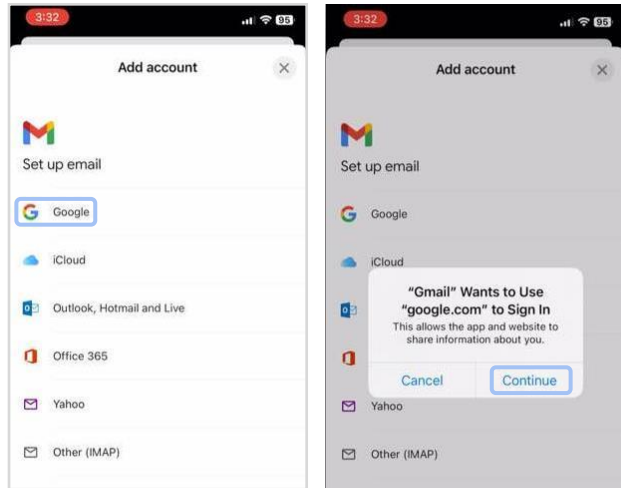
Sign in into your Gmail account

01

Open the Gmail application on your phone and click on **Add Account**.

02

Select **Google** and click on **Continue**.

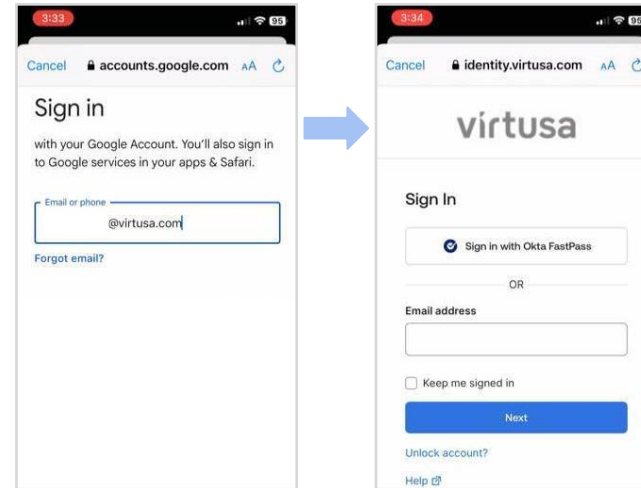


03

Enter your email address and click **Next**.

04

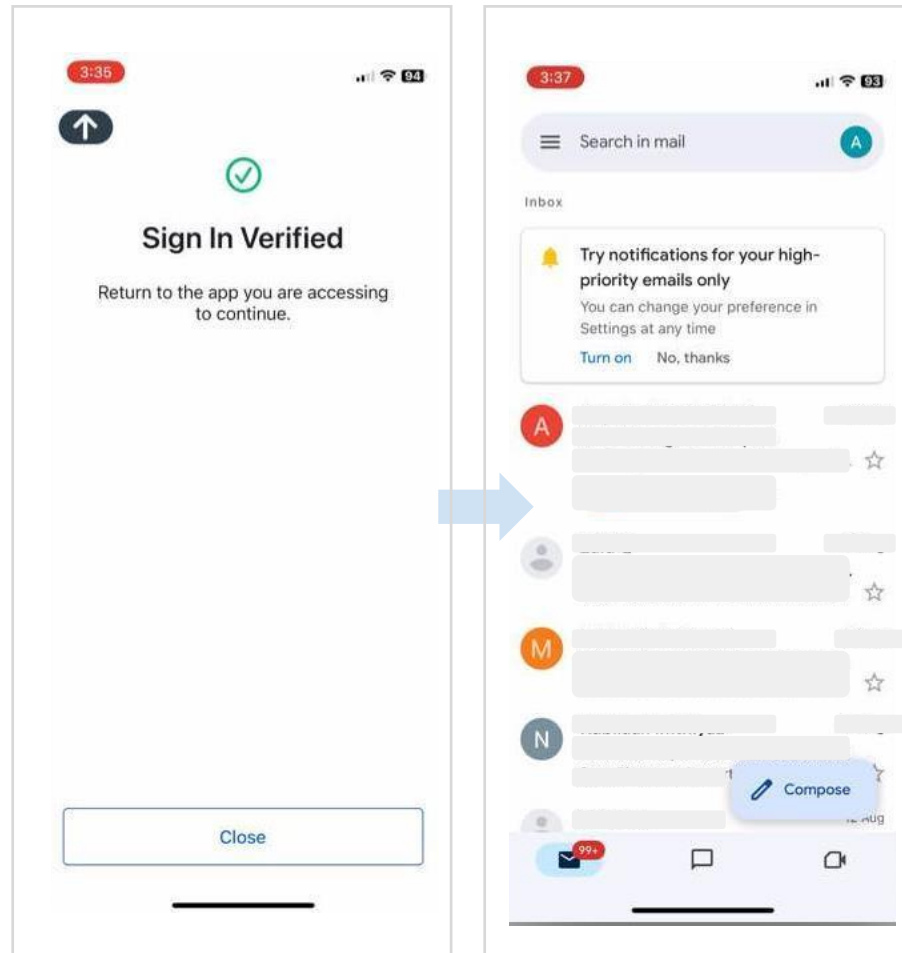
You will be redirected to Identity portal.



STEP 3

Complete the MFA process

Enter your email address and you click next. You will be signed in to your Gmail account automatically.





Thank you