BYOD Enrollment

User-guide for iOS Devices

[Version 1.5 – April 17, 2023]

vírtusa

1)   Virtusa BYOD Program

The Virtusa BYOD (Bring Your Own Device) program allows all Virtusa employees to access corporate data and applications from Apple and Android mobile devices using Intune secure Mobile Device Management (MDM) platform.

The program is intended to provide access to Virtusa information whilst keeping your device secure without interfering with your personal information and settings. It also provides you the additional feature of wiping the device in situations where it is lost or stolen.

2)   Prerequisites for Enrollment

- Device OS should be updated to the latest version of iOS: 13.0 or higher
- Devices should not be rooted/jail broken
- Devices should not be enrolled with any other Mobile Device Management (MDM) solution
- Minimum of 600 MB free space should be available in the device prior installation
- An iCloud ID is required, and Wi-Fi connectivity is preferred for enrollment
- Configuration time will take around 15 minutes

3)   Virtusa BYOD Portal

The Virtusa BYOD portal provides a comprehensive view on the MDM solution provided by Virtusa for its employees. This portal will guide and assist employees in the entire journey of enrolling, managing and unenrolling devices. You can access this site by:
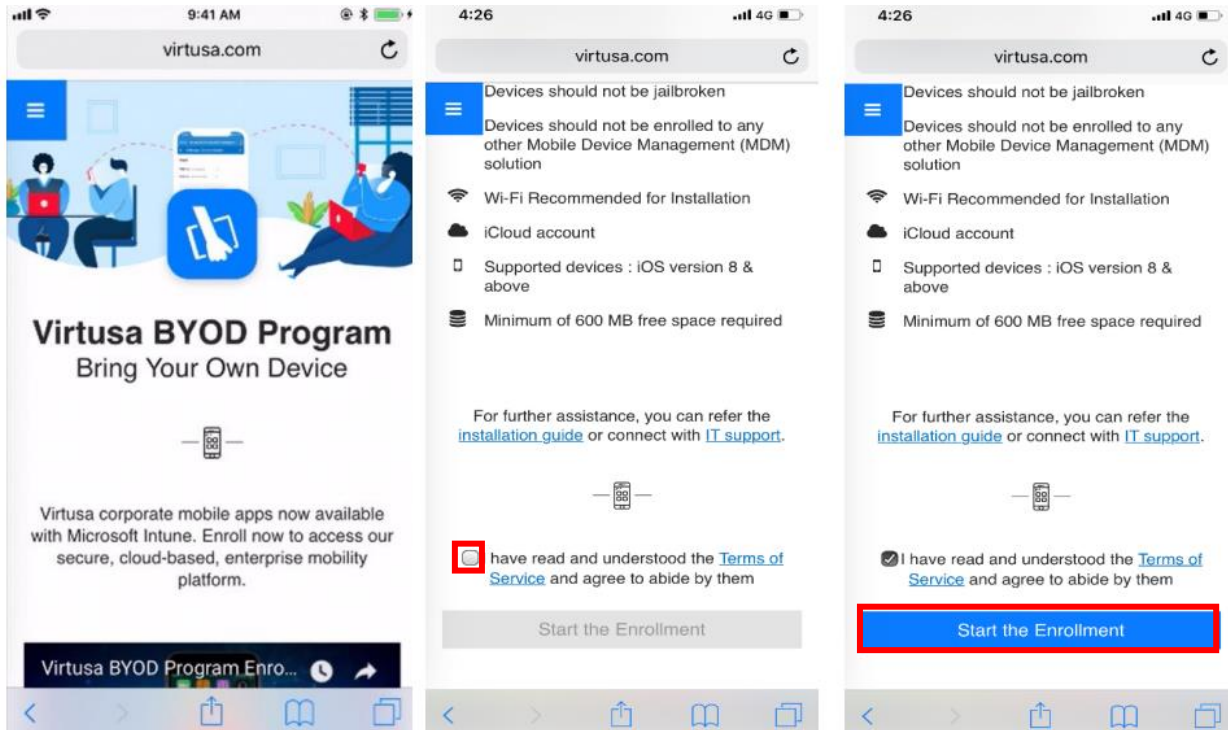
- **Scanning the below QR code**

- **Typing byod.virtusa.com on your mobile device browser**
  In addition to the information on default and featured apps available in the program, the BYOD portal is also equipped with videos and guides to assist you in enrolling devices. Before the enrollment process please review the terms of use available in the portal to understand what Virtusa can see and cannot see

Transform the way we work, learn, share and connect.

4) BYOD (Intune MDM) Enrollment Steps

Step 01: Visit the Virtusa BYOD Portal **<byod.virtusa.com>** via your mobile device
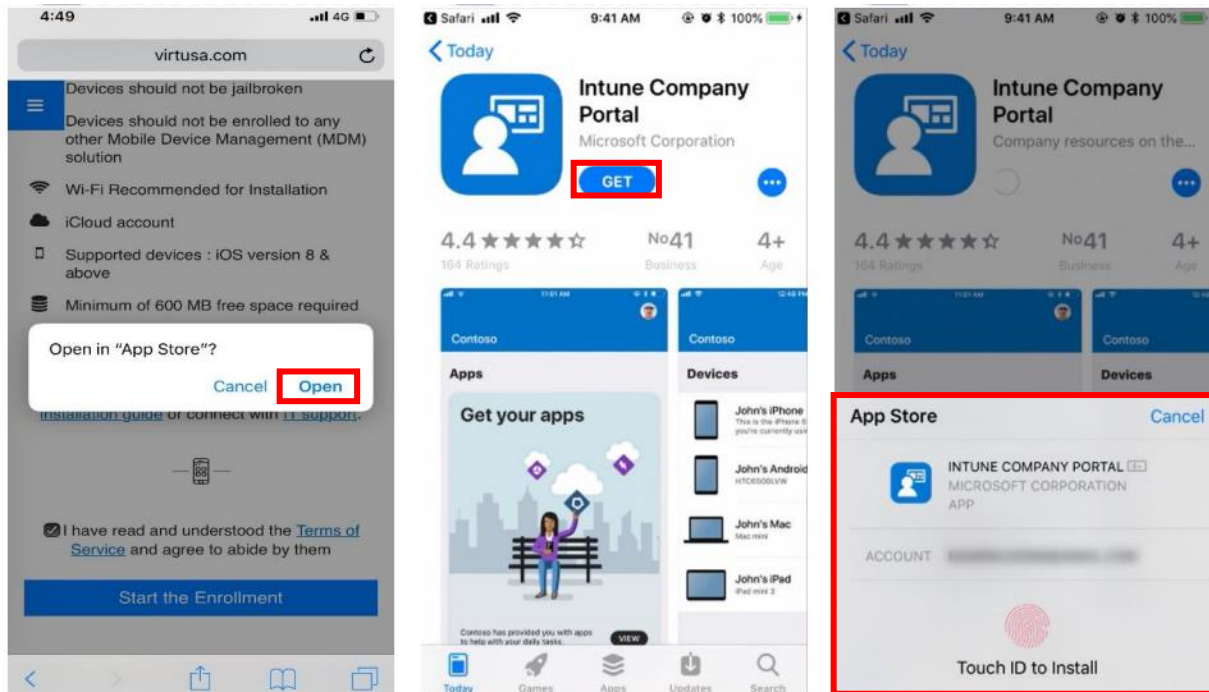
Step 02: Read and accept the **Terms of Service**

Step 03: Tap on 'Start the Enrollment'

Step 04: Tap on 'Open' to open the App Store

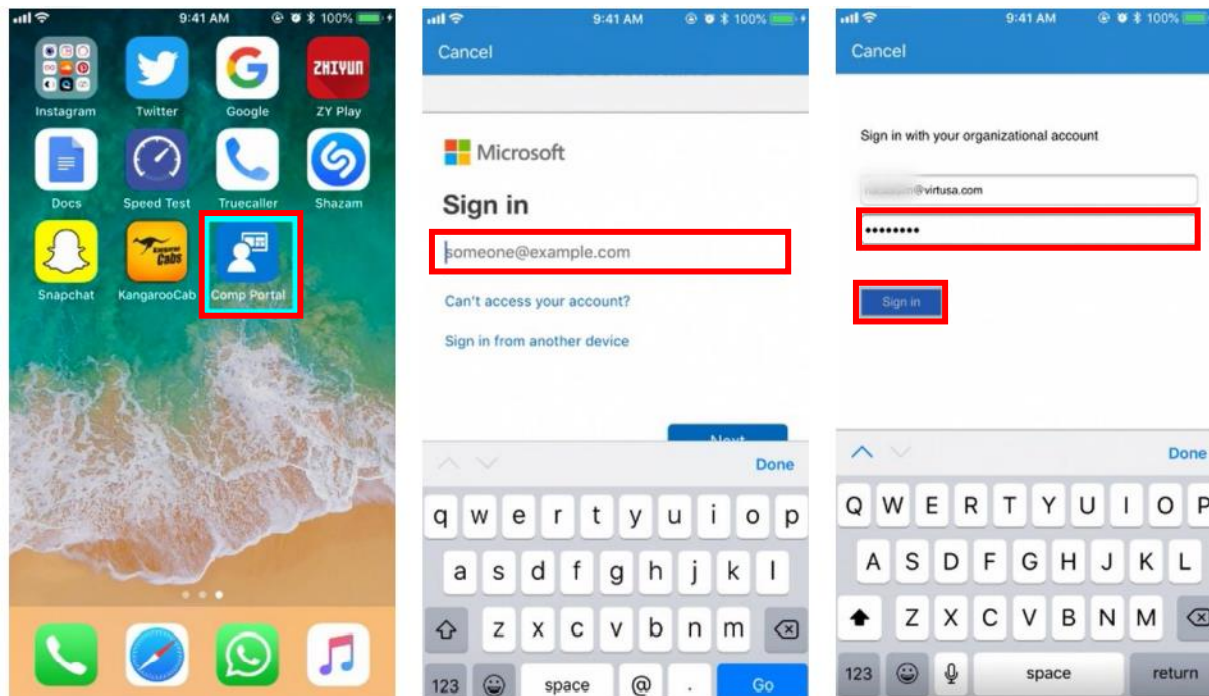Step 05: Tap on 'Get' to install the Intune Company Portal app

Step 06: Authenticate to start the installation

5

Step 07: Open the Company Portal app after installed

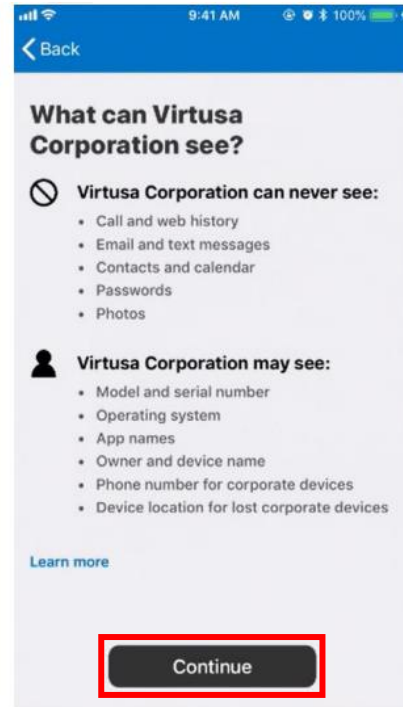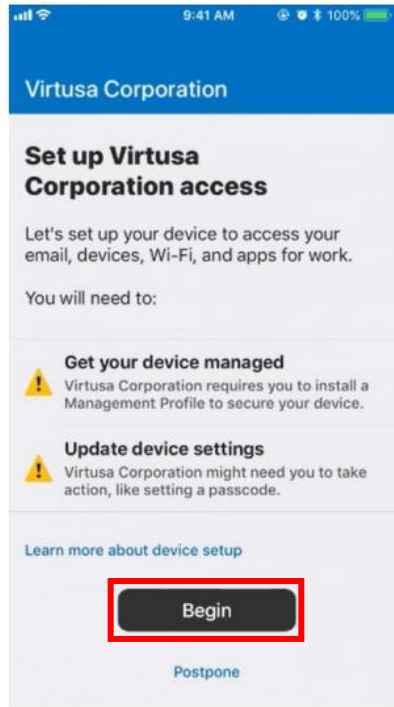Step 08: Enter your Virtusa username (e-mail address) and tap on 'Next'
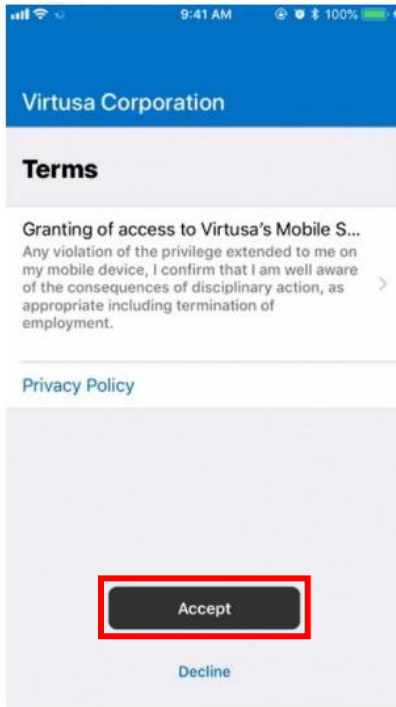
Step 09: Enter your Virtusa password and tap on 'Sign in'

6

Step 10: Read and tap on 'Accept' to proceed further

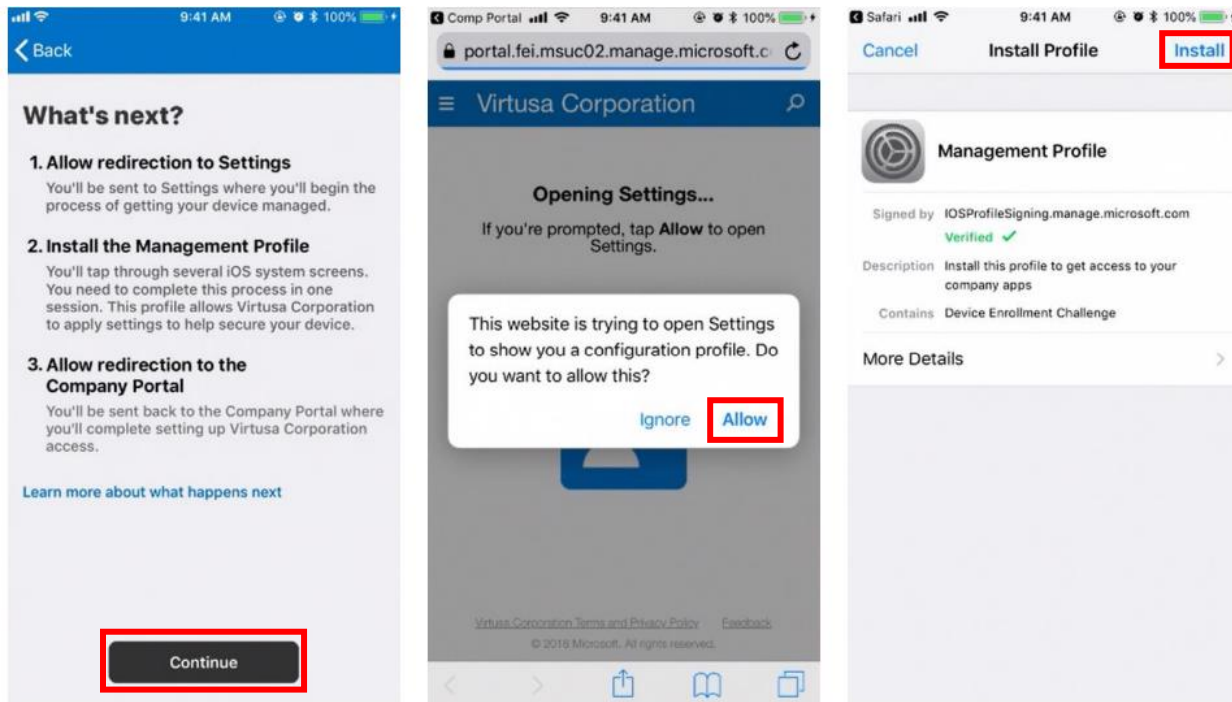Step 11: Tap on 'Begin' to start the configuration

Step 12: Read and tap on 'Continue' to proceed

Step 13: Tap on 'Continue'
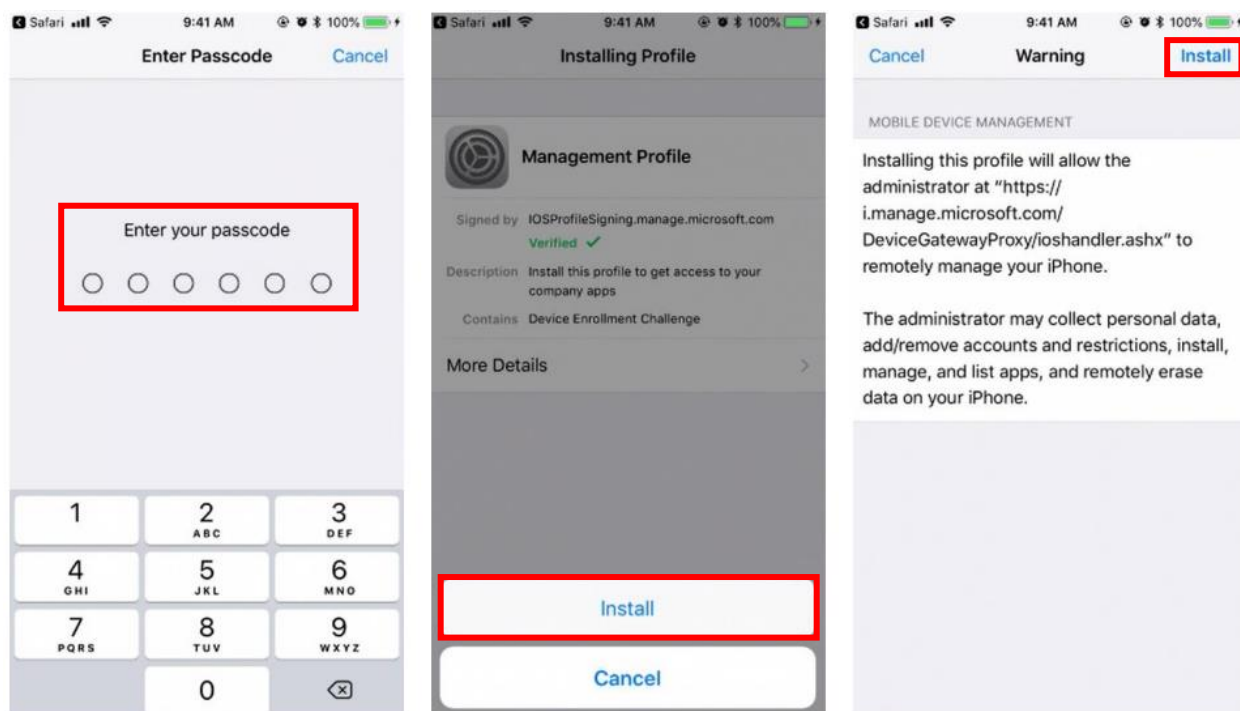
Step 14: Tap on 'Allow'

Step 15: Tap on 'Install' to update the Mobile Device Management Profile

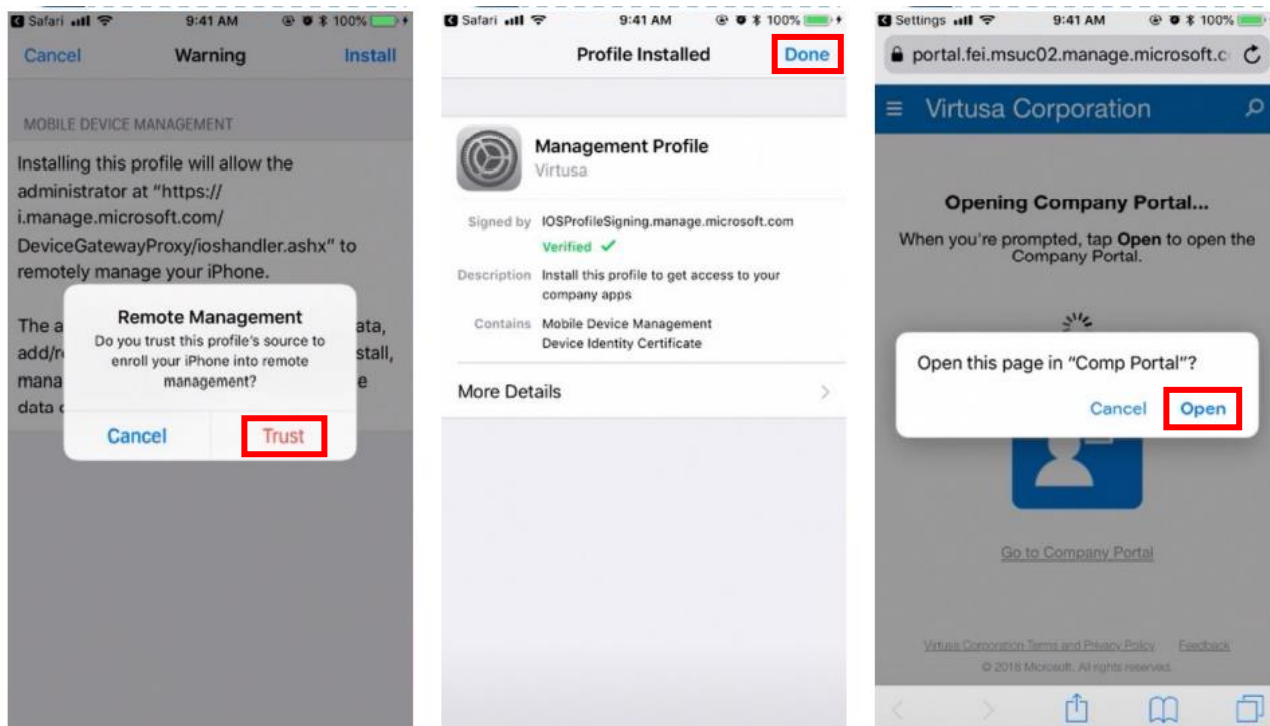Step 16: Enter your device passcode

Step 17: Tap on 'Install'

Step 18: Tap on 'Install'

Step 19: Tap on 'Trust'

Step 20: Tap on 'Done' when the installation is completed
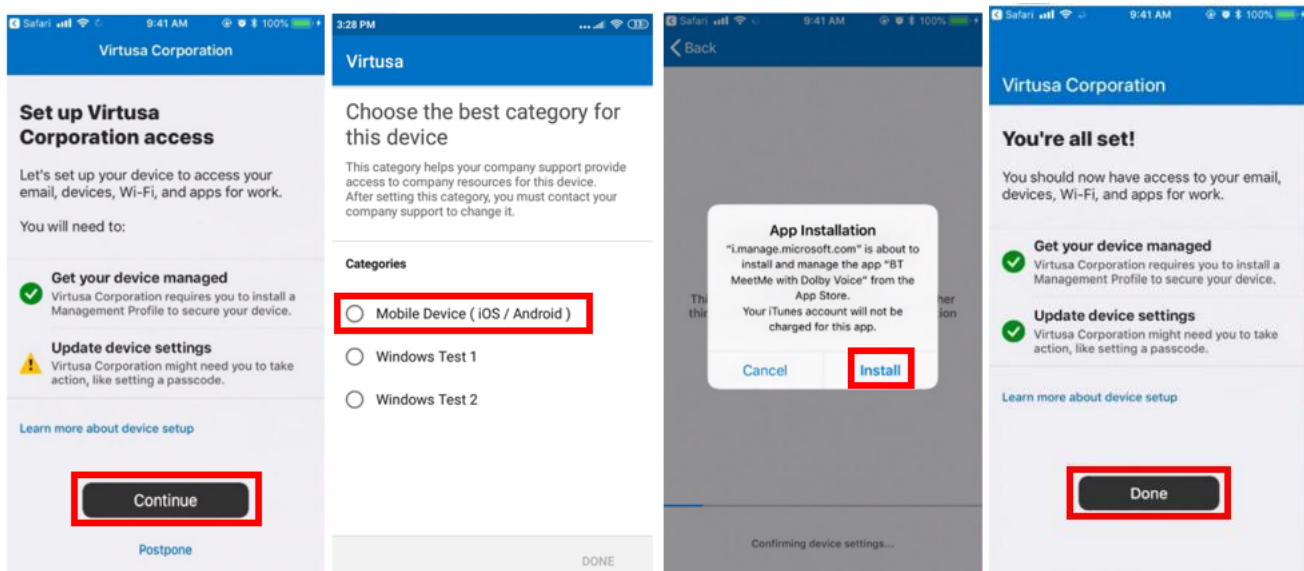
Step 21: Tap on 'Open'

Step 22: Tap on 'Continue'

Step 23: Select 'Mobile Device (iOS/ Android)' as the category

Note: You will now be prompted to install the default Virtusa apps [Edge, Authenticator, Teams, Outlook, and Microsoft Defender]. The **Microsoft Defender** app is a mandetory app for Tier 0, Tier 01, Tier 02 and Tier 05 employees excluding Tier 03 and Tier 04 to complete the mobile device enrollemt. This app protects your device and its applications from cyber security threats.

Step 24: Tap on 'Install' as prompted to get these apps

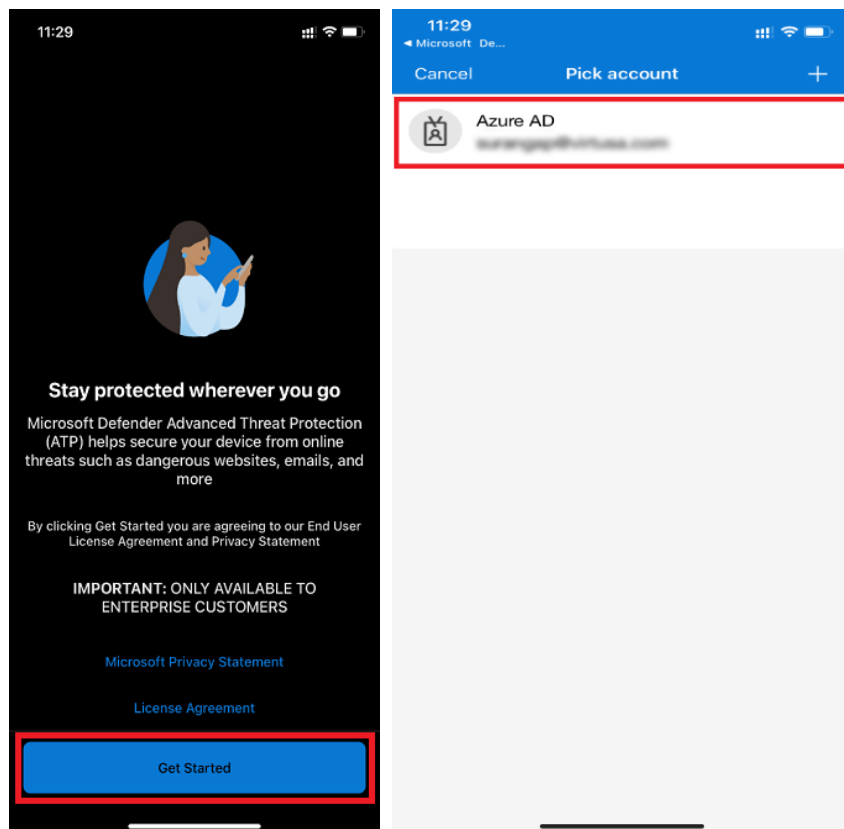Note: The apps will be available on your mobile home screen once installed.

Step 25: Tap on 'Done' to complete the process

5)   Microsoft Defender Configuration Steps

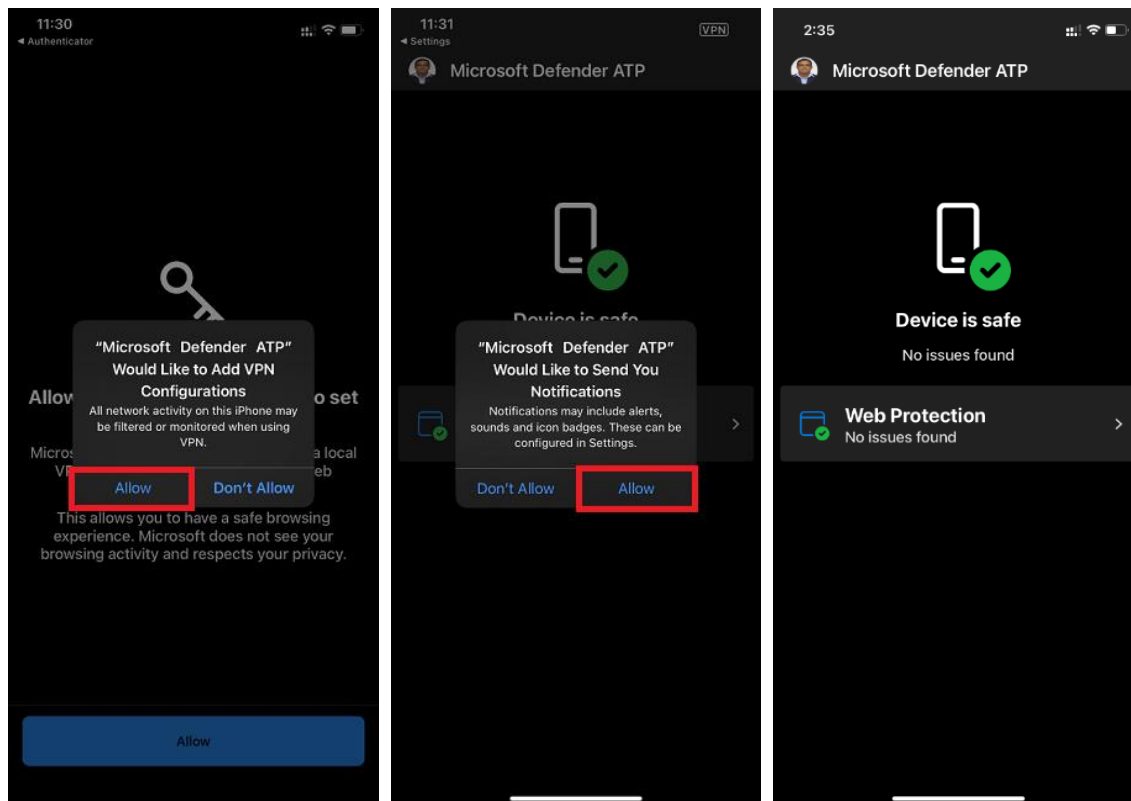Step 1: Open the Microsoft Defender for Endpoint app and tap on 'Get Started'

Step 2: Tap on your Virtusa account

Step 3: Tap on 'Allow'

Step 4: Tap on 'Allow'

Note: Your device enrollment is now completed.

Transform the way we work, learn, share and connect.