virtusa

BYOD enrollment

User-guide for iOS devices

1. Prerequisites for enrollment

- Device OS should be updated to the latest version of iOS 16.x or above.

- Devices should not be rooted/jail broken.

- Devices should not be enrolled with any other Mobile Device Management (MDM) solution.

- An iCloud ID is required, and Wi-Fi connectivity is preferred for enrollment.

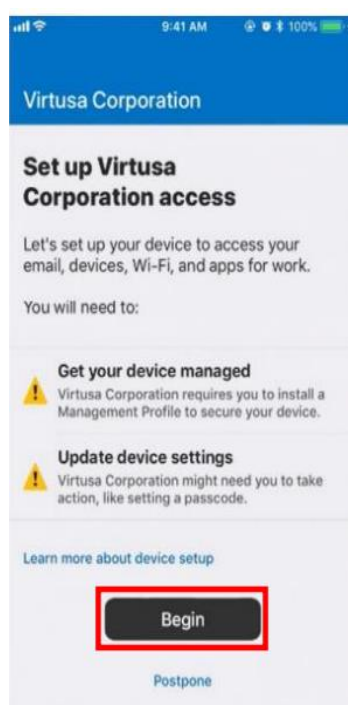- Configuration time will take around 15 minutes.

2. Enrollment steps

Step 1: Install the 'Intune Company Portal' app from the Apple App Store, and sign in using your Virtusa username (email ID) and password.
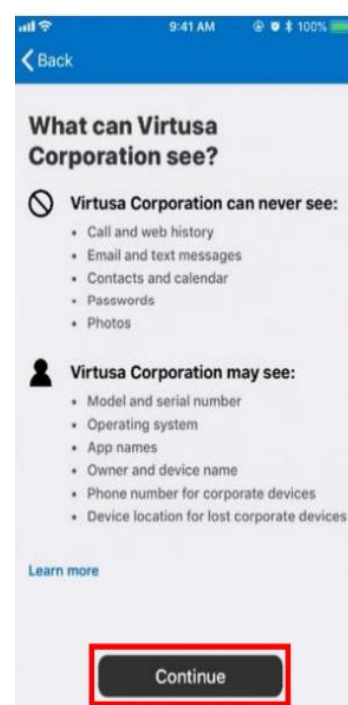
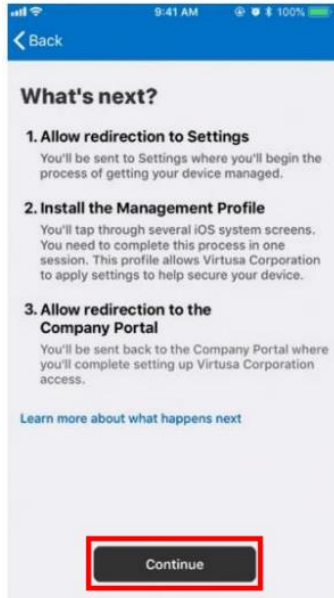**Step 2:** Read and tap on 'Accept all' to proceed further.
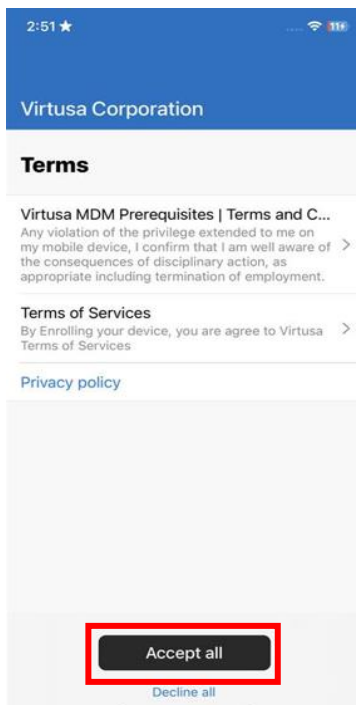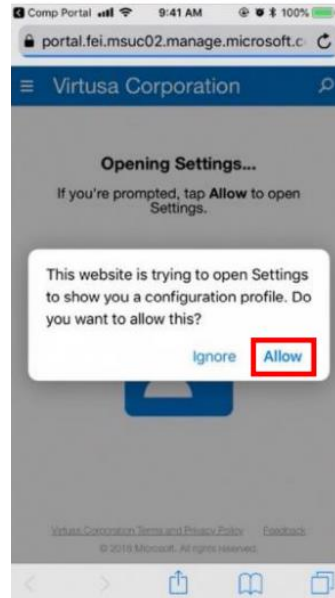
Step 3: Tap on 'Begin' to start the configuration

Step 4: Tap on 'Continue' to proceed.
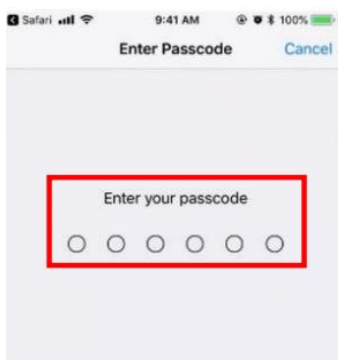
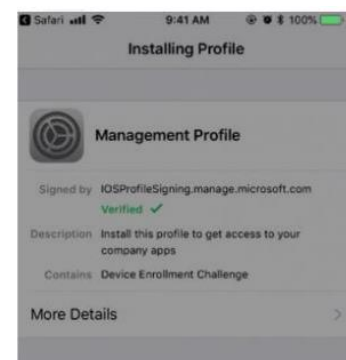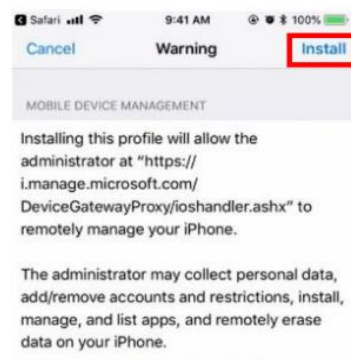**Step 5:** Tap to continue'

Note: Tap on 'Allow'.

Step 6: Tap on 'Install' to add the Mobile Device Management Profile - (Settings > General > VPN & Device Management).
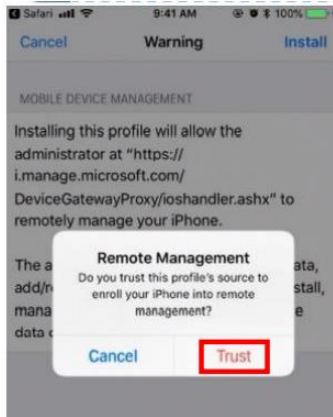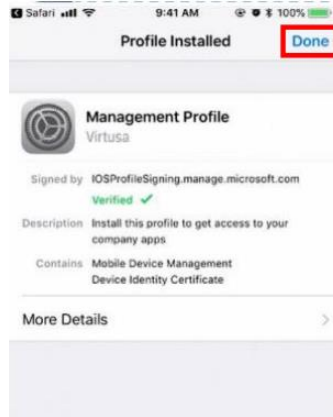

Note: Enter your device passcode

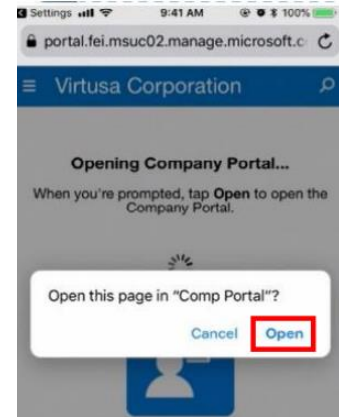**Step 7:** Review the warning message and tap on 'Install' to update the Profile..

Step 8: Tap on 'Trust'
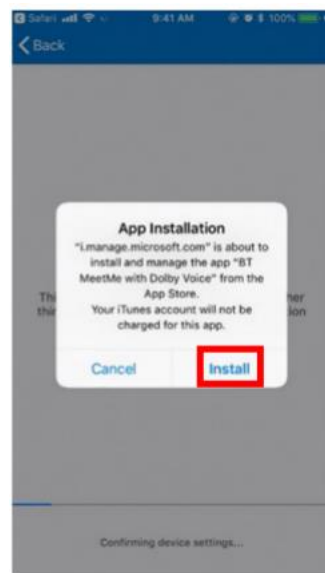

Step 9: Then tap on 'Done'

Step 10: Once the installation is completed, tap on 'Open'
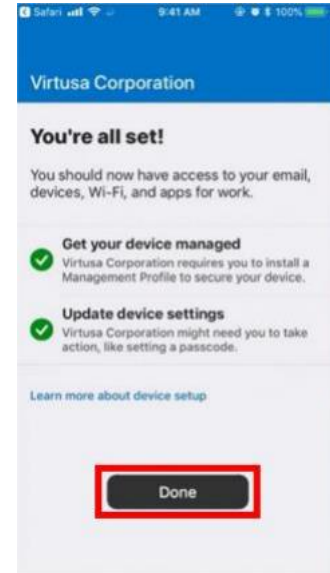

Step 11: Step 13: Tap on 'Continue'

Step 12: Tap on 'Install' as prompted to get the default company apps on your mobile.

Step 13: Tap on 'Done' to complete the process.

Note: You'll be prompted to install the default Virtusa apps [Edge, Authenticator, Teams, Outlook, and Microsoft Defender]. Microsoft Defender is mandatory for Tier 0, 1, 2, and 5 employees. Tier 3 and 4 employees can skip the Defender installation steps, as they are not eligible.
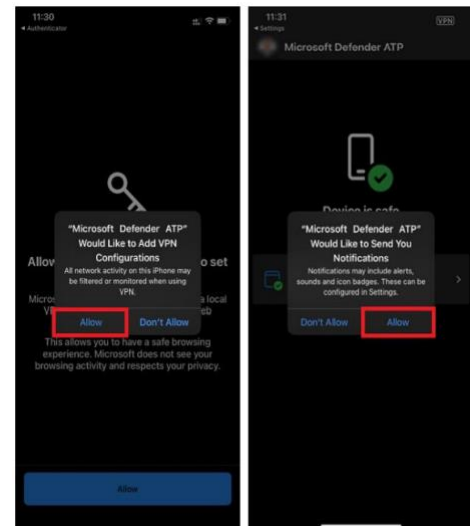
3. Microsoft Defender configuration steps

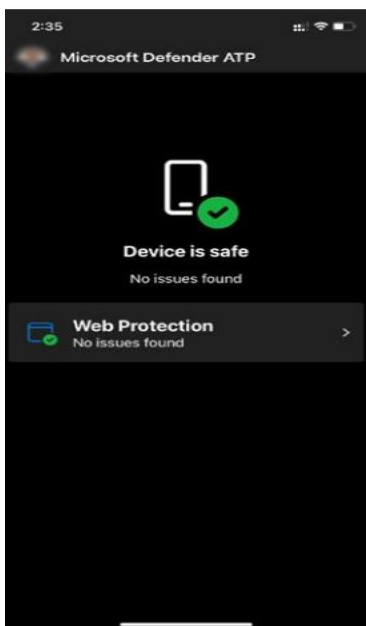**Step 1:** Open the Microsoft Defender app and tap on 'Get Started'

Step 2: Tap on your Virtusa account.
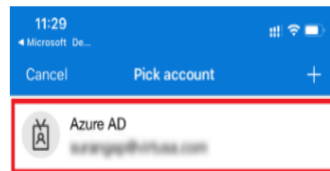
Step 3: Tap on 'Allow' to enable VPN and Notification settings.

Note: Your device enrollment is now completed.

Note: You can search for additional Virtusa apps in the Company Portal app and install them as needed. For more information, visit **byod.virtusa.com.**