SOM Mobile Device Management Install Guide

Purpose & Overview:

This document outlines the process to enroll in the UCR School of Medicine (SOM) Mobile Device Management program and secure work-related data on a non-corporate mobile device. This will involve removing some existing applications (apps), installing and enrolling in the Intune Company Portal app, and re-installing approved apps. The result is a separation of SOM data from the rest of the device.

Support Info:

Preparation work:

1. Before enrolling in the SOM Mobile Device Management program, please remove any of the following apps from your mobile device.

   a. REMOVE any Microsoft apps such as Word, Excel, PowerPoint, Outlook, Teams, SharePoint, and OneDrive; also remove Tiger Connect aka Tiger Text and Zoom.

      i. These apps will be re-added through the Company Portal which will have the approved work version of the app.

   b. Please refer to the following link that will help explain the process of removing apps

      i. Android: https://support.google.com/googleplay/answer/2521768?hl=en

      ii. Apple iOS: https://osxdaily.com/2019/10/06/how-delete-apps-ios-13/

Installing the Company Intune Portal App

2. **Android** https://docs.microsoft.com/en-us/mem/intune/user-help/install-the-company-portal-app-android

    a. Launch your mobile devices app store and Search for *"Intune Company Portal".*
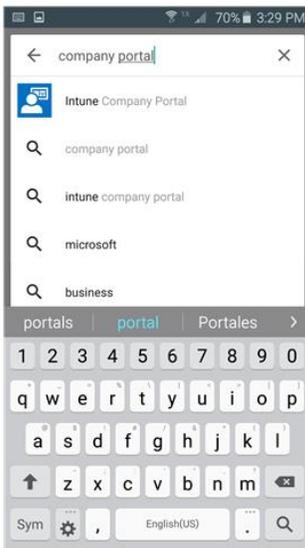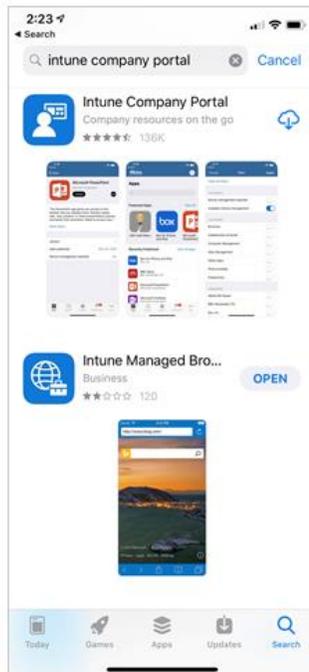

    b. Tap to install the app.

    c. Accept all permissions to complete the install of the app.

3. **Apple iOS** https://docs.microsoft.com/en-us/mem/intune/user-help/install-and-sign-in-to-the-intune-company-portal-app-ios
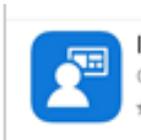
   a.   Launch your mobile devices app store and Search for *"Intune Company Portal".*

    b.   Click on the Cloud Install button to complete the install.

Signing into the Company Portal App

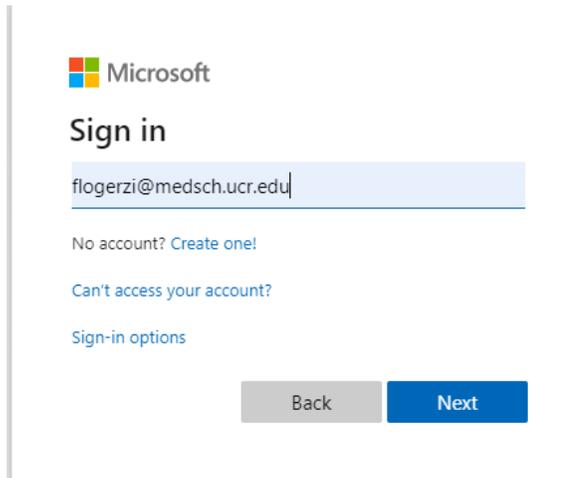4. The process is similar for both Android and iOS.

    a.   Launch the Company Portal app by locating this icon on your home screen or list of applications

    b.   Click the sign in button once the app launches.
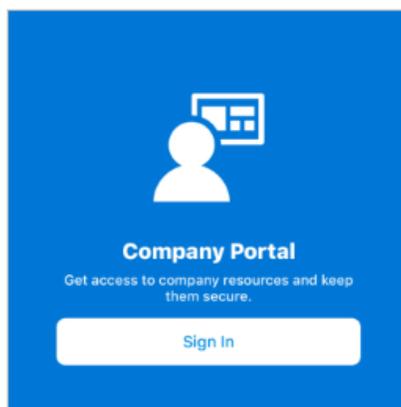
    c. Enter medsch email address. Please use <u>netid</u>@medsch[.]ucr[.]edu and not first.last@medsch.

    d. Click on next and enter password.

    e. Complete any MFA/Duo challenge prompts.

Enrolling your personal Device

SOM requires a complex password on all devices that access work data. Your mobile device password should be unique and not the same as your SOM password. You will be prompted to change it every 180 days.

5. **Apple iOS process**

    a. After completing the sign in process, the enrollment will start.

        i. A disclaimer from the Regents of the University of CA Riverside will explain what data and settings can and cannot been seen. Please email info-sec@medsch.ucr.edu for further questions or concerns.

        ii. After reading and accepting the Privacy Policy, a new window will pop-up asking to download a management profile. Please allow the profile to be downloaded. Once completed, this profile needs to be installed.

        iii. To install Management Profile

            1. Bring up settings.

            2. At the very top select the notification called *Profile downloaded.*

            3. Select Install in the upper right corner.

            4. Enter your current Pass Code.

            5. Select Install at the bottom of the screen.

            6. Select Install in the upper right corner again.

            7. Select trust on the remote Management Profile.

            8. Once Completed Select Done in the upper right.

            9. Go back to the home screen.

      iv.   Update unlock code to comply with SOM password requirements.

           1. If the profile was installed correctly, a passcode requirement notification will pop-up asking to update the unlock passcode. Please note if your device already uses a secure method, a password update will not be required. The following next steps can be skipped.

           2. Press Continue to start this process.

           3. Enter the devices current unlock code.

           4. New password must be 5 characters long and must contain special characters.

           5. Enter new passcode and complete the process.

      v.   Continue Device enrollment

           1. Relaunch the Company Intune Portal App.

           2. It will open the screen Download Management profile. Click Continue Now in blue text.

           3. If done correctly all checkboxes will show green as shown below.
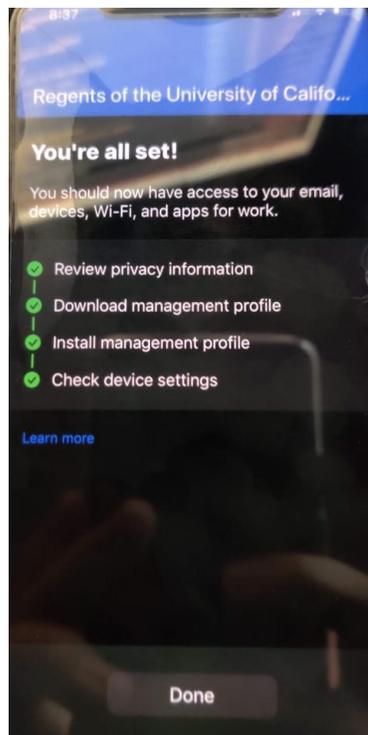
           4. Click Done to complete the enrollment.

           5. Select Personal device for device category and press continue.

           6. You can choose to receive notifications or not (Allow is the recommended setting).

6. Android Process

Please follow the instructions provided by Microsoft. Step by step instructions are available at: https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-device-android-work-profile

Installing Apps from the Company Portal

7. **Apple iOS Devices**

    a. Launch the Company Portal app by locating this icon on your home screen.

    b. Select Apps as highlighted below.


    c. Select View All Apps.

    d. Install each app as needed. This will ensure work data and personal data do not mix.

    e. For each app selected, a pop-up will display on the screen to approve the app install.

    f. To check the progress, go back to the home screen to see the newly installed apps.
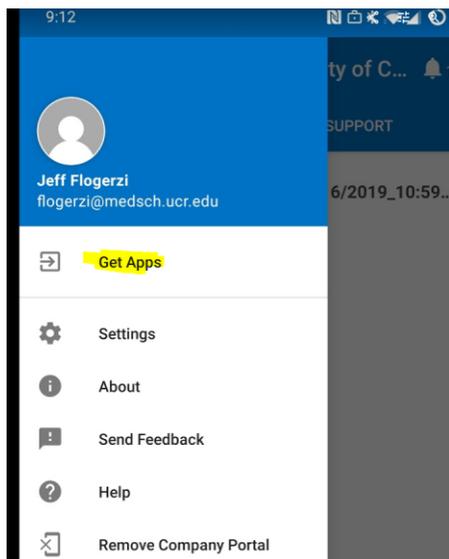
8. **Android Devices**

   a. Launch the Company Portal app by locating the Icon in your Work Container. Depending on what manufacture of Android this can vary in location.
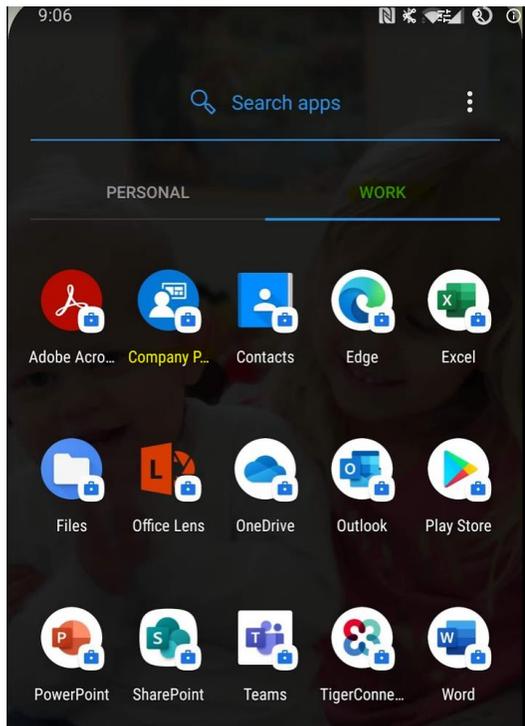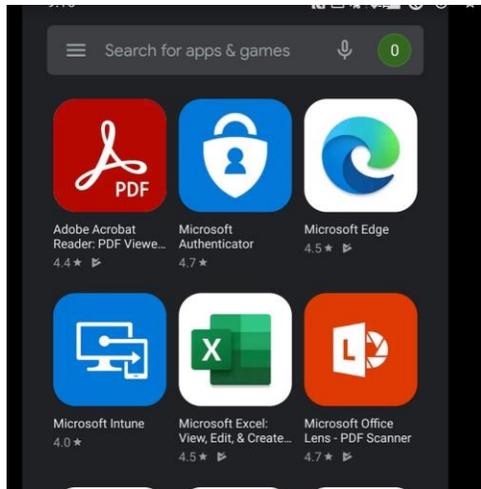

   b. Click the 3 horizontal bars in the upper left to reveal the menu.

   c. Select the Get Apps option.

d. This will launch a company version of the Google Play store with only company approved apps.

e. To install apps, select any app just like any normal Android app. These apps will be stored in the encrypted Work Container as shown below. Notice the brief-case picture in the app icon. This denotes it is a managed or work app. These apps can be added to your home screen in the same manner as standard apps would.