Intune
All Staff

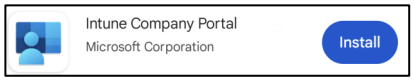
Install Intune on Android Devices

Microsoft Intune Mobile Device Management (MDM) secures PHI data and provides mobile device protection by configuring mobile devices in accordance with hospital security policies. It allows you to securely access The Health System applications. If your device is lost or stolen, hospital apps can be removed.

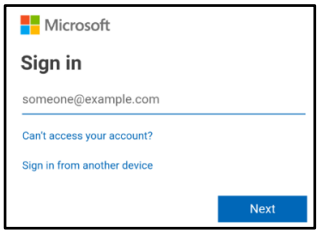
Intune is required for health system employees.

Install Intune

1. From the Google Play store, search for and install **Intune Company Portal**.

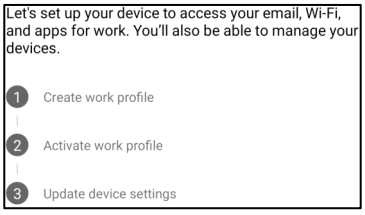


2. Open **Company Portal** app.
3. Allow Company Portal to send notifications.
4. Tap **Sign in**.
5. Enter your network email address (username@kumc.edu) and click **Next**.

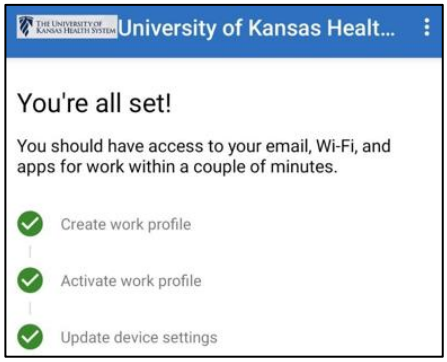


6. The user will be redirected to the KUMC Central Authentication Services webpage.
7. Enter network username and password and click **Login**.

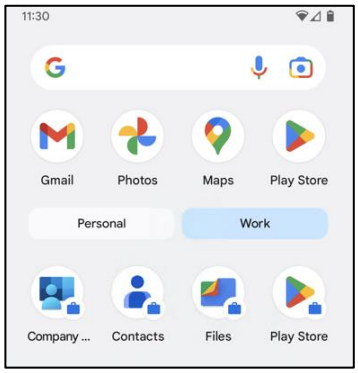
8. Follow the prompts, **Intune** will show the steps it is working on to bring the device into compliance.



9. Read and follow the prompts to click continue or next through this process.
    a. If you receive a Company Portal notification to Update device settings, the most frequent cause is a weak device PIN. Click the notification to update your PIN. HITS recommends at least a 4 digit, complex, PIN. (I.e., 1234, 9999, and other simple PINs are not allowed.)
10. Upon completion you will see the below message.



11. To access Play Store on the work profile, open the app drawer and select **Work**.
12. Then install Teams, Outlook, and other approved work apps.



On Samsung KNOX devices, the first time the user accesses the mailbox they will be prompted to enter their domain.

- Domain\username, for example: KUMC\jdoe6.
- Enter password.
- Select Activate.

Enable Wifi Certificate to Connect to “UKHS-Prod”

If your Android device is not enrolled in Intune or you are unable to sign in, your device will not be able to access the Wi-Fi certificates required to connect to our secure network, "UKHS-Prod." Resolve by enabling browser access in the Company Portal app.

1. In the **Company Portal** app, select **Menu** (three horizontal lines icon) from the left-hand corner.
2. Select Settings.
3. Next to Enable Browser Access, select Enable.
4. On the Device Administrator screen, select Wifi-Certificate. Next select "Ok"
5. The certification name will populate automatically. Select "Ok"
6. Certificates should start to load on to your device.

FOR MORE INFORMATION CONTACT:

Report O2 Issue | For urgent issue call 913-945-9999 | Request an O2 Optimization