This covers how to install Microsoft Intune Mobile Device Management on your Apple iPhone. The installation process may change slightly as Apple updates its software, but shouldn’t be substantially different from what you see here. The same is true if you’re installing on an iPad.
Intune encrypts your device and requires you to set a long passcode or a biometric ID to use it. It also allows the device to connect to our secure Wi-Fi network. We require these safeguards to prevent unauthorized individuals from accessing Protected Health Information (PHI) or other sensitive data.

Although HSIS can’t use Intune to view your personal information, it’s an added layer of security for your device, even if you own it. If you don’t want to install Intune, you may be eligible to get a Basic Work Device — check with your department.

Please note that you are prohibited from storing PHI in third-party applications like Notes that sync data through iCloud.
You must be enrolled in Multi Factor Authentication to proceed. If you haven’t done that yet, please refer to the MFA tutorial before proceeding. If you’re already enrolled in MFA, you can install Intune on any data network.
You will also need an Apple ID, which lets you use Apple services like the mobile App Store. An Apple ID is always an email address. If you’re installing Intune on a personal device, you may already have one set up with your own email address. It’s better to use it rather than your uabmc.edu address as your Apple ID, even if you’re installing on a Basic Work Device. This will make it easier to purchase any apps and take them with you when you leave UAB.

Consult Apple’s support page, shown here, for more information on Apple ID.
If you’re running iOS version 17.3 or later, open the Settings app and navigate to Face ID & Passcode, as shown. Look for Stolen Device Protection and make sure it’s turned off. (You can re-activate it after Intune installation is complete.)
Open the App Store on your device and search for “Intune company portal”. Next, install the app, which is called Comp Portal. After installing it, tap Open or navigate to the app on your home screen and launch it from there.
You’ll see a Microsoft Intune Sign In screen like this. Enter your full uabmc.edu email address (someone@uabmc.edu) and tap Next. **Make sure not to enter your uab.edu email address by mistake.**
Now, enter your uabmc.edu password and tap Sign In. This is the same password you use to log in to IMPACT and other systems.
This is where Multi Factor Authentication comes in. You’ll be asked to approve the sign in request using the method you specified when you enrolled in MFA. In most cases, that will involve the same device that you’re installing Intune on. In this example, you would respond to the approval notification and tap Approve to proceed.
You’ll see a screen with four installation steps, as shown here. Tap the Begin button at the bottom to go to the next step.
This screen shows you how Mobile Device Management with Intune affects your privacy. You can display what HSIS Can’t and Can do by tapping the appropriate tab. Tap Continue when you’re ready to go ahead with the installation.
A check mark will appear next to the first step. Tap Continue at the bottom of the screen to proceed.
Next, you’ll be asked for permission to download a configuration profile for Intune to your device. Tap Allow to go to the next step.
Once the profile has been downloaded to your device, which shouldn’t take too long, tap Close.
Now, go to the Settings app on your device. You can do this by going to your home screen and tapping the Settings icon or by using the app picker to go directly to the Settings app, as shown here.
In the Settings app, tap Profile Downloaded. The profile contains everything Intune requires to set up your device for work use.
Tap Install at the top right. You’ll have several opportunities to confirm that you want to go ahead with the installation.
Tap Install at the bottom of the screen to install the profile.
Enter your device’s passcode to proceed. This is the character sequence you use to unlock it.
A warning screen like this one will appear. Read the notice, then tap Install at the top right of the display. Please note that this information, which was provided by Microsoft, doesn’t accurately reflect what HSIS can do with Intune. For example, we can’t access any of your personal data, nor can we see or manage your apps. Although we can completely erase the device if it’s lost or stolen, we will only wipe your personal information if you ask us to.
You’ll see yet another warning asking if you trust the source of the profile. Tap Trust to go ahead.
A spinner at the top right will indicate that the profile is being installed. It shouldn’t take more than a minute or so to finish.
Profile installation will be complete when you see this screen. Tap Done at the top right to proceed.
Go back to the Comp Portal app on your device. All four steps should now be checked. Tap Done.
On the next screen, tap Ok to enable notifications for Intune.
This screen lets you approve receiving notifications by tapping Allow. You can change this any time in the Settings app.
Go back to the Settings app, where you’ll be prompted to enter your uabmc.edu Exchange password, as shown here. This is required to access your email, calendar, and contacts using the phone’s Mail, Calendar, and Contacts apps.
It’s normal for your device to be placed in “quarantine” after MDM installation. You’ll receive a notice like this that you may view on any other device that lets you access your uabmc.edu email. This should resolve without any further action on your part, allowing your device to connect to the secure Wi-Fi network and access your uabmc.edu email.

Call the HSIS Help Desk (205-934-8888) if your device has not been released by approximately one hour.
THE END