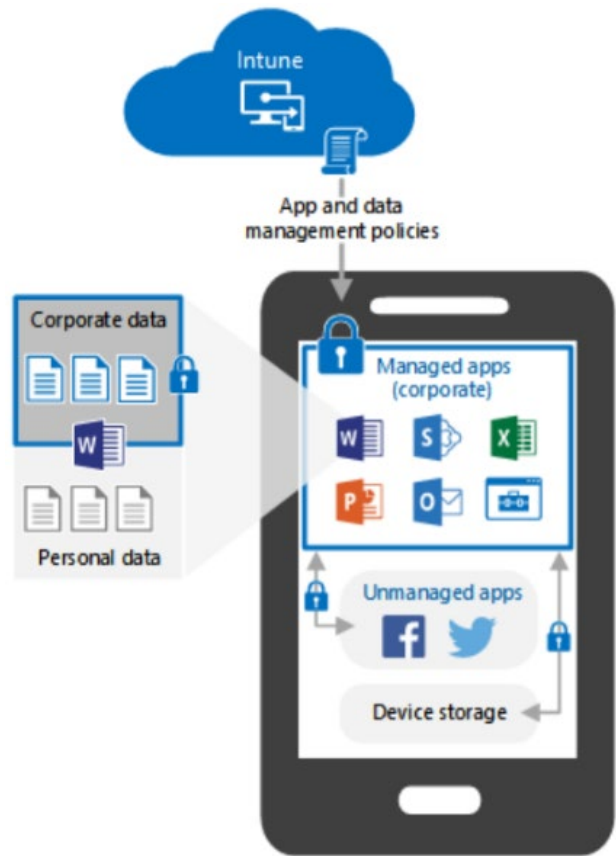


## Microsoft Azure GCC High iOS / iPadOS

### Q: What is happening here?

Today Trideum operates in the Azure commercial cloud. To satisfy data protection requirements imposed by the DoD, we are moving from an Azure commercial cloud to Azure GCC-High Gov Cloud. The system Trideum uses to manage mobile device access to company data will also move to Gov Cloud.

If you want to load and access Trideum data on your personal iOS / iPadOS device – it’s totally safe. We (Trideum IT) can’t see any of your personal data. The Trideum apps get loaded in a special “sandbox” designed by Apple that lets Trideum control “Trideum” data. Your device does require a few basic security items (6 digit passcode, recent iOS versions, etc.) but otherwise your data is yours, and Trideum data is controlled by Trideum.



[What info can your organization see when you enroll your device? | Microsoft Learn](#)

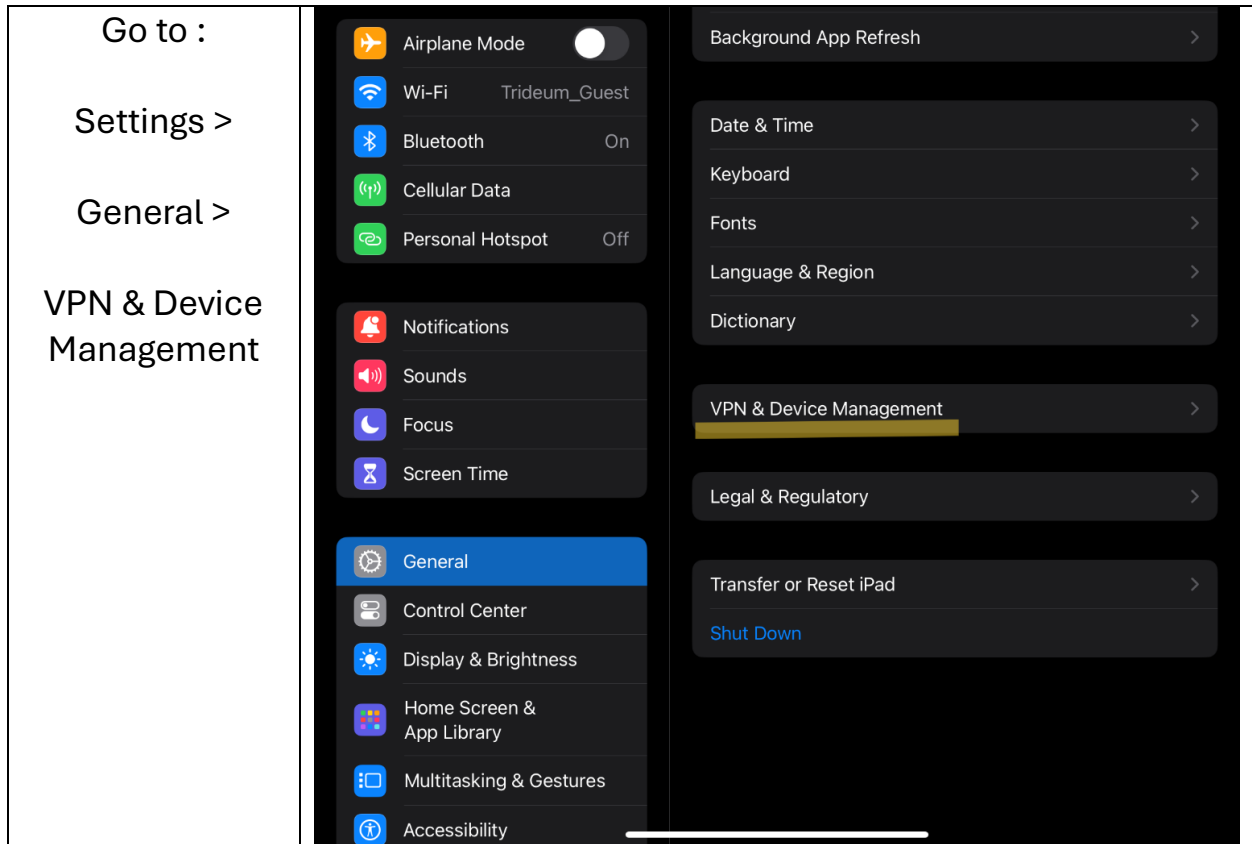
If you’re already using Trideum Data or you want to – here’s the path ahead:

Step 1	Step 2	Step 3	Step 4a	Step 4b	Step 5
IT will “Retire” your device from Trideum’s 365	Logout & delete Microsoft Apps	Install MS Authenticator App	Install the Intune Company Portal App	Install new Trideum Profile	Install new Office Apps

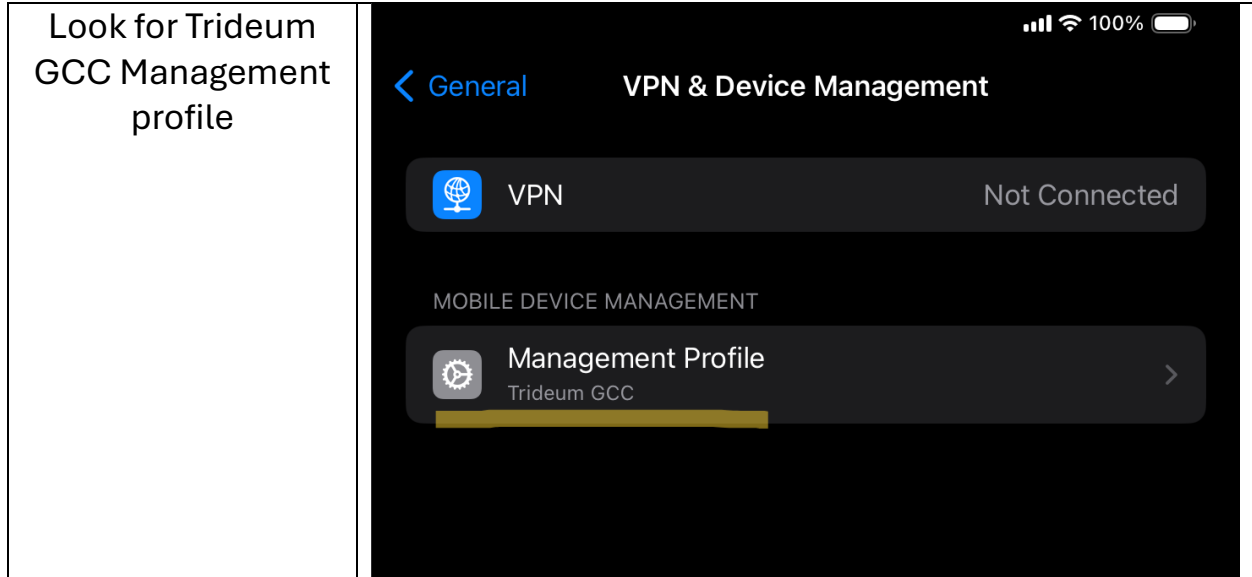
## Step 1: Remove old Trideum Management Profile

# Step 1: Remove the old Trideum Management Profile

Trideum IT will send out a “Retire” command at the Work freeze on 6 September; this command should remove the Trideum Profile and Data from any existing apps – let’s confirm that the old Trideum management profile is gone

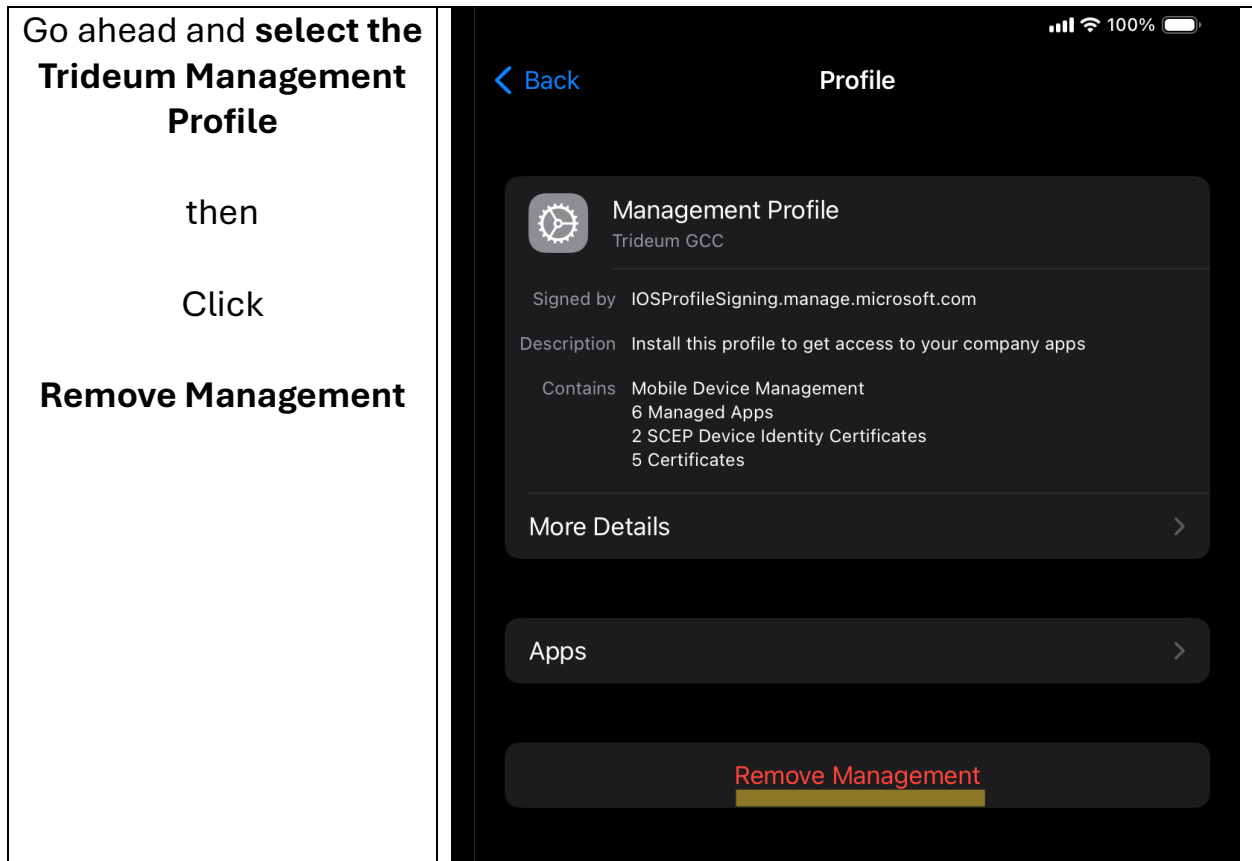


Step 1: Remove any old Trideum Management Profiles

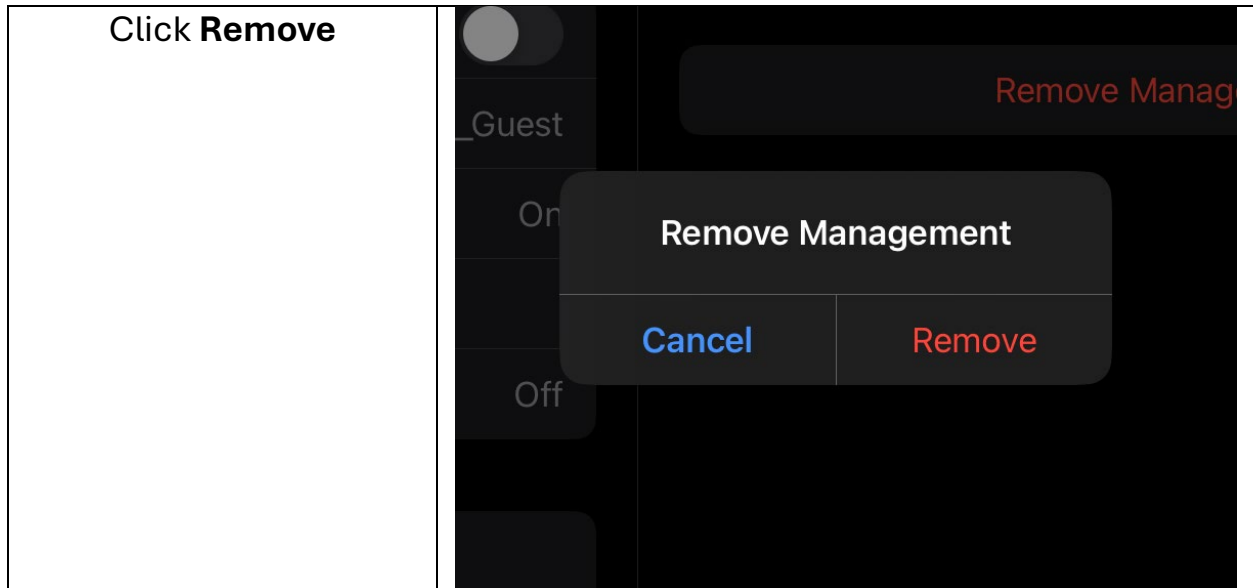


If the Management Profile is already missing from this screen skip ahead to [Step 2](#)

If it's still there – then the “Retire” command the IT team sent hasn't activated yet



Step 1: Remove any old Trideum Management Profiles



## Step 2: Logout and delete apps where you signed in with your Trideum account

(except MS Authenticator)



Typical apps you may have previously used with Trideum Data include:

Intune Company Portal	A blue icon representing a person's profile next to a blue square with a white circle.
Outlook	A blue icon of an envelope with a white 'O' on it.
Teams	A purple icon with a white 'T' and two stylized human figures.
OneDrive	A blue icon of a cloud with a white 'O' on it.
Word, PowerPoint, Excel	Three icons: a blue 'W' on a square, a red 'P' on a circle, and a green 'X' on a square.
Microsoft 365	A purple and blue icon of a stylized '3' or '6' shape.

Step 3: Install the Microsoft Authenticator App

## Step 3: Microsoft Authenticator App



If you don't already have the Microsoft Authenticator App, now's the time to install it!

**Download Microsoft Authenticator**

Use simple, fast, and highly secure two-factor authentication across apps.

## Get the app on your phone

Scan the QR code with your Android or IOS mobile device.



*Trideum doesn't control the MS Authenticator App, you can use it for Trideum logins as well as for personal accounts.*

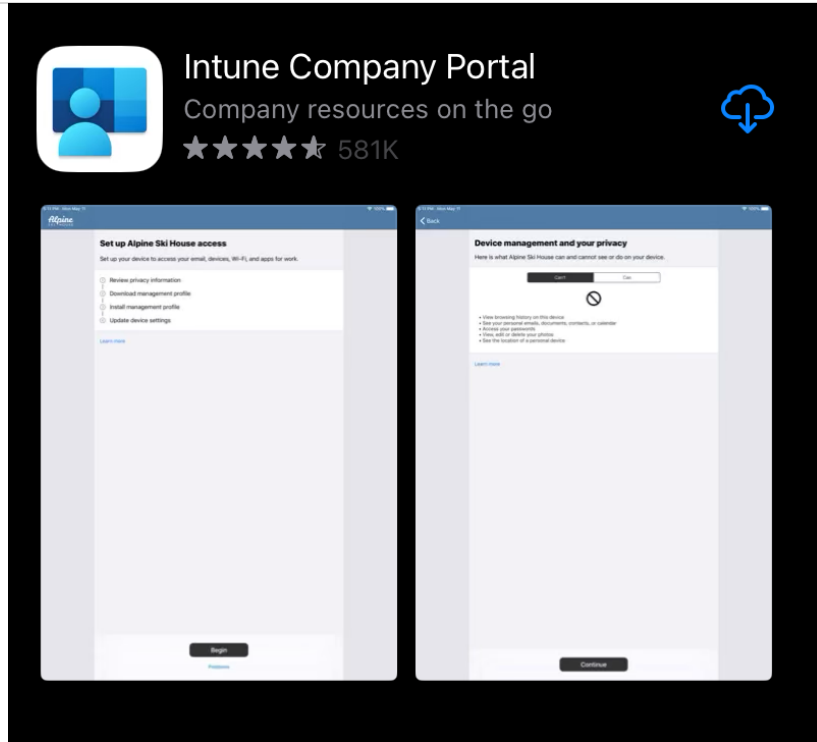
*For more information check out:*

<https://www.microsoft.com/en-us/security/mobile-authenticator-app>

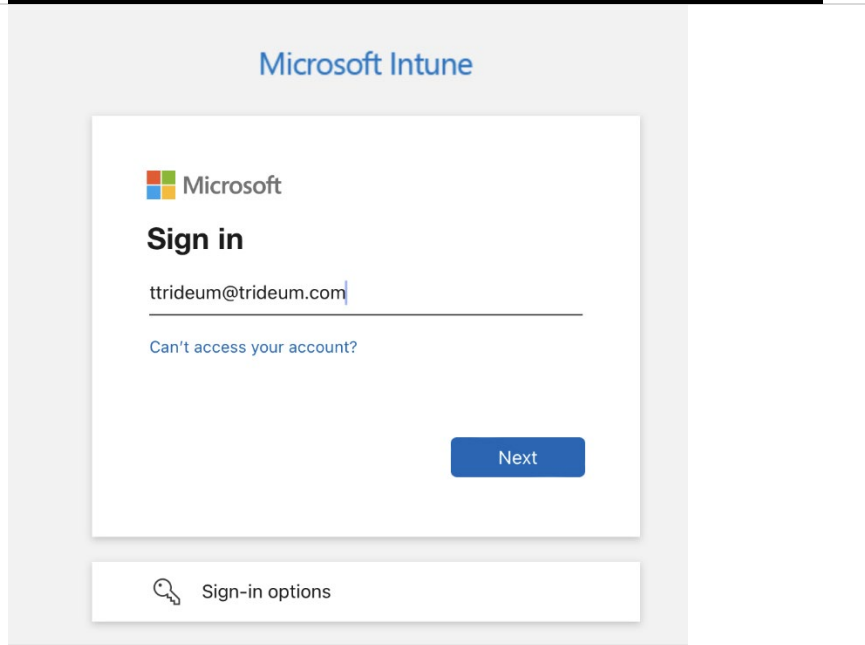
Step 4a: Install the Intune Company Portal

## Step 4a: Intune Company Portal

First download the Intune Company Portal from the Apple app store

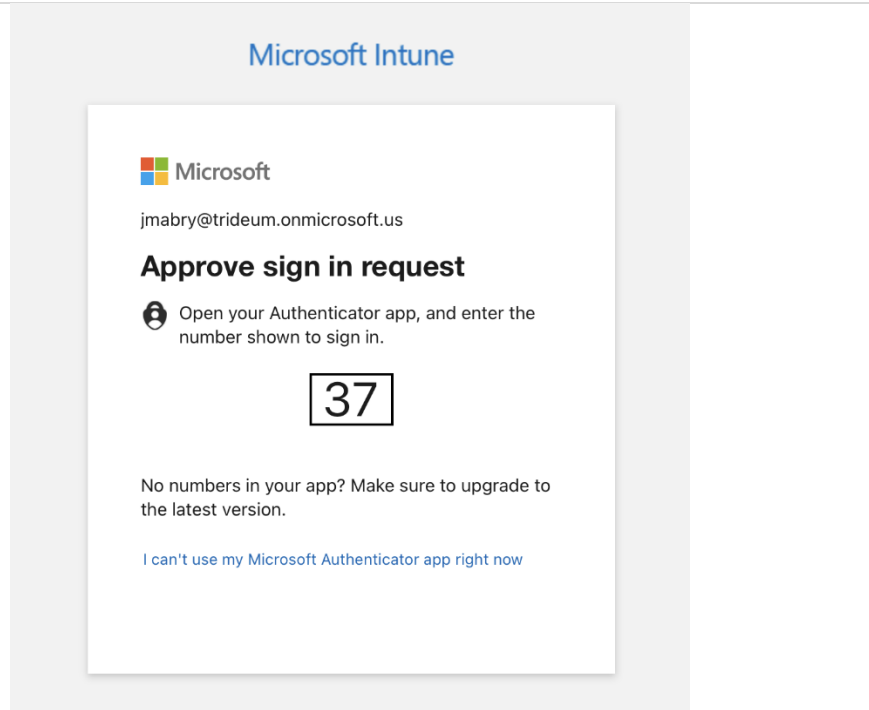


Open the Company Portal app and login

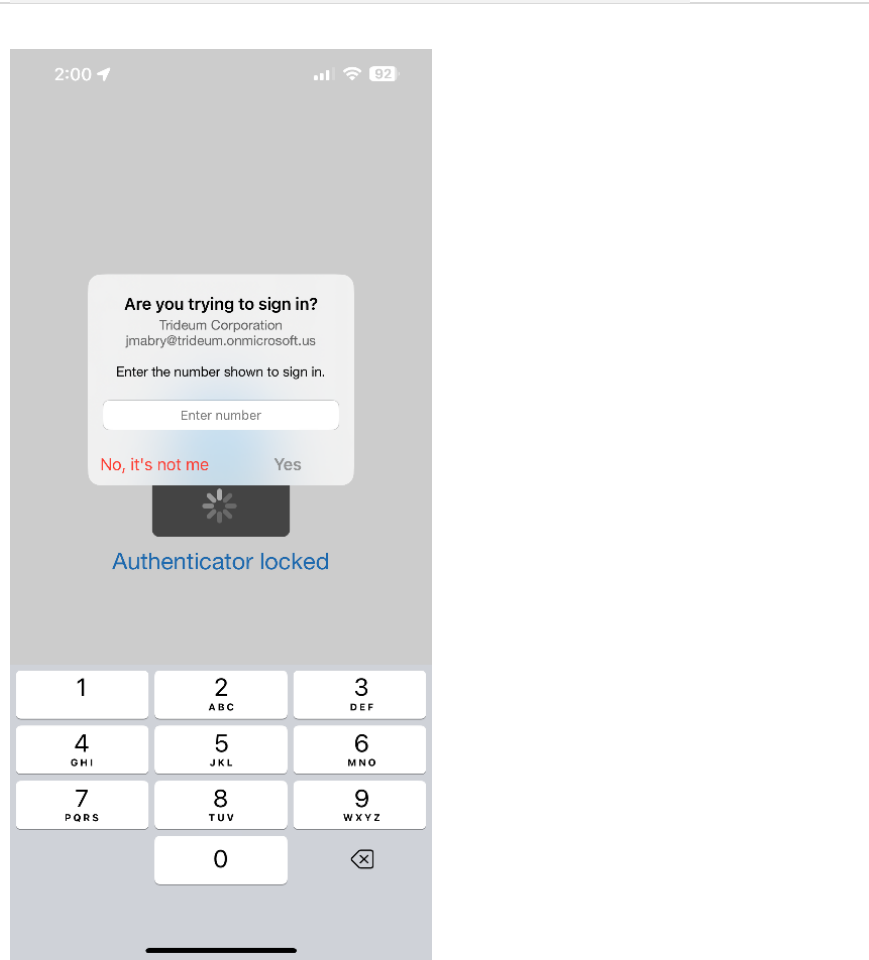


Step 4a: Install the Intune Company Portal

You will receive a multi-factor authentication challenge code

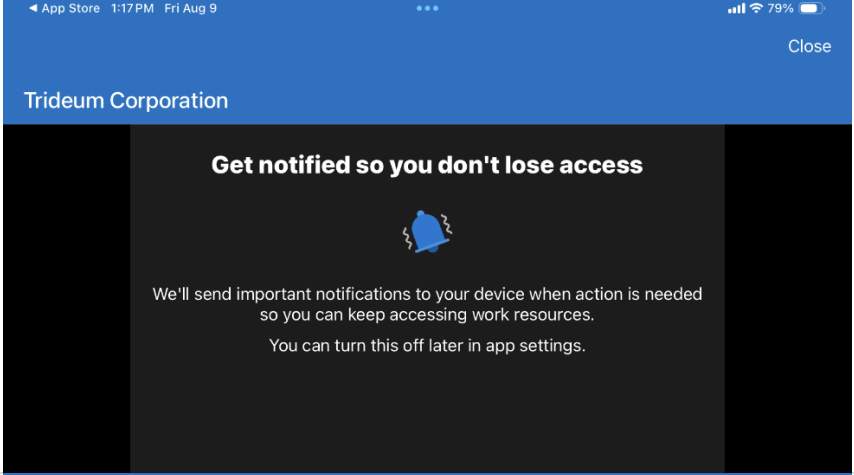
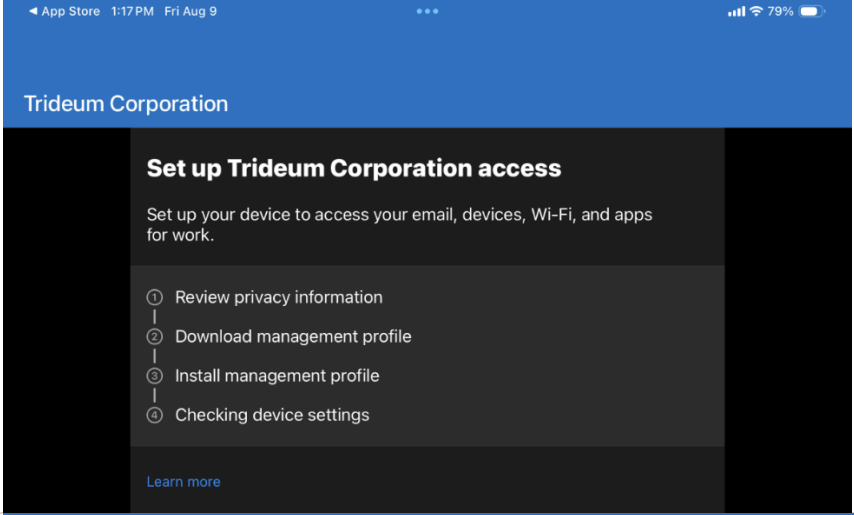
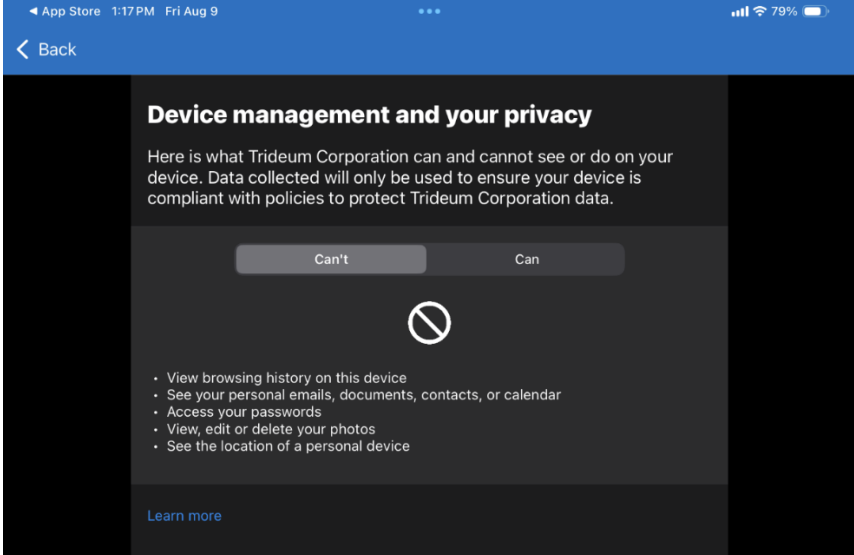


enter the number presented in the Microsoft Authenticator

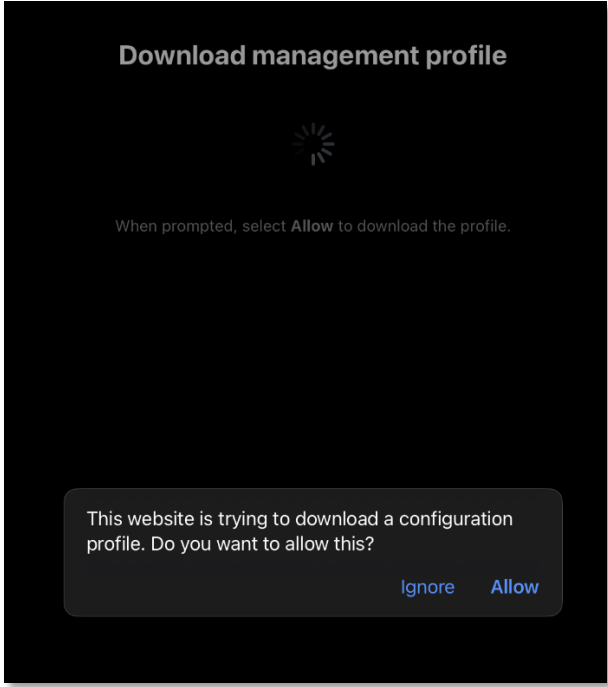
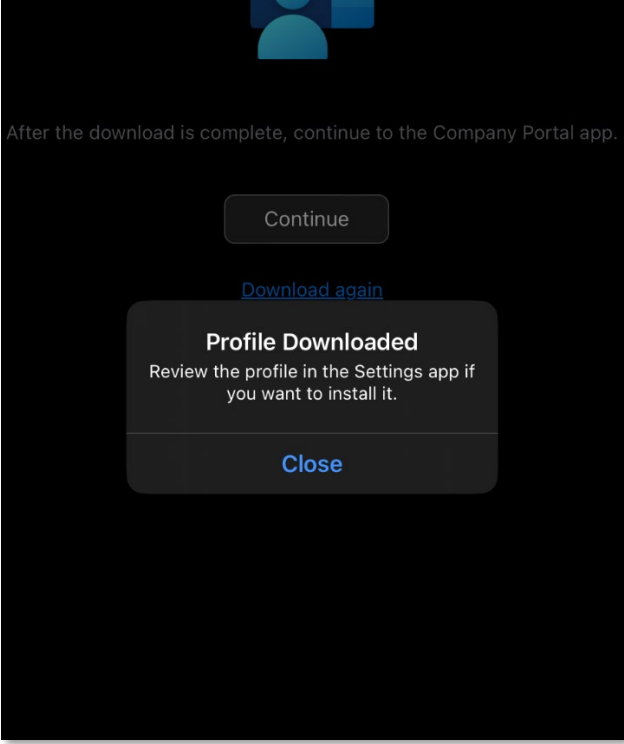




## Step 4a: Install the Intune Company Portal

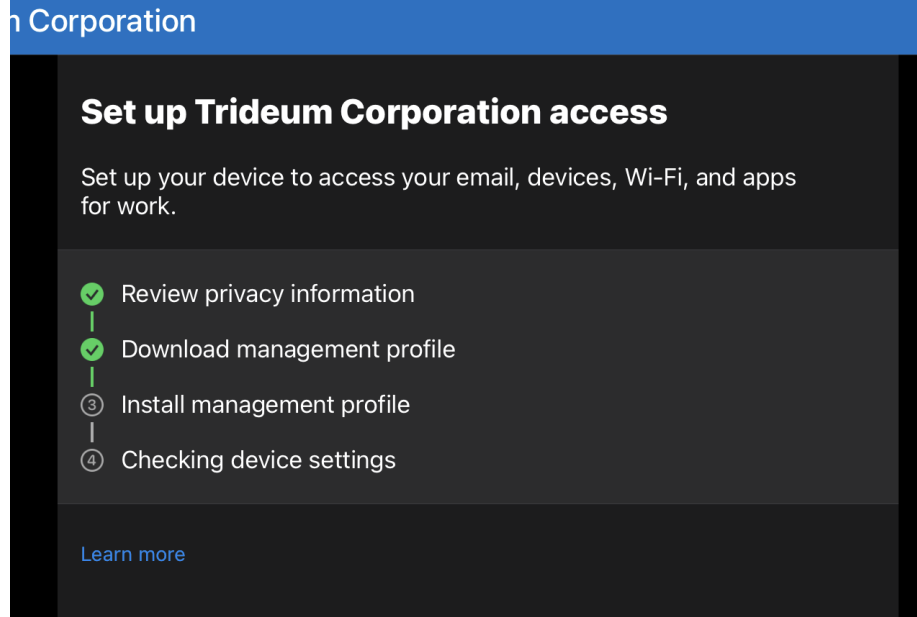
<p>Choose if you want notifications from the Company Portal app</p>	 <p>The screenshot shows the Trideum Corporation app interface. At the top, it says "Trideum Corporation" and "Close". Below that, the heading is "Get notified so you don't lose access" with a blue bell icon. The text reads: "We'll send important notifications to your device when action is needed so you can keep accessing work resources. You can turn this off later in app settings."</p>
<p>Follow the prompts to review privacy information</p>	 <p>The screenshot shows the Trideum Corporation app setup screen. At the top, it says "Trideum Corporation". Below that, the heading is "Set up Trideum Corporation access". The text reads: "Set up your device to access your email, devices, Wi-Fi, and apps for work." Below this is a numbered list of steps: 1. Review privacy information, 2. Download management profile, 3. Install management profile, 4. Checking device settings. There is a "Learn more" link at the bottom.</p>
<p>Review privacy information</p>	 <p>The screenshot shows the Trideum Corporation app privacy review screen. At the top, it says "Trideum Corporation" and "Back". Below that, the heading is "Device management and your privacy". The text reads: "Here is what Trideum Corporation can and cannot see or do on your device. Data collected will only be used to ensure your device is compliant with policies to protect Trideum Corporation data." Below this is a "Can't" button and a "Can" button. A large "No" symbol is displayed. Below the symbol is a list of permissions: "View browsing history on this device", "See your personal emails, documents, contacts, or calendar", "Access your passwords", "View, edit or delete your photos", "See the location of a personal device". There is a "Learn more" link at the bottom.</p>

## Step 4b: Download the Trideum Configuration Profile

<p>Download the new management profile,  select <b>Allow</b> to start the download</p>	
<p>Once the profile downloads, select <b>Close</b></p>	

## Step 4b: Install the Trideum Management Profile

Once “Download management profile” is green, go install the profile in your phone settings

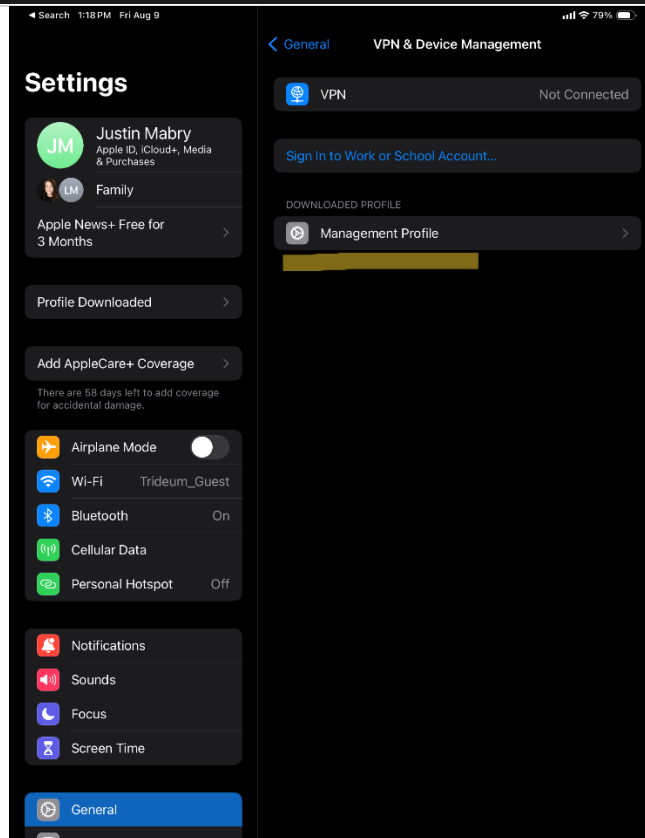


**Settings**>

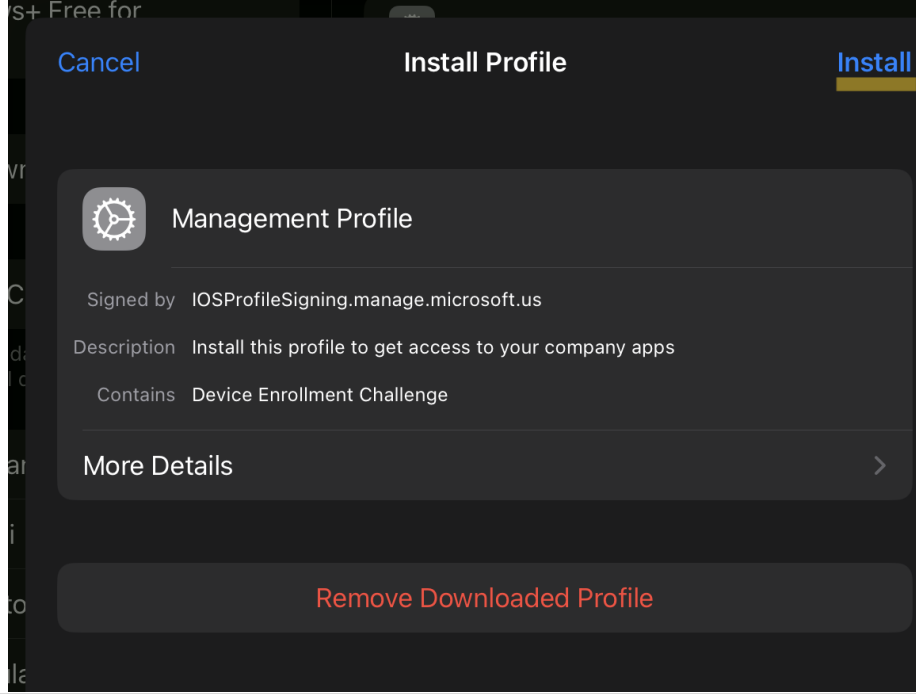
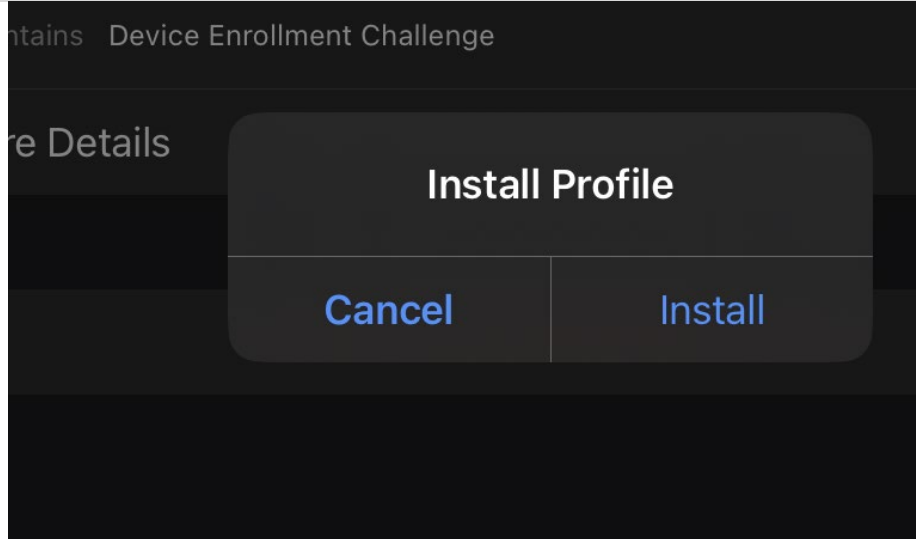
**General**>

**VPN & Device Management**>

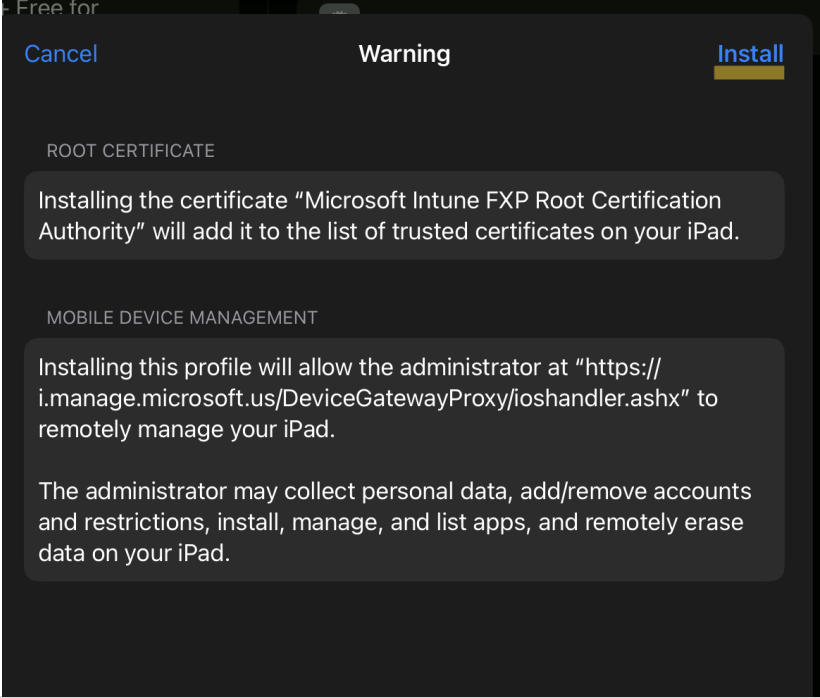
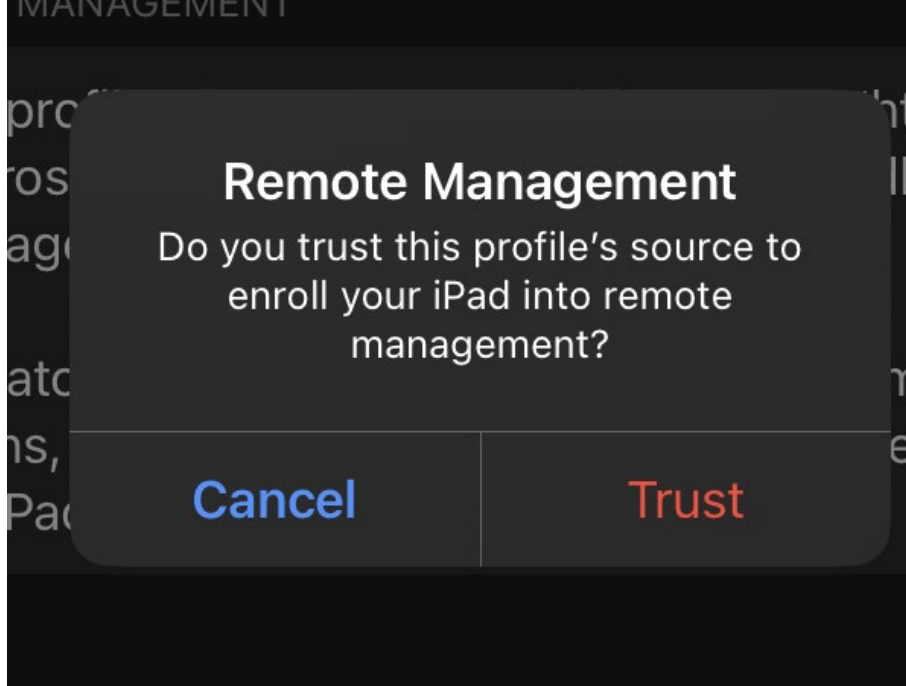
click on  
**Management Profile**



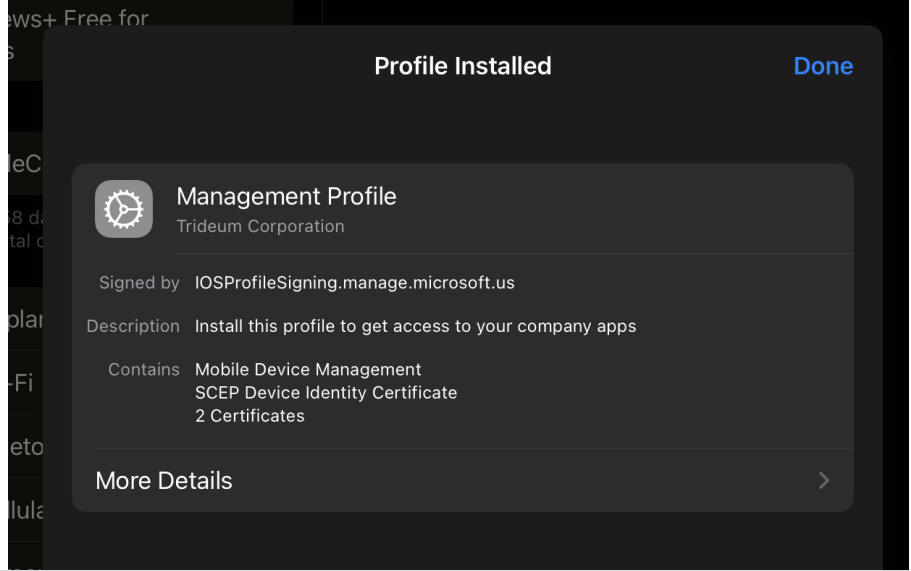
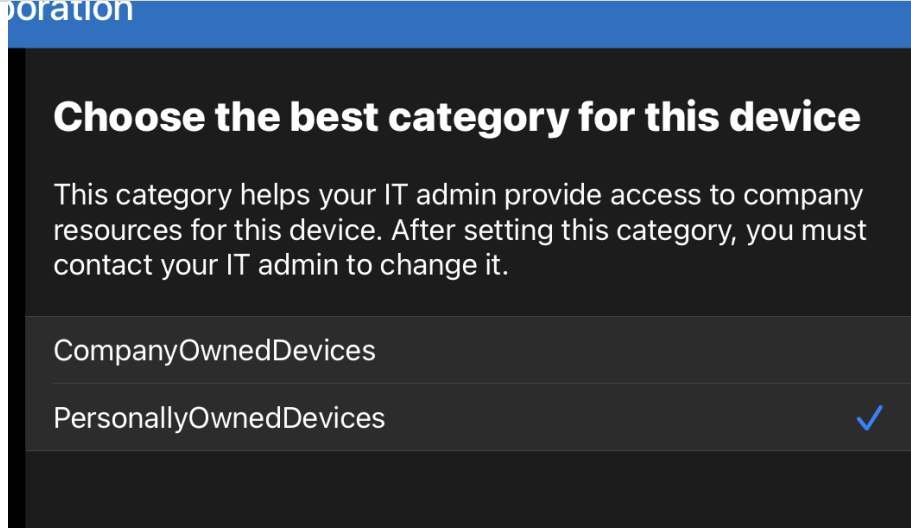
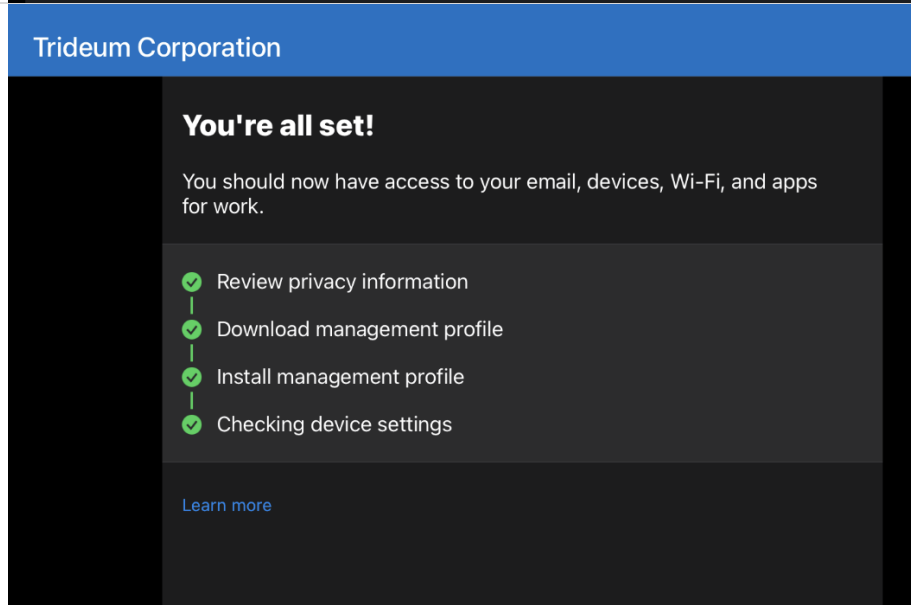
Step 4b: Install the Trideum Management Profile

<p>Click on <b>Install</b> in the top right corner</p>	
<p>Click <b>Install</b></p>	

Step 4b: Install the Trideum Management Profile

<p>You will receive a warning, click <b>Install</b> in the top right corner</p>	 <p>The image shows a warning dialog box with a dark background and white text. At the top, it says "Warning" in the center, with "Cancel" on the left and "Install" on the right. Below this, there are two sections: "ROOT CERTIFICATE" and "MOBILE DEVICE MANAGEMENT". The "ROOT CERTIFICATE" section states: "Installing the certificate 'Microsoft Intune FXP Root Certification Authority' will add it to the list of trusted certificates on your iPad." The "MOBILE DEVICE MANAGEMENT" section states: "Installing this profile will allow the administrator at 'https://i.manage.microsoft.us/DeviceGatewayProxy/ioshandler.ashx' to remotely manage your iPad." At the bottom, it says: "The administrator may collect personal data, add/remove accounts and restrictions, install, manage, and list apps, and remotely erase data on your iPad."</p>
<p>Click <b>Trust</b></p>	 <p>The image shows a "Remote Management" dialog box with a dark background and white text. The title "Remote Management" is at the top. Below it, the text asks: "Do you trust this profile's source to enroll your iPad into remote management?" At the bottom, there are two buttons: "Cancel" on the left and "Trust" on the right.</p>

## Step 4b: Install the Trideum Management Profile

<p>The management profile is now installed, click <b>Done</b> and return to the Company Portal app</p>	
<p>You will be asked to identify who owns the device, choose <b>Personally Owned Devices</b></p>	
<p>You have completed the enrollment process</p>	

Step 5: Install Microsoft Apps to access Trideum data

## Step 5: Install Apps from the Company Portal

You can now download and login to Trideum apps from inside the **Company Portal**

