

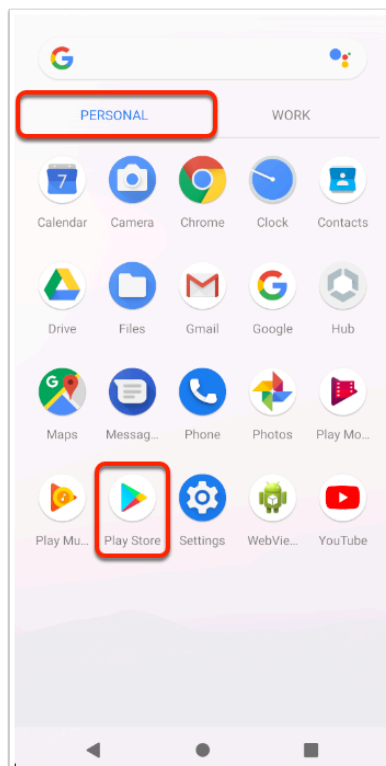
Securing applications in the Android work profile

i In this lab we are going to configure work profile settings for an Android device, so we can secure the behaviour of corporate applications and the interaction between these and personal apps.

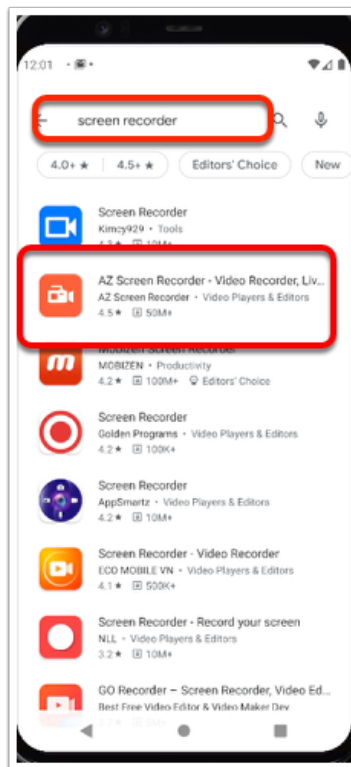
You'll be using the Android device you already enrolled and used in previous labs.

Part 1: Downloading necessary applications

On this part we are going to download applications that will allow us to test the interaction between the personal and work profiles.

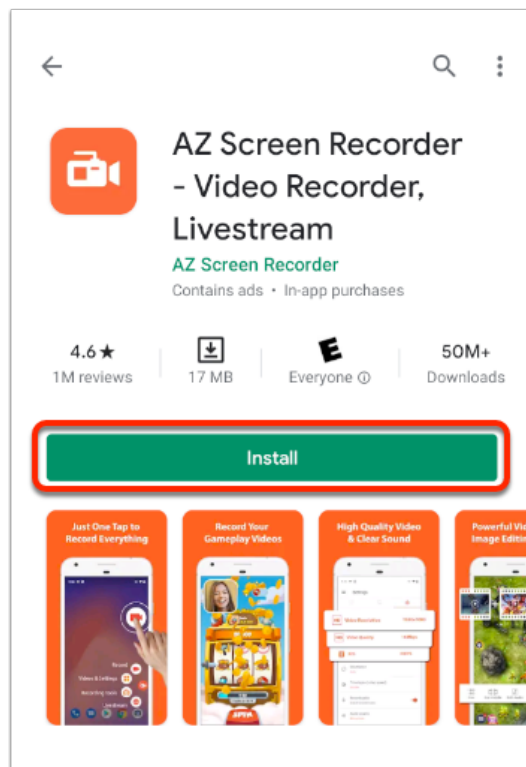


1. On your Android device
 - Select the **PERSONAL** profile
 - Select **Play Store**

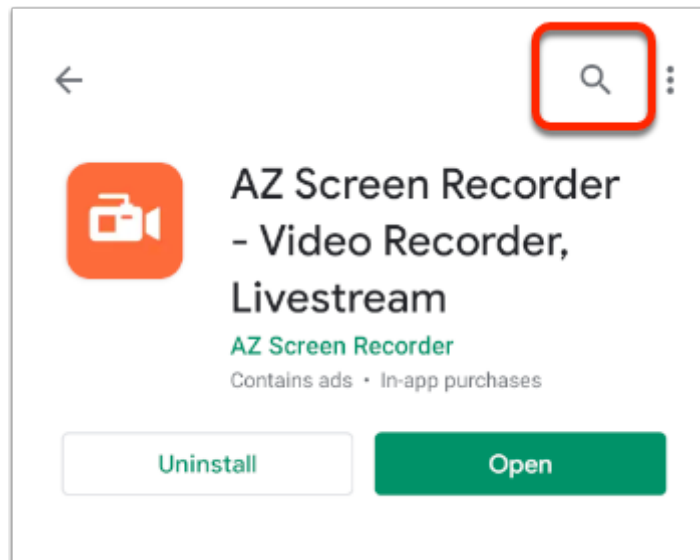


2. To download a screen recorder app:

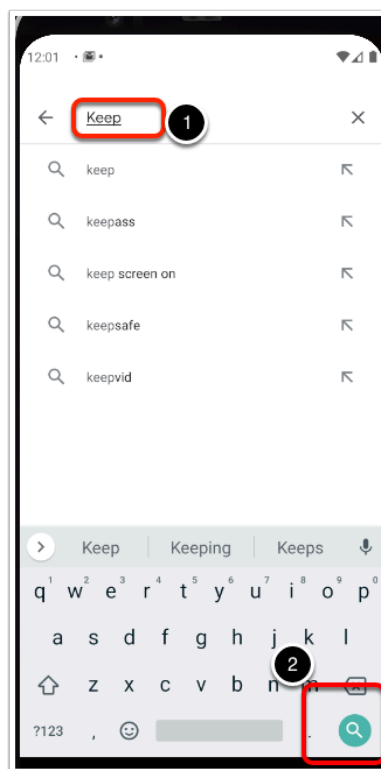
- In the **Search** bar type **screen recorder**
- tap on **AZ Screen Recorder**



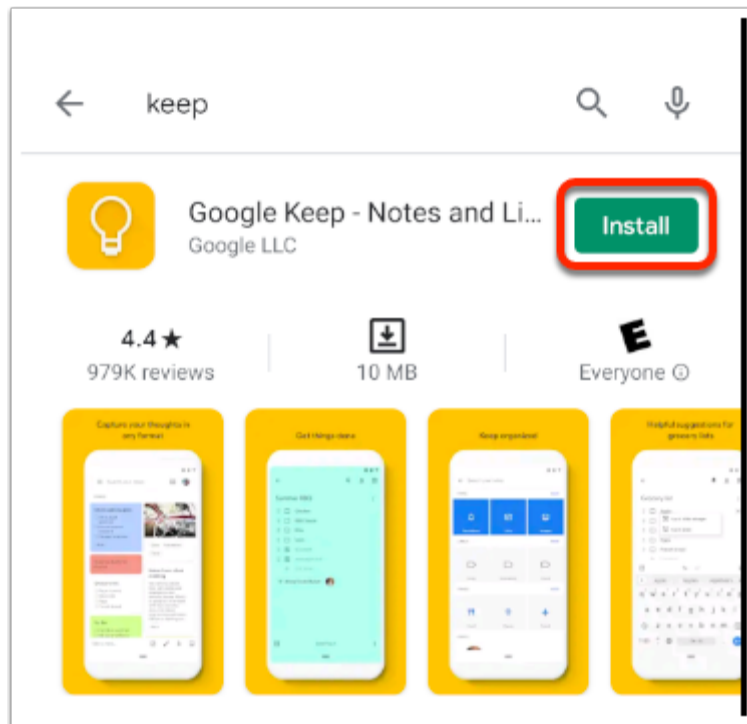
3. In the **AZ Screen Recorder** application window, Select **Install**



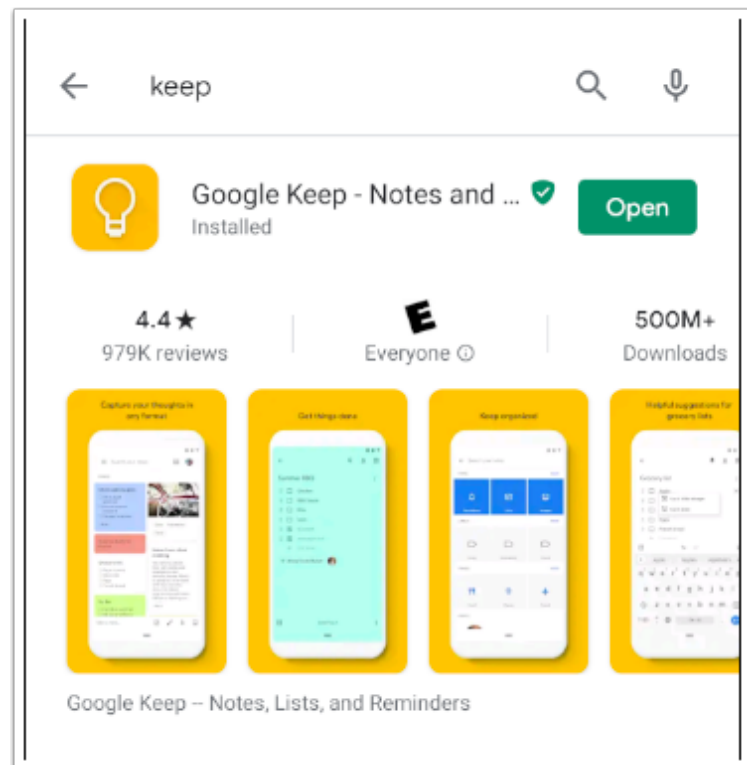
4. In your **Playstore** App, at the top of the application window, select the **Search** icon



5. In the Search bar, type **keep** and select the **Blue Search** Icon in the bottom, right-corner



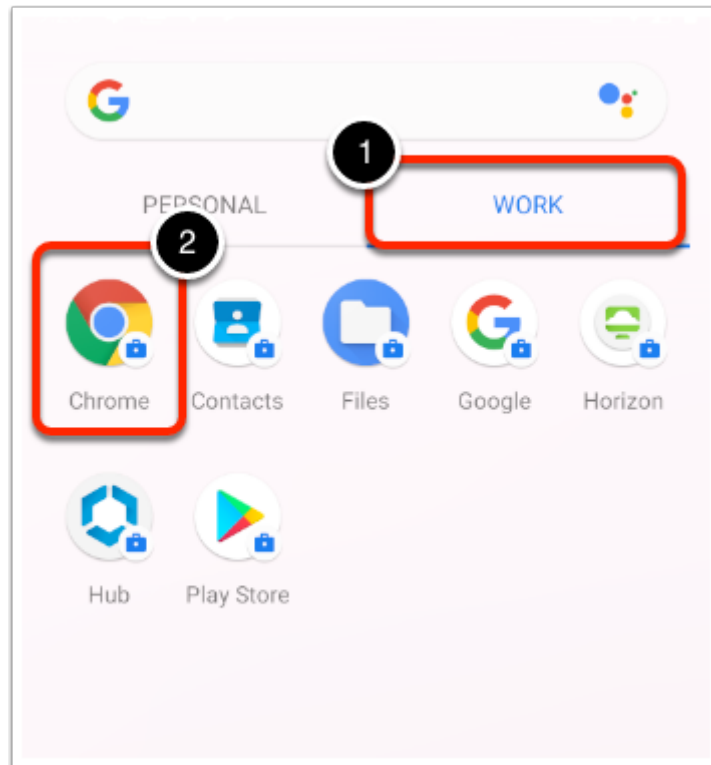
6. Next to **Google Keep**, select **Install**



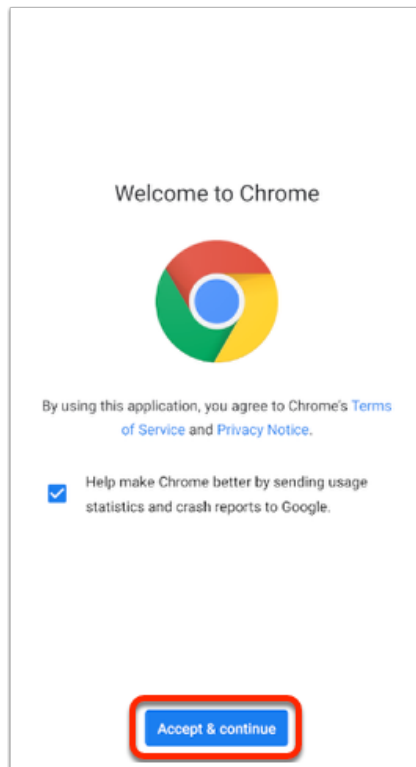
7. Once the download completes move on to the next part.

Part 2: Testing initial copy and paste behaviour

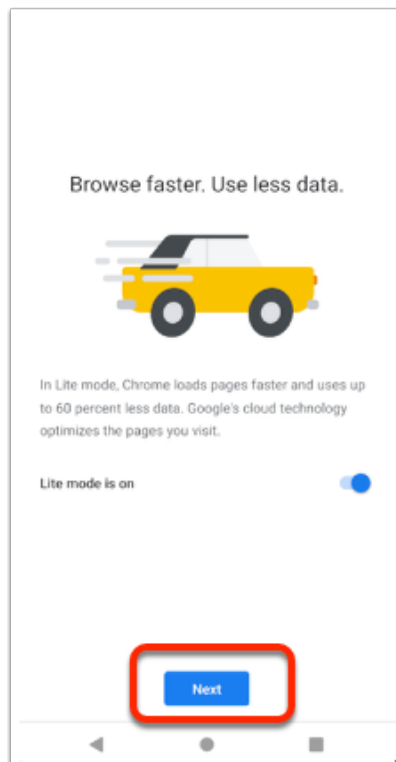
In this part we are testing the default copy and paste behaviour between apps in the personal and work profiles, without any policies applied to them.



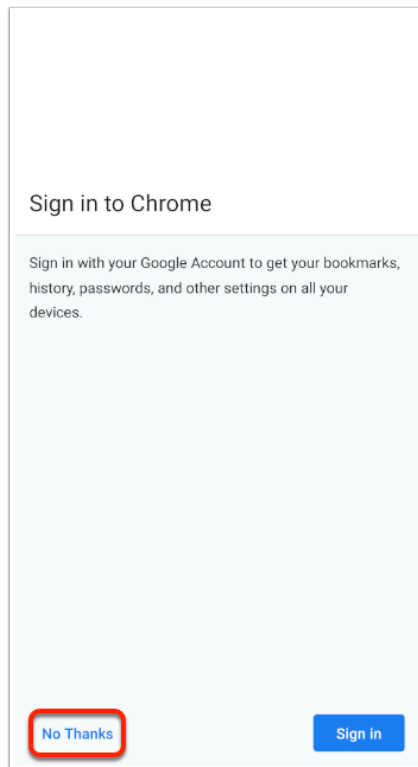
1. On your Android device
 - Revert back to your devices **Application Menu**.
 - Select your **WORK** Profile
 - In your **WORK** Profile, open the **Chrome** browser



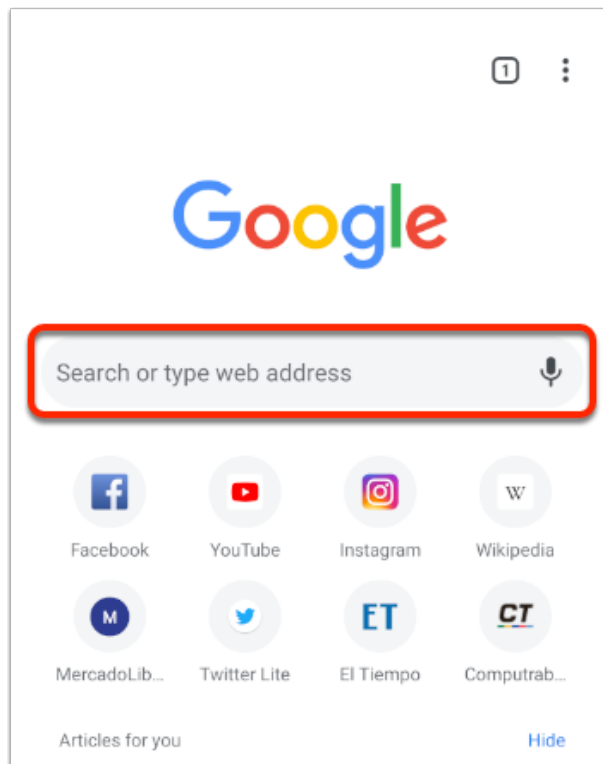
2. If prompted, in the **Welcome to Chrome** screen Select **Accept & continue**



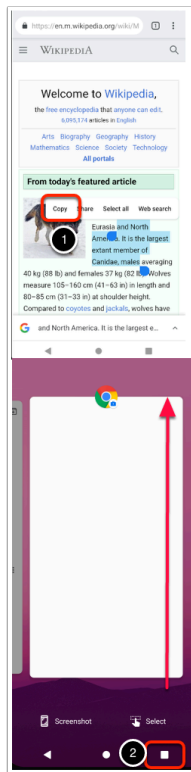
3. If prompted, to **Turn on Sync**, select **No thanks**
 - If prompted, in the **Lite mode** window, Select **Next**



4. If prompted, in the **Sign in to Chrome** window, select **No Thanks**

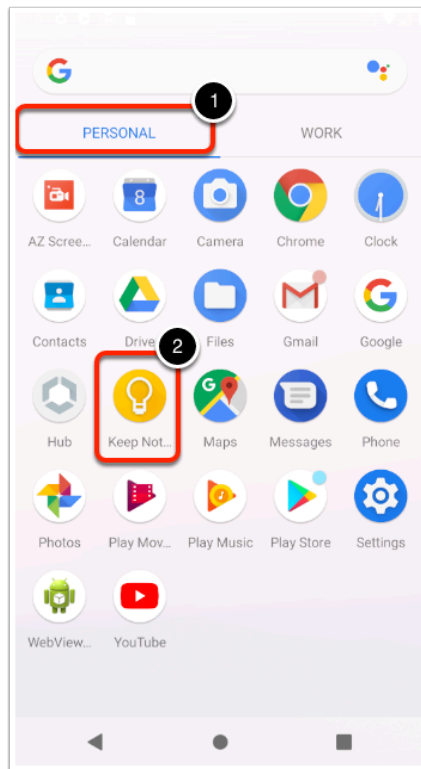


5. In the Chrome Browser,
- In the **Search** area,
 - Enter a website , like <https://en.m.wikipedia.org/>

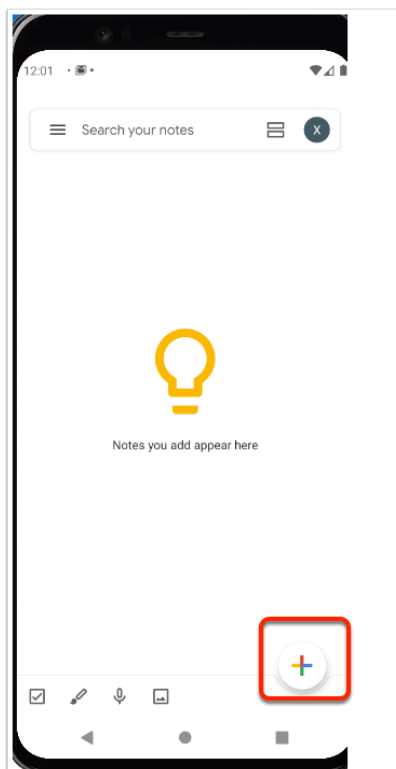


6. In your **Wikipedia** page

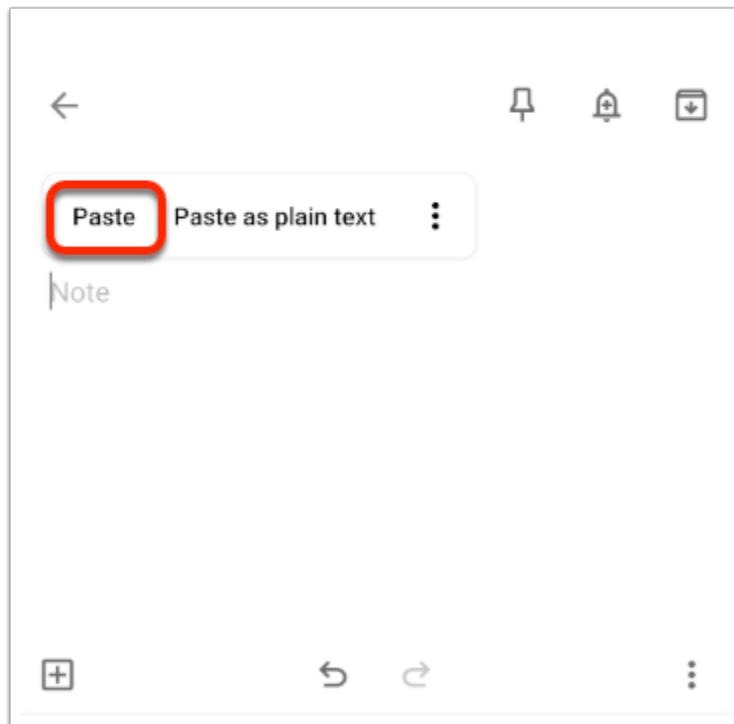
- **Copy** a section of text , If you are using the emulator, double click on the text and move the selection indicators to include more.
- When you are complete, **Close** the Chrome window (Use the "Menu"button and swipe up on your chrome application)



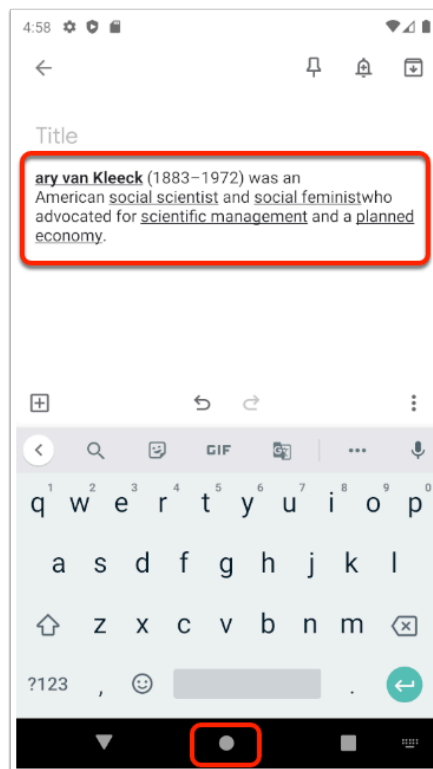
7. Open your **Application** Menu,
- Select the **Personal** apps
 - Select the **Google Keep** app.



8. On the **Google Keep** app select the **Plus Sign** to add a new note.

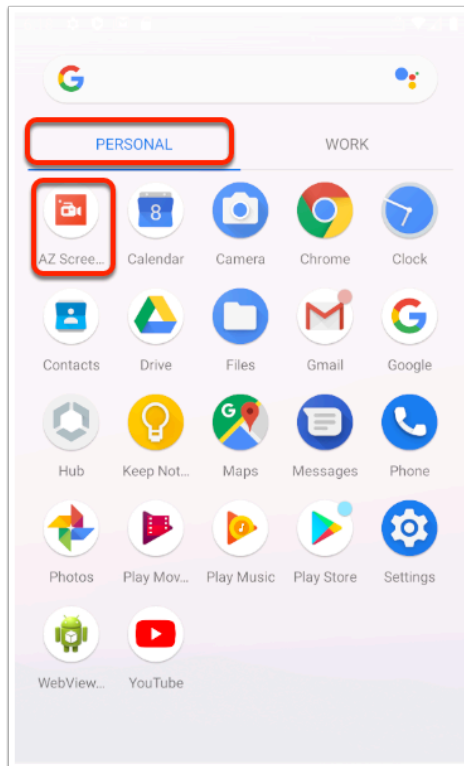


9. Tap and hold *within* the main text field and Select **Paste**

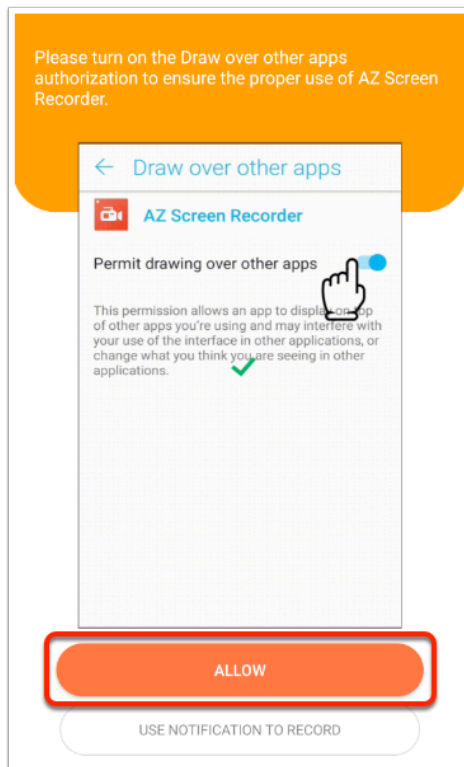


- i** Your paste operation should have been successful, that means theres no limitation on copy and paste operations between personal and work profiles with the current settings in Workspace ONE UEM. You can now close this window.

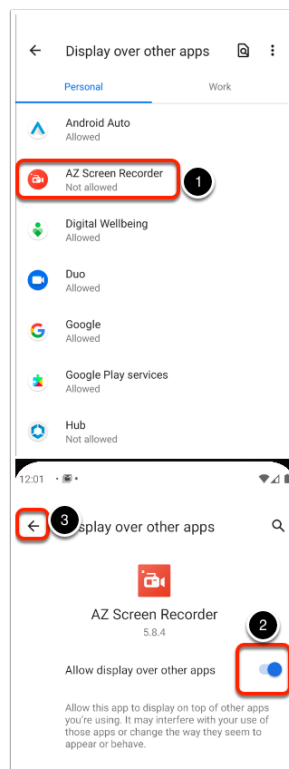
Part 3: Testing initial screen recording behaviour



1. On your Android device
 - In the **Application menu** , select your **PERSONAL** profile
 - Open **AZ Screen Recorder**

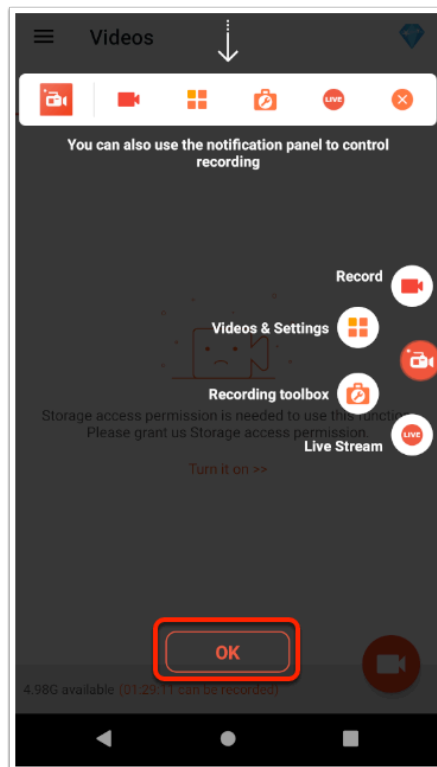


2. On the Draw over other apps prompt select **ALLOW**, this will Permit drawing over other apps

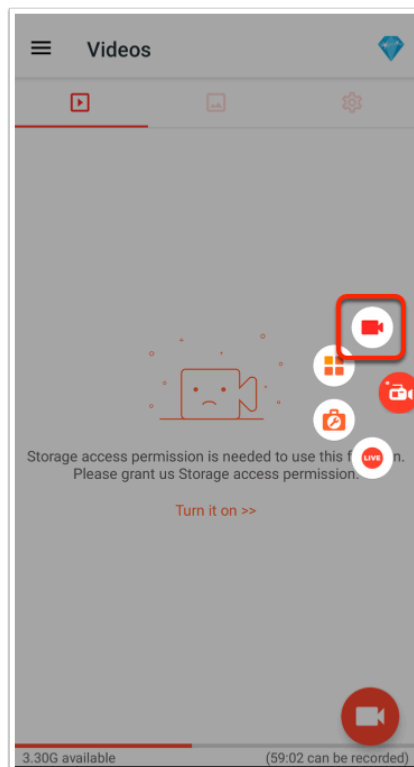


3. In the **application permission** window:
 - Tap Az screen Recorder
 - Move the slider next to **Allow display over other apps** from NO to YES (blue)

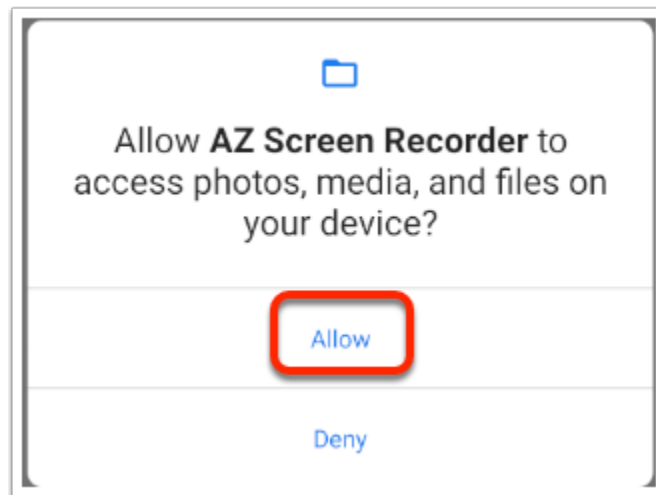
- Tap **back** twice to return to the application



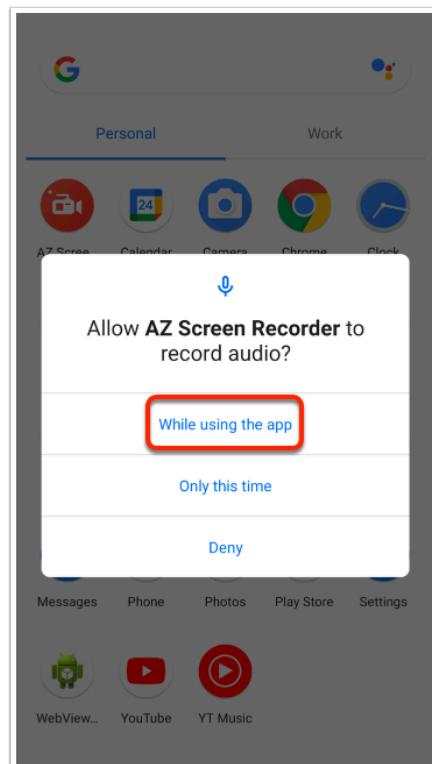
4. Select **OK** to acknowledge the information window



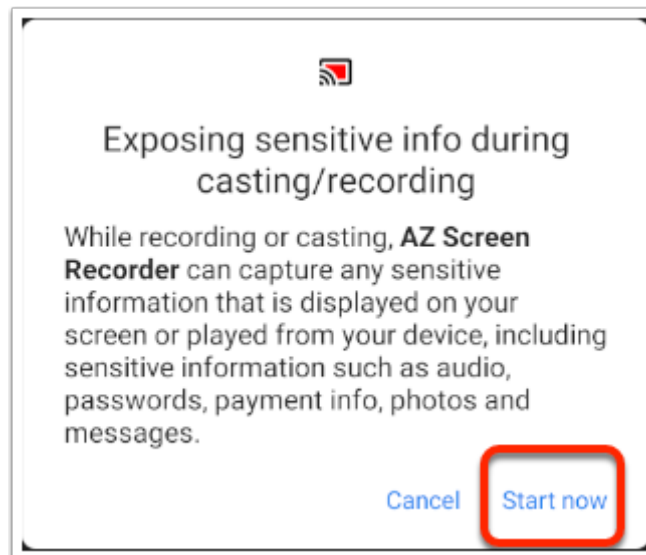
5. Select **the camera icon** to start recording



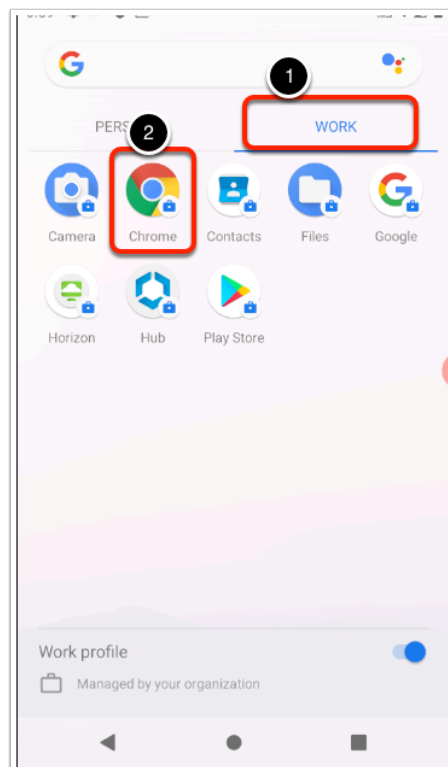
6. In the **Allow AZ Screen Recorder** window select **Allow** to grant **device Access**



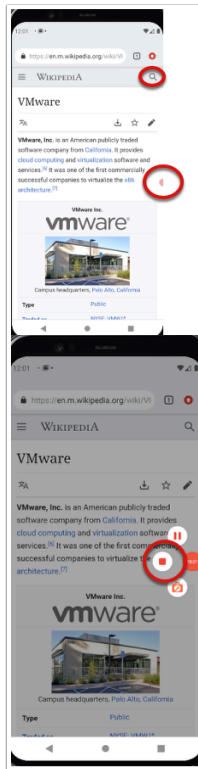
7. In the **Allow AZ Screen Recorder to record audio** window select **While using the app** to grant audio recording permission



8. In the **Exposing sensitive info during casting/recording** window select **Start now**

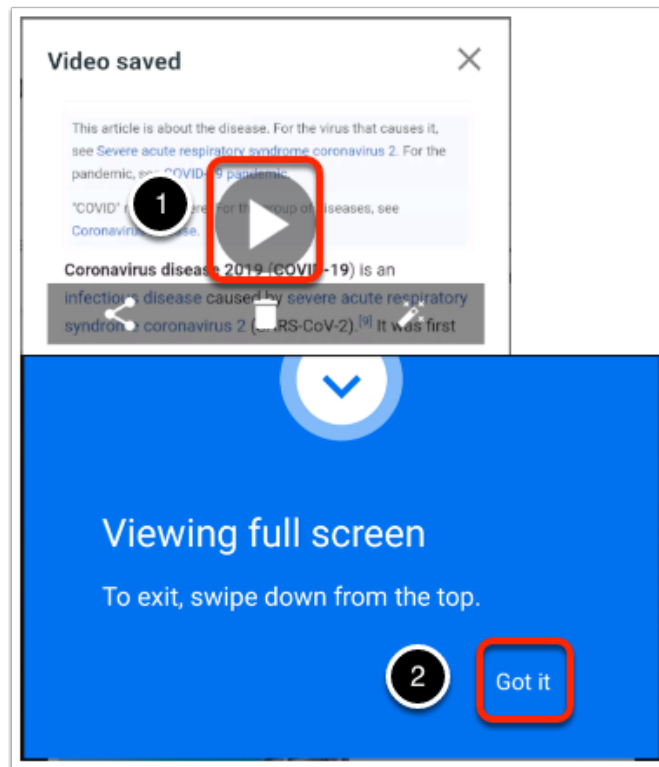


9. On your Android device
- Switch to the **Application Menu**
 - Select your **WORK** profile
 - Open **Chrome**



10. In the Chrome browser

- Navigate to a **different web page** so we can try to capture a couple of seconds of video
- Open the AZ Recorder menu by pressing the round **red button** stick half-way out on the right side
- Select the **stop button**

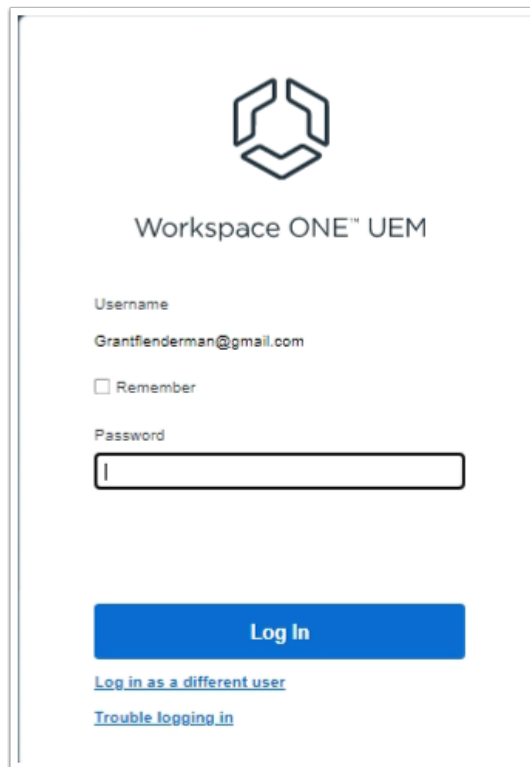


11. In the Video saved window

- Select **Play** the resulting video
- Tap **Got it** to continue watching the video in full screen
- It should have captured what you did in your **WORK** profile Chrome application which means currently there is no limitation in the screen recording functionality and the capture of your corporate apps.

Part 4: Creating a profile to protect the work apps

- i** We are now going to configure a device profile to control the interaction between apps in the work and personal profiles. This configuration is done on the **Workspace One UEM** console and you can do it from the browser on your own computer.



Workspace ONE™ UEM

Username
Grantfienderman@gmail.com

☐ Remember

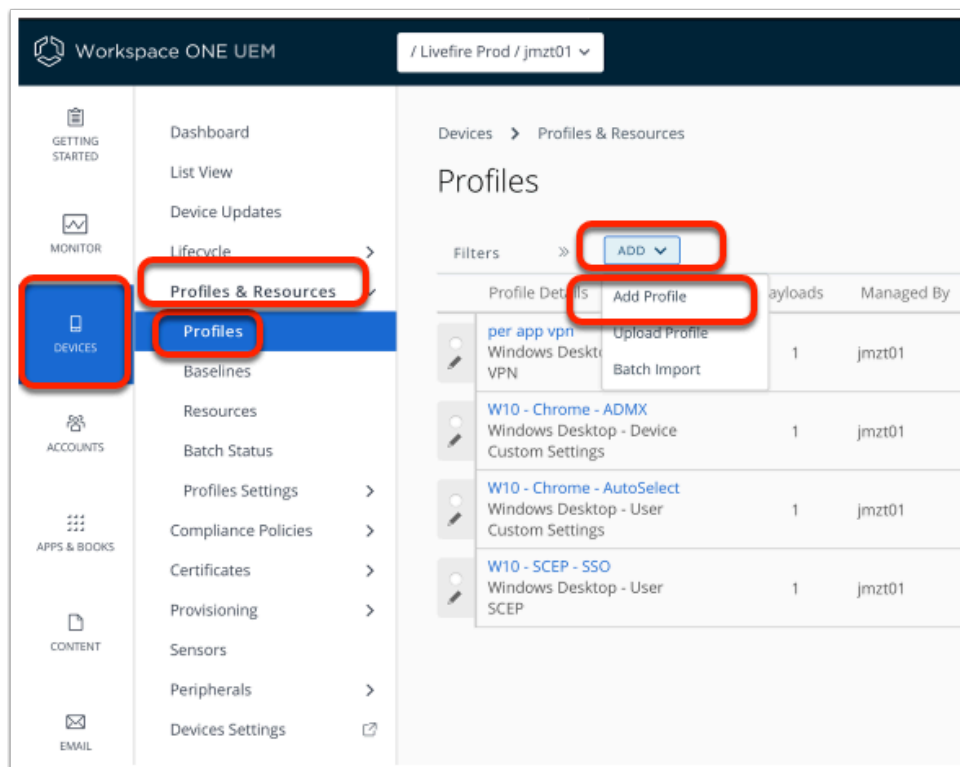
Password
|

Log In

[Log in as a different user](#)

[Trouble logging in](#)

- From your browser,
 - Type <https://cn-livewire.awmdm.com>
 - Log in with the custom credentials you received in your email.



Workspace ONE UEM / Livefire Prod / jmzt01

GETTING STARTED

MONITOR

DEVICES

ACCOUNTS

APPS & BOOKS

CONTENT

EMAIL

Dashboard

List View

Device Updates

Lifecycle

Profiles & Resources

Profiles

Baselines

Resources

Batch Status

Profiles Settings

Compliance Policies

Certificates

Provisioning

Sensors

Peripherals

Devices Settings

Devices > Profiles & Resources

Profiles

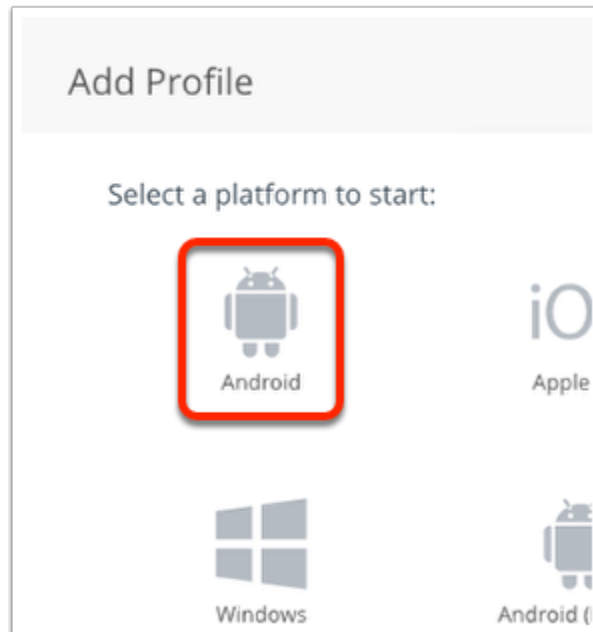
Filters > ADD

Profile Details Add Profile

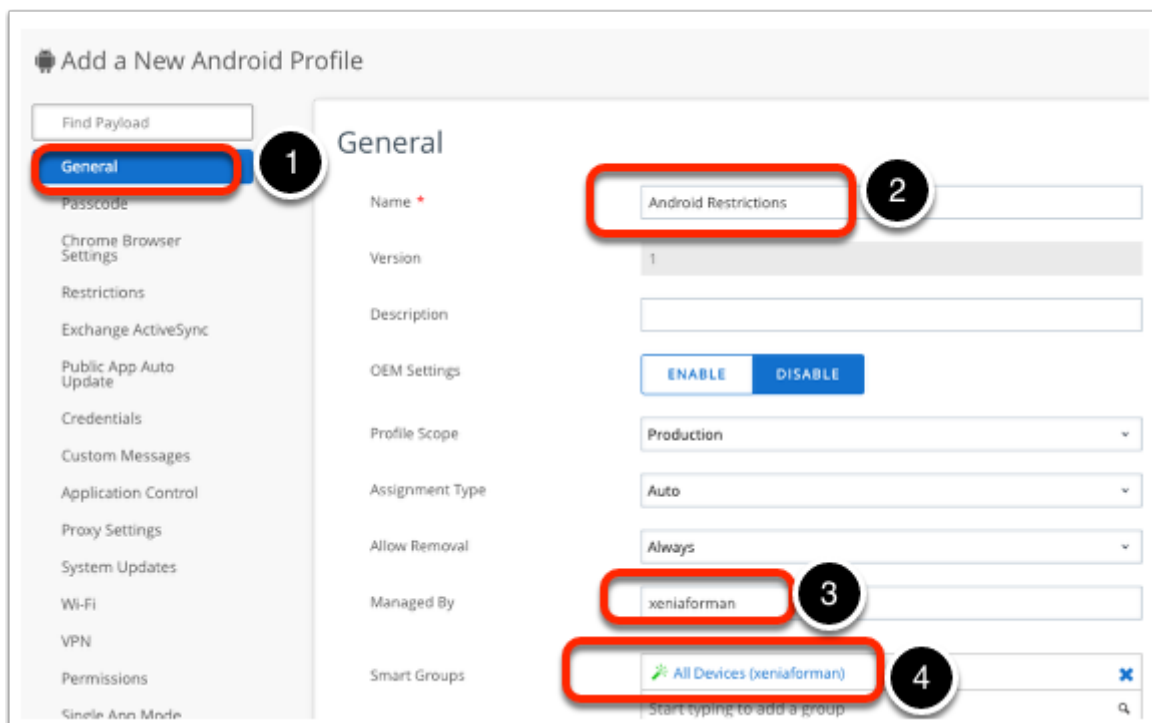
Profile Details	Upload Profile	Batch Import	ayloads	Managed By
per app vpn Windows Desktop - User VPN	1			jmzt01
W10 - Chrome - ADMX Windows Desktop - Device Custom Settings	1			jmzt01
W10 - Chrome - AutoSelect Windows Desktop - User Custom Settings	1			jmzt01
W10 - SCEP - SSO Windows Desktop - User SCEP	1			jmzt01

- In the Workspace ONE UEM Console follow the follow steps to create a device profile:
 - On the left side Menu, select **Devices**

- Expand **Profiles & Resources**
- Select **Profiles**
- Under profiles select **ADD**
- In **ADD** dropdown select **Add Profile**



3. In the Add Profile window
 - Select **Android**



4. In the Add a New Android Profile window, **General** options
 - In the **Name** field, type **Android Restrictions**
 - In the **"Managed By"** field, ensure your **Organizational Group** is selected.

- In the **Smart Groups** field, select **All Devices**
- Scroll down to the end of the page

Add a New Android Profile

Find Payload

General

Passcode

Chrome Browser Settings

Restrictions

Exchange ActiveSync

Public App Auto Update

Credentials

Custom Messages

Application Control

Proxy Settings

System Updates

Wi-Fi

VPN

Permissions

Single App Mode

Launcher

Enterprise Factory Reset Protection

OEM Settings: **ENABLE** **DISABLE**

Profile Scope: Production

Assignment Type: Auto

Allow Removal: Always

Managed By: Jesus_ZeroTrust

Smart Groups: All Devices (Jesus_ZeroTrust) **X**

Start typing to add a group

Exclusions: **NO** **YES**

VIEW DEVICE ASSIGNMENT

Additional Assignment Criteria

☐ Install only on devices inside selected areas

☐ Enable Scheduling and install only during selected time periods

SAVE AND PUBLISH **CANCEL**

5. Select **VIEW DEVICE ASSIGNMENT**

View Device Assignment

Assignment Status: All Filter Grid

Assignment Status	Friendly Name	User	Platform/OS/Model	Phone Number	Organization Group
Added	Mark Android Android 12.0.0 RIAL	Mark	Android / Android 12.0.0 / Android	+15551234567	grant2TRNEL
Added	Mark Android Android 12.0.0 RIAL	Mark	Android / Android 12.0.0 / Android	+15551234567	grant2TRNEL

Items 1-2 of 2

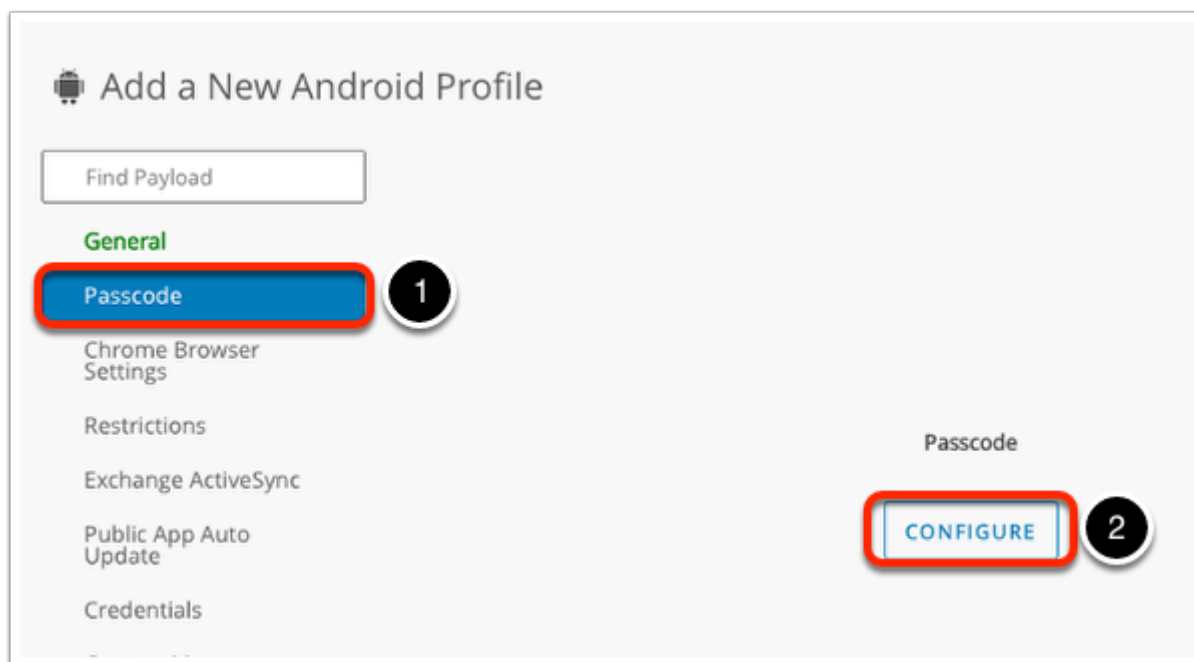
Page Size: 20

CANCEL

6. In the **VIEW DEVICE ASSIGNMENT** window

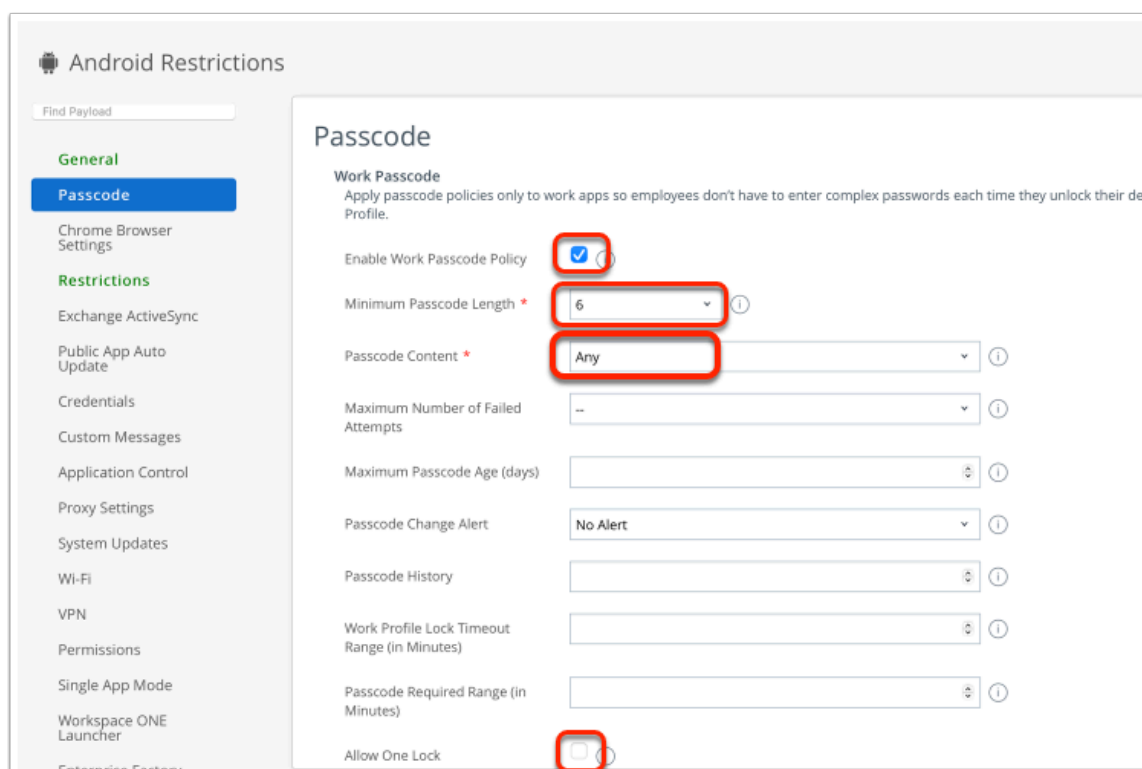
- Check the device list, and verify you enrolled android device is there

- Select **CANCEL**



7. In the **Add a New Android Profile** window

- In the left pane select **Passcode**
- Select **CONFIGURE** in the main pane.



8. On the **Passcode** settings:

- Check the box next to **Enable Work Passcode policy**
- Change the **Minimum Passcode Length** to **6**

- **Passcode Content** dropdown menu select **Any**
- Uncheck the box next to **Allow One Lock**.
 - This will force the user to configure a different passcode for the work profile.



9. In the **Add a New Android Profile** window:

- In the left hand menu, select **Restrictions**
- Select **CONFIGURE**
- Please take a moment to look at the available options while going through the steps in this guide.

android restrictions

Find Payload

General

Passcode

Chrome Browser Settings

Restrictions

Exchange ActiveSync

Public App Auto Update

Credentials

Custom Messages

Application Control

Proxy Settings

Restrictions

Configure Work Profile settings to manage policies across work-only apps. Configure Work Mar apply policies across the entire device. Configuration of both Work Profile and Work Managed I Corporate Owned Personally Enabled devices.

Device Functionality

	Work Managed Device	Work Profile
Allow Factory Reset	<input checked="" type="checkbox"/>	
Allow screen capture	<input type="checkbox"/>	<input type="checkbox"/>
Allow adding Google accounts	<input type="checkbox"/>	<input type="checkbox"/>
Allow removing the Android Work account	<input checked="" type="checkbox"/>	

10. Under **Device functionality**,
 - Uncheck the boxes next to **Allow screen capture**
 - Under both **Work Managed Device** and **Work Profile**

Custom Messages

Application Control

Proxy Settings

System Updates

Wi-Fi

VPN

Permissions

Single App Mode

Workspace ONE Launcher

Enterprise Factory Reset Protection

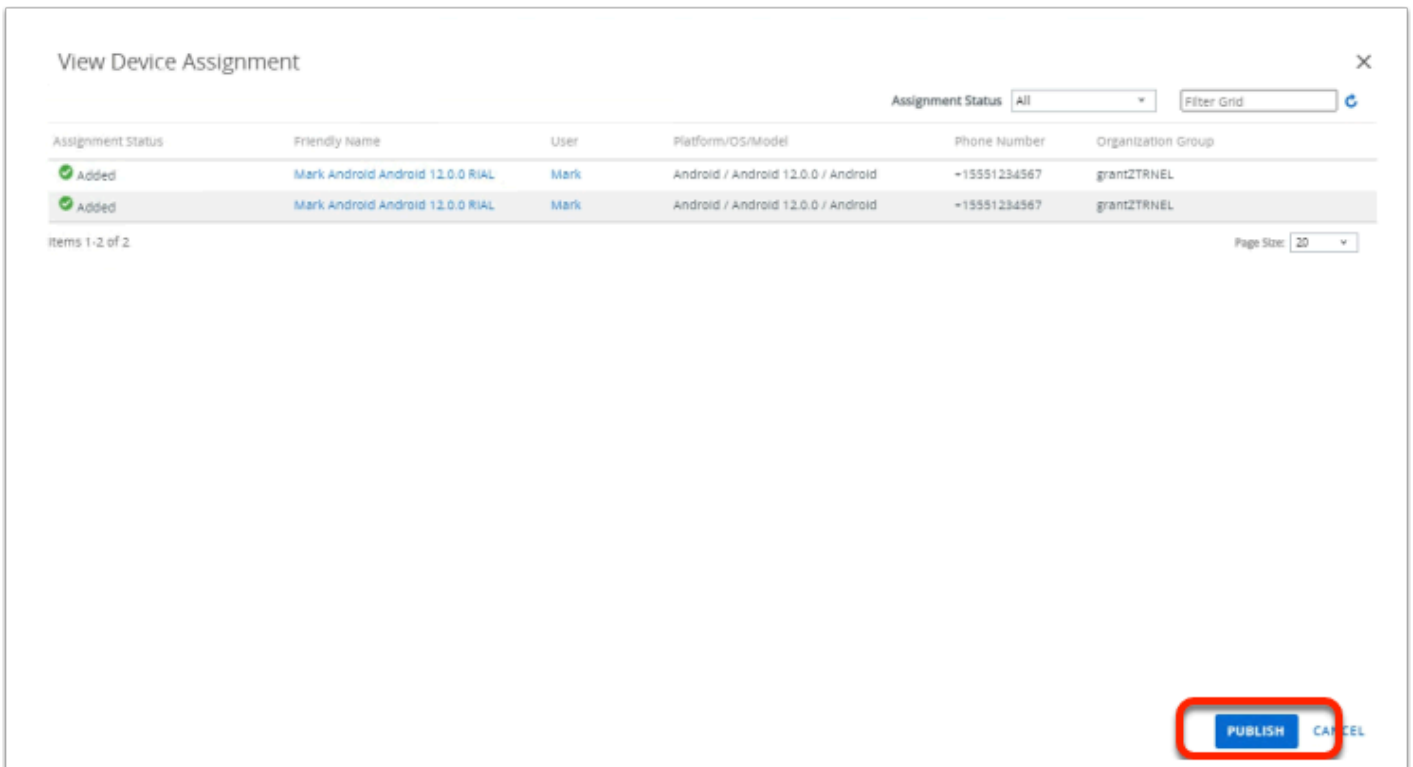
Work and Personal

	Work Managed Device	Work Profile
Allow Pasting clipboard between work and personal apps		<input type="checkbox"/>
Allow personal apps to share data with work apps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Allow work apps to access documents from personal apps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Allow personal apps to access documents from work apps	<input type="checkbox"/>	<input type="checkbox"/>

Android 9.0+

SAVE AND PUBLISH CANCEL

11. **Scroll down** to the **Work and Personal** section:
 - Verify the box next to **Allow pasting clipboard between work and personal apps** is unchecked
 - Select **SAVE AND PUBLISH**

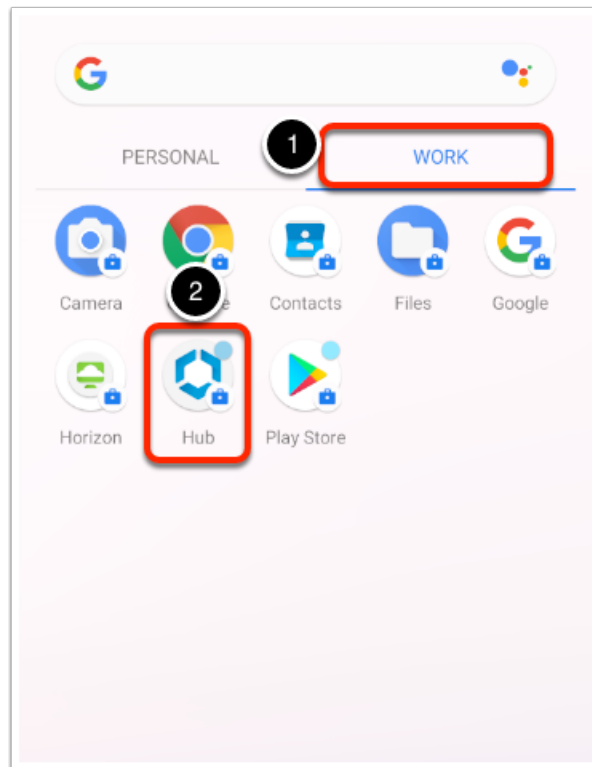


12. In the **view assignment** window

- Select **PUBLISH**.
 - You can now close this browser window.
 - It can take up to 5 minutes for the policies to get to the device, so it's a good time for a brake.

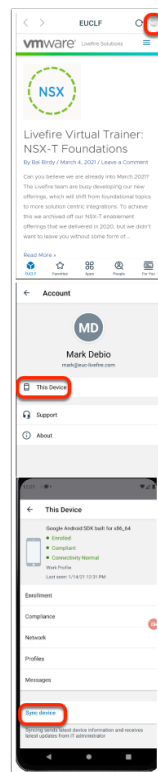
Part 5: Testing the passcode policy

The following steps will make sure your device has synced and your profile has been downloaded. If you get a prompt saying "**Your current passcode does not satisfy the requirement set by the organization**" move on to step 3



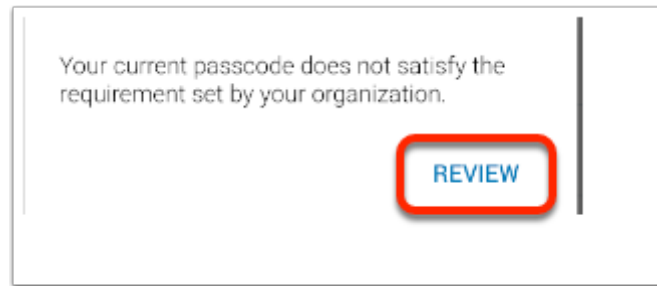
1. On your android device from your Application menu:

- Select the **WORK** profile
- Open the **Intelligent hub**

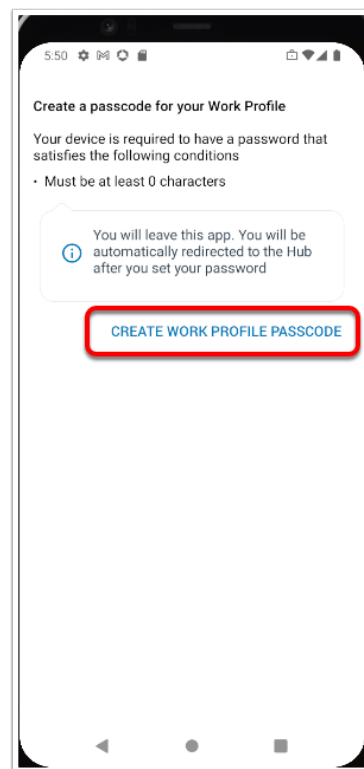


2. On your Android Device's intelligent hub

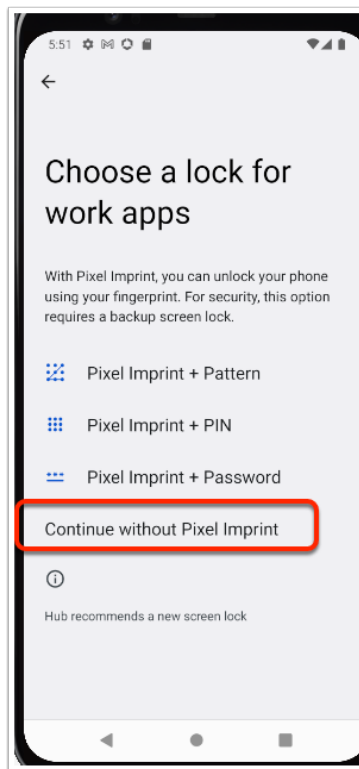
- Tap the "**MD**" icon on the top right (initials for Mark Debio)
- Under **Accounts**, select **This Device**
- In This Device, select **Sync device**
 - This will ensure that your profile is synced and will trigger the policies in the next step



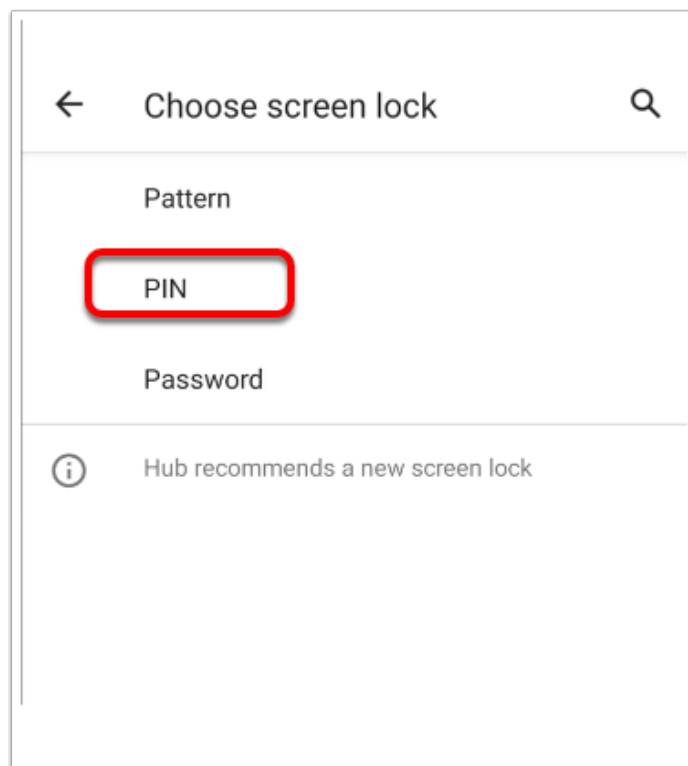
3. When prompted
 - In the "**Your current passcode does not satisfy the requirement set by your organization**" message
 - Select **REVIEW**



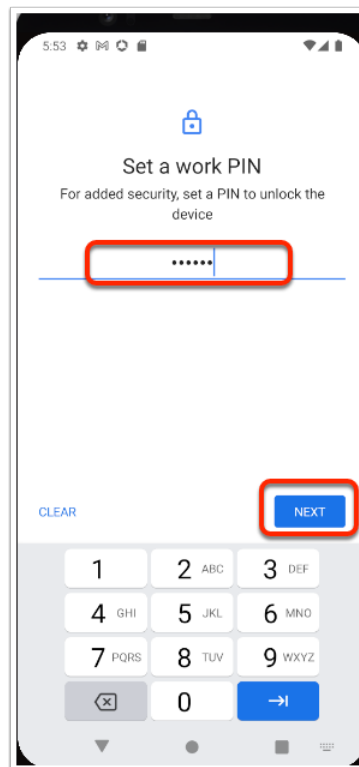
4. In the **Create a passcode for your Work Profile** window
 - Select **CREATE WORK PROFILE PASSCODE**



5. On the **Choose screen lock** window,
 - Select **Continue without Pixel imprint**

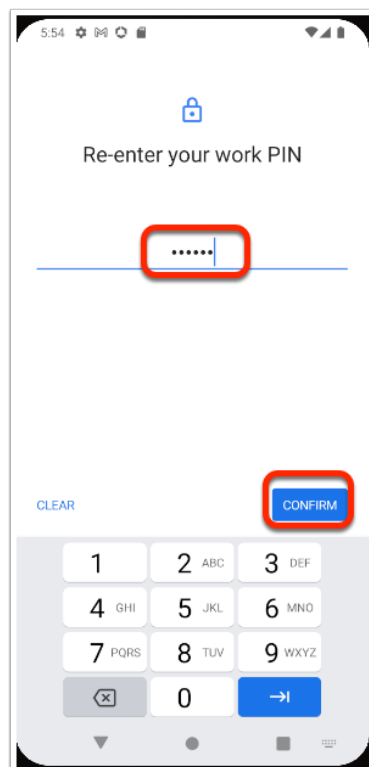


6. In the **Choose screen lock** window
 - Select **PIN**



7. In the Set a work PIN window

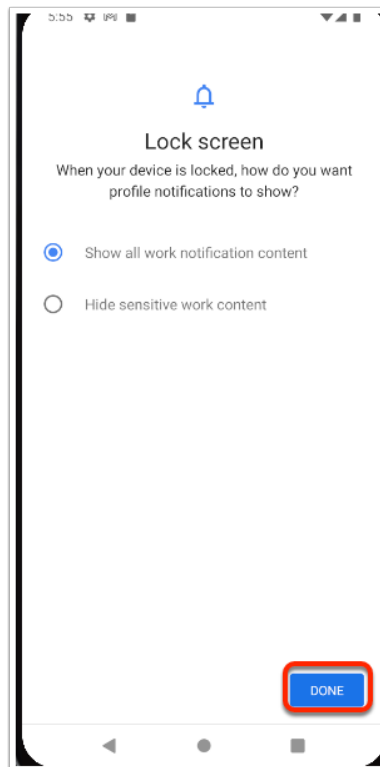
- Type **111111** for the device PIN
- Select **NEXT**



8. On the **Re-enter** screen

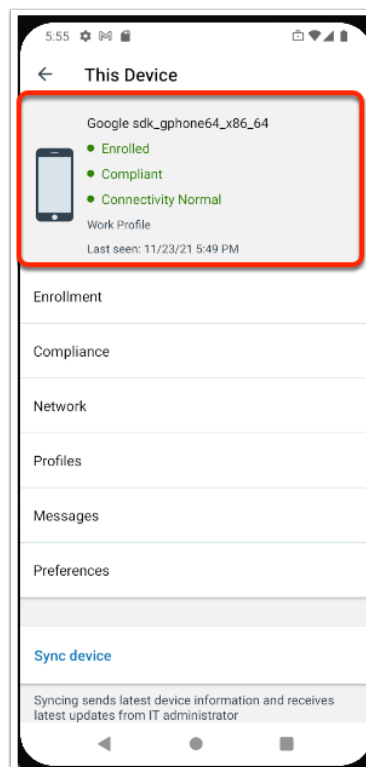
- Type **111111** for the device PIN

- Select **CONFIRM**



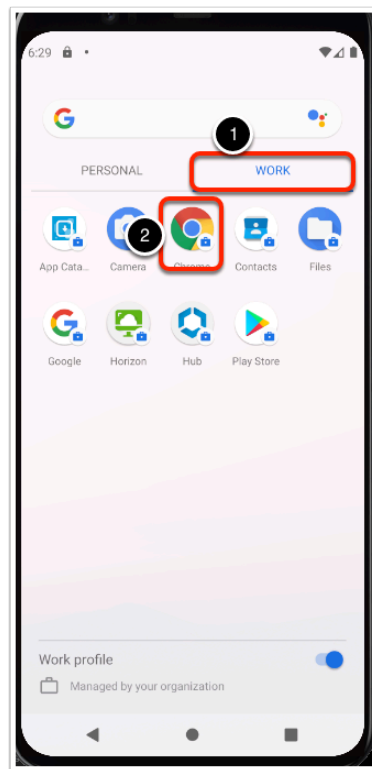
9. On the **Lock screen** window

- Select **DONE**



10. In the **This Device** window

- Observe that your device shows up as **Enrolled** and **Compliant**



11. On your Android Device

- Switch to the Applications menu
- Select your **WORK** profile
- Open **Chrome**
 - Note. If you have difficulty getting this to work.
 - On your laptop / Desktop.
 - Go to Android Studio.
 - Select your device and Cold Boot the device
 - The go back to your WORK profile
 - Open Chrome

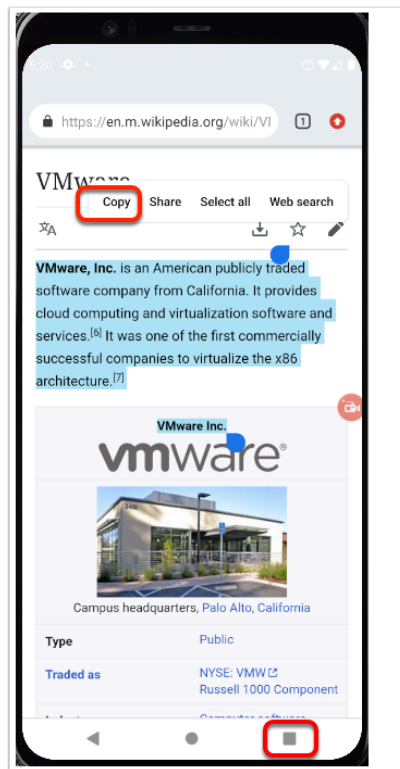


12. On the Re-enter your PIN

- Enter **111111**
- Select **Enter**

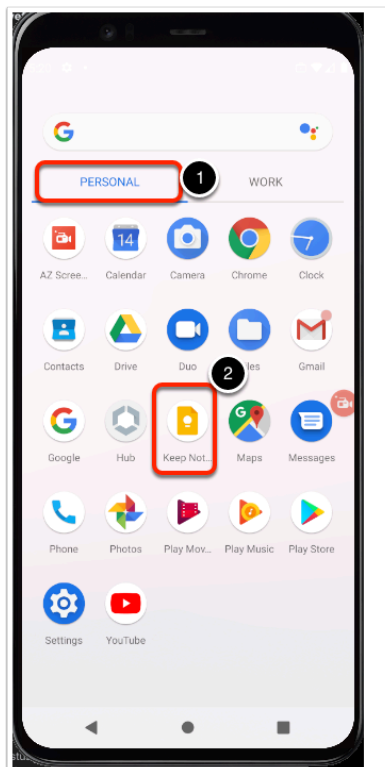
Part 6: Testing application behaviour

In this part we will check the behaviour of the applications after the policy is applied.



1. On the corporate Chrome browser

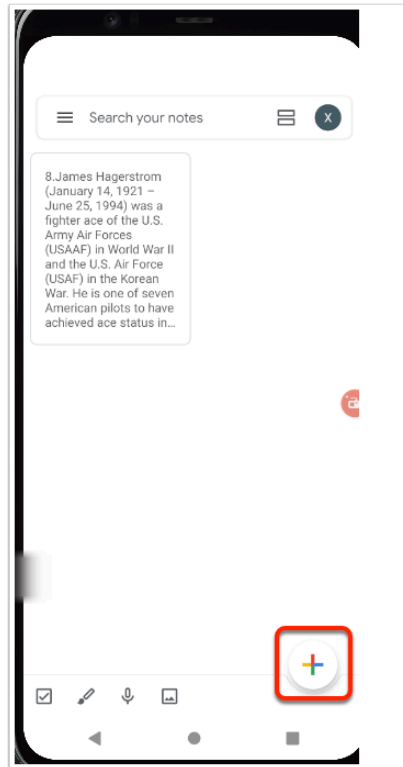
- Select and **Copy** text from any website you left open on the previous step
- After copying, **close** the browser



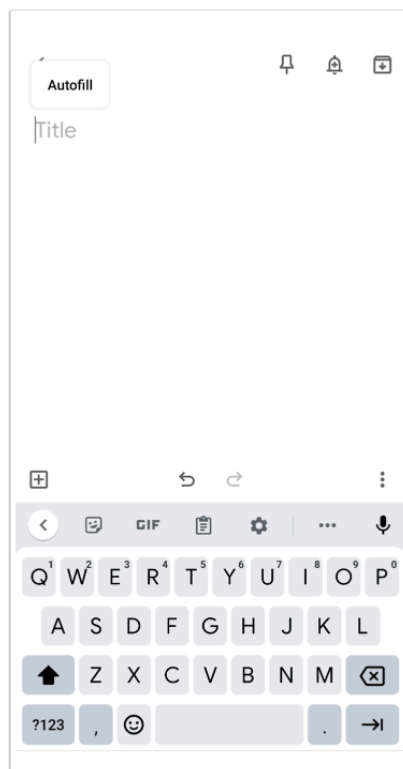
2. From your Application menu,

- Select your **PERSONAL** profile

- Select **Google Keep**



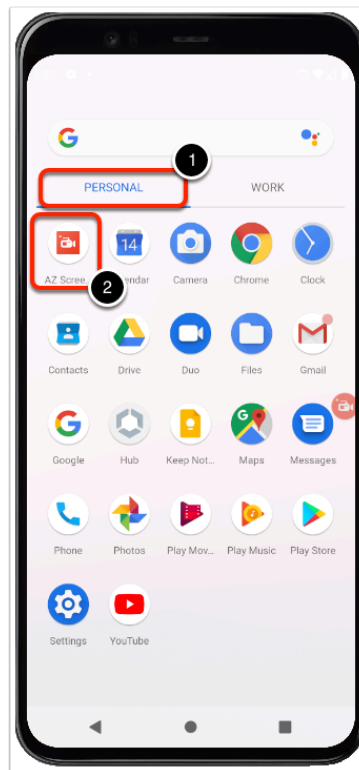
3. In Google Keep, Tap on the **Plus Sign** to create a new document



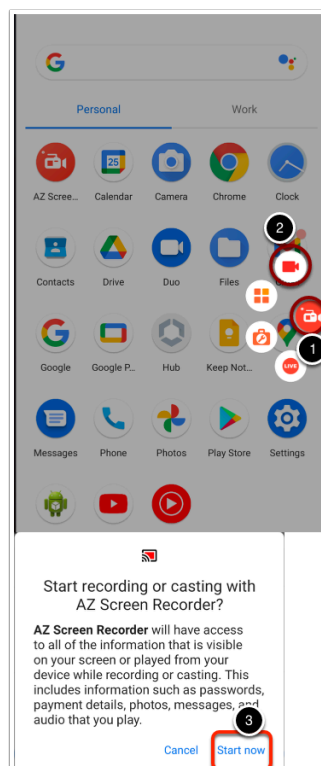
4. In Google Keep

- Tap and hold on the text field to **attempt** to **Paste** from the context menu.

- The operation should fail due to the policy applied earlier

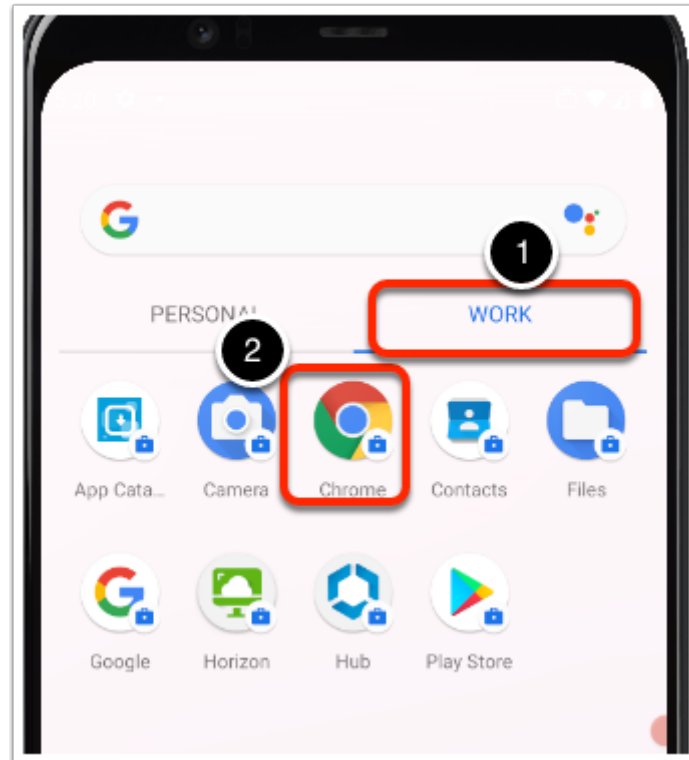


5. In your application menu, In the PERSONAL profile, Open the **AZ Screen recorder**

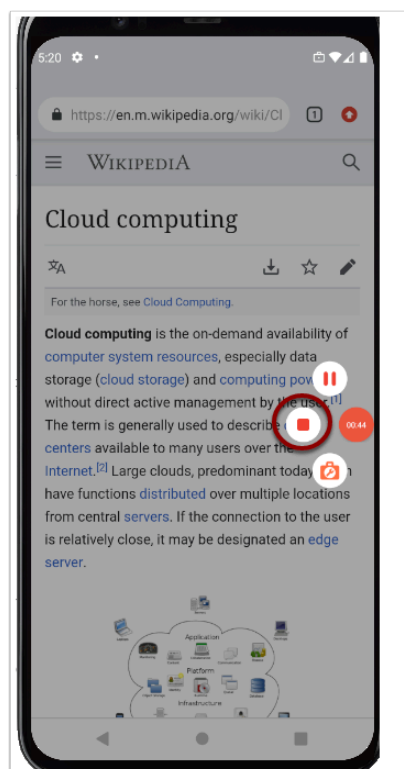


6. To start a recording:
- Select the **AZ icon** sticking out of the right side
 - Select the **Camera icon** to start recording

- When prompted tap **Start now**

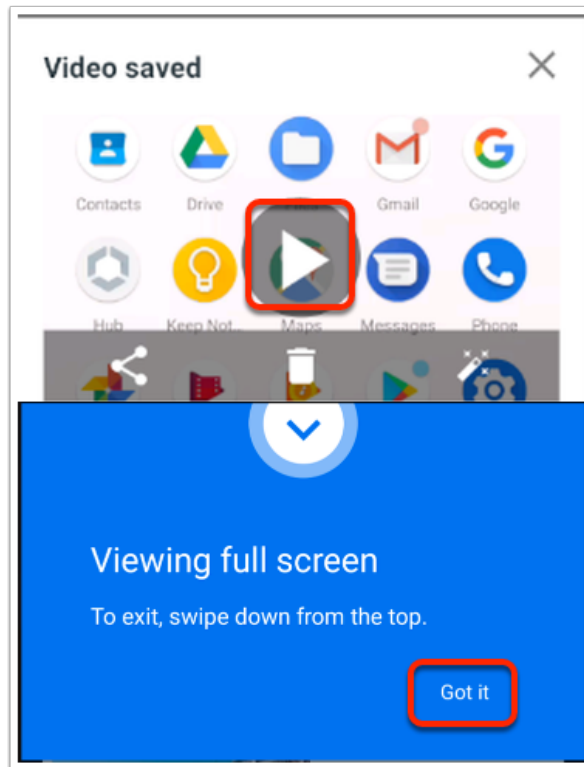


7. On your Applications menu,
 - Select the **WORK** profile
 - Open **Chrome**



8. In your Chrome browser

- Load a page, to test to see if the Screen Recorder controls continue to record
- stop the recording by tapping the **Stop** icon on the AZ Recorder app menu



9. On your Android Device

- Play the recording, and if prompted tap **Got it** in the "**Viewing full Screen**" prompt
- It should show a black screen when you open Chrome, this means the policy is blocking the recording of the screen.

i These results mean we successfully controlled interaction between personal and work profiles, in a real scenario this would help organizations prevent data leaks from the use of personal devices.