android

Fully managed device

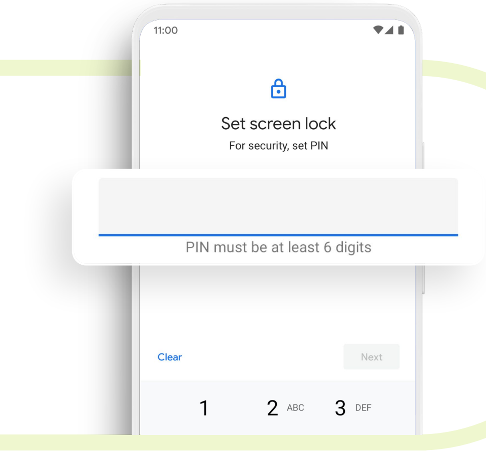
For company-owned devices that are meant to be actively managed with no personal usage allowed, Android Enterprise offers fully managed device management. The solution set offers a higher degree of control over an extended range of device settings, with extra policy controls and full access to device data compared to the work profile. It works well for knowledge workers who are expected to use the device for work only.

How to use this guide

This demo guide will take you on a quick tour of some of the top features of a fully managed device. When you're done, you can delete the demo. **Note: This demo will require that the device has been factory reset.**

STEP 1

Set strong passcode on device



Set screen lock

For security, set PIN

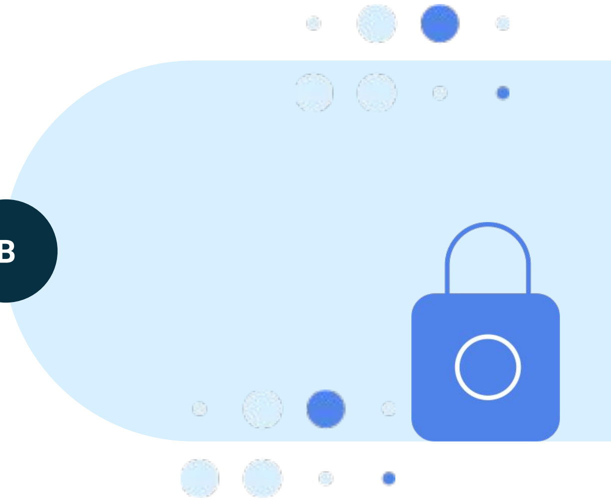
PIN must be at least 6 digits

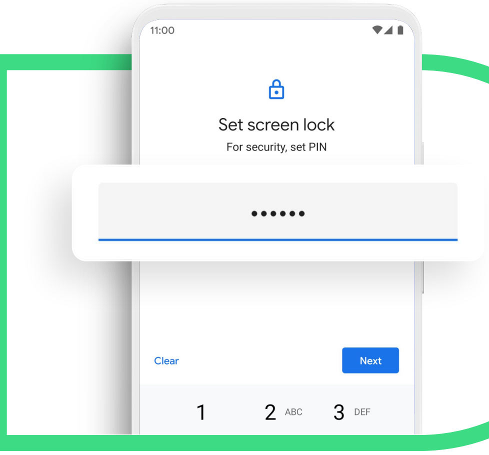
A

During the setup process, you'll come to a step that requires you to "Set a screen lock". Select an option that includes a PIN. Notice how the device will require that "Your PIN must be at least 6 digits".

B

This demonstrates that your organization can set various levels of complexity for your passcode to ensure your passcode meets its requirements.





Set screen lock

For security, set PIN

••••••

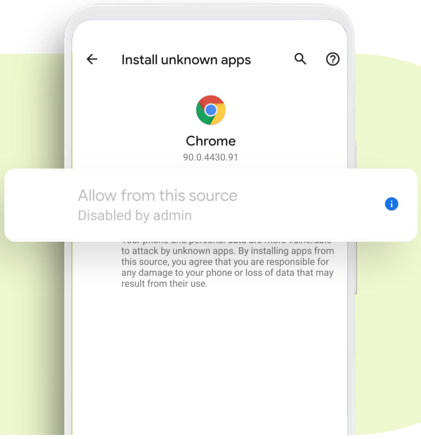
C

Enter a 6 digit passcode and confirm the passcode to move on.

Illustrations and steps based on Google Pixel devices. Your experience may vary based on your device.

STEP 2

Disable downloading of unknown apps



Install unknown apps

Chrome
90.0.4430.91

Allow from this source
Disabled by admin

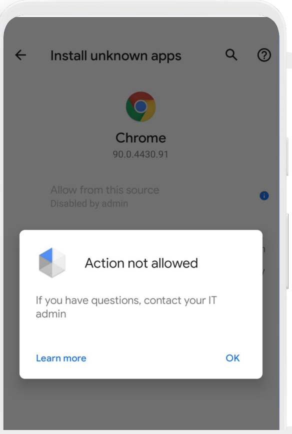
Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.

A

In settings, navigate to Apps & notifications. The exact name may appear differently on your phone. Select “Special app access” and then tap “Install unknown apps” Select one of the apps to try and allow unknown apps from this source. Notice that the option to “Allow from this source” has been “Disabled by admin.”

This is an important control that allows IT to ensure that employees are not downloading potentially harmful apps from the Internet or through email or other sources. It means that employees will access apps through the Google Play store where applications are reviewed and vetted by Google Play Protect.

B



Install unknown apps

Chrome
90.0.4430.91

Allow from this source
Disabled by admin

Action not allowed

If you have questions, contact your IT admin

Learn more   OK

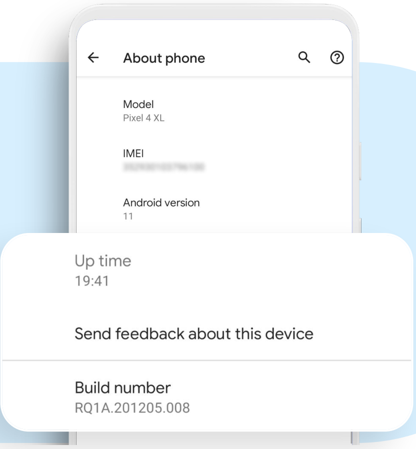
C

Click on the information icon. That’s where a toggle would normally be to allow unknown apps. You’ll see the message: “Action not allowed”.

android

STEP 3

Disable developer options


About phone

Model
Pixel 4 XL

IMEI
[redacted]

Android version
11

Up time
19:41

Send feedback about this device

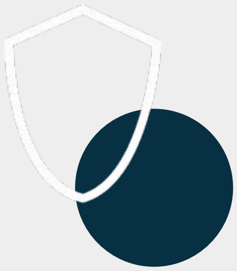
Build number
RQ1A.201205.008

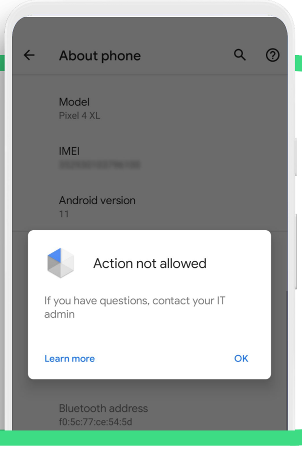
A

In settings, select “About phone” and then scroll down to the “Build number.” On unmanaged phones, you can tap on the “Build number” to access developer options. With Android Enterprise you can disable this feature so employees will not have access to these options.

This is an important control as it ensures employees are not able to do things that might break the device or enable things like USB debugging, which may facilitate a connection to another device that could be insecure.

B




About phone

Model
Pixel 4 XL

IMEI
[redacted]

Android version
11

Action not allowed

If you have questions, contact your IT admin

Learn more OK

Bluetooth address
f0:5c:77:ce:54:5d

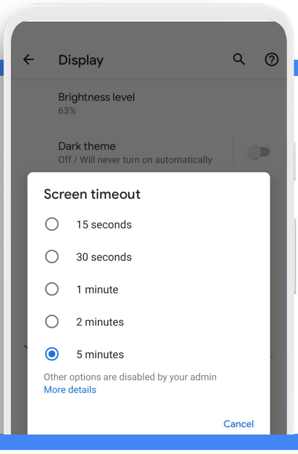
C

Tap the “Build number” and notice that you should get a message that you are unable to perform the action.

android

STEP 4

Lockscreen time-out


Display

Brightness level
63%

Dark theme
Off / Will never turn on automatically

Screen timeout

○ 15 seconds
○ 30 seconds
○ 1 minute
○ 2 minutes
● 5 minutes

Other options are disabled by your admin
More details

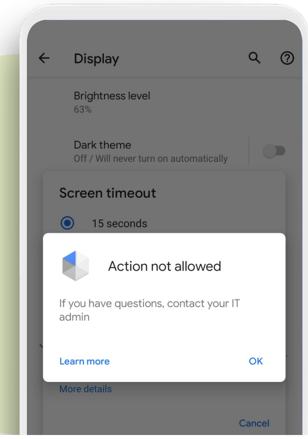
Cancel

A

In settings, select “Display” and then “Screen timeout.” You’ll notice that the maximum screen time allowed is 5 minutes. That’s in contrast to consumer devices that can have screen timeouts of up to 30 min. This means that if an employee’s device is not used for 5 minutes, they’ll need to enter a passcode to unlock the device. You can see that “Other options are disabled by your admin,” which indicates that this is a feature that is managed by IT.

This an important control that helps IT ensure that employees who leave their devices unattended aren’t exposing company data to anyone who picks up the unlocked device.

B


Display

Brightness level
63%

Dark theme
Off / Will never turn on automatically

Screen timeout

● 15 seconds

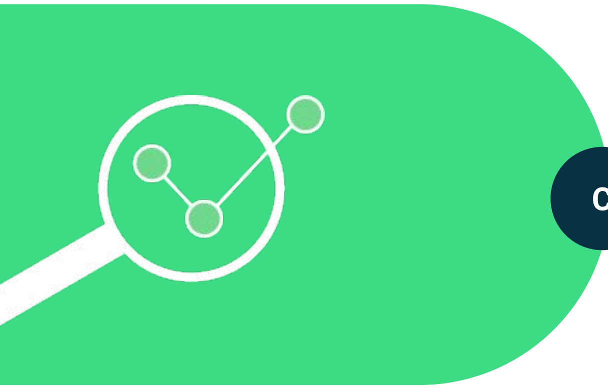
Action not allowed

If you have questions, contact your IT admin

Learn more OK

More details

Cancel

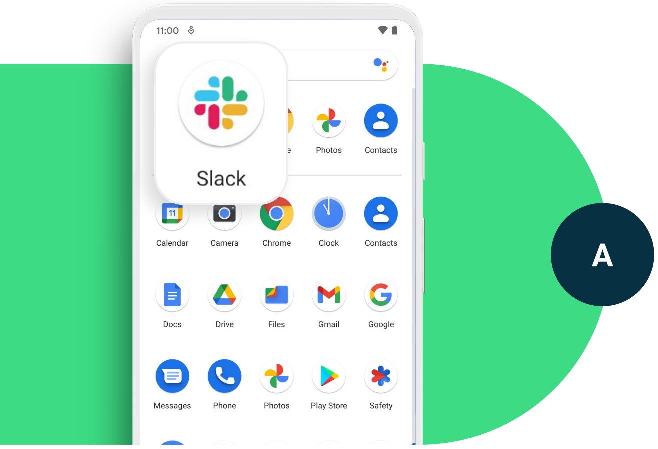


C

Set a different timeout if you like **or select “More details” to get more information.** Employees can choose a shorter timeout but can’t choose anything longer than 5 minutes.

STEP 5

Silently installed apps



In the All Apps drawer, find the Slack app. You’ll notice that this is not a system app but a third-party app.

This demonstrates how IT can silently install apps on a fully managed device.

Conclusion

We hope this guide has been helpful in demonstrating what full device management is like on a managed phone. This is a good solution when a device is meant only for work usage and there is no mixing of personal data on the phone. It offers granular control for full device and app management.

You can keep using this demo to get more experience with it. Or you can remove it by going to settings and factory resetting this device. For more information, visit android.com/enterprise/demo.

android