android

Vollständig verwaltetes Gerät

Für unternehmenseigene Geräte, die aktiv verwaltet werden sollen, aber nicht für private Zwecke verwendet werden dürfen, bietet Ihnen Android Enterprise eine vollständige Geräteverwaltung. Die Lösung bietet mehr Kontrolle über zahlreiche Einstellungen, unter anderem eine strengere Überprüfung der Richtlinien und einen im Vergleich zum Arbeitsprofil vollständigen Zugriff auf Gerätedaten. Die vollständige Geräteverwaltung eignet sich besonders für Wissensarbeiter, die ihr Gerät nur für die Arbeit nutzen dürfen.

Verwendung des Leitfadens

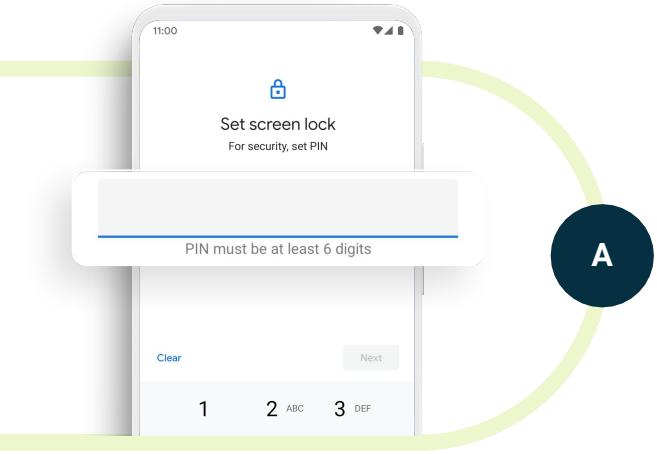
Dieser Demo-Leitfaden gibt Ihnen einen kurzen Überblick über einige der wichtigsten Funktionen eines vollständig verwalteten Geräts. Sobald Sie fertig sind, können Sie die Demo löschen.

Hinweis: Für diese Demo ist es erforderlich, dass das Gerät auf die Werkseinstellungen zurückgesetzt wurde.

android

SCHRITT 1

Einen starken Sicherheitscode auf dem Gerät einstellen

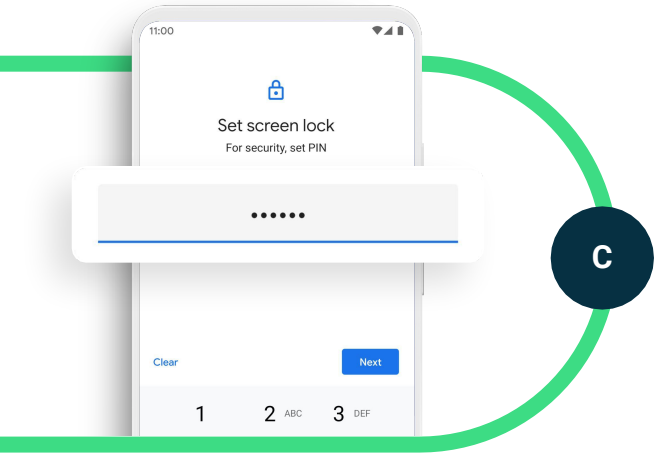


A

Während der Einrichtung gelangen Sie zu dem Schritt „Displaysperre einrichten“. Wählen Sie eine Option, die eine PIN enthält. Achten Sie auf den Hinweis „Die PIN muss aus mindestens 6 Zeichen bestehen“.

Dies zeigt, dass Ihr Unternehmen verschiedene Stufen der Komplexität für Ihren Sicherheitscode festlegen kann, um sicherzustellen, dass er den Anforderungen des Unternehmens entspricht.

B



C

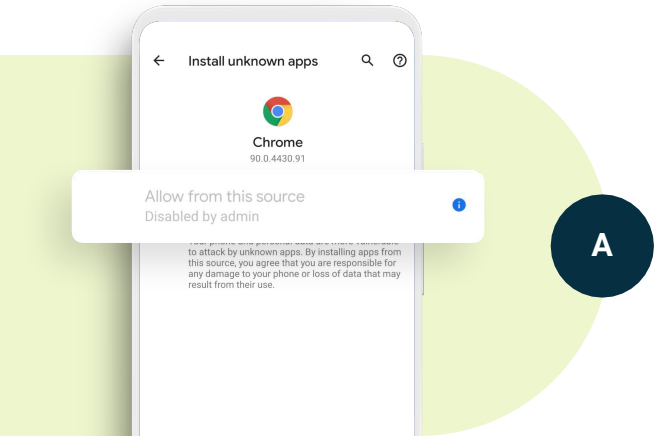
Geben Sie einen Sicherheitscode mit 6 Ziffern ein und bestätigen Sie ihn, um fortzufahren.

Illustrationen und Schritte beziehen sich auf die Einrichtung von Google Pixel-Geräten. Die Einrichtung kann je nach Gerät variieren.

android

SCHRITT 2

2 Download unbekannter Apps deaktivieren

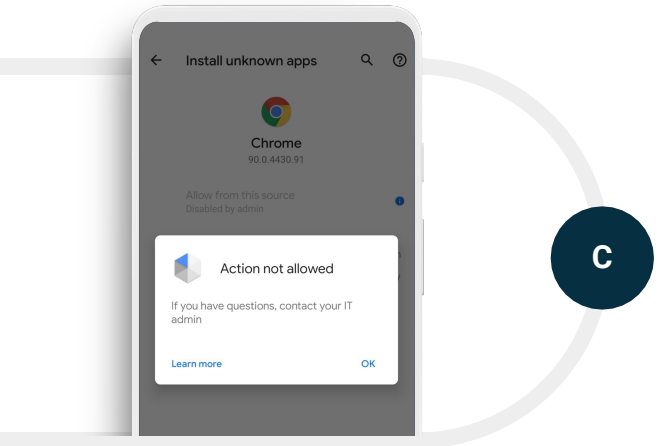


A

Wählen Sie in den Einstellungen die Option „Apps & Benachrichtigungen“ aus. Die genaue Bezeichnung kann auf Ihrem Gerät abweichen. Wählen Sie „Spezieller App-Zugriff“ aus und tippen Sie dann auf „Unbekannte Apps installieren“. Wählen Sie eine der Apps aus, um zum Test unbekannte Apps aus dieser Quelle zuzulassen. Sie sehen, dass die Option „Dieser Quelle vertrauen“ auf „Vom Administrator deaktiviert“ steht.

Dies ist eine wichtige Einstellung, mit der die IT-Abteilung dafür sorgen kann, dass Mitarbeiter keine potenziell schädlichen Apps aus dem Internet, über Links in E-Mails oder aus anderen Quellen herunterladen. Wenn die obige Einstellung ausgewählt ist, können Mitarbeiter nur über den Google Play Store auf Apps zugreifen. Im Google Play Store sind nur Apps verfügbar, die von Google Play Protect geprüft wurden.

B



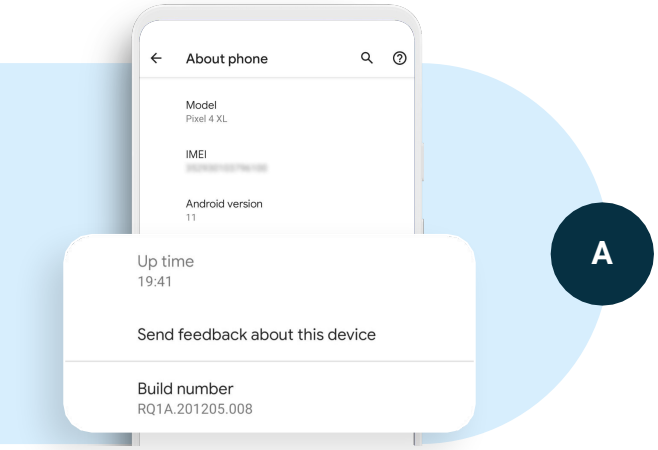
C

Klicken Sie auf das Informationssymbol. Hier würde sich normalerweise eine Ein-/Aus-Schaltfläche befinden, mit der Sie unbekannte Apps erlauben können. Sie sehen allerdings die Benachrichtigung „Aktion nicht zulässig“.

android

SCHRITT 3

3 Entwickleroptionen deaktivieren

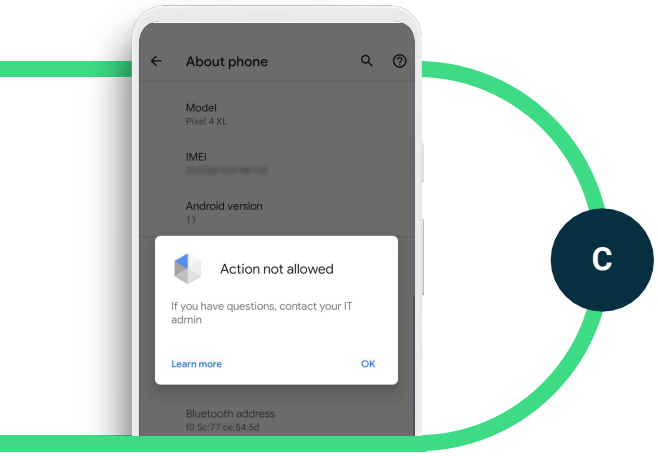


A

Wählen Sie in den Einstellungen „Über das Telefon“ aus und scrollen Sie nach unten zur „Build-Nummer“. Auf Smartphones, die nicht verwaltet werden, können Sie auf die Build-Nummer tippen, um auf die Entwickleroptionen zuzugreifen. Mit Android Enterprise können Sie diese Funktion deaktivieren, sodass Mitarbeiter keinen Zugriff auf diese Optionen haben.

Dies ist eine wichtige Einstellung, die verhindert, dass Mitarbeiter das Gerät schädigen oder Funktionen wie USB-Debugging aktivieren können, wodurch eine Verbindung zu einem anderen, möglicherweise unsicheren Gerät ermöglicht werden könnte.

B



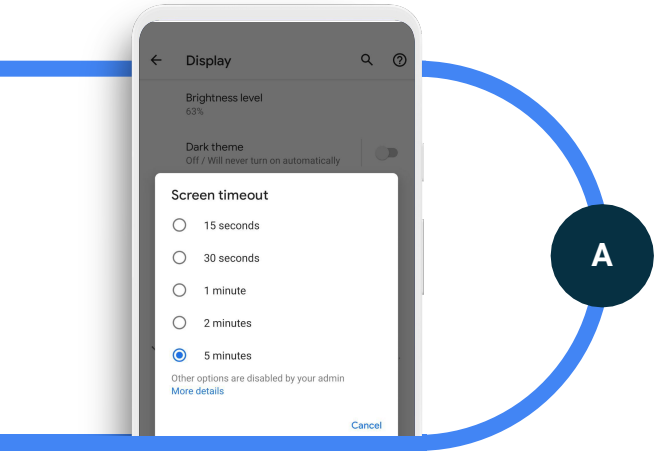
C

Wenn Sie auf die Build-Nummer tippen, sollten Sie eine Benachrichtigung erhalten, dass die Aktion nicht ausgeführt werden kann.

android

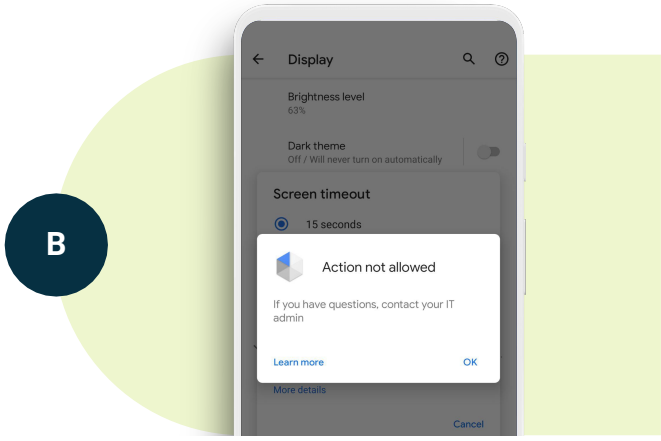
SCHRITT 4

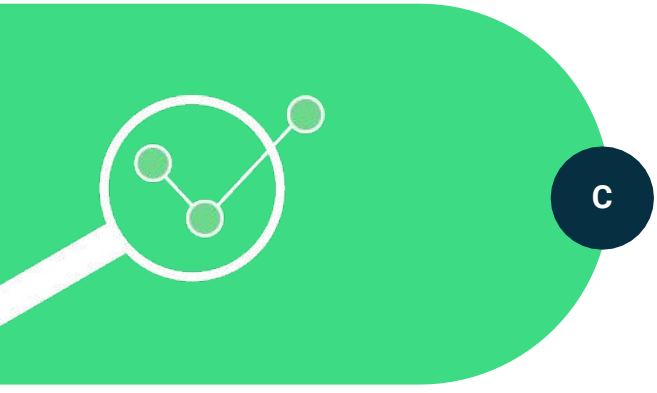
4 Zeitüberschreitung des Sperrbildschirms



Wählen Sie in den Einstellungen „Display“ und dann „Display automatisch ausschalten“ aus. Sie werden sehen, dass die maximale Bildschirmzeit 5 Minuten beträgt, wohingegen die Bildschirmzeit auf Verbrauchergeräten bis zu 30 Minuten betragen kann. Mit der obigen Einstellung legen Sie fest, dass ein Mitarbeiter einen Sicherheitscode eingeben muss, um das Gerät zu entsperren, wenn es länger als 5 Minuten nicht verwendet wurde. Die Option „Andere Optionen wurden von deinem Administrator deaktiviert“ zeigt an, dass es sich um eine Funktion handelt, die von der IT-Abteilung verwaltet wird.

Dies ist eine wichtige Einstellung, die verhindern soll, dass Unternehmensdaten weitergegeben werden, wenn ein Mitarbeiter sein entsperrtes Gerät unbeaufsichtigt lässt.



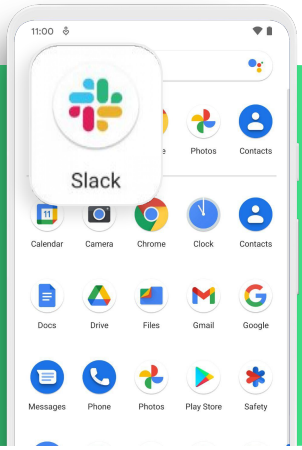


Sie können eine andere Bildschirmzeit einstellen **oder „Weitere Details“ auswählen.** Mitarbeiter können auch eine kürzere Bildschirmzeit wählen, haben aber nicht die Möglichkeit, eine längere Bildschirmzeit als 5 Minuten festzulegen.

android

SCHRITT 5

5 Automatisch installierte Apps



A

Wählen Sie in der Leiste „Alle Apps“ die Slack App aus. Sie werden feststellen, dass es sich dabei um keine System-App, sondern um eine Drittanbieter-App handelt.

Dies zeigt, wie die IT-Abteilung Apps auf einem vollständig verwalteten Gerät automatisch installieren kann.

B

Fazit

Wir hoffen, dass dieser Leitfaden geholfen hat, die vollständige Geräteverwaltung bei Smartphones zu veranschaulichen. Dies stellt eine gute Lösung dar, wenn ein Gerät nur für berufliche Zwecke verwendet wird und sich keine privaten Daten darauf befinden sollen. Durch die vollständige Geräteverwaltung haben Sie volle Kontrolle über alle Geräte- und App-Einstellungen.

Sie können diese Demo weiterhin nutzen, um sich mit ihr vertrauter zu machen. Andernfalls können Sie die Demo löschen, indem Sie das Gerät auf die Werkseinstellungen zurücksetzen. Weitere Informationen finden Sie unter android.com/enterprise/demo.

android