Schutz mobiler Endgeräte mit Lookout Advanced Quick-Start-Guide

vodafone business

Schutz mobiler Endgeräte mit Lookout Advanced

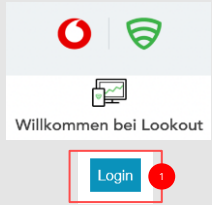
Anleitung Deutsch

Willkommen zu Lookout Advanced

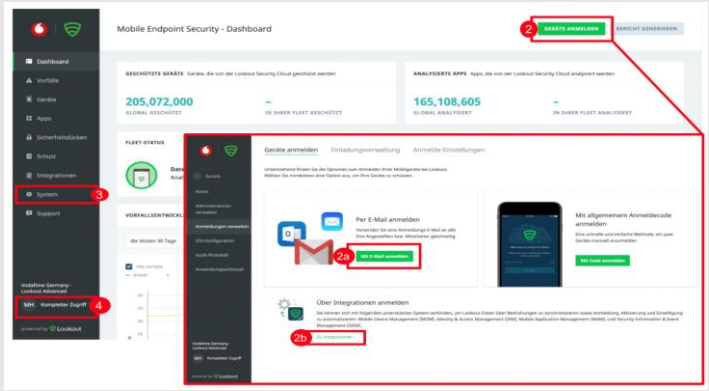
Ihr Start mit Lookout – Schützen Sie Ihre mobilen Geräte in wenigen einfachen Schritten

1 **Öffnen Sie die „Willkommen bei Lookout“ E-Mail auf Ihrem PC oder Laptop (schauen Sie auch im Spam-Ordner).**

a Klicken Sie auf „Login” um ein Passwort zu erstellen:



b Sobald Sie Ihre Login-Daten festgelegt haben, loggen Sie sich damit bei Lookout unter **https://app.lookout.com** ein.



2 Registrieren Sie Ihre Geräte, damit diese von Lookout geschützt werden können:
Klicken Sie auf „**Geräte anmelden“** oben rechts im Dashboard.

a Klicken Sie auf „**Per E-Mail anmelden**“. Geben Sie Adressen in das Textfeld ein und trennen Sie diese mit Kommata. Sie können E-Mail-Adressen hier jederzeit ergänzen.

b Wenn Ihre Lookout-Bereitstellung eine Verbindung zu einem Mobile Device Manager beinhaltet, wählen Sie bitte „**Zu Integrationen”** und wählen Sie den relevanten MDM connector guide unter **https://enterprise.support.lookout.com/hc/en-us/requests.**

3 Sie können zusätzliche Lookout-Administratoren hinzufügen, indem Sie **Einstellungen > Administratoren verwalten** aufrufen.

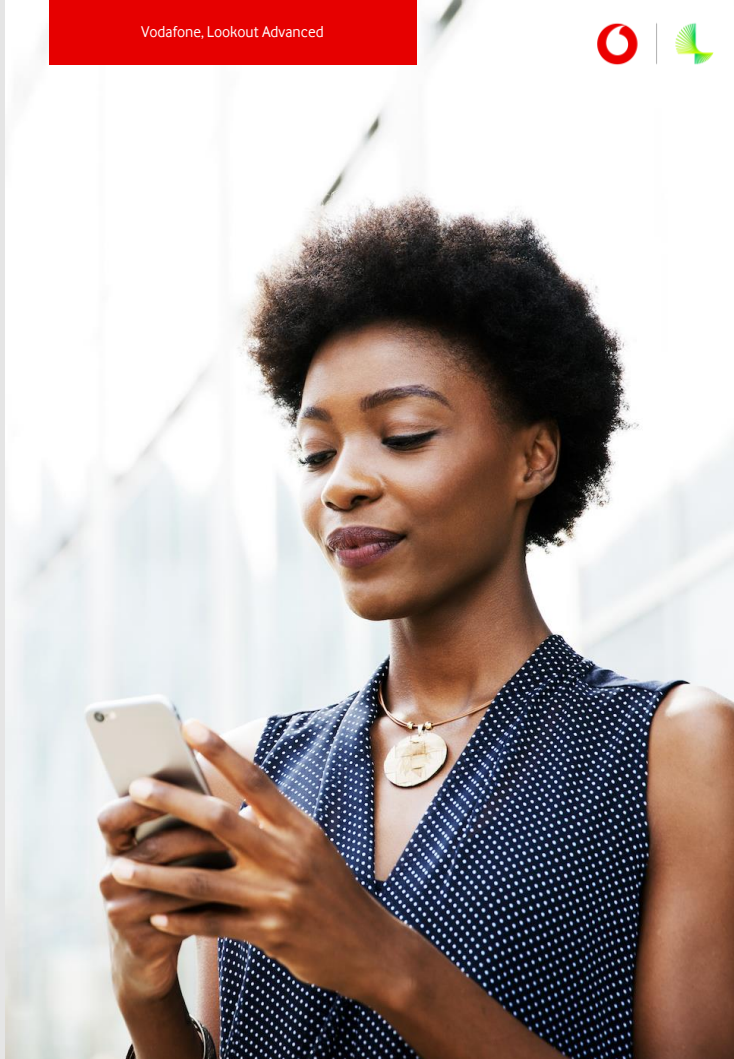
4 Stellen Sie ein, wie häufig Sie E-Mail Benachrichtigungen von Lookout erhalten wollen, indem Sie auf Ihren Nutzernamen in der unteren linken Ecke klicken.

Woher weiß ich, ob meine Mitarbeiter:innen sich registriert haben?

Scrollen Sie in der Managementkonsole nach unten und überprüfen Sie den **Bereitstellungsstatus:**

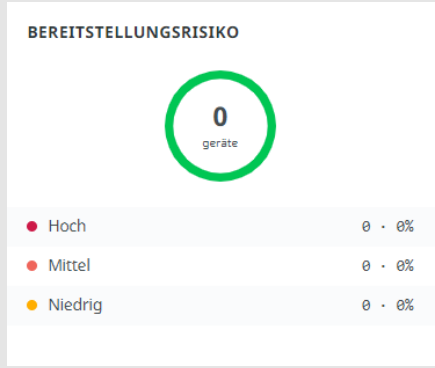
- **Aktive** Geräte haben die Lookout for Work App installiert und erfolgreich aktiviert.
- **Ausstehende** Geräte, die noch nicht vollständig registriert sind haben eine Einladung erhalten, aber die App noch nicht installiert oder diese nach der Installation noch nicht aktiviert.
- **Nicht verbundene** Geräte haben innerhalb der letzten 30 Tage keine Antwort an Lookout gesendet. Das Gerät könnte ausgeschaltet sein, keine Internetverbindung haben oder anderweitig temporär nicht verfügbar sein.
- **Nicht erreichbare** Geräte haben die Lookout for Work App deinstalliert.

Sie können Erinnerungsmails oder neue Einladungen versenden, indem sie **„Anmeldung“** in der linken Navigationsleiste klicken und anschließend die **„Einladungsverwaltung“**-Schaltfläche oben auf der Seite klicken.



Woher weiß ich, ob meine Geräte sicher sind?

Im Dashboard bietet der Abschnitt „**Bereitstellungsrisiko**“ eine Zusammenfassung aller Risiken, die Lookout auf Ihren registrierten Geräten erkennt hat:



a. Gefahren mit **niedrigem Risiko**, wie Adware, verunsichern manche Ihrer Nutzer. Lassen Sie diese die Lookout for Work App auf ihrem Gerät öffnen und die in der App vorgeschlagenen Schritte befolgen, um die Bedrohung zu entfernen.

b. Gefahren mit **mittlerem Risiko**, wie Spyware oder Daten-Lecks, stellen ein ernsteres Risiko dar. Informieren Sie jeden Nutzer, für dessen Gerät ein mittleres Risiko angezeigt wird, um sicherzustellen, dass dieses behoben wird.

c. Gefahren mit **hohem Risiko**, wie Überwachungssoftware, stellen ein direktes, kritisches Problem dar. Jede:r mit einem Hochrisikogerät muss die Bedrohung unverzüglich beheben und sollte vermeiden, das Gerät bis zur Eliminierung der Bedrohung weiter zu nutzen.

Klicken Sie auf **„Schutz“** in der Navigationsleiste links, um Risikolevel und Reaktionsoptionen auf unterschiedliche Risiken zu überprüfen oder anzupassen.

Mobile Endpoint Protection
Lookout Advanced

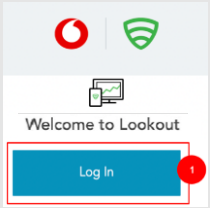
Quick Start Guide - English

Welcome to Lookout Advanced

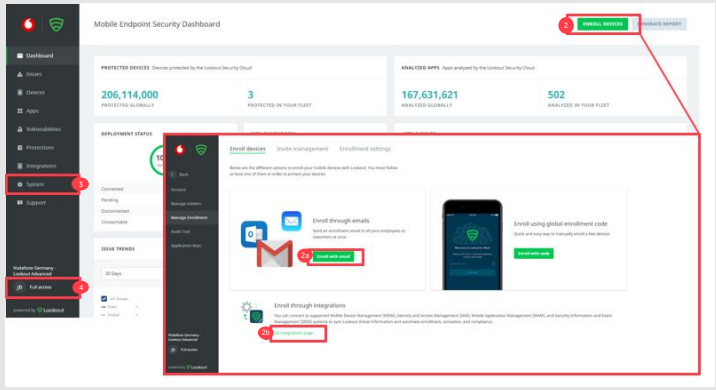
Getting Started with Lookout – Protect your mobile devices in a few simple steps

1 **Check your email (and your spam folder!) for the "Welcome to Lookout" email.**

a Click Log In button in the email to create a password:



b Once your credentials are set, log in to the Lookout web-based console at **https://app.lookout.com**



2 Enroll devices so Lookout can protect them:
Click **Enroll Devices** at the top of the main dashboard page.

a Click **Enroll with email.** Enter addresses in the text field separated with commas.
You can always add more emails later.

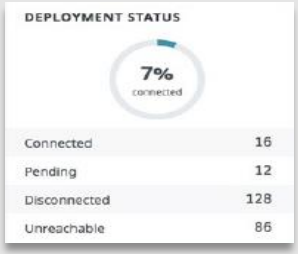
b If your Lookout deployment involves connecting to an Mobile Device Manager, please select **Enroll through integrations** and find the relevant MDM connector guide at **https://enterprise.support.lookout.com/hc/en-us/requests**

3 If required, add more Lookout Console administrators by clicking **System > Manage Admins**.

4 Modify how often you get email notifications from Lookout by clicking your initials in the lower left corner to adjust your preferences.

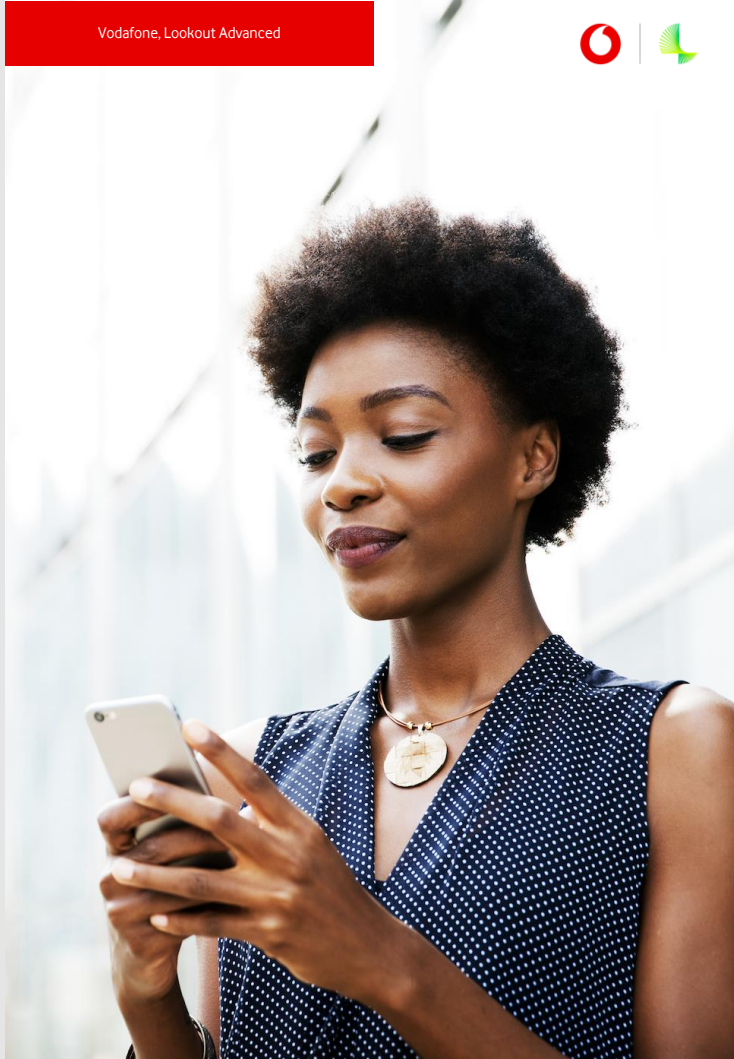
How do I know if my employees have enrolled?

From the Dashboard, scroll down and check the **Deployment Status:**



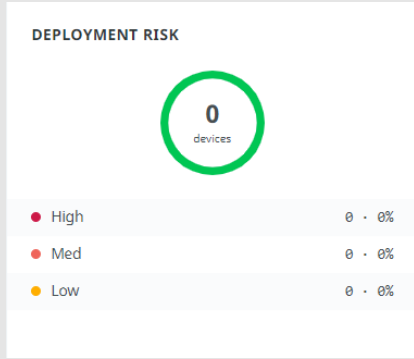
- **Connected** devices have installed Lookout for Work and activated it successfully.
- **Pending** devices have received an invite but either haven't installed the app, or haven't activated it after installing.
- **Disconnected** devices haven't sent a response to Lookout for 30 days.The device may be off, out of Wi-Fi range or there might be some other temporary cause.
- **Unreachable** devices have uninstalled the app.

You can send reminders or new invites by clicking **Enrolment** in the left navigation bar and then clicking the **Invite Management** tab at the top of the screen.



How do I know if my devices are safe?

In the Dashboard the section "**Deployment Risk"** provides a summary of any risks Lookout detects on your enrolled devices:



a. **Low Risk** threats like Adware may somewhat disrupt your users. Encourage them to open Lookout for Work and follow the steps in the app to remove the threat.

b. **Medium Risk** threats like Spyware or Data Leaks present a more serious risk. Follow up with anyone who owns a Medium Risk device to ensure they're aware of it and taking action.

c. **High Risk** threats like Surveillanceware present an immediate, critical issue. Anyone with a High Risk device needs to fix the problem right away and avoid doing business on their device until it is secured.

Click **Protections** in the left navigation bar to review or customise the risk levels and responses for different types of threats.


Together we can
vodafone
business