Lookout for Small Business

Quick-Start-Guide SMB

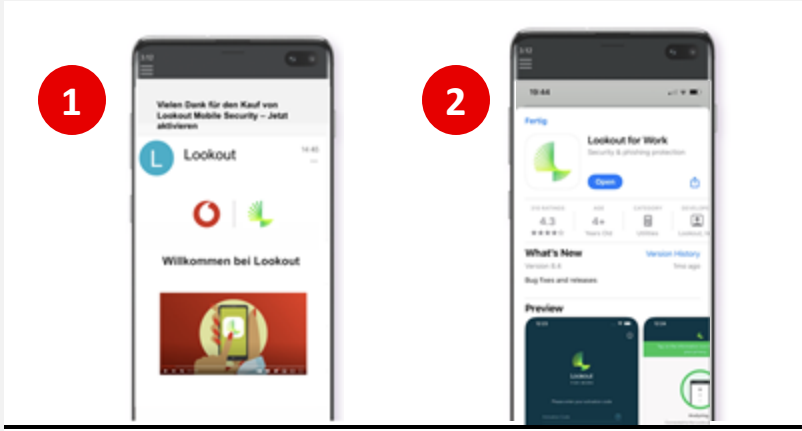
English Guide below

Lookout for Small Business

Erste Schritte mit Lookout – Schützen Sie Ihre mobilen Endgeräte in wenigen einfachen Schritten

Option 1
Aktivieren und implementieren Sie Lookout von mobilen Endgeräten aus

1. Schauen Sie in Ihren E-Mails (und Ihrem Spam-Ordner) nach der E-Mail „**Willkommen bei Lookout**“.
2. Folgen Sie den Anweisungen zur mobilen Aktivierung in der E-Mail. Kopieren Sie zunächst Ihren **Lookout-Registrierungscode** und klicken Sie auf den Link, um die Lookout for Work Mobile-App zu installieren.
3. Sobald die App heruntergeladen ist, geben Sie den Registrierungscode ein, wenn Sie dazu aufgefordert werden. **Befolgen Sie weiterhin die Aktivierungsanweisungen** und akzeptieren Sie die erforderlichen Berechtigungen, bis Ihr Schutz aktiv ist.
4. Sobald die App auf Ihrem Mobilgerät aktiv ist, verwenden Sie die von Ihnen gewählte mobile Messaging-App, um Ihren Mitarbeitenden **Einladungen zur Aktivierung von Lookout zu senden**. Sie können sie auch bitten, den QR-Code zu scannen, wenn sie persönlich bei Ihnen sind.



Melden Sie sich jederzeit von einem PC oder Laptop aus in der Lookout-Dashboard unter app.lookout.com an, um mehr Übersicht und Kontrolle zu erhalten.

Lookout for Small Business

Erste Schritte mit Lookout – Schützen Sie Ihre mobilen Endgeräte in wenigen einfachen Schritten

Option 2
Aktivieren und implementieren Sie Lookout von Ihrem PC oder Laptop aus

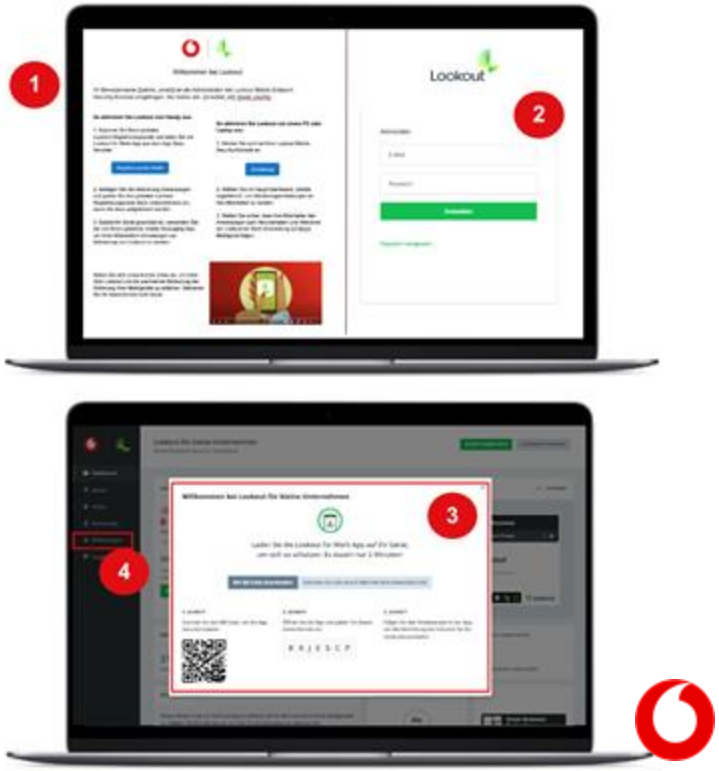
1. Schauen Sie in Ihren E-Mails (und Ihrem Spam-Ordner) nach der E-Mail „**Willkommen bei Lookout**“.

2. Folgen Sie den Anweisungen zur PC- und Laptop-Aktivierung in der E-Mail. Klicken Sie zunächst auf den Button **„Anmelden“**, um auf das web-based Lookout-Dashboard zuzugreifen.

3. Sobald Sie angemeldet sind, **scannen Sie den QR-Code**, der angezeigt wird, mit Ihrem mobilen Endgerät. Folgen Sie den Schritten, um die Lookout for Work-Mobile-App zu aktivieren.

4. Registrieren Sie weitere Geräte, damit Lookout Ihre Benutzer:innen schützen kann. Klicken Sie im linken **Menübereich auf „Anmeldung“**. Wählen Sie **„Mit E-Mail anmelden“** und geben Sie die E-Mail-Adressen der Benutzer:innen in das Textfeld ein.

Sie können weitere Lookout Administratoren hinzufügen, indem Sie auf **Einstellungen > Administratoren verwalten** klicken. Ändern Sie, wie oft Sie E-Mail-Benachrichtigungen von Lookout erhalten, indem Sie unten links auf Ihren Benutzernamen klicken.



Wie erfahre ich, ob sich meine Mitarbeitarbeitenden angemeldet haben?

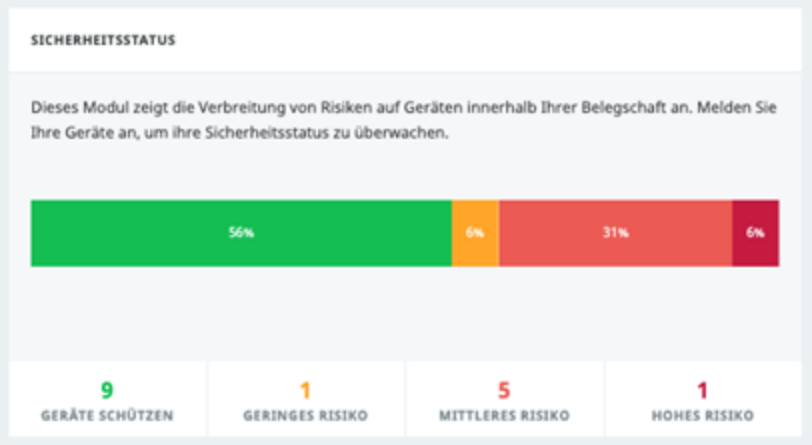
Wenn Sie mit einem PC oder Laptop auf das Lookout-Dashboard zugreifen, scrollen Sie nach unten und überprüfen Sie den **Bereitstellungsstatus:**

- **Angeschlossene** Geräte haben Lookout for Work installiert und erfolgreich aktiviert.
- **Getrennte** Geräte haben 30 Tage lang keine Antwort an Lookout gesendet. Das Gerät ist möglicherweise ausgeschaltet, befindet sich außerhalb der WLAN-Reichweite oder es liegen andere vorübergehende Ursachen vor.
- **Nicht erreichbare** Geräte haben die App deinstalliert.

Sie können Erinnerungen oder neue Einladungen senden, indem Sie in der linken Navigationsleiste auf **„Anmeldung“** und dann oben auf dem Bildschirm auf die Registerkarte **„Einladungsverwaltung“** klicken.

Woher weiß ich, ob meine Geräte sicher sind?

Der Abschnitt **„Sicherheitsstatus“** des Lookout-Dashboards bietet eine Zusammenfassung aller Risiken, die Lookout auf Ihren registrierten Geräten erkennt:



a **Bedrohungen mit geringem Risiko** wie Adware können Ihre Benutzer:innen etwas stören. Ermutigen Sie sie, Lookout for Work zu öffnen und die Schritte in der App zu befolgen, um die Bedrohung zu entfernen.

b **Bedrohungen mit mittlerem Risiko** wie ein veraltetes Betriebssystem oder Apps, die vertrauliche Daten preisgeben, stellen ein ernsteres Risiko dar. Kontaktieren Sie alle, die ein Gerät mit mittlerem Risiko besitzten, um sicherzustellen, dass er*sie sich dessen bewusst ist und aktiv Maßnahmen ergreift.

c **Hochriskante Bedrohungen** wie Surveillanceware oder Phishing können ein unmittelbares oder kritisches Problem darstellen. Jeder*jede, der*die ein Gerät mit hohem Risiko besitzt, bei dem die Bedrohung nicht automatisch behoben wird, muss das Problem sofort beheben und darf keine Geschäfte auf seinem Gerät tätigen, bis es gesichert ist.

Klicken Sie in der linken Navigationsleiste auf **„Schutz“**, um die Risikostufen und Reaktionen für verschiedene Arten von Bedrohungen zu überprüfen oder anzupassen.

Mit der **On Device Threat Protection**-Funktion von Lookout können Sie bestimmte Domains hinzufügen, auf die riskante Geräte keinen Zugriff haben. Fügen Sie www.office365.com zur Sperrliste zu, um beispielsweise sicherzustellen, dass Benutzer:innen mit riskanten Mobilgeräten nicht auf Unternehmensdokumente von Microsoft zugreifen können, bis ihr Gerät wieder in einen sicheren Zustand zurückkehrt, wodurch das Risiko einer Datenkompromittierung weiter verringert wird.


Together we can
vodafone
business

Lookout for Small Business

Quick-Start-Guide

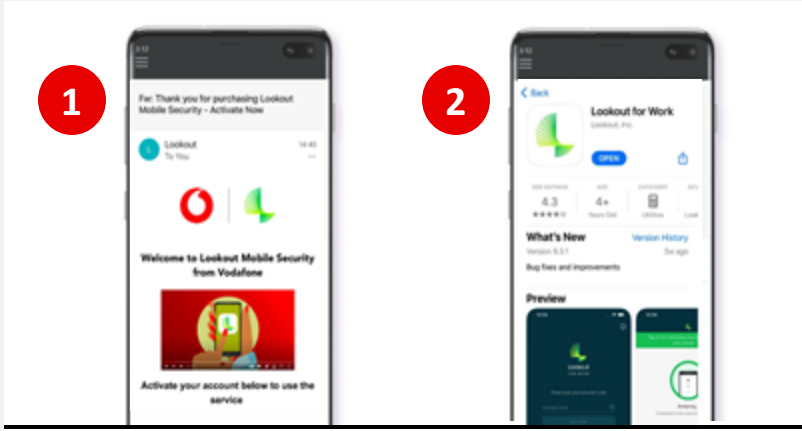
vodafone business

Lookout for Small Business

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

Option 1
Activate & deploy Lookout from mobile

1. Check your email (and your spam folder) for the **"Welcome to Lookout"** email.
2. Follow the mobile activation instructions in the email. First copy your **Lookout enrollment code** and click the link to install the Lookout for Work mobile app.
3. Once the app is downloaded, paste the enrollment code when prompted. Continue to **follow the activation prompts**, accept the required permissions until your protection is active.
4. Once the app is active on your mobile device, use your chosen mobile messaging app to **send your employees invitations** to activate Lookout. You can also ask them to scan the QR code if they are with you in person.



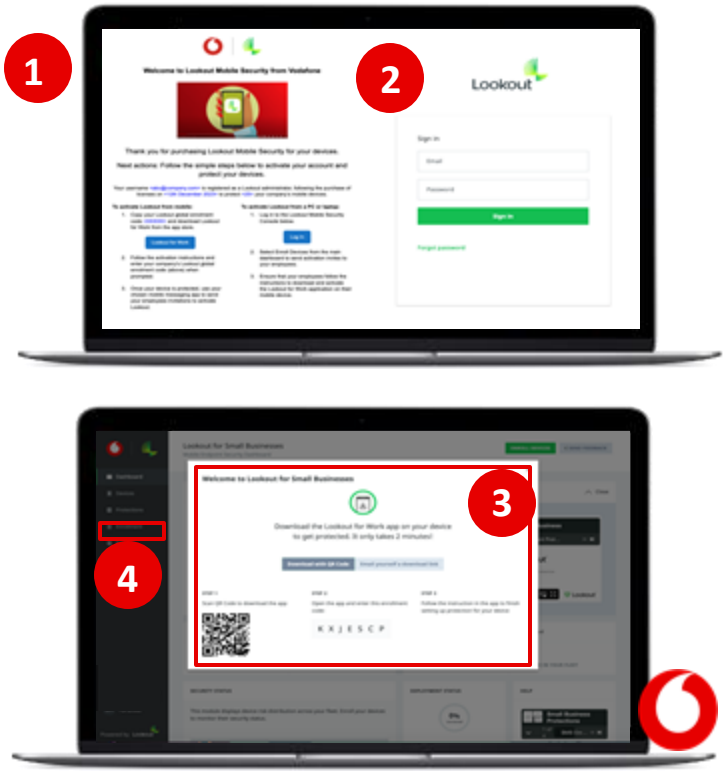
Log in to the main Lookout dashboard at app.lookout.com from a PC or laptop at any time for more visibility and control.

Lookout for Small Business

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

Option 2
Activate & deploy Lookout from PC or laptop

1. Check your email (and your spam folder) for the **"Welcome to Lookout"** email.
2. Follow the PC and laptop activation instructions in the email. First click the "**Login"** button to access the web based Lookout dashboard.
3. Once logged in **scan the QR code** which pops up using your mobile device. Follow the steps to activate the Lookout for Work mobile app.
4. Enrol more devices so Lookout can protect your users.
   Click "Enrollment" from the left menu pane. Select **"Enroll with email"** and enter user email addresses in the text field.

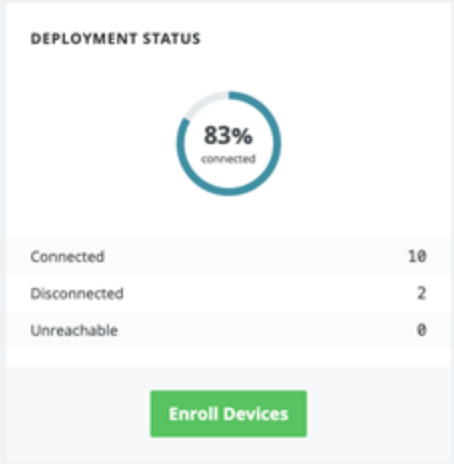


You can add more Lookout administrators by clicking **Settings > Manage Admins.** Modify how often you get email notifications from Lookout by clicking your username in the lower left corner.

How do I know if my employees have enrolled?

Using a PC or laptop to access the Lookout dashboard, scroll down and check the **Deployment Status:**

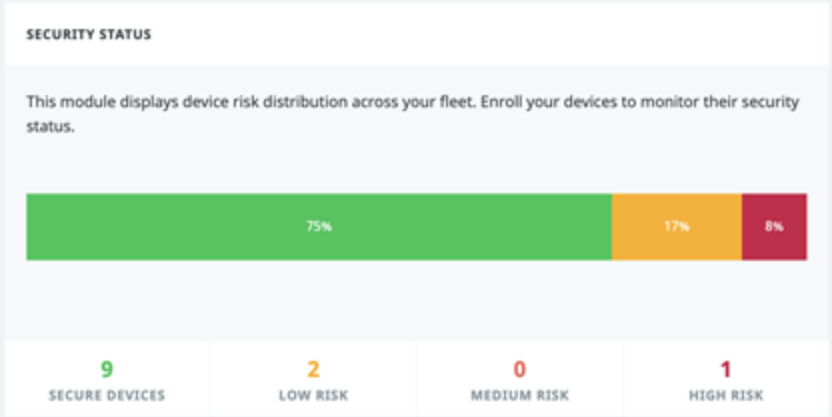
- **Connected** devices have installed Lookout for Work and activated it successfully.
- **Disconnected** devices haven't sent a response to Lookout for 30 days. The device may be off, out of Wi-Fi range or there might be some other temporary cause.
- **Unreachable** devices have uninstalled the app.



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?

The Dashboard **"Security Status"** section 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 an out-of-date operating system or apps which leak sensitive data present a more serious risk. Follow up with anyone who owns a Medium Risk device to ensure they're aware of it and are taking action.

c **High Risk** threats like surveillanceware or phishing could present an immediate or critical issue. Anyone with a High-Risk device where the threat isn't automatically remediated 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.

Lookout's **On Device Threat Protection** feature allows you to add specific domains which risky devices are denied access to. Adding www.office365.com to the deny list for example would ensure users with risky mobile devices are blocked from accessing any corporate Microsoft documents until their device returns to a secure state, further mitigating the risk of data being compromised.


Together we can
vodafone
business