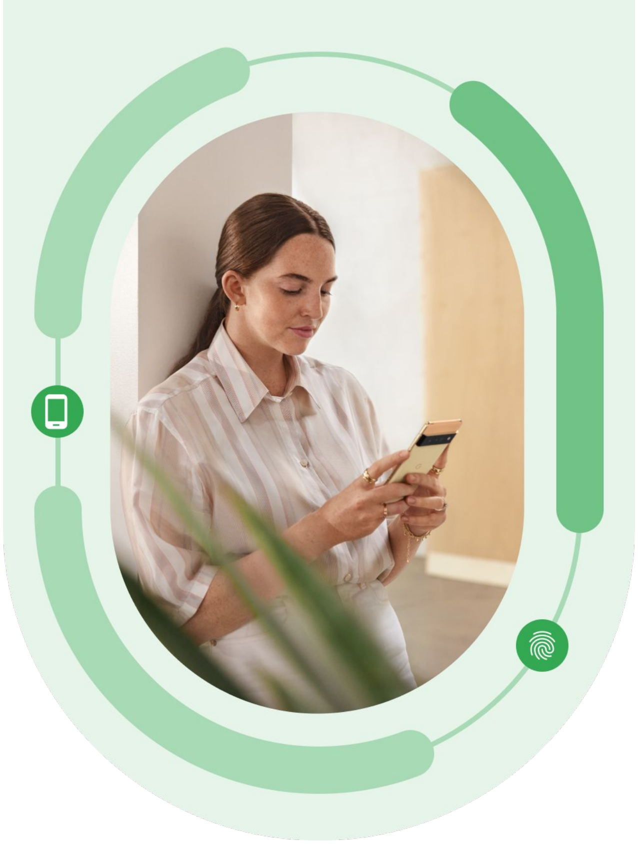
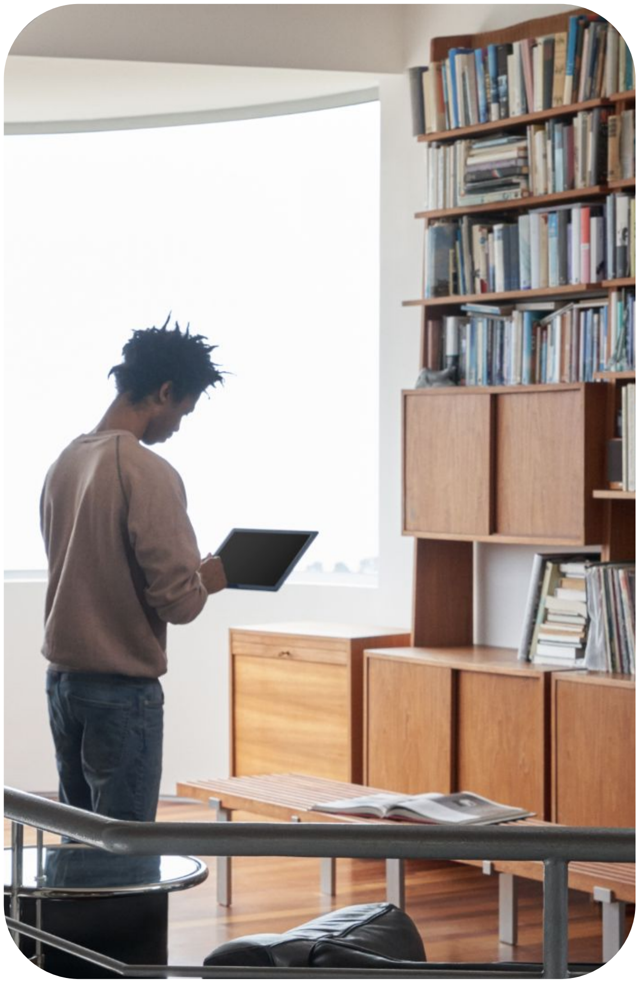
Verify mobile access with Device Trust from Android Enterprise





In today's mobile-first world, 71% of employees[1] use smartphones for work, making traditional perimeter-based security — which relies on a well-defined boundary like a firewall to protect the corporate network — less effective.

That's why 63% of organizations[2] have adopted a Zero Trust approach to security. By verifying the device, user, and other attributes before allowing access to work data, organizations can better protect critical resources.

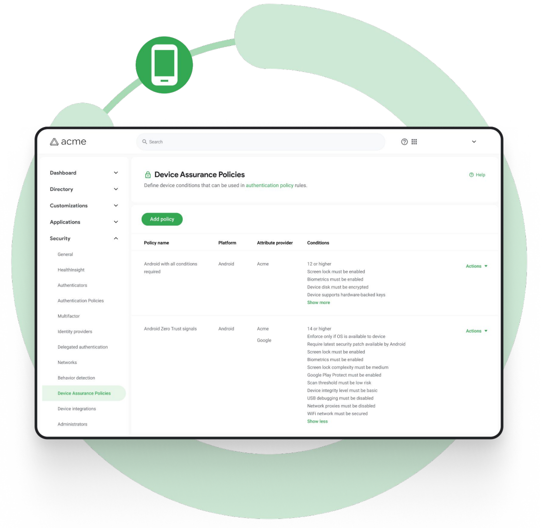
Introducing Device Trust from Android Enterprise

Device Trust from Android Enterprise* is a new security solution that extends device trust signals to all Android work devices, including EMM-managed and unmanaged devices.

[1] Zimperium: 2024 : "Global Mobile Threat Report," 2024.
[2] Gartner: "Gartner Survey Reveals 63% of Organizations Worldwide Have Implemented a Zero-Trust Strategy," April 22, 2024.

* Device Trust from Android Enterprise solutions are built and offered by third-party providers integrating into the Android Management API. Exact features may vary depending on third-party integrations. Access on unmanaged devices requires user consent to use the Android Device Policy app.

Device Trust from Android Enterprise



acme

Search

Dashboard

Directory

Customizations

Applications

Security

General

HealthInsight

Authenticators

Authentication Policies

Multifactor

Identity providers

Delegated authentication

Networks

Behavior detection

Device Assurance Policies

Device integrations

Administrators

Device Assurance Policies

Define device conditions that can be used in authentication policy rules.

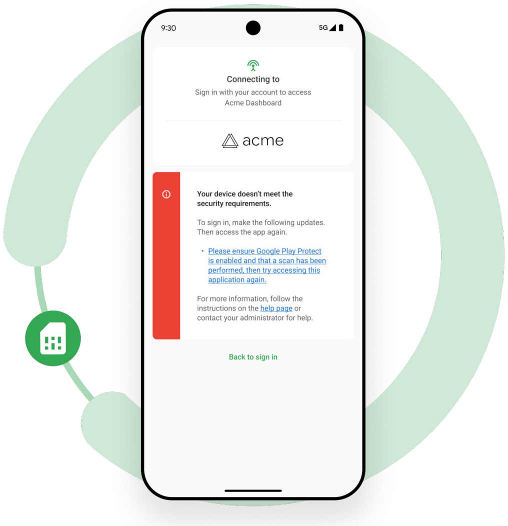
Help

Add policy

Policy name	Platform	Attribute provider	Conditions	
Android with all conditions required	Android	Acme	12 or higher Screen lock must be enabled Biometrics must be enabled Device disk must be encrypted Device supports hardware-backed keys Show more	Actions
Android Zero Trust signals	Android	Acme Google	14 or higher Enforce only if OS is available to device Require latest security patch available by Android Screen lock must be enabled Biometrics must be enabled Screen lock complexity must be medium Google Play Protect must be enabled Scan threshold must be low risk Device integrity level must be basic USB debugging must be disabled Network proxies must be disabled WiFi network must be secured Show less	Actions

Security for the modern workplace

- **Control access using 20+ device trust signals:** Authenticate the trust status of Android work devices with signals like device security patch level, OS version & pending OTA, network status, screen lock, and more.
- **Secure managed and unmanaged devices:** Enforce device trust policies on both Android Enterprise-managed devices and unmanaged devices through a Device Trust from Android Enterprise partner.
- **Meet cybersecurity standards:** Align with industry best practices around Zero Trust and mobile security, including ISO/IEC 27001, 27002, 27005.



9:30

5G

Connecting to

Sign in with your account to access Acme Dashboard

acme

Your device doesn't meet the security requirements.

To sign in, make the following updates. Then access the app again.

- Please ensure Google Play Protect is enabled and that a scan has been performed, then try accessing this application again.

For more information, follow the instructions on the help page or contact your administrator for help.

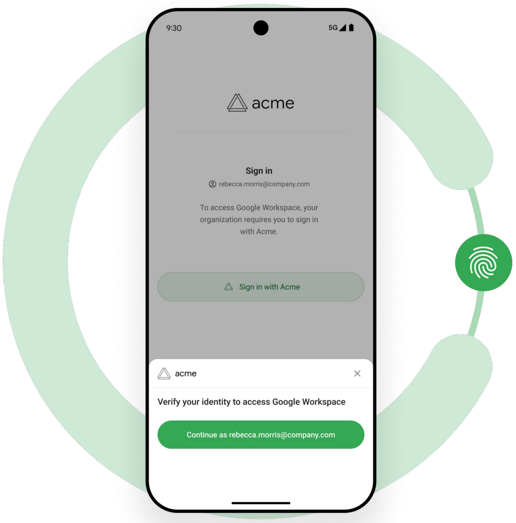
Back to sign in

Flexible solutions for diverse use case

- **Integrate mobile fully into your security systems:** Incorporate Android devices into the same security approach used for laptops, via (EDR) vendors, identity providers (IdPs) and security information and event management (SIEMs).
- **Respond quickly to threats with reliable trust signals:** Leverage direct access to device trust signals, helping you make more intelligent access decisions and respond to threats as they arise.
- **Layer trust solutions with Android's diverse partner ecosystem:** Tap into a diverse set of security partners whose solutions can work in concert to provide layered security across more access surfaces.

The employee experience, uninterrupted

- **Continuously evaluate signals without disrupting users:** Evaluate the ongoing security posture of the device to provide real-time security across more points of access.
- **Empower employees to work without enrolling the device:** Get working right away without needing to formally enroll the device — particularly useful for casual work scenarios that don't require full EMM management.
- **Protect work data while respecting employee privacy:** Deploy a device trust solution with signals built with end-user privacy in mind and partners that are vetted and trusted through secured interfaces.



9:30

5G

acme

Sign in

rebecca.morris@company.com

To access Google Workspace, your organization requires you to sign in with Acme.

Sign in with Acme

acme

Verify your identity to access Google Workspace

Continue as rebecca.morris@company.com

Device Trust from Android Enterprise security partner integrations:

- Identity management
- Mobile threat defense
- SIEM
- Endpoint detection and response
- Endpoint management (UEM/EMM)
- Security operations tools

Learn more about Android Enterprise security at www.android.com/enterprise/security/

For more information on pricing & integration, reach out to your [Partner Name] representative.

Android ZIMPERIUM