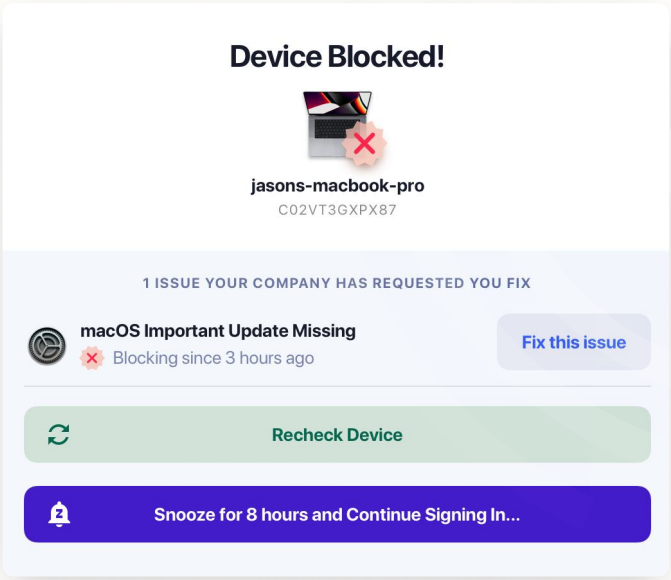
Device Trust for Google Workspace

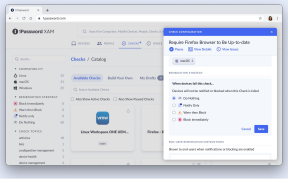


Are insecure and non-compliant devices accessing your sensitive data?

1Password Device Trust ensures all devices are known and secure before they can access company apps and resources.

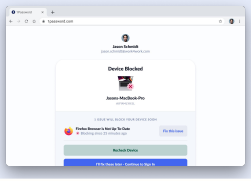
- Enforce a wider range of health checks than mobile device management (MDM).
- Reduce support tickets by enabling your team to secure their own devices.
- Secure all devices including managed, employee-owned (BYOD), and Linux.
- Block unknown devices from signing in to protected applications.

Key features



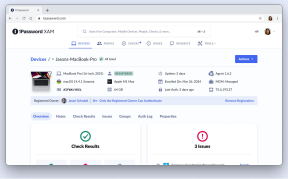
Device health checks

Select from a library of over 100 pre-built device health checks, or build your own. Notify users if a problem is detected, or block access immediately.



Self-serve remediation

When Device Trust detects a problem and blocks a device, team members are provided with step-by-step instructions so they can get back to work without IT assistance.



Device reporting

Get visibility into every device accessing company resources and search for device properties, such as browser extensions that may pose a security risk.

Integrating with Google Workspace

Device Trust integrates with Google Workspace by acting as an SSO provider for specific apps that you configure within the Device Trust dashboard. When a team member attempts to log in to a protected application, they will first be prompted to sign into their Google account. After that, they're redirected to Device Trust so device health checks can run. Once team members remediate any issues, authentication completes and they are signed in.

For more Information about Device Trust: View interactive demo | Contact sales