1Password | DRATA

1Password Device Trust & Drata

Integration Solutions Brief

1Password and Drata are redefining how modern businesses secure access and support audit readiness, helping customers tackle security and compliance at scale. By integrating 1Password Device Trust with Drata’s automated compliance monitoring, organizations gain continuous visibility, validate and monitor device compliance status for audit readiness. Our partnership simplifies and automates compliance evidence collection, helping IT and Security teams scale securely while meeting compliance framework requirements.

Drata's integration for 1Password Device Trust provides device trust evidence for access controls, reduces access-related risk, and helps meet compliance framework requirements.

1Password Device Trust and Drata Integration Overview

What 1Password and Drata help address

- **Reduced security risk** – helps reduce access-related risk from compromised credentials.
- **Continuous insights into device compliance** - through the integration, companies can verify that every device meets the security and compliance requirements for each standard.
- **Automated evidence collection for device trust and access controls** - this integration reduces manual evidence collection for access-related controls without having to manually collect records for compliance frameworks to be audit ready.

The Drata & 1Password Device Trust integration continuously monitors across various Device Trust Checks that are critical for compliance to validate if an end user's device has a/an:

- Password manager installed
- Antivirus software installed
  - "Require (antivirus vendor) is installed and running"
- Operating system security patches auto-applied
  - "Require (platform) meets minimum required version"
  - "Require automatic updates to be enabled"
- Hard drive encryption enabled
  - "Require disk to be encrypted"
- Screensaver lock configured to activate
  - "Require screen lock configuration"

User Benefits

- **Device Trust enforcement:** Ensures device compliance evidence is continuously monitored and available for audits.
- **Continuous control monitoring:** Provides ongoing oversight and visibility of compliance status, allowing IT and Security teams to maintain visibility into access-related control evidence and prioritize critical compliance issues as they arise.
- **Automated evidence collection:** Reduces any manual effort (screenshots or log exports) from IT and Security teams to gather proof of device compliance, streamlining the audit process and freeing up their time.

How It Works

Drata's integration with 1Password Device Trust retrieves Device Trust check results via the Checks API to support evidence for access-related controls

What's the setup process?

Visit Device Trust (formerly known as Kolide) help article

1. Make sure you have Administrator or Super Administrator access to your company's Device Trust account. Specifically, you'll need the ability to create a new Custom API Token.
2. Create and copy your Device Trust API Token
3. Select Connections on the side navigation menu.
4. Select the Available connections tab, search for Device Trust, and select Connect.
5. Select Create connection.
6. Enter the API Token you previously created.
7. Choose any relevant checks to map for Drata's compliance monitoring tests.

Data being exchanged:

Drata only requires read access, which is the default setting for all Device Trust API tokens. You do not need to add any write privileges.

Learn more about the integration and how to set it up today.