JOINT SOLUTION BRIEF

zscaler™ + 1Password

Secure Access, Reduce Attack Surface, and Practice Principles of Zero Trust.

1Password

INTEGRATION HIGHLIGHTS

- Continuously evaluates devices against pre-defined checks
- Validate devices have Zscaler installed and configured
- Protect unhealthy devices from accessing company data

The Challenge: Securing Access in a BYOD, Perimeter-less World

In today's remote-first, SaaS-heavy environments, it's challenging for organizations to ensure that only secure, compliant devices access company systems. As Bring Your Own Device (BYOD) becomes the norm, and users access company resources from unmanaged or managed devices, legacy security tools like mobile device management (MDM) have little ability to secure these unmanaged personal devices. Security teams face a growing trust gap, while identity verification through single sign-on (SSO) and multi-factor authentication (MFA) is common, device-level trust is often missing.

That's where 1Password Device Trust (formerly Kolide) comes in. Part of the 1Password Extended Access Management (XAM) solution, Device Trust specifically closes this gap by adding a crucial device-based factor to your authentication flow. It ensures that users are not just who they say they are; but are using trusted, compliant devices before authenticating into company resources.

The Solution

The 1Password Device Trust and Zscaler integration enables organizations to secure devices and protect sensitive company resources. This integration enables organizations to enforce access policies based on the presence and status of Zscaler on a user's device.

Using the 1Password Device Trust Checks agent, organizations can set policies that determine whether:

- The Zscaler App is installed.
- The Zscaler Client Connector Service is configured correctly.
- The Zscaler ZSTunnel Service is active and secure.

If a device fails these checks, the user can be blocked from access or warned to take action and is presented with dynamic self-remediation instructions from IT teams to fix the problem. Once the issue is resolved, users regain access to the protected company resources automatically.

Together, Zscaler and 1Password allow all joint customers to ensure that critical company applications and data are accessed only from trusted, healthy devices where Zscaler is properly installed and configured.

What Is 1Password Device Trust?

1Password Device Trust ensures that any device accessing company protected resources are known,trusted, and compliant with preset requirements.

- **Known**: Is this a device the organization is aware of and has visibility into?
- **Trusted**: Does the device meet the security and compliance standards defined by your IT or Security team?

Backed by 1Password's Device Trust agent (which utilizes the open-source project OSquery), the system continuously evaluates whether the device passes a set of checks ranging from simple criteria such as whether disk encryption is enabled to more complex requirements like verifying the configuration of specific security apps, including Zscaler.

Even if a malicious actor phishes your most important credentials, Device Trust ensures they can't gain access unless they're using a known, trusted, and compliant device.

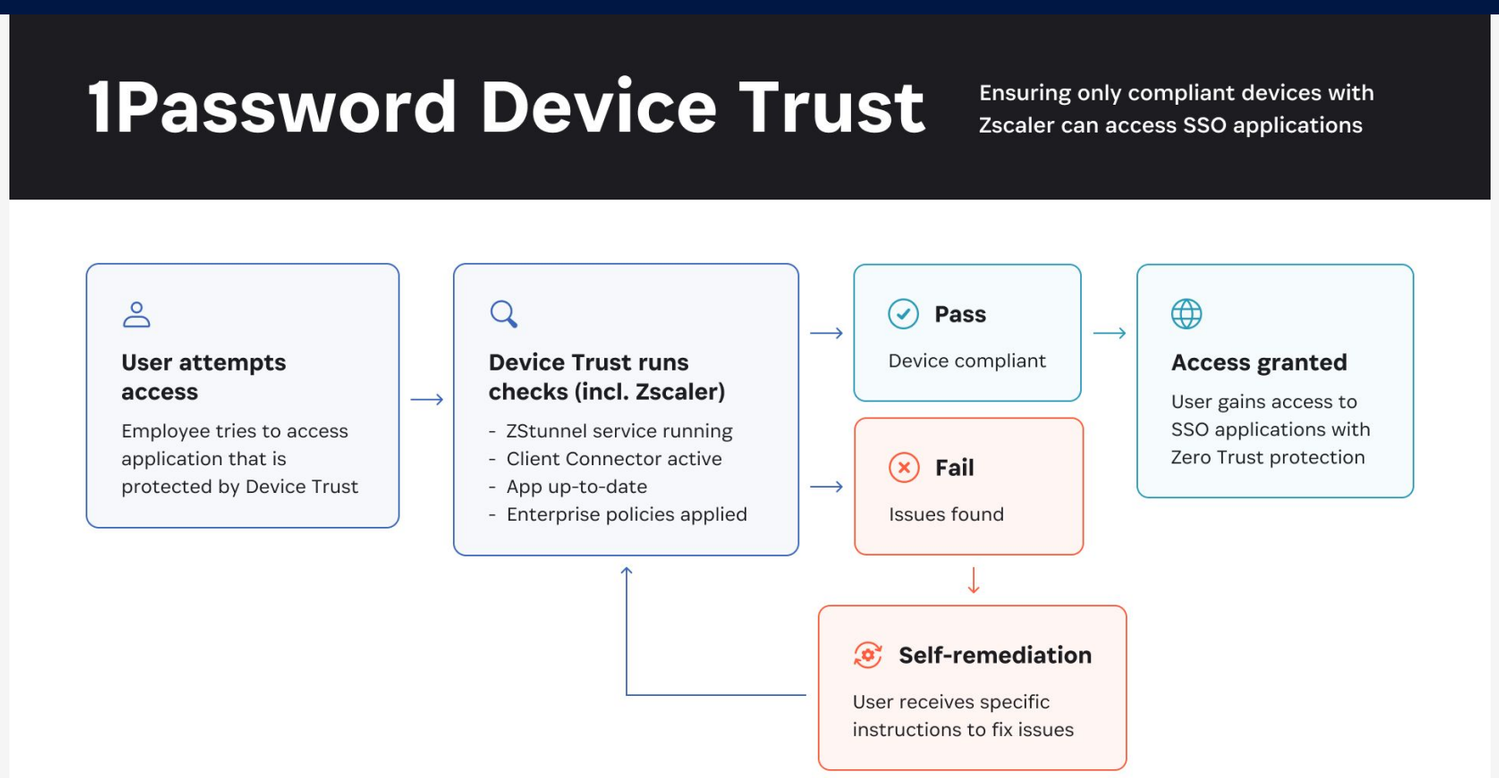
HOW IT WORKS

The 1Password Device Trust service runs an osquery SQL query against the Device Trust local agent on the device to look for the presence of the installed Zscaler application bundle and associated running processes. The local agent also executes the Zscaler CLI tool (currently available only on macOS and Windows) with the following invocation "zscli status -s all", and parses the JSON output of the CLI to determine the state of the Zscaler application, and its components.

Depending on the Check's configuration options (listed above) chosen by the administrator in the Device Trust admin interface, the Check will determine whether the device satisfies the required criteria and is in a passing or failing state.

It runs these evaluations hourly (or more frequently based on admin policy) against the user's device.

If the Check has a remediation strategy configured which is "Warn Then Block" or "Block Immediately", the user will observe an interruptive message during their next attempt to authenticate into a Device Trust protected application.



Zscaler + 1Password Benefits

ACTION	DESCRIPTION
Empower end users	Users can resolve device compliance issues on their own through guided self-remediation provided by IT teams and regain access automatically.
Secure BYOD environments	Gain control over managed and unmanaged devices, great for companies without MDM or hybrid device fleets.
Phishing-resistant access	Credentials alone are not enough; device state matters and 1Password Device Trust enables your team to ensure user devices are compliant and secure with your requirements before access is given.
Reduce help desk load	Self-guided user remediation eliminates IT team's involvement for device access issues and allows your users to get access to company resources without any IT involvement.

Conclusion

Implement Zero Trust principles with Zscaler and 1Password

The 1Password Device Trust and Zscaler integration allows organizations to secure devices and protect sensitive company resources, enabling organizations to enforce access policies based on the presence and status of Zscaler on a user's device. If a device does not meet these policies then the user can be warned or blocked from accessing company resources. In order to proceed, the user must follow the self-remediation instructions to ensure Zscaler is setup as required to regain access automatically.

Learn more at **www.zscaler.com/partners/technology**

zscaler™ | **Experience your world, secured.™**

About Zscaler: Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest in line cloud security platform. Learn more at zscaler.com or follow us on X (Twitter) @zscaler.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

©2025 Zscaler, Inc. All rights reserved.