DATA SHEET

Smallstep + VPN

Scalable Zero Trust Enforcement

Smallstep brings our award-winning Device Identity platform to secure access to your IPSec VPN. Our platform offers the strongest possible assurance that only the devices in your inventory can connect to your private network or zero trust edge, making credential theft unfeasible.

How does it work?

Smallstep uses ACME Device Attestation,
a standard we developed with Google to replace legacy shared secrets with device-bound, remotely-attested credentials. ACME DA automates certificate issuance and renewal on trusted, approved devices.

It offers cryptographic proof that a specific device received a credential, and that the credential cannot be exported from that device.

And it's seamless

your devices are VPN-ready in minutes, not days.

Key Features

Hardware-attested device identity

We enforce ACME Device Attestation, only issuing VPN client certificates when there is proof of TPM or Secure Enclave-backed private keys.

Device-bound, short-lived certificates

Smallstep uses device-bound private keys that are tied to hardware, auto-rotated, and not exportable.

Trustworthy device inventory

Maintain a verified catalog of managed devices, with status and provenance. The platform integrates with Jamf, Intune, Google Workspace, Okta, and more to sync your devices and users.

One platform, many uses

Use strong device identity to secure VPN, Enterprise Wi-Fi, internal web apps, and sensitive SaaS apps.

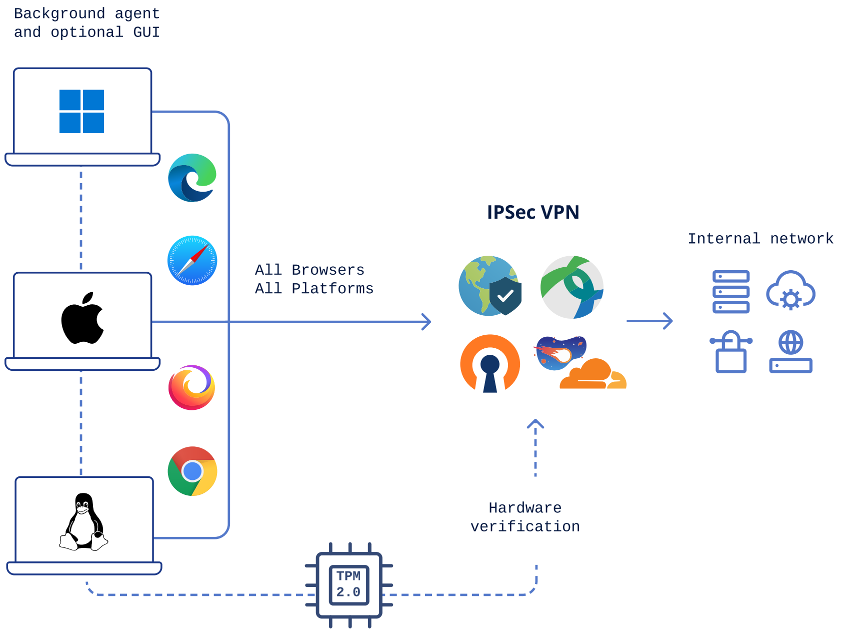
Cross-OS

Smallstep's agent and platform support device attestation on Apple, Windows, Linux, and ChromeOS. It offers VPN auto-configuration on Apple, ChromeOS, and Windows devices.

Stronger security, seamless experience.

Smallstep is an invisible second factor, where the silicon is the key. Users log in from authorized devices without any additional steps—no YubiKeys to plug in, no codes to enter.

> "We were going to replace Palo Alto Global Protect to attain Zero Trust. However, with Smallstep Device Identity we can now leverage hardware-bound certs before granting access to the VPN tunnel, which **achieves NIST AAL3 compliance without having to replace our existing infrastructure**."
>
> – VP Networks



How it works

1. Register devices or sync your device inventory from Jamf, Intune, or another MDM into Smallstep. Connect Okta, Google Workspace, or other IdPs to sync users, as desired.
2. Devices use their secure element (TPM or Secure Enclave) to perform ACME Device Attestation, requesting a device certificate.
3. The device certificate is the device's key to Smallstep; it is used to issue client certificates for VPN, Wi-Fi, web apps, or other apps.
4. Your VPN gateway validates the client certificate via mTLS during IKEv2/IPSec setup. Smallstep's agent keeps the certificate fresh.

Smallstep's device certificates work with any standards-compliant IPSec VPN that supports IKEv2 with mutual TLS certificate authentication, including:

- F5 BIG-IP APM
- Cisco AnyConnect with IKEv2
- Juniper Mist
- Palo Alto Networks GlobalProtect
- StrongSwan

Because the credentials are standard TLS certificates, you can also front legacy or third-party VPNs via your existing ZTNA edge, as long as it can validate client certificates.

Smallstep device identity also integrates with:

- Smallstep RADIUS Server for Enterprise Wi-Fi and wired networks
- Smallstep Device IdP for browser-based device checks inside your SSO flow
- Smallstep Enterprise Relay for protected access to SaaS apps and internal services

Smallstep is the world's first Device Identity Platform™, enabling Zero Trust, certificate-based access to infrastructure, applications, and networks. Built in partnership with Apple and Google, Smallstep uses cryptographic attestation and short-lived, hardware-backed credentials to replace passwords, SSH keys, and VPN clients. By integrating with tools like Jamf, Intune, and Okta, Smallstep ensures that only trusted users on compliant devices can access sensitive systems—delivering true Zero Trust security without user friction.