DATA SHEET

Smallstep + ChromeOS

Hardware-Backed Device Identity for the Chrome ecosystem

ChromeOS is the Google-built operating system at the heart of the Chrome ecosystem.

Smallstep integrates with ChromeOS to add unphishable credentials for accessing Enterprise Wi-Fi, VPN, internal websites, and sensitive SaaS apps.

We issue device-attested certificates for strong, hardware-backed security. Smallstep can ensure that only trusted, managed Chrome devices can enroll, with ACME Device Attestation providing hardware-backed proof of identity.

Smallstep's cross-platform device identity ensures only real, trusted hardware can authenticate—eliminating phishing, credential theft, and impersonation attacks that routinely target IT help desks and call centers.

Key Features

Trustworthy Device Inventory:
Keep a verified list of company-owned devices across all platforms.

Hardware-bound Credentials
Issue credentials tied to the device's hardware, enhancing security and compliance.

Sensitive Resource Protection
Ensure that only authorized devices can access critical enterprise resources.

Smallstep for ChromeOS can protect a wide range of resources, including:

- Wi-Fi networks (WPA3 Enterprise EAP-TLS) and wired networks
- IPSec VPN access
- Internal web apps and cloud services (Google Workspace, Microsoft Office365, etc.)
- Any web service that supports mutual TLS authentication (Entra ID, Dropbox, etc.) hardware-bound solution, reducing costs.

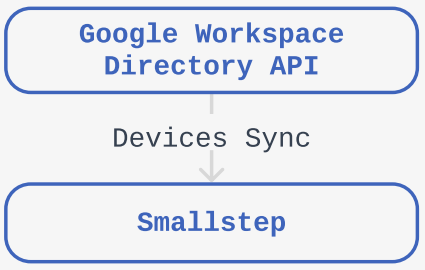
chromeOS

With Smallstep a device's hardware identity becomes an authentication factor. Instead of relying solely on shared secrets and user credentials, Smallstep silently verifies device trust at enrollment—blocking unauthorized machines without adding friction for users.

How it works

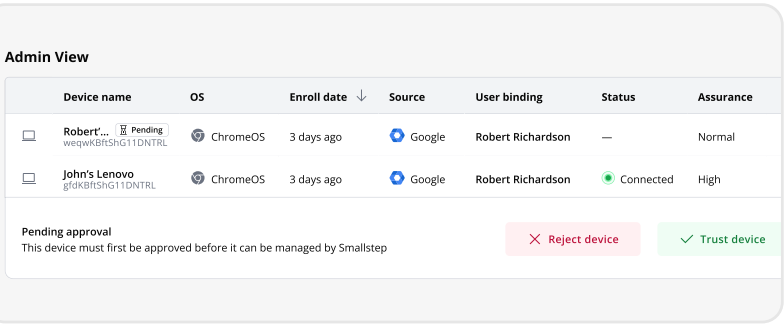
The Smallstep ChromeOS extension authenticates devices to Smallstep Device IdP (an OpenID Connect IdP), Smallstep RADIUS Server, or any browser-based app that uses mutual TLS authentication.

1



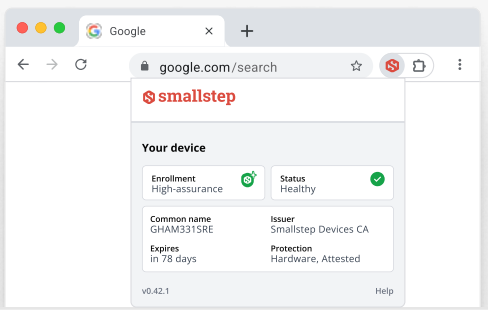
Connect Smallstep with Google Workspace to sync your devices.

2



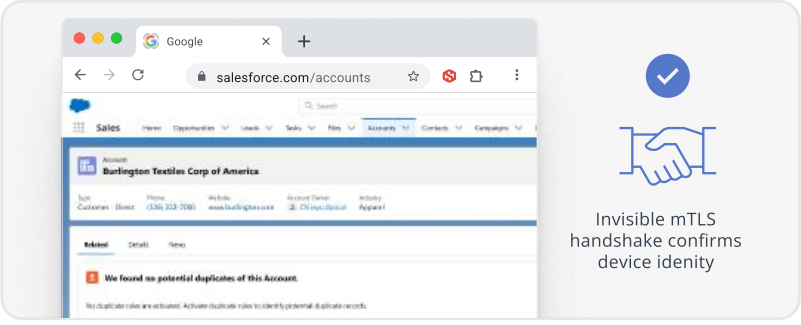
In Smallstep, admin can approve devices adding them to managed inventory.

3



Install Smallstep ChromeOS extension via Google Workspace. The browser extension uses ACME Device Attestation to get a device-bound certificate from Smallstep. It manages the device's endpoint certificates and keeps them up to date.

4



When the user connects to a sensitive resource, Smallstep acts as an invisible second factor. Authentication is seamless.

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.

smallstep