DATA SHEET

Enterprise Relay by Smallstep

Scalable Zero Trust Enforcement

Smallstep helps ensure that access to financial data, code repositories, PII and other sensitive resources is only possible from trusted, company-managed devices.

Smallstep Enterprise Relay

Smallstep Enterprise Relay is a transparent VPN that wraps a layer of TLS client authentication around your sensitive SaaS apps and internal networks. It is a standards-based [[RFC9298](https://datatracker.ietf.org/doc/rfc9298/)] private MASQUE relay.

It uses hardware-attested device certificates and mutual TLS to offer the strongest possible guarantee that *only* the devices you choose can access your most sensitive resources.

It works device-wide. Configure a list of allowed domains or excluded domains via MDM.

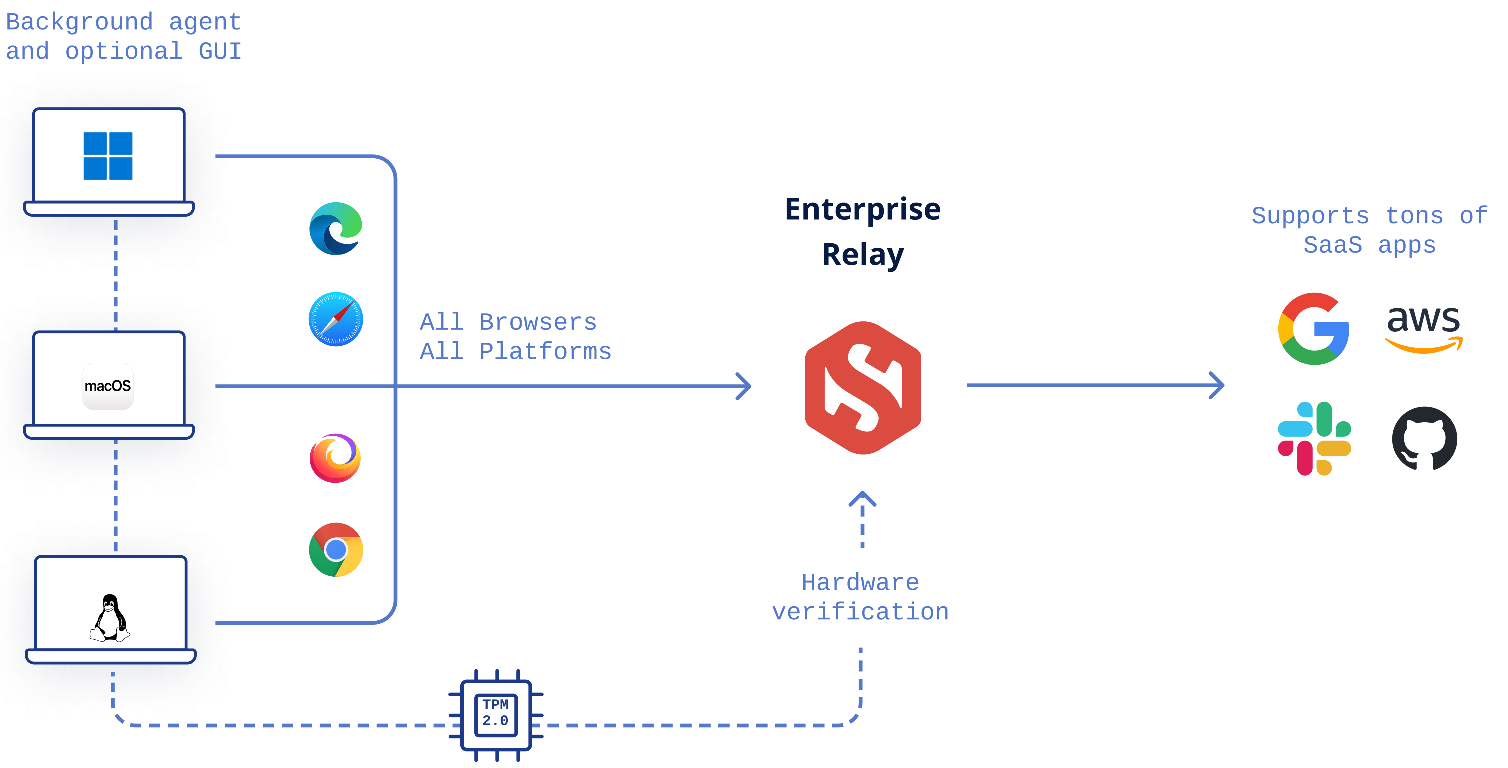
And it's seamless

it's transparent to the end user. No certificate dialogs, no authentication screens.

Key Features

- Restricts SaaS and private network traffic to your company-owned devices.
- Deploys via the [Managed Relay MDM payload] *(https://support.apple.com/guide/deployment/relay-payload-settings-dep131693e6b/web).*
- Uses mutual TLS authentication and hardware-bound, attested private keys.
- Can be combined with iCloud Private Relay as needed.
- Supported by managed Apple devices *(https://support.apple.com/guide/deployment/use-network-relays-dep91a6e427d/web)* in iOS 17, iPadOS 17, macOS 14, and tvOS 17.
- Smallstep agent adds cross-platform support for Apple, Windows, and Linux.

> "Our main gripe with our existing VPN was that it granted users access to our entire network, prohibiting us from reaching Zero Trust. **Smallstep's Enterprise Relay grants access per device/identity pairing** using short-lived certificates tied to hardware. This was an immediate security upgrade and reduced overall VPN maintenance pain."
>
> – Sr. Director, Network Engineering


Background agent and optional GUI
macOS
All Browsers All Platforms
Enterprise Relay
Supports tons of SaaS apps
aws
Hardware verification
TPM 2.0

How it works

Mutual TLS is the strongest authentication mechanism on the internet. But most SaaS apps don't offer mutual TLS authentication.

Furthermore, mutual TLS can be confusing to end users if not deployed properly.

Smallstep's network relay bridges these gaps. We offer mutual TLS authentication to your most sensitive apps and networks, while remaining transparent to the end user.

Smallstep issues hardware-attested device certificates to your iOS 18, iPadOS 18, macOS 15, and tvOS 18 clients via MDM.

Smallstep issues hardware-attested device certificates to your iOS 18, iPadOS 18, macOS 15, and tvOS 18 clients via MDM.

The Smallstep relay authenticates your clients using mutual TLS authentication.

It then routes your sensitive traffic so that you can filter by IP within SaaS apps, and all of your authenticated device traffic will appear (to the SaaS app) to come from the relay's outbound IP address range.

The relay's outbound IP address range is exclusive to your organization.

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.