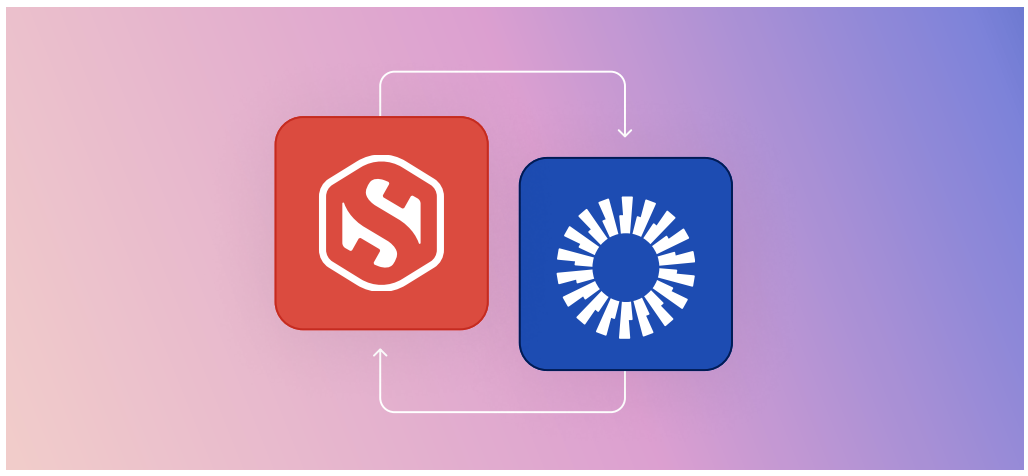
DATA SHEET

Okta + Smallstep

Raising the Bar on Device Trust



Secure your most sensitive resources with Smallstep's high-assurance device authentication.

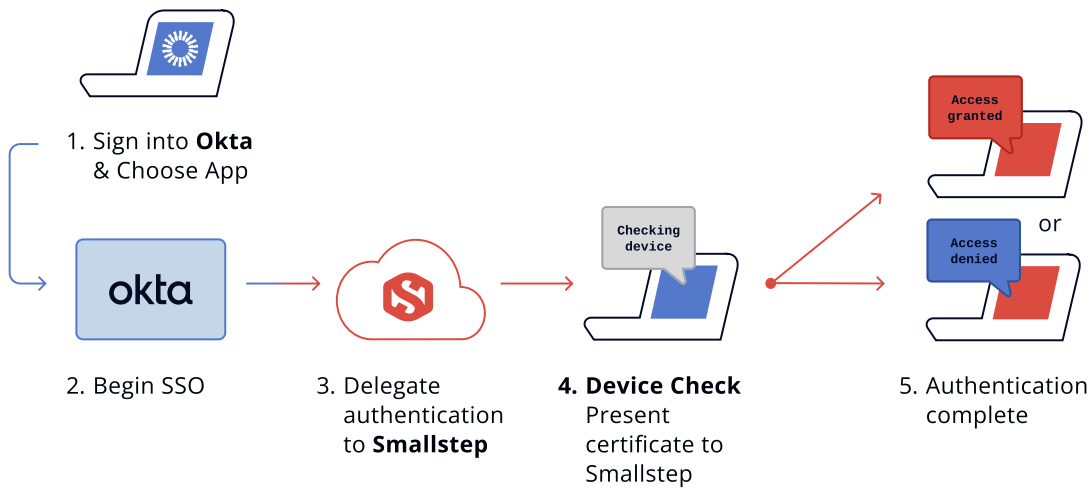
Smallstep's seamless Okta SSO integration provides the strongest guarantee that your Okta apps are accessible only from trusted devices.

Our cross-platform desktop application issues cryptographic IDs bound to each device's hardware, ensuring that credentials cannot be transferred to another device. This method significantly reduces the attack surface for sensitive resources.

Smallstep Device Trust Features

- **High-Assurance Device Verification**
  Add device identity checks to Okta, ensuring only trusted devices access sensitive resources.
- **Non-Exportable Credentials**
  Device keys are hardware-bound and cannot be exported, preventing theft.
- **Segregate Personal Devices**
  Limit access to critical resources by authorizing only company-owned devices.
- **Granular Access Control**
  Choose which SSO apps require device identity for enhanced security.
- **User and Device Authentication**
  Combine device identity with user authentication for stronger security.
- **Cost-Effective MFA Alternative**
  Replace Okta Adaptive MFA with a hardware-bound solution, reducing costs.

When Smallstep is integrated with an Okta app, device identity becomes a core authentication factor. Device IDs are verified seamlessly at login, without introducing additional steps or burdens for users.



Seamless Okta Integration

Smallstep serves as an external Identity Provider (IdP) factor for Okta, using industry-standard OpenID Connect (OIDC) flows and SCIM sync for efficient cross-domain identity management. This seamless integration strengthens your Okta environment by adding high-assurance device identity.

Stronger Security than YubiKey

Unlike a YubiKey, which identifies only users, Smallstep secures both user identity and device identity, ensuring access is restricted to trusted, company-issued devices. YubiKeys are portable, which introduces new attack vectors.

The June 2024 Snowflake data breach highlighted the risk of device portability. In that incident, malware on a personal device captured Snowflake credentials, enabling unauthorized access.

Smallstep prevents this by binding cryptographic credentials to the specific hardware of each device, ensuring they cannot be exported or transferred.

Enhanced Security, No Extra Steps for Users

With Smallstep, the hardware becomes the key. Users accessing resources from trusted devices experience no additional authentication steps. No physical tokens to plug in, no codes to enter—just seamless, secure access.

Smallstep is the market leader in end-to-end encryption across infrastructure. The comprehensive platform detects and mitigates anomalies, equipping developers with a toolkit that continuously monitors everything, everywhere. Smallstep removes the gap traditional secrets create, using certificates to enable trusted communications between technology and people. Learn more about operationalizing end-to-end encryption for all your devices, workloads, and people at smallstep.com.