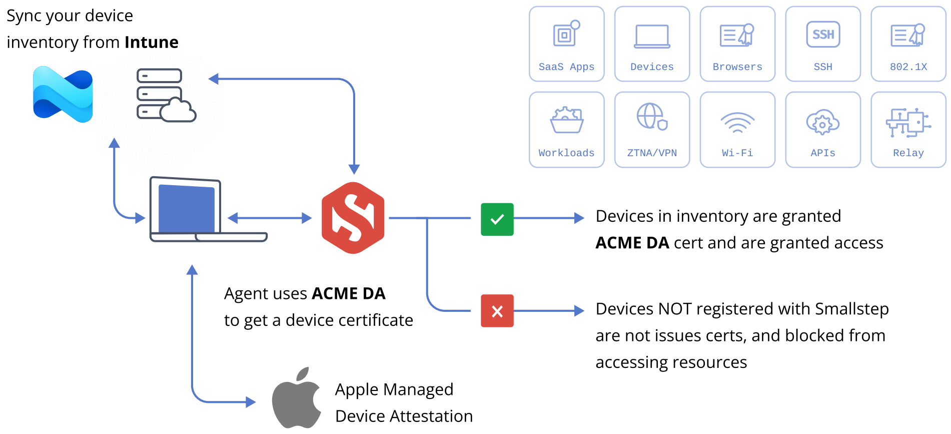
DATA SHEET

Intune + Smallstep

Trusted device enrollment with hardware based validation

Intune is the gold standard for managing enterprise Windows fleets, and Smallstep elevates that foundation with stronger, hardware-backed security. Our lightweight Intune integration ensures that only trusted, Windows devices can successfully enroll, with ACME Device Attestation providing hardware-backed proof of identity.

Enrolled devices receive non-exportable client certificates to access Wi-Fi, VPN, and other internal services securely.


Sync your device
inventory from **Intune**
SaaS Apps
Devices
Browsers
SSH
802.1X
Workloads
ZTNA/VPN
Wi-Fi
APIs
Relay
Devices in inventory are granted **ACME DA** cert and are granted access
Agent uses **ACME DA** to get a device certificate
Devices NOT registered with Smallstep are not issues certs, and blocked from accessing resources
Apple Managed Device Attestation

Smallstep Device Trust Features

When you add device trust to your security model, it becomes easier to contain threats—an attacker would need access to both valid credentials and a trusted device to gain entry.

Smallstep Trusted Device Inventory

- High-assurance device checks during MDM enrollment
- Hardware-bound keys that cannot be exported or cloned
- Prevent personal or unmanaged devices from accessing sensitive resources
- Strong device authentication layered with user authentication
- Seamless user sync from Okta, Google Workspace, and other IdPs
- Eliminate static SCEP secrets with dynamic, per-device enrollment challenges
- Extend trust beyond macOS to Windows and Linux fleets

When **Smallstep** is added to **Intune**, a device's hardware identity becomes an authentication factor. Instead of relying solely on shared secrets and user credentials, Smallstep silently verifies device trust —blocking unauthorized machines without adding friction for users.

Seamless Intune Integration

Smallstep brings together Intune's device management and hardware-backed device identity through ACME Device Attestation (ACME DA). This ensures that only verified, company-owned devices can access sensitive resources.

Instead of relying on user-based credentials or weak enrollment protocols, Smallstep cryptographically binds certificates to hardware, establishing true device identity. amf inventories are synced with Smallstep's Trusted Inventory, and the Smallstep Agent automates attestation, enrollment, and certificate lifecycle management across macOS and beyond.

Raising the Bar with Intune and ACME DA

Together, Intune, and Smallstep deliver the strongest assurance of identity across users and devices—without adding friction.

- **Replace SCEP with ACME DA:** Upgrade to hardware-backed enrollment for unspoofable, high-assurance device identity.
- **Build Trusted Inventories:** Combine Intune's device records with attestation data to guarantee only company-owned devices are trusted.
- **Enable Zero-Touch Provisioning:** New Windows devices and other endpoints prove their identity at first boot, allowing automatic enrollment without IT intervention.
- **Upgrade Existing Fleets:** Post-enrollment workflows raise devices to high-assurance standards without reimaging or manual rebuilds.
- **Cross-Platform Coverage:** Extend Intune's Windows focus to macOS and Linux with the same level of attested assurance.

Frictionless for Users

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. Stronger security, seamless experience.

Upgrading from SCEP to ACME DA

Most MDMs, including Intune, still rely on the Simple Certificate Enrollment Protocol (SCEP) for device enrollment. SCEP depends on portable credentials which can be replayed or misused by unauthorized devices. It offers no cryptographic proof that the enrolling device is the one intended.

ACME Device Attestation (ACME DA) is a new certificate enrollment protocol that solves this. Instead of passwords or profiles, ACME DA uses hardware-bound keys generated by Apple in the Secure Enclave during manufacturing. Only physical devices with those secure elements can enroll. **The result:** credentials that are non-exfiltratable, tamper- resistant, and cross-platform.

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.