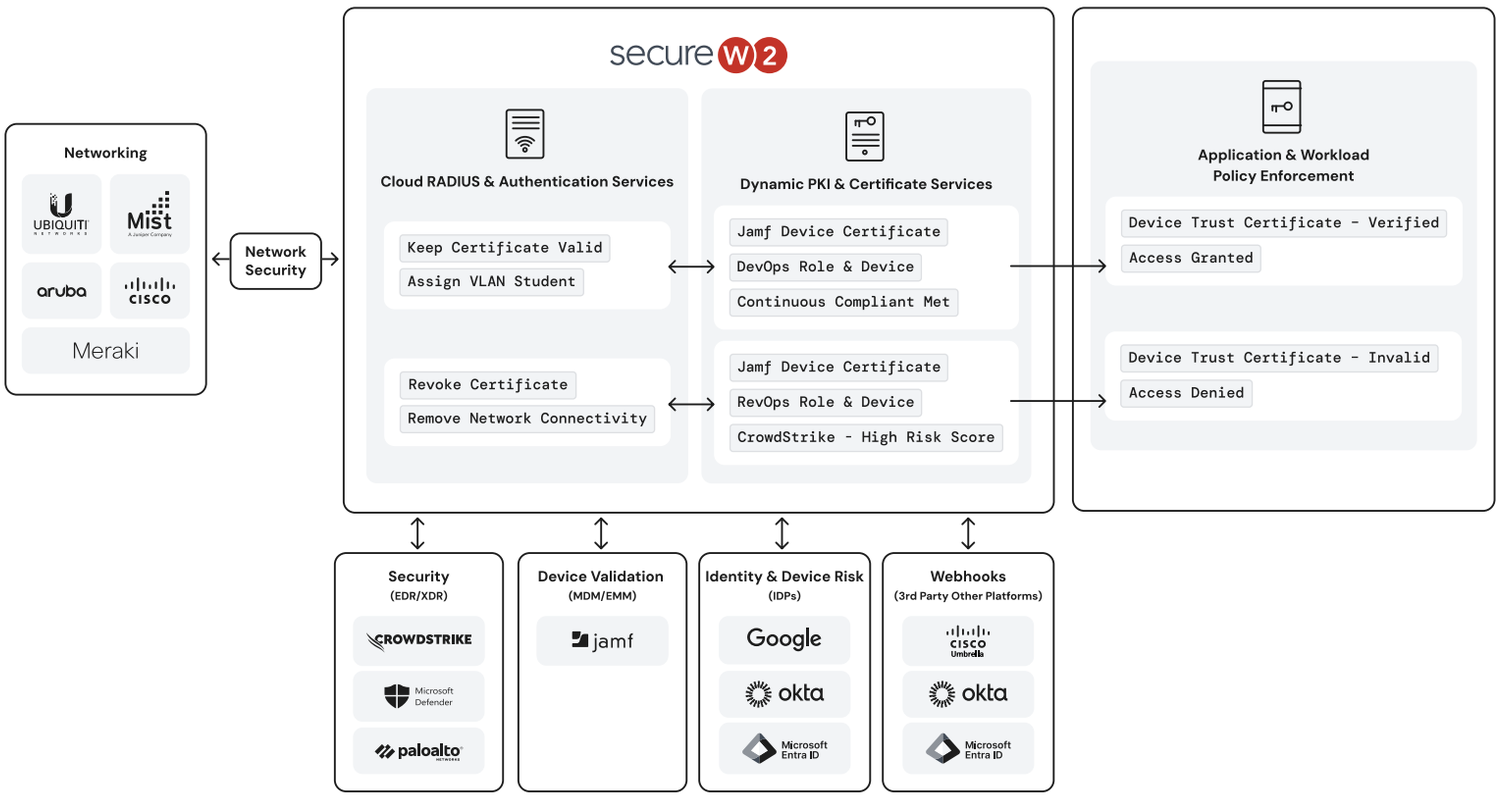
SecureW2 + Jamf Pro®
Integration Overview

Building & Maintaining Continuous Trust for Managed Apple Devices

With SecureW2 and Jamf Pro working together, organizations simplify certificate lifecycle management for Apple endpoints. Certificates are automatically issued to managed devices, continuously validated, and revoked if a device falls out of compliance or leaves management.

Unlike legacy SCEP, which relies on static shared secrets vulnerable to misuse, SecureW2 leverages the ACME protocol to securely automate issuance and renewal, while Apple Managed Device Attestation (MDA) cryptographically proves a device is genuine Apple hardware. The result is a system where device identity is continuously assured, and only Jamf-compliant devices can access networks and applications.



Organizations Using SecureW2 with Jamf

Figma Gigamon® PELOTON

"

"Securew2's ability to seamlessly integrate with leading MDM platforms (JAMF & Google Workspace for example) and identity providers has been invaluable."
—Francois S,
Telecom & Network Project Manager

North America Sales
(888) 363-3824
(512) 900-5515

UK, Europe and Middle East Sales
+44 20 3912 9916

Email
sales@securew2.com

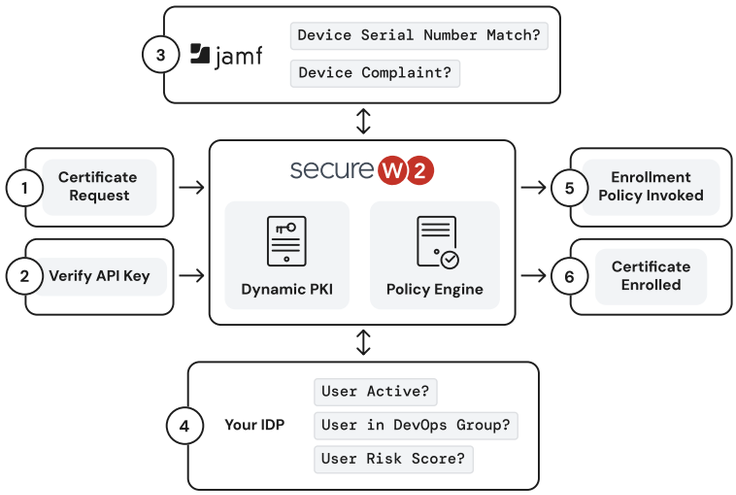
Website
securew2.com

SecureW2 + Jamf Pro® Integration Overview

Solid, Proven Device Trust for Managed Apple Devices

By integrating SecureW2 with Jamf Pro, organizations enforce trust at the source — certificates are issued only to Jamf-managed, policy-aligned devices and revoked the moment compliance fails.

With secure enrollment via ACME and hardware-level identity checks through Apple MDA, authentication decisions are always tied to verified device trust rather than static, one-time approvals.

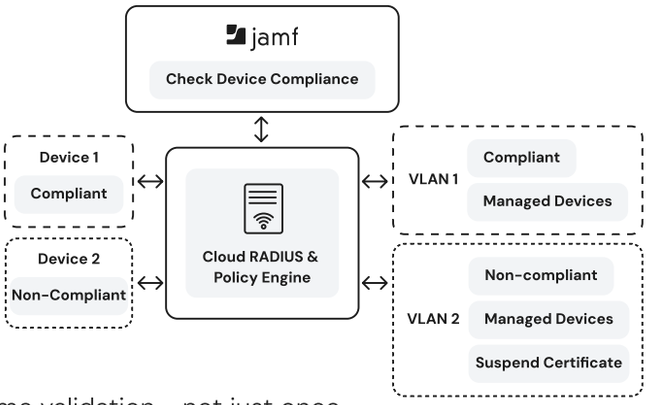


- **Jamf-Verified Device Identity** ensures only managed Apple devices receive certificates
- **Secure Issuance Protocols** such as ACME and Dynamic SCEP replace legacy static SCEP challenges.
- **Hardware-Level Assurance** with Apple MDA prevent spoofed devices from gaining trust.
- **Granular Certificate Policies** allow organizations to define issuance rules based on Jamf device attributes

Policy-Driven Lifecycle Management with Jamf Compliance

SecureW2 and Jamf work together to eliminate the manual overhead of managing certificates across Apple devices. Issuance, renewal, and revocation are tied to Jamf compliance workflows, so IT no longer needs to track certificate status or chase down rogue devices.

Certificates adjust automatically to changes in policy and device health, giving organizations a self-sustaining trust foundation.



- **Real-Time Compliance Checks** for continuous, real-time validation - not just once.
- **Jamf-Based Workflows** that automatically remove certs from non-compliant devices
- **Automated Renewal** to refresh certs before expiration and prevent downtime
- **Zero-Touch Segmentation** powered by a passwordless Cloud RADIUS

North America Sales
(888) 363-3824
(512) 900-5515

UK, Europe and Middle East Sales
+44 20 3912 9916

Email
sales@securew2.com

Website
securew2.com