digicert® x jamf

Automated Certificate Management & Device Security Integration

SOLUTION BRIEF

Automated Certificate Management & Device Security Integration

The Challenge:

Modern organizations with Apple devices use Jamf Pro, a cloud-based mobile device management (MDM) and mobile application management (MAM) service, to control how their devices and data are used.

These organizations need to deliver and secure digital experiences for the Apple devices and users across on-premises, hybrid, and multi-cloud infrastructures. Manual management of TLS/SSL certificates within these complex ecosystems creates risk, delay, and compliance gaps.

Certificates expire without visibility, and they can be provisioned inconsistently across virtual servers, or fail to comply with new short-lived validity policies. This exposes critical applications to outages and security incidents.

The Solution:

This integration allows Apple mobile devices and computers enrolled or managed in Jamf Pro to authenticate to corporate applications and resources without the need for usernames, passwords, or tokens for access. Using preconfigured certificate templates and automated lifecycle operations, IT teams can eliminate manual tasks and avoid costly authentication disruptions while maintaining a high level of security.

- Integrates DigiCert® Trust Lifecycle Manager with Jamf Pro for certificate-based device and user authentication
- Automates certificate enrollment, renewal, and revocation through the Simple Certificate Enrollment Protocol (SCEP) with enhanced security through dynamic challenge
- Supports API integration between Trust Lifecycle Manager and Jamf Pro for automation of the complete certificate management lifecycle. For example, unlike SCEP, the API integration supports certificate revocation and CRL Distribution or OCSP Checking
- Uses preconfigured templates for device and user authentication to corporate resources
- Synchronizes certificate events with Jamf Pro for real-time lifecycle updates and revocation handling
- Centralizes certificate visibility and policy control

Why it matters

- Improves user experience: Enables seamless enrollment and access without passwords, tokens, or repeated sign-ins
- Reduces helpdesk workload: Eliminates manual certificate requests and resets due to expiration or user error, while making user and device onboarding easier and more efficient
- Strengthens security posture: Enforces consistent, policy-based certificate issuance and revocation
- Prevents access outages: Automates renewals to ensure endpoints always have valid credentials
- Supports hybrid environments: Extends consistent identity assurance across mobile, desktop, and workstation endpoints
- Improves cryptoagility: Centralized certificate lifecycle management in Trust Lifecycle Manager eases the response to adverse events like revocations and facilitates the adoption of cryptographic improvements like Post-Quantum Cryptography

How it integrates

- Trust Lifecycle Manager connects with Jamf Pro via a cloud-based API and purpose-built connector
- Certificates are issued automatically to Jamf-managed devices
- Synchronizes lifecycle events—issuance, renewal, and revocation—between DigiCert and Jamf
- Administrators manage policies and certificate templates directly from Trust Lifecycle Manager

Business Value

Key Feature	Description	Data Points
Automated Certificate Management	End-to-end automation of issuance, deployment, and renewal on organizational Apple devices	Eliminates manual errors, outages, and ticket backlog
Centralized Visibility & Governance	Unified view of all device and user certificates from the Trust Lifecycle Manager dashboard	Simplifies oversight and enforces policy consistency
Scalable Deployment	Supports global deployment and management of devices	Eliminates manual errors, outages, and ticket backlog
Enhanced Auditing & Reporting	Logs every certificate action with full metadata for audit trails	Accelerates compliance with PCI-DSS, ISO 27001, NIST 800-57

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.