Jamf and Google – Managing and Securing Apple Devices for Cloud-Native Organizations

*For organizations offering device choice and work-flexibility, the challenge for technology leaders is driving **efficient**, **secure**, and **scalable operations**, without compromising end-user experience.*

Google Cloud

Google Workspace

chrome enterprise

Offering Apple in the enterprise should be a strategic decision, not a compromise. When organizations offer Apple endpoints for their workforce, they need tools built specifically for the platform. It's beneficial for productivity tools like Google Workspace to cross-platform but when it comes to when it comes to management and security, depth of platform expertise is critical.

Using cross-platform or Windows-centric tools to support Apple often creates friction, complexity, and blind spots:

1. Bloated endpoint agents that degrade performance.
2. Traditional VPNs increase attack surface and frustrate users.
3. Under-managed macOS and iOS endpoints with poor visibility.

Platform-specific tooling is a proven foundation for long-term device program success. Moving away from legacy management stacks to purpose-built Apple solutions helps empower users and realizes your companies investments into the Google ecosystem.

Jamf offers the only Apple-first solution that integrates deeply with Google Workspace, Chrome Enterprise, Google Cloud Identity, and Google Security Operations. The result? A streamlined, zero-trust ecosystem designed for internal IT and Security teams in cloud-forward organizations.

Google and Jamf work together so that organizations of all sizes can connect, create, collaborate and work securely.

Together, Jamf and Google deliver productivity and collaboration for your Apple-enabled workforce, all secured by an identity-driven, zero-trust outcome for Apple in the enterprise.

This enables organization to ensure only authorized users on enrolled, secured devices can access business applications and data. These devices are protected through robust management, network controls, and endpoint security. With all traffic governed by Zero Trust Network Access (ZTNA) for secure, scalable remote connectivity.

Jamf and Google have long shared a vision for replacing legacy VPNs with modern, layered security solutions. Together, we deliver a seamless, Apple-first zero-trust experience tailored for the needs of today's hybrid enterprises.

With Google Workspace enabling secure collaboration and productivity and Chrome delivering secure, policy driven browsing on Mac and mobile, organizations can confidently support Apple users with best-in-class management and security.

By combining Jamf with Google's cloud-first productivity tools and secure browsing, organizations can confidently embrace a zero-trust strategy that puts Apple at the center. This integrated approach not only protects users and data, but also empowers employees to work flexibly, securely, and productively, wherever they are.

Integrated Zero Trust Security, Powered by Jamf and Google

Integration overview	Description	Product Documentation or Marketplace Listing	Jamf Product	Google Product
Secure LDAP for Querying Users and Groups	Directory information about an organization's users (name, email, role, etc.). This information can be used to ensure the right apps and settings get to the right end users. By pulling this information in, the admin doesn't have to recreate it manually.	**Integrating with Google Secure LDAP**	Jamf Pro, Jamf School	Google Workspace, Google Cloud Identity
Google Context Aware Access Integrations	The integration allows mobile and Mac devices to share the Jamf-determined compliance state with BeyondCorp. Restrict access to applications protected by Context-Aware policies.	**Google BeyondCorp Enterprise**	Jamf Pro, Jamf Connect	Google Workspace, Google Cloud Identity, Google Cloud
Enabling Chrome Enterprise Core and Premium	Chrome Enterprise has features and functionality that benefit organizations at scale. Jamf Pro and Jamf School can help enable the enterprise features within Google Chrome.	**Enroll browsers on macOS with Jamf Pro** **Enroll browsers on mobile with Jamf Pro**	Jamf Pro, Jamf School	Chrome Enterprise
SSO for Cloud Identity	This allows for the Admin(s) at an organization to login to their Jamf Pro instance, Jamf macOS Security Cloud portal and Jamf Security cloud portal, with their Google credentials.	**Configuring Single Sign-On with Google Workspace**	Jamf Account	Google Workspace, Google Cloud Identity
Cloud based identity for Mac	This allows for the end users at an organization to login to their Mac using their Google credentials. This is the same experience available on Chromebook or on Windows with GCPW.	**Integrating with Google Identity**	Jamf Connect	Google Workspace, Google Cloud Identity
Jamf Protect Parsers for Google Security Operations	The Jamf Protect and Google Security Operations integration allows detailed event data, Alert and Unified Logging events captured by Jamf Protect be sent to SecOps for logging and analysis.	**Google Security Operations**	Jamf Protect	Google Security Operations
Jamf Pro Parsers for Google Security Operations	Inventory information from Jamf Pro can be parsed by Google Security Operations	**Google Security Operations**	Jamf Pro	Google Security Operations
Account Driven User Enrollment with Google Identity for iOS BYOD	Provide device management that respects user privacy on personal mobile devices. Users simply onboard via the settings app, leveraging their Google credentials to enroll into device management, to receive profiles and apps.	**User Enrollment for BYOD**	Jamf Pro, Jamf School	Google Workspace, Google Cloud Identity

C3779449-0626