jamf | okta

Manage and **secure** identity and access for Apple at work

Jamf and Okta share a vision of modern cloud identity for an uninterrupted, native login experience on Apple devices. Our integrated technology allows us to provide unified identity access across apps, secure access to company apps and a fast, identity-led onboarding experience for modern, seamless identity management.

Trusted Access combines the best elements of device management, identity, connectivity and endpoint security into a cohesive whole that is stronger than the sum of its parts. Cloud identity is at the heart of Trusted Access.

Device Management serves as the foundation of Trusted Access, supporting verified enrollment of company-owned and BYO devices. Device deployment is easy and secure, reducing the number of sign-ins required when enrolling into MDM.

Identity and Access Management is made easy with Okta as a cloud identity provider. Accessing all apps and company resources with just one set of Okta credentials saves IT and end users time.

Endpoint security ensures only trusted devices can access sensitive company resources, adjusting user access permissions based on device risk or device management status. This way vulnerabilities are instantly acted upon and both new connections and active sessions are secured, reducing risk of unauthorized access from non-trusted users and preventing bad actors from accessing compromised devices.

With Jamf and Okta, organizations can:

- Provide easy access to company resources and apps through Okta
- Enable smooth device deployment with Enrollment Single Sign-on (ESSO), deploying Okta FastPass for passwordless app logins using biometrics
- Leverage secure and user-friendly multifactor authentication (MFA), passwordless Single Sign-on (SSO) and Platform Single Sign-on (PSSO)
- Ensure device trust for managed devices
- Ensure continuous conditional access – notify Okta when there is a change in management, security or compliance status
- Leverage managed device attestation and network relay for stronger and more context-aware identity protection

Integrations

With Okta as the identity provider and Jamf as the management and security solution, joint customers can offer their end users seamless uninterrupted, productive workflows anywhere and anytime. Here is how Jamf and Okta integrate to achieve this:

Integration	Description	Jamf solutions	Okta solutions
MacOS account provisioning and password sync	Create local Mac user accounts on managed devices that authenticate users with their Okta credentials and keeps their password in sync. Having the user's cloud identity bound to their device gives IT granular control over access and permissions and simplifies ongoing authentication for end users, keeping them productive thanks to uninterrupted workflows.	Jamf Connect Jamf Pro or Jamf School	Okta Identity Cloud
Enrollment SSO (ESSO) for iPhone and iPad	Designed to make user enrollment faster and easier, ESSO reduces the number of sign-ins required of a user when enrolling into devices. By installing Okta Verify, new employees no longer need to worry about repeated authentication during and after the enrollment process.	Jamf Connect Jamf Pro or Jamf School Jamf BYOD	Okta Identity Cloud/ Okta Verify
Platform Single Sign-on (PSSO) for Mac	End users can access all relevant applications on a Mac device by signing in only once, reducing the number of requests for users to enter the same credentials repeatedly for every app. Leveraging PSSO increases efficiency, user productivity and security by reducing the risk of authentication errors.	Jamf Connect Jamf Pro or Jamf School	Okta Identity Cloud
Passwordless authentication with Okta FastPass	Okta FastPass can be enhanced with Touch ID or Face ID, Apple's native on-device biometric security that is even faster and more phishing-resistant than previous MFA workflows requiring password and out-of-band authentication methods such as SMS, email, or push notifications.	Jamf Connect Jamf Pro or Jamf School	Okta Identity Cloud/Okta Verify
User/Group Synchronization	Jamf Pro can access users and groups stored in Okta through Okta's LDAP interface, eliminating the requirement to connect MDM to Active Directory. In addition, when enabled, Jamf Pro or Jamf School can assign customized content and policies to devices that belong to users who are members of particular LDAP groups.	Jamf Pro or Jamf School	Okta Identity Cloud
Automations for user identities	Okta Workflows provide a codeless, drag-and-drop platform to automate the processes of onboarding and offboarding employees. These workflows can work with any API to centralize coordination of IT tasks such as adding new employees to user groups or ensuring former ones don't have access to systems.	Jamf Pro	Okta Workflows
Continuous conditional access	Okta continuously adjusts user access based on changes in device risk and management status from Jamf, keeping both new connections and active sessions secure.	Jamf Pro Jamf Protect	Okta Identity Threat Protection

jamf

www.jamf.com

Find out how Jamf and Okta can simplify your work and enhance user experience. **Request a trial** or contact your preferred reseller.