Power the Mac Experience with Cloud Identity

Reduce IT tickets and increase security with Okta and Jamf Connect.

Modern authentication, zero-trust user access and an excellent user experience can now co-exist.

As employees and their devices become increasingly mobile, security requirements are harder than ever to satisfy. As such, it's essential to have tools in place that ensure only the right people, devices and networks are accessing your sensitive corporate data.

Unfortunately, these security requirements generally mean a heavy burden on employees, forcing them to jump through a series of hoops to simply access the resources they need to get their work done. All too often users have multiple accounts, disparate applications (with no awareness of each other), and far too many usernames and passwords to juggle at any given time.

In a recent **Mac in the Enterprise survey** conducted by Vanson Bourne, 31% of Mac users surveyed cited login and credential issues as a top problem they experience at work.

And when users are unable to login or have credentials verified, work comes to a screeching halt.

31%

of Mac users surveyed cited login and credential issues as a top problem they experience at work.

-Vanson Bourne

Streamline user productivity in a security-minded manner.

With Okta Identity Cloud and Jamf Connect, organizations can ensure a high level of user trust by unifying identity across apps and devices through a seamless single sign-on experience with Mac. This best-of-breed approach to access management, user management and device management empowers organizations with three unique benefits.

1

Modern provisioning and authentication out of the box.
With Jamf Connect and Okta, employees have a simple, secure onboarding experience on their Mac. This provides a single set of credentials to login to the workstation and the Okta dashboard; empowering IT to secure the login process by enforcing multifactor authentication and pre-configured devices for employees on day one.

2

Sync user identities and device credentials.
Jamf Connect enables users to keep their corporate identity from Okta (or Azure Active Directory accounts) in sync with their local Mac account password at all times. This helps eliminate IT tickets for forgotten passwords, and empowers users to sign into their Okta account and manage their shared cloud and Mac credentials.

3

Passwordless access to business-critical apps.
Configuring Okta single sign-on with Jamf Connect enables organizations to deliver a reliable, passwordless login experience to web and mobile apps — with standards-based federation and configurable access policies. Jamf helps eliminate the need for users to enter credentials to login to Okta, delivering passwordless authentication once a user logs into their Mac for the first time.

"We put Okta in front of our applications and that then allowed a single username and password from the desktop all the way into the application itself, which accelerated the usage of those apps."

— Dan Backer, Director of Campus Technology, National Geographic

EXTEND IDENTITY-DRIVEN SECURITY WITH DEVICE MANAGEMENT.

Jamf Connect pairs with most modern device management solutions, but when organizations leverage Jamf Pro — the gold standard for Apple device management — and Okta Device Trust, they can also prevent unmanaged Macs from accessing corporate SAML and WS-Fed apps. Device Trust ensures that only known and secured devices can access Okta-managed applications.

With Jamf Connect, Jamf Pro and Okta, seamless and secure access to the applications users need most is a reality. Put these tools in place and bridge the IT and business gap and start innovating faster at your organization.

Ready to leverage the Jamf and Okta solution to better serve users, IT and your entire organization?

Get Started Today

Embrace cloud identity to drive an unparalleled Mac user experience and strengthen your organization's security posture.

Get started at **jamf.com/okta.**

 jamf

www.jamf.com