okta | jamf

Unifying strong security and seamless device management with Okta + Jamf

When it comes to device management, enterprises find themselves at an inflection point. The shift to hybrid work has created the need to manage a complex web of device ecosystems––and these ecosystems include a growing number of Apple devices, both managed and BYOD. These devices empower your workforce and make innovation possible, but they also create a network of opportunities for bad actors looking to breach safeguards and access sensitive information.

Addressing this problem requires a strong option for managing and securing devices. Many device management systems, however, lack out-of-the-box functionality in key security areas such as Identity and access management (IAM). And while employees tend to love Apple devices for their ease-of-use and popular applications, some IT, security, and Identity leaders have reservations concerning the secure management and control of these devices. This Apple "comfort gap" between employees and administrators is a thorn in the side of many enterprise organizations.

Okta + Jamf closes that gap. By adding best-in-class IAM to your endpoint device management solution, the combination of Okta and Jamf strikes a perfect balance between robust security and seamless user experience.

With Okta + Jamf, IT and security teams can lead with confidence, knowing they have a combined IAM/MDM solution that offers:

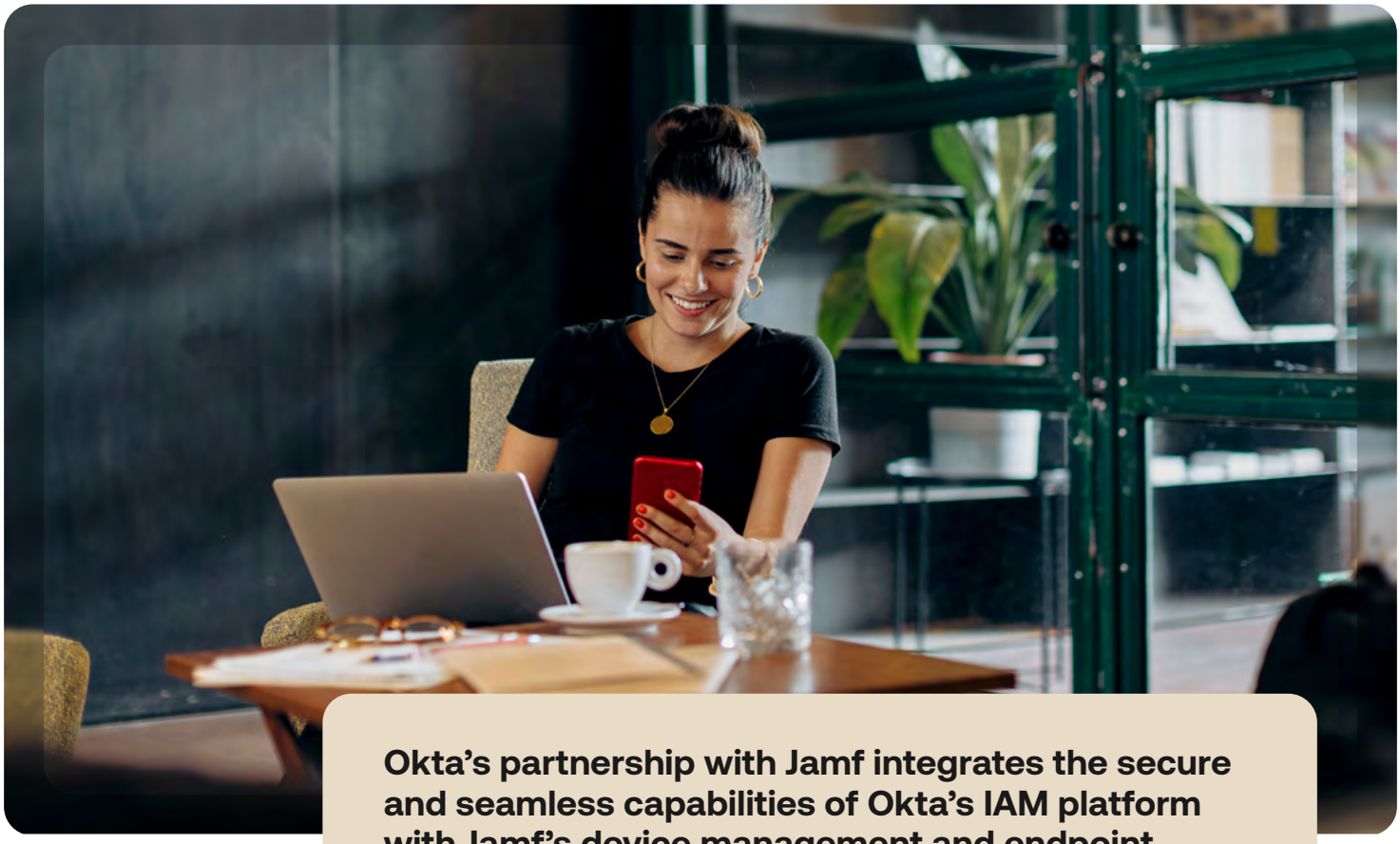
Streamlined, secure enrollment for managed devices, keeping company and employee data safe on company hardware.

Unified MDM with strong threat protection, that satisfies core IT and security goals.

Delightful user experiences that keep employees happy and productive.

AI-powered continuous risk monitoring and adaptive responses, preventing threats without disrupting user workflows.

okta | jamf



Okta's partnership with Jamf integrates the secure and seamless capabilities of Okta's IAM platform with Jamf's device management and endpoint security solutions for Apple devices

This integrated offering establishes Identity-powered trust in all Jamf-managed devices, enabling smooth and seamless device enrollment and admin access while enhancing overall security with core Okta features like Adaptive MFA. The result is an approach to device management that achieves the best of both worlds:

Employees get to leverage the convenience of single sign-on, which consolidates individual desktop, mobile, and app logins into one set of credentials.

IT and security leaders get to rest easy knowing that sensitive company and employee information is protected by an industry-leading, cloud-native Identity solution.

Here's how it works

Apple Platform SSO (PSSO) for managed desktop applications

This integration, supported by Jamf Pro, syncs users' local Mac password with Okta for secure, streamlined device access. Users have the option to unlock their devices using passwordless or secure biometric authentication. Effectively, this delivers a user experience as intuitive as leading consumer apps, but combined with enterprise-grade phishing-resistant security.

Enrollment SSO for bring your own device (BYOD) applications

This integration streamlines the initiation of BYOD devices into remote management by facilitating the installment of Okta Verify onto users' devices. This enables the apps used on the managed device to use Okta's SSO extension, further unifying and simplifying secure access to key tools for employees.

Identity Threat Protection with Okta AI

This integration leverages Okta's AI-powered Identity Threat Protection (ITP) to continuously assess risk across the user journey. ITP ingests alerts from Jamf Pro, as well as other security solutions, enabling automated responses through inline actions based on suspicious behavior, for example by initiating a Universal Logout in response to a malware download detection. ITP uses the Continuous Access Evaluation Protocol (CAEP), which is part of the OpenID Shared Signals Framework (SSF), to share real-time, session-related security events between Okta and Jamf.

okta | jamf

Key Benefits

Greater Simplicity

Let your team focus on strategic initiatives, not administrative busywork.

Managing Apple devices and user identities within a single integrated solution reduces administrative overhead and improves efficiency.

Stronger Security

Streamline processes without compromising on data protection.

A unified approach to Identity management, combined with advanced threat detection and response, ensures secure access to devices and core applications.

Superior UX

Support your team with user experiences that boost productivity.

Integrating Managed Apple IDs with Okta's sign-on capabilities creates streamlined access that doesn't undermine security.

For more information on this integration, visit okta.com/partners/jamf.
If you have more questions, please contact our sales team at okta.com/contact-sales.

About Okta

Okta is the World's Identity Company. We free everyone to safely use any technology—anywhere, on any device or app. Our Workforce and Customer Identity Clouds enable secure yet flexible access, authentication, and automation that transforms how people move through the digital world and puts Identity at the heart of business security and growth.