

Expanding the reach of Universal Logout for enhanced security

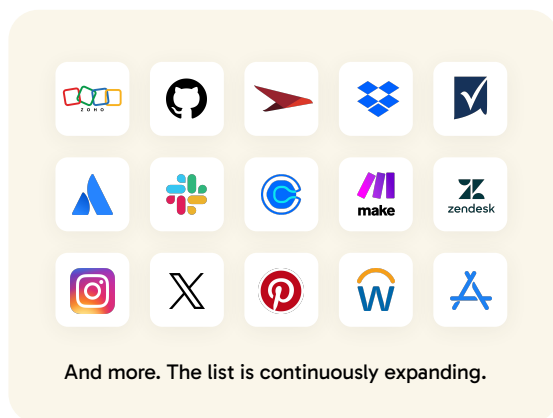
Overview

Cerby, the identity security solution for disconnected apps, and Okta have introduced a new integration that extends Universal Logout, part of Okta Identity Threat Protection, to any application. This integration enables instant logout and access revocation across all devices and apps—without requiring APIs—enhancing threat detection and response while reducing risks from compromised accounts.

How it works

Cerby's technology enables Okta to build scalable, reliable integrations without requiring app changes. It extends protection to a broader set of apps, including those not typically supported by identity providers. Cerby and Okta handle logout, with actions audited and integrated into SIEM systems, creating a closed feedback loop to ensure remediation is completed. Together, Cerby and Okta secure the entire app ecosystem and reduce the risk of compromised accounts.

Applications supported



Key benefits & features

Comprehensive & deep access revocation

- One-click revocation across all devices and supported applications
- Continuous expansion of supported applications
- Eliminates all active tokens and session data, ensuring no lingering access remains
- Dismantles the entire chain of authorization inheritance

Intelligent, context-aware action

- Responds to changes in device context without user interaction
- Triggers logout even for out-of-band signals, a unique capability in the industry

Seamless integration

- Works with Okta's Post-Auth Actions and Entity Risk Policy
- Complements Identity Threat Protection's precision risk response capabilities

Why choose Cerby + Okta?

In an era of increasingly sophisticated cyber threats, Cerby and Okta provide fast, intelligent, and comprehensive solutions for identity and access management, enabling organizations to strengthen security, improve operational efficiency, and respond to threats instantly.

About Cerby

Cerby is the only identity security platform built for disconnected applications, providing IT and Security teams with comprehensive control over apps that lack APIs or support for protocols like SAML or SCIM. Seamlessly integrating with existing identity providers (Okta, Azure AD, etc.), Cerby extends critical security automations—such as single sign-on, multi-factor authentication, and lifecycle management—to any application without incurring the costly “SSO tax.” Cerby automates essential tasks like user deprovisioning and password rotations, reducing manual work while closing security gaps. With Cerby, teams gain full control over their app ecosystem, strengthen security, and reduce costs.

Visit us at [Cerby.com](https://cerby.com) and follow us on social at [@CerbyHQ](https://twitter.com/CerbyHQ).