



# Credential Management & SSO

## Secure and automated credential management

Disconnected applications often leave users managing their own passwords, MFA settings, and access sharing. The result: weak passwords, inconsistently applied MFA, and lingering shared access.

Cerby eliminates these risks by centralizing credential management across SaaS, legacy, and on-premise apps. Credentials are stored in a zero-knowledge vault and governed by policies for password complexity, rotation, and access.

Cerby also delivers a secure SSO and MFA experience to disconnected apps. Users click on tiles from their IdP dashboard while Cerby securely autofills credentials and MFA codes. Shared access is granted without exposing credentials and automatically revoked.

This approach brings modern identity practices to every app, even those without SAML, avoiding the high "SSO tax" vendors often charge.

# 78%

reduction in administrative  
access tasks

# FOX

## The Cerby Solution

Every Credential. Fully Governed.



### Centralize credential management

Securely manage credentials for SaaS, legacy, and on-premise apps from a unified platform. Cerby stores credentials in a zero-knowledge vault and enforces policies for password complexity, rotation, and access permissions.



### Enable secure shared access

Provide shared account access without revealing passwords or MFA codes. Maintain full audit logs, and automatically revoke access when it's no longer required.



### Automate access to credentials

Integrate with your IdP to automatically trigger the provisioning, rotation, and revocation of credentials for disconnected apps. Eliminate manual updates, tickets, and spreadsheets.



### Deliver a seamless SSO experience

Cerby lets users access disconnected apps from their IdP dashboard just like any SAML-connected app. Credentials and MFA codes are autofilled securely, providing a consistent and secure login experience.



## Cerby Features & Capabilities



### Zero-Knowledge Vault & Credential Sharing

Credentials are never exposed—not even to Cerby. Share access securely and automatically revoke it.



### Automated Credential Management

Manage the full credential lifecycle—capture, create, rotate, and revoke—with policy-driven automation.



### SSO And MFA For Disconnected Apps

Enable SSO and enforce MFA for apps without native SAML support. Cerby auto-fills credentials and MFA codes.



### Public APIs

Programmatically create, manage, and rotate credentials at scale.



### IdP Integrations

Use existing IdP roles and groups to control access. Launch disconnected apps from your IdP dashboard.



### Comprehensive Logging

Monitor who accessed which apps and when. Export logs or connect to your SIEM for compliance and visibility.



Cerby automatically logs us in using our corporate credentials and handles 2FA. No more password or 2FA code sharing.

□ Siobhan Sullivan

Director of Global Community Marketing



### 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).