



How Cerby integrates your disconnected applications

A practical guide to connecting your existing identity stack to every application

Today's organizations rely on a large and ever-growing number of applications. Even smaller companies may use well over 100, and enterprises—many of which have reached immense scale through mergers and acquisitions—typically manage several hundreds.

Unfortunately, attaining full coverage across—and control over—this application ecosystem has proven elusive.

Closing the application gap

An identity platform's ability to manage applications depends heavily on their support for integration standards, such as SAML, SCIM, OIDC, or offering usable APIs.

But many applications don't. These disconnected applications either lack integration capabilities altogether or lock them behind expensive enterprise plans—what we call the "SSO tax." In both cases, IT and security teams are forced into costly, manual workarounds that don't scale and increase risk.

Cerby solves this with a purpose-built platform that reliably integrates any application into your existing identity infrastructure—without requiring native standards support or expensive licensing tiers.

Why organizations choose Cerby



To close the application gap

Connect any application—even those without standard protocols or APIs (e.g., SAML, SCIM, OIDC)



To maximize existing IAM, IGA, and PAM investments

Extend your current tools to cover every application in your environment—Cerby completes your stack—no rip-and-replace required



To connect applications on day one

Start fast with thousands of pre-built integrations available in the Cerby Application Network



To get rapid time to value

Cerby delivers integrations faster than any other platform, accelerating time to value and ROI



To keep pace with change

We continuously monitor and update integrations—and use self-healing automation to detect and adjust to UI or workflow changes in real time, so the application gap stays closed



The Cerby Application Network

Cerby already supports thousands of applications out of the box—and we're always adding more



GitHub



GitLab



Asana



Atlassian



ServiceNow



Looker



Adobe



Braintree



Carta



QuickBooks



Xero



ADP



BambooHR



LinkedIn



Meta



Google



Youtube



Reddit

[See what's already integrated in the Cerby Application Network](#)

Cerby integration process

Our proprietary integration engine combines API operations, patent-pending agentic AI technology, and advanced UI automation to deliver reliable, scalable integrations—regardless of the application's native capabilities—that Cerby proactively monitors and maintains.

We guide your team through each of the four key phases, as described below, to ensure your integration works smoothly with existing identity systems and meets your access, security, and compliance needs.

Our team stays closely involved throughout, sharing regular updates and responding quickly to feedback or questions.

Steps to make the integration process successful:



Involve the application owner or admin early in the process



Share clear documentation for workflows and permissions



Provide timely feedback during testing



Stay aligned through open communication

Requirements and access

Our integration process starts by thoroughly documenting your **integration requirements** and **application details**.

Information	Purpose	Examples
Integration requirements	Understand what identity automation workflows you'd like Cerby to build	• Identity lifecycle management (IdLCM) • Password rotation • Multi-factor authentication (MFA) • Access control and authorization preferences
Application details	Understand your current production environment (e.g., application deployment and configuration)	• App version/license type • User authentication method (SSO vs credentials) • MFA requirements • Account sharing practices (if any) • User roles and permissions structure • Any network, security, or compliance requirements

Next, our team will need **application access**. There are three options available, and we will recommend the best approach based upon the integration requirements and application details.

	Best for	Your involvement	What to expect
Integration requirements	• Apps that are harder to obtain and you have an Enterprise-tier subscription • High-security environments • Legacy or custom applications accessible in a web browser	• Provide Cerby a temporary admin account in a test or sandbox environment • Share permission structure	• Most comprehensive setup • Integration matches your exact environment
Automated Exploration		Install Scout by Cerby extension (read the article to learn more)	Exploration in <30 minutes
Self-Service Access	SaaS applications where a self-service account or a trial period is available	Validate that Cerby's account has features and permissions consistent with your own	Development can start as soon as Cerby's application access and permissions are validated for consistency

PHASE 2

Development and testing

During this phase, Cerby's team builds the necessary workflows and automations based on your requirements. Each integration is tested for functional accuracy, performance, and reliability before moving to the next phase.

PHASE 3

Validation

Once the integration is live in your Cerby workspace (e.g., <company>.cerby.com), we run a full set of validation tests in your environment. We'll confirm that automated workflows behave as expected and deliver a report summarizing results, including any workflows that need tuning.

PHASE 4

Continuous improvement

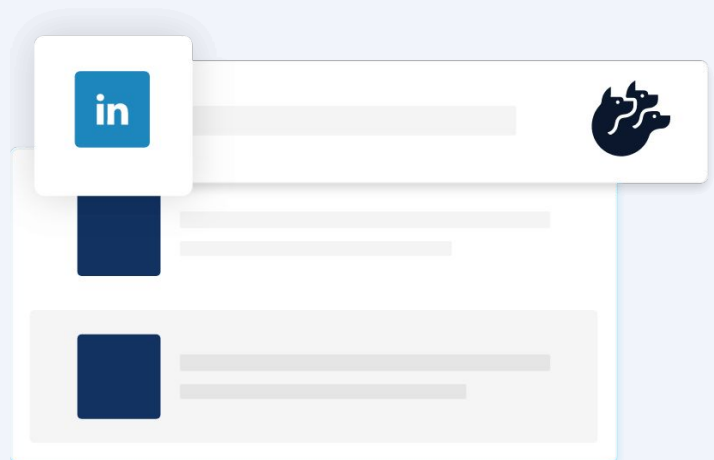
After deployment, Cerby continues to monitor integration health. As applications evolve, we use self-healing automations to maintain performance—eliminating the drift and degradation that often come with custom-built or one-off scripts.

Got an application that needs to be connected?

If you're tired of...

- Tracking access in spreadsheets?
- Writing custom scripts?
- Employing ticketing systems and manual fulfillment workflows to request and grant access?
- Building and maintaining custom integrations for high-priority applications?

Request a Cerby integration today and get the coverage your identity stack is missing



About Cerby

Cerby is the identity automation platform purpose-built to secure disconnected applications—those that fall outside the reach of traditional identity security tools. By integrating with existing IAM, IGA, and PAM systems, Cerby brings centralized access controls, automates manual security tasks, and extends governance across your entire application ecosystem. IT and security teams gain complete visibility and control, reducing risk and operational overhead. Founded in 2020, Cerby is backed by leading investors and trusted by enterprises across the globe.

To learn more, visit www.cerby.com