cerby® + Microsoft Azure Active Directory

Stay secure, increase productivity, and protect your brand, automatically.

Cerby delivers Zero Trust principles for any application—even unmanageable ones that don't support standards like SAML, OIDC, and SCIM. Cerby increases the reach of Microsoft's Azure Active Directory by extending its lifecycle management to any non-standards supporting application. Combining Azure Active Directory and Cerby's automation platform helps reduce cyber risk by helping IT and security teams manage authentication for any application and then delegate authorization to business owners. Cerby then detects and automatically corrects security lapses using its robotic process automation engine while ensuring only valid employees and trusted third parties can access your applications.

About the integration:

Today's application landscape is complex. Many organizations leverage dozens of cloud-based applications for business purposes. Most of these applications, however, do not support industry identity and security standards such as SAML and OIDC for single sign-on or SCIM for the automated creation, update, and removal of users.

Pulling from Azure Active Directory users and groups, IT and security teams can now include applications previously outside their reach into key security initiatives like Zero Trust.

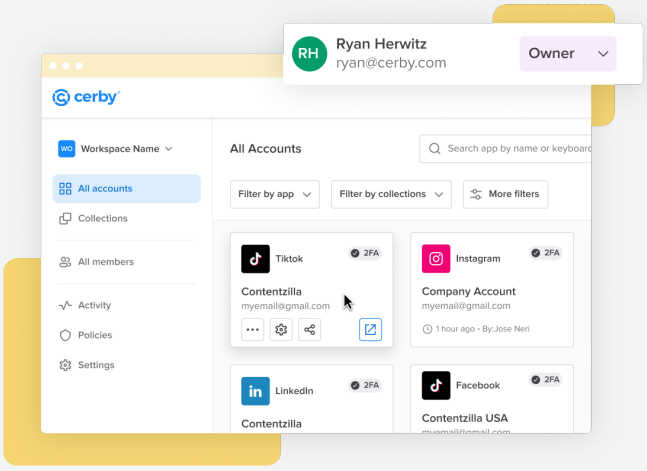
The Okta + Azure Active Directory integration allows users to

- Extend Azure Active Directory's single sign-on to any application regardless of the underlying platform APIs.
- Manage the lifecycle of creating, modifying, and removing access for any application.
- Include any application in your Zero Trust protect surface.

Integration benefits

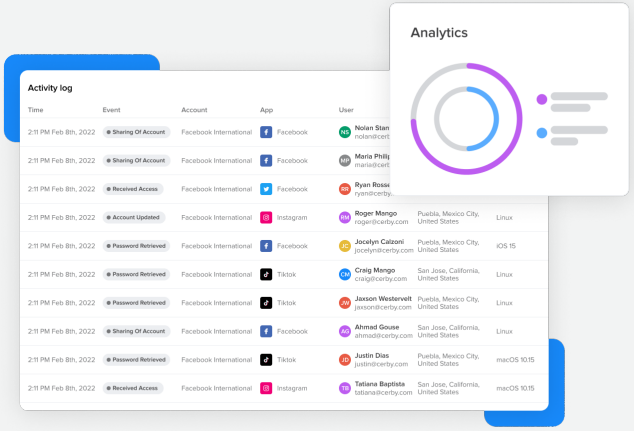
Secure any application

Cerby's out-of-box integration with Azure Active Directory enables secure SSO-like login and other automated procedures even when the underlying application does not support SAML or OIDC. Cerby can work with any web-based service or mobile application, enabling users to deploy the best application for the job.



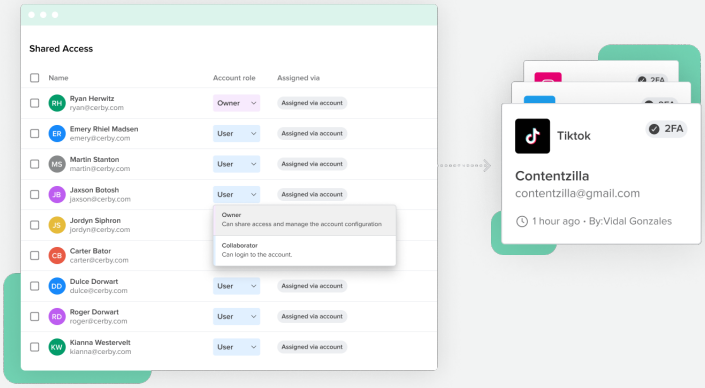
Get granular visibility

Trying to track what's happening across applications that aren't connected via Azure Active Directory is hard. With Cerby + Azure Active Directory, all access is individualized and tracked even when multiple users are utilizing the same account, as is common with the business use of social media applications like Twitter and Facebook as well as many corporate banking applications and IT tools.



Create smart policies

For shared accounts, you may not want a particular user to be able to carry out operations, like resetting a password. With Cerby, you can configure and apply your own roles–even when users are accessing with the same account.



Get started in 4 easy steps

STEP 1

Request a workspace invite from sales@cerby.com

STEP 2

Configure SSO with your Azure Active Directory tenant.

STEP 3

Configure your security policies in Cerby

STEP 4

Add your users and applications

That's it! Cerby starts protecting applications on your behalf, in concert with your Azure Active Directory tenant.

cerby® + Microsoft Azure Active Directory

Cerby is a fast-growing identity security innovator that uses robotic process automation to connect applications that lack support for security standards, like single sign-on, to corporate identity providers. Best known as Unmanageable Applications, Cerby removes the error-prone process of manually managing access and remediates insecure configurations like disabled 2FA. Cerby's patent-pending technology understands Unmanageable Applications in a business context and automatically enforces security best practices before misconfigurations turn into breaches. Cerby is a must-have for teams to protect the brand, stay secure and increase productivity.