Enterprise-Grade Identity Management with Seamless Secure Access

Balancing Access and Security

Modern IT administrators must balance a dichotomy of frictionless access while securing authentication, authorization, and access to more applications, systems, and networks than ever before. A person's individual ability to access every tool they need, without unnecessary barriers is crucial to their productivity. Yet the security of the organization as a whole is paramount, as the brand and, ultimately, their customers' trust is at stake. The secret to balancing these sometimes-conflicting priorities is to secure the core identity of individuals at a directory level, then automate access to every least privileged resource to make work happen across your organization.

Zero Trust, Fully Cloud

The modern security perimeter is anywhere that access happens it's global, fully remote, and multi-device. To some organizations, this can sound challenging, but by embracing a zero-trust mentality, employees and IT organizations can feel empowered and secure. With a cloud-based Directory-as-a-Service™ and a modern MFA and policy engine from Duo, organizations can implement a zero-trust framework, whether you're co-located, spread across multiple offices, or have no offices at all. The integration allows you to balance enterprise-grade identity management with seamless secure access regardless of where or on which devices work is done.

Push to Access Identity

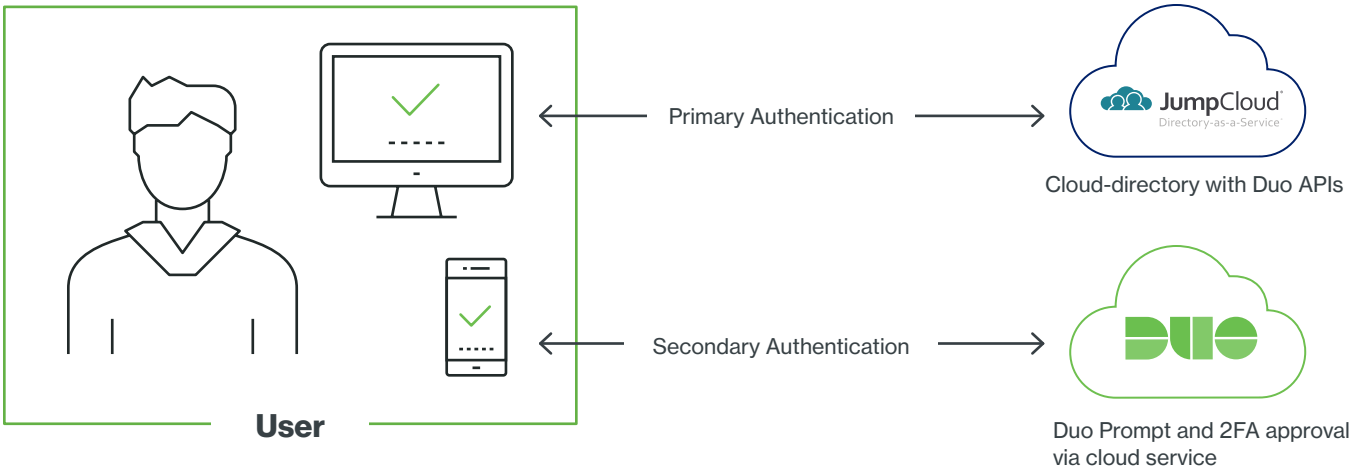
Duo Security's integration into JumpCloud's Directory-as-a-Service, provides a consistent authentication experience for users. Duo offers several authentication methods, including mobile apps, push notifications, offline options, WebAuthn, security keys and more. Customers can choose their preferred authentication methods for JumpCloud that best fit their security strategy. Additionally, when new identities are created, administrators can allow a grace period for new users to enable multi-factor authentication (MFA), force MFA for sensitive applications, and see which users have MFA enabled. Thereby ensuring that only the right people have access to the right resources while protecting the entire organization.

Joint Solution Highlights

+ **Frictionless access to least privileged applications for users**

+ **Grant access remotely and globally with a cloud-based directory**

+ **Full visibility into the uses and devices - and the security hygiene of those devices – accessing applications**



Summary

The integration of Duo and JumpCloud allows IT administrators to balance the dichotomy of seamless user access within a modern security perimeter. The joint solution ensures that only authorized users can access their accounts. The added flexibility of push notification access, alongside the remote visibility from a cloud directory, lets administrators know who in the organization has enabled MFA.

Duo Security is now part of Cisco.

Duo is the worldwide leader in providing Trusted Access for companies of all sizes. Duo Security protects organizations against data breaches by ensuring only legitimate users and trusted devices have access to sensitive data and applications – anytime, anywhere. Duo supports thousands of customers and millions of users in organizations like Accenture, Boston Medical, Emblem Health, Facebook, Twitter, Virginia Tech, Yelp and many others.
Start your free trial at duo.com.

JumpCloud® Directory-as-a-Service® is Active Directory® and LDAP reimagined. JumpCloud securely manages and connects users to their systems, applications, files, and networks. Try JumpCloud free up to 10 users forever, at jumpcloud.com.