JumpCloud's

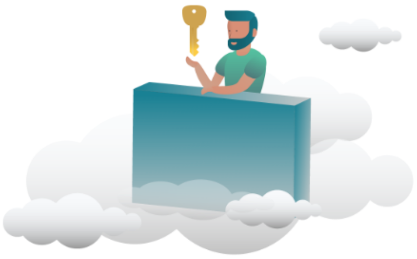
Remote Work Solutions

Technical tips for supporting your remote workforce with Directory-as-a-Service®

VPNs for Remote Employees

VPN Access

Your remote employees can launch a VPN client and connect to your VPN by authenticating with their JumpCloud username and password, the only credentials needed to confirm their identity and access the resources they need, from anywhere they're working. VPNs are a great way to secure network traffic when accessing IT resources, and are necessary if you use a traditional domain environment. With JumpCloud's domainless architecture, your users may not need to use a VPN but can still be secure.



Manage VPN Accounts

VPN access can be managed via JumpCloud's cloud LDAP or RADIUS services. Admins can enable access to the VPN through group membership in JumpCloud, and users can authenticate through their JumpCloud credentials. JumpCloud supports VPNs like Cisco AnyConnect, OpenVPN, and others so you can use your favorite VPN solution. In addition, JumpCloud allows admins to enforce MFA for VPN network access, adding another level of safety for your business.

VPNs with Active Directory

VPNs are practically required infrastructure when using Active Directory (AD) for remote users, but managing user access and accounts from AD can be painful. JumpCloud's AD Integration (ADI) feature provides an easier way to sync and extend AD identities to your VPN (with MFA, if desired) and other non-AD bound IT resources such as web applications, cloud servers, and Mac or Linux devices.

JumpCloud Directory-as-a-Service is an all-in-one user access control and device management platform designed to support a remote workforce. Your first 10 users and systems are free, forever. Discover more at JumpCloud.com.