Whitepaper

jumpcloud

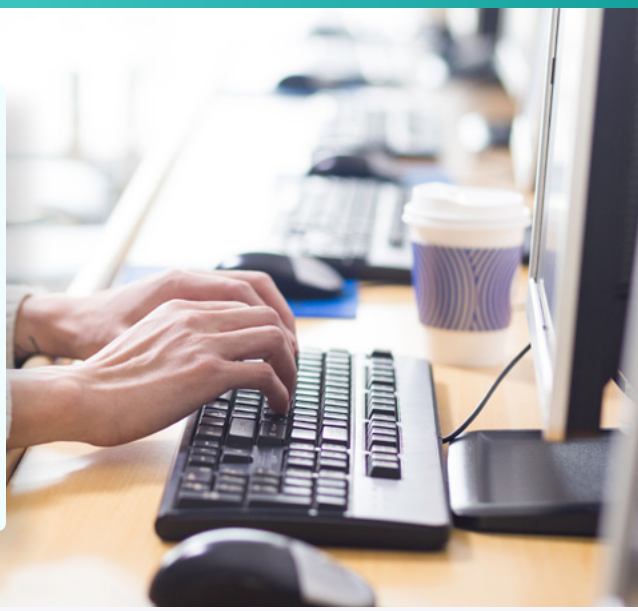
Active Directory and JumpCloud: A Complete IAM Approach

Contents

Version 2 | 版二
www.version-2.com

Maybe you can't picture a world without Microsoft Active Directory. (In fact, you might be thinking something along the lines of, "You can pry my domain controllers out of my cold, dead hands," right now.)

However, you might also seek more elegant ways to extend AD to resources outside the domain. There are ways to make Active Directory do even more for you — like managing Macs and federating identities to web applications — through a single solution.



Active Directory's Position in the Workplace

IT admins value AD because they can customize it thoroughly, tailor it to AD-reliant applications, and build extensive knowledge of the domain. AD also represents significant investments in time, infrastructure, and licensing for their organizations.

Although AD is powerful in connecting to domain-bound resources, it does not connect natively to cloud and non-Microsoft resources, which are proliferating in the modern age of IT and remote work.

This means admins have to maintain "mini" directories — essentially, a directory in each application or on each server — and each of them require manual access management. Managing more than one directory (and more than one set of identities per employee) and a collection of third-party services and SSO tools is inefficient and insecure.

Cybersecurity research indicates identity and access management (IAM) is critical to organizational security, and the digital identity is at its core.

A Unified Solution: Active Directory Integration

JumpCloud is a cloud directory platform that unifies IAM across virtually all the resources employees need to do their work, whether remote or in the office. This includes multi-OS devices (including Windows, Mac and Linux), SSO to cloud applications using SAML LDAP and other secure protocols, RADIUS for secure VPN and network access, and more.

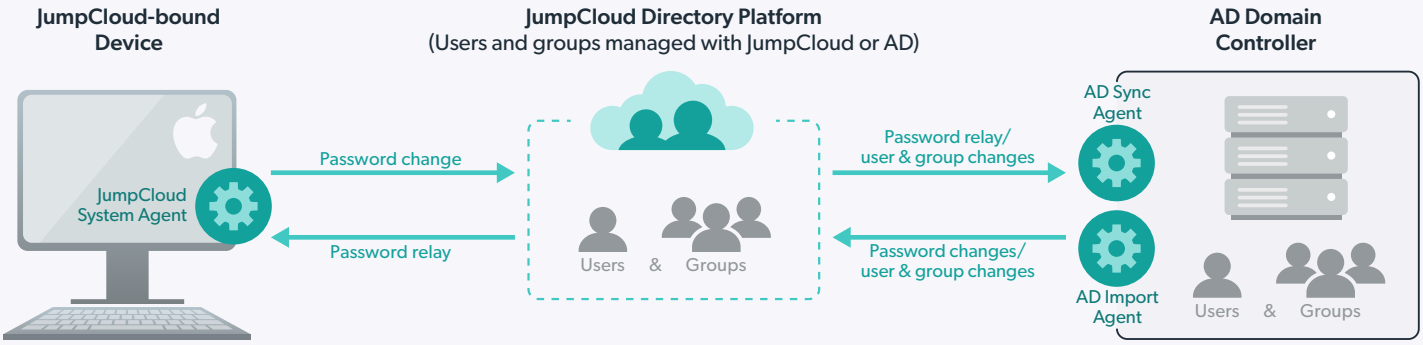
JumpCloud features **Active Directory Integration**, through which AD remains the authoritative source of identity, and JumpCloud increases AD's value and utility by serving as a conduit to the resources that have historically challenged admins.

With Active Directory Integration, admins can eliminate other third-party IAM services and federate core AD identities to virtually all resources, including systems, applications, files, and networks.

Let's explore how JumpCloud interacts with AD.

> **"The core objective of IAM systems is one digital identity per individual.**[1]
>
> *— Laura M. Hars*

How JumpCloud's Active Directory Integration Works



JumpCloud enables tight integration and bi-directional syncing between AD and JumpCloud. Using Active Directory Integration, admins can bring information from AD into JumpCloud and send information from JumpCloud back to AD, including user and group attributes.

The transmission of information between AD and JumpCloud uses lightweight agents, which enable routine syncs. Admins download the agents through the JumpCloud Admin Portal, save and configure them in AD, select which users and groups to sync, and let JumpCloud work in the background. (Learn more about the details of this process in our **AD Integration documentation**.)

Through the JumpCloud Admin Portal, admins can provision AD users to macOS and Linux systems, web applications, file servers, WiFi networks, and more.

They can create users in JumpCloud and provision those new users to AD automatically, as well as control user state through either platform. For example, they can specify that users suspended in JumpCloud are automatically disabled in AD, too.

In essence, admins can leave AD in place, wrap JumpCloud around it, and extend identities anywhere they're needed via JumpCloud's LDAP, RADIUS, and SAML protocols. Further, IT admins can start to control and manage their ongoing AD tasks from JumpCloud, with the potential to manage only one IAM platform, but also keep AD intact for their Windows-based resources. Admins then have centralized control over their IAM infrastructure from AD and/or potentially from JumpCloud.

AD Integration Use Cases

The following three scenarios illustrate some of the ways our Active Directory Integration can help optimize and centralize an organization's IT environment.

1

Scenario 1: Bind Mac Systems to AD

Let's take an example organization, Company A. Company A has 100 employees, 10 of whom asked for Mac systems. In the past, Company A's sysadmin struggled to bind those systems to the domain.

After configuring Active Directory Integration, the sysadmin can log in to the JumpCloud Admin Portal, establish a group of Mac users, and create local accounts for those users on each of their machines using their AD identities. Admins can enable multi-factor authentication, too, so those users access their machines with a second factor like TOTP, Push notification, or even biometrics for an added layer of security.

The sysadmin can select **GPO-like functions** to do everything from enabling FileVault 2 full disk encryption to requiring **lock screens** after one minute of inactivity on each of the machines at once. Users enter their AD credentials (and second factor, where required) to access their machines, the company's WiFi network, and their authorized applications like Salesforce.

2

Scenario 2: User Password Changes

At Company B, the sysadmin has been swamped with password tickets and trying to manage multiple identities for each employee.

After configuring Active Directory Integration, users can change their own passwords through their JumpCloud User Portals or, for Mac users, through the **JumpCloud Mac app** nested in their own toolbars. Those passwords are written back to AD automatically and extended elsewhere as appropriate.

3

Scenario 3: Sync with Google Workspace and Microsoft 365

At Company C, the sysadmin has been searching for a way to streamline the process of syncing his AD and Google Workspace (or Microsoft 365) instances, rather than managing them separately or setting up syncing solutions such as Google Cloud Directory Sync (or Azure Active Directory Connect in the case of M365).

After configuring Active Directory Integration, an admin can sync AD with Google Workspace (or M365) accounts to create one authoritative identity for each user to access both AD-bound resources and their online productivity suites.

They don't need to use GCDS or AD Connect to do so because Active Directory Integration acts as a comprehensive tool. Another interesting benefit is that, by using JumpCloud, an organization can leverage both G Suite and M365 with one set of login credentials per user and a single pane of glass for management.

Features & Benefits Overview

At its core, Active Directory Integration enables a centralized and secure approach to IAM by ensuring each user accesses virtually all their resources with one secure authoritative identity.

This approach benefits both admins and users, and here we've detailed some of the ways JumpCloud enhances AD's functionality.

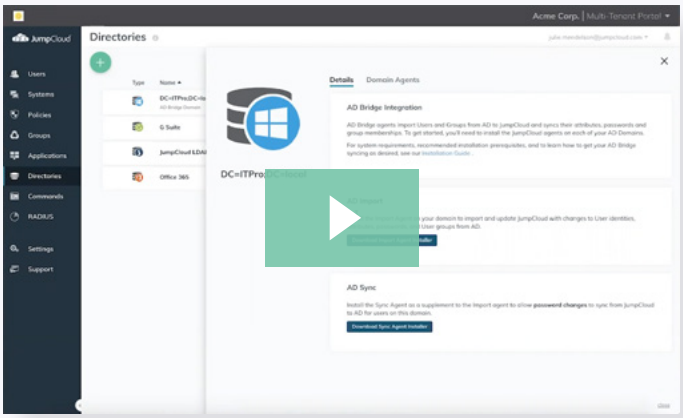
Feature	Active Directory	Active Directory with JumpCloud
Native Connection to Web Apps (SAML)	—	✓
System Endpoint Management for Windows	✓	✓
System Endpoint Management for macOS	—	✓
System Endpoint Management for Linux	—	✓
PowerShell	✓	✓
GPO Functions for Windows	✓	✓
GPO-Like Functions for macOS and Linux	—	✓
RADIUS Functionality	✓	✓
LDAP Functionality	✓	✓
Integration with AWS	—	✓
MFA for Mac, Linux, Windows, apps, etc.	—	✓

Testing JumpCloud

Now that you've read about the Active Directory Integration feature, give it a try yourself. We recommend working in a test environment: You can spin up a virtual domain controller to do so.

Otherwise, you can simply launch a **JumpCloud Free** account and learn more about the interface and features. Although you won't see the sync in action — you'll need an AD server either in a test lab or production for that — you'll still get a feel for what the platform offers you.

Before you take either of these steps, we recommend you start with this seven-minute tutorial video with one of our product managers to get an overview of Active Directory Integration and its setup.



The Active Directory Integration tutorial

1. Hars, Laura M. "Understanding Identity and Access Management as a Cybersecurity Construct." **Cybersecurity in the Digital Age**, edited by Gregory Garrett, 151 – 152. Illinois: Wolters Kluwer, 2019.