jumpcloud™

# 2023 Year in Review: JumpCloud for MSPs

JumpCloud for MSPs provides everything your MSP needs in one open directory platform. It offers a comprehensive stack of security and productivity solutions that allow you to manage diverse client environments while centralizing core workflows with deep integrations to the tools you already use. Adopt a Zero Trust framework internally and across your customer base via passwordless authentication, multi-factor authentication (MFA) everywhere, and conditional policies.

In 2023, we headed into the year with the goal of enabling our partners to take on additional clients without the need to hire additional staff or acquire new tooling to secure new environments. We did this by streamlining the identity management lifecycle, extending access control and security to more resources, and deepening our investment in device management and patching to help our partners better protect identities wherever they reside and make compliance and reporting more turnkey for all client types.

## 2023 At-a-Glance

**FEBRUARY**

**New Users Page in the Multi-Tenant Portal**
See all users in one place and **take quick action** across all orgs from that view.

**APRIL**

**Password Manager 2.0**
**Keep passwords secure** with compliance and usability enhancements.

**MAY**

**Google Workspace Partnership**
Use **Google Workspace identities** with JumpCloud to manage access and devices.

**View & Action Users & Devices in MTP**
Perform **critical actions** directly from the MTP, saving time and clicks.

**JUNE**

**Android EMM**
JumpCloud now supports Android device management at **no additional cost**.

**Enhancements to Bulk Actions in MTP**
Add new users, export user lists, add new devices, and unlock, suspend, and reset passwords **in bulk**.

**JULY**

**Windows MDM**
More easily **onboard Windows 10/11** devices.

**SEPTEMBER**

**Ad Hoc Commands on Devices from MTP**
Quickly **run commands** and **troubleshoot issues** without having to navigate to each org's portal.

**OCTOBER**

**JumpCloud Go™**
Integrated, cross-platform, **phishing-resistant** authentication.

**NOVEMBER**

**Organization Cloning on the MTP**
**Standardize tenant creation** and quickly set up new clients.

# Multi-Tenant Portal Updates

JumpCloud's **Multi-Tenant Portal** (MTP) enables technicians to customize their homepage view and widgets with actionable information. It's easier than ever to take actions on endpoints and users without having to navigate into every organization's portal. Create new organizations based upon your standard client configurations or clone similar organizations. Take on new clients using Google Workspace, Mac devices, or Microsoft-centric environments, and manage them the same way via a single pane of glass.

## MTP Homepage Widgets: MDM & Reporting

These new features help you keep track of upcoming certificate expirations and receive alerts when a report is ready for download across all of your organizations. As a result, you can spend more time adding value for your clients and less time on unplanned system maintenance.

## Organization Cloning on the MTP

MSPs with multiple tenants can standardize their tenant creation process and quickly set up a new tenant with the settings, commands, policies, user and device groups, and more for a new client.

This reduces the time it takes to set up a tenant for an incoming client and minimizes mistakes that can crop up when setting up new organizations.

## New Users Page in the MTP

MSP admins can see all users through a single pane of glass in the MTP and take quick action across all orgs from there.

## SyncroMSP PSA Ticketing

Stay informed of customers' product usage, and get alerted to high-priority actionable incidents.

## View and Action Users & Devices in MTP

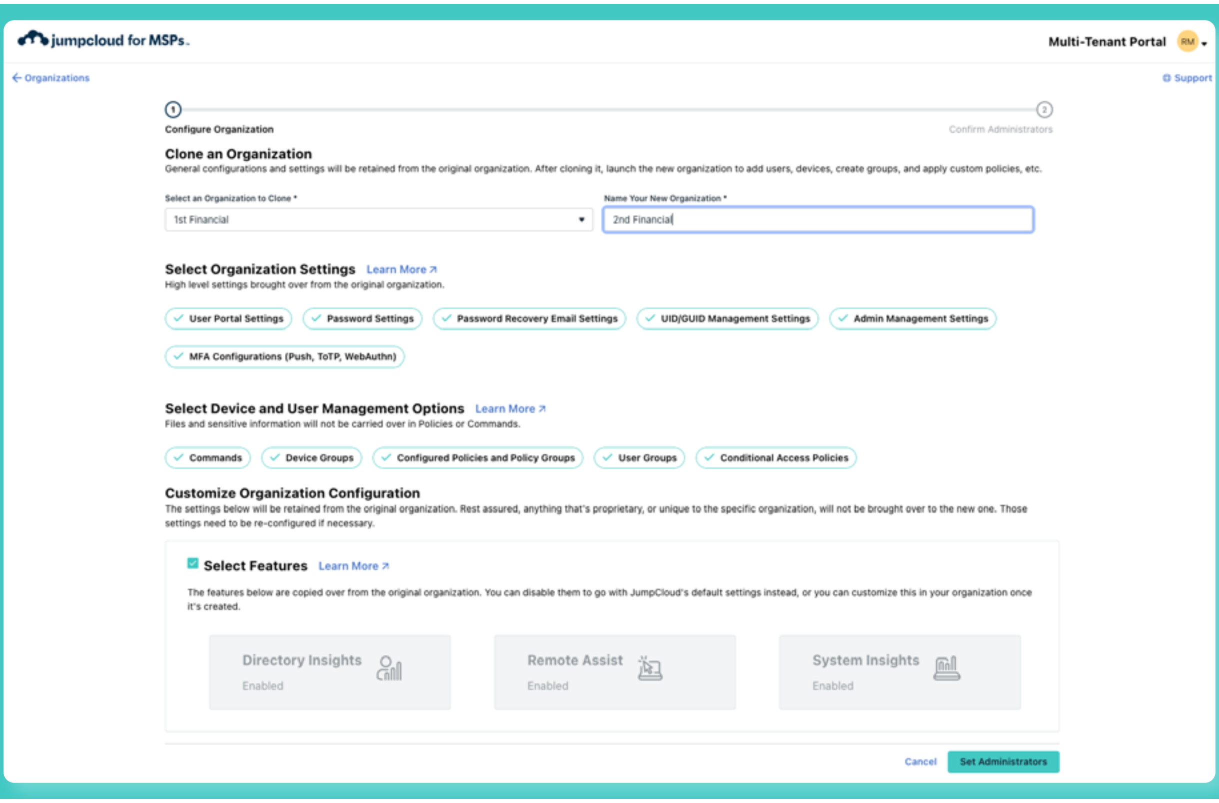
MSPs can perform critical actions directly from the MTP, saving them time — and clicks — to support clients effectively.

## Enhancements to Bulk Actions in MTP

MSP admins can add new users, export user lists, add new devices, and unlock, suspend, and reset passwords in bulk directly from the MTP. This release streamlines admins' workflows and offers easier data viewing.

## Ad Hoc Commands on Devices from MTP

Admins can take direct action to quickly run commands and troubleshoot issues without having to navigate to each org's portal and perform all the additional steps to run a command there. This saves time and effort, and focuses admins in the MTP to reduce confusion and opportunities for human error.



Clone an Organization

General configurations and settings will be retained from the original organization. After cloning it, launch the new organization to add users, devices, create groups, and apply custom policies, etc.

Select an Organization to Clone *: 1st Financial

Name Your New Organization *: 2nd Financial

Select Organization Settings Learn More ↗

High level settings brought over from the original organization.

✓ User Portal Settings ✓ Password Settings ✓ Password Recovery Email Settings ✓ UID/GUID Management Settings ✓ Admin Management Settings ✓ MFA Configurations (Push, ToTP, WebAuthn)

Select Device and User Management Options Learn More ↗

Files and sensitive information will not be carried over in Policies or Commands.

✓ Commands ✓ Device Groups ✓ Configured Policies and Policy Groups ✓ User Groups ✓ Conditional Access Policies

Customize Organization Configuration

The settings below will be retained from the original organization. Rest assured, anything that's proprietary, or unique to the specific organization, will not be brought over to the new one. Those settings need to be re-configured if necessary.

☑ Select Features Learn More ↗

The features below are copied over from the original organization. You can disable them to go with JumpCloud's default settings instead, or you can customize this in your organization once it's created.

Directory Insights: Enabled

Remote Assist: Enabled

System Insights: Enabled

# Identity

JumpCloud has made managing identities even easier by breaking down the barrier between human resources and IT, lowering overhead and making it easier to **automate group memberships**.

## Dynamic Groups

Dynamic Groups make it possible to manage user and device groups' membership via rules based on automation using commonly leveraged attributes and operators. Once dynamic groups have been configured, admins can unlock the power of automation around many of their day-to-day tasks, from user onboarding to device hardening and more, saving time for bigger, more strategic work.

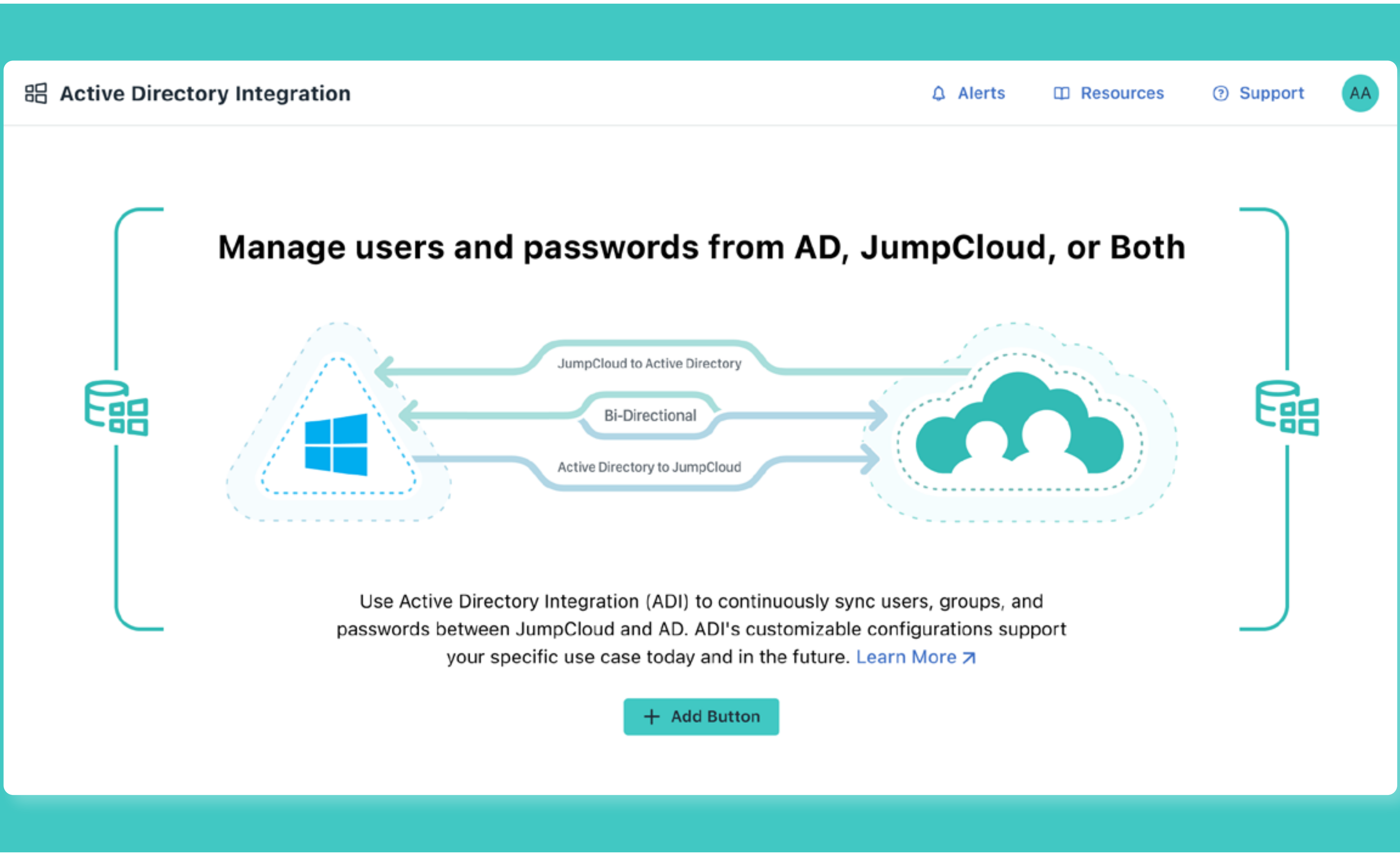
## Automatic Sync Support for New Directories

Organizations using external directories that aren't in our catalog can create new integrations that automatically sync user data into JumpCloud.

## Active Directory Integration (ADI)

ADI agents are installable on member servers when JumpCloud is the password authority and can sync multiple domains. Fewer agents will need to be managed and the requirement to install the agent on all domain controllers is removed in certain cases. Organizations that are required to maintain local authentication stores for compliance purposes can deploy ADI using a pass-through authentication model versus bidirectional syncing.

MSPs have much more flexibility with their domain configurations and user management. Choose from three possible configurations: 1) no domains, 2) one or more domains, no default domain, or 3) a list of one or more domains with one default domain. This update gives MSPs greater flexibility to extend their AD environments to the cloud, manage their clients' users and groups in AD or JumpCloud, and help with migration.


Active Directory Integration
Alerts
Resources
Support
AA
JumpCloud to Active Directory
Bi-Directional
Active Directory to JumpCloud
+ Add Button

Manage users and passwords from AD, JumpCloud, or Both

Use Active Directory Integration (ADI) to continuously sync users, groups, and passwords between JumpCloud and AD. ADI's customizable configurations support your specific use case today and in the future. Learn More ↗

# Access

JumpCloud can be your identity provider (IdP) or extend to your existing IdP. The open directory platform uniquely integrates identity and access management (IAM) with UEM.

## Enhancements to MFA

### Push Bombing Mitigation

Limit the number of push MFA user attempts for a resource or endpoint to increase cybersecurity.

### Improved MFA Approval Workflow for End Users

Users can confirm an MFA push notification directly on their mobile device lock screen without opening the app directly, while still using a biometric check (if required) through Face ID/fingerprint/passcode before the Accept/Deny is accepted.

### New Conditional Access Policy – Disk Encryption Enabled

An administrator can block access to SSO applications from managed devices where disk encryption isn't enabled.

## JumpCloud Admin Mobile App for iOS & Android

A new JumpCloud Admin mobile app helps admins resolve issues on the go.

## JumpCloud Go™ | Phishing-Resistant Passwordless Login

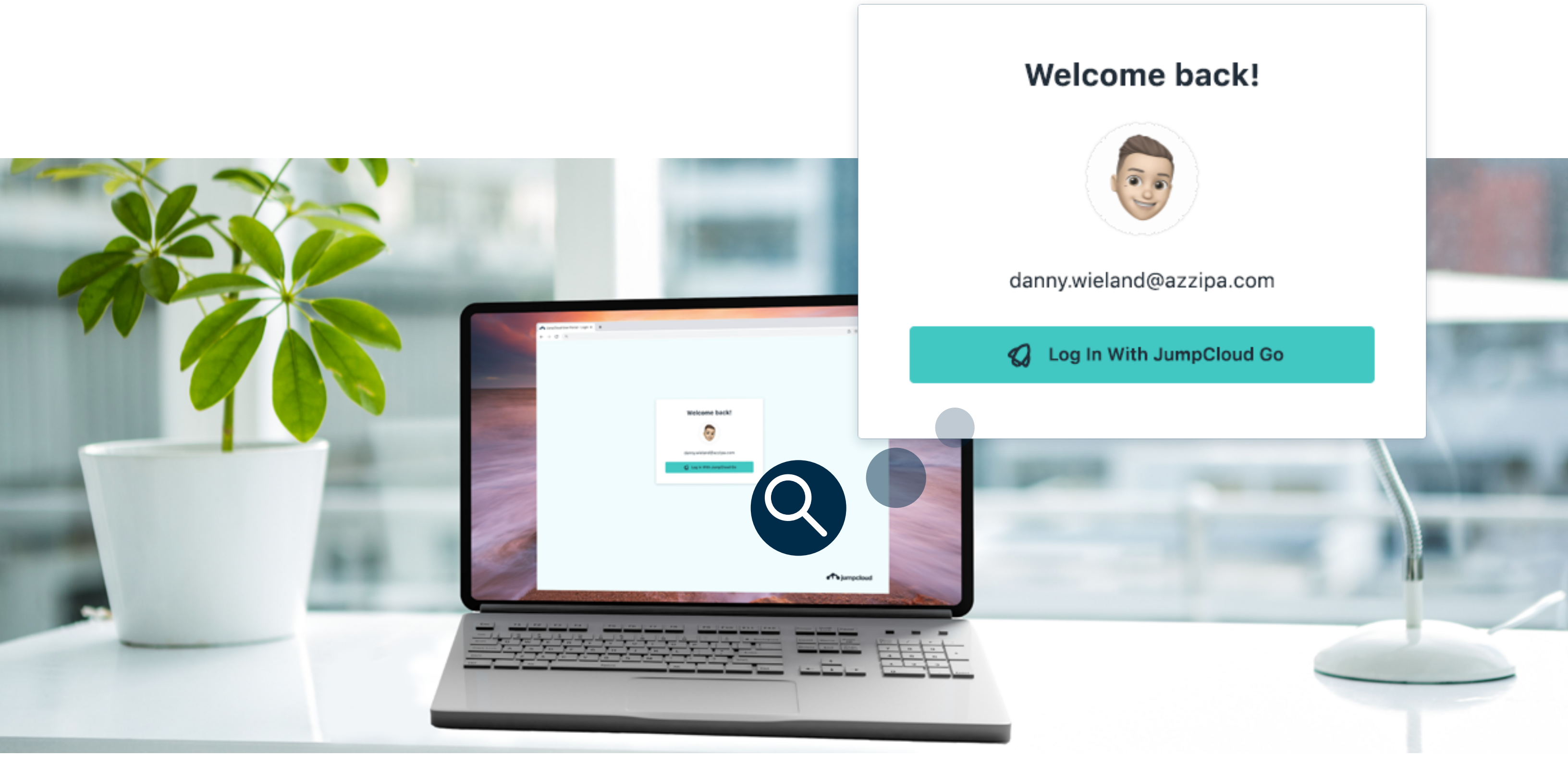
The repeated need for MFA can wear on end users, making it challenging to find the right balance of robust security and usability.

JumpCloud Go delivers an integrated, cross-platform, phishing-resistant, and hardware-backed authentication that verifies a managed user on a managed device to enable secure, frictionless access.

JumpCloud Go combines technologies like Apple's Touch ID and Windows Hello to create another layer of user verification that's more secure than traditional MFA methods.

## Application Creation Workflow

A new guided workflow will assist you when creating an application integration. JumpCloud can now authenticate to service providers whose SAML integration requires multiple internal and external ACS URLs, or uses geographically distributed URLs.



Welcome back!

danny.wieland@azzipa.com

# Devices

JumpCloud now provides UEM with the inclusion of comprehensive Android EMM and Windows WDM. This brings access control closer to your assets to provide a Zero Trust security model.

## Remote Access

JumpCloud Remote Access facilitates **remote tech support** by allowing admins to control a user's device, regardless of their location. It's received many enhancements this year:

### Remote Access Clipboard Sync and macOS Permissions Prompt

Continuous improvements were made to Remote Access including clipboard syncing, multi-monitor support, macOS permission prompts, and an uninstall/install toggle.

### Remote Access for Linux

Remote Access is now supported for popular Linux desktop distributions including Ubuntu, Debian, Mint, and Rocky.

### Users Can Join Remote Access Session

Remote Assist added the option for end users to join a session and share their screens by only accepting a consent prompt. Admins can now initiate a remote support session without the end user needing to be present. With Silent Assist (Unattended Access), admins can launch a remote session from the JumpCloud Admin portal and connect to users' devices directly, reducing the time to issue resolution.

### Background Access: Remote Command Line + Remote File Transfer

JumpCloud provides a remote command line and file transfer solution that allows admins to support devices without interrupting the user.

## Self-Service Account Provisioning

Self-Service Account Provisioning lets users bind their JumpCloud account to managed macOS and Windows devices directly from the login window. This feature also enables the new macOS login window with wireless connectivity controls.

Self-service account provisioning supports federated user identities when accessing JumpCloud-managed devices to enhance your onboarding workflow.

## Improved Communication Around Expiry Events

You will now receive improved communications when expiry events occur throughout your instance. This can include expirations of MDM, SSO, and EntraID certificates or tokens, as well as expiring or invalid M365, Azure AD/EntraID Cloud Directory Sync tokens. You can be more responsive without the burden of checking (and remembering) certificate and token statuses individually.

## Android EMM

JumpCloud's EMM offering makes all Android device types available for management, and is included at no additional cost. Pre-built policies offer more rapid deployments.

### Fully Managed & Dedicated Devices

JumpCloud's EMM offering makes all Android device types available for management including support for fully managed and dedicated Android devices. In addition to new policies that help admins control those device types, such as Kiosk Mode, Factory Reset, and Software Updates.

## Windows MDM

This update enables MSPs to easily onboard Windows 10/11 devices for their end users, leveraging the capabilities of the industry-trusted and standardized Windows MDM protocol. We recommend enabling the auto-enrollment toggle feature to migrate agent-managed devices. Upcoming feature: Admins will have a new, streamlined method for provisioning Windows 10 and 11 devices using a provisioning package.

## MacOS

### Mac MDM Software Update Commands

JumpCloud can now deliver MDM commands to managed macOS devices to better manage updates to help you address zero-day security threats.

### MacOS Patch Management Major OS Upgrade Support

Admins can easily enforce "fire and forget" settings for minor updates and major upgrades in addition to day zero support for iOS and iPadOS 17 and macOS Sonoma.

## Run Ad Hoc Commands

Admins can now run ad hoc commands on their systems for tasks that are rarely repeated.

# Security and Compliance

## JumpCloud Policy Group Template Gallery

Templates help JumpCloud admins to establish baselines for device settings and compliance right out of the box.

## Enrollment Commands

Customize your new device experience using enrollment commands. JumpCloud now delivers enrollment commands on macOS, Linux, and Windows devices so you can easily ensure commands run on any device added to JumpCloud. This automates your workloads, improves onboarding experiences, and strengthens device posture.

## Remote Access Install/Uninstall Toggle

Admins can now easily install or uninstall JumpCloud's Remote assist app on all devices with a single toggle in the admin console.

## New PowerShell Function: Get-JCSystemApp

A new JumpCloud PowerShell Module helps admins easily gather information on what software (and which version of it) is on their systems to help guide your clients through compliance audits. You can filter by systemID, systemOS, softwareName, and softwareVersion.

## JumpCloud Password Manager 2.0

Last year, we launched a **decentralized password manager and vault** to protect and manage passwords across your organization. We've spent 2023 making it even better.

### Compliance and Usability

JumpCloud Password Manager 2.0 builds on that foundation and offers features that make it possible to reset user PINs in the desktop application, view password histories, and enroll existing accounts in two-factor authentication. Users can assign user groups to shared folders on the desktop app.

Technicians now have even more visibility into the overall health and security of users' passwords. This provides password protection and assurance that users are using high quality passphrases. See info on password complexity, age, repeated use, and shared status via the dashboard widgets and Directory Insights.

### Password Manager Cloud Backup

Cloud Backup minimizes the chance of data loss, especially in the case of a lost device.

## Get More Out of JumpCloud

### New Advanced Certification for JumpCloud

Dive even deeper into JumpCloud's capabilities with a **new certification** that will empower you to do more with the platform than ever before.