

2022 Year in Review: MSP Edition

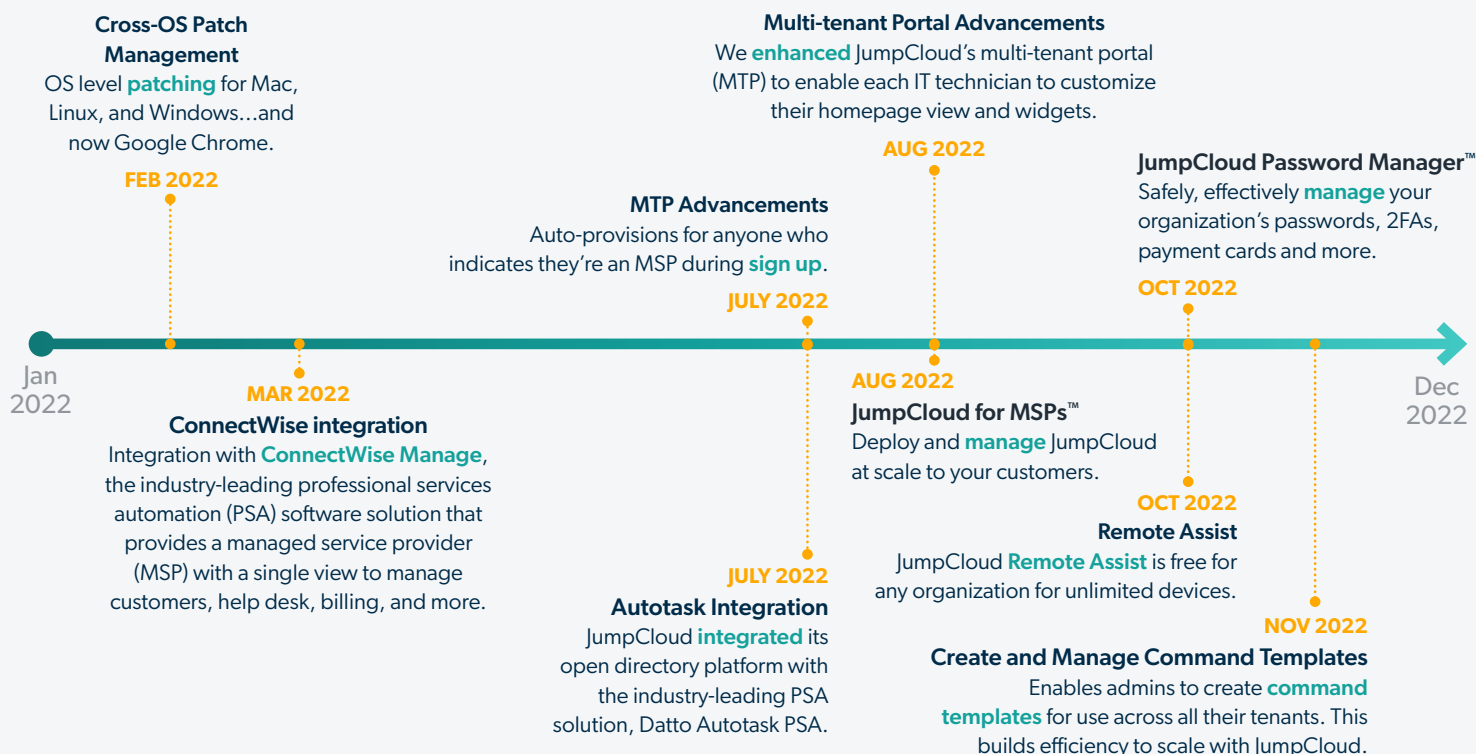
Welcome to JumpCloud for MSPs™

JumpCloud for MSPs is here.

Fill in the gaps in your stack — without having to rip and replace any solution you’re already using. It’s a powerful Open Directory Platform that allows you to centrally manage identity, access, and device capabilities in a single, multi-tenant console. These features combine with a partner program that provides implementation, marketing, and sales support. Other enhancements enable you to be proactive, become your clients’ most trusted advisor, and establish identity as their new perimeter. This focus makes it possible for clients to securely access resources and unify access control while staying ahead of security threats and compliance regulations.

This year, our strategy was to add more depth and value to our open directory platform; streamlining the identity management lifecycle, extending access control and security to more resources, and investing in device management and patching to help you better protect identities wherever they reside and make compliance and reporting more turnkey for clients.

2022 At-a-Glance



JumpCloud for MSPs™ is built with your business in mind. In addition to all of the features that the JumpCloud platform offers, our partners now have access to the below features:

- Multi-tenant admin console
- Single pane of glass alerting dashboard
- PSA billing and ticketing integrations
- Bulk license purchasing and management
- Centralized invoicing

Everything Your MSP Needs in One Open Directory Platform

JumpCloud for MSPs provides MSPs an open directory platform for delivering modern IT services that are identity-centric, cloud native, and vendor agnostic. Using JumpCloud, MSPs can centralize identity, access, and device management capabilities under a single Multi-Tenant Portal.

Unified: A single platform that manages identity, access, and devices in the cloud, without having to rip and replace any platforms you already have in place.

Integrated: Deep integrations with directory platforms, PSAs, and HR systems enable you to manage your users and devices from within the JumpCloud console.

Secure: Centralizing identity, access, and device management capabilities under one umbrella reduces complexity and allows you to lower security risk by making it easier for your team and your clients to be productive.

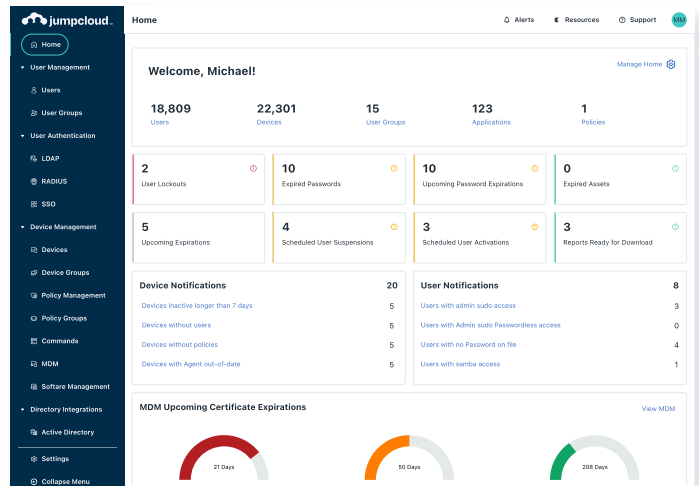
Multi-Tenant Portal Updates

JumpCloud's **purpose-built multi-tenant portal** (MTP) enables every technician to customize their homepage view and widgets with actionable information. Targeted alerts and notifications surface problems that should be attended to immediately, so it's no longer necessary to wait for support requests to escalate before acting. The workflow is: alert, investigate, and remediate.

It's easier than ever for MSPs to try JumpCloud. The MTP will auto-provision for anyone who indicates they're an MSP when they sign up, without requiring any other applications.

Single Pane of Glass for Alerting

The JumpCloud multi-tenant admin console provides an alerts dashboard that centralizes a growing list of alerts, giving real-time visibility into your clients' environments.



Unify identity, access, and device management in the JumpCloud for MSPs admin console.

This includes:

- User alerts (lockouts, expired passwords, about to expire passwords)
- Device alerts (inactive more than 7 days, uptime greater than 30 days, disk encryption)
- Software alerts (install failed, software not found, restricted software found, app not used in 30 days)
- Security vulnerabilities (OS patch management, MFA enabled, antivirus software)

Integrated Billing and Ticketing

Integrate your billing and ticketing systems to accurately manage licensing for your clients and generate. JumpCloud expanded its **MSP program** with ConnectWise integration. This simplifies administrative tasks by automating account management between ConnectWise Manage and JumpCloud accounts, enabling an automated process for client billing that reduces the time needed to update ConnectWise information while increasing the service provider's confidence in the accuracy of billable items. We also Integrated with Autotask PSA to streamline client management and billing operations.

Simplified Licensing Control

Bulk license purchasing with user-based allocation and capping for each client, directly from the Multi-Tenant Portal.

Command Templates

MTP admins can create and **manage command templates** from any of their tenant organizations. We allow our admins who manage multiple tenants create command templates they want to use across all their tenants. This builds efficiency and allows them to scale with JumpCloud.

Identity

Onboarding users and identity lifecycle management can be time consuming and the possibility of introducing errors while provisioning users is a security risk. JumpCloud has made managing identities easier by breaking down the barrier between human resources and IT, which lowers management overhead and makes it easier for IT admins to automate group memberships.

Identity Lifecycle and Maintenance

Admins can now **schedule activation** for a staged user's start date. The scheduled event can be configured to send an activation email, which permits the user to set their own password and finish their onboarding. Likewise, scheduled suspension is also available to off-board users. You may enable a recovery email address to be used when users need to reset their passwords.

You can now enroll company-owned iOS, iPadOS, and tvOS devices in Mobile Device Management (MDM) using Apple's Automated Device Enrollment and zero-touch onboarding.

HRIS Integrations

JumpCloud introduced more, and deeper, integration options with **HRIS platforms**, through native integrations or using a generic **REST API** integration connector. The connector allows you to integrate with applications that have a REST API and support token-based (API Key or Bearer token) authentication, which includes solutions including BambooHR, APD, BreatheHR, Personio, and SaplingHR.

Access

JumpCloud enables access to more resources, more securely, than other directories. The open directory platform integrates IAM with device management, making possible to introduce new and more powerful conditional access policies available to authentication privilege users.

OIDC and OAUTH Support

More applications are accessible with the addition of **OAUTH and OIDC** protocol support, providing robust and lightweight options for SSO with custom and mobile apps. MFA is now environment wide, including Push and TOTP configuration options for RADIUS and LDAP.

Delegated Authentication for RADIUS

JumpCloud made it possible to bring your own identity from other directories for **delegated authentication** into RADIUS resources, extending access control to VPNs and the network.

Automated Group Management

Group management is **becoming fully automated**, providing more mature entitlements management without the hassle of maintaining role-based access. IT admins can choose to be prompted about recommended changes or configure automatic attribute-based access control.

Device Management

Advancements in device management capabilities spanned the gamut of operating systems and the unique systems and software that manage them. Cross-OS device management helps MSPs to manage the whole environment while preventing data loss by protecting identities.

Cross-OS Patch Management

This year saw the introduction of **patch management policies** for Windows, Mac, and Linux Devices. With them, visibility and clarity to the current state of device operating systems (OS), browsers, and applications is easier than ever, with tools to automate patch deployment so devices are up-to-date and secure.

In addition to these capabilities, admins can seamlessly manage cross platform patch policies using automated OS Patch Policy default groups built around a deployment ring implementation model. Each OS Patch Policy default group is configured with best practice defaults, one for macOS, one for Windows, and one for **Linux** (Ubuntu).

JumpCloud also delivered a Google Chrome **Universal Browser Patch Management policy**. A universal policy saves you time by automatically scheduling and enforcing security patches on managed devices in bulk. This addresses rising zero day vulnerability risks.

Remote Assist

JumpCloud **Remote Assist** facilitates remote tech support by allowing technicians to remotely see and control a user's device, regardless of their location, and free of charge. This avoids IT tool sprawl, and limits unauthorized solutions, even within your organization.

Windows | Better Cohesion with AD/AAD Environments

JumpCloud now supports **integrating with Windows Server**, and delivers deeper functionality to patch and onboard your devices. We also extended cross-OS support with the ability to coexist with Windows domain controllers and Active Directory. A commands queue was made available to admins who want to review and manage their **in-flight commands** as they await execution, tailoring their effect.

If your organization has on-prem Active Directory (AD) or Azure Active Directory (AAD) joined Windows devices, you can install the JumpCloud agent on those devices and bring them into your JumpCloud dashboard. JumpCloud is also adding self-service Windows deployments to streamline user onboarding in support of remote work and time-savings.

Macs | Expansion of Supported Devices and Programs

As 2022 began, support for iOS and iPadOS had just debuted. Throughout the year more support came to automate device enrollment for these devices, where all company-owned iOS, iPadOS, and tvOS devices purchased from Apple or supported retailers can be enrolled in JumpCloud's MDM during Setup Assistant and take advantage of the same zero-touch deployment experience.

IT admins can now remotely add and assign **Volume Purchase Plan (VPP)** applications to iOS and iPadOS devices or device groups, previously just available for macOS. New policies that pre-approve certain permissions, extensions, and more help your Apple apps work efficiently and securely with less user intervention. And as new releases come to life, like the recent macOS 13 Ventura major release, JumpCloud is ready with release day support and pre-built policies to delay installation.



CrowdStrike awarded JumpCloud its **2022 Ecosystem Emerging Partner of the Year**

award in recognition of providing “innovative security solutions and services to customers.”

JumpCloud is now available through the CrowdStrike Store to help secure identities.

Security and Compliance

It's easier to support one solution. Having one centralized platform to deploy policies, manage reporting, and (easily) train technicians on helps to improve efficiency and ultimately, margins.

JumpCloud Password Manager™

A decentralized **password manager** and vault to protect and manage passwords across your organization. It also brings apps that cannot participate in an SSO or other automated authentication process into a unified scenario that makes the user experience easier and more consistent regardless of how they need to authenticate. It plays an active role in protecting your organization from malicious actors.

Enhanced Security Posture

Through platform expansions, partnerships, and integrations, JumpCloud's open directory platform pushed its ability to secure access in dynamic ways, including:

- **Expanded conditional access rules** that consider device state such as encryption and compliance with patching.
- JumpCloud is working with CrowdStrike and Sentinel One for Extended Detection and Response (XDR) integration to secure your identities even further.

Windows BitLocker

Major new investments into **BitLocker deployments**, including visibility into TPM presence and device state to support audit cases and simply troubleshooting. We added recovery key escrow for lockout use cases and extended policy support to all system volumes.

Robust, Proactive Apple MDM

Day-0 **readiness for macOS Ventura** and policies to block the manual installation of profiles, set a device name, and establish an enterprise Wi-Fi policy deepened Apple support. These updates include the ability to make tightly controlled supervised iOS devices, and new policies for macOS around key management tool areas, like system extensions, kernel extensions, and privacy preferences.

Linux Compliance

An extended collection of pre-built Linux **compliance policies** to blacklist services, manage full disk encryption, and a secure boot policy.

Cloud Insights

We previewed this new tool for observability and **monitoring cloud infrastructures**. It makes compliance and data forensics easier for SMEs and helps to enforce least privilege. The initial release focuses on Amazon Web Services (AWS); support for Google Cloud (GCP) will be introduced next year to offer governance and compliance for clients' multi-cloud strategies.

JumpCloud Reports

is the capability for IT Admins to pull essential data from the JumpCloud platform in pre-defined and aggregated lists in order to help meet compliance, troubleshoot issues, assess governance, evaluate security posture, and more. It now includes a stored reports queue for comparative historical analysis. The **pre-built reports** added in 2022 are:

- OS Patch Compliance Report
- Stored Reports Queue
- Users to SSO
- OS Patch Management Status
- Browser Patch Management Status

Growth and Accolades

Awards

ChannelPro Readers Choice Award - Bronze - Best Cloud Management Vendor



JumpCloud is critical for our clients, and the JumpCloud roadmap is very much aligned with a managed service provider and what I'm trying to do as an MSP.

— Antonio Wint, Founder and CEO, Syn Ack Fin

CrowdStrike awarded JumpCloud its 2022 Ecosystem Emerging Partner of the Year award in recognition of providing “innovative security solutions and services to customers.” JumpCloud is now available through the CrowdStrike Store to help secure identities.

Each year, the **Cybersecurity Excellence Awards** identifies individuals and companies that demonstrate “excellence, innovation and leadership in information security,” and awards them across numerous categories including company, product and services, professionals, and industry solutions. Owing to the strength of its nomination, and the popular vote of the members of the Information Security Committee, JumpCloud has been awarded three gold medals in the following categories:

- **Multi-Factor Authentication**
- **Secure Remote Access**
- **Policy and User Management**

JumpCloud for MSPs™ provides MSPs an Open Directory Platform for delivering modern IT services that are identity-centric, cloud native, and vendor agnostic. Using JumpCloud, MSPs can centralize identity, access and device management capabilities under a single Multi-Tenant Portal. To learn more, please visit jumpcloud.com/msp.

JumpCloud® helps IT teams **Make Work Happen®** by centralizing management of user identities and devices, enabling small and medium-sized enterprises to adopt Zero Trust security models. JumpCloud® has a global user base of more than 180,000 organizations, with more than 5,000 paying customers including Cars.com, GoFundMe, Grab, ClassPass, Uplight, Beyond Finance, and Foursquare. JumpCloud has raised over \$400M from world-class investors including Sapphire Ventures, General Atlantic, Sands Capital, Atlassian, and CrowdStrike.



Try JumpCloud Free →