

Automating Device Security and Management with JumpCloud and MDM Solutions



By: Joy Dada





Scenario:

BloomingTech Services, a rapidly expanding tech startup, faces the challenge of Expanding their IT infrastructure securely and efficiently.



Our mission: As IT professionals is to leverage JumpCloud in transforming their IT landscape, ensuring scalability and security as they evolve from a startup to a industry leader.



Securing and Streamlining Operations: The Three Phases of Device Management

01

Core Components for Enhanced Security

- Jumpcloud for device/user management
- MDM for device enrollment & policy
- User management for authentication
- Chocolatey for software deployment

02

Demonstrating JumpCloud in Action

- User and Device Management
- Application Deployment with Chocolatey:
- Remote Device Actions
- Software and Policy Updates

03

Benefits for BloomingTech Services utilizing Jumpcloud Going Forward

- Best Practices for Continuous Improvement
- Mitigations
- Future Outlook

Core Components for Enhanced Security



SECURITY

- JumpCloud for LDAP & device/user management.
- MDM for device enrollment & policy.
 - a. Cross OS management
- Chocolatey for software deployment.

JumpCloud Implementation: Lab Setup



Setting Up a Diverse IT Lab with Mac's and Windows

JumpCloud Agent: & Policies Enhancing IT Management and Security

The screenshot shows the 'Devices' page in the JumpCloud Admin Portal. The left sidebar contains navigation links for Discover, Home, Users, User Groups, LDAP, RADIUS, SSO Applications, Password Manager, Device Management, Policy Management, Commands, MDM, Software Management, Directory, and Reports. The main content area has tabs for Overview, Devices, and Settings. The 'Devices' tab is active, showing a table of devices. A table with columns 'Status', 'Device Name', 'OS', 'Primary Adapter ID', 'Created', 'MFA Status', and 'Last Contact' is displayed. One device is listed: 'MacBook-Pro.lan' with OS 'macOS 14.0', Primary Adapter ID '192.168.0.225', and Created '03-12-2024'. The bottom status bar shows the time as 2024-04-24 09:55 AM.

The screenshot shows the 'Discover' page in the JumpCloud Admin Portal. The left sidebar is identical to the previous screenshot. The main content area has tabs for Discover, Home, Users, User Groups, LDAP, RADIUS, SSO Applications, Password Manager, Device Management, Policy Management, Commands, MDM, Software Management, Directory, and Reports. The 'Discover' tab is active, showing a 'Get Started Checklist' with a progress bar at 95%. The checklist items are: 'Create Admin Account', 'Add Users', 'Add Devices', 'Assign Users to Devices', 'View Directory Insights', and 'View System Insights'. A 'View Directory Insights' section is also visible, stating 'Your trial ends: 10 April 2024' and 'Contact Us'. The bottom status bar shows the time as 2024-04-24 09:55 PM.

Key Points: Simplifies device management- Controls USB device access- Enforces encryption and security policies-Automates screen locking for unattended devices.

Simplifying User Onboarding with JumpCloud

The screenshot displays the JumpCloud web interface for managing users. The top navigation bar includes links for Product Tour, Pricing, Alerts, What's New, Support, and a Checklist. A sidebar on the left provides access to various management tools categorized by User Management, User Authentication, Device Management, Directory Integrations, Security Management, and Privacy. The main content area is titled 'Users' and features a filter bar with tabs for All, Staged, Active, and Suspended. A search bar and a 'Filter by' dropdown are also present. Below the filter bar, a table lists user information, including User State, Name, Email, Password Status, and MFA/TOTP. A single user, Christina Lowe, is shown in the 'Active' state with a password status of 'OK' and an 'IN ENROLLMENT' MFA/TOTP status. A 'Settings' button is located in the top right corner of the main content area.

JumpCloud
FREE TRIAL 177 days left

Users

Product Tour Pricing Alerts What's New Support Checklist

Set the default user state for different creation methods by clicking the Settings button below.

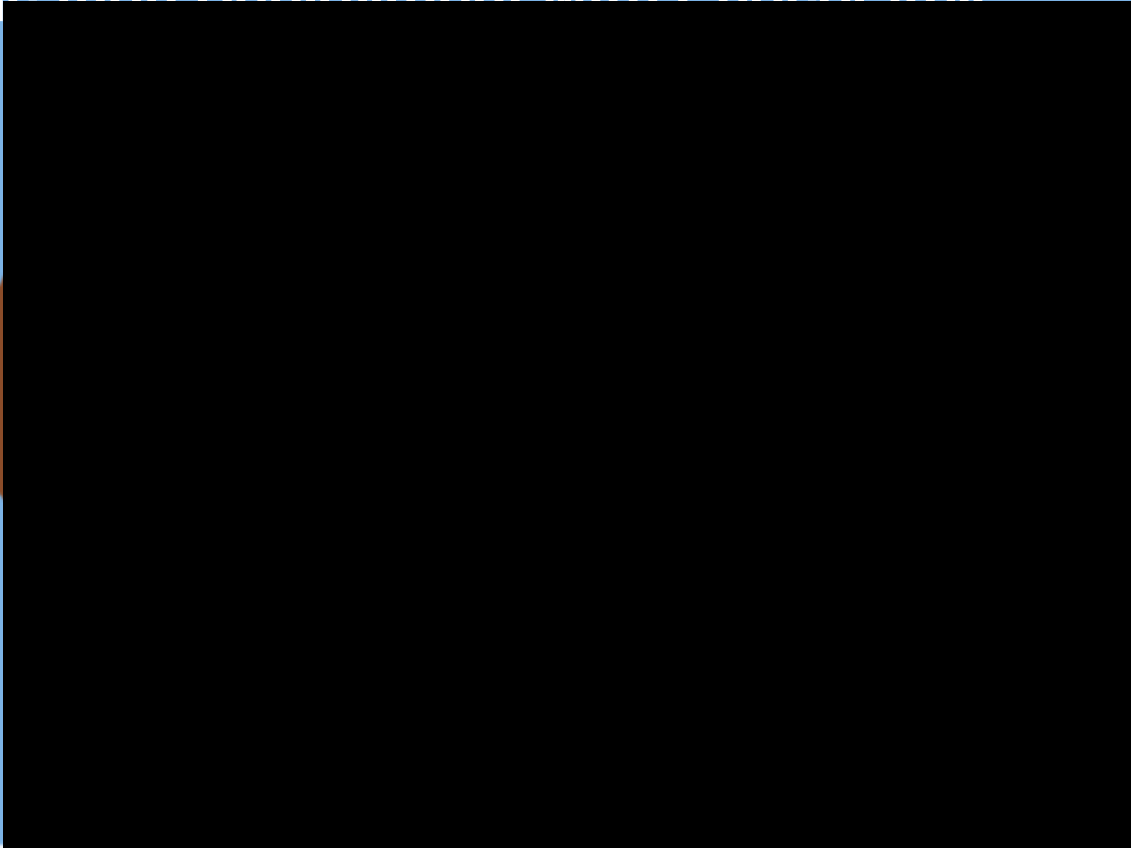
All Staged Active Suspended Settings

+ Search Filter by 1 user change state more actions delete columns export

User State	Name	Email	Password Status	MFA: TOTP
Active	Lowe, Christina	christina.lowe@blissingsystems.com	OK	IN ENROLLMENT

Live Chat Settings Account Collapse Menu

Application Deployment with Chocolatey:

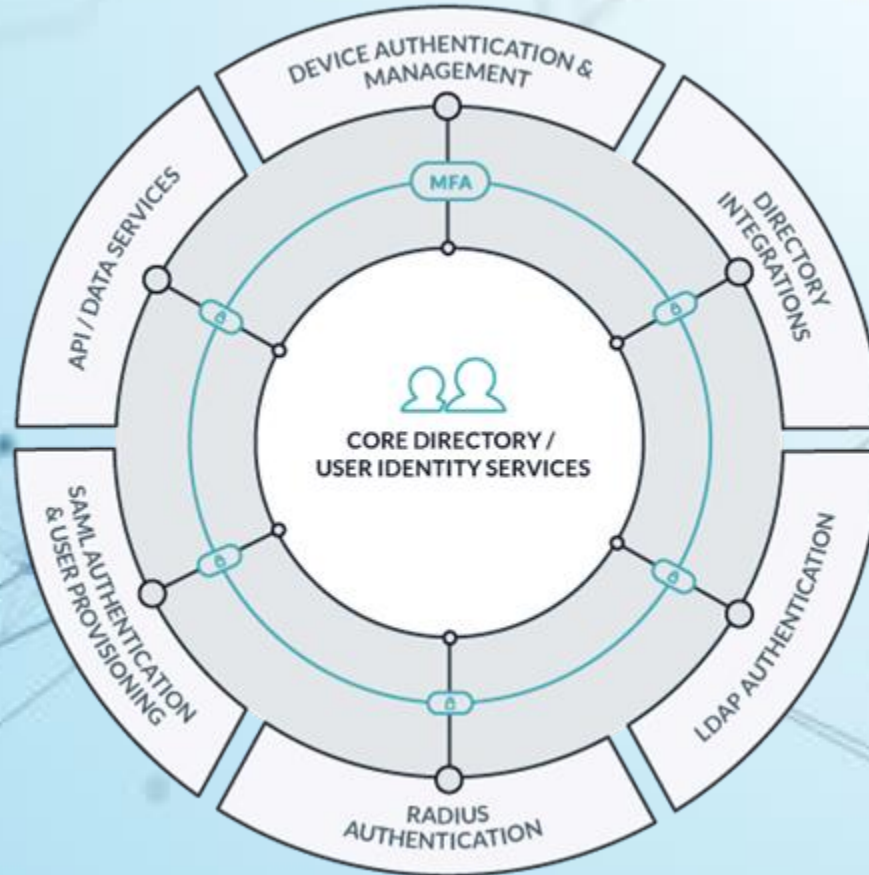


Remote Device Actions:

The screenshot shows the JumpCloud console interface. The top navigation bar includes links for Product Tour, Pricing, Alerts, What's New, Support, and Checklist. The left sidebar contains a menu with categories like User Management, User Authentication, Device Management, Directory Integrations, Security Management, and Insights. The main content area is titled 'Devices' and shows a table of managed devices.

Status	Device Name	OS	Primary Adapter IP	Created	MFA Status	Last Contact	Actions
	DellTest	Windows 11 Pro (22H2.3296) MDM	10.121.231.118	03-10-2024		17 minutes ago	Actions >
	MacBook-Pro.lan	macOS 14.4	10.121.234.61	03-10-2024		a few seconds ago	Actions >

Visualization Sketch



Mitigation

Key Points:

- **Security Policies**
- **Maintain Device Inventory**
- **Access Management**
- **Monitoring**



Conclusion: Strengthening BloomingTech's Future

Key Points:

- Advanced Security Features
- Stringent Access Controls
- Continuous Monitoring
- Comprehensive Device Inventory



References

Chocolatey Software, Inc. (2023). Using Chocolatey for software deployment. Retrieved March 20, 2024, from <https://chocolatey.org/>

JumpCloud. (2023). Comprehensive guide to device management and security with JumpCloud. Retrieved March 20, 2024, from <https://www.jumpcloud.com/docs/device-management-security>

Lujan, V. (2018, January 16). SAAS IDP: Software-as-a-service identity provider. JumpCloud. <https://jumpcloud.com/blog/saas-idp-software-as-a-service-identity-provider>

National Institute of Standards and Technology. (2023). Framework for improving critical infrastructure cybersecurity. Retrieved March 20, 2024, from <https://www.nist.gov/cyberframework>

OpenAI. (2023). Insights on JumpCloud implementation and IT management strategies [Personal communication]. ChatGPT conversation on March 20, 2024.