JumpCloud Integration Guide

JumpCloud delivers a unified open directory platform that enables secure, frictionless access to any resource, from a known and trusted device, from wherever your employees need to work. Their platform offers the ability to manage devices and identities in a single pane of glass

Important: This direct source was constructed with JumpCloud's API 1.0 version.

Deployment Type

This integration requires your environment to support **vendor cloud** deployments over **port 443**.

If you already know that your environment supports vendor cloud deployments, continue to step 2. If you are unsure about your organization's ability to use vendor cloud deployments, please work with your internal teams to determine your compatibility before continuing.

Required Information and Setup

Collect authentication information:

- API URL
  - Default value: https://console.jumpcloud.com/api
- API key (Client_api_key for admin user, from the JumpCloud console)
- Organization ID

Generate an API Key with Admin permissions

Your user must have (at least) the **Manager** role to generate the API Key. You must also have **Enable API access** enabled in your permissions (Settings > Edit Administrator).

1. Click on your username dropdown in the top right corner.
2. Select **My API Key**.
3. Click **Generate API key value**.

Retrieve the Organization ID

1. Navigate to **Settings**.
2. Click **Organization Profile**.
3. Click **Copy Organization ID** and paste it somewhere safe. You will need to send it via ShareFile to either your CSM or Implementations Specialist.

Send the Information to ReliaQuest

- Hostnames
- Usernames

Your integration will then be constructed by ReliaQuest's internal teams. They will notify you of its completion. If you have any questions, do not hesitate to reach out to your CSM or Implementations Specialist.

Permissions and Functionality

Permissions

Vendor Documentation: JumpCloud API Docs and Admin Portal Roles

GreyMatter Capability	Minimum Required Role	Scopes
Respond-Enrich Host	Manager	["systems","systems.readonly"]
Respond - Enrich User	Manager	["commandrunner.legacy","users","users.readonly"]
Respond - Disable User	Manager	["users"]
Respond - Enable User	Manager	["users"]
Respond - Shutdown Host	Manager	["systems"] ["commands","commands.readonly"]
Respond - Reset Password	Manager	["users"]

Respond

PLAYBOOK NAME	REQUIRED INPUT VARIABLE(S)	EXPECTED OUTPUT RESULTS
Enrich Host	Hostname or Host ID • Hostname example: Computer123 • Host ID example: 633f3f295482343ff32add41	Returns host information. In the JumpCloud console, navigate to "Device Management" > "Devices" > "Devices" to view host information.
Enrich User	Username or Email • Username Example: jsmith • Email Example: jsmith@company.com	Returns user information. In the JumpCloud console, navigate to "User Management" > "Users" to view user information.
Enable User	Username or Email • Username Example: jsmith • Email Example: jsmith@company.com	Updates a user's account status to "Active". In the JumpCloud console, navigate to "User Management" > "Users" to view user information. Immediately provision a user account and enable a user's access to assigned resources and policies. See vendor documentation.
Disable User*	Username or Email • Username Example: jsmith • Email Example: jsmith@company.com	Updates a user's account status to "Suspended". In the JumpCloud console, navigate to "User Management" > "Users" to view user information.
Reset Password**	Username or Email • Username Example: jsmith • Email Example: jsmith@company.com	The user's password is immediately expired and the user is logged out of their device and all JumpCloud-managed resources.

		In the JumpCloud console, navigate to “User Management“ > “Users“ to view user information.
Shutdown Host	Hostname or Host ID • Hostname example: Computer123 • Host ID example: 633f3f295482343ff32add41	Sends a shutdown command to the host. If the device is offline, the command will be run when the device becomes available. In the JumpCloud console, navigate to “Device Management“ > “Devices“ > “Devices“ to view host information.

* Suspended user accounts can’t access any resources they’re connected or assigned to, including email. Users with suspended accounts can’t unlock or reset their password to regain access to their account. Access to a suspended account can only be regained if the account is reactivated by their IT admin.

- When a user is suspended, they're automatically logged out of their device and connected resources and are prevented from accessing these resources during account suspension.
- Currently, Suspend User doesn’t support Windows Home. If a user of Windows Home is suspended, they aren’t automatically logged out of their device. However, if they switch user accounts, log out, or reboot, they're denied access to the device.
- Currently, Suspend User doesn’t support remote logins. If a user that is currently logged in to a device via remote session is suspended, they aren’t automatically logged out of the device. However, if they switch user accounts, log out, or reboot, they're denied access to the device.
- JumpCloud requires a password reset after users are connected to AD, Google Workspace, and Microsoft 365.
    - Active accounts receive emails instructing them to change their password after they're connected to these resources.
    - Suspended accounts can’t receive emails, so they won’t receive password reset emails after they're connected to these resources.
    - When a suspended account is reactivated, admins need to manually resend password reset emails. Admins can resend password reset emails from the Admin Portal “more actions menu” by clicking on their initials in the top right corner.

See vendor documentation.

** The user must change their password the next time they log in to their device:

- If JumpCloud detects the user is on a Mac or Windows device, they’re asked to update their password on their device login screen. If you've required MFA for the User Portal, users are required to verify their identity when they change their password.
- If JumpCloud detects the user is on a Linux device, they can log in to their User Portal using expired credentials and are shown a password change prompt. This prompt can’t be dismissed. If you've required MFA for the User Portal, users are required to verify their identity when they change their password.

See vendor documentation.

ReliaQuest Team Instructions*

**Only visible to ReliaQuest employees.*

JumpCloud Integration Guide

Disclaimer: All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.