ManageEngine
ADManager Plus

Integrate ManageEngine

ADManager Plus and JumpCloud for seamless employee life cycle management

The challenge

In enterprises, human resources (HR) teams work in tandem with other teams to provision accounts for new hires and deprovision accounts when employees leave. Apart from user account provisioning and deprovisioning, there will be timely requests to update profiles when the users want to change their personal information or move to a different team or location. This dependency on HR and other teams can create bottlenecks in employee onboarding and increase security risks when the access rights of former employees are not revoked in time.

The solution

Integrating JumpCloud with ADManager Plus allows you to synchronize data stored in JumpCloud with AD. ADManager Plus' integration with JumpCloud aims to improve the efficiency and security of employee onboarding, modification, and offboarding processes.

Benefits of HR-driven life cycle management

- Accelerate the employee onboarding process.
- Mitigate potential compromise of ex-employee accounts.
- Synchronize updates made in the HR system with AD.
- Keep stakeholders, such as managers, appraised about employee onboarding, offboarding, and account modifications.
- Minimize dependency on external teams.

Integration overview

When ManageEngine ADManagerPlus is integrated with JumpCloud, it can perform the following actions based on the users' attribute values in JumpCloud.

Create user accounts	Add users to groups
Modify user attributes	Remove users from groups
Modify user accounts by template	Create mailboxes
Reset passwords	Disable or delete mailboxes

Unlock users	Move home folder
Disable users	Delete home folder
Enable users	Revoke Microsoft 365 licenses
Delete users	Manage user photos
Run custom scripts	Disable Lync accounts
Move users across groups	Auto reply

When this integration is in place, admins will be able to provision, modify, and deprovision AD users automatically based on the respective details entered in JumpCloud.

Prerequisites

You must have an API key which will be passed in as a header called x-api-key. If you have admin access, follow the steps given in this JumpCloud documentation to retrieve the key. Otherwise, contact your JumpCloud admin.

Having appropriate permissions lets ADManager Plus fetch information from the following data fields in JumpCloud.

_id	allow_public_key	enable_user_portal_multifactor
account_locked	alternateEmail	external_dn
account_locked_date	company	external_password_expiration_date
activated	costCenter	external_source_type
addresses	created	externally_managed
country	creationSource	firstname
extendedAddress	department	jobTitle
id	description	lastname

locality	disableDeviceMaxLoginAttempts	ldap_binding_user
poBox	displayname	location
postalCode	email	managedAppleId
region	employeeIdentifier	manager
streetAddress	employeeType	mfa
type	enable_managed_uid	mfaEnrollment
middlename	password_expiration_date	passwordless_sudo
organization	password_expired	phoneNumbers
password_date	password_never_expires	public_key
recoveryEmail		

Configuration steps

Steps to configure JumpCloud settings in ADManager Plus

1. Log in to the **ADManager Plus** console, navigate to the **Automation** tab, and select **Application Integrations.**
2. Under *Enterprise Applications*, click **JumpCloud.**
3. JumpCloud uses **API Key** to authorize API requests. Generate a value by performing the steps listed in the section and paste it in the **Value** field.
4. Click **Configure.**
5. In the **API Endpoint Configuration** section, the **Endpoint URL**, API **Method, Headers, Parameters**, and **Message Type** are all pre-configured. This is the **Endpoint URL** for JumpCloud: https://console.JumpCloud.com/api/systemusers

Note:

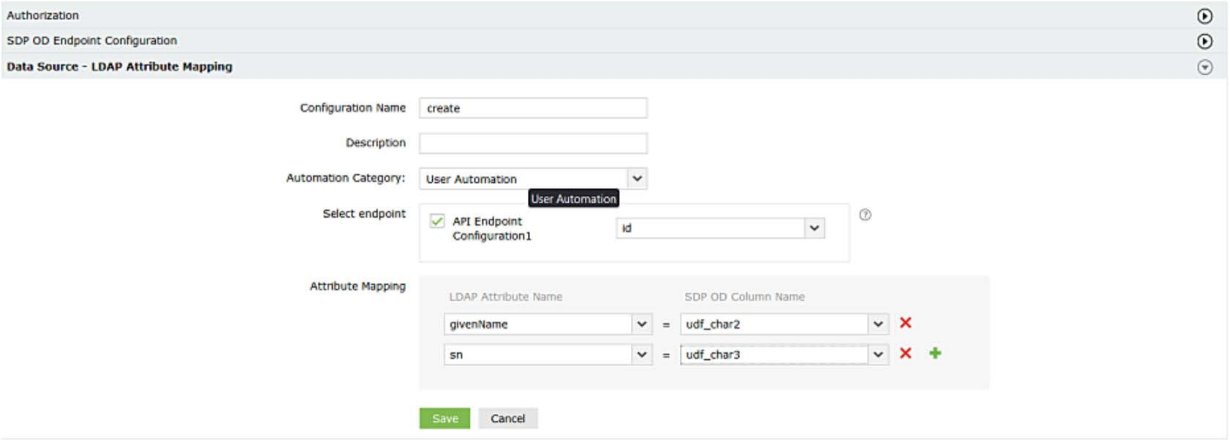
- Click here to learn more about JumpCloud's API references.
- Additional headers and parameters can also be configured. Click here to learn how.
- The **Message Body** can be customized, per your organization's needs.
- The API will repeatedly be called until a response without the term rows is received. This is preconfigured as well.
- You can configure multiple endpoints for this solution.

6. Once done, click **Test & Save.**

7. A response window will display the response schema. Click **Proceed.**

8. Click **Data Source - LDAP Attribute Mapping** to map AD LDAP attributes with the respective attributes in JumpCloud.

9. Enter the **Configuration Name** and **Description** and select the **Automation Category** from the drop-down menu.



Authorization
SDP OD Endpoint Configuration
Data Source - LDAP Attribute Mapping
User Automation
Save
Cancel

Configuration Name: create

Description:

Automation Category: User Automation

Select endpoint: ☑ API Endpoint Configuration1 — id

Attribute Mapping:

LDAP Attribute Name		SDP OD Column Name
givenName	=	udf_char2
sn	=	udf_char3

10. In the **Select Endpoint** field, select a **Primary Key** that is unique to a user (e.g. employeeIdenifier).

Note: When multiple endpoints are configured, this attribute must hold the same value in all the endpoints.

11. In the **Attribute Mapping** field, select the attribute from the LDAP Attribute Name drop-down menu and map it with the respective column in JumpCloud.

12. Click **Save.**

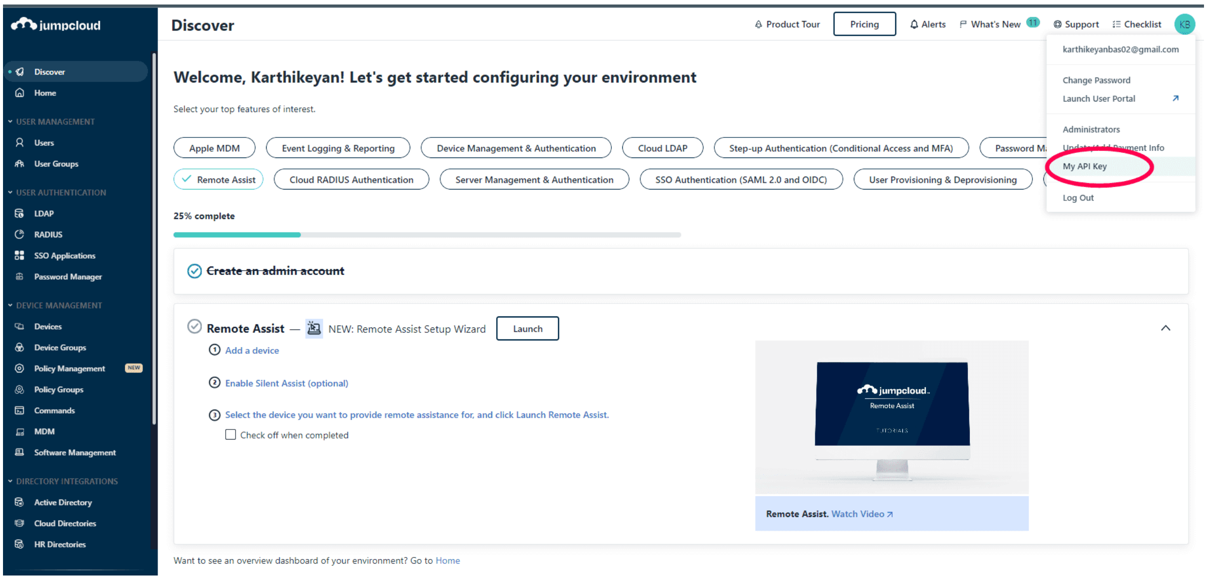
Steps to generate API key in JumpCloud

1. Log into the JumpCloud admin console.

2. Navigate to the username drop down located in the top-right of the console.

3. Select **My API Key** and click **Generate New API Key**.

4. Copy the generated value and paste it while configuring authorization for JumpCloud in ADManager Plus.



Welcome, Karthikeyan! Let's get started configuring your environment

Select your top features of interest.

25% complete

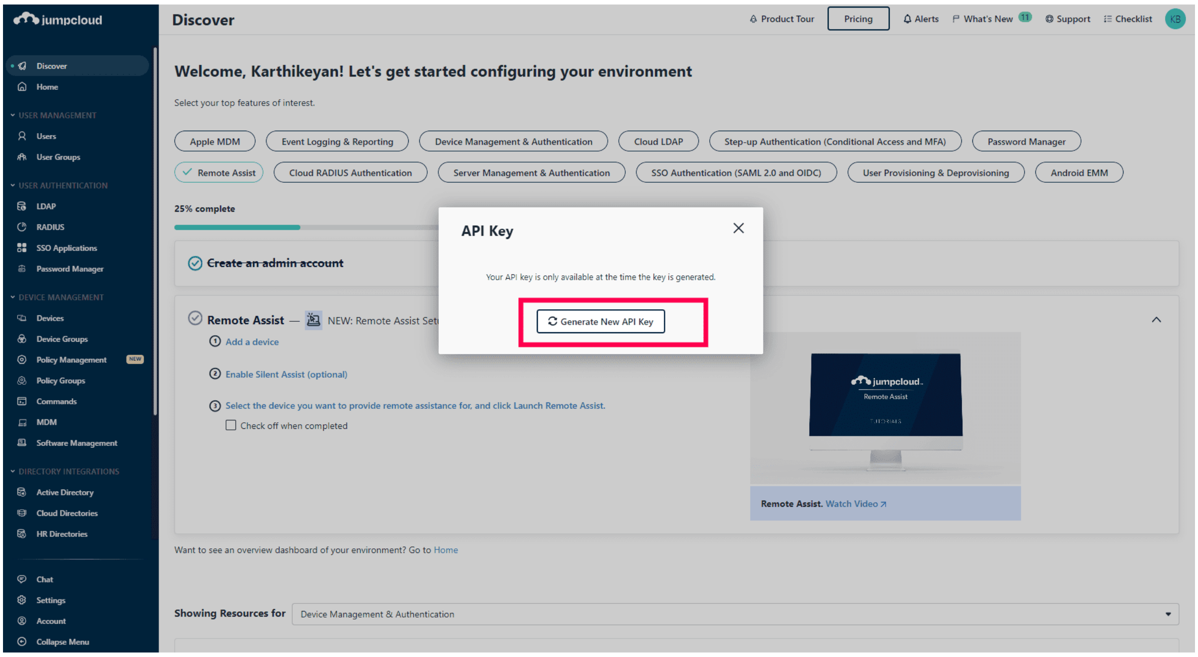
~~Create an admin account~~

Remote Assist — NEW: Remote Assist Setup Wizard

1. Add a device
2. Enable Silent Assist (optional)
3. Select the device you want to provide remote assistance for, and click Launch Remote Assist.

□ Check off when completed

Want to see an overview dashboard of your environment? Go to Home



API Key

Your API key is only available at the time the key is generated.

Showing Resources for: Device Management & Authentication

Steps to automate user provisioning in ADManager Plus

ADManager Plus' Automation feature simplifies the process of configuring and scheduling user provisioning, deprovisioning, and reprovisioning from JumpCloud, allowing you to automatically perform the task without the need for manual labor.

Follow the below steps to automate user provisioning effortlessly:

1. Click the Automation tab.
2. From the left pane, click Automation.
3. Click Create New Automation in the top-right corner.

4. Enter a suitable automation name and description.
5. Select User Automation from the Automation Category drop-down list.
6. Choose a domain and OU.
7. In the Automation Task/Policy section, choose the desired task (Create Users, Modify User Attributes) or an automation policy from the drop-down list.
8. In the Select objects section, select Data from JumpCloud.
9. Set your execution date and time.
10. Click Save.

How does the integration work?

In ADManager Plus, create an automation that will run at a set frequency to provision users. When the automation is executed, ADManager Plus will fetch user data from JumpCloud by initiating the API calls configured in earlier steps.

Once ADManager Plus receives data from JumpCloud, it will be stored in the product's built-in PostgreSQL database (or in your Microsoft SQL database), and the corresponding changes will be made in the AD environment.

What information is stored in ADManager Plus?

After the initial configuration is complete, ADManager Plus will fetch data from JumpCloud at the scheduled time. The fetched data is stored in ADManager Plus' database, which is located on premises. The stored data is used to perform management actions such as provisioning, reprovisioning, or deprovisioning users based on the configured automations.