jumpcloud™

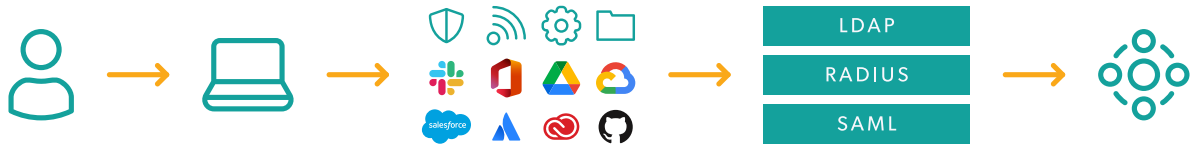
Guide

Implementation Guide

Table of Contents

Get to Know JumpCloud

JumpCloud is a comprehensive and flexible cloud directory platform. From one pane of glass, manage user identities and resource access, secure macOS, Windows, and Linux devices, and get a full view of your environment.



As you implement JumpCloud into your organization it is important to understand the best practices related to getting your existing users onboarded, enrolling devices while taking over existing user accounts, integrating with existing IT tools, and enabling user access to all their resources. Implementing resources in piecemeal fashion without a cohesive plan could result in wasted time and a poor user experience. For example, users who come from a preexisting directory (e.g., Active Directory/Azure AD) or an MDM will have a different implementation pathway than organizations implementing a directory platform solution for the first time. Be sure to take advantage of the following resources to streamline your implementation.

Sign up for an account in JumpCloud University!

Check out this easy-to-follow infographic for the steps to register for a free account.

JCU gives you access to many resources including interactive courses, short tutorial videos, hands-on practice with guided simulations, and help from our experts. Plus, your progress is saved and tracked as you go.

This quick 30-minute course is a great introduction to JumpCloud and is designed to help familiarize you with JumpCloud University.

What is JumpCloud?

Become certified through JCU!

Why get certified:

- Feel more confident in your ability to use the JumpCloud platform.
- Be the go-to JumpCloud admin for your IT org.
- Showcase your skills by displaying your certification badge on your professional profiles.

Prep Work

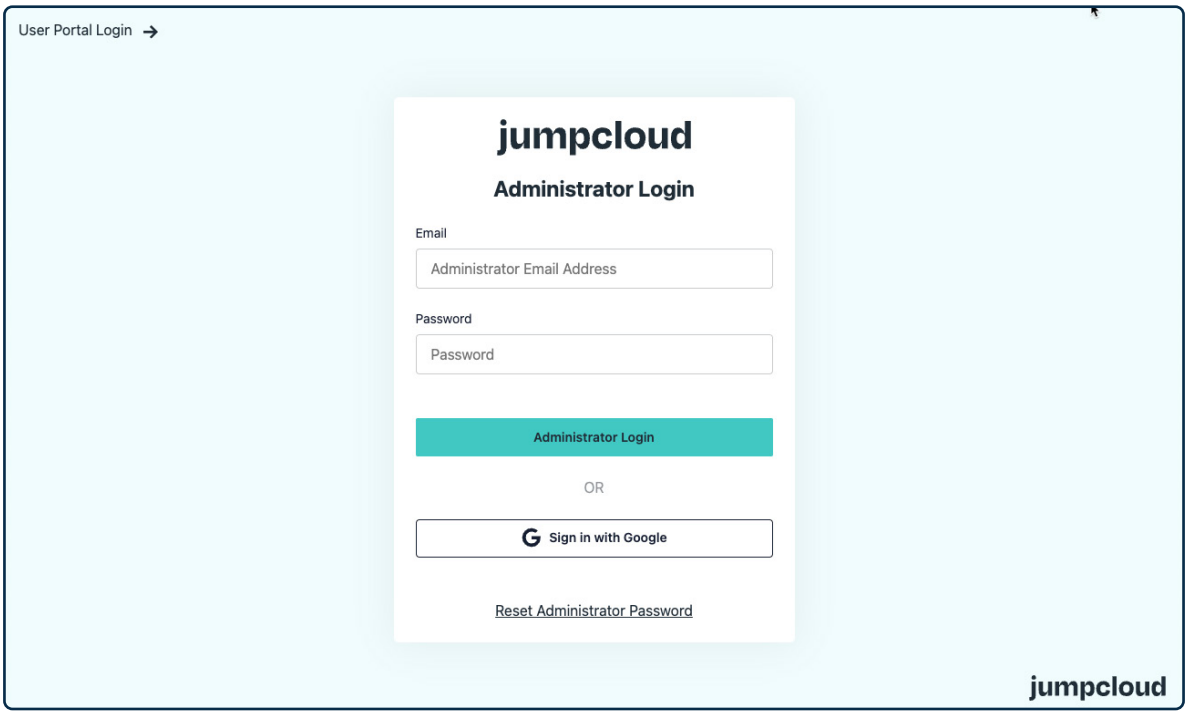
The first section of this guide begins with preparation work. You will log in to your account, learn how to edit basic settings, and get familiar with JumpCloud's educational resources. It is important that these steps are completed before starting the implementation process.

1. Get Access to the JumpCloud Admin Portal with Your Administrator Account

2. Bookmark the JumpCloud Admin Portal

Add this link to your browser bookmarks for future access.

3. Log in to the Admin Portal with Your JumpCloud Admin Account



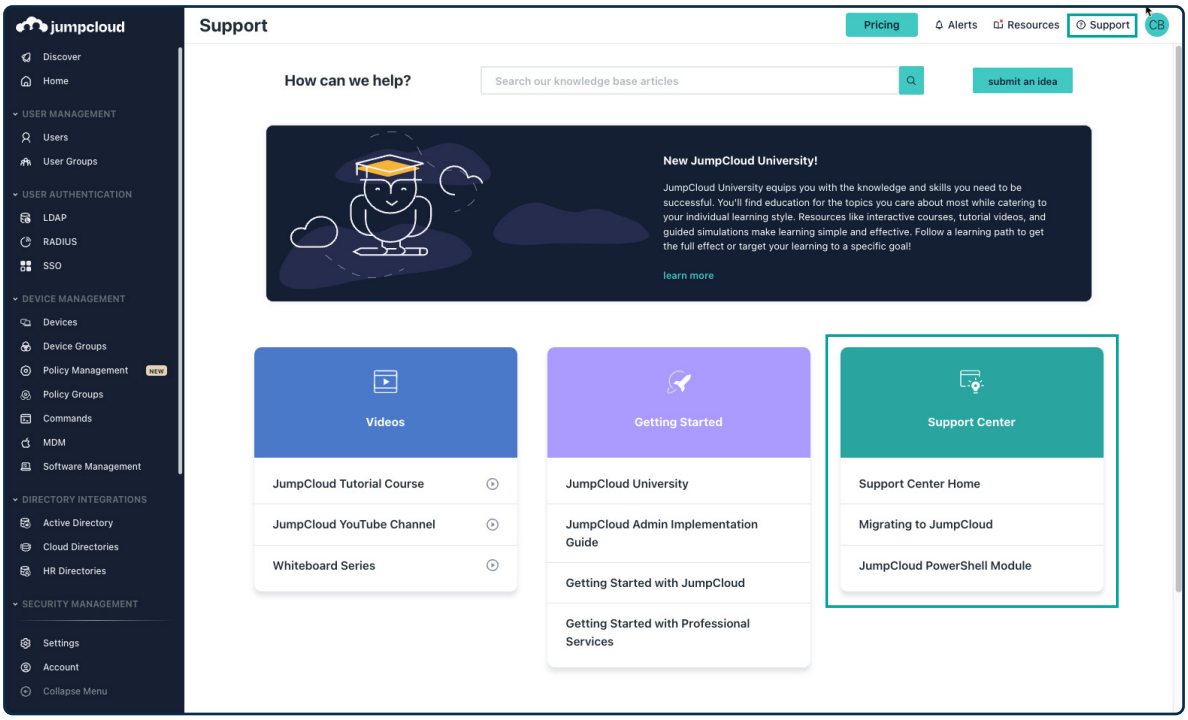
4. Access the Support Knowledge Base Portal

JumpCloud Knowledge Base

Tip: The Knowledge Base Articles can be searched by topic. Bookmark this site too!

5. Create a Test Support Case

Our team supports our customers and partners across-the-board, from implementations and integration guidance, to ongoing education and issue triage. Are you experiencing an issue and need to get in touch with JumpCloud Support?



Check out this video to learn how to create a Support ticket:

Submit a Support Request

Use this link to access the Knowledge Base article on how to create a Support ticket:

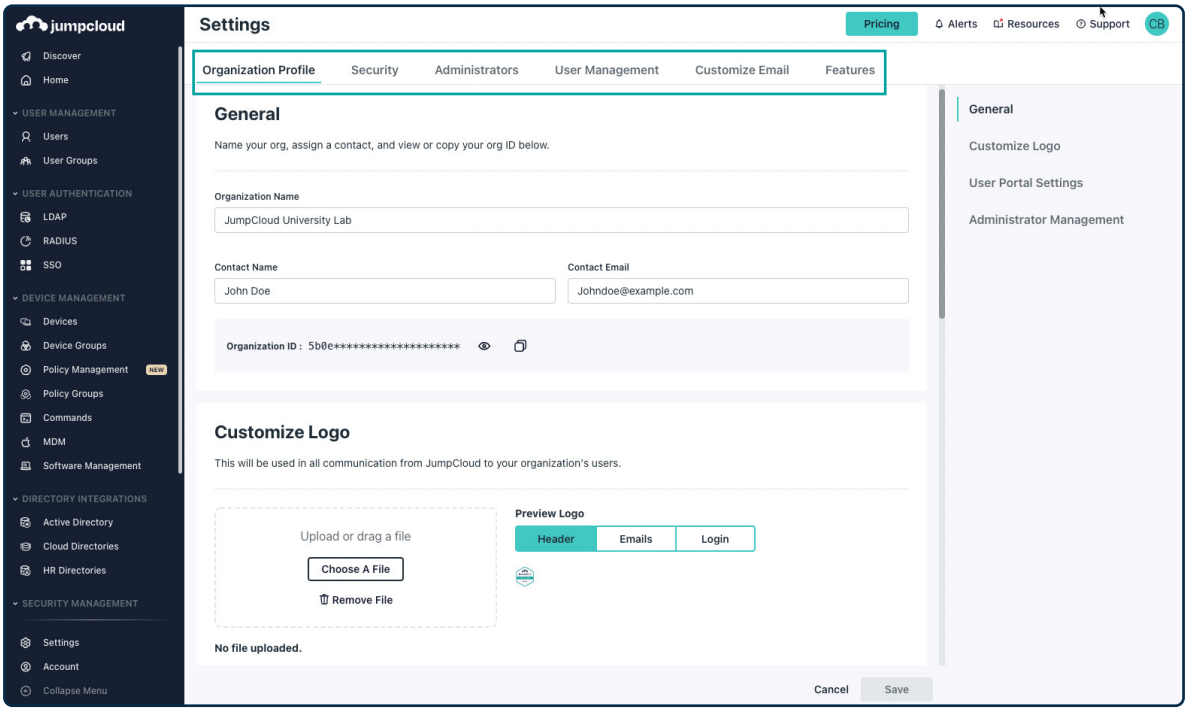
Contacting JumpCloud Support

6. Find Organizational Settings

Your Organization Profile houses general settings that your user's will encounter, like the company logo, enabling read-only access for users, along with User Portal session timeout and requests to delete the organization.

To access your settings:

1. Log in to your JumpCloud Admin Portal.
2. Select Settings at the bottom of the left-hand navigation panel.
3. There are five tabs under Settings that you can navigate between, some have their own menu of features on the right-hand side. Select the tabs and features you want to view and update.

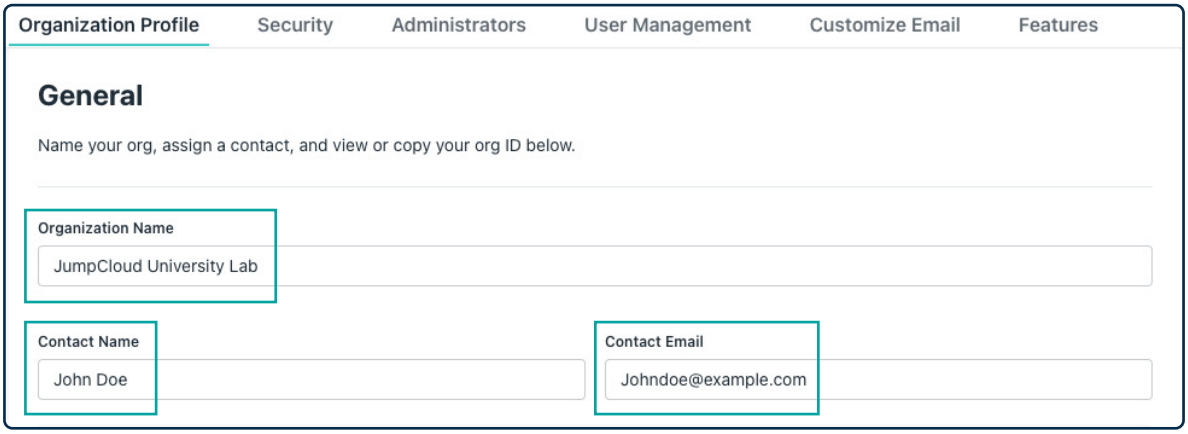


4. Once you are finished making updates in a given tab, select Save.

7. Name Your Organization and Access Your Org ID

Under the Settings > Organization Profile > General section, you can apply an Organization Name, primary Contact Name, and primary Contact Email.

Note: Emails will include a contact link to this contact name and email.



To access your Organization ID:

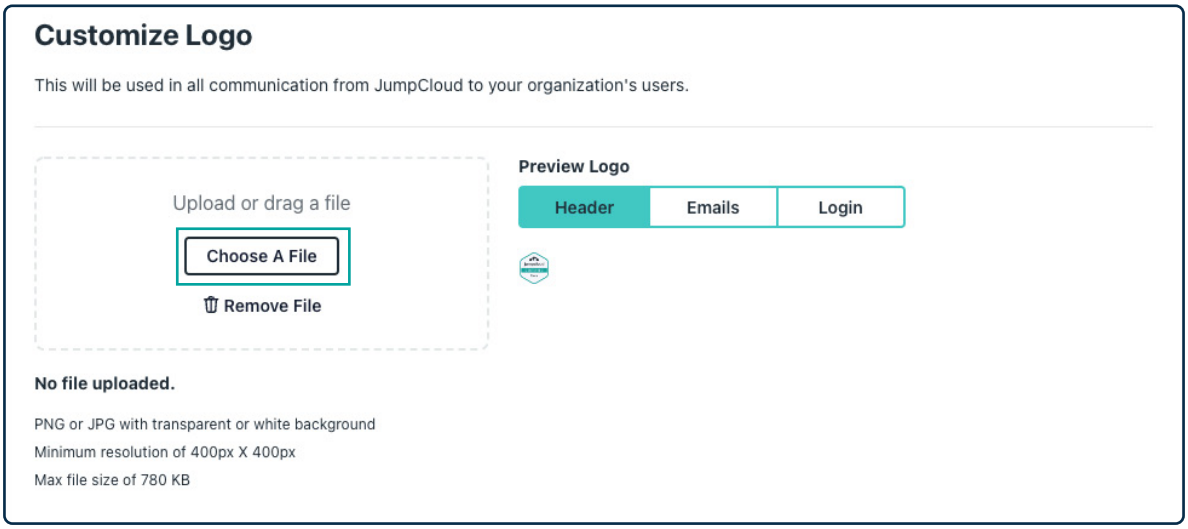
1. To view and/or copy your Organization ID, select the 'eye' icon to remove the obscured view.
2. Select the "double page" icon to copy the ID.

8. Upload Your Company Logo

To customize the Logo:

1. Select Choose A File or Upload/Drag & Drop a .png or .jpg with a transparent or white background. You can see what your logo will look like in communication from JumpCloud to your org's users under Preview Logo.
2. Select Save.

Note: The logo must meet a minimum resolution of 400px X 400px and a max file size of 780 KB.



9. Review the JumpCloud Admin Portal Layout

Watch this tutorial to review the overall UI of the Admin Portal:

Admin Portal

10. Educate Users on the Upcoming Implementation of JumpCloud

Visit this Knowledge Base article for email templates designed to introduce your organization to the JumpCloud platform. You can copy the email templates and paste them into an email in your email provider.

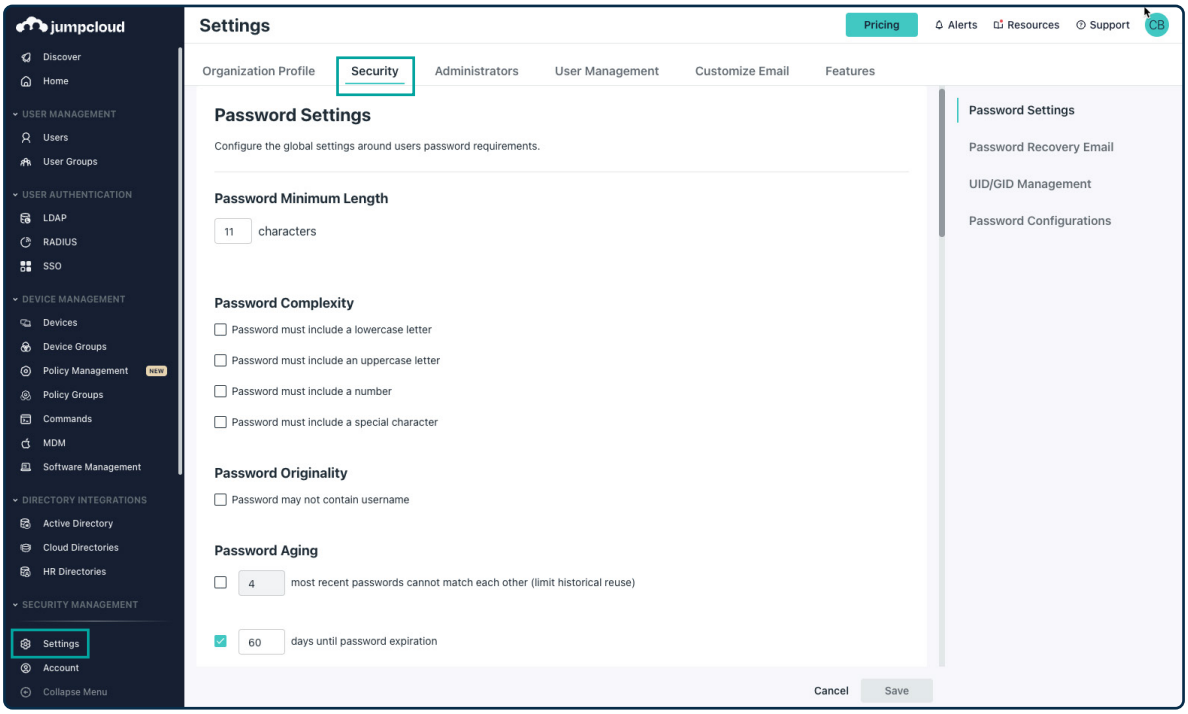
 Email Templates and Recommendations for Educating New Users

Phase 1: The JumpCloud Admin Portal

There are various settings within the JumpCloud Admin Portal. This section helps you to understand editing security settings, creating password settings, configuring multi-factor authentication (MFA), and making additional admin accounts.

1. Find User Security Settings

JumpCloud's password settings give you the ability to set password length, complexity, originality, aging, and lockout rules for your entire organization to meet your security needs. The user account password governs access to the JumpCloud user account, as well as to all resources that the account can access, like computers and SSO applications.



2. Configure Password Complexity

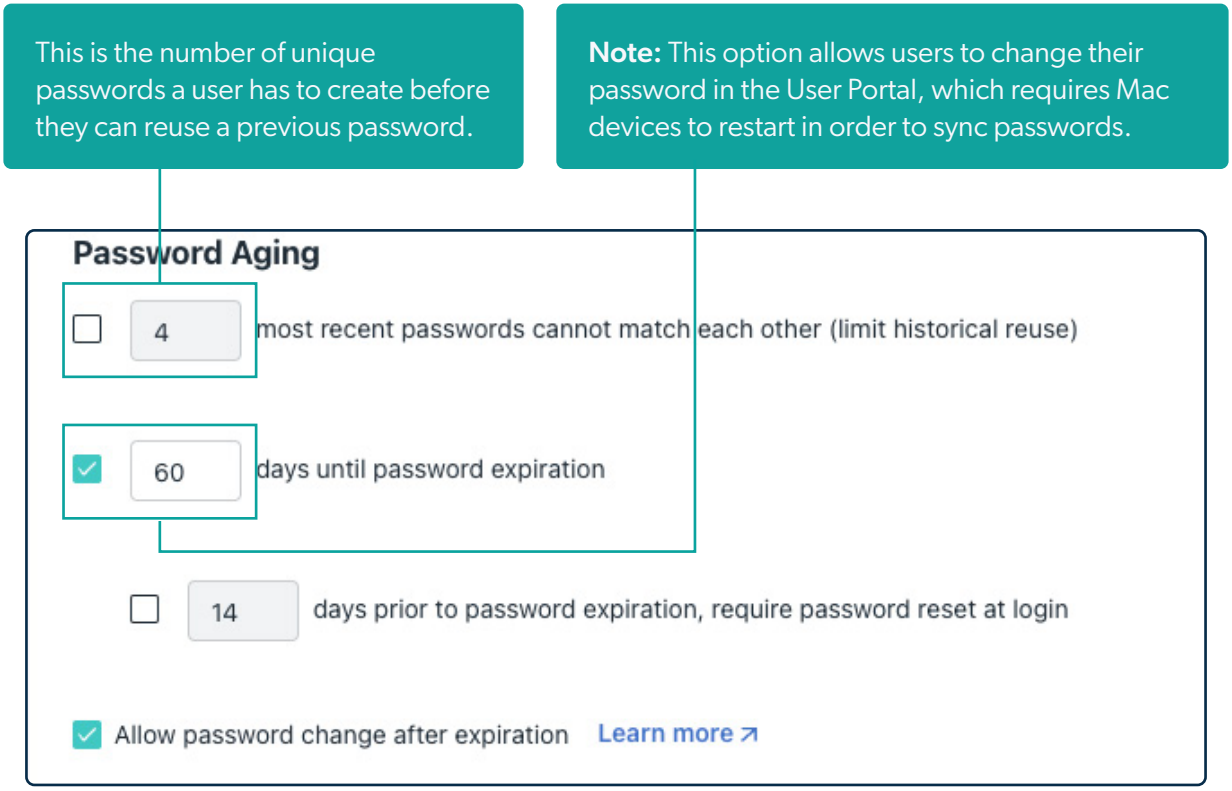
1. Under Settings > Security > Password Settings, set the Password Minimum Length to the desired number of characters.
2. Optionally, select one or more Password Complexity requirements to apply to all user passwords in your organization. Users won't be able to create a password that doesn't adhere to the complexity you specify. The options are:

    - Password must include a lowercase letter.
    - Password must include an uppercase letter.
    - Password must include a number.
    - Password must include a special character.

3. Optionally, under Password Originality, select whether or not the password may contain the username.
4. Select Save.

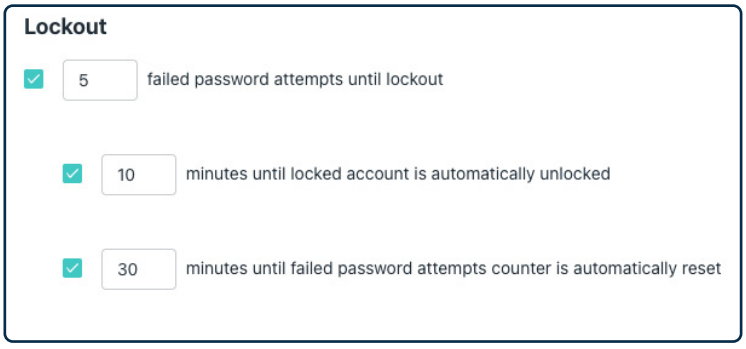
3. Configure Password Aging

Password aging is a mechanism you can use to force users to periodically change their passwords.



4. Password Lockout

You can trigger account lockout to protect your managed devices. Account lockout is triggered from the User Portal and locks users out of the User Portal and device endpoints.

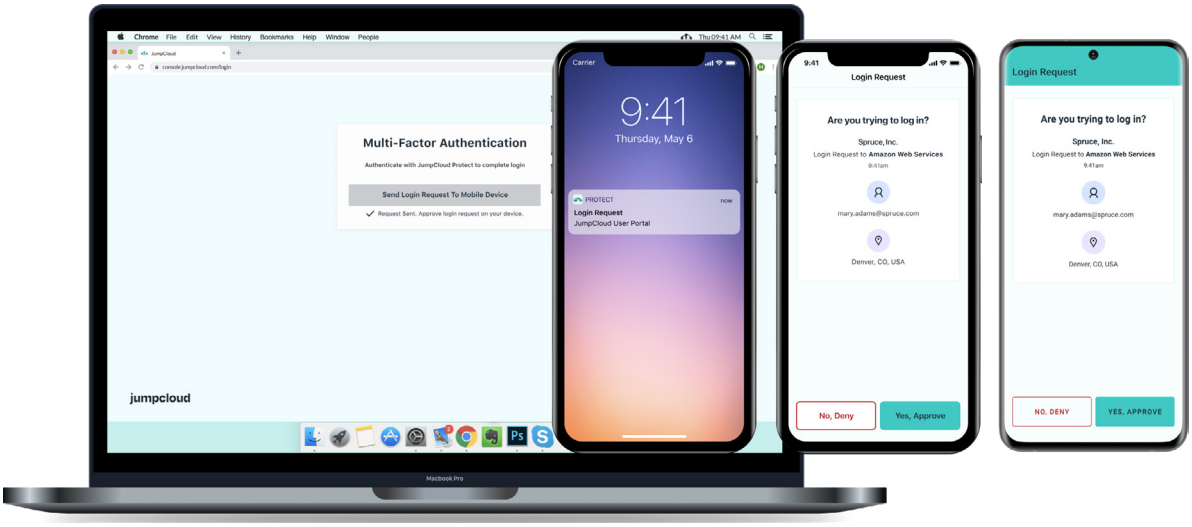


Note: If a user becomes locked out while they are in a session, they will remain logged into their account until they log out. Once the user logs out, they won't be able to log back in until their account becomes unlocked.

5. Configure Global MFA Settings and Options

Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.

Verification Code (TOTP) MFA uses authentication codes called Time-Based One-Time Passwords (TOTP). These codes are generated from an authenticator application on a mobile phone or computer, like Google Authenticator or Yubico Authenticator.



Check out this course to learn more about enabling MFA:

Enabling MFA

Here you will find the Knowledge Base article that explains the different options for setting up MFA:

JumpCloud MFA Guide

6. Invite IT Staff as JumpCloud Administrators

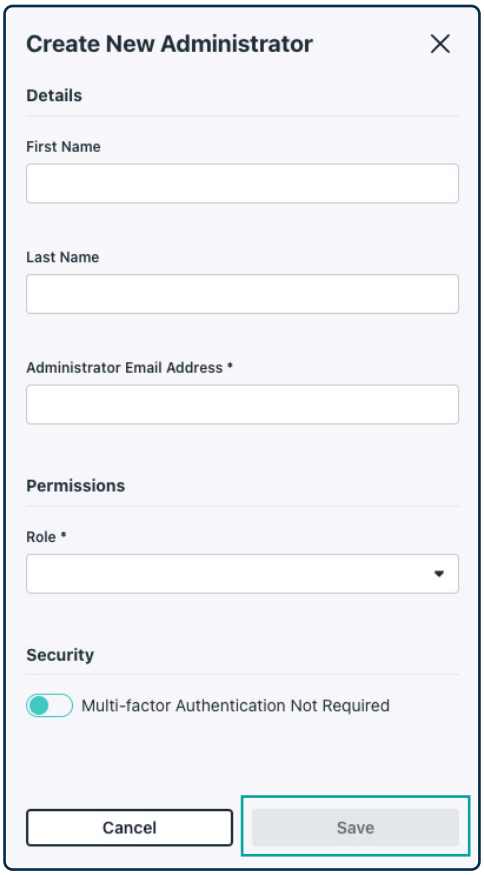
Administrator accounts are separate from user accounts. While not required, best practice is to have a minimum of two (2) administrator accounts that have the administrator with billing role.

Note: Administrators cannot delete their own accounts.

To create administrator accounts:

1. Log in to the JumpCloud Admin Portal.
2. In the top right of the Admin Portal, select the circle with your initials to access your JumpCloud Account menu.
3. Select Administrators. The Administrators panel appears.

4. Select (+). The New Administrator panel appears.
5. Enter a unique email address, then select a Role for the administrator account. Learn about JumpCloud administrator account roles here.
6. *Select Enable Multi-Factor Authentication for Login (*optional).
7. Select Create.
8. The user will receive an email to the specified address with a link to create a password. Once their password is set, the administrator can log in to the Admin Portal and manage JumpCloud.
9. The administrator account user is sent an email to the address you specify during account creation. This email contains a link to set the initial password for their account. After they set their password, the new admin can log in to the Admin Portal and manage JumpCloud.



To learn more about Administrator Settings, check out this course:

Administrator Settings

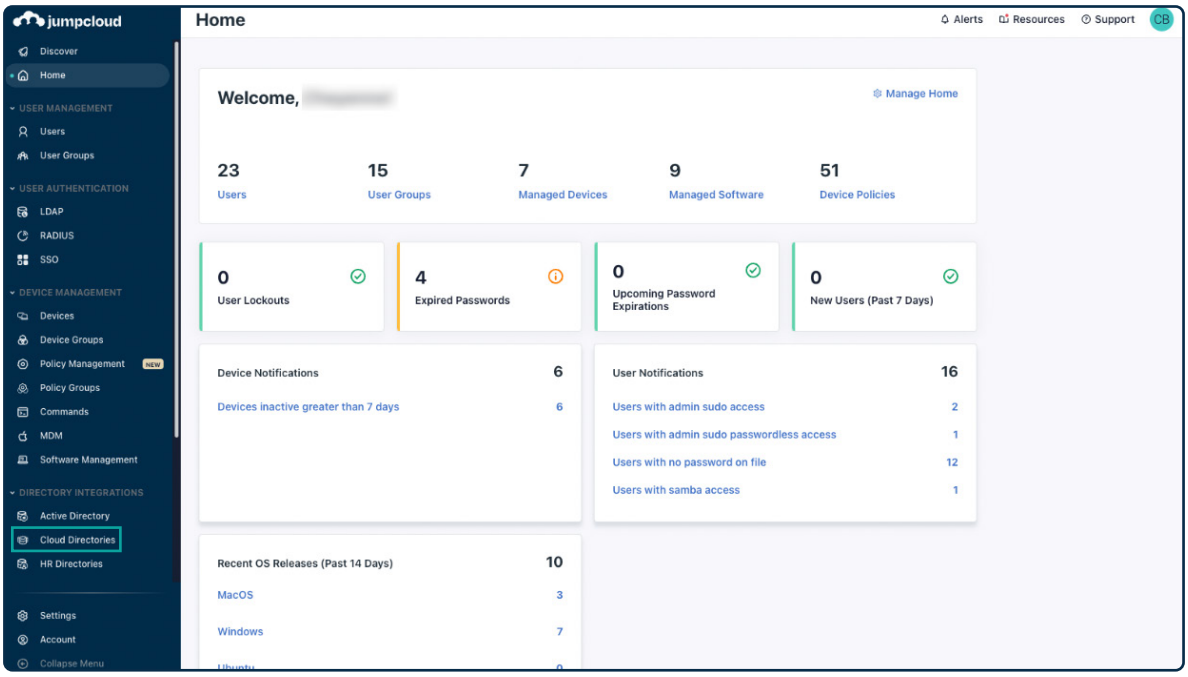
Phase 2: Users

Adding Users From an Existing Cloud Directory

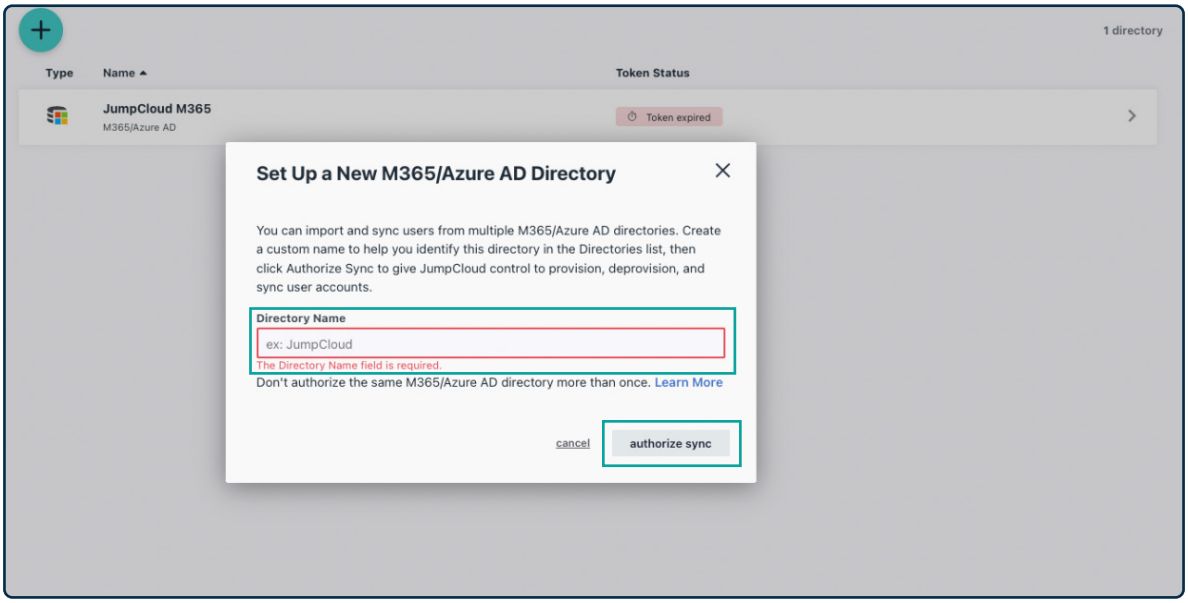
1. **Obtain Cloud Directory Admin Credentials**
   You will need administrator access to your current cloud directory to begin importing users.

   > JumpCloud integrates with a variety of popular directory services to synchronize user accounts. These integrations let JumpCloud act as an authoritative directory with a single set of credentials that can be used across all directory services. When you integrate with a directory service, you can securely import existing user accounts as well as persistently replicate data across directories. You're in control of which users get replicated.

2. **Navigate to the Cloud Directories Menu**



3. **Create a new directory, and provide a display name**
   1. Select Cloud Directories under Directory Integrations.
   2. Select the (+) and choose your company's cloud directory to import from the following:
      - Import from Google Workspace
      - Import from M365/ Azure AD
      - Real-time import from Okta
      - Import JumpCloud LDAP into Okta
   3. Enter the directory name in the Directory Name field. Then select authorize sync.



4. Utilize the cloud directories admin credentials already obtained to sync with JumpCloud.

Check out these Knowledge Base articles for more details:

- Importing Office 365 Users
- Importing G-Suite Users
- Configure Okta Real-time User and Password Import

Importing Users from CSV

Considerations:

- Each user you import must be a unique user with a unique email address.
- CSV file headings are case sensitive and will fail if they don't match JumpCloud's expected case. To see the case JumpCloud is expecting, you can download the CSV template and update the headings of the file you want to import accordingly.
- Users without passwords are imported into JumpCloud in an inactive state.
- Users created with or without a password are not sent an activation email on CSV import.
- You can also import users from a CSV file using JumpCloud's PowerShell Module.

  Importing Users into JumpCloud from CSV Using the PowerShell Module

Note: Keep in mind that the functionality between the two CSV import methods differs.

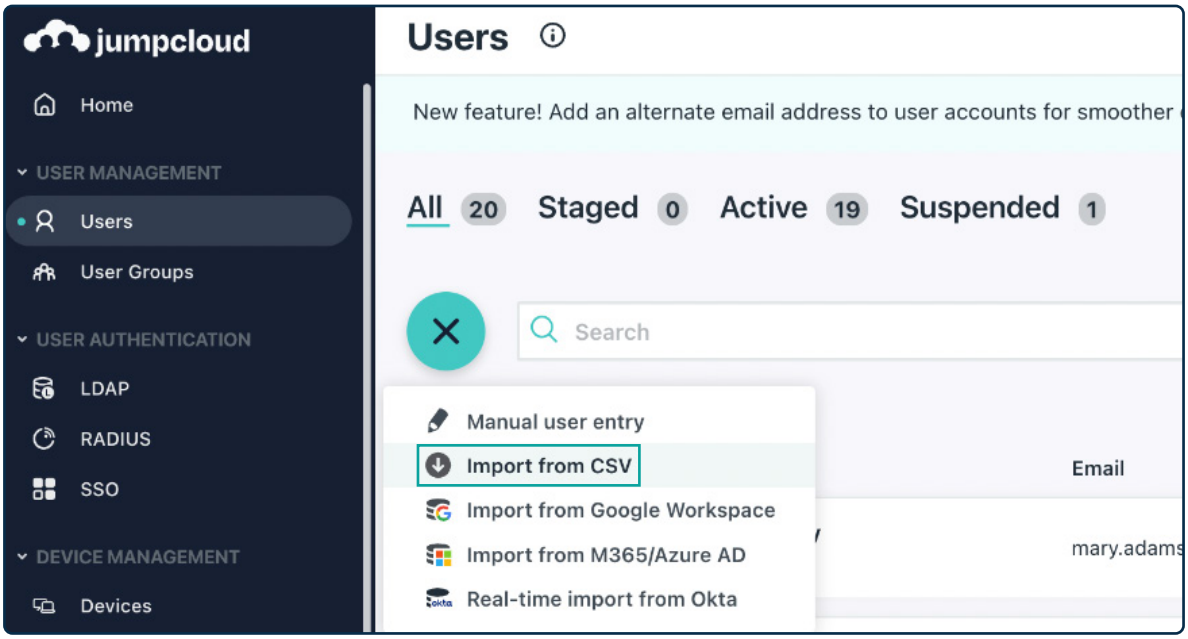
Importing Users from the JumpCloud Admin Portal vs. PowerShell Module

Keep the following differences in mind as you decide whether to import users from CSV into the Admin Portal or the PowerShell Module:

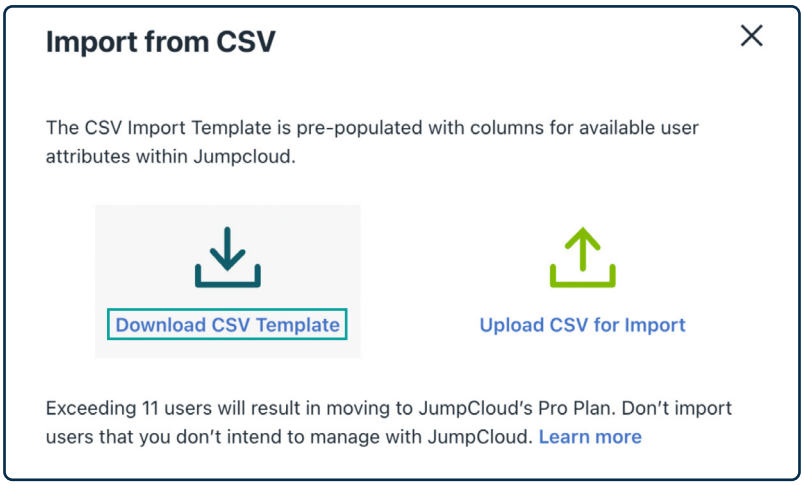
- Users imported from CSV into the Admin Portal can't automatically be connected to user groups. You can create group associations using the PowerShell Module.
- Users imported from CSV into the Admin Portal can't automatically be connected to systems. You can create system associations using the PowerShell Module.
- Users imported from CSV into the Admin Portal can only be created with the following attributes:
    1. First Name
    2. Last Name
    3. Username
    4. Email
    5. Password
- You can import users from CSV with more than the previously mentioned attributes using the PowerShell Module.

To add users via CSV in the Admin Portal:

1. Log in to the JumpCloud Admin Portal.
2. Go to USER MANAGEMENT > Users.
3. Select (+), then select Import from CSV user entry.



4. You will need to download the CSV template first. Please select Download CSV Template.



5. Once you've downloaded the CSV template, fill it out using the template form and save the CSV with all of your users.

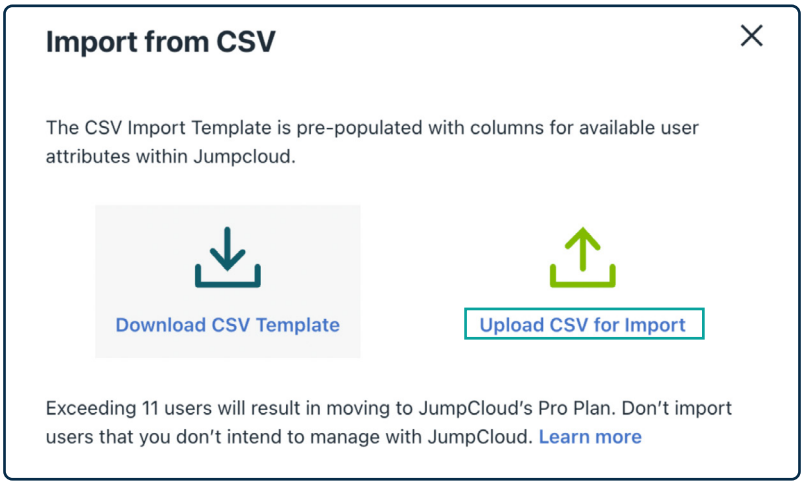
   Below are the contents and format of the CSV:

   firstname,lastname,username,email,password
   "","","","","",""

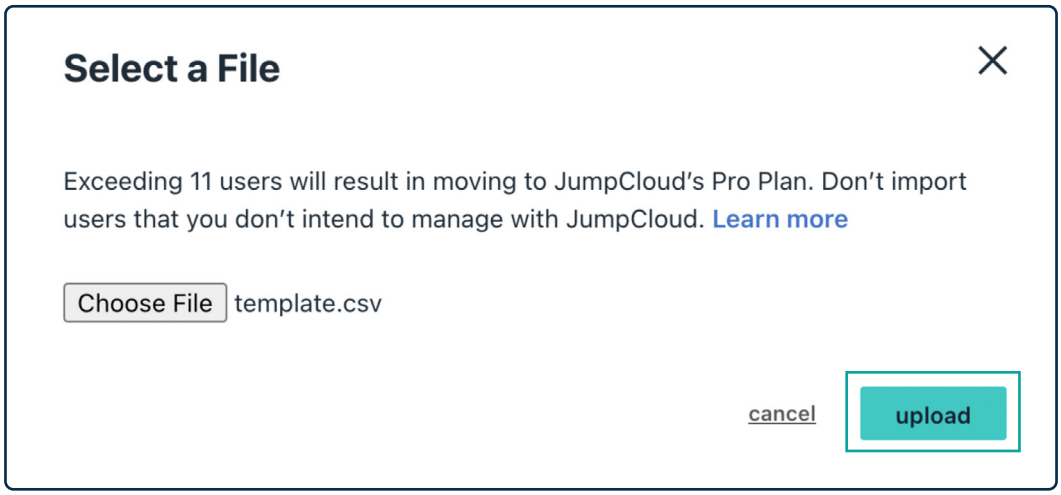
   You must adhere to the CSV format with these five attributes.

Note: If you put passwords in the CSV, this will add the users in an activated state with the password you entered in the CSV. Users will not be automatically emailed an activation or welcome email from JumpCloud.

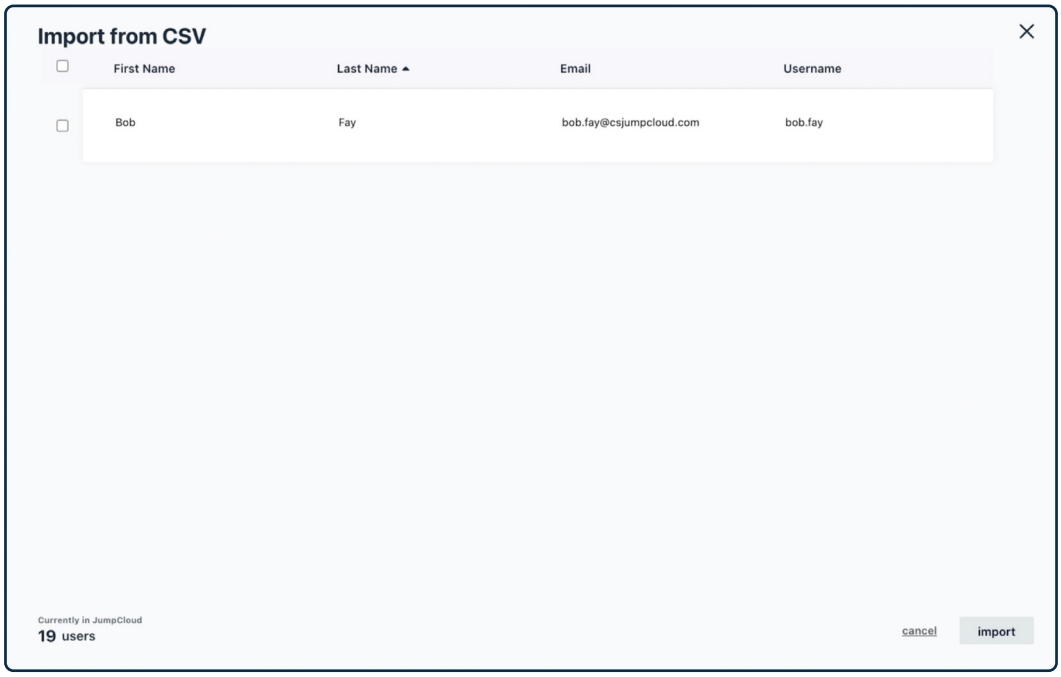
6. When you've finished compiling the CSV, you can then select Upload CSV for Import and upload the CSV you just made.



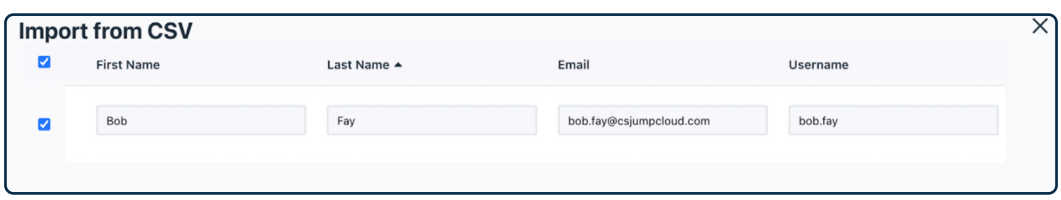
7. Once you've selected your CSV from your local file folder where it's stored, select Upload.



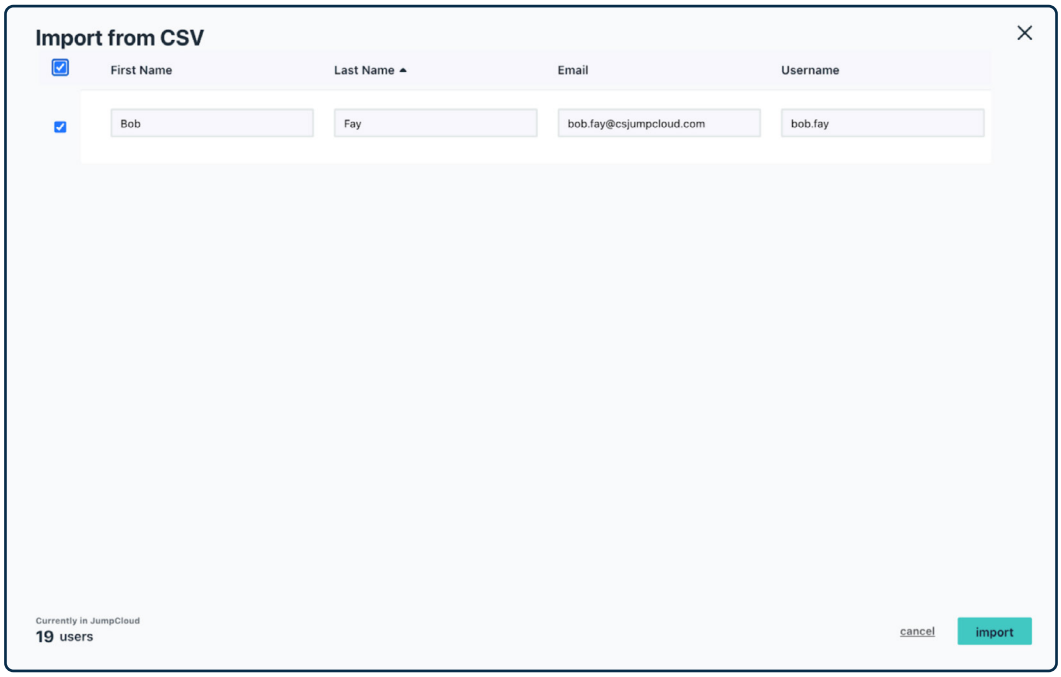
8. The next screen shows all of the users you just added to the CSV.



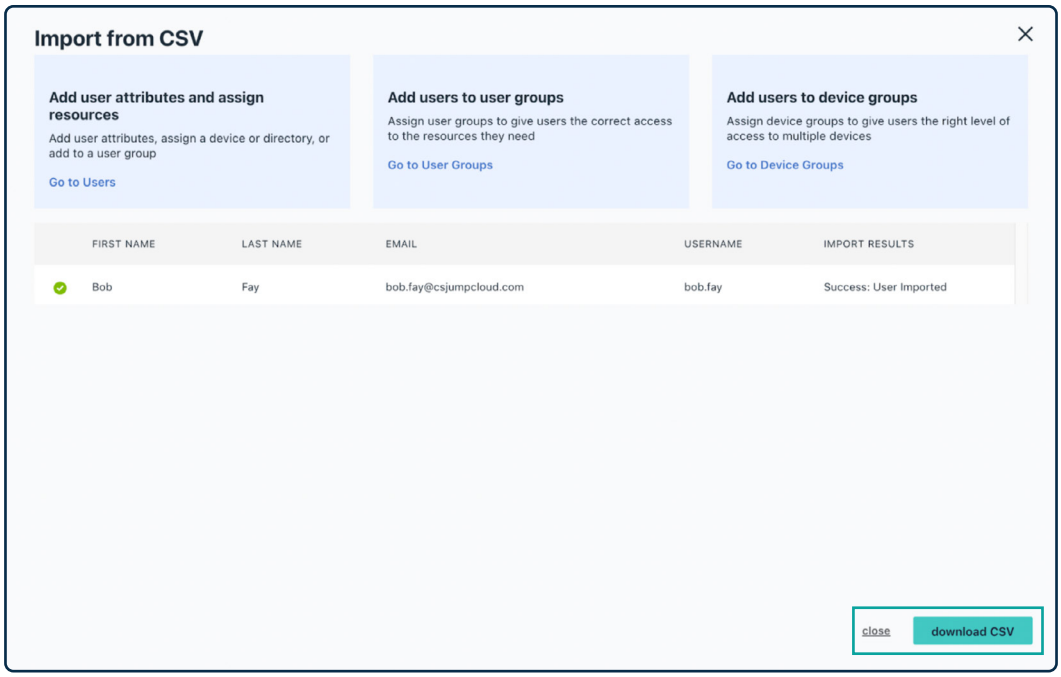
9. Select all of the users by selecting the top left checkbox button.
10. You will see all of the users with a checked checkbox now. Optionally, you can now change any of the attributes in this list if you need to, such as email address or username.



11. Next, select the **Import** button in the bottom right to fully import the users into JumpCloud.

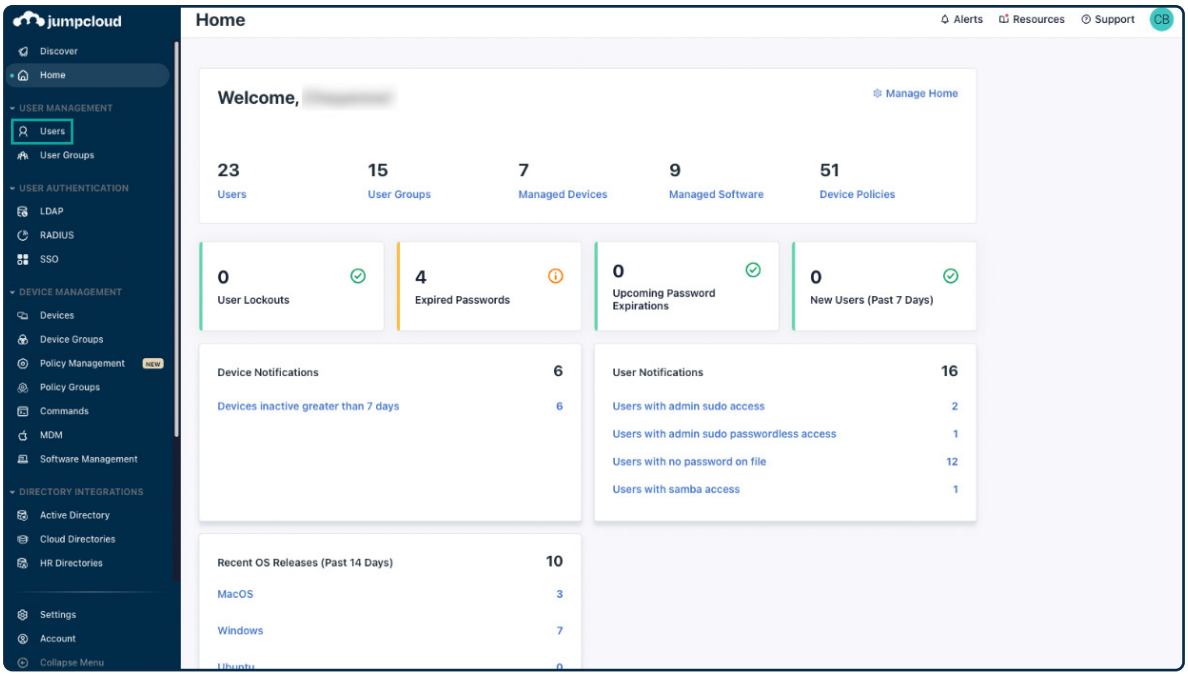


12. This pane will go through the entire user list and add them into JumpCloud. For larger batches over 100 users, this could take several minutes.
13. Once completed, as indicated by a green checkmark next to the user entry, you can download the confirmation CSV by selecting the download CSV button in the bottom right, or you can close the window by hitting the close button in the bottom right.



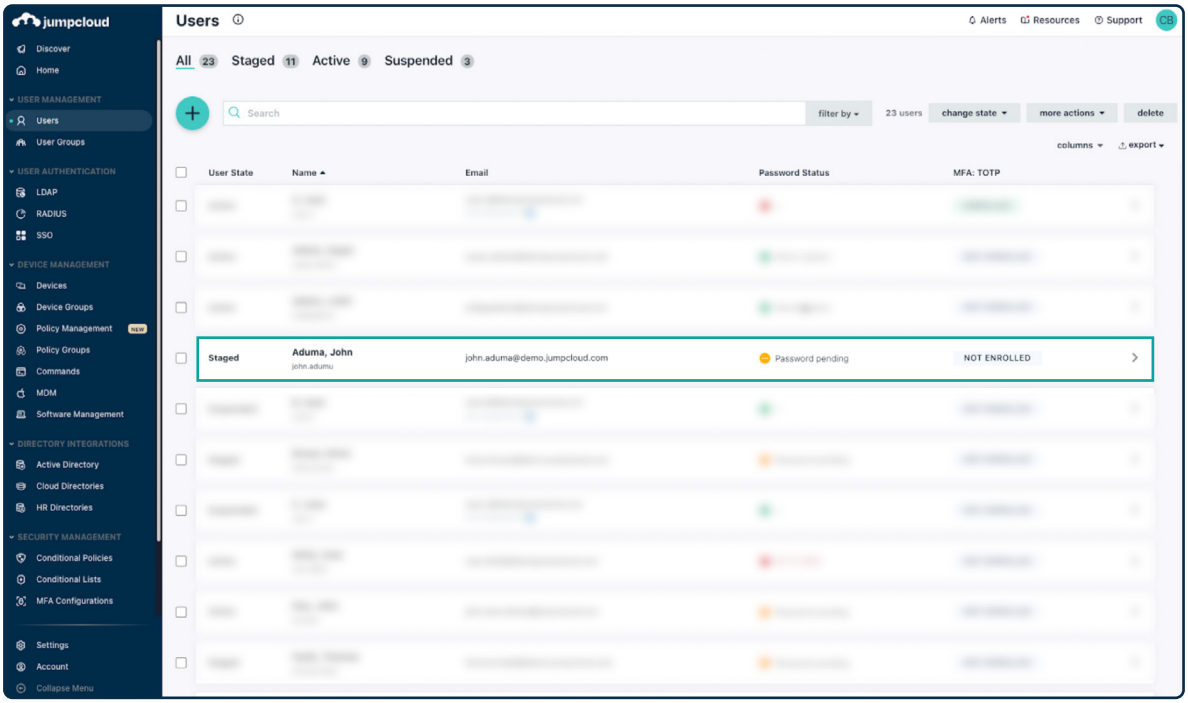
Navigate to Users Menu in JumpCloud Admin Portal

1. For User Management, navigate to Users in JumpCloud Admin Portal.

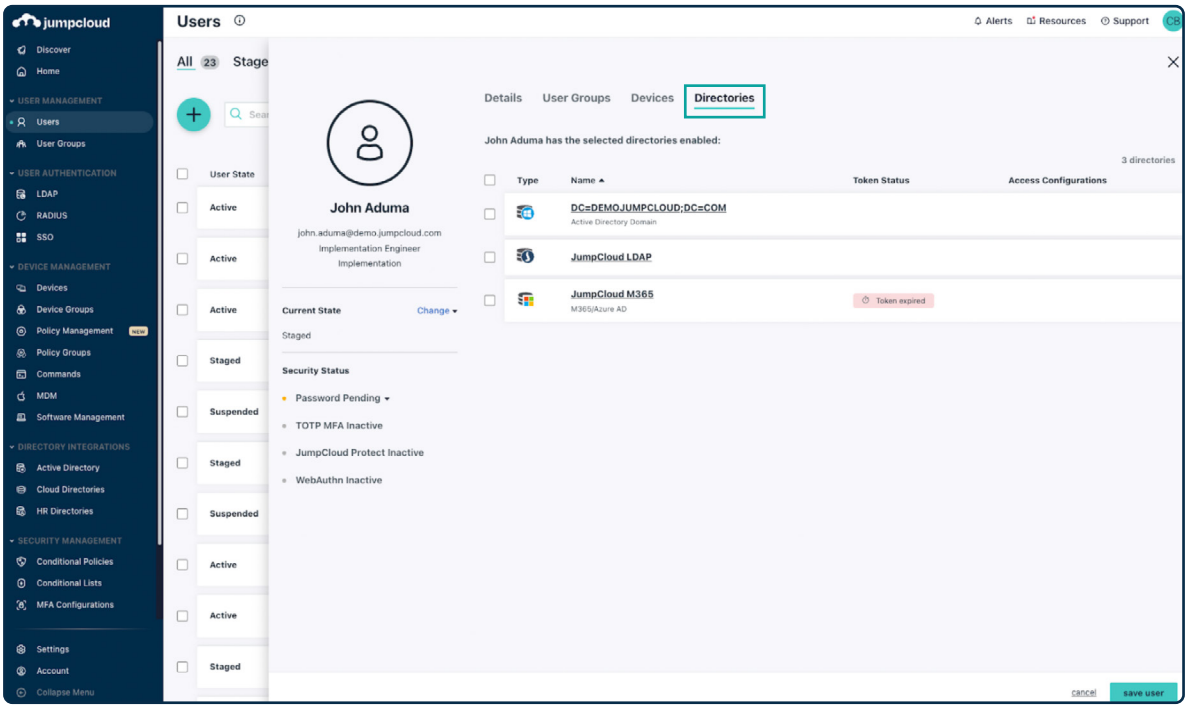


2. Select the newly imported users to access their information.

Note: You can select more than one user at a time.



3. Select the Directories tab for this user, and bind to the cloud directory.



Bind a User to the JumpCloud Directory

Please follow the instructions in these Knowledge Base icon articles:

- Binding JumpCloud Users to Microsoft 365
- Binding JumpCloud Users and Groups to Google Workspace

After the User Is Bound

1. The user will receive a Get Started email that requires them to set a JumpCloud password, and in turn update their cloud directory password.
2. The user will become active within JumpCloud.

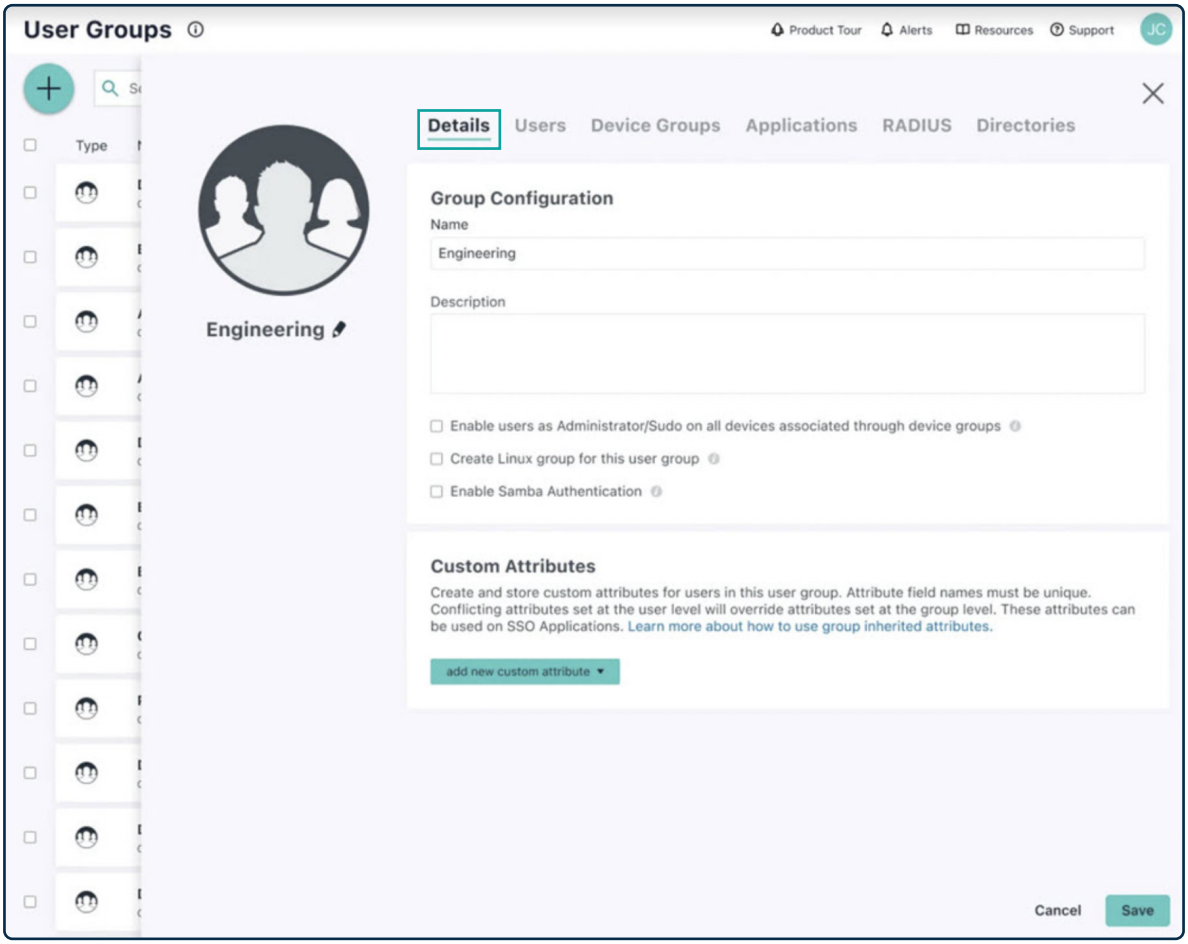
Create User Groups to Align with Org Layout

JumpCloud saves you time by letting you create groups of users, devices, and policies. Performing group-based assignments on resources can save you time.

User groups grant users access to resources, and connect the resources you want users to be able to access (applications, LDAP resources, networks, and more).

Complete the following steps to create a user group:

1. Log in to the JumpCloud Admin Portal.
2. Go to USER MANAGEMENT > User Groups.
3. Select (+). The Details tab appears by default.



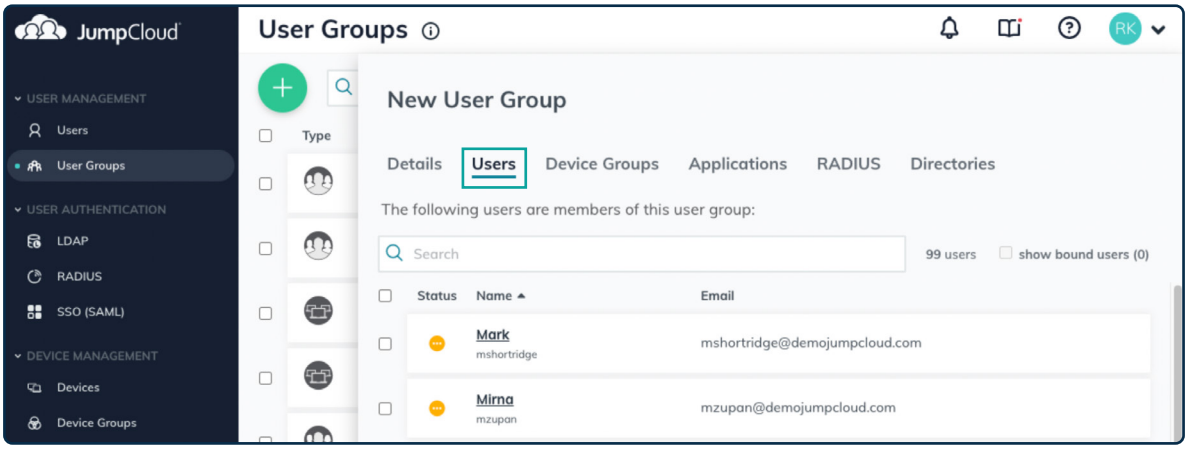
4. For the Name field, enter a description or purpose for the group name.
5. For the Description field, enter the purpose of the group.
6. (Optional) Under Custom Attributes, select add new custom attribute and choose an attribute.

Custom User Attributes

Adding Users to the Group

Complete the following steps to add users to the group:

1. On the New User Group panel, select the Users tab.
2. Select users from the list.
3. Select Save.



Additionally, JumpCloud has a tutorial, course, and module on User & Device Groups.

Enroll Users in MFA

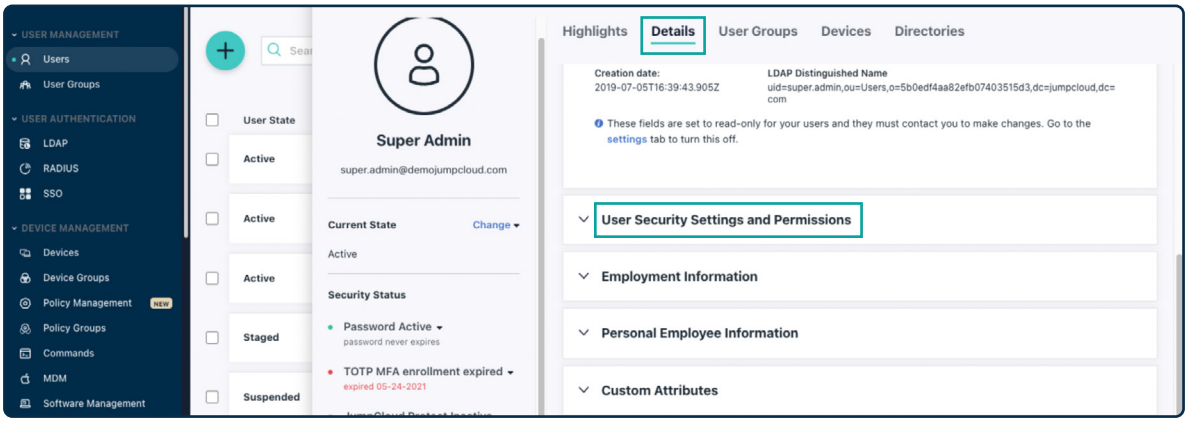
Use multi-factor authentication (MFA) with JumpCloud to secure user access to your organization's resources. Admins can use Verification Code (TOTP) MFA, Duo Security MFA, WebAuthn MFA, and Push MFA to strengthen security in their organization.

JumpCloud MFA Guide

Requiring Multi-Factor Authentication on an Individual User Account

To require MFA on an individual user account:

1. Go to User Management > Users.
2. Select a user to view their details. See Getting Started: Users.
3. In the User Security Settings and Permissions section, select Require Multi-Factor Authentication for User Portal.



4. Specify the number of days the user has to enroll in TOTP MFA before they are required to have MFA at login. You can specify a number of days between 1 and 365. The default value is 7 days. The enrollment period applies only to TOTP MFA and not to other MFA factors.
5. Select save user. After you save, users are notified in an email and are prompted to set up TOTP MFA the next time they log in to their User Portal.
6. During enrollment, the user's details indicate how much time remains on their enrollment period.
7. After the enrollment period expires, the user is locked out of the User Portal.

Phase 3: Devices

Identify Initial Devices to Test Deployment Methods

You can connect Mac, Windows, and Linux devices to JumpCloud by installing the JumpCloud agent. Check JumpCloud Agent Compatibility, System Requirements, and Impacts before you install an agent. After the agent is installed and connected to a device, you can:

- Remotely and securely manage the device and its user accounts and policies.
- Enable MFA.
- Create, modify, and disable local user accounts.
- Manage SSHD configuration (Linux).
- Enforce MFA on Windows, Mac, and Linux SSH.
- Execute commands.

Adding Windows and Linux Devices

To add a new device:

1. Log in to the JumpCloud Admin Portal.
2. Go to DEVICE MANAGEMENT > Devices.
3. Select the Devices tab.
4. Select (+). The New Device panel that appears contains various device tabs. Each tab includes information about downloading and installing the JumpCloud agent for that device's OS. You can also read the following about installing agents from the command line, template or system image, or the JumpCloud API.
5. (Optional) You can add the JumpCloud agent to your allow list with your antivirus vendor.
6. After installation completes, the agent checks in with JumpCloud and is active in the Admin Portal. You can view details about the device on the Device panel.

Watch this video about installing the agent remotely:


Enabling User Agent Installs

This Knowledge Base article shows you how to install the agent from the User Portal:


Installing the JumpCloud Agent from Your User Portal

Adding Apple Devices Using MDM

Configure JumpCloud as a Mobile Device Management (MDM) server by establishing a secure connection between Apple and JumpCloud using certificate-based authentication. You can use a push certificate to establish a secure connection between JumpCloud and Apple Push Notification service (APNs). MDM lets you securely and remotely configure your organization's devices, including updating software and device settings and monitoring compliance with your organization's policies.

In order to get the most out of JumpCloud with your Apple devices, you must enroll your devices in JumpCloud's MDM. If you do not enroll your macOS devices in MDM, you will not be able to use the following JumpCloud features:

- Policy Management
- Software Management
- Remote lock, Restart, Shutdown & Erase Security Commands
- Zero-Touch Enrollment
- OS Patch Management

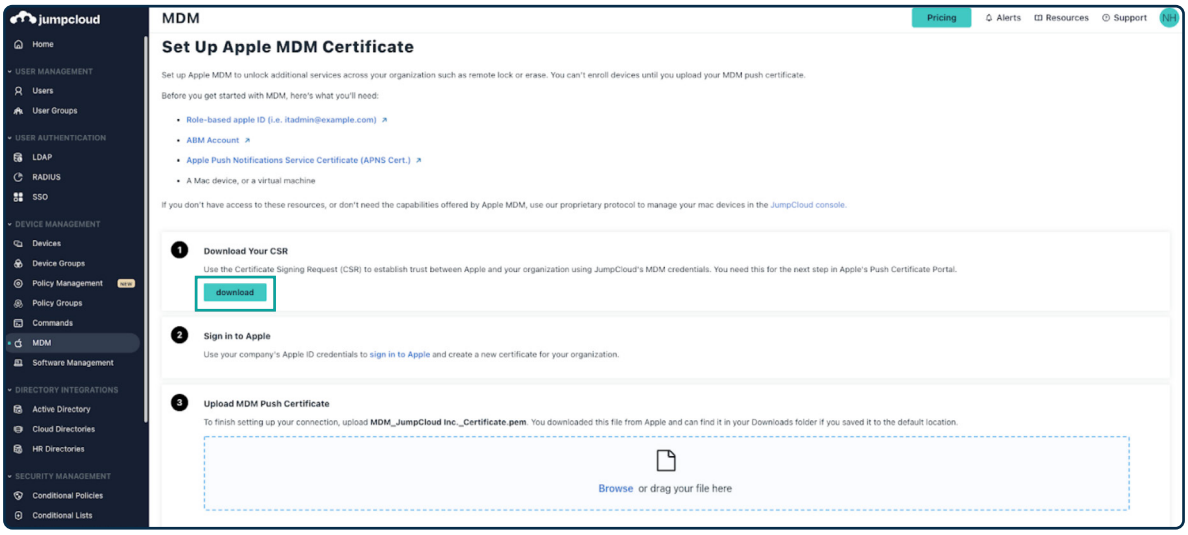
Note: As a prerequisite, you will need an Apple ID and password.

Configuring Your JumpCloud MDM Server

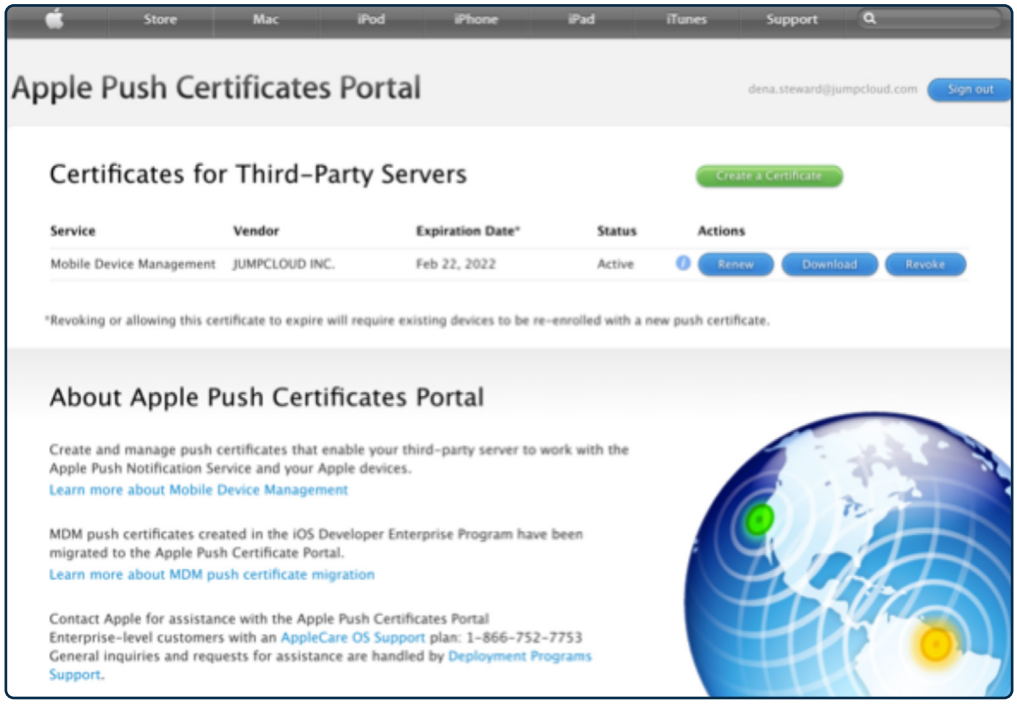
You must download a Certificate Signing Request (CSR) from the JumpCloud Admin Portal. The unique CSR contains your organization's MDM configuration within JumpCloud. Next, you log in to the Apple Push Certificate Portal and upload the CSR file. Apple validates JumpCloud's information and issues a push certificate with the public key included in the CSR. After you download the push certificate, you upload it to JumpCloud to create a secure connection. You need to renew the certificate yearly.

To configure MDM:

1. Log in to the JumpCloud Admin Portal.
2. Go to DEVICE MANAGEMENT > MDM.
3. On the MDM homepage, select Configure MDM.
4. Under Download Your CSR, select download and save the file.



5. Under Sign in to Apple, select sign in to Apple or log in to the Apple Push Certificate Portal.
6. Select Create A Certificate.



Enroll Devices into MDM using Mac MDM policy

After you configure JumpCloud's MDM server, you can enroll your macOS, iOS, and iPadOS devices in MDM. MDM lets you securely and remotely configure your organization's devices and update software and device settings.

There are a variety of ways to enroll company-owned and personal devices.

Enrollment Methods	Company-Owned macOS	Company-Owned iOS, iPadOS	Personal iOS, iPadOS
Automated Device Enrollment with Supervision	✓	✓	✗
Device Enrollment	✓	✓	✗
User Enrollment	✗	✗	✓ (iOS and iPadOS only)

You can enroll Apple devices in MDM with these enrollment methods:

- **Apple's automated device enrollment** – Remotely enroll company-owned macOS Apple devices in MDM so that you can securely configure and deploy devices. The device must be added to your Apple Business Manager (ABM) or Apple School Manager (ASM) account. Supervision can provide additional control over a device.

- **Device enrollment** – If a company-owned iOS device was not added to ABM or ASM, you can't use Apple's Automated Device Enrollment. Instead, you can go to the JumpCloud Admin Portal and scan the QR code or you can download the enrollment profile to enroll the device in MDM. Device enrollment is supported for devices that run iOS 13 and later.

- **User approval** – You can enroll personal iOS and iPadOS devices in MDM so that users can access company resources. These devices must run iOS 13 and later, and are owned by the user and enrolled by the user.

This Knowledge Base article covers these MDM enrollment methods:


Choosing an MDM Enrollment Method

For more information on MDM, check out this short course:

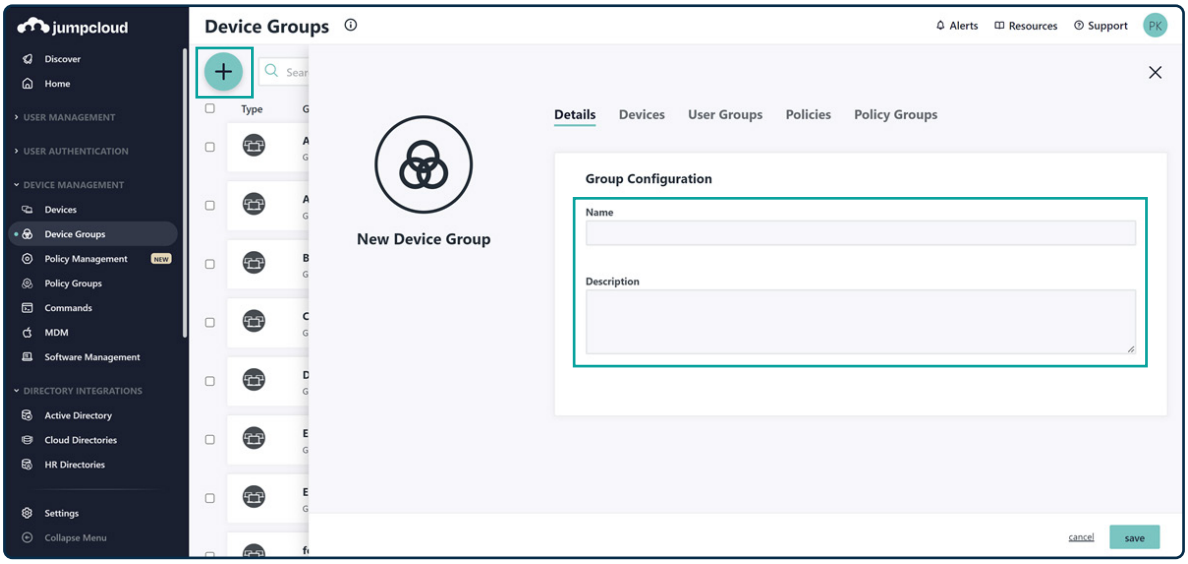

Intro to MDM

Assign Users to Their Respective Devices

View the article(s) relevant to the devices you are trying to connect to JumpCloud.


Connecting Users to Windows Devices


Connecting Users to macOS Devices



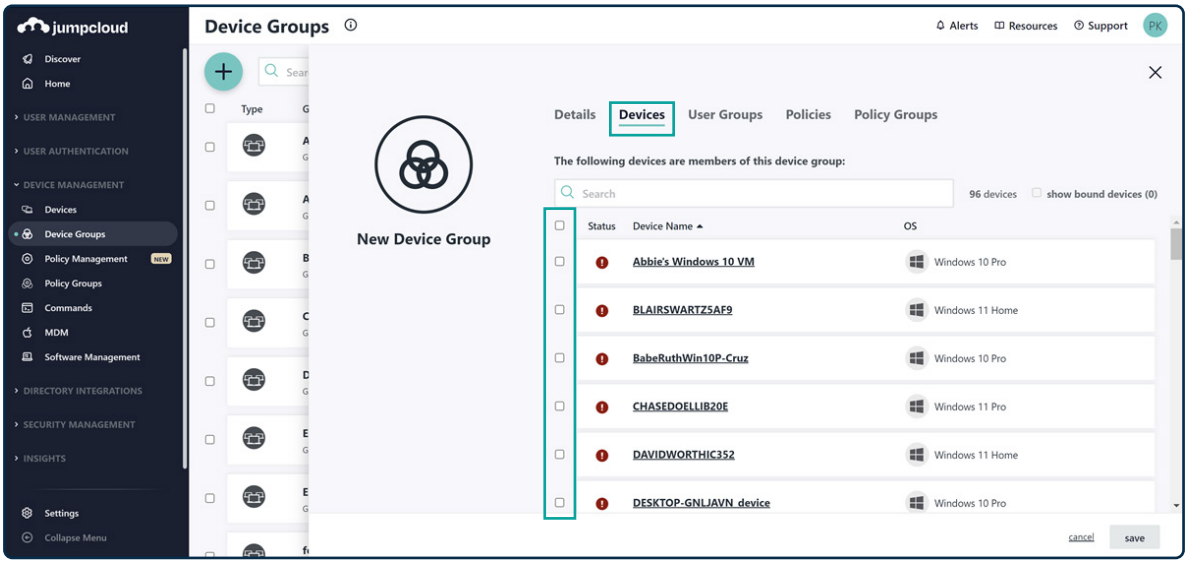
Create Device Groups

Complete the following steps to create a device group:

1. Log in to the JumpCloud Admin Portal.
2. Go to DEVICE MANAGEMENT > Device Groups.
3. Select (+) to add a new device group.
4. Enter the device group Name.
5. (Optional) Enter a short Description of the group's purpose.
6. Select save.

Adding Devices to the Device Group

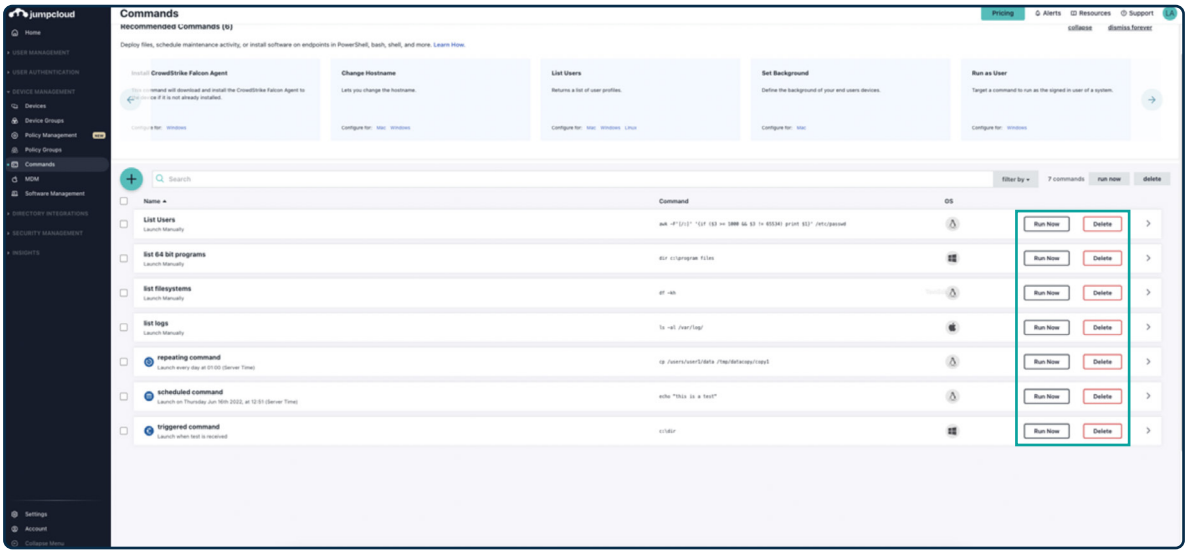
Complete the following steps to add devices to the device group:



Configure and Test Commands (if applicable)

You can run JumpCloud commands to execute scripts on fleets of machines through JumpCloud's system agent. You can deploy files, schedule maintenance activity, or install software on endpoints in PowerShell, Bash, Shell, and more. Commands can run across one or more devices in parallel and retrieve command results (including stdout, stderr, and exit codes).

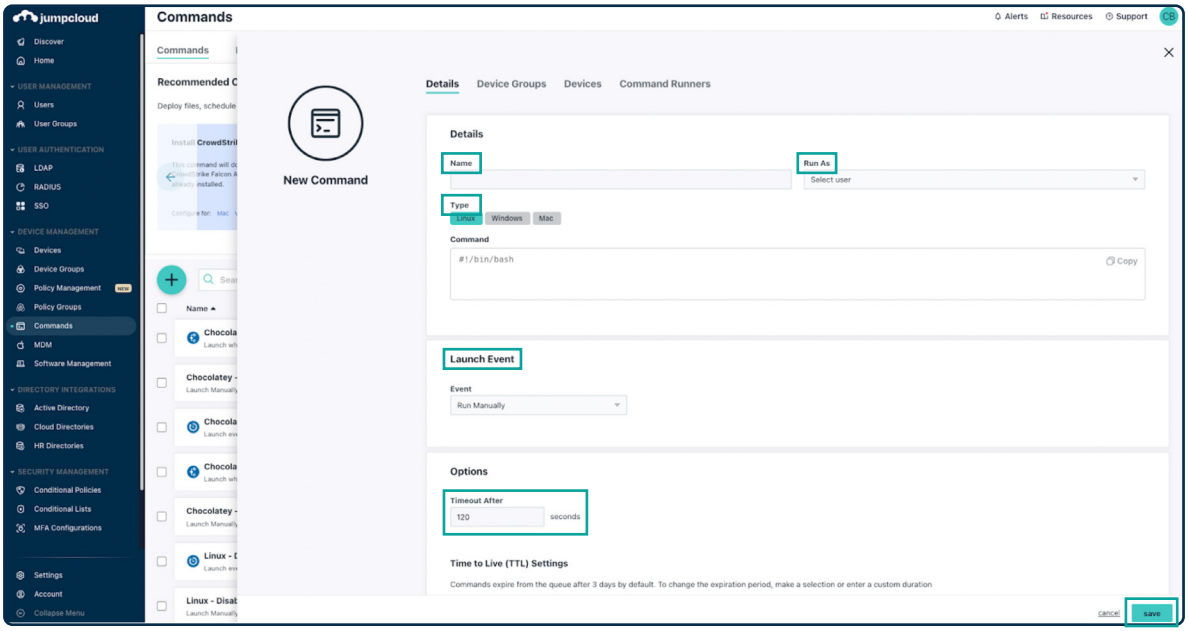
Commands let you quickly and easily automate tasks across multiple servers, launch those tasks based on a number of different types of events, and get full auditing of all command results. From the commands list, you can quickly run or delete a command using the Run Now or Delete buttons.



Create a New Command

To create a new command:

1. Log in to the JumpCloud Admin Portal.
2. Go to DEVICE MANAGEMENT > Commands.
3. In the Commands panel, select (+). The New Command panel appears.



4. On the Details tab, enter a name for the new command. This is the name shown in the sortable list view of commands.
5. Select users that you would like the command to Run As.
6. Select your operating device type: Linux, Windows, or Mac.
    - Linux only: Select the Run As user account to use to run the command.
    - Windows only: Commands will be run as the LocalSystem account and optionally can be run as Powershell.
7. Type or paste in a script. The script can be in any language that your servers can execute.
8. Select the Launch Event.
9. Enter a Timeout After value (in seconds). This determines how long the command can continue running before the agent will terminate it.
10. (Optional) Select Upload File to attach a file to the command (see below for details).
11. Select the Device Groups tab to set the specific device groups on which this command will execute.
12. Select the Devices tab to set the specific devices on which this command will execute.
13. (Optional) Select the Command Runners tab to select a user as a Command Runner with access to run the command. By default, admins can run commands on all devices.
14. Select save.

For more information on commands, check out this tutorial:

Commands

Enable MFA for Devices

JumpCloud gives organizations the power to layer multi-factor authentication (MFA) on top of nearly any resource you need to secure: Windows, Mac, Linux, applications, networks, infrastructure, and more.

If you'd like to use the JumpCloud Protect™ Push MFA mobile app for your MFA needs, see Logging into your Device with JumpCloud Protect Push MFA.

Check out this Knowledge Base article for more details on how to enable TOTP MFA:

 Enabling TOTP MFA for Devices

You can also view this tutorial:

 TOTP MFA for Devices

Configure Device Configurations/Policies for Mac, Windows, & Linux

You can save time by creating JumpCloud policies to remotely apply a set of rules to one managed device, a group of devices, or your entire fleet. Applying policies lets you customize these types of managed devices and make them more secure:

- Windows
- MacOS
- iOS and iPadOS
- Linux

You can also create a policy group, adding multiple policies to it, and apply the policy group to multiple devices or device groups. For example, you create a policy group that uses JumpCloud's Lock Screen policy to automatically turn on the screen saver if a device is inactive for a specific amount of time. The policy group could also contain a policy to control Apple App Store purchases to allow only updates to existing apps. A policy group is especially useful in implementing security or compliance-related issues on managed devices.

Every policy contains these sections:

- **Policy name** – You can customize this or keep the default. Your policy names must be unique. (All references to policies in this documentation use the default name.)
- **Policy description** – Provides more information on the policy's function and lists the specific OS versions this policy supports.
- **Policy behavior** – Describes the device behavior when the policy is applied.
- **Policy activation** – Lists any additional steps you must take after creating the policy and saving it. After you complete these additional steps, the policy takes effect.
- **Settings** – These options vary depending on the policy and allow you to further define the behavior you want to enforce on a device.

After you apply and save a policy, the system agent checks in with JumpCloud. The agent on an individual device continuously compares the local policy with the policies you set in JumpCloud. If a user modifies the device policy, JumpCloud automatically modifies the device's policy to comply with the JumpCloud policy. This process ensures that JumpCloud policies and local devices are kept in sync.

Check out this tutorial to learn more about configuring policies:

 Configuring Policies

Configure Full-Disk Encryption for Mac and Windows

Mac

You can use this policy to remotely enforce FileVault on macOS devices and easily view Recovery Keys. FileVault full-disk encryption (FileVault 2) helps prevent unauthorized access to the information on your user's startup disks. FileVault 2 uses XTS-AES-128 encryption with a 256-bit key.

After you enforce a FileVault policy, your users need a secure token to enable it. The advent of Apple File Systems (APFS) in macOS 10.13 changed the way Apple manages FileVault encryption keys. To secure and provide access to encryption keys required for FileVault decryption, Apple introduced Secure Tokens. Ensure your users have Secure Tokens by following the instructions in Installing and Using the Service Account for macOS.

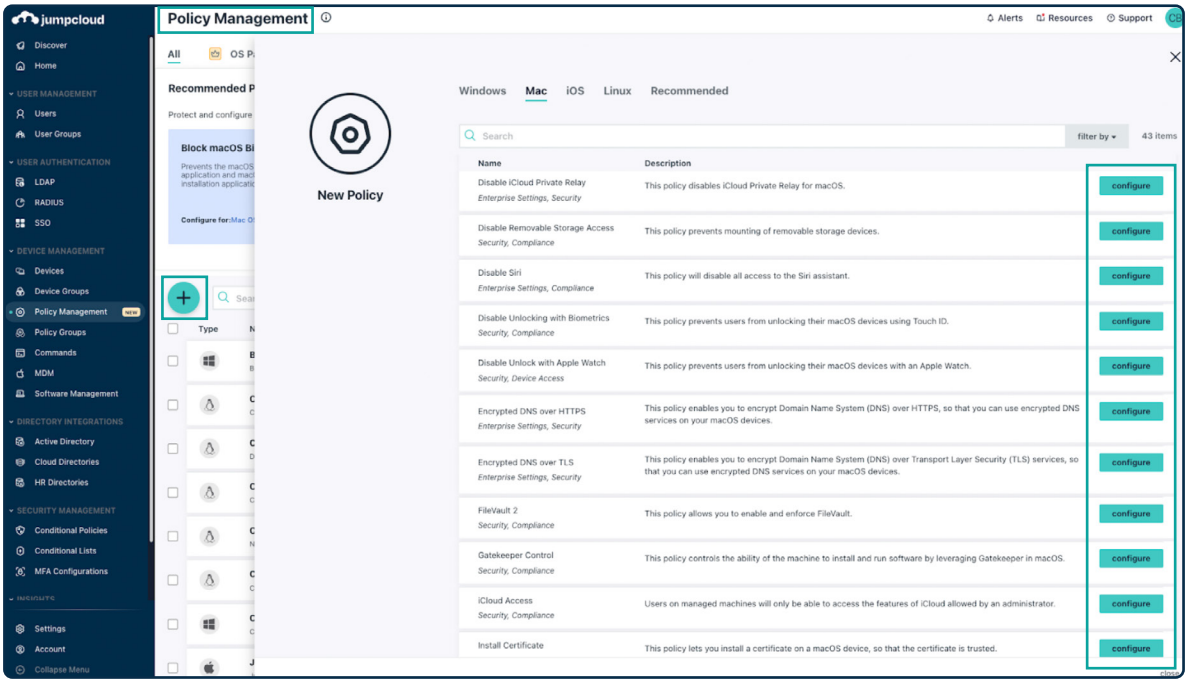
Administrator Experience

When you create a FileVault policy, you can enable and configure the following settings:

- **Show the FileVault Recovery Key to the user when enabled**: When this option is selected, the user sees the Recovery Key and can store it in a safe place.
- **Do not prompt the user to enable FileVault at logout**: There are two possible prompt locations for the user to enable FileVault, at login and at logout. With this option selected, the user is only prompted to enable FileVault when they log in.
- **Number of times the user can bypass enabling FileVault**: You can let the user postpone enabling FileVault for the number of times you enter in this field. When the value you enter has been exceeded the user is forced to enable FileVault before they can login to their device.

To create a FileVault 2 policy:

1. Log in to the JumpCloud Admin Portal.
2. Go to DEVICE MANAGEMENT > Policy Management.
3. Select (+).
4. In the New Policy panel, select the Mac tab.
5. Next to the FileVault 2 policy, select configure.



6. On the New Policy panel, optionally enter a new name for the policy, or keep the default. Policy names must be unique.
7. Select or clear the Show the FileVault Recovery Key to the user when enabled option.
8. Select or clear the Do not prompt the user to enable FileVault at logout option.
9. If you select the Do not prompt the user to enable FileVault at logout option, in Number Of Times The User Can Bypass Enabling FileVault, enter a number greater than zero.
10. Select the Device Groups tab. Optionally, select one or more device groups to apply this policy to. For device groups with multiple OS member types, the policy is applied only to the supported OS.
11. Select the Devices tab. Optionally, select one or more device groups to apply this policy to.
12. Note in the POLICY ACTIVATION that a user will need to log out and log back in for the policy to take effect.
13. Select save policy.

After you save the policy and the user logs out and back in, the policy takes effect on active devices in near-real time, but could take up to a few minutes. The policy is enforced on any inactive devices the next time they become active.

In the Admin Portal, you can check the policy to see if it's successfully applied. If FileVault is already enabled on the device when the policy is applied, the following behavior occurs:

- JumpCloud rotates the Recovery Key on the device.
- Key rotation may be immediate, but may also take up to one hour.
- In order for JumpCloud to rotate the Recovery Key, the JumpCloud Service Account must be present on the device.
- Once the Recovery Key is successfully rotated, JumpCloud records the new Recovery Key in the Admin Portal on the device's details.

At this point, FileVault is now completely enabled on the devices where you applied this policy. You can view the Recovery Key for the device, and users can't disable FileVault.

Here is a tutorial on FileVault management:

 FileVault

Windows

BitLocker is an encryption feature built into computers running Windows. It secures your data by scrambling it so it can't be read without using a recovery key. BitLocker differs from most other encryption programs because it uses your Windows login to secure your data; no extra passwords necessary. Once you're logged in, you can access your files normally. After you log out, everything's secured.

JumpCloud's BitLocker policy lets administrators remotely enforce BitLocker Full Disk Encryption on JumpCloud managed devices.

Administrator Experience

Administrators can create a policy to force BitLocker encryption on managed devices and easily view Recovery Keys.

To create a BitLocker policy:

1. Log in to the JumpCloud Admin Portal.
2. Go to DEVICE MANAGEMENT > Policies.
3. Select (+).
4. On the New Policy panel, select Windows.
5. Find the BitLocker Full Disk Encryption policy, then select policy.
6. (Optional) Select Encrypt All Non-Removable Drives to encrypt all fixed drives on the devices the policy will be enforced on.
7. Apply the policy to a Group of Devices in the Device Groups list, or to an individual device in the Devices list.
8. Select save policy.

After an administrator saves the policy, JumpCloud enables BitLocker on the devices where this policy is applied.

- When the device's volume is completely encrypted, you can view a Recovery Key that can be used to unlock all encrypted drives on that device.
- The drive isn't fully encrypted until the policy result shows that it was applied successfully in the Administrator Portal.
- Removing this policy doesn't disable BitLocker or remove key protectors.

The administrator must wait for the following actions to happen before viewing Recovery Keys:

1. A user sees a prompt requesting that they restart their device to enable BitLocker.
2. On the Administrator Portal the Policy Status is updated to BitLocker Not Protected - Encryption has been enabled. Device drive encryption will begin on the next boot.
3. The user restarts their device.
4. BitLocker begins encrypting the user's volume.

After the drive is completely encrypted, Administrators can view the Recovery Key:

1. In the Administrator Portal, go to DEVICE MANAGEMENT > Policy Management.
2. Select the BitLocker Full Disk Encryption policy and select the Devices tab to display a list of encrypted devices.
3. From the displayed list, locate your desired device, and select "View Key" to display the system's Recovery Key. Users who are not administrators on the device can't disable BitLocker.

Here is a tutorial on BitLocker Policy:

 BitLocker Policy

For more information on these topics, please refer to the following courses:

 Adding Windows and Linux Devices

 Adding Apple Devices using MDM

 Enabling MFA

Phase 4: SSO

Configure SAML App Integration (if applicable)

JumpCloud's Directory-as-a-Service gives your organization's employees access to supported applications using their JumpCloud credentials. This centralized method of identity uses one set of employee credentials to gain access to all applications, versus creating individual logins for each application. This single sign-on (SSO) workflow lets the JumpCloud-managed identity be asserted via the SAML protocol to an application.

Using SAML (SSO) Applications with JumpCloud

1. Select an App

Select an application you want to connect with JumpCloud through SAML 2.0-based SSO.

You may see some applications in the list with a beta flag. We're currently evaluating these connectors in various real-world environments so we can gather feedback to enhance their performance.

You may see some applications with a JIT provisioning label. This signals that you can provision users to that application using Just-In-Time provisioning. Learn about SAML-supported JIT provisioning.

Some applications use a shared login with the services they provide. For example, the Atlassian connector provides SSO to JIRA, Confluence, and Bitbucket. When you search for these applications, the Atlassian connector shows up in the search results because it's the connector the applications share a login with.

You can connect on-prem/legacy applications that use LDAP to JumpCloud's LDAP services. See Using JumpCloud's LDAP-as-a-Service.

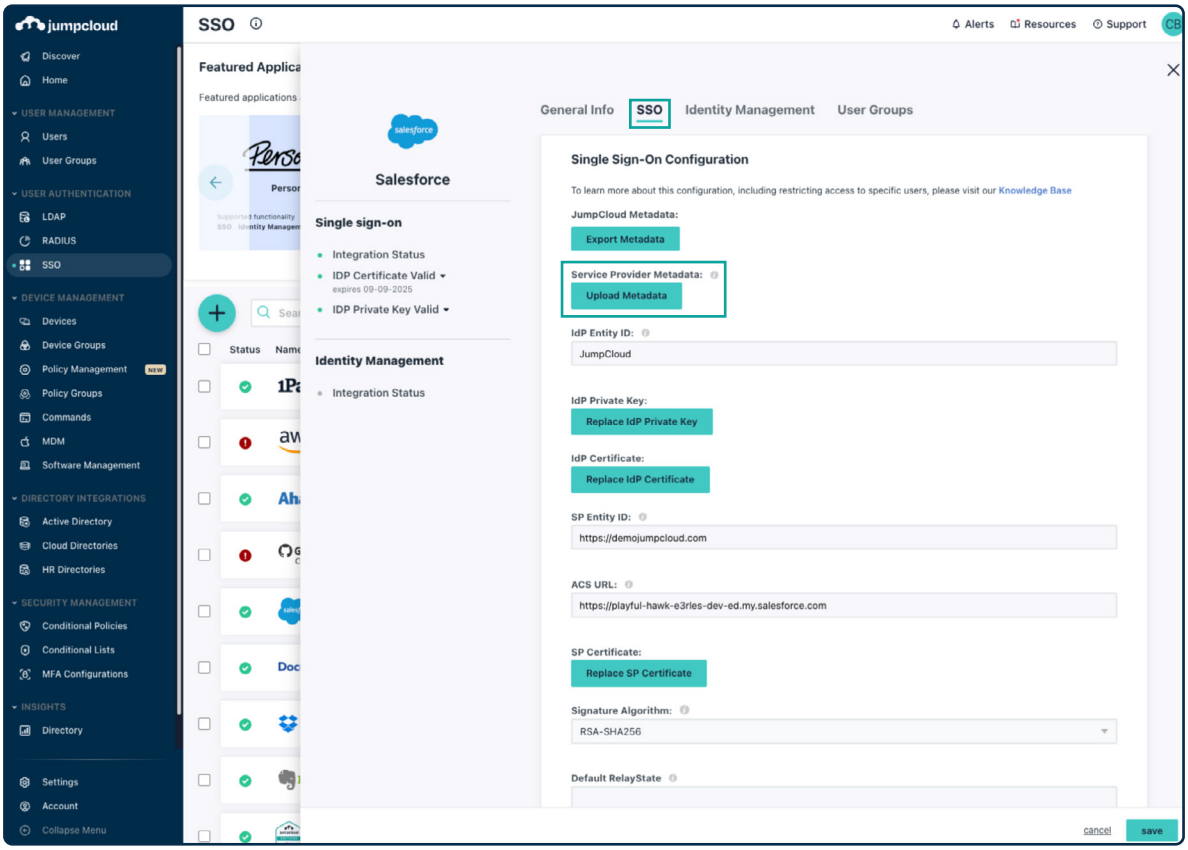
2. Configure Your App

You can set various SAML configurations with JumpCloud acting as the app's "IdP," or identity provider. Each application connector has explicit instructions required to establish the connection. Refer to an application's SAML/SSO connection documentation for information on setting up your application to integrate with JumpCloud.

3. Upload a Metadata File

You can upload service provider application XML metadata files to populate connector attributes for applications.

To apply a metadata file for an application you're connecting, select Upload Metadata. Navigate to the file you want to upload, then select Open. You'll see a confirmation of a successful upload.



Tip: Be aware that if you upload more than one metadata file, you'll overwrite the attribute values applied in the previously uploaded file.

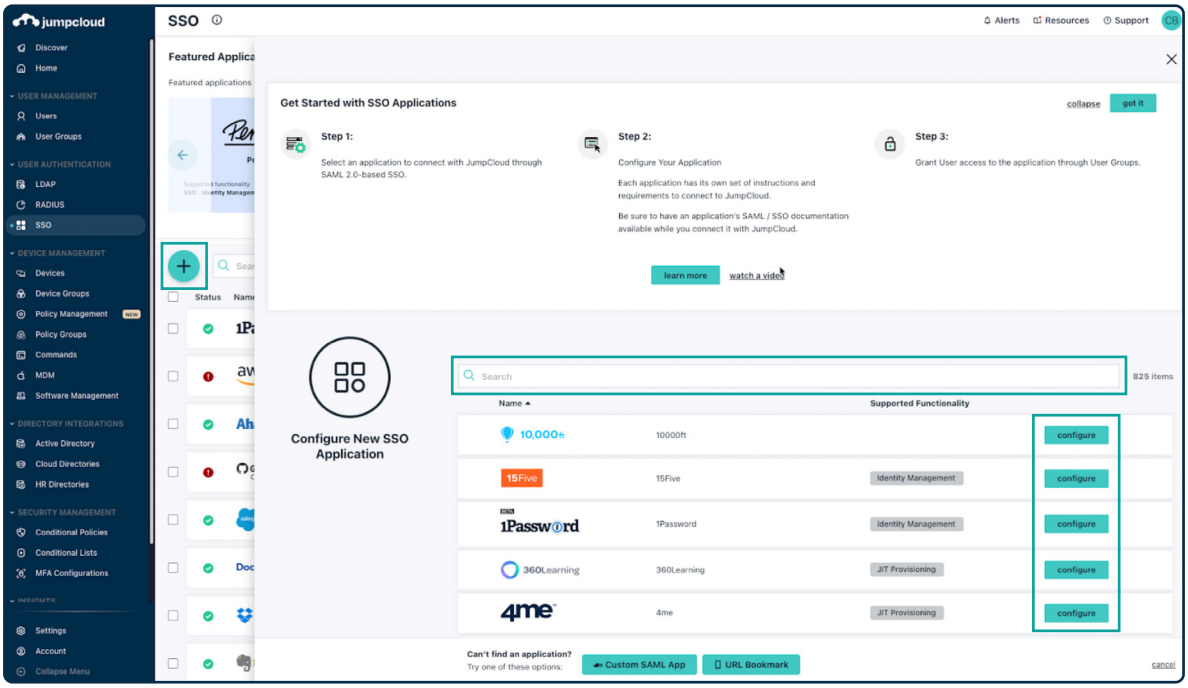
4. Connect Your App to a User Group

After you connect the application to JumpCloud, you can connect it to user groups. Members of connected groups gain access to the application through SAML. They see the application icon in the User Portal in Applications. Many service provider applications allow users to log in from their application. If users log in from the application, they are redirected to JumpCloud for SAML authentication.

Setting Up SAML-Based SSO with an Application

To connect an application to JumpCloud:

1. Log in to the JumpCloud Admin Portal.
2. Go to User Authentication > SSO, then select (+). The Configure New Application panel appears.
3. Search for an application by name using the search bar at the top of the panel.
4. When you find the application you want to connect, select configure.



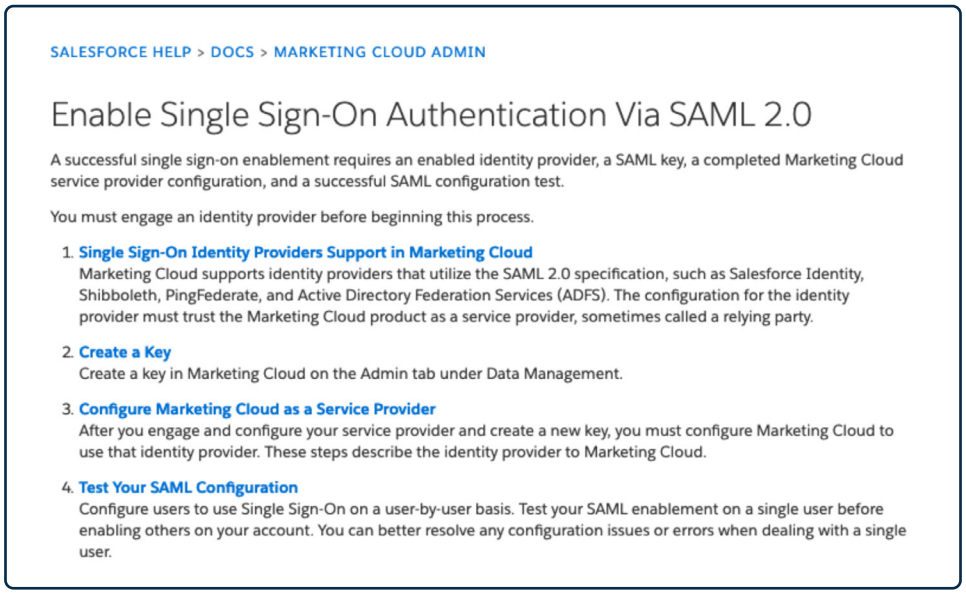
If there isn't a connector for an application you want to connect to JumpCloud, check out this Knowledge Base article to learn how to connect that app to JumpCloud using the SAML 2.0 Connector:

Single Sign On (SSO) with SAML 2.0 Connector (Custom SAML App)

Configuring Authentication from the Application Service Provider

The service provider (SP) typically provides SAML configuration parameters to set up SSO from a compatible IdP like JumpCloud.

The following image shows Salesforce instructions for setting up the Marketing Cloud for SAML SSO.

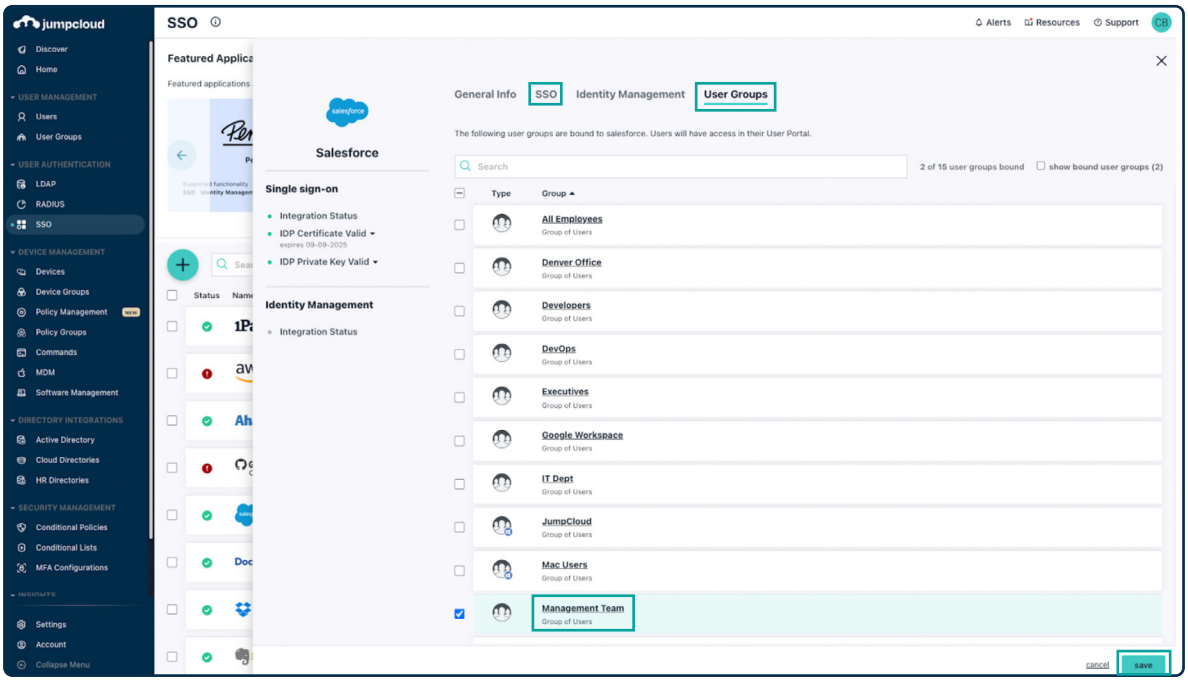


Managing Employee Access to Applications

Users are implicitly denied access to all JumpCloud resources, including applications. JumpCloud admins must explicitly grant access to SSO applications through the use of user groups.

To grant access to a user group:

1. Log in to the JumpCloud Admin Portal.
2. If you haven't already created a user group, create a new group.
3. If the group exists, in the Admin Portal, go to User Authentication > SSO.
4. Select the SSO application.
5. On the Application panel, select the User Groups tab.
6. Select the user group, then select save.



For more information on SSO, watch this tutorial:

Configuring an SSO Application

End-User Experience

To further understand the user experience, refer to the following Knowledge Base articles.

After you configure both the IdP and SP for SSO, employees can access the applications in two ways:

IdP-Initiated – Access from the JumpCloud User Portal

SP-Initiated – Access directly from the application

Configure JIT App Integration (if applicable)

Just-in-Time (JIT) provisioning lets you onboard new users to single sign-on (SSO) applications more efficiently. When JIT provisioning is in use, you don't have to manually create new user accounts in an application. Instead, a user account is created when a user authenticates into an application for the first time using SSO. JumpCloud supports the use of JIT provisioning by including the user attributes a service provider requires for account creation.

Benefits

JIT provisioning lets you automate user provisioning to SSO applications, giving you more time to focus on higher value projects. End users also benefit by gaining faster access to the SSO applications they need to do their jobs.

How JIT Provisioning Works

The typical JIT provisional workflow looks like this:

1. Enable JIT provisioning in the service provider.
2. Configure the appropriate SAML SSO connector in the identity provider and service provider, making sure to set up the JIT required user attributes.
3. Authorize a user's access to the application in the identity provider.

To complete the provisioning process, a user logs in to the application using SSO. The SAML assertion passes from the identity provider to the service provider, and gives the service provider the information it needs to create the user account.

This Knowledge Base article will walk you through the steps of SAML supported JIT provisioning:

SAML Supported JIT Provisioning

Configure SCIM App Integration (if applicable)

JumpCloud Identity Management Connectors

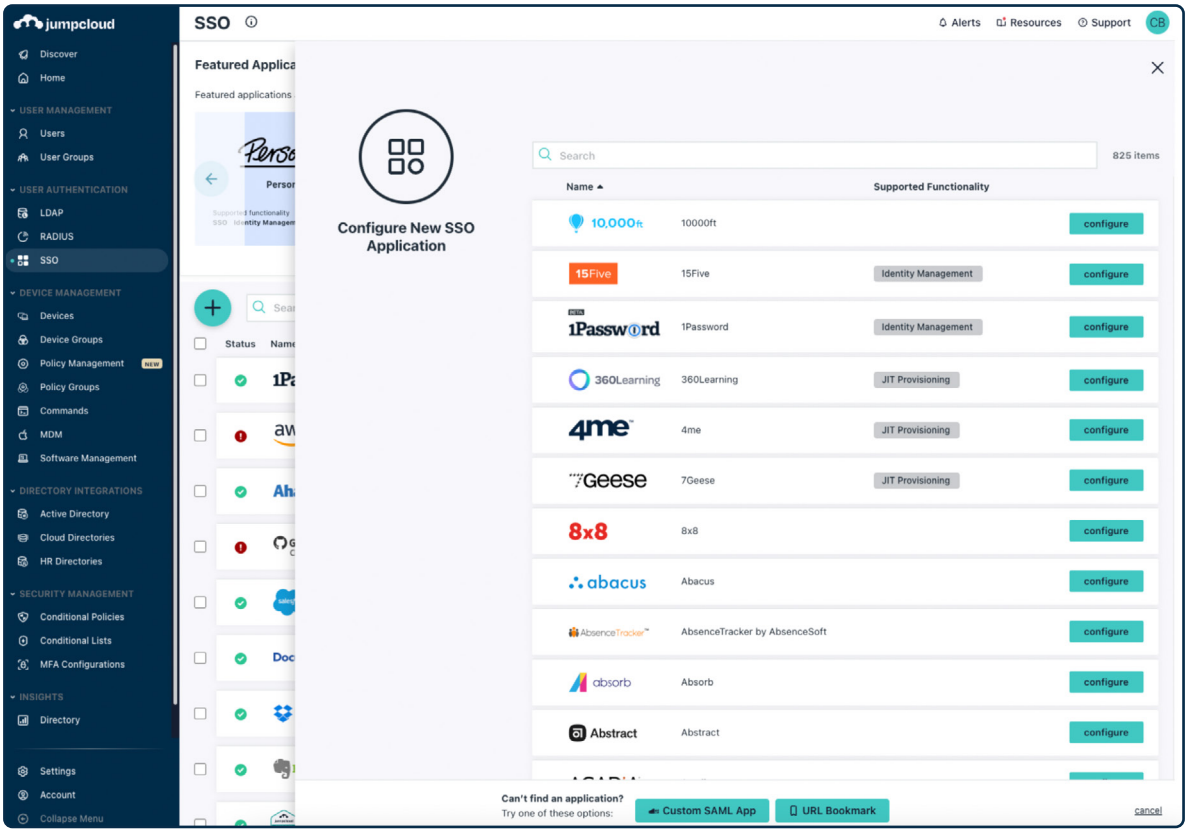
These integrations allow you to automate and centralize user and group management, depending on the application's group management support, through the full lifecycle from your JumpCloud Admin Portal. Connect the applications your organization uses with JumpCloud. Our Identity Management Connectors manage application user accounts through the Identity Management (SCIM) protocol.

As your company grows and experiences employee churn, you can easily manage application user accounts with Identity Management Connectors. After you integrate an application with JumpCloud, depending on an application's Identity Management action support, you can provision, update, and deprovision users.

To find applications you can integrate with JumpCloud using Identity Management Connectors:

1. Log in to the JumpCloud Admin Portal.
2. Go to USER AUTHENTICATION > SSO. If you've connected any applications with JumpCloud, you will see them in this list.
3. To connect a new application, select (+).

Applications that you can integrate with JumpCloud through an Identity Management Connector can be found on the Configure New Applications panel. The supported ones have a User Export listed under the Supported Functionality column.



Phase 5: RADIUS

Create a RADIUS Endpoint in JumpCloud

JumpCloud's cloud-based RADIUS service extends your organization's user JumpCloud credentials to your Wi-Fi and other resources that support the RADIUS protocol. Each RADIUS server you add to JumpCloud can be connected to user groups, segmenting which users can access specific resources.

By leveraging your users' JumpCloud credentials for your network, you can ensure secure access and easy provisioning/deprovisioning to users. You'll also get access to prebuilt, preconfigured, and fully managed RADIUS servers.

You can proceed to the instructions below or follow along with this course that guides you through adding RADIUS as a Server:

Configuring RADIUS

Add a RADIUS Server

1. Log in to the JumpCloud Admin Portal.
2. Go to RADIUS.
3. Select (+). The New RADIUS server panel appears.
4. Configure the RADIUS server:
    - Enter a name for the server. This value is arbitrary.
    - Enter a public IP address from which your organization's traffic will originate.
    - Provide a shared secret. This value is shared with the device or service endpoint you're pairing with the RADIUS server.

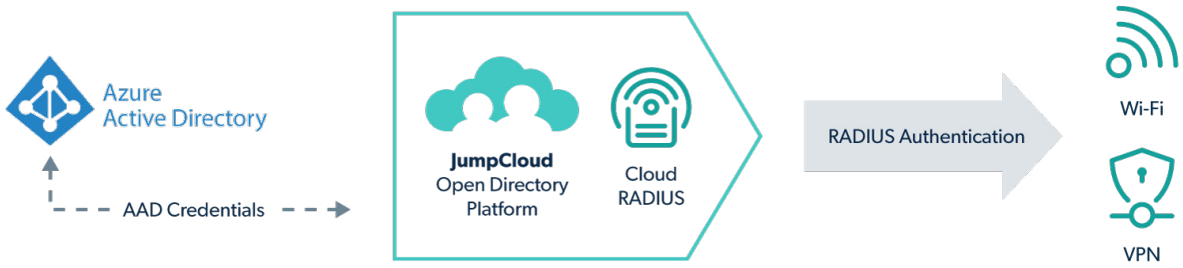
Set Up Primary Authentication

1. To select how your users will authenticate into this RADIUS server, select the Authentication tab and choose an Identity Provider from the dropdown menu.

    If the selection is Azure AD, users will be able to access this RADIUS server using their existing Azure AD credentials. MFA cannot be configured when Azure AD is the identity provider.

    Important:

    - Once Azure AD is selected and confirmed, this selection cannot be changed without deleting this RADIUS configuration and starting over.
    - Azure AD doesn't pass the user's password to JumpCloud, so the user remains in a Password Pending status. If an Azure AD organization is using JumpCloud exclusively for RADIUS, admins do not require users to create a password in JumpCloud, so the Password Pending status can be ignored.



2. If the selection is JumpCloud, the multi-factor authentication (MFA) configuration section will be available.

Configure Your Wireless Access Point (WAP)

Check out this Knowledge Base article to learn more about configuring your WAP.

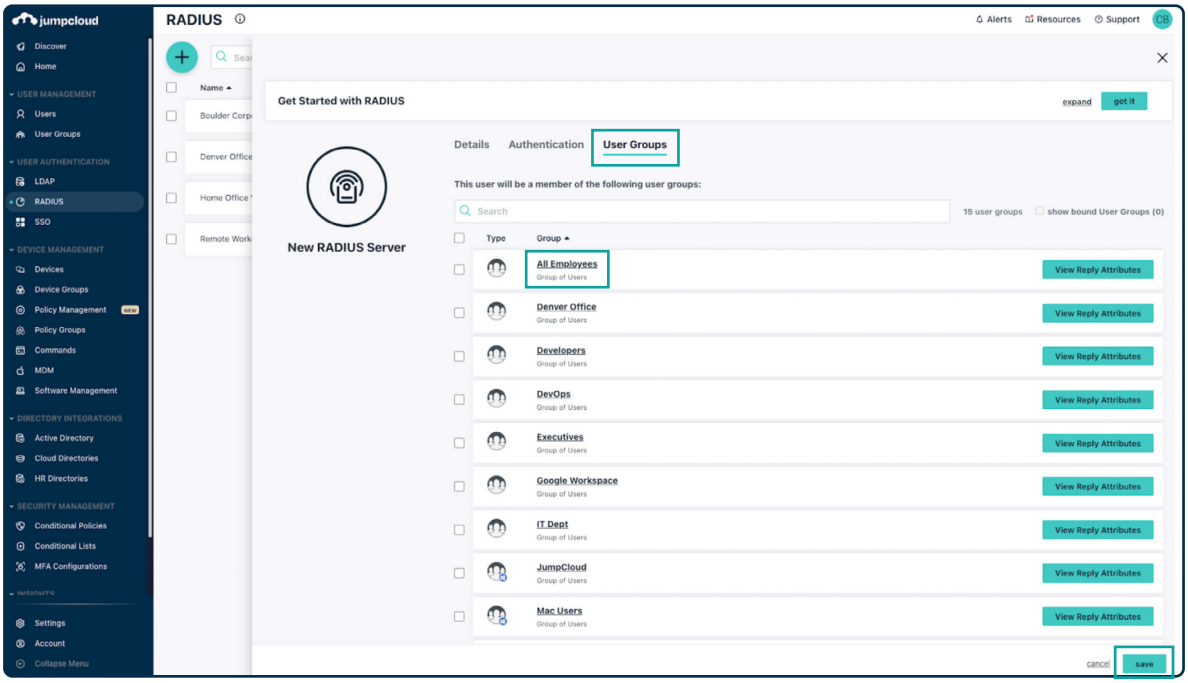
Configuring a Wireless Access Point (WAP), VPN, or Router for JumpCloud's RADIUS

Configure Multi-Factor Authentication for the RADIUS Server

1. Select the Authentication tab. If using JumpCloud as the identity provider, the MFA configuration section will be available.
2. Toggle the MFA requirement option to "On" for this server. This option is "Off" by default.
3. Select Require MFA on all users or only require MFA on users enrolled in MFA.
   - If selecting Require MFA on all users, a sub-bullet allows you to exclude users in a TOTP enrollment period, but this does not apply to JumpCloud Protect (users in a TOTP enrollment period who are successfully enrolled in Protect will still be required to complete MFA).
   - If JumpCloud Protect is not yet enabled, users can select the Enable Now link.

Grant User Groups Access to the RADIUS Server

1. To grant access to the RADIUS server, select the User Groups tab then select the appropriate groups of users you want to connect to the server.



2. Select save.

Note: Users who are granted access to a RADIUS server that will authenticate with the IdP of Azure AD must be imported into JumpCloud and then assigned to a User Group.

Enable MFA for RADIUS Networks (if applicable)

To configure RADIUS MFA for an existing server:

1. Log in to the JumpCloud Admin Portal.
2. Go to User Authentication > RADIUS.
3. Select an existing RADIUS server.
4. Configure TOTP multi-factor authentication for the RADIUS server:
    - Toggle the MFA requirement for this RADIUS server option to "On" to enable MFA for this server. This option is disabled by default.
    - Select Require MFA on all users or only require MFA on users enrolled in MFA. If selecting Require MFA on all users, a sub-bullet allows you to exclude users in a TOTP enrollment period.
5. Select save.

The RADIUS MFA settings have been updated from a previous version:

- Require MFA on all users (previously was Challenge all users, including during an enrollment period)
- Require MFA on all users, but exclude users in TOTP enrollment period (previously was Challenge all users, unless they are in an enrollment period)
- Only require MFA on users enrolled in MFA (previously was Challenge active TOTP MFA users)

Configure RADIUS Reply Attributes for User Groups (if applicable)

Get the strength and security of RADIUS without building, maintaining, or monitoring physical servers. It's quick to roll out managed RADIUS to your organization to authenticate users to Wi-Fi, VPNs, switches, and network devices securely. Read this article to learn how to use functions in the JumpCloud PowerShell module to configure RADIUS reply attributes like VLAN tagging for user groups.

Configure RADIUS Reply Attributes for User Groups in the API

Phase 6: LDAP & Samba

Create LDAP Service Account with BindDN Privileges

Cloud-hosted LDAP gives you the power of the LDAP protocol with none of the usual setup, maintenance, or failover requirements of traditional LDAP implementations. All you need to do is point your LDAP-connected endpoints to JumpCloud and you're on your way. Read this article to learn how to get started with cloud LDAP.

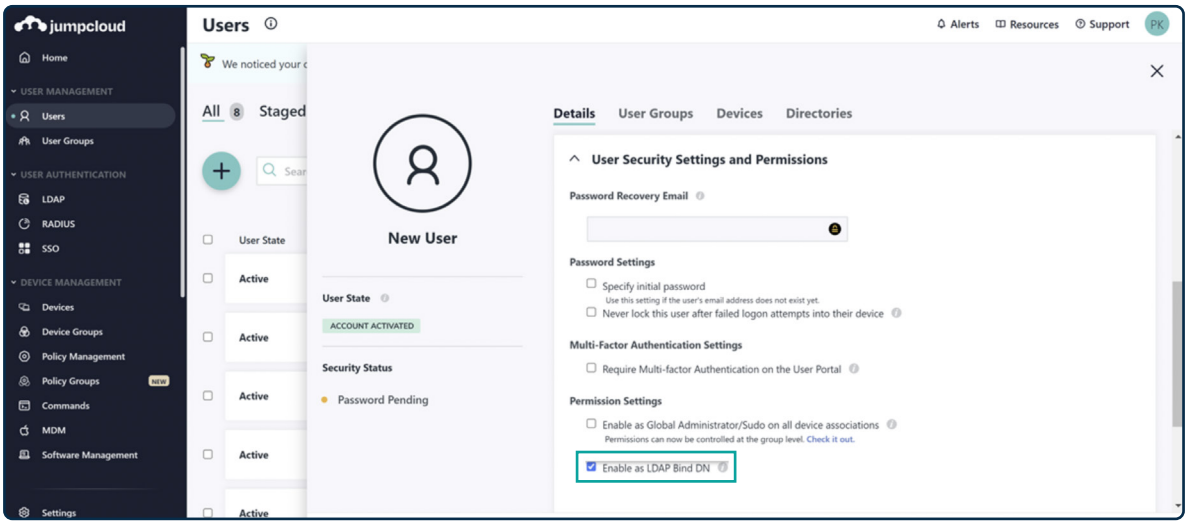
To familiarize yourself with configuring LDAP, proceed to the instructions below or watch this video:

Configuring LDAP

The LDAP binding user is created to allow the application to gain access to the LDAP directory in order to facilitate authentication requests when a regular LDAP user is attempting to log in. JumpCloud does not support anonymous binds. When a user is designated as the Bind DN, they are automatically bound to the JumpCloud LDAP directory.

To create a binding user:

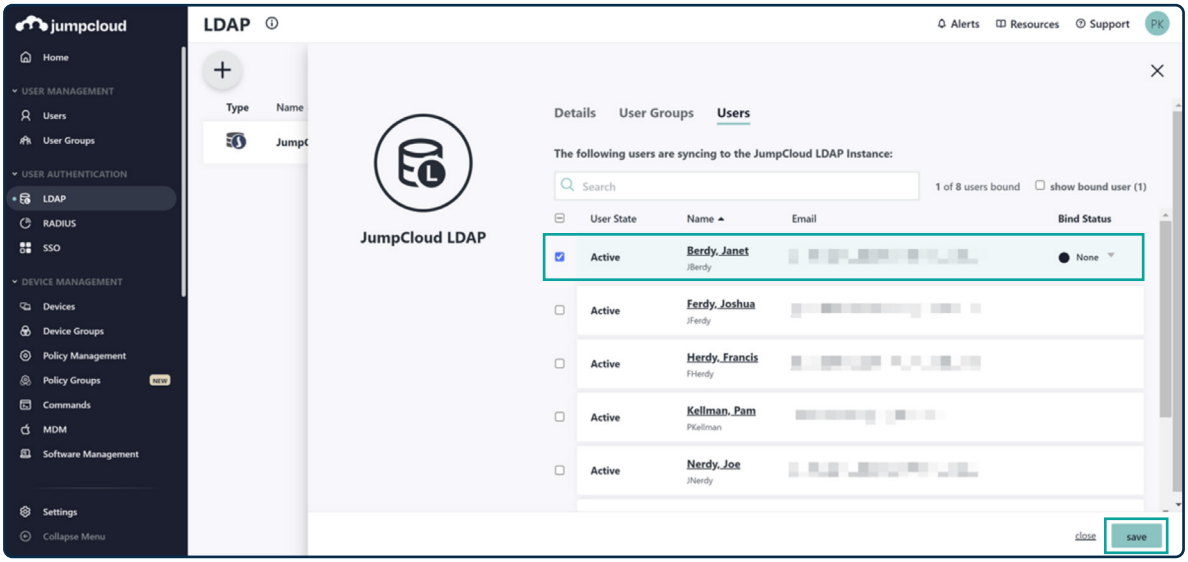
1. Log in to the JumpCloud Admin Portal.
2. Go to USER MANAGEMENT > Users.
3. Select (+), then select Manual user entry.
4. Input user information:
    - First name
    - Last name
    - Username (Required)
    - Company email (Required)
    - Description
5. Under User Security Settings and Permission > Permission Settings, check the box next to Enable as LDAP Bind DN. When enabled, this user acts to bind and search the JumpCloud LDAP directory; one or more users can enable this option.



Add Users to the LDAP Directory

To add users to the LDAP directory:

1. Log in to the JumpCloud Admin Portal.
2. Go to USER AUTHENTICATION > LDAP.
3. Go to the Users tab.
4. Select users in the list.
5. Select save.



Enabling Samba Support with JumpCloud LDAP

Enabling Samba support allows LDAP users to authenticate to endpoints that require Samba attributes within the LDAP directory. This article explains the JumpCloud configuration. Configuration of the endpoint authenticating to JumpCloud varies and may require vendor documentation to complete.

Check out this Knowldege Base article to learn more about Samba support:

Enabling Samba Support with JumpCloud LDAP

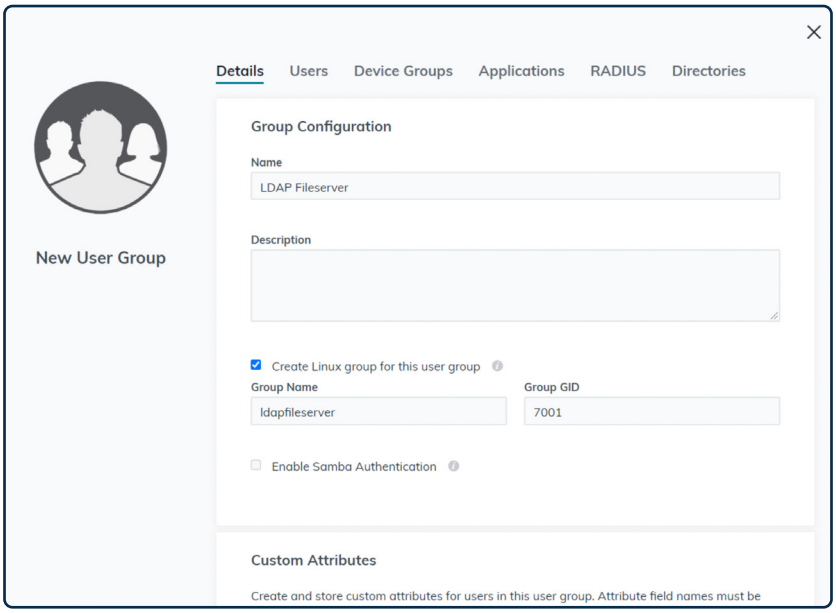
Creating LDAP Groups

When groups of users are bound to the JumpCloud LDAP directory, LDAP groups are created. Creating a user group helps you manage which users have access to specific applications, resources, and networks. User groups can save you time and ensure that each user has the appropriate level of access. For more information about JumpCloud groups, see Getting Started: Groups.

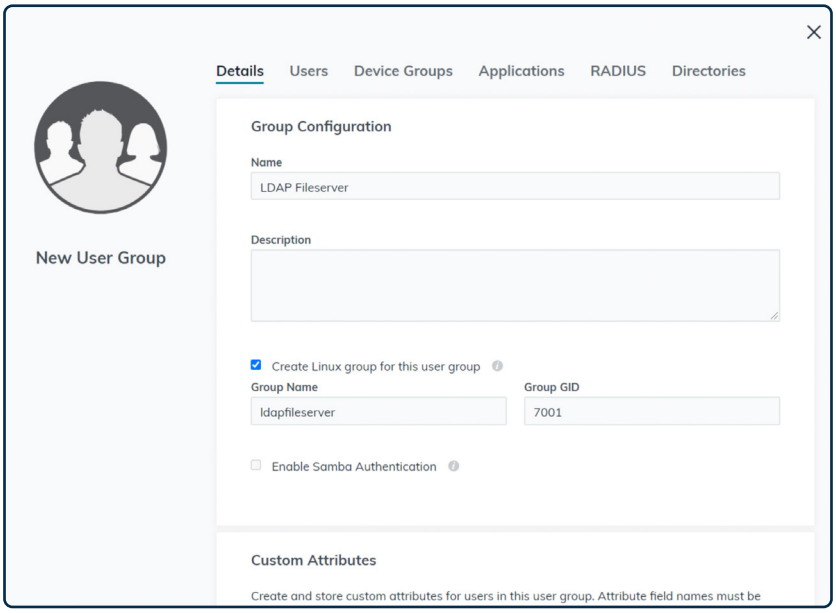
Note: Groups will not be created in LDAP unless the group contains individual members. An LDAP user must be bound to an LDAP group in order for the LDAP group to appear in an ldapsearch.

To create an LDAP group:

1. Create a new group. The group name will correspond to its `cn` in `groupOfNames`. (Optional) Create a Linux group name and GID, this will correspond with the `cn` in the `posixGroup` objectClass. Linux group names are case sensitive. Some LDAP-enabled resources require this option for LDAP group presentation.



2. On the Users tab, select the users to belong to this group.
3. On the Directories tab, bind the group to LDAP by selecting JumpCloud LDAP from the list.



For more details, check out this Knowledge Base article:

Creating LDAP Groups

Phase 7: Conditional Access Policies

Use conditional access policies to implement Zero Trust security in your organization. You can create conditional access policies that secure access to resources based on conditions like a user's identity and the network and device they're on. For example, lock down your environment with policies that deny access when users are on unmanaged devices or unapproved networks. Alternatively, relax access and let users log in to the User Portal without Multi-factor Authentication (MFA) when they're on a VPN or managed device.

Supported Browsers

Conditional access policies are only supported on the following browsers:

Windows:

- Google Chrome
- Microsoft Edge
- Internet Explorer

macOS:

- Google Chrome
- Safari

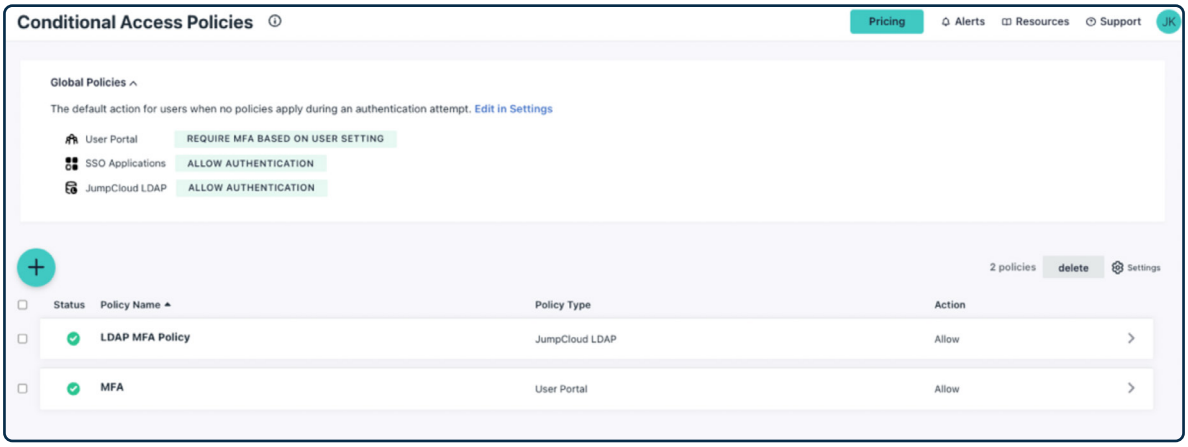
Linux:

- Google Chrome

Conditional Access Policies List View

To find the list view:

1. Log in to the JumpCloud Admin Portal.
2. Go to SECURITY MANAGEMENT > Conditional Policies.



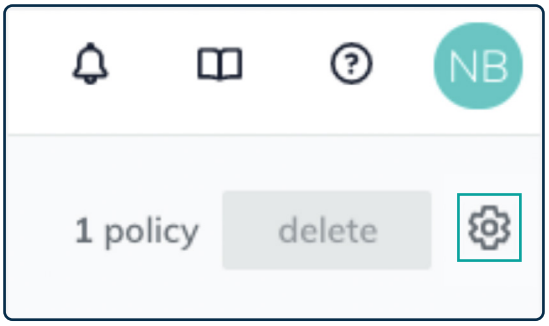
From the list view you can:

1. See a list of the conditional access policies that you configured.
2. View the status of the configured Global Policies. To make changes to these policies, select Edit in Settings.
3. Configure new conditional access policies for:
   - User Portal
   - SSO Applications
4. Delete conditional access policies.
5. Access the Conditional Policy Settings page.

Conditional Policy Settings Page

To find the Conditional Policy Settings page:

1. Log in to the JumpCloud Admin Portal.
2. Go to SECURITY MANAGEMENT > Conditional Policies.
3. In the top right, select the Settings icon.



For more information on policies, check out this Knowledge Base article:

Getting Started: Conditional Access Policies

Or watch this tutorial:

Conditional Access Policy - Device Trust Policy

Phase 8: Insights

JumpCloud Directory Insights AWS Serverless Application

The AWS Serverless Application automatically provisions all of the resources required to export JumpCloud Directory Insights data into an AWS S3 bucket.

After you install and deploy the application, it:

- Creates a role to access and operate the pieces required to export data to AWS.
- Creates an S3 bucket to store your data in.
- Places your JumpCloud API keys in AWS Secrets Manager.
- Creates the lamda function that ties everything together.

After everything is created, the application waits until your specified time increment passes and then gathers the JumpCloud Directory Insights data from the specified time period, puts it in a zipped JSON file, and sends it to the S3 bucket for storage. The application goes through this process until the CloudFormation template is deleted or the CloudWatch event that triggers the lamda function is disabled.

If an entire increment goes by without any Directory Insights data, a data point is placed in a CloudWatch metric in the JumpCloudDirectoryInsights namespace. This namespace isn't created if you don't experience increments without events.

Installing the Application

You can install the Directory Insights serverless application from the AWS Serverless Application Repository. You can also manually install the application from GitHub.

You need to provide the following when you install the Directory Insights serverless application:

- **Application name:** Many of the AWS resources this application generates for you base the name off the application name you provide.
- **Increment amount and increment type:** These parameters specify the cadence at which Directory Insights data is exported.
- **JumpCloud API key:** Your API key is safely stored in the AWS Secrets Manager.

Check out this course to learn more about Directory Insights:

Intro to Directory Insights


jumpcloud™