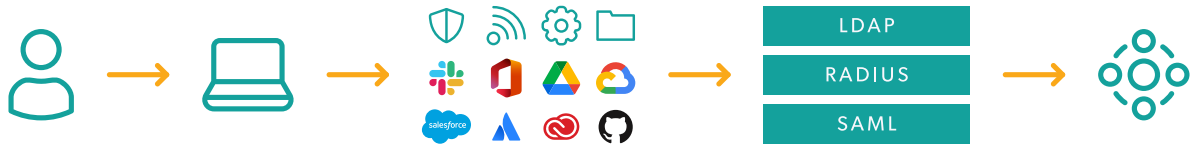

Guide

# Implementation Guide
## The JumpCloud Admin Portal

# 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:

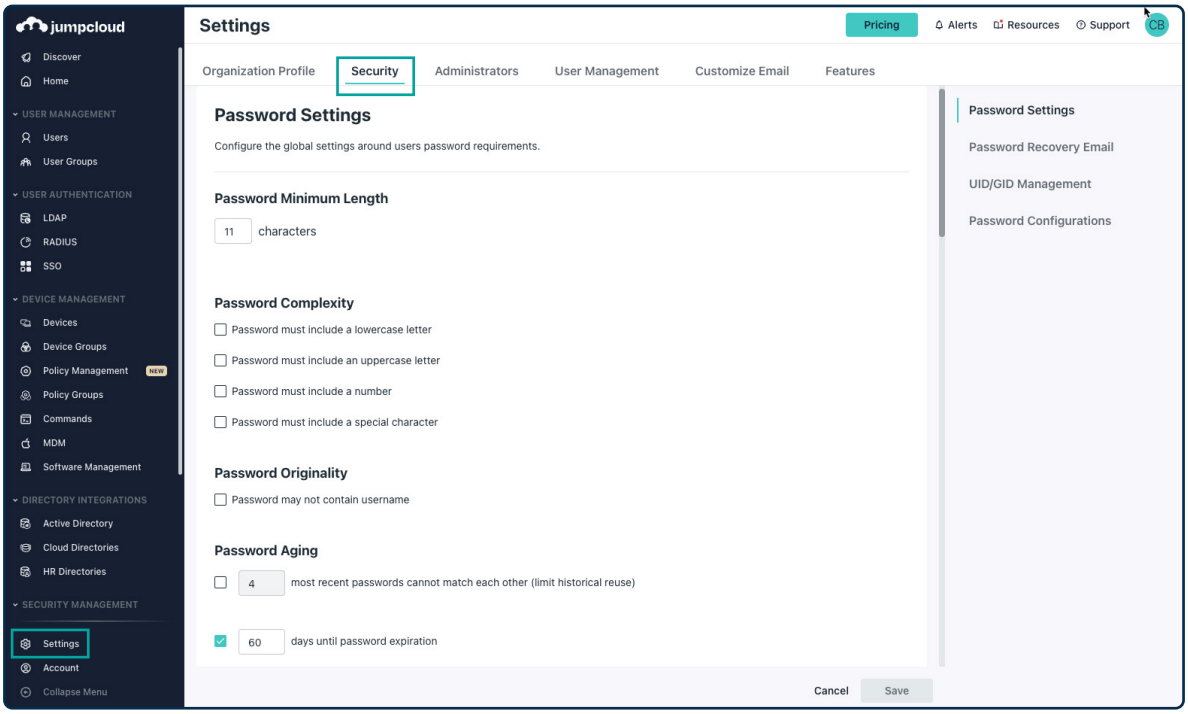
- Feel more confident in your ability to use the JumpCloud platform.
- Be the go-to JumpCloud admin for your IT org.
- Showcase your skills by displaying your certification badge on your professional profiles.

# 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

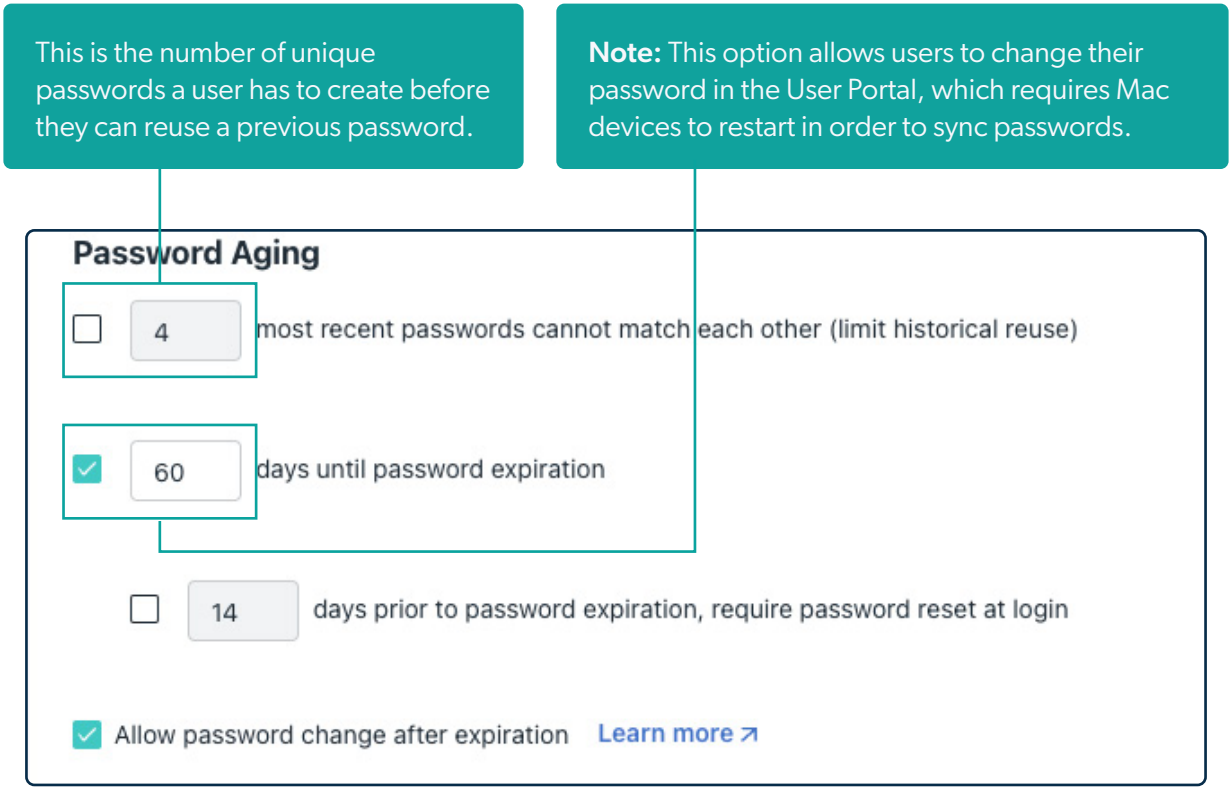
1. Under Settings > Security > Password Settings, set the Password Minimum Length to the desired number of characters.
2. Optionally, select one or more Password Complexity requirements to apply to all user passwords in your organization. Users won't be able to create a password that doesn't adhere to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

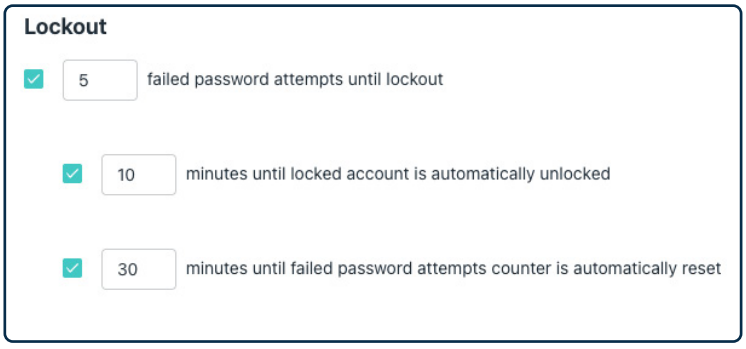
## 3. Configure Password Aging

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.

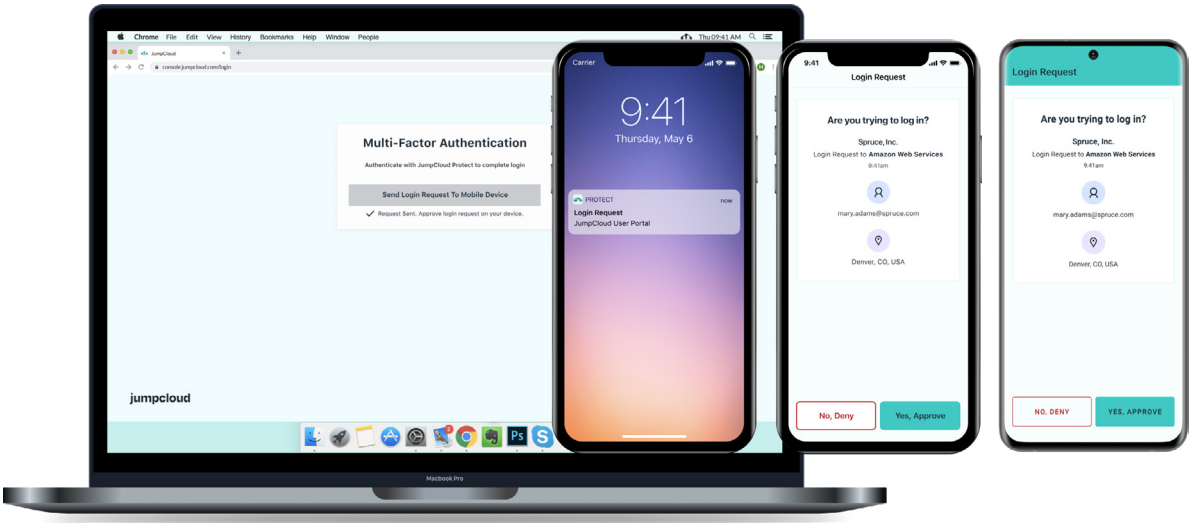



**Note:** If a user becomes locked out while they are in a session, they will remain logged into their account until they log out. Once the user logs out, they won't be able to log back in until their account becomes unlocked.

## 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

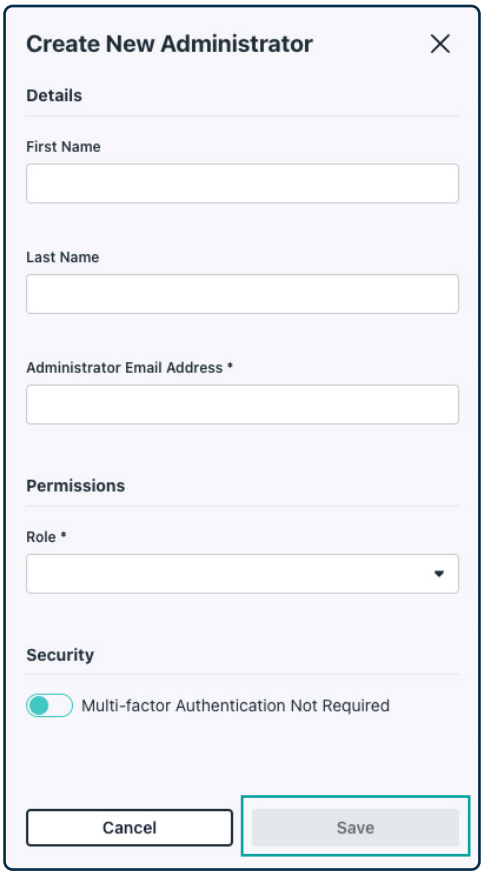
Administrator accounts are separate from user accounts. While not required, best practice is to have a minimum of two (2) administrator accounts that have the administrator with billing role.

**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