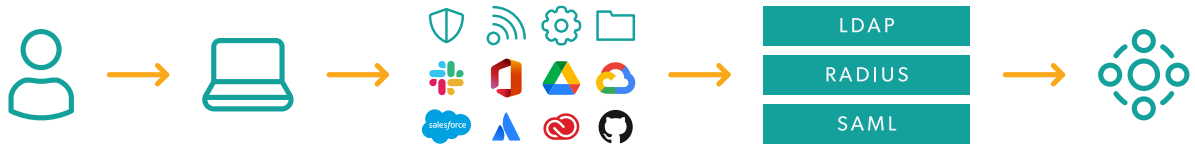
jumpcloud™

Guide

Implementation Guide
LDAP & Samba

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 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.

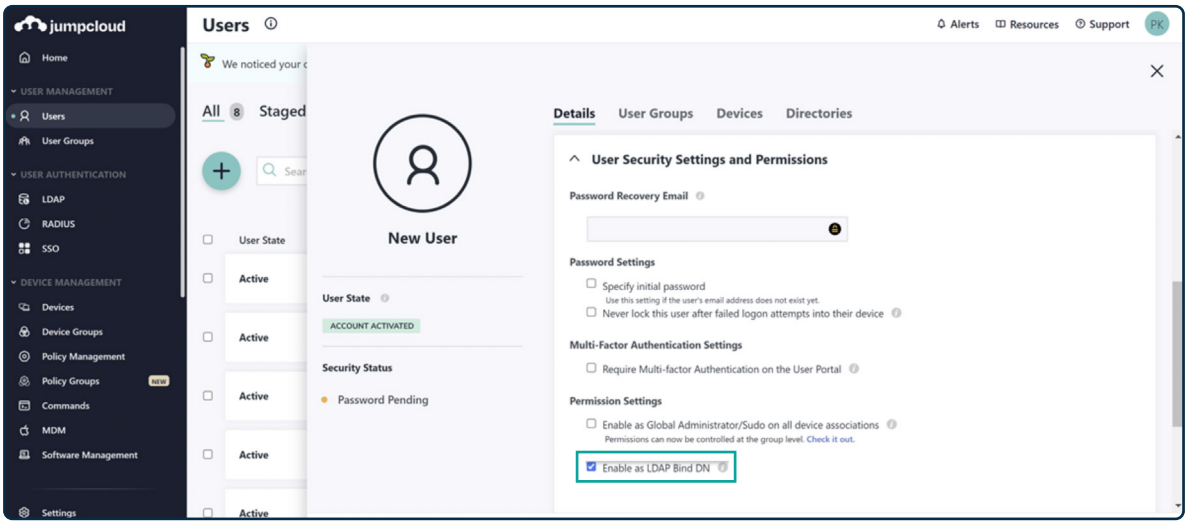
To familiarize yourself with configuring LDAP, proceed to the instructions below or watch this video:

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:

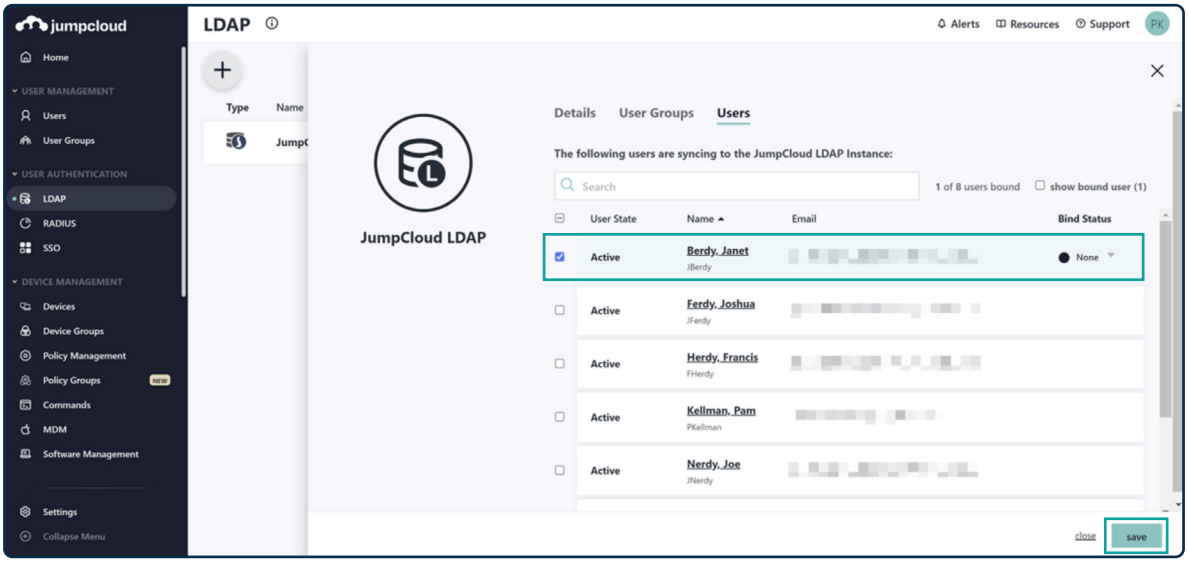
1. Log in to the JumpCloud Admin Portal.
2. Go to USER MANAGEMENT > Users.
3. Select (+), then select Manual user entry.
4. Input user information:
    - First name
    - Last name
    - Username (Required)
    - Company email (Required)
    - Description
5. Under User Security Settings and Permission > 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

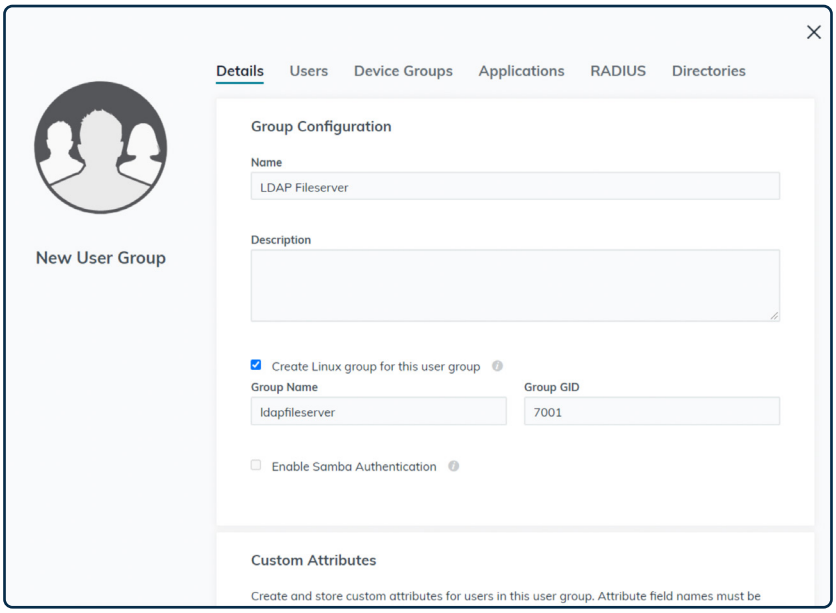
Creating LDAP Groups

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.

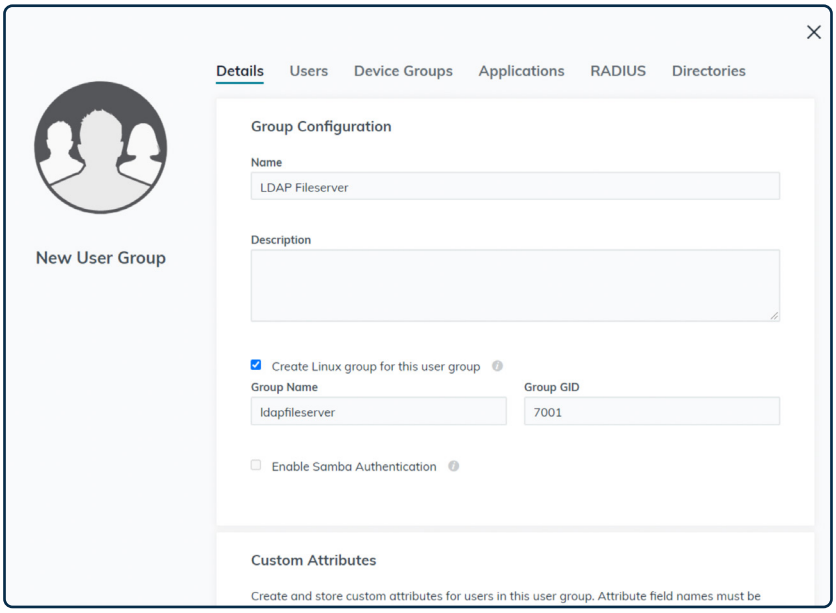
Note: Groups will not be created in LDAP unless the group contains individual members. An LDAP user must be bound to an LDAP group in order for the LDAP group to appear in an ldapsearch.

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