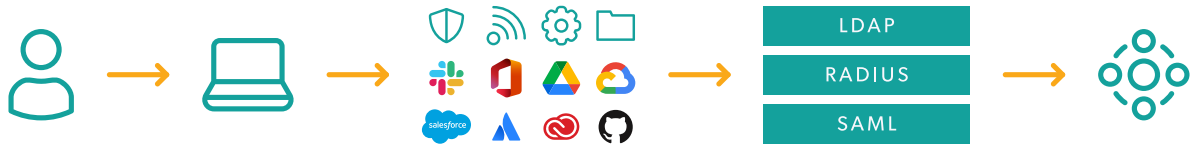
Guide

Implementation Guide
Conditional Access Policies

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 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

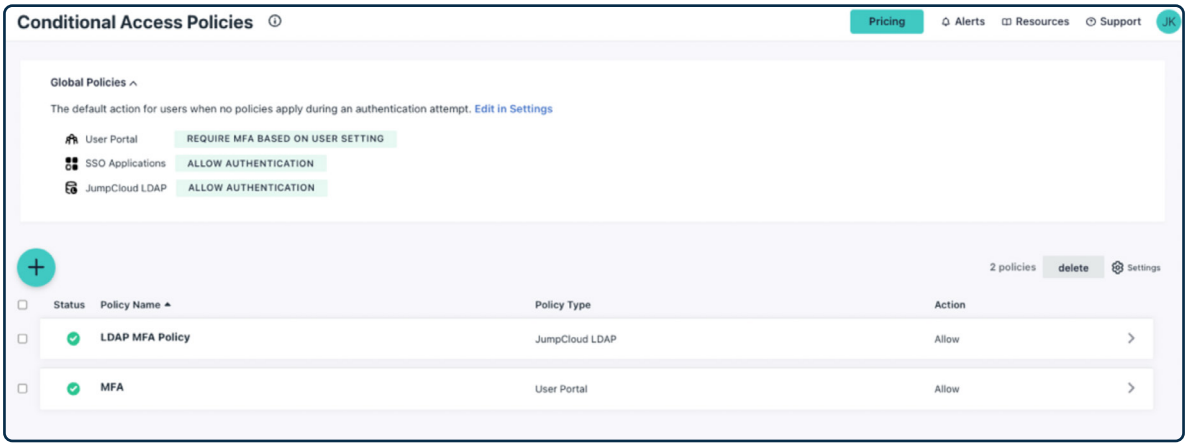
Linux:

- 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.



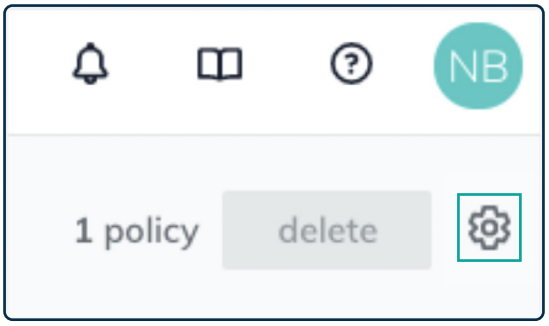
From the list view you can:

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