JumpCloud

Detection Strategy Guide

January 2026

Product Overview

JumpCloud is a cloud-based directory and identity platform designed to help organizations securely manage users, access, and devices from one place — without the need for traditional on-premises directory infrastructure (like Active Directory) or stitching together lots of separate tools

JumpCloud provides a unified, cloud-native directory platform that centralizes identity and access management (IAM), device management, and resource access in a single console. It supports cross-platform environments (Windows, macOS, Linux, and mobile) and enables secure access to networks, applications, files, and systems.

Expel's integration with Jumpcloud currently focuses on the following key areas of detection:

- Attempted use of expired Jumpcloud API keys
- Suspicious authentication events & admin activity
- Possible bypass of MFA
- Suspicious successful authentications
- Risky configuration changes

Detection Strategy for Identity Integrations

Detection

Our identity security detection strategy focuses on optimizing user authentication and application access activity monitoring. This is achieved by directly integrating with identity providers and polling for audit and data access logs.

These events are analyzed through a combination of raw log analysis and security alert processing, which are then evaluated by our detection engine for signs of suspicious login activity or post-exploitation behavior. When a threat is identified, our automated response bot, Ruxie, enriches evidence fields with first- and third-party threat intelligence. Additionally, Ruxie queries a wide range of technologies to provide analysts with critical investigative information and related events.

Response

For alerts that contain source user information, identity technologies can provide rich context such as groups, locations, job title, and other pieces of metadata. Additionally, for cloud and SaaS

alerts, identity technologies are queried to provide verbose context around user login behavior. This allows analysts to investigate the underlying session behind the activity they are triaging.

To learn more about our overall approach to detection strategy, see About Detection Strategy in the Help Center.

What We Support for JumpCloud

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for JumpCloud, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ All
Supported event log sources	■ As available via the JumpCloud Directory Insights API
JumpCloud detection rules support	No.
Detection rules written by Expel	Yes.
Hunting support	No. Hunting is not currently available for this integration.

Additional Details and Common Questions

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench