Okta Workforce Identity

Detection Strategy Guide

June 2025

Product Overview

Okta Workforce Identity is an Identity and Access Management (IAM) company that provides numerous cloud-based services around Multi-Factor Authentication (MFA) and Single Sign-On (SSO). It provides cloud software that helps companies manage and secure user authentication into modern applications and helps developers build identity controls into applications, web services, and devices. Okta can also provide qualified lead alerting potential user/account compromise .

Data produced by Okta is valuable during the investigative process when gathering more context on user authentication and application access activity. Expel uses a direct integration to pull system events from the Okta platform.

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 Okta Workforce Identity

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 Okta Workforce Identity, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported event log sources	Expel leverages data from the Okta System Log API. Generally, the following services are supported: ■ Single sign-on ■ Multi-factor authentication
Okta Workforce Identity detection rules support	Yes.
Detection rules written by Expel	Yes.
Auto remediations	Yes. Expel supports automatic execution of some remediation actions for this integration when you follow our setup guide to update the permissions in your vendor device, and then enable the auto remediation in Workbench. The available auto remediations for this integration include: ■ Disable Accounts ■ Reset Credentials To enable auto remediations for your environment, see Enable an Auto Remediation in Workbench in the Help Center.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query IP ■ Query user ■ Query logs
Hunting support	Yes. Hunting is available for this integration to customers who purchase this option. Contact your Sales or Support rep for help understanding the hypotheses and objectives

	for each hunting technique. For a full list of techniques by integration, see Hunting Techniques in the Help Center.

Additional Details and Common Questions

Console Access

A vendor alert does not typically include all of the contextual timeline activity surrounding the event of interest. Because this integration does not allow us to get all necessary data via the API, we will ask you for a certain level of console access during onboarding.

The level of access that we require is meant to support essential triage and research activities, and to help us determine the vector and extent of attacker activity for an identified threat. At minimum, we will ask for visibility into alert data, timeline events recorded, and live response/real time response shell (if applicable).

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.

Additional Add-Ons Available

- Okta ThreatInsight can be enabled to provide Expel with a contextual security signal for credential stuffing attacks and suspicious IPs (these signals provide our analysts with investigative support).
- Okta Verify with Strong MFA (the push method is recommended) can be enabled to reduce the attack surface and provide our analysts with stronger indicators to determine the fidelity of an activity (an Okta user with weak MFA is more likely to become compromised).