



Microsoft Defender for Identity

Detection Strategy Guide

September 2025

Product Overview

Microsoft Defender for Identity is a cloud-based security solution that helps secure your identity monitoring across your organization. Defender for Identity leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization.

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 Defender for Identity

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**did you expect this**) that we support for Defender for Identity, you can visit the [Detections page](#) in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	<ul style="list-style-type: none"> ■ All versions supported.
Supported platforms	<ul style="list-style-type: none"> ■ Windows ■ Linux ■ MacOS
Defender for Identity detection rules support	Yes.
Detection rules written by Expel	Yes.
Investigative support through Workbench	<p>Yes. Expel analysts are able to take the following investigative actions to gather data for triage and investigation of events.</p> <ul style="list-style-type: none"> ■ Query Host ■ Query IP ■ Query Logs ■ Query User
Hunting support	No. Hunting is not currently available for this integration.

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 (**did you expect this**) 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.