Microsoft Entra ID Protection

Detection Strategy Guide

June 2025

Product Overview

Microsoft Entra ID Protection (formerly known as Azure AD Identity Protection) provides real-time detection and automated response to identity-based threats, including risky sign-ins and users. It helps organizations protect against account compromise using adaptive access policies and integrates with Microsoft Defender and Sentinel for enhanced protection.

The following are examples of the types of data that Microsoft gathers, correlates, and assesses to help build their machine-learning-based detection models — User and Entity Behavior Analytics (UEBA):

- Device identification
- IP addresses
- IP carrier
- Browser information
- Domain information

Microsoft Entra ID Protection reports on activities within three broad identity-based authentication categories. Microsoft uses these categories to filter activities by detections and sign-in to indicate risky users:

- Risk detections
- Risky sign-ins
- Risky users

These three broad categories include the following detection types, which are gathered by Expel through API from Microsoft:

- Admin confirmed user compromised
- Anonymous IP address
- Atypical travel
- Microsoft Entra ID threat intelligence
- Impossible travel
- Leaked credentials
- Malicious IP address
- Malware linked IP address
- Password spray
- Unfamiliar sign-in properties

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 Microsoft Entra ID Protection

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 Microsoft Entra ID Protection, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported event log sources	■ Microsoft Entra ID Protection (through Microsoft Graph API) MCAS Sentinel
Microsoft Entra ID Protection 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: ■ Remove Malicious Email ■ 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 Cloud User Activity (Obtain cloud user details from Azure) ■ Query Alerts/Logs (Obtain cloud user and IP information details from Azure) ■ Within Azure, review Risky Detections, Risky-Sign In, or Risk Users reports
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 (**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.