

Microsoft
CERTIFIED

EXPERT



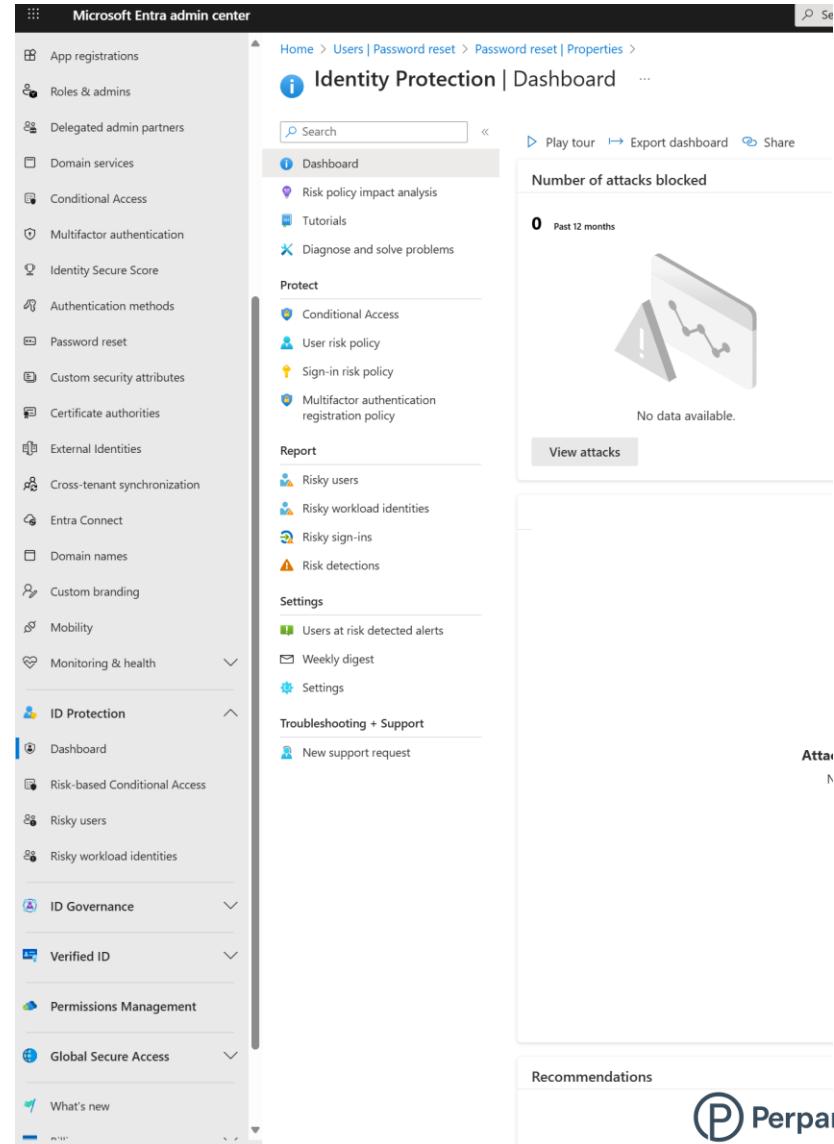
Investigating Identity Risks with Microsoft 365 Defender

From Detection to Response across
Microsoft Entra ID, Defender, and Sentinel

PerparimLabs

Why identity-based threats matter

- 80% of breaches begin with compromised credentials
- Entra ID Protection continuously analyzes sign-in and user risk
 - Defender correlates those risks with incidents for deeper investigation



The screenshot shows the Microsoft Entra admin center Identity Protection dashboard. The left sidebar contains a navigation menu with sections like App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, Authentication methods, Password reset, Custom security attributes, Certificate authorities, External Identities, Cross-tenant synchronization, Entra Connect, Domain names, Custom branding, Mobility, Monitoring & health, ID Protection, Verified ID, Permissions Management, Global Secure Access, and What's new. The main content area is titled 'Identity Protection | Dashboard' and includes a search bar, a 'Dashboard' section with links to Risk policy impact analysis, Tutorials, and Diagnose and solve problems, a 'Protect' section with links to Conditional Access, User risk policy, Sign-in risk policy, Multifactor authentication registration policy, a 'Report' section with links to Risky users, Risky workload identities, Risky sign-ins, and Risk detections, a 'Settings' section with links to Users at risk detected alerts, Weekly digest, and Settings, and a 'Troubleshooting + Support' section with a 'New support request' link. At the bottom, there is a 'Recommendations' section and the PerparimLabs logo.

Risk detection powered by trillions of Microsoft signals

- Detects risky **sign-ins, users, and workload identities**
- Evaluates behaviors (location, time, device, IP reputation)
- Auto-remediates through MFA or password reset

The image displays two side-by-side screenshots of the Microsoft Entra admin center interface, specifically focusing on Identity Protection settings.

Left Screenshot (Identity Protection | Sign-in risk policy):

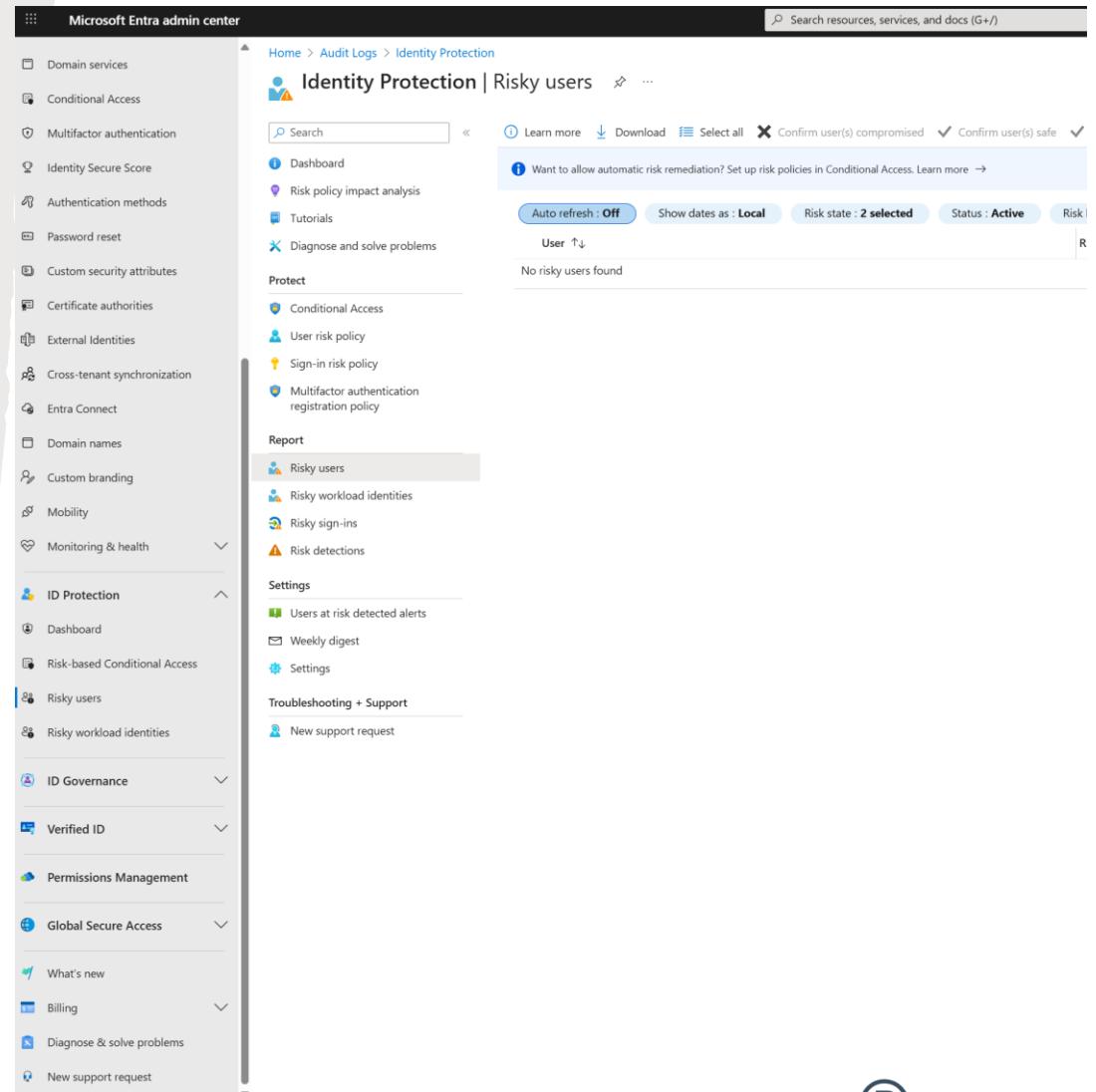
- Policy Name:** Sign-in risk remediation policy
- Assignments:** All users included and 1 user excluded
- Sign-in risk:** Medium and above
- Controls:** Access (radio button selected), Require multifactor authentication
- Policy enforcement:** Enabled (button is blue)
- Save button:** Located at the bottom right.

Right Screenshot (Identity Protection | User risk policy):

- Policy Name:** User risk remediation policy
- Assignments:** All users
- User risk:** Low and above
- Controls:** Access (radio button selected), Require password change
- Policy enforcement:** Enabled (button is blue)
- Save button:** Located at the bottom right.

Bridging detection with investigation

- Identity Protection flags a user as risky
- Admin clicks “**Investigate with Microsoft 365 Defender**”
- Defender aggregates alerts, devices, and lateral movement paths



The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains a navigation menu with various options like Domain services, Conditional Access, Multifactor authentication, and Identity Protection. The main content area is titled "Identity Protection | Risky users". It includes a search bar, a message about automatic risk remediation, and filters for "Auto refresh: Off", "Show dates as: Local", "Risk state: 2 selected", "Status: Active", and "Risk". A table below shows "No risky users found". The "Report" section is expanded, showing "Risky users" (which is selected), "Risky workload identities", "Risky sign-ins", and "Risk detections". The "Settings" section shows "Users at risk detected alerts", "Weekly digest", and "Settings". The "Troubleshooting + Support" section shows "New support request".

Detection → Investigation → Response (Microsoft Security)

From identity signals to automated incident response — unified under Microsoft Security.

Microsoft Entra ID Protection

- Detects risky sign-ins
- Flags risky users
- AI risk scoring

Microsoft 365 Defender

- Incidents & alerts
- Lateral movement
- Unified timeline

Microsoft Sentinel

- Correlation & hunting
- KQL analytics rules
- Automation (SOAR)

Detection

Investigation

Response

Identity is the new attack surface – align Detection → Investigation → Response in one ecosystem



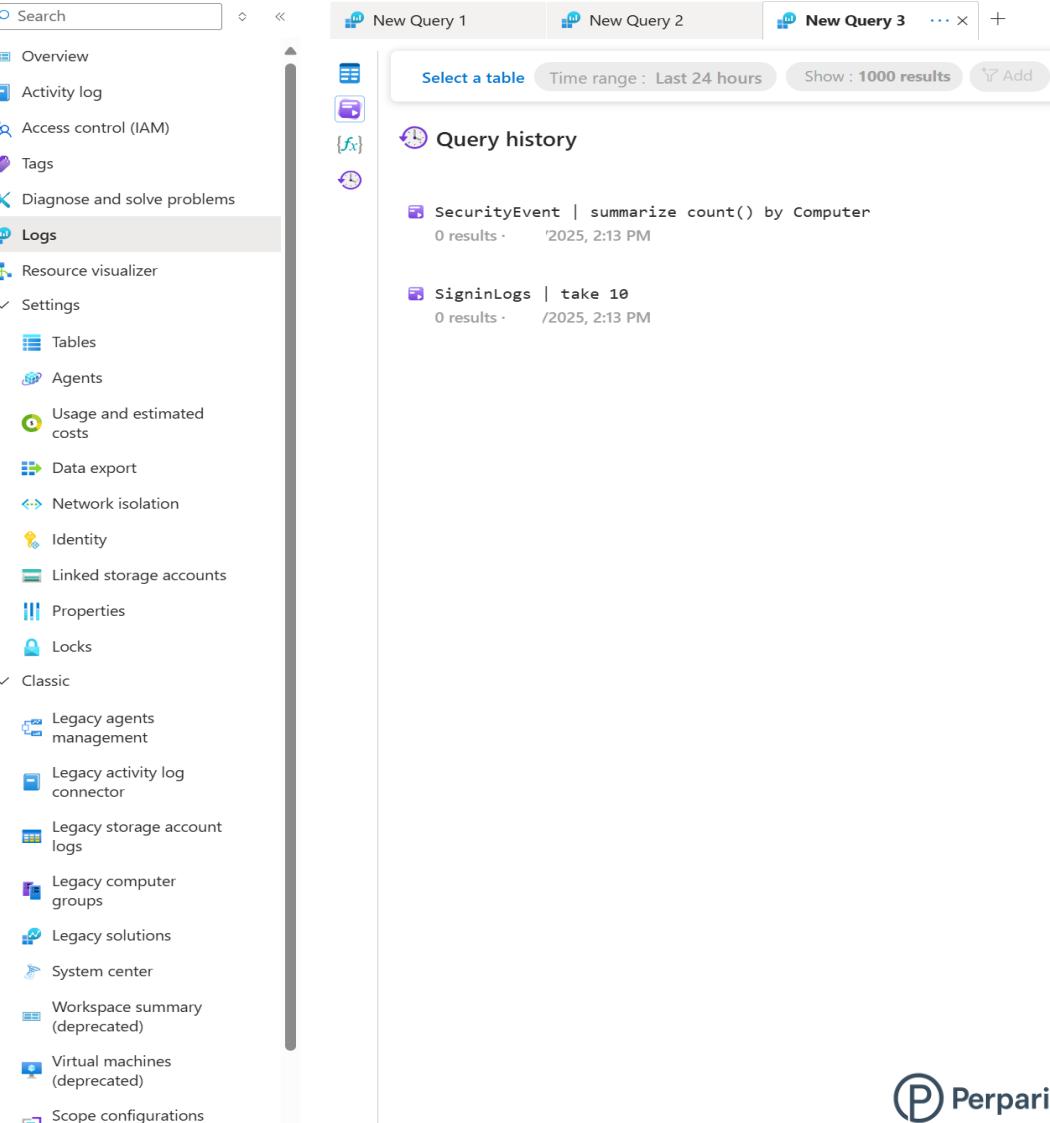
Extending investigation into proactive hunting

- Logs and alerts from Entra + Defender feed Sentinel
- SOC analysts can run KQL queries for deep correlation
- Supports custom analytics rules and automation

Home > SentinelLogWorkspace

SentinelLogWorkspace | Logs

Log Analytics workspace



Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Logs**
- Resource visualizer
- Settings
 - Tables
 - Agents
 - Usage and estimated costs
 - Data export
 - Network isolation
 - Identity
 - Linked storage accounts
 - Properties
 - Locks
- Classic
 - Legacy agents management
 - Legacy activity log connector
 - Legacy storage account logs
 - Legacy computer groups
 - Legacy solutions
 - System center
 - Workspace summary (deprecated)
 - Virtual machines (deprecated)
 - Scope configurations (deprecated)

New Query 1 New Query 2 New Query 3

Select a table Time range : Last 24 hours Show : 1000 results Add

Query history

SecurityEvent | summarize count() by Computer
0 results · 2025, 2:13 PM

SigninLogs | take 10
0 results · 2025, 2:13 PM

Unified incident timeline



- Defender shows correlated alerts across workloads
- Provides user context, device timeline, and incident severity
- Helps SOC teams prioritize real threats faster

Lessons learned

-  Entra ID Protection detects risk in real time
-  Microsoft 365 Defender centralizes investigation
-  Sentinel enables proactive threat hunting
-  Together: Continuous detection, investigation, and response loop