Microsoft
CERTIFIED
EXPERT

Detecting and Responding to Identity Risks with Microsoft Entra ID Protection

Combining AI-driven risk signals with Conditional Access for secure authentication

PerparimLabs

#PerparimLabs #MicrosoftEntra #IdentityProtection
#ZeroTrust #CloudSecurity

What Is Entra ID Protection?

Formerly *Azure AD Identity Protection*

Detects, investigates, and remediates identity-based risks

Uses AI signals like location, device, and behavior

Integrates with Conditional Access and Sentinel for automated defense

PerparimLabs

#PerparimLabs #MicrosoftEntra #IdentityProtection #ZeroTrust #CloudSecurity

How Risk Detection Works

Risky sign-ins: Detected during authentication (e.g., atypical travel, anonymous IPs)

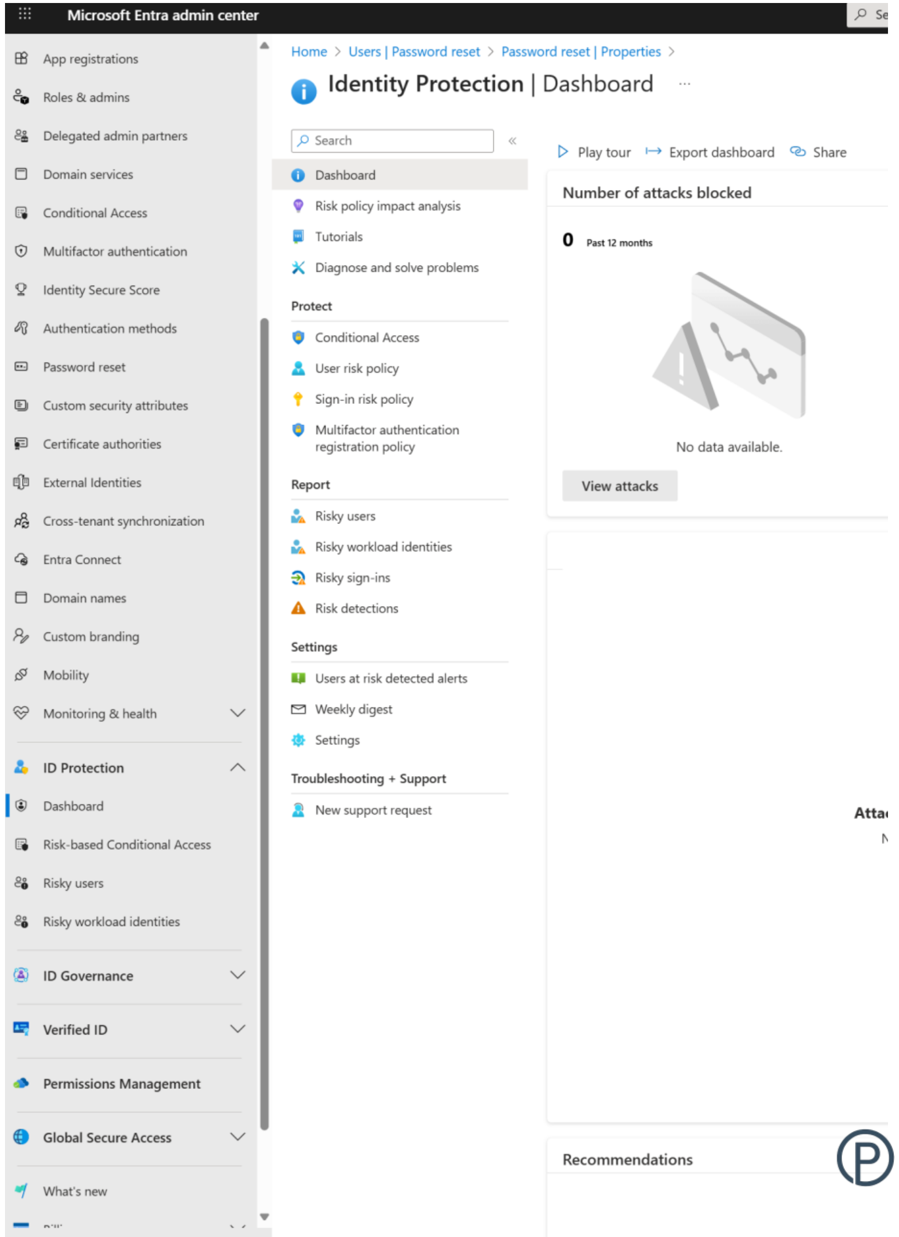
Risky users: Based on behavior anomalies or dark web credential leaks

Microsoft AI analyzes **trillions of signals** to assign risk levels (Low / Medium / High).

#PerparimLabs #MicrosoftEntra #IdentityProtection
#ZeroTrust #CloudSecurity

Dashboard Overview

- Centralized view of risky users, sign-ins, and policy enforcement.



Microsoft Entra admin center

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
Dashboard
Risk-based Conditional Access
Risky users
Risky workload identities

ID Governance
Verified ID
Permissions Management
Global Secure Access
What's new

Home > Users | Password reset > Password reset | Properties >

Identity Protection | Dashboard ···

Search

Dashboard
Risk policy impact analysis
Tutorials
Diagnose and solve problems

Protect
Conditional Access
User risk policy
Sign-in risk policy
Multifactor authentication registration policy

Report
Risky users
Risky workload identities
Risky sign-ins
Risk detections

Settings
Users at risk detected alerts
Weekly digest
Settings

Troubleshooting + Support
New support request

Play tour · Export dashboard · Share

Number of attacks blocked

0 Past 12 months

No data available.

View attacks

Atta

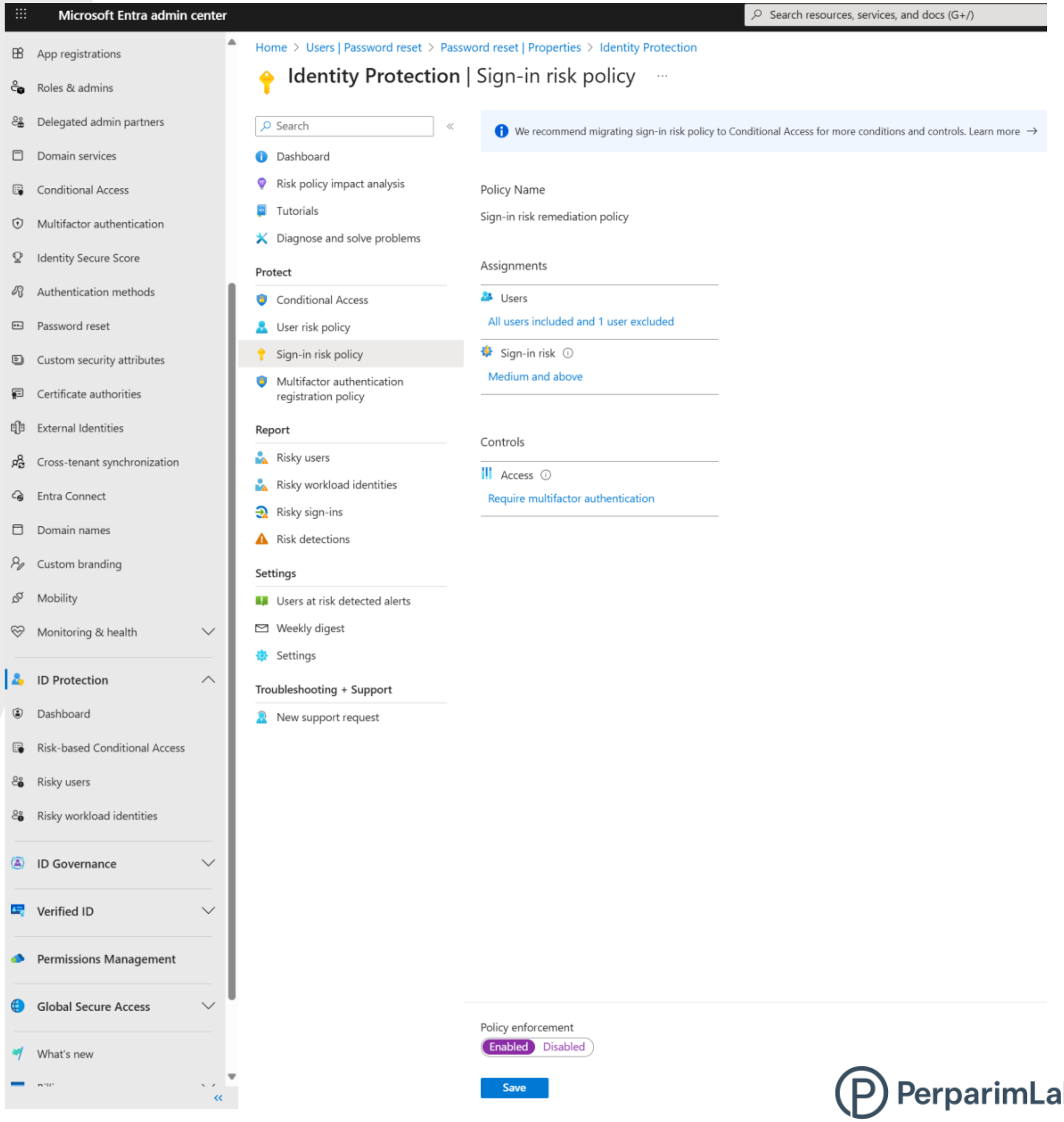
Recommendations

PerparimLabs

#PerparimLabs #MicrosoftEntra #IdentityProtection #ZeroTrust #CloudSecurity

Sign-in Risk Policy

- Applied to all users
- Risk threshold: *Medium and above*
- Action: *Require MFA*
- Reinforces Zero Trust by verifying user authenticity before access.



Microsoft Entra admin center

Home > Users | Password reset > Password reset | Properties > Identity Protection

Identity Protection | Sign-in risk policy

We recommend migrating sign-in risk policy to Conditional Access for more conditions and controls. Learn more →

Policy Name

Sign-in risk remediation policy

Assignments

Users

All users included and 1 user excluded

Sign-in risk

Medium and above

Controls

Access

Require multifactor authentication

Policy enforcement

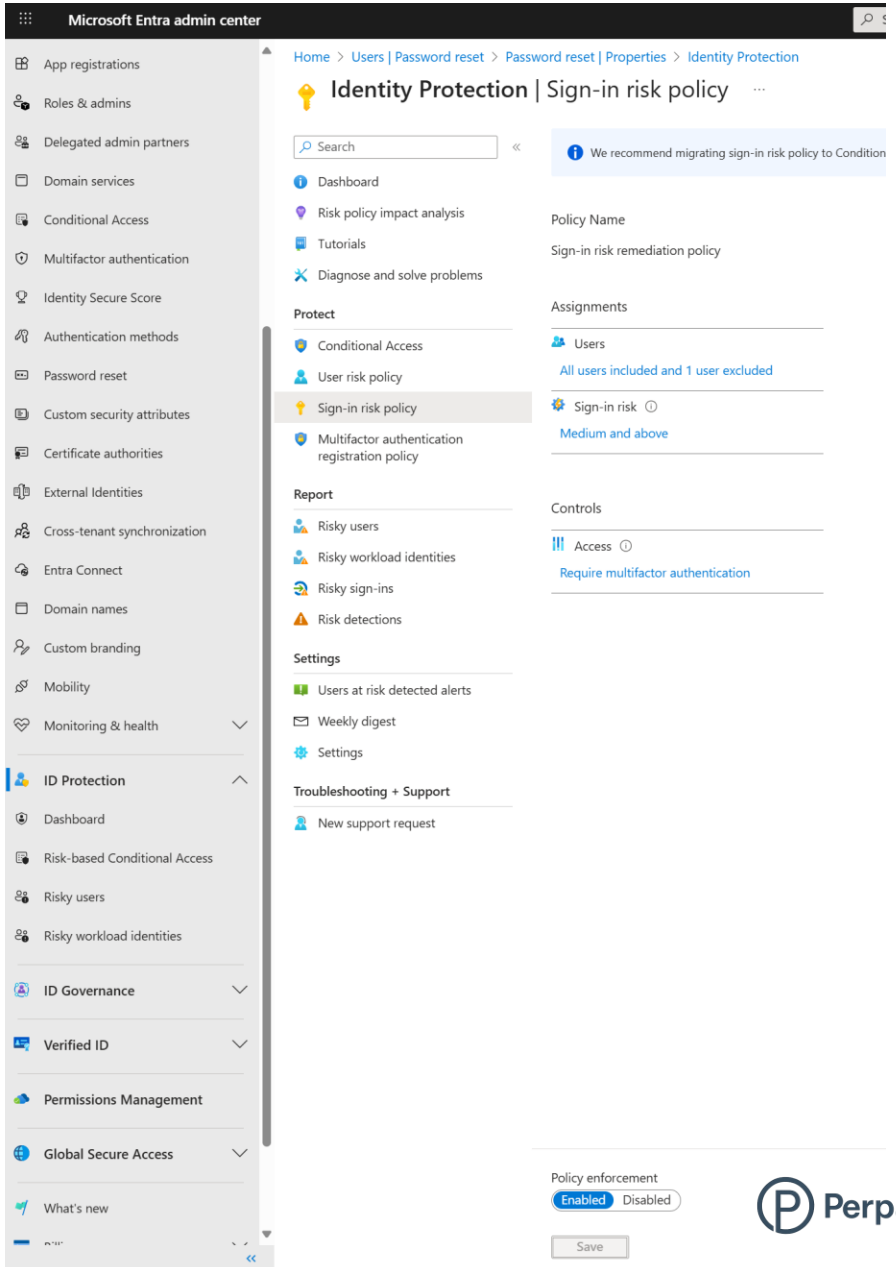
Enabled Disabled

Save

#PerparimLabs #MicrosoftEntra #IdentityProtection
#ZeroTrust #CloudSecurity

User Risk Policy

- Triggered when abnormal user activity occurs (odd login times, leaked credentials)
- Action: *Require password change*
- Level: *Low and above* — most sensitive policy



Identity Protection | Sign-in risk policy

We recommend migrating sign-in risk policy to Condition

Policy Name

Sign-in risk remediation policy

Assignments

Users

All users included and 1 user excluded

Sign-in risk

Medium and above

Controls

Access

Require multifactor authentication

Policy enforcement

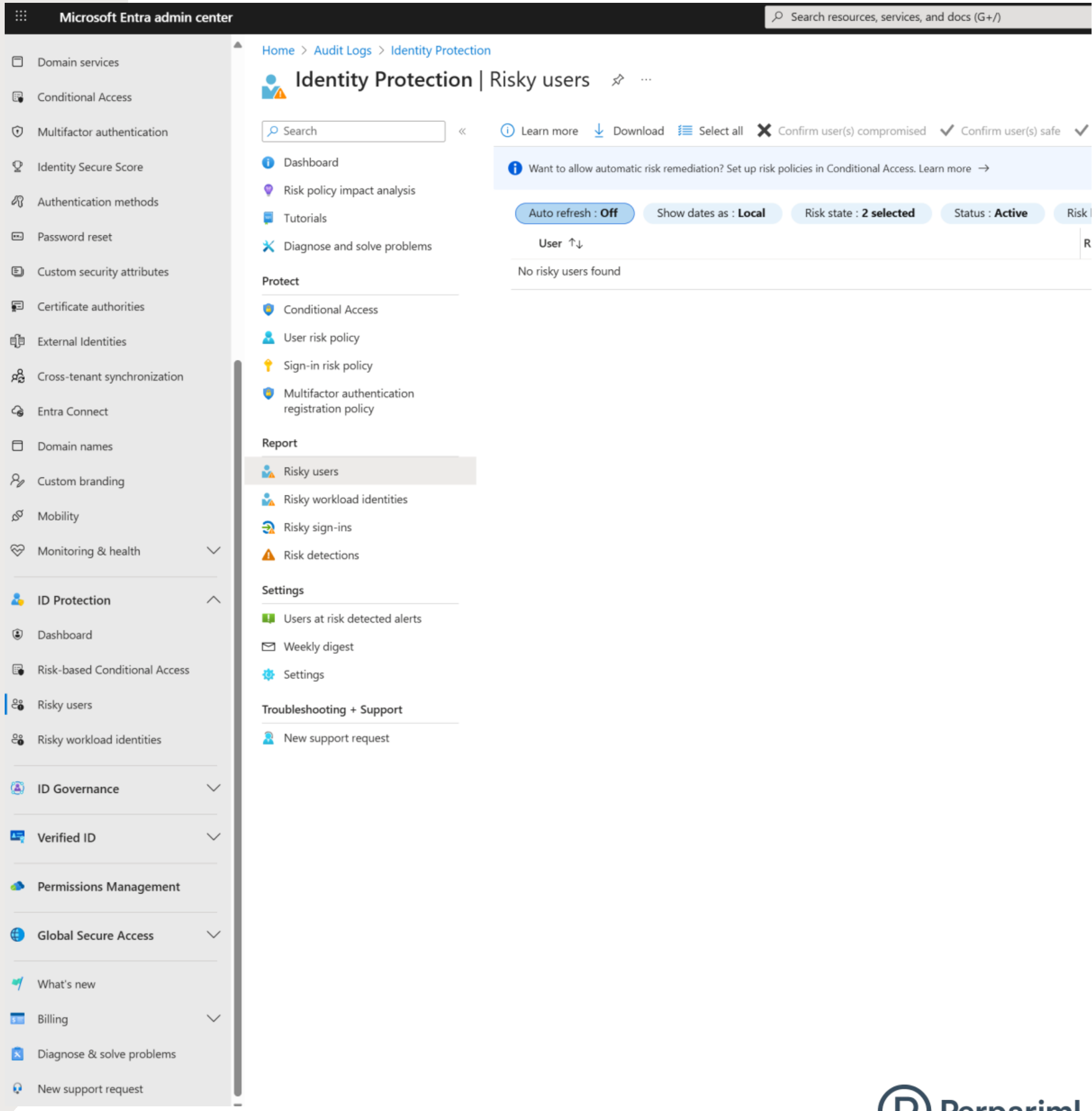
[✓ Enabled] Disabled

PerparimLabs

#PerparimLabs #MicrosoftEntra #IdentityProtection
#ZeroTrust #CloudSecurity

Risky User Monitoring

- In production environments, this report populates automatically with risky sign-ins and behaviors, allowing security teams to take proactive actions.



Want to allow automatic risk remediation? Set up risk policies in Conditional Access. Learn more →

Auto refresh : Off | Show dates as : Local | Risk state : 2 selected | Status : Active | Risk l

User ↑↓ | R

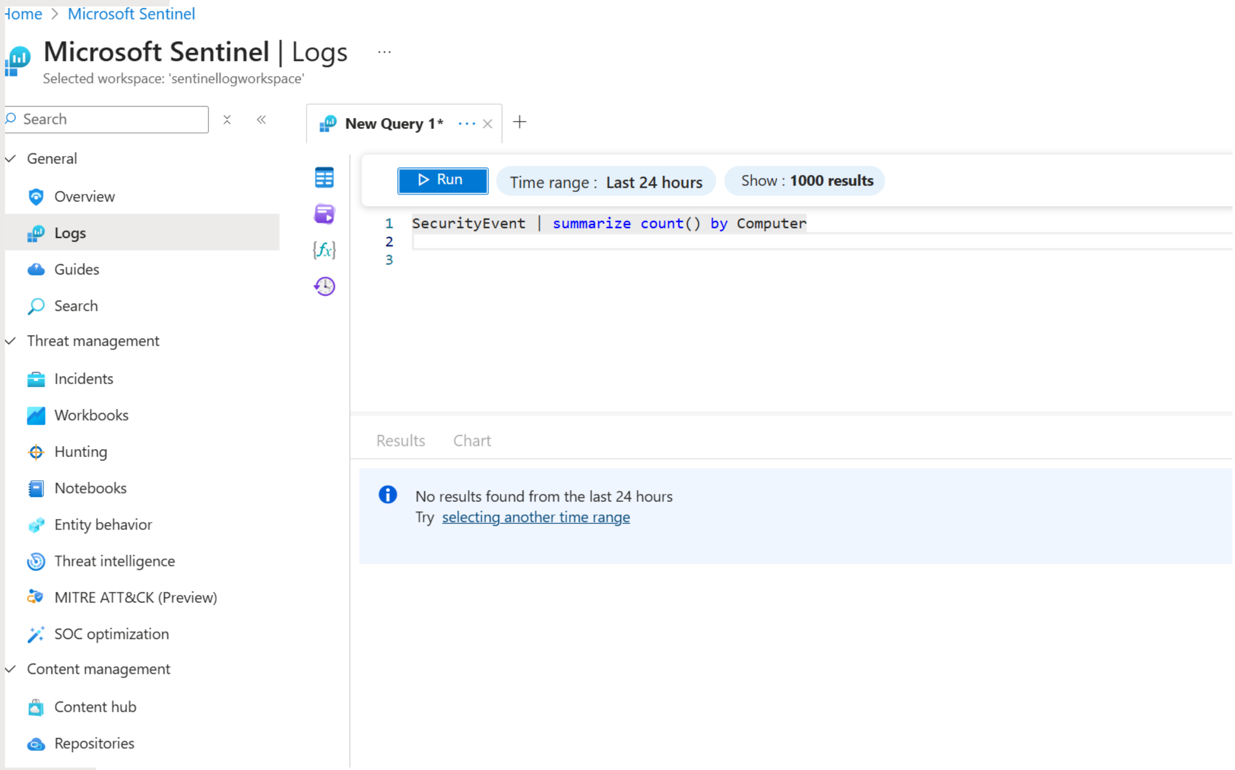
No risky users found

PerparimLabs

#PerparimLabs #MicrosoftEntra #IdentityProtection
#ZeroTrust #CloudSecurity

Sentinel Integration

- Logs can be queried from Microsoft Sentinel for risk correlation.
- Even when no live data is found, this lab demonstrates how Entra Identity Protection can feed SIEM pipelines through *Log Analytics workspace integration*.



```
SecurityEvent | summarize count() by Computer
```

No results found from the last 24 hours
Try selecting another time range

PerparimLabs

#PerparimLabs #MicrosoftEntra #IdentityProtection #ZeroTrust #CloudSecurity

Key Takeaways

✅ Detect risks automatically using AI signals
✅ Enforce MFA or password reset based on risk level
✅ Integrate with Sentinel for continuous monitoring
✅ Simplify remediation with automation and reports

PerparimLabs

#PerparimLabs #MicrosoftEntra #IdentityProtection
#ZeroTrust #CloudSecurity