



Microsoft Entra ID Protection – User Risk Policy Demo

- Real-Time Identity Protection in Action

What Is Microsoft Entra ID Protection?

Entra ID Protection uses machine learning to detect risky behavior like:

- Leaked credentials
- TOR-based or unfamiliar sign-ins
- Impossible travel

It works with Conditional Access to:

- Require MFA
- Block access
- Trigger admin response

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Custom security attributes

Risky activities

Identity Governance

External Identities

Show more

Home > Perparims Cloud Solutions > Id

Identity Protection |

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

Navigating to Identity Protection

- Go to **Microsoft Entra Admin Center** → **Protection** → **Identity Protection**
This dashboard shows active detections, policies, and reports.

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Home > Perparims Cloud Solutions > Identity Protection

Identity Protection | User risk policy

Search

We recommend migrating user risk policy to Conditional Acc

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

Policy Name

User risk remediation policy

Assignments

Users

All users

User risk

Medium and above

Controls

Access

Block access

Policy enforcement

Enabled Disabled

Save

Creating the User Risk Policy

- I created a **User Risk Policy** to block sign-in for users with **Medium and above** risk. You can scope this to all users or a test group.

Microsoft Entra admin center

Home > Perparims Cloud Solutions > Identity Protection

Identity Protection | User risk policy

Search

We recommend migrating user risk policy to Conditional Access

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

Policy Name

User risk remediation policy

Assignments

Users

All users

User risk ⓘ

Medium and above

Controls

Access ⓘ

Block access

Policy enforcement

Enabled Disabled

Save

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Custom security attributes

Risky activities

Identity Governance


External Identities

Show more

Protection

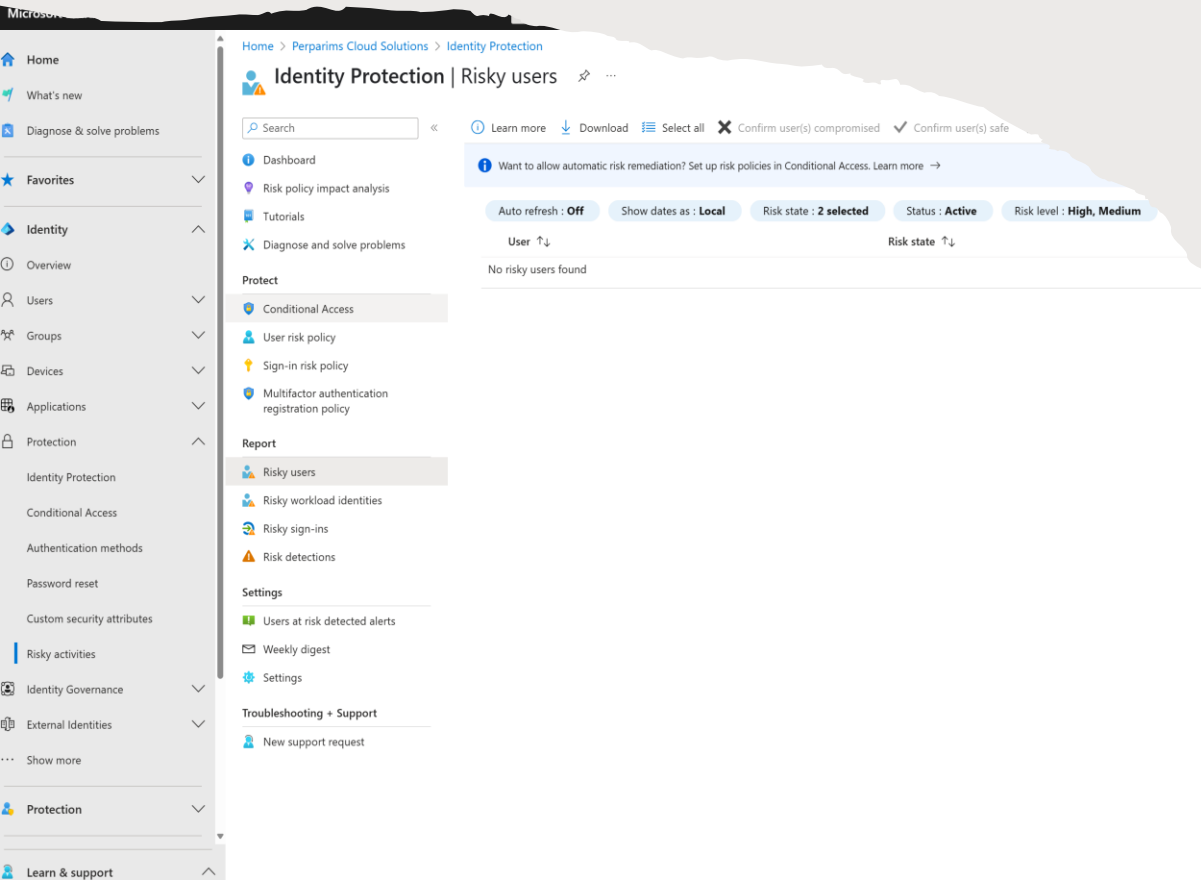
Learn & support

User Risk Policy Enabled

- Policy enforcement switched to  **Enabled**. Microsoft Entra will now automatically take action on risky users.

Monitoring Risky Users

This view shows users Entra has flagged as compromised.
It updates in real time based on AI/ML detections.
No risky users now — but protection is live.



Real-World Value



Protects accounts
from takeover



Enforces Zero Trust
policies



Built into Microsoft
Entra ID P2

Even without risky sign-ins
in this lab, this demo
shows how quickly you
can configure real identity
protection.

My Takeaway

Microsoft Entra ID Protection makes Zero Trust security easy to implement. With built-in ML and automated enforcement, I can stop threats before they escalate.

This is a must-know for SC-300, real-world Azure work, and client security demos.