



Lab: Protecting Identities with Microsoft Entra ID Protection

Configure and Monitor User & Sign-in Risk Policies using Entra ID P2



Perparim Abdullahu

AZ-305 Certified

#PerparimLabs

What is Microsoft Entra ID Protection?

- Formerly known as Azure AD Identity Protection
- Uses AI and risk signals to detect compromised identities
- Protects users via automatic response policies
- Requires **Microsoft Entra ID P2 license**



Lab Objectives



CONFIGURE **SIGN-IN**
RISK POLICY



CONFIGURE **USER**
RISK POLICY



MONITOR **RISKY**
SIGN-INS AND RISKY
USERS

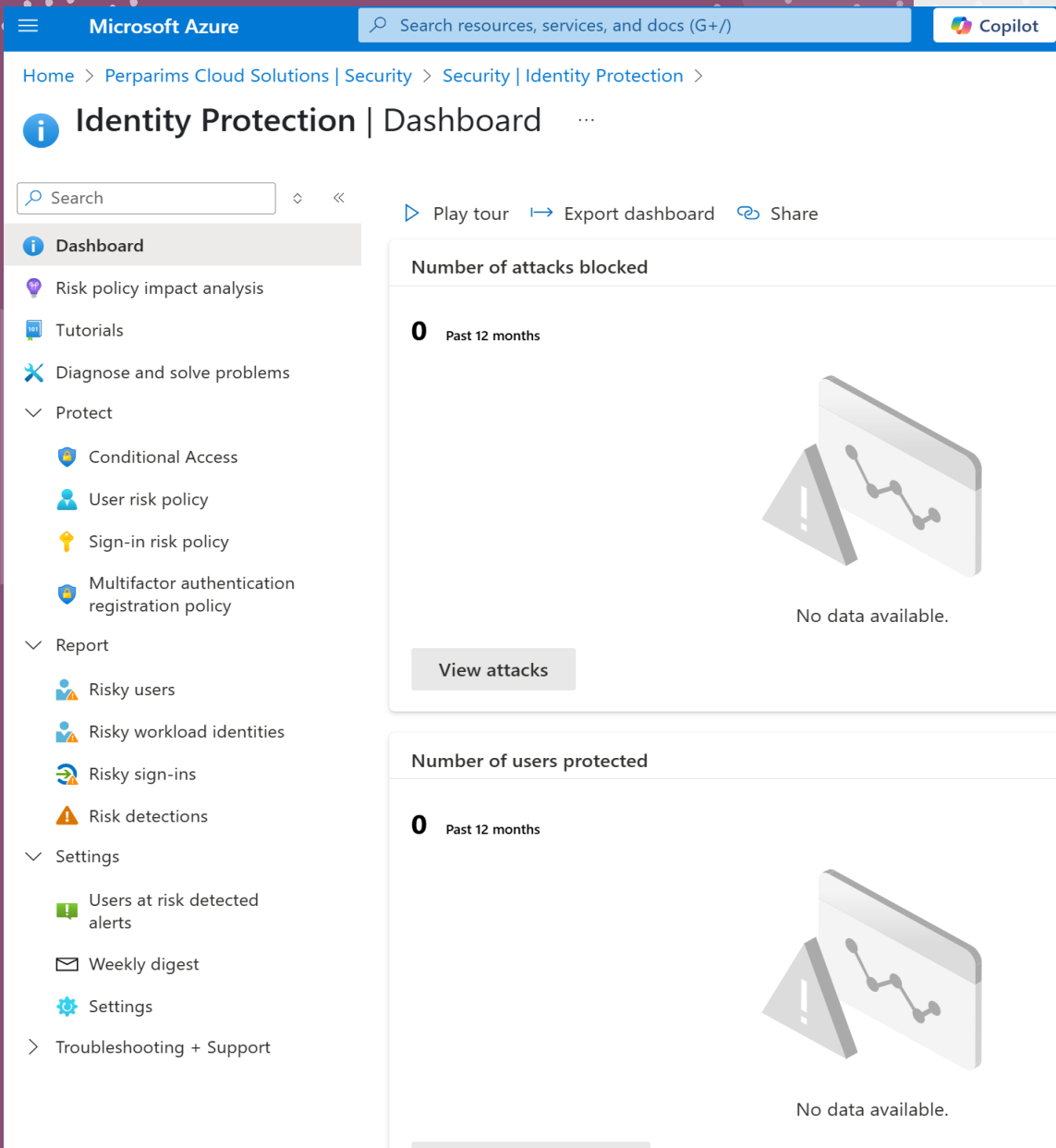


TRIGGER AND
REVIEW RISK
DETECTIONS



LEARN REAL-WORLD
ALERTING AND
REMEDATION FLOW

Step 1 – Access Identity Protection



The screenshot shows the Microsoft Azure portal interface. At the top, the header includes the Microsoft Azure logo, a search bar, and the Copilot icon. Below the header, the breadcrumb navigation path is: Home > Perparims Cloud Solutions | Security > Security | Identity Protection >. The main heading is "Identity Protection | Dashboard". A search bar is located below the heading. The left sidebar contains a navigation menu with the following items: Dashboard (selected), Risk policy impact analysis, Tutorials, Diagnose and solve problems, Protect (expanded), Conditional Access, User risk policy, Sign-in risk policy, Multifactor authentication registration policy, Report (expanded), Risky users, Risky workload identities, Risky sign-ins, Risk detections, Settings (expanded), Users at risk detected alerts, Weekly digest, Settings, and Troubleshooting + Support. The main content area displays two cards. The first card is titled "Number of attacks blocked" and shows "0 Past 12 months" with a line graph icon and the text "No data available." Below the card is a "View attacks" button. The second card is titled "Number of users protected" and also shows "0 Past 12 months" with a line graph icon and the text "No data available."



GO TO
PORTAL.AZURE.COM



OPEN MICROSOFT
ENTRA ID



NAVIGATE TO:
SECURITY > IDENTITY
PROTECTION

Step 2 – Sign-in Risk Policy

Microsoft Azure | Search resources, services, and docs (G+)

Home > Perparims Cloud Solutions | Security > Security | Identity Protection > Identity Protection

Identity Protection | Sign-in risk policy

Search

We recommend migrating sign-in risk policy to Conditional Access for more conditions.

Policy Name
Sign-in risk remediation policy

Assignments

- Users
 - All users
- Sign-in risk
 - Medium and above

Controls

- Access
 - Block access

Policy enforcement
Enabled Disabled

Save

Left Sidebar:

- 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



TARGET: ALL USERS
(OR TEST GROUP)



RISK LEVEL: MEDIUM
AND ABOVE (OR LOW
TO TEST EASILY)



ACCESS CONTROL:
REQUIRE MFA

Step 3 – User Risk Policy

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Perparims Cloud Solutions | Security > Security | Identity Protection > Identity Protection

Identity Protection | User risk policy

Search

We recommend migrating user risk policy to Conditional Access for more conditions

Policy Name

User risk remediation policy

Assignments

- Users
 - All users
- User risk
 - Medium and above

Controls

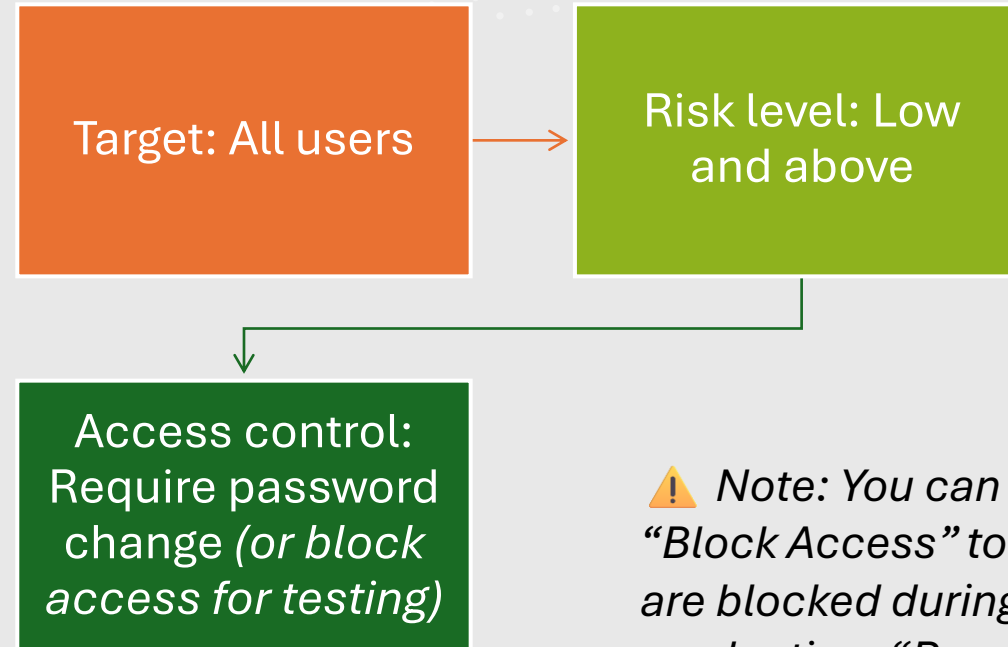
- Access
 - Block access
- User risk
 - Medium and above

We use Block Access for testing, but Require Password Change is preferred for production.

Policy enforcement

Enabled Disabled

Save



Step 4 – View Risky Users

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Perparims Cloud Solutions | Security > Security | Identity Protection > Identity Protection

Identity Protection | Risky users

Search

Learn more Download Select all Confirm user(s) compromised Confirm user(s) safe

We recommend migrating Identity Protection policies to Conditional Access for more conditions and controls. [Learn more](#)

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

Risk level : **High, Medium** [Add filters](#)

User ↑↓	Risk state ↑↓	Risk last updated ↑↓
No risky users found		

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



Navigate to: Identity Protection > Risky Users



View flagged users with detected anomalies



Click into details for risk type (e.g., unfamiliar sign-in)

Step 5 – View Risky Sign-ins

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Perparims Cloud Solutions | Security > Security | Identity Protection > Identity Protection

Identity Protection | Risky sign-ins

Search

Download Learn more Export Data Settings Configure trusted IPs Troubleshoot

We recommend migrating Identity Protection policies to Conditional Access for more conditions and controls. Learn more


Auto refresh : Off Date : Last 7 days Show dates as : Local Risk state : 2 selected

Risk level (real-time) : None Selected Risk level (aggregate) : None Selected


Detection type(s) : None Selected Sign-in Type : 2 selected Add filters

Date ↑↓	User ↑↓	IP address	Location
No results.			

Users can also have detections not linked to sign-in activity. To see all the detections, go to Risk detections.

 *Want to simulate a risk?
Use the Tor browser to sign in
with a masked IP and trigger
Entra ID Protection alerts.*

- Navigate to: Identity Protection > Risky Sign-ins
- Filter by time range or user
- Look for risk types like:
 - Atypical travel
 - Anonymous IP
 - Malicious browser

 *Filter by last 7 days or custom interval to analyze suspicious sign-ins and trends.*



Identity Protection – Key Takeaways



- Entra ID Protection helps detect & block compromised accounts
- Policies can auto-remediate based on real-time risk
- Works best with Conditional Access + P2 license
- Great addition to any Zero Trust strategy

[Home](#) > [Perparims Cloud Solutions](#) >

Perparims Cloud Solutions

