Identity Security
Azure AD
Identity Protection

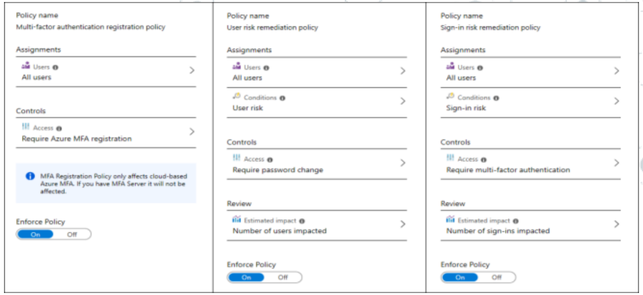
Hello!

I am Eng Teong Cheah

Microsoft MVP

Azure AD
Identity Protection

Identity Protection



Policy name
Multi-factor authentication registration policy

Assignments

Users
All users

Controls

Access
Require Azure MFA registration

MFA Registration Policy only affects cloud-based Azure MFA. If you have MFA Server it will not be affected.

Enforce Policy
● On ○ Off

Policy name
User risk remediation policy

Assignments

Users
All users

Conditions
User risk

Controls

Access
Require password change

Review

Estimated impact
Number of users impacted

Enforce Policy
● On ○ Off

Policy name
Sign-in risk remediation policy

Assignments

Users
All users

Conditions
Sign-in risk

Controls

Access
Require multi-factor authentication

Review

Estimated impact
Number of sign-ins impacted

Enforce Policy
● On ○ Off

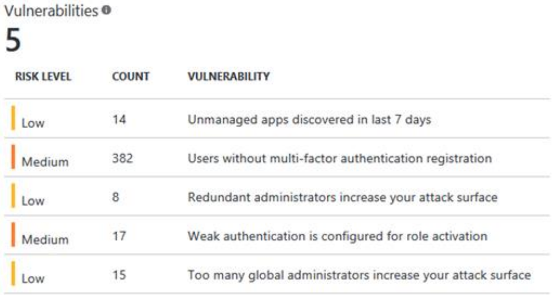
Identity Protection is a tool that allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

Risk detection and remediation

Identity Protection identifies risks in the following classifications:

- Leaked credentials
- Sign in from anonymous IP addresses
- Impossible travel to a typical locations
- Sign-in from unfamiliar locations
- Sign-ins from infected devices
- Sign-ins from IP addresses with suspicious activity

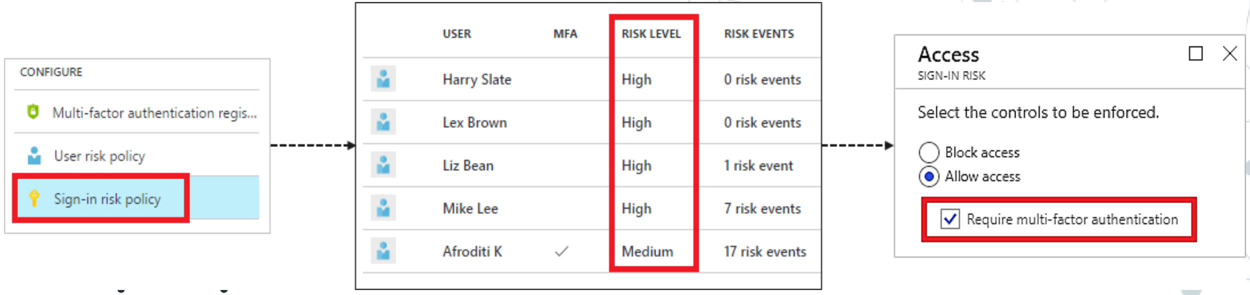


Vulnerabilities

5

RISK LEVEL	COUNT	VULNERABILITY
Low	14	Unmanaged apps discovered in last 7 days
Medium	382	Users without multi-factor authentication registration
Low	8	Redundant administrators increase your attack surface
Medium	17	Weak authentication is configured for role activation
Low	15	Too many global administrators increase your attack surface

User Risk Policy



CONFIGURE

- Multi-factor authentication regis...
- User risk policy
- Sign-in risk policy

USER	MFA	RISK LEVEL	RISK EVENTS
Harry Slate		High	0 risk events
Lex Brown		High	0 risk events
Liz Bean		High	1 risk event
Mike Lee		High	7 risk events
Afroditi K	✓	Medium	17 risk events

Access
SIGN-IN RISK

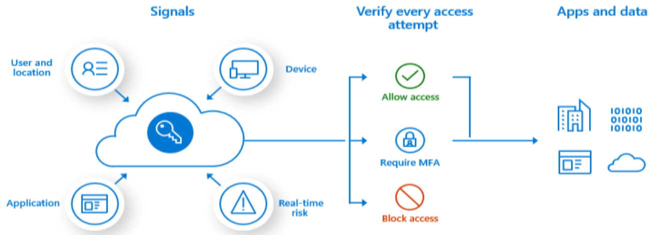
Select the controls to be enforced.

○ Block access
● Allow access

☑ Require multi-factor authentication

- Applied to user sign-ins
- Provide the condition (risk level) and action (block or allow)
- Automatically respond based on specific user’s risk level
- Use a high threshold during policy roll out
- Use a low threshold for greater security

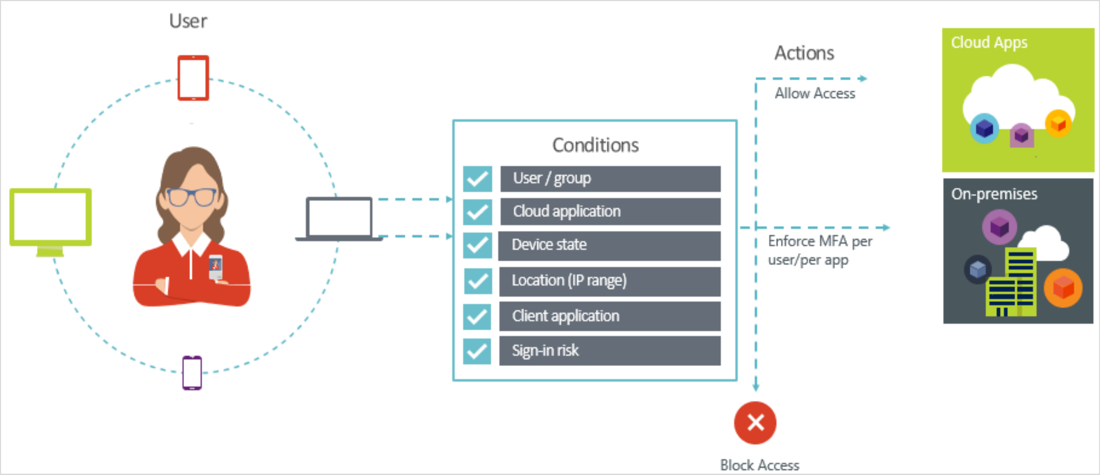
Sign-in Risk Policy



- Applied to all browser traffic and sign-ins using modern authentication
- Automatically respond to a specific risk level
- Provide the condition (risk level) and action (block or allow)
- Target all policies to specific users – omit certain types of users

Conditions

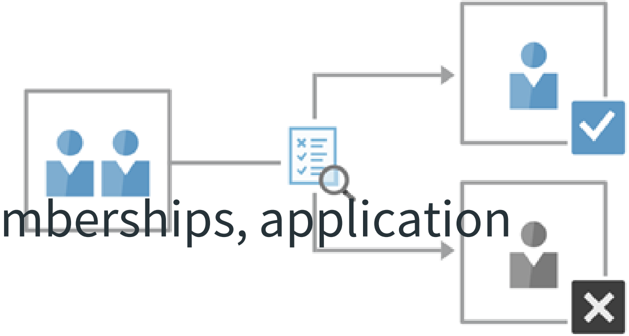
- Provide two step authentication verification
- Lets you enforce controls on access to apps based on specific conditions



Conditions –
“When this happens”

Access controls –
“Then do this”

Access Reviews



Enable organizations to recertify group memberships, application access, and privileged role assignments

- Evaluate guest user access
- Evaluate employee access to applications and group membership
- Track reviews for compliance or risk-sensitive applications
- Evaluate the role assignment of administrative users (PIM)
- Premium P2 license – Global admins and User Admins membership

Demostrations

Azure Policy

Thanks!

Any questions?

You can find me at:

@walkercet

References

- https://docs.microsoft.com/en-us/