Introduction to Azure AD Identity Protection

Identity Protection capabilities





Azure AD Identity Protection is a feature of Azure Active Directory Premium P2



- Vulnerabilities AAD analyses your configuration and detects vulnerabilities that can have an impact on your user's identities.
- Risk Events AAD uses adaptive machine learning algorithms and heuristics to detect suspicious actions that are related to your user's identities.



- Identity Protection dashboard provides reports
- Reports such as Users flagged for risk, Risk events and Vulnerabilities
- Settings such as the configuration of your Security Policies, Notifications and multifactor authentication registration



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

Types of risks





Sign in risk

- A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.
- Sign-in risk real time (such as sign-ins from anonymous IP addresses)
- Sign-in risk aggregate Total sign-in risk is the aggregate of detected real-time sign-in risks as well as any subsequent non-real-time risk events associated with the user's sign ins



User risk

- User risk reflects the overall likelihood that a bad actor has compromised a given identity. User risk contains all the risk activities for a given user, including:
 - Real-time sign-in risk
 - Subsequent sign-in risk
 - Risky user detections.

Identity protection risk detection flow



