IMPLEMENTING AZURE AD IDENTITY PROTECTION

IDENTITY PROTECTION IS A TOOL ALLOWING ORGANIZATIONS TO ACCOMPLISH 3 TASKS: AUTOMATING DETECTION AND REMEDIDATION OF IDENTITY-BASED RISKS, INVESTIGATING RISKS USING DATA IN PORTAL, AND EXPORTING RISK DETECTION DATA TO SIEM.

NOTE: FOR MORE INFORMATION CHECK OUT: [What is Azure Active Directory Identity Protection? - Microsoft Entra | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection)

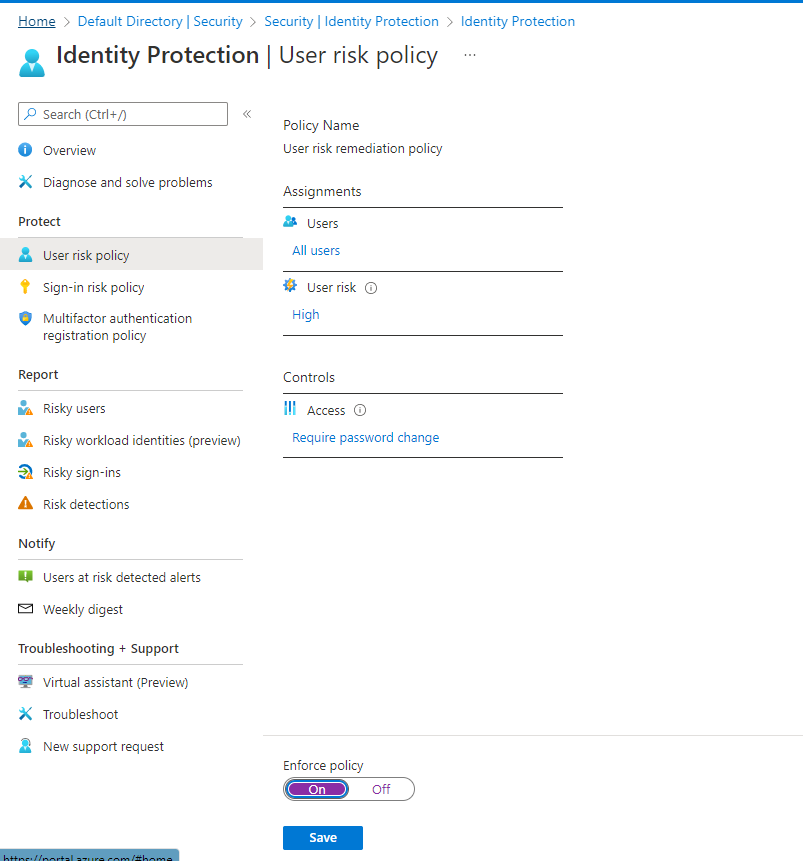
IDENTITY PROTECTION INCLUDES 3 DEFAULT POLICIES: MULTI-FACTOR AUTHENTICATION REGISTRATION POLICY, USER RISK REMEDIATION POLICY AND SIGN-IN RISK REMEDIATION POLICY.

NOTE: FOR MORE INFORMATION CHECK OUT: [Azure AD Identity Protection policies - Microsoft Entra | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies)

LAB CREATING A USER POLICY

TO GET TO POLICIES CREATION; GO TO AZURE AD 🡪 SECURITY🡪 IDENTITY PROTECTION. FROM THERE YOU CAN MANAGE THE DIFFERENT TYPE OF POLICIES, VIEW RISK REPORTS AND SEE A GRAPHICAL OVERVIEW OF RISK POLICIES OCCURRING IN YOUR ORGANIZATION.

USER RISK POLICY



FROM THE ABOVE IMAGE I CONFIGURED THE USER RISK POLICY AS FOLLOWED: TO INCLUDED ALL USERS AND NOT EXCLUDED ANYONE FOR THIS LAB PURPOSE.SET RISK LEVEL TO HIGH FOLLOWING MICROSOFTS RECOMMEDATION FOR USER RISK POLICY AND ALLOWED ACCESS WITH PASSWORD CHANGE

NOTE: FOR MORE INFORMATION ON CHOOSING RISK ACCEPTANCE CHECK OUT: [Risk policies - Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies)