Configure Azure Identity Protection (Portal)

(LAB-103-10-03)

Step 1: Enable Azure Identity Protection

1. Switch browser, login with **root administrative credentials**
2. Select the **+ Create a resource** and search for **Azure AD Identity Protection**
3. Select **Azure AD Identity Protection** and Select **Create**
4. Click on **Create**
5. Select the **All services** and search for **Azure AD Identity Protection**
6. Select **Azure AD Identity Protection** to open
7. On the **Azure AD Identity Protection** page, in the **Configure** section, click **Sign-in risk policy**.
8. On the policy page, in the **Assignments** section, click **Users**.
9. On the **Users** page, click **Select individuals and groups**
10. On the **Select users** page, select **User3**, and then click **Select**.
11. On the **Users** page, click **Done**.
12. On the policy page, in the **Assignments** section, click **Conditions**.
13. On the **Conditions** page, click **Sign-in risk**.
14. On the Sign-in risk page, select **Medium and above**, and then click **Select.**
15. On the Conditions page, click **Done**.
16. On the policy page, in the Controls section, click **Access.**
17. On the Access page, click **Allow access**, select **Require multi-factor authentication**, and then click **Select**.
18. On the policy page, click **Save.**
19. Select **Enforce Policy** as **On** & Select **Save**

Step 2: Test your conditional access policy

1. Download Tor Browser & Install

   https://www.torproject.org/download/alpha/

2. To test your policy, try to sign-in to your Azure portal as **User3** using the Tor Browser. Your sign-in attempt should be blocked by your conditional access policy.