Lab-Enable sign in and user risk policies

Lab scenario

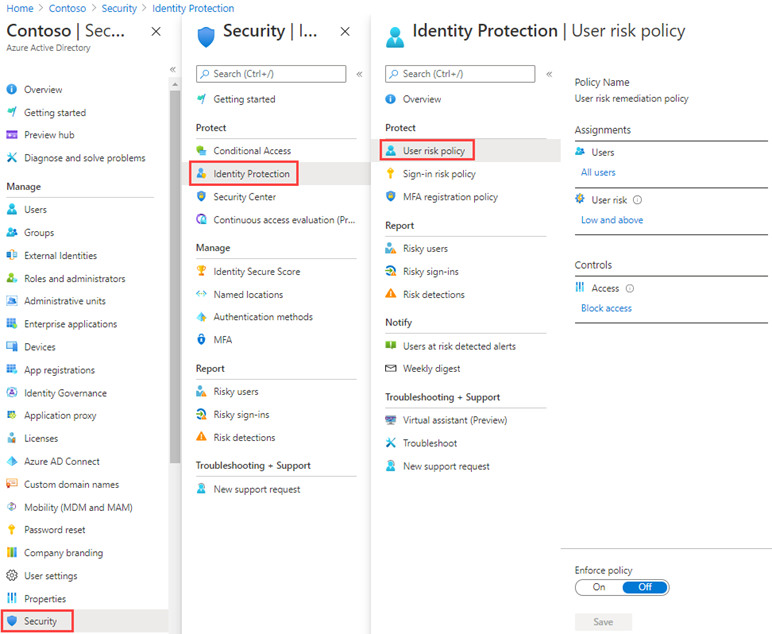
As an additional layer of security, you need to enable and configure your Azure AD organization’s sign in and user risk policies.

Estimated time: 10 minutes

Exercise 1 - Enable User risk policy

Task 1 - Configure the policy

1. Sign in to the [https://portal.azure.com](https://portal.azure.com/) using a Global administrator account.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the Azure Active Directory page, under **Manage**, select **Security**.
4. On the Security page, in the left navigation, select **Identity protection**.
5. In the Identity protection page, in the left navigation, select **User risk policy**.

[](https://microsoftlearning.github.io/SC-300-Identity-and-Access-Administrator/Instructions/Labs/media/lp2-mod4-browse-to-identity-protection.png)

1. Under **Assignments**, select **All users** and review the available options.
2. You can select from **All users** or **Select individuals and groups** if limiting your rollout.
3. Additionally, you can choose to exclude users from the policy.
4. Under **User risk**, select **Low and above**.
5. In the User risk pane, select **High** and then select **Done**.
6. Under **Controls** > **Access**, select **Block access**.
7. In the Access pane, review the available options.

**Tip** - Microsoft’s recommendation is to Allow access and Require password change.

1. Select the **Require password change** check box and then select **Done**.
2. Under **Enforce Policy**, select **On** and then select **Save**.

Task 2 - Enable Sign-in risk policy

1. On the Identity protection page, in the left navigation, select **Sign-in risk policy**.
2. As with the User risk policy, the Sign-in risk policy can be assigned to users and groups and allows you to exclude users from the policy.
3. Under **Sign-in risk**, select **Low and above**.
4. In the Sign-in risk pane, select **High** and then select **Done**.
5. Under **Controls** > **Access**, select **Block access**.
6. Select the **Require multi-factor authentication** check box and then select **Done**.
7. Under **Enforce Policy**, select **On** and then select **Save**.