**Configure conditional access (require MFA)**

In this task I will review conditional access policy settings and create a policy that requires MFA when signing into the Portal.

**Configure the policy**

1. In the **Portal,** search for and select **Microsoft Entra ID**.
2. Under **Manage,** select **Security**.
3. Under **Protect,** select **Conditional access**.
4. Click **New Policy**, then I completed the following steps:
   * Name: **AZ500Policy1**
   * Users and groups > Select users and groups > Users and Groups > Select: **AZ500User1**
   * Cloud apps or actions > Select apps > Select: **Microsoft Azure Management**
   * Review the warning that this policy impacts Portal access.
   * Conditions > Sign-in risk > Review the risk levels
   * Device platforms > Review the devices that can be included, such as Android and iOS.
   * Locations > Review the physical location selections.
   * Under **Access controls** click **Grant**.
   * Review the Grant options such as MFA. You may require one or more of the controls.
   * Select **Require multi-factor authentication**.
   * For **Enable policy,** select **On**.
5. Click **Create**.

**Test the policy**

1. Sign in to the **Portal** as the **AZ500User1**.
2. Before you can sign in, a second authentication is required.
3. If you have a phone number associated with the user, provide and verify the text code. You should be able to sign into the Portal successfully.
4. If you do not have a phone number associated with the user, this demonstrates that MFA is in effect.
5. Return to the **AZ500Policy1** and turn the policy **Off**.

**Access review**

I will configure an access review.

1. In the **Portal**, search for and select **Identity Governance**.
2. Under **Access Reviews,** select **Access Reviews**.
3. Click **New Access Review**.
4. I created an access review to ensure we validate the AZ500Admin group membership.
5. Configuration settings are added as I made selections. For example, a weekly access review, I will be prompted for the duration.
   * Review name: **AZ500Review**
   * Start date: **current date**
   * Frequency: **One-time**
   * Users to review: **Members of a group**
   * Scope: **Everyone**
   * Select a group: **AZ500Admins**
   * Reviewers: **Selected user**
   * Select reviewers: **add yourself as a reviewer**
   * Review the **Upon completion settings**, specifically the action if a reviewer doesn't respond.
   * Review **Advanced settings**.
6. **Start** the access review.
7. On the **Access review** page, ensure the new access review is listed.
8. The **Status** will change from **Not started** to **Initializing**.

**Conduct an access review.**

In this task, I conducted an access review.

1. When the access review is complete, you will receive an email. This is the email associated with your reviewer account.
2. In the email, click **Start review**.
3. On the **Access reviews** page, click the **AZ500Review**.
4. Use the **Details** link to view information about the user.
5. Select **Approve** or **Deny**. Be sure to provide a **Reason**.
6. **Submit** reviews.

**Review the access review results.**

In this task, we will review the access review results.

1. Return to the **Portal**.
2. Click the **AZ500Review**.
3. From the **Overview** blade, review the results.
4. The member is **approved** or **denied**.
5. Click **Results** for more detailed information about the reviewer and their reasons.
6. From the **Overview** blade, click **Stop** and confirm you want to stop the review.
7. The **Review status** should now be **Complete**.

**Apply the access review.**

In this task, l appled the review results.

1. In the **Portal**, search for and select **Microsoft Entra ID**.
2. Under **Manage,** select **Groups**.
3. Locate the **AZ500Admins** group.
4. Review the members of the group.
5. Confirm the members.
6. Return to the **AZ500Review**.
7. Click **Apply**.
8. Confirm that you want to remove any denied members.
9. The **Review status** will change from **Applying** to **Result applied**.
10. Verify the **AZ500Admins** group now only has approved members.