Multi-Factor Authentication (MFA) enhances the security of user sign-ins for Microsoft Entra ID (Azure Active Directory). Here’s how you can configure and enforce MFA for users using the Azure portal:

**Step 1: Sign in to the Azure Portal**

1. **Go to the Azure portal**: [Azure Portal](https://portal.azure.com/)
2. **Sign in** with your Azure account credentials.

**Step 2: Navigate to Azure Active Directory**

1. **Open Azure Active Directory**:
   * In the left-hand navigation pane, click on **Azure Active Directory**.

**Step 3: Access Security Settings**

1. **Go to Security**:
   * In the Azure Active Directory pane, select **Security**.
2. **Select MFA**:
   * In the Security pane, click on **Multi-Factor Authentication**.

**Step 4: Configure MFA**

1. **Go to MFA Service Settings**:
   * In the Multi-Factor Authentication pane, click on **MFA service settings**.
2. **Configure User Settings**:
   * Under **Verification options**, select the methods that users can use to verify their identities (e.g., call to phone, text message to phone, notification through mobile app, verification code from mobile app or hardware token).
   * Under **Remember multi-factor authentication**, select the option to allow users to bypass MFA for a certain number of days on trusted devices if you want.
3. **Save the Settings**:
   * Click **Save** to apply your settings.

**Step 5: Enforce MFA for Users**

1. **Go to Users**:
   * In the Azure Active Directory pane, click on **Users**.
2. **Manage Multi-Factor Authentication**:
   * Click on **Per-user MFA**. This will open a new tab showing the Multi-Factor Authentication page for your directory.
3. **Enable MFA for Users**:
   * On the Multi-Factor Authentication page, you will see a list of your users.
   * Select the users you want to enable MFA for.
   * Click on **Enable** to enable MFA for the selected users.
   * Confirm by clicking **Enable multi-factor auth** in the dialog box that appears.

**Step 6: User Setup**

1. **User Sign-In**:
   * When users next sign in, they will be prompted to set up MFA.
2. **Follow Setup Steps**:
   * Users will need to follow the on-screen instructions to complete the setup, which typically includes verifying a phone number and setting up an authentication app.

**Optional: Configure Conditional Access Policies**

For more granular control, you can use Conditional Access policies to enforce MFA under specific conditions.

1. **Go to Conditional Access**:
   * In the Azure Active Directory pane, select **Security** and then **Conditional Access**.
2. **Create a New Policy**:
   * Click **+ New policy**.
3. **Name and Assignments**:
   * **Name**: Give your policy a name.
   * **Assignments**: Select users or groups to apply the policy to.
   * **Cloud apps or actions**: Choose the applications or actions the policy will apply to.
4. **Conditions**:
   * Configure conditions such as sign-in risk, device platforms, and locations if needed.
5. **Access Controls**:
   * Under **Grant**, select **Require multi-factor authentication**.
6. **Enable the Policy**:
   * Set **Enable policy** to **On**.
   * Click **Create** to create and apply the policy.