**Prerequisites**

To complete the scenario in this tutorial, you need:

* **Access to Azure AD Premium edition**, which includes conditional access policy capabilities. To enforce MFA, you need to create an Azure AD conditional access policy. Note that MFA policies are always enforced at your organization, regardless of whether the partner has MFA capabilities. If you set up MFA for your organization, you’ll need to make sure you have sufficient Azure AD Premium licenses for your guest users.
* **A valid external email account** that you can add to your tenant directory as a guest user and use to sign in.

**Create a test guest user in Azure AD**

1. Sign in to the [Azure portal](https://portal.azure.com/) as an Azure AD administrator.
2. In the left pane, select **Azure Active Directory**.
3. Under **Manage**, select **Users**.
4. Select **New guest user**.
5. Under **User name**, enter the email address of the external user. Optionally, include a welcome message.
6. Select **Invite** to automatically send the invitation to the guest user. A **Successfully invited user** message appears.
7. After you send the invitation, the user account is automatically added to the directory as a guest.

**Test the sign-in experience before MFA setup**

1. Use your test user name and password to sign in to your [Azure portal](https://portal.azure.com/).
2. Note that you’re able to access the Azure portal using just your sign-in credentials. No additional authentication is required.
3. Sign out.

**Create a conditional access policy that requires MFA**

1. Sign in to your [Azure portal](https://portal.azure.com/) as global administrator, security administrator, or a conditional access administrator.
2. In the Azure portal, select **Azure Active Directory**.
3. On the **Azure Active Directory** page, in the **Security** section, select **Conditional access**.
4. On the **Conditional Access** page, in the toolbar on the top, select **New policy**.
5. On the **New** page, in the **Name** textbox, type **Require MFA for B2B portal access**.
6. In the **Assignments** section, select **Users and groups**.
7. On the **Users and groups** page, choose **Select users and groups**, and then select **All guest users (preview)**.
8. Select **Done**.
9. On the **New** page, in the **Assignments** section, select **Cloud apps**.
10. On the **Cloud apps** page, choose **Select apps**, and then choose **Select**.
11. On the **Select** page, choose **Microsoft Azure Management**, and then choose **Select**.
12. On the **Cloud apps** page, select **Done**.
13. On the **New** page, in the **Access controls** section, select **Grant**.
14. On the **Grant** page, choose **Grant access**, select the **Require multi-factor authentication**check box, and then choose **Select**.
15. Under **Enable policy**, select **On**.
16. Select **Create**.

**Use the What If option to simulate sign-in**

1. On the **Conditional access - Policies** page, select **What If**.
2. Select **User**, choose your test guest user, and then choose **Select**.
3. Select **Cloud apps**.
4. On the **Cloud apps** page, choose **Select apps** and then click **Select**. In the applications list, select **Microsoft Azure Management**, and then click **Select**.
5. On the **Cloud apps** page, select **Done**.
6. Select **What If**, and verify that your new policy appears under **Evaluation results** on the **Policies that will apply** tab.

**Test your conditional access policy**

1. Use your test user name and password to sign in to your [Azure portal](https://portal.azure.com/).
2. You should see a request for additional authentication methods. Note that it could take some time for the policy to take effect.
3. Sign out.

**Clean up resources**

When no longer needed, remove the test user and the test conditional access policy.

1. Sign in to the [Azure portal](https://portal.azure.com/) as an Azure AD administrator.
2. In the left pane, select **Azure Active Directory**.
3. Under **Manage**, select **Users**.
4. Select the test user, and then select **Delete user**.
5. In the left pane, select **Azure Active Directory**.
6. Under **Security**, select **Conditional Access**.
7. In the **Policy Name** list, select the context menu (…) for your test policy, and then select **Delete**. Select **Yes** to confirm. ## Next steps In this tutorial, you’ve created a conditional access policy that requires guest users to use MFA when signing in to one of your cloud apps. To learn more about adding guest users for collaboration, see [Add Azure Active Directory B2B collaboration users in the Azure portal](https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-users-administrator).