**Lesson 4 Demo 2**

**AAD Identity Protection**

**Objective**: Demonstrate Azure AD Premium features for Identity Protection

**Tools required**: Azure account with administrator access

**Prerequisites**: None

**Steps to be performed:**

1. Deploy an Azure VM (Virtual Machine) by using an Azure Resource Manager template
2. Implement Azure AD (Active Directory) Identity Protection
3. Validate Azure AD Identity Protection configuration by simulating risk events

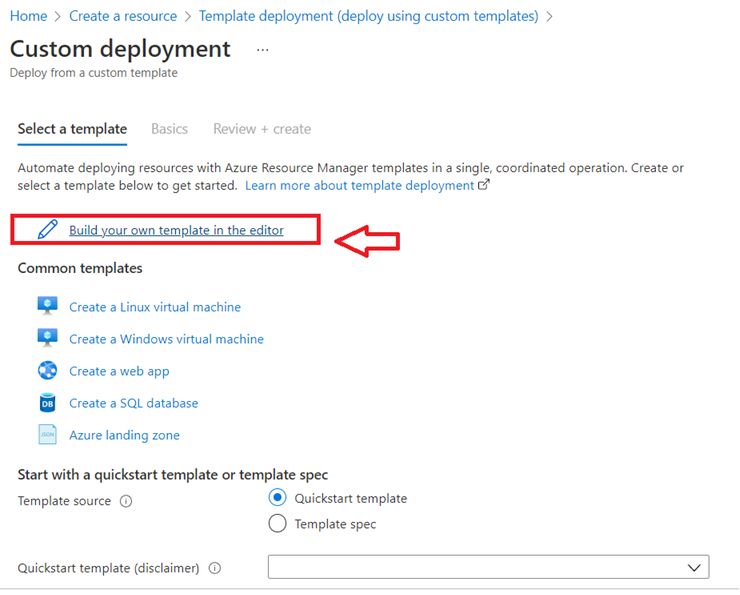
**Step 1: Deploy an Azure VM by using an Azure Resource Manager template**

* 1. Browse to the Azure portal at [**http://portal.azure.com**](http://portal.azure.com/) and sign in by using a Microsoft account
  2. In the Azure portal, navigate to the **New** blade
  3. From the **New** blade, search Azure Marketplace for **Template deployment**

Graphical user interface, text, application

Description automatically generated

* 1. Use the list of search results to navigate to the **Custom deployment** blade
  2. On the **Custom deployment** blade, select the **Build your own template in the editor**

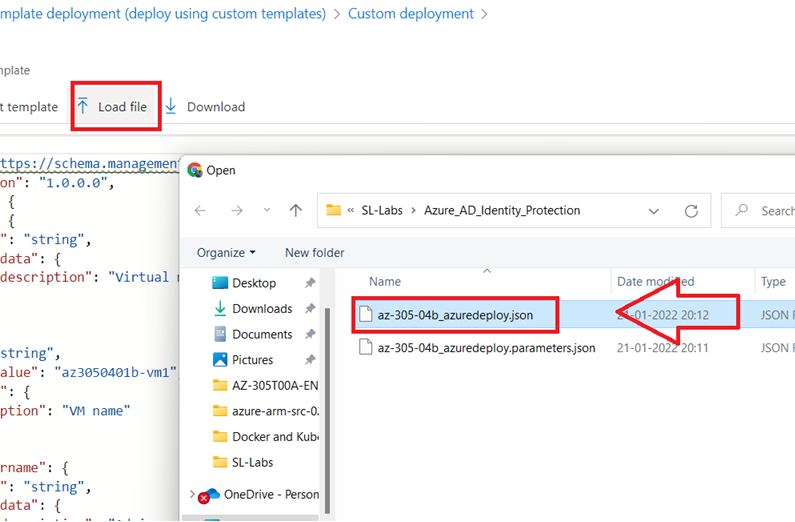


* 1. From the **Edit template** blade, load the template file from

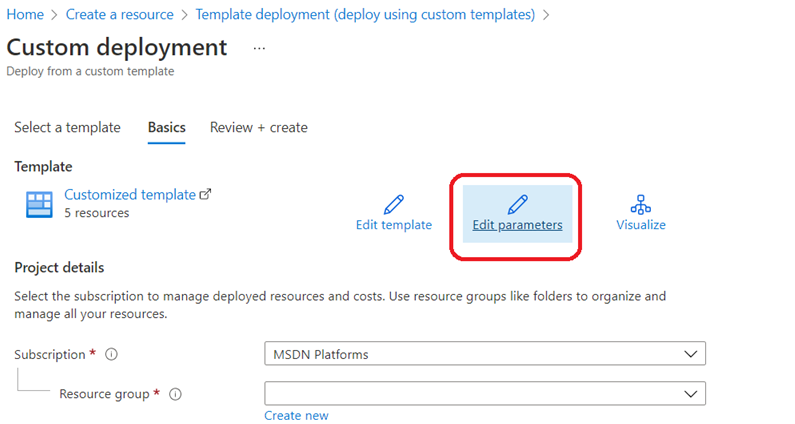
[**https://github.com/Simplilearn-Edu/AZ-305/4.02\_azuredeploy.json**](https://github.com/Simplilearn-Edu/AZ-305/4.02_azuredeploy.json)

**Github link:** [**https://github.com/Simplilearn-Edu/AZ-305**](https://github.com/Simplilearn-Edu/AZ-305)

**Note**: Review the content of the template and note that it defines deployment of an Azure VM hosting Windows Server 2016 Datacentre.

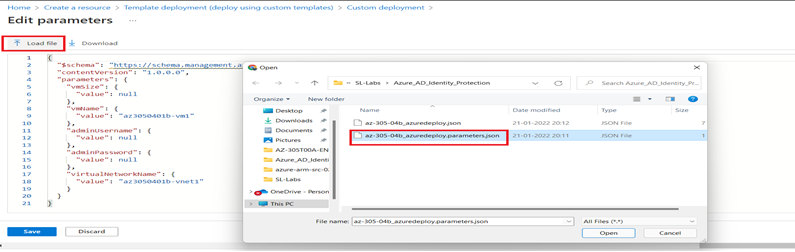


* 1. Save the template and return to the **Custom deployment blade**
  2. From the **Custom deployment** blade, navigate to the **Edit parameters** blade



1.9 From the **Edit parameters** blade, load the parameters file **https://github.com/Simplilearn-Edu/AZ-305/4.02\_azuredeploy.parameters.json**

**Github Link: https://github.com/Simplilearn-Edu/AZ-305**



* 1. Save the parameters and return to the **Custom deployment** blade
  2. From the **Custom deployment** blade, initiate a template deployment with the following settings:

Subscription: The name of the subscription you are using in this lab

Resource group: The name of a new resource group **az3050401b-RG**

Location: The name of the Azure region which is closest to the lab location and where you can provision Azure VMs (virtual machines)

VM Size: **Standard\_D2S\_V3**

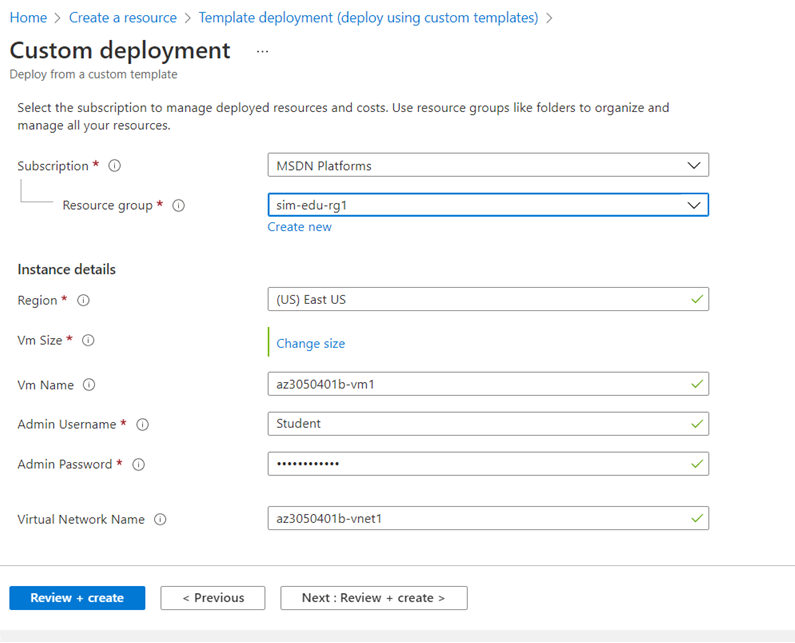
VM Name: **az3050401b-vm1**

Admin Username: **Student**

Admin Password: **Pa55w.rd1234**

Virtual Network Name: **az3050401b-vnet1**

**Note**: To identify Azure regions where you can provision Azure VMs, refer to [**https://azure.microsoft.com/en-us/regions/offers/**](https://azure.microsoft.com/en-us/regions/offers/)

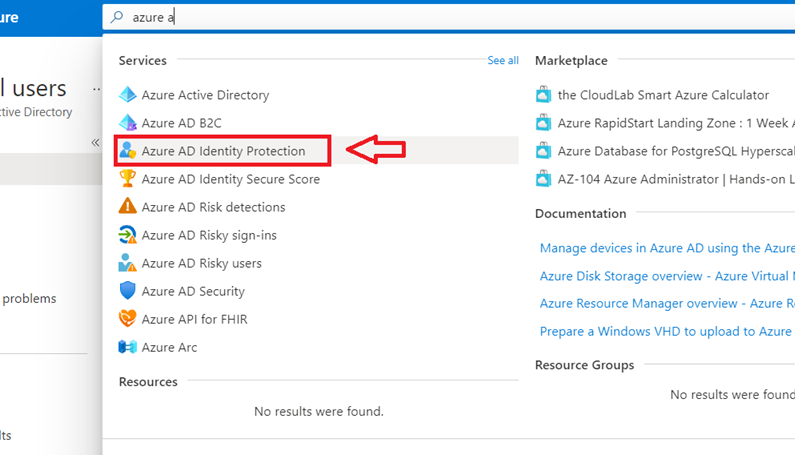


**Note**: Do not wait for the deployment to complete but proceed to the next exercise. You will use the virtual machine included in this deployment in the last exercise of this lab.

**Result**: After you completed this exercise, you have initiated a template deployment of an Azure VM **az3050401b-vm1** that you will use in the next exercise of this lab.

**Step 2: Implement Azure AD Identity Protection**

* 1. From the **Azure AD Identity Protection** blade, navigate to the **Azure AD Identity Protection - User risk policy** blade



* 1. On the **Azure AD Identity Protection - User risk policy** blade, configure the **User risk remediation policy** with the following settings:

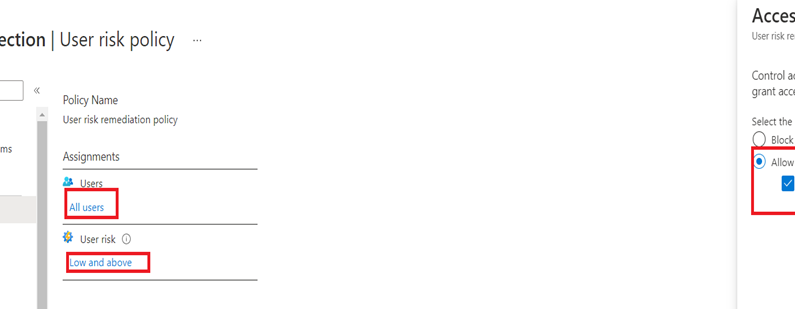
Assignments:

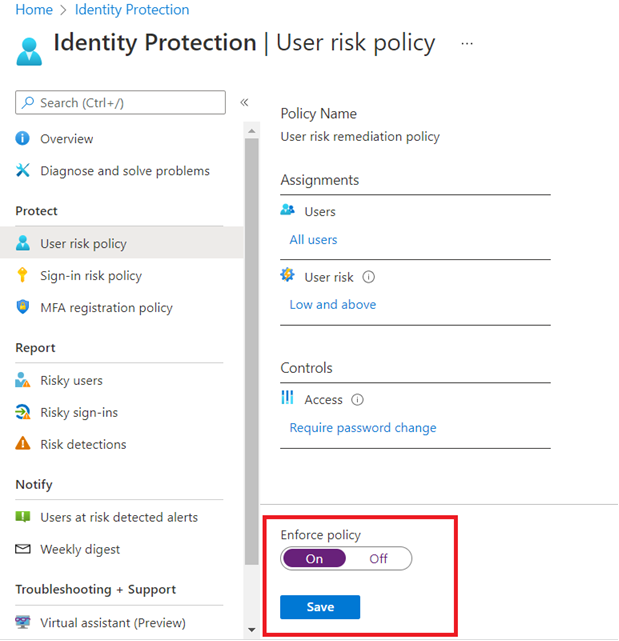
Users: **All users** (be sure to exclude the current admin account to avoid getting locked out of the tenant)

Conditions > User risk: **Low and above**

Controls > Access: **Allow access**

**Require password change** > Enforce Policy: **On**





2.3 From the **Azure AD Identity Protection - User risk policy** blade, navigate to the **Azure AD Identity Protection - Sign-in risk policy** blade

* 1. On the **Azure AD Identity Protection - Sign-in risk policy** blade, configure the **Sign-in risk remediation policy** with the following settings:

Assignments:

Users: **All users**

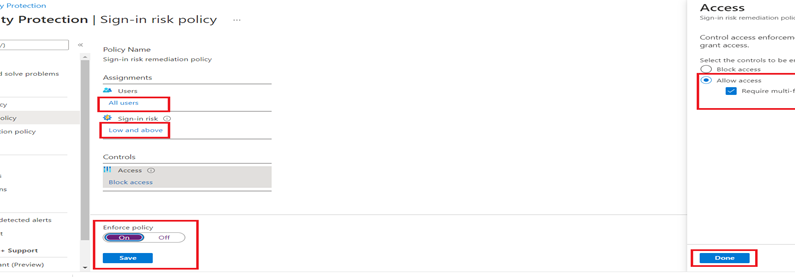
Conditions > User risk: **Medium and above**

Controls > Access: **Allow access**

**Require multi-factor authentication**

Enforce Policy: **On**

2.5 Click on **Save** and **Done**



**Step 3: Validate Azure AD Identity Protection configuration by simulating risk events**

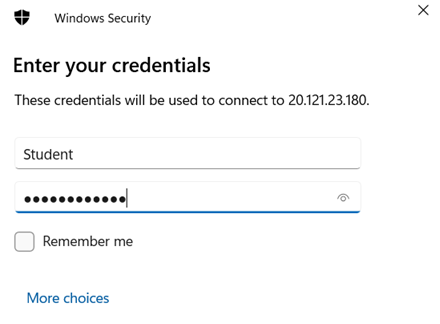
**Note**: Before you start this task, ensure that the template deployment you started has been completed.

3.1 In the Azure portal, navigate to the **az3050401b-vm1** blade

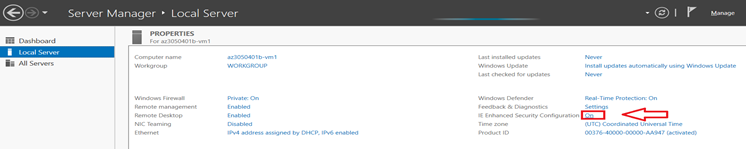
3.2 From the **az3050401b-vm1** blade, connect to the Azure VM via Remote Desktop session and when prompted to sign in, provide the following credentials:

Admin Username: **Student**

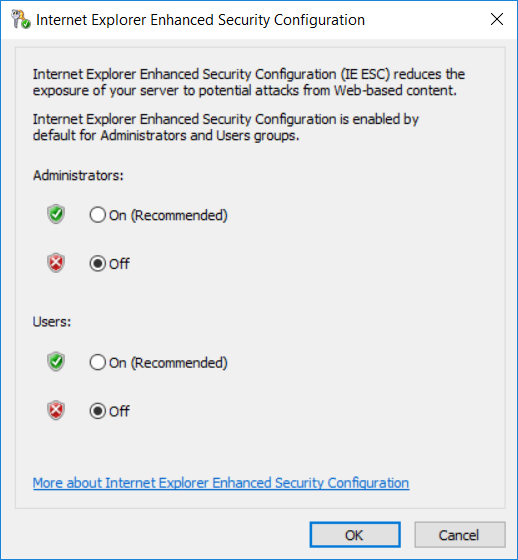
Admin Password: **Pa55w.rd1234**



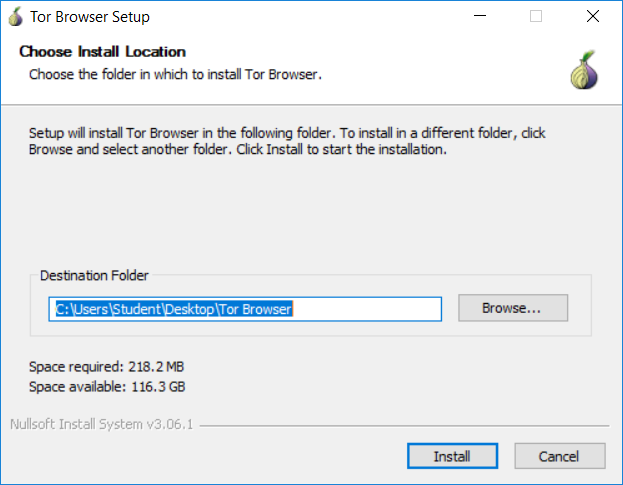
* 1. Within the Remote Desktop session, in Server Manager, click on **Local Server** and then click on **IE Enhanced Security Configuration**



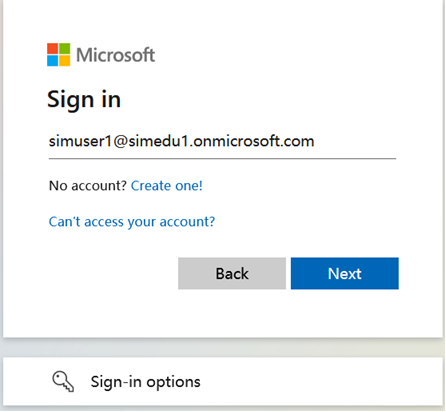
* 1. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click on **OK**



* 1. Within the Remote Desktop session, open an InPrivate Internet Explorer window
  2. In the new browser window, navigate to the ToR Browser Project at [**https://www.torproject.org/projects/torbrowser.html.en**](https://www.torproject.org/projects/torbrowser.html.en), download the ToR Browser, and install it with the default options



* 1. Once the installation completes, start the ToR Browser, use the **Connect** option on the initial page, and navigate to the Application Access Panel at [**https://myapps.microsoft.com**](https://myapps.microsoft.com/)
  2. When prompted, sign in with the **simuser1@simedu1.onmicrosoft.com** account you created in the previous exercise



* 1. You will be presented with the message **Your sign-in was blocked**. This is expected since this account is not configured with multi-factor authentication, which is required due to increased sign-in risk associated with the use of ToR Browser.

