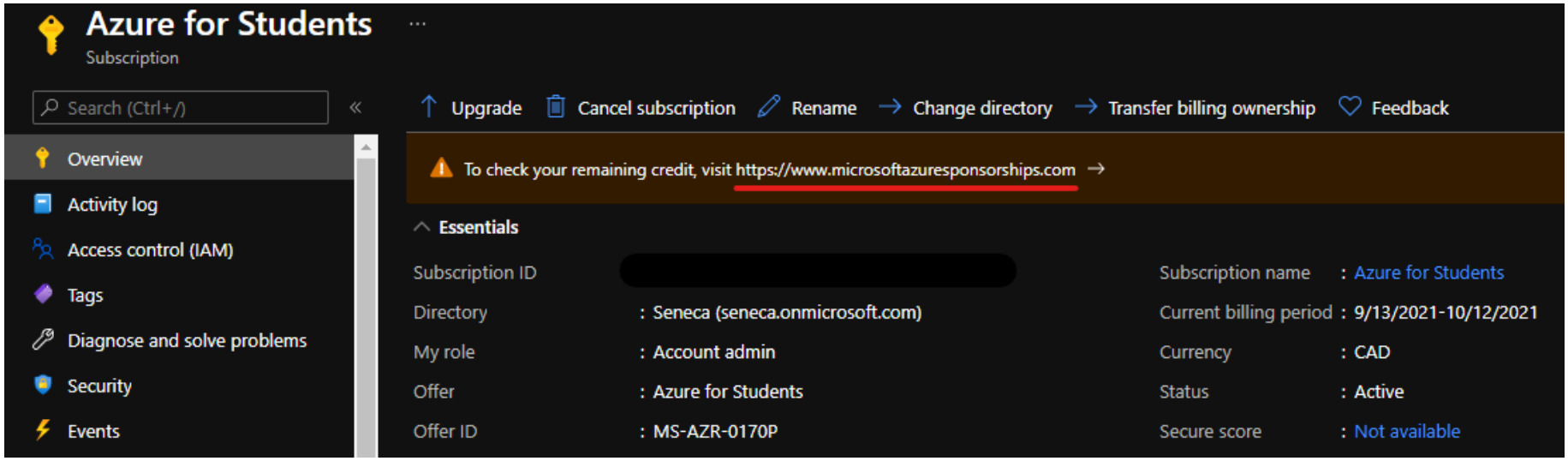
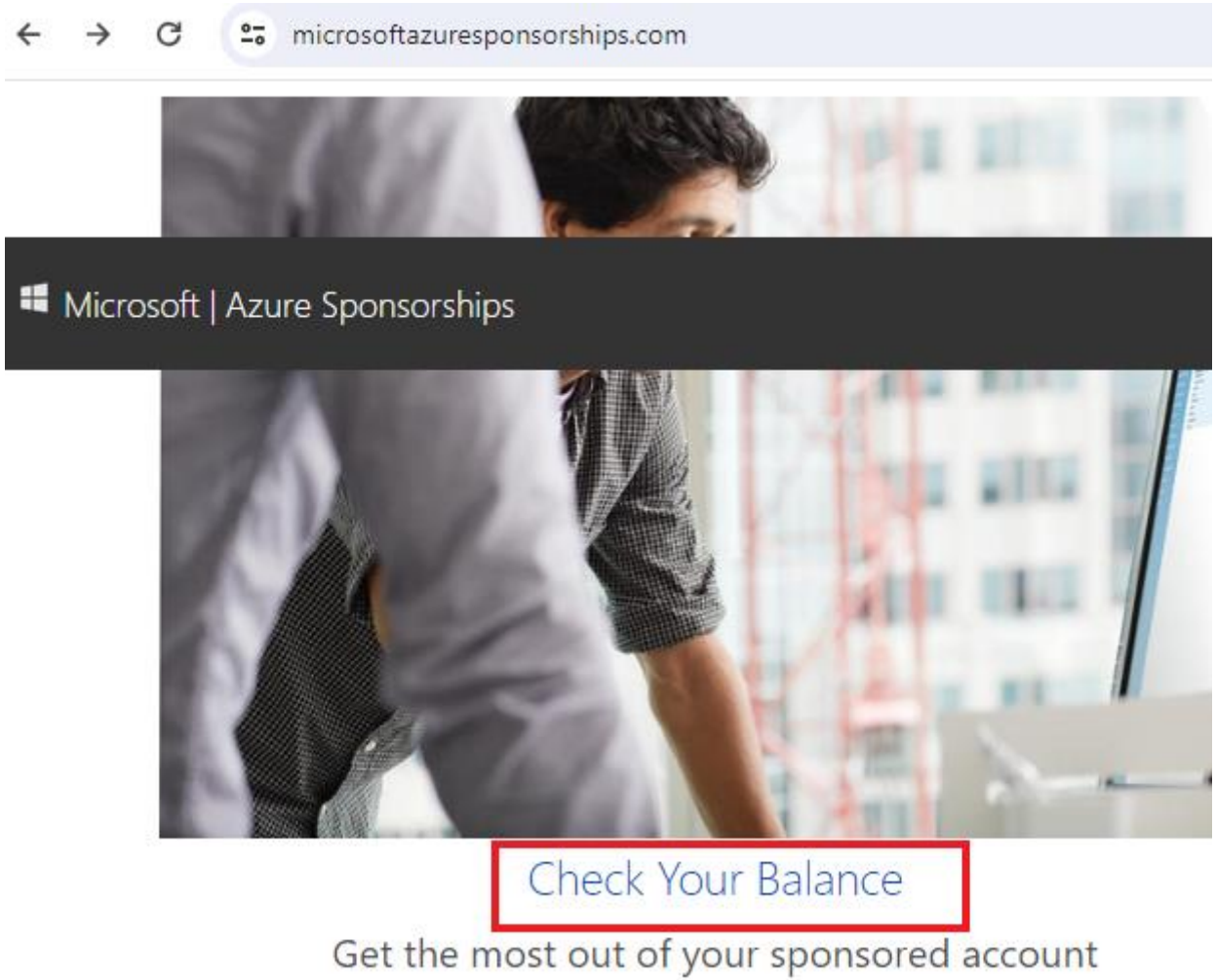
Seneca

Lab 12: Implement Azure Key Vault

At the end of each lab, any resources you created in your account will be preserved. Some Azure resources, such as VM instances, may be automatically shut down, while other resources, such as storage services will be left running. Keep in mind that some Azure features cannot be stopped and can still incur charges (i.e. Azure Bastion). To minimize your costs, delete all resources and recreate them as needed to test your work during a session.





Reference: AZ-900T0X-MICROSOFTAZUREFUNDAMENTALS

12 - Implement Azure Key Vault

In this walkthrough, we will create an Azure Key vault and then create a password secret within that key vault, providing a securely stored, centrally managed password for use with applications.

Task 1: Create an Azure Key Vault (5 min)

1. Sign in to the Azure portal with your **`odl_user_xxx`** azure account
2. From the **All services** blade, search for and select **Key vaults**, then select **+ Create.**
3. Configure the key vault (replace **xxxx** in the name of the key vault with letters and digits such that the name is globally unique). Leave the defaults for everything else.

Setting	Value
Subscription	**Use your subscription** (you should see “Seneca College : <course name>”)
Resource group	**myRGKV** (create new)
Key vault name	**<studentID>keyvaulttestxxx (example: smore1keyvaulttest1234)**
Location	**East US**
Pricing tier	**Standard**

4. Click **Review + create**, and then click **Create**.
5. Once the new key vault is provisioned, click **Go to resource**. Or you can locate your new key vault by searching for it.

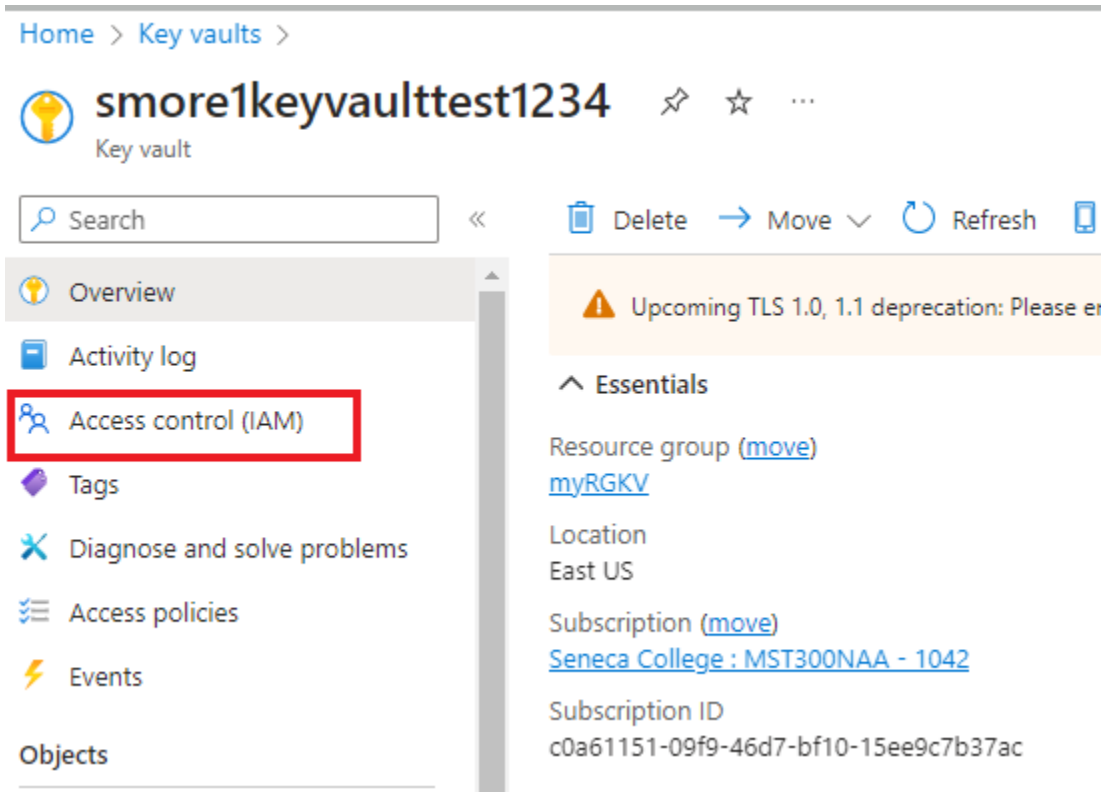
6. Click on the key vault **Overview** tab and take note of the **DNS name**. Applications that use your vault through the REST API will need this URI.
7. Take a moment to browse through some of the other key vault options.
   Under **Settings** review **Keys**, **Secrets**, **Certificates**, **Access Policies**, **Firewalls and virtual networks**.

   Note: Your Azure account is the only one authorized to perform operations on this new vault. You can modify this if you wish in the **Settings** and then the **Access policies** section.

Task 2: Add a secret to the Key Vault

In this task, we grant the proper permission to manage the key vault.

1. Add the KeyVaul Admin access to your odl_user account. Go to your KeyVault and select **Access control (IAM)**
2. Select the **+ Add** and **Add Role Assignemnt** tab
3. Select **Role** and seach/select for **Key Vault Administrator**
4. Go to the Members tab and click in **+select members** and look for **`odl_user_xxx`** account
5. Click in **Review + assign**



In this task, we will add a password to the key vault.

6. Under **Objects** click **Secrets**, then click **+ Generate/Import**.
7. Configure the secret. Leave the other values at their defaults. Notice you can set an activation and expiration date. Notice you can also disable the secret.

Setting	Value
Upload options	**Manual**
Name	**ExamplePassword**
Value	**<studentID>password (example: smore1password)**

8. Click **Create**.
9. Once the secret has been successfully created, click on the **ExamplePassword**, and note it has a status of **Enabled**
10. Click the current version, note the the **Secret Identifier**. This is the url value that you can now use with applications. It provides a centrally managed and securely stored password.
11. Click the button **Show Secret Value**, to display the password you specified earlier.

Congratulations! You have created an Azure Key vault and then created a password secret in that key vault, providing a securely stored, centrally managed password for use with applications.

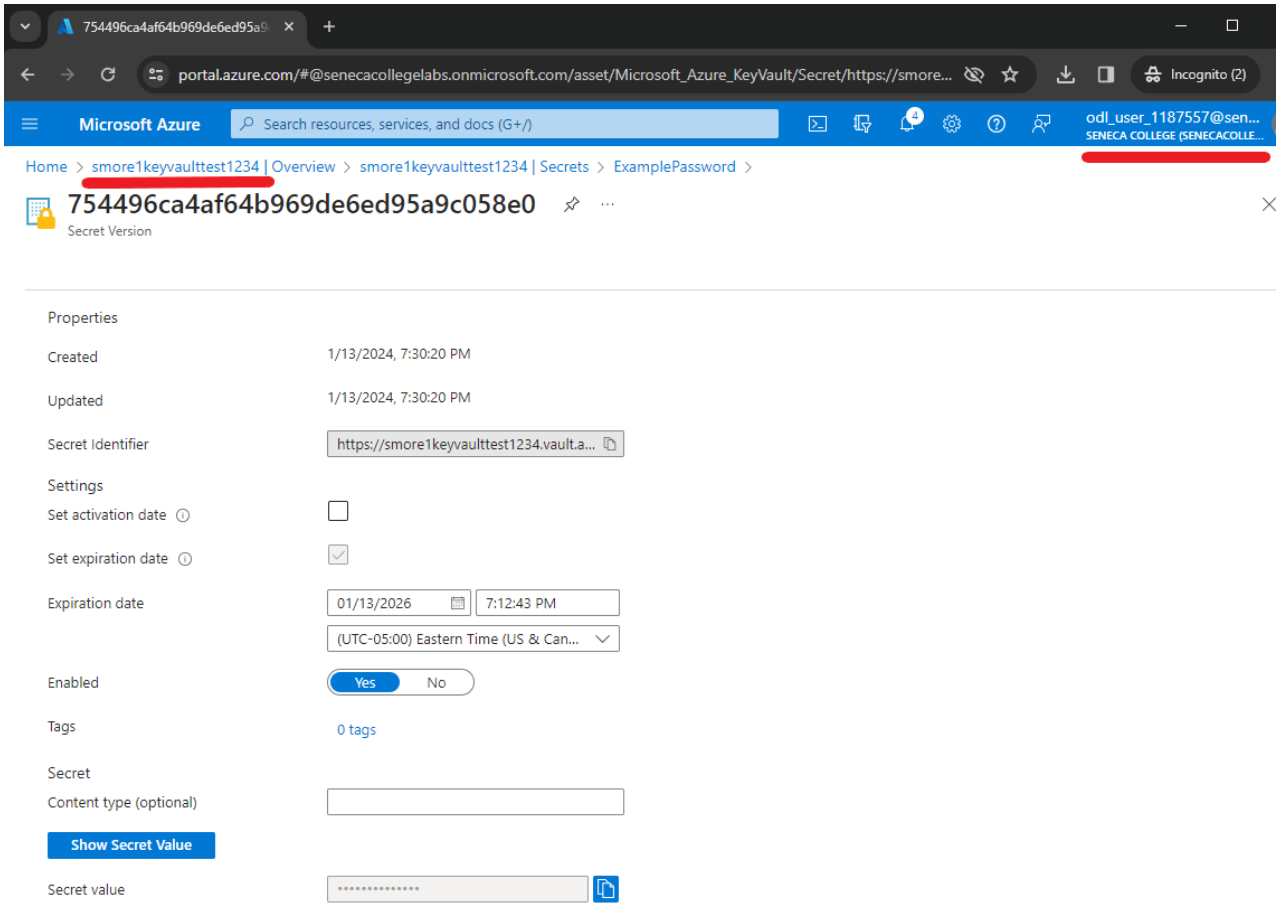
Note: To avoid additional costs, you can remove all resources in the resource group. Search for resource groups, click your resource group, and then delete the resources within the resource group. **DO NOT DELETE YOUR RESOURCE GROUP.**

Submission Requirements

Submit a screenshot with the following information:

Screenshot #1:

- Value of secret created in Key Vault
- The Azure Portal with your login ID
    - **Note**: underline the above items as described in the below picture



Screenshot #2:

- Successful deletion of all resources within resource group. **DO NOT DELETE YOUR RESOURCE GROUP!**
    - To delete all resources with a resource group, go to "**Resource Group**", select "**myRGKV**", select all resources within the resource group, and select "**Delete**"