

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Course: **Cloud and Network Security C3-2024**

Student Name: **Loise Murugi Murage**

Student No: **CS-CNS07-24115.**

Sunday, November 10, 2024

Week 9 Assignment 1

Class Exercise: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Contents

Class Exercise: Key Vault (Implementing Secure Data by setting up Always Encrypted).....	1
Introduction.....	3
Instructions	3
Exercise 1: Deploy the base infrastructure from an ARM template	3
Task 1: Deploy an Azure VM and an Azure SQL database	3
Exercise 2: Configure the Key Vault resource with a key and a secret	8
Task 1: Create and configure a Key Vault	8
Task 2: Add a key to Key Vault	14
Task 3: Add a Secret to Key Vault	18
Exercise 3: Configure an Azure SQL database and a data-driven application	22
Task 1: Enable a client application to access the Azure SQL Database service.	22
Task 2: Create a policy allowing the application access to the Key Vault.....	28
Task 3: Retrieve SQL Azure database ADO.NET Connection String.....	31
Task 4: Log on to the Azure VM running Visual Studio 2019 and SQL Management Studio	34
Task 5: Create a table in the SQL Database and select data columns for encryption	35
Exercise 4: Demonstrate the use of Azure Key Vault in encrypting the Azure SQL database	49
Task 1: Run a data-driven application to demonstrate the use of Azure Key Vault	49
Clean up resources	60
Conclusion	62

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Introduction

In this exercise, we will be using Azure SQL Database to encrypting content of columns in database tables by using Always Encrypted and set up automated ARM template deployment, to set up a Virtual Machine with Visual Studio 2019 .NET, and use C# language and SQL Server Management Studio 19. Then we will configure the Key Vault resource with a key and a secret, the keys and the secret will be stored in vault. Key Vault enables Microsoft Azure applications and users to store and use several types of secret/key data which are collectively referred to as objects.

We will be using JSON Azure Resource Manager (ARM) templates to enable us to define the infrastructure requirements.

For this lab, I have used West US region.

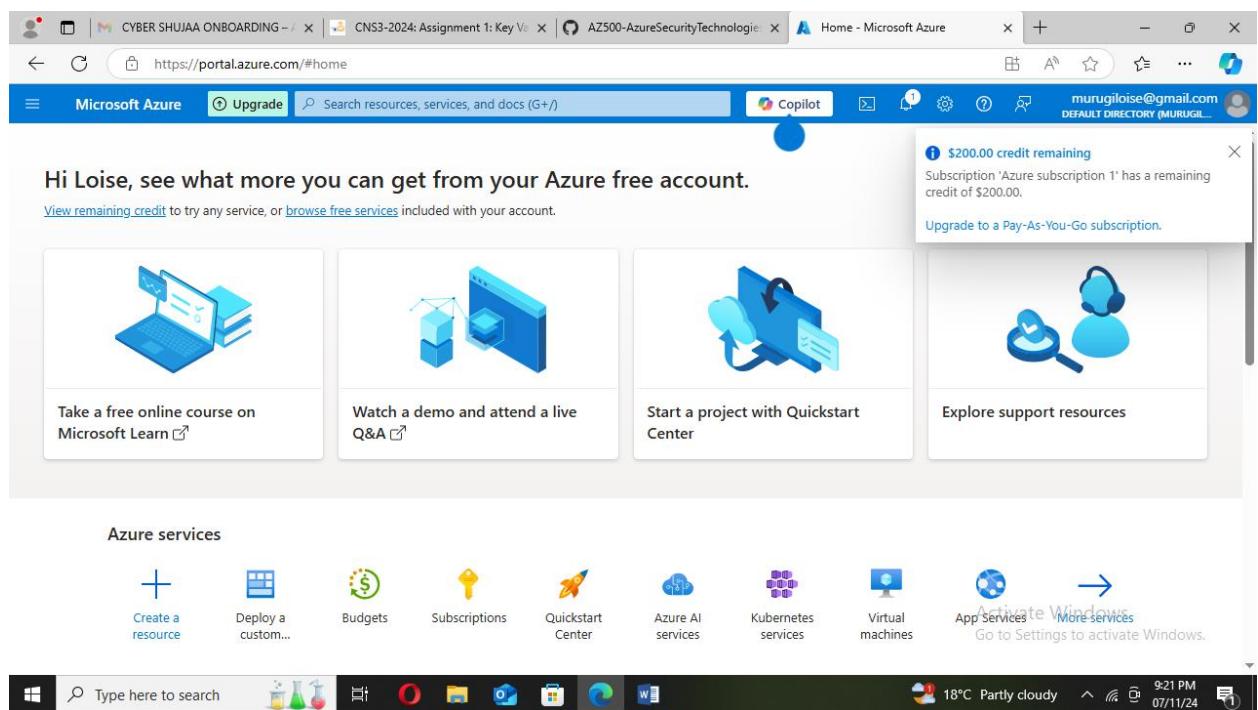
Instructions

Exercise 1: Deploy the base infrastructure from an ARM template

Task 1: Deploy an Azure VM and an Azure SQL database

In this task, you will deploy an Azure VM, which will automatically install Visual Studio 2019 and SQL Server Management Studio 19 as part of the deployment.

1. Sign-in to the Azure portal <https://portal.azure.com/>.



Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Deploy a custom template** and press the **Enter** key

The screenshot shows the Azure portal's 'Custom deployment' blade. At the top, there are tabs for 'Select a template', 'Basics', and 'Review + create'. Below these, a section titled 'Common templates' lists options like 'Create a Linux virtual machine', 'Create a Windows virtual machine', 'Create a web app', 'Create a SQL database', and 'Azure landing zone'. A note below says 'Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started.' A link 'Learn more about template deployment' is provided. Under 'Start with a quickstart template or template spec', there are 'Template source' and 'Quickstart template' options. On the right, there are 'Activate Windows' and 'Go to Settings to activate Windows' links. The browser address bar shows 'https://portal.azure.com/#create/Microsoft.Template'.

3. On the **Custom deployment** blade, click the **Build your own template in the editor** option.

The screenshot shows the Azure portal's 'Edit template' blade. At the top, there are tabs for '+ Add resource', 'Quickstart template', 'Load file', and 'Download'. Below these, a sidebar lists 'Parameters (0)', 'Variables (0)', and 'Resources (0)'. The main area contains a JSON code editor with the following content:

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {},
5   "resources": []
6 }
```

At the bottom, there are 'Save' and 'Discard' buttons. On the right, there are 'Activate Windows' and 'Go to Settings to activate Windows' links. The browser address bar shows 'https://portal.azure.com/#view/HubsExtension/TemplateEditorBladeV2/template/%7B%0A%20%20%20%24schema%3A%20"https...'

4. On the **Edit template** blade, click **Load file**, locate the **\Allfiles\Labs\10\az-500-10_azuredeploy.json** file and click **Open**.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

```
$schema: "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
contentVersion: "1.0.0.0",
parameters": {
  "adminUsername": {
    "type": "string",
    "minLength": 1,
    "defaultValue": "Student",
    "metadata": {
      "description": "Username for the Virtual Machine."
    }
  },
  "adminPassword": {
    "type": "securestring",
    "defaultValue": "Pa55w.rdi1234",
    "metadata": {
      "description": "Password for the Virtual Machine."
    }
  }
}
```

Save Discard

- On the **Edit template** blade, click **Save**.

Select a template Basics Review + create

Template

Customized template 7 resources

Edit template Edit parameters Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * (Azure subscription 1) Resource group * (Create new)

Previous Next Review + create

- On the **Custom deployment** blade, under **Deployment Scope** ensure that the following settings are configured (leave any others with their default values):

Setting	Value
Subscription	the name of the Azure subscription you will be using in this lab

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Setting	Value
Resource group	click Create new and type the name AZ500LAB10
Location	East US
Username	Student
Password	Please use your personal password created in Lab 02 > Exercise 2 > Task 1 > Step 3.

1. **Note:** While you can change the administrative credentials used for logging on to the Virtual Machine, you don't have to.⁷ Click the **Review and Create** button, and confirm the deployment by clicking the **Create** button.

Note: This initiates the deployment of the Azure VM and Azure SQL Database required for this lab.

Note: Do not wait for the ARM template deployment to be completed, but instead continue to the next exercise. The deployment might take between **20-25 minutes**.

The screenshot shows the Microsoft Azure portal interface for creating a new resource group. The URL in the browser is <https://portal.azure.com/#create/Microsoft.Template>. The page title is "Custom deployment". The "Project details" section shows "Subscription * (Azure subscription 1)" and "Resource group * (AZ500LAB10)". A link to "Create new" is visible. The "Instance details" section includes "Region * (US) West US", "Admin Username (Student)", and "Admin Password (*****)". At the bottom, there are "Previous" and "Next" buttons, and a prominent blue "Review + create" button. The status bar at the bottom right shows "Activate Windows Go to Settings to activate Windows.", the date "08/11/24", and the time "12:29 PM".

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Microsoft Azure 'Custom deployment' interface. At the top, there are tabs for 'Select a template', 'Basics', and 'Review + create'. The 'Review + create' tab is selected. Below it, under 'Summary', there is a section for a 'Customized template' which contains '7 resources'. There is also a 'Terms' section with links to 'Azure Marketplace Terms' and 'Azure Marketplace'. A note states: 'By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.' Another note says: 'Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.' At the bottom, there are 'Previous', 'Next', and 'Create' buttons. On the right, there is an 'Activate Windows' link.

At this point we have initiated a deployment of the Azure VM and Azure SQL Database. From the screenshot below, our deployment is completed.

The screenshot shows the Microsoft Azure 'Overview' page for a deployment named 'Microsoft.Template-20241108215449'. The main panel displays the message: 'Your deployment is complete'. It provides deployment details: Deployment name: Microsoft.Template-20241108215449, Start time: 11/8/2024, 9:55:13 PM, Subscription: Azure subscription 1, Correlation ID: f5f96628-e2d7-4eff-ab49-37fd..., and Resource group: AZ500LAB10. Below this, there are sections for 'Deployment details' and 'Next steps', with a 'Go to resource group' button. To the right, there are promotional cards for 'Cost management', 'Microsoft Defender for Cloud', 'Free Microsoft tutorials', and 'Work with an expert'. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date as 08/11/24.

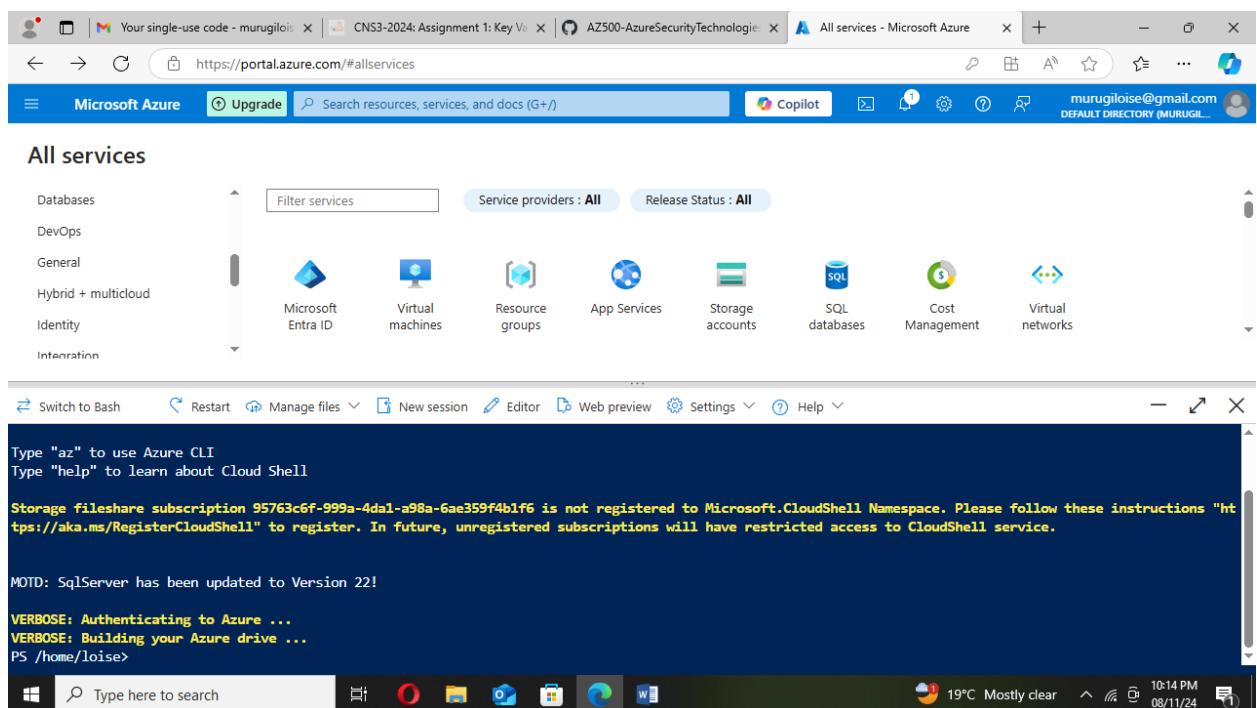
Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Exercise 2: Configure the Key Vault resource with a key and a secret

Task 1: Create and configure a Key Vault

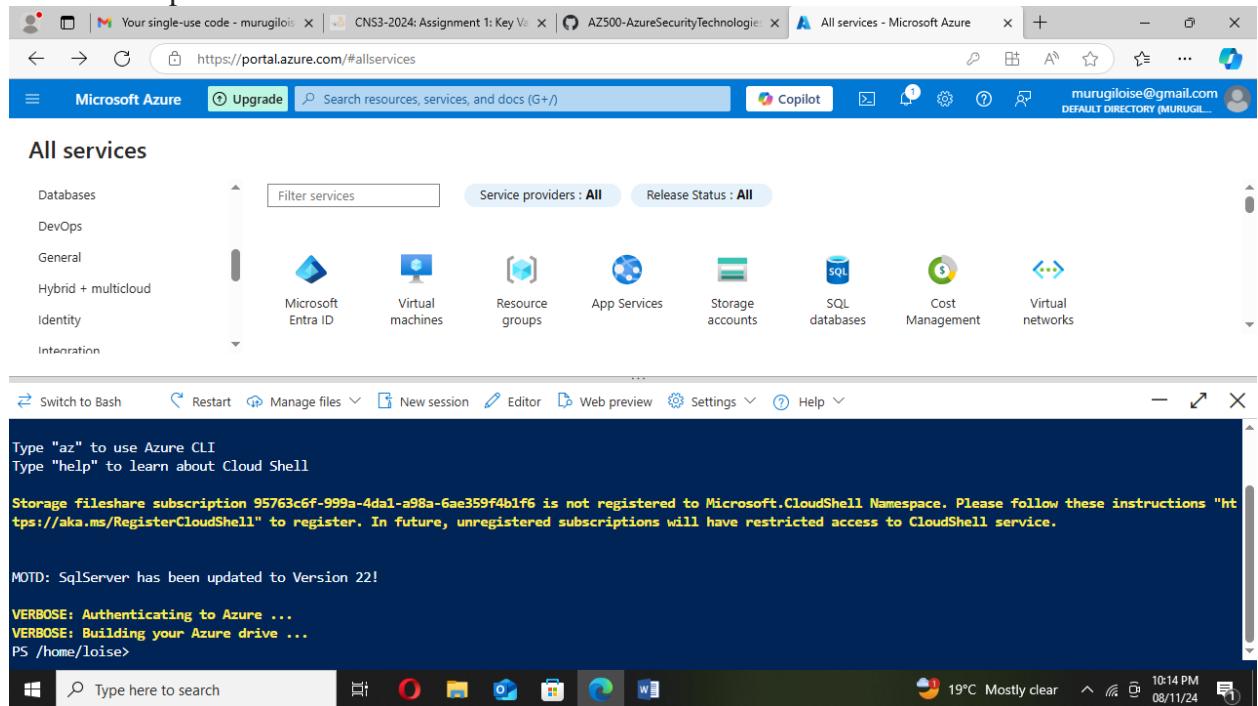
In this task, you will create an Azure Key Vault resource. You will also configure the Azure Key Vault permissions.

1. Open the Cloud Shell by clicking the first icon (next to the search bar) at the top right of the Azure portal. If prompted, select **PowerShell** and **Create storage**.



Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.



3. In the PowerShell session within the Cloud Shell pane, run the following to create an Azure Key Vault in the resource group **AZ500LAB10**. (If you chose another name for this lab's Resource Group out of Task 1, use that name for this task as well). The Key Vault name must be unique. Remember the name you have chosen. You will need it throughout this lab.

```
$kvName = 'az500kv' + $(Get-Random)
```

```
$location = (Get-AzResourceGroup -ResourceGroupName 'AZ500LAB10').Location
```

```
New-AzKeyVault -VaultName $kvName -ResourceGroupName 'AZ500LAB10' -Location $location –  
DisableRbacAuthorization
```

From the screenshot below, our key vault is Vault Name : az500kv1700071371

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Azure Cloud Shell interface. At the top, there are several tabs: 'Your single-use code - m...', 'CNS3-2024: Assignment 1', '(173) AZ500_Lab 10 - Key...', 'AZ500-AzureSecurityTech', and 'All services - Microsoft Az...'. The main area is titled 'All services' and shows categories like Databases, DevOps, General, Hybrid + multicloud, Identity, and Infrastructure. Below these are icons for Microsoft Entra ID, Virtual machines, Resource groups, App Services, Storage accounts, SQL databases, Cost Management, and Virtual networks. A search bar at the top says 'Search resources, services, and docs (G+)'. On the right, there's a user profile for 'murugiloise@gmail.com'.

Vault Name: az500kv1700071371
Resource Group Name: AZ500LAB10
Location: westus
Resource ID: /subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB10/providers/Microsoft.KeyVault/vaults/az500kv1700071371
Vault URI: https://az500kv1700071371.vault.azure.net/
Tenant ID: 87db5642-2fd0-40a2-b4d3-a0c56a5b95e5
SKU: Standard
Enabled For Deployment?: False
Enabled For Template Deployment?: False
Enabled For Disk Encryption?: False
Enabled For RBAC Authorization?: False
Soft Delete Enabled?: True

4. Close the Cloud Shell pane. Vault URI : <https://az500kv1700071371.vault.azure.net/> name az500kv1700071371
5. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type **Resource groups** and press the Enter key.

The screenshot shows the Azure portal with the URL 'https://portal.azure.com/#browse/resourcegroups'. The top navigation bar includes tabs for 'All services', 'Upgrade', and 'Copilot'. The main content area is titled 'Resource groups' and shows a list of resource groups. The columns are 'Name', 'Subscription', and 'Location'. There are four entries:

Name	Subscription	Location
AZ500LAB08	Azure subscription 1	East US
AZ500LAB10	Azure subscription 1	West US
cloud-shell-storage-westeurope	Azure subscription 1	West Europe
NetworkWatcherRG	Azure subscription 1	Brazil South

At the bottom, it says 'Showing 1 - 4 of 4. Display count: 10' and has a 'Give feedback' link. The taskbar at the bottom shows the Windows Start button, a search bar, and various pinned icons.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

6. On the **Resource groups** blade, in the list of resource group, click the **AZ500LAB10** (or other name you chose earlier for the resource group) entry.

The screenshot shows the Microsoft Azure Resource groups blade. The left sidebar lists resource groups: AZ500LAB08, AZ500LAB10 (selected), cloud-shell-storage-westeurope, and NetworkWatcherRG. The main pane displays the details for the AZ500LAB10 resource group, which is a Resource group. It contains a table listing nine resources: az500-10-nic1 (Network Interface, West US), az500-10-nsg1 (Network security group, West US), az500-10-pip1 (Public IP address, West US), az500-10-vm1 (Virtual machine, West US), az500-10-vnet1 (Virtual network, West US), and az500kv1700071371 (Key vault, West US). The table has columns for Name, Type, and Location.

7. On the Resource Group blade, click the entry representing the newly created Key Vault.

The screenshot shows the Microsoft Azure Key vault blade for the key vault az500kv1700071371. The left sidebar lists vault features: Overview (selected), Activity log, Access control (IAM), Tags, Diagnose and solve problems, Access policies, Events, Objects, Settings, Monitoring, Automation, and Help. The main pane displays the vault's properties: Resource group (AZ500LAB10), Location (West US), Subscription (Azure subscription 1), Subscription ID (95763c6f-999a-4da1-a98a-6ae359f4b1f6), and a JSON View tab. The right side shows the vault's URL (https://az500kv1700071371.vault.azure.net/), Sku (Standard), Directory ID (87db5642-2f0d-40a2-b4d3-a0c56a5b95e5), Directory Name (Default Directory), Soft-delete (Enabled), and Purge protection (Disabled).

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

8. On the Key Vault blade, in the **Overview** section, click **Access Policies** and then click **+ Create**.

The screenshot shows the 'Access policies' blade for the 'az500kv1700071371' key vault. The left sidebar has 'Access policies' selected. The main area displays a message: 'Access policies enable you to have fine grained control over access to vault items. Learn more'. Below this, it says 'Showing 0 to 0 of 0 records.' and 'No access policies found'. The top navigation bar includes tabs for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Access policies.

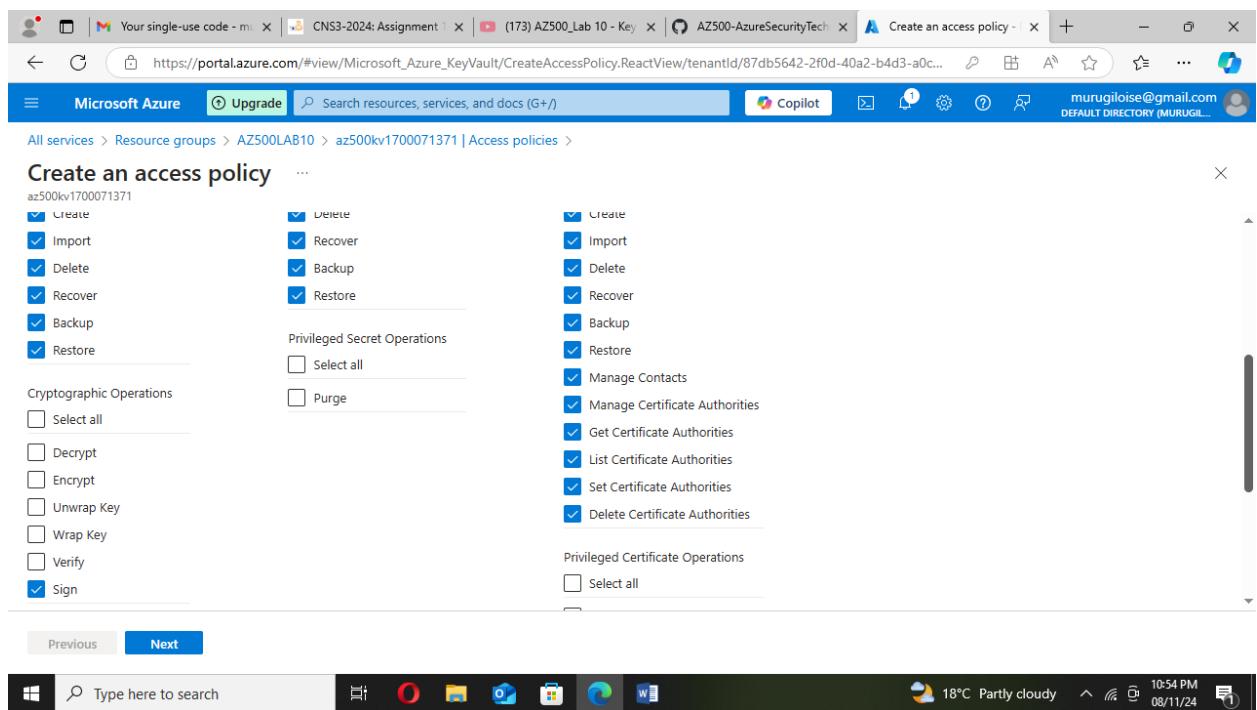
The screenshot shows the 'Create an access policy' blade at step 1: Permissions. It has tabs for Permissions (selected), Principal, Application (optional), and Review + create. Under 'Configure from a template', there is a dropdown menu 'Select a template'. The main area is divided into three sections: Key permissions, Secret permissions, and Certificate permissions, each with a list of checkboxes for various operations like Get, List, Update, Create, Import, etc.

9. On the **Create an access policy** blade, specify the following settings (leave all others with their default values):

Some of the key permissions for the vault are Get, Update, Create, Import, Delete, Backup, Recover, List, Restore.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Setting	Value
Configure from template (optional)	Key, Secret, & Certificate Management
Key permissions	click Select all resulting in total of 9 selected permissions
Key permissions/Cryptographic Operations	click Sign resulting in total of 1 selected permissions
Secret permissions	click Select all resulting in total of 7 selected permissions
Certification permissions	click Select all resulting in total of 15 selected permissions
Select principal	click None selected , on the Principal blade, select your user account, and click Next
Application (optional)	click Next
Review + create	click Create



The screenshot below shows my user account as the principal assigned the permissions to.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Microsoft Azure portal interface. The user is navigating through the Azure Key Vault service to create an access policy. The current step is 'Principal'. A search bar contains the email address 'murugiloise@gmail.com'. Below it, a list shows a single result: 'Loise Murage' with the email 'murugiloise@gmail.com'. The table below lists the principal and its permissions:

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions
Loise Murage	murugiloise@gmail.com#EXT...@outlook.com	Get, List, Update, Create, Import...	Get, List, Set, Delete, Recover...	Get, List, Update, Create, Import...

At the bottom of the page, there are 'Previous' and 'Next' buttons.

The screenshot shows the 'Access policies' page for the Key Vault. The left sidebar has 'Access policies' selected. The main area shows a table of access policies for the 'USER' category. One record is listed:

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions
Loise Murage	murugiloise@gmail.com#EXT...@outlook.com	Get, List, Update, Create, Import...	Get, List, Set, Delete, Recover...	Get, List, Update, Create, Import...

At the bottom of the page, there are 'Type here to search' and 'Refresh' buttons.

Task 2: Add a key to Key Vault

1. In the Azure portal, open a PowerShell session in the Cloud Shell pane.
2. In this task, you will add a key to the Key Vault and view information about the key. Ensure **PowerShell** is selected in the upper-left drop-down menu of the Cloud Shell pane.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

3. In the PowerShell session within the Cloud Shell pane, run the following to add a software-protected key to the Key Vault:

```
$kv = Get-AzKeyVault -ResourceGroupName 'AZ500LAB10'
```

```
$key = Add-AZKeyVaultKey -VaultName $kv.VaultName -Name 'MyLabKey' -Destination 'Software'
```

Note: The name of the key is **MyLabKey**

The screenshot shows the Azure portal interface. At the top, there are several tabs and a search bar. Below the header, the URL is https://portal.azure.com/#@murugiloisegmail.onmicrosoft.com/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/... . On the left, there's a sidebar with 'Microsoft Azure' branding and a 'Keys' section selected. The main content area shows a table of keys with one entry: 'MyLabKey' under 'Name', 'Enabled' under 'Status', and an empty field under 'Expiration date'. Below the table, there's a 'Keys' tab and a 'Cloud Shell' pane. The Cloud Shell pane contains a PowerShell session with the following commands:

```
Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

MOTD: SqlServer has been updated to Version 22!

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/loise> $kv = Get-AzKeyVault -ResourceGroupName 'AZ500LAB10'
PS /home/loise>
PS /home/loise> $key = Add-AZKeyVaultKey -VaultName $kv.VaultName -Name 'MyLabKey' -Destination 'Software'
PS /home/loise> []
```

4. In the PowerShell session within the Cloud Shell pane, run the following to verify the key was created: Get-AZKeyVaultKey -VaultName \$kv.VaultName

From the screenshot below MyLabKey was created.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Azure Cloud Shell interface. At the top, there are several tabs open, including 'Your single-use code', 'CNS3-2024: A...', '(173) AZ500_Lab 10', '(173) AZ500_Lab 10', 'AZ500-AzureSecurity', and 'az500kv1700071371'. The main pane displays a table of keys in the 'az500kv1700071371' key vault. One key, 'MyLabKey', is listed with the status 'Enabled'. Below the table, a PowerShell session is running, showing the properties of the 'MyLabKey' key. The session output includes:

```
Vault/HSM Name : az500kv1700071371
Name : MyLabKey
Version :
Id : https://az500kv1700071371.vault.azure.net:443/keys/MyLabKey
Enabled : True
Expires :
Not Before :
Created : 11/8/2024 8:12:53 PM
Updated : 11/8/2024 8:12:53 PM
Recovery Level : Recoverable+Purgeable
Tags :
```

PS /home/loise>

5. In the PowerShell session within the Cloud Shell pane, run the following to display the key identifier:

```
$key.key.kid
```

The screenshot shows the Azure Cloud Shell interface. The PowerShell session now displays the result of the '\$key.key.kid' command, which outputs the key identifier:

```
https://az500kv1700071371.vault.azure.net/keys/MyLabKey/d5a22f87db464972987fe44d5a4a4f82
```

6. Minimize the Cloud Shell pane.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

7. Back in the Azure portal, on the Key Vault blade, in the Objects section, click Keys.

All services > Resource groups > AZ500LAB10 > az500kv1700071371

az500kv1700071371 | Keys

Name	Status	Expiration date
MyLabKey	✓ Enabled	

8. In the list of keys, click the **MyLabKey** entry and then, on the **MyLabKey** blade, click the entry representing the current version of the key.

Note: Examine the information about the key you created.

All services > Resource groups > AZ500LAB10 > az500kv1700071371 | Keys > MyLabKey

d5a22f87db464972987fe44d5a4a4f82

Properties	
Key type	RSA
RSA key size	2048
Created	11/8/2024, 11:12:53 PM
Updated	11/8/2024, 11:12:53 PM
Key identifier	https://az500kv1700071371.vault.azure.net/keys...

Save Discard changes Download public key

Properties

Key type: RSA
RSA key size: 2048
Created: 11/8/2024, 11:12:53 PM
Updated: 11/8/2024, 11:12:53 PM
Key identifier: <https://az500kv1700071371.vault.azure.net/keys...>

Settings

Set activation date
Set expiration date

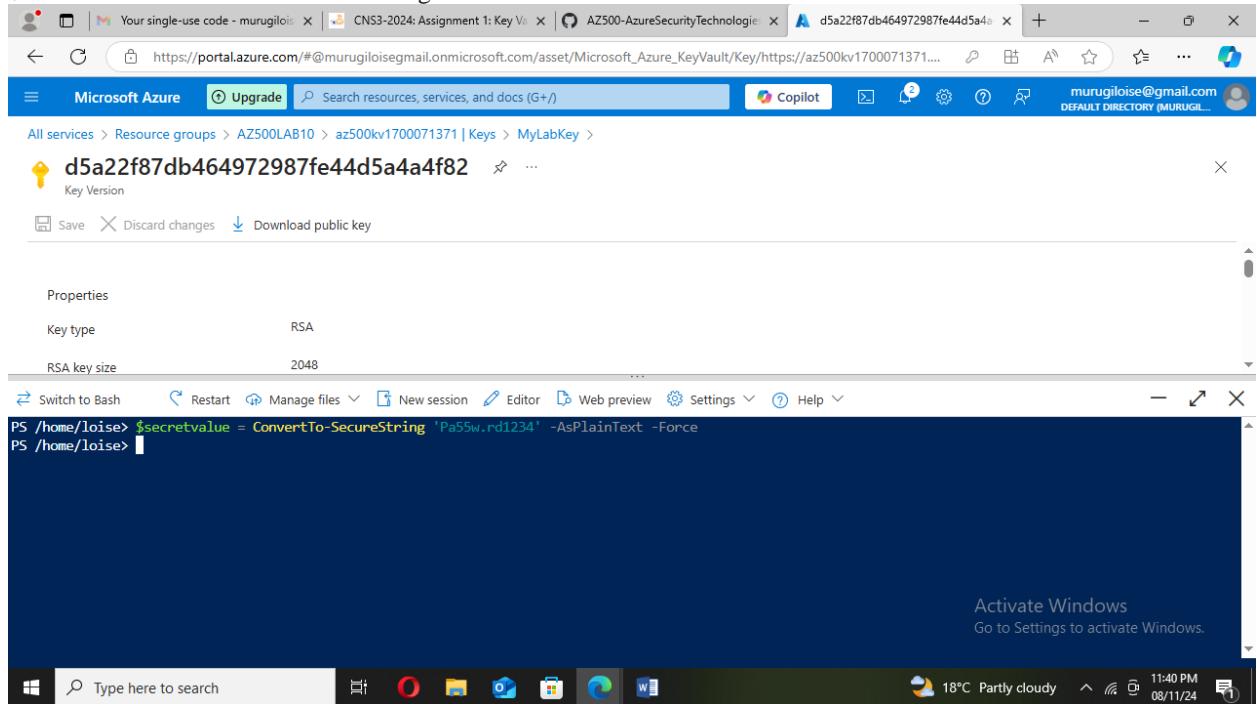
Enabled: Yes

Tags: 0 tags

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Task 3: Add a Secret to Key Vault

1. Switch back to the Cloud Shell pane. In the PowerShell session within the Cloud Shell pane, run the following to create a variable with a secure string value:
2. \$secretvalue = ConvertTo-SecureString 'Pa55w.rd1234' -AsPlainText -Force



3. In the PowerShell session within the Cloud Shell pane, run the following to add the secret to the vault:

To generate the value of the Vault name

```
$secret = Set-AZKeyVaultSecret -VaultName $kv.VaultName -Name 'SQLPassword' -SecretValue  
$secretvalue
```

Note: The name of the secret is SQLPassword.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Azure Key Vault Properties page for a key named 'd5a22f87db464972987fe44d5a4a4f82'. The key type is RSA and the key size is 2048. Below the properties, there is a Cloud Shell session window. The session shows the following PowerShell commands:

```
PS /home/loise> $secretvalue = ConvertTo-SecureString 'Pa55w_rd1234' -AsPlainText -Force
PS /home/loise> $secret = Set-AZKeyVaultSecret -VaultName $kv.VaultName -Name 'SQLPassword' -SecretValue $secretvalue
PS /home/loise>
```

4. In the PowerShell session within the Cloud Shell pane, run the following to verify the secret was created.

1. Get-AZKeyVaultSecret -VaultName \$kv.VaultName

The screenshot shows the Azure Key Vault Properties page for the same key. Below the properties, there is a Cloud Shell session window. The session shows the following PowerShell command:

```
PS /home/loise> Get-AZKeyVaultSecret -VaultName az500kv1700071371
```

The output of the command is displayed in the session window, showing the secret details:

Property	Value
Vault Name	az500kv1700071371
Name	SQLPassword
Version	
Id	https://az500kv1700071371.vault.azure.net:443/secrets/SQLPassword
Enabled	True
Expires	
Not Before	
Created	11/8/2024 8:42:10 PM
Updated	11/8/2024 8:42:10 PM
Content Type	
Tags	

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

5. Minimize the Cloud Shell pane.
6. In the Azure portal, navigate back to the Key Vault blade, in the **Objects** section, click **Secrets**.

A secret has been created SQLPassword

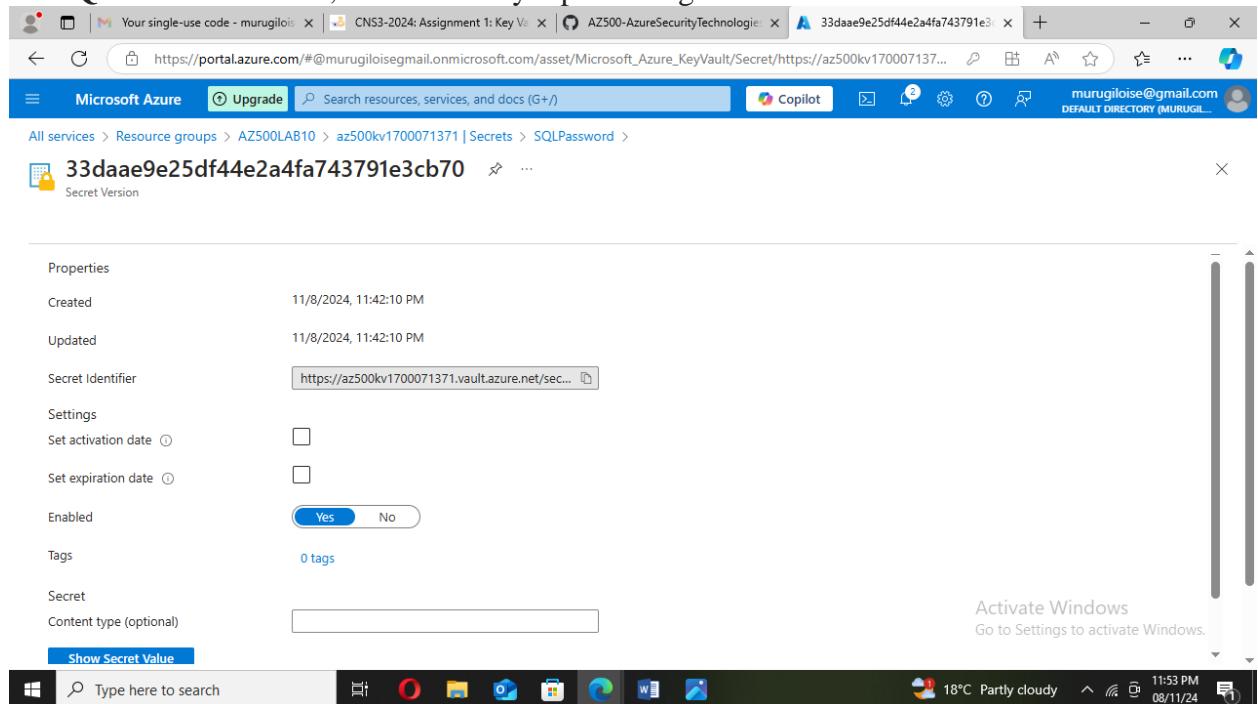
The screenshot shows the Azure portal interface with the URL <https://portal.azure.com/#@murugiloisegmail.onmicrosoft.com/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB10/providers/Microsoft.KeyVault/vaults/az500kv1700071371/secrets>. The page title is "az500kv1700071371 | Secrets". The left sidebar shows "Key vault" selected under "Objects". The main content area displays a table of secrets:

Name	Type	Status	Expiration date
SQLPassword		✓ Enabled	

The status bar at the bottom shows the URL <https://portal.azure.com/#@murugiloisegmail.onmicrosoft.com/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB10/providers/Microsoft.KeyVault/vaults/az500kv1700071371/secrets>, the date "08/11/24", and the time "11:50 PM".

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

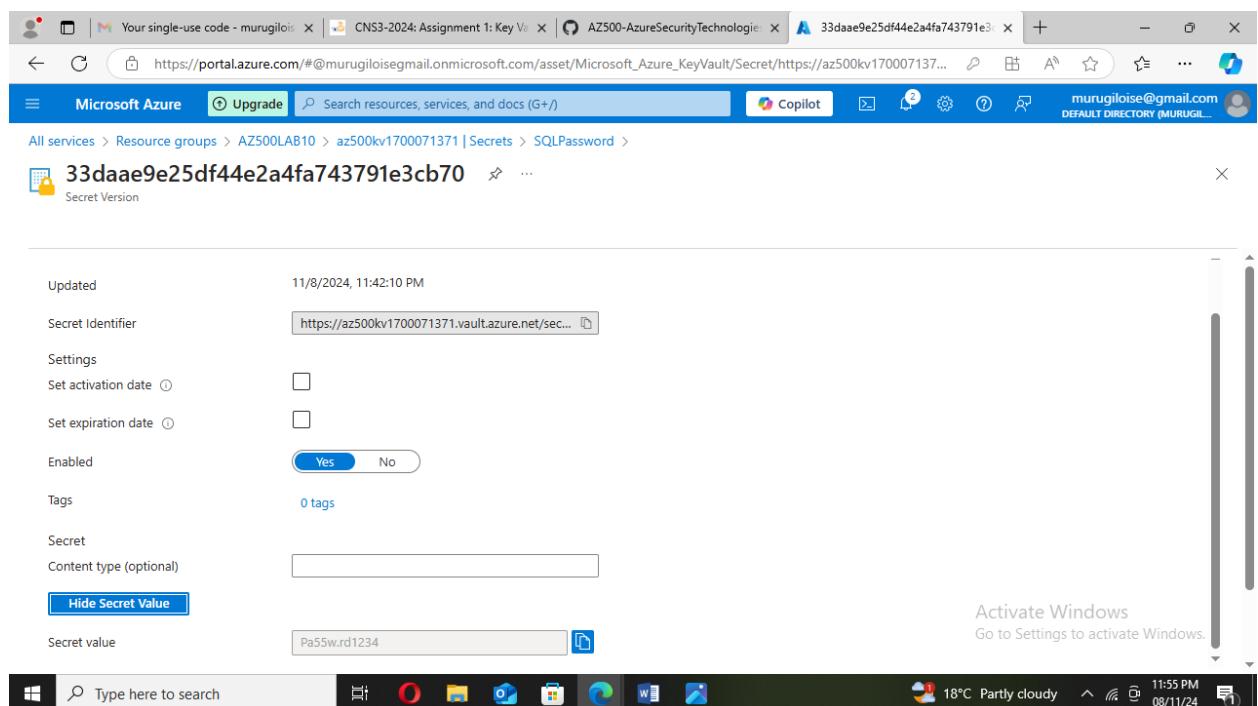
7. In the list of secrets, click the **SQLPassword** entry and then, on the **SQLPassword** blade, click the entry representing the current version of the secret.



The screenshot shows the Azure portal interface. The URL in the address bar is https://portal.azure.com/#@murugiliosegmail.onmicrosoft.com/asset/Microsoft_Azure_KeyVault/Secret/https://az500kv1700071371e3cb70. The page title is "33daae9e25df44e2a4fa743791e3cb70". The "Secret Version" section is expanded, showing the following properties:

Properties	
Created	11/8/2024, 11:42:10 PM
Updated	11/8/2024, 11:42:10 PM
Secret Identifier	https://az500kv1700071371.vault.azure.net/sec...
Settings	<input type="checkbox"/> Set activation date <input type="checkbox"/> Set expiration date
Enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
Tags	0 tags
Secret	Content type (optional) <input type="text"/>

A "Show Secret Value" button is visible above the secret identifier. The Windows taskbar at the bottom shows the search bar and pinned icons for File Explorer, Edge, and File History. The system tray indicates it's 11:53 PM on 08/11/24, 18°C, and Partly cloudy.



The screenshot shows the same Azure portal interface as the previous one, but the "Show Secret Value" button has been clicked, revealing the secret value in the "Secret value" input field: "Pa55w.rd1234". The rest of the secret details remain the same as in the first screenshot.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Exercise 3: Configure an Azure SQL database and a data-driven application

Task 1: Enable a client application to access the Azure SQL Database service.

In this task, you will enable a client application to access the Azure SQL Database service. This will be done by setting up the required authentication and acquiring the Application ID and Secret that you will need to authenticate your application.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **App Registrations** and press the **Enter** key.

The screenshot shows the Azure portal interface with the URL https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade. The title bar includes tabs for 'Your single-use code - murugiloise' and 'CNS3-2024: Assignment 1: Key Va...'. The main content area is titled 'App registrations' with a sub-header 'Owned applications'. A message banner at the top states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)'. Below the banner, there are tabs for 'All applications', 'Owned applications' (which is selected), 'Deleted applications', and 'Applications from personal account'. A search bar contains the placeholder 'Start typing a display name or application (client) ID to filter these r...'. A blue button labeled '+ Add filters' is visible. A message below the search bar says 'This account isn't listed as an owner of any applications in this directory.' with two buttons: 'View all applications in the directory' and 'View all applications from personal account'. At the bottom right, there is a 'Activate Windows' message: 'Activate Windows Go to Settings to activate Windows.' The taskbar at the bottom shows the Windows Start button, a search bar, and various pinned icons like File Explorer, Edge, and Mail. The system tray shows the date and time as '12:00 AM 09/11/24'.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

2. On the **App Registrations** blade, click **+ New registration**.

The screenshot shows the 'Register an application' blade in the Azure portal. At the top, there is a search bar and a 'Copilot' button. The main section is titled 'Register an application'. It has a required field 'Name' with a placeholder 'The user-facing display name for this application (this can be changed later)'. Below it is a section for 'Supported account types' with four options: 'Accounts in this organizational directory only (Default Directory only - Single tenant)' (selected), 'Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)', 'Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)', and 'Personal Microsoft accounts only'. There is also a 'Help me choose...' link. Below these sections is a note 'By proceeding, you agree to the Microsoft Platform Policies' with a link. At the bottom right, there is an 'Activate Windows' link and a system tray with icons for battery, signal, and date/time.

3. On the **Register an application** blade, specify the following settings (leave all others with their default values):

Setting	Value
Name	sqlApp
Redirect URI (optional)	Web and https://sqlapp

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/CreateApplicationBlade. The page title is "Register an application".
The "Accounts in this organizational directory only (Default Directory only - Single tenant)" option is selected.
The "Redirect URI (optional)" field contains "Web" and "https://sqlapp".
A note states: "We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios."
A "Help me choose..." link is present.
A "By proceeding, you agree to the Microsoft Platform Policies" link is at the bottom left.
A "Register" button is at the bottom center.
A "Activate Windows" link is on the right.
The taskbar at the bottom shows various pinned icons.

4. On the **Register an application** blade, click **Register**.

Note: Once the registration is completed, the browser will automatically redirect you to **sqlApp** blade.

The screenshot shows the Microsoft Azure portal with the URL https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Overview/appId/940a72c8-d02b-4bfa-88be-0661bc4cec1f. The page title is "sqlApp - Microsoft Azure".
The "Overview" tab is selected in the left sidebar.
The "Essentials" section displays:

- Display name: sqlApp
- Application (client) ID: 940a72c8-d02b-4bfa-88be-0661bc4cec1f
- Object ID: ce48b450-1888-4e18-ae6e-a918afee96f1
- Directory (tenant) ID: 87db5642-2fd4-40a2-b4d3-a0c56a5b95e
- Supported account types: My organization only
- Client credentials: Add a certificate or secret
- Redirect URIs: 1 web, 0 spa, 0 public client
- Application ID URI: Add an Application ID URI
- Managed application in local directory: sqlApp

Information banners at the bottom:

- Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)
- Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

The taskbar at the bottom shows various pinned icons.

5. On the **sqlApp** blade, identify the value of **Application (client) ID**. The application app ID is 940a72c8-d02b-4bfa-88be-0661bc4cec1f

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Note: Record this value. You will need it in the next task.

The screenshot shows the Azure portal interface. The top navigation bar includes tabs for 'Your single-use code - murugiloise', 'CNS3-2024: Assignment 1: Key Va...', 'AZ500-AzureSecurityTechnolog...', and 'sqlApp - Microsoft Azure'. The main content area is titled 'sqlApp' under 'App registrations'. The left sidebar has sections like 'Overview', 'Quickstart', 'Integration assistant', 'Diagnose and solve problems', 'Manage', and 'Support + Troubleshooting'. The 'Manage' section is currently selected. The main pane displays details for the application 'sqlApp', including its display name, application ID, object ID, directory ID, and supported account types. A message at the bottom states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph.' A status bar at the bottom shows the date '09/11/24' and time '12:11 AM'.

- On the sqlApp blade, in the Manage section, click Certificates & secrets.

The screenshot shows the 'Certificates & secrets' blade for the 'sqlApp' application. The left sidebar shows 'Manage' selected, with 'Certificates & secrets' highlighted. The main pane displays a message about certificates enabling confidential applications to identify themselves. It shows tabs for 'Certificates (0)', 'Client secrets (0)', and 'Federated credentials (0)'. Under 'Client secrets (0)', there is a table with columns 'Description', 'Expires', 'Value', and 'Secret ID'. A note says 'No client secrets have been created for this application.' A status bar at the bottom shows the date '09/11/24' and time '12:15 AM'.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

7. On the **sqlApp | Certificates & secrets** blade / **Client Secrets** section, click + New client secret

The screenshot shows the Azure portal interface. The left sidebar has 'sqlApp | Certificates & secrets' selected under 'Certificates & secrets'. The main area is titled 'Add a client secret'. It has two input fields: 'Description' (with placeholder 'Enter a description for this client secret') and 'Expires' (set to 'Recommended: 180 days (6 months)'). A note below says 'No client secrets have been created for this application.' At the bottom are 'Add' and 'Cancel' buttons.

8. In the **Add a client secret** pane, specify the following settings:

Setting	Value
Description	Key1
Expires	12months

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Microsoft Azure portal interface. The left sidebar is for the 'sqlApp | Certificates & secrets' blade, with 'Certificates & secrets' selected. The main content area is titled 'Add a client secret'. It has fields for 'Description' (set to 'Key1') and 'Expires' (set to '365 days (12 months)'). A note says 'Certificates enable confidential applications to identify themselves to the scheme. For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.' Below this, there are tabs for 'Certificates (0)', 'Client secrets (0)' (which is selected), and 'Federated credentials (0)'. A button to '+ New client secret' is shown. At the bottom right are 'Add' and 'Cancel' buttons.

9. Click Add to update the application credentials.

The screenshot shows the Microsoft Azure portal interface. The left sidebar is for the 'sqlApp | Certificates & secrets' blade, with 'Certificates & secrets' selected. The main content area shows a table for client secrets. There is one entry: 'Key1' with an expiration date of '11/9/2025', a value of '64S8Q~OtoN0RHsUXp4enE2CqZW3H7dNa0~C5Ab90', and a secret ID of 'd45109d8-e785-4f01-89b8-4051384b9168'. A note says 'Application registration certificates, secrets and federated credentials can be found in the tabs below.' Below the table, there are tabs for 'Certificates (0)', 'Client secrets (1)' (selected), and 'Federated credentials (0)'. A button to '+ New client secret' is shown. At the bottom right are 'Activate Windows' and 'Go to Settings to activate Windows' buttons.

10. On the **sqlApp | Certificates & secrets** blade, identify the value of **Key1**.

Value of Key1 is 64S8Q~OtoN0RHsUXp4enE2CqZW3H7dNa0~C5Ab90
Secret ID is d45109d8-e785-4f01-89b8-4051384b9168

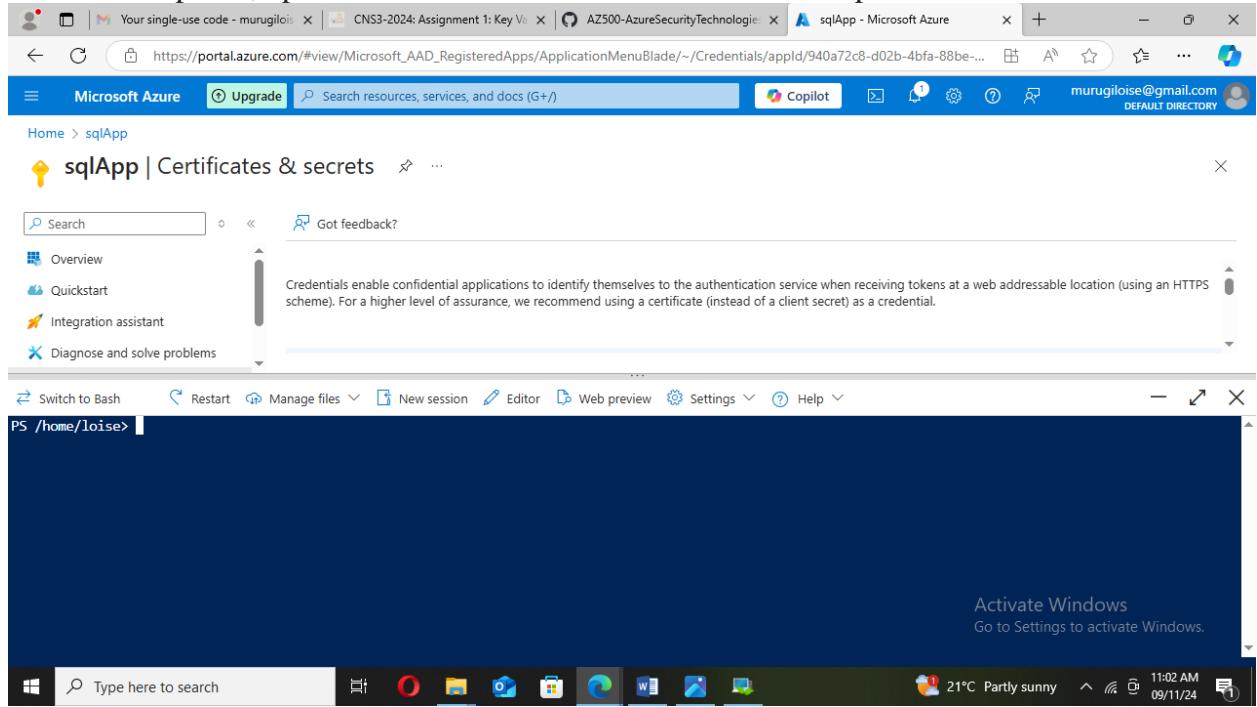
Our Application ID: 940a72c8-d02b-4bfa-88be-0661bc4cec1f
Object ID: ce48b450-1888-4e18-ae6e-a918afee96f1

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Task 2: Create a policy allowing the application access to the Key Vault.

In this task, you will grant the newly registered app permissions to access secrets stored in the Key Vault.

1. In the Azure portal, open a PowerShell session in the Cloud Shell pane.

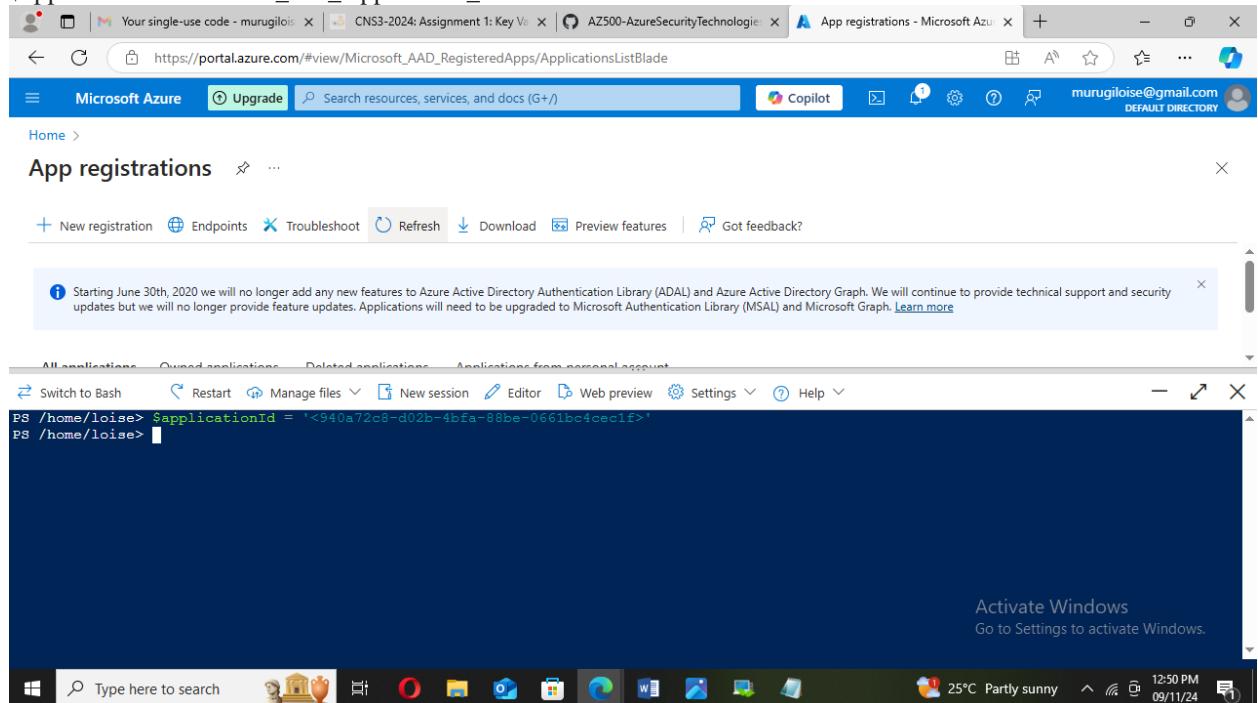


2. Ensure **PowerShell** is selected in the upper-left drop-down menu of the Cloud Shell pane.

3. In the PowerShell session within the Cloud Shell pane, run the following to create a variable storing the **Application (client) ID** you recorded in the previous task (replace the <Azure_AD_Application_ID> placeholder with the value of the **Application (client) ID**):

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

```
$applicationId = '<Azure_AD_Application_ID>' ID 940a72c8-d02b-4bfa-88be-0661bc4cec1f
```

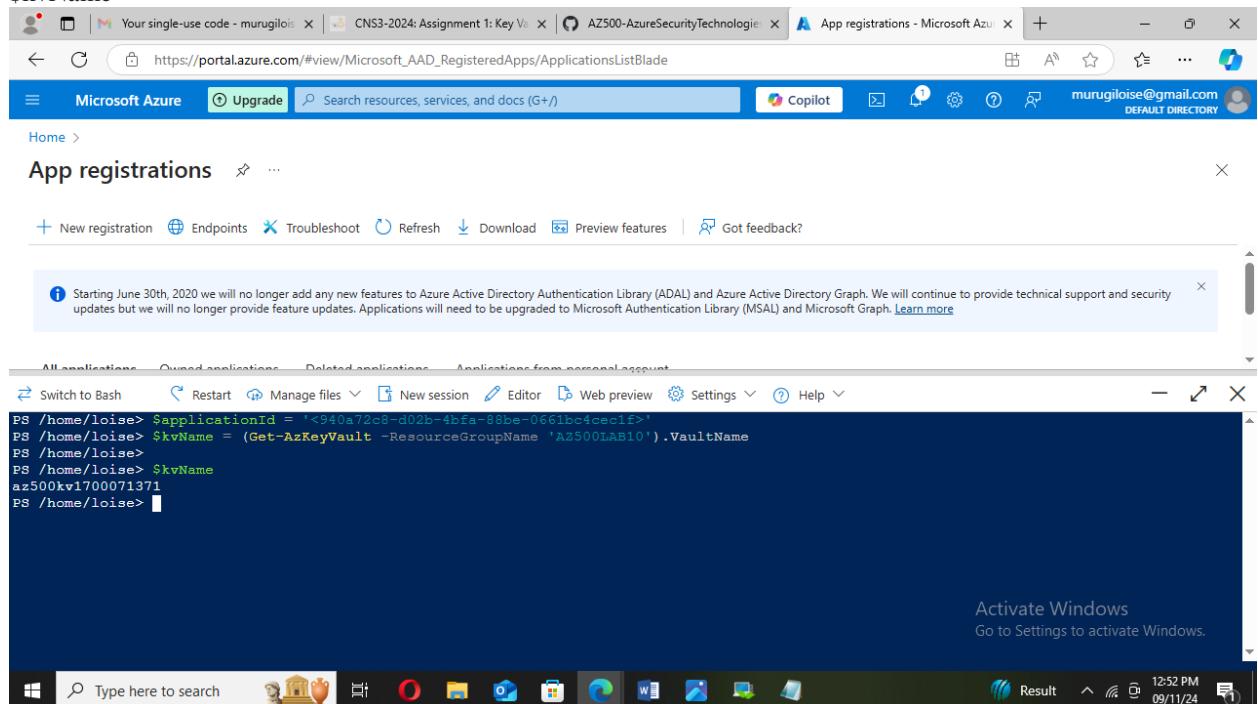


The screenshot shows a Microsoft Azure Cloud Shell interface. At the top, there are several tabs: 'Your single-use code - murugiloise', 'CNS3-2024: Assignment 1: Key Va...', 'AZ500-AzureSecurityTechnologie...', and 'App registrations - Microsoft Az...'. The main area is titled 'App registrations' with a sub-header 'All applications'. A message at the top states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)'. Below this, a terminal window shows a PowerShell session with the command: PS /home/loise> \$applicationId = '<940a72c8-d02b-4bfa-88be-0661bc4cec1f>'. The bottom of the screen shows the Windows taskbar with various icons and the system tray indicating it's 12:50 PM on 09/11/24.

4. In the PowerShell session within the Cloud Shell pane, run the following to create a variable storing the Key Vault name.

```
$kvName = (Get-AzKeyVault -ResourceGroupName 'AZ500LAB10').VaultName
```

```
$kvName
```



The screenshot shows a Microsoft Azure Cloud Shell interface, identical to the previous one but with a different command. The terminal window shows: PS /home/loise> \$kvName = (Get-AzKeyVault -ResourceGroupName 'AZ500LAB10').VaultName. The bottom of the screen shows the Windows taskbar with various icons and the system tray indicating it's 12:52 PM on 09/11/24.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Microsoft Azure Cloud Shell interface. The top navigation bar includes tabs for 'Your single-use code - murugiloise', 'CNS3-2024: Assignment 1: Key Va...', 'AZ500-AzureSecurityTechnologie...', 'sqlApp - Microsoft Azure', and 'Copilot'. The main title is 'sqlApp | Certificates & secrets'. On the left, a sidebar lists 'Authentication', 'Certificates & secrets' (which is selected), 'Token configuration', and 'API permissions'. The main pane displays a PowerShell session with the following commands:

```
PS /home/loise> $applicationId = '645B0-Ot0N0RhsUxp4enE2CqZW3H7dNa0-C5Ab90'
PS /home/loise> $kvName = (Get-AzKeyVault -ResourceGroupName 'AZ500LAB10').VaultName
PS /home/loise> $kvName
az500kv1700071371
PS /home/loise>
```

The bottom status bar shows the date as 09/11/24 and the time as 11:35 AM.

5. In the PowerShell session within the Cloud Shell pane, run the following to grant permissions on the Key Vault to the application you registered in the previous task:

```
Set-AZKeyVaultAccessPolicy -VaultName $kvName -ResourceGroupName AZ500LAB10 -ServicePrincipalName $applicationId -PermissionsToKeys get,wrapKey,unwrapKey,sign,verify,list
```

The screenshot shows the Microsoft Azure Cloud Shell interface. The top navigation bar includes tabs for 'Your single-use code - murugiloise', 'CNS3-2024: Assignment 1: Key Va...', 'AZ500-AzureSecurityTechnologie...', 'App registrations - Microsoft Azure', and 'Copilot'. The main title is 'App registrations'. On the left, a sidebar lists 'All applications', 'Owned applications', 'Deleted applications', and 'Applications from personal account'. The main pane displays a PowerShell session with the following commands:

```
PS /home/loise> $applicationId = '940a72c8-d02b-4bfa-88be-0661bc4cec1f'
PS /home/loise> $kvName = (Get-AzKeyVault -ResourceGroupName 'AZ500LAB10').VaultName
PS /home/loise> $kvName
az500kv1700071371
PS /home/loise> Set-AZKeyVaultAccessPolicy -VaultName $kvName -ResourceGroupName AZ500LAB10 -ServicePrincipalName $applicationId -PermissionsToKeys get,wrapKey,unwrapKey,sign,verify,list
PS /home/loise>
```

The bottom status bar shows the date as 09/11/24 and the time as 1:00 PM.

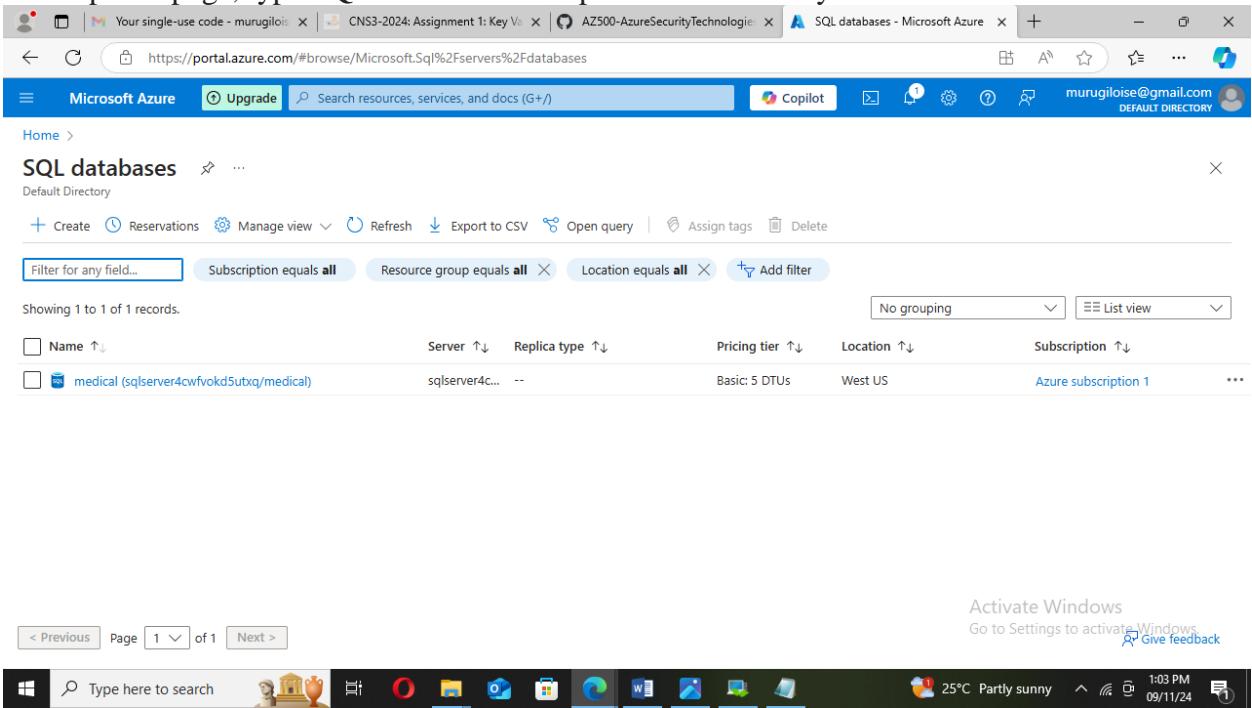
6. Close the Cloud Shell pane.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Task 3: Retrieve SQL Azure database ADO.NET Connection String

The ARM-template deployment in Exercise 1 provisioned an Azure SQL Server instance and an Azure SQL database named **medical**. You will update the empty database resource with a new table structure and select data columns for encryption

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **SQL databases** and press the **Enter** key.



The screenshot shows the Azure portal interface with the search bar set to "SQL databases". The results list displays one database entry:

Name	Server	Replica type	Pricing tier	Location	Subscription
medical (sqlserver4cwfvoqd5utxa/medical)	sqlserver4c...	--	Basic: 5 DTUs	West US	Azure subscription 1

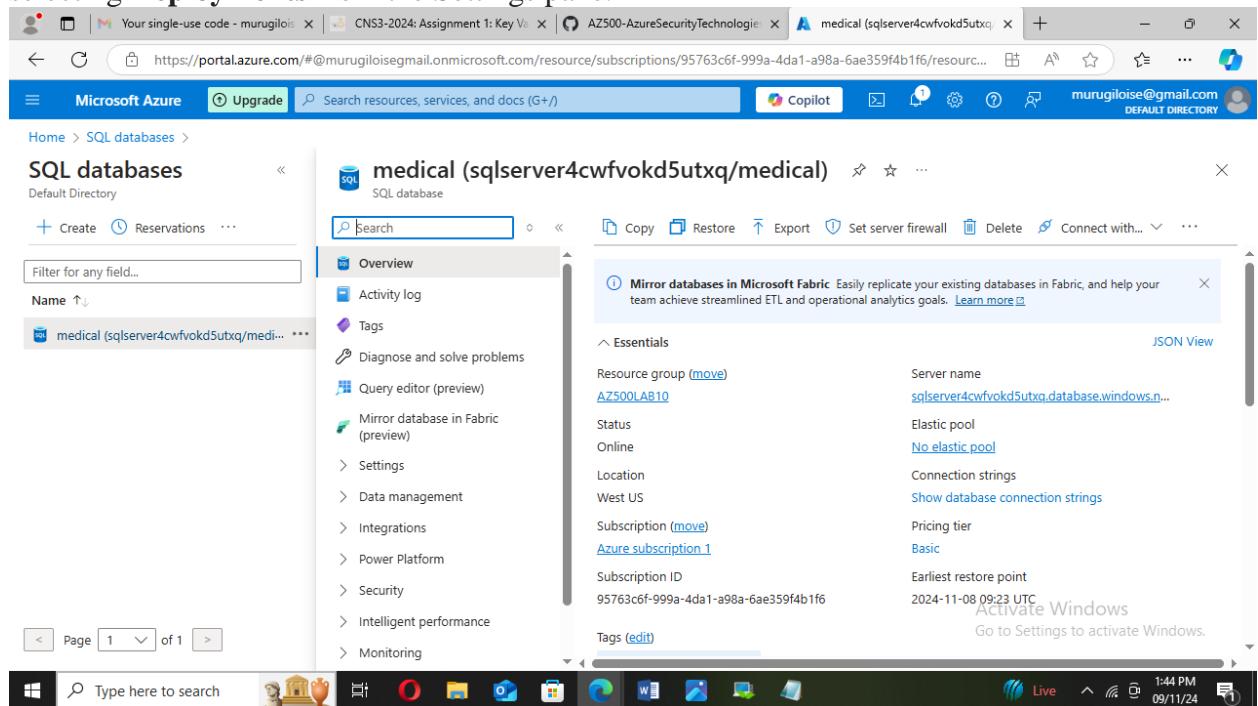
Below the table, there are navigation controls: < Previous, Page 1 of 1, Next >, and links for Activate Windows and Give feedback.

2. In the list of SQL databases, click the **medical()** entry.

Note: If the database cannot be found, this likely means the deployment you initiated in Exercise 1 has not completed yet. You can validate this by browsing to the Azure Resource Group "AZ500LAB10" (or the name you chose), and

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

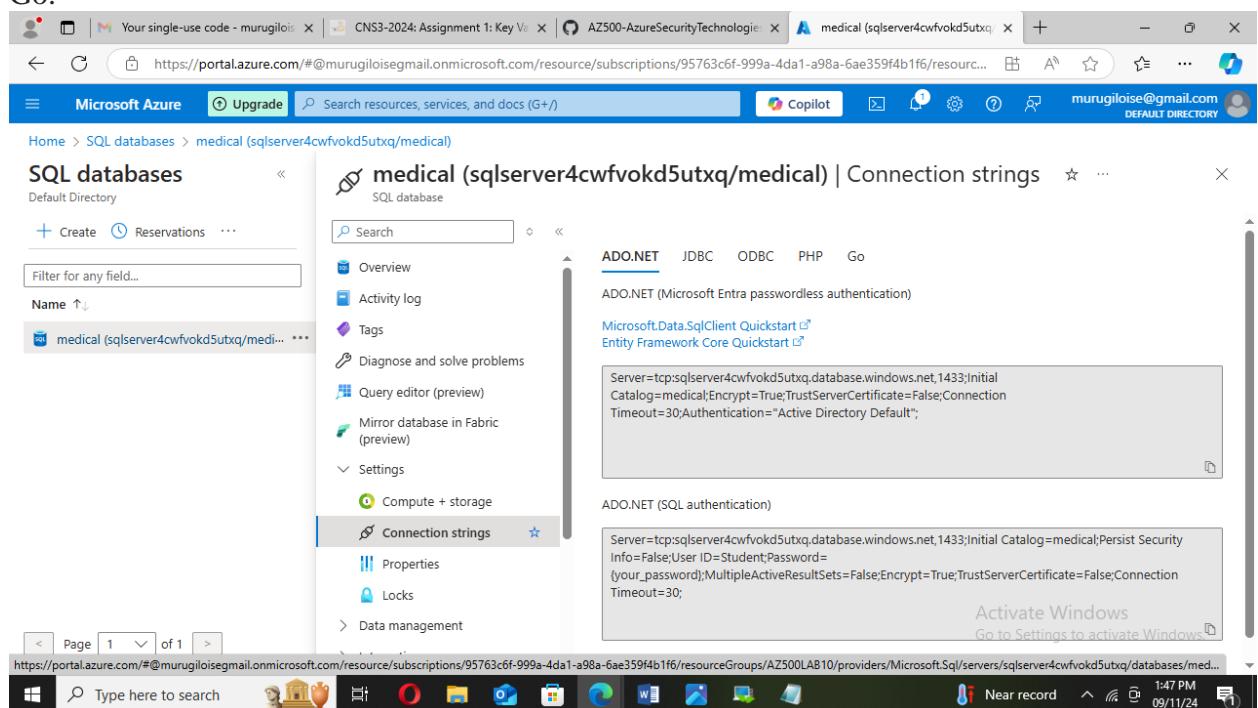
selecting Deployments from the Settings pane.



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'Your single-use code - murugiloise', 'CNS3-2024: Assignment 1: Key Va...', 'AZ500-AzureSecurityTechnologie...', and 'medical (sqlserver4cwfvokd5utxq/medical)'. The main content area is titled 'medical (sqlserver4cwfvokd5utxq/medical)' and shows the 'SQL databases' blade. On the left, there's a sidebar with links like 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Query editor (preview)', 'Mirror database in Fabric (preview)', 'Settings', 'Data management', 'Integrations', 'Power Platform', 'Security', 'Intelligent performance', and 'Monitoring'. The right side displays detailed information about the database, including its resource group ('AZ500LAB10'), status ('Online'), location ('West US'), subscription ('Azure subscription 1'), and tags. A 'Connection strings' section is also visible. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time as 09/11/24 at 1:44 PM.

3. On the SQL database blade, in the **Settings** section, click **Connection strings**.

Note: The interface includes connection strings for ADO.NET, JDBC, ODBC, PHP, and Go.



This screenshot shows the 'Connection strings' section of the 'medical' database blade. The left sidebar has a 'Connection strings' link under the 'Settings' category. The right panel lists connection strings for different technologies: ADO.NET, JDBC, ODBC, PHP, and Go. The ADO.NET section contains two entries: 'ADO.NET (Microsoft Entra passwordless authentication)' and 'ADO.NET (SQL authentication)'. The 'ADO.NET (SQL authentication)' entry shows a connection string template: 'Server=tcp:sqlserver4cwfvokd5utxq.database.windows.net,1433;Initial Catalog=medical;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;Authentication="Active Directory Default";'. Below this, there's a note to 'Activate Windows' with a link to 'Go to Settings to activate Windows'. The bottom of the screen shows the Windows taskbar and system tray.

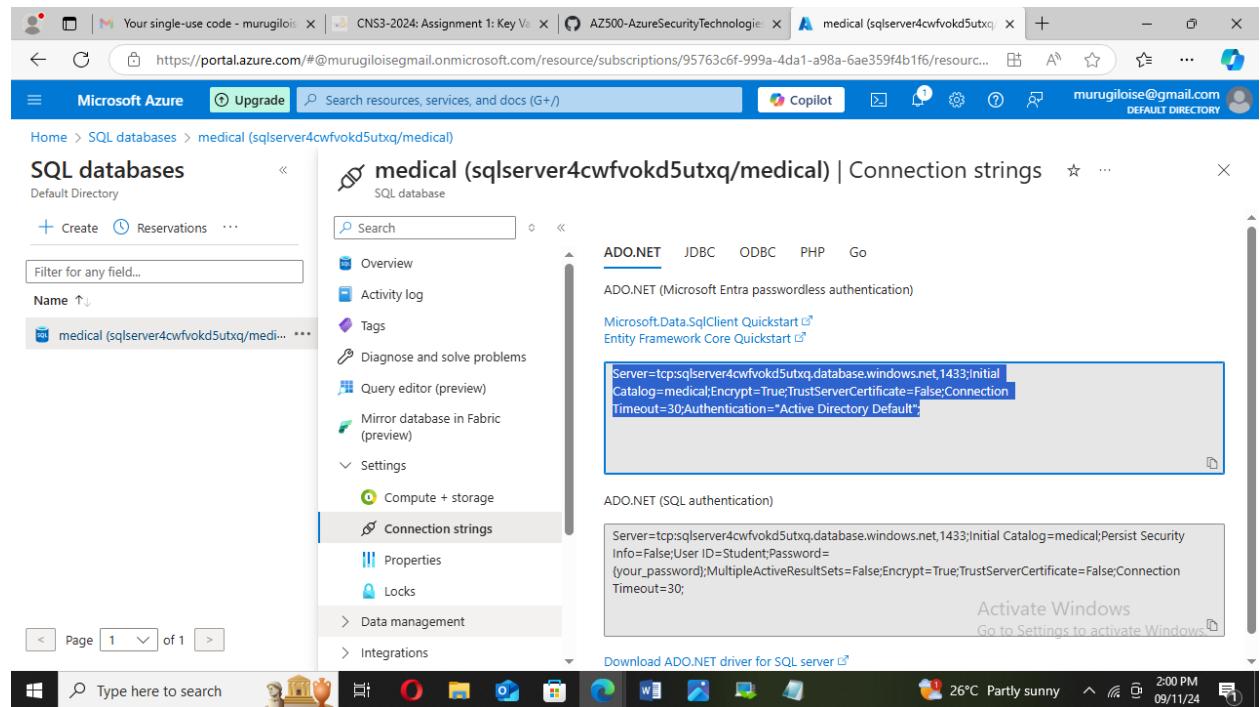
4. Record the **ADO.NET (SQL authentication)** connection string. You will need it later.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Note: When you use the connection string, make sure to replace the {your_password} placeholder with the password that you configured with the deployment in Exercise 1.

ADO.NET (SQL Authentication)

```
Server=tcp:sqlserver4cwfvokd5utxq.database.windows.net,1433;Initial Catalog=medical;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;Authentication="Active Directory Default";
```



The screenshot shows the Microsoft Azure portal interface. The user is navigating through the Azure portal to manage a SQL database named 'medical' located on the server 'sqlserver4cwfvokd5utxq'. The current view is the 'Connection strings' section under the 'ADO.NET' tab. The connection string is defined as follows:

```
Server=tcp:sqlserver4cwfvokd5utxq.database.windows.net,1433;Initial Catalog=medical;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;Authentication="Active Directory Default";
```

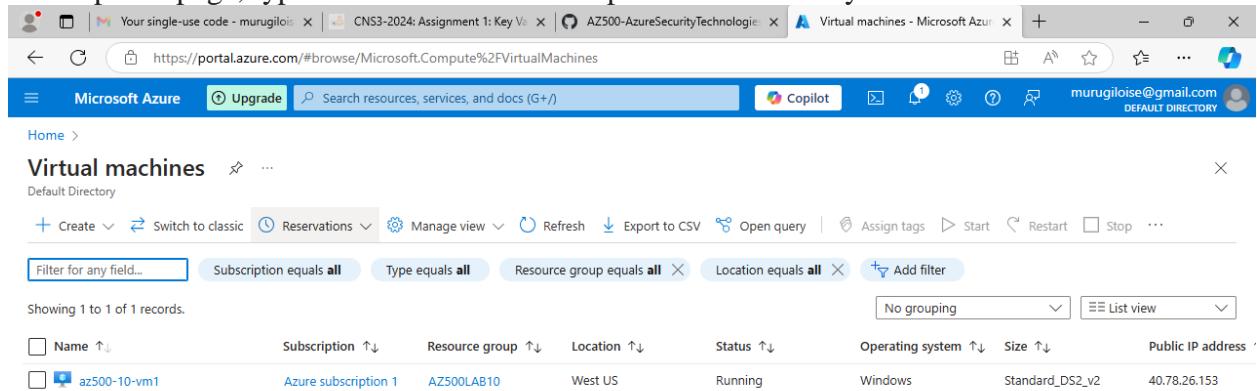
The portal also displays other tabs for JDBC, ODBC, PHP, and Go, along with links for Microsoft.Data.SqlClient Quickstart and Entity Framework Core Quickstart. The bottom of the screen shows the Windows taskbar with various pinned icons and system status information.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Task 4: Log on to the Azure VM running Visual Studio 2019 and SQL Management Studio 19

In this task, you log on to the Azure VM, which deployment you initiated in Exercise 1. This Azure VM hosts Visual Studio 2019 and SQL Server Management Studio 19.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **virtual machines** and press the **Enter** key.



The screenshot shows the Azure portal interface with the search bar set to "Virtual machines". The results table displays one record:

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address
az500-10-vm1	Azure subscription 1	AZ500LAB10	West US	Running	Windows	Standard_DS2_v2	40.78.26.153

2. In the list of Virtual Machines shown, select the **az500-10-vm1** entry. On the **az500-10-vm1** blade, on the **Essentials** pane, take note of the **Public IP address**. You will use this later.



The screenshot shows the Windows Start menu with the search bar containing "az500-10-vm1". The results pane shows the Public IP address: 40.78.26.153.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Public IP address 40.78.26.153

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar titled 'Virtual machines' with a list of VMs, including 'az500-10-vm1'. The main area is focused on 'az500-10-vm1'. In the top right of the main area, there's a tooltip for the 'Public IP address' field, which displays '40.78.26.153'. The tooltip also includes options to 'Copy to clipboard' and 'Copy to clipboard' again.

Task 5: Create a table in the SQL Database and select data columns for encryption

In this task, you will connect to the SQL Database with SQL Server Management Studio and create a table. You will then encrypt two data columns using an autogenerated key from the Azure Key Vault.

1. In the Azure portal, navigate to the blade of the **medical** SQL database, in the **Essentials** section, identify the **Server name** (copy to clipboard), and then, in the toolbar, click **Set server firewall**.

Note: Record the server name. You will need the server name later in this task.

Server name: sqlserver4cwfvodk5utxq.database.windows.net

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Microsoft Azure portal interface. The URL in the address bar is <https://portal.azure.com/#@murugiloisegmail.onmicrosoft.com/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/sqlserver4cwfvokd5utxq/providers/Microsoft.DBforSQL/servers/sqlserver4cwfvokd5utxq/databases/medical/networking>. The page title is "sqlserver4cwfvokd5utxq | Networking". The left sidebar shows the "Networking" section under "Security". The main content area shows the "Public access" tab selected. Under "Public network access", the "Selected networks" radio button is selected, with a note: "Connections from the IP addresses configured in the Firewall rules section below will have access to this database. By default, no public IP addresses are allowed." Below this, there is a "Virtual networks" section with a "Add a virtual network rule" button. At the bottom are "Save" and "Discard" buttons. The status bar at the bottom right shows "Activate Windows" and "Go to Settings to activate Windows.", the date "09/11/24", and the time "3:04 PM".

2. On the **Firewall settings** blade, scroll down to Rule Name, click + **Add a firewall rule**, and specify the following settings:

Setting	Value
Rule Name	Allow Mgmt VM
Start IP	the Public IP Address of the az500-10-vm1
End IP	the Public IP Address of the az500-10-vm1

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Microsoft Azure portal interface. The user is navigating through the Azure Security Technologies lab, specifically under the 'Networking' section of a SQL server named 'sqlserver4cwfvokd5utxq'. A modal window titled 'Add a firewall rule' is open, prompting the user to enter a rule name ('Allow Mgmt VM'), a start IP address ('40.78.26.153'), and an end IP address ('40.78.26.153'). The 'OK' button is visible at the bottom right of the modal.

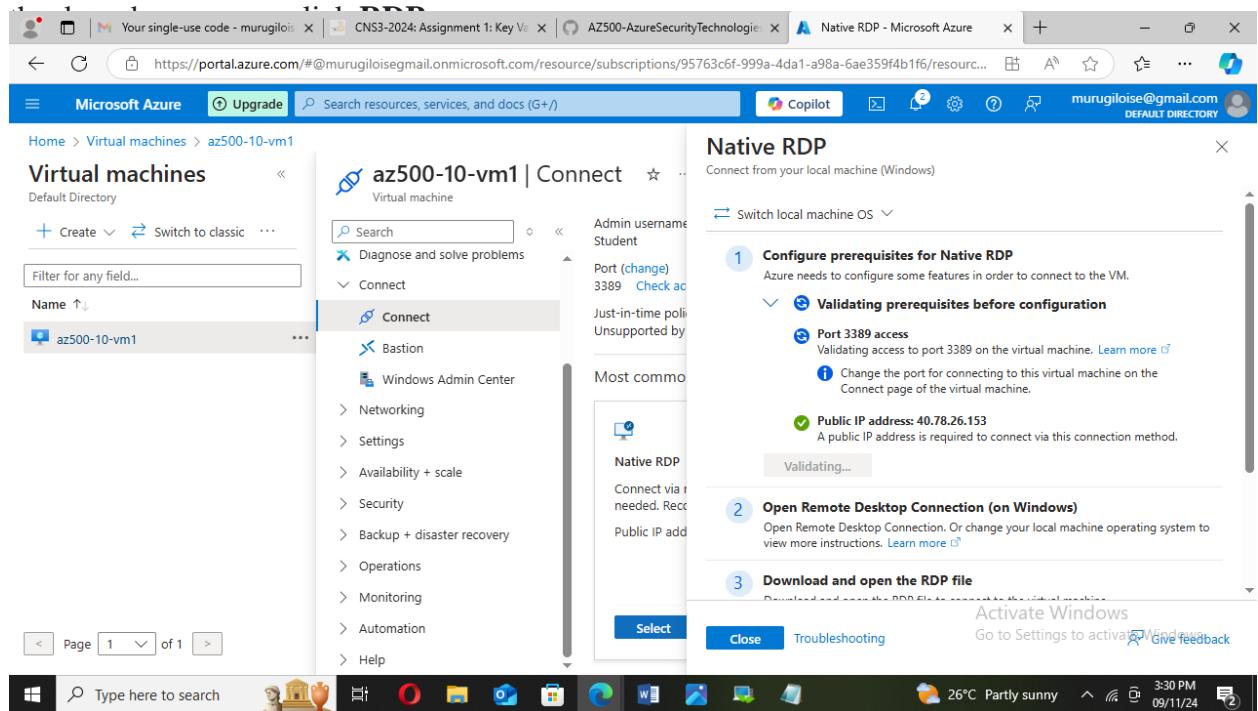
- Click Save to save the change and close the confirmation pane.

Note: This modifies the server firewall settings, allowing connections to the medical database from the Azure VM's public IP address you deployed in this lab.

The screenshot shows the Microsoft Azure portal after saving the firewall rule. A success message box is displayed in the top right corner, stating 'Successfully updated server firewall rules' and 'Successfully updated server firewall rules for server sqlserver4cwfvokd5utxq'. The main interface shows the newly added rule 'Allow Mgmt VM' with the specified IP range in the list of firewall rules.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

4. Navigate back to the **az500-10-vm1** blade, click **Overview**, next click **Connect** and, in



5. Click **Download RDP File** and use it to connect to the **az500-10-vm1** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credentials:

Setting	Value
---------	-------

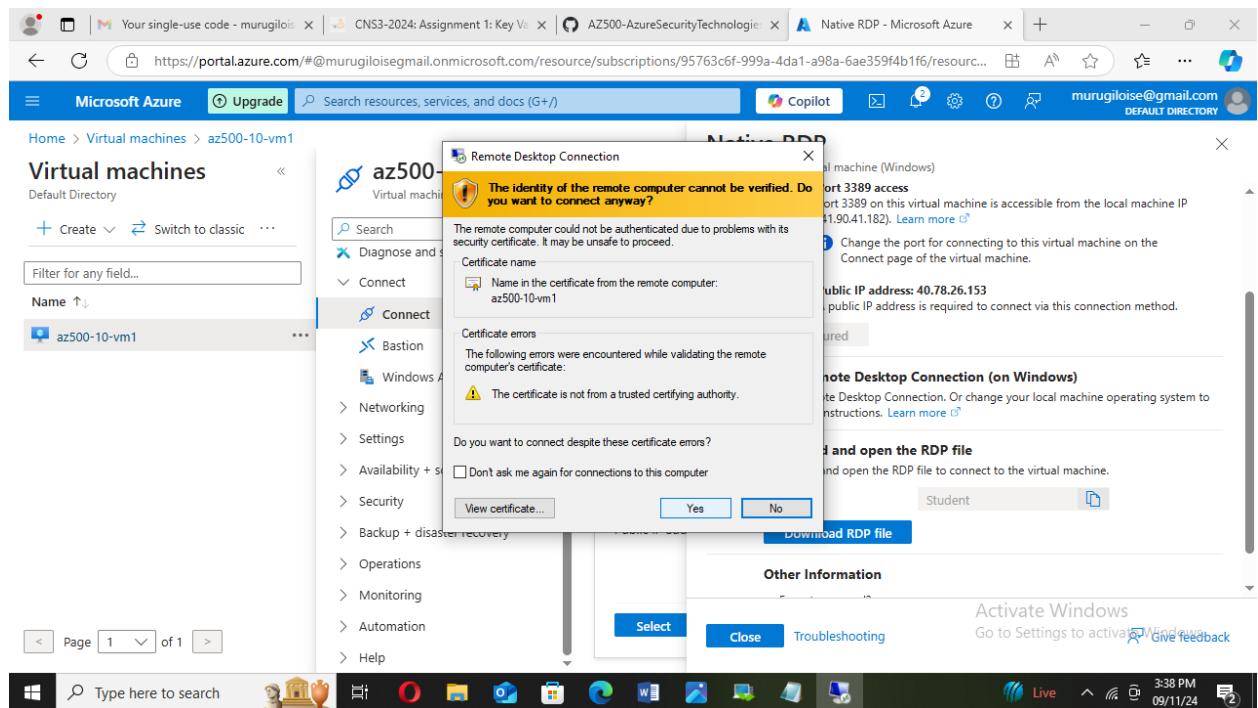
Username	Student
----------	----------------

Password	Please use your personal password created in Lab 02 > Exercise 1 > Task 1 > Step 9.
----------	---

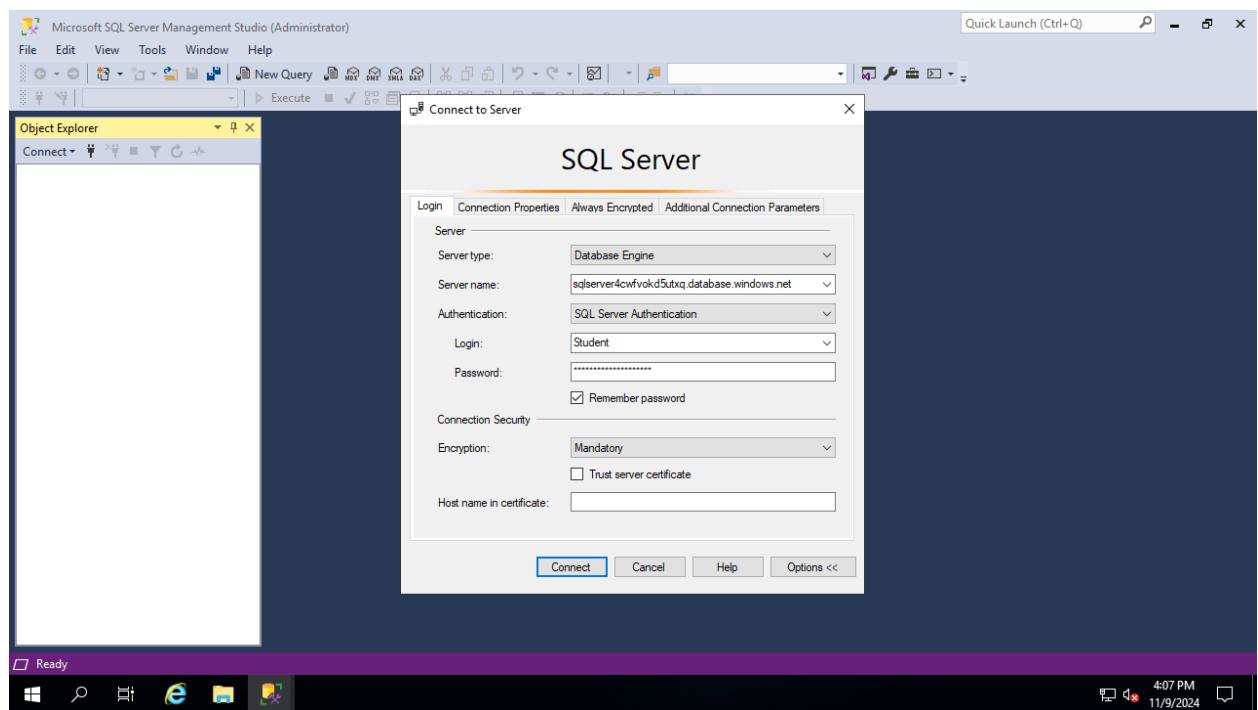
Note: Wait for the Remote Desktop session and **Server Manager** to load. Close Server Manager.

Note: The remaining steps in this lab are performed within the Remote Desktop session to the **az500-10-vm1** Azure VM.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)



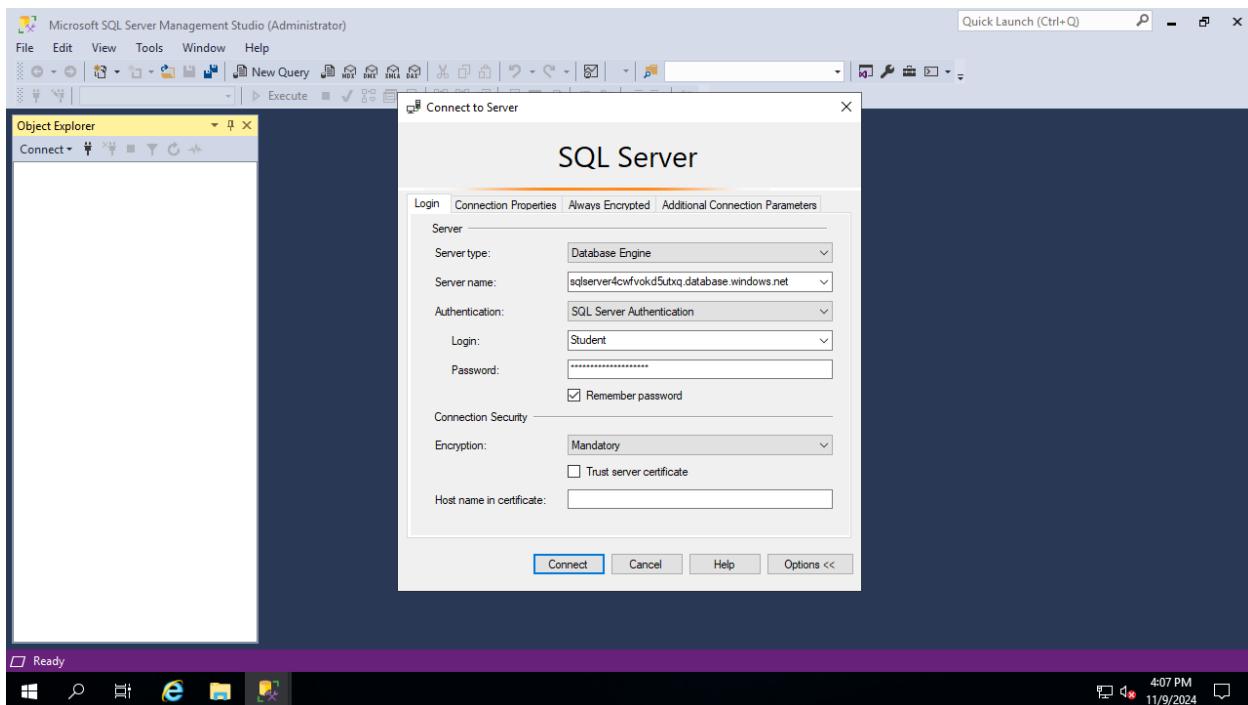
6. Install [SQL Server Management Studio](#) on **az500-10-vm1**. Azure VM.
7. Open **SQL Server Management Studio**. In this part we've opened the sql server management studio



8. In the **Connect to Server** dialog box, specify the following settings:

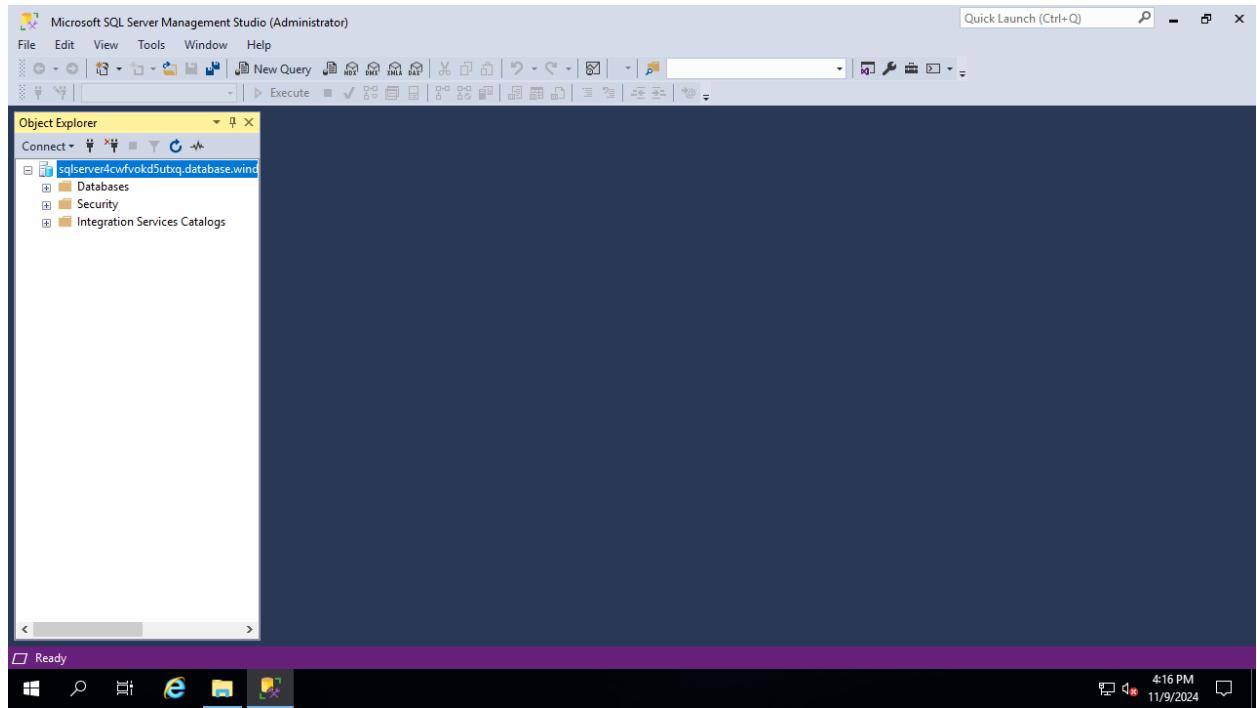
Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Setting	Value
Server Type	Database Engine
Server Name	the server name you identified earlier in this task
Authentication	SQL Server Authentication
Username	Student
Password	Please use your personal password created in Lab 02 > Exercise 2 > Task 1 > Step 3.

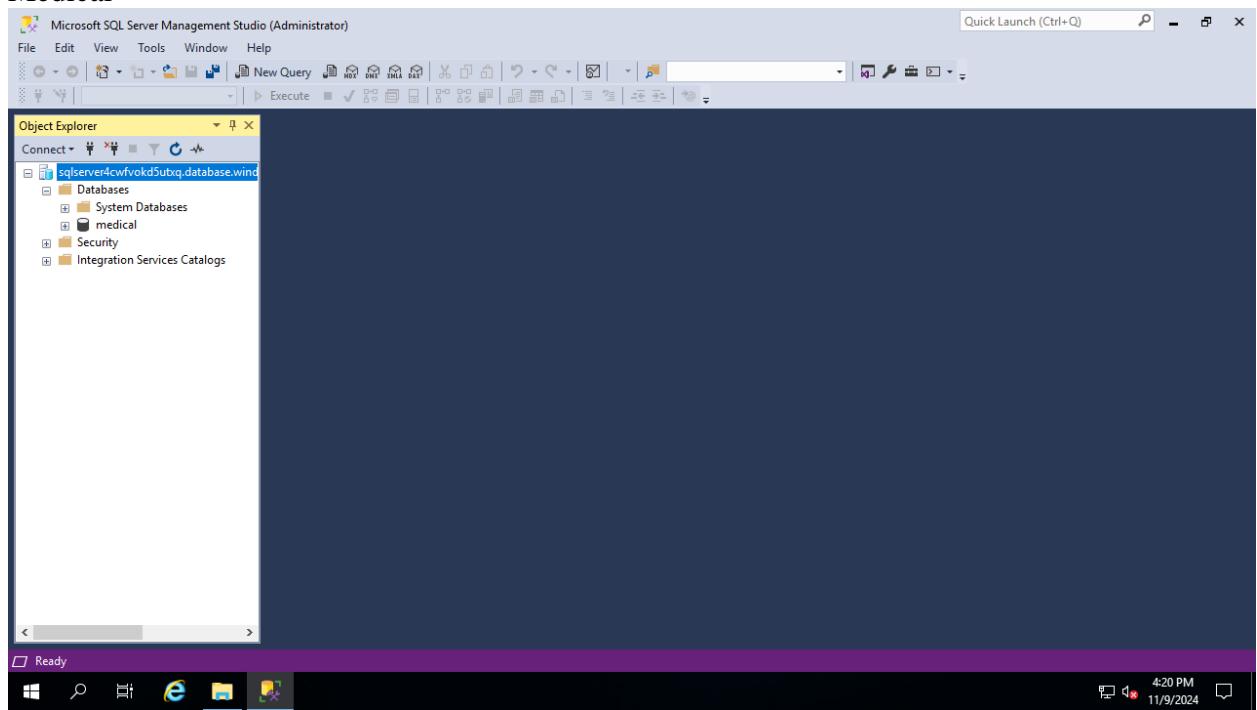


Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

9. In the **Connect to Server** dialog box, click **Connect**. We have successfully connected to the server.

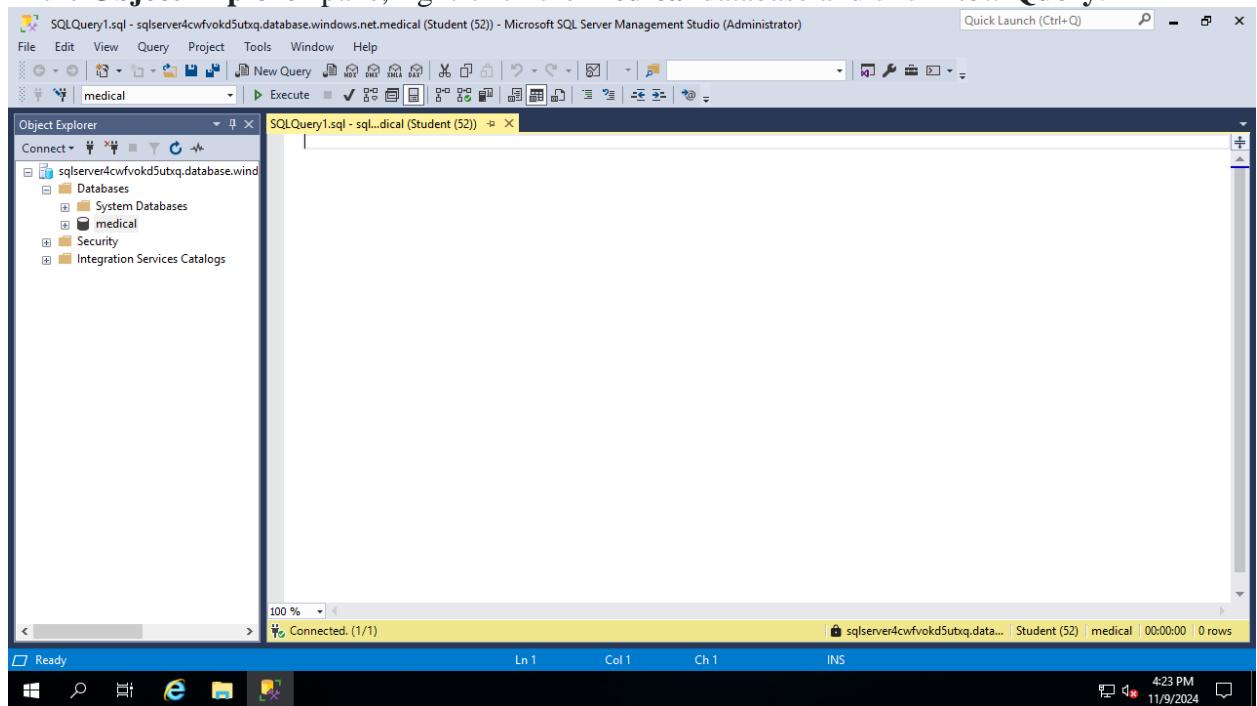


10. Within the **SQL Server Management Studio** console, in the **Object Explorer** pane, expand the **Databases** folder. From the screenshot below we can see our database **Medical**



Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

11. In the **Object Explorer** pane, right-click the **medical** database and click **New Query**.

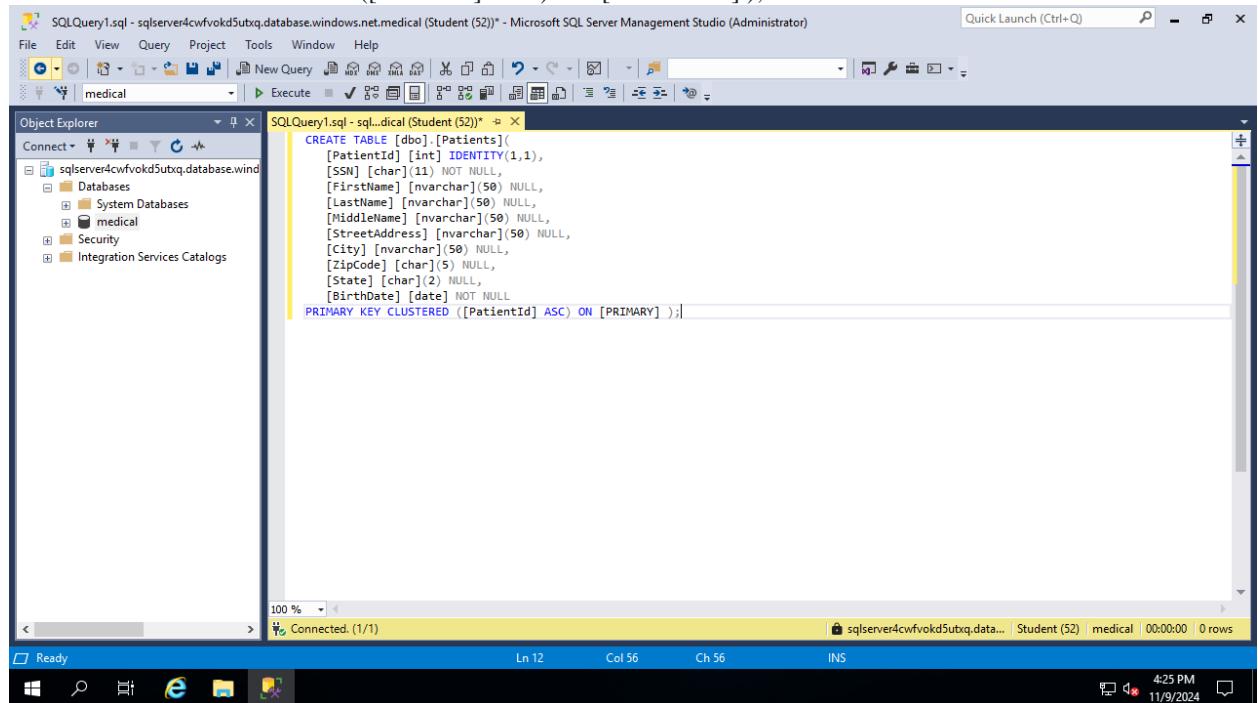


12. Paste the following code into the query window and click **Execute**. This will create a **Patients** table.

```
CREATE TABLE [dbo].[Patients](
    [PatientId] [int] IDENTITY(1,1),
    [SSN] [char](11) NOT NULL,
    [FirstName] [nvarchar](50) NULL,
    [LastName] [nvarchar](50) NULL,
    [MiddleName] [nvarchar](50) NULL,
    [StreetAddress] [nvarchar](50) NULL,
    [City] [nvarchar](50) NULL,
    [ZipCode] [char](5) NULL,
    [State] [char](2) NULL,
    [BirthDate] [date] NOT NULL
```

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

PRIMARY KEY CLUSTERED ([PatientId] ASC) ON [PRIMARY]);

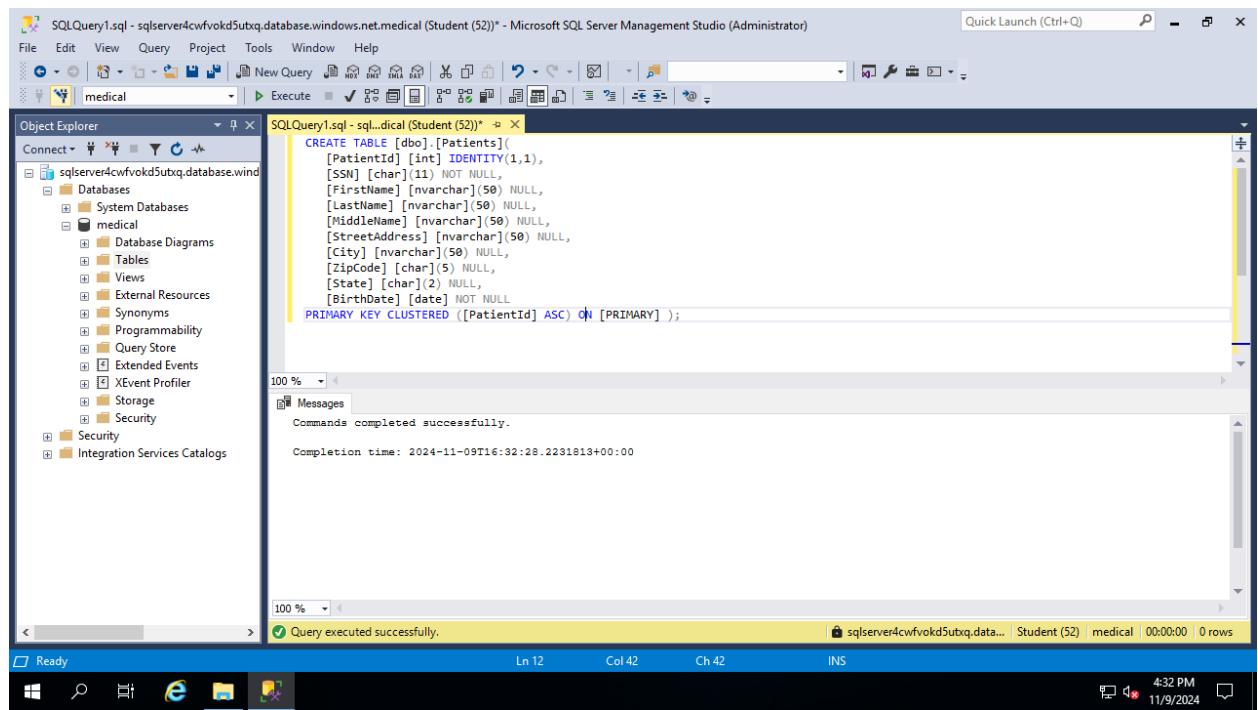


The screenshot shows the Microsoft SQL Server Management Studio interface. In the Object Explorer pane, the 'medical' database is selected. In the center query editor window, the following T-SQL code is displayed:

```
CREATE TABLE [dbo].[Patients]
(
    [PatientId] [int] IDENTITY(1,1),
    [SSN] [char](11) NOT NULL,
    [FirstName] [nvarchar](50) NULL,
    [LastName] [nvarchar](50) NULL,
    [MiddleName] [nvarchar](50) NULL,
    [StreetAddress] [nvarchar](50) NULL,
    [City] [nvarchar](50) NULL,
    [ZipCode] [char](5) NULL,
    [State] [char](2) NULL,
    [BirthDate] [date] NOT NULL
)
PRIMARY KEY CLUSTERED ([PatientId] ASC) ON [PRIMARY] ;
```

The status bar at the bottom indicates 'Connected (1/1)', 'Ln 12', 'Col 56', 'Ch 56', and 'INS'. The system tray shows the date and time as 11/9/2024 4:25 PM.

The command has been executed successfully.

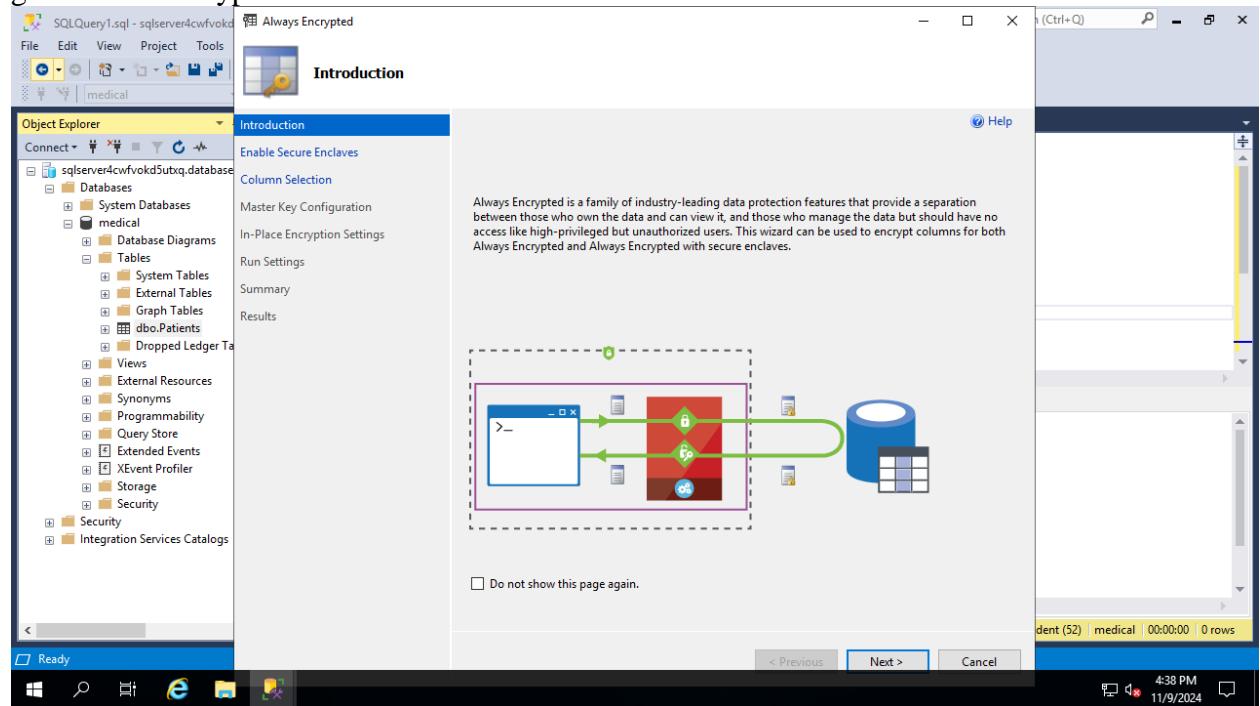


The screenshot shows the Microsoft SQL Server Management Studio interface. In the Object Explorer pane, the 'medical' database is selected. In the center query editor window, the same T-SQL code is displayed. Below the code, the message 'Commands completed successfully.' is shown, along with the completion time 'Completion time: 2024-11-09T16:32:28.2231813+00:00'. The status bar at the bottom indicates 'Query executed successfully.', 'Ln 12', 'Col 42', 'Ch 42', and 'INS'. The system tray shows the date and time as 11/9/2024 4:32 PM.

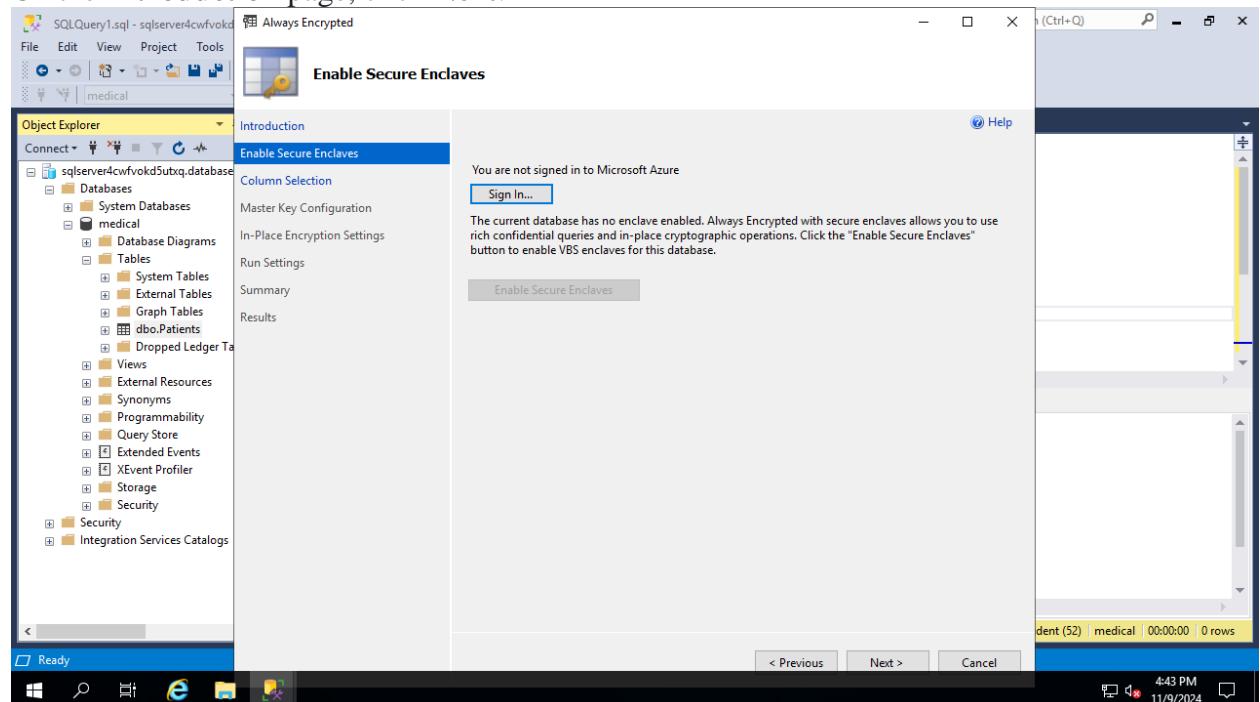
13. After the table is created successfully, in the **Object Explorer** pane, expand the **medical** database node, the **tables** node, right-click the **dbo.Patients** node, and click **Encrypt Columns**.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Note: This will initiate the **Always Encrypted** wizard. From the screenshot below we've gone to the encryption wizard.



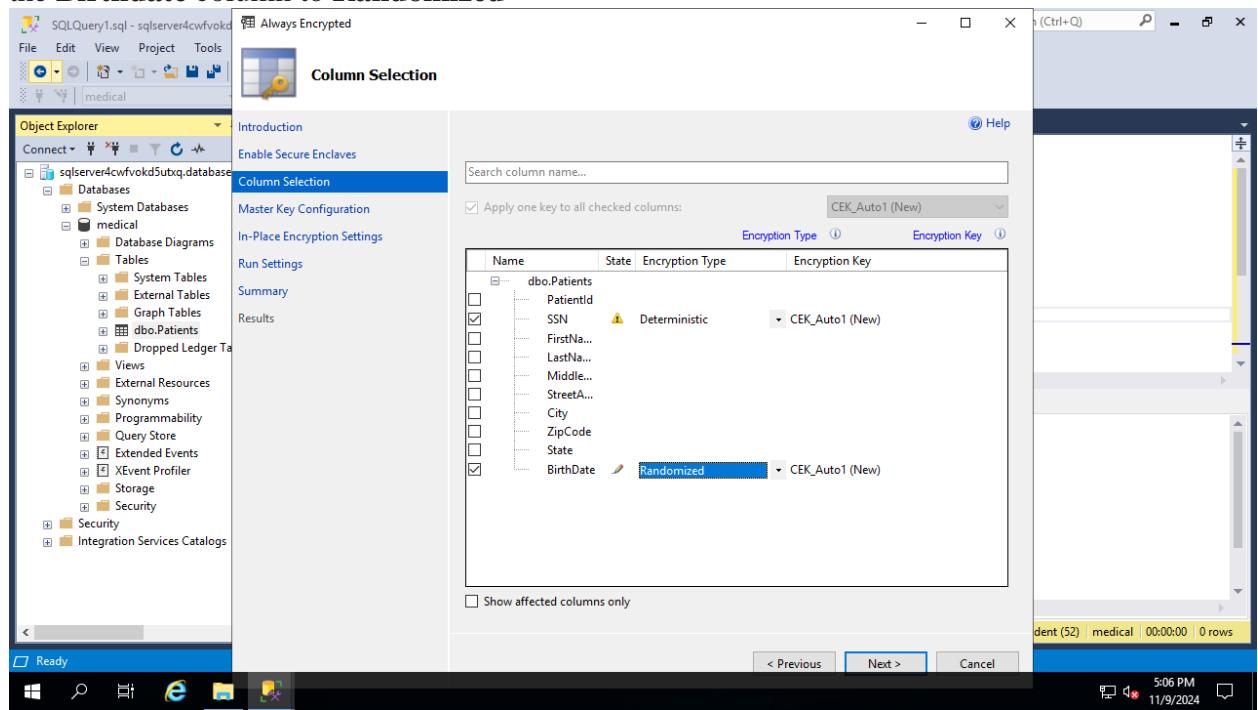
14. On the **Introduction** page, click **Next**.



15. On the **Column Selection** page, select the **SSN** and **Birthdate** columns, set the **Encryption Type** of the **SSN** column to **Deterministic** and of the **Birthdate** column to **Randomized**, and click **Next**.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

From the screenshot below we have set SSN column to **Deterministic** and of the Birthdate column to **Randomized**

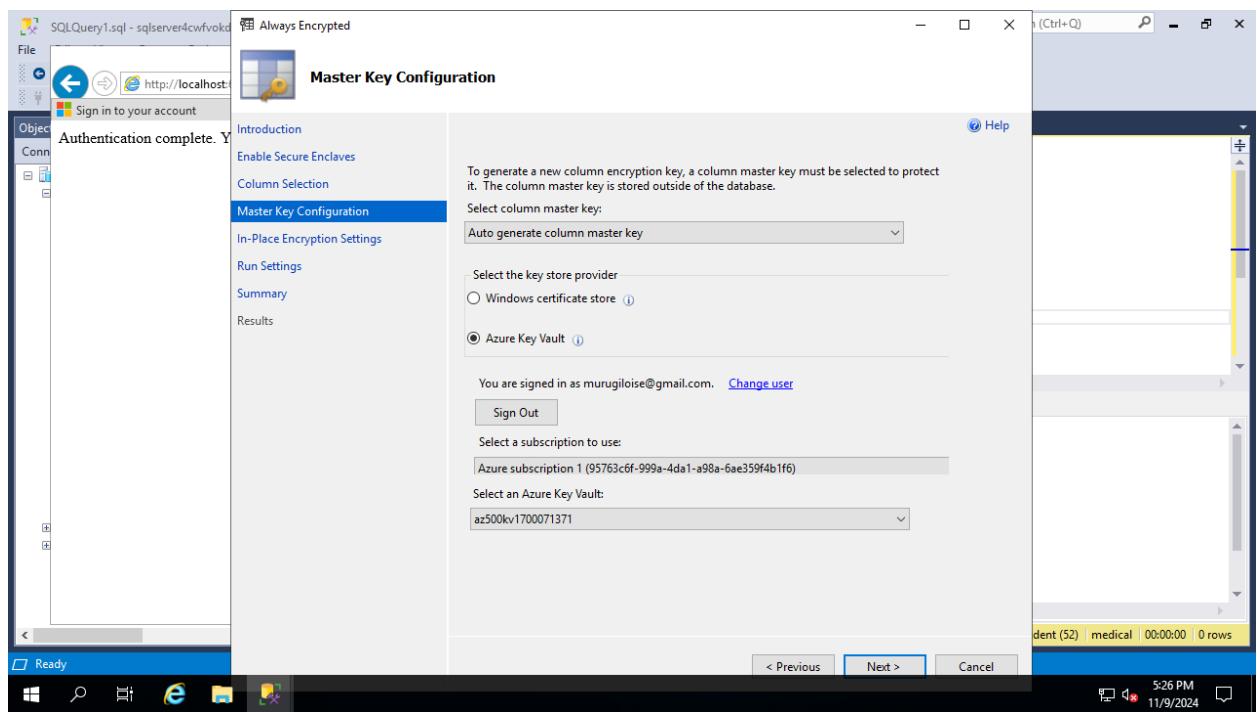


Note: While performing the encryption if any error thrown like **Exception has been thrown by the target of an invocation** related to **Rotary(Microsoft.SqlServer.Management.ServiceManagement)** then make sure the **Key Permission's values of Rotation Policy Operations** are **unchecked**, if not in the Azure portal navigate to the **Key Vault >> Access Policies >> Key Permissions >>** Uncheck all the values under the **Rotation Policy Operations >> Under Privileged Key Operations >> Uncheck Release**.

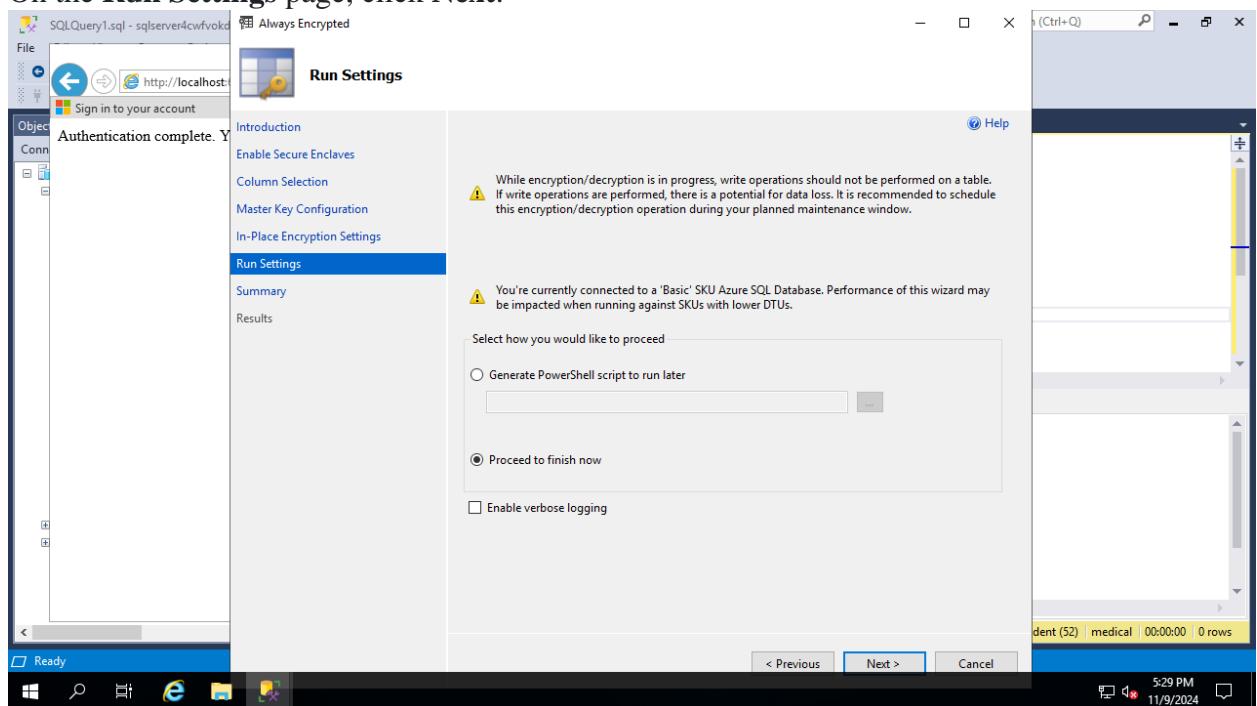
16. On the **Master Key Configuration** page, select **Azure Key Vault**, click **Sign in**, when prompted, authenticate by using the same user account you used to provision the Azure Key Vault instance earlier in this lab, ensure that that Key Vault appears in the **Select an Azure Key Vault** drop down list, and click **Next**.

After logging in to Azure we were able to pull the Azure Key Vault and the subscription as seen below.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)



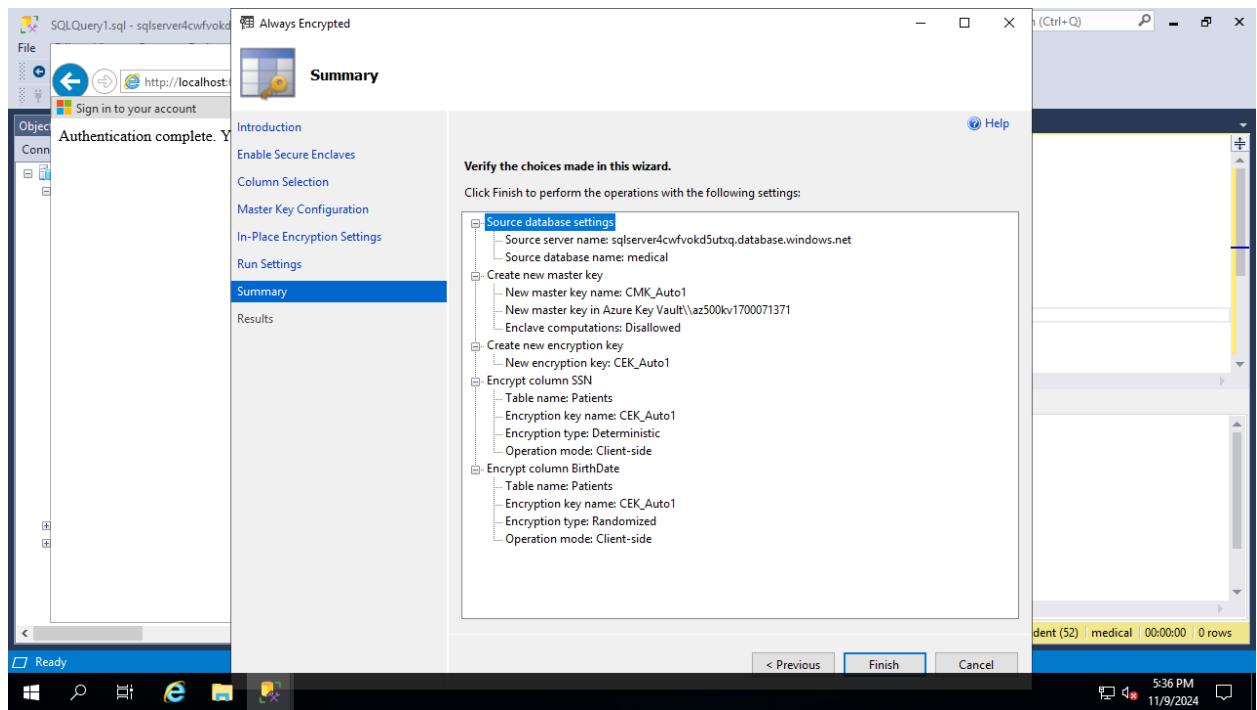
17. On the Run Settings page, click Next.



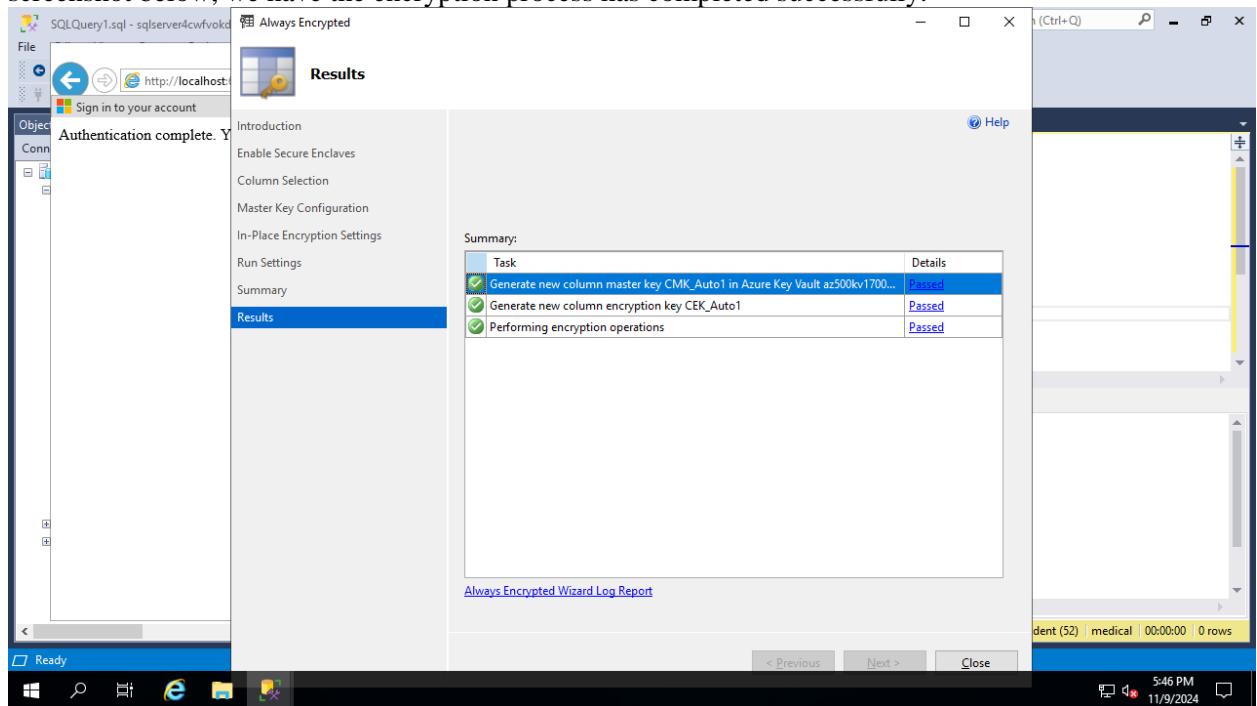
18. On the Summary page, click **Finish** to proceed with the encryption. When prompted, sign in again by using the same user account you used to provision the Azure Key Vault instance earlier in this lab.

At this point we click on finish.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)



19. Once the encryption process is complete, on the **Results** page, click **Close**. From The screenshot below, we have the encryption process has completed successfully.



20. In the **SQL Server Management Studio** console, in the **Object Explorer** pane, under the **medical** node, expand the **Security** and **Always Encrypted Keys** subnodes.

Note: The **Always Encrypted Keys** subnode contains the **Column Master Keys** and **Column Encryption Keys** subfolders.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

From the screenshot below, under Security and Always Encrypted Keys subnodes. We can see the Column Master Keys and Column Encryption Keys subfolders.

The screenshot shows the Microsoft SQL Server Management Studio interface. In the Object Explorer, the database 'medical' is selected, and the 'Security' node is expanded, showing 'Always Encrypted Keys' as a subnode. Under 'Always Encrypted Keys', there are two subfolders: 'Column Master Keys' and 'Column Encryption Keys'. In the center pane, a query window displays the creation of a 'Patients' table:

```
CREATE TABLE [dbo].[Patients]
(
    [PatientId] [int] IDENTITY(1,1),
    [SSN] [char](11) NOT NULL,
    [FirstName] [nvarchar](50) NULL,
    [LastName] [nvarchar](50) NULL,
    [MiddleName] [nvarchar](50) NULL,
    [StreetAddress] [nvarchar](50) NULL,
    [City] [nvarchar](50) NULL,
    [ZipCode] [char](5) NULL,
    [State] [char](2) NULL,
    [BirthDate] [date] NOT NULL
)
PRIMARY KEY CLUSTERED ([PatientId] ASC) ON [PRIMARY];
```

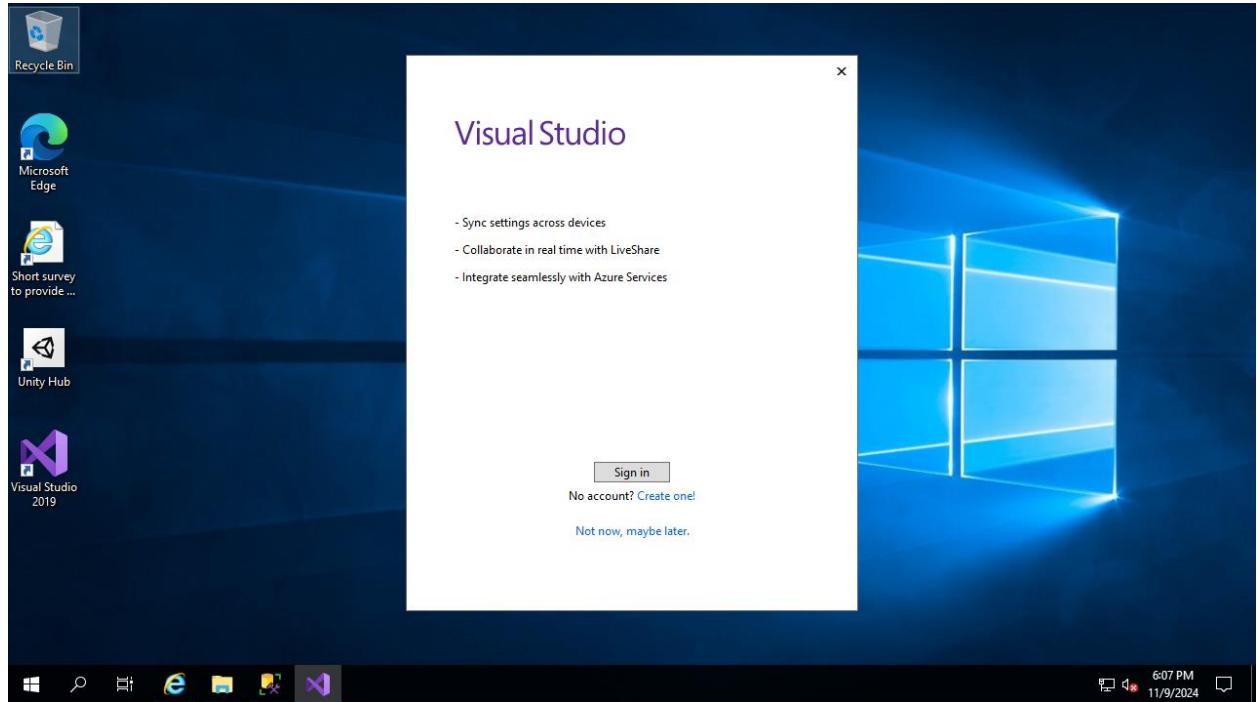
The status bar at the bottom right indicates the session is running as 'Student (52)' on the 'medical' database with a connection time of '00:00:00' and '0 rows' affected.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Exercise 4: Demonstrate the use of Azure Key Vault in encrypting the Azure SQL database

Task 1: Run a data-driven application to demonstrate the use of Azure Key Vault in encrypting the Azure SQL database

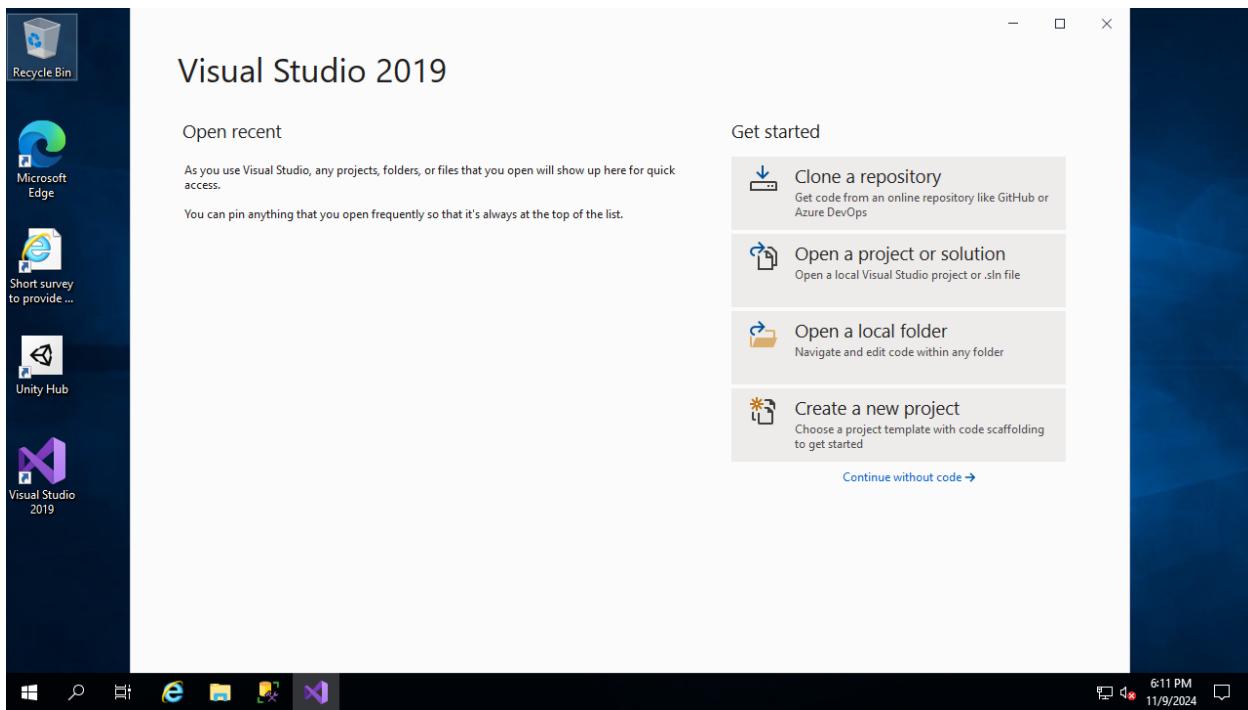
1. From the RDP session to the **az500-10-vm1**, launch **Visual Studio 2019** from the **Start menu**.



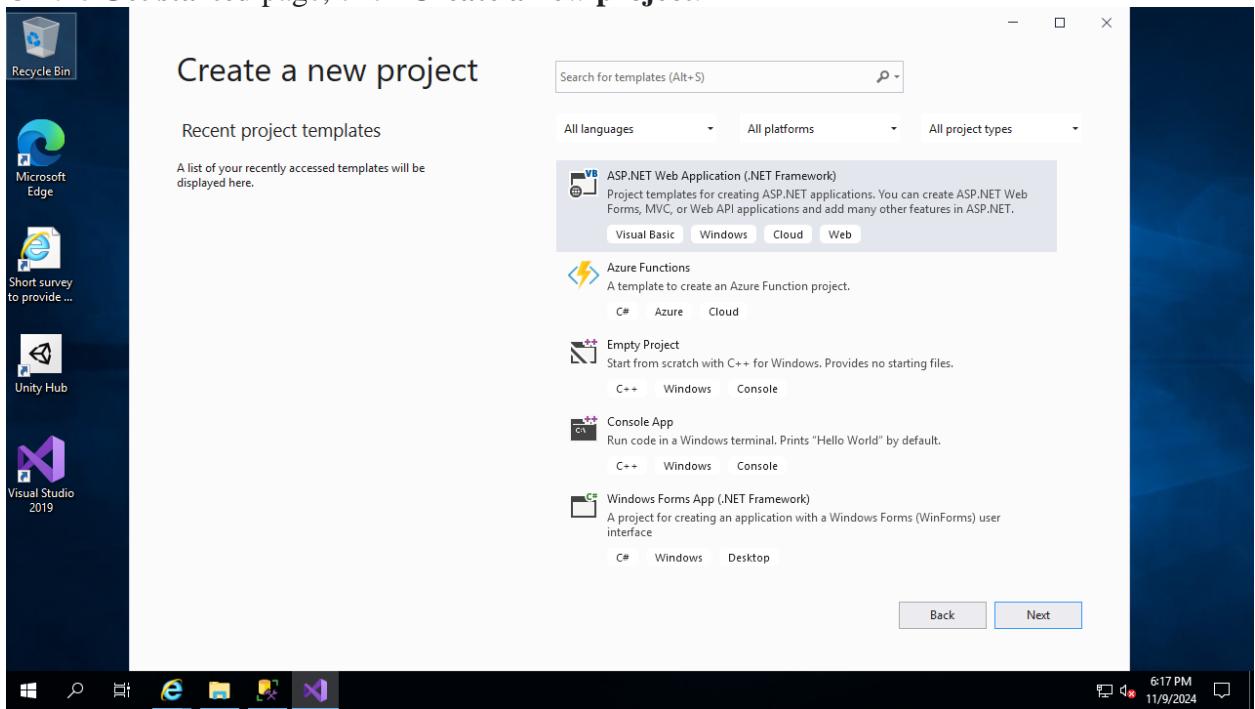
2. Switch to the window displaying Visual Studio 2019 welcome message, click the **Sign in** button and, when prompted, provide the credentials you used to authenticate to the Azure subscription you are using in this lab.

We have been able to login successfully to the visual studio as seen below.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

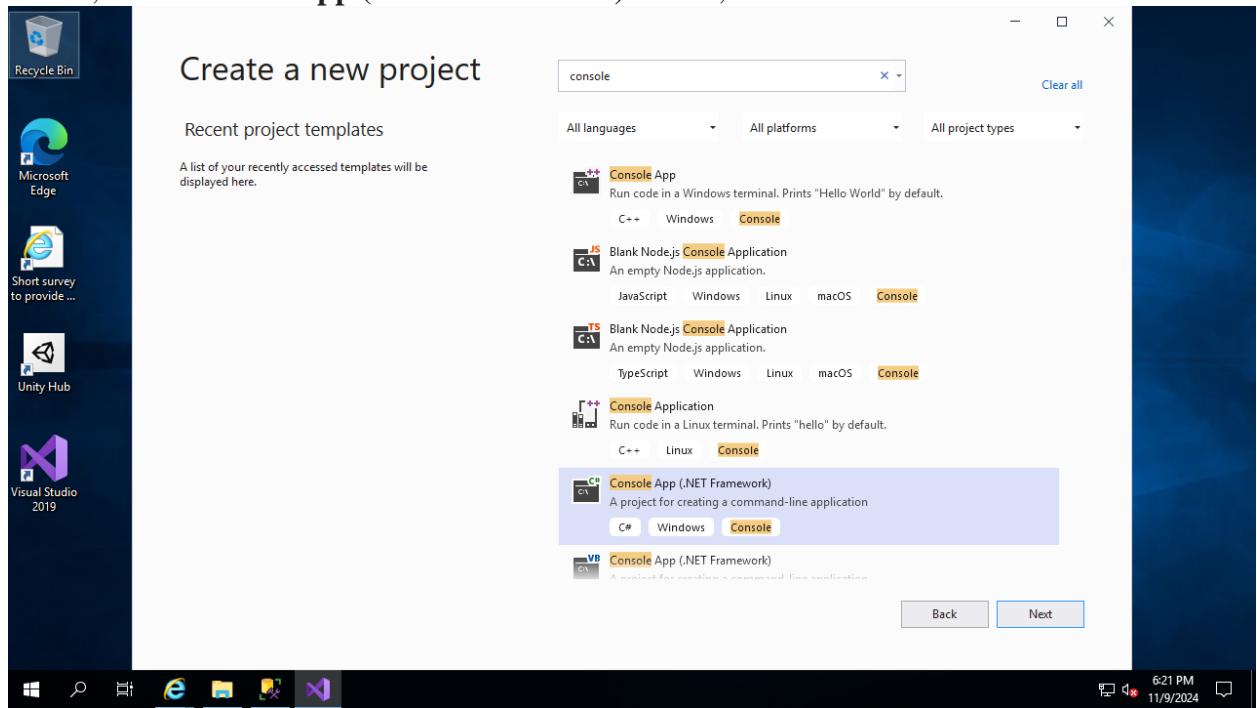


3. On the **Get started** page, click **Create a new project**.



Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

4. In the list of project templates, search for **Console App (.NET Framework)**, in the list of results, click **Console App (.NET Framework)** for C#, and click **Next**.



5. On the **Configure your new project** page, specify the following settings (leave other settings with their default values), then click **Create**:

Setting

Project name

Solution name

Framework

Value

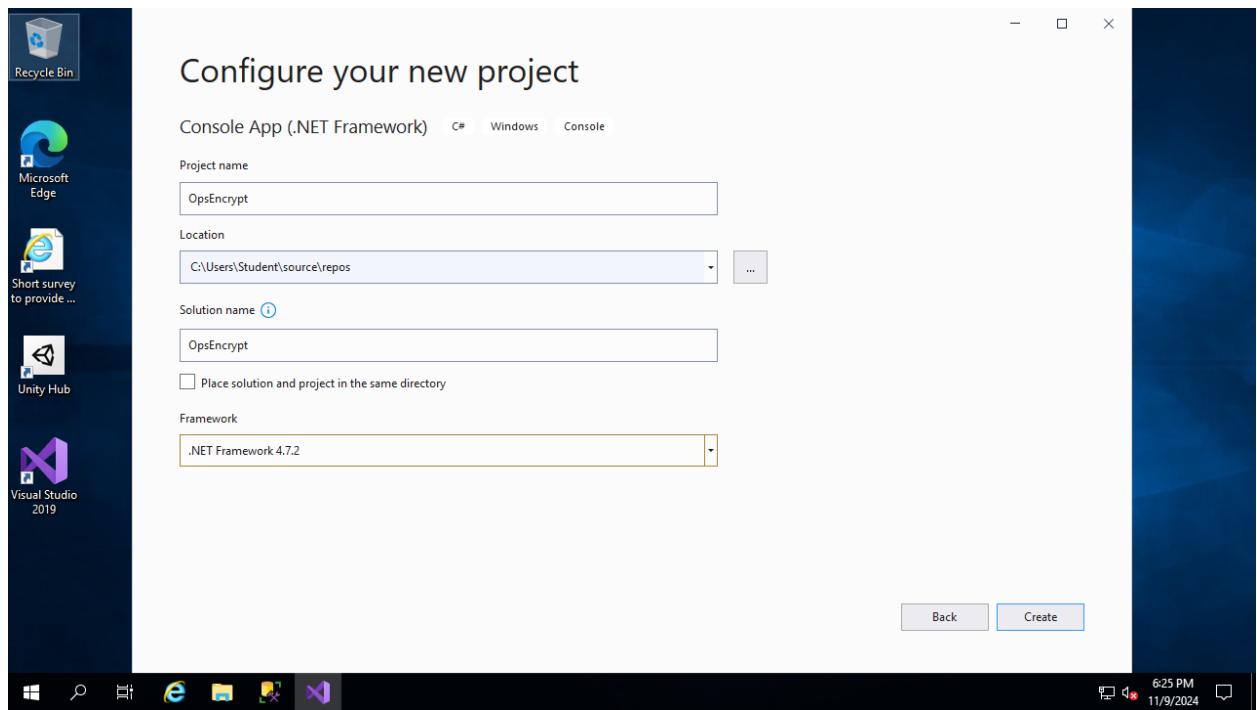
OpsEncrypt

OpsEncrypt

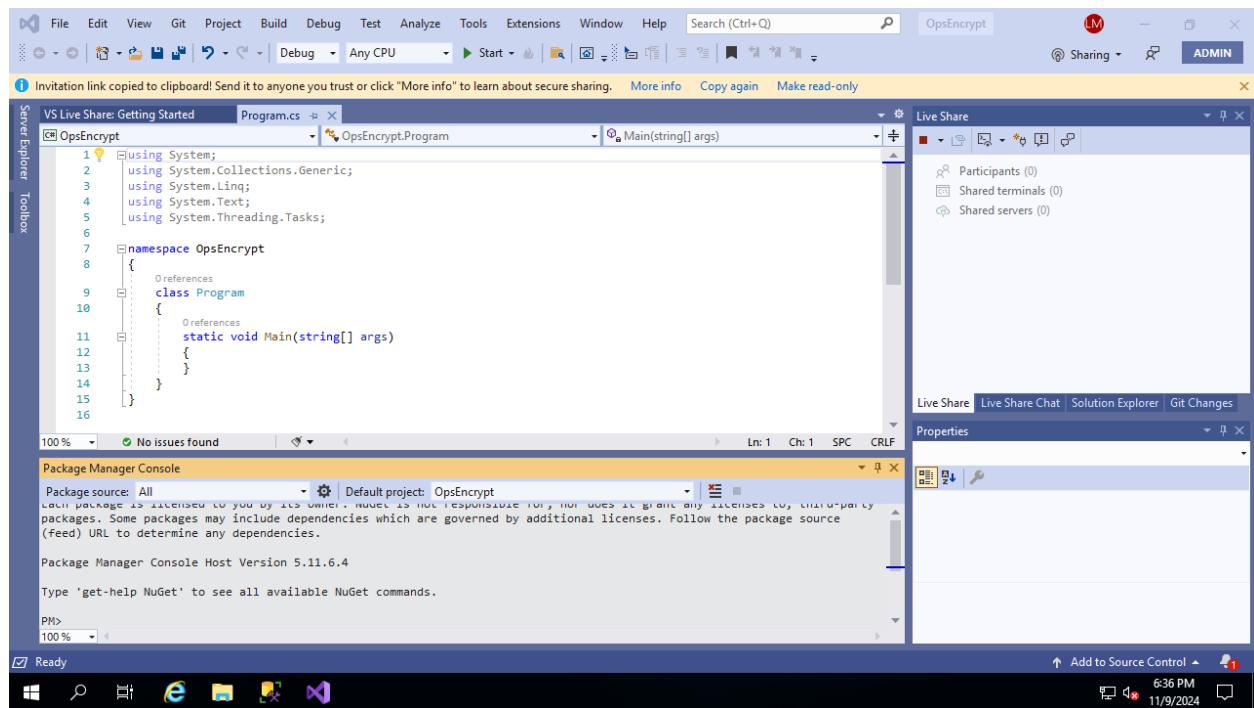
**.NET Framework
4.7.2**

From the screenshot below we have configured our new project **OpsEncrypt**

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)



- In the Visual Studio console, click the **Tools** menu, in the drop down menu, click **NuGet Package Manager**, and, in the cascading menu, click **Package Manager Console**. From the screenshot below, we have successfully navigated to the Package Manager Console



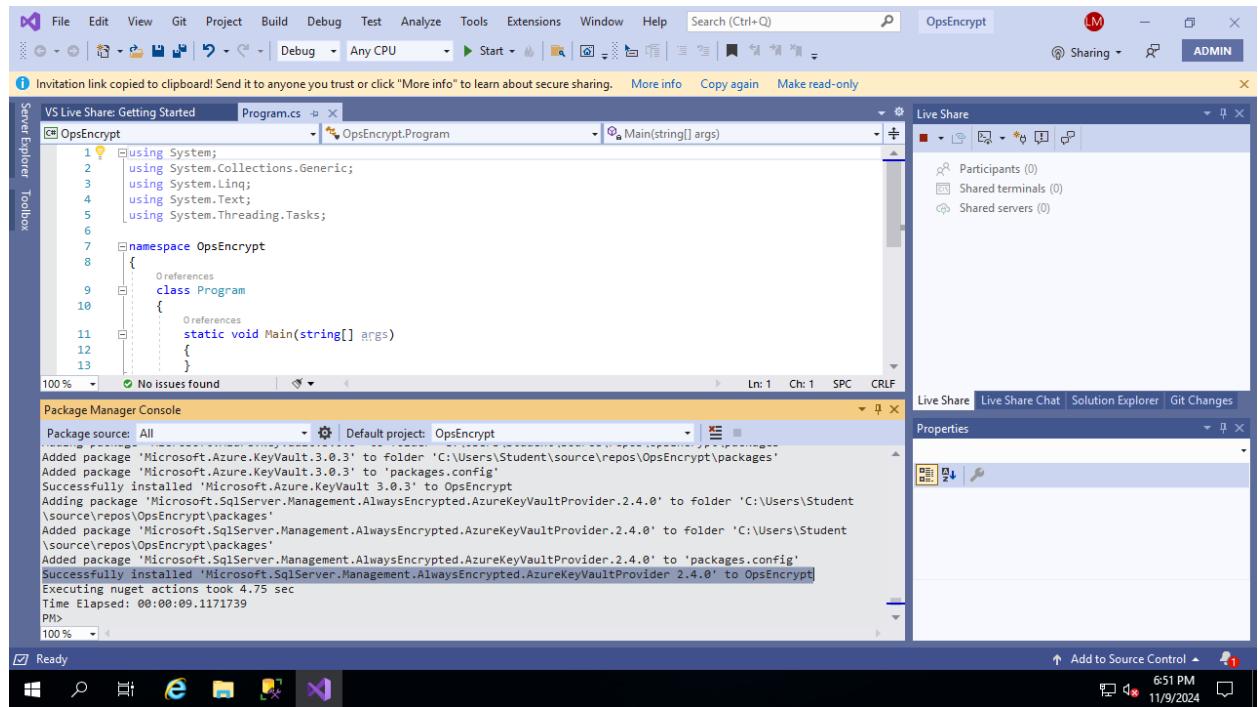
- In the **Package Manager Console** pane, run the following to install the first required **NuGet** package:

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Install-Package Microsoft.SqlServer.Management.AlwaysEncrypted.AzureKeyVaultProvider

We have successfully installed the package

Microsoft.SqlServer.Management.AlwaysEncrypted.AzureKeyVaultProvider



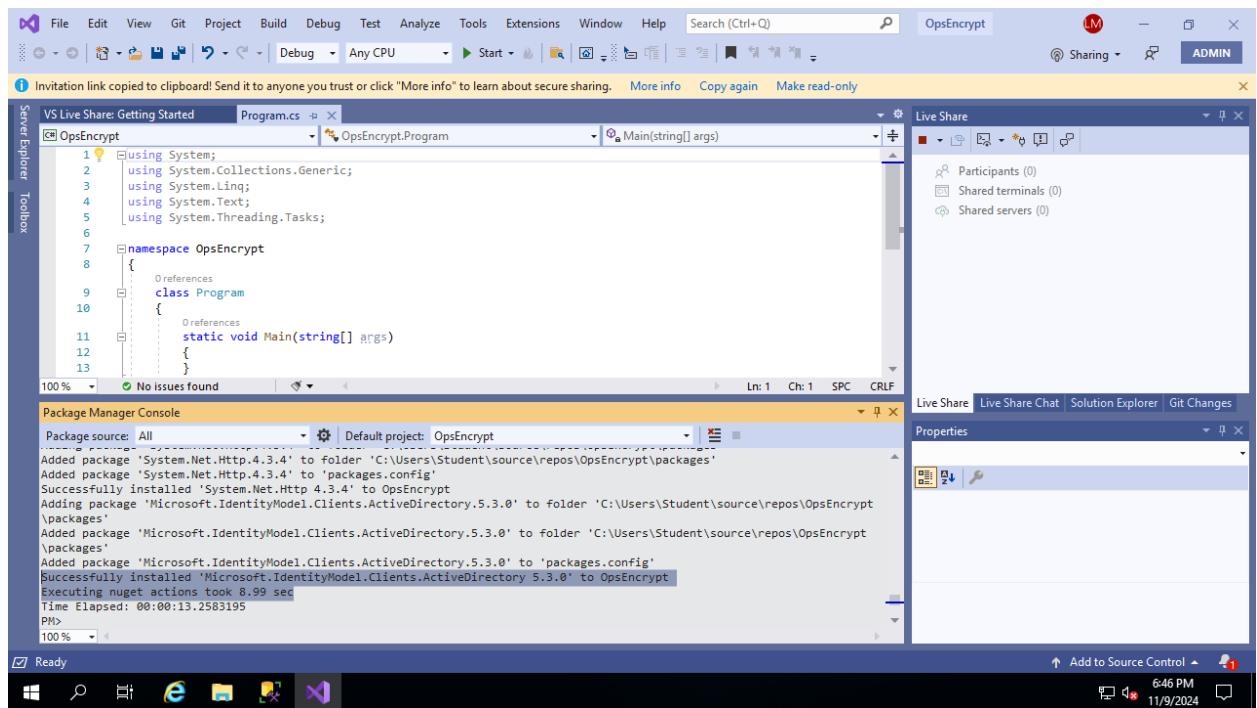
8. In the **Package Manager Console** pane, run the following to install the second required **NuGet** package:

Install-Package Microsoft.IdentityModel.Clients.ActiveDirectory

We have successfully installed the package

Microsoft.IdentityModel.Clients.ActiveDirectory

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)



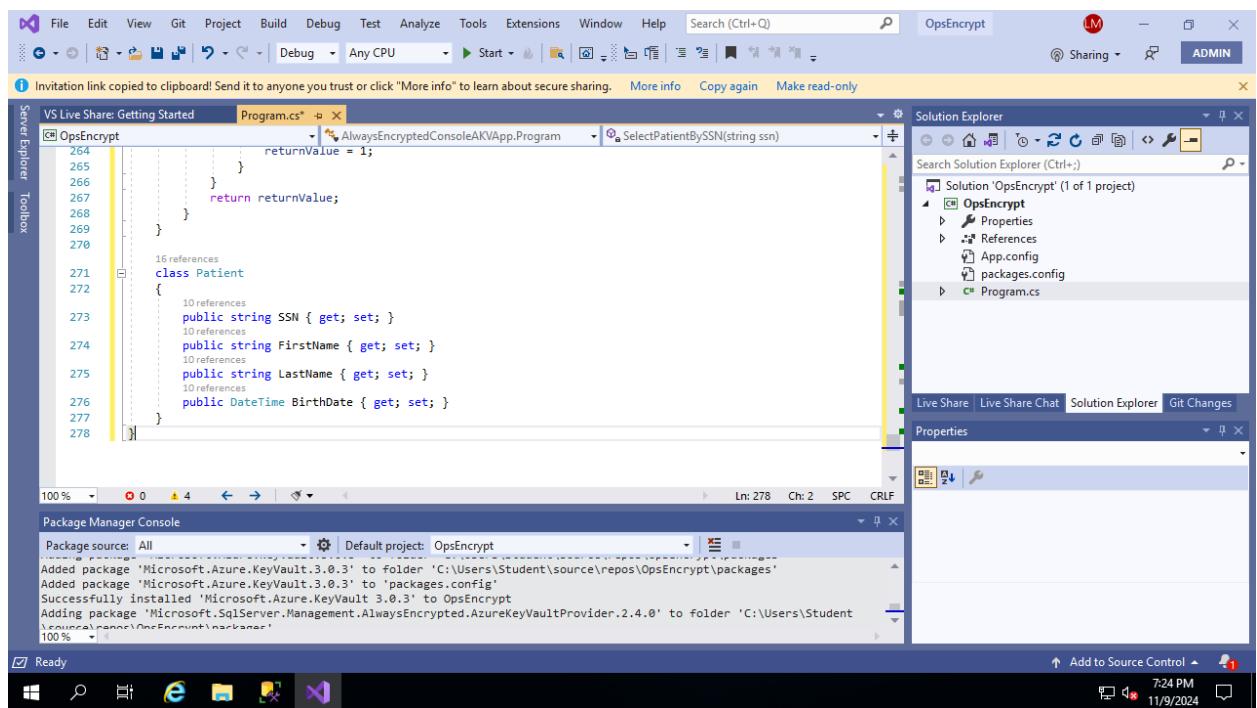
- Minimize the RDP session to your Azure virtual machine, then navigate to **\Allfiles\Labs\10\program.cs**, open it in Notepad, and copy its content into Clipboard.

We have copied the content program.cs on a clipboard

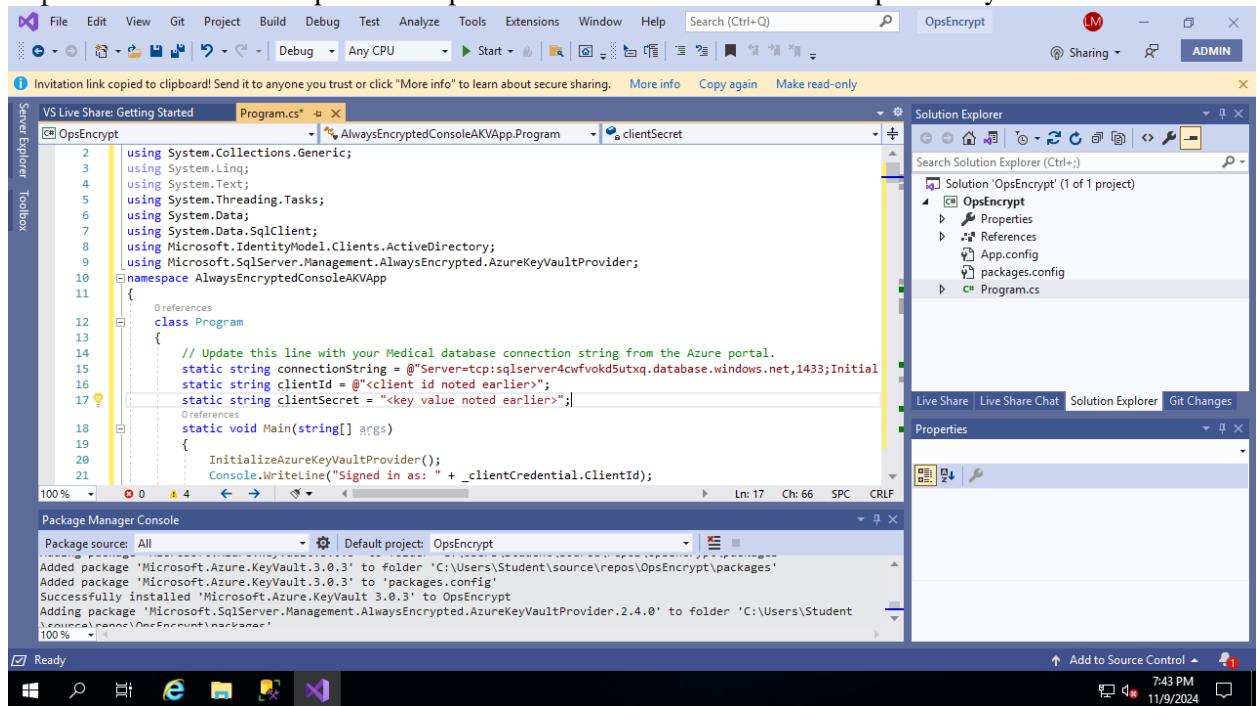
- Return to the RDP session, and in the Visual Studio console, in the **Solution Explorer** window, click **Program.cs** and replace its content with the code you copied into Clipboard.

We have replaced the code we had copied from program.cs lab 10 in the solution explorer on the visual studio as seen below.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

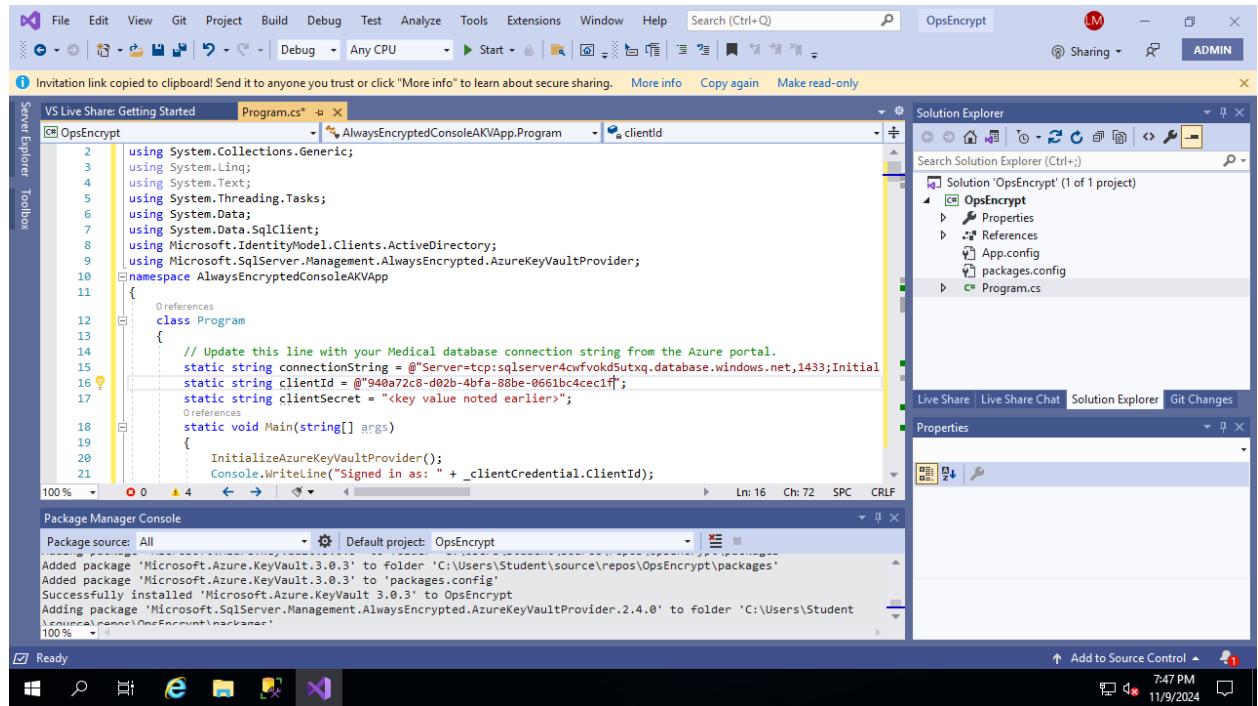


11. In the Visual Studio window, in the **Program.cs** pane, in line 15, replace the <connection string noted earlier> placeholder with the Azure SQL database **ADO.NET** connection string you recorded earlier in the lab. In the connection string, replace the {your_password} placeholder, with the password that you specified in the deployment in Exercise 1. If you saved the string on the lab computer, you may need to leave the RDP session to copy the ADO string, then return to the Azure virtual machine to paste it in. We have replaced the password and ADO.NET as we had previously saved.



Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

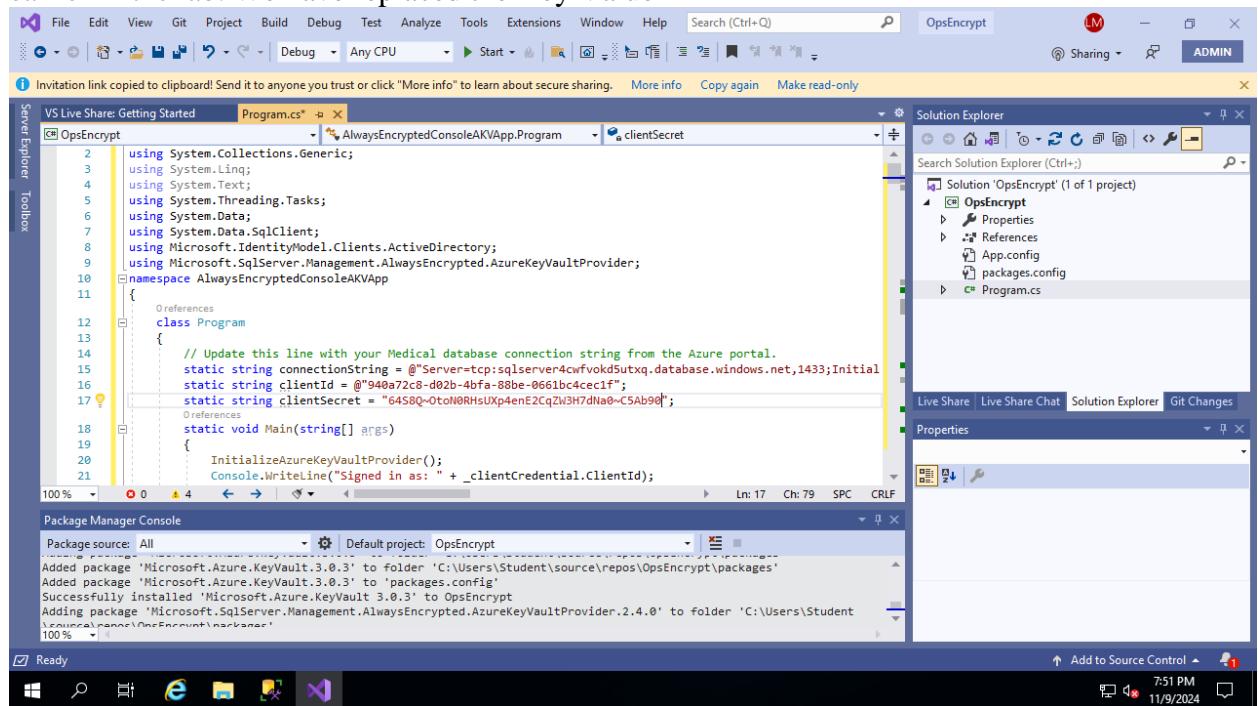
12. In the Visual Studio window, in the **Program.cs** pane, in line 16, replace the <client id noted earlier> placeholder with the value of **Application (client) ID** of the registered app you recorded earlier in the lab. We have replaced the Apploication ID as previously registered.



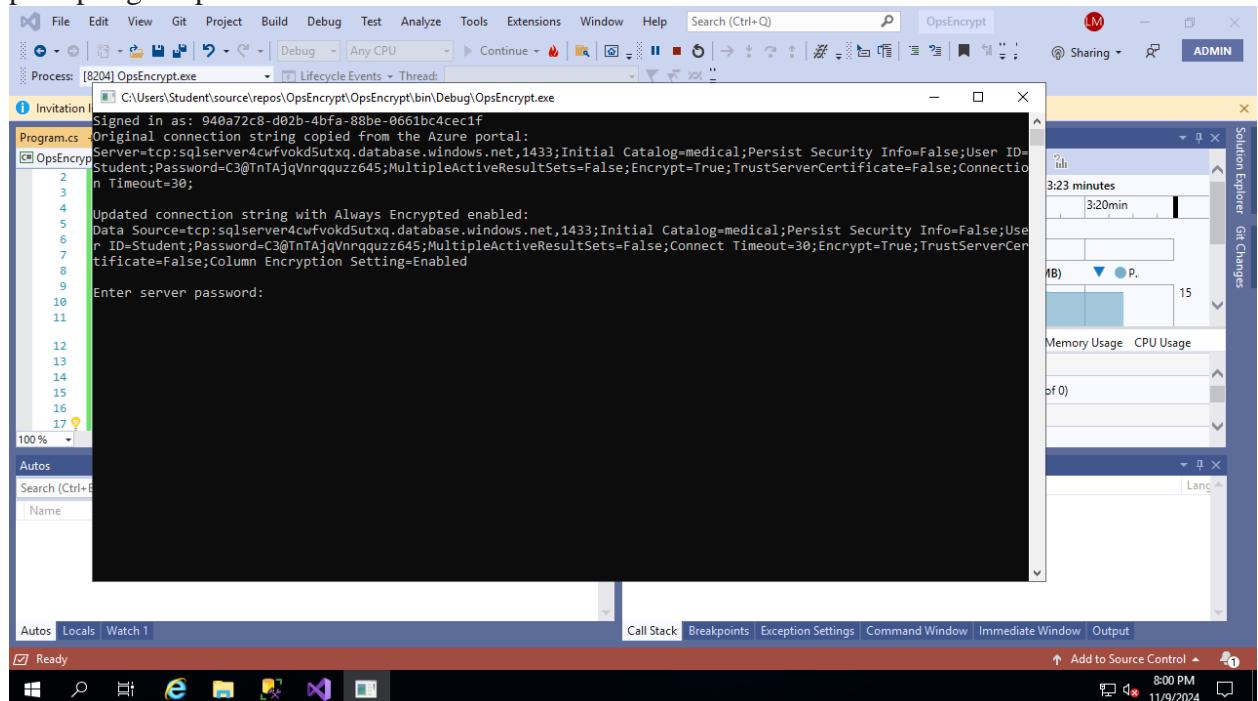
13. In the Visual Studio window, in the **Program.cs** pane, in line 17, replace the <key value noted earlier> placeholder with the the value of **Key1** of the registered app you recorded

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

earlier in the lab. We have replaced the Key Value 1



14. In the Visual Studio console, click the **Start** button to initiate the build of the console application and start it. After pressing the start button we get a command prompt window prompting for password as seen below.



15. The application will start a Command Prompt window. When prompted for password, type the password that you specified in the deployment in Exercise 1 to connect to Azure SQL Database.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

From the screenshot below we have added sample patient data to the database

```
Process: [9268] OpsEncrypt.exe
File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help Search (Ctrl+Q) OpsEncrypt
Sharing ADMIN

Process: [9268] OpsEncrypt.exe Lifecycle Events Thread: 
Invitation
Program.cs
OpsEncrypt

Signed in as: 940a72c8-d02b-4bfa-88be-0661bc4ce1f
Original connection string copied from the Azure portal:
Server=tcp:sqlserver4cuvfokd5utxq.database.windows.net,1433;Initial Catalog=medical;Persist Security Info=False;User ID=Student;Password=C3@nTAjqVnrquzz645;MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;

Updated connection string with Always Encrypted enabled:
Data Source=tcp:sqlserver4cuvfokd5utxq.database.windows.net,1433;Initial Catalog=medical;Persist Security Info=False;User ID=Student;Password=C3@nTAjqVnrquzz645;MultipleActiveResultSets=False;Connect Timeout=30;Encrypt=True;TrustServerCertificate=False;Column Encryption Setting=Enabled

Enter server password:
C3@nTAjqVnrquzz645

Adding sample patient data to the database...
All the records currently in the Patients table:
Orlando Gee SSN: 999-99-0001 Birthdate: 1/4/1964 12:00:00 AM
Keith Harris SSN: 999-99-0002 Birthdate: 6/20/1977 12:00:00 AM
Donna Carreras SSN: 999-99-0003 Birthdate: 2/9/1973 12:00:00 AM
Janet Gates SSN: 999-99-0004 Birthdate: 8/31/1985 12:00:00 AM
Lucy Harrington SSN: 999-99-0005 Birthdate: 5/6/1993 12:00:00 AM

Autos Now lets locate records by searching the encrypted SSN column.
Search (Ctrl+F)
Name

Call Stack Breakpoints Exception Settings Command Window Immediate Window Output
 Autos Locals Watch 1 Add to Source Control ▾ 8:10 PM 11/9/2024
```

16. Leave the console app running and switch to the **SQL Management Studio** console. We have switched to the SQL Management studio as seen below

The screenshot shows the Microsoft SQL Server Management Studio interface. The title bar indicates the connection is to 'SQLQuery1.sql - sqlserver4cwfvolkd5utxq.database.windows.net.medical (Student (52))' with 'Administrator' privileges. The 'File', 'Edit', 'View', 'Project', 'Tools', 'Window', and 'Help' menus are visible at the top. Below the menu bar is a toolbar with various icons for database management tasks. The 'Object Explorer' pane on the left lists the database structure, including 'Databases', 'Tables', 'Views', 'External Resources', 'Synonyms', 'Programmability', 'Query Store', 'Extended Events', 'XEvent Profiler', 'Storage', 'Security' (which is expanded to show 'Users', 'Roles', 'Schemas', 'Asymmetric Keys', 'Certificates', 'Symmetric Keys', 'Always Encrypted Keys', 'Column Master Keys', 'Column Encryption Keys', and 'Security Policies'), and 'Filegroup'. The 'Tables' node under 'medical' is selected. The 'SQLQuery1.sql' editor pane on the right contains the T-SQL code for creating the 'Patients' table:

```
CREATE TABLE [dbo].[Patients](
    [PatientId] [int] IDENTITY(1,1),
    [SSN] [char](11) NOT NULL,
    [FirstName] [nvarchar](50) NULL,
    [LastName] [nvarchar](50) NULL,
    [MiddleName] [nvarchar](50) NULL,
    [StreetAddress] [nvarchar](50) NULL,
    [City] [nvarchar](50) NULL,
    [ZipCode] [char](5) NULL,
    [State] [char](2) NULL,
    [BirthDate] [date] NOT NULL
)
PRIMARY KEY CLUSTERED ([PatientId] ASC) ON [PRIMARY];
```

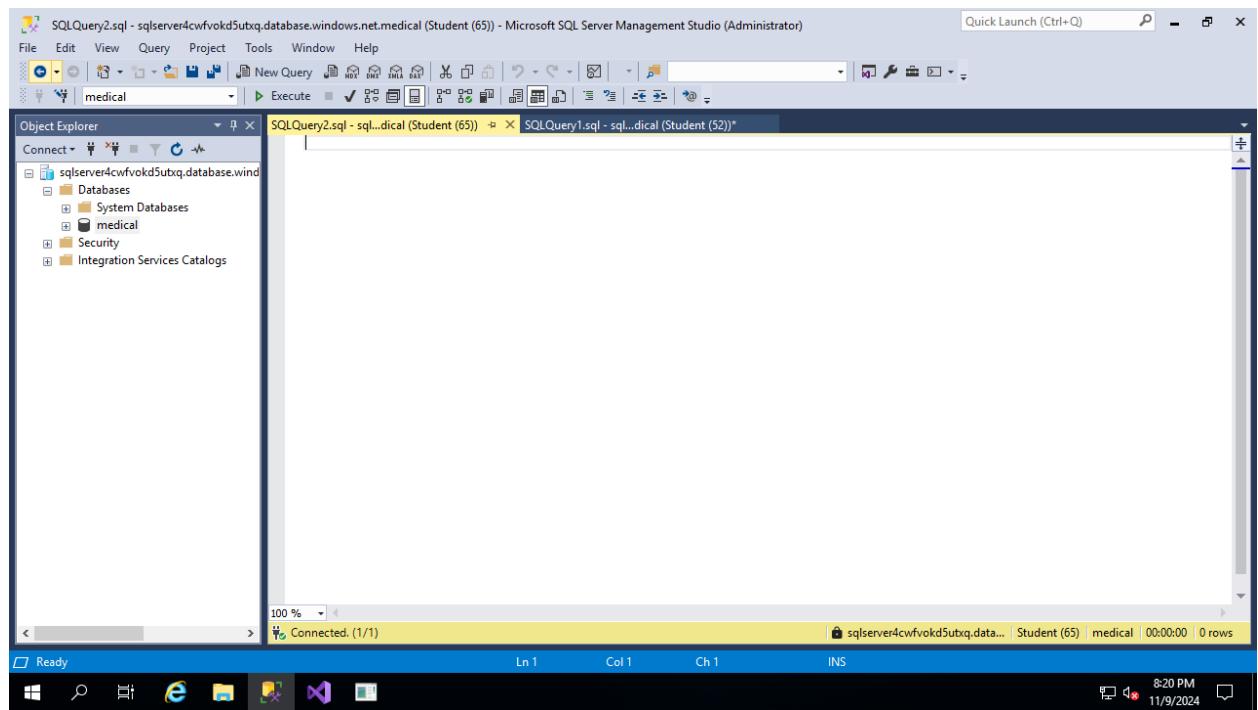
The 'Messages' pane below the editor shows the execution results:

```
Commands completed successfully.  
Completion time: 2024-11-09T16:32:28.2231813+00:00
```

The status bar at the bottom right shows the date and time as '11/9/2024 8:17 PM'.

17. In the **Object Explorer** pane, right-click the **medical database** and, in the right-click menu, click **New Query**

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)



- From the query window, run the following query to verify that the data that loaded into the database from the console app is encrypted.

SELECT FirstName, LastName, SSN, BirthDate FROM Patients;

From the screenshot below we can see that the SSN and birth date are encrypted.

The screenshot shows the Microsoft SQL Server Management Studio (SSMS) interface with the results of the query. The title bar reads "SQLQuery2.sql - sqlserver4cwfvolkd5utbxq.database.windows.net.medical (Student (65)) - Microsoft SQL Server Management Studio (Administrator)". The main pane displays the query "SELECT FirstName, LastName, SSN, BirthDate FROM Patients;". Below the query, the results grid shows five rows of patient data:

	FirstName	LastName	SSN	BirthDate
1	Orlando	Gee	0x0149D9F1D3ED3CD15E5BEE0D498C430404FFBBE67BDCB2...	0x01A83D04AB794D7133F987C09DC8BE35153AEDB54F6FF2...
2	Keith	Haris	0x01AA1A775A806E72CE4678CDE1170CCDD404C37CE0EFC1...	0x01C1FFAF48465E745F2C9F4ACBBB66ED757E328F09220A0...
3	Donna	Cameras	0x019BC37E4EC30E8B340CE10ED121F23A397C31CD05986BD...	0x01072C4FB255E9B06115BAAF7ECE39E3CC64D40A0155833...
4	Janet	Gates	0x011180348AC25B43742588B85C22D88D071BF5906B5A568B...	0x01E6ABCFC76899396E17FCEA0252C98CD34498ECC75D25...
5	Lucy	Harrington	0x01450EFE0E849BB48BAC481D7A1ABC0909E37B8C74F92...	0x0139578BA6381FA8702F9A43A241872F24BD85FF6CE0309...

The status bar at the bottom shows "Query executed successfully.", "ln 1 Col 58 Ch 58 INS", and the date/time "11/9/2024 8:23 PM".

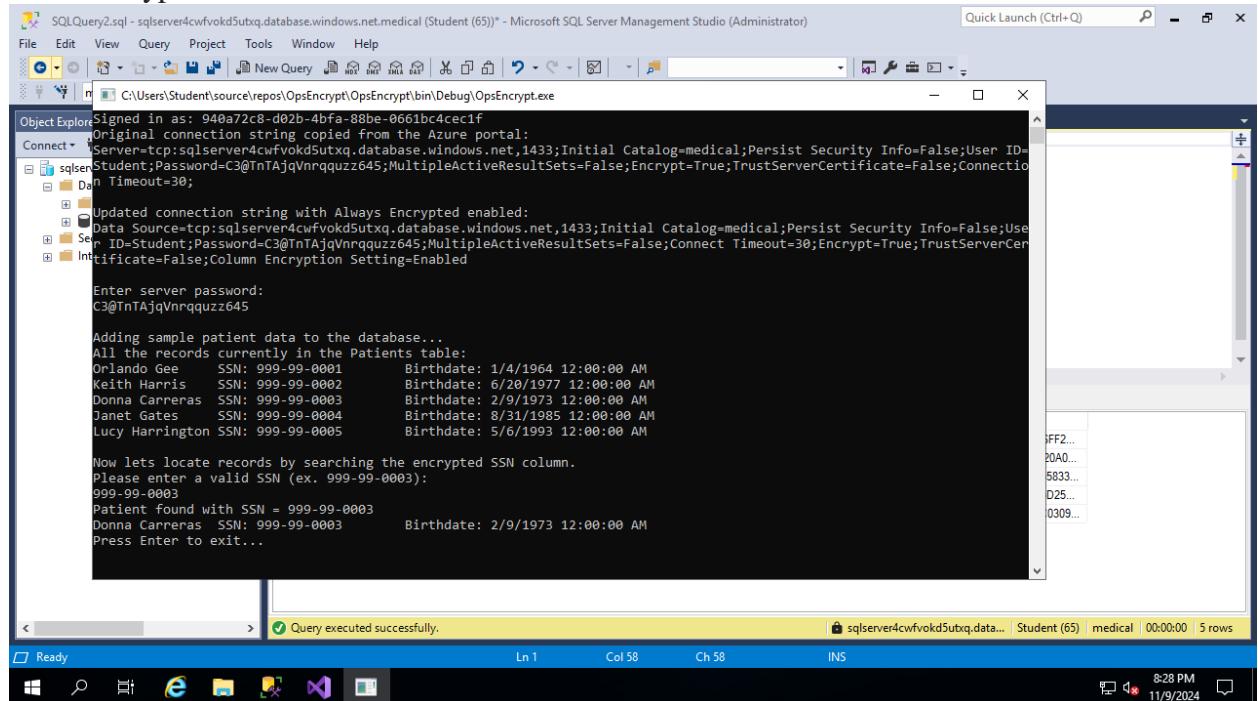
Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

19. Switch back to the console application where you are prompted to enter a valid SSN. This will query the encrypted column for the data. At the Command Prompt, type the following and press the Enter key:

```
999-99-0003
```

Note: Verify that the data returned by the query is not encrypted.

From the screenshot below we can see the data pulled for patient with SSN 999-99-0003 is not encrypted.



The screenshot shows the Microsoft SQL Server Management Studio interface. In the Object Explorer, a connection to 'sqlserver4cwfvoid5utxq.database.windows.net.medical (Student (65))' is selected. A query window titled 'SQLQuery2.sql - sqlserver4cwfvoid5utxq.database.windows.net.medical (Student (65)) - Microsoft SQL Server Management Studio (Administrator)' displays the following output:

```
Signed in as: 940a72c8-d02b-4bfa-88be-0661bc4cec1f
Original connection string copied from the Azure portal:
Server=tcp:sqlserver4cwfvoid5utxq.database.windows.net,1433;Initial Catalog=medical;Persist Security Info=False;User ID=Student;Password=C3@InTAjqVnrqquzz645;MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;
Updated connection string with Always Encrypted enabled:
Data Source=tcp:sqlserver4cwfvoid5utxq.database.windows.net,1433;Initial Catalog=medical;Persist Security Info=False;User ID=Student;Password=C3@InTAjqVnrqquzz645;MultipleActiveResultSets=False;Connect Timeout=30;Encrypt=True;TrustServerCertificate=False;Column Encryption Setting=Enabled
Enter server password:
C3@InTAjqVnrqquzz645

Adding sample patient data to the database...
All the records currently in the Patients table:
Orlando Gee    SSN: 999-99-0001    Birthdate: 1/4/1964 12:00:00 AM
Keith Harris    SSN: 999-99-0002    Birthdate: 6/20/1977 12:00:00 AM
Donna Carreras  SSN: 999-99-0003    Birthdate: 2/9/1973 12:00:00 AM
Janet Gates    SSN: 999-99-0004    Birthdate: 8/31/1985 12:00:00 AM
Lucy Harrington SSN: 999-99-0005    Birthdate: 5/6/1993 12:00:00 AM

Now lets locate records by searching the encrypted SSN column.
Please enter a valid SSN (ex. 999-99-0003):
999-99-0003
Patient Found with SSN = 999-99-0003
Donna Carreras  SSN: 999-99-0003    Birthdate: 2/9/1973 12:00:00 AM
Press Enter to exit...
```

The status bar at the bottom indicates 'Query executed successfully.' and shows the session details: 'sqlserver4cwfvoid5utxq.data... | Student (65) | medical | 00:00:00 | 5 rows'.

20. To terminate the console app, press the Enter key

Press enter to exit

Clean up resources

1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure portal.
2. In the upper-left drop-down menu of the Cloud Shell pane, if needed select **PowerShell** and, when prompted, click **Confirm**.
3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource groups you created in this lab:

```
Remove-AzResourceGroup -Name "AZ500LAB10" -Force –AsJob
```

We have successfully removed the AZ500LAB10 resources as seen below.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

The screenshot shows the Microsoft Azure portal interface. At the top, there are several tabs: 'Your single...', 'CNS3-2024', 'AZ500-Azur...', 'AZ500-Azur...', 'AZ500-Azur...', 'Virtual mach...', and 'Lightshot...'. Below the tabs, the URL is https://portal.azure.com/#browse/Microsoft.Compute%2FVirtualMachines.

The main navigation bar includes 'Microsoft Azure' with an 'Upgrade' button, a search bar 'Search resources, services, and docs (G+)', and various icons for Copilot, AI, and system settings. The user's email 'murugiloise@gmail.com' and 'DEFAULT DIRECTORY (MURUGI...' are also visible.

The page title is 'Virtual machines' with a 'Create' button. Below the title, it says 'Default Directory (murugiloisegmail.onmicrosoft.com)'. There are filters for 'Subscription equals all', 'Type equals all', 'Resource group equals all', 'Location equals all', and an 'Add filter' button. A message 'Showing 1 to 1 of 1 records.' is displayed.

At the bottom of the page, there are buttons for '< Previous', 'Page 1 of 1', and 'Next >'. On the right, there are buttons for 'Give feedback', 'Switch to Bash', 'Restart', 'Manage files', 'New session', 'Editor', 'Web preview', 'Settings', 'Help', and a 'PS /home/loise>' command prompt.

The terminal window shows the command PS /home/loise> Remove-AzResourceGroup -Name "AZ500LAB10" -Force -AsJob. The output table shows one resource group:

ID	Name	PSJobTypeName	State	HasMoreData	Location	Command	
1	Long	Running	0...	AzureLongRunni...	True	localhost	Remove-AzResourceGroup

The terminal window has a dark blue background with white text. The Windows taskbar at the bottom shows the Start button, a search bar with 'Type here to search', and various pinned icons. The system tray shows the date and time as '09/11/24 11:40 PM'.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)

Conclusion

In this exercise, we have deployed an Azure VM and an Azure SQL database setting up Azure subscription 1, with a resource group AZ500LAB10 with West US as the region. We have then created a Key Vault resource in PowerShell then set access policies, then set the key as MyLabKey and add a secret to the Key Vault. We have registered an application sqlApp with an Application ID and secret.

We then logged in to the Azure VM, the deployment we initiated in earlier in the activity. The Azure VM hosts Visual Studio 2019 and SQL Server Management Studio 19 and updated Azure SQL database named medical with a new table structure and selected data columns for encryption. Then set the server firewall with a rule name Allow Mgmt VM with the Public IP Address of the az500-10-vm1. Then Download RDP File and use it to connect to the az500-10-vm1 Azure VM via Remote Desktop.

We then installed Install SQL Server Management Studio on az500-10-vm1. Azure VM where we created Patients table and encrypted columns for dbo.Patients. We then created a Console application using Visual Studio to load data into the encrypted columns and then access that data securely using a connection string that accesses the key in the Key Vault where the SSN and Birthdate were encrypted and from the console when we enter the SSN to query the encrypted column for the data.

Week 9 Assignment 1: Key Vault (Implementing Secure Data by setting up Always Encrypted)