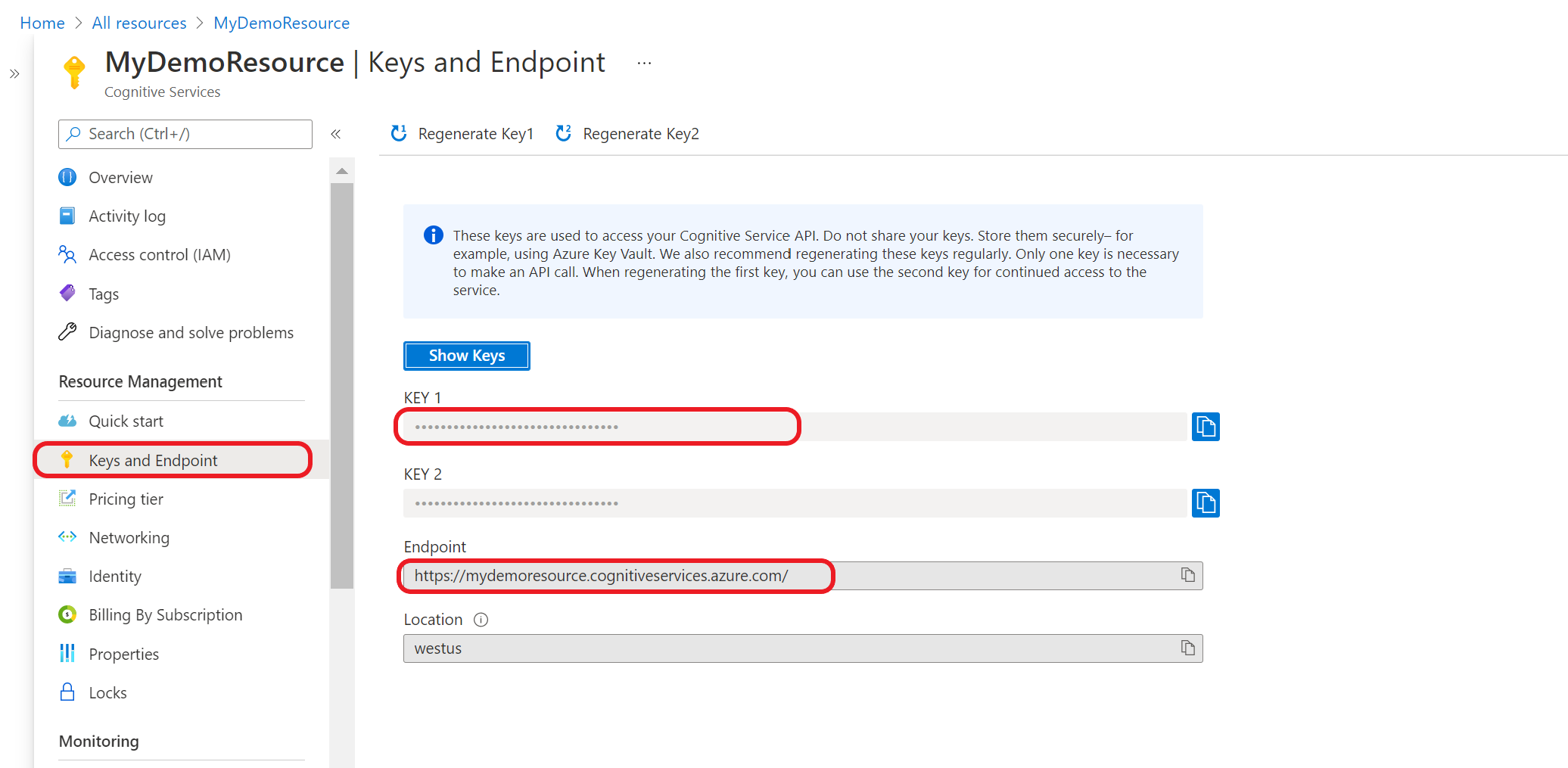
**Protect account keys by using Azure Key Vault**

**Get your credentials from your Azure AI services resource**

Before you add your credential information to your Azure key vault, you need to retrieve them from your Azure AI services resource. For example, if your service needs a key and endpoint, you would find them using the following steps:

1. Navigate to your Azure resource in the [Azure portal](https://portal.azure.com/).
2. From the collapsible menu on the left, select **Keys and Endpoint**.

[](https://learn.microsoft.com/en-us/azure/ai-services/language-service/custom-text-classification/media/get-endpoint-azure.png#lightbox)

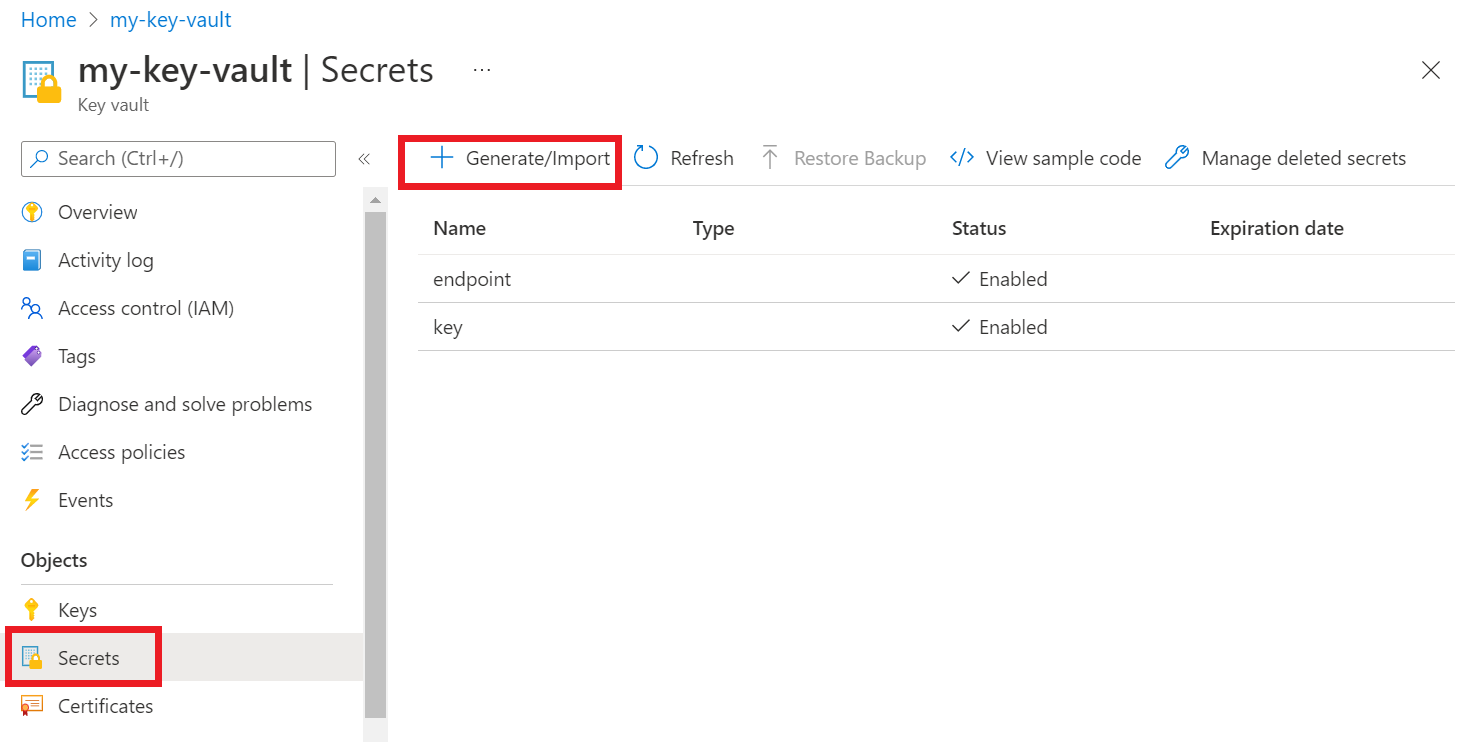
Some Azure AI services require different information to authenticate API calls, such as a key and region. Make sure to retrieve this information before continuing on.

**Add your credentials to your key vault**

For your application to retrieve and use your credentials to authenticate API calls, you will need to add them to your [key vault secrets](https://learn.microsoft.com/en-us/azure/key-vault/secrets/about-secrets).

Repeat these steps to generate a secret for each required resource credential. For example, a key and endpoint. These secret names will be used later to authenticate your application.

1. Open a new browser tab or window. Navigate to your key vault in the [Azure portal](https://portal.azure.com/#create/Microsoft.CognitiveServicesSpeechServices).
2. From the collapsible menu on the left, select **Objects** > **Secrets**.
3. Select **Generate/Import**.

[](https://learn.microsoft.com/en-us/azure/ai-services/media/key-vault/store-secrets.png#lightbox)

1. On the **Create a secret** screen, enter the following values:

A screenshot of a computer

Description automatically generated

1. Leave the other values as their defaults. Select **Create**.

**Grant access to your key vault**

Create an access policy for your key vault that grants secret permissions to your user account.

**Azure CLI**

To set the access policy, run the [az keyvault set-policy](https://learn.microsoft.com/en-us/cli/azure/keyvault#az-keyvault-set-policy) command. Replace Your-Key-Vault-Name with the name of your key vault. Replace user@domain.com with your Microsoft Entra username.

A close-up of a computer code

Description automatically generated A screenshot of a computer error

Description automatically generated

**PowerShell**

To set the access policy, run the [Set-AzKeyVaultAccessPolicy](https://learn.microsoft.com/en-us/powershell/module/az.accounts/set-azcontext) command. Replace Your-Key-Vault-Name with the name of your key vault. Replace user@domain.com with your Microsoft Entra user name.

A close-up of a computer

Description automatically generated A computer screen shot of a message

Description automatically generated

Run the application by selecting the **Debug** button at the top of Visual Studio. Your key and endpoint secrets will be retrieved from your key vault.

A screenshot of a computer program

Description automatically generated