* 5 minutes

In this exercise, you add a password to Azure Key Vault. A password is an example of sensitive information that you need to protect. You then read the password from Azure Key Vault to verify that the password is accessible.

In practice, there are several ways to add secrets to and read secrets from Key Vault. You can use the Azure portal, the Azure CLI, or Azure PowerShell. By using your favorite programming language, your applications can also securely access the secrets that they need.

Here, you create a secret in Key Vault by using the Azure portal. You then access the secret from the portal and from the Azure CLI in Azure Cloud Shell.

The Azure CLI is a way to work with Azure resources from the command line or from scripts. Cloud Shell is a browser-based shell experience to manage and develop Azure resources. Think of Cloud Shell as an interactive console that runs in the cloud.

## Create a key vault

1. Go to the [Azure portal](https://portal.azure.com/learn.docs.microsoft.com).
2. On the Azure portal menu, or from the **Home** page, under **Azure services**, select **Create a resource**. The **Create a resource** pane appears.
3. In the search bar, enter *Key Vault*, and then select **Key Vault** from the results. **The Key Vault** pane appears.
4. Select **Create**. The **Create a key vault** pane appears.
5. On the **Basics** tab, enter the following values for each setting.

* Note
* Replace *NNN* with a series of numbers. This helps ensure that the name of your key vault is unique.
* **Setting**
* **Value**
* **Project details**
* Subscription
* **Concierge Subscription**
* Resource group
* **[sandbox resource group name]**
* **Instance details**
* Key vault name
* **my-keyvault-NNN** where NNN is a unique identifier
* Accept the remaining settings at their default values.

1. Select **Review + create**, and after passing validation, select **Create**.

* Wait for deployment to successfully complete.

1. Select **Go to resource**.
2. Take note of some of the details about your key vault.

* For example, the **Vault URI** field shows the URI that your application can use to access your vault from the REST API.
* Here’s an example for a key vault that’s named **my-keyvault-321**: ![A screenshot of the Azure portal showing details about a key vault. It shows fields such as the parent resource group, location, and DNS name.](data:image/png;base64;base64,)

1. As an optional step, on the left menu pane, under **Settings**, examine some of the other features.

* Although they’re initially empty, here you’ll find places where you can store keys, secrets, and certificates.
* Note
* Your Azure subscription is the only one that’s authorized to access this vault. Under **Settings**, the **Access policies** feature enables you to configure access to the vault.

## Add a password to the key vault

1. On the left menu pane, under **Settings**, select **Secrets**. Your key vault pane appears.
2. From the top menu bar, select **Generate/Import**. The **Create a secret** pane appears.
3. Fill in the following values for each setting.

* **Setting**
* **Value**
* Upload options
* **Manual**
* Name
* **MyPassword**
* Value
* **hVFkk96**
* Accept the remaining settings at their default values. Notice that you can specify properties such as the activation date and the expiration date. You can also disable access to the secret.

1. Select **Create**.

## Show the password

Here, you access the password from Key Vault two times. First, you access it from the Azure portal. Next, you access it from the Azure CLI.

1. From your **Key Vault/Secrets** pane, select **MyPassword**. The **MyPassword/Versions** pane appears. You see that the current version is enabled.
2. Select the current version. The **Secret Version** pane appears.

* Under **Secret Identifier**, you see a URI that you can now use with applications to access the secret. Remember, only authorized applications can access this secret.

1. Select **Show Secret Value**. The unique value for this version of the password appears.

* ![A screenshot of the Azure portal showing the secret value in the key vault.](data:image/png;base64;base64,)
* A screenshot of the Azure portal showing the secret value in the key vault.

1. From Cloud Shell, run this command.

* Note
* Replace **my-keyvault-NNN** with the name you used earlier.
* az keyvault secret show \  
   --name MyPassword \  
   --vault-name my-keyvault-NNN \  
   --query value \  
   --output tsv
* You see the password in the output.
* hVFkk96

Good work! At this point, you have a key vault that contains a password secret that’s securely stored for use with your applications.

## Clean up

The sandbox automatically cleans up your resources when you’re finished with this module.

When you’re working in your own subscription, it’s a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

## Next unit: Host your Azure virtual machines on dedicated physical servers by using Azure Dedicated Host

[Continue](https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/6-host-virtual-machines-dedicated-hosts/)

Need help? See our [troubleshooting guide](https://docs.microsoft.com/en-us/learn/support/troubleshooting?uid=learn.azure.protect-against-security-threats-azure.5-manage-password-key-vault&documentId=d66f2ca6-f024-3f13-4224-3cf198c05680&versionIndependentDocumentId=953ba660-eb66-557a-4fdd-19377ed7b6e9&contentPath=%2FMicrosoftDocs%2Flearn-pr%2Fblob%2Flive%2Flearn-pr%2Fazure-fundamentals%2Fprotect-against-security-threats-azure%2F5-manage-password-key-vault.yml&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Flearn%2Fmodules%2Fprotect-against-security-threats-azure%2F5-manage-password-key-vault&author=rknapp) or provide specific feedback by [reporting an issue](https://docs.microsoft.com/en-us/learn/support/troubleshooting?uid=learn.azure.protect-against-security-threats-azure.5-manage-password-key-vault&documentId=d66f2ca6-f024-3f13-4224-3cf198c05680&versionIndependentDocumentId=953ba660-eb66-557a-4fdd-19377ed7b6e9&contentPath=%2FMicrosoftDocs%2Flearn-pr%2Fblob%2Flive%2Flearn-pr%2Fazure-fundamentals%2Fprotect-against-security-threats-azure%2F5-manage-password-key-vault.yml&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Flearn%2Fmodules%2Fprotect-against-security-threats-azure%2F5-manage-password-key-vault&author=rknapp#report-feedback).