

12 - Implement Azure Key Vault

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

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

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

Setting	Value
Subscription	Use your subscription
Resource group	myRGKV (create new)
Key vault name	keyvaulttestxxx
Location	East US
Pricing tier	Standard

4. Click **Review + create**, and then click **Create**.
5. Once the new key vault is provisioned, click **Go to resource**. Or you can locate your new key vault by searching for it.
6. Click on the key vault **Overview** tab and take note of the **DNS name**. Applications that use your vault through the REST API will need this URI.
7. Take a moment to browse through some of the other key vault options. Under **Settings** review **Keys**, **Secrets**, **Certificates**, **Access Policies**, **Firewalls and virtual networks**.

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

Task 2: Add a secret to the Key Vault

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

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

Setting	Value
Upload options	Manual
Name	ExamplePassword
Value	hVFkk96

3. Click **Create**.

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

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

Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click **Delete resource group**. Verify the name of the resource group and then click **Delete**. Monitor the **Notifications** to see how the delete is proceeding.