Quickstart - Set and retrieve a secret from Azure Key Vault

By msmbaldwin

Archived: 2026-04-06 00:13:02 UTC

In this quickstart, you create a key vault in Azure Key Vault with Azure CLI. Azure Key Vault is a cloud service that works as a secure secrets store. You can securely store keys, passwords, certificates, and other secrets. For more information on Key Vault you may review the Overview. Azure CLI is used to create and manage Azure resources using commands or scripts. Once you've completed that, you will store a secret.

If you don't have an Azure account, create a free account before you begin.

- Use the Bash environment in Azure Cloud Shell. For more information, see Get started with Azure Cloud Shell.

  

- If you prefer to run CLI reference commands locally, install the Azure CLI. If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see How to run the Azure CLI in a Docker container.

  - If you're using a local installation, sign in to the Azure CLI by using the az login command. To finish the authentication process, follow the steps displayed in your terminal. For other sign-in options, see Authenticate to Azure using Azure CLI.

  - When you're prompted, install the Azure CLI extension on first use. For more information about extensions, see Use and manage extensions with the Azure CLI.

  - Run az version to find the version and dependent libraries that are installed. To upgrade to the latest version, run az upgrade.

This quickstart requires version 2.0.4 or later of the Azure CLI. If using Azure Cloud Shell, the latest version is already installed.

A resource group is a logical container into which Azure resources are deployed and managed. Use the az group create command to create a resource group named *myResourceGroup* in the *eastus* location.

```
az group create --name "myResourceGroup" --location "EastUS"
```

Use the Azure CLI az keyvault create command to create a Key Vault in the resource group from the previous step. You will need to provide some information:

- Key vault name: A string of 3 to 24 characters that can contain only numbers (0-9), letters (a-z, A-Z), and hyphens (-)

  Important

  Each key vault must have a unique name. Replace `<vault-name>` with the name of your key vault in the following examples.

- Resource group name: **myResourceGroup**
- The location: **EastUS**

```
az keyvault create --name "<vault-name>" --resource-group "myResourceGroup" --enable-rbac-authorization true
```

The output of this command shows properties of the newly created key vault. Take note of these two properties:

- **Vault Name**: The name you provided to the `--name` parameter.
- **Vault URI**: In this example, the vault URI is `https://<vault-name>.vault.azure.net/`. Applications that use your vault through its REST API must use this URI.

To gain permissions to your key vault through Role-Based Access Control (RBAC), assign a role to your "User Principal Name" (UPN) using the Azure CLI command az role assignment create.

```
az role assignment create --role "Key Vault Secrets Officer" --assignee "<upn>" --scope "/subscriptions/<subscr
```

Replace `<upn>`, `<subscription-id>`, and `<vault-name>` with your actual values. If you used a different resource group name, replace "myResourceGroup" as well. Your UPN will typically be in the format of an email address (e.g., username@domain.com).

To add a secret to the vault, you just need to take a couple of additional steps. This password could be used by an application. The password will be called **ExamplePassword** and will store the value of **hVFkk965BuUv** in it.

Use the Azure CLI az keyvault secret set command below to create a secret in Key Vault called **ExamplePassword** that will store the value **hVFkk965BuUv** :

```
az keyvault secret set --vault-name "<vault-name>" --name "ExamplePassword" --value "hVFkk965BuUv"
```

You can now reference this password that you added to Azure Key Vault by using its URI. Use `https://<vault-name>.vault.azure.net/secrets/ExamplePassword` to get the current version.

To view the value contained in the secret as plain text, use the Azure CLI az keyvault secret show command:

```
az keyvault secret show --name "ExamplePassword" --vault-name "<vault-name>" --query "value"
```

Now, you have created a Key Vault, stored a secret, and retrieved it.

Other quickstarts and tutorials in this collection build upon this quickstart. If you plan to continue on to work with subsequent quickstarts and tutorials, you may wish to leave these resources in place.

When no longer needed, you can use the Azure CLI az group delete command to remove the resource group and all related resources:

```
az group delete --name "myResourceGroup"
```

In this quickstart you created a Key Vault and stored a secret in it. To learn more about Key Vault and how to integrate it with your applications, continue on to the articles below.

- Read an Overview of Azure Key Vault
- Learn how to store multiline secrets in Key Vault
- See the reference for the Azure CLI az keyvault commands
- Review the Key Vault security overview
- Review secrets-specific security best practices
