

Create Password secret with Azure Key Vault

Use Case:

In this walkthrough task 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.

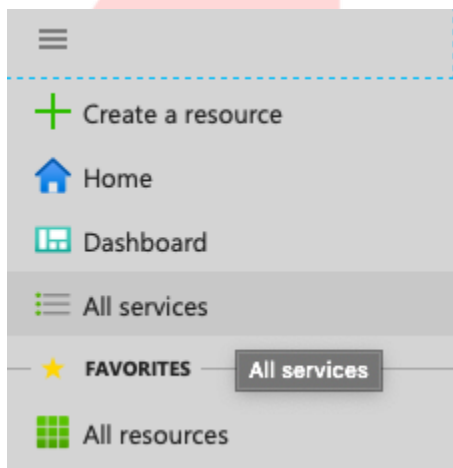
Prerequisites:

You require need an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the [Create your Azure free account today](#) webpage.

Steps:

Create a vault in Azure Key Vault

1. Sign into the Azure Portal and go to All services > Security and then select Key vaults.



2. In the Key vaults pane click on Create key vault.

All services

Overview

Categories

- All
- General
- Compute
- Networking
- Storage
- Web
- Mobile
- Containers
- Databases
- Analytics
- Blockchain
- AI + machine learning
- Internet of things
- Mixed reality
- Integration
- Identity
- Security
- DevOps
- Migrate
- Monitor
- Management + governance

SECURITY (9)

- Security Center
- Application Gateways
- Virtual network gateways
- Application security groups

Key vaults

Key vaults

+ Create View

Free training from Microsoft [See all](#)

Secure your cloud data

6 units • 6 hr 45

Azure was designed for security and compliance. Learn how to leverage the built-in services to store your app data securely to ensure that only authorized services and clients have access to it.

[Start](#)

Top 5 security items to consider before pushing to production

6 units • 45 min

Secure your web applications on Azure and protect your apps against the most common and dangerous web application attacks.

[Start](#)

Security, responsibility and trust in Azure

13 units • 1 hr 3 min

Discuss the basic concepts for protecting your infrastructure and data when you work in the cloud. Understand what responsibilities are yours and what Azure takes care of for you.

[Start](#)

Create key vault

3. In the **Create key vault** blade, enter the details as below and click **Create**

- **Name:** a name for your vault i.e. **akvtest1**
- **Subscription:** < your subscription >
- **Resource Group:** select **Create new** and enter a new resource group name i.e. **akvrg**
- **Location:** < a Datacenter location near you i.e. **Central US** >
- **Pricing Tier:** Standard

Create key vault

[Basics](#) [Access policy](#) [Virtual network](#) [Tags](#) [Review + create](#)

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance. [Learn more](#)

Project details

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

Subscription *

Visual Studio Enterprise – MPN

Resource group *

(New) akvrg

[Create new](#)

Instance details

Key vault name * ⓘ

az900test1

Region *

Central US

Pricing tier * ⓘ

Standard

[Review + create](#)

[< Previous](#)

[Next : Access policy >](#)

- **Pricing Tier:** Standard
- **Access policies:** < accept default value i.e. **1 principal selected** >

Basics

Access policy

Virtual network

Tags

Review + create

Enable Access to:

☐

 Azure Virtual Machines for deployment ⓘ

☐

 Azure Resource Manager for template deployment ⓘ

☐

 Azure Disk Encryption for volume encryption ⓘ

+ Add Access Policy

Current Access Policies

Name	Category	Email	Key Permissions	Secret Permissions	Certificate Permissions	Action
USER						
 Abdul Rasheed Feroz Khan	USER	feroz@codesizzler.info	9 selected	7 selected	15 selected	Delete

Review + create

< Previous

Next : Virtual network >

- **Virtual Network Access:** < accept default value i.e. **all networks can access** >

Basics Access policy **Virtual network** Tags Review + create

Allow access from:

☒ All networks ☐ Selected networks

i All networks, including the internet, can access this key vault. [Learn More](#)

Review + create

< Previous

Next : Tags >

Click on create button.

Create key vault

✓ Validation passed

[Basics](#) [Access policy](#) [Virtual network](#) [Tags](#) [Review + create](#)

Basics

Subscription	Visual Studio Enterprise – MPN
Resource group	akvrg
Key vault name	az900test1
Region	Central US
Pricing tier	Standard

Access policy

Azure Virtual Machines for deployment	Not Enabled
Azure Resource Manager for template deployment	Not Enabled
Azure Disk Encryption for volume encryption	Not Enabled
Access policies	1

Virtual network

Allow access from:	All networks
--------------------	--------------

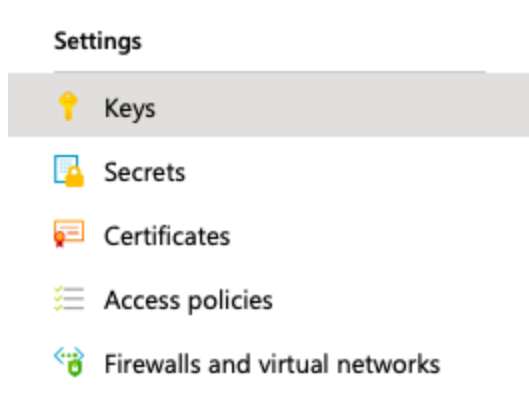
Create

< Previous

Next >

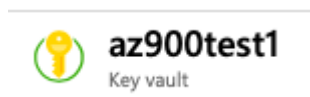
[Download a template for automation](#)

4. Go to the newly created Key vault and verify it is present. You can take a moment to browse through some of the options available within it, primarily under Settings and then options concerning Keys, Secrets, Certificates, Access Policies, Firewalls and virtual networks.



5. Take note of two values in the key vault

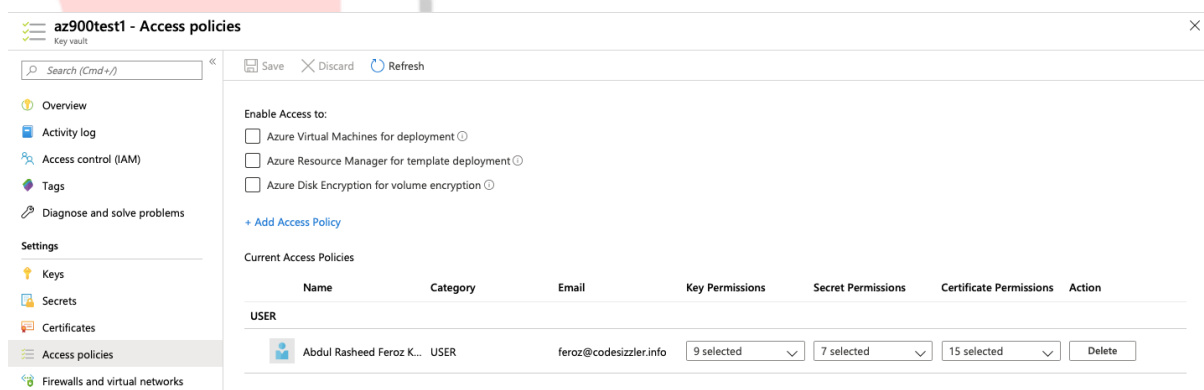
- **Vault Name:** In the example it is **akvtest1**



- **DNS name** (also sometimes referred to as the **Vault URI**): In this example it is `https://akvtest1.vault.azure.net/`. Applications that use your vault through its REST API must use this URI.

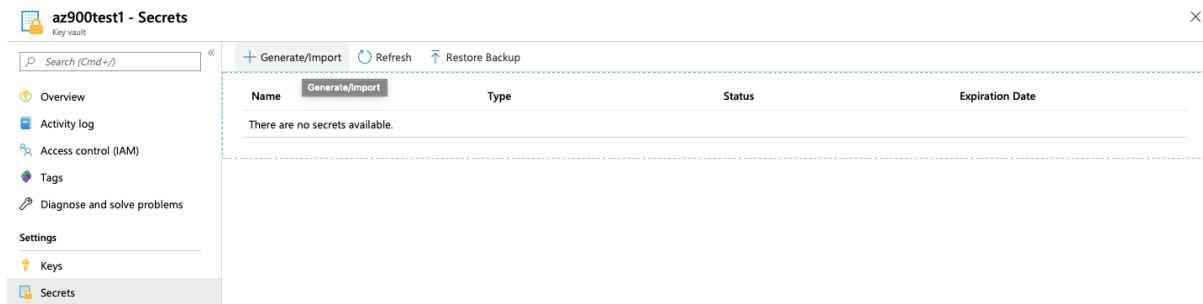
DNS Name : `https://az900test1.vault.azure.net/`

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 > Access policies** section.



Add a secret to the Key Vault

1. On the Key Vault properties pages select **Secrets**, then select **Generate/Import**.



2. On the Create a secret blade enter the below values, leave the other values at their defaults and then click Create.

- **Upload options:** Manual
- **Name:** ExamplePassword
- **Value:** hVFkk965BuUv96!



Create a secret

Upload options

Manual

Name *

ExamplePassword

Value *

.....

Content type (optional)

Set activation date? ☐

Set expiration date? ☐

Enabled?

Yes

No

Create

- Once the secret has been successfully created, on the **Secrets** pane, click on the **ExamplePassword**, and note it has a status of **Enabled**

Name	Type	Status	Expiration Date
ExamplePassword		✓ Enabled	

4. Double click on the password and in the password pane, note the presence of the **Secret Identifier**. This is the url value that you can now use with applications. It provides a centrally managed and securely stored password for use with applications.

Version	Status	Activation Date	Expiration Date
CURRENT VERSION			
5d785bcd0647e48b2e9a2ecb0b6d00	✓ Enabled		



5d785bcd0647e48b2e9a2ecb0b6d00

Secret Version



Save



Discard

Properties

Created 10/29/2019, 11:47:07 AM

Updated 10/29/2019, 11:47:07 AM

Secret Identifier

https://az900test1.vault.azure.net/secrets/ExamplePasswor...



Copy to clipboard

Settings

Set activation date? ⓘ ☐

Set expiration date? ⓘ ☐

Enabled?

Yes

No

Tags

0 tags



Secret

Content type (optional)

Show Secret Value

.....



5. In the same pane click the button **Show Secret Value**, to display the password you specified earlier.

Note: It is also possible to set time limitations on when a password is available for use, using the activation and expiration date settings.

Hide Secret Value

hVFkk965BuUv96!

Copy to clipboard

