

How to create Azure Key Vault with Azure SDK for .NET

<https://github.com/Azure/azure-sdk-for-net/tree/main/sdk/keyvault/Azure.Security.KeyVault.Secrets>

<https://github.com/Azure/azure-sdk-for-net/tree/main/sdk/keyvault/Azure.Security.KeyVault.Secrets/samples>

1. Cretate an Azure KeyVault

Login in Azure portal and navigate into the KeyVault service.

Create a new KeyVault pressing the "Create key vault" button

portal.azure.com/#view/HubsExtension/BrowseResource/resourceType/Microsoft.KeyVault%2Fvaults

Microsoft Azure

Search resources, services, and docs (G+)

Home >

Key vaults


particular (luiscocoenriquez@hotmail.onmicrosoft.com)

+ Create Manage deleted vaults Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 0 to 0 of 0 records.

Name ↑↓	Type ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓	Tags
---------	---------	-------------------	-------------	-----------------	------





No key vaults to display












Safeguard cryptographic keys and other secrets used by cloud apps and services.

[Create key vault](#)

[Learn more](#)

 Create a resource Home Dashboard All services

★ FAVORITES

 All resources Resource groups Quickstart Center App Services Function App SQL databases Azure Cosmos DB Virtual machines Load balancers Storage accounts Virtual networks Microsoft Entra ID Monitor Advisor[Home](#) > [Key vaults](#) >

Create a key vault

Basics[Access configuration](#)[Networking](#)[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.

Project details

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

Subscription *

Azure subscription 1

Resource group *

(New) my_VaultRG

[Create new](#)

Instance details

Key vault name * ⓘ

myNewVault2000 ✓

[Previous](#)[Next](#)[Review + create](#)

Microsoft Azure

+

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

Quickstart Center

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Microsoft Entra ID

Monitor

Advisor

Home > Key vaults >

Create a key vault

Key vault name * ⓘ

Region *

Pricing tier * ⓘ

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft-delete ⓘ

Enabled

Days to retain deleted vaults * ⓘ

Purge protection ⓘ

☒ Disable purge protection (allow key vault and objects to be purged during retention period)

☐ Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

Previous

Next

Review + create

IMPORTANT NOTE: pay attention go to the "Access configuration" tab, and select the option "Azure role-based access control (recommended)"

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Key vaults >

Create a key vault

Basics **Access configuration** Networking Tags Review + create

Configure data plane access for this key vault

To access a key vault in data plane, all callers (users or applications) must have proper authentication and authorization. Authentication establishes the identity of the caller. Authorization determines which operations the caller can execute. [Learn more](#)

Permission model

Grant data plane access by using a [Azure RBAC](#) or [Key Vault access policy](#)

☒ Azure role-based access control (recommended) ⓘ

☐ Vault access policy ⓘ

Resource access

☐ Azure Virtual Machines for deployment ⓘ

☐ Azure Resource Manager for template deployment ⓘ

☐ Azure Disk Encryption for volume encryption ⓘ

[Previous](#) [Next](#) [Review + create](#)

[Give feedback](#)

2. Grant permission to the KeyVault ResourceGroup to

Navigate to the Azure ResourceGroup where the Azure KeyVault was created

Microsoft Azure

Search resources, services, and docs (G+/)

Home >

Resource groups

particular (luiscocoenriquezhotmail.onmicrosoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Location equals all Add filter

Showing 1 to 1 of 1 records.

Name ↑↓	Subscription ↑↓	Location ↑↓
my_VaultRG	Azure subscription 1	West Europe

Grant permission to the ResourceGroup as KeyVault Administrator

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Resource groups > my_VaultRG

Resource groups

particular (luiscocoenriquezhotmail.onmicrosoft.c...)

+ Create Manage view ...

Filter for any field...

Name ↑↓

my_VaultRG

my_VaultRG | Access control (IAM)

Resource group

Search

+ Add Download role assignments Edit columns Refresh Remove Feedback

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Deployment stacks

Policies

Properties

Locks

Cost Management

Check access

Role assignments

Roles

Deny assignments

Classic administrators

My access

View my level of access to this resource.

View my access

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Check access

Grant access to this resource

Grant access to resources by assigning a role. [Learn more](#)

Add role assignment

View access to this resource

View the role assignments that grant access to this and other resources. [Learn more](#)

View

Microsoft Azure

Search resources, services, and docs (G+)

Home > Resource groups > my_VaultRG

Microsoft Azure

Search resources, services, and docs (G+)

Home > Resource groups > myVaultRG | Access control (IAM) >

Add role assignment

Role Members Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Assignment type

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

key Type: All Category: All

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Classic Storage Account Key Operator Serv...	Classic Storage Account Key Operators are allowed to list and regenerate keys on Classic Storage Accounts	BuiltInRole	Storage	View
Cognitive Services Contributor	Lets you create, read, update, delete and manage keys of Cognitive Services.	BuiltInRole	AI + Machine Learning	View
Cognitive Services User	Lets you read and list keys of Cognitive Services.	BuiltInRole	AI + Machine Learning	View
Cosmos DB Operator	Lets you manage Azure Cosmos DB accounts, but not access data in them. Prevents access to account keys an...	BuiltInRole	Databases	View
Key Vault Administrator	Perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secrets. C...	BuiltInRole	Security	View
Key Vault Certificates Officer	Perform any action on the certificates of a key vault, except manage permissions. Only works for key vaults th...	BuiltInRole	Security	View
Key Vault Contributor	Lets you manage key vaults, but not access to them.	BuiltInRole	Security	View
Key Vault Crypto Officer	Perform any action on the keys of a key vault, except manage permissions. Only works for key vaults that use ...	BuiltInRole	Security	View
Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap operations. Only works for key vaults that use the 'Azure rol...	BuiltInRole	Security	View

Microsoft Azure

Search resources, services, and docs (G+)

Home > Resource groups > my_VaultRG | Access control (IAM) >

Add role assignment

Role **Members** Review + assign

Selected role Key Vault Administrator

Assign access to ☒ User, group, or service principal ☐ Managed identity

Members [+ Select members](#)

Name	Object ID	Type
No members selected		

Description Optional

Review + assign Previous Next

Select members

Select ⓘ

Search by name or email address

No users, groups, or service principals found.

Selected members:

LC	luis coco enriquez luiscoenriquez_hotmail.com#EXT#...	Remove
----	--	------------------------

Select Close

Microsoft Azure

Search resources, services, and docs (G+)

luiscoenriquez@hotmail...
PARTICULAR (LUISCOCENRIQU...)

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

Quickstart Center

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Microsoft Entra ID

Monitor

Advisor

Microsoft Defender for

Home > Resource groups > my_VaultRG | Access control (IAM) >

Add role assignment

Role **Members** Review + assign

Selected role

Key Vault Administrator

Assign access to

☒ User, group, or service principal
☐ Managed identity

Members

+ Select members

Name	Object ID	Type	
luis coco enriquez	40520058-0714-4e1f-a880-5f33776e5efe	User	

Description

Optional

Review + assign

Previous

Next

Feedback

Microsoft Azure

Search resources, services, and docs (G+)

Home > Resource groups > my_VaultRG | Access control (IAM) >

Add role assignment

Role Members Review + assign

Role Key Vault Administrator

Scope /subscriptions/846901e6-da09-45c8-98ca-7cca2353ff0e/resourceGroups/my_VaultRG

Members

Name	Object ID	Type
luis coco enriquez	40520058-0714-4e1f-a880-5f33776e5efe	User

Description No description

Review + assign Previous Next

Feedback

3. Input the C# console application source code

```
using Azure.Identity;
using Azure.Security.KeyVault.Secrets;

// Create a secret client using the DefaultAzureCredential
var client = new SecretClient(new Uri("https://myNewVault2000.vault.azure.net/"), new DefaultAzureCredential());

try
{
    KeyVaultSecret secret = client.SetSecret("mysecret1", "LuisCoco123456789");
}
```

```
// Retrieve a secret using the secret client.  
secret = client.GetSecret("mysecret1");  
Console.WriteLine(secret.Value);  
}  
catch (AuthenticationFailedException e)  
{  
    Console.WriteLine($"Authentication Failed. {e.Message}");  
}
```