

Custom Azure RBAC Role for Key Vault Secrets Access

Assign precise read-only access to
secrets in Azure Key Vault using
custom roles

#PerparimLabs #AzureSecurity #EntraRBAC



Why Create a Custom Role for Azure Key Vault?

- **Built-in roles** like ***Reader*** or ***Contributor*** may grant more permissions than needed
- Custom roles allow precise control — e.g., **read-only access to secrets**
- Helps enforce **least privilege** and **segregation of duties**
- Applies across **RBAC-supported scopes** (subscription, resource group, or vault level)

Create a Custom Role for Azure Key Vault

#AzureRBAC #CustomRole #KeyVaultAccess

Microsoft Azure

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

Home > Azure subscription 1 | Access control (IAM) >

Create a custom role

Basics Permissions Assignable scopes JSON Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

Custom role name *

Description

Baseline permissions ☐ Clone a role ☒ Start from scratch ☐ Start from JSON

- Navigate to **Subscriptions** > select your subscription
- Go to **Access Control (IAM)** > click **+ Add** → **Add Custom Role**
- Choose **Start from scratch** and give your role a name (e.g., "Key Vault Secrets Reader - Custom")
- Optionally, add a **description** for clarity

Microsoft Azure

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

Copilot

Home > Azure subscription 1 | Access control (IAM) >

Create a custom role

BasicsPermissionsAssignable scopesJSONReview + create

+ Add permissions+ Exclude permissions

Click Add permissions to select the permissions you want to add to this custom role.

To add a wildcard (*) permission, you must manually add the permission on the JSON tab. [Learn more](#)

To exclude specific permissions from a wildcard permission, click Exclude permissions. [Learn more](#)

Permission	Description	Permission type
Microsoft.KeyVault/vaults/read	View the properties of a key vault	Action
Microsoft.KeyVault/vaults/write	Creates a new key vault or updates the properties of an existing key vault. ...	Action
Microsoft.KeyVault/vaults/delete	Deletes a key vault	Action
Microsoft.KeyVault/vaults/secrets/read	View the properties of a secret, but not its value.	Action
Microsoft.KeyVault/vaults/secrets/write	Creates a new secret or updates the value of an existing secret.	Action

Definitions

Control plane

Actions specify the operations that a role is allowed to perform. NotActions specify the operations that are excluded from the allowed Actions (this is useful if a role has wildcards).

Data plane

DataActions specify the operations that a role is allowed to perform to the data within an object. NotDataActions specify the operations that are excluded from the allowed DataActions (this is useful if a role has wildcards).

Wildcards (*)

A wildcard (*) extends a permission to everything that matches the string you provide. To add a wildcard permission, use the JSON tab.

Define Permissions for the Custom Role

- In the **Permissions** tab, click **+ Add permissions**
- Use the search bar to find:
 - Microsoft.KeyVault/vaults/* – full Key Vault permissions
 - Or specific actions like secrets/read, secrets/list
- Select only the permissions your role requires
- Click **Add** to confirm selection

#LeastPrivilege #CustomRBAC #AzureKeyVault

Create a New Azure Key Vault

- Go to **portal.azure.com**
- Search for **Key Vaults** in the top search bar
- Click **+ Create**
- Fill in:
 - **Resource Group:** (e.g., KeyVaultDemo-RG)
 - **Key Vault Name:** (e.g., MyCustomKV)
 - **Region:** East US or your preferred one
 - **Pricing Tier:** Standard (or Premium if needed)
- **Access Configuration:** Choose **Azure Role-Based Access Control (RBAC)**
- Click **Review + Create** → **Create**



Choosing Azure Role-Based Access Control lets us use the custom role we created earlier.

Microsoft Azure

[Home](#) > [Key vaults](#) >

Create a key vault ...

Basics Access configuration Networking Tags Review + create

[View Automation Template](#)

Basics

Subscription	Azure subscription 1
Resource group	KeyVaultDemo-RG
Key vault name	MyCustomKV
Region	East US
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

Access configuration

Azure Virtual Machines for deployment	Disabled
Azure Resource Manager for template deployment	Disabled
Azure Disk Encryption for volume encryption	Disabled
Permission model	Azure role-based access control

Networking

Connectivity method	Public endpoint (all networks)
---------------------	--------------------------------

Previous

Next

Create

Assign Custom Role to a User via IAM

- Go to the **Key Vault** you just created
- On the left blade, click **Access control (IAM)**
- Click **+ Add** → **Add role assignment**
- In the Role dropdown, search and select your **custom role** (e.g., Key Vault Secrets Reader - Custom)
- Click **Next**
- Under Members, choose a **User, Group, or Service Principal**
- Select the member and click **Next** → **Review + assign**

Microsoft Azure

Home > MyCustomKV | Access control (IAM) >

Add role assignment

Role

Members

Conditions

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](#)

Job function roles

Privileged administrator roles

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

Search by role name, description, permission, or ID

Type : AllCategory : All

Name	Description	Type	Category	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
App Compliance Automation Administrator	Allows managing App Compliance Automation tool for Microsoft 365	BuiltInRole	None	View
App Compliance Automation Reader	Allows read-only access to App Compliance Automation tool for Microsoft 365	BuiltInRole	None	View
Azure AI Administrator	A Built-In Role that has all control plane permissions to work with Azure AI and its dependencies.	BuiltInRole	None	View
Azure AI Enterprise Network Connection Approver	Can approve private endpoint connections to Azure AI common dependency resources	BuiltInRole	None	View
Desktop Virtualization Virtual Machine Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to create, delete, update, start, and stop virtual machi...	BuiltInRole	None	View
Key Vault Administrator	Perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secrets. Cannot manage key vault resources or manage role assign...	BuiltInRole	Security	View
Key Vault Certificate User	Read certificate contents. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltInRole	None	View
Key Vault Certificates Officer	Perform any action on the certificates of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based access control' permission m...	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 the 'Azure role-based access control' permission model.	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 role-based access control' permission model.	BuiltInRole	Security	View
Key Vault Crypto Service Release User	Release keys. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltInRole	None	View
Key Vault Crypto User	Perform cryptographic operations using keys. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltInRole	Security	View
Key Vault Data Access Administrator	Manage access to Azure Key Vault by adding or removing role assignments for the Key Vault Administrator, Key Vault Certificates Officer, Key Vault Crypto Officer, Key ...	BuiltInRole	None	View
Key Vault Reader	Read metadata of key vaults and its certificates, keys, and secrets. Cannot read sensitive values such as secret contents or key material. Only works for key vaults that u...	BuiltInRole	Security	View
Key Vault Secrets Officer	Perform any action on the secrets of a key vault, except manage permissions. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltInRole	Security	View
Key Vault Secrets Reader - Custom	Allows users to manage specific Key Vault secrets and certificates without full administrative access. This custom role is scoped to least-privilege actions needed for sec...	CustomRole	None	View

Microsoft Azure

Home > MyCustomKV | Access control (IAM) >

Add role assignment

Role

Members

Conditions

Review + assign

Selected role

Key Vault Secrets Reader - Custom

Assign access to

☒ User, group, or service principal

☐ Managed identity

Members

+ Select members

Name

Perparim Abdullahu

Description

Optional

Review + assign

Previous

Next

#RoleAssignment #AzureSecurity #IAMControl

Microsoft Azure

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

Copilot

Home > MyCustomKV

MyCustomKV | Access control (IAM) ☆ ...

Key vault

Search

+ Add ▾ ▾ Download role assignments ▾ Edit columns ↻ Refresh | 🗑 Delete | 🗨 Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Access policies

Resource visualizer

Events

Objects

Settings

Monitoring

Automation

Help

⚠ Action required: 1 user has elevated access in your tenant. You should take immediate action and remove all role assignments with elevated access. [View role assignments](#)

Check access Role assignments Roles Deny assignments Classic administrators



Number of role assignments for this subscription ⓘ

3 4000

Search by name or email

Type : All Role : All Scope : All scopes Group by : Role


All (4) Job function roles (1) Privileged administrator roles (3)

<input type="checkbox"/> Name ↑↓	Type ↑↓	Role ↑↓	Scope ↑↓	Condition ↑↓
<input checked="" type="checkbox"/> Key Vault Secrets Reader - Custom (1)				
<input type="checkbox"/>  Perparim Abdullahu PerparimAbdullahu@PerparimSC300lab.onmicr...	User	Key Vault Secrets Reader - Custom	 This resource	None






Showing 1 - 1 of 1 results.

Confirm Custom Role Assignment

- Go back to the **Key Vault** → **Access control (IAM)**
- Click **Role assignments** tab
- Confirm that the **custom role** is assigned to your user
- Click your user to view **permissions inherited from the custom role**
- Optional: Try accessing Key Vault items (e.g., Secrets) to test the effective permission
- If your role included secrets/list, confirm visibility
- If secrets/get, confirm value access

 Use “*Check access*” if you want to *validate permissions for a specific user.*

Key Takeaways from the Lab

-  Created a **custom Azure RBAC role** for granular Key Vault access
-  Selected only required permissions (e.g., secrets/list, secrets/get) — following **least privilege** principle
-  Assigned the role at the **Key Vault scope** via IAM blade
-  Verified access by confirming role assignment and testing access
-  This setup mirrors real-world scenarios where teams need **controlled access to secrets** without granting full admin rights

