Azure Keyvault

gollnickdata.de

Key Vault

Advantages of using key vault

- Central management of secrets
- Increased security
- Developers do not have direct access to production keys
- Access control – who can access what
- Logging and control – accesses to key vault are logged

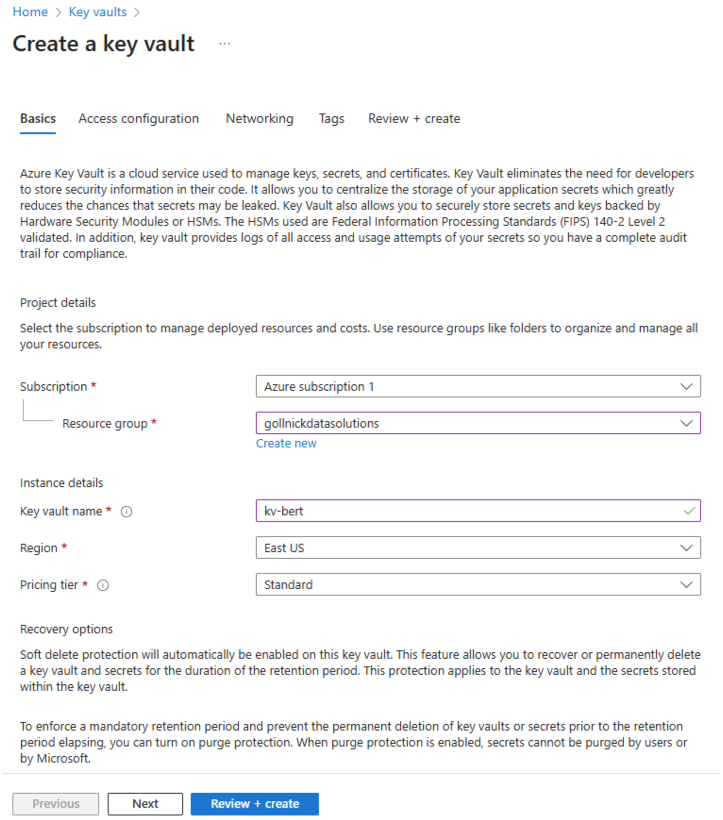
Key Vault

Management of Keys

1. Create Key Vault
2. Create a secret
3. Create service principal
4. Create Service Principal (App Registration in Entra ID)
5. Allow key vault access to Service Principal
6. Set secret permissions in key vault

Key Vault

Create a new Key Vault



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 * : gollnickdatasolutions

Create new

Instance details

Key vault name * ⓘ : kv-bert ✓

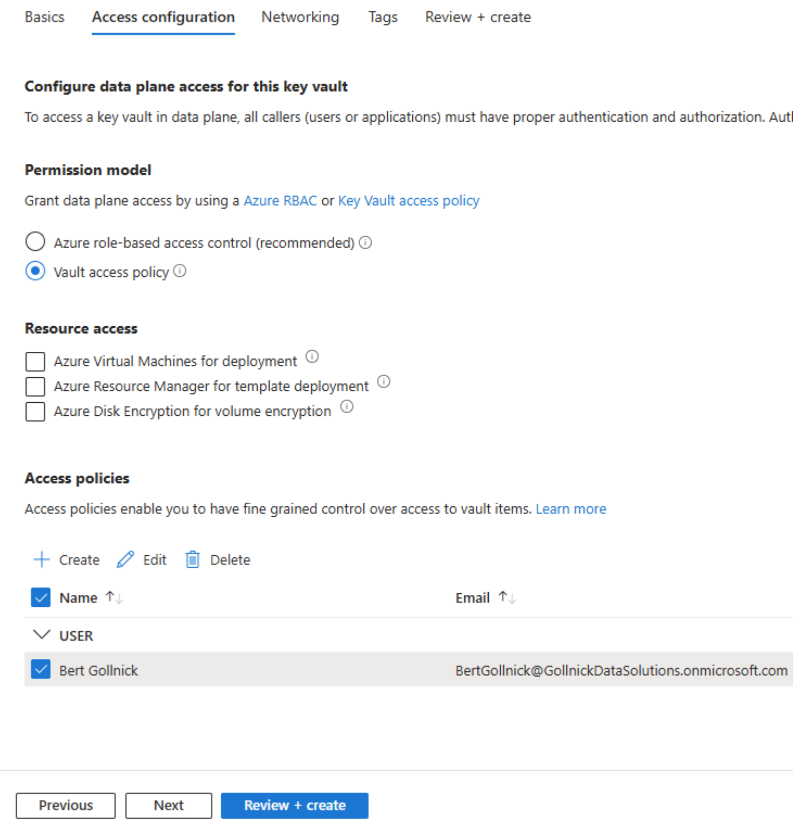
Region * : East US

Pricing tier * ⓘ : Standard

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.



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. Autl

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 ⓘ

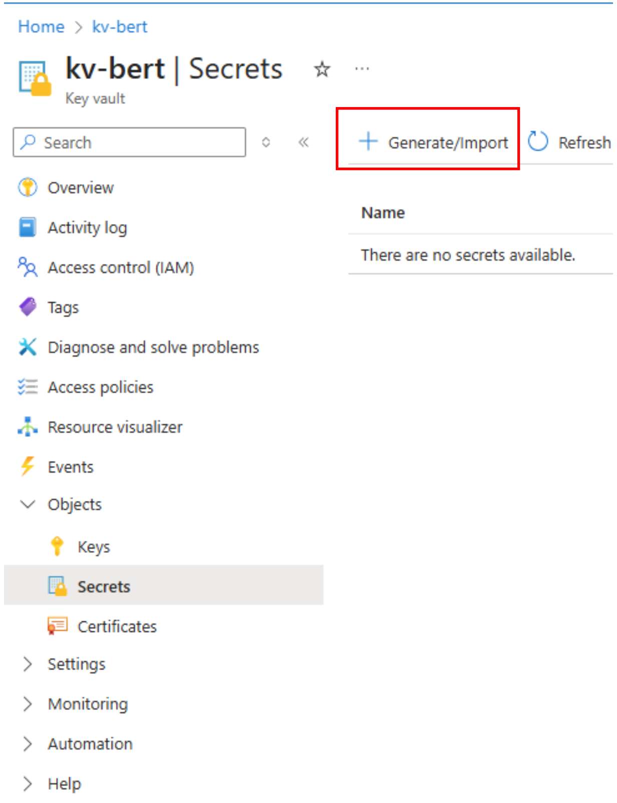
Access policies

Access policies enable you to have fine grained control over access to vault items. Learn more

☑ Name ↑↓	Email ↑↓
USER	
☑ Bert Gollnick	BertGollnick@GollnickDataSolutions.onmicrosoft.com

Key Vault

Create Secrets

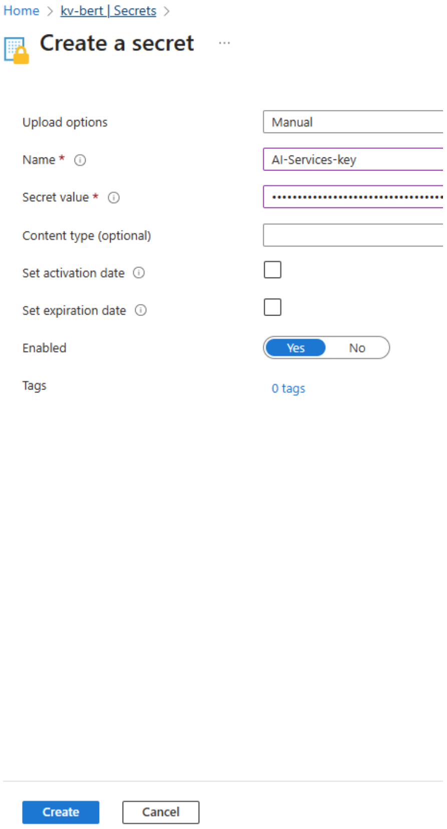


Home > kv-bert

kv-bert | Secrets ☆ ···

Key vault

Name
There are no secrets available.



Home > kv-bert | Secrets >

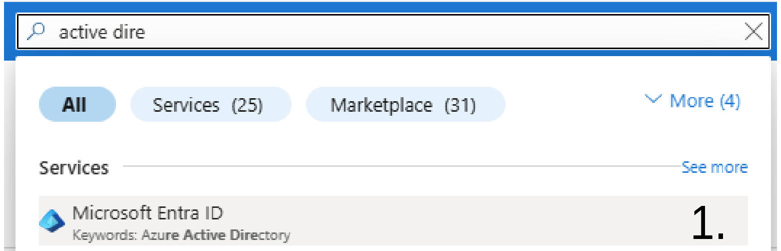
Create a secret ···

Upload options	Manual
Name *	AI-Services-key
Secret value *	••••••••••••••••••••••••••••••••••
Content type (optional)	
Set activation date	□
Set expiration date	□
Enabled	[✓ Yes] No
Tags	0 tags

← Copied from AI Services

Key Vault

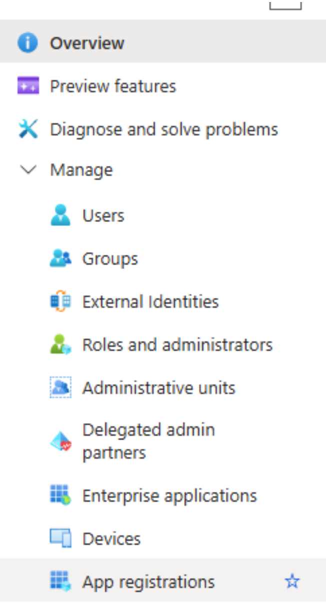
App Registration



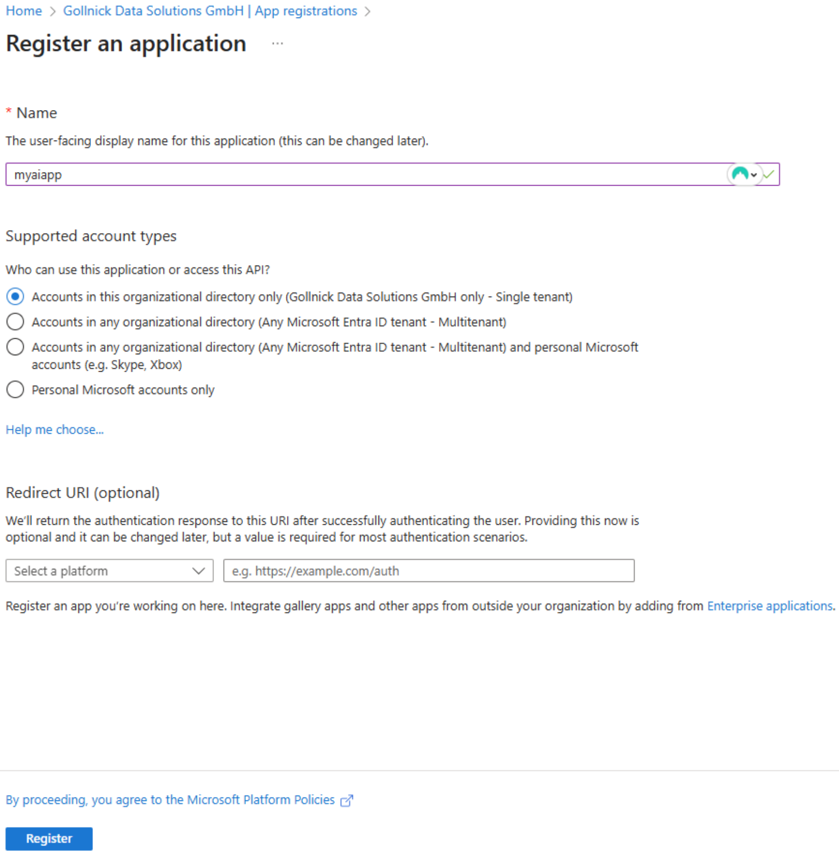
active dire

1.

2.



3.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

myaiapp

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Gollnick Data Solutions GmbH only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

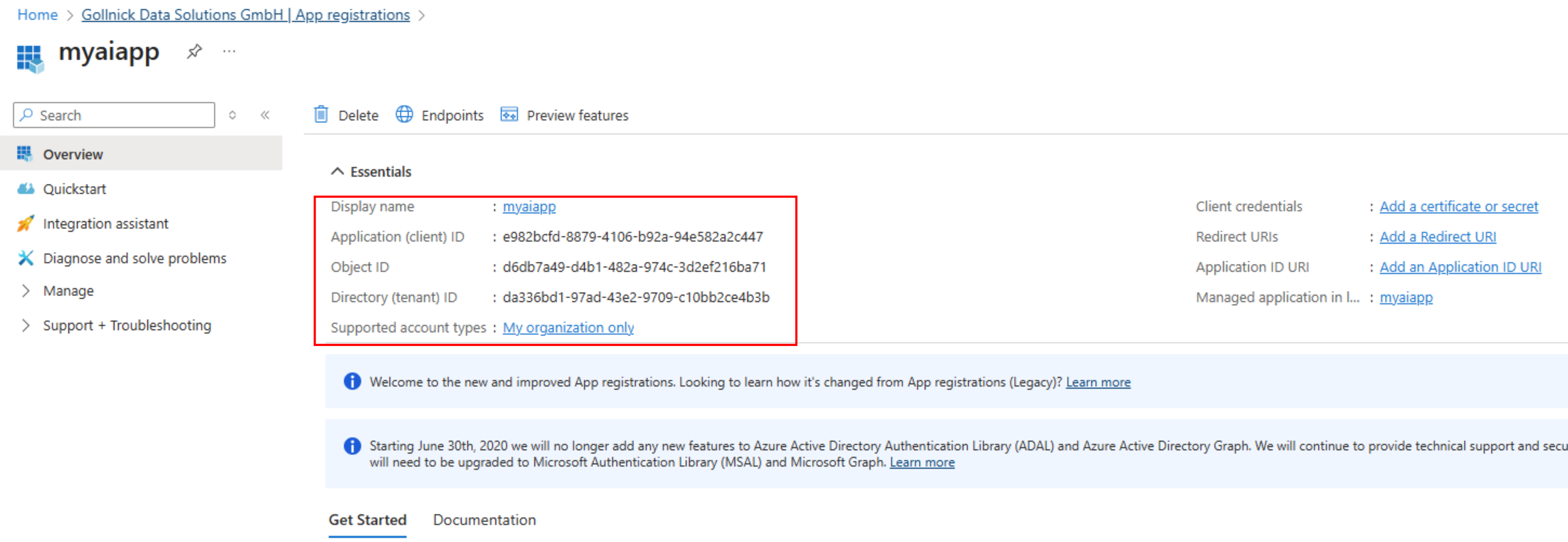
Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

Key Vault

App Registration



Home > Gollnick Data Solutions GmbH | App registrations >

myaiapp

Essentials

Display name	: myaiapp
Application (client) ID	: e982bcfd-8879-4106-b92a-94e582a2c447
Object ID	: d6db7a49-d4b1-482a-974c-3d2ef216ba71
Directory (tenant) ID	: da336bd1-97ad-43e2-9709-c10bb2ce4b3b
Supported account types	: My organization only

Client credentials	: Add a certificate or secret
Redirect URIs	: Add a Redirect URI
Application ID URI	: Add an Application ID URI
Managed application in l...	: myaiapp

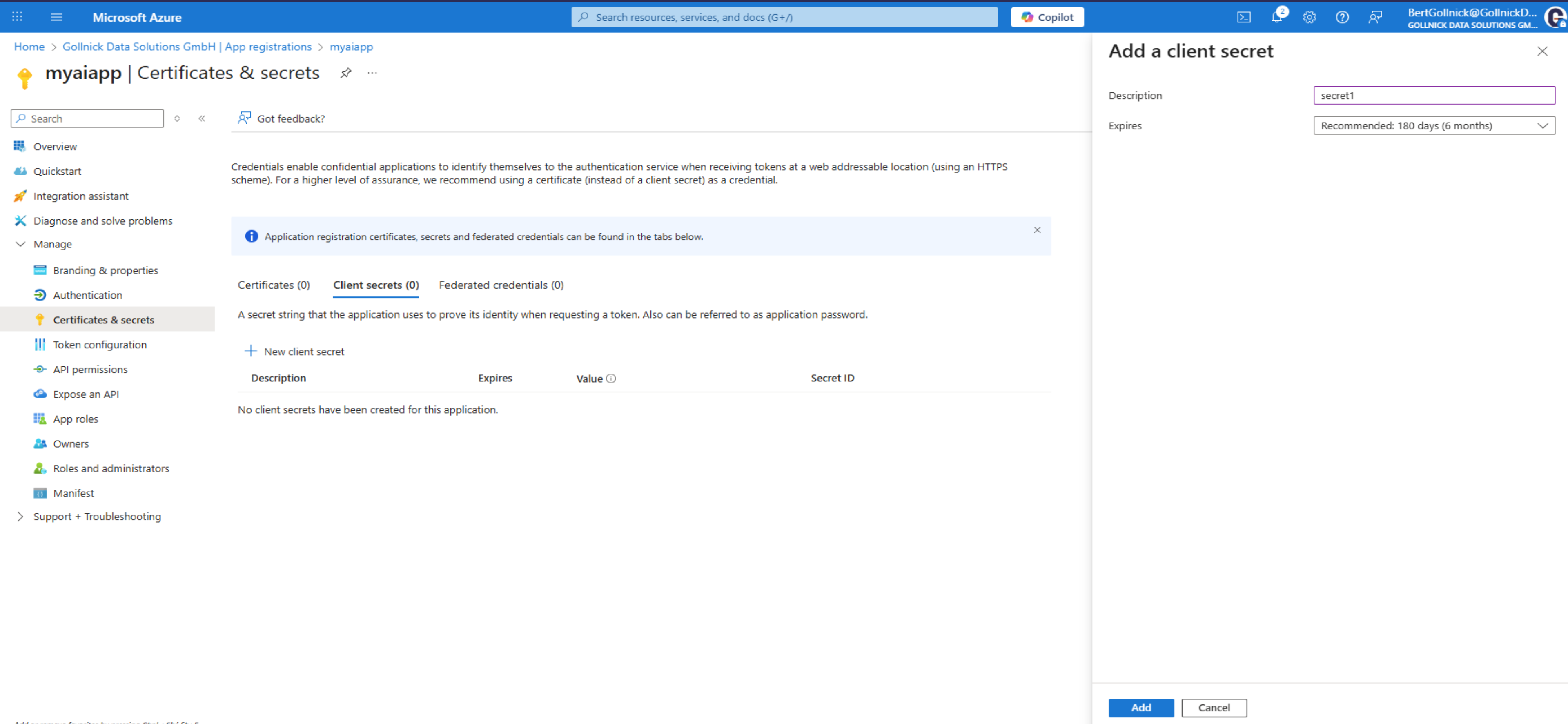
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and secu will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

gollnickdata.de

Key Vault

Create Secrets



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

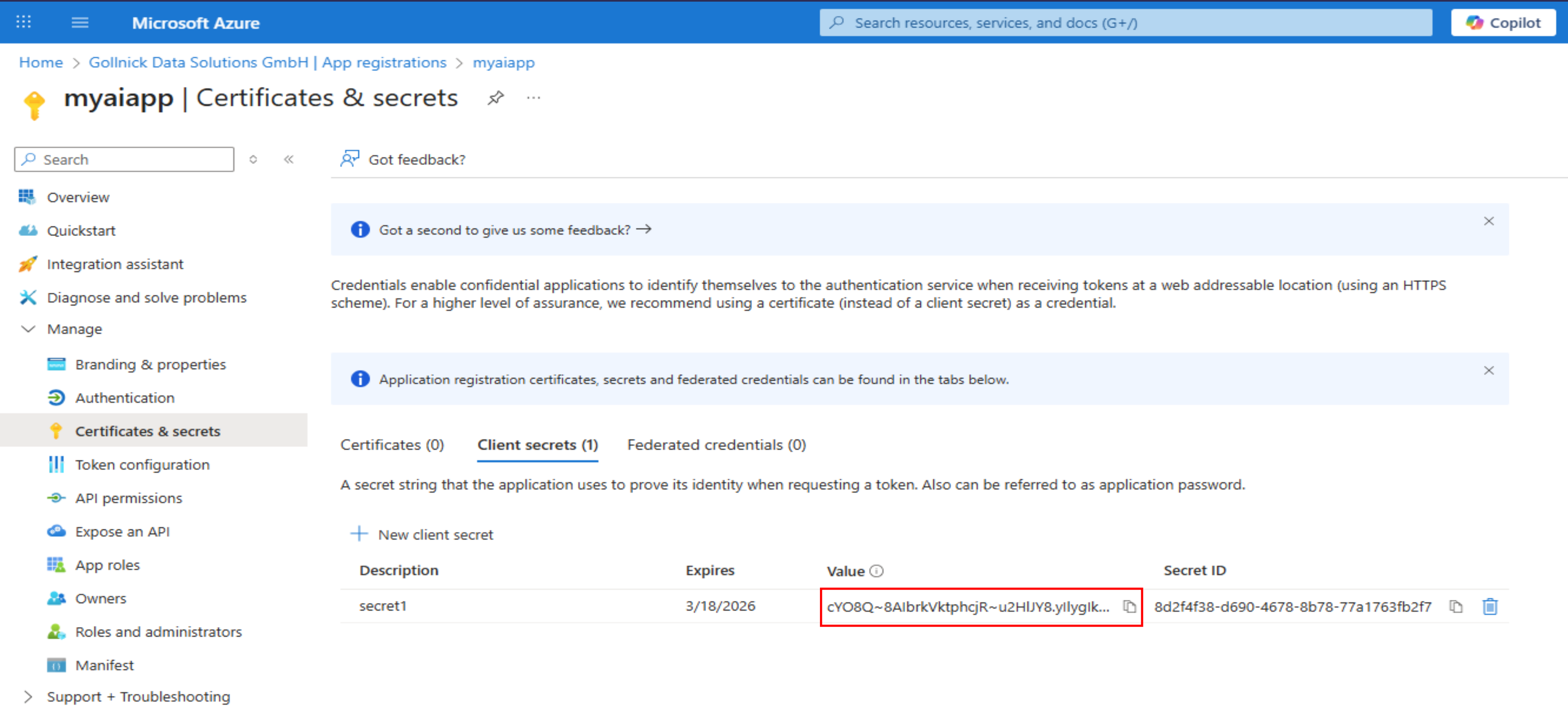
No client secrets have been created for this application.

Add a client secret

Description	secret1
Expires	Recommended: 180 days (6 months)

Key Vault

Create Secrets


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Gollnick Data Solutions GmbH | App registrations > myaiapp

myaiapp | Certificates & secrets

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

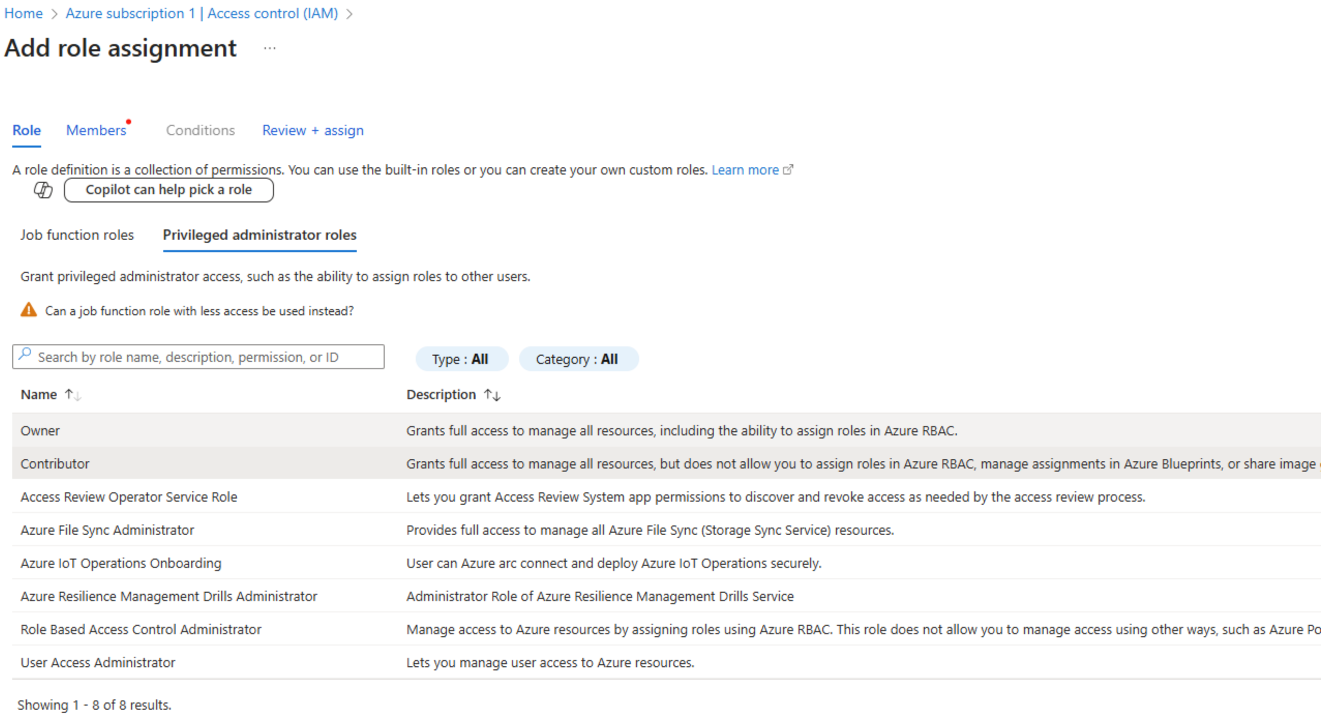
Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value ⓘ	Secret ID
secret1	3/18/2026	cYO8Q~8AIbrkVktphcjR~u2HlJY8.yIlygIk...	8d2f4f38-d690-4678-8b78-77a1763fb2f7

Key Vault

IAM



Home > Azure subscription 1 | 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

Copilot can help pick a role
Job function roles
Privileged administrator roles

Grant privileged administrator access, such as the ability to assign roles to other users.

⚠ Can a job function role with less access be used instead?

Search by role name, description, permission, or ID
Type : All
Category : All

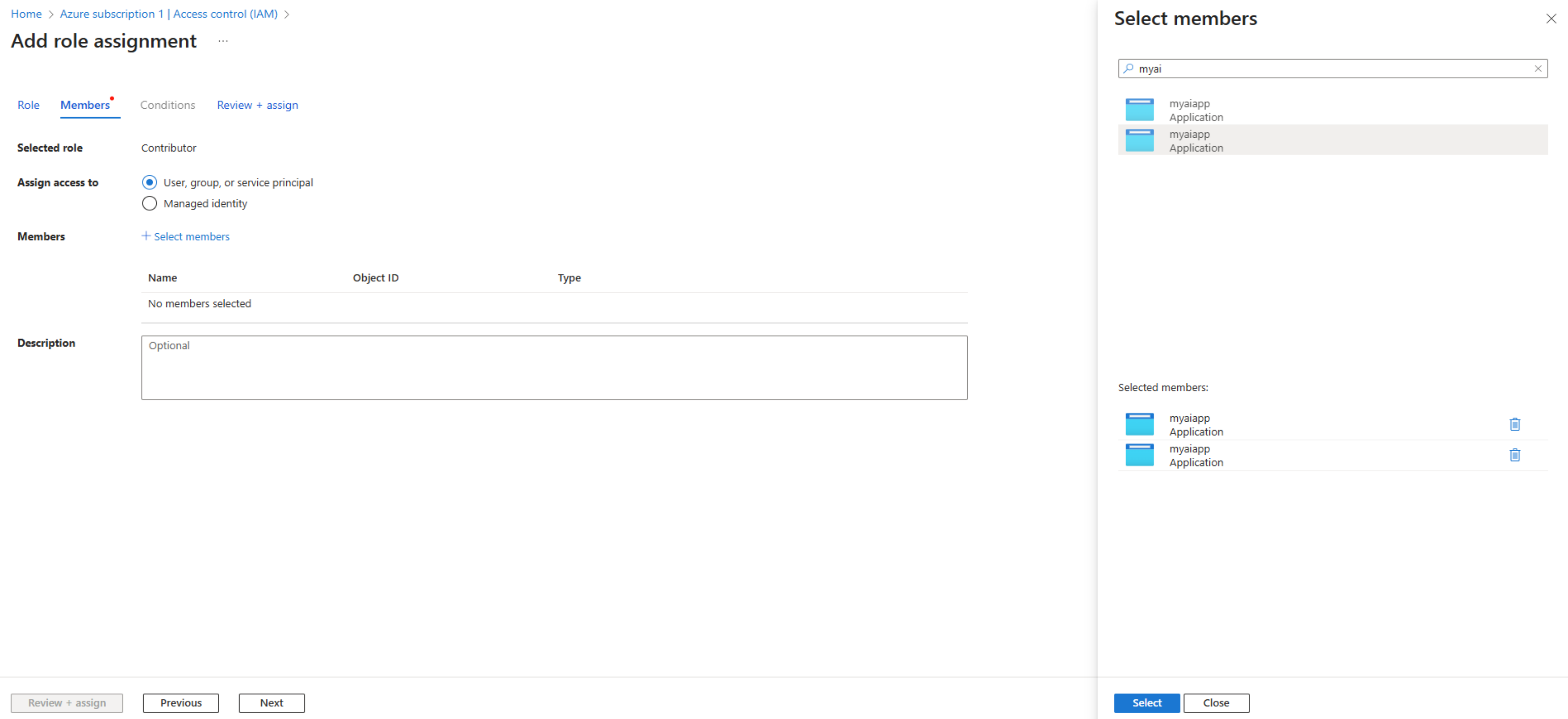
Name ↑↓	Description ↑↓
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed by the access review process.
Azure File Sync Administrator	Provides full access to manage all Azure File Sync (Storage Sync Service) resources.
Azure IoT Operations Onboarding	User can Azure arc connect and deploy Azure IoT Operations securely.
Azure Resilience Management Drills Administrator	Administrator Role of Azure Resilience Management Drills Service
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using other ways, such as Azure Po
User Access Administrator	Lets you manage user access to Azure resources.

Showing 1 - 8 of 8 results.

Add contributor role

Key Vault

Create Secrets



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

Add role assignment ...

Role | Members | Conditions | Review + assign

Selected role Contributor

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

myai

myaiapp
Application

myaiapp
Application

Selected members:

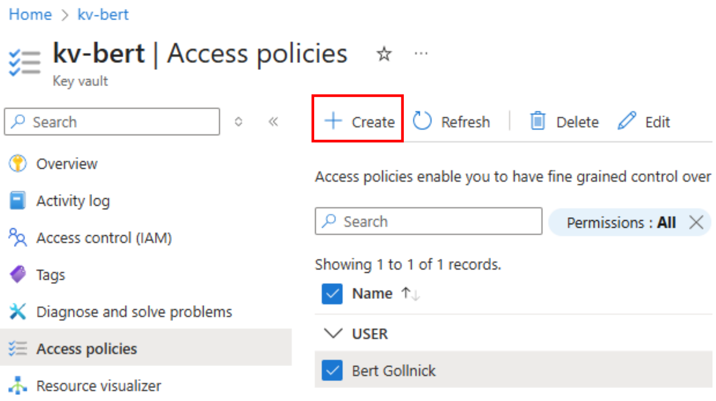
myaiapp
Application

myaiapp
Application

Select | Close

Key Vault

Set Permission in Key Vault



Home > kv-bert

kv-bert | Access policies ☆ ···

Key vault

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- **Access policies**
- Resource visualizer

+ Create | Refresh | Delete | Edit

Access policies enable you to have fine grained control over

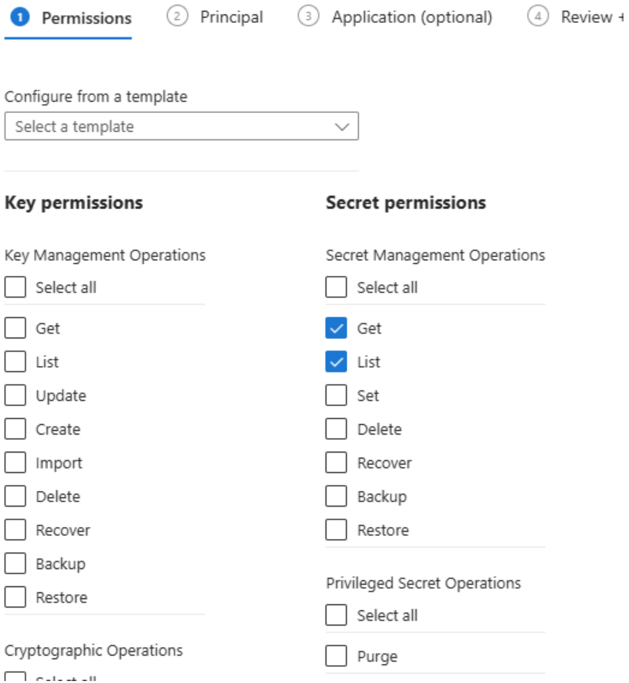
Search | Permissions : **All** ✕

Showing 1 to 1 of 1 records.

☑ **Name** ↑↓

USER

☑ Bert Gollnick



❶ **Permissions** | ② Principal | ③ Application (optional) | ④ Review +

Configure from a template

Select a template

Key permissions

Key Management Operations

☐ Select all

☐ Get
☐ List
☐ Update
☐ Create
☐ Import
☐ Delete
☐ Recover
☐ Backup
☐ Restore

Cryptographic Operations

☐ Select all

Secret permissions

Secret Management Operations

☐ Select all

☑ Get
☑ List
☐ Set
☐ Delete
☐ Recover
☐ Backup
☐ Restore

Privileged Secret Operations

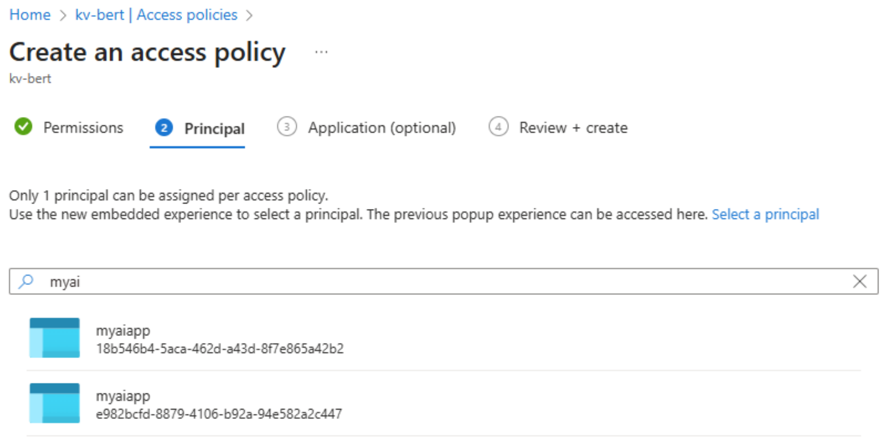
☐ Select all

☐ Purge

gollnickdata.de

Key Vault

Set Permission in Key Vault



Create an access policy

kv-bert

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. Select a principal

myai

myaiapp
18b546b4-5aca-462d-a43d-8f7e865a42b2

myaiapp
e982bcfd-8879-4106-b92a-94e582a2c447