Assuming...

A function app is set up

Go to FunctionApp > Identity > System assigned = On

Now your FunctionApp is visible in the Key Vault for when you want to attach an Access Policy to the FunctionApp.

| FunctionAppNam | e Identity ☆ … |
|--------------------------------|--|
| ✓ Search « | System assigned User assigned |
| ♦ Overview | A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this rest |
| Activity log | to store any credentials in code. |
| Access control (IAM) | 🔚 Save 🗙 Discard 🜔 Refresh 🤌 Troubleshoot 🔗 Got feedback? |
| 🗳 Tags | |
| Diagnose and solve problems | Status 🕕 |
| Ø Microsoft Defender for Cloud | Off On |
| 🗲 Events (preview) | Object (principal) ID 🕕 |
| Functions | Object ID |
| 📍 App keys | Permissions ① |
| 💀 App files | Azure role assignments |
| ➔ Proxies | |
| Deployment | This resource is registered with Microsoft Entra ID. The managed identity can be configured to allow access |
| 🖶 Deployment slots | |
| 💗 Deployment Center | |
| Settings | |
| - Configuration | |
| Authentication | |
| Application Insights | |
| 🚷 Identity | |
| | |

Create a Key Vault 1

- 1. Select appropriate subscription and resource group.
- 2. Give the Key vault a name and select the appropriate settings for your use case.

| Create a key vault | |
|---|--|
| | |
| Project details | |
| Select the subscription to manage deploy your resources. | ed resources and costs. Use resource groups like folders to organize and manage all |
| Subscription * | ~ · |
| Resource group * | \checkmark |
| | Create new |
| Instance details | |
| Key vault name * 🕕 | |
| Region * | West Europe |
| Pricing tier * ① | Standard \checkmark |
| Recovery options Soft delete protection will automatically b a key vault and secrets for the duration of within the key vault. | e enabled on this key vault. This feature allows you to recover or permanently delete the retention period. This protection applies to the key vault and the secrets stored |
| To enforce a mandatory retention period period elapsing, you can turn on purge pr by Microsoft. | and prevent the permanent deletion of key vaults or secrets prior to the retention otection. When purge protection is enabled, secrets cannot be purged by users or |
| Soft-delete 🕕 | Enabled |
| Days to retain deleted vaults * 🛈 | 7 |
| Purge protection ① | 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) |

Create an Access Policy (create a Key Vault 2)

- 1. We will use "Vault access policy" as a permission model for our specific use case.
- 2. Create an Access Policy with "Get" and "List" for secret permissions.
- 3. Assign the principal (in our case, the FunctionApp). It should pop up in the tab "Principal" now that we have turned the system assigned managed identity on.
- 4. Create the Access Policy.

| Create a key vault | | | |
|--|---|---|--|
| | Create an access policy | | |
| Basics Access configuration Networking Tags Review + create | | | |
| | O Permissions (2) Principal | ③ Application (optional) ④ 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. | Configure from a template | | |
| n state and t | Select a template | \sim | |
| Fremission model | | | |
| Azure role-based access control (recommended) | Key permissions | Secret permissions | |
| Vault access policy ① | Key Management Operations | Secret Management Operations | |
| Resource access Azure Virtual Machines for deployment Azure Resource Manager for template deployment Azure Disk Encryption for volume encryption Azure Disk Encryption for volume encryption Access policies Access policies enable you to have fine grained control over access to vault items. Learn more + Create | Get Uist Update Create Import Delete | Select all Get Uist Set Delete Recover Backup | |

Other settings & creating the secret (create a Key Vault 2)

- 1. For our specific use case I will leave all other settings on the subsequent tabs as default. Your requirements may vary.
- 2. Create a secret in the Key Vault.

Linking to Key Vault Secret in FunctionApp environment variables (Application settings)

Refer to the secret in one of two ways

1. With this method it takes some time before changes in the secret are synchronised in Azure Functions.

| FunctionAppName Configur | ration 🛧 … | | | |
|--|---|-------------------------|--|--|
| P Search ≪ Č Refresh ⊟ Save X D | Discard 🗢 Leave Feedback | Add/Edit application s | etting | |
| Overview Application settings Function | ion runtime settings General | Name | accounts | |
| Access control (IAM) Application settings | | Value | @Microsoft.KeyVault(VaultName=yourvaultname:SecretName=yoursecretname) | |
| Tags Application settings are encryp Diagnose and solve problems application at runtime. Learn m | ted at rest and transmitted over a ore | Deployment slot setting | | |
| Microsoft Defender for Cloud + New application setting | Show values Advanced | | | |
| Fevents (preview) Filter application settings | | | | |
| Punctions App keys Name | | | | |
| App files accounts | | | | |
| Proxies APPLICATIONINSIGHTS_CONNEC | TION_STRING | | | |
| Deployment AzureStorageAccountName AzureStorageAccountName | | | | |
| Deployment slots AzureWebJobsFeatureFlags | | | | |
| AzureWebJobsStorage | _ | | | |
| ConnectionStringBlob | N | | | |
| Authentication FUNCTIONS_EXTENSION_VERSIO FUNCTIONS_WORKER_RUNTIME | | | | |

2. With this method changes in the secret are recognized immediately.

| | ame ∣Configuration ☆ … | | | |
|---|--|-------------------------|---|--|
| ₽ Search « | 🖔 Refresh 🗟 Save 🗙 Discard 🗢 Leave Feedback | Add/Edit application | setting | |
| Overview Activity log | Application settings Function runtime settings General | Name | accounts | |
| Access control (IAM) | Application settings | Value | @Microsoft.KeyVault(SecretUri=SecretIdentifier) | |
| Tags Diagnose and solve problems | Application settings are encrypted at rest and transmitted over a application at runtime. Learn more | Deployment slot setting | | |
| Microsoft Defender for Cloud | + New application setting 🗢 Show values 🖉 Advanced | | | |
| Events (preview) | ☑ Filter application settings | | | |
| Functions | | | | |
| 📍 App keys | Name | | | |
| Magazine App files | accounts | | | |
| - Proxies | APPLICATIONINSIGHTS_CONNECTION_STRING | | | |
| Deployment | AzureBlobContainerName | | | |
| Deployment clots | AzureStorageAccountName | | | |
| | AzureWebJobsFeatureFlags | | | |
| Deployment Center | AzureWebJobsStorage | | | |
| Settings | ConnectionStringBlob | | | |
| Configuration | FUNCTIONS_EXTENSION_VERSION | | | |
| Authentication | FUNCTIONS_WORKER_RUNTIME | | | |
| | | | | |

Retrieving the secret in your script through the set environment variable

You can retrieve the values in this environment variable (named 'accounts' in this specific case) by using the Python code below:

os.environ.get('accounts')