Microsoft Azure Setup for Certificate and Key Discovery

This document outlines how to prepare Microsoft Azure so the discovery extension can enumerate certificates and keys, how to create the read only credentials it needs, and how to enter those credentials into the discovery configuration. Steps are given for both the Azure Portal and the Azure CLI.

The discovery reads cryptographic material from across your Azure estate:

- Azure Key Vault: keys (RSA, ECDSA, AES) and certificates with full X.509 metadata and CA hierarchy
- Azure Managed HSM: the extended Key Vault key inventory held in validated HSM hardware
- App Service Certificates: TLS bindings and custom domain SSL configurations
- Azure Application Gateway: SSL profiles, backend certificates, and listener certificates
- Azure Front Door: custom domain SSL bindings
- Azure API Management: API level certificates and gateway certificates

Discovery is read only. It reads object metadata such as type, algorithm, key length, and validity. It never creates, changes, exports, or deletes anything in Azure, and private key material is never extracted.

---

0. The Two Ways to Work with Azure

Everything below can be done two ways. Pick whichever you prefer for each step:

Mode	How you access it	Best for
Azure Portal	A browser at `https://portal.azure.com`	Point and click setup, one off changes
Azure CLI	The `az` command line tool on your computer	Scripting, copy and paste setup, generating credentials

> Install the Azure CLI from https://learn.microsoft.com/cli/azure/install-azure-cli if you want to use the command line. Sign in first with `az login`.

---

1. Prerequisites

- An Azure subscription containing the Key Vaults, HSMs, or services you want to inventory.
- Permission to create an app registration (a Service Principal) in your Microsoft Entra ID tenant, or an administrator who can create one for you.

- Permission to assign read only roles on the subscriptions, resource groups, or vaults you want scanned.
- The discovery host must be able to reach the Azure management and Key Vault endpoints over the network.

No software installation is required on your side. You provide the credentials and the scope to scan.

---

2. Choose an Authentication Method

Discovery signs in to Azure using one of the following. Service Principal is recommended for automated use.

Method	What you provide	Best for
Service Principal (recommended)	Tenant ID, Client ID, and Client Secret	Automated, unattended discovery
Managed Identity	Nothing to copy; the identity is bound to the host	Discovery running on an Azure VM or service
Azure CLI context	An existing `az login` session on the discovery host	Quick tests from a signed in machine

The rest of this guide sets up a Service Principal, since it is the most portable option.

---

3. Create the Discovery Service Principal

Azure Portal

1. Go to Microsoft Entra ID, then App registrations, then New registration.
2. Name it, for example, cbom_discovery, and click Register.
3. On the app overview, copy the Application (client) ID and the Directory (tenant) ID.
4. Go to Certificates and secrets, then New client secret. Set a description and expiry, then click Add.
5. Copy the secret Value immediately. It is shown only once.

Azure CLI

```
# Creates the app registration, a service principal, and a client secret in one step
az ad sp create-for-rbac --name cbom_discovery --role Reader \
    --scopes /subscriptions/<subscription-id>
```

The command prints `appId` (Client ID), `password` (Client Secret), and `tenant` (Tenant ID). Copy all three now.

---

4. Grant Read Only Access

The Service Principal needs just enough access to list and read metadata, nothing more.

4.1 Subscription or resource group scope

Assign the built in Reader role at the scope you want scanned (a whole subscription, or a single resource group).

Azure Portal

1. Open the subscription or resource group, then Access control (IAM).
2. Click Add, then Add role assignment.
3. Choose the Reader role, then select your cbom_discovery app, then Save.

Azure CLI

```
az role assignment create --assignee <client-id> \
    --role Reader \
    --scope /subscriptions/<subscription-id>
```

4.2 Key Vault data access

The Reader role sees vault metadata but not the objects inside a vault. Grant read only data access as well, depending on the vault permission model.

For vaults using Azure RBAC, assign these built in roles to cbom_discovery:

```
az role assignment create --assignee <client-id> \
    --role "Key Vault Reader" \
    --scope /subscriptions/<subscription-id>
# Read only "get" and "list" on certificates, keys, and secrets metadata
```

For vaults using access policies (the classic model), open the vault, then Access policies, then add a policy for cbom_discovery granting List and Get on Keys, Certificates, and Secrets only. Do not grant create, import, delete, or purge.

> Grant only List and Get. Discovery reads metadata; it never needs write, delete, or key export rights.

---

5. Collect Your Connection Values

Before configuring discovery, gather these:

Value	Where it comes from
Tenant ID	The Directory (tenant) ID from Section 3
Client ID	The Application (client) ID from Section 3

Value	Where it comes from
Client Secret	The secret Value copied in Section 3 (Service Principal only)
Subscription ID	The subscription that holds the resources to scan
Authentication method	Service Principal, Managed Identity, or Azure CLI context (Section 2)
Scope to scan	Whole subscription, one or more resource groups, or specific vaults
Services to include	Any of Key Vault, Managed HSM, App Service, Application Gateway, Front Door, API Management

---

6. Enter the Values in the Discovery Configuration

In the CBOM platform, create a new Microsoft Azure discovery task and fill in the form:

Field	What to enter
Scan Name	A label for this run, for example `Azure_Discovery`
Authentication Method	Choose Service Principal, Managed Identity, or Azure CLI context
Tenant ID	The Directory (tenant) ID from Section 5
Client ID	The Application (client) ID from Section 5
Client Secret	Service Principal only: the secret Value from Section 3
Subscription ID	The subscription to scan
Scope	Whole subscription, or specific resource groups or vaults
Services to Scan	Select Key Vault, Managed HSM, App Service, Application Gateway, Front Door, and/or API Management

Save and run the task.

---

7. Validate

After running the discovery task, confirm:

- The task completes without an authentication or authorization error.
- Certificates and keys from your Key Vaults appear in the inventory, with algorithm, key length, and validity.
- Service certificates from App Service, Application Gateway, Front Door, or API Management appear where those services are in scope.

You can double check the credential access with the Azure CLI, using the same Service Principal discovery uses:

```
az login --service-principal -u <client-id> -p <client-secret> --tenant <tenant-id>
az keyvault list
az keyvault certificate list --vault-name <your-vault>
```

---

8. Troubleshooting

Symptom	Likely cause	Fix
`AADSTS700016` or invalid client	Wrong Client ID or Tenant ID	Confirm the values from Section 3 match the app registration
`invalid client secret`	Secret mistyped or expired	Create a new client secret (Section 3) and update the configuration
`AuthorizationFailed`	The Reader role is not assigned at the scope	Assign Reader at the subscription or resource group (Section 4.1)
Vault metadata visible but no objects	Missing Key Vault data access	Grant Key Vault Reader (RBAC) or a List and Get access policy (Section 4.2)
Nothing discovered	Wrong subscription or scope, or no resources present	Confirm the Subscription ID and that the scope contains vaults or services
Timeout or network error	Discovery host cannot reach Azure endpoints	Confirm outbound access to the Azure management and Key Vault endpoints

---

Final Checklist

- ☐ A Service Principal (app registration) created for discovery
- ☐ Tenant ID, Client ID, and Client Secret copied
- ☐ Reader role assigned at the subscription or resource group scope
- ☐ Key Vault data access granted (Key Vault Reader, or a List and Get access policy)
- ☐ Services chosen: Key Vault, Managed HSM, App Service, Application Gateway, Front Door, API Management
- ☐ Values entered in the Microsoft Azure discovery configuration and the task runs without errors