

Azure Key Vault Integration Guide

Prerequisites

A system administrator with the necessary Azure permissions must:

- Have access to **Microsoft Entra ID (Azure AD)**.
- Have permission to **create app registrations**.
- Have permission to **assign roles or create access policies** in Azure Key Vault.
- Have the necessary access to **CertSecure Manager** for registration.

Integration Steps

STEP 1: Register an App in Microsoft Entra ID (Azure AD)

1. Go to **Microsoft Entra ID > App registrations**.
2. Click **New registration**:
 - **Name**: CertSecure_Manager_AKV
 - **Supported account types**: Single tenant
 - Leave **Redirect URI** empty.
3. Click **Register**.

STEP 2: Generate a Client Secret

1. Open your registered app → Go to Manage → **Certificates & secrets**.
2. Under **Client secrets**, click **New client secret**:
 - **Description**: e.g., AKVTesting
 - **Expiration**: Choose a validity period (6 or 12 months).
3. After saving, **copy the secret value immediately** (you won't see it again).

STEP 3: Note the Following Values

You will need the following for CertSecure Manager:

- **Tenant ID** → Found in app **Overview** under “Directory (tenant) ID”.
- **Client ID** → Found in app **Overview** under “Application (client) ID”.
- **Client Secret** → Copied from Step 2.

STEP 4: Assign Access to Key Vault

Option 1: Using Role-Based Access Control (RBAC)

1. Go to **Key Vault** in Azure Portal > **Access control (IAM)**.
2. Click **Add > Add role assignment**.
3. **Role:** Select Key Vault Certificates Officer.
4. **Assign access to:**
User, group, or service principal → Search for your app name (e.g., CertSecure_Manager_AKV_Test)
5. Click **Review + assign**.

Option 2: Using Access Policy

1. Go to **Key Vault > Access policies**.
2. Click **+ Add Access Policy**.
3. Set **Certificate permissions**: check: Get, List, Import.
4. Select your registered app as the **Principal**.
5. Click **Review + create**.

STEP 5: Add Azure Key Vault in CertSecure Manager

Once you've completed the Azure-side configuration (App registration, client secret, and access permissions), follow these steps to **add Azure Key Vault to CertSecure Manager**:

- **Login as Admin** to the **CertSecure Manager** portal.
- Navigate to **Utilities > Azure Key Vault**. This section is **visible only to administrators**.
- Click on **"Add Azure Key Vault"**.
- In the form that appears, fill in the following fields using the values you gathered earlier:
 - **Key Vault Name:** Provide a friendly name for internal reference.
 - **Tenant ID:** Copied from the Entra ID app overview.
 - **Client ID:** Application (client) ID from the registered app.
 - **Client Secret:** The secret value you generated.

Click **Save**.

Add New Azure Key Vault [X]

Vault Name *
Add Vault Name

Client ID *
Add Client ID

Tenant ID *
Add Tenant ID

Client Secret *
Add Client Secret

Save **Cancel**

STEP 6: To Upload a Certificate to Azure Key Vault:

1. Navigate to **Enrollment > Generate Certificate**.
2. Fill in the required details and click the **Generate Certificate** button.
3. If Azure Key Vault integration is active, a **pop-up window** will appear.
4. In the pop-up:
 - Select the desired **Azure Key Vault**.
 - Specify a **name** (this becomes the unique identifier for the certificate in Key Vault).
 - Select the **certificate format**.

Want to add this certificate to Azure Key Vault? [X]

Select Azure Key Vault *
Select

Name *
Add Name

Format *
☒ PEM
 ☐ PFX

Yes **No**

5. Click **Yes** to proceed.
6. Once the certificate is issued, it will be **automatically uploaded** to the selected Azure Key Vault.
7. A log entry will be created under **Misc > Logging > Certificate Management**, indicating the **success or failure** of the upload.

Logging

Access detailed logs of system activities. Monitor events for auditing, troubleshooting, and compliance maintenance.

Certificate Download

Certificate Management

Environment

Ownership Transfer

User Management

Search Keyword

Clear

Refresh

ID	Severity	Date	Details	Source
297	Info	Sat Apr 16 2025 21:44:02 GMT+0530 (India Standard Time)	Certificate with EID (190) has been uploaded to Azure Key Vault	192.168.1.25