**About Azure Key Vault**

Azure Key Vault is a cloud-based service that enables you to safeguard and control cryptographic keys, certificates, and secrets used by your applications.

This article provides guidance on how to create a new key vault, add secrets or keys to it, configure access policies for different users or applications, and manage the lifecycle of these resources.

**Important:** Before you begin, make sure that you have an Azure subscription with sufficient permission and knowledge about the main concepts, such as encryption algorithms and key rotation.

**Reference Video:**

<https://www.youtube.com/watch?v=RTq72C10x88>

**Create a new Key Vault**

1. In the Azure portal, select **+ Create a resource** in the left pane.
2. Search for **Key Vault** in the search bar at the top of the page.
3. Select **Key Vault** from the results, and then select **Create**.
4. Fill out all required fields in the Basic tab, such as Subscription, Resource group, Name, and so on.
5. Select your preferred region to host your key vault resources under Networking tab.
6. Under the Tags tab, provide any metadata about this key vault if needed (optional).
7. Review the **+ Create** tab, which summarizes everything that you've configured so far, including pricing details, and so on.
8. Select the **Create** button to deploy your new key vault.

**Manage an existing Key Vault**

Azure Key Vault is a cloud service that provides secure storage of keys, secrets, and certificates. After you've created a key vault in Azure, there are several management tasks that you may need to perform. Here are some common management tasks and how to perform them:

**Add secrets, certificates, and keys to Key Vault**

To add a **Secret**, use the following steps:

1. In the Azure portal, go to your KeyVault resource.
2. In the Key Vault's object section, select **Secrets.**
3. Select the **+ Generate/Import** button.
4. Enter in the **Name & Secret Value** for the secret.
5. Select the appropriate options, if required.
6. Select **Create.**

For more detailed steps, see [this tutorial](https://learn.microsoft.com/azure/key-vault/secrets/quick-create-portal).

To add a **Certificate**, use the following steps:

1. In the Azure portal, go to your KeyVault resource.
2. In the Key Vault's object section, select **Certificate.**
3. Select the **+ Generate/Import** button.
4. Enter in the **Name & Certificate** file and PFX file details.
5. Set the appropriate options, if required.
6. Select **Create.**

For more detailed steps, see [this tutorial](https://learn.microsoft.com/azure/key-vault/certificates/quick-create-portal).

To add a Key, use the following steps:

1. In the Azure portal, go to your KeyVault resource.
2. In the Key Vault's object section, select **Key.**
3. Select the **+ Generate/Import** button.
4. Enter in the **Name** and other details.
5. Set the appropriate options, if required.
6. Select **Create.**

**Note:** You can also import existing keys.

For more detailed steps, see [this tutorial](https://learn.microsoft.com/azure/key-vault/keys/quick-create-portal).

**Configure Access policies in Key Vault**

**RBAC Permission Model (Recommended)**

Azure role-based access control (Azure RBAC) is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources. Azure RBAC allows users to manage Key, Secrets, and Certificates permissions. It provides one place to manage all permissions across all key vaults. To configure RBAC policies, use the following steps:

1. In the Azure portal, go to your KeyVault resource.
2. Select **Add** > **Add role assignment** to open the Add role assignment page.
3. Assign the role.

For more detailed info, [refer to this tutorial](https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli)

**Access Policy Permission Model (legacy)**

Access policies determine which users or applications can access the resources stored in your key vault. To add or remove access policies, use the following steps:

1. In the Azure portal, go to your KeyVault resource.
2. In the Key Vault's object section, select **Access policies**.
3. To add a new policy, select **+Add Access Policy**.
4. Select the permissions that you want to grant for this policy (for example, get/list/delete), and then specify the identity of the user or application that should be granted these permissions.
5. Select **OK** to save the new policy.

To remove an existing policy:

1. Go back to the **Access policies** blade for your key vault resource.
2. Locate the policy that you want to remove, and then select **Remove**.

For more detailed steps, see [this tutorial](https://learn.microsoft.com/azure/key-vault/general/assign-access-policy?tabs=azure-portal).

**Rotate keys**

Key rotation is an important security practice that involves regularly generating new encryption keys and retiring old ones. This way, if one key is compromised, it limits the exposure of data encrypted with previous versions of keys.

To rotate keys, use the following steps.

1. In the Azure portal, go to your KeyVault resource.
2. In the Key Vault's object section, select the **Keys** tab.
3. Select the **Rotate** button next to each active version of each managed key.
4. Generate a new version of the key. See [Create Key](https://learn.microsoft.com/rest/api/keyvault/keys/create-key/create-key?view=rest-keyvault-keys-7.4&tabs=HTTP).
5. Safely back up the new version. See [Key Vault backup and restore](https://learn.microsoft.com/azure/key-vault/general/backup?tabs=azure-cli).
6. Notify all the clients that are using old version, providing them with details on how to update their systems.

For more detailed steps, see [this tutorial](https://learn.microsoft.com/azure/key-vault/keys/how-to-configure-key-rotation).

**Backup and restore secrets**

Backing up secrets is critical in case data loss occurs due accidental deletion, file corruption, and so on. You can restore backed-up secrets from another location, move them to another subscription, and so on.

To back up a secret, use the following steps:

1. In the Azure portal, go to your KeyVault resource.
2. In the Key Vault's object section, select the **Secrets** tab.
3. Select that secret that needs to be backed up.
4. Select the **Backup** button. The backup process will download an encrypted blob of the secret.
5. Store this encrypted blob in a secure location of your choosing, not necessarily in Azure Storage.

To restore a secret, use the following steps:

1. In the Azure portal, go to your KeyVault resource.
2. In the Key Vault's object section, select the **Secrets** tab.
3. Select the **Restore** button to initiate the restoration process.
4. Specify the location of the encrypted backup blob you previously saved.
5. Execute the restore operation, which will add the secret back to your Key Vault.

For more detailed steps, see [this tutorial](https://learn.microsoft.com/azure/key-vault/general/backup?tabs=azure-cli).