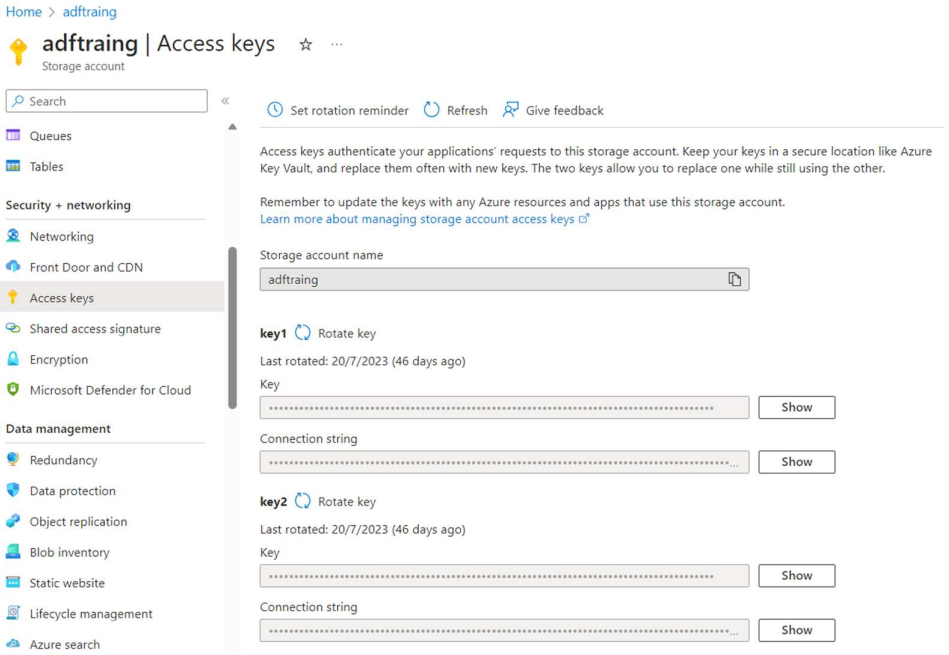
# Access Keys

Access keys in Azure Storage are used to authenticate and authorize access to various Azure Storage services, such as Blob Storage, Queue Storage, and Table Storage. These keys are essentially pairs of an account name and a key (either a primary or secondary key), which grant access to the associated storage account. Access keys provide a simple way to secure and manage access to your Azure Storage resources.

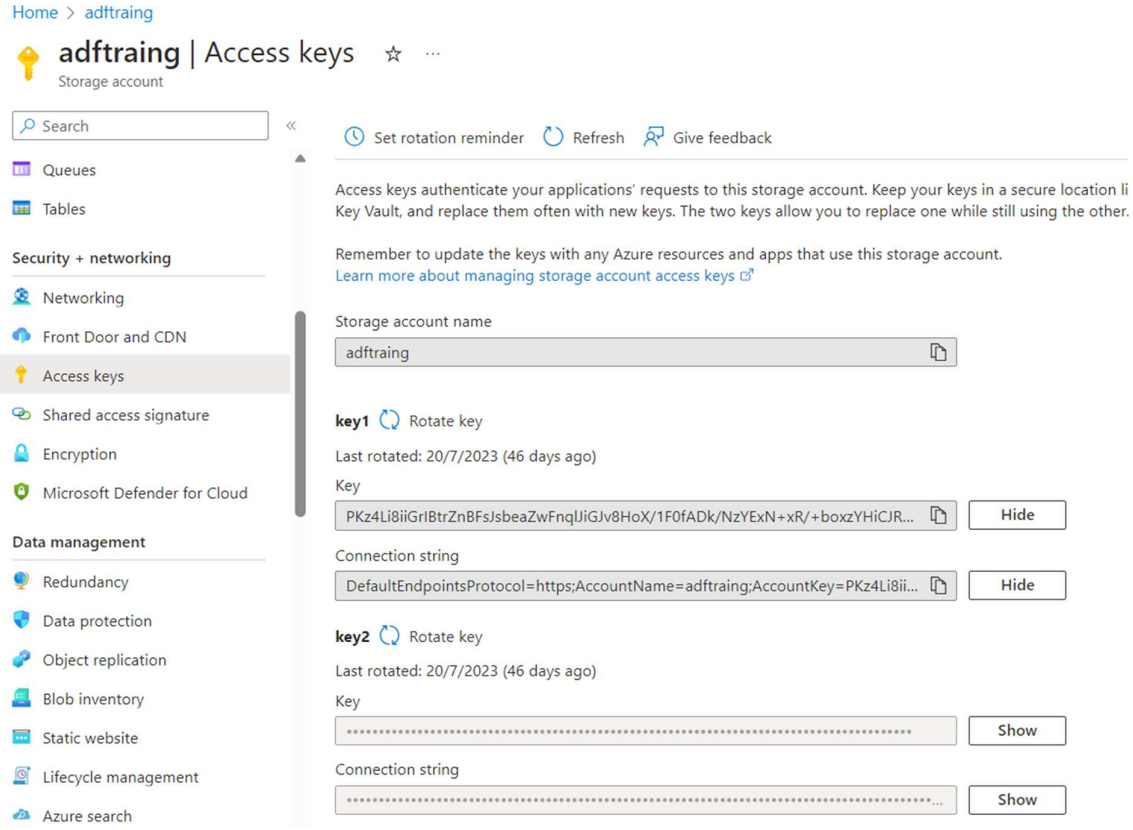
You can use the access keys to authenticate and authorize access to your storage account in various ways:

- **Storage Explorer:** If you're using Microsoft's Azure Storage Explorer tool, you can provide the account name and either the primary or secondary access key to connect to your storage account.
- **Azure SDKs and Libraries:** When writing code to interact with Azure Storage services, you can use the access keys to authenticate. Most Azure SDKs and libraries provide a way to set the account name and access key in your application's configuration or code.
- **Azure PowerShell and Azure CLI:** You can use Azure PowerShell and Azure CLI commands to interact with Azure Storage. These tools allow you to set the storage account name and access key as part of their configuration.

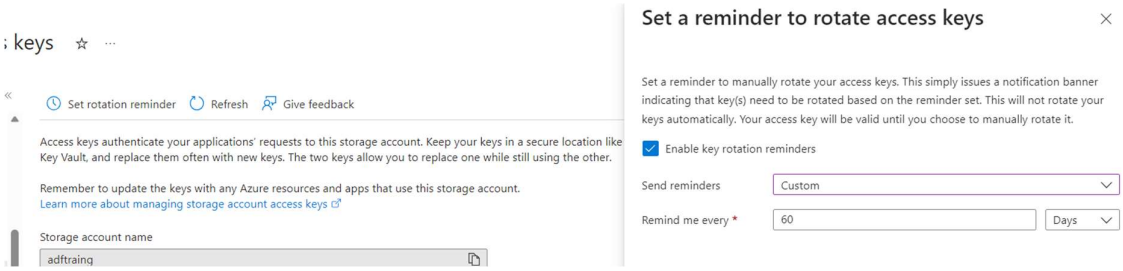
1. In the Storage account under Access Keys you will see the keys.



2. Click on Show to copy the Keys.
3. Click on Rotate Key to regenerate the key.




4. Or you can set the rotation time. Click on the St rotation remainder and set the days as shown below.



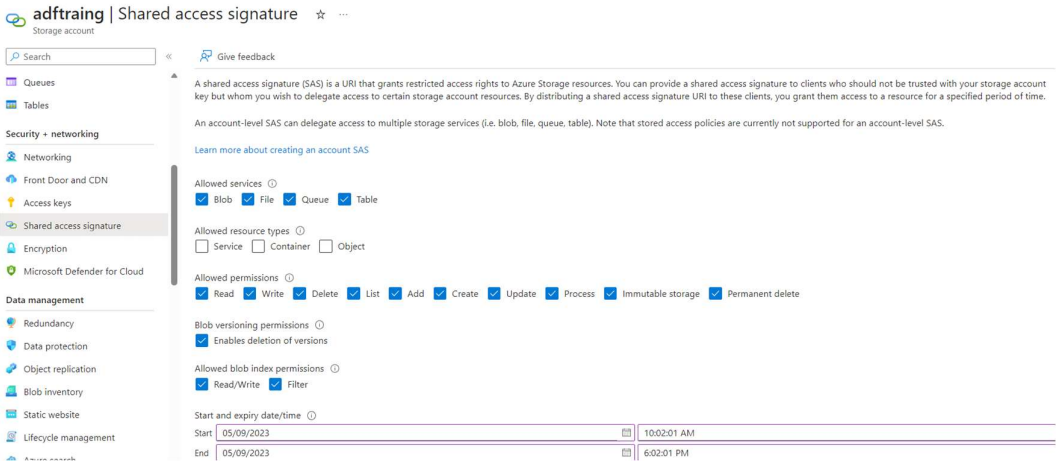
# Shared Access Signatures

Shared Access Signatures (SAS) in Azure Storage provide a way to grant limited and time-bound access to specific resources within your Azure Storage account without sharing your account keys. SAS tokens are a more secure and flexible way to manage access to your storage resources compared to directly using access keys.

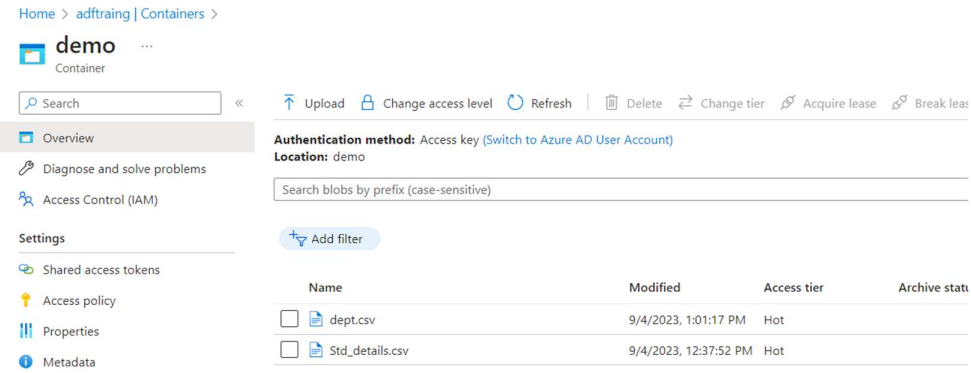
There are two main types of SAS tokens in Azure Storage:

- **Service SAS:** Grants access to a specific service (e.g., Blob Storage, Queue Storage, Table Storage) and allows operations on multiple resources within that service.
- **Account SAS:** Grants access to one or more storage services and can be used to perform operations on different types of resources within those services.

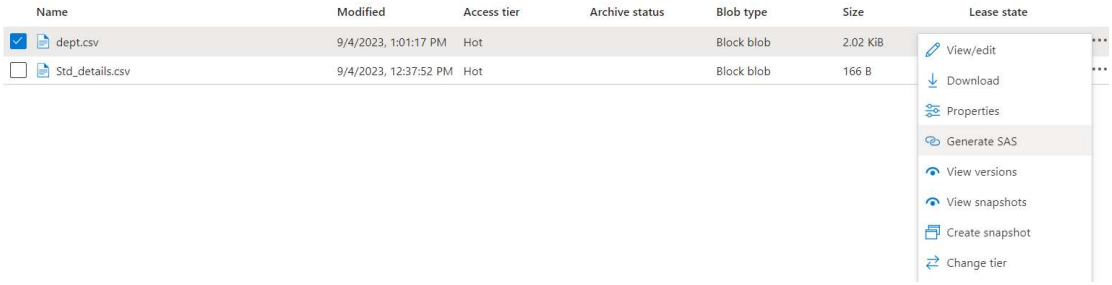
1. In the Storage Account, Under Shared Access Signatures we can grant access to the services and set the expiration time also.



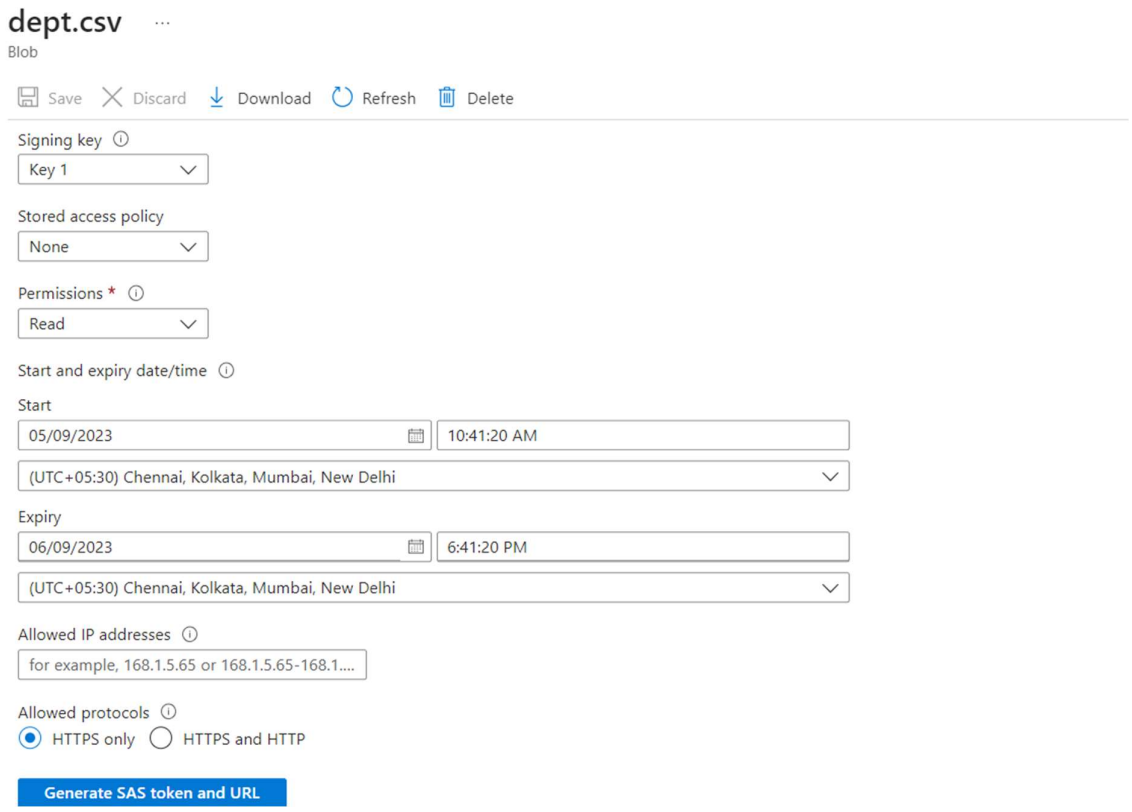

2. In this example we will create SAS for this dept file.



3. Right click on the file and click on Generate SAS as shown below.




4. Set the Start and Expiry time and click on Generate SAS token and URL.




5. Copy Blob SAS URL.

6. Paste it in the chrome or Edge. The dept file will download automatically.