# AWS Cross-Account Secret Access

## Documentation

AWS Secrets Manager is a great way to safely store secrets needed by applications. Sometimes you need to access those secrets from an AWS account other than the account where the secret is stored. Here are some notes about that.

AWS documentation about cross-account secret access: https://aws.amazon.com/premiumsupport/knowledge-center/secrets-manager-share-between-accounts/

## Notes

- Secrets to be shared across AWS accounts need to be encrypted with a customer KMS key, not the default KMS key that AWS provides.
    - It's easy to switch the KMS key used for a particular secret. When you switch the KMS key for the secret be sure to have Secrets Manager re-encrypt the secret with the new key. If using the web console, the wizard will offer to do that for you.
- In the end, you will have a resource policy to both the target secret and the KMS key used for encrypting the secret.
- Don't forget that in the AWS account from which the secret is being accessed, the IAM security principal (Role, User) will also need explicit privileges to access the secret (in addition to the resource policies attached to the Secret and KMS key).
- The policies provided in the above link allow access to only the most recent version of the secret (i.e., `AWSCURRENT`). Be sure to include that version stage in the API/CLI request. E.g.,

```
$ aws secretsmanager get-secret-value --secret-id arn:aws:secretsmanager:us-east-1:HOMEACCOUNT:secret:
MySecret --region us-east-1 --version-stage AWSCURRENT
```