How to Manually Set up a Role Related to a Keystore

To grant the BYOK web service access to creating and maintaining keys in the KMS of your account you must create a policy and include it in a role.

Create a Policy

1. In the AWS Management Console go to “Identity and Access Management (IAM)”.
2. Click "Policies" in the left navigation bar. The "Policies" pane appears to the right.
3. In the upper right corner click the "Create Policy" button. The "Create policy" start page appears.
4. Add at least the following KMS permissions:

   kms:EnableKey, kms:ImportKeyMaterial, kms:UntagResource, kms:GenerateRandom, kms:PutKeyPolicy, kms:ListResourceTags, kms:CancelKeyDeletion, kms:GetParametersForImport, kms:TagResource, kms:ScheduleKeyDeletion, kms:DescribeKey, kms:CreateKey, kms:ListKeyPolicies, kms:UpdateKeyDescription, kms:GetKeyPolicy, kms:DeleteImportedKeyMaterial, kms:DisableKey, kms:UpdateAlias, kms:ListKeys, kms:ListAliases, kms:CreateAlias

   This can be done either by using the "Visual editor" tab or from the "JSON" tab by copy-and-pasting the example policy.
5. Click the "Next: Tags" button in the lower right corner. The "Create policy | Add tags (Optional)" page appears.
6. Click the "Next: Review" button in the lower right corner. The Create policy | Review policy" page appears.
7. In the "Name" field, provide a name for the policy and click the "Create policy" in the lower right corner.

The policy is now created.

Create a Role

1. In AWS Management Console, go to “Identity and Access Management (IAM)”.
2. Click "Roles" in the left navigation bar.
3. Click the "Create role" button in the upper right corner. The "Select trusted entity" page appears below.
4. In the "Trusted entity type" field, choose "AWS account". The section "An AWS account" appears.
5. In the "An AWS account" section, choose "Another AWS account" and enter the **AWS account number** from the "Create new key store" BYOK web service page.
6. In "Options" in the "An AWS account" section, choose "Require external ID (Best practice when a third party will assume this role)" and enter the **external ID** from the "Create new key store" BYOK web service page.
7. Click the "Next" button in the lower right corner. The "App permissions" page appears.
8. Search for the policy created previously and select it.
9. Click the "Next" button in the lower right corner. The "Name, review, and create" page appears.
10. Provide a name for the role in the "Role name" field and click the "Create role" button in the lower right corner.

The role is created. On the "Create new key store" BYOK service web page, enter the **ARN** of the newly created role.

Copy-and-Paste Example Policy

An example AWS policy JSON document granting access to the minimum set of KMS operations is shown below.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "kms:EnableKey",
                "kms:ImportKeyMaterial",
                "kms:UntagResource",
                "kms:GenerateRandom",
                "kms:PutKeyPolicy",
                "kms:ListResourceTags",
                "kms:CancelKeyDeletion",
                "kms:GetParametersForImport",
                "kms:TagResource",
                "kms:ScheduleKeyDeletion",
                "kms:DescribeKey",
                "kms:CreateKey",
                "kms:ListKeyPolicies",
                "kms:UpdateKeyDescription",
                "kms:GetKeyPolicy",
                "kms:DeleteImportedKeyMaterial",
                "kms:DisableKey",
                "kms:UpdateAlias",
                "kms:ListKeys",
                "kms:ListAliases",
                "kms:CreateAlias"
            ],
            "Resource": "*"
        }
    ]
}
```