

# How To Recover Management Access to AWS KMS Keys

- [Introduction](#)
- [Process](#)
- [References](#)

## Introduction

Each key managed by the AWS Key Management Service (KMS) must have a resource policy that describes what AWS security principals can use and manage the key. If you create a policy that does not include management privileges for any principal or if principals named in the policy are themselves deleted, you may find yourself unable to manage a KMS key. Fortunately AWS provides a way to regain control of the key in such a situation.

⚠️ Note that even the root user for the AWS account cannot manage KSM keys unless specifically allowed in the key policy! As of 01 Sep 2022, we could not find AWS documentation that discusses how to recover management access to a key, thus we created this short article.

To avoid being locked out of a KMS key from an accidentally deleted IAM principal, using a Condition in the Key Policy is recommended.

### Key Policy Example

```
{
  "Sid": "Allow administration",
  "Effect": "Allow",
  "Principal": {
    "AWS": "*"
  },
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::${SOME_ACCOUNT_ID}:role/shib-admin",
        "arn:aws:iam::${SOME_ACCOUNT_ID}:root"
      ]
    }
  }
}
```

## Process

1. First, try to access the KMS key with any/all security principals (IAM Roles and Users) that might have previously had access to the key. If any principal has even **kms:DescribeKey** privileges to the target key, use that principal to review the key policy (resource policy) attached to the key. That may reveal a security principal that has access to manage the key.
2. If Step 1 doesn't reveal any way to manage the key, create a support ticket for the CIT Cloud Team ([cloud-support@cornell.edu](mailto:cloud-support@cornell.edu)) describing the situation. Be sure to include the ID/Arn of the problematic key.
  - The CIT Cloud Team will in turn create a support case with AWS to aid in recovering access to the key. As a Cornell AWS user, you *could* also directly create the AWS support case, but you will still need to involve the CIT Cloud Team because part of the recovery process is a phone call to the phone number associated with the AWS account. For most Cornell AWS accounts, that phone number is directed to a CIT Cloud Team phone extension.

## References

- AWS documentation
  - [Authentication and access control for KMS](#)