Insert Trust Relationship in AWS IAM Role

If you are using per-user authentication through an AWS IAM role, you must insert a trust relationship into the role so that Trifacta® SaaS can leverage it.

Prerequisites:

Please acquire the following information:

- **Account ID:** The AWS account identifier that Trifacta SaaS should use for access.

  > **NOTE:** This value is provided to you by Trifacta.

  After it has been specified, this value is available for workspace administrators through the Admin console. See *AWS Settings Page*.

- **External ID:**The external identifier is set within Trifacta SaaS. This value is available for workspace administrators through the Admin console. See *AWS Settings Page*.

- **IAM role:** The AWS IAM role that Trifacta SaaS should use.

For more information on the AWS Principal options described below, please review *https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html*.

Steps:

1. Login to the AWS console.
2. Open the IAM role for use with Trifacta SaaS.
3. Insert the following AWS policy snippet to define the trust relationship for this role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "<aws_account_id>"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "sts:ExternalId": [
            "<external_id>"
          ]
        }
      }
    }
  ]
}
```

where:

Setting	Description
`<aws_account_id>`	The AWS account identifier for Trifacta SaaS

`<external_id>`	The external identifier generated by Trifacta SaaS

4. Save the IAM role definition.

> **NOTE:** The AWS account ID value must be applied to every user profile that requires access through this IAM role. See *User Profile Page*.