IAM Account

Feature: AWS

Editions: Cloud, Corporate, Store

> This topic is for reference purposes only. Use AWS provisioning to automatically create these resources for each organization.

As a best security practice, we always ensure that a client has its own AWS access credentials to access their services. This ensures that we do not accidentally expose a client's information to other clients.

The automated provisioning process creates the IAM user:

- The generated name uses the format rms_orgId, where orgId is the unique Organization ID.
- Given an example organization ID of xmsqa1, the user name would be rms_xmsqa1.
- The IAM user is programmatic access only; the user cannot access the AWS console.
- Permissions are not set; we generally attach policies on individual resources instead.
- A OrgID tag is added to make billing reports easier.

> An access key is not created by the provisioning purpose. A Kensium administration must use the AWS console to create the access key manually.
>
> - Copy these values to the Kensium password manager, as you will not see these values later.
> - Do not store the access key values in a file, and do not communicate them using insecure communications.
> - If you lose the values the AWS console has a feature to regenerate the access key ID and secret, although you will need to re-apply them to all servers that use them.