

## ACCT-002 - Define identity security best practice on how to access customer environment by leveraging IAM

Depending on the user access permission configuration, we present best practices for maintaining user identity security. We maintain the minimum required roles or permissions, setting temporary credentials where applicable for accessing IAM roles. Each Partner administrator user must have dedicated credentials.

### Policy

#### Account settings [info](#)

##### Password policy [info](#)

Configure the password requirements for the IAM users.

[Edit](#)

##### This AWS account uses the following default password policy:

Password minimum length  
8 characters

##### Password strength

Include a minimum of three of the following mix of character types:

- Uppercase
- Lowercase
- Numbers
- Non-alphanumeric characters

##### Other requirements

- Never expire password
- Must not be identical to your AWS account name or email address

##### Security Token Service (STS) [info](#)

STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources.

##### Session Tokens from the STS endpoints

AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions. If you use regional STS endpoints, no action is required. Session tokens from the global STS endpoint (<https://sts.amazonaws.com>) are valid only in AWS Regions that are enabled by default. If you intend to enable a new Region for your account, you can use session tokens from regional STS endpoints or activate the global STS endpoint to issue session tokens that are valid in all AWS Regions.

##### Global endpoint

Valid only in AWS Regions enabled by default | [Change](#)

##### Regional endpoints

Valid in all AWS Regions

### Grant least privileges

IAM users are defined and classified based on the role or activities they can run in the console for the management and operation of current Infinity Gifts Souvenirs workloads.

This definition is done similarly to the on-premises environment, although the use of IAM policies achieves greater control over the privileges assigned.

Since we manage the environment through terraform, only the user assigned for those purposes has administrative permissions on the account.

In addition to that, the client requested a single user for administrative access, was assigned the minimum permissions allowed, and there was no need to create user groups.

For example, one of the resources assigned to the management of this account only has access to the management of the EC2s within the account.

## ARN

### Console access

Access key 1

Create access key

Last console sign-in

✔ Today

## Groups

## Tags

## Security credentials







Last Accessed

Permissions are defined by policies attached to the user directly or through groups.

Search

### Filter by Type

All types

<input type="checkbox"/>	Policy name 	Type	Attached via 
<input type="checkbox"/>	 <a href="#">AmazonEC2FullAccess</a>	AWS managed	Directly
<input type="checkbox"/>	 <a href="#">IAMUserChangePassword</a>	AWS managed	Directly
<input type="checkbox"/>	 <a href="#">MFA-Enable-Policy</a>	Customer managed	Directly
<input type="checkbox"/>	 <a href="#">ReadOnlyAccess</a>	AWS managed - job function	Directly