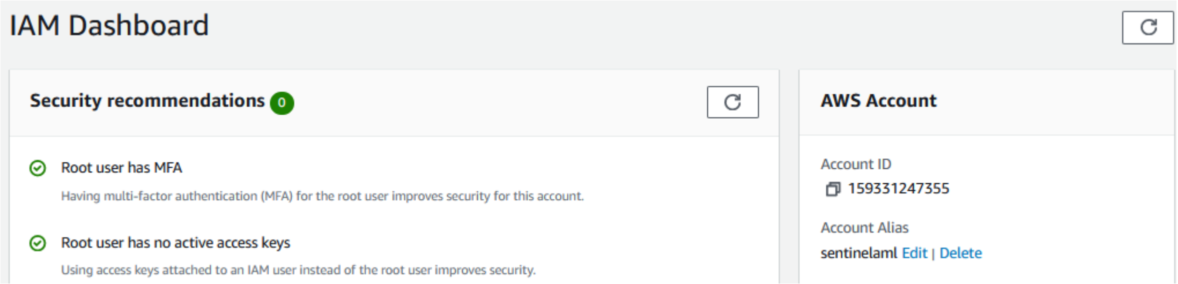
SEC-002 - Prevention of Public Access of Cloud Resources

The root user is secured

The Root user has administrative roles, with MFA enabled. Users with access to the Customer's AWS portal have minimal access roles: read only. The CloudTrail application is used to monitor user activity.



IAM Dashboard

Security recommendations 0

✓ Root user has MFA

Having multi-factor authentication (MFA) for the root user improves security for this account.

✓ Root user has no active access keys

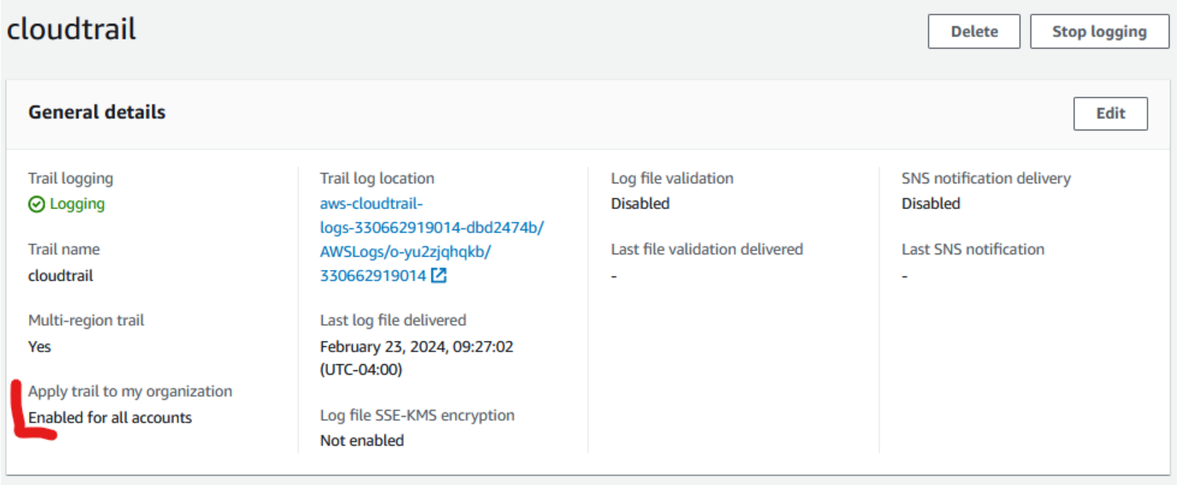
Using access keys attached to an IAM user instead of the root user improves security.

AWS Account

Account ID
159331247355

Account Alias
sentinelaml Edit | Delete

Using CloudTrail for user event logging:



cloudtrail

General details

Trail logging
✓ Logging

Trail name
cloudtrail

Multi-region trail
Yes

Apply trail to my organization
Enabled for all accounts

Trail log location
aws-cloudtrail-logs-330662919014-dbd2474b/AWSLogs/o-yu2zjqhqkb/330662919014

Last log file delivered
February 23, 2024, 09:27:02 (UTC-04:00)

Log file SSE-KMS encryption
Not enabled

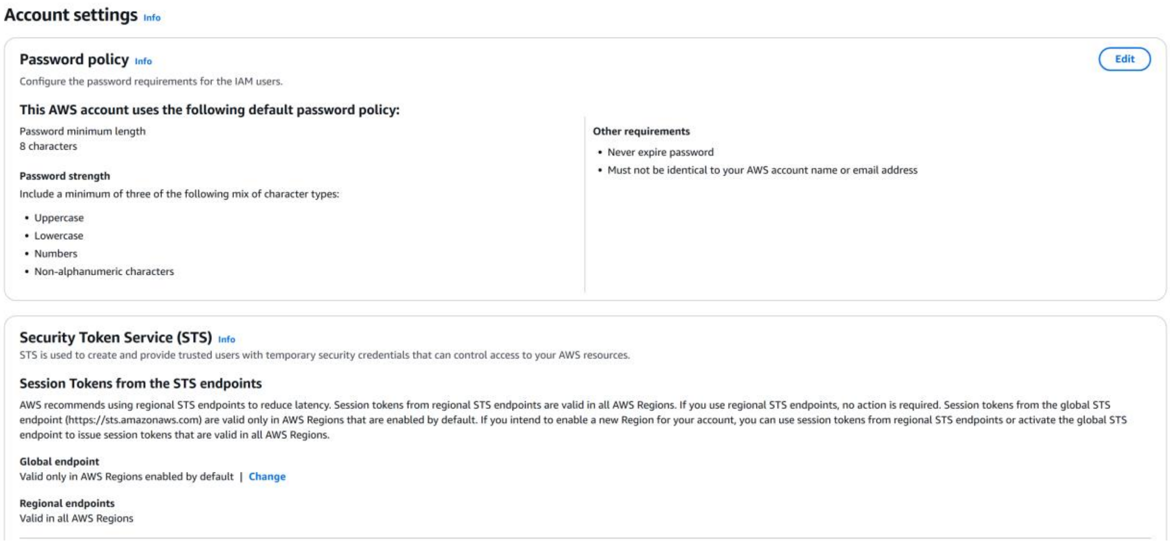
Log file validation
Disabled

Last file validation delivered
-

SNS notification delivery
Disabled

Last SNS notification
-

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.



Account settings Info

Password policy Info

Configure the password requirements for the IAM users.

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