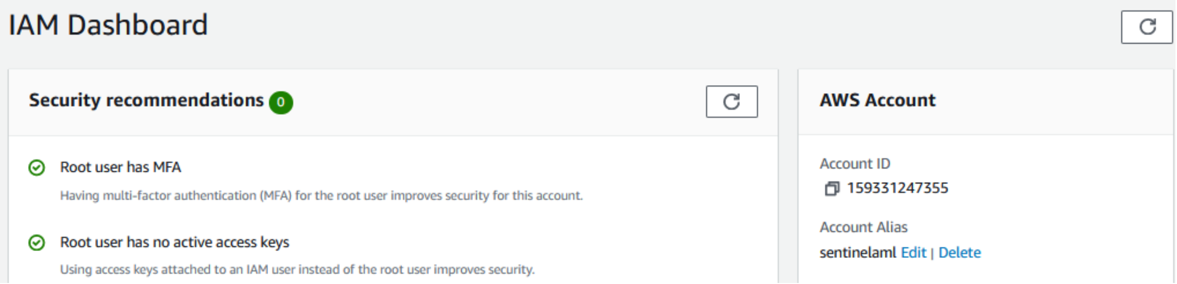
ACCT-001 - Define Secure AWS Account Governance Best Practice

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.

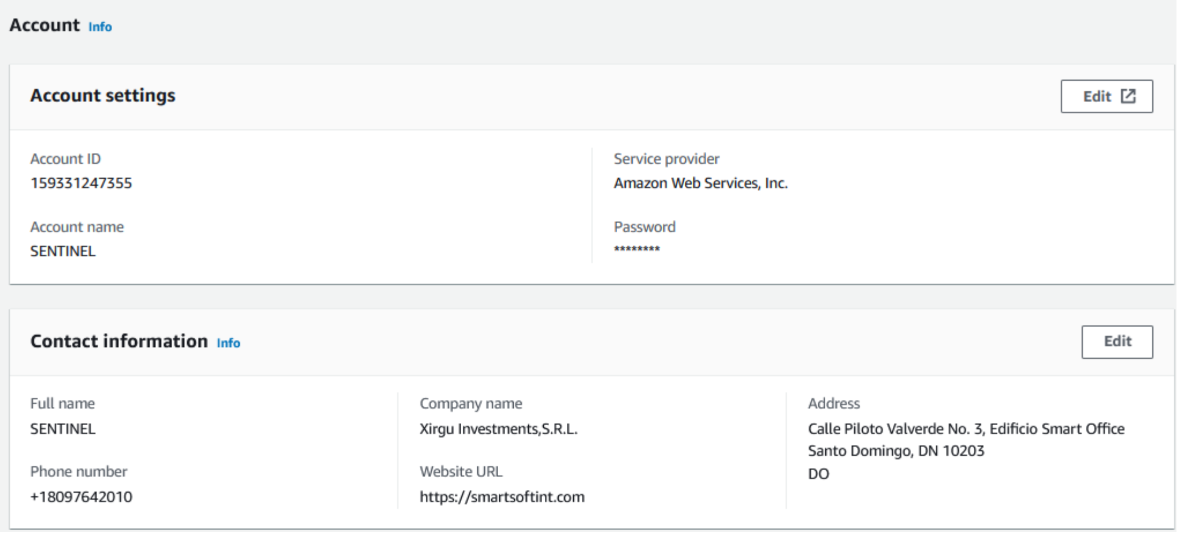
✓ Root user has no active access keys

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



Account Info

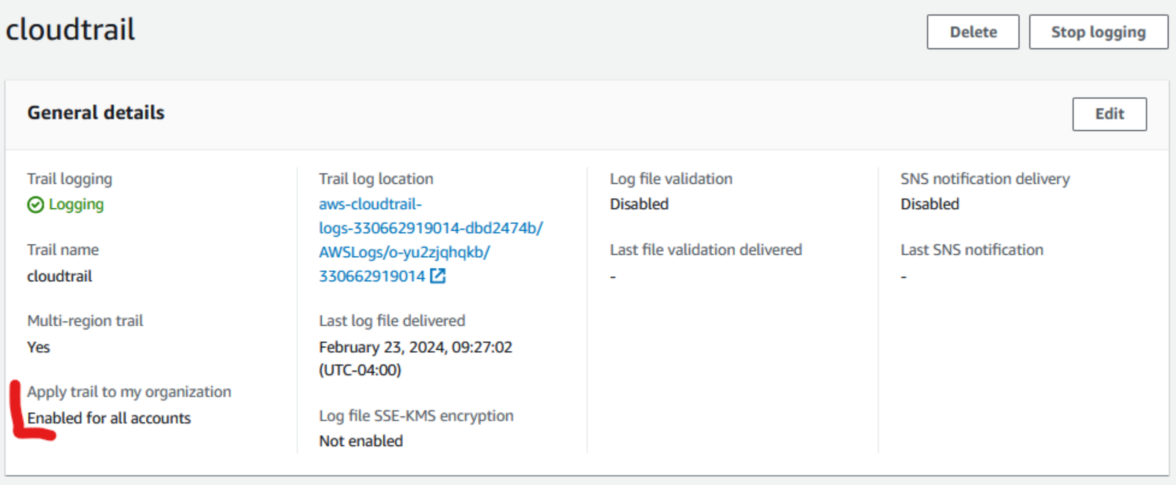
Account settings

Account ID 159331247355	Service provider Amazon Web Services, Inc.
Account name SENTINEL	Password ********

Contact information Info

Full name SENTINEL	Company name Xirgu Investments,S.R.L.	Address Calle Piloto Valverde No. 3, Edificio Smart Office Santo Domingo, DN 10203 DO
Phone number +18097642010	Website URL https://smartsoftint.com	

Using CloudTrail for user event logging:



cloudtrail

General details

Trail logging ✓ Logging	Trail log location aws-cloudtrail-logs-330662919014-dbd2474b/AWSLogs/o-yu2zjqhqkb/330662919014	Log file validation Disabled	SNS notification delivery Disabled
Trail name cloudtrail		Last file validation delivered -	Last SNS notification -
Multi-region trail Yes	Last log file delivered February 23, 2024, 09:27:02 (UTC-04:00)		
Apply trail to my organization Enabled for all accounts	Log file SSE-KMS encryption Not enabled		