

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.

The screenshot shows the AWS IAM Dashboard with a 'Security recommendations' section. It lists three recommendations: 'Root user has MFA' (checked), 'Add MFA for yourself' (warning), and 'Deactivate or delete your access keys unused for more than a year' (warning). Buttons for 'Add MFA' and 'Manage access keys' are visible.

Recommendation	Status	Action
Root user has MFA	✓	
Add MFA for yourself	⚠	Add MFA
Deactivate or delete your access keys unused for more than a year	⚠	Manage access keys

Using CloudTrail for user event logging:

The screenshot shows the AWS CloudTrail console for the 'management-events' trail. The trail is active and logging events. The console displays general details, trail log location, log file validation, and SNS notification delivery settings.

General details	Trail log location	Log file validation	SNS notification delivery
Trail logging Logging	aws-cloudtrail-logs-992382705250-39e6a0dc/AWSLogs/992382705250	Disabled	Disabled
Trail name management-events	Last log file delivered February 14, 2025, 23:33:40 (UTC-04:00)	Last file validation delivered -	Last SNS notification -
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled		
Apply trail to my organization Not enabled			