

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.

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. It displays general details such as trail logging status, trail name, multi-region trail, and log file location. Buttons for 'Delete', 'Stop logging', and 'Edit' are visible.

General details	Trail log location	Log file validation	SMS 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 SMS notification: -
Multi-region trail: Yes	Log file SSE-KMS encryption: Not enabled		
Apply trail to my organization: Not enabled			

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.

[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

IAM users are defined and classified into groups based on the role or activities they can run in the console for the management and operation of current Seguros Patria workloads.

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

Implementation of user groups for assigning permissions.

Identity and Access Management (IAM)		User groups (3) Info																	
<input type="text" value="Search IAM"/>		<input type="text" value="Search"/>																	
<div>Dashboard</div> <div>Access management</div> <div>User groups</div> <div>Users</div> <div>Policies</div>		<div>A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.</div> <table> <thead> <tr> <th><input type="checkbox"/></th><th>Group name</th><th>Users</th><th>Permissions</th></tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td><td>AdministracionEC2Instances</td><td>2</td><td>Defined</td></tr> <tr> <td><input type="checkbox"/></td><td>Administrador</td><td>4</td><td>Defined</td></tr> <tr> <td><input type="checkbox"/></td><td>ReadOnly</td><td>1</td><td>Defined</td></tr> </tbody> </table>		<input type="checkbox"/>	Group name	Users	Permissions	<input type="checkbox"/>	AdministracionEC2Instances	2	Defined	<input type="checkbox"/>	Administrador	4	Defined	<input type="checkbox"/>	ReadOnly	1	Defined
<input type="checkbox"/>	Group name	Users	Permissions																
<input type="checkbox"/>	AdministracionEC2Instances	2	Defined																
<input type="checkbox"/>	Administrador	4	Defined																
<input type="checkbox"/>	ReadOnly	1	Defined																

Based on the methodology and design of the solution, security groups are defined in such a way as to allow traffic only to and from where it belongs.

Considerations:

The entire implemented environment required a Landing Zone. Here we defined the VPC to be used and the security groups that would allow us to define access and restrictions for incoming and outgoing traffic. For more details, please review the networking documentation.

Security groups and permitted or denied access to specific ports on the Seguros Patria platform.



The Directory services are implemented using certificates issued by the Certificate Manager service are associated. The Organization using Customer manager Keys.

KMS > Customer managed keys

Customer managed keys (1)

Filter keys by properties or tags

Aliases	Key ID	Status	Key type	Key spec	Key usage
seguropatria-ad-kms	5491e529-743a-40d1-90f3-02875371...	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt

AWS Certificate Manager > Certificates > 234287c8-75b9-4a98-a0bb-022085626cb6

234287c8-75b9-4a98-a0bb-022085626cb6

Delete

Certificate status

Identifier	234287c8-75b9-4a98-a0bb-022085626cb6	Status	Issued
ARN	arn:aws:acm:us-east-2:612977391817:certificate/234287c8-75b9-4a98-a0bb-022085626cb6		
Type	Amazon Issued		

Domains (1)

Create records in Route 53 Export to CSV

Domain	Status	Renewal status	Type	CNAME name	CNAME value
patria.plus	Success	-	CNAME	_a96838b4b2675d709f0d99569a95b54d.patria.plus.	_2438f1c8b74cbe59cf08eb2ef0c662.duyqrlejt.acm-validations.aws.

Details

In use	Serial number	Requested at	Renewal eligibility
No	0bcdc7cf1352262addfec3352a744a23	December 13, 2023, 21:59:08 (UTC-04:00)	Ineligible
Domain name	Public key info	Issued at	
patria.plus	RSA 2048	December 13, 2023, 21:59:42 (UTC-04:00)	
Number of additional names	Signature algorithm	Not before	
0	SHA-256 with RSA	December 13, 2023, 20:00:00 (UTC-04:00)	
	Can be used with	Not after	
	CloudFront, Elastic Load Balancing, API Gateway and other integrated services. ⓘ	January 12, 2025, 19:59:59 (UTC-04:00)	

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie pref

Data stores are in private subnets.

Cryptographic keys are managed securely

Encryption keys are controlled by the client.

KMS > Customer managed keys

Customer managed keys (1)

Filter keys by properties or tags

Aliases	Key ID	Status	Key type	Key spec	Key usage
seguropatria-ad-kms	5491e529-743a-40d1-90f3-02875371...	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt