

StickSecure

Your friendly compliance and security platform.

AWS Integration



AWS Integration

We have put together some rough screen shots for users to set up their authentication token with AWS that is used to run the scans. Ideally the client should create a new user account to use for the scans for ease of management from their side.

1. Access the Identity and Access Management (IAM) service in AWS. This can be found by searching for IAM in the search bar and selecting IAM from the Services category.





2. Click on the Users option to load users attached to the AWS account. NOTE: The client should set up a new user.

WS Services Q Search		[Alt+S]		D 4 Ø		nolo una Califa
Identity and Access × Management (IAM)	IAM > Users					
Q Search IAM	Users (2) Info An IAM user is an identity with long-ter	n credentials that is used to interact t	with AWS in an account.		C Delete	Create user
Dashboard	Q, Search				<	1 > ©
Access management	User name	▲ Path ▼	Group: ▼ Last activity	▼ MFA ▼ Passwor	d age 🔻 🛛 Console last sign-in	▼ Access k
Jser groups	provide the second	7	1	- 🔗 83 da	November 01, 2023, 0	Active - /
Jsers	C	1	1 .	- 🕑 50 da	iys -	
oles	4.0					
entity providers						
ccount settings						
ccess reports						
ccess analyzer						
Archive rules						
Analyzers						
Settings						

- 3. Select a User and click the Create access key link to start the process.
- 4. Select the appropriate option that best describes the use of the Access key being generated (e.g. Third-party service). Confirm the Terms and Conditions and the 'Next' button.

Access key best practices & alternatives	Access key best practices & alternatives Info Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.
Step 2 - optional Set description tag	Use case
itep 3	Command Line Interface (CLI) You plan to use this access key to enable the AWS CLI to access your AWS account.
Retrieve access keys	C Local code You plan to use this access key to enable application code in a local development environment to access your AWS account.
	Application running on an AWS compute service You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon EC5, or AWS Lambda to access your AWS account.
	Third-party service You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources
	Application running outside AWS You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
	O Other Your use case is not listed here.
	Alternative recommended As a best practice, use temporary security credentials (IAM roles) instead of creating long-term credentials like access keys, and don't create AWS account root user access keys. Learn more 2
	Confirmation I understand the above recommendation and want to proceed to create an access key.



5. Enter a description that best describes the use of the tag (e.g. Stick Secure AWS Scanner). Click the 'Create access key' button to generate the key.

aws	G Search	[Alt+5]			D	\$	0	٢
=	IAM > Users >	> Create access key						
	Step 1 Access key best practices & alternatives	Set description tag - optional Info The description for this access key will be attached to this user as a tag and shown alongside the access key.						
	Step 2 - optional Set description tag	Description tag value Description tag value						
	Step 3 Retrieve access keys	Havimum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and::: / = + - @						
		,	Cancel	Previous	Cre	ate acce	ss key	

6. Step 3. After the key is generated 'Download .csv file' to get a hard copy of the generated key. Copy/Paste the Access key and Secret access key for storage as they cannot be accessed after clicking away from the page.

Services Q Search	[Alt+S]		<u>ک</u> ا	\$ @
Access key created This is the only time that the secret	access key can be viewed or downloaded. You cannot recover it lat	er. However, you can create a new access key any time.		
IAM > Users >	> Create access key			
Step 1 Access key best practices & alternatives	Retrieve access keys Info			
Step 2 - optional Set description tag	Access key If you lose or forget your secret access key, you cannot retrieve i	it. Instead, create a new access key and make the old key inactive.		
	Access key	Secret access key		
Step 3 Retrieve access keys	🗇 ,	O Hide		
	Access key best practices	epository, or in code.		
	Disable or delete access key when no longer needed	d.		
	Enable least-privilege permissions.			
	Rotate access keys regularly.			
	For more details about managing access keys, see the	best practices for managing AWS access keys.		
			Download .csv file	

7. The Access key and Secret access key values are then used in StickSecure to Connect to AWS.



8. The AWS_REGION value should be 'ap-southeast-2' for targeting Australia. This value would change based on the region the user is hosting their framework.

Enter Profile name	0/250
AWS_SECRET_ACCESS_KEY	
Enter AWS_SECRET_ACCESS_KEY	
AWS_ACCESS_KEY_ID	
Enter AWS_ACCESS_KEY_ID	
AWS_REGION	
Enter AWS_REGION	