AI Translation with Amazon AWS Translate

Introduction

Infradox has implemented an AI Translation interface in Infradox XS websites. This allows you to make use of 3rd party AI API's to automatically translate metadata of the assets on your website into other languages.

This document describes what you need to do to allow the use of the AWS Translate API from Amazon in your Infradox website.

Prerequisites

To start with, you'll need to register an account with Amazon Web Services (AWS) if you don't already have an account there. Please visit <u>https://aws.amazon.com</u> to create an account.

Enable Amazon Translate

Once you have your AWS account set up, you can enable Amazon Rekognition. To do so, visit <u>https://aws.amazon.com/rekognition/resources</u> and follow these steps described in the **Get Started** section:

Step 1 - Create an AWS Account and User in IAM

After creating your AWS account and logging in, go to the Identity and Access Management (IAM) console:

Identity and Access Management (IAM)	×	IAM > Users	
Q Search IAM		Users (4) Info Create user An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.	
Dashboard		Q Search	
Access management	- 8		
User groups	- 8	□ User name ▲ Path ⊽ Group: ⊽ Last activity ⊽	

There you can create a (new) user and accesskey that can be used by your website to access the AWS Translate API:



Leave the *Provide user access to the AWS Management Console* option unchecked. On the next page, choose the *Add user to group* option and use the *Create group* button to create it:

step 1 Specify user details	Set permissions Add user to an existing group or create a new one. Using groups
itep 2 Get permissions	is a best-practice way to manage user's permissions by job functions. Learn more 🖸
itep 3 Review and create	Permissions options
	• Add user to group Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
	Copy permissions Copy all group memberships, attached managed policies, and inline policies from an existing user.
	Attach policies directly Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
	User groups (3) C Create group

reate user group			
Name the group			
User group name Enter a meaningful name to identify this group.			
TranslateAccessGroup			
Maximum 128 characters. Use alphanumeric and	'+=,.@' characters.		
Add users to the group - Option An IAM user is an entity that you create in AWS to	al (4) Info	plication that uses it to	C o interact with AWS.
Q Search			< 1 > ③
🗌 User name 🔀		Groups	Last activity ⊽
User name 🖸 Attach permissions policies - Op You can attach up to 10 policies to this user grou selected policies.	ptional (1/927) Info	Groups	Last activity
User name 🔀 Attach permissions policies - Op You can attach up to 10 policies to this user grou selected policies.	■ ptional (1/927) Info p. All the users in this group Filter by Type	Groups	Last activity ▼ C that are defined in the
□ User name I Attach permissions policies - Op You can attach up to 10 policies to this user grou selected policies. Q translate	otional (1/927) Info p. All the users in this group Filter by Type All types	Groups Groups Owill have permissions 2 matches	Last activity ▼ C that are defined in the < 1 > ③
□ User name I Attach permissions policies - Oµ You can attach up to 10 policies to this user grou selected policies. Q translate → Policy name	ptional (1/927) Info p. All the users in this group Filter by Type C All types Type	Groups Groups Control	Last activity ▼ C that are defined in the < 1 > ③ Description
□ User name [] Attach permissions policies - Oµ You can attach up to 10 policies to this user grou selected policies. Q translate ■ Policy name ■ Policy name ■ Image: TranslateFullAccess	ptional (1/927) Info p. All the users in this group Filter by Type All types Type AWS managed	Groups Group	Last activity ▼ C that are defined in the < 1 > ③ Description Provides full access to
□ User name [] Attach permissions policies - Op You can attach up to 10 policies to this user grouselected policies. Q translate ■ Policy name ● ●	ptional (1/927) Info p. All the users in this group Filter by Type All types Type AWS managed AWS managed	Groups Group Groups	Last activity ▼ C that are defined in the < 1 > ③ Description Provides full access to Provides read-only ac

Assign the policy *TranslateReadOnly* to the user group; this will allow the users in this group to access the API to translate text into other languages.

Click the *Create user group* button and select the created user group in the create user screen when you're returned to the create user page.

Alternatively, you can also link the policy directly to the new user account:

© Xpertise-ICT BV / Infradox



© Xpertise-ICT BV / Infradox

Review and create the account:

Review and create Review your choices. After you create enabled.	the user, you can view and down	lload the autogenerated password, if
User details		
User name TranslateUser	Console password type None	Require password reset No
Permissions summary		< 1 >
Name 🖸 🔺	Type 🗸	7 Used as ♥
TranslateReadOnly	AWS managed	Permissions policy
Tags - optional Tags are key-value pairs you can add to a you want to associate with this user. No tags associated with the resour Add new tag You can add up to 50 more tags.	AWS resources to help identify, organi CC.	ize, or search for resources. Choose any tags
	Cance	el Previous Create user

After the user has been created, click the View user button:



On the user details page, click the *Security credentials* tab and click the *Create access key* button to create an API access key:

C Permissions Groups (1)	ags Security credentials Acce
Console sign-in	Enable console access
Console sign-in link	Console password Not enabled
Access keys (0) Use access keys to send programmatic calls to AWS SDKs, or direct AWS API calls. You can have a maxin time. Learn more	Create access key 5 from the AWS CLI, AWS Tools for PowerShell, AW mum of two access keys (active or inactive) at a
authentication code from an MFA device. Each user assigned. Learn more	can have a maximum or o PirA devices

On the create access key page, choose *Third-party service*:

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.
Use case
Command Line Interface (CLI) You plan to use this access key to enable the AWS CLI to access your AWS account.
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 ECS, 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.

You can ignore the warning message as this is not a root account and it has just read-only access to the Translate API only.

Also creating temporary keys would require you to regularly generate a new key and make sure it's updated on the website too.

	nstead of crea	ting long-term	credentials lik	e access keys, a	nd don't
Confirmati	ion				
I under access	stand the abo key.	ve recommend	lation and wan	t to proceed to	create an

After clicking the *Next* button, you can add a description for the key:

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.
Description tag value Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.
Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: : / = + - @
Cancel Previous Create access key

When you click *Create access key*, the key will be generated:

Retrieve access keys Info
Access key If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.
Access key Secret access key
口 ***************** <u>Show</u>
<
Access key best practices
 Never store your access key in plain text, in a code repository, or in code. Disable or delete access key when no longer needed. Enable least-privilege permissions.
 Never store your access key in plain text, in a code repository, or in code. Disable or delete access key when no longer needed. Enable least-privilege permissions. Rotate access keys regularly. For more details about managing access keys, see the best practices for managing AWS access keys.

You'll need to provide us with these keys (both Access key and Secret access key) to set up the Translate API in your website.

We'll also need to know which AWS region and endpoint you'll be using, e.g.:

Region: eu-west-1 Endpoint: eu-west-1.amazonaws.com