

AI Visual Keywording with Amazon AWS Rekognition

Introduction

Infradox has implemented an AI Visual Keywording interface in Infradox XS websites. This allows you to make use of 3rd party AI API's to generate keywords for your images.

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

Prerequisites

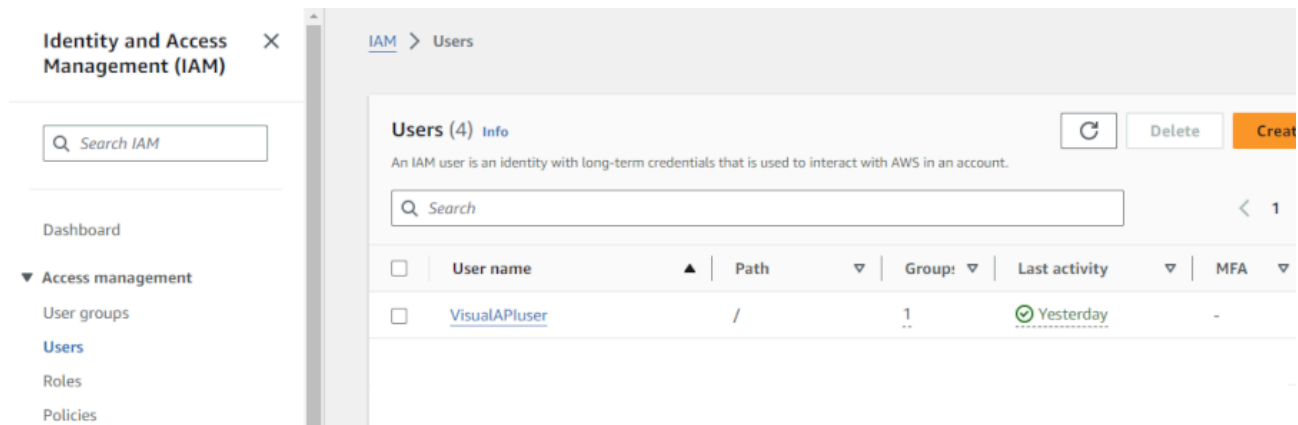
To start with, you'll need to register an account with Amazon Web Services (AWS) if you don't already have an account there. Please visit <https://aws.amazon.com> to create an account.

Enable Amazon Rekognition

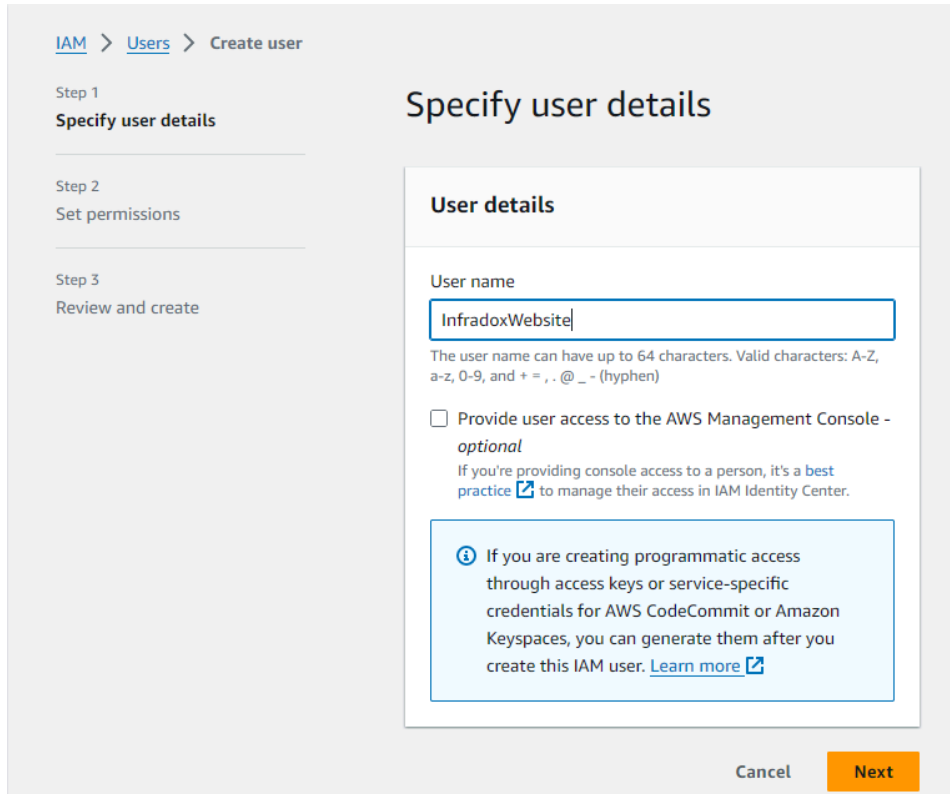
Once you have your AWS account set up, you can enable Amazon Rekognition. To do so, visit <https://aws.amazon.com/rekognition/resources> and follow these steps described in the **Get Started** section:

Step 1 - Create an AWS Account and User in IAM

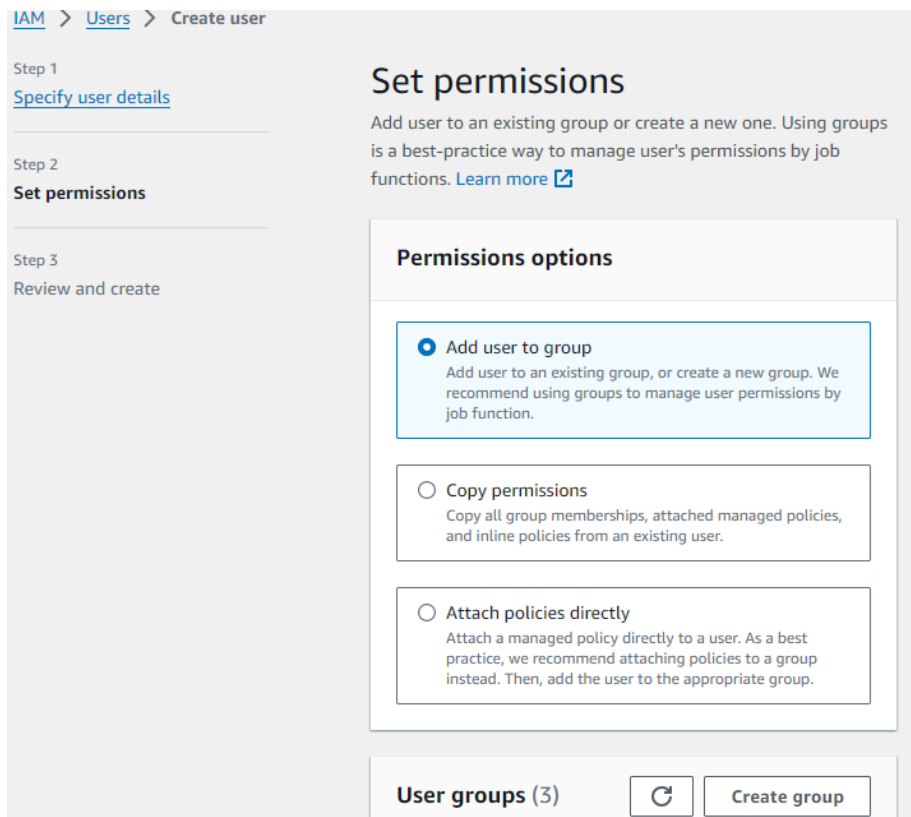
After creating your AWS account and logging in, go to the Identity and Access Management (IAM) console:



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



Create user group ✕

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name
Enter a meaningful name to identify this group.

RekognitionAccessGroup

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Permissions policies (1/927) ↻ Create policy

Filter by Type

✕

All types ▼

4 matches
< 1 >
⚙️

<input type="checkbox"/>	Policy name	Type	Use...	Description
<input type="checkbox"/>	AmazonRekognitionCustomLabelsFu...	AWS managed	None	This policy specif
<input type="checkbox"/>	AmazonRekognitionFullAccess	AWS managed	Permis...	Access to all Ama
<input checked="" type="checkbox"/>	AmazonRekognitionReadOnlyAccess	AWS managed	None	Access to all Reac
<input type="checkbox"/>	AmazonRekognitionServiceRole	AWS managed	None	Allows Rekognitio

Cancel
Create user group

Assign the policy *AmazonRekognitionReadOnlyAccess* to the user group; this will allow the users in this group to access the API to generate keywords based on an image.

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:

🔔 RekognitionAccessGroup user group created.

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 (1/4) ↻ Create group

Search

< 1 >
⚙️

<input type="checkbox"/>	Group name	Users	Atta...
<input type="checkbox"/>	AWSadmins	2	Admini...
<input type="checkbox"/>	DomainManagement	1	Amazo...
<input checked="" type="checkbox"/>	RekognitionAccessGroup	0	Amazo...
<input type="checkbox"/>	VisualAPI	1	Amazo...

▶ Set permissions boundary - optional

Cancel
Previous
Next

Review and create the account:

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name InfradoxWebsite	Console password type None
Require password reset No	

Permissions summary

< 1 >

Name	Type	Used as
RekognitionAccessGroup	Group	Permissions group

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

Cancel Previous **Create user**

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

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

[View user](#)

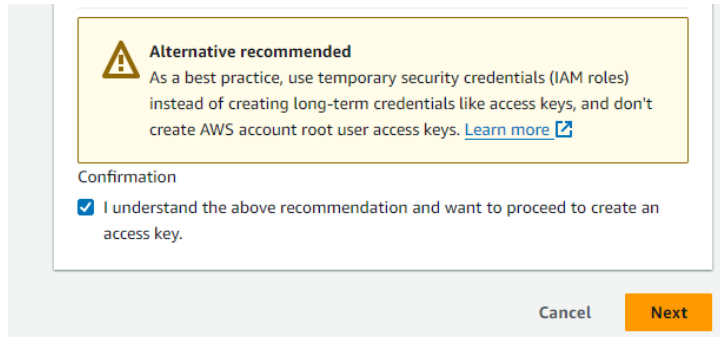
On the user details page, click the *Security credentials* tab and click the *Create access key* button to create an API access key:

The screenshot shows the 'Security credentials' tab selected in the navigation bar. Below the navigation bar, there are two main sections. The first section is 'Console sign-in', which includes an 'Enable console access' button. Below this, there are two fields: 'Console sign-in link' with a copy icon and a partially visible URL 'https://', and 'Console password' which is 'Not enabled'. The second section is 'Access keys (0)', which includes a 'Create access key' button. Below this, there is explanatory text: 'Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more' with a link icon. Below that, there is another line of text: 'authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more' with a link icon.

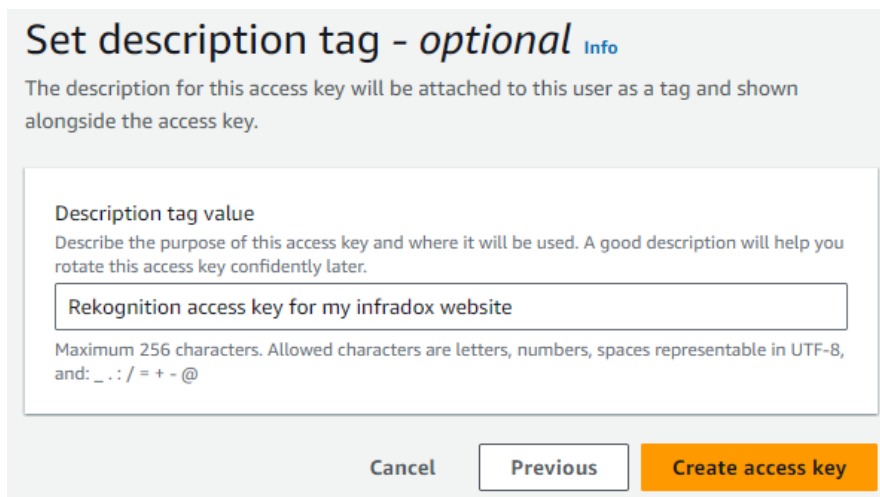
On the create access key page, choose *Third-party service*:

The screenshot shows the 'Access key best practices & alternatives' page. The title is 'Access key best practices & alternatives' with an 'Info' link. Below the title, there is a paragraph: 'Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.' Below this paragraph, there is a 'Use case' section with four radio button options. The first option is 'Command Line Interface (CLI)' with the description 'You plan to use this access key to enable the AWS CLI to access your AWS account.' The second option is 'Local code' with the description 'You plan to use this access key to enable application code in a local development environment to access your AWS account.' The third option is 'Application running on an AWS compute service' with the description '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.' The fourth option is 'Third-party service' with the description 'You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.' The 'Third-party service' option is selected, indicated by a blue dot and a blue border around its box.

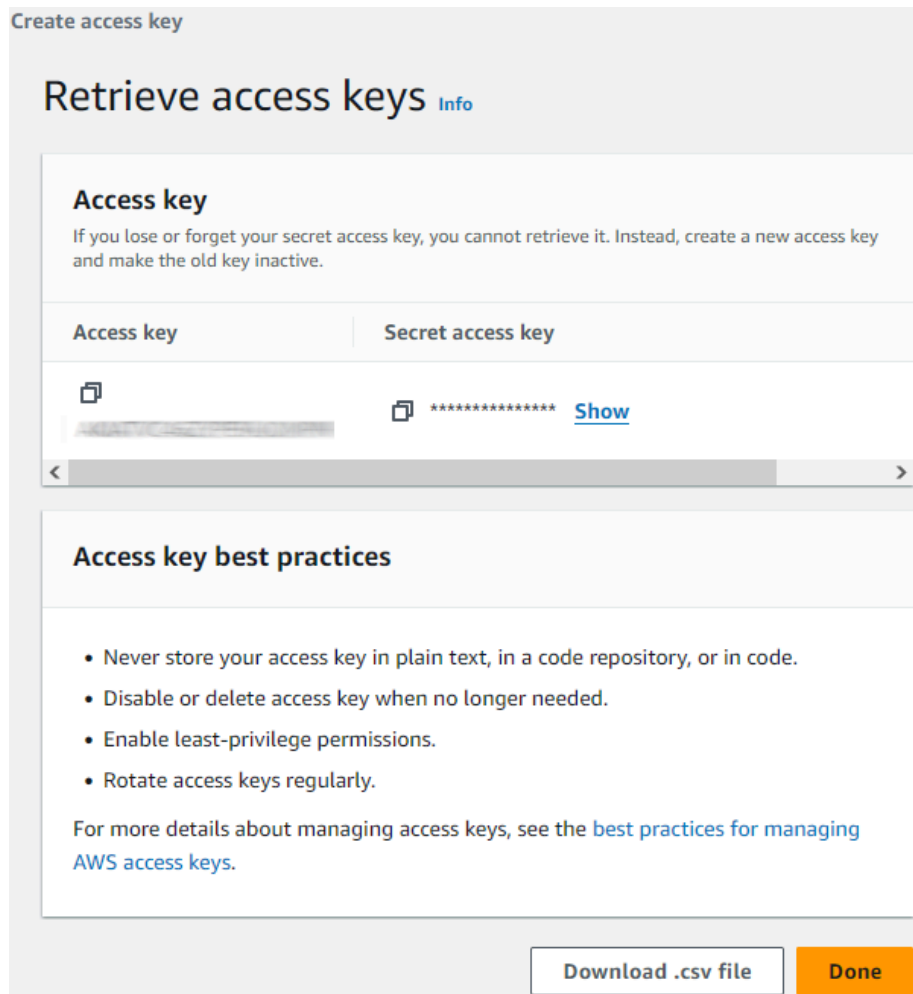
You can ignore the warning message as this is not a root account and it has just read-only access to the Rekognition API only.
Also creating temporary keys would require you to regularly generate a new key and make sure it's updated on the website too.



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



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



You'll need to provide us with these keys (both Access key and Secret access key) to set up the Rekognition 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: rekognition.eu-west-1.amazonaws.com