

How to create a new Amazon AWS access key

Author : Dan Nanni

Categories : [Cloud Services](#), [Security](#)

Tagged as : [aws](#)

Question: I was asked to provide an **AWS access key ID** and **secret access key** when configuring an application which requires access to my Amazon AWS account. How can I create a new AWS access key?

Amazon AWS security credentials are used to authenticate you and authorize any third-party application to access your AWS account. There are different types of AWS security credentials available, e.g., password, access key, multi-factor authentication, X.509 certificates, etc.

If you want to create a new access key (access key ID and secret access key), here is how to do it.

First, log in to [AWS console](#).

Choose "Security Credentials" menu from the top bar.



In the next page, choose "Access Keys (Access Key ID and Secret Access Key) option.

Ask Xmodulo

Find answers to commonly asked Linux questions

<http://ask.xmodulo.com>

Dashboard

Services ▾ Edit ▾

Dan Nanni ▾ Global ▾ Help ▾

Dashboard

Details

Groups

Users

Roles

Identity Providers

Password Policy

Credential Report

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- + Password
- + Multi-Factor Authentication (MFA)
- + Access Keys (Access Key ID and Secret Access Key)
- + CloudFront Key Pairs
- + X.509 Certificates
- + Account Identifiers

In the next page, you will see a list of existing access key IDs (if any). Note that you cannot retrieve "secret access keys" of existing access key IDs. For security reason, a secret access key is visible only at the time you create a new access key.

+ Password

+ Multi-Factor Authentication (MFA)

- Access Keys (Access Key ID and Secret Access Key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

Created	Deleted	Access Key ID	Status	Actions
Sep 6th 2014		[REDACTED]	Active	Make Inactive Delete
Sep 7th 2014	Sep 7th 2014	[REDACTED]	Deleted	

[Create New Access Key](#)

Click on "Create New Access Key", and it will create a new pair of access key ID and secret access key

Ask Xmodulo

Find answers to commonly asked Linux questions
<http://ask.xmodulo.com>

instantly.

Create Access Key ✕

✔ Your access key (access key ID and secret access key) has been created successfully.

Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

To help protect your security, store your secret access key securely and do not share it.

▼ [Hide Access Key](#)

Access Key ID: [REDACTED]

Secret Access Key: [REDACTED]

[Download Key File](#) [Close](#)

Either download a key file which contains a new access key, or copy and paste a new access key information. Again remember. Once you close this window, the secret access key will not be available again unless you download a key file.

Multi-User AWS Account

If you are a corporate which has a corporate AWS account shared by multiple employees, you may want to use Identity and Access Management (IAM) to create and manage their access keys.

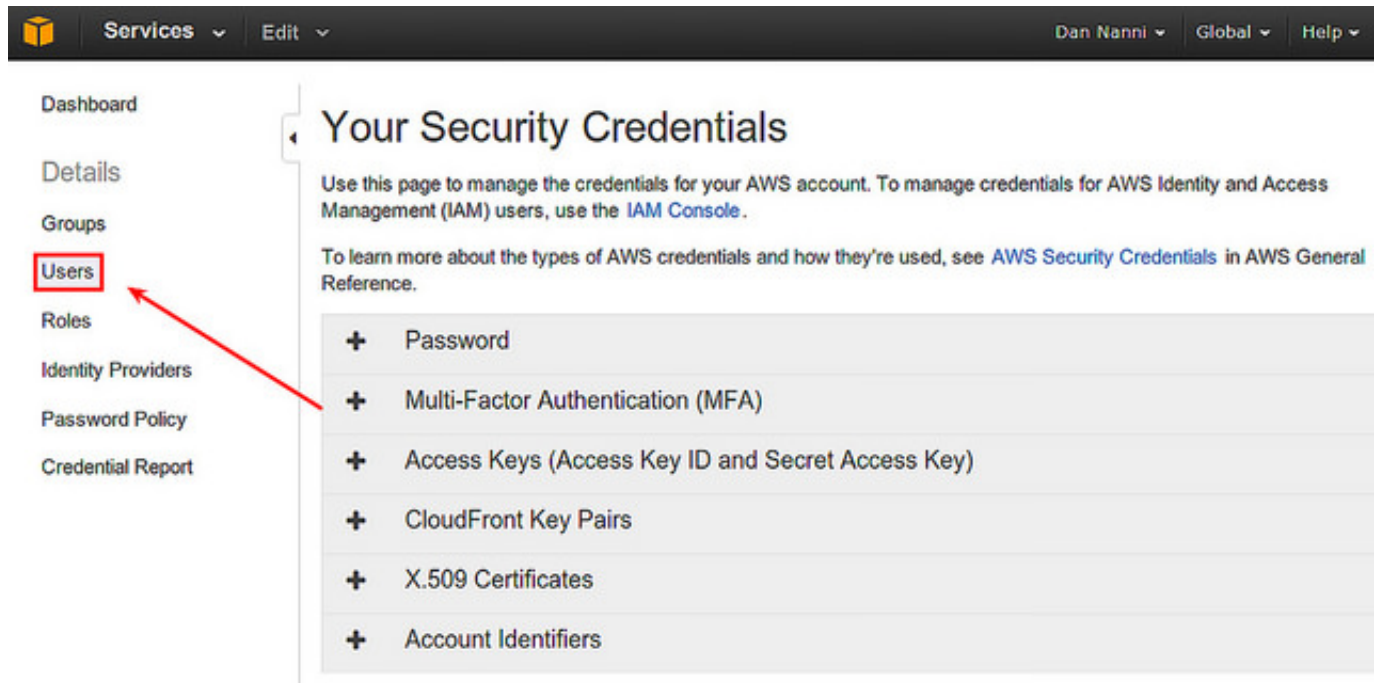
IAM is a web service which allows a corporate to manage multiple users and their associated security credentials under a single AWS account. Using IAM, multiple users can sign in as different identities under a single AWS account, and manage their own security credentials without tampering with each other's keys.

To manage IAM users, click on "Users" menu on the "Security Credentials" page.

Ask Xmodulo

Find answers to commonly asked Linux questions

<http://ask.xmodulo.com>



Services Edit Dan Nanni Global Help

Dashboard

Details

Groups

Users

Roles

Identity Providers

Password Policy

Credential Report

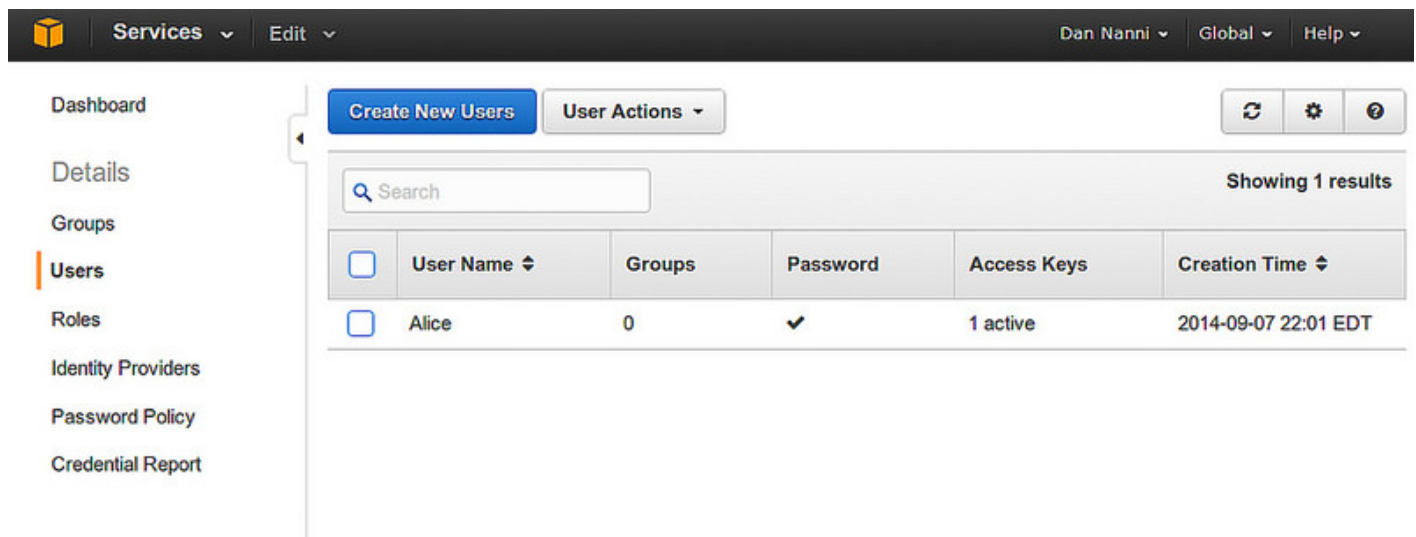
Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- + Password
- + Multi-Factor Authentication (MFA)
- + Access Keys (Access Key ID and Secret Access Key)
- + CloudFront Key Pairs
- + X.509 Certificates
- + Account Identifiers

Then you can create a new IAM user and manage their security credentials such as access keys.



Services Edit Dan Nanni Global Help

Dashboard

Details

Groups

Users

Roles

Identity Providers

Password Policy

Credential Report

Create New Users User Actions

Search Showing 1 results

<input type="checkbox"/>	User Name ↕	Groups	Password	Access Keys	Creation Time ↕
<input type="checkbox"/>	Alice	0	✓	1 active	2014-09-07 22:01 EDT