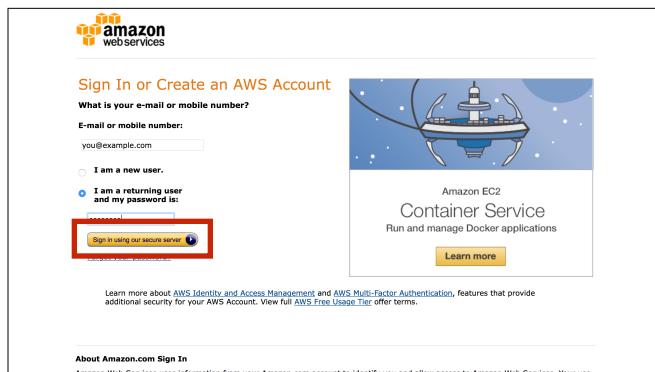
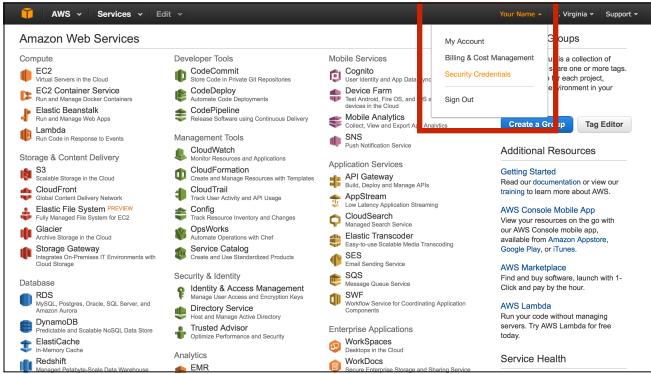


Login (or create an account) on AWS at <https://console.aws.amazon.com>. You may be charged a small amount (a few cents) for this tutorial.



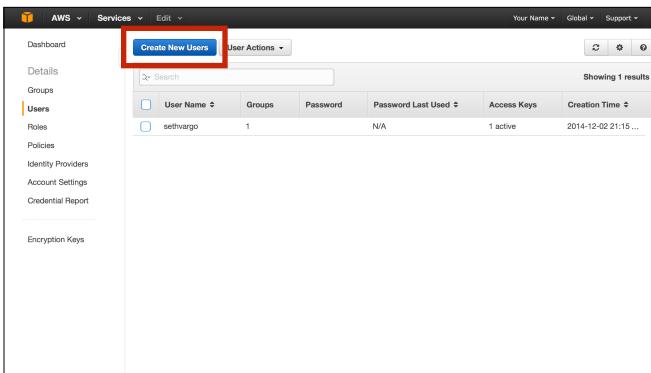
Enter your username and password (or desired username and password if you do not already have an account) and click "Sign in".

- If you are an existing user with 2FA enabled, you will need to enter your 2FA code. Please do so.
- If you are a new user, you may be asked to verify yourself via telephone. Please do so.
- If you are a new user, you may be asked for a credit card. Please supply one. The tutorial will cost a few cents.
- If you are a new user, you may be asked to choose a support plan. Please choose "none" (or the one that costs nothing).



Once you login and verify your account, you should see a screen like this. This is the management console dashboard.

In the upper right-hand corner, click on <Your Name> and choose "Security Credentials" from the dropdown.



You should see a page like this. If you see a notification popup about IAM users, click "Take me to IAM user management".

Click the "Create New Users" button at the top.

AWS Services Edit Your Name Global Support

Create User

Enter User Names:

1 tutorial
2
3
4
5

Maximum 64 characters each

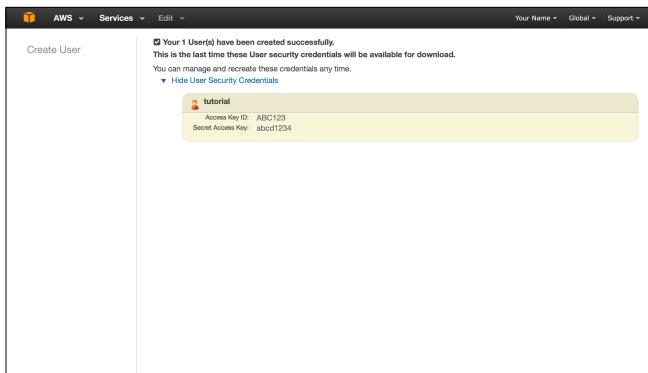
Generate an access key for each user

Users need access keys to make secure REST or Query protocol requests to AWS service APIs.

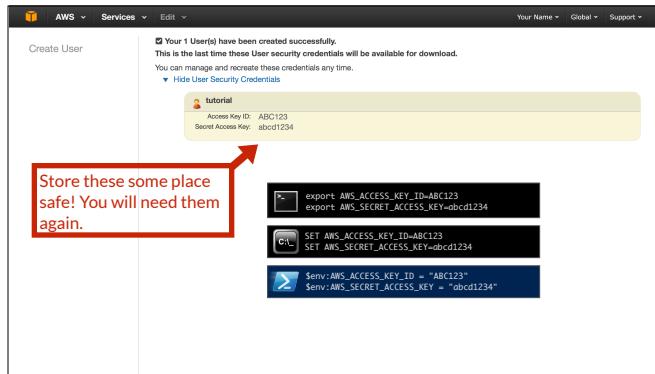
For users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard.

Cancel Create

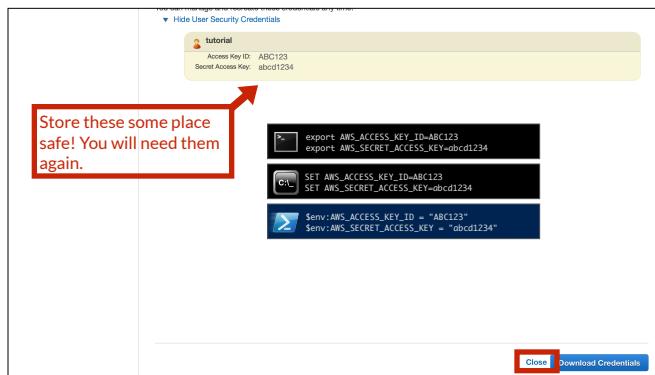
You can create multiple users at a time, but we only need one user for this tutorial. I have named the user "tutorial", but you can name it whatever you would like. When you are finished, click "Create" at the bottom.



Next, you will see the user's credentials. You may need to click the text to make it appear. The Access Key ID and Secret Access Key should be treated like a username and password. Do not share them.



Store these keys in a safe place. We usually recommend storing them in something like 1Password or LastPass. We will use these keys in the tutorial.

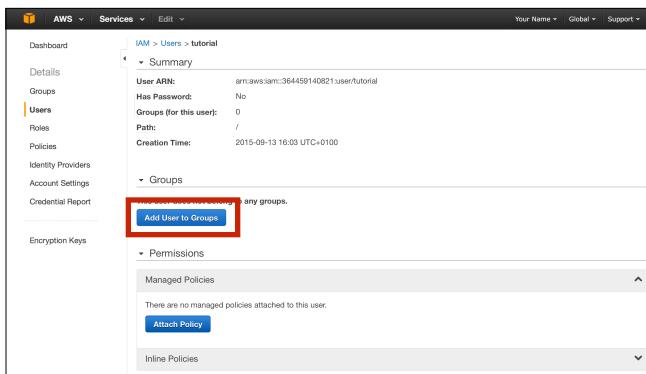


When you are done, click "Close" on the bottom.

Create New Users					
User Actions					
Showing 2 results					
User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
sethvargo	1	N/A	1 active	2014-12-02 21:15 ...	
tutorial	0	N/A	1 active	2015-09-13 16:03 ...	

We have successfully created the user, but that user has no permissions in our environment. We need to grant the proper permissions on the user in order to manage resources.

Click on the row named "tutorial" (or whatever you named the user).



The screenshot shows the AWS IAM User Details page for a user named 'tutorial'. The 'Groups' section is expanded, showing that the user is currently not assigned to any groups. A prominent blue button labeled 'Add User to Groups' is visible, with a red box drawn around it to indicate it as the next step. Other sections like 'Permissions' and 'Managed Policies' are also visible but not interacted with in this specific view.

Click "Add User to Groups"

The screenshot shows the 'Attach Policy' interface in the AWS IAM service. At the top, there's a header with 'AWS Services Edit' and dropdowns for 'Your Name', 'Global', and 'Support'. Below the header, the title 'Attach Policy' is displayed. A note says 'Select one or more policies to attach. Each user can have up to 10 policies attached.' A search bar and a filter dropdown ('Policy Type') are also present. The main area is a table titled 'Showing 150 results' with columns: 'Policy Name', 'Attached Entities', 'Creation Time', and 'Edited Time'. The first row, 'AdministratorAccess', has a checked checkbox in the 'Attached Entities' column. Other rows represent various AWS services like API Gateway, AppStream, Cognito, and DynamoDB.

Policy Name	Attached Entities	Creation Time	Edited Time
AdministratorAccess	0	2015-02-06 18:39 UTC	2015-02-06 18:39 UTC
AmazonAPIGatewayAdmin...	0	2015-07-09 18:34 UTC-01...	2015-07-09 18:34 UTC...
AmazonAPIGatewayInvoke...	0	2015-07-09 18:36 UTC-01...	2015-07-09 18:36 UTC...
AmazonAppStreamFull...	0	2015-02-06 18:40 UTC	2015-02-06 18:40 UTC
AmazonAppStreamRead...	0	2015-02-06 18:40 UTC	2015-02-06 18:40 UTC
AmazonAppStreamDevelop...	0	2015-03-24 17:22 UTC	2015-03-24 17:22 UTC
AmazonCognitoPowerUser	0	2015-03-24 17:14 UTC	2015-03-24 17:14 UTC
AmazonCognitoReadOnly	0	2015-03-24 17:06 UTC	2015-03-24 17:06 UTC
AmazonORSVPCManager...	0	2015-09-02 01:09 UTC-01...	2015-09-02 01:09 UTC...
AmazonDynamoDBFull...	0	2015-02-06 18:40 UTC	2015-02-06 18:40 UTC
AmazonDynamoDBFull...	0	2015-02-06 18:40 UTC	2015-02-06 18:40 UTC
AmazonDynamoDBRead...	0	2015-02-06 18:40 UTC	2015-02-06 18:40 UTC
AmazonDynamoDBWrite...	0	2015-02-06 18:40 UTC	2015-02-06 18:40 UTC

Find the group named "AdministratorAccess" and check the box next to it.

Please note, for the purposes of this tutorial, we are creating an administrator user. In a real production scenario, you would likely create an IAM policy with stricter permissions.

This screenshot shows the same 'Attach Policy' interface as the first one, but with a red box highlighting the 'Attach Policy' button at the bottom right of the page. The rest of the interface is identical to the first screenshot.

Click "Attach Policy" at the bottom.

The screenshot shows the AWS IAM 'Users' section. A user named 'tutorial' has been created. The 'Managed Policies' table lists a single policy, 'AdministratorAccess', which is highlighted with a red border. The 'Actions' column for this policy contains three buttons: 'Show Policy', 'Detach Policy', and 'Simulate Policy'.

Policy Name	Actions
AdministratorAccess	Show Policy Detach Policy Simulate Policy

Verify that "Administrator Access" is displayed under the list of policies.

That's it! You have successfully created an IAM user for this tutorial. Please be sure to keep your credentials in a secure place.