lab

lab title

# AWS Identity and Access Management (IAM)

## V1.07

Course title

BackSpace Academy
AWS Certified Associate

BackSpace

# Table of Contents

## Contents

Table of Contents ..... 1
About the Lab ..... 2
Creating an IAM User ..... 3
Creating an IAM Group ..... 6
    Adding a User to a Group ..... 7
Setting a Password Policy ..... 9
    Setting an initial user password ..... 9
    Setting an account password policy ..... 10
Creating an IAM Role ..... 12
Creating an Account Alias ..... 14
Creating a Credentials Report ..... 16
    Clean Up ..... 16
Implementing Multi Factor Authentication (MFA) ..... 17
    Adding account using Authy Desktop app: ..... 20
    Adding account using Authy Mobile app: ..... 21
    Entering Authentication codes ..... 21
    Implementing MFA on an IAM User ..... 23
    What to do if you are locked out of your root account ..... 24


Copyright all rights reserved - BackSpace.Academy

# About the Lab

**Please note that not all AWS services are supported in all regions. Please use the US-East-1 (North Virginia) region for this lab.**

These lab notes are to support the hands on instructional videos of the Identity and Access Management (IAM) section of the AWS Certified Associate Course.

**Please note that AWS services change on a weekly basis and it is extremely important you check the version number on this document to ensure you have the lastest version with any updates or corrections.**

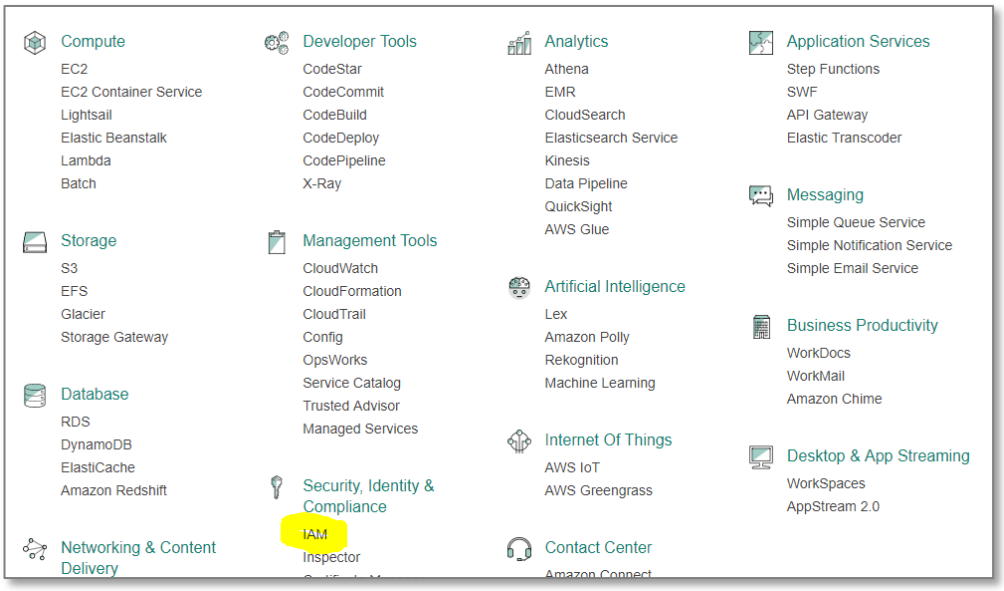
Copyright all rights reserved - BackSpace.Academy

# Creating an IAM User

**In this section, we will use the Identity and Access Management (IAM) service to create a user with console access and programmatic access.**

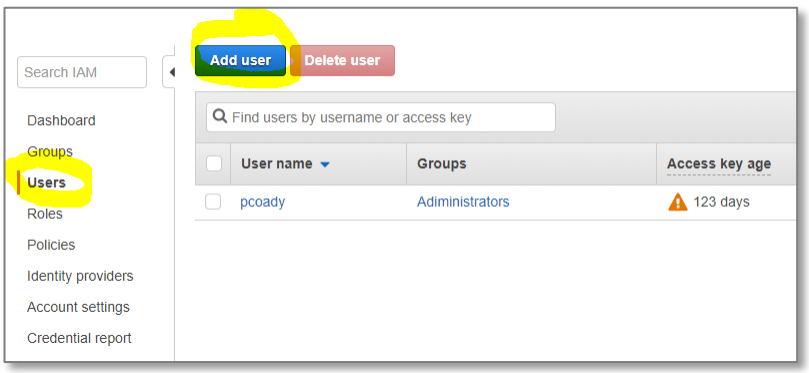
From the AWS console click 'Services"

Select 'IAM" from the Security, Identity & Compliance services.




Select 'Users"

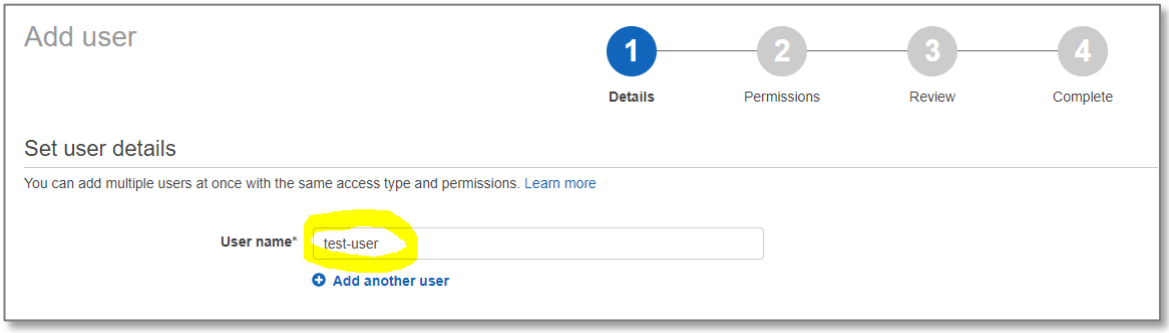
Click 'Add user"




Give the user a name

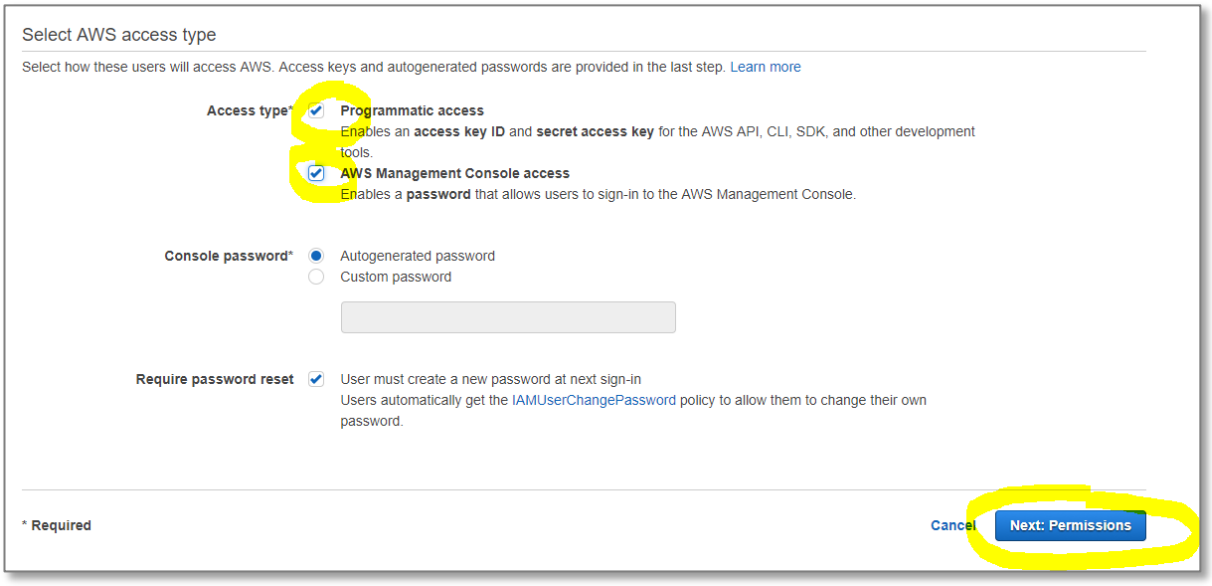


Copyright all rights reserved - BackSpace.Academy



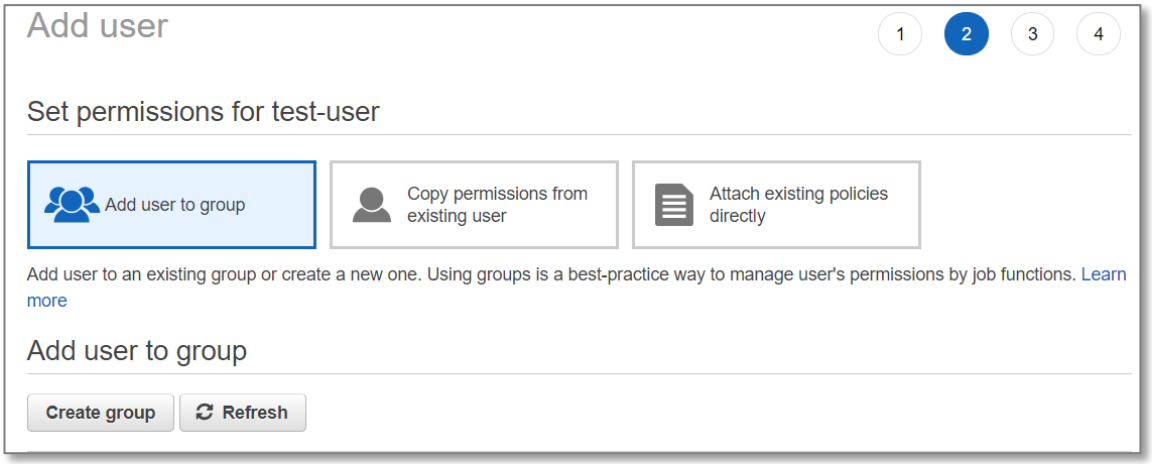

Check 'Programmatic access"

Check 'AWS Management Console access"

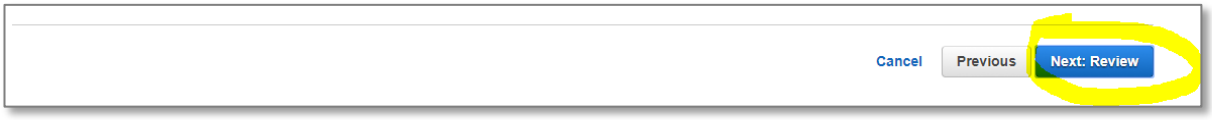



We won't set any permissions for the user at this point.

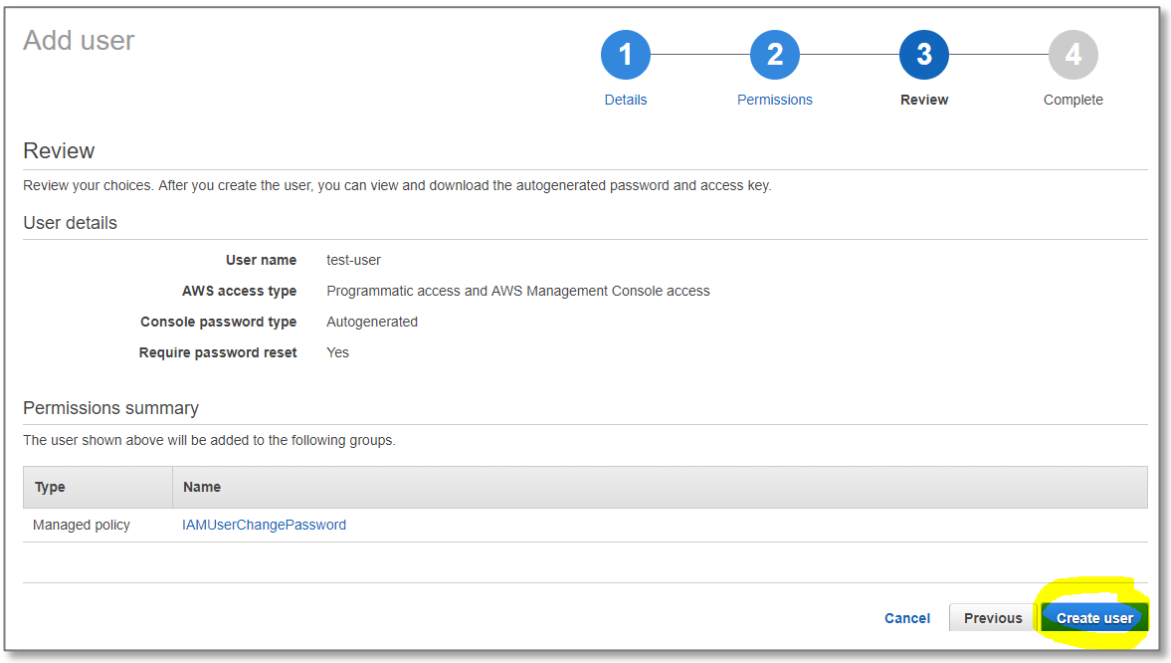
Click 'Next Review"




Copyright all rights reserved - BackSpace.Academy

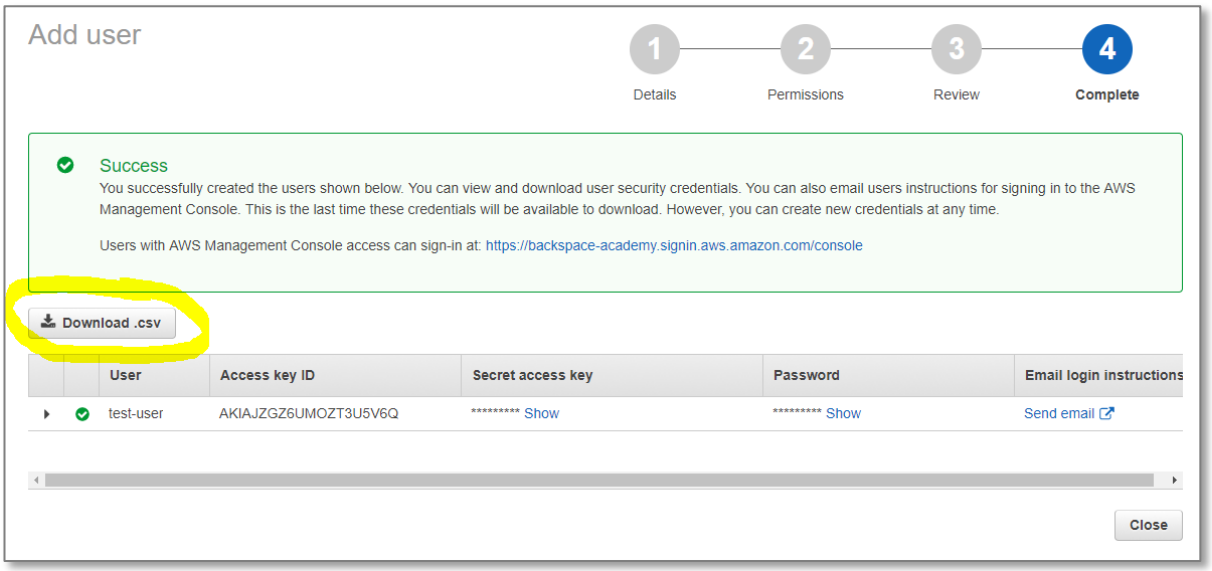



Click 'Create user"




Download the csv file containing the user credentials (access key and secret access key) to a safe location.

You will need this for access using the Command Line Interface (CLI) later in the course.





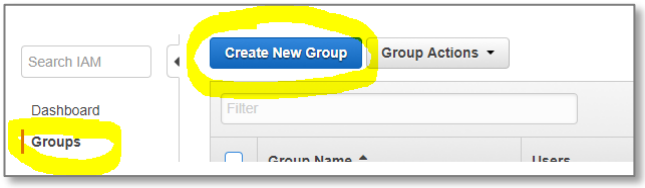
Copyright all rights reserved - BackSpace.Academy

# Creating an IAM Group

**In this section, we will use the Identity and Access Management (IAM) service to create a group with administrator access. We will also add our newly created user to the group.**

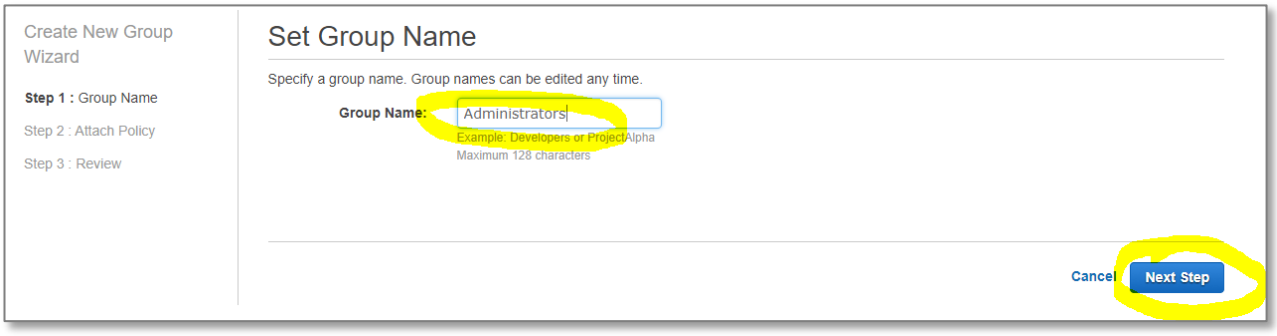
Select 'Group"

Click 'Create New Group"




Give the group a name

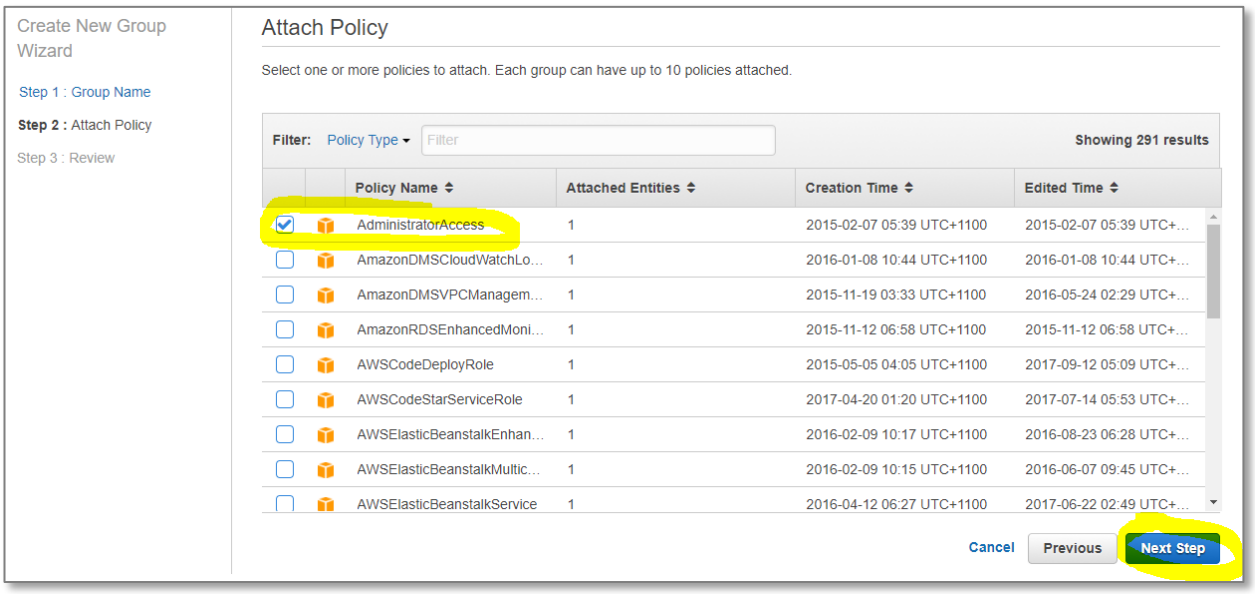
Click 'Next Step"



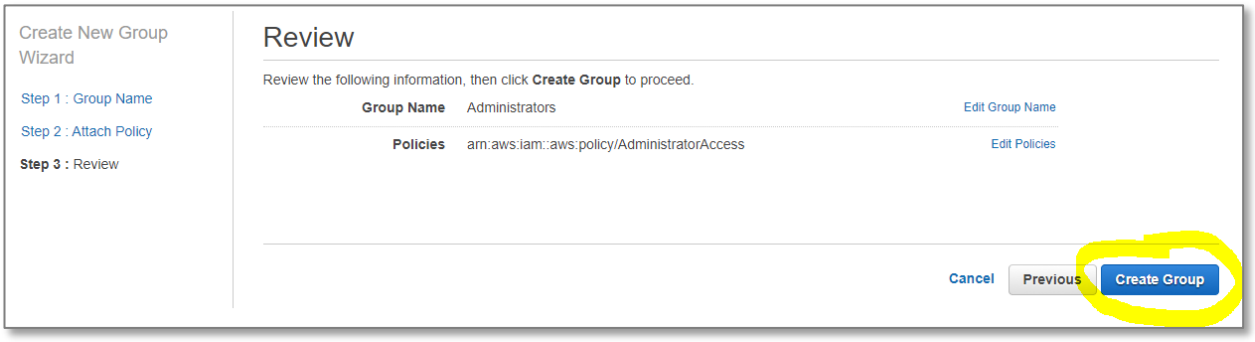

Select the 'AdministratorAccess" policy

Click 'Next Step"

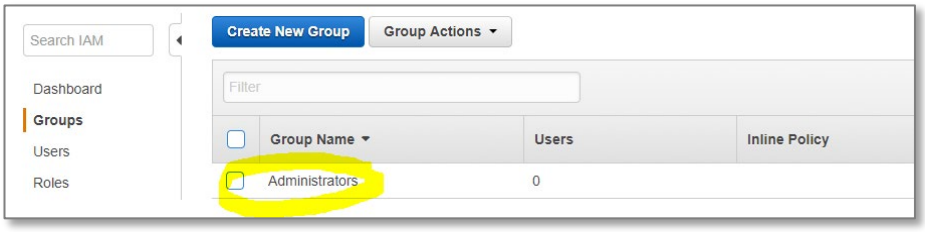
Copyright all rights reserved - BackSpace.Academy




Click 'Create Group"




The Group has been created

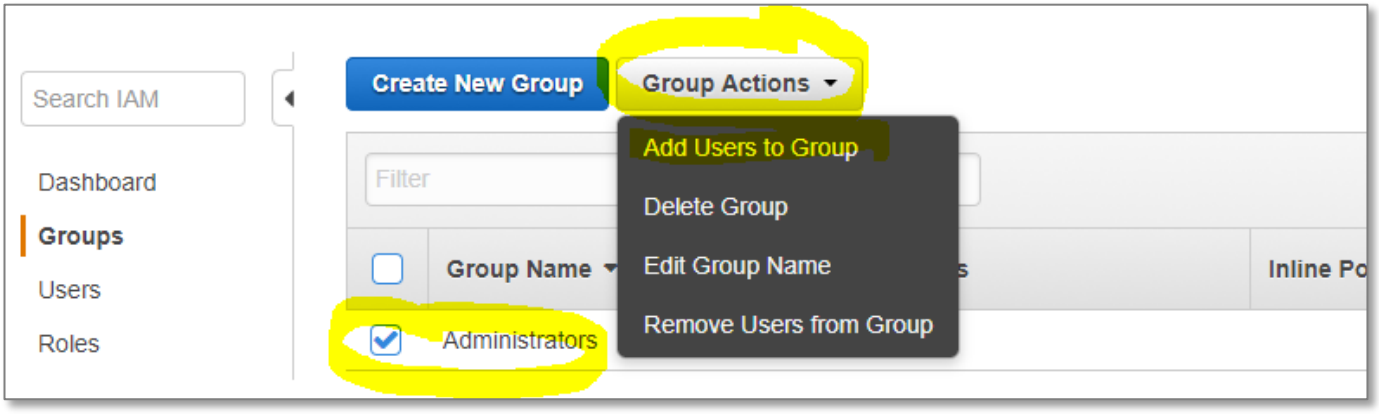



## Adding a User to a Group

Select the group

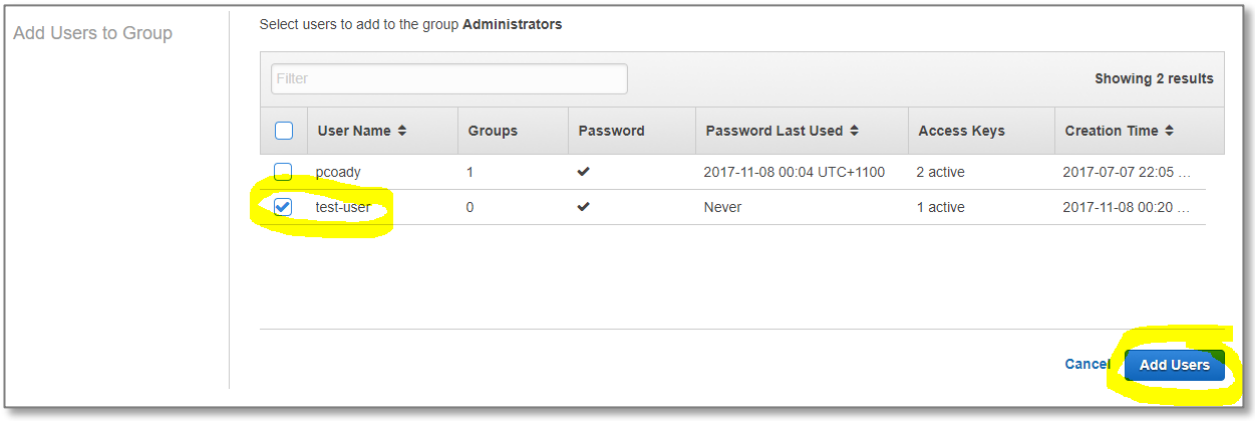
Click 'Group Actions" – 'Add users to group"


Copyright all rights reserved - BackSpace.Academy




Select the newly created user

Click 'Add Users"




Copyright all rights reserved - BackSpace.Academy

# Setting a Password Policy

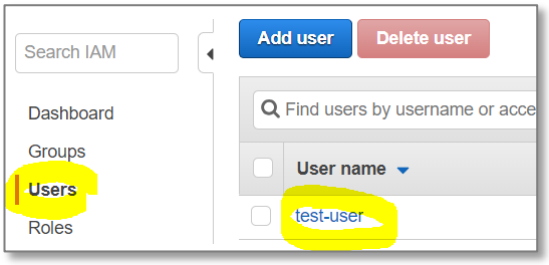
**In this section, we will use the Identity and Access Management (IAM) service to set a password policy for our account and also set initial password details of an IAM user.**

## Setting an initial user password

First we will setup the initial password for our new user.

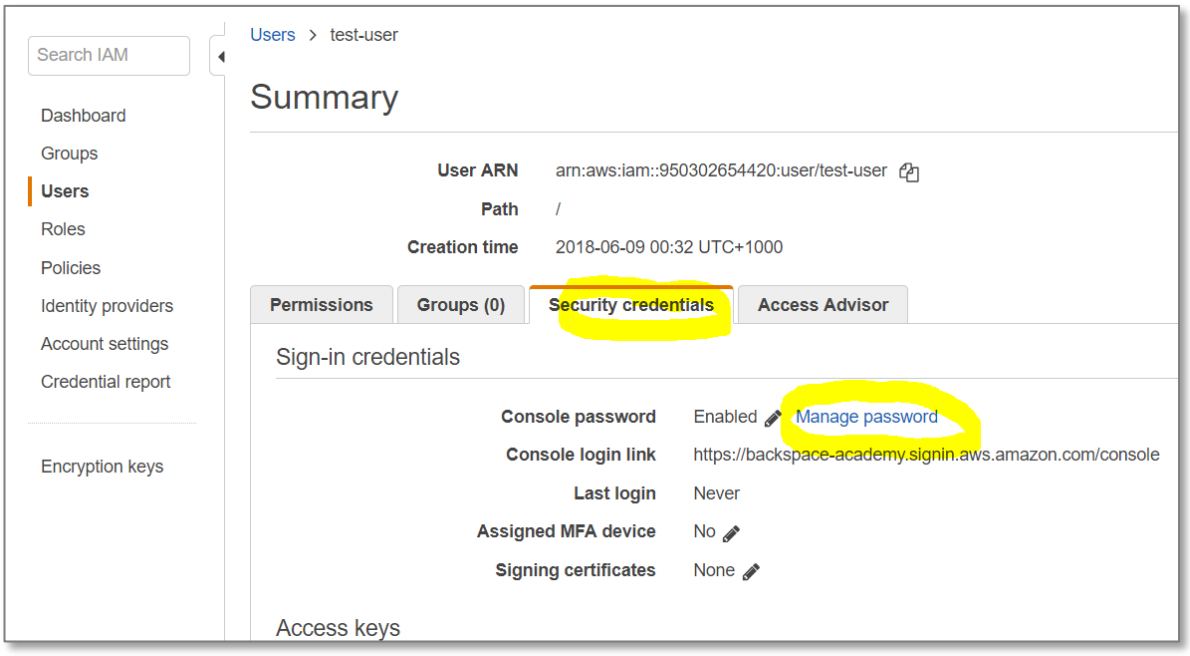
Select 'Users"

Select our new user.




Select 'Security Credentials"

Click 'Manage password"



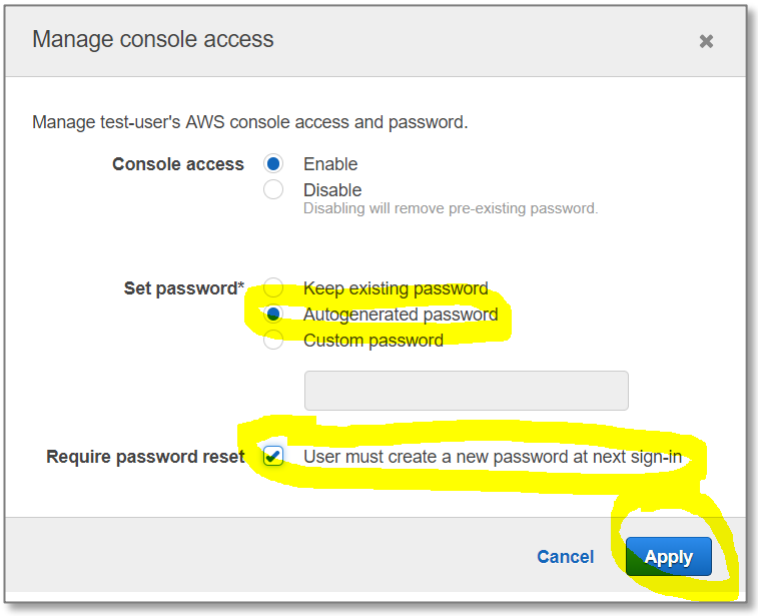



Copyright all rights reserved - BackSpace.Academy

Select 'Autogenerated password"

Select 'User must create a new password at next sign-in"

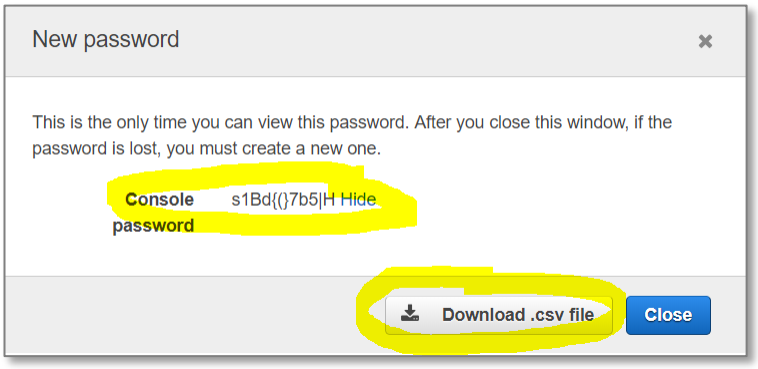
Click 'Apply"




Click on 'Show" to see the password.

If you click 'Download .csv file" you will download a file containing the login details. These details can be given to the user.

Take note '*This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.*"



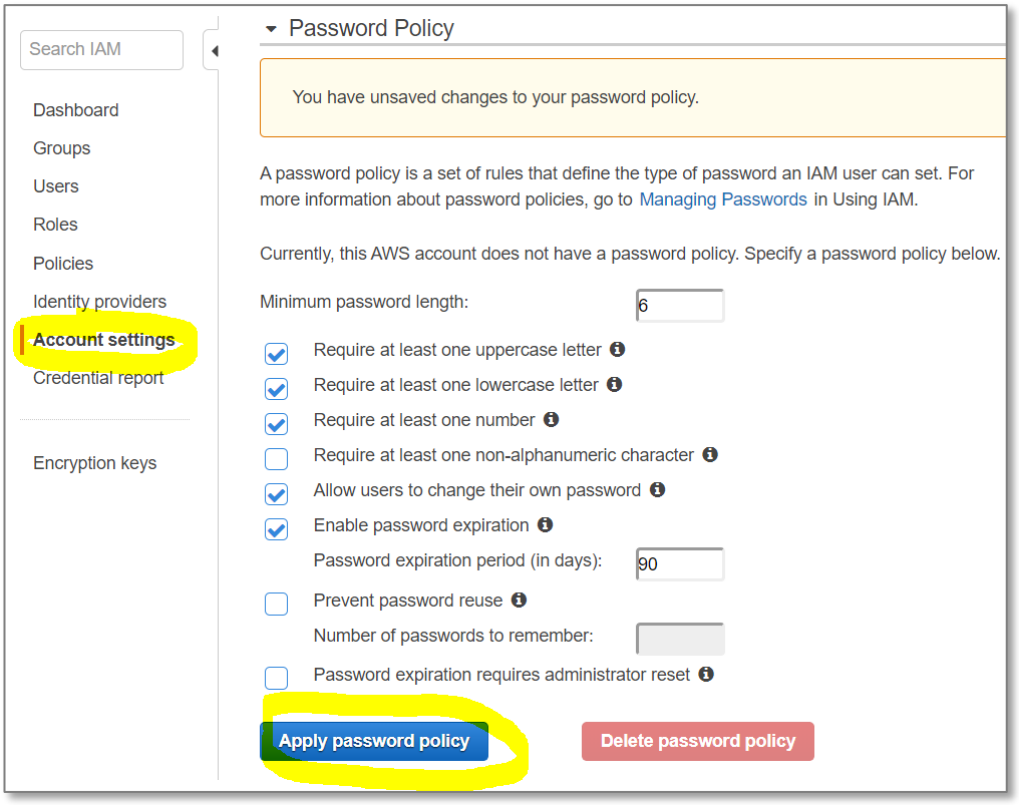

## Setting an account password policy

Select 'Account settings"

From here you can set a password policy for the account.

Copyright all rights reserved - BackSpace.Academy

Click 'Apply password policy"

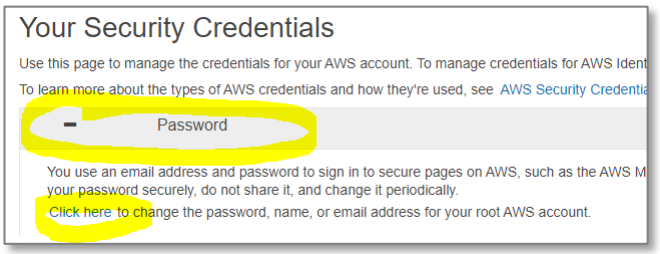



Now make sure your root user account conforms to the password policy

Sign out of your account

Sign in using root account credentials

Go to 'My security credentials"




Finish up by signing out of your root user account and signing back in as an IAM user.

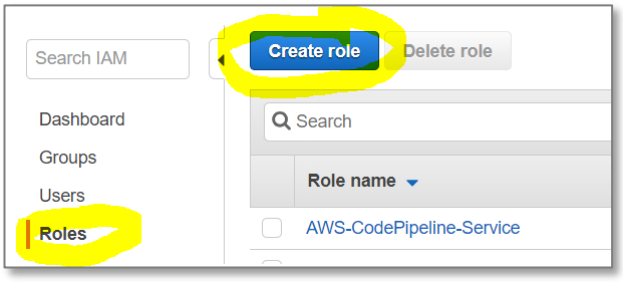

Copyright all rights reserved - BackSpace.Academy

# Creating an IAM Role

**In this section, we will use the Identity and Access Management (IAM) service to create an IAM role for an EC2 instance. This will allow EC2 instances running on our account to access other services on our account.**

Select 'Roles"

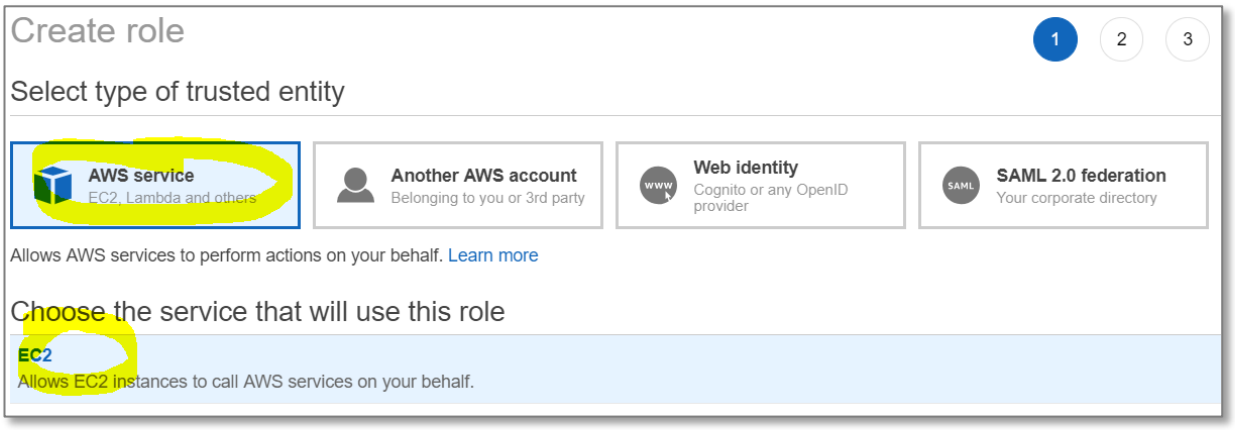
Click 'Create role"




Select 'AWS service"

Select 'EC2"

Click 'Next: Permissions"



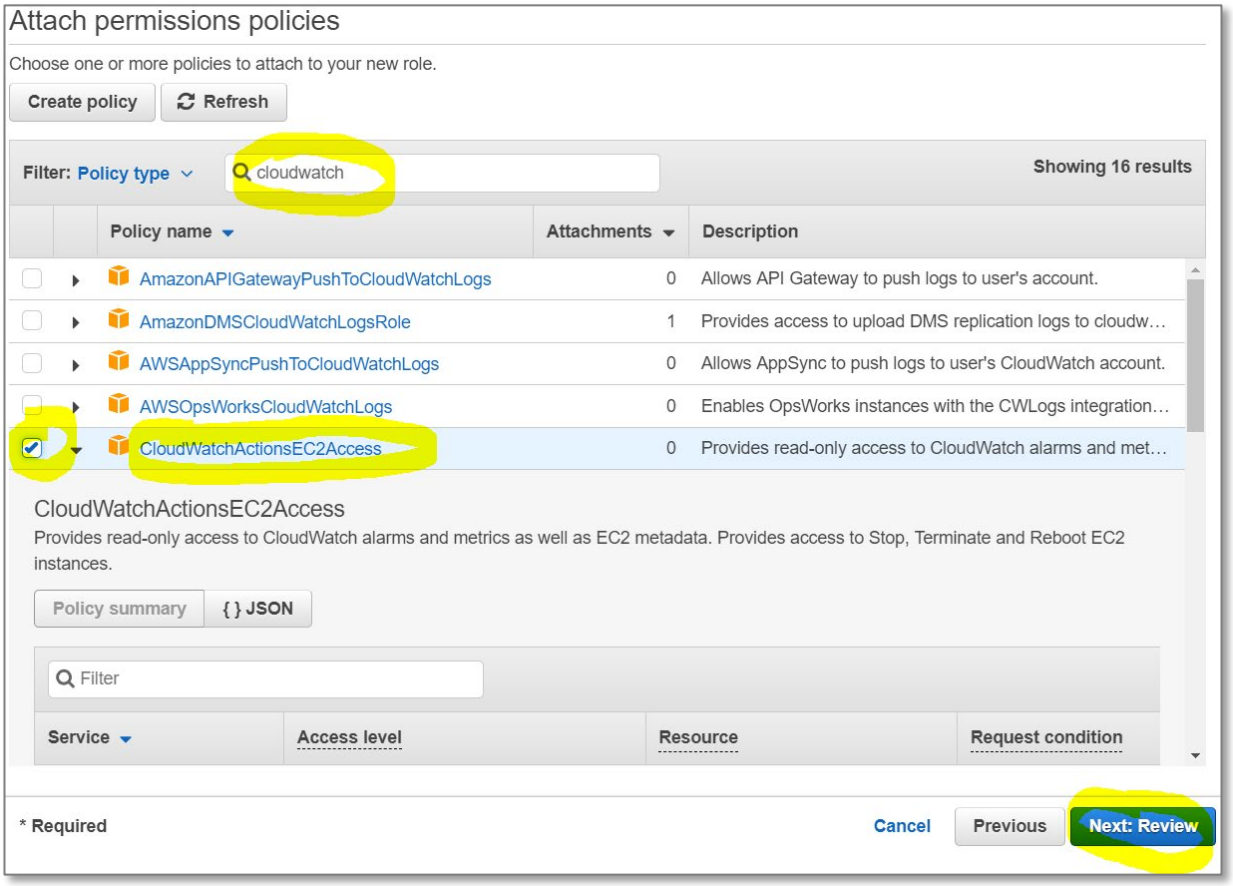

Search for a policy for CloudWatch access

Select 'CloudWatchActionsEC2Access"

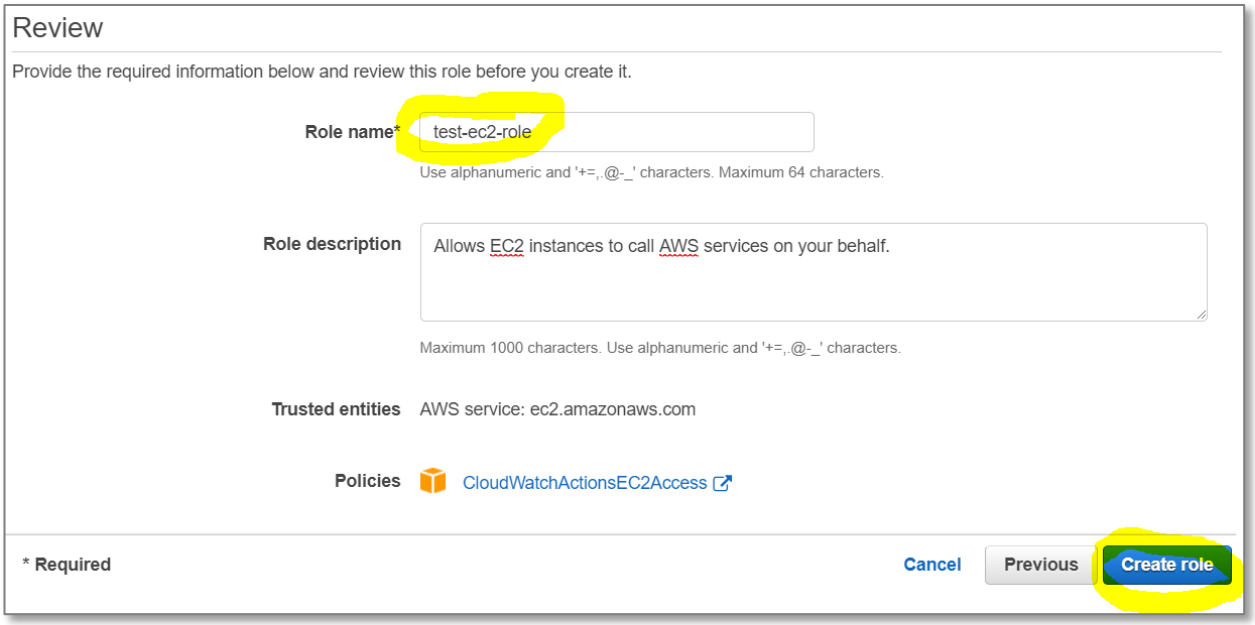
Note in a real environment you would select a policy that 'grants least privilege". In other words you would attach a policy that only allows access to the service required.

Copyright all rights reserved - BackSpace.Academy

Click 'Next; Review"




Give your role a name and click 'Create Role"





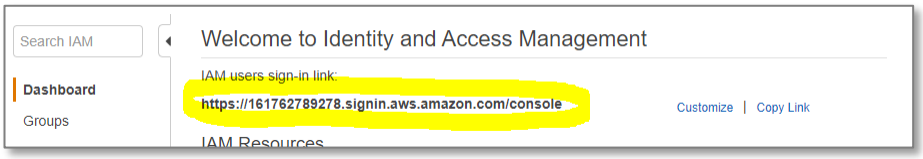

Copyright all rights reserved - BackSpace.Academy

# Creating an Account Alias

**In this section, we will use the Identity and Access Management (IAM) service to create an alias for our account. This will simplify the login process for our users.**

Go to the IAM Dashboard

Here you can see the login url requires the account number.

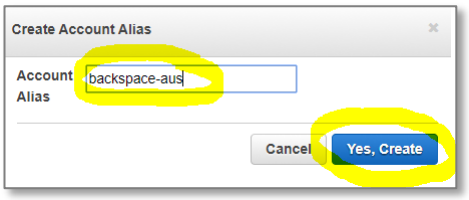



Creating an account alias makes it easier for users to remember the account to login to.

Click 'Customize"

Create a unique alias name

Click 'Yes, Create"




We can now use the account alias for logging in.

Copyright all rights reserved - BackSpace.Academy

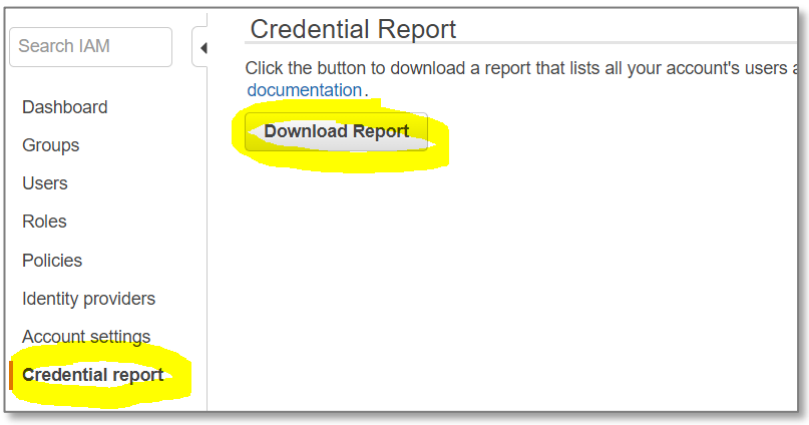
Copyright all rights reserved - BackSpace.Academy

# Creating a Credentials Report

**In this section, we will use the Identity and Access Management (IAM) service to create a Credentials Report of our account. This can be used to identify accounts that should be removed or have privileges changed.**

Select 'Credential report"

Click 'Download Report"




Open the report to see information on the new user and root accounts.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | user | arn | user_creat | password_ | password_ | password_ | password_ | mfa_activ | access_ke | access_ke | access_ke | access_ke | access_ke | access_ke | access_ke | ac |
| 2 | <root_acc | arn:aws:ia | 2017-07-0 | not_suppo | 2017-10-1 | not_suppo | not_suppo | FALSE | FALSE | N/A | N/A | N/A | N/A | FALSE | N/A | N/ |
| 3 | test-user | arn:aws:ia | 2018-06-0 | TRUE | no_inform | 2018-06-0 | N/A | FALSE | TRUE | 2018-06-0 | N/A | N/A | N/A | FALSE | N/A | N/ |
| 4 | | | | | | | | | | | | | | | | |

## Clean Up

IAM is a free service so there is no need to clean up to avoid a bill.

Copyright all rights reserved - BackSpace.Academy

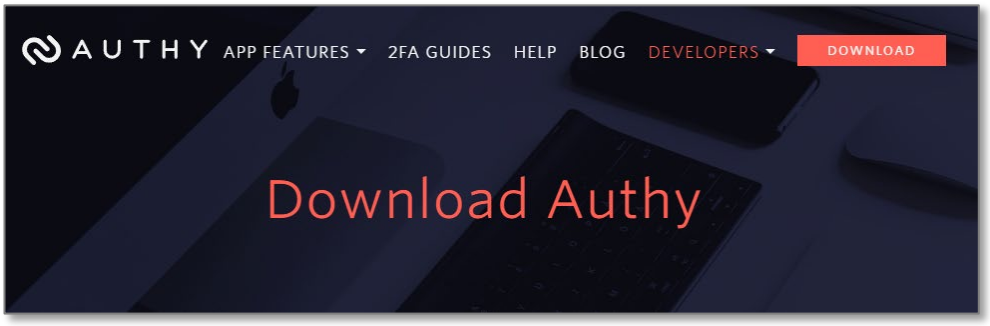
# Implementing Multi Factor Authentication (MFA)

**In this section, we will use the Identity and Access Management (IAM) service to implement multi factor authentication (MFA) for root access on our account.**

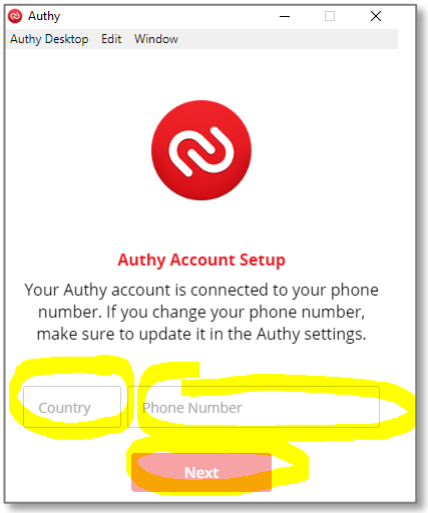
Download and install Authy to your desktop or mobile.

It is recommended to install it on mobile and desktop in case the app is accidently deleted.

https://authy.com/download/

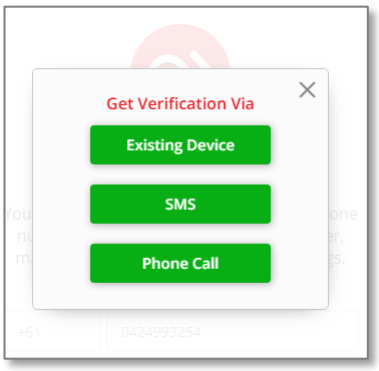



Enter your phone number details




Verify by 'SMS" (mobile phone) or 'Phone Call" (landline)

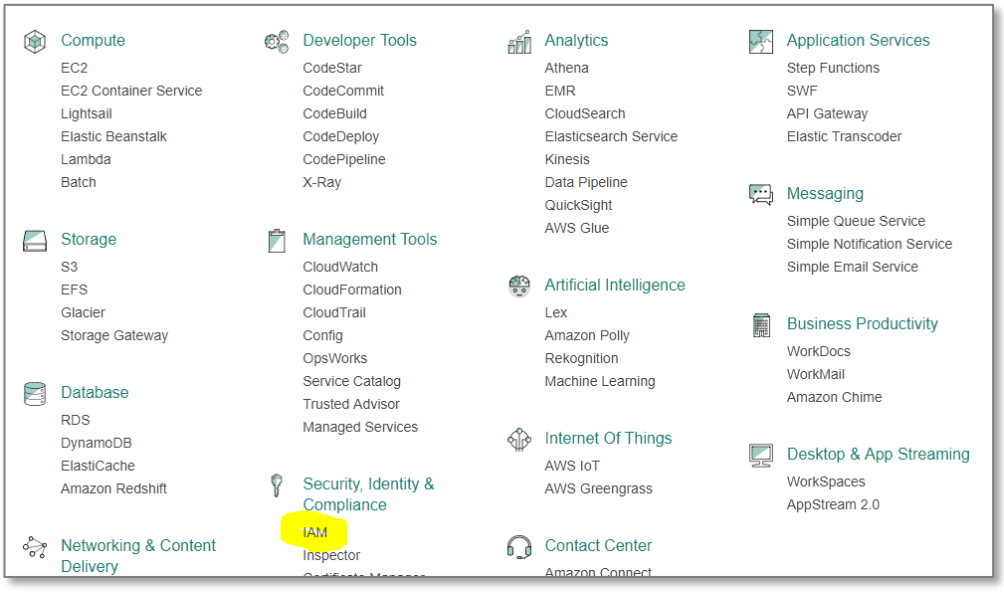

Copyright all rights reserved - BackSpace.Academy




After you have setup Authy

From the AWS console click 'Services"

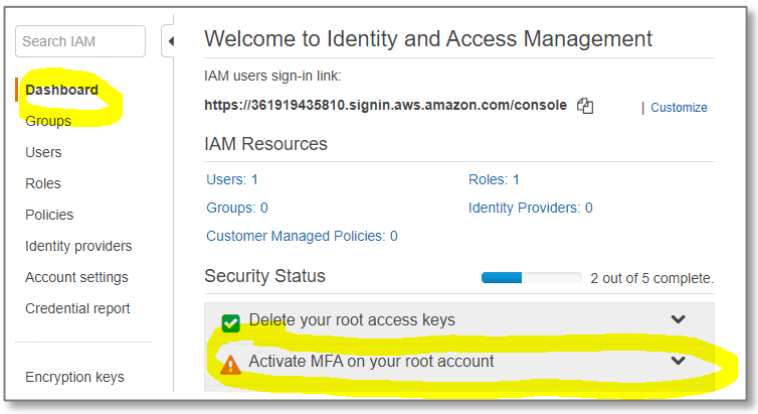
Select 'IAM" from the Security, Identity & Compliance services.



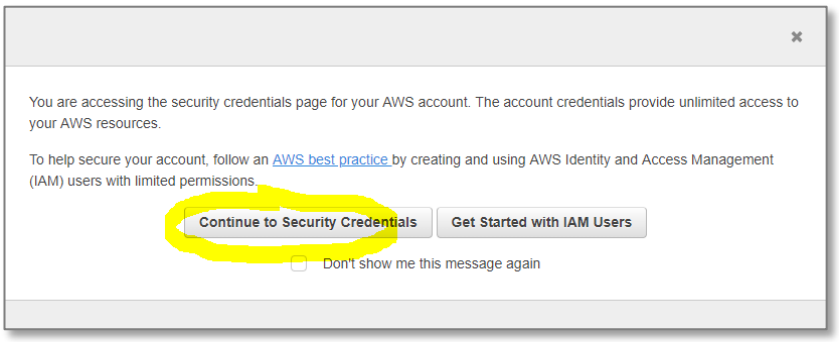

Select 'Dashboard"

Select 'Activate MFA on your root account"

Copyright all rights reserved - BackSpace.Academy




Click *Continue to Security Credentials*

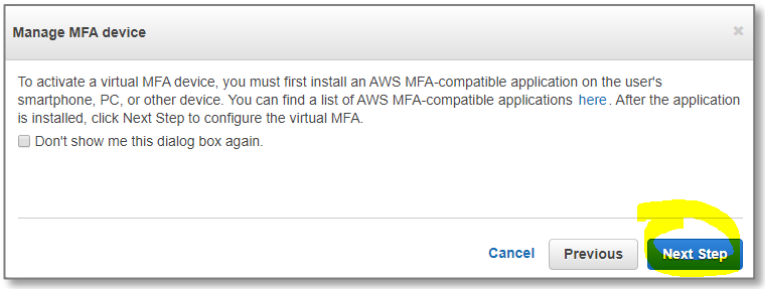



Click 'Manage MFA"

Select 'A virtual MFA device"

Click 'Next Step"

Click 'Next Step"





Copyright all rights reserved - BackSpace.Academy

Open Authy app

## Adding account using Authy Desktop app:

Click on 'Show secret key for manual configuration"

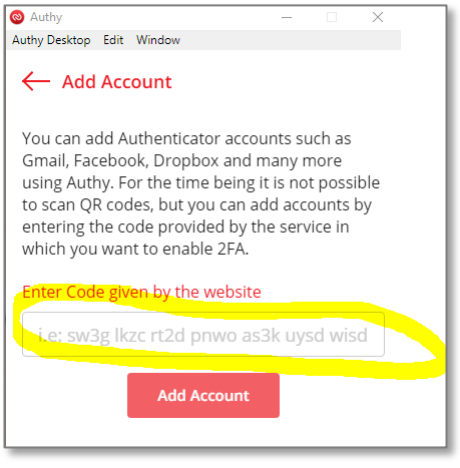
Copy the secret key

Open Authy app

Click the add icon

Paste the secret key

Click 'Add Account"

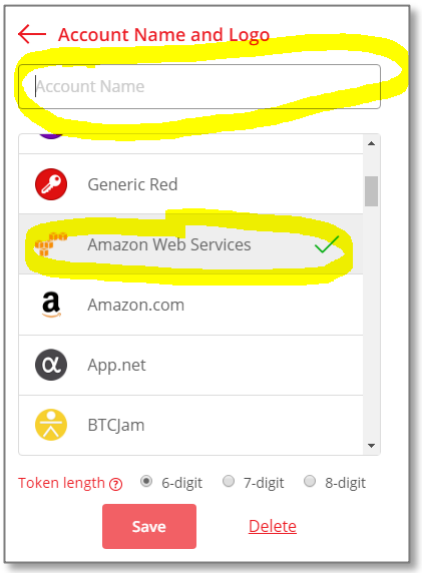



Copyright all rights reserved - BackSpace.Academy

Give your account a name

Scroll down to select the 'Amazon Web Services" icon.

Click 'Save"




## Adding account using Authy Mobile app:

Select 'Add Account" from the top right hand side dropdown menu

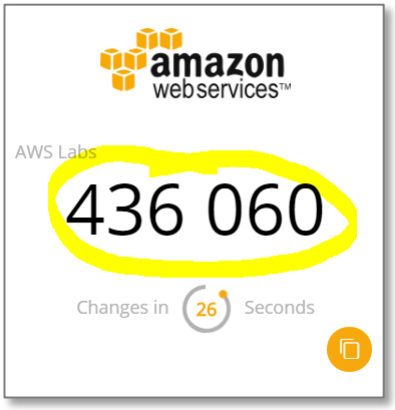
Select 'SCAN QR CODE"

Scan the QR code

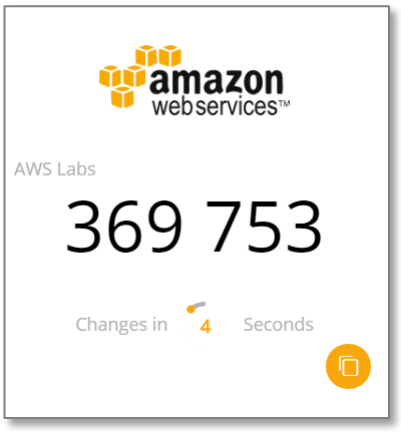
## Entering Authentication codes

Type the code into 'Authentication code 1"


Copyright all rights reserved - BackSpace.Academy

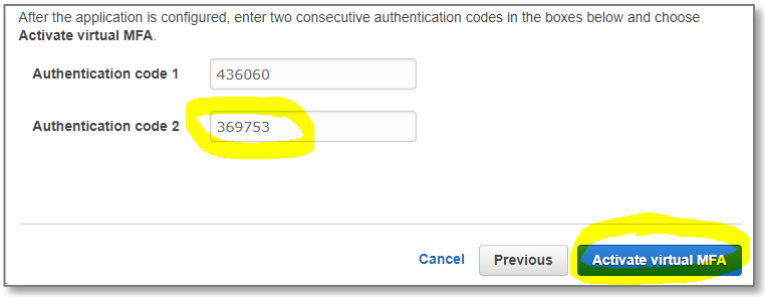


Wait for the code to change on the Authy app




Enter the second code

Click 'Activate virtual MFA"

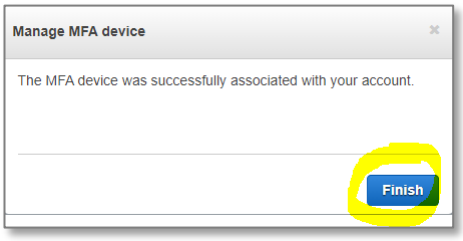



If you get an error: ' *We encountered the following errors while processing your request: Failed to associate the token"*
You have been too slow and the token has expired. Input another two consecutive codes.

Copyright all rights reserved - BackSpace.Academy

You should see a success dialog

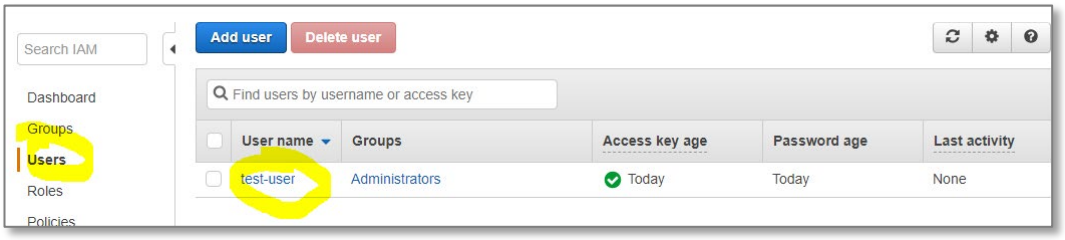
Click 'Finish"




## Implementing MFA on an IAM User

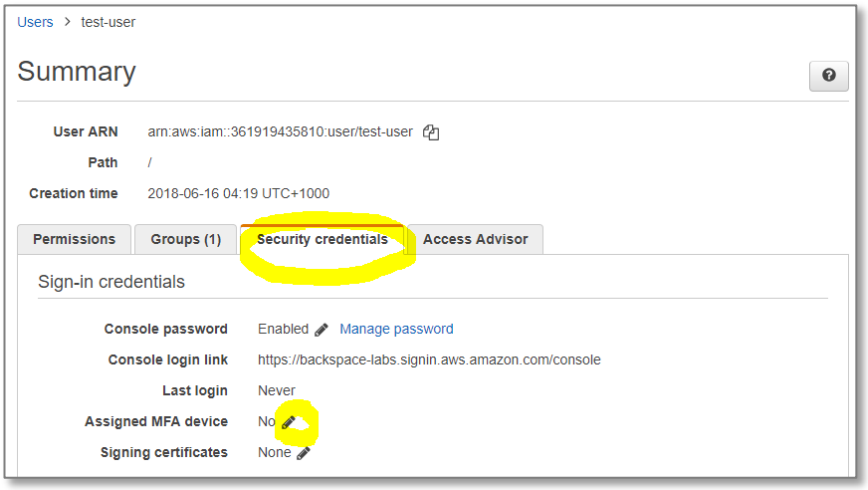
You can implement MFA on a user:

click on the user



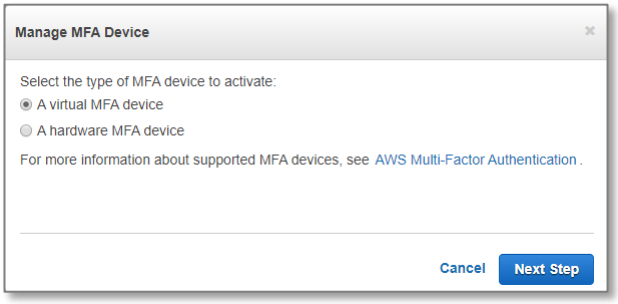

Select "Security credentials" tab

Click the edit icon for "Assigned MFA device"




Repeat the MFA process


Copyright all rights reserved - BackSpace.Academy



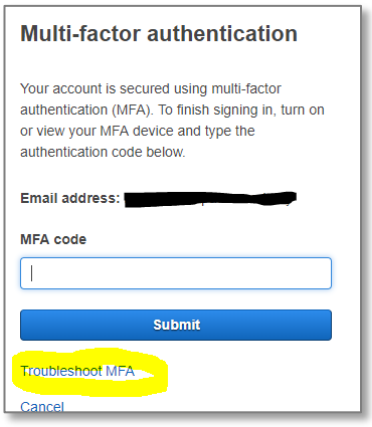

## What to do if you are locked out of your root account

You can always get back into your account provided you have the email address and phone number used to set up the account.

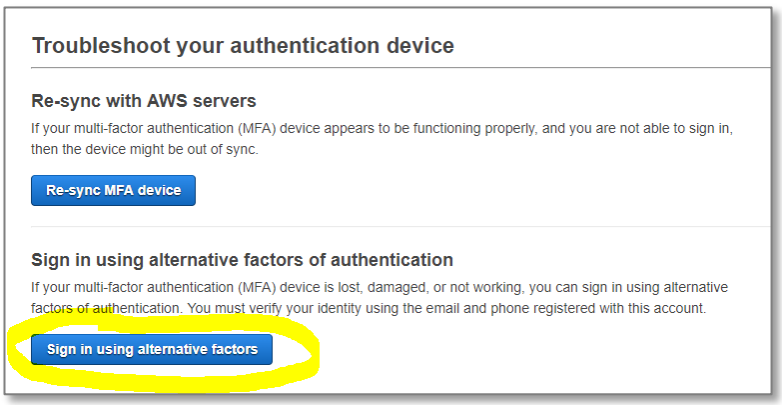
If you have not enabled MFA then you can simply click on the lost password link.

If you have enabled MFA then you can use alternative factors of authentication

After you enter your account name and password and are at the MFA login stage, click 'Troubleshoot MFA"




Select 'Sign in using alternative factors of authentication"




Copyright all rights reserved - BackSpace.Academy

Copyright all rights reserved - BackSpace.Academy