aws CERTIFIED Developer Associate

aws CERTIFIED Solutions Architect Associate

aws CERTIFIED SysOps Administrator Associate

lab

lab title

AWS Identity and Access Management (IAM) V1.06

Course title

BackSpace Academy
AWS Certified Associate

Table of Contents

Contents

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.

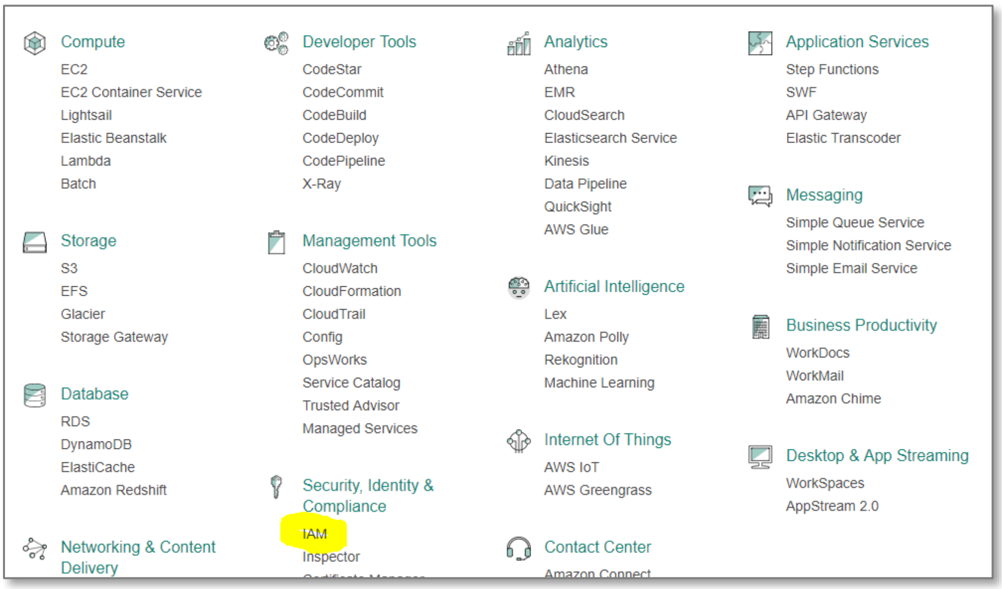
Please note that AWS services change on a weekly basis and it is extremely important you check the version number on this document to ensure you have the lastest version with any updates or corrections.

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.

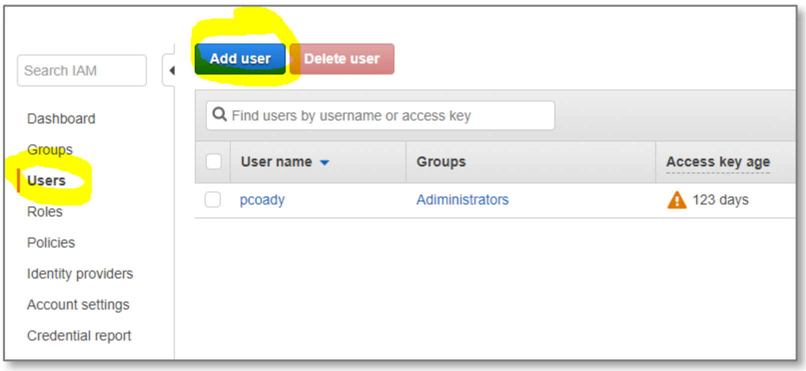
From the AWS console click “Services”

Select “IAM” from the Security, Identity & Compliance services.



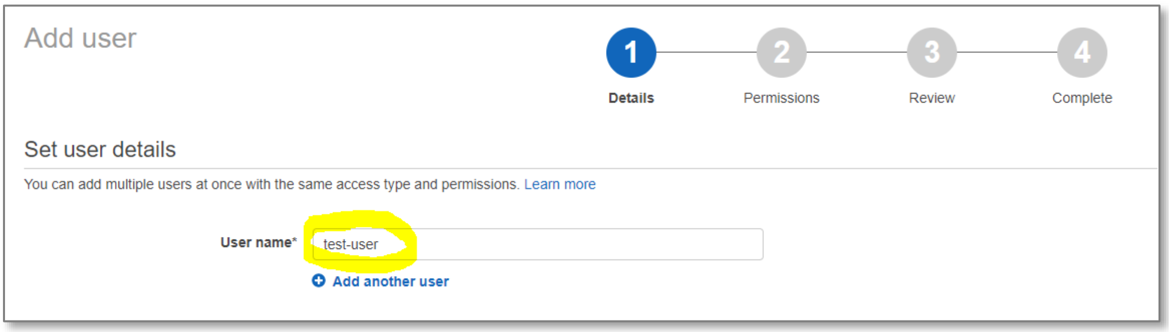
Select “Users”

Click “Add user”



□	User name ▾	Groups	Access key age
□	pcoady	Adiministrators	⚠ 123 days

Give the user a name



Add user

1 Details — 2 Permissions — 3 Review — 4 Complete

Set user details

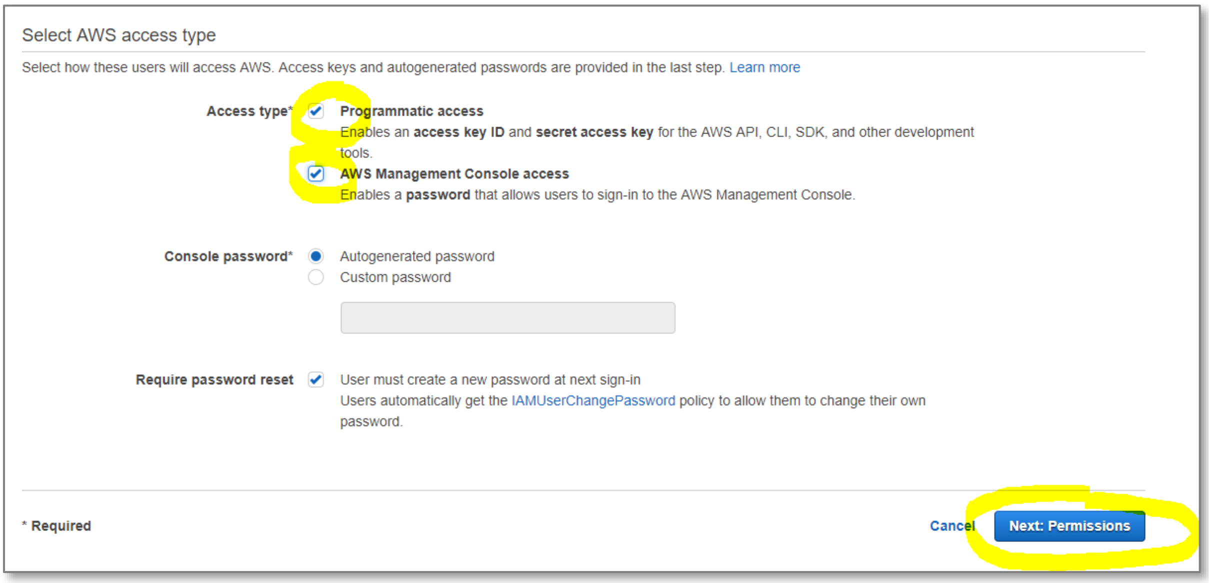
You can add multiple users at once with the same access type and permissions. Learn more

User name* test-user

Add another user

Check “Programmatic access”

Check “AWS Management Console access”



Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ● Autogenerated password
○ Custom password

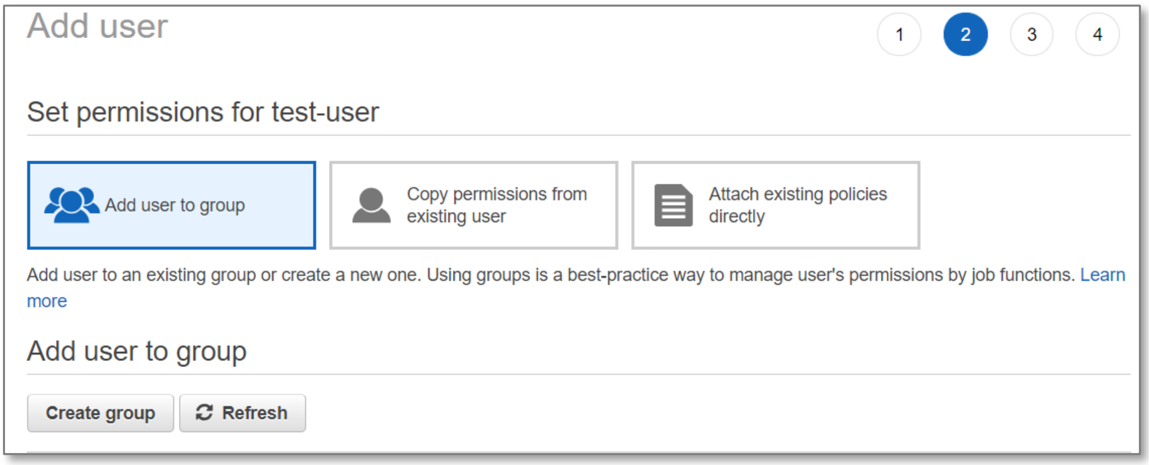
Require password reset ☑ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required

Cancel **Next: Permissions**

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

Click “Next Review”



Add user

1 2 3 4

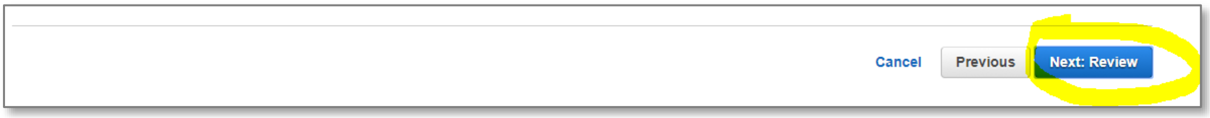
Set permissions for test-user

Add user to group | Copy permissions from existing user | Attach existing policies directly

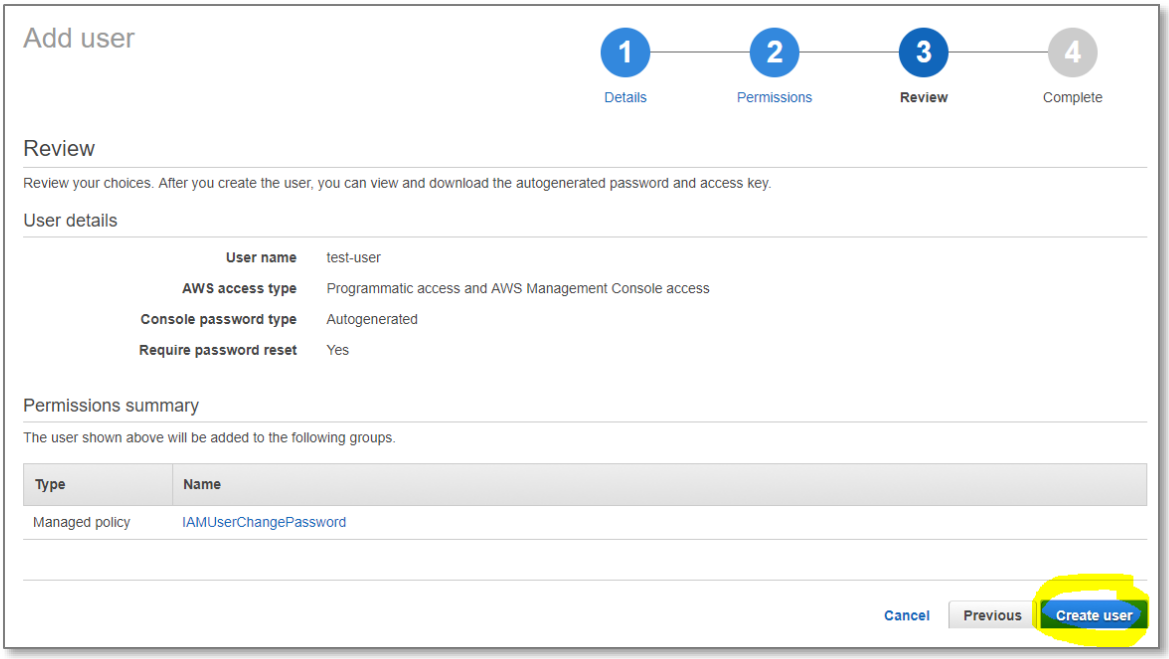
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

Create group | Refresh



Click “Create user”



Review

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

User details

User name	test-user
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes

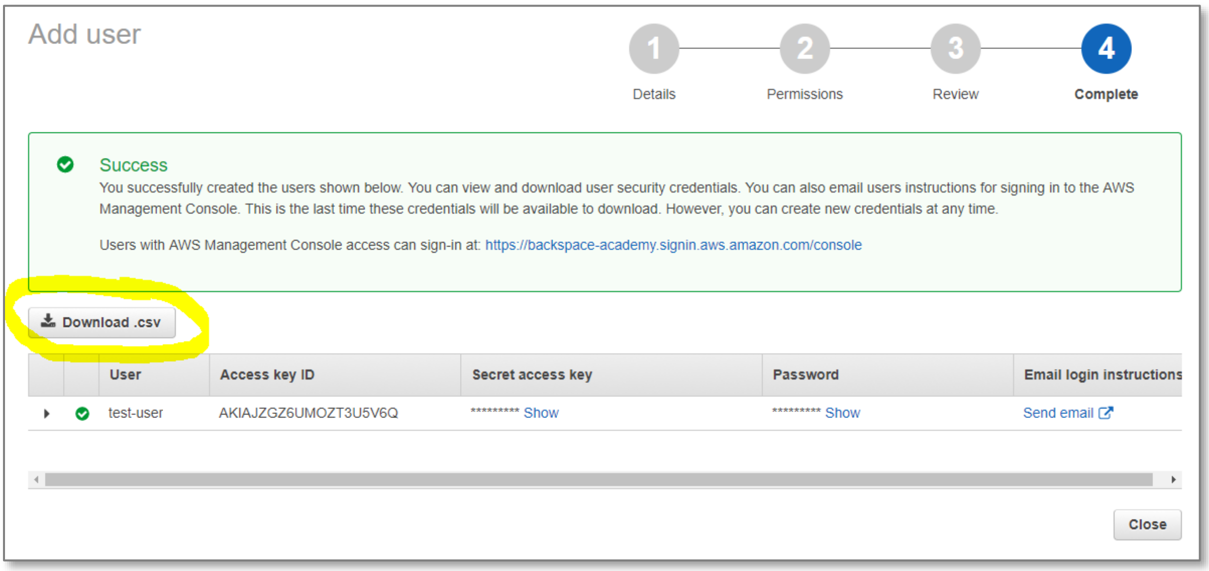
Permissions summary

The user shown above will be added to the following groups.

Type	Name
Managed policy	IAMUserChangePassword

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.



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://backspace-academy.signin.aws.amazon.com/console

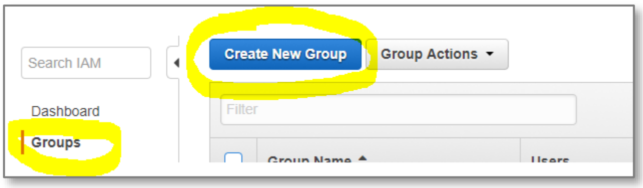
		User	Access key ID	Secret access key	Password	Email login instructions
▸	✓	test-user	AKIAJZGZ6UMOZT3U5V6Q	********* Show	********* Show	Send email

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.

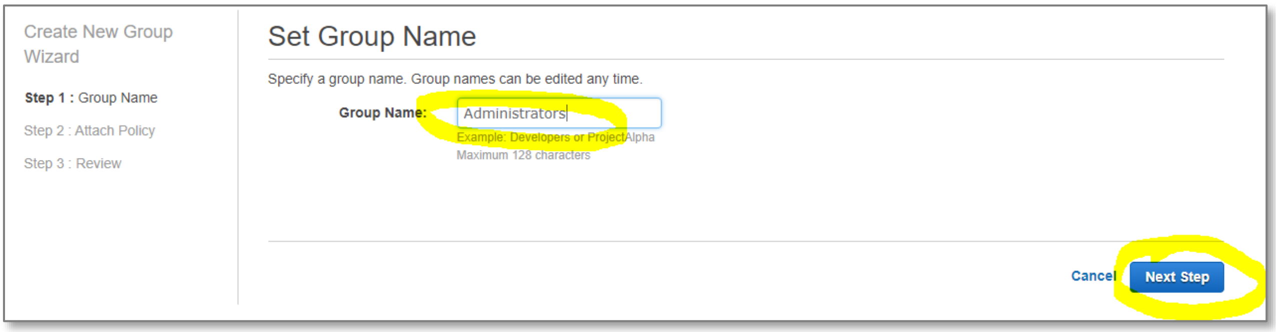
Select "Group"

Click "Create New Group"



Give the group a name

Click "Next Step"



Set Group Name

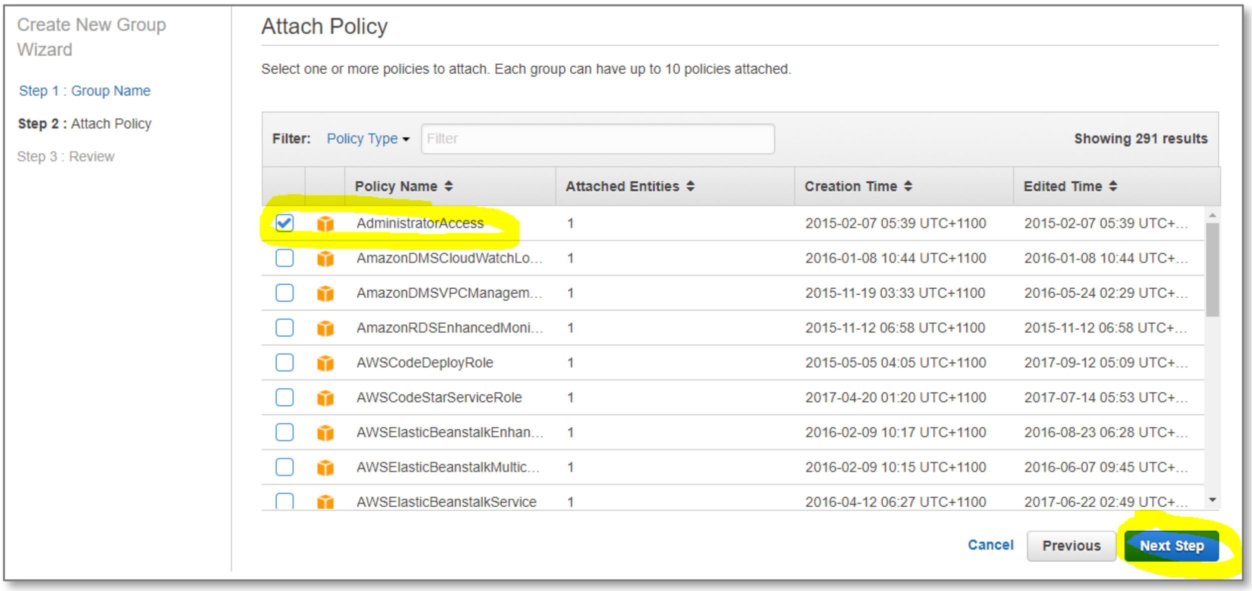
Specify a group name. Group names can be edited any time.

Group Name: Administrators

Example: Developers or ProjectAlpha
Maximum 128 characters

Select the "AdministratorAccess" policy

Click "Next Step"



Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

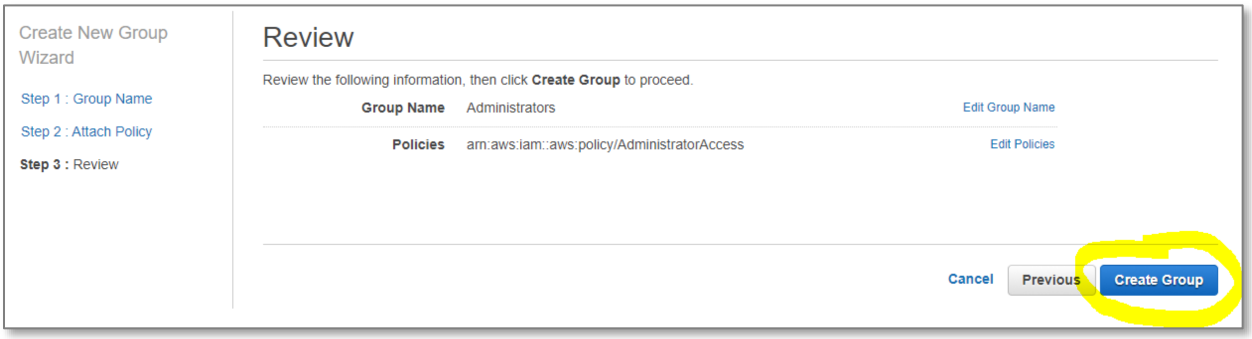
Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ Filter **Showing 291 results**

		Policy Name	Attached Entities	Creation Time	Edited Time
☑		AdministratorAccess	1	2015-02-07 05:39 UTC+1100	2015-02-07 05:39 UTC+...
□		AmazonDMSCloudWatchLo...	1	2016-01-08 10:44 UTC+1100	2016-01-08 10:44 UTC+...
□		AmazonDMSVPCManagem...	1	2015-11-19 03:33 UTC+1100	2016-05-24 02:29 UTC+...
□		AmazonRDSEnhancedMoni...	1	2015-11-12 06:58 UTC+1100	2015-11-12 06:58 UTC+...
□		AWSCodeDeployRole	1	2015-05-05 04:05 UTC+1100	2017-09-12 05:09 UTC+...
□		AWSCodeStarServiceRole	1	2017-04-20 01:20 UTC+1100	2017-07-14 05:53 UTC+...
□		AWSElasticBeanstalkEnhan...	1	2016-02-09 10:17 UTC+1100	2016-08-23 06:28 UTC+...
□		AWSElasticBeanstalkMultic...	1	2016-02-09 10:15 UTC+1100	2016-06-07 09:45 UTC+...
□		AWSElasticBeanstalkService	1	2016-04-12 06:27 UTC+1100	2017-06-22 02:49 UTC+...

Click “Create Group”



Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

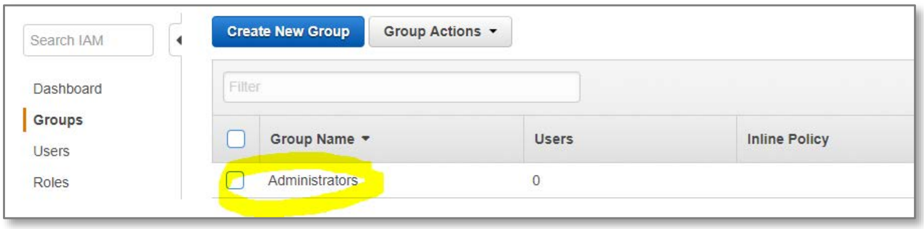
Review

Review the following information, then click **Create Group** to proceed.

Group Name Administrators

Policies arn:aws:iam::aws:policy/AdministratorAccess

The Group has been created

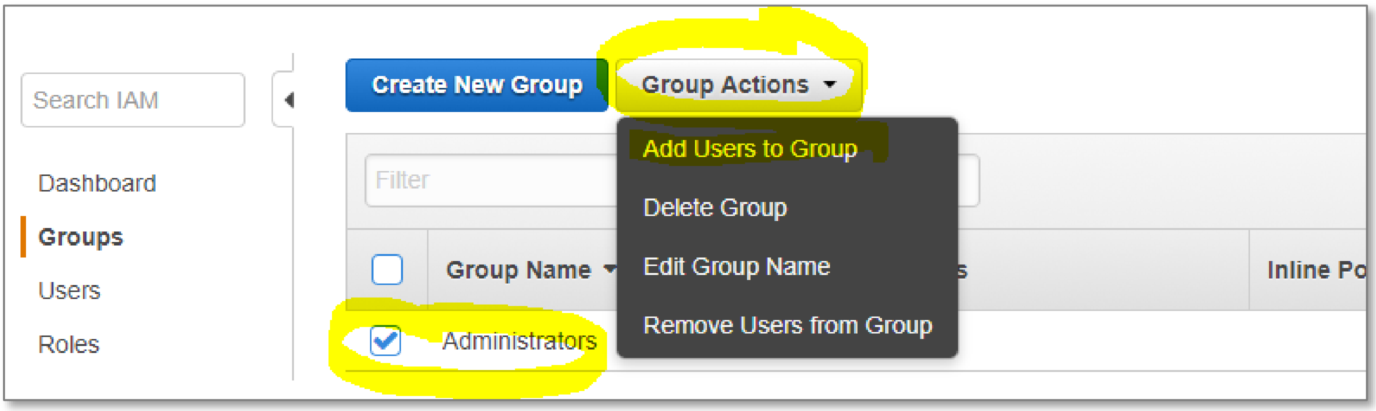


□	Group Name	Users	Inline Policy
□	Administrators	0	

Adding a User to a Group

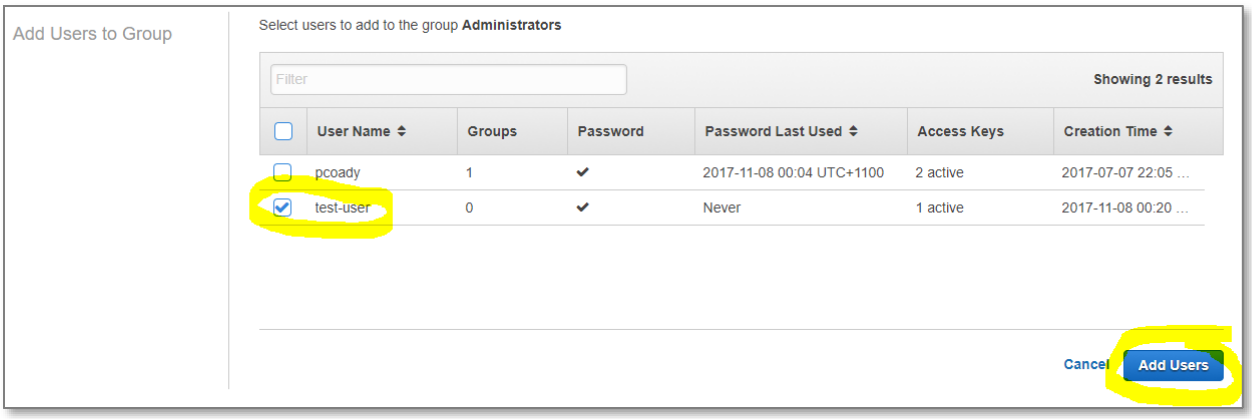
Select the group

Click “Group Actions” – “Add users to group”



Select the newly created user

Click “Add Users”



Select users to add to the group **Administrators**

Showing 2 results

□	User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
□	pcoady	1	✓	2017-11-08 00:04 UTC+1100	2 active	2017-07-07 22:05 ...
☑	test-user	0	✓	Never	1 active	2017-11-08 00:20 ...

Setting a Password Policy

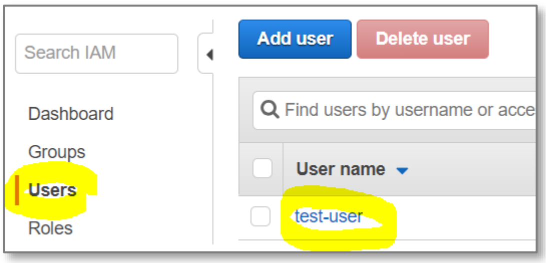
In this section, we will use the Identity and Access Management (IAM) service to set a password policy for our account and also set initial password details of an IAM user.

Setting an initial user password

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

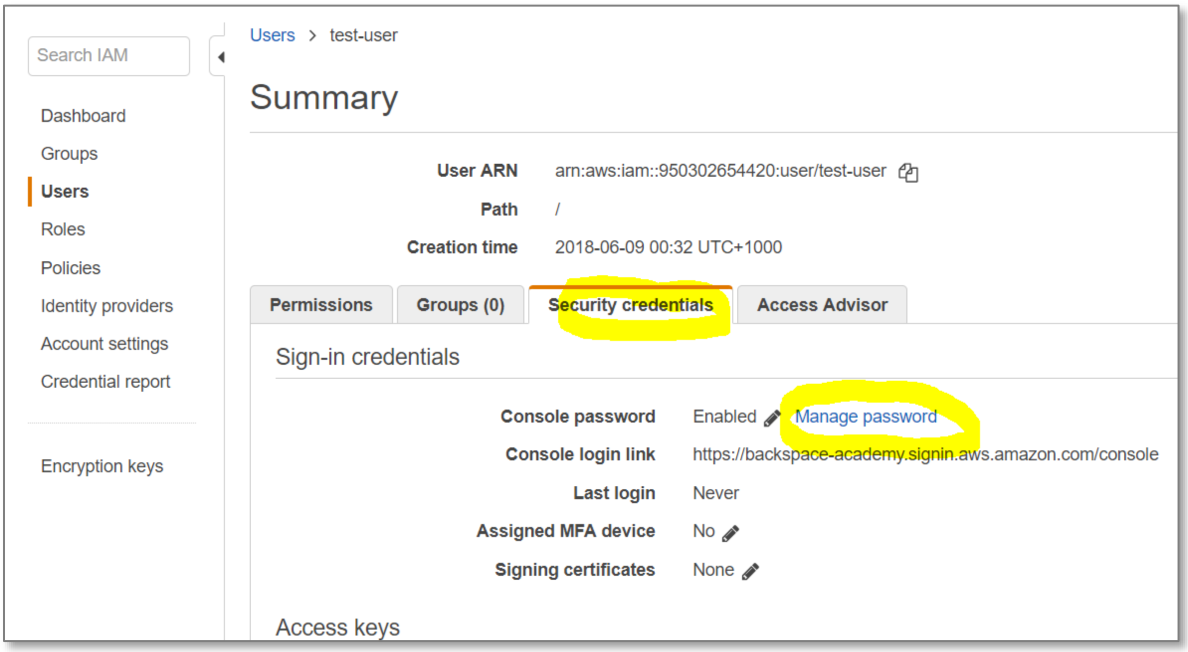
Select "Users"

Select our new user.



Select "Security Credentials"

Click "Manage password"



Summary

User ARN arn:aws:iam::950302654420:user/test-user

Path /

Creation time 2018-06-09 00:32 UTC+1000

Sign-in credentials

Console password Enabled

Console login link https://backspace-academy.signin.aws.amazon.com/console

Last login Never

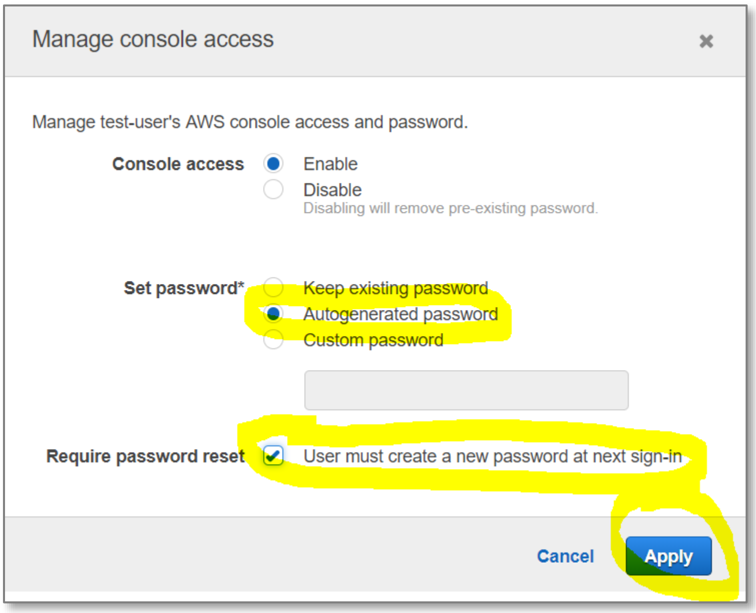
Assigned MFA device No

Signing certificates None

Select “Autogenerated password”

Select “User must create a new password at next sign-in”

Click “Apply”



Manage console access

Manage test-user's AWS console access and password.

Console access ● Enable ○ Disable
Disabling will remove pre-existing password.

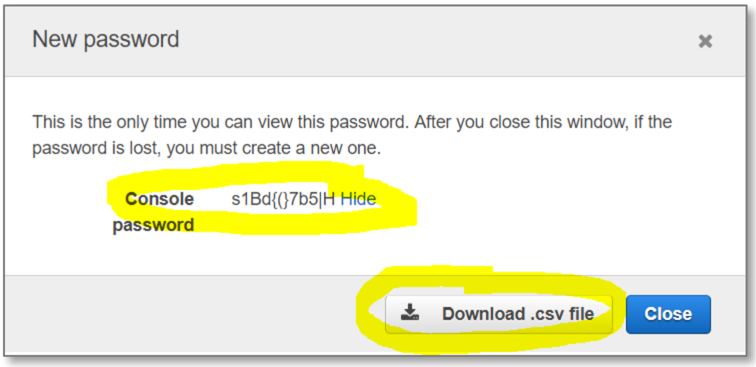
Set password* ○ Keep existing password ● Autogenerated password ○ Custom password

Require password reset ☑ User must create a new password at next sign-in

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.*”



New password

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.

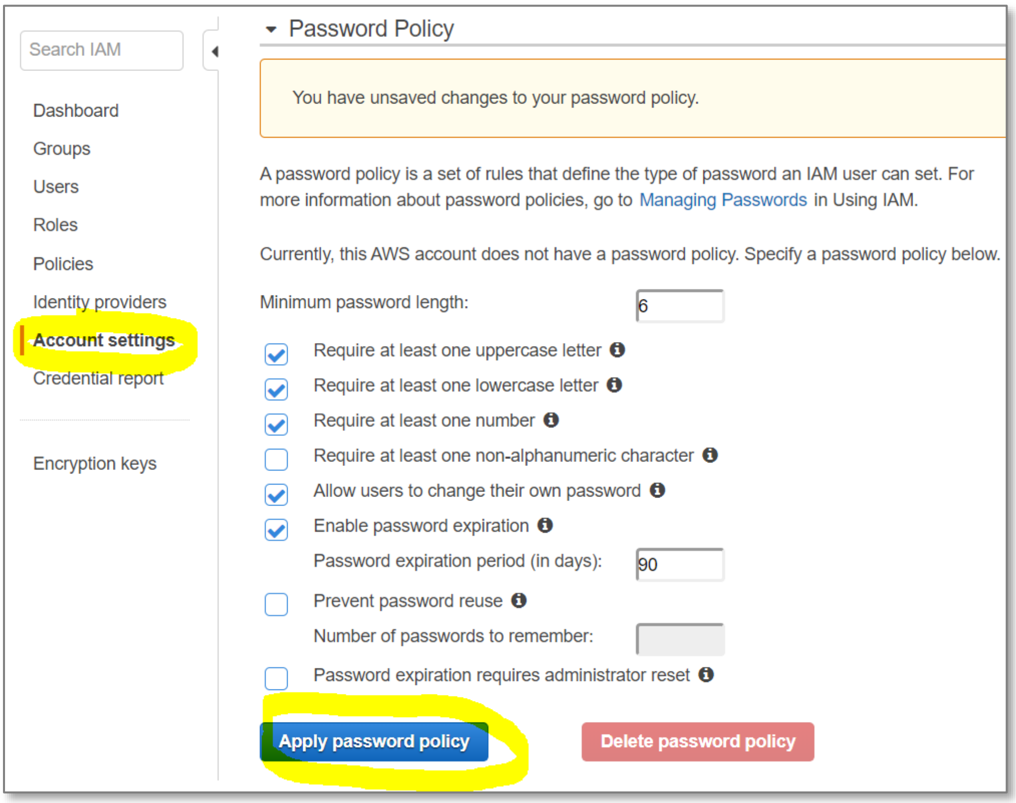
Console password s1Bd{(}7b5|H Hide

Setting an account password policy

Select “Account settings”

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

Click “Apply password policy”



Password Policy

You have unsaved changes to your password policy.

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to Managing Passwords in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length: 6

☑ Require at least one uppercase letter

☑ Require at least one lowercase letter

☑ Require at least one number

□ Require at least one non-alphanumeric character

☑ Allow users to change their own password

☑ Enable password expiration

Password expiration period (in days): 90

□ Prevent password reuse

Number of passwords to remember:

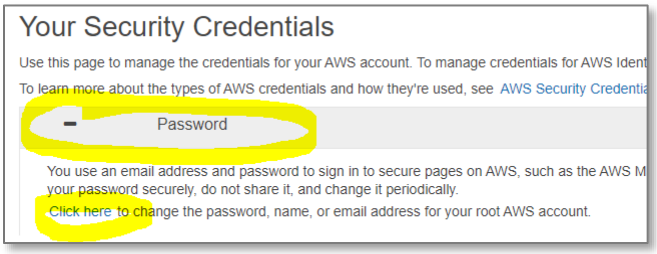
□ Password expiration requires administrator reset

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”



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Ident

To learn more about the types of AWS credentials and how they're used, see AWS Security Credenti

You use an email address and password to sign in to secure pages on AWS, such as the AWS M your password securely, do not share it, and change it periodically.

Click here to change the password, name, or email address for your root AWS account.

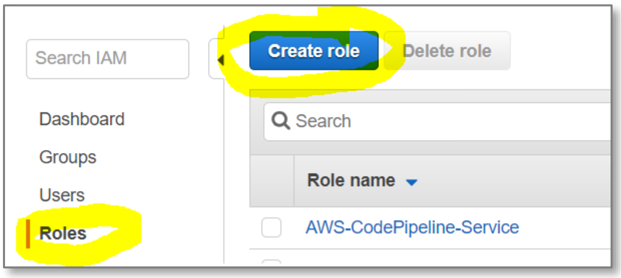
Finish up by signing out of your root user account and signing back in as an IAM user.

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”

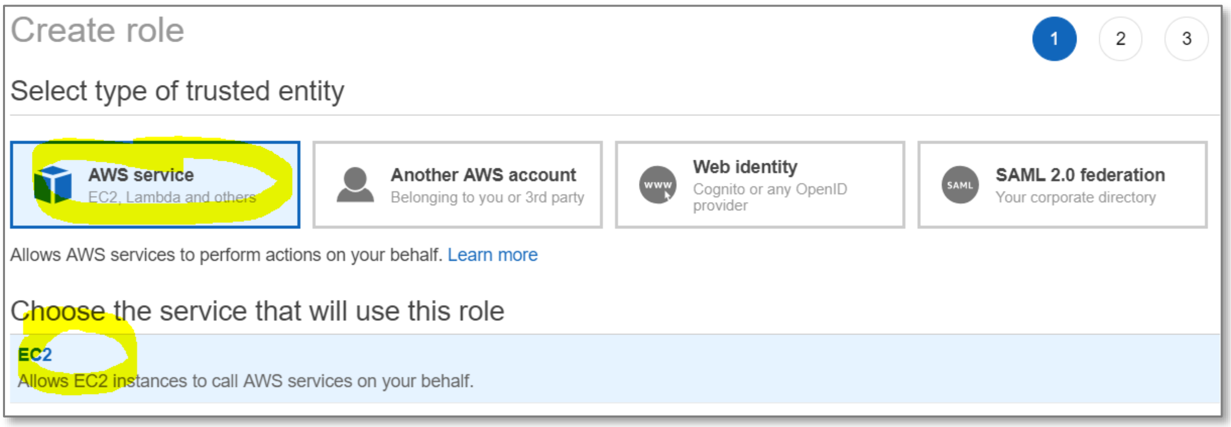
Click “Create role”



Select “AWS service”

Select “EC2”

Click “Next: Permissions”

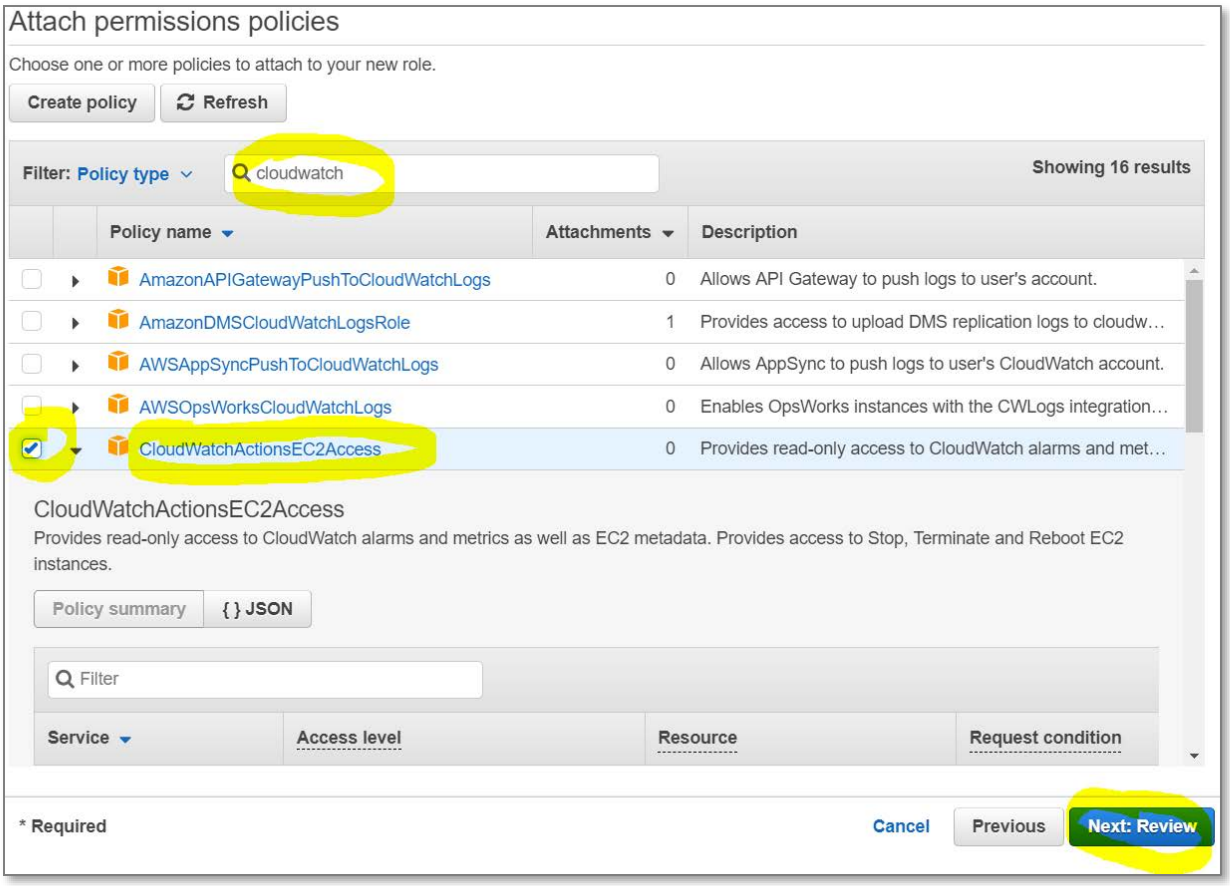

Create role
1
2
3
Select type of trusted entity
AWS service
EC2, Lambda and others
Another AWS account
Belonging to you or 3rd party
Web identity
Cognito or any OpenID provider
SAML 2.0 federation
Your corporate directory
Allows AWS services to perform actions on your behalf. Learn more
Choose the service that will use this role
EC2
Allows EC2 instances to call AWS services on your behalf.

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.

Click “Next; Review”



Attach permissions policies

Choose one or more policies to attach to your new role.

cloudwatch

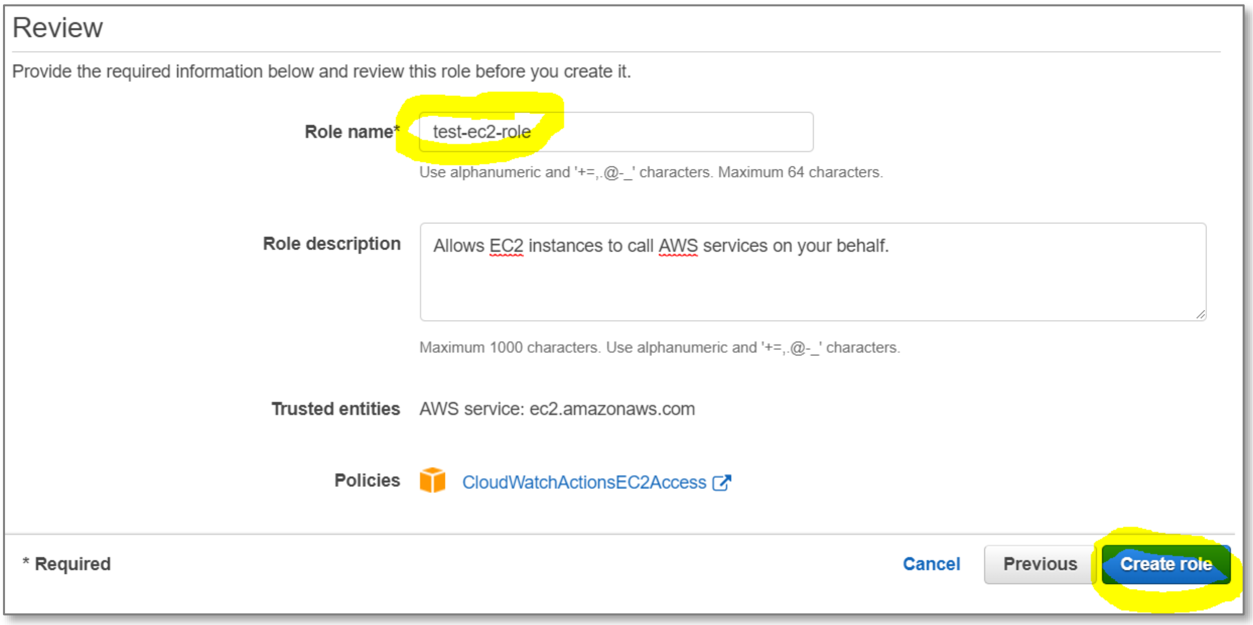
Showing 16 results

		Policy name	Attachments	Description
□	▸	AmazonAPIGatewayPushToCloudWatchLogs	0	Allows API Gateway to push logs to user's account.
□	▸	AmazonDMSCloudWatchLogsRole	1	Provides access to upload DMS replication logs to cloudw…
□	▸	AWSAppSyncPushToCloudWatchLogs	0	Allows AppSync to push logs to user's CloudWatch account.
□	▸	AWSOpsWorksCloudWatchLogs	0	Enables OpsWorks instances with the CWLogs integration…
☑	▾	CloudWatchActionsEC2Access	0	Provides read-only access to CloudWatch alarms and met…

CloudWatchActionsEC2Access

Provides read-only access to CloudWatch alarms and metrics as well as EC2 metadata. Provides access to Stop, Terminate and Reboot EC2 instances.

Give your role a name and click “Create Role”



Review

Provide the required information below and review this role before you create it.

Role name* test-ec2-role

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

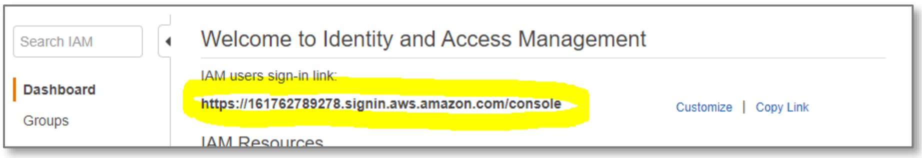
Policies CloudWatchActionsEC2Access

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.



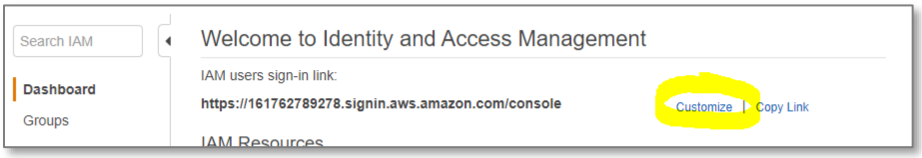
Welcome to Identity and Access Management

IAM users sign-in link:

https://161762789278.signin.aws.amazon.com/console

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

Click “Customize”



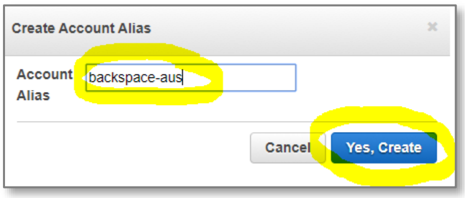
Welcome to Identity and Access Management

IAM users sign-in link:

https://161762789278.signin.aws.amazon.com/console

Create a unique alias name

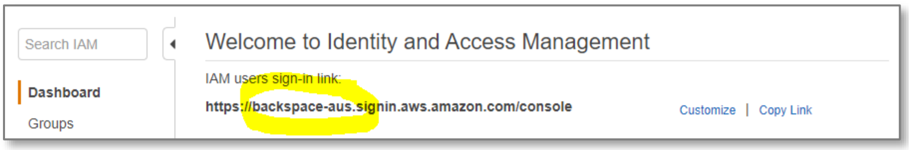
Click “Yes, Create”



Create Account Alias

Account Alias: backspace-aus

We can now use the account alias for logging in.



Welcome to Identity and Access Management

IAM users sign-in link:

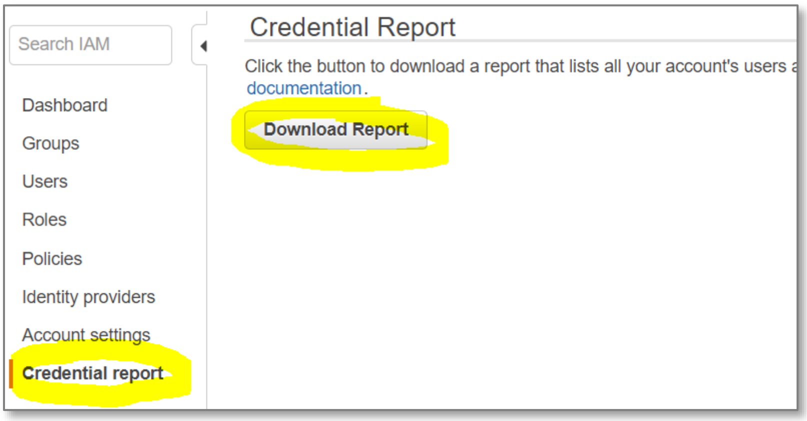
https://backspace-aus.signin.aws.amazon.com/console

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”



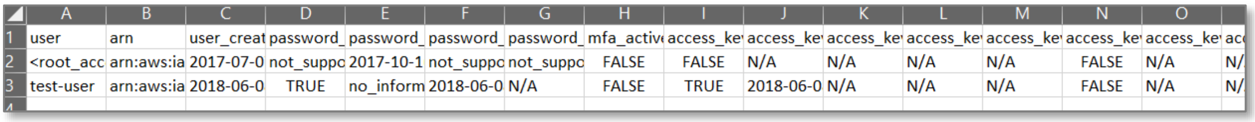
Search IAM

- Dashboard
- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report

Credential Report

Click the button to download a report that lists all your account's users a
documentation.

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_active	access_ke	access_ke	access_ke	access_ke	access_ke	access_ke	access_ke	acc
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.

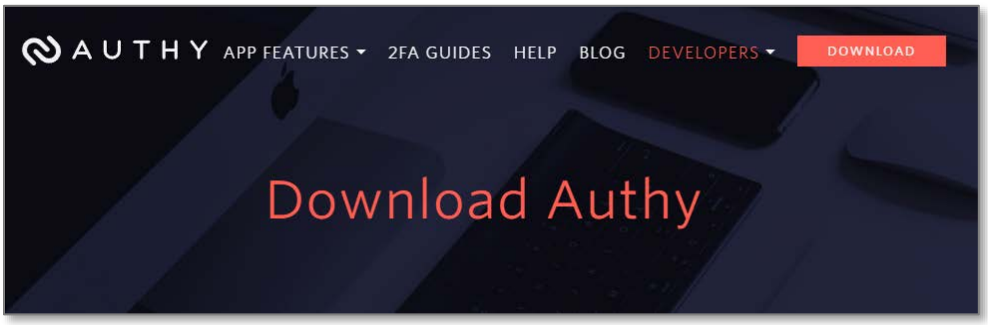
Implementing Multi Factor Authentication (MFA)

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.

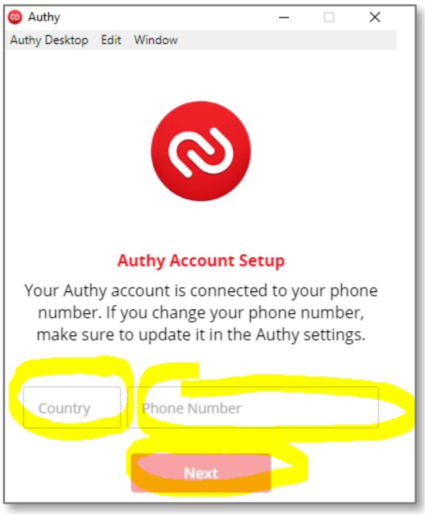
Download and install Authy to your desktop or mobile.

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

https://authy.com/download/



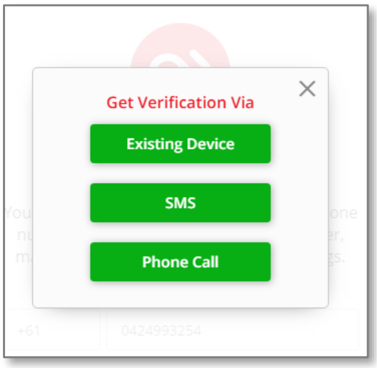
Enter your phone number details



Authy Account Setup

Your Authy account is connected to your phone number. If you change your phone number, make sure to update it in the Authy settings.

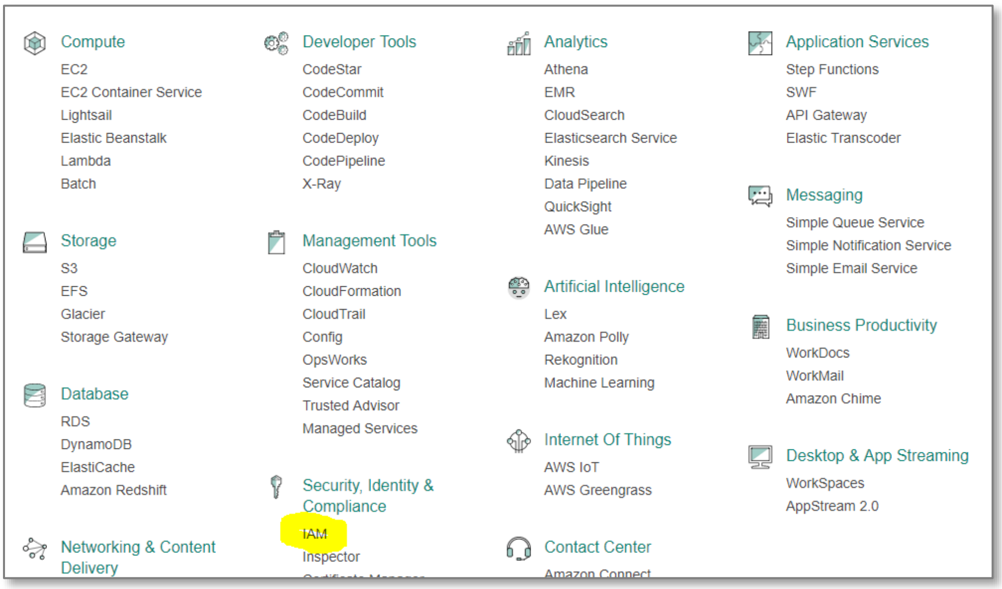
Verify by “SMS” (mobile phone) or “Phone Call” (landline)



After you have setup Authy

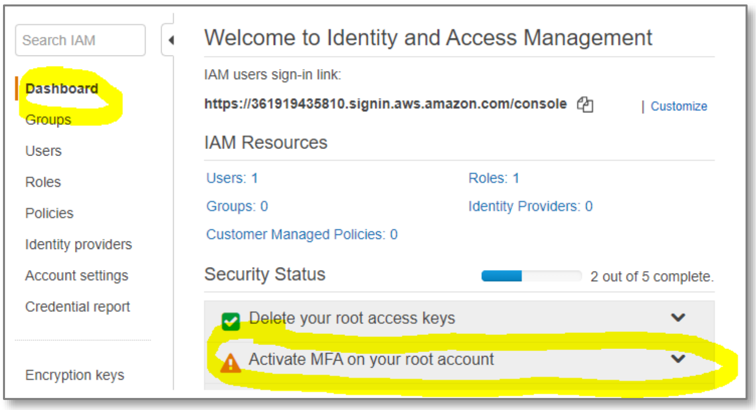
From the AWS console click “Services”

Select “IAM” from the Security, Identity & Compliance services.



Select “Dashboard”

Select “Activate MFA on your root account”



Welcome to Identity and Access Management

IAM users sign-in link:

https://361919435810.signin.aws.amazon.com/console

IAM Resources

Users: 1 Roles: 1

Groups: 0 Identity Providers: 0

Customer Managed Policies: 0

Security Status 2 out of 5 complete.

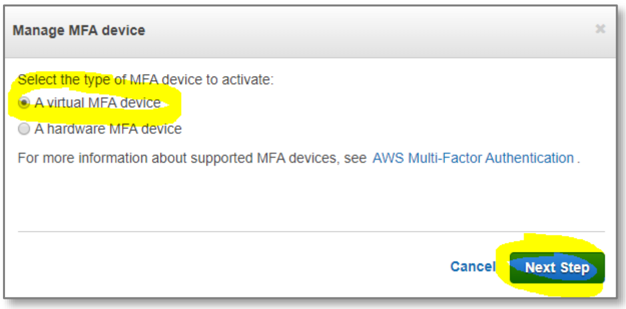
✓ Delete your root access keys

⚠ Activate MFA on your root account

Click “Manage MFA”

Select “A virtual MFA device”

Click “Next Step”



Manage MFA device

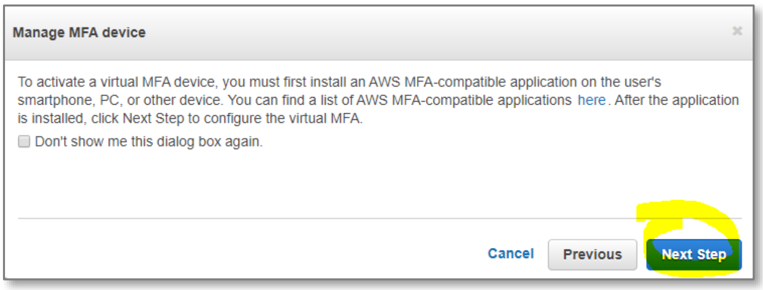
Select the type of MFA device to activate:

● A virtual MFA device

○ A hardware MFA device

For more information about supported MFA devices, see AWS Multi-Factor Authentication .

Click “Next Step”



Manage MFA device

To activate a virtual MFA device, you must first install an AWS MFA-compatible application on the user's smartphone, PC, or other device. You can find a list of AWS MFA-compatible applications here . After the application is installed, click Next Step to configure the virtual MFA.

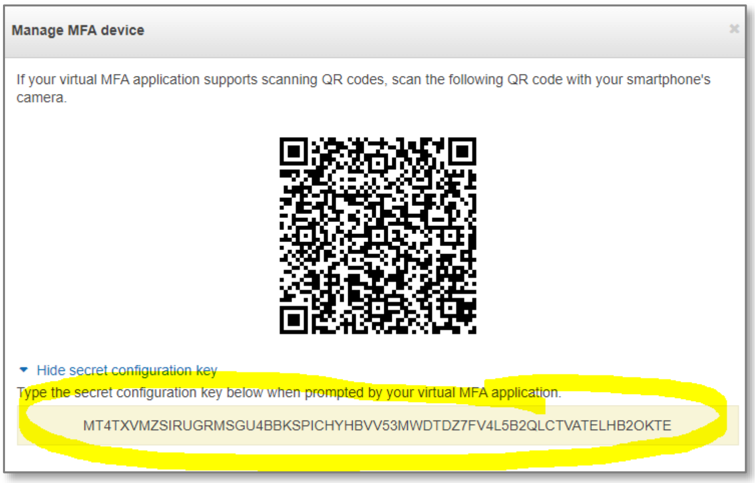
□ Don't show me this dialog box again.

Open Authy app

Adding account using Authy Desktop app:

Click on “Show secret key for manual configuration”

Copy the secret key



Manage MFA device

If your virtual MFA application supports scanning QR codes, scan the following QR code with your smartphone's camera.

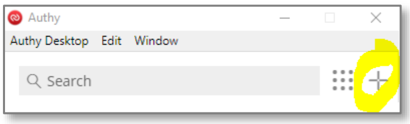
▾ Hide secret configuration key

Type the secret configuration key below when prompted by your virtual MFA application.

MT4TXVMZSIRUGRMSGU4BBKSPICHYHBVV53MWDTDZ7FV4L5B2QLCTVATELHB2OKTE

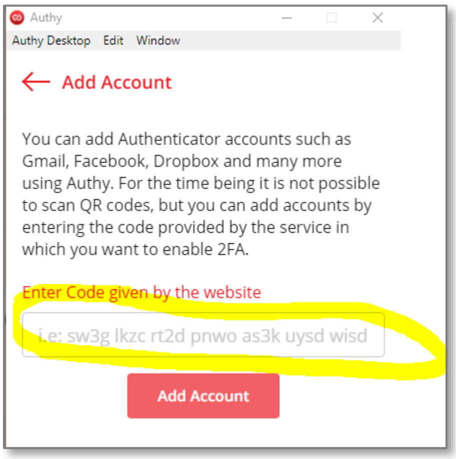
Open Authy app

Click the add icon



Paste the secret key

Click “Add Account”



Add Account

You can add Authenticator accounts such as Gmail, Facebook, Dropbox and many more using Authy. For the time being it is not possible to scan QR codes, but you can add accounts by entering the code provided by the service in which you want to enable 2FA.

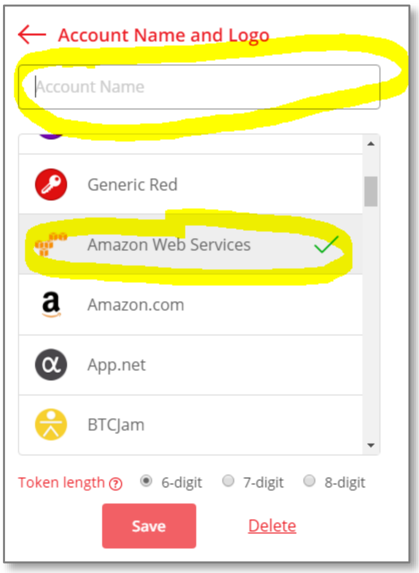
Enter Code given by the website

i.e: sw3g lkzc rt2d pnwo as3k uysd wisd

Give your account a name

Scroll down to select the “Amazon Web Services” icon.

Click “Save”


Account Name and Logo

Account Name

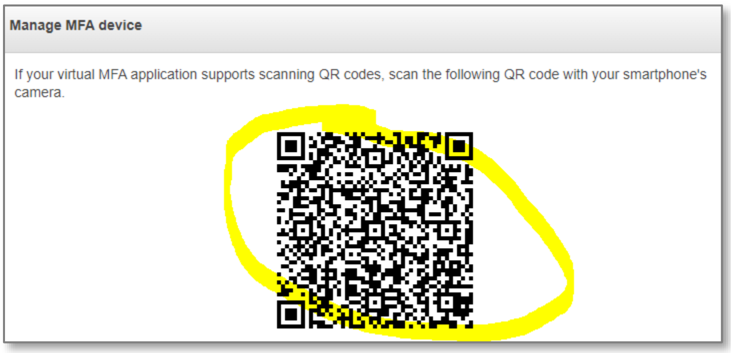
Token length ● 6-digit ○ 7-digit ○ 8-digit

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

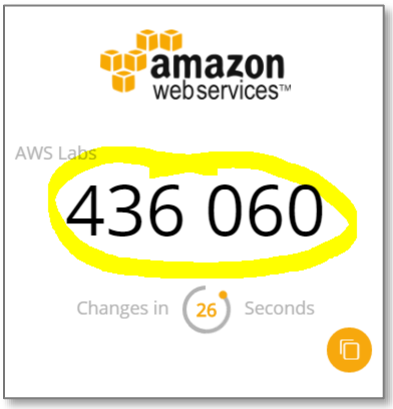


Manage MFA device

If your virtual MFA application supports scanning QR codes, scan the following QR code with your smartphone's camera.

Entering Authentication codes

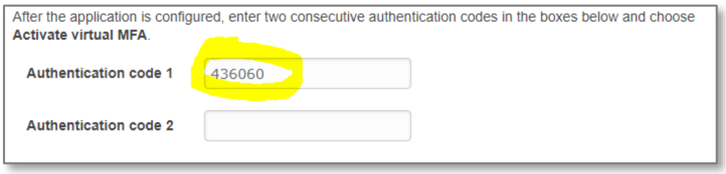
Type the code into “Authentication code 1”



AWS Labs

436 060

Changes in 26 Seconds

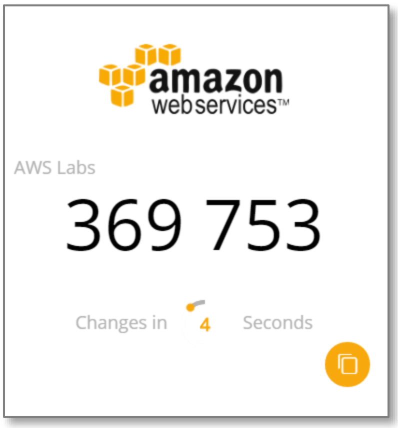


After the application is configured, enter two consecutive authentication codes in the boxes below and choose **Activate virtual MFA**.

Authentication code 1 436060

Authentication code 2

Wait for the code to change on the Authy app



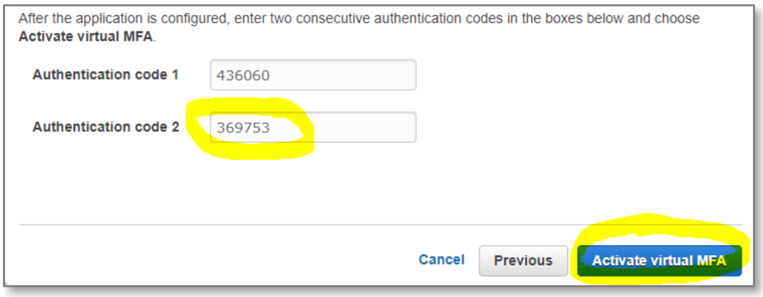
AWS Labs

369 753

Changes in 4 Seconds

Enter the second code

Click “Activate virtual MFA”



After the application is configured, enter two consecutive authentication codes in the boxes below and choose **Activate virtual MFA**.

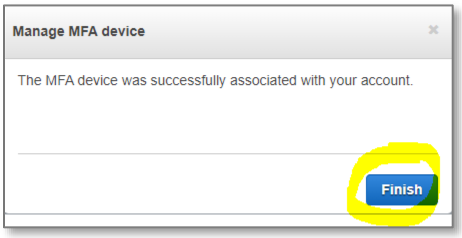
Authentication code 1: 436060

Authentication code 2: 369753

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.

You should see a success dialog

Click “Finish”



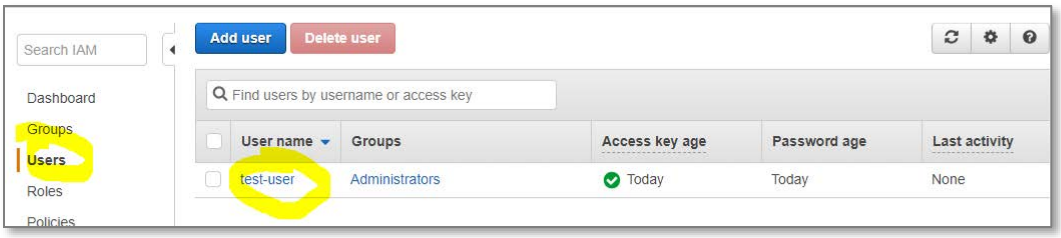
Manage MFA device

The MFA device was successfully associated with your account.

Implementing MFA on an IAM User

You can implement MFA on a user:

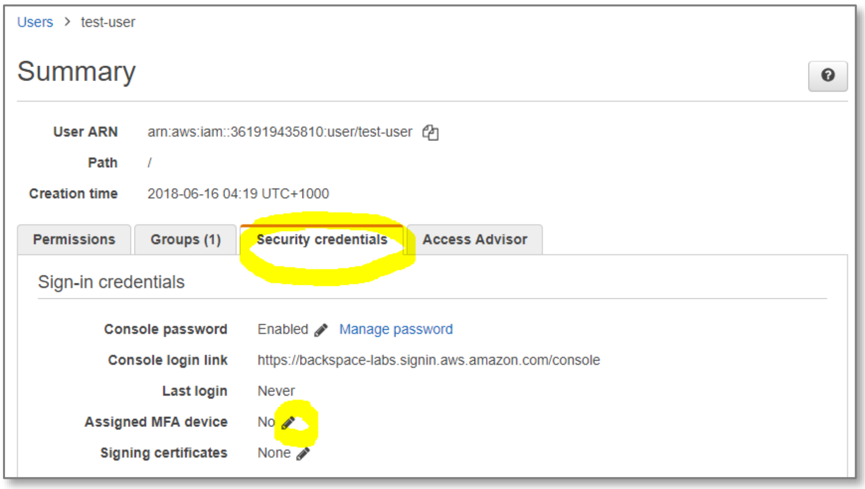
click on the user



User name	Groups	Access key age	Password age	Last activity
test-user	Administrators	✓ Today	Today	None

Select “Security credentials” tab

Click the edit icon for “Assigned MFA device”



User ARN arn:aws:iam::361919435810:user/test-user

Path /

Creation time 2018-06-16 04:19 UTC+1000

Console password Enabled Manage password

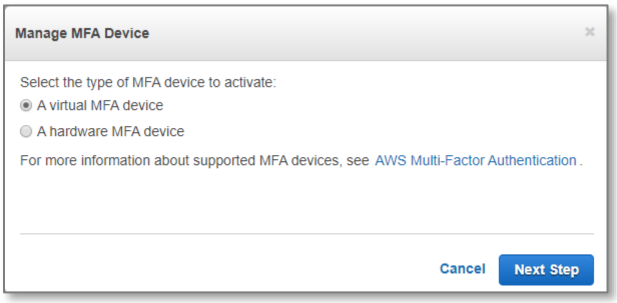
Console login link https://backspace-labs.signin.aws.amazon.com/console

Last login Never

Assigned MFA device No

Signing certificates None

Repeat the MFA process



Select the type of MFA device to activate:

● A virtual MFA device

○ A hardware MFA device

For more information about supported MFA devices, see AWS Multi-Factor Authentication .

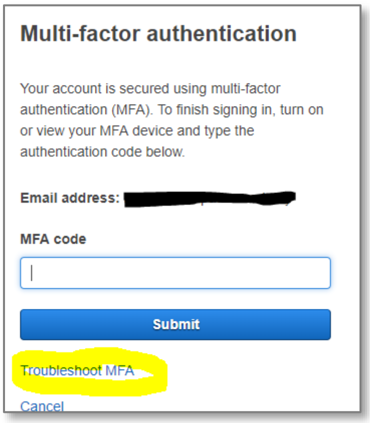
What to do if you are locked out of your root account

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”



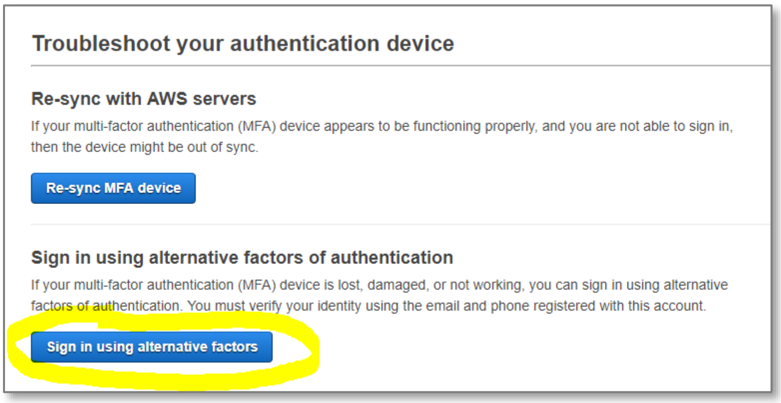
Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: [redacted]

MFA code

Select “Sign in using alternative factors of authentication”



Troubleshoot your authentication device

Re-sync with AWS servers

If your multi-factor authentication (MFA) device appears to be functioning properly, and you are not able to sign in, then the device might be out of sync.

Sign in using alternative factors of authentication

If your multi-factor authentication (MFA) device is lost, damaged, or not working, you can sign in using alternative factors of authentication. You must verify your identity using the email and phone registered with this account.