



lab



lab title

AWS Identity and Access Management (IAM) V1.09



Course title

**BackSpace Academy
AWS Certified Associate**



Table of Contents

Contents

Table of Contents.....	1
About the Lab	2
Creating an IAM User.....	3
Creating an IAM Group	7
Adding a User to a Group	8
Setting a Password Policy.....	10
Setting an initial user password.....	10
Setting an account password policy	12
Creating an IAM Role	14
Creating an Account Alias	16
Creating a Credentials Report	18
Clean Up.....	18
Implementing Multi Factor Authentication (MFA).....	19
Adding account using Authy Desktop app:.....	21
Adding account using Authy Mobile app:.....	23
Entering Authentication codes	23
Implementing MFA on an IAM User	25
What to do if you are locked out of your root account.....	26

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.

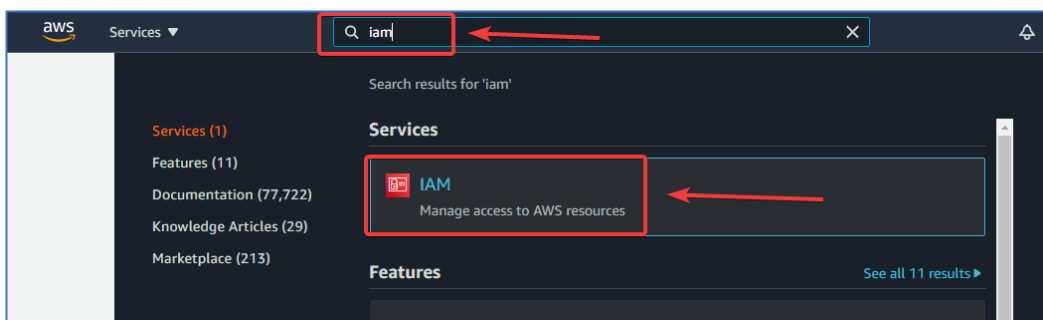
These lab notes are to support the hands on instructional videos of the Identity and Access Management (IAM) section of the AWS Certified Associate Course.

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 latest version with any updates or corrections.

Creating an IAM User

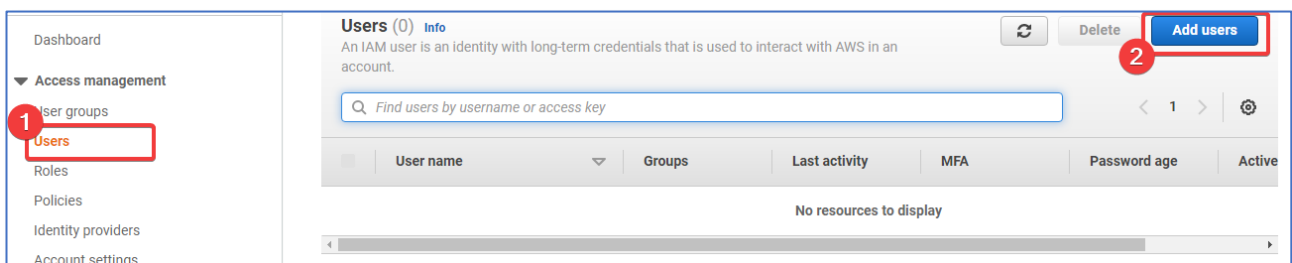
In this section, we will use the Identity and Access Management (IAM) service to create a user with console access and programmatic access.

AWS console search IAM.



Select *Users*

Click *Add user*



Give the user a name

Check *Programmatic access*

Check *AWS Management Console access*

Click *Next: Permissions*

The screenshot shows the 'Add user' wizard in the AWS IAM console. It consists of five steps, with the first step 'Set user details' being the active one. The wizard is titled 'Add user' and has five numbered tabs at the top: 1 (active), 2, 3, 4, and 5.

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* 1 [+ Add another user](#)

Select AWS access type

Select how these users will access AWS. 2 Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

- 3 ☒ **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 password.

*** Required** 4 [Cancel](#) [Next: Permissions](#)

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

Click *Next Tags*

Add user

1 2 3 4 5

▼ Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Get started with groups
You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

► Set permissions boundary

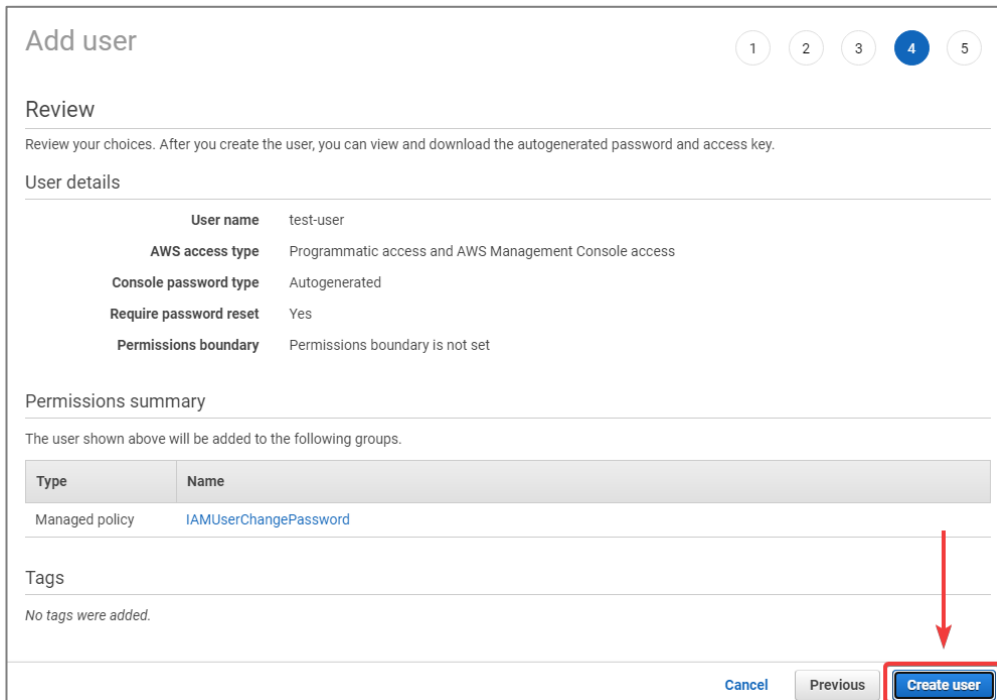
Cancel Previous **Next: Tags**

We won't add any tags to the user

Click *Next Review*

Cancel Previous **Next: Review**

Click *Create user*



Add user 1 2 3 4 5

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 boundary	Permissions boundary is not set

Permissions summary

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

Type	Name
Managed policy	IAMUserChangePassword

Tags

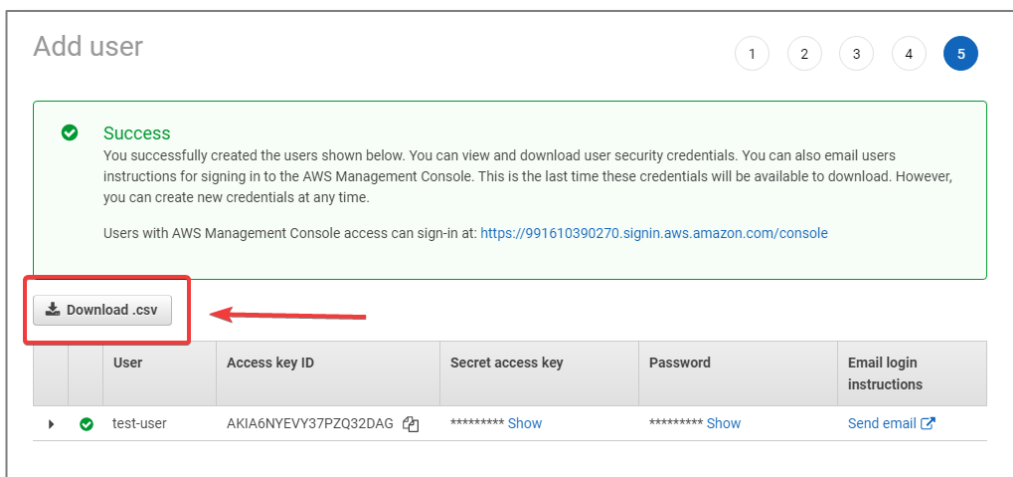
No tags were added.

Cancel Previous **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.

Click *Close*



Add user 1 2 3 4 5

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://991610390270.signin.aws.amazon.com/console>

Download .csv

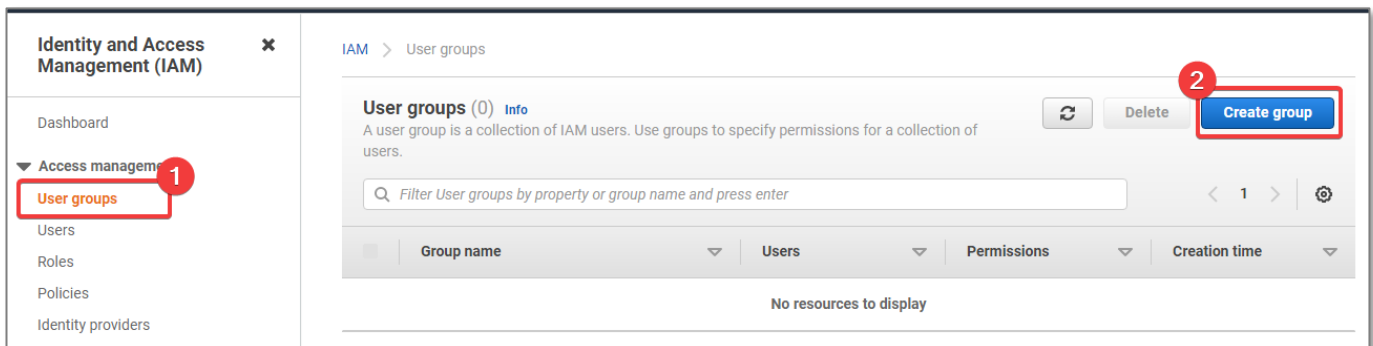
	User	Access key ID	Secret access key	Password	Email login instructions
▶	test-user	AKIA6NVEVY37PZQ32DAG	***** Show	***** Show	Send email

Creating an IAM Group

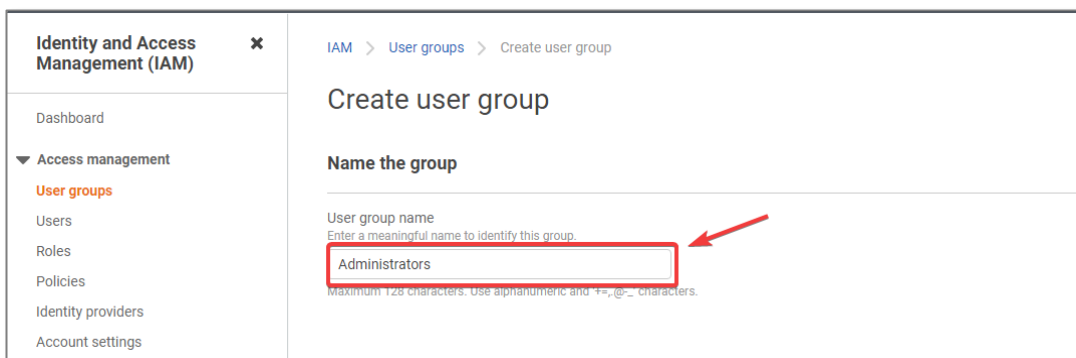
In this section, we will use the Identity and Access Management (IAM) service to create a group with administrator access. We will also add our newly created user to the group.

Select *User groups*

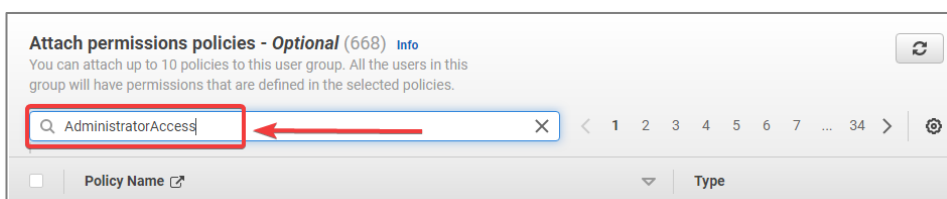
Click *Create group*

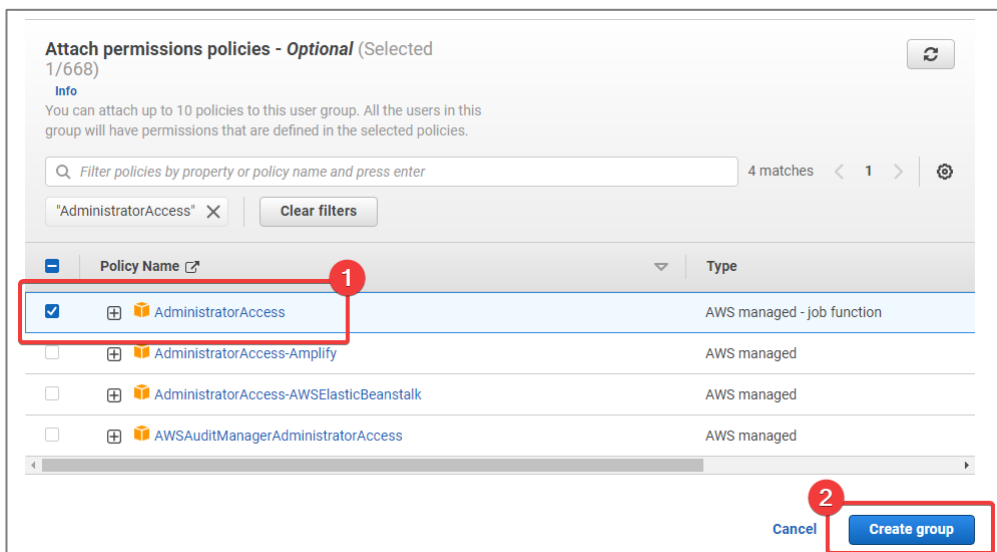


Give the group a name, Scroll down to Policy

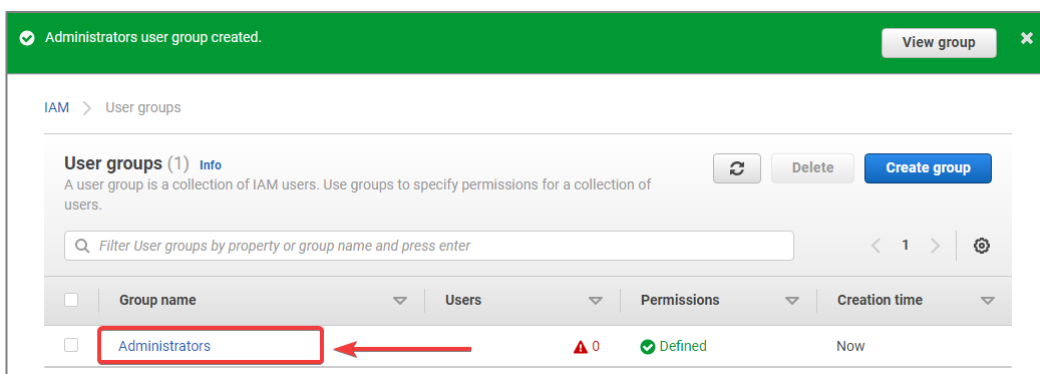


Search for *AdministratorAccess* and click *Create group*



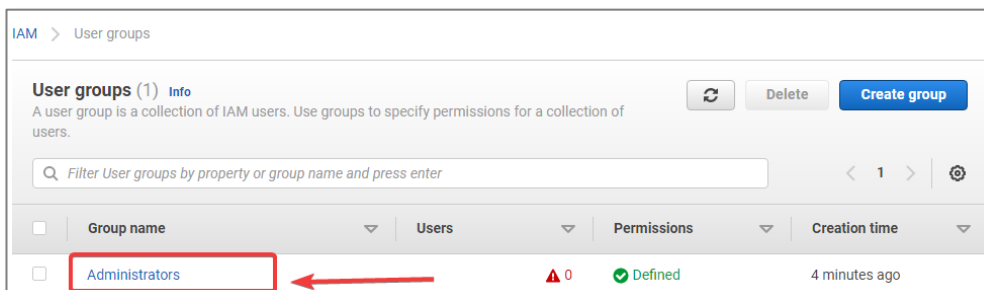


The Group has been created



Adding a User to a Group

Select the group *Administrator*



Click *Add Users*

The screenshot shows the AWS IAM console page for the 'Administrators' user group. The breadcrumb trail is 'IAM > User groups > Administrators'. The page title is 'Administrators'. There are 'Delete' and 'Edit' buttons in the top right. The 'Summary' section shows the group name 'Administrators', creation time 'July 28, 2021, 10:53 (UTC+08:00)', and ARN 'arn:aws:iam::991610390270:group/Administrators'. Below this are tabs for 'Users', 'Permissions', and 'Access advisor'. The 'Users' tab is active, showing 'Users in this group (0)'. A red box highlights the 'Add users' button, with a red arrow pointing to it from the right. Below the button is a search bar and a table with columns: 'User name', 'Groups', 'Last activity', and 'Creation time'. The table is empty, showing 'No resources to display'.

Select the newly created user then Click *Add users*

The screenshot shows the 'Add users to Administrators' page in the AWS IAM console. The breadcrumb trail is 'IAM > User groups > Administrators > Add users'. The page title is 'Add users to Administrators'. The 'Other users in this account (Selected 1/1)' section shows a search bar and a table with columns: 'User name', 'Groups', 'Last activity', and 'Creation time'. The table has one row with 'test-user' selected, indicated by a red box and a red circle with the number '1'. The 'Add users' button is highlighted with a red box and a red circle with the number '2'. There is also a 'Cancel' button.

Setting a Password Policy

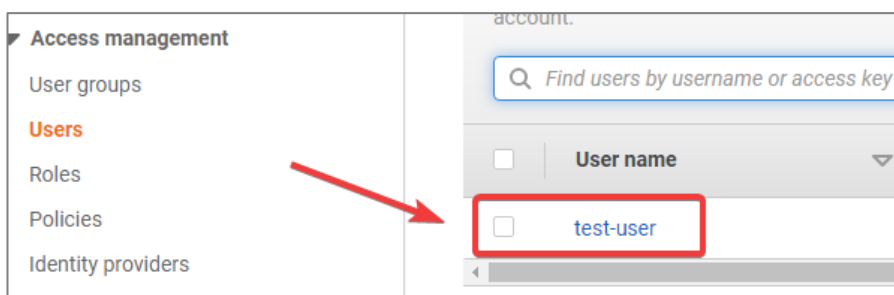
In this section, we will use the Identity and Access Management (IAM) service to set a password policy for our account and also set initial password details of an IAM user.

Setting an initial user password

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

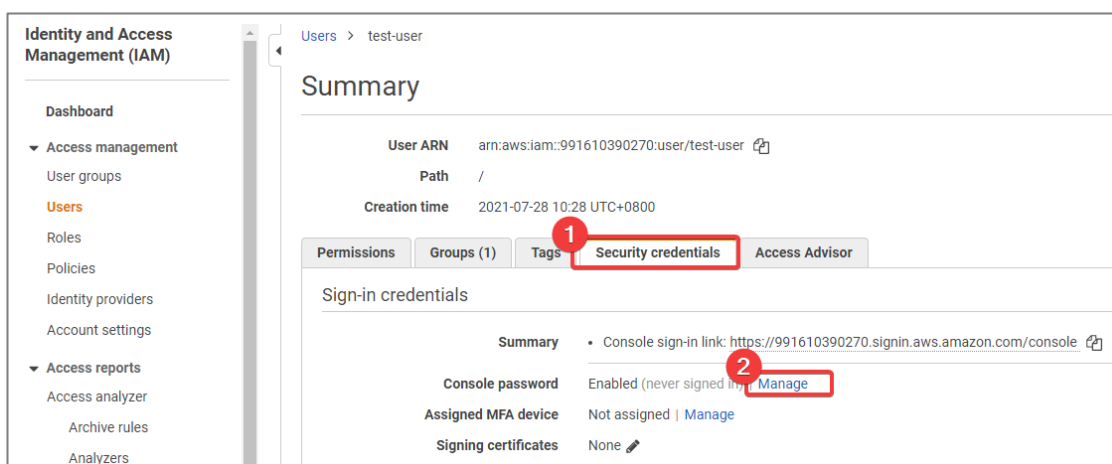
Select *Users*

Select our new user.



Select *Security Credentials*

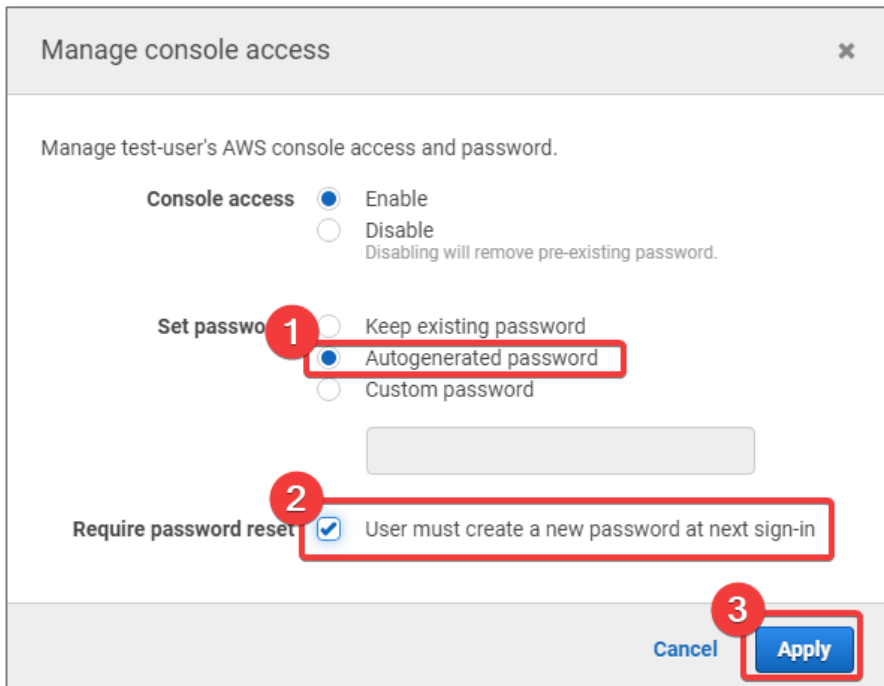
Click *Manage password*



Select *Autogenerated password*

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

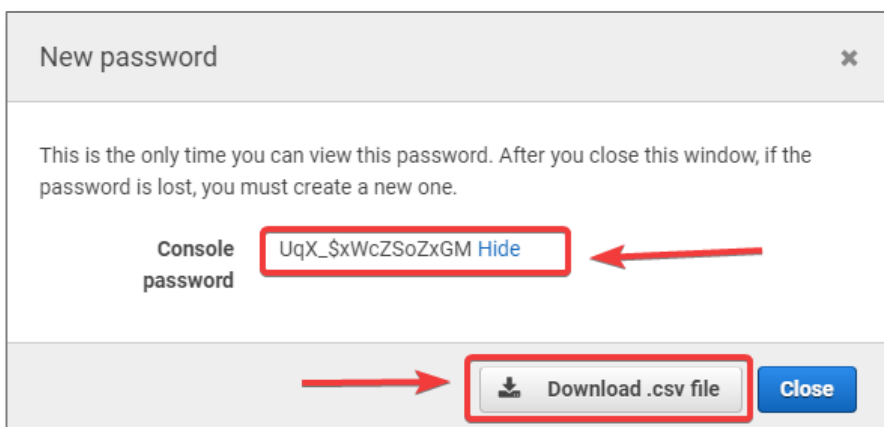
Click *Apply*



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.

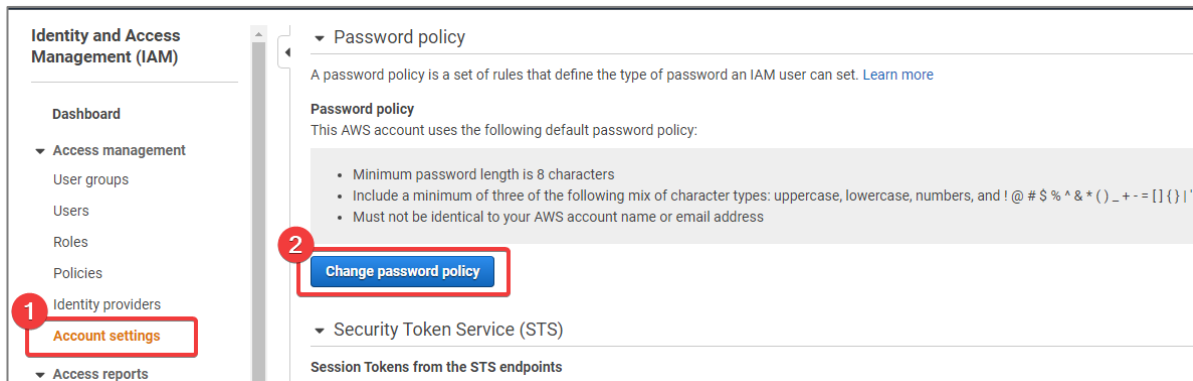
Take note “*This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.*”



Setting an account password policy

Select *Account settings*

Then Click *Change 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

The screenshot shows the 'Set password policy' form in the AWS IAM console. The form title is 'Set password policy'. Below the title, it explains that a password policy is a set of rules that define complexity requirements and mandatory rotation periods for IAM users' passwords. The section 'Select your account password policy requirements:' contains several options:

- ☒ Enforce minimum password length: 8 characters (indicated by a red arrow).
- ☒ Require at least one uppercase letter from Latin alphabet (A-Z)
- ☒ Require at least one lowercase letter from Latin alphabet (a-z)
- ☒ Require at least one number
- ☐ Require at least one non-alphanumeric character (! @ # \$ % ^ & * () _ + - = [] { } | ')
- ☒ Enable password expiration: Expire passwords in 90 day(s)
- ☐ Password expiration requires administrator reset
- ☒ Allow users to change their own password
- ☐ Prevent password reuse

 The entire list of requirements is enclosed in a red box. At the bottom right of the form, there are two buttons: 'Cancel' and 'Save changes'. The 'Save changes' button is highlighted with a red box and a red arrow pointing to it.

Go to *My security credentials*

Dashboard

- Access management
 - User groups
 - Users**
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analysts

Summary

User ARN `arn:aws:iam::991610390270:user/test-user`

Path `/`

Creation time 2021-07-28 10:28 UTC+0800

Permissions **Groups (1)** **Tags** **Security credentials** **Access Advisor**

Sign-in credentials

Summary

- Console sign-in link: <https://991610390270.signin.aws.amazon.com/console>

Console password Enabled (never signed in) [Manage](#)

Assigned MFA device Not assigned | [Manage](#)

Signing certificates None

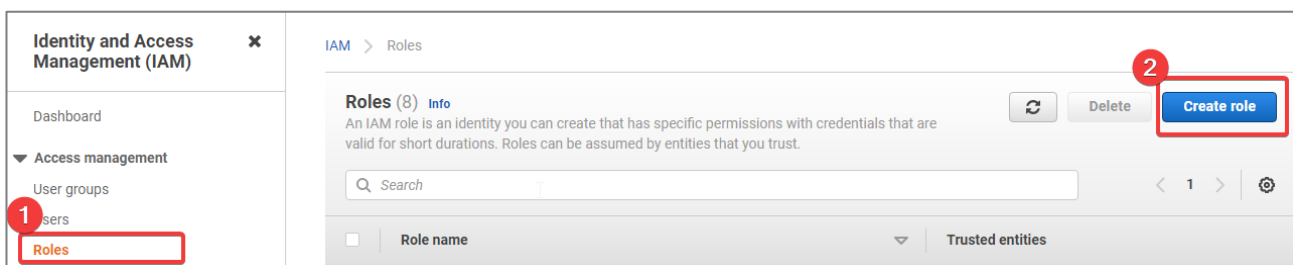
Finish up by signing out of your root user account and signing back in as an *IAM user*.

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*

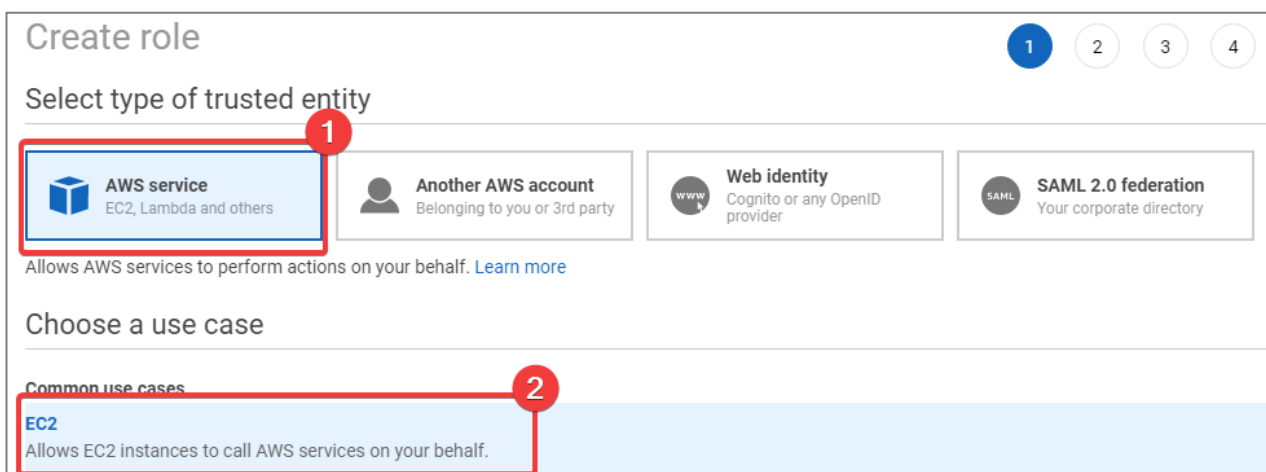
Click *Create role*



Select *AWS service*

Select *EC2*

Click *Next: Permissions*



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*; *Tags* and *Next*; *Review*

Create role

1 2 3 4

▼ Attach permissions policies

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

Create policy

Filter policies 1 Showing 27 results

	Policy name	Used as
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	None
<input type="checkbox"/>	AmazonDMSCloudWatchLogsRole	None
<input type="checkbox"/>	AWSAppSyncPushToCloudWatchLogs	None
<input type="checkbox"/>	AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy	None
<input type="checkbox"/>	AWSOpsWorksCloudWatchLogs	None
<input type="checkbox"/>	AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy	None
<input type="checkbox"/>	CloudWatch-CrossAccountAccess	None
2 <input checked="" type="checkbox"/>	CloudWatchActionsEC2Access	None

► Set permissions boundary

* Required

Cancel Previous 3 **Next: Tags**

Give your role a name and click “*Create role*”

Create role

1 2 3 4

Review

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

1 Role name
Use alphanumeric and '+,_,@,-' characters. Maximum 64 characters.

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

Trusted entities AWS service: ec2.amazonaws.com

Policies CloudWatchActionsEC2Access

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

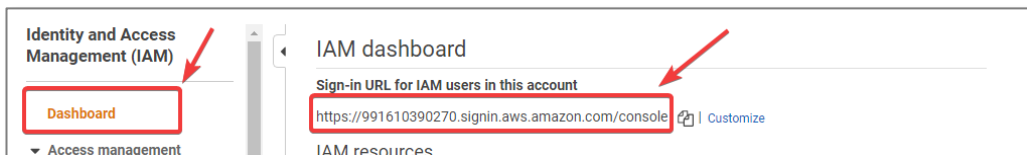
Cancel Previous 2 **Create role**

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.

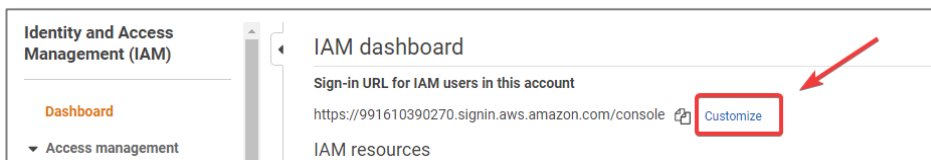
Go to the IAM *Dashboard*

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



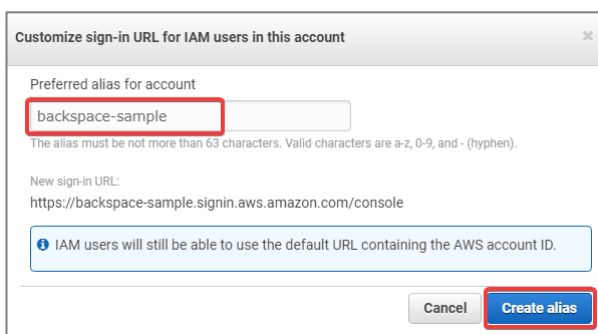
Creating an account alias makes it easier for users to remember the account to login to.

Click *Customize*

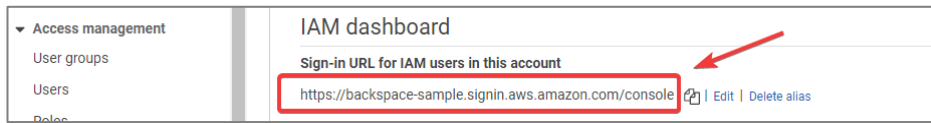


Create a unique alias name

Click *Create alias*



We can now use the account alias for logging in.

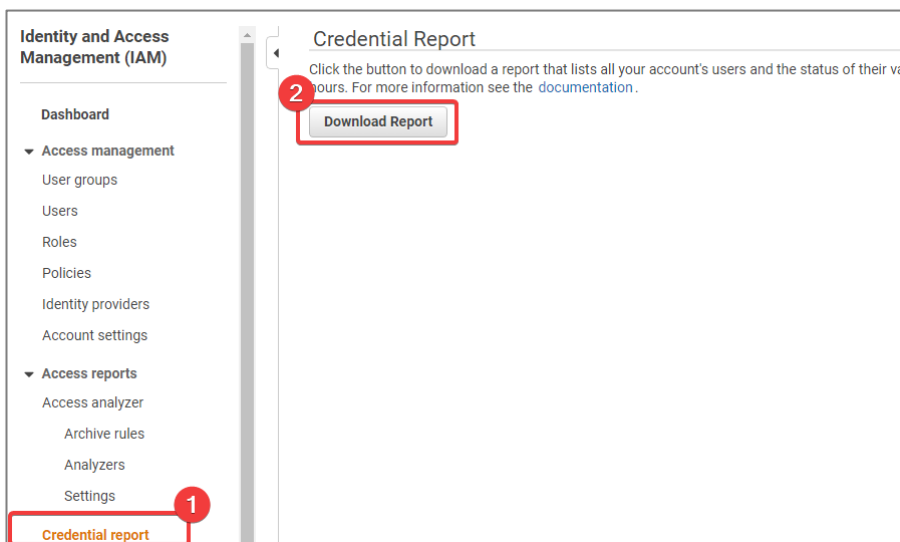


Creating a Credentials Report

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_crea	password	password	password	password	mfa_activ	access_ke	access_ke	access_ke	access_ke	access_ke	access_ke	access_ke
2	<root_acc	arn:aws:iam::	2021-07-1	not_supp	2021-07-2	not_supp	not_supp	FALSE	FALSE	N/A	N/A	N/A	N/A	FALSE	N/A
3	test-user	arn:aws:iam::	2021-07-2	TRUE	no_inform	2021-07-2	2021-10-2	FALSE	TRUE	2021-07-2	N/A	N/A	N/A	FALSE	N/A
4															

Clean Up

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

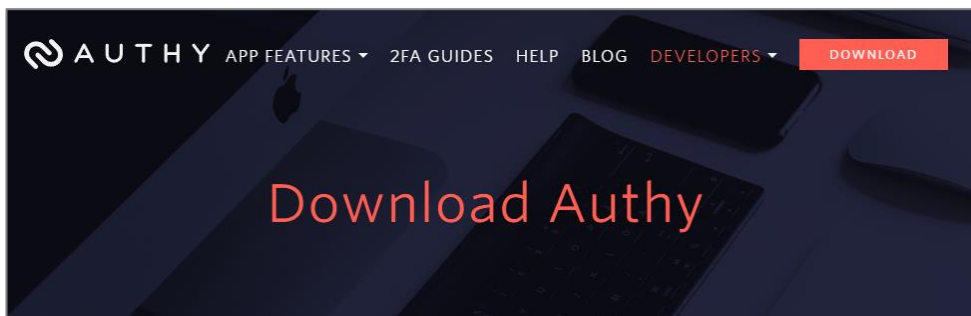
🎥 Implementing Multi Factor Authentication (MFA)

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.

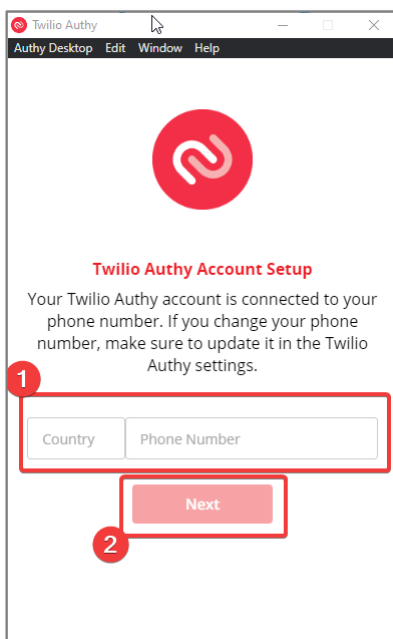
Download and install *Authy* to your desktop or mobile.

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

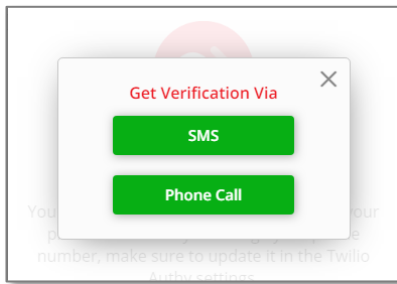
<https://authy.com/download/>



Enter your phone number details



Verify by *SMS (mobile phone)* or *Phone Call (landline)*

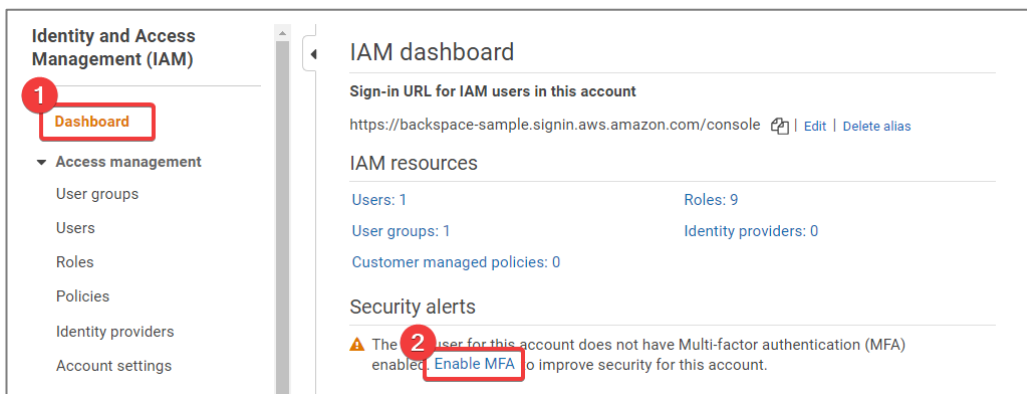


After you have setup Authy

Go to the IAM Management console

Select *Dashboard*

Select *Enable MFA*

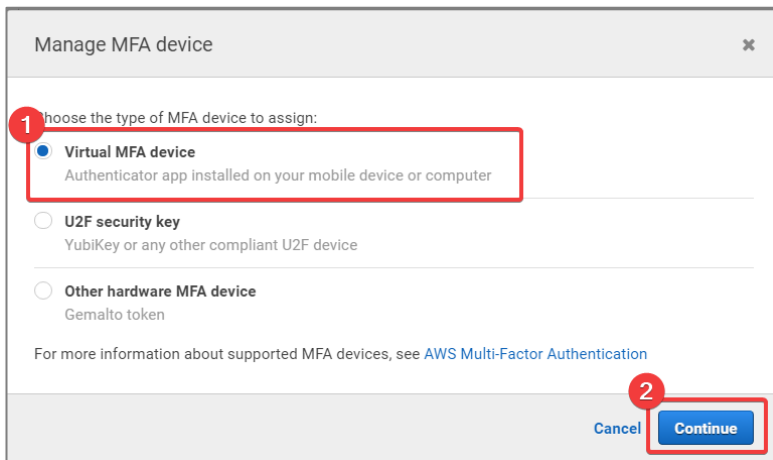


Click *Activate MFA*



Select *Virtual MFA device*

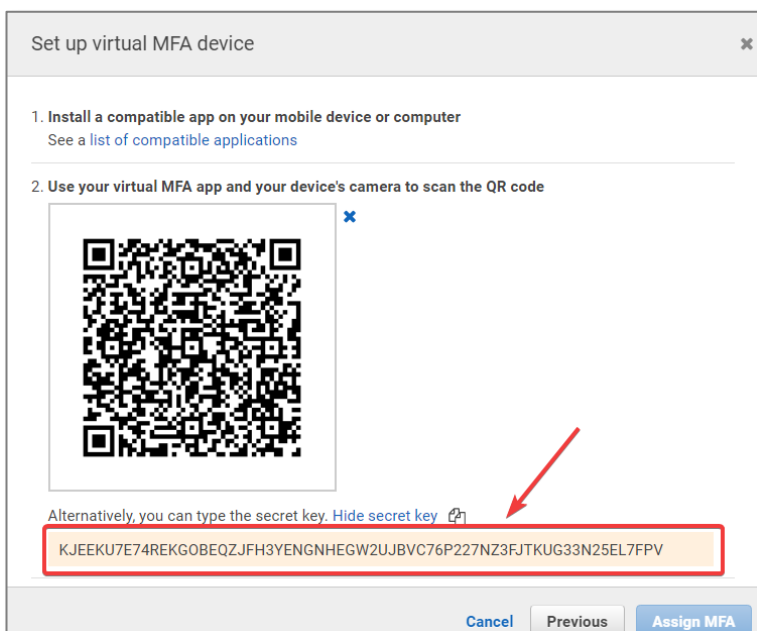
Click *Continue*



Adding account using Authy Desktop app:

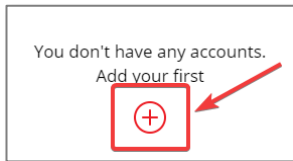
Click on *Show secret key for manual configuration*

Copy the *secret key*



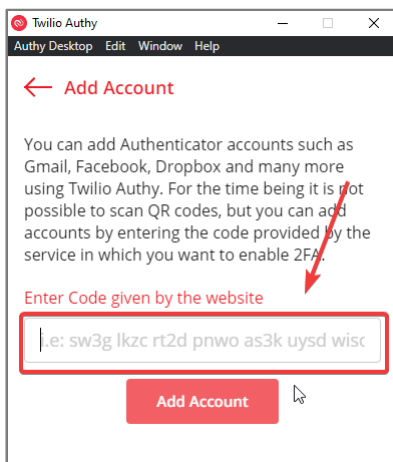
Open *Authy* app

Click the *add icon*



Paste the secret key

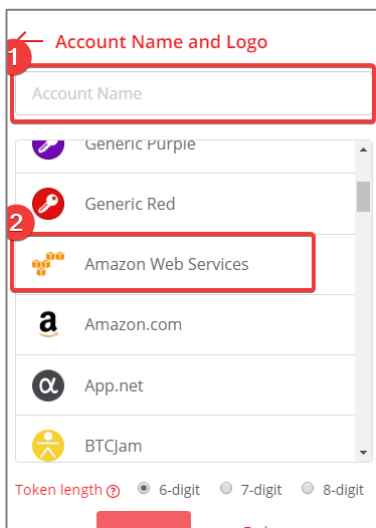
Click *Add Account*



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

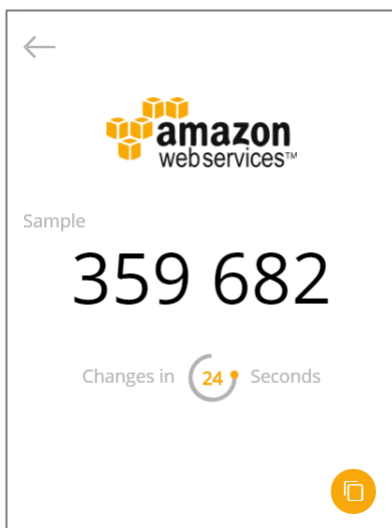
Select *SCAN QR CODE*

Scan the QR code



Entering Authentication codes


Type the code into *Authentication code 1*



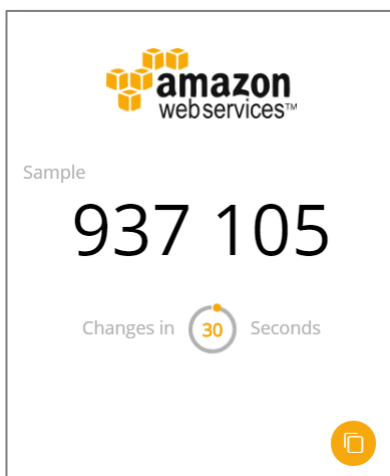
3. Type two consecutive MFA codes below

MFA code 1

MFA code 2



Wait for the code to change on the *Authy* app




Enter the second code

Click *Activate virtual MFA*

3. Type two consecutive MFA codes below

MFA code 1

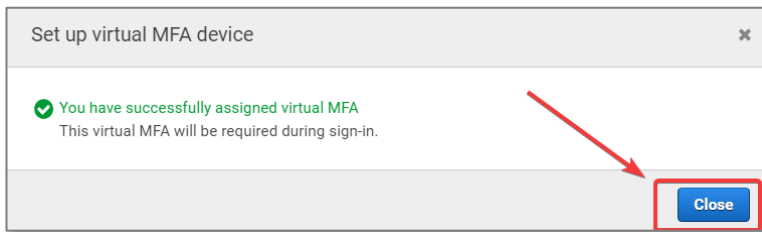
MFA code 2



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

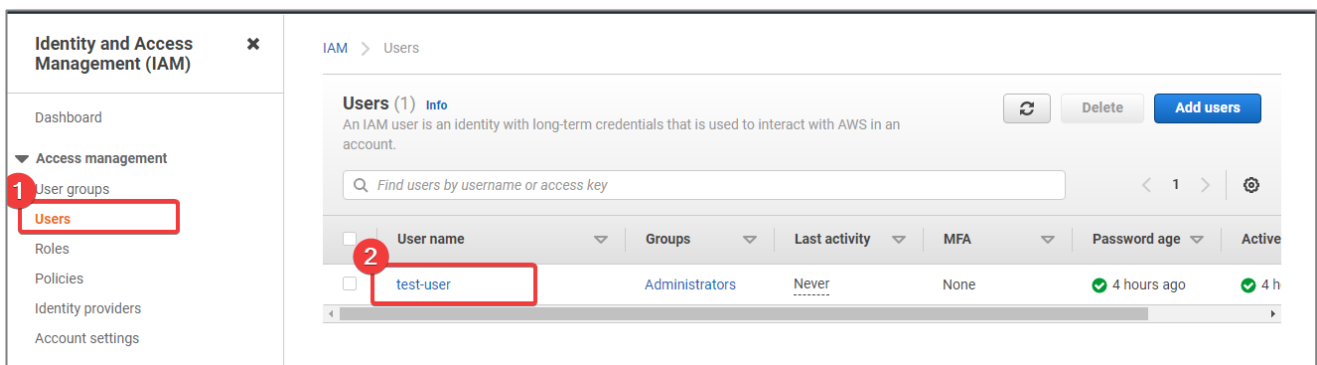
Click *Close*



Implementing MFA on an IAM User

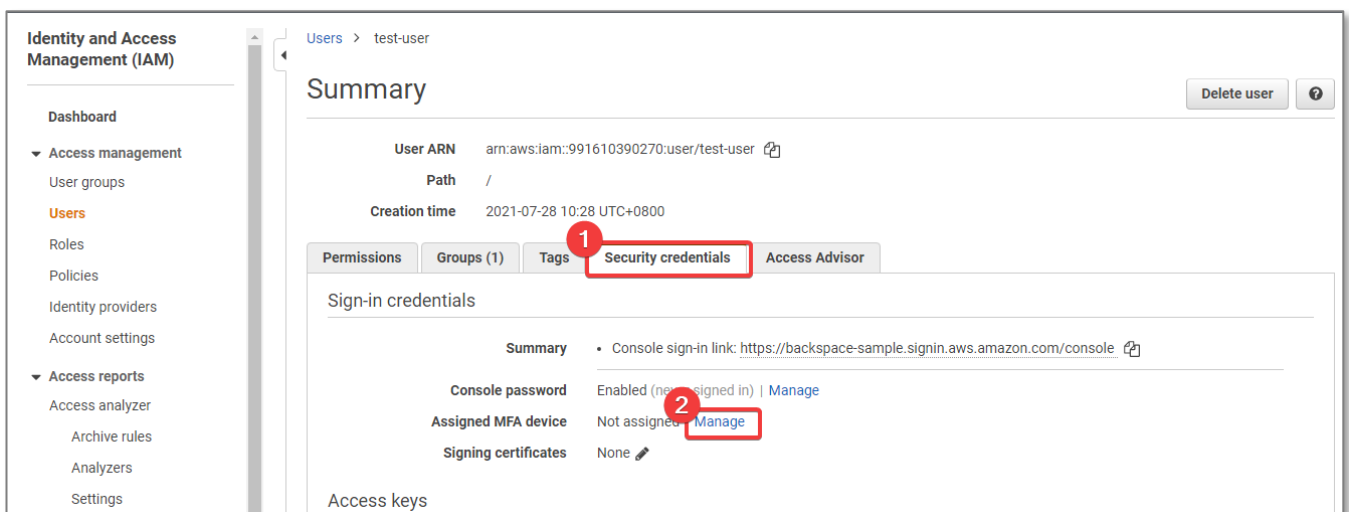
You can implement MFA on a user:

Click on the *Users*

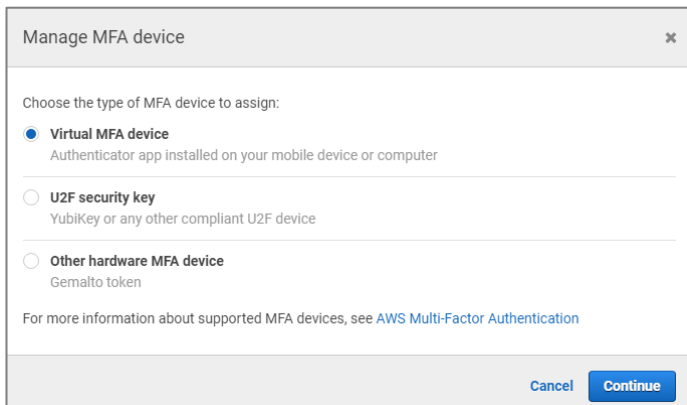


Select *Security credentials* tab

Click *Manage* for Assigned MFA device



Repeat the *MFA process*



The screenshot shows a 'Manage MFA device' dialog box with a close button (X) in the top right corner. The main heading is 'Choose the type of MFA device to assign:'. There are three radio button options: 'Virtual MFA device' (selected), 'U2F security key', and 'Other hardware MFA device'. Below 'Virtual MFA device' is the text 'Authenticator app installed on your mobile device or computer'. Below 'U2F security key' is 'YubiKey or any other compliant U2F device'. Below 'Other hardware MFA device' is 'Gemalto token'. At the bottom, there is a link: 'For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)'. At the very bottom are 'Cancel' and 'Continue' buttons.

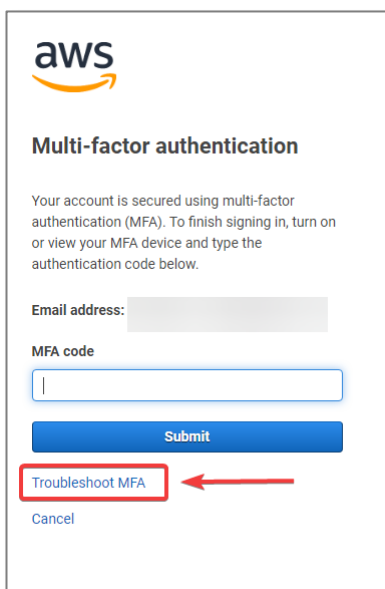
What to do if you are locked out of your root account

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*



The screenshot shows the AWS 'Multi-factor authentication' login screen. At the top is the AWS logo. Below it is the title 'Multi-factor authentication'. The text reads: '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.' There is an 'Email address:' label followed by a text input field. Below that is an 'MFA code' label followed by a text input field. A blue 'Submit' button is below the MFA code field. At the bottom, there is a link 'Troubleshoot MFA' which is highlighted with a red rectangular box. A red arrow points from the right towards this box. Below the 'Troubleshoot MFA' link is a 'Cancel' link.

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.

[Re-sync MFA device](#)

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.

[Sign in using alternative factors](#)

