

## Task 1:

Products

Solutions

Pricing

Documentation

Learn

Partner Network

AWS Marketplace

Customer Enablement

Events

Explore More

About AWS


Contact Us

Support

English

My Account

Sign In to the Console



### Congratulations!

Thank you for signing up with AWS.

We are activating your account, which should take a few minutes. You will receive an email when this is complete.

Go to the AWS Management Console

[Sign up for another account](#) or [Contact Sales](#)

As an additional step, tell us more about

In this step, I have created my AWS account.

Multi-factor authentication (MFA) (1)

Remove

Resync

Assign MFA device

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

	Device type	Identifier	Certifications	Created on
<input type="radio"/>	Virtual	arn:aws:iam::992382676655:mfa/Tims-Phone	Not Applicable	Now

In this step, I have set up my phone for MFA.

### Review and create

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

User details

User name Tim	Console password type Custom password	Require password reset Yes
------------------	--	-------------------------------

Permissions summary

< 1 >

Name	Type	Used as
<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy
<a href="#">IAMUserChangePassword</a>	AWS managed	Permissions policy

Tags - optional

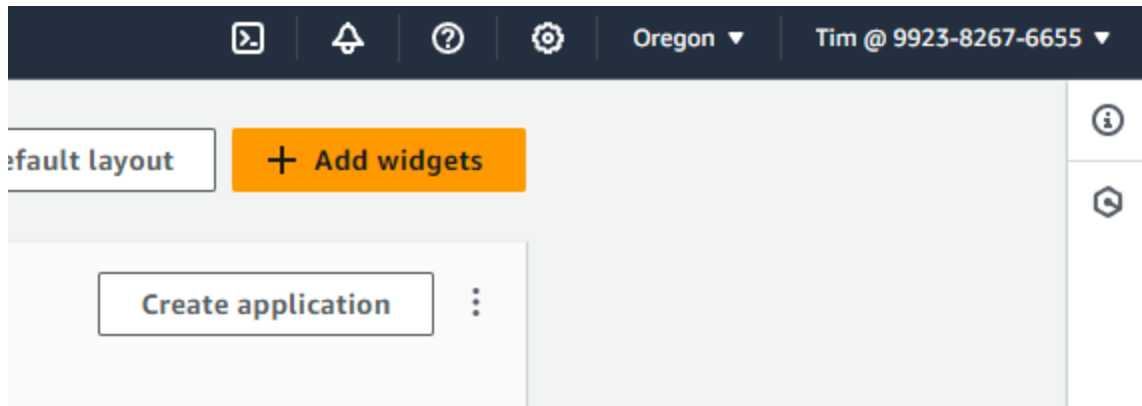
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

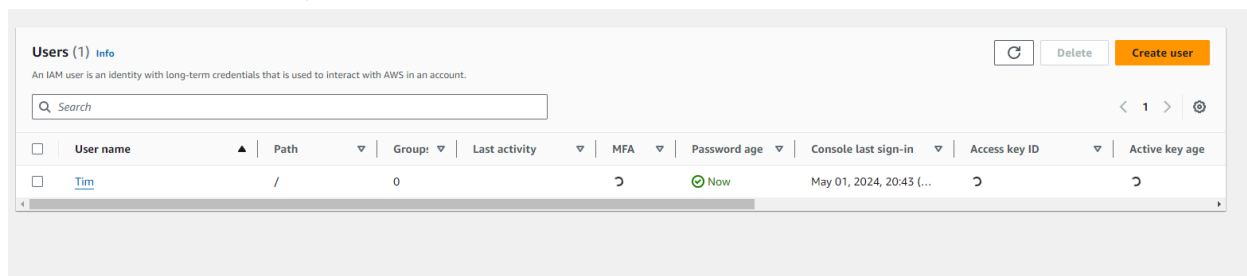
Add new tag

You can add up to 50 more tags.

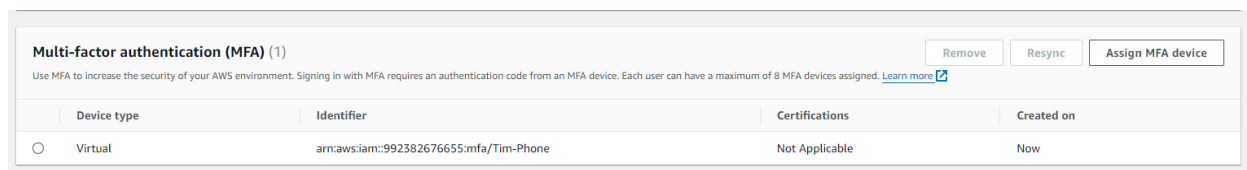
In this step, I have created a new user. <https://992382676655.signin.aws.amazon.com/console>



I am now signed in as my IAM admin.

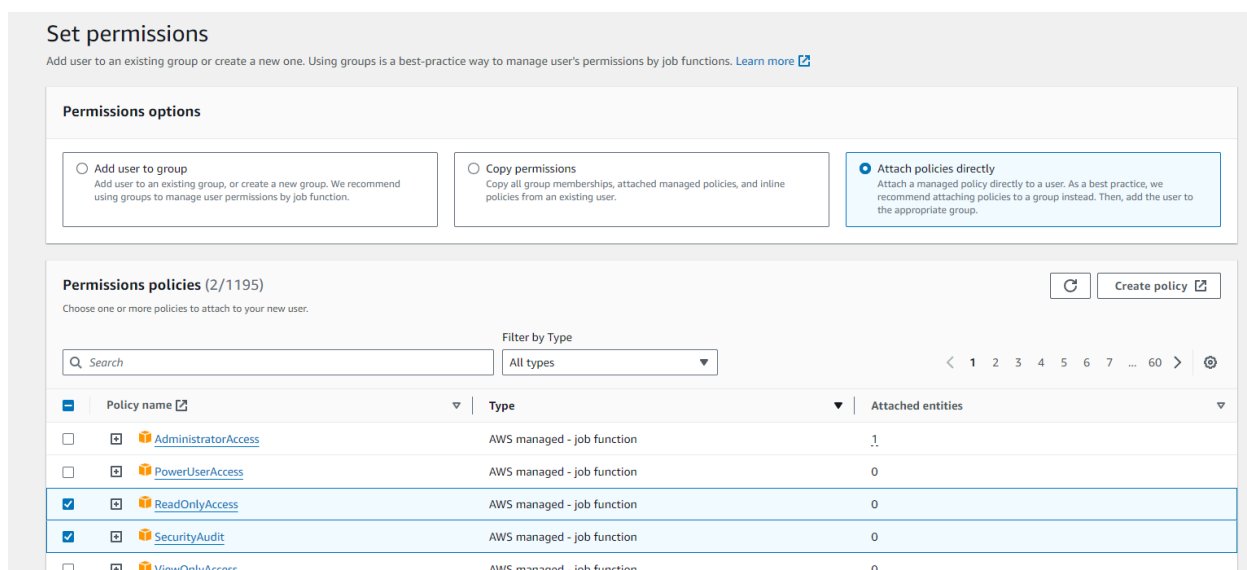


Here I can see the user that I created.



I have set up my phone as an MFA device for this user as well.

## Task 2:



In this step, I have created a new user named “auditor” and am assigning it less permissions. Instead of giving it admin permissions, I only give them the 2 that are checked in the picture.



```
timothyd@ubuntu:~$ virtualenv -p python3 venv
created virtual environment CPython3.10.12.final.0-64 in 254ms
creator CPython3Posix(dest=/home/timothyd/venv, clear=False, no_vcs_ignore=False, global=False)
seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy, app_data_dir=/home/timothyd/.local/share/virtualenv)
added seed packages: pip==22.0.2, setuptools==59.6.0, wheel==0.37.1
activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowerShellActivator,PythonActivator
timothyd@ubuntu:~$ source venv/bin/activate
(venv) timothyd@ubuntu:~$ pip install scoutsuite
```

In this step, I have created the virtual environment and then downloaded scoutsuite.

```
(venv) timothyd@ubuntu:~$ scout --help
usage: scout [-h] [-v] {aws,gcp,azure,aliyun,oci,kubernetes} ...

options:
  -h, --help            show this help message and exit
  -v, --version          show program's version number and exit

The provider you want to run scout against:
{aws,gcp,azure,aliyun,oci,kubernetes}
  aws                  Run Scout against an Amazon Web Services account
  gcp                  Run Scout against a Google Cloud Platform account
  azure                Run Scout against a Microsoft Azure account
  aliyun               Run Scout against an Alibaba Cloud account
  oci                  Run Scout against an Oracle Cloud Infrastructure account
  kubernetes           Run Scout against a Kubernetes cluster

To get additional help on a specific provider run: scout.py {provider} -h
(venv) timothyd@ubuntu:~$
```

Scout has been successfully installed.

```
(venv) timothyd@ubuntu:~$ scout aws --profile auditor
2024-05-01 21:35:32 ubuntu scout[5605] INFO Launching Scout
2024-05-01 21:35:32 ubuntu scout[5605] INFO Authenticating to cloud provider
2024-05-01 21:35:34 ubuntu scout[5605] INFO Gathering data from APIs
2024-05-01 21:35:34 ubuntu scout[5605] INFO Fetching resources for the ACM service
2024-05-01 21:35:35 ubuntu scout[5605] INFO Fetching resources for the Lambda service
2024-05-01 21:35:35 ubuntu scout[5605] INFO Fetching resources for the CloudFormation service
2024-05-01 21:35:36 ubuntu scout[5605] INFO Fetching resources for the CloudTrail service
2024-05-01 21:35:36 ubuntu scout[5605] INFO Fetching resources for the CloudWatch service
2024-05-01 21:35:37 ubuntu scout[5605] INFO Fetching resources for the CloudFront service
2024-05-01 21:35:37 ubuntu scout[5605] INFO Fetching resources for the CodeBuild service
2024-05-01 21:35:38 ubuntu scout[5605] INFO Fetching resources for the Config service
2024-05-01 21:35:38 ubuntu scout[5605] INFO Fetching resources for the Direct Connect service
2024-05-01 21:35:39 ubuntu scout[5605] INFO Fetching resources for the DynamoDB service
2024-05-01 21:35:39 ubuntu scout[5605] INFO Fetching resources for the EC2 service
2024-05-01 21:35:40 ubuntu scout[5605] INFO Fetching resources for the EFS service
2024-05-01 21:35:40 ubuntu scout[5605] INFO Fetching resources for the ElastiCache service
2024-05-01 21:35:40 ubuntu scout[5605] INFO Fetching resources for the ELB service
2024-05-01 21:35:41 ubuntu scout[5605] INFO Fetching resources for the ELBv2 service
2024-05-01 21:35:41 ubuntu scout[5605] INFO Fetching resources for the EMR service
2024-05-01 21:35:42 ubuntu scout[5605] INFO Fetching resources for the IAM service
```

In this step, I have started the scan.

Scout Analytics Compute Containers Database Management Messaging Network Security Storage Filters				
Amazon Web Services > 992382676655				
Dashboard				
Service	Resources	Rules	Findings	Checks
ACM	0	2	0	0
Lambda	0	0	0	0
CloudFormation	0	1	0	0
CloudFront	0	3	0	0
CloudTrail	0	9	17	17
CloudWatch	0	1	0	0
Codebuild	0	0	0	0
Config	0	1	17	17
Directconnect	0	0	0	0
DynamoDB	0	0	0	0
EC2	17	28	68	476
EFS	0	0	0	0
ElastiCache	0	0	0	0
ELB	0	3	0	0
ELBV2	0	5	0	0

The scan has been completed and the report has been made.

Scout Analytics Compute Containers Database Management Messaging Network Security Storage Filters				
IAM Dashboard				
Filter findings	Show All	Good	Warning	Danger
Managed Policy Allows All Actions				+
Minimum Password Length Too Short				+
Password Expiration Disabled				+
Password Policy Allows the Reuse of Passwords				+
Passwords Expire after 90 Days				+
Root Account Used Recently				+
Root Account without Hardware MFA				+
AssumeRole Policy Allows All Principals				+
Credentials Unused for 90 Days or Greater Are Not Disabled				+
Cross-Account AssumeRole Policy Lacks External ID and MFA				+
Lack of Key Rotation for (Active) Days				+
Lack of Key Rotation for (Inactive) Days				+
Managed Policy Allows "iam:PassRole" For All Resources				+
Managed Policy Allows "NotActions"				+

The vulnerability that I have picked is the “Password Policy Allows the Reuse of Passwords” in the IAM service. This vulnerability pretty much just means that when setting or resetting a password, it should not be a password that has already been used on the account. This is a vulnerability because if your account has been compromised and you need to reset your password, you should not reset it to a password that has been already exposed to a hacker. This will just allow for your account to be easily compromised again. Instead, you should pick a new unique password that will make it more difficult for an attacker to get into your account.

The steps that are needed to fix this is to first go into the “Account Settings” and then go into “Edit Password Policy”. From here , you check the “Custom” box and it will allow you to change the password policies. Check the box that says “Prevent password reuse” and then input the number of

previous passwords that you want to be remembered. Then hit “Save Changes”.

[IAM](#) > [Account Settings](#) > Edit password policy

## Edit password policy [Info](#)

### Password policy

☐ IAM default

Apply default password requirements.

☒ Custom

Apply customized password requirements.

#### Password minimum length.

Enforce a minimum length of characters.

characters

Needs to be between 6 and 128.

#### Password strength

- ☐ Require at least one uppercase letter from the Latin alphabet (A-Z)
- ☐ Require at least one lowercase letter from the Latin alphabet (a-z)
- ☐ Require at least one number
- ☐ Require at least one non-alphanumeric character (!@#\$%^&\*()\_+-=[]{}|')

#### Other requirements

- ☐ Turn on password expiration
- ☐ Password expiration requires administrator reset
- ☐ Allow users to change their own password
- ☒ Prevent password reuse

Remember  password(s)

Needs to be between 1 and 24.

[Cancel](#)

[Save changes](#)

❗ Managed Policy Allows All Actions	+
❗ Minimum Password Length Too Short	+
❗ Password Expiration Disabled	+
❗ Passwords Expire after 90 Days	+
❗ Root Account Used Recently	+
❗ Root Account without Hardware MFA	+
✅ AssumeRole Policy Allows All Principals	+
✅ Credentials Unused for 90 Days or Greater Are Not Disabled	+
✅ Cross-Account AssumeRole Policy Lacks External ID and MFA	+
✅ Lack of Key Rotation for (Active) Days	+
✅ Lack of Key Rotation for (Inactive) Days	+
✅ Managed Policy Allows "iam:PassRole" For All Resources	+
✅ Managed Policy Allows "NotActions"	+
✅ Managed Policy Allows "sts:AssumeRole" For All Resources	+
✅ Managed Policy Not Attached to Any Entity	+
✅ Password Policy Allows the Reuse of Passwords	+
✅ Policy with Denied User Actions for Group Objects	.

After rerunning the scan, we can now see that "Password Policy Allows the Reuse of Passwords" is no longer a vulnerability. This fix does not cost any money to implement.