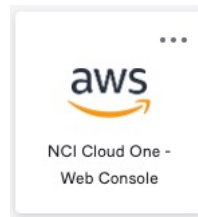
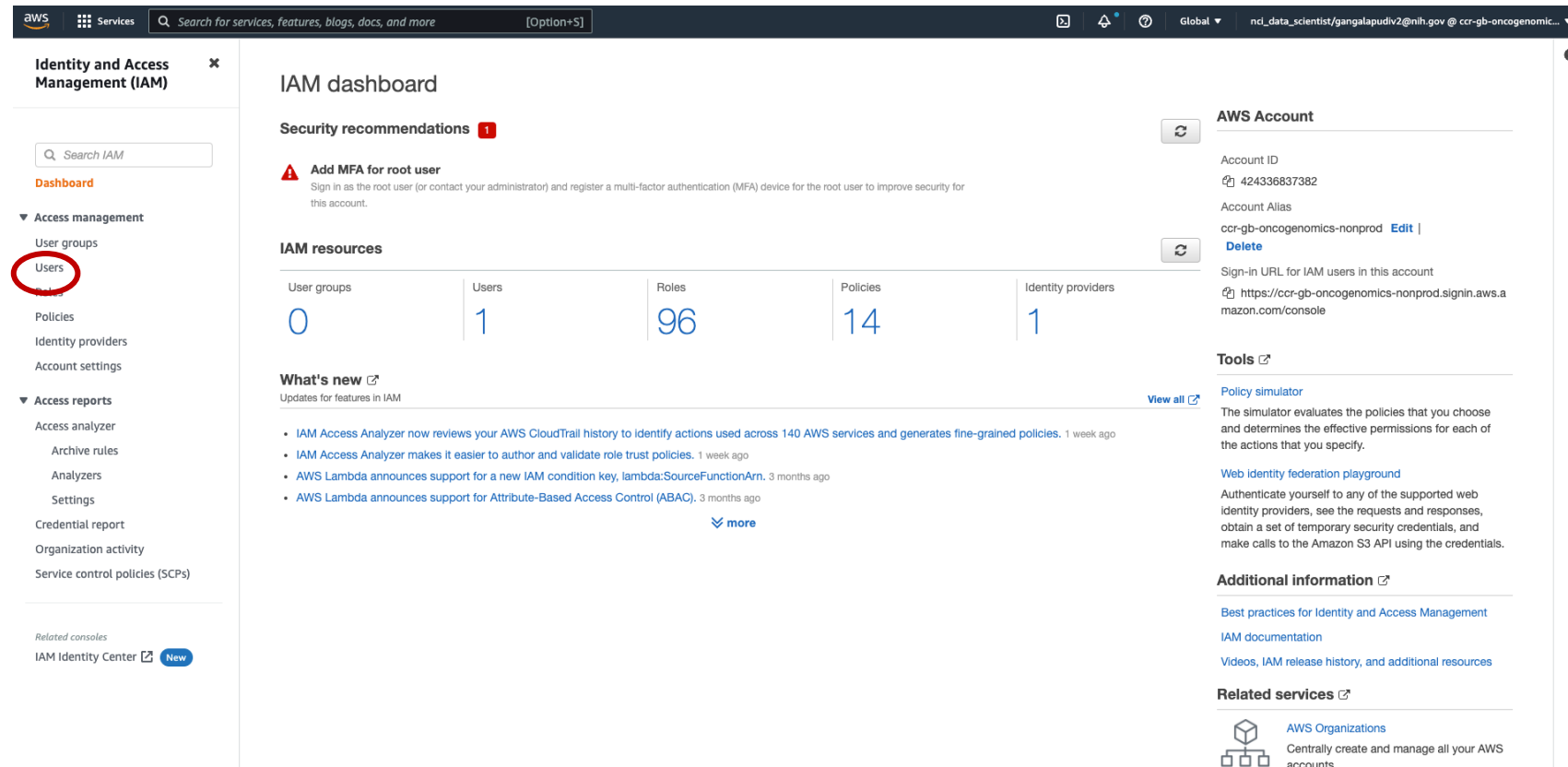


Adding User on IAM



- Login in to iam.cancer.gov and click on [aws](#) (NCI cloud one web console)
- In the search box type **IAM** and click on the popup to reach the IAM dashboard.
- Click on **Users** tab in the left side of the page



The screenshot shows the AWS IAM dashboard. The left sidebar is titled 'Identity and Access Management (IAM)' and contains a search bar and a list of navigation items. The 'Users' item is highlighted with a red circle. The main content area is titled 'IAM dashboard' and includes a 'Security recommendations' section with a warning icon and text about adding MFA for the root user. Below this is a table of 'IAM resources' with columns for User groups, Users, Roles, Policies, and Identity providers. The 'Users' column shows a count of 1. There is also a 'What's new' section with updates for IAM features. On the right side, there is an 'AWS Account' section with account details and a 'Tools' section with links to the Policy simulator and Web identity federation playground. At the bottom right, there is an 'Additional information' section with links to best practices, documentation, and release history, and a 'Related services' section with a link to AWS Organizations.

Identity and Access Management (IAM)

Search IAM

Access management

- User groups
- Users**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related consoles

- IAM Identity Center **New**

IAM dashboard

Security recommendations

Add MFA for root user

Sign in as the root user (or contact your administrator) and register a multi-factor authentication (MFA) device for the root user to improve security for this account.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	1	96	14	1

What's new

Updates for features in IAM

- IAM Access Analyzer now reviews your AWS CloudTrail history to identify actions used across 140 AWS services and generates fine-grained policies. 1 week ago
- IAM Access Analyzer makes it easier to author and validate role trust policies. 1 week ago
- AWS Lambda announces support for a new IAM condition key, `lambda:SourceFunctionArn`. 3 months ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC). 3 months ago

AWS Account

Account ID
424336837382

Account Alias
ccr-gb-oncogenomics-nonprod [Edit](#) | [Delete](#)

Sign-in URL for IAM users in this account
<https://ccr-gb-oncogenomics-nonprod.signin.aws.amazon.com/console>

Tools

[Policy simulator](#)

The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

[Web identity federation playground](#)

Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API using the credentials.

Additional information


- [Best practices for Identity and Access Management](#)
- [IAM documentation](#)
- [Videos, IAM release history, and additional resources](#)

Related services

[AWS Organizations](#)




Centrally create and manage all your AWS accounts.

Click on **Add users** tab

 Services

Search for services, features, blogs, docs, and more

[Option+S]



Global

nd_data_scientist/gangalapudiv2@nih.gov @ ccr-gb-oncogenic...

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers


Settings

Credential report

Organization activity

Service control policies (SCPs)

Related consoles




IAM Identity Center 

Introducing the new Users list experience


We've redesigned the Users list experience to make it easier to use. [Let us know what you think.](#)



IAM > Users

Users (1) [Info](#)



Find users by username or access key

< 1 > 

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	data-science-testuser1	None	 5 hours ago	None	None	 Yesterday

- Enter the User name under [Set user details](#); Username must prefix with [data-science-](#)
- Under [select AWS access type](#) select [Access key – programmatic access](#) and click Next

aws

Services

Search for services, features, blogs, docs, and more

[Option+S]

Global

nci_data_scientist/gangalapudiv2@nih.gov @ ccr-gb-oncogenic...

Add user

12345

Set user details

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

User name*

data-science-testuser2

+ Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

☒ Access key - Programmatic access

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

☐ Password - AWS Management Console access

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

* Required

Cancel

Next: Permissions

- Leave [Set permissions](#) section as it is.
- Under [Set permissions boundary](#) Select [Use a permissions boundary to control the maximum user permissions](#)
- Enter [science](#) in the search box and select “[PermissionBoundary_DataScience](#)” from the drop down then click on Next

aws

Services

Search for services, features, blogs, docs, and more

[Option+S]

?

Global

nci_data_scientist/gangalapudiv2@nih.gov @ ccr-gb-oncogenic...

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

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

☐

Create user without a permissions boundary

☒

Use a permissions boundary to control the maximum user permissions

Select policy to set the permissions boundary

Create policy

Filter policies

science

Showing 1 result

	Policy name	Type	Used as
<input checked="" type="radio"/>	PermissionBoundary_DataScience	Customer managed	Boundary (2)

Cancel

Previous

Next: Tags

Skip Section 3 and click Next.

aws

Services

Search for services, features, blogs, docs, and more

[Option+S]

Global

nci_data_scientist/gangalapudiv2@nih.gov @ ccr-gb-oncogenic...

Add user

1

2

3

4

5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<div>Add new key</div>		

You can add 50 more tags.

Cancel

Previous

Next: Review

click [create user](#).

aws

Services

Search for services, features, blogs, docs, and more

[Option+S]

Global

nci_data_scientist/gangalapudiv2@nih.gov @ ccr-gb-oncogenic...

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.

This user has no permissions

You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions.

User details

User name

data-science-testuser2

AWS access type

Programmatic access - with an access key

Permissions boundary

[PermissionBoundary_DataScience](#)

Tags

No tags were added.

Cancel

Previous

Create user

The user will be created; click on [download .csv](#) tab . This file contains the password, Access key ID, secret access key.

aws

Services

Search for services, features, blogs, docs, and more

[Option+S]

Global

nci_data_scientist/gangalapudiv2@nih.gov @ ccr-gb-oncogenic...

Add user

12345

✓

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://ccr-gb-oncogenomics-nonprod.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶	✓ data-science-testuser2	AKIAWFTDSJMDEUFJZAH3	***** Show

Close

- After downloading the csv file, log into biowulf and run the following commands and enter the [AWS Accesss key ID](#), [AWS secret Access Key](#) information from the downloaded csv file.
- Enter Default region name as [us-east-1](#)
- Enter Default output format as [json](#)

```
module load aws/current
aws configure
AWS Access Key ID [None]: AKITDSJMDBPIKMNXM
AWS Secret Access Key [None]: wE1Er7wei5In1Q723LD+jeY/I8YoTbtZR
Default region name [None]: us-east-1
Default output format [None]: json
```

- This will enable access to the s3 bucket. You can verify using the following command

```
[gangalapudiv2/ngs_pipeline_testing]$ aws s3 ls s3://ccr-genomics-testdata/testdata/
2022-10-06 14:13:43    184546 Test1_R_T_R1.fastq.gz
2022-10-06 14:13:44    186371 Test1_R_T_R2.fastq.gz
2022-10-06 14:13:44    160880 Test2_R_T_R1.fastq.gz
2022-10-06 14:13:43    163153 Test2_R_T_R2.fastq.gz
2022-10-06 14:13:45    159281 Test3_R_T_R1.fastq.gz
2022-10-06 14:13:44    162359 Test3_R_T_R2.fastq.gz
```