

Search IAM

when on this page, click on usergroups

create a new group called manage-.....
see below, mine is manage-airsoft-workshop

User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

User groups (1) <small>Info</small>			
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.			
<input type="text"/> Filter User groups by property or group name and press enter			
<input type="checkbox"/>	Group name	Users	Permissions



Delete

Create group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

manage-airsoft-workshop

Maximum 128 characters. Use alphanumeric and '+,-,.,@-' characters.

skip the policies part, we will create one in a moment,

submit and create group

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	manage-airsoft-workshop		⚠ 0 ⚠ Not defined	Now

now heead over to the policies under access management

click create a new policy

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Policies (1017) Info

A policy is an object in AWS that defines permissions.



Actions ▾

Create policy

now in the top corner click import managed policies

1 2 3

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Visual editor JSON

Import managed policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": []  
4 }
```

Import managed policies

search AmazonS3FullAccess and click import

Choose policies to import			
The permissions for the chosen policies will be added to your policy. You can review your policy's final permissions before you save it.			
Filter policies		Policy name	Description
<input type="radio"/>	▶	AmazonDMSRedshiftS3Role	None
<input checked="" type="radio"/>	▶	AmazonS3FullAccess	Provides full access to all buckets via ...
<input type="radio"/>	▶	AmazonS3ObjectLambdaExecutionRolePolicy	Provides AWS Lambda functions permis...
<input type="radio"/>	▶	AmazonS3OutpostsFullAccess	Provides full access to Amazon S3 on ...
<input type="radio"/>	▶	AmazonS3OutpostsReadOnlyAccess	Provides read only access to Amazon ...
<input type="radio"/>	▶	AmazonS3ReadOnlyAccess	Provides read only access to all bucket...
<input type="radio"/>	▶	AWSBackupServiceRolePolicyForS3Backup	Policy containing permissions necessa...
<input type="radio"/>	▶	AWSBackupServiceRolePolicyForS3Restore	Policy containing permissions necessa...
<input type="radio"/>	▶	IVSRecordToS3	Service Linked Role to perform S3 Put...
<input type="radio"/>	▶	QuickSightAccessForS3StorageManagementA...	Policy used by QuickSight team to acc...
<input type="radio"/>	▶	S3StorageLensServiceRolePolicy	Enables access to AWS Services and ...

Cancel Import

now it will open a json template, we need to fill with our s3 bucket policy (airsoft-workshop).

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Visual editor JSON

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "s3:*",  
8         "s3-object-lambda:*"  
9       ],  
10      "Resource": "*"  
11    }  
12  ]  
13 }
```

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Bridge the gap between on-premises environments and the cloud with AWS Storage Gateway.

Amazon S3 > Buckets > airsoft-workshop

airsoft-workshop [Info](#)

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access

⚠️ Public

copy the arn

```
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::airsoft-workshop/*"
```

add it into the resource... create a list... one item is thebucket itself, and the /* adds another rule for all files/folders in the bucket

Visual editor

JSON

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Action": [  
7                 "s3:*",  
8                 "s3-object-lambda:*"  
9             ],  
10            "Resource": [  
11                "arn:aws:s3:::airsoft-workshop",  
12                "arn:aws:s3:::airsoft-workshop/*"  
13            ]  
14        }  
15    ]  
16 }
```

go forward to review and add a name and description for the policy

Review policy

Name*

airsoft-workshop-policy

Use alphanumeric and '+=_@-' characters. Maximum 128 characters.

Description

Access to S3 bucket for Airsoft Workshop static files

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

click create policy and return back to the policy page view

The policy [airsoft-workshop-policy](#) has been created.

IAM > Policies

Policies (1019) [Info](#)

A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter.

1

Policy name

Type

Used as

Description

airsoft-workshop-policy

Customer managed

None

Access to S3 bucket for Airsoft Workshop static files

now we got to attach it to groups that were created click on user groups and then permission click on policy, add permissions and attach policy

IAM > User groups

User groups (2) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

Group name

Users

Permissions

manage-airsoft-workshop

⚠ 0

>Loading

IAM > User groups > manage-airsoft-workshop

manage-airsoft-workshop

[Delete](#)

[Edit](#)

Summary

User group name: manage-airsoft-workshop | Creation time: November 30, 2022, 20:38 (UTC) | ARN: arn:aws:iam::761603658625:group/manage-airsoft-workshop

[Users](#) [Permissions](#) [Access Advisor](#)

Permissions policies (0) [Info](#)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

Policy name



[Simulate](#)

[Remove](#)

[Add permissions](#)

[Attach policies](#)

[Create inline policy](#)

No resources to display

search and select the policy. and then hit attach policy

Other permission policies (Selected 1/799)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter policies by property or policy name and press enter.

Policies attached to this user group.

Policy name

IAM > User groups > manage-airsoft-workshop

airsoft-workshop-policy

manage-airsoft-workshop

Summary

User group name: manage-airsoft-workshop | Creation time: November 30, 2022, 20:38 (UTC)

the group, on the user page click add user...

IAM > Users

Users (1) Info						
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.						
Find users by username or access key						
User name	Groups	Last activity	MFA	Password age	Active key age	
gwils-boutique-ado-staticfiles-user	manage-gwils-boutique-ado	32 days ago	None	None	81 days ago	Edit Delete Add users

step1)

Add user

- 1
- 2
- 3
- 4
- 5

Set user details

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

User name*

[+ 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.

Step 2)

Add user

- 1
- 2
- 3
- 4
- 5

▼ Set permissions

 [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
<input type="text" value="Search"/>		
Group	Attached policies	
<input checked="" type="checkbox"/> manage-airsoft-workshop	airsoft-workshop-policy	
<input type="checkbox"/> manage-gwils-boutique-ado	gwils-boutique-ado-policy	

► Set permissions boundary

Step 3) skip

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
Add new key		

You can add 50 more tags.

Step 4) 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	airsoft-workshop-staticfiles-user
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

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

Type	Name
Group	manage-airsoft-workshop

Tags

No tags were added.

Step 5) Download the .csv and save it as you cant get this later

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://761603658625.signin.aws.amazon.com/console>

[Download .csv](#)

	User	Access key ID	Secret access key
▶	airsoft-workshop-staticfiles-user	AKIA3CUY5SOAYG2HHAER	***** Show

AKIA3CUY5SOAYG2HHAER ***** Show