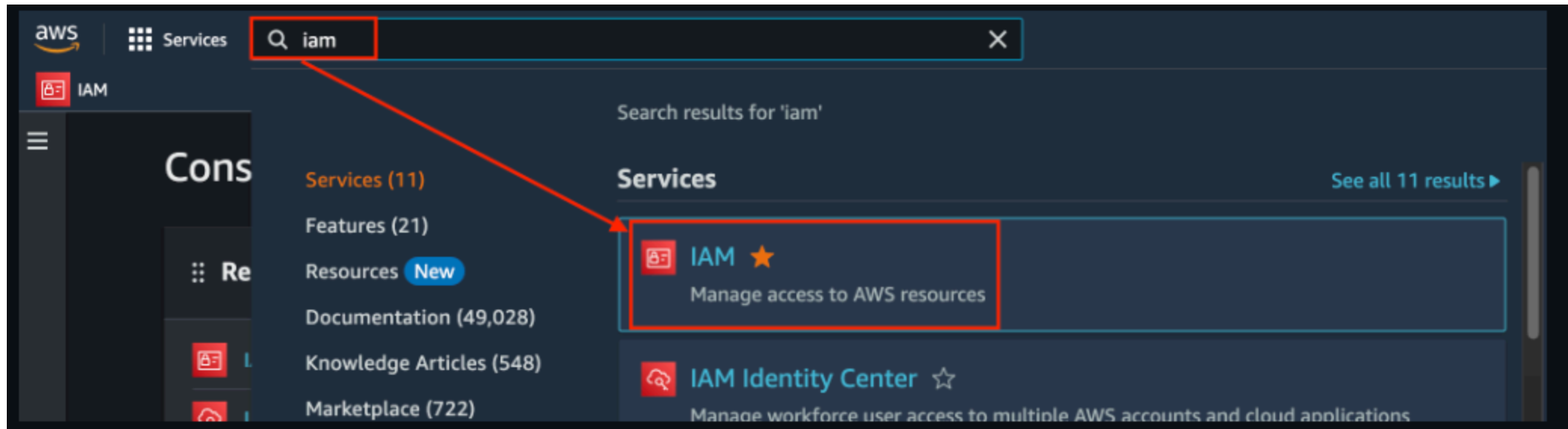


# AWS Admin 계정 만들기

- AWS에 처음 가입한 이메일로 로그인하면 **루트 사용자**입니다.
- **루트 사용자**는 AWS의 요금/정산 등 중요한 리소스에 접근이 가능한 계정이다.

따라서 AWS에서 제공하는 리소스를 사용(개발)하는 경우에는 IAM 사용자를 만들어서 계정별 권한을 부여하여 사용해야 한다.

## 단계1: IAM 접속



## 단계2: User groups 생성

The screenshot shows the AWS IAM console interface. On the left sidebar, under 'Access management', the 'User groups' link is highlighted with a red box. A red arrow points from this link to the 'Create group' button in the top right corner of the 'User groups' main content area. The main content area shows a table with one user group, 'Administrators', which was created 14 days ago and has 'Defined' permissions.

**Identity and Access Management (IAM)**

Search IAM

Dashboard

▼ Access management

- User groups
- Users
- Roles

**User groups (1)** Info

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

Search

< 1 > ⚙

<input type="checkbox"/>	Group name ▲	Users ▼	Permissions ▼	Creation time ▼
<input type="checkbox"/>	<a href="#">Administrators</a>	1	Defined	14 days ago

- User groups 설정

User group name

Enter a meaningful name to identify this group.

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

Add users to the group - Optional (1) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Q Search

< 1 >

<input type="checkbox"/>	User name <a href="#">↗</a>	▲ Groups	Last activity ▼	Creation time ▼
<input type="checkbox"/>	<a href="#">admin</a>	1	6 days ago	14 days ago

- Policies 정의

**Attach permissions policies - Optional (1/906)** [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

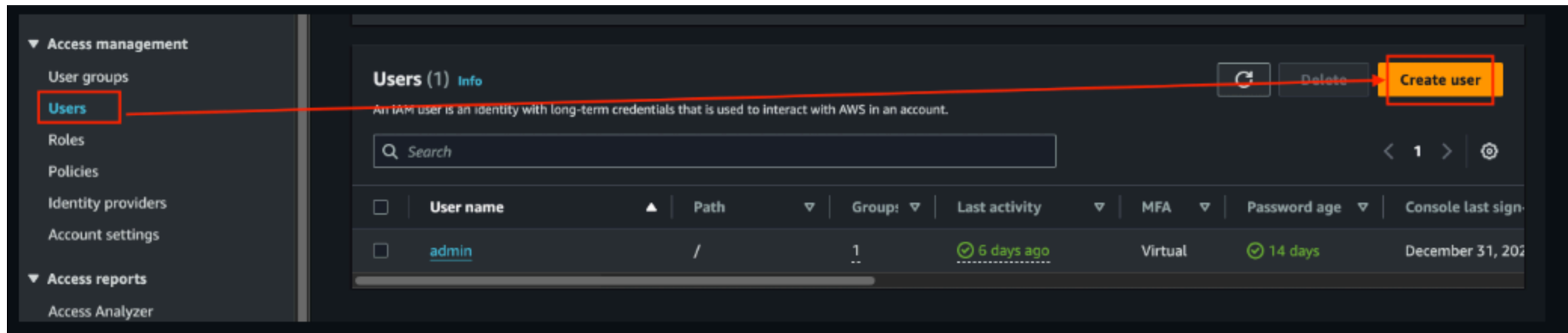
Filter by Type

Search:  4 matches

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy (2)	Provides full access to AWS services an...
<input type="checkbox"/>	<a href="#">AdministratorAccess-Am...</a>	AWS managed	None	Grants account administrative permis...
<input type="checkbox"/>	<a href="#">AdministratorAccess-AW...</a>	AWS managed	None	Grants account administrative permis...
<input type="checkbox"/>	<a href="#">AWSAuditManagerAdmi...</a>	AWS managed	None	Provides administrative access to enab...

[Cancel](#) [Create group](#)

## 단계3: Users 생성



- Specify user details

User name

manager

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ \_ - (hyphen)

☒ Provide user access to the AWS Management Console - *optional*  
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

**Are you providing console access to a person?**

User type

☐ Specify a user in Identity Center - Recommended  
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user  
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☒ Autogenerated password  
You can view the password after you create the user.

☐ Custom password  
Enter a custom password for the user.

☐ Show password

☒ Users must create a new password at next sign-in - Recommended  
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

**If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)**

Cancel Next

- Set permissions

## Set permissions

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](#)

### Permissions options

☒ **Add user to group**  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ **Copy permissions**  
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ **Attach policies directly**  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

### User groups (1/1)

☒

[Group name](#)

☐

[Administrators](#)

▲

Users

▼

☒

[Attached policies](#)

☐

[AdministratorAccess](#)

▼

Created

▼

2023-12-22 (14 days ago)

Cancel

Previous

Next




- Review and create

### User details

User name manager	Console password type Autogenerated	Require password reset Yes
----------------------	--	-------------------------------

### Permissions summary

< 1 >

Name 	Type	Used as
<a href="#">Administrators</a>	Group	Permissions group
<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.

Cancel

Previous

Create user

- Retrieve password

Console sign-in details

Email sign-in instructions

Console sign-in URL

https://426653742146.signin.aws.amazon.com/console

User name

manager

Console password

\*\*\*\*\* Show

Cancel

Download .csv file

Return to users list

manager\_credentials

User name	Password	Console sign-in URL
manager	mNhA4&3A	https://426653742146.signin.aws.amazon.com/console

## 단계4: 콘솔 로그인

### IAM 사용자로 로그인

계정 ID(12자리) 또는 계정 별칭

426653742146

사용자 이름:

manager

암호:

.....

☐ 이 계정 기억하기

로그인



- 새 비밀번호 생성

**AWS 계정** 426653742146

**IAM 사용자 이름** manager

이전 비밀번호

새 비밀번호

새 비밀번호 재입력

비밀번호 변경 확인

루트 사용자 이메일을 사용하여 로그인

## 단계5: 사용 가능한 MFA 앱 설치

운영 체제	테스트를 거친 인증 앱
Android	<a href="#">Authy</a> , <a href="#">Duo Mobile</a> , <a href="#">Microsoft Authenticator</a> , <a href="#">Google Authenticator</a>
iOS	<a href="#">Authy</a> , <a href="#">Duo Mobile</a> , <a href="#">Microsoft Authenticator</a> , <a href="#">Google Authenticator</a>

## 단계6: MFA devices 설정

The screenshot shows the AWS IAM console interface. In the left sidebar, the 'Identity and Access Management (IAM)' menu is highlighted. Below it, the 'Users' link is also highlighted. The main content area shows the 'Users (1/2)' page. A table lists the users, with the 'manager' user row highlighted. The 'manager' user has a checkmark in the 'MFA' column, indicating MFA is enabled. The 'Last activity' column shows '3 minutes ago' and the 'Password age' column shows '1 minute'.

	User name	Path	Group	Last activity	MFA	Password age	Console last used
<input type="checkbox"/>	<a href="#">admin</a>	/	1	6 days ago	Virtual	14 days	December
<input checked="" type="checkbox"/>	<a href="#">manager</a>	/	1	3 minutes ago	-	1 minute	January 06

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

Console sign-in

Manage console access

Console sign-in link

https://426653742146.signin.aws.amazon.com/console

Console password

Updated 3 minutes ago (2024-01-06 16:15 GMT+9)

Last console sign-in

6 minutes ago (2024-01-06 16:13 GMT+9)

Multi-factor authentication (MFA) (0)

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
No MFA devices. Assign an MFA device to improve the security of your AWS environment			
Assign MFA device			

### Device name

Enter a meaningful name to identify this device.

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

### MFA device

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.



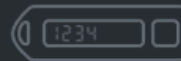
#### Authenticator app

Authenticate using a code generated by an app installed on your mobile device or computer.



#### Security Key

Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.



#### Hardware TOTP token

Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

Cancel

Next



- MFA 앱 적용


Step 1  
[Select MFA device](#)

Step 2  
**Set up device**

### Set up device Info

#### Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.  
[See a list of compatible applications](#)
- 2  Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code.  
Alternatively, you can type a secret key. [Show secret key](#)
- 3 Fill in two consecutive codes from your MFA device.  
MFA code 1  
  
MFA code 2

[Cancel](#) [Previous](#) [Add MFA](#)