Introduction to IAM

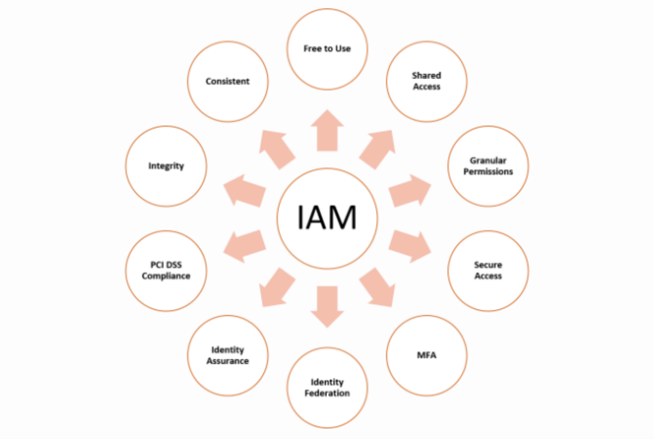
What is IAM?

AWS IAM stands for Identity & Access Management and is the primary service that handles authentication and authorization processes within AWS environments. As an AWS account management service, it lets you control access to AWS services in a secure manner and helps to monitor who is authenticated and allowed to use resources.

- By using AWS console, you can manage users and their access level.
- All account settings are made through this service.
- It allows us to create and manage objects such as User, Group, Role, and Policy.
- Account owner can identify and allow the user to use specified services.
- All kinds of user password restrictions and multifactor authentication settings are also made through IAM.

So, in general, it can also be considered as the guard of the AWS.

IAM Features



AWS Features

- **Free to use:**

AWS IAM is an AWS account feature which is offered at no extra charge. By using IAM, you will only be paid when you use other AWS services.

- **Shared access to your AWS account:**

Users can share the resources for collaborative projects among themselves. You can also allow other users in your AWS account to manage and use services without having to share your password or access key.

- **Granular permissions:**

Different people can be granted permissions for different resources. So, it also means setting the authorization for the user to use a specific service but not others.

- **Secure access to AWS resources for applications that run on Amazon EC2:**

The IAM features can be used to provide secure credentials to applications running on EC2 instances.

- **Multi-factor authentication (MFA):**

AWS offers multifactor authentication to sign in to the AWS Management Console. Users not only need to provide a password or access key to work with your account, but also a code from a device that has been configured specifically.

- **Identity federation:**

You can allow users who already have passwords elsewhere - such as Twitter, Facebook, Linkedin - to access your AWS account temporarily. Users can log in to the AWS Console with the same username and password as they log in to Facebook, Twitter, etc.

- **Identity information for assurance:**

You receive log records that contain information about those who have made resource requests based on IAM identities.

- **PCI DSS Compliance:**

IAM supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS).

- **Integrated with many AWS services:**

IAM is integrated with many different AWS services.

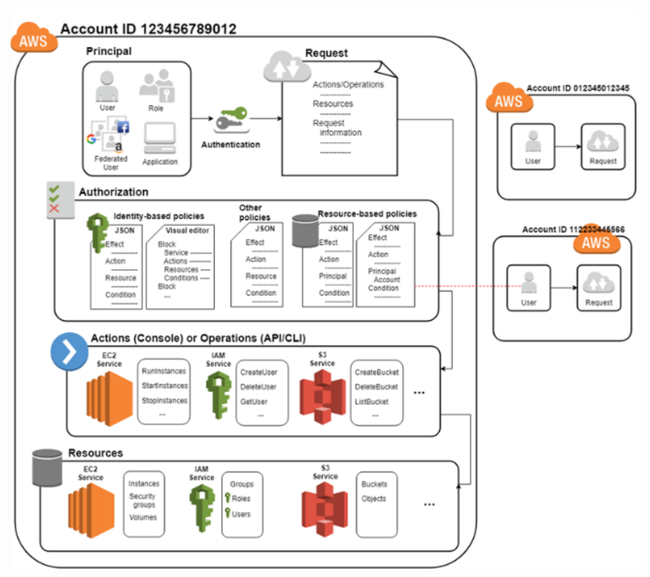
- **Eventually Consistent:**

Basically, IAM service is fairly consistent because it achieves high availability by replicating the data through multiple servers in the Amazon data center around the world.

For a more detailed explanation, you can follow this link.

IAM Workflow & Components

The general operating logic and systematic of IAM have been designed by AWS as follows.



IAM Workflow

The IAM infrastructure includes the following elements which provide the necessary infrastructure for managing the account authentication and authorization. Now we will take a look at these components one by one and in the end, we will try to grasp the general logic of IAM.

- **Principal:**

In AWS architecture, the principal is a person or application that can request an action or operation for an AWS resource. To make requests to AWS, it is authenticated as the root user of the AWS account or an IAM entity. Principals might be a user, role, federated user, or an application.

If you match it with yourself in your daily life, you can think of yourself, for example, as a user on the Clarusway website. When you use the website via the browser, you are now a principal within the website.

- **Authentication:**

To make a request to AWS, principals must be authenticated (signed in to AWS) using their credentials. A principal can be authenticated for AWS both from the console and the API or AWS CLI. For console authentication, you have to sign in with your email address and password. For API/AWS CLI authentication, you have to provide your access key and secret key.

You can think of it as entering the site using your username, e-mail address and password similarly in the example of the Clarusway website. By presenting the necessary information as a principal, you now log in to the site and take the first step to use the services offered on the site. Now, you are an authenticated user.

- **Request:**

When a principal attempts to use the AWS Management Console/API/CLI, that principal will send a request to AWS. The request can be actions or operations such as using any service, resource, or role.

Similarly, when you want to use the courses, resources, activities available on the Clarusway website, you can think of these things as requests.

- **Authorization:**

You must also have the authorization (allowance) to complete the request during the authorization process, AWS can check for relevant policies using values from the context of the request. It then makes use of the policies to decide whether the application should be allowed or denied.

For example, you want to follow a course within the Clarusway organization. When you request for this, if you provide the necessary conditions according to the rules or policies within the organization, you are authorized for that request.

- **Actions or Operations:**

After authentication and authorization of your request get done, AWS approves the actions or operations in your request. A service describes operations that include things you can do to a resource, such as accessing, creating, modifying, and removing the resource.

You can consider this as a transaction that you can apply after completing the authorization process. For example, your usage preferences, such as changes you can make to the services offered by Clarusway.

- **Resources:**

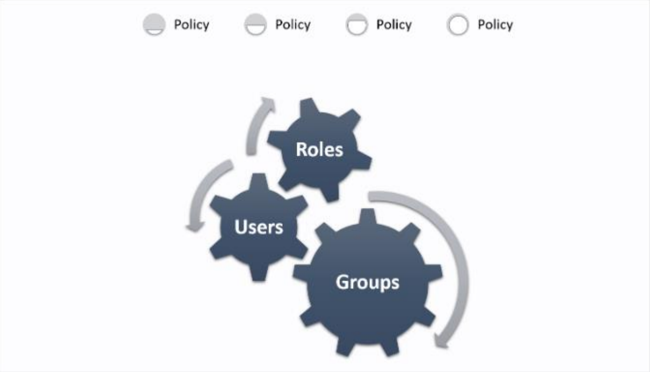
Once the operations in your request are accepted by AWS, they can be carried out on the relevant resources within your account. A resource is any object that exists within an AWS service.

Considering the example of Clarusway, you can access the resources available to you after your request has been approved. You can also think of the resources as different teaching materials with different titles offered to you by Clarusway.

This is how we can summarize the AWS IAM workflow in general. As we can see in the diagram above, there are many details regarding the application of this workflow. We will examine these details separately in future lessons as the time comes.

Categorizing IAM Components

IAM components can be mainly categorized under two terms; identities and permissions.



Identities & Permissions

IAM identities are created to give people and processes authentication in an AWS account. There are three identities in AWS IAM:

- Users
- Groups
- Roles

Permissions can be defined as different types of policies that use authorization to users.

- Policies

Security Credentials

While interacting with the AWS as any kind of user, you can have different kinds of security credentials that depend on how you communicate with the AWS. For example; you can use an email and password when logging in to the AWS console as a root user, whereas when logging in as an IAM user, you use a username and password. These combinations are called Security credentials in AWS.

Here are the security credentials you will commonly use when interacting with the AWS resources :

Root User
E-mail & Password
AWS
Management
Console

E-mail address and password is used when connecting to the AWS Management Console with the root account.

IAM Users
Username & Password
AWS
Management
Console

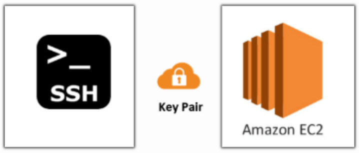
IAM username and password is used for accessing the AWS Management Console as an IAM user.

Root & IAM Users
MFA
AWS
Management
Console

Multifactor authentication (MFA) is an additional layer of security that can be used with both the root account and IAM user as well.

CLI
SDK
APIs
Access Keys
AWS

Access keys are used with the CLI, APIs, and SDKs.



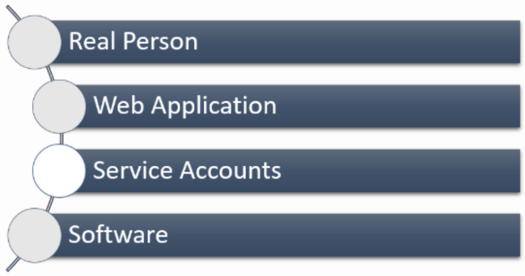
Key pair is used with Amazon EC2 for logging in to the servers/instances.

How AWS Identifies an IAM user?

An IAM user is an entity that you create in AWS.

- The IAM user represents the person or service who uses AWS services.
- A primary use for IAM users is to give people the ability to sign in to the AWS Management Console for interactive tasks and to make programmatic requests to AWS services using the API or CLI.
- A user in AWS consists of a name, a password to sign in to the AWS Management Console, and up to two access keys that can be used with the API or CLI.
- When you create an IAM user, you grant it permissions by making it a member of a group that has appropriate permission policies attached (recommended), or by directly attaching policies to the user.
- You can also clone the permissions of an existing IAM user, which automatically makes the new user a member of the same groups and attaches all the same policies.

IAM User Types



IAM User Types

An IAM user is an identity that has an associated credential and the permissions attached. This could be a real person who is a user or a web application, service account, auditing or back-up software. Firstly, we will focus on users who are real persons.

We created an AWS Free Tier account at the end of the previous section. This account is defined as a root user in the AWS world. Now let's continue to get to know the features of the IAM service, starting with the root user.

Account Root User

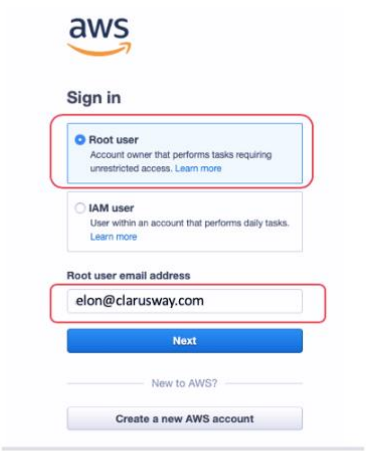
By first creating an AWS account, you create **a root user identity account** that is used to log in to the AWS. This identity is called the **AWS Account Root *User*.**

- **AWS account owner** is also an AWS account root user.
- An account root user has **complete access to all AWS services**.
- This **access authorization can not be restricted** in any way.
- The account owner can sign in to the AWS console as a root user by using the email address and password that was defined when creating the account. These are also known as **root user credentials**. MFA code can also be used as an optional but recommended feature.
- A root user can create new IAM users and give them authorization for using AWS services within the account. The limit of creating new IAM users is restricted to 5000 users per account.

> **Tip:**
> - Using account root user in daily work is not recommended by AWS.
> - Instead, it is recommended to create an IAM user with administrative privileges by the account owner.
> - Therefore, using the root user only to create new users is considered as best practice.

Root User Sign-in

- Let's connect to the AWS console by using this link.



Sign in

● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

○ IAM user
User within an account that performs daily tasks. Learn more

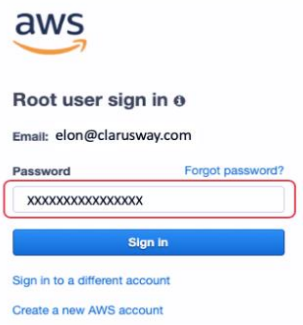
Root user email address
elon@clarusway.com

Next

New to AWS?

Create a new AWS account

- First, choose the **Root User** tab. Then, type the **email** you defined when creating your AWS account, and then press the **Next** button.



Root user sign in

Email: elon@clarusway.com

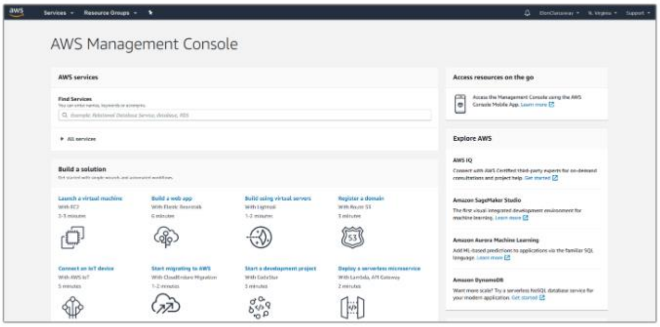
Password — Forgot password?
XXXXXXXXXXXXXXXX

Sign in

Sign in to a different account

Create a new AWS account

- Type **password** you defined when creating your AWS account, and then press the **Next** button.
- If you have activated MFA before, it will ask for MFA code at this stage, if not, the AWS console home page will open as below.



Services ▾ Resource Groups ▾ ElonClarusway ▾ N. Virginia ▾ Support ▾

AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.
Example: Relational Database Service, database, RDS

▸ All services

Build a solution
Get started with simple wizards and automated workflows.

Launch a virtual machine
With EC2
2-3 minutes

Build a web app
With Elastic Beanstalk
6 minutes

Build using virtual servers
With Lightsail
1-2 minutes

Register a domain
With Route 53
3 minutes

Connect an IoT device
With AWS IoT
5 minutes

Start migrating to AWS
With CloudEndure Migration
1-2 minutes

Start a development project
With CodeStar
5 minutes

Deploy a serverless microservice
With Lambda, API Gateway
2 minutes

Access resources on the go
Access the Management Console using the AWS Console Mobile App. Learn more

Explore AWS

AWS IQ
Connect with AWS Certified third-party experts for on-demand consultations and project help. Get started

Amazon SageMaker Studio
The first visual integrated development environment for machine learning. Learn more

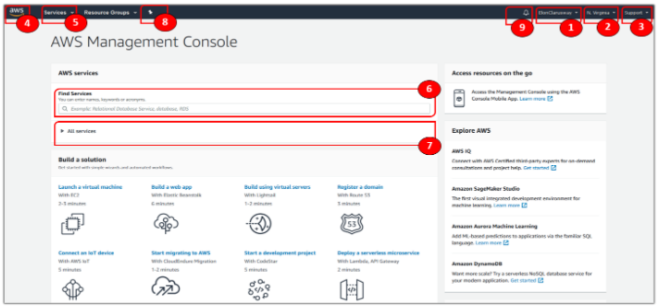
Amazon Aurora Machine Learning
Add ML-based predictions to applications via the familiar SQL language. Learn more

Amazon DynamoDB
Want more scale? Try a serverless NoSQL database service for your modern application. Get started

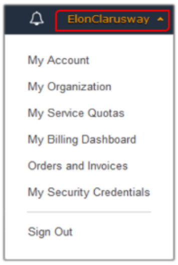
- Welcome to the AWS world.

AWS Home Page Console Tour

AWS Management Console is a web application for AWS management that offers users a built-in user interface for AWS tasks. Now, let's go on a quick tour of the homepage and know some important features of the console menu.



1. User Account Menu:

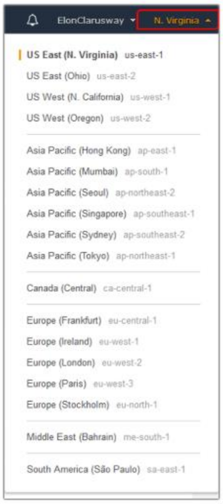


ElonClarusway ▴

My Account
My Organization
My Service Quotas
My Billing Dashboard
Orders and Invoices
My Security Credentials
Sign Out

This menu allows you to manage all your user transactions and has been named as your user name. You can access and manage many processes such as account details, organization, billing and passwords through this menu.

2. Region:



ElonClarusway ▾ N. Virginia ▴

US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2

Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Mumbai) ap-south-1
Asia Pacific (Seoul) ap-northeast-2
Asia Pacific (Singapore) ap-southeast-1
Asia Pacific (Sydney) ap-southeast-2
Asia Pacific (Tokyo) ap-northeast-1

Canada (Central) ca-central-1

Europe (Frankfurt) eu-central-1
Europe (Ireland) eu-west-1
Europe (London) eu-west-2
Europe (Paris) eu-west-3
Europe (Stockholm) eu-north-1

Middle East (Bahrain) me-south-1

South America (São Paulo) sa-east-1

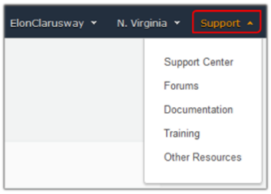
This menu shows the AWS region under operation and we can change, select and switch the region by using region list through this menu.

- After May 17, 2017, the default region when you access a resource from the AWS Management Console is **US East (Ohio) (us-east-2).**
- In AWS, not every region supports every service and other features of these services. You can reach which regions support which services from AWS Region Table.

⚠ **Caution! :**

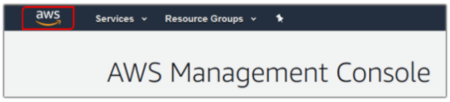
- Some services such as S3 and IAM are not region-based and are therefore exhibited globally.

3. Support Menu:



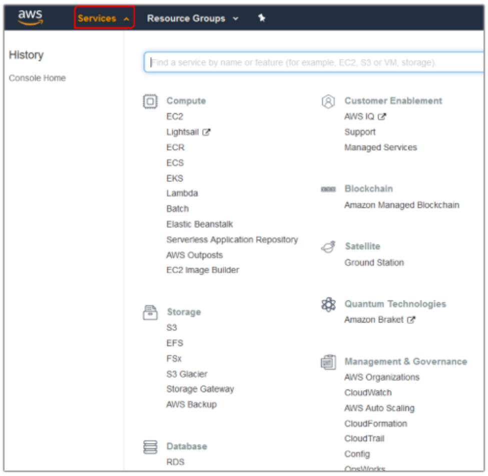
This is the menu where you can access support services of AWS such as technical, documentation, forums.

4. Home Page - Tab:



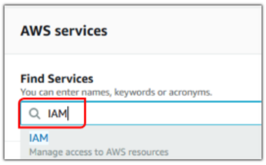
When we log into our AWS account using user credentials, the page that opens is the home page. Whenever we want to return to this home page, we can click on this tab with AWS in the upper left corner of the management console.

5. Services - Tab:



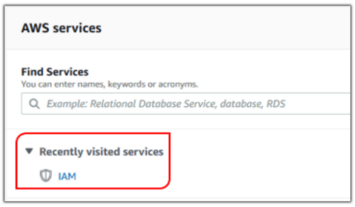
When we click the Services tab, all services offered by AWS are displayed on the management console.

6. Find Services - Search Bar:


AWS services
Find Services
You can enter names, keywords or acronyms.
IAM
IAM
Manage access to AWS resources

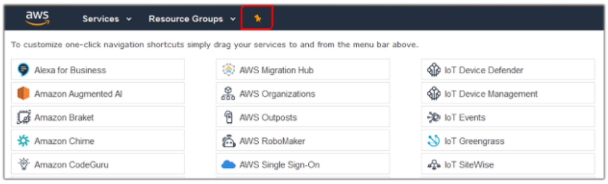
In addition to the services tab, when we want to access a service via the management console, AWS also provides us with a search bar where we can call

7. Recently Visited Services:


AWS services
Find Services
You can enter names, keywords or acronyms.
Example: Relational Database Service, database, RDS
Recently visited services
IAM

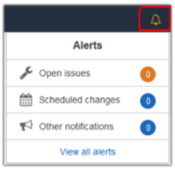
After visiting any service in the management console, this tab stores it as a recently visited service. In this way, an additional opportunity is provided by AWS to switch between services while on the home page and to reach the services you use last.

8. Pin - Menu:



With this tab, you can pin the services you use most frequently to the menu bar. In this way, you will have the opportunity to access the services, you frequently switch to, faster via the menu bar. But this is a browser-based option. When you log into your account from different browsers, if you don't pin frequently used services again, you won't be able to see them in the menu bar.

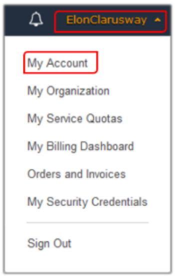
9. Notifications:



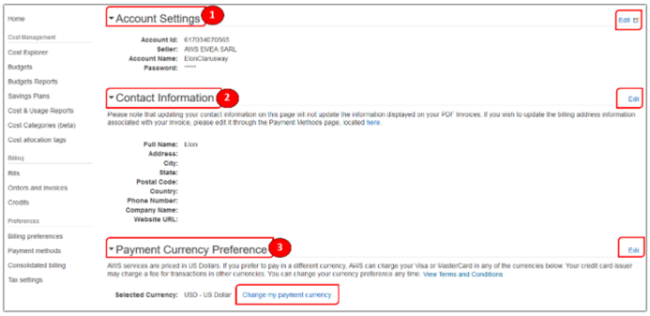
It is the tab that shows all warnings and alarms to the user such as open issues and changes. You can also view all the event logs via **"View all alerts"** option.

Account Information

Now let's take a look at some of our account introductory information.



After you select the **My Account** tab from the **User Menu**, the following page containing your account information will open.



Account Settings 1

Account Id: 617034070565
Seller: AWS EMEA SARL
Account Name: ElonClarusway
Password: *****

Contact Information 2

Please note that updating your contact information on this page will not update the information displayed on your PDF invoices. If you wish to update the billing address information associated with your invoice, please edit it through the Payment Methods page, located here.

Full Name: Elon
Address:
City:
State:
Postal Code:
Country:
Phone Number:
Company Name:
Website URL:

Payment Currency Preference 3

AWS services are priced in US Dollars. If you prefer to pay in a different currency, AWS can charge your Visa or MasterCard in any of the currencies below. Your credit card issuer may charge a fee for transactions in other currencies. You can change your currency preference any time. View Terms and Conditions

Selected Currency: USD - US Dollar

1. Account Settings:

- **Account Name** and **Account ID** information are available in the Account Settings section.
- You can view and rearrange your "**name, email and password**" at any time by clicking the Edit tab on the right.
- **Account ID** is a unique 12-digit number like 123456789000 and can not be changed. It's automatically created by AWS when you had created your account. Account ID helps to distinguish your resources from other AWS accounts resources.

2. Contact Information:

- In the Contact Information section, your personal information such as **name, address, phone number, website,** and **company name** are included.
- You can also update your information in this section at any time by using the **Edit** tab.
- The point to be noted here is that; when you update your contact information, the information displayed on your PDF invoices will not be updated automatically. You should also edit it through the **Payment Methods** page.

3. Payment Currency Preference:

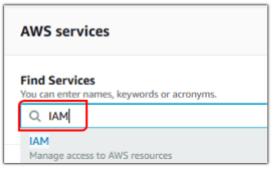
- AWS services are priced in **US Dollars**.
- If you prefer to pay in a different currency, AWS can charge your Visa or MasterCard in any of the currencies.
- You can change your currency preference at any time via **Change my payment currency** tab.

There are also some other options as listed below that you can view and change/arrange at any time.

- Alternate ContactsGovCloud (US)
- Configure Security Challenge Questions
- AWS Regions
- IAM User and Role Access to Billing Information
- Reserved Instance Marketplace Settings
- Account Contract Information
- Communication Preferences
- Manage AWS Support Plans

IAM Dashboard

Now let's take a look at IAM Dashboard and get some important concepts about it. To see the IAM Dashboard, type **IAM** in **Find Services** search bar as below and then click **IAM**.



AWS services

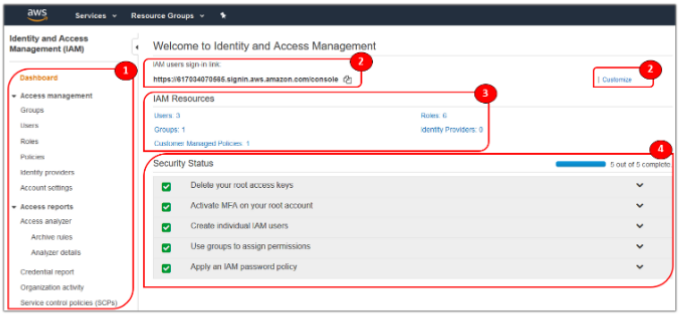
Find Services

You can enter names, keywords or acronyms.

IAM

IAM
Manage access to AWS resources

The IAM dashboard page will be opened then.



Welcome to Identity and Access Management

IAM users sign-in link:
https://617034070565.signin.aws.amazon.com/console

IAM Resources

Users: 3
Roles: 6
Groups: 1
Identity Providers: 0
Customer Managed Policies: 1

Security Status — 5 out of 5 complete

- ☑ Delete your root access keys
- ☑ Activate MFA on your root account
- ☑ Create individual IAM users
- ☑ Use groups to assign permissions
- ☑ Apply an IAM password policy

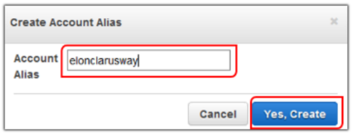
1. Dashboard Menu:

There are relevant menu tabs under **Access Management** and **Access Reports** subjects of this menu. We will see the usage of these menus as we use them throughout the course.

2. IAM User Sign-in Link:

- Sign-in Link is **the URL for your sign-in page** and contains your account ID by default.

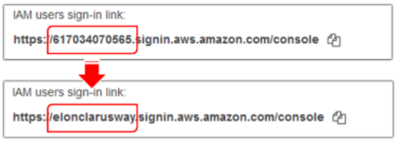
- You can customize this URL with anything such as your name, company name, etc. by clicking the Customize link at any time.
- To change the account ID part of the sign-in link to anything you desire is called creating an alias.
- Let's create an alias by selecting the customize link and typing a preferred alias.



Create Account Alias

Account Alias: elonclarusway

- After clicking **Yes, Create** tab, your new alias for the sign-in link will be created like below.



IAM users sign-in link:
https://617034070565.signin.aws.amazon.com/console

IAM users sign-in link:
https://elonclarusway.signin.aws.amazon.com/console

3. IAM Resources:

- This section shows the IAM resources such as **users, groups, roles, etc**. which were created earlier.
- Because there were no IAM resources when you first created the account, all the numbers in this section would be zero at the beginning.

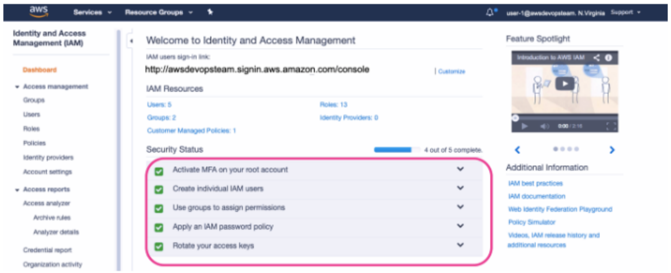
4. Security Status:

AWS offers a **5-step security system** arrangement and suggests to complete these 5 processes and secure the account.

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy

Since all these 5 step security status transactions are completed in the account in the picture above, they all appear as done.

Security Status



Welcome to Identity and Access Management

IAM users sign-in link:
http://awsdevopsteam.signin.aws.amazon.com/console

IAM Resources

Users: 5
Roles: 13
Groups: 2
Identity Providers: 0
Customer Managed Policies: 1

Security Status — 4 out of 5 complete.

- ☑ Activate MFA on your root account
- ☑ Create individual IAM users
- ☑ Use groups to assign permissions
- ☑ Apply an IAM password policy
- ☑ Rotate your access keys

Security Status:

- **Step-1 Activate MFA on your root account:**

AWS highly recommends activating MFA (Multi-Factor Authentication) in the root account. When signing in as a user without activating MFA, users used to enter only their user name and password, which is the only factor. MFA, if activated, is an obligation to enter a code that is produced by another device. So, this is an extra security layer in addition to the user name and password. Even if some people learn our password, they will not be able to sign in our account because they don't know the MFA code.

- **Step-2 Create individual IAM users:**

We have already mentioned that AWS does **not recommend using the root account** for daily operations. This security step also means that you do not use the root account, define yourself new users and do your operations with those users.

- **Step-3 Use groups to assign permissions**

Groups are particularly useful resources when creating new users. We can create a group and authorize the users through these groups. For example;

- If we have 1-2 users, this may not be very important.
- However, if you think of an AWS account with 100 users, you can create the privileges of all users belonging to the groups only by editing the group members and then change it with a single operation for the whole group.

- **Step-4 Apply an IAM password policy:**

Password policy is a way that we **determine how users create their passwords**. For example;

- Have to set a new password in a while, like 90 days, etc.
- When changing password, do not use the last 5 passwords
- Create a password with at least 8 characters

To create a password policy, we can click the **Apply an IAM password policy** tab or we can reach the same policy setting page by clicking the **Account settings** tab in the menus on the left.

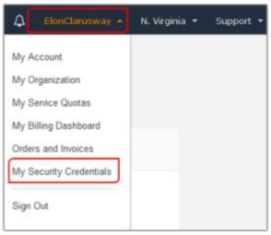
- **Step-5 Rotate your access keys:**

AWS recommends you to change your access keys regularly (at least once per year) and delete unused access keys to reduce your risk in case of accidental exposure.

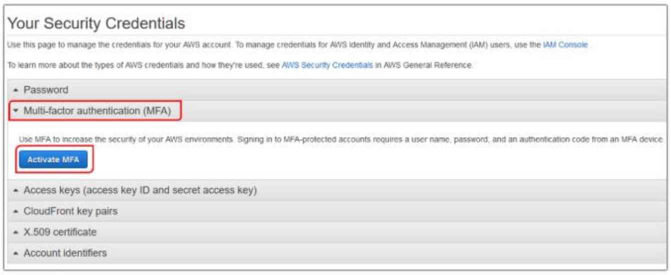
Root User MFA Activation

Let's get started with AWS multi-factor authentication.

- Sign in to the AWS Management Console.
- Select the user menu by clicking **your account name** on the right side of the navigation, and choose **My Security Credentials**.



- Extend the Multi-Factor Authentication (MFA) page section.
- Select **Activate MFA**.



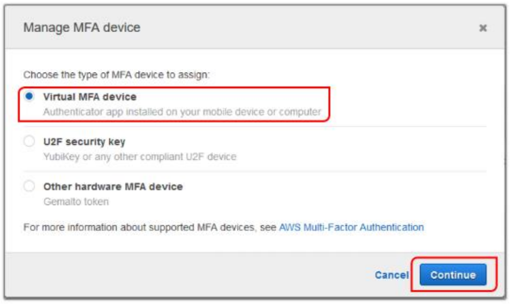
Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console .

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

- Select **Virtual MFA device**, and then choose **Continue**.



Manage MFA device

Choose the type of MFA device to assign:

● **Virtual MFA device**
Authenticator app installed on your mobile device or computer

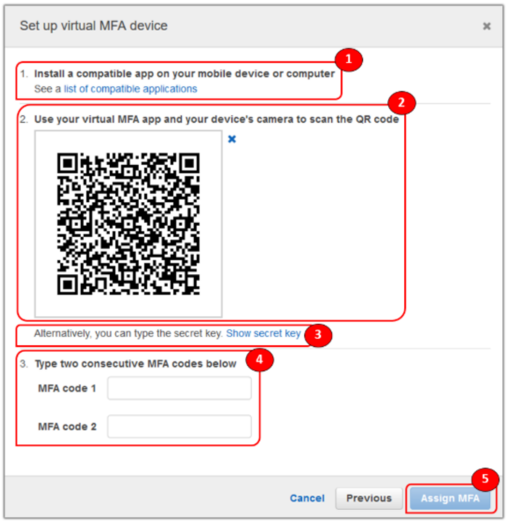
○ **U2F security key**
YubiKey or any other compliant U2F device

○ **Other hardware MFA device**
Gemalto token

For more information about supported MFA devices, see AWS Multi-Factor Authentication

- IAM produces and displays virtual MFA system configuration information including a QR code graphic.

- IAM produces and displays virtual MFA system configuration information including a QR code graphic.



Set up virtual MFA device

1. Install a compatible app on your mobile device or computer
See a list of compatible applications

2. Use your virtual MFA app and your device's camera to scan the QR code

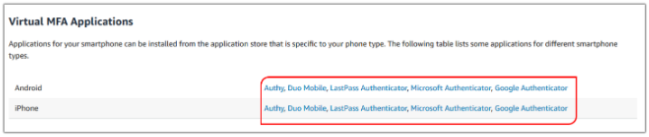
Alternatively, you can type the secret key. Show secret key

3. Type two consecutive MFA codes below

MFA code 1

MFA code 2

- **Firstly**, you should install a compatible app on your mobile device or computer. You can look at different available applications by clicking **a list of compatible applications** link.

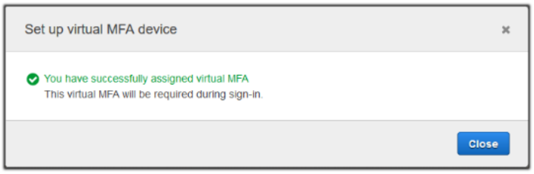


Virtual MFA Applications

Applications for your smartphone can be installed from the application store that is specific to your phone type. The following table lists some applications for different smartphone types.

Android	Authy, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator
iPhone	Authy, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator

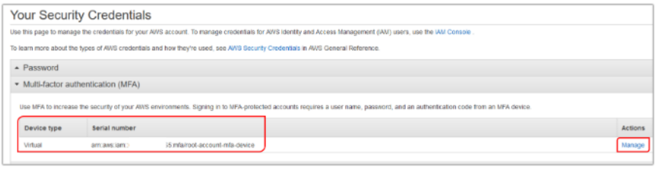
- You can select which application you want. For the demo purpose, let's choose Authy and install it on our mobile device.
- **Secondly**, use your virtual MFA app which is Authy in this case and your device's camera to scan the QR code.
- **Thirdly**, if you do not have a QR scanning application on your mobile device, you can alternatively learn secret key clicking **Show secret key** link and then type it into Authy application on your mobile device.
- **Fourthly**, get 2 consecutive MFA codes from the application and type them in **MFA code 1** and **MFA code 2** sections.
- **Finally**, click the **Assign MFA** button.



Set up virtual MFA device

You have successfully assigned virtual MFA
This virtual MFA will be required during sign-in.

- Congrats! You have successfully assigned virtual MFA to your account. AWS will require an MFA code for the next sign-in to your account.



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console .

To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

Device type	Serial number	Actions
Virtual	arn:aws:iam: [redacted] 5:mfa/root-account-mfa-device	Manage

- You can manage MFA at any time, **Remove** or **Resync** it via **Manage** link on the right.

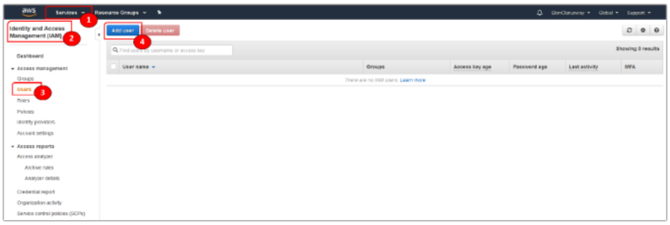
Creating IAM User

We have already mentioned that AWS does not recommend us to use the root user account. Instead, it is recommended that account owners create an IAM user that complies with administrative authority and do daily work with this user.

In addition, you may need to create other users connected to your AWS account or you may need to create an IAM user for staff working at the Company.

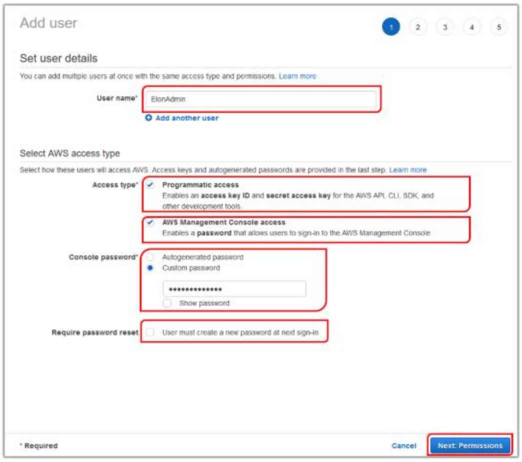
Now we will create an IAM user with Administrative authority for using instead of the root user.

- Sign in to the AWS Management Console.
- Open the **IAM** page using the **Services** tab from the menu bar.
- Click the **Users** link from the menu on the left.
- If you have not created a user before, the page will return empty as below.



- Let's create our first user by clicking the "Add User" tab at the top of the page. Creating a new IAM user will be performed in 5 steps.

Creating IAM User - Set User Details



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* ElonAdmin

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* ☑ **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 ************** □ Show password

Require password reset □ User must create a new password at next sign-in

* Required

- **User name:**

  Since we created this first account for ourselves, let's choose a username for ourselves. I chose ElonAdmin as the user name, you can also choose any name you want. However, it is useful that the user name you set is descriptive. This benefit can be neglected when the number of users in your account is low, but it will make your job easier when there are too many users.

- **Access Type:**

  AWS offers us 2 options as "Access Type" for the user. Programmatic access, AWS Management Console access. Here, we determine how the user we created can access AWS resources.

If AWS Management Console access is selected, the user can log in to AWS via the web browser and perform their operations through the AWS console. To access the console, the user needs a "username and password".

Additionally, if we also select Programmatic access, this user can also access AWS resources outside the console via the AWS API with the command line and the applications via the AWS SDK. In order to access AWS resources, the user must have additional information called Access Key and Secret Access Key.

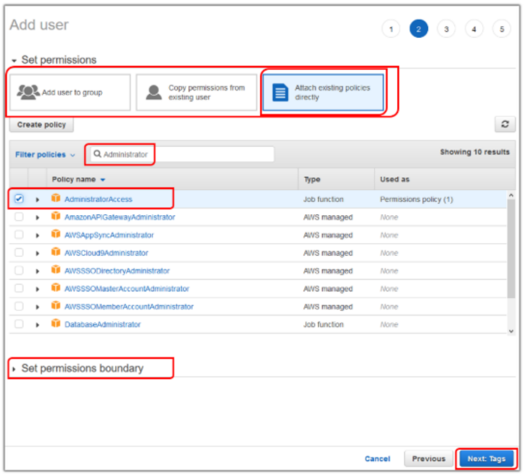
- **Console password:**

  AWS offers 2 different password determination preferences as **autogenerated** or **custom** for the user's password. Let's choose the custom option and create our password.

- **Require password reset:**

  As the last operation in Step-1, we determine whether the user should change his password when he first signs in. Then we go to the Permissions page by pressing the Next tab.

Creating IAM User - Set Permissions



Add user

Set permissions

Filter policies: Administrator — Showing 10 results

	Policy name	Type	Used as
☑	AdministratorAccess	Job function	Permissions policy (1)
□	AmazonAPIGatewayAdministrator	AWS managed	None
□	AWSAppSyncAdministrator	AWS managed	None
□	AWSCloud9Administrator	AWS managed	None
□	AWSSSODirectoryAdministrator	AWS managed	None
□	AWSSSOMasterAccountAdministrator	AWS managed	None
□	AWSSSOMemberAccountAdministrator	AWS managed	None
□	DatabaseAdministrator	Job function	None

Set permissions boundary

1
2
3
4
5
Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy
Cancel
Previous
Next: Tags

AWS gives us 3 options for authorization of the IAM user (Set Permission Options).

Add user to the group:

- By creating a group, policies are assigned to this group.
- When the user is a member of this group, they automatically have the privileges in the policy assigned to the group.
- So that they are authorized through the group.

Copy permissions from an existing user:

- We transfer the privileges of another user.
- A user should already be available to use this option.

Attach existing policies directly:

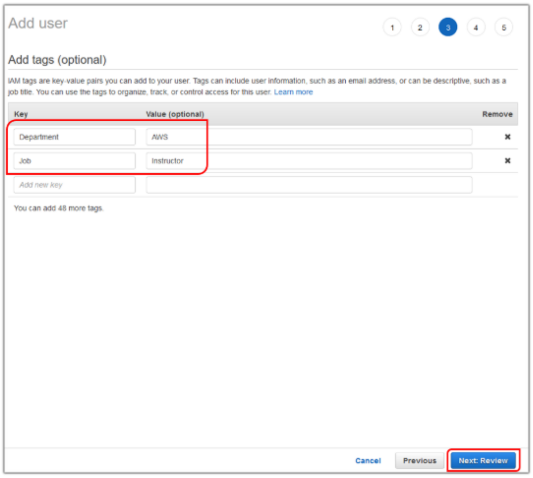
- We assign one of the policies available in AWS to the user we create.
- Policies are JSON files that determine how users can access and use AWS resources. We will look at the policy concept in more detail in the following lessons. For now, you only need to know that the policies as JSON files used to authorize users to AWS resources.

We can also create our own custom policy by clicking the **Create policy** tab as the fourth option.

Since no other users or groups have been created in the account yet, we will continue by selecting the **Attach existing policies directly** option.

- Firstly, type **Administrator** in the policy search bar.
- Then click the **AdministratorAccess** check-box.
- We want to equip this user with the highest privileges in AWS since we created it for ourselves and therefore we choose the AdministratorAccess policy.
- So, the user with AdministratorAccess can access nearly all AWS resources.
- Continue by leaving the Set permissions boundary section as default for now.
- Then go to the **Tags** page by pressing the **Next** tab.

Creating IAM User - Add Tags



Add user

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
Department	AWS	✖
Job	Instructor	✖
Add new key		

You can add 48 more tags.

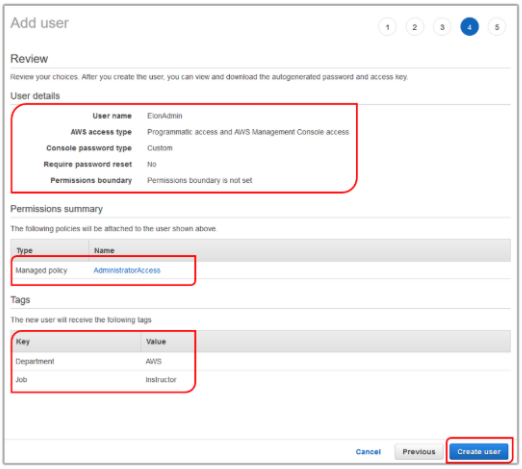
Tags are labels created as key-value pairs and can be assigned to all resources in AWS. Tags let you categorize your AWS resources in various ways. In this way, resources can be collected and displayed together. Then, what this source is about can be easily understood.

As an example, let's create 2 tags for this user.

- Department: AWS
- Job: Instructor

In this way, we tagged the user's department as AWS and the job as an instructor. Then, when we search the resources in AWS Resource groups with the instructor or AWS tag, we will be able to see this user as well.

Creating IAM User - Review



Review

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

User details

User name	ElonAdmin
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess

Tags

The new user will receive the following tags

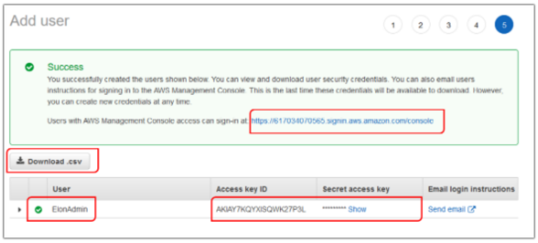
Key	Value
Department	AWS
Job	Instructor

In the review page, we have the opportunity to see everything we have done so far, and if there is anything we have done wrong after checking it, we can return there and correct it again.

Then, let's click the **Create user** tab.

Creating IAM User - Credentials

Congratulations! The creation of an IAM user with administrator authority process is completed.



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://617034070565.signin.aws.amazon.com/console

User	Access key ID	Secret access key	Email login instructions
ElonAdmin	AKIAY7KQYXISQWK27P3L	********* Show	Send email

The created user can access the AWS console with the username and password via the URL in the image.

Since we also define the **Programmatic Access** authorization for the user, the **Access key ID** and **Secret access key** information of the user has also been created. It is useful to save this information elsewhere or to download it by clicking the **Download .csv** option. Because this information appears here once and we cannot reach this information through the console again. However, if we want, we can recreate these keys later.