AWS Security - Part 1

Task: Create AWS account and set up for below tasks

- First step is to secure root user by enable MFA on root user
- Create a news user or group for day to day tasks

What is the need to perform this:

Securing an AWS root account is crucial because it has **unrestricted access** to all resources and services within your AWS environment. If compromised, an attacker could **delete resources, steal data, or even lock you out of your own account**.

Key Reasons to Secure the Root Account:

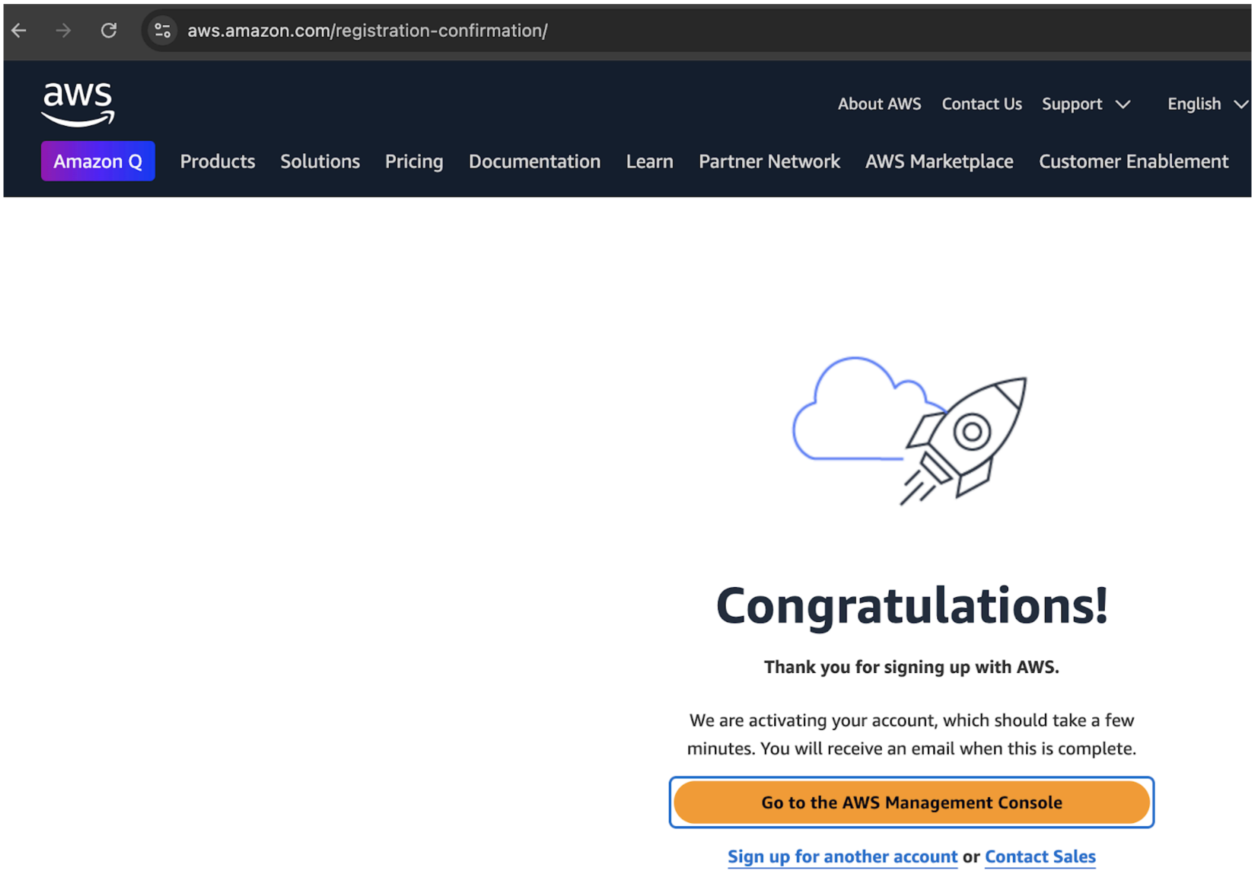
1. **Prevents Unauthorized Access** – The root account has full control, making it a prime target for hackers.

2. **Mitigates Security Risks –** Without security measures, an attacker could create malicious users, change billing details, or shut down services.

3. **Aligns with Best Practices** – AWS recommends using the root account **only for initial setup** and securing it with **Multi-Factor Authentication (MFA)**.

The best practice is to **enable MFA on the root user and create separate IAM users** with **least privilege access** for daily operations.

Once you have setup your account click on “Go to the AWS Management Console”



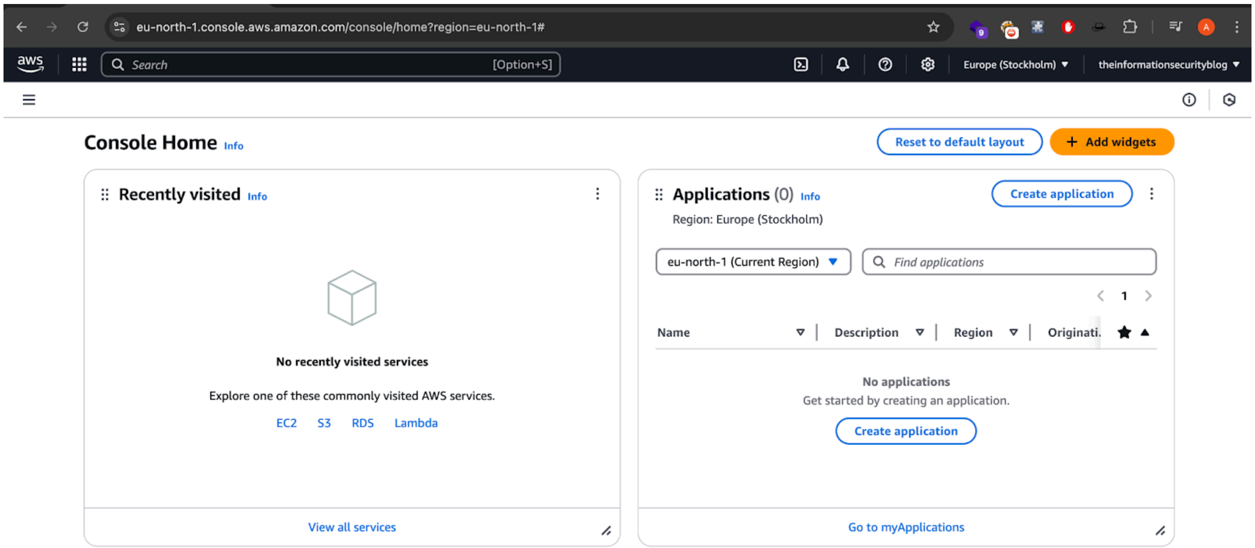
Congratulations!

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

Management Console



No recently visited services

Explore one of these commonly visited AWS services.

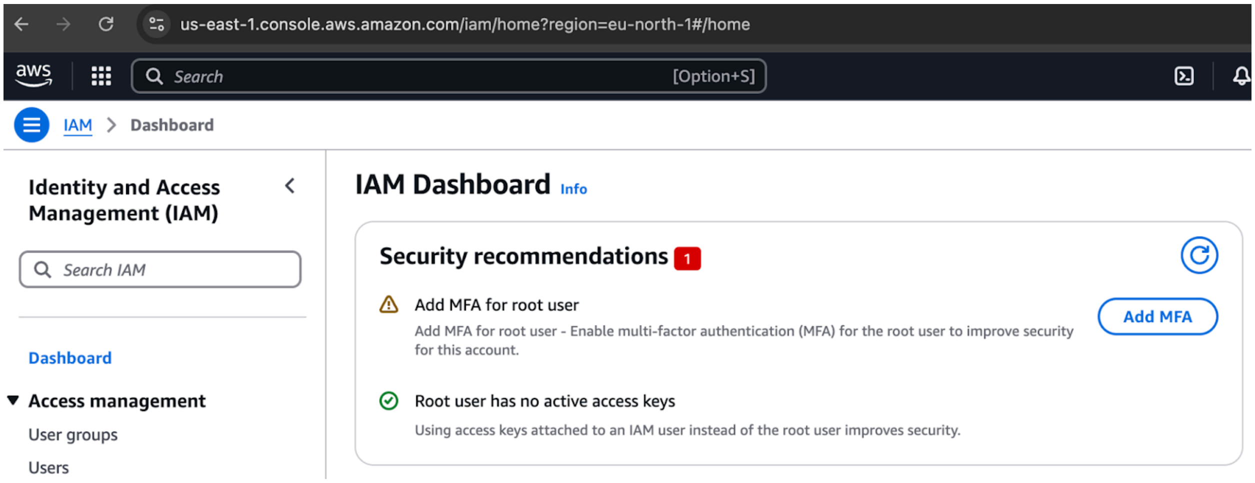
Region: Europe (Stockholm)

No applications

Get started by creating an application.

Now you are logged in using your root user

In the search box type IAM



us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/home

IAM > Dashboard

Identity and Access Management (IAM)

Dashboard

▼ Access management

User groups

Users

IAM Dashboard Info

Security recommendations 1

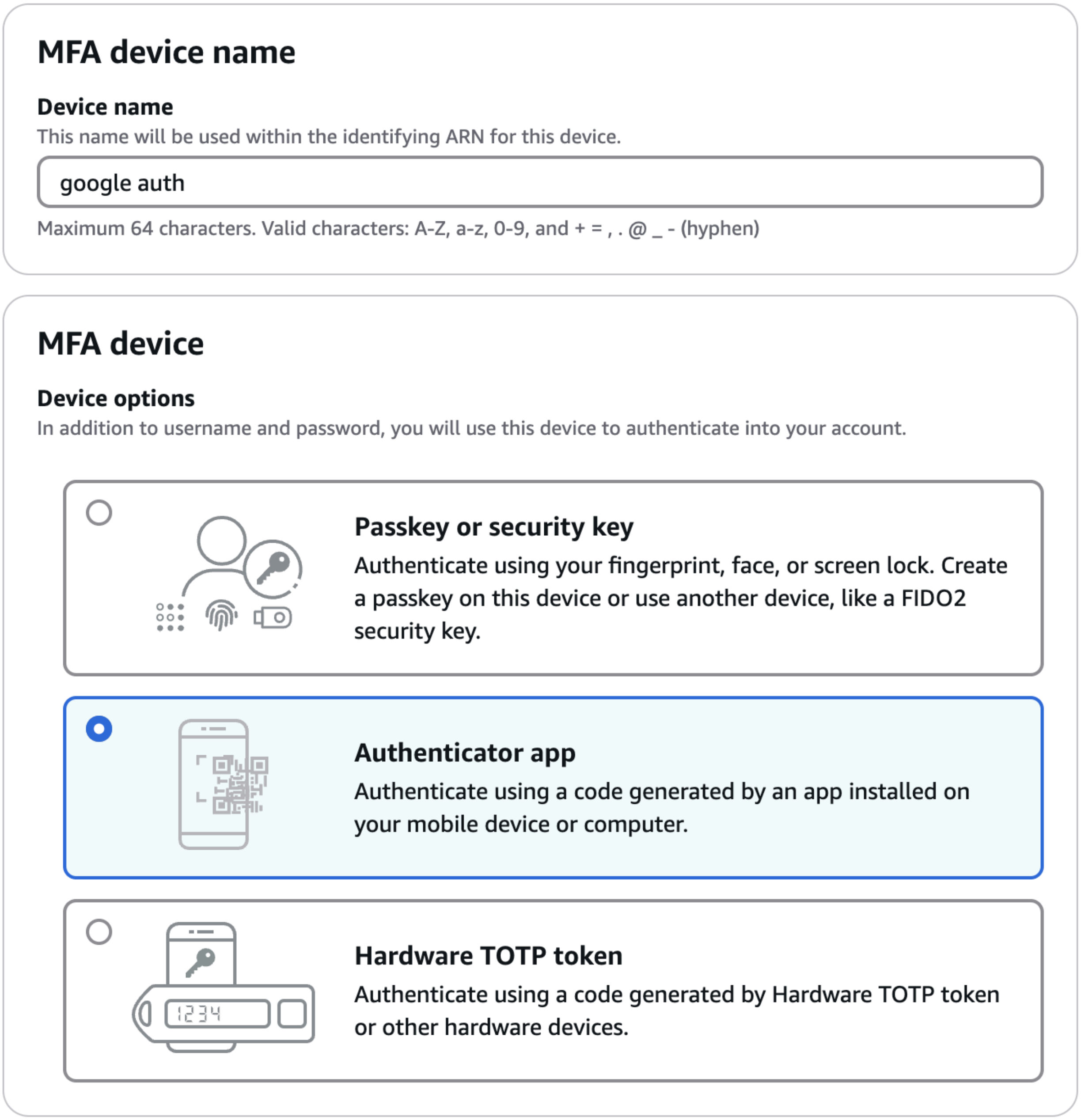
⚠ Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

✓ Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

And click on add MFA



MFA device name

Device name

This name will be used within the identifying ARN for this device.

google auth

Maximum 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

MFA device

Device options

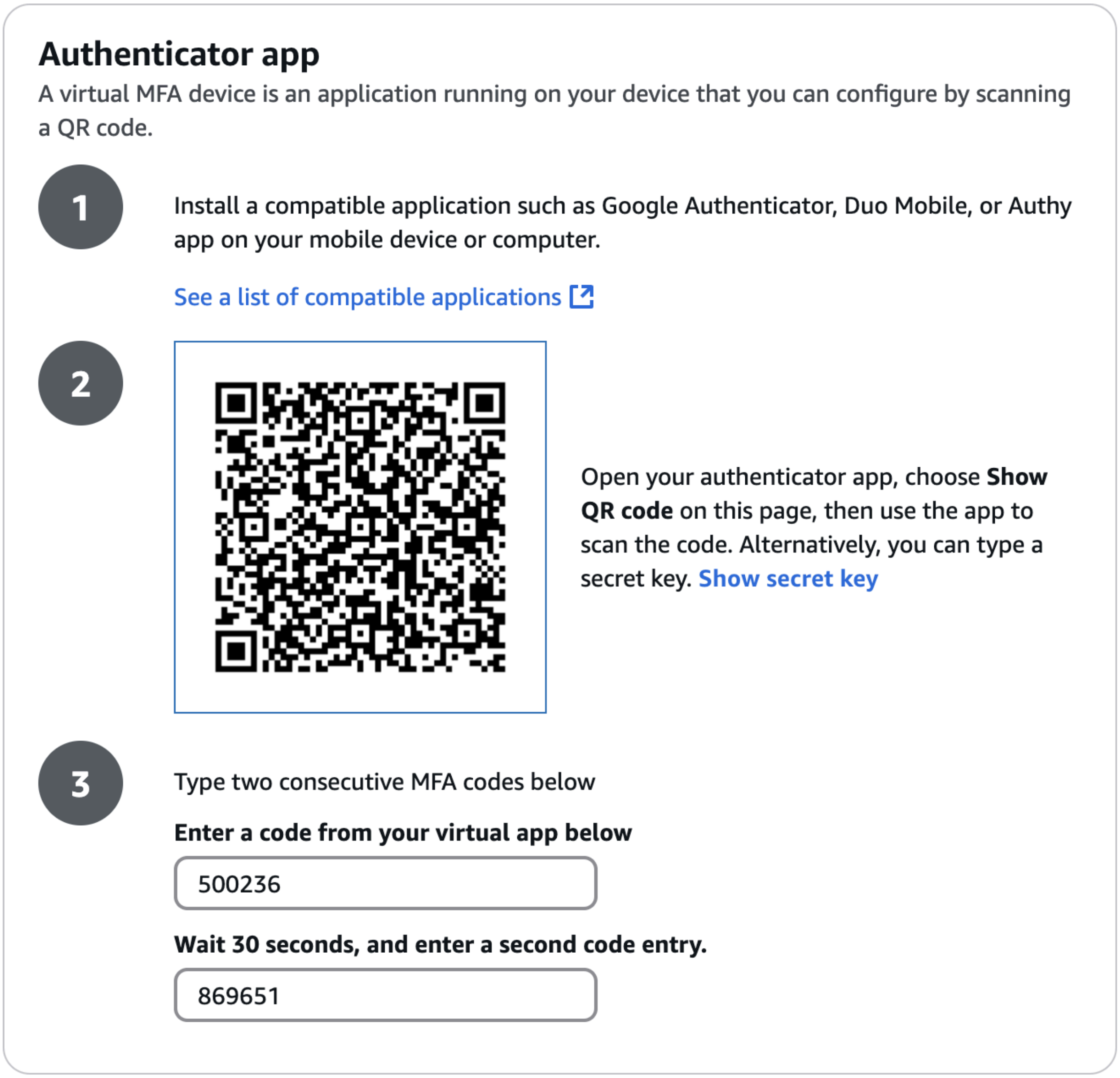
In addition to username and password, you will use this device to authenticate into your account.

○ **Passkey or security key**
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

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

○ **Hardware TOTP token**
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

And click on next. Follow the below steps:



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 Type two consecutive MFA codes below

Enter a code from your virtual app below

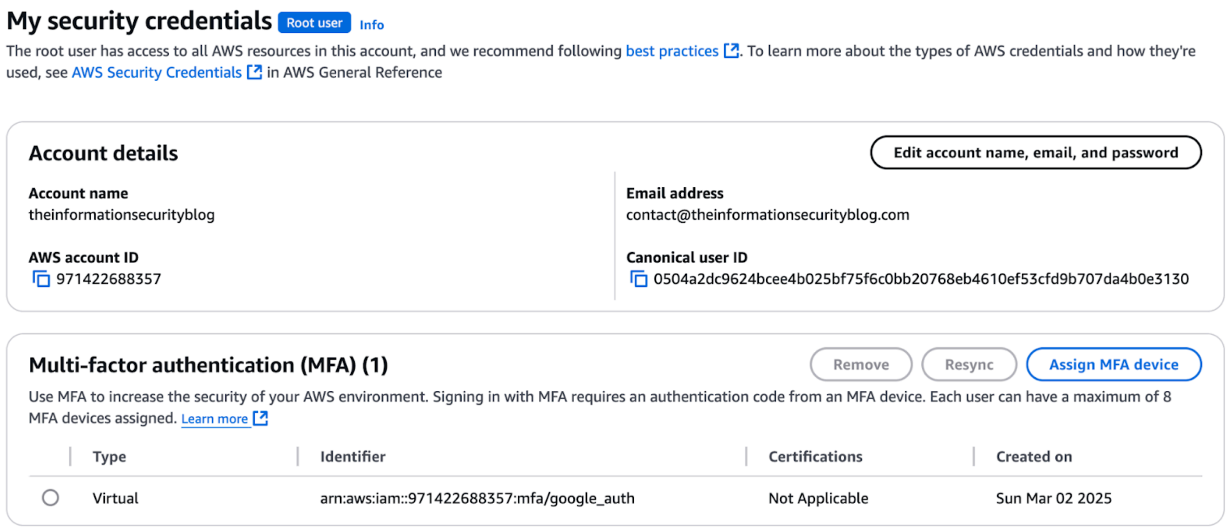
500236

Wait 30 seconds, and enter a second code entry.

869651

Click on Add MFA.

Congratulations, MFA is set for root user.



My security credentials

The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference

Account details

Account name
theinformationsecurityblog

Email address
contact@theinformationsecurityblog.com

AWS account ID
971422688357

Canonical user ID
0504a2dc9624bcee4b025bf75f6c0bb20768eb4610ef53cfd9b707da4b0e3130

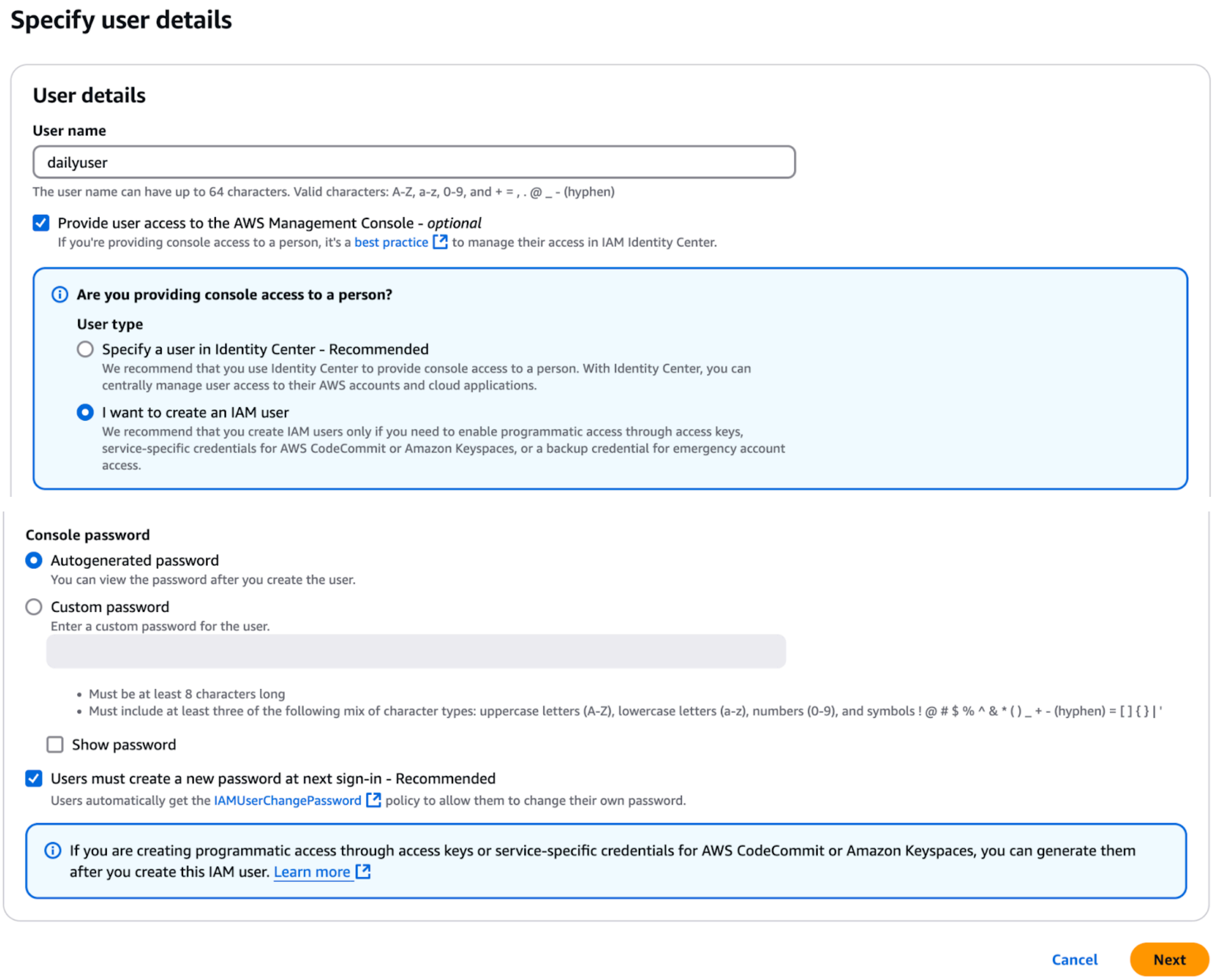
Multi-factor authentication (MFA) (1)

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

	Type	Identifier	Certifications	Created on
○	Virtual	arn:aws:iam::971422688357:mfa/google_auth	Not Applicable	Sun Mar 02 2025

Now, let's create a user or group for day to day activities.

So, as per the above snapshot on the left side there is an option “Users”. Click on it and then click on Create user.



Specify user details

User details

User name

dailyuser

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.

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

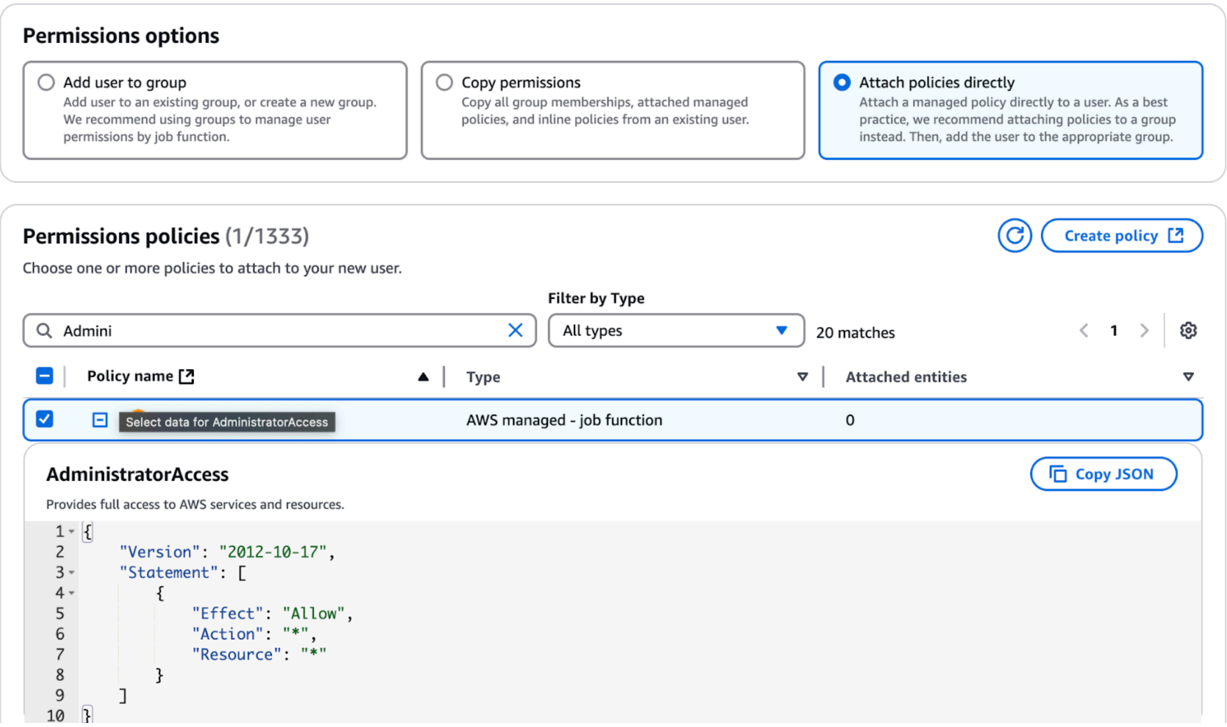
☐ Show password

☑ 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

Click on Next. Attach policy to the user. For now, since we need this user to perform admin tasks we are providing administrative access. Remember for unprivileged user always follow principle of least privilege.



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.

Permissions policies (1/1333)

Choose one or more policies to attach to your new user.

Filter by Type

Admini | All types | 20 matches | 1

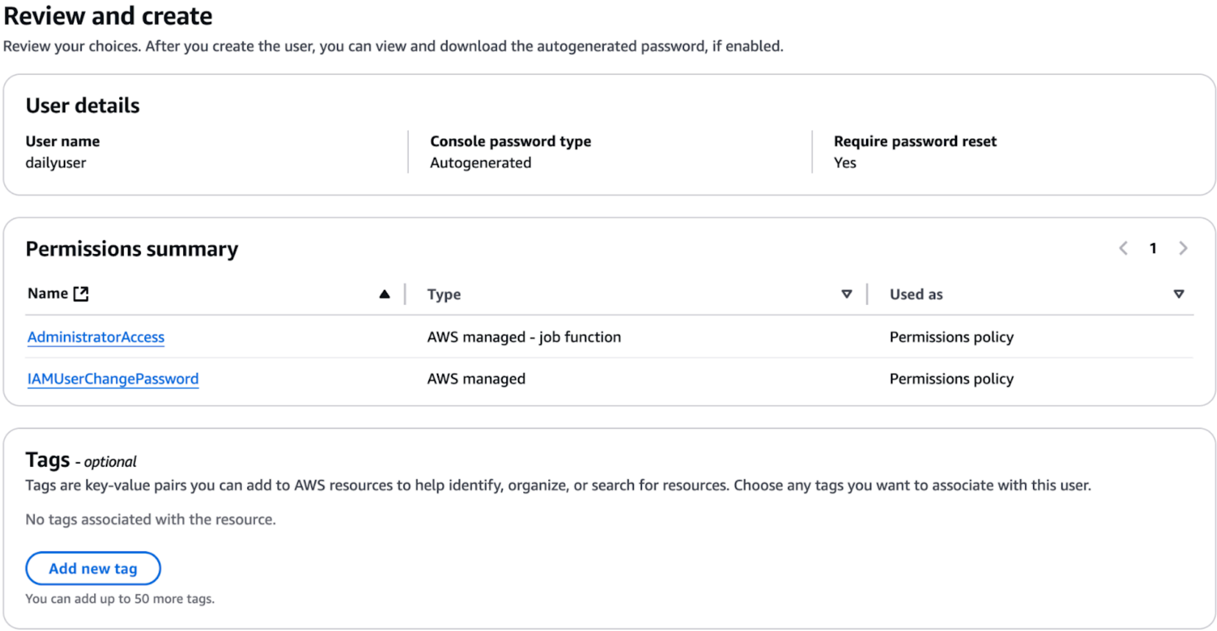
	Policy name	Type	Attached entities
☑	⊟ Select data for AdministratorAccess	AWS managed - job function	0

AdministratorAccess

Provides full access to AWS services and resources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Review the below configuration for the new user.



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	Console password type	Require password reset
dailyuser	Autogenerated	Yes

Permissions summary

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

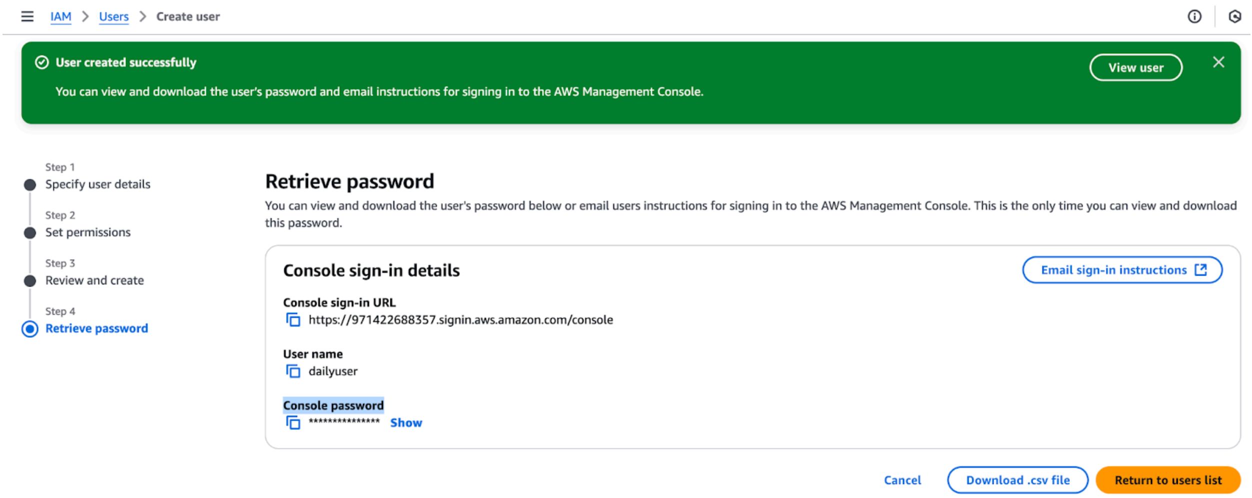
Tags - *optional*

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.

You can add up to 50 more tags.

And click on create user. The password is mentioned below and can be copied or the login instructions can be sent over email by using "Email sign-in instructions" option on the right hand side.



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

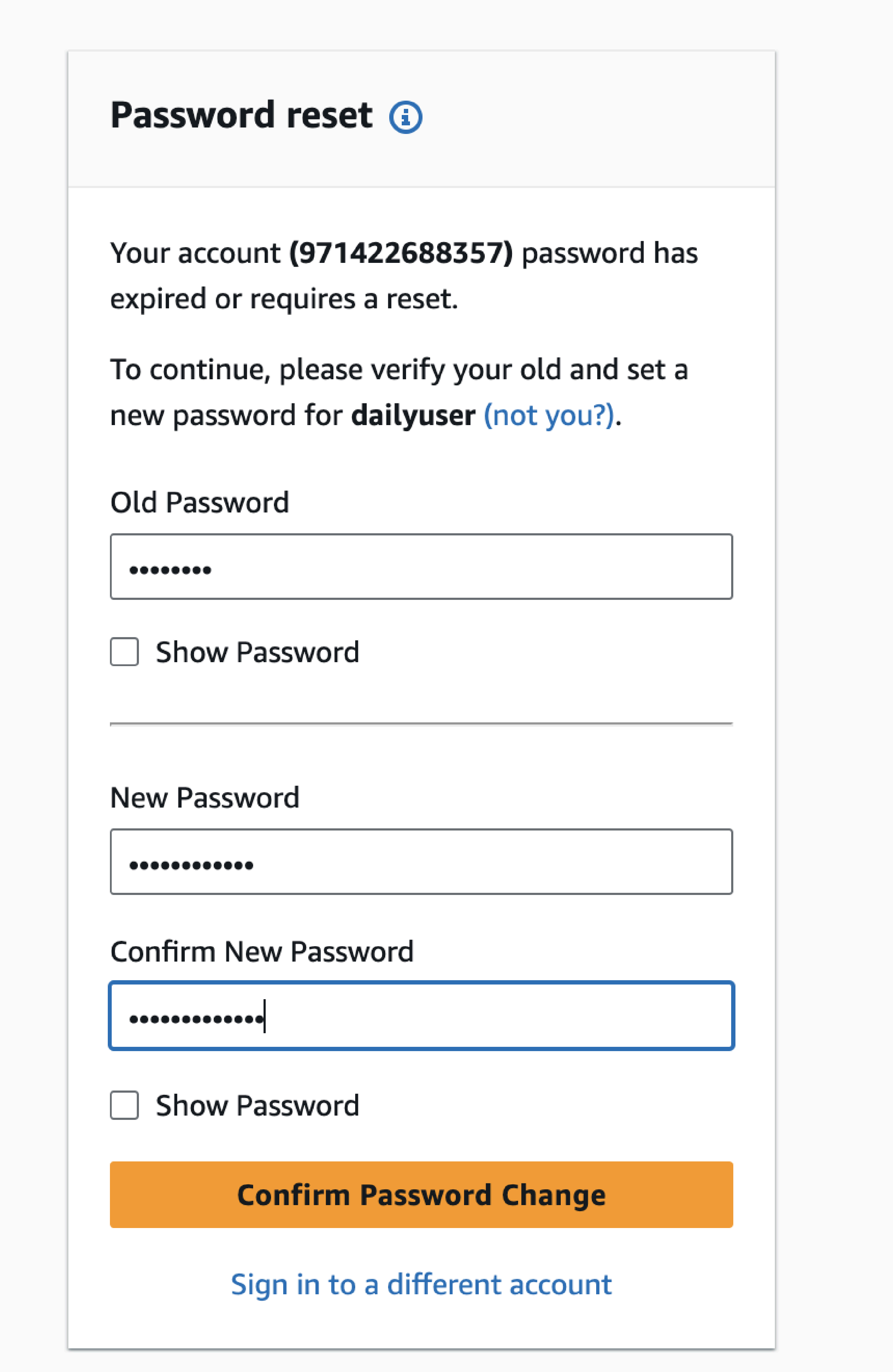
Console sign-in details

Console sign-in URL
https://971422688357.signin.aws.amazon.com/console

User name
dailyuser

Console password
*************** Show

Copied the sign-in URL, username and console password. Let's try to sign in with that new user. Now as per the policy set the user will have to set a new password in order to proceed.



Password reset ⓘ

Your account **(971422688357)** password has expired or requires a reset.

To continue, please verify your old and set a new password for **dailyuser** (not you?).

Old Password

•••••••••

□ Show Password

New Password

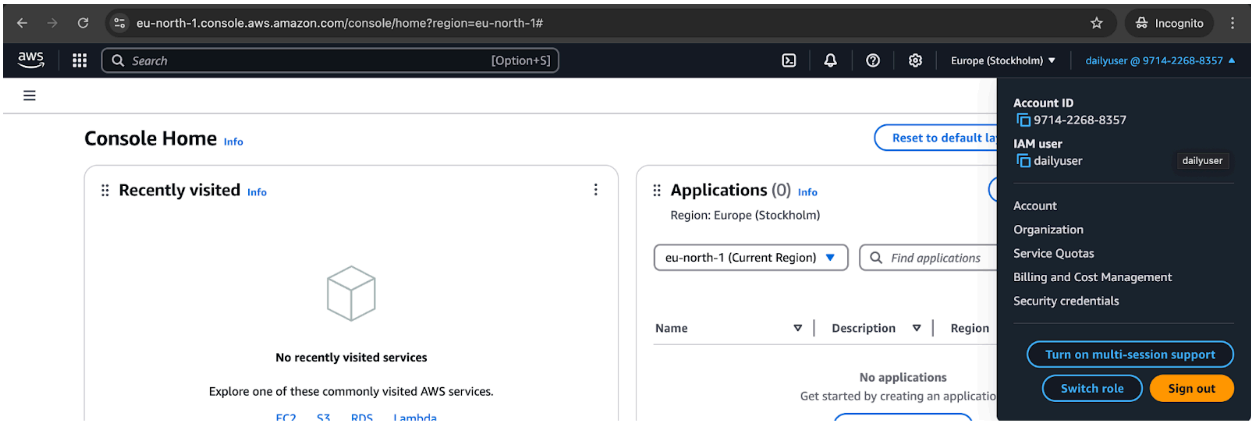
•••••••••••••

Confirm New Password

•••••••••••••

□ Show Password

Once password is set. The new user is logged in.



eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1#

Account ID
9714-2268-8357
IAM user
dailyuser

Region: Europe (Stockholm)

No recently visited services

Explore one of these commonly visited AWS services.

No applications
Get started by creating an applicatio

Congratulations, we have now secured our root account with MFA and created a new admin user for daily activities.