



Cloud Management Unit

WIPO AWS Cloud Offshore users authentication

Playbook

Author: Fayçal RABAHI
Document reference:
Version: 1.0

WIPO AWS CLOUD OFFSHORE USERS AUTHENTICATION

1. Document Maintenance

1.1. [Introduction](#)

This document describes the configuration that should be followed by the offshore users to authenticate to WIPO AWS cloud.

1.2. [Purpose of document](#)

This document summarizes, on the understanding of the existing solution, the required steps to setup a new configured offshore user in the WIPO Cloud solution.

1.3. [Document location](#)

This document is valid from the day of its official publication (marked in the revision history table below) and until a new version of the document is made available.

1.4. [Revision History](#)

Revision date	Version	Summary of Changes	Author
March 06, 2020	1.0	First Draft	Fayçal RABAHI
Approval Date	Status		Approver
			William Meridith

1.5. [Associated documentation](#)

- WIPO AWS Cloud IAM Strategy
- WIPO AWS Cloud Tagging and Naming convention Standard

Table of Content

1. Document Maintenance2

1.1. Introduction2

1.2. Purpose of document2

1.3. Document location2

1.4. Revision History2

1.5. Associated documentation.....2

2. IMPORTANT:4

3. Login to AWS5

4. Change your password:.....6

5. Create you access key:.....7

6. Assign an MFA.....8

7. Login To WIPO account 11

8. Setup AWS CLI access 13

2. IMPORTANT:

For offshore users:

- In no case S3 Public access should be created
- In no case, 0.0.0.0/0 permission should be created in the security groups.
- For VPC creation, CIDR should be requested from your business owner.
- Respect the naming convention
- Please keep the dev and sandbox environment as clean as possible.
- Tag all your resources with the service you are affiliated to (TAG → service : service name) (ask your business owner)
- In all your resources with company name (TAG → company: company name)
- Check the billing each day.
- Report any incident or issue to your business owner and cloud-support@wipo.int
- Use cloudformation as automation tool as much as you can.

WIPO AWS CLOUD ACCOUNT CREATION

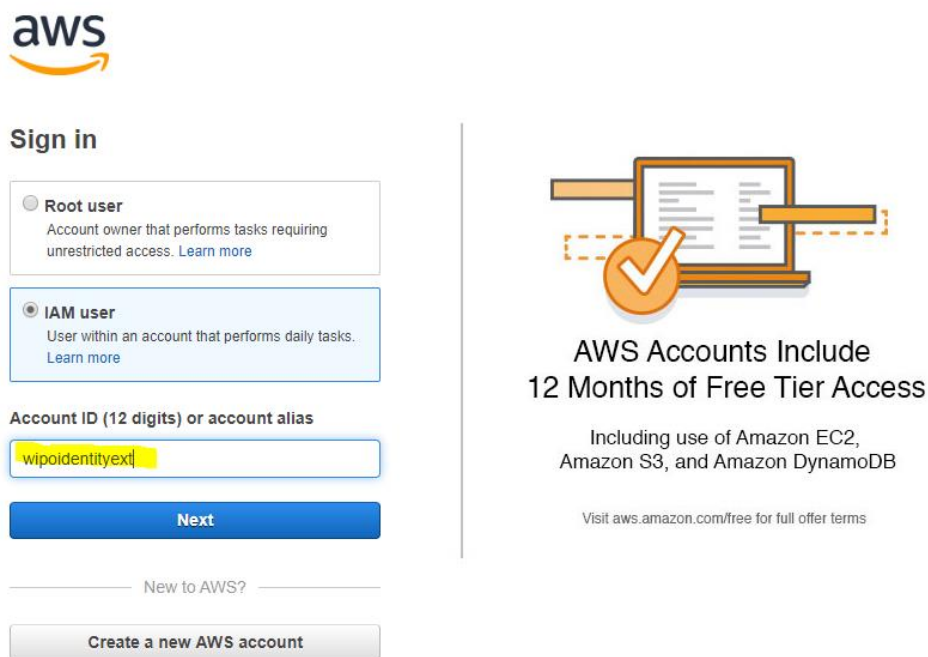
This guide will help you setup your Multi Factor Authentication (MFA) device that will be used to manage your AWS credentials and as well as programmatically access your AWS environment (CLI/SDK/...).

All access to WIPO AWS accounts requires multifactor authentication, you will need to ensure completing all steps in a timely manner without mistake in order to avoid partially assigning MFA. In case the MFA device setup was not properly completed, you prohibited from further steps. Contact WIPO AWS Administrator or Cloud Support

3. Login to AWS

- Connect to aws.amazon.com
- Select IAM user
- enter: **wipoidentityext**

Or sign in <https://wipoidentityext.signin.aws.amazon.com/console/>



aws

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](#)

Account ID (12 digits) or account alias
wipoidentityext

Next

[New to AWS?](#)

Create a new AWS account

**AWS Accounts Include
12 Months of Free Tier Access**

Including use of Amazon EC2,
Amazon S3, and Amazon DynamoDB

Visit aws.amazon.com/free for full offer terms

In the next page, enter the username and the password you received from wipo administrator

WIPO AWS CLOUD OFFSHORE USERS AUTHENTICATION

The image shows the AWS IAM user sign-in interface. On the left, there is a 'Sign in as IAM user' section with three input fields: 'Account ID (12 digits) or account alias' containing 'wipoidentityext', 'IAM user name' containing a redacted name followed by '@wipo.int', and 'Password' containing a masked password. Below these fields is a blue 'Sign in' button. Underneath the button are links for 'Sign in using root user email' and 'Forgot password?'. To the right of the sign-in form is a large banner for the 'aws RE:INFORCE' event, dated 'June 30 - July 1, 2020 • Houston, TX'. The banner text reads: 'Two days and hundreds of sessions focused on cloud security, identity, and compliance.' with a 'Register Now' button. At the bottom of the page, there is a language selector set to 'English' and a small link for 'Terms of Use Privacy Policy © 1996-2020, Amazon Web Services, Inc. or its affiliates.'

4. Change your password:

You will be prompted to change your password, please change it respecting the requirement below:

- Minimum password length is 14 characters
- Require at least one uppercase letter from Latin alphabet (A-Z)
- Require at least one lowercase letter from Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character (!@#\$%^&*()_+=[{}]|')
- Password expiration requires administrator reset
- Allow users to change their own password
- Remember last 24 password(s) and prevent reuse
- Password expiration requires administrator reset

Password expiration requires administrator reset : For information the password expiration is set 180 days (6 months) after this period please ask you project Business Owner for a renewal.

WIPO AWS CLOUD ACCOUNT CREATION



You must change your password to continue

AWS account [REDACTED]

IAM user name [REDACTED]@wipo.int

Old password

New password

Retype new password

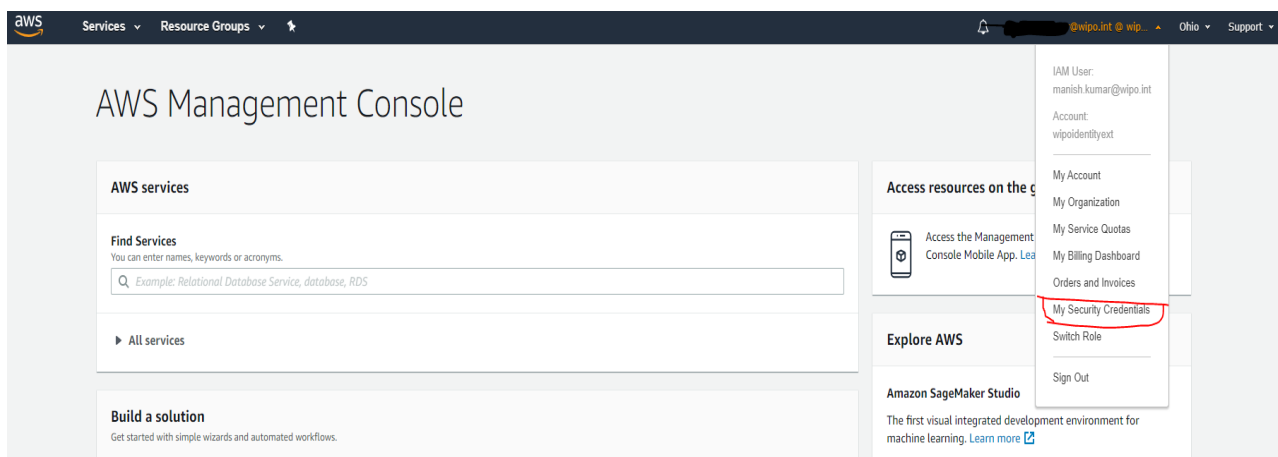
[Confirm password change](#)

[Sign in using root user email](#)

5. Create you access key:

Once you changed your password, in the top right of the page:

- click on your email
- Select My Security Credentials



- In the Access keys for CLI, SDK, &API access delete the access key created by default.
- Click create access key
- Download the CSV file which contain you credentials.

This key is strictly personal and nominative; it should never be shared or integrated to any code.

WIPO AWS CLOUD OFFSHORE USERS AUTHENTICATION

AWS IAM credentials AWS CodeCommit credentials Amazon MCS credentials

Password for console access

As an IAM user, you need a password to access the AWS Management Console. We recommend changing your password on a regular basis. Your current password is 0 days old. [Learn more](#)

[Change password](#)

Access keys for CLI, SDK, & API access

Use access keys to make programmatic calls to AWS from the AWS Command Line Interface (AWS CLI), Tools for Windows PowerShell, the AWS SDKs, or direct AWS API calls. **If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.** [Learn more](#)

[Create access key](#)

Access key ID	Status	Created	Last used	Actions
AKIAZ4M5GGQWTVML3SLF	Active	2020-03-03 16:10 UTC+0100	N/A	Make inactive Delete

Create access key

✓ Your new access key is now available.

This is the only time that the secret access key can be viewed or downloaded.
You cannot recover it later. However, you can create new access keys at any time.

[Download .csv file](#)

Access key ID	AKIAZ4M5GGQW3GDSQIXK	Copy
Secret access key	Show secret access key	

[Close](#)

6. Assign an MFA

MFA is a requirement to access to WIPO AWS accounts.

Before going further download an MFA app to your mobile (Ex: google authenticator).

- In my security credentials page, click assign MFA

WIPO AWS CLOUD ACCOUNT CREATION

AWS IAM credentials | AWS CodeCommit credentials | Amazon MCS credentials

Password for console access

As an IAM user, you need a password to access the AWS Management Console. We recommend changing your password on a regular basis. Your current password is 0 days old. [Learn more](#)

[Change password](#)

Access keys for CLI, SDK, & API access

Use access keys to make programmatic calls to AWS from the AWS Command Line Interface (AWS CLI), Tools for Windows PowerShell, the AWS SDKs, or direct AWS API calls. **If you lose or forget your secret key, instead, create a new access key and make the old key inactive.** [Learn more](#)

[Create access key](#)

Access key ID	Status	Created	Last used	Actions
AKIAZ4M5GGQWTVML3SLF	Active	2020-03-03 16:10 UTC+0100	N/A	Make inactive Delete

Multi-factor authentication (MFA)

For increased security, we recommend configuring MFA to help protect your AWS resources. MFA requires users to type a unique authentication code from an approved authentication device when they sign in to AWS

[Assign MFA device](#)

- It displays the page below:

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](#)

[Cancel](#) [Continue](#)

- Click continue
- Scan the QR code with your mobile app
- Enter the first MFA code and the second MFA code.
- Click assign MFA

WIPO AWS CLOUD OFFSHORE USERS AUTHENTICATION

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

Show 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

Cancel

Previous

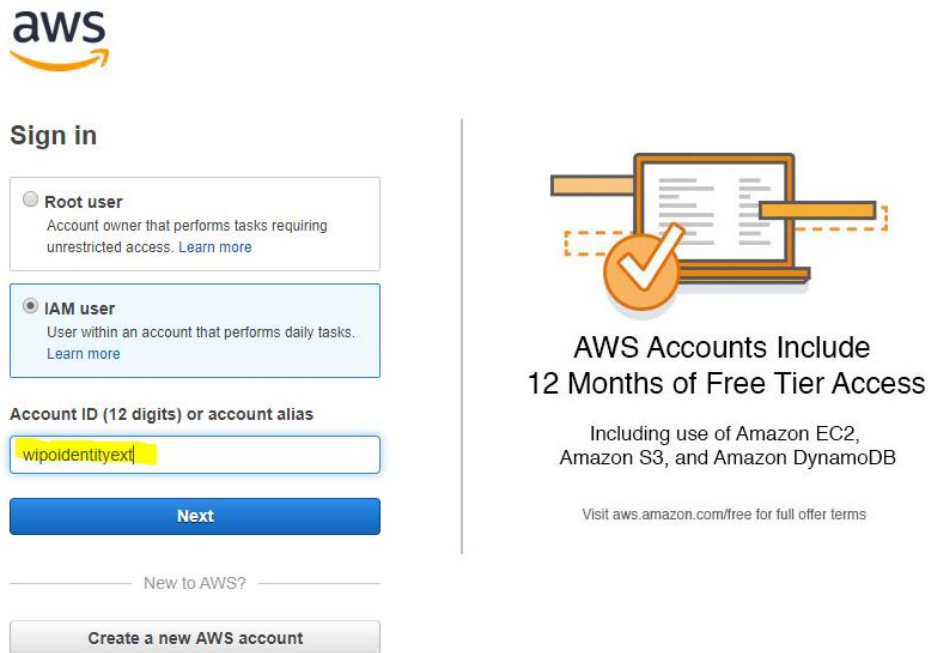
Assign MFA

- Go to the top right of the page.
- Click on your email and sign out. (this step is mandatory as you have to sign in with your MFA you just set)

WIPO AWS CLOUD ACCOUNT CREATION

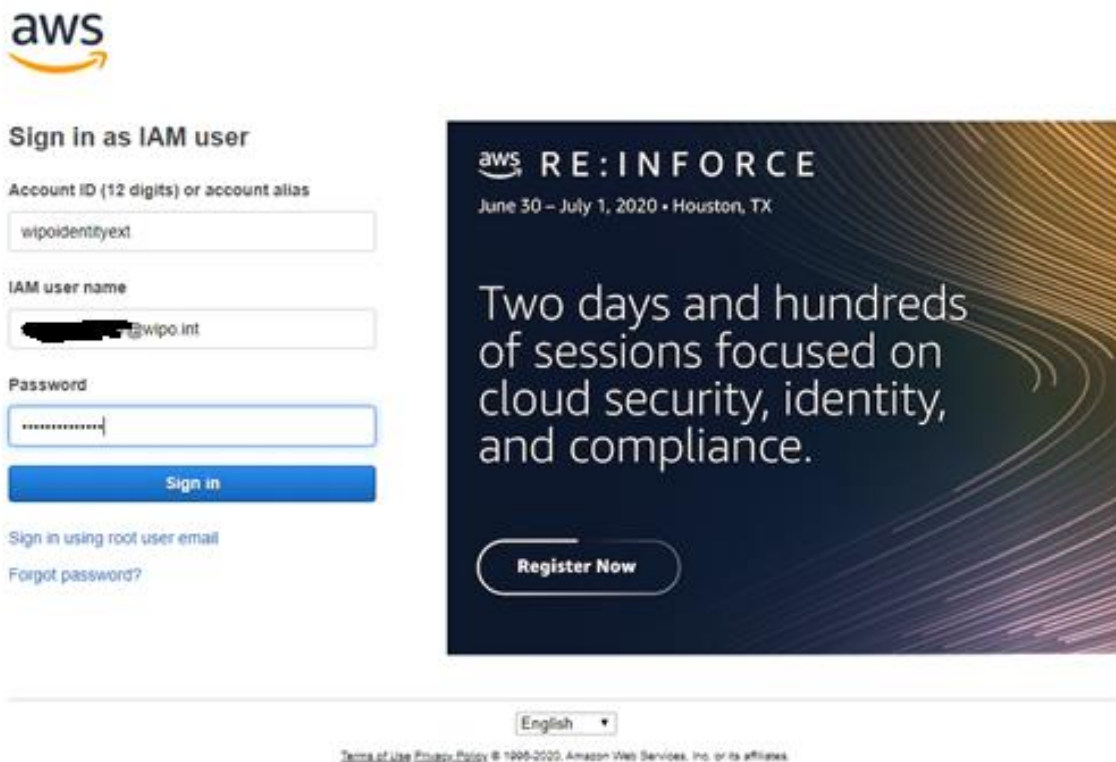
7. Login To WIPO account

- sign in <https://wipoidentityext.signin.aws.amazon.com/console/>



The screenshot shows the AWS Sign in page. On the left, there's a 'Sign in' section with two options: 'Root user' (Account owner that performs tasks requiring unrestricted access. [Learn more](#)) and 'IAM user' (User within an account that performs daily tasks. [Learn more](#)). The 'IAM user' option is selected. Below this is a field for 'Account ID (12 digits) or account alias' containing 'wipoidentityext'. A blue 'Next' button is below the field. At the bottom, there's a link 'New to AWS?' and a button 'Create a new AWS account'. On the right, there's a graphic of a document with a checkmark and the text 'AWS Accounts Include 12 Months of Free Tier Access'. Below this, it says 'Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB' and 'Visit aws.amazon.com/free for full offer terms'.

- Enter you username and Password



The screenshot shows the AWS Sign in as IAM user page. On the left, there's a 'Sign in as IAM user' section with three fields: 'Account ID (12 digits) or account alias' containing 'wipoidentityext', 'IAM user name' containing 'wipo.int', and 'Password' containing a masked password. A blue 'Sign in' button is below the fields. Below the button, there's a link 'Sign in using root user email' and a link 'Forgot password?'. On the right, there's a banner for 'aws RE:INFORCE' with the text 'June 30 – July 1, 2020 • Houston, TX' and 'Two days and hundreds of sessions focused on cloud security, identity, and compliance.' Below the banner is a button 'Register Now'. At the bottom, there's a language dropdown menu set to 'English' and a link 'Terms of Use Privacy Policy © 1996-2020, Amazon Web Services, Inc. or its affiliates'.

- Enter your MFA



Multi-factor Authentication

Please enter an MFA code to complete sign-in.

MFA Code:

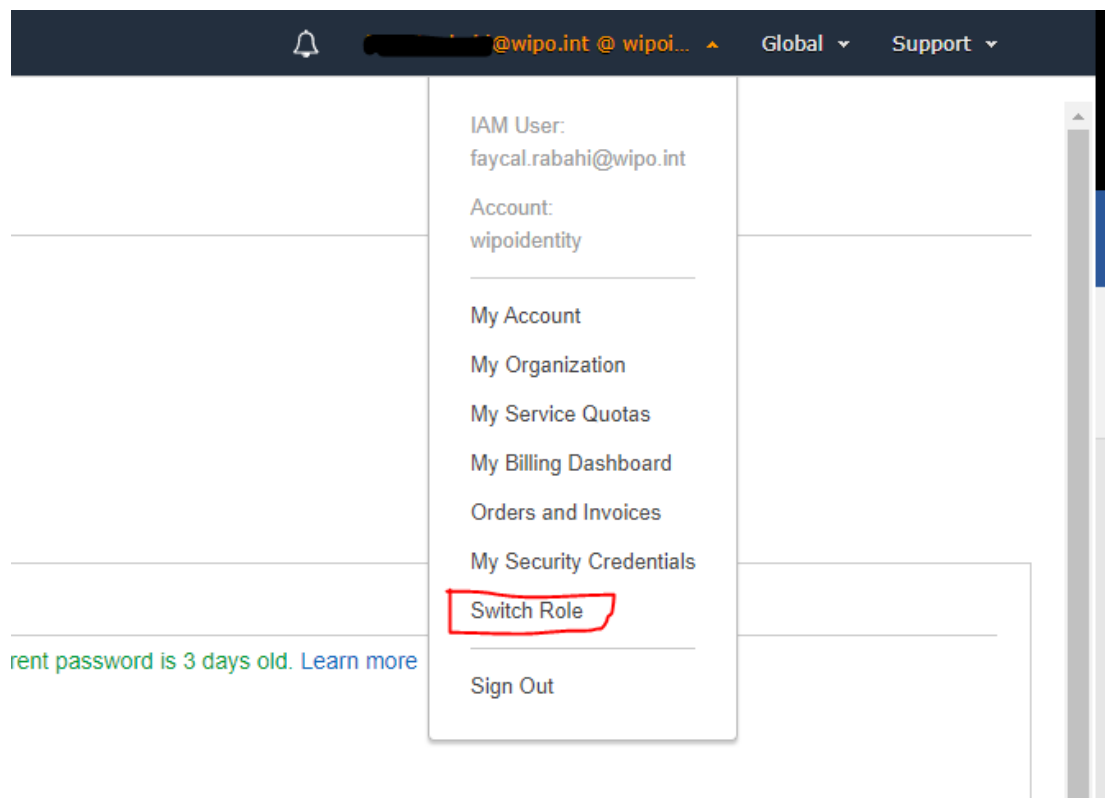
Submit

[Cancel](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2020, Amazon Web Services, Inc. or its affiliates.

- From the wipoidentityext account, in the top right of the page click on your email, and then switch role




In the displayed page :

- the account given to you by the Business owner or WIPO Administrators

WIPO AWS CLOUD ACCOUNT CREATION

- the role given to you by Business owner or WIPO Administrators



Switch Role

Allows management of resources across AWS accounts using a single user ID and password. You can switch roles after an AWS administrator has configured a role and given you the account and role details. [Learn more](#).

Account* ⓘ

Role* ⓘ

Display Name ⓘ

Color a a a a a a

*Required Cancel Switch Role

You should now be connected to the WIPO account.

8. Setup AWS CLI access

- Download and install AWS Client
<https://aws.amazon.com/cli/>
- Configure AWS CLI profile
 - Add credentials to be used by AWS CLI
Open command prompt and type
 - `aws configure --profile with-mfa`
 - enter AWS Access Key ID
 - enter AWS Secret Access Key

without “--profile” to setup default profile
“--profile *credentials_profile_name*” to name profile to your convenience
 - Add profile to AWS CLI configuration
 - Edit the AWS Config file and add access profile for incumbent *AWS account ID* and *role*

Only values in orange need to be edited.

```
[profile configuration_profile_name]
role_arn = arn:aws:iam::AWS Account ID:role/role
mfa_serial = MFA device ARN
source_profile = with-mfa
region = eu-central-1
```

 - The *AWS Account ID* and *role* are provided to you with the account availability notification
 - The *mfa_serial* ARN can be found from the AWS Console under your security credentials
 - The *source_profile* corresponds to value set for *credentials_profile_name*
 - Test access

WIPO AWS CLOUD OFFSHORE USERS AUTHENTICATION

Open command prompt and type

➤ `aws iam --profile configuration_profile_name s3 ls`