

AWS Security

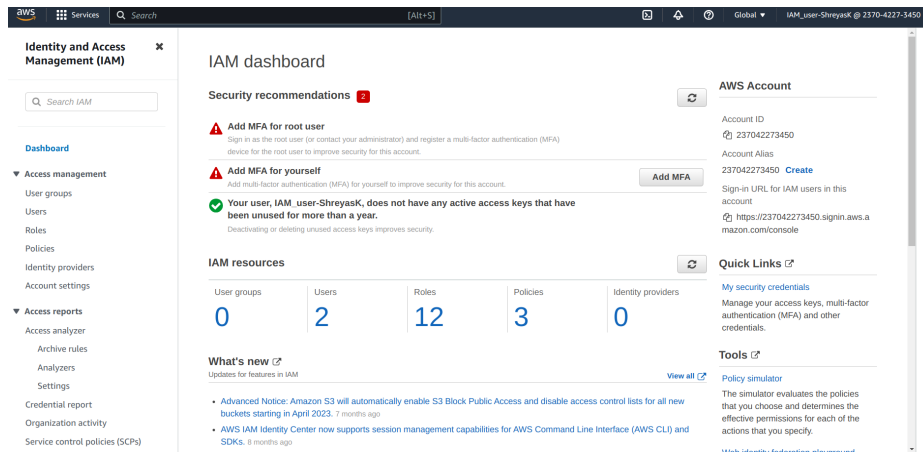
Day 1 - Assignment

10th July 2023

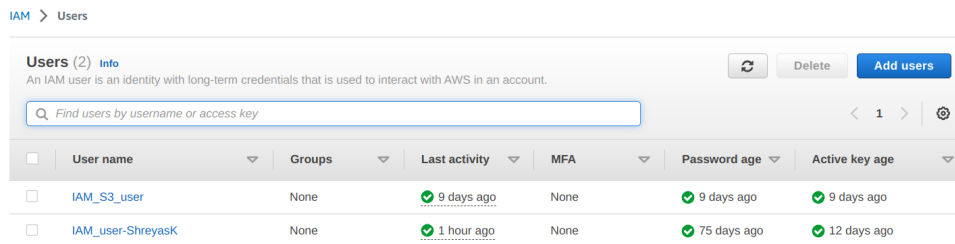
Assignment 1

Creating an IAM with MFA enabled.

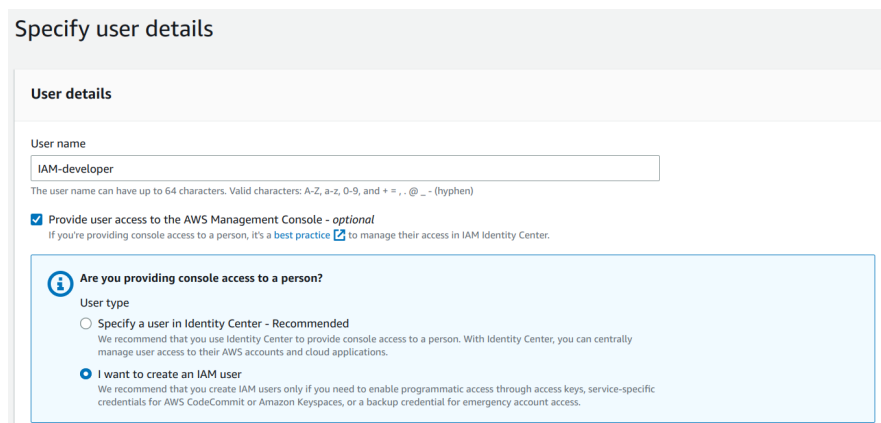
Step 1 - Login to AWS management console as an admin user. Browse to the IAM console.



Step 2 - Click on “Users” on the left navigation pane. Then click on “Add Users” to create a new IAM user.



Step 3 - Enter the username for the IAM user. Select a password for the user.



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](#)

Cancel Next

Step 4 - click next. Select “Add user to a group” then click on “Create group”.

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.

ⓘ Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

► Set permissions boundary - optional

Cancel Previous Next

Step 5 - Enter the name for the group “Developer” then select a policy to attach to the group. Here the “PowerUserAccess” policy allows access to all AWS services but not to manage and create users and groups.

Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

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

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

Permissions policies (1/864)

Filter by Type

1 match

| <input checked="" type="checkbox"/> | Policy name | Type | Use... | Description |
|-------------------------------------|-----------------|-----------------|--------|--------------------------------------|
| <input checked="" type="checkbox"/> | PowerUserAccess | AWS managed ... | None | Provides full access to AWS services |

Cancel Create user group

Step 6 - Select the created group and click “Next”.

User groups (1/1)

Search

| <input checked="" type="checkbox"/> | Group name ↗ | Users | Attached policies ↗ | Created |
|-------------------------------------|------------------------------|-------|-------------------------------------|---------------------------|
| <input checked="" type="checkbox"/> | Developer | 0 | PowerUserAccess | 2023-07-10 (1 minute ago) |

► Set permissions boundary - optional

Cancel Previous **Next**

Step 7 - Review and create the user.

The user is created successfully, download the .csv file to retrieve the username and 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 [Email sign-in instructions ↗](#)

Console sign-in URL
<https://237042273450.signin.aws.amazon.com/console>

User name
[IAM-developer](#)

Console password
***** [Show](#)

[Download .csv file](#) **Return to users list**

Step 8 - Open the details of the IAM user created above and click on “Assign MFA device”

Multi-factor authentication (MFA) (0)

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 ↗](#)

[Remove](#) [Resync](#) **Assign MFA device**

| Device type | Identifier | Certifications | Created on |
|--|------------|----------------|------------|
| No MFA devices. Assign an MFA device to improve the security of your AWS environment | | | |

[Assign MFA device](#)

Select MFA device

Specify MFA device name

Device name
Enter a meaningful name to identify this device.


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

Assign MFA device

Select MFA device [Info](#)

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

Authenticate through an Authenticator app.

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

307657

MFA code 2

451945

Cancel


Previous

Add MFA

Step 9 - Login to the IAM user with the link displayed in the console.

Console sign-in [Manage console access](#)


Console sign-in link

 <https://237042273450.signin.aws.amazon.com/console>

Console password

Updated 5 minutes ago (2023-07-10 16:41 GMT+5:30)

Last console sign-in

 Never

Step 10 - Open the “console sign-in link” and enter the details to login.

Sign in as IAM user

Account ID (12 digits) or account alias

237042273450

IAM user name

IAM-developer

Password

.....

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Step 11 - Enter the MFA code from the authenticator app.

Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

973410

Submit

[Cancel](#)

Step 12 - Change the password. The new password should be strong enough and kept secure.

AWS account 237042273450

IAM user name IAM-developer

Old password

New password

Retype new password

Confirm password change

Step 13 - It is seen that the IAM user “IAM-developer” cannot access or view anything in the IAM console.

[Alt+S]

Global

IAM-developer @ 2370-4227-3450

IAM dashboard

Security recommendations

Access denied
You don't have permission to `iam:GetAccountSummary`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::237042273450:user/IAM-developer
Service: iam
Action: GetAccountSummary
On resource(s): *
Context: no identity-based policy allows the iam:GetAccountSummary action

Copy

Access denied
You don't have permission to `iam:ListMFADevices`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::237042273450:user/IAM-developer
Service: iam
Action: ListMFADevices
On resource(s): user

Copy

AWS Account

Access denied

Quick Links

[My security credentials](#)
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

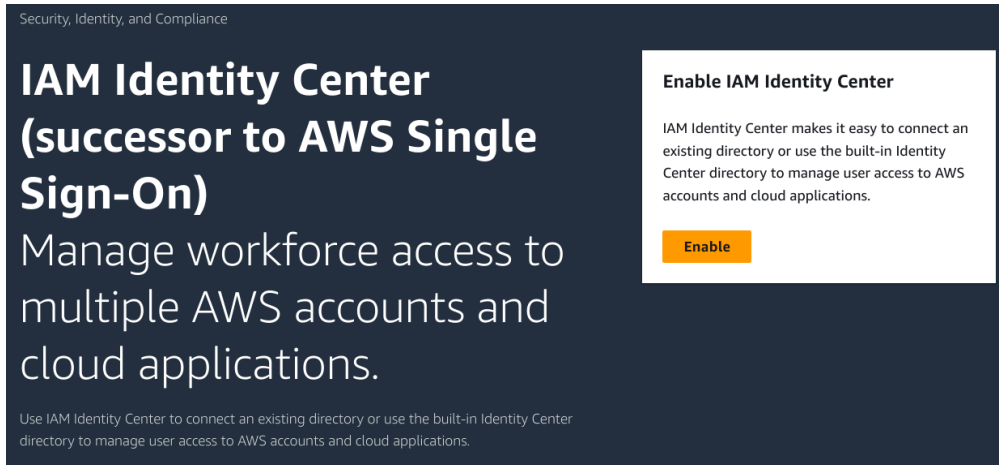
[Policy simulator](#)
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

[Web identity federation playground](#)
Authenticate yourself to any of the supported web identity providers, see

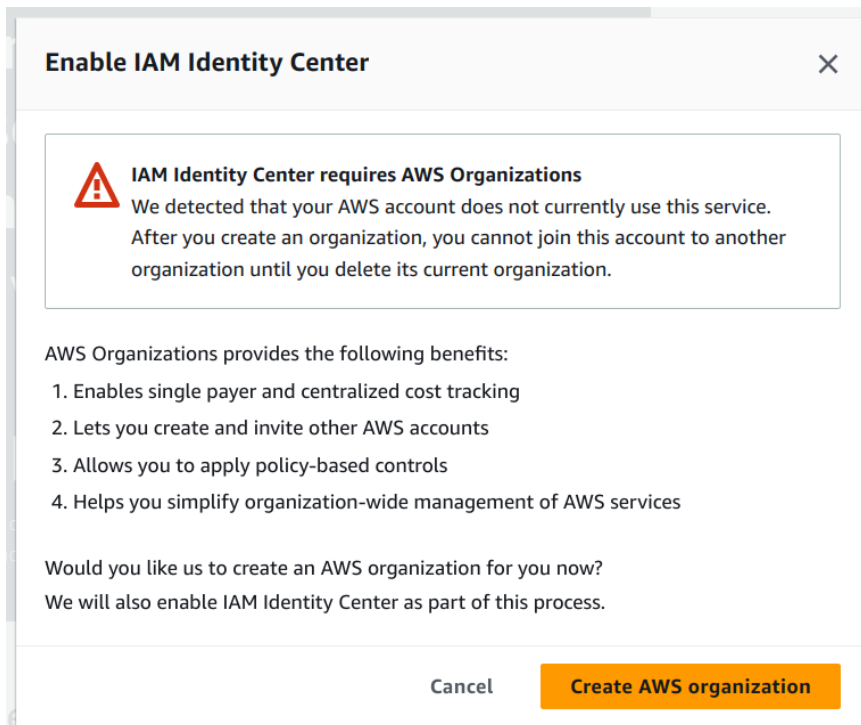
Assignment 2

Creating groups in the Identity Center.

Step 1 - Login to the AWS console and browse to the Identity Center console.




Step 2 - Click on Enable. It will ask to enable AWS organization as Identity Center requires it.




Step 3 - Create a new group in the Identity Center.

IAM Identity Center > Groups

Groups (0)
With groups, you can grant or deny permissions to groups of workforce users, rather than having to apply those permissions to each user. [Learn more](#)



< 1 > 

| Group name | Description | Created by |
|---|-------------|------------|
| No groups found | | |
| <input type="button" value="Create group"/> | | |

Create group

Group details

Group name

Maximum of 128 characters

Description - optional
Group description detailing the permissions assigned to this group.

Maximum of 256 characters

Create a new user

Specify user details

Primary information

Username
This username will be required for this user to sign in to the AWS access portal. The username can't be changed later.

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +,=,@,-_

Password
Choose how you want this user to receive their password. [Learn more](#)

☐ Send an email to this user with password setup instructions.

☒ Generate a one-time password that you can share with this user.

Email address

Confirm email address


First name

Last name


Display name
This is typically the full name of the workforce user (first and last name), is searchable, and appears in the users list.


Copy the sign-in instructions


One-time password ✕

 User password was reset for user "Developer-User1".


You can copy and share the instructions for signing in to the AWS access portal with this user, or email them the instructions. This is the one-time password.


AWS access portal URL
 <https://d-9f671c4aeb.awsapps.com/start>

Username
 Developer-User1

One-time password
 *****

☐ Show password

 Copy


 Sign in instructions copied


Close

Step 4 - Add the user to the “Developer-Group” group.

Add users to group - optional (1/1)
Select workforce users to add to this group.

Username ▼

< 1 > 

| <input checked="" type="checkbox"/> | Username | Display name | Status | MFA devices | Created by |
|-------------------------------------|-----------------|-----------------|---|-------------|------------|
| <input checked="" type="checkbox"/> | Developer-User1 | Developer User1 |  Enabled | None | Manual |

Cancel **Create group**

Step 5 - Create a new group “Sys-Admin”.

Create group

Group details

Group name

Maximum of 128 characters

Description - optional

Group description detailing the permissions assigned to this group.

Maximum of 256 characters

Create a new user.

Primary information

Username
This username will be required for this user to sign in to the AWS access portal. The username can't be changed later.

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +,=,@,-_

Password
Choose how you want this user to receive their password. [Learn more](#)
☐ Send an email to this user with password setup instructions.
☒ Generate a one-time password that you can share with this user.

Email address

Confirm email address

First name

Last name

Display name
This is typically the full name of the workforce user (first and last name), is searchable, and appears in the users list.

Step 6 - Add the user to the group “Sys-Admin”

Group details

Group name

Maximum of 128 characters

Description - optional
Group description detailing the permissions assigned to this group.

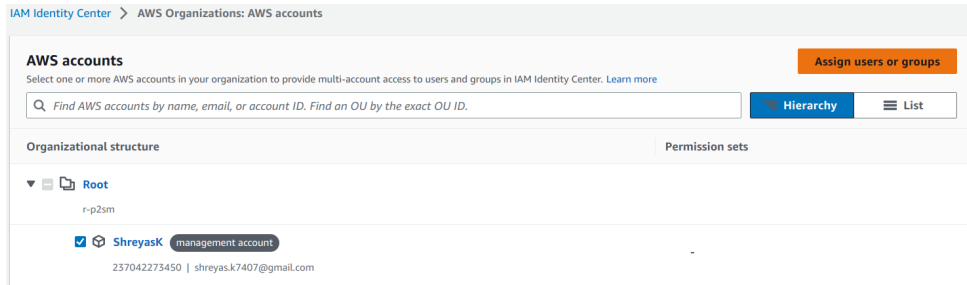
Maximum of 256 characters

Add users to group - optional (1/2)
Select workforce users to add to this group.

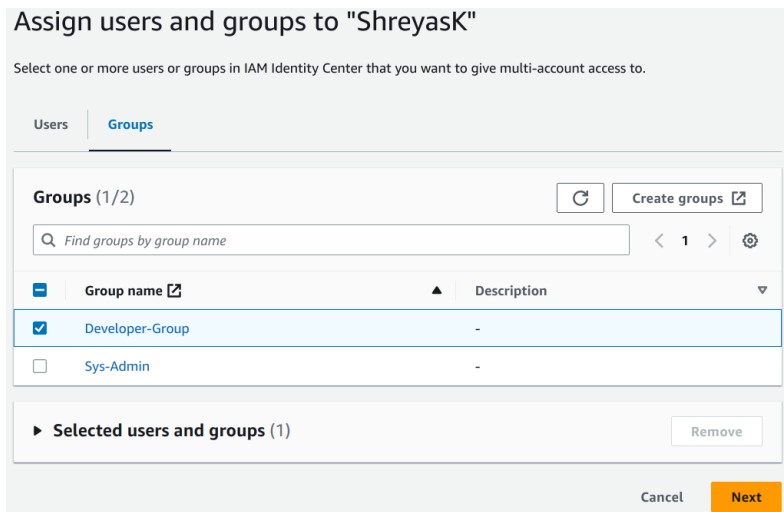
1

| <input type="checkbox"/> | Username | Display name | Status | MFA devices | Created by |
|-------------------------------------|-----------------|-----------------|---------|-------------|------------|
| <input type="checkbox"/> | Developer-User1 | Developer User1 | Enabled | None | Manual |
| <input checked="" type="checkbox"/> | Sys-Admin-User1 | SysAdmin User1 | Enabled | None | Manual |

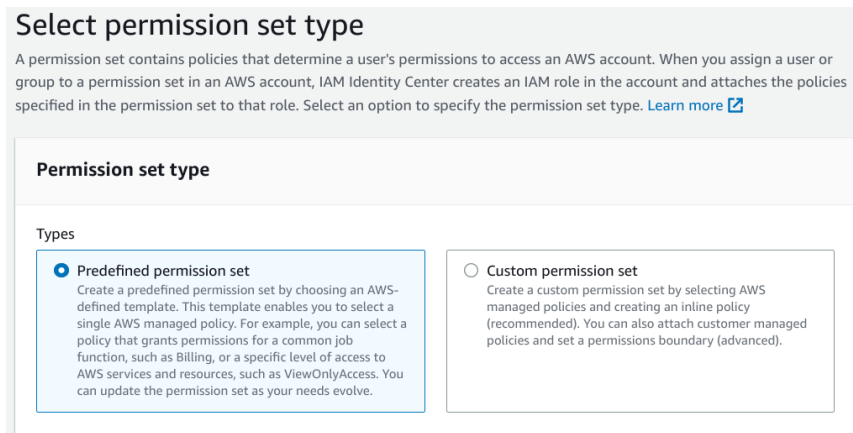
Step 7 - Assign groups to an AWS account in AWS organization. Here the “Developer-Group” and “Sys-Admin” groups are assigned to the management account of the AWS organization. The users inside these groups can perform only allowed permissions which are defined in their permission sets.



Click on “Assign users or groups”, then select the group you want to assign to the selected account.



Step 8 - Create a permission set which defines the permission allowed to users to perform in the account.



Select “PowerUserAccess” for the developer group.

The screenshot shows a list of AWS IAM policies. The "PowerUserAccess" policy is selected with a radio button. Below the list are "Cancel" and "Next" buttons.

- ☐ **DataScientist**
Grants permissions to AWS data analytics services.
- ☐ **NetworkAdministrator**
Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.
- ☒ **PowerUserAccess**
Provides full access to AWS services and resources, but does not allow management of Users and groups.
- ☐ **ReadOnlyAccess**
Provides read-only access to AWS services and resources.
- ☐ **SecurityAudit**
The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.
- ☐ **SupportUser**
This policy grants permissions to troubleshoot and resolve issues in an AWS account. This policy also enables the user to contact AWS support to create and manage cases.
- ☐ **SystemAdministrator**
Grants full access permissions necessary for resources required for application and development operations.
- ☐ **ViewOnlyAccess**
This policy grants permissions to view resources and basic metadata across all AWS services.

Cancel Next

Select the permission set and click on submit to successfully assign the developer group to the account.

Step 9 - Now assign the “Sys-Admin” group to the account.

The screenshot shows the "Assign users and groups to 'Shreyask'" page. The "Groups" tab is selected. A table lists the available groups, with "Sys-Admin" selected. Below the table, the "Selected users and groups (1)" section shows the assigned group. "Cancel" and "Next" buttons are at the bottom.

Assign users and groups to "Shreyask"

Select one or more users or groups in IAM Identity Center that you want to give multi-account access to.

Users Groups

Groups (1/2) Refresh Create groups

< 1 > Settings

| <input type="checkbox"/> | Group name | Description |
|-------------------------------------|-----------------|-------------|
| <input type="checkbox"/> | Developer-Group | - |
| <input checked="" type="checkbox"/> | Sys-Admin | - |

► Selected users and groups (1) Remove

Cancel Next

Create a permission set for the above group. Select “SystemAdministrator” and click next.

database services.

- ☐ **DataScientist**
Grants permissions to AWS data analytics services.
- ☐ **NetworkAdministrator**
Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.
- ☐ **PowerUserAccess**
Provides full access to AWS services and resources, but does not allow management of Users and groups.
- ☐ **ReadOnlyAccess**
Provides read-only access to AWS services and resources.
- ☐ **SecurityAudit**
The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.
- ☐ **SupportUser**
This policy grants permissions to troubleshoot and resolve issues in an AWS account. This policy also enables the user to contact AWS support to create and manage cases.
- ☒ **SystemAdministrator**
Grants full access permissions necessary for resources required for application and development operations.
- ☐ **ViewOnlyAccess**
This policy grants permissions to view resources and basic metadata across all AWS services.

Cancel Next

Select the permission set created. Click on next, review and submit to assign the group with the specific permission set to the account.

Assign permission sets to "Shreyask"

Permission sets define the level of access that users and groups in IAM Identity Center have to an AWS account. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users in IAM Identity Center with multiple permission sets on an AWS account must pick a specific permission set when selecting the account and then return to the AWS access portal to pick a different set when necessary. [Learn more](#)

Permission sets (1/2) ↻ 🔗 Create permission set

🔍 Find permission sets by name, ARN, or ID (i.e., ps-abcdefg123456789) < 1 > ⚙️

| Permission set 🔗 | Description | ARN |
|---|-------------|---|
| <input type="checkbox"/> PowerUserAccess | | arn:aws:sso::permissionSet/ssoins-6595a6acfb1449b/ps-d8e001318c85abc1 |
| <input checked="" type="checkbox"/> SystemAdministrator | | arn:aws:sso::permissionSet/ssoins-6595a6acfb1449b/ps-a5f2b222d667a0cb |

Cancel Previous Next

Review and submit assignments to "ShreyasK"

Step 1: Select users and groups Edit

Users and groups (1)

< 1 >

| Username / group name 🔗 | Type |
|---|-------|
| Sys-Admin | Group |

Step 2: Select permission sets Edit

Permission sets (1)

| Permission set | Description | ARN | Creation time |
|---------------------|-------------|--|---------------|
| SystemAdministrator | | arn:aws:sso:::permissionSet/ssoins-6595a6acfbcb1449b/ps-a5f2b222d667a0cb | Now |

Cancel Previous **Submit**

Step 10 - Sign-in to the new user created. Open the Access log-in link and enter the username.



Sign in

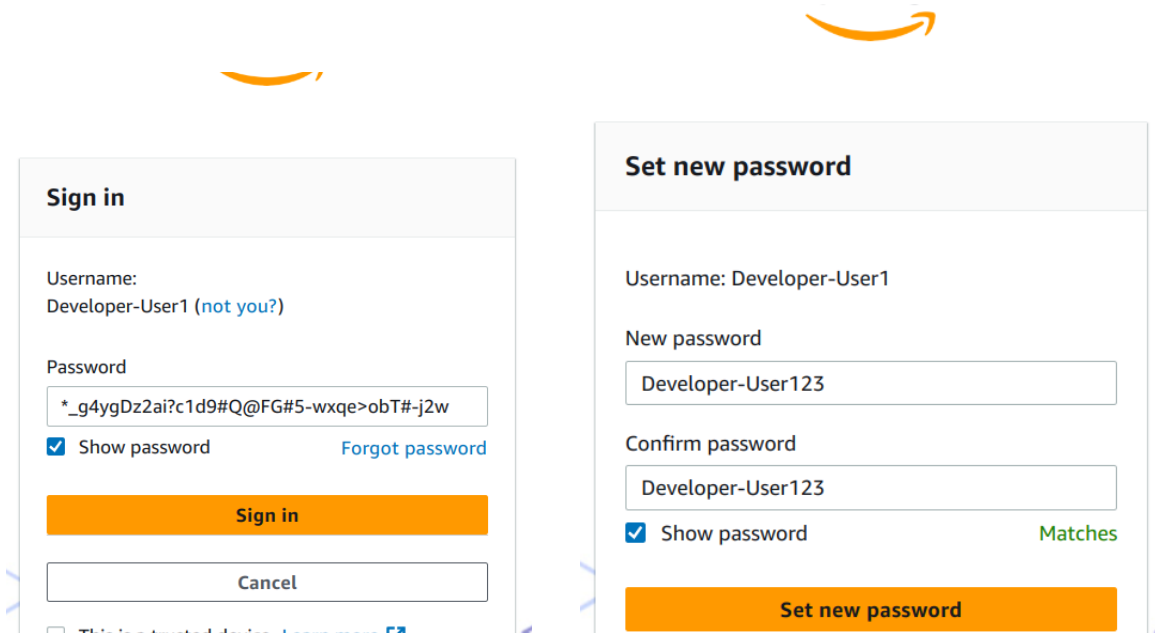
Username

Developer-User1

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

Enter the auto generated one time password for the user and create a new password.



The image displays two side-by-side screenshots of the AWS IAM console interface.

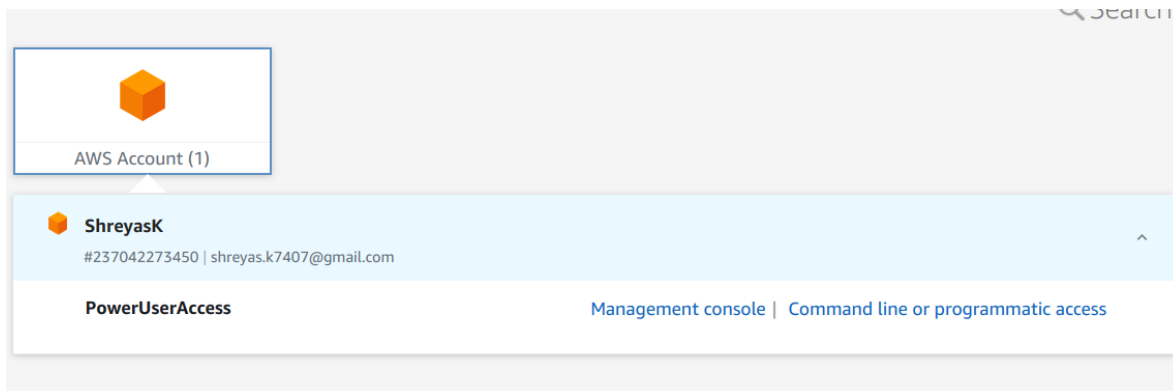
Left Screenshot: Sign in

- Username:** Developer-User1 (not you?)
- Password:** *_g4ygDz2ai?c1d9#Q@FG#5-wxqe>obT#-j2w
- ☒ Show password [Forgot password](#)
- Sign in** (orange button)
- Cancel** (white button)
- ☐ This is a trusted device [Learn more](#)

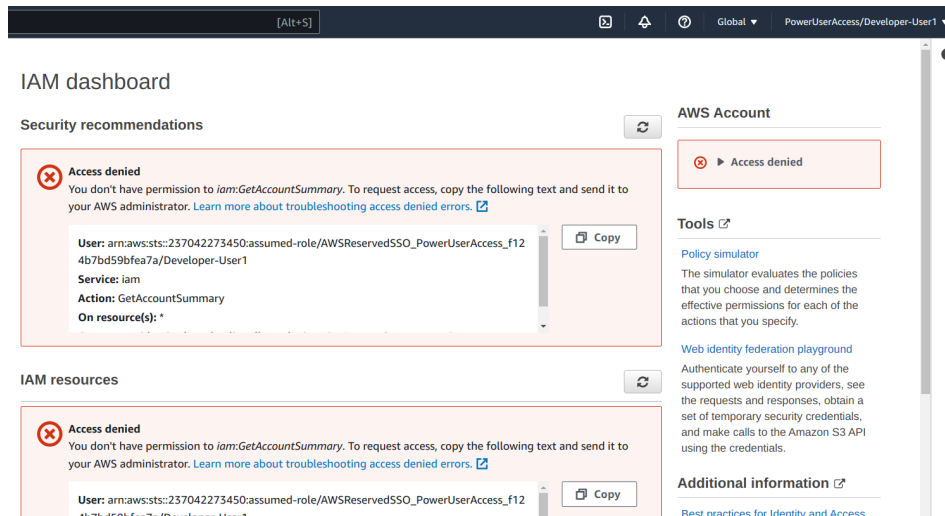
Right Screenshot: Set new password

- Username:** Developer-User1
- New password:** Developer-User123
- Confirm password:** Developer-User123
- ☒ Show password **Matches**
- Set new password** (orange button)

Click on “management console” for the Role “PowerUserAccess”. To open the AWS management console and perform only the allowed actions.



It is visible that the “PowerUserAccess” can not perform actions related to IAM.



Step 11 - Login to the “Sys-Admin” user and create a new password. Open the AWS management console.

