

Phase5-15 Create an IAM User

This section will guide you to:

- Create an IAM user
- Validate the newly created IAM user

Selecting the IAM from the AWS console

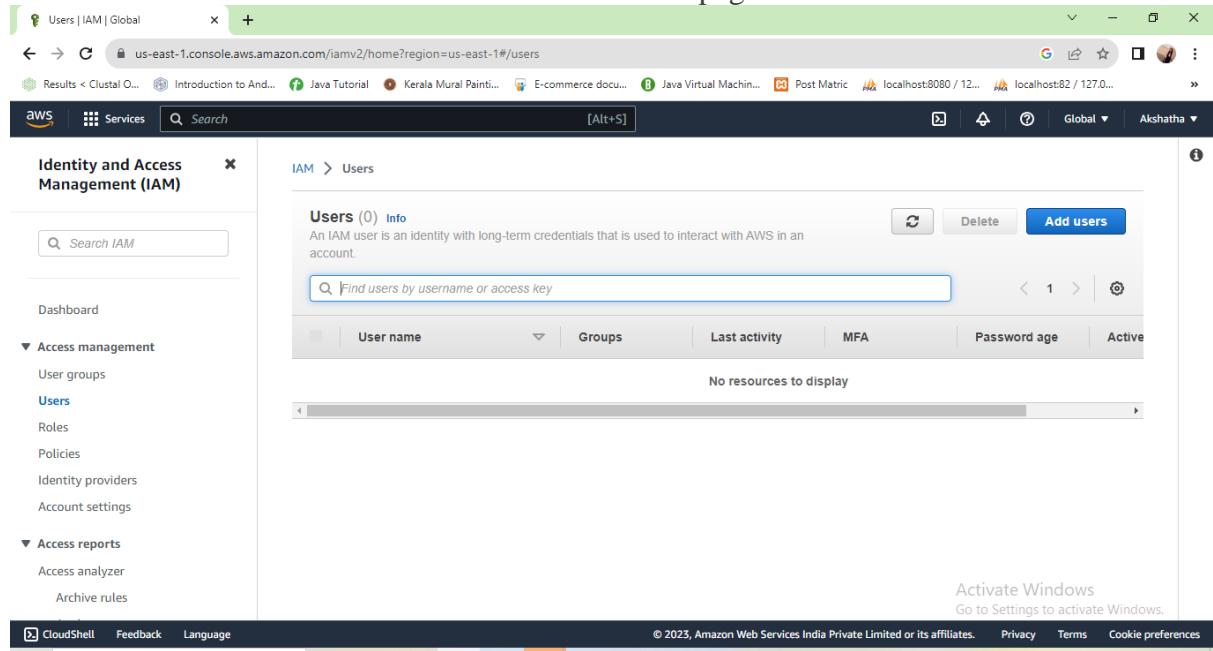
- Login to your AWS console and search for IAM

The image shows two screenshots of the AWS Management Console.

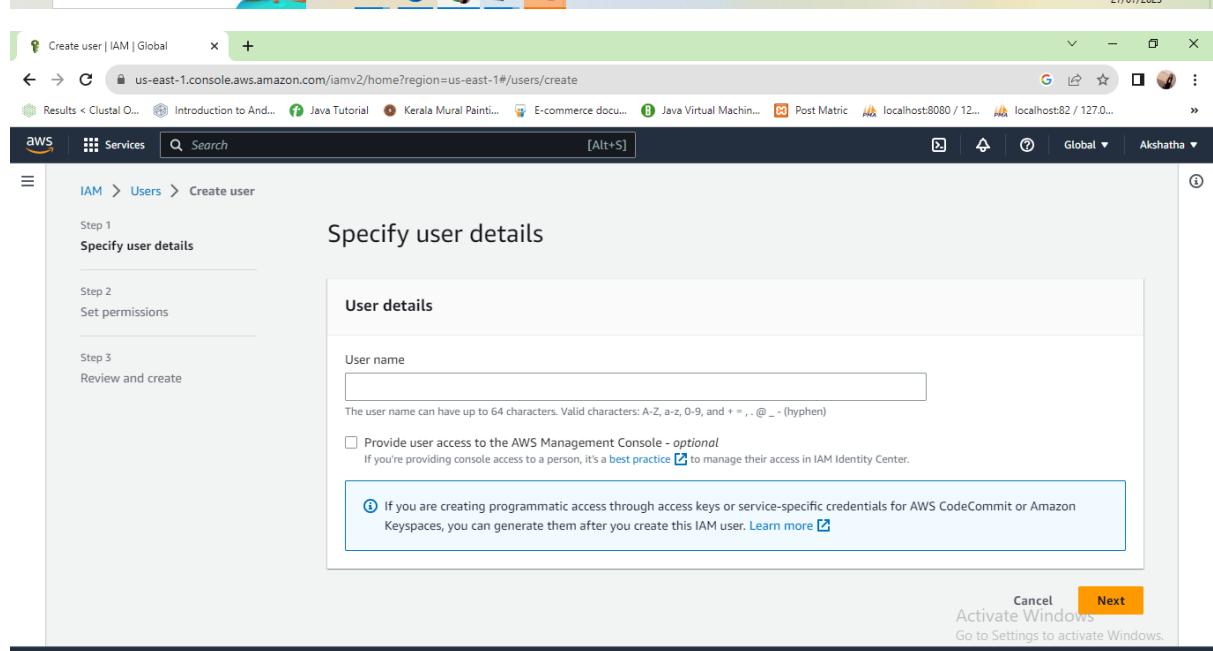
The top screenshot displays the search results for 'iam'. The search bar at the top has 'iam' typed into it. Below the search bar, there is a sidebar titled 'Services (9)' containing links like 'Features (20)', 'Resources New', 'Blogs (1,595)', 'Documentation (46,850)', 'Knowledge Articles (20)', 'Tutorials (2)', 'Events (12)', and 'Marketplace (546)'. The main content area shows 'Search results for 'iam'' and a list of services: 'IAM' (Manage access to AWS resources), 'IAM Identity Center (successor to AWS Single Sign-On)' (Manage workforce user access to multiple AWS accounts and cloud applications), 'Resource Access Manager' (Share AWS resources with other accounts or AWS Organizations), and 'Serverless Application Repository' (Assemble, deploy, and share serverless applications within teams or publicly). A tooltip 'upload files bucket where' is visible on the right.

The bottom screenshot shows the 'IAM dashboard'. The left sidebar has 'Identity and Access Management (IAM)' selected. It includes sections for 'Dashboard', 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), and 'Access reports' (Access analyzer, Archive rules). The main dashboard area has a heading 'IAM dashboard' and a 'Security recommendations' section with a red warning icon for '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) and a green checkmark for 'Root user has no active access keys' (Using access keys attached to an IAM user instead of the root user improves security). Below this is an 'IAM resources' section with tables for User groups (0), Users (0), Roles (2), Policies (0), and Identity providers (0). A 'What's new' section indicates 'Updates for features in IAM' with a 'View all' link. The right sidebar contains 'AWS Account' information (Account ID: 065338297267, Account Alias: 065338297267 Create, Sign-in URL: https://065338297267.sigin.aws.amazon.com/console) and 'Quick Links' (My security credentials, Manage your access keys, multi-factor authentication (MFA) and other credentials, Activate Windows, Tools to activate Windows).

- Click on Users to redirect to the user creation page to create IAM users



The screenshot shows the AWS IAM service interface. On the left, there's a navigation pane with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'Users' is also selected. The main content area is titled 'Users (0) Info' and contains a message: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' Below this is a search bar labeled 'Find users by username or access key'. A table header row includes columns for 'User name', 'Groups', 'Last activity', 'MFA', 'Password age', and 'Active'. A message 'No resources to display' is centered below the table. At the top right of the main area are 'Delete' and 'Add users' buttons.



The screenshot shows the 'Create user' wizard. The title is 'Specify user details'. It's step 1 of 3. The left sidebar shows 'Step 1: Specify user details', 'Step 2: Set permissions', and 'Step 3: Review and create'. The main area has a section titled 'User details' with a 'User name' input field. Below it, a note says: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, . @ _ - (hyphen)'. There's an optional checkbox for 'Provide user access to the AWS Management Console'. A callout box provides information about generating programmatic access keys. At the bottom are 'Cancel', 'Next', and 'Activate Windows' buttons.

Create user | IAM | Global

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/create

Results < Clustal O... Introduction to And... Java Tutorial Kerala Mural Painti... E-commerce docu... Java Virtual Machin... Post Metric localhost:8080 / 12... localhost:82 / 127.0...

Services Search [Alt+S]

IAM > Users > Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

User details

User name: akshi

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](#).

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

Activate Windows
Go to Settings to activate Windows.

Create user | IAM | Global

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/create

Results < Clustal O... Introduction to And... Java Tutorial Kerala Mural Painti... E-commerce docu... Java Virtual Machin... Post Metric localhost:8080 / 12... localhost:82 / 127.0...

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:29 27/07/2023

Services Search [Alt+S]

Review and create

Step 4 Retrieve password

User name: akshi

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.

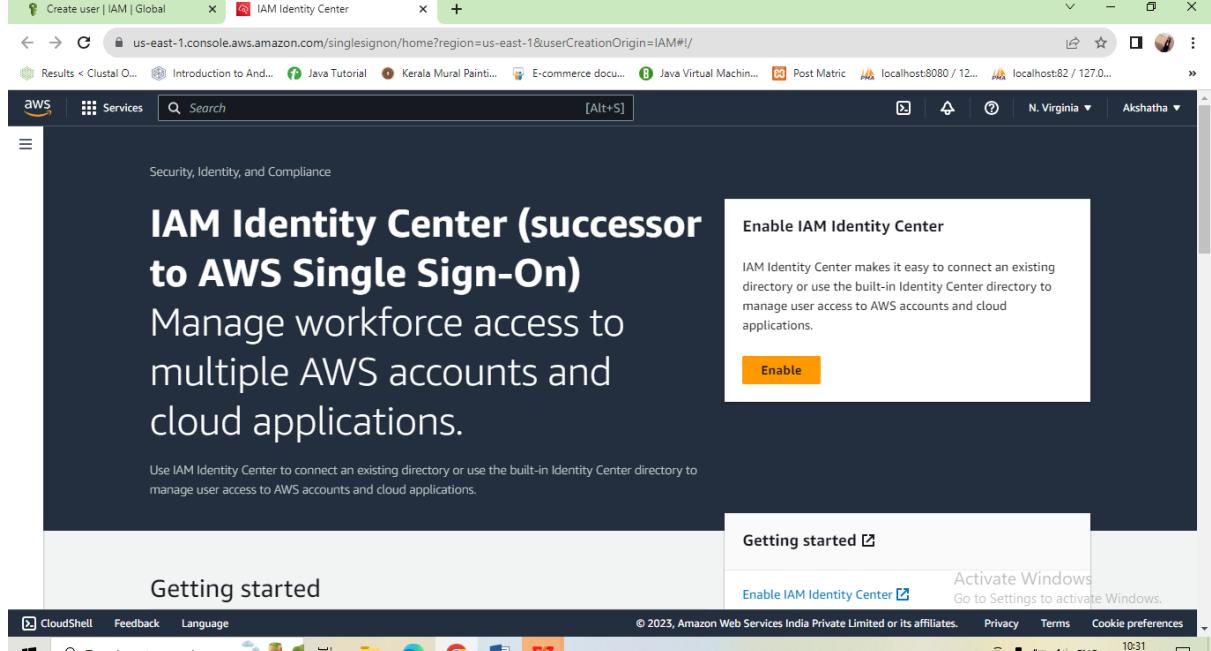
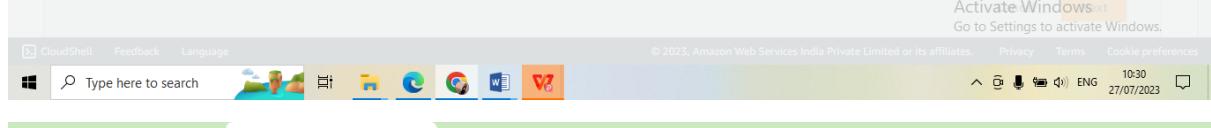
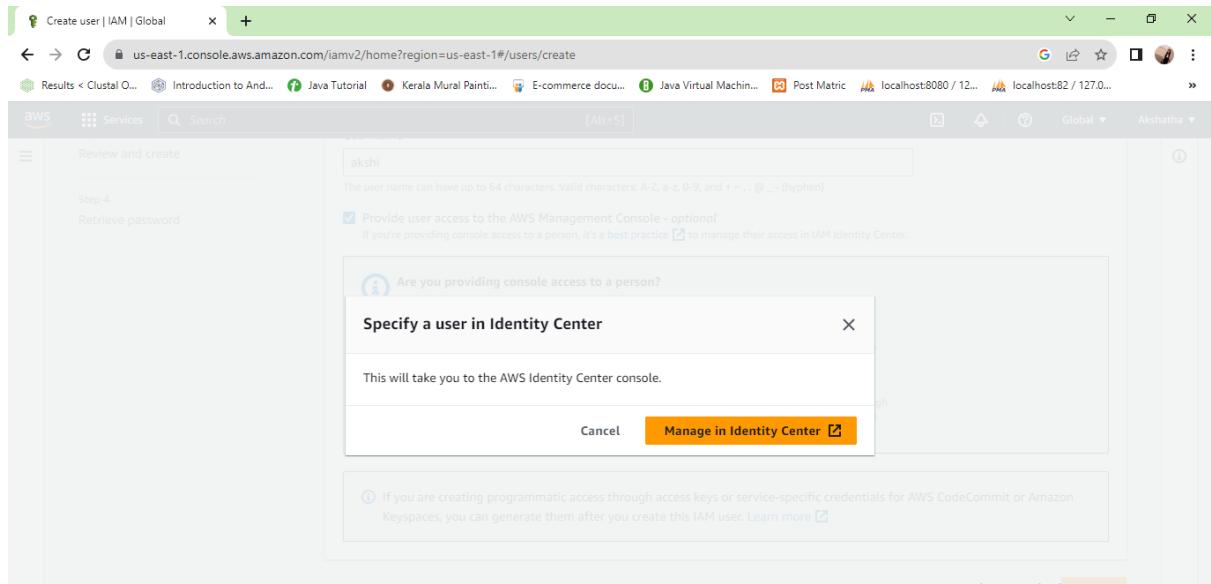
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Activate window
Go to Settings to activate Windows.

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:30 27/07/2023



Screenshot of the AWS IAM Identity Center - Add user wizard showing the "Specify user details" step.

Step 1: Specify user details

Primary information

Username: akshath (Entered)

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

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: abc@gmail.com

Confirm email address: abc@gmail.com

Contact methods - optional

Optional contact methods for this user. These methods are used for password reset requests and other notifications.

Activate Windows
Go to Settings to activate Windows.

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback Language Type here to search 10:35 27/07/2023

CloudShell Feedback Language Type here to search 10:35 27/07/2023

CloudShell Feedback Language Type here to search 10:35 27/07/2023

- Either we can add user to the created group or we can add policy as shown below:

Screenshot of the AWS IAM Identity Center - Add user wizard showing the "Attach permissions policies - Optional" step. The user group "Akshatha" has been created and is being assigned policies.

Attach permissions policies - *Optional* (Selected 1/865)

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

Filter policies by property or policy name and press enter.

Policy name	Type	Description
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	Provides full access to AWS services a...
<input type="checkbox"/> PowerUserAccess	AWS managed - job function	Provides full access to AWS services a...
<input type="checkbox"/> ReadOnlyAccess	AWS managed - job function	Provides read-only access to AWS serv...
<input type="checkbox"/> AWSCloudFormationReadOnlyAccess	AWS managed	Provides access to AWS CloudFormati...
<input type="checkbox"/> CloudFrontFullAccess	AWS managed	Provides full access to the CloudFront ...
<input type="checkbox"/> AWSCloudHSMFullAccess	AWS managed	Provides full access to all CloudHSM re...
<input type="checkbox"/> AWSCloudHSMReadOnlyAccess	AWS managed	Provides read-only access to all Cloud...

Next Step **Create policy**

CloudShell Feedback Language Type here to search © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:49 27/07/2023

Screenshot of the AWS IAM Identity Center - Add user wizard showing the "Add user to groups - optional" step. The user "Akshatha" is being assigned to groups.

Add user to groups - *optional*

You can assign this user to one or more groups.

Groups (0)

Create group

Find groups by group name

No groups found

Create group

Cancel Previous Next

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback Language Type here to search © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

10:36 27/07/2023

Create group

Group details

Group name: devs
Maximum of 128 characters

Description - optional:
Group description detailing the permissions assigned to this group.
developers
Maximum of 256 characters

Add users to group - optional (0)
Select workforce users to add to this group.

IAM Identity Center - Groups

Groups (1)

Group name	Description	Created by
devs	developers	Manual

In case a user needs to add a policy first, then he or she needs to search and then add policy to the user

The screenshot shows the AWS Resource Groups console with the URL <https://us-east-1.console.aws.amazon.com/resource-groups/groups/new?region=us-east-1>. The page title is "Create query-based group". On the left, there's a sidebar with "AWS Resource Groups" navigation, including "Create Resource Group", "Saved Resource Groups", "Settings", "Tagging", "Tag Editor", "Tag Policies", and "What's new". The main content area has two tabs: "Group type" (selected) and "CloudFormation stack based". Under "Group type", it says "Select a group type to define a group based on resource types and tags, or create a group based on your existing CloudFormation stack." The "Tag based" option is selected, with the sub-instruction "Group resources by specifying tags that are shared by the resources." The "CloudFormation stack based" option is also present with its description. Below this, the "Grouping criteria" section is shown, with the instruction "Define a group based on resource types and tags." It includes a "Resource types" dropdown set to "Select resource types" and a "All supported resource types" button. A watermark for "Activate Windows" is visible on the right.

This screenshot is from the same session, showing the "Grouping criteria" configuration step. The URL is the same: <https://us-east-1.console.aws.amazon.com/resource-groups/groups/new?region=us-east-1>. The "Grouping criteria" section is expanded, showing the "Resource types" dropdown set to "Select resource types" and the "Tags" section where "AWS::ACMPCA::CertificateAuthority" is listed in the dropdown. A search bar contains "lab" and a tag named "sl" is selected. There's a "Preview group resources" button. The "Group resources" section below is partially visible. The watermark for "Activate Windows" is still present.

The screenshot shows the AWS Resource Groups console. On the left, a sidebar has sections for Resources (Create Resource Group, Saved Resource Groups, Settings) and Tagging (Tag Editor, Tag Policies). The main area is titled 'AWS Resource Groups' and shows a table with one row labeled 'No resources.' A 'Group details' section contains fields for 'Group name' (set to 'deves') and 'Group description - optional' (with placeholder 'Type a description'). Below this is a section for 'Group tags - optional'. At the bottom right are 'Cancel' and 'Create group' buttons.

- Finally, it will create a user with a group or an added policy

The screenshot shows the AWS Resource Groups console after the group 'deves' was created. A green success message at the top states: 'The resource group "deves" has been successfully created in the current region (us-east-1)'. The main area displays the 'Group details' for 'deves', including the group name, ARN, and type (Tag based). The sidebar remains the same as in the previous screenshot. The status bar at the bottom indicates the date and time as 27/07/2023 10:44.

The screenshot shows the AWS Resource Groups console interface. On the left, a sidebar menu includes 'Create Resource Group', 'Saved Resource Groups', 'Settings', 'Tag Editor', and 'Tag Policies'. The main area is titled 'AWS Resource Groups' and shows a search bar with the ARN 'arn:aws:resource-groups:us-east-1:065338297267:group/deves'. Below this, the 'Group type and grouping criteria' section is displayed, with 'Group type' set to 'Tag based' and 'Resource types' set to 'AWS::ACMPCA::CertificateAuthority'. A tag 'lab: sl' is also listed. The 'Group resources' section shows a table with one row, which is currently empty. The table has columns for Identifier, Tag: Name, Service, Type, Region, and Tags. The status bar at the bottom indicates the date as 27/07/2023.

Group ARN
arn:aws:resource-groups:us-east-1:065338297267:group/deves

Group type and grouping criteria

Group type: Tag based

Resource types: AWS::ACMPCA::CertificateAuthority

Tags: lab: sl

Group resources

Filter resources

Export to CSV

CloudShell Feedback Language

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Activate Windows Go to Settings to activate Windows.

CloudShell Feedback Language

Type here to search

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Activate Windows Go to Settings to activate Windows.

Screenshot of the AWS IAM Identity Center - Add user page showing the 'Set permissions' step.

The 'Permissions options' section contains three choices:

- 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.

The 'User groups (1)' section shows a table with one item:

Group name	Users	Attached policies	Created
developers	0	AdministratorAccess	2023-07-27 (2 minutes ago)

Screenshot of the AWS IAM Identity Center - Add user page showing the 'Review and create' step.

The 'User details' section shows the following information:

User name	Console password type	Require password reset
akshu1	None	No

The 'Permissions summary' section shows the following information:

Name	Type	Used as
developers	Group	Permissions group

The 'Tags - optional' section indicates that tags are key-value pairs used to identify, organize, or search for resources.

The screenshot shows the AWS IAM Identity Center - Add user page. The user is being created with the following details:

User name	Console password type	Require password reset
akshu1	None	No

Permissions summary:

Name	Type	Used as
developers	Group	Permissions group

Tags - optional:

Key	Value - optional
ec2admin	ec2

IAM > Users

Ready to streamline human access to AWS and cloud apps?

Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.

[Learn more](#) | [Watch how it works](#)

Users (1) Info

User name	Groups	Last activity	MFA	Password a...	Action
akshu1	developers	None	None	None	Edit

Activate Windows
Go to Settings to activate Windows

The screenshot shows the AWS IAM User Details page for a user named 'akshu1'. The top navigation bar includes tabs for 'Create user | IAM | Global', 'IAM Identity Center - Users', 'Create user | IAM | Global', 'IAM Identity Center - Add user', and 'akshu1 | IAM | Global'. The main content area displays the 'Summary' tab for 'akshu1'. Key details shown include:

ARN	Console access	Access key 1
arn:aws:iam::065338297267:user/akshu1	Disabled	Not enabled

Below the summary, there are tabs for 'Permissions', 'Groups (1)', 'Tags (1)', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is selected, showing one policy attached: 'Permissions policies (1)'. A note states: 'Permissions are defined by policies attached to the user directly or through groups.' There is a 'Remove' button and a 'Add permissions' button.

The screenshot shows the AWS IAM User Groups Membership page for the same user 'akshu1'. The top navigation bar is identical to the previous screenshot. The main content area displays the 'Summary' tab for 'akshu1'. Below it, the 'Groups' tab is selected, showing one group attached: 'User groups membership (1)'. A note states: 'A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.' A table lists the group 'developers' with the policy 'AdministratorAccess' attached. There are buttons for 'Remove' and 'Add user to groups'.

The screenshot shows the AWS IAM Identity Center interface. The top navigation bar has tabs for 'Create user | IAM | Global', 'IAM Identity Center - Users', 'Create user | IAM | Global', 'IAM Identity Center - Add user', and 'akshu1 | IAM | Global'. The main content area is titled 'Identity and Access Management (IAM)'. On the left, a sidebar lists 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access analyzer, Archive rules), and a search bar. The right side shows the 'Security credentials' tab selected. It contains sections for 'Console sign-in' (Console sign-in link: https://065338297267.signin.aws.amazon.com/console, Console password: Not enabled, with an 'Enable console access' button) and 'Multi-factor authentication (MFA) (0)' (with 'Assign MFA device' and 'Remove' buttons). A large 'Assign MFA device' button is centered at the bottom. The status bar at the bottom indicates '© 2023, Amazon Web Services India Private Limited or its affiliates.' and shows system icons like battery level, signal strength, and network.

This screenshot shows the 'Access Advisor' tab for the same user 'akshu1'. The top navigation bar and sidebar are identical. The main content area shows the 'Summary' section for 'akshu1' (Info button, Delete button). Below it is a table with three columns: ARN (arn:aws:iam::065338297267:user/akshu1), Console access (Disabled, Not enabled), and Access key 1 (Access key 2, Not enabled). At the bottom, there's a note about the Access Advisor showing services accessible by the user and their last access times, with a 'Learn More' link. The status bar at the bottom indicates '© 2023, Amazon Web Services India Private Limited or its affiliates.' and shows system icons.