



IAM IDENTITY CENTER

AWS IAM Identity Center is the recommended AWS service for managing human user access to AWS resources. It is a single place where you can assign your workforce users, also known as workforce identities, consistent access to multiple AWS accounts and applications.

With IAM Identity Center, you can create or connect workforce users and centrally manage their access across all their AWS accounts and applications. You can use multi-account permissions to assign your workforce users access to AWS accounts. You can use application assignments to assign your users access to AWS managed and customer managed applications.



IAM Identity Center capabilities

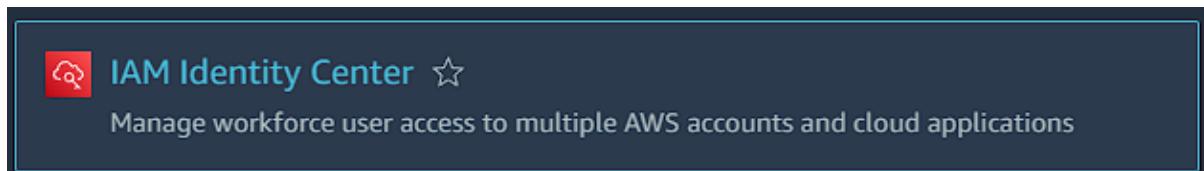
IAM Identity Center includes the following core capabilities and features:

1. **Manage workforce identities:** Human users who build or operate workloads in AWS are also known as workforce users, or workforce identities. Workforce users are employees or contractors who you allow to access AWS accounts in your organization and internal business applications. These individuals might be developers who build your internal and customer-facing systems, or users of internal database systems and applications. You can create workforce users and groups in IAM Identity Center, or connect and synchronize to an existing set of users and groups in your own identity source for use across all your AWS accounts and applications. For more information, see [Manage your identity source](#).
2. **Manage instances of IAM Identity Center:** IAM Identity Center supports two types of instances: organization instances and account instances. An organization instance is the best practice. It's the only instance that enables you to manage access to AWS accounts and it's recommended for all production use of applications. An organization instance is deployed in the AWS Organizations management account and gives you a single point from which to manage user access across the AWS environment. Account instances are bound to the AWS account in which they are enabled. Use account instances of IAM Identity Center only to support isolated deployments of select AWS managed applications. For more information, see [Manage organization and account instances of IAM Identity Center](#).
3. **Manage access to multiple AWS accounts:** With multi-account permissions, you can plan for and centrally implement permissions across multiple AWS accounts at one time without needing to configure each of your accounts manually. You can create permissions based on common job functions or define custom permissions that meet your security needs. You can then assign those permissions to workforce users to control their access over specific accounts. This optional feature is available only for organization instances. If you're using per-account IAM role management in your environment, both systems can coexist. If you want to try multi-account permissions, you can start by implementing this system on a limited basis and migrate more of your environment to use this system over time.

4. **Manage access to applications:** IAM Identity Center enables you to simplify application access management. With IAM Identity Center, you can grant your workforce users in IAM Identity Center single sign-on access to applications.
5. **AWS managed applications:** AWS provides applications such as Amazon Redshift, Amazon Managed Grafana, and Amazon Monitron, that integrate with IAM Identity Center. These applications can use IAM Identity Center for authentication, directory services, and trusted identity propagation. Your users benefit from a consistent single sign-on experience, and because the applications share a common view of users, groups, and group membership, users also have a consistent experience when sharing application resources with others. You can configure AWS managed applications to work with IAM Identity Center directly from within the relevant application consoles or through the APIs.
6. **Customer managed applications:** You can grant your workforce users in IAM Identity Center single sign-on access to applications that support identity federation with SAML 2.0. Many commonly used SAML 2.0 applications, such as Salesforce and Microsoft 365, work with IAM Identity Center and are available in the application catalog in the IAM Identity Center console. This is an optional feature that can be helpful if you use such applications and you create your users and groups in IAM Identity Center, or you use Microsoft Active Directory Domain Service as your identity source.
7. **Trusted identity propagation across applications:** Trusted identity propagation provides a streamlined single sign-on experience for users of query tools and business intelligence (BI) applications who require access to data in AWS services. Data access management is based on a user's identity, so administrators can grant access based on users' existing user and group memberships. User access to AWS services and other events is recorded in service-specific logs and in CloudTrail events, so that auditors know what actions the users took and which resources the users accessed.
8. **AWS access portal access for your users:** The AWS access portal is a simple web portal that provides your users with seamless access to all their assigned AWS accounts and applications.

😊 TO BEGIN WITH THE LAB

1. Login to AWS Console then search for IAM identity center. Choose this service accordingly.



2. Then you need to enable your IAM identity center.
3. So, to create IAM identity center you will need an AWS organization account in place.

4. Go and create your AWS Organization. It is just simple to create it. Just click on create AWS Organization. And it will create it by itself.

The screenshot shows the IAM Identity Center dashboard. At the top right, there is a callout box with the title "Enable IAM Identity Center". Inside the box, text explains that IAM Identity Center makes it easy to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications. Below this text is an orange "Enable" button. A cursor arrow points towards the "Enable" button. At the bottom of the dashboard, there is a "Getting started" button.

Enable IAM Identity Center



IAM Identity Center requires AWS Organizations

We detected that your AWS account does not currently use this service.

After you create an organization, you cannot join this account to another organization until you delete its current organization.

AWS Organizations provides the following benefits:

1. Enables single payer and centralized cost tracking
2. Lets you create and invite other AWS accounts
3. Allows you to apply policy-based controls
4. Helps you simplify organization-wide management of AWS services



Would you like us to create an AWS organization for you now?

We will also enable IAM Identity Center as part of this process.

Cancel

Create AWS organization

5. This is the dashboard for IAM identity center.

IAM Identity Center

Dashboard

AWS IAM Identity Center is the updated console for the features of AWS Single Sign-On (AWS SSO). The features that comprised AWS Single Sign-On (AWS SSO) are available through the IAM Identity Center console. They offer a better way to connect or create a workforce directory, and to manage users' access across AWS accounts and integrated applications. [Learn more](#)

Recommended setup steps

Step 1
Choose your identity source
The identity source is where you administer users and groups, and is the service that authenticates your users.

Step 2
Manage access to multiple AWS accounts
Give users and groups access to specific AWS accounts in your organization.

Settings summary

Go to settings

Identity source: Identity Center directory

Region: Asia Pacific (Mumbai) | ap-south-1

AWS access portal URL: <https://d-9f671ebb97.awsapps.com/start>

6. Now you can go into users and start adding users.
7. So, basically this service is different from IAM, the user you define in IAM cannot be seen here and the user you create in Identity center will not be a part of IAM itself.

IAM Identity Center

Users

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. [Learn more](#)

Users (0)

No users found

Add user

8. If in another tab you will go to AWS Organization, you will see that it has gone ahead and created an AWS organization account for you.

AWS Organizations

AWS accounts

Invitations

Services

Policies

Settings [New](#)

Get started

Organization ID
o-x0717tivat

AWS accounts

Add an AWS account

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Actions ▾

Search by name, email, account ID or OU ID.

Hierarchy List

Organizational structure

Account created/joined date

Root

r-de5y

4000 management account

678586570493 | 4000@gmail.com

Joined 2023/08/21

9. Now go back to Identity center and start adding users. Click on add users.
10. Now in the first step, you will need to give a user name and an email address to verify things for identity center.

Specify user details

Step 2 - optional

Add user to groups

Step 3

Review and add 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.

appteam10

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

appteam10@gmail.com

Confirm email address

appteam10@gmail.com

First name

Enter first name

11. Choose **to generate a one-time password** then give first name and last name. And it will show you the display name.

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

Email address

appteam10@gmail.com

Confirm email address

appteam10@gmail.com

First name

app

Last name

team10



Display name

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

app team10

12. You will also see that you can add more relevant information to it.
13. But for now, just click on next.
14. Then skip step as it is not needed right now. Then review your user and add user to the identity center.

► Contact methods - *optional*

► Job-related information - *optional*



► Address - *optional*

► Preferences - *optional*

► Additional attributes - *optional*

Cancel

Next

15. Then it will give you an AWS access portal URL, with username and the one-time password.

One-time password

X

 User password was reset for user "appteam10".

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 only time you can view and copy this password.

AWS access portal URL

 Copy

Username

 appteam10



One-time password

 *****

 Show password

 Close

16. Now in the other browser you should put that URL and open it.
17. Now give your username here.
18. Then click on next.



Sign in

Username

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.

19. Now put the password which was generated.
20. Once you've entered the one-time password, it will ask you to create your own password.



Sign in

Username:
appteam10 (not you?)

Password

Show password

[Forgot password](#)

Sign in

Cancel

This is a trusted device. [Learn more](#)



Set new password

Username: appteam10

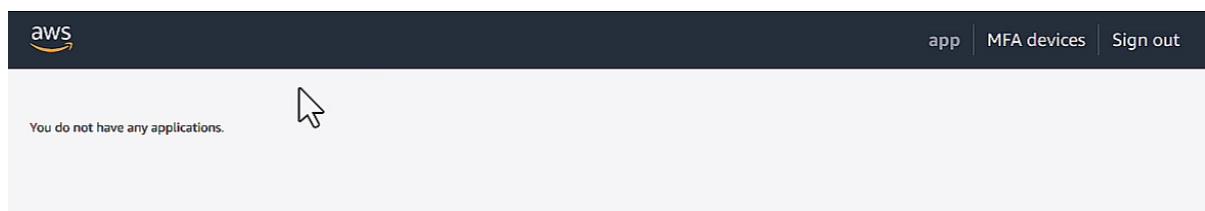
New password

Confirm password

Show password

Set new password

21. Once you have created your own password, then you will see that a blank has been open saying that you do not have any application.



22. Now you are going to give access to this user of your S3 buckets that you have in your root account.
23. For that you need to click on Permission sets.
24. Then you need click on create permission set.

▼ Multi-account permissions

AWS accounts

Permission sets

The screenshot shows the 'Permission sets' section of the AWS IAM Identity Center console. At the top, there is a heading 'Permission sets (0)' with a note about permission sets defining access levels. Below this are buttons for 'Create permission set' (which is highlighted with a red box), 'Delete', and a refresh icon. A search bar contains the placeholder text 'Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789)'. To the right of the search bar are navigation icons for back, forward, and refresh. A table header row includes columns for 'Permission set', 'Description', and 'ARN'. Below the table, a message says 'No matches' and 'No valid ARN or permission set id provided.' A 'Clear filter' button is located at the bottom of the table area.

25. Now you will have two options for permission set type. But here you are going to choose Custom permission set.
26. Then click on next.

The screenshot shows the 'Permission set type' configuration page. It has a title 'Permission set type' and a section 'Types'. Two options are shown: 'Predefined permission set' and 'Custom permission set'. The 'Custom permission set' option is selected (indicated by a blue circle with a dot) and highlighted with a blue border. A cursor arrow points towards the 'Custom permission set' box. At the bottom right are 'Cancel' and 'Next' buttons.

27. On the next page you can choose from your existing IAM policies that you created for S3. For that go back to IAM then go to your policy which you want to choose copy its name. Then come back to permission set.
28. Then you from customer managed policies you need to click on Attach policies.

▼ Customer managed policies (not set)

Customer managed policies are standalone policies that you create and manage in your AWS accounts to define custom permissions. You can attach up to 10 managed policies (AWS managed policies and customer managed policies) to your permission set by specifying the names of the policies exactly as they appear in your accounts. Customer managed policies are intended for advanced use cases. To ensure that you understand your shared security responsibility and best practices for configuring these policies, review the IAM Identity Center documentation. [Learn more](#)

No customer managed policies attached

Attach policies

29. Then you need to give policy name.

Policy names

To attach a customer managed policy to your permission set, you must specify the policy name exactly as it appears in the IAM console. To find the policy name, sign in to the [IAM console](#) using the same AWS account as your permission set. If your permission set will be provisioned in multiple AWS accounts, a policy with the same name must exist in each account.

S3_BucketAccess

Attach more



30. Then just click on next and move to give your permission set a name. Then move to review page and create your permission set.

31. So, you will have a permission set in place. But if you will scroll you permission set to right then you will see that it is not provisioned. So, you need to assign this permission set to a user.

Permission sets (1)

Permission sets define the level of access that users in IAM Identity Center have to their assigned AWS accounts. The names of permission sets appear as available roles in the AWS access portal. Users who are assigned to multiple AWS permission sets can sign in to the AWS access portal, choose an account, and then choose a role that AWS created from an assigned permission set. [Learn more](#)



Delete

Create permission set



Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789).



1



Permission set	Description	ARN
○ Permission_S3BucketA...	-	arn:aws:sso:::permissionSet/ssoins-6595680e835e32a4/ps-36a773...

ARN	Provisioned status	Creation t...
arn:aws:sso:::permissionSet/ssoins-6595680e835e32a4/ps-36a77303e45...	Not provisioned	N

32. Now click on AWS Accounts.

33. Then you need to choose your management account and click on Assign users or groups.

▼ Multi-account permissions

AWS accounts

Permission sets

IAM Identity Center > AWS Organizations: AWS accounts

AWS accounts
Select one or more AWS accounts in your organization to provide multi-account access to users and groups in IAM Identity Center. [Learn more](#)

Assign users or groups

Search by name, email, account ID or OU ID.

Hierarchy List

Organizational structure

Root
r-de5y

management account
678586570493 | [REDACTED]@gmail.com

34. Now select your user and click on next.

Assign users and groups to [REDACTED]

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

Users Groups

Users (1)

Username Find users in IAM Identity Center by username or display name

Username	Display name	Status
appteam10	app team10	Enabled

Selected users and groups (0)

Remove

Cancel Next

35. Then select your permission and assign it to the user.

Assign permission sets to [REDACTED]

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](#)

The screenshot shows a table titled 'Permission sets (1/1)'. The table has columns: 'Permission set' (with a checkbox), 'Description', and 'ARN'. There is one row visible, representing the permission set 'Permission_S3BucketAccess' with the ARN: arn:aws:ssos:::permissionSet/ssoinset-6595680e835e32a4/ps-36a77303e4564a11.

Permission set	Description	ARN
Permission_S3BucketAccess		arn:aws:ssos:::permissionSet/ssoinset-6595680e835e32a4/ps-36a77303e4564a11

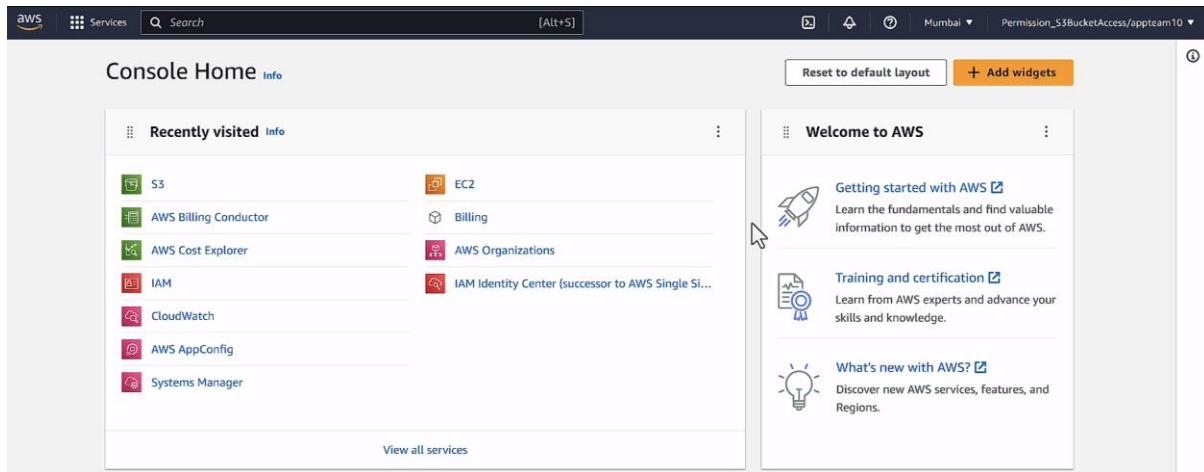
36. After you will go to your permission set you will see that it has been provisioned now.
37. Now if you go back to the user in another browser where you logged in with it and refresh the page.
38. You will see that an AWS account is attached to it now.

The screenshot shows a user profile with an attached AWS account. The account is represented by an orange cube icon and labeled 'AWS Account (1)'.

39. Now you will see that you have your primary account in place with the user.
40. Now you have to click on Management console.

The screenshot shows the user's management console access. It displays the user's name, ID, and email, along with the permission set 'Permission_S3BucketAccess' and access options 'Management console | Command line or programmatic access'.

41. There you will see that you have your management console in place.
42. Now if you will click on S3 and navigate to it.



43. You will your buckets in place.

44. And based on the policy of your choice you can access the buckets.

The screenshot shows the Amazon S3 'Buckets' list. It displays two buckets: 'appbucket8000' and 'appbucket9000'. Both buckets are located in the 'Asia Pacific (Mumbai) ap-south-1' region. The 'Access' column for both buckets shows a red 'Insufficient permissions' message with a crossed-out key icon. The 'Creation date' column shows 'August 20, 2023, 18:06:22 (UTC+04:00)' for the first bucket and 'August 20, 2023, 18:07:17 (UTC+04:00)' for the second. The top right of the screen has a 'View Storage Lens dashboard' button. The top navigation bar includes the AWS logo, a search bar, and account information for 'Amazon S3'.

Name	AWS Region	Access	Creation date
appbucket8000	Asia Pacific (Mumbai) ap-south-1	Insufficient permissions	August 20, 2023, 18:06:22 (UTC+04:00)
appbucket9000	Asia Pacific (Singapore) ap-southeast-1	Insufficient permissions	August 20, 2023, 18:07:17 (UTC+04:00)