😊 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

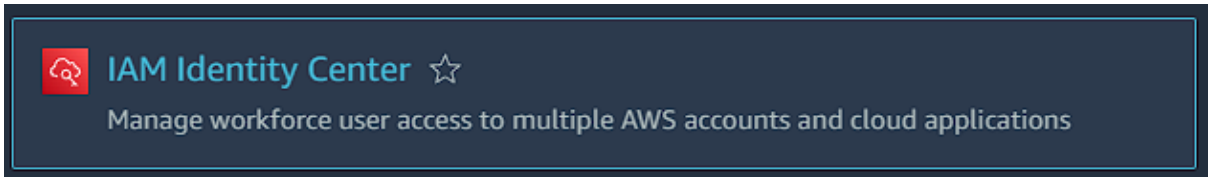
IAM Identity Center includes the following core capabilities and features:

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.

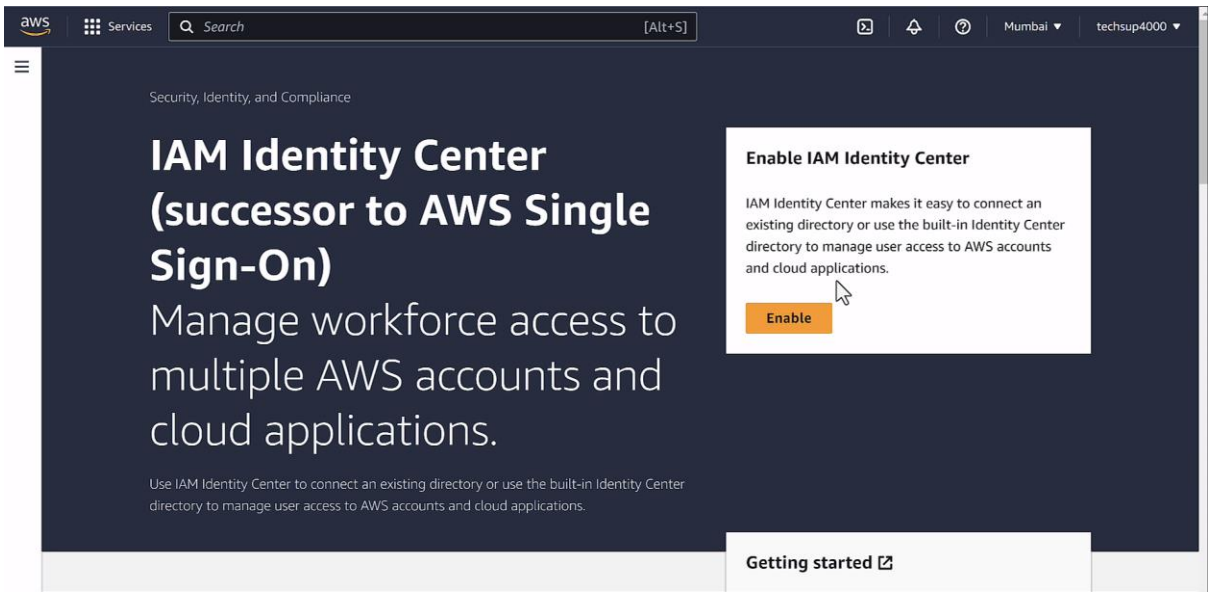
😁 TO BEGIN WITH THE LAB

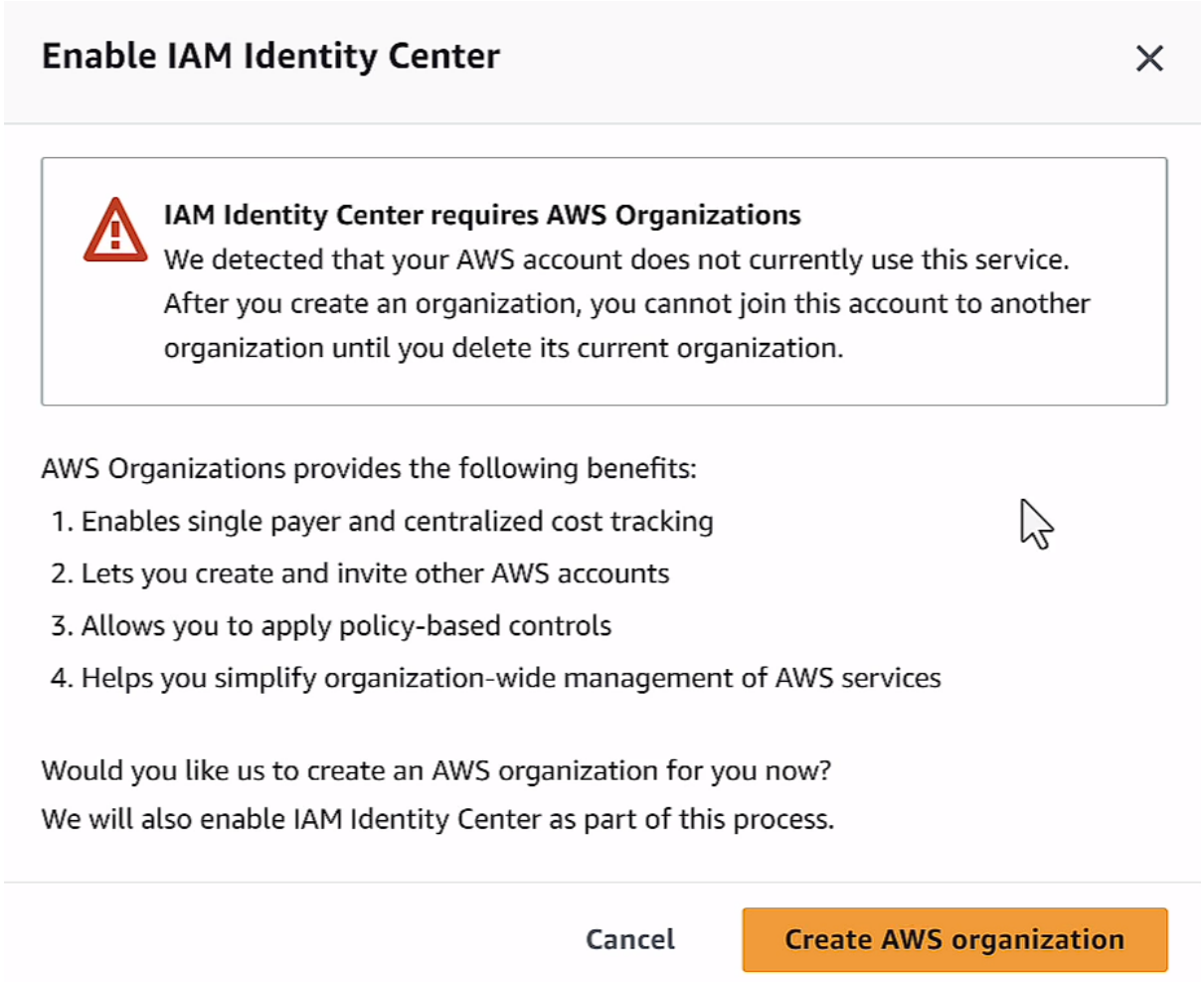
1. Login to AWS Console then search for IAM identity center. Choose this service accordingly.



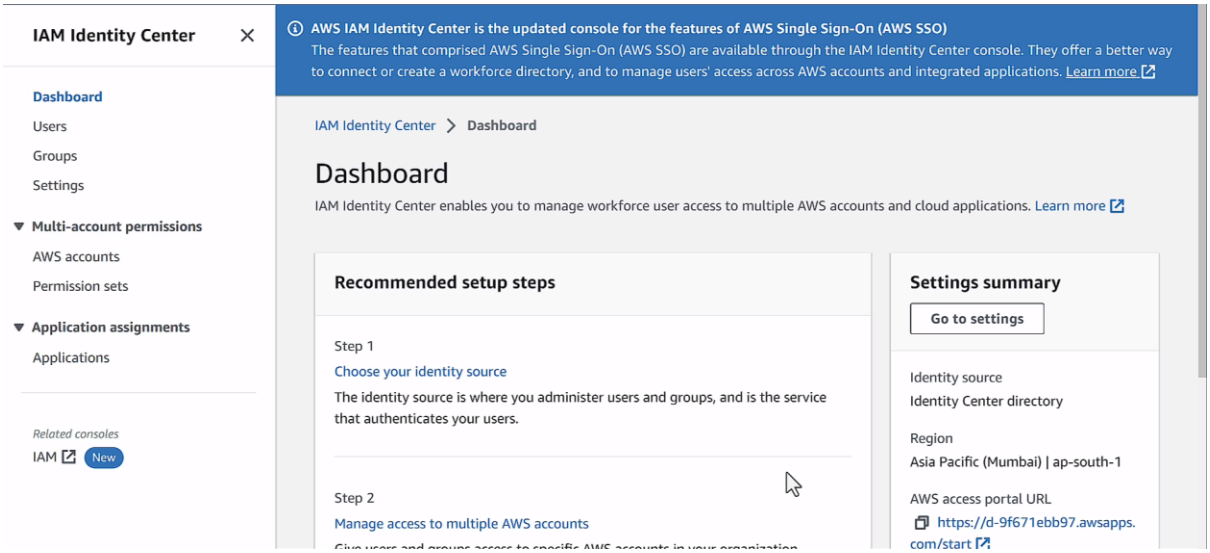
2. Then you need to enable your IAM identity center.
3. So, to create IAM identity center you will need an AWS organization account in place.

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

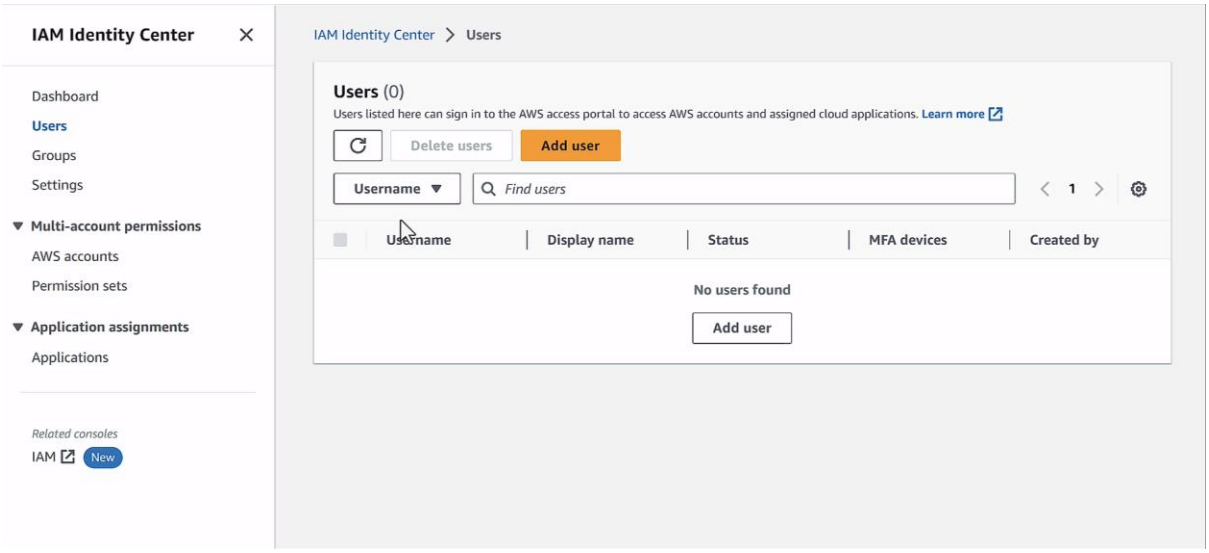




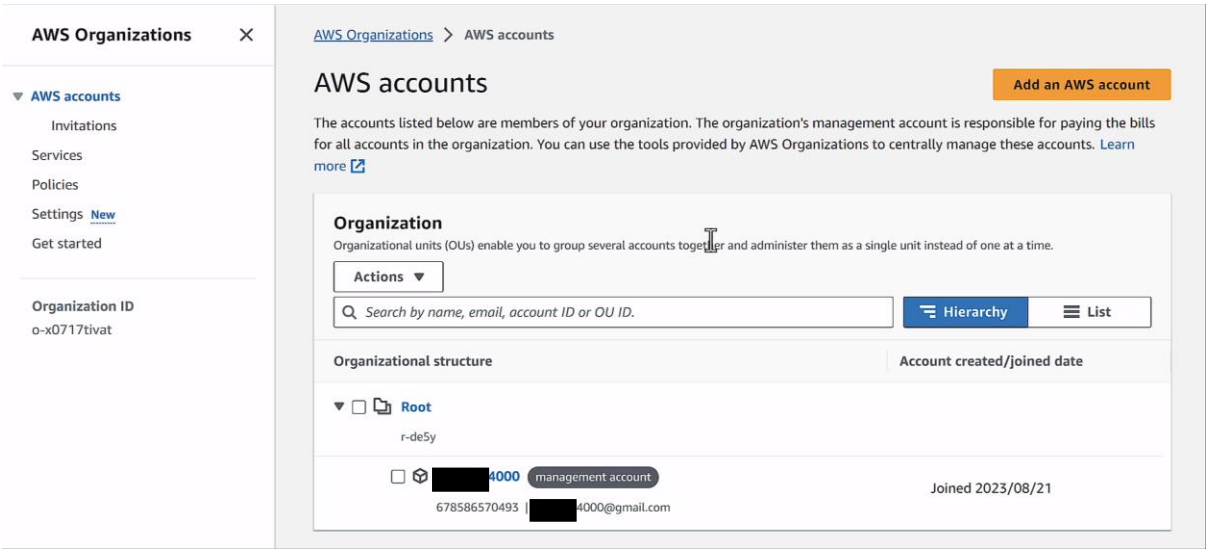
5. This is the dashboard for IAM identity center.



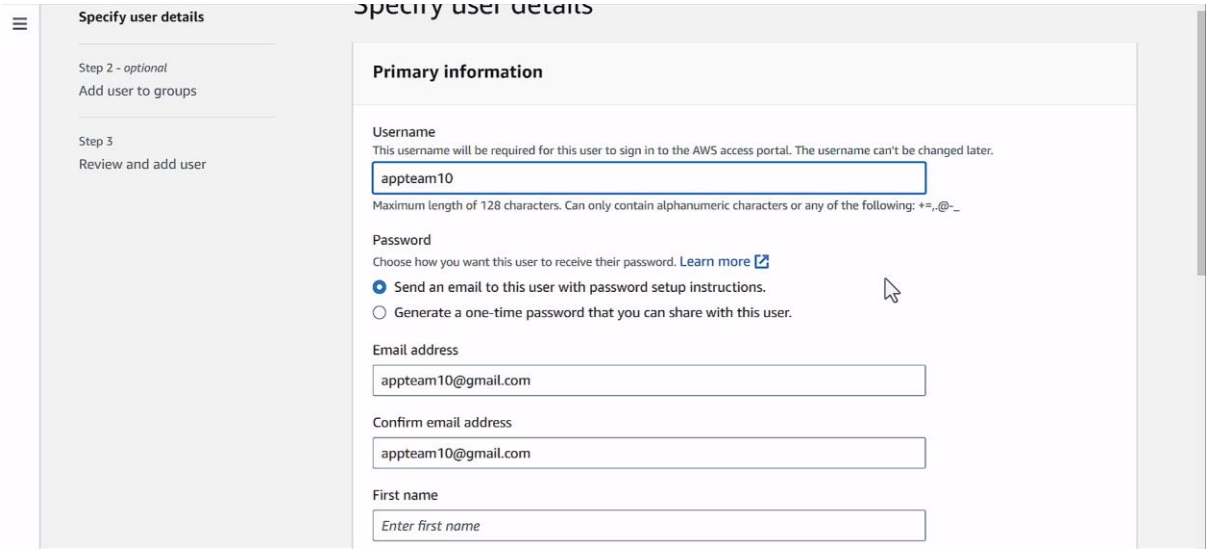
6. Now you can go into users and start adding users.
7. So, basically this service is different from IAM, the user you define in IAM cannot be seen here and the user you create in Identity center will not be a part of IAM itself.



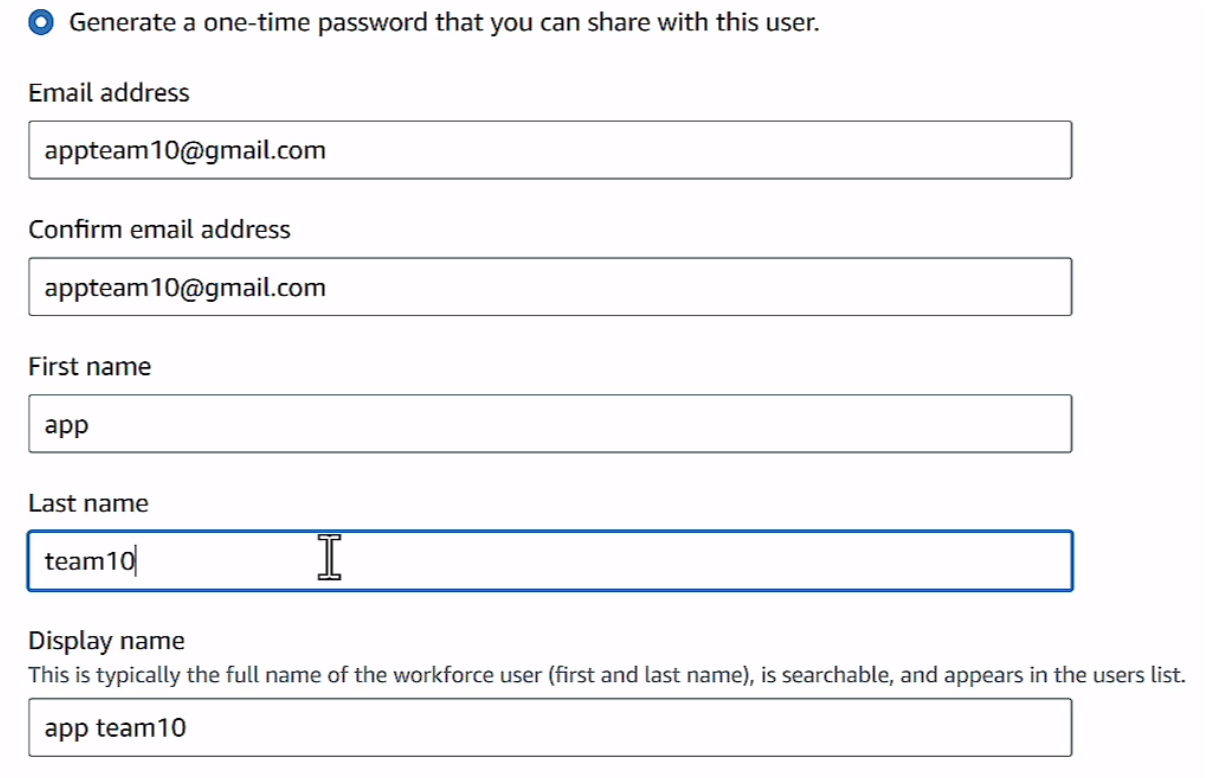
8. If in another tab you will go to AWS Organization, you will see that it has gone ahead and created an AWS organization account for you.



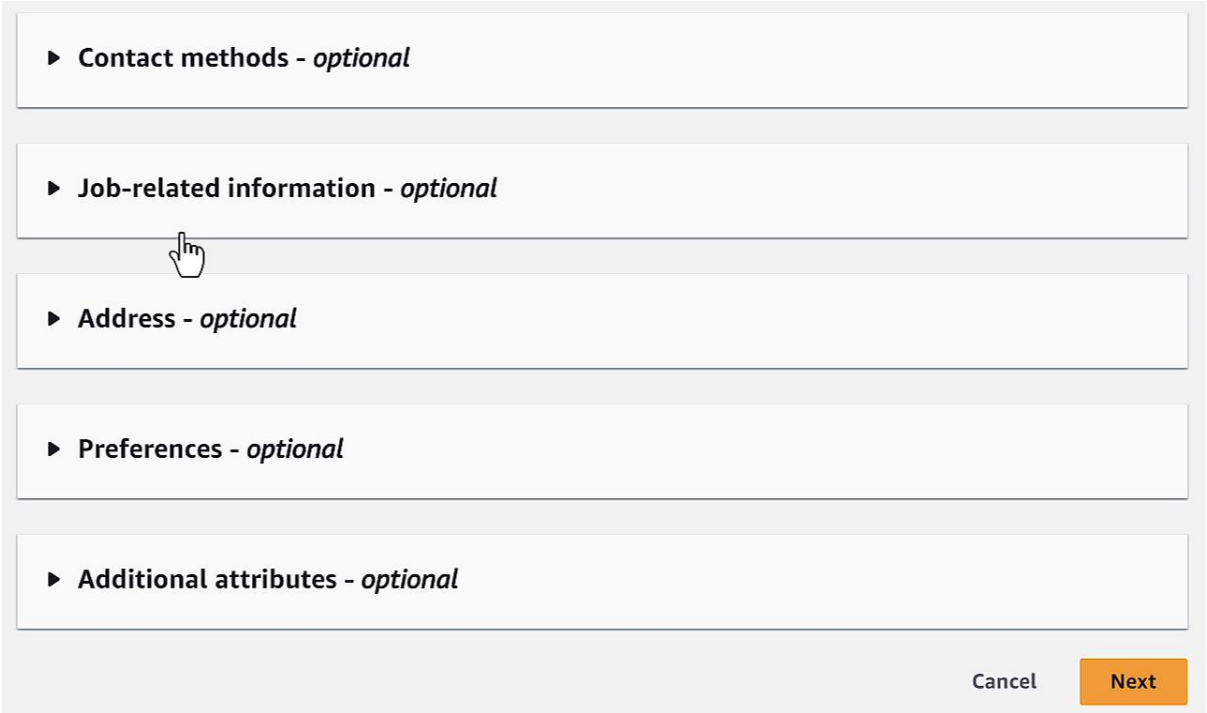
9. Now go back to Identity center and start adding users. Click on add users.
10. Now in the first step, you will need to give a user name and an email address to verify things for identity center.



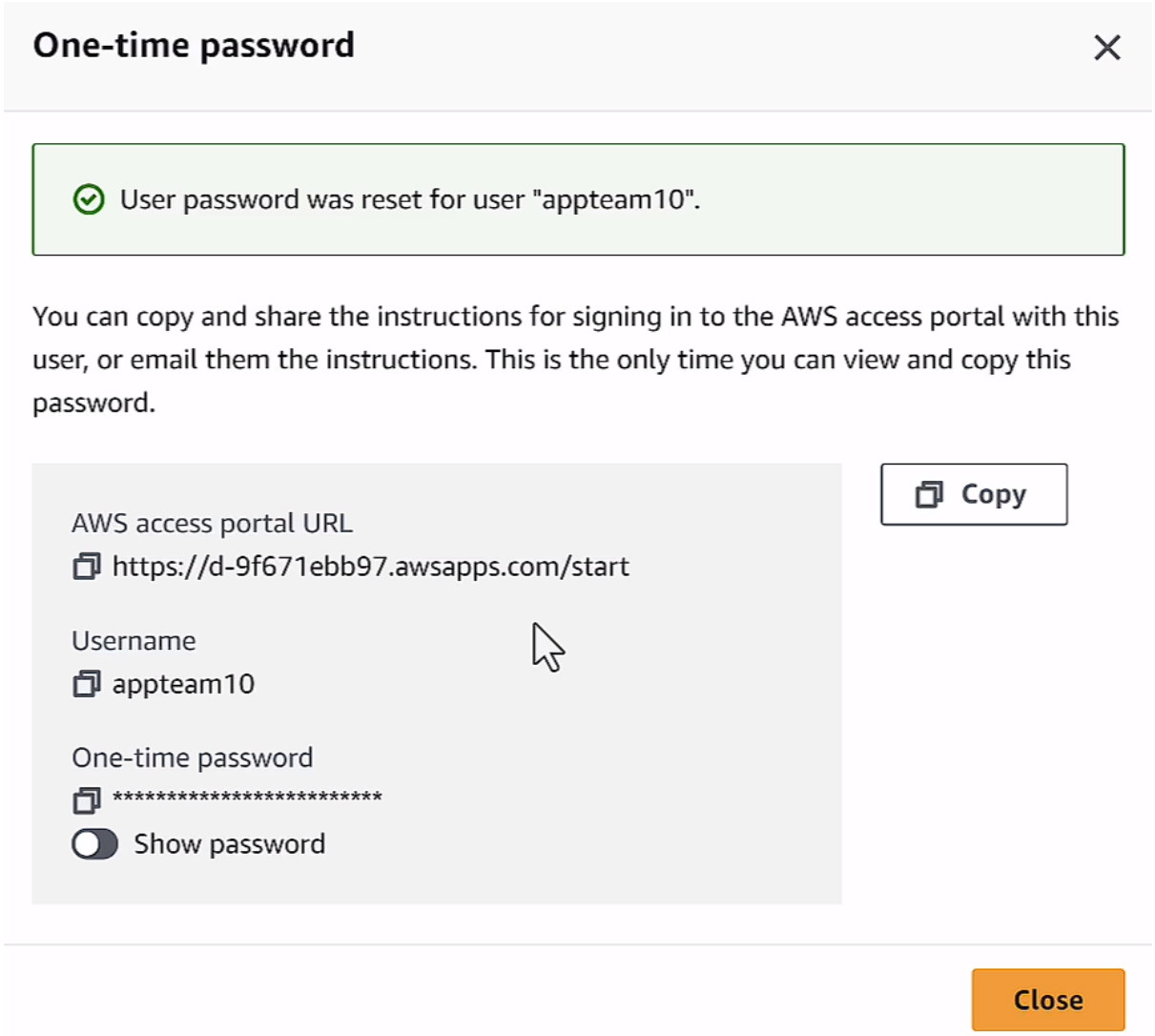
11. Choose **to generate a one-time password** then give first name and last name. And it will show you the display name.



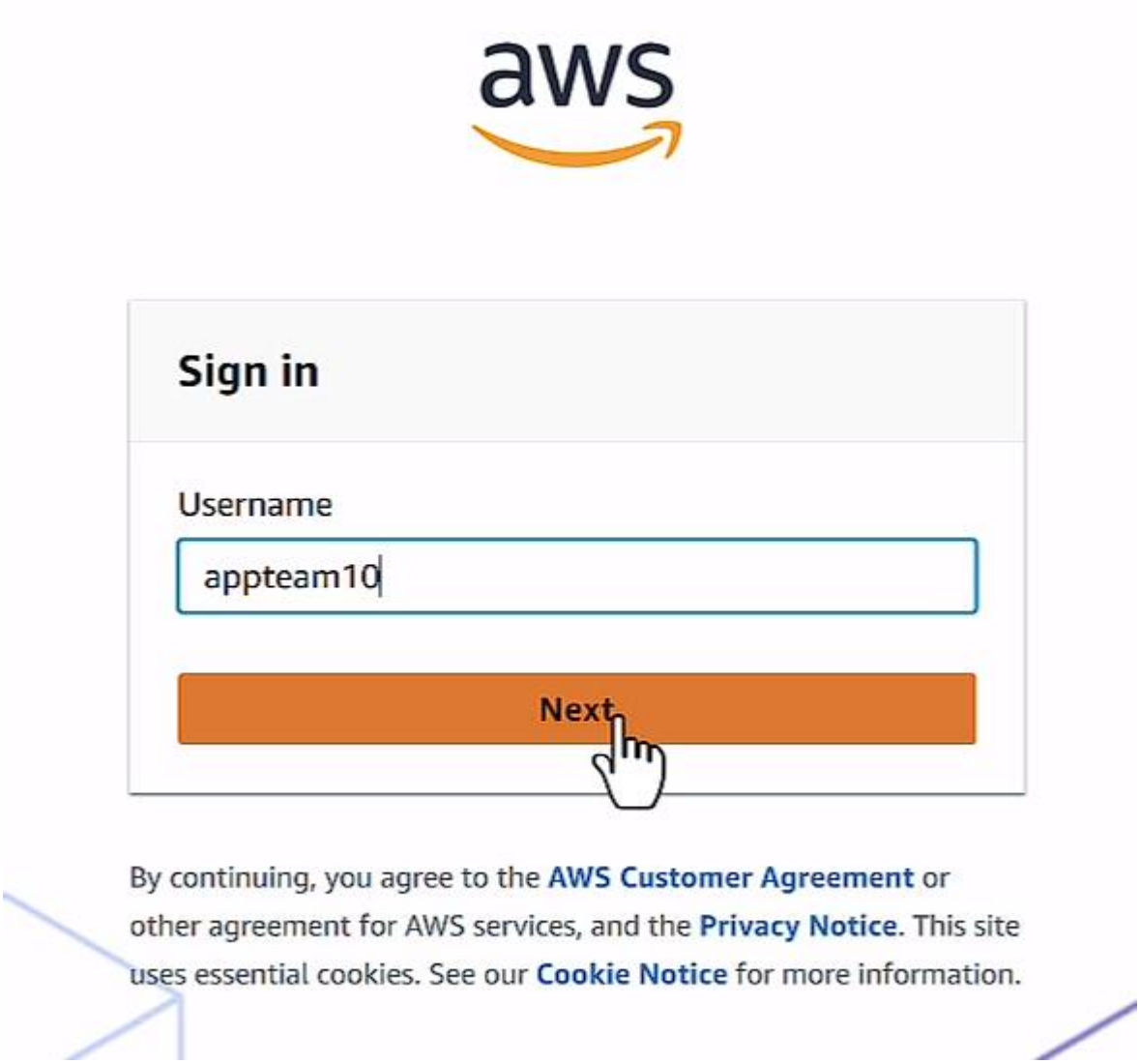
12. You will also see that you can add more relevant information to it.
13. But for now, just click on next.
14. Then skip step as it is not needed right now. Then review your user and add user to the identity center.



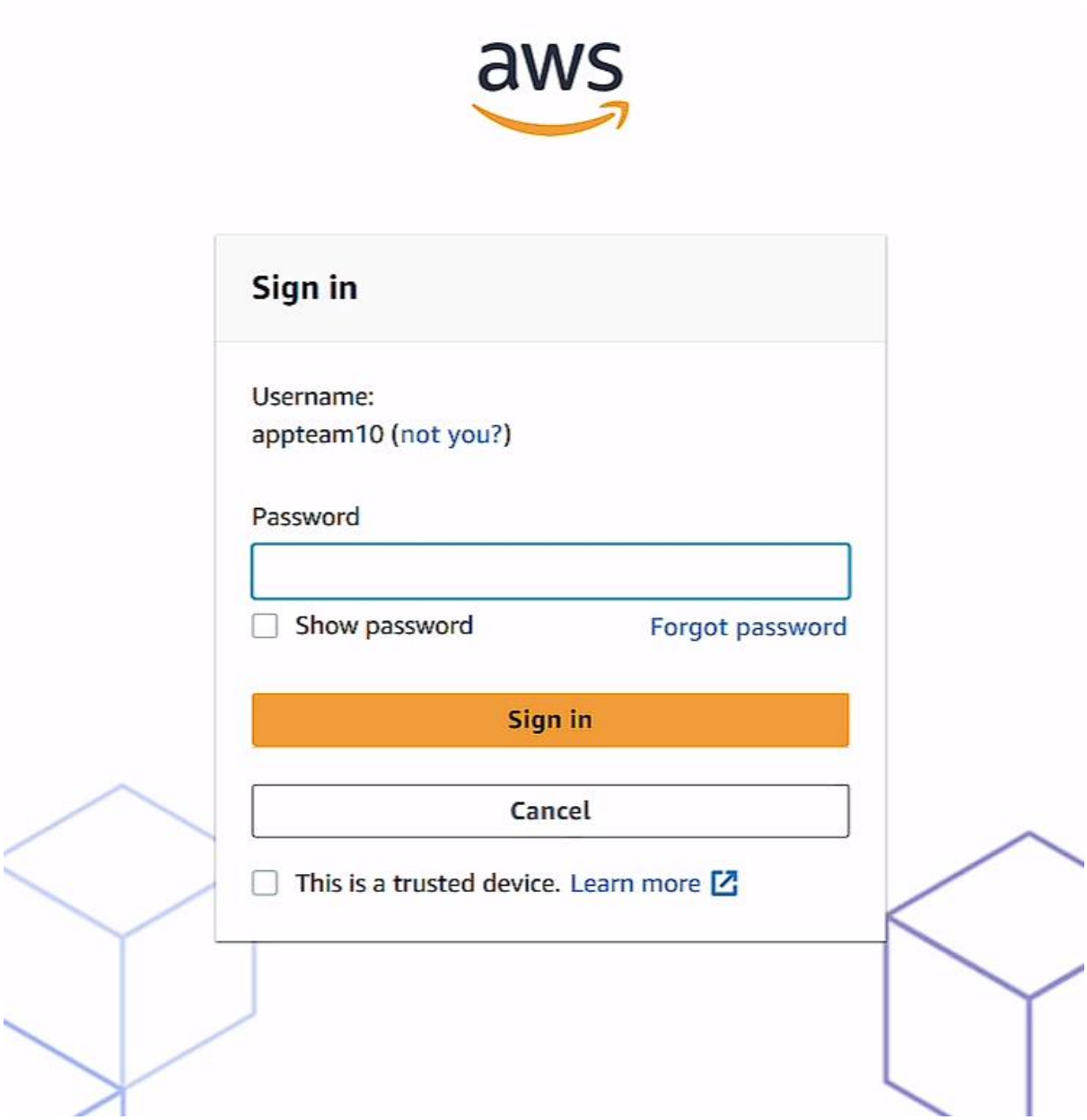
15. Then it will give you an AWS access portal URL, with username and the one-time password.

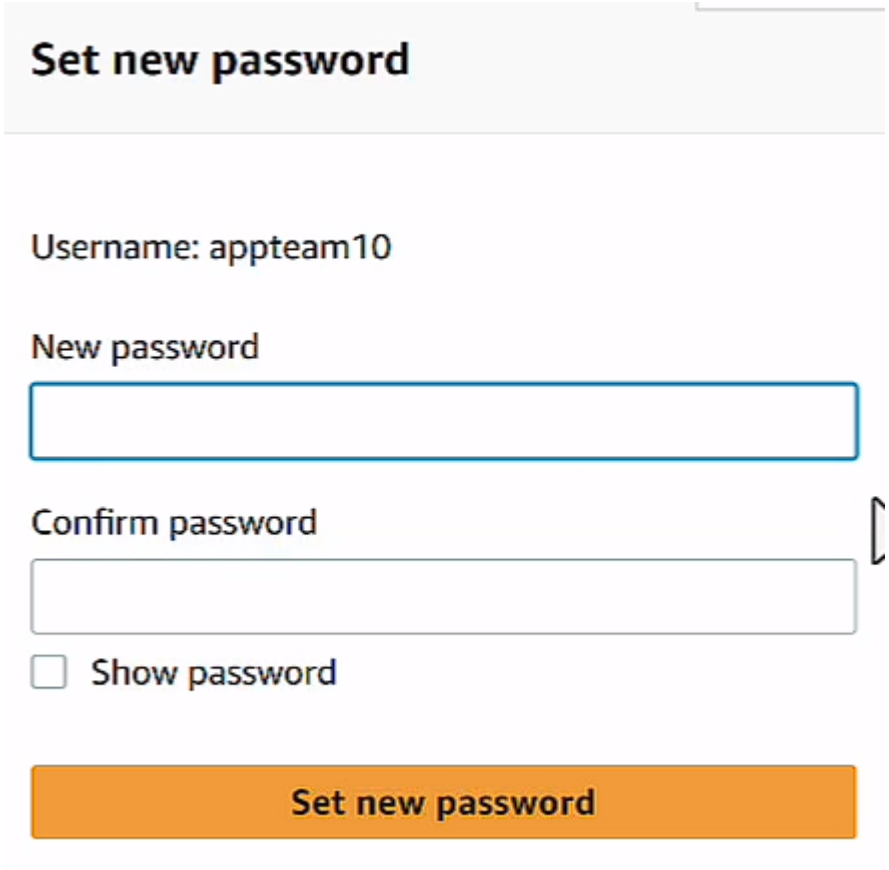


16. Now in the other browser you should put that URL and open it.
17. Now give your username here.
18. Then click on next.

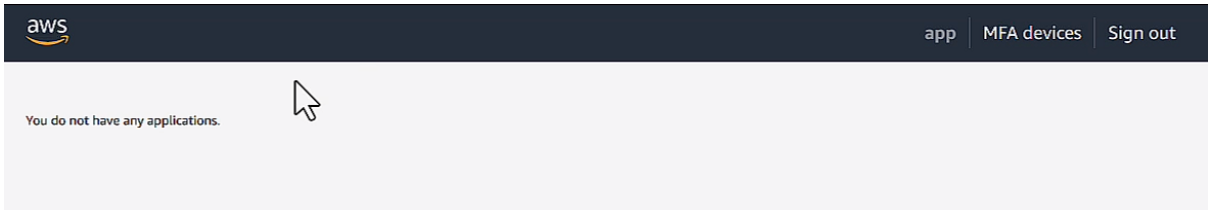


19. Now put the password which was generated.
20. Once you've entered the one-time password, it will ask you to create you own password.

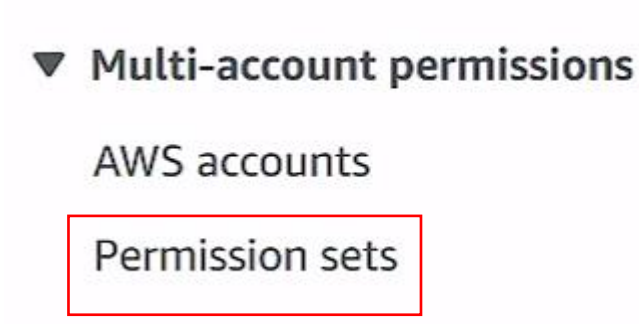

aws
Sign in
Username:
appteam10 (not you?)
Password
Show password
Forgot password
Sign in
Cancel
This is a trusted device. Learn more

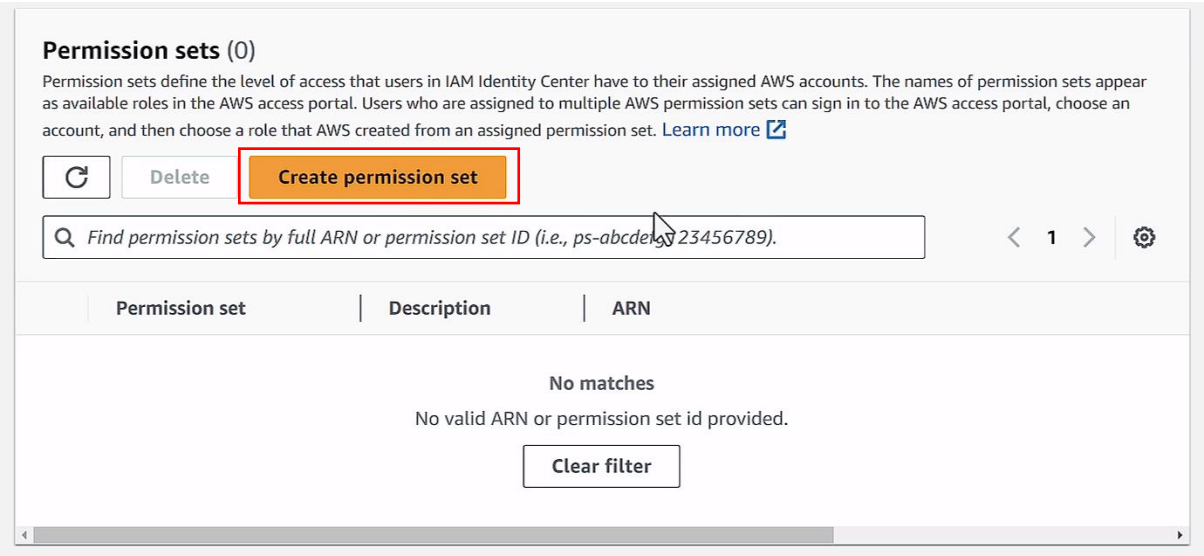


21. Once you have created your own password, then you will see that a blank has been open saying that you do not have any application.

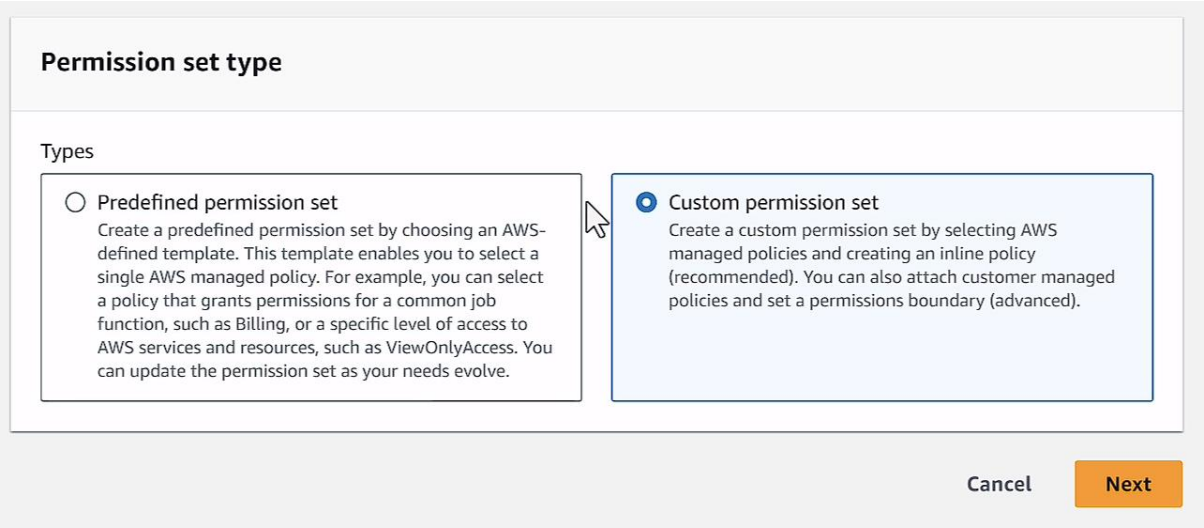


22. Now you are going to give access to this user of your S3 buckets that you have in your root account.
23. For that you need to click on Permission sets.
24. Then you need click on create permission set.

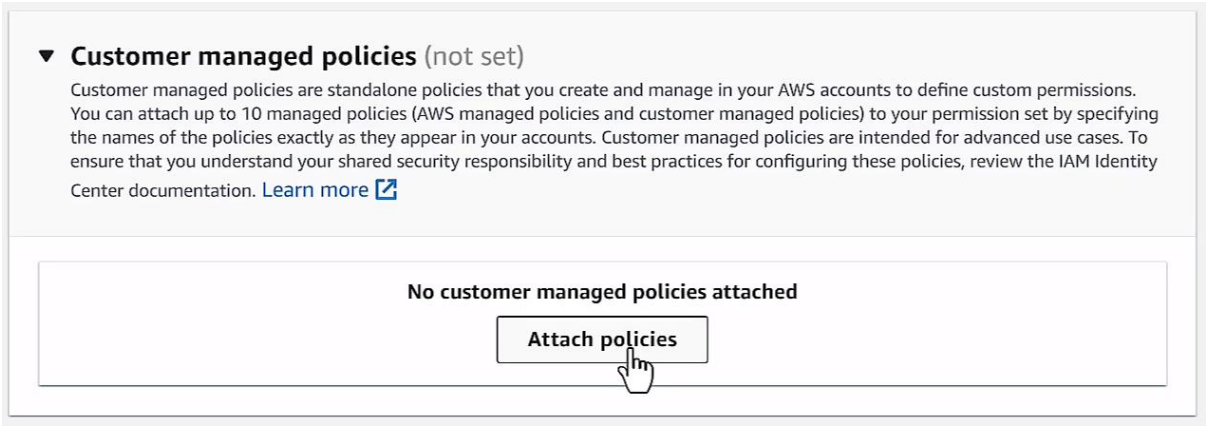




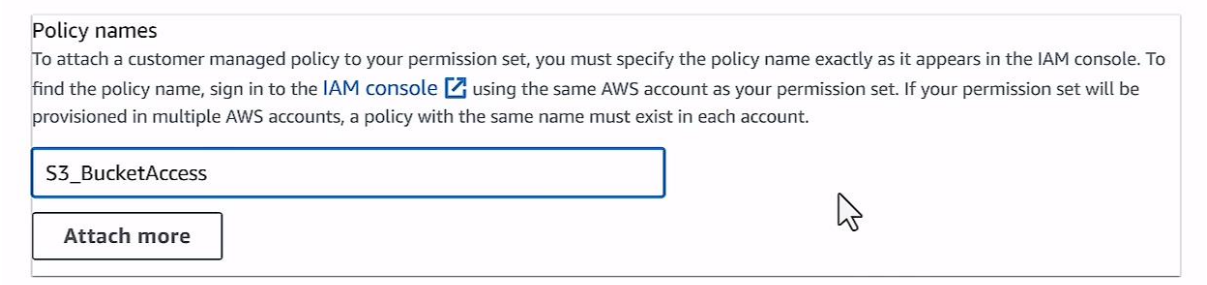
25. Now you will have two options for permission set type. But here you are going to choose Custom permission set.
26. Then click on next.



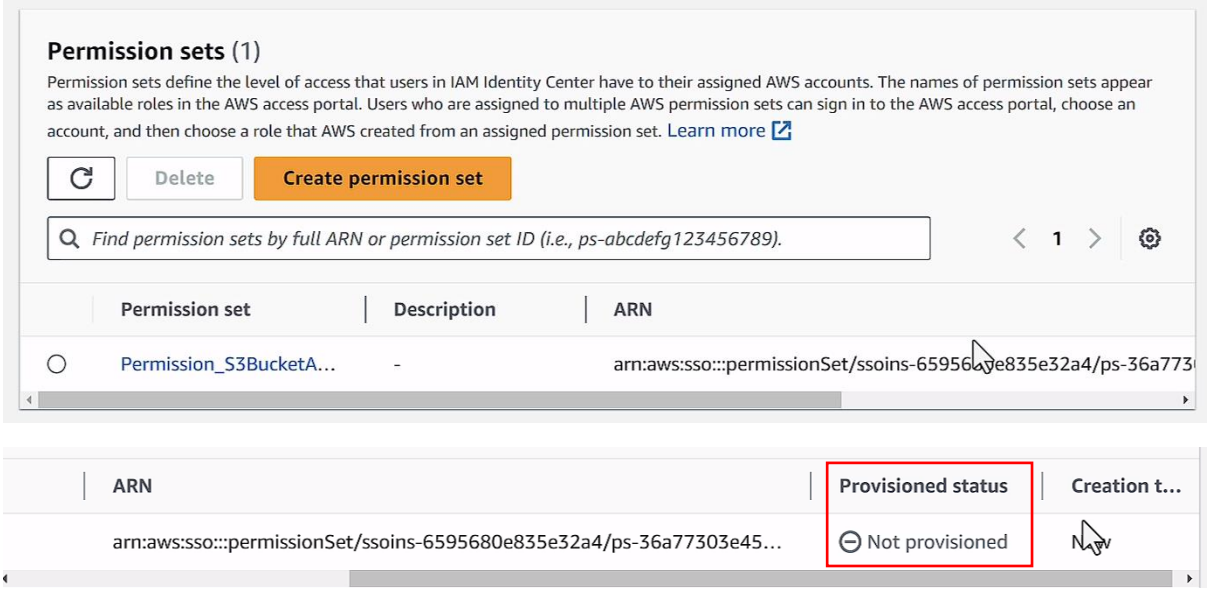
27. On the next page you can choose from you existing IAM policies that you created for S3. For that go back to IAM then go to your policy which you want to choose copy its name. Then come back to permission set.
28. Then you from customer manages policies you need to click on Attach policies.



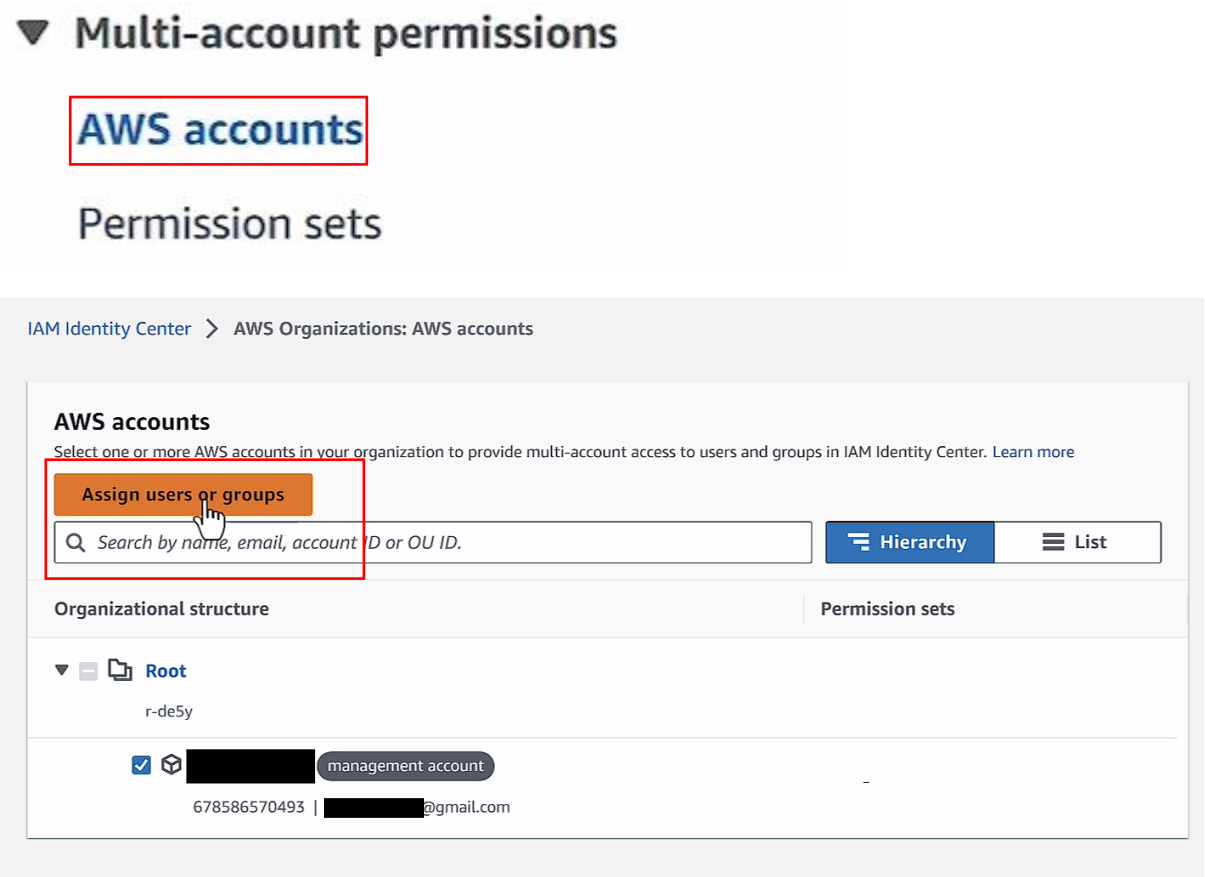
29. Then you need to give policy name.



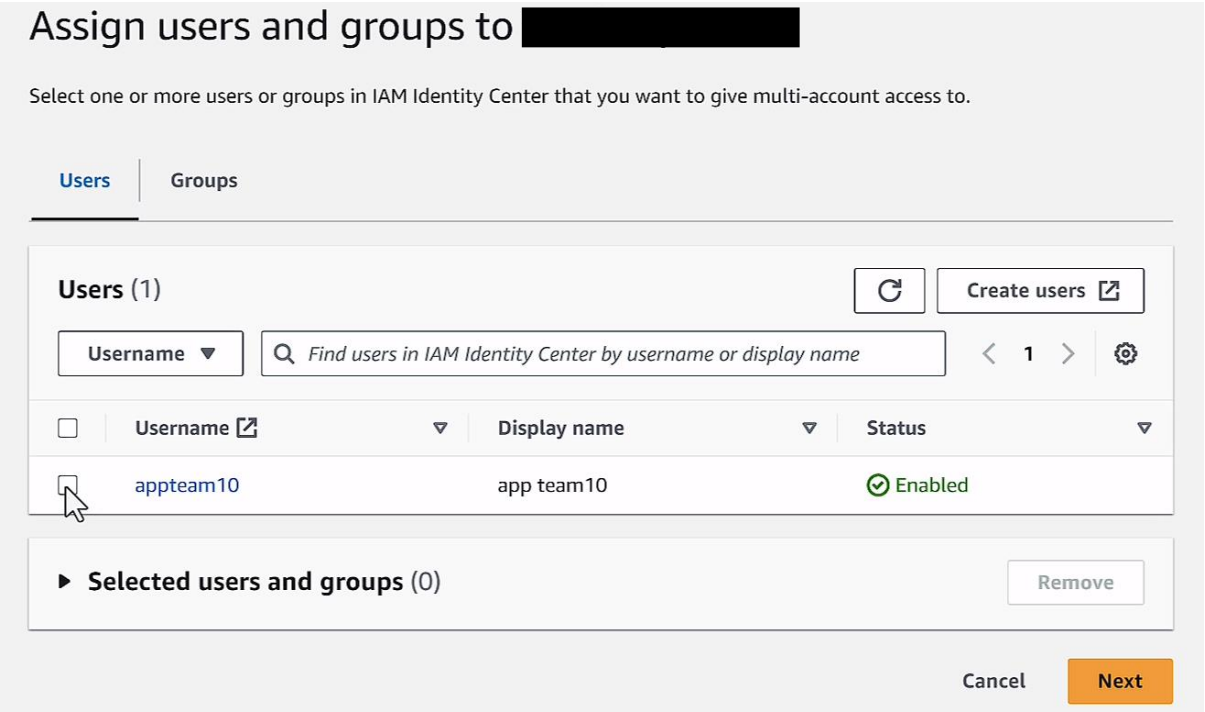
30. Then just click on next and move to give your permission set a name. Then move to review page and create your permission set.
31. So, you will have a permission set in place. But if you will scroll you permission set to right then you will see that it is not provisioned. So, you need to assign this permission set to a user.



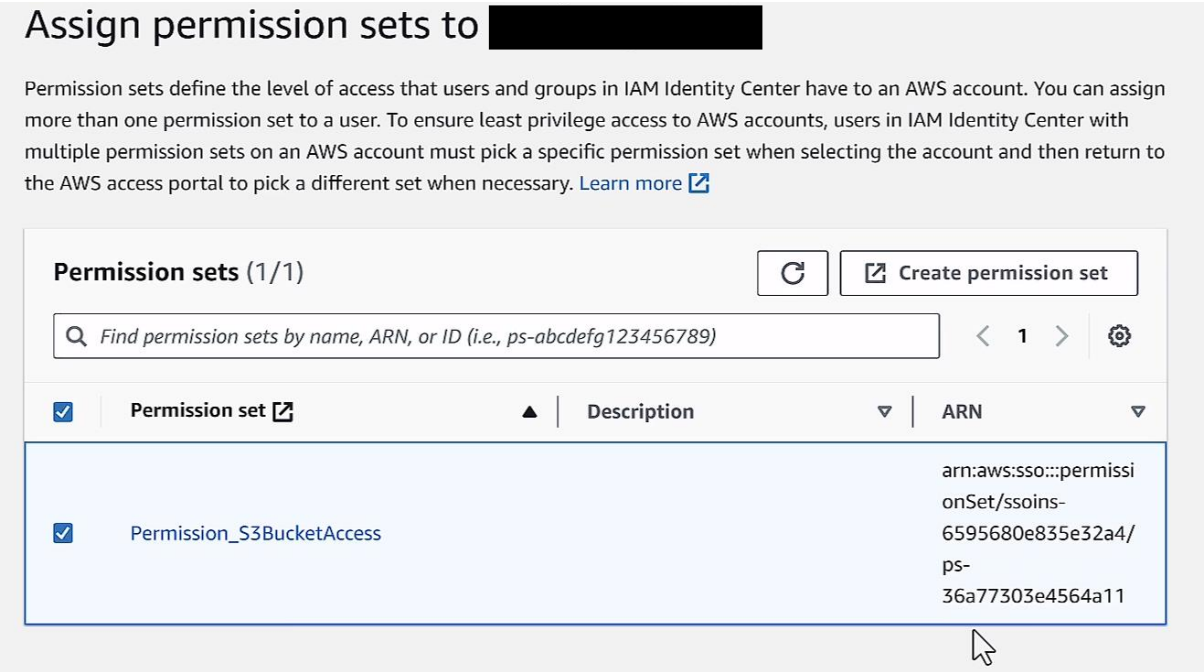
32. Now click on AWS Accounts.
33. Then you need to choose your management account and click on Assign users or groups.



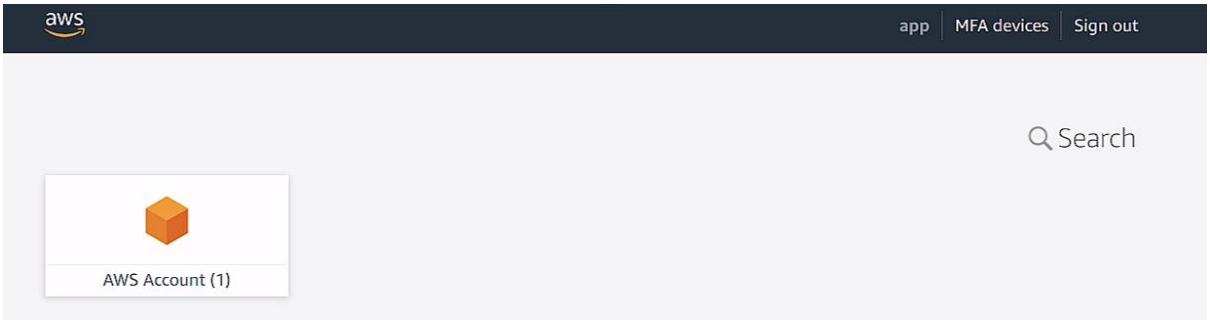
34. Now select your user and click on next.



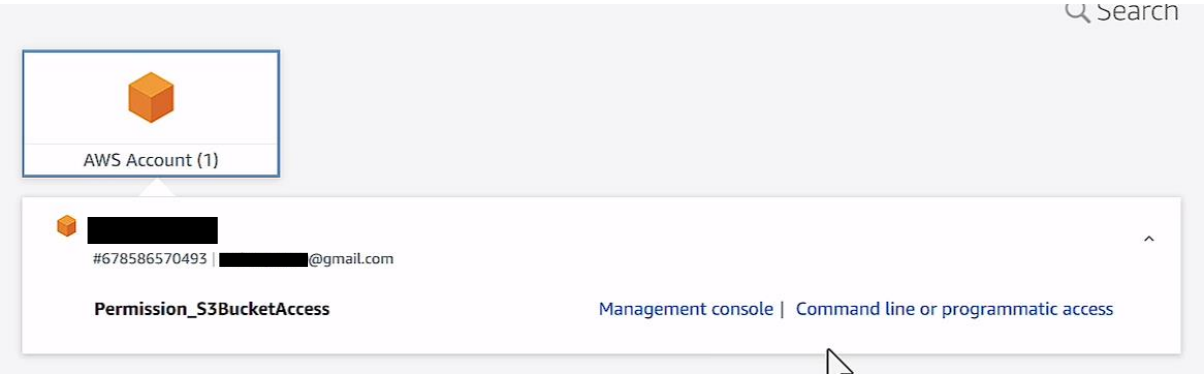
35. Then select your permission and assign it to the user.



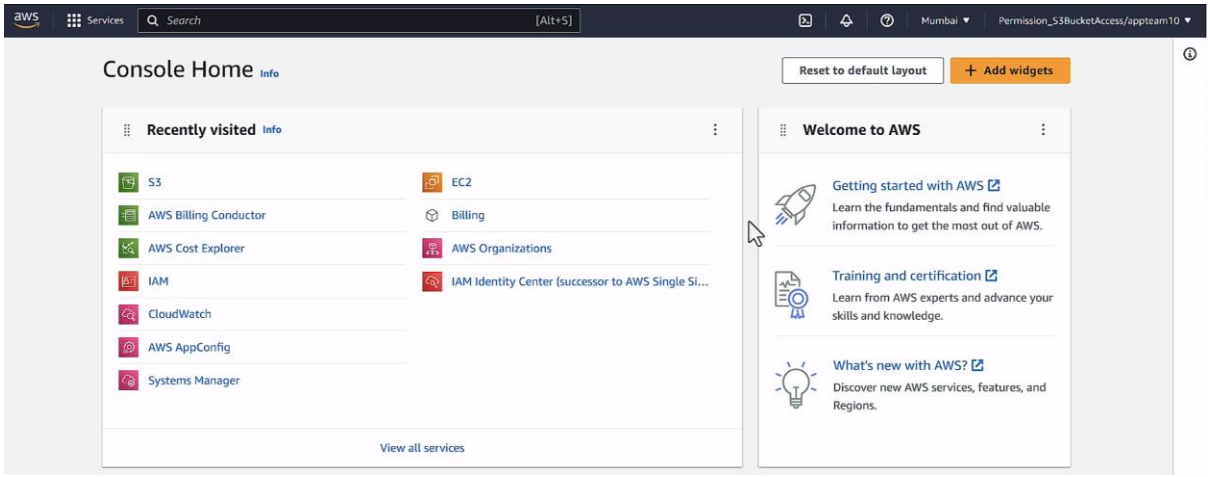
36. After if you will you go to your permission set you will see that it has been provisioned now.
37. Now if you go back to the user in another browser where you logged in with it and refresh the page.
38. You will see that an AWS account is attached to it now.



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.



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.