😊 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.

🤔 What are we doing in this Lab?

In this process, you're setting up and using AWS IAM Identity Center (formerly AWS SSO) to manage user access and permissions within an AWS organization. Here's a brief summary:

1. **Set Up AWS Organization and IAM Identity Center**: You start by creating an AWS Organization and enabling IAM Identity Center. This service allows you to centrally manage access to AWS accounts.

2. **Create and Configure a User**: A new user is created in IAM Identity Center with a temporary password. The user is then required to log in through the AWS access portal URL, set a permanent password, and access the system.

3. **Assign Permissions**: You create a permission set with specific access rights (e.g., administrator access) and assign it to the user.

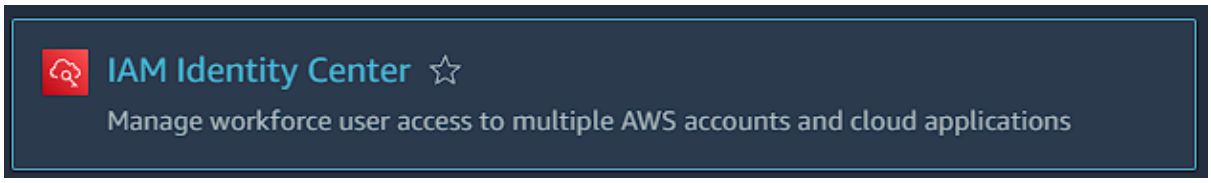
4. **Provision Access**: The user is assigned to an AWS account within the organization with the specified permission set. The user can then access the AWS Management Console with the appropriate permissions.

End Goal: The goal is to set up a system where you can easily manage who can access your AWS accounts and what they can do in them, all from one place. This way, you can give people

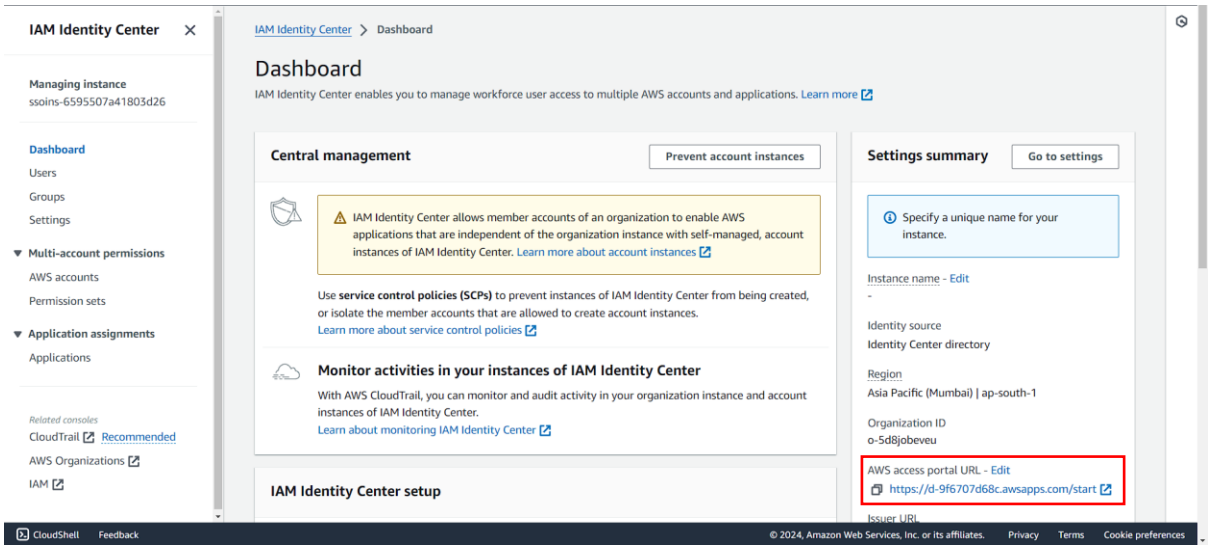
access to specific AWS accounts and set permissions without creating separate user accounts in each AWS account. It makes it simple and secure for users to log in and do their work.

😁 To begin with the Lab

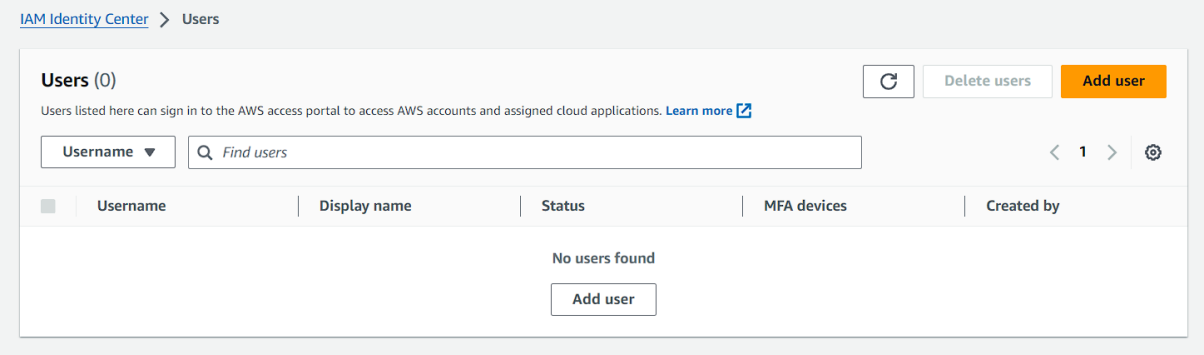
1. Login to AWS Console then search for IAM identity center. Choose this service accordingly.



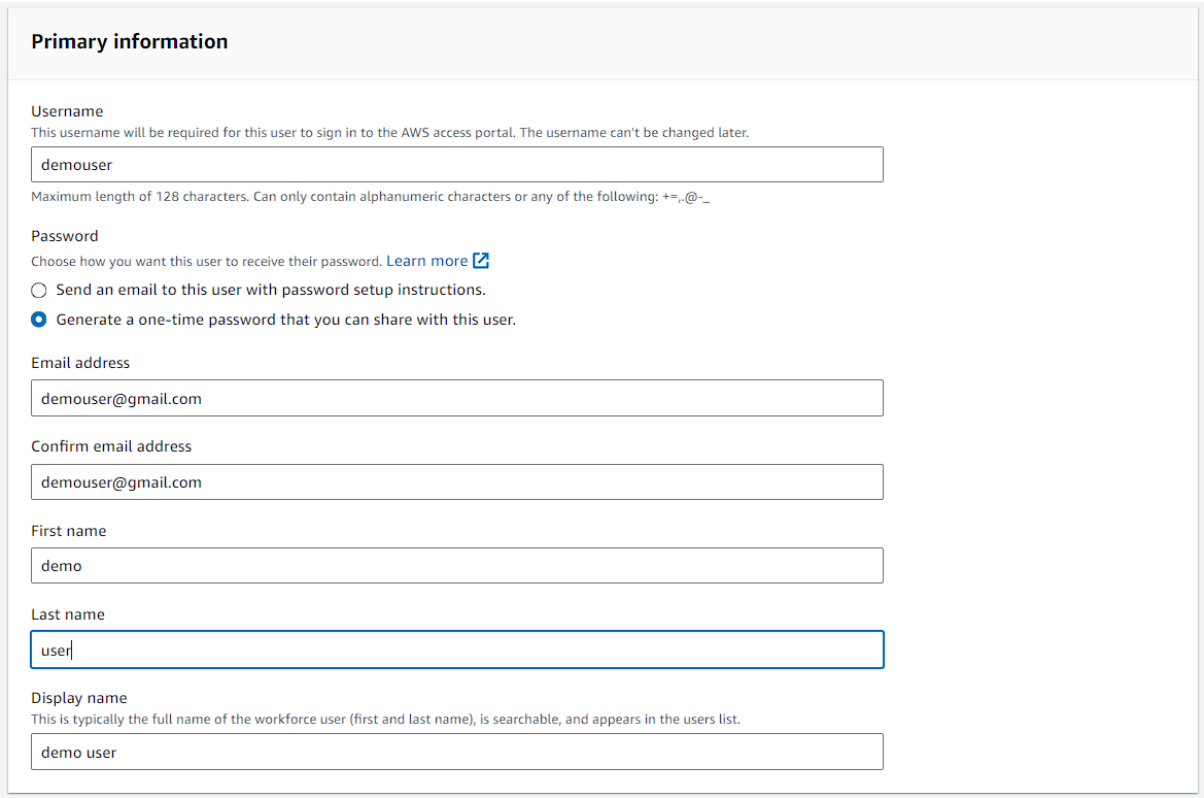
2. Then you need to enable your IAM identity center.
3. So, to create an IAM identity center you will need an AWS organization account in place.
4. Go and create your AWS Organization. It is just simple to create it. Just click on Create AWS Organization. And it will create it by itself.
5. Now come back to the IAM identity center and enable it. Once it is enabled then you will be able to see its dashboard.
6. In addition, you can see that it has given you the AWS access portal URL. So, this is the URL that the users will use to log in to the overall access portal.



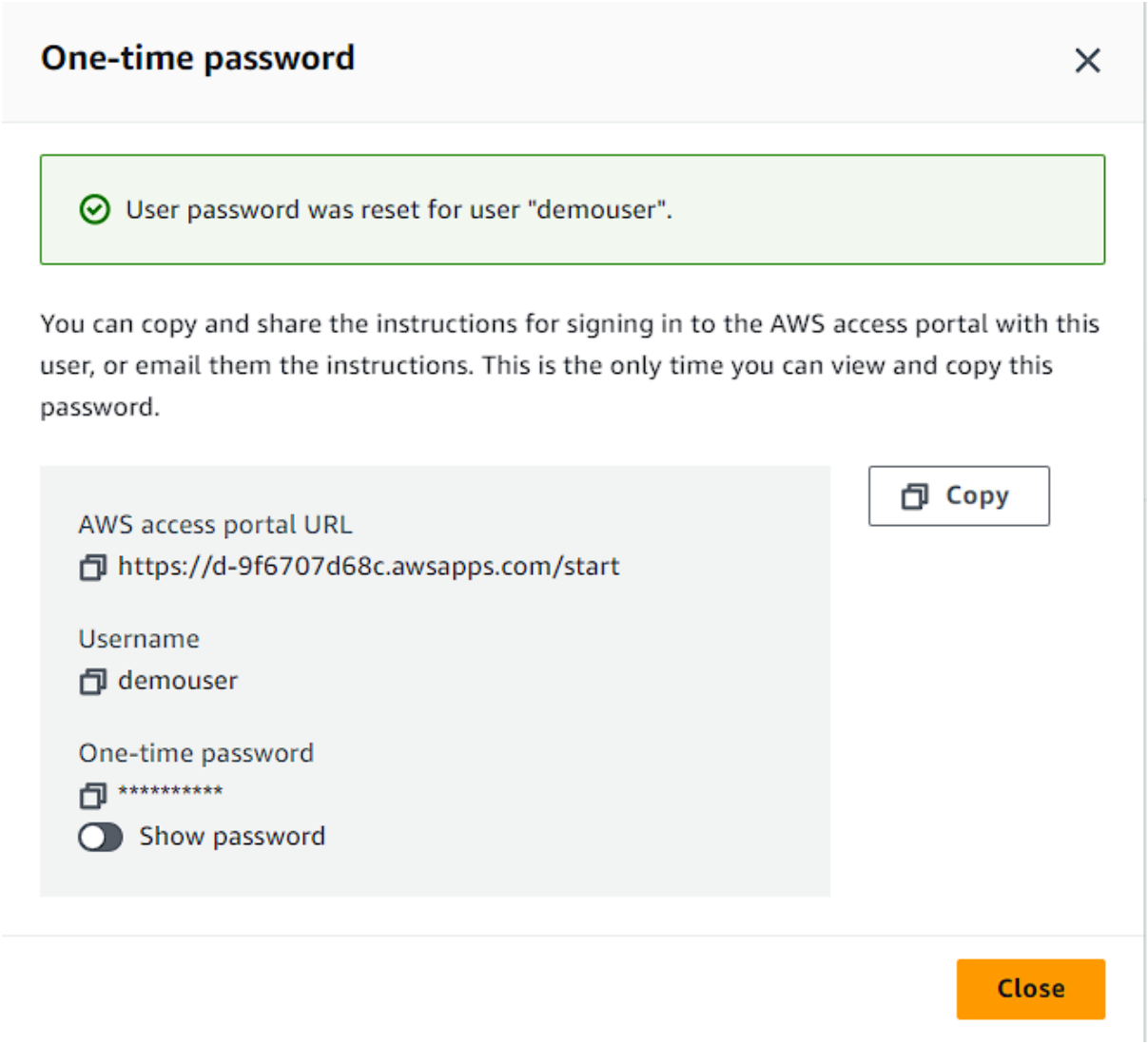
7. First things first you have to create a new user. From the left pane click on users and then click on add users.



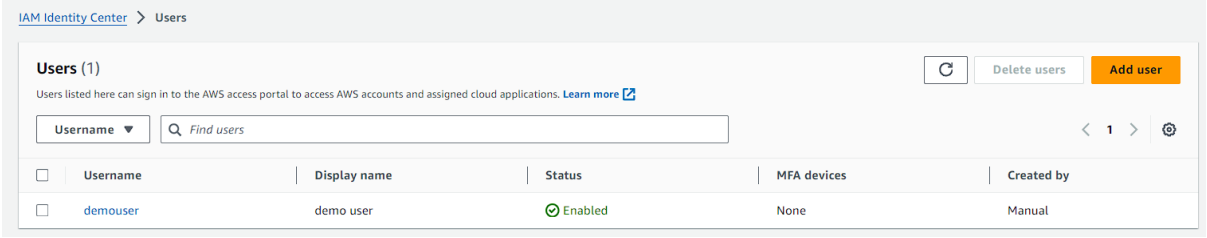
8. Here you are going to give a user name then you have to select generate one one-time password.
9. Then you have to specify an email address. After that give the first and last name of the user.
10. Then just add your user and leave everything else as it is.



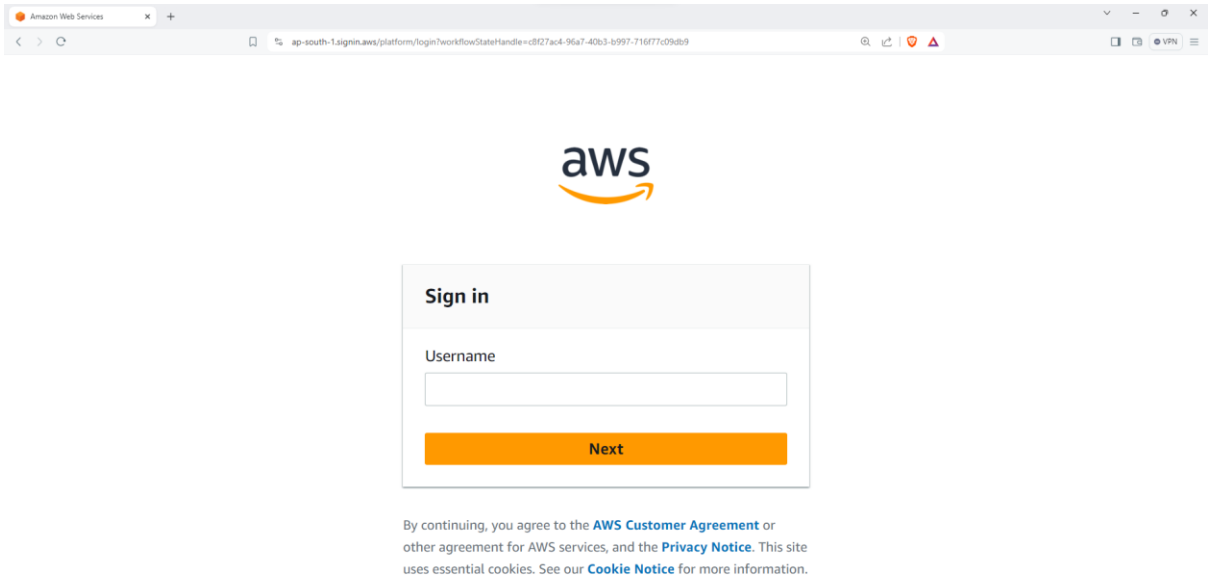
11. Once you have clicked on add user you will see that it has given you the login credentials. Save them in your notepad.



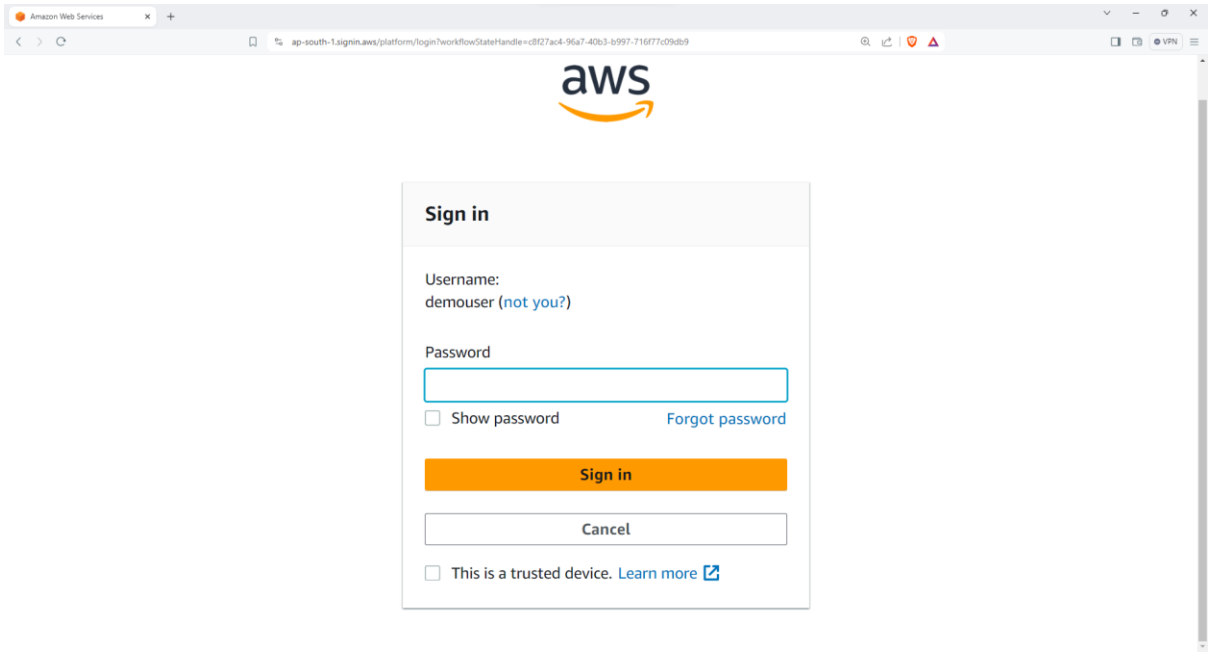
12. After that you will be able to see your user.



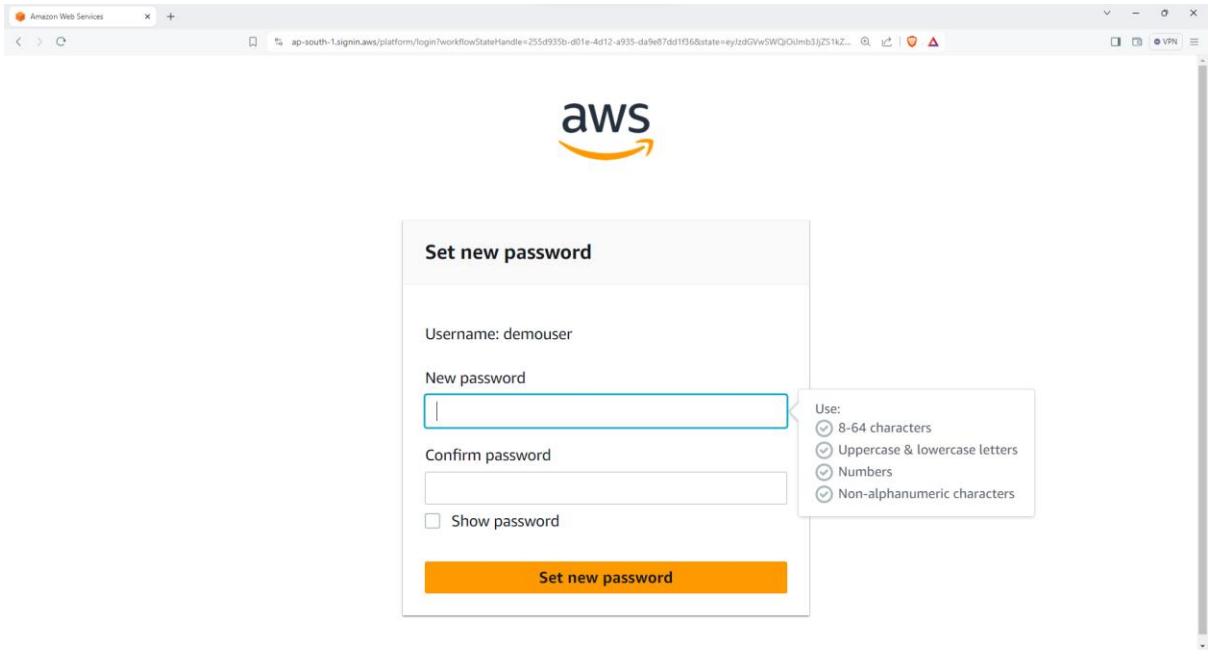
13. Now you are going to copy the access portal URL for this user and paste it in a new browser.
14. Now once you have pasted the URL you will see a log in screen here you have to give your username.



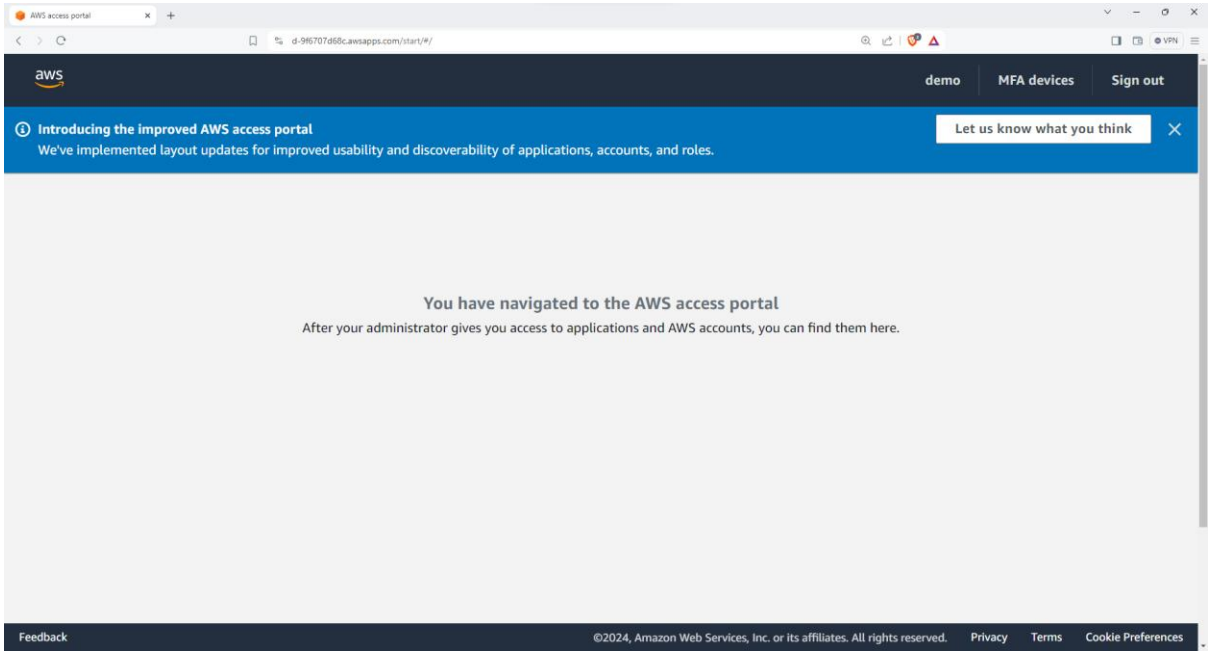
15. After that it will ask for the password, enter the one-time password that AWS has generated.



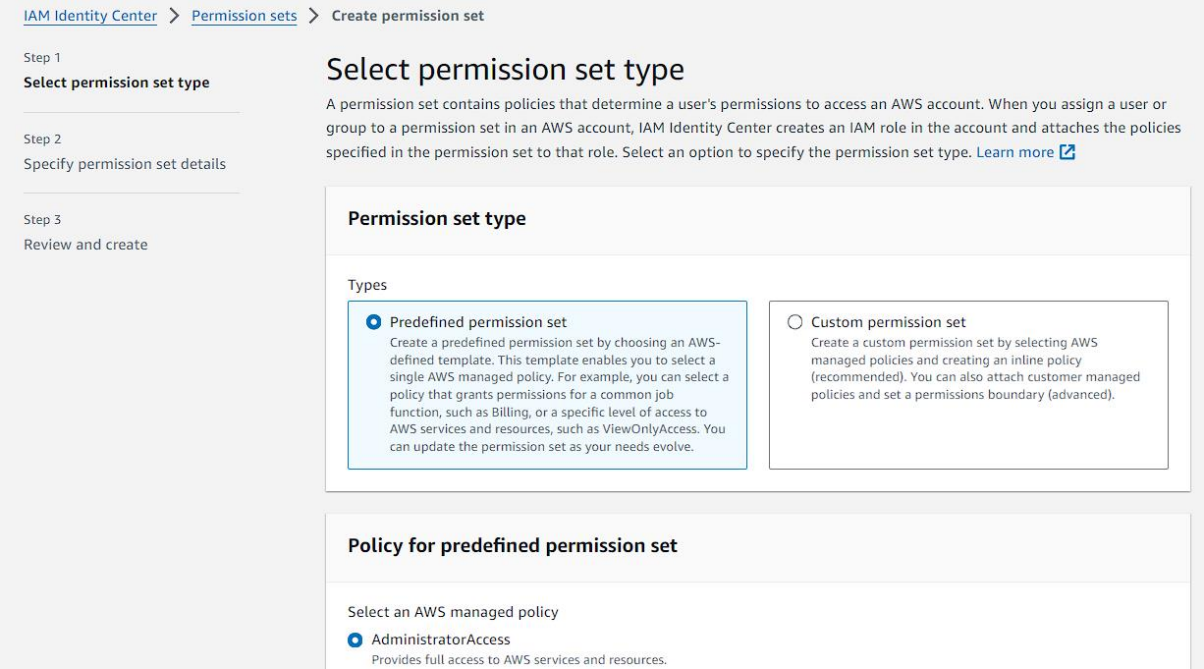
16. Now it will ask you to create a new password. Once your new password has been created, it will ask you again to sign in.



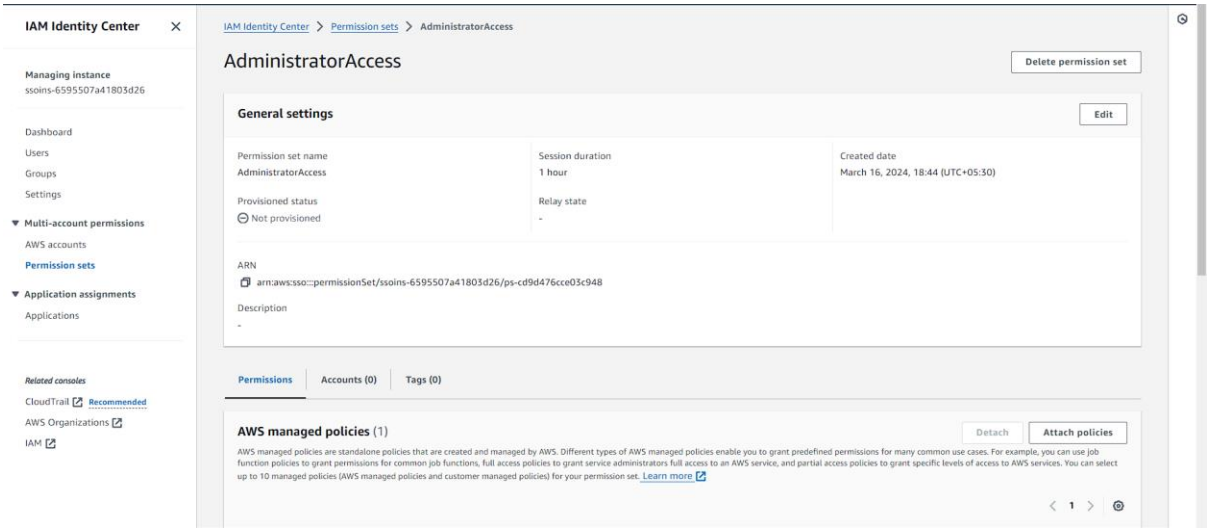
17. Once you have signed in you will see this blank page because there is no permission attached to this certain user.



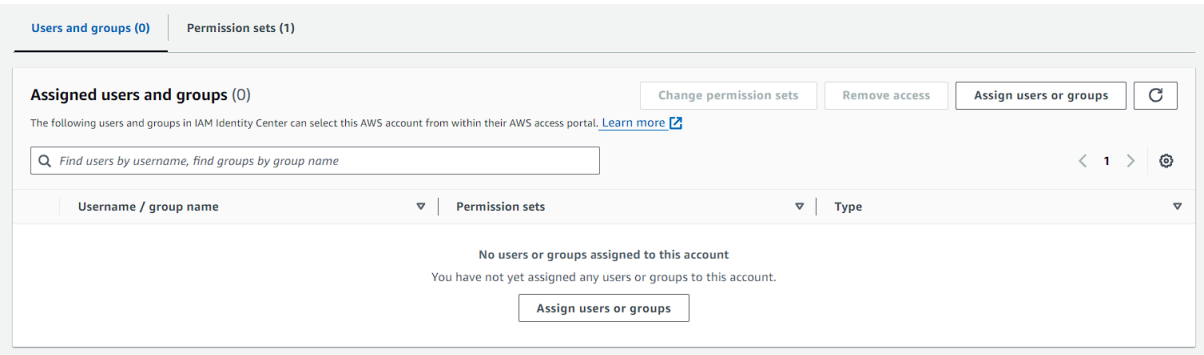
18. Now come back to the identity center navigate to permission sets and then click on create permission sets.
19. For simplicity select the predefined permission set and select administrator access. Then just create your permission set.



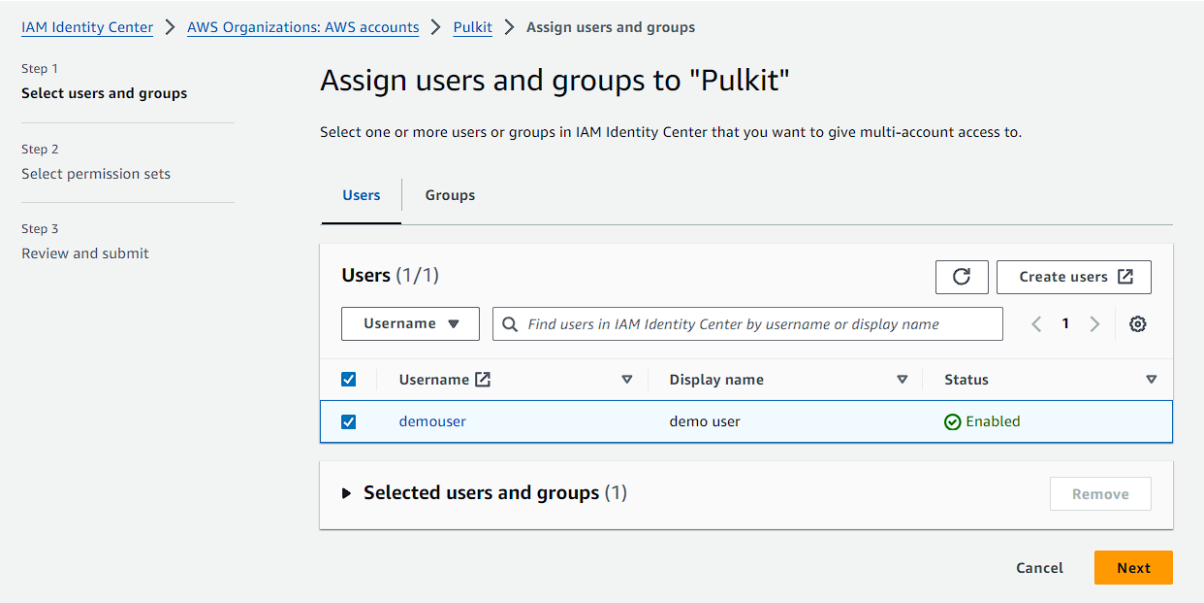
20. Now if you open your permission set you will see that it is not provisioned. So, now we have to provision this, currently there is no account added with this permission set first we are going to add user to it.



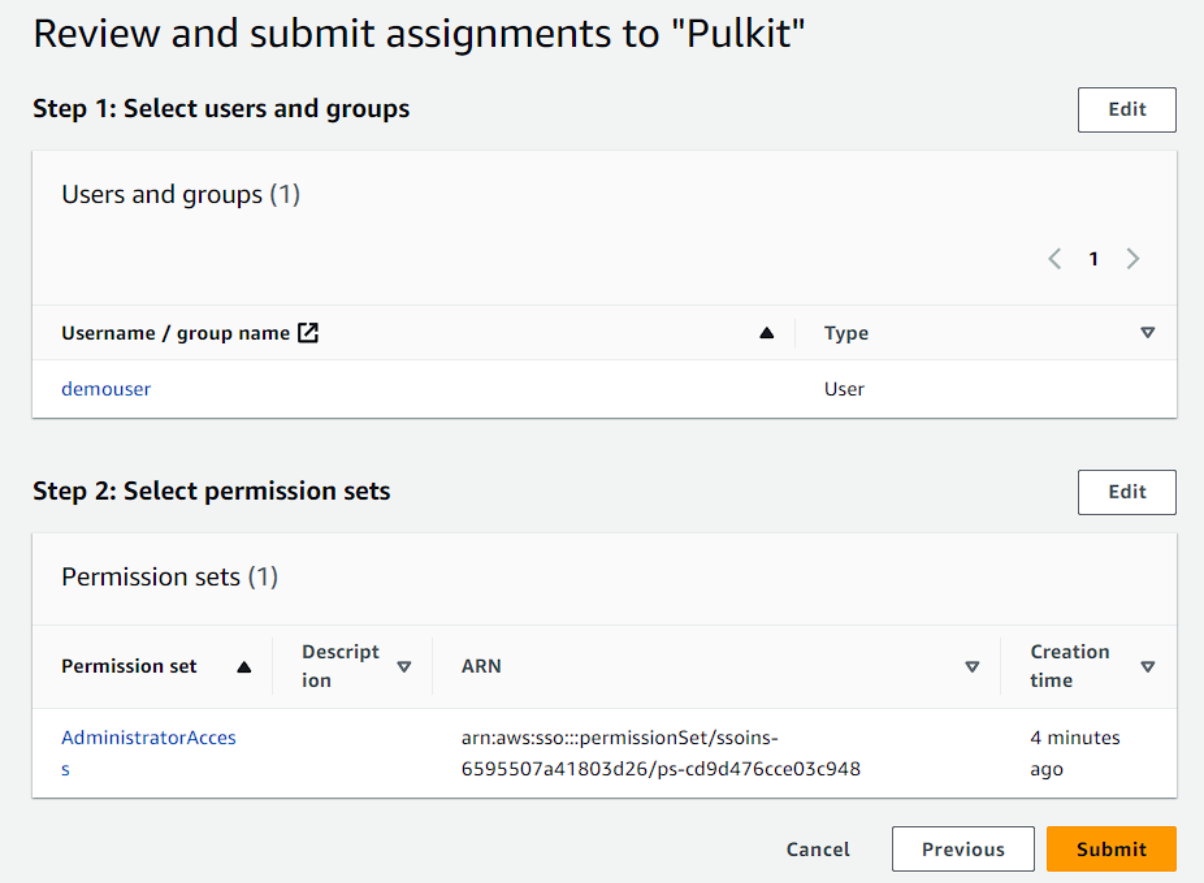
21. For that click on AWS Accounts then select your account and you will see this option to assign users. Click on it.



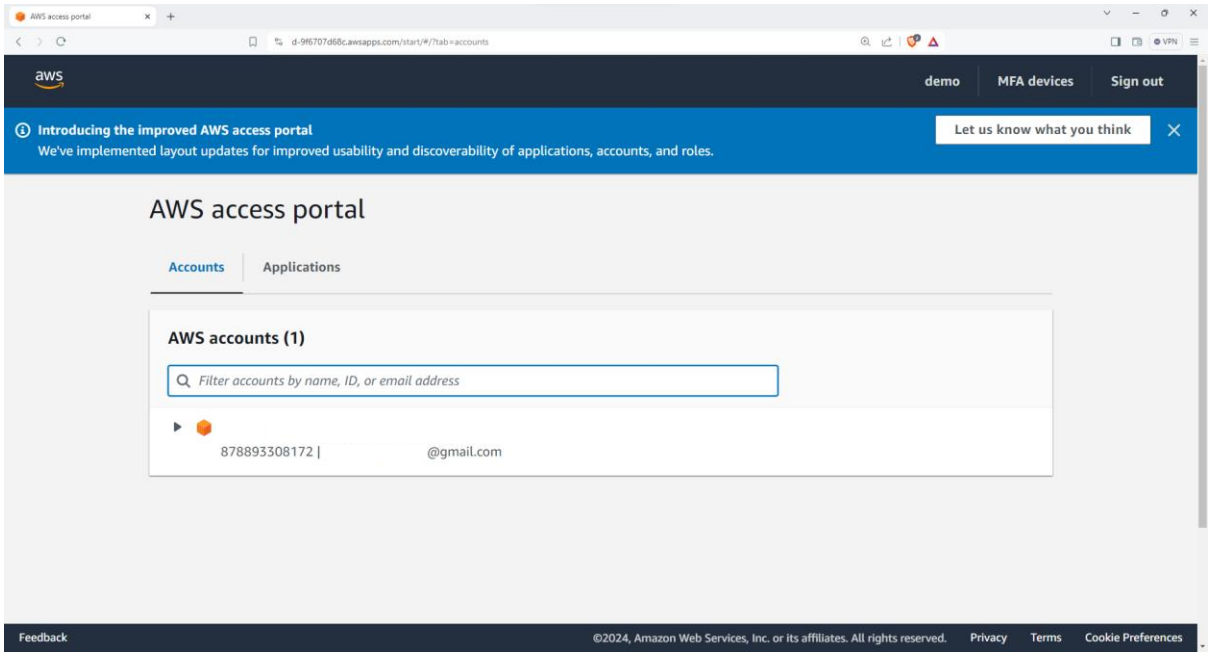
22. Now you have to select the user and click on next and after that select your permission set.



23. Now in the review you can see your user and permission set. Click on submit.



24. Once it is completed now go back to another browser and refresh the page. You will see that your account is getting reflected.



25. After that click on this account and open up the management console then you will be able to see your console.