Azure AD SSO integration with AWS Single-Account Access

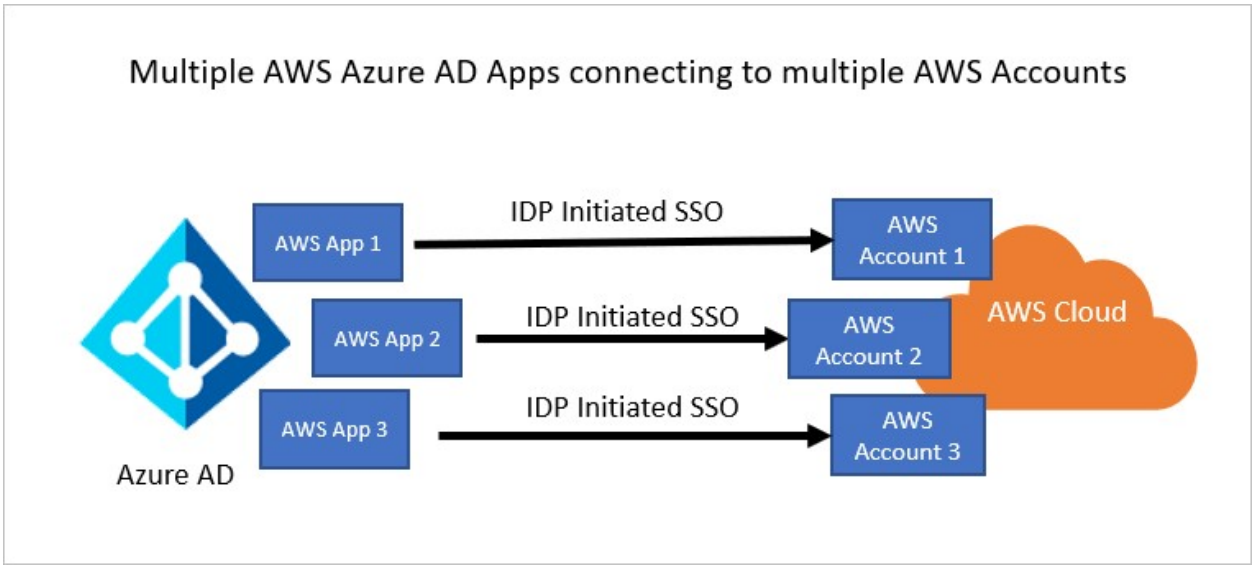
AWS Single Sign-On

AWS Single Sign-On makes it easy to manage access centrally to multiple AWS accounts and AWS applications, with sign-in through Microsoft Azure AD. Federate Microsoft Azure AD with AWS SSO once, and use AWS SSO to manage permissions across all of your AWS accounts from one place. AWS SSO provisions permissions automatically and keeps them current as you update policies and access assignments. End users can authenticate with their Azure AD credentials to access the AWS Console, Command Line Interface, and AWS SSO integrated applications.

AWS Single-Account Access

AWS Single-Account Access has been used by customers over the past several years and enables you to federate Azure AD to a single AWS account and use Azure AD to manage access to AWS IAM roles. AWS IAM administrators define roles and policies in each AWS account. For each AWS account, Azure AD administrators federate to AWS IAM, assign users or groups to the account, and configure Azure AD to send assertions that authorize role access.

AWS Single-Account Access architecture



You can configure multiple identifiers for multiple instances. For example:

- `https://signin.aws.amazon.com/saml#1`
- `https://signin.aws.amazon.com/saml#2`

Prerequisites

To get started, you need the following items:

- An Azure AD subscription. If you don't have a subscription, you can get a free account.
- An AWS IAM IdP enabled subscription.
- Along with Cloud Application Administrator, Application Administrator can also add or manage applications in Azure AD. For more information, see Azure built-in roles.

Adding AWS Single-Account Access from the gallery

To configure the integration of AWS Single-Account Access into Azure AD, you need to add AWS Single-Account Access from the gallery to your list of managed SaaS apps.

1. Sign in to the Azure portal using a work account, school account, or personal Microsoft account.
2. In the Azure portal, search for and select Azure Active Directory.
3. Within the Azure Active Directory overview menu, choose Enterprise Applications > All applications.
4. Select New application to add an application.
5. In the Add from the gallery section, type AWS Single-Account Access in the search box.
6. Select AWS Single-Account Access from results panel and then add the app. Wait a few seconds while the app is added to your tenant.

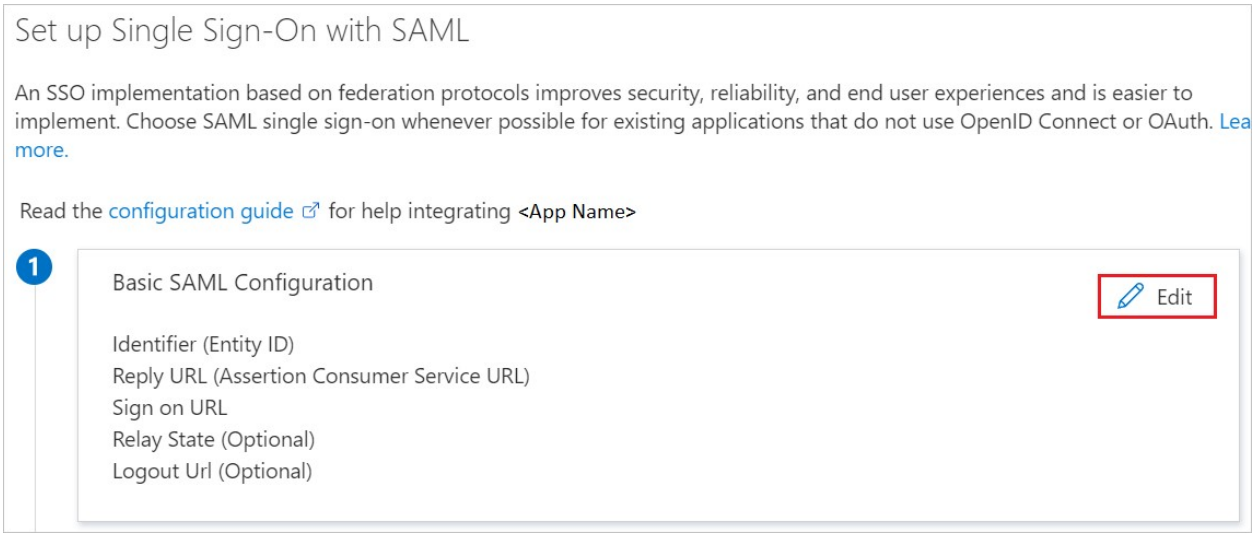
Alternatively, you can also use the Enterprise App Configuration Wizard

Configure Azure AD SSO

Follow these steps to enable Azure AD SSO in the Azure portal.

1. In the Azure portal, on the AWS Single-Account Access application integration page, find the Manage section and select single sign-on.
2. On the Select a single sign-on method page, select SAML.

3. On the Set up single sign-on with SAML page, click the pencil icon for Basic SAML Configuration to edit the settings.

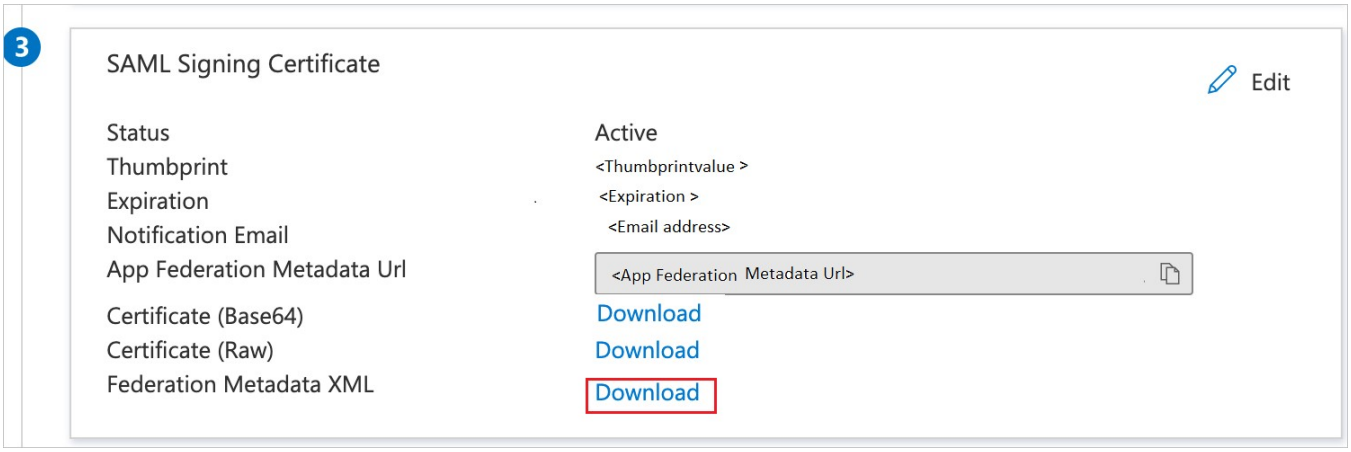


4. In the Basic SAML Configuration section, update both Identifier (Entity ID) and Reply URL with the same default value: `https://signin.aws.amazon.com/saml`. You must select Save to save the configuration changes.
5. When you are configuring more than one instance, provide an identifier value. From second instance onwards, use the following format, including a # sign to specify a unique SPN value.
   `https://signin.aws.amazon.com/saml#2`
6. AWS application expects the SAML assertions in a specific format, which requires you to add custom attribute mappings to your SAML token attributes configuration. The following screenshot shows the list of default attributes.

7. In addition to above, AWS application expects few more attributes to be passed back in SAML response which are shown below. These attributes are also pre populated but you can review them as per your requirements.

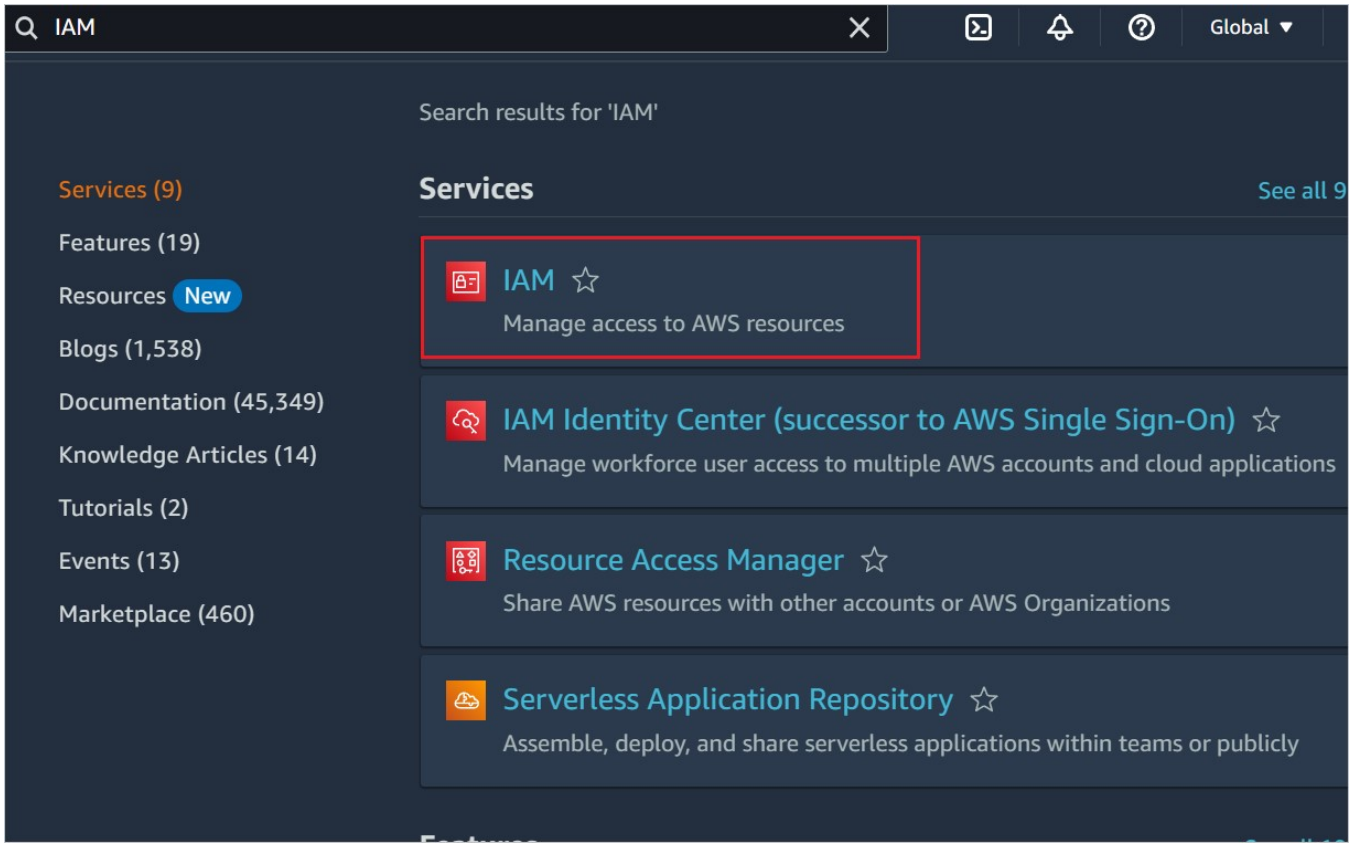
Name	Source attribute	Namespace
RoleSessionName	user.userprincipalname	`https://aws.amazon.com/SAML/Attributes`
Role	user.assignedroles	`https://aws.amazon.com/SAML/Attributes`
SessionDuration	"provide a value between 900 seconds (15 minutes) to 43200 seconds (12 hours)"	`https://aws.amazon.com/SAML/Attributes`

8. On the Set up Single Sign-On with SAML page, in the SAML Signing Certificate section, select Download to download the federation metadata XML file, and then save it to your computer.

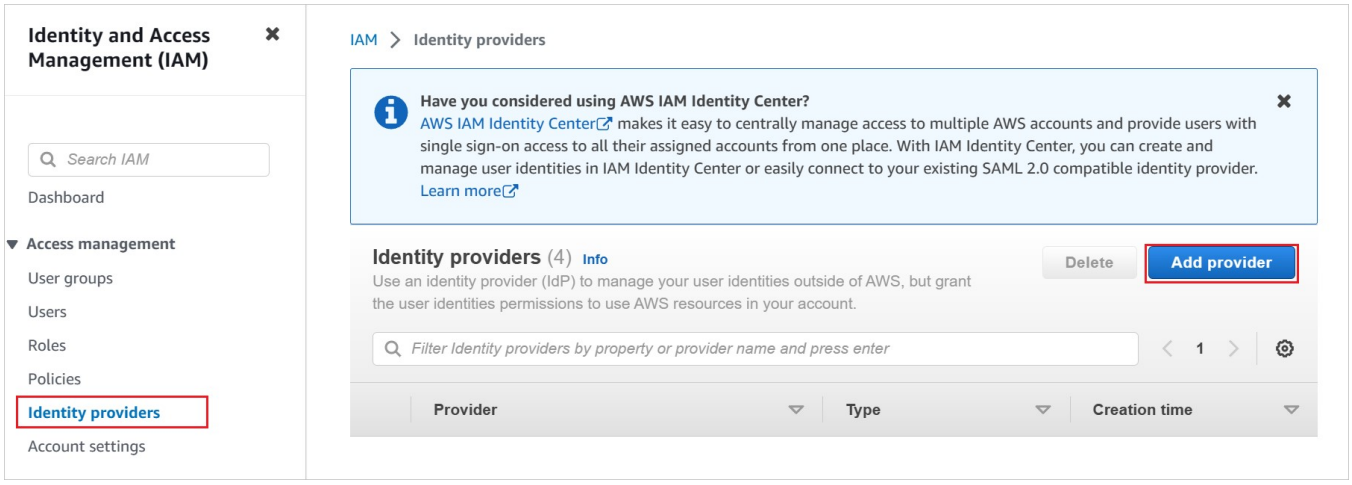


Configure AWS Single-Account Access SSO

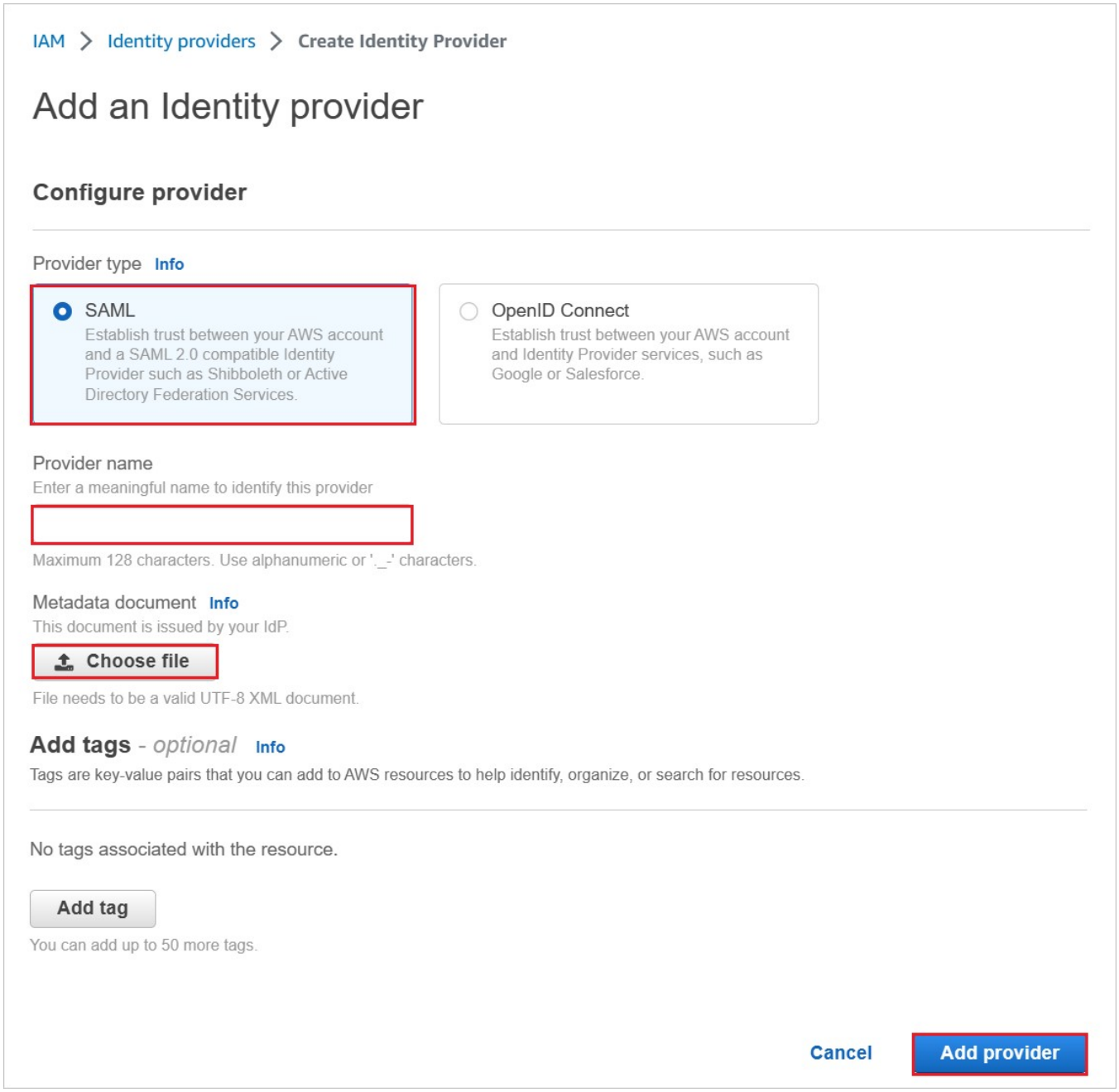
1. In a different browser window, sign-on to your AWS company site as an administrator.
2. In AWS home page, search for IAM and click it.



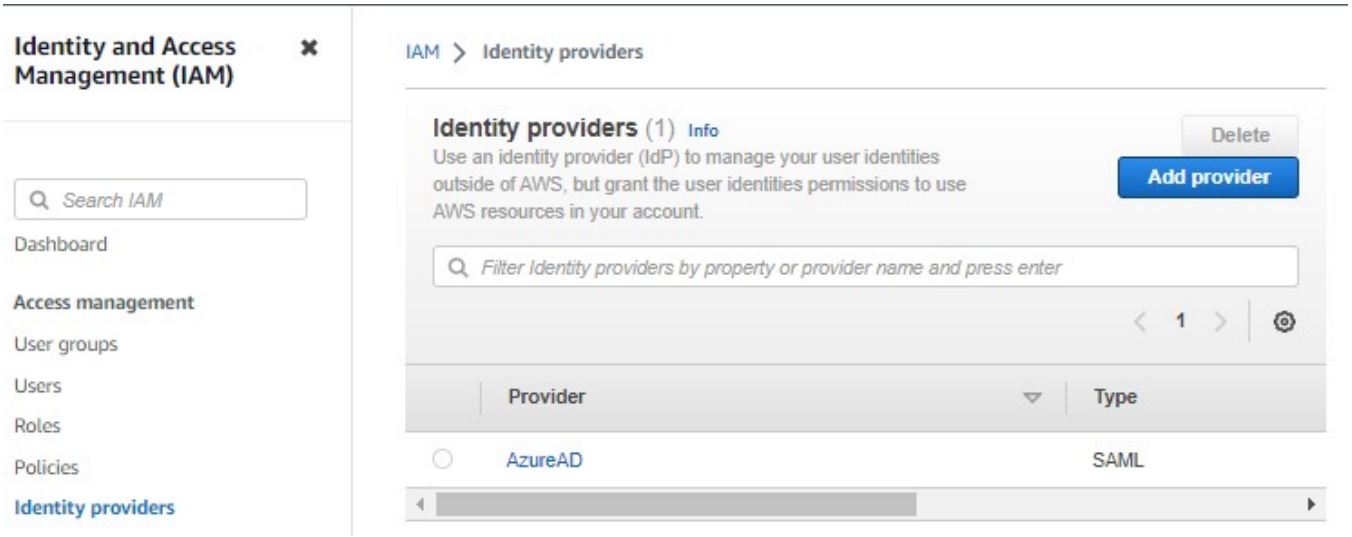
3. Go to Access management -> Identity Providers and click Add provider button.



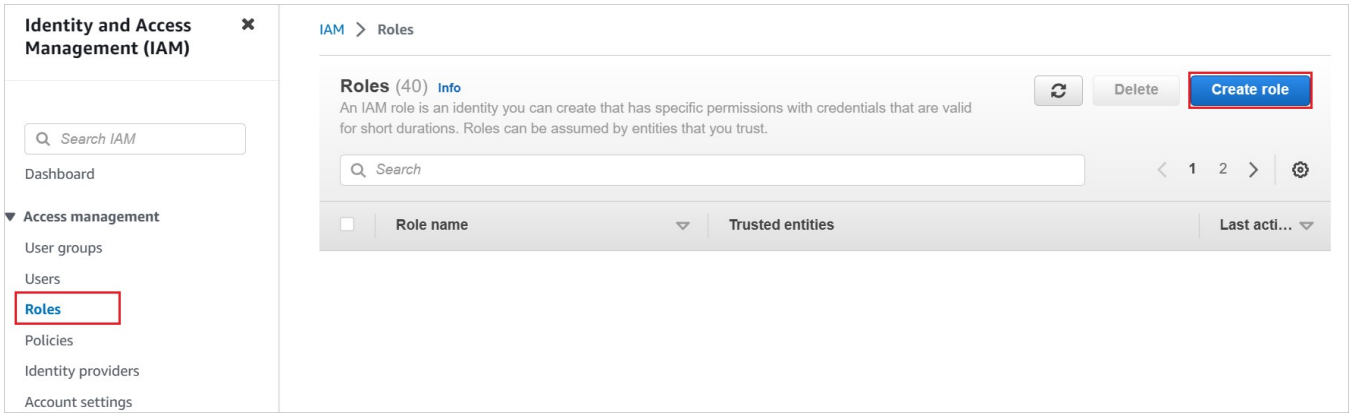
4. In the Add an Identity provider page, perform the following steps:



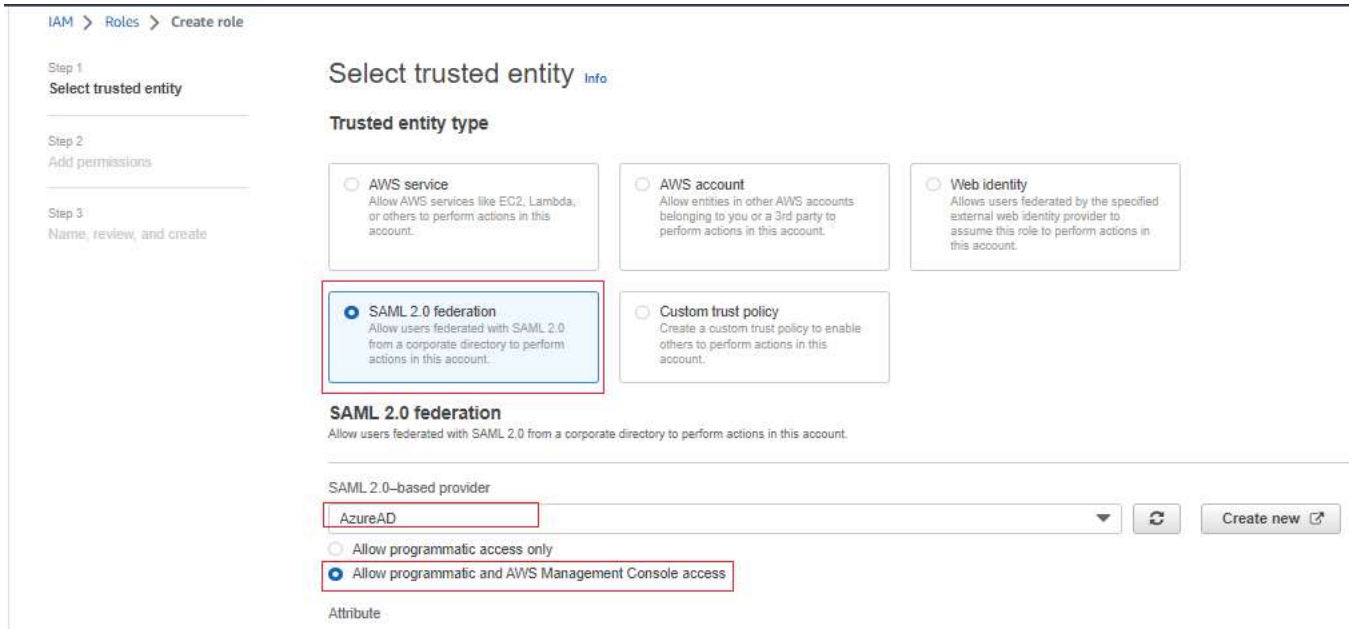
a. For Provider type, select SAML.
b. For Provider name, type a provider name (for example: *AzureAD*).
c. To upload your downloaded metadata file from the Azure portal, select Choose file.
d. Click Add provider.



5. Select Roles > Create role.



6. On the Create role page, perform the following steps:



a. Choose Trusted entity type, select SAML 2.0 federation.

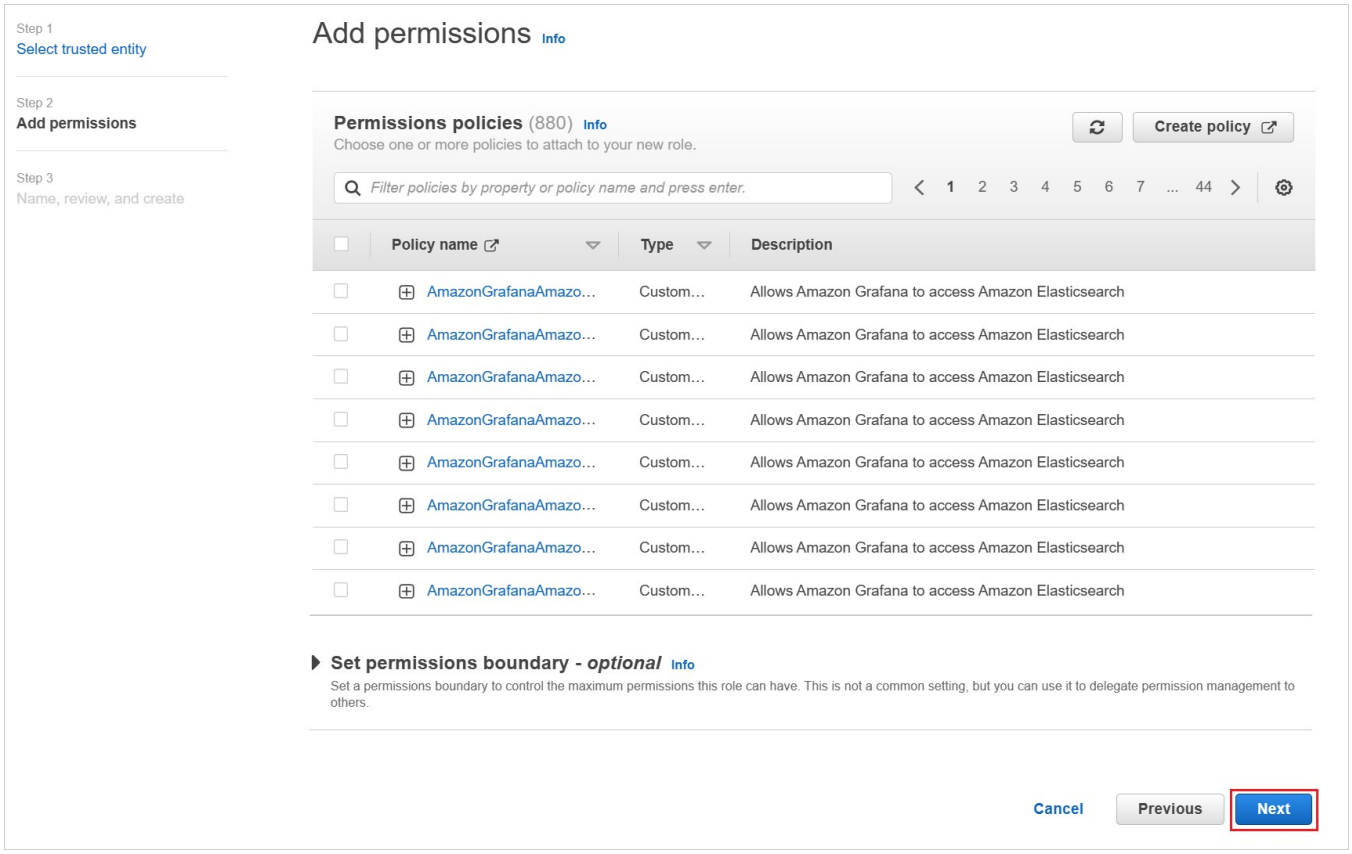
b. Under SAML 2.0 based provider, select the SAML provider you created previously

(for example: *AzureAd*).

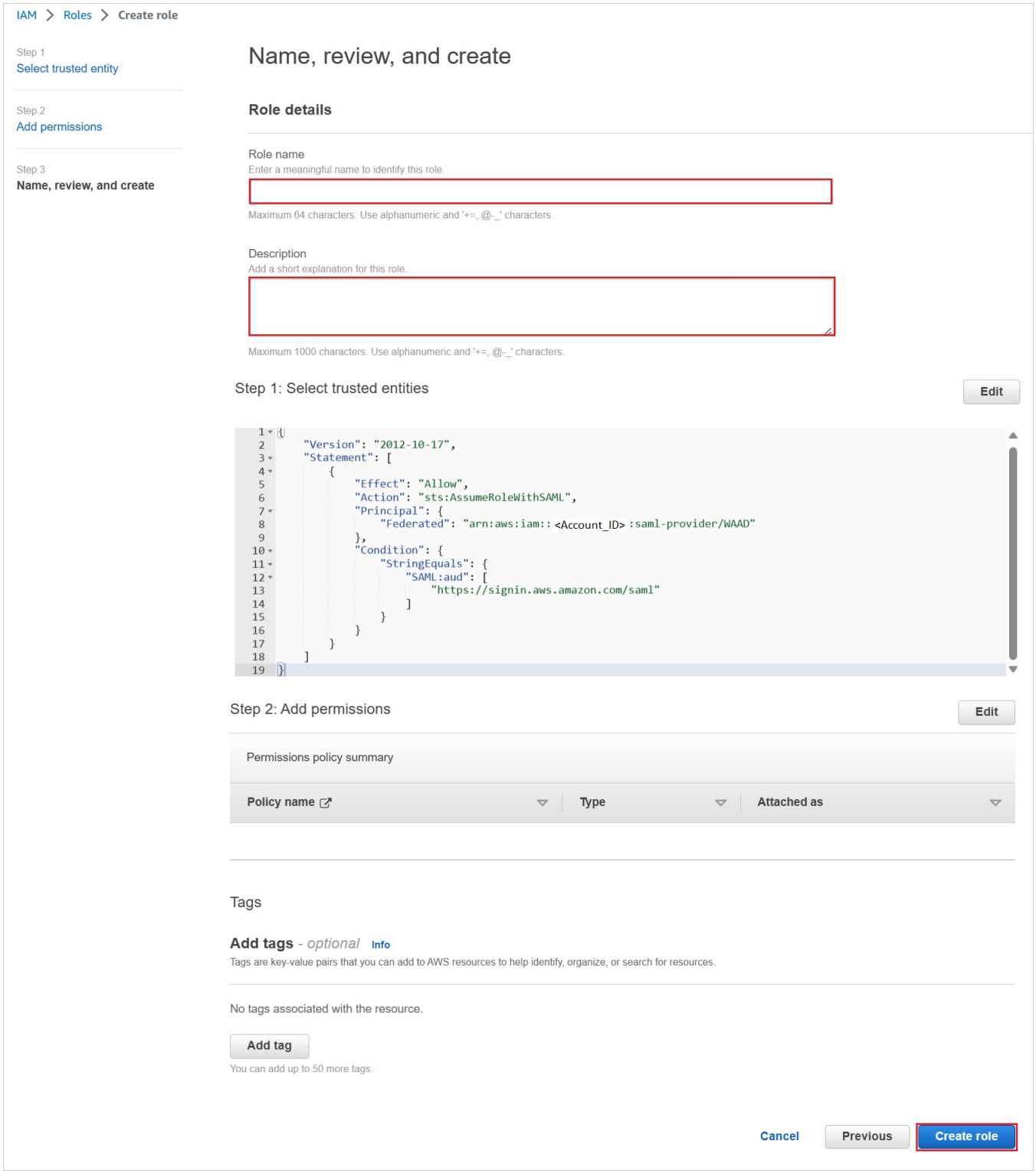
c. Select Allow programmatic and AWS Management Console access.

d. Select Next.

7. On the Permissions policies dialog box, attach the appropriate policy, per your organization. Then select Next.



8. On the Review dialog box, perform the following steps:



a. In Role name, enter your role name example **SysOps-Viewer** .

b. In Description, enter the role description.

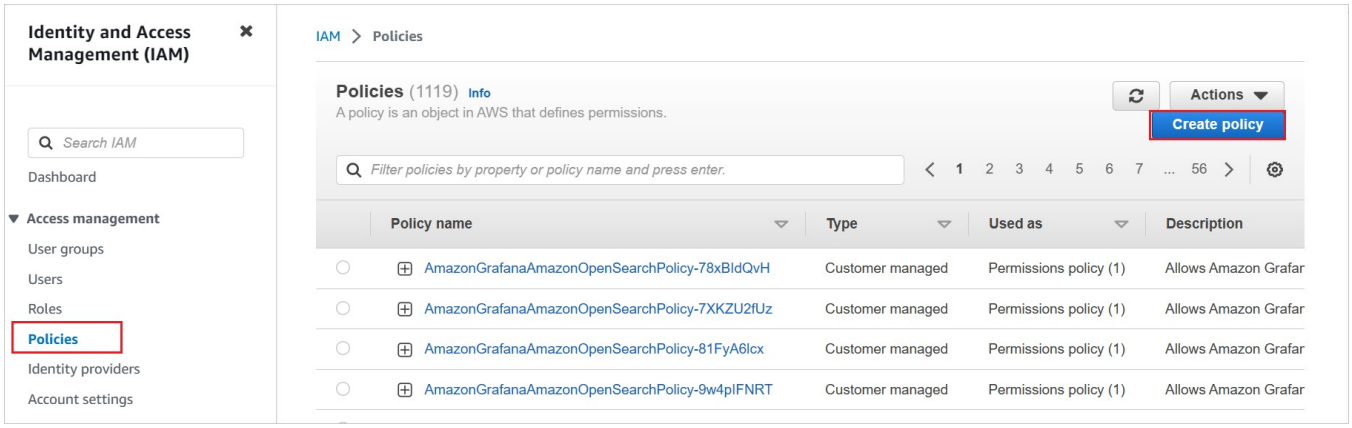
c. Select Create role.

d. Create as many roles as needed and map them to the Azure identity provider.

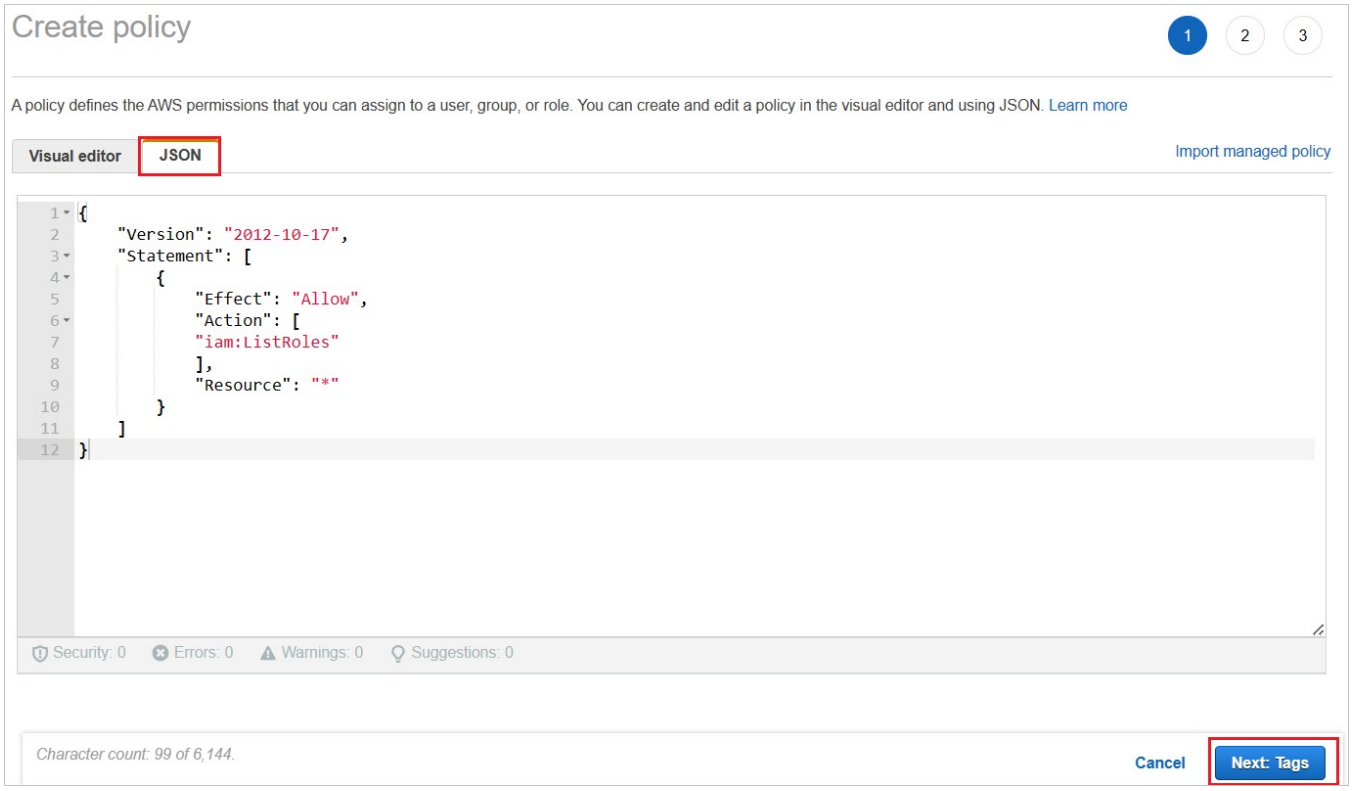
Role name	Trusted entities
billing-readonly	Identity Provider: arn:aws:iam::012094719592:saml-provider/AzureAD
SysOps-Role	Identity Provider: arn:aws:iam::012094719592:saml-provider/AzureAD
SysOps-Viewer	Identity Provider: arn:aws:iam::012094719592:saml-provider/AzureAD

Note: later these roles will be adeed to Azure Provisioning.

9. Use AWS service account credentials for fetching the roles from the AWS account in Azure AD user provisioning. For this, open the AWS console home.
10. In the IAM section, select Policies and click Create policy.



11. Create your own policy to fetch all the roles from AWS accounts.

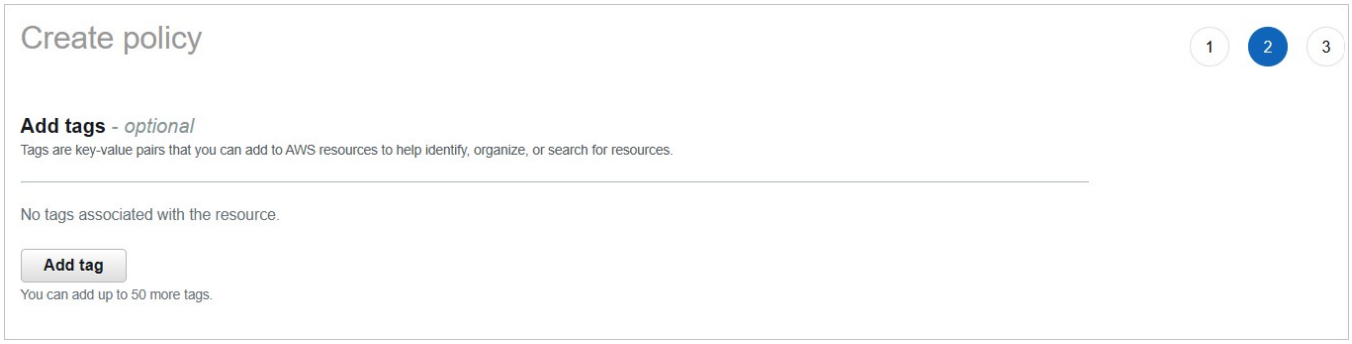


a. In Create policy, select the JSON tab.
b. In the policy document, add the following JSON:

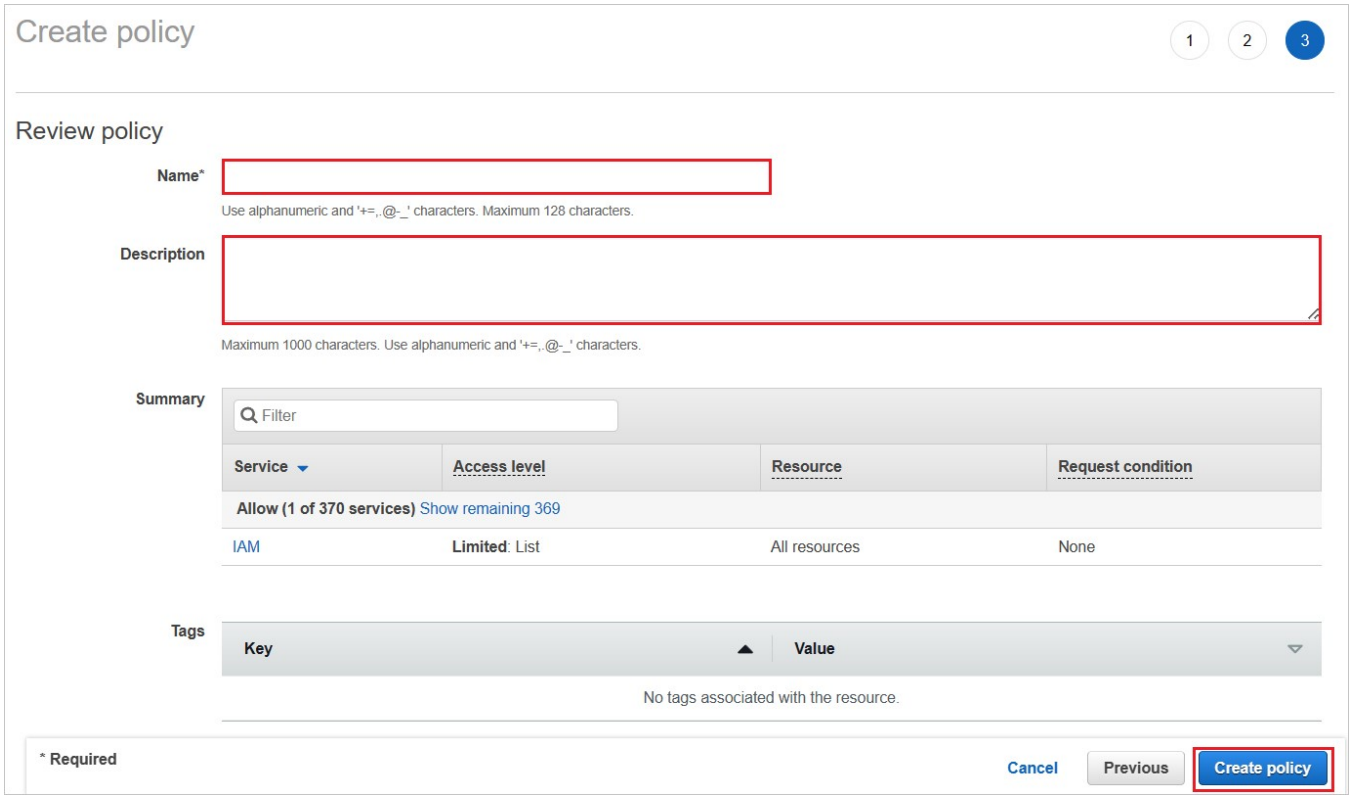
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

c. Click **Next: Tags.**

12. You can also add the required tags in the below page and click Next: Review.



13. Define the new policy.



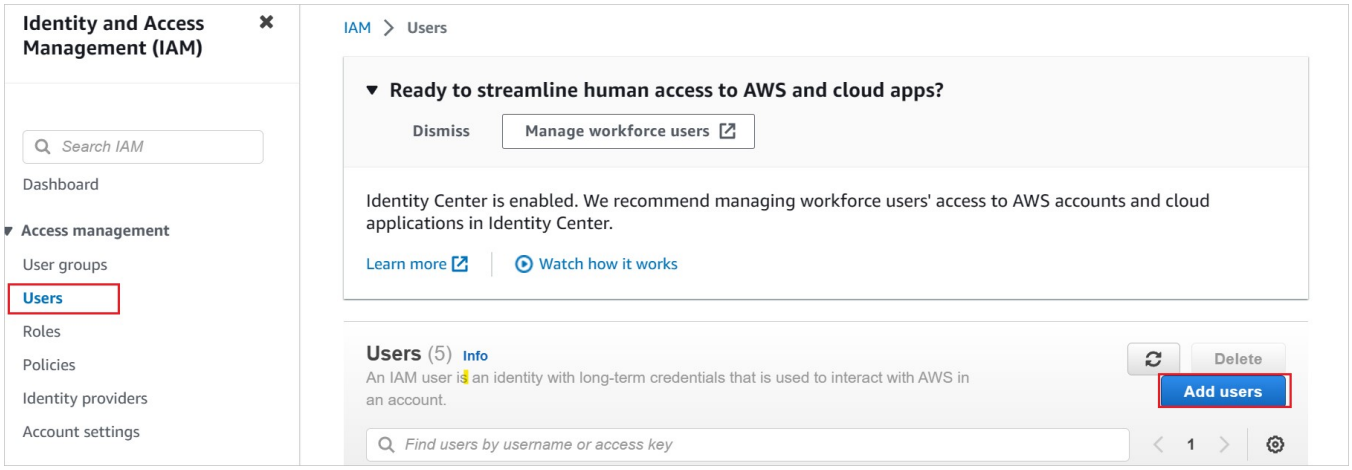
a. For Name, enter AzureAD_SSOUserRole_Policy.

b. For Description, enter This policy will allow to fetch the roles from AWS accounts.

c. Select Create policy.

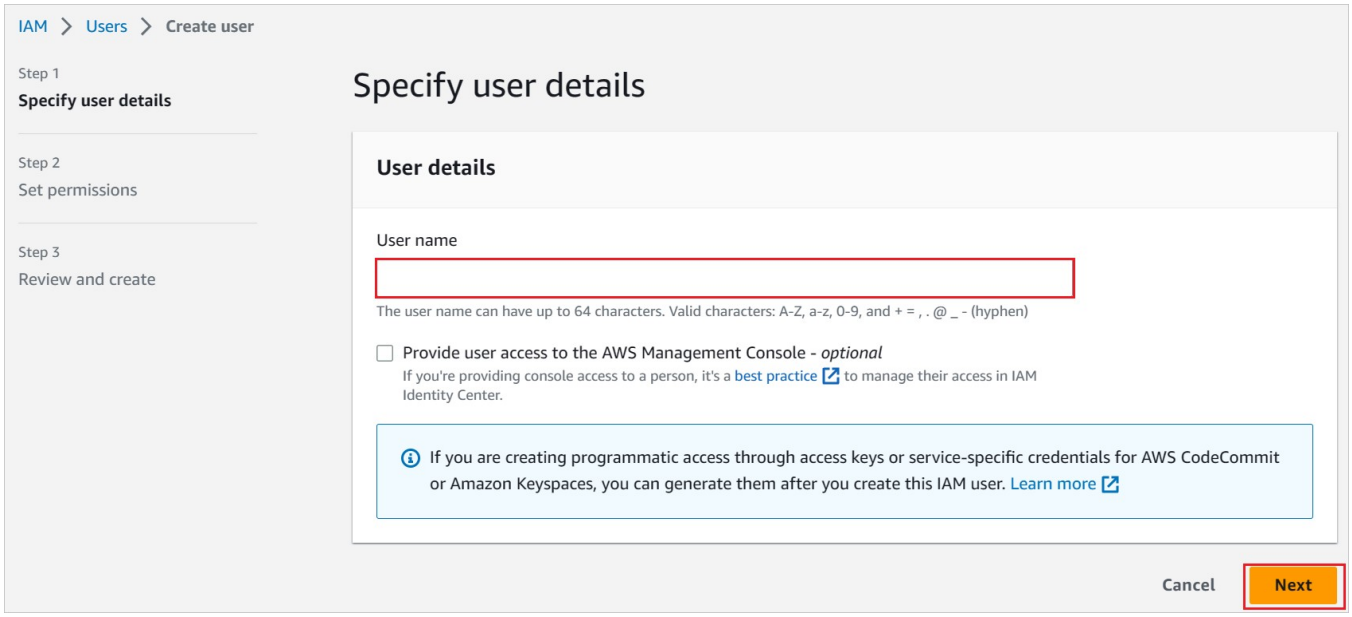
14. Create a new user account in the AWS IAM service.

a. In the AWS IAM console, select Users and click Add users.



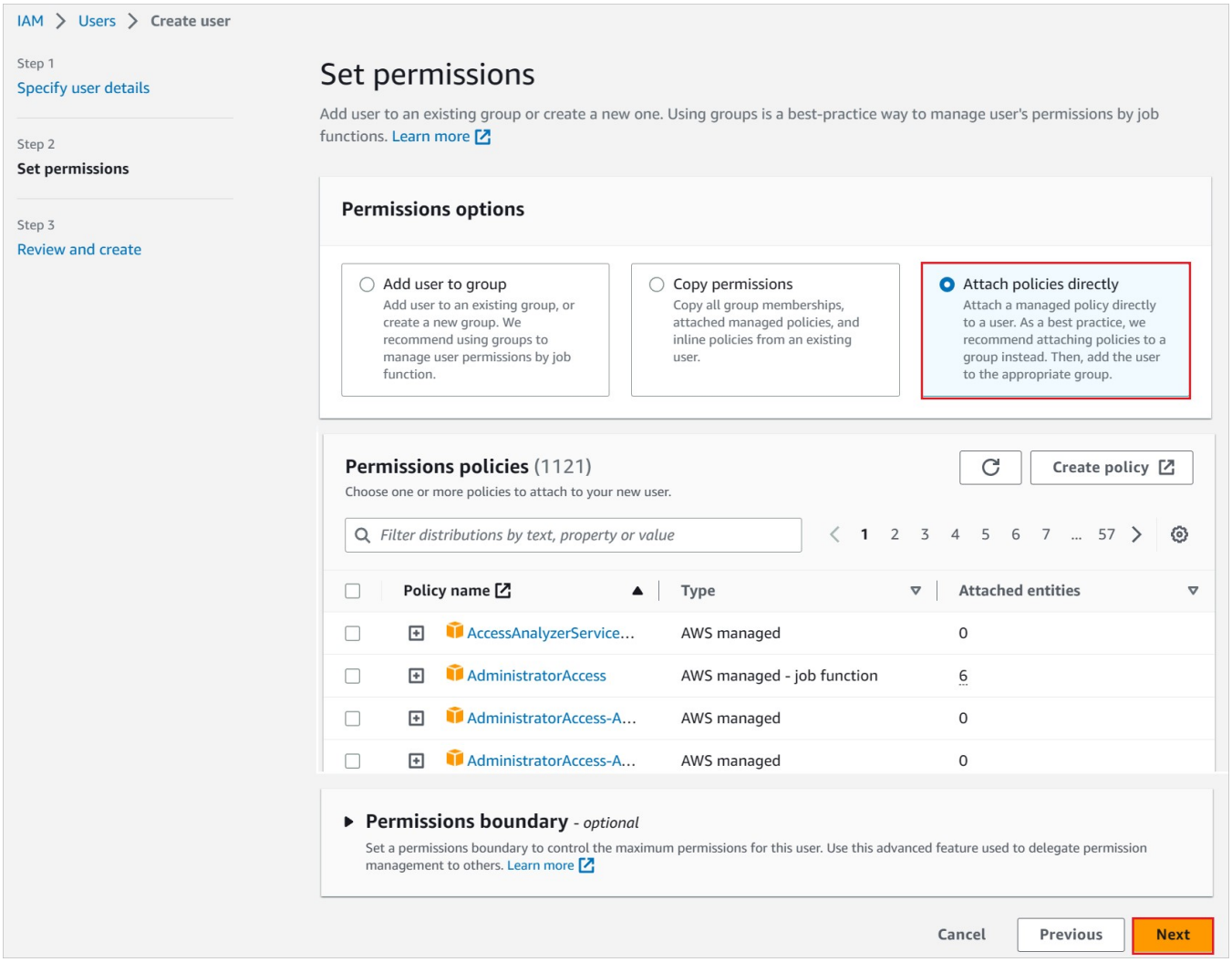
b. In the Specify user details section, enter the user name as AzureADRoleManager

and select Next.



Notes: Do not select "Aws Managment Console Access" because this credential only using by Azure ADProvsioning.

c. Create a new policy for this user.



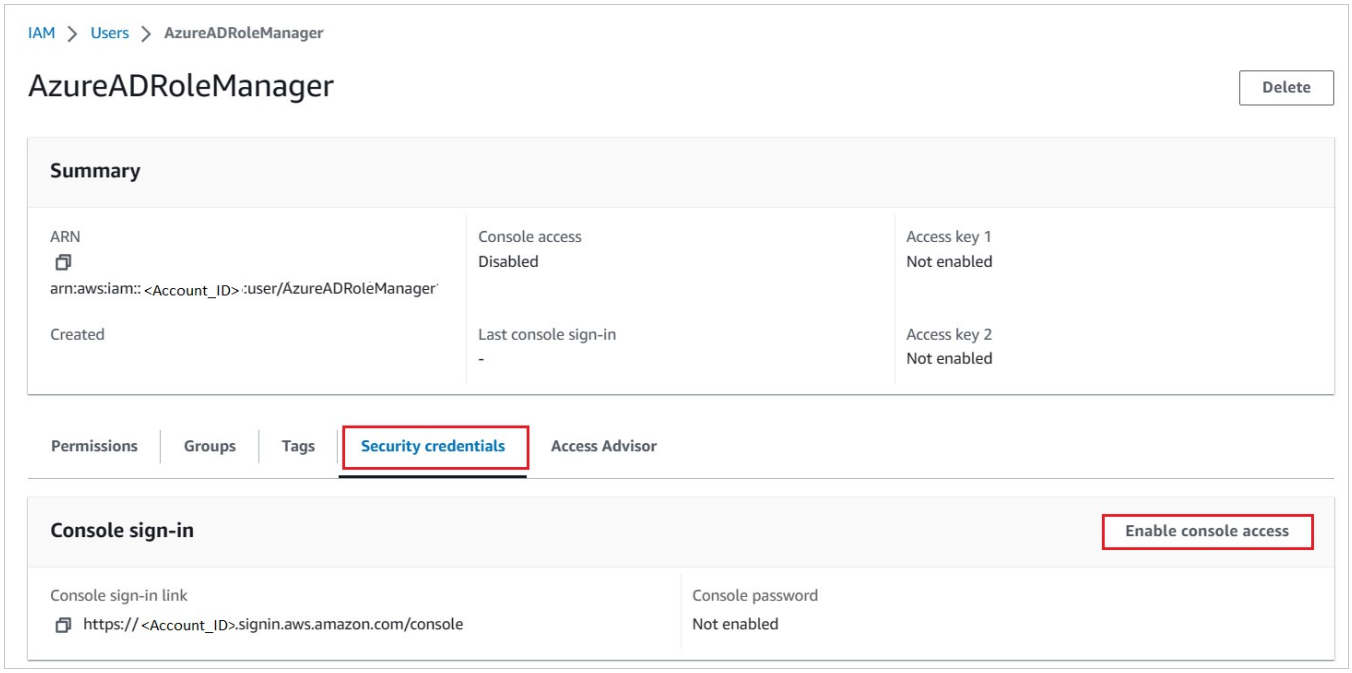
d. Select Attach existing policies directly.

e. Search for the newly created policy in the filter section AzureAD_SSOUserRole_Policy.

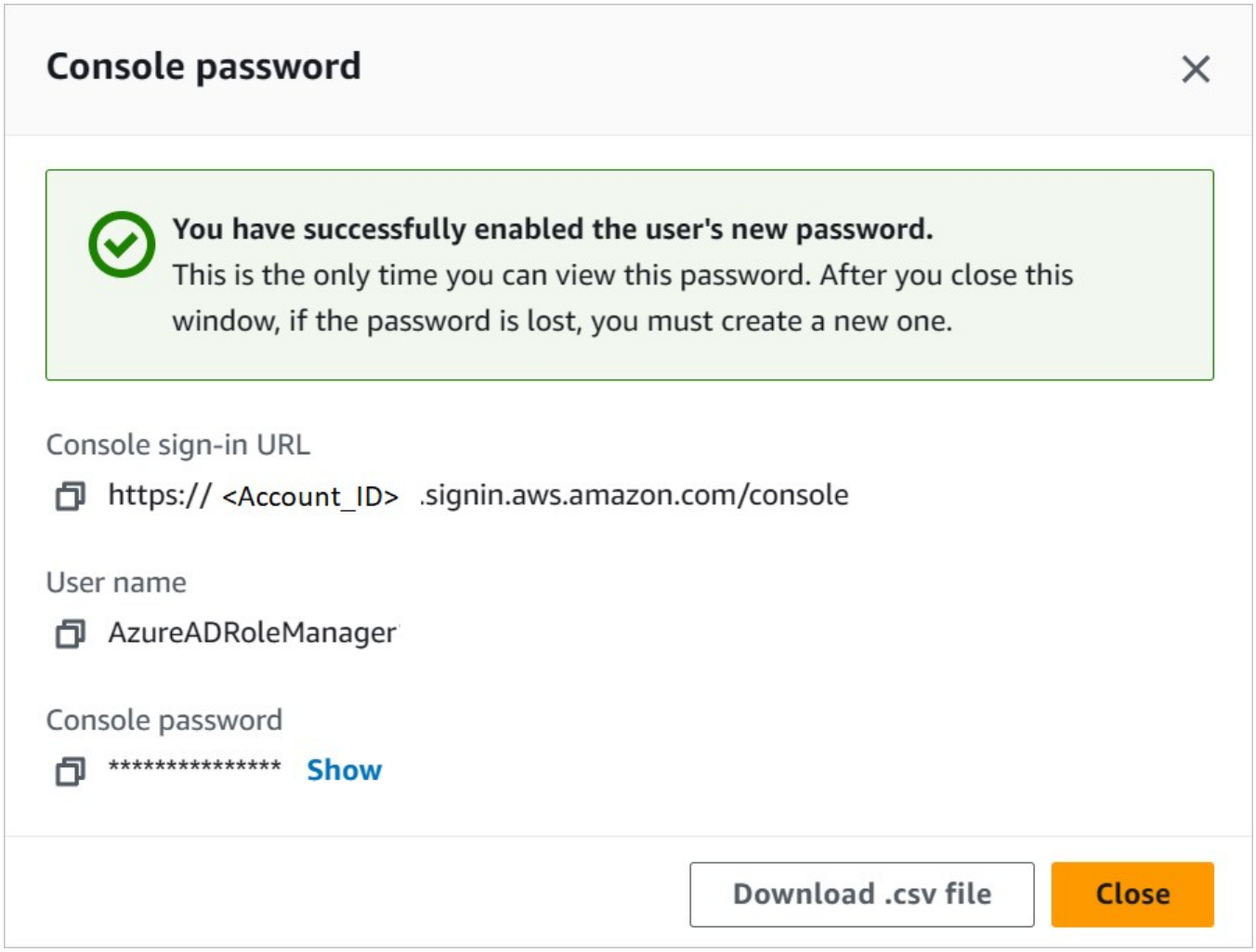
f. Select the policy, and then select Next.

15. Review your choices and select Create user.

16. To download the user credentials of a user, enable the console access in Security credentials tab.

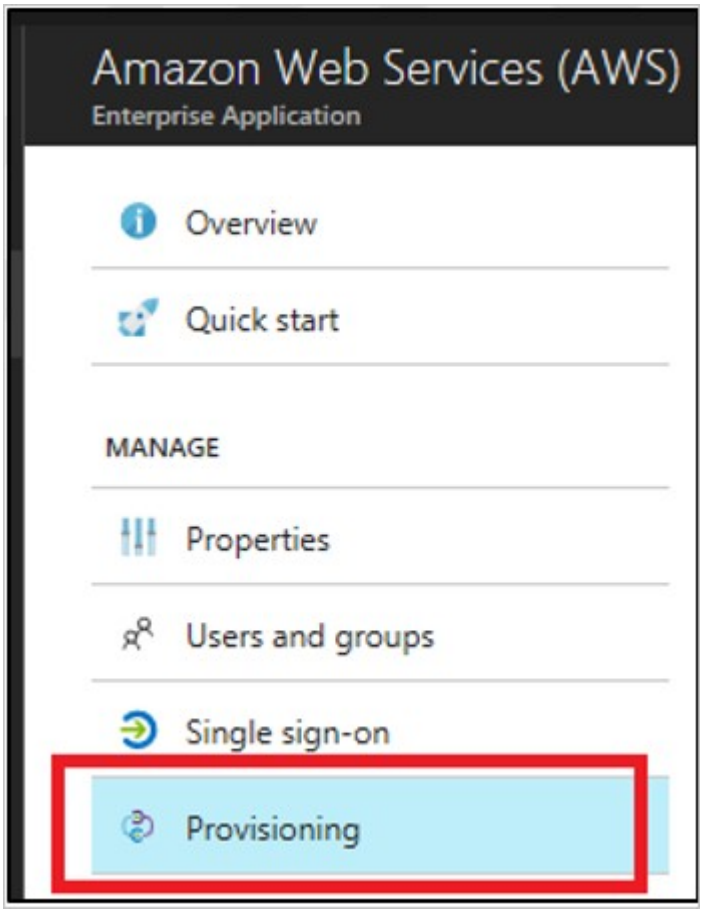


17. Enter these credentials into the Azure AD user provisioning section to fetch the roles from the AWS console.

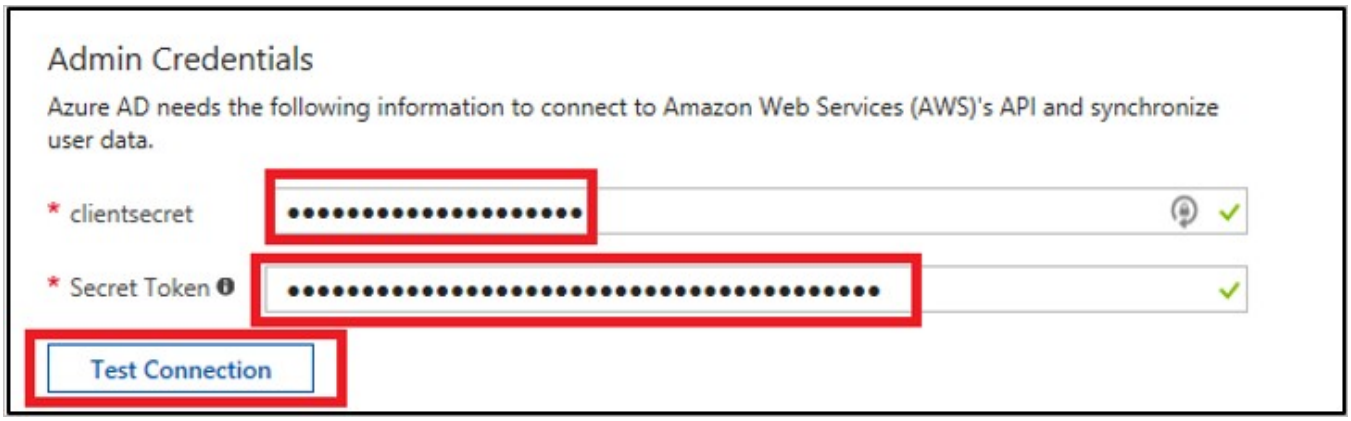


Configure role provisioning in AWS Single-Account Access

1. In the Azure AD management portal, in the AWS app, go to Provisioning.

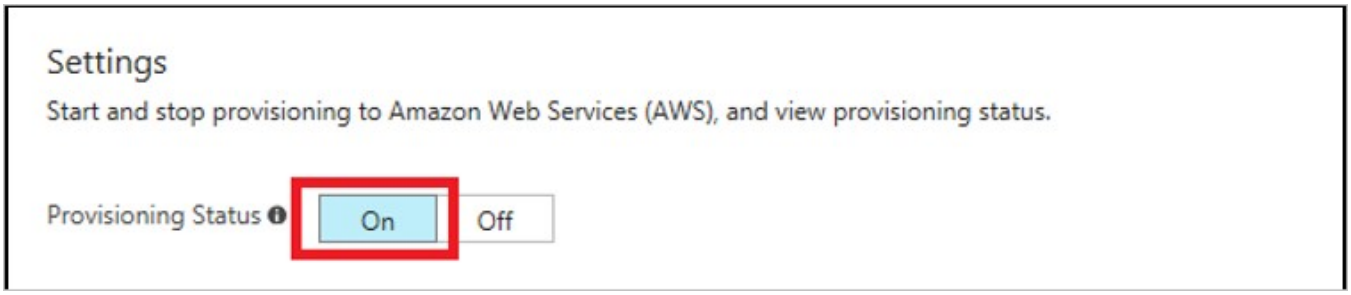


2. Enter the access key and secret in the clientsecret and Secret Token fields, respectively.



a. Enter the AWS user access key in the clientsecret field.
b. Enter the AWS user secret in the Secret Token field.
c. Select Test Connection.
d. Save the setting by selecting Save.

3. In the Settings section, for Provisioning Status, select On. Then select Save.



Create Azure AD user for AWS console access

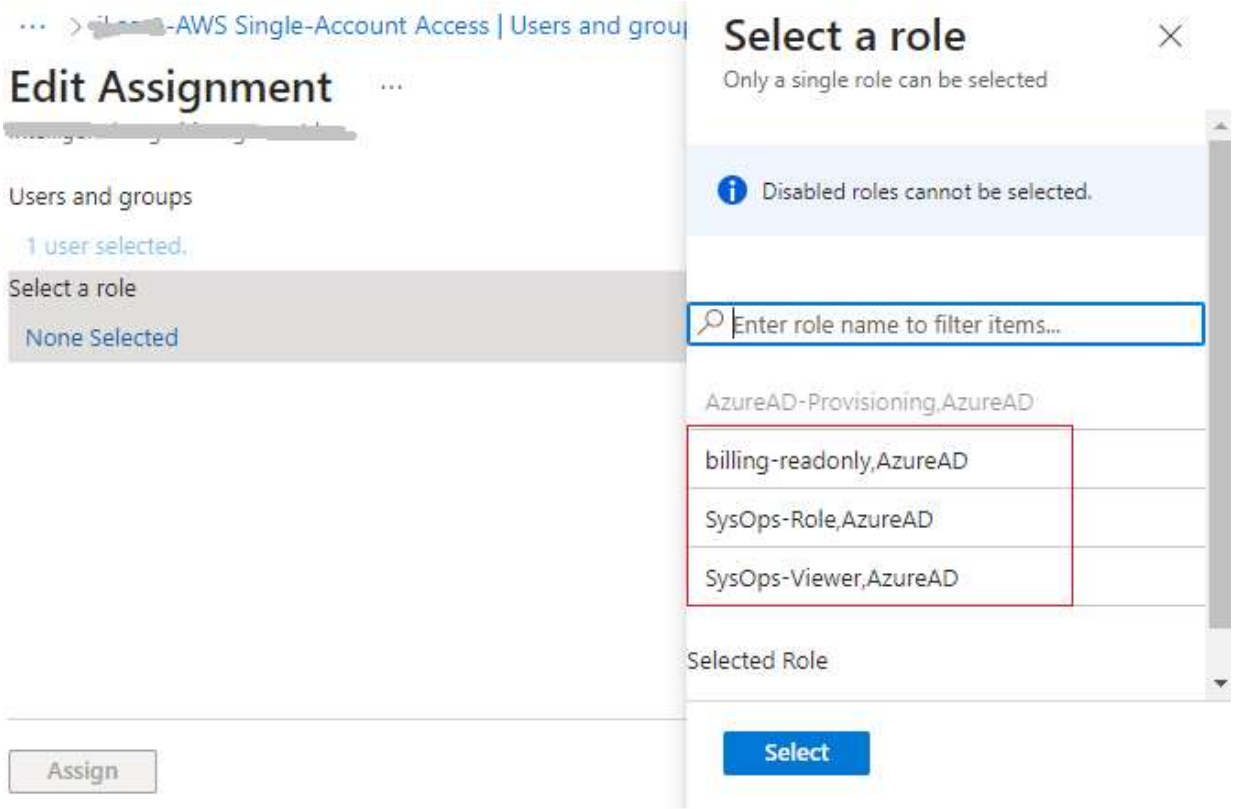
In this section, you'll create a test user in the Azure portal called Maruf.

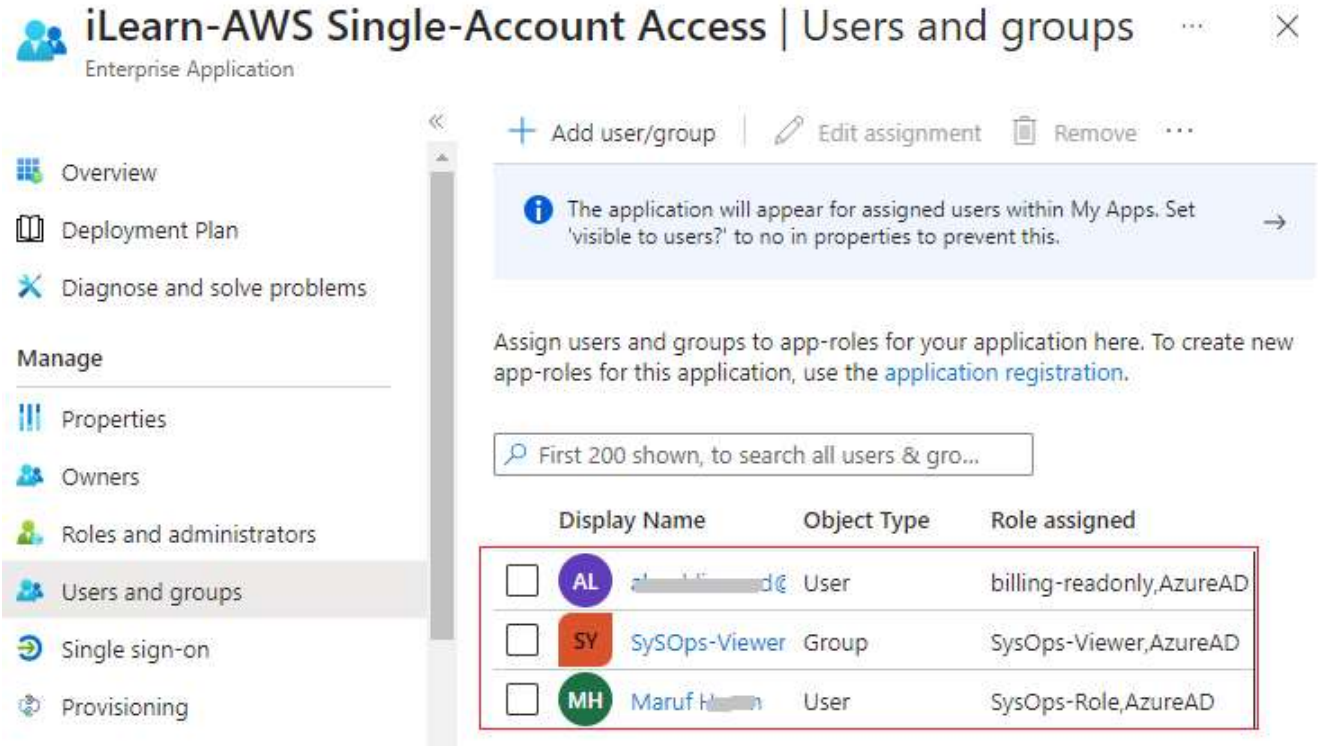
1. In the Azure portal, search for and select Azure Active Directory.
2. Within the Azure Active Directory overview menu, choose Users > All users.
3. Select New user at the top of the screen.
4. In the User properties, follow these steps:
    a. In the Name field, enter `maruf`
    b. In the User name field, enter the username@companydomain.extension. For example, `maruf@companydomain.com`.
    c. Select the Show password check box, and then write down the value that's displayed in the Password box.
    d. Click Create.

Assign the Azure AD user or group

In this section, you'll enable Maruf to use Azure single sign-on by granting access to AWS Single-Account Access.

1. In the Azure portal, select Enterprise Applications, and then select All applications.
2. In the applications list, select AWS Single-Account Access.
3. In the app's overview page, find the Manage section and select Users and groups.
4. Select Add user, then select Users and groups in the Add Assignment dialog.
5. In the Users and groups dialog, select B.Simon from the Users list, then click the Select button at the bottom of the screen.
6. If you are expecting a role to be assigned to the users, you can select it from the Select a role dropdown. If no role has been set up for this app, you see "Default Access" role selected.
7. In the Add Assignment dialog, click the Assign button.


-AWS Single-Account Access | Users and grou
Edit Assignment
Users and groups
1 user selected.
Select a role
None Selected
Assign
Select a role
Only a single role can be selected
Disabled roles cannot be selected.
Enter role name to filter items...
AzureAD-Provisioning,AzureAD
billing-readonly,AzureAD
SysOps-Role,AzureAD
SysOps-Viewer,AzureAD
Selected Role
Select


iLearn-AWS Single-Account Access | Users and groups
Enterprise Application
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Add user/group
Edit assignment
Remove
The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.
Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.
First 200 shown, to search all users & gro...
Display Name
Object Type
Role assigned
AL
User
billing-readonly,AzureAD
SY
SySOps-Viewer
Group
SysOps-Viewer,AzureAD
MH
Maruf
User
SysOps-Role,AzureAD

Test SSO

In this section, you test your Azure AD single sign-on configuration with following options.

After log in to https://myapplications.microsoft.com/ using you Azure ID you will find the aws application name to log in AWS console.