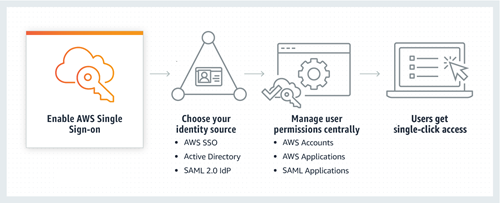
|  |
| --- |
|  |

|  |
| --- |
|  |
| Azure AD and AWS IAM Identity Center (AWS SSO Integration) |
|  |

**AWS Single Sign-On (SSO) with Azure Active Directory (AD)**

# AWS SSO now provides a directory that you can use to create users, organize them into groups, and set permissions across those groups. You can also grant the users that you create in AWS SSO permissions to applications such as Office 365 and Azure AD.



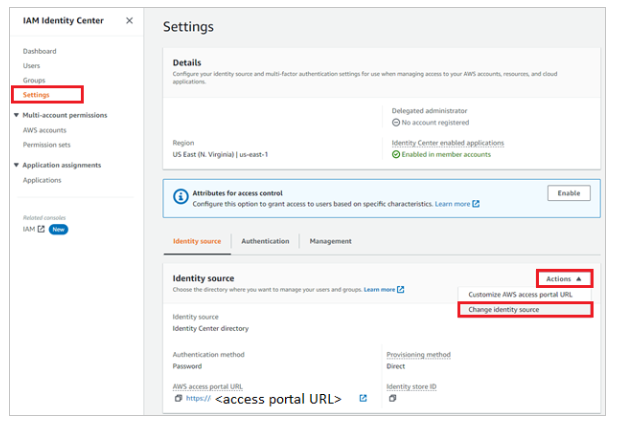
AWS SSO also helps us manage access and permissions to commonly used third-party software. AWS SSO-integrated applications as well as custom applications that support [Security Assertion Markup Language (SAML) 2.0](https://auth0.com/blog/how-saml-authentication-works/).

AWS SSO includes a user portal where your end-users can find and access all their assigned AWS accounts, cloud applications, and custom applications in one place.

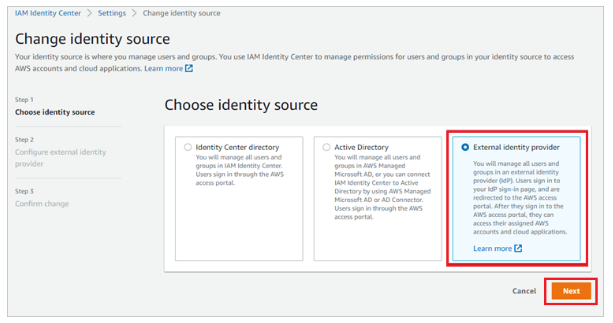
To configure AWS SSO with Azure Active Directory, follow the Steps As Below

**Step 1:**

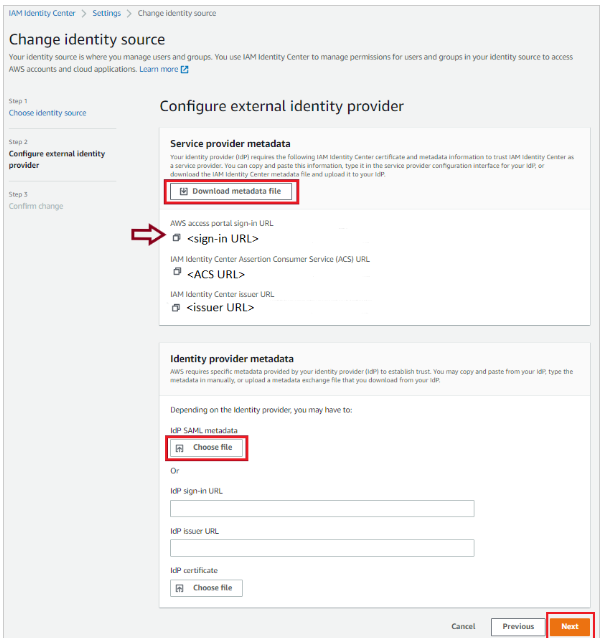
* Go to AWS Console and select **AWS IAM Identity Center** from the console.
* In the left navigation pane, choose **Settings**
* On the **Settings** page, find **Identity source**, click on **Actions** pull-down menu, and select Change **identity source**.



* On the Change identity source page, choose **External identity provider**.



* Perform the below steps in the **Configure external identity provider** section:



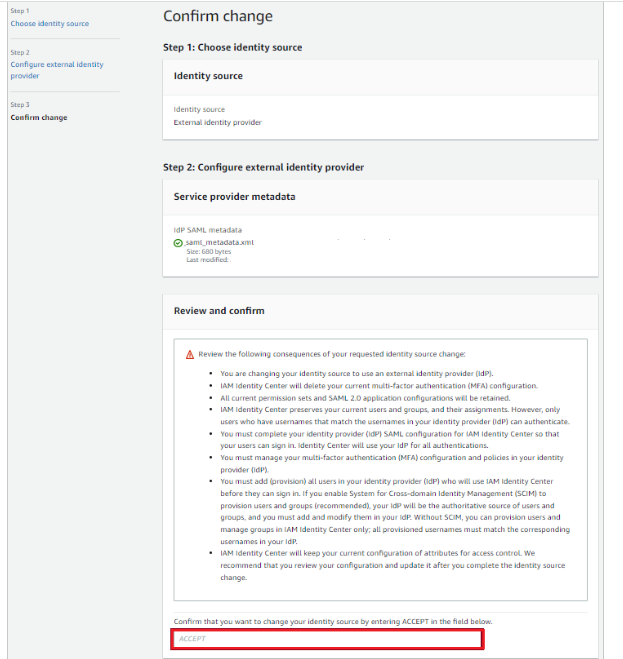
a. In the **Service provider metadata** section, find **AWS SSO SAML metadata**, select **Download metadata file** to download the metadata file and save it on your computer and use this metadata file to upload on Azure portal.

b. Copy **AWS access portal sign-in URL** value, paste this value into the **Sign on URL** text box in the **Basic SAML Configuration section** in the Azure portal.

c. In the **Identity provider metadata** section, select **Choose file** to upload the metadata file which you have downloaded from the Azure portal.

d. Choose **Next: Review**.

* In the text box, type **ACCEPT** to change the identity source.





**Step 4:**

## On Azure Cloud Portal, Add AWS IAM Identity Center from the gallery

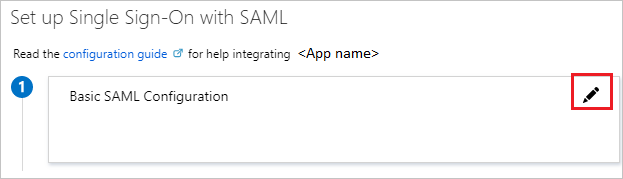
To configure the integration of AWS IAM Identity Center into Azure AD, you need to add AWS IAM Identity Center from the gallery to your list of managed SaaS apps.

1. Sign in to the Azure portal using either a work or school account, or a personal Microsoft account.
2. On the left navigation pane, select the **Azure Active Directory** service.
3. Navigate to **Enterprise Applications** and then select **All Applications**.
4. To add new application, select **New application**.
5. In the **Add from the gallery** section, type **AWS IAM Identity Center** in the search box.
6. Select **AWS IAM Identity Center** from results panel and then add the app. Wait a few seconds while the app is added to your tenant.

## Configure Azure AD SSO

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

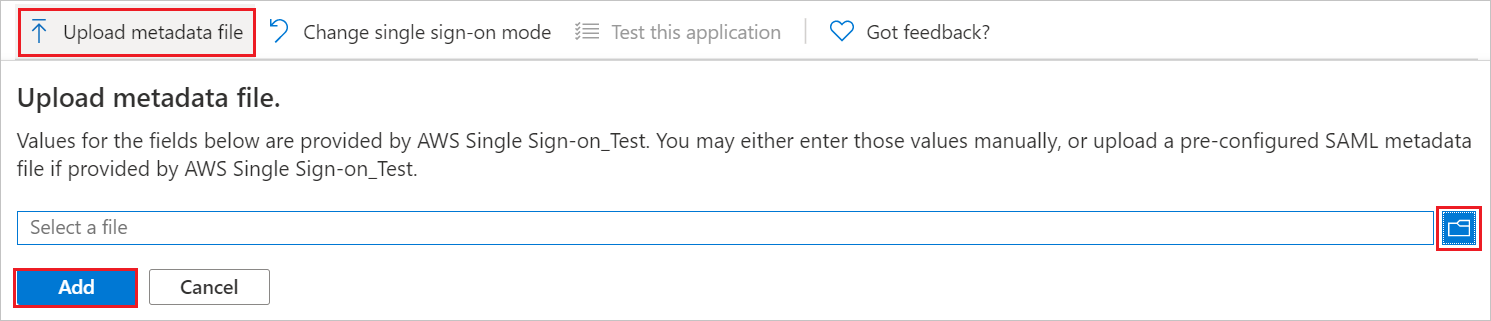
1. In the Azure portal, on the **AWS IAM Identity Center** application integration page, find the **Manage** section and select **single sign-on**.
2. On the **Select a single sign-on method** page, select **SAML**.
3. On the **Set up single sign-on with SAML** page, click the pencil icon for **Basic SAML Configuration** to edit the settings.



1. If you have **Service Provider metadata file**, on the **Basic SAML Configuration** section, perform the following steps:

a. Click **Upload metadata file**.

b. Click on **folder logo** to select metadata file which is explained to download in [**Configure AWS IAM Identity Center SSO**](https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/aws-single-sign-on-tutorial#configure-aws-iam-identity-center-sso) section and click **Add**.

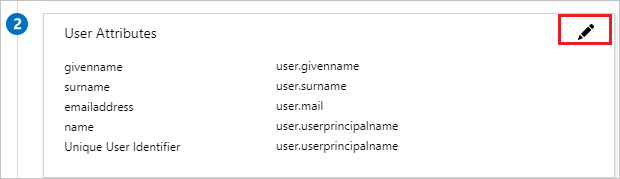


c. Once the metadata file is successfully uploaded, the **Identifier** and **Reply URL** values get auto populated in Basic SAML Configuration section.

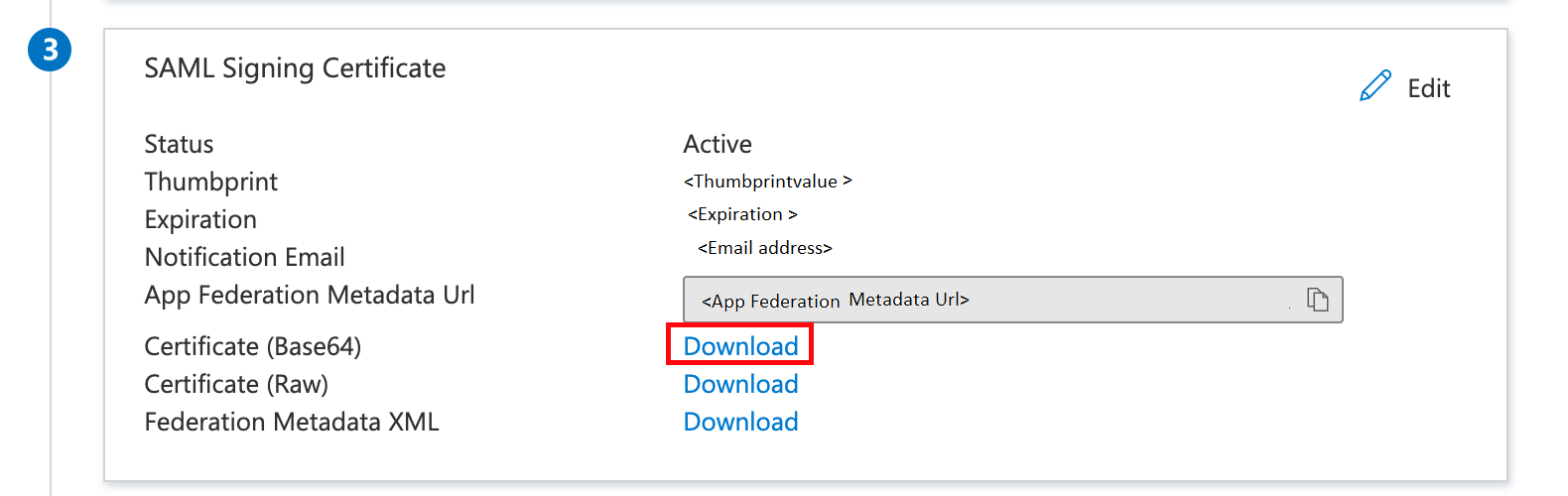
1. Click **Set additional URLs** and perform the following step if you wish to configure the application in **SP** initiated mode:

In the **Sign-on URL** text box, type a URL using the following pattern: https://portal.sso.<REGION>.amazonaws.com/saml/assertion/<ID>

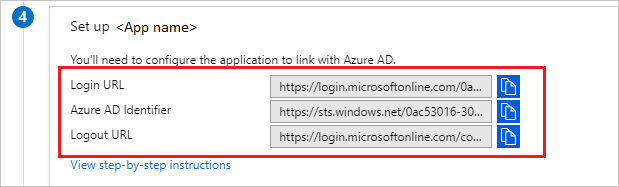
1. AWS IAM Identity Center application expects the SAML assertions in a specific format, which requires you to add custom attribute mappings to your SAML token attributes configuration. The following screenshot shows the list of default attributes.



1. On the **Set up single sign-on with SAML** page, in the **SAML Signing Certificate** section, find **Certificate(Base64)** and select **Download** to download the certificate and save it on your computer.



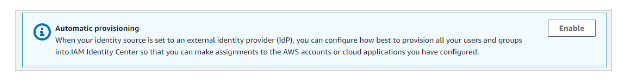
1. On the Set up AWS IAM Identity Center section, copy the appropriate URL(s) based on your requirement.

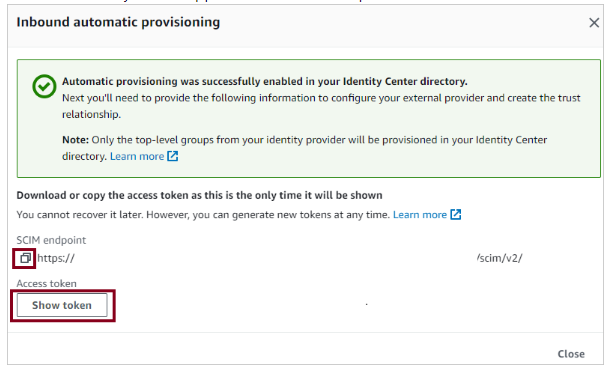


## Step 1. Plan your provisioning deployment

1. Learn about [how the provisioning service works](https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/user-provisioning).
2. Determine who will be in [scope for provisioning](https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/define-conditional-rules-for-provisioning-user-accounts).
3. Determine what data to [map between Azure AD and AWS IAM Identity Center](https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/customize-application-attributes).

## Step 2. Configure AWS IAM Identity Center to support provisioning with Azure AD

1. Open the [AWS IAM Identity Center](https://console.aws.amazon.com/singlesignon).
2. Choose **Settings** in the left navigation pane
3. In **Settings**, click on Enable in the Automatic provisioning section. 
4. In the Inbound automatic provisioning dialog box, copy and save the **SCIM endpoint** and **Access Token** (visible after clicking on Show Token). These values will be entered in the **Tenant URL** and **Secret Token** field in the Provisioning tab of your AWS IAM Identity Center application in the Azure portal.



## Step 3. Add AWS IAM Identity Center from the Azure AD application gallery

Add AWS IAM Identity Center from the Azure AD application gallery to start managing provisioning to AWS IAM Identity Center. If you have previously setup AWS IAM Identity Center for SSO, you can use the same application. Learn more about adding an application from the gallery [here](https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal).

## Step 4. Define who will be in scope for provisioning

The Azure AD provisioning service allows you to scope who will be provisioned based on assignment to the application and or based on attributes of the user / group. If you choose to scope who will be provisioned to your app based on assignment, you can use the following [steps](https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal) to assign users and groups to the application. If you choose to scope who will be provisioned based solely on attributes of the user or group, you can use a scoping filter as described [here](https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/define-conditional-rules-for-provisioning-user-accounts).

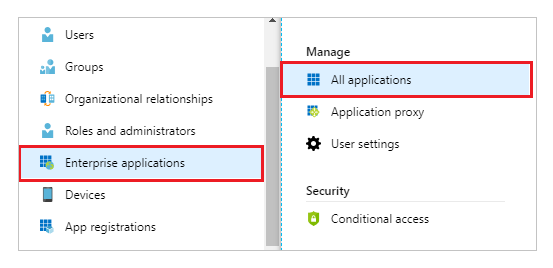
* Start small. Test with a small set of users and groups before rolling out to everyone. When scope for provisioning is set to assigned users and groups, you can control this by assigning one or two users or groups to the app. When scope is set to all users and groups, you can specify an [attribute based scoping filter](https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/define-conditional-rules-for-provisioning-user-accounts).
* If you need additional roles, you can [update the application manifest](https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-add-app-roles-in-azure-ad-apps) to add new roles.

## Step 5. Configure automatic user provisioning to AWS IAM Identity Center

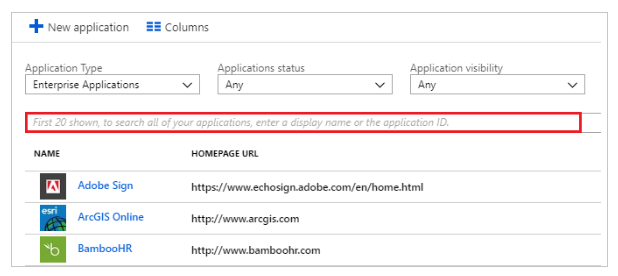
This section guides you through the steps to configure the Azure AD provisioning service to create, update, and disable users and/or groups in TestApp based on user and/or group assignments in Azure AD.

### To configure automatic user provisioning for AWS IAM Identity Center in Azure AD:

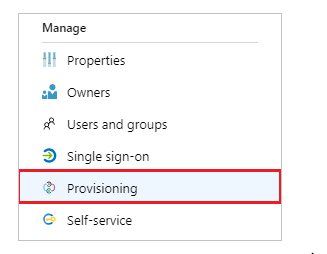
1. Sign in to the [Azure portal](https://portal.azure.com/). Select **Enterprise Applications**, then select **All applications**.



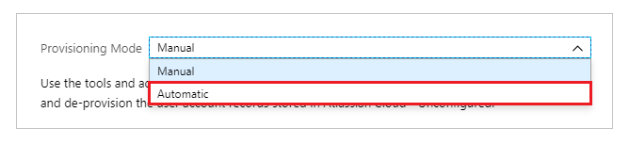
1. In the applications list, select **AWS IAM Identity Center**.



1. Select the **Provisioning** tab.



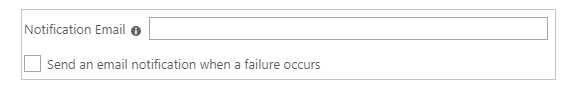
1. Set the **Provisioning Mode** to **Automatic**.



1. Under the **Admin Credentials** section, input your AWS IAM Identity Center **Tenant URL** and **Secret Token** retrieved earlier in Step 2. Click **Test Connection** to ensure Azure AD can connect to AWS IAM Identity Center.



1. In the **Notification Email** field, enter the email address of a person or group who should receive the provisioning error notifications and select the **Send an email notification when a failure occurs** check box.



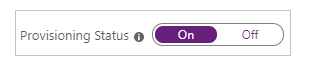
1. Select **Save**.
2. Under the **Mappings** section, select **Synchronize Azure Active Directory Users to AWS IAM Identity Center**.
3. Review the user attributes that are synchronized from Azure AD to AWS IAM Identity Center in the **Attribute-Mapping** section. The attributes selected as **Matching** properties are used to match the user accounts in AWS IAM Identity Center for update operations. If you choose to change the [matching target attribute](https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/customize-application-attributes), you will need to ensure that the AWS IAM Identity Center API supports filtering users based on that attribute. Select the **Save** button to commit any changes.

| **Attribute** | **Type** | **Supported for Filtering** |
| --- | --- | --- |
| userName | String | ✓ |
| active | Boolean |  |
| displayName | String |  |
| title | String |  |
| emails[type eq "work"].value | String |  |
| preferredLanguage | String |  |
| name.givenName | String |  |
| name.familyName | String |  |
| name.formatted | String |  |
| addresses[type eq "work"].formatted | String |  |
| addresses[type eq "work"].streetAddress | String |  |
| addresses[type eq "work"].locality | String |  |
| addresses[type eq "work"].region | String |  |
| addresses[type eq "work"].postalCode | String |  |
| addresses[type eq "work"].country | String |  |
| phoneNumbers[type eq "work"].value | String |  |
| externalId | String |  |
| locale | String |  |
| timezone | String |  |
| urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNumber | String |  |
| urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department | String |  |
| urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:division | String |  |
| urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:costCenter | String |  |
| urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization | String |  |
| urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:manager | Reference |  |

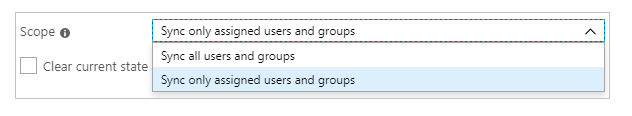
1. Under the **Mappings** section, select **Synchronize Azure Active Directory Groups to AWS IAM Identity Center**.
2. Review the group attributes that are synchronized from Azure AD to AWS IAM Identity Center in the **Attribute-Mapping** section. The attributes selected as **Matching** properties are used to match the groups in AWS IAM Identity Center for update operations. Select the **Save** button to commit any changes.

| **Attribute** | **Type** | **Supported for Filtering** |
| --- | --- | --- |
| displayName | String | ✓ |
| externalId | String |  |
| members | Reference |  |

1. To configure scoping filters, refer to the following instructions provided in the [Scoping filter tutorial](https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/define-conditional-rules-for-provisioning-user-accounts).
2. To enable the Azure AD provisioning service for AWS IAM Identity Center, change the **Provisioning Status** to **On** in the **Settings** section.



1. Define the users and/or groups that you would like to provision to AWS IAM Identity Center by choosing the desired values in **Scope** in the **Settings** section.



1. When you are ready to provision, click **Save**.



This operation starts the initial synchronization cycle of all users and groups defined in **Scope** in the **Settings** section. The initial cycle takes longer to perform than subsequent cycles, which occur approximately every 40 minutes as long as the Azure AD provisioning service is running.

## Step 6. Monitor your deployment

Once you've configured provisioning, use the following resources to monitor your deployment:

1. Use the [provisioning logs](https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-provisioning-logs) to determine which users have been provisioned successfully or unsuccessfully
2. Check the [progress bar](https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/application-provisioning-when-will-provisioning-finish-specific-user) to see the status of the provisioning cycle and how close it is to completion
3. If the provisioning configuration seems to be in an unhealthy state, the application will go into quarantine. Learn more about quarantine states [here](https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/application-provisioning-quarantine-status).

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/aws-single-sign-on-tutorial>

https://learn.microsoft.com/en-us/azure/active-directory/saas-apps/aws-single-sign-on-provisioning-tutorial?source=recommendations