Resources

<https://learn.microsoft.com/en-us/microsoftsearch/servicenow-knowledge-connector>

<https://learn.microsoft.com/en-us/microsoftsearch/configure-connector>

[Configure an OAuth OIDC provider on the Now Platform](https://docs.servicenow.com/bundle/vancouver-platform-security/page/administer/security/task/add-OIDC-entity.html)

[Register an application](https://learn.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app#register-an-application)

The activities in this guide require accounts with the following roles

At least a Cloud Application Administrator to register an Entra ID application

At least a Search Administrator to add and configure the ServiceNow Knowledge Connector

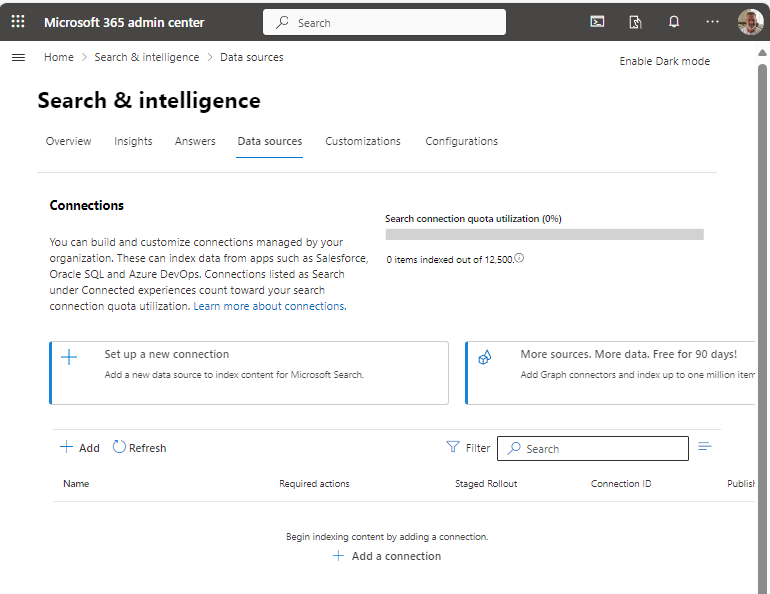
Admin role in ServiceNow

Add ServiceNow Knowledge Connector

As an account with at least the **Cloud Application Administrator** role

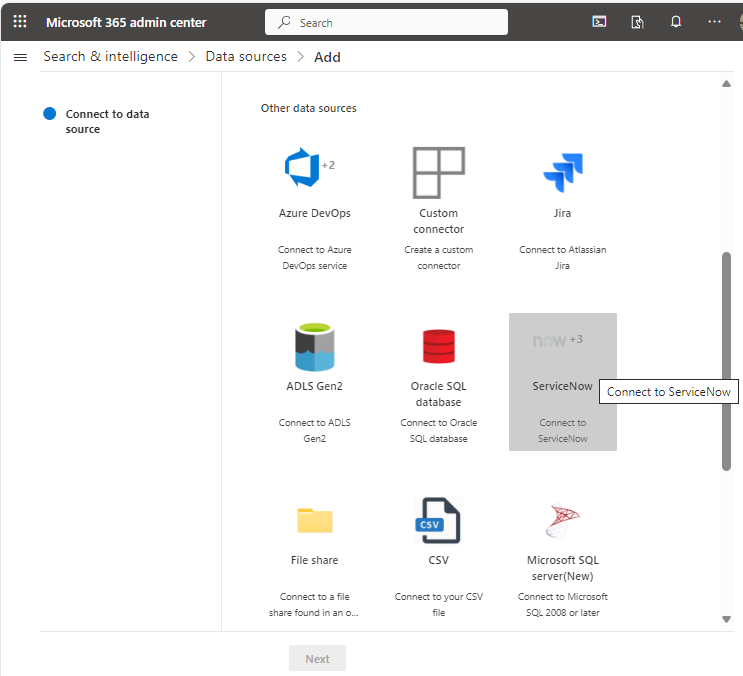
Navigate to M365 Admin Center > Settings > Search & Intelligence > Data Sources

<https://admin.microsoft.com/adminportal/home#/MicrosoftSearch/Connectors>

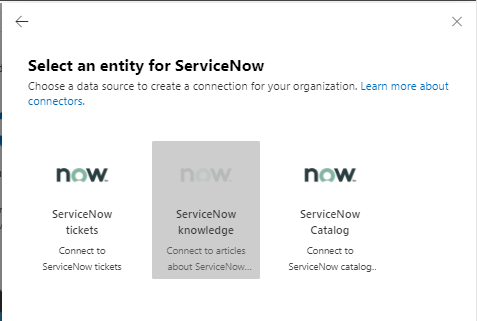


Click **Set up a new connection**

On the **Connect to data source** page, scroll down to the **Other data sources** section and click on the **ServiceNow** option.



On the **Select an entity for ServiceNow** panel that slides out from the right, click on **ServiceNow knowledge**



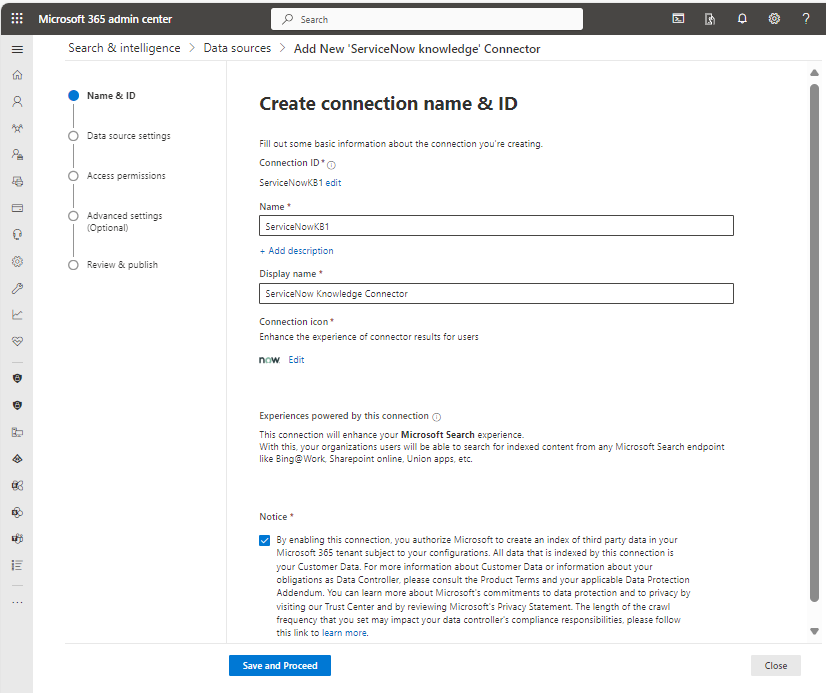
Click **Next**

On the **Create connection name & ID** page, enter a value for the **Name** and **Display name** fields. You can optionally provide a description for the connector by clicking on the **Add description** link.

You can also change the system provide Connection ID by clicking the edit link next to that value.

One more thing you can edit is the icon that shows up on the Search results page next to a ServiceNow knowledge article.

Tick the checkbox in the Notice at the bottom of the page to agree to allow Microsoft to index third party data.



Click the **Save and Proceed** button.

Leave the Data source settings alone for now.

On the Data source settings page, enter the ServiceNow instance URL. For Wells Fargo, the instance ID would be:

|  |  |
| --- | --- |
| Dev | https://wellsfargoqa.servicenowservices.com |
| UAT/QA | https://wellsfargoqa.servicenowservices.com |
| UAT/Test | https://wellsfargotest.servicenowservices.com |
| Prod/BCP | https://wellsfargoprod.servicenowservices.com |

In this documentation, we’re using the URL for a Personal Developer Instance:

https://dev214283.service-now.com

There are 3 choices for the Authentication method, each providing different levels of security from lowest to highest from the top to the bottom of the list. Wells Fargo Enterprise Architecture and Information Security both recommend selecting the most secure option, **Azure Active Directory (OIDC)**.

In order to set that up, we need an Entra ID application registered. So we’ll leave the ServiceNow Connector setup as is for now and switch to creating the Entra ID application registration.

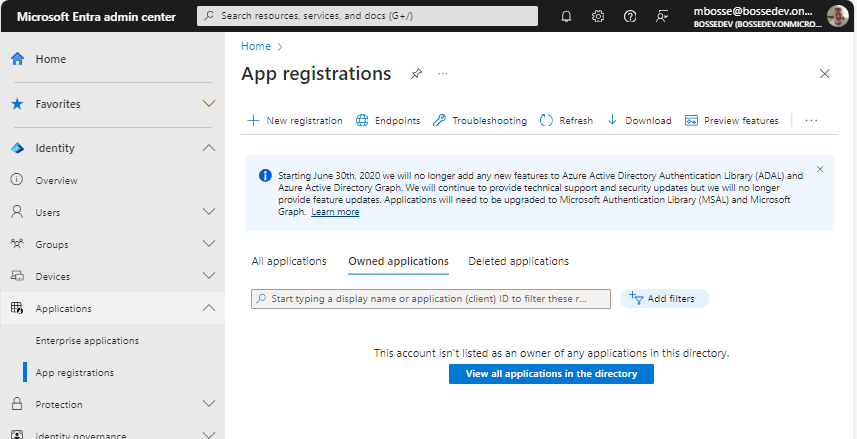
Registering an Entra ID Application

This is like setting up a service account. The Entra ID application will have a service principal name that is used when configuring the ServiceNow account later in this setup.

Sign in to the [Microsoft Entra admin center](https://entra.microsoft.com/) as at least a Cloud Application Administrator.

Browse to Identity > Applications > App registrations

[App registrations - Microsoft Entra admin center](https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade/quickStartType~/null/sourceType/Microsoft_AAD_IAM)

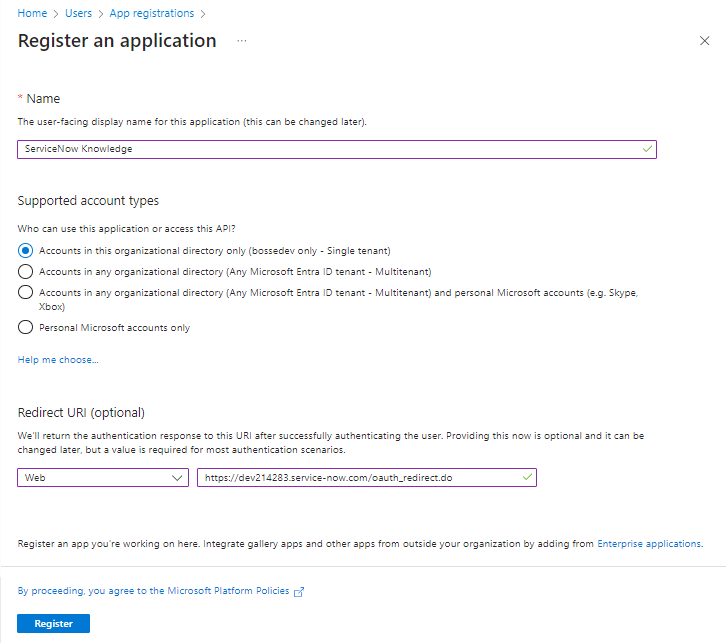


Select **New registration**.

Provide a **Name** for the application.

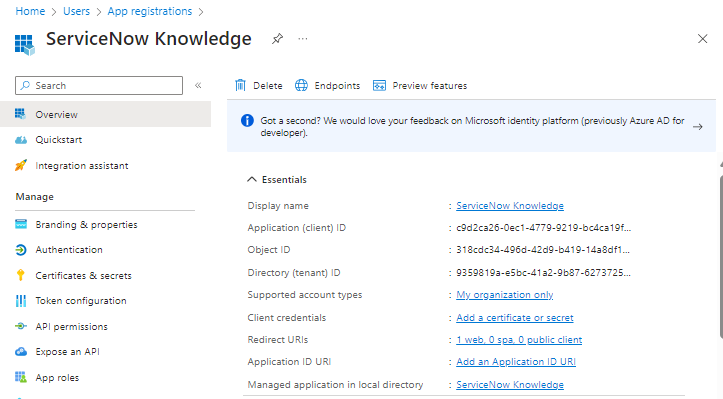
For the **Supported account types**, select **Accounts in this organizational directory only** (single tenant).

For the **Redirect URI**, select **Web** and **enter https://<Instance-Name>.service-now.com/oauth\_redirect.do**



Click **Register**.

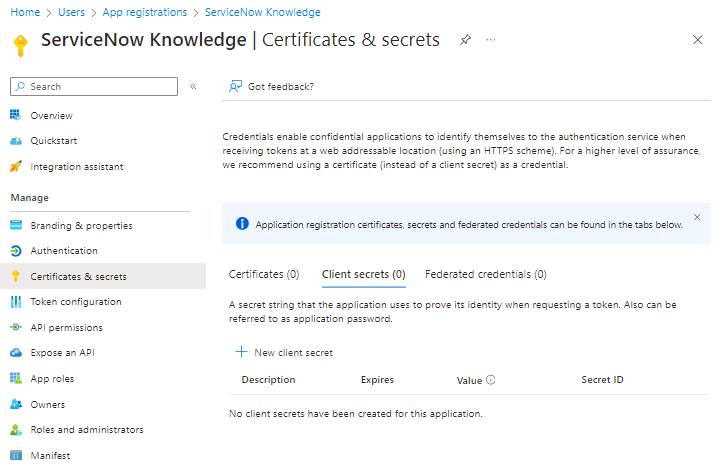
On the Overview page for the application you just registered, note the Application (client) ID and Directory (tenant) ID.



Create a client secret

If you’ve navigated away from the application you registered, in the Microsoft Entra admin center, in App registrations, select your application.

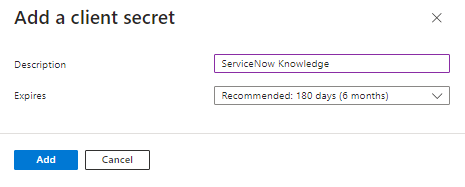
Select **Certificates & secrets** in the left navigation



Click **New client secret**.

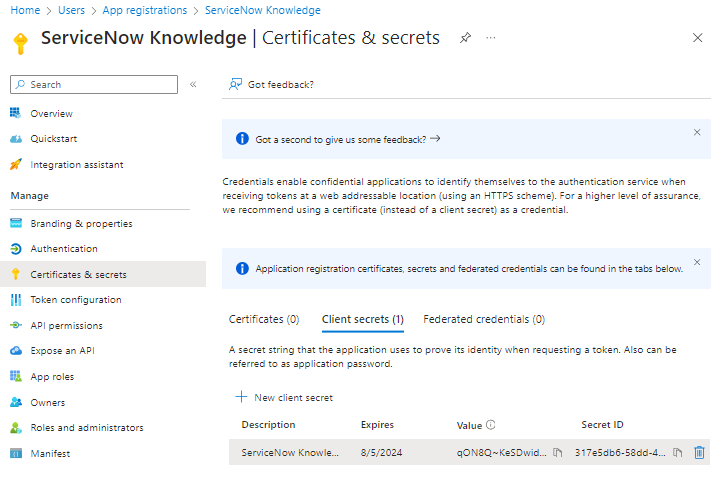
Fill in the **Description** for your client secret.

Select a value for the **Expires** field. Need to check with Channel Secure to see if they have a recommended value. MS recommends less than 12 months.



Click **Add**.

Do not leave the Certificates & secrets page without first *recording the secret's value* for use in the setup of the ServiceNow OIDC Provider. This secret value is *never displayed again* after you leave this page.



Retrieve the Service Principal Object Identifier

Run PowerShell

Install the Azure PowerShell module

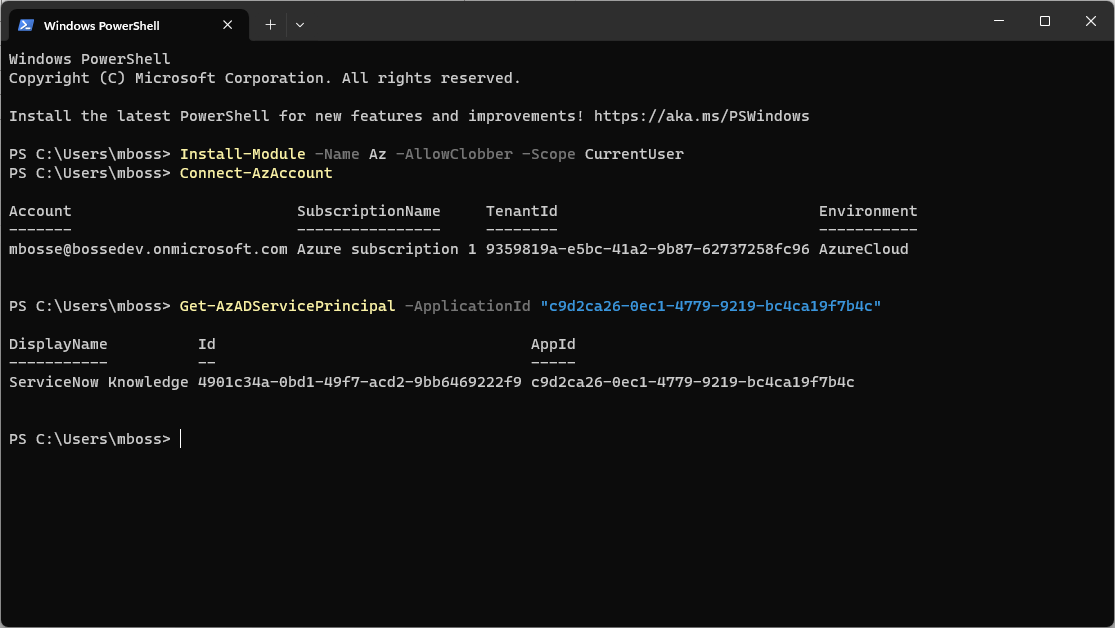
Install-Module -Name Az -AllowClobber -Scope CurrentUser

Connect to Azure

Connect-AzAccount

Get the Service Principal Object Identifier

Get-AzADServicePrincipal -ApplicationId "Application-ID"



Copy the value for the Id of the application. You’ll need this when setting up the ServiceNow account.

Register a ServiceNow Application

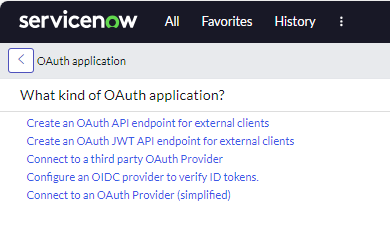
Register a new OAuth OIDC entity

[Create an OAuth OIDC provider](https://docs.servicenow.com/bundle/vancouver-platform-security/page/administer/security/task/add-OIDC-entity.html)

Navigate to the ServiceNow instance as an account with the **admin** role

Navigate to All > System OAuth > Application Registration

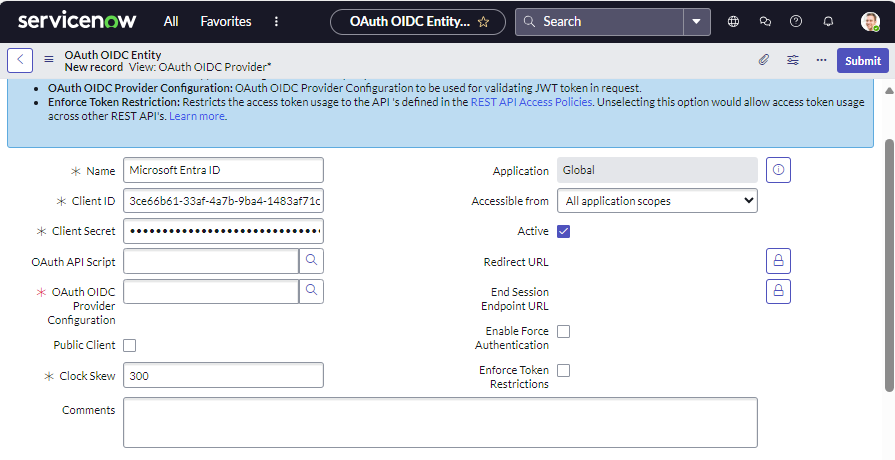
Click **New**, click **Configure an OIDC provider to verify ID tokens**



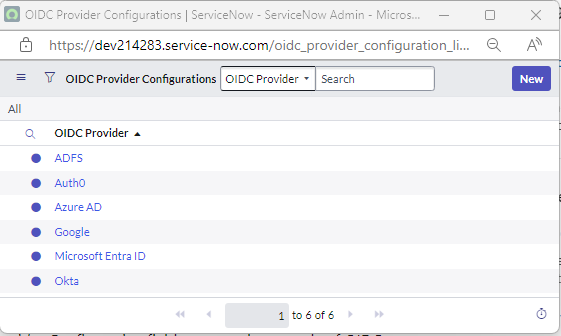
Use this table to help fill out the OIDC provider registration form:

|  |  |  |
| --- | --- | --- |
| **Field** | **Description** | **Recommended Value** |
| Name | A unique name that identifies the OAuth OIDC entity. | Microsoft Entra ID |
| Client ID | The client ID of the application registered in the third-party OAuth OIDC server. The instance uses the client ID when requesting an access token. | Your Entra ID application’s Application (Client) ID |
| Client Secret | The client secret of the application registered in the third-party OAuth OIDC server. | Your Entra ID application’s Client Secret value. |

All other values can be default.

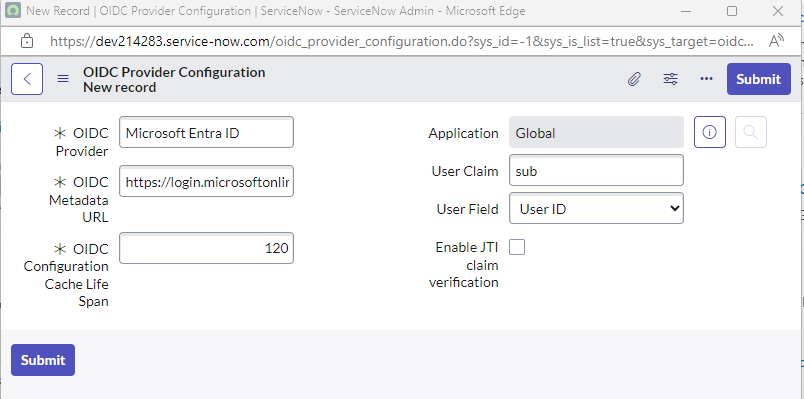


For the **OAuth OIDC Provider Configuration** field, click the magnifying glass icon and then on the OIDC Provider Configurations form, click **New**.



Use this table to help fill out the OIDC Provider Configuration New record form:

|  |  |
| --- | --- |
| **Field** | **Recommended Value** |
| OIDC Provider | Microsoft Entra ID |
| OIDC Metadata URL | The URL must be in the form https://login.microsoftonline.com/<tenandId>/.well-known/openid-configuration |
| Replace "tenantID" with Directory (tenant) ID from step 3.a. |  |
| OIDC Configuration Cache Life Span | 120 |
| Application | Global |
| User Claim | sub |
| User Field | User ID |
| Enable JTI claim verification | Disabled |



Click **Submit**.

Then click **Submit** on the OAuth OIDC Entity form.

If you ever have to delete a IODC Provider Configuration, use the navigation, select All and in the text box enter oidc\_provider\_configuration.list. It won’t be found, but click Enter anyway. You will be taken to the OIDC Provider Configurations list where you can select a configuration and delete it.

Or you can go here directly:

https://<your-instance>.service-now.com/now/nav/ui/classic/params/target/oidc\_provider\_configuration\_list.do

Create a ServiceNow account

Navigate to Your ServiceNow instance using an account in the **user\_admin** role

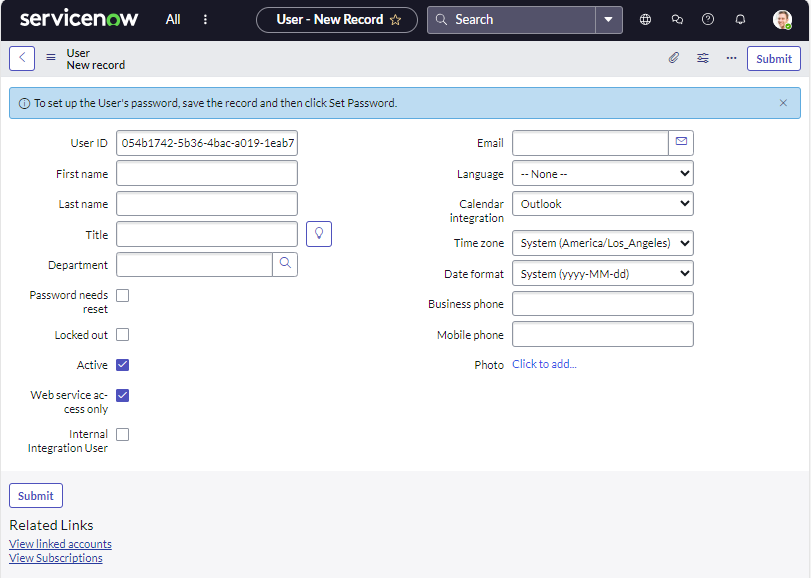
Navigate to All > User Administration > Users

Click **New** at the top of the Users page.

Use this table to help fill out the form:

|  |  |
| --- | --- |
| **Field** | **Recommended Value** |
| User ID | Service Principal Object ID from the Entra ID application registered earlier. |
| Web service access only | Checked |

All other values can be left to default.

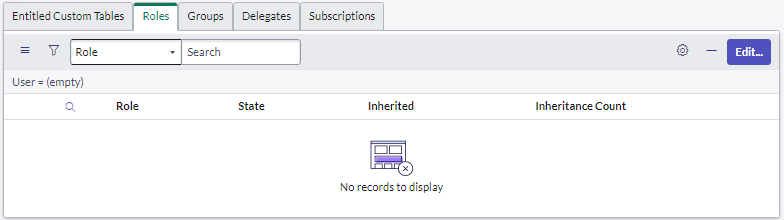


Click **Submit**

Enable Knowledge role for the ServiceNow account

Access the ServiceNow account you created with ServiceNow Principal ID as User ID and assign the knowledge role.

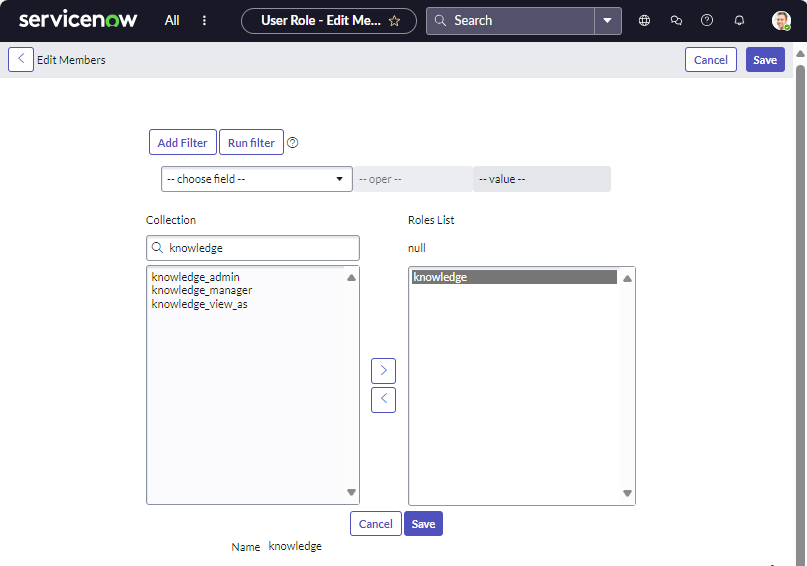
On the user page for the ServiceNow account you created, scroll down and select the **Roles** tab at the bottom of the page.



On the **Roles** tab, click **Edit**.

Use the search box to filter the role options to **knowledge**.

Select the knowledge role in the Collection list and move it to the Roles List by clicking the right carat button between the lists.



Click **Save**.

ServiceNow Connector Access Permissions

Navigate back to the Entra ID admin center and navigate to the Data source settings page for the ServiceNow Connector registered earlier.

For the authentication type select Azure Active Directory (OIDC)

Use this table to help fill out the rest of the form:

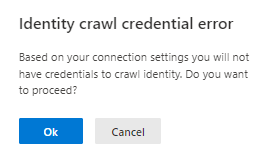
|  |  |
| --- | --- |
| Field | Value |
| Client ID | The Client ID of the Entra ID application registered earlier |
| Client Secret | The Client Secret Value of the Client Secret created for the Entra ID application earlier |
|  |  |

You can leave the Resource ID blank

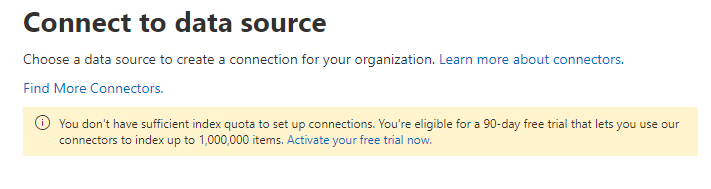
Click **Sign In**.

I got an error and I’m not sure why.

Said I would not be able to crawl with the credentials I provided.



I wonder if that has anything to do with the quota message that said I would not be able to index anything and the New data source page:



I was hesitant to start a free trial because that will run out in 90 days.

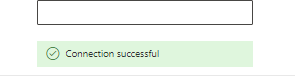
I don’t recall seeing that last time I went through this process.

I might have to delete everything and start over.

I also remember noticing the ServiceNow profile set up being mentioned but very subtly. I was not able to find instructions for creating the profile for the ServiceNow OIDC provider.

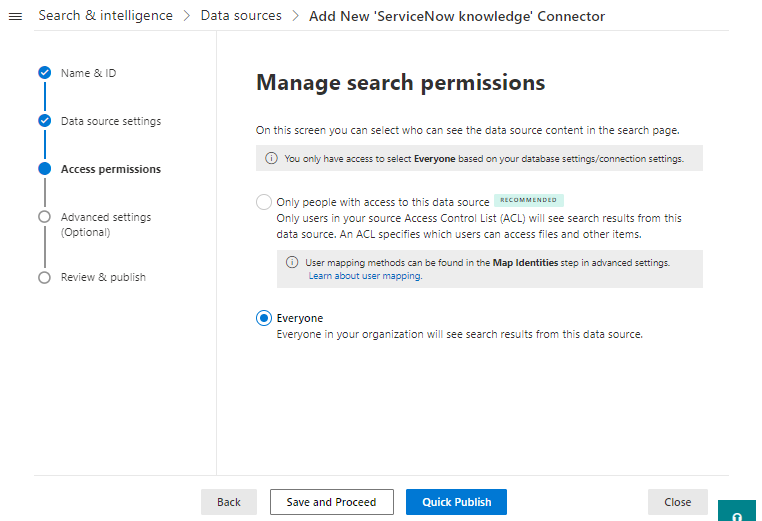
I clicked Ok to proceed.

This was displayed on the form:



Click **Save and Proceed**.

On the Manage search permissions page, select **Everyone**.



Click **Quick Publish**.

Review the information on the **Review connection** page

Click **Publish**.

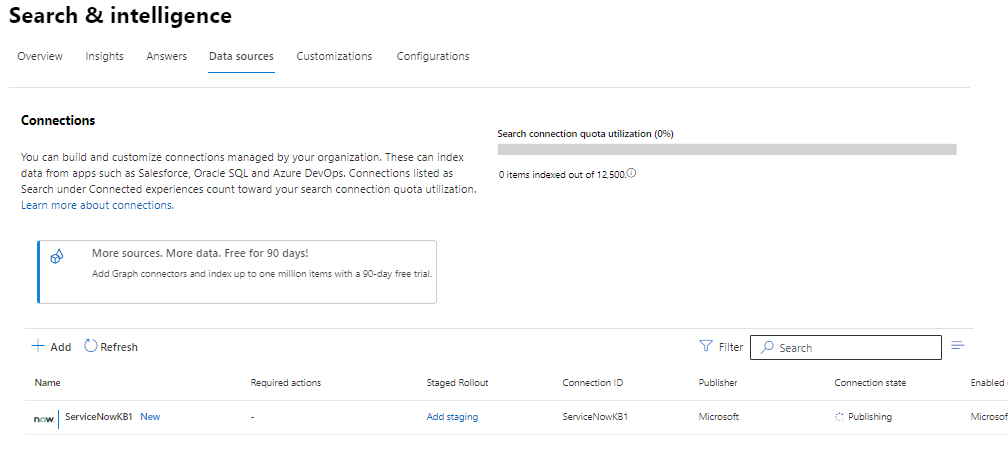
On the Connection Published page, leave the toggle set to **On** for **Show results in ‘All’ vertical**.

Click **Save and Close**.

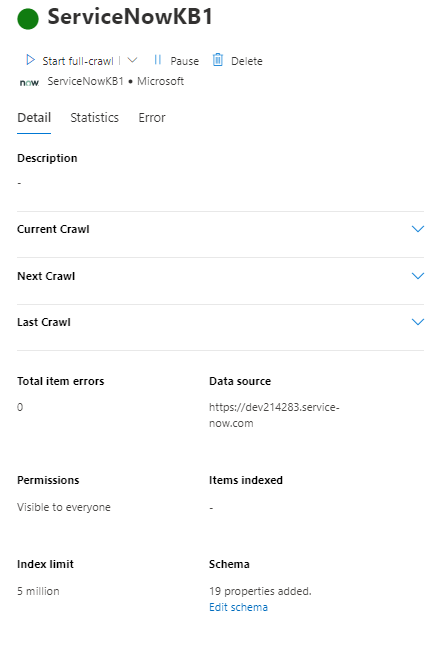
Check the Connector status

Immediately following the configuration of the Connector, it will be in the “Add staging” state and the Connection state will be “Publishing”. It will take a few minutes to finish the configuration.

Periodically, click **Refresh** to update the information.



Once the Connection status is “Ready”, click on the connection and view the details. On the Details panel, start a full crawl.



After a few minutes, you should see the number of indexed items increase.

