[Setting up REST Services with Appian 1](#_Toc415307540)

[1. Client Registration 1](#_Toc1350234730)

[Register Client 1](#_Toc1421304403)

[Edit Client 4](#_Toc1342828778)

[2. Integration System User (ISU) 4](#_Toc438552445)

[Create ISU 4](#_Toc1450125021)

[Create Security Group 5](#_Toc1257467796)

[3a. Authentication: JWT Set-up 8](#_Toc2001714304)

[Deploy JWT Tools Plug-in 8](#_Toc1987861197)

[Set Up Third Party Credential Store 8](#_Toc740670101)

[Configure Connected System 9](#_Toc1830671555)

[Verify 9](#_Toc1006055684)

[3b. Authentication: OAuth Auth Code Set-up 10](#_Toc2040227466)

[Outbound EIB 11](#_Toc2132470011)

[Create Appian “Service” Account 11](#_Toc1462315335)

[Create WebAPI that intakes a document 11](#_Toc1391729536)

[Create EIB 12](#_Toc1157580868)

[Edit Your EIB 14](#_Toc1093036474)

[Test Your EIB 15](#_Toc1696792021)

[Setting Up Custom Report For Integrations 17](#_Toc1449984653)

[Set-up 17](#_Toc40423869)

[Permissions 18](#_Toc1641476964)

[Filtering 19](#_Toc499586038)

# Setting up REST Services with Appian

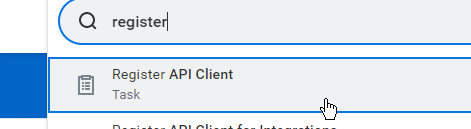
To set up REST services between Appian and Workday, you will need:

1. Register an API client with appropriate scopes
2. An Integration system account with appropriate permissions
3. Appian set-up for JWT

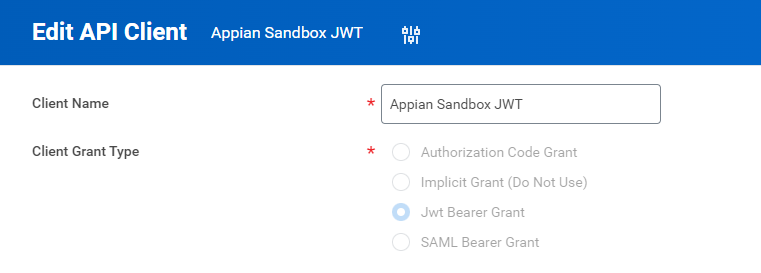
## 1. Client Registration

### Register Client

As a Workday Admin, access the **Register API Client** task



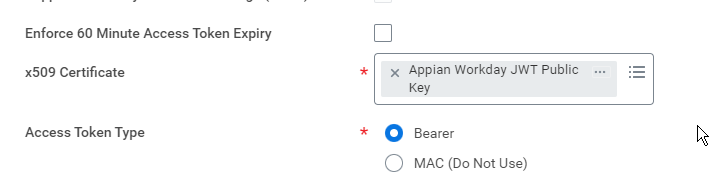
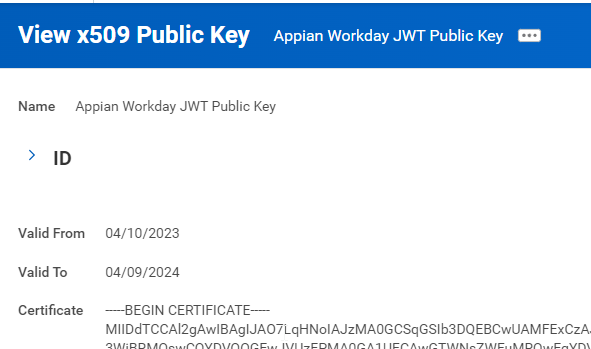
Use JWT as Grant Type by default. If you aren’t going to have users directly calling integrations, OAuth Auth Code might be a feasible alternative.



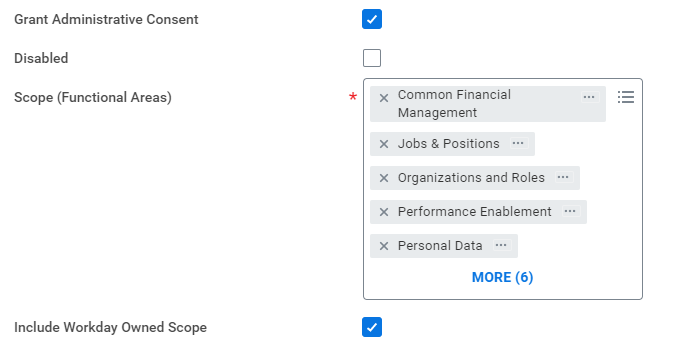
Create a certificate in Workday OR KeytoolOpenSSL to create an x509 compliant public/private pair. Example code:

* Keytool
  + keytool -genkey -keyalg RSA -alias Workday -keystore JWTkeystore.jks -storepass Workday123! -validity 360 -keysize 2048
* Openssl
  + openssl genrsa -out keypair.pem 2048
  + openssl rsa -in keypair.pem -pubout -out publickey.crt
  + openssl pkcs8 -topk8 -inform PEM -outform PEM -nocrypt -in keypair.pem -out pkcs8.key

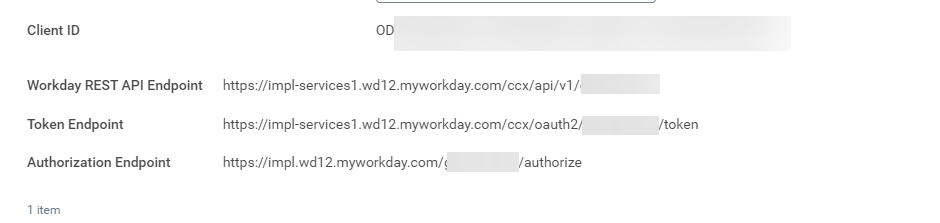
***Note: paste the FULL text of the keys in all boxes!***

Set Scopes needed for the API. Use the REST Reference to determine basic families required for your needs:

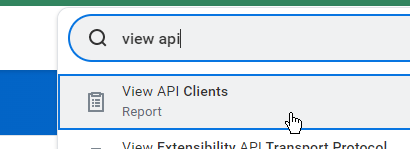


Save your ClientID and endpoints for future reference



### Edit Client

Access clients by running the **View API Client** report

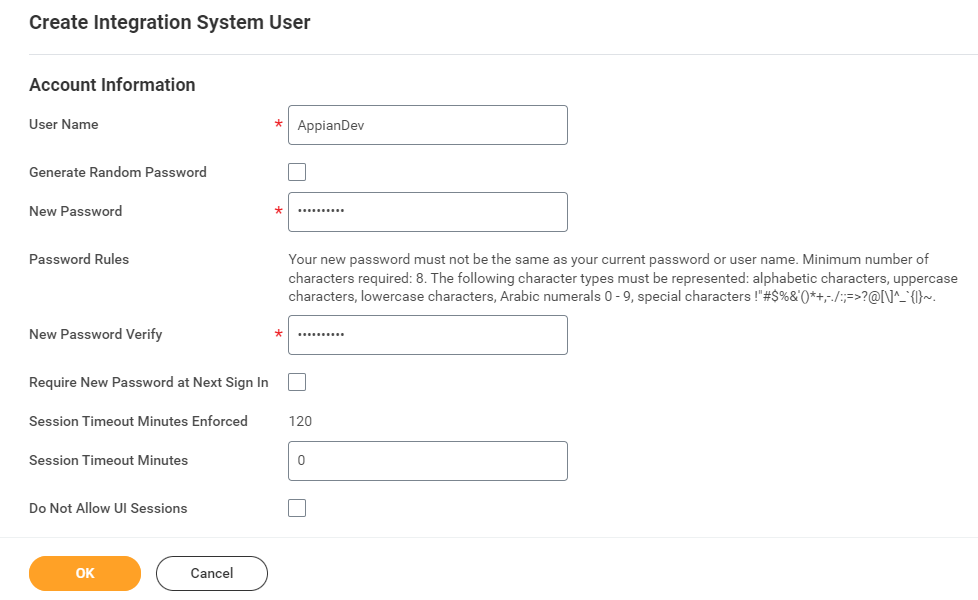


Select your client and edit where needed.

## 2. Integration System User (ISU)

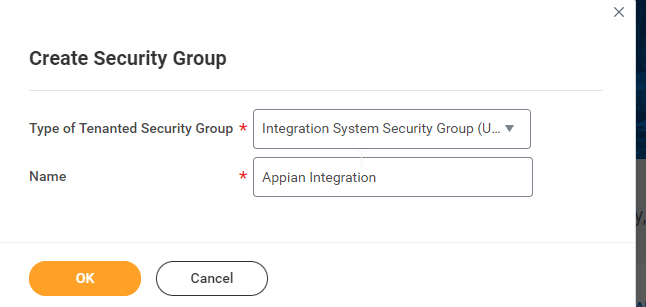
### Create ISU

JWT requires an ISU context so create one in Workday.

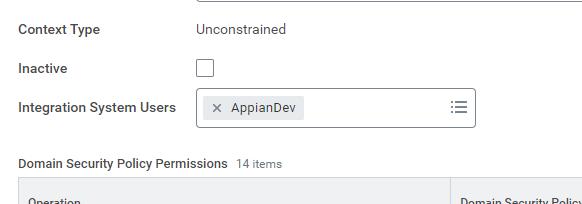


### Create Security Group

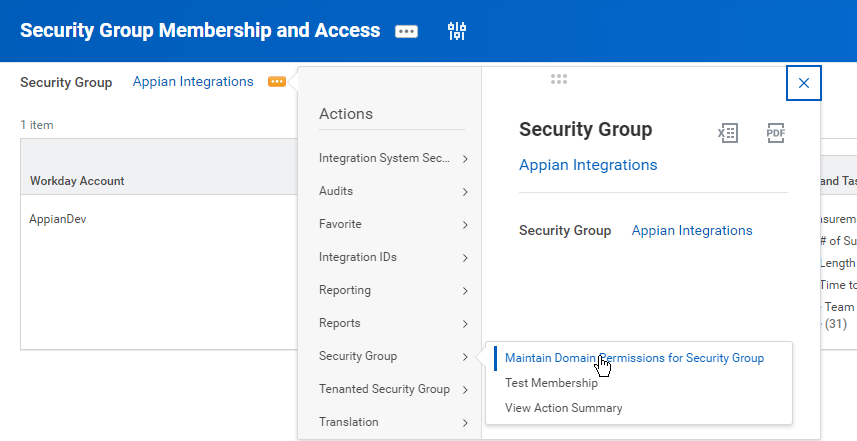
Create a new security group. Can use Integration System Security Group for this example:

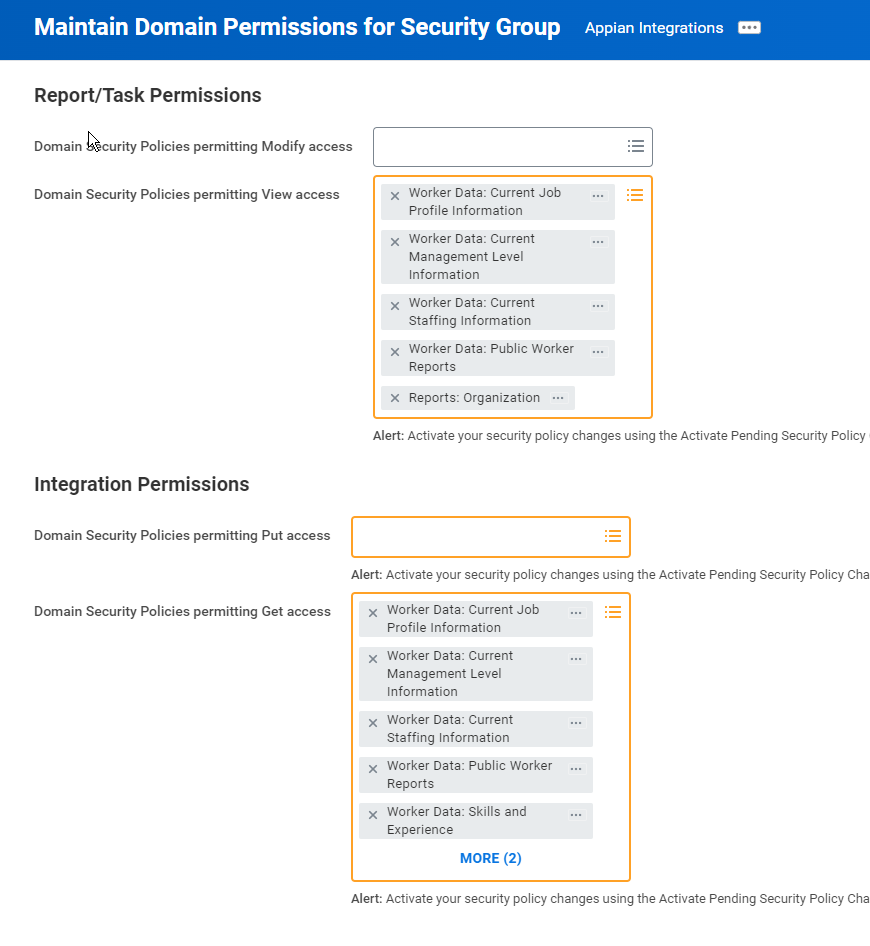


Edit the group and add your ISU as a user.

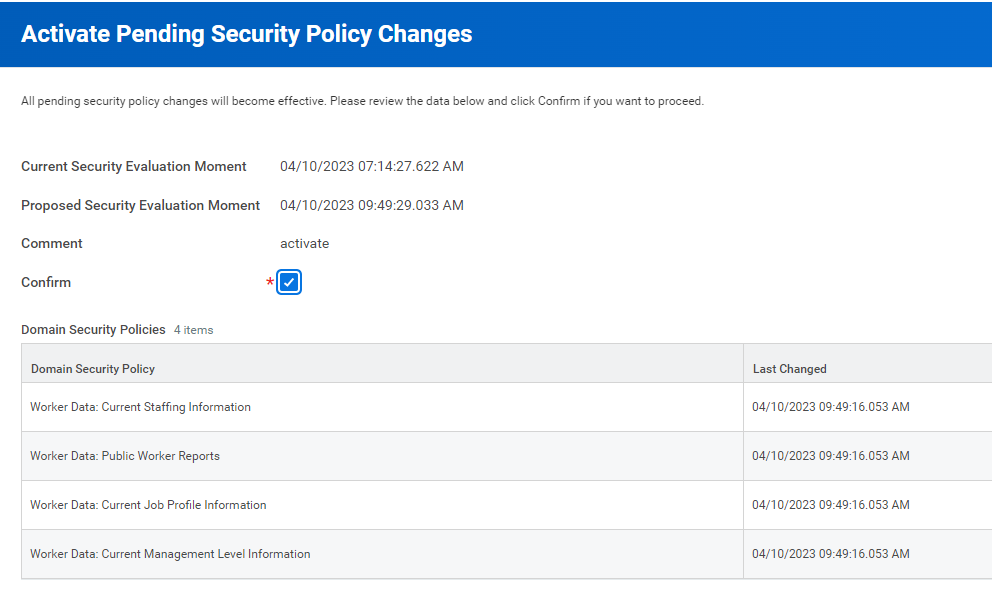
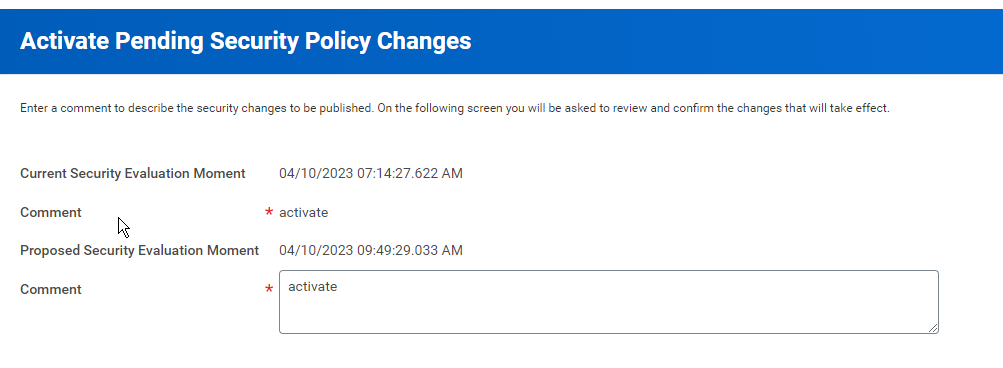


Edit Domain Permissions to include the appropriate security roles that align with the API needs/



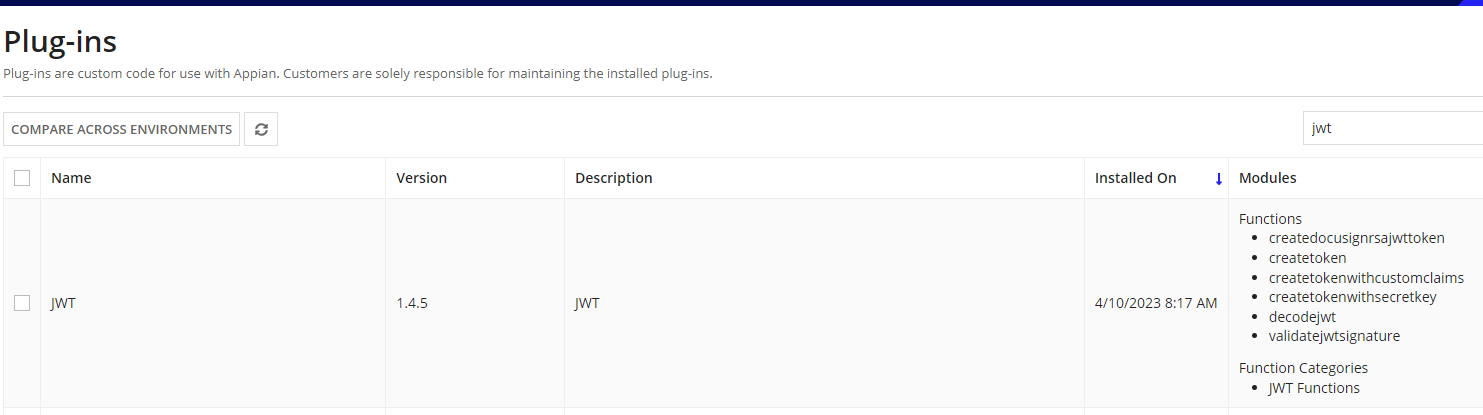


Run the **Activate Pending Security Policy Changes** task to enable/activate those permissions.



## 3a. Authentication: JWT Set-up

### Deploy JWT Tools Plug-in

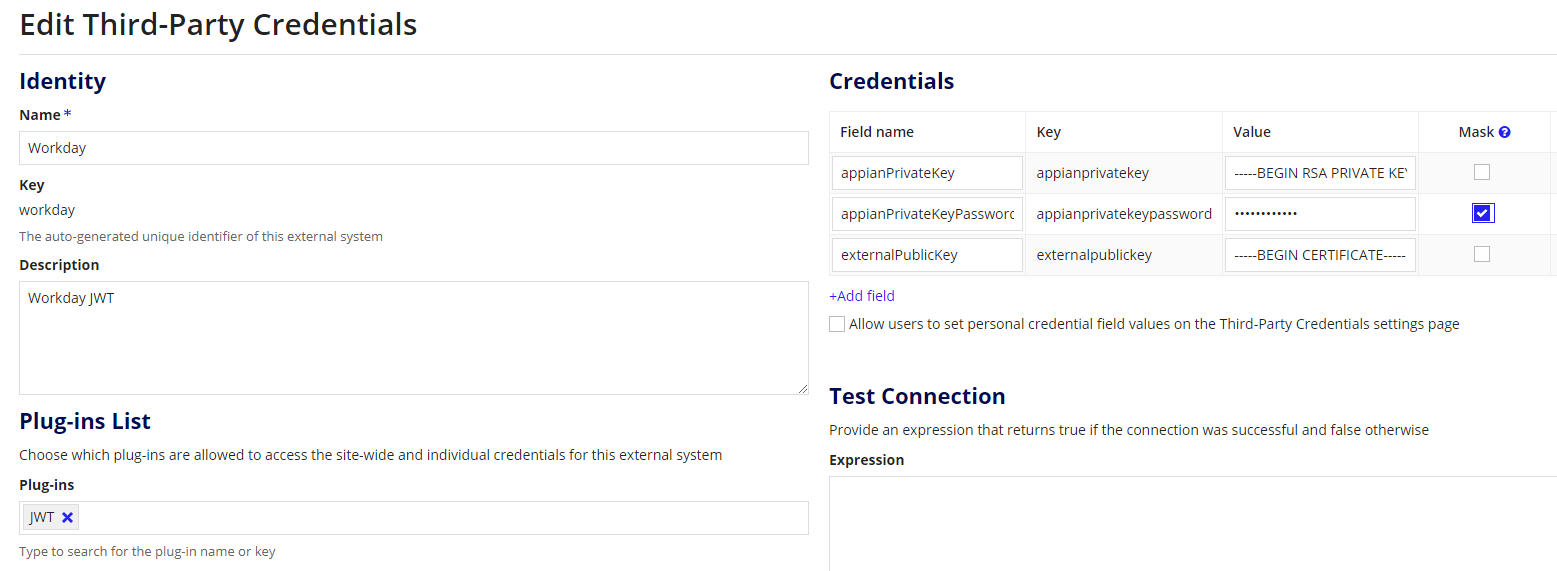


### Set Up Third Party Credential Store

Using the JWT Tools plug-in, set up a credential store and enter your private key and password strings. Make sure to enable JWT plugin to access these credentials.

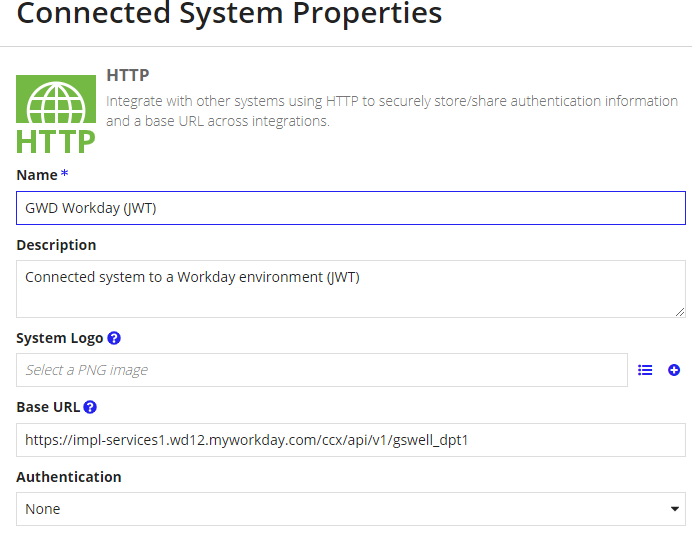
AppianPrivateKey – full text of private key

AppianPrivateKeyPassword – password for key

Configure Helper Rules

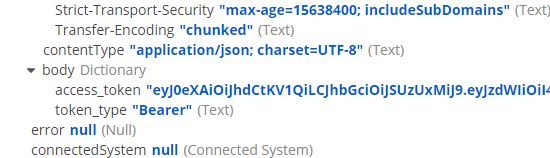
* Constant **GWD\_TEXT\_CLIENT\_ID**
  + Set to Client ID from Step 1
* Constant **GWD\_TEXT\_SCS\_KEY**
  + Set to SCS key from previous step

### Configure Connected System

* Constant GWD\_TEXT\_BASE\_TENANT\_URL
  + Your base environment URL (I.e. ***https://impl-services1.wd12.myworkday.com/ccx/***)
* Constant **GWD\_TEXT\_TENANT\_ID**
  + Your tenant (I.e. ***gswell\_dpt1***)
* GWD Workday (JWT)
  + 

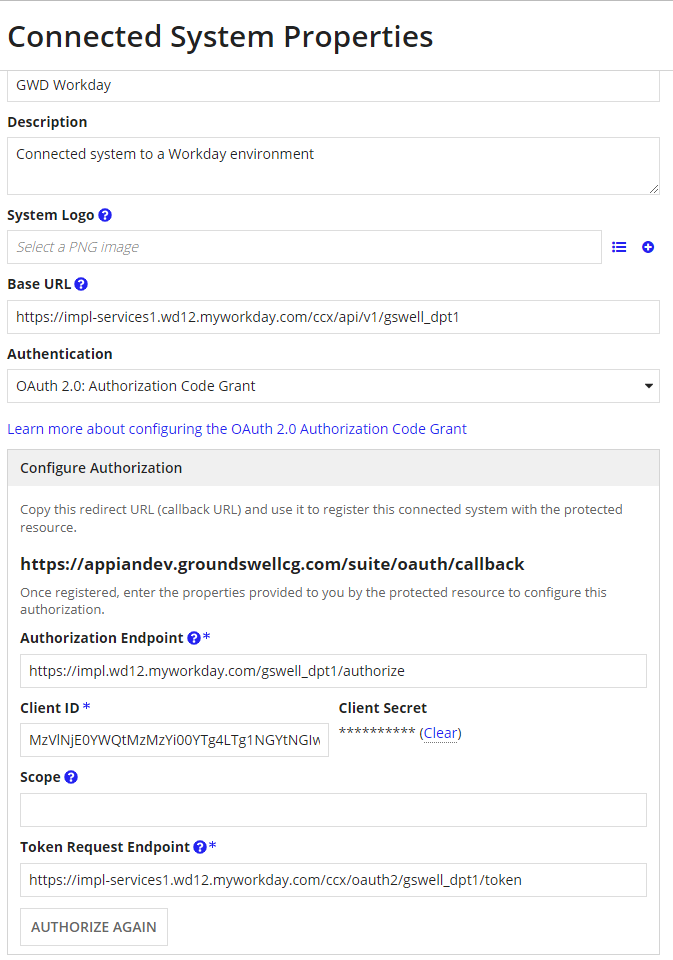
### Verify

Execute GWD\_JWT\_EXT\_GET\_token to conform successful token retrieval. If you get an error, double check your client ID



## 3b. Authentication: OAuth Auth Code Set-up

If using Auth Code, you can set up the GWD Workday Connected System instead and point integrations to that. The steps above are mostly the same except you select Auth Code in your Client API and store your ID/Secret in the CS:



# Outbound EIB

EIBs are useful for scheduling data pushes to Appian for purposes of data migration, triggering record updates, etc.

## Create Appian “Service” Account

For Workday outbound EIBs, we need to use username/password authentication due to incompatibilities in Workday and Appian auth mechanisms for Web APIs.

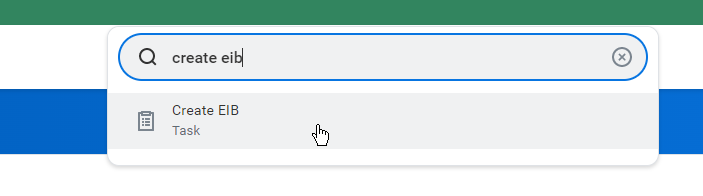
## Create WebAPI that intakes a document

Inbound EIBs send XML files by default. Example is like **GWD Upload Document**:

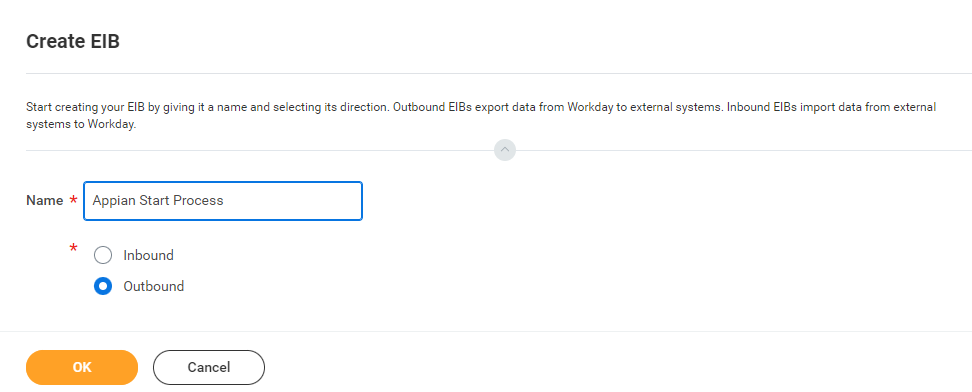


## Create EIB

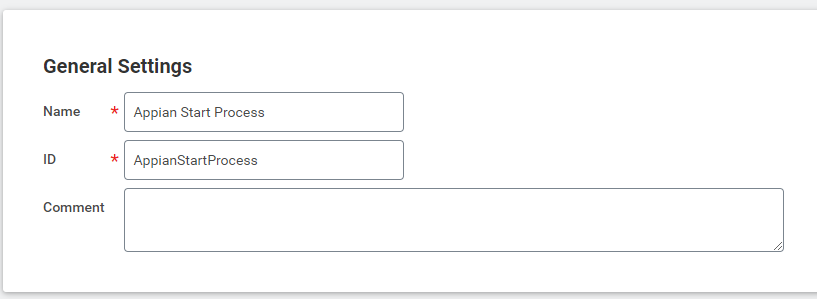
In Workday, access the **Create EIB** task.



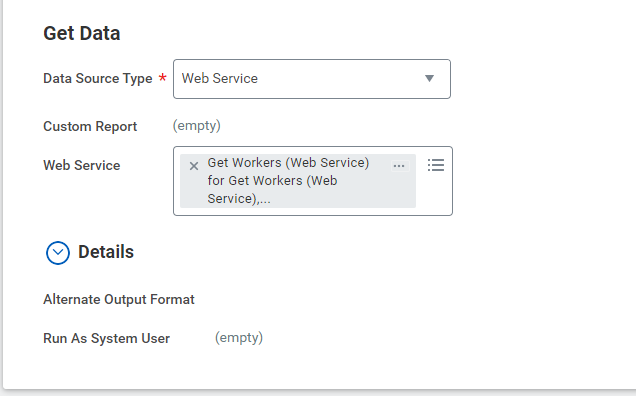
Mark the EIB as Outbound and give it a clear name.



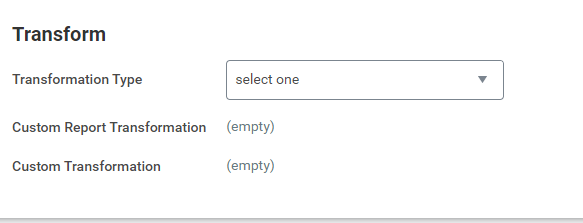
Update General Settings as needed.



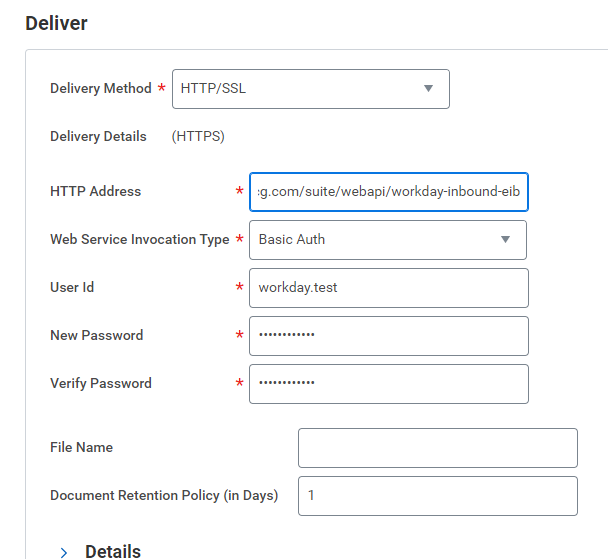
Set up the **Data Source Type** as ***Web Service***, and identify which report you want to run.



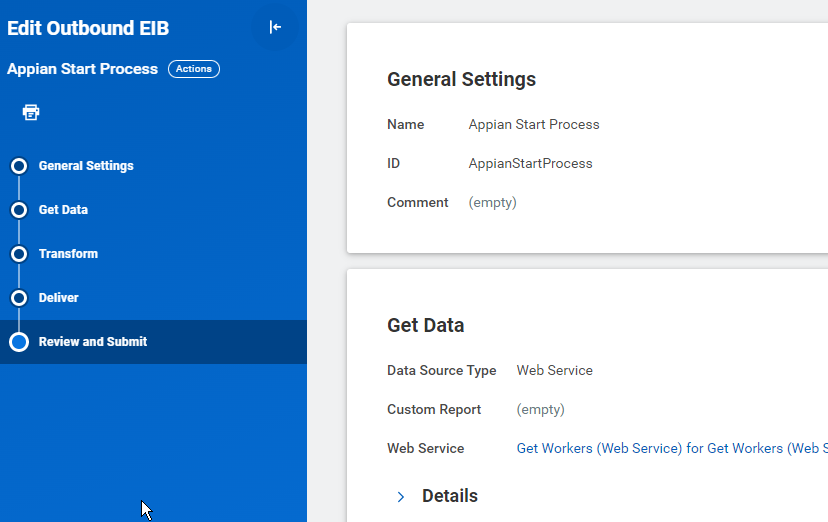
For simple cases, leave **Transformation Type** as empty.



Configure delivery for HTTP and put in your WebAPI and credentials.

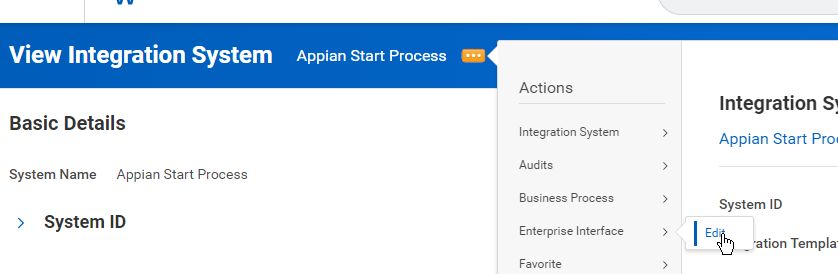


Complete review of settings and save your EIB.



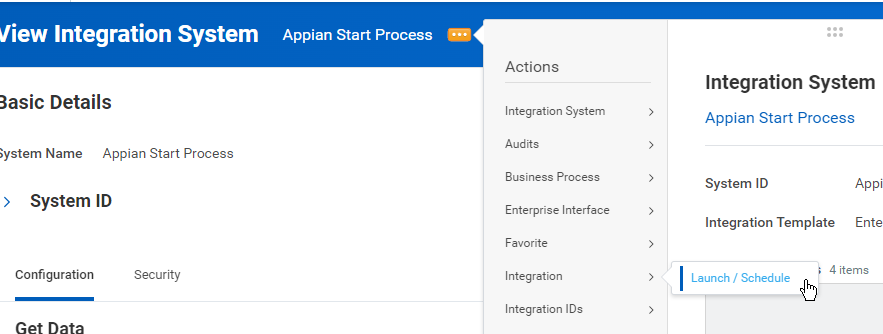
## Edit Your EIB

If you need to edit your EIB, access the **Enterprise Interface->Edit** action from the **Integration System** object.

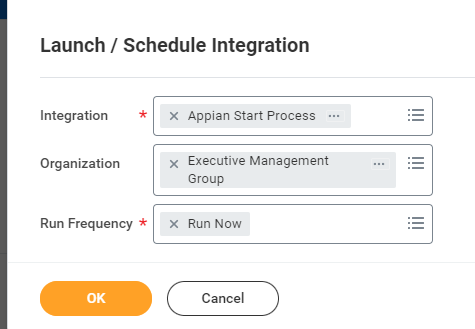


## Test Your EIB

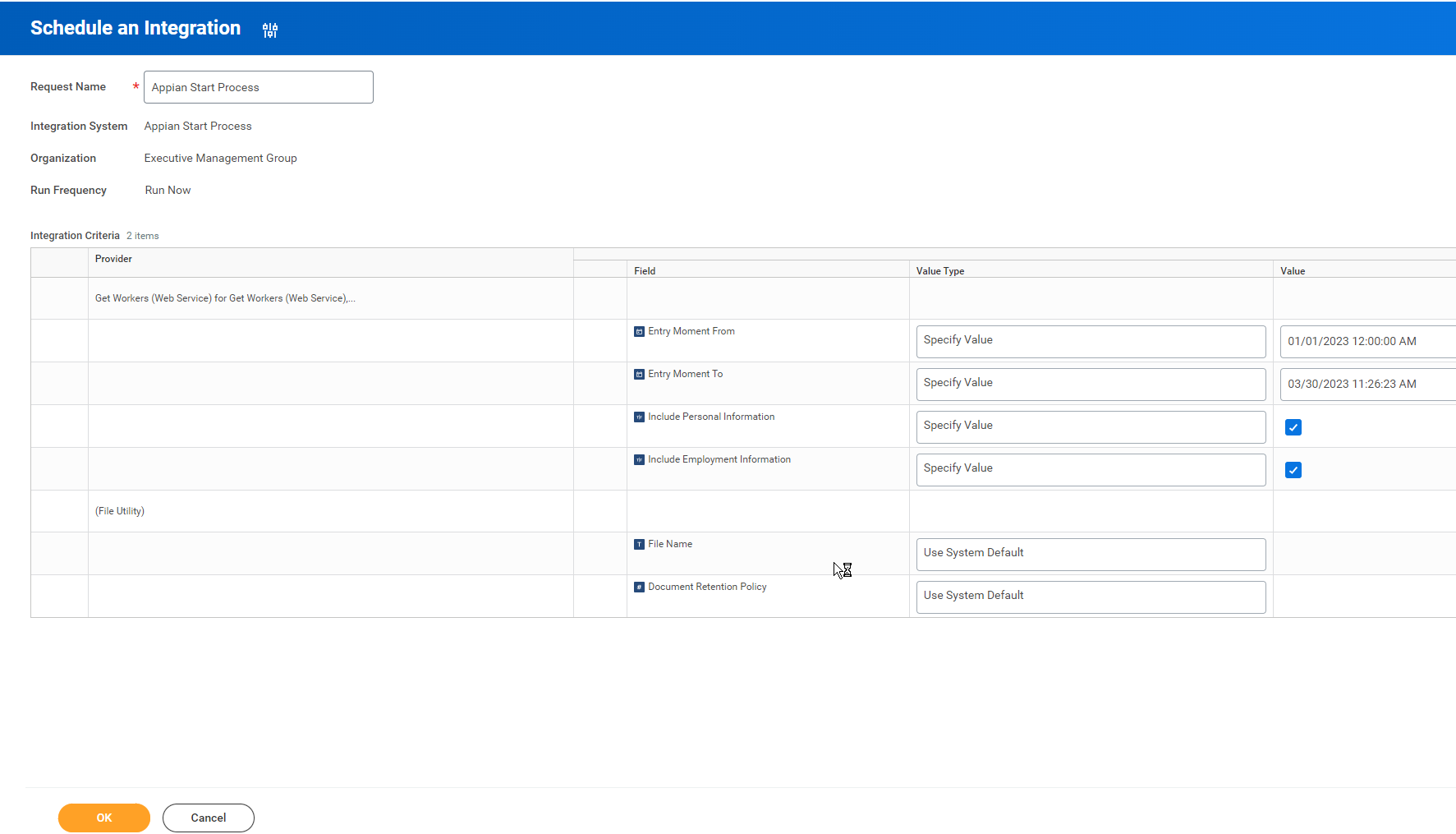
On-demand or scheduled launching can then be set-up from the **Integration->Launch/Schedule** action available from the EIB itself.



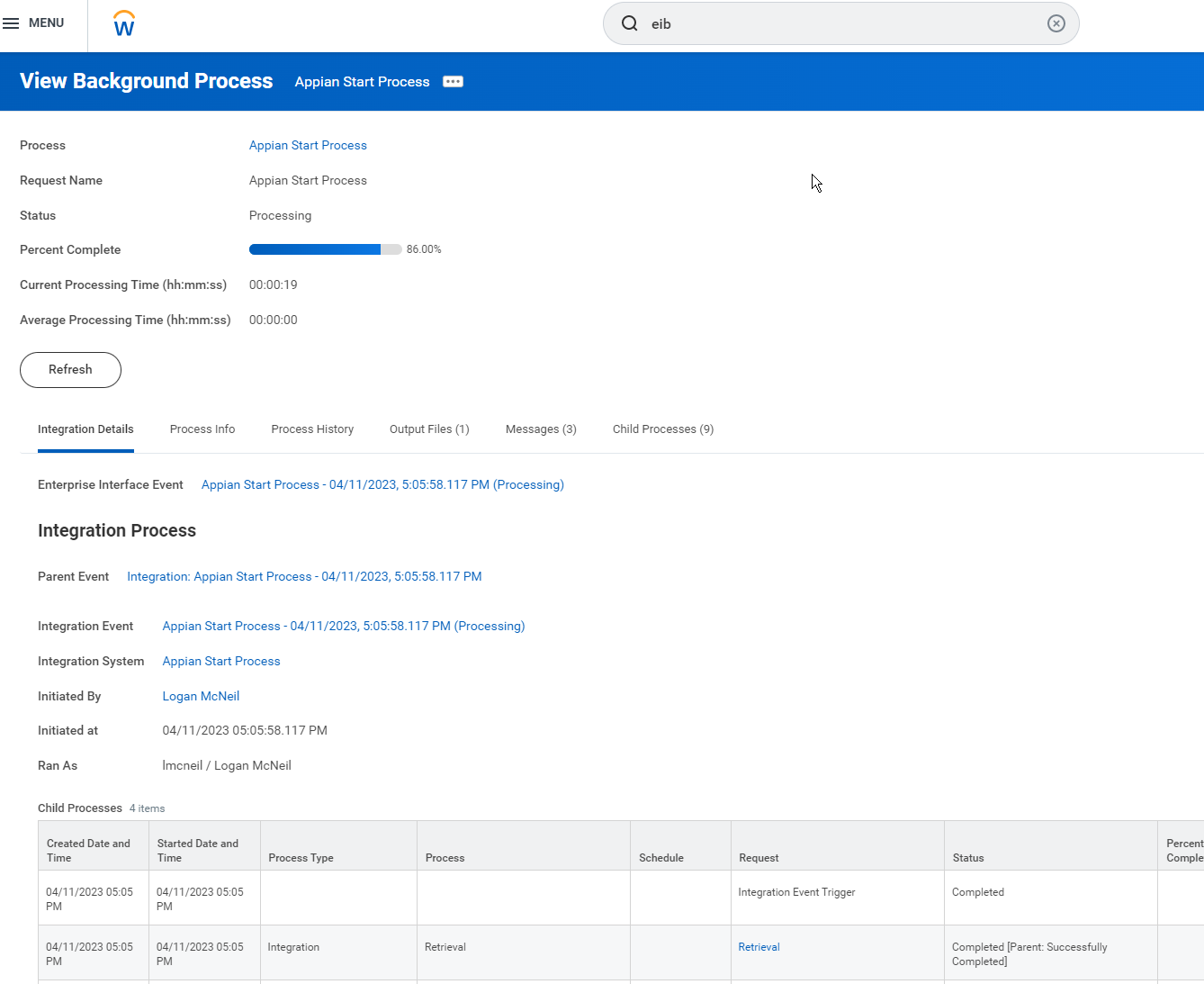
As a test, use the default settings where applicable, and set additional inputs that are applicable to your report. In this example, the ***Get Workers report*** needs a root organization



Continue with set-up, but default values can work for initial testing.



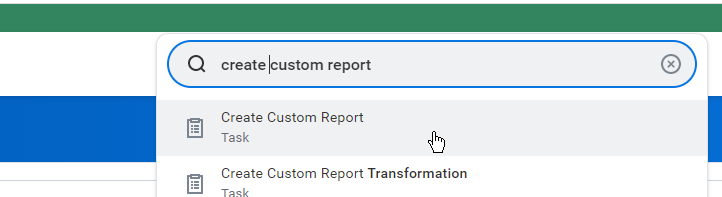
Click **OK** to launch and monitor from the resulting background process page:



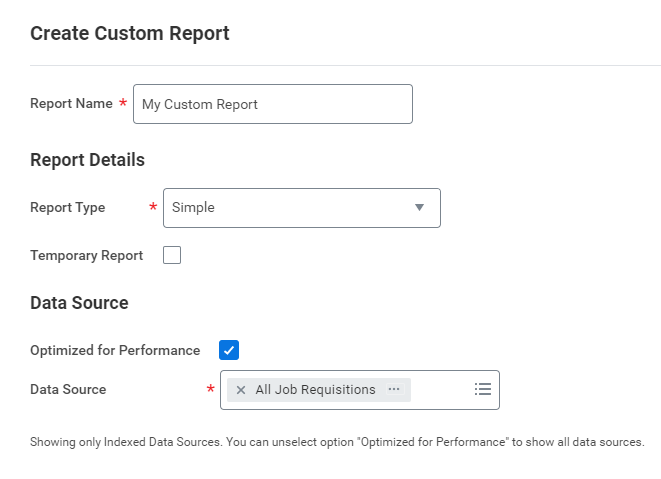
# Setting Up Custom Report For Integrations

## Set-up

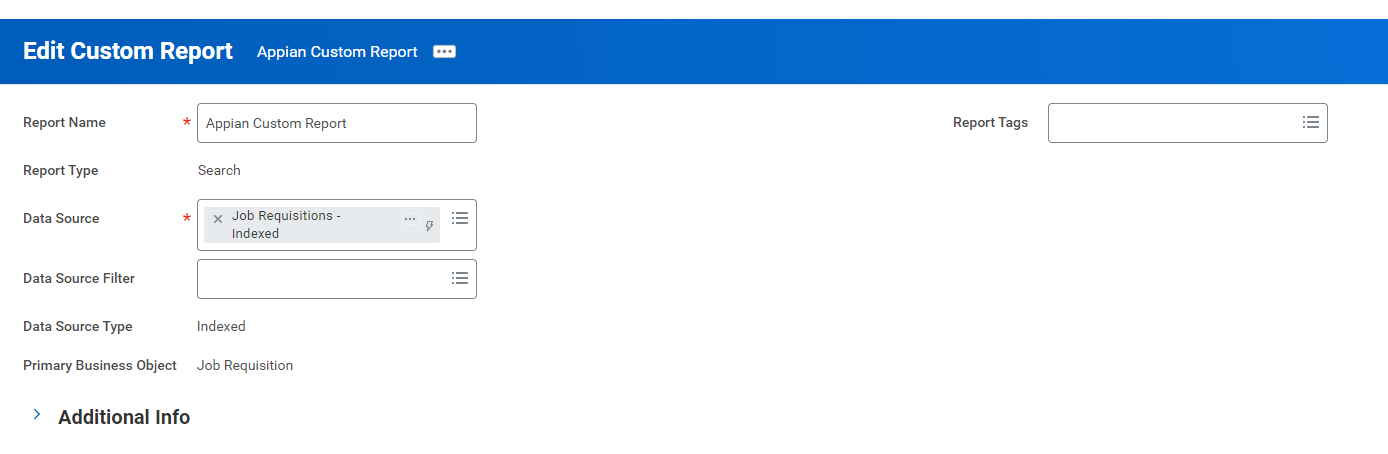
Start the **Create Custom Report** task



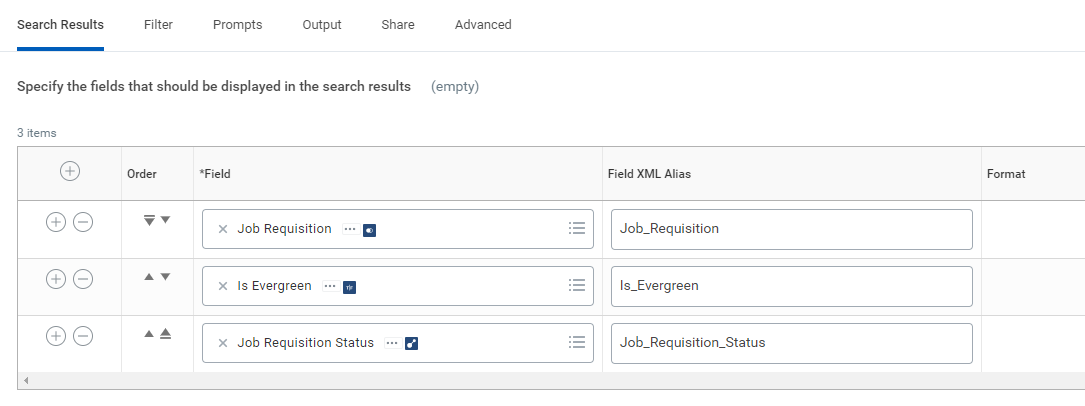
Complete the basic details



Confirm Baseline looks like

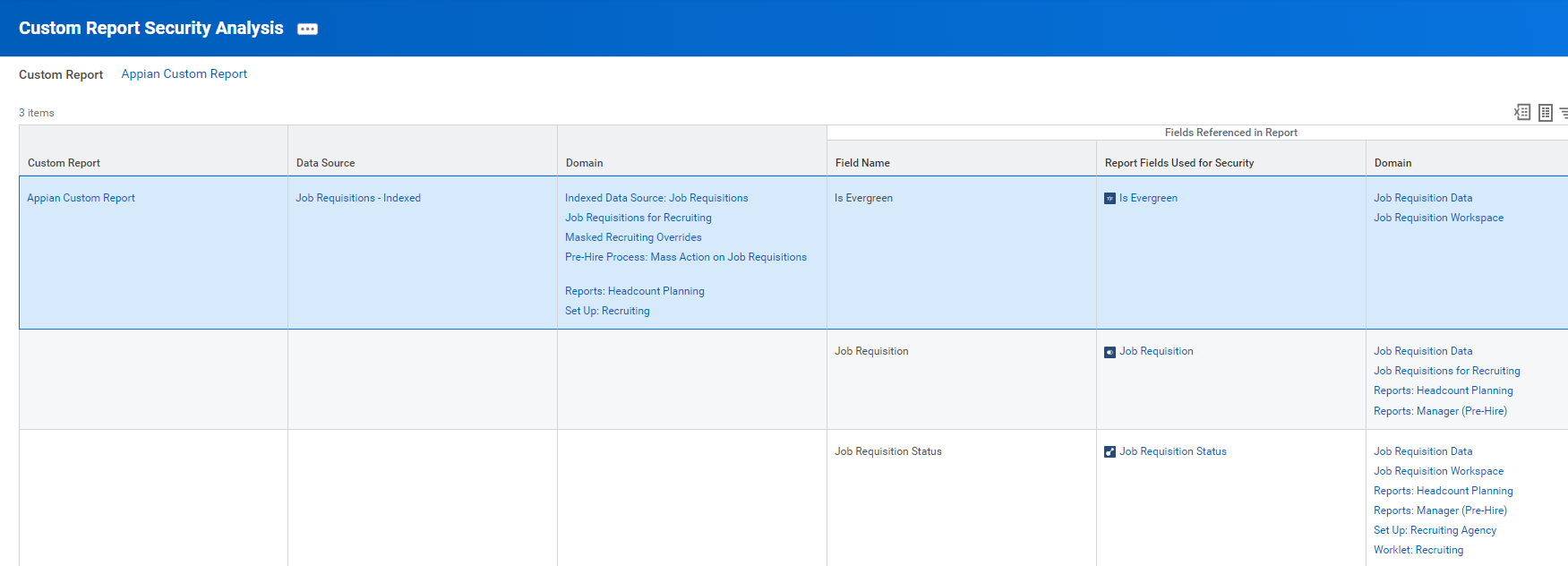


Configure Fields in your search results

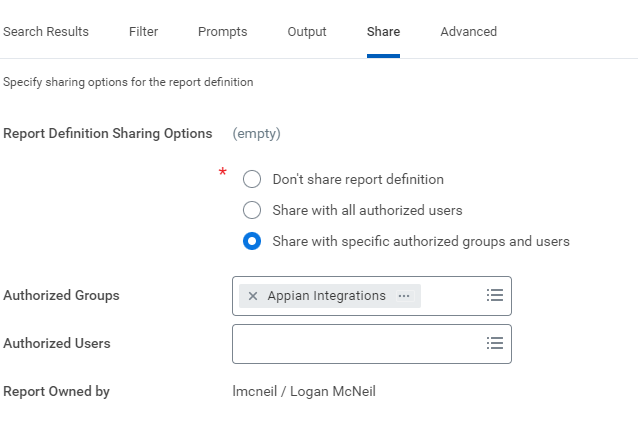


### Permissions

Make sure your ISU has Report permissions on every field in your report. This can be view in the **Custom Report Security Analysis** tab



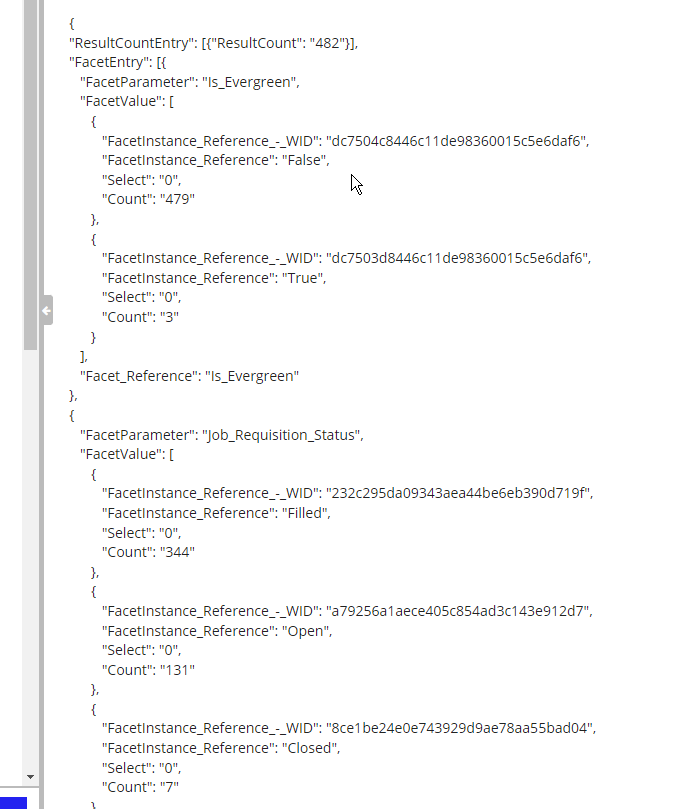
You will also need to share your report with your ISU (preferably via a security group)



### Filtering

Filtering can be accomplished by Query Parameters that map to Field XML Alias provided in report set-up. An Example is in **GWD\_EXT\_JWT\_Reporting\_GET\_customReport** or **GWD\_JWT\_EXT\_Reporting\_GET\_customReportWithPaging.**

You must provide valid filter value IDs based on the facet values returns at the top of a report result:



If filters are not clear, you can review a report configuration OR WSDL to get the key names (they should align with Prompt XML Alias):

