

# Workday HR

#### **Table of Contents**

WORKDAY HR	1
Workday - How do I link using OAuth?	1
Overview	1
Prerequisites	2
Insturctions	2
Step 1: Obtain the web services endpoint URL	2
Step 2: Enter in your tenant name	3
Step 3: Register a new API Client for Integrations	4
Step 4: Generate a non-expiring Refresh Token	6
Workday - How do I link my account with an Integration System User?	9
Overview	9
Prerequisites	9
Instructions	9
Step 2: Create a Security Group and assign an Integration System User	
Step 3: Configure domain security policy permissions	
Step 4: Activate security policy changes	
Step 5: Validate the authentication policy is sufficient	
Step 6: Activate all pending authentication policy changes	
Step 7: Obtain the web services endpoint URL	
Important Notes	21

## Workday - How do I link using OAuth?

## Overview

To authenticate your Workday account, you will need to provide the following information:

- WSDL
- Workday Tenant Name
- Client ID
- Client Secret
- Refresh Token
- Token Endpoint



## **Prerequisites**

Please ensure you fulfill all the requirements to set up the integration:

- You have Administrator permissions in your company's Workday instance

## Insturctions

## Step 1: Obtain the web services endpoint URL

1. Search in Workday for Public Web Services



- 2. Find Human Resources (Public) as you are connecting Workday HRIS.
- 3. Click the three dots to access the menu. Click Web Services > View WSDL

3 items			
Web Service			
Dynamic Document Generation (I	Public)		
External Integrations (Public)			
Financial Aid (Public)			
Financial Management (Public)			
Human Resources (Public) 🚥		×	
	Web Service 2	> View Custom WSDL	
Identity Management (Public)	Integration IDs	> View WSDL 3	
Integrations (Public)	Security	>	



- 4. Navigate to the bottom of the page that opens (it may take a few seconds to load)
- 5. Copy the full URL provided under Human\_ResourcesService (Workday HRIS). The URL will have a format similar to https://wd2-implservices1.workday.com/ccx

×

</wsdl:binding> v<wsdl:service name="Human\_ResourcesService"> w<wsdl:port name="Human\_Resources" binding="wd-wsdl:Human\_ResourcesBinding"> <soapbind:address location="https://wd2-impl-services1.workday.com/ccx/service/acme/Human\_Resources/v43.0"/> </wsdl:port> </wsdl:service> Copy this

6. Enter the Web Services Endpoint URL prefix into the linking flow

< Back workday Enter your web services endpoint URL 1 Search in Workday for Public Web Services Open the Public Web Services Report 2 3 Hover over Human Resource and click the three dots to access the menu Click Web Services, and then click View 4

- WSDL
- 5 Navigate to the bottom of the page that opens and then you'll find the host
- 6 Copy everything until you see /service and paste below. This should look something like https://wd5-services1.myworkday.com/ccx

/service/ac...

7. Click Next

## Step 2: Enter in your tenant name

1. From the web services URL find your tenant name. In this example, the value

is "acme"	
<pre>v<wsdl:service name="Human_ResourcesService"></wsdl:service></pre>	
<pre>v<wsdl:port binding="wd-wsdl:Human_ResourcesBinding" name="Human_Resources"></wsdl:port></pre>	
<soapbind:address location="https://wd2-impl-services1.workday.com/ccx/service/acme/Human_Resources/v43.0"></soapbind:address>	
<td></td>	

2. Enter the tenant name into the linking flow





3. Click Next

## Step 3: Register a new API Client for Integrations

1. In the Search field, select the Task Register API Client for Integrations.

(	כ	register api client for integrations	
		Register API Client for Integrations Task	
		VIEW MORE	

- On the Register API client for Integrations page, in the Client Name field, enter the Client Name, Scope (Functional Areas), and check Non-Expiring Refresh Tokens and Include Workday Owned Scope. Add the following Scope (Functional Areas):
  - a. Staffing
  - b. Tenant Non-Configurable
  - c. Public data



Client Name	* Test_Client
Refresh Token Timeout (in days)	0
Non-Expiring Refresh Tokens	* 🗸
Disabled	
Scope (Functional Areas)	* X Staffing $(\cdots)$ $\vdots \equiv$
	× Public Data
	$\times$ Tenant Non-Configurable $(\cdots)$
	$\times$ Time Off and Leave $\hfillion{\hfilliot{\hfilliot{\hfilliot{\hfilliot{\hfilli$
Include Workday Owned Scope	
Locked Out due to Excessive Failed Signon Attempts	3
Restricted to IP Ranges	:=
	Cancel

Х

- 3. Click Ok. Save the Client Secret and Client ID. Click Done.
- 4. Enter the Client Secret and Client ID to the linking flow

< Back



#### Enter your client ID and client secret

	client name
4	Select the Non-Expiring Refresh Tokens option
5	In the Scope (Functional Areas) field, select: Tenant Non-Configurable, Staffing, Time Off, and Leave
6	Click <b>OK</b>
7	Enter Client ID and Client Secret below
8	Click Done.
St	ruck? See detailed instructions with screenshots
Clie	nt ID
Clie	nt secret

5. Click Next

## Step 4: Generate a non-expiring Refresh Token

1. In the Search field, select View API Client.



Next

Report

#### **VIEW MORE**

2. On the View API Clients page, click the API Clients for Integrations tab. Save your Token Endpoint.



View API Clients	
Workday REST API Endpoint	https://impl-services1.wd12.myworkday.com/ccx/api/v1/r
Token Endpoint Authorization Endpoint	https://impl-services1.wd12.myworkday.com/ccx/oauth2/ token https://impl.wd12.myworkday.com/ 1/authorize
API Clients API Cl	ients for Integrations

API Clients for Integrations 11 items

- 3. Click the client you created in Step 3: Register a new API Client for Integrations
- 4. Open the three dots > API Client > Click on Manage Refresh Tokens for Integrations

		×
Client Name	API Client	Edit API Client for Integrations
Chent Name	Audits	> Generate New Client Secret
Client Grant Type	Favorite	Manage Refresh Tokens for Integrations
Access Token Type	Integration IDs	>
Refresh Token Timeout (in days)	View API Clients	>

5. On the Manage Refresh Tokens for Integrations page, in the Workday Account field add a user. Save your Refresh Token.

Delete or Regenerate	e Refresh Token 🛛 🍿				
Continuing with this task will DELET 'Generate New Refresh Token', no to	TE any existing refresh token for this when will be generated and you will no	API client and user. Any existing integrations that rely on the ed to re-run this task to get a new one.	ihat token will no longer work,	unless they are updated to use th	e new token. If you do not select
API Client for Integrations API_M Workday Account ISU_M Existing Refresh Token 1 item	ик_то IK_то				<b>⊽ ⊡ .</b> ' 🏾 🖽
API Client	Workday Account	Refresh Token	Issue Time	Expiration Time	Non-Expiring
API_MK_TO	ISU_MK_TO	20 sj8edd h8	09/23/2024 10:44:47.138 AM		
Generate New Refresh Token					

Confirm Delete

#### 6. Add your Token URL and Refresh Token to the linking flow

< Back

 $\times$ 



Enter your refresh token and token URL

<ol> <li>Log in to your Workday tenant</li> <li>In the search field, type View API Client</li> <li>Select the View API Clients task</li> <li>On the View API Clients page, save the URI in the Token Endpoint field</li> <li>Enter the token endpoint URL below</li> <li>Generate a non-expiring refresh token</li> <li>In the search field. type View API client</li> <li>Stuck? See detailed instructions with screenshots</li> <li>Workday OAuth token URL</li> <li>Workday Refresh token</li> </ol>
<ul> <li>2 In the search field, type View API Client</li> <li>3 Select the View API Clients task</li> <li>4 On the View API Clients page, save the URI in the Token Endpoint field</li> <li>5 Enter the token endpoint URL below</li> <li>6 In the search field. type View API client</li> <li>6 Stuck? See detailed instructions with screenshots</li> <li>Workday OAuth token URL</li> <li>Workday Refresh token</li> </ul>
<ul> <li>3 Select the View API Clients task</li> <li>4 On the View API Clients page, save the URI in the Token Endpoint field</li> <li>5 Enter the token endpoint URL below</li> <li>6 In the search field. type View API client</li> <li>6 Stuck? See detailed instructions with screenshots</li> <li>Workday OAuth token URL</li> <li>Workday Refresh token</li> </ul>
<ul> <li>On the View API Clients page, save the URI in the Token Endpoint field</li> <li>Enter the token endpoint URL below</li> <li>Generate a non-expiring refresh token</li> <li>In the search field. type View API client</li> <li>Stuck? See detailed instructions with screenshots</li> <li>Workday OAuth token URL</li> <li>Workday Refresh token</li> </ul>
<ul> <li>5 Enter the token endpoint URL below</li> <li>6 In the search field. type View API client</li> <li>6 Stuck? See detailed instructions with screenshots</li> <li>Workday OAuth token URL</li> <li>Workday Refresh token</li> </ul>
Generate a non-expiring refresh token <ul> <li>In the search field. type View API client</li> <li>Stuck? See detailed instructions with screenshots</li> </ul> Workday OAuth token URL Workday Refresh token Next
Workday OAuth token URL Workday Refresh token Next
Workday Refresh token
Next

8. You are done 😊

7. Click Submit

If you face any issues during this process, please don't hesitate to reach out to us!



## *Workday - How do I link my account with an Integration System User?*

## Overview

To authenticate your Workday account, you will need to provide the following information:

- o WSDL
- o ISU Username
- o ISU Password
- o Workday Tenant Name

## **Prerequisites**

Please ensure you fulfill all the requirements to set up the integration:

- You have Administrator permissions in your company's Workday instance

## Instructions

Step 1: Create an Integration System User (ISU)

- 1. In your Workday portal, log into the Workday tenant
- 2. In the Search field, type Create Integration System User
- 3. Select the Create Integration System User task





- 4. On the Create Integration System User page, in the Account Information section, enter a user name, and enter and confirm a password
  - a. Important: "&", "<", or ">" characters cannot be included in the password
- 5. Click OK

Account Information	
User Name	* ISU_MergeTest2
Generate Random Password	
New Password	* 2
Password Rules	Your new password must not be the same as your current password or user name. Minimum number of characters required: 8. The following character types must be represented: alphabetic characters, uppercase characters, lowercase characters, Arabic numerals 0 - 9, special characters !"#\$%&'()*+,/:;=>?@[\]^_`{}~.
New Password Verify	*3
Require New Password at Next Sign In	🗙 🛶 Do not check this box
Session Timeout Minutes Enforced	120
Session Timeout Minutes	0
Do Not Allow III Sessions	

To ensure the password doesn't expire, you'll want to add this new user to the list of System Users. To do this, search for the Maintain Password Rules task.





6. Add the ISU to the System Users exempt from password expiration field

Default Session Timeout Minutes * 120	
* 🗿 Apply to	o Users with no Individual Session Timeout
Override	e Session Timeout for All Users
System Users exempt from password expiration	× cjdevera-impl / CJ De Vera ∷Ξ
	$\times$ ic2vertexsandboxint
2 Add the ISU here	× IS_Assessment
	× ISULoopIntegrationUser
	× wd-developer / Developer Generic User
	MORE (2)

- 7. Enter the Integration System User name in the linking flow
- 8. Enter the Integration System User password in the linking flow



Exter the credentials for the ISU         How do I find this information?         1       Sign in to Workday         2       Access the Create Integration System User         3       Enter a new username         4       Enter and confirm password         5       Click OK         Stuck? See detailed instructions with screenshots
Enter the credentials for the ISU         How do I find this information?         1       Sign in to Workday         2       Access the Create Integration System User         3       Enter a new username         4       Enter and confirm password         5       Click OK         Stuck? See detailed instructions with screenshots         ISU_MergeTest2
How do I find this information?         1       Sign in to Workday         2       Access the Create Integration System User         3       Enter a new username         4       Enter and confirm password         5       Click OK         Stuck? See detailed instructions with screenshots         ISU_MergeTest2
1       Sign in to Workday         2       Access the Create Integration System User         3       Enter a new username         4       Enter and confirm password         5       Click OK         Stuck? See detailed instructions with screenshots         ISU_MergeTest2
Access the Create Integration System User     Access the Create Integration System User     Access the Create Integration System User     Bitter a new username     Access the Create Integration System User     Click OK     Stuck? See detailed instructions with screenshots     ISU_MergeTest2
3 Enter a new username     4 Enter and confirm password     5 Click OK     Stuck? See detailed instructions with screenshots     ISU_MergeTest2
Enter and confirm password     Source Click OK     Stuck? See detailed instructions with screenshots     ISU_MergeTest2
5 Click OK Stuck? See detailed instructions with screenshots ISU_MergeTest2
Stuck? See detailed instructions with screenshots ISU_MergeTest2
ISU_MergeTest2
Submit

Step 2: Create a Security Group and assign an Integration System User

1. In the Search field, type Create Security Group

Q	Create Security Group	(
	Create Security Group	
	VIEW MORE	



2. Select the Create Security Group task.

On the Create Security Group page, select Integration System Security Group (Unconstrained) from the Type of Tenanted Security Group pull-down menu.

Create Security Group		
Type of Tenanted Security Group *	Integration System Security Group (U 🔻	
Namo *	select one	
Name	Aggregation Security Group	ļ
	Compensation Level-Based Security Group	
	Conditional Role-Based Security Group	
	Integration System Security Group (Constrained)	ок
	Integration System Security Group (Unconstrained)	
	Intersection Security Group	

- 3. In the Name field, enter a name
- 4. Click OK
- 5. On the Edit Integration System Security Group (Unconstrained) page, in the Integration System Users field, enter the same name you entered when creating the ISU in the first section



ISU_Merge_Test2_securityGroup	
Unconstrained	
	Enter the ISU name from Step 1
ISH MergeTest2	
Partial List (First 500 Entries)	>
	ISU_Merge_Test2_securityGroup Unconstrained ISU_MergeTest2 Partial List (First 500 Entries)

6. Click OK

## **Step 3: Configure domain security policy permissions**

1. In the Search field, type Maintain Permissions for Security Group

Q	Maintain permissions	$\times$
	Maintain Permissions for Security Group	
	VIEW MORE	

2. Make sure the Operation is Maintain, and the Source Security Group is the same as the security group that was assigned in Step 2



Modify and review see group. When you copy select Copy User Assi	urity permissions on a specified sec to an existing security group, the exi gnments to copy users from one use	urity group, or copy security permissi isting security group can be of the sa r-based security group to another.	ions from one security group to an existing or new me or different type as the source security group. '	securit 'ou cai
Operation	* O Maintain 1 O Copy			
Source Security Group	<pre>1 * ISU_Merge_Test_securityGreater up</pre>	° … ≔ 2		

3. On the next screen, add the corresponding Domain Security Policies depending on your use case:

Modify, review, an security group, we	d copy security pe e provide a default	ermissions from the source secur aname for the new security group	ity group. Clear the Select that you can modify.	t All check box to exclude all permise	sions from the source security gro	oup. When you copy security p	permissions to a new
Source Security G	Froup ISU_Merg	e_Test_securityGroup					
Domain Securit	y Policy Permission	ns Business Process Security	Policy Permissions 0	Other Usages			
	, , , , , , , , , , , , , , , , , , , ,	_					

4. As you are connecting Workday HRIS HRIS Permissions

## Step 4: Activate security policy changes

1. In the search bar, type "Activate Pending Security Policy Changes" to view a summary of the changes in the security policy that needs to be approved





- 2. Add any relevant comments on the window that pops up
- 3. Confirm the changes in order to accept the changes that are being made and hit OK

Activate r chang occu	try roncy onlinges
All pending security policy changes will	become effective. Please review the data below and click Confirm if you want to procee
Current Security Evaluation Moment	05/10/2024 09:45:13.397 AM
Proposed Security Evaluation Moment	05/16/2024 05:06:22.400 PM
Comment	test
Confirm	

Step 5: Validate the authentication policy is sufficient

1. Search for Manage Authentication Policies



Q	Manage authentication <u>po</u>	$\otimes$
	Manage Authentication Policies	
	VIEW MORE	

2. Click Edit on the authentication policy row

Authentication Policy Evaluation Moment	05/10/2024 09:47:3	39.261 AM			
Comment confirm					
Note	Certain Implemente	ers are required to use VCR IP ranges			
1 item					XIII = 🗆 🖍 🖽
Authentication Policy		Restricted to Environment	Authentication Policy Enabled	Pending Changes	
Authentication Policy for kornferry_dpt1 - Sales		Sales	Yes	No	Edit 1

3. Create an Authentication Rule

Restricted	to Environ	ment 🔸	× Sales	:=				
Authentic	ation Policy	Enabled	<ul> <li>Image: A start of the start of</li></ul>					
Note: The	Network D	enylist will I	be processed prior to the Auther	tication Allowlist.				
<ul> <li>Ne</li> </ul>	twork D	enylist			Manag	je Network	(5)	
ſ			:=					
			:=					
A.,	houtioo	tion All						
✓ Au Authentica	thentica	tion Alle	i≡_ owlist					



4. Enter a name, add the Security Group, and ensure Allowed Authentication Types is set to Specific User Name Password or Any

						Conditions
Authentication Rule Name	*Security Group		Order	*Authentication Condition Name	*Authentication Conditions	*Allowed Authentication Types
ISU_Merge_Test	Sroup	+				
Enter a name for the policy	4 Add the Security Group	(  i )	▼ ▼	condition	Specific     Image: Specific     Any     Any except for other conditions  Device is Managed	Specific  X User Name Password  Any None  Set this to User Name Password or Any

- Note: You don't have to create a new Authentication Rule if you already have an existing one set to User Name Password or Any. You can add the ISU you created to that rule instead.
- You will need to create a new rule if SAML is the only Authentication Rule you see for "Allowed Authentication Types."

### Step 6: Activate all pending authentication policy changes

1. In the search bar type, activate all pending authentication policy changes

Q	Activate all pendin	$\otimes$
	Activate All Pending Authentication Policy Changes Task	-
	VIEW MORE	

2. Proceed to the next screen and confirm the changes. This will save the Authentication Policy that was just created or edited



## Step 7: Obtain the web services endpoint URL

1. Search in Workday for Public Web Services

Q	public web services
	Public Web Services
	Public Web Services and Related Operations Report
	VIEW MORE

- 2. Find Human Resources (Public)
- 3. Click the three dots to access the menu. Click Web Services > View WSDL

Web Service			
Dynamic Document Generation (F	Public)		
External Integrations (Public)			
Financial Aid (Public)			
Financial Management (Public)			
Human Resources (Public) 🚥 🚺		X	
-	Web Service 2	> View Custom WSDL	
Identity Management (Public)	Integration IDs	> View WSDL 3	
Integrations (Public)	Security	>	



- 4. Navigate to the bottom of the page that opens (it may take a few seconds to load)
- 5. Copy the full URL provided under Human\_ResourcesService (Workday HRIS)



6. Enter the Web Services Endpoint URL into the linking flow

	<b>WOIKUUy</b> ®
Step Indp	7/7: Enter your Web Services point URL
4	Click wed Services, and then click view WSDL
5	Navigate to the bottom of the page that opens and look for the web services URL
6	Copy the entire URL and paste below. This should look something like https://services1.myworkday.com/ccx/servic e/acme/Human_Resources/v42.1
St	uck? See detailed instructions with screenshots
http	os://wd2-impl-services1.workday.com/ccx/

7. Click Submit

8. After the connection is established, you will be given the option to map 4 fields to the equivalent of a RydooBranchName, RydooBranchID, RydooGroupName and RydooGroupID.

Map and	additional fields b Hibob. Standard fi	etwee elds a	en Rydoo Productio re already include
	contact_preference	<i>→</i>	call_or_email
	do_not_disturb	→	do_not_call
	is_private	÷	not_public
	M	ap tiei	as
	Ski	p for r	iow

- If you skip this step, the Rydoo default mapping will be used for these fields.
- If you choose to continue with the field mapping, you will see the following options, and you have the chance to map any field from your HR tool to the Rydoo equivalent fields.

Q Select or start typing	]	÷	RydooBranchID Employee
Q Select or start typing	]	÷	RydooBranchName Employee
Q Select or start typing	]	→	RydooGroupID Employee
Q Select or start typing	J	→	RydooGroupName Employee

- 9. You can type in the field name or select from the dropdown.
- 10. After completing the mapping, you can click save and the authentication is now complete.





### **Important Notes**

- Implementation/sandbox tenant Workday accounts will result in slower syncs, as fewer resources are dedicated to the tenant
- In order to increase resourcing for API limits for your Workday tenant, please reach out to Workday Support or your Workday Customer Account Manager.
- You can submit a request to Workday Support through the Workday Community support portal

