

Delinea Workday Integration – Setup Guide

This document describes the steps necessary to setup the Delinea Workday Integration in a Workday customer tenant. Please consult your Delinea technical contact or Delinea account representative for any questions.

Contents

Deliverables to Delinea Technical Contact.....	2
Create Integration System User	3
Create Security Group	3
Exempt Password Expiration.....	9
Add Security Group to Authentication Policy	10
Configure Web Service Security	13
Register API Client.....	16
Create Custom Report: “All Workday Accounts – Delinea”	18
Create Custom Report: “All Security Groups - Delinea”	22

Deliverables to Delinea Technical Contact

The below table lists the items that are to be delivered to your Delinea Technical Contact or Delinea account representative. These items will be the result of fully completing this Setup Guide.

Deliverable	Example <i><u>(Use the values from your tenant, NOT the values below as they are not real)</u></i>
Integration System User (ISU): Username and Password	ISU_Delinea
Client ID	Aaaaaaaaabbbbbbb11111777777777
Workday REST API Endpoint	https://wdtest-impl-services1.workday.com/ccx/api/v1/ customertenant
Token Endpoint	https:// wdtest -impl-services1.workday.com/ccx/oauth2/ customertenant /token
Authorization Endpoint	https://impl.workday.com/ customertenant /authorize
Endpoint URL: All Workday Accounts – Delinea	https:// wdtest -impl-services1.workday.com/ccx/service/customreport2/ customertenant /ISU_Delinea/All_Workday_Accounts_-_Delinea?User_Name=12345&format=json
Endpoint URL: All Security Groups – Delinea	https:// wdtest -impl-services1.workday.com/ccx/service/customreport2/ customertenant /ISU_Delinea/All_Security_Groups_-_Delinea?Reference_ID=12345&format=json

Create Integration System User

1. Search for task, “**Create Integration System User**” in Workday. Enter the following information in the task to create the integration system user (ISU). Click OK when complete:

Create Integration System User

Account Information

User Name

*

ISU_Delinea

Generate Random Password

☐

New Password

*

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 !"#%&'()*+,-./:;<=>?@[\\]^_`{|}~. The password must not have been used within the following number of last passwords: 4.

New Password Verify

*

Require New Password at Next Sign In

☐

Session Timeout Minutes Enforced

480

Session Timeout Minutes

0

Do Not Allow UI Sessions

☒

Cancel

OK

2. Please note the password assigned to the ISU, as well as the ISU username

Create Security Group

1. Search for task, “**Create Security Group**” in Workday. Enter the following information in the task to create the security group. In the “Type of Tenanted Security Group” field, select *Integration System Security Group (Unconstrained)*. Click OK when complete.

Create Security Group

✕

Type of Tenanted Security Group *

Integration System Security Group (U... ▼

Name *

ISSG_Delinea

Cancel

OK

- On the next screen, enter the name of the ISU you created previously (ISU_Delinea). Click OK when complete.

Edit Integration System Security Group (Unconstrained)

ISSG_Delinea

⋮

Name *

ISSG_Delinea

Comment

Context Type

Unconstrained

Inactive

☐

Integration System Users

✕ ISU_Delinea

⋮

Search

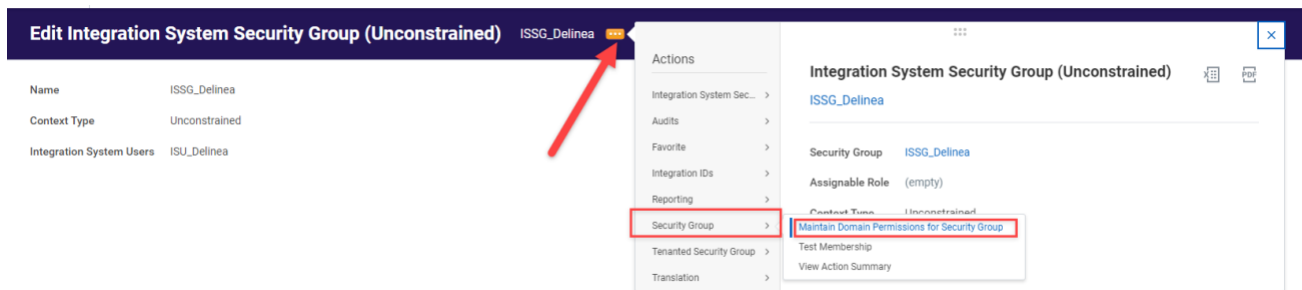
Search Results (1)

☒ ISU_Delinea

OK

Cancel

- After clicking OK to save the newly created security group, click the related action on the security group name and navigate to “Security Group” > **“Maintain Domain Permissions for Security Group”**.



4. On this screen, you will grant the domain security permissions necessary. Please enter the below domains. Click OK when complete.
 - a. If any of the below domains are unavailable for selection, you may need to enable the domain. Please see this Workday Community article for more information: [Steps: Enable Functional Areas and Security Policies \(workday.com\)](https://workday.com/enable-functional-areas-and-security-policies)

Report/Task Permissions

Domain Security Policies permitting Modify access

- × Custom Report Administration ...
- × Custom Report Creation ...

Domain Security Policies permitting View access

- × Custom Report Creation ...
 - × Security Activation ...
 - × Security Administration ...
 - × Security Configuration ...
 - × Workday Accounts ...
 - × Worker Data: Worker ID ...
- [LESS \(1\)](#)

Integration Permissions

Domain Security Policies permitting Put access

- × Workday Accounts ...

Domain Security Policies permitting Get access

- × Special OX Web Services ...
- × User-Based Security Group Administration ...
- × Workday Account Passwords ...
- × Workday Accounts ...

OK

Cancel

5. Search for task, “**Activate Pending Security Policy Changes**” in Workday. Enter a comment. Click OK when complete.

Activate Pending Security Policy Changes

Enter a comment to describe the security changes to be published. On the following screen you will be asked to review and confirm the changes that will take effect.

Current Security Evaluation Moment 02/13/2024 12:14:30.311 PM

Comment * isd

Proposed Security Evaluation Moment 02/13/2024 03:37:30.467 PM

Comment * ISU and ISSG activation.

OK

Cancel

6. On the next screen, click the “Confirm” checkbox and then click OK to activate the security policy changes for the new security group.

Activate Pending Security Policy Changes

All pending security policy changes will become effective. Please review the data below and click Confirm if you want to proceed.

Current Security Evaluation Moment

02/13/2024 12:14:30.311 PM

Proposed Security Evaluation Moment


02/13/2024 03:37:30.467 PM

Comment

ISU and ISSG activation.

Confirm

* ☒



Domain Security Policies

16 items

Domain Security Policy	Last Changed
Workday Accounts	02/13/2024 03:37:14.735 PM
Security Activation	02/13/2024 03:37:14.735 PM
Provisioning Group Administration	02/13/2024 03:37:14.735 PM
Security Configuration	02/13/2024 03:37:14.735 PM
User-Based Security Group Administration	02/13/2024 03:37:14.735 PM
Security Administration	02/13/2024 03:37:14.735 PM
Workday Account Passwords	02/13/2024 03:37:14.735 PM
Special OX Web Services	02/13/2024 03:37:14.735 PM
Set Up: Public Profile	02/13/2024 03:37:14.735 PM

OK

Cancel

Exempt Password Expiration

1. The password for the new ISU you created needs to be set to not expire. Search for task, “**Maintain Password Rules**” in Workday. Scroll to the bottom of the task and enter the ISU you created previously (ISU_Delinea) in the “System Users exempt from password expiration” list. Click OK when complete.

Failed Signon Attempts Before Lockout *

5

Number of Failed Password Reset Attempts Allowed

3

Lockout Minutes

30

Force Password Reset Upon Login

☐

Session Timeout

Default Session Timeout Minutes *

480

*

☐ Apply to Users with no Individual Session Timeout

☒ Override Session Timeout for All Users

System Users exempt from password expiration

x

integration

x

Daily Digest Integration System User

x

E-Verify

x

INT017 Expenses Inbound ISU /

x

INT034a Recruiter System Connect Export

[MORE \(69\)](#)

OK

Cancel

Add Security Group to Authentication Policy

1. The security group that was created (ISSG_Delinea) needs to be added to the authentication allowlist on the authentication policy for your Workday tenant. For details on proper configuration and setting up authentication policies in your Workday tenant, please see the following Workday Admin Guide article: [Steps: Set Up Authentication Policies \(workday.com\)](https://workday.com/Steps: Set Up Authentication Policies (workday.com))
2. Search for task, “**Manage Authentication Policies**” in Workday. (The configuration of the authentication policies in your tenant may be vastly different than what is shown in this setup guide.) Select the “**Edit**” button next to the authentication policy for the Workday tenant you are configuring this integration for:

Manage Authentication Policies

Authentication Policy Evaluation Moment 01/30/2024 11:59:14.878 AM

Comment isd

Note Certain implementers are required to use VCR IP ranges

1 item

Authentication Policy	Restricted to Environment	Authentication Policy Enabled	Pending Changes	
Authentication Policy for centrify5 - Implementation, Production, Sandbox	Implementation Production Sandbox	Yes	No	Edit

[Add Authentication Policy](#)

3. On the next screen, add previously created security group (ISSG_Delinea) to a row in the Authentication Allowlist. Be sure the “Authentication Conditions” and “Allowed Authentication Types” is set to **Any**. Click OK when complete.

Edit Authentication Policy Authentication Policy for centrify5 - Implementation, Production, Sandbox

Restricted to Environment ☒ Implementation ☐ Production ☐ Sandbox

Authentication Policy Enabled ☒ [Manage Networks](#)

Note: The Network Denylist will be processed prior to the Authentication Allowlist.

☒ Network Denylist

☒ Authentication Allowlist

Authentication Ruleset 10 items

Order	Disabled	*Authentication Rule Name	*Security Group	Order	*Authentication Condition Name	*Authentication Conditions	*Allowed Authentication Types
+	-	Product Development	<input checked="" type="checkbox"/> ISSG_Product_Dev	+	API Access	<input checked="" type="radio"/> Any	<input checked="" type="radio"/> Any
+	-			+			
+	-			+			
+	-			+			
+	-			+			
+	-			+			
+	-			+			
+	-			+			
+	-			+			
+	-			+			

[OK](#) [Cancel](#)

4. Search for task, “**Activate All Pending Authentication Policy Changes**” in Workday. Enter a comment. Click OK when complete.

Activate All Pending Authentication Policy Changes

Please review the data below. Enter a comment to describe the authentication policy changes to be published. On the following screen you will be asked to confirm the changes

Current Authentication Policy Evaluation Moment

01/30/2024 11:59:14.878 AM

Comment

isd

Proposed Authentication Policy Evaluation Moment

02/15/2024 09:49:39.396 AM

Comment

* test

Implementation, Production, Sandbox

Authentication Policy

Authentication Policy for centrify5 - Implementation, Production, Sandbox

Restricted to Environment

Implementation
Production
Sandbox

Authentication Policy Enabled

☒

Network Denylist

(empty)

Authentication Ruleset

10 items

Disabled	Authentication Rule Name	Security Group	Authentication Condition Name	Authentication Conditions
<input type="checkbox"/>	Product Development	ISSG_Product_Dev	API Access	*

OK

Cancel

5. On the next screen, click the “Confirm” checkbox and then click OK to activate the authentication policy changes.

All pending authentication policy changes will become effective. Click Confirm if you want to proceed.

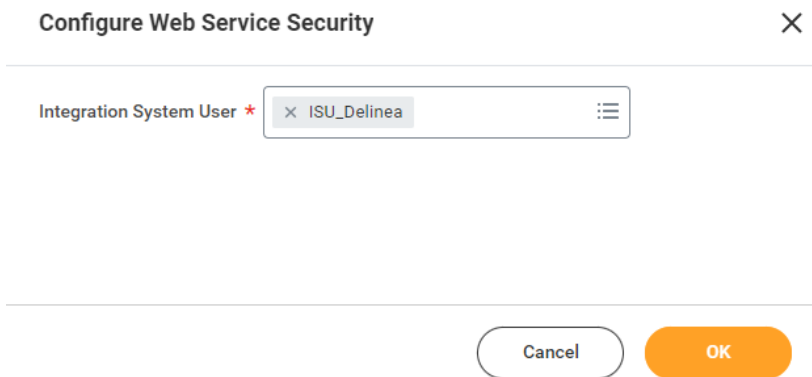
Proposed Authentication Policy Evaluation Moment 02/15/2024 09:49:39.396 AM

Comment test

Confirm ☒

Configure Web Service Security

1. Search for task, “**Configure Web Service Security**” in Workday. Enter the ISU you created in an earlier step (ISU_Delinea) in the prompt. Click OK when complete.

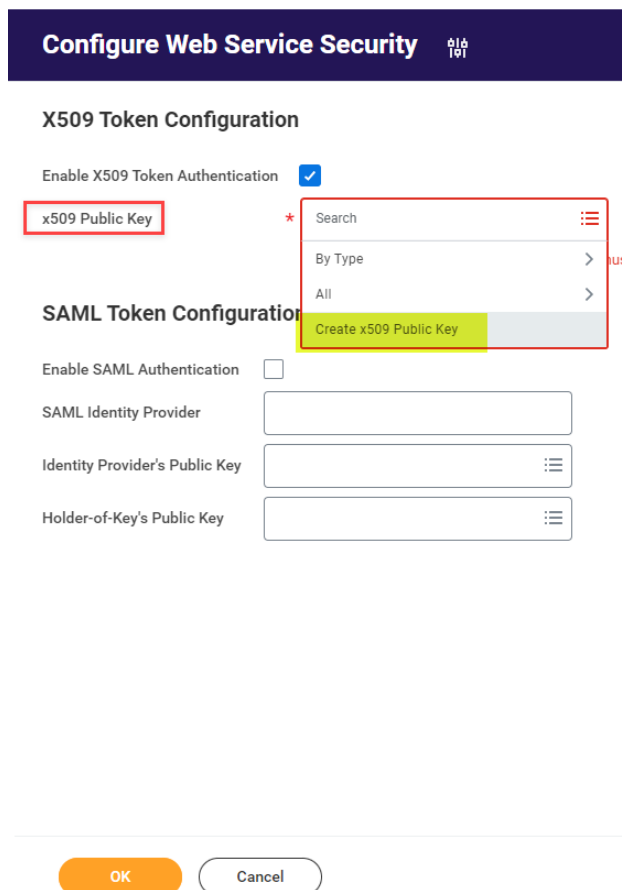


Configure Web Service Security

Integration System User * ISU_Delinea

Cancel OK

2. On the next screen, click the dropdown for the “x509 Public Key” and click “**Create x509 Public Key**”.



Configure Web Service Security

X509 Token Configuration

Enable X509 Token Authentication ☒

x509 Public Key * Search

By Type >

All >

Create x509 Public Key

SAML Token Configuration

Enable SAML Authentication ☐

SAML Identity Provider

Identity Provider's Public Key

Holder-of-Key's Public Key

OK Cancel

- On the Create x509 Public Key screen, paste in the public key was provided to you by your Delinea technical contact. Be sure there are no added spaces, tabs, or returns in the pasted text. If pasted correctly, the “Valid From” and “Valid To” dates will populate. Click OK when complete.

Create x509 Public Key

Name *

Delinea - x509 Public Key

Valid From

02/01/2024

Valid To

01/26/2025

Certificate *

-----BEGIN CERTIFICATE-----
MIID0zCCArugAwIBAgIIU9zgaAO4rpwwDQYJKoZIhvcNAQELBQAwgZcxZCZAJBgNV
BAYTAmNvMQ0wCwYDVQQIEwR0ZXN0MQ0wCwYDVQQHEwR0ZXN0MSIwIAYDVQQDBIJu
U1VfUHJvZHVjdF9EZXAyVudHJpZnk1MSIwIAYDVQQDLDBlJuU1VfUHJvZHVjdF9E
ZXZAY2VudHJpZnk1MSIwIAYDVQQDDDBlJuU1VfUHJvZHVjdF9EZXAyVudHJpZnk1
MB4XDTI0MDIwMTE2MzEyMVoXDTI1MDEyNjE2MzEyMVowgZcxZCZAJBgNVBAYTAmNv
MQ0wCwYDVQQIEwR0ZXN0MQ0wCwYDVQQHEwR0ZXN0MSIwIAYDVQQDBIJuU1VfUHJv
ZHVjdF9EZXAyVudHJpZnk1MSIwIAYDVQQDLDBlJuU1VfUHJvZHVjdF9EZXAyVud
dHJpZnk1MSIwIAYDVQQDDDBlJuU1VfUHJvZHVjdF9EZXAyVudHJpZnk1MIIlBjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKA1H5h4sYynZevr0QzWUvd8i3Yiy
lsXM6m4B4xM5ol6ugRyEgryiZQLz4H4NScw48JyDlfcfkfJtUE/XCQBNXBW+kBI
PTBOK89IWjy0rhY1Imu/QbogFEuBw2NBSFqVZgSedJ+IRqHJj84M490VCbPRJ/B7
3gUWEZ9EYsy6njew4yis5rkN+clOQxLGhwF1oRkaLOZFSpZFVnzUi5Q64ydkcvS3
wIwYQVskHCfwEOSZF6O2PWsN/7JM/mMu3FBIpPjoAXeSS3F6EULOsJPPv8esvfo
oFdR126cQynXVn85vGZZWSavjdrBCzRjPRqNiPicxbOb7ACB7YoWojBN3QIDAQAB
oyEwHzAdBgNVHQ4EFgQUKVmxyFI+cEab4ESDwRupYecXoa4wdQYJKoZIhvcNAQEL
BQADggEBAGoUDR2qgTvlXQPdmMLHCM/qC3GpIHhRGS3Wbg6/nZ7ox5KE87HoU4Nd
6TcYSFgrsn0DOKGzzDIDVXAHXK1Smeyc8/rw2rCjD5q3B7qxGcrrvqLA2H85ST/zX
2+VpSwilJaz71ta482MTAVeY7KievzMBwW+JP2z0zScS7t6lQCMV8Q5al50ev7I

OK

Cancel

4. You should be taken back to the previous Configure Web Service Security screen. Be sure the **“Enable X509 Token Authentication”** checkbox is checked. Click OK when complete.

Configure Web Service Security

X509 Token Configuration

Enable X509 Token Authentication ☒

x509 Public Key *

x Delinea - x509 Public Key

SAML Token Configuration

Enable SAML Authentication ☐

SAML Identity Provider

Identity Provider's Public Key

Holder-of-Key's Public Key

OK

Cancel

Register API Client

6. Search for task, “**Register API Client**” in Workday. Enter the following information in the task to create the API client to allow the Delinea application to access your Workday tenant. Click OK when complete.

Register API Client

Client Name	<input type="text" value="Delinea Integration"/>
Client Grant Type	<div><div><input checked="" type="radio"/> Authorization Code Grant</div><div><input type="radio"/> Implicit Grant (Do Not Use)</div><div><input checked="" type="radio"/> Jwt Bearer Grant</div><div><input type="radio"/> SAML Bearer Grant</div></div>
Support Proof Key for Code Exchange (PKCE)	<input type="checkbox"/>
Enforce 60 Minute Access Token Expiry	<input checked="" type="checkbox"/>
x509 Certificate	<div><div><input checked="" type="radio"/> Delinea - x509 Public Key ...</div><div><input type="radio"/> ISU_Delinea ...</div></div>
Integration System User	<div><div><input checked="" type="radio"/> ISU_Delinea ...</div></div>
Access Token Type	<div><div><input checked="" type="radio"/> Bearer</div><div><input type="radio"/> MAC (Do Not Use)</div></div>
Allow Integration Messages	<input checked="" type="checkbox"/>
Non-Expiring Refresh Tokens	<input type="checkbox"/>
Grant Administrative Consent	<input checked="" type="checkbox"/>
Disabled	<input type="checkbox"/>
Scope (Functional Areas)	<div><div><input checked="" type="radio"/> System ...</div><div><input type="radio"/> System Health Dashboard ...</div><div><input type="radio"/> Tenant Non-Configurable ...</div></div>
Include Workday Owned Scope	<input checked="" type="checkbox"/>
Locked Out due to Excessive Failed Signon Attempts	<input type="checkbox"/>
Restricted to IP Ranges	<input type="text"/>

0 items

	Allowed Origin
<input type="text"/>	

OK

Cancel

Select the x509 Public Key and Integration System User you previously created.

7. On the confirmation screen after clicking OK, **save the highlighted information below from your tenant and provide it to your Delinea technical contact.**

Grant Administrative Consent	Yes
Disabled	No
Scope (Functional Areas)	System System Health Dashboard Tenant Non-Configurable
Include Workday Owned Scope	Yes
Locked Out due to Excessive Failed Signon Attempts	No
Restricted to IP Ranges	(empty)

Client ID

YWM0ZjgyZTgtZjJjOS00OWM2LThiN2MtOTdhMDA3ZWUzMdc0

Workday REST API Endpoint	https://wd2-impl-services1.workday.com/ccx/api/v1/centrify5
Token Endpoint	https://wd2-impl-services1.workday.com/ccx/oauth2/centrify5/token
Authorization Endpoint	https://impl.workday.com/centrify5/authorize

Create Custom Report: “All Workday Accounts – Delinea”

1. Search for task, “**Create Custom Report**” in Workday. Enter the information for the custom report as shown below. **Be sure the “Enable As a Web Service” box is checked.** Click OK when complete.

Create Custom Report

Report Name * All Workday Accounts - Delinea

Report Details

Report Type * Advanced

Temporary Report ☐

Enable As Web Service ☒

Data Source

Optimized for Performance ☐

Alert: Clearing this check box enables you to select a non-indexed data source and non-indexed filters.

Data Source * x All Workday Accounts ...

OK

Cancel

2. Build out the custom report using the report definition .pdf file attached below. Be sure to add all fields, prompts, and filters as defined in the document.



All_Workday_Accounts_Delinea_RAAS.pdf

- Once you have saved the new custom report, All Workday Accounts – Delinea, you need to transfer ownership of the report to the ISU you created previously (ISU_Delinea). On the related action of the report definition, navigate to **“Custom Report” > “Transfer Ownership”**.

View Custom Report All Workday Accounts - Delinea

Report Name: All Workday Accounts - Delinea

Report Type: Advanced

Data Source: All Workday Accounts

Data Source Type: Standard

Primary Business Object: Workday Account

Additional Info

Columns: Sort Filter Prompts Output Share Adva

11 items

Business Object	Field
Workday Account	User Name

- On the screen that appears, select the ISU you created previously (ISU_Delinea) as the New Owner. Click OK when complete.

Transfer Ownership of Custom Reports

Select the reports to be transferred and the new owner

Report Name(s) *

New Owner *

5. You need to provide the web service URL of the custom report, All Workday Accounts – Delinea. On the related action of the report definition, navigate to “Web Service” > “View URLs”.

View Custom Report All Workday Accounts - Delinea

Report Name: All Workday Accounts - Delinea
Report Type: Advanced
Data Source: All Workday Accounts
Data Source Type: Standard
Primary Business Object: Workday Account

> **Additional Info**

Columns | Sort | Filter | Prompts | Output | Share | Advanced

11 items

Business Object	Field

Actions

- Custom Report >
- Audits >
- Favorite >
- Instance >
- Integration IDs >
- Layout >
- Report Definition >
- Reporting >
- Reports >
- Schedule Future Process >
- Solution >
- Web Service > View URLs

6. Enter 12345 in the User Name field that appears, then click OK. (The value entered is irrelevant, it is just needed to temporarily fill the prompt).

View URLs Web Service X

All Workday Accounts - Delinea

User Name

Cancel OK

7. On the next screen, scroll to the bottom to the “JSON” heading. Right click on your mouse on the JSON hyperlink and click “Copy URL”. **The copied URL should be given to your Delinea technical contact. The url you copied should look similar to the following:**

https://wd2-impl-services1.workday.com/ccx/service/customreport2/customertenant/ISU_Delinea/All_Workday_Accounts_-_Delinea?User_Name=12345&format=json


RSS

RSS [RSS](#)

GData

GData [GData](#)

JSON

JSON [JSON](#) 
Copy URL
> Depre [Depre](#) [RLs](#)
Copy Text

Create Custom Report: “All Security Groups - Delinea”

1. Search for task, “**Create Custom Report**” in Workday. Enter the information for the custom report as shown below. **Be sure the “Enable As a Web Service” box is checked.** Click OK when complete.

Create Custom Report

Report Name * All Security Groups - Delinea

Report Details

Report Type * Advanced ▼

Temporary Report ☐

Enable As Web Service ☒

Data Source

Optimized for Performance ☐
Alert: Clearing this check box enables you to select a non-indexed data source and non-indexed data source.

Data Source *

2. Build out the custom report using the report definition .pdf file attached below. Be sure to add all fields, prompts, and filters as defined in the document.



All_Security_Groups
-_Delinea_RAAS_Re

3. Once you have saved the new custom report, All Security Groups - Delinea, you need to transfer ownership of the report to the ISU you created previously (ISU_Delinea). On the related action of the report definition, navigate to “**Custom Report**” > “**Transfer Ownership**”.

MENU

Delinea

Q Search

Edit Custom Report

All Security Groups - Delinea

...

Report Definition

All Security Groups - Delinea

Report Name

All Security Groups - Delinea

Report Type

Advanced

Data Source

Security Groups

Data Source Type

Standard

Primary Business Object

Security Group

> Additional Info

Columns

Sort

Filter

Prompts

Output

Share

6 items

Business Object	Field	Column Heading Override XML A
Security Group	Security Group	Security_Group

Actions

Custom Report

Audits

Favorite

Instance

Integration IDs

Layout

Report Definition

Reporting

Reports

Schedule Future Process

Solution

Web Service

Custom Report

Edit

Configure Alert

Copy

Run

Schedule

Test

Transfer Ownership

Translate

Delete

Custom Report

ps - Delinea

(empty)

Security Groups

Object Security Group

- On the screen that appears, select the ISU you created previously (ISU_Delinea) as the New Owner. Click OK when complete.

Transfer Ownership of Custom Reports



Select the reports to be transferred and the new owner

Report Name(s) *

×

All Security Groups - Delinea

...

:

:

:

New Owner *

×

ISU_Delinea

:

:

:

Cancel

OK

5. You need to provide the web service URL of the custom report, All Security Groups – Delinea. On the related action of the report definition, navigate to “Web Service” > “View URLs”.

The screenshot shows the Delinea user interface. At the top, there's a 'MENU' icon and the 'Delinea' logo. A search bar is on the right. The main header reads 'View Custom Report All Security Groups - Delinea'. Below this, a table lists report details: Report Name (All Security Groups - Delinea), Report Type (Advanced), Data Source (Security Groups), Data Source Type (Standard), and Primary Business Object (Security Group). An 'Additional Info' section is partially visible. A dropdown menu is open from the three-dot icon next to the report title. The menu items include: Actions, Custom Report, Audits, Favorite, Instance, Integration IDs, Layout, Report Definition, Reporting, Reports, Schedule Future Process, Solution, and Web Service. The 'Web Service' item is highlighted with a red box, and its sub-item 'View URLs' is also highlighted with a red box. The right sidebar shows the 'Custom Report' details for 'All Security Groups - Delinea', including a brief description (empty), data source (Security Groups), and primary business object (Security Group).

6. Enter 12345 in the Reference ID field that appears, then click OK. (The value entered is irrelevant, it is just needed to temporarily fill the prompt).

The screenshot shows a dialog box titled 'View URLs Web Service'. Inside the dialog, there's a header with the report title 'All Security Groups - Delinea'. Below the header, there's a 'Reference ID' field with the value '12345' entered. At the bottom of the dialog, there are two buttons: 'Cancel' and 'OK'.

7. On the next screen, scroll to the bottom to the “JSON” heading. Right click on your mouse on the JSON hyperlink and click “Copy URL”. **The copied URL should be given to your Delinea technical contact.** The url you copied should look similar to the following:
`https://wd2-impl-services1.workday.com/ccx/service/customreport2/customertenant/ISU_Delinea/All_Security_Groups_-_Delinea?Reference_ID=12345&format=json`

RSS

RSS RSS

GData

GData GData

JSON

JSON [JSON D...](#)
Copy URL
> Depre Copy Text RLs

About Delinea

Delinea is a leading provider of privileged access management (PAM) solutions for the modern, hybrid enterprise. We make privileged access more accessible by eliminating complexity and defining the boundaries of access to reduce risk, ensure compliance, and simplify security. Delinea empowers thousands of customers worldwide, including over half the Fortune 100. Our customers include the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. delinea.com