Saviynt – Okta Integration Guide

February 2023

Table of Contents

[Document Control 3](#_Toc126854383)

[Pre-Implementation Steps 3](#_Toc126854384)

[Introduction 4](#_Toc126854385)

[Deployment Steps 4](#_Toc126854386)

[Validation Steps 16](#_Toc126854387)

Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version control** | | | |
| **Version** | **Name** | **Role** | **Date** |
| v1 | Geetha S | Author | 01/30/2023 |
| v2 | Gaurav Khandelwal | Author | 02/01/2023 |

Pre-Implementation Steps

|  |  |
| --- | --- |
| Step | Step Instruction |
| 1 | Request Saviynt to take the base snapshot of Saviynt instance before deploying. |
| 2 | Okta Authorization token is generated for the target environment and available for the implementation. |
| 3 | The OKTA SSL certificate for the target environment is deployed in Saviynt and is available for configuring connection. |
| 4 | OKTA deployment export package is available from a lower environment |

Introduction

This document details the deployment steps involved in setting up the Saviynt – Okta connector for group reconciliation, provisioning and managing user access to Okta groups via Saviynt.

Deployment Steps

|  |  |
| --- | --- |
| Step | Step Instruction |
| 1.1 | Login to Saviynt QA environment with administrator user credential. |
| 1.2 | Click on “Admin” on the top right corner and then on “Export Package” under the “Transport”. |
| 1.3 | * Select ‘Connection’ from the drop down ‘Please select the Objects to Export’ * Search and Select the connection from the below table and click on ‘View Summary’.   Note: Update the connection list as per environment. Highlighted in yellow   |  | | --- | | **Connections:** | | [oktanonprod](https://am-dev.saviyntcloud.com/ECM/ecmConfig/addnewconnection/84) | | [oktanonprod\_rest](https://am-dev.saviyntcloud.com/ECM/ecmConfig/addnewconnection/92) |  * Verify and click on ‘Export’ * Rename the exported zip file to CompanyOkta\_Connections.zip |
| 2.1 | Login to Prod Saviynt Security Manager (SSM) as administrator. |
| 2.2 | Click on “Admin” tab from the top right corner menu. |
| 2.3 | Click “Transport” Under “Transport” select “Import Package”. |
| 2.4 | Click on “Browse” next to “Choose package to import” and navigate to release package folder. |
| 2.5 | * Select “CompanyOkta\_Connections .zip”   folder and click on open. Provide the Business Justification. |
| 2.6 | Click on “View Summary”. It will go to next page. |
| 2.7 | Click on “Request”. |
| 3.1 | Login to Saviynt Security Manager (SSM) as administrator |
| 3.2 | Click on “Admin” tab from the top right corner menu. Under “Identity Repository” select “Connections”. |
| 3.3 | Search for “oktanonprod” connection. Edit it |
| 3.4 | Update “oktanonprod” connection as below   |  |  | | --- | --- | | **Attribute Name** | **Attribute Value** | | Connection Name | oktanonprod | | Default SAV Role | ROLE\_COMPANY\_ADMIN | | SSL Certificate | N/A | | ImportURL | [https://company-admin.oktanonprod.com/api/v1](https://cigna-admin.oktapreview.com/api/v1) | | Authtoken | OKTAACCOUNTAUTHTOKEN | | AccountFieldMappings | customproperty1=firstName,  customproperty2=lastName,  customproperty3=email,  customproperty4=secondEmail,  customproperty5=mobilePhone,  customproperty6=status,  customproperty7=employeeID | | OKTA\_APPLICATION\_SECURITYSYSTEM \* | oktanonprod\_securitysystem | | OKTA\_GROUPS\_FILTER | type eq "OKTA\_GROUP" | | STATUS\_THRESHOLD\_CONFIG | {  "statusAndThresholdConfig": {  "statusColumn": "customproperty6",  "activeStatus": ["PROVISIONED","active","ACTIVE"],  "deleteLinks": true,  "accountThresholdValue": 1000,  "correlateInactiveAccounts": false,  "inactivateAccountsNotInFile": false  }  } | |  |  | |
| 3.5 | Save and test the connection |
| 4.1 | Login to Saviynt Security Manager (SSM) as administrator |
| 4.2 | Click on “Admin” tab from the top right corner menu. Under “Identity Repository” select “Connections”. |
| 4.3 | Search for “oktanonprod\_rest” connection. Edit it |
| 4.4 | Update “oktanonprod\_rest” connection as below   |  |  | | --- | --- | | **Attribute Name** | **Attribute Value** | | Connection Name | oktanonprod\_rest | | Default SAV Role | ROLE\_COMPANY\_ADMIN | | SSL Certificate | Select certificate: Select “OKTA Decrypt cert” | |  |  | | ConnectionJSON | {  "authentications": {  "acctAuth": {  "authType": "oauth2",  "url": "https://company-admin.oktanonprod.com/api/v1",  "httpMethod": "POST",  "httpHeaders": {  "contentType": "application/json"  },  "httpContentType": "application/json",  "expiryError": "ExpiredAuthenticationToken",  "authError": [  "InvalidAuthenticationToken",  "AuthenticationFailed"  ],  "timeOutError": "Read timed out",  "errorPath": "error.code",  "maxRefreshTryCount": 5,  "tokenResponsePath": "access\_token",  "tokenType": "SSWS",  "accessToken": "SSWS xxxxxxxxxxxxxxxx"  }  }  } | |  | Note: For access token the provided token must be prefixed with SSWS. | | AddAccessJSON | {  "call": [  {  "name": "OktaGroup",  "connection": "acctAuth",  "url": "https://company-admin.oktanonprod.com/api/v1/groups/${entitlementValue.entitlementID}/users/${account.accountID}",  "httpMethod": "PUT",  "httpHeaders": {  "Authorization": "${access\_token}",  "Accept": "application/json"  },  "httpContentType": "application/json",  "successResponses": {  "statusCode": [  200,204  ]  }  }  ]  } | | RemoveAccessJSON | Updated the highlighted part per environment. In production the preview is removed.  {  "call": [{  "name": "OktaGroup",  "connection": "acctAuth",  "url": "https://company-admin.oktanonprod.com/api/v1/groups/${entitlementValue.entitlementID}/users/${account.accountID}",  "httpMethod": "DELETE",  "httpHeaders": {  "Authorization": "${access\_token}",  "Accept": "application/json"  },  "httpContentType": "application/json",  "successResponses": {  "statusCode": [  200, 204  ]  }  }]  } | |
| 4.5 | Save and test the connection |
| 5.1 | Login to SSM with administrator user credential. |
| 5.2 | Click on “Admin” on the top right corner and then on “Security Systems” under the “Identity Repository”. |
| 5.3 | **Security System:**  Click on “Action” and then select “Create Security System”. |
| 5.4 | Fill the details of the Security System as below.   |  |  | | --- | --- | | **Attribute Name** | **Attribute Value** | | System Name | oktanonprod | | Display Name | okta workforce preview tenant security system | | Connections | oktanonprod | | Provisioning Connection | oktanonprod\_rest | | Policy Rule | N/A | | Access Add Workflow | Requried Approval Workflow | | Access Remove Workflow | Requried Approval Workflow | | Default System | No | | Automated Provisioning | Enable | | Manage Entity | No | | Persistent Data | Yes | | Use open connector | No | | Recon Application | Yes | | Instant Provisioning | Enable | |
| 5.5 | Click on “Create” |
| 6.1 | Once the Security System is created, again go to “Security Systems”, under the “Identity Repository”. Click on “Endpoints” |
| 6.2 | CIick on “Actions”, then select “Create Endpoint” |
| 6.3 | Fill the details of the Endpoint as below.   |  |  | | --- | --- | | **Attribute Name** | **Attribute Value** | | Endpoint Name | oktanonprod | | Display Name | OKTA Non-prod | | Security System | okta nonprod | | Description | OKTA Workforce Test system | |
| 6.4 | Click on “Create” |
| 6.5 | Once endpoint is created, update with below details.   |  |  | | --- | --- | | **Attribute Name** | **Attribute Value** | | Access Query | WHERE USERS.USERKEY in( select USERKEY from user\_accounts where ACCOUNTKEY in( select ACCOUNTKEY from accounts where ENDPOINTKEY = OKTAENDPOINTKEY and STATUS in( 1,'Manually Provisioned')))  Endpoint key needs to be updated after the OKTANONPROD endpoint is created in PROD | | User Account Correlation rule | * Click on ‘Add’   Set username set to customproperty7   * Save | |  |  | | Connection Configuration | <conf></conf> | | ON | Disable Remove Account  Disable New Account Request if Account Already Exists  Disable Remove Service Account  Disable Modify Service Account  Disable New Account Request if Service Account Already Exists  Requestable | | OFF | Enable Copy Access  Disable Modify Account, Create Dependent Entitlement Task for Remove Access  Ask For Start Date While Removing Application Role along with Entitlements Request  Copy Service Account Request Data  Allow Remove All Roles while Request  Block any request due to existing request/task in-flight  Ask For Start Date End Date While Adding Application Role along with Entitlements Request  Disable Sorting for selected entitlements for step 2 page of request form | |  |  | |
| 6.6 | Click on Update. |
| 6.7 | Go to “Entitlement Type” Tab. |
| 6.8 | Create new entitlement type |
| 6.9 | Fill the details as below.   |  |  | | --- | --- | | **Attribute Name** | **Attribute Value** | | Entitlement Name | OktaGroup | | Display Name | Groups | | Endpoint Name | oktanonprod | | Entitlement Description | Select the ADD button to request additional Groups defined in Okta Workforce | | ADD Workflow | Required Approval Workflow | |
| 6.10 | Click on ‘Create’. |
| 6.11 | Change the “Request-Option” as “Table” for “Group” Entitlement Type. |
| 7.1 | Login to SSM with administrator user credential. |
| 7.2 | Click on “Admin” on the top right corner and then on “Security Systems”. Under the “Identity Repository”. |
| 7.3 | Click on the Endpoints and search for  oktanonprod  Go to “Other Attributes” tab and add below   |  |  | | --- | --- | | **User Profile Custom Property** | **Label** | | Account Custom Property 1 Label | First Name | | Account Custom Property 2 Label | Last Name | | Account Custom Property 3 Label | Email | | Account Custom Property 4 Label | Second Email | | Account Custom Property 5 Label | Mobile Phone | | Account Custom Property 6 Label | Okta Status | | Account Custom Property 7 Label | Employee ID | | Account Custom Property 31 label | Status Field for Internal Processing | |
| 8.1 | Login to SSM with administrator user credential. |
| 8.2 | Click on “Admin” tab from the top right corner menu. Under “Job Control Panel” select “Job Control Panel”. |
| 8.3 | Click on “+Add New Job” |
| 8.4 | Provide the Job Name as “OKTANONPROD\_FULL\_ACCOUNT\_RECON” and select Job Type as “Application Data Import (Multi Threaded)” under “Data” category.  Provide the System name as  okta nonprod security system  Provide the connection name as  oktanonprod |
| 8.5 | Provide the Job Type name as “Full Import”  Provide the Import Type name as “Oktaaccounts” |
| 8.6 | Click on “Save”. |
| 8.7 | Repeat above steps 8.1 to 8.6 to create below jobs   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Job Name** | **Job Type** | **System** | **Connection** | **Job Type** | **Import Type** | | OKTANONPROD\_FULL\_GROUP\_RECON | Application Data Import (Multi Threaded) | Same as step 8.4 | Same as step 8.4 | Full Import | Groups | | OKTANONPROD\_INCREMENTAL\_ACCOUNT\_RECON | Application Data Import (Multi Threaded) | Same as step 8.4 | Same as step 8.4 | Incremental Import | Oktaaccounts | | OKTANONPROD\_INCREMENTAL\_GROUP\_RECON | Application Data Import (Multi Threaded) | Same as step 8.4 | Same as step 8.4 | Incremental Import | Groups | |
| 9.1 | Schedule OKTANONPROD\_FULL\_ACCOUNT\_RECON  Once a week (Prod only) |
| 9.2 | Schedule OKTANONPROD\_FULL\_GROUP\_RECON  Once a week (Prod only) |
| 9.3 | Schedule OKTANONPROD\_INCREMENTAL\_ACCOUNT\_RECON  Daily (Prod only) |
| 9.4 | Schedule OKTANONPROD\_INCREMENTAL\_GROUP\_RECON  Daily (Prod only) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Steps to update SHOW FAILED TASKS FOR OKTA GROUP MANAGEMENT report | | | | |
| 10.1 |  |  | Login to SSM with administrator user credential. |  |
| 10.2 |  |  | Click on “Intelligence” on the top right corner |  |
| 10.3 |  |  | Search for “SHOW FAILED TASKS FOR OKTA GROUP MANAGEMENT”. |  |
| 10.3 |  |  | Click the analytics name to edit it. |  |
| 10.4 |  |  | Scroll down to the bottom and click on “Edit” button. |  |
| 10.5 |  |  | Replace the Analytics Query with the following  select  arstasks.taskkey as 'Task Id',  roles.role\_name as 'Okta Group name',  roles.description as 'Okta Group Description',  roles.displayname as 'Okta Group Display Name',  case  when arstasks.tasktype='24' then 'Create Entitlement'  when arstasks.tasktype='1' then 'Add Access'  END as 'Task Type',  (  SELECT CONCAT(users\_tbl.FIRSTNAME,' ',users\_tbl.LASTNAME)  FROM USERS users\_tbl  where users\_tbl.USERKEY = arstasks.userkey  )'Requested For',  arstasks.accountname as 'Account Name',  securitysystems.displayname as 'Security System',  endpoints.displayname as 'Endpoint',  CASE  WHEN arstasks.STATUS =1 THEN 'New'  WHEN arstasks.STATUS =2 THEN 'In Progress'  WHEN arstasks.STATUS =3 THEN 'Completed'  WHEN arstasks.STATUS =4 THEN 'Discontinued'  WHEN arstasks.STATUS =5 THEN 'Pending Create'  WHEN arstasks.STATUS =6 THEN 'Pending Provisioning'  WHEN arstasks.STATUS =7 THEN 'Provisioning Failed'  WHEN arstasks.STATUS= 8 THEN 'Error'  WHEN arstasks.STATUS= 9 THEN 'STATUS\_NO\_ACTION\_REQUIRED'  END AS 'Task Status',  arstasks.taskdate as 'Task Date',  arstasks.provisioningcomments as 'Provisioning Comments',  arstasks.provisioningmetadata as 'Provisioning Metadata',  arstasks.updatedate as 'Task Update Date'  from  arstasks,  users,  securitysystems,  endpoints,  roles  where  arstasks.userkey=users.userkey  and securitysystems.systemkey=arstasks.securitysystem  and endpoints.endpointkey=arstasks.endpoint  and arstasks.sourceid=roles.rolekey  and (arstasks.tasktype='24' OR arstasks.tasktype='1')  and arstasks.PROVISIONINGTRIES IS NOT NULL  and arstasks.PROVISIONINGTRIES >= 1  and arstasks.status NOT IN (3,4,9)  and endpoints.endpointname in ('oktanonprod', 'core::okta::company\_okta::okta')  UNION  select  arstasks.taskkey as 'Task Id',  entitlement\_values.entitlement\_value as 'Okta Group name',  entitlement\_values.description as 'Okta Group Description',  entitlement\_values.displayname as 'Okta Group Display Name',  case  when arstasks.tasktype='1' then 'Add Access'  END as 'Task Type',  (  SELECT CONCAT(users\_tbl.FIRSTNAME,' ',users\_tbl.LASTNAME)  FROM USERS users\_tbl  where users\_tbl.USERKEY = arstasks.userkey  )'Requested For',  arstasks.accountname as 'Account Name',  securitysystems.displayname as 'Security System',  endpoints.displayname as 'Endpoint',  CASE  WHEN arstasks.STATUS =1 THEN 'New'  WHEN arstasks.STATUS =2 THEN 'In Progress'  WHEN arstasks.STATUS =3 THEN 'Completed'  WHEN arstasks.STATUS =4 THEN 'Discontinued'  WHEN arstasks.STATUS =5 THEN 'Pending Create'  WHEN arstasks.STATUS =6 THEN 'Pending Provisioning'  WHEN arstasks.STATUS =7 THEN 'Provisioning Failed'  WHEN arstasks.STATUS= 8 THEN 'Error'  WHEN arstasks.STATUS= 9 THEN 'STATUS\_NO\_ACTION\_REQUIRED'  END AS 'Task Status',  arstasks.taskdate as 'Task Date',  arstasks.provisioningcomments as 'Provisioning Comments',  arstasks.provisioningmetadata as 'Provisioning Metadata',  arstasks.updatedate as 'Task Update Date'  from  arstasks,  users,  securitysystems,  endpoints,  entitlement\_values  where  arstasks.userkey=users.userkey  and arstasks.entitlement\_valuekey=entitlement\_values.entitlement\_valuekey  and securitysystems.systemkey=arstasks.securitysystem  and endpoints.endpointkey=arstasks.endpoint  and arstasks.tasktype='1'  and arstasks.PROVISIONINGTRIES IS NOT NULL  and arstasks.PROVISIONINGTRIES >= 1  and arstasks.status NOT IN (3,4,9)  and endpoints.endpointname in ('oktanonprod') |  |
| 10.6 |  |  | Click “Update”. |  |
| 10.7 |  |  | Confirm the columns to show and click “Submit”. |  |

Validation Steps

*These steps validate the change.*

|  |  |
| --- | --- |
| Step | Step Instruction |
| 1 | Validate following connection, security system, endpoint, jobs, SAV role and report are configured as instructed  Connection   * oktanonprod * oktanonprod\_rest   Security System   * oktanonprod   Endpoint   * oktanonprod   Job   * OKTANONPROD\_FULL\_ACCOUNT\_RECON * OKTANONPROD\_FULL\_GROUP\_RECON * OKTANONPROD\_INCREMENTAL\_ACCOUNT\_RECON * OKTANONPROD\_INCREMENTAL\_GROUP\_RECON   Analytics   * SHOW FAILED TASKS FOR OKTA GROUP MANAGEMENT |