

# LAB GUIDE - Tip Sheet Outline

## 1 - Building Identity Warehouse - Lab

*Use case 1: Import User Records from Authoritative Applications (HRMS)*

Use case 2: Onboard Application (Connected) – Active Directory

Use case 3: Onboard Application – Generic Disconnected

Use case 4: Manage Entitlements

Use case 5: View Imported Data from Oracle – EBS

Use case 6: Identity Warehouse Validation

Building Identity Warehouse [Lab Guide p12] - How to:

Upload users from external flat files.

Create Security Systems, Endpoints, Connections and associate them.

Onboard connected and disconnected applications.

Import Accounts, Entitlements and Roles.

### **Use Case 1: Import User Records from Authoritative Applications (HRMS)**

Reference Use Case 1 – To add new authoritative source

Refer to lab pages #14 – 24

### **Use Case 2: Onboard Connected Application – Active Directory**

Task 1- Create Security System

1 - Admin > Identity Repository > Security System

2 - Actions > Create Security System

3 - Enter System name

Active Directory > Enter details as shown > Select Create

Successfully created Active Directory Security System

Task 2- Create an Endpoint

1 - Admin > Identity Repository > Security System

2 - Endpoints > Actions > Create Endpoint

3 - Create a new Endpoint Active Directory with the details as shown >  
Select Create

Successfully created the Active Directory Endpoint.

Task 3- Configure Endpoint

1 - Admin > Identity Repository > Security System

2 - Select Endpoints > Select Active Directory Endpoint

3 - User Account Correlation Rule > Select Add

User Account Correlation Rules are used to map users to accounts

4 - Add the User Account Correlation Rule > Select Save

5 - Account Name Rule > Select Add

6 - Add Account Name Rule > Select Save

7 - Select Update

8 - Select Continue

Successfully configured the Active Directory Endpoint

#### Task 4 – Create Connection

- 1 - Admin > Identity Repository > Connections
- 2 - Select Actions > Create Connection
- 3 - Enter details as shown

Enter the connection details using the file - adConnectionParams.txt (from the Data Files folder)

*Note: Enter the connection parameters from adConnectionParams.txt. Ensure no white spaces are present in the entered value as it will lead to a connection failure.*

- 4 - Select Save & Test Connection after entering all parameters from the file.
- 5 - Confirm that connection is Successful

Successfully created a connection for Active Directory

#### Task 5- Configure Connection in Security System

- 1 - Admin > Identity Repository > Security System
- 2 - Select Active Directory Security System
- 3 - Select the connection as Active Directory from the Connection and Provisioning drop-down list  
> Select Update

Successfully configured the Active Directory connection in Security System.

#### Task 6- Reconcile Data from Active Directory

- 1 - Admin > Job Control Panel
- 2 - Select Add New Job
- 3 - Enter the following details
  - Job Name: AD\_Import
  - Job Type: Application Data Import (Single-Threaded)
  - System: Active Directory
  - External Connection: Active Directory (*This will be Auto Populated*)
  - Job Type: Full Import
  - Import Type: Accounts (*This will import the accounts*)
- 4 - Save
- 5 - Search for the AD\_Import Job and Select the Play icon. This will run the import job.
- 6 - Verify the job status as success
- 7 - Select the Edit icon
- 8 - Change the Import Type as Access (to import the entitlements) > Select Save
- 9 - Search for the AD\_Import Job > Select the Play icon again > Verify that the job Status is Success

Successfully reconciled data from the Active directory into Saviynt EIC

*Note: If you run only the Accounts job, it will import only entitlements that are assigned to the accounts.*

*Entitlements which are not assigned to any account will not be imported. Ensure that you run both Accounts and Access job to import both accounts and entitlements.*

#### Task 7- Validate Imported Data

- 1 - Admin > Identity Repository > Security System
- 2 - Select Endpoints > Select Active Directory Endpoint
- 3 - Verify the imported Active Directory Entitlement Type
- 4 - Verify the imported Active Directory Accounts
- 5 - Verify the imported Active Directory Entitlements
- 6 - Search and Select entitlement  
CN=Finance,OU=Groups,OU=Training,DC=aspire,DC=saviynt,DC=com
- 7 - Change the status to Active > Select Update

Successfully validated imported data in Active Directory

### Use Case 3: Onboard Disconnected Application – Amigopod

Import accounts and entitlements from Amigopod into EIC and link them to existing Users.

This is a Disconnected application and Data is imported from flat files.

#### Task 1- Create and Configure Amigopod Application

- 1 - Admin > Identity Repository > Security System
- 2 - Actions > Create Security System
- 3 - Enter System name Amigopod > Enter details, Leave other settings as default > Select Create
- 4 - Identity Repository > Security System
- 5 - Endpoints > Actions > Create Endpoint
- 6 - Endpoint name as Amigopod > Enter details as shown > Select Create
- 7 - User Account Correlation Rule > Select Add
- 8 - Add User Account Correlation Rule > Select Save
- 9 - Account Name Rule > Select Add
- 10 - Add Account Name Rule > Select Save
- 11 - Select Update
- 12 - Select Continue

Successfully configured the Amigopod Application

#### Task 2- Import Amigopod Accounts

Import Amigopod accounts from a file as it is a Disconnected Application

- 1 - Admin > Identity Repository > Accounts
  - 2 - Select Actions > Upload Accounts
  - 3 - Select the AmigopodAccounts.csv file from the Data Files folder > Enter the System Name as Amigopod > Select Upload & Preview
    - 3a - Create New under Entitlement Type
    - 3b - Enter Role in the pop-up window > Select Submit
    - 3c - Select ROLE from the drop-down list as shown
  - 4 - Select Create New under Entitlement Type
- Select the attribute mapping as below:
- Column 1 = Account Name
  - Column 2 = Endpoint
  - Column 3 = ROLE (Follow the steps to create this new field)
  - Column 4 = Status
- 5 - Verify the mapped columns > Select Import Now
- You will land on summary page – displays upload details*

Successfully imported Amigopod accounts

#### Task 3- Import Amigopod Entitlements

- 1 - Admin > Identity Repository > Entitlements
- 2 - Select Actions > Upload Entitlement From CSV
- 3 - Select the file AmigopodEntitlements.csv > Select Upload & Preview
- 4 - Select Import Now *[You will land on summary page – displays upload details]*

Successfully imported Amigopod Entitlements into EIC from a file

#### Task 4- Validate Imported Accounts and Entitlements

- 1 - Admin > Identity Repository > Security System
- 2 - Select Endpoints > Select Amigopod Endpoint
- 3 - Select Accounts > Validate the imported accounts
- 4 - Select Entitlements > Validate the imported entitlements

Successfully validated imported Amigopod Accounts and Entitlements

## Use Case 4: Onboard Disconnected Application - Siebel MRM

Import accounts and entitlements from Siebel MRM into EIC and link them to the existing Users.

This is a Disconnected application.

### Task 1- Create and Configure Siebel MRM Application

- 1 - Admin > Identity Repository > Security System
- 2 - Select Actions > Create Security System
- 3 - Enter the System name as Siebel MRM > Enter details as shown > Select Create
- 4 - Identity Repository > Security System > Endpoints > Actions > Create Endpoint
- 5 - Enter the Endpoint name as Siebel MRM > Enter details as shown > Select Create
- 6 - User Account Correlation Rule > Select Add
- 7 - Add the User Account Correlation Rule > Select Save
- 8 - Account Name Rule > Select Add
- 9 - Add Account Name Rule as shown > Select Save
- 10 - Select Update
- 11 - Select Continue

Successfully configured the Siebel MRM Application

### Task 2- Import Siebel MRM Accounts

Import Siebel MRM accounts from a CSV file (Disconnected Application)

- 1 - Admin > Identity Repository > Accounts
- 2 - Select Actions > Upload Accounts
- 3 - Select the SiebelAccounts.csv file from the Data Files folder > Enter the System Name as Siebel MRM > Select Upload & Preview
  - 3a - Select Create New under Entitlementment Type
  - 3b - Enter Responsibility in the pop-up window
  - 3c - Select Responsibility from the drop-down list
- 4 - Select the attribute mapping as below
  - Column1 = Account Name
  - Column2 = Endpoint
  - Column3 = Responsibility (Follow the steps to create new field)
  - Column 4 = Status
- 4 - Select Import Now > *(You will land on the summary page)*

Successfully imported Siebel MRM Accounts

### Task 3- Import Siebel MRM Entitlements

- 1 - Admin > Identity Repository > Entitlements
- 2 - Select Actions > Upload Entitlementment From CSV
- 3 - Select the file SiebelEntitlements.csv > Select Upload & Preview
- 4 - Select Import Now > You will land on the summary page

### Task 4- Validate Imported Accounts and Entitlements

- 1 - Identity Repository > Security System > Endpoints [Search and Select the Siebel MRM Endpoint]
- 2 - Select Accounts > Validate the imported accounts
- 3 - Select Entitlements > Validate the imported Entitlements

Successfully validated imported Siebel MRM Accounts and Entitlements

## Use Case 5: Import Roles

### Task 1- Set-up Global configuration

- 1 - Admin > Global Configurations
- 2 - Select Roles from the drop-down list > Verify that Role modification auto approve box is checked

Successfully set-up global configuration for importing roles.

#### Task 2- Import Roles from File

- 1 - Admin > Identity Repository > Roles
- 2 - Select Actions > Upload Role Association
- 3 - Select the Roles.csv file from folder > Select Upload & Preview
- 4 - Select Import Now
- 5 - Validate Imported Roles
- 6 - Validate associated entitlements of Role Analyst Level 2
- 7 - Admin > Identity Repository > Roles > Select Mortgage Manager2
- 8 - Validate associated entitlements of Role Mortgage Manager2

#### Use Case 6: Verify Imported Data from Oracle EBS

Accounts and entitlements from Oracle EBS are already imported

##### Task 1- Verify Security System, Accounts and Entitlements (Oracle EBS)

- 1 - Admin > Identity Repository > Security System
- 2 - Search and Select OracleEBS
- 3 - Select Endpoints > Select OracleEBS
- 4 - Validate Accounts
- 5 - Validate Entitlements

Successfully verified the imported Oracle EBS data in Saviynt EIC.

#### Use Case 7: Validate Identity Warehouse Data

##### Task 1- Validate the imported and correlated data in Saviynt EIC

- 1 - Admin > Identity Repository > Users
- 2 - Search for the User "jdoe" > Select the User
- 3 - Verify "jdoe's" accounts as shown

Successfully validated Identity Warehouse

## 2 - Saviynt Roles - Lab

Use case 1: Verify and assign out-of-the-box SAV Roles

Use case 2: Create and assign Custom SAV Roles for Reporting Manager

Use case 3: Create and assign Custom SAV Roles for End-User

Use case 4: Reset the password of a User in Saviynt EIC

#### Lab Guide [page 84] - How to:

Create custom SAV Roles

Assign SAV Roles to different users

Reset User passwords

#### Use Case 1: Verify and assign out-of-the-box SAV Roles

##### Task 1- Validate out-of-the-box SAV Roles

- 1 - Admin > Sav Roles
- 2 - Select ROLE\_ADMIN
- 3 - Verify the details as shown

Successfully validated SAV Role ROLE\_ADMIN

##### Task 2 - Assign out-of-the-box SAV Admin Role to a User

- 1 - Select Users > Select Actions > Add new user
  - 2 - Search and Select the user to assign the ROLE\_ADMIN Role > For Example - U138859 > Select Save
- Task 3- Validate out-of-the-box SAV Admin Role for a User

*Tip: You can assign a SAV role to multiple users by searching & selecting multiple users together*

Successfully assigned admin SAV Role to a user.

Task 3- Validate out-of-the-box SAV Admin Role for a User

1 - Admin > Identity Repository > Users

2 - Search and Select the username for which you assigned ROLE\_ADMIN [Example – U138859]

3 - Select SAV Roles > Validate SAV Role assigned to the user

*Tip: You can add a new SAV Role to the user from this page by selecting Action > Add SAV Role.*

Successfully validated the user's SAV Role.

## **Use Case 2: Create & Assign Custom SAV Role - Reporting Manager**

Reporting Manager should have access to perform the following tasks in Saviynt EIC:

Request access for all the users in the organization.

Approve the requests assigned to the manager.

View all requests associated with the manager, direct reports, and direct report's reportees.

Task 1- Create a Custom SAV Role for Reporting Manager

1 - Admin > Sav Roles

2 - Select Create SAV Role

3 - Select Create New

4 - Enter the details as shown > Select Create

5 - Select Feature Access > Actions > Add New Access to add access to SAV Role

6 - Search for the features one by one > Select Add to add them to SAV Role.

Application Request steps are shown - Follow the same steps for other 10 items listed.

- Application Request
- Home
- All Campaign Certification Review Access
- Create Delegate
- Pending Actions
- Pending Approvals
- Request Access for Others
- Request Access for Others – Multi-User
- Request Access for Self
- Request History
- View Delegates

Select Done once all are added.

*Note: The Home Feature access is mandatory for users to Login to Saviynt EIC.*

7 - Confirm that the Feature Access is added

8 - Select Create Request Home Option > Select the options as shown

Successfully created a Custom SAV Role for Reporting Manager.

Task 2- Assign Custom Reporting Manager SAV Role to a User

1 - Users > Actions > Add new user

2 - Search/Select the user to assign the ROLE\_MANAGER\_TRAINING Role > Example –jwen > Select Save

3 - Confirm that the User is added as shown.

Successfully assigned a custom Manager Sav Role to a user

## **Use Case 3: Create & Assign Custom SAV Roles for End-User**

End user should have access to perform the following tasks in Saviynt EIC:

Request access for himself.

Approve the requests assigned to the user.

View all requests associated with the user.

#### Task 1- Create a Custom SAV Role for End-User

- 1 - Admin > Sav Roles
- 2 - Create SAV Role
- 3 - Select Create New
- 4 - Enter the details as shown > Select Create
- 5 - Feature Access > Actions > Add New Access to add access to SAV Role
- 6 - Search for the features one by one > Select Add to add them to SAV Role.

Application Request steps are shown - Follow the same steps for other 5 items listed.

- Application Request
- Home
- Pending Actions
- Pending Approvals
- Request Access for Self
- Request History

> Select Done once all are added.

*Note: Feature access allows to control users' access to various modules and features based on their SAV roles.*

*Home Feature access is mandatory for users to Login to Saviynt EIC.*

7 - Confirm that the Feature Access is added as shown

8 - Select Create Request Home Option > Select the options as shown >

*(Controls enabling/disabling tiles on the Request Home menu)*

Successfully created a Custom SAV Role End User

#### Task 2- Assign Custom End-User SAV Role to a User

- 1 - Users > Actions > Add new user
- 2 - Search/Select the user to assign the ROLE\_END\_USER\_TRAINING Role [Example – jdoe] > Select Save
- 3 - Confirm the users is added as shown

Successfully assigned the End User SAV Role to a User

### Use Case 4: Reset the password of a User in Saviynt EIC

#### Task 1- Reset the password of a User in Saviynt EIC

- 1 - Admin > Admin Function > Admin Functions
- 2 - Search for the user [N084731] > Select Manage
- 3 - Select Change Password > Enter a temporary password > Select Save

## 3 - Rules Engineering – Lab

Use case 1: Set up Technical Rule for Birthright access.

Use case 2: Set up User Update Rules for Employee Transfer.

Use case 3: Set up User Update Rules to revoke access past Employment End Date.

Use case 4: Set up User Update Rules for Employee Termination.

Lab Guide [page 109] - How to:

Create & trigger Technical Rules for Birthright access

Create & trigger User Update Rules during Employee Transfer

Create & trigger User Update Rules during Employee Termination

### Use Case 1: Set up Technical Rule for Birthright Access

Automate Access Provisioning during the different Identity lifecycle events

\*Provide Birthright Access to New hires from Saviynt EIC

Ex: Create a technical rule which gets triggered when a new User from Bangalore is created

Task 1- Create Provisioning Rules for Birthright Access

1 - Admin > Policies > Technical Rules

2 - Actions > Create Technical Rules

Ex: Create a technical rule which gets triggered when a new User from Bangalore is created

3 - Enter the details as shown > Select Send for Approval

4 - Confirm that the status of Rule is Active

*Note: To set the Technical Rule for auto approval, Go to Admin > Global Configurations > Rules > Select the checkbox for Rule auto Approve.*

Successfully created a provisioning rule for birthright access.

Task 2- Trigger Provisioning Rules for Birthright Access

1 - Admin > Identity Repository > Users

2 - Select Actions > Create User

3 - Enter the user details as shown > Select Create

**Caution: Values are case sensitive. Ensure the way the city field was entered matches the rule created in Task 1.**

Task 3- Validate Tasks created for provisioning Birthright Access

1 - Home > Tasks > Pending Tasks

2 - Confirm the tasks generated as shown.

Successfully triggered Technical Rules to provision Birthright Access

*Note: Refresh the page if you don't see the tasks right away.*

### **Use Case 2: Set up User Update Rules for Employee Transfer**

Create a User Update Rule to trigger/Remove access from an Employee when transferred to a different city.

Task 1- Create User Update Rules for Employee Transfer

1 - Admin > Policies > User Update Rules

2 - Actions > Create User Update Rule

3 - Enter the details as shown > Select Send for Approval

4 - Confirm that the status of Rule is Active

Successfully created User Update rule for Employee Transfer.

Task 2- Trigger User Update Rules for Employee Transfer

1 - Admin > Identity Repository > Users

2 - Search and Select the user GMarkle

3 - Update GMarkle's city to Vancouver > Select Update

Task 3- Validate Tasks created by User Update Rules for Employee Transfer

1 - Home > Tasks > Pending Tasks

2 - Confirm that the task is generated

*Note: Refresh the page if you don't see the tasks right away.*

### **Use Case 3: Set up User Update Rules - Revoke access past Employment End Date**

Remove access from users whose Employment End Date has already passed.

Task 1- Create User Update Rules to revoke access past Employment End Date

1 - Admin > Policies > User Update Rules

2 - Select Actions > Create User Update Rule

3 - Enter the details as shown > Select Send for Approval

4 - Confirm that the status of Rule is Active.

Task 2- Trigger User Update Rules to revoke access past Employment End Date

Import Users from a file with a past Employment End Date to trigger the rule

1 - Admin > Identity Repository > Users

2 - Select Actions > Upload User

3 - Select the Users\_Lab3.csv file from the folder > Enter the details as shown > Select Upload & Preview

- 4 - Select Import Now
- 5 - Verify the summary page

Task 3- Validate Tasks created by User Update Rules to revoke access past Employment End Date

- 1 - Home > Tasks > Pending Tasks
- 2 - Confirm that the tasks are generated

*Note: These tasks were created because the CSV file uploaded had two users whose End Date has passed.*

#### **Use Case 4: Set up User Update Rules for Employee Termination**

Remove access from terminated Employees. Create a User Update Rule to trigger when a User is Offboarded from Saviynt EIC through One-Click Disable Functionality.

Task 1- Create User Update Rules for Employee Termination

- 1 - Admin > Policies > User Update Rules
- 2 - Actions > Create User Update Rule
- 3 - Enter the details as shown > Select Send for Approval
- 4 - Confirm that the status of Rule is Active

*Note: The column statuskey=0 indicates that user is inactive and statuskey=1 indicates that user is active.*

Successfully created a User Update rule for Employee Termination

Task 2- Trigger User Update Rule for Employee Termination

- 1 - Home > Select One Click Disable tile
- 2 - Search & Select tmarshall > Select Remove
- 3 - Select Yes
- 4 - Confirm the message as shown

Task 3- Validate Tasks created - User Update Rule for Employee Termination

- 1 - Home > Tasks > Pending Tasks
- 2 - Search for tmarshall > Confirm tasks generated

Successfully validated the generated tasks for Access removal.

## **4 - Access Request System - Lab**

*Use case 1: Set Up Auto-Approval Access Request*

*Use Case 2: Set Up Single-level Manager-Approval Access Request*

*Use Case 3: Set Up Two-level Risk-based Access Request*

*Use Case 4: Configure Request forms and Approvals*

*Use case 5: Request Access for Self*

*Use case 6: Request Access for Others*

*Use case 7: Approve Access Requests*

*Use case 8: Access Fulfilment for connected Application*

*Use case 9: Access Fulfilment for disconnected Application*

*Use case 10: Verify provisioned Access*

*Use Case 11: Set up Delegates*

*Use Case 12: Email Templates*

Lab Guide [page 135] – How to:

Create and assign Auto-Approval, Single-level Manager-Approval and Two-level Risk-based Workflows.

Configure Request forms and Approvals

Request Access for Self and Others.

Approve requests.

Fulfill access.

Check user's existing access.

Create email Templates.

Create a delegate.

## Use Case 8: Access Fulfilment for connected Application

How to provision a connected Application

Task 1- View Provisioning tasks

- 1 - Home > Tasks > Pending Tasks
- 2 - Validate provisioning tasks created for Active Directory and Amigopod.

Successfully validated the generated provisioning tasks.

Task 2- Create and Execute Provisioning job

- 1 - Admin > Job Control Panel
- 2 - Select Add New Job
- 3 - Enter the following details
  - Job Name: Provisioning\_Job
  - Job Type: Provisioning Job (WSRETRYJOB)
  - System: Active Directory
- 4 - Select Save
- 5 - Search for the Provisioning\_Job Job > Select the Play icon. *[This will run the provisioning job].*
- 6 - Verify the job Status as Success

Successfully executed provisioning job for Active Directory.

## Use Case 10: Verify Provisioned Access

Task 1- Verify Provisioned Access

- 1 - Select View Existing Access
- 2 - Confirm Joe\_Enduser's existing access > Select Active Directory from Application drop down

Successfully verified the provisioned access.

## Use Case 11: Email Templates

Task 1- View Existing Email Templates

- 1 -Admin > Settings > Email Templates
- 2 - Verify the pre-configured email templates as shown

Task 2- Create Email Template

- 1 - Select Create Email Template
- 2 - Enter the details as shown > Select Create
  - From: Delegate Email
  - Name: Delegate Email Template
  - To: \${delegateuser.email}
  - Subject: Delegation Notification for \${user.firstname}\${user.lastname}
  - Body: Employee ID: \${user.username}, \${user.firstname} \${user.lastname} has assigned you as their delegate. <br>You have been granted delegation permissions on behalf of \${user.firstname} \${user.lastname} from \${delegate.startdate} to:\${delegate.enddate}.

## Use Case 12: Set Up Delegates

Task 1- Configure Delegates

- 1 - Admin > Global Configuration
  - 2 - Select Request from drop down
  - 3 - Enter details as shown in the screenshot
- Note: Different email templates can be set up for different access request notifications from Global Configurations.*

Task 2- Create a Delegate

- 1 - Home > Manage Delegates > Create Delegate
- 2 - Enter details as shown > Search and Select Parent User and Delegate User
  - > Select a Future date for Start Date and End Date > Select Create

*Note: All pending approvals of Tracy\_Manager will be directed to Siu Han Chung (between Start Date & End Date).*

## 5 - Segregation of Duties - Lab

Use case 1: Validate Pre-loaded Rulesets  
Use Case 2: Create and Enable Custom Rulesets  
Use Case 3: Create and Approve Custom Functions  
Use Case 4: Create Custom Risks  
Use Case 5: Validate Ruleset  
Use case 6: Preventative SOD  
Use case 7: Detective SOD  
Use case 8: Remediate SOD Violation  
Use case 9: Mitigating controls  
Use case 10: SOD Reports

Lab page 193, How to:

Create Rulesets, Functions and Risks  
Implement Preventative SOD  
Implement Detective SOD  
Set up and apply mitigating controls  
Download customized SOD reports

### Use Case 1: Validate Pre-loaded Rulesets

The Ruleset objects are used to manage SOD violations

Task 1- Validate Pre-loaded Rulesets

- 1 - SOD > Ruleset > Rulesets
- 2 - Select Oracle\_Training
- 3 - Select Risks
- 4 - Validate the Risks under the ruleset as shown

Successfully validated the pre-loaded Ruleset and Risks

### Use Case 2: Create and Enable Custom Rulesets

Task 1- Create a Custom Ruleset

- 1 - SOD > Ruleset > Rulesets
- 2 - Select Actions > Create Ruleset
- 3 - Enter details as shown > Select Create

Successfully created a custom Ruleset

Task 2- Enable Custom Ruleset

- 1 - Select Yes under Evaluate SODs in Access Request > Select Update

Successfully enabled custom Rulesets to evaluate SODs

### Use Case 3: Create and Approve Custom Function

Functions are logical grouping of entitlements that define the ability of users to perform business tasks.  
Create two conflicting custom functions to generate a Risk.

Task 1- Create Conflicting Functions

- 1 - SOD > Ruleset > Functions
- 2 - Select Actions > Create Functions
- 3 - Select Create New
- 4 - Enter the details as given below. Select Create.
  - Function: AD\_Function\_1
  - Description: Training Function 1 for AD
  - Ruleset: Active Directory\_Ruleset
  - Status: Active
  - Saviynt Function Type: Non-SAP

5 - Select Entitlements > Select  
entval=CN=Finance,OU=Groups,OU=Training,DC=aspire,DC=saviynt,DC=com  
from the list of entitlements > Select Save

*Tip: The entitlement list will get populated as you type inside the text box as shown in the screenshot.*

6 - Enter Business Justification > Select Yes

7 - Sent for Approval confirmation message is displayed.

8 - SOD > Ruleset > Functions

9 - Select Actions > Create Functions

10 - Select Create New

11 - Enter the details as given > Select Create

- Function: AD\_Function\_2
- Ruleset: Active Directory\_Ruleset
- Description: Training Function 2 for AD
- Status: Active
- Saviynt Function Type: Non-SAP

12 - Select Entitlements > Select

entval=CN=Saviynt\_Finance\_Support\_2021,OU=Groups,OU=Training,DC=aspire,DC=saviynt,DC=com  
from the list of entitlements > Select Save

13 - Enter Business Justification > Select Yes

14 - Sent for Approval confirmation message

Successfully created two conflicting functions.

#### Task 2- Approve Conflicting Functions

1 - SOD > View Requests

2 - Select AD Function\_1 > Select Approve

3 - Enter comments > Select Submit

4 - Select AD Function\_2 > Select Approve

5 - Enter comments > Select Submit

6 - Confirm the status of both functions = Approved

Successfully approved the created functions

### Use Case 4: Create Custom Risks

Task 1- Create a Custom Risk

1 - SOD > Ruleset > Risks

2 - Select Actions > Create Risk

3 - Select Create New

4 - Enter the details as given below > Select Create

- Risk Name: AD Finance Risk
- Priority: High
- Risk Type: SOD
- Ruleset: Active Directory\_Ruleset
- Function 1: AD\_Function1
- Function 2: AD\_Function 2

Successfully created a custom Risk.

### Use Case 5: Validate Ruleset

Validate the custom Ruleset, Functions and Risks which we created in the previous Use Cases

Task 1- Validate the custom Ruleset

1 - SOD > Ruleset > Rulesets

2 - Select Active Directory\_Ruleset

3 - Select Risks > Details of AD Finance Risk

4 - Verify the functions under the Risk

Successfully validated the custom Ruleset.

## Use Case 6: Preventative SOD

Proactive process that ensures that the risks defined within a ruleset are not violated or mitigated while requesting access via Saviynt EIC.

Task 1- Configure SOD parameters

Configurations to enable Preventative SOD

- 1 - Admin > SAV Roles
- 2 - Select ROLE\_ADMIN
- 3 - Confirm the settings as shown
- 4 - Go to Admin > Global Configuration

Successfully configured parameters for preventative SOD.

Task 2- Request access for conflicting entitlements

If a user requests access for two conflicting entitlements in Active Directory, EIC should flag a SOD violation

- 1 - Home > Select Request New Access
- 2 - Select Active Directory
- 3 - Select Modify
- 4 - Select Add
- 5 - Search for the entitlements > Add the entitlements as shown > Select Done  
Entitlement 1: CN=Finance,OU=Groups,OU=Training,DC=aspire,DC=saviynt,DC=com  
Entitlement 2: N=Saviynt\_Finance\_Support\_2021,OU=Groups,OU=Training,DC=aspire,DC=saviynt,DC=com
- 6 - Select Review & Submit
- 7 - Verify the Segregation of Duty Violation as shown > Select Click Here to view the details
- 8 - Confirm the SOD details as shown > Select Confirm > Select Submit

Successfully generated and analyzed a preventative SOD violation during access request.

## Use Case 7: Detective SOD

Identify conflicts or violations after they have occurred according to the predefined rulesets.

Task 1- Create and Run SOD Evaluation Job

The SOD evaluation job captures all existing SOD violations in Saviynt EIC

- 1 - Admin > Job Control Panel
- 2 - Select Add New Job
- 3 - Enter the following details:
  - Job Name: Detective\_SOD\_Evaluation
  - Job Type: SOD Evaluation
  - Ruleset: Active Directory\_Ruleset
  - System: Active Directory

- 4 - Select Save
- 5 - Select the Play icon to run the job
- 6 - Verify the job Status as Success

Successfully created and executed an SOD Evaluation job.

Task 2- Analyze SOD Violations Workbench

SOD violations are displayed within the SOD Violations workbench, where each line item is a violation.

- 1 - SOD > SOD Violations
- 2 - Existing SOD violations are displayed
- 3 - Select Advanced
- 4 - Enter Risk Name as AD finance Risk > Select Search
- 5 - Confirm the different violations as shown
- 6 - Select any Violation > Select in Process (Under Move To)
- 7 - Enter a comment > Enter a future Start Date and End Date > Select Next
- 8 - Confirm that the open violation moved to in process state

Successfully analyzed violations in an SOD workbench.

### Use Case 8: Remediate SOD Violation

Remediation of the SOD violations identified through detective SOD analysis using the SOD Violations workbench.

#### Task 1- Remediate an SOD Violation

- 1 - Select Open
- 2 - Select any Violation
- 3 - Select Actions > Remediate
- 4 - Select one of the functions > Select Remediate Now
- 5 - Select Confirm
- 6 - Select Closed > Verify that the remediated SOD is under closed state

*Note: A remediated SOD Violation will move to closed state if Remediate Option is set to Create Task in Global Configurations.*

### Use Case 9: Mitigating Controls

SOD Violations need to be accepted for a limited period by assigning Mitigating control.

#### Task 1- Create a Mitigating control

- 1 - SOD > Mitigating Controls
- 2 - Select Actions > Create Mitigating Control
- 3 - Enter the details as given below > Select Create
  - Mitigating Control Name: AD\_Mitigating Control
  - Provide Description: This Mitigating Control is for Active Directory
  - Ruleset: Active Directory\_Ruleset
  - Expiry Date: Provide a future date
- 4 - Select Pre-Mitigated Associations > Select Actions > Add
- 5 - Enter the details as shown > Select Save

Successfully created a mitigating control.

#### Task 2- Apply Mitigating control

- 1 - SOD > SOD Violations
- 2 - Select any AD Finance Risk Violation
- 3 - Select Actions > Add Mitigating Control
- 4 - Select the mitigating control you created in Task 1 > Enter comment > Enter a future Start Date & End Date > Select Next
- 5 - Confirm the applied mitigating control details
- 6 - Go to SOD Violations > Select Risk Accepted > Verify the mitigated Risk

*Reminder: An Open violation will move to Risk Accepted state when a mitigating control is applied.*

Successfully applied a mitigating control.

### Use Case 10: SOD Reports

Download reports which can be configured and exported directly from SOD Violation Workbench.

Saviynt EIC allows the users to download reports from all pages in SOD module.

#### Task 1- Download customized SOD reports

- 1 - SOD > SOD Violations
  - 2 - Select Actions > Export > L1 Summary Report
  - 3 - Select the attributes needed in SOD report > Select Export
- This will download the SOD report in a CSV format to your local drive.

Successfully downloaded SOD reports.

## 6 - Certification - Lab

- Use case 1: Set Up User Manager Campaign
- Use Case 2: Set Up Entitlement Owner Campaign
- Use Case 3: Download Certification Reports
- Use Case 4: Discontinue a Campaign

Lab page 237; How to:

- Configure & Create User Manager Campaign
- Configure & Create Entitlement Owner Campaign
- Download Certification Reports
- Discontinue a Campaign

### Use Case 1: Set Up User Manager Campaign

Managers verify the employment status of reports to approve/reject access to different entitlements/accounts.

User Manager Campaigns help in achieving this.

Task 1- Create a User Manager Campaign

- 1 - Certifications module
- 2 - Select Create Campaign
- 3 - Enter details as shown
- 4 - Expand Configuration > Employment Verification [Enter the details as shown]
- 5 - Expand Select Certifier > Select Certifier from List > Search & Select a Certifier from the list  
Example: Tracy\_Manager > Select Create Now
- 6 - Select Still Launch
- 7 - Certifications > Campaign List
- 8 - Confirm that the status of campaign is In Progress

Successfully created a User Manager Campaign.

Task 2- Perform User Manager Certification

- 1 – Login as Manager
- 2 - Select Pending Certifications
- 3 - Select Start Certification
- 4 - Select Works For Me > Select Next
- 5 - Approve all access as shown > Select Finish Access Review
- 6 - Select Yes to lock the Certification
- 7 - Confirm that the certification is locked

*Caution: A certification is locked to prevent further changes. Make sure that all appropriate actions are taken before you lock the certification.*

Successfully executed a User Manager Certification.

### Use Case 2: Set Up Entitlement Owner Campaign

Entitlement owners need to review the entitlements, child entitlements, and accounts associated with those entitlements. [Entitlement Owner Campaign help]

Task 1- Add Entitlement Owner to Entitlements

- 1 - Admin > Identity Repository > Entitlements
- 2 - Search & Select WU Admin entitlement
- 3 - Select Owner tab > Select Actions > Add Owner
- 4 - Search & Select an Owner > Example U045101(Siu Han Chung) > Select Save
- 5 - Verify the message > Select Close
- 6 - Change the Rank to Primary Certifier
- 7 - Repeat Steps 1–6 for WU Admin Log (Support only) entitlement > Confirm that the owner is added

Successfully added Owners to WU Admin and WU Admin Log (Support only) entitlements.

#### Task 2- Configure Entitlement Owner Campaign

- 1 - Admin > Global Configuration
- 2 - Select Campaign Config Entitlement Owner from drop-down > Expand Policy Settings > Enter details
- 3 - Expand Entitlement Ownership Verification > Enter details as shown
- Note: Configure Campaign from Global Configuration [Default settings]; Modify further during Campaign launch.*
- 4 - Expand Access Approval > Enter details as shown
- 5 - Expand Revoke Access > Enter details as shown

Successfully configured Entitlement Owner Campaign.

#### Task 3- Create an Entitlement Owner Campaign

- 1 - Go to Certifications
- 2 - Select Create Campaign
- 3 - Expand Entitlement Ownership Verification > Enter details as shown
- 4 - Expand Select Certifier > Choose Select Certifier from List > Search & Select a Certifier from the list [Example: U045101] > Select Create Now
- 5 - Select Still Launch
- 6 - Certifications > Campaign List
- 7 - Confirm that the status of campaign is In Progress.

#### Task 4- Perform Entitlement Owner Certification

- 1 - Login as U045101 (Certifier)
- 2 - Home > Pending Certifications
- 3 - Select Start Certification
- 4 - Select Belongs to Me for all the entitlements as shown > Select Next
- 5 - Approve/Reject the access as shown > Select Finish Access Review
- 6 - Select Yes to lock the Certification
- 7 - Certifications > Campaign List

*Note: Comments are mandatory for Rejected Access. This is configured under Global Configuration.*

- 8 - Filter Complete Certifications > Select Entitlement Owner Campaign
- 9 - Confirm that the certification is Fully Executed

Successfully executed an Entitlement Owner Certification.

### Use Case 3: Download Certification Reports

Download various reports related to Certification.

#### Task 1- Download Campaign List

- 1 - Certifications > Campaign List
- 2 - Select Complete from drop-down list > Select Export to download Campaign list

Successfully downloaded Certification Reports.

#### Task 2- Download Individual Campaign Details

- 1 - Certifications > Campaign List
- 2 - Select Export to download individual certification reports.

Successfully downloaded Certification Reports.

### Use Case 4: Discontinue a Campaign

Discontinue Campaigns which are no longer relevant

#### Task 1- Discontinue a Campaign

- 1 - Certifications > Campaign List
- 2 - Select Discontinue
- 3 - Select Yes
- 4 - Confirm the message > Select Close
- 5 - Select Discontinued from drop-down list > Confirm

Successfully discontinued a Campaign.

## 7 - Intelligence - Lab

Use Case 1: Custom Analytics Control

Use Case 2: Analytics using SQL Query

Use Case 3: Runtime Analytics

Lab page 263 - How to:

Create Custom Analytics Control

Create Analytics using SQL Query

Create Runtime Analytics

### Use Case 1: Custom Analytics Control

Users need to generate customized actionable reports using built-in Actions

Task 1- Create a User Manager Campaign

- 1 - Intelligence > Analytics Configuration List
- 2 - Select Create New Analytics
- 3 - Select Custom Analytics Control
- 4 - Enter the details as shown
- 5 - Scroll down > Enter the details as shown > Select Create
- 6 - Select Submit

Task 2- Run Analytics report and revoke accounts of Inactive Users

- 1 - Select Run > Dry Run
- 2 - Verify the number of records > Select Close
- 3 - Select Run > Run Now
- 4 - Verify the number of records > Select Close
- Note: Dry Run will give a preview of the number of records and Run Now will SAVE the records.*
- 5 - Go to Analytics History > Analytics History V2 to view all Analytics history
- 6 - Select Inactive Users with Active accounts
- 7 - Select Revoke for both accounts
- 8 - Enter comment > Select Save
- 9 - Confirm that both accounts are revoked

Successfully run a Custom Analytics and revoked the accounts of Inactive Users.

### Use Case 2: Analytics using SQL Query

Users need to generate actionable reports using SQL Queries.

Task 1- Create Analytics report of Orphan Accounts

- 1 - Intelligence > Analytics Configuration List
  - 2 - Select Create New Analytics
  - 3 - Select Using SQL Query
  - 4 - Enter the details as shown > Enter the string provided below on the Analytics Query field  
> Select Create
- ```
select a.accountkey as acctKey,a.name, e.endpointname from accounts a, endpoints e where  
a.endpointkey=e.ENDPOINTKEY and a.ACCOUNTKEY not in (select distinct accountkey from user_accounts) and  
endpointname='Siebel MRM';
```
- 5 - Select Submit

Successfully created Analytics using SQL Query.

Task 2- Run Analytics report and Deprovision Orphan accounts

- 1 - Select Run > Dry Run
- 2 - Verify the number of records > Select Close
- 3 - Select Run > Run Now
- 4 - Verify the number of records > Select Close
- Note: Dry Run will give a preview of the number of records and Run Now will SAVE the records.*
- 5 - Select Run History

- 6 - Select Open Conflict
- 7 - Select Map Orphan Account for account tsmith
- 8 - Search & Select tsmith(U114674) > Select Submit
- 9 - Enter comment > Select Save
- 10 - Select Delete Account for account tnotte
- 11 - Enter comment > Select Save
- 12 - Confirm the details as shown

*Note: Go to Home > Tasks > Pending Tasks to view the Delete Account task generated for tnotte.*

*Go to Admin > Users > Search & Select tsmith(U114674) Verify the mapped account under Accounts tab.*

Successfully run Analytics using SQL Query.

### **Use Case 3: Runtime Analytics**

Generate report during real-time application processing [Number of Inactive & Active Users]

Task 1- Create Analytics report of Inactive and Active Users

- 1 - Intelligence > Analytics Configuration List
  - 2 - Select Create New Analytics
  - 3 - Select Runtime Analytics
  - 4 - Enter the details as shown > Enter the string provided below on the Analytics Query field  
> Select Create
- ```
SELECT case statuskey when '0' then 'Inactive' when '1' then 'Active' end as 'label', count(*) as 'data' FROM users
group by label
```
- 5 - Select Submit

Successfully created Runtime Analytics.

Task 2- Run Analytics report and Deprovision Orphan accounts

- 1 - Select Run > Run Now
- 2 - Verify the details as shown
- 3 - Select Action > CSV to download report in CSV format
- 4 - Go to Analytics History > Analytics History V2 to view all Analytics history
- 5 - Verify the Analytics History as shown

Successfully created and downloaded Runtime Analytics.