Saviynt – Active Directory Integration & Design Document

February 2023

Table of Contents

[Document Control 3](#_Toc126764759)

[Introduction 4](#_Toc126764760)

[Supported Features 5](#_Toc126764761)

[Supported Version 5](#_Toc126764762)

[Saviynt – AD Integration Design 6](#_Toc126764763)

[Reconciliation 6](#_Toc126764764)

[Process for Account Reconciliation in Saviynt 7](#_Toc126764765)

[Create Account 8](#_Toc126764766)

[Create Group 9](#_Toc126764767)

[Group Membership 10](#_Toc126764768)

[Process for Request Access - Add Access in Saviynt 10](#_Toc126764769)

[Process for Request Access – Remove Access in Saviynt 12](#_Toc126764770)

Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version control** | | | |
| **Version** | **Name** | **Role** | **Date** |
| v1 | Gaurav Khandelwal | Author | 02/08/2023 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision history** | | | | |
| **Version** | **Changed Sections** | **Details of Change** | **Date** | **Changed By** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Introduction

**Saviynt Active Directory (AD) connector** provides ability to create an integration with Active Directory and perform operations on user and group objects located in single domain. The connector simplifies the overall deployment and integration of single domain level Active Directory with the Saviynt Security Manager (SSM).

Active Directory (AD) connector leverages the LDAP protocol to query and manipulate Active Directory objects and automate common tasks. These tasks include adding users and groups, managing service accounts, and setting permissions on users, accounts, and groups within single domain level only. Saviynt highly recommends using the Active Directory connector If we are integrating Saviynt Security Manager with a single domain.

(Note:  Saviynt recommends ADSI Connector for managing users and groups from multiple domains in a single or multiple forest (with trust relationships).

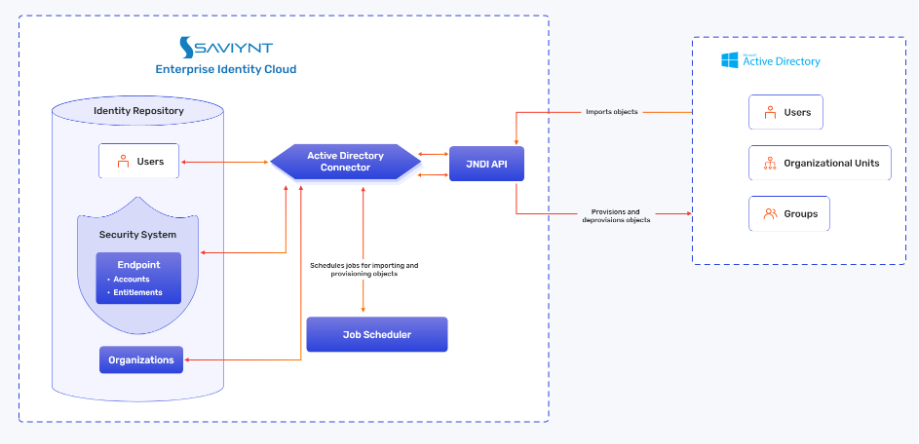


Figure 1: Architecture diagram of AD Connector

1. The AD connector deployed on SSM (Saviynt Security Manager) establishes communication via the JNDI APIs. The JNDI APIs are authenticated through the JNDI protocol.

Supported Features

The Saviynt AD connector supports the following features:

|  |  |  |
| --- | --- | --- |
| **Feature** | **Supported Operation** | **Description** |
| **Reconciliation** | Account Management (import accounts) | Supports full or incremental import of accounts to SSM after the users are available in SSM. SSM uses the User Account Correlation rule to map accounts with users. |
| Access Management (import access) | Supports full or incremental import of entitlements to SSM along with the accounts that have access to those entitlements. This operation also supports a single or nested group import. |
| Group Membership | Add Access | Supports Adding Access (Group Membership) to an account |
| Remove Access | Supports Removing Access (Group Membership) from an account |

Supported Version

Active Directory 2016 and later.

Saviynt – AD Integration Design

|  |  |
| --- | --- |
| ***Security System Name*** | Active Directory |
| ***Endpoint Name*** | Active Directory |
| ***Connection Name*** | Active Directory |

## Reconciliation

**Group reconciliation** will be configured for Saviynt - Active Directory. This process will make Saviynt aware of the existing Active Directory groups



Process for Group Reconciliation in Saviynt

1. Entitlement Recon Job will be executed in Saviynt to import all the groups from AD into SSM. It will import the groups along with its members
2. If group already exists in Saviynt, then this will update the existing group attributes along with its members in SSM.
3. In order to import only the groups which are updated/created after previous group import, Incremental Entitlement Recon Job can be executed

**Jobs to be configured:**

|  |  |
| --- | --- |
| Job Name | Purpose |
| AD\_FULL\_ENTITLEMENT\_RECON | It will bring full set of active directory groups along with its members into Saviynt. |
| AD\_INCREMENTAL\_ENTITLEMENT\_RECON | It will bring groups created or updated after the previous incremental or full entitlement recon along with its members into Saviynt. |

**Account reconciliation** will be configured for Active Directory. This process will make Saviynt aware of the existing Active Directory accounts

## Process for Account Reconciliation in Saviynt

1. Account Reconciliation Job will be executed to import all the accounts from Active Directory to Saviynt. It will import the account into Saviynt if it does not already exist in Saviynt and correlate it to the user’s identity if co-relation rule is matched. Account co-relation rule is defined in the Endpoint settings.
2. If account already exists in Saviynt, then this process should update the existing account fields instead of creating new one.
3. Set the status of account to In-active/Active in Saviynt for all disabled/enabled AD users.
   1. Account status is determined during the reconciliation process based on the value of “useraccountcontrol” AD attribute. Active values ex: 512 are configured using the status\_threshold\_config setting on the connection.
4. In order to import only the accounts which are updated/created after previous account import, Incremental Account Recon Job can be executed.

**Jobs to be configured:**

|  |  |
| --- | --- |
| Job Name | Purpose |
| AD\_FULL\_ACCOUNT\_RECON | It will bring full set of active directory user accounts along with their group membership into Saviynt. |
| AD\_INCREMENTAL\_ACCOUNT\_RECON | It will bring accounts created or updated after the previous incremental or full account recon into Saviynt. |

## Create Account

**Create Account** is enabled for Active Directory application in Saviynt. This process allows to create a new account for new/returning users in Active Directory



* + 1. Launch the ARS. User can request to create an account for others or for self.
    2. Select AD endpoint and modify which will redirect to account modification page.
    3. Create the request to add a new user account in Active Directory.
    4. Once request approved, it will create pending tasks. If no approval workflow is defined, requests are auto approved.
    5. If instant provisioning is enabled at the Security system settings, tasks will be auto processed.
    6. To manually process the tasks, execute the WSRETRY Provisioning job to complete the pending tasks.

## Create Group

**Create Group** is enabled for Active Directory application in Saviynt. This process allows to create a new group in which they can add users new/existing users in Active Directory



1. Launch the ARS. User can request to create a group for others or for self.
2. Select AD endpoint and modify which will redirect to account modification page.
3. Create the request to add a new Group in Active Directory.
4. Once request approved, it will create pending tasks. If no approval workflow is defined, requests are auto approved.
5. If instant provisioning is enabled at the Security system settings, tasks will be auto processed.
6. To manually process the tasks, execute the WSRETRY Provisioning job to complete the pending tasks.

## Group Membership

**Adding Group Membership (Add Access)** to an account is enabled for Active Directory application in Saviynt. This process allows users to request for access to Active Directory groups for existing/new Active Directory accounts.

## Process for Request Access - Add Access in Saviynt

The user can request access to Active Directory groups through Saviynt request form.

1. User logs in to SSM and selects either the “Request Access” or “Request for others” option. If user selects “Request access for Others”, user must select the end user for whom access is being requested.
2. The Active Directory application name will be displayed on the request form.
3. The user selects the AD endpoint and will be directed to the request form.
4. Select the required entitlements/access.
   1. User can select single/multiple groups to **add** membership for the user accounts in a single request
5. Click Review and Submit after selecting the groups
6. The next screen shows the summary of the request. User can submit the request.

A request ID will be generated.

1. Once the request is approved, tasks will be created for **add access**. If no approval workflow is defined, request will be auto approved.
2. If Instant provisioning is not on for AD security system, provisioning job must be executed once these tasks are created. This job will complete these provisioning tasks and provision appropriate access for user in Active Directory.



**Provisioning Jobs:**

|  |  |
| --- | --- |
| Job Name | Purpose |
| AD\_PROVISIONING (Provisioning Job(WSRETRY)) | To perform provisioning and de-provisioning of identity objects and automatically complete the task, the WSRETRYJOB is executed. Once it successfully completes provisioning or de-provisioning in AD, the respective task is completed in Saviynt. If any error is encountered, appropriate details are added as provisioning comments to the task. |

**Removing Group Membership (Remove Access)** to an account is enabled for Active Directory application in Saviynt. This process allows users to request for removing an account’s membership to group(s)



## Process for Request Access – Remove Access in Saviynt

The user can request removal of group membership through Saviynt request form.

1. User logs into SSM and selects either the “Request Access” or “Request for others”. If user selects “Request access for Others”, user must select the end user for whom access needs to be removed.
2. The Active Directory application name will be displayed on the request form.
3. User will select the existing account 🡪 Modify button and will be redirected to the request form.
4. User can select single/multiple groups to **remove** membership in a single request
5. The next screen shows the summary of the selection and user can submit the request. A request ID will be generated.
6. Once the request is approved, tasks will be created for **remove access**. If no approval workflow is defined, request will be auto approved.
7. If Instant provisioning is not on for AD security system, provisioning job must be executed once these tasks are created. This job will complete these provisioning tasks and provision appropriate access for user in Active Directory.