



SAP IDENTITY MANAGEMENT

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com



<https://www.facebook.com/tutorialspointindia>



<https://twitter.com/tutorialspoint>

About the Tutorial

SAP IdM is an identity management system to perform the user management and business workflows in large and complex enterprise. You can integrate SAP and non-SAP systems to identity management using default packages to import identity data and to provide self-service access management feature to end users.

Audience

This tutorial has been prepared for someone who wants to learn and understand the processes in Identity management. After completing this tutorial, you will find yourself at a moderate level of expertise in SAP IdM.

Prerequisites

Before you start proceeding with this tutorial, we assume that you are well-versed with basic access management concepts. You should have basic knowledge on how an Identity and Access management system works.

Copyright & Disclaimer

© Copyright 2021 by Tutorials Point (I) Pvt. Ltd.

All the content and graphics published in this e-book are the property of Tutorials Point (I) Pvt. Ltd. The user of this e-book is prohibited to reuse, retain, copy, distribute or republish any contents or a part of contents of this e-book in any manner without written consent of the publisher.

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com

Table of Contents

About the Tutorial	ii
Audience.....	ii
Prerequisites.....	ii
Copyright & Disclaimer	ii
Table of Contents	iii
1. SAP IDM — Introduction	1
2. SAP IDM — Architecture	3
3. SAP IDM — Installation	5
Installing IdM core components.....	5
Installing SAP IdM runtime and other developer components	8
Installing SAP IdM deployable components	10
Installing Active Directory Server Virtually	12
4. SAP IDM — Developer Studio	14
Configuring SAP IdM Developer Studio	15
5. SAP IDM — Setting up the Framework.....	17
6. SAP IDM — Repository Types.....	19
7. SAP IDM — Using Identity Stores	21
8. SAP IDM — Identity Center Properties.....	24
9. SAP IDM — Maintaining Packages	28
10. SAP IDM — Using Processes.....	30
11. SAP IDM — Identity Store Forms	32
12. SAP IDM — Maintaining Jobs	35
13. SAP IDM — Self Service Password Reset	37
Defining Password Reset Parameters.....	38
14. SAP IDM — Setting Email Notifications	40
15. SAP IDM — Connecting SAP ABAP Systems.....	42

Creating a job for update 42

16. SAP IDM — Connecting non-SAP Systems 44

17. SAP IDM — Identity Reporting using SAP BW 46

18. SAP IDM — Integration using GRC 10.0 47

19. SAP IDM — Migration to New Version 49

20. SAP IdM — Job Responsibilities 50

1. SAP IDM — Introduction

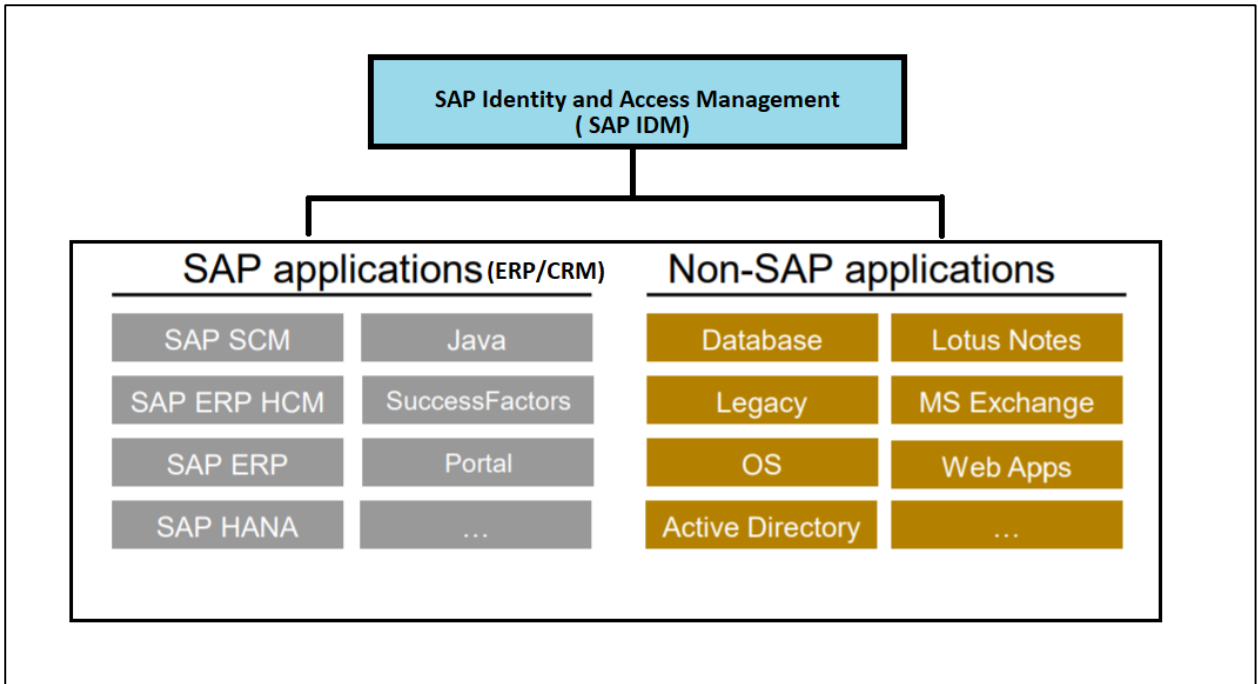
In large enterprises, main challenge is to organize and maintain identity data and privilege securely. Enterprise data is stored in different applications and collected from multiple source so it includes major risk to manage the data confidentiality. To distribute the data security, there is need to manage and maintain identity data and privileges up to date. There are various Identity and access management modules in market which helps Data owner in managing identity information accurately and up to date.

Major ERP software providers provide inbuilt capability to manage identity with other modules. These identity management tools are embedded in ERP/CRM software and no need to install or configure explicitly.

SAP Identity Management is similar tool provided by SAP which help companies managing their user accounts in complex environment for both SAP and non-SAP systems. With use of SAP Identity management tool, companies can manage and provide access to different heterogenous applications without much manual work and that too securely.

There are various reasons why an Identity and Access Management soln is required:

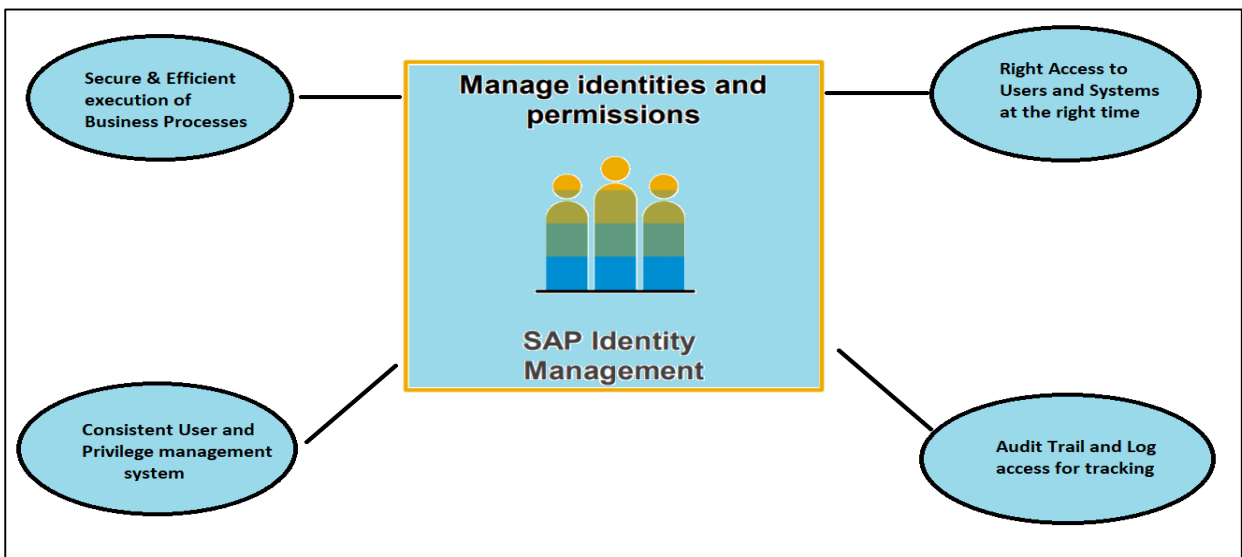
- As business processes running on on-premise and cloud both there is need to manage user access management seamlessly.
- Need to assign application and information access based on user roles and irrespective of technical hierarchies in directory
- To provide self-service user and password management system and to avoid manual password reset for critical applications
- To pull the reports based on current and previous access
- Reduce the operational cost to perform user provisioning in complex landscape
- Ease to manage multiple source of identities
- Availability of audit trails and log system to track identity changes
- To meet company specific requirements for user access management solution
- To prevent the unauthorized access to company resources- Enterprise applications, Database, Webapps, Active Directory, etc. in multi- enterprise environments



Key Benefits

Following are the key benefits of using SAP Identity Management:

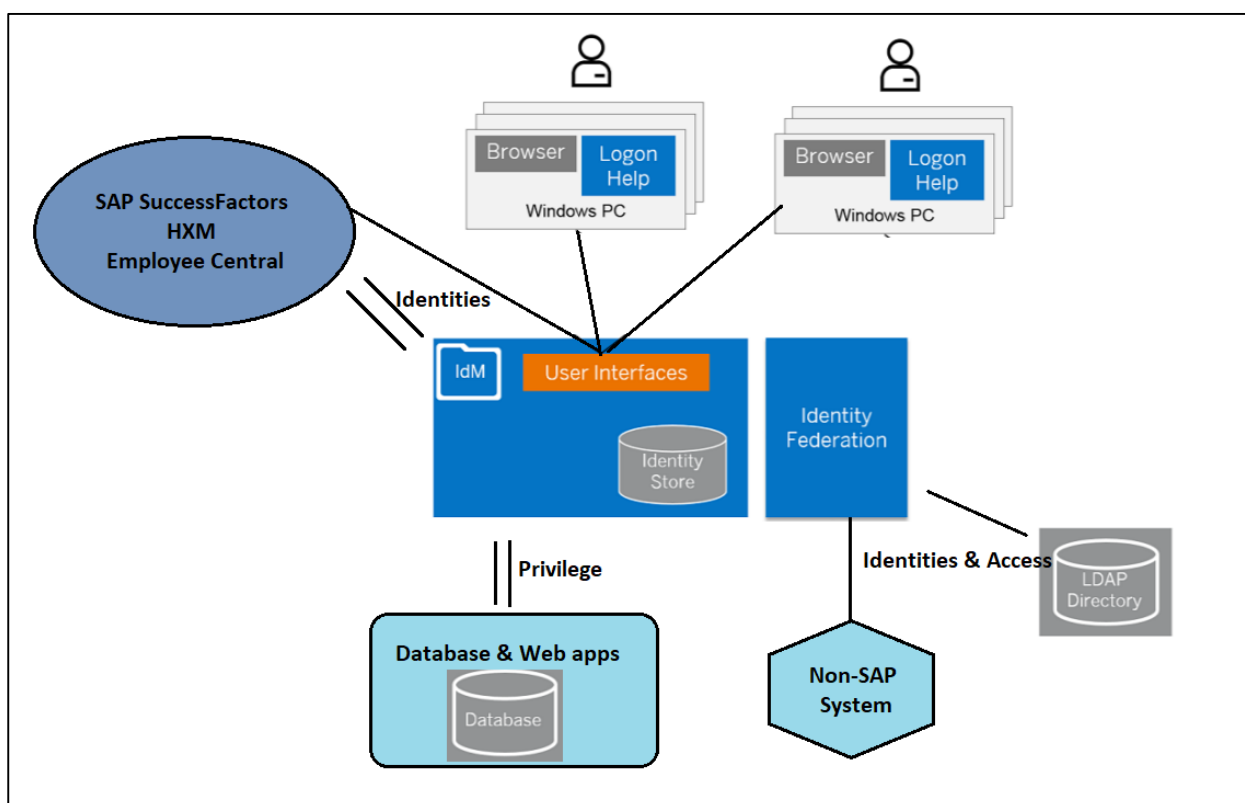
- To ensure that user permissions are assigned to required systems at right time and prevent unauthorize access
- Consistency in managing user roles and permission across multiple complex enterprise landscape
- Secure execution of business approval workflows and processes
- Ease of managing audit trail and log systems for tracking



2. SAP IDM — Architecture

SAP identity management system is used to maintain identity data across different ECC applications. You can import data from different SAP applications to IDM based on available authorizations. From backend application, after importing the authorizations- privileges are added to system and this is then sync to backend applications.

User interfaces are used to perform the different self-management identity tasks in identity store and changes are replicated back to backend applications.



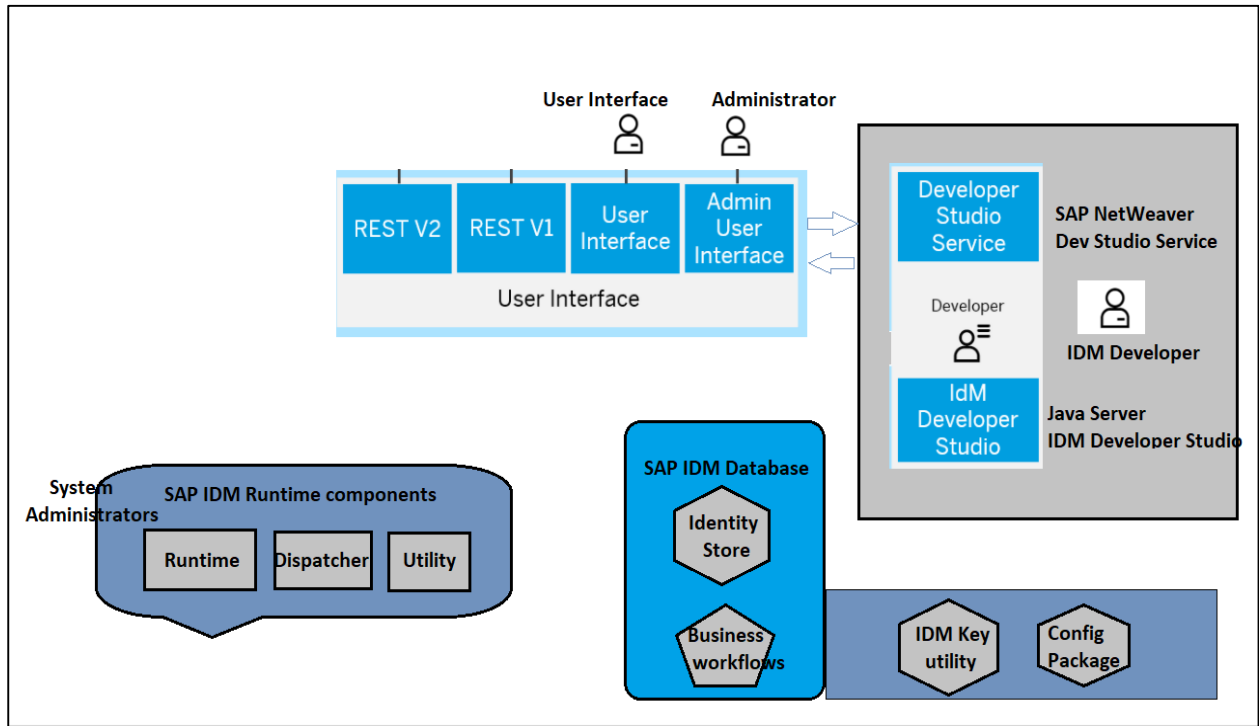
Most of SAP Identity management components run on NetWeaver application and Java server. Few of important component of SAP IdM includes:

- SAP Identity Store
- User interface for users and Administrators
- IdM Database
- IdM Developer Studio
- Developer Studio Service
- Runtime component

Identity store provides a consistent view of identity data from multiple sources and helps in managing business processes, logging and auditing, password management and reporting feature for access management. Identity center collects the data from different

application repositories, transform to required formats and replicate it back to source repositories.

Few components of IDM run on SAP NetWeaver AS for Java and this includes Identity Management User Interface for users and administrators however few of other components are installed separately and stand-alone components. Key components of SAP IDM architecture mentioned below:



Administrators can install SAP Identity Management using Software Provisioning Manager 1.0 installation tool. Provisioning Manager 1.0v installs all SAP Identity Management components except IDM Developer Studio client, Logon Help and SAP IDM Password management utility. Mentioned components to be installed manually using external client tools.

SAP IDM Dispatcher Utility

This is used to create new dispatchers in IDM system. With use of user interface component- you can also stop or start the dispatchers. This can be done via user interface component or using command line option.

IDM Runtime Engine

This component of IDM is used for synchronization and provision tasks and requires SAP Java Virtual Machine for execution.

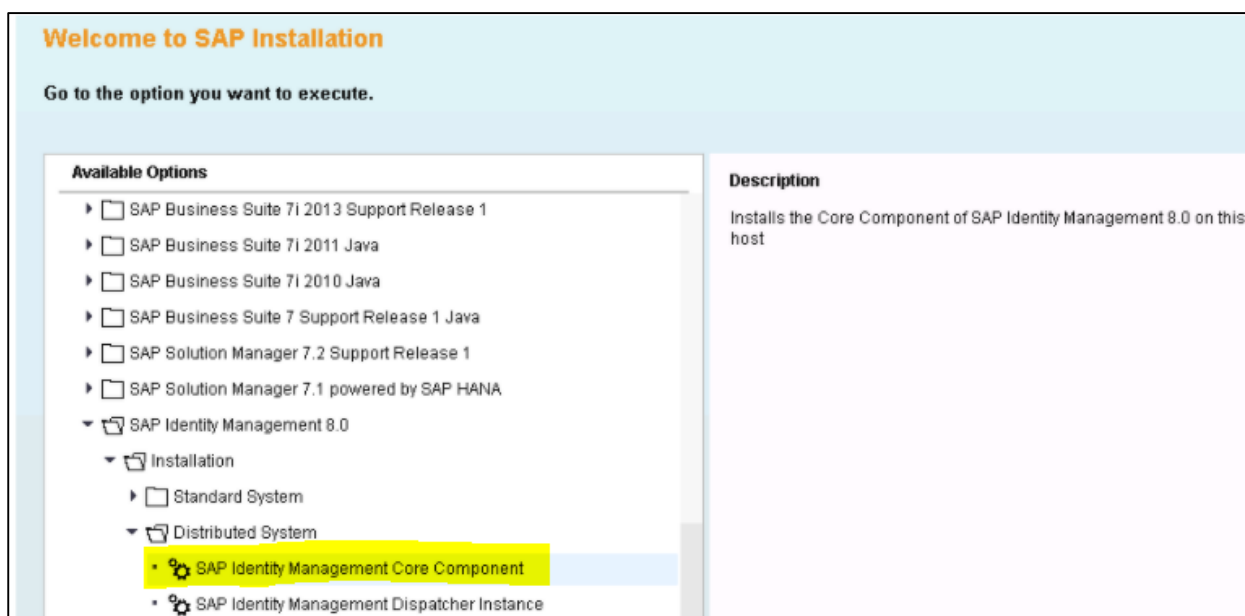
3. SAP IDM — Installation

You can install SAP IdM system in distributed environment where each process runs on separate system. You can use any of OS to perform the installation and select any of database like MS SQL, Oracle, DB2, etc.

You can use Software Provisioning Manager (SWPM) tool for performing the installation of IdM. By following the below steps, you can install SAP IdM:

Installing IdM core components

To install IdM core component, login using an OD administrator account and start Software Provisioning manager tool (sapinst.exe) and select SAP Identity Management 8.0 → Installation → Distributed System → SAP Identity Management Core Component as shown below



Run the installation in Typical mode. You need to pass you SAP SID and destination drive after starting core component installation.

The screenshot shows the 'Define Parameters' step of the SAP Identity Management installation wizard. At the top, a progress bar indicates four steps: 1. Define Parameters (active), 2. Review Parameters, 3. Execute Service, and 4. Service Completed. The main heading is 'General SAP System Parameters'. Below it, the instruction reads: 'Enter the system ID and destination drive.' The form contains the following fields:

- SAP System**
 - *SAP System ID (SAPSID):
 - Destination Drive: (dropdown menu)
- Additional Information**

The SAP System ID is an identifier for your SAP system. It must be unique throughout your system landscape.
The system is installed under <Destination Drive>:\usr\sap\<SAPSID>\...

Follow the installation steps and pass the path of SAP archives, SAP host agent, etc. Next you will be prompted to select the database system:

The screenshot shows the 'Define Parameters' step of the SAP Identity Management installation wizard, specifically the 'SAP Identity Management Database System' screen. The progress bar at the top is the same as in the previous screenshot. The main heading is 'SAP Identity Management Database System'. Below it, the instruction reads: 'Select the database type for your SAP Identity Management installation.' The form contains the following fields:

- Database System**
 - Database Type: (dropdown menu)
- Additional Information**

SAP Identity Management supports the following database types:

 - Microsoft SQL Server
 - Oracle
 - IBM Db2 for Linux, UNIX, and Windows (IBM Db2)

Provide the host name where database is running, port# and credentials for IdM database:

1 **Define Parameters** 2 Review Parameters 3 Execute Service 4 Service Completed

SAP Identity Management Database Credentials

Enter the credentials for the SAP Identity Management database.

Database Credentials

*Administrator User

*Administrator Password

Additional Information

The *Administrator User* is the user name for the system administrator.

The *Administrator Password* is the password for the system administrator.

In next window, you have to provide the Database schema prefix and base qualified name to be used for IdM packages:

1 **Define Parameters** 2 Review Parameters 3 Execute Service 4 Service Completed

SAP Identity Management Database Schema and Base-Qualified Name

Enter the SAP Identity Management database parameters

SAP Identity Management Database Schema and Base Qualified Name

*Database Schema Prefix

*Base-Qualified Name

Additional Information

The *Database Schema Prefix* is the prefix of the Identity Management database.

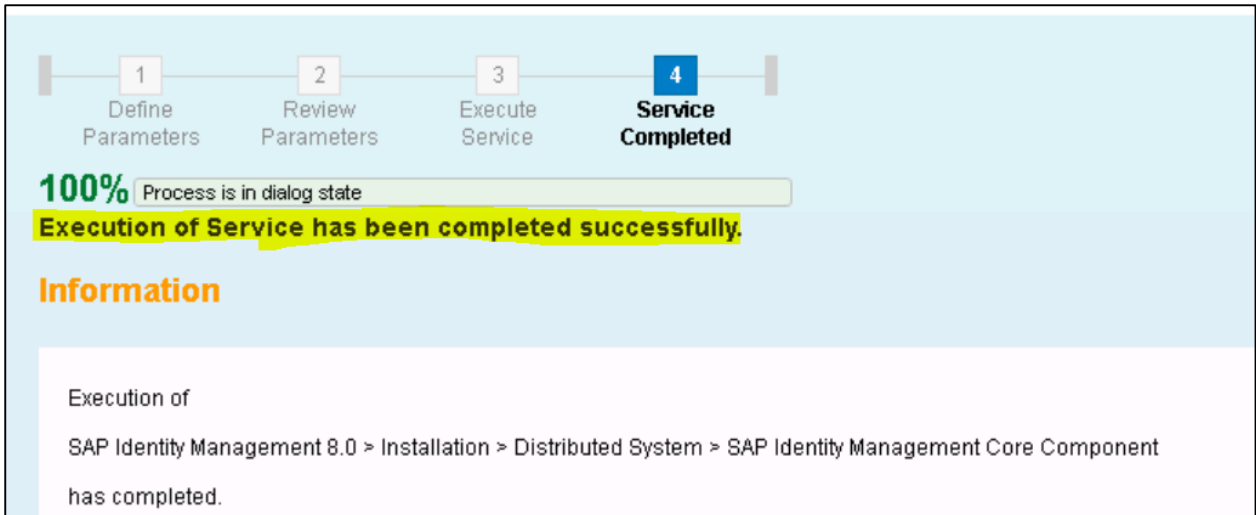
If you want to have several Identity Management databases on the same installation of Microsoft SQL Server, Oracle, SAP ASE or IBM Db2 for Linux, UNIX, and Windows (IBM Db2), each SAP Identity Management database must have its own prefix.

We recommend using uppercase alphanumeric values (A-Z, 0-9) for the prefix, except for IBM Db2 on UNIX operating systems, where the prefix must contain lowercase alphanumeric values only (a-z, 0-9). When using IBM Db2, make sure that the length of the prefix does not exceed two characters. For example: IC (on Windows) or ic (on UNIX operating systems).

The *Base-Qualified Name* is used for all SAP Identity Management packages in this database. The *Base-Qualified Name* can contain only alphanumeric values (A-Z, a-z, 0-9), underscore (_) and period (.). For example: com.acme

Back Next Cancel

Pass the other parameters in subsequent steps and follow the instruction steps and click on Next button to run the installation. When the installation of IdM core component is completed, below message will appear:



1 Define Parameters 2 Review Parameters 3 Execute Service 4 **Service Completed**

100% Process is in dialog state

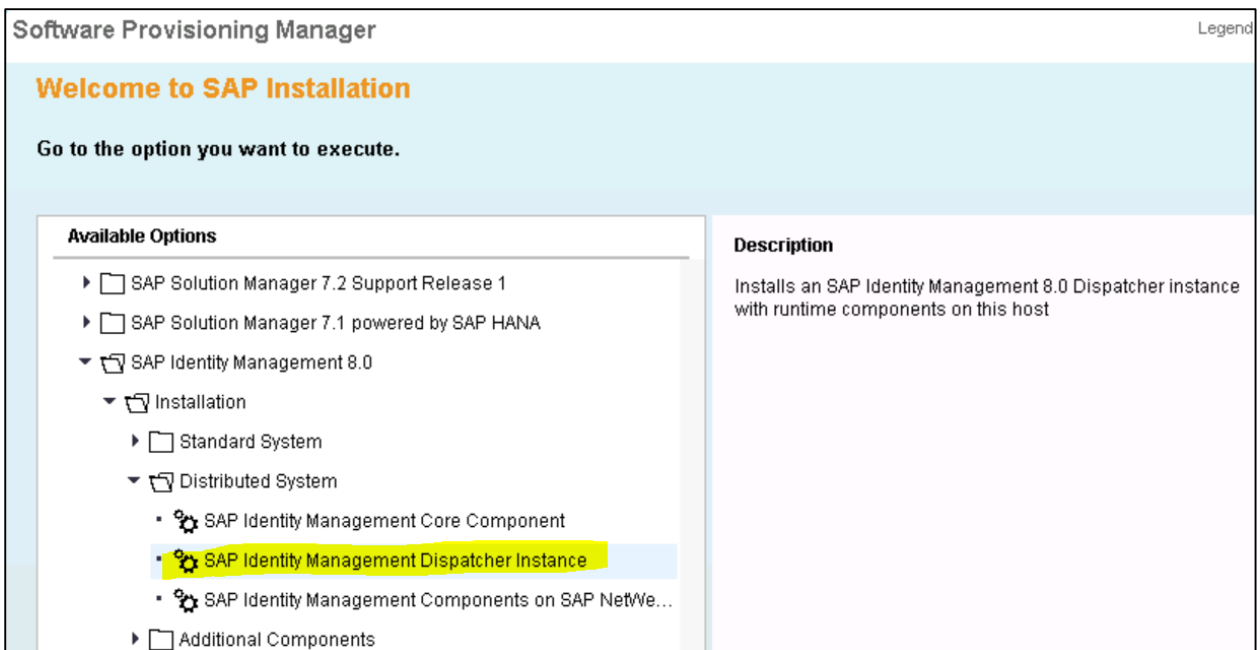
Execution of Service has been completed successfully.

Information

Execution of
SAP Identity Management 8.0 > Installation > Distributed System > SAP Identity Management Core Component
has completed.

Installing SAP IdM runtime and other developer components

Logon to other host where you want to install IdM runtime and other deployable components, and open Software Provisioning Manager and select SAP Identity Management 8.0 → Installation → Distributed System → SAP Identity Management Dispatcher Instance.



Software Provisioning Manager Legend

Welcome to SAP Installation

Go to the option you want to execute.

Available Options	Description
<ul style="list-style-type: none"> ▶ <input type="checkbox"/> SAP Solution Manager 7.2 Support Release 1 ▶ <input type="checkbox"/> SAP Solution Manager 7.1 powered by SAP HANA ▼ <input checked="" type="checkbox"/> SAP Identity Management 8.0 <ul style="list-style-type: none"> ▼ <input checked="" type="checkbox"/> Installation <ul style="list-style-type: none"> ▶ <input type="checkbox"/> Standard System ▼ <input checked="" type="checkbox"/> Distributed System <ul style="list-style-type: none"> ▪ <input checked="" type="checkbox"/> SAP Identity Management Core Component ▪ <input checked="" type="checkbox"/> SAP Identity Management Dispatcher Instance ▪ <input checked="" type="checkbox"/> SAP Identity Management Components on SAP NetWe... ▶ <input type="checkbox"/> Additional Components 	<p>Description</p> <p>Installs an SAP Identity Management 8.0 Dispatcher instance with runtime components on this host</p>

Start the installation process in a Typical mode and provide the profile ddir patch of SAP IdM system as shown below:

1 Define Parameters 2 Review Parameters 3 Execute Service 4 Service Completed

General SAP System Parameters

Enter the profile directory of the SAP system.

SAP System Identification

Profile Directory: [Redacted Path]

Destination Drive: D: [Dropdown Arrow]

Additional Information

Existing parameters are retrieved from the SAP system profile directory. The location of your SAP system profile directory is as follows:

Follow the steps as per installation steps and pass the instance number assigned to SAP IdM dispatcher or you can also use the default value.

1 Define Parameters 2 Review Parameters 3 Execute Service 4 Service Completed

Identity Management Instance

Enter the identity management instance parameters.

Identity Management Instance

The following SAP system instances already exist on this host:

	SAP System ID (SAPSID)	Instance Name	Instance Number
1	IDM	J00	00
2	IDM	SCS01	01
3	DAA	SMDA97	97

*Instance Number: 02

Additional Information

The *Instance Number* for the identity management instance is a technical identifier for controlling internal processes, such as assigned memory. This number must be unique for this installation host.

In the next step, provide the driver path and JDBC driver class name. Review the parameters and proceed with completing the installation steps.

Installing SAP IdM deployable components

Open Software Provisioning Manager. Select SAP Identity Management 8.0 → Installation → Distributed System → SAP Identity Management Components on SAP NetWeaver AS Java.

This will install the below components:

Mandatory Components

- SAP IdM Developer Studio Service
- SAP IdM User interface

Additional Components

- SAP IdM REST interface
- SAP IdM Portal Content
- Identity Federation

Follow the steps in previous installation and provide SAP SID of the NetWeaver Java system where these components to be used:

1 Define Parameters 2 Review Parameters 3 Execute Service 4 Service Completed

SAP NetWeaver System Parameters

Enter the SAP system ID of the SAP NetWeaver Java system to be used for the SAP Identity Management system.

SAP NetWeaver System

SAP System ID (SAPSID)

Additional Information
This is the *SAP System ID (SAPSID)* of the SAP NetWeaver Java system that is to be used for the SAP Identity Management components you want to install or update.

In the next step, you need to select the additional IdM deployable components you want to deploy:

Additional SAP Identity Management Components

Select additional SAP Identity Management components to be installed.

Additional IDM Components

Verify that the prerequisites and dependencies between components deployed on SAP NetWeaver AS Java are met, as described in the Planning section in the SAP Identity Management Installation and Update Guide at <http://help.sap.com/idm>. Otherwise, the deployment on AS Java might fail.

- SAP Identity Management REST Interface Version 2
- SAP Identity Management User Interface for HTML5
- SAP Identity Management Portal Content
- Identity Federation

Additional Information

SAP Identity Management REST Interface Version 2 is a service API that supports the Identity Management User Interface for HTML5 and other custom-made user interfaces. SAP OData library (odata4j) is required for this component.

SAP Identity Management User Interface for HTML5 is a user interface based on HTML5 and JavaScript, developed using the

After selecting the additional components, click on Next button and installation will complete for SAP IdM deployable components.

Additional Information

SAP Identity Management REST Interface Version 2 is a service API that supports the Identity Management User Interface for HTML5 and other custom-made user interfaces. SAP OData library (odata4j) is required for this component.

SAP Identity Management User Interface for HTML5 is a user interface based on HTML5 and JavaScript, developed using the SAP UI Development Toolkit for HTML5 (SAPUI5). It also uses the SAP Identity Management REST Interface Version 2. The SAPUI5 library is required for this component.

SAP Identity Management Portal Content integrates SAP Identity Management with the Universal Worklist (UWL). Configured Universal Worklist (UWL) on the portal is required for this component.

Identity Federation is used for Single Sign-On (SSO) for SAP and non-SAP systems. It supplies a SAML 2.0-compliant identity provider for web-based access, and a security token service for web services SSO.

Back Next Cancel

Installing Active Directory Server Virtually

Open Software Provisioning Manager and select SAP Identity Management 8.0 → Installation → Additional Components → SAP Identity Management Virtual Directory Server. This will install Virtual directory server instance 8.0 on selected host.

Available Options	Description
<ul style="list-style-type: none"> ▶ <input type="checkbox"/> SAP Business Suite 7i 2016 ▶ <input type="checkbox"/> SAP Business Suite 7i 2013 Support Release 2 ▶ <input type="checkbox"/> SAP Business Suite 7i 2013 Support Release 1 ▶ <input type="checkbox"/> SAP Business Suite 7i 2011 Java ▶ <input type="checkbox"/> SAP Business Suite 7i 2010 Java ▶ <input type="checkbox"/> SAP Business Suite 7 Support Release 1 Java ▶ <input type="checkbox"/> SAP Solution Manager 7.2 Support Release 1 ▶ <input type="checkbox"/> SAP Solution Manager 7.1 powered by SAP HANA ▼ <input checked="" type="checkbox"/> SAP Identity Management 8.0 <ul style="list-style-type: none"> ▼ <input checked="" type="checkbox"/> Installation <ul style="list-style-type: none"> ▶ <input type="checkbox"/> Standard System ▶ <input type="checkbox"/> Distributed System ▼ <input checked="" type="checkbox"/> Additional Components <ul style="list-style-type: none"> ▪ <input type="checkbox"/> Additional SAP Identity Management Dispatcher ... ▪ <input checked="" type="checkbox"/> SAP Identity Management Virtual Directory Serve... 	<p>Description</p> <p>Installs a Virtual Directory Server instance of SAP Identity Management 8.0 on this host</p>

Follow the installation steps and provide instance number to assign to Virtual Directory server or you can use default provided.

Identity Management Instance

Enter the identity management instance parameters.

Identity Management Instance

The following SAP system instances already exist on this host:

	SAP System ID (SAPSID)	Instance Name	Instance Number
1	IDM	[REDACTED]	00
2	IDM	[REDACTED]	01
3	IMJ	[REDACTED]	02
4	DAA	[REDACTED]	97

*Instance Number

Additional Information

Next step is to review the parameters and complete the installation process.

Software Provisioning Manager

Leg



100% Process is in finished state

Execution of Service has been completed successfully.

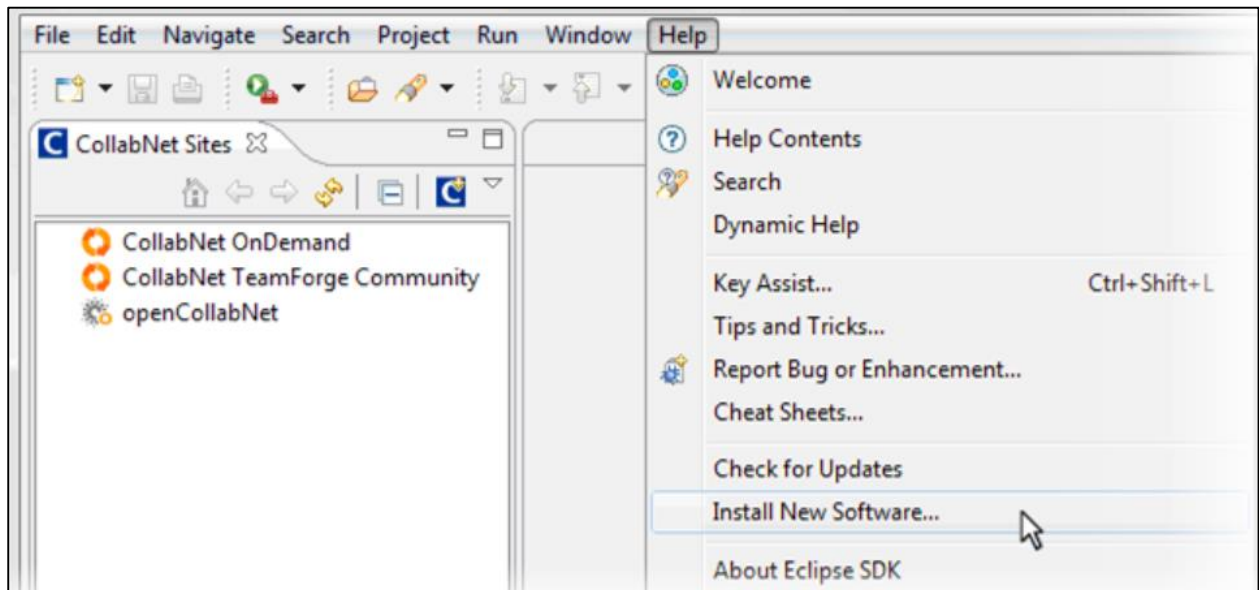


The process execution is finished successfully

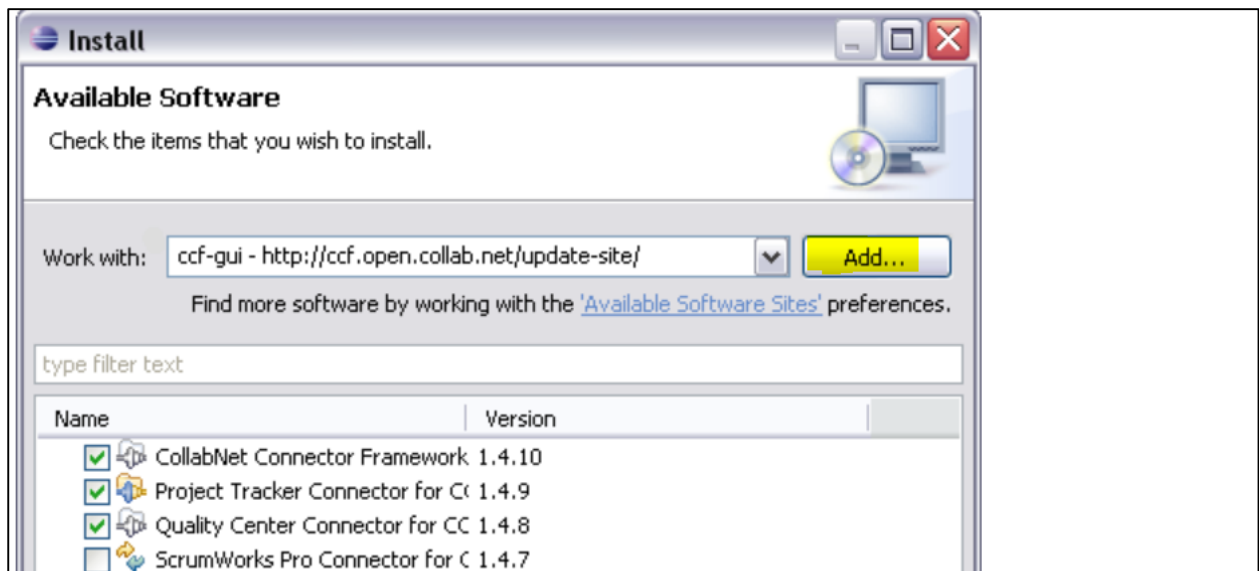
Exit

4. SAP IDM — Developer Studio

SAP IDM Developer Studio is an Eclipse based plug in and used to configure Identity management solution. This is a client-based tool and has to be installed on each developer or administrator system. To enable Identity Management developer studio, From Eclipse User interface, navigate to Help -> Install New software.

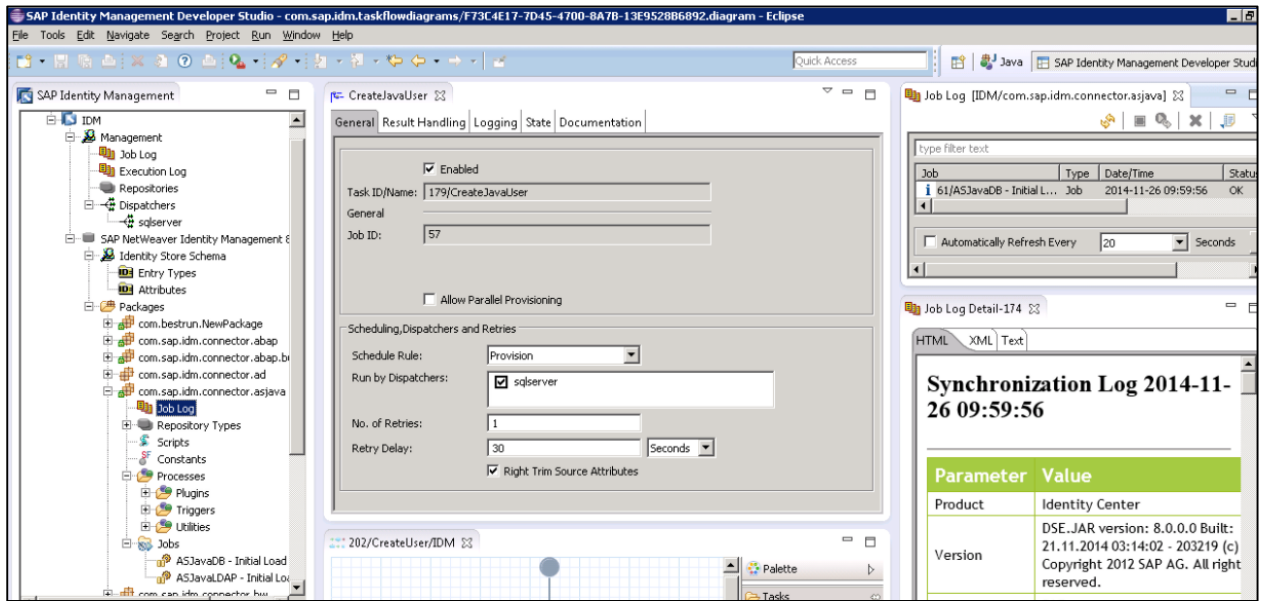


Next is to provide the repository site where the plugin is available from. Click on "Add..." as shown in below screenshot:



This will open Add Repository dialog box, pass the name like- "SAP Identity Management Developer Studio: and under location field, pass URL of Identity Management Developer Studio plugin. Provide this URL <https://tools.hana.ondemand.com/oxygen> for Eclipse Oxygen (4.7) -> OK.

When you expand SAP Identity Management Tools, Select SAP Identity Management Developer Studio checkbox and click on Next.

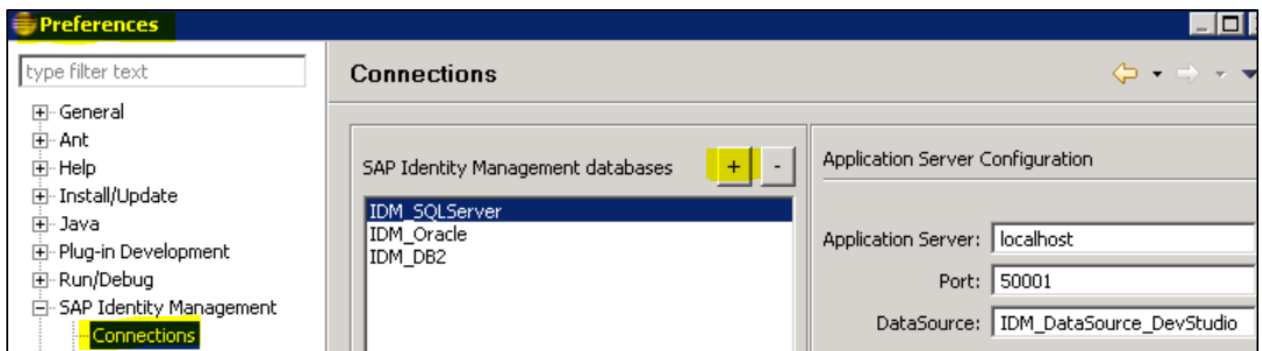


Configuring SAP IdM Developer Studio

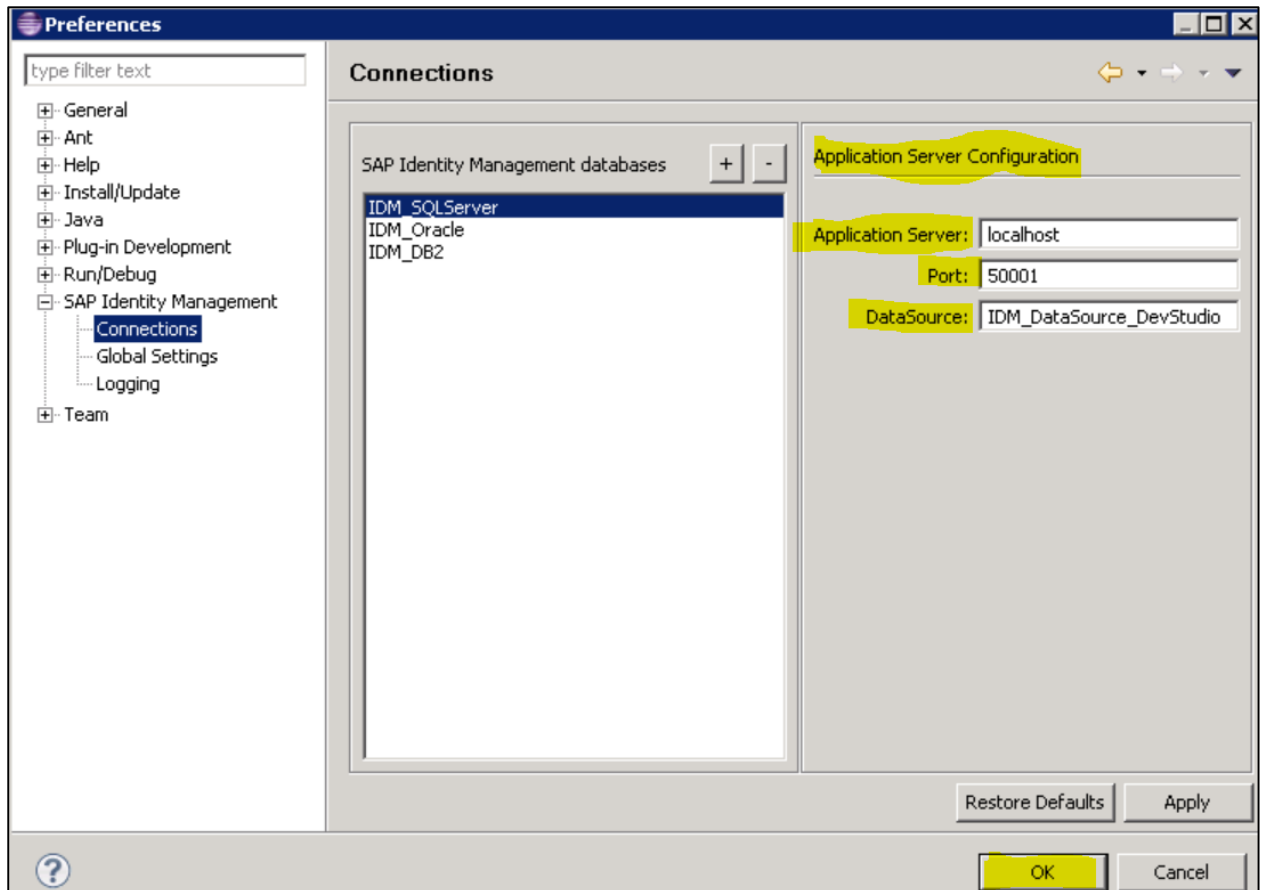
In SAP IDM Developer studio, you can add connection to IDM database. You need to pass the below details:

- Application Server name
- Port
- Data Source

Under Preferences -> Connections -> " click on + sign ".



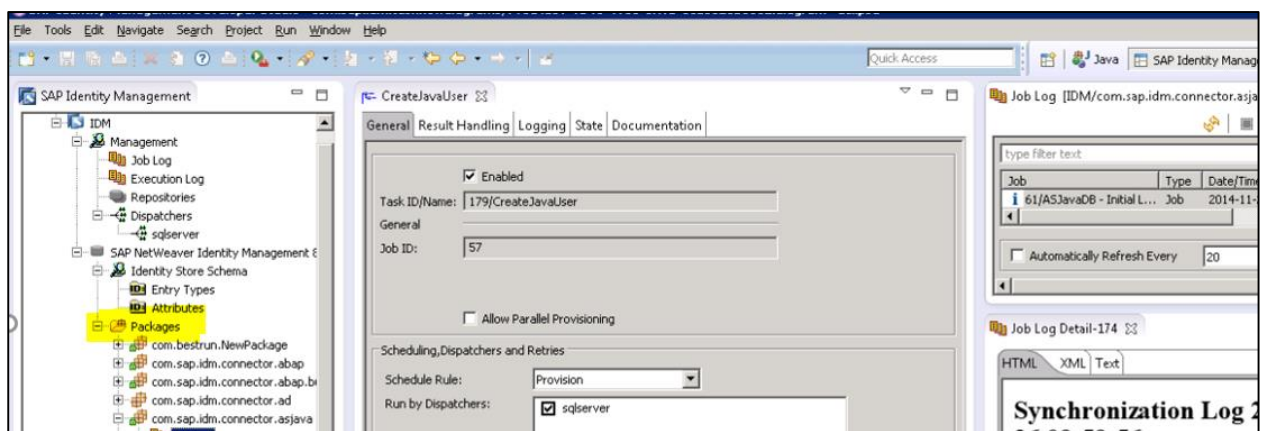
Provide the required information and click on OK to add the Database. Once you add the database, you can expand and see the tree view.



5. SAP IDM — Setting up the Framework

In SAP Identity Management, you can use set of templates to connect to SAP systems and setting up the jobs, processes for different tasks. A Package in SAP IDM is smallest unit of code that can be a connector type or set of utilities used by other packages. Administrators can gran permissions to user to transport each package separately and then work on configuration to customize them. IDM provides configuration packages as default component to provide starting point customization.

Each package is identified with global unique name which means you cannot have same package name in any of identity store.



You can usually find below package types:

Engine package

This package provides the core flows which are responsible for triggering the necessary processes and other common scripts used in other packages.

Connector package

This package provides the connector, which is used for provisioning the specific systems like SAP ABAP, etc.

Forms package

This package stores definition of all user interface tasks for different transaction types

Notification package

This package contains the notification task and templates which are used to send notifications for provisioning, approval tasks and business work flows.

Custom package

This package is used to customize the provisioning framework without altering the other stored packages. This package contains the customize scripts from other customers and few of default custom scripts which can be used to customize other packages.

User Authorization to access packages

To access the content of package, user must have required authorization on that package. Below authorization exists for packages:

- View
- Developer
- Layout Developer
- Import
- Owner

6. SAP IDM – Repository Types

To connect your SAP and non-SAP system to SAP Identity Management, repositories has to be created based on different types. Repository type tells the common constants for all the repository type available and assist in repository configuration process.

Below are the advantages of using Repository type:

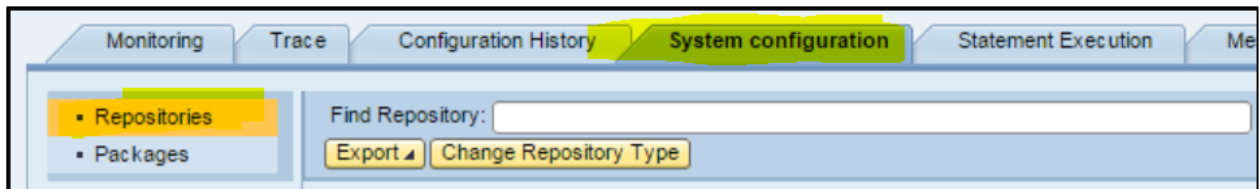
- For all the repository type, you can change repository constant and this will apply to already existing and new repositories.
- You can also add new constant for all the repositories of any types and this includes existing and new repositories.

You usually require changes to the Repository type of given repository in following scenarios:

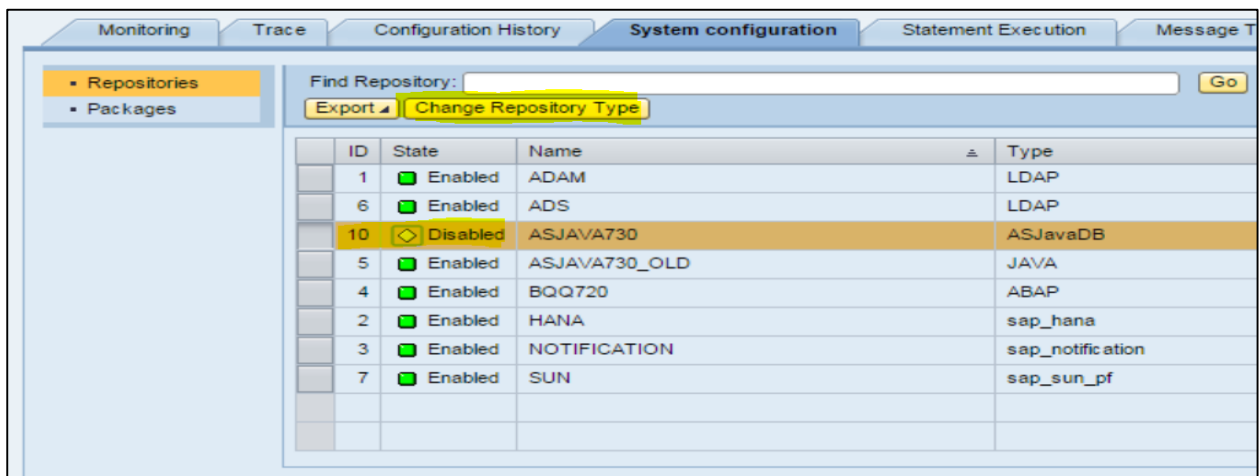
- While upgrade SAP Identity Management from v7.2 to 8.0 and to use provisioning framework in SAP IDM 8.0. This will allow you to configure v7.2 repositories to change type of repositories delivered in new framework.
- There is custom repository type with the custom features and you want to change any existing repository type to custom.

To change the Repository type, you have to log on to SAP Identity Management Administration UI- "http://<host>:<port>/idm/admin".

Next is to choose the System Configuration tab -> click on Repositories from left menu.



You can select a repository which is disabled and click on "Change Repository Type".



Next is to Select the Repository type -> Provide description (optional field) -> OK. Next is to validate the Repository constants and fix the values if required as below.

Details of Repository "IDENTITY_AUTHENTICATION":

Constants Jobs

Edit constants of repository "IDENTITY_AUTHENTICATION"

Save Refresh

Name	Value
PROXY_PORT	
PROXY_USER	
READ_TIMEOUT	60000
SCI_HOST	[REDACTED]

You can also view the Repository changes history by navigating to "Configuration History Repository Operations."

Monitoring Trace **Configuration History** System configuration Statement Execution Me

Repositories Packages

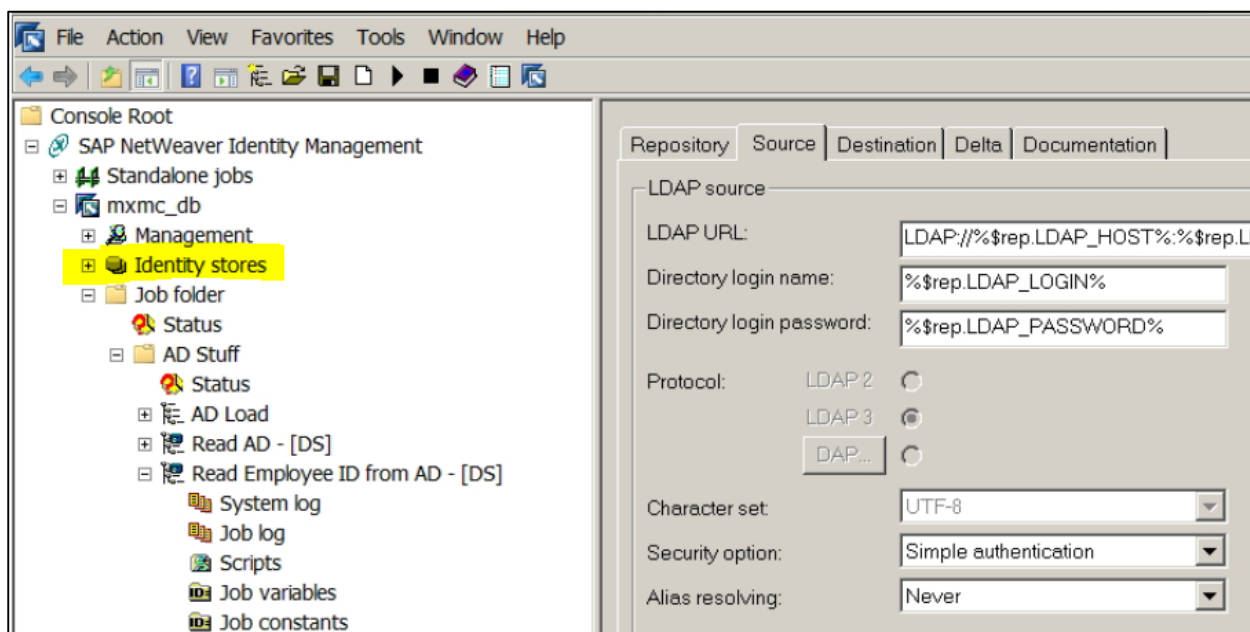
Find Repository:

Export Change Repository Type

You can also view the Repository constants changes due to change in the Repository type, Navigate to Configuration History → Repository Constants

7. SAP IDM — Using Identity Stores

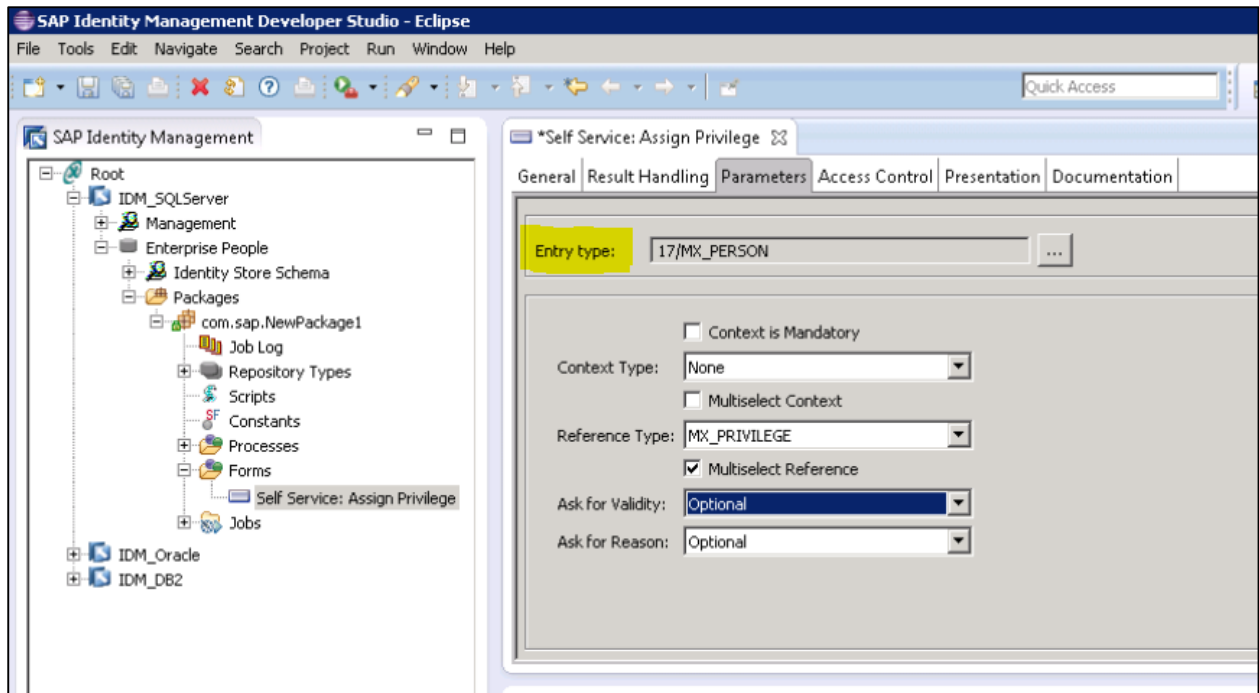
In SAP IDM, information stored in Identity stores are used in provisioning framework and this provides a centralized repository for managing identity related information like Dept, Emp name, Groups, BU, etc. Identity store also provides extensive audit trail and tracking functionality to monitor attributes which can be changed.



Usually an Identity store is connected to identity management user interface in SAP NetWeaver AS for Java and each Java installation can only connect to one identity store. There are number of system attributes added in the system when an identity store is created. There is an identifier- MSKEYVALUE which stores unique identifier in Identity store across all entry types.

In Identity Management, you use entry type to define an entry property such as allowed and mandatory attributes.

Note: MSKEY number is unique across in an identity center across all identity stores.



Managing Entry types in Identity store

Usually it is not recommended to delete entry types in an identity store as they are required for audit trail and tracking purpose. You can mark it as inactive or use a state field to mark the status of that entry type.

Ex: An employee can join back a company later and in that can it simplifies the process if the same entry type can be used for that employee.

The screenshot displays the SAP Identity Management configuration interface. On the left is a tree view with the following structure:

- Management
 - Status
 - System log
 - Job log
 - Global scripts
 - Global variables
 - Global constants
 - Repositories
 - BQ720
 - NOTES
 - NOTIFICATION
 - Scheduling
 - Dispatchers
 - 72inc4
 - External event handlers
 - Identity stores
 - Attribute types
 - Enterprise People
 - Identity store schema
 - Identity store metadata
 - Lost and Found
 - Provisioning Framework
 - CORE
 - Web Enabled Tasks
 - Identity
 - Change Own Data (Self-Service)
 - Request Role Assignment (Self-Service)
 - Display Identity
 - Create Identity
 - Modify Identity
 - Assign
 - Disable Identity
 - Inactivate Identity
 - Inactivate Identity
 - Identity SearchTask
 - Delete Identity
 - Delete Identity
 - Delete Identity
 - System log
 - Job log
 - Scripts
 - Job variables
 - Job constants
 - Delete Identity

On the right, the 'Destination Identity store' configuration panel is shown with the following settings:

- Repository: Source | Destination | Delta | Documentation
- Destination Identity store:
 - Identity store: Enterprise People
 - Entry type: MX_PERSON
 - Multivalue delimiter: |
 - User info: JobId=%\$ddm.mcjob%
 - Insert template

Below the configuration panel is a table with the following content:

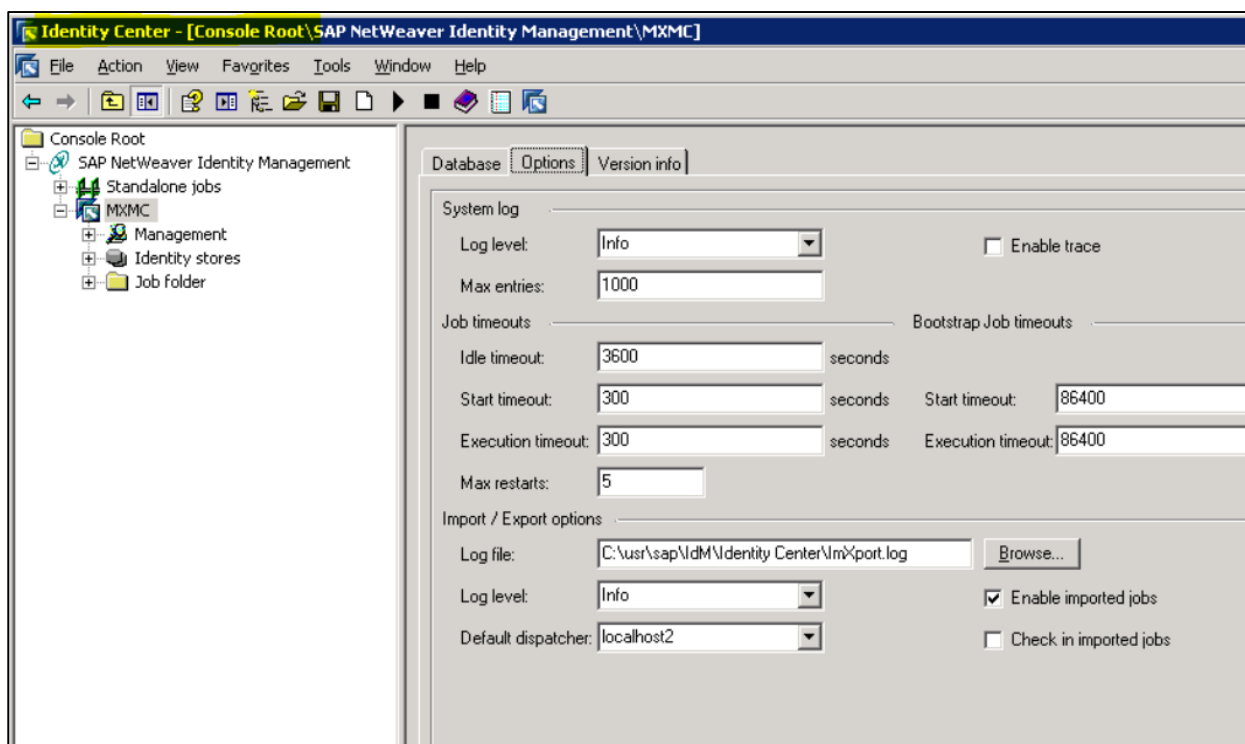
| Attribute | Value |
|------------|--------------|
| MSKEYVALUE | %MSKEYVALUE% |
| ChangeType | delete |

8. SAP IDM — Identity Center Properties

Identity Center is the main component of SAP IDM which provides key functionality for identity management system. Identity center uses identity store to manage all the key functions. SAP Identity center is usually installed with a management console, and other runtime components. For using logon service via Active Directory server for self-service password management, SAP IDM should be configured with Identity center.

Following are the key functions performed using Identity Center:

- Password reset
- Business and workflows
- Logging
- Audit trail
- Reporting
- Provisioning



SAP Identity Center contains the following components:

Management Console

Management console is a plug in in MMC and is used for setting up the starting configuration for different tasks and jobs in provisioning flows.

Database Management

SAP Identity center uses the database to maintain all the information about provisioning tasks and business workflows, logging information and audit trails, and identity store, etc. You can use following DB's in identity Center:

- Oracle Version 10/11
- DB2
- MS SQL Server 2005/2008

Copying Identity Center Configuration

To copy SAP Identity center configuration and data from one database to other, you can use system copy. For this task, you can find job in SAP Community network. Download the Zip file from SCN and extracts the file and below steps to be performed:

- Creating Dispatcher
- Import the job folder
- Configuring the imported repository

To pass dispatcher script, you have to navigate to Options Tab -> Create Dispatcher Scripts

The screenshot shows the 'Options' tab in the SAP Identity Center configuration interface. The 'Dispatcher task execution policy' section is visible, with the following settings:

- Check intv.: 5 Seconds
- Handle tasks
- Evaluate relations
- Evaluate approvals
- Housekeeping actions
- Housekeeping intv.: 30 Seconds
- Run jobs

The screenshot shows the 'Options' tab in the SAP Identity Center configuration interface, displaying the configuration details for a dispatcher. The 'Create dispatcher scripts...' button is highlighted in yellow.

Configuration details:

- Name: idmdispatcher1
- Version: MxDispatcher v7.2.8.0
- Max it engines to start: 1
- Last check: 1/30/2013 3:06:43 PM
- Max concurrent it engines: 0
- Log level: Error
- Max loops for it engine: 10
- Advanced button

After script is created, you need to pass the details for run jobs and runtime engine. To define this, navigate to Policy tab - > select Run Jobs check box.

Options | Policy | Jobs

Dispatcher task execution policy

Check intv.: 5 Seconds

Handle tasks

Evaluate relations

Evaluate approvals

Housekeeping actions

Housekeeping intv.: 30 Seconds

Run jobs

Java runtime engine

Run provisioning jobs

Run regular jobs

Log level: Info

Stack trace: Topmost entry

Java options:

Windows runtime engine

Run provisioning jobs

Run regular jobs

You can check the Dispatcher status under Options tab -> To update the status click on Refresh button. The status is showing under Service state field.

Options | Policy | Jobs

Name: idmdispatcher1 Create dispatcher scripts...

Version: MxDDispatcher v7.2.8.0

Max it engines to start: 1 Last check: 1/30/2013 3:06:43 PM

Max concurrent it engines: 0 Log level: Error

Max loops for it engine: 10 Advanced

Status: Running threads: JOBEXECUTE

Windows Service

Service state: Running Refresh Test

You can also select dispatcher service to auto start. For this, select the checkbox Automatic start field to enable the same.

Options | Policy | Jobs

Name:

Version:

Max rt engines to start: Last check:

Max concurrent rt engines: Log level:

Max loops for rt engine:

Status:

Windows Service

Service state:

Automatic startup

You can also manage Dispatcher job to stop/start manually. For this, you can use Start and Stop option below Service State:

Options | Policy | Jobs

Name:

Version:

Max rt engines to start: Last check:

Max concurrent rt engines: Log level:

Max loops for rt engine:

Status:

Windows Service

Service state:

Automatic startup

9. SAP IDM — Maintaining Packages

As mentioned earlier in this tutorial, Package is smallest unit of configuration which can be a connector or collection of utilities used by other packages in Repository. Few default packages are delivered as a part of Identity management core component and imported to database to provide the starting point for solution.

Package has set of features which are used to maintain them in the Identity management repositories. Following are the key features:

- Package Qualified name
- User Editing
- Authorization
- Version control
- Objects
- Transporting packages

Package Qualified Name

Each package in SAP Identity system has qualified name which contains base name which is provided during installation and package name which is passed during package creation. Base name passed during installation usually contains alphanumeric, numbers, underscore and dot. Ex: XYZ.com. Package name passed during package creation is globally unique i.e., you cannot have same package name in different identity stores in SAP IDM.

User Editing

To make changes to a package, you must check out and once changes are done, you should check in to make updated configuration available to other packages. When a package is checked out, no other user can make the configuration modification to that package.

Authorization

To access the package content, user should have permissions on that package. Users can have different level of authorization on packages in identity store. Below are common authorization exists on the package:

- Owner
- View
- Developer
- Import
- Layout Developer

Version Control

Using version control of package, you can restore the previous version of the package. Package usually has two version numbers, Major version and Minor version.

Major Version: Whenever you make changes to a package and make it public, major version is incremented.

Minor Version: When you check in a package every time, minor version is incremented.

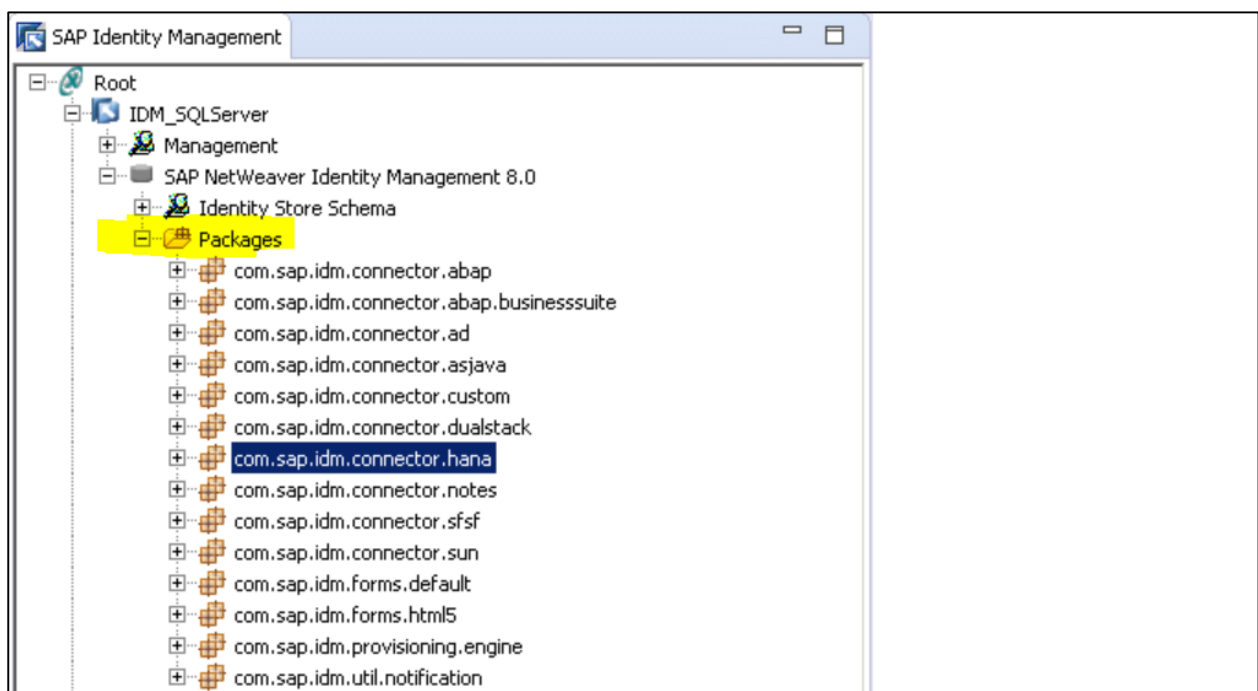
Objects

You can define the objects used in package as public or private. A public object can be called by other packages.

Transporting Packages

Each package in an identity store is transported separately.

Note: To perform provisioning framework in SAP IDM Developer Studio, you must import an engine package, a custom package and connector package.



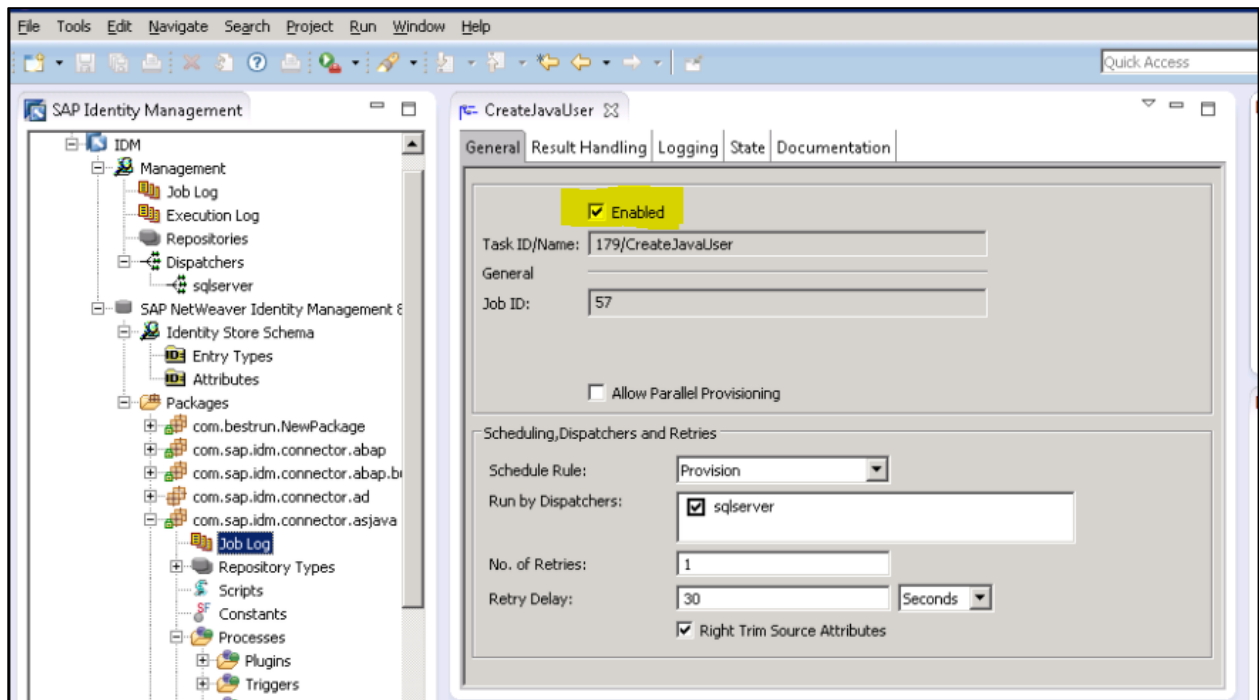
10. SAP IDM — Using Processes

In SAP Identity management, you can create new processes and use developer studio to drag processes in workflow. You can disable/enable packages by navigating to Package properties.

Navigate to General tab of process properties to enable/disable the Process. Under General tab, you have the following options:

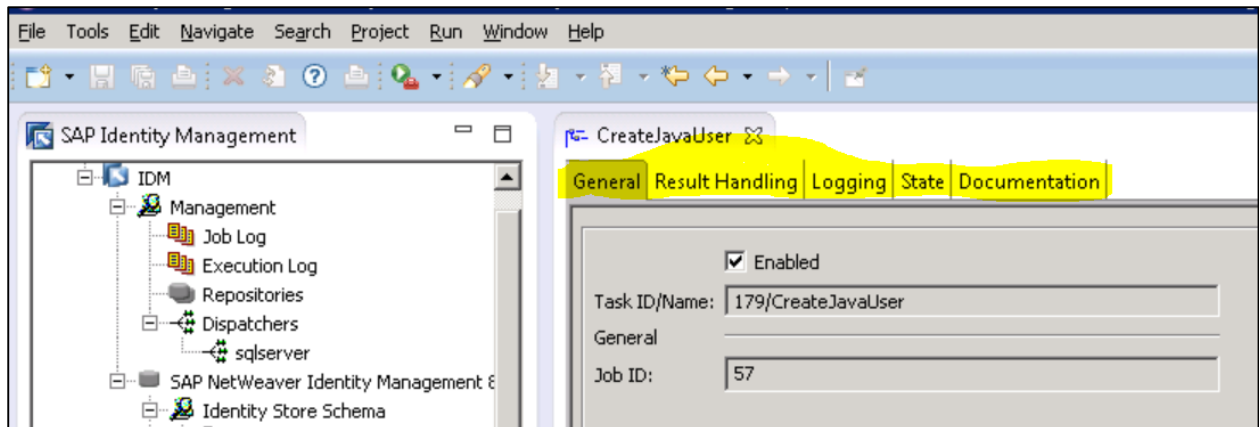
- Field
- Description
- Enabled
- Process ID/Name

Process ID shows the number that is used to identify the process in IdM database.



Using Process Properties

A process in an Identity store defines the set of operations that are executed in a particular sequence. You see the below options for Process property:



General

Using General tab, you can enable/disable the process or define the process type. You can also define a repository for the process.

Result Handling

This tab can be used to perform result handling for the processes.

Documentation

In this field, you can provide the documentation of a process.

11. SAP IDM — Identity Store Forms

Identity store forms are used to maintain entries in identity store such as privilege, user, roles, etc. A set of forms are default delivered as package in provisioning framework. An identity form usually contains below fields:

- Attribute definitions
- Access control
- UI configuration details

Usually forms are defined as public objects inside a package however you can remove them from public and read them. There are other guided activities apart from default form as given below:

View Assignment Request Forms

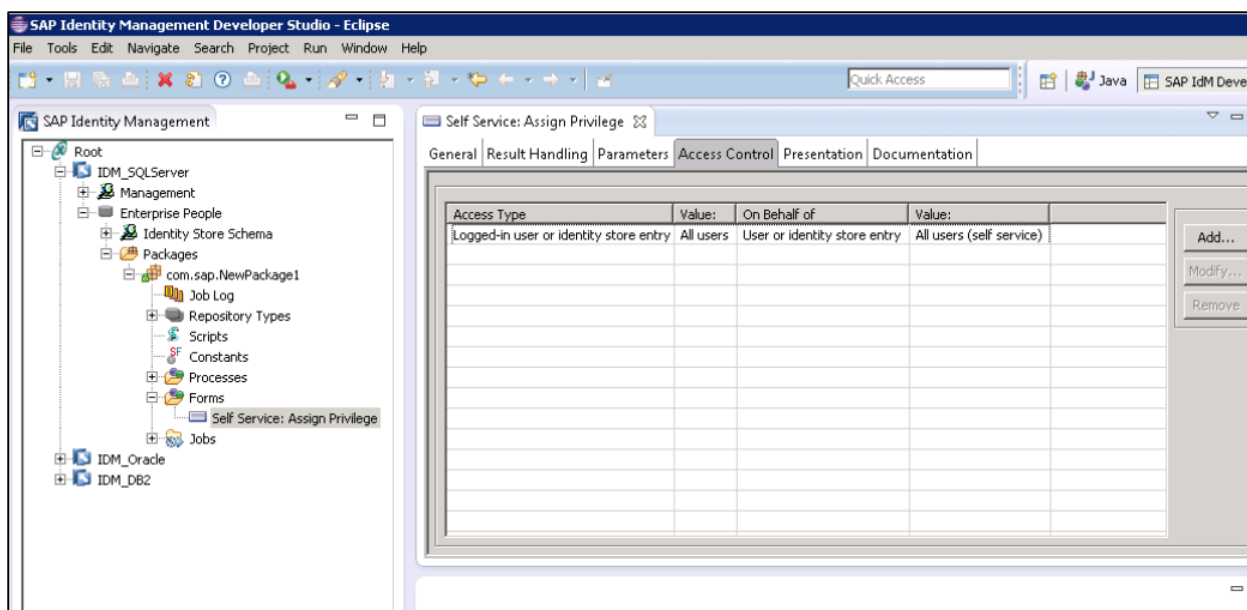
These forms can be used to check the status of assignment requests and can be used to authorize user to restart any failed activity.

Assignment Request Form

This is used to provide one or more assignment to a user and usually use for providing context-based roles.

Password Reset

This is used to provide user with guided activity to reset the passwords.



To create a form, navigate to Forms folder in the package using Identity Management developer studio → New.

Next is to take action as per below form options:

If you want to create a Form folder, Select Folder option.

Or to create a form → Select Form.

Or to create a guided task form → Select Assignment Request/ View Assignment Request/Password Reset form.

You can also configure the form properties, following tabs are available and after making changes, navigate to File -> Save.

- General
- Result Handling
- Attributes
- Access Control
- Presentation
- Documentation

General

This tab is used to perform general properties for a form. Below are the options under General tab:

| Field | Description |
|---------|------------------------|
| Enabled | To enable/disable form |

FormID/Name

This shows a number that identifies the form within the Identity Management database.

Form Type

This is used to define the form type. The following values are available:

- Regular
- Access Control Form
- Display Form
- Search Form

Repository

This option can be used to link the repository to the form. While running the form, selected repository is used.

Result Handling

This is used to configure the result handling part of the form.

Attributes

This is used to define the form attributes.

Parameters

Parameter is used to configure the guided activity- assignment request/view assignment request/ password reset.

Access Control

Using this tab, you can define the access part for the form.

Presentation

This is used to configure form presentation.

Documentation

You can provide form description in this tab.

12. SAP IDM — Maintaining Jobs

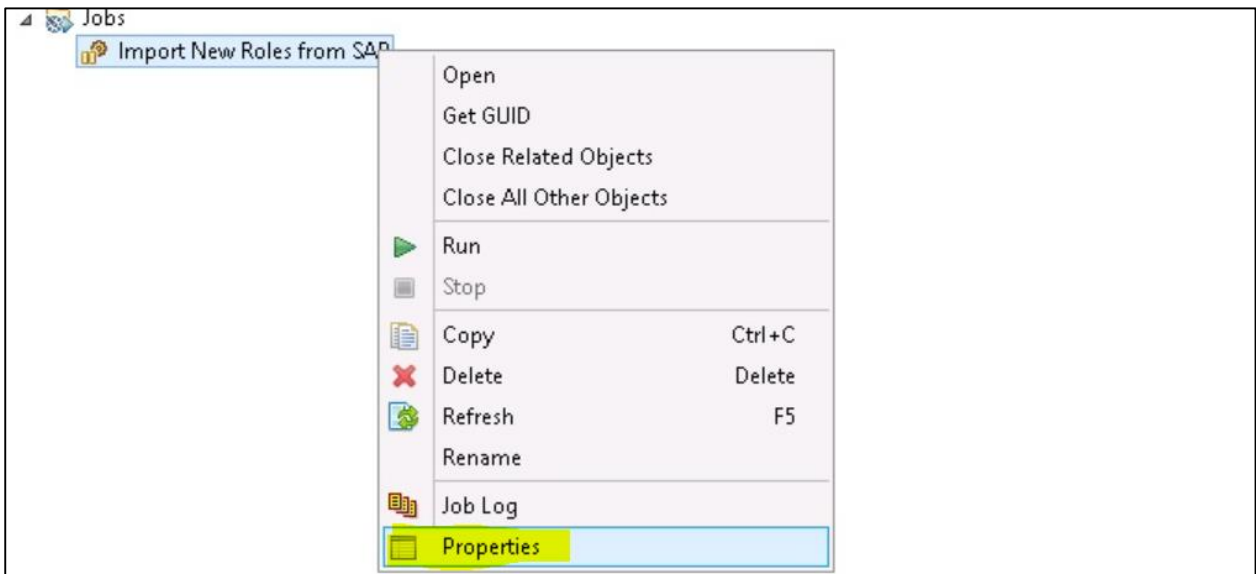
In SAP IDM, jobs are stored inside Job folder under package and are executed inside an identity store. Following actions can be performed:

- Creating a new job
- Enable/Disable an existing job
- Executing a job

To create a new Job, select Job Folder of the package and select New → Job. You can pass the Job name, connect to a dispatcher and define the Job properties.



You can also define the Job properties. To define the Job properties -> Select the job in the tree view and click on Properties option from context menu.



Below options are available:

- General
- Logging
- State
- Documentation



To save the changes to a Job, go to File → Save.

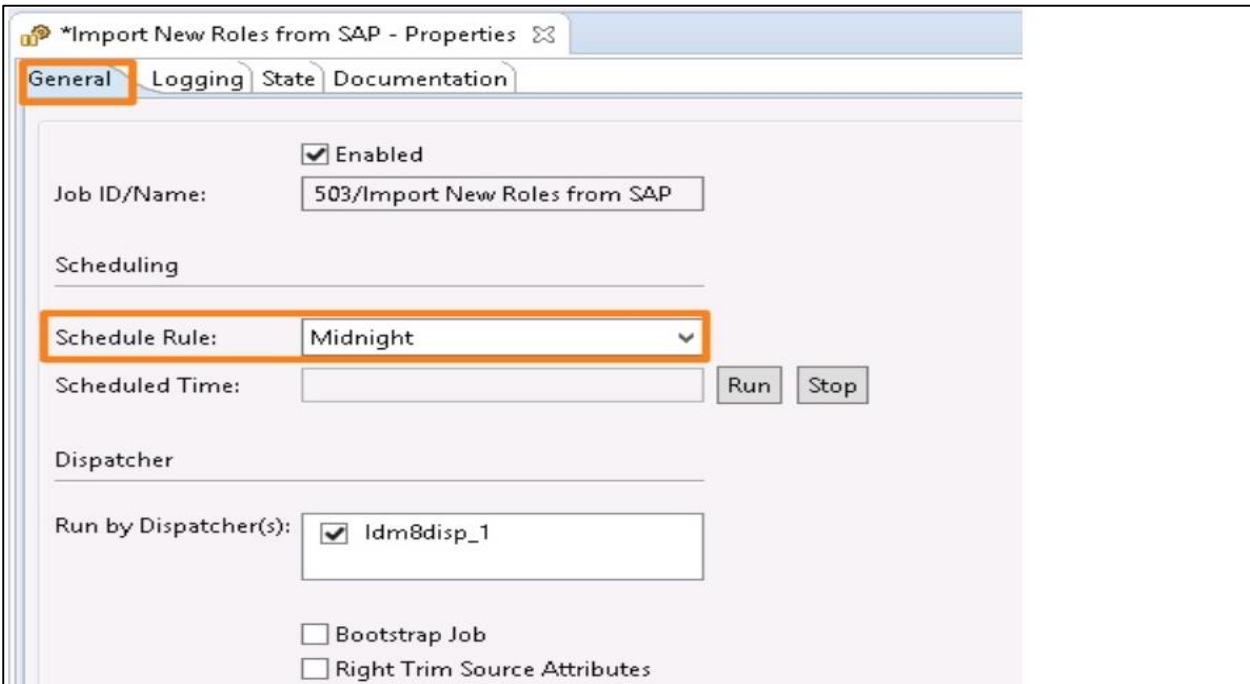
Below options are available to define Job Properties under General tab:

Enabled: This check box can be used to enable/disable the job.

Job ID/Name: This shows the unique ID and job name.

Schedule Rule: The schedule rule is used to define job execution frequency.

Schedule Time: The schedule time displays the time when the job is scheduled to run. You can also select "Run to schedule the job" to be run immediately. The scheduled time is set to the current time.



The screenshot shows the 'Import New Roles from SAP - Properties' dialog box with the 'General' tab selected. The 'Enabled' checkbox is checked. The 'Job ID/Name' field contains '503/Import New Roles from SAP'. Under the 'Scheduling' section, the 'Schedule Rule' dropdown menu is set to 'Midnight' and is highlighted with an orange border. The 'Scheduled Time' field is empty, and there are 'Run' and 'Stop' buttons next to it. Under the 'Dispatcher' section, the 'Run by Dispatcher(s)' field contains 'Idm8disp_1' with a checked checkbox. At the bottom, there are two unchecked checkboxes: 'Bootstrap Job' and 'Right Trim Source Attributes'.

To stop a running job, you can click on "Stop" button.

Run by Dispatcher(s): You can choose the dispatcher(s) that are allowed to run this job.

13. SAP IDM — Self Service Password Reset

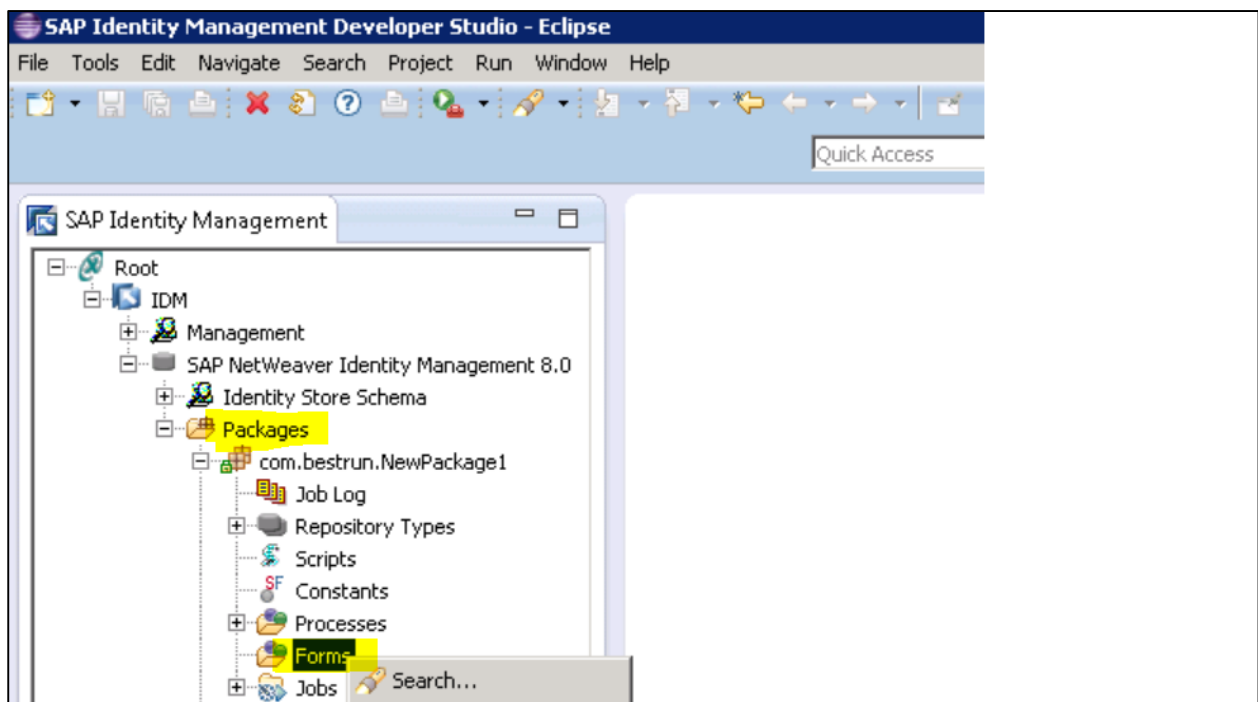
In SAP IdM 8.0 or upper version, you can configure Logon help service or self-service password reset for end users. With login help service, end users can change their password. To configure Self-service password reset, below prechecks should be met:

- You should have minimum one dispatcher running in landscape.
- There should be one user account exists apart from administrator.
- There should be an Identity Management User Interface configured.
- There should be UME role with action "idm_anonymous" assigned Anonymous Users groups in UME.

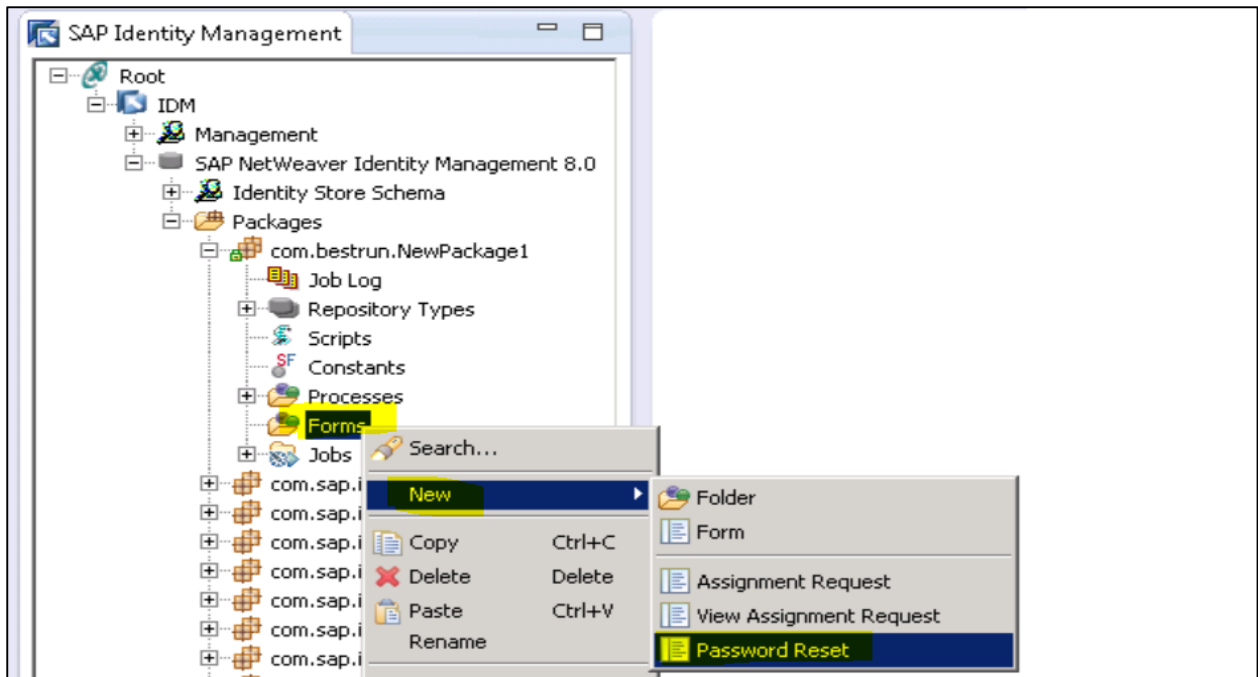
Next step is to create password reset form for end users and to add to identity store configuration.

Follow the steps to create password reset form:

Go to SAP IdM developer studio → Navigate to package where you want to create the form for self-service password reset -> Form.

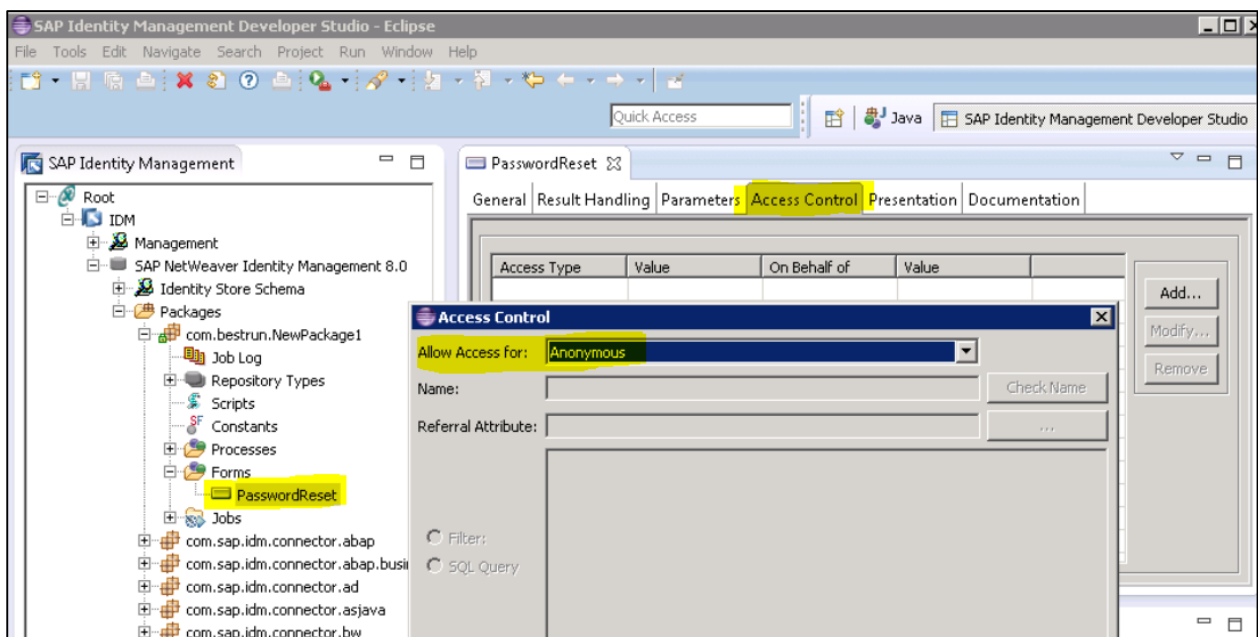


Go to Context menu → New → Password reset. You can rename the form to PasswordReset form.



Next is to assign Anonymous user group to allows access. For this go to "Access Control" tab of the newly created form → Select Anonymous in Allow access drop down → OK.

To save the changes, go to File → Save.



Defining Password Reset Parameters

To use self-service password reset, you need to define password reset parameters like number of questions should prompt, minimum number of correct answers for validation, etc.

To define the parameters, go to Context menu of the Password reset form → Properties. Navigate to Parameters tab and configure the parameters as required.

PasswordReset

General | Result Handling | **Parameters** | Access Control | Presentation | Documentation

Entry type: 6/MX_PERSON

Account Validation
 Min. no of Validation Answers: 5

Identify
 Description: TASK_PASSWORDRESET_STEP1
 Identification Attribute: MSKEYVALUE
 Alternative Identification Attr:

Set Password
 Description: #MX_PWDRCV_STEP3
 Password Creation Method: Ask the User
 Save the Password to UME

Verify Identity
 Description: MX_TASK_PASSWORDRESET_STEP2
 No of Questions to Show: 2
 No of Answers Required: 2
 Maximum no of Attempts: 3

Finish
 Confirmation Message: #MX_PWDRCV_STEP4
 Password Reset Failed Task: 386/PasswordResetFailed

14. SAP IDM — Setting Email Notifications

You can use notification package available in SAP provisioning framework to set up the email notification in SAP Identity Management 8.0. There is package available in Developer Studio "com.sap.idm.util.notification" that contains the notification package and the templates to enable the notification.

To configure email notification, you need to pass the value of "NOTIFYEVENT" package constant and make this point to notification template. You have below notification event types available:

NOTIFYEVENT_ASSIGNMENT_COMPLETED: To send notification related to assigning a privilege

NOTIFYEVENT_ASSIGNMENT_FAILED: To send notification related to failed assignment

NOTIFYEVENT_ASSIGNMENT_REVOKED: To send notification related to access removal

NOTIFYEVENT_PASSWORD_CHANGED: To send notification related to password change

NOTIFYEVENT_USER_MODIFIED: To send notification related to modifying user account

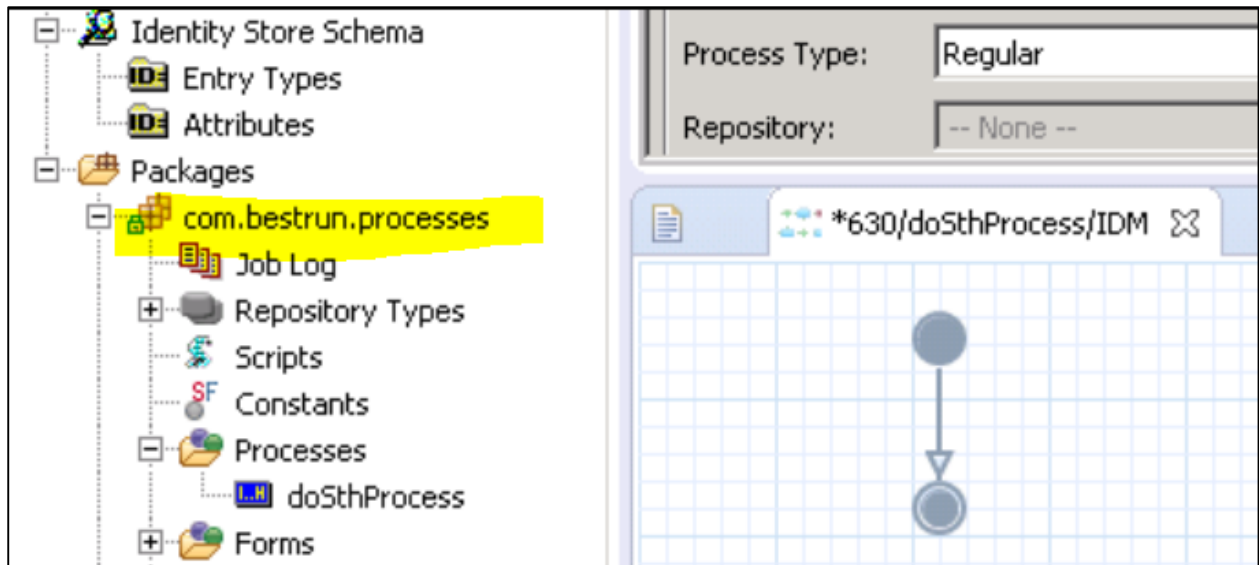
NOTIFYEVENT_USERACCOUNT_CREATED: To send notification related to user account

NOTIFYEVENT_USERACCOUNT_DELETED: To send notification regarding user deletion

NOTIFYEVENT_USERACCOUNT_DISABLED: To send notification related to user account disablement

NOTIFYEVENT_USERACCOUNT_ENABLED: To enable the user notification

To use this notification events, you need to check out a package in IdM Developer Studio and create a process.

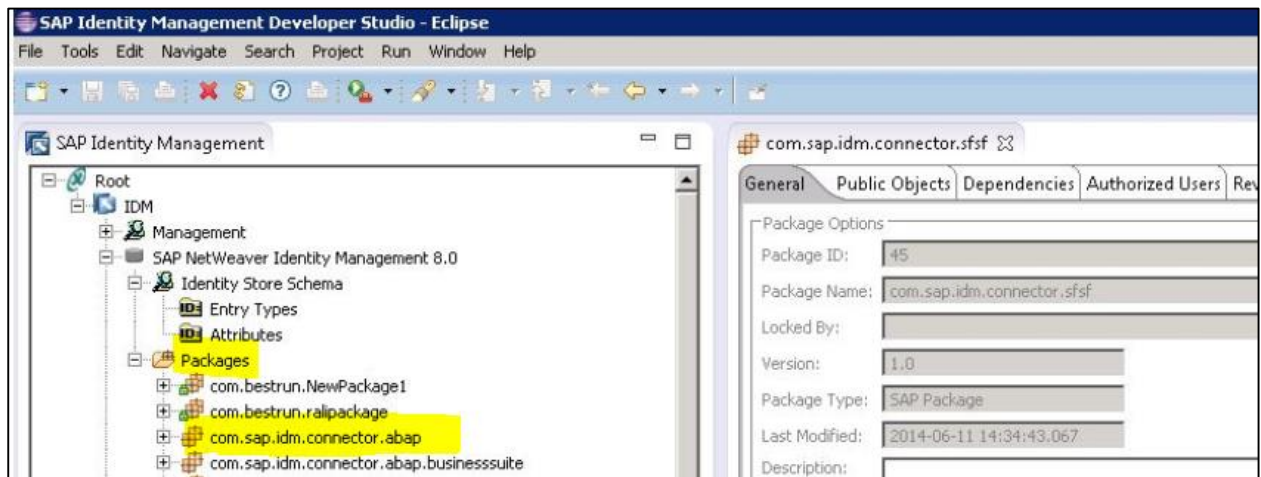


After configuring the notification event types, you need to add the mail template names in the Notification Package constants.

| | | |
|----------------------------------|------------------------------|---------------------------------------------------------|
| NOTIFYEVENT_ASSIGNMENT_COMPLETED | | The mail template used for completed assignment eve... |
| NOTIFYEVENT_ASSIGNMENT_FAILED | | The mail template used for assignment failed event. |
| NOTIFYEVENT_ASSIGNMENT_REVOKED | | The mail template used for revoked assignment event. |
| NOTIFYEVENT_PASSWORD_CHANGED | | The mail template used for password changed event.P... |
| NOTIFYEVENT_USERACCOUNT_CREATED | PF Created user notification | The mail template used for user account created event. |
| NOTIFYEVENT_USERACCOUNT_DELETED | | The mail template used for user account deleted event. |
| NOTIFYEVENT_USERACCOUNT_DISABLED | | The mail template used for user account disabled event. |
| NOTIFYEVENT_USERACCOUNT_ENABLED | | The mail template used for user account enabled event. |
| NOTIFYEVENT_USER_MODIFIED | | The mail template used for user modified event. |

15. SAP IDM — Connecting SAP ABAP Systems

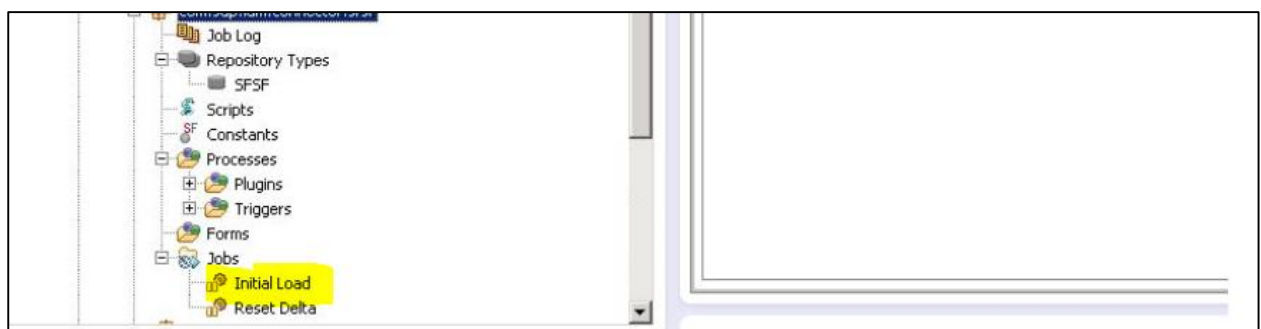
You can configure your SAP Identity management system to connect to SAP ABAP system and provision ABAP users. In SAP IdM 8.0 or higher Provisioning framework, you have connector delivered as separate package with name "com.sap.idm.connector.abap". This connector can be used to communicate SAP Identity management system with SAP ABAP system for user provisioning.



Creating a job for update

In IdM developer studio tree view, you have to select connector package for which you want to create job. Ex: For ABAP connector package "com.sap.idm.connector.abap".

Next is to go to Jobs folder, copy the initial job load and rename the Job for ABAP update in required update, "ABAP- Update".



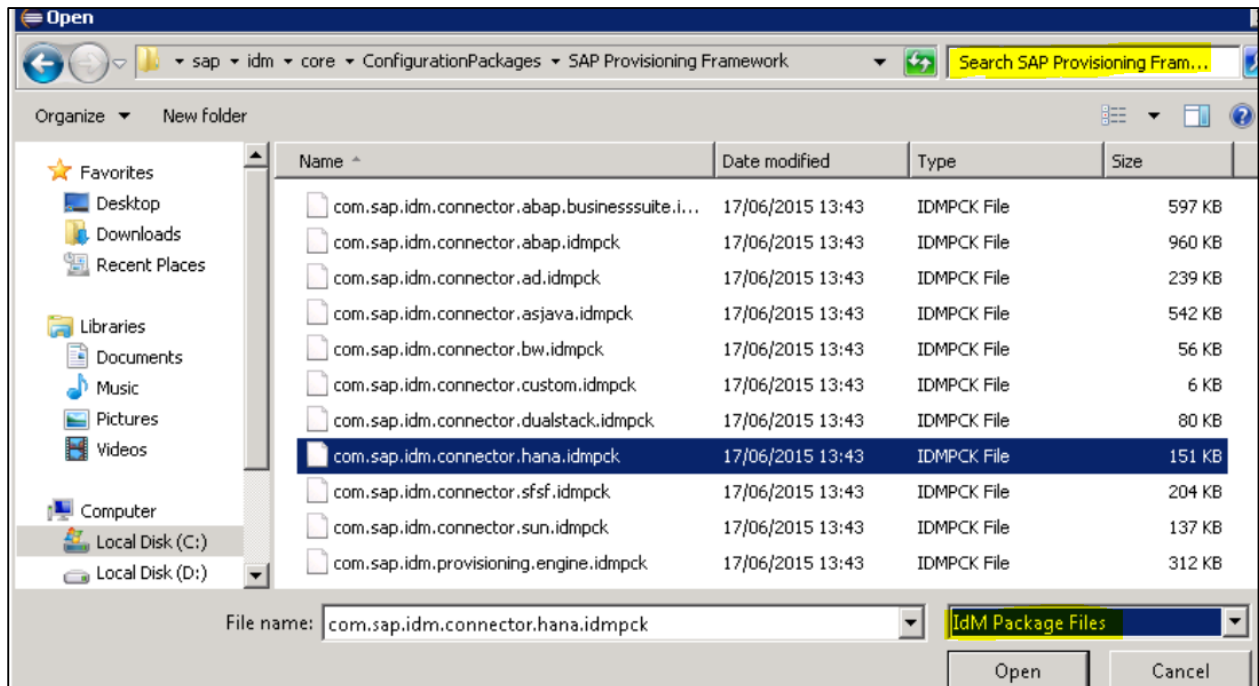
Keep the below pass active and disable the other passes:

- ReadABAPRoles
- ReadABAPProfiles
- ReadABAPCompanyAddress
- ReadJavaRoles
- WriteABAPRolePrivileges: only if corresponding Read pass is active

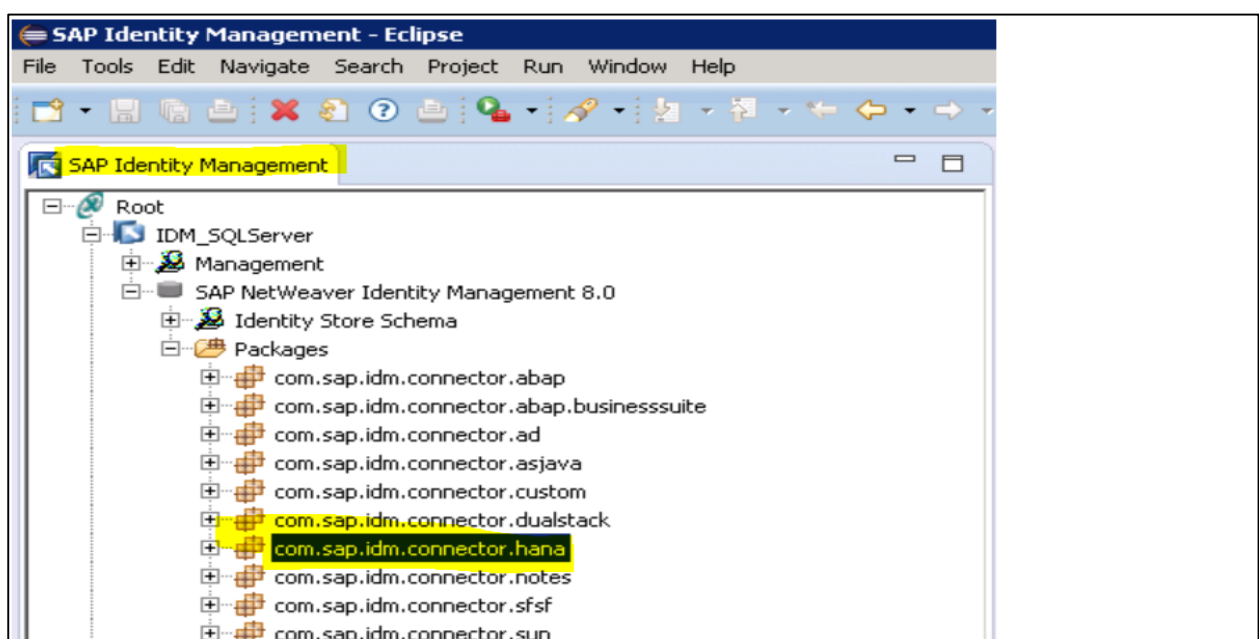
- WriteABAPProfilePrivileges: only if corresponding Read pass is active
- WriteABAPCompanyAddress: only if ReadJavaRoles pass is active
- WriteJavaRolePrivileges: only if corresponding ReadJavaRoles pass is active

There are other packages in SAP IdM developer Studio which can be used to connect to other SAP systems. You have to search for SAP Provisioning Framework packages, choose IdM files and select the correct file.

For example, to connect to SAP HANA system, you can select the HANA connector package file "com.sap.idm.connector.hana.idmpck".



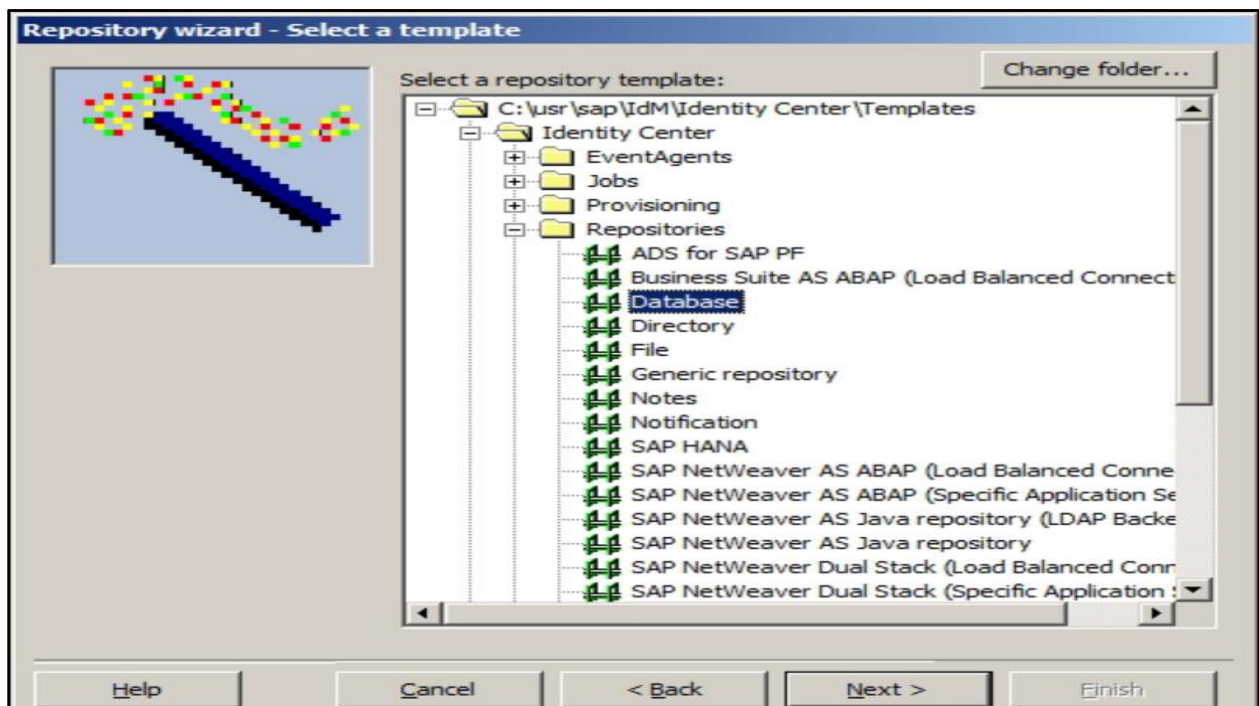
Select the required package, and the package will be imported to Identity Management Developer Studio.



16. SAP IDM — Connecting non-SAP Systems

To connect to non-SAP systems to SAP Identity Management, if default connector package is not available then you can build your own connector for these commonly used systems (JDBC, Web Services, flat files, Database, LDAP, etc.).

First step is to setup the Repository and initial load. For setting up the repository you can use Repository wizard.



Below table confirm the list of connectors Provided in SAP Identity Management:

| | | |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dual Stack | AS Java / J2EE Engine applications
Third-party products that support SPML
AS ABAP applications (SU01 users),
SAP HCM employee data (export to SAP Identity Management) | SAP NetWeaver Dual Stack 6.40 and higher |
| AS ABAP for SAP Business Suite systems | SAP Business Suite applications (provisions SU01 users plus application-specific identity information such as business partners) | SAP Enhancement Package 4 for SAP ERP 6.0
For application-specific dependencies, see the table below |
| Microsoft Active Directory
Microsoft Exchange | Microsoft Active Directory | Microsoft Active Directory Versions with Microsoft Windows Server
2000/2003/2008/2010 Platform: MS Windows Server
2000/2003/2008/2010
Platform: MS Windows Server
2000/2003/2008/2010
Microsoft Exchange 2007/2010 |
| SUN One | Any LDAP directory server using the generic LDAP API
Novell eDirectory
SunOne Directory
Special requirements for other directory servers, for example, schema modifications, on a project base | Platform: Supported platforms for the respective directory server Novell eDirectory or SunOne Directory: Any release |
| SAP HANA Connector | SAP HANA Platform Edition | SAP HANA Platform Support Package Stack 04 |
| Lotus Notes | IBM Lotus Notes | Lotus Domino server version 8.5.3 |

17. SAP IDM — Identity Reporting using SAP BW

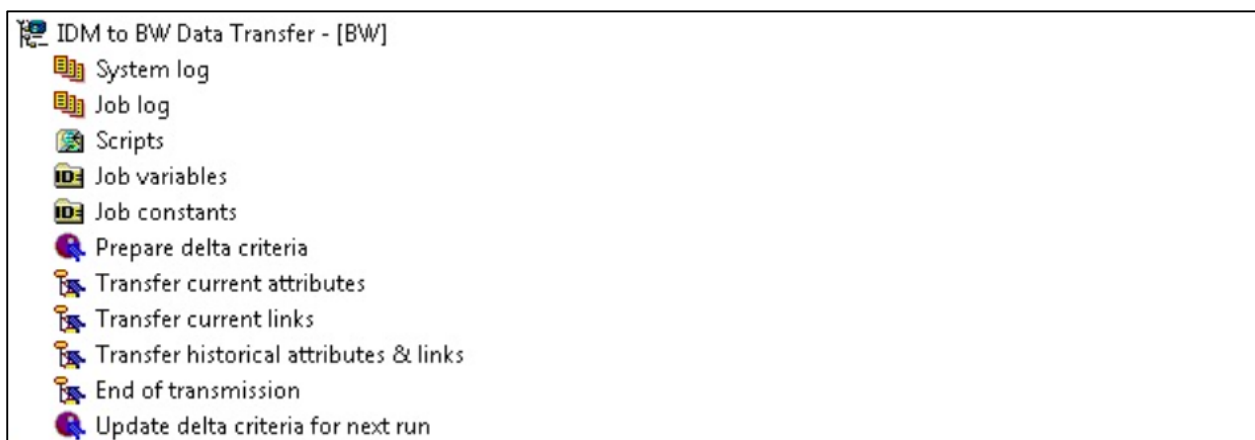
You can also use SAP Business Warehouse system for reporting purpose. To use BW for reporting, you should setup the connectivity between SAP IDM and BW. Post that you need to transfer identity store data to BW. To connect SAP BW, you can use SAP package available in IdM developer Studio.

Below software components will be required while using SAP BW for reporting purpose:

- Identity Center
- Virtual Directory Server (VDS)
- SAP NetWeaver BW
- Web service on the BW system

To start with the data transfer, you need to create a job in the Identity Center that triggers a Web service call from the Virtual Directory Service to the Persistent Staging Area on the BW system.

You can have multiple call configured depends on the amount of data to be transferred. This is used for both, i.e., initial load of the data and to perform the subsequent delta loads.



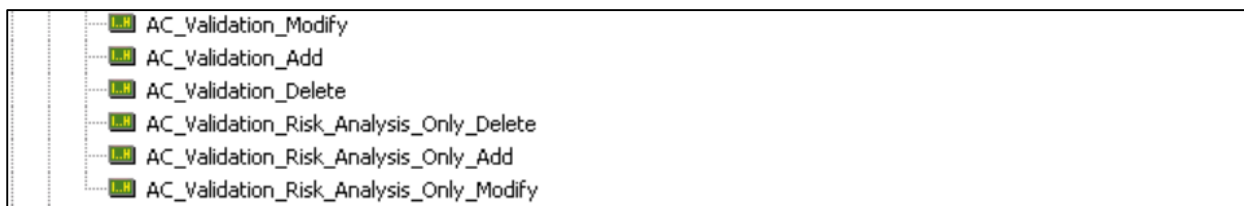
18. SAP IDM — Integration using GRC 10.0

You can integrate SAP Identity management system with Access control GRC by enabling set of processes in Identity center. With use of SAP IdM system, you can perform Provisioning in multiple connected systems based on compliance rules defined in Access Control. Based on communication defined between Identity management and Access Control, you can trigger below calls for implementing role synchronization.

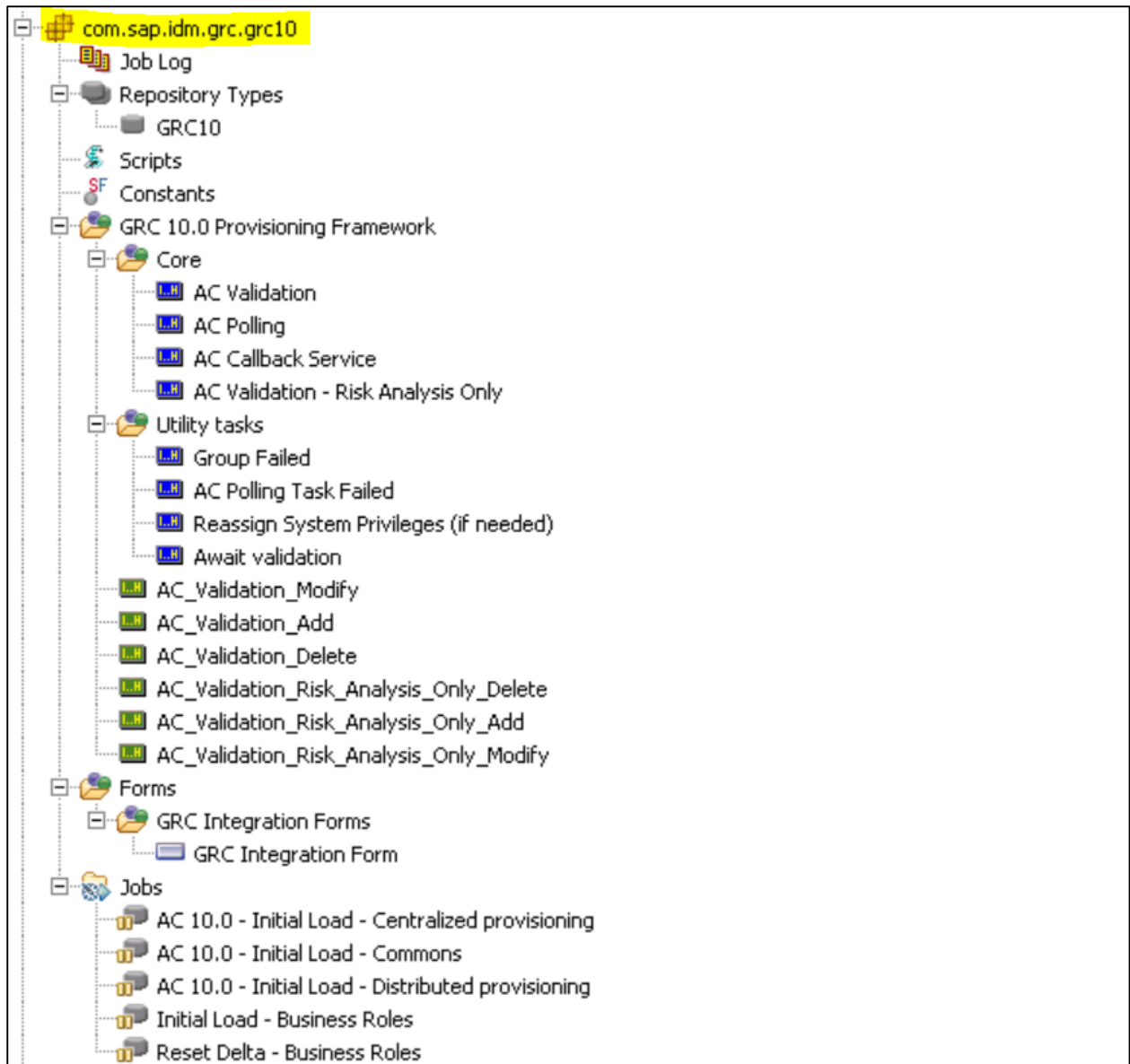
- RFC Communication
- Web Service Communication

To import GRC Provisioning framework to Identity Center, you can use the separate package "**com.sap.idm.grc.grc10**" in SAP Identity Management 8.0 version. This package provides the repository type, initial provisioning processes, jobs, and scripts to perform the initial load.

This package **com.sap.idm.grc.grc10** provides the set of internal and public processes. Below shows the list of public processes:



Following screenshot shows the package structure for integrating GRC Access control to Identity Management:



19. SAP IDM — Migration to New Version

You can also upgrade SAP Identity Management 7.1/7.2 to version 8.0. If you are running with SAP IdM v7.1 then to upgrade to version 8.0, you need to first upgrade to SAP IdM v7.2. To migrate to SAP identity management 8.0, your current system should be running on v7.2 SP09 or v7.2 SP10.

SAP Identity Management v8.0 has some critical improvements from older versions:

- Option to use IDM Developer Studio as Eclipse plug-in
- Ease of integration with other SAP systems
- Better security and access controls

Below checks should be performed before starting the upgrade:

- All dispatchers should be stopped.
- REST API and user interface should be stopped.
- Backup of database and identity data should be taken.
- To upgrade SAP IdM database, you should use mxmc_update script.

You can perform the installation of SAP Idm 8.0 version separately and post installation, you need to copy key.ini file from 7.2 system to mentioned path:

- Use this location on DB node-
/usr/sap/<SID>/SYS/global/security/data/Key/Keys.ini
- Use this location on runtime environment-
/usr/sap/<SAPSID>/IDM<Instance_Number>/Identity_Center/Key/Keys.ini
- You should set Keys.ini file referred to this path-
\\<host>\sapmnt\<SAPSID>\SYS\global\security\data\Key\Keys.ini, where
<SAPSID> is the SAP system ID of SAP Identity Management system
- Next is to perform the Import of identity store from SAP IdM v7.2
- Next is to perform the Import of repositories from SAP IdM v7.2
- Next is to perform the Import job folders from SAP IdM v7.2
- Next is to perform the Import data from SAP IdM v7.2

20. SAP IdM — Job Responsibilities

Key responsibilities of SAP IdM Administrator are as follows:

- With minimum 3-6 years of experience in SAP IdM
- Experience in connecting IdM to SAP and non-SAP systems, AD system and Database
- Ability to handle business role-based assignments
- Setting and monitoring the IdM jobs
- Good understanding and experience in SAP Security and authorizations
- Experience in performing SAP IdM tasks- user management, business and process workflows, managing identity stores
- Setting up the repositories for different SAP and non-SAP apps
- Knowledge of SAP GRC v10 Access Control and segregation of duties based on roles including GRC rules
- Good understanding on Information Security controls and knowledge of ISO27001 controls