

Upgrade Guide | PUBLIC
Document Version: 1.12 – 2025-01-20

Upgrading SAP Identity Management from 7.2 to 8.0

© 2025 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Upgrading SAP Identity Management from 7.2 to 8.0. 3

2 Upgrade Strategies. 4

2.1 Upgrading Entire Existing System. 4

Installing SAP Identity Management Developer Studio. 9

Post-Upgrade Results. 32

Upgrading QA and PROD Systems. 35

2.2 Installing SAP Identity Management 8.0 and Importing Existing Configuration and Data. 36

Importing Identity Stores. 38

Importing Repositories. 39

Importing Single Jobs and Job Folders. 40

Importing the Data. 42

1 Upgrading SAP Identity Management from 7.2 to 8.0

This document describes how you upgrade a production system with the provisioning framework for SAP systems from SAP Identity Management 7.2 to 8.0.

If you are currently running version 7.1, you need to upgrade first to 7.2 and then to 8.0, but you can do that in the same upgrade project without running live on 7.2.

> **Note**
>
> Before starting the upgrade process, make sure you read the whole document.

Related Information

Upgrade Strategies [page 4]

2 Upgrade Strategies

There are two main strategies for an SAP Identity Management upgrade:

- Upgrade the entire existing system to the new version.
- Install SAP Identity Management version 8.0 as a side box, move the configuration and data from the old system, and retire the old one.

> ⚠ Caution
>
> To move data from 7.2 to 8.0 system, customers need to implement their own solutions. This guide covers only importing users and privileges and provides an example for importing roles. Moving data, such as dynamic groups, historic and future values, audit information, logs and others, is subject to customers' implementation.

> → Recommendation
>
> Deciding upon an upgrade strategy depends on the complexity of the SAP Identity Management configuration scenarios for each customer. Based on the considerations regarding moving data from 7.2 to 8.0 system, we recommend you to upgrade your entire existing system to the new version.

Related Information

Upgrading Entire Existing System [page 4]
Installing SAP Identity Management 8.0 and Importing Existing Configuration and Data [page 36]

2.1 Upgrading Entire Existing System

The initial upgrade process is quite similar to a 7.2 SP update process.

Prerequisites

To execute a successful SAP Identity Management upgrade, you need to fulfil the following prerequisites:

- You are running 7.2 SP09 at least (preferably 7.2 SP10).

> **Note**
>
> If you are currently running a lower 7.2 SP, you need to update to 7.2 SP09 at least (preferably 7.2 SP10), and then upgrade to 8.0. You can do that in the same upgrade project without running live on 7.2 SP09 or SP10.

- You have upgraded all underlying components to the currently supported ones - check the Product Availability Matrix (PAM). For example, first upgrade SAP NetWeaver to 7.3 SP09 or higher.
- You have switched the JVM on all places to SAP JVM, as defined in the PAM.
  SAP Identity Management 8.0 supports only SAP JVM. You should use SAP JVM, where version 8.1 (Java 1.8) is required for the runtime components and the Virtual Directory Server. For information about how to download the SAP JVM, see SAP Note 1442124

  > **Note**
  >
  > It is recommended to use the latest SAP JVM released version.

  All SAP Identity Management components deployed on SAP NetWeaver AS for Java can run with SAP JVM version 6.1 (Java 1.6).
- You have switched any job that uses Windows Runtime or VBScripts to Java Runtime and JavaScripts, as Windows Runtime and VBScripts are not supported in version 8.0.
  To identify those jobs, execute the following query:

  ```
  SELECT JobGuid, Name FROM mc_jobs WHERE Engine_Type <> 2
  ```

  Adjust the jobs, otherwise you will not be able to run them. For more information, see SAP Note 2907067
- You have set the SAP_MASTER_IDS_ID global constant to the identity store where the SAP provisioning framework is imported.
- Make sure that there are no repository constants of type Job Reference which refer to missing jobs.
- Make sure that there is no cyclic dependency between tasks (that is, in a task hierarchy, a child task refers to one or more parent tasks). If there is a cyclic dependency between tasks, perform the queries in the following KBA: 2681454
- If you upgrade from version 7.2 to 8.0 and you want to use the Java-based Lotus Notes connector, you need to run the Migrate Data from 7.2 job. See Migrating to Java-Based Lotus Notes Connector

> **Note**
>
> Although terminology has changed in version 8.0, content has been kept stable. A UI task has been renamed to a Form, but its content does not need to be changed.

> **Caution**
>
> Although the provisioning queue does not need to be empty when you start the upgrade process, we recommend that you limit the number of queue items, for example, by executing the upgrade during a period of low system usage.

> **→ Recommendation**
>
> Do not upgrade your productive system directly. We recommend that you upgrade a copy of your productive system.

Context

This upgrade strategy consists of the following steps:

Procedure

1. Before executing the upgrade, stop all dispatchers.
2. Back up your database schema and data.
3. Stop the user interface and REST API applications. See Starting and Stopping
4. Upgrade the SAP Identity Management database using the `mxmc_update` script.

   For Microsoft SQL Server, Oracle or IBM DB2, see

   - Updating SAP Identity Management Core on Windows
   - Updating SAP Identity Management Core on UNIX

   > ⚠ Caution
   >
   > You need to define a system namespace, which is used as the core for qualified names, including the default package that is created during the upgrade process.

   > ⓘ Note
   >
   > You need to define a developer administrator that specifies which users are IDM developers.
5. Upgrade the runtime components. See
   - Updating Runtime Components on Windows
   - Updating Runtime Components on UNIX
6. Copy the `Keys.ini` file of version 7.2 (containing the old encryption key) to the following location: `<IdM install directory>\core\KeysIniUtility\Key`.

   > ⓘ Note
   >
   > We recommend that you use the SAP Identity Management Keys Utility from now on to manage keys.

   > ⚠ Caution
   >
   > For security reasons, we recommend that you also change the hashing and encryption keys so that developers no longer know them. In 7.2, the `keys.ini` file was used also by the Management Console and thus a developer might have a copy. In version 8, you no longer need to distribute the `keys.ini` file to the developers.

   Copy the `Keys.ini` file to the Identity Management Runtime Components installation folder `<IdM Runtime Components installation>\Key`. For example: `C:\usr\sap\idm\Identity Center\Key`. The `Keys.ini` file is now ready for use.
7. Upgrade the SAP Identity Management user interfaces.

   For SAP Identity Management User Interface, see

- Updating Identity Management User Interface on Windows
- Updating Identity Management User Interface on UNIX

For SAP Identity Management User Interface for HTML5, see

- Updating the Identity Management User Interface for HTML5 on Windows
- Updating the Identity Management User Interface for HTML5 on UNIX

8. Upgrade the REST service. See
   - Updating the REST Interface Version 2 on Windows
   - Updating the REST Interface Version 2 on UNIX
9. Deploy the new Identity Management Developer Studio service. See Deploying the Identity Management Developer Studio Service [page 15]
10. Configure the JDBC connection to be used by the Developer Studio service. See Defining the JDBC Connection for Identity Management Developer Studio Service [page 16]
11. Configure the properties for the deployed Identity Management Developer Studio service on your SAP NetWeaver AS for Java. See Configuring the Java System Properties [page 19]
12. Install the Identity Management Developer Studio on each developer workstation. See Installing the Identity Management Developer Studio [page 22]

> **Note**
>
> Before SAP Identity Management developers can connect to the SAP Identity Management Developer Studio service, they need to be created in the UME as well as added as developers by the developer administrator. In addition, they need the `idm_authenticated_studio` UME action assigned to them through a UME role. You can use the `idm.developer` role, as it already contains this action.
>
> You can do this now or later after the upgrade.

13. Log on to SAP Identity Management Developer Studio and expand the default package where all 7.2 configurations are migrated. When you expand the default package for the first time, it may take a while to display the package structure.

> **Note**
>
> It is very important to expand the default package at this stage of the upgrade process. Expanding it starts the migration of repository types, repositories, repository constants and repository type variables. Skipping this step results in data loss.
>
> You can have more than one package in the Identity Management Developer Studio, because every migrated identity store from your 7.2 system contains its own default package in 8.0. This means that if you have two identity stores in 7.2, you will again have two identity stores in 8.0, each of them containing its own default package where the 7.2 configuration is migrated. Each default package must be expanded separately.

14. Uninstall the Management Console.

> **Caution**
>
> For security reasons, we recommend that you change the password of the mxmc_admin user in order to guarantee that no copy of the Management Console can connect anymore.

15. Start all stopped components. See Starting and Stopping

16. (Optional) If you want to use the new packaged provisioning framework that comes with version 8.0, you have to import the provisioning framework packages explicitly and adapt your configuration to use them. See: Importing the Provisioning Framework for SAP Identity Management 8.0

> **Note**
>
> Using the old provisioning framework has clear disadvantages. You cannot get support for it, as it is part of version 7.2 which is out of mainstream maintenance. Furthermore, you cannot benefit from new features, improvements and bug fixes delivered with the new provisioning framework.

> **Caution**
>
> When you choose to migrate the 7.2 provisioning framework to 8.0, importing the provisioning framework as stated in this step is not the only mandatory step that needs to be performed in order to use the higher version of the provisioning framework.

As updating the provisioning framework overwrites the existing framework, we do not recommend changing the framework itself. Instead, import the packages that you want to modify under a new name and make the changes there or use the custom package for your customizations.

> **Note**
>
> If you have implemented package customizations (for example, in packages imported under new names, package copies or the custom package), note that when you import a new version of SAP delivered packages, you should manually apply the changes in your customized packages.

After importing the new 8.0 framework packages, following the procedure above, execute the steps below:

- Before migrating to the new repository types, check and maintain all necessary repository constants according to your custom business logic needs. Repository constants that are shared between the (old) 7.2 and the new 8.0 repository types are automatically entered when a repository is migrated.
- Migrate all repositories included in your 7.2 provisioning framework configuration to the new repository types delivered with the 8.0 provisioning framework. See: Changing Repository Type of Repositories.

17. (Optional) Manual restructuring of the default package into multiple packages can start. Restructuring logic is customer-specific and use case-specific.

Results

The SAP Identity Management system is up and running with the old content and can be made live again.

If the upgrade fails, check the logs described in Identity Management: Error When Upgrading from 7.2 to 8.0.

Related Information

Product Availability Matrix
Post-Upgrade Results [page 32]
Upgrading QA and PROD Systems [page 35]

2.1.1 Installing SAP Identity Management Developer Studio

This section describes how to install and configure the SAP Identity Management Developer Studio.

Prerequisites

The following prerequisites are present:

- An Identity Management database correctly installed.
- Java Runtime Environment and Identity Management Runtime Components correctly installed and configured.
- 64-bit Java, version 1.8.
- JDBC driver for the Identity Management database.
- One of the following SAP NetWeaver versions must be correctly installed and licensed:
  - SAP NetWeaver 7.3 SP09 or higher.
  - SAP NetWeaver 7.3 including Enhancement Package 1 (EHP1) SP06 Patch 3 or higher. service must be deployed on your
  - SAP NetWeaver 7.4 SP02 or higher.
  - SAP NetWeaver 7.5 SP08 or higher.
- Basic knowledge about the SAP NetWeaver AS for Java service must be and its tools.
- Administrator rights for the SAP NetWeaver AS for Java server.
- SAP Cryptographic Library installed for your SAP NetWeaver AS for Java version according to *Installing the SAP Cryptographic Library for SSL*.
- As of version 8.0 SP04 and higher, SAP Identity Management software components are delivered as *.SAR files. You require the SAPCAR archiving tool to be able to unpack software component archives (`*.SAR` files).
  Make sure the latest version of the SAPCAR archiving tool is available on each installation host. You can download the latest version of SAPCAR from:
  http://support.sap.com/swdc *Support Packages and Patches* > *A - Z Index* > *S* > *SAPCAR*.
  For more information about SAPCAR, see SAP Note 212876.

The following steps are covered in this section:

Step	Description
Installing/deploying the Identity Management Developer Studio service on your SAP NetWeaver AS for Java.	The Identity Management Developer StudioSAP NetWeaver AS for Java. You use the Software Update Manager (SUM) to deploy the service. For details see topics Deploying the Identity Management Developer Studio Service [page 15] and Using the Software Update Manager (SUM) 1.0.

Step	Description
Defining the JDBC connection	Defining the JDBC connection on your SAP NetWeaver AS for Java involves adding the Identity Management database as a data source in the SAP NetWeaver Administrator. Before the Identity Management database can be defined as a data source, you need to make sure that the JDBC drivers for your database are available/deployed on your SAP NetWeaver AS for Java. See topics Defining the JDBC Connection for Identity Management Developer Studio Service [page 16], Deploying the JDBC Driver [page 16] and Adding the Database as the Data Source [page 17].
Configuring the Java System Properties	This step covers the configuration of properties of the deployed Identity Management Developer Studio service on your AS Java. See topic Configuring the Java System Properties [page 19].
Installing the Identity Management Developer Studio	The client is available as an Eclipse plugin, and requires the Eclipse version 2024-09 and your Java to be 64-bit and version 6 or higher. For details see Installing the Identity Management Developer Studio [page 22].
Using and configuring the HTTP Security (SSL)	To ensure the security between the deployed Identity Management Developer Studio service and the client, you need to secure the web server (your SAP NetWeaver AS for Java) using the HTTPS (SSL) to secure the connection. Configure the SAP NetWeaver AS for Java to use SSL, then export and install the SSL certificate into the client keystore. For details see Using the HTTP Security (Secure Sockets Layer/SSL) [page 24] and Exporting and Installing the SSL Certificate [page 26].
Initial configuration of the Identity Management Developer Studio	Set up the connection to the application server, its (HTTPS) port and the Identity Management database. To be able to login and access the contents in the Identity Management Developer Studio, you would also need to make sure that an inital admin user for the Identity Management Developer Studio exists in the UME.

Step	Description
	See topics Initial Configuration of Identity Management Developer Studio [page 27] and Creating the Developer Administrator User in UME [page 30].

Related Information

Installing the Java Runtime Environment [page 11]
Installing the JDBC Drivers [page 12]
SAP NetWeaver 7.3
Installing the SAP Cryptographic Library for SSL
SAP NetWeaver 7.3 EHP1
Installing the SAP Cryptographic Library for SSL
SAP NetWeaver 7.4
Installing the SAP Cryptographic Library for SSL
SAP NetWeaver 7.5
Installing the SAP Cryptographic Library for SSL

2.1.1.1 Installing the Java Runtime Environment

The runtime components of Identity Management require a Java Virtual Machine. It must be installed on all of the servers running one of the Identity Management components:

- Dispatcher
- Runtime engine (Java)

SAP Identity Management 8.0 supports only SAP JVM. You should use SAP JVM, where version 8.1 (Java 1.8) is required for the runtime components and the Virtual Directory Server. For information about how to download the SAP JVM, see SAP Note 1442124.

> **Note**
>
> It is recommended to use the latest SAP JVM released version.

All SAP Identity Management components deployed on SAP NetWeaver AS for Java can run with SAP JVM version 6.1 (Java 1.6).

> **Note**
>
> For an overview of the installation prerequisites for the SAP JVM, see SAP Note 1367498.

> **Note**
>
> If you run on a 64-bit platform, you can install either the 32-bit or the 64-bit version of the Java Runtime Environment. If you use Oracle as your database system, make sure that the version of the Java Runtime Environment matches the version of the database client.

Java Cryptographic Extension Jurisdiction Policy Files

The Java Cryptographic Extension Jurisdiction Policy files are a prerequisite for the SAP JVM must be downloaded separately as described in SAP Note 1240081.

2.1.1.2 Installing the JDBC Drivers

The JDBC drivers are used by the runtime components to access databases, both the Identity Management database and other data sources that are accessed using JDBC.

The SAP NetWeaver AS for Java running the Identity Management user interface needs the JDBC driver to access the Identity Management database.

The correct JDBC driver must be installed on all servers running any of the following components:

- Runtime components
  - Dispatcher - JDBC driver for the Identity Management database
  - Runtime engine (Java) - JDBC driver(s) for the Identity Management database and any other databases/data sources that are accessed
- Identity Management Developer Studio service - JDBC driver for the Identity Management database
- Identity Management user interface - JDBC driver for the Identity Management database

Related Information

Oracle JDBC Driver [page 13]
IBM DB2 JDBC Driver [page 13]
SAP ASE JDBC Driver [page 14]
JDBC Drivers for External Systems [page 14]

2.1.1.2.1 Microsoft SQL Server JDBC Driver

> **Note**
>
> Be aware of the dependencies between the SAP NetWeaver version, the required JVM and the supported JDBC driver. Always use the JDBC driver version that is compatible with the JVM version of your SAP NetWeaver release.

Use the recommended JDBC driver for your Microsoft SQL Server version.

Download the JDBC driver for your Microsoft SQL Server version from the Microsoft Download Center. Follow the installation instructions provided on the installation web page.

The name of the JDBC driver is:

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

For more information, see the system requirements for the JDBC driver in the Microsoft Developer Network.

Related Information

Microsoft SQL Server Web Page
System Requirements for the JDBC Driver from Microsoft Developer Network

2.1.1.2.2 Oracle JDBC Driver

Use the recommended JDBC driver for your Oracle version.

You can download the JDBC driver `ojdbc<JDK version>.jar` for your Oracle version from the Oracle JDBC Downloads page. Follow the installation instructions provided on the installation web page.

Related Information

Oracle Web Site

2.1.1.2.3 IBM DB2 JDBC Driver

The JDBC driver for IBM DB2 is installed with the database client.

By default it is installed in this folder:

The file name is: `db2jcc4.jar`.

The JDBC driver name is: *com.ibm.db2.jcc.DB2Driver*.

Make sure that the file name is added to the classpath.

2.1.1.2.4 SAP ASE JDBC Driver

Use the following JDBC driver:

Database Version	JDBC Driver Version
SAP ASE 16.0	JDBC 4.0
SAP ASE 16.0 SP04	JDBC 4.2

The JDBC driver for SAP ASE is installed with the database client. Depending on the database version used, it is installed in the following folder:

- **SAP ASE version 16.0**
  The `jconn4.jar` file is located in .
  The name of the JDBC driver is: *com.sybase.jdbc4.jdbc.SybDriver*
  Make sure that the CLASSPATH is set to the correct file: .
- **SAP ASE version 16.0 SP04**
  The `jconn42.jar` file is located in
  The name of the JDBC driver is: *com.sybase.jdbc42.jdbc.SybDriver*
  Make sure that the CLASSPATH is set to the correct file: .

> ⚠ Caution
>
> If you experience issues with the JDBC connection, refer to the SAP Note 2270221.

2.1.1.2.5 JDBC Drivers for External Systems

Any JDBC drivers that are accessed by the runtime components must be installed and made available on all servers. These JDBC drivers must be obtained from the vendor of the database or another data source.

2.1.1.3 Deploying the Identity Management Developer Studio Service

Prerequisites

You require the SAPCAR archiving tool to be able to unpack software component archives (`*.SAR` files).

Context

To deploy the SAP Identity Management Developer Studio service on your SAP NetWeaver AS for Java, proceed as follows:

Procedure

1. In the SAP Software Download Center, navigate to the area of SAP Identity Management 8.0 and download the installation set for `IDMCLMRESTAPI` component.
2. Unpack the installation kit using the following command:

   ```
   SAPCAR -xvf <your-SAR-file>
   ```

3. Make sure that your have the Identity Management Developer Studio service to be deployed (the SCA file `IDMCLMRESTAPI<version>.SCA`) available on your system.
4. Use the Software Update Manager (SUM) to deploy the SCA file on your SAP NetWeaver AS for Java.

   For more information, see: Using the Software Update Manager (SUM) 1.0

   > **Note**
   >
   > For the performance purposes it is recommended that the Identity Management Developer Studio service is installed on the same server where the Identity Management database is installed.

Related Information

SAP Software Download Center (SAP Support Portal)

2.1.1.4 Defining the JDBC Connection for Identity Management Developer Studio Service

In order to be able to retrieve data from the identity store of the Identity Management Developer Studio, a JDBC data source needs to be pointing to the Identity Management database.

To set up the JDBC connection, the following steps need to be completed:

- Before creating a JDBC data source, make sure that the driver for your database system are deployed on your SAP NetWeaver AS for Java.

  > ### Note
  >
  > If operating with multiple Java nodes, the driver needs to be installed on all these.

  > ### Note
  >
  > The JDBC driver you use must be compatible with the SAP JVM of your SAP NetWeaver version. For example, SAP NetWeaver 7.3 is compatible with SAP JVM 6.1 (JDK 1.6). This means that you cannot use JDBC driver version higher than 4.0.

- Add the Identity Management database as a data source on your SAP NetWeaver AS for Java server.

The procedure may be different depending on your version of SAP NetWeaver. To set up this connection for the supported SAP NetWeaver versions, use the SAP NetWeaver Administrator (NWA).

To access the SAP NetWeaver Administrator, enter **`http(s)://<host>:<port>`** in your browser (which will take you to your start page) and select *SAP NetWeaver Administrator*. Alternatively, just enter **`http(s)://<host>:<port>/nwa`** directly in your browser. Both will display the login page for the SAP NetWeaver Administrator. Provide your credentials to access.

Related Information

Deploying the JDBC Driver [page 16]
Adding the Database as the Data Source [page 17]
Configuring the Java System Properties [page 19]

2.1.1.4.1 Deploying the JDBC Driver

Make sure that the driver for your Identity Management database system is deployed on your SAP NetWeaver AS for Java.

To deploy the driver for your database system, follow the descriptions of managing the JDBC drivers for your SAP NetWeaver version (see *Related Information*).

> **Note**
>
> Even though specifying an arbitrary name for your driver entry (such as myDriver) will be sufficient, it is recommended to give the driver a logical name, for example, ORACLE, DB2.

Related Information

Managing JDBC Drivers for SAP NetWeaver 7.3
Managing JDBC Drivers for SAP NetWeaver 7.3 EHP1
Managing JDBC Drivers for SAP NetWeaver 7.4
Managing JDBC Drivers for SAP NetWeaver 7.5

2.1.1.4.2 Adding the Database as the Data Source

To add the Identity Management database as the data source on your SAP NetWeaver AS for Java, follow the descriptions of managing the JDBC data sources for your SAP NetWeaver version.

> **Note**
>
> You have to choose the JDBC version 1.x when creating a JDBC data source in the SAP NetWeaver AS for Java. It is important to emphasize that the mentioned JDBC version is not related to the version of the JDBC driver you are using. You may use all supported JDBC driver versions for the supported databases.

- Managing JDBC DataSources for SAP NetWeaver 7.3
- Managing JDBC DataSources for SAP NetWeaver 7.3 EHP1
- Managing JDBC DataSources for SAP NetWeaver 7.4
- Managing JDBC DataSources for SAP NetWeaver 7.5

Make sure to save the defined data source when all the necessary information is provided.

Following the processes for adding the database as a data source, pay special attention to the following fields (and apply the values listed) on the *Settings* tab:

Name of the Field	Value/Comments
Data Source Name	No special requirements for the name of the data source. E.g. *IDM_DataSource_DevStudio*. You may create an alias for your data source, but this is not required. Read more about creating and managing aliases for SAP NetWeaver here: • Managing JDBC DataSource Aliases for SAP NetWeaver 7.3

Name of the Field	Value/Comments
	• Managing JDBC DataSource Aliases for SAP NetWeaver 7.3 EHP1 • Managing JDBC DataSource Aliases for SAP NetWeaver 7.4 • Managing JDBC DataSource Aliases for SAP NetWeaver 7.5
Driver Name	Select the JDBC driver that you have deployed in the previous step.
SQL Engine	Choose *Vendor SQL* for Oracle, IBM DB2 and SAP ASE.
Isolation Level	Select *Transaction Read Commited*.
JDBC Version	Make sure that the 1.x JDBC version is selected.
Driver Class Name	Fill in the driver class: • *oracle.jdbc.driver.OracleDriver* for Oracle • *com.ibm.db2.jcc.DB2Driver* for IBM DB2 • *com.sybase.jdbc4.jdbc.SybDriver* for SAP ASE
Database URL	Provide the correct database URL: • For Oracle: jdbc:oracle:thin:@<host>:<port>:< SID> (e.g. jdbc:oracle:thin:@10.55.165.63:1521:orcl) • For IBM DB2: jdbc:db2://<server>:<port>/<prefix>_DB:currentSchema=<PREFIX>_OPER;currentFunctionPath=<PREFIX>_OPER;maxStatements=100;retrieveMessagesFromServerOnGetMessage=true; **Note** When using IBM DB2, make sure the `<PREFIX>_OPER` user in the database URL is in uppercase letters. For example: jdbc:db2://MyServer:52222/IC_DB:currentSchema=IC_OPER;currentFunctionPath=IC_OPER;maxStatements=100;retrieveMessagesFromServerOnGetMessage=true; • For SAP ASE: jdbc:sybase:Tds:<host>:<port>/<prefix>_db
User Name	Enter the admin user name that you use to log in to the database server. For example, <prefix>_admin (for example MXMC_admin or IC_admin).

Name of the Field	Value/Comments
Password	Provide the password of the provisioning user defined in the *User Name* field.

2.1.1.5 Configuring the Java System Properties

You can change the settings or properties of your SAP NetWeaver AS for Java, or deployed applications/ services on your SAP NetWeaver AS for Java.

To configure the properties for the deployed Identity Management Developer Studio service and Identity Management REST Interface version 2 on your SAP NetWeaver AS for Java, follow the descriptions of how to manage the properties in Java System Properties tool for your SAP NetWeaver version:

- Java System Properties for SAP NetWeaver 7.3
- Java System Properties for SAP NetWeaver 7.3 EHP1
- Java System Properties for SAP NetWeaver 7.4
- Java System Properties for SAP NetWeaver 7.5

Identity Management Developer Studio service

Log on to SAP NetWeaver Administrator and choose *Configuration* > *Infrastructure* > *Java System Properties* > *Applications* . Following the descriptions for your SAP NetWeaver AS for Java, configure the following properties for the *idmdevstudio* application (service):

Properties for idmdevstudio application (service)

Property	Value
`com.sap.idm.rcp.crypt.keyfile`	A full path to the file holding the 3DES keys, i.e. the `Keys.ini` file. For example: **Note** If SAP NetWeaver AS for Java is not installed on the same host as the Runtime components, the `Keys.ini` file that is located in the folder: `/usr/sap/IdM/Identity Center/Key` should be copied to the `/sapmnt` directory of the AS Java. It is the global directory of SAP NetWeaver AS Java which is accessible for all Java instances in cluster environment. Ensure that the <SID>adm user has the proper permissions to copy the `Keys.ini` file to the `/sapmnt` directory of the AS Java.
`com.sap.idm.rcp.dsehome.java`	Path to *sapjvm 8*, unless you are using Java 8 by default.
`com.sap.idm.rcp.jdbcdriverjar`	Path to the JDBC driver JAR file. For example: This can also be a list of paths (to several JDBC driver JAR files). List items are separated as follows:
`com.sap.idm.rcp.jdbcdrivers`	A list of JDBC driver names. For example, oracle.jdbc.driver.OracleDriver;com.ibm.db2.jcc.DB2Driver;com.sap.db.jdbc.Driver;com.sybase.jdbc4.jdbc.SybDriver. **Note** List items are separated as follows:
`com.sap.idm.rcp.dsehome`	The path relative to which the runtime engine is found. For example: This is needed for data discovery purposes.

Property	Value
`com.sap.idm.rcp.multicheckouts`	Controls whether multiple users are allowed to check out one and the same configuration package. • *False* - Only one user is allowed to check out a package and work on its configuration. This is the default value. • *True* - Multiple users are allowed to check out a package and work simultaneously on its configuration. **Note** Be careful when setting this property to *True*. We do not recommend multiple users to check out one and the same package. If multiple users modify one and the same package object, (for example, a process) they will override each other's changes. **Note** The first user who checks in the package, checks in (saves) the changes of all the users that checked out this package. **Note** Allowing multiple users to check out one and the same package is suitable for systems that are upgraded from version 7.2. In this case, all configurations are placed into one default package that needs to be restructured manually into multiple packages.

Identity Management REST Interface Version 2

Log on to SAP NetWeaver Administrator and choose *Configuration* > *Infrastructure* > *Java System Properties* > *Applications*. Configure the following properties for the *tc~idm~rest~ear* application:

Properties for restapi-ear application

Property	Value
`v2AllowHttp`	You can configure SAP Identity Management REST Interface v2 to use HTTP or HTTPS communication. • *false* - Allows HTTPS communication. This is the default value. → Recommendation For security reasons, it is recommended to you use HTTPS communication. For more information how to configure the Secure Sockets Layer (SSL) on your SAP NetWeaver AS Java, see Using the HTTP Security (Secure Sockets Layer/ SSL) • *true* - Allows HTTP communication.
`v2ReturnNullValuesInResponse`	Controls whether single value attributes for a specific entry with value `null` are returned in the response body. • *true* - Single value attributes for a specific entry with value `null` are returned in the response body. This is the default value. • *false* - Single value attributes for a specific entry with value `null` are not returned unless this attribute is listed for the entry type, since all listed attributes for the entry will be returned in the response body.

2.1.1.6 Installing the Identity Management Developer Studio

The SAP Identity Management Developer Studio client is available as an Eclipse plugin. You need to install the Identity Management Developer Studio client on every developer or developer administrator machine.

Prerequisites

- Make sure your 64-bit SAP JVM is version 8.1
- Eclipse version 2024-09 is required. We recommend you to choose the package *Eclipse IDE for Java Developers*.

Context

To install the Identity Management Developer Studio plugin, proceed with the following steps:

Procedure

1. In your Eclipse User Interface, select *Help* > *Install New Software...* from the main menu.
2. Specify the repository site where the plugin is available from. Choose *Add...* to the right of the *Work with* field.
3. In the *Add Repository* dialog box, enter a descriptive name (for example, SAP Identity Management Developer Studio) in the *Name* field. In the *Location* field, enter the URL the Identity Management Developer Studio plugin for Eclipse is available from. Enter the following URL:

   - `https://tools.hana.ondemand.com/2024-09/` for Eclipse 2024-09 (4.33)

   Choose *OK* to add the repository.
4. Select the defined repository from the list in the *Work with* field. The plugin for the SAP Identity Management Developer Studio appears in the list by opening the *SAP Identity Management Tools*.
5. Select *SAP Identity Management Developer Studio* checkbox and then choose *Next >*.

   The installer will calculate the dependencies and installation details for the software, and display these (if any).
6. Choose *Next >*.
7. Review the licenses and choose *I accept the terms of the license agreement*.
8. Choose *Finish*.
9. You will need to restart Eclipse for the changes to take effect. Choose *Yes* to restart immediately, or *No* to restart later.
10. In the main menu, select *Window* > *Perspective* > *Open Perspective* > *Other...* and select the perspective *SAP Identity Management*. Choose *OK* to open the perspective. If you need to reset the perspective to its default state, choose *Tools* > *Reset Perspective*.

2.1.1.7 Using the HTTP Security (Secure Sockets Layer/ SSL)

Security between the Identity Management Developer Studio service and client is done by securing the web server (your SAP NetWeaver AS for Java). Make sure to use HTTPS to secure the connection.

Prerequisites

To configure the use of Secure Sockets Layer (SSL) on your SAP NetWeaver AS for Java, you would need the following:

- Administrator rights for the SAP NetWeaver AS for Java server
- SAP Cryptographic Library installed (see *Installing the SAP Cryptographic Library for SSL* for your SAP NetWeaver AS for Java version for details)

Configuring the Use of SSL on SAP NetWeaver AS for Java

To configure the use of SSL on your SAP NetWeaver AS for Java, follow the descriptions of SSL configuration for your SAP NetWeaver version (see *Related Information*).

You can use the SSL configuration tool in the SAP NetWeaver Administrator to add a new SSL access point (port). See *Adding New SSL Access Points* for your SAP NetWeaver AS for Java version for details.

Following the processes for adding the SSL access point (port) on your SAP NetWeaver AS for Java, pay special attention to the following fields (and apply the values listed):

Name of the Field	Value/Comments
Protocol	Select *HTTPS* as the protocol for the new port.
Client Authentication Mode	Select the mode *Do Not Request*.
Keystore View Name	Select option *Instance Default*, to use the default server key pair and trusted CA certificates.

Upon creation of the new access point, the SSL configuration tool creates a keystore view for the specified port. If the default SAP NetWeaver AS for Java port for SSL communications (port 50001) is used, the corresponding keystore view will be *ICM_SSL_<instance_ID>*. If other port number is used for the SSL communications, the corresponding keystore view will be *ICM_SSL_<instance_ID>_<port>*. The created view contains the server key pair and trusted CA certificates to use for this port.

Exporting and Installing the SSL X.509 Certificate

In order for the secure SSL communications to work, the SSL server's (SAP NetWeaver AS Java's) certificate should be exported from the SAP NetWeaver Administrator and imported to the keystore used by the client

Identity Management Developer Studio. Modifying the client's keystore, you are making the client trust the server thus enabling secure communication.

For details on how to export and install the certificate, see *Exporting and Installing the SSL Certificate*.

Configuring the Identity Management Developer Studio for HTTPS Connection

When configuring connections and the application server configuration in the Identity Management Developer Studio client, make sure to provide the port number defined as the SSL access point in the SAP NetWeaver Administrator. For details see *Initial Configuration of the Identity Management Developer Studio*.

Related Information

Exporting and Installing the SSL Certificate [page 26]
Initial Configuration of Identity Management Developer Studio [page 27]
SAP NetWeaver 7.3
Configuring Transport Layer Security on SAP NetWeaver AS for Java
Installing the SAP Cryptographic Library for SSL
Adding New SSL Access Points
SAP NetWeaver 7.3 EHP1
Configuring Transport Layer Security on SAP NetWeaver AS for Java
Installing the SAP Cryptographic Library for SSL
Adding New SSL Access Points
SAP NetWeaver 7.4
Configuring Transport Layer Security on SAP NetWeaver AS for Java
Installing the SAP Cryptographic Library for SSL
Adding New SSL Access Points
SAP NetWeaver 7.5
Configuring Transport Layer Security on SAP NetWeaver AS for Java
Installing the SAP Cryptographic Library for SSL
Adding New SSL Access Points

2.1.1.7.1 Exporting and Installing the SSL Certificate

The SSL server's (SAP NetWeaver AS Java's) certificate should be exported from the SAP NetWeaver Administrator and imported to the keystore used by the client Identity Management Developer Studio. Modifying the client's keystore, you are making the client trust the server thus enabling secure communication.

Context

The certificate must be imported to the keystore of every Identity Management Developer Studio client that needs to be communicating securely with the server. To export and correctly install the SSL certificate, proceed with the following steps:

Procedure

1. Start the SSL configuration tool in the SAP NetWeaver Administrator by following the path *Configuration Management* > *Security* > *SSL*.
2. Select the added SSL access point (port) in the *SSL Access Points* section. The details of the selected port will be displayed.
3. From the *Server Identity* tab for the SSL port, select the private key entry and choose *Export Entry* to export the server's certificate directly from its private key entry.
4. In the *Export Entry to File* dialog box, select export format *PKCS#8 Key Pair*.

   Two files will be produced, a PKCS#8 key pair file and an X.509 certificate file (for example `ssl-credentials-cert1.crt`). Download the certificate file and store it in the same directory as the client keystore (i.e. the `cacerts` file of the Identity Management Developer Studio). The location of the keystore (the `cacerts` file) depends on the location of your Java Virtual Machine, by default `<JAVA_HOME>\jre\lib\security\cacerts`.

   > **Note**
   >
   > A way to locate the <JAVA_HOME> path for the Java your Identity Management Developer Studio is using, is described in the following Eclipse documentation: Find the JVM .

5. Now that the certificate is downloaded, import it to client's keystore `cacerts` by using the keytool utility. In a command prompt, navigate to the directory `<JAVA_HOME>\jre\lib\security\` and use the following command: `keytool -import -alias <local certificate name> -file <certificate file> -keystore cacerts`. For example: `keytool -import -alias my_ssl_cert -file ssl-credentials-cert1.crt -keystore cacerts`.

   > **Note**
   >
   > Make sure you are able to access the keytool utility from the above mentioned directory. The utility is by default located in `<JAVA_HOME>\bin\` directory.

You will be asked to provide a keystore password. The initial password of the `cacerts` keystore is *changeit*. System administrators should change the password and the default access permissions of that file after installing the SDK.

You are asked if you trust the certificate you are about to import. Type **y** and press `Enter` and the certificate will be added to the client keystore `cacerts`.

2.1.1.8 Initial Configuration of Identity Management Developer Studio

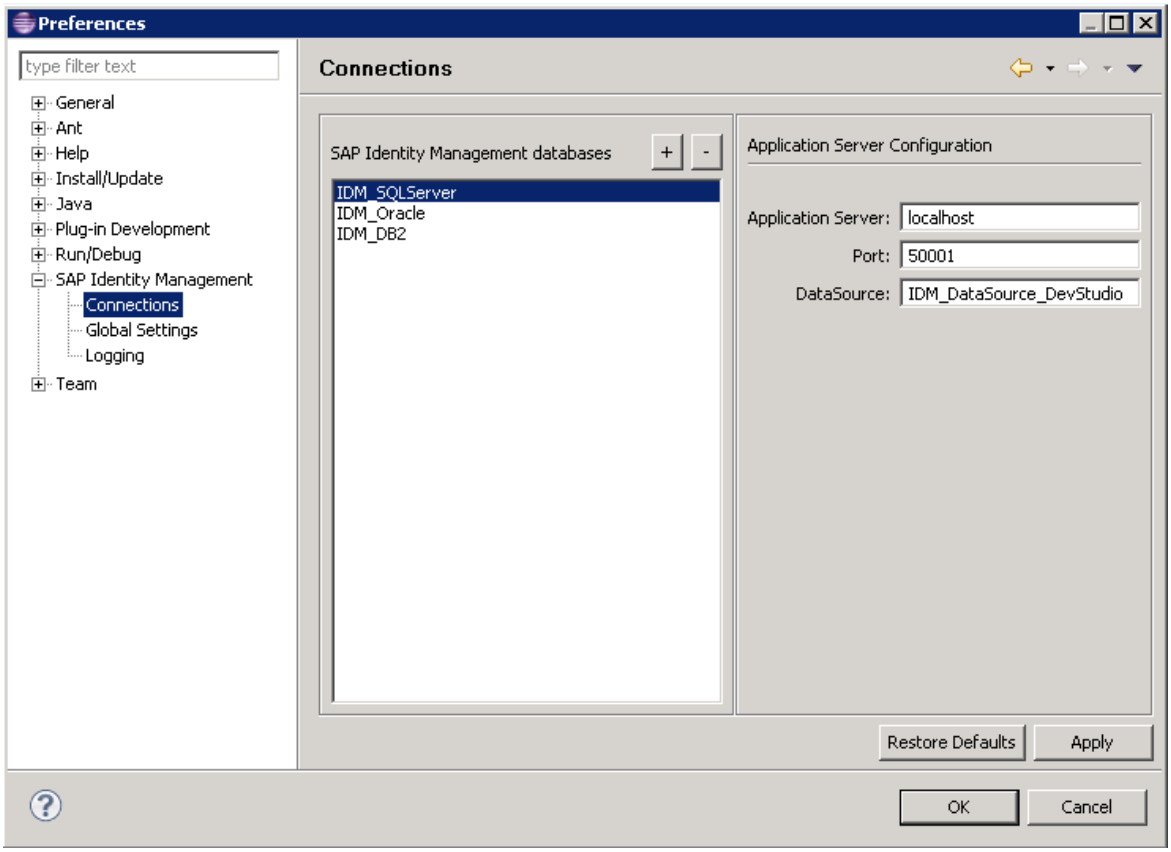
Once the SAP Identity Management Developer Studio plugin is installed in your Eclipse environment and the perspective is opened, you would need some initial configuration in order to access the Identity Management database and the identity store(s).

Context

To initially configure the Identity Management Developer Studio, proceed with the following steps:

Procedure

1. From the main menu, select:
   - For Windows and Linux, *Window* > *Preferences*.
   - For Mac OS X, *Eclipse IDE for Lean DI Developers* > *Preferences*.
2. Expand *SAP Identity Management* and select *Connections* in the menu on the left.
3. Add a connection to the Identity Management database by choosing +, then enter a name and optionally a description for the connection.
4. Choose *OK* to add the connection to the list.
5. Enter the details in the *Application Server Configuration* section:



Fill in the following fields:

Option	Description
Application Server	Enter the IP address or the name of the application server (e.g. localhost or 10.66.185.255).
Port	When you have configured the use of SSL (HTTPS) on your SAP NetWeaver Application Server Java, make sure to here provide the SSL (HTTPS) port number. **Note** If you are running through proxy, define the SSL (HTTPS) port as an allowed port. For more details see, Using the HTTP Security (Secure Sockets Layer/SSL) [page 24] and Exporting and Installing the SSL Certificate [page 26].
DataSource	Enter the name of the created data source for your Identity Management database. The name of the data source should be the same as the one you have configured in SAP NetWeaver Administrator under *Configuration* > *Infrastructure* > *Application Resources*. For example, **`IDM_DataSource_DevStudio`**.

6. Choose *Apply* and then *OK* to close the dialog box.
7. Select the *Root* node in the tree view. Select *Refresh* from the context menu, and then expand the node.
8. Expand the node for the Identity Management database in the tree view. Provide the credentials for the initial administrator user for Identity Management Developer Studio to login.

> **Note**
>
> The initial administrator user for Identity Management Developer Studio is created when creating/ updating to the Identity Management 8.0 database. To be able to login and access the Identity Management database in your Identity Management Developer Studio client, you must make sure that this user also exists in the User Management Engine (UME) and is assigned the `idm_authenticated_studio` UME action. See *Creating the Developer Administrator User in UME* and *Assigning idm_authenticated_studio UME action* for details.

> **Note**
>
> If you are experiencing any issues with displaying the characters in your Identity Management Developer Studio, you should use the Java System Properties tool for your SAP NetWeaver version to specify the UTF-8 encoding for your system (add a JVM parameter on your instance). For more information see *Configuring the Java System Properties*.

> **Note**
>
> If you are experiencing issues with the data discovery in your Identity Management Developer Studio, due to the connection string not being correctly defined or not defined at all, you encounter the following error message: `JDBC_URL global variable is not configured properly. Please use dispatcher utility to do that.`. For details on how to define the connection string correctly see *Defining the Settings for the Identity Management Dispatcher Utility*.

Next Steps

Once the Identity Management database in your Identity Management Developer Studio client is accessed, and its node in the tree view expanded, you need to create an identity store for your data. For details, see *Adding the Initial Identity Store*.

Related Information

Creating the Developer Administrator User in UME [page 30]
Assigning idm_authenticated_studio UME action [page 31]
Configuring the Java System Properties [page 19]
Adding the Initial Identity Store [page 31]

2.1.1.8.1 Creating the Developer Administrator User in UME

The initial administrator user for Identity Management Developer Studio needs to exist both in the database and in the User Management Engine (UME), in order to be able to log on to the Identity Management Developer Studio.

This means that you need to manually create the initial administrator user for Identity Management Developer Studio in the UME, with a corresponding password. In addition, the user also needs the `idm_authenticated_studio` UME action assigned to it through a UME role. You can use the `idm.developer` role, as it already contains this action.

> **Note**
>
> The user must be named the same in both the database and the UME.

Create the user as a technical user, using the description for your SAP NetWeaver version:

SAP NetWeaver Version	Description
SAP NetWeaver 7.3	For details on how to create the user in the UME, see Creating a Technical User
SAP NetWeaver 7.3 EHP1	For details on how to create the user in the UME, see Creating a Technical User.
SAP NetWeaver 7.4	For details on how to create the user in the UME, see Creating a Technical User.
SAP NetWeaver 7.5	For details on how to create the user in the UME, see Creating a Technical User

Related Information

Assigning idm_authenticated_studio UME action [page 31]

2.1.1.8.2 Assigning idm_authenticated_studio UME action

To log on to SAP Identity Management Developer Studio, the user must be added to the UME. In addition, the user needs the `idm_authenticated_studio` UME action that can be assigned to the user through a UME role.

Context

To assign the `idm_authenticated_studio` UME action to a user, proceed as follows:

Procedure

1. Log on to SAP NetWeaver Administrator at `http(s)://<host>:<port>/nwa` and navigate to *Configuration* > *Identity Management*.
2. In *Identity Management: Overview*, search for the user. On the *Assigned Roles* tab page assign the `idm.developer` role to this user. This role already contains the `idm_authenticated_studio` action.

   You can also assign the `idm_authenticated_studio` action to another role of your choice or use the `Administrator` role, which also contains this action.
3. Choose *Save*.

Results

All the users with assigned `idm_authenticated_studio` UME action are now able to log on to the Identity Management Developer Studio.

2.1.1.8.3 Adding the Initial Identity Store

The first time you are accessing the Identity Management Developer Studio and the Identity Management database, there will be no identity store. The only exception to this is when you upgrade your entire existing system from version 7.2 to 8.0. In this case, every identity store from your 7.2 system is migrated into your 8.0 system. The identity store contains its own default package that must be expanded.

You need to add an identity store. You have the following options:

- Create a new identity store. For more information, see Adding an Identity Store.
  Once the identity store is created, you can continue with importing the configuration packages from the directory where you have unpacked the Core component. For more information, see Unpacking the Core Component

- Import an already existing identity store(s) into your Identity Management Developer Studio. This is only relevant for an upgrade scenario when you install SAP Identity Management 8.0 as a side box and move the configuration and data from your 7.2 system. Only identity stores from a 7.2 system can be exported and then imported into the Identity Management Developer Studio.
  To import an existing identity store, select the Identity Management database node in the tree view and choose *Import...* from the context menu.

2.1.2 Post-Upgrade Results

After the upgrade, you get the following results:

Default Package of the Upgraded System

All 7.2 configurations are migrated into one package - the default package of the upgraded system.

You can have more than one package in the Identity Management Developer Studio, because every migrated identity store from your 7.2 system contains its own default package in 8.0. This means that if you have two identity stores in 7.2, you will again have two identity stores in 8.0, each of them containing its own default package where the 7.2 configuration is migrated. Each default package must be expanded separately.

Repository Types

Repository types are automatically created. They define common parameters for one type of repository.

Tasks

Tasks are split into processes and forms.

- Processes
  Public tasks or top tasks of task groups are transformed into processes.
  Tasks that are referenced by other tasks in 7.2 are transformed into processes.
  After the upgrade, the process type is set to its default value *Regular*. The process continues to work as in the 7.2 system. You can use the regular process in different events (validation, execution or notification) or reference this process from another process or form (on the *Result Handling* tab). Additionally, you can choose a proper process type for your process. For more information about the process types, see General (Process).
  Event processes are defined on the repository type. They are common for all repositories of that type.
- Forms
  Web enabled tasks (UI tasks) are now forms.
  If a UI task contains one or more tasks, after the upgrade the following takes place: The UI task becomes a form. A process with the same name as the form is created. This process contains all the child tasks of the UI task. The form references the process.
  Unspecified UI tasks become regular forms. Note that you can use regular forms to search or display details about entries of entry types (that is, to add *Regular* forms in the *Display Form* and *Search Form* fields on the *General* tab of an entry type) only if you enable *Show Backwards Compatibility Settings*. You do this in SAP Identity Management Developer Studio. In the main menu, choose *Window* > *Preferences* > *SAP Identity Management* > *Global Settings* > *Show Backwards Compatibility Settings*.

To copy a form or a process from one identity store to another, you need to export the package containing that form or process and import it to the identity store you want.

Jobs

Jobs are now located in the identity store. (In 7.2 jobs are located in a *Job* folder outside the identity store.)

Only jobs that have a repository defined for them on the *Options* tab are transformed into repository jobs. All other jobs (although they may contain passes with defined repositories) are transformed into regular jobs.

> **Note**
>
> It is not possible to change the repository type of an existing repository job. In case you need to this, your only option is to create a new repository job and then copy all the passes from the old job to the new repository job.

After completing the upgrade, you can run the initial load job only in the SAP Identity Management Developer Studio. To run any repository job in the SAP Identity Management Administration User Interface, create a repository type constant of data type *Job Reference* and select the repository job to be the value of the repository type constant.

Global Constants

Global constants are now transformed into package constants. They are located in the default package.

When expanding the default package for the first time, global constants are transported from `mc_global_variables` to `mc_package_variables` database table, except for those starting with **`MX_`** and those used internally. After upgrade, they are still stored in `mc_global_variables` table.

Constants that are not starting with **`MX_`** and that are not used internally are moved to the default package of the identity store. If there are more than one identity stores, they are also copied to the default package of each identity store.

In version 8.0, the option to manage global constants in the Identity Management Administration User Interface under *System Parameters* > *Global Constants* is replaced by *System Configuration* > *Packages* > *Constants* where the same functionality is available for package constants.

For more information, see: Package Constants and Modifying Package Constants.

> **Note**
>
> The old *%GLB.* prefix will continue to work. However, warnings are added to the job log. We recommend that you replace any references to the new *%PCK.* prefix.

Global Scripts

Global scripts are now transformed into package scripts. They are located in the default package.

> **Note**
>
> The old *%GLB.* prefix will continue to work. However, warnings are added to the job log. We recommend that you replace any references to the new *%PCK.* prefix.

Variables

Repository variables are available only from scripts. In 8.0, the variables are visible only in the `mc_repository_vars` table in the database.

Global variables are available only from scripts using uSetGlobalVar and uGetGlobalVar functions.

Hook Tasks

There are no hook task repository constants in version 8.0. The plug-in processes of a repository are now referenced by repository type constants that are defined on the repository type. However, when upgrading from version 7.2 to 8.0, hook task repository constants are transformed into repository type constants with override and can be edited in the SAP Identity Management Administration User Interface.

Reverse Privilege Inheritance

Reverse privilege inheritance (that is, a privilege can be inherited top-down (reverse) in a role hierarchy) is no longer supported in version 8.0. If you use reverse privilege inheritance in version 7.2 and you upgrade to version 8.0, you need to change the value of the MX_REVERSE_PRIVILEGE global constant to FALSE by using scripts in SAP Identity Management Developer Studio.

SAP Identity Management User Interface

SAP Identity Management User Interface took over the management of business roles, privileges, dynamic groups and repositories from the Identity Center Management Console that is now replaced by SAP Identity Management Developer Studio.

Roles, Privileges, Dynamic Groups

Identity store entries, such as business roles, privileges and dynamic groups are now managed by forms in SAP Identity Management User Interface. You can create, modify and delete them in the SAP Identity Management User Interface, as well as define member event processes for roles and privileges and configure contexts and assignments. For more information, see Maintaining Identity Store Entries.

SYSTEM privilege

The SYSTEM privilege and its properties are no longer visible along with all available privileges, as in version 7.2. It is only visible as a read-only repository constant in the SAP Identity Management Administration User Interface. If you want to manage the trigger attributes for the SYSTEM privilege, you can do this by jobs and scripts only (set the value of the MX_MODIFYTASK_ATTR attribute of the SYSTEM privilege).

Repositories

Repositories are now managed in SAP Identity Management Administration User Interface, where you can create, copy, import, export, enable, disable, delete and change the repository type of the repositories. For more information, see Maintaining Repositories.

SAP Provisioning Framework

SAP Provisioning Framework from 7.2 is also part of the default package and will continue to work.

> **Note**
>
> Using the old provisioning framework has clear disadvantages. You cannot get support for it, as it is part of version 7.2 which is out of mainstream maintenance. Furthermore, you cannot benefit from new features, improvements and bug fixes delivered with the new provisioning framework.

> **Note**
>
> If you want to use the new packaged provisioning framework that comes with version 8.0, you have to import the provisioning framework packages explicitly and adapt your configuration to use them.

To edit the package in order to work on its configurations, you need to first check out this package. By default, only one user can check out a package and work on its configuration. If explicitly required, you can change this so that multiple users to check out the same package. See Configuring the Java System Properties [page 19].

Allowing multiple users to check out the same package is suitable for systems that are upgraded from version 7.2. In this case, all configurations are placed into one default package that needs to be restructured manually into multiple packages.

The same login is not allowed from two clients.

Manual restructuring into multiple packages can start. Restructuring logic is customer-specific and use case-specific.

Execution is as before.

2.1.3 Upgrading QA and PROD Systems

Context

Although you can choose a different upgrade strategy for your QA and PROD systems, we recommend you use the same one as for the DEV system.

Procedure

1. Once your configuration is migrated to the new package, do the package restructuring in your DEV system.
2. Transport all packages to the QA and PROD systems.

   If your QA and PROD configuration differs from the DEV configuration for any reason, first apply the changes in the DEV system and then do the transport.

2.2 Installing SAP Identity Management 8.0 and Importing Existing Configuration and Data

To upgrade from Identity Management 7.2 to 8.0, you can install SAP Identity Management 8.0 as a side box, move the configuration and data from your 7.2 system and retire the old system.

Prerequisites

> ⚠ Caution
>
> To move data from 7.2 to 8.0 system, customers need to implement their own solutions. This guide covers only importing users and privileges and provides an example for importing roles. Moving data, such as dynamic groups, historic and future values, audit information, logs and others, is subject to customers' implementation.

To execute a successful SAP Identity Management upgrade, you need to fulfill the following prerequisites:

- You are running 7.2 SP09 at least (preferably 7.2 SP10).

  > ⓘ Note
  >
  > If you are currently running a lower 7.2 SP, you need to update to 7.2 SP09 at least (preferably 7.2 SP10), without running live on 7.2 SP09 or SP10.

- You have installed all underlying components to the currently supported ones - check the Product Availability Matrix (PAM). For example, first upgrade SAP NetWeaver to 7.3 SP09 or higher.
- SAP Identity Management 8.0 supports only SAP JVM. You should use SAP JVM, where version 8.1 (Java 1.8) is required for the runtime components and the Virtual Directory Server. For information about how to download the SAP JVM, see SAP Note 1442124
  All SAP Identity Management components deployed on SAP NetWeaver AS for Java can run with SAP JVM version 6.1 (Java 1.6).

> ⓘ Note
>
> Although terminology has changed in SAP Identity Management 8.0, content has been kept stable. For example, a UI task has been renamed to a Form, but its content does not need to be changed.

Context

This upgrade strategy consists of the following steps, which should be executed in the given sequence:

Procedure

1. Install SAP Identity Management 8.0 as a side box. See
   - SAP Identity Management Installation and Update Guide on Windows
   - SAP Identity Management Installation and Update Guide on UNIX
2. After the installation has finished successfully, do not forget to copy the Keys.ini file of version 7.2 (containing the old encryption key) to the following locations:
   - On the database host: `/usr/sap/<SID>/SYS/global/security/data/Key/Keys.ini`
   - On every host where Runtime instance is created: `/usr/sap/<SAPSID>/IDM<Instance_Number>/Identity_Center/Key/Keys.ini`
   - Set the reference to the Keys.ini file where it is needed (the JMX parameter `com.sap.idm.jmx.crypt.keyfile` and the Java system property `com.sap.idm.rcp.crypt.keyfile`, for example). The path to the Keys.ini file should point to: `\\<host>\sapmnt\<SAPSID>\SYS\global\security\data\Key\Keys.ini`, where <SAPSID> is the SAP system ID of SAP Identity Management system.

   Finally, you need to regenerate the dispatcher scripts. Start the Dispatcher Utility and choose *Dispatcher* > *Regenerate Scripts*.

   For information about distributing and activating new key(s), see SAP Identity Management Security Guide
3. Import the identity stores from your 7.2 system. See Importing Identity Stores [page 38]
4. Import the repositories from your 7.2 system. See Importing Repositories [page 39]
5. Import the single jobs from your 7.2 system. See Importing Single Jobs and Job Folders [page 40]
6. Import the job folders from your 7.2 system. See Importing Single Jobs and Job Folders [page 40]

   > **Note**
   >
   > Tasks from 7.2 are imported into 8.0 with the identity store. Importing only tasks is not supported.

   Note that if you plan to run SAP Identity Management 8.0 on SAP ASE, after the installation of SAP ASE, you have to adjust the scripts imported with the 7.2 configuration that are directly communicating to the database via SQL statements. For example, you can check how this was done in the *sap_core_getMaxChangeNumber* script in the *com.sap.idm.provisioning.engine* package of the Provisioning Framework for SAP Identity Management 8.0. All new scripts imported with the Provisioning Framework for SAP Identity Management 8.0 are already updated.
7. Import the data from your 7.2 system. See Importing the Data [page 42]
8. Retire your 7.2 system.

Results

The SAP Identity Management system is up and running with the old content and can be made live.

If the upgrade fails, check the logs described in *Identity Management: Error When Upgrading from 7.2 to 8.0* in the *Troubleshooting* section of *SAP Identity Management Solution Operation Guide*.

Related Information

SAP Identity Management Security Guide
Product Availability Matrix
Troubleshooting

2.2.1 Importing Identity Stores

You can import identity stores from your 7.2 system into the Identity Management 8.0 database using the Identity Management Developer Studio.

Prerequisites

- You have exported the identity store from your 7.2 system as `.mcc` file.
- You have created a default dispatcher. The default dispatcher is assigned to the imported jobs and is started.

Context

To import an identity store, proceed as follows:

Procedure

1. In the Identity Management Developer Studio tree view, select the *Identity Management database* node.
2. Choose *Import...* from the context menu.
3. Select the exported `.mcc` file and choose *Open*.
4. In the *Identity Store File (.mcc) Information* dialog box, (optionally) enter a reason for the import and choose *OK*.

> **Note**
>
> How long the import will take to complete depends on the size of the import file.

Results

The identity store is imported with the same name, and the corresponding node is added to the tree view. The imported identity store contains the identity store schema of your 7.2 system and a default package. The 7.2 configuration is put into that default package.

For more information, see Post-Upgrade Results [page 32].

After the import of the identity store, also note the following:

- If some jobs or tasks are missing after the import of the identity store, then the respective repository or package constants will get value -1 (meaning the job or task is not referenced by any repository or package constant). You will get a warning pop-up message guiding you how to proceed.
- All translated texts (this includes translations of entry types/attributes and also any translations of task names and other objects with translatable names) are available too.
- The logged-in user in the Identity Management Developer Studio automatically becomes an admin user with access to manager/administrator tabs in the Identity Management User Interface.

2.2.2 Importing Repositories

You can import repositories from your 7.2 system into the Identity Management 8.0 database using the Identity Management Developer Studio.

Prerequisites

- You have exported the repositories from your 7.2 system as `.mcc` file.
- You have imported the identity store from your 7.2 system.
- You have checked out the default package.

Context

To import repositories, proceed as follows:

Procedure

1. In the Identity Management Developer Studio tree view, select the default package in the imported identity store from your 7.2 system.
2. Choose *Import...* from the context menu.
3. Select the exported `.mcc` file and choose *Open*.
4. In the *Repository Configuration File (.mcc) Information* dialog box, (optionally) enter a reason for the import and choose *OK*.

Results

The repositories are imported and visible in the Identity Management Administration User Interface. The repository types of the imported repositories are created automatically. The repository constants are imported as repository type constants with override.

For more information, see Post-Upgrade Results [page 32].

After the import of the repositories, also note the following:

- Tasks that are imported with the identity store are referenced by the respective repository constants. If some tasks are missing, then the respective repository constants will get value -1 (meaning the task is not referenced by any repository constant). You will get a warning pop-up message guiding you how to proceed.
- If the imported 7.2 repositories already exist due to previous import, their repository constants are overwritten.

2.2.3 Importing Single Jobs and Job Folders

You can import single jobs or job folders from your 7.2 system into the Identity Management 8.0 database using the Identity Management Developer Studio.

Prerequisites

- You have exported a single job and/or job folder from your 7.2 system as `.mcc` file.
- You have imported the identity store and repositories from your 7.2 system.

- You have checked out the default package.

Context

> **Note**
>
> We recommend that you import the single job before the job folder. In this case, the single job is imported in the *Jobs* folder of the default package. If you import a single job after importing a job folder, the single job is imported in a random job folder.

To import a single job and/or a job folder, proceed as follows:

Procedure

1. In the Identity Management Developer Studio tree view, select the default package in the imported identity store from your 7.2 system.
2. Choose *Import...* from the context menu.
3. Select the exported `.mcc` file and choose *Open*.
4. In the *Job Configuration File (.mcc) Information* dialog box, (optionally) enter a reason for the import and choose *OK*.

   > **Note**
   >
   > In SAP Identity Management 8.0, jobs are stored and run within an identity store in the SAP Identity Management Developer Studio. To run any repository job in the SAP Identity Management Administration User Interface, create a repository type constant of data type *Job Reference* and select the repository job to be the value of the repository type constant.

Results

- The single job is imported and visible in the *Jobs* folder of the default package.
  The single job is imported with all added passes and its job definition (i.e. scheduling rules, repository references (if any) and others).

  > **Note**
  >
  > Only predefinded scheduling rules are imported with the jobs. If you have defined your own scheduling rules for the jobs in version 7.2, these rules will not be imported with the jobs in version 8.0.

- Jobs with repository references in version 7.2 are transformed into repository jobs.
  - If a repository is referenced by a job or its passes, this repository is created and the job can run with it. If the imported 7.2 repository already exists due to previous import, its repository constants are overwritten.

- If in version 7.2 you have a job connected to one or more repositories of the same repository type, in version 8.0 there will be a separate job for each repository sharing the same job definition of the main job. After successful import of 7.2 configuration, some jobs with repository references might not be visible in the SAP Identity Management Developer Studio. All missing jobs will be automatically created when the repository job is executed against the corresponding repositories.
- > ⓘ Note
  >
  > It is not possible to change the repository type of an existing repository job. In case you need to this, your only option is to create a new repository job and then copy all the passes from the old job to the new repository job.

- The imported job folder is visible in the default package.
- The job folder is imported with all its subfolders (if any) and all single jobs.
- The default dispatcher is assigned to the imported jobs.

2.2.4 Importing the Data

Prerequisites

- You have installed SAP Identity Management 8.0 as a side box. See SAP Identity Management Installation and Update Guide
- You have imported the configuration from your 7.2 system. See
  - Importing Identity Stores [page 38]
  - Importing Repositories [page 39]
  - Importing Single Jobs and Job Folders [page 40]

Context

Once you have imported the configuration from your 7.2 system (identity stores, repositories and jobs), you need to import the data.

To import users and privileges, you need to run the initial load job for every repository you have in your 8.0 system. To retrieve other data (such as roles, dynamic groups, historic and future values, audit information, logs and others) customers need to implement their own solutions. This guide covers an example for retrieving roles.

Procedure

1. Run the initial load jobs to retrieve users and privileges from the connected systems.

   > **Note**
   >
   > Be aware that the initial load jobs retrieve all user privileges as direct assignments. This means that indirect privileges that are assigned to a user through a role in version 7.2 are retrieved as direct assignments. When proceeding with steps 2 and 3 to export and import roles, you must think of your own solution to correct direct and indirect assignment inconsistencies.

2. Retrieve data from your 7.2 system. The following gives an example how to create jobs to export and import roles. You can create similar jobs to export and import other data (such as dynamic groups, historic and future values, audit information, logs and others).

Example

1. In the Identity Center Management Console of your 7.2 system, create a job to export business roles in a `.csv` file.
   If you are using SAP Identity Management Rapid Deployment Solution (RDS) in version 7.2, you can run the job SAPC Export Business Roles to export business roles in a `.csv` file and skip the next sub-steps.
   1. Create an empty job and add a `To ASCII file` pass to the job.
   2. Enter the definition of the pass on the *Destination* tab. Enter the attributes holding information about the business roles, such as the MSKEYVALUE, the entry reference attributes (starting with MXMEMBER and MXREF) and the attributes' value.
   3. Run the job.
2. In the SAP Identity Management Developer Studio of your 8.0 system, create a job to import business roles from a `.csv` file.
   1. Create a regular job and add two passes to it: `From ASCII file` pass and To Identity Store pass.
   2. Enter the definition of the two passes on the *Destination* tab.
   3. Run the job.

The imported roles are linked automatically to their child privileges.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2025 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP