Installation Guide | PUBLIC
Document Version: 1.10 – 2026-05-28

SAP Identity Management Installation and Update Guide on Windows

Using Software Provisioning Manager 1.0

Content

1 SAP Identity Management Installation and Update Guide on Windows. 4

2 Installing SAP Identity Management. 5

2.1 Installation Checklist. 6

2.2 Planning SAP Identity Management Installation. 7

Installation Overview. 8

Installation Options. 10

Hardware and Software Requirements. 14

Installation Parameters. 33

SAP Identity Management System Directories. 41

2.3 Preparing for SAP Identity Management Installation. 44

Performing Basic Windows Preparation Steps. 44

Required User Authorization for Running Software Provisioning Manager. 46

Performing a Domain Installation Without Being a Domain Administrator. 48

Creating Users and Accounts on Windows. 49

Preparing the Installation Media. 51

2.4 Installing SAP Identity Management. 56

Prerequisites for Running Software Provisioning Manager. 57

Running Software Provisioning Manager. 58

Additional Information About Software Provisioning Manager. 61

Installing the Identity Management Developer Studio. 70

2.5 Post-Installation Tasks. 71

Post-Installation Checklist. 71

Unpacking the Core Component. 73

Identity Management Database on Microsoft SQL Server. 74

Identity Management Database on Oracle. 88

Identity Management Database on IBM DB2. 94

Identity Management Database on SAP ASE. 99

Creating Encryption Keys. 110

Creating and Configuring Dispatchers. 115

Using the SAP Java Connector (JCo). 126

Defining the JDBC Connection for Identity Management Developer Studio Service. 127

Configuring the Java System Properties. 131

Using the HTTP Security (Secure Sockets Layer/SSL). 134

Initial Configuration of Identity Management Developer Studio. 137

Defining the JDBC Connection for the JMX Layer. 142

Configuring the JMX Layer. 147

Initial Configuration of Identity Management User Interface. 154
Defining Customer Specific Themes for Web Dynpro Applications. 171
Keyboard Access for User Interface Elements in Web Dynpro. 172
Integrating Identity Management User Interface in the SAP Enterprise Portal (optional). 172
Initial Configuration of Identity Management User Interface for HTML5. 175
Starting the Virtual Directory Server. 184
Initial Configuration of Identity Management Virtual Directory Server. 185
2.6 Starting and Stopping SAP Identity Management. 194

3 Updating SAP Identity Management. 196
3.1 Updating SAP Identity Management with Software Provisioning Manager 1.0. 196
3.2 Updating SAP Identity Management Components. 199
Updating SAP Identity Management Core. 200
Updating Runtime Components. 211
Updating Identity Management Developer Studio Service. 220
Updating Identity Management Developer Studio. 230
Updating the Virtual Directory Server. 232
Updating Identity Management User Interface. 235
Updating the REST Interface Version 2. 241
Updating the Identity Management User Interface for HTML5. 248
Updating IDM Connector for UWL. 254
Downloading and Installing the Federation Software. 256

1 SAP Identity Management Installation and Update Guide on Windows

This guide describes how to install and update SAP Identity Management 8.0 on Windows.

2 Installing SAP Identity Management

This section describes how to install SAP Identity Management 8.0.

As of version 8.0 SP04 and higher, you install SAP Identity Management using the Software Provisioning Manager 1.0 installation tool. You can use the Software Provisioning Manager 1.0 tool to install all SAP Identity Management components, except for SAP Identity Management Developer Studio client, SAP Identity Management Logon Help and SAP Identity Management Password Hook. The installation procedure for those three components has not changed, that is, they must be installed manually.

About Software Provisioning Manager

Software Provisioning Manager 1.0 is the successor of the product- and release-specific delivery of provisioning tools, such as SAPinst. Before you run it, we recommend that you always download the latest version of Software Provisioning Manager 1.0. Software Provisioning Manager 1.0 is part of the Software Logistics Toolset 1.0 (“SL Toolset” for short). This way, you automatically get the latest fixes and supported processes. As a result, “SAPinst” has been renamed to “Software Provisioning Manager 1.0” in this documentation. However, the term “SAPinst” is still used in:

- Texts and screen elements in the Software Provisioning Manager GUI
- Naming of executables, for example `sapinst.exe`

Important SAP Notes

Read the following SAP Notes before you start the installation.

These SAP Notes contain the most recent information about installation, as well as corrections to the installation documentation. Make sure that you have the up-to-date version of each SAP Note, which you can find at http://support.sap.com/notes.

SAP Notes for the Installation

SAP Note Number	Title	Description
2036858	SAP Identity Management 8.0	This note is a central entry point for all information and notes relating to SAP Identity Management 8.0.
2296259	Inst.SAP Identity Management 8.0 SP04 and higher using Software Provisioning Manager	This note provides information about installation and update of SAP Identity Management 8.0 SP04 and higher using Software Provisioning Manager.

SAP Note Number	Title	Description
1680045	Release Note for Software Provisioning Manager 1.0	This note provides information about Software Provisioning Manager as well as products and releases supported by it.

Related Information

Installation Overview [page 8]
Installation Checklist [page 6]

2.1 Installation Checklist

This section describes how you install SAP Identity Management step by step.

Planning

1. Plan your SAP Identity Management system installation according to the Master Guide at http://help.sap.com/nwidm80 *Installation and Upgrade Information*. Familiarize yourself with the following documentation:
   - Software Components of SAP Identity Management
   - Overall Implementation Sequence
   - Installation Overview [page 8]
2. Decide whether you want to install your SAP Identity Management system with all instances on one host or with the instances distributed over several hosts. For more information, see Installation Options [page 10]
3. Check the hardware and software requirements for each installation host:
   - Requirements on Windows [page 16]
4. Install the database software for SAP Identity Management system. For more information, see Supported Database Systems (Overview) [page 17]
5. Install the JDBC driver for the corresponding database. For more information, see Installing the JDBC Drivers [page 22]
6. To deploy SAP Identity Management components on SAP NetWeaver AS Java, make sure that an SAP Java system based on SAP NetWeaver 7.3 or higher is available in your system landscape.
   Familiarize yourself with the dependencies between SAP Identity Management deployable components. For more information, see Prerequisites and Dependencies Between Deployable Components [page 25]
7. Plan and prepare installation parameters before you start the installation. For more information, see Installation Parameters [page 33].

8. Check the requirements for the SAP Identity Management System Directories [page 41].

Preparation

1. Do the required preparations for your operating system platform as described in the relevant sections:
   - Ensure that you have the required authorizations for running Software Provisioning Manager [page 46]
   - Perform the required steps if you want to perform a domain installation without being a domain administrator [page 48].
   - Make yourself familiar how users and accounts are created [page 49] during the installation.
2. You prepare the installation media [page 51]

Installation

1. You run the installation for the required system variant:
   - **Standard System**
     You run Software Provisioning Manager [page 58] to install an SAP Identity Management system with all components on one host.
   - **Distributed System**
     1. You run Software Provisioning Manager [page 58] to install the SAP Identity Management Core Components on the host where you want to have them running.
     2. You run Software Provisioning Manager [page 58] to install additional SAP Identity Management Dispatcher instances on the hosts where you want to have them running.
     3. You run Software Provisioning Manager [page 58] to install the Virtual Directory Server on the host where you want to have it running.
     4. You run Software Provisioning Manager [page 58] to deploy additional SAP Identity Management components on SAP NetWeaver AS Java.
2. You install the SAP Identity Management Developer Studio client. See Installing the Identity Management Developer Studio [page 70]

Post-Installation

1. You perform post-installation tasks [page 71].

2.2 Planning SAP Identity Management Installation

This section describes the planning phase of SAP Identity Management installation.

Related Information

Hardware and Software Requirements [page 14]
Installation Parameters [page 33]
SAP Identity Management System Directories [page 41]

2.2.1 Installation Overview

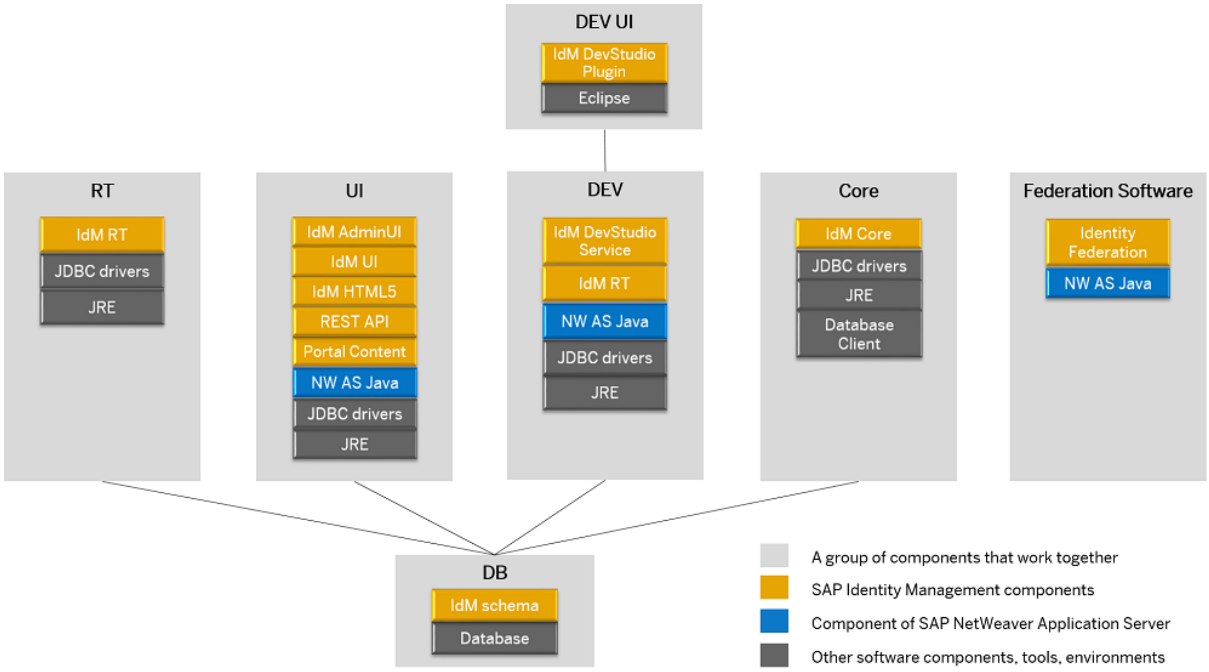
SAP Identity Management 8.0 consists of several components. Some of the components run on SAP NetWeaver AS Java, for example, the Identity Management user interface. Other components are stand-alone and are installed separately.

The software components can be installed on the same server or on several servers, depending on the requirements and purpose of the installation. For a smaller development environment, all components could be installed on the same server. In a production environment, the components are normally divided between several servers prepared for high availability and high performance:

- The database server must be clustered to ensure high availability of the data. For more information, see High Availability
- The servers with SAP NetWeaver AS Java for the Identity Management user interface must be clustered, to ensure high availability. Load balancing is handled by SAP NetWeaver AS Java.
- The servers with the runtime components are duplicated by setting up two or more servers with identical configurations. This will ensure high availability and load sharing of the processing. The runtime components can also be distributed to the servers with SAP NetWeaver AS Java.

> **Note**
>
> The Identity Management Runtime Components is usually installed on several servers when using the SAP Identity Management. For data discovery purposes, the Identity Management Runtime Components must also be installed on the same server as where the Identity Management Developer Studio service is installed.

Data discovery refers to the ability to configure From/To passes more easily by analyzing the source/target data source. This functionality allows the system to discover source/target system attributes related to the current pass. For example, if you have a `FromASCII` pass and you are reading a `CSV` file with 5 columns, choosing *Insert Template* > *Data Source Template* (on the *Destination* tab of the pass) will fetch the file, identify the 5 columns and insert them as pass attributes.
To do this, SAP Identity Management relies on the existing connector implementations (`FromASCII`, `FromLDAP` and others) which are part of the Runtime component. To use the data discovery functionality, you need to install said Runtime components in a place accessible by the SAP NetWeaver AS Java hosting the Identity Management Developer Studio service which needs to use them. Typically, installation is done on the same server.
It is a valid approach to have this installed on the Development landscape where pass configuration is done, and not on the Productive landscape where pass configuration is only transported, not modified.



SAP Identity Management Components

This table explains the mapping between the software component name and the technical component name.

Software Component	Technical Component
SAP Identity Management Developer Studio (in short, IdM DevStudio plugin)	IDM_CLM_ECLIPSE
SAP Identity Management Developer Studio Service (in short, IdM DevStudio service)	IDM_CLM_REST_API
SAP Identity Management Runtime (in short, IdM RT)	IDENTITYCENTERRT
SAP Identity Management User Interface (in short, IdM UI, IdM Admin UI)	IDMIC
SAP Identity Management User Interface for HTML5 (in short, IdM HTML5)	IDMUI5
SAP Identity Management REST Interface Version 2 (in short, REST API)	IDMREST
SAP Identity Management Portal Content (in short, Portal Content)	IDMPORTALCONT
SAP Identity Management Core (in short, IdM Core)	IDENTITYCENTERCORE
Federation Software (in short, Identity Federation)	IDMFEDERATION

The SAP Identity Management components are available for download from the SAP Software Download Center on the SAP Support Portal. Install the prerequisites and the components in accordance with the diagram above and the installation sections covered by this guide.

The complete set of software components that make up SAP Identity Management is described in *Software Components of SAP Identity Management* section in *SAP Identity Management Master Guide*.

Related Information

Software Components of SAP Identity Management

2.2.2 Installation Options

This section describes the installation options covered by this installation guide.

You have to decide whether you want to install your SAP Identity Management system with all instances on one host or with the instances distributed over several hosts. The steps you have to perform vary according to the installation option you choose. You can choose between the following installation options:

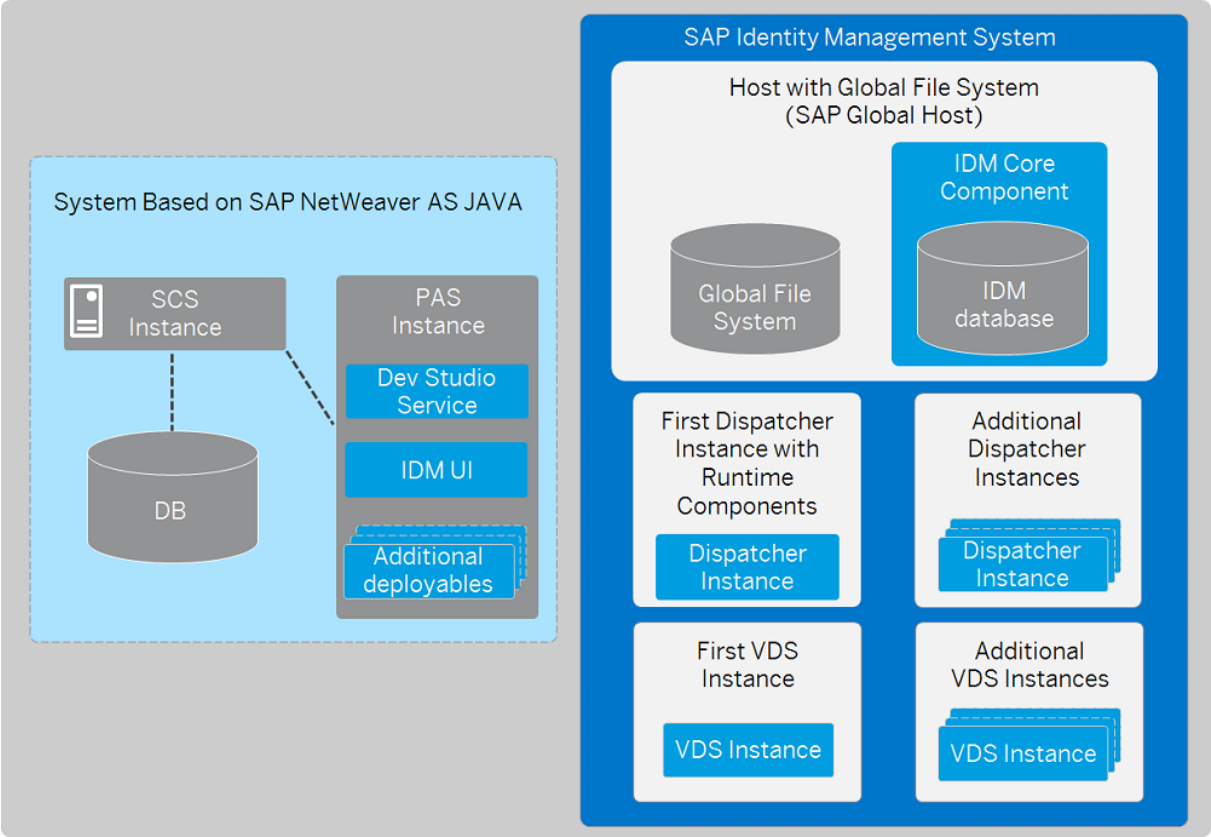
- Standard System on One Host [page 10]
- Distributed System [page 12]

2.2.2.1 Standard System on One Host

You can install a **standard** system on a **single** host.

> **Note**
>
> When installing a standard system, you must start the Software Provisioning Manager installation tool on the host where you want to install SAP Identity Management components.

An SAP system consists of SAP instances. An SAP instance is a group of processes that are started and stopped at the same time. In a **standard** system, all instances of the SAP Identity Management system and of the SAP NetWeaver AS Java with the additional deployables run on one host.



SAP Identity Management System with all Instances on One Host

The host where SAP Identity Management Core component is installed is considered the SAP global host. SAP global host is the host with the global file system.

> **Note**
>
> As SAP Identity Management Core component consists of several parts: Identity Management database schema, configuration packages and keys utility, all of them must be installed on one host. It is not possible to install different parts of the Core component on different hosts (for example, installing Core component on `<host 1>` and Identity Management database schema on `<host 2>`).

> **Note**
>
> Installing SAP Identity Management Core component on a remote database host is not supported. During installation, a message warns you that the database host you provide differs from the localhost where SWPM is started and where the Core component is to be installed.

In case of a standard system, the SAP Identity Management Core component, the first SAP Identity Management Dispatcher instance with Runtime components, the SAP Identity Management Developer Studio Service and the SAP Identity Management User Interface are installed on one host. The SAP NetWeaver Application Server (AS) Java that is necessary for some additional SAP Identity Management deployable components (see *Prerequisites and Dependencies Between Deployable Components*) is installed on the same host.

However, in a distributed system installation, it is recommended that this SAP NW AS Java system runs on a host different from SAP Identity Management Core component and the remaining SAP Identity Management

instances (see Distributed System [page 12]) For more information about installing an SAP Java system based on the supported SAP NetWeaver releases, see *Requirements on Windows*.

SAP Identity Management Virtual Directory Server (first VDS instance) can be installed on the same host as well.

In addition to the first SAP Identity Management Dispatcher instance with Runtime components, you can install one or more additional Dispatcher instances and Virtual Directory Server instances which can also reside on the same host.

Related Information

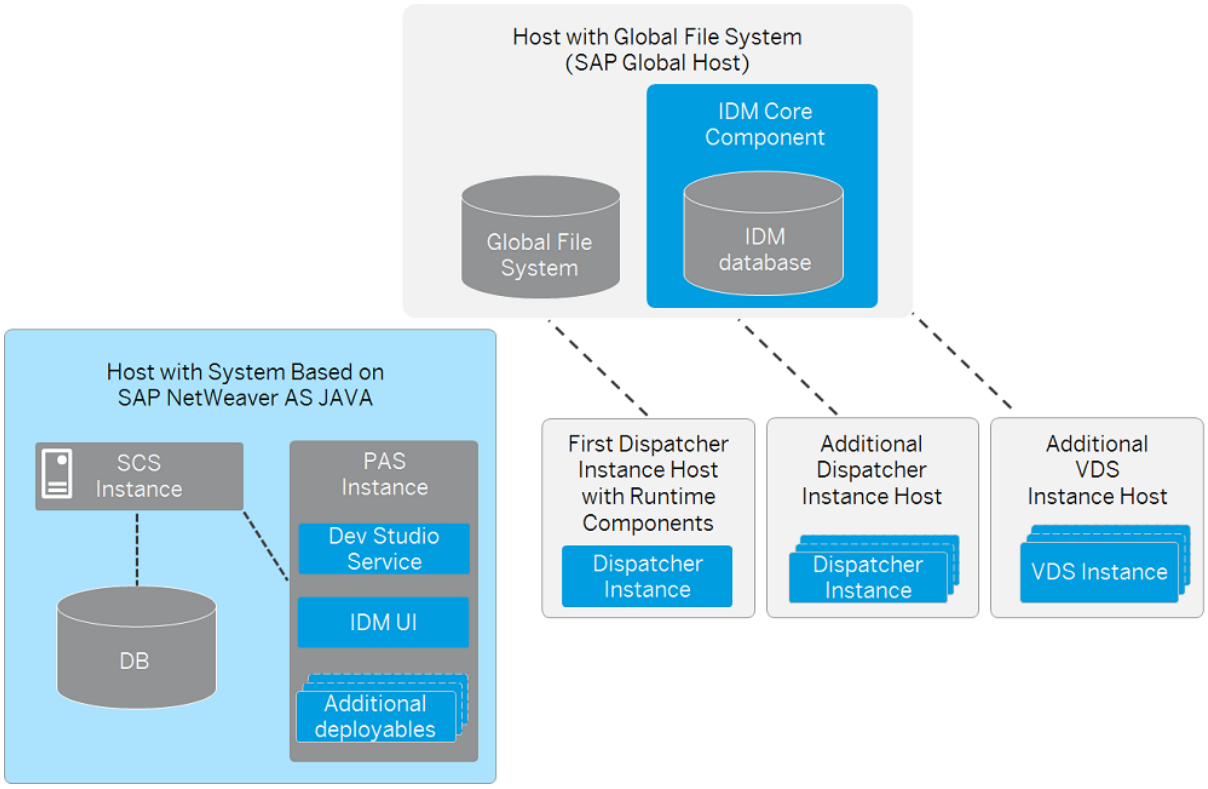
Distributed System [page 12]
Prerequisites and Dependencies Between Deployable Components [page 25]
Requirements on Windows [page 16]

2.2.2.2 Distributed System

You can install a system distributed over several hosts.

> ⓘ Note
>
> When installing a distributed system, you must start the Software Provisioning Manager installation tool on the hosts where you want to install SAP Identity Management components.

An SAP system consists of SAP instances. An SAP instance is a group of processes that are started and stopped at the same time. In a **distributed** system, every instance can run on a separate host.



SAP Identity Management System Distributed Over Several Hosts

The host where SAP Identity Management Core component is installed is considered the SAP global host. SAP global host is the host with the global file system.

> **Note**
>
> As SAP Identity Management Core component consists of several parts: Identity Management database schema, configuration packages and keys utility, all of them must be installed on one host. It is not possible to install different parts of the Core component on different hosts (for example, installing Core component on `<host 1>` and Identity Management database schema on `<host 2>`).

> **Note**
>
> Installing SAP Identity Management Core component on a remote database host is not supported. During installation, a message warns you that the database host you provide differs from the localhost where SWPM is started and where the Core component is to be installed.

There must be at least one Dispatcher instance (the First Dispatcher instance) which can be installed to a host different from the SAP Identity Management Core component. In addition to the First Dispatcher instance, you can install one or more Additional Dispatcher instances and Virtual Directory Server (VDS) instances which can reside either on the same host as the First Dispatcher instance or on different hosts.

You have to deploy the required SAP Identity Management Developer Studio Service and SAP Identity Management User Interface components on an SAP system based on SAP NetWeaver Application Server (AS) Java. It is recommended that this AS Java system runs on a host different from SAP Identity Management Core component and the remaining SAP Identity Management instances.

You can also deploy additional SAP Identity Management components (additional deployables) on this AS Java system, such as SAP Identity Management REST Interface Version 2, SAP Identity Management User Interface for HTML5 and SAP Identity Management Portal Content. For more information, see Prerequisites and Dependencies Between Deployable Components [page 25]

For more information about installing an SAP Java system based on the supported SAP NetWeaver releases, see *Requirements on Windows*.

Related Information

Standard System on One Host [page 10]
Requirements on Windows [page 16]

2.2.3 Hardware and Software Requirements

Here you find information about the hardware and software requirements for the SAP Identity Management system hosts.

Related Information

Requirements on Windows [page 16]

2.2.3.1 Running the Prerequisites Check in Standalone Mode (Optional)

This section describes how to run the prerequisites check in standalone mode. Running the prerequisites check in standalone mode is optional.

Context

When you install an SAP system, the Software Provisioning Manager automatically starts the prerequisites check and checks the hardware and software requirements in the background. As an optional step during planning, you can also run the prerequisites check in standalone mode to check the hardware and software requirements for your operating system and the SAP instances before the actual installation.

→ Recommendation

Procedure

1. Download and unpack the Software Provisioning Manager archive to a local directory as described in Downloading and Extracting the Software Provisioning Manager 1.0 Archive [page 52] .
2. Make either the separate SAPEXE`<Version>`.SAR archive or the complete kernel medium available as described in Preparing the Installation Media [page 51] .
3. Start the Software Provisioning Manager as described in Running Software Provisioning Manager [page 58].
4. On the *Welcome* screen, choose ▶ `<SAP_Product>` ▶ `<Database>` ▶ *Preparations* ▶ *Prerequisites Check* ▶.
5. Follow the instructions in the Software Provisioning Manager dialogs and enter the required parameters.

   > **Note**
   >
   > To find more information on each parameter during the *Define Parameters* phase, position the cursor on the required parameter input field , and choose either `F1` or the *HELP* tab. Then the available help text is displayed in the *HELP* tab.

   After you have finished, the *Parameter Summary* screen appears. This screen summarizes all parameters that you have entered and that you want to have checked. If you want to make a change, select the relevant parameters and choose *Revise*.
6. To start the prerequisites check, choose *Next*.

Results

The *Prerequisite Checker Results* screen displays the results found. If required, you can also check the results in file `prerequisite_checker_results.html`, which you can find in the installation directory.

Related Information

Downloading and Extracting the Software Provisioning Manager 1.0 Archive [page 52]

2.2.3.2 Requirements on Windows

Here you find the requirements for the installation on Windows.

Requirements on Windows

Requirement	Description
Minimum disk space	• SAP Identity Management Core Components (not including paging file): 4.0 GB • Additional SAP Identity Management Dispatcher instance (not including paging file): 2.0 GB • Up to 2.0 GB for each Virtual Directory Server instance. • Up to 2.0 GB for each additional SAP Identity Management 8.0 components on a host where SAP NetWeaver AS Java is installed. • Temporary disk space for every required installation medium that you have to copy to a local hard disk: 4.3 GB See also SAP Identity Management System Directories [page 41].
Minimum RAM	• SAP Identity Management Core Components: 4.0 GB • Additional SAP Identity Management Dispatcher instance: 2.0 GB • Up to 2.0 GB for each Virtual Directory Server instance. • Up to 2.0 GB for each additional SAP Identity Management 8.0 components on a host where SAP NetWeaver AS Java is installed.
Paging file size	For more information, see SAP Note 1518419.
Processing units	SAP Identity Management Core Component: The number of physical or virtual processing units usable by the operating system image must be equal to or greater than 2. SAP Identity Management Dispatcher Instance: One physical or virtual processing unit usable by the operating system image might be sufficient. Examples of processing units are processor cores or hardware threads (multithreading). In a virtualized environment, ensure that adequate processor resources are available to support the workloads of the running SAP systems.
Windows operating system	Check the *Product Availability Matrix* at Product Availability Matrix for supported operating system releases.

Requirement	Description
Database software	You must have installed the database software before you start the installation of the SAP Identity Management system. For more information about supported database versions, see Supported Database Systems (Overview) [page 17]. When installing the Identity Management database on the supported database systems, note the following prerequisites and recommendations: • Prerequisites and Recommendations (Microsoft SQL Server) [page 18] • Prerequisites and Recommendations (Oracle) [page 19] • Prerequisites and Recommendations (IBM DB2) [page 20] • Prerequisites and Recommendations (SAP ASE) [page 20]
JDBC driver	You must have downloaded the JDBC driver for the corresponding database. For more information, see Installing the JDBC Drivers [page 22].
SAP NetWeaver Java system for SAP Identity Management components	To deploy SAP Identity Management components on a SAP NetWeaver Java system, make sure that a SAP Java system based on SAP NetWeaver is available in your system landscape. The following SAP NetWeaver releases are supported: • SAP NetWeaver 7.3 SP09 or higher • SAP NetWeaver 7.3 including Enhancement Package 1 SP06 Patch 3 or higher • SAP NetWeaver 7.4 SP02 or higher • SAP NetWeaver 7.5 SP08 or higher For more information about installing an SAP Java system based on the listed SAP NetWeaver releases, see the installation guides at http://help.sap.com/sltoolset *System Provisioning* *Guide for Systems Based on SAP NetWeaver 7.1 and Higher* *Installation Guides by Database* `<Database>` *Java*
Windows regional settings	*English (United States)* must be set by default. For more information about localized Windows versions, see SAP Note 362379. You can install additional languages but the default setting for new users must always be *English (United States)*.

2.2.3.3 Supported Database Systems (Overview)

SAP Identity Management supports the following database systems:

- Microsoft SQL Server
- Oracle
- IBM DB2

The installation is available from the SAP Software Download Center on the SAP Support Portal. In the SAP Software Download Center, go to *Databases* > *Database and Database Patches* and download installation and support package files for SAP and third-party databases.

> **Note**
>
> If you are running the IBM DB2 database on the same server as the SAP NetWeaver AS Java, change the port number from 50000 to something else, as this will conflict with the default port number of SAP NetWeaver AS Java. The default value used in the database install scripts for the Identity Center database is 52222.

- SAP Adaptive Server Enterprise (SAP ASE)

> **Caution**
>
> Do not use native database tools to maintain the Identity Management database in a productive system. Do not manually delete queues or update entries, for example. Perform all database maintenance using the tools provided by SAP Identity Management, such as user interfaces, jobs, and tasks.

> **Note**
>
> We recommend that you always use the most recent database version. For more information about the supported database versions, see the Product Availability Matrix

Refer to the database system documentation for details about installation and how to install and configure a clustered database.

Related Information

SAP Software Download Center on SAP Support Portal

2.2.3.3.1 Prerequisites and Recommendations (Microsoft SQL Server)

The following configuration must be done/verified on the database server.

Collation

The default collation for Microsoft SQL Server is `SQL_Latin1_General_CP850_BIN2`.

Nevertheless, regardless of this installed server collation, the Identity Management database will use the server collation `SQL_Latin1_General_CP1_CI_AS`.

Mixed Mode Security

To log on to the accounts in question, the Microsoft SQL Server must support *Mixed Mode security*. This is configured in the Microsoft SQL Server properties for the specific database. See the Microsoft SQL Server help file for details.

> **Note**
>
> If you have installed a default SAP installation of Microsoft SQL Server, the `sa` user will be disabled with a random password. You need to enable the `sa` user and set a password in the SQL Server Management Studio.

Instance Configuration

SAP Identity Management does not support named instances on Microsoft SQL Server.

When installing Microsoft SQL Server, use the default instance option.

2.2.3.3.2 Prerequisites and Recommendations (Oracle)

When installing the Identity Management database on Oracle, note the following prerequisites and recommendations:

- Oracle provider for OLE DB/Starter database
  When installing the Oracle server on Microsoft Windows, you should include the component `Oracle provider for OLE DB` and a starter database, i.e. an empty database. For details, see the documentation for your Oracle system.
- Character set
  When installing the Identity Management database on Oracle, make sure that the database has been created with the AL32UTF8 character set so that it is possible to store data in the Japanese character set using UTF-8.
- Database naming
  If you plan to install remote Oracle clients that can access your database on the server, it might be a good idea to use the same database name (SID) on the Oracle server and the Oracle clients. If your server name is SERVER1 for example, you could call your database ORCL_DBSERVER1 and use this name when defining the connections strings for the dispatcher and data sources in SAP NetWeaver.
- Create as Container database
  If you use Oracle 12.1 (12c Release 1), 18.0.0.0 and 19.0.0.0, make sure the *Create as Container database* option is not selected.
- Oracle DB tablespaces
  You need to create a tablespace named USERS and a temporary tablespace named TEMP in the Oracle database.
- Number of cursors
  Make sure that the maximum number of cursors in Oracle is set to 600 or more. If not, increase the number and restart the Oracle database.

- Access Control List for the network utility package UTL_INADDR
  The database installation script can create the necessary `Access Control List` to allow the `<prefix>_prov_role` the necessary access to `UTL_INADDR`.
  To create the `Access Control List` in an existing database, see 1610907.
- > ⓘ Note
  >
  > Installing SAP Identity Management and SAP NetWeaver AS Java on the same Oracle database is not supported. You must install SAP Identity Management and SAP NetWeaver AS Java either on different databases on the same database server, or on different Oracle database servers.

2.2.3.3.3 Prerequisites and Recommendations (IBM DB2)

> ⚠ Caution
>
> Do not use SAPinst for the installation of IBM DB2. The DB2 installation has to be created by using db2setup wizard. If a default instance is created, groups, users, home directory, and environment variables are as expected by the setup script. For the IDM installation, you need to set the DB2_COMPATIBILITY_VECTOR registry variable to the value ORA, for example: DB2_COMPATIBILITY_VECTOR=ORA. This setting cannot be set if SAPinst is used for the installation.

For Microsoft Windows

To install the database on Microsoft Windows, the following software is required:

- PowerShell 2.0
- Command Window – Administrator (installed with the IBM DB2 database)
- Command Line Processor Plus (installed with the IBM DB2 database)

2.2.3.3.4 Prerequisites and Recommendations (SAP ASE)

Currently, you are able to choose between two SAP ASE editions - SAP ASE Enterprise edition and SAP ASE for Bussiness Suite Edition (SAP ASE Enterprise Edition with SAP ASE Runtime license for installation with SWPM).

Installing SAP ASE

When installing the Identity Management database on SAP ASE, note the following prerequisites and recommendations:

- **SAP ASE Enterprise edition**
  Install the SAP ASE Enterprise edition using the SAP ASE installer with you own enterprise license.

  > ⚠ Caution
  >
  > Do not use SAPinst for the installation of SAP ASE.

  For more information about how to install SAP ASE on different platforms, see SAP ASE Installation Guides in the SAP Adaptive Server Enterprise documentation.
- **SAP ASE for Bussiness Suite Edition (SAP ASE Enterprise Edition with SAP ASE Runtime license for installation with SWPM)**
  After the release of SWPM 1.0 SP39, you are able to use SWPM to install the SAP ASE for Bussiness Suite Edition with an embedded runtime license. For more information, see 2686693.
  To install the SAP ASE for Bussiness Suite Edition via SWPM, follow the steps below :
  1. On the *Welcome screen* of SWPM, choose *SAP Identity Management* > *Preparations* > *SAP ASE* > *SAP ASE Database Instance for SAP Identity Management System* .
  2. Follow the Software Provisioning Manager guidance to set up your SAP ASE database instance. The database server will be installed with the configuration options mentioned below.

     > ⓘ Note
     >
     > As **database software media** use *SAP ADAPTIVE SERVER ENTERPRISE* > *DATABASE* > *SAP ASE FOR BUSINESS SUITE* > *SAP ASE 16.0 FOR BUS. SUITE* from SAP Software Center.
- **Page Size**
  The Page Size should be **`16K`**. The default value is **`4K`**.
- **Character Set**
  The Default Character Set should be **`utf8: Unicode 3.1 UTF-8 Character Set`**
- **Sort Order**
  The Default Sort Order should be **`utf8_nocase: Case insensitive ordering, for use with any utf8-based 8-bit environment.`**
- **Transaction Log**
  The *trunc log on chkpt* database option (truncates the transaction log when an automatic checkpoint occurs) is set to *off*. This is the default value.

  > ⚠ Caution
  >
  > If you leave the *trunc log on chkpt* option set to *off*, the transaction log continues to grow. To protect your log from running out of space, you need to implement your backup solution that copies the transaction log before truncating it. For more information, see *Truncating the Log After Automatic Checkpoints*.
- **Optimization Goal and Optimizer Level**

  > → Recommendation
  >
  > If you are using SAP Identity Management on SAP ASE 16 or higher, we recommend you to check that the configuration parameters are set as follows: `optimization goal` to **`allrows_mix`**, and `optimizer level` to **`ase_default`** at the server level.

> ⚠ Caution
>
> Installing SAP Identity Management and SAP NetWeaver AS Java on the same SAP ASE database server is not supported. However, you can install them on separate SAP ASE database servers, running on the same or on separate hosts. For more information, see 1811976.

- **net password encryption reqd**
  Do not change the default value: `0`. Otherwise, you may receive "Incorrect password or settings" error when logging into the Dispatcher Utility.
  When set to its default value, this property allows the client to choose the encryption algorithm used for login passwords on the network, including no password encryption.

Patching SAP ASE Database Instance for SAP Identity Management System

Both images, SAP ASE Enterprise Edition and SAP ASE for Bussiness Suite Edition, include the same database software and can be used to patch the SAP ASE Database Instance for SAP Identity Management System. Updating the database software will not change the SAP ASE license type.

Related Information

Truncating the Log After Automatic Checkpoints

2.2.3.4 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

Microsoft SQL Server JDBC Driver [page 23]
Oracle JDBC Driver [page 23]
IBM DB2 JDBC Driver [page 24]
SAP ASE JDBC Driver [page 24]
JDBC Drivers for External Systems [page 25]

2.2.3.4.1 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

2.2.3.4.2 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

2.2.3.4.3 IBM DB2 JDBC Driver

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

By default it is installed in this folder:

- Microsoft Windows: `C:\Program Files\IBM\SQLLIB\java\`

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.

2.2.3.4.4 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 `<ASE_install_directory>\jConnect-16_0\classes\`.
  The name of the JDBC driver is: *com.sybase.jdbc4.jdbc.SybDriver*
  Make sure that the CLASSPATH is set to the correct file:
  `<ASE_install_directory>\jConnect-16_0\classes\jconn4.jar`.
- **SAP ASE version 16.0 SP04**
  The `jconn42.jar` file is located in `<ASE_install_directory>\jConnect-16_0\classes\`
  The name of the JDBC driver is: *com.sybase.jdbc42.jdbc.SybDriver*
  Make sure that the CLASSPATH is set to the correct file:
  `<ASE_install_directory>\jConnect-16_0\classes\jconn42.jar`.

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

2.2.3.4.5 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.

2.2.3.5 Prerequisites and Dependencies Between Deployable Components

This section describes the prerequisites for the SAP Identity Management components deployed on SAP NetWeaver AS Java, as well as the dependencies between those components.

Verify that the prerequisites and dependencies between components deployed on SAP NetWeaver AS Java are met. Otherwise, the deployment on AS Java might fail.

> **Note**
>
> The following installation tools are used for deploying SAP Identity Management components on SAP NetWeaver AS Java:
>
> - Software Provisioning Manager (SWPM) tool deploys SAP Identity Management components on SAP NetWeaver AS Java.
> - Software Update Manager (SUM) tool deploys AS Java Extension (SCA file) that is a prerequisite for SAP Identity Management User Interface for HTML5 component.
>
> You need to use SUM to fulfil the required prerequisites before running the SWPM tool. For more information, see Using the Software Update Manager (SUM) 1.0 [page 29]

Components Deployed on SAP NetWeaver AS Java

Components	Prerequisites	Dependencies

SAP Identity Management REST Interface Version 2	• One of the supported SAP NetWeaver versions is correctly installed and licensed.
	  • SAP NetWeaver 7.3 SP09 or higher
	  • SAP NetWeaver 7.3 including Enhancement Package 1 SP06 Patch 3 or higher
	  • SAP NetWeaver 7.4 SP02 or higher
	  • SAP NetWeaver 7.5 SP08 or higher
		SAP Identity Management User Interface is installed and configured.

Components	Prerequisites	Dependencies

SAP Identity Management User Interface for HTML5	• One of the supported SAP NetWeaver versions is correctly installed and licensed.
	  • SAP NetWeaver 7.3 SP09 or higher
	  • SAP NetWeaver 7.3 including Enhancement Package 1 SP06 Patch 3 or higher
	  • SAP NetWeaver 7.4 SP02 or higher
	  • SAP NetWeaver 7.5 SP08 or higher
	• SAPUI5 library is required. The library is available as an AS Java Extension for the SAP NetWeaver version you are using. Download the library extension from the SAP Software Download Center and deploy the downloaded SCA file on your AS Java server, using the Software Update Manager [page 29].
	Locate the correct SAPUI5 library on the SAP Software Download Center:
	Support Packages and Patches > *A - Z Index* > *N* > *SAP NETWEAVER* > *<your SAP NETWEAVER version>* > *Entry by Component* > *AS Java Extensions* > *SAPUI5 CLIENT RT AS JAVA <your SAP NW version>* > *# OS independent*.
	• For browser support information, see the SAP note for your SAP NetWeaver version:
	  • For SAP NetWeaver 7.3: 1509421
	  • For SAP NetWeaver 7.4: 1793938
	• You should have the following knowledge:
	  • Thorough knowledge about SAP NetWeaver AS for Java and its tools.
	  • Thorough knowledge about SAP Identity Management, and SAP Identity Management Developer Studio, in particular.
		SAP Identity Management User Interface is installed and configured.
		
		SAP Identity Management REST Interface Version 2 is deployed on your AS Java (where the SAP Identity Management User Interface is deployed).
		
		SAP Identity Management Developer Studio version 8.0, must be installed and licensed.

Components	Prerequisites	Dependencies

SAP Identity Management Portal Content	• One of the supported SAP NetWeaver versions is correctly installed and licensed.
	  • SAP NetWeaver 7.3 SP09 or higher
	  • SAP NetWeaver 7.3 including Enhancement Package 1 SP06 Patch 3 or higher
	  • SAP NetWeaver 7.4 SP02 or higher
	  • SAP NetWeaver 7.5 SP08 or higher
	• SAP Enterprise Portal is available on one of the supported SAP NetWeaver versions.
	• Universal Worklist (UWL) is configured on the portal.
	  • Configuring the Universal Worklist for SAP NetWeaver 7.3
	  • Configuring the Universal Worklist for SAP NetWeaver 7.3 EHP1
	  • Configuring the Universal Worklist for SAP NetWeaver 7.4
	  • Configuring the Universal Worklist for SAP NetWeaver 7.5
	• You have the administrative authorizations on the portal and on the SAP Identity Management systems.
		SAP Identity Management User Interface is installed and configured.

SAP Identity Management Developer Studio Service	• One of the supported SAP NetWeaver versions is correctly installed and licensed.
	  • SAP NetWeaver 7.3 SP09 or higher
	  • SAP NetWeaver 7.3 including Enhancement Package 1 SP06 Patch 3 or higher
	  • SAP NetWeaver 7.4 SP02 or higher
	  • SAP NetWeaver 7.5 SP08 or higher
	• SAP Cryptographic Library is installed for your SAP NetWeaver AS for Java version.
	  • Installing the SAP Cryptographic Library for SSL for SAP NetWeaver 7.3
	  • Installing the SAP Cryptographic Library for SSL for SAP NetWeaver 7.3 EHP1
	  • Installing the SAP Cryptographic Library for SSL for SAP NetWeaver 7.4
	  • Installing the SAP Cryptographic Library for SSL for SAP NetWeaver 7.5
	• Basic knowledge about the SAP NetWeaver AS for Java and its tools.
	• Administrator rights for the SAP NetWeaver AS for Java server.
		SAP Identity Management Runtime components are installed.
		Note
		For data discovery purposes, the SAP Identity Management Runtime components must be installed on the same server as where the SAP Identity Management Developer Studio service is installed.

Components	Prerequisites	Dependencies

SAP Identity Management User Interface	• One of the supported SAP NetWeaver versions is correctly installed and licensed.
	  • SAP NetWeaver 7.3 SP09 or higher
	  • SAP NetWeaver 7.3 including Enhancement Package 1 SP06 Patch 3 or higher
	  • SAP NetWeaver 7.4 SP02 or higher
	  • SAP NetWeaver 7.5 SP08 or higher
	• Clickjacking protection service for AS Java is enabled:
	  • Enabling the Clickjacking Protection Service for SAP NetWeaver 7.3
	  • Enabling the Clickjacking Protection Service for EHP 1 for SAP NetWeaver 7.3
	  • Enabling the Clickjacking Protection Service for SAP NetWeaver 7.4
	  • Enabling the Clickjacking Protection Service for SAP NetWeaver 7.5
	• Basic knowledge about the SAP NetWeaver AS for Java and its tools.
	• When giving certain accesses to the Identity Management User Interface, basic knowledge about the Identity Management Developer Studio is required.
	• For browser support information, see the SAP note for your SAP NetWeaver version:
	  • For SAP NetWeaver 7.3: 1509421
	  • For SAP NetWeaver 7.4: 1793938
	For questions related to browser support with Web Dynpro for Java, see the SAP KBA: 1618309
		SAP Identity Management Developer Studio version 8.0, must be correctly installed and licensed.
		This includes deploying the Identity Management Developer Studio service, adding the Identity Management database as the data source on your AS Java and installing an Identity Management Developer Studio client.

2.2.3.5.1 Using the Software Update Manager (SUM) 1.0

The Software Update Manager (SUM) is a multi-purpose tool that supports various processes, such as performing a release upgrade, installing enhancement packages, applying Support Package Stacks, installing add-ons, or updating single components on SAP NetWeaver.

Prerequisites

- Make sure that the latest version of Software Update Manager 1.0 is downloaded and available on your SAP NetWeaver AS for Java. Software Update Manager 1.0 is part of the Software Logistics Toolset delivery and available for download from SAP Software Download Center.
  You can download the SUM archive from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Download SUM* *SOFTWARE UPDATE MANAGER 1.0* *SUPPORT PACKAGE PATCHES* `<your OS>`.
- You can access the SUM documentation from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Software Update Manager (SUM) scenarios* *Software Update/Upgrade with SUM 1.0 SP*`<Version>` *Guides for SUM 1.0 SP*`<Version>`
  For SAP NetWeaver AS for Java, there are specific guides for the combinations of operating systems and databases.
- Before running and using the SUM 1.0, you have to complete all required preparation and planning actions in the SUM 1.0 user guide.
- Make sure that the SAP system and its database are started.
- On the host where you want to start the SL Common GUI of the Software Update Manager, Java 6 or higher has to be installed.
- SAP Host Agent has been configured on your system with the minimum version required for your scenario. For more information, see *Installing or Updating SAP Host Agent* in the *Update of SAP Systems Using Software Update Manager* guide that is relevant for your operating system and database.

Context

In the case of SAP Identity Management, you need SUM in the following processes:

- **SAP Identity Management installation with SWPM**
  In this case, you need SUM to deploy AS Java Extensions (SCA files) on the SAP NetWeaver AS Java system as a prerequisite for the following two components:
  - SAP Identity Management User Interface for HTML5

  For more information about the SCA files, see Prerequisites and Dependencies Between Deployable Components [page 25]
- **SAP Identity Management manual update** (that is, without using SWPM)
  In this case, you need SUM to deploy the new version of SAP Identity Management components that are deployed on SAP NetWeaver AS Java system:
  - SAP Identity Management Developer Studio Service

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

For more information about deploying a new version of SAP Identity Management components, see the topics under Updating SAP Identity Management Components [page 199] section.

To start and use the Software Update Manager 1.0, proceed as follows:

Procedure

1. Get the Software Update Manager running on the primary application server instance, as described in Running the Software Update Manager [page 30]
2. Start the SL Common GUI of the Software Update Manager, as described in Starting the SL Common GUI of the Software Update Manager [page 31].
3. Logon to the Software Update Manager and deploy the SCA file(s), as described in Deploying Using the Software Update Manager [page 32].

2.2.3.5.1.1 Running the Software Update Manager

Context

To run the Software Update Manager on the application server (primary application server instance), proceed as follows:

Procedure

1. Log on to the host on which the primary application server instance is running as user <SAPSID>adm (instance user).
2. Unpack the Software Update Manager package (<archive>.SAR) with the following command:
   - for Microsoft Windows:

     ```
     SAPCAR –xf <download directory>\<path>\<Archive>.SAR -R
     <DRIVE>:\usr\sap\<sapsid>
     ```

     This command creates the directory SUM under the `<DRIVE>:\usr\sap\<sapsid>` directory. You can also specify a directory other than `<DRIVE>:\usr\sap\<sapsid>`. In the following, the directory `\<path to SUM directory>\SUM` is referred to as <update directory>.

> **Note**
>
> The complete path to the `SUM` folder must not exceed 30 characters.

3. Start the Software Update Manager entering the following command:
   - for Microsoft Windows:

     ```
     <DRIVE>:\<update directory>\STARTUP.BAT confighostagent
     ```

     For Microsoft Windows and MS SQL Server, enter the following command:

     ```
     <DRIVE>:\<update directory>\STARTUP.BAT confighostagent jvm6
     ```

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

2.2.3.5.1.2 Starting the SL Common GUI of the Software Update Manager

Context

This section describes how you start the SL Common UI and the SUM back-end process.

Procedure

1. Open a web browser window.
2. In the address bar, enter the following URL: **`https://<hostname>:1129/lmsl/sumjava/<SID>/index.html`**.

   Replace *<hostname>* with the name of the host on which the Software Update Manager is running.

   > **Note**
   >
   > If the SSL is not configured, use http instead of https at the beginning of the URL, and use port 1128: **`http://<hostname>:1128/lmsl/sumjava/<SID>/index.html`**

3. In the dialog box that appears, enter the user name **`<sid>adm`** and the password.

Results

The SAP Host Agent starts the Software Update Manager, and the SL Common GUI of the Software Update Manager is displayed in the web browser.

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

2.2.3.5.1.3 Deploying Using the Software Update Manager

Context

The Software Update Manager controls the entire procedure, from checking the system requirements and importing the necessary programs through stopping production operation until production operation is resumed. The procedure is divided up into a number of different roadmap steps. The roadmap steps are in turn divided into phases. Many phases require no user input - step through those by choosing *Next*. The successful completion of a phase is a precondition for the success of all subsequent phases.

> ⓘ Note
>
> User actions are also required when errors occur. If an error occurs, correct it and repeat the phase in which the error has occurred. Once the phase has been repeated successfully, you can continue with the update.

To logon to the Software Update Manager and deploy the SCA file(s), do the following:

Procedure

1. Enter the user name and the password for the AS Java administrator user with which you log in to the system.
2. In the *Specify Credentials* roadmap step, specify the password for the instance user (<sapsid>adm), and then choose *Next*.
3. In the *Select Target* roadmap step, specify the path to the SCA file in the *Directory* field, then choose *Next*.
4. In the *Confirm Target* roadmap step, enter the keyword that is specified in the current *Central Software Update Manager Note* (which you can find in the Software Update Manager upgrade guide or in SAP Support Portal). Confirm the selected target system version by choosing *Next*.
5. In the *Configuration* roadmap step, provide the password of the AS Java administrator before proceeding. In this step it is also possible to specify the composition of the target release system.

6. Step through the phases requiring no user input by choosing *Next* and complete the process. Upon completing the process successfully, the important statistics are collected in a comprehensive report.

Next Steps

Every time you have used SUM, you need to either delete the `SUM` folder or rename it and keep it (if you would like, but this is not necessary). Then you have to extract a new `SUM` folder from the `SUM.SAR` file.

Use `SAPCAR.EXE` to extract the SAR file. Do the following:

1. In the command prompt, change to the directory to which you have downloaded or copied the SUM archives (the directory of the `SUM.SAR` file).
2. Start SAPCAR to extract the archive to the current directory. Enter
   `<path to sapcar.exe>\sapcar.exe -xvf SUM.SAR`
   and run the command line.
3. The `SUM.SAR` file should now be extracted and the new `SUM` folder created. You may now use SUM again.

Related Information

SAP Notes & SAP Knowledge Base Articles
Using the Software Update Manager (SUM) 1.0 [page 29]

2.2.4 Installation Parameters

This section lists the input parameters you are recommended to plan and prepare **before** you start the installation.

Note that this is not a complete list of input parameters. Further parameters that you do not need to plan and prepare beforehand are documented on the screens and in the F1 Help of Software Provisioning Manager.

General Parameters

Parameter	Description
Master Password	Common password for all users that are created during the installation: • Operating system users For example `<sapsid>adm`, `SAPService<sapsid>` **⚠ Caution** If you did not create the operating system users manually before the installation, Software Provisioning Manager creates them with the common master password (see *Operating System Users*). In this case, make sure that the master password meets the requirements of your operating system. **Password policy** The master password must meet the following requirements: • It must be 8 to 30 characters long • It must contain at least one digit (0-9) • It must not contain \ (backslash) and " (double quote) **ⓘ Note** Check the password policy of your database vendor for other special characters that are not allowed in passwords. • It must contain at least one letter in uppercase (A-Z) • It must contain at least one letter in lowercase (a-z) • **Oracle**: It must not begin with a digit nor an underscore • **Oracle:** It can contain the following characters: _, #, $, a-z, A-Z, 0-9 • Depending on the configuration of the password policy, additional restrictions may apply.

Parameter	Description
SAP System ID `<SAPSID>` of the SAP Identity Management Core Component system to be installed	The SAP system ID `<SAPSID>` identifies the entire SAP Identity Management system. Software Provisioning Manager prompts you for the `<SAPSID>` when you execute the **first** installation option to install a new SAP system. If there are further installation options to be executed, Software Provisioning Manager prompts you for the `profile` directory. For more information, see the description of the parameter *SAP System Profile Directory*. **⚠ Caution** Choose your SAP system ID carefully. Renaming is difficult and might require a system reinstallation. Make sure that your SAP system ID: • Is unique throughout your organization. Do not use an existing `<SAPSID>` when installing a new SAP system. • Consists of exactly three alphanumeric characters • Contains only uppercase letters • Has a letter for the first character • Does not include any of the reserved IDs listed in SAP Note 1979280.
Windows: Destination drive	Base directory for the SAP system. **ⓘ Note** If you install a subsequent SAP system, the `saploc` share already exists and you cannot select the installation drive. Software Provisioning Manager uses the installation drive where the `saploc` share points to.

Parameter	Description
Instance Number	An instance number is assigned to the following instances of the SAP Identity Management system: • SAP Identity Management Dispatcher instance • Virtual Directory Server instance Technical identifier for internal processes. It consists of a two-digit number from 00 to 97. The instance number must be unique on a host. That is, if more than one SAP instance is running on the same host, these instances must be assigned different numbers. If you do not enter a specific value, the instance number is set automatically to the next free and valid instance number that has not yet been assigned to the SAP system to be installed or to SAP systems that already exist on the installation host. To find out the instance numbers of SAP systems that already exist on the installation host, look for subdirectories ending with `<Instance_Number>` of local (not mounted) `\usr\sap\<SAPSID>` directories. **⚠ Caution** Do **not** use 43, and 89 for the instance number because: • 43 is part of the port number for high availability • 89 is part of the port number for Windows Terminal Server
SAP System ID `<SAPSID>` of the existing SAP NetWeaver Java system required for deployment of additional SAP Identity Management components	The SAP system ID `<SAPSID>` identifies the entire SAP NetWeaver Java system which is required on the host where additional SAP Identity Management components are to be deployed.
SAP Identity Management Secure Store	• Encryption Algorithm • Hash Algorithm For more information, see Encryption and Hashing.

Database Parameters

Parameter	Description
SAP Identity Management Database Schema and Base Qualified Name	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. **→ Recommendation** 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). The Base-Qualified Name is used for all SAP Identity Management packages in this database. **ⓘ Note** The base qualified name can contain only alphanumeric values (A-Z, a-z, 0-9), underscore (_) and period (.). Following the convention, you can use your company's reversed Internet domain name for the base qualified name of your packages. For example, if your company has the domain name **`acme.com`**, you can use the reversed domain name **`com.acme`** for the base qualified name.
Database Host	The Database Host is the host name of the server where the SAP Identity Management database is to run.
Database Port	The Database Port is the port of the server where the SAP Identity Management database is to run.
Database Users	The Identity Management database uses roles, which are assigned to users. See Database Roles and Users [page 40].
Developer Administrator User	The name of the developer administrator for this database. **ⓘ Note** This user must either exist in the UME or be added to the UME before you can log on to Identity Management Developer Studio.

Parameter	Description
JDBC Driver Parameters	The JDBC drivers are used by the runtime components to access the Identity Management database. • JDBC Driver Location This is the path to JDBC Driver. **MS SQL Server:** For example: `C:\Program Files\Microsoft SQL Server JDBC Driver 4.0` **IBM DB2:** For example: `C:\Program Files\IBM\SQLLIB\java\`. **Oracle:** You can choose between Oracle Thin Driver and Oracle OCI Driver **SAP ASE:** For example: `<ASE_install_directory>\jConnect-16_0\classes\jconn4.jar` • JDBC Driver Class This is the JDBC Driver Class Name of the JDBC driver that is required by the runtime engine. **MS SQL Server:** For example: com.microsoft.sqlserver.jdbc.SQLServerDriver for MS SQL Server **IBM DB2:** For example: com.ibm.db2.jcc.DB2Driver **Oracle:** For example: oracle.jdbc.driver.OracleDriver **SAP ASE:** For example: com.sybase.jdbc4.jdbc.SybDriver For more information, see Installing the JDBC Drivers [page 22].
Oracle Database Parameters	The data tablespace and the index tablespace are containers of data files in which database tables and indexes are stored. • Data Tablespace Name and Index Tablespace Name: The default value of the Data Tablespace Name and Index Tablespace Name is USERS. • Net Service Name: The Net Service Name is the name you want to use to connect to the database over the network. The default value is orcl. • Access Control List: You can specify whether you want the Access Control List for the network utility package UTL_INADDR to be created. The Access Control List grants the `<prefix>_prov_role` the necessary access to UTL_INADDR.
Database Parameters for IBM DB2 for UNIX, Windows, and Linux:	Storage Path: The `Storage Path` is the path to the folder where the database is to be installed. For example: `C:\usr\DB2\IC` Temporary Tablespace Name: The `Temporary Tablespace Name` used by IBM DB2. For example: USERTEMP

Parameter	Description
Database Parameters for SAP ASE:	SAP ASE Data Path: The `SAP ASE Data Path` is the path to the data file of MXMC_db. For example: `C:\SAP\data` SAP ASE Log Path: The `SAP ASE Log Path` is the path to the log file. It has to be the same as the SAP ASE Data Path.

Operating System Users

Parameter	Definition

Windows: Password of Operating System Users	The passwords of the operating system users **must** comply with the Windows password policy. Software Provisioning Manager processes the passwords of operating system users as follows:
	• If the operating system users do **not** exist, SAP creates the following users:
	  • `<sapsid>adm`
	  This user is the SAP system administrator user. It is a member of the local `Administrators` group.
	  • `SAPService<SAPSID>`
	  This user is the Windows account to run the SAP system. It is not a member of the local `Administrators` group.
	  • `sapadm`
	  The SAP Host Agent user `sapadm` is used for central monitoring services. Software Provisioning Manager creates this user by default as a local user although it is not a member of the local `Administrators` group.
	  If required, you can change this user to become a domain user on the *Parameter Summary* screen. For more information, see Performing a Domain Installation Without Being a Domain Administrator [page 48]. For security reasons, however, SAP strongly recommends you to create this user as a local user.
	Software Provisioning Manager sets the master password for these users by default. You can overwrite and change the passwords either by using the parameter mode *Custom* or by changing them on the *Parameter Summary* screen.
	• If the operating system users already exist, Software Provisioning Manager prompts you for the existing password, except the password of these users is the same as the master password.
	⚠ Caution
	Make sure that you have the required user authorization [page 46] for these accounts before you start the installation.

Parameter	Definition
Windows Domain Organizational Units	You can choose the organizational units (OUs) within the Windows domain where you want to create the SAP system accounts. By default, Software Provisioning Manager creates the domain users `SAPService<SAPSID>`, `<SAPSID>adm`, and the domain group `SAP_<SAPSID>_Globaladmin` in the domain Users container. Here you can specify an optional organizational unit where Software Provisioning Manager creates these domain users and group. The user who performs the installation needs read and write permissions to this organizational unit. The OU feature is only available when you select *Custom mode* in SWPM and choose *Use Domain of current user*. For more information, see SAP Note 2247673.

2.2.4.1 Database Roles and Users

The Identity Management database uses the following roles, which are assigned to users:

Database Roles and Users

Roles	Logins	Database	Description
db_owner	<prefix>_oper	MS SQL Server SAP ASE	This user is the owner of the database. This user has permission to modify the table structure of the database. The purpose of this user is to delegate database administration without distributing the password to the SYSTEM user. For security reasons, this role should only be used when updating the database schema.
	<prefix>_OPER	Oracle IBM DB2	
<prefix>_admin_role	<prefix>_oper <prefix>_admin	MS SQL Server SAP ASE	This role is used as login for the REST server for Identity Management Developer Studio. For security reasons, no users should have access to this role.
<prefix>_ADMIN_ROLE	<prefix>_ADMIN	Oracle IBM DB2	
<prefix>_rt_role	<prefix>_oper <prefix>_rt	MS SQL Server SAP ASE	This role is used by the runtime engine and is configured by the Dispatcher Utility.

Roles	Logins	Database	Description
<prefix>_RT_ROLE	<prefix>_RT	Oracle IBM DB2	
<prefix>_prov_role	<prefix>_oper <prefix>_prov	MS SQL Server SAP ASE	This role is used as login for the Identity Management User Interface.
<prefix>_PROV_ROLE	<prefix>_PROV	Oracle IBM DB2	
<prefix>_USER_ROLE	<prefix>_USER	IBM DB2	This role can view jobs and groups in Identity Management, but is not allowed to change any information, except for scheduling information.

For more information, see *Identity Center Database Logins and Roles* in *SAP Identity Management Security Guide*.

Related Information

Identity Center Database Logins and Roles
Creating and Configuring Dispatchers [page 115]

2.2.5 SAP Identity Management System Directories

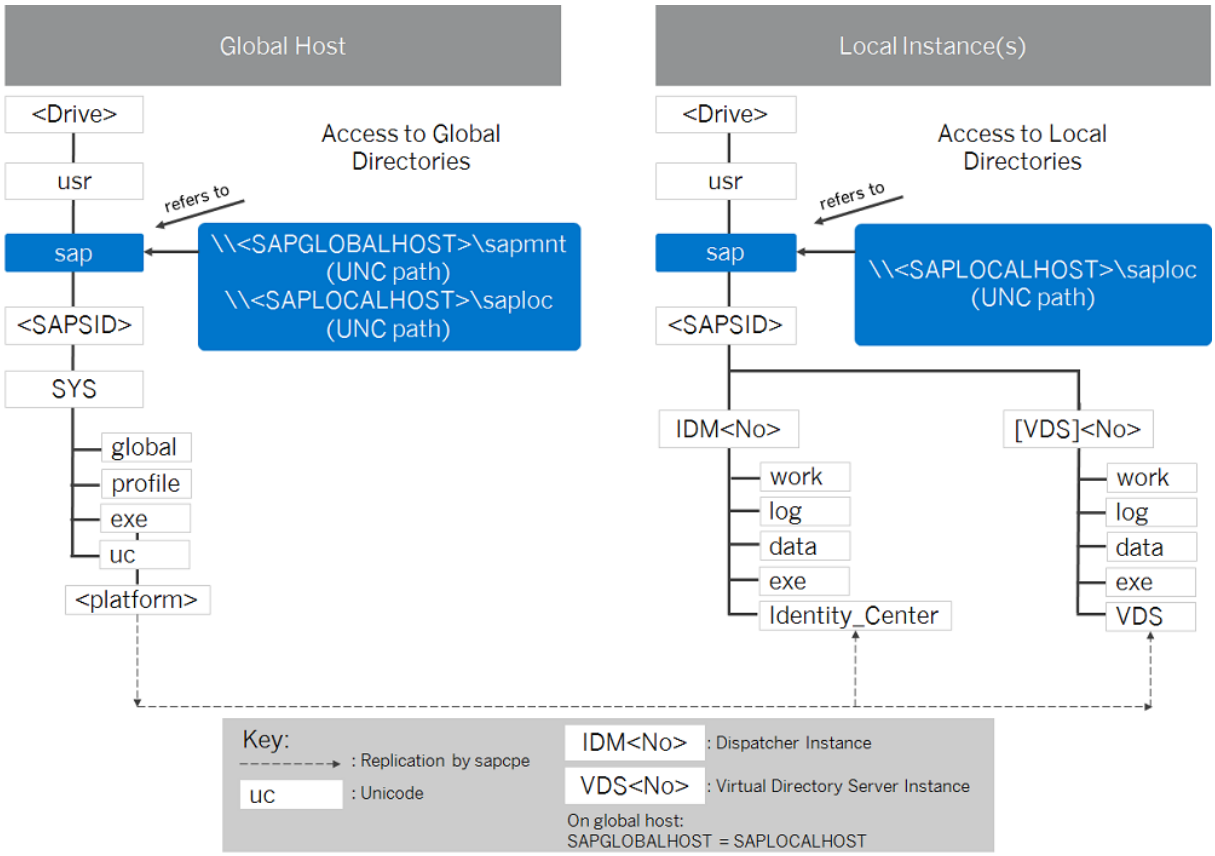
Here you find information about the required directories for the SAP Identity Management system and the required disk space.

Related Information

System Directories on Windows [page 42]

2.2.5.1 System Directories on Windows

Software Provisioning Manager automatically creates the following directories during the installation.



Directory Structure for an SAP Identity Management System on Windows

Directory	Description	Required Minimum Disc Space

`<Drive> : \usr\sap`	This directory is recommended to reside on the database host of the SAP Identity Management system and is created on the:
	• **Global** host and **shared** with the network share `sapmnt`
	On global hosts, the `\usr\sap` directory contains general SAP software, global, and local (instance-specific) data.
	For this, the installer creates the global directory `usr\sap\<SAPSID>\SYS`, which physically exists only once for each SAP system. It consists of the following subdirectories:
	  • `global` – contains globally shared data
	  • `profile` – contains the profiles for all instances
	  • `exe` – contains executable replication directory for all instances and platforms
	• **Local** host and **shared** with the name `saploc`.
	On local hosts, the `\usr\sap\<SAPSID>\<Instance_Name>` directory contains copies of the SAP software and local (instance-specific) data.
	Note
	• Since SAP traces for the instance are created in `\usr\sap`, make sure that there is sufficient space available in this directory. Changes in SAP profiles can also affect the disk space.
	• The executables on the local host are replicated from those on the global host every time the local instance is started. The SAP copy program `sapcpe` compares the binaries in the `<Platform>` directory on the global host and the binaries in the `exe` directory on the application server. If the binaries in the `exe` directory are older than those in the `<Platform>` directory, `sapcpe` replaces them with the newer version of the global host.
	Other application servers access the global data using the Universal Naming Convention (UNC) path `\\<SAPGLOBALHOST>\sapmnt`. The SAP programs access their instance-specific data with the UNC path `\\<SAPLOCALHOST>\saploc`. If the UNC path points to a local directory, the local path (and not the UNC path) is used to access the directory.
	The parameters `SAPGLOBALHOST` and `SAPLOCALHOST` have the **same** values on the global host.
		5.0 GB

`<Drive> : \usr\sap\<SAPSID>\IDM<Instance_Number>`	Instance directory of the SAP Identity Management Dispatcher instance The dispatcher instance directory contains the `log`, `data`, `work`, `exe`, and `Identity_Center` subdirectories.	2.0 GB

Directory	Description	Required Minimum Disc Space
<Drive>:\usr\sap\<SAPSID>\VDS<Instance_Number>	Virtual Directory Server instance The virtual directory server instance directory contains the log, data, work, exe, and VDS subdirectories.	1.5 GB
<Drive>:\usr\sap\<SAPSID>\SYS	System directory	1.0 GB

Related Information

SAP Identity Management System Directories [page 41]

2.3 Preparing for SAP Identity Management Installation

This section describes the preparation phase of SAP Identity Management installation.

Related Information

Performing Basic Windows Preparation Steps [page 44]
Required User Authorization for Running Software Provisioning Manager [page 46]
Performing a Domain Installation Without Being a Domain Administrator [page 48]
Creating Users and Accounts on Windows [page 49]

2.3.1 Performing Basic Windows Preparation Steps

Use

This section informs you about basic preparation steps that you have to perform before you install the SAP system, including the following:

- Deactivate the file and directory attribute caches
- Checking the Windows file system
- Checking the Windows domain structure (domain installation only)

- Deciding whether you want to use organizational units (OUs) in the Windows domain (domain installation only)

Procedure

Deactivate the File and Directory Attribute Caches

You need to set the following three file and directory attribute caches to 0:

For more information, see 3358301.

Perform as follows:

1. Open PowerShell
2. Enter the following three commands:
   - Set-SmbClientConfiguration -FileInfoCacheLifetime 0
   - Set-SmbClientConfiguration -FileNotFoundCacheLifetime 0
   - Set-SmbClientConfiguration -DirectoryCacheLifetime 0

Checking the Windows File System

You need to check which Windows file system you are using on hosts where you want to install the SAP system.

You should use the Windows file system ReFs or NTFS. Older Windows Server versions must use NTFS.

> ⓘ Note
>
> Do **not** install the SAP system on a FAT partition.

Perform the check as follows:

- Use PowerShell:
  1. Open PowerShell in elevated mode, and enter the following command:
     ```
     get-volume
     ```
  2. Check that the value *FileSystem* is ReFs or NTFS.
- Use Windows Explorer:
  1. Open the Windows Explorer.
  2. Select the relevant disk.
  3. Choose *Properties* > *General*.
     The system displays the type of file system in use.
  4. Check that the file system is NTFS.

Checking the Windows Domain Structure

> ⓘ Note
>
> You do **not** need this step for a local installation.

For a domain installation, we recommend that you check that all SAP system hosts are members of a single Windows domain. We recommend this for all SAP system setups.

We assume that you are familiar with checking Windows domain structures. For more information, see the Windows documentation.

In Windows, you can implement either of the following domain models for the SAP system:

- Extra domain
  In this model, the SAP system is embedded in its own domain, which is specially defined for SAP. A second domain exists for the user accounts.
  In Windows, the SAP domain and user domain must be incorporated in a domain tree. In this tree, the user accounts must form the root domain and the SAP domain must be a child domain of this.
- Single domain
  In this model, the SAP system, and the user accounts are included in a single domain.

> ⚠ Caution
>
> You cannot create local users and groups on the host that is used as domain controller. Therefore, we do **not** support running an SAP instance (including the database instance) on the host where the domain controller is installed.

Deciding Whether to Use Organizational Units (OUs) in the Windows Domain

> ⓘ Note
>
> You do **not** need this step for a local installation.

For a domain installation, the Software Provisioning Manager needs to create certain OS users for SAP and database operations in the Windows domain, also called the “Active Directory” (AD). These users are created by default in the AD container “Users”.

Depending on a customer's AD landscape and security policy, there are certain restrictions on where to store users and groups in AD. Contact the administrator of your AD infrastructure to understand where to store all SAP and database-related domain users and domain groups.

The SAP Software Provisioning Manager offers to define an existing OU in AD to create all needed SAP and database users in this OU.

There are many different scenarios and prerequisites concerning how to use OUs. For more information, see SAP Note 2247673, which explains these issues in detail and shows some examples of how to use them.

> ⚠ Caution
>
> The Software Provisioning Manager does **not** create OUs. The Software Provisioning Manager does **not** move existing domain users or groups. The Software Provisioning Manager does **not** delete existing users, groups, OUs, nor any other object in a Windows domain.
>
> The only exception to this rule is the Uninstall option in the software provisioning manager.

2.3.2 Required User Authorization for Running Software Provisioning Manager

Although the Software Provisioning Manager automatically grants the rights required for the installation to the user account used for the installation, you have to check whether this account has the required authorization

to perform the installation. The authorization required depends on whether you intend to perform a **domain** or **local** installation. If necessary, you have to ask the system administrator to grant the account the necessary authorization **before** you start the installation. If you attempt the installation with an account that does not have the required authorization, the installation aborts.

This section informs you about the authorization required for a domain and a local installation.

Procedure

> ⚠ Caution
>
> Do **not** use the user `<sapsid>adm` or the built-in administrator account for the installation of the SAP system.

Domain Installation

For a domain installation the account used for the installation needs to be a member of the local `Administrators` group. In many old installation guides, you find the information that the account must be a member of the `Domain Admins` group. The account can be either a member of the `Domain Admins` group or belong to the `Domain Users` group and have the necessary rights to create/modify objects in the domain.

All machines in the system must belong to the same domain. In a domain installation, the user information is stored centrally on the domain controller and is accessible to all hosts in the system.

If the SAP system is to be distributed across **more than one** machine, SAP strongly recommends that you perform a domain installation to avoid authorization problems.

For a domain installation, you need to:

1. Check that the account used for the installation is a member of the domain `Admins` group.
2. If required, obtain these rights by asking the system administrator to enter the account as a member of the domain `Admins` group.

Local Installation

For a local installation the account used for the installation needs to be a member of the local `Administrators` group of the machine involved. In a local installation, all Windows account information is stored locally on one host and is not visible to any other hosts in the system.

If the SAP system is to run on a **single** machine, you can perform a local installation.

> ⚠ Caution
>
> Do not use the Windows built-in account `Administrator` or the renamed built-in account to install your SAP system. The built-in account only has restricted network access rights that are required by the Software Provisioning Manager. If you renamed the built-in account `Administrator`, do not create a new account named `Administrator`.

For a local installation, you need to:

1. Check that the account used for the installation is a member of the local `Administrators` group.
2. If required, obtain these rights by asking the system administrator to enter the account as a member of the local `Administrators` group.

Related Information

Performing a Domain Installation Without Being a Domain Administrator [page 48]

2.3.3 Performing a Domain Installation Without Being a Domain Administrator

An alternative is to ask the domain administrator to grant the required permissions to the user which installs SAP or the database. This domain user must be a member of the local Administrators group. In most cases the domain administrator will define an OU (Organizational Unit) structure, where all SAP systems and their related domain objects belong to.

To perform the installation with a domain user, the user account must meet the following requirements:

1. Create/Delete/Modify Users and Groups within OUs only. Ask the AD administrator about the company's OU concept.
2. Create/Delete/Modify Computer Objects within this OU. This is required for users which install SAP or database applications in Failover Clusters, SAP Landscape Management environments or other high-availability (HA) environments.
   Optional rights might be necessary related to your company's security policy, for example:
3. Create/Delete/Modify DNS server records within a specific DNS zone, where the Windows hosts with SAP software belong to.
4. Create/Delete/Modify Organizational Unit objects within a specific OUs only.

The required objects in the domain are:

1. Domain group `SAP_<SAPSID>_GlobalAdmin`
   The group scope should be `GLOBAL`, the group type should be `SECURITY`.
2. Two new SAP system users `<sapsid>adm` and `SAPService<SAPSID>`.
3. The users `<sapsid>adm` and `SAPServiceSAPSID` must be members of the domain group `SAP_<SAPSID>_GlobalAdmin`.

> **Note**
>
> The Software Provisioning Manager creates the operating system user for the SAP Host Agent by default as a local user that is not
>
> a member of the local Administrators group. If you want to create this user manually as a domain user,
>
> you must perform the following steps:
>
> Creating the SAP Host Agent User and Group Manually
>
> 1. Create the new global group `SAP_GlobalAdmin`
> 2. Create the SAP system user `sapadm`.
> 3. Add the user sapadm to the newly created group `SAP_GlobalAdmin`.
>
> However, for security reasons we strongly recommend that you create this user as a local user.

2.3.4 Creating Users and Accounts on Windows

In a standard SAP system installation, Software Provisioning Manager automatically performs all steps relevant for security.

Although Software Provisioning Manager makes sure that the system is protected against unauthorized access, you must still check that no security breaches can occur.

For central and straightforward administration of the SAP system, you have to install distributed SAP systems with multiple application servers in a Windows **domain**. This section describes the user accounts and groups that Software Provisioning Manager creates during a domain installation and shows how these are related to the SAP directories.

User Accounts

Software Provisioning Manager creates the following accounts for SAP system administration:

User account	Description
`<sapsid>adm`	This is the SAP system administrator account that enables interactive administration of the system.
`SAPService<SAPSID>`	This is the user account that is required to start the SAP system. It has the local user right to log on as a service. The advantage of the additional `SAPService<SAPSID>` account is that it does not allow interactive logon, which prevents abuse of the account. Therefore, you do not need to set an expiration date for the password and you do not have to set the option *user must change password at next logon.*
`sapadm`	This is the user for the SAP Host Agent. By default it is a local user and not a member of the local `Administrators` group. You can change this user into a domain user on the *Parameter Summary* screen. For security reasons, however, SAP strongly recommends to create this user as a local user. The SAP Host Agent contains all of the required elements for centrally monitoring any host with the Alert Monitor or the SAP NetWeaver Administrator.

Domain and Local Groups

The only function of a domain group is to group users at the domain level so that they can be placed in the appropriate local groups.

Only local groups are created and maintained on each local host. A local group can only be given permissions and rights to the system where it is located. The system is part of a particular domain, and the local group can contain users and domain (global) groups from this domain.

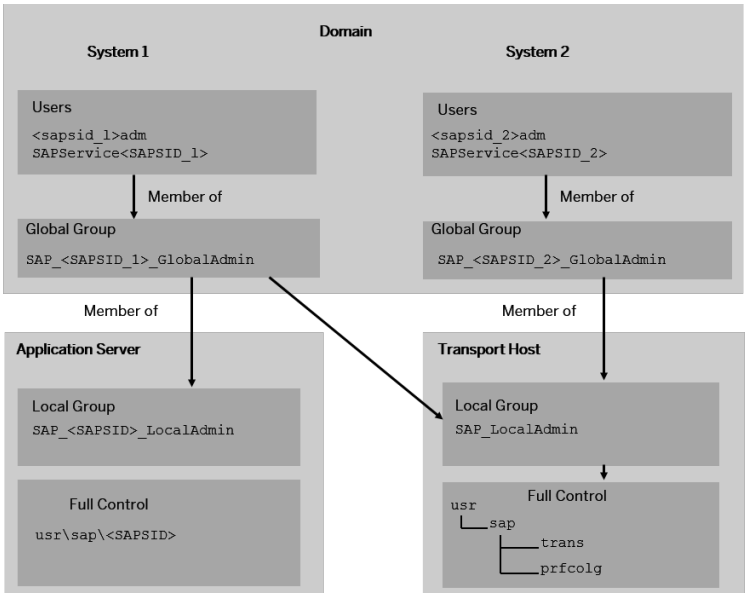
During a domain installation, Software Provisioning Manager creates the following domain and local groups:

Group	Description
SAP_<SAPSID>_GlobalAdmin	This domain (global) group is a domain-level SAP administration group for organizing SAP system administrators.
SAP_<SAPSID>_LocalAdmin	This local group is created on each host.
SAP_LocalAdmin	This local group is created on all hosts, but is particularly important for the transport host. Members of the group have full control over the transport directory (\usr\sap\trans) that allows transports to take place between systems. The SAP_<SAPSID>_GlobalAdmin groups of all the SAP systems that are part of the transport infrastructure are added to the SAP_LocalAdmin group. Therefore, the users <sapsid>adm and SAPService<SAPSID> of all systems in the transport infrastructure are members of the SAP_LocalAdmin group and have the required authorizations necessary to initiate and execute transports.

SAP Directories

Software Provisioning Manager protects the SAP directories under \usr\sap\<SAPSID> by only granting the group SAP_<SAPSID>_LocalAdmin full control over these directories.

The following graphic illustrates the users and groups that are created by Software Provisioning Manager for the <sapsid>adm and SAPService<SAPSID> users in a system infrastructure consisting of two SAP systems.



User Groups and Accounts

> **Note**
>
> An access control list (ACL) controls access to SAP system objects. For maximum security in the SAP system, only the following are members of **all** SAP system object ACLs:
>
> - Local group `SAP_<SAPSID>_LocalAdmin`
> - Group `Administrators`
> - User `SYSTEM`

2.3.5 Preparing the Installation Media

This section describes how to prepare the installation media.

Installation media are available as follows:

- The Software Provisioning Manager archive containing the installer.
  You always have to download the latest version of the Software Provisioning Manager archive.
- The dedicated installation archives (SAR files) containing the software to be installed, which are available as follows:
  - You can use the physical installation media as part of the installation package as described in *Using the Physical Media from the Installation Package*.
  - You can download the required **installation archives** (SAR files), as described in *Downloading Specific Installation Archives (Archive-Based Installation)*.

    > → Recommendation
    >
    > We recommend that you always download the latest patch level of SAP Identity Management components from the SAP Software Download Center.

For more information about which kernel version to use, see SAP Note 1680045. In addition, check the Product Availability Matrix at: http://support.sap.com/pam.

Related Information

Downloading and Extracting the Software Provisioning Manager 1.0 Archive [page 52]
Using Physical Media from the Installation Package [page 53]
Downloading Specific Installation Archives (Archive-Based Installation) [page 55]

2.3.5.1 Downloading and Extracting the Software Provisioning Manager 1.0 Archive

This section describes how to make the Software Provisioning Manager 1.0 available.

Prerequisites

You must always download and extract the Software Provisioning Manager 1.0 archive from the SAP Software Download Center because you must use the latest version.

- Make sure that you use the **latest** version of the SAPCAR tool when manually extracting the Software Provisioning Manager archive. You need the SAPCAR tool to be able to unpack and verify software component archives (*.SAR files). *.SAR is the format of software life-cycle media and tools that you can download from the SAP Software Download Center.

  > ⓘ Note
  >
  > An older SAPCAR version might extract archive files in a wrong way and this could prevent the Software Provisioning Manager from working consistently.

  Proceed as follows to get the latest version of the SAPCAR tool:

  1. Go to https://me.sap.com/softwarecenter > *SUPPORT PACKAGES & PATCHES* > *By Category* > *SAP TECHNOLOGY COMPONENTS* > *SAPCAR* .
  2. Select the SAPCAR for your operating system and download it to an empty directory.
  3. Even if you have the latest SAPCAR already available, we strongly recommend that you verify its digital signature anyway, unless you downloaded it directly from https://me.sap.com/softwarecenter/ yourself. You can do this by verifying the checksum of the downloaded SAPCAR tool:
     1. Depending on what operating system you are using, compute a hash of the downloaded SAPCAR tool, using the SHA-256 algorithm used by SAP .
     2. Now verify the digital signature of the downloaded SAPCAR tool by comparing the hash with the checksum (generated by SAP using the SHA-256 algorithm) from the *Content Info* button in the *Related Info* column on the right-hand side of the place where you downloaded the SAPCAR tool.
  4. To improve usability, we recommend that you rename the executable to **SAPCAR**.

  For more information about SAPCAR, see SAP Note 212876.

Procedure

1. Download the latest version of the Software Provisioning Manager 1.0 archive `SWPM10SP<Support_Package_Number>_<Version_Number>.SAR` :

   https://support.sap.com/sltoolset > *System Provisioning* > *Download Software Provisioning Manager*
2. Using the latest version of SAPCAR, you can verify the digital signature of the downloaded `SWPM10SP<Support_Package_Number>_<Version_Number>.SAR` archive as follows:

a. Get the latest version of the SAPCRYPTOLIB archive to your installation host as follows:

   1. Go to https://me.sap.com/softwarecenter *SUPPORT PACKAGES & PATCHES* and search for "**sapcryptolib**".
   2. Select the archive file for your operating system and download it to the same directory where you have put the SAPCAR executable.
   3. Use the following command to extract the SAPCRYPTOLIB archive to the same directory where you have put the SAPCAR executable:
      SAPCAR -xvf sapcryptolibp_84…sar -R <target directory>
   4. Download the Certificate Revocation List from https://tcs.mysap.com/crl/crlbag.p7s and move it to the same directory.

b. Verify the digital signature of the downloaded SWPM10SP<Support_Package_Number>_<Version_Number>.SAR archive by executing the following command:

> **Note**
>
> Check SAP Notes 2178665 and 1680045 whether additional information is available.

```
<Path to SAPCAR>\sapcar.exe -tvVf<Path to Download
Directory>\SWPM10SP<Support_Package_Number>_<Version_Number>.SAR -crl <file
name of revocation list>
```

3. Unpack the Software Provisioning Manager archive to a local directory using the following command:

```
<Path to SAPCAR>\sapcar.exe -xvf <Path to Download
Directory>\SWPM10SP<Support_Package_Number>_<Version_Number>.SAR -R <Path to
Unpack Directory>
```

> **Note**
>
> Make sure that all users have at least read permissions for the directory to which you unpack the Software Provisioning Manager archive.

> **Caution**
>
> Make sure that you unpack the Software Provisioning Manager archive to a dedicated folder. Do not unpack it to the same folder as other installation media.

2.3.5.2 Using Physical Media from the Installation Package

Context

You use the physical installation media as part of the installation package.

Procedure

1. Identify the required media for your installation as listed below.

SAP Identity Management Instance Installation	Required Software Packages from Installation Media
SAP Identity Management Core	• Software Provisioning Manager archive • UC Kernel (folder K_<Version>_U_<OS>) where U means Unicode. • SAP IDENTITY MANAGEMENT 8.0
SAP Identity Management Dispatcher instance	• Software Provisioning Manager archive • UC Kernel (folder K_<Version>_U_<OS>) where U means Unicode. • SAP IDENTITY MANAGEMENT 8.0
Virtual Directory Server instance of SAP Identity Management	• Software Provisioning Manager archive • UC Kernel (folder K_<Version>_U_<OS>) where U means Unicode. • SAP IDENTITY MANAGEMENT 8.0
Additional SAP Identity Management components	• Software Provisioning Manager archive • UC Kernel (folder K_<Version>_<U>_<OS>) where U means Unicode. • SAP IDENTITY MANAGEMENT 8.0

2. Make the installation media available on each installation host as follows:
   a. Download the latest version of the Software Provisioning Manager archive from:

      http://support.sap.com/swdc *Support Packages and Patches* > *A – Z Index* > *S* > *SL Toolset* > *SL Toolset* <Release> > *Entry by Component* > *Software Provisioning Manager* > *Software Provisioning Manager 1.0* > *Support Package Patches* > <OS>
   b. Unpack the Software Provisioning Manager 1.0 archive as described in Downloading and Extracting the Software Provisioning Manager 1.0 Archive [page 52].
   c. Make the media containing the software to be installed available on each installation host.

      You can do this in one of the following ways:

      - Copy the required media folders directly to the installation hosts.
      - Mount the media on a central media server that can be accessed from the installation hosts.

      > ⚠ Caution
      >
      > - If you copy the media to disk, make sure that the paths to the destination location of the copied media do not contain any blanks.
      > - If you perform a domain installation and do not want to copy the media but use network drives for mapping the installation media, make sure that the <sapsid>adm user has access to the UNC paths of the network drives.

If the user does not yet exist, you have to create the user manually before you install the SAP system.

> ⓘ Note
>
> The signature of media is checked **automatically** by the installer during the *Define Parameters* phase while the *Media Browser* screens are processed (see also Running Software Provisioning Manager [page 58]). As of now the installer only accepts media whose signature has been checked. For more information, see SAP Note 2393060.

2.3.5.3 Downloading Specific Installation Archives (Archive-Based Installation)

You can download the specifically required installation archives for your SAP Identity Management system installation. During the installation, you can either specify the path to each archive separately, or provide the path to a download basket with all downloaded archives.

Procedure

1. Download and unpack the latest version of Software Provisioning Manager as described in Downloading and Extracting the Software Provisioning Manager 1.0 Archive [page 52].
2. Download the latest patch level of SAP Identity Management installation archives from: https://support.sap.com/swdc *Software Downloads* *Support Packages & Patches* *Browse our Download Catalog* *By Category* *SAP NetWeaver and complementary products* *SAP NW IDENTITY MANAGEMENT* *SAP IDENTITY MANAGEMENT 8.0* *COMPRISED SOFTWARE COMPONENT VERSIONS*

   > → Recommendation
   >
   > We recommend that you always download the latest patch level of SAP Identity Management components from the SAP Software Download Center.

   - `ICCORE<Version>.SAR`
   - `IDMREST<Version>.SAR`
   - `ICRUNTIME<Version>.SAR`
   - `IDMPORTALCONT<Version>.SAR`
   - `IDMCLMRESTAPI<Version>.SAR`
   - `IDMFEDERATION<Version>.SAR`
   - `IDMIC<Version>.SAR`
   - `IDMUI5<Version>.SAR`

- VDSERVER<Version>.SAR

During the installation, you can either specify the path to each archive separately, or provide the path to a download basket with all downloaded archives.

3. Download the specifically required installation archives for your SAP Identity Management system installation.

> ⚠ Caution

- SAPEXE<Version>.SAR
  Download the latest patch level of SAPEXE.SAR from: http://support.sap.com/swdc *Software Downloads* *Support Packages and Patches* *Browse our Download Catalog* *By Category* *Additional Components* *SAP Kernel* *SAP KERNEL 64-BIT UNICODE* <SAP KERNEL 7.45 64-BIT UNICODE or SAP KERNEL 7.49 64-BIT UNICODE> <Select your operating system> *#Database independent*
- SAPHOSTAGENT<Version>.SAR
  Download the latest patch level of SAPHOSTAGENT<Version>.SAR from: http://support.sap.com/swdc *Software Downloads* *Support Packages and Patches* *Browse Download Catalog* *By Category* *SAP Technology Components* *SAP HOST AGENT* *SAP HOST AGENT 7.21* <Select your operating system>
- SAPJVM8_<Version>.SAR
  Download the latest patch level of SAPJVM8_<Version>.SAR from SAP Note 1442124. Choose the location specified for SAP JVM 8.1.

During the installation, you can either specify the path to each archive separately, or provide the path to a download basket with all downloaded archives.

2.4 Installing SAP Identity Management

This section describes the installation phase of SAP Identity Management.

Related Information

Prerequisites for Running Software Provisioning Manager [page 57]
Running Software Provisioning Manager [page 58]
Additional Information About Software Provisioning Manager [page 61]
Installing the Identity Management Developer Studio [page 70]

2.4.1 Prerequisites for Running Software Provisioning Manager

Make sure you meet the following prerequisites before running the Software Provisioning Manager.

- For the SL-UI, make sure that the following web browser requirements are met:
  - You have one of the following supported browsers on the device where you want to run the SL-UI:
    - Google Chrome (recommended)
    - Mozilla Firefox
    - Microsoft Edge

    Always use the latest version of these web browsers.
  - If you copy the SL-UI URL manually in the browser window, make sure that you open a new Web browser window in private browsing mode (Internet Explorer), incognito mode (Chrome) or private browsing mode (Firefox). This is to prevent Web browser plugins and settings from interfering with the SL-UI.

  > ⚠ Caution
  >
  > The Software Provisioning Manager uses a self-signed certificate, which is used temporarily only while the Software Provisioning Manager is running. This certificate is not trusted by the browser unless it is imported manually by the user running the Software Provisioning Manager. This behavior is intentionally designed in this way because - unlike ordinary public web servers - the Software Provisioning Manager has different usage patterns. You must configure your browser do trust the self-issued certificate of the Software Provisioning Manager after carefully performing the “thumbprint” verification described in Running Software Provisioning Manager [page 58] . For more information about adding trusted certificates, see the documentation of your browser.

  For more information about the SL-UI, see Useful Information about Software Provisioning Manager [page 62].

- The SAPinst framework of Software Provisioning Manager checks certificates for the Software Provisioning Manager, archives and media and therefore uses a certificate revocation list (CRL). Make sure that this CRL is available. For more information, see SAP Note 3207613.
- If you want to enable Internet Protocol Version 6 (IPv6), make sure that you set **`SAP_IPv6_ACTIVE=1`** in the environment of the user with the required authorization [page 46] to run the Software Provisioning Manager. While running the Software Provisioning Manager, this setting is then also added to the environment of the `<sapsid>adm` user.

  > ⓘ Note
  >
  > By applying this setting the SAP system administrator is responsible for configuring the IP version on each host of the system landscape, before installing any additional instance to it.

- You need at least 700 MB of free space in the installation directory for each installation option. In addition, you need 700 MB free space for the Software Provisioning Manager executables. The Software Provisioning Manager creates an installation directory `sapinst_instdir`, where it keeps its log files, and which is located directly in the `%ProgramFiles%` directory. For more information, see Useful Information about Software Provisioning Manager [page 62].
- Make sure that the following ports are not used by other processes:
  - Port 4237 is used by default as HTTPS port for communication between the Software Provisioning Manager and the SL-UI.

If this port cannot be used, you can assign a free port number by executing `sapinst.exe` with the following command line parameter:
`SAPINST_HTTPS_PORT=<Free Port Number>`

- Port 4239 is used by default for displaying the feedback evaluation form at the end of the Software Provisioning Manager processing.
  The filled-out evaluation form is then sent to SAP using HTTPS.
  If this port cannot be used, you can assign a free port number by executing `sapinst.exe` with the following command line parameter:
  `SAPINST_HTTP_PORT=<Free Port Number>`

2.4.2 Running Software Provisioning Manager

This section describes how to run the Software Provisioning Manager.

Prerequisites

For more information, see Prerequisites for Running Software Provisioning Manager [page 57].

Context

The Software Provisioning Manager has a web browser-based GUI named “SL-UI of the Software Provisioning Manager” - “SL-UI” for short.

This procedure describes an installation where you run the Software Provisioning Manager and use the SL-UI, that is you can control the processing of the Software Provisioning Manager from a browser running on any device.

For more information about the SL-UI, see Useful Information about Software Provisioning Manager [page 62].

Procedure

1. Start the Software Provisioning Manager from the directory to which you unpacked the Software Provisioning Manager archive with the following command:

   `sapinst.exe` (in a command prompt)

   `.\sapinst.exe` (in PowerShell)

   By default, the SL-UI uses the default browser defined for the host where you run the Software Provisioning Manager. However, you can also specify another supported web browser available on the host where you start the Software Provisioning Manager. You can do this by starting the `sapinst`

executable with command line option **SAPINST_BROWSER=<Path to Browser Executable>**, for example **SAPINST_BROWSER=firefox.exe**.

> **Note**
>
> 1. Open a command prompt or `PowerShell` window in elevated mode and change to the directory to which you unpacked the Software Provisioning Manager archive.
> 2. Start the Software Provisioning Manager with the following command:
>   **sapinst.exe SAPINST_USE_HOSTNAME=<Virtual_Host_Name>** (in a command prompt)
>   **.\sapinst.exe SAPINST_USE_HOSTNAME=<Virtual_Host_Name>** (in `PowerShell`)

2. The Software Provisioning Manager now starts and waits for the connection with the SL-UI.

   If you have a supported web browser (see Prerequisites for Running Software Provisioning Manager [page 57]) installed on the host where you run the Software Provisioning Manager, the SL-UI starts automatically by displaying the *Welcome* screen.

   If the SL-UI does not open automatically, you can find the URL you require to access the SL-UI at the bottom of the *Program Starter* window of the Software Provisioning Manager. You find the icon of the *Program Starter* window in the taskbar of your Windows host. Open a supported web browser and run the URL from there.

```
...
************************************************************************
Open your browser and paste the following URL address to access the GUI
https://[<hostname>]:4237/sapinst/docs/index.html
Logon users: [<users>]
************************************************************************
...
```

> **Note**
>
> If the host specified by `<hostname>` cannot be reached due to a special network configuration, proceed as follows:
>
> 1. Terminate the Software Provisioning Manager as described in Useful Information about Software Provisioning Manager [page 62].
> 2. Restart the Software Provisioning Manager from the command line with the **SAPINST_GUI_HOSTNAME=<hostname>** property.
>   You can use a fully-qualified host name.

> **Caution**
>
> After opening the browser URL, make sure that the URL in the browser starts with “https://” to avoid security risks such as SSL stripping.
>
> Before you reach the *Welcome* screen, your browser warns you that the certificate of the `sapinst` process on this computer could not be verified.
>
> Proceed as follows to avoid security risks such as a man-in-the-middle attack:
>
> 1. Click on the certificate area on the left hand side in the address bar of your browser, and view the certificate.
> 2. Open the certificate fingerprint or thumbprint, and compare all hexadecimal numbers to the ones displayed in the console output of the Software Provisioning Manager.

Proceed as follows to get the certificate fingerprint or thumbprint from the server certificate printed in the Software Provisioning Manager console:

1. Go to the `sapinst_exe.xxxxxx.xxxx` directory in the temporary directory to which the Software Provisioning Manager has extracted itself: `%userprofile%\.sapinst\`
2. In the `sapinst_exe.xxxxxx.xxxx` directory, execute the `sapgenpse` tool with the command line option **`get_my_name -p`**.

As a result, you get the server fingerprint or thumbprint from the server certificate.

3. Accept the warning to inform your browser that it can trust this site, even if the certificate could not be verified.

The SL-UI opens in the browser by displaying the *Welcome* screen.

3. On the *Welcome* screen, choose the required option:

   To prepare, install, or update an SAP Identity Management system, go to the *SAP Identity Management 8.0* folder and select the required option from the appropriate sub-folder:

   - *Preparations*
     You can prepare an SAP ASE Database instance with runtime license for an SAP Identity Management System
   - *Install*
     - You can install a *Standard System* with all required components of an SAP Identity Management 8.0 system on one host.
     - You can install a *Distributed System* with the SAP Identity Management 8.0 instances distributed over several host.
     - You can install *Additional Components* of SAP Identity Management 8.0.
   - *Update*
     - You can update a *Standard System* with all required components of an SAP Identity Management 8.0 system on one host.
     - You can update a *Distributed System* with the SAP Identity Management 8.0 instances distributed over several host.
     - You can update *Additional Components* of SAP Identity Management 8.0.

   To uninstall an SAP Identity Management 8.0 system, choose *Generic Options* > `<Database>` > *Uninstall - SAP Systems or Single Instances*

4. Choose *Next*.

> **Note**
>
> If there are errors during the self-extraction process of the Software Provisioning Manager, you can find the log file `dev_selfex.out` in the temporary directory.

5. If the Software Provisioning Manager prompts you to log off from your system, log off and log on again.

   The Software Provisioning Manager restarts automatically.

6. Follow the instructions on the Software Provisioning Manager screens and enter the required parameters.

> **Note**
>
> To find more information on each parameter during the *Define Parameters* phase, position the cursor on the required parameter input field , and choose either F1 or the *HELP* tab. Then the available help text is displayed in the *HELP* tab.

> **Caution**
>
> The digital signature of installation media and installation archives is checked **automatically** during the *Define Parameters* phase while processing the *Media Browser* and - if you perform an archive-based installation - the *Software Package Browser* screens.
>
> Note that this automatic check is only committed once and **not** repeated if you modify artifacts such as SAR archives or files on the media **after** the initial check has been done. This means that - if you modify artefacts later on either during the remaining *Define Parameters* phase or later on during the *Execute Service* phase - the digital signature is not checked again.
>
> For more information, see SAP Note 2393060.

After you have entered all requested input parameters, the Software Provisioning Manager displays the *Parameter Summary* screen. This screen shows both the parameters that you entered and those that the Software Provisioning Manager set by default. If required, you can revise the parameters before starting the installation.

7. To start the installation, choose *Next*.

   The Software Provisioning Manager starts the installation and displays the progress of the installation. When the installation has finished, the Software Provisioning Manager shows the message: `Execution of <Option_Name> has completed`.

8. If you copied the Software Provisioning Manager software to your hard disk, you can delete these files when the installation has successfully completed.
9. For security reasons, we recommend that you delete the `.sapinst` directory within the home directory of the user with which you ran the Software Provisioning Manager:

   ```
   %userprofile%\.sapinst\
   ```

10. The Software Provisioning Manager log files contain IP addresses and User IDs such as the ID of your S-User. For security, data protection, and privacy-related reasons we strongly recommend that you delete these log files once you do not need them any longer.

    You find the Software Provisioning Manager log files in the `sapinst_instdir` directory. For more information, see Useful Information about Software Provisioning Manager [page 62].

2.4.3 Additional Information About Software Provisioning Manager

2.4.3.1 Useful Information about Software Provisioning Manager

This section contains some useful technical background information about the Software Provisioning Manager and the SL-UI.

- The Software Provisioning Manager has a framework named “SAPinst”. For more information about the current SAPinst Framework version and its features, see SAP Note 3207613 (*SAPinst Framework 753 Central Note*).
- The Software Provisioning Manager has the web browser-based “SL-UI of the Software Provisioning Manager” - “SL-UI” for short.
  The SL-UI uses the SAP UI Development Toolkit for HTML5 - also known as SAPUI5 - a client-side HTML5 rendering library based on JavaScript. The benefits of this user interface technology for the user are:
  - Zero foot print, since only a web browser is required on the client
  - Controls and functionality, for example, view logs in web browser.

  As of version 1.0 SP24 Patch Level 5, the Software Provisioning Manager has an updated look and feel of the SL-UI. For more information, see https://blogs.sap.com/2018/11/10/new-look-for-software-provisioning-manager/.
  The SL-UI connects the web browser on a client with the `sapinst` executable - which is part of Software Provisioning Manager - running on the installation host using the standard protocol HTTPS.
  For the SL-UI, the Software Provisioning Manager provides a pre-generated URL in the *Program Starter* window. If you have a supported web browser installed on the host where you run the Software Provisioning Manager, the SL-UI starts automatically.
  By default, the SL-UI uses the default browser defined for the host where you run the Software Provisioning Manager. However, you can also specify another supported web browser available on the host where you start the Software Provisioning Manager. You can do this by starting the `sapinst` executable with command line option **`SAPINST_BROWSER=<Path to Browser Executable>`**, for example **`SAPINST_BROWSER=firefox.exe`**.
  Alternatively you can open a supported web browser on any device and run the URL from there.
  For more information about supported web browsers see Prerequisites for Running Software Provisioning Manager [page 57].
  If you need to run the **SL-UI** in **accessibility mode**, apply the standard accessibility functions of your web browser.
- As soon as you have started the `sapinst.exe` executable, the Software Provisioning Manager creates a `.sapinst` directory underneath the `<Drive>:\Users\<User>` directory where it keeps its logs and other technical files. `<User>` is the user which you used to start the Software Provisioning Manager.
  After you have reached the *Welcome* screen and selected the relevant Software Provisioning Manager option for the SAP system or instance to be installed , the Software Provisioning Manager creates a directory `sapinst_instdir`, where it keeps its logs and other technical files, and which is located directly in the `%ProgramFiles%` directory. If the Software Provisioning Manager is not able to create `sapinst_instdir` there, it tries to create `sapinst_instdir` in the directory defined by the `TEMP` environment variable.
  All log files which have been stored so far in the `.sapinst` folder are moved to the `sapinst_instdir` directory as soon as the latter has been created.
  The Software Provisioning Manager records its progress in the `keydb.xml` file located in the `sapinst_instdir` directory. Therefore, if required, you can continue with the Software Provisioning Manager from any point of failure, without having to repeat the already completed steps and without having to reenter the already processed input parameters. For security reasons, a variable encryption key

is generated as soon as the `sapinst_instdir` directory is created by the Software Provisioning Manager. This key is used to encrypt the values written to the `keydb.xml` file.

> → Recommendation
>
> We recommend that you keep all installation directories until the system is completely and correctly installed.

- The Software Provisioning Manager extracts itself to a temporary directory (`TEMP`, `TMP`, `TMPDIR`, or `SystemRoot`). These executables are deleted after the Software Provisioning Manager has stopped running.
  Directories called `sapinst_exe.xxxxxx.xxxx` sometimes remain in the temporary directory after the Software Provisioning Manager has finished. You can safely delete them.
  The temporary directory also contains the log file `dev_selfex.out` from the self-extraction process of the Software Provisioning Manager, which might be useful if an error occurs.

  > ⚠ Caution
  >
  > If the Software Provisioning Manager cannot find a temporary directory, the installation terminates with the error `FCO-00058`.

- To see a list of all available Software Provisioning Manager properties (command line options) and related documentation, open a command prompt and start the Software Provisioning Manager with command line parameter `-p`:
  ```
  sapinst -p
  ```

- If required, stop the Software Provisioning Manager by choosing the *Cancel* button.

  > ⓘ Note
  >
  > If you need to terminate the Software Provisioning Manager, choose *File* > *Exit* in the menu of the *Program Starter* window.

2.4.3.2 How to Avoid Automatic Logoff by Software Provisioning Manager

When you install the SAP system, the installation tool checks whether the user account used for the installation has the required privileges and authorization.

For a local or domain installation, the account needs to be a member of the local `Administrators` group.

For domain installations the account can be either a member of the `Domain Admins` group, or belongs to the `Domain Users` group and has the necessary rights to create/modify objects in the domain.

In both cases, the user account must be authorized to do the following:

- Act as part of the operating system
- Adjust memory quotas for a process
- Replace a process level token

If the user account does not have these rights assigned, the Software Provisioning Manager assigns them and automatically logs the account off to activate them. To avoid the software provisioning manager logging the account off, you can set these rights manually before you start the installation.

Procedure

You perform the following steps to assign these rights to the user account used for the installation.

> ⚠ Caution
>
> Be aware that domain policies override locally defined policies. This means that if you want to grant domain administrator rights to a user who belongs to the local `Administrators` group, make sure that you have also defined domain administrator rights for this user on domain level.

1. Press `Ctrl` + `Esc` and choose *Windows Tools* > *Computer Management* > *Local User and Groups* > *Administrators*.
2. Double-click the *Administrators* group.
3. In the *Administrators* window, choose the required user and choose *Add*.
   The selected user appears under *Members*.
4. Confirm your entry and then repeat the steps for each remaining policy that the user requires for the installation.
5. Log off and log on again to apply the changes.

Related Information

Required User Authorization for Running Software Provisioning Manager [page 46]

2.4.3.3 Restarting Interrupted Processing of Software Provisioning Manager

Here you find information about how to restart the Software Provisioning Manager if its processing has been interrupted.

Context

The processing of the Software Provisioning Manager might be interrupted for one of the following reasons:

- An error occurred during the *Define Parameters* or *Execute* phase:
  The Software Provisioning Manager does not terminate in error situations. If an error occurs, processing is paused and a dialog box appears. The dialog box contains a short description of the choices listed in the table below as well as a path to a log file that contains detailed information about the error.

- You interrupted the processing of the Software Provisioning Manager by choosing *Cancel* in the SL-UI.

> ⚠ Caution
>
> If you stop an option in the *Execute* phase, any system or component **processed** by this option is incomplete and not ready to be used. Any system or component **removed** by this option is not completely removed.

The following table describes the options in the dialog box:

Option	Definition
Retry	The Software Provisioning Manager retries the installation from the point of failure without repeating any of the previous steps. This is possible because the Software Provisioning Manager records its progress in the `keydb.xml` file. We recommend that you view the entries in the log files, try to solve the problem, and then choose *Retry*. If the same or a different error occurs, the Software Provisioning Manager displays the same dialog box again.
Stop	The Software Provisioning Manager stops the installation, closing the dialog box and the Software Provisioning Manager's SL-UI. The Software Provisioning Manager records its progress in the `keydb.xml` file. Therefore, you can continue with the Software Provisioning Manager from the point of failure without repeating any of the previous steps. See the procedure below.
Continue	The Software Provisioning Manager continues the installation from the current point.
View Log	Access installation log files.

The following procedure describes the steps to restart an installation, which you stopped by choosing *Stop*, or to continue an interrupted installation after an error situation.

Procedure

1. Log on to the host where Software Provisioning Manager is running as a user with the required permissions as described in Running Software Provisioning Manager [page 58] .
2. Make sure that the installation media are still available.

   For more information, see Preparing the Installation Media [page 51] .

   > → Recommendation
   >
   > Make the media available **locally**. For example, if you use remote file shares on other Windows hosts, CIFS shares on third-party SMB-servers, or Network File System (NFS), reading from media mounted with NFS might fail.

3. Restart the Software Provisioning Manager by double-clicking **`sapinst.exe`** from the directory to which you unpacked the Software Provisioning Manager archive.

   By default, the SL-UI uses the default browser defined for the host where you run the Software Provisioning Manager. However, you can also specify another supported web browser available on the host where you start the Software Provisioning Manager. You can do this by starting the `sapinst` executable with command line option **`SAPINST_BROWSER=<Path to Browser Executable>`**, for example **`SAPINST_BROWSER=firefox.exe`**.

4. The Software Provisioning Manager is restarting.

   If you have a supported web browser (see Prerequisites for Running Software Provisioning Manager [page 57]) installed on the host where you run the Software Provisioning Manager, the SL-UI starts automatically by displaying the *Welcome* screen.

   If the SL-UI does not open automatically, you can find the URL you require to access the SL-UI at the bottom of the *Program Starter* window of the Software Provisioning Manager. You find the icon of the *Program Starter* window in the taskbar of your Windows host. Open a supported web browser and run the URL from there.

```
...
************************************************************************
Open your browser and paste the following URL address to access the GUI
https://[<hostname>]:4237/sapinst/docs/index.html
Logon users: [<users>]
************************************************************************
...
```

> **Note**
>
> If the host specified by `<hostname>` cannot be reached due to a special network configuration, proceed as follows:
>
> 1. Terminate the Software Provisioning Manager as described in Useful Information about Software Provisioning Manager [page 62].
> 2. Restart the Software Provisioning Manager from the command line with the **`SAPINST_GUI_HOSTNAME=<hostname>`** property.
>   You can use a fully-qualified host name.

> **Caution**
>
> After opening the browser URL, make sure that the URL in the browser starts with “https://” to avoid security risks such as SSL stripping.
>
> Before you reach the *Welcome* screen, your browser warns you that the certificate of the `sapinst` process on this computer could not be verified.
>
> Proceed as follows to avoid security risks such as a man-in-the-middle attack:
>
> 1. Click on the certificate area on the left hand side in the address bar of your browser, and view the certificate.
> 2. Open the certificate fingerprint or thumbprint, and compare all hexadecimal numbers to the ones displayed in the console output of the Software Provisioning Manager.

Proceed as follows to get the certificate fingerprint or thumbprint from the server certificate printed in the Software Provisioning Manager console:

1. Go to the `sapinst_exe.xxxxxx.xxxx` directory in the temporary directory to which the Software Provisioning Manager has extracted itself: `%userprofile%\.sapinst\`
2. In the `sapinst_exe.xxxxxx.xxxx` directory, execute the `sapgenpse` tool with the command line option **`get_my_name -p`**.

As a result, you get the server fingerprint or thumbprint from the server certificate.

3. Accept the warning to inform your browser that it can trust this site, even if the certificate could not be verified.

The SL-UI opens in the browser by displaying the *Welcome* screen.

5. From the tree structure on the *Welcome* screen, select the installation option that you want to continue and choose *Next*.

   The *What do you want to do?* screen appears.

6. On the *What do you want to do?* screen, decide between the following alternatives and continue with *Next*:

Alternative	Behavior

Perform a new run	The Software Provisioning Manager does not continue the interrupted installation option. Instead, it moves the content of the old Software Provisioning Manager directory and all Software Provisioning Manager-specific files to a backup directory. Afterwards, you can no longer continue the old option.
	
	The following naming convention is used for the backup directory:
	
	`log_<Day>_<Month>_<Year>_<Hours>_<Minutes>_<Seconds>`
	
	Example
	`log_01_Oct_2016_13_47_56`
	
	Note
	All actions taken by the installation before you stopped it (such as creating directories or users) are not revoked.
	
	Caution
	The Software Provisioning Manager moves all the files and folders to a new log directory, even if these files and folders are owned by other users. If there are any processes currently running on these files and folders, they might no longer function properly.

Continue with the existing one	The Software Provisioning Manager continues the interrupted installation from the point of failure.

2.4.3.4 Using the Step State Editor (SAP Support Experts Only)

This section describes how to use the `Step State Editor` available in the Software Provisioning Manager.

> **Note**
>
> Only use the `Step State Editor` if the SAP Support requests you to do so, for example to resolve a case in SAP for Me.

Prerequisites

- SAP Support requests you to use the `Step State Editor`.
- Make sure that the host where you run the Software Provisioning Manager meets the requirements listed in Prerequisites for Running Software Provisioning Manager [page 57].

Procedure

1. Start the Software Provisioning Manager from the command line as described in Running Software Provisioning Manager [page 58] with the additional command line parameter **`SAPINST_SET_STEPSTATE=true`**
2. Follow the instructions on the Software Provisioning Manager screens and fill in the parameters prompted during the *Define Parameters* phase until you reach the *Parameter Summary* screen.
3. Choose *Next*.

   The `Step State Editor` opens as an additional dialog. Within this dialog you see a list of all steps to be executed by the Software Provisioning Manager during the *Execute Service* phase. By default all steps are in an initial state. Underneath each step, you see the assigned Software Provisioning Manager component. For each step you have a *Skip* and a *Break* option.

   - Mark the checkbox in front of the *Break* option of the steps where you want the Software Provisioning Manager to pause.
   - Mark the checkbox in front of the *Skip* option of the steps which you want the Software Provisioning Manager to skip.
4. After you have marked all required steps with either the *Break* or the *Skip* option, choose *OK* on the *Step State Editor* dialog.

   The Software Provisioning Manager starts processing the *Execute Service* phase and pauses one after another when reaching each step whose *Break* option you have marked. You can now choose one of the following:

   - Choose *OK* to continue with this step.
   - Choose *Step State Editor* to return to the `Step State Editor` and make changes, for example you can repeat the step by marking the checkbox in front of the *Repeat* option.

- Choose *Cancel* to abort the Software Provisioning Manager.

5. Continue until you have run through all the steps of the *Execute Service* phase of the Software Provisioning Manager.

2.4.3.5 Troubleshooting with Software Provisioning Manager

This section tells you how to proceed when errors occur while the Software Provisioning Manager is running.

Context

If an error occurs, the Software Provisioning Manager:

- Stops processing
- Displays a dialog informing you about the error

Procedure

1. Check SAP Note SAP Note 3207613 (*SAPinst Framework 753 Central Note*) for known Software Provisioning Manager issues.
2. If an error occurs during the *Define Parameters* or the *Execute Service* phase, do one of the following:
   - Try to solve the problem:
     - To check the Software Provisioning Manager log files (`sapinst.log` and `sapinst_dev.log`) for errors, choose the *LOG FILES* tab.

       > **Note**
       >
       > The *LOG FILES* tab is only available if you have selected on the *Welcome* screen the relevant Software Provisioning Manager option for the SAP product to be installed .
       >
       > If you need to access the log files before you have done this selection, you can find the files in the `.sapinst` directory underneath the `<Drive>:\Users\<User>` directory, where `<User>` is the user that you used to start the Software Provisioning Manager.
       >
       > For more information, see Useful Information about Software Provisioning Manager [page 62].

     - To check the log and trace files of the Software Provisioning Manager's SL-UI for errors, go to the directory `%userprofile%\.sapinst\`
     - Then continue by choosing *Retry*.
   - If required, abort the Software Provisioning Manager by choosing *Cancel* in the tool menu and restart the Software Provisioning Manager. For more information, see Restarting Interrupted Processing of Software Provisioning Manager [page 64].

3. If you cannot resolve the problem, report a case in SAP for Me using the appropriate subcomponent of BC-INS*.

   For more information about using subcomponents of BC-INS*, see SAP Note 1669327.

2.4.4 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 you use a 64-bit Java SE 21.
- 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*.

2.5 Post-Installation Tasks

This section describes the post-installation tasks, which are required before using SAP Identity Management components.

Once you install the SAP Identity Management system, check the post-installation checklist for the required post-installation tasks and perform the initial configuration of SAP Identity Management components.

Related Information

Post-Installation Checklist [page 71]

2.5.1 Post-Installation Checklist

This section describes how you perform post-installation tasks related to separate SAP Identity Management components step by step.

Core Components Tasks

The SAP Identity Management Core component is installed.

Proceed as follows:

1. To use the configuration packages, database scripts and some additional components, you need to unpack the Core component [page 73].
2. To proceed with some SAP Identity Management database post-installation activities, see the relevant documentation for your database system:
   - Identity Management Database on Microsoft SQL Server [page 74]
   - Identity Management Database on Oracle [page 88]
   - Identity Management Database on IBM DB2 [page 94]
   - Identity Management Database on SAP ASE [page 99]

3. You can also create and maintain the encryption key(s) and the Keys.ini file [page 110]

Runtime Components Tasks

The initial dispatcher is created and started with the <sapsid>adm user. It is set as the default dispatcher. You can manage the initial dispatcher, as described in Creating and Managing the Dispatcher(s) [page 121]

In case you need to create additional dispatchers, proceed as follows:

1. Set the JAVA_HOME environment variable for the `<sapsid>adm` user to point to `<drive>:\usr\sap\<SAPSID>\IDM<No>\exe\sapjvm_<No>`. Use the `<sapsid>adm` user to start the dispatcher utility and to create and manage dispatchers.
2. Creating and Configuring Dispatchers [page 115]

If you want to use the SAP Java Connector that is included in the installation of the Runtime Components for Microsoft Windows, see Using the SAP Java Connector (JCo) [page 126]

SAP Identity Management Developer Studio Tasks

The SAP Identity Management Developer Studio service is deployed on your SAP NetWeaver AS Java. You need to have also the Identity Management Developer Studio client installed manually on every developer or developer administrator machine as described in Installing the Identity Management Developer Studio [page 70]

Proceed as follows:

1. Define the JDBC connection for Identity Management Developer Studio service [page 127].
2. Configure the Java system properties [page 131] of the deployed Identity Management Developer Studio service on your SAP NetWeaver AS Java.
3. Use and configure the HTTP security (SSL) [page 134] to ensure the security between the deployed Identity Management Developer Studio service and the Identity Management Developer Studio client.
4. Perform the initial configuration of Identity Management Developer studio [page 137].
    1. Creating the Developer Administrator User in UME [page 140]
    2. Add the initial identity store [page 142]

SAP Identity Management User Interface Tasks

The SAP Identity Management User Interface is deployed on your SAP NetWeaver AS Java.

Proceed as follows:

1. Define the JDBC connection for the JMX layer [page 142].
2. Configure the JMX layer [page 147] to change settings, like configuring the cache, defining which identity store you are working on and configuring the encryption key-file.

3. Perform initial configuration of Identity Management User Interface [page 154] to add user(s) to the identity store, to give access to *Self Services* and *Monitoring* tab, to configure the language settings and others.
4. Customize Web Dynpro Java applications [page 171] to define a specific theme (the look and feel) of your User Interface application and create and activate keyboard access for User Interface elements.
5. (Optionally) Integrate Identity Management User Interface in the SAP Enterprise Portal [page 172]

SAP Identity Management User Interface for HTML5 Tasks

The SAP Identity Management User Interface for HTML5 is deployed on your SAP NetWeaver AS Java.

Proceed as follows:

1. Perform initial configuration of Identity Management User Interface for HTML5 [page 175] to be able to access the Identity Management User Interface for HTML5, to add the predefined forms in the Identity Management Developer Studio and others.

Virtual Directory Server Tasks

The Virtual Directory Server is installed.

Proceed as follows:

1. Set the JAVA_HOME environment variable for the `<sapsid>adm` user to point to `<drive>:\usr\sap\<SAPSID>\IDM<No>\exe\sapjvm_<No>`. Use the `<sapsid>adm` user to run the `Virtual Directory Server.bat` file.
2. Start the Virtual Directory Server [page 184]
3. Perform initial configuration of Identity Management Virtual Directory Server [page 185]

2.5.2 Unpacking the Core Component

Context

After installing SAP Identity Management with the Software Provisioning Manager, you need to unpack the Core component (`ICCORE.SAR`) using the SAPCAR archiving tool. The Core component contains the following:

- Configuration packages that contain SAP Identity Management frameworks and connectors
- Database scripts needed for post-installation activities
- Password Hook `setup.exe` file
- Additional Components

Procedure

1. Open a command prompt and navigate to the directory where you want to unpack the Core component.
2. Execute the following command:

```
<Path to SAPCAR>\sapcar.exe -xvf <Path to Download
Directory>\ICCORE<Support_Package_Number>_<Version_Number>.SAR
```

Results

You have unpacked the Core component. To use the configuration packages, proceed with importing them in the SAP Identity Management Developer Studio. See: Importing the Provisioning Framework for SAP Identity Management 8.0

2.5.3 Identity Management Database on Microsoft SQL Server

After installing the Identity Management database on Microsoft SQL Server, you can perform the following post-installation activities:

- Create additional logins
- Enable full-text search
- Enable or disable the 7.2 approval mechanism
- Create additional developer administrator
- Remove the Identity Management database on Microsoft SQL Server

Proceed as follows:

1. Unpack the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool. The Core component contains the database scripts you need to perform those post-installation activities. See Unpacking the Core Component [page 73]
2. Run the scripts as described in the sections below.

Related Information

Database Script Files [page 75]
Creating Additional Logins [page 77]
Enabling Full-Text Search [page 77]
Enabling or Disabling the 7.2 Approval Mechanism [page 81]
Creating Additional Developer Administrator [page 85]
Removing Identity Management Database on Microsoft SQL Server [page 87]

2.5.3.1 Database Script Files

The Identity Management database script files are included in the installation kit for the `Core` component. After installation, the script files are located in the `/DatabaseSchema/SQL-Server` folder.

> **Note**
>
> The script files need write access to the folder from where they are run, so if the installation kit is located on a CD or another read-only location, copy the folder with the database scripts to a location with write access before you run them.

> **Note**
>
> Do not run the scripts directly from Microsoft Windows Explorer. Open the command prompt and navigate to the installation folder of the database, and run the scripts from here.

> **Note**
>
> If you have installed a default SAP installation of Microsoft SQL Server, the `sa` user will be disabled with a random password. You need to enable the `sa` user and set a password in the SQL Server Management Studio.

You can use the following scripts:

Utility Script Files

Script	Description	Parameters
`mxmc-versions.cmd`	Lists all databases defined on the database server including version number for the Identity Management databases.	Runs as `sa` (system administrator) Run the script without parameters to see what is required.
`mxmc-enable-fulltext.cmd`	Enables full-text search on an Identity Management database.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-xenable-fulltext.cmd`	Enables full-text search on an Identity Management database with a given prefix.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-enable-72-approvals.cmd`	Enables the 7.2 approval mechanism for an Identity Management database.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-disable-72-approvals.cmd`	Disables the 7.2 approval mechanism for an Identity Management database.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.

Script	Description	Parameters
`mxmc-xenable-72-approvals.cmd`	Enables the 7.2 approval mechanism for an Identity Management database with a given prefix.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-xdisable-72-approvals.cmd`	Disables the 7.2 approval mechanism for an Identity Management database with a given prefix.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-create-dev-admin.cmd`	Creates an (additional) *Developer Administrator*. This is normally done from the Identity Management Developer Studio, but in cases where this is not possible, a *Developer Administrator* with a script. **Note** This user must either exist in the UME or be added to the UME before you can log on to the Identity Management Developer Studio.	Runs as `<prefix>_oper`.
`mxmc-xcreate-dev-admin.cmd`	Creates an (additional) *Developer Administrator* for an Identity Management database with a given prefix. This is normally done from the Identity Management Developer Studio, but in cases where this is not possible, a *Developer Administrator* with a script. **Note** This user must either exist in the UME or be added to the UME before you can log on to the Identity Management Developer Studio.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.

Database Script Files

Script	Description	Parameters
`mxmc-remove.cmd`	Removes an Identity Management database. Calls the script `mxmc-xremove.cmd` with default values for database prefix, host name and user name (`sa`).	The script prompts for the passwords for `sa`.

Script	Description	Parameters
`mxmc-xremove.cmd`	Removes an Identity Management database with a given prefix. Requires the parameters database prefix, host name, user name (`sa`) and password.	Runs as `sa` (system administrator) Run the script without parameters to see what is required.

2.5.3.2 Creating Additional Logins

You may want to create additional logins or rename the default logins created by the installation scripts. To do this, you can modify the `1-create-db.sql` script.

Context

> ⓘ Note
>
> If you want to add logins after installation of the Identity Management database, you can do this using the database's administrative tools. Make sure that you assign the correct roles. Run the script using a SQL Query execution tool (native tools like SQL*Plus or SQL Server Native Client for example).

Procedure

1. Open the `1-create-db.sql` script in a text editor.
2. Modify or add the logins in the file.
3. Save the file.

2.5.3.3 Enabling Full-Text Search

You can enable full-text search in the Identity Management database. The full-text search will then be available in the Identity Management User Interface.

The full-text search is enabled by running the script described below. If you run the script on a large database, it might take some time to complete. For performance reasons, you should disable full-text search while performing a bulk load in the database. This is done by stopping the *SQL Server FullText Search* service in the *Control Panel* (*Administrative Tools/Services*) before performing the bulk load and enabling it again once the bulk load is complete.

The full-text index is created with the language defined for the database server. If you need to set another language for the full-text index, use the database tool to create the full-text index, where you can specify the language option.

For details about administration and usage of the full-text search, see the documentation for the Microsoft SQL Server.

Related Information

Enabling Full-Text Search on an Identity Management Database [page 78]
Enabling Full-Text Search for an Identity Management Database with a Given Prefix [page 79]
Configuring the Stop Word List [page 79]

2.5.3.3.1 Enabling Full-Text Search on an Identity Management Database

Context

To enable full-text search, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the command file `mxmc-enable-fulltext.cmd`.

   You are prompted for the password for `mxmc_oper`.

   Full-text is enabled on the database.
3. Close the command prompt window.

2.5.3.3.2 Enabling Full-Text Search for an Identity Management Database with a Given Prefix

Context

To enable full-text search, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the command file `mxmc-xenable-fulltext.cmd`. The parameters to the command file are:
   - Host name of the server running the Microsoft SQL Server
   - Prefix of the Identity Management database
   - User name for `<prefix>_oper`
   - Optional: Password for `prefix_oper`

   Full-text is enabled on the database.
3. Close the command prompt window.

2.5.3.4 Configuring the Stop Word List

Context

The stop word (noise word) list is a list that contains words that are not indexed. These are words like "a", "the", "or", which should not be included in searches. Most of the words in this list do not affect searches in the Identity Management User Interface. An exception is the naming of privileges with the word "only", as this is also considered a stop word. To be able to search for privileges with names containing the word "only", the stop word list has to be be modified.

> **Note**
>
> Make sure that you modify the stop word list for all relevant languages.

Microsoft SQL Server 2008 and higher uses stop words stored in the database. To customize the list, proceed as follows:

Procedure

1. Make a copy of the system stop word list.
2. Assign it for use with the full-text index (ftfull) for SAP Identity Management. This can be done using these commands or from the SQL Server Management Studio user interface.

```
CREATE FULLTEXT STOPLIST idmStopList FROM SYSTEM STOPLIST
-- Remove the words you want to include in the index:
ALTER FULLTEXT STOPLIST idmStopList DROP 'only' LANGUAGE 1033
ALTER FULLTEXT INDEX ON mxi_values SET STOPLIST idmStopList
```

2.5.3.4.1 Querying the Stop Word List

You can also view stop words using queries. This example shows listing languages blocking the word "only".

To list all entries of 'only' stop words in the stoplist (can be many languages), enter the following code:

```
SELECT * FROM sys.fulltext_stopwords WHERE stoplist_id = (SELECT stoplist_id FROM
sys.fulltext_stoplists where name = 'idmStopList') and stopword = 'only'
```

The result is displayed like this:

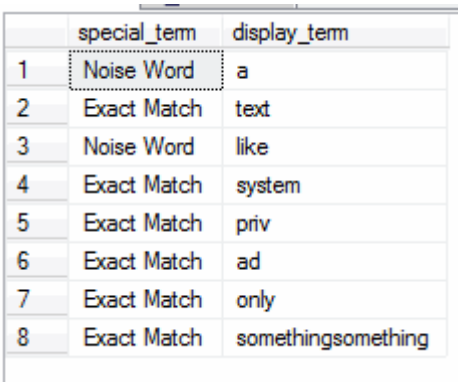
Results | Messages

	stoplist_id	stopword	language	language_id
1	7	only	British English	2057
2	7	only	Simplified Chinese	2052
3	7	only	Thai	1054
4	7	only	Japanese	1041
5	7	only	Traditional Chinese	1028
6	7	only	Neutral	0

You can also test how a string will be interpreted by the full text indexing engine by entering the following code:

```
SELECT special_term, display_term FROM sys.dm_fts_parser (' "a text like system
priv ad
only somethingsomething" ', 1033,(SELECT stoplist_id FROM sys.fulltext_stoplists
where
name = 'idmStopList'), 0)
```

The result is displayed like this:



	special_term	display_term
1	Noise Word	a
2	Exact Match	text
3	Noise Word	like
4	Exact Match	system
5	Exact Match	priv
6	Exact Match	ad
7	Exact Match	only
8	Exact Match	somethingsomething

2.5.3.5 Enabling or Disabling the 7.2 Approval Mechanism

The 7.2 approval mechanism was introduced with SAP NetWeaver Identity Management 7.2 SP4. This mechanism is enabled by default for new installations, as well as for updates to a higher SP or patch level and upgrades from version 7.2 to 8.0. It is also possible to disable the 7.2 approval mechanism.

The 7.2 approval mechanism provides:

- Improved performance
- New functionality:
  - Escalations
  - Multi-approver
- Enhanced Identity Management User Interface (optional)
  - Show history
  - More information

When you run the script to enable the 7.2 approval mechanism, it will:

- Turn on the 7.2 approval mechanism.
- Convert any pending approvals to the new format.
- Enable the properties to configure the new approval mechanism on the approval task in Identity Management Developer Studio.

> ⓘ Note
>
> If you run the database scripts for enabling/disabling the 7.2 approval mechanism when it is already enabled or disabled, you will receive a message, and the script will not perform any updates.

2.5.3.5.1 Enabling the 7.2 Approval Mechanism

Context

To enable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers that are currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.
3. Run script `mxmc-enable-72-approvals.cmd`. You are prompted to enter the password for `mxmc_oper`.
4. Start the dispatchers.

2.5.3.5.2 Enabling the 7.2 Approval Mechanism on a Database with a Given Prefix

Context

To enable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers that are currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.
3. Run script `mxmc-xenable-72-approvals.cmd`. The parameters to the command file are:
   - Host name of the server running the Microsoft SQL Server
   - Prefix of the Identity Management database
   - User name for `<prefix>_oper`
   - Optional: Password for `<prefix>_oper`
4. Start the dispatchers.

2.5.3.5.3 Disabling the 7.2 Approval Mechanism

Context

To disable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.
3. Run the script `mxmc-disable-72-approvals.cmd`. You are prompted for the password for `mxmc_oper`.
4. Start the dispatchers.

Results

The 7.2 approval mechanism is disabled.

> **Note**
>
> Since this mechanism is enabled by default for new installations, updates to a higher SP or patch level and upgrades to version 8.0, if you want to keep it disabled, you need to run the script again.

2.5.3.5.4 Disabling the 7.2 Approval Mechanism on a Database with a Given Prefix

Context

To disable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers currently running .
2. Open a command prompt and navigate to the directory where the database installation scripts are located.
3. Run the script `mxmc-xdisable-72-approvals.cmd`. The parameters to the command file are:
   - Host name of the server running the Microsoft SQL Server
   - Prefix of the Identity Management database
   - User name for `<prefix>_oper`
   - Optional: Password for `<prefix>_oper`
4. Start the dispatchers.

Results

The 7.2 approval mechanism is disabled.

> ⓘ Note
>
> Since this mechanism is enabled by default for new installations, updates to a higher SP or patch level and upgrades to version 8.0, if you want to keep it disabled, you need to run the script again.

2.5.3.6 Creating Additional Developer Administrator

Context

The initial *Developer Administrator* is created when the database is installed, and other users are added using Identity Management Developer Studio. If the *Developer Administrator* has lost access to Identity Management Developer Studio, you can run a script that creates a *Developer Administrator*.

> **Note**
>
> This user must either exist in the UME or be added to the UME before you can log on to Identity Management Developer Studio.

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the command file `mxmc-create-dev-admin.cmd`. You are prompted to provide the following information:
   - Password for `mxmc_oper`
   - The name of the *Developer Administrator*.
3. Close the command prompt window.

Next Steps

The user must also exist in UME to be able to log on to Identity Management Developer Studio.

Related Information

Creating the Developer Administrator User in UME [page 140]
SAP Identity Management Security Guide

2.5.3.7 Creating Additional Developer Administrator for a Database with a Given Prefix

Context

The initial *Developer Administrator* is created when the database is installed, and other users are added using Identity Management Developer Studio. If the *Developer Administrator* has lost access to Identity Management Developer Studio, you can run a script that creates a *Developer Administrator*.

> **Note**
>
> This user must either exist in the UME or be added to the UME before you can log on to Identity Management Developer Studio.

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the command file `mxmc-xcreate-dev-admin.cmd`. The parameters to the command file are as follows:
   - Host name of the server running the Microsoft SQL Server
   - Prefix of the Identity Management database
   - User name for `<prefix>_oper`
   - Optional: Password for `<prefix>_oper`
   - The name of the *Developer Administrator* for this database.
3. Close the command prompt window.

Next Steps

The user must also exist in UME to be able to log on to Identity Management Developer Studio.

Related Information

Creating the Developer Administrator User in UME [page 140]
SAP Identity Management Security Guide

2.5.3.8 Removing Identity Management Database on Microsoft SQL Server

Context

> ⓘ Note
>
> It is not possible to revert this function, so make sure that the correct database name is referenced in the script.

To remove an Identity Management database, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the `mxmc-remove.cmd` command file.

   You are prompted to enter the password for `sa`.
3. Close the command prompt window.

2.5.3.9 Removing Identity Management Database with a Given Prefix on Microsoft SQL Server

Context

> ⓘ Note
>
> It is not possible to revert this function, so make sure that you specify the correct database name.

To remove an Identity Management database, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.

2. Run the `mxmc-xremove.cmd` command file. The parameters to the command file are:
   - Host name of the server running the Microsoft SQL Server
   - Prefix of the Identity Management database
   - User name for `sa`
   - Optional: Password for `sa`
3. Close the command prompt window.

2.5.4 Identity Management Database on Oracle

After installing the Identity Management database on Oracle, you can perform the following post-installation activities:

- Create additional users
- Enable or disable the 7.2 approval mechanism
- Create additional developer administrator
- Remove the Identity Management database on Oracle

Proceed as follows:

1. Unpack the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool. The Core component contains the database scripts you need to perform those post-installation activities. See Unpacking the Core Component [page 73]
2. Define the parameters in the `include.sql` configuration file that is unpacked with the Core component. The parameters include the database prefix (The default <prefix> is MXMC. We recommend using uppercase alphanumeric values (A-Z, 0-9) for the prefix), JDBC connection parameters, database user passwords and others.

   > **Note**
   >
   > In the `include.sql` file, the commented-out code is considered as an executable code. Comments are ignored by the Identity Management installation procedure.

3. Run the scripts as described in the sections below.

Related Information

Database Script Files [page 89]
Creating Additional Users [page 90]
Enabling and Disabling the 7.2 Approval Mechanism [page 90]
Creating Additional Developer Administrator [page 92]
Removing Identity Management Database on Oracle [page 93]

2.5.4.1 Database Script Files

The Identity Management database script files are included in the installation kit for the `Core` component. After installation, the script files are located in the `/DatabaseSchema/Oracle` folder.

> **Note**
>
> All the scripts in that folder should have execute permission. In addition, the script files need write access to the folder where they are run from, so if the installation kit is located on a CD or another read-only location, copy the folder with the database scripts to a location with write access before running them.

You can use the following scripts:

Utility Script Files

Script	Description	Parameters
`mxmc-enable-72-approvals.cmd`	Enables the 7.2 approval mechanism for an Identity Management database. See Enabling the 7.2 Approval Mechanism [page 91]	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-disable-72-approvals.cmd`	Disables the 7.2 approval mechanism for an Identity Management database. See Disabling the 7.2 Approval Mechanism [page 91]	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-create-dev-admin.cmd`	Creates an (additional) *Developer Administrator*. See Creating Additional Developer Administrator [page 92] This is normally done from Identity Management Developer Studio, but if this is not possible, a *Developer Administrator* is created with a script. **Note** This user must either exist in the UME or be added to it before you can log on to Identity Management Developer Studio.	Runs as `<prefix>_oper`.

Database Script Files

Script	Description	Parameters
`mxmc-remove.cmd`	Removes an Identity Management database. See Removing Identity Management Database on Oracle [page 93]	The script prompts for the passwords for `SYSTEM user`.

2.5.4.2 Creating Additional Users

Prerequisites

You have unpacked the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool. Thus, you will unpack the `2-create-users.sql` script.

Context

You might want to create other users or rename the default users created by the installation scripts. You can do this by modifying the `2-create-users.sql` script.

> ⓘ Note
>
> Make sure that you assign the correct roles to the users.

If you want to add users after installation of the Identity Management database, you can do this using the database's administrative tools.

2.5.4.3 Enabling and Disabling the 7.2 Approval Mechanism

The 7.2 approval mechanism was introduced with SAP NetWeaver Identity Management 7.2 SP4. This mechanism is enabled by default for new installations, as well as for updates to a higher SP or patch level and upgrades from version 7.2 to 8.0. It is also possible to disable the 7.2 approval mechanism.

The 7.2 approval mechanism provides:

- Improved performance
- New functionality:
  - Escalations
  - Multi-approver
- Enhanced Identity Management User Interface (optional)
  - Show history
  - More information

When you run the script to enable the 7.2 approval mechanism, it will:

- Activate the 7.2 approval mechanism.
- Convert any pending approvals to the new format.
- Enable the properties to configure the new approval mechanism on the approval task in Identity Management Developer Studio.

> **Note**
>
> If you run the database scripts for enabling/disabling the 7.2 approval mechanism when it is already enabled or disabled, you will receive a message, and the script will not perform any updates.

2.5.4.3.1 Enabling the 7.2 Approval Mechanism

Prerequisites

You have unpacked the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool.

You have defined the parameters in the `include.sql` configuration file.

Context

To enable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers that are currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.

   Make sure you have the same `include.sql` file as you used during installation.
3. Run script `mxmc-enable-72-approvals.cmd`. You are prompted to enter the password for `mxmc_oper`.
4. Start the dispatchers.

2.5.4.3.2 Disabling the 7.2 Approval Mechanism

Prerequisites

You have unpacked the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool.

You have defined the parameters in the `include.sql` configuration file.

Context

To disable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.

   Make sure that you have the same `include.sql` file as you used during installation.
3. Run script `mxmc-disable-72-approvals.cmd`. You are prompted for the password for `mxmc_oper`.
4. Start the dispatchers.

Results

The 7.2 approval mechanism is disabled.

> **Note**
>
> Since this mechanism is enabled by default for new installations, updates to a higher SP or patch level and upgrades to version 8.0, if you want to keep it disabled, you need to run the script again.

2.5.4.4 Creating Additional Developer Administrator

Prerequisites

You have unpacked the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool.

You have defined the parameters in the `include.sql` configuration file.

Context

The initial *Developer Administrator* is created when the database is installed, and other users are added using Identity Management Developer Studio. If the *Developer Administrator* has lost access to Identity Management Developer Studio for some reason, you can run a script that creates a *Developer Administrator*.

> **Note**
>
> This user must either exist in the UME or be added to the UME before you can log on to Identity Management Developer Studio.

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run script `mxmc-create-dev-admin.cmd`. You are prompted to provide the following information:
   - Password for `mxmc_oper`
   - The name of the *Developer Administrator*.
3. Close the command prompt window.

Next Steps

The user must also exist in UME to be able to log on to Identity Management Developer Studio.

Related Information

Creating the Developer Administrator User in UME [page 140]
SAP Identity Management Security Guide

2.5.4.5 Removing Identity Management Database on Oracle

Prerequisites

You have unpacked the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool.

You have defined the parameters in the `include.sql` configuration file.

Context

> **Note**
>
> It is not possible to revert this function, so make sure that the correct database name is referenced in the script.

To remove an Identity Management database, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory containing the Identity Management database script files.
2. Run command file `mxmc-remove.cmd`. You are prompted to enter the system password.

   You can check log file `mxmc-update.log` for any warnings or errors.
3. Close the command prompt window.

2.5.5 Identity Management Database on IBM DB2

After installing the Identity Management database on IBM DB2, you can perform the following post-installation activities:

- Create additional users
- Remove the Identity Management database on IBM DB2

Proceed as follows:

1. Unpack the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool. The Core component contains the database scripts you need to perform those post-installation activities. See Unpacking the Core Component [page 73]
2. Define the parameters in the `include.sql` configuration file that is unpacked with the Core component. The parameters include the database prefix (We recommend using uppercase alphanumeric values (A-Z, 0-9) for the prefix. When using IBM DB2, make sure that the length of the prefix does not exceed two characters, for example, 'IC' (on Windows), JDBC connection parameters, database user passwords and others.

   > **Note**
   >
   > In the `include.sql` file, the commented-out code is considered as an executable code. Comments are ignored by the Identity Management installation procedure.
3. Run the scripts as described in the sections below.

Related Information

Database Script Files [page 95]
Creating Additional Users [page 96]
Removing Identity Management Database on IBM DB2 [page 99]

2.5.5.1 Database Script Files

The Identity Management database script files are included in the installation kit for the `Core` component. After installation, the script files are located in the `/DatabaseSchema/DB2` folder.

> **Note**
>
> All the scripts in that folder should have execute permission. In addition, the script files need write access to the folder from where they are run. If the installation kit is located on a CD or another read-only location, you therefore have to copy the folder with the database scripts to a location with write access before running them.

> **Note**
>
> Take care when editing shell scripts (.sh files) in Windows format. Make sure the shell scripts are saved in Unix format.

You can use the following scripts:

Utility Script Files

Script	Description	Account (run as)
`mxmc-create-dev-admin.cmd`	Creates an (additional) Developer Administrator. This is normally done from the Identity Management Developer Studio, but in cases where this is not possible, a *Developer Administrator* is created with a script. **Note** This user must either exist in the UME or be added to the UME before you can log on to the Identity Management Developer Studio.	Runs as `<prefix>_oper`.

Script	Description	Account (run as)
`mxmc-enable-72-approvals.cmd`	Enables the 7.2 approval mechanism for an Identity Management database.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-disable-72-approvals.cmd`	Disables the 7.2 approval mechanism for an Identity Management database.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.

Database Script Files

Script	Description	Account (run as)
`mxmc-remove.cmd`	Removes an Identity Management database.	<prefix>_oper

> **Note**
>
> The value substituting <prefix> is defined in the `include.sql` file.

2.5.5.2 Creating Additional Users

You might want to create other users or rename the default users created by the installation scripts.

On Microsoft Windows, you can use the following Windows PowerShell scripts:

- CreateLocalUser.ps1
- AddLocalUserToGroup.ps1
- DeleteLocalUser.ps1

Make sure that you assign the correct roles to the users. For information about how to do this, see the `2-create-roles.sql` script file.

2.5.5.3 Enabling and Disabling the 7.2 Approval Mechanism

The 7.2 approval mechanism was introduced with SAP NetWeaver Identity Management 7.2 SP4. This mechanism is enabled by default for new installations, as well as for updates to a higher SP or patch level and upgrades from version 7.2 to 8.0. It is also possible to disable the 7.2 approval mechanism.

The 7.2 approval mechanism provides:

- Improved performance
- New functionality:
  - Escalations
  - Multi-approver

- Enhanced Identity Management User Interface (optional)
  - Show history
  - More information

When you run the script to enable the 7.2 approval mechanism, it will:

- Activate the 7.2 approval mechanism.
- Convert any pending approvals to the new format.
- Enable the properties to configure the new approval mechanism on the approval task in Identity Management Developer Studio.

> **Note**
>
> If you run the database scripts for enabling/disabling the 7.2 approval mechanism when it is already enabled or disabled, you will receive a message, and the script will not perform any updates.

2.5.5.3.1 Enabling the 7.2 Approval Mechanism

Prerequisites

You have unpacked the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool.

You have defined the parameters in the `include.sql` configuration file.

Context

To enable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers that are currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.

   Make sure you have the same `include.sql` file as you used during installation.
3. Run script `mxmc-enable-72-approvals.cmd`. You are prompted to enter the password for `mxmc_oper`.
4. Start the dispatchers.

2.5.5.3.2 Disabling the 7.2 Approval Mechanism

Prerequisites

You have unpacked the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool.

You have defined the parameters in the `include.sql` configuration file.

Context

To disable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.

   Make sure that you have the same `include.sql` file as you used during installation.
3. Run script `mxmc-disable-72-approvals.cmd`. You are prompted for the password for `mxmc_oper`.
4. Start the dispatchers.

Results

The 7.2 approval mechanism is disabled.

> **Note**
>
> Since this mechanism is enabled by default for new installations, updates to a higher SP or patch level and upgrades to version 8.0, if you want to keep it disabled, you need to run the script again.

2.5.5.4 Removing Identity Management Database on IBM DB2

Context

> **Note**
>
> It is not possible to revert this function, so make sure that the correct database name is referenced in the script.

To remove an Identity Management database, proceed as follows:

Procedure

1. For **Microsoft Windows:** Open the IBM DB2 command window. From the Start menu, choose *IBM DB2/<Database>/Command window - Administrator*.
2. Navigate to the directory containing the Identity Management script files.
3. Run the `mxmc-remove.cmd` command file. You are prompted to enter the system password.
   You can check the `mxmc-update.log` log file for warnings or errors.
4. Close the command prompt window.

   In Microsoft Windows, the default operating system users will also be removed.

2.5.6 Identity Management Database on SAP ASE

.

After installing the Identity Management database on SAP ASE, you can perform the following post-installation activities:

- Create additional logins
- Enable or disable the 7.2 approval mechanism
- Create additional developer administrator
- Remove the Identity Management database on SAP ASE

Proceed as follows:

1. Unpack the Core component (ICCORE.SAR) in a dedicated directory using the SAPCAR archiving tool. The Core component contains the database scripts you need to perform those post-installation activities. See Unpacking the Core Component [page 73]
2. Run the scripts as described in the sections below.

Related Information

Database Script Files [page 100]
Creating Aditional Logins [page 102]
Enabling or Disabling the 7.2 Approval Mechanism [page 103]
Creating an Additional Developer Administrator [page 107]
Removing Identity Management Database on SAP ASE [page 109]

2.5.6.1 Database Script Files

The Identity Management database script files are included in the installation kit for the `Core` component. After installation, the script files are located in the `/DatabaseSchema/ASE` folder.

> **Note**
>
> All the scripts in that folder should have execute permission. In addition, the script files need write access to the folder from where they are run, so if the installation kit is located on a CD or another read-only location, copy the folder with the database scripts to a location with write access before you run them.

> **Note**
>
> Do not run the scripts directly from Microsoft Windows Explorer. Open the command prompt and navigate to the installation folder of the database, and run the scripts from here.

> **Note**
>
> The isql command line tool must be installed on the machine where the scripts are executed. This is required for the SAP Identity Management scripts to function properly. The isql command line tool is provided either with the ASE server installation or with the ASE OpenServer client which is a part of the ASE SDK Suite.

You can use the following scripts:

Utility Script Files

Script	Description	Parameters
`mxmc-test.cmd`	Tests the connection to the database server. The output is a list of databases.	Runs as `sa` (system administrator) Run the script without parameters to see what is required.
`mxmc-versions.cmd`	Lists all databases defined on the database server including version number for the Identity Management databases.	Runs as `sa` (system administrator) Run the script without parameters to see what is required.

Script	Description	Parameters
`mxmc-enable-72-approvals.cmd`	Enables the 7.2 approval mechanism for an Identity Management database.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-disable-72-approvals.cmd`	Disables the 7.2 approval mechanism for an Identity Management database.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-xenable-72-approvals.cmd`	Enables the 7.2 approval mechanism for an Identity Management database with a given prefix.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-xdisable-72-approvals.cmd`	Disables the 7.2 approval mechanism for an Identity Management database with a given prefix.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-create-dev-admin.cmd`	Creates an (additional) *Developer Administrator*. This is normally done from the Identity Management Developer Studio, but in cases where this is not possible, a *Developer Administrator* with a script. **Note** This user must either exist in the UME or be added to the UME before you can log on to the Identity Management Developer Studio.	Runs as `<prefix>_oper`.
`mxmc-xcreate-dev-admin.cmd`	Creates an (additional) *Developer Administrator* for an Identity Management database with a given prefix. This is normally done from the Identity Management Developer Studio, but in cases where this is not possible, a *Developer Administrator* with a script. **Note** This user must either exist in the UME or be added to the UME before you can log on to the Identity Management Developer Studio.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.

Database Script Files

Script	Description	Parameters
`mxmc-remove.cmd`	Removes an Identity Management database. Calls the script `mxmc-xremove.cmd` with default values for database prefix, host name and user name (`sa`).	The script prompts for the passwords for `sa`.
`mxmc-xremove.cmd`	Removes an Identity Management database with a given prefix. Requires the parameters database prefix, host name, user name (`sa`) and password.	Runs as `sa` (system administrator) Run the script without parameters to see what is required.

2.5.6.2 Creating Aditional Logins

Context

You may want to create additional logins or rename the default logins created by the installation scripts. To do this, you can modify the `1-create-db.sql` script. It is used to set the default settings when creating the database. For example, max memory, number of user connections and so on.

> **Note**
>
> If you want to add logins after installation of the Identity Management database, you can do this using the database's administrative tools. Make sure that you assign the correct roles. Run the script using an SQL Query execution tool (native tools like isql, for example). In ASE Windows version, you can also use a graphic tool Interactive SQL.

Procedure

1. Open the `1-create-db.sql` script in a text editor.
2. Modify or add the logins in the file.
3. Save the file.

2.5.6.3 Enabling or Disabling the 7.2 Approval Mechanism

The 7.2 approval mechanism was introduced with SAP NetWeaver Identity Management 7.2 SP4. This mechanism is enabled by default for new installations, as well as for updates to a higher SP or patch level and upgrades from version 7.2 to 8.0. It is also possible to disable the 7.2 approval mechanism.

The 7.2 approval mechanism provides:

- Improved performance
- New functionality:
  - Escalations
  - Multi-approver
- Enhanced Identity Management User Interface (optional)
  - Show history
  - More information

When you run the script to enable the 7.2 approval mechanism, it will:

- Turn on the 7.2 approval mechanism.
- Convert any pending approvals to the new format.
- Enable the properties to configure the new approval mechanism on the approval task in Identity Management Developer Studio.

> ⓘ Note
>
> If you run the database scripts for enabling/disabling the 7.2 approval mechanism when it is already enabled or disabled, you will receive a message, and the script will not perform any updates.

Related Information

Enabling the 7.2 Approval Mechanism [page 104]
Enabling the 7.2 Approval Mechanism on a Database with a Given Prefix [page 104]
Disabling the 7.2 Approval Mechanism [page 105]
Disabling the 7.2 Approval Mechanism on a Database with a Given Prefix [page 106]

2.5.6.3.1 Enabling the 7.2 Approval Mechanism

Context

To enable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers that are currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.
3. Run the command file `mxmc-enable-72-approvals.cmd`. You are prompted to enter the password for `mxmc_oper`.
4. Start the dispatchers.

2.5.6.3.2 Enabling the 7.2 Approval Mechanism on a Database with a Given Prefix

Context

To enable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers that are currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.
3. Run script `mxmc-xenable-72-approvals.cmd`. The parameters to the command file are:
   - Host name of the server running the SAP ASE
   - Port of the server running the SAP ASE
   - Prefix of the Identity Management database
   - Optional: Password for `<prefix>_oper`
4. Start the dispatchers.

2.5.6.3.3 Disabling the 7.2 Approval Mechanism

Context

To disable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.
3. Run the command file `mxmc-disable-72-approvals.cmd`. You are prompted for the password for `mxmc_oper`.
4. Start the dispatchers.

Results

The 7.2 approval mechanism is disabled.

> ⓘ Note
>
> Since this mechanism is enabled by default for new installations, updates to a higher SP or patch level and upgrades to version 8.0, if you want to keep it disabled, you need to run the script again.

2.5.6.3.4 Disabling the 7.2 Approval Mechanism on a Database with a Given Prefix

Context

To disable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any dispatchers currently running.
2. Open a command prompt and navigate to the directory where the database installation scripts are located.
3. Run the script `mxmc-xdisable-72-approvals.cmd`. The parameters to the command file are:
   - Host name of the server running the SAP ASE
   - Port of the server running the SAP ASE
   - Prefix of the Identity Management database
   - Optional: Password for `<prefix>_oper`
4. Start the dispatchers.

Results

The 7.2 approval mechanism is disabled.

> **Note**
>
> Since this mechanism is enabled by default for new installations, updates to a higher SP or patch level and upgrades to version 8.0, if you want to keep it disabled, you need to run the script again.

2.5.6.4 Creating an Additional Developer Administrator

Context

The initial *Developer Administrator* is created when the database is installed, and other users are added using Identity Management Developer Studio. If the *Developer Administrator* has lost access to Identity Management Developer Studio, you can run a script that creates a *Developer Administrator*.

> **Note**
>
> This user must either exist in the UME or be added to the UME before you can log on to Identity Management Developer Studio.

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the command file `mxmc-create-dev-admin.cmd`. You are prompted to provide the following information:
   - Password for `mxmc_oper`
   - The name of the *Developer Administrator*.
3. Close the command prompt window.

Next Steps

The user must also exist in UME to be able to log on to Identity Management Developer Studio.

Related Information

Creating the Developer Administrator User in UME [page 140]
SAP Identity Management Security Guide

2.5.6.5 Creating an Additional Developer Administrator for a Database with a Given Prefix

Context

The initial *Developer Administrator* is created when the database is installed, and other users are added using Identity Management Developer Studio. If the *Developer Administrator* has lost access to Identity Management Developer Studio, you can run a script that creates a *Developer Administrator*.

> **Note**
>
> This user must either exist in the UME or be added to the UME before you can log on to Identity Management Developer Studio.

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the command file `mxmc-xcreate-dev-admin.cmd`. The parameters to the command file are as follows:
   - Host name of the server running the SAP ASE
   - Port of the server running the SAP ASE
   - Prefix of the Identity Management database
   - Password for `<prefix>_oper`
   - The name of the *Developer Administrator* for this database.
3. Close the command prompt window.

Next Steps

The user must also exist in UME to be able to log on to Identity Management Developer Studio.

2.5.6.6 Removing Identity Management Database on SAP ASE

Context

> **Note**
>
> It is not possible to revert this function, so make sure that the correct database name is referenced in the script.

To remove an Identity Management database, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the command file `mxmc-remove.cmd`.

   You are prompted for:
   - The host name of the server running the SAP ASE
   - The port of the server running the SAP ASE
   - The password for `sa`
3. Close the command prompt window.

2.5.6.7 Removing Identity Management Database with a Given Prefix on SAP ASE

Context

> **Note**
>
> It is not possible to revert this function, so make sure that you specify the correct database name.

To remove an Identity Management database, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the `mxmc-xremove.cmd` command file. The parameters to the command file are:
   - Host name of the server running the SAP ASE
   - Port of the server running the SAP ASE
   - Prefix of the Identity Management database
   - User name for `sa`
   - Optional: Password for `sa`
3. Close the command prompt window.

2.5.7 Creating Encryption Keys

To create an encryption key, you use a utility delivered with SAP Identity Management called SAP Identity Management Keys Utility.

Prerequisites

You have installed the Identity Management Runtime Components.

Context

After installing SAP Identity Management 8.0 with Software Provisioning Manager 1.0, the initial encryption key is created and stored in the `Keys.ini` file.

The `Keys.ini` file is located in `<drive>:\usr\sap\<SAPSID>\SYS\global\security\data\Key\Keys.ini` directory and distributed to the installation directory of SAP Identity Management Runtime Components: `<drive>:\usr\sap\<SAPSID>\IDM<Instance_Number>\Identity_Center\Key\Keys.ini`.

If you need to create and maintain additional encryption key(s) using the Keys Utility, proceed as follows:

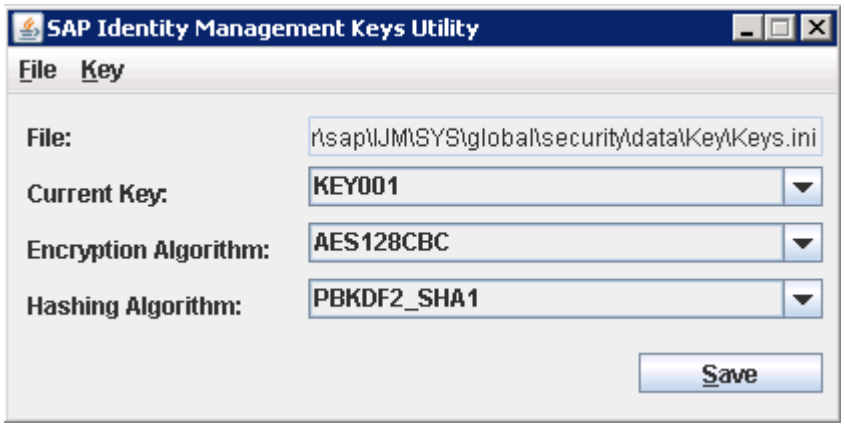
Procedure

1. From a command prompt, navigate to the directory of the Keys Utility: `<drive>:\usr\sap\<SAPSID>\SYS\global\security\data\KeysIniUtility`.

2. Start the utility user interface by executing the command `keysiniutil gui file=<file location>`. For example, `keysiniutil gui file=<drive>:\usr\sap\<SAPSID>\SYS\global\security\data\Key\Keys.ini`.

   Use the `keysiniutil.bat` file for Microsoft Windows.

   This opens the *SAP Identity Management Keys Utility* dialog box (the graphical user interface). You can use it to add a new key and to fill in the parameters/fields for this key.

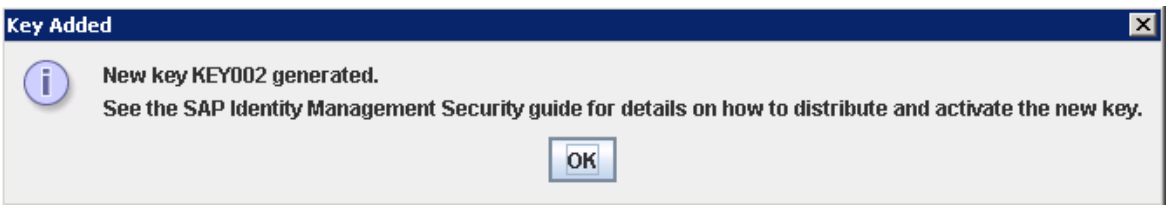


File	Path to the `Keys.ini` file. By default, the key(s) are stored in `<drive>:\usr\sap\<SAPSID>\SYS\global\security\data\Key\Keys.ini`.
Current Key	Specify the currently active key. **Note** After installing SAP Identity Management 8.0 system, the initial encryption key (KEY001) is created and set as the currently active key.

Encryption Algorithm	Select the encryption algorithm for the key. **Note** You can no longer select *Standard* and *DES3* encryption algorithms for the key. Existing configurations with *Standard* and *DES3* algorithms will continue to work, but we highly recommend that you choose another encryption algorithm. Once you do this, you cannot switch back to *Standard* and *DES3* again. You can choose from the following: • *DES3CBC* • *AES128CBC* • *AES192CBC* • *AES256CBC* *AES128CBC* is the default encryption algorithm.
Hash Algorithm	Select the hash algorithm for the key. **Note** You can no longer select *MD5* hash algorithm for the key. Existing configurations with *MD5* algorithm will continue to work, but we highly recommend that you choose another hash algorithm. Once you do this, you cannot switch back to *MD5* again. You can choose from the following: • *SSHA* • *SHA256* • *SHA384* • *SHA512* • *PBKDF2_SHA1* *PBKDF2_SHA1* is the default hash algorithm.

3. To create a new key, choose *Key* > *Generate*.

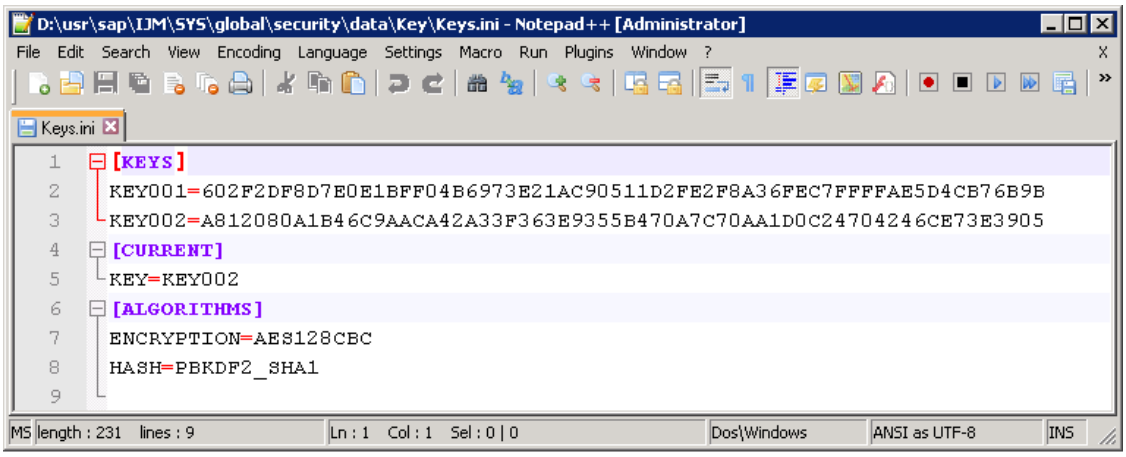
   This will generate the new key:



   a. Choose *OK* to close the *Key Added* dialog box.

b. Choose *Save*. This will add the new key to the `Keys.ini` file. If the new key is selected in the *Current Key* field, this will also set it as the currently active key.

   You can check that the `Keys.ini` file now contains the *KEY002* key. It is set as the currently active key.



c. If you need to add any more keys, choose *Key* > *Generate* from the main menu. If you have more than one key in the `Keys.ini` file, you need to select one of the keys in the *Current Key* field as currently active. Choose *Save* to save the changes to the `Keys.ini` file.

   You can also delete keys. To do this, choose *Key* > *Delete* from the main menu. This will delete whichever key is set as the current key. Once you have deleted this, the key above it in the list (n-1) will be set as the current key. Alternatively, you can set a different key as the current one and choose *Save* to save the changes to the `Keys.ini` file.

d. Select *File* > *Exit* from the main menu to exit and close the utility user interface.

4. You need to copy the `Keys.ini` file to the installation directory of SAP Identity Management Runtime Components. For example: `<drive>:\usr\sap\<SAPSID>\IDM<Instance_Number>\Identity_Center\Key\Keys.ini`.
5. Set the value for the *com.sap.idm.jmx.crypt.keyfile* property to be the full path to the `Keys.ini` file. For example: `<drive>:\usr\sap\<SAPSID>\SYS\global\security\data\Key\Keys.ini`. See *Configuring the JMX Layer* for information about how to edit a property value.
6. See *SAP Identity Management Security Guide* for information about distributing and activating new key(s).

Related Information

Using Commands to Create and Maintain Encryption Keys in the Keys.ini File [page 114]
Configuring the JMX Layer [page 147]
SAP Identity Management Security Guide

2.5.7.1 Using Commands to Create and Maintain Encryption Keys in the Keys.ini File

A set of commands is available with SAP Identity Management Keys Utility. These allow you to create and maintain the encryption key(s) and the `Keys.ini` file without using the graphical user interface.

The following set of commands is available:

> **Note**
>
> From a command prompt, navigate to `<drive>:\usr\sap\<SAPSID>\IDM<Instance_Number>\Identity_Center\KeysIniUtility` directory. Use the `keysiniutil.bat` file for Microsoft Windows .

Command	Description
`keysiniutil`	Displays the usage information for the utility.
`keysiniutil add file=<file location>`	Generates an encryption key and adds it to the `Keys.ini` file. This command will generate the `Keys.ini` file if it does not already exist, and then add the generated key to it. The default directory is `<drive>:\usr\sap\<SAPSID>\SYS\global\security\data\Key\Keys.ini`. If the key is initial, it will automatically be defined as the currently active key. If the key is not initial, you will need to select the currently active key using the command `keysiniutil setkey <name of the key that exists in the Keys.ini file>`.
`keysiniutil print`	Prints/displays the content of the `Keys.ini` file.
`keysiniutil setkey <name of the key that exists in the Keys.ini file>`	Sets the given encryption key as the currently active key. Example: `keysiniutil setkey KEY002`.
`keysiniutil setenc <encryption algorithm>`	Specifies the encryption algorithm for the key(s). Example: `keysiniutil setenc Scramble`, `keysiniutil setenc DES3` or `keysiniutil setenc DES3CBC`. *DES3CBC* is selected as the default encryption algorithm.
`keysiniutil sethash <hash algorithm>`	Specifies the hash algorithm for the key(s). Example: `keysiniutil sethash MD5` or `keysiniutil sethash SSHA`.

Command	Description
	SSHA is selected as the default hash algorithm.
`keysiniutil delete <name of the key>`	Deletes the specified key. Example: `keysiniutil delete KEY001`. If the key you are deleting is defined as the current key, the command sets the key with the lowest number as the current key by default. To set another key, as the current key, use the command `keysiniutil setkey <name of the key that exists in the Keys.ini file>`.
`keysiniutil gui file=<file location>`	Opens the *SAP Identity Management Keys Utility* dialog box (the graphical user interface).

See *SAP Identity Management Security Guide* for details about distributing and activating the new key(s).

Related Information

SAP Identity Management Security Guide

2.5.8 Creating and Configuring Dispatchers

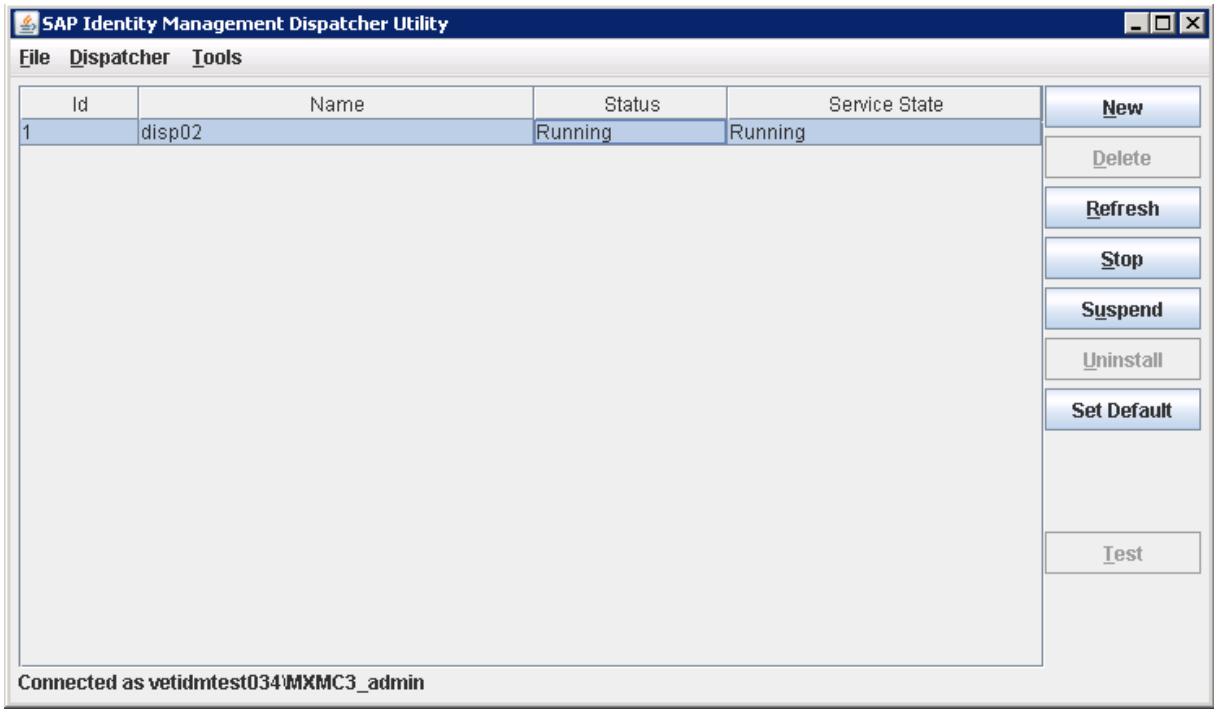
To create and configure dispatchers, you use a utility delivered with SAP Identity Management called SAP Identity Management Dispatcher Utility.

Prerequisites

- The `Keys.ini` file is available. The file is created and maintained centrally using the SAP Identity Management Keys Utility and then distributed manually to necessary locations. See Creating Encryption Keys [page 110].
- The administrator user must have permissions to edit the Windows Registry.
- You use the `<sapsid>adm` user to start the dispatcher utility and to manage the dispatchers (that is, to create, start, delete, resume and others).
- You have set the JAVA_HOME environment variable for the `<sapsid>adm` user to point to `<drive>:\usr\sap\<SAPSID>\IDM<No>\exe\sapjvm_<No>`

Context

After installing SAP Identity Management 8.0 with Software Provisioning Manager 1.0, the initial dispatcher is created and started. It is set as the default dispatcher.



If you need to create and configure additional dispatcher using the utility, proceed as follows:

Procedure

1. From a command prompt, navigate to the directory of the Dispatcher Utility: `<drive>:\usr\sap\<SAPSID>\IDM<Instance_Number>\Identity_Center`.

   > **Note**
   >
   > Run the command prompt as the administrator on Microsoft Windows.

2. Start the utility user interface by executing the command **`dispatcherutil gui`** (use the file `dispatcherutil.bat` for Microsoft Windows).

   This opens the *SAP Identity Management Dispatcher Utility* dialog box (the graphical user interface).

3. The first time the utility is run, you will see that some settings of the Dispatcher Utility are already defined, including the connection strings to access the Identity Management database with your `<prefix>_admin` user and the `<prefix>_rt` user. See *Defining the Settings for the Identity Management Dispatcher Utility* for details.
4. To create and manage dispatchers, you can either use the utility's graphical user interface or alternatively use the commands allowing you to create and manage the dispatcher(s) without using the graphical

user interface. See *Creating and Managing the Dispatcher(s)* for details when using the graphical user interface, and *Using Commands to Create and Manage the Dispatcher(s)* for more details about the available commands.

Related Information

SAP Identity Management Security Guide
Defining the Settings for the Identity Management Dispatcher Utility [page 117]
Creating and Managing the Dispatcher(s) [page 121]
Using Commands to Create and Manage the Dispatcher(s) [page 125]

2.5.8.1 Defining the Settings for the Identity Management Dispatcher Utility

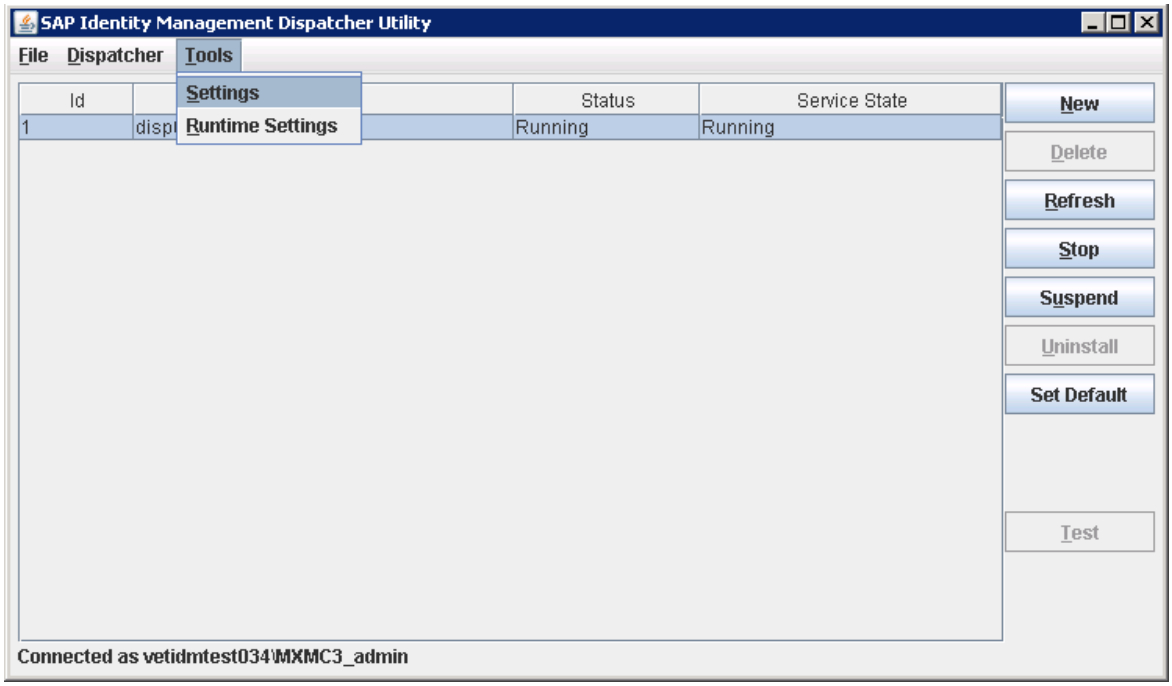
The first time the utility is run you will see that some settings of the Dispatcher Utility are already defined, including the connection strings to access the Identity Management database with your `<prefix>_admin` user and the `<prefix>_rt` user.

Context

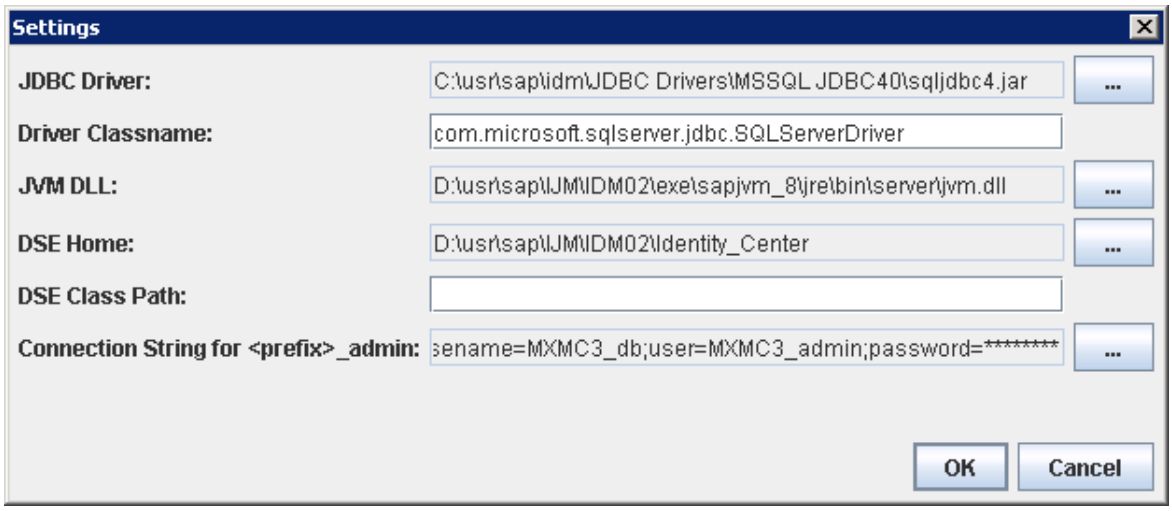
If you need to review or change any of the settings for the utility, proceed as follows:

Procedure

1. In the *SAP Identity Management Dispatcher Utility* dialog, choose *Tools* > *Settings*



2. In the *Settings* dialog, fill in the following parameters/fields:

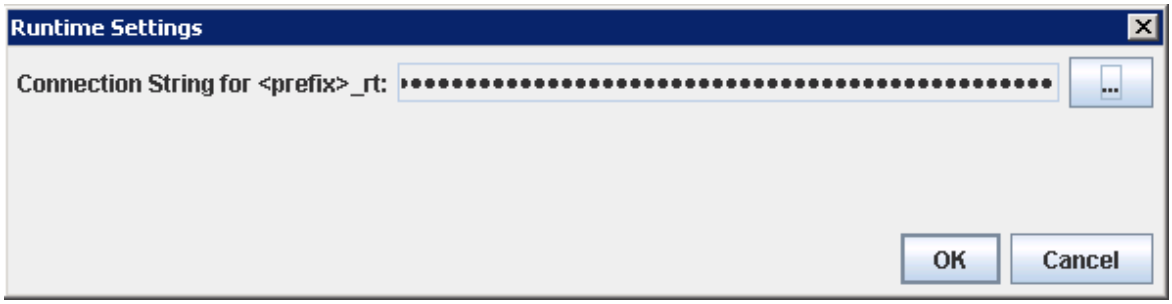


Field	Value
JDBC Driver	Choose the ... button to the right of the field to browse the file system to locate the database driver (JAR file) that the dispatcher should use to access the Identity Management database.
Driver Classname	Enter classnames of all JDBC drivers that the runtime engine needs. Example: *com.microsoft.sqlserver.jdbc.SQLServerDriver*.

Field	Value
JVM DLL	Define the path to `jvm.dll` file. Choose the ... button to the right of the field to browse the file system to locate the correct `jvm.dll` file. You should use SAP JVM 8.
DSE Home	Define the directory where the runtime engine is installed, by default `<drive>:\usr\sap\<SAPSID>\IDM<Instance_Number>\Identity_Center`. Choose the ... button to the right of the field to browse the file system to locate the correct directory.
DSE Class Path	Enter the Identity Management dispatcher class path that is passed to the Java runtime engine. For example: `C:\Users\userlibrary1.jar;C:\Users\userlibrary2.jar`
Connection String (<prefix>_admin)	Define the connection string to access the Identity Management database with your `<prefix>_admin` user. Choose the ... button to the right of the field to open *JDBC URL Wizard*. Select the correct JDBC driver for your Identity Management database: • For Microsoft SQL Server, select the driver of Microsoft SQL Server. • For Oracle, select *Oracle thin driver* from the list. • For IBM DB2, select *DB2 universal driver* from the list. • For SAP ASE, select *SAP Adaptive Server Enterprise dirver* from the list. Choose *Next >* and fill in connection information for the database, e.g. servername (or the IP address), port number, database name and the admin user or other information requested by the wizard. **Note** When using IBM DB2, the wizard prompts you for the *Current Schema* and the *Current Function Path*. In both fields, enter the `<PREFIX>_OPER` user in uppercase letters. For example: **`IC_OPER`**. Choose *Finish* to add the connection string to the field. The connection string is not displayed in clear text.

3. Choose *OK* to save the settings.

   You need to restart the application to load the defined settings. Choose *OK* to close the restart warning and the application.
4. Restart the application. You will get a login dialog box. Provide the credentials for your database admin user.
5. The connection string for the `<prefix>_rt` user needs to be defined (a warning appears after login). Choose *Yes* to open the *Runtime Settings* dialog and define the connection string.



Define the following field:

Option	Description
Connection String (<prefix>_rt)	Choose the ... button to the right of the field to open the *JDBC URL Wizard*. Select the correct JDBC driver for your Identity Management database: • For Microsoft SQL Server, select the driver of Microsoft SQL Server. • For Oracle, select *Oracle thin driver* from the list. • For IBM DB2, select *DB2 universal driver* from the list. • For SAP ASE, select *SAP Adaptive Server Enterprise dirver* from the list. Choose *Next >* and fill in connection information for the database, e.g. servername (or the IP address), port number, database name, the credentials for your RT user or other information requested by the wizard. **Note** When using IBM DB2, the wizard prompts you for the *Current Schema* and the *Current Function Path*. In both fields, enter the `<PREFIX>_OPER` user in uppercase letters. For example: **`IC_OPER`**. Choose *Finish* to add the connection string to the field. The connection string is not displayed in clear text.

6. Choose *OK* to save the settings and close the dialog box.

   The list of dispatchers is displayed. You can now create the dispatcher(s). See *Creating and Managing the Dispatcher(s)* for details.

   Alternatively, you can close the graphical user interface and instead use commands to create and manage the dispatcher(s) (see *Using Commands to Create and Manage the Dispatcher(s)* for more details). To exit and close the graphical user interface, select *File* > *Exit* from the main menu.

Related Information

Creating and Configuring Dispatchers [page 115]
Creating and Managing the Dispatcher(s) [page 121]
Using Commands to Create and Manage the Dispatcher(s) [page 125]

2.5.8.2 Creating and Managing the Dispatcher(s)

To create and manage the dispatcher(s), you use SAP Identity Management Dispatcher Utility. The utility offers a graphical user interface for dispatcher handling.

Prerequisites

- You use the `<sapsid>adm` user to start the dispatcher utility and to manage the dispatchers (that is, to create, start, delete, resume and others).
- You have set the JAVA_HOME environment variable for the `<sapsid>adm` user to point to `<drive>:\usr\sap\<SAPSID>\IDM<No>\exe\sapjvm_<No>`

Context

To create and manage dispatchers using the utility's graphical user interface, proceed as follows:

Procedure

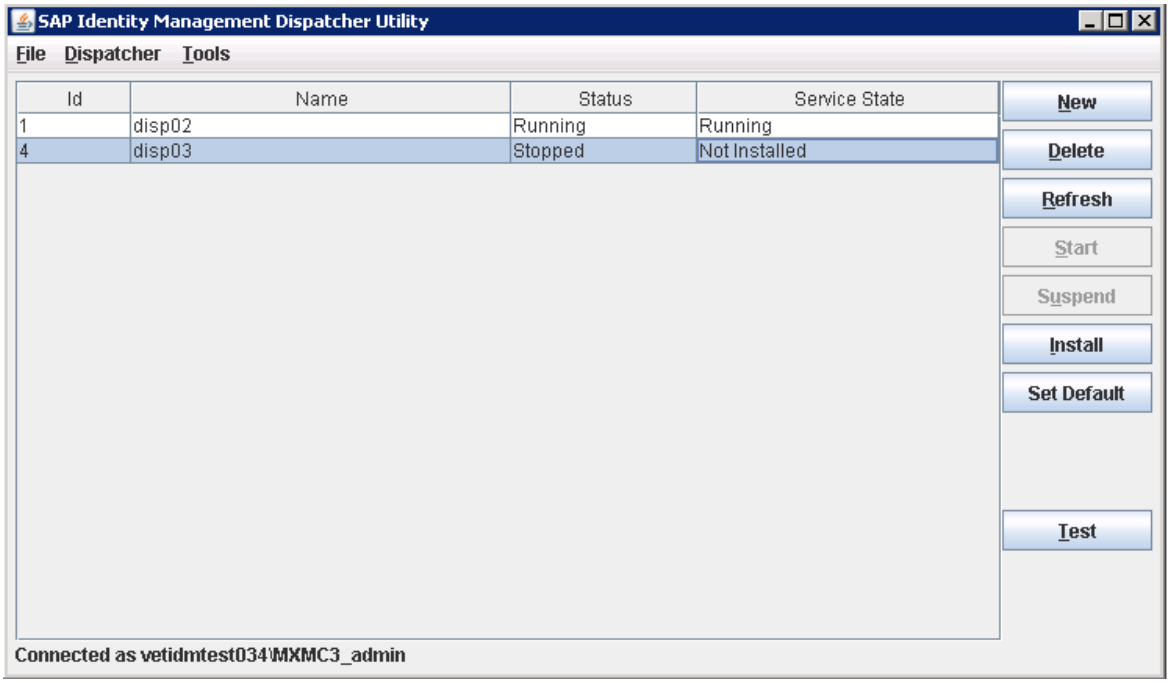
1. To create a dispatcher, choose *New* from the menu on the right (or select *File* > *New* from the main menu). This will open the *New Dispatcher* dialog box.
2. In the *Name* field, enter a dispatcher name.

   > **Note**
   >
   > The name of the dispatcher should not contain space characters only and should not be empty. Depending on your operating system, the name of the dispatcher should not contain the following symbols:
   >
   > - Microsoft Windows – backslash (\), slash (/), colon (:), asterisk (*), question mark (?), quotation marks ("), angle brackets (< >), and vertical slash (|)
   > - Mac OS – slash (/), and colon (:)

   The location of the dispatcher service scripts that will be created is displayed in the *Target Location* field (by default `<drive>:\usr\sap\<SAPSID>\IDM<No>\Identity_Center\Service-Scripts`).
3. Choose *OK* to create the dispatcher and add it to the dispatcher list.

   > **Note**
   >
   > The following file is generated for the dispatcher: `Dispatcher_Service_<name>.bat` when running on Microsoft Windows, where <name> is the name of the dispatcher as defined upon creation. In addition, a property file is created, that is, `Dispatcher_Service_<name>.prop`.

   The service state of the new dispatcher is *Not Installed* and its status *Stopped*.

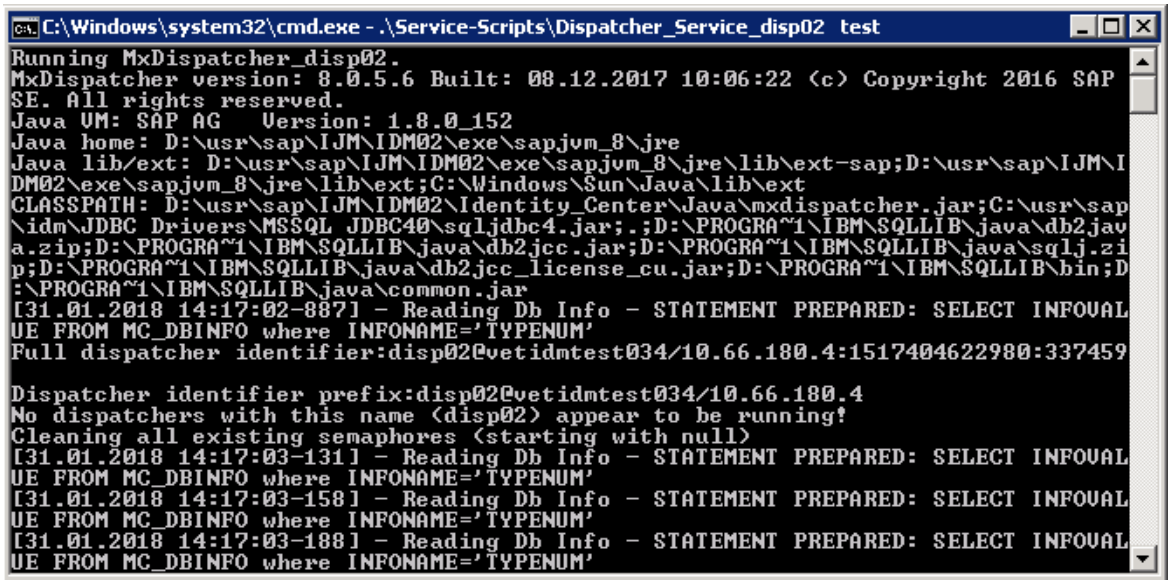


4. To set a default dispatcher, select it from the dispatcher list and choose *Set Default* or choose *Yes* when you are asked `Do you want to set <Dispatcher Name> as the default dispatcher?`

   Use this option to have a default dispatcher selected for jobs and tasks in the imported configuration packages in SAP Identity Management Developer Studio.

5. To verify the dispatcher configuration, choose *Test* from the menu on the right. This will verify that the dispatcher is able to start. The dispatcher must be stopped (not running) before it can be tested.

   You should be able to see the following:



Verify that no error messages are displayed during the process. Abort the execution by pressing CTRL + C.

6. The dispatcher can be installed as a service. Make sure that the dispatcher is not running in the test mode before you continue. Select the dispatcher and choose *Install* from the menu on the right (or select *Dispatcher* > *Install* from the main menu). The service state of the dispatcher will now change to *Stopped*.

   > **Note**
   >
   > This is only relevant for installing the dispatcher as a Windows service.

7. You can now choose *Start* from the menu on the right (or select *Dispatcher* > *Start* from the main menu) to start the created and installed dispatcher service. Both the service state and the status of the dispatcher will change to *Running*. You may have to choose *Refresh* (or select *File* > *Refresh* from the main menu) to update the fields.

   By default, the dispatcher is started automatically each time the system is started.

8. Once the dispatcher is up and running, you have the possibility to:

Option	Description
Suspend the dispatcher	Select the running dispatcher you want to suspend from the list and choose the *Suspend* button from the menu on the right (alternatively, select *Dispatcher* > *Suspend* from the main menu). When suspended, the dispatcher service will still be running (state), but its processing is suspended (status). **Note** The *Suspend* button is not visible if the dispatcher is already suspended (you will then only see the *Resume* button).
Resume the dispatcher	Select the suspended dispatcher you want to resume from the list and choose the *Resume* button from the menu on the right (alternatively, select *Dispatcher* > *Resume* from the main menu). When resumed, the dispatcher service is running and processing (both its state and status are *Running*). **Note** The *Resume* button is not visible if the dispatcher is already running (you will then only see the *Suspend* button).
Stop the dispatcher	Select the dispatcher you want to stop from the list and choose the *Stop* button from the menu on the right (alternatively, select *Dispatcher* > *Stop* from the main menu).
Test the dispatcher	Select the dispatcher you want to test from the list and choose the *Test* button from the menu on the right. **Note** The dispatcher must be stopped (not running) before it can be tested. To abort the test execution in the command prompt, press CTRL + C.

Option	Description
Uninstall the dispatcher	Select the dispatcher you want to uninstall from the list and choose the *Uninstall* button from the menu on the right (alternatively, select *Dispatcher* > *Uninstall* from the main menu). **Note** The dispatcher must be stopped (not running) before it can be uninstalled.
Delete the dispatcher	Select the dispatcher you want to delete from the list and choose the *Delete* button from the menu on the right (alternatively, select *File* > *Delete* from the main menu). Deleting the dispatcher will also delete the generated dispatcher files. **Note** The dispatcher must be stopped (not running) before it can be deleted. **Note** Deleting a dispatcher will remove any reference to it (e.g. from jobs) as well. You have to reconfigure the dispatcher for the affected jobs.
Regenerate the dispatcher scripts	From the dispatcher list, select the dispatcher you want to regenerate the scripts for and select *Dispatcher* > *Regenerate Scripts* from the main menu). You would normally regenerate the scripts for a dispatcher after a configuration change.

9. You can create as many dispatchers as you need, which will be listed in the dispatcher list. To update the list and the displayed dispatcher properties, choose the *Refresh* button from the menu on the right or select *File* > *Refresh* from the main menu. To exit the utility and close its graphical user interface, select *File* > *Exit* from the main menu.

> **Note**
>
> Keep in mind that, when installing the Identity Management dispatcher, the corresponding Windows Service will be started with default recovery actions *Take no action*. This will prevent services to recover automatically in case the database connection got temporarily lost. Based on your configuration requirements, you can change the action to *Restart the Service* with an appropriate restart interval or choose any other available recovery actions.

Related Information

Creating and Configuring Dispatchers [page 115]
Using Commands to Create and Manage the Dispatcher(s) [page 125]

2.5.8.3 Using Commands to Create and Manage the Dispatcher(s)

A set of commands is available with SAP Identity Management Dispatcher Utility, allowing you to create and manage the dispatcher(s) without using the graphical user interface.

1. From a command prompt, navigate to the directory `<drive>:\usr\sap\<SAPSID>\IDM<Instance_Number>\Identity_Center`.
2. Use the file `dispatcherutil.bat` for Microsoft Windows.

> **Note**
>
> For Microsoft Windows, run the command prompt as administrator.

The following set of commands is available:

Command	Description
`dispatcherutil`	Displays the usage information for the utility.
`dispatcherutil add <dispatcher name>`	Creates a dispatcher with the given name and generates necessary service files and a property file. **Note** The following file is generated for the dispatcher: `Dispatcher_Service_<name>.bat`, where <name> is the name of the dispatcher as defined upon creation. In addition, a property file is created, that is, `Dispatcher_Service_<name>.prop`. You can create as many dispatchers as you need.
`dispatcherutil test <dispatcher name>`	Dispatcher with a given name is tested to verify the dispatcher configuration. This will verify that the dispatcher is able to start. Verify that no error messages are displayed during the process. Abort the test execution by pressing CTRL + C.
`dispatcherutil install <dispatcher name>`	Installs the dispatcher with the given name.
`dispatcherutil set_default <dispatcher name>`	Sets an installed dispatcher as the default one.
`dispatcherutil start <dispatcher name>`	Starts the installed dispatcher with the given name.
`dispatcherutil suspend <dispatcher name>`	Suspends a running dispatcher. The dispatcher service will still be running, but its processing is on hold (suspended).
`dispatcherutil resume <dispatcher name>`	Resumes a suspended dispatcher. The dispatcher service will then be running and processing.

Command	Description
`dispatcherutil stop <dispatcher name>`	Immediately stops the running dispatcher with the given name (hard stop).
`dispatcherutil softstop <dispatcher name>`	Stops the running dispatcher with the given name, when the ongoing processes handled by the dispatcher have completed (soft stop).
`dispatcherutil uninstall <dispatcher name>`	Uninstalls the stopped dispatcher with the given name.
`dispatcherutil delete <dispatcher name>`	Deletes the stopped dispatcher with the given name. The belonging service script files and the property file of the given dispatcher will also be deleted.
`dispatcherutil list`	Lists all available dispatchers in the dispatcher list.
`dispatcherutil gui`	Opens the *SAP Identity Management Dispatcher Utility* dialog box (the graphical user interface).
`dispatcherutil set_jdbc_url <JDBC URL>`	Defines the connection string to access the Identity Management database for the `<prefix>_rt` user. Note that the JDBC URL must be enclosed in double quotes ("").

2.5.9 Using the SAP Java Connector (JCo)

The SAP Java Connector version 3 (JCo 3) is included in the installation of Runtime Components for Microsoft Windows.

> ⓘ Note
>
> The JCo library is 64-bit, and requires 64-bit version of the Java Runtime Environment.

> ⓘ Note
>
> If you previously have used JCo 2, you must regenerate the dispatcher scripts before starting the dispatcher after the upgrade.

In order to use the SAP Java Connector, proceed with the following step:

- Installing additional Microsoft runtime DLLs for the SAP Java Connector

Related Information

Installing Additional Microsoft Runtime DLLs [page 127]

2.5.9.1 Installing Additional Microsoft Runtime DLLs

For using JCo on Microsoft Windows, some additional files are required.

The required files may already be present on the system. If not, you receive error messages about missing DLLs when accessing an ABAP system (`java.lang.UnsatisfiedLinkError: <path_to_dll>\sapjco3.dll: This application has failed to start because the application configuration is incorrect`).

Download and install these DLLs for the Visual Studio 2005 Compiler as described in SAP Note 684106.

For general information about the SAP Java Connector, see the file `useful.html` in the downloaded `JCo 3.x.zip` file.

2.5.10 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. The following versions are supported:
  - SAP NetWeaver 7.3 SP09 or higher
  - SAP NetWeaver 7.3 including Enhancement Package 1 SP06 Patch 3 or higher
  - SAP NetWeaver 7.4 SP02 or higher
  - SAP NetWeaver 7.5 SP08 or higher

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 128]
Adding the Database as the Data Source [page 128]
Configuring the Java System Properties [page 131]

2.5.10.1 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, SQL2005, 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

2.5.10.2 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. For Microsoft SQL Server for instance, you may not only use the JDBC driver version 1.2, which might appear to match the JDBC version 1.x, but also the driver version 3.0.

- 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 • 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 *Native SQL* for MS SQL Server. 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: • *com.microsoft.sqlserver.jdbc.SQLServerDriver* for MS SQL Server • *oracle.jdbc.driver.OracleDriver* for Oracle

Name of the Field	Value/Comments
	• *com.ibm.db2.jcc.DB2Driver* for IBM DB2 • *com.sybase.jdbc4.jdbc.SybDriver* for SAP ASE
Database URL	Provide the correct database URL: • For MS SQL Server: jdbc:sqlserver:// <host>;databasename=<prefix>_db (e.g. jdbc:sqlserver:// trd90500010.example.com;databasename=MXMC_db) Port for a non-default JDBC connection is a part of the JDBC URL, e.g. jdbc:sqlserver:// <host>:<port>;databasename=<prefix>_db. • 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;curren tFunctionPath=<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;retrieveMessagesFro mServerOnGetMessage=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).
Password	Provide the password of the provisioning user defined in the *User Name* field.

2.5.11 Configuring the Java System Properties

You can change the settings or properties of your SAP NetWeaver AS Java, or of the applications and services that are deployed on your SAP NetWeaver AS Java.

To configure the properties of the deployed Identity Management Developer Studio service and Identity Management REST Interface version 2 on your SAP NetWeaver AS 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*. 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, that is, the `Keys.ini` file. For example: `\\<host>\sapmnt\<SAPSID>\SYS\global\security\data\Key\Keys.ini`, where `<SAPSID>` is the SAP system ID of SAP Identity Management system. **Note** The value of this property must be the same in the SAP NetWeaver Config Tool. Make sure you have provided the same path to the `Keys.ini` file, you have saved your configuration and restarted the `idmdevstudio` application. For more information about the `Keys.ini` file, see *SAP Identity Management Security Guide*.
`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, `C:\usr\sap\IdM\jdbc\MSSQL2005\sqljdbc.jar`. This can also be a list of paths (to several JDBC driver JAR files). List items are separated by `;` in Microsoft Windows systems.

Property	Value
`com.sap.idm.rcp.jdbcdrivers`	A list of JDBC driver names. For example, com.microsoft.sqlserver.jdbc.SQLServer-Driver;oracle.jdbc.driver.Oracle-Driver;com.ibm.db2.jcc.DB2Driver;com.sap.db.jdbc.Driver;com.sybase.jdbc4.jdbc.SybDriver. **Note** List items are separated by *;* in Microsoft Windows systems.
`com.sap.idm.rcp.dsehome`	The path relative to which the runtime engine is found, by default `<drive>:\usr\sap\<SAPSID>\IDM<Instance_Number>\Identity_Center`. Needed for data discovery purposes.
`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) [page 134] • *true* - Allows HTTP communication.
`v2ReturnNullValuesInResponse`	Controls if `null` value is returned in the response body for single-value attributes that do not contain value. • *true* - `null` value is returned for single-value attributes that do not contain value. This is the default value. • *false* - `null` value is not returned for single-value attributes that do not contain value.

Related Information

Initial Configuration of Identity Management Developer Studio [page 137]
SAP Identity Management Security Guide

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

Security between the Identity Management Developer Studio service and client, as well as the Identity Management REST Interface Version 2 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 Transport Layer Security on SAP NetWeaver AS for Java

To configure the transport layer security (TLS), commonly referred to as 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

To ensure properly working secure SSL communications, 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 136]
Initial Configuration of Identity Management Developer Studio [page 137]
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

2.5.12.1 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`.

2.5.13 Initial Configuration of Identity Management Developer Studio

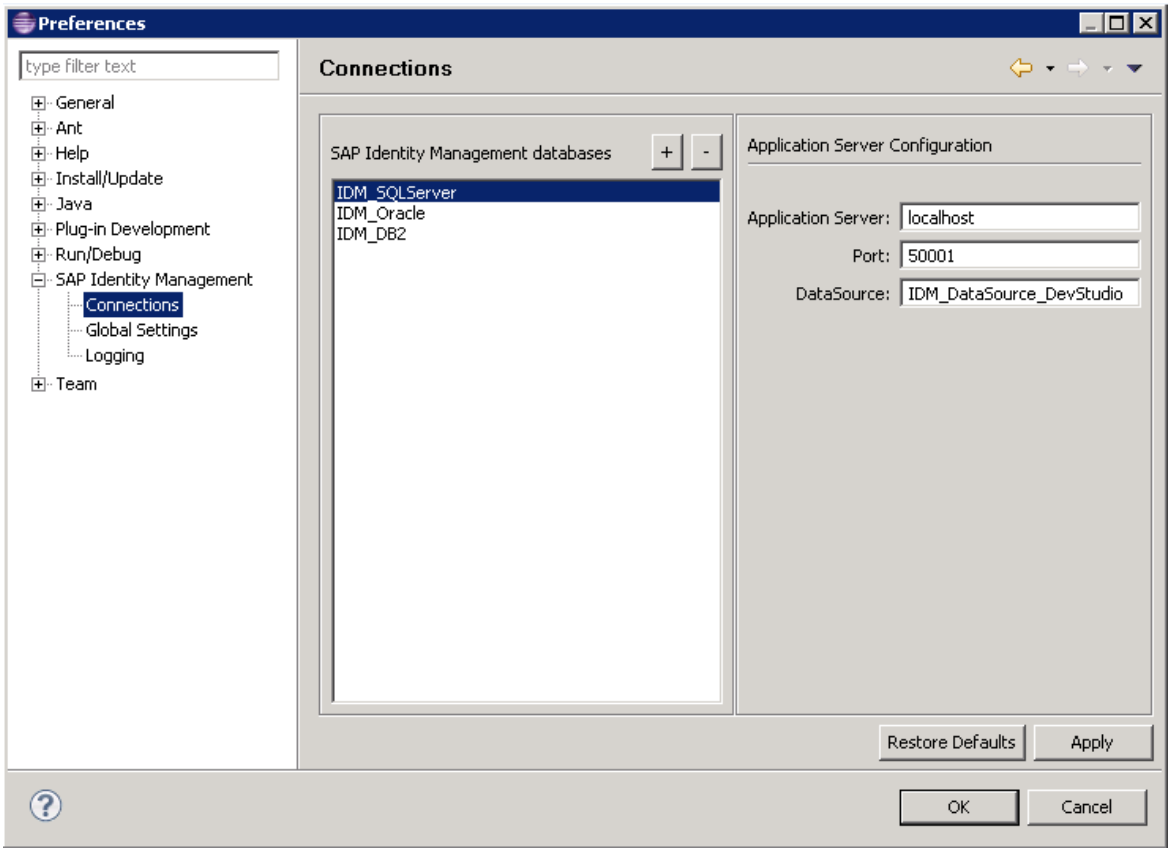
Once the SAP Identity Management Developer Studio plugin is installed in your Eclipse environment and the perspective is opened, you would need some initial configuration in order to access the Identity Management database and the identity store(s).

Context

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

Procedure

1. From the main menu, select:
   - For Windows, *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 134] and Exporting and Installing the SSL Certificate [page 136].
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* 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

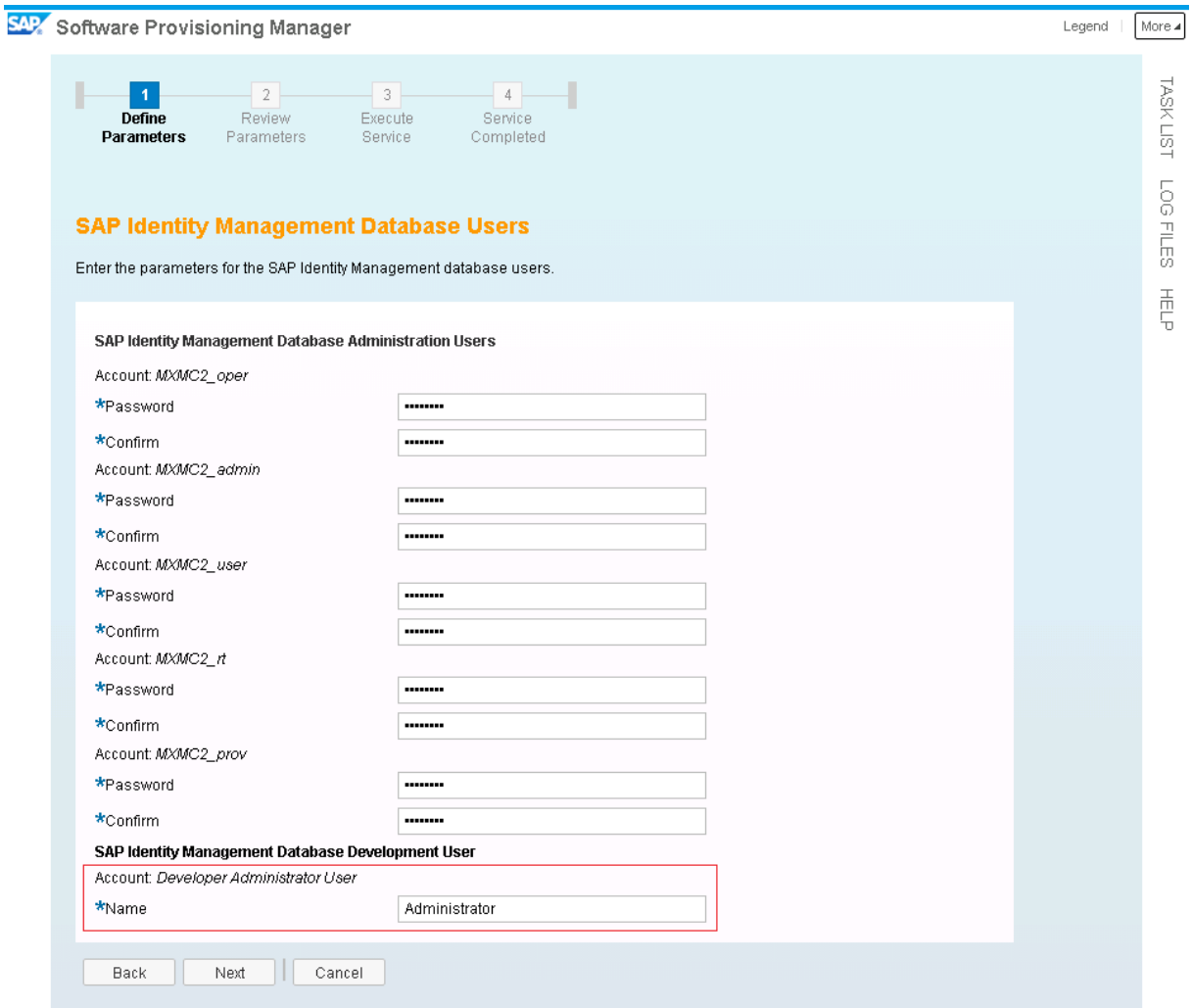
Creating the Developer Administrator User in UME [page 140]
Configuring the Java System Properties [page 131]
Defining the Settings for the Identity Management Dispatcher Utility [page 117]
Adding the Initial Identity Store [page 142]

2.5.13.1 Creating the Developer Administrator User in UME

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

Context

The initial developer administrator for Identity Management Developer Studio is created when the Identity Management Core component is installed with SWPM. For this user, you have provided a name in the *SAP Identity Management Database Users* dialog (under *SAP Identity Management Database Development User Account: Developer Administrator User*). See the example below:



The initial developer administrator user needs to exist both in the Identity Management database and in the UME, to be able to log on to the Identity Management Developer Studio. This means that you need to manually

create the initial developer administrator user for Identity Management Developer Studio in the UME, with a corresponding password.

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

The user also needs the `idm_authenticated_studio` UME action assigned to it through a UME role.

Procedure

1. Log on to SAP NetWeaver Administrator at `http(s)://<host>:<port>/nwa` and navigate to *Configuration* > *Identity Management*.
2. Create the user as a technical user, following 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

3. Assign the `idm_authenticated_studio` UME action to the user. Proceed with one of the following options:
   - On the *Assigned Roles* tab page, assign the `idm.developer` or the `Administrator` role to the user. Both roles contain the `idm_authenticated_studio` action.
   - Assign the `idm_authenticated_studio` action to another role of your choice and then assign the role to this user.
4. Choose *Save*.

Results

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

2.5.13.2 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.

2.5.14 Defining the JDBC Connection for the JMX Layer

In order to be able to retrieve data from the identity store, the JMX layer of the Identity Management User Interface needs a JDBC data source pointing to the Identity Management database.

Before creating the JDBC data source, make sure that a database driver is installed.

> ⓘ 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.

The procedures may be different, depending on what database system you are using. The procedures are the same for all database systems unless stated otherwise in this document.

To set up the connection for the supported SAP NetWeaver version, use SAP NetWeaver Administrator.

To access the SAP NetWeaver Administrator, do the following:

1. Enter **`http(s)://<host>:<port>`** in your browser, which will take you to your index page.
2. Then select SAP NetWeaver Administrator. Or you can just enter **`http(s)://<host>:<port>/nwa`** in your browser. Both procedures will display the login page for the SAP NetWeaver Administrator.

3. Enter the credentials, the correct user ID and the password.

2.5.14.1 Deploying the JDBC Driver

Follow the descriptions on how to deploy the drivers for your SAP NetWeaver version. See the Related Information for details.

> **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, SQL2005, 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

2.5.14.2 Adding the Identity Management Database as a Data Source

To create the data source, 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 AS 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. For Microsoft SQL Server for instance, you may not only use the JDBC driver version 1.2, which might appear to match the JDBC version 1.x, but also the driver version 3.0.

- 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

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

Name of the field	Value
Data Source Name	Name the data source *IDM_DataSource* (must be in this exact casing). If you choose to name the data source differently, then you must create alias IDM_Data-Source for the data source. Read more about creating and managing aliases here: • Managing JDBC DataSource Aliases for SAP NetWeaver 7.3 • 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.
SQL Engine	Choose *Native SQL* for MS SQL Server. 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: • *com.microsoft.sqlserver.jdbc.SQLServerDriver* for MS SQL Server • *oracle.jdbc.driver.OracleDriver* for Oracle • *com.ibm.db2.jcc.DB2Driver* for IBM DB2 • *com.sybase.jdbc4.jdbc.SybDriver*

Name of the field	Value
Database URL	Provide the correct database URL: **For MS SQL Server**: `jdbc:sqlserver://<host>;database=<prefix>_db` For example: `jdbc:sqlserver://trd90500010.example.com;database=MXMC_db` Port for a non-default JDBC connection is a part of the JDBC URL, for example: `jdbc:sqlserver://<host>:<port>;database=<prefix>_db`. **For Oracle**: `jdbc:oracle:thin:@<host>:<port>:<database SID>` For example: `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;retrieveMessagesFromServerO nGetMessage=true;` **For SAP ASE**: `jdbc:sybase:Tds:<host>:<port>/<prefix>_db`
User Name	Enter the user name that you use to log in to the database server, the provisioning user. For example: <prefix>_prov (for example MXMC_prov or IC_prov).
Password	Provide the password of the provisioning user defined in the *User Name* field.

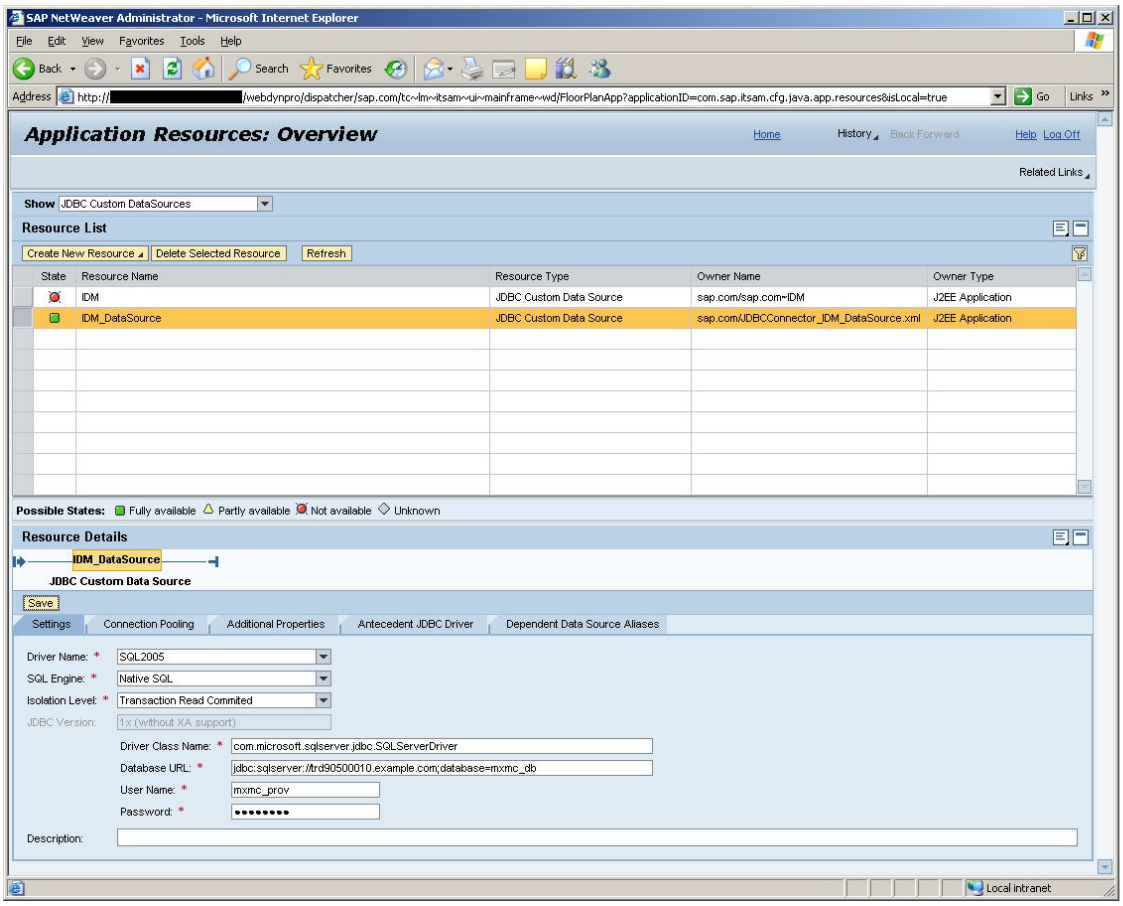
2.5.14.3 Updating the Data Source

Context

If you need to update the data source information (e.g. changes in server, database, password etc), do the following:

Procedure

1. In the SAP NetWeaver Administrator, go to *Configuration Management* > *Infrastructure* > *Application Resources*.
2. Select *JDBC Custom DataSources* in the *Show* field to list all created data sources:



Find and select the data source you need to update. This will display the resource details in the *Resource Details* section (below the *Resource List* section).

3. Update the data and choose *Save* to save the changes.

4. An information dialog box appears confirming that the data source has been saved successfully. Choose *Close* to close the dialog box.

2.5.15 Configuring the JMX Layer

This section describes how to change the settings, like configuring the cache, defining which identity store you are working on and configuring the encryption key-file.

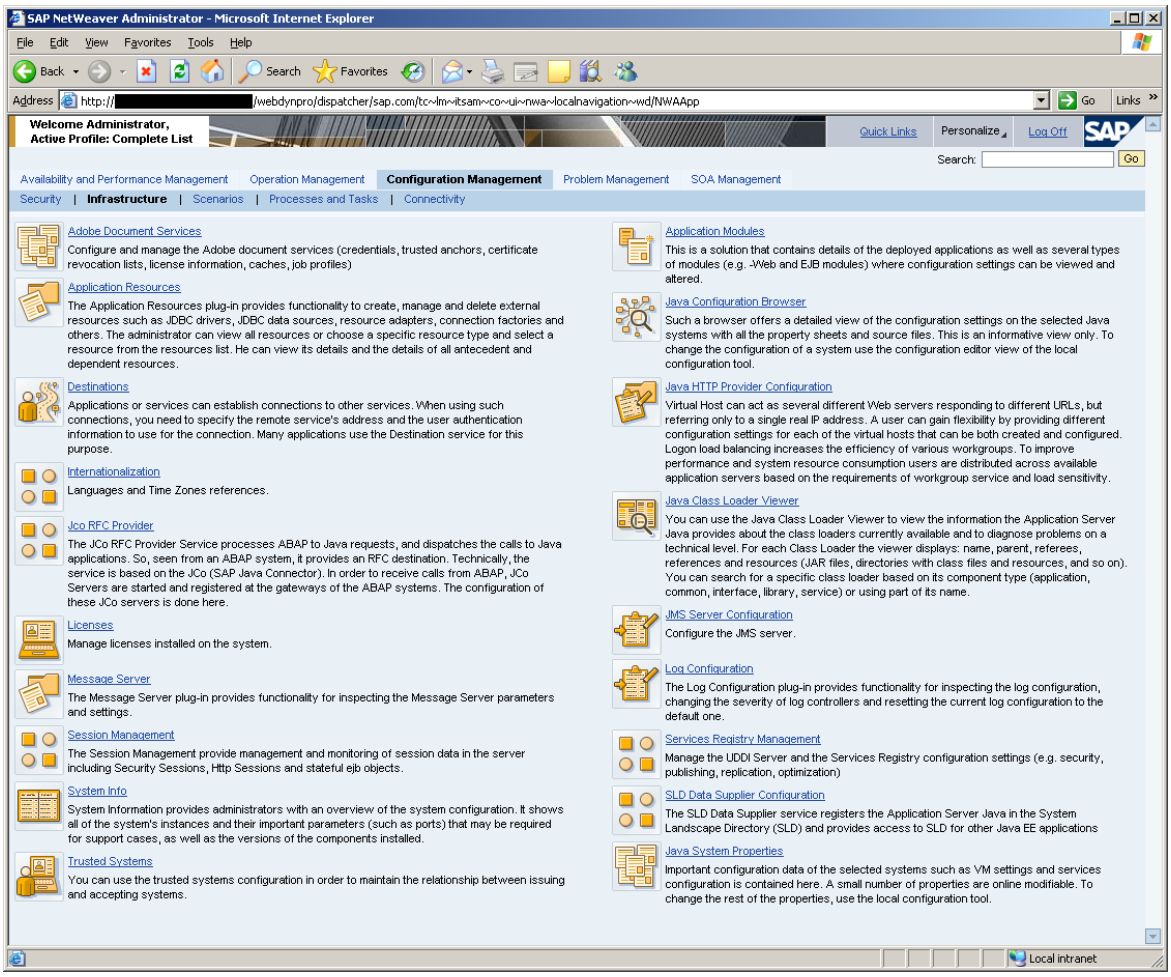
Context

The procedure is the same for the supported SAP NetWeaver versions.

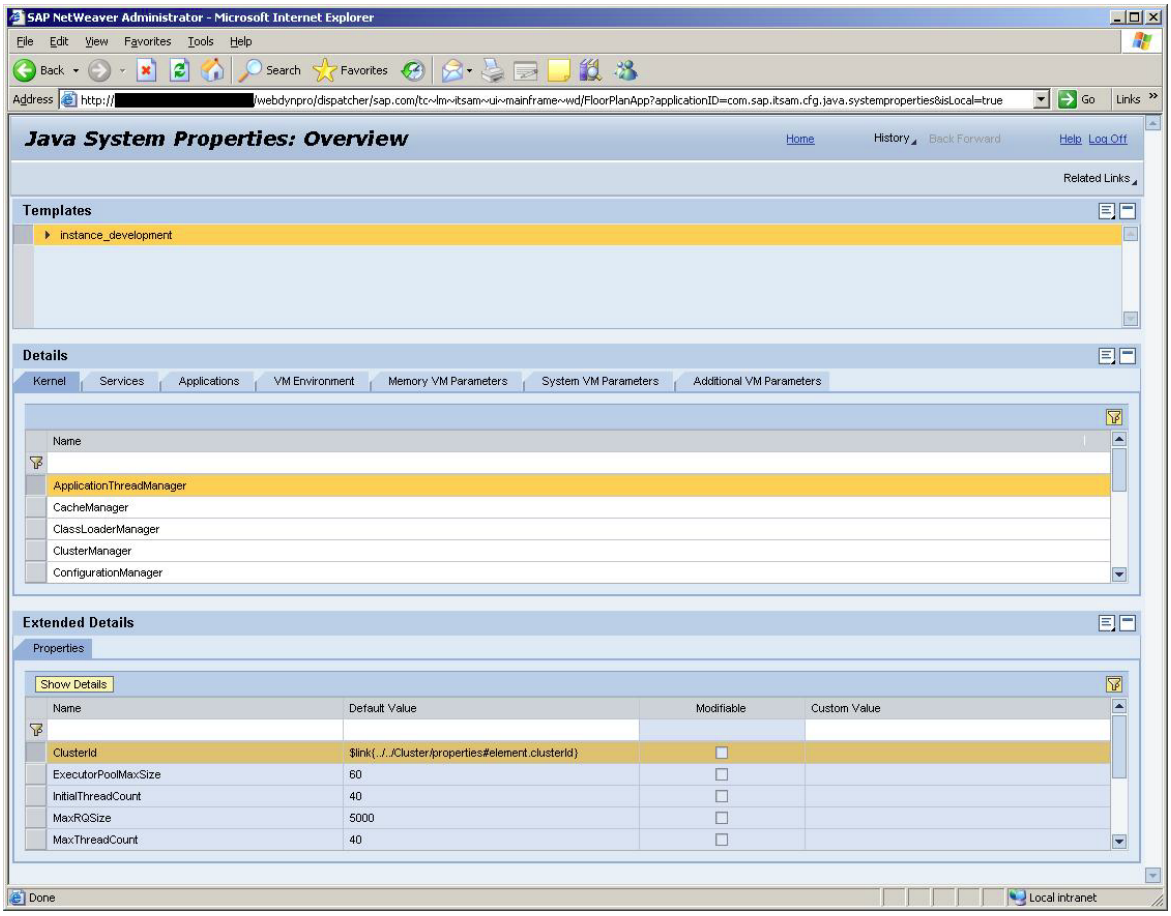
To alter the configuration, proceed as follows:

Procedure

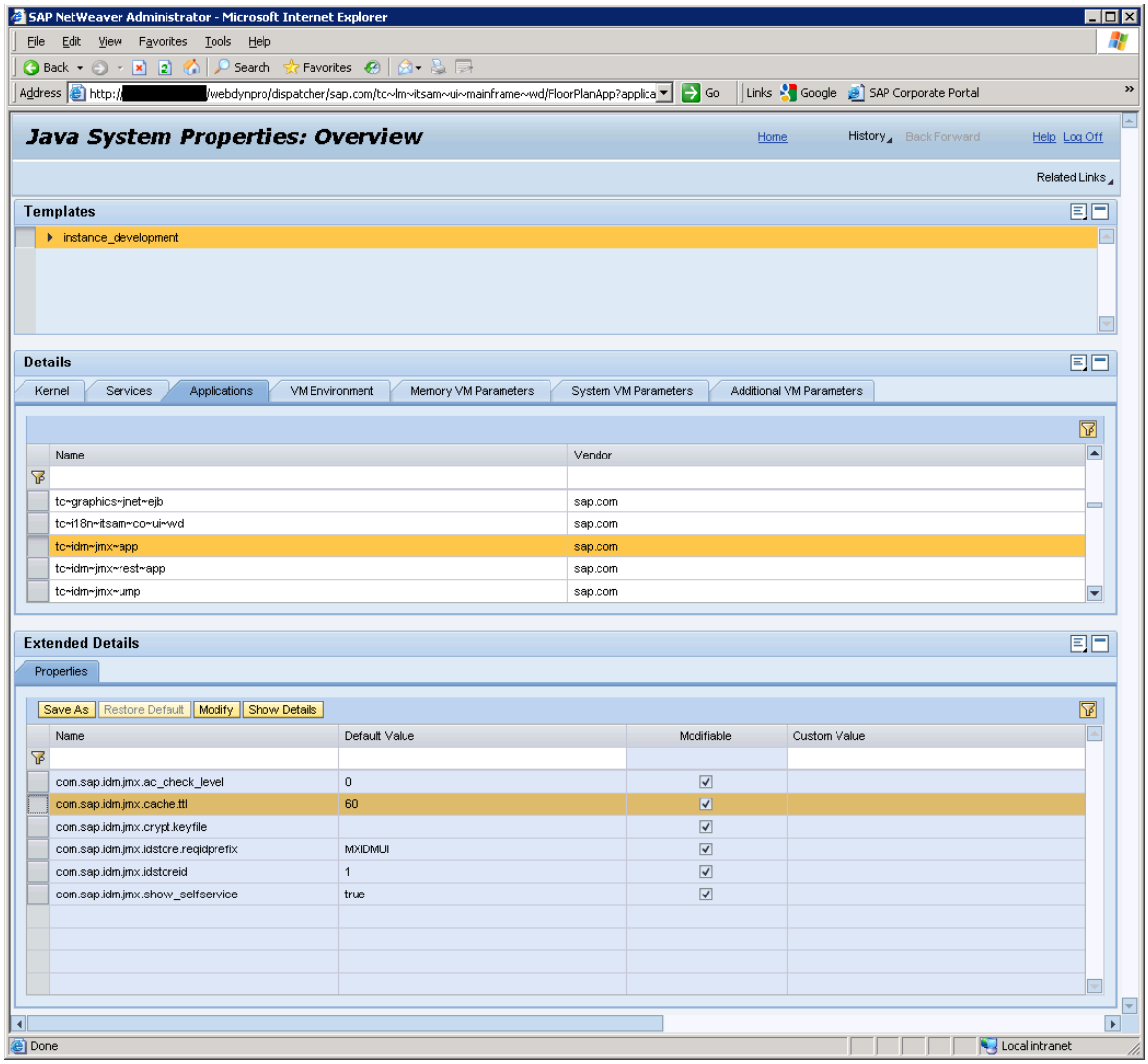
1. In the SAP NetWeaver Administrator, go to ▶ *Configuration* ▶ *Infrastructure* ▶.



2. Select *Java System Properties*.



3. Select the *Applications* tab in the *Details* section.



4. Find and select the *tc~idm~jmx~app*. In the *Extended Details* section, you can see the following properties:

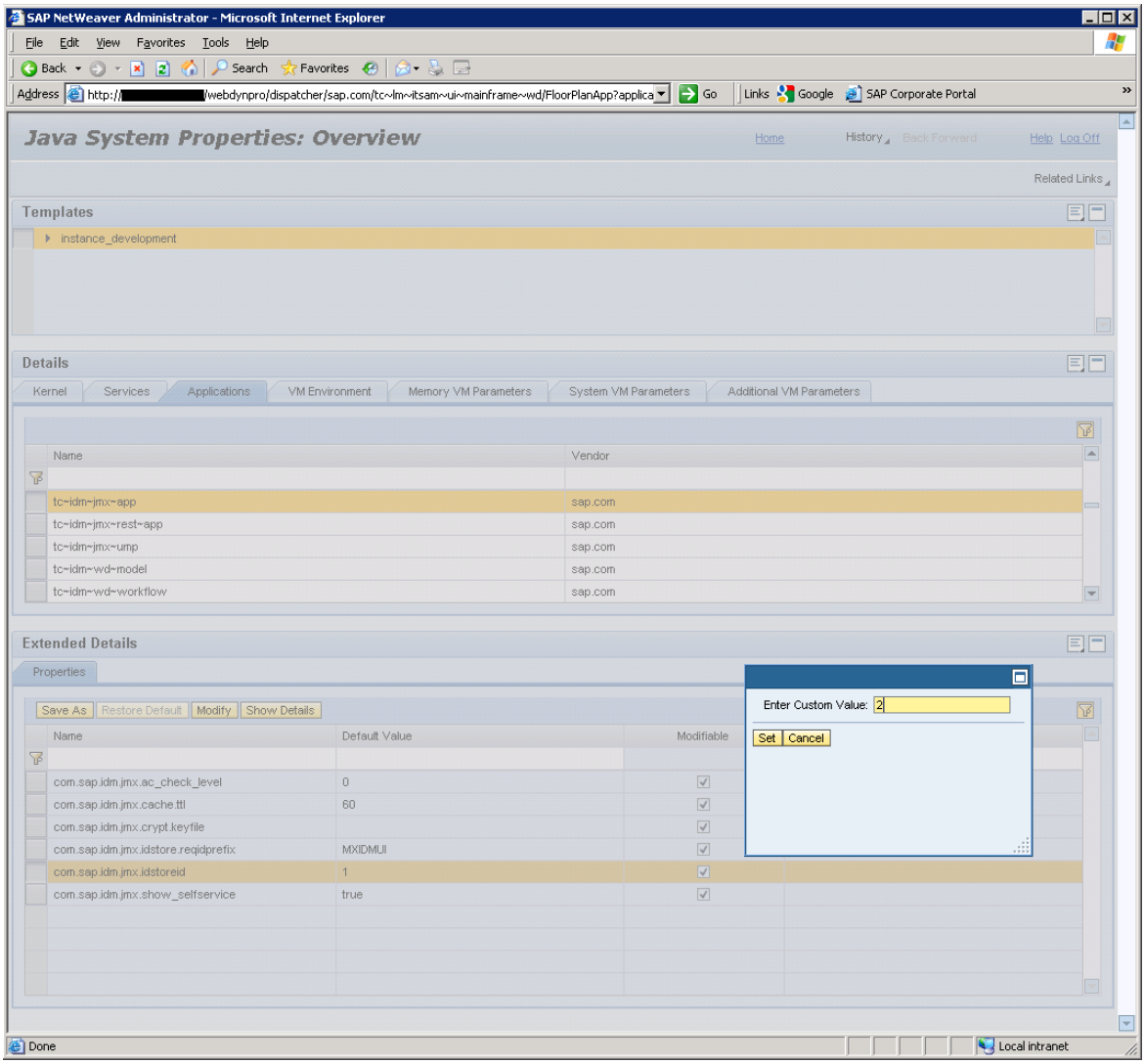
Property	Description

`com.sap.idm.jmx.ac_check_level`	This property is used to specify how to display task folders in the Identity Management User Interface improving performance for task access control. By using this mechanism the initial display of the folders in the task selector will be optimized, but depending on the setting, empty folders may be shown. Possible values are:
	• **8**: Displays all available task folders. No access control rules are enforced while displaying the task folders.
	• **4**: Performs a check to decide if the task(s) in a folder are applicable to the selected entry type. This is the recommended value in a production system.
	• **2**: Performs a check to decide if the task(s) in a folder are applicable to the selected entry type and if the current user is allowed to see them. This does not check if the user is allowed to execute the task(s) on the selected entry.
	• **0**: Performs a full check of all the folders and tasks in the task tree, including the following:
	  • If the task(s) in a folder are applicable to the selected entry type
	  • If the current user is allowed to see them
	  • If the current user is allowed to execute the task(s) on the selected entry. This is the default value.
	Note
	The recommended property value for optimal performance in a production system is **4**. There is a chance that empty folders are initially displayed but regardless of the property value, full access check (property value **0**) is always performed for tasks. Thus, only those tasks that the user is allowed to execute are displayed.

`com.sap.idm.jmx.cache.ttl`	This is time-to-live for the elements in the cache. Set to 60 minutes by default. **Note** The cache property set to 60 minutes is recommended for the production systems. To achieve more reactive system behaviour in a development/test system, set the value to 1 or 2 minutes.

Property	Description
`com.sap.idm.jmx.crypt.keyfile`	A file holding the 3DES keys, that is, the `Keys.ini` file. Set the value to be the full path to the `Keys.ini` file. For example: `\\<host>\sapmnt\<SAPSID>\SYS\global\security\data\Key\Keys.ini`, where `<SAPSID>` is the SAP system ID of SAP Identity Management system. **Note** The value of this property must be the same in the SAP NetWeaver Config Tool. Make sure you have provided the same path to the `Keys.ini` file, you have saved your configuration and restarted the `tc~idm~jmx~app` application. See *SAP Identity Management Security Guide* for details about managing the `Keys.ini` file.
`com.sap.idm.jmx.idstore.reqidprefix`	This holds a string with a prefix for all the requests sent, identifying the application which owns requests – here MXIDMUI, used by the Identity Management User Interface. The string contains only letters a through z (upper or lower case) and the numbers 0 to 9. Application strings starting with MX are reserved. The following applications are defined: • MXGRC: Used by the GRC integration. • MXIDMUI: Used by the Identity Management User Interface. **Note** Any application identifier may be defined as a user defined application identifier in a project, as long as it does not start with MX.
`com.sap.idm.jmx.idstoreid`	Identifier of the IDStore to log into.
`com.sap.idm.jmx.show_selfservice`	A Boolean property determining visibility of the *Self Services* tab in the User Interface. Set to true by default (i.e. the *Self Services* tab is visible by default).

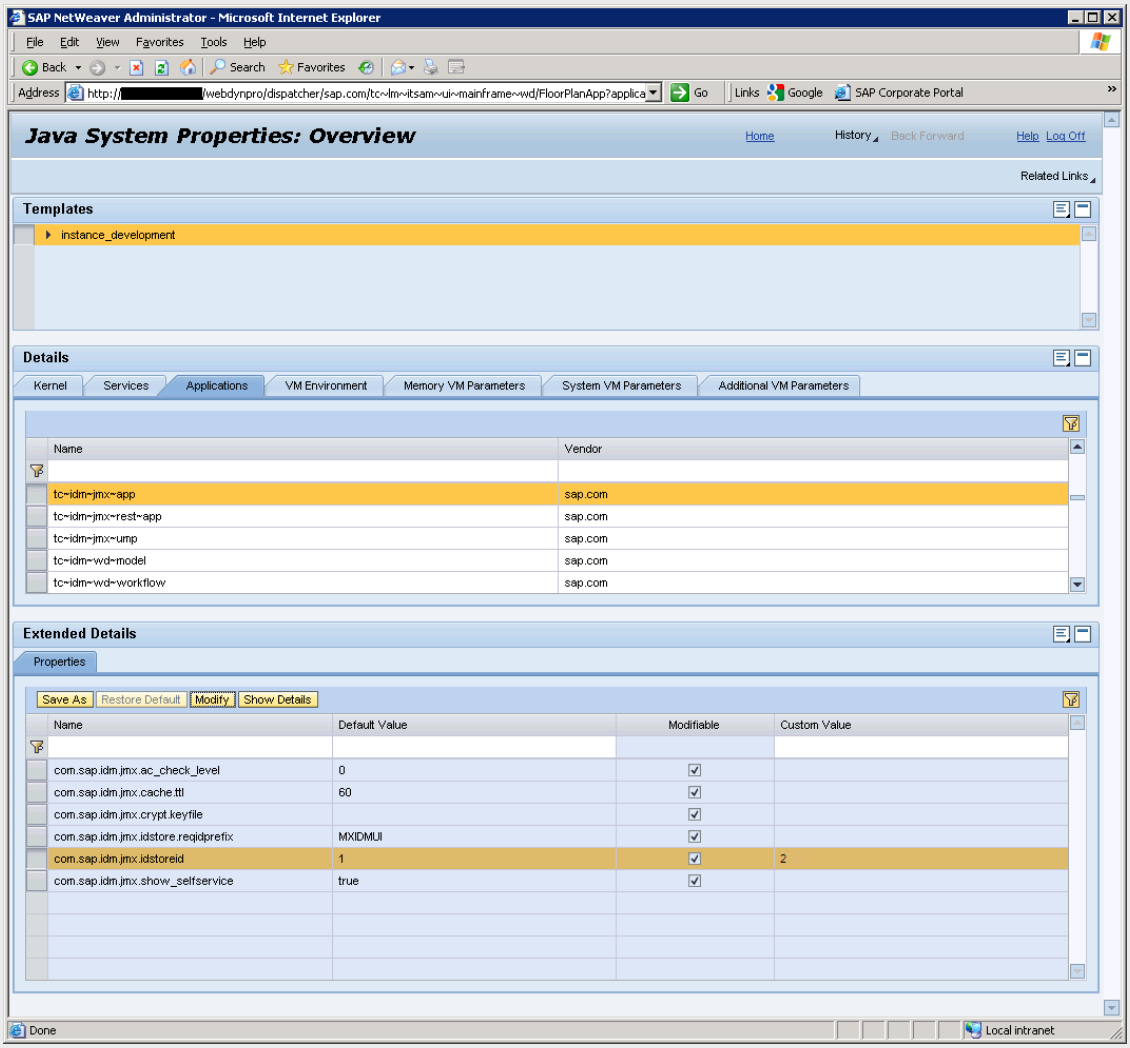
5. To make changes to the configuration, select the property you wish to edit and change (e.g. com.sap.idm.jmx.idstoreid), and choose *Modify*.



6. Enter the custom value and choose *Set* to change it.

> ### Note
>
> Changing the com.sap.idm.jmx.idstoreid property is used as an example of how to edit and change the properties in the JMX layer. The properties should only be changed if necessary. Here, the value 2 is used for demonstration purposes. Be sure to use the real identity store IDs from your Identity Center when editing the com.sap.idm.jmx.idstoreid property.

The new value is now inserted:



7. Choose *Save As* to confirm the change.

Related Information

SAP Identity Management Security Guide

2.5.16 Initial Configuration of Identity Management User Interface

Authentication of the users logging on to the Identity Management User Interface is done by the User Management Engine (UME). There are three URLs that can be used to access the Identity Management User Interface, where two of them are in scope of this document:

- `http(s)://<host>:<port>/idm` to access the main Identity Management User Interface containing the self-service tab and the manager tabs.
- `http(s)://<host>:<port>/idm/admin` to access the administrator tabs of the Identity Management Administration User Interface.

For more information on the Identity Management User Interface URLs, see *SAP Identity Management Security Guide* (section *5.1.1 Access to the Identity Management User Interfaces (URLs)*).

What parts of the Identity Management User Interface are available depends on which UME actions are assigned to the user and what privileges are given in the Identity Center. For details, see *SAP Identity Management Security Guide* (sections *5.1.2 Providing General Access (UME Actions) and 5.1.3 Providing Specific Access (Identity Management Privileges)*.

Before running the User Interface a role needs to be created, giving any authenticated user a general access to the Identity Management User Interface. To do so, you must have a user that has a permission to create and assign roles when logged-on the UME.

Related Information

Adding User(s) to the Identity Store [page 154]
General Access (Self Services Tab) [page 156]
Access to Monitoring (Monitoring Tab) [page 162]
Configuring the Language Settings for the Identity Management User Interface [page 163]
General Access to Identity Management User Interface [page 164]
Access to Manager and Administrator Tabs [page 165]

2.5.16.1 Adding User(s) to the Identity Store

Context

To be able to use the *Self Services* tab and other manager and administrator tabs (except the *Monitoring* tab) in the Identity Management User Interface, the user must be defined in both UME and in the Identity Management identity store. This is not necessary for access to the *Monitoring* tab, i.e. it is sufficient that the user exists in UME.

The link between the users is the UME `User ID` and the user's `MSKEYVALUE` in the identity store. These must match (casing is ignored). Whether this user is created in the identity store before or after the role creation is not of importance.

> **Note**
>
> Any user can be added using the below described procedure. However, typically only admin users (and/or some test users) are created this way (manually) to get started, while end-users usually are imported and synchronized using for instance SAP Provisioning Framework, or independently of the SAP Provisioning Framework.

To create an admin user (user with manager and/or administrator privileges) in the identity store, do the following:

Procedure

1. In Identity Management Developer Studio, select the identity store in the tree view and open the identity store properties.
2. In the *General* tab, choose *Add User...* button. This will open *Add Identity Store User* dialog box:

   Enter the user name in the *User Name* field.

   Select *Add Manager Privileges* and/or *Add Administrator Privileges* to give access to manager/ administrator tabs in the Identity Management User Interface. See section *Access to Manager and Administrator Tabs* for more information. For access to *Monitoring* tab, see section *Access to Monitoring (Monitoring Tab)*.
3. Choose *OK* to close the dialog box and add the user to the identity store.

   > **Note**
   >
   > A check is performed if the user to be created exists in the UME or not, and a message is displayed. If the user does not exist in the UME, you will need to create it there too in order to access the Identity Management User Interface. To close the message and to create the user in the identity store, choose *OK*.

Related Information

Access to Manager and Administrator Tabs [page 165]

Access to Monitoring (Monitoring Tab) [page 162]

2.5.16.2 General Access (Self Services Tab)

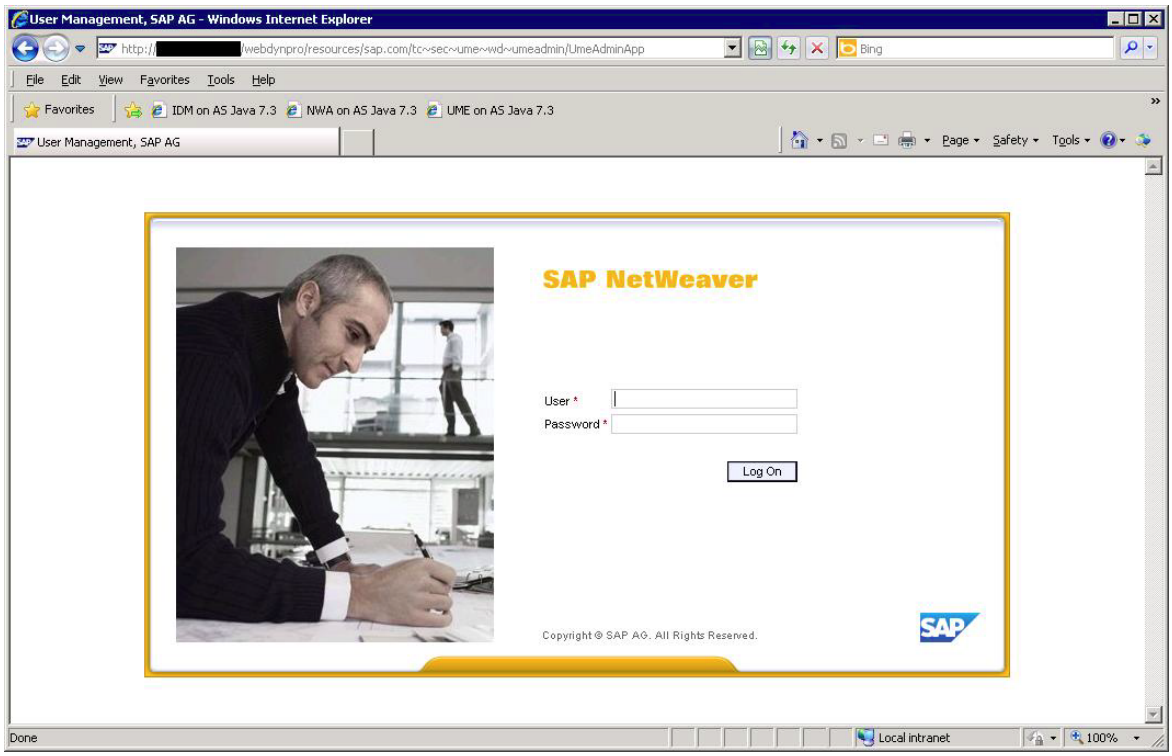
Self service forms, where users can change its own user data, request the role etc, can be accessed from the *Self Services* tab.

Context

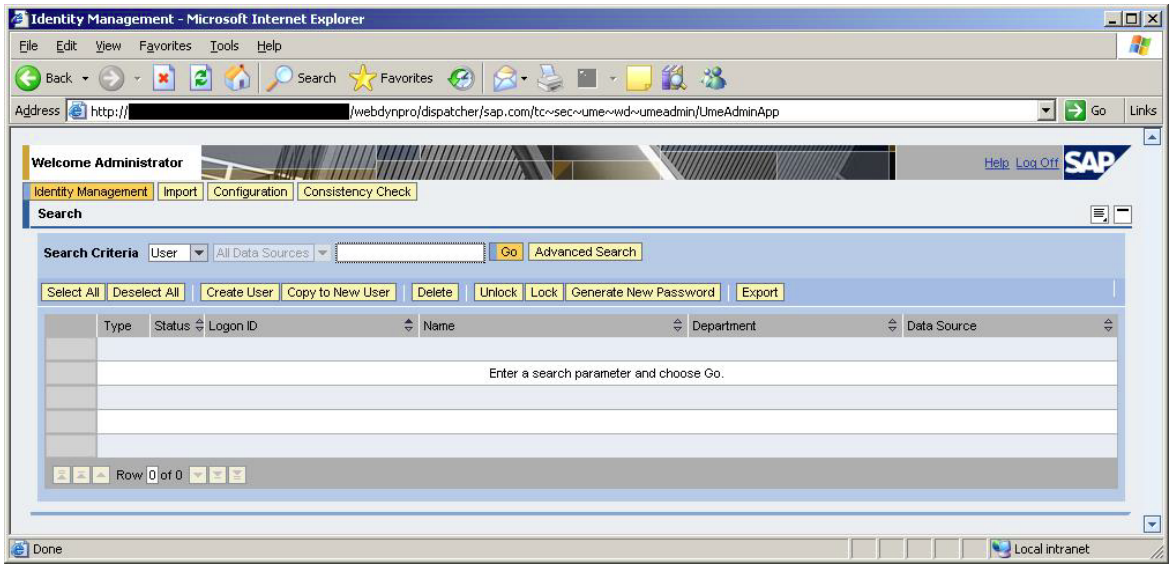
To create a role that gives access to *Self Services* tab, do the following:

Procedure

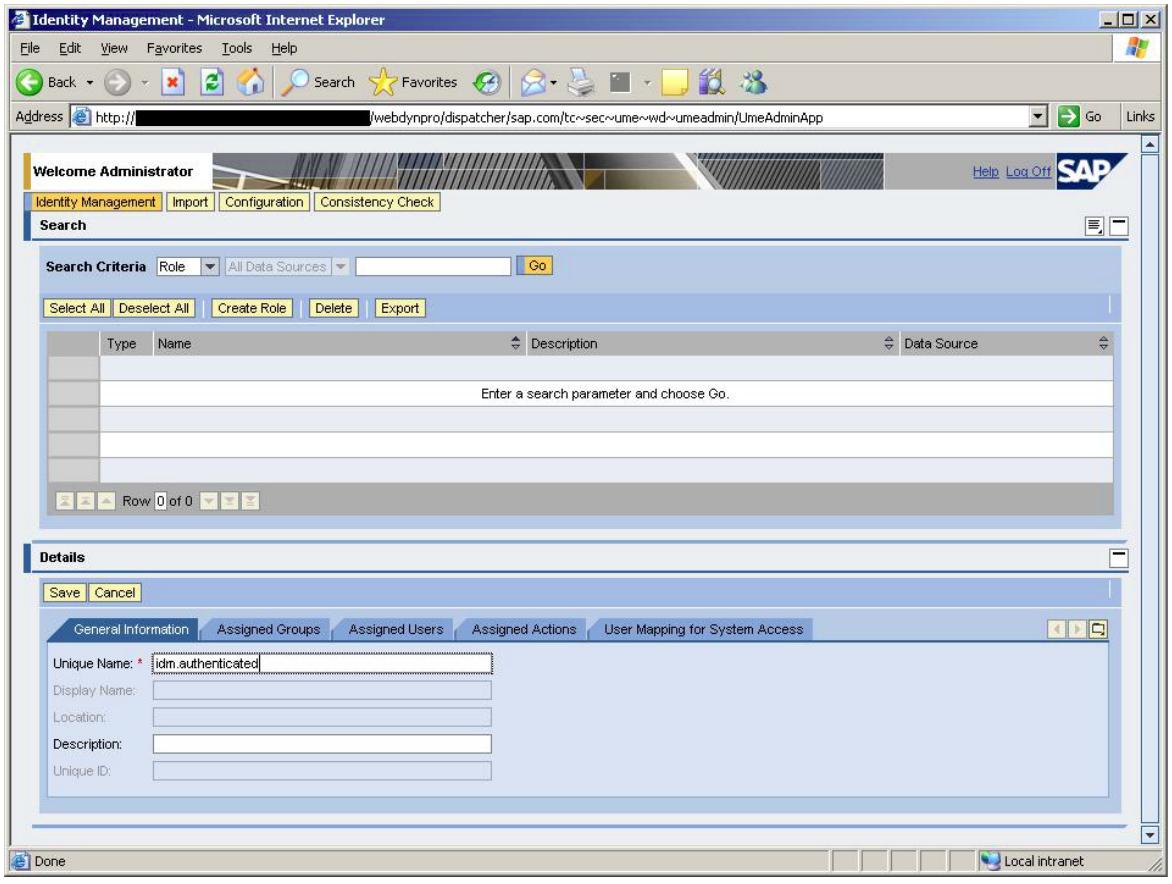
1. Enter: `//<host>:<port>` in your browser. This will open the SAP J2EE Engine Start Page.
2. Select *User Management*, which starts the user management administration console for the User Management Engine (UME).



3. Provide your UME credentials and choose *Log On*:



4. Change search criteria to *Role*, and then choose *Create Role*:



In the *General Information* tab fill in the following:

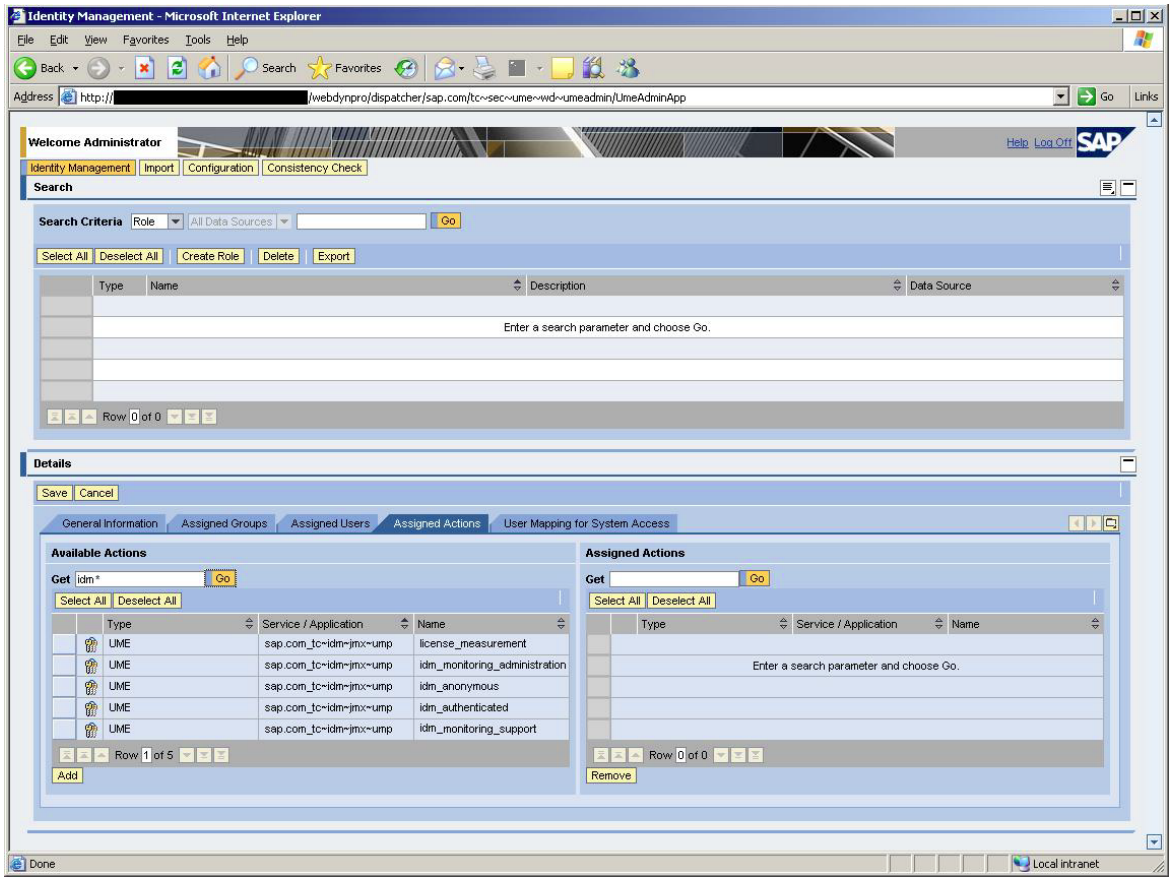
Unique Name

Give the role a describing name. The name `idm.authenticated` is used as example, but any name can be used.

Description

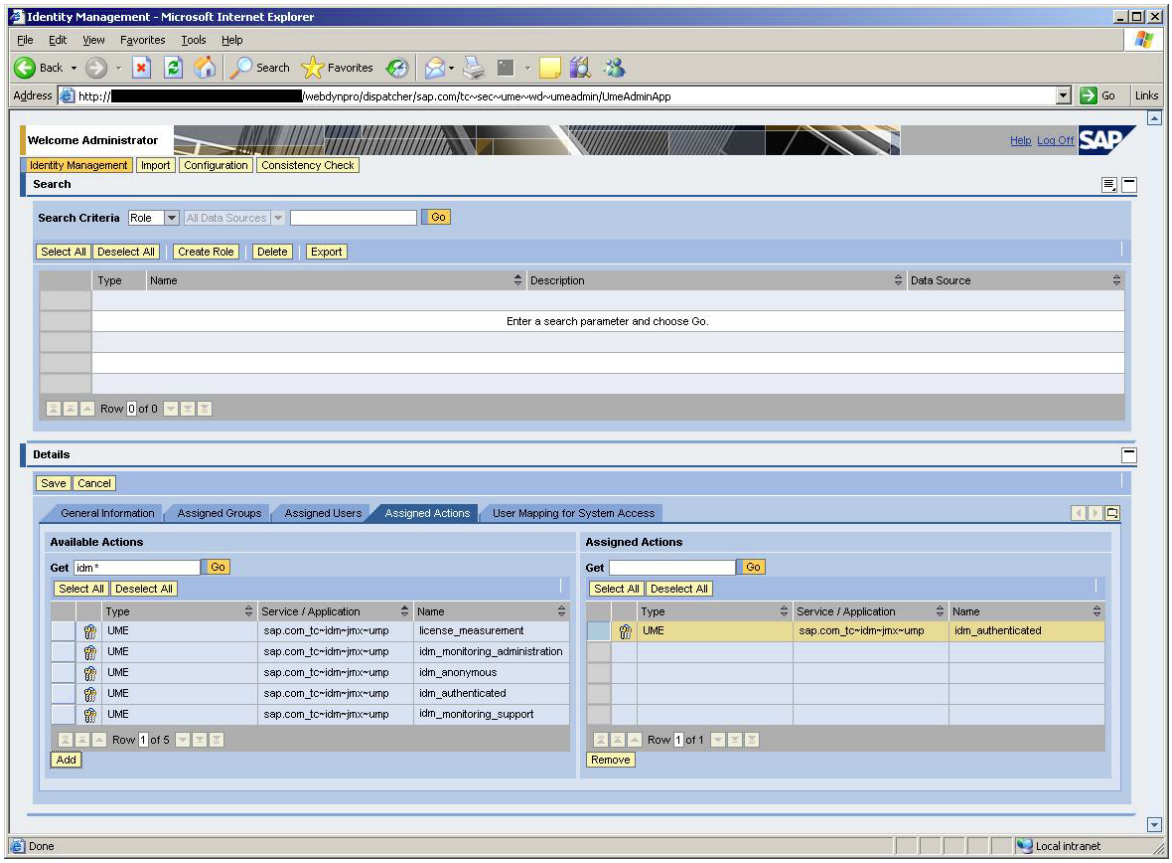
Short description of the role can be added as well. This is not a mandatory field.

5. Select the *Assigned Actions* tab.



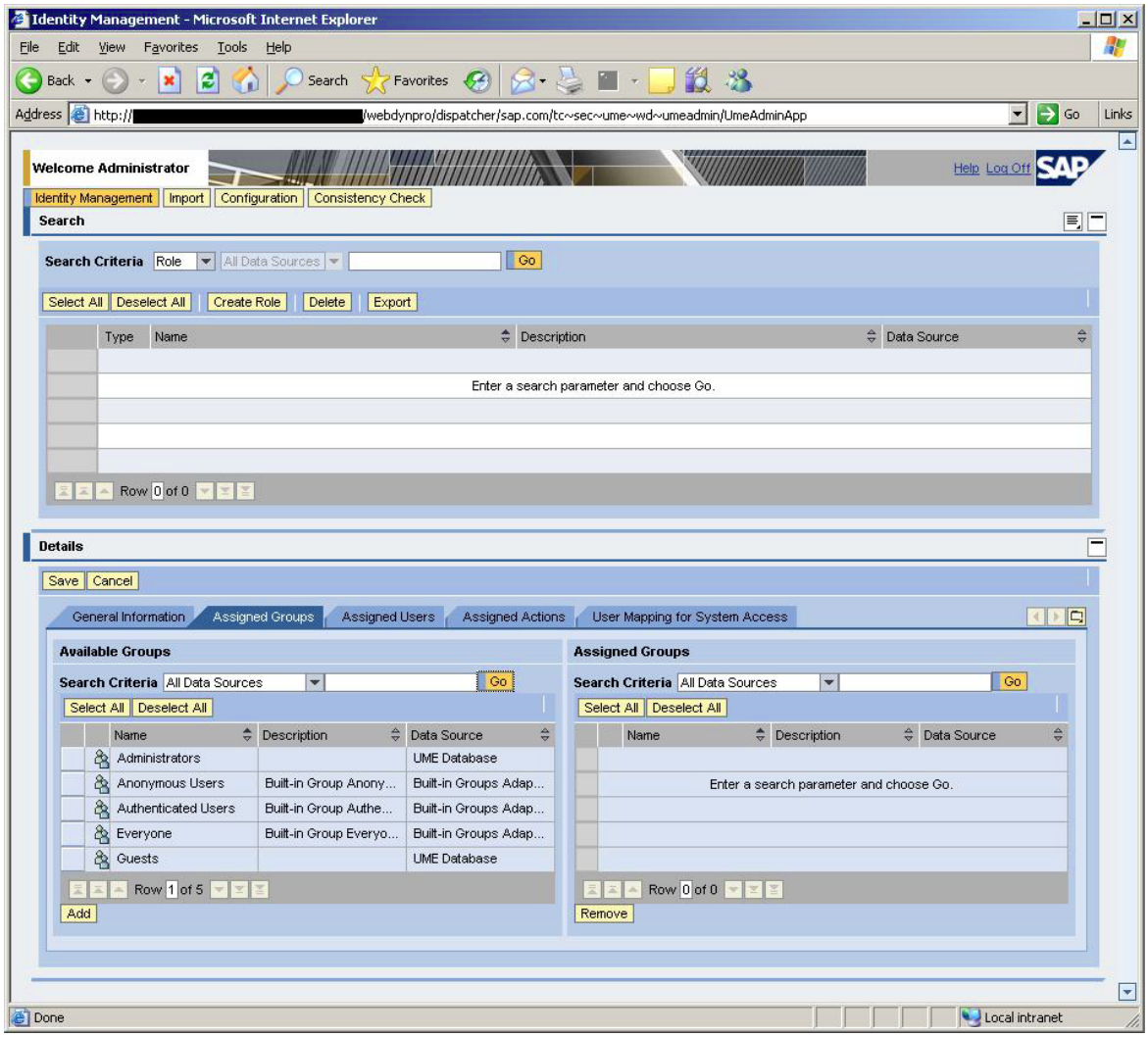
In the left pane (*Available Actions*): Type **`idm*`** in the field *Get* and choose *Go*. This will list the actions/ access rights it is possible to link to the role.

6. Select the *idm_authenticated* action and choose *Add*.



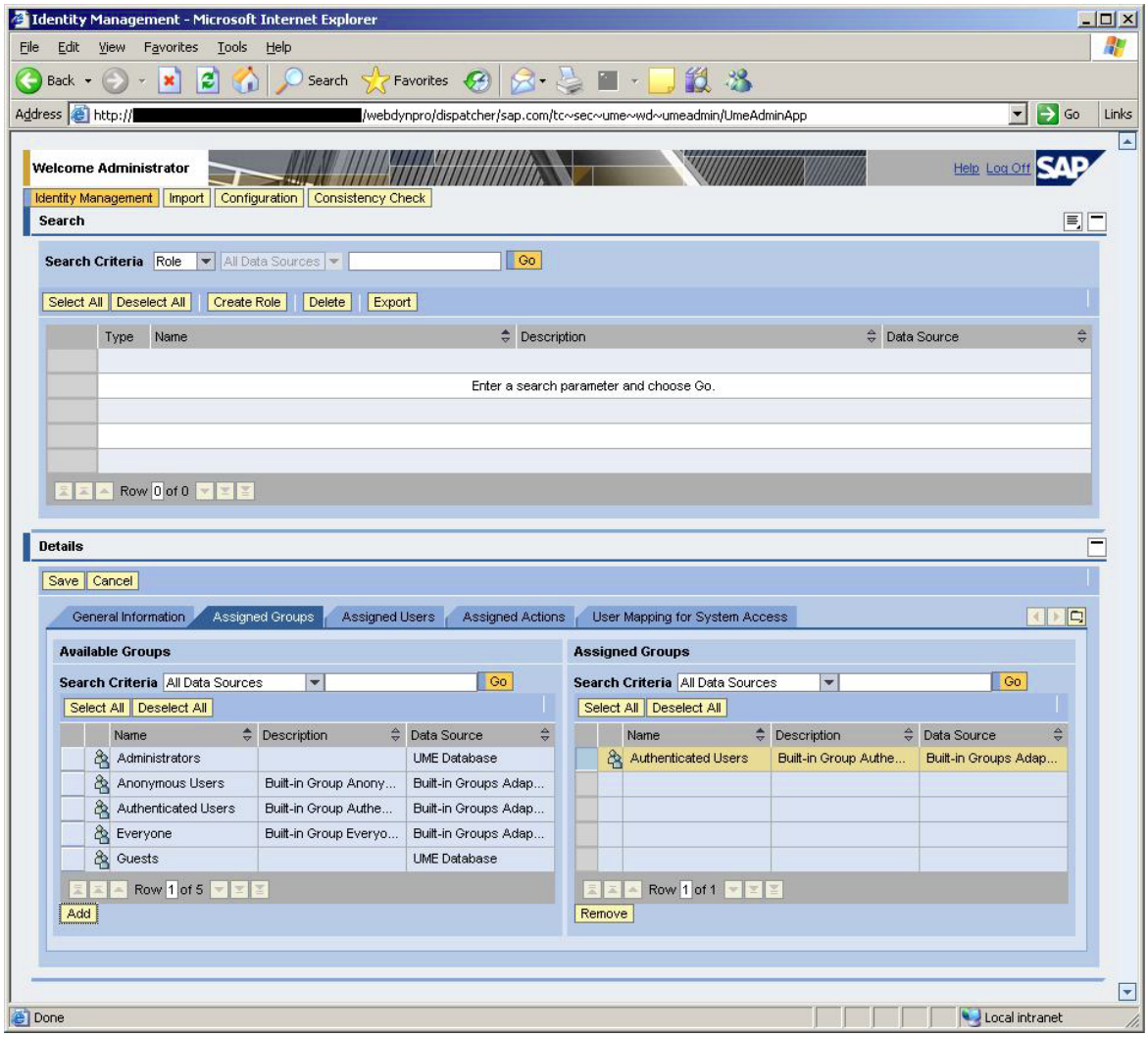
The *idm_authenticated* action is now assigned to the role and this will be shown in the right pane (*Assigned Actions*).

7. Select the *Assigned Groups* tab:



In the *Available Groups* pane, choose *Go* to list all available groups.

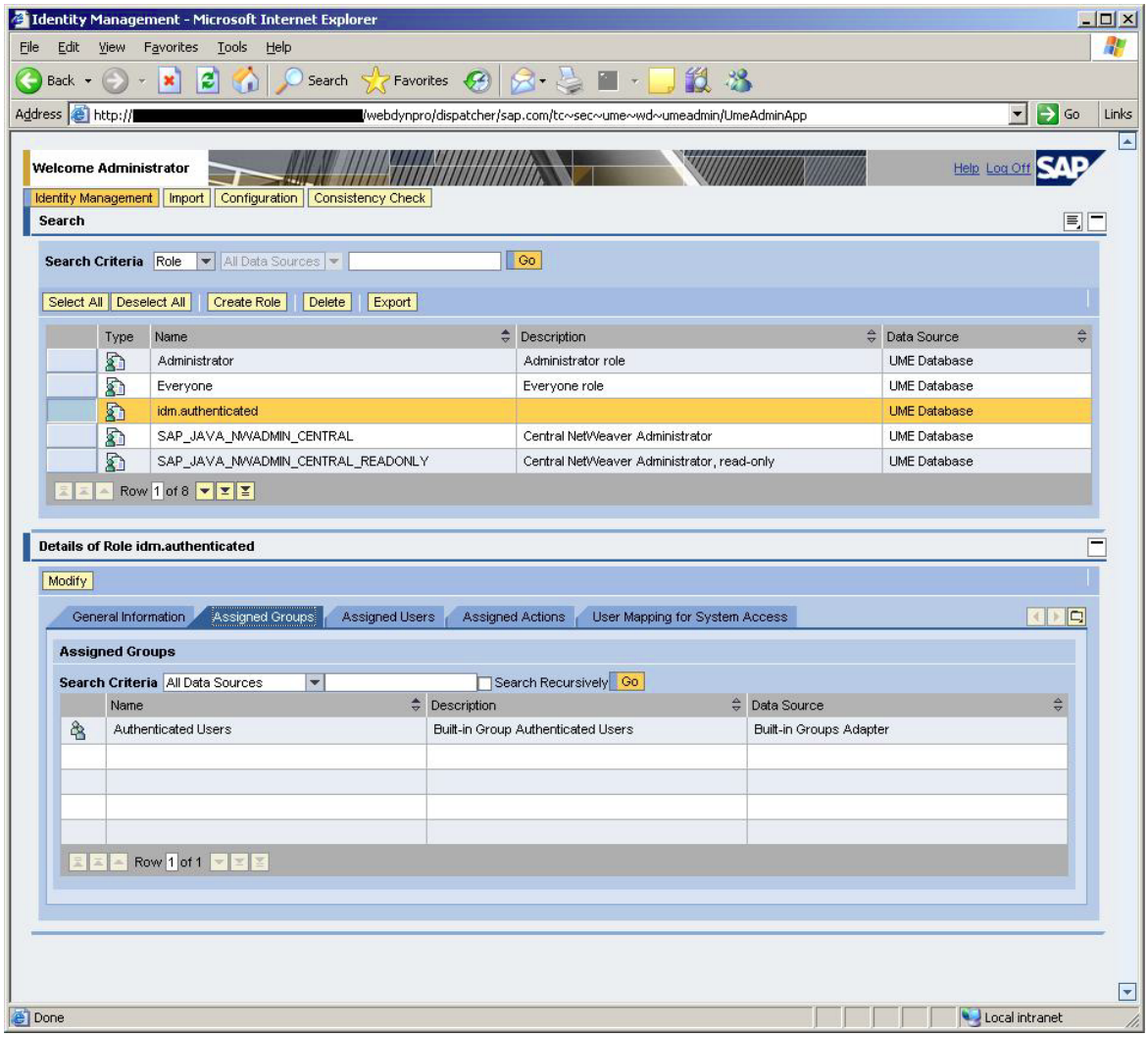
8. Select the *Authenticated Users* group and choose *Add*.



The *Authenticated Users* group is now given the role and this will be shown in the right pane (*Assigned Groups*).

Assigning the idm.authenticated role to a user group is just one of several ways to give general access to the User Interface. If only some of the users need access to the User Interface, access can be given by assigning the role directly to those users.

9. Choose *Save* to confirm and create the new role, which will give a general access to the User Interface to every authenticated user. The just created role will be displayed in the list of the roles available:



Now that the role is created, you are able to access the Identity Management User Interface (and the *Self Services* tab).

2.5.16.3 Access to Monitoring (Monitoring Tab)

Context

It is also possible to give access to the *Monitoring* tab to those who need it. A monitoring role can be created and actions `idm_monitoring_support` (giving read only access to *Monitoring* tab) or `idm_monitoring_administration` (giving read and write access to *Monitoring* tab) can be assigned by following the same procedure as for `idm_authenticated` giving access to *Self Services* tab described in section *General Access (Self Services Tab)*. Assign the created monitoring role to *Administrators* group or a specific user who needs access to *Monitoring* tab in the Identity Management User Interface.

The *Monitoring* tab is available in the Identity Management Administration User Interface, with URL *http(s)://<host>:<port>/idm/admin*.

For more information about monitoring, see *SAP Identity Management Solution Operation Guide*.

Related Information

General Access (Self Services Tab) [page 156]
SAP Identity Management Solution Operation Guide

2.5.16.4 Configuring the Language Settings for the Identity Management User Interface

Context

The language settings for the Identity Management User Interface are determined by the language settings for user in User Management Engine (UME):

Procedure

1. Logon to UME and search for the user you want to configure the language settings for.
2. Select the user from the search list and choose *Modify* in the details pane below the list. This will open the entry detail information for editing.
3. Choose the *General Information* tab.
4. Select a language from the list in the *Language* field and choose *Save*.

   The language settings are now configured. The change will take effect after the next logon.

   > ⓘ Note
   >
   > If you have configured customized favorite buttons in the Identity Management User Interface, the language of the text on these buttons (labels) will not be automatically updated according to the new language settings. To update the language for the favorite buttons, you need to remove the existing buttons and add the updated ones.

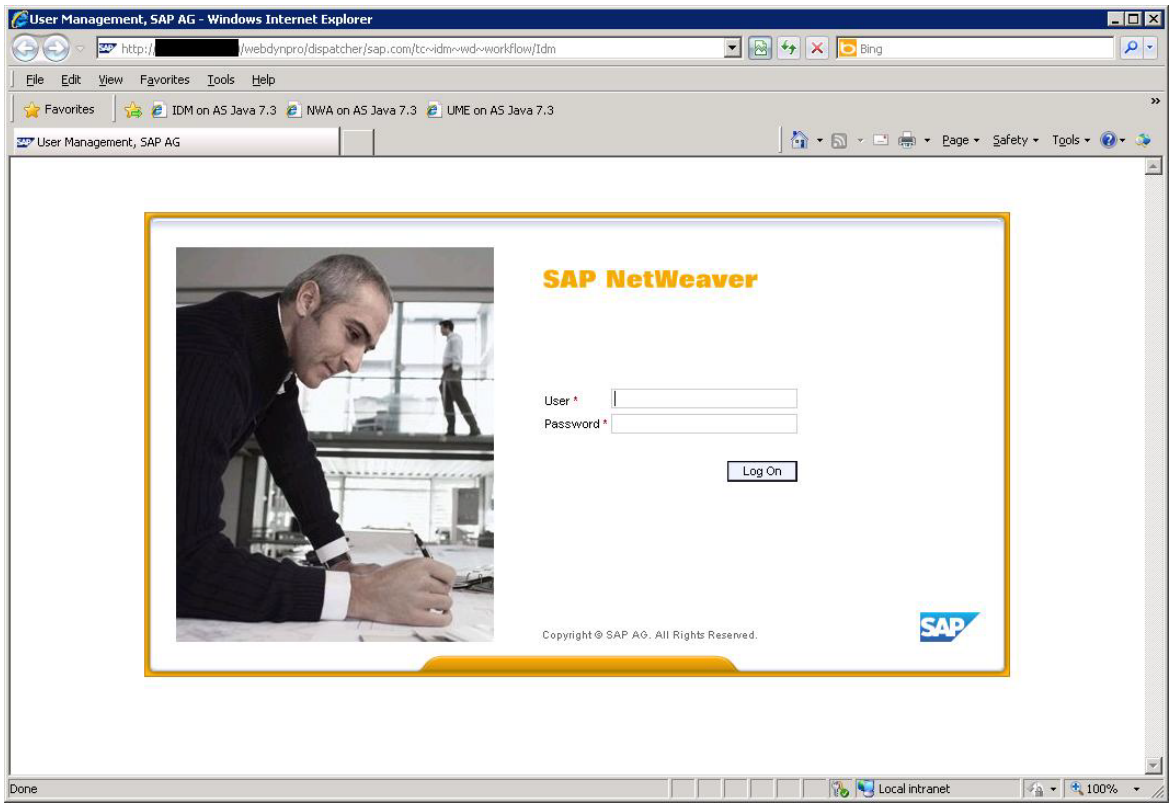
2.5.16.5 General Access to Identity Management User Interface

Context

To access the Identity Management User Interface do the following:

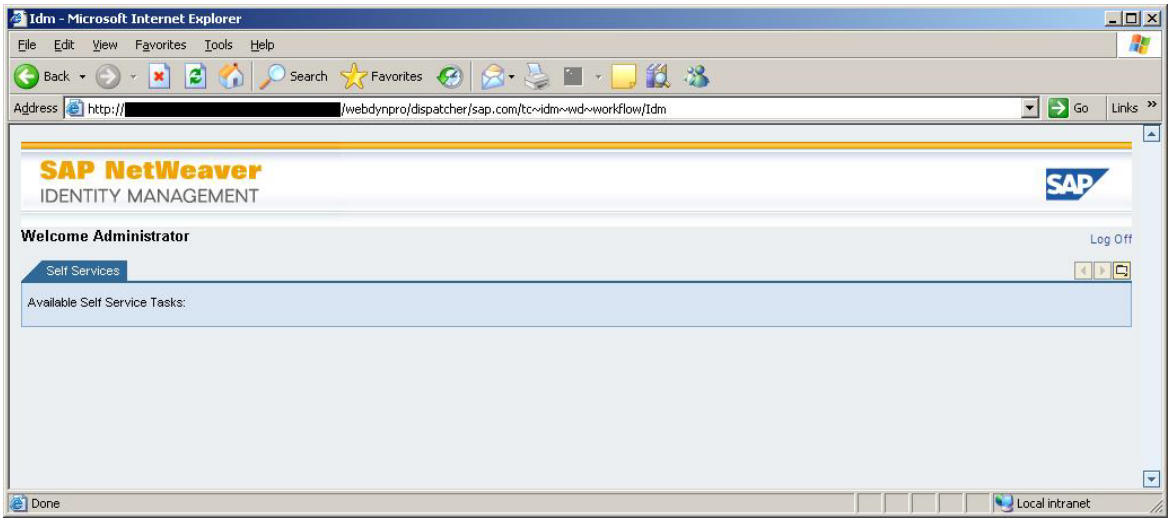
Procedure

1. Enter `http(s)://<host>:<port>/idm` in your browser.



   Provide the credentials in the log-in window.

2. Choose *Log On*.



You are now logged on to the User Interface. The image above shows the logged-in user with access to only *Self Services* tab.

2.5.16.6 Access to Manager and Administrator Tabs

Access to other tabs than the *Monitoring* tab in the Identity Management User Interface is controlled by assigning privileges to the person entries in the identity store, in the Identity Management Developer Studio.

Context

For more details about each privilege, see *SAP Identity Management Security Guide* (section *5.1.3 Providing Specific Access (Identity Management Privileges)*).

In section *Adding User(s) to the Identity Store*, the manager and administrator privileges (all) are given the created admin user automatically by selecting *Add Manager Privileges* and *Add Administrator Privileges* when adding the user to the identity store. But these privileges can also be assigned to users manually and on the need-to basis, for instance by creating a self service form for privilege assignment. You can do this in the following way:

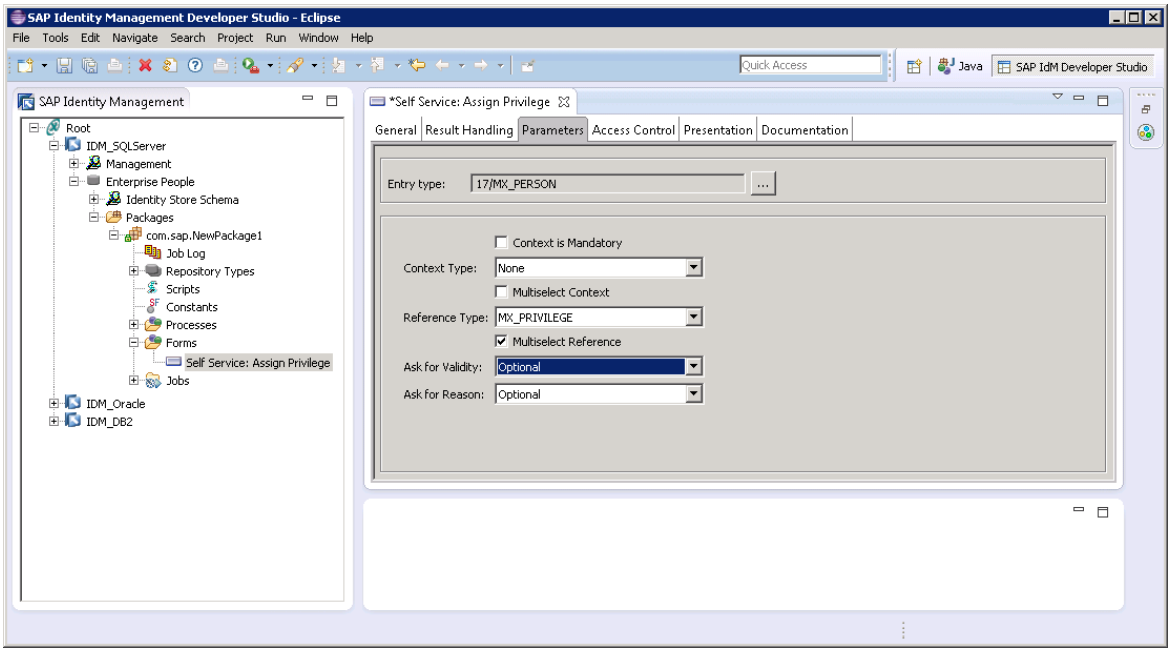
Procedure

1. In the Identity Management Developer Studio, select a package of your identity store and choose *Check out* from the context menu.
2. Select the *Forms* folder of the package and choose *New* > *Assignment Request* from the context menu to create a new form for the Identity Management User Interface.

   The form is added and the properties are displayed. Rename the form to e.g. *Self Service: Assign Privilege* (select the form in the tree view and choose *Rename* from the context menu).

3. Select the *Parameters* tab and define the following fields:

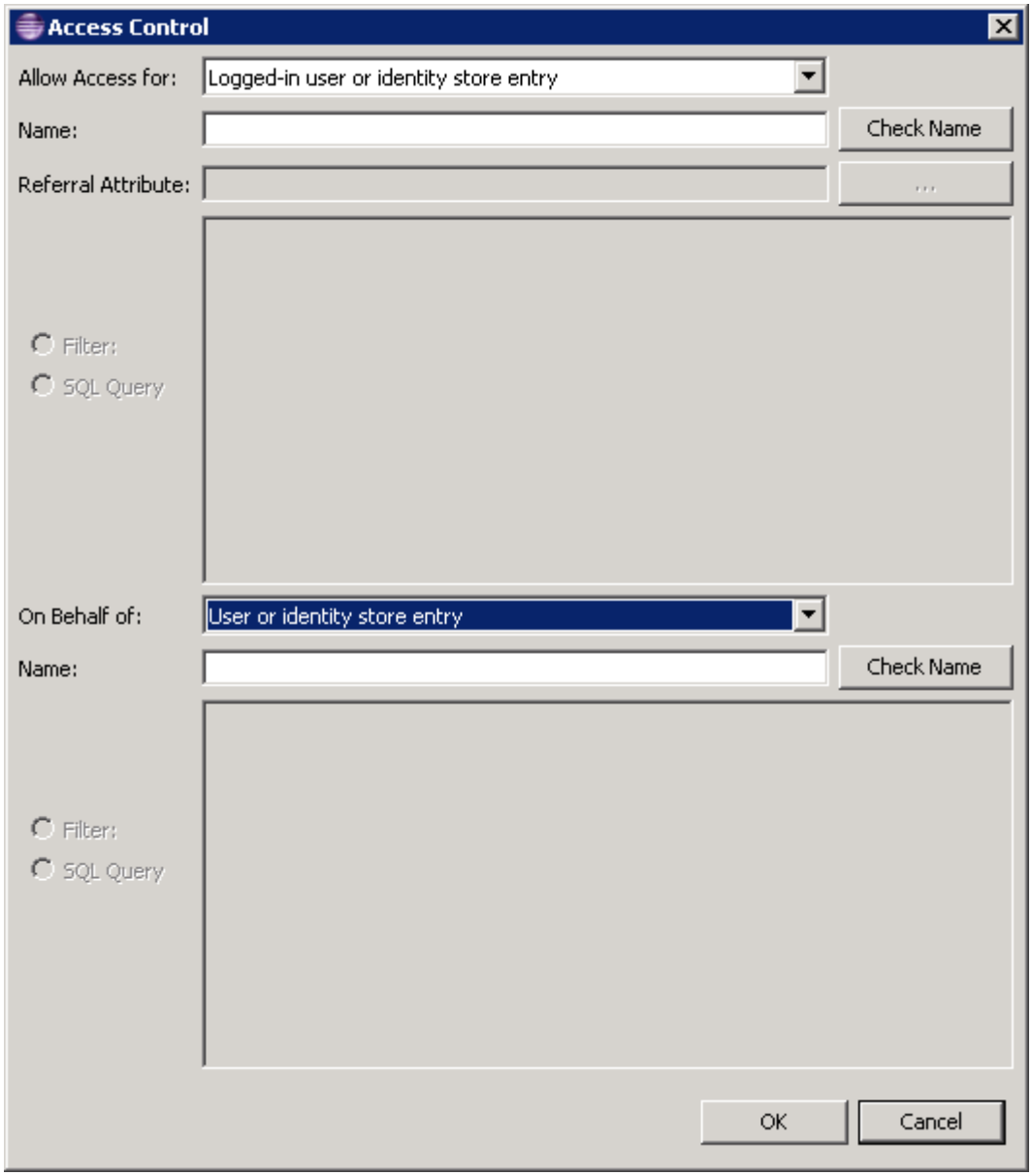
Entry Type	Select *MX_PERSON* entry type.
Context Type	Select *None*.
Reference Type	Select *MX_PRIVILEGE*.
Multiselect Reference	Select this option if you want to enable multiselection of privileges to assign to a user.
Ask for Validity	Select *Optional* to give the posibility to define a validity periode for the requested privilege(s).



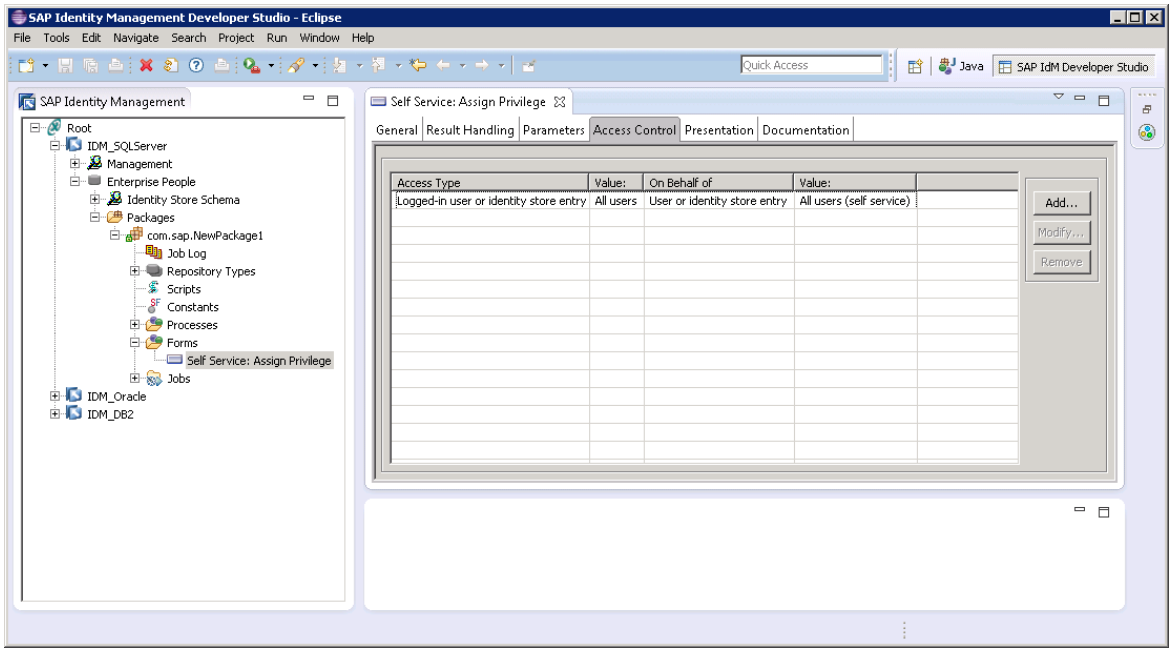
4. Select the *Access Control* tab and choose *Add...*.

   This opens the *Access Control* dialog box. Fill in the following:

Allow Access for	Select *Logged-in user or identity store entry*.
Name	Leaving this field empty will make the task accessible to everyone. Name is entered when restricting the access to the task (e.g. enter *Administrator* name to give access to this task only to the *Administrator* user).
On Behalf of	There are two ways of creating a self service task. You either select *User or identity store entity* or *Relation - Self*. Both ways are legitimate.

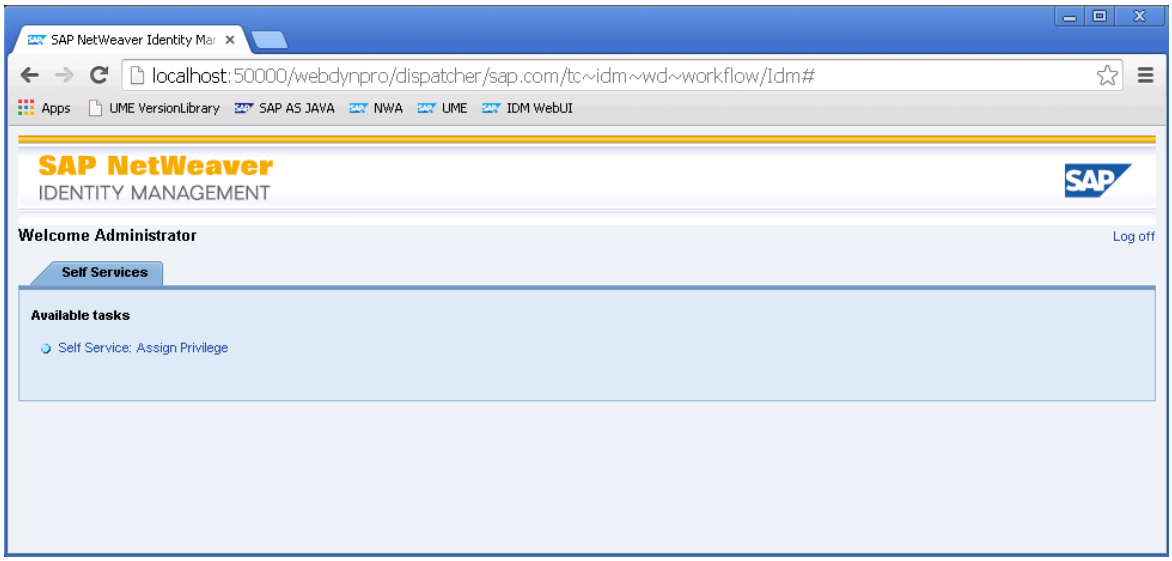


5. Choose *OK* to close the dialog box and add the defined access control to the form.

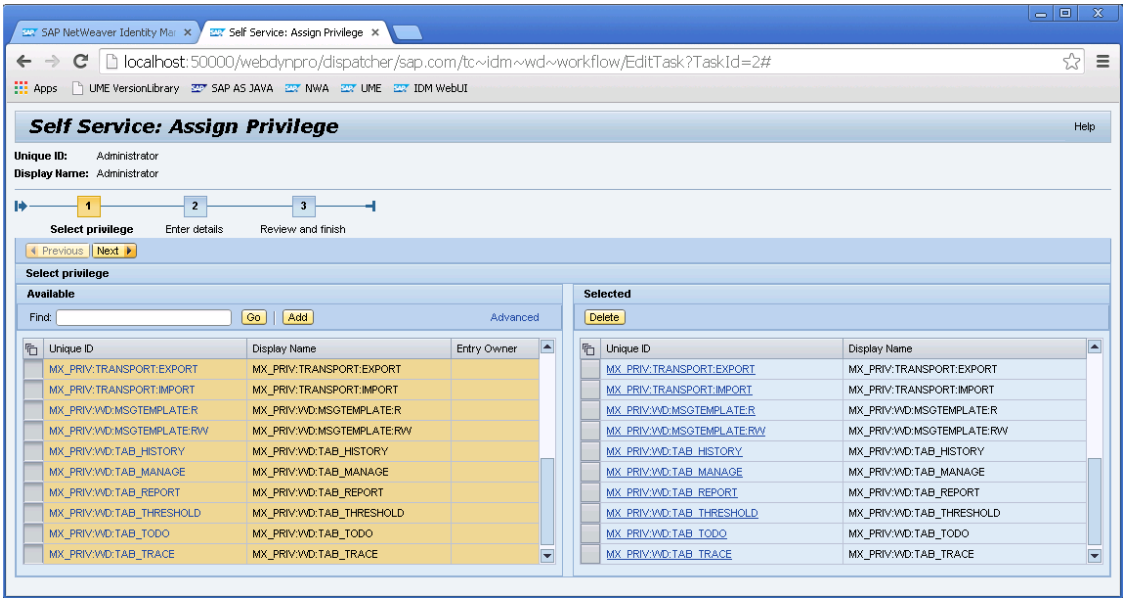


6. Save the changes applied to the form. Choose *File* > *Save* or press Ctrl + S.

   Now the self service form is created and visible in the *Self Services* tab of the Identity Management User Interface:



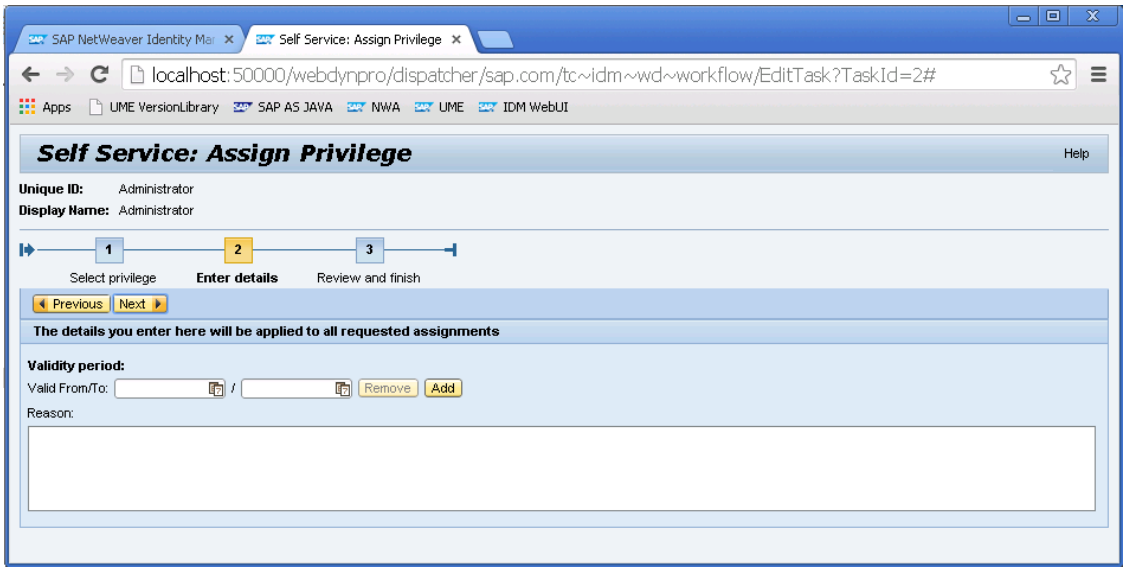
7. To assign privileges and give access to other tabs than the *Self Services* tab, do the following:
   a. Select and open the self service form in the Identity Management User Interface.
   b. Choose *Go* on the left side of the pane (under *Available*) to list available privileges:



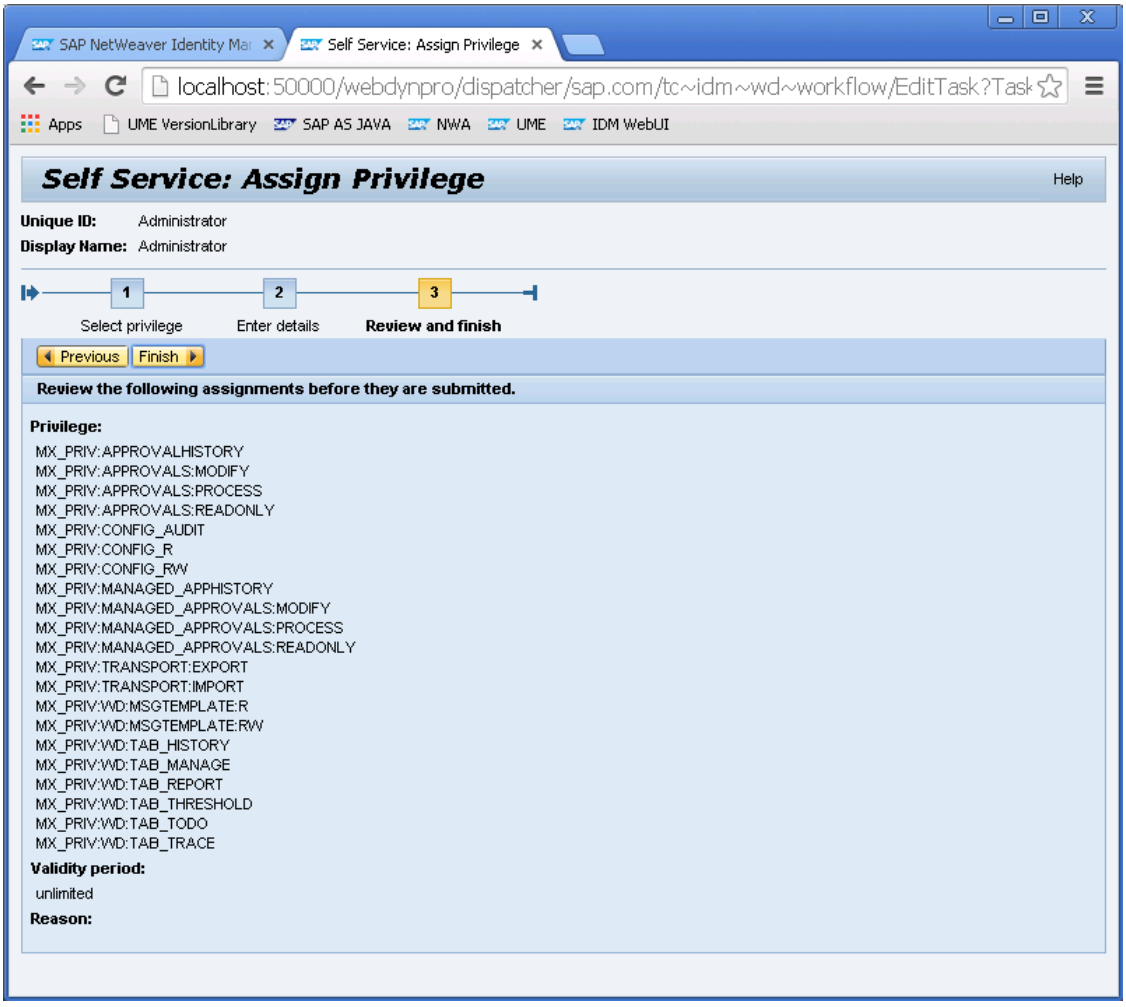
> **Note**
>
> When searching for any specific entry (persons, roles, privileges and so on) in the Identity Management User Interface, make sure you always provide the language-specific characters of that entry. For example: To search for an entry containing an accented "e" ("é"), you should type "é". If you provide only "e", the entry will not be displayed in the search result.

c. Select the desired privileges. In order to select multiple rows simultaneously, enable the option *Multiselect Reference* in step 3. Choose *Add*.

d. Choose *Next*, and optionally define validity periode and reason for the privileges that are to be assigned:



e. Choose *Next* and review the selections:



Confirm and execute the form by choosing *Finish*.

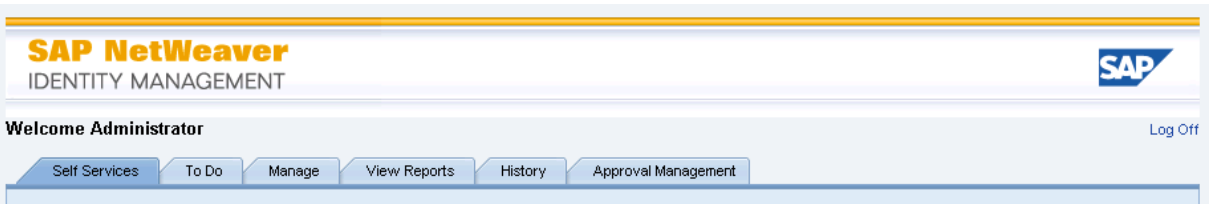
8. Close the self service form.

Results

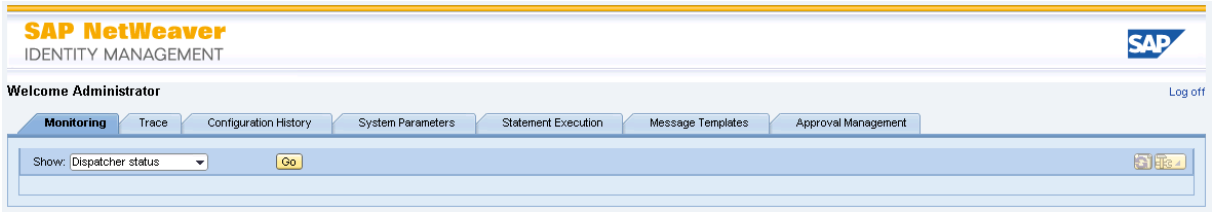
The privileges are now added and the tabs should be visible in the Identity Management User Interface.

> ⓘ Note
>
> You will need to choose the *Refresh* button before the tabs are visible.

Here for the URL `http(s)://<host>:<port>/idm`:



And for the **`http(s)://<host>:<port>/idm/admin`**:



Related Information

SAP Identity Management Security Guide
Adding User(s) to the Identity Store [page 154]

2.5.17 Defining Customer Specific Themes for Web Dynpro Applications

As a Web Dynpro application, SAP Identity Management User Interface may be adapted. You can define a specific theme (the look and feel) of your User Interface application.

Customer-specific themes can be defined for Web Dynpro applications. Users are advised to set their themes according to where their applications run. The applications can run as standalone applications or inside the SAP Enterprise Portal. The process of defining the themes depends on whether your application runs standalone or inside the portal, and on the SAP NetWeaver version you are using.

For more information, see the Related Information.

Related Information

SAP NetWeaver 7.3
Configuring the Web Dynpro Runtime Environment
Setting the Theme
SAP NetWeaver 7.3 EHP1
Configuring the Web Dynpro Runtime Environment
Setting the Theme
SAP NetWeaver 7.4
Configuring the Web Dynpro Runtime Environment
Setting the Theme
SAP NetWeaver 7.5
Configuring the Web Dynpro Runtime Environment
Setting the Theme

2.5.18 Keyboard Access for User Interface Elements in Web Dynpro

As a Web Dynpro application, SAP Identity Management User Interface may be adapted. You can create and activate keyboard access for User Interface elements.

It is possible to activate keyboard access for User Interface elements in applications running in the HTML client and based on Web Dynpro for ABAP or Java. This information is relevant to you if you use the keyboard to navigate around your application's UI and use its functions.

To use the keyboard commands, you must enable the accessibility mode. Many of the commands also work when accessibility mode is disabled, but others, such as group navigation or navigation of inactive UI elements, only work when it is enabled.

For more information about how to enable keyboard access, see the Related Information (for supported SAP NetWeaver versions).

Related Information

Keyboard Access for Web Dynpro for ABAP / for Java for SAP NetWeaver 7.3
Keyboard Access for Web Dynpro for ABAP / for Java for EHP 1 for SAP NetWeaver 7.3
Keyboard Access for UI Elements in Web Dynpro (New Rendering) for SAP NetWeaver 7.4
Keyboard Access for UI Elements in Web Dynpro (New Rendering) for SAP NetWeaver 7.5

2.5.19 Integrating Identity Management User Interface in the SAP Enterprise Portal (optional)

You can integrate the Identity Management User Interface in the SAP Enterprise Portal. Before it can be integrated in the SAP Enterprise Portal, the Identity Management User Interface should be installed and configured locally on the SAP Enterprise Portal, as described in this document.

You need to perform the following configuration in the SAP Enterprise Portal:

- Import the predefined content for the SAP Enterprise Portal.
- Check the Portal integration of the Identity Management User Interface.

2.5.19.1 Importing Predefined Contents for the SAP NetWeaver

Context

To import the contents to the Portal, do the following:

Procedure

1. Log on to the Portal as system administrator.
2. Select the *System Administration* tab and its sub-tab *Transport*, and then navigate to *Transport Packages/ Import*.
3. Import the .EPA archive (role, worksets, iViews). The .EPA archive is provided in the *Misc* subdirectory in the installation kit for the Designtime Components.

   For more details on importing and deploying of EPA archives, see the Related Information.

Related Information

Importing and Deploying EPA Archives for SAP NetWeaver 7.3
Importing and Deploying EPA Archives for EHP 1 for SAP NetWeaver 7.3
Importing and Deploying EPA Archives for SAP NetWeaver 7.4
Importing and Deploying EPA Archives for SAP NetWeaver 7.5

2.5.19.2 Verifying the Portal integration of the Identity Management User Interface

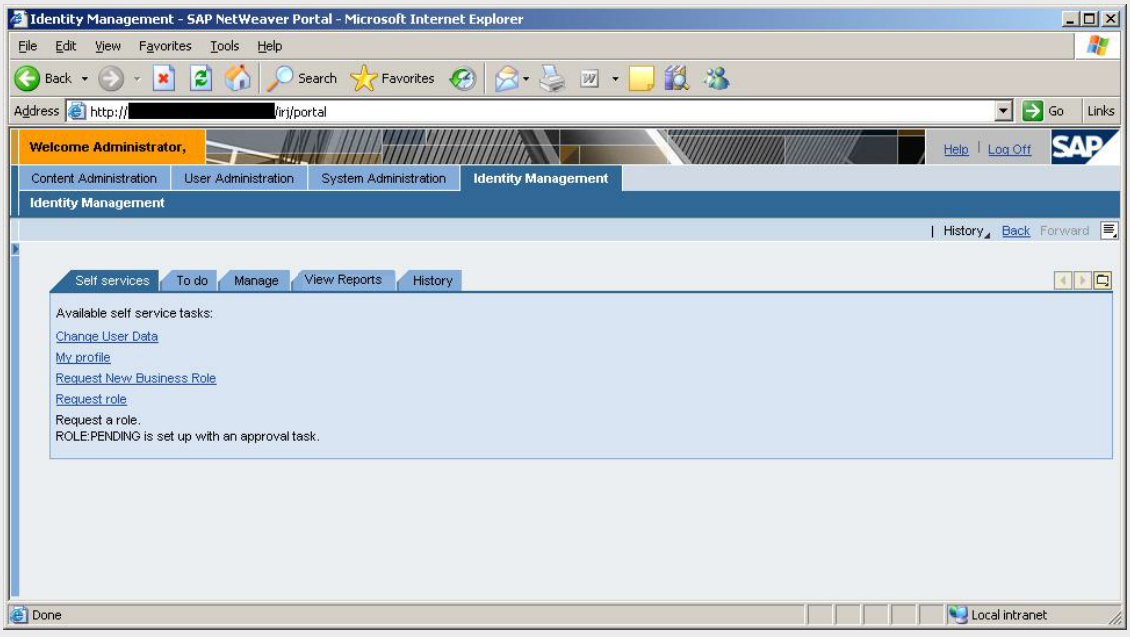
Context

To verify the Portal integration, do the following:

Procedure

1. Log on to the SAP Enterprise Portal with your admin user (that also exists in the identity store you would like to access through the Portal).
2. Select the *Identity Management* tab in the Portal and verify that you have the access to the User Interface and its contents.

> ⓘ Note
>
> In order for this to work, you must have configured the Identity Management User Interface correctly, giving at least a general access to the User Interface to users, as described in the section *Initial configuration*.
>
> If everything is done correctly, the contents of the Identity Management User Interface will be presented under the *Identity Management* tab in the SAP Enterprise Portal. The content will be something similar to the one shown below:



Related Information

Initial Configuration of Identity Management User Interface [page 154]

2.5.20 Initial Configuration of Identity Management User Interface for HTML5

Configuring the Identity Management User Interface for HTML5 involves the following steps:

- Authorization and authentication for the REST interface:
  - Assigning the required role and actions in User Management Engine (UME)
  - Enabling single sign-on with logon tickets
- Adding the predefined forms in the Identity Management Developer Studio
- Configuring the solution

Related Information

Authorization and Authentication for the Identity Management User Interface for HTML5 [page 175]
Adding the Predefined Forms and Configuring the Solution [page 177]
Configuring the Solution [page 179]

2.5.20.1 Authorization and Authentication for the Identity Management User Interface for HTML5

To access the REST API v2, the user requires the UME action `idm_authenticated_restapi`. To access Identity Management User Interface for HTML5, the user needs the UME action `idm_authenticated_ui5` in addition to the actions required for the REST API v2. The role `idm.user` contains all three of these UME actions, and you should assign it to the user so that he or she has the appropriate authorization and authentication for the Identity Management User Interface for HTML5. These actions and the role are provided as part of the software component containing the Identity Management User Interface and the REST service. All other necessary authorizations for a service call are defined by the access control of the related Identity Management form.

The default configuration of the SAP NetWeaver Identity Management 7.2 REST API forces a logon on all requests using the provided basic authentication credentials, which consumes time and leads to a high number of security sessions in the SAP NetWeaver AS for Java. Using single sign-on (SSO) with logon tickets for the REST API improves the performance.

2.5.20.1.1 Assigning the Role idm.user

Context

Make sure that all users that will use the Identity Management User Interface for HTML5 are assigned the role `idm.user` (this assigns the neccessary UME actions `idm_authenticated_restapi` and `idm_authenticated_ui5` to the user).

To assign the role to the users, proceed as follows:

Procedure

1. In the UME (**`http(s)://<server>:<port>/useradmin`**), search for the role `idm.user`.
2. Assign the role to all users that you want to be able to access the Identity Management User Interface for HTML5.

Related Information

Administration of Users and Roles for SAP NetWeaver 7.3
Administration of Users and Roles for EHP1 for SAP NetWeaver 7.3
Administration of Users and Roles for SAP NetWeaver 7.4
Administration of Users and Roles for SAP NetWeaver 7.5

2.5.20.1.2 Enabling Single Sign-On with Logon Tickets

To improve performance, make sure that single sign-on with logon tickets is enabled for the REST service, as described in *SAP Identity Management REST Interface Version 2* (see topic *Configuring Single Sign-On With Logon Tickets in the REST Interface for AS Java 7.1 and higher*).

Related Information

SAP Identity Management REST Interface Version 2

2.5.20.2 Adding the Predefined Forms and Configuring the Solution

You can manage information displayed in the Identity Management User Interface for HTML5 and the access restrictions for this information through forms in the Identity Management Developer Studio. You need to import the predefined forms into the Identity Management Developer Studio. You should not change the Identity Management User Interface for HTML5, and therefore should not delete, replace, or modify the imported, predefined forms in any way.

Some configuration is required for the solution.

2.5.20.2.1 Importing the Forms

Context

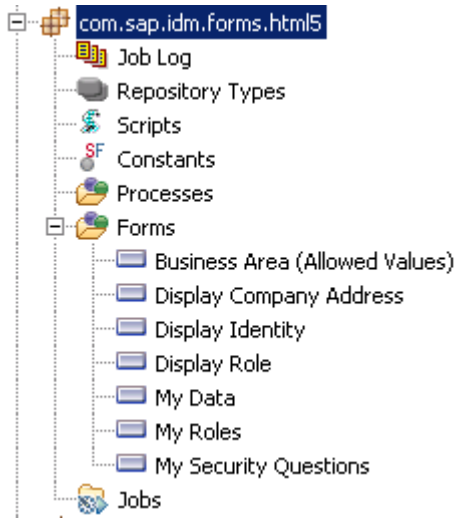
The package `com.sap.idm.forms.html5` contains a set of predefined forms for Identity Management User Interface for HTML5. To import the package into the Identity Management Developer Studio, proceed as follows:

Procedure

1. In the Identity Management Developer Studio, select the *Packages* node of your identity store in the tree view.
2. Choose *Import...* from the context menu.
3. Navigate to the package directory (by default `C:\usr\sap\idm\core\ConfigurationPackages\SAP Provisioning Framework`) and select the form package for Identity Management User Interface for HTML5.
4. Choose *Open* and a dialog box appears. Optionally, enter a reason for import and make sure that *Import* is selected.
5. Choose *OK* to close the dialog box and to import the package.

Results

The imported package with all the forms for Identity Management User Interface for HTML5 is added to the identity store:



The imported package contains the following forms:

Name of the Form	Description
Business Area (Allowed Values)	Retrieves the list of defined business areas, which can be used to search for roles that are relevant for a specific business area. Associated with the *My Requests* page in the Identity Management User Interface for HTML5.
Display Company Address	Displays detailed information for company address (information like company name, location, phone number, and so on). Associated with the *Workplace Data* section of the *My Data* page in the Identity Management User Interface for HTML5.
Display Identity	Displays the details of an identity entry. For future use.
Display Role	Displays detailed information of a role (for example, role description). Associated with the pages *My Requests* and *My Roles* in the Identity Management User Interface for HTML5.
My Data	Retrieves and updates the user data (for example, user picture, name (first, last and middle name(s)), title, language, and so on). Associated with the *My Data* page (overview data) and the *Change My Data* page (accessed from the *My Data* page by choosing the *Change My Data* button) in the Identity Management User Interface for HTML5.
My Roles	Retrieves and updates details about the assigned roles and requested new roles. Associated with the *My Roles* page and the *My Requests* page in the Identity Management User Interface for HTML5. Assignments in status Pending, Rejected and Assigned OK will be displayed.

Name of the Form	Description
My Security Questions	Retrieves the currently available security questions and updates the answers to these questions. Associated with the *My Security Questions* section of the *My Data* page and the *Change My Security Question* page (accessed from the *My Data* page, under the *My Security Questions* section) in the Identity Management User Interface for HTML5.

Do not delete, replace, or modify the imported, predefined forms in any way.

> **Note**
>
> The imported forms cannot be deleted or replaced by any similar forms in the configuration, because the `GUID`s are referred to directly in the code of the user interface.

> **Note**
>
> Do not modify the imported forms to include new attributes.

> **Note**
>
> Do not modify access control for the predefined forms.

2.5.20.2.2 Configuring the Solution

To use the predefined forms for Identity Management User Interface for HTML5, you need to configure or maintain the following:

- In the *List* column of the *Attributes* tab of the `MX_ROLE` entry type, select the `DESCRIPTION` attribute.
- Maintain the values of the attributes `MX_SALUTATION`, `MX_TITLE_SUPPLEMENT`, and `MXREF_MX_COMPANY_ADDRESS` for the *My Data* form.
- Maintain the values for the attribute `MX_BUSINESS_AREA` for the entry type `MX_ROLE`.
- View the access control defined for the forms.
- Activate HTTPS (the use of SSL) on your AS Java.

2.5.20.2.2.1 Defining the DESCRIPTION Attribute for the MX_ROLE Entry Type

Context

For the entry type `MX_ROLE`, you need to select the attribute `DESCRIPTION` in the *List* column of the entry type's *Attributes* tab. This is important for the description information displayed on the *My Requests* page in the Identity Management User Interface for HTML5.

Procedure

1. In the tree view of Identity Management Developer Studio, display the entry types in the identity store (double click the *Entry Types* node of your identity store schema).
2. View the properties of the *MX_ROLE* entry type and select the *Attributes* tab.
3. Find the `DESCRIPTION` attribute and select the *List* option.
4. Choose *File* > *Save* or press `Ctrl` + `S` to save the changes.

2.5.20.2.2.2 Maintaining the Attributes for the My Data Form

The *My Data* form is responsible for retrieving and updating the user data like user picture, name (first, last, and middle name(s)), title, or language. No actual configuration of the form is necessary, but you need to maintain some attribute values:

- `MX_SALUTATION`: Language-specific, ABAP mapping attribute displaying the title of the user (Mr, Mrs, and so on). Retrieve the input help for the attribute needs to be from the system (read customizing table (TSAD3, TSAD3T)) or maintain it manually. The value defined for this attribute for the given identity entry also needs to be retrieved from the system, and any changes in the value should be updated in the system.
- `MX_TITLE_SUPPLEMENT`: Language-specific, ABAP mapping attribute displaying a title supplement, such as a noble title. Retrieve the input help for the attribute from the system (read customizing table (TSAD5)) or maintain it manually. The value defined for this attribute for the given identity entry also needs to be retrieved from the system, and any changes in the value should be updated in the system.
- `MXREF_MX_COMPANY_ADDRESS`: This entry reference attribute should be retrieved from the system (or maintained manually). The workplace location data displayed in the user interface is derived from this value.

The allowed values for attributes `MX_SALUTATION` and `MX_TITLE_SUPPLEMENT`, and the valid entries for the entry reference `MXREF_MX_COMPANY_ADDRESS` can be obtained using the standard initial load job templates of the SAP Provisioning Framework. Check if the necessary data is already available in your identity store and that it is correct. If not, obtain the data using the initial load jobs. You can also use the SAP Provisioning Framework

to read the values/references defined for the identity entries into the identity store and to provision this data to target systems. For more details about the SAP Provisioning Framework and the initial load jobs, see

Related Information

SAP Identity Management Configuration Guide

2.5.20.2.2.2.1 Virus Scan Interface

The option to upload user pictures to the Identity Management User Interface for HTML5 could be abused, by utilizing it for virus distribution. Identity Management REST Interface 2.0 supports the virus scan interface of the AS Java for write access of the binary attributes in the identity store. For details about how to set up the virus scan interface and how to configure it for different services, such as the Identity Management REST Interface, see the documentation regarding the virus scan interface for your AS Java on SAP Help Portal.

To learn more about the details that are specific to using the virus scan interface together with the Identity Management REST Interface, see *SAP Identity Management REST Interface Version 2*.

Related Information

Virus Scan Interface for SAP NetWeaver 7.3
Virus Scan Interface for SAP NetWeaver 7.3 EHP1
Virus Scan Interface for SAP NetWeaver 7.4
Virus Scan Interface for SAP NetWeaver 7.5
SAP Identity Management REST Interface Version 2

2.5.20.2.2.3 Maintaining the Attribute MX_BUSINESS_AREA for Entry Type MX_ROLE

We recommend that you categorize the roles into business areas, which means maintaining the `MX_BUSINESS_AREA` attribute of the `MX_ROLE` entry type.

This information is used/displayed by the *My Roles* form, which retrieves and updates the details about the assigned roles and requested new roles for a user. The *My Requests* page of the Identity Management User Interface for HTML5 allows the filtering of roles by business area.

2.5.20.2.2.4 Access Control for the Forms

Do not modify access control for the predefined forms.

2.5.20.2.2.5 Configuring the AS Java for SSL Use

Context

To be able to update the answers of the security questions on the *Change My Security Questions* page in the Identity Management User Interface for HTML5, HTTPS must be activated for your AS Java where the Identity Management User Interface for HTML5 is installed. There are two ways you can configure the use of SSL - either manually by configuring the ICM and the AS Java keystore separately, or by using the SSL configuration tool in SAP NetWeaver Administrator.

Proceed as follows:

Procedure

1. Follow the steps described in *Configuring Transport Layer Security on SAP NetWeaver AS for Java*.
2. Your AS Java is ready to use SSL. You may want to test the SSL connection to the AS Java after performing the configuration.

Related Information

SAP NetWeaver 7.3
Configuring Transport Layer Security on SAP NetWeaver AS for Java
SAP NetWeaver 7.3 EHP1
Configuring Transport Layer Security on SAP NetWeaver AS for Java
SAP NetWeaver 7.4
Configuring Transport Layer Security on SAP NetWeaver AS for Java
SAP NetWeaver 7.5
Configuring Transport Layer Security on SAP NetWeaver AS for Java

2.5.20.3 Accessing the Identity Management User Interface for HTML5

Context

To access the Identity Management User Interface for HTML5, proceed as follows:

Procedure

1. Enter **`http(s)://<host>:<port>/idmui5`** in your browser.
2. Provide the credentials in the logon window and choose *Log On*.
3. You are now logged on to the Identity Management User Interface for HTML5. The *My Data* page appears.

2.5.20.4 Restrictions and Considerations

Modifications of the Identity Management User Interface for HTML5

Any modifications of the Identity Management User Interface for HTML5 are not supported.

- The imported forms should not be deleted or replaced by any similar forms in the configuration, because the `GUID`s are referred directly in the code of the user interface.
- The imported, predefined forms should not be modified in any way (including attributes and the access control defined on the forms).
- JavaScript files in the deployment package should not be replaced, removed or modified in any way.

Language Settings

You change the language for the Identity Management User Interface for HTML5 by modifying the language setting for the respective browser. For more information on how to update the browser language, see the browser documentation. For more language information for the SAPUI5 applications, see *Identifying the Language Code / Locale* for your AS Java version.

> **Note**
>
> A limitation of the Microsoft Internet Explorer 9 is that it takes the language configured for the operating system. In such a case, it is recommended that you update to Microsoft Internet Explorer 10, which browser does not have such a limitation.

Pictures Uploads

The upload of pictures in any format is not supported by the Microsoft Internet Explorer 9. In such a case, you will receive the following error message: `Browser does not support getting the file for uploading`. Then, you need to upgrade to Microsoft Internet Explorer 10.

Related Information

Identifying the Language Code / Locale
Identifying the Language Code / Locale for SAP NetWeaver 7.4

2.5.21 Starting the Virtual Directory Server

On Microsoft Windows

Prerequisites

Set the JAVA_HOME environment variable for the `<sapsid>adm` user to point to `<drive>:\usr\sap\<SAPSID>\IDM<No>\exe\sapjvm_<No>`. Use the `<sapsid>adm` user to run the `Virtual Directory Server.bat` file.

Context

To start the Virtual Directory Server on Microsoft Windows, proceed as follows:

Procedure

1. Navigate to the installation directory of the Virtual Directory Server. By default: `<drive>:\usr\sap\<SAPSID>\VDS<Instance_Number>\VDS`.
2. Execute `Virtual Directory Server.bat`.

2.5.22 Initial Configuration of Identity Management Virtual Directory Server

After the Virtual Directory Server is installed, some initial configuration is necessary.

Depending on how you plan to use the Virtual Directory Server, you may also need to add some external components.

Related Information

Configuring the Virtual Directory Server Environment [page 186]
Access to Keys.ini File by Virtual Directory Server Components [page 192]

2.5.22.1 Configuring the Virtual Directory Server Environment

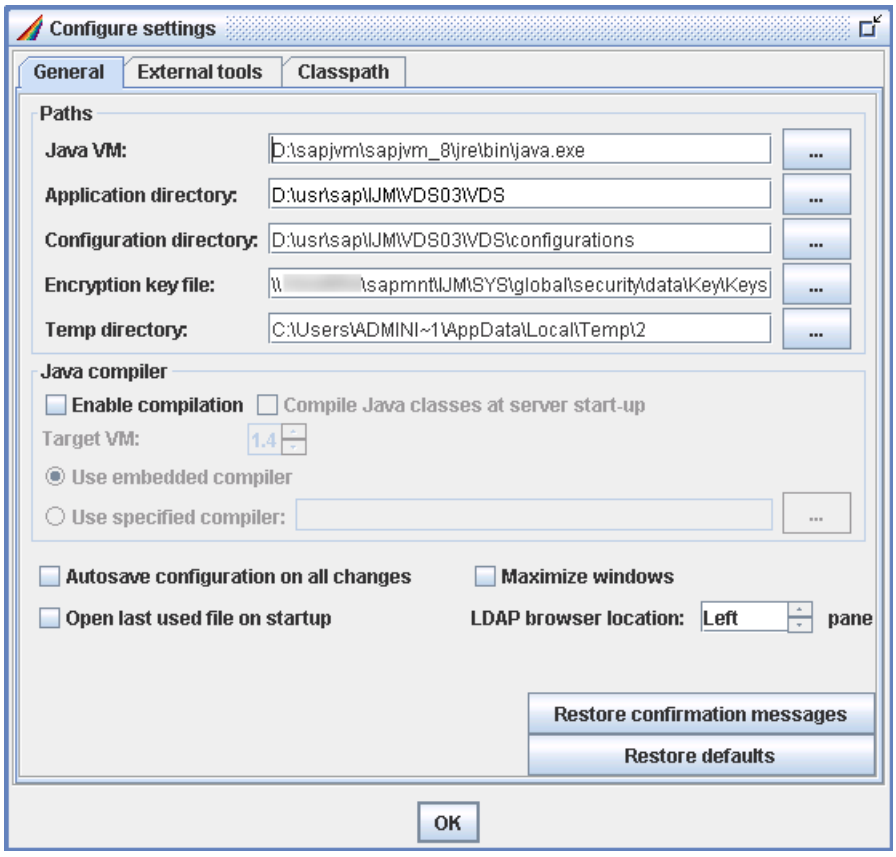
The Virtual Directory Server needs some initial information in order to operate properly.

Context

To configure the Virtual Directory Server environment, proceed as follows:

Procedure

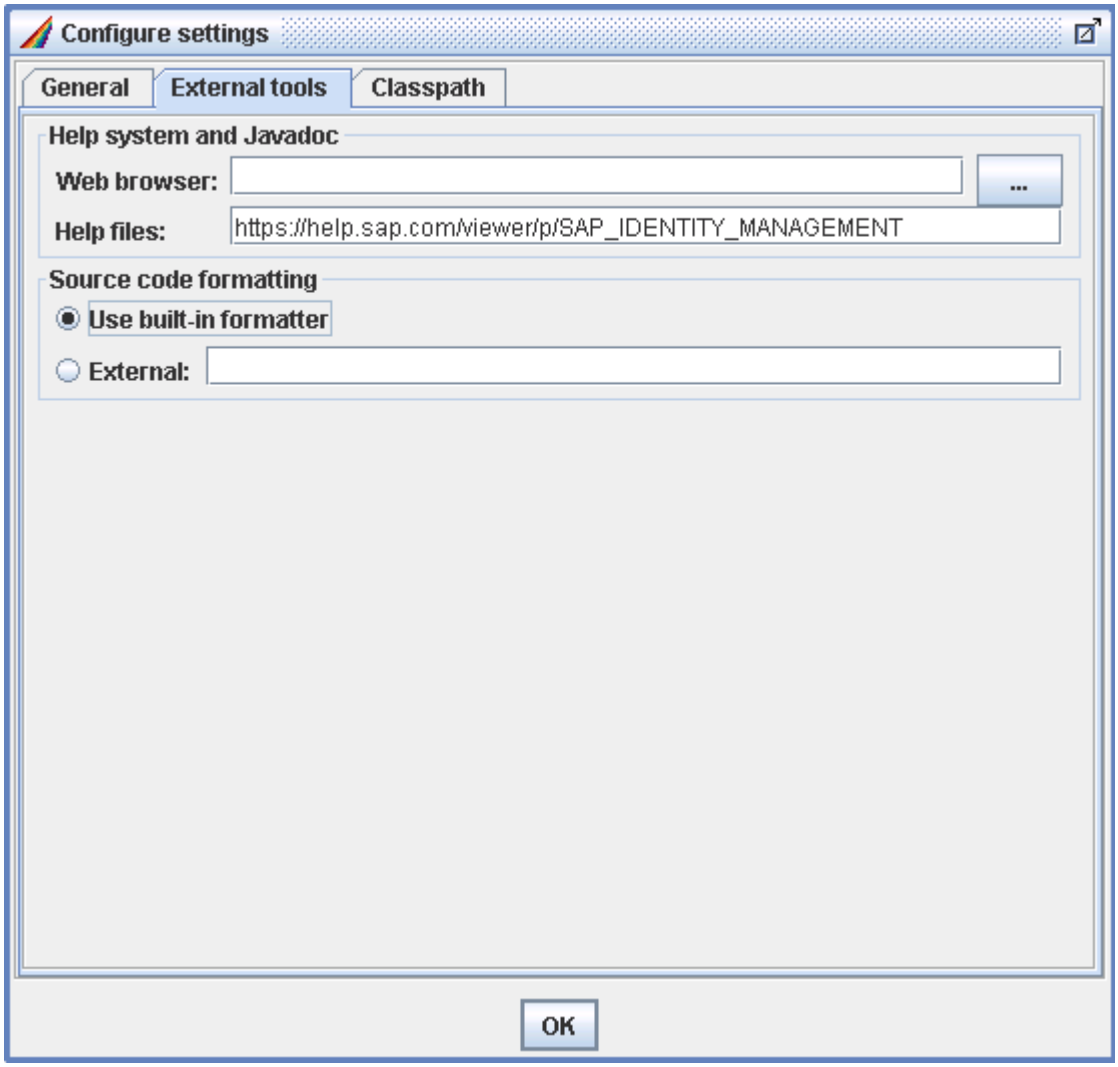
1. In the *Configure settings* dialog box, select the *General* tab.



2. Configure the following properties:

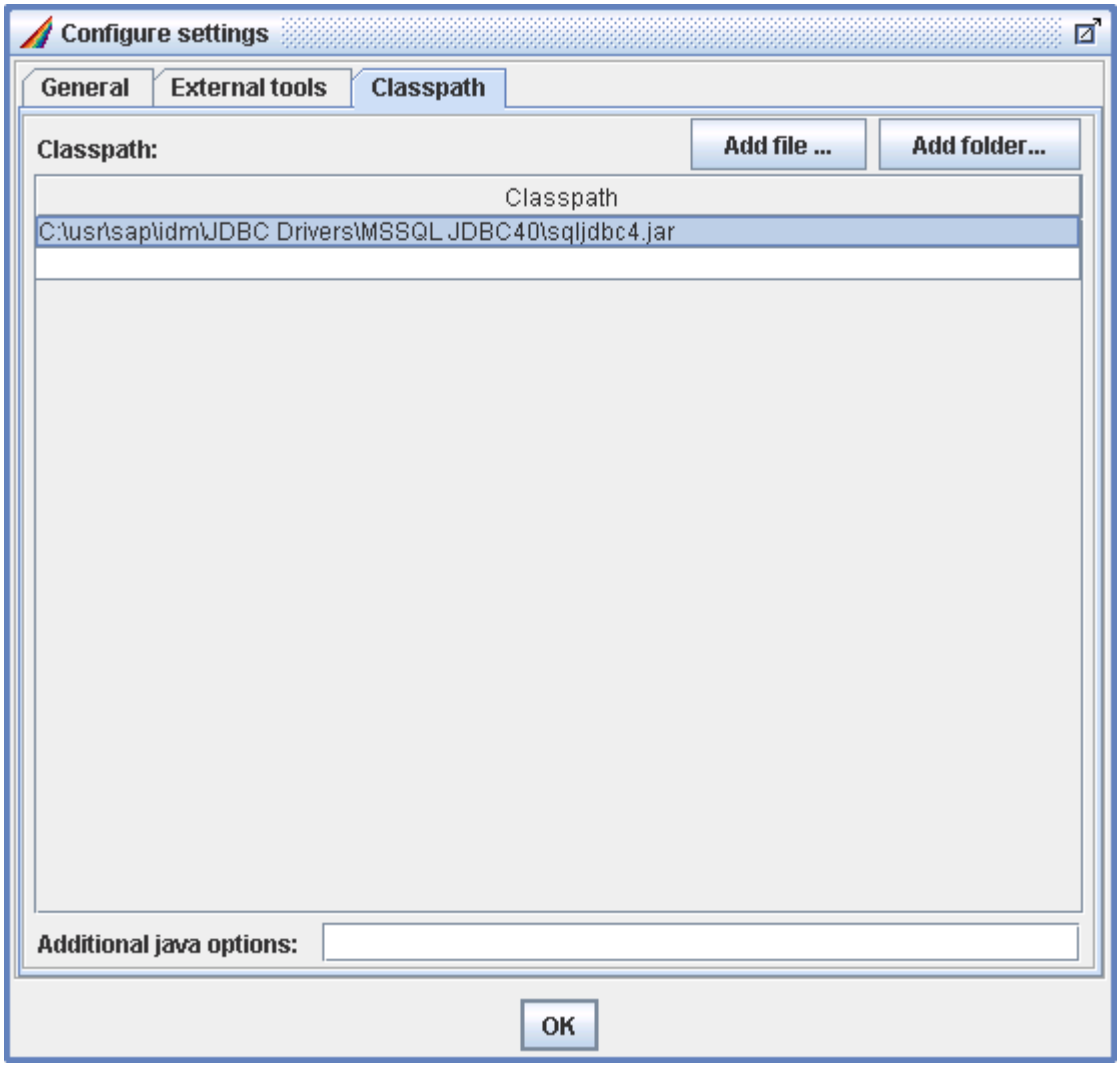
Property	Description
Paths	Verify that the paths for to the different directories are correct.
Encryption key file	Provide the path to the `Keys.ini` file. For example: `\\<host>\sapmnt\<SAPSID>\SYS\global\security\data\Key\Keys.ini`. For more information about the `Keys.ini` file, see SAP Identity Management Security Guide
Java compiler	Configure the parameters for the Java compiler if you want to compile Java classes. Select *Use embedded compiler* if you run JRE and have downloaded `tools.jar` as described in *Installing a Java compiler*. If you have installed JDK, select *Use specified compiler* and select `javac.exe` from your JDK installation. *Autosave configuration on all changes* should normally be selected.

3. Select the *External tools* tab.



- Select the browser you want to use for viewing the help file and Javadoc. The *Help files* field contains the default start page for the help file.
- Select which tool you want to use for the formatting of the Java source code. You can either use the built-in formatter or an external formatter (for instance Jalopy).

4. Select the *Classpath* tab.



If necessary, add any files or folders to the classpath that are specific to the Virtual Directory Server, for instance if they are needed by the specified JDBC drivers.

5. Choose *OK*.

Related Information

Installing a Java Compiler [page 189]

2.5.22.1.1 Installing a Java Compiler

A Java compiler is required to develop and compile Java classes.

You can choose between the following options:

- Download and install the JDK (version 1.4, 1.5, 1.6 or 1.8). Select *Use specified compiler* and then select the `javac.exe` of the JDK installation in the *Options* dialog box.
- If you have installed JRE and do not want to install the complete JDK, you can download `tools.jar` corresponding to your version of JRE. Place it in the `<inst dir>\lib\jdk1.x` directory and select *Use embedded compiler* in the *Options* dialog box.

2.5.22.2 Paging Mechanism

You can use the paging mechanism when accessing an LDAP directory.

Context

To use the paging mechanism when accessing an LDAP directory, do the following:

Procedure

1. Download and install the LDAP Booster Pack that is part of the Java Naming and Directory Interface (JNDI).
2. Locate the file `ldapbp.jar` in the download.
3. Add the file to classpath, as described in *Configuring the Virtual Directory Server environment*.

Related Information

Configuring the Virtual Directory Server Environment [page 186]

2.5.22.3 Alternative LDAP connector

You can use the alternative (low-memory-consumption) LDAP connector.

Context

To use the alternative LDAP connector, do the following:

Procedure

1. Download the file `ldapjdk.jar` from Netscape Directory SDK for Java.
2. Follow the instructions and copy the file to `<inst dir>\lib`.

Related Information

Netscape Directory SDK for Java

2.5.22.4 SAML Outbound Connector

You can use the SAML outbound connector.

Context

To use the SAML outbound connector, do the following:

Procedure

1. Download the file `opensaml.jar`.
2. Copy the file to `<inst dir>\lib`.

Related Information

OpenSAML

2.5.22.5 Event Triggers and SendMail Event

You can use event triggers and SendMail event actions.

Context

To use event triggers and SendMail event actions, do the following:

Procedure

1. Download the `mail.jar` from the JavaMail API.
2. Copy the file to `<inst dir>\lib`.

2.5.22.6 External LDAP Client

Context

The Virtual Directory Server contains an internal LDAP client, but you may need an external LDAP client for viewing the contents of the Virtual Directory Server.

2.5.22.7 Access to Keys.ini File by Virtual Directory Server Components

This section describes how the various Virtual Directory Server components handle the `Keys.ini` file.

For more information about managing `Keys.ini` file, see *SAP Identity Management Security Guide*.

Virtual Directory Management Console

The Virtual Directory Management Console (configuration user interface) checks for `Keys.ini` in the following locations:

- The folder specified with the parameter KEYS_INI_FILE in the file `.vdssettings`
  The `.vdssettings` file is created in the `<drive>:\usr\sap\<SAPSID>\VDS<Instance_Number>\VDS` folder after you have configured the Virtual Directory Server environment. See Configuring the Virtual Directory Server Environment [page 186]
- The folder specified with the environment variable VDS_HOME

If no `Keys.ini` file is found, the Virtual Directory Management Console will give a warning when it is started (even if encryption is not or will not be used). All encryption will be done using the built-in scrambling and all hashing will be done with MD5.

Decryption will fail, except for scrambled values.

Deployed Mode

In a deployed mode, the Virtual Directory Server configuration is exported as a deployable archive (EAR file). This archive is deployed on SAP NetWeaver AS Java. It runs on SAP NetWeaver AS Java as an application. For more information, see SAP NetWeaver Identity Management Identity Services Configuration Guide *Deploying the configuration on SAP NetWeaver* > *Deploying the configuration* > *Other SAP NetWeaver versions*.

A configuration that is deployed on SAP NetWeaver AS for Java retrieves the location of `Keys.ini` from the configuration in SAP NetWeaver AS for Java. Every deployed configuration has a corresponding sap.application.global.properties associated with it. Use SAP NetWeaver Administrator and locate the property com.sap.idm.vds.keyfile and enter the path to the Keys.ini file.

If no `Keys.ini` file is found, encryption will be done with scrambling and hashing with MD5. Decryption will fail, except for scrambled values.

Standalone Mode

In a standalone mode, the Virtual Directory Server is run as a standalone server directly on the host where it is installed.

A configuration that is run in standalone mode retrieves the location of Keys.ini file in the following locations:

- A file specified with the command line parameter KEYS_INI_FILE (Java option)
- The folder specified with the environment variable DSE_HOME
- The folder specified with the environment variable VDS_HOME

If no `Keys.ini` is found, encryption will be done with scrambling and hashing with MD5. Decryption will fail, except for scrambled values.

Related Information

SAP Identity Management Security Guide

2.6 Starting and Stopping SAP Identity Management

Starting and Stopping the SAP Identity Management User Interface

The Identity Management User Interface is deployed on SAP NetWeaver AS for Java, and the service is controlled from there (using the SAP NetWeaver Administrator).

Starting and Stopping the Processing in the SAP Identity Management Developer Studio

The processing of jobs, tasks and processes in the Identity Management Developer Studio is controlled by the dispatchers. You can start and stop any or all of these dispatcher services by using the Identity Management Dispatcher Utility. In addition, the dispatcher services can be suspended (set to sleep-mode), and resumed when needed. For details see *Creating and Managing the Dispatcher(s)*.

From the Identity Management Developer Studio, you are only able to suspend, resume and stop the dispatcher services. See *Suspending and Resuming a Dispatcher* and *Stopping a Dispatcher* for details.

Starting and Stopping the SAP Identity Management Virtual Directory Server

An Identity Management Virtual Directory Server configuration can either be deployed as a web service on SAP NetWeaver AS for Java or be run locally as an LDAP server. When deployed locally, the server is started and stopped from the Virtual Directory Server user interface.

When deployed on SAP NetWeaver AS for Java the service is controlled by SAP NetWeaver AS for Java (using the SAP NetWeaver Administrator).

Related Information

Creating and Managing the Dispatcher(s) on Windows

Creating and Managing the Dispatcher(s) on UNIX
Suspending and Resuming a Dispatcher
Stopping a Dispatcher

3 Updating SAP Identity Management

This section describes how to update SAP Identity Management 8.0 to implement support packages or patches.

If your SAP Identity Management system is installed with the Software Provisioning Manager 1.0 tool, use this installation tool to implement patches or update your system to a higher SP level.

For manual SAP Identity Management installations, the update procedure is performed by manually updating all the necessary components to a higher SP level.

The following sections describe how to update SAP Identity Management:

- By using Software Provisioning Manager 1.0 [page 196]
- By manually updating SAP Identity Management components to a higher SP level [page 199]

3.1 Updating SAP Identity Management with Software Provisioning Manager 1.0

This section describes how to patch and update SAP Identity Management 8.0 with Software Provisioning Manager 1.0.

Prerequisites

- You have installed SAP Identity Management using Software Provisioning Manager 1.0
- You have downloaded the dedicated installation archives (SAR files) containing the software to be installed. See Preparing the Installation Media [page 51]

  > → Recommendation
  >
  > We recommend that you always download the latest patch level of SAP Identity Management components from the SAP Software Download Center.

- You are logged on to the installation host as a user that is a member of the local administrators group.
- > ⚠ Caution
  >
  > Before updating runtime instances, make sure all dispatchers, that you created manually, are stopped and no jobs are running.

- You have stopped the Virtual Directory Server. See Starting and Stopping SAP Identity Management Virtual Directory Server [page 194]

Procedure

1. Start the Software Provisioning Manager on the host where you installed SAP Identity Management components.
2. On the *Welcome* screen, choose the required option.

   To update an SAP Identity Management system, choose *SAP Identity Management 8.0* > *Update* option.
3. You can update the following system variants and additional components:
   - **Standard System**
     This option updates all must-have components of an system on one host.

Update	Description

SAP Identity Management Standard System	Updates all components of an SAP Identity Management 8.0 system on one host:
	• Updates SAP Identity Management 8.0 Core
	• Updates SAP Identity Management 8.0 Dispatcher Instance with Runtime Components
	• Updates the following required SAP Identity Management components:
	  • SAP Identity Management 8.0 Developer Studio Service
	  • SAP Identity Management 8.0 User Interface
	In addition, this option enables you to update the following optional components:
	• SAP Identity Management 8.0 REST Interface Version 2
	• SAP Identity Management 8.0 User Interface for HTML5
	• SAP Identity Management 8.0 Portal Content
	• Identity Federation
	• Update of a Virtual Directory Server instance

   - **Distributed System**
     Options to update SAP Identity Management 8.0 instances distributed over several hosts

Update	Description
SAP Identity Management Core ComponentsSAP Identity Management	Updates the SAP Identity Management 8.0 Core on one host.
SAP Identity Management Dispatcher Instance	Updates SAP Identity Management 8.0 Dispatcher Instance with Runtime Components on this host.

Update	Description
SAP Identity Management Components on SAP NetWeaver AS Java	Run this option on a host where SAP NetWeaver AS Java is installed and where is at least one AS Java instance running. This option updates the following required SAP Identity Management components on this host: • SAP Identity Management 8.0 Developer Studio Service • SAP Identity Management 8.0 User Interface In addition, this option enables you to update the following optional components: • SAP Identity Management 8.0 REST Interface Version 2 • SAP Identity ManagementSAP 8.0 User Interface for HTML5 • SAP Identity Management 8.0 Portal Content • Identity Federation

- **Additional Components**
  Options to update additional SAP Identity Management 8.0 components.

Update	Description
SAP Identity Management Virtual Directory Server (VDS)	Updates a Virtual Directory Server instance of SAP Identity Management on this host.
SAP Identity Management Components on SAP NetWeaver AS Java	Updates the following SAP Identity Management components on this host: • SAP Identity Management 8.0 REST Interface Version 2 • SAP Identity Management 8.0 User Interface for HTML • SAP Identity Management 8.0 Portal Content • Identity Federation

4. Follow the instructions in the Software Provisioning Manager input dialogs.

> ⓘ Note
>
> When updating the database, the identity store schema is also updated. By default, the update of the identity store schema does not override the existing schema. That is, only new attributes and entry types are added to the database and the existing ones are preserved.

Results

SAP Identity Management 8.0 system is updated.

Next Steps

You can proceed with the following steps:

1. Unpack the Core Component [page 73] that contains the configuration packages, database scripts and some additional components.
   1. Reimport the configuration packages. See Updating the Provisioning Framework
   2. (Optional) To update Password Hook, see Upgrading Password Hook.
2. Update the SAP Identity Management Developer Studio [page 230]

3.2 Updating SAP Identity Management Components

This section describes how to update SAP Identity Management components. The update procedure is relevant only for manual SAP Identity Management installations.

Make sure that all installed components of SAP Identity Management are updated to the latest patch levels (PLs) of the corresponding SP level. This is recommended because of probable future releases of dependent component versions. The omission of update to the latest patch version of a component may result in errors and unexpected behavior.

Prerequisites

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.

Next Steps

If you are updating SAP Identity Management to version 8.0 SP05 or higher, you must use SAP JVM version 8.1 (Java 1.8). After the update, you need to regenerate the dispatcher scripts. For more information, see Managing the Dispatcher(s) [page 216].

3.2.1 Updating SAP Identity Management Core

This section describes how to update an Identity Management database on the supported database systems.

SAP Identity Management supports the following database systems:

- Microsoft SQL Server
- Oracle
- IBM DB2
- SAP Adaptive Server Enterprise (SAP ASE)

Choose the update description that corresponds to your database system.

> ⓘ Note
>
> Before you install a new version, it is important that any services (dispatchers) are stopped and that no jobs are running.

When updating the database, the identity store schema is also updated. This requires a Java environment on the server where the command file is run. The server does not need to be the same as the database server.

By default, the update of the identity store schema does not override the existing schema. That is, only new attributes and entry types are added to the database and the existing ones are preserved.

Related Information

Installing the Java Runtime Environment [page 211]
Installing the JDBC Drivers [page 22]

3.2.1.1 Updating Identity Management Database on Microsoft SQL Server

You want to know how to update the Identity Management database on Microsoft SQL Server.

Prerequisites

- The database must be updated to 7.2 pure mode before upgrading to SAP Identity Management 8.0. The update script will not run if this condition is not met.
- The update scripts require a Java Rruntime Engine and a JDBC driver to update the database schema.
- You require the SAPCAR archiving tool to be able to unpack software component archives (`*.SAR` files).

Context

> **Note**
>
> Before updating the Identity Management database, make sure that a backup has been made of the database.

To update an Identity Management database, 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 kit for the `Core` component.
2. Unpack the installation kit using the following command:

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

3. Open a command prompt and navigate to the directory where the database installation scripts are located.

   The script files are located in the `/DatabaseSchema/SQL-Server` folder.

   > **Note**
   >
   > The script files need write access to the folder from where they are run, so if the installation kit is located on a CD or another read-only location, copy the folder with the database scripts to a location with write access before you run them.

   > **Note**
   >
   > Do not run the scripts directly from Microsoft Windows Explorer. Open the command prompt and navigate to the installation folder of the database, and run the scripts from here.

   > **Note**
   >
   > Check whether the prefix of the Identity Management database is case sensitive. Make sure that you use the right case when running the `mxmc-update.cmd` command file.

4. Run the `mxmc-update.cmd` command file. You are prompted for the following information:
   - The JDBC URL to the Identity Management database. The syntax is `jdbc:sqlserver://<host>:<port>;databasename=<prefix>_db;user=<prefix>_oper;password=<password>`
   - The path to the JDBC driver used when connecting to the database (in double quotes), for instance `C:\usr\sap\IdM\Identity Center\jdbc\sqljdbc4.jar`.
   - The password for `mxmc_oper`.

   If you are upgrading to SAP Identity Management 8.0, you are prompted for the following information:

   - The name of the *Developer Administrator* for this database.

> **Note**
>
> This user must either exist in the UME or be added to the UME before you can log on to the Identity Management Developer Studio.

- The base qualified name to be used for all packages in this database.

If the file completes without error messages, the database is updated correctly. You can also check the `<prefix>_update.log` log file.

5. Close the command prompt window.

Related Information

Creating the Developer Administrator User in UME

3.2.1.2 Updating Identity Management Database with a Given Prefix on Microsoft SQL Server

You want to know how to update the Identity Management database with a given prefix on Microsoft SQL Server.

Prerequisites

The database must be updated to 7.2 pure mode before upgrading to SAP Identity Management 8.0. The update script will not run if this condition is not met.

The update scripts require a Java Rruntime Engine and a JDBC driver to update the database schema.

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

Context

> **Note**
>
> Before updating the Identity Management database, make sure that a backup has been made of the database.

To update an Identity Management database with a given prefix, 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 kit for the `Core` component.
2. Unpack the installation kit using the following command:

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

3. Open a command prompt and navigate to the directory where the database installation scripts are located.

   The script files are located in the `/DatabaseSchema/SQL-Server` folder.

   > ### Note
   >
   > The script files need write access to the folder from where they are run, so if the installation kit is located on a CD or another read-only location, copy the folder with the database scripts to a location with write access before you run them.

   > ### Note
   >
   > Do not run the scripts directly from Microsoft Windows Explorer. Open the command prompt and navigate to the installation folder of the database, and run the scripts from here.

   > ### Note
   >
   > Check whether the prefix of the Identity Management database is case sensitive. Make sure that you use the right case when running the `mxmc-update.cmd` command file.

4. Run the `mxmc-xupdate.cmd` command file. The parameters to the command file are:
   - Host name of the server running the Microsoft SQL Server
   - Prefix of the Identity Management database
   - Path to the JDBC driver used when connecting to the database (in double quotes). For instance `C:\usr\sap\IdM\Identity Center\jdbc\sqljdbc4.jar`.
   - JDBC URL to the Identity Management database (in double quotes). The syntax is `jdbc:sqlserver://<host>:<port>;databasename=<prefix>_db;user=<prefix>_oper;password=<password>`
   - Optional: Password for `<prefix>_oper`

   If you upgrade to SAP Identity Management 8.0, you are prompted for:

   - The name of the *Developer Administrator* for this database.

     > ### Note
     >
     > This user must either exist in the UME or be added to the UME before you can log on to the Identity Management Developer Studio.

   - The base qualified name to be used for all packages in this database.

When the file completes without error messages, the database is updated correctly. You can also check the log file `<prefix>_update.log`.

5. Close the command prompt window.

Related Information

Creating the Developer Administrator User in UME

3.2.1.3 Updating Identity Management Database on Oracle

You want to know how to update the Identity Management database on Oracle.

Prerequisites

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

Context

> **Note**
>
> Before updating the Identity Management database, make sure that a backup has been made of the database.

To update an Identity Management database, 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 kit for the `Core` component.
2. Unpack the installation kit using the following command:

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

3. Open a command prompt and navigate to the directory containing the Identity Management database script files.

   The script files are located in the /DatabaseSchema/Oracle folder.

> **Note**
>
> All the scripts in that folder should have execute permission. In addition, the script files need write access to the folder where they are run from, so if the installation kit is located on a CD or another read-only location, copy the folder with the database scripts to a location with write access before running them.

> **Note**
>
> Check whether the prefix of the Identity Management database is case sensitive. Make sure that you use the right case when running the `mxmc-update.cmd` command file.

Make sure that you have the same `include.sql` file as you used during installation.

4. Run the command file `mxmc-update.cmd`. You are prompted for the following:
   - JDBC URL to the Identity Management database (in double quotes). The syntax is `jdbc:oracle:thin:PREFIX_oper/PWDOPER@<host>:<port>:<SID>`
   - The path to the JDBC driver used when connecting to the database (in double quotes). For example, `C:\usr\sap\IdM\Identity Center\jdbc\ojdbc6.jar`.
   - The password for mxmc_oper

     > **Note**
     >
     > It can contain the following characters: `_, #, $, a-z, A-Z, 0-9`. It must not begin with a digit nor an underscore.

   If you are upgrading to SAP Identity Management 8.0, you are prompted for the following information:
   - The name of the *Developer Administrator* for this database.

     > **Note**
     >
     > This user must either exist in the UME or be added to the UME before you can log on to the Identity Management Developer Studio.

   - The base qualified name to be used for all packages in this database.

   You can check the `mxmc-update.log` log file for warnings or errors.
5. Close the command prompt window.

Related Information

Creating the Developer Administrator User in UME

3.2.1.4 Updating Identity Management Database on IBM DB2

You want to know how to update the Identity Management database on IBM DB2.

Prerequisites

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

Context

> **Note**
>
> Before updating the Identity Management database, make sure that a backup has been made of the database.

> **Note**
>
> Make sure that you use the same values in the `include.sql` file as you used during installation. The following parameters are required in the `include.sql` file: `PREFIX`, `DB2PORT`, `PWDOPER`, `ADMINUSER`, `BASENAME`, `JDBCURL`, `JDBCDRIVER`.

Procedure

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

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

3. Proceed as follows:
   - **For Microsoft Windows:** Open the IBM DB2 command window. From the *Start* menu, choose *IBM DB2/<Database>/Command window - Administrator* .
4. Navigate to the directory containing the Identity Management script files.

   The script files are located in the /DatabaseSchema/DB2 folder.

   > **Note**
   >
   > All the scripts in that folder should have execute permission. In addition, the script files need write access to the folder from where they are run. If the installation kit is located on a CD or another

read-only location, you therefore have to copy the folder with the database scripts to a location with write access before running them.

> **Note**
>
> Take care when editing shell scripts (.sh files) in Windows format. Make sure the shell scripts are saved in Unix format.

> **Note**
>
> Check whether the prefix of the Identity Management database is case sensitive. Make sure that you use the right case when running the `mxmc-update.cmd` command file.

5. Run command file `mxmc-update.cmd` (Microsoft Windows). You are prompted for the following:
   - JDBC URL to the Identity Management database
   - The path to the JDBC driver used when connecting to the database
   - Password for <prefix>_oper

     > **Note**
     >
     > It can contain the following characters: `_, #, $, a-z, A-Z, 0-9`. It must not begin with a digit nor an underscore.

   If you are upgrading to SAP Identity Management 8.0, you are prompted for the following information:
   - The name of the *Developer Administrator* for this database.

     > **Note**
     >
     > This user must either exist in the UME or be added to the UME before you can log on to the Identity Management Developer Studio.

   - The base qualified name to be used for all packages in this database.

   You can check the `mxmc-update.log` log file for warnings or errors.
6. Close the command prompt window.

Related Information

Creating the Developer Administrator User in UME

3.2.1.5 Updating Identity Management Database on SAP ASE

You want to know how to update the Identity Management database on SAP ASE.

Prerequisites

The update scripts require a Java Rruntime Engine and a JDBC driver to update the database schema.

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

Context

> **Note**
>
> Before updating the Identity Management database, make sure that a backup has been made of the database.

To update an Identity Management database, 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 kit for the `Core` component.
2. Unpack the installation kit using the following command:

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

3. Open a command prompt and navigate to the directory where the database installation scripts are located.

   The script files are located in the /DatabaseSchema/ASE folder.

   > **Note**
   >
   > All the scripts in that folder should have execute permission. In addition, the script files need write access to the folder from where they are run, so if the installation kit is located on a CD or another read-only location, copy the folder with the database scripts to a location with write access before you run them.

   > **Note**
   >
   > Do not run the scripts directly from Microsoft Windows Explorer. Open the command prompt and navigate to the installation folder of the database, and run the scripts from here.

> ### Note
>
> Check whether the prefix of the Identity Management database is case sensitive. Make sure that you use the right case when running the `mxmc-update.cmd` command file.

> ### Note
>
> The isql command line tool must be installed on the machine where the scripts are executed. This is required for the SAP Identity Management scripts to function properly. The isql command line tool is provided either with the ASE server installation or with the ASE OpenServer client which is a part of the ASE SDK Suite.

4. Run the command file `mxmc-update.cmd`. You are prompted for the following information:
   - The path and name of the JDBC driver used when connecting to the database (in double quotes). For example, For example: `<ASE_install_directory>\jConnect-16_0\classes\jconn4.jar`.
   - The password for `mxmc_oper`.

   If the file completes without error messages, the database is updated correctly. You can also check the `<prefix>_update.log` log file.
5. Close the command prompt window.

3.2.1.6 Updating Identity Management Database with a Given Prefix on SAP ASE

You want to know how to update the Identity Management database with a given prefix on SAP ASE.

Prerequisites

The update scripts require a Java Rruntime Engine and a JDBC driver to update the database schema.

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

Context

> ### Note
>
> Before updating the Identity Management database, make sure that a backup has been made of the database.

To update an Identity Management database with a given prefix, 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 kit for the `Core` component.
2. Unpack the installation kit using the following command:

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

3. Open a command prompt and navigate to the directory where the database installation scripts are located.

   The script files are located in the /DatabaseSchema/ASE folder.

   > ### Note
   >
   > All the scripts in that folder should have execute permission. In addition, the script files need write access to the folder from where they are run, so if the installation kit is located on a CD or another read-only location, copy the folder with the database scripts to a location with write access before you run them.

   > ### Note
   >
   > Do not run the scripts directly from Microsoft Windows Explorer. Open the command prompt and navigate to the installation folder of the database, and run the scripts from here.

   > ### Note
   >
   > Check whether the prefix of the Identity Management database is case sensitive. Make sure that you use the right case when running the `mxmc-update.cmd` command file.

   > ### Note
   >
   > The isql command line tool must be installed on the machine where the scripts are executed. This is required for the SAP Identity Management scripts to function properly. The isql command line tool is provided either with the ASE server installation or with the ASE OpenServer client which is a part of the ASE SDK Suite.

4. Run the `mxmc-xupdate.cmd` command file. The parameters to the command file are:
   - Host name of the server running the SAP ASE
   - Port of the server running the SAP ASE
   - Prefix of the Identity Management database
   - Path to the JDBC driver used when connecting to the database (in double quotes). For example, `C:\SAP\jConnect-16_0\classes\jconn4.jar`.
   - JDBC URL to the Identity Management database (in double quotes). The syntax is `jdbc:sybase:Tds:<host>:<port>/<prefix>_db?user=<oper_user>&password=<oper_password>`
   - Optional: Password for `<prefix>_oper`

When the file completes without error messages, the database is updated correctly. You can also check the log file `<prefix>_update.log`.

5. Close the command prompt window.

3.2.2 Updating Runtime Components

> **Note**
>
> Before you install a new version, it is important that any services (dispatchers) are stopped and that no jobs are running.

An update is performed by running the installation job as described in *Installing the Runtime Components on Microsoft Windows*.

Next Steps

1. After the update, you may be prompted to restart the server. This will be the case if any services were running while you updated.
2. You need to regenerate the dispatcher scripts and then start the dispatchers. See *Managing the Dispatcher(s)*.

Related Information

Installing the Runtime Components on Microsoft Windows [page 215]
Managing the Dispatcher(s) [page 216]

3.2.2.1 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. Make sure you install the specified Microsoft libraries.

> **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.

3.2.2.2 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

Microsoft SQL Server JDBC Driver [page 23]
Oracle JDBC Driver [page 23]
IBM DB2 JDBC Driver [page 24]
SAP ASE JDBC Driver [page 24]
JDBC Drivers for External Systems [page 25]

3.2.2.2.1 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

3.2.2.2.2 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

3.2.2.2.3 IBM DB2 JDBC Driver

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

By default it is installed in this folder:

- Microsoft Windows: `C:\Program Files\IBM\SQLLIB\java\`

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.

3.2.2.2.4 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 `<ASE_install_directory>\jConnect-16_0\classes\`.
  The name of the JDBC driver is: *com.sybase.jdbc4.jdbc.SybDriver*
  Make sure that the CLASSPATH is set to the correct file:
  `<ASE_install_directory>\jConnect-16_0\classes\jconn4.jar`.
- **SAP ASE version 16.0 SP04**
  The `jconn42.jar` file is located in `<ASE_install_directory>\jConnect-16_0\classes\`
  The name of the JDBC driver is: *com.sybase.jdbc42.jdbc.SybDriver*
  Make sure that the CLASSPATH is set to the correct file:
  `<ASE_install_directory>\jConnect-16_0\classes\jconn42.jar`.

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

3.2.2.2.5 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.

3.2.2.3 Installing the Runtime Components on Microsoft Windows

Context

To install Identity Management Runtime Components on Microsoft Windows, proceed as follows:

Procedure

1. Navigate to the download area of SAP Identity Management 8.0 on the SAP Software Download Center and download the installation kit for Identity Management Runtime Components.
2. Unpack the installation kit using the following command:

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

3. Run the file `install.exe` located in the `\RuntimeComponents\Setup\CDROM_Installers\Windows\Disk1\InstData\VM` folder.
4. The wizard leads you through the installation. Keep the default values or enter values specific for your installation.

   > **Note**
   >
   > If your operating system is Windows 8, Windows Server 2012 or Windows Server 2012 R2, the **.exe** installation file should run in *Compatibility* mode for Windows 7. For more information, see 2237907.

Next Steps

When the installation is completed, you may need to restart your computer.

In case the wizard stops prematurely, you can try specifying which Java version to start when you run the `install.exe` file, for instance: `install.exe LAX_VM c:\usr\sap\sapjvm_8\bin\java.exe`

Related Information

SAP Software Download Center on SAP Support Portal

3.2.2.4 Managing the Dispatcher(s)

To manage the dispatcher(s), you use SAP Identity Management Dispatcher Utility. The utility offers a graphical user interface for dispatcher handling. Alternatively, you can use commands allowing you to manage the dispatcher(s) without using the graphical user interface.

Prerequisites

- The `Keys.ini` file is available. The file is created and maintained centrally using the SAP Identity Management Keys Utility and then distributed manually to necessary locations.
- On Windows, the administrator user must have permissions to edit the Windows Registry.
- The system administrator must limit the operating system user running the dispatcher to access SAP Identity Management installation directory, jobs and processes directories, only. See Preventing Path Traversal Attacks.

Context

The utility is available on the installation set for `Runtime components`, and its directory is `<IdM install directory>\Identity_Center` (by default after installation `<drive>:\usr\sap\idm\Identity Center`).

To manage dispatchers using the utility's graphical user interface, proceed with the following steps:

Procedure

1. From a command prompt, navigate to the directory `<drive>:\usr\sap\idm\Identity Center`.

   > **Note**
   >
   > Run the command prompt as the administrator on Microsoft Windows.

2. Start the utility user interface by executing the command **`dispatcherutil gui`** (use the file `dispatcherutil.bat` for Microsoft Windows).

   This opens the *SAP Identity Management Dispatcher Utility* dialog box (the graphical user interface).
3. To set a default dispatcher, select it from the dispatcher list and choose *Set Default*.
4. You can choose *Start* from the menu on the right (or select *Dispatcher* > *Start* from the main menu) to start the created and installed dispatcher service. Both the service state and the status of the dispatcher will change to *Running*. You may have to choose *Refresh* (or select *File* > *Refresh* from the main menu) to update the fields.

   By default, the dispatcher is started automatically each time the system is started.

5. Once the dispatcher is up and running, you have the possibility to:

Option	Description
Suspend the dispatcher	Select the running dispatcher you want to suspend from the list and choose the *Suspend* button from the menu on the right (alternatively, select *Dispatcher* > *Suspend* from the main menu). When suspended, the dispatcher service will still be running (state), but its processing is suspended (status). **Note** The *Suspend* button is not visible if the dispatcher is already suspended (you will then only see the *Resume* button).
Resume the dispatcher	Select the suspended dispatcher you want to resume from the list and choose the *Resume* button from the menu on the right (alternatively, select *Dispatcher* > *Resume* from the main menu). When resumed, the dispatcher service is running and processing (both its state and status are *Running*). **Note** The *Resume* button is not visible if the dispatcher is already running (you will then only see the *Suspend* button).
Stop the dispatcher	Select the dispatcher you want to stop from the list and choose the *Stop* button from the menu on the right (alternatively, select *Dispatcher* > *Stop* from the main menu).
Test the dispatcher	Select the dispatcher you want to test from the list and choose the *Test* button from the menu on the right. **Note** The dispatcher must be stopped (not running) before it can be tested. To abort the test execution in the command prompt, press CTRL + C.
Uninstall the dispatcher	Select the dispatcher you want to uninstall from the list and choose the *Uninstall* button from the menu on the right (alternatively, select *Dispatcher* > *Uninstall* from the main menu). **Note** The dispatcher must be stopped (not running) before it can be uninstalled.
Delete the dispatcher	Select the dispatcher you want to delete from the list and choose the *Delete* button from the menu on the right (alternatively, select *File* > *Delete* from the main menu). Deleting the dispatcher will also delete the generated dispatcher files. **Note** The dispatcher must be stopped (not running) before it can be deleted.

Option	Description
	Note Deleting a dispatcher will remove any reference to it (e.g. from jobs) as well. You have to reconfigure the dispatcher for the affected jobs.
Regenerate the dispatcher scripts	From the dispatcher list, select the dispatcher you want to regenerate the scripts for and select *Dispatcher* > *Regenerate Scripts* from the main menu). You would normally regenerate the scripts for a dispatcher after a configuration change.

6. You can create as many dispatchers as you need, which will be listed in the dispatcher list. To update the list and the displayed dispatcher properties, choose the *Refresh* button from the menu on the right or select *File* > *Refresh* from the main menu. To exit the utility and close its graphical user interface, select *File* > *Exit* from the main menu.

> **Note**
>
> Keep in mind that, when installing the Identity Management dispatcher, the corresponding Windows Service will be started with default recovery actions *Take no action*. This will prevent services to recover automatically in case the database connection got temporarily lost. Based on your configuration requirements, you can change the action to *Restart the Service* with an appropriate restart interval or choose any other available recovery actions.

3.2.2.4.1 Using Commands to Manage the Dispatcher(s)

A set of commands is available with SAP Identity Management Dispatcher Utility, allowing you to manage the dispatcher(s) without using the graphical user interface.

The following set of commands is available:

> **Note**
>
> From a command prompt, navigate to the directory `<drive>:\usr\sap\idm\Identity Center`. Use the file `dispatcherutil.bat` for Microsoft Windows.

> **Note**
>
> Run the command prompt as administrator.

Command	Description
`dispatcherutil`	Displays the usage information for the utility.
`dispatcherutil test <dispatcher name>`	Dispatcher with a given name is tested to verify the dispatcher configuration. This will verify that the dispatcher

Command	Description
	is able to start. Verify that no error messages are displayed during the process. Abort the test execution by pressing CTRL + C.
`dispatcherutil set_default <dispatcher name>`	Sets an installed dispatcher as the default one.
`dispatcherutil start <dispatcher name>`	Starts the installed dispatcher with the given name.
`dispatcherutil suspend <dispatcher name>`	Suspends a running dispatcher. The dispatcher service will still be running, but its processing is on hold (suspended).
`dispatcherutil resume <dispatcher name>`	Resumes a suspended dispatcher. The dispatcher service will then be running and processing.
`dispatcherutil stop <dispatcher name>`	Immediately stops the running dispatcher with the given name (hard stop).
`dispatcherutil softstop <dispatcher name>`	Stops the running dispatcher with the given name, when the ongoing processes handled by the dispatcher have completed (soft stop).
`dispatcherutil uninstall <dispatcher name>`	Uninstalls the stopped dispatcher with the given name.
`dispatcherutil delete <dispatcher name>`	Deletes the stopped dispatcher with the given name. The belonging service script files and the property file of the given dispatcher will also be deleted.
`dispatcherutil list`	Lists all available dispatchers in the dispatcher list.
`dispatcherutil gui`	Opens the *SAP Identity Management Dispatcher Utility* dialog box (the graphical user interface).
`dispatcherutil set_jdbc_url <JDBC URL>`	Defines the connection string to access the Identity Management database for the `<prefix>_rt` user. Note that the JDBC URL must be enclosed in double quotes ("").

3.2.3 Updating Identity Management Developer Studio Service

Context

To update the Identity Management Developer Studio service, proceed as follows:

Procedure

1. Download and deploy the new version of the Identity Management Developer Studio service as described in *Deploying the Identity Management Developer Studio Service*.
2. Review the Java system properties as described in *Configuring the Java System Properties*, and verify that the properties are still defined and valid.

> **Note**
>
> If you are experiencing issues with the service after deployment, try uninstalling the deployed version and then re-deploying. To uninstall (undeploy) the service SCA file, you can use Telnet (see *Undeploying Using Telnet*).

Related Information

Deploying the Identity Management Developer Studio Service [page 220]
Configuring the Java System Properties [page 226]
Undeploying Using Telnet [page 229]

3.2.3.1 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)

3.2.3.1.1 Using the Software Update Manager (SUM) 1.0

The Software Update Manager (SUM) is a multi-purpose tool that supports various processes, such as performing a release upgrade, installing enhancement packages, applying Support Package Stacks, installing add-ons, or updating single components on SAP NetWeaver.

Prerequisites

- Make sure that the latest version of Software Update Manager 1.0 is downloaded and available on your SAP NetWeaver AS for Java. Software Update Manager 1.0 is part of the Software Logistics Toolset delivery and available for download from SAP Software Download Center.

You can download the SUM archive from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Download SUM* > *SOFTWARE UPDATE MANAGER 1.0* > *SUPPORT PACKAGE PATCHES* > `<your OS>`.

- You can access the SUM documentation from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Software Update Manager (SUM) scenarios* > *Software Update/Upgrade with SUM 1.0 SP*`<Version>` > *Guides for SUM 1.0 SP*`<Version>`
  For SAP NetWeaver AS for Java, there are specific guides for the combinations of operating systems and databases.
- Before running and using the SUM 1.0, you have to complete all required preparation and planning actions in the SUM 1.0 user guide.
- Make sure that the SAP system and its database are started.
- On the host where you want to start the SL Common GUI of the Software Update Manager, Java 6 or higher has to be installed.
- SAP Host Agent has been configured on your system with the minimum version required for your scenario. For more information, see *Installing or Updating SAP Host Agent* in the *Update of SAP Systems Using Software Update Manager* guide that is relevant for your operating system and database.

Context

In the case of SAP Identity Management, you need SUM in the following processes:

- **SAP Identity Management installation with SWPM**
  In this case, you need SUM to deploy AS Java Extensions (SCA files) on the SAP NetWeaver AS Java system as a prerequisite for the following two components:
  - SAP Identity Management User Interface for HTML5

  For more information about the SCA files, see Prerequisites and Dependencies Between Deployable Components [page 25]
- **SAP Identity Management manual update** (that is, without using SWPM)
  In this case, you need SUM to deploy the new version of SAP Identity Management components that are deployed on SAP NetWeaver AS Java system:
  - SAP Identity Management Developer Studio Service
  - SAP Identity Management User Interface
  - SAP Identity Management REST Interface version 2
  - SAP Identity Management User Interface for HTML5
  - SAP Identity Management Portal Content
  - Identity Federation

  For more information about deploying a new version of SAP Identity Management components, see the topics under Updating SAP Identity Management Components [page 199] section.

To start and use the Software Update Manager 1.0, proceed as follows:

Procedure

1. Get the Software Update Manager running on the primary application server instance, as described in Running the Software Update Manager [page 30]
2. Start the SL Common GUI of the Software Update Manager, as described in Starting the SL Common GUI of the Software Update Manager [page 31].
3. Logon to the Software Update Manager and deploy the SCA file(s), as described in Deploying Using the Software Update Manager [page 32].

3.2.3.1.1.1 Running the Software Update Manager

Context

To run the Software Update Manager on the application server (primary application server instance), proceed as follows:

Procedure

1. Log on to the host on which the primary application server instance is running as user <SAPSID>adm (instance user).
2. Unpack the Software Update Manager package (<archive>.SAR) with the following command:
   - for Microsoft Windows:

     ```
     SAPCAR –xf <download directory>\<path>\<Archive>.SAR -R
     <DRIVE>:\usr\sap\<sapsid>
     ```

     This command creates the directory SUM under the `<DRIVE>:\usr\sap\<sapsid>` directory. You can also specify a directory other than `<DRIVE>:\usr\sap\<sapsid>`. In the following, the directory `\<path to SUM directory>\SUM` is referred to as <update directory>.

   > **Note**
   >
   > The complete path to the `SUM` folder must not exceed 30 characters.

3. Start the Software Update Manager entering the following command:
   - for Microsoft Windows:

     ```
     <DRIVE>:\<update directory>\STARTUP.BAT confighostagent
     ```

For Microsoft Windows and MS SQL Server, enter the following command:

```
<DRIVE>:\<update directory>\STARTUP.BAT confighostagent jvm6
```

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.3.1.1.2 Starting the SL Common GUI of the Software Update Manager

Context

This section describes how you start the SL Common UI and the SUM back-end process.

Procedure

1. Open a web browser window.
2. In the address bar, enter the following URL: **`https://<hostname>:1129/lmsl/sumjava/<SID>/index.html`**.

   Replace *<hostname>* with the name of the host on which the Software Update Manager is running.

   > **Note**
   >
   > If the SSL is not configured, use http instead of https at the beginning of the URL, and use port 1128: **`http://<hostname>:1128/lmsl/sumjava/<SID>/index.html`**
3. In the dialog box that appears, enter the user name **`<sid>adm`** and the password.

Results

The SAP Host Agent starts the Software Update Manager, and the SL Common GUI of the Software Update Manager is displayed in the web browser.

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.3.1.1.3 Deploying Using the Software Update Manager

Context

The Software Update Manager controls the entire procedure, from checking the system requirements and importing the necessary programs through stopping production operation until production operation is resumed. The procedure is divided up into a number of different roadmap steps. The roadmap steps are in turn divided into phases. Many phases require no user input - step through those by choosing *Next*. The successful completion of a phase is a precondition for the success of all subsequent phases.

> **Note**
>
> User actions are also required when errors occur. If an error occurs, correct it and repeat the phase in which the error has occurred. Once the phase has been repeated successfully, you can continue with the update.

To logon to the Software Update Manager and deploy the SCA file(s), do the following:

Procedure

1. Enter the user name and the password for the AS Java administrator user with which you log in to the system.
2. In the *Specify Credentials* roadmap step, specify the password for the instance user (<sapsid>adm), and then choose *Next*.
3. In the *Select Target* roadmap step, specify the path to the SCA file in the *Directory* field, then choose *Next*.
4. In the *Confirm Target* roadmap step, enter the keyword that is specified in the current *Central Software Update Manager Note* (which you can find in the Software Update Manager upgrade guide or in SAP Support Portal). Confirm the selected target system version by choosing *Next*.
5. In the *Configuration* roadmap step, provide the password of the AS Java administrator before proceeding. In this step it is also possible to specify the composition of the target release system.
6. Step through the phases requiring no user input by choosing *Next* and complete the process. Upon completing the process successfully, the important statistics are collected in a comprehensive report.

Next Steps

Every time you have used SUM, you need to either delete the `SUM` folder or rename it and keep it (if you would like, but this is not necessary). Then you have to extract a new `SUM` folder from the `SUM.SAR` file.

Use `SAPCAR.EXE` to extract the SAR file. Do the following:

1. In the command prompt, change to the directory to which you have downloaded or copied the SUM archives (the directory of the `SUM.SAR` file).
2. Start SAPCAR to extract the archive to the current directory. Enter
   `<path to sapcar.exe>\sapcar.exe -xvf SUM.SAR`
   and run the command line.
3. The `SUM.SAR` file should now be extracted and the new `SUM` folder created. You may now use SUM again.

Related Information

SAP Notes & SAP Knowledge Base Articles
Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.3.2 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: `for Windows: C:\usr\sap\IdM\Identity Center\Key\Keys.ini` **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: `for Windows: C:\usr\sap\IdM\jdbc\MSSQL2005\sqljdbc.jar` This can also be a list of paths (to several JDBC driver JAR files). List items are separated as follows: *;* in Microsoft Windows systems
`com.sap.idm.rcp.jdbcdrivers`	A list of JDBC driver names. For example, com.microsoft.sqlserver.jdbc.SQLServerDriver;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: *;* in Microsoft Windows systems

Property	Value
`com.sap.idm.rcp.dsehome`	The path relative to which the runtime engine is found. For example: `For Windows: C:\usr\sap\IdM\Identity Center` This is needed for data discovery purposes.
`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.

3.2.3.3 Undeploying Using Telnet

To undeploy the SCA files from your SAP NetWeaver AS for Java, you can use Telnet.

Context

To undeploy a file using Telnet commands, do the following:

Procedure

1. Open a Telnet connection to your SAP NetWeaver AS for Java from which you want to undeploy the application. Enter the following command (for example from a DOS prompt on Microsoft Windows): `telnet <host IP address> <port>`, where *<port>* is the Telnet port of your server.

For example, if your server installation directory is `\usr\sap\<some_three_letter_SID>\JCxx\...`, then your Telnet port should be *5xx08*. E.g. if the server installation is `\usr\sap\N73\J30\...` then the Telnet port is *53008*.

2. Log on using your SAP NetWeaver AS for Java administrator username and password.
3. When you have logged on, type the following Telnet command: `> lsc`. This will list the cluster elements.
4. Find *Server 0* and look up the value in the *ID* column. Enter your next command: `> jump X`, where *X* is this ID value.
5. Enter the following commands:

   ```
   > add deploy
   ```

   ```
   > undeploy name=<name of the component> vendor=<the vendor of the component>
   ```

   In this case, the name of the component is *idmdevstudio* and the vendor is *sap.com*, resulting in the following undeploy command:`> undeploy name=idmdevstudio vendor=sap.com`

   > ⓘ Note
   >
   > Using the command `undeploy -h`, you can get more information about the command syntax.

3.2.4 Updating Identity Management Developer Studio

Context

When updating the Identity Management Developer Studio client, you need to do this on each developer or developer administrator machine where it is installed.

> ⓘ Note
>
> Use Eclipse version *2024-09*.

You can update the Identity Management Developer Studio from the following locations:

- Eclipse update site: https://tools.hana.ondemand.com/2024-09/
  Use this option to update the Identity Management Developer Studio to the latest support package (SP) level and to apply patches for this SP.
- SAP Software Download Center: https://support.sap.com/swdc
  Use this option if your Identity Management 8.0 system is not updated to the latest SP and you want to apply patches for the Identity Management Developer Studio for your current (lower) SP.

Updating to the Latest SP Level and Applying Patches

Context

You want to update your Identity Management Developer Studio to the latest SP and to apply patches for this SP.

Procedure

1. In the Eclipse environment, from your *SAP Identity Management* perspective, select *Help* > *Check for Updates* from the main menu.

   The provided repository sites for the software are checked for updates. Available updates (if any) are displayed in the *Available Updates* dialog box.
2. Select *SAP Identity Management Developer Studio* (select the check-box in front of the name), and choose *Next >*.
3. Review any update details and confirm the update by choosing *Next >*.
4. Review the licenses and choose *I accept the terms of the license agreement*.
5. Choose *Finish*.

   The installation will proceed to self-signing of the content. Select the provided certificate (localSigning; localSigning; localSigning) and choose *OK*.
6. You will need to restart Eclipse for the changes to take effect. Choose *Yes* to restart immediately, or *No* to restart later.
7. In the tree view, expand the *Root* node and then the node for your Identity Management database. Provide the credentials for your initial administrator user for Identity Management Developer Studio to login.

Applying Patches for Lower SP Levels

Context

Your Identity Management 8.0 system is not updated to the latest SP and you want to apply patches for the Identity Management Developer Studio for your current (lower) SP.

> ⓘ Note
>
> You can only download the latest available patch for your current SP. For example, if you are running version 8.0 SP06, you can only download patch level 25.

Procedure

1. In the SAP Software Download Center, navigate to the area of SAP Identity Management 8.0 and download the `.ZIP` archive for the IDM CONFIG LM FOR ECLIPSE 8.0 component (https://support.sap.com/swdc *Software Downloads* *Support Packages & Patches* *(A-Z)* *N* *SAP NW IDENTITY MANAGEMENT* *SAP IDENTITY MANAGEMENT 8.0* *COMPRISED SOFTWARE COMPONENT VERSIONS* *IDM CONFIG LM FOR ECLIPSE 8.0* *IDMCLMECLIPSE*`<SP level>_<Patch level>-<GUID number>`*.ZIP*)
2. In your Eclipse User Interface, select *Help* *Install New Software...* from the main menu.
3. Specify the repository site where the plugin is available from. Choose *Add...* to the right of the *Work with* field.
4. 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, choose *Archive* and add the *IDMCLMECLIPSE*`<SP level>_<Patch level>-<GUID number>`*.ZIP* file you have downloaded from the SAP Software Download Center

   Choose *OK* to add the repository.
5. 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*.
6. 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).
7. Choose *Next >*.
8. Review the licenses and choose *I accept the terms of the license agreement*.
9. Choose *Finish*.
10. You will need to restart Eclipse for the changes to take effect. Choose *Yes* to restart immediately, or *No* to restart later.

3.2.5 Updating the Virtual Directory Server

Prerequisites

You should use SAP JVM, where version 8.1 (Java 1.8) is required for 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.

Context

To update the Virtual Directory Server, proceed as follows:

Procedure

1. Update the software.
   a. Stop any local services.

      > **Note**
      >
      > Deployments on SAP NetWeaver Application Server Java are not affected.

   b. Close the user interface.
   c. Update the software by running the installation job as described in *Installing the Virtual Directory Server*.

      > **Note**
      >
      > All data source templates are removed, except those prefixed with custom.

2. Update the configuration files.
   a. To update the deployed configurations, you need to open the configuration file in the user interface. The configuration file is patched to the new version.
   b. Restart any local services.
   c. Redeploy deployed configurations.

Related Information

Installing the Virtual Directory Server [page 233]

3.2.5.1 Installing the Virtual Directory Server

Prerequisites

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

Context

To install the Virtual Directory Server, 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 kit.
2. Unpack the installation set to a separate directory using the following command:

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

3. Start the installation job corresponding to your platform and supply the necessary information.

   > **Note**
   >
   > If your operating system is Windows 8, Windows Server 2012 or Windows Server 2012 R2, the .exe installation file should run in Compatibility mode for Windows 7. The installation will fail, if this condition is not met.

Related Information

SAP Software Download Center on SAP Support Portal
Command Line Switches to the Installation Job [page 234]
Starting the Virtual Directory Server on Microsoft Windows [page 235]

3.2.5.1.1 Command Line Switches to the Installation Job

You can use command line switches to the installation job to control:

- For silent install
- To specify a specific Java Virtual Machine

Silent install of the Virtual Directory Server

It is possible to start the installation job in silent mode by starting the installation job with a command line option: `<setupfile> -silent`.

When running the installation job in this mode, the installation wizard will not be displayed, and default values are used for the installation directory.

If you want to use another than the default installation directory, you can use a second command line switch: `<setupfile> -silent -P installLocation=<Path to installdir>`.

> **Note**
>
> Make sure that the path does not contain spaces if you install on a Unix system.

Specifying a specific Java Virtual Machine

If there are more than one Java Virtual Machines on your computer, it may be necessary to specify which of them should be used when installing the Virtual Directory Server. You can use the following command line switch: `<setupfile> -is:javahome <path to java home>`.

3.2.5.1.2 Starting the Virtual Directory Server on Microsoft Windows

How you start the Virtual Directory Server depends on the platform.

Context

To start the Virtual Directory Server on Microsoft Windows, do the following:

Procedure

From the *Start* menu, choose *Programs* > *SAP NetWeaver Identity Management* > *Virtual Directory Server* > .

3.2.6 Updating Identity Management User Interface

To update an already deployed Identity Management User Interface, download the updated SCA file and use Software Update Manager (SUM) to deploy the file as described in *Deploying the Identity Management User Interface*. The procedure is the same for the supported versions of SAP NetWeaver.

- SAP NetWeaver 7.3 SP09 or higher
- SAP NetWeaver 7.3 including Enhancement Package 1 SP06 Patch 3 or higher
- SAP NetWeaver 7.4 SP02 or higher

- SAP NetWeaver 7.5 SP08 or higher

Related Information

Deploying Identity Management User Interface [page 236]

3.2.6.1 Deploying Identity Management User Interface

Context

To deploy the Identity Management User Interface, proceed as follows:

Procedure

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

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

   The `IDMIC<version>.SCA` file is now ready to be deployed.

   You can use Software Update Manager (SUM) to deploy the Identity Management User Interface.

Related Information

SAP Software Download Center on SAP Support Portal
Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.6.1.1 Using the Software Update Manager (SUM) 1.0

The Software Update Manager (SUM) is a multi-purpose tool that supports various processes, such as performing a release upgrade, installing enhancement packages, applying Support Package Stacks, installing add-ons, or updating single components on SAP NetWeaver.

Prerequisites

- Make sure that the latest version of Software Update Manager 1.0 is downloaded and available on your SAP NetWeaver AS for Java. Software Update Manager 1.0 is part of the Software Logistics Toolset delivery and available for download from SAP Software Download Center.
  You can download the SUM archive from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Download SUM* *SOFTWARE UPDATE MANAGER 1.0* *SUPPORT PACKAGE PATCHES* `<your OS>`.
- You can access the SUM documentation from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Software Update Manager (SUM) scenarios* *Software Update/Upgrade with SUM 1.0 SP*`<Version>` *Guides for SUM 1.0 SP*`<Version>`
  For SAP NetWeaver AS for Java, there are specific guides for the combinations of operating systems and databases.
- Before running and using the SUM 1.0, you have to complete all required preparation and planning actions in the SUM 1.0 user guide.
- Make sure that the SAP system and its database are started.
- On the host where you want to start the SL Common GUI of the Software Update Manager, Java 6 or higher has to be installed.
- SAP Host Agent has been configured on your system with the minimum version required for your scenario. For more information, see *Installing or Updating SAP Host Agent* in the *Update of SAP Systems Using Software Update Manager* guide that is relevant for your operating system and database.

Context

In the case of SAP Identity Management, you need SUM in the following processes:

- **SAP Identity Management installation with SWPM**
  In this case, you need SUM to deploy AS Java Extensions (SCA files) on the SAP NetWeaver AS Java system as a prerequisite for the following two components:
  - SAP Identity Management User Interface for HTML5

  For more information about the SCA files, see Prerequisites and Dependencies Between Deployable Components [page 25]
- **SAP Identity Management manual update** (that is, without using SWPM)
  In this case, you need SUM to deploy the new version of SAP Identity Management components that are deployed on SAP NetWeaver AS Java system:
  - SAP Identity Management Developer Studio Service

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

For more information about deploying a new version of SAP Identity Management components, see the topics under Updating SAP Identity Management Components [page 199] section.

To start and use the Software Update Manager 1.0, proceed as follows:

Procedure

1. Get the Software Update Manager running on the primary application server instance, as described in Running the Software Update Manager [page 30]
2. Start the SL Common GUI of the Software Update Manager, as described in Starting the SL Common GUI of the Software Update Manager [page 31].
3. Logon to the Software Update Manager and deploy the SCA file(s), as described in Deploying Using the Software Update Manager [page 32].

3.2.6.1.1.1 Running the Software Update Manager

Context

To run the Software Update Manager on the application server (primary application server instance), proceed as follows:

Procedure

1. Log on to the host on which the primary application server instance is running as user <SAPSID>adm (instance user).
2. Unpack the Software Update Manager package (<archive>.SAR) with the following command:
   - for Microsoft Windows:

     ```
     SAPCAR –xf <download directory>\<path>\<Archive>.SAR -R
     <DRIVE>:\usr\sap\<sapsid>
     ```

     This command creates the directory SUM under the `<DRIVE>:\usr\sap\<sapsid>` directory. You can also specify a directory other than `<DRIVE>:\usr\sap\<sapsid>`. In the following, the directory `\<path to SUM directory>\SUM` is referred to as <update directory>.

> **Note**
>
> The complete path to the `SUM` folder must not exceed 30 characters.

3. Start the Software Update Manager entering the following command:
   - for Microsoft Windows:

     ```
     <DRIVE>:\<update directory>\STARTUP.BAT confighostagent
     ```

     For Microsoft Windows and MS SQL Server, enter the following command:

     ```
     <DRIVE>:\<update directory>\STARTUP.BAT confighostagent jvm6
     ```

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.6.1.1.2 Starting the SL Common GUI of the Software Update Manager

Context

This section describes how you start the SL Common UI and the SUM back-end process.

Procedure

1. Open a web browser window.
2. In the address bar, enter the following URL: **`https://<hostname>:1129/lmsl/sumjava/<SID>/index.html`**.

   Replace *<hostname>* with the name of the host on which the Software Update Manager is running.

   > **Note**
   >
   > If the SSL is not configured, use http instead of https at the beginning of the URL, and use port 1128: **`http://<hostname>:1128/lmsl/sumjava/<SID>/index.html`**

3. In the dialog box that appears, enter the user name **`<sid>adm`** and the password.

Results

The SAP Host Agent starts the Software Update Manager, and the SL Common GUI of the Software Update Manager is displayed in the web browser.

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.6.1.1.3 Deploying Using the Software Update Manager

Context

The Software Update Manager controls the entire procedure, from checking the system requirements and importing the necessary programs through stopping production operation until production operation is resumed. The procedure is divided up into a number of different roadmap steps. The roadmap steps are in turn divided into phases. Many phases require no user input - step through those by choosing *Next*. The successful completion of a phase is a precondition for the success of all subsequent phases.

> ⓘ Note
>
> User actions are also required when errors occur. If an error occurs, correct it and repeat the phase in which the error has occurred. Once the phase has been repeated successfully, you can continue with the update.

To logon to the Software Update Manager and deploy the SCA file(s), do the following:

Procedure

1. Enter the user name and the password for the AS Java administrator user with which you log in to the system.
2. In the *Specify Credentials* roadmap step, specify the password for the instance user (<sapsid>adm), and then choose *Next*.
3. In the *Select Target* roadmap step, specify the path to the SCA file in the *Directory* field, then choose *Next*.
4. In the *Confirm Target* roadmap step, enter the keyword that is specified in the current *Central Software Update Manager Note* (which you can find in the Software Update Manager upgrade guide or in SAP Support Portal). Confirm the selected target system version by choosing *Next*.
5. In the *Configuration* roadmap step, provide the password of the AS Java administrator before proceeding. In this step it is also possible to specify the composition of the target release system.

6. Step through the phases requiring no user input by choosing *Next* and complete the process. Upon completing the process successfully, the important statistics are collected in a comprehensive report.

Next Steps

Every time you have used SUM, you need to either delete the `SUM` folder or rename it and keep it (if you would like, but this is not necessary). Then you have to extract a new `SUM` folder from the `SUM.SAR` file.

Use `SAPCAR.EXE` to extract the SAR file. Do the following:

1. In the command prompt, change to the directory to which you have downloaded or copied the SUM archives (the directory of the `SUM.SAR` file).
2. Start SAPCAR to extract the archive to the current directory. Enter
   `<path to sapcar.exe>\sapcar.exe -xvf SUM.SAR`
   and run the command line.
3. The `SUM.SAR` file should now be extracted and the new `SUM` folder created. You may now use SUM again.

Related Information

SAP Notes & SAP Knowledge Base Articles
Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.7 Updating the REST Interface Version 2

Context

To update an already deployed Identity Management REST Interface Version 2 component, proceed as follows:

> **Note**
>
> The SCA file for the Identity Management REST Interface Version 2 must be on the same SP level as SAP Identity Management (and its User Interface). Updating the Identity Management REST Interface Version 2 to a new SP version requires update of the other component to the same SP version first.

Procedure

1. Update the Identity Management REST Interface Version 2 by deploying the new SCA file as described in *Deploying the REST Interface Version 2*.

It is not necessary to update the configuration after update of the REST Interface Version 2 component.

2. Make sure your Identity Management REST Interface Version 2 uses HTTPS communication.

   As of SAP Identity Management 8.0 SP06 and higher, Identity Management REST Interface v2 requires HTTPS communication by default. If you have used Identity Management REST Interface v2 over HTTPS in version 8.0 SP05 or lower, you do not need to do anything.

   If you have used Identity Management REST Interface v2 over HTTP in version 8.0 SP05 or lower, when updating to version 8.0 SP06 or higher, you will get the following error message: "For security reasons, SAP Identity Management requires HTTPS communication by default. In case you need HTTP, please contact your SAP Identity Management Administrator for assistance." You have the following options:

   - (Required) To allow 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)
   - To allow HTTP communication - For more information how to configure HTTP communication, see Configuring the Java System Properties [page 226]

Related Information

Deploying the REST Interface Version 2 [page 242]

3.2.7.1 Deploying the REST Interface Version 2

Prerequisites

Before you deploy the SAP Identity Management REST Interface Version 2, make sure that the following prerequisites are fulfilled:

- One of the following SAP NetWeaver versions must be installed and licensed:
  - SAP NetWeaver 7.3 SP09 or higher
  - SAP NetWeaver 7.3 including Enhancement Package 1 SP06 Patch 3 or higher
  - SAP NetWeaver 7.4 SP02 or higher
  - SAP NetWeaver 7.5 SP08 or higher
- SAP Identity Management Identity Center 8.0 or higher must be correctly installed and licensed.
- SAP Identity Management User Interface 8.0 or higher needs to be correctly installed and configured.
- You require the SAPCAR archiving tool to be able to unpack software component archives (`*.SAR` files).

Context

To deploy the REST Interface Version 2, 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 kit for the REST component.
2. Unpack the installation kit using the following command:

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

   > ⓘ Note
   >
   > Make sure that the SCA file for the REST Interface Version 2 has the same SP version as the SAP Identity Management and its User Interface. The SCA file name is `IDMREST<IdM SP version>_<IdM Patch version>.sca`. For example, for SAP Identity Management 8.0 SP00 (Patch 0), the file name is `IDMREST00_0.sca`.
3. Use Software Update Manager (SUM) to deploy the SCA file on your SAP NetWeaver AS for Java where the SAP Identity Management User Interface is deployed.

Related Information

SAP Software Download Center on SAP Support Portal

3.2.7.1.1 Using the Software Update Manager (SUM) 1.0

The Software Update Manager (SUM) is a multi-purpose tool that supports various processes, such as performing a release upgrade, installing enhancement packages, applying Support Package Stacks, installing add-ons, or updating single components on SAP NetWeaver.

Prerequisites

- Make sure that the latest version of Software Update Manager 1.0 is downloaded and available on your SAP NetWeaver AS for Java. Software Update Manager 1.0 is part of the Software Logistics Toolset delivery and available for download from SAP Software Download Center.
  You can download the SUM archive from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Download SUM* *SOFTWARE UPDATE MANAGER 1.0* *SUPPORT PACKAGE PATCHES* `<your OS>`.

- You can access the SUM documentation from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Software Update Manager (SUM) scenarios* *Software Update/Upgrade with SUM 1.0 SP*<Version> *Guides for SUM 1.0 SP*<Version>
  For SAP NetWeaver AS for Java, there are specific guides for the combinations of operating systems and databases.
- Before running and using the SUM 1.0, you have to complete all required preparation and planning actions in the SUM 1.0 user guide.
- Make sure that the SAP system and its database are started.
- On the host where you want to start the SL Common GUI of the Software Update Manager, Java 6 or higher has to be installed.
- SAP Host Agent has been configured on your system with the minimum version required for your scenario. For more information, see *Installing or Updating SAP Host Agent* in the *Update of SAP Systems Using Software Update Manager* guide that is relevant for your operating system and database.

Context

In the case of SAP Identity Management, you need SUM in the following processes:

- **SAP Identity Management installation with SWPM**
  In this case, you need SUM to deploy AS Java Extensions (SCA files) on the SAP NetWeaver AS Java system as a prerequisite for the following two components:
  - SAP Identity Management User Interface for HTML5

  For more information about the SCA files, see Prerequisites and Dependencies Between Deployable Components [page 25]
- **SAP Identity Management manual update** (that is, without using SWPM)
  In this case, you need SUM to deploy the new version of SAP Identity Management components that are deployed on SAP NetWeaver AS Java system:
  - SAP Identity Management Developer Studio Service
  - SAP Identity Management User Interface
  - SAP Identity Management REST Interface version 2
  - SAP Identity Management User Interface for HTML5
  - SAP Identity Management Portal Content
  - Identity Federation

  For more information about deploying a new version of SAP Identity Management components, see the topics under Updating SAP Identity Management Components [page 199] section.

To start and use the Software Update Manager 1.0, proceed as follows:

Procedure

1. Get the Software Update Manager running on the primary application server instance, as described in Running the Software Update Manager [page 30]
2. Start the SL Common GUI of the Software Update Manager, as described in Starting the SL Common GUI of the Software Update Manager [page 31].

3. Logon to the Software Update Manager and deploy the SCA file(s), as described in Deploying Using the Software Update Manager [page 32].

3.2.7.1.1.1 Running the Software Update Manager

Context

To run the Software Update Manager on the application server (primary application server instance), proceed as follows:

Procedure

1. Log on to the host on which the primary application server instance is running as user <SAPSID>adm (instance user).
2. Unpack the Software Update Manager package (<archive>.SAR) with the following command:
   - for Microsoft Windows:

     ```
     SAPCAR –xf <download directory>\<path>\<Archive>.SAR -R
     <DRIVE>:\usr\sap\<sapsid>
     ```

     This command creates the directory SUM under the `<DRIVE>:\usr\sap\<sapsid>` directory. You can also specify a directory other than `<DRIVE>:\usr\sap\<sapsid>`. In the following, the directory `\<path to SUM directory>\SUM` is referred to as <update directory>.

   > **Note**
   >
   > The complete path to the `SUM` folder must not exceed 30 characters.

3. Start the Software Update Manager entering the following command:
   - for Microsoft Windows:

     ```
     <DRIVE>:\<update directory>\STARTUP.BAT confighostagent
     ```

     For Microsoft Windows and MS SQL Server, enter the following command:

     ```
     <DRIVE>:\<update directory>\STARTUP.BAT confighostagent jvm6
     ```

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.7.1.1.2 Starting the SL Common GUI of the Software Update Manager

Context

This section describes how you start the SL Common UI and the SUM back-end process.

Procedure

1. Open a web browser window.
2. In the address bar, enter the following URL: **`https://<hostname>:1129/lmsl/sumjava/<SID>/index.html`**.

   Replace *<hostname>* with the name of the host on which the Software Update Manager is running.

   > ⓘ Note
   >
   > If the SSL is not configured, use http instead of https at the beginning of the URL, and use port 1128: **`http://<hostname>:1128/lmsl/sumjava/<SID>/index.html`**
3. In the dialog box that appears, enter the user name **`<sid>adm`** and the password.

Results

The SAP Host Agent starts the Software Update Manager, and the SL Common GUI of the Software Update Manager is displayed in the web browser.

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.7.1.1.3 Deploying Using the Software Update Manager

Context

The Software Update Manager controls the entire procedure, from checking the system requirements and importing the necessary programs through stopping production operation until production operation is resumed. The procedure is divided up into a number of different roadmap steps. The roadmap steps are in turn divided into phases. Many phases require no user input - step through those by choosing *Next*. The successful completion of a phase is a precondition for the success of all subsequent phases.

> **Note**
>
> User actions are also required when errors occur. If an error occurs, correct it and repeat the phase in which the error has occurred. Once the phase has been repeated successfully, you can continue with the update.

To logon to the Software Update Manager and deploy the SCA file(s), do the following:

Procedure

1. Enter the user name and the password for the AS Java administrator user with which you log in to the system.
2. In the *Specify Credentials* roadmap step, specify the password for the instance user (<sapsid>adm), and then choose *Next*.
3. In the *Select Target* roadmap step, specify the path to the SCA file in the *Directory* field, then choose *Next*.
4. In the *Confirm Target* roadmap step, enter the keyword that is specified in the current *Central Software Update Manager Note* (which you can find in the Software Update Manager upgrade guide or in SAP Support Portal). Confirm the selected target system version by choosing *Next*.
5. In the *Configuration* roadmap step, provide the password of the AS Java administrator before proceeding. In this step it is also possible to specify the composition of the target release system.
6. Step through the phases requiring no user input by choosing *Next* and complete the process. Upon completing the process successfully, the important statistics are collected in a comprehensive report.

Next Steps

Every time you have used SUM, you need to either delete the `SUM` folder or rename it and keep it (if you would like, but this is not necessary). Then you have to extract a new `SUM` folder from the `SUM.SAR` file.

Use `SAPCAR.EXE` to extract the SAR file. Do the following:

1. In the command prompt, change to the directory to which you have downloaded or copied the SUM archives (the directory of the `SUM.SAR` file).

2. Start SAPCAR to extract the archive to the current directory. Enter
   `<path to sapcar.exe>\sapcar.exe -xvf SUM.SAR`
   and run the command line.
3. The `SUM.SAR` file should now be extracted and the new `SUM` folder created. You may now use SUM again.

Related Information

SAP Notes & SAP Knowledge Base Articles
Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.8 Updating the Identity Management User Interface for HTML5

Context

To update an already deployed Identity Management User Interface for HTML5 component, proceed as follows:

> **Note**
>
> The SCA file for the Identity Management User Interface for HTML5 must be on the same SP level as SAP Identity Management (and its User Interface) and SAP Identity Management REST Interface Version 2. Updating the Identity Management User Interface for HTML5 to a new SP version requires the upgrading of the other components to the same SP version first.

Procedure

1. If a newer version of the package containing the predefined forms for the Identity Management User Interface for HTML5 is available, import the package to the Identity Management Developer Studio and configure the solution as described in *Adding the Predefined Forms and Configuring the Solution* and its subsections.

   > **Note**
   >
   > Importing the newer version of the package will overwrite the contents of the existing package.

2. Update the Identity Management User Interface for HTML5 by deploying the new SCA file as described in *Deploying the Identity Management User Interface for HTML5*.

Related Information

Adding the Predefined Forms and Configuring the Solution [page 177]
Deploying the Identity Management User Interface for HTML5 [page 249]

3.2.8.1 Deploying the Identity Management User Interface for HTML5

Context

To deploy the Identity Management User Interface for HTML5, 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 kit for the the Identity Management User Interface for HTML5 component.
2. Unpack the installation kit using the following command:

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

   > **Note**
   >
   > Make sure that the SCA file for the Identity Management User Interface for HTML5 has the same SP version as the SAP Identity Management (and its user interface) and the SAP Identity Management REST Interface Version 2. The SCA file name is `IDMUI5 <IdM SP version>_<IdM Patch version>.sca`. For example, for SAP Identity Management 8.0 SP00 (Patch 0), the file name is `IDMUI500_0.sca`.

3. Use the Software Update Manager (SUM) to deploy the Identity Management User Interface for HTML5 (the `.SCA` file) on your SAP NetWeaver AS for Java where both the Identity Management REST Interface Version 2 and the Identity Management User Interface are deployed.

Related Information

SAP Software Download Center on SAP Support Portal

3.2.8.1.1 Using the Software Update Manager (SUM) 1.0

The Software Update Manager (SUM) is a multi-purpose tool that supports various processes, such as performing a release upgrade, installing enhancement packages, applying Support Package Stacks, installing add-ons, or updating single components on SAP NetWeaver.

Prerequisites

- Make sure that the latest version of Software Update Manager 1.0 is downloaded and available on your SAP NetWeaver AS for Java. Software Update Manager 1.0 is part of the Software Logistics Toolset delivery and available for download from SAP Software Download Center.
  You can download the SUM archive from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Download SUM* *SOFTWARE UPDATE MANAGER 1.0* *SUPPORT PACKAGE PATCHES* `<your OS>`.
- You can access the SUM documentation from the main Software Logistics Toolset page at: https://support.sap.com/en/tools/software-logistics-tools.html *Software Update Manager (SUM) scenarios* *Software Update/Upgrade with SUM 1.0 SP*`<Version>` *Guides for SUM 1.0 SP*`<Version>`
  For SAP NetWeaver AS for Java, there are specific guides for the combinations of operating systems and databases.
- Before running and using the SUM 1.0, you have to complete all required preparation and planning actions in the SUM 1.0 user guide.
- Make sure that the SAP system and its database are started.
- On the host where you want to start the SL Common GUI of the Software Update Manager, Java 6 or higher has to be installed.
- SAP Host Agent has been configured on your system with the minimum version required for your scenario. For more information, see *Installing or Updating SAP Host Agent* in the *Update of SAP Systems Using Software Update Manager* guide that is relevant for your operating system and database.

Context

In the case of SAP Identity Management, you need SUM in the following processes:

- **SAP Identity Management installation with SWPM**
  In this case, you need SUM to deploy AS Java Extensions (SCA files) on the SAP NetWeaver AS Java system as a prerequisite for the following two components:
  - SAP Identity Management User Interface for HTML5

  For more information about the SCA files, see Prerequisites and Dependencies Between Deployable Components [page 25]
- **SAP Identity Management manual update** (that is, without using SWPM)
  In this case, you need SUM to deploy the new version of SAP Identity Management components that are deployed on SAP NetWeaver AS Java system:
  - SAP Identity Management Developer Studio Service

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

For more information about deploying a new version of SAP Identity Management components, see the topics under Updating SAP Identity Management Components [page 199] section.

To start and use the Software Update Manager 1.0, proceed as follows:

Procedure

1. Get the Software Update Manager running on the primary application server instance, as described in Running the Software Update Manager [page 30]
2. Start the SL Common GUI of the Software Update Manager, as described in Starting the SL Common GUI of the Software Update Manager [page 31].
3. Logon to the Software Update Manager and deploy the SCA file(s), as described in Deploying Using the Software Update Manager [page 32].

3.2.8.1.1.1 Running the Software Update Manager

Context

To run the Software Update Manager on the application server (primary application server instance), proceed as follows:

Procedure

1. Log on to the host on which the primary application server instance is running as user <SAPSID>adm (instance user).
2. Unpack the Software Update Manager package (<archive>.SAR) with the following command:
   - for Microsoft Windows:

     ```
     SAPCAR –xf <download directory>\<path>\<Archive>.SAR -R
     <DRIVE>:\usr\sap\<sapsid>
     ```

     This command creates the directory SUM under the `<DRIVE>:\usr\sap\<sapsid>` directory. You can also specify a directory other than `<DRIVE>:\usr\sap\<sapsid>`. In the following, the directory `\<path to SUM directory>\SUM` is referred to as <update directory>.

> **Note**
>
> The complete path to the `SUM` folder must not exceed 30 characters.

3. Start the Software Update Manager entering the following command:
   - for Microsoft Windows:

     ```
     <DRIVE>:\<update directory>\STARTUP.BAT confighostagent
     ```

     For Microsoft Windows and MS SQL Server, enter the following command:

     ```
     <DRIVE>:\<update directory>\STARTUP.BAT confighostagent jvm6
     ```

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.8.1.1.2 Starting the SL Common GUI of the Software Update Manager

Context

This section describes how you start the SL Common UI and the SUM back-end process.

Procedure

1. Open a web browser window.
2. In the address bar, enter the following URL: **`https://<hostname>:1129/lmsl/sumjava/<SID>/index.html`**.

   Replace *<hostname>* with the name of the host on which the Software Update Manager is running.

   > **Note**
   >
   > If the SSL is not configured, use http instead of https at the beginning of the URL, and use port 1128: **`http://<hostname>:1128/lmsl/sumjava/<SID>/index.html`**

3. In the dialog box that appears, enter the user name **`<sid>adm`** and the password.

Results

The SAP Host Agent starts the Software Update Manager, and the SL Common GUI of the Software Update Manager is displayed in the web browser.

Related Information

Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.8.1.1.3 Deploying Using the Software Update Manager

Context

The Software Update Manager controls the entire procedure, from checking the system requirements and importing the necessary programs through stopping production operation until production operation is resumed. The procedure is divided up into a number of different roadmap steps. The roadmap steps are in turn divided into phases. Many phases require no user input - step through those by choosing *Next*. The successful completion of a phase is a precondition for the success of all subsequent phases.

> ⓘ Note
>
> User actions are also required when errors occur. If an error occurs, correct it and repeat the phase in which the error has occurred. Once the phase has been repeated successfully, you can continue with the update.

To logon to the Software Update Manager and deploy the SCA file(s), do the following:

Procedure

1. Enter the user name and the password for the AS Java administrator user with which you log in to the system.
2. In the *Specify Credentials* roadmap step, specify the password for the instance user (<sapsid>adm), and then choose *Next*.
3. In the *Select Target* roadmap step, specify the path to the SCA file in the *Directory* field, then choose *Next*.
4. In the *Confirm Target* roadmap step, enter the keyword that is specified in the current *Central Software Update Manager Note* (which you can find in the Software Update Manager upgrade guide or in SAP Support Portal). Confirm the selected target system version by choosing *Next*.
5. In the *Configuration* roadmap step, provide the password of the AS Java administrator before proceeding. In this step it is also possible to specify the composition of the target release system.

6. Step through the phases requiring no user input by choosing *Next* and complete the process. Upon completing the process successfully, the important statistics are collected in a comprehensive report.

Next Steps

Every time you have used SUM, you need to either delete the `SUM` folder or rename it and keep it (if you would like, but this is not necessary). Then you have to extract a new `SUM` folder from the `SUM.SAR` file.

Use `SAPCAR.EXE` to extract the SAR file. Do the following:

1. In the command prompt, change to the directory to which you have downloaded or copied the SUM archives (the directory of the `SUM.SAR` file).
2. Start SAPCAR to extract the archive to the current directory. Enter
   `<path to sapcar.exe>\sapcar.exe -xvf SUM.SAR`
   and run the command line.
3. The `SUM.SAR` file should now be extracted and the new `SUM` folder created. You may now use SUM again.

Related Information

SAP Notes & SAP Knowledge Base Articles
Using the Software Update Manager (SUM) 1.0 [page 29]

3.2.9 Updating IDM Connector for UWL

To update an already deployed IDM Connector for UWL, download the updated SCA file (`IDMPORTALCONT<version>.sca`) from the SAP Support Portal and deploy the file as described in *Deploying IDM Connector for UWL*.

Related Information

Deploying IDM Connector for UWL [page 255]

3.2.9.1 Deploying IDM Connector for UWL

Prerequisites

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

Context

The IDM connector for UWL is provided with SAP Identity Management as a `*.SAR` file. You can find the component with the name `IDMPORTALCONT<version>.sca` in the installation directory along with the workflow UIs or they are available for download in the SAP Software Download Center on the SAP Support Portal.

The deployment procedure is the same as for other SCAs on the AS Java. For more information, see the deployment documentation on the SAP Help Portal regarding your release.

Procedure

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

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

3. Deploy the archive on the AS Java where the SAP Identity Management workflow UIs are running.
4. If the portal is running on a remote system, deploy both the SAP Identity Management workflow UIs (`IDMIC<version>.sca`) and the IDM connector for UWL (`IDMPORTALCONT<version>.sca`) on the portal system.

Related Information

Installation and Upgrades > *A-Z Index* > *N* > *SAP NW IDENTITY MANAGEMENT*
Release 7.1
Release 7.2
Release 7.3
UWL Integration Configuration Guide

3.2.10 Downloading and Installing the Federation Software

Context

As of SAP Single Sign-On 3.0 and SAP NetWeaver Identity Management 7.2 7.2, the federation software component archive (SCA) includes the identity provider and the security token service software.

To download the federation software component archive, proceed as follows:

Procedure

1. Go to the SAP Software Download Center at https://support.sap.com/swdc.
2. In the navigation pane, choose *SAP Software Download Center* > *Support Packages and Patches*.
3. In the A-Z Index, navigate to the *S* section.
4. Navigate to the following product: *SAP SINGLE SIGN ON* > *SAP SINGLE SIGN ON 3.0* > *Comprised Software Component Versions* > *IDM FEDERATION 7.2*
5. Download `IDMFEDERATION<Version>.SCA`.
6. Deploy the SCA to the AS Java.
   You can use the *Deployment Job* view of the SAP NetWeaver Developer Studio.

Related Information

SAP Single Sign-On

SAP Identity Management 8.0

Prerequisites

As of SAP Identity Management 8.0 SP04 and higher, the federation software is delivered as `*.SAR` file.

If you are running SAP Identity Management 8.0 SP04 or higher, you require the SAPCAR archiving tool to be able to unpack software component archives (`*.SAR` files).

Procedure

1. Go to the SAP Software Download Center at https://support.sap.com/swdc.
2. In the navigation pane, choose *SAP Software Download Center* > *Software Downloads* > *Support Packages and Patches*.
3. In the A-Z Index, navigate to the *N* section.
4. Navigate to the following product: *SAP NW IDENTITY MANAGEMENT* > *SAP IDENTITY MANAGEMENT 8.0* > *Comprised Software Component Versions* > *IDM FEDERATION 7.2*
5. Depending on your SAP Identity Management 8.0 SP release, download the following:
   - For version 8.0 SP03 or lower: `IDMFEDERATION<Version>.SCA`
   - For version 8.0 SP04 or higher: `IDMFEDERATION<Version>.SAR`
6. For version 8.0 SP04 or higher, unpack the installation kit using the following command:

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

7. Deploy the `IDMFEDERATION<Version>.SCA` to the AS Java.

   You can use the *Deployment Job* view of the SAP NetWeaver Developer Studio.

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